

NSX-T Data Center 管理指南

修改日期: 2019 年 5 月 24 日
VMware NSX-T Data Center 2.3



vmware®

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

如果您对本文档有任何意见或建议, 请将反馈信息发送至:

docfeedback@vmware.com

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 © 2018, 2019 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 9

1 逻辑交换机和配置虚拟机连接 10

了解 BUM 帧复制模式 11

创建逻辑交换机 12

第 2 层桥接 13

创建网桥群集 14

创建网桥配置文件 15

创建支持网桥的第 2 层逻辑交换机 16

为 NSX Edge 上行链路创建 VLAN 逻辑交换机 17

将虚拟机连接到逻辑交换机 19

将 vCenter Server 上托管的虚拟机连接到 NSX-T Data Center 逻辑交换机 19

将单独 ESXi 上托管的虚拟机连接到 NSX-T Data Center 逻辑交换机 21

将 KVM 上托管的虚拟机连接到 NSX-T Data Center 逻辑交换机 25

测试第 2 层连接 26

2 逻辑交换机端口 30

创建逻辑交换机端口 30

监控逻辑交换机端口活动 31

3 逻辑交换机和逻辑端口的交换配置文件 32

了解 QoS 交换配置文件 33

配置自定义 QoS 交换配置文件 33

了解 IP 发现交换配置文件 35

配置 IP 发现交换配置文件 35

了解 SpoofGuard 36

配置端口地址绑定 37

配置 SpoofGuard 交换配置文件 37

了解交换机安全交换配置文件 38

配置自定义交换机安全交换配置文件 38

了解 MAC 管理交换配置文件 39

配置 MAC 管理交换配置文件 40

将自定义配置文件与逻辑交换机相关联 41

将自定义配置文件与逻辑端口相关联 42

4 Tier-1 逻辑路由器 43

创建 Tier-1 逻辑路由器 44

- 在 Tier-1 逻辑路由器上添加下行链路端口 45
- 在 Tier-0 或 Tier-1 逻辑路由器上添加 VLAN 端口 46
- 在 Tier-1 逻辑路由器上配置路由通告 46
- 配置 Tier-1 逻辑路由器静态路由 48
- 创建独立 Tier-1 逻辑路由器 50

5 Tier-0 逻辑路由器 52

- 创建 Tier-0 逻辑路由器 54
- 连接 Tier-0 和 Tier-1 55
 - 验证 Tier-0 路由器是否发现来自 Tier-1 路由器的路由 56
- 将 Tier-0 逻辑路由器连接到 NSX Edge 上行链路的 VLAN 逻辑交换机 57
 - 验证 Tier-0 逻辑路由器和 TOR 连接 59
- 添加环回路由器端口 60
- 在 Tier-0 或 Tier-1 逻辑路由器上添加 VLAN 端口 61
- 配置静态路由 62
 - 验证静态路由 63
- BGP 配置选项 65
 - 在 Tier-0 逻辑路由器上配置 BGP 66
 - 从 Tier-0 服务路由器中验证 BGP 连接 68
- 在 Tier-0 逻辑路由器上配置 BFD 70
- 在 Tier-0 逻辑路由器上启用路由重新分发 70
 - 验证南北向连接和路由重新分发 71
- 了解 ECMP 路由 73
 - 为第二个 Edge 节点添加上行链路端口 73
 - 添加第二个 BGP 邻居并启用 ECMP 路由 74
 - 验证 ECMP 路由连接 75
- 创建 IP 前缀列表 77
- 创建社区属性列表 78
- 创建路由映射 79
- 配置转发启动定时器 80

6 网络地址转换 81

- Tier-1 NAT 82
 - 在 Tier-1 路由器上配置源 NAT 82
 - 在 Tier-1 路由器上配置目标 NAT 84
 - 将 Tier-1 NAT 路由通告到上游 Tier-0 路由器 86
 - 将 Tier-1 NAT 路由通告到物理架构 87
 - 验证 Tier-1 NAT 87
- Tier-0 NAT 88
 - 在 Tier-0 路由器上配置源和目标 NAT 88
- 反射 NAT 89

在 Tier-0 或 Tier-1 逻辑路由器上配置反射 NAT 91

7 防火墙区域和防火墙规则 93

- 添加防火墙规则区域 94
- 删除防火墙规则区域 95
- 启用和禁用区域规则 95
- 启用和禁用区域日志 95
- 关于防火墙规则 96
- 添加防火墙规则 97
- 删除防火墙规则 99
- 编辑默认分布式防火墙规则 99
- 更改防火墙规则的顺序 100
- 筛选防火墙规则 100
- 为逻辑交换机网桥端口配置防火墙 101
- 配置防火墙排除列表 101
- 启用和禁用防火墙 101
- 在逻辑路由器中添加或删除防火墙规则 102

8 虚拟专用网络 103

- 配置 IPSec VPN 104
- 配置 L2VPN 107

9 管理对象、组、服务和虚拟机 109

- 创建 IP 集 109
- 创建 IP 池 110
- 创建 MAC 集 110
- 创建 NS 组 111
- 配置服务和组 112
 - 创建 NS 服务 112
- 管理虚拟机的标记 113

10 逻辑负载均衡器 114

- 负载均衡器重要概念 115
 - 缩放负载均衡器资源 115
 - 支持的负载均衡器功能 116
 - 负载均衡器拓扑 117
- 配置负载均衡器组件 118
 - 创建负载均衡器 119
 - 配置主动运行状况监控器 120
 - 配置被动运行状况监控器 123
 - 添加服务器池用于负载均衡 124

配置虚拟服务器组件 127

11 DHCP 145[创建 DHCP 服务器配置文件 145](#)[创建 DHCP 服务器 146](#)[将 DHCP 服务器连接到逻辑交换机 147](#)[将 DHCP 服务器与逻辑交换机断开连接 147](#)[创建 DHCP 中继配置文件 147](#)[创建 DHCP 中继服务 148](#)[将 DHCP 服务添加到逻辑路由器端口 148](#)**12 元数据代理 149**[添加元数据代理服务器 149](#)[将元数据代理服务器连接到逻辑交换机 150](#)[将元数据代理服务器与逻辑交换机断开连接 151](#)**13 IP 地址管理 152**[管理 IP 块 152](#)[管理 IP 块的子网 153](#)**14 NSX 策略 154**[概述 154](#)[添加实施点 155](#)[添加服务 156](#)[添加域 156](#)[配置 NSX Policy Manager 的备份 157](#)[备份 NSX Policy Manager 158](#)[还原 NSX Policy Manager 158](#)[将 vIDM 主机与 NSX Policy Manager 相关联 159](#)[管理角色分配 160](#)**15 服务插入 161**[概述 161](#)[注册服务 162](#)[部署服务实例 164](#)[配置流量重定向 165](#)[监控流量重定向 165](#)**16 NSX Cloud 166**[Cloud Service Manager 166](#)[云 166](#)

系统	173
管理隔离策略	176
如何启用或禁用隔离策略	176
禁用隔离策略时的影响	177
启用隔离策略时的影响	178
公有云的 NSX Cloud 安全组	179
载入并管理工作负载虚拟机概览	180
支持的操作系统	180
如何从 Microsoft Azure 载入工作负载虚拟机	181
如何从 AWS 载入工作负载虚拟机	182
载入工作负载虚拟机	182
在公有云中标记虚拟机	183
安装 NSX 代理	183
自动安装 NSX 代理	187
管理工作负载虚拟机	188
访问受管工作负载虚拟机	188
使用 NSX-T Data Center 和公有云标记对虚拟机分组	189
为工作负载虚拟机设置微分段	192
如何对公有云使用 NSX-T Data Center 功能	192
使用 NSX Cloud 高级功能	195
启用 Syslog 转发	195
故障排除	196
验证 NSX Cloud 组件	196
对常见问题进行故障排除	197
17 操作和管理	198
添加许可证密钥	199
管理用户帐户和基于角色的访问控制	199
更改 CLI 用户的密码	199
身份验证策略设置	200
从 vIDM 主机中获取证书指纹	201
将 vIDM 主机与 NSX-T 相关联	201
NSX Manager、vIDM 和相关组件之间的时间同步	202
基于角色的访问控制	204
管理角色分配	207
查看主体身份	208
设置证书	208
创建证书签名请求文件	209
导入 CA 证书	210
导入证书	210
创建自签名证书	211

- 替换证书 212
- 导入证书吊销列表 212
- 为 CSR 导入证书 213
- 配置设备 214
- 添加计算管理器 214
- 管理标记 215
- 搜索对象 216
- 查找远程服务器的 SSH 指纹 217
- 备份和还原 NSX Manager 218
 - 备份 NSX Manager 配置 218
 - 还原 NSX Manager 配置 220
 - 还原 NSX Controller 群集 223
- 管理设备和设备群集 225
 - 管理 NSX Manager 225
 - 管理 NSX Controller 群集 226
 - 管理 NSX Edge 群集 232
- 日志消息 236
 - 配置远程日志记录 237
 - 日志消息 ID 238
- 配置 IPFIX 239
 - 配置交换机 IPFIX 配置文件 240
 - 配置防火墙 IPFIX 收集器 241
 - ESXi IPFIX 模板 242
 - KVM IPFIX 模板 247
- 使用跟踪流跟踪数据包路径 409
- 查看端口连接信息 411
- 监控逻辑交换机端口活动 411
- 监控端口镜像会话 412
- 监控结构层节点 414
- 查看有关在虚拟机上运行的应用程序的数据 415
- 收集支持包 415
- 客户体验提升计划 416
 - 编辑客户体验提升计划配置 416

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以及如何为分层逻辑路由器设置网络。本文档还介绍了如何配置 NAT、防火墙、SpoofGuard、分组和 DHCP。

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 技术文档中使用的术语的定义，请访问 <http://www.vmware.com/support/pubs>。

逻辑交换机和配置虚拟机连接

1

NSX-T Data Center 逻辑交换机在完全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）。

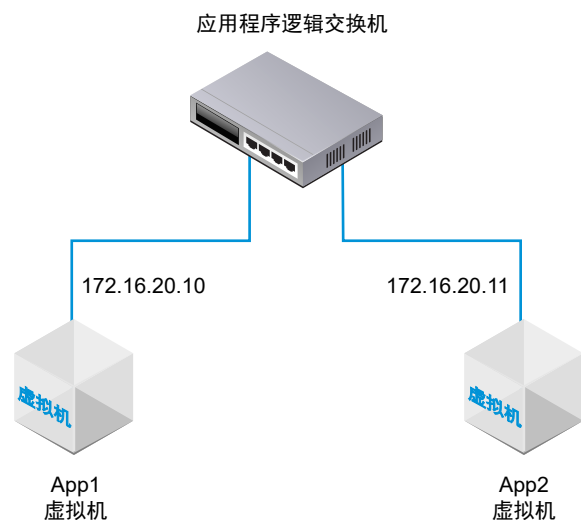
NSX Cloud 说明 如果使用 NSX Cloud，请参见[如何对公有云使用 NSX-T Data Center 功能](#)，获得自动生成的逻辑实体、支持的功能和 NSX Cloud 所需配置的列表。

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**结构层 > 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 1-1. 逻辑交换机拓扑



例如，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群集或同一主机群集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。

本章讨论了以下主题：

- 了解 BUM 帧复制模式
- 创建逻辑交换机
- 第 2 层桥接
- 为 NSX Edge 上行链路创建 VLAN 逻辑交换机
- 将虚拟机连接到逻辑交换机
- 测试第 2 层连接

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，将在与两个管理程序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管理程序。需要将给定管理程序上的虚拟机发出的 BUM 流量复制到远程管理程序，这些管理程序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 1 章 [逻辑交换机和配置虚拟机连接](#) 和了解 [BUM 帧复制模式](#)。
- 确认 NSX Controller 群集处于稳定状态。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 的 NSX Manager。
- 2 选择 **交换 > 交换机**。
- 3 单击 **添加**。
- 4 输入逻辑交换机的名称和可选描述。
- 5 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。
- 6 输入上行链路绑定策略的名称。
- 7 将 **管理状态** 设置为 **开启** 或 **关闭**。

8 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。

9 （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。

10 （可选）单击**交换配置文件**选项卡，然后选择交换配置文件。

11 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](#)。

第 2 层桥接

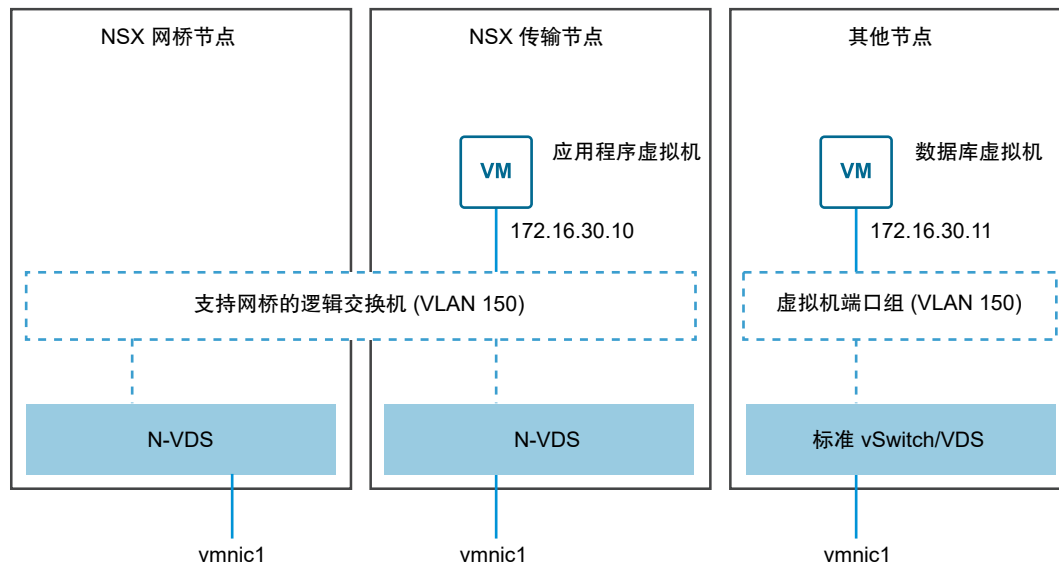
如果 NSX-T Data Center 逻辑交换机需要建立到支持 VLAN 的端口组的第 2 层连接，或者需要访问位于 NSX-T Data Center 部署外部的其他设备（如网关），您可以使用 NSX-T Data Center 第 2 层网桥。这在迁移情况下特别有用，此时，您需要在物理和虚拟工作负载之间拆分子网。

第 2 层桥接中涉及的 NSX-T Data Center 概念是网桥群集、网桥端点和网桥节点。网桥群集是高可用性 (High Availability, HA) 网桥节点集合。网桥节点是进行桥接的传输节点。用于桥接虚拟和物理部署的每个逻辑交换机具有关联的 VLAN ID。网桥端点确定网桥的物理属性，例如，网桥群集 ID 和关联的 VLAN ID。

可以使用 ESXi 主机传输节点或 NSX Edge 传输节点配置第 2 层桥接。要使用 ESXi 主机传输节点进行桥接，需要创建网桥群集。要使用 NSX Edge 传输节点进行桥接，需要创建网桥配置文件。

在以下示例中，两个 NSX-T Data Center 传输节点是同一覆盖网络传输区域的一部分。这使其 NSX 受管虚拟分布式交换机（N-VDS，以前称为主机交换机）可以连接到同一个支持网桥的逻辑交换机。

图 1-2. 网桥拓扑



左侧的传输节点属于一个网桥群集，因此，它是一个网桥节点。

由于逻辑交换机连接到一个网桥群集，因此，它称为支持网桥的逻辑交换机。要能够支持网桥，逻辑交换机必须位于覆盖网络传输区域中，而不能位于 VLAN 传输区域中。

中间传输节点不是网桥群集的一部分。它是一个常规传输节点。它可以是 KVM 或 ESXi 主机。在该图中，该节点上称为“应用程序虚拟机”的虚拟机连接到支持网桥的逻辑交换机。

右侧的节点不是 NSX-T Data Center 覆盖网络的一部分。它可能是具有虚拟机的任何管理程序（如图中所示），也可能是物理网络节点。如果非 NSX-T Data Center 节点是 ESXi 主机，您可以使用标准 vSwitch 或 vSphere Distributed Switch 进行端口连接。一个要求是，与端口连接关联的 VLAN ID 必须与支持网桥的逻辑交换机上的 VLAN ID 相匹配。此外，还会在第 2 层上进行通信，因此，两个终端设备的 IP 地址必须位于同一子网中。

如上所述，网桥的用途是在两个虚拟机之间启用第 2 层通信。在两个虚拟机之间传输流量时，流量将通过网桥节点。

注 使用在 ESXi 主机上运行的 Edge 虚拟机提供第 2 层桥接时，标准交换机或分布式交换机上在 VLAN 端发送和接收流量的端口组应处于混杂模式。为获得最佳性能，请注意以下事项：

- 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。
- 主动和备用 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，吞吐量可能会下降至 7 Gbps，因为 VLAN 流量需要同时转发至处于混杂模式的两个虚拟机。

创建网桥群集

网桥群集是一组 ESXi 主机传输节点，可以提供与逻辑交换机的第 2 层桥接。

一个网桥群集最多可以有两个 ESXi 主机传输节点作为网桥节点。通过这两个网桥节点，网桥群集将在“主动-备用”模式下提供高可用性。即使您只需要一个网桥节点，也必须创建网桥群集。创建网桥群集后，可以稍后再添加另一个网桥节点。

前提条件

- 创建至少一个 NSX-T Data Center 传输节点以用作网桥节点。
- 用作网桥节点的传输节点必须是 ESXi 主机。网桥节点不支持 KVM。
- 建议不要在网桥节点上托管任何虚拟机。
- 只能将传输节点添加到一个网桥群集中。您无法将同一传输节点添加到多个网桥群集中。

步骤

- 1 从导航面板中选择**结构层 > 节点**。
- 2 单击 **ESXi 网桥群集**选项卡。
- 3 单击**添加**。
- 4 输入名称和可选的说明。
- 5 为网桥群集选择一个传输区域。
- 6 从**可用**列中，选择传输节点并单击右箭头以将其移到**已选择**列中。
- 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群集相关联。

创建网桥配置文件

网桥配置文件使 NSX Edge 群集能够提供与逻辑交换机的第 2 层桥接。

前提条件

- 验证您的 NSX Edge 群集是否具有两个 NSX Edge 传输节点。

步骤

- 1 从导航面板中选择**结构层 > 配置文件**。
- 2 单击 **Edge 网桥配置文件**选项卡。
- 3 单击**添加**。
- 4 输入名称和可选的说明。
- 5 选择一个 NSX Edge 群集。
- 6 选择一个主节点。
- 7 选择一个备份节点。
- 8 选择一种故障切换模式。
选项为**主动**和**非主动**。
- 9 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。

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。

有关示例拓扑，请参阅图 1-2. 网桥拓扑。

前提条件

- 验证您是否有网桥群集或网桥配置文件。
- 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 从导航面板中选择 **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 **相关 > ESXi 网桥群集** 或 **相关 > Edge 网桥配置文件**。
- 5 单击 **连接**。
- 6 要连接到网桥群集，请执行以下操作
 - a 选择一个网桥群集。
 - b 输入 VLAN ID。
 - c 启用或禁用 **VLAN 上的 HA**。
 - d 单击 **连接**。
- 7 要连接到网桥配置文件，请执行以下操作
 - a 选择一个网桥配置文件。
 - b 选择一个传输区域。
 - c 输入 VLAN ID。
 - d 单击 **保存**。
- 8 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网桥群集或网桥配置文件所在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。例如，在图 1-2. 网桥拓扑 中，NSX-T Data Center 传输节点上的应用程序虚拟机应该能够 ping 通外部节点上的数据库虚拟机，反之亦然。

可以通过单击 **监控** 选项卡来监控网桥交换机上的流量。

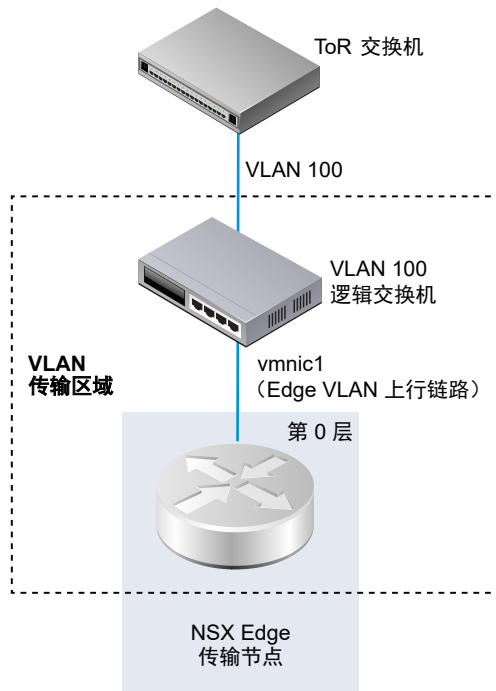
还可以使用 GET `https://192.168.110.31/api/v1/bridge-endpoints/<endpoint-id>/statistics` API 调用来查看网桥流量：

```
{
  "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"
}
```

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 NSX Controller 群集处于稳定状态。
- 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 从导航面板中选择 **网络 > 交换**。
- 3 单击 **添加**。
- 4 键入逻辑交换机的名称。
- 5 为逻辑交换机选择一个传输区域。
- 6 选择上行链路绑定策略。
- 7 对于管理状态，选择 **开启** 或 **关闭**。
- 8 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。

- 9 （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。

将虚拟机连接到逻辑交换机

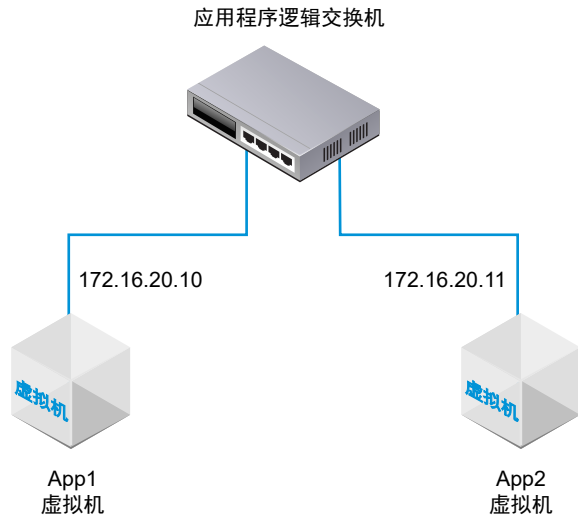
根据您的主机，将虚拟机连接到逻辑交换机的配置可能会有所不同。

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 NSX Manager 的 **交换 > 端口** 中查看逻辑交换机端口。

在 NSX-T Data Center API 中，您可以使用 GET <https://<nsx-mgr>/api/v1/fabric/virtual-machines> API 调用查看 NSX-T Data Center 连接的虚拟机。

在 NSX-T Data Center Manager UI 中的 **交换 > 端口** 下面，VIF 连接 ID 与在 API 调用中找到的 externalId 相匹配。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

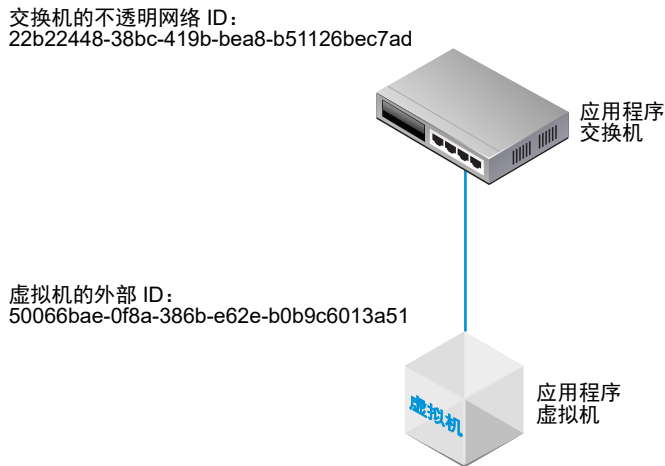
添加逻辑路由器。

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。



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-fe7-08c5-5bf7-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 **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

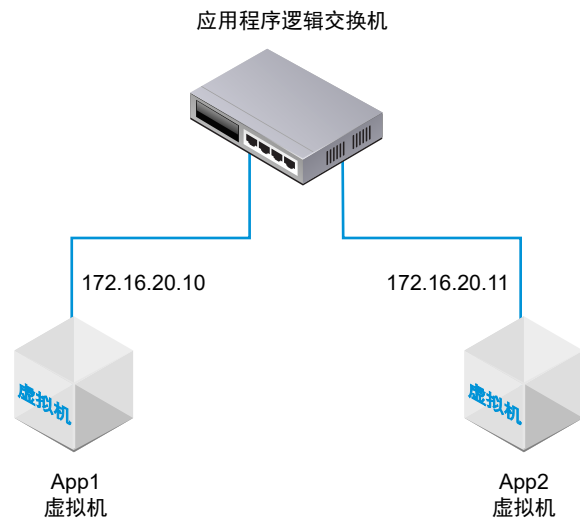
添加逻辑路由器。

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**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。

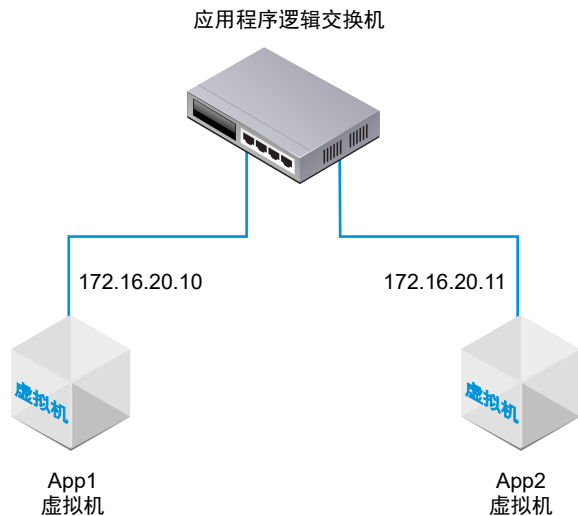
您可以监控逻辑交换机端口上的活动以解决问题。请参阅《NSX-T Data Center 管理指南》中的“监控逻辑交换机端口活动”。

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 1-3. 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 **交换 > 交换机**。

- e 单击逻辑交换机并记下 UUID 和 VNI 信息。
- f 从 NSX Controller 中，运行以下命令以解决该问题。

命令	说明
get logical-switch <vni-or-uuid> arp-table	<p>显示指定逻辑交换机的 ARP 表。</p> <p>示例输出。</p> <pre>nsx-controller1> 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	<p>显示指定逻辑交换机的连接。</p> <p>示例输出。</p> <pre>nsx-controller1> 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	<p>显示指定逻辑交换机的 MAC 表。</p> <p>示例输出。</p> <pre>nsx-controller1> 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	<p>显示有关指定逻辑交换机的统计信息。</p> <p>示例输出。</p> <pre>nsx-controller1> 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	<p>显示一段时间的所有逻辑交换机统计信息的摘要。</p> <p>示例输出。</p> <pre>nsx-controller1> 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>
get logical-switch <vni-or-uuid> vtep	<p>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。</p> <pre>nsx-controller1> 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。

逻辑交换机端口

2

逻辑交换机具有多个交换机端口。路由器、虚拟机或容器等实体可以通过逻辑交换机端口连接到逻辑交换机。

本章讨论了以下主题：

- [创建逻辑交换机端口](#)
- [监控逻辑交换机端口活动](#)

创建逻辑交换机端口

通过使用逻辑交换机端口，您可以将另一个网络组件、虚拟机或容器连接到逻辑交换机。

有关将虚拟机连接到逻辑交换机的详细信息，请参阅[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。

前提条件

确认创建了一个逻辑交换机端口。请参见[第 1 章 逻辑交换机和配置虚拟机连接](#)。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 的 NSX Manager。
- 2 从导航面板中选择 **网络 > 交换**。
- 3 单击 **端口** 选项卡。
- 4 单击 **添加**。
- 5 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	从下拉列表选择一个逻辑交换机。
管理状态	选择 已连接 或 未连接 。

选项	说明
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。

6 （可选）在**交换配置文件**选项卡中，选择交换配置文件。

7 单击**保存**。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。

2 从导航面板中选择**网络 > 交换**。

3 单击**端口**选项卡。

4 单击端口的名称。

5 单击**监控**选项卡。

此时将显示端口状态和统计信息。

6 要下载主机已发现的 MAC 地址的 CSV 文件，请单击**下载 MAC 表**。

7 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](#)。

逻辑交换机和逻辑端口的交换配置文件

3

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）
- 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。

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于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。

本章讨论了以下主题：

- [了解 QoS 交换配置文件](#)
- [了解 IP 发现交换配置文件](#)
- [了解 SpoofGuard](#)
- [了解交换机安全交换配置文件](#)
- [了解 MAC 管理交换配置文件](#)
- [将自定义配置文件与逻辑交换机相关联](#)
- [将自定义配置文件与逻辑端口相关联](#)

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管理程序中的流量。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **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 **QoS**。
- 5 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管理程序中的流量。</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，突发持续时间是突发大小设置中设置的。您不能保证带宽。不过，您可以使用该设置限制网络带宽。默认值 0 禁用输入流量。</p> <p>例如，在将逻辑交换机的平均带宽设置为 30 Mbps 时，该策略将限制带宽。您可以将突发流量限制为以 100 Mbps 速度传输 20 字节。</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>默认值 0 禁用输入广播流量。</p> <p>例如，在将逻辑交换机的平均带宽设置为 50 Kbps 时，该策略将限制带宽。您可以将突发流量限制为以 400 Kbps 速度传输 60 字节。</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 禁用输出流量。</p>

如果未配置输入、输入广播和输出选项，则将默认值作为协议缓冲区。

- 6 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 IP 发现交换配置文件

IP 发现使用 DHCP 侦听、ARP 侦听或 VM Tools 发现虚拟机 MAC 和 IP 地址。在发现 MAC 和 IP 地址后，将与 NSX Controller 共享这些条目以实现 ARP 抑制。ARP 抑制最大限度减少了连接到同一逻辑交换机的虚拟机中的 ARP 流量泛洪。

DHCP 侦听检查在虚拟机 DHCP 客户端和 DHCP 服务器之间传输的 DHCP 数据包以发现虚拟机 IP 和 MAC 地址。

ARP 侦听检查虚拟机的出站 ARP 和 GARP 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 地址。该 IP 发现方法仅适用于在 ESXi 主机上运行的虚拟机。

注 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

您可以启用 ARP 侦听、DHCP 侦听或 VM Tools 以创建自定义 IP 发现交换配置文件，以便发现 IP 和 MAC 地址以确保逻辑交换机的 IP 完整性。VM Tools IP 发现方法仅适用于 ESXi 托管的虚拟机。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **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 **IP 发现**。
- 5 填写 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	<p>切换 ARP 侦听 按钮以启用该功能。</p> <p>ARP 侦听检查虚拟机出站 ARP 和 GARP 以发现虚拟机 MAC 和 IP 地址。如果虚拟机使用静态 IP 地址而不是 DHCP，ARP 侦听才适用。</p>

选项	说明
ARP 绑定限制	指定值为 1 到 128 的 ARP 绑定限制。
DHCP 侦听	切换 DHCP 侦听 按钮以启用该功能。 DHCP 侦听检查在虚拟机 DHCP 客户端和 DHCP 服务器之间传输的 DHCP 数据包以发现虚拟机 MAC 和 IP 地址。
VM Tools	切换 VM Tools 按钮以启用该功能。该选项仅适用于 ESXi 托管的虚拟机。 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 MAC 和 IP 地址。

6 单击保存。

结果

自定义 IP 发现交换配置文件将显示为一个链接。

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 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。

在交换机级别，允许的 MAC/VLAN/IP 白名单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 交换机配置文件控制启用或禁用端口和交换机级别 SpoofGuard。

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，导航到**网络 > 交换**。
- 2 单击**端口**选项卡。
- 3 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。
- 4 在**概览**选项卡中，展开**地址绑定**。
- 5 单击**添加**。
将显示“添加地址绑定”对话框。
- 6 指定要将地址绑定应用到的逻辑端口的 IP 和 MAC 地址。还可以指定 VLAN ID。
- 7 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**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 **SpoofGuard**。
- 5 输入名称和可选的说明。
- 6 要启用端口级别的 **SpoofGuard**，请将**端口绑定**设置为已启用。
- 7 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经授权的数据包。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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**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。 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。
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。 “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。
阻止非 IP 流量	切换 阻止非 IP 流量 按钮以仅允许 IPv4、IPv6、ARP、GARP 和 BPDU 流量。 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。 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。
速率限制	为输入或输出广播和多播流量设置速率限制。 例如，配置速率限制以防止逻辑交换机或虚拟机受到广播流量风暴的影响。 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。

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。

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。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **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 **MAC 管理**。
- 5 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。
状态	启用或禁用 MAC 发现功能。

- 6 单击 **添加**。

结果

MAC 管理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](#)。

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[第 3 章 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，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 的 NSX Manager。
- 2 从导航面板中选择**网络 > 交换**。
- 3 单击**交换机**选项卡。
- 4 单击该逻辑交换机以应用自定义交换配置文件。
- 5 单击**管理**选项卡。
- 6 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
- 7 单击**更改**。
- 8 从下拉菜单中选择以前创建的自定义交换配置文件。
- 9 单击**保存**。
逻辑交换机现在与自定义交换配置文件相关联。
- 10 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。
- 11 （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[第 3 章 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 交换**。
- 3 单击**端口**选项卡。
- 4 单击该逻辑端口以应用自定义交换配置文件。
- 5 单击**管理**选项卡。
- 6 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
- 7 单击**更改**。
- 8 从下拉菜单中选择以前创建的自定义交换配置文件。
- 9 单击**保存**。

该逻辑端口现在与自定义交换配置文件相关联。

- 10 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](#)”。

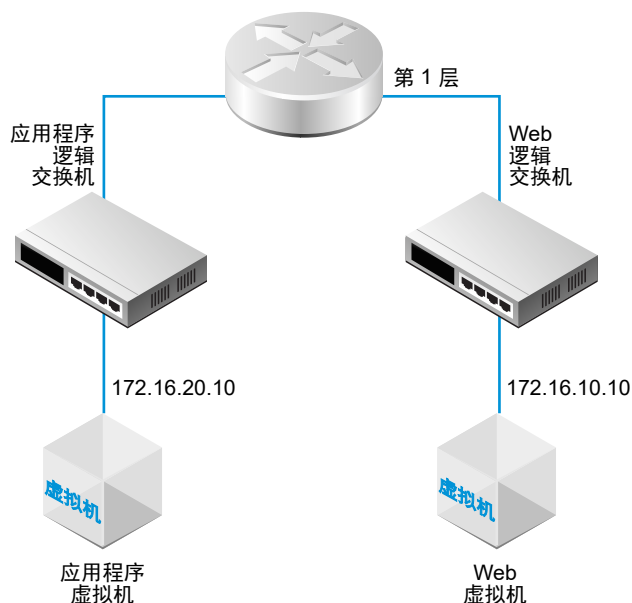
Tier-1 逻辑路由器

4

NSX-T Data Center 逻辑路由器在完全脱离底层硬件的虚拟环境中再现路由功能。Tier-1 逻辑路由器具有下行链路端口以连接到 NSX-T Data Center 逻辑交换机，并具有上行链路端口以连接到 NSX-T Data Center 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 4-1. 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群集或同一主机群集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。

本章讨论了以下主题：

- 创建 Tier-1 逻辑路由器
- 在 Tier-1 逻辑路由器上添加下行链路端口
- 在 Tier-0 或 Tier-1 逻辑路由器上添加 VLAN 端口

- 在 **Tier-1** 逻辑路由器上配置路由通告
- 配置 **Tier-1** 逻辑路由器静态路由
- 创建独立 **Tier-1** 逻辑路由器

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。请参见第 4 章 **Tier-1 逻辑路由器**。

步骤

1 从浏览器中，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 的 NSX Manager。

2 从导航面板中选择**网络 > 路由**。

3 单击**添加**，然后选择 **Tier-1 路由器**。

4 输入逻辑路由器的名称和可选描述。

5 （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。

6 （可选） 选择一个 NSX Edge 群集以连接到该 Tier-1 逻辑路由器。

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。

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**。

在 NSX Manager UI 中，新逻辑路由器是一个可单击的链接。

结果

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **网络 > 路由**。
- 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。

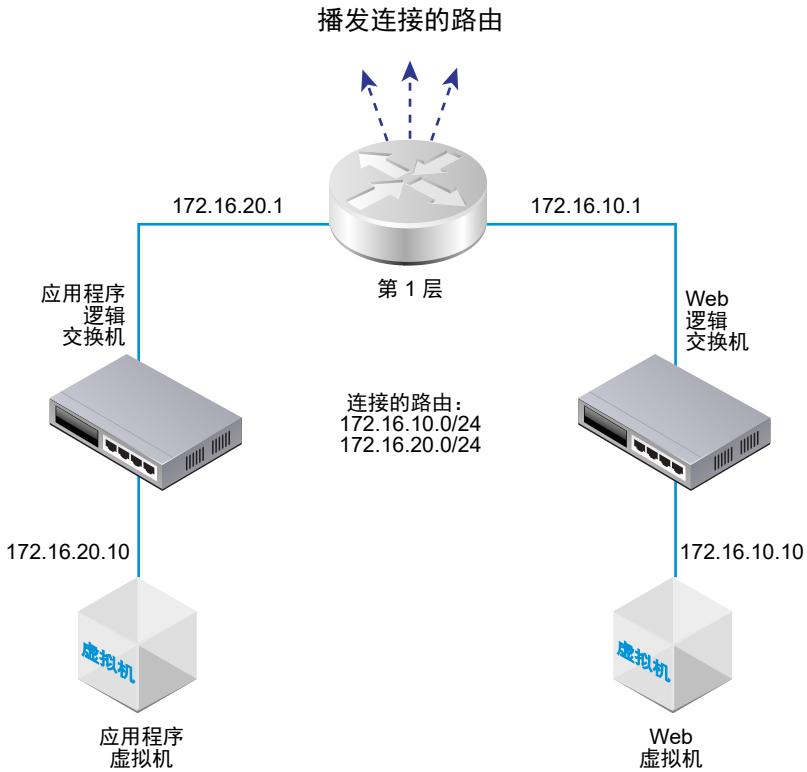
步骤

- 1 从浏览器中，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 的 NSX Manager。
- 2 从导航面板中选择 **网络 > 路由**。
- 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连接的路由，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 1 章 [逻辑交换机和配置虚拟机连接](#)。
- 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **网络 > 路由**。
- 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

- 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。请参见第 5 章 [Tier-0 逻辑路由器](#)。

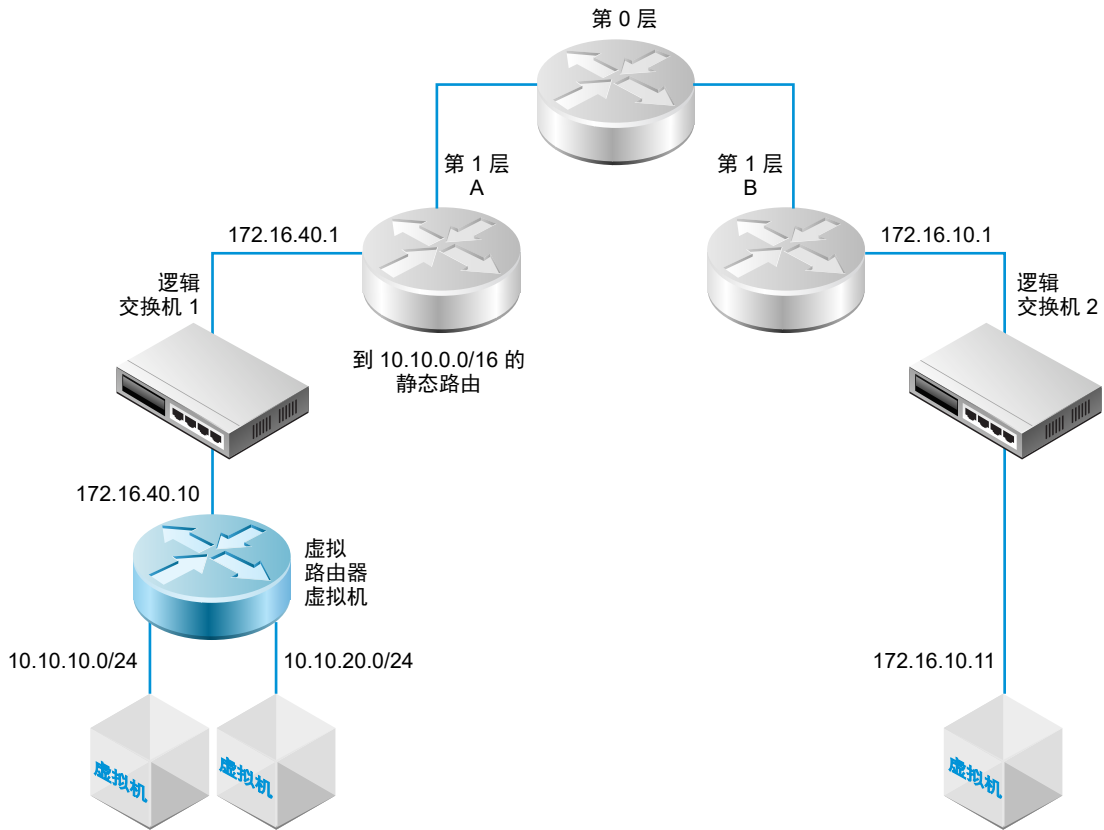
如果已将一个 Tier-0 逻辑路由器连接到 Tier-1 逻辑路由器，您可以验证该 Tier-0 路由器是否发现 Tier-1 路由器连接的路由。请参见[验证 Tier-0 路由器是否发现来自 Tier-1 路由器的路由](#)。

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 4-2. Tier-1 逻辑路由器静态路由拓扑



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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **网络 > 路由**。
- 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。
例如，10.10.10.0/16。
- 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。
- 仅支持负载均衡和 NAT 服务。

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。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。
- 3 单击**添加**，然后选择**Tier-1 路由器**。
- 4 输入逻辑路由器的名称和可选描述。
- 5 （必选） 选择一个 NSX Edge 群集以连接到该 Tier-1 逻辑路由器。
- 6 （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。

- 7 单击**添加**。
- 8 单击刚创建的路由器的名称。
- 9 单击**配置**选项卡，然后选择**路由器端口**。
- 10 单击**添加**。

- 11 输入路由器端口的名称和可选描述。
- 12 在**类型**字段中，选择**集中式**。
- 13 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。
- 14 （必选）选择逻辑交换机。
- 15 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。
- 16 以 CIDR 表示法输入路由器端口 IP 地址。
- 17 单击**添加**。

结果

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。
- 不支持独立路由器上的 ARP 代理。因此，不得在 CSP 子网中配置 LB 虚拟服务器 IP 或 LB SNAT IP，除非使用 CSP IP。例如，如果 CSP IP 为 1.1.1.1/24，虚拟 IP 必须为 1.1.1.1 或某些其他子网 IP 地址。不能是 1.1.1.1/24 子网中的任何其他地址。
- 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。

Tier-0 逻辑路由器

5

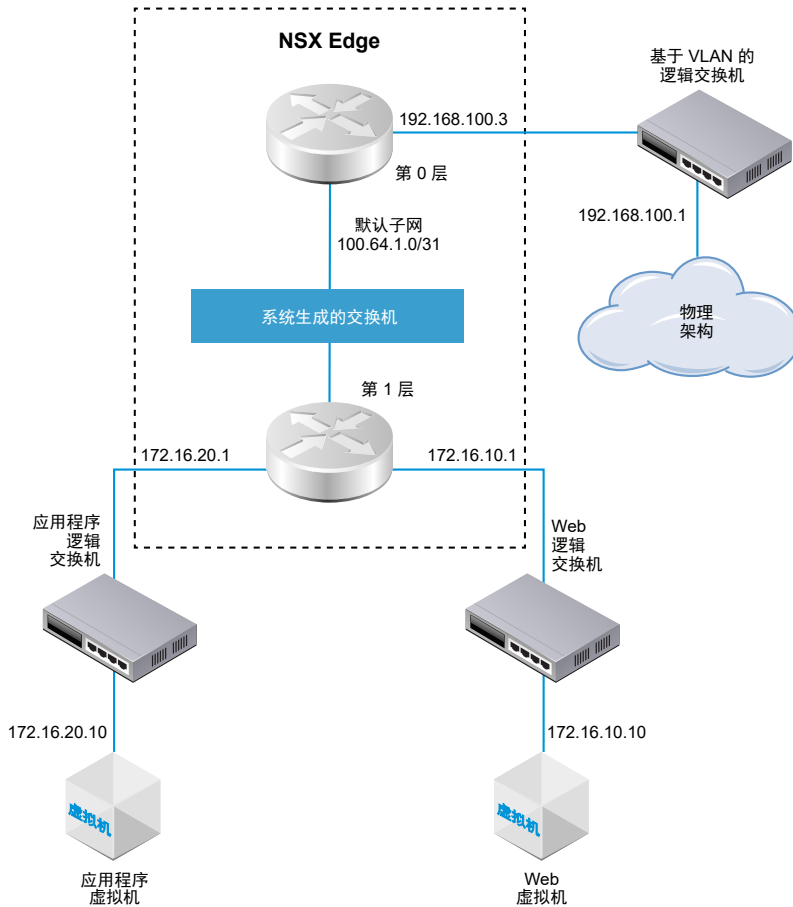
NSX-T Data Center 逻辑路由器在完全脱离底层硬件的虚拟环境中再现路由功能。Tier-0 逻辑路由器在逻辑和物理网络之间提供打开和关闭网关服务。

NSX Cloud 说明 如果使用 NSX Cloud，请参见[如何对公有云使用 NSX-T Data Center 功能](#)，获得自动生成的逻辑实体、支持的功能和 NSX Cloud 所需配置的列表。

NSX Edge 群集可以支持多个 Tier-0 逻辑路由器。Tier-0 路由器支持 BGP 动态路由协议和 ECMP。

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 5-1. 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。

本章讨论了以下主题：

- 创建 Tier-0 逻辑路由器
- 连接 Tier-0 和 Tier-1
- 将 Tier-0 逻辑路由器连接到 NSX Edge 上行链路的 VLAN 逻辑交换机
- 添加环回路由器端口
- 在 Tier-0 或 Tier-1 逻辑路由器上添加 VLAN 端口
- 配置静态路由
- BGP 配置选项

- 在 Tier-0 逻辑路由器上配置 BFD
- 在 Tier-0 逻辑路由器上启用路由重新分发
- 了解 ECMP 路由
- 创建 IP 前缀列表
- 创建社区属性列表
- 创建路由映射
- 配置转发启动定时器

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 NSX Controller 群集处于稳定状态。
- 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。请参见第 5 章 Tier-0 逻辑路由器。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。
- 3 单击**添加**以创建一个 Tier-0 逻辑路由器。
- 4 从下拉菜单中选择 **Tier-0 路由器**。
- 5 指定 Tier-0 逻辑路由器的名称。
- 6 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。
- 7 （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。

- 8 （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。

- 9 （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 100.64.0.0/10。将在 100.64.0.0/10 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。

- 10 单击**保存**。

新的 Tier-0 逻辑路由器将显示为一个链接。

- 11 （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。

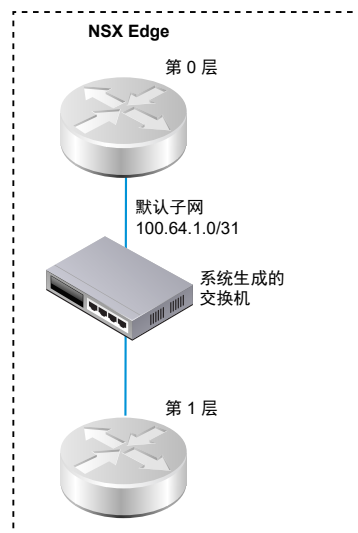
配置 Tier-0 逻辑路由器以将其连接到 VLAN 逻辑交换机，以便创建到外部网络的上行链路。请参见[将 Tier-0 逻辑路由器连接到 NSX Edge 上行链路的 VLAN 逻辑交换机](#)。

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 100.64.0.0/10。将在 100.64.0.0/10 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。

- 3 选择第 1 层逻辑路由器。
- 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-0 逻辑路由器。
- 11 单击 Tier-0 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-0 路由器是否发现 Tier-1 路由器通告的路由。

验证 Tier-0 路由器是否发现来自 Tier-1 路由器的路由

在 Tier-1 逻辑路由器将路由通告到 Tier-0 逻辑路由器时，这些路由将在 Tier-0 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-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

```

- 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)>

```

- 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 路由器发现的，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

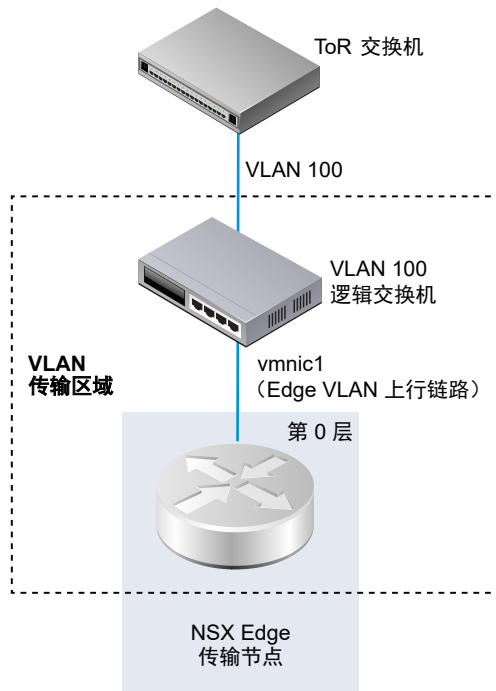
b   10.10.10.0/24      [20/0]      via 192.168.100.254
rl  100.91.176.0/31   [0/0]      via 169.254.0.1
c   169.254.0.0/28    [0/0]      via 169.254.0.2
ns  172.16.10.0/24 [3/3] via 169.254.0.1 ns 172.16.20.0/24 [3/3] via 169.254.0.1
c   192.168.100.0/24  [0/0]      via 192.168.100.2

```

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。
- 3 选择第 0 层逻辑路由器。
- 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-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 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。
- 3 选择第 0 层逻辑路由器。
- 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。
- 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。

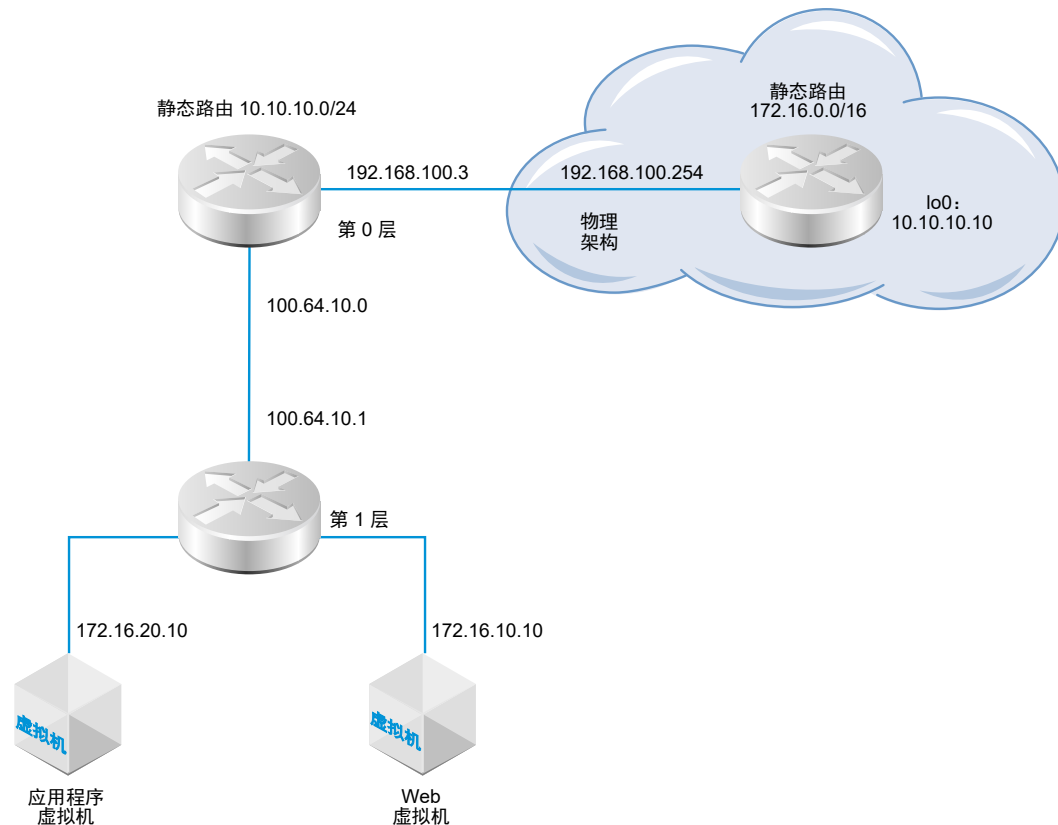
12 单击添加。

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 5-2. 静态路由拓扑



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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择网络 > 路由。
- 3 选择第 0 层逻辑路由器。

- 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 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。

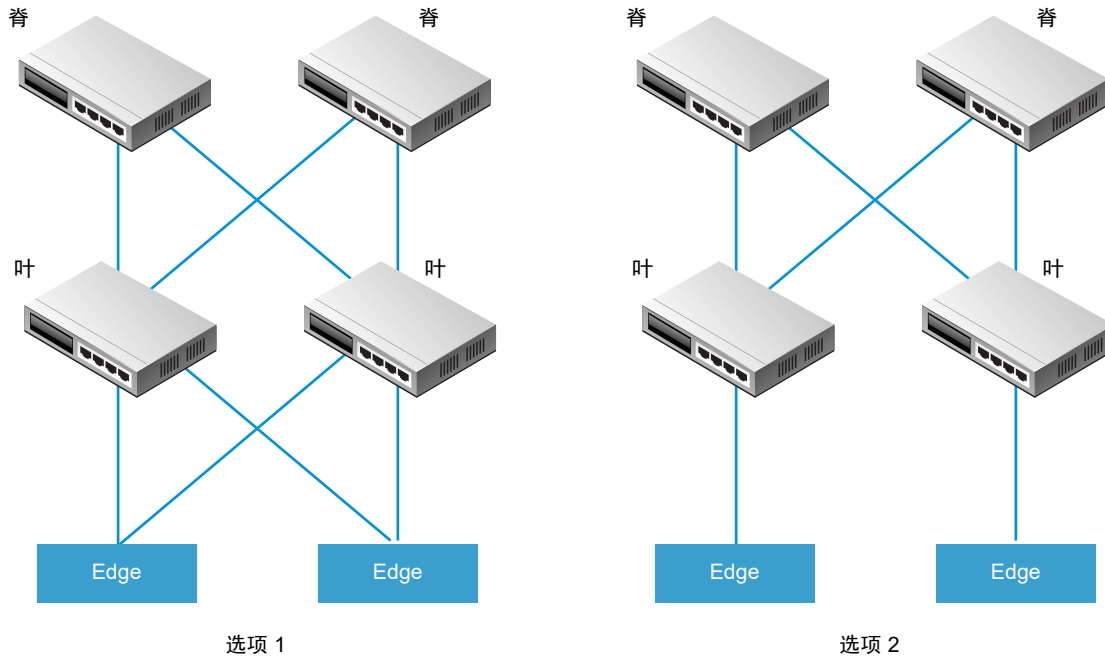
```
ping 10.10.10.10
```

```
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

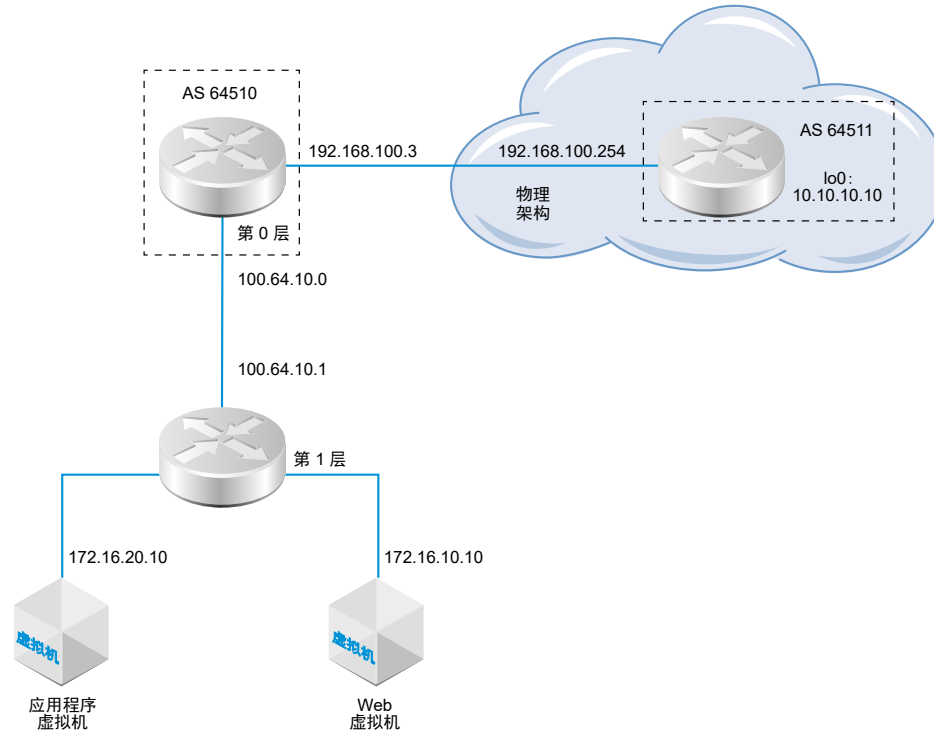
要在您的虚拟机和外界之间启用访问，您可以在 Tier-0 逻辑路由器和您的物理基础架构中的路由器之间配置外部 BGP (eBGP) 连接。

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。您还必须配置物理路由器的远程 AS 编号。在该示例中，远程 AS 编号为 64511。远程邻居 IP 地址为 192.168.100.254。该邻居必须位于与 Tier-0 逻辑路由器上的上行链路相同的 IP 子网中。支持 BGP 多跃点。

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。

注 系统会自动从在 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 节点上形成 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 5-3. BGP 连接拓扑



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 路由器是否发现来自 Tier-1 路由器的路由](#)。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **网络 > 路由**。
- 3 选择第 0 层逻辑路由器。
- 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 配置本地 AS 编号。

例如，64.510。

- b 单击**状态**切换按钮以启用 BGP。

“状态”按钮必须显示为“已启用”。

- c （可选）单击 **ECMP** 切换按钮以启用 ECMP。

- d （可选）单击**平滑重启**切换按钮以启动平滑重启。

- e （可选）配置路由聚合，启用正常重新启动以及启用 ECMP。

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。

- f 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 （可选）指定最大跃点限制。

默认值为 1。

9 输入远程 AS 编号。

例如，64.511。

10 （可选）配置定时器（保持活动状态时间和抑制时间）和密码。**11 （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。

12 （可选）单击地址系列选项卡以添加一个地址系列。**13 （可选）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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。
- 3 选择第 0 层逻辑路由器。
- 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。

- 3 选择第 0 层逻辑路由器。
- 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**添加**以满足路由重新分发条件。

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	选中要重新分发的源路由的复选框。 静态 - Tier-0 静态路由。 NSX 已连接 - Tier-1 连接的路由。 NSX 静态 - Tier-1 静态路由。将自动创建这些静态路由。 Tier-0 NAT - 在 Tier-0 逻辑路由器上配置 NAT 时生成的路由。 Tier-1 NAT - 在 Tier-1 逻辑路由器上配置 NAT 时生成的路由。
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。

- 6 单击**保存**。
- 7 单击**状态**切换按钮以启用路由重新分发。
“状态”按钮将显示为“已启用”。

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。

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
 2 100.91.176.1 (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

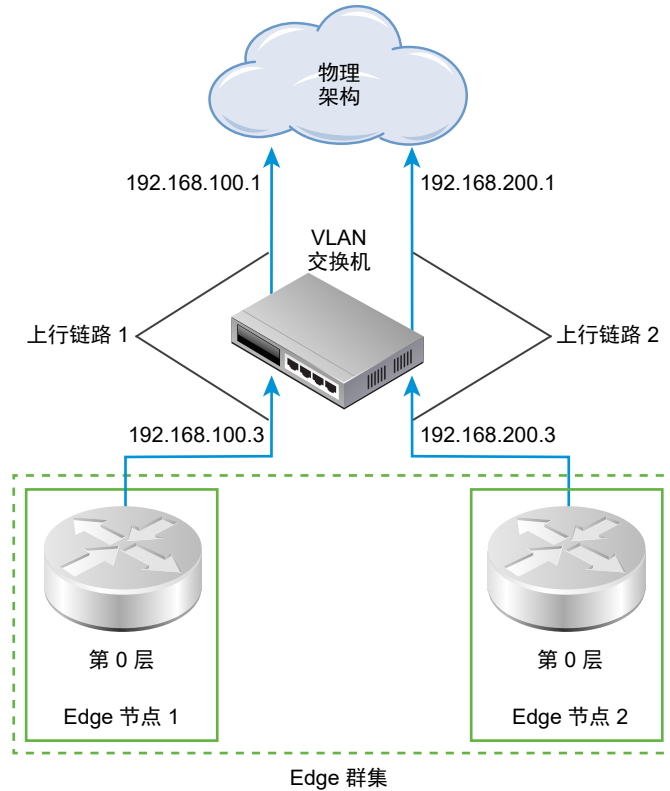
配置额外的路由功能，例如，ECMP。

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 群集中的每个 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平衡并为发生故障的路径提供容错。

将自动创建从连接到逻辑交换机的虚拟机到在其中实例化 Tier-0 逻辑路由器的 Edge 节点的 ECMP 路径。最多支持 8 个 ECMP 路径。

图 5-4. ECMP 路由拓扑



例如，拓扑显示 NSX Edge 群集中的两个 Tier-0 逻辑路由器。每个 Tier-0 逻辑路由器位于一个 Edge 节点中，并且这些节点是群集的一部分。上行链路端口 192.168.100.3 和 198.168.200.3 定义了传输节点如何连接到逻辑交换机以访问物理网络。如果启用了 ECMP 路由路径，这些路径将连接到逻辑交换机的虚拟机与 NSX Edge 群集中的两个 Edge 节点相连。多个 ECMP 路由路径提高了网络吞吐量和弹性。

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[为 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。
- 3 选择第 0 层逻辑路由器。
- 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 。
传输节点	从下拉菜单中分配主机传输节点。
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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。

- 3 选择第 0 层逻辑路由器。
- 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 打开 Tier-0 逻辑路由器的活动控制器。

8 验证是否连接了控制器节点上的 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**。

9 在两个 Edge 节点上启动 SSH 会话。

- 10 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>
```

- 11 导航到控制中心并双击 `httpdata11.bat` 和 `httpdata12.bat` 脚本。

将向两个 Web 虚拟机发送大量 HTTP 请求，并看到对流量进行哈希处理以发送到两个使用 Edge 节点的路径，这表明 ECMP 正常工作。

- 12 停止捕获会话。

```
del capture session 0
```

- 13 移除 bat 脚本。

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，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。
- 3 选择第 0 层逻辑路由器。
- 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。
- 3 选择第 0 层逻辑路由器。
- 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。
- 3 选择第 0 层逻辑路由器。
- 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **网络 > 路由**。
- 3 选择第 0 层逻辑路由器。
- 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**。

网络地址转换

6

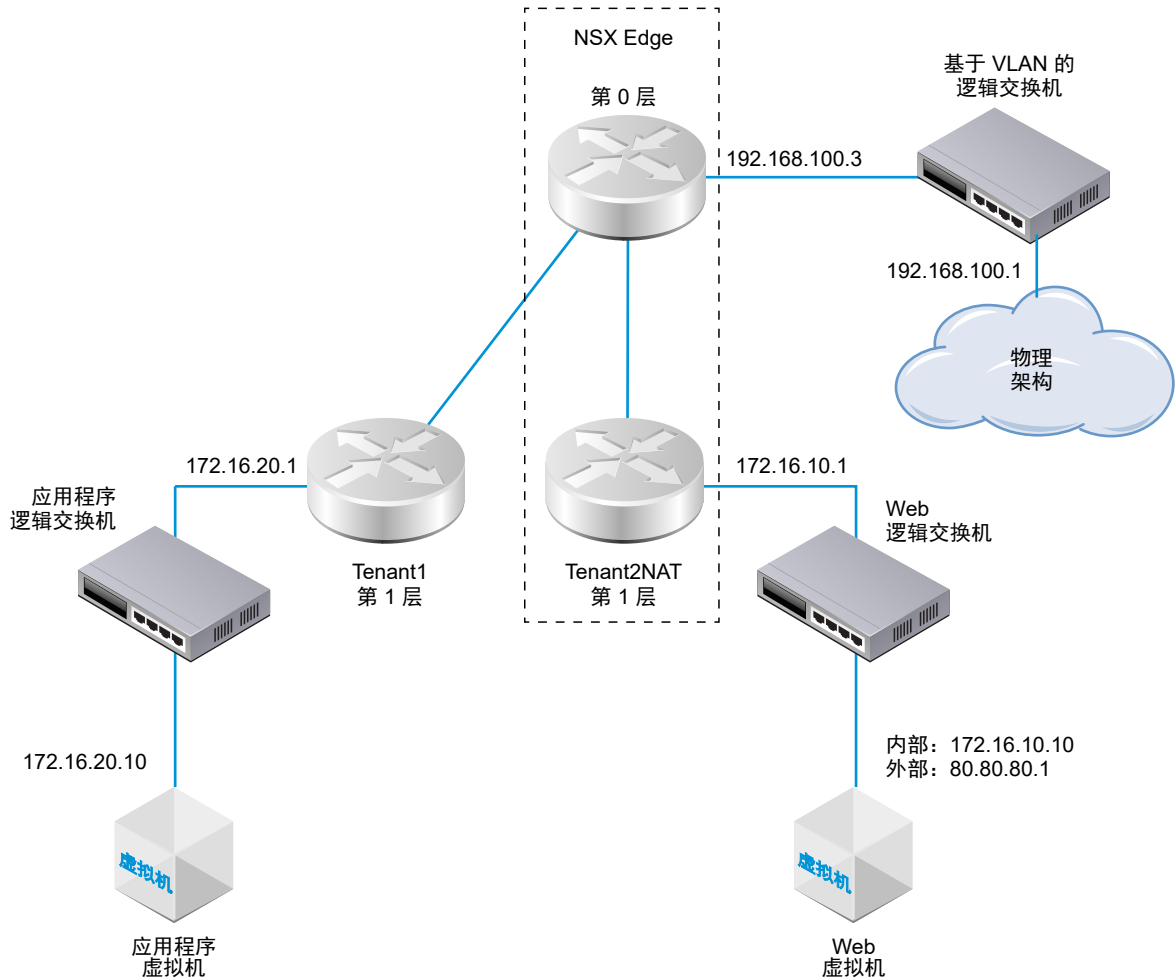
可以在 Tier-0 和 Tier-1 逻辑路由器上配置 NSX-T Data Center 中的网络地址转换 (NAT)。

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 群集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 6-1. NAT 拓扑



本章讨论了以下主题：

- Tier-1 NAT
- Tier-0 NAT
- 反射 NAT

Tier-1 NAT

Tier-1 逻辑路由器支持源 NAT 和目标 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。它还可能会更改 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，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。
- 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。
- 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **网络 > 路由**。
- 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 编辑路由通告规则以启用 NAT 路由通告。

结果

Tenant2NAT	
概览 配置 路由 服务	
路由通告 编辑	
状态	● 已启用
通告所有 NSX 连接的路由	● 是
通告所有 NAT 路由	● 是
通告所有静态路由	● 否
通告所有 LB VIP 路由	● 否
通告所有 LB SNAT IP 路由	● 否
已通告的网络	5 网络

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 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 编辑路由通告规则以启用 Tier-1 NAT 路由通告。

结果

编辑重新分发条件 - rule1

名称 * rule1

描述 Rule

源 *

☐ 静态 ☒ 第 1 层 NAT

☒ NSX 已连接 ☐ 第 1 层 LB VIP

☒ NSX 静态 ☐ 第 1 层 LB SNAT

☐ 第 0 层 NAT

路由映射

取消 保存

后续步骤

验证 NAT 是否正常工作。

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。

- 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
...
```

- 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。
- 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。
- 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

Tier-0 逻辑路由器支持源 NAT、目标 NAT 和反射 NAT。

在 Tier-0 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 路由器上配置源和目标 NAT。

此外，还可以配置“无 NAT”、“NO_SNAT”或“NO_DNAT”，以便对某个 IP 地址或地址范围禁用 NAT。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。

步骤

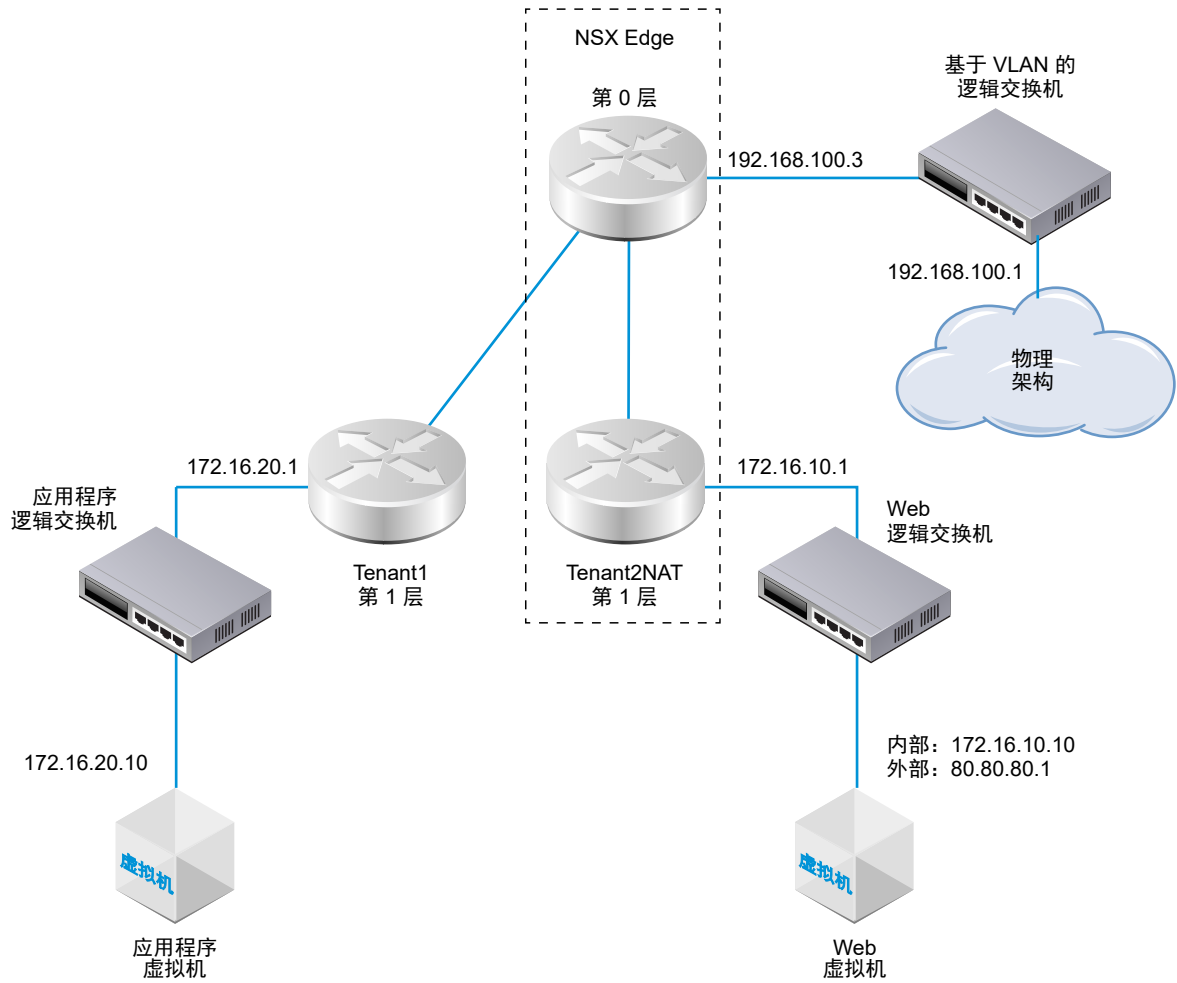
- 从浏览器中，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 的 NSX Manager。
- 从导航面板中选择 **网络 > 路由**。
- 单击 Tier-0 逻辑路由器。
- 选择 **服务 > NAT**。
- 单击 **添加** 以添加 NAT 规则。
- 指定优先级值。
较低的值意味着更高的优先级。
- 对于 **操作**，选择 **SNAT**、**DNAT**、**无 NAT**、**NO_SNAT** 或 **NO_DNAT**。
- 选择协议类型。
默认情况下，将选择 **任何协议**。
- （必选）对于 **源 IP**，以 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 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。

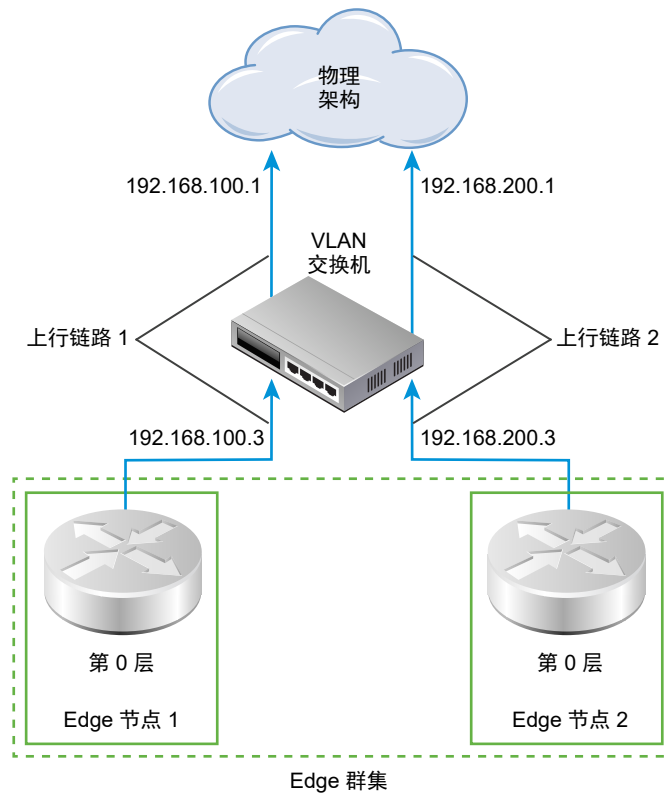
反射 NAT

如果 Tier-0 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）。

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。



在涉及两个主动-主动 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。
- 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		

防火墙区域和防火墙规则

7

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。

本章讨论了以下主题：

- [添加防火墙规则区域](#)
- [删除防火墙规则区域](#)
- [启用和禁用区域规则](#)
- [启用和禁用区域日志](#)
- [关于防火墙规则](#)
- [添加防火墙规则](#)
- [删除防火墙规则](#)
- [编辑默认分布式防火墙规则](#)
- [更改防火墙规则的顺序](#)
- [筛选防火墙规则](#)

- 为逻辑交换机网桥端口配置防火墙
- 配置防火墙排除列表
- 启用和禁用防火墙
- 在逻辑路由器中添加或删除防火墙规则

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 从导航面板中选择**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。有状态防火墙可以监控从一端到另一端的流量流。在较高的流量负载情况下，无状态防火墙通常速度更快，性能更好。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 从导航面板中选择**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 从导航面板中选择**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 vSphere ESXi 和 KVM 主机上的 `/var/log/dfwpktlogs.log` 文件中。

步骤

- 1 从导航面板中选择**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**。

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 对于 TCP 协议，自动为有状态规则启用 TCP 严格检查。这意味着仅当网络连接以 SYN 数据包开始时，数据包才会与 TCP 规则相匹配。

表 7-1. 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。源或目标范围不支持 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。源或目标范围不支持 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/dfwptlogs.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。

表 7-1. 防火墙规则的属性（续）

属性	说明
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 从导航面板中选择**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 从导航面板中选择**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 从导航面板中选择**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 从导航面板中选择**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 从导航面板中选择**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。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**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。

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。

步骤

- 1 从导航面板中选择**安全 > 分布式防火墙**。
- 2 单击**排除列表**选项卡。
- 3 单击**添加**。
- 4 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**。
- 5 单击**确定**。
- 6 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**。

启用和禁用防火墙

您可以启用或禁用分布式防火墙功能。如果禁用该功能，则不会实施任何规则。

步骤

- 1 从导航面板中选择**安全 > 分布式防火墙**。
- 2 单击**设置**选项卡。
- 3 单击**编辑**。

- 4 在对话框中，将防火墙状态设置为绿色（已启用）或灰色（已禁用）。
- 5 单击**保存**。

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。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > 路由**。
- 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。

NSX-T Data Center 在 NSX Edge 上支持 IPsec VPN 和第 2 层 VPN (L2VPN)。

注 IPsec VPN 和 L2VPN 在 NSX-T Data Center Limited Export 版本中不受支持。

IPSEC VPN

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。

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 4500。

注 IPsec VPN 仅在第 0 层逻辑路由器上受支持。

NSX Edge 支持两种类型的 VPN：基于策略的 VPN 和基于路由的 VPN。

基于策略的 VPN 要求对转发到 IPsec 服务的数据包应用策略。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，还必须更新策略设置以适应相关更改。

基于路由的 VPN 根据通过特殊接口（称为虚拟隧道接口 (VTI)）使用 BGP 等协议动态学习的路由提供流量隧道。IPsec 会保护流经虚拟隧道接口 (VTI) 的所有流量。

L2VPN

借助 L2VPN 连接，可以将第 2 层网络从内部部署数据中心扩展至诸如 VMware Cloud on Amazon (VMC) 等云。该连接受基于路由的 IPsec 隧道保护。

扩展的网络是具有单个广播域的单个子网，因此您可以在内部部署数据中心和公有云之间迁移虚拟机，而不必更改其 IP 地址。

除了支持数据中心迁移，还可以使用借助 L2VPN 扩展的内部部署网络来进行灾难恢复以及动态预留外部部署计算资源，以满足云突发需求增加。

每个 L2VPN 会话都有一个 GRE 隧道。不支持隧道冗余。一个 L2VPN 会话最多可以扩展至 4094 个第 2 层网络。

注 在 NSX-T Data Center 与 NSX Data Center for vSphere 中管理或未管理的 NSX Edge 之间支持 L2VPN。

本章讨论了以下主题：

- [配置 IPsec VPN](#)
- [配置 L2VPN](#)

配置 IPsec VPN

只能使用 API 来创建基于路由的 VPN 会话和基于策略的 VPN 会话。

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

不能在同一网络配置文件中同时使用 NAT 和 IPsec VPN。请确保将 NAT 和 IPsec VPN 放在不同的网络配置文件上。

前提条件

熟悉 IPsec VPN。请参见 [IPSEC VPN](#)。

步骤

- 1 在第 0 层逻辑路由器上配置 IPsec VPN 服务。

使用 `POST /api/v1/vpn/ipsec/services` 调用。

```
POST /api/v1/vpn/ipsec/services
{
  "display_name": "IPsec VPN service",
  "logical_router_id": "f81f220f-3072-4a6e-9f53-ad3b8bb8af57"
}
```

- 2 配置不活动对等检测 (Dead Peer Detection, DPD) 配置文件。

使用 `POST /api/v1/vpn/ipsec/dpd-profiles` 调用。

默认配置文件置备了 60 秒 DPD 探测间隔。

```
POST /api/v1/vpn/ipsec/dpd-profiles
{
  "enabled": "true",
  "dpd_probe_interval": 60,
  "description": "DPD profile",
  "display_name": "DPD profile"
}
```


3 配置 IKE 配置文件参数。

使用 POST /api/v1/vpn/ipsec/ike-profiles 调用。

```
POST /api/v1/vpn/ipsec/ike-profiles
{
  "digest_algorithms": ["SHA2_256"],
  "description": "IKEProfile for site1",
  "display_name": "IKEProfile site1",
  "encryption_algorithms": ["AES_128"],
  "ike_version": "IKE_V2",
  "dh_groups": ["GROUP14"],
  "sa_life_time": 21600
}
```

4 为 IPSec VPN 配置隧道配置文件。

使用 POST /api/v1/vpn/ipsec/tunnel-profiles 调用。

```
POST /api/v1/vpn/ipsec/tunnel-profiles/
{
  "digest_algorithms": ["SHA1","SHA2_256"],
  "description": "Tunnel Profile for site 1",
  "display_name": "Tunnel Profile for site 1",
  "encapsulation_mode": "TUNNEL_MODE",
  "encryption_algorithms": ["AES_128","AES_256"],
  "enable_perfect_forward_secrecy": true,
  "dh_groups": ["GROUP14"],
  "transform_protocol": "ESP",
  "sa_life_time": 3600,
  "df_policy": "CLEAR"
}
```

5 配置对等端点以与 IPSec VPN 对等通信。

使用 POST /api/v1/vpn/ipsec/peer-endpoints 调用。

```
POST /api/v1/vpn/ipsec/peer-endpoints
{
  "display_name": "Peer endpoint for site 1",
  "connection_initiation_mode": "INITIATOR",
  "authentication_mode": "PSK",
  "ipsec_tunnel_profile_id": "640607f3-bb83-4e54-a153-57939965881c",
  "dpd_profile_id": "4808d04e-572d-480d-8182-61ddaa146461",
  "psk": "6721b9f1f5936956c0a8b4ed95286b452db04dae721edd0f264f0fcc6e94882b",
  "ike_profile_id": "a4db6863-b6f0-45bd-967e-a2e22c260329",
  "peer_address": "10.14.24.4",
  "peer_id": "10.14.24.4"
}
```

6 为 VPN 端点配置本地端点。

使用 POST /api/v1/vpn/ipsec/local-endpoints 调用。

```
POST /api/v1/vpn/ipsec/local-endpoints
{
  "local_address": "1.1.1.12",
  "local_id": "1.1.1.12",
  "display_name": "Local endpoint",
  "ipsec_vpn_service_id": {
    "target_id" : "81388ec0-b5e3-4a9e-b551-e372e700772c"
  }
}
```

7 配置基于路由的 VPN 会话。

使用 POST /api/v1/vpn/ipsec/sessions 调用。

```
POST /api/v1/vpn/ipsec/sessions
{
  "resource_type": "RouteBasedIPSecVPNSession",
  "display_name": "RouteSession1",
  "ipsec_vpn_service_id": "657bcb55-48ce-4e0f-bfc7-a5a91b2990ae",
  "peer_endpoint_id": "cfc70ab5-16d1-4292-9391-fcee23ccea96",
  "local_endpoint_id": "9d4b44f1-0bfa-4705-ac67-09244a17d42e",
  "enabled": true,
  "tunnel_ports": [
    {
      "ip_subnets": [
        {
          "ip_addresses" : [
            "192.168.50.1"
          ],
          "prefix_length" : 24
        }
      ]
    }
  ]
}
```

8 配置基于策略的 VPN 会话。

使用 POST /api/v1/vpn/ipsec/sessions 调用。

```
POST /api/v1/vpn/ipsec/sessions
{
  "resource_type": "PolicyBasedIPSecVPNSession",
  "display_name": "PolicySession1",
  "ipsec_vpn_service_id": "ea071856-9e91-4826-a841-9ec7ee9ea534",
  "peer_endpoint_id": "0c2447d2-8890-4b55-bf02-8c6b1a94d1ce",
  "local_endpoint_id": "161acb63-c3f2-438d-9e5c-cb655e6a1099",
  "enabled": true,
  "policy_rules": [
    {
      "sources": [
```

```

    {
      "subnet": "2.2.2.0/24"
    }
  ],
  "logged": true,
  "destinations": [
    {
      "subnet": "3.3.3.0/24"
    }
  ],
  "action": "PROTECT",
  "enabled": true
}
]
}

```

配置 L2VPN

只能使用 API 来创建 L2VPN 服务和会话。

注 L2VPN 在 NSX-T Data Center Limited Export 版本中不受支持。

前提条件

- 熟悉 L2VPN。请参见 [L2VPN](#)。
- 验证是否为第 0 层逻辑路由器配置了上行链路配置文件。请参见《NSX-T Data Center 安装指南》。
- 确认配置了一个逻辑交换机。请参见 [创建逻辑交换机](#)。
- 验证非受管 NSX Edge 在 NSX Data Center for vSphere 中是否可用。
- 确认已配置 IPsec VPN。配置 [IPsec VPN](#)

步骤

1 配置 L2VPN 服务。

使用 POST /api/v1/vpn/l2vpn/services 调用。

```

POST /api/v1/vpn/l2vpn/services
{
  "logical_router_id": "b6fe5455-619b-4030-b5f8-8575749f4404",
  "logical_tap_ip_pool" : [ "169.254.64.0/28" ],
  "enable_full_mesh" : true
}

```

2 配置 L2VPN 会话。

使用 POST /api/v1/vpn/l2vpn/sessions 调用。

```
POST /api/v1/vpn/l2vpn/sessions
{
  "l2vpn_service_id" : "421de3a2-c6ec-4c42-a891-5bde3b5feb68",
  "transport_tunnels" : [
    {
      "target_id" : "801e5140-6da8-4e78-ab44-f966de75f311"
    }
  ]
}
```

3 为逻辑端口配置连接。

使用 POST /api/v1/vpn/logical-ports 调用。

```
POST /api/v1/logical-ports/
{
  "resource_type": "LogicalPort",
  "display_name": "Extend logicalSwitch, port for service",
  "logical_switch_id": "f52abcee-27a7-426c-a128-037db2283582",
  "admin_state" : "UP",
  "attachment": {
    "attachment_type": "L2VPN_SESSION",
    "id": "6806c4ea-3b77-4b8a-8af2-ccc47b1ba8a9",
    "context" : {
      "resource_type" : "L2VpnAttachmentContext",
      "tunnel_id" : 10
    }
  }
}
```

4 下载 L2VPN 对等代码配置。

GET /api/v1/vpn/l2vpn/sessions/<L2VPN-session-ID>/peer-codes

5 登录到内部部署 NSX Data Center for vSphere 非受管 NSX Edge CLI。

6 粘贴 L2VPN 对等代码配置。

7 （可选）监控 L2VPN 会话。

- L2VPN 会话摘要: GET /api/v1/vpn/l2vpn/sessions/summary。
- L2VPN 会话统计信息: GET /api/v1/vpn/l2vpn/sessions/<L2VPN-session-ID>/statistics。

管理对象、组、服务和虚拟机

9

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。

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。

注 防火墙规则的源或目标范围不支持 IPv6。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**清单 > 组**。
- 3 选择主面板顶部的 **IP 集**。
- 4 单击**添加**。
- 5 输入名称。
- 6 （可选）输入说明。
- 7 输入各个地址或地址范围。
- 8 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**清单 > 组**。
- 3 选择主面板顶部的 **IP 池**。
- 4 单击**添加**。
- 5 输入名称。
- 6 （可选）输入说明。
- 7 单击**添加**。
- 8 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。

- 9 （可选）输入网关。
- 10 输入具有后缀的 CIDR IP 地址。
- 11 （可选）输入 DNS 服务器。
- 12 （可选）输入 DNS 后缀。
- 13 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**清单 > 组**。
- 3 选择主面板顶部的 **MAC 集**。
- 4 单击**添加**。
- 5 输入名称。
- 6 （可选）输入说明。
- 7 输入 MAC 地址。
- 8 单击**保存**。

创建 NS 组

您可以配置一个 NS 组以包含 IP 集、MAC 集、逻辑端口、逻辑交换机和其他 NS 组的组合。您可以在防火墙规则（以及 **Applied To** 字段）中将 NS 组指定为源和目标。

NSX Cloud 说明 如果使用 NSX Cloud，请参见[如何对公有云使用 NSX-T Data Center 功能](#)，获得自动生成的逻辑实体、支持的功能和 NSX Cloud 所需配置的列表。

NS 组具有以下特性：

- 您可以指定直接成员，它们可能是 IP 集、MAC 集、逻辑交换机、逻辑端口和 NS 组。
- 您可以最多指定 5 个应用于逻辑交换机、逻辑端口或虚拟机的成员资格条件。对于应用于逻辑交换机或逻辑端口的条件，可以指定标记和可选范围。对于应用于虚拟机的条件，可以指定以特定字符串开头、等于或包含该字符串的名称。
- 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，您添加 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。
- 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。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。在 NSX Manager 上，在 NS 组的有效成员数超过 5000 的 80% 时，将在日志文件中显示警告消息 NS 组 xyz 即将超过最大成员限制。NS 组中的总数为... (NSGroup xyz is about to exceed the maximum member limit. Total number in NSGroup is ...); 在该数字超过 5000 时，将显示警告消息 NS 组 xyz 已达到最大数字限制。NS 组中的总数 = ... (NSGroup xyz has reached the maximum numbers limit. Total number in NSGroup = ...)。在 NSX Controller 上，在 NS 组中的转换的 VIF/IP/MAC 数超过 5000 时，将在日志文件中显示警告消息容器 xyz 已达到最大 IP/MAC/VIF 转换限制。容器中的当前转换计数 - IP:..., MAC:..., VIF:... (Container xyz has reached the maximum IP/MAC/VIF translations limit. Current translations count in Container - IPs:..., MACs:..., VIFs:...)。NSX Manager 和 NSX Controller 每天检查两次 NS 组是否超过该限制（早晨 7 点和晚上 7 点）。
- 支持的最大虚拟机数为 10,000 个。

对于可作为成员添加到 NS 组的所有对象（即，逻辑交换机、逻辑端口、IP 集、MAC 集、虚拟机和 NS 组），您可以导航到任何对象的屏幕，然后选择**相关 > NS 组**以查看直接或间接将该对象作为成员的所有 NS 组。例如，在上面的示例中，在导航到 LogicalSwitch-1 屏幕后，选择**相关 > NS 组**将显示 NSGroup-1、NSGroup-2 和 NSGroup-3，因为所有三个组直接或间接将 LogicalSwitch-1 作为成员。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**清单 > 组**。

- 3 单击**组**选项卡（如果尚未选择该选项卡）。
- 4 单击**添加**。
- 5 输入 NS 组的名称。
- 6 （可选）输入说明。
- 7 （可选）单击**成员资格条件**。

条件可以应用于逻辑交换机、逻辑端口或虚拟机。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。对于应用于逻辑交换机或逻辑端口的规则，可以指定标记和可选范围。对于应用于虚拟机的规则，可以指定以特定字符串开头、等于或包含该字符串的名称。

最多可以指定五个条件，且这些条件可与逻辑 **OR** 运算符结合使用。

- 8 （可选）单击**成员**以选择成员。

可用的类型是 **IP 集**、**MAC 集**、**逻辑交换机**、**逻辑端口**以及 **NS 组**。

- 9 单击**保存**。

配置服务和服务组

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。

- 2 从导航面板中选择**清单 > 服务**。
- 3 单击**添加**。
- 4 输入名称。
- 5 （可选）输入说明。
- 6 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。
- 7 对于单个服务，请选择类型和协议。
可用的类型是以太网、IP、IGMP、ICMP、ALG 和 L4 端口集。
- 8 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。
- 9 单击**保存**。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。

- 2 从导航面板中选择**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。您可以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 选择一个虚拟机。
- 4 单击**管理标记**。
- 5 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 。

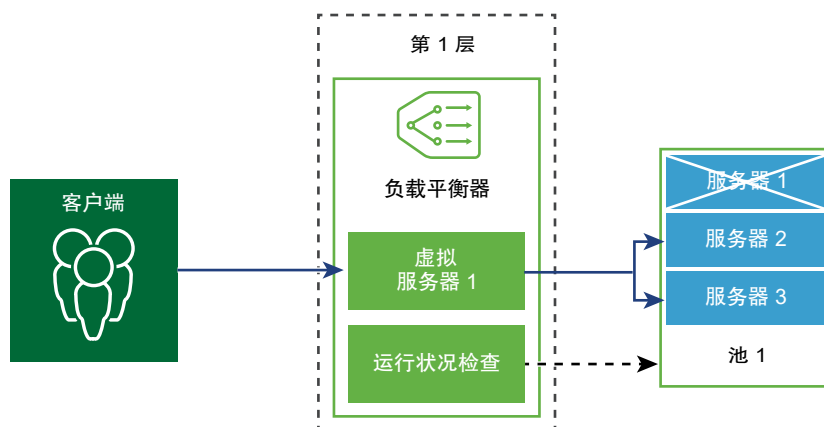
虚拟机最多可以具有 15 个标记。

- 6 单击**保存**。

逻辑负载均衡器

10

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 仅在第 1 层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第 1 层逻辑路由器。

本章讨论了以下主题：

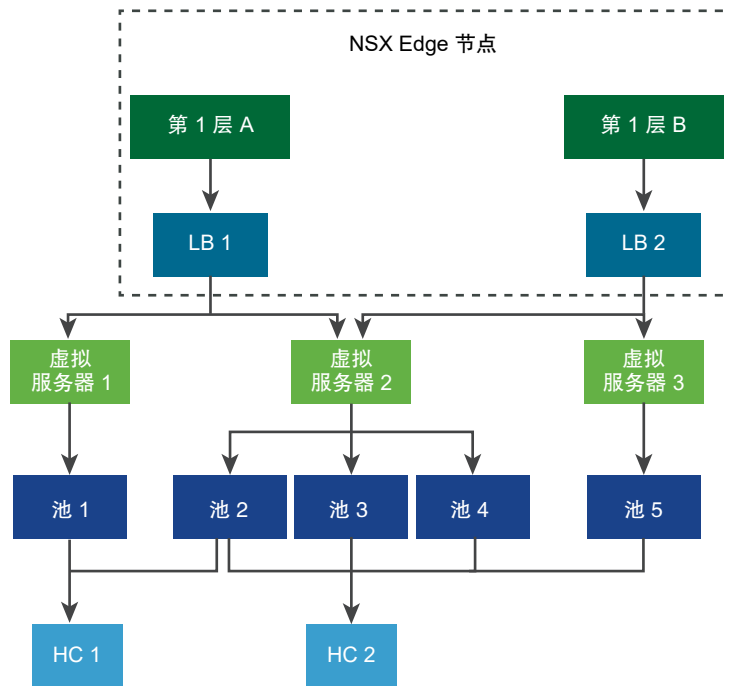
- [负载均衡器重要概念](#)
- [配置负载均衡器组件](#)

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。



缩放负载均衡器资源

负载均衡器有大中小三种规模。根据负载均衡器的规模，负载均衡器可以托管不同的虚拟服务器和池成员。

负载均衡器连接到 **Tier-1** 逻辑路由器。该 **Tier-1** 逻辑路由器托管在 **NSX Edge** 节点上。**NSX Edge** 具有以下规格：裸机、小型、中型和大型虚拟机设备。根据形式，**NSX Edge** 节点可以托管不同数量的负载均衡器。

表 10-1. 负载均衡器服务的负载均衡器规模

负载均衡器服务	小型负载均衡器	中型负载均衡器	大型负载均衡器
每个负载均衡器的虚拟服务器数量	10	100	1000
每个负载均衡器的池数量	20	200	2000
每个负载均衡器的池成员数量	200	2000	10,000

表 10-2. NSX Edge 节点的负载均衡器规模

每个 NSX Edge 节点的负载均衡器	小型负载均衡器	中型负载均衡器	大型负载均衡器	最大池成员数
NSX Edge 虚拟机 - 小型	不适用	不适用	不适用	不适用
NSX Edge 虚拟机 - 中型	1	不适用	不适用	200
NSX Edge 虚拟机 - 大型	40	4	不适用	5000
NSX Edge 虚拟机 - 裸机	750	75	7	20,000

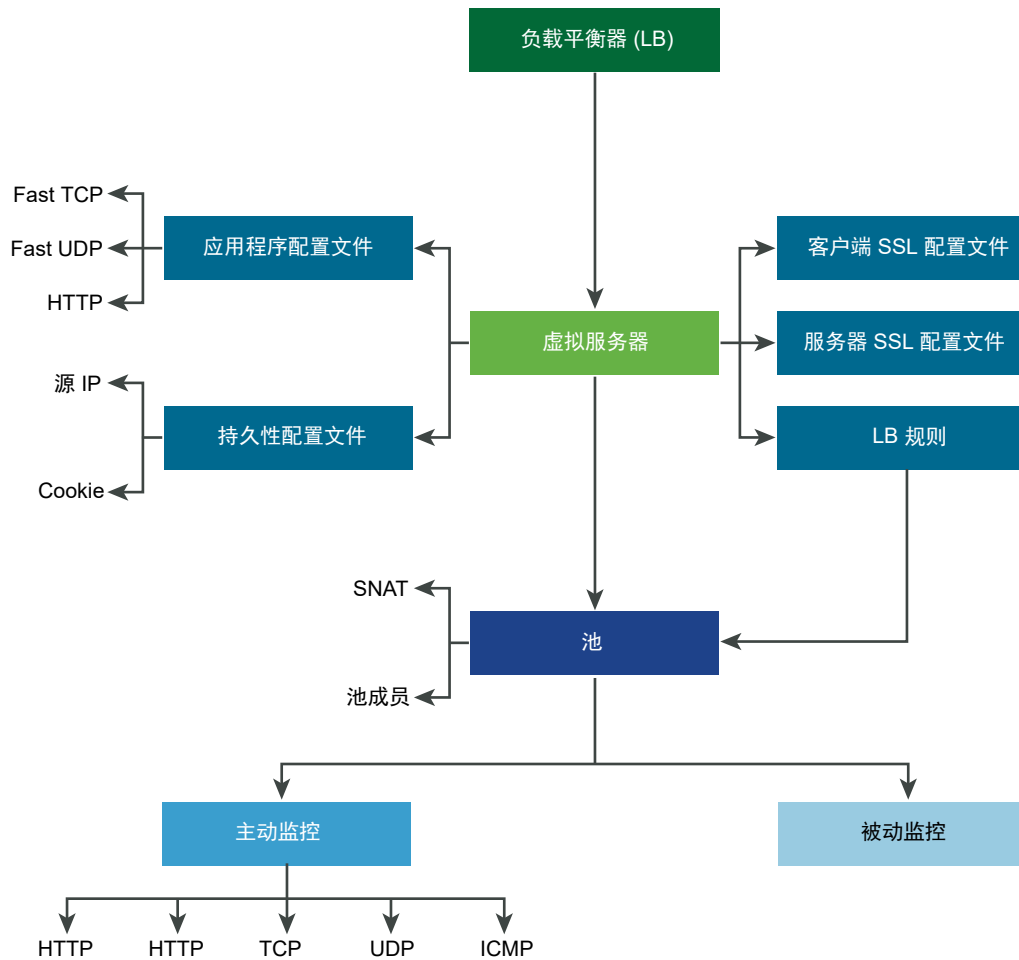
支持的负载均衡器功能

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。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的连接。

注意：SSL 终止模式和代理模式在 NSX-T Data Center 2.2 Limited Export 版本中不受支持。

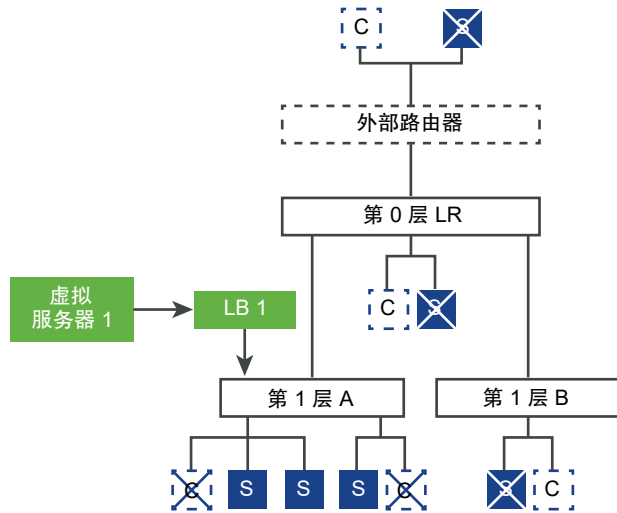


负载均衡器拓扑

负载均衡器通常在内嵌或单臂模式下部署。

内嵌拓扑

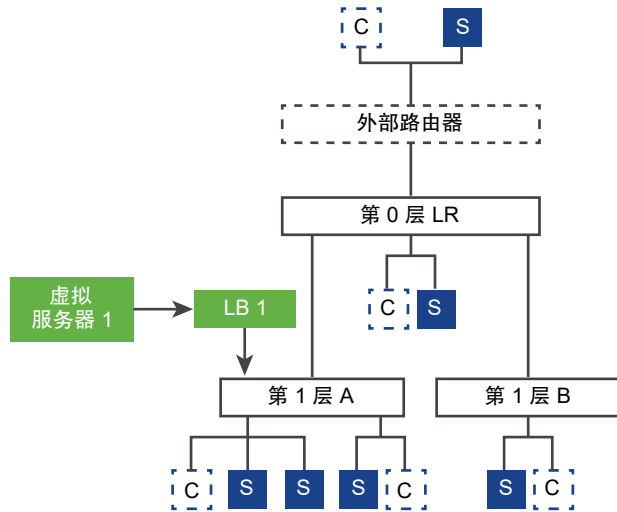
在内嵌模式下，负载均衡器位于客户端和服务端之间的流量路径中。客户端和服务端不得连接到相同的 Tier-1 逻辑路由器。此拓扑不需要虚拟服务器 SNAT。



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。

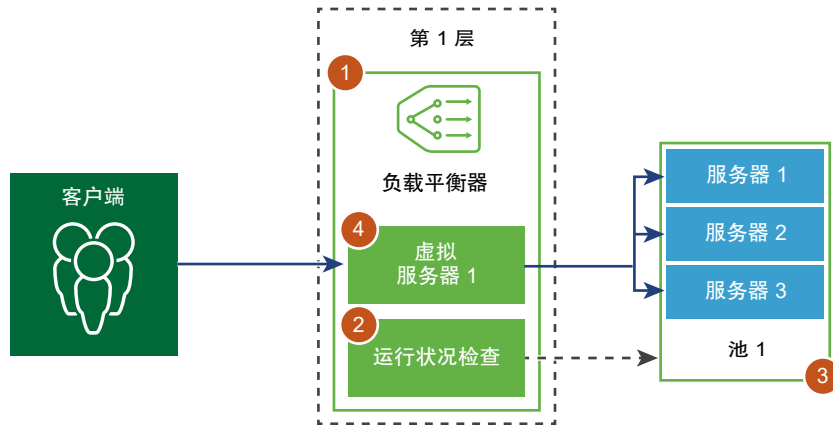
当负载均衡器收到发往虚拟 IP 地址的客户端流量时，负载均衡器会选择一个服务器池成员并将客户端流量转发给该成员。在单臂模式下，负载均衡器将客户端 IP 地址替换为负载均衡器 IP 地址，以便服务器响应始终发送到负载均衡器，然后负载均衡器将该响应转发给客户端。



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。

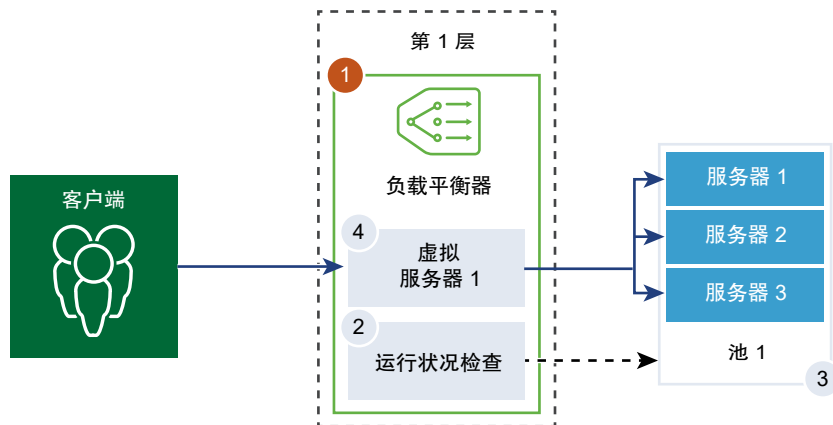


创建负载均衡器

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 选择网络 > 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。

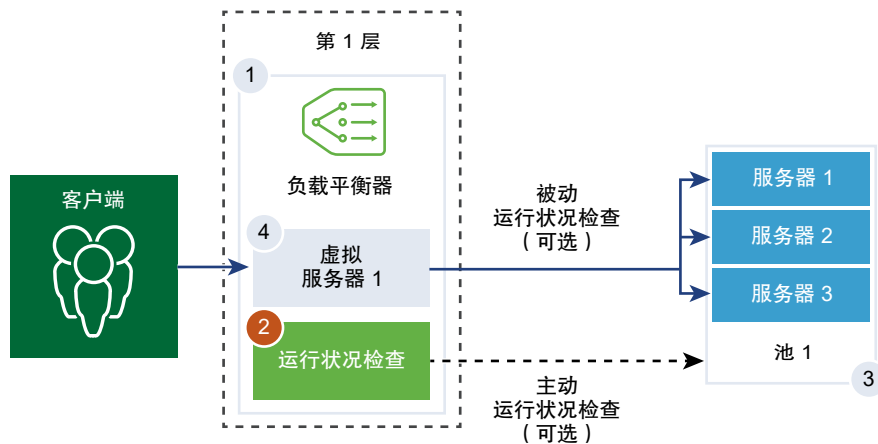
配置主动运行状况监控器

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，向服务器发送基本的 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。

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** 逻辑路由器后，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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。

- 2 选择**负载均衡器 > 网络 > 监控 > 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。

还可以在 NSX Manager 中使用预定义的协议：**http-monitor**、**https-monitor**、**icmp-monitor**、**Tcp-monitor** 和 **Udp-monitor**。

- 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。
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。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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 选择 **网络 > 负载均衡器 > 监控 > 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。

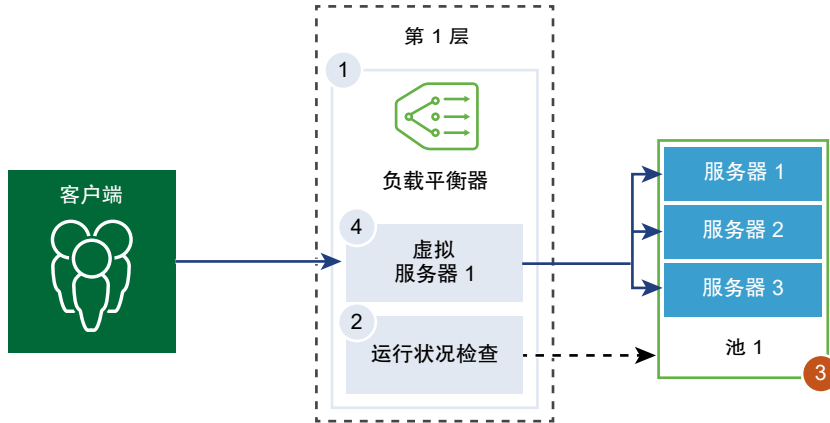
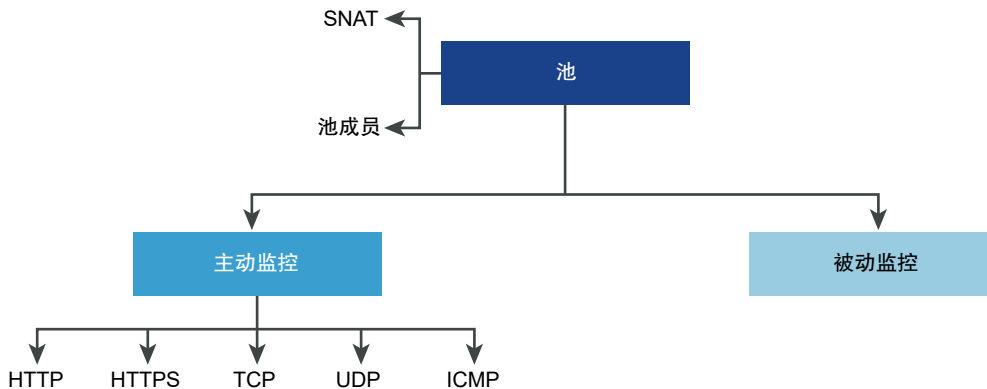


图 10-1. 服务器池参数配置



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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 选择网络 > 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** 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公平地分发负载。 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。如果主动成员未通过运行状况检查，则会对备份成员执行流量故障切换。

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。

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。

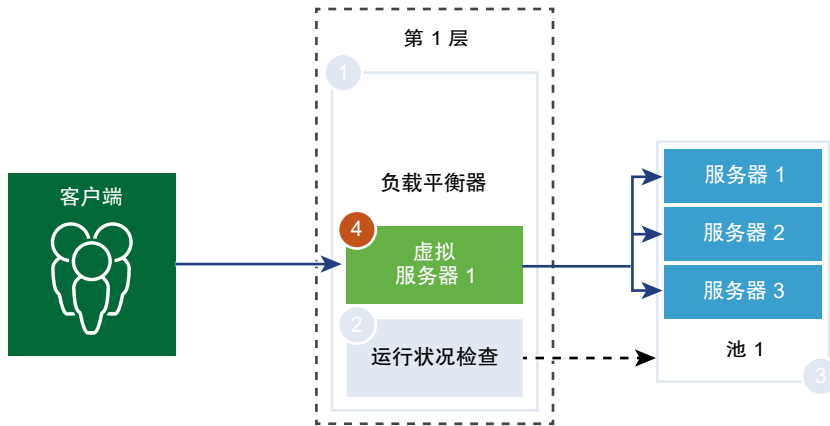
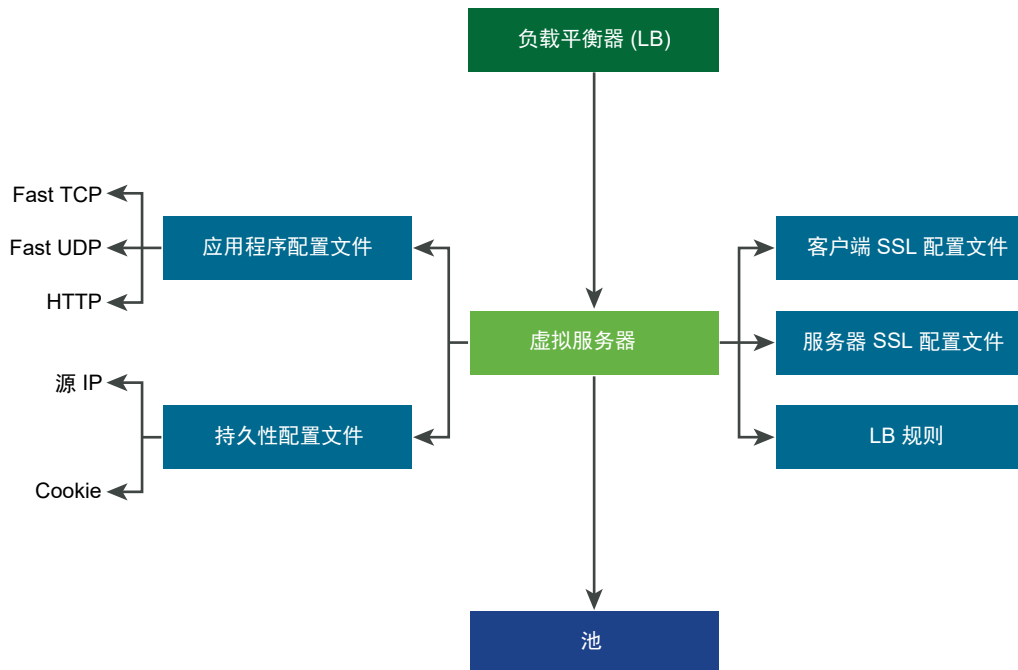


图 10-2. 虚拟服务器组件



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。快速 TCP、快速 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 10-3. 第 4 层 TCP 和 UDP 应用程序配置文件

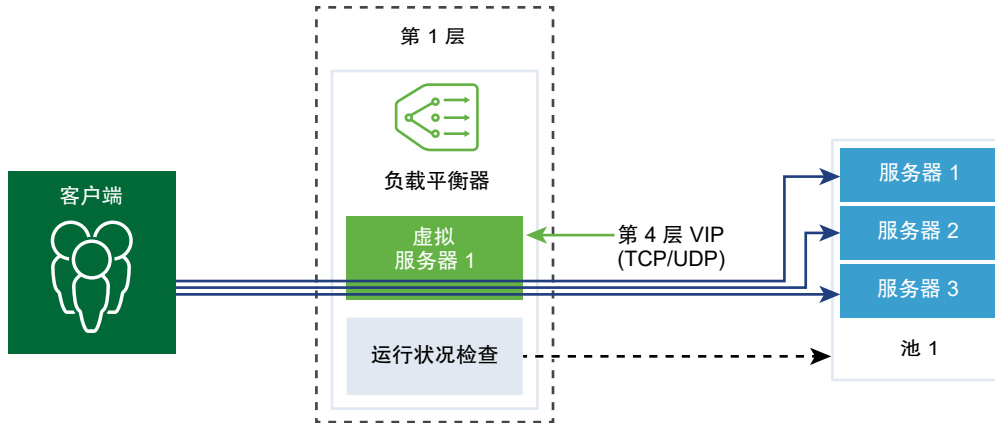
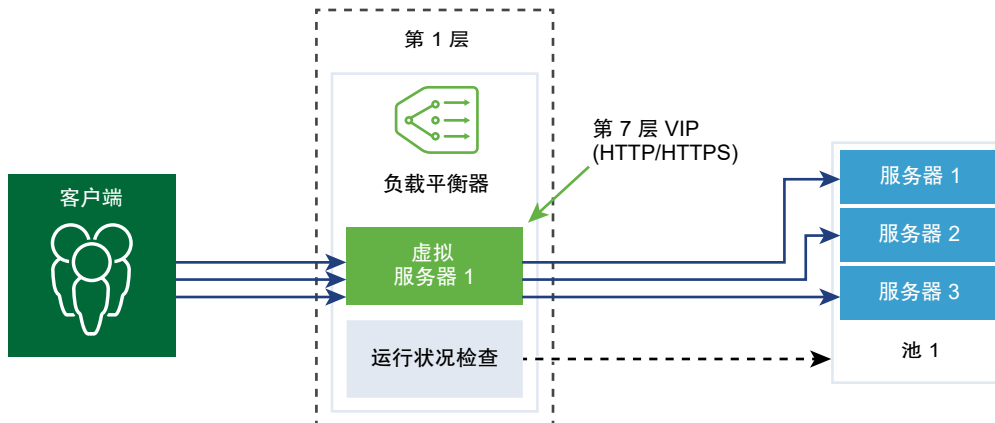


图 10-4. 第 7 层 HTTPS 应用程序配置文件



步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 选择网络 > 负载均衡器 > 配置文件 > 应用程序配置文件。
- 3 创建一个快速 TCP 应用程序配置文件。
 - a 从下拉菜单中选择添加 > 快速 TCP 配置文件。
 - b 输入快速 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。

您也可以接受快速 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 创建一个快速 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 > 快速 UDP 配置文件**。
- 输入快速 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平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，则必须使用负载平衡规则。
X-Forwarded-For (XFF)	<ul style="list-style-type: none"> ■ INSERT - 如果入站请求中不存在 XFF HTTP 标头，则负载平衡器会插入一个带有客户端 IP 地址的新 XFF 标头。 ■ REPLACE - 如果入站请求中已存在 XFF HTTP 标头，则负载平衡器可以替换该标头。 <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平衡器上进行 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，可以将负载平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>
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平衡器关闭 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 身份验证的负载平衡，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，则负载平衡器将升级到 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。

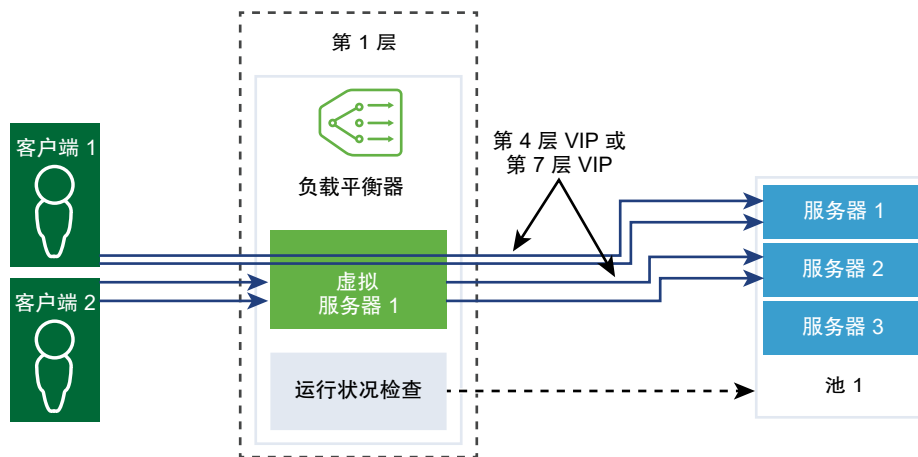
配置持久配置文件

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。



步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 选择网络 > 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	<p>切换该按钮以将持久性条目同步到 HA 对等项。</p>
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。

- a 从下拉菜单中选择**添加 > Cookie 持久性**。
- b 输入 Cookie 持久性配置文件的名称和描述。
- c 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。
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。 关闭浏览器后，会话 Cookie 和持久性 Cookie 类型都会过期。
最长空闲时间	输入 Cookie 过期之前可以处于空闲状态的时间（秒）。

- 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。负载平衡器充当客户端和服务器的 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 配置文件是指负载平衡器充当 SSL 服务器并终止客户端 SSL 连接。服务器端 SSL 配置文件是指负载平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 10-5. SSL 卸载

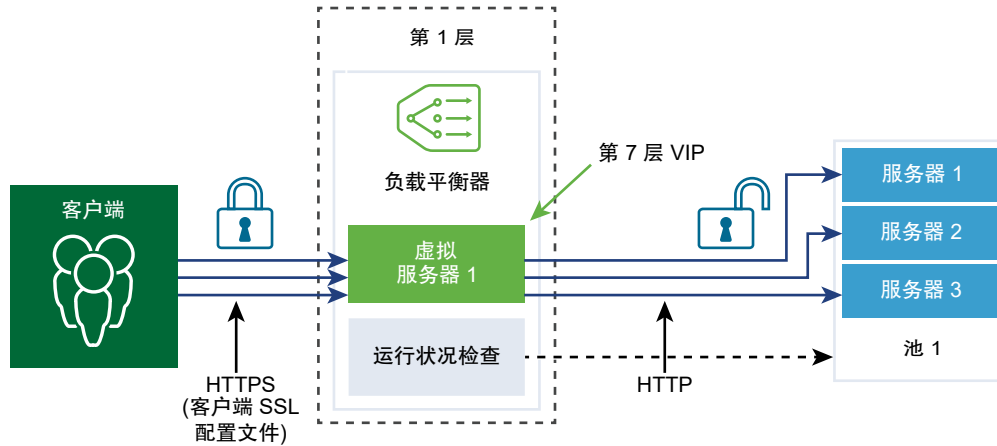
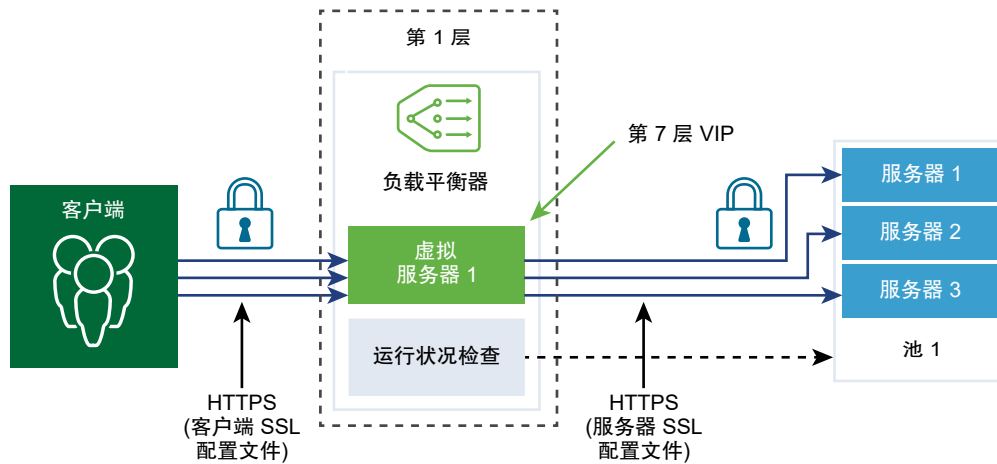


图 10-6. 端到端 SSL



步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 选择网络 > 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 选择**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 配置文件和服务端 SSL 配置文件。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 的 NSX Manager。
- 2 选择**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 `\0dd` 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。

- `$_args` - 请求中的参数
- `$_cookie_<name>` - `<name>` Cookie 的值
- `$_host` - 按优先级顺序，请求行中的主机名，或者“Host”请求标头字段中的主机名或与请求匹配的服务器名称
- `$_hostname` - 主机名
- `$_http_<name>` - 任意请求标头字段，`<name>` 是字段名称，该字段名称将转换为小写，并且其中的短划线将替换为下划线
- `$_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
- `$_ssl_server_name` - 通过 SNI 返回请求的服务器名称

■ \$_uri - 请求中的 URI 路径

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平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平衡器规则。

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

支持的匹配条件	说明
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
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

支持的匹配条件	说明
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 2.2 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，虚拟服务器可与快速 **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平衡器的服务器证书。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。

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。在这种情况下，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。

本章讨论了以下主题：

- 创建 DHCP 服务器配置文件
- 创建 DHCP 服务器
- 将 DHCP 服务器连接到逻辑交换机
- 将 DHCP 服务器与逻辑交换机断开连接
- 创建 DHCP 中继配置文件
- 创建 DHCP 中继服务
- 将 DHCP 服务添加到逻辑路由器端口

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **网络 > DHCP**。

- 3 单击**服务器配置文件**，然后单击**添加**。
- 4 输入名称和可选的说明。
- 5 从下拉菜单中选择一个 NSX Edge 群集。
- 6 （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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > DHCP**。
- 3 单击**服务器**，然后单击**添加**。
- 4 输入名称和可选的说明。
- 5 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。
- 6 （必选）从下拉菜单中选择一个 DHCP 配置文件。
- 7 （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。
- 8 （可选）输入无类静态路由选项。
- 9 （可选）输入其他选项。
- 10 单击**保存**。
- 11 选择新创建的 DHCP 服务器。
- 12 展开“IP 池”部分。
- 13 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。
- 14 展开“静态绑定”部分。
- 15 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。VLAN 逻辑交换机不支持 DHCP 服务器。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **网络 > 交换**。
- 3 单击要将 DHCP 服务器连接到的逻辑交换机。
- 4 单击 **操作 > 连接 DHCP 服务器**。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **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 服务器。在创建 DHCP 中继服务时，您必须指定一个 DHCP 中继配置文件。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **网络 > DHCP**。
- 3 单击 **中继配置文件**，然后单击 **添加**。
- 4 输入名称和可选的说明。
- 5 输入一个或多个外部 DHCP 服务器地址。

后续步骤

创建 DHCP 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **网络 > DHCP**。
- 3 单击 **中继服务**，然后单击 **添加**。
- 4 输入名称和可选的说明。
- 5 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 服务添加到逻辑路由器端口](#)。

将 DHCP 服务添加到逻辑路由器端口

在将 DHCP 中继服务添加到逻辑路由器端口时，连接到该端口的逻辑交换机上的虚拟机可以与中继服务中配置的 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](#)。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **网络 > 路由**。
- 3 选择连接到所需逻辑交换机的路由器，然后单击 **配置** 选项卡。
- 4 选择连接到所需逻辑交换机的路由器端口，然后单击 **编辑**。
- 5 从 **DHCP 服务** 下拉列表选择一个 DHCP 中继服务，然后单击 **保存**。

逻辑路由器端口将在 **DHCP 服务** 列中显示该 DHCP 中继服务。

也可以在添加新的逻辑路由器端口时选择 DHCP 中继服务。

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 群集中的两个或更多 NSX Edge 节点上运行。

本章讨论了以下主题：

- [添加元数据代理服务器](#)
- [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与逻辑交换机断开连接](#)

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，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 的 NSX Manager。
- 2 从导航面板中选择 **网络 > DHCP**。
- 3 单击 **元数据代理** 选项卡。
- 4 单击 **添加**。

- 5 输入元数据代理服务器的名称。
- 6 （可选）输入说明。
- 7 输入 Nova 服务器的 URL 和端口。
有效端口值为 3000 - 9000。
- 8 输入密钥的值。
- 9 从下拉列表中选择一个 NSX Edge 群集。
- 10 （可选）选择该 NSX Edge 群集的成员。

示例

例如：

New Metadata Proxy Server ⓘ ×

Name* metadata-proxy-1

Description

Nova Server URL* https://123.1.1.1:8775

Secret* *****

Edge Cluster* edge_cluster_p1r1 ▼

Members 53524616-c67f-11e8-837f-020046520048 × ▼

CANCEL ADD

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，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 的 NSX Manager。
- 2 从导航面板中选择 **网络 > DHCP**。

- 3 单击**元数据代理**选项卡。
- 4 选择一个元数据代理服务器。
- 5 选择**操作 > 连接到逻辑交换机**菜单选项。
- 6 从下拉列表中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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**网络 > DHCP**。
- 3 单击**元数据代理**选项卡。
- 4 选择一个元数据代理服务器。
- 5 选择**操作 > 与逻辑交换机断开连接**菜单选项。
- 6 从下拉列表中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-T 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》。

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-T Container Plug-in 要求您为这些容器创建 IP 块。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**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**。

策略是规则和服务的组合，其中，规则定义资源访问和使用条件。通过 **NSX 策略**，您可以管理资源访问和使用情况，而不必担心较低级别的细节。

本章讨论了以下主题：

- [概述](#)
- [添加实施点](#)
- [添加服务](#)
- [添加域](#)
- [配置 NSX Policy Manager 的备份](#)
- [备份 NSX Policy Manager](#)
- [还原 NSX Policy Manager](#)
- [将 vIDM 主机与 NSX Policy Manager 相关联](#)
- [管理角色分配](#)

概述

通过 **NSX 策略**，您可以为虚拟机、逻辑端口、IP 地址和 MAC 地址等对象指定规则，而不必担心这些规则的机制。您可以通过 **NSX Policy Manager**（而不是 **NSX Manager**）管理策略。

在配置策略之前，您必须安装 **NSX Policy Manager**。有关详细信息，请参见《**NSX-T 安装指南**》。在 **NSX Policy Manager** 中，您还必须添加一个或多个实施点，以提供有关将应用策略的 **NSX Manager** 的信息。

以下示例说明了如何使用策略管理应用程序的网络连接。

应用程序具有三层（**Web**、应用程序和数据库），并且您希望将以下规则应用于应用程序的虚拟机：

- 允许 **Web** 层和应用程序层之间的流量。
- 允许应用程序层和数据库层之间的流量。
- 允许任何系统和 **Web** 层之间的流量。

在 **NSX Manager** 上执行以下步骤：

- 将 **Web** 虚拟机的工作负载名称设置为 **Web**，并后跟某个标识字符串。

- 将应用程序虚拟机的工作负载名称设置为 **App**，并后跟某个标识字符串。
- 将数据库虚拟机的工作负载名称设置为 **DB**，并后跟某个标识字符串。

在 **NSX Policy Manager** 上执行以下步骤：

- 创建一个域并指定以下内容：
 - 创建一个名为 **WebGroup** 的组，其中包含工作负载名称以 **Web** 开头的虚拟机。
 - 创建一个名为 **AppGroup** 的组，其中包含工作负载名称以 **App** 开头的虚拟机。
 - 创建一个名为 **DBGGroup** 的组，其中包含工作负载名称以 **DB** 开头的虚拟机。
 - 指定用于控制组之间通信的安全策略。
- 验证域配置以确保没有错误。
- 选择实施点。

选择实施点后，**NSX Policy Manager** 将在这些实施点与 **NSX Manager** 通信，而这些实施点将实施安全策略。

基于角色的访问控制

NSX Policy Manager 具有两个内置用户：**admin** 和 **audit**。您可以将 **NSX Policy Manager** 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 Policy Manager** 的身份验证策略，后者仅适用于 **admin** 和 **audit** 用户。

添加实施点

实施点是要应用策略规则的位置。在该版本中，实施点必须是 **NSX-T** 安装，**NSX Policy Manager** 仅支持一个实施点。

步骤

- 1 从浏览器中，登录到 **NSX Policy Manager**，网址为 <https://nsx-policy-manager-IP-address>。
- 2 从导航面板中选择 **系统 > 实施点**。
- 3 单击 **添加**。
- 4 提供以下信息。

参数	说明
名称	实施点的名称。
凭据	用于登录到 NSX Manager 的用户名和密码。
实施地址	NSX Manager 的 IP 地址。
指纹	NSX Manager 的证书指纹。

5 单击保存。

添加服务

服务是您环境中的协议或软件组件。策略包含应用于服务的规则。

服务示例包括 FTP、HTTP、AD 服务器、DHCP 服务器、Oracle 数据库等。

步骤

- 1 从浏览器中，登录到 NSX Policy Manager，网址为 <https://nsx-policy-manager-IP-address>。
- 2 从导航面板中选择**基础架构 > 服务**。
- 3 单击**添加新服务**。
- 4 输入服务的名称。
- 5 单击**设置服务条目**以添加服务条目。
 - a 单击**添加新的服务条目**。
 - b 选择服务类型。

可用类型为 **IP**、**IGMP**、**ICMP**、**ALG**、**TCP** 和 **UDP**。
 - c 单击**其他属性**下拉列表以选择属性。

可以添加其他条目，还可以编辑或删除条目。
- 6 单击**保存**。

添加域

域是具有一个共同的业务目标且需要应用策略的工作负载的逻辑集合。它包含一系列组及其相应的通信要求。

如果您计划创建多个大型域（每个域具有 200 个以上结果规则），请务必按顺序将其部署到实施点，等待每个域实现后，再继续下一个域。如果使用 API 部署这些域，建议先创建通信条目，然后再将域部署到实施点。

步骤

- 1 从浏览器中，登录到 NSX Policy Manager，网址为 <https://nsx-policy-manager-IP-address>。
- 2 从导航面板中选择**基础架构 > 域**。
- 3 单击**添加域**以添加一个域。
- 4 指定域名和描述（可选）。
- 5 单击**下一步**转到“工作负载组”步骤。

- 6 单击**添加组**以添加一个或多个工作负载组。对于每个工作负载组，
 - a 请指定一个名称。
 - b 单击**成员类型**字段以选择成员的类型。
可用选项为**虚拟机**、**IP 地址**和**成员资格条件**。
 - c 对于**虚拟机**和**IP 地址**，请指定一个值。
 - d 对于**成员资格条件**，请单击**设置成员资格条件**以指定如何选择成员。
- 7 单击**下一步**转到“安全”步骤。
- 8 单击**添加新区域**以添加防火墙区域，或者单击**添加新规则**以添加防火墙规则。
您可以添加多个区域和多个规则。
- 9 单击**下一步**转到“验证域配置”步骤。
将显示域的图形表示。
- 10 单击**下一步**转到“选择实施点”步骤。
- 11 选择一个或多个实施点。
- 12 单击**完成**以部署域。

配置 NSX Policy Manager 的备份

您可以备份 NSX Policy Manager 来保护 Policy Manager 存储的数据。在执行备份之前，您必须配置备份属性。

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 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，登录到 NSX Policy Manager，网址为 <https://nsx-policy-manager-IP-address>。
- 2 从导航面板中选择**系统 > 实用程序**。
- 3 单击**配置**。
- 4 单击**自动备份**开关以启用或禁用自动备份。
- 5 输入备份文件服务器的 IP 地址或主机名。
- 6 根据需要编辑默认端口。
- 7 输入登录到备份文件服务器所需的用户名和密码。
- 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。

- 9 输入用于加密备份数据的密码短语。

您需要使用该密码短语还原备份。如果忘记了备份密码短语，则无法还原任何备份。

- 10 输入存储备份的服务器的 SSH 指纹。请参见[查找远程服务器的 SSH 指纹](#)。

- 11 单击**计划**选项卡。

- 12 选择频率。

如果选择**每周**，则指定星期几以及当天的时间。如果选择**间隔**，则指定间隔。

- 13 单击**保存**。

备份 NSX Policy Manager

您可以自动或手动备份 NSX Policy Manager。

如果您已配置自动备份，则备份将自动运行。此过程适用于手动启动备份。

前提条件

确认您已配置备份属性。请参见[配置 NSX Policy Manager 的备份](#)。

步骤

- 1 从浏览器中，登录到 NSX Policy Manager，网址为 <https://nsx-policy-manager-IP-address>。
- 2 从导航面板中选择**系统 > 实用程序**。
- 3 单击**立即备份**。

还原 NSX Policy Manager

您可以从备份将 NSX Policy Manager 还原到过去的状态。

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 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，登录到 NSX Policy Manager，网址为 <https://nsx-policy-manager-IP-address>。
- 2 从导航面板中选择**系统 > 实用程序**。
- 3 单击**立即还原**。
- 4 确认有关必备条件和风险的消息，然后单击**下一步**。
- 5 输入备份服务器的 IP 地址或主机名。
- 6 根据需要更改端口号。

默认值为 22。

- 7 输入用户名和密码以登录到服务器。
- 8 在**备份目录**字段中，输入存储备份的绝对目录路径。
- 9 输入用于加密备份数据的密码短语。
- 10 输入备份服务器的 SSH 指纹。
- 11 单击**下一步**。
- 12 选择一个备份。
- 13 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结构层节点或传输节点，将提示您执行某些操作，例如，登录到节点并运行脚本。

在还原操作完成后，将显示“还原完成”屏幕，将在其中显示还原结果、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，该屏幕将显示发生故障的步骤。要重试还原操作，必须使用新的 Policy Manager 设备，而不能使用发生故障的设备。

将 vIDM 主机与 NSX Policy Manager 相关联

要允许将 NSX Policy Manager 与 vIDM 集成在一起，您必须提供有关 vIDM 主机的信息。

vIDM 服务器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 Policy Manager 登录到 vIDM。有关在 vIDM 上安装 CA 签名证书的信息，请参见 <https://docs.vmware.com/cn/VMware-Identity-Manager/3.1/vdm-install/GUID-B76761BF-4B12-4CD5-9366-B0A1A2BF2A8B.html>。

在向 vIDM 注册 NSX Policy Manager 时，指定指向 Policy 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 Policy 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。

前提条件

- 确认您具有从 vIDM 主机中获取的证书指纹。请参见[从 vIDM 主机中获取证书指纹](#)。
- 确认在 vIDM 主机中将 NSX Policy 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，请参阅 VMware Identity Manager 文档，网址为 [《》](#)。

步骤

- 1 从浏览器中，登录到 NSX Policy Manager，网址为 <https://nsx-policy-manager-IP-address>。
- 2 从导航面板中选择**系统 > 用户**。
- 3 单击**配置**选项卡。
- 4 单击**编辑**。
- 5 将 **VMware Identity Manager 集成** 切换按钮设置为已启用。

6 提供以下信息。

参数	说明
VMware Identity Manager 设备	vIDM 主机的完全限定域名 (Fully Qualified Domain Name, FQDN)。
OAuth 客户端 ID	在 vIDM 主机中注册 NSX Policy Manager 时创建的 ID。
OAuth 客户端密码	在 vIDM 主机中注册 NSX Policy Manager 时创建的密码。
SHA-256 指纹	vIDM 主机的证书指纹。
NSX 策略设备	NSX Policy Manager 的 IP 地址或完全限定域名 (FQDN)。如果您指定 FQDN，则必须在 URL 中使用 NSX Policy Manager 的 FQDN 从浏览器访问管理器，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 Policy Manager 客户端，以便使用 FQDN 或 IP 地址进行连接。

7 单击保存。

管理角色分配

如果 VMware Identity Manager 与 NSX Policy Manager 集成在一起，您可以添加、更改和删除为用户或用户组分配的角色。

系统预定义了以下角色。您无法添加新角色。

- 企业管理员
- 审核员
- 站点可靠性工程师（在 VMware Cloud 部署中可用）
- 云服务管理员（在 VMware Cloud 部署中可用）
- 云服务审核员（在 VMware Cloud 部署中可用）

前提条件

- 确认 vIDM 主机与 NSX Policy Manager 相关联。有关详细信息，请参见 [将 vIDM 主机与 NSX Policy Manager 相关联](#)。

步骤

- 1 从浏览器中，登录到 NSX Policy Manager，网址为 <https://nsx-policy-manager-IP-address>。
- 2 从导航面板中选择 **系统 > 用户**。
- 3 如果尚未选择 **角色分配** 选项卡，请单击该选项卡。
- 4 添加、更改或删除角色分配。

选项	操作
添加角色分配	单击 添加 ，选择用户或用户组，然后选择角色。
更改角色分配	选择一个用户或用户组，然后单击 编辑 。
删除角色分配	选择一个用户或用户组，然后单击 删除 。

使用服务插入，可以对通过路由器的南北向流量和东西向流量应用第三方服务。通常情况下，这些服务会提供高级安全功能，例如，入侵检测系统 (IDS) 或入侵防御系统 (IPS)。

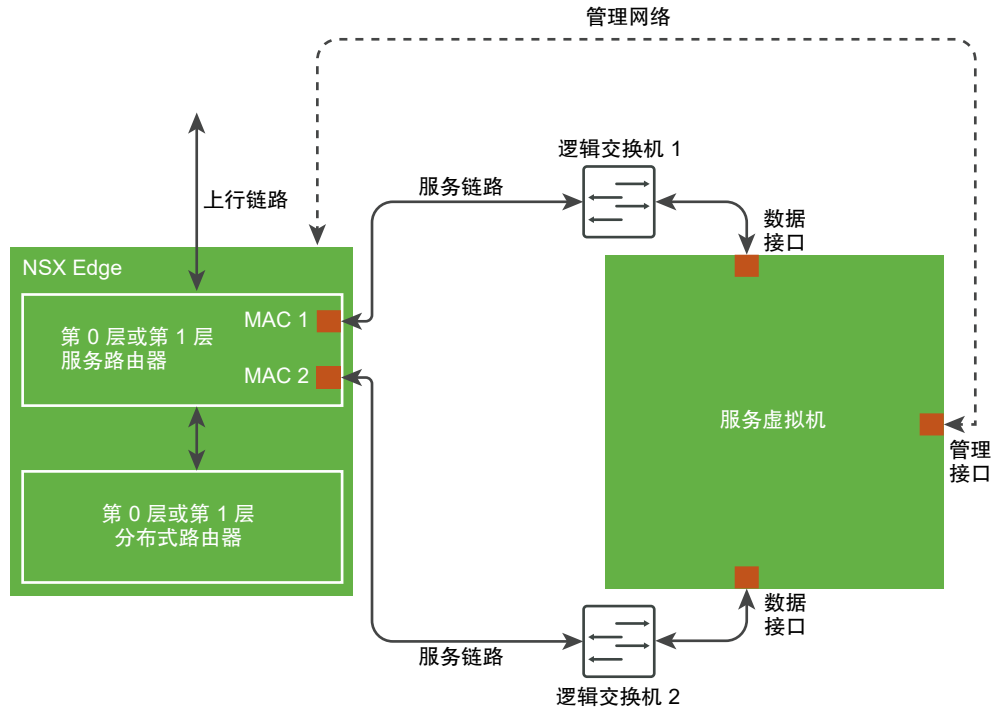
本章讨论了以下主题：

- [概述](#)
- [注册服务](#)
- [部署服务实例](#)
- [配置流量重定向](#)
- [监控流量重定向](#)

概述

可以设置服务插入，以将第 0 层路由器上的南北向流量或第 1 层路由器上的东西向流量重定向到虚拟机。在虚拟机中运行的服务可以处理流量，并采取适当操作。

以下架构图显示了配置有服务插入时的数据流。



服务插入在具有两个 **Edge** 节点和两个服务虚拟机的主动-备用模式下支持高可用性 (HA)。在主动-主动模式下不支持 HA。一个路由器只支持一个服务。

设置服务插入需要执行以下步骤：

- 注册服务。
- 部署服务实例。
- 配置流量重定向。

注册服务

注册服务需要进行 API 调用。注册服务后，可以在 NSX Manager UI 中进行查看。

有关 API 调用和输入参数的详细信息，请参见《NSX-T Data Center API 参考》。

步骤

- 1 执行以下 API 调用，以注册服务：

```
POST /api/v1/serviceinsertion/services
```

例如，

```
POST https://<nsx-mgr>/api/v1/serviceinsertion/services
{
  "display_name": "NS Service for ABC partner",
  "description": "This service is inserted at T0 router and it provides advanced security",
  "attachment_point": [
```

```

    "TIER0_LR"
  ],
  "functionalities": [
    "NG_FW"
  ],
  "implementations": [
    "NORTH_SOUTH"
  ],
  "transports": [
    "L2_BRIDGE"
  ],
  "vendor_id": "ABC_Partner",
  "on_failure_policy": "ALLOW",
  "service_deployment_spec": {
    "deployment_specs": [{
      "ovf_url": "http://server.com/dir1/ABC-Company-HA-OVF/ABC-VM-ESX-2.0.ovf",
      "name": "NS_DepSpec",
      "host_type": "ESXI",
      "service_form_factor": "MEDIUM"
    }],
    "nic_metadata_list": [
      {
        "interface_label": "eth",
        "interface_index": 0,
        "interface_type": "MANAGEMENT"
      },
      {
        "interface_label": "eth",
        "interface_index": 1,
        "interface_type": "DATA1"
      },
      {
        "interface_label": "eth",
        "interface_index": 2,
        "interface_type": "DATA2"
      }
    ]
  },
  "deployment_template": [{
    "name": "NS_DepTemp",
    "attributes": [{
      "attribute_type": "STRING",
      "display_name": "License",
      "key": "LicenseKey"
    }]
  }]
}

```

- 2 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 3 从导航面板中选择**合作伙伴服务**。
- 4 单击**目录**选项卡，并确保已注册服务。

后续步骤

部署服务的实例。请参见[部署服务实例](#)。

部署服务实例

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。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 的 NSX Manager。
- 2 从导航面板中选择**合作伙伴服务**。
- 3 单击**部署**。
- 4 输入实例名称和可选描述。
- 5 单击**合作伙伴服务**字段，然后选择一个服务。
- 6 选择**部署规范**。
- 7 选择逻辑路由器。
将仅显示未配置服务插入的路由器。
- 8 单击**下一步**。
- 9 单击**计算管理器**字段，然后选择一个计算管理器。
- 10 单击**群集**字段，然后选择一个群集。
- 11 （可选）单击**资源池**字段，然后选择一个资源池（如果已在 vCenter Server 中配置）。
- 12 单击**数据存储**字段，然后选择一个数据存储。
- 13 选择**部署模式**。
选项包括**独立**或**高可用性**。
- 14 选择**故障策略**。
选项包括**允许**或**阻止**。
- 15 输入虚拟机的 IP 地址。
- 16 输入虚拟机 IP 地址的默认网关。
- 17 输入虚拟机 IP 地址的子网掩码。
- 18 单击**下一步**。
- 19 选择**部署模板**。
- 20 输入合作伙伴服务的许可证。
- 21 单击**完成**。

结果

部署过程可能需要一些时间，具体取决于供应商的实施。您可以在管理器用户界面中查看状态。部署成功后，状态将为部署成功。

后续步骤

为服务实例配置流量重定向。请参见[配置流量重定向](#)。

配置流量重定向

部署服务实例后，可以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[第 7 章 防火墙区域和防火墙规则](#)。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**合作伙伴服务**。
- 3 单击服务实例的名称。
- 4 单击**流量重定向**选项卡。
- 5 添加或移除区域和规则。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**合作伙伴服务**。
- 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。

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 组件的列表和说明，请参见《NSX-T Data Center 安装指南》中的 [NSX Cloud 架构和组件](#)。

本章讨论了以下主题：

- [Cloud Service Manager](#)
- [管理隔离策略](#)
- [载入并管理工作负载虚拟机概览](#)
- [载入工作负载虚拟机](#)
- [管理工作负载虚拟机](#)
- [使用 NSX Cloud 高级功能](#)
- [故障排除](#)

Cloud Service Manager

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 管理隔离策略 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专用网络的数量。
- 您可以查看每个专用网络的工作负载虚拟机的数量。

云下有四个选项卡。

另请参见 [CSM 图表和图标](#)，了解 UI 元素的说明。

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”下方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 或 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 运行状况指示信息。

云 > {Your Public Cloud} > VPC 或 VNet

“VPC 或 VNet” 部分显示私有云清单。

可以按帐户和区域筛选清单。

- 每个卡代表一个 VPC 或 VNet。
- 可以在每个 VPC 或 VNet 上部署一个或两个（实现 HA）PCG。
- 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。
- 单击操作可访问以下界面：
 - **编辑配置：**
 - 启用或禁用隔离策略。
 - 更改代理服务器选择。
 - **部署 NSX Cloud 网关：**单击此选项可开始在此 VPC 或 VNet 上部署 PCG。如果已部署一个 PCG 或一对高可用性 PCG，则此选项不可用。有关详细说明，请参见《NSX-T Data Center 安装指南》中的部署 PCG。

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。

注 CSM 显示 NSX 管理的虚拟机的操作系统版本值，但对于不由 NSX 管理的虚拟机，显示的操作系统类型非常笼统，因为是从云提供商 API 获取的。

CSM 图表和图标

CSM 使用直观的描述性图标来显示公有云构造的状态和运行状况。

注 仅当开启启用隔离设置时，隔离 workflow 才适用。默认情况下，该设置处于禁用状态。

VNet

图 16-1. 由 NSX Cloud 管理的处于正常状态的虚拟机的 VNet

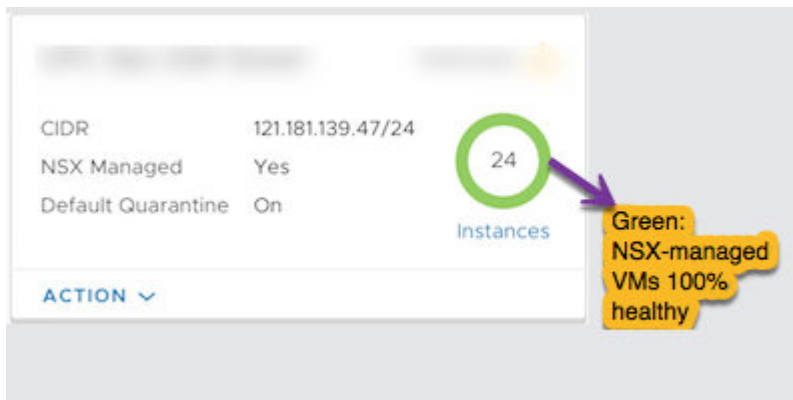


图 16-2. 由 NSX Cloud 管理的存在错误的虚拟机的 VNet

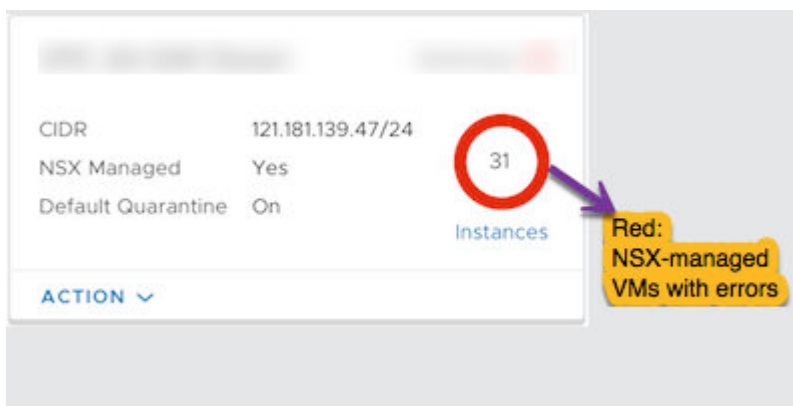


图 16-3. 虚拟机已关闭电源的 VNet

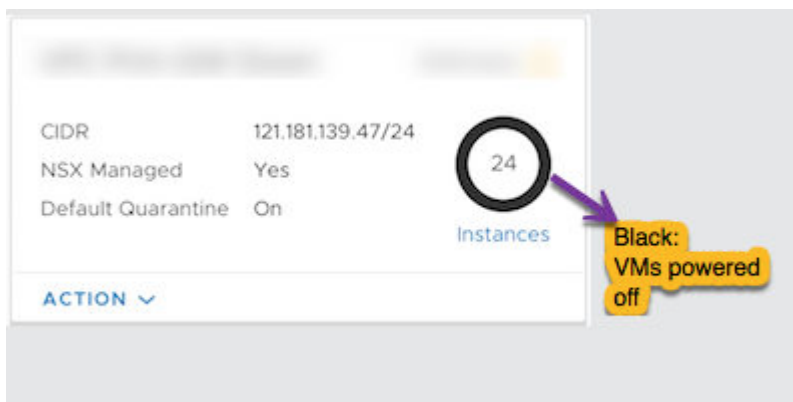


图 16-4. 显示“默认隔离”状态的 VNet

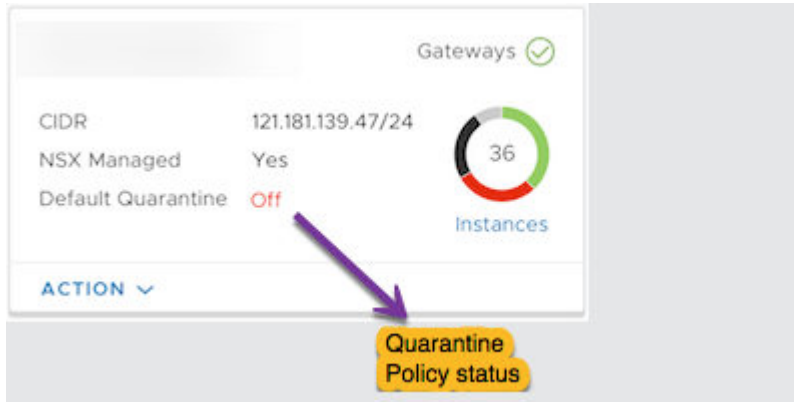
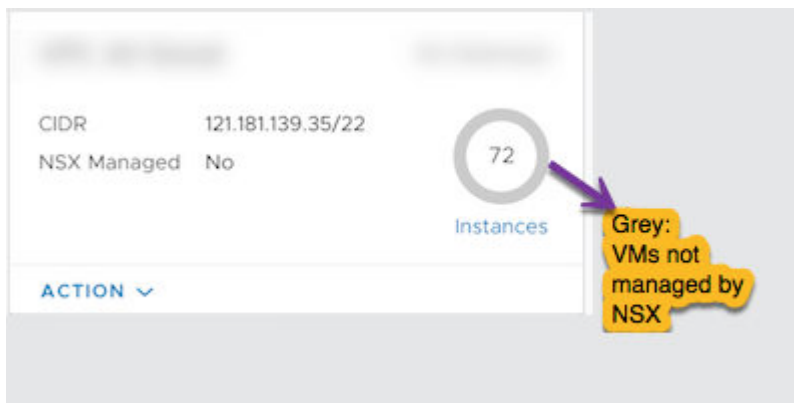


图 16-5. 不由 NSX Cloud 管理的虚拟机的 VNet



实例

受管实例

图 16-6. 由 NSX Cloud 管理的处于正常状态的实例

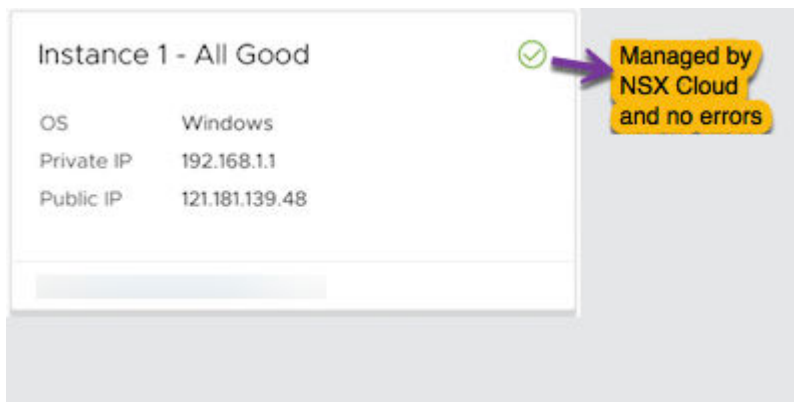


图 16-7. 由 NSX Cloud 管理的存在错误的实例

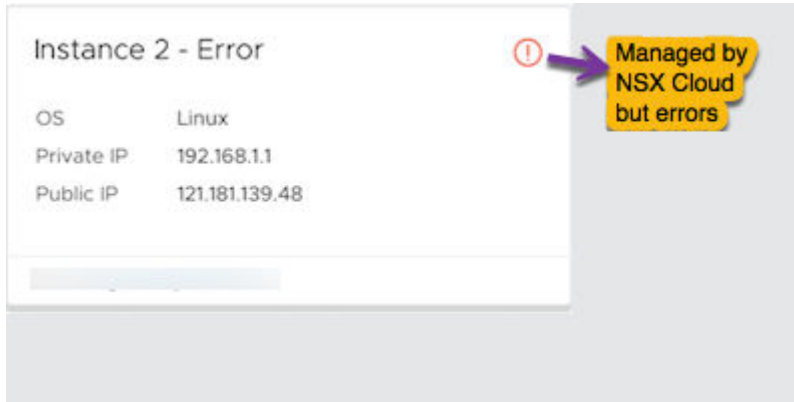


图 16-8. 由 NSX Cloud 管理的存在错误且已隔离的实例

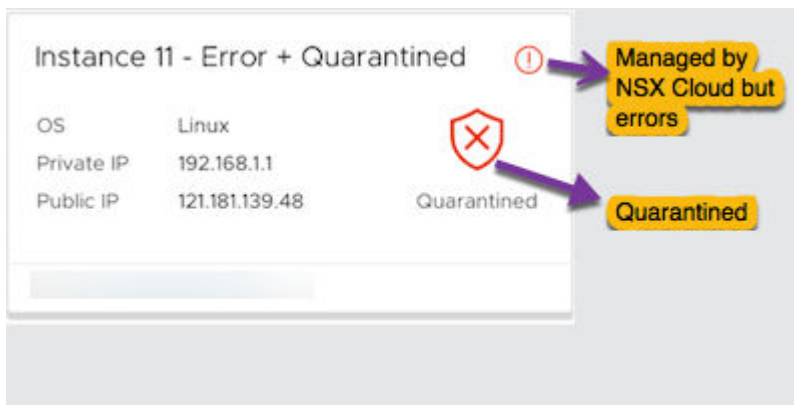
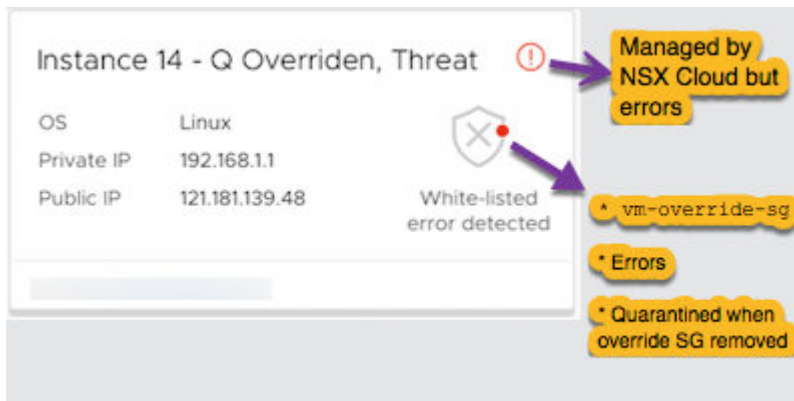
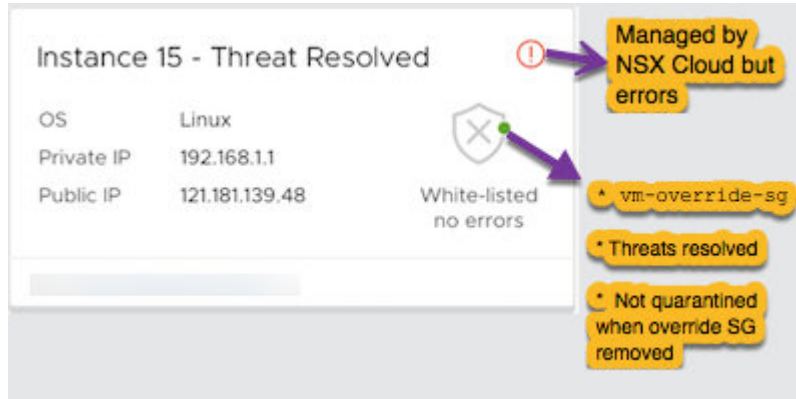
图 16-9. NSX Cloud 管理且已隔离的实例，但已通过应用 `vm-override-sg` 网络安全组来将其列入白名单

图 16-10. 由 NSX Cloud 管理且已隔离的实例，已解决错误并列入白名单。



非受管实例

图 16-11. 虚拟机不由 NSX Cloud 管理，且已默认隔离

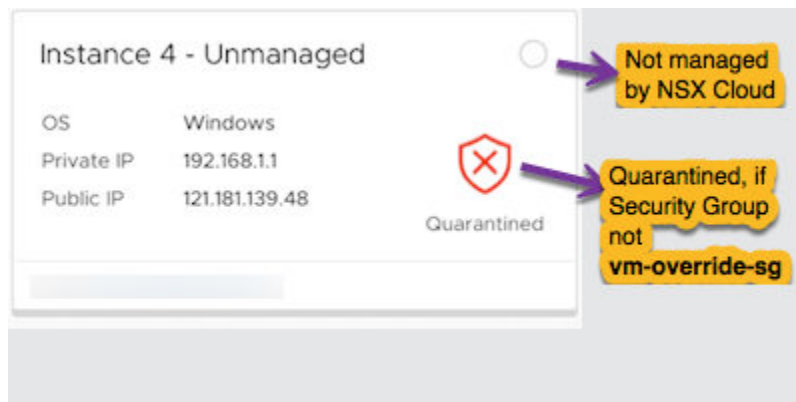
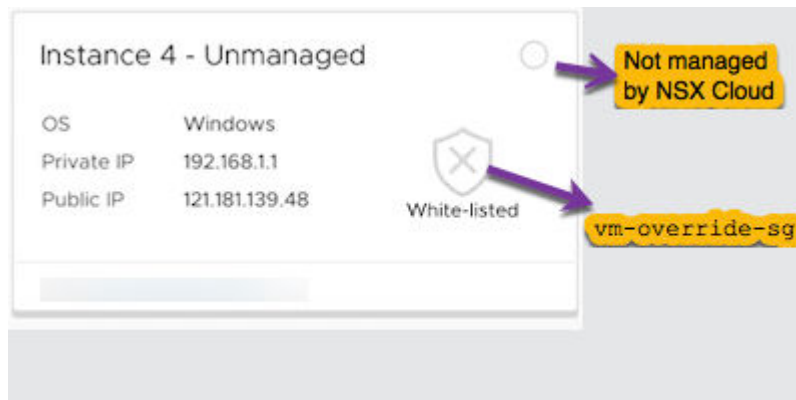


图 16-12. 虚拟机不由 NSX Cloud 管理，但已通过应用 vm-override-sg 来将其列入白名单



公有云网关 (PCG)

图 16-13. 主要 PCG 和辅助 PCG 均已启动的 VNet

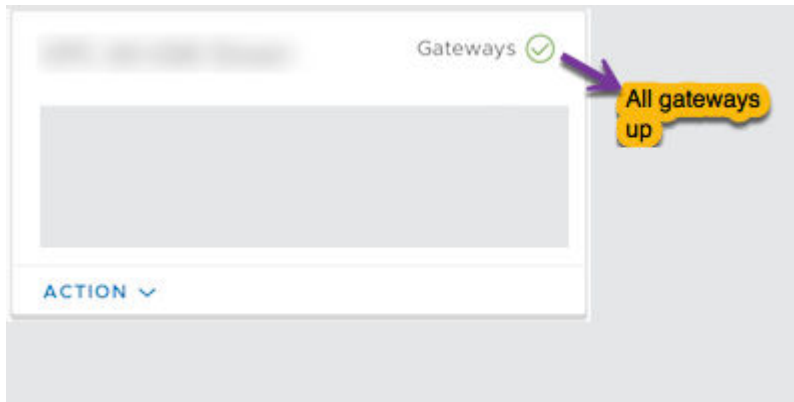


图 16-14. 主要 PCG 或辅助 PCG 已关闭的 VNet

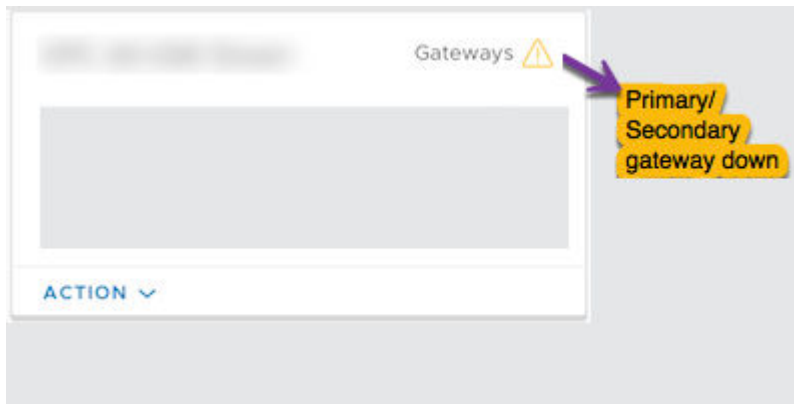
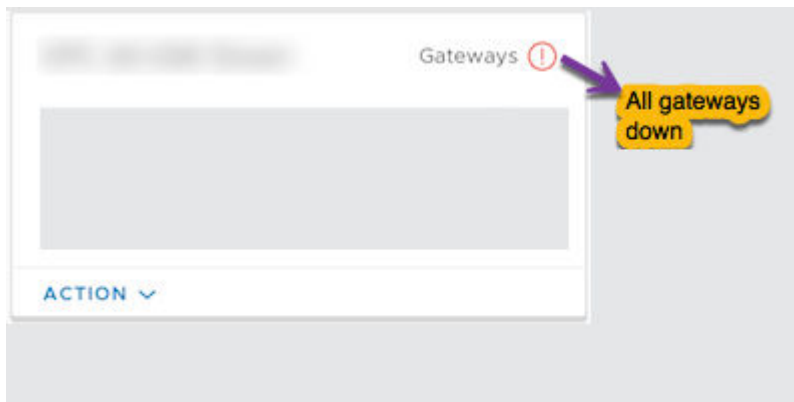


图 16-15. 主要 PCG 和辅助 PCG 均已关闭的 VNet



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，并且您必须具有管理员特权，以便登录到 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 打开到 NSX Manager 的 SSH 会话。
- 2 在 NSX Manager 上，运行 `get certificate api thumbprint` 命令。

```
NSX-Manager> get certificate api thumbprint
```

命令输出是该 NSX Manager 特有的数字串。

- 3 以企业管理员角色登录到 CSM。
- 4 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**。

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。

- 5 输入 NSX Manager 的详细信息。

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	输入企业管理员角色的用户名和密码。
Manager 指纹	输入您在步骤 2 获取的 NSX Manager 的指纹值。

- 6 单击**连接**。

CSM 将验证 NSX Manager 指纹并建立连接。

（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。

管理隔离策略

了解如何启用或禁用隔离策略并了解由此对工作负载虚拟机带来的影响。

NSX Cloud 使用公有云安全组执行威胁检测。例如，启用隔离策略时，如果 NSX 代理被迫在具有恶意企图的受管虚拟机上停止，则会使用 `quarantine`（在 Microsoft Azure 中）或 `default`（在 AWS 中）安全组将受到危害的虚拟机隔离。

一般建议：

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。

注 启用隔离策略后，请对工作负载虚拟机应用 `vm_override_sg`，以便能够将其载入，然后在由 NSX Cloud 管理后移除此安全组。请在两分钟内将合适的安全组应用到虚拟机。

如何启用或禁用隔离策略

部署 PCG 时，可以选择启用或禁用隔离策略。请执行以下步骤按顺序启用或禁用隔离策略。

前提条件

必须在 VPC 或 VNet 上部署一个或一对 PCG。

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。单击部署并运行一个或一对 PCG 的 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。
- 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**。



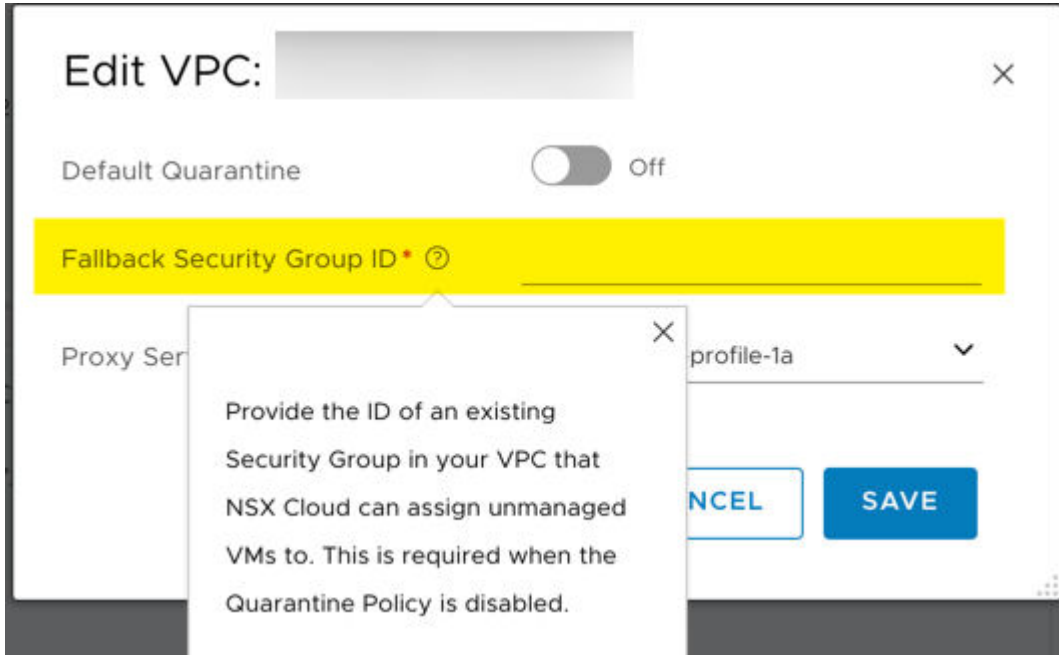
- ◆ 如果位于 VPC 或 VNet 的页面中，请单击“操作”图标以转到**编辑配置**。



- 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。有关 NSX Cloud 安全组列表，请参见 [公有云的 NSX Cloud 安全组](#)。



- 禁用隔离策略后，此 VPC 或 VNet 中的所有非受管虚拟机或隔离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

隔离策略：已禁用

当隔离策略已禁用时：

- NSX Cloud 不会将任何安全组分配给在此 VPC 或 VNet 中启动的虚拟机。必须将相应的 NSX Cloud 安全组分配给虚拟机才可启用威胁检测。

从 Microsoft Azure 门户或 AWS 控制台：

- ■ 将 `vm-underlay-sg` 分配给您希望对其使用 Microsoft Azure 或 AWS 提供的底层网络的虚拟机。

隔离策略：已启用，然后再禁用

下表列出了隔离策略已启用然后再禁用时对安全组分配的影响：

表 16-1. 禁用隔离策略对安全组的影响

虚拟机 ID	受管？	安全组	禁用隔离策略后的虚拟机安全组
虚拟机 1	是	vm_underlay_sg	vm_underlay_sg。从此虚拟机移除 <code>nsx.network</code> 标记以使其不受 NSX 管理时，此虚拟机还会分配有回退安全组。
虚拟机 2	是	default (AWS) 或 quarantine (Microsoft Azure)	禁用隔离策略时您指定的回退安全组。请参见 如何启用或禁用隔离策略 以了解详细信息。
虚拟机 3	否	vm_override_sg	禁用隔离策略时您指定的回退安全组。
虚拟机 4	否	default (AWS) 或 quarantine (Microsoft Azure)	禁用隔离策略时您指定的回退安全组。

注 要取消部署 PCG，必须禁用隔离策略。有关详细信息，请参见《NSX-T Data Center 安装指南》中的取消部署 PCG。

启用隔离策略时的影响

隔离策略：已启用

当隔离策略已启用时：

- 针对属于此 VPC 或 VNet 的任何工作负载虚拟机的所有接口进行的安全组 (SG) 或网络安全组 (NSG) 分配均由 NSX Cloud 管理，如下所示：
 - 为非受管虚拟机分配 quarantine NSG（在 Microsoft Azure 中）和 default 安全组（在 AWS 中）并将其隔离。这将限制此类虚拟机的出站流量并停止其所有入站流量。
 - 在虚拟机上安装 NSX 代理并在公有云中使用 `nsx.network` 对其进行标记时，未受管虚拟机可能会变为 NSX 管理的虚拟机。在默认情况下，NSX Cloud 将分配 vm-underlay-sg 以允许适当的入站/出站流量。
 - 如果在某个 NSX 管理的虚拟机上检测到威胁（如该虚拟机上的 NSX 代理被停止），则仍可向其分配 quarantine 或 default 安全组并将其隔离。
 - 对安全组进行的任何手动更改将在 2 分钟内恢复为 NSX 确定的安全组。

- 如果要将任何虚拟机移出隔离区，请将 `vm-override-sg` 作为唯一安全组分配给此虚拟机。NSX Cloud 不会自动更改 `vm-override-sg` 安全组，并允许通过 SSH 和 RDP 访问该虚拟机。移除 `vm-override-sg` 将再次导致虚拟机安全组恢复为 NSX 确定的安全组。

注 启用隔离策略后，在虚拟机上安装 NSX 代理之前将 `vm-override-sg` 分配给虚拟机。按照安装 NSX 代理并将虚拟机标记为底层的过程执行操作后，从虚拟机中移除 `vm-override-sg` NSG。此后，NSX Cloud 会自动向 NSX 管理的虚拟机分配适当的安全组。必须执行此步骤，才能确保您在为 NSX Cloud 准备虚拟机时不会向虚拟机分配 `quarantine` 或 `default` 安全组。

隔离策略：已禁用，然后再启用

下表列出了隔离策略已禁用然后再启用时对安全组分配的影响：

表 16-2. 启用隔离策略对安全组的影响

虚拟机 ID	受管?	检测到威胁?	启用隔离策略后的安全组
虚拟机 1	是	否	<code>vm_underlay_sg</code> 。
虚拟机 2	是	是	<code>default</code> (AWS) 或 <code>quarantine</code> (Microsoft Azure)
注 可以手动为受管虚拟机分配 <code>vm-override-sg</code> 。此操作会使其退出隔离模式，您可以通过 SSH 或 RDP 访问此类虚拟机来修复该问题。请参见 隔离策略：已启用			
虚拟机 3	否	不适用	<code>default</code> (AWS) 或 <code>quarantine</code> (Microsoft Azure)

公有云的 NSX Cloud 安全组

部署 PCG 时，NSX Cloud 将创建以下安全组：

`gw` 安全组应用于相应的 PCG 接口。

表 16-3. NSX Cloud 为 PCG 接口创建的公有云安全组

安全组名称	在 Microsoft Azure 中可用?	在 AWS 中可用?	全名
<code>gw-mgmt-sg</code>	是	是	网关管理安全组
<code>gw-uplink-sg</code>	是	是	网关上行链路安全组
<code>gw-vtep-sg</code>	是	是	网关下行链路安全组

表 16-4. NSX Cloud 为工作负载虚拟机创建的公有云安全组

安全组名称	在 Microsoft Azure 中可用?	在 AWS 中可用?	描述
quarantine	是	否	Microsoft Azure 隔离安全组
default	否	是	AWS 的隔离安全组
vm-underlay-sg	是	是	虚拟机非覆盖网络安全组
vm-override-sg	是	是	虚拟机替代安全组
vm-overlay-sg	是	是	虚拟机覆盖网络安全组（当前版本中未使用）
vm-outbound-bypass-sg	是	是	虚拟机出站绕过安全组（当前版本中未使用）
vm-inbound-bypass-sg	是	是	虚拟机进站绕过安全组（当前版本中未使用）

载入并管理工作负载虚拟机概览

有关公有云中载入工作流的概览，请参阅流程图。

有关第 0 天工作流，请参见《《NSX-T Data Center 安装指南》》中的[安装 NSX Cloud 组件](#)。

支持的操作系统

下表列出了 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。

- Red Hat Enterprise Linux (RHEL) 7.2、7.3、7.4、7.5
- CentOS 7.2、7.3、7.4、7.5
- Oracle Enterprise Linux 7.2、7.3、7.4（不支持 Unbreakable Enterprise Kernel 版本）。

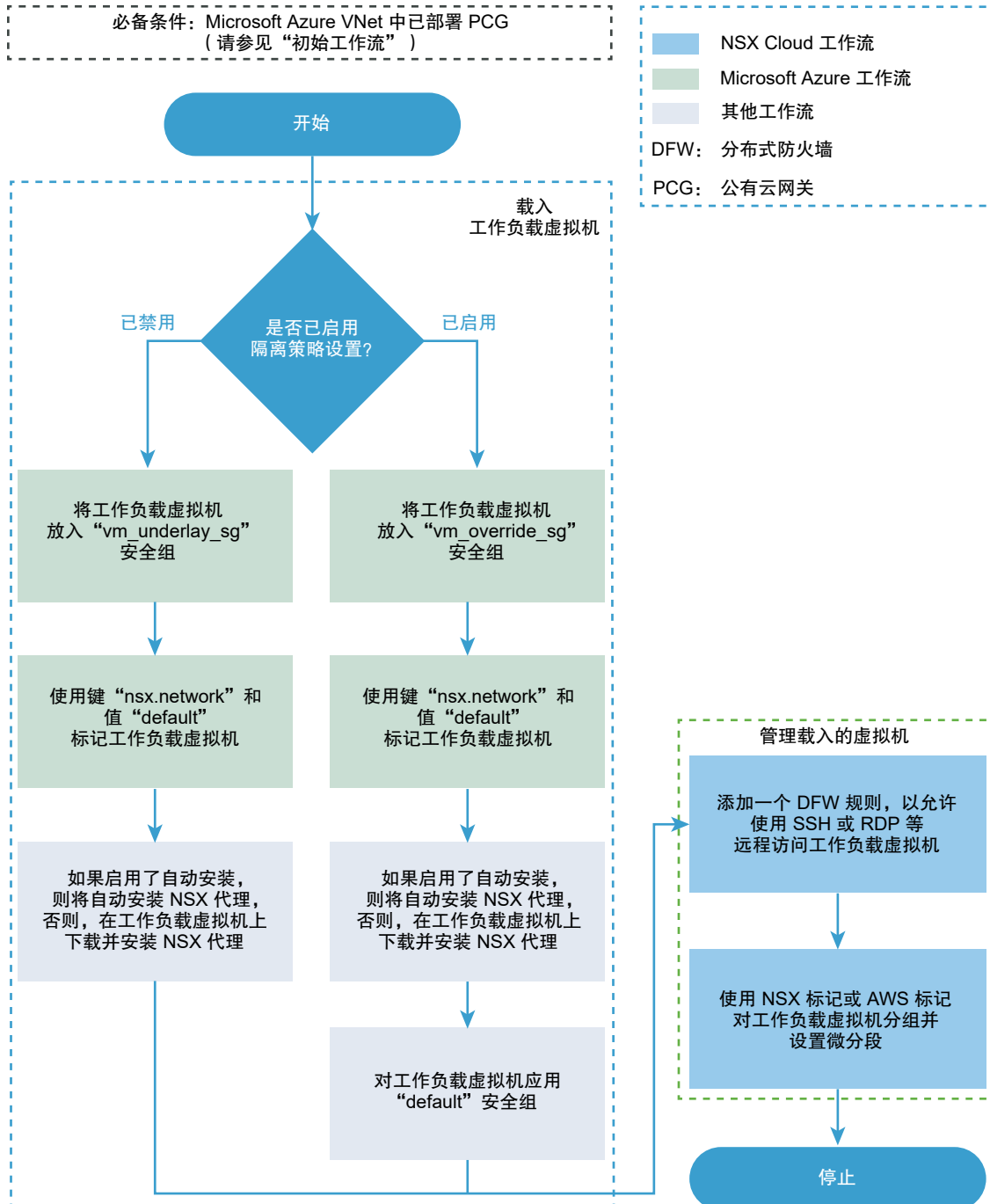
注 对于 Oracle Enterprise Linux、Red Hat Enterprise Linux 和 CentOS，不支持 SE Linux

- Ubuntu 14.04、16.04
- Microsoft Windows Server 2012 R2
- Microsoft Windows Sever 2016

如何从 Microsoft Azure 载入工作负载虚拟机

请参阅以下流程图，大概了解从 Microsoft Azure 载入工作负载虚拟机时涉及的步骤。

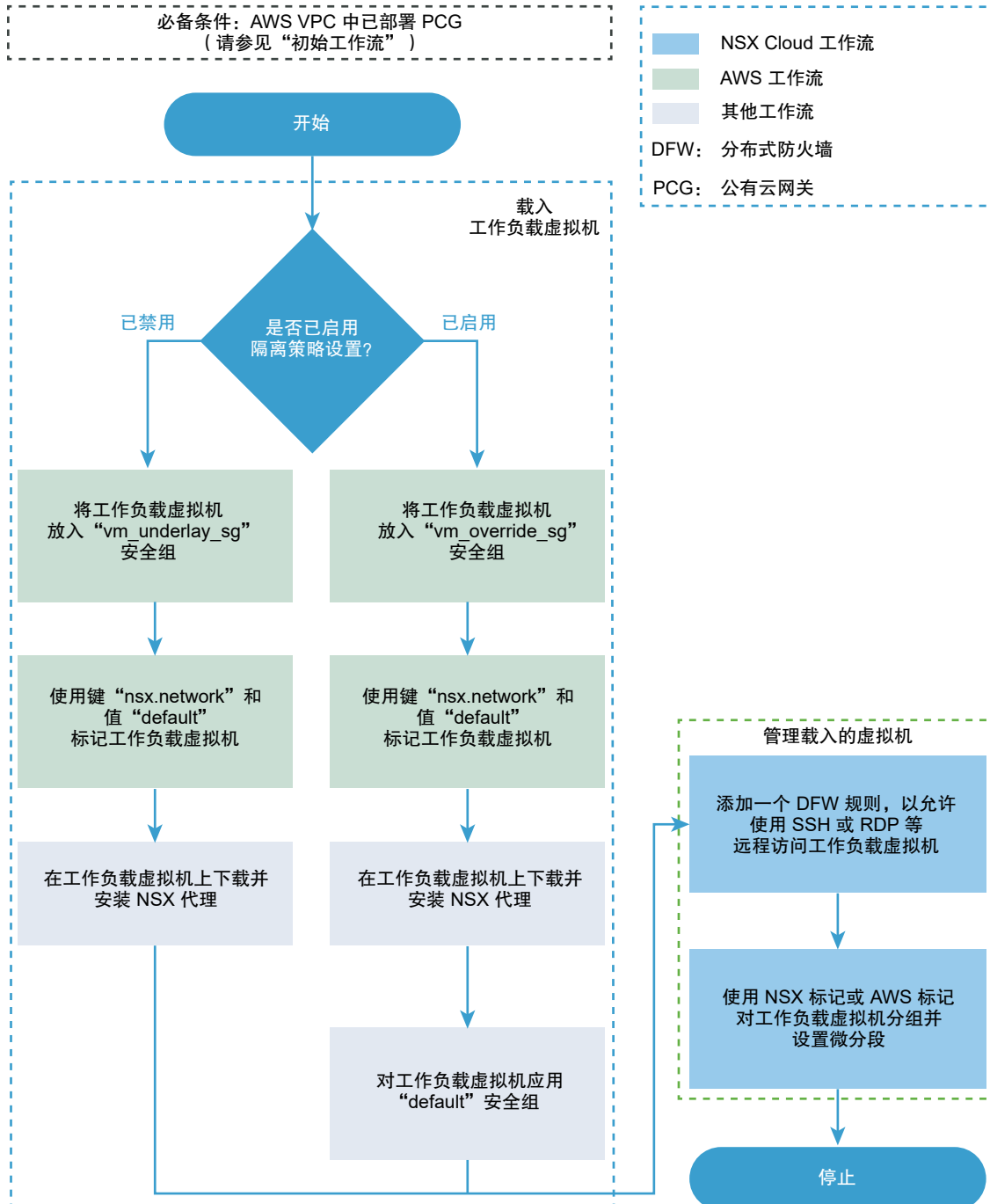
图 16-16. Microsoft Azure 的第 N 天载入工作流



如何从 AWS 载入工作负载虚拟机

请参阅以下流程图，大概了解从 AWS 载入工作负载虚拟机时涉及的步骤。

图 16-17. AWS 的第 N 天载入 workflow



载入工作负载虚拟机

载入工作负载虚拟机，以开始使用 NSX-T Data Center 对其进行管理。

在公有云中标记虚拟机

将 **nsx.network** 标记应用到要使用 NSX-T Data Center 管理的虚拟机。

前提条件

必须在 NSX Cloud 中载入托管工作负载虚拟机的 VPC 或 VNet。有关详细信息，请参见《NSX-T Data Center 安装指南》中的[添加公有云清单](#)。

步骤

- 1 登录到公有云帐户，然后转到已在 NSX Cloud 中载入的 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。

```
Name: nsx.network
Value: default
```

注 您可以在虚拟机级别或在接口级别应用此标记，二者效果相同。

示例

后续步骤

在这些虚拟机上安装 NSX 代理。请参见[安装 NSX 代理](#)。

如果使用 Microsoft Azure，则可以选择在标记的虚拟机上自动安装 NSX 代理。请参见[自动安装 NSX 代理](#)以了解详细信息。

安装 NSX 代理

在工作负载虚拟机上安装 NSX 代理

在 Windows 虚拟机上安装 NSX 代理

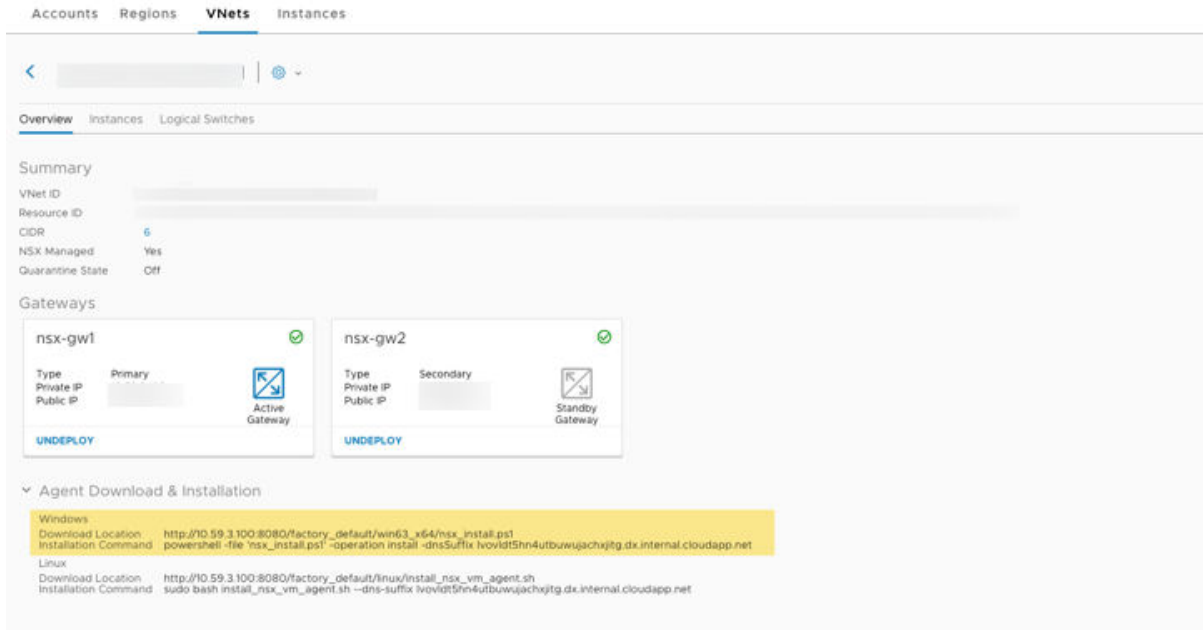
请按照以下说明在 Windows 工作负载虚拟机上安装 NSX 代理。

请参见[支持的操作系统](#)，获取当前支持的 Microsoft Windows 版本列表。

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。单击部署并运行一个或一对 PCG 的 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。

2 从屏幕的代理下载和安装部分中，记录 **Windows** 下的下载位置和安装命令。



注 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。

- 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。
- 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 代理安装是否成功。

注 该脚本会将主网络接口视为默认设置。

有关所有脚本选项列表和卸载说明，请参见[适用于 Windows 虚拟机的 NSX 代理安装脚本选项](#)

后续步骤

[管理工作负载虚拟机](#)

在 Linux 虚拟机上安装 NSX 代理

请按照以下说明在 Linux 工作负载虚拟机上安装 NSX 代理。

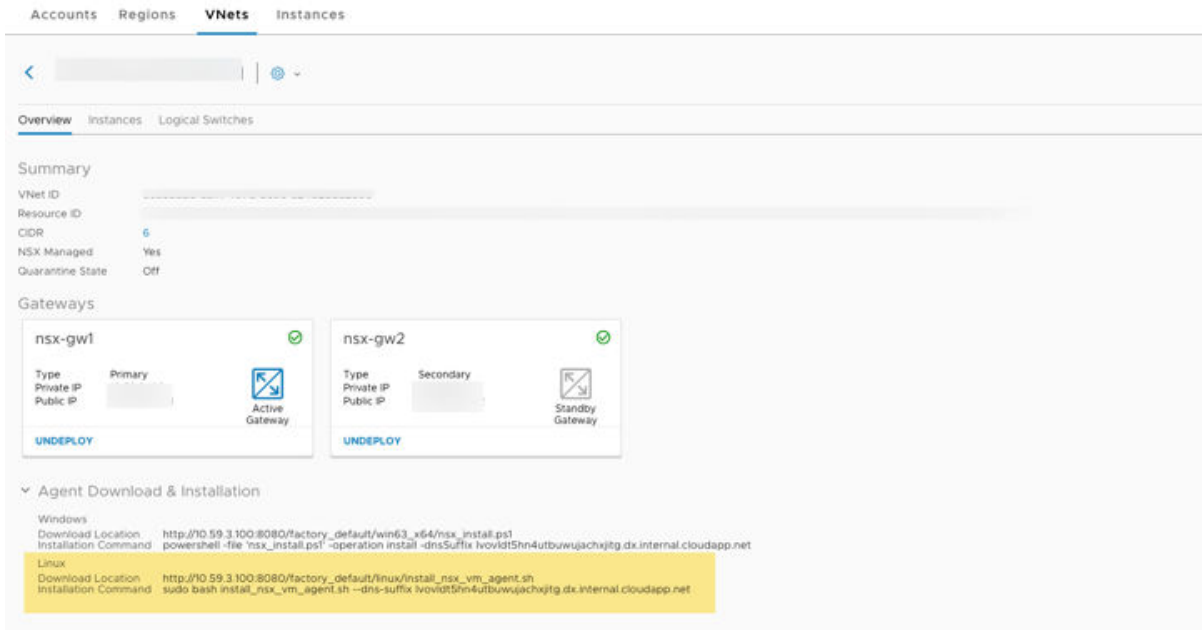
请参见[支持的操作系统](#)获取当前支持的 Linux 发行版列表。

前提条件

您需要使用 **wget** 和 **nslookup** 命令来运行 NSX 代理安装脚本。

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。单击部署并运行一个或一对 PCG 的 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。
- 2 在屏幕的代理下载和安装部分中，记录 Linux 下的下载位置和安装命令。



注 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。

- 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。
- 5 根据需要更改安装脚本的权限，使其成为可执行文件，并运行该脚本：

```
$ sudo chmod +x install_nsx_vm_agent.sh
$ sudo bash install_nsx_vm_agent.sh --dns-suffix <>
```

注意：在 Red Hat Enterprise Linux 及其衍生产品上，不支持 SELinux。请禁止 SELinux 安装 NSX 代理。

- NSX 代理安装开始后，您将断开与 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.**。重新连接到虚拟机，完成载入过程。

结果

NSX 代理安装在工作负载虚拟机上。

注

- NSX 代理成功安装后，端口 8888 在虚拟机上显示为打开，但对于处于底层模式的虚拟机，此端口被阻止，应仅在需要时用于进行高级故障排除。
- 该脚本使用 **eth0** 作为默认接口。有关脚本选项列表和卸载说明，请参见[适用于 Linux 虚拟机的 NSX 代理安装脚本选项](#)

后续步骤

[管理工作负载虚拟机](#)

NSX 代理安装脚本选项和卸载

NSX 代理安装脚本提供可配置的选项。下表列出了这些选项。

适用于 Windows 虚拟机的 NSX 代理安装脚本选项

表 16-5.

选项	说明
<code>--gateway <ip dns></code>	<p>NSX Public Cloud Gateway IP 或 DNS 名称。</p> <p>如果要使用 PCG 的 IP 地址，请指定此选项。如果未指定此参数，则使用 PCG 的默认 DNS 名称。</p> <ul style="list-style-type: none"> AWS 中的 PCG DNS 名称为：<code>nsx-gw.vmware.local</code> Microsoft Azure 中的 PCG DNS 名称为：<code>nsx-gw</code> <p>注 在 PCG 的 HA 模式下，指定带两个 PCG 名称的 “<code>--gateway</code>” 选项，例如，在 Microsoft Azure 虚拟机中：<code>--gateway "nsx-gw1;nsx-gw2"</code></p>
<code>--noStart true</code>	<p>在虚拟机上安装 NSX 代理后，可以创建该虚拟机的 VHD。使用此选项运行安装脚本。然后，从 Microsoft Azure 门户创建此虚拟机的 VHD。</p>
<code>--downloadPath <path></code>	<p>这是文件应当下载到的目录的路径。如果路径中包含转义字符，则使用单引号将其括起来。</p> <p>默认值 = <code>%temp%</code></p>
<code>--silentInstall <true/false></code>	<p>如果此选项设置为 <code>true</code>，脚本将运行静默安装。</p> <p>默认值为 <code>false</code>。</p>

表 16-5. (续)

选项	说明
<code>-noSigCheck <true/false></code>	用于指定是否检查二进制文件中的签名。 默认值 = <code>false</code>
<code>-logLevel <value></code>	用于指定 NSX 组件的日志级别 默认值 = 1 详细 = 3
<code>-operation <install/uninstall></code>	用于指定要执行的操作: <code>install</code> 或 <code>uninstall</code> 默认值 = <code>install</code>
<code>-bundlePath <path></code>	用于指定 NSX 虚拟机代理包的本地路径 默认选项是从 PCG 下载包。

从 Windows 虚拟机中卸载 NSX 代理

- 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
```

适用于 Linux 虚拟机的 NSX 代理安装脚本选项

表 16-6.

选项	说明
<code>--gateway <ip dns></code>	NSX Public Cloud Gateway IP 或 DNS 名称。 如果要使用 PCG 的 IP 地址, 请指定此选项。如果未指定此参数, 则使用 PCG 的默认 DNS 名称。 <ul style="list-style-type: none"> ■ AWS 中的 PCG DNS 名称为: <code>nsx-gw.vmware.local</code> ■ Microsoft Azure 中的 PCG DNS 名称为: <code>nsx-gw</code> <p>注 在 PCG 的 HA 模式下, 指定带两个 PCG 名称的 “<code>--gateway</code>” 选项, 例如, 在 Microsoft Azure 虚拟机中: <code>--gateway "nsx-gw1;nsx-gw2"</code></p>
<code>--no-start</code>	在虚拟机上安装 NSX 代理后, 可以创建该虚拟机的 VHD。使用此选项运行安装脚本。然后, 从 Microsoft Azure 门户创建此虚拟机的 VHD。
<code>--uninstall</code>	使用此选项运行脚本以卸载 NSX 代理。

自动安装 NSX 代理

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 代理:

- 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](#)。
- 已使用 `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 NSX 代理的虚拟机所在的 VNet。
- 3 使用以下任一方法启用此选项：

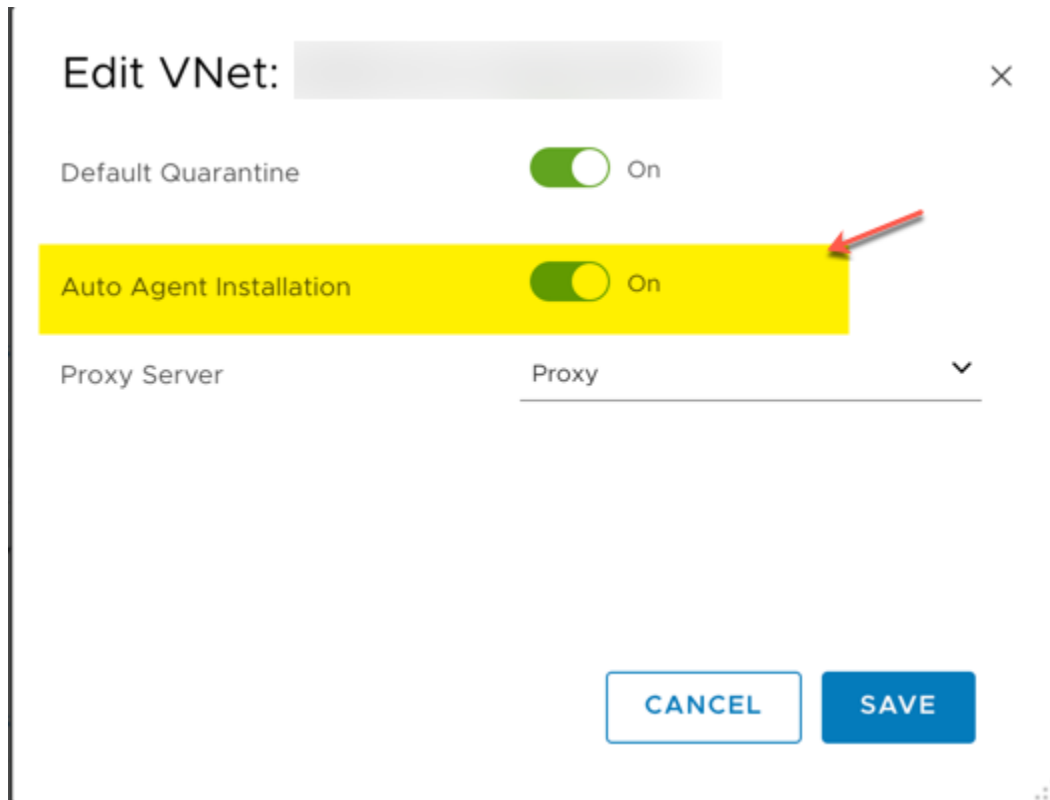
- 在图标视图中，单击操作 > 编辑配置。



- 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 的页面中，请单击“操作”图标以转到编辑配置。



管理工作负载虚拟机

成功载入工作负载虚拟机后，可以使用 NSX-T Data Center 对其进行管理。

访问受管工作负载虚拟机

按照以下工作流访问处于底层模式的受管虚拟机。

在 VPC 或 VNet 上部署 PCG 时，NSX Cloud 将创建默认防火墙规则以增强工作负载虚拟机的安全性。要访问处于底层模式的受管工作负载虚拟机，您需要添加一个可访问虚拟机的分布式防火墙 (DFW) 规则。执行以下操作：

- 1 打开 NSX Manager 控制台。
- 2 转到 **防火墙 > 常规 > 添加规则**
- 3 添加配置如下的规则。有关详细说明，请参见 [添加防火墙规则](#)。

表 16-7.

选项	说明
名称	提供一个名称以定义此规则的用途，例如 AllowRemoteAccessToUnderlay 。
源	选择 任意 。
目标	选择逻辑交换机、端口或此虚拟机所连接的或它所属的 NS 组。
服务	为此工作负载虚拟机选择远程访问服务，例如，选择 SSH（针对 Linux）或 RDP（针对 Windows）。
操作	选择 允许 。

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。

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 标记的等效组件
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
 - aws:vpc
 - aws:availabilityzone
- **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。这些标记带有前缀 **dis:azure:**，表示它们是从 Microsoft Azure 中发现的。

在公有云中对标记进行任何更改时，所做的更改两分钟内即反映在 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 16-8. 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:availabilityzone 	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 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 16-9.

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

表 16-9。（续）

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
Abcdefghijklmnopqrstuvwxyz=value2	否（键超过 20 个字符）	无
tag3=AbcdefghijklmnopqrstuvwxyzAb23690hgijuytreswqacvbcdefghijklmnopqrstuvwxyz	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[为工作负载虚拟机设置微分段](#)。

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载入的工作负载虚拟机：

- 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** 等层创建 NS 组。有关说明，请参阅[创建 NS 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

- 2 根据需要创建防火墙规则区域并应用于 NS 组。请参见[添加防火墙规则区域](#)。
 - 3 创建防火墙规则，并按照安全策略的要求对源和目标使用 NS 组。请参见[添加防火墙规则](#)。
- 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 后的大约两分钟内生效。

如何对公有云使用 NSX-T Data Center 功能

NSX Cloud 会为公有云创建网络拓扑，您不能编辑或删除自动生成的 NSX-T Data Center 逻辑实体。

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，供您快速参考。

NSX Manager 配置

在 NSX Manager 中会自动创建以下实体：

重要事项 请勿编辑或删除所有这些自动创建的实体。

- 创建名为公有云网关 (PCG) 的 Edge 节点。
- PCG 添加到 Edge 群集中。在高可用性部署中，有两个 PCG。
- PCG（或两个 PCG）注册为创建了两个传输区域的传输节点。
- 创建两个默认逻辑交换机。
- 创建一个第 0 层逻辑路由器。
- 创建 IP 发现配置文件。此配置文件用于覆盖网络逻辑交换机。
- 创建 DHCP 配置文件。此配置文件用于 DHCP 服务器。

注 尽管创建了 DHCP 配置文件，但在当前版本中不受支持，因为它用于覆盖网络。

- 创建名为 **PublicCloudSecurityGroup** 的默认 NS 组，其中包含以下成员：
 - 默认 VLAN 逻辑交换机
 - 逻辑端口，每个对应一个 PCG 上行链路端口（如果已启用 HA）。
 - IP 地址
- 创建三个默认的分布式防火墙规则：
 - LogicalSwitchToLogicalSwitch
 - LogicalSwitchToAnywhere
 - AnywhereToLogicalSwitch

注 这些 DFW 规则会阻止所有流量，需要根据具体要求进行调整。

在 NSX Manager 中验证这些配置：

- 1 从 NSX Cloud 仪表板，单击 **NSX Manager**。
- 2 转到**结构层 > 节点 > Edge**。您应看到 **PCG-<your-VPC-or-VNet-name>** 为 Edge 节点。

注 验证部署状态、管理器连接和控制器连接是否为已连接（状态显示**已连接**并带有绿点）。

- 3 浏览到**结构层 > 节点 > Edge 群集**，以验证是否已添加 **PCG-Cluster-<your-VPC-or-VNet-name>**。
- 4 浏览到**结构层 > 节点 > 传输节点**，以验证 PCG 是否注册为传输节点且已连接到部署 PCG 时自动创建的两个传输区域：
 - 流量类型 VLAN -- 用于连接到 PCG 上行链路
 - 流量类型覆盖网络 -- 用于覆盖逻辑网络

注 当前版本不支持覆盖网络。

5 验证是否已创建逻辑交换机和第 0 层逻辑路由器且逻辑路由器是否已添加到 Edge 群集。

- 转到 **网络 > 交换 > 交换机**。您应看到 **DefaultSwitch-Overlay-<your-VPC-or-VNet-name>** 和 **DefaultSwitch-VLAN-<your-VPC-or-VNet-name>** 交换机已自动创建。
- 转到 **网络 > 路由 > 路由器**。您应看到 **PCG-Tier0-LR-<your-VPC-or-VNet-name>** 路由器已自动创建。

逻辑交换常见问题解答

表 16-10.

问题	回答
部署 PCG 时，NSX Cloud 是否创建任何默认交换机？	是。NSX Cloud 会为部署 PCG 的每个 VPC 或 VNet 创建两个默认交换机。交换机名称格式如下所示： DefaultSwitch-Overlay-<vpc-or-vnet-name> DefaultSwitch-VLAN-<vpc-or-vnet-name>
除了 NSX Cloud 创建的默认逻辑交换机之外，能否自行创建 VLAN 逻辑交换机？	否。请勿创建 VLAN 逻辑交换机。
能否编辑或删除 NSX Cloud 创建的默认逻辑交换机？	可以在用户界面中编辑或删除默认逻辑实体，但是，请勿编辑或删除 NSX Cloud 自动创建的任何内容。
是否应创建端口？	否。无需创建任何端口。标记 AWS 或 Microsoft Azure 中的虚拟机时，NSX Cloud 会创建端口。请勿编辑或删除 NSX Cloud 自动创建的任何端口。
是否应创建交换配置文件？	否。无需创建任何交换配置文件。使用 PublicCloud-Global-SpoofGuardProfile 。请勿编辑或删除默认交换配置文件。
从何处可以找到有关逻辑交换机的详细信息？	请参见第 1 章 逻辑交换机和配置虚拟机连接 。

逻辑路由器常见问题解答

表 16-11.

问题	回答
部署 PCG 时，NSX Cloud 是否自动创建逻辑路由器？	是。在 VPC 或 VNet 上部署 PCG 时，NSX Cloud 会自动创建第 0 层逻辑路由器。
从何处可以找到有关逻辑路由器的更多信息？	请参见第 5 章 Tier-0 逻辑路由器 。

IPFIX 常见问题解答

表 16-12.

问题	回答
IPFIX 是否需要任何特定的配置以在公有云上运行？	<p>是：</p> <ul style="list-style-type: none"> ■ 在 NSX Cloud 中，仅 UDP 端口 4739 支持 IPFIX。 ■ 收集器必须与应用 IPFIX 配置文件的虚拟机位于同一个 VPC 或 VNet。 ■ 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。
从何处可以找到有关 IPFIX 的更多信息？	请参见 配置 IPFIX 。

端口镜像常见问题解答

表 16-13.

问题	回答
端口镜像是否需要任何特定的配置以在公有云中运行？	<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。
从何处可以找到有关端口镜像的更多信息？	请参见 监控端口镜像会话 。

其他常见问题解答

表 16-14.

问题	回答
应用到公有云中工作负载虚拟机的标记在 NSX-T Data Center 中是否可用？	是。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。
如何为由 NSX-T Data Center 管理的工作负载虚拟机设置微分段？	请参见 为工作负载虚拟机设置微分段 。

使用 NSX Cloud 高级功能

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>
```

故障排除

了解 NSX Cloud 提供的验证选项和故障排除选项。

验证 NSX Cloud 组件

在生产环境中部署之前，最好验证所有组件是否都已启动并正在运行。

验证 NSX 代理是否已连接到 PCG

要验证工作负载虚拟机上的 NSX 代理是否已经连接到 PCG，请执行以下操作：

- 1 键入 **nsxcli** 命令以打开 NSX-T Data Center CLI。
- 2 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
```

验证虚拟机的接口/网络模式

验证安装了 NSX 代理的接口，如下所示：

- 1 键入 **nsxcli** 命令以打开 NSX-T Data Center CLI。
- 2 键入命令以查看切换模式，例如：

```
get vm-network-mode
VM-Network-Mode : underlay Interface : eth0
```

验证 AWS 或 Microsoft Azure 中的虚拟机接口标记

工作负载虚拟机必须具有正确的标记才能连接到 PCG。

- 1 登录到 AWS 控制台或 Microsoft Azure 门户。

2 验证虚拟机的 eth0 或接口标记。

`nsx.network` 键的值必须为 `default`。

对常见问题进行故障排除

下面列出了一些常见问题。

我已正确标记我的虚拟机并安装了代理，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.managed` 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？

在某些很少见的情况下，与受管 Linux 或 Windows 工作负载虚拟机的连接可能会断开。尝试执行以下步骤：

从公有云（AWS 或 Microsoft Azure）

- 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[管理隔离策略](#)。
- NSX-T Data Center DFW 规则。请参见[访问受管工作负载虚拟机](#)以了解详细信息。
- Linux 上的 Windows 防火墙或 IPTables。
- 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。
- 可以重新引导锁定的虚拟机。
- 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。

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：

- 添加许可证密钥
- 管理用户帐户和基于角色的访问控制
- 设置证书
- 配置设备
- 添加计算管理器
- 管理标记
- 搜索对象
- 查找远程服务器的 **SSH** 指纹
- 备份和还原 **NSX Manager**
- 管理设备和设备群集
- 日志消息
- 配置 **IPFIX**
- 使用跟踪流跟踪数据包路径
- 查看端口连接信息
- 监控逻辑交换机端口活动
- 监控端口镜像会话
- 监控结构层节点
- 查看有关在虚拟机上运行的应用程序的数据
- 收集支持包
- 客户体验提升计划

添加许可证密钥

您可以使用 NSX Manager UI 添加一个或多个许可证密钥。

可以使用以下非评估许可证类型：

- 标准
- 高级
- 企业

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。

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。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **系统 > 配置 > 许可证**。
- 3 单击 **添加** 以输入许可证密钥。
- 4 单击 **保存**。

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。

更改 CLI 用户的密码

每个设备具有两个内置用户（admin 和 audit），您可以使用这些用户登录并运行 CLI 命令。您可以更改这些用户的密码，但无法添加或删除用户。

步骤

- 1 登录到设备的 CLI。

2 运行 `set user` 命令。例如，

```
nsx> set user admin
Current password:
New password:
Confirm new password:
nsx>
```

密码必须满足以下密码复杂性要求：

- 长度至少为 8 个字符
- 至少一个大写字符
- 至少一个小写字符
- 至少一个数字字符
- 至少一个特殊字符

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、NSX Controller 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。

步骤

- 1 通过 SSH 访问 vIDM 主机并以 **sshuser** 身份登录。
- 2 运行以下命令以成为 **root** 用户。

```
su root
```

- 3 编辑 `/etc/ssh/sshd_config` 文件，以将 `PermitRootLogin` 值更改为 `yes` 并将 `StrictModes` 值更改为 `no`。

```
PermitRootLogin yes
StrictModes no
```

- 4 运行以下命令以重新启动 `sshd` 服务。

```
service sshd restart
```

- 5 注销并以 **root** 身份登录。
- 6 运行以下命令以更改目录。

```
cd /usr/local/horizon/conf
```

- 7 运行以下命令以获取指纹。

```
openssl s_client -connect <FQDN of vIDM host>:443 < /dev/null 2>/dev/null | openssl x509 -
sha256 -fingerprint -noout -in /dev/stdin
```

例如：

```
openssl s_client -connect vidm.corp.local:443 < /dev/null 2>/dev/null | openssl x509 -sha256 -
fingerprint -noout -in /dev/stdin
```

将 vIDM 主机与 NSX-T 相关联

要允许将 NSX-T 与 vIDM 集成在一起，您必须提供有关 vIDM 主机的信息。

vIDM 服务器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 <https://docs.vmware.com/cn/VMware-Identity-Manager/3.1/vidm-install/GUID-B76761BF-4B12-4CD5-9366-B0A1A2BF2A8B.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。

前提条件

- 确认您具有从 vIDM 主机中获取的证书指纹。请参见[从 vIDM 主机中获取证书指纹](#)。
- 确认在 vIDM 主机中将 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，请参阅 VMware Identity Manager 文档，网址为 [《》](#)。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **系统 > 用户**。
- 3 单击 **配置** 选项卡。
- 4 单击 **编辑**。
- 5 提供以下信息。

参数	说明
VMware Identity Manager 设备	vIDM 主机的完全限定域名 (Fully Qualified Domain Name, FQDN)。
客户端 ID	在 vIDM 主机中注册 NSX Manager 时创建的 ID。
客户端密码	在 vIDM 主机中注册 NSX Manager 时创建的密码。
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。

- 6 单击 **保存**。

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>

有关同步虚拟机和主机的信息，请参阅 https://docs.vmware.com/cn/VMware-vSphere/6.0/com.vmware.vsphere.vm_admin.doc/GUID-C0D8326A-B6E7-4E61-8470-6C173FDDF656.html。虚拟机可能运行 NSX Manager、vIDM、Active Directory 或其他服务提供程序。

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 server time.nist.gov
server server pool.ntp.org
server server time.is dynamic
```

- 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
- 云服务管理员
- 云服务审核员
- 负载均衡器管理员
- 负载均衡器审核员

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 17-1. 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
- CS Adm - 云服务管理员

- CS Aud - 云服务审核员
- LB Adm - 负载均衡器管理员
- LB Aud - 负载均衡器审核员
- FA - 完全访问
- E - 执行
- R - 读取

表 17-1. 角色和权限

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
工具 > 端口连接	E	R	E	E	E	E	E	R	E	E
工具 > 跟踪流	E	R	E	E	E	E	E	R	E	E
工具 > 端口镜像	FA	R	FA	FA	FA	FA	FA	R	无	无
工具 > IPFIX	FA	R	FA	R	FA	R	FA	R	无	无
防火墙 > 常规	FA	R	R	R	FA	R	FA	R	无	无
防火墙 > 配置	FA	R	R	R	FA	R	FA	R	无	无
加密	FA	R	FA	R	FA	FA	无	无	无	无
路由 > 路由器	FA	R	FA	R	R	R	FA	R	R	R
路由 > NAT	FA	R	FA	R	FA	R	FA	R	R	R
DHCP > 服务器配置文件	FA	R	FA	R	FA	无	FA	R	无	无
DHCP > 服务器	FA	R	FA	R	FA	无	FA	R	无	无
DHCP > 中继配置文件	FA	R	FA	R	FA	无	FA	R	无	无
DHCP > 中继服务	FA	R	FA	R	FA	无	FA	R	无	无
DHCP > 元数据代理	FA	R	FA	R	FA	无	无	无	无	无
IPAM	FA	R	FA	R	FA	无	无	无	无	无
交换 > 交换机	FA	R	FA	FA	R	R	FA	R	R	R
交换 > 端口	FA	R	FA	FA	R	R	FA	R	R	R
交换 > 交换配置文件	FA	R	FA	FA	FA	FA	FA	R	R	R
负载均衡 > 负载均衡器	FA	R	无	无	无	无	FA	R	FA	R
负载均衡 > 虚拟服务器	FA	R	无	无	无	无	FA	R	FA	R

表 17-1. 角色和权限（续）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
负载均衡 > 配置文件 > 应用程序配置文件	FA	R	无	无	无	无	FA	R	FA	R
负载均衡 > 配置文件 > 持久性配置文件	FA	R	无	无	无	无	FA	R	FA	R
负载均衡 > 配置文件 > SSL 配置文件	FA	R	无	无	FA	R	FA	R	FA	R
负载均衡 > 服务器池	FA	R	无	无	无	无	FA	R	FA	R
负载均衡 > 监控器	FA	R	无	无	无	无	FA	R	FA	R
清单 > 组	FA	R	FA	R	FA	R	FA	R	R	R
清单 > IP 集	FA	R	FA	R	FA	R	FA	R	R	R
清单 > IP 池	FA	R	FA	R	无	R	无	无	R	R
清单 > MAC 集	FA	R	FA	R	FA	R	FA	R	R	R
清单 > 服务	FA	R	FA	R	FA	R	FA	R	R	R
清单 > 虚拟机	R	R	R	R	R	R	R	R	R	R
清单 > 虚拟机 > 创建和分配标记	FA	R	FA	FA	FA	FA	FA	R	R	R
清单 > 虚拟机 > 配置标记	FA	无	无	无	FA	无	无	无	无	无
结构层 > 节点 > 主机	FA	R	R	R	R	R	R	R	无	无
架构 > 节点 > 节点	FA	R	FA	R	FA	R	R	R	无	无
结构层 > 节点 > Edge	FA	R	FA	R	R	R	R	R	无	无
结构层 > 节点 > Edge 群集	FA	R	FA	R	R	R	R	R	无	无
结构层 > 节点 > 网桥	FA	R	FA	R	R	R	无	无	R	R
结构层 > 节点 > 传输节点	FA	R	R	R	R	R	R	R	R	R
架构 > 节点 > 隧道	R	R	R	R	R	R	R	R	R	R

表 17-1. 角色和权限（续）

操作	EA	A	NE	NO	SE	SO	CS Adm	CS Aud	LB Adm	LB Aud
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
结构层 > 配置文件 > Edge 群集配置文件	FA	R	FA	R	R	R	R	R	R	R
结构层 > 配置文件 > 配置	FA	R	无	无	无	无	R	R	无	无
架构 > 传输区域 > 传输区域	FA	R	R	R	R	R	R	R	R	R
架构 > 传输区域 > 传输区域配置文件	FA	R	R	R	R	R	R	R	R	R
结构层 > 计算管理器	FA	R	R	R	R	R	R	R	无	无
系统 > 信任	FA	R	无	无	FA	R	无	无	FA	R
系统 > 配置	E	R	R	R	R	R	无	无	无	无
系统 > 实用程序 > 支持包	FA	R	R	R	R	R	R	R	无	无
系统 > 实用程序 > 备份	FA	R	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
系统 > 实用程序 > 升级	FA	R	R	R	R	R	无	无	无	无
系统 > 用户 > 角色分配	FA	R	无	无	无	无	无	无	无	无
系统 > 用户 > 配置	FA	R	无	无	无	无	无	无	无	无

管理角色分配

如果 VMware Identity Manager 与 NSX-T Data Center 集成在一起，您可以添加、更改和删除为用户或用户组分配的角色。

前提条件

- 确认 vIDM 主机与 NSX-T 相关联。有关详细信息，请参阅[将 vIDM 主机与 NSX-T 相关联](#)。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **系统 > 用户**。

- 3 如果尚未选择**角色分配**选项卡，请单击该选项卡。
- 4 添加、更改或删除角色分配。

选项	操作
添加角色分配	单击 添加 ，选择用户或用户组，然后选择角色。
更改角色分配	选择一个用户或用户组，然后单击 编辑 。
删除角色分配	选择一个用户或用户组，然后单击 删除 。

查看主体身份

主体可以是 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
- 证书
- RBAC 角色，指明该主体的访问权限
- 标记，指明该主体创建的对象是否受保护

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。企业管理员用户只能使用 NSX-T Data Center API 删除受保护对象，而不能使用 NSX Manager UI。

只能使用 NSX-T API 创建或删除主体身份。有关详细信息，请参见《NSX-T Data Center API 参考》。但是，您可以通过 NSX Manager UI 查看主体身份。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**系统 > 用户**。
- 3 单击**角色分配**选项卡。

将显示用户、用户组和主体身份。

设置证书

您可以在 NSX Manager 中生成一个证书签名请求 (Certificate Signing Request, CSR)，并将其发送到证书颁发机构 (Certificate Authority, CA) 以获取服务器证书。

还可以使用 CSR 生成自签名证书。如果当前具有证书或 CA 证书，您可以导入以使用该证书。也可以导入包含吊销的证书的证书吊销列表 (Certificate Revocation List, CRL)。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **系统 > 信任**。
- 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**保存**。

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 证书以成为公司的临时 CA。在导入证书后，您有权对自己的证书进行签名。

前提条件

确认具有一个 CA 证书。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**系统 > 信任**。
- 3 单击**证书**选项卡。
- 4 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。

5 单击**保存**。**结果**

您现在可以对自己的证书进行签名。

导入证书

您可以导入具有私钥的证书以创建自签名证书。

前提条件

确认具有一个证书。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **系统 > 信任**。
- 3 单击 **证书** 选项卡。
- 4 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 CA 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。
私钥	浏览到计算机上的私钥文件并添加该文件。
密码	为该证书添加密码。
说明	输入该证书中包含的内容的摘要。

- 5 单击 **保存**。

结果

您现在可以创建自己的自签名证书。

创建自签名证书

使用自签名证书可能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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **系统 > 信任**。
- 3 单击 **CSR** 选项卡。
- 4 选择现有的 CSR。
- 5 单击 **操作**，然后从下拉菜单中选择 **CSR 的自签名证书**。
- 6 输入自签名证书的有效天数。
默认时间范围是 10 年。
- 7 单击 **保存**。

结果

将在证书列表中显示自签名证书，并将证书类型指定为自签名。

替换证书

如果您需要替换证书（例如，如果证书将要过期），您可以发出 API 调用以替换现有的证书。

前提条件

确认在 NSX Manager 中具有一个证书。请参见[创建自签名证书](#)和[导入证书](#)。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 `https://nsx-manager-ip-address` 的 NSX Manager。
- 2 从导航面板中选择 **系统 > 信任**。
- 3 单击 **证书** 选项卡。
- 4 单击要使用的证书的 ID，然后从弹出窗口中复制该证书 ID。
- 5 使用 `POST /api/v1/node/services/http?action=apply_certificate` API 调用替换现有的证书。例如，

```
POST https://<nsx-mgr>/api/v1/node/services/http?
action=apply_certificate&certificate_id=e61c7537-3090-4149-b2b6-19915c20504f
```

有关详细信息，请参阅《NSX-T API 参考》。

结果

该 API 调用将重新启动 HTTP 服务，以便该服务开始使用新证书。在 POST 请求成功完成时，响应代码为 200 Accepted。

导入证书吊销列表

证书吊销列表 (Certificate Revocation List, 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **系统 > 信任**。
- 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	复制 CRL 中的所有项目并将其粘贴到该部分中。 示例 CRL。 <pre>-----BEGIN X509 CRL----- MIIBODCB4zANBgkqhkiG9w0BAQQFADBGMQswCQYDVQQGEwJBVTEMMAoGA1UECBM D UUxEMRkwFwYDVQQKEwBNaw5jb20gUHR5LiBMdGQuMQswCQYDVQQLEwJDUzEhMBk G A1UEAxMSU1NMZW51IGRlbW8gc2VydmlvFw0wMTAxMTUxNjI2NTdaFw0wMTAyMTQ x NjI2NTdaMFwiEgIBARcNOTUxMDA5MjMzMjA1WjASAgEDFw05NTEyMDEwMTAwMDB a MBMCAhI0Fw0wMTAxMTUxNjE5NDdaMBMCAhI1Fw0wMTAxMTUxNjIzNDZaMA0GCSq G SIb3DQEBAUA0EAHPjQ3M93Q0j8Ufi+jZM7Y78TfAzG4jJn/ E6MYBPFVQFY0/Gp UZexfjSV05CIyyS0tYscz8o07avwBxTiMpDEQg== -----END X509 CRL--</pre>
说明	输入该 CRL 中包含的内容的摘要。

- 5 单击 **保存**。

结果

导入的 CRL 将显示为一个链接。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **系统 > 信任**。

- 3 单击 **CSR** 选项卡。
- 4 选择现有的 CSR。
- 5 单击**操作**，然后从下拉菜单中选择为 **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**保存**。

结果

将在**证书**列表中显示自签名证书，并将证书类型指定为自签名。

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 17-2. 系统配置命令和 API 请求。

任务	命令行 (NSX Manager、NSX Controller、NSX Edge)	API 请求 (仅限 NSX Manager)
设置系统时区	set timezone <timezone>	PUT https://<nsx-mgr>/api/v1/node
设置 NTP 服务器	set ntp-server <ntp-server>	PUT https://<nsx-mgr>/api/v1/node/services/ntp
设置 DNS 服务器	set name-servers <dns-server>	PUT https://<nsx-mgr>/api/v1/node/network/name-servers
设置 DNS 搜索域	set search-domains <domain>	PUT https://<nsx-mgr>/api/v1/node/network/search-domains

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 轮询计算管理器以了解更改（如添加或移除主机或虚拟机），并相应地更新其清单。添加计算管理器是可选操作，因为 NSX-T 即使没有计算管理器也会获取清单信息，例如独立主机和虚拟机。

在该版本中，该功能支持：

- vCenter Server 版本 6.5 Update 1、6.5 Update 2 和 6.7。
- 与 vCenter Server 的 IPv6 以及 IPv4 通信。
- 最多 5 个计算管理器。

步骤

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

- 2 从导航面板中选择**结构层 > 计算管理器**。
- 3 单击**添加**。
- 4 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。

- 5 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

“计算管理器”面板将显示一个计算管理器列表。您可以单击管理器的名称以查看或编辑有关管理器的详细信息，或者管理适用于管理器的标记。

管理标记

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[如何对公有云使用 NSX-T Data Center 功能](#)，获得自动生成的逻辑实体、支持的功能和 NSX Cloud 所需配置的列表。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://insx-manager-ip-address> 的 NSX Manager。
- 2 导航到一个对象类别。
例如，导航到**交换 > 交换机**。
- 3 单击交换机的名称。
- 4 选择菜单选项**操作 > 管理标记**，或者单击标记旁边的**管理**。

5 添加或删除标记。

选项	操作
添加标记	单击 添加 以指定标记和可选的范围。
删除标记	选择一个现有的标记，然后单击 删除 。

对象最多可以具有 30 个标记。标记的最大长度为 256 个字符。范围的最大长度为 128 个字符。

6 单击**保存**。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 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。

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 17-3. 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
```

备份和还原 NSX Manager

如果 NSX Manager 变得无法运行，可以从备份进行还原。NSX Manager 无法运行时，数据层面不受影响，但无法进行配置更改。

共有三种类型的备份：

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。
清单备份	该备份包含一组 ESX 和 KVM 主机以及 Edge。在还原操作期间，将使用该信息检测并修复管理层面的所需状态与这些主机之间的差异。

共有两种备份方法：

手动 NSX Manager 节点备份和群集备份	可以根据需要随时运行手动节点和群集备份。
自动 NSX Manager 节点备份、群集备份和清单备份	自动备份是根据您制订的计划运行的。强烈建议使用自动备份。请参见 计划自动备份 。

要确保具有最新的备份，您应该配置自动备份。请务必定期运行群集和清单备份。

您可以将 NSX-T Data Center 配置还原回在任何群集备份中捕获的状态。在还原备份时，您必须还原到一个新 NSX Manager 设备，该设备运行与备份的设备相同的 NSX Manager 版本。

备份 NSX Manager 配置

NSX Manager 配置备份包含 NSX Manager 节点备份、群集备份和清单备份。

步骤

1 配置备份位置

备份将保存到 NSX Manager 可访问的文件服务器中。您必须先配置该服务器的位置，然后才能创建备份。

2 计划自动备份

计划日常备份，以便还原无法运行的 NSX Manager 及其配置数据。默认情况下，将禁用自动备份。您可以计划在每周的特定日期或按指定的间隔执行自动备份。强烈建议使用计划的备份。

配置备份位置

备份将保存到 NSX Manager 可访问的文件服务器中。您必须先配置该服务器的位置，然后才能创建备份。

注 按照设计，NSX Manager 不会删除备份文件服务器上的备份文件。您必须管理备份轮换并确保服务器具有足够的磁盘空间用于备份。可以考虑通过运行脚本自动删除旧备份。

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 密钥作为指纹。请参见[查找远程服务器的 SSH 指纹](#)。

步骤

- 1 在浏览器中，以管理员身份登录到 NSX Manager，网址为 `https://<nsx-manager-ip-address>`。
- 2 单击**系统 > 实用程序 > 备份**。
- 3 要提供备份位置的访问凭据，请单击页面右上角的**编辑**。
- 4 单击**自动备份**开关以启用自动备份。
- 5 输入备份文件服务器的 IP 地址或主机名。
- 6 根据需要编辑默认端口。
- 7 输入登录到备份文件服务器所需的用户名和密码。
- 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。如果有多个 NSX-T Data Center 部署，请为每个部署使用不同的目录。
- 9 输入用于加密备份数据的密码短语。
您需要使用该密码短语还原备份。如果忘记了备份密码短语，则无法还原任何备份。
- 10 输入存储备份的服务器的 SSH 指纹。请参见[查找远程服务器的 SSH 指纹](#)。
- 11 单击**保存**。
- 12 单击页面底部的**立即备份**，以确认可以将文件写入到备份文件服务器中。

后续步骤

计划自动备份。

计划自动备份

计划日常备份，以便还原无法运行的 NSX Manager 及其配置数据。默认情况下，将禁用自动备份。您可以计划在每周的特定日期或按指定的间隔执行自动备份。强烈建议使用计划的备份。

前提条件

- 确定相应的备份位置。选择一个可以防止单点故障的位置。例如，不要将备份放在与设备相同的文件存储中。该文件存储上的故障可能会影响设备及其备份。
- 找到存储备份的服务器的 SSH 指纹。请参见[查找远程服务器的 SSH 指纹](#)。备份和还原 API 请求要求 SSH 指纹不包含冒号。

步骤

- 1 在浏览器中，以管理员身份登录到 NSX Manager，网址为 `https://<nsx-manager-ip-address>`。
- 2 单击**系统 > 实用程序 > 备份**。

- 3 单击页面右上角的**编辑**。
- 4 单击**文件服务器**，然后验证是否启用了自动备份。
- 5 单击页面顶部的**计划**。
- 6 对于节点/群集备份，请单击**每周**并设置备份到 SFTP 服务器的日期和时间，或者单击**间隔**并设置备份时间。
- 7 默认情况下，清单备份设置为每隔 5 分钟执行一次，并且应经常执行该备份。根据需要，接受或更改默认设置。
- 8 单击**保存**。

结果

注 第一个计划的每周备份在指定的工作日和时间执行。第一个计划的间隔备份在保存启用的自动备份的备份配置后立即执行。

NSX Manager 存储三个单独的备份文件：节点级别、群集级别和清单。备份文件保存到 SFTP 服务器上由备份配置指定的目录中。在该目录中，这些文件保存在以下目录中：

- /<user specified directory>/cluster-node-backups（群集和节点备份）
- /<user specified directory>/inventory-summary（清单备份）

还原 NSX Manager 配置

如果 NSX Manager 无法运行，可以从备份进行还原。您需要创建备份时指定的密码短语。

注 不支持在创建备份的相同 NSX Manager 设备上还原备份。

步骤

1 准备还原 NSX Manager 备份

在还原 NSX Manager 备份之前，您必须安装新的 NSX Manager 设备。必须使用与以前的 NSX Manager 相同的管理 IP 地址部署新的 NSX Manager。

2 还原备份

还原备份将导致还原创建备份时的网络状态，还原由 NSX Manager 维护的配置以及协调在创建备份后对结构层进行的任何更改，例如，添加或删除节点。

3 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。如果您不想将此 vCenter Server 注册到任何 NSX-T Data Center 安装，则可以通过 vCenter Server 的受管对象浏览器 (MOB) 移除该扩展。

准备还原 NSX Manager 备份

在还原 NSX Manager 备份之前，您必须安装新的 NSX Manager 设备。必须使用与以前的 NSX Manager 相同的管理 IP 地址部署新的 NSX Manager。

注 不支持在创建备份的相同 NSX Manager 设备上还原备份。

前提条件

- 确认您了解用于创建备份的 NSX Manager 版本，并具有相同版本的相应安装文件（OVA、OVF 或 QCOW2）。
- 确认您了解为用于创建节点备份的 NSX Manager 分配的 IP 地址。
- 确认没有人尝试对 NSX Manager 配置进行更改，直到还原过程完成。

步骤

- 1 如果旧 NSX Manager 设备仍在运行（例如，如果进行还原以回滚升级尝试），请将其关闭。
- 2 安装新的 NSX Manager 设备。
 - 新 NSX Manager 设备的版本必须与用于创建备份的设备版本相同。
 - 必须为此设备配置与管理器备份对应的 IP 地址。有关这些步骤的信息和说明，请参阅《《NSX-T Data Center 安装指南》》。

后续步骤

还原备份。

还原备份

还原备份将导致还原创建备份时的网络状态，还原由 NSX Manager 维护的配置以及协调在创建备份后对结构层进行的任何更改，例如，添加或删除节点。

注 不支持在创建备份的相同 NSX Manager 设备上还原备份。

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 密钥作为指纹。请参见[查找远程服务器的 SSH 指纹](#)。
- 确认您具有节点和群集备份文件的密码短语。
- 确认您具有未配置任何对象的 NSX Manager 新安装。请参见[准备还原 NSX Manager 备份](#)。

步骤

- 1 从浏览器登录到全新安装的 NSX Manager。
- 2 从导航面板中选择 **系统 > 实用程序**。
- 3 单击 **还原** 选项卡。
- 4 单击 **编辑** 以配置备份文件服务器。

- 5 输入 IP 地址或主机名。
- 6 根据需要更改端口号。
默认值为 22。
- 7 输入用户名和密码以登录到服务器。
- 8 在**目标目录**字段中，输入存储备份的目录的绝对路径。
- 9 输入用于加密备份数据的密码短语。
- 10 输入存储备份的服务器的 SSH 指纹。
- 11 单击**保存**。
- 12 选择一个备份。
- 13 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结构层节点或传输节点，将提示您执行某些操作，例如，登录到节点并运行脚本。

在还原操作完成后，将显示“还原完成”屏幕，将在其中显示还原结果、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，该屏幕将显示发生失败的步骤，例如，**Current Step: Restoring Cluster (DB)** 或 **Current Step: Restoring Node**。如果群集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，还原将继续进行。

也可以运行以下 CLI 命令以查看系统日志文件，然后搜索 **Cluster restore failed** 和 **Node restore failed** 字符串以确定群集还原或节点还原是否失败。

```
get log-file syslog
```

要重新启动管理器，请运行以下 CLI 命令：

```
restart service manager
```

要重新引导管理器，请运行以下 CLI 命令：

```
reboot
```

结果

注 如果您在备份之后添加了一个计算管理器，完成还原后，如果您尝试再次添加该计算管理器，则会显示一条错误消息，指示注册失败。您可以解决该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 5。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。

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。如果您不想将此 vCenter Server 注册到任何 NSX-T Data Center 安装，则可以通过 vCenter Server 的受管对象浏览器 (MOB) 移除该扩展。

步骤

- 1 以管理员身份登录到 vSphere Web Client。
- 2 选择 ESXi 主机。
- 3 单击 **管理 > 设置** 选项卡。
- 4 从菜单中选择 **高级系统设置**。
- 5 启用 **Config.HostAgent.plugins.solo.enableMob** 选项。
- 6 登录到 MOB。
- 7 单击 **content** 链接，即，“属性”表中 **content** 属性的值。
- 8 单击 **ExtensionManager** 链接，即，“属性”表中 **extensionManager** 属性的值。
- 9 单击“方法”表中的 **UnregisterExtension** 链接。
- 10 在值文本字段中输入 **com.vmware.nsx.management.nsx**。
- 11 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。
- 12 要确保移除该扩展，请单击上一页面中的 **FindExtension** 方法，然后通过为该扩展输入相同的值进行调用。
结果应为 **void**。

还原 NSX Controller 群集

如果无法恢复 NSX Controller 群集，或者由于更改了群集成员资格而需要替换一个或多个控制器，则应该还原整个控制器群集。

在还原控制器群集之前，请先确定是否将控制群集成员资格从管理层面已知的成员资格更改为控制器本身已知的实际成员资格或相反。如果在备份后进行了更改，则成员资格可能会有所不同。

- 如果无法恢复整个群集，请参阅[重新部署 NSX Controller 群集](#)。
- 按照下面的步骤确定是否更改了群集成员资格；如果是，请通过备份进行还原。

前提条件

- 确认您具有最新的备份。
- 执行还原。请参见[还原备份](#)。

步骤

- 1 登录到 NSX Manager 的 CLI，然后运行 **get management-cluster status** 命令。
- 2 登录到 NSX Controller 的 CLI，然后运行 **get managers** 命令以确保在管理器中注册该控制器。
- 3 运行 **get control-cluster status** 命令。

- 4 要确定是否更改了成员资格，请将 `get management-cluster status` 命令输出中的 IP 地址与 `get control-cluster status` 命令输出进行比较。

如果 IP 地址集相同，则不需要执行任何操作。如果任何 IP 地址不相同，请继续执行其余步骤以还原整个控制器群集。

- 5 登录到 NSX Controller 的 CLI，然后运行 `get control-cluster status` 命令以确定哪个控制器是主控制器。

主控制器输出将显示 `is master: true`。

- 6 在某个非主控制器上运行 `stop service <controller>` 命令。
- 7 登录到主控制器，然后运行 `detach control-cluster <ip-address[:port]>` 命令以断开连接上一步中的非主控制器。
- 8 （可选）只有在 `get management-cluster status` 命令在 NSX Manager 上显示该控制器时，才应在 NSX Manager 上运行 `detach controller <uuid>` 命令以断开连接该控制器。
- 9 登录到 NSX Controller 的 CLI，然后运行 `deactivate control-cluster` 命令。
- 10 使用以下命令移除引导文件和 uuid 文件：`rm -r /opt/vmware/etc/bootstrap-config` 和 `rm -r /config/vmware/node-uuid`
- 11 对于其余非主控制器，执行步骤 6-10。
- 12 登录到主控制器的 CLI，然后运行 `stop service <controller>` 命令。
- 13 在 NSX Manager 上运行 `detach controller <uuid>` 命令以断开连接该控制器。
- 14 登录到主控制器的 CLI，然后运行 `deactivate control-cluster` 命令。
- 15 使用以下命令移除引导文件和 uuid 文件：`rm -r /opt/vmware/etc/bootstrap-config` 和 `rm -r /config/vmware/node-uuid`
- 16 从 NSX Manager 中运行 `get management-cluster status` 命令。如果在输出中仍显示控制器，请运行 `detach controller <uuid>` 命令以断开连接任何剩余的控制器。

后续步骤

按列出的顺序完成以下任务。

- 1 完成还原。
- 2 将 NSX Controller 加入管理层面，如《NSX-T 安装指南》中所述。
- 3 重新部署 NSX Controller 群集，如《NSX-T 安装指南》中所述。

管理设备和设备群集

每个 NSX-T Data Center 安装仅需要使用和支持一个 NSX Manager 实例。NSX Controller 群集应具有三个成员。NSX Edge 群集应具有至少两个成员。

如果 NSX Controller 或 NSX Edge 群集中的设备无法运行，或者由于任何原因需要将其移除，可以将其替换为新设备。

重要事项 如果对 NSX Controller 或 NSX Edge 群集成员资格进行任何更改，您必须随后创建群集备份以备份新配置。请参见[备份和还原 NSX Manager](#)。

管理 NSX Manager

如果 NSX Manager 变得无法运行，可以检查其状态并重新引导。

获取 NSX Manager 状态

可以通过 NSX Manager UI 查看 NSX Manager 的状态，也可以使用 CLI 命令获取状态。

步骤

- 1 在浏览器中，登录到 NSX Manager，网址为 `http://<nsx-manager-ip-address>`。
- 2 在导航面板上选择 **系统 > 组件**。
将显示 NSX Manager 的状态。
- 3 或者，登录到 NSX Manager 的 CLI。
- 4 运行 `get management-cluster status` 命令。例如，

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 10.172.121.217 (UUID 42191561-79dc-710a-74f1-d15f10cd2c40) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 10.172.121.91 (UUID ab35851f-e616-4760-8d7a-c4386c537382)
- 10.172.122.187 (UUID d159b758-c320-411f-aa67-1e2fd35f5ef2)
- 10.172.122.138 (UUID 12a3b19d-26a0-492e-836e-e9a3cc25e799)

Control cluster status: DEGRADED
```

注 即使结果显示管理群集，也只能有一个 NSX Manager 实例。

重新引导 NSX Manager

您可以使用 CLI 命令重新引导 NSX Manager 以从严重错误中恢复。

步骤

- 1 登录到 NSX Manager 的 CLI。

2 运行 reboot 命令。例如，

```
nsx-manager> reboot
Are you sure you want to reboot (yes/no): y
```

管理 NSX Controller 群集

要使生产部署避免 NSX 控制层面出现任何停机，NSX Controller 群集必须具有三个成员。每个控制器均应放在一个唯一的管理程序主机上（共有三个物理管理程序主机），以避免单个物理管理程序主机故障影响 NSX 控制层面。对于不存在任何生产工作负载的实验室和概念证明部署，为了节省资源，可以运行单个控制器。

NSX Controller 群集仅在联机成员达到多数的情况下才能正常工作。如果三个成员中有两个处于联机状态，则群集符合联机成员达到多数的要求。您应该启动脱机 NSX Controller 以恢复三成员群集。如果不能进行备份，则可以替换它。请参见 [替换 NSX Controller 群集的成员](#)。

如果三个成员中只有一个成员处于联机状态，则群集中联机成员未达到多数，群集无法正常工作。如果无法备份任一脱机成员，则可以替换发生故障的 NSX Controller 或重新部署 NSX Controller 群集。请参见 [重新部署 NSX Controller 群集](#)。

前提条件

通过故障排除确认无法恢复设备。例如，以下步骤可以恢复设备，而无需更换这些设备。

- 确认设备具有网络连接；如果没有，请解决该问题。
- 重新引导设备。

后续步骤

获取 NSX Controller 群集状态。请参见[获取 NSX Controller 群集状态](#)。

获取 NSX Controller 群集状态

您可以从 NSX Manager 中确定 NSX Controller 群集的状态。也可以从命令行界面中检查每个 NSX Controller 的状态。

获取 NSX Controller 群集和群集成员的状态可以帮助您确定 NSX Controller 群集问题的来源。

表 17-4. NSX Controller 群集状态

	是否在 NSX Manager 中注册至少一个控制器？	NSX Controller 群集是否占多数？	任何 NSX Controller 群集成员是否发生故障？
NO_CONTROLLERS	否	不适用	不适用
UNAVAILABLE	未知	未知	未知
STABLE	是	是	否
DEGRADED	是	是	是
UNSTABLE	是	否	否

步骤

- 1 登录到 NSX Manager CLI。
- 2 运行 `get management-cluster status` 命令。

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)

Control cluster status: STABLE
```

- 3 登录到 NSX Controller CLI。
- 4 运行 `get control-cluster status` 命令。

```
nsx-controller-1> get control-cluster status
uuid: 03fad907-612f-4068-8109-efdf73002038
is master: true
in majority: true
uuid                address                status
03fad907-612f-4068-8109-efdf73002038 192.168.110.51         active
1228c336-3932-4b5b-b87e-9f66259cebcd 192.168.110.52         active
f5348a2e-2d59-4edc-9618-2c05ac073fd8 192.168.110.53         active
```

重新引导 NSX Controller 群集成员

如果需要重新引导多个 NSX Controller 群集成员，您必须每次重新引导一个成员。如果一个成员处于脱机状态，则三成员群集可以占多数。如果两个成员处于脱机状态，群集将不占多数，而无法正常工作。

步骤

- 1 登录到 NSX Manager 的 CLI。
- 2 获取管理和控制群集的状态。

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
```

```
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
```

```
Control cluster status: STABLE
```

- 3 登录到需要重新引导的 NSX Controller 的 CLI，然后将其重新引导。

```
nsx-controller-2> reboot
Are you sure you want to reboot (yes/no): y
```

- 4 再次获取管理和控制群集的状态。等到控制群集具有 STABLE 状态，然后再重新引导任何其他成员。

在该示例中，NSX Controller 192.168.110.53 正在重新引导，并且控制群集具有 DEGRADED 状态。这意味着群集占多数，但其中的一个成员已关闭。有关 NSX Controller 群集状态的详细信息，请参阅[获取 NSX Controller 群集状态](#)。

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)

Control cluster status: DEGRADED
```

在 NSX Controller 群集处于 STABLE 状态后，就可以安全地重新引导任何其他成员。

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 564D2E9C-A521-6C27-104F-76BBB5FCAC7F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID f5348a2e-2d59-4edc-9618-2c05ac073fd8)
- 192.168.110.51 (UUID 03fad907-612f-4068-8109-efdf73002038)
- 192.168.110.52 (UUID 1228c336-3932-4b5b-b87e-9f66259cebcd)

Control cluster status: STABLE
```

- 5 如果需要了解有关各种 NSX Controller 设备状态的信息，您可以登录到 NSX Controller 并运行 `get control-cluster status` 命令。

```
nsx-controller-1> get control-cluster status
uuid: 03fad907-612f-4068-8109-efdf73002038
is master: true
in majority: true
```

uuid	address	status
03fad907-612f-4068-8109-efdf73002038	192.168.110.51	active
1228c336-3932-4b5b-b87e-9f66259cebcd	192.168.110.52	active
f5348a2e-2d59-4edc-9618-2c05ac073fd8	192.168.110.53	not active

- 6 如果需要，请重复这些步骤以重新引导其他 NSX Controller 设备。

替换 NSX Controller 群集的成员

NSX Controller 群集必须具有至少三个成员。如果 NSX Controller 设备无法运行，或者出于其他任何原因需要从群集中移除该设备，您必须先添加新的 NSX Controller 设备以创建四个成员的群集。在添加第四个成员后，您可以从群集中移除一个 NSX Controller 设备。

前提条件

- 通过故障排除确认无法恢复设备。例如，以下步骤可以恢复设备，而无需更换这些设备。
 - 确认设备具有网络连接；如果没有，请解决该问题。
 - 重新引导设备。
- 确认您了解要替换的 NSX Controller 版本，并具有相同版本的相应安装文件（OVA、OVF 或 QCOW2）。

步骤

- 1 安装并配置新的 NSX Controller。

有关这些步骤的信息和说明，请参阅《《NSX-T Data Center 安装指南》》。

- a 安装新的 NSX Controller 设备。

新 NSX Controller 的版本必须与要替换的 NSX Controller 相同。

- b 将新的 NSX Controller 加入管理层面。

- c 将新的 NSX Controller 加入控制群集。

- 2 关闭要从群集中移除的 NSX Controller。

- 3 登录到另一个 NSX Controller，然后检查要移除的 NSX Controller 是否具有 not active 状态。

```
nsx-controller-1> get control-cluster status
uuid: e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b
is master: true
in majority: true
  uuid                address                status
  06996547-f50c-43c0-95c1-8bb644dea498 192.168.110.53         active
  471e5ac0-194b-437c-9359-564cea845333 192.168.110.54         active
  e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b 192.168.110.51         active
  863f9669-509f-4eba-b0ac-61a9702a242b 192.168.110.52         not active
```

- 4 将控制器与群集断开连接。

```
nsx-controller-1> detach control-cluster 192.168.110.52
Successfully detached node from the control cluster.
```

5 将控制器与管理层面断开连接。

```
nsx-manager-1> detach controller 863f9669-509f-4eba-b0ac-61a9702a242b
The detach operation completed successfully
```

6 验证控制器是否处于活动状态，以及控制群集是否处于稳定状态。

从 NSX Controller 中：

```
nsx-controller-1> get control-cluster status
uuid: e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b
is master: true
in majority: true
```

uuid	address	status
06996547-f50c-43c0-95c1-8bb644dea498	192.168.110.53	active
471e5ac0-194b-437c-9359-564cea845333	192.168.110.54	active
e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b	192.168.110.51	active

从 NSX Manager 中：

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 4213216E-F93A-71B2-DA20-AFE5E714644F) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.51 (UUID e075cf44-0d49-4eb2-9e4f-d8b10ca97a3b)
- 192.168.110.53 (UUID 06996547-f50c-43c0-95c1-8bb644dea498)
- 192.168.110.54 (UUID 471e5ac0-194b-437c-9359-564cea845333)

Control cluster status: STABLE
```

结果

注 已使用 `detach` 命令移除的控制器仍保留某些配置信息。如果要再次将控制器加入到任何控制器群集，则必须在控制器上运行以下 CLI 命令以移除失效信息：

```
deactivate control-cluster
```

重新部署 NSX Controller 群集

如果替换一个控制器并未解决 NSX Controller 群集问题，或者无法恢复多个 NSX Controller 设备，您可以重新部署整个群集。NSX Manager 包含所需的所有配置状态，可以使用该管理器重新创建 NSX Controller 群集。

在还原 NSX Controller 群集期间，数据路径连接不会中断。

前提条件

- 通过故障排除确认无法恢复设备。例如，以下步骤可以恢复设备，而无需更换这些设备。
 - 确认设备具有网络连接；如果没有，请解决该问题。
 - 重新引导设备。
- 确认您了解要替换的 **NSX Controller** 版本，并具有相同版本的相应安装文件（OVA、OVF 或 QCOW2）。
- 确认您了解分配给 **NSX Controller** 设备的 IP 地址。

步骤

- 1 关闭 **NSX Controller** 群集中的所有控制器。
- 2 将控制器与 **NSX Manager** 断开连接。
 - a 登录到 **NSX Manager CLI**。
 - b 使用 `get management-cluster status` 命令获取控制器列表。

```
nsx-manager-1> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.201 (UUID 422EC8D8-B43F-D206-5048-781A5AECDC6) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.53 (UUID c28d0ac7-3107-4548-817a-50d76db007ab)
- 192.168.110.51 (UUID 4a0916c7-2f4d-48c2-81b6-29b7b3758ef4)
- 192.168.110.52 (UUID 1a409f24-9b9a-431e-a03a-1929db74bf00)

Control cluster status: UNSTABLE
```

- c 使用 `detach controller` 命令断开连接控制器。

```
nsx-manager-1> detach controller 1a409f24-9b9a-431e-a03a-1929db74bf00
The detach operation completed successfully
nsx-manager-1> detach controller 4a0916c7-2f4d-48c2-81b6-29b7b3758ef4
The detach operation completed successfully
nsx-manager-1> detach controller c28d0ac7-3107-4548-817a-50d76db007ab
The detach operation completed successfully
```

- 3 安装三个 **NSX Controller** 设备并创建新的 **NSX Controller** 群集。

有关这些步骤的信息和说明，请参阅《《**NSX-T Data Center 安装指南**》》。

- a 安装三个 **NSX Controller** 设备。
 - 新 **NSX Controller** 设备的版本必须与要替换的 **NSX Controller** 设备相同。
 - 为新控制器分配在旧控制器上使用的相同 IP 地址。
- b 将 **NSX Controller** 设备加入管理层面。

- c 在其中的一个 NSX Controller 设备上，初始化控制群集。
- d 将两个其他控制器加入控制群集。

管理 NSX Edge 群集

您可以在以下情况下替换 NSX Edge：该设备无法运行或需要替换硬件。在安装新的 NSX Edge 并创建新的传输节点后，您可以修改 NSX Edge 群集以将旧传输节点替换为新传输节点。

注 移除 Tier-1 NSX Edge 群集将导致 Tier-1 分布式路由器 (DR) 实例暂时停止工作。

步骤

- 1 如果要替换的 NSX Edge 仍在运行，您可以将其置于维护模式以最大限度减少停机时间。如果在关联的逻辑路由器上启用了高可用性，进入维护模式将导致逻辑路由器使用不同的 NSX Edge 群集成员。如果 NSX Edge 无法运行，您不需要执行该操作。

- a 获取发生故障的结构层节点的结构层节点 ID。

```
https://192.168.110.201/api/v1/fabric/nodes
...
  "resource_type": "EdgeNode",
  "id": "a0f4fa74-e77c-11e5-8701-005056aeed61",
  "display_name": "edgenode-02a",
...
```

- b 将发生故障的 NSX Edge 节点置于维护模式。

```
POST https://192.168.110.201/api/v1/fabric/nodes/a0f4fa74-e77c-11e5-8701-005056aeed61?
action=enter_maintenance_mode
```

- 2 安装新的 NSX Edge。

有关这些步骤的信息和说明，请参阅《《NSX-T Data Center 安装指南》》。

- 3 使用 `join management-plane` 命令将新的 NSX Edge 加入管理层面。

有关这些步骤的信息和说明，请参阅《《NSX-T Data Center 安装指南》》。

- 4 将 NSX Edge 配置为传输节点。

有关这些步骤的信息和说明，请参阅《《NSX-T Data Center 安装指南》》。

您可以从 API 中获取发生故障的 NSX Edge 设备的传输节点配置，然后使用该信息创建新的传输节点。

- a 获取新结构层节点的结构层节点 ID。

```
https://192.168.110.201/api/v1/fabric/nodes
...
  "resource_type": "EdgeNode",
  "id": "d61c8d86-f4b8-11e5-b1b2-005056ae3c10",
  "display_name": "edgenode-03a",
...
```

- b 获取发生故障的传输节点的传输节点 ID。

```
GET https://192.168.110.201/api/v1/transport-nodes
...
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
...
}
```

- c 获取发生故障的传输节点的传输节点配置。

```
GET https://192.168.110.201/api/v1/transport-nodes/73cb00c9-70d0-4808-abfe-a12a43251133
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "73cb00c9-70d0-4808-abfe-a12a43251133",
  "display_name": "TN-edgenode-01a",
  "tags": [],
  "transport_zone_endpoints": [
    ...
  ],
  "host_switches": [
    ...
  ],
  "node_id": "a0f4fa74-e77c-11e5-8701-005056aeed61",
  "_create_time": 1457696199196,
  "_last_modified_user": "admin",
  "_last_modified_time": 1457696225606,
  "_create_user": "admin",
  "_revision": 2
}
```

- d 使用 POST /api/v1/transport-nodes 创建新的传输节点。

在请求正文中，为新传输节点提供以下信息：

- 新传输节点的 **description**（可选）
- 新传输节点的 **display_name**
- 用于创建新传输节点的结构层节点的 **node_id**

在请求正文中，从发生故障的传输节点中复制以下信息：

- **transport_zone_endpoints**
- **host_switches**
- **tags**（可选）

```
POST https://192.168.110.201/api/v1/transport-nodes
{
  "description": "",
  "display_name": "TN-edgenode-03a",
  "tags": [
    ...
  ],
  "transport_zone_endpoints": [
    ...
  ],
  "host_switches": [
    ...
  ],
  "node_id": "d61c8d86-f4b8-11e5-b1b2-005056ae3c10"
}
```

5 编辑 NSX Edge 群集以将发生故障的传输节点替换为新传输节点。

- a 获取新传输节点和发生故障的传输节点的 ID。id 字段包含传输节点 ID。

```
GET https://192.168.110.201/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",
    ...
  }
}
```

- b 获取 NSX Edge 群集的 ID。id 字段包含 NSX Edge 群集 ID。从 members 阵列中获取 NSX Edge 群集的成员。

```
GET https://192.168.110.201/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"
    }
  ],
}
```

- c 编辑 NSX Edge 群集以将发生故障的传输节点替换为新传输节点。member_index 必须与发生故障的传输节点的索引相匹配。

小心 如果 NSX Edge 仍在运行，这是一个破坏性操作。这会将所有逻辑路由器端口从发生故障的传输节点移动到新传输节点。

在该示例中，传输节点 TN-edgenode-01a (73cb00c9-70d0-4808-abfe-a12a43251133) 发生故障，并将其替换为 NSX Edge 群集 Edge-Cluster-1 (9a302df7-0833-4237-af1f-4d826c25ad78) 中的传输节点 TN-edgenode-03a (890f0e3c-aa81-46aa-843b-8ac25fe30bd3)。

```
POST http://192.168.110.201/api/v1/edge-clusters/9a302df7-0833-4237-af1f-4d826c25ad78?
action=replace_transport_node
```

```
{
  "member_index": 0,
  "transport_node_id" : "890f0e3c-aa81-46aa-843b-8ac25fe30bd3"
}
```

6 （可选）删除发生故障的传输节点和 NSX Edge 节点。

日志消息

来自所有 NSX-T Data Center 组件（包括 ESXi 主机上运行的组件）的日志消息均符合 RFC 5424 中指定的 syslog 格式。来自 KVM 主机的日志消息采用 RFC 3164 格式。日志文件位于 /var/log 目录中。

在 NSX-T Data Center 设备上，可以运行以下 NSX-T Data Center CLI 命令以查看日志：

```
get log-file <auth.log | http.log | kern.log | manager.log | node-mgmt.log | syslog> [follow]
```

在管理程序上，可以使用 `tac`、`tail`、`grep` 和 `more` 等 Linux 命令查看日志。也可以在 NSX-T Data Center 设备上使用这些命令。

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.
```

每条消息都具有组件 (comp) 和子组件 (subcomp) 信息，可帮助标识消息的来源。

NSX-T Data Center 生成常规日志（程序模块 `local6`，它具有数值 22）和审核日志（程序模块 `local7`，它具有数值 23）。所有 API 调用将触发一个审核日志。

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 定义以下严重性级别：

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

严重性级别	说明
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。

MSGID 字段标识消息的类型。有关消息 ID 列表，请参见[日志消息 ID](#)。

配置远程日志记录

您可以配置 NSX-T Data Center 设备和管理程序以将日志消息发送到远程日志记录服务器。

NSX Manager、NSX Controller、NSX Edge 和管理程序支持远程日志记录。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` 目录中来自动配置 rsyslog 守护进程。

前提条件

- 配置日志记录服务器以接收日志。

步骤

- 1 要在 NSX-T Data Center 设备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>] [certificate <filename>] [structured-data <structured-data>]
```

有关此命令的详细信息，请参见《NSX-T CLI 参考》。您可以多次运行该命令以添加多个日志记录服务器配置。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
```

- b 可以使用 `get logging-server` 命令查看日志记录配置。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
```

2 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
```

3 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 17-5. 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
	群集配置文件
	Edge 群集
	网桥群集和端点
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

表 17-5. 日志消息 ID（续）

消息 ID	示例
ROUTING	逻辑路由器 逻辑路由器端口 静态路由 动态路由 NAT
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） 群集管理 信任管理 许可 用户和角色 任务管理 安装（NSX Manager、NSX Controller） 升级（NSX Manager、NSX Controller、NSX Edge 和主机软件包升级） 实现 标记
MONITORING	SNMP 端口连接 跟踪流
-	所有其他日志消息。

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[如何对公有云使用 NSX-T Data Center 功能](#)，获得自动生成的逻辑实体、支持的功能和 NSX Cloud 所需配置的列表。

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。

前提条件

- 安装至少一个 IPFIX 收集器。
- 确认 IPFIX 收集器具有到管理程序的网络连接。
- 确认任何相关的防火墙（包括 ESXi 防火墙）允许 IPFIX 收集器端口上的流量通过。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **工具 > IPFIX**。
- 3 要配置交换机 IPFIX，请单击 **交换机 IPFIX 收集器** 选项卡。
- 4 单击 **添加**。
- 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 **保存**。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。

2 从导航面板中选择**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。
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 。
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。
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**应用对象**以将配置文件应用于一个或多个对象。

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。

6 单击**保存**。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 **NSX Manager**。

2 从导航面板中选择**工具 > IPFIX**。

3 单击**防火墙 IPFIX 收集器**选项卡。

4 输入名称和可选的说明。

5 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。

6 单击**保存**。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **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。
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。
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 **应用对象** 以将配置文件应用于一个或多个对象。

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。

- 6 单击 **保存**。

ESXi IPFIX 模板

一个 ESXi 主机传输节点支持八个 IPFIX 流量模板。

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()

```

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。

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。

使用跟踪流跟踪数据包路径

在数据包从逻辑网络上的一个逻辑端口传输到同一网络上的另一个逻辑端口时，可以使用跟踪流检查数据包路径。跟踪流跟踪在逻辑端口中注入的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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 导航到“跟踪流”屏幕。您可以使用两种方法。
 - 从导航面板中选择**工具 > 跟踪流**。
 - 从导航面板中选择**交换**，单击**端口**选项卡，选择一个 VIF 连接的端口，然后单击**操作 > 跟踪流**。
- 3 选择一种流量类型。
选项是“单播”、“多播”和“广播”。

4 根据流量类型，指定源和目标信息。

流量类型	指定源信息	指定目标信息
单播	<p>选择一个虚拟机和虚拟接口。</p> <p>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，请从下拉菜单中选择一个地址。</p> <p>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> <p>这也适用于“多播”和“广播”。</p>	<p>从“类型”下拉菜单中选择“虚拟机名称”或“IP-MAC”。</p> <ul style="list-style-type: none"> 如果选择“虚拟机名称”，请选择一个虚拟机和虚拟接口。选择或输入一个 IP 地址和 MAC 地址。 如果选择“IP-MAC”，请选择跟踪类型（第 2 层或第 3 层）。如果跟踪类型为第 2 层，请输入一个 IP 地址和 MAC 地址。如果跟踪类型为第 3 层，请输入一个 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。

5 （可选）单击**高级**以查看高级选项。

6 （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	例如，128
TTL	例如，64
超时 (毫秒)	例如，10000
EtherType	例如，2048
负载类型	从下拉菜单中选择一个选项。
负载数据	根据选定的负载类型（Base64、十六进制、纯文本、二进制或十进制）设置格式的负载

7 （可选）在左侧的列中的“协议”下面，从“类型”下拉菜单中选择一种协议。

8 （可选）根据选择的协议，完成下表中的相关步骤。

协议	步骤 1	步骤 2	步骤 3
TCP	输入一个源端口。	输入一个目标端口。	从下拉菜单中选择所需的 TCP 标记。
UDP	输入一个源端口。	输入一个目标端口。	不适用
ICMP	输入一个 ICMP ID。	输入一个序列值。	不适用

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。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **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。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **网络 > 交换**。
- 3 单击**端口**选项卡。
- 4 单击端口的名称。
- 5 单击**监控**选项卡。

此时将显示端口状态和统计信息。

- 6 要下载主机已发现的 MAC 地址的 CSV 文件，请单击**下载 MAC 表**。
- 7 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](#)。

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。

NSX Cloud 说明 如果使用 NSX Cloud，请参见[如何对公有云使用 NSX-T Data Center 功能](#)，获得自动生成的逻辑实体、支持的功能和 NSX Cloud 所需配置的列表。

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。
- 目标端口只能接收镜像流量。
- 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。
- 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。
- 使用数据层面开发工具包 (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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择 **工具 > 端口镜像会话**。
- 3 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**。
- 4 输入会话名称和可选描述。
- 5 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。
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。 ■ 传输节点 - 如果封装为 ERSPAN II 或 ERSPAN III，则指定一个传输节点。 ■ 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。

- 6 单击 **下一步**。

- 7 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。

会话类型	参数
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。

8 单击下一步。

9 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。

10 单击保存。

保存端口镜像会话后，无法更改源或目标。

监控结构层节点

您可以从 NSX Manager UI 中监控结构层节点，例如，主机、Edge、NSX Edge 群集、网桥和传输节点。

步骤

- 1 从浏览器中，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**结构层 > 节点**。
- 3 选择以下选项卡之一。
 - 主机
 - Edge
 - Edge 群集
 - 网桥
 - 传输节点

结果

注 在“主机”屏幕上，如果主机的 MPA 连接状态为“关闭”或“未知”，请忽略 LCP 连接状态，因为该状态可能不准确。

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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**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。

收集支持包

您可以在注册的群集和结构层节点上收集支持包，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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 从导航面板中选择**系统 > 实用程序**。
- 3 单击**支持包**选项卡。
- 4 选择目标节点。

可用的节点类型包括管理节点、控制器节点、Edge、主机和公有云网关。

- 5 （可选）指定日志期限天数以排除早于指定天数的日志。
- 6 （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。

- 7 （可选）选中相应的复选框以将包上载到文件服务器中。

- 8 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。
- 9 监控收集过程的状态。
状态字段显示完成支持包收集的节点的百分比。
- 10 如果未设置将包发送到文件服务器的选项，请单击**下载**以下载包。

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。

还可以编辑现有 CEIP 配置以加入或退出该计划，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管理程序同步。
- 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，使用管理员权特权登录到位于 <https://nsx-manager-ip-address> 的 NSX Manager。
- 2 选择**系统 > 配置 > 属性**。
- 3 在“状态和统计信息”部分中，单击**编辑**。
- 4 切换**数据收集**菜单项。
- 5 在“客户体验提升计划”部分中，单击**编辑**。
- 6 切换**加入 VMware 客户体验提升计划**菜单项。
- 7 （可选）配置数据收集设置和上载重复周期设置。
- 8 （可选）单击**代理**选项卡。
- 9 切换**代理**菜单项以配置用于发送数据的代理服务器设置。

选项	说明
主机名	输入代理服务器的 FQDN 或 IP 地址。
端口	输入代理服务器端口。
用户名	（可选）输入用于向代理服务器进行身份验证的用户名。

选项	说明
密码	(可选) 输入用于向代理服务器进行身份验证的密码。
方案	通过下拉菜单设置代理服务器可接受 HTTP 还是 HTTPS 方案。

10 单击 **保存**。