

NSX 管理指南

Update 3

修改日期：2017 年 11 月 20 日

VMware NSX Data Center for vSphere 6.2



vmware®

您可以从 VMware 网站下载最新的技术文档：

<https://docs.vmware.com/cn/>。

VMware 网站还提供了最近的产品更新。

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

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

目录

NSX 管理指南	8
1 NSX 的系统要求	9
2 NSX 所需的端口和协议	11
3 NSX 概览	14
NSX 组件	15
NSX Edge	17
NSX Services	19
4 跨 vCenter 网络和安全概述	22
跨 vCenter NSX 的优点	22
跨 vCenter NSX 的工作方式	23
跨 vCenter NSX 中支持的 NSX Services 列表	24
通用控制器群集	25
通用传输区域	25
通用逻辑交换机	26
通用逻辑（分布式）路由器	26
通用防火墙规则	26
通用网络和安全对象	27
跨 vCenter NSX 拓扑	27
修改 NSX Manager 角色	30
5 传输区域	32
添加传输区域	34
查看和编辑传输区域	36
扩大传输区域	36
缩小传输区域	36
6 逻辑交换机	37
添加逻辑交换机	38
将虚拟机连接到逻辑交换机	42
测试逻辑交换机连接	42
避免逻辑交换机中出现欺骗行为	43
编辑逻辑交换机	43
逻辑交换机场景	43

7 配置硬件网关 48

场景：硬件网关示例配置 49

8 L2 网桥 54

添加 L2 网桥 55

向逻辑路由环境添加 L2 网桥 55

9 路由 57

添加逻辑（分布式）路由器 57

添加 Edge 服务网关 69

指定全局配置 78

NSX Edge 配置 80

添加静态路由 94

在逻辑（分布式）路由器上配置 OSPF 95

在 Edge 服务网关上配置 OSPF 101

配置 BGP 106

配置 IS-IS 协议 110

配置路由重新分发 112

查看 NSX Manager 区域设置 ID 113

在通用逻辑（分布式）路由器上配置区域设置 ID 113

在主机或群集上配置区域设置 ID 113

10 逻辑防火墙 115

分布式防火墙 115

Edge 防火墙 117

使用防火墙规则区域 117

使用防火墙规则 119

从防火墙保护中排除虚拟机 131

虚拟机的 IP 发现 132

查看防火墙 CPU 和内存阈值事件 133

防火墙日志 133

使用 NSX Edge 防火墙规则 135

11 身份防火墙概述 143

身份防火墙 workflow 144

12 使用 Active Directory 域 145

向 NSX Manager 注册 Windows 域 145

将 Windows 域与 Active Directory 同步 146

编辑 Windows 域 147

在 Windows 2008 上启用安全只读日志访问 147

[验证目录权限](#) 148

13 使用 SpoofGuard 149

[创建 SpoofGuard 策略](#) 150

[批准 IP 地址](#) 150

[编辑 IP 地址](#) 151

[清除 IP 地址](#) 151

14 虚拟专用网络 (VPN) 153

[SSL VPN-Plus 概览](#) 153

[IPSec VPN 概览](#) 177

[L2 VPN 概述](#) 184

15 逻辑负载均衡器 193

[设置负载均衡](#) 193

[管理应用程序配置文件](#) 209

[管理服务监控器](#) 210

[管理服务器池](#) 211

[管理虚拟服务器](#) 213

[管理应用程序规则](#) 213

[对使用 NTLM 身份验证的 Web 服务器进行负载均衡](#) 214

[NSX 负载均衡器配置场景](#) 215

16 其他 Edge 服务 225

[管理 DHCP 服务](#) 225

[配置 DHCP 中继](#) 228

[配置 DNS 服务器](#) 230

17 服务编排 231

[使用服务编排](#) 232

[服务编排的图形视图](#) 239

[使用安全标记](#) 242

[查看有效服务](#) 244

[使用安全策略](#) 245

[编辑安全组](#) 246

[服务编排场景](#) 246

18 Guest Introspection 252

[安装 Guest Introspection](#) 252

[查看 Guest Introspection 状态](#) 255

[Guest Introspection 警报](#) 256

- [Guest Introspection 事件](#) 256
- [Guest Introspection 审核消息](#) 257
- [收集 Guest Introspection 故障排除数据](#) 257
- [卸载 Guest Introspection 模块](#) 258

19 数据安全 259

- [安装 NSX 数据安全](#) 259
- [NSX 数据安全用户角色](#) 260
- [定义数据安全策略](#) 261
- [运行数据安全扫描](#) 262
- [查看和下载报告](#) 263
- [创建正则表达式](#) 263
- [卸载 NSX 数据安全](#) 264

20 网络可扩展性 265

- [分布式服务插入](#) 266
- [基于 Edge 的服务插入](#) 266
- [集成第三方服务](#) 266
- [部署合作伙伴服务](#) 266
- [通过服务编排使用供应商服务](#) 268
- [通过逻辑防火墙将流量重定向到供应商解决方案](#) 268
- [使用合作伙伴负载均衡器](#) 269
- [移除第三方集成](#) 269

21 用户管理 271

- [NSX 用户和各功能访问权限](#) 271
- [配置 Single Sign On](#) 286
- [管理用户权限](#) 287
- [管理默认用户帐户](#) 288
- [将角色分配给 vCenter 用户](#) 288
- [编辑用户帐户](#) 291
- [更改用户角色](#) 291
- [禁用或启用用户帐户](#) 292
- [删除用户帐户](#) 292

22 网络对象和安全对象 293

- [使用 IP 地址组](#) 293
- [使用 MAC 地址组](#) 294
- [使用 IP 池](#) 296
- [使用安全组](#) 297
- [使用服务和服务组](#) 299

23 操作和管理 302

更改控制器密码 302

从 NSX Controller 故障恢复 303

更改 VXLAN 端口 304

检查通信通道运行状况 305

客户体验改进计划 306

系统事件和审核日志 307

管理系统设置 311

使用 SNMP 陷阱 317

NSX 备份和还原 320

流量监控 324

活动监控 330

跟踪流 344

24 NSX Edge VPN 配置示例 353

术语 354

IKE 阶段 1 和阶段 2 354

配置 IPSec VPN 服务示例 356

使用 Cisco 2821 集成服务路由器 358

使用 Cisco ASA 5510 361

配置 WatchGuard Firebox X500 363

NSX Edge 配置故障排除示例 363

NSX 管理指南

《NSX 管理指南》介绍如何使用 **NSX Manager** 用户界面和 **vSphere Web Client** 配置、监控和维护 VMware® NSX™ 系统。此信息包括分步配置说明以及建议的最佳做法。

目标读者

本手册专供要在 VMware vCenter 环境中安装或使用 NSX 的用户使用。本手册的目标读者为熟悉虚拟机技术和虚拟数据中心操作且经验丰富的系统管理员。本手册假设您熟悉 VMware Infrastructure 5.x，包括 VMware ESX、vCenter Server 和 vSphere Web Client。

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>。

NSX 的系统要求

在安装或升级 NSX 之前，请考虑您的网络配置和资源。您可以在每个 vCenter Server 中安装一个 NSX Manager，在每个 ESXi™ 主机上安装一个 Guest Introspection 和数据安全实例，并在每个数据中心安装多个 NSX Edge 实例。

硬件

表 1-1. 硬件要求

设备	内存	vCPU	磁盘空间
NSX Manager	16 GB（某些 NSX 部署规模为 24 GB*）	4（某些 NSX 部署规模为 8*）	60 GB
NSX Controller	4 GB	4	20 GB
NSX Edge	<ul style="list-style-type: none"> ■ 精简：512 MB ■ 中型：1 GB ■ 大型：1 GB ■ 超大型：8 GB 	<ul style="list-style-type: none"> ■ 精简：1 ■ 中型：2 ■ 大型：4 ■ 超大型：6 	<ul style="list-style-type: none"> ■ 精简：1 磁盘 500 MB ■ 中型：1 磁盘 500 MB + 1 磁盘 512 MB ■ 大型：1 磁盘 500 MB + 1 磁盘 512 MB ■ 超大型：1 磁盘 500 MB + 1 磁盘 2 GB
Guest Introspection	1 GB	2	4 GB
NSX 数据安全	512 MB	1	每个 ESXi 主机 6 GB

作为一般准则，如果您的 NSX 受管环境包含超过 256 个管理程序或 2000 个虚拟机，您应该将 NSX Manager 资源增加到 8 个 vCPU 和 24 GB RAM。

有关特定规模的详细信息，请联系 VMware 支持人员。

有关为虚拟设备增加内存和 vCPU 分配的信息，请参见《vSphere 虚拟机管理》中的“分配内存资源”和“更改虚拟 CPU 数目”。

软件

有关互操作性的最新信息，请参见产品互操作性列表，网址为 http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php。

有关建议的 NSX、vCenter Server 和 ESXi 版本，请参见位于 <https://docs.vmware.com/cn/VMware-NSX-for-vSphere/index.html> 的发行说明。

注意，要让 NSX Manager 加入跨 vCenter NSX 部署，需要满足以下条件：

组件	版本
NSX Manager	6.2 或更高版本
NSX Controller	6.2 或更高版本
vCenter Server	6.0 或更高版本
ESXi	<ul style="list-style-type: none"> ESXi 6.0 或更高版本 为 NSX 6.2 或更高版本的 VIB 准备的主机群集

要从单个 vSphere Web Client 管理跨 vCenter NSX 部署中的所有 NSX Manager，必须在增强型链接模式下连接 vCenter Server。请参见《vCenter Server 和主机管理》中的“使用增强型链接模式”。

要检查合作伙伴解决方案与 NSX 的兼容性，请参见《VMware Networking and Security 兼容性指南》，网址为 <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>。

客户端和用户访问权限

- 如果按名称将 ESXi 主机添加到 vSphere 清单中，请确保正向和反向名称解析正常工作。否则，NSX Manager 将无法解析 IP 地址。
- 添加和打开虚拟机电源的权限
- 访问存储虚拟机文件的数据存储的权限，以及将文件复制到该数据存储的帐户权限
- 在 Web 浏览器中启用 cookie 以访问 NSX Manager 用户界面
- 从 NSX Manager 中，确保可以从要部署的 ESXi 主机、vCenter Server 和 NSX 设备中访问端口 443。需要使用该端口在 ESXi 主机上下载 OVF 文件以进行部署。
- 使用的 vSphere Web Client 版本支持的 Web 浏览器。请参见《vCenter Server 和主机管理》文档中的“使用 vSphere Web Client”以了解详细信息。

NSX 所需的端口和协议

以下端口必须处于打开状态才能使 NSX 正常工作。

表 2-1. NSX 所需的端口和协议

源	目标	端口	协议	用途	敏感	TLS	身份验证
客户端 PC	NSX Manager	443	TCP	NSX Manager 管理接口	否	是	PAM 身份验证
客户端 PC	NSX Manager	80	TCP	NSX Manager VIB 访问	否	否	PAM 身份验证
ESXi 主机	vCenter Server	443	TCP	ESXi 主机准备	否	否	
vCenter Server	ESXi 主机	443	TCP	ESXi 主机准备	否	否	
ESXi 主机	NSX Manager	5671	TCP	RabbitMQ	否	是	RabbitMQ 用户/密码
ESXi 主机	NSX Controller	1234	TCP	用户方代理连接	否	是	
NSX Controller	NSX Controller	2878、2888、3888	TCP	控制器群集 - 状态同步	否	是	IPsec
NSX Controller	NSX Controller	7777	TCP	内部控制器 RPC 端口	否	是	IPsec
NSX Controller	NSX Controller	30865	TCP	控制器群集 - 状态同步	否	是	IPsec
NSX Manager	NSX Controller	443	TCP	控制器与 Manager 通信	否	是	用户/密码
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	否	是	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	否	是	
NSX Manager	ESXi 主机	443	TCP	管理和置备连接	否	是	
NSX Manager	ESXi 主机	902	TCP	管理和置备连接	否	是	
NSX Manager	DNS 服务器	53	TCP	DNS 客户端连接	否	否	
NSX Manager	DNS 服务器	53	UDP	DNS 客户端连接	否	否	
NSX Manager	Syslog 服务器	514	TCP	Syslog 连接	否	否	

表 2-1. NSX 所需的端口和协议（续）

源	目标	端口	协议	用途	敏感	TLS	身份验证
NSX Manager	Syslog 服务器	514	UDP	Syslog 连接	否	否	
NSX Manager	NTP Time Server	123	TCP	NTP 客户端连接	否	是	
NSX Manager	NTP Time Server	123	UDP	NTP 客户端连接	否	是	
vCenter Server	NSX Manager	80	TCP	主机准备	否	是	
REST 客户端	NSX Manager	443	TCP	NSX Manager REST API	否	是	用户/密码
VXLAN 隧道端点 (VTEP)	VXLAN 隧道端点 (VTEP)	8472 (NSX 6.2.3 之前的默认值) 或 4789 (新安装的 NSX 6.2.3 及更高版本中的默认值)	UDP	VTEP 之间的传输网络封装	否	是	
ESXi 主机	ESXi 主机	6999	UDP	防止 VLAN LIF 上的 ARP	否	是	
ESXi 主机	NSX Manager	8301、8302	UDP	DVS 同步	否	是	
NSX Manager	ESXi 主机	8301、8302	UDP	DVS 同步	否	是	
Guest Introspection 虚拟机	NSX Manager	5671	TCP	RabbitMQ	否	是	RabbitMQ 用户/密码
主 NSX Manager	辅助 NSX Manager	443	TCP	跨 vCenter NSX 通用同步服务	否	是	
主 NSX Manager	vCenter Server	443	TCP	vSphere API	否	是	
辅助 NSX Manager	vCenter Server	443	TCP	vSphere API	否	是	
主 NSX Manager	NSX 通用控制器群集	443	TCP	NSX Controller REST API	否	是	用户/密码
辅助 NSX Manager	NSX 通用控制器群集	443	TCP	NSX Controller REST API	否	是	用户/密码
ESXi 主机	NSX 通用控制器群集	1234	TCP	NSX 控制层面协议	否	是	

表 2-1. NSX 所需的端口和协议（续）

源	目标	端口	协议	用途	敏感	TLS	身份验证
ESXi 主机	主 NSX Manager	5671	TCP	RabbitMQ	否	是	RabbitMQ 用户/密码
ESXi 主机	辅助 NSX Manager	5671	TCP	RabbitMQ	否	是	RabbitMQ 用户/密码

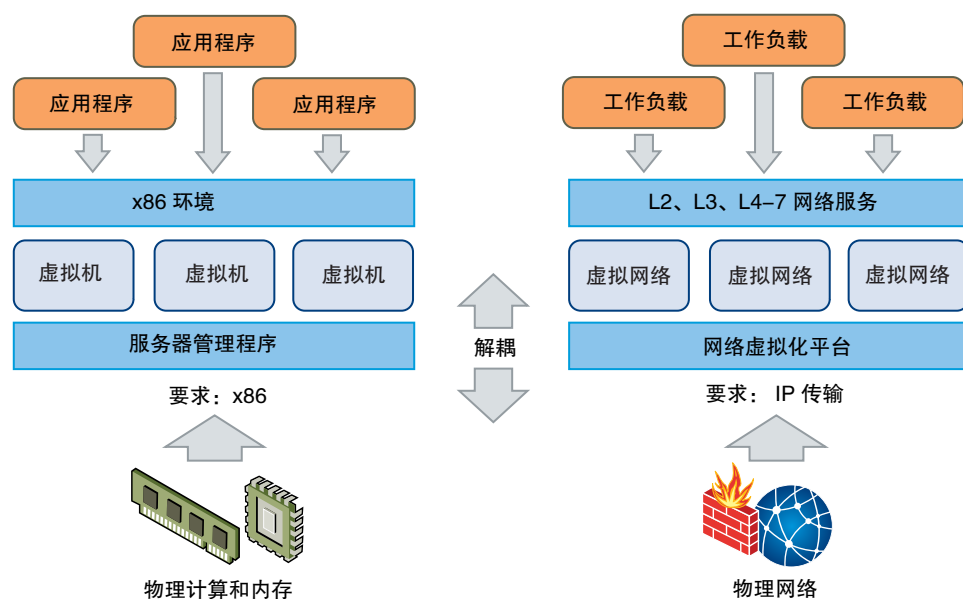
跨 vCenter NSX 和增强型链接模式的端口

如果您有一个跨 vCenter NSX 环境，并且 vCenter Server 系统处于增强型链接模式，则要从任何 vCenter Server 系统中管理任何 NSX Manager，每个 NSX Manager 设备必须具有到该环境中每个 vCenter Server 系统的所需连接。

NSX 概览

IT 组织已经从服务器虚拟化中明显获益。服务器整合降低了物理复杂性，提高了运营效率，并且能够动态地重新调整基础资源的用途，使其以最佳方式快速满足日益动态化的业务应用需求。

现在，VMware 的软件定义数据中心 (SDDC) 架构正将虚拟化技术延展至整个物理数据中心基础架构。VMware NSX[®] 网络虚拟化平台是 SDDC 架构中的一个重要产品。使用 NSX 可以实现网络虚拟化，正如计算和存储虚拟化交付。与服务器虚拟化的工作原理（通过编程方式对基于软件的虚拟机 (VM) 执行创建、生成快照、删除和还原操作）大致相同，NSX 网络虚拟化也是通过编程方式对基于软件的虚拟网络执行创建、生成快照、删除和还原操作。这使得联网方式发生了彻底变革，不仅使数据中心管理人员能够将敏捷性和经济性提高若干数量级，而且还能极大地简化底层物理网络的运营模式。NSX 能够部署在任何 IP 网络上，包括现有的传统网络模型以及任何供应商提供的新一代体系结构，它为您提供了一个彻底无中断的解决方案。事实上，使用 NSX，您只需利用现有的物理网络基础架构即可部署软件定义的数据中心。



上图对计算和网络虚拟化进行了类比。通过服务器虚拟化，软件抽象层（服务器虚拟机管理程序）可在软件中重现人们所熟悉的 x86 物理服务器属性（例如 CPU、内存、磁盘、网卡），从而可通过编程方式来任意组合这些属性，只需短短数秒，即可生成一台独一无二的虚拟机。

通过网络虚拟化，与网络虚拟机管理程序等效的功能可在软件中重现第 2 层到第 7 层的一整套网络服务（例如，交换、路由、访问控制、防火墙、QoS 和负载均衡）。因此，可通过编程方式任意组合这些服务，只需短短数秒，即可生成独一无二的独立虚拟网络。

通过网络虚拟化，带来了类似于服务器虚拟化的优势。例如，就像虚拟机独立于基础 x86 平台并允许 IT 将物理主机视为计算容量池一样，虚拟网络也独立于底层 IP 网络硬件并允许 IT 将物理网络视为可以按需使用和调整用途的传输容量池。与传统架构不同的是，无需重新配置底层物理硬件或拓扑，即可通过编程方式置备、更改、存储、删除和还原虚拟网络。与企业从熟悉的服务器和存储虚拟化解决方案获得的功能和优势相匹配，这一革命性的联网方式可发挥软件定义的数据中心的全部潜能。

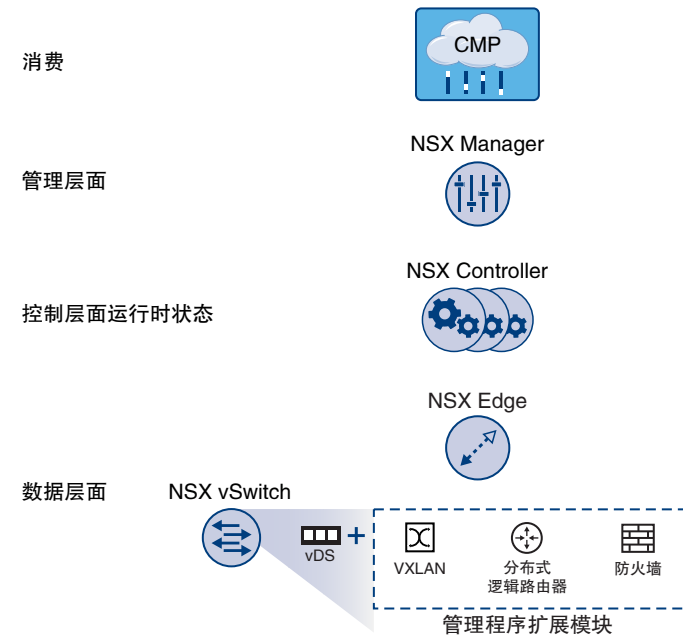
可通过 vSphere Web Client、命令行界面 (CLI) 和 REST API 配置 NSX。

本章讨论了以下主题：

- [NSX 组件](#)
- [NSX Edge](#)
- [NSX Services](#)

NSX 组件

本部分介绍 NSX 解决方案的各个组件。



请注意，云管理平台 (CMP) 不是 NSX 的组件，但 NSX 通过 REST API 以虚拟方式提供与任何 CMP 的集成以及与 VMware CMP 的开箱即用集成功能。

数据层面

NSX 数据层面由 NSX vSwitch 组成，在 vSphere Distributed Switch (VDS) 基础上增加了支持服务的组件。NSX 内核模块、用户空间代理、配置文件和安装脚本均打包为 VIB，并在虚拟机管理程序内核内运行，以提供诸如分布式路由和逻辑防火墙的服务，并启用 VXLAN 桥接功能。

NSX vSwitch（基于 **vDS**）可对物理网络进行抽象化处理并在虚拟机管理程序中提供访问级别的交换。它是网络虚拟化的核心，因为它可实现独立于物理构造的逻辑网络（如 **VLAN**）。**vSwitch** 的一些优势包括：

- 利用协议（如 **VXLAN**）和集中式网络配置支持覆盖网络。覆盖网络可实现以下功能：
 - 减少了 **VLAN ID** 在物理网络中的使用。
 - 在现有物理基础架构的现有 **IP** 网络上创建一个叠加的灵活逻辑层 2 (**L2**)，而无需重新设计任何数据中心网络
 - 置备通信（东西向和南北向），同时保持租户之间的隔离状态
 - 应用程序工作负载和虚拟机独立于覆盖网络，就像连接到物理 **L2** 网络一样运行
- 有利于实现虚拟机管理程序的大规模扩展
- 端口镜像、**NetFlow/IPFIX**、配置备份和还原、网络运行状况检查、**QoS** 和 **LACP** 等多种功能构成了一个完整的工具包，可以在虚拟网络内执行流量管理、监控和故障排除等操作。

逻辑路由器的 **L2** 可以将逻辑网络空间 (**VXLAN**) 与物理网络 (**VLAN**) 桥接。

网关设备通常是 **NSX Edge** 虚拟设备。**NSX Edge** 提供 **L2**、**L3**、外围防火墙、负载平衡以及 **SSL VPN** 和 **DHCP** 等其他服务。

控制层面

NSX 控制层面在 **NSX Controller** 群集中运行。**NSX Controller** 是一个高级分布式状态管理系统，它提供了控制层面功能以实现 **NSX** 逻辑交换和路由功能。对于网络内的所有逻辑交换机而言，它是中央控制点，负责维护所有主机、逻辑交换机 (**VXLAN**) 和分布式逻辑路由器的相关信息。

控制器群集负责管理虚拟机管理程序中的分布式交互和路由模块。控制器中没有任何数据层面的流量通过。控制器节点部署在包含三个成员的群集中，以实现高可用性和可扩展性。控制器节点的任何故障都不会影响数据层面的流量。

NSX Controller 通过将网络信息分发到主机来进行工作。为实现高度弹性，**NSX Controller** 进行了群集化以实现横向扩展和 **HA**。**NSX Controller** 必须部署在三节点群集中。三个虚拟设备将提供、维护并更新在 **NSX** 域中工作的所有网络的状态。**NSX Manager** 用于部署 **NSX Controller** 节点。

三个 **NSX Controller** 节点形成一个控制器群集。控制器群集需要达到仲裁数（也称为多数），以避免出现“脑裂情况”。在脑裂情况下，数据不一致性是由维护两个重叠的单独数据集引起的。不一致性可能由错误状况和数据同步问题导致。部署三个控制器节点可在其中一个 **NSX Controller** 节点出现故障时确保数据冗余。

一个控制器群集具有多个角色，包括：

- **API** 提供程序
- 持久服务器
- 交换机管理器
- 逻辑管理器
- 目录服务器

每个角色都具有一个主控制器节点。如果某个角色的主控制器节点失败，则群集会从可用的 **NSX Controller** 节点中为该角色选择一个新的主节点。该角色新的主 **NSX Controller** 节点将在其余 **NSX Controller** 节点之中重新分配丢失的部分工作。

NSX 支持三个逻辑交换机控制层面模式：多播、单播和混合。使用控制器群集管理基于 **VXLAN** 的逻辑交换机无需物理网络架构的多播支持。您无需置备多播组 IP 地址，也不需要物理交换机或路由器上启用 **PIM** 路由或 **IGMP** 侦听功能。因此，单播模式和混合模式可以将 **NSX** 从物理网络脱离。处于单播控制层面模式的 **VXLAN** 不需要物理网络支持多播以处理逻辑交换机中的广播、未知单播和多播 (**BUM**) 流量。单播模式会在本地复制主机上所有 **BUM** 流量，且无需任何物理网络配置。在混合模式中，一些 **BUM** 流量复制将卸载到第一个跃点物理交换机上以获得更好性能。混合模式需要在第一个跃点交换机上进行 **IGMP** 侦听，并需要访问每个 **VTEP** 子网中的 **IGMP** 查询器。

管理层面

NSX 管理层面由 **NSX Manager** 构建，是 **NSX** 的集中式网络管理组件。该层面提供单个配置点和 **REST API** 入口点。

NSX Manager 可作为虚拟设备安装在 **vCenter Server** 环境中的任意 **ESX™** 主机上。**NSX Manager** 和 **vCenter** 是一对一的关系。**NSX Manager** 的每个实例对应于一个 **vCenter Server**。在跨 **vCenter NSX** 环境中，情况也是这样。

在跨 **vCenter NSX** 环境中，同时存在一个主 **NSX Manager** 和一个或多个辅助 **NSX Manager**。主 **NSX Manager** 用于创建和管理通用逻辑交换机、通用逻辑（分布式）路由器和通用防火墙规则。辅助 **NSX Manager** 用于管理特定 **NSX Manager** 的本地网络服务。在一个跨 **vCenter NSX** 环境中，主 **NSX Manager** 最多可关联七个辅助 **NSX Manager**。

消费平台

NSX 的消费使用可通过 **vSphere Web Client** 中的 **NSX Manager** 用户界面查看。通常，最终用户将网络虚拟化与其云管理平台相融合，以部署应用。**NSX** 通过 **REST API** 提供丰富的集成功能，几乎可集成到任何 **CMP** 中。还可通过 **VMware vCloud Automation Center**、**vCloud Director** 和带有适用于 **NSX** 的 **Neutron** 插件的 **OpenStack** 获得开箱即用的集成功能。

NSX Edge

可以安装 **NSX Edge** 作为 **Edge 服务网关 (ESG)** 或分布式逻辑路由器 (**DLR**)。每个主机上的 **Edge** 设备数量（包括 **ESG** 和 **DLR**）限制为 250 个。

Edge 服务网关

通过 ESG，您可以访问所有 NSX Edge 服务，例如防火墙、NAT、DHCP、VPN、负载平衡和高可用性。您可以在数据中心中安装多个 ESG 虚拟设备。每个 ESG 虚拟设备总共可以拥有十个上行链路和内部网络接口。借助中继，一个 ESG 最多可以拥有 200 个子接口。内部接口连接至安全的端口组，并充当端口组中所有受保护虚拟机的网关。分配给内部接口的子网可以是公开路由的 IP 空间，也可以是采用 NAT/路由的 RFC 1918 专用空间。对网络接口之间的流量会实施防火墙规则和其他 NSX Edge 服务。

ESG 的上行链路接口连接至上行链路端口组，后者可以访问共享企业网络或提供访问层网络连接功能的服务。可以为负载平衡器、点对点 VPN 和 NAT 服务配置多个外部 IP 地址。

分布式逻辑路由器

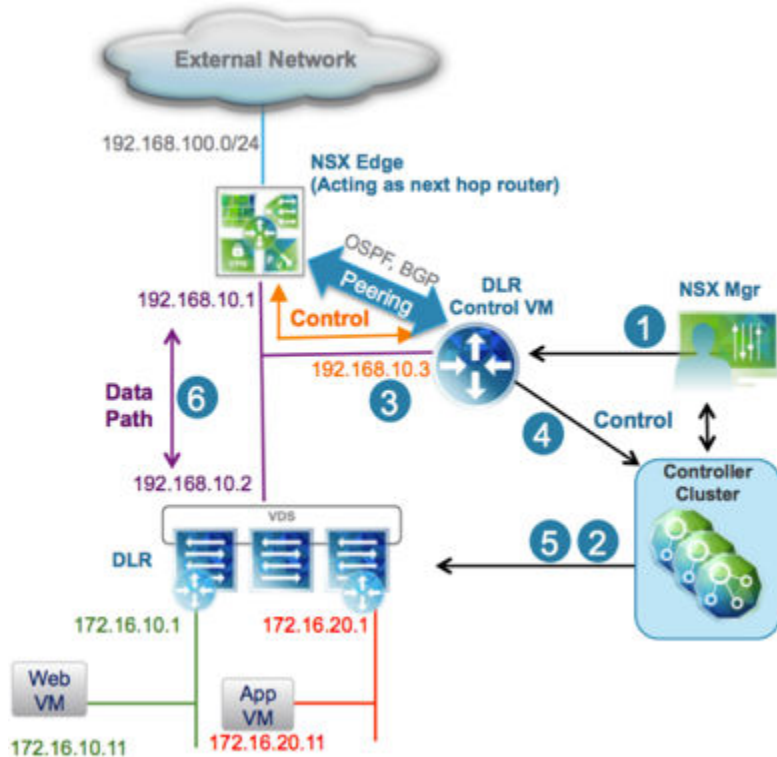
DLR 提供东西向分布式路由，可实现租户 IP 地址空间和数据路径隔离。位于不同子网中同一台主机上的虚拟机或工作负载可以彼此通信，而无需遍历传统的路由接口。

逻辑路由器可以有八个上行链路接口和多达一千个内部接口。DLR 上的上行链路接口通常与 ESG 建立对等关系，DLR 与 ESG 之间存在第 2 层逻辑转换交换机。DLR 上的内部接口与 ESX 管理程序上托管的虚拟机建立对等关系，虚拟机与 DLR 之间存在逻辑交换机。

DLR 有两个主要组件：

- DLR 控制层面由 DLR 虚拟设备提供（也称为控制虚拟机）：此虚拟机支持动态路由协议（BGP 和 OSPF），与下一个第 3 层跃点设备（通常为 Edge 服务网关）交换路由更新，并与 NSX Manager 和 NSX Controller 群集进行通信。通过活动-待机配置支持 DLR 虚拟设备的高可用性：当您创建启用了 HA 的 DLR 时，系统将提供一对在活动/待机模式下运行的虚拟机。
- 在数据层面级别，属于 NSX 域中的 ESXi 主机上安装有 DLR 内核模块 (VIB)。内核模块类似于支持第 3 层路由的模块化机架中的线路卡。内核模块具有通过控制器群集推送的路由信息库 (RIB)（也称为路由表）。路由查找、ARP 条目查找的数据层面功能均由内核模块执行。内核模块配有逻辑接口（称为 LIF），可连接到不同的逻辑交换机以及任意 VLAN 支持的端口组。每个 LIF 都分配有一个 IP 地址（代表其所连接的逻辑 L2 分段的默认 IP 网关）和一个 vMAC 地址。IP 地址对每个 LIF 而言是唯一的，而为所有已定义的 LIF 分配的 vMAC 都相同。

图 3-1. 逻辑路由组件



- 1 DLR 实例已利用 OSPF 或 BGP 从 NSX Manager UI（或通过 API 调用）创建，并且路由已启用。
- 2 NSX Controller 利用控制层面和 ESXi 主机推送新的 DLR 配置（包括 LIF 及其关联的 IP 和 vMAC 地址）。
- 3 如果假定在下一个跃点设备（在本例中为 NSX Edge [ESG]）上也启用路由协议，则会在 ESG 与 DLR 控制虚拟机之间建立 OSPF 或 BGP 对等互连。ESG 和 DLR 就可以交换路由信息：
 - DLR 控制虚拟机可以配置为将所有已连接逻辑网络的 IP 前缀（在本例中为 172.16.10.0/24 和 172.16.20.0/24）重新分发到 OSPF 中。结果是将其这些路由播发推送到 NSX Edge 中。注意，这些前缀的下一跃点不是分配给控制虚拟机的 IP 地址 (192.168.10.3)，而是标识 DLR 的数据层面组件的 IP 地址 (192.168.10.2)。前者称为 DLR “协议地址”，而后者是“转发地址”。
 - NSX Edge 将前缀推送到控制虚拟机，以访问外部网络中的 IP 网络。在大多数情况下，NSX Edge 很有可能发送一个默认路由，因为该路由代表面向物理网络基础架构的单个退出点。
- 4 DLR 控制虚拟机将从 NSX Edge 获知的 IP 路由推送到控制器群集中。
- 5 控制器群集负责在虚拟化管理程序之间分发从 DLR 控制虚拟机获知的路由。群集中的每个控制器节点负责为特殊的逻辑路由器实例分发信息。在部署了多个逻辑路由器实例的部署中，负载跨多个控制器节点分布。单独的逻辑路由器实例通常与每个部署的租户关联。
- 6 主机上的 DLR 路由内核模块处理数据路径流量，以通过 NSX Edge 与外部网络通信。

NSX Services

NSX 各组件协同工作以提供以下功能性服务。

逻辑交换机

云部署或虚拟数据中心具有跨多个租户的多种应用程序。出于安全、故障隔离和避免 IP 地址重叠等目的，这些应用程序和租户需要互相隔离。**NSX** 允许创建多个逻辑交换机，每一个交换机都是一个逻辑广播域。应用程序或租户虚拟机可以按逻辑有线连接到逻辑交换机。这可以在仍提供物理网络广播域 (VLAN) 的所有特性的同时保证部署的灵活性和速度，而不出现物理第 2 层散乱或生成树问题。

逻辑交换机是分布式的，可以跨越 **vCenter** 中的所有主机（或跨 **vCenter NSX** 环境中的所有主机）。这样，虚拟机可以在数据中心内移动 (vMotion)，而不会受到物理第 2 层 (VLAN) 边界的限制。物理基础架构不受 MAC/FIB 表限制的约束，因为逻辑交换机以软件形式包含广播域。

逻辑路由器

动态路由可在第 2 层广播域之间提供必需的转发信息，从而帮助减小第 2 层广播域的大小，提高网络效率，改进网络的可扩展性。**NSX** 还将此信息扩展到工作负载所在的位置，用于东西向路由。这样，虚拟机之间就可以直接进行通信，无需花费额外的成本和时间来扩展跃点。同时，**NSX** 逻辑路由器也提供南北向连接，从而使租户可以访问公用网络。

逻辑防火墙

逻辑防火墙为动态虚拟数据中心提供安全机制。逻辑防火墙的分布式防火墙组件允许您基于以下各项对虚拟机之类的虚拟数据中心实体进行分段：虚拟机名称和属性、用户标识、**vCenter** 对象（如数据中心）、主机以及传统的网络连接属性（如 IP 地址、VLAN 等）。Edge 防火墙组件可帮助您实现关键外围安全需求，例如，基于 IP/VLAN 构造建立 DMZ，在多租户虚拟数据中心内让租户彼此隔离。

流量监控功能会显示在应用程序协议级别的虚拟机之间的网络活动。您可以使用此信息审核网络流量、定义和细化防火墙策略以及识别对网络的威胁。

逻辑虚拟专用网络 (VPN)

SSL VPN-Plus 允许远程用户访问专用的企业应用程序。IPSec VPN 可以在 **NSX Edge** 实例与具有 **NSX** 或第三方供应商提供的硬件路由器/VPN 网关的远程站点之间提供点对点连接。L2 VPN 让虚拟机在跨地域界限限时不但可以维持网络连接，而且可以保持 IP 地址不变，从而让您扩展数据中心。

逻辑负载均衡器

NSX Edge 负载均衡器在配置为负载均衡池成员的多个目标之间分配指向同一虚拟 IP 地址的客户端连接。它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。这样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。

服务编排

服务编排有助于置备网络和安全服务并将其分配给虚拟基础架构中的应用程序。您可以将这些服务映射到安全组，这些服务即会通过安全策略应用到安全组中的虚拟机。

可通过数据安全查看存储在组织的虚拟化环境和云环境中的敏感数据并报告任何数据安全违规事件。

NSX 可扩展性

第三方解决方案提供商可以将其解决方案与 NSX 平台集成，从而使客户获得 VMware 产品和合作伙伴解决方案之间的集成体验。数据中心操作员可以在独立于底层网络拓扑或组件的情况下，于数秒内置备复杂的多层虚拟网络。

跨 vCenter 网络和安全概述

NSX 6.2 用于通过单一主 NSX Manager 管理多个 vCenter NSX 环境。

本章讨论了以下主题：

- 跨 vCenter NSX 的优点
- 跨 vCenter NSX 的工作方式
- 跨 vCenter NSX 中支持的 NSX Services 列表
- 通用控制器群集
- 通用传输区域
- 通用逻辑交换机
- 通用逻辑（分布式）路由器
- 通用防火墙规则
- 通用网络和安全对象
- 跨 vCenter NSX 拓扑
- 修改 NSX Manager 角色

跨 vCenter NSX 的优点

包含多个 vCenter Server 系统的 NSX 环境可以进行集中管理。

需要多个 vCenter Server 系统的原因可能有许多种，例如：

- 解决 vCenter Server 的扩展限制
- 适应需要专用或多个 vCenter Server 系统的产品（例如，Horizon View 或 Site Recovery Manager）
- 分隔各个环境，例如，按业务单位、租户、组织或环境类型

在 NSX 6.1 和更低版本中，如果部署了多个 vCenter NSX 环境，则您必须单独管理这些环境。在 NSX 6.2 中，您可以在主 NSX Manager 上创建通用对象，这些对象会在环境中的所有 vCenter Server 系统之间同步。

跨 vCenter NSX 包含以下功能：

- 增加了 NSX 逻辑网络的跨度。同一逻辑网络在整个 vCenter NSX 环境中可用，因此，位于任何 vCenter Server 系统上的任何群集中的虚拟机都可以连接到同一逻辑网络。

- 集中式安全策略管理。防火墙规则可从一个中央位置进行管理，并且应用到虚拟机，不受位置和 vCenter Server 系统影响。
- vSphere 6 中支持新的移动性边界，包括跨 vCenter 和跨多个逻辑交换机的远距离 vMotion。
- 增强了对多站点环境的支持，从城域距离到 150 毫秒 RTT。这包括主动-主动数据中心和主动-被动数据中心。

跨 vCenter NSX 环境具有许多优点：

- 集中式管理通用对象，减少了管理工作的负担。
- 提高了工作负载的移动性，虚拟机无需重新配置或更改防火墙规则即可在 vCenter Server 之间进行 vMotion 操作。
- 增强了 NSX 多站点和灾难恢复功能。

注 跨 vCenter NSX 功能仅受 vSphere 6.0 支持。

跨 vCenter NSX 的工作方式

在跨 vCenter NSX 环境中，可以拥有多个 vCenter Server，每个都必须与其自己的 NSX Manager 进行配对。一个 NSX Manager 分配为主 NSX Manager 的角色，其他 NSX Manager 分配为辅助 NSX Manager 的角色。

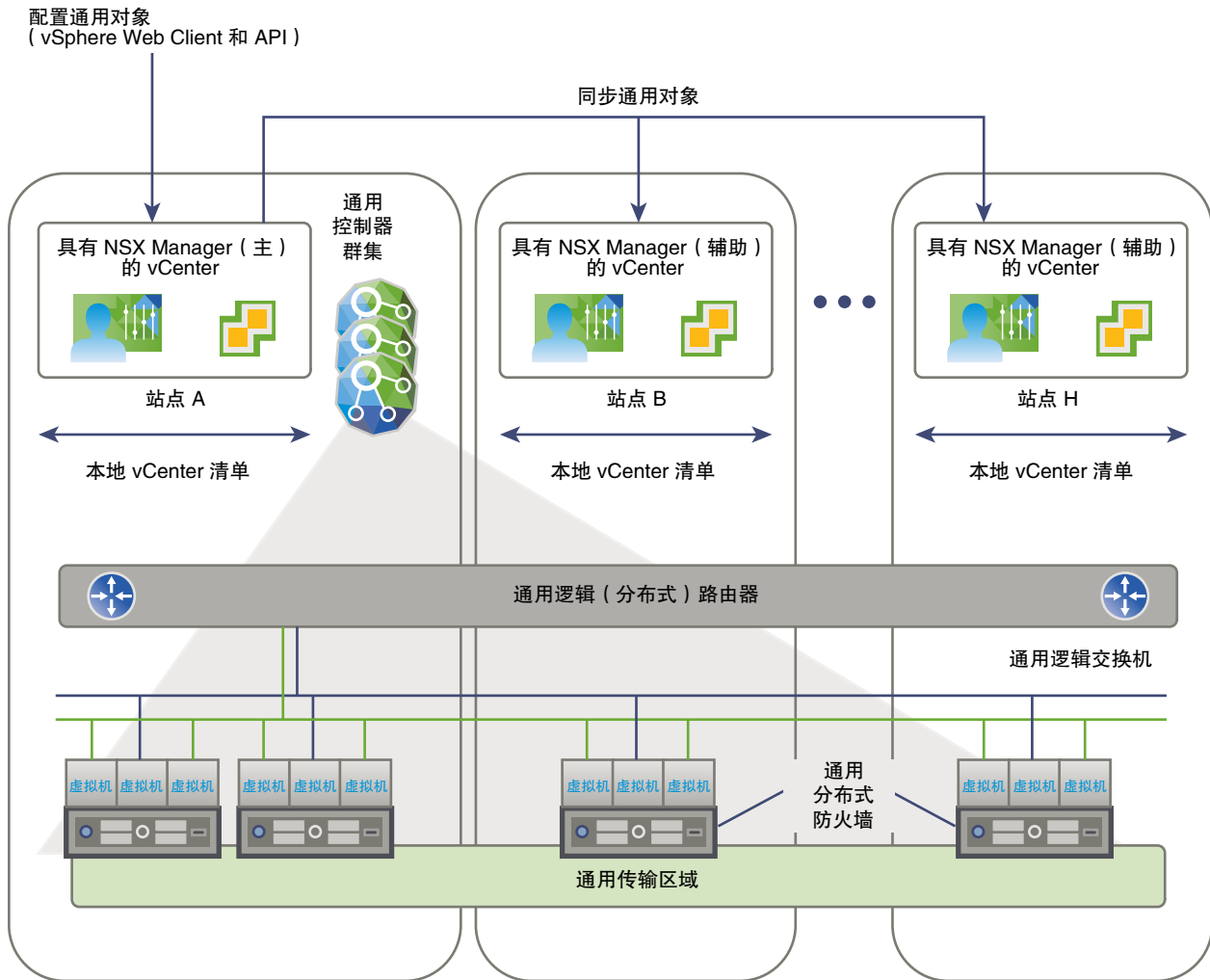
主 NSX Manager 用于部署通用控制器群集，为跨 vCenter NSX 环境提供控制层面的管理。辅助 NSX Manager 没有其自己的控制器群集。

主 NSX Manager 可以创建通用对象，如通用逻辑交换机。这些对象通过 NSX 通用同步服务同步到辅助 NSX Manager。可以从辅助 NSX Manager 中查看这些对象，但无法在其中编辑这些对象。必须使用主 NSX Manager 来管理通用对象。主 NSX Manager 可用于配置环境中的任何辅助 NSX Manager。

在主和辅助 NSX Manager 中，可以创建特定 vCenter NSX 环境的本地对象，如逻辑交换机和逻辑（分布式）路由器。这些对象仅存在于创建它们的 vCenter NSX 环境中。这些对象在跨 vCenter NSX 环境中的其他 NSX Manager 中将不可见。

可以为 NSX Manager 分配独立角色。这相当于具有一个 NSX Manager 和一个 vCenter 的 NSX 6.2 之前版本的环境。独立 NSX Manager 无法创建通用对象。

注 如果将主 NSX Manager 的角色更改为独立，则当 NSX 环境中存在任何通用对象时，将为 NSX Manager 分配转换角色。这些通用对象将保留，但您无法更改它们，也无法创建其他通用对象。您可以从转换角色中删除通用对象。转换角色仅供临时使用，例如，当更改主 NSX Manager 时。



跨 vCenter NSX 中支持的 NSX Services 列表

NSX Services 的子集适用于跨 vCenter NSX 中的通用同步。

表 4-1. 跨 vCenter NSX 中 NSX Services 的支持列表

NSX Service	详细信息	在 NSX 6.2 中是否支持跨 vCenter NSX 同步?
逻辑交换机	传输区域	是
	逻辑交换机	是
L2 网桥		否
路由	逻辑 (分布式) 路由器	是
	逻辑 (分布式) 路由器设备	在设计原理上不支持。如果每个通用逻辑路由器需要多个设备, 则必须在每个 NSX Manager 上创建这些设备。这样允许每个设备使用不同的配置, 而配置了本地输出的环境可能具有此需求。
	NSX Edge 服务网关	否

表 4-1. 跨 vCenter NSX 中 NSX Services 的支持列表（续）

NSX Service	详细信息	在 NSX 6.2 中是否支持跨 vCenter NSX 同步？
逻辑防火墙	Distributed Firewall	是
	排除列表	否
	SpoofGuard	否
	汇总流的流量监控	否
	Network Service Insertion	否
	Edge 防火墙	否
VPN		否
逻辑负载均衡器		否
其他 Edge 服务		否
服务编排		否
数据安全		否
网络可扩展性		否
网络对象和安全对象	IP 地址组（IP 集）	是
	MAC 地址组（MAC 集）	是
	IP 池	否
	安全组	是，但通用安全组只能包含已包括在内的对象，不能包含动态成员资格或已排除的对象
	服务	是
	服务组	是

通用控制器群集

每个跨 vCenter NSX 环境都有一个通用控制器群集与主 NSX Manager 关联。辅助 NSX Manager 没有控制器群集。

作为跨 vCenter NSX 环境仅有的控制器群集，通用控制器群集将维护有关通用逻辑交换机和通用逻辑路由器以及 vCenter NSX 对的本地逻辑交换机和本地逻辑路由器的信息。

为避免任何对象 ID 重叠，系统会为通用对象和本地对象维护单独的 ID 池。

通用传输区域

在跨 vCenter NSX 环境中，只能存在一个通用传输区域。

通用传输区域在主 NSX Manager 上创建，并同步到辅助 NSX Manager。需要加入通用逻辑网络的群集必须从其 NSX Manager 添加到通用传输区域中。

通用逻辑交换机

通用逻辑交换机允许第 2 层网络跨多个站点。

在通用传输区域中创建逻辑交换机时，即会创建一个通用逻辑交换机。此交换机在通用传输区域中的所有群集上可用。通用传输区域可以包括跨 vCenter NSX 环境中的所有 vCenter 中的群集。

分段 ID 池用于向逻辑交换机分配 VNI，而通用分段 ID 池用于向通用逻辑交换机分配 VNI。这些池不得重叠。

必须使用通用逻辑路由器在通用逻辑交换机之间路由。如果需要在通用逻辑交换机与逻辑交换机之间路由，则必须使用 Edge 服务网关。

通用逻辑（分布式）路由器

通用逻辑（分布式）路由器提供能够在通用逻辑路由器、群集或主机级别自定义的集中式管理和路由配置。

创建通用逻辑路由器时，必须选择是否启用本地输出，因为此设置在创建后无法更改。本地输出允许您根据标识符（即区域设置 ID）控制向 ESXi 主机提供的路由。

每个 NSX Manager 都分配有一个区域设置 ID，该 ID 默认设置为 NSX Manager 的 UUID。可以在以下级别替代区域设置 ID：

- 通用逻辑路由器
- 群集
- ESXi 主机

如果不启用本地输出，区域设置 ID 将被忽略，连接到通用逻辑路由器的所有 ESXi 主机将收到相同的路由。是否在跨 vCenter NSX 环境中启用本地输出是设计时需要考虑的一点，但并非所有跨 vCenter NSX 配置都需要使用该功能。

通用防火墙规则

通过跨 vCenter NSX 环境中的 Distributed Firewall，可以集中管理适用于您的环境中的所有 vCenter Server 的规则。Distributed Firewall 支持跨 vCenter 的 vMotion。通过执行该 vMotion 操作，可以将工作负载或虚拟机从一个 vCenter Server 移至另一个，无缝扩展了软件定义数据中心的安全性。

您的数据中心需要不断扩大，但现有 vCenter Server 可能无法扩展到同一级别。这可能需要您将一组应用程序移至不同的 vCenter Server 管理的较新的主机。或者，您可能需要将应用程序从环境中的转储服务器移至生产服务器，其中转储服务器由一个 vCenter Server 进行管理，生产服务器由不同的 vCenter Server 进行管理。Distributed Firewall 支持这些跨 vCenter 的 vMotion 方案，可以把为主 NSX Manager 定义的防火墙策略复制到多达七个辅助 NSX Manager。

在主 NSX Manager 中，您可以创建一个标记为用于通用同步的 Distributed Firewall 规则区域。您可以创建一个通用 L2 规则区域和一个通用 L3 规则区域。这些区域及其规则都同步到环境中的所有辅助 NSX Manager。其他区域中的规则保持为相应的 NSX Manager 的本地规则。

以下 Distributed Firewall 功能在跨 vCenter NSX 环境中不受支持：

- 排除列表

- SpoofGuard
- 汇总流的流量监控
- Network Service Insertion
- Edge 防火墙

服务编排不支持通用同步，因此，您无法在通用区域中使用服务编排创建 **Distributed Firewall** 规则。

通用网络和安全对象

可以创建自定义网络和安全对象，以在通用区域中的 **Distributed Firewall** 规则中使用。

- 通用 IP 集
- 通用 MAC 集
- 通用安全组
- 通用服务
- 通用服务组

只能从主 **NSX Manager** 创建通用网络和安全对象。

通用安全组只能包含通用 IP 集、通用 MAC 集以及通用安全组。成员资格仅由包含的对象定义，您不能使用动态成员资格或已排除的对象。

无法从服务编排创建通用安全组。从服务编排创建的安全组将对于该 **NSX Manager** 为本地安全组。

跨 vCenter NSX 拓扑

您可以在单个物理站点中部署跨 vCenter NSX，也可以跨多个站点进行部署。

多站点和单站点跨 vCenter NSX

通过跨 vCenter NSX 环境，您可以在多个 vCenter NSX 设置中使用同一逻辑交换机和其他网络对象。多个 vCenter 可以位于同一站点，也可以位于不同的站点。

无论跨 vCenter NSX 环境是包含于单个站点之中还是跨多个站点，您都可以使用相似配置。这两个示例拓扑包含以下内容：

- 一个通用传输区域，其中的所有群集包含于单个或多个站点。
- 附加到该通用传输区域的通用逻辑交换机。两个通用逻辑交换机用于连接虚拟机，其中一个用作路由器上行链路的转换网络。
- 添加到通用逻辑交换机的虚拟机。
- 一个带有 **NSX Edge** 设备的通用逻辑路由器，用于启用动态路由。通用逻辑路由器设备拥有虚拟机通用逻辑交换机上的内部接口，并拥有转换网络通用逻辑交换机上的上行链路接口。
- 已连接到转换网络和物理输出路由器网络的 **Edge 服务网关 (ESG)**。

图 4-1. 位于单个站点中的 跨 vCenter NSX

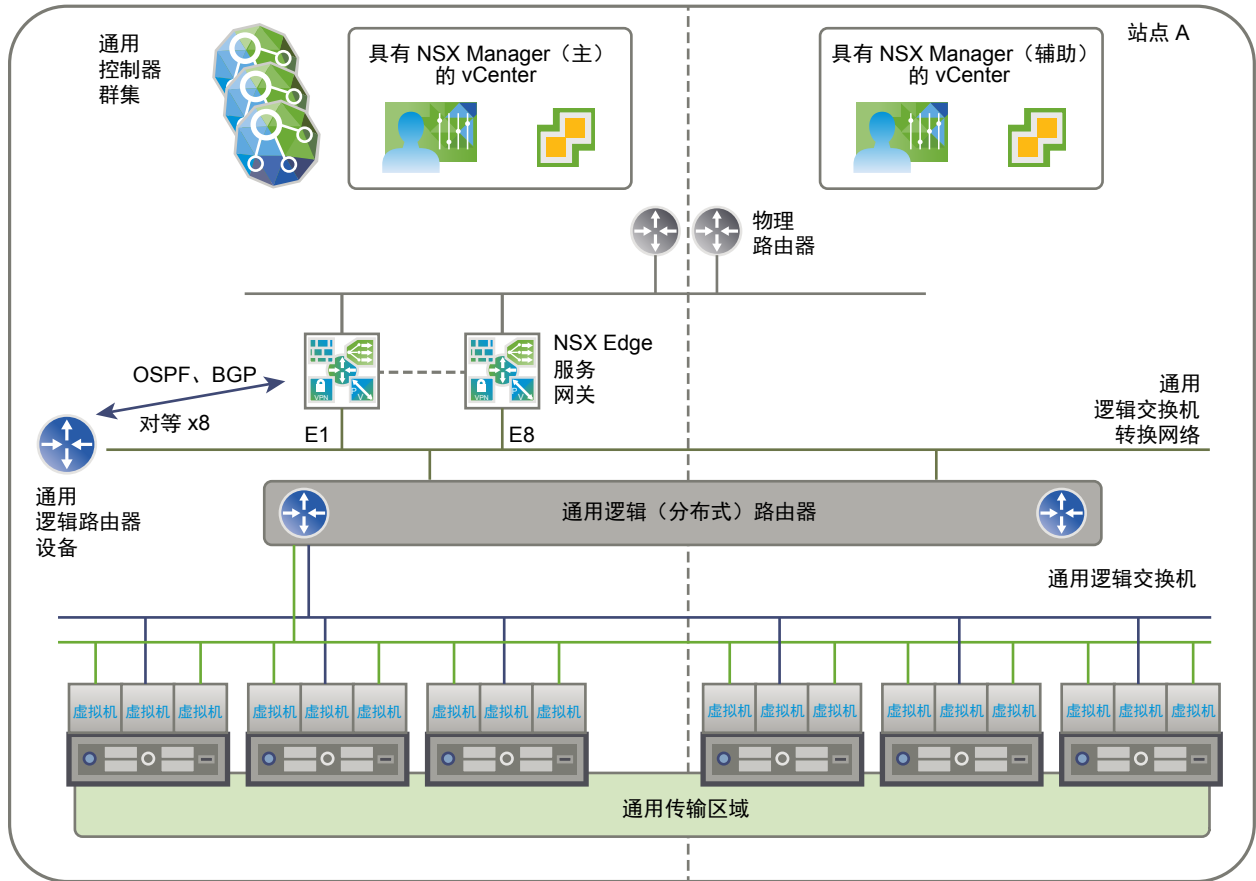
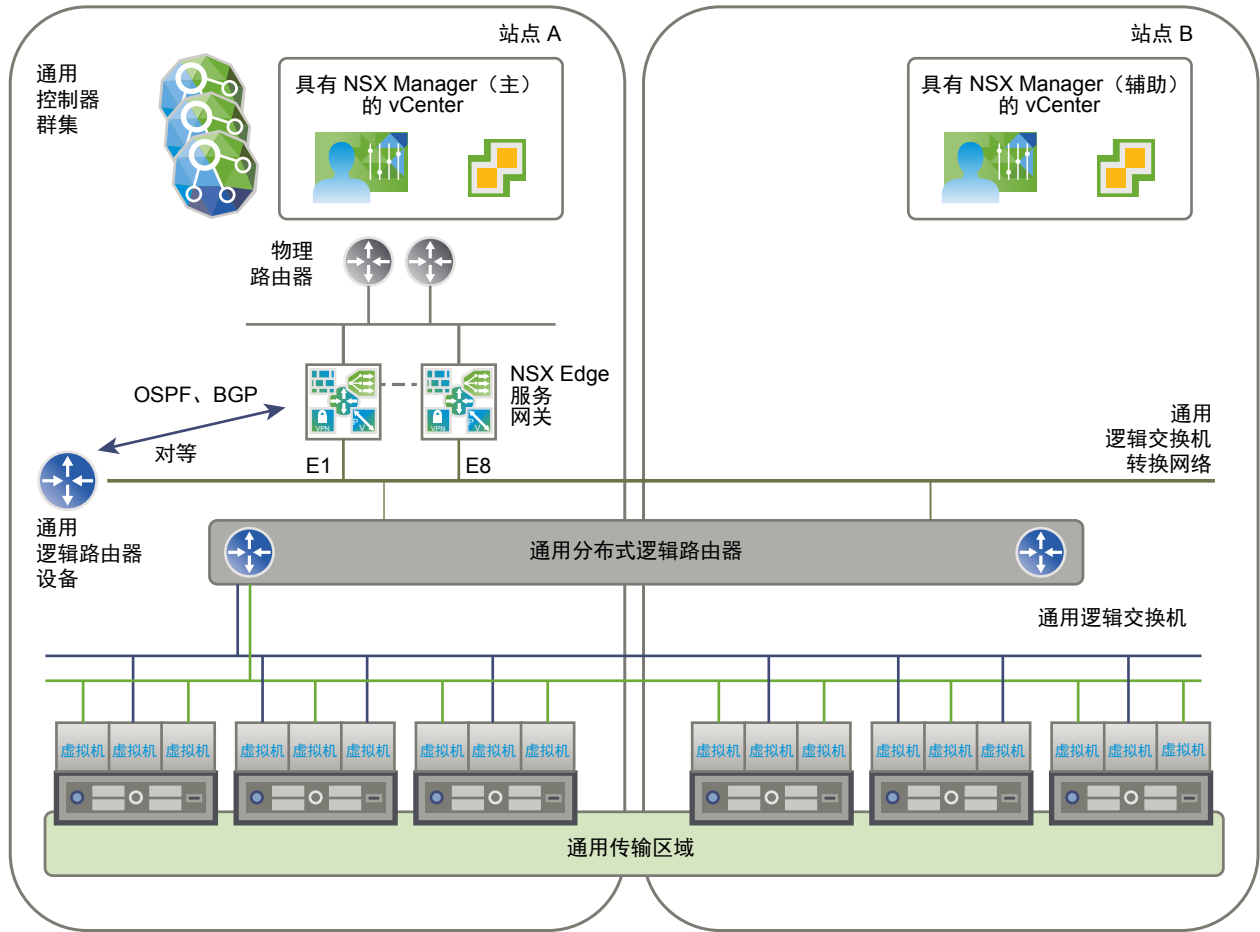


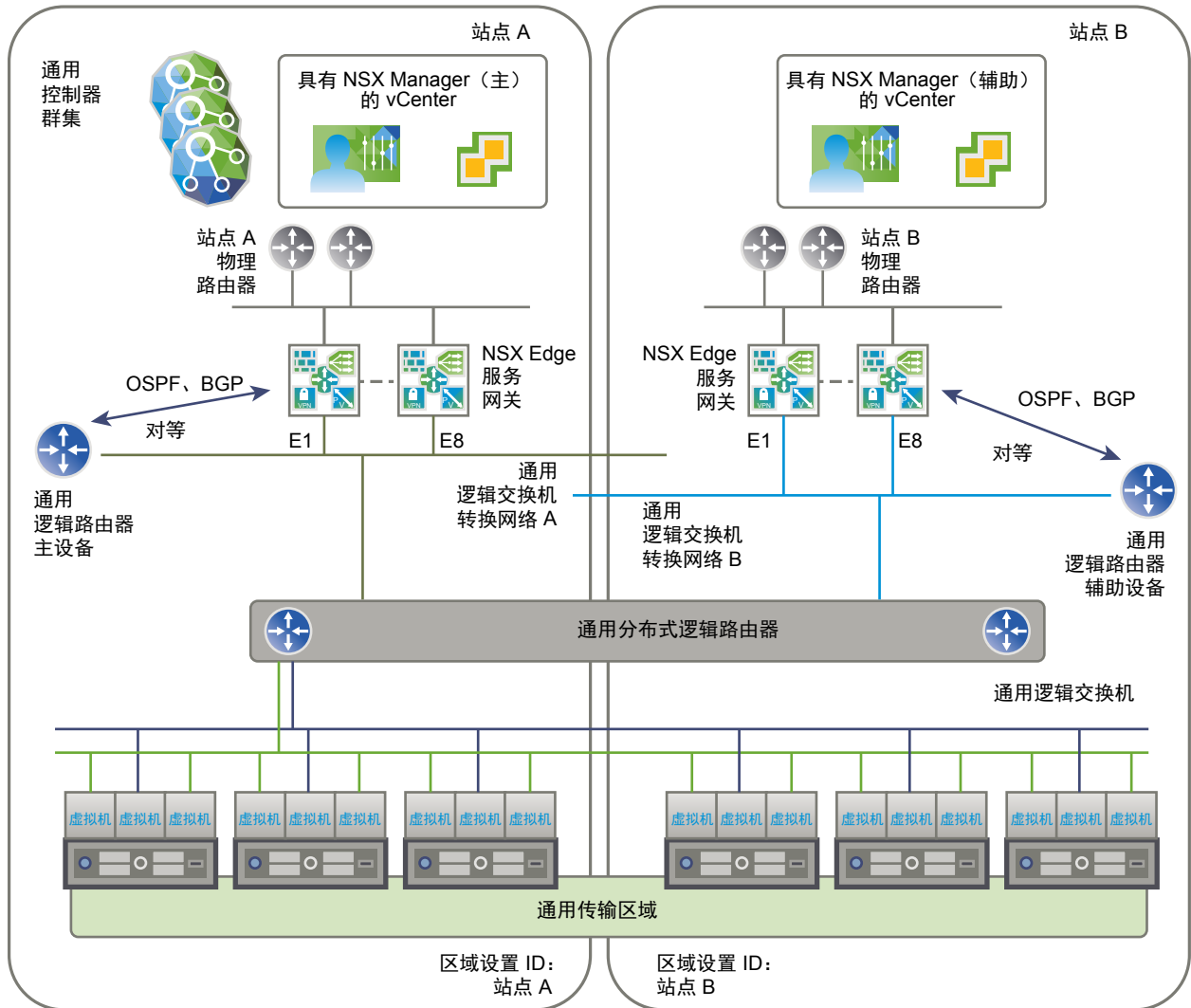
图 4-2. 跨两个站点的 跨 vCenter NSX



本地输出

多站点跨 vCenter NSX 环境中的所有站点都可以使用同一物理路由器来处理输出流量。但是，如果需要自定义输出路由，则您必须在创建通用逻辑路由器时启用本地输出功能。这样，您便可以在通用逻辑路由器级别、群集级别或主机级别自定义路由。

此多站点跨 vCenter NSX 环境示例已启用本地输出。每个站点中的 Edge 服务网关 (ESG) 都具有一个默认路由，此默认路由通过该站点的物理路由器发出流量。通用逻辑路由器配置了两个设备，每个站点各配置一个。这两个设备从其站点的 ESG 获知路由。已获知的路由会发送到通用控制器群集。由于本地输出已启用，因此该站点的区域设置 ID 与这些路由关联。通用控制器群集会将具有匹配的区域设置 ID 的路由发送给主机。从站点 A 设备获知的路由会发送给站点 A 中的主机，而从站点 B 设备获知的路由会发送给站点 B 中的主机。



修改 NSX Manager 角色

NSX Manager 可以具有主角色、辅助角色或独立角色。专用的同步软件在主 NSX Manager 上运行，并将所有通用对象同步到辅助 NSX Manager。

您必须了解更改 NSX Manager 的角色时产生的影响。

设置为主角色

此操作会将 NSX Manager 的角色设置为主角色并启动同步软件。当 NSX Manager 已具有主角色或辅助角色时，此操作将失败。

设置为独立角色（从辅助角色切换）

此操作可将 NSX Manager 的角色设置为独立或转换模式。当 NSX Manager 已具有独立角色时，此操作可能会失败。

设置为独立角色（从主角色切换）

此操作可将主 NSX Manager 重置为独立或转换模式，停止软件同步，并取消注册所有辅助 NSX Manager。当 NSX Manager 已具有独立角色或任意辅助 NSX Manager 无法访问时，此操作可能会失败。

从主角色断开连接

在辅助 NSX Manager 上运行此操作时，辅助 NSX Manager 将单方面从主 NSX Manager 断开连接。当主 NSX Manager 遇到了不可恢复的故障并且您想要将辅助 NSX Manager 注册到新的主 NSX Manager 时，应使用此操作。如果原始的主 NSX Manager 恢复正常工作，则其数据库会继续将辅助 NSX Manager 列出为已注册。要解决此问题，请在从原始的主 NSX Manager 断开或取消注册辅助 NSX Manager 时包含 **force** 选项。**force** 选项可将辅助 NSX Manager 从原始的主 NSX Manager 的数据库中移除。

传输区域

传输区域控制逻辑交换机可以延伸到的主机。它可以跨越一个或多个 **vSphere** 群集。传输区域确定了哪些群集可以参与使用特定网络，进而确定了哪些虚拟机可以参与使用该网络。在跨 **vCenter NSX** 环境中，您可以创建一个通用传输区域，该区域可以包含环境中任意 **vCenter** 的群集。您只能创建一个通用传输区域。

NSX 环境可以根据您的需要包含一个或多个传输区域。一个主机群集可以属于多个传输区域。一个逻辑交换机只能属于一个传输区域。

NSX 不允许连接位于不同传输区域的虚拟机。逻辑交换机的跨度仅限于一个传输区域，因此不同传输区域中的虚拟机不能位于同一第 2 层网络。分布式逻辑路由器无法连接到位于不同传输区域的逻辑交换机。连接第一个逻辑交换机后，只能在同一传输区域中选择其他逻辑交换机。同样，Edge 服务网关 (ESG) 只能访问一个传输区域中的逻辑交换机。

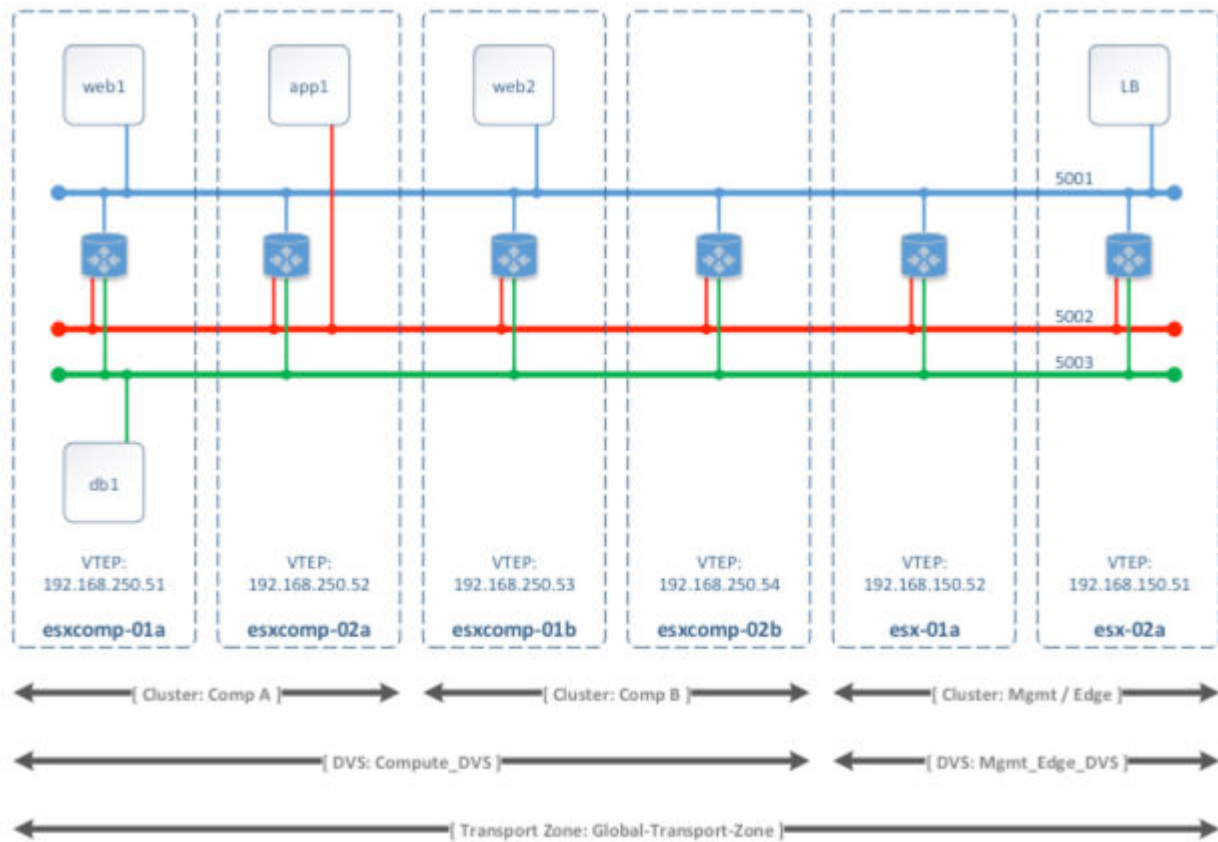
以下准则旨在帮助您设计传输区域：

NSX 不允许连接位于不同传输区域的虚拟机。逻辑交换机的跨度仅限于一个传输区域，因此不同传输区域中的虚拟机不能位于同一第 2 层网络。分布式逻辑路由器无法连接到位于不同传输区域的逻辑交换机。连接第一个逻辑交换机后，只能在同一传输区域中选择其他逻辑交换机。同样，Edge 服务网关 (ESG) 只能访问一个传输区域中的逻辑交换机。

以下准则旨在帮助您设计传输区域：

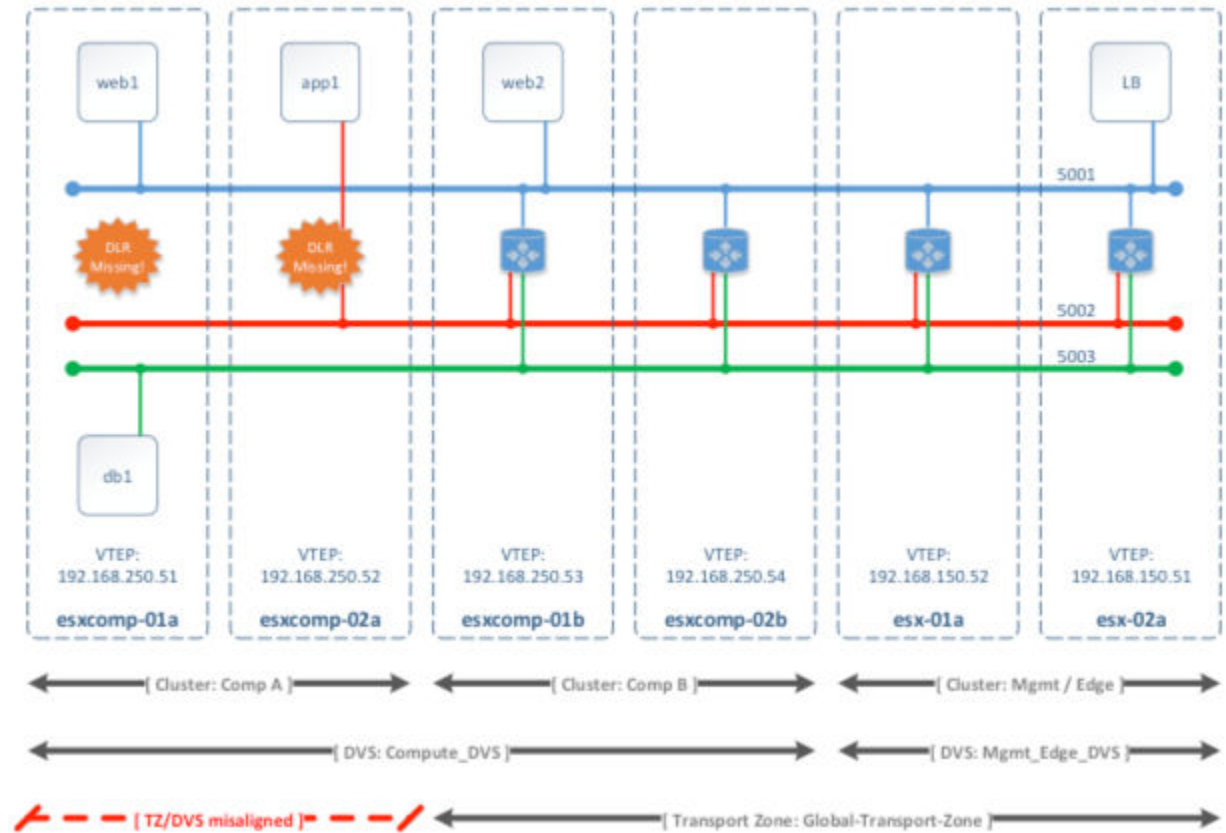
- 如果某个群集需要第 3 层连接，则该群集必须位于同时包含 Edge 群集（即，具有分布式逻辑路由器和 Edge 服务网关等第 3 层 Edge 设备的群集）的传输区域中。
- 假设您有两个群集，一个用于 Web 服务，另一个用于应用程序服务。要在这两个群集中的虚拟机之间建立 **VXLAN** 连接，这两个群集必须包含在传输区域中。
- 请记住，传输区域中所有逻辑交换机都将对传输区域中群集内的所有虚拟机可用并可见。如果某个群集包含安全环境，您可能不希望使其可用于其他群集中的虚拟机。相反，您可以将安全群集放置在更为孤立的传输区域中。
- **vSphere Distributed Switch**（**VDS** 或 **DVS**）的跨度应与传输区域跨度相匹配。在多群集 **VDS** 配置中创建传输区域时，确保选定 **VDS** 中的所有群集都包含在传输区域中。这可确保 **DLR** 在提供了 **VDS dvPortgroup** 的所有群集上都可用。

下图显示了一个与 **VDS** 边界正确对齐的传输区域。



如果您不遵循此最佳做法，请记住，如果 VDS 跨越多个主机群集，且传输区域只包含其中一个（或部分）群集，则该传输区域中包含的任何逻辑交换机都可以访问 VDS 跨越的所有群集中的虚拟机。换句话说，传输区域将无法将逻辑交换机跨度限制为部分群集。如果稍后将此逻辑交换机连接到 DLR，则必须确保仅在传输区域中包含的群集上创建路由器实例，以避免出现任何第 3 层问题。

例如，当传输区域与 VDS 边界不对应时，逻辑交换机（5001、5002 和 5003）的范围和这些逻辑交换机连接到的 DLR 实例将被拆散，从而导致群集 Comp A 中的虚拟机无法访问 DLR 逻辑接口 (LIF)。



本章讨论了以下主题：

- [添加传输区域](#)
- [查看和编辑传输区域](#)
- [扩大传输区域](#)
- [缩小传输区域](#)

添加传输区域

传输区域控制逻辑交换机可以访问的主机，且可跨越一个或多个 vSphere 群集。传输区域确定了哪些群集可以参与使用特定网络，进而确定了哪些虚拟机可以参与使用该网络。通用传输区域可跨 vCenter NSX 环境中的 vSphere 群集。

跨 vCenter NSX 环境中只能存在一个通用传输区域。

前提条件

确定要对其进行更改的相应 NSX Manager。

- 在独立或单个 vCenter NSX 环境中，仅有一个 NSX Manager，因此无需进行选择。

- 必须从主 NSX Manager 管理通用对象。
- 某个 NSX Manager 的本地对象必须使用该 NSX Manager 进行管理。
- 在未启用增强型链接模式的跨 vCenter NSX 环境中，您必须从链接至您要修改的 NSX Manager 的 vCenter 中更改配置。
- 在处于增强型链接模式的跨 vCenter NSX 环境中，您可以从任意链接的 vCenter 更改任意 NSX Manager 的配置。从 NSX Manager 下拉菜单中选择相应的 NSX Manager。

步骤

- 1 在 vCenter 中，导航到主页 > 网络和安全 > 安装 (Home > Networking & Security > Installation)，然后选择逻辑网络准备 (Logical Network Preparation) 选项卡。
- 2 单击传输区域 (Transport Zones)，然后单击新建传输区域 (New Transport Zone) (+) 图标。
- 3 (可选) 要添加通用传输区域，请选择标记此对象待进行通用同步 (Mark this object for universal synchronization)。
- 4 选择复制模式：
 - **多播 (Multicast)**：物理网络中的多播 IP 地址用于控制层面。仅在您从较旧的 VXLAN 部署升级时才推荐使用该模式。在物理网络中需要 PIM/IGMP。
 - **单播 (Unicast)**：控制层面由 NSX Controller 处理。所有单播流量都利用优化的头端复制。不需要任何多播 IP 地址或特殊的网络配置。
 - **混合 (Hybrid)**：将本地流量复制卸载到物理网络 (L2 多播)。这在第一个跃点交换机上需要 IGMP 侦听，并且需要在每个 VTEP 子网中访问 IGMP 查询器，但是不需要 PIM。第一个跃点交换机将处理该子网的流量复制。

重要 如果创建一个通用传输区域并选择混合作为复制模式，则必须确保使用的多播地址不与环境中的任何 NSX Manager 上分配的任何其他多播地址冲突。

- 5 选择要添加到传输区域的群集

Transport-Zone 是在其创建时所在的 NSX Manager 的本地传输区域。

Universal-Transport-Zone 是在跨 vCenter NSX 环境中所有 NSX Manager 上均可用的通用传输区域。

Name	Description	Control Plane Mode	Logical Switches
Transport-Zone		Unicast	1
Universal-Transport-Zone		Unicast	4

后续步骤

如果添加了传输区域，可以添加逻辑交换机。

如果添加了通用传输区域，可以添加通用逻辑交换机。

如果添加了通用传输区域，可以选择辅助 NSX Manager 并将它们的群集添加到通用传输区域。

查看和编辑传输区域

您可以查看选定传输区域中的逻辑网络、该传输区域中的群集，以及该传输区域的控制层面模式。

步骤

- 1 在“传输区域”中，双击一个传输区域。

“摘要”选项卡将显示传输区域的名称和说明，以及与其相关联的逻辑交换机数量。“传输区域详细信息”将显示传输区域中的群集。

- 2 单击**传输区域详细信息 (Transport Zone Details)**部分中的**编辑设置 (Edit Settings)**图标，编辑传输区域的名称、描述或控制层面模式。

如果您更改了传输区域的控制层面模式，请选择**将现有逻辑交换机迁移到新控制层面模式 (Migrate existing Logical Switches to the new control plane mode)**，以更改与该传输区域链接的现有逻辑交换机的控制层面模式。如果不选中此复选框，则只有在完成编辑后与该传输区域链接的逻辑交换机将具有新的控制层面模式。

- 3 单击**确定 (OK)**。


扩大传输区域

可以向传输区域中添加群集。所有现有传输区域在新添加的群集中均可用。

前提条件

您添加到传输区域的群集已安装网络基础架构，并已针对 **VXLAN** 进行了配置。请参见 **NSX 安装指南**。

步骤

- 1 在“传输区域”中，单击某个传输区域。
- 2 单击**添加群集 (Add Cluster)** () 图标。
- 3 选择要添加到该传输区域的群集，然后单击**确定 (OK)**。

缩小传输区域

可以从传输区域移除群集。现有传输区域的大小已缩减，以适应缩小后的范围。

步骤

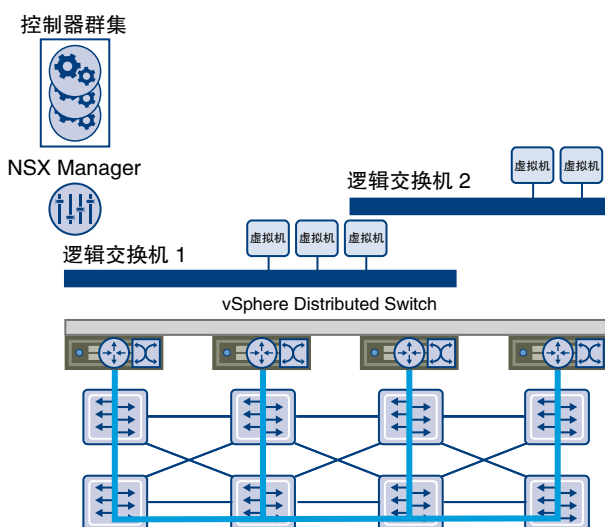
- 1 在**传输区域 (Transport Zones)**中，双击一个传输区域。
- 2 在**传输区域详细信息 (Transport Zones Details)**中，单击**移除群集 (Remove Clusters)** () 图标。
- 3 选择要移除的群集。
- 4 单击**确定 (OK)**。

逻辑交换机

云部署或虚拟数据中心具有跨多个租户的多种应用程序。出于安全和故障隔离的目的，以及为了避免重叠 IP 寻址问题，这些应用程序和租户要求互相隔离。**NSX** 逻辑交换机将创建应用程序或租户虚拟机可逻辑接线的逻辑广播域或逻辑分段。这可以在仍提供物理网络广播域 (**VLAN**) 的所有特性的同时保证部署的灵活性和速度，而不出现物理第 2 层散乱或生成树问题。

逻辑交换机是分布式的，可以跨越任意大小的计算群集。这样使得数据中心内的虚拟机移动性 (**vMotion**) 不受物理第 2 层 (**VLAN**) 边界的限制。物理基础架构无需处理 **MAC/FIB** 表限制，因为逻辑交换机的软件中包含广播域。

将逻辑交换机映射到唯一的 **VXLAN**，这封装了虚拟机流量并将通过物理 IP 网络传输。



NSX Controller 是网络内所有逻辑交换机的中央控制点，并维护所有虚拟机、主机、逻辑交换机和 **VXLAN** 的相关信息。该控制器支持两种新的逻辑交换机控制层面模式：单播和混合。这些模式可将 **NSX** 从物理网络脱离。**VXLAN** 不再要求物理网络支持多播以处理逻辑交换机中的广播、未知单播和多播 (**BUM**) 流量。单播模式会在本地复制主机上所有 **BUM** 流量，且无需任何物理网络配置。在混合模式中，一些 **BUM** 流量复制将卸载到第一个跃点物理交换机上以获得更好性能。此模式需要在第一个跃点物理交换机上打开 **IGMP** 侦听。逻辑交换机内的虚拟机可使用和发送任意类型的流量，包括 **IPv6** 和多播。

您可以通过添加 **L2** 网桥将逻辑交换机扩展到物理设备。请参见第 8 章，**L2 网桥**。

您必须具有超级管理员或企业管理员角色权限才能管理逻辑交换机。

本章讨论了以下主题：

- [添加逻辑交换机](#)
- [将虚拟机连接到逻辑交换机](#)
- [测试逻辑交换机连接](#)
- [避免逻辑交换机中出现欺骗行为](#)
- [编辑逻辑交换机](#)
- [逻辑交换机场景](#)

添加逻辑交换机

前提条件

- 具有“超级管理员”或“企业管理员”角色权限才能配置和管理逻辑交换机。
- VXLAN UDP 端口在防火墙规则中打开（如果适用）。可通过 API 配置 VXLAN UDP 端口。
- 物理架构 MTU 必须至少比虚拟机虚拟网卡的 MTU 多 50 字节。
- 在 vCenter Server 运行时设置中，为每个 vCenter Server 设置了受管 IP 地址。请参见《vCenter Server 和主机管理》。
- 如果使用 DHCP 进行 VMKNic 的 IP 分配，则可在 VXLAN 传输 VLAN 上获得 DHCP。
- 在指定的传输区域范围内，将使用一致的分布式虚拟交换机类型（供应商等等）和版本。交换机类型不一致会导致逻辑交换机出现未定义行为。
- 您已配置了相应的 LACP 成组策略，并将物理网卡连接到端口。有关成组模式的详细信息，请参阅 VMware vSphere 文档。
- 为链路聚合控制协议 (LACP) 启用了 5 元组哈希分布。
- 对于多播模式，如果 VXLAN 流量正在遍历路由器，则多播路由已启用。您已从网络管理员处获得多播地址范围。
- 端口 1234（默认控制器侦听端口）在防火墙上打开，以使 ESX 主机能够与控制器通信。
- （推荐）对于多播模式和混合模式，您已在 VXLAN 加入主机所连接的 L2 交换机上启用 IGMP 侦听。如果在 L2 上启用 IGMP 侦听，则 IGMP 查询器必须在路由器或 L3 交换机上启用，且后者已连接启用了多播的网络。

添加逻辑交换机

NSX 逻辑交换机可在完全脱离底层硬件的虚拟环境中再现交换功能（单播、多播和广播）。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。逻辑交换机是单个本地 vCenter NSX 部署。在跨 vCenter NSX 部署中，您可以创建跨所有 vCenter 的通用逻辑交换机。传输区域类型确定新交换机是逻辑交换机还是通用逻辑交换机。

前提条件

表 6-1. 创建逻辑交换机或通用逻辑交换机的必备条件

逻辑交换机	通用逻辑交换机
<ul style="list-style-type: none"> 必须配置 vSphere Distributed Switch。 必须安装 NSX Manager。 必须部署控制器。 必须为 NSX 准备主机群集。 必须配置 VXLAN。 必须配置分段 ID 池。 必须创建传输区域。 	<ul style="list-style-type: none"> 必须配置 vSphere Distributed Switch。 必须安装 NSX Manager。 必须部署控制器。 必须为 NSX 准备主机群集。 必须配置 VXLAN。 必须分配主 NSX Manager。 必须配置通用分段 ID 池。 必须创建通用传输区域。

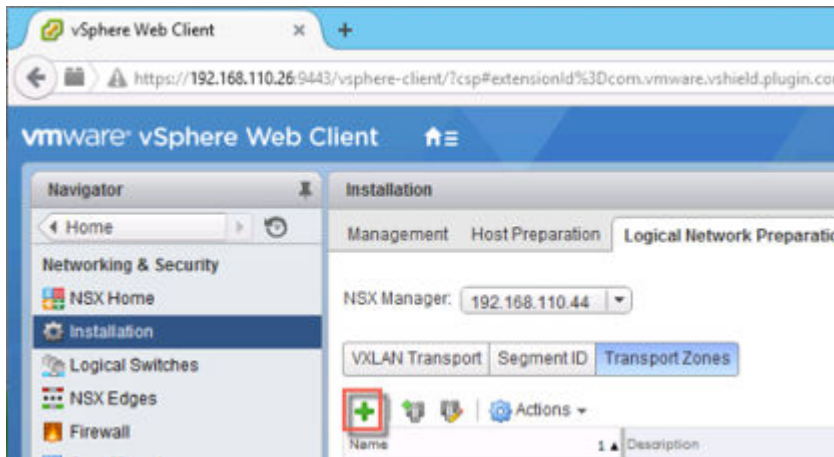
确定要对其进行更改的相应 NSX Manager。

- 在独立或单个 vCenter NSX 环境中，仅有一个 NSX Manager，因此无需进行选择。
- 必须从主 NSX Manager 管理通用对象。
- 某个 NSX Manager 的本地对象必须使用该 NSX Manager 进行管理。
- 在未启用增强型链接模式的跨 vCenter NSX 环境中，您必须从链接至您想要修改的 NSX Manager 的 vCenter 中更改配置。
- 在处于增强型链接模式的跨 vCenter NSX 环境中，您可以从任意链接的 vCenter 更改任意 NSX Manager 的配置。从 NSX Manager 下拉菜单中选择相应的 NSX Manager。

步骤

- 在 vSphere Web Client 中，导航到主页 > 网络和安全 > 逻辑交换机 (Home > Networking & Security > Logical Switches)。
- 选择要在其上创建逻辑交换机的 NSX Manager。要创建通用逻辑交换机，必须选择主 NSX Manager。
- 单击新建逻辑交换机 (New Logical Switch) (+) 图标。

例如：



4 键入逻辑交换机的名称和可选描述。

5 选择要在其中创建逻辑交换机的传输区域。选择通用传输区域将创建通用逻辑交换机。

默认情况下，逻辑交换机从传输区域继承控制层面复制模式。您可以将其更改为其他可用模式之一。可用模式包括单播、混合和多播。

如果创建一个通用逻辑交换机并选择混合作为复制模式，则必须确保使用的多播地址不与环境中的任何 NSX Manager 上分配的任何其他多播地址冲突。

6 （可选）单击**启用 IP 发现 (Enable IP Discovery)**以启用 ARP 禁止功能。

此设置可最大限度地减少各个 VXLAN 分段中（即连接到同一逻辑交换机的虚拟机之间）的 ARP 流量泛洪。默认情况下，IP 发现处于启用状态。

7 （可选）如果您的虚拟机拥有多个 MAC 地址或正在使用中继 VLAN 的虚拟网卡，请单击**启用 MAC 校准 (Enable MAC learning)**。

启用 MAC 校准会在每个虚拟网卡上构建一个 VLAN/MAC 对校准表。此表会作为 dvfilter 数据的一部分进行保存。在进行 vMotion 的过程中，dvfilter 会在新位置保存并存储该表。然后，交换机会针对表中的所有 VLAN/MAC 条目发出 RARP。





此示例显示了具有默认设置的应用程序逻辑交换机。

The screenshot shows the 'New Logical Switch' configuration window. The 'Name' field is set to 'app'. The 'Description' field is empty. The 'Transport Zone' is set to 'tz1'. Under 'Replication mode', 'Unicast' is selected, with a note 'VXLAN control plane handled by NSX Controller Cluster.' Below this, there are two checkboxes: 'Enable IP Discovery' (checked) and 'Enable MAC Learning' (unchecked). At the bottom right, there are 'OK' and 'Cancel' buttons.

DB-Tier-00 是连接到传输区域的逻辑交换机。它仅在创建时所在的 NSX Manager 上可用。

DB-Tier-01 是连接到通用传输区域的通用逻辑交换机。它可在跨 vCenter NSX 环境中的任何一个 NSX Manager 上使用。

逻辑交换机和通用逻辑交换机的分段 ID 来自于不同的分段 ID 池。

 DB-Tier-00	 Normal	 Transport-Zone	10000	Unicast
 DB-Tier-01	 Normal	 Universal-Transport-Zone	900003	Unicast

后续步骤

将虚拟机添加到逻辑交换机或通用逻辑交换机。

创建一个逻辑路由器并将其连接到逻辑交换机，以启用连接到不同逻辑交换机的虚拟机之间的连接。

创建一个通用逻辑路由器并将其连接到通用逻辑交换机，以启用连接到不同通用逻辑交换机的虚拟机之间的连接。

将逻辑交换机连接到 NSX Edge

如果将逻辑交换机与 NSX Edge 服务网关或 NSX Edge 逻辑路由器连接，则可提供东西向流量路由（在逻辑交换机之间）或南北向流量路由（通向外部环境），或用于提供高级服务。

步骤

- 1 在逻辑交换机中，选择要连接 NSX Edge 的逻辑交换机。
- 2 单击 **连接 Edge (Connect an Edge)** () 图标。
- 3 选择要与逻辑交换机连接的 NSX Edge，然后单击 **下一步 (Next)**。
- 4 选择要连接到逻辑交换机的接口，然后单击 **下一步 (Next)**。
逻辑网络通常连接到内部接口。
- 5 在“编辑 NSX Edge 接口”页面上，键入 NSX Edge 接口的名称。
- 6 单击 **内部 (Internal)** 或 **上行链路 (Uplink)** 以指示是内部接口还是上行链路接口。
- 7 选择接口的连接状态。
- 8 如果要连接逻辑交换机的 NSX Edge 选择了 **手动 HA 配置 (Manual HA Configuration)**，请指定 CIDR 格式的两个管理 IP 地址。
- 9 根据需要编辑默认 MTU。
- 10 单击 **下一步 (Next)**。
- 11 查看 NSX Edge 连接详细信息，然后单击 **完成 (Finish)**。

在逻辑交换机上部署服务

您可以在逻辑交换机上部署第三方服务。

前提条件

您的基础架构中必须已安装一个或多个第三方虚拟设备。


步骤

- 1 在**逻辑交换机 (Logical Switches)**中，选择要部署服务的逻辑交换机。
- 2 单击**添加服务配置文件 (Add Service Profile)** () 图标。
- 3 选择要应用的服务和服务配置文件。
- 4 单击**确定 (OK)**。

将虚拟机连接到逻辑交换机

您可以将虚拟机连接到逻辑交换机或通用逻辑交换机。

步骤

- 1 在**逻辑交换机 (Logical Switches)**中，选择要将虚拟机添加到的逻辑交换机。
- 2 单击**添加虚拟机 (Add Virtual Machine)** () 图标。
- 3 选择要向其添加逻辑交换机的虚拟机。
- 4 选择要连接的虚拟网卡。
- 5 单击**下一步 (Next)**。
- 6 检查选定的虚拟网卡。
- 7 单击**完成 (Finish)**。

测试逻辑交换机连接

ping 测试用于检查位于一个 VXLAN 传输网络中的两台主机是否可以相互访问。

- 1 在**逻辑交换机 (Logical Switches)**中，双击**名称 (Name)**列中要测试的逻辑交换机。
- 2 单击**监控 (Monitor)**选项卡。
- 3 单击**主机 (Hosts)**选项卡。
- 4 在“源主机”区域中，单击**浏览 (Browse)**。在“选择主机”对话框中，选择目标主机。
- 5 选择测试数据包的大小。

VXLAN 标准大小为 1550 个字节（无碎片，应与物理基础架构 MTU 匹配）。在这一大小设置下，NSX 可以检查连接并验证基础架构是否已为传输 VXLAN 流量做好准备。

最小数据包大小允许存在碎片。因此，在最小数据包大小设置下，NSX 只能检查连接，但不能检查基础架构是否已为更大的帧做好准备。

- 6 在“目标主机”区域中，单击**浏览 (Browse)**。在“选择主机”对话框中，选择目标主机。
- 7 单击**开始测试 (Start Test)**。

此时将显示主机对主机的 ping 测试结果。

避免逻辑交换机中出现欺骗行为

与 vCenter Server 同步后，NSX Manager 会从每个虚拟机上的 VMware Tools 中收集所有 vCenter 客户机虚拟机的 IP 地址，或通过 IP 发现（如果已启用）进行收集。NSX 并不信任 VMware Tools 或 IP 发现所提供的 IP 地址。如果虚拟机被攻击，则 IP 地址可能被假冒，恶意传输信息可能会绕过防火墙策略。

使用 SpoofGuard，您可以授权 VMware Tools 或 IP 发现所报告的 IP 地址，并可以根据需要更改这些地址以防止欺骗。SpoofGuard 本身还信任从 VMX 文件和 vSphere SDK 收集的虚拟机的 MAC 地址。可以在防火墙规则之外使用 SpoofGuard 阻止已确认为虚假的通信。

有关详细信息，请参见第 13 章，使用 SpoofGuard。

编辑逻辑交换机

可以编辑逻辑交换机的名称、描述和控制层面模式。

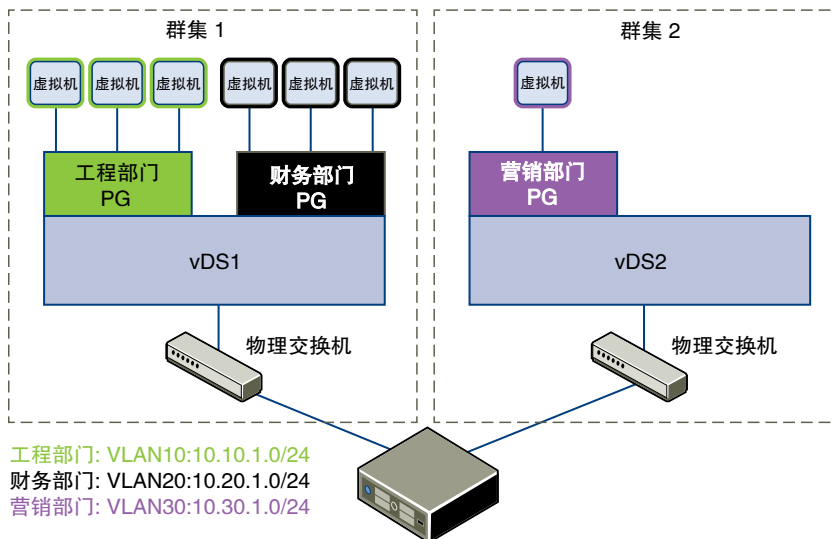
步骤

- 1 在**逻辑交换机 (Logical Switches)**中，选择要编辑的逻辑交换机。
- 2 单击**编辑 (Edit)**图标。
- 3 进行所需更改。
- 4 单击**确定 (OK)**。

逻辑交换机场景

此场景的情形如下：公司 ACME Enterprise 在数据中心 (ACME_Datacenter) 的两个群集上有多个 ESX 主机。工程部门（位于端口组 PG-Engineering 上）和财务部门（位于端口组 PG-Finance 上）都在 Cluster1 上。营销部门 (PG-Marketing) 在 Cluster2 上。两个群集都由单个 vCenter Server 5.5 管理。

图 6-1. 实施逻辑交换机前的 ACME Enterprise 网络

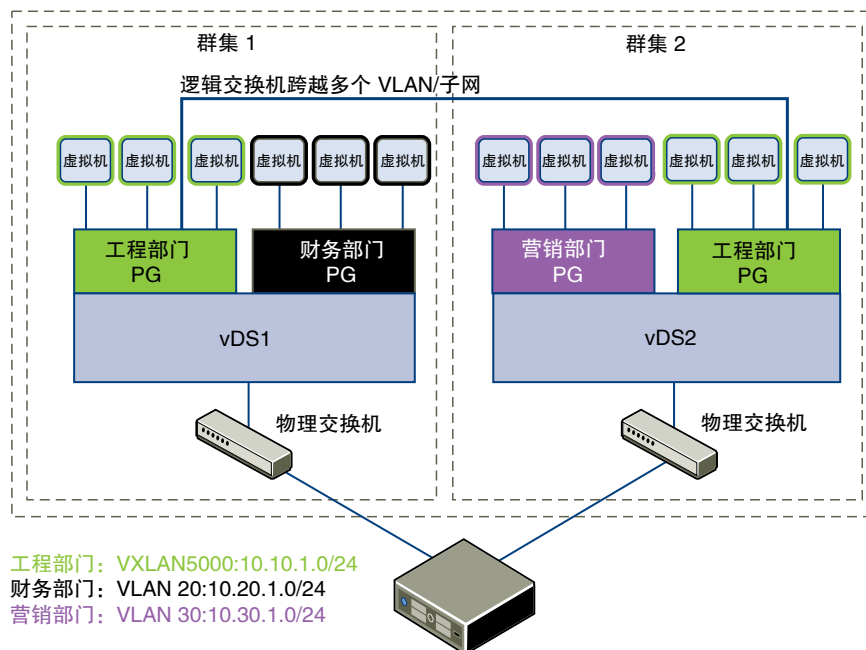


Cluster1 上的 ACME 计算空间不足，而 Cluster2 未充分利用。ACME 网络管理员要求 John 管理员（ACME 的虚拟化管理员）找出能够将工程部门扩展到 Cluster2 的方法，通过这种方法使同属于工程部门的虚拟机位于两个群集中，并且能够彼此通信。这将通过延伸 ACME 的 L2 层使 ACME 能够利用两个群集的计算容量。

如果 John 管理员使用传统方法解决此问题，他需要以特殊方式连接单独的 VLAN 以便使两个群集处于同一 L2 域中。这可能需要 ACME 购买新的物理设备以分离流量，并可能导致诸如 VLAN 散乱、网络循环以及系统和管理开销等问题。

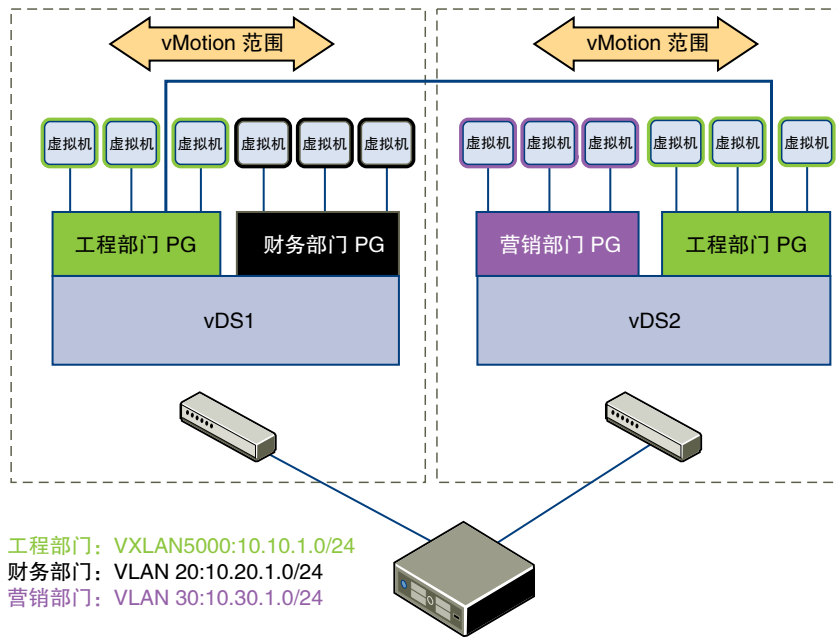
管理员 John 记得在 VMworld 上看过逻辑网络演示，决定评估 NSX。他认为通过构建跨 dvSwitch1 和 dvSwitch2 的逻辑交换机可以延伸 ACME 的 L2 层。由于可利用 NSX Controller，John 无需改变 ACME 的物理基础架构，因为 NSX 是在现有 IP 网络上运行。

图 6-2. ACME Enterprise 实施了逻辑交换机



管理员 John 构建了跨两个群集的逻辑交换机后，他可以使用 vMotion 在 VDS 内迁移虚拟机。

图 6-3. 逻辑网络上的 vMotion



我们来逐步了解一下管理员 John 在 ACME Enterprise 上构建逻辑网络的步骤。

管理员 John 为 NSX Manager 分配分段 ID 池和多播地址范围

管理员 John 必须指定接收到的分段 ID 池来隔离 ABC 公司的网络流量。

前提条件

- 1 管理员 John 验证 dvSwitch1 和 dvSwitch2 是否为 VMware Distributed Switch 版本 5.5。
- 2 John 管理员为 vCenter Server 设置受管 IP 地址。
 - a 选择**系统管理 (Administration) > vCenter Server 设置 (vCenter Server Settings) > 运行时设置 (Runtime Settings)**。
 - b 在 vCenter Server Managed IP 中，键入 **10.115.198.165**。
 - c 单击**确定 (OK)**。
- 3 管理员 John 在 Cluster1 和 Cluster2 上安装网络虚拟化组件。请参见 NSX 安装指南。
- 4 管理员 John 从 ACME 的 NSX Manager 管理员处获得分段 ID 池 (5000 - 5250)。由于利用了 NSX Controller，因此物理网络中不需要多播。
- 5 管理员 John 创建 IP 池，以便将该 IP 池中的静态 IP 地址分配给 VXLAN VTEP。请参见[添加 IP 池](#)。

步骤

- 1 在 vSphere Web Client 中，单击**网络和安全 (Networking & Security) > 安装 (Installation)**。
- 2 单击**逻辑网络准备 (Logical Network Preparation)**选项卡，然后单击**分段 ID (Segment ID)**。
- 3 单击**编辑 (Edit)**。

- 4 在“分段 ID 池”中，键入 **5000 – 5250**。
- 5 不要选择启用多播寻址 (**Enable multicast addressing**)。
- 6 单击**确定 (OK)**。

管理员 John 配置 VXLAN 传输参数

管理员 John 在 Cluster 1 和 Cluster 2 上配置 VXLAN，并将每个群集映射到一个 vDS。将群集映射到交换机时，将为逻辑交换机启用该群集中的每个主机。

步骤

- 1 单击**主机准备 (Host Preparation)**选项卡。
- 2 对于 Cluster 1，请在“VXLAN”列中选择**配置 (Configure)**。
- 3 在“配置 VXLAN 网络”对话框中，选择“dvSwitch1”作为群集的虚拟分布式交换机。
- 4 为 dvSwitch1 键入 **10** 以用作 ACME 传输 VLAN。
- 5 在“指定传输属性”中，将 **1600** 作为 dvSwitch1 的最大传输单元 (MTU)。
MTU 是在一个数据包分为更小的数据包之前可在其中传输的最大数据量。John 管理员知道 VXLAN 逻辑交换机流量帧由于封装原因在大小上稍微大些，因此每个交换机的 MTU 必须设置为 **1550** 或更大值。
- 6 在 **VMKNic IP 寻址 (VMKNic IP Addressing)** 中，选择**使用 IP 池 (Use IP Pool)**，然后选择一个 IP 池。
- 7 对于 **VMKNic 成组策略 (VMKNic Teaming Policy)**，请选择**故障切换 (Failover)**。
John 管理员希望通过保持逻辑交换机在正常和故障情况下的性能相同，来保持其网络中的服务质量。因此，选择“故障切换”作为成组策略。
- 8 单击**添加 (Add)**。
- 9 重复第 4 步到第 8 步，在 Cluster2 上配置 VXLAN。

管理员 John 将 Cluster1 和 Cluster2 映射到相应的交换机后，为逻辑交换机准备这些群集中的主机：

- 1 将 VXLAN 内核模块和 vmknics 添加到 Cluster 1 和 Cluster 2 中的每个主机。
- 2 将在与逻辑交换机关联的 vSwitch 上创建特定的 dvPortGroup，并将其与 VMKNic 相连接。

管理员 John 添加传输区域

用于支持逻辑网络的物理网络称为 transport zone。传输区域是虚拟化网络所跨越的计算直径。

步骤

- 1 单击**逻辑网络准备 (Logical Network Preparation)**，然后单击**传输区域 (Transport Zones)**。
- 2 单击**新建传输区域 (New Transport Zone)**图标。
- 3 在“名称”中，键入 **ACME Zone**。
- 4 在“描述”中，键入 **Zone containing ACME's clusters**。

- 5 选择要添加到传输区域的 **Cluster 1** 和 **Cluster 2**。
- 6 在**控制层面模式 (Control Plane Mode)**中，选择**单播 (Unicast)**。
- 7 单击**确定 (OK)**。

管理员 John 创建逻辑交换机

管理员 John 在配置 VXLAN 传输参数后，开始创建逻辑交换机。

步骤

- 1 单击**逻辑交换机 (Logical Switches)**，然后单击**新建逻辑交换机 (New Logical Network)**图标。
- 2 在“名称”中，键入 **ACME logical network**。
- 3 在“描述”中，键入
Logical Network for extending ACME Engineering network to Cluster2。
- 4 在**传输区域 (Transport Zone)**中，选择“ACME 区域”。
- 5 单击**确定 (OK)**。

NSX 将创建逻辑交换机，从而在 dvSwitch1 和 dvSwitch2 之间建立 L2 连接。

后续步骤

管理员 John 现在可将 ACME 生产虚拟机连接到逻辑交换机，并将逻辑交换机连接到 NSX Edge 服务网关或逻辑路由器。

配置硬件网关

硬件网关配置将物理网络映射到虚拟网络。映射配置允许 NSX 利用 Open vSwitch 数据库 (Open vSwitch Database, OVSDb)。

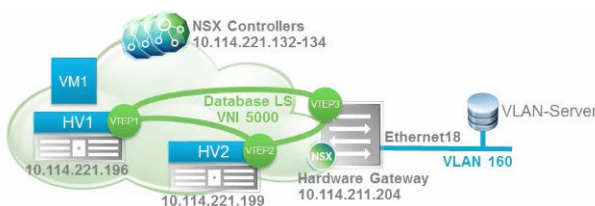
OVSDb 数据库包含有关物理硬件和虚拟网络的信息。供应商硬件承载数据库服务器。

NSX 逻辑网络中的硬件网关交换机终止 VXLAN 隧道。对于虚拟网络，硬件网关交换机称为硬件 VTEP。有关 VTEP 的详细信息，请参见《NSX 安装指南》和《NSX 网络虚拟化设计指南》。

具有硬件网关的最小拓扑包含以下组件：

- 物理服务器
- 硬件网关交换机（L2 端口）
- IP 网络
- 最少四个管理程序，包括两个具有虚拟机的复制群集
- 具有至少三个节点的控制器群集

具有硬件网关的示例拓扑将 HV1 和 HV2 显示为两个管理程序。VM1 虚拟机位于 HV1 上。VTEP1 位于 HV1 上，VTEP2 位于 HV2 上，VTEP3 位于硬件网关上。与位于同一子网 221 的两个管理程序相比，硬件网关位于不同的子网 211。



硬件网关底层配置可能包含以下组件之一：

- 单个交换机
- 具有不同 IP 地址的多个物理总线交换机
- 具有多个交换机的硬件交换机控制器

NSX Controller 使用其 IP 地址在端口 6640 上与硬件网关进行通信。该连接用于与硬件网关之间发送和接收 OVSDb 事务。

场景：硬件网关示例配置

该场景描述了用于为 NSX 部署配置硬件网关交换机的典型任务。任务顺序显示如何将虚拟机 VM1 连接到物理服务器，以及如何使用硬件网关将 WebService 逻辑交换机连接到 VLAN 服务器 VLAN 160。

示例拓扑显示虚拟机 VM1 和 VLAN 服务器在子网 10 中配置了一个 IP 地址。VM1 连接到 WebService 逻辑交换机。VLAN 服务器连接到物理服务器上的 VLAN 160。



前提条件

- 阅读供应商文档以了解如何满足物理网络要求。
- 确认满足硬件网关配置的 NSX 系统和硬件要求。请参见第 1 章，NSX 的系统要求。
- 确认正确设置了逻辑网络。请参见《NSX 安装指南》。
- 确认 VXLAN 中的传输参数映射准确无误。请参见《NSX 安装指南》。
- 检索硬件网关的供应商证书。
- 确认 VXLAN 端口值设置为 4789。请参见《NSX 升级指南》。

您可以使用 REST API 命令 `PUT /2.0/vdn/config/vxlan/udp/port/4789` 修改端口号。该 API 不返回任何响应。

步骤

1 设置复制群集

复制群集是一组管理程序，负责转发从硬件网关中发送的广播流量。广播流量可能是未知的单播和多播流量。

2 将硬件网关连接到 NSX Controller

您必须在 ToR 物理交换机上配置 OVSDB 管理器表以将硬件网关连接到 NSX Controller。

3 添加硬件网关证书

必须将硬件网关证书添加到硬件设备中，配置才能正常工作。

4 将逻辑交换机绑定到物理交换机

连接到虚拟机 VM1 的 WebService 逻辑交换机必须与同一子网上的硬件网关进行通信。

设置复制群集

复制群集是一组管理程序，负责转发从硬件网关中发送的广播流量。广播流量可能是未知的单播和多播流量。

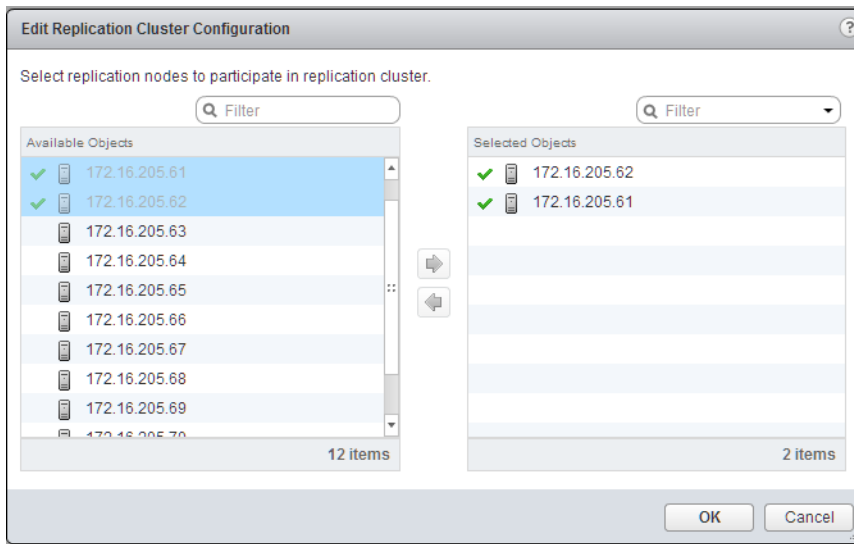
注 复制节点和硬件网关交换机不能位于相同的 IP 子网上。

前提条件

确认您具有管理程序以作为有效复制节点。

步骤

- 1 登录到 vSphere Web Client。
- 2 选择**网络和安全** > **服务定义**。
- 3 单击**硬件设备**选项卡。
- 4 在“复制群集”部分中单击**编辑**，以选择管理程序以作为该复制群集中的复制节点。
- 5 选择管理程序，然后单击蓝色箭头。



选定的管理程序将移到“选定对象”列中。

- 6 单击**确定**。

复制节点将添加到复制群集中。复制群集中必须至少具有一个主机。

将硬件网关连接到 NSX Controller

您必须在 ToR 物理交换机上配置 OVSDB 管理器表以将硬件网关连接到 NSX Controller。

Controller 被动侦听来自 ToR 的连接尝试。因此，硬件网关必须使用 OVSDB 管理器表启动连接。

步骤

- 1 请使用适用于您的环境的命令将硬件网关连接到 NSX Controller。

连接硬件网关和 NSX Controller 的示例命令。

```
prmh-nsx-tor-7050sx-3#enable
prmh-nsx-tor-7050sx-3#configure terminal
prmh-nsx-tor-7050sx-3(config)#cvx
prmh-nsx-tor-7050sx-3(config-cvx)#service hsc
prmh-nsx-tor-7050sx-3(config-cvx-hsc)#manager 172.16.2.95 6640
prmh-nsx-tor-7050sx-3(config-cvx-hsc)#no shutdown
prmh-nsx-tor-7050sx-3(config-cvx-hsc)#end
```

- 2 在硬件网关上设置 OVSDB 管理器表。
- 3 将 OVSDB 端口号值设置为 6640。
- 4 （可选）验证硬件网关是否通过 OVSDB 通道连接到 NSX Controller。
 - 检查连接状态是否为已连接。
 - ping VM1 和 VLAN 160 以验证连接是否成功。
- 5 （可选）验证硬件网关是否连接到正确的 NSX Controller。
 - a 登录到 vSphere Web Client。
 - b 选择**网络和安全 > > 安装 > NSX Controller** 节点。

添加硬件网关证书

必须将硬件网关证书添加到硬件设备中，配置才能正常工作。

前提条件

确认您的环境中的硬件网关证书可用。

步骤

- 1 登录到 vSphere Web Client。
- 2 选择**网络和安全 (Networking & Security) > 服务定义 (Service Definitions)**。
- 3 单击**硬件设备 (Hardware Devices)**选项卡。

- 4 单击“添加” (+) 图标以创建硬件网关配置文件详细信息。

Add Hardware Device

Name: *

hardware_registration

Description:

Certificate: *

-----BEGIN CERTIFICATE REQUEST-----
MIICujCCAaICAQAwTElMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbmGmb3JuaWEx
EjAQBgNVBAcTCVBhbG8gQWw0bzESMBAGA1U
ECxMJVGVjaCBQdWJzMRQwEgYDVQQK
EwtWtXdhcmUgSW5jLjETMBEGA1UEAxMKdm1
3YXJlLnNvbTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQcCggEBAIZaGpix6LIF
f8DMKpeU4TG39K2OY1P3OWOqX3ev
wLYkS6WwMRN7TpnA1/OR28HKYICXZHggQz

☒ Enable BFD

OK

Cancel

选项	说明
名称和说明	指定硬件网关名称。 您可以在描述部分中添加配置文件详细信息。
证书	粘贴从您的环境中提取的证书。
启用 BFD	默认情况下，将启用双向转发检测 (directional Forwarding Detection, BFD) 协议。 该协议用于同步硬件网关配置信息。

- 5 单击**确定 (OK)**。
- 将创建一个表示硬件网关的配置文件。
- 6 刷新屏幕以验证硬件网关是否可用并且正在运行。
- 连接应处于“已连接”状态。
- 7 （可选）单击硬件网关配置文件，然后右键单击以从下拉菜单中选择**查看 BFD 隧道状态 (View the BFD Tunnel Status)**。

torgateway-8 - Hardware Gateway BFD Tunnel Status

Diagnostic	Enabled	Error Message	Forwarding	Information	Local VTEP
	✓		✗		50.40.1.1
	✓		✗		50.40.1.1

Tunnel State Details

Remote Diagnostic	
Remote State	UP
Remote VTEP IP	172.16.205.84
Tunnel State	UP

OK

Cancel

该对话框将显示诊断隧道状态详细信息以进行故障排除。

将逻辑交换机绑定到物理交换机

连接到虚拟机 VM1 的 WebService 逻辑交换机必须与同一子网上的硬件网关进行通信。

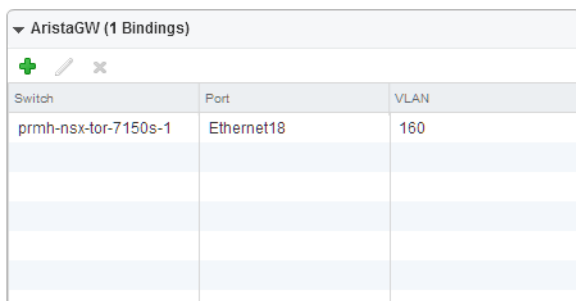
注 如果将多个逻辑交换机绑定到硬件端口，您必须为每个逻辑交换机应用这些步骤。

前提条件

- 确认 WebService 逻辑交换机可用。请参见[添加逻辑交换机](#)。
- 确认物理交换机可用。

步骤

- 1 登录到 vSphere Web Client。
- 2 选择**网络和安全 (Networking & Security) > 逻辑交换机 (Logical Switches)**。
- 3 找到 WebService 逻辑交换机，然后右键单击以从下拉菜单中选择**管理硬件绑定 (Manage Hardware Bindings)**。
- 4 选择硬件网关配置文件。
- 5 单击“添加” (+) 图标，然后从下拉菜单中选择物理交换机。
例如，AristaGW。
- 6 单击**选择 (Select)**以从“可用对象”列表选择一个物理端口。
例如，Ethernet 18。
- 7 单击**确定 (OK)**。
- 8 指定 VLAN 名称。



Switch	Port	VLAN
prmh-nsx-tor-7150s-1	Ethernet18	160

例如，160。

- 9 单击**确定 (OK)**。

将完成绑定。

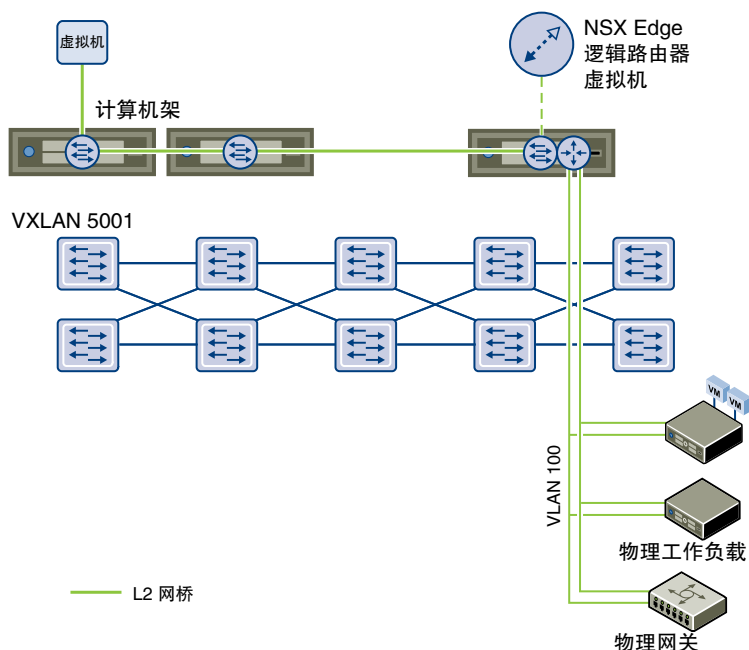
NSX Controller 将物理和逻辑配置信息与硬件网关进行同步。

L2 网桥

可以在逻辑交换机和 VLAN 之间创建 L2 网桥，从而将虚拟工作负载迁移到物理设备而不会对 IP 地址产生任何影响。通过将逻辑交换机广播域桥接到 VLAN 广播域，逻辑网络可以利用物理 L3 网关并访问现有物理网络和安全资源。

L2 网桥在具有 NSX Edge 逻辑路由器虚拟机的主机上运行。一个 L2 网桥实例映射到一个 VLAN，但可以有多个网桥实例。逻辑路由器无法用作连接到网桥的设备的网关。

如果在逻辑路由器上启用 High Availability 的情况下主 NSX Edge 虚拟机出现故障，则网桥将自动移到具有辅助虚拟机的主机。要进行此无缝迁移，必须在具有辅助 NSX Edge 虚拟机的主机上配置 VLAN。



请注意，不应使用 L2 网桥将逻辑交换机连接到其他逻辑交换机、将 VLAN 网络连接到其他 VLAN 网络或互连数据中心。此外，无法使用通用逻辑路由器配置桥接，也无法向通用逻辑交换机添加网桥。

本章讨论了以下主题：

- 添加 L2 网桥
- 向逻辑路由环境添加 L2 网桥

添加 L2 网桥

可以添加从逻辑交换机到分布式虚拟端口组的网桥。

前提条件

必须在您的环境中部署了 NSX 逻辑路由器。

不能使用通用逻辑路由器配置桥接，且不能将网桥添加到通用逻辑交换机。

步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击逻辑路由器。
- 4 单击**管理**，然后单击**桥接**。
- 5 单击**添加 (+)** 图标。
- 6 键入网桥的名称。
- 7 选择要为其创建网桥的逻辑交换机。
- 8 选择逻辑交换机所要桥接的分布式虚拟端口组。
- 9 单击**确定**。

向逻辑路由环境添加 L2 网桥

一个逻辑路由器可以具有多个桥接实例，但路由实例和桥接实例不能共享同一 vxlan/vlan 网络。流入和流出桥接 vlan 和桥接 vxlan 的流量无法路由至桥接网络，反之亦然。

前提条件

- 必须在您的环境中部署了 NSX 逻辑路由器。
- 不能使用通用逻辑路由器配置桥接，且不能将网桥添加到通用逻辑交换机。

步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击将用于桥接的逻辑路由器。

注 网桥实例必须在 vxlan 连接到的同一路由实例中创建。一个网桥实例可以具有一个 vxlan 和一个 vlan，但该 vxlan 和 vlan 不能重叠。同一 vxlan 和 vlan 不能连接到多个网桥实例。

- 4 单击**管理 (Manage)**，然后单击**桥接 (Bridging)**。
正在用作路由器的逻辑交换机将声明“已启用路由”。

- 5 单击**添加 (Add) (+)** 图标。
- 6 键入网桥的名称。
- 7 选择要为其创建网桥的逻辑交换机。
- 8 选择逻辑交换机所要桥接的分布式虚拟端口组。
- 9 单击**确定 (OK)**。
- 10 再次单击“添加桥接”窗口中的**确定 (OK)**。
- 11 单击“发布”，使桥接配置更改生效。

此时将显示用于桥接的逻辑交换机，并指定**已启用路由 (Routing Enabled)**。有关更多信息，请参见[添加逻辑交换机](#)和[将虚拟机连接到逻辑交换机](#)。

路由

您可以为每个 **NSX Edge** 指定静态路由和动态路由。

动态路由可在第 2 层广播域之间提供必需的转发信息，从而帮助减少第 2 层广播域，提高网络效率，扩大网络规模。**NSX** 还将此信息扩展到工作负载所在的位置，用于东西向路由。这样，虚拟机之间就可以直接进行通信，无需花费额外的成本和时间来扩展跃点。同时，**NSX** 也提供南北向连接，从而使租户可以访问公用网络。

本章讨论了以下主题：

- [添加逻辑（分布式）路由器](#)
- [添加 Edge 服务网关](#)
- [指定全局配置](#)
- [NSX Edge 配置](#)
- [添加静态路由](#)
- [在逻辑（分布式）路由器上配置 OSPF](#)
- [在 Edge 服务网关上配置 OSPF](#)
- [配置 BGP](#)
- [配置 IS-IS 协议](#)
- [配置路由重新分发](#)
- [查看 NSX Manager 区域设置 ID](#)
- [在通用逻辑（分布式）路由器上配置区域设置 ID](#)
- [在主机或群集上配置区域设置 ID](#)

添加逻辑（分布式）路由器

主机中的逻辑路由器内核模块在 **VXLAN** 网络之间以及虚拟和物理网络之间执行路由。如果需要，**NSX Edge** 设备可提供动态路由功能。在跨 **vCenter NSX** 环境中，逻辑路由器可以在主 **NSX Manager** 和辅助 **NSX Manager** 上创建，但通用逻辑路由器只能在主 **NSX Manager** 上创建。

以下列表介绍了逻辑路由器上的接口类型（上行链路和内部）支持的功能：

- 动态路由协议（**BGP** 和 **OSPF**）仅在上行链路接口上受支持。

- 防火墙规则仅在上行链路接口上适用，且限制为控制和管理传至 **Edge** 虚拟设备的流量。
- 有关 **DLR** 管理接口的详细信息，请参见知识库文章“分布式逻辑路由器控制虚拟机的管理接口注意事项”，网址为 <http://kb.vmware.com/kb/2122060>。

前提条件

- 您必须已获得企业管理员或 **NSX** 管理员角色。
- 安装逻辑路由器之前，您的环境必须包含正常运行的控制器群集。
- 即使不打算创建 **NSX** 逻辑交换机，您也必须创建本地分段 ID 池。
- 如果缺少 **NSX Controller**，逻辑路由器便无法将路由信息分发给主机。逻辑路由器依靠 **NSX Controller** 来运行，而 **Edge** 服务网关 (**ESG**) 不会这样。在创建或更改逻辑路由器配置之前，确保控制器群集已启动且可用。
- 如果逻辑路由器将连接到 **VLAN dvPortgroup**，请确保已安装逻辑路由器设备的所有虚拟机管理程序主机都可以在 **UDP** 端口 **6999** 上相互访问，以便基于逻辑路由器 **VLAN** 的 **ARP** 代理能够正常工作。
- 逻辑路由器接口和桥接接口无法连接到 **VLAN ID** 设置为 **0** 的 **dvPortgroup**。
- 给定的逻辑路由器实例无法连接到位于不同传输区域的逻辑交换机。此操作旨在确保所有逻辑交换机和逻辑路由器实例相对应。
- 如果某个逻辑路由器连接到跨越多个 **vSphere Distributed Switch (VDS)** 的逻辑交换机，则该逻辑路由器将无法连接到支持 **VLAN** 的端口组。此操作旨在确保各主机间的逻辑路由器实例与逻辑交换机 **dvPortgroup** 相对应。
- 如果两个网络位于同一 **vSphere Distributed Switch** 中，则不应在两个具有相同 **VLAN ID** 的不同分布式端口组 (**dvPortgroup**) 上创建逻辑路由器接口。
- 如果两个网络位于不同的 **vSphere Distributed Switch** 中，但这两个 **vSphere Distributed Switch** 共享相同的主机，则不应在两个具有相同 **VLAN ID** 的不同 **dvPortgroup** 上创建逻辑路由器接口。换句话说，如果两个 **dvPortgroup** 位于两个不同的 **vSphere Distributed Switch** 中，且这两个 **vSphere Distributed Switch** 不共享主机，则可以在两个具有相同 **VLAN ID** 的不同网络上创建逻辑路由器接口。
- 与 **NSX** 版本 **6.0** 和 **6.1** 不同，**NSX** 版本 **6.2** 允许将逻辑路由器路由的逻辑接口 (**LIF**) 连接到桥接至 **VLAN** 的 **VXLAN**。
- 选择放置逻辑路由器虚拟设备时，如果在 **ECMP** 设置中使用 **ESG**，则避免将逻辑路由器虚拟设备与其一个或多个上游 **ESG** 放置在相同主机上。可以使用 **DRS** 反关联性规则强制执行这一点，从而减少主机故障对逻辑路由器转发的影响。如果您具有一个单独的或处于 **HA** 模式下的上游 **ESG**，则此准则不适用。有关详细信息，请参见 <https://communities.vmware.com/docs/DOC-27683> 上的《VMware NSX for vSphere 网络虚拟化设计指南》。

确定要对其进行更改的相应 **NSX Manager**。

- 在独立或单个 **vCenter NSX** 环境中，仅有一个 **NSX Manager**，因此无需进行选择。
- 必须从主 **NSX Manager** 管理通用对象。
- 某个 **NSX Manager** 的本地对象必须使用该 **NSX Manager** 进行管理。

- 在未启用增强型链接模式的跨 vCenter NSX 环境中，您必须从链接至您想要修改的 NSX Manager 的 vCenter 中更改配置。
- 在处于增强型链接模式的跨 vCenter NSX 环境中，您可以从任意链接的 vCenter 更改任意 NSX Manager 的配置。从 NSX Manager 下拉菜单中选择相应的 NSX Manager。
- 确定您需要添加的逻辑路由器的种类：
 - 如果需要连接逻辑交换机，则必须添加逻辑路由器
 - 如果需要连接通用逻辑交换机，则必须添加通用逻辑路由器
- 如果您要添加通用逻辑路由器，请确定您是否需要启用本地输出。本地输出允许您选择性地向主机发送路由。如果 NSX 部署跨多个站点，您可能需要此功能。有关详细信息，请参见[跨 vCenter NSX 拓扑](#)。无法在创建通用逻辑路由器后启用本地输出。

步骤

- 1 在 vSphere Web Client 中，导航到主页 > 网络和安全 > NSX Edge (Home > Networking & Security > NSX Edges)。
- 2 选择要进行更改的相应 NSX Manager。如果要创建通用逻辑路由器，则必须选择主 NSX Manager。
- 3 单击添加 (Add) (+) 图标。
- 4 选择要添加的逻辑路由器类型：
 - 选择**逻辑 (分布式) 路由器 (Logical (Distributed) Router)**以添加选定 NSX Manager 的本地逻辑路由器。
 - 选择**通用逻辑 (分布式) 路由器 (Universal Logical (Distributed) Router)**，添加可以跨跨 vCenter NSX 环境的逻辑路由器。此选项只有在您已经分配主 NSX Manager 且正从主 NSX Manager 进行更改的情况下才可用。
- a 如果选择**通用逻辑 (分布式) 路由器 (Universal Logical (Distributed) Router)**，则还必须选择是否启用本地输出。
- 5 键入设备的名称。

该名称会显示在 vCenter 清单中。该名称在单个租户内的所有逻辑路由器中都应唯一。

此外，还可以输入主机名。该名称会显示在 CLI 中。如果未指定主机名，则 CLI 中将显示自动创建的 Edge ID。

此外，还可以输入描述和租户。

- 6 部署一个 Edge 设备。

默认情况下，将选择**部署 Edge 设备 (Deploy Edge Appliance)**。Edge 设备（也称为逻辑路由器虚拟设备）是动态路由和逻辑路由器设备的防火墙所必需的，适用于逻辑路由器 ping、SSH 访问和动态路由流量。

如果您只需要静态路由，且不希望部署 Edge 设备，则可以取消选择 Edge 设备选项。无法在创建逻辑路由器之后向其添加 Edge 设备。

7 （可选）启用高可用性。

默认情况下，不会选择“启用高可用性”。请选中“启用高可用性”复选框以启用并配置高可用性。如果您计划执行动态路由，则需要高可用性。

8 键入逻辑路由器的密码，然后重新键入一次。

该密码必须是 **12-255** 个字符，且必须包含：

- 至少一个大写字母
- 至少一个小写字母
- 至少一个数字
- 至少一个特殊字符

9 （可选）启用 SSH 并设置日志级别。

默认情况下，SSH 处于禁用状态。如果未启用 SSH，则仍可通过打开虚拟设备控制台来访问逻辑路由器。在此处启用 SSH 会导致 SSH 进程在逻辑路由器虚拟设备上运行，但您还将需要手动调整逻辑路由器防火墙配置，以允许对逻辑路由器的协议地址进行 SSH 访问。协议地址会在逻辑路由器上配置动态路由时进行配置。

默认情况下，日志级别为紧急。

例如：

The screenshot shows the 'New NSX Edge' configuration wizard. On the left, a sidebar lists steps: 1 Name and description, 2 Settings (selected), 3 Configure deployment, 4 Configure interfaces, 5 Default gateway settings, and 6 Ready to complete. The main area is titled 'Settings' and contains the following information:

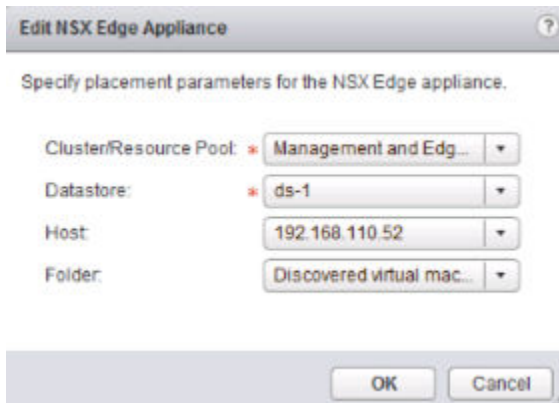
- CLI credentials will be set on the NSX Edge appliance(s). These credentials can be used to login to the read only command line interface of the appliance.
- User Name:
- Password:
- Confirm password:
- ☒ Enable SSH access
- ☐ Enable High Availability
- Enable HA, for enabling and configuring High Availability:*
- Edge Control Level Logging:
- Set the Edge Control Level Logging*

At the bottom, there are four buttons: Back, Next, Finish, and Cancel.

10 配置部署。

- ◆ 如果未选择**部署 NSX Edge (Deploy NSX Edge)**，则**添加 (Add)** (+) 图标为灰显状态。单击**下一步 (Next)**继续配置。
- ◆ 如果选择了**部署 NSX Edge (Deploy NSX Edge)**，请输入将添加到 vCenter 清单的逻辑路由器虚拟设备的设置。

例如：



11 配置接口。

在逻辑路由器上，仅支持 IPv4 寻址。

在“HA 接口配置”中，如果选择了**部署 NSX Edge (Deploy NSX Edge)**，您必须将接口连接到分布式端口组。建议将 VXLAN 逻辑交换机用于 HA 接口。将从链路本地地址空间 169.250.0.0/16 中分别选择两个 NSX Edge 设备的 IP 地址。不需要进行进一步配置以配置 HA 服务。

注 在先前版本的 NSX 中，HA 接口称为管理接口。远程访问逻辑路由器不支持 HA 接口。对于与 HA 接口不在同一 IP 子网上的位置，无法通过 SSH 方式连接 HA 接口。无法配置将 HA 接口排除在外的静态路由，这意味着 RPF 将丢弃入站流量。理论上可以禁用 RPF，但这将不利于实现高可用性。对于 SSH，使用逻辑路由器的协议地址，这将在稍后配置动态路由时进行配置。

在 NSX 6.2 中，逻辑路由器的 HA 接口会自动从路由重新分布中排除。

在配置此 NSX Edge 的接口 (Configure interfaces of this NSX Edge) 中，内部接口用于连接到允许虚拟机间（有时称为东西向）通信的交换机。内部接口将在逻辑路由器虚拟设备上作为伪虚拟网卡进行创建。上行链路接口用于南北向通信。逻辑路由器上行链路接口可能会连接到 NSX Edge 服务网关、其第三方路由器虚拟机或支持 VLAN 的 dvPortgroup，以使逻辑路由器直接与物理路由器连接。您必须至少有一个上行链路接口才能进行动态路由。上行链路接口将在逻辑路由器虚拟设备上作为虚拟网卡进行创建。

您在此处输入的接口配置可在以后进行修改。可以在部署逻辑路由器后添加、移除和修改接口。

以下示例显示连接到管理分布式端口组的 HA 接口。该示例还显示两个内部接口（应用程序和 Web）和一个上行链路接口（通向 ESG）。

New NSX Edge

- 1 Name and description
- 2 Settings
- 3 Configure deployment
- 4 Configure interfaces**
- 5 Default gateway settings
- 6 Ready to complete

Configure interfaces

HA Interface Configuration

Connected To: [Change](#) [Remove](#)

IP Address	Subnet Prefix Length
192.168.110.60*	24

HA interface is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Configure interfaces of this NSX Edge

Name	IP Address	Subnet Prefix Length	Connected To
app	172.16.20.1*	24	app
web	172.16.10.1*	24	web
to-ESG	192.168.10.2*	29	transit

Buttons: Back, Next, Finish, Cancel

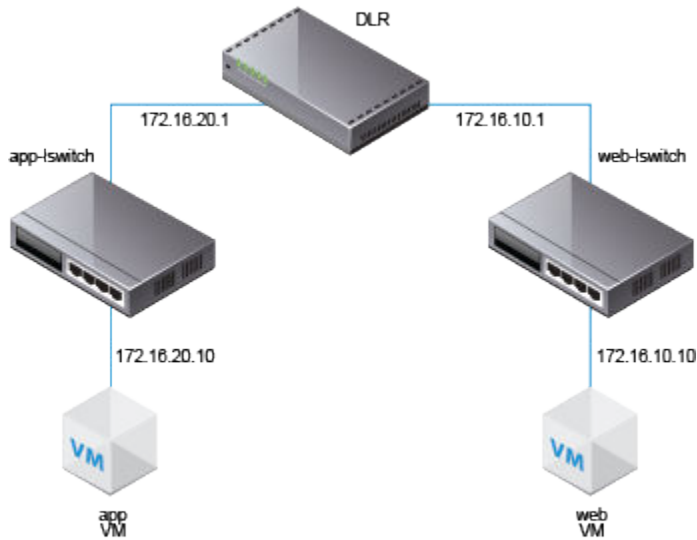
12 配置默认网关。

例如：

The screenshot shows the 'New NSX Edge' configuration wizard. On the left, a sidebar lists six steps: 1 Name and description, 2 Settings, 3 Configure deployment, 4 Configure interfaces, 5 Default gateway settings (highlighted), and 6 Ready to complete. The main area is titled 'Default gateway settings' and contains a checkbox 'Configure Default Gateway' which is checked. Below this are three input fields: 'vNIC:' with a dropdown menu showing 'to-ESG', 'Gateway IP:' with a text box containing '192.168.10.1', and 'MTU:' with a text box containing '1500'. At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

13 确保连接到逻辑交换机的任何虚拟机的默认网关都正确设置为逻辑路由器接口 IP 地址。

在以下示例拓扑中，应用程序虚拟机的默认网关应为 **172.16.20.1**。Web 虚拟机的默认网关应为 **172.16.10.1**。确保这些虚拟机可以相互 ping 其默认网关。



通过 SSH 登录到 NSX Manager，然后运行以下命令：

- 列出所有逻辑路由器实例信息。

```
nsxmgr-l-01a> show logical-router list all
```

Edge-id	Vdr Name	Vdr id	#Lifs
edge-1	default+edge-1	0x00001388	3

- 列出已从控制器群集收到逻辑路由器的路由信息的主机。

```
nsxmgr-l-01a> show logical-router list dlr edge-1 host
```

ID	HostName
host-25	192.168.210.52
host-26	192.168.210.53
host-24	192.168.110.53

输出包括配置为传输区域的成员的所有主机群集中的所有主机，该传输区域拥有连接到指定逻辑路由器（本示例中为 **edge-1**）的逻辑交换机。

- 列出由逻辑路由器传送给主机的路由表信息。所有主机间的路由表条目应一致。

```
nsxmgr-l-01a> show logical-router host host-25 dlr edge-1 route
```

VDR default+edge-1 Route Table

Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]

Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]

Destination	GenMask	Gateway	Flags	Ref	Origin	UpTime	Interface
0.0.0.0	0.0.0.0	192.168.10.1	UG	1	AUTO	4101	138800000002
172.16.10.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10195	13880000000b
172.16.20.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10196	13880000000a
192.168.10.0	255.255.255.248	0.0.0.0	UCI	1	MANUAL	10196	138800000002
192.168.100.0	255.255.255.0	192.168.10.1	UG	1	AUTO	3802	138800000002

- 从其中某个主机的角度，列出有关路由器的其他信息。这有助于了解哪个控制器正在与该主机进行通信。

```
nsx-mgr-l-01a> show logical-router host host-25 dlr edge-1 verbose
```

```
VDR Instance Information :
```

```
-----
Vdr Name:                default+edge-1
Vdr Id:                  0x00001388
Number of Lifs:          3
Number of Routes:        5
State:                   Enabled
Controller IP:           192.168.110.203
Control Plane IP:        192.168.210.52
Control Plane Active:     Yes
Num unique nexthops:      1
Generation Number:        0
Edge Active:             No
```

在 `show logical-router host host-25 dlr edge-1 verbose` 命令的输出中，检查“控制器 IP”字段。通过 SSH 登录到控制器，并运行以下命令以显示控制器获知的 VNI、VTEP、MAC 和 ARP 表状态信息。

```
192.168.110.202 # show control-cluster logical-switches vni 5000
VNI      Controller      BUM-Replication ARP-Proxy Connections
5000     192.168.110.201 Enabled           Enabled      0
```

VNI 5000 的输出显示零个连接，并将控制器 192.168.110.201 列为 VNI 5000 的所有者。登录到此控制器，以收集 VNI 5000 的更多信息。

```
192.168.110.201 # show control-cluster logical-switches vni 5000
VNI      Controller      BUM-Replication ARP-Proxy Connections
5000     192.168.110.201 Enabled           Enabled      3
```

192.168.110.201 上的输出显示三个连接。检查其他 VNI。

```
192.168.110.201 # show control-cluster logical-switches vni 5001
VNI      Controller      BUM-Replication ARP-Proxy Connections
5001     192.168.110.201 Enabled           Enabled      3
```

```
192.168.110.201 # show control-cluster logical-switches vni 5002
VNI      Controller      BUM-Replication ARP-Proxy Connections
5002     192.168.110.201 Enabled           Enabled      3
```

由于 192.168.110.201 拥有全部三个 VNI 连接，我们预期会在另一个控制器 192.168.110.203 上看到零个连接。

```
192.168.110.203 # show control-cluster logical-switches vni 5000
VNI      Controller      BUM-Replication ARP-Proxy Connections
5000     192.168.110.201 Enabled           Enabled      0
```

- 在检查 MAC 和 ARP 表之前，开始从一个虚拟机 ping 到另一个虚拟机。

从应用程序虚拟机到 Web 虚拟机：

```
vmware@vmware-virtual-machine:~$ 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_seq=1 ttl=63 time=2.15 ms
64 bytes from 172.16.10.10: icmp_seq=2 ttl=63 time=1.60 ms
```

检查 MAC 表。

```
192.168.110.201 # show control-cluster logical-switches mac-table 5000
VNI      MAC                VTEP-IP            Connection-ID
5000     00:50:56:a6:23:ae 192.168.250.52     7
```

```
192.168.110.201 # show control-cluster logical-switches mac-table 5001
VNI      MAC                VTEP-IP            Connection-ID
5001     00:50:56:a6:8d:72 192.168.250.51     23
```

检查 ARP 表。

```
192.168.110.201 # show control-cluster logical-switches arp-table 5000
VNI      IP                MAC                Connection-ID
5000     172.16.20.10     00:50:56:a6:23:ae 7
```

```
192.168.110.201 # show control-cluster logical-switches arp-table 5001
VNI      IP                MAC                Connection-ID
5001     172.16.10.10     00:50:56:a6:8d:72 23
```

检查逻辑路由器信息。每个逻辑路由器实例都由某个控制器节点提供服务。

`show control-cluster logical-routers` 命令的 `instance` 子命令显示连接到此控制器的逻辑路由器的列表。

`interface-summary` 子命令显示控制器从 NSX Manager 获知的 LIF。此信息将发送到由传输区域管理的主机群集中的主机。

`routes` 子命令显示由逻辑路由器的虚拟设备（也称为控制虚拟机）发送到此控制器的路由表。请注意，不像在 ESXi 主机上，此路由表不包括直接连接的子网，因为此信息由 LIF 配置提供。ESXi 主机上的路由信息包括直接连接的子网，因为在这种情况下，它是一个由 ESXi 主机的数据路径使用的转发表。

- ```
controller # show control-cluster logical-routers instance all
LR-Id LR-Name Universal Service-Controller Egress-Locale
0x1388 default+edge-1 false 192.168.110.201 local
```

记下 LR-Id 并用于以下命令。

- `controller # show control-cluster logical-routers interface-summary 0x1388`

| Interface    | Type | Id     | IP[]            |
|--------------|------|--------|-----------------|
| 13880000000b | vlan | 0x1389 | 172.16.10.1/24  |
| 13880000000a | vlan | 0x1388 | 172.16.20.1/24  |
| 138800000002 | vlan | 0x138a | 192.168.10.2/29 |

- `controller # show control-cluster logical-routers routes 0x1388`

| Destination      | Next-Hop[]   | Preference | Locale-Id                            | Source     |
|------------------|--------------|------------|--------------------------------------|------------|
| 192.168.100.0/24 | 192.168.10.1 | 110        | 00000000-0000-0000-0000-000000000000 | CONTROL_VM |
| 0.0.0.0/0        | 192.168.10.1 | 0          | 00000000-0000-0000-0000-000000000000 | CONTROL_VM |

```
[root@comp02a:~] esxcfg-route -l
```

VMkernel Routes:

| Network       | Netmask       | Gateway       | Interface |
|---------------|---------------|---------------|-----------|
| 10.20.20.0    | 255.255.255.0 | Local Subnet  | vmk1      |
| 192.168.210.0 | 255.255.255.0 | Local Subnet  | vmk0      |
| default       | 0.0.0.0       | 192.168.210.1 | vmk0      |

- 显示控制器与特定 VNI 之间的连接。

```
192.168.110.203 # show control-cluster logical-switches connection-table 5000
```

| Host-IP        | Port  | ID |
|----------------|-------|----|
| 192.168.110.53 | 26167 | 4  |
| 192.168.210.52 | 27645 | 5  |
| 192.168.210.53 | 40895 | 6  |

```
192.168.110.202 # show control-cluster logical-switches connection-table 5001
```

| Host-IP        | Port  | ID |
|----------------|-------|----|
| 192.168.110.53 | 26167 | 4  |
| 192.168.210.52 | 27645 | 5  |
| 192.168.210.53 | 40895 | 6  |

这些主机 IP 地址是 vmk0 接口，而非 VTEP。ESXi 主机与控制器之间的连接将在管理网络上创建。此处的端口号是主机与控制器建立连接时由 ESXi 主机 IP 堆栈分配的极短 TCP 端口。

- 在主机上，可以查看与端口号匹配的控制器网络连接。

```
[root@192.168.110.53:~] #esxcli network ip connection list | grep 26167
```

|         |               |   |                      |                      |             |       |
|---------|---------------|---|----------------------|----------------------|-------------|-------|
| tcp     | 0             | 0 | 192.168.110.53:26167 | 192.168.110.101:1234 | ESTABLISHED | 96416 |
| newreno | netcpa-worker |   |                      |                      |             |       |

- 显示主机上的活动 VNI。观察各主机间输出的不同之处。并非所有主机上的所有 VNI 都处于活动状态。如果主机的某个虚拟机已连接到逻辑交换机，则该主机上的 VNI 处于活动状态。

```
[root@192.168.210.52:~] # esxcli network vswitch dvs vmware vxlan network list --vds-name Compute_VDS
```

| VXLAN ID | Multicast IP    | Control Plane   | Controller Connection | Port  |
|----------|-----------------|-----------------|-----------------------|-------|
| Count    | MAC Entry Count | ARP Entry Count | VTEP Count            |       |
| -----    | -----           | -----           | -----                 | ----- |
| -----    | -----           | -----           | -----                 | ----- |

|      |                           |                                     |                 |
|------|---------------------------|-------------------------------------|-----------------|
| 5000 | N/A (headend replication) | Enabled (multicast proxy,ARP proxy) | 192.168.110.203 |
| (up) | 1                         | 0                                   | 0               |
| 5001 | N/A (headend replication) | Enabled (multicast proxy,ARP proxy) | 192.168.110.202 |
| (up) | 1                         | 0                                   | 0               |

**注** 要在 vSphere 6 及更高版本中启用 vxlan 命名空间，请运行 `/etc/init.d/hostd restart` 命令。

对于处于混合模式或单播模式的逻辑交换机，`esxcli network vswitch dvs vmware vxlan network list --vds-name <vds-name>` 命令应包含以下输出：

- 将启用控制层面。
- 将列出多播代理和 ARP 代理。将列出 AARP 代理，即使已禁用 IP 发现。
- 将列出有效的控制器 IP 地址并建立连接。
- 如果将逻辑路由器连接到 ESXi 主机，则端口计数至少为 1，即使主机上没有任何虚拟机连接到逻辑交换机。此端口为 `vdrPort`，是连接到 ESXi 主机上逻辑路由器内核模块的特殊 `dvPort`。
- 首先从虚拟机 ping 到不同子网上的另一个虚拟机，然后显示 MAC 表。请注意，内部 MAC 是虚拟机条目，而外部 MAC 和外部 IP 指 VTEP。

```
~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-name=Compute_VDS --vxlan-id=5000
Inner MAC Outer MAC Outer IP Flags

00:50:56:a6:23:ae 00:50:56:6a:65:c2 192.168.250.52 00000111

~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-name=Compute_VDS --vxlan-id=5001
Inner MAC Outer MAC Outer IP Flags

02:50:56:56:44:52 00:50:56:6a:65:c2 192.168.250.52 00000101
00:50:56:f0:d7:e4 00:50:56:6a:65:c2 192.168.250.52 00000111
```

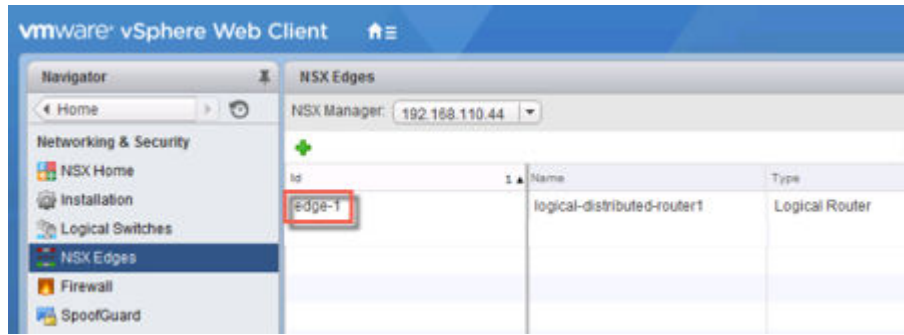
## 后续步骤

在第一次部署 NSX Edge 设备的主机上，NSX 会启用自动虚拟机启动/关机。如果设备虚拟机后来被迁移到其他主机，则新的主机可能不会启用自动虚拟机启动/关机。因此，VMware 建议您检查群集中的所有主机，以确保启用了自动虚拟机启动/关机。请参见

[http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm\\_admin.doc%2FGUID-5FE08AC7-4486-438E-AF88-80D6C7928810.html](http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-5FE08AC7-4486-438E-AF88-80D6C7928810.html)。

部署逻辑路由器后，双击逻辑路由器 ID 以配置其他设置，如接口、路由、防火墙、桥接和 DHCP 中继。

例如：



## 添加 Edge 服务网关

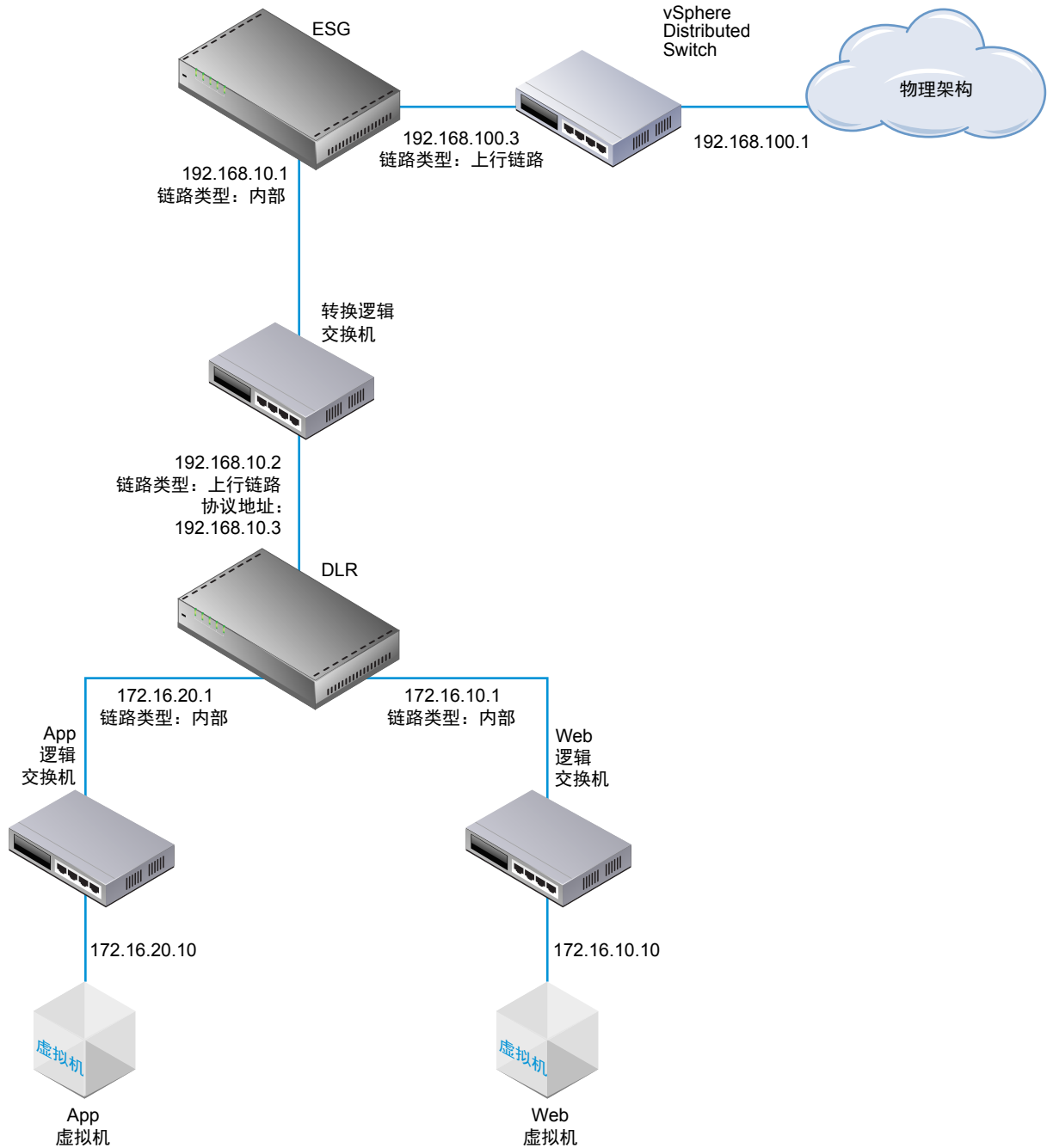
您可以在一个数据中心中安装多个 **NSX Edge** 服务网关虚拟设备。每个 **NSX Edge** 虚拟设备总共可以有十个上行链路和内部网络接口。内部接口连接至安全的端口组，并充当端口组中所有受保护虚拟机的网关。分配给内部接口的子网可以是公开路由的 IP 地址空间，或者是采用 NAT/路由的 RFC 1918 专用空间。会对接口之间的流量实施防火墙规则和其他 **NSX Edge** 服务。

**ESG** 的上行链路接口连接至上行链路端口组，后者可以访问共享企业网络或提供访问层网络连接功能的服务。

以下列表介绍了 **ESG** 上的接口类型（内部和上行链路）支持的功能。

- **DHCP**：上行链路接口不支持。
- **DNS 转发器**：上行链路接口不支持。
- **HA**：上行链路接口不支持，至少需要一个内部接口。
- **SSL VPN**：侦听器 IP 必须属于上行链路接口。
- **IPSec VPN**：本地站点 IP 必须属于上行链路接口。
- **L2 VPN**：仅可延伸内部网络。

下图显示了一个拓扑示例，其中 **ESG** 的上行链路接口通过 **vSphere Distributed Switch** 连接到物理基础架构，**ESG** 的内部接口通过 **NSX 逻辑转换交换机** 连接到 **NSX 逻辑路由器**。



可以为负载平衡、点对点 VPN 和 NAT 服务配置多个外部 IP 地址。

#### 前提条件

您必须已获得企业管理员或 NSX 管理员角色。

验证资源池是否具有足够的容量用于部署 Edge 服务网关 (ESG) 虚拟设备。请参见第 1 章，NSX 的系统要求。

## 步骤

- 1 在 vCenter 中，导航到主页 > 网络和安全 > NSX Edge (Home > Networking & Security > NSX Edges)，然后单击添加 (Add) (+) 图标。

- 2 选择 Edge 服务网关 (Edge Services Gateway)，然后键入设备的名称。

该名称会显示在 vCenter 清单中。该名称在单个租户内的所有 ESG 中都应唯一。

此外，还可以输入主机名。该名称会显示在 CLI 中。如果未指定主机名，则 CLI 中将显示自动创建的 Edge ID。

此外，还可以输入描述和租户，并启用高可用性。

例如：

The screenshot shows the 'New NSX Edge' configuration window. On the left, a sidebar lists steps: 1 Name and description (selected), 2 Settings, 3 Configure deployment, 4 Configure interfaces, 5 Default gateway settings, 6 Firewall and HA, and 7 Ready to complete. The main area is titled 'Name and description'. Under 'Install Type', 'Edge Services Gateway' is selected with a radio button, and 'Logical (Distributed) Router' is unselected. Below this, the 'Name' field is filled with 'ESG-1', 'Hostname' is empty, 'Description' is empty, and 'Tenant' is empty. At the bottom, the 'Deploy NSX Edge' checkbox is checked, and the 'Enable High Availability' checkbox is unchecked. The bottom of the window has four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

- 3 键入 ESG 的密码，然后重新键入一次。

该密码必须至少为 12 个字符，且必须遵循以下 4 个规则中的 3 个：

- 至少一个大写字母
- 至少一个小写字母
- 至少一个数字

- 至少一个特殊字符

#### 4 （可选）启用 SSH、高可用性和自动规则生成，并设置日志级别。

如果不启用自动规则生成，则必须手动添加防火墙、NAT 和路由配置，以便控制某些 NSX Edge 服务（包括负载平衡和 VPN）的流量。自动规则生成不会为数据通道流量创建规则。

默认情况下，SSH 和高可用性处于禁用状态，而自动规则生成处于启用状态。默认情况下，日志级别为紧急。

默认情况下，将在所有新的 NSX Edge 设备上启用日志记录。默认日志记录级别为“通知”。

例如：

The screenshot shows the 'New NSX Edge' configuration wizard. On the left, a sidebar lists the steps: 1 Name and description, 2 Settings (selected), 3 Configure deployment, 4 Configure interfaces, 5 Default gateway settings, 6 Firewall and HA, and 7 Ready to complete. The main area is titled 'Settings' and contains the following information:

- A note: 'CLI credentials will be set on the NSX Edge appliance(s). These credentials can be used to login to the read only command line interface of the appliance.'
- Fields for 'User Name' (admin), 'Password' (masked with asterisks), and 'Confirm password' (masked with asterisks).
- Checkboxes for 'Enable SSH access' and 'Enable auto rule generation' (checked).
- A description for the auto rule generation checkbox: 'Enable auto rule generation, to automatically generate service rules to allow flow of control traffic.'
- A dropdown menu for 'Edge Control Level Logging' set to 'EMERGENCY'.
- A link: 'Set the Edge Control Level Logging'.

At the bottom, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

#### 5 基于系统资源选择 NSX Edge 实例的大小。

**中型 (Large)** NSX Edge 的 CPU、内存和磁盘空间量高于**精简 (Compact)** NSX Edge，并且支持的并发 SSL VPN-Plus 用户数更多。**超大型 (X-Large)** NSX Edge 适合具有负载平衡器以及数百万个并发会话的环境。大型的 NSX Edge 推荐用于高吞吐量和高连接速率要求的环境。

请参见第 1 章，NSX 的系统要求。

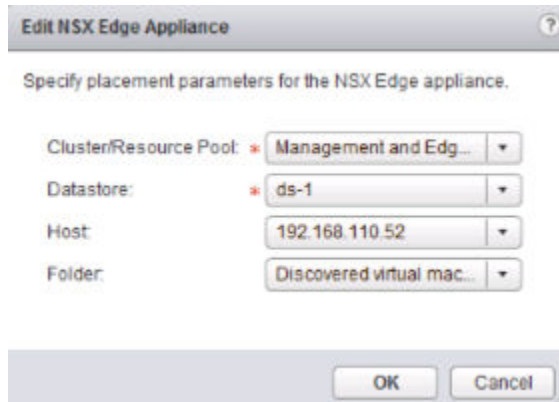


## 6 创建一个 Edge 设备。

输入将添加到 vCenter 清单的 ESG 虚拟设备的设置。如果安装 NSX Edge 时未添加设备，NSX Edge 将保持脱机模式，直到您添加设备为止。

如果已启用 HA，则可以添加两个设备。如果添加一个设备，NSX Edge 会为备用设备复制其配置，并确保即使在您使用 DRS 和 vMotion 之后，两个 HA NSX Edge 虚拟机也不在同一个 ESX 主机上（除非以手动方式通过 vMotion 将二者移至同一个主机）。要使 HA 正常工作，必须将两个设备部署在共享数据存储上。

例如：



- 7 选择**部署 NSX Edge (Deploy NSX Edge)**，以便添加处于已部署模式的 Edge。必须先为 Edge 配置设备和接口，然后才能对其进行部署。

## 8 配置接口。

在 ESG 上，同时支持 IPv4 地址和 IPv6 地址。

您必须至少添加一个内部接口才能使 HA 工作。

一个接口可以具有多个非重叠的子网。

如果为一个接口输入多个 IP 地址，则可以选择主 IP 地址。一个接口可以具有一个主 IP 地址和多个辅助 IP 地址。NSX Edge 将主 IP 地址视为本地生成流量（例如，远程 syslog 和操作员启动的 ping）的源地址。

必须将 IP 地址添加到接口，才能在所有功能配置中使用该地址。

此外，还可以输入接口的 MAC 地址。

如果已启用 HA，可以采用 CIDR 格式输入两个管理 IP 地址。两个 NSX Edge HA 虚拟机的检测信号通过这些管理 IP 地址进行通信。管理 IP 地址必须在同一 L2/子网中，并且能够彼此通信。

此外，还可以修改 MTU。

如果要允许 ESG 响应面向其他计算机的 ARP 请求，请启用代理 ARP。例如，当在 WAN 连接的两端具有相同子网时，这会非常有用。

启用 ICMP 重定向，以将路由信息传输给主机。

启用反向路径筛选器，以验证正转发的数据包中源地址的可访问性。在启用模式下，必须在路由器将用来转发返回数据包的接口上接收数据包。在宽松模式下，源地址必须显示在路由表中。

如果要在不同的受防护环境之间重用 IP 和 MAC 地址，请配置防护参数。例如，在 Cloud Management Platform (CMP) 中，通过防护可以同时运行多个具有相同 IP 和 MAC 地址且完全隔离或“受防护”的云实例。

例如：

**Edit NSX Edge Interface**

VNIC#: 1

Name: \* Internal

Type: ☒ Internal ☐ Uplink

Connected To: transit-switch [Change](#) [Remove](#)

Connectivity Status: ☒ Connected ☐ Disconnected

Configure subnets

| IP Address    | Subnet Prefix Length |
|---------------|----------------------|
| 192.168.10.1* | 29                   |
|               |                      |
|               |                      |
|               |                      |

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU:

Options: ☐ Enable Proxy ARP ☐ Send ICMP Redirect Reverse Path Filter [Disable](#) ▼

Fence Parameters:

Example: ethernet0.filter1.param1=1

[OK](#) [Cancel](#)

以下示例显示了两个接口，一个接口通过 vSphere Distributed Switch 上的上行链路端口组将 ESG 连接到外界，另一个接口将 ESG 连接到同时连接分布式逻辑路由器的逻辑转换交换机。

New NSX Edge

✓ 1 Name and description

✓ 2 Settings

✓ 3 Configure deployment

✓ 4 Configure interfaces

5 Default gateway settings

6 Firewall and HA

7 Ready to complete

Configure interfaces

Configure interfaces of this NSX Edge

+

✗

| vNIC# | Name     | IP Address    | Subnet Prefix Length | Connected To         |
|-------|----------|---------------|----------------------|----------------------|
| 0     | uplink   | 192.168.100.3 | 24                   | Mgmt_VDS - HQ_Uplink |
| 1     | internal | 192.168.10.1  | 29                   | transit-switch       |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |

Back

Next

Finish

Cancel

## 9 配置默认网关。

您可以编辑 MTU 值，但其不能超过接口上配置的 MTU 值。

例如：

## 10 配置防火墙策略、日志记录和 HA 参数。



**小心** 如果您未配置防火墙策略，则默认策略将设置为拒绝所有流量。

默认情况下，将在所有新的 **NSX Edge** 设备上启用日志。默认日志记录级别为“通知”。如果将日志本地存储在 **ESG** 上，则日志记录可能会生成过多日志，并影响 **NSX Edge** 的性能。因此，建议您配置远程 **syslog** 服务器，并将所有日志转发到集中式收集器以进行分析和监控。

如果已启用高可用性，请完成 **HA** 部分。默认情况下，**HA** 会自动选择内部接口，并自动分配本地链接 IP 地址。**NSX Edge** 支持两个虚拟机实现高可用性，这两个虚拟机都保持最新的用户配置。如果主虚拟机上出现检测信号故障，则辅助虚拟机状态将变为活动。因此，网络上始终有一个 **NSX Edge** 虚拟机处于活动状态。**NSX Edge** 会为备用设备复制主设备的配置，并确保即使在您使用 **DRS** 和 **vMotion** 之后，

两个 HA NSX Edge 虚拟机也不在同一个 ESX 主机上。两个虚拟机都在 vCenter 上部署，与您配置的设备处于同一资源池和数据存储中。系统会为 NSX Edge HA 中的 HA 虚拟机分配本地链接 IP 地址，以便它们彼此进行通信。选择要为其配置 HA 参数的内部接口。如果为接口选择“任意”，但未配置任何内部接口，则 UI 不会显示错误。将创建两个 Edge 设备，但由于未配置任何内部接口，新的 Edge 将保持备用状态且会禁用 HA。配置内部接口后，便会在该 Edge 设备上启用 HA。以秒为单位键入时间段，如果备用设备在该时间段内未从主设备收到检测信号，则主设备将被视为不活动，并被该备用设备取代。默认时间间隔为 15 秒。此外，还可以采用 CIDR 格式输入两个管理 IP 地址，以替代分配给 HA 虚拟机的本地链接 IP 地址。确保管理 IP 地址不与用于任何其他接口的 IP 地址重叠，并且不干扰流量路由。不得使用网络上其他地方存在的 IP 地址，即使该网络未直接连接到 NSX Edge 也是如此。

例如：

**New NSX Edge**

1 Name and description  
2 Settings  
3 Configure deployment  
4 Configure interfaces  
5 Default gateway settings  
**6 Firewall and HA**  
7 Ready to complete

**Firewall and HA**

☒ Configure Firewall default policy

Default Traffic Policy: ☒ Accept ☐ Deny

Logging: ☐ Enable ☒ Disable

**Configure HA parameters**  
Configuring HA parameters is mandatory for HA to work.

vNIC: \* internal

Declare Dead Time: 15 (seconds)

Management IPs:

You can specify pair of IPs (in CIDR format) with /30 subnet. Management IPs must not overlap with any vnic subnets.

Back Next Finish Cancel

部署 ESG 之后，转到“主机和群集”视图，并打开 Edge 虚拟设备的控制台。从控制台中，确保可以 ping 已连接的接口。

## 后续步骤

在第一次部署 NSX Edge 设备的主机上，NSX 会启用自动虚拟机启动/关机。如果设备虚拟机后来被迁移到其他主机，则新的主机可能不会启用自动虚拟机启动/关机。因此，VMware 建议您检查群集中的所有主机，以确保启用了自动虚拟机启动/关机。请参见

[http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm\\_admin.doc%2FGUID-5FE08AC7-4486-438E-AF88-80D6C7928810.html](http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-5FE08AC7-4486-438E-AF88-80D6C7928810.html)。

现在，便可配置路由以允许外部设备到虚拟机的连接。

## 指定全局配置

可以为静态路由配置默认网关，为 Edge 服务网关或分布式路由器指定动态路由详细信息。

必须具有正在运行的 NSX Edge 实例才能在其上配置路由。有关设置 NSX Edge 的信息，请参见 [NSX Edge 配置](#)。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击 **路由 (Routing)**，然后单击 **全局配置 (Global Configuration)**。
- 5 要更改等价多路径 (ECMP) 路由的配置，请单击 **路由配置 (Routing Configuration)** 旁边的 **编辑 (Edit)**，然后执行以下操作。

| 选项           | 说明                                                                                                    |
|--------------|-------------------------------------------------------------------------------------------------------|
| 对于 Edge 服务网关 | 要编辑 ECMP，请单击 ECMP 旁边的 <b>启用 (Enable)</b> 或 <b>禁用 (Disable)</b> 。                                      |
| 对于逻辑路由器      | <ol style="list-style-type: none"> <li>a 选中“ECMP”将其启用，或者取消选中“ECMP”将其禁用。</li> <li>b 单击“确定”。</li> </ol> |

ECMP 是允许通过多个最佳路径将下一跃点数据包转发到单个目标的路由策略。这些最佳路径可以是静态添加的，也可以是 OSPF 或 BGP 等动态路由协议执行衡量指标计算而得到的结果。可以通过在“静态路由”对话框中提供多个以逗号分隔的下一跃点来添加多个静态路由路径。有关详细信息，请参见 [添加静态路由](#)。

Edge 服务网关利用 Linux 网络堆栈实施，这是对随机组件使用的循环算法。为某个特定源和目标 IP 地址对选择下一跃点后，路由缓存将存储选定的下一跃点。该特定流的所有数据包将流向选定的下一跃点。默认 IPv4 路由缓存超时为 300 秒 (gc\_timeout)。如果某个条目在该时间段内一直不活动，则可以从路由缓存中移除。实际的移除操作在垃圾数据收集计时器激活时发生 (gc\_interval = 60 秒)。

逻辑路由器使用 XOR 算法从可能的 ECMP 下一跃点列表中确定下一跃点。此算法使用出站数据包上的源和目标 IP 地址作为熵的源。

在 6.1.2 及之前的版本中，启用 ECMP 将在 Edge 服务网关虚拟机上禁用分布式防火墙。NAT 等有状态服务无法与 ECMP 配合使用。自 NSX for vSphere 6.1.3 起，ECMP 和分布式防火墙可以协同工作。

- 6 要更改逻辑路由器上的**区域设置 ID (Locale ID)**，请单击**路由配置 (Routing Configuration)**旁边的**编辑 (Edit)**。输入区域设置 ID，然后单击“确定”。

默认情况下，区域设置 ID 设置为 NSX Manager 的 UUID，但是，如果创建通用逻辑路由器时启用了本地输出，则可以覆盖该 UUID。区域设置 ID 用于有选择地在跨 vCenter NSX 或多站点环境中配置路由。有关详细信息，请参见[跨 vCenter NSX 拓扑](#)。

区域设置 ID 必须采用 UUID 格式。例如，XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX，其中每个 X 都替换为 16 进制数字 (0-F)。

- 7 要指定默认网关，请单击**默认网关 (Default Gateway)**旁边的**编辑 (Edit)**。

- a 选择一个接口，从该接口可以访问朝向目标网络的下一跃点。
- b 键入网关 IP。
- c （可选）键入区域设置 ID。“区域设置 ID”这个选项只存在于通用逻辑路由器上。
- d （可选）编辑 MTU。
- e 如果出现提示，请键入**管理员距离 (Admin Distance)**。

选择一个介于 1 和 255 之间的值。当给定网络具有多个路由时，可根据管理员距离选择要使用的路由。管理员距离越小，就越优先选择相应路由。

**表 9-1. 默认管理员距离**

| 路由源      | 默认管理员距离 |
|----------|---------|
| 已连接      | 0       |
| 静态       | 1       |
| 外部 BGP   | 20      |
| OSPF 区域内 | 30      |
| OSPF 区域内 | 110     |
| 内部 BGP   | 200     |

- f （可选）键入默认网关的描述。
  - g 单击**保存 (Save)**。
- 8 要配置动态路由，请单击**动态路由配置 (Dynamic Routing Configuration)**旁边的**编辑 (Edit)**。
- a **路由器 ID (Router ID)** 显示用于将路由推送至内核以实现动态路由的 NSX Edge 的第一个上行链路 IP 地址。
  - b 请勿在此启用任何协议。
  - c 选择**启用日志记录 (Enable Logging)**以保存日志记录信息，然后选择日志级别。

**注** 如果您的环境中配置了 IPSec VPN，则不应使用动态路由。

- 9 单击**发布更改 (Publish Changes)**。

## 后续步骤

要删除路由配置，请单击**重置 (Reset)**。这将删除所有路由配置（默认配置、静态配置、OSPF 配置和 BGP 配置以及路由重新分发）。

## NSX Edge 配置

一旦您安装了一个能够运行的 NSX Edge（即，添加了一个或多个设备和接口并配置了默认网关、防火墙策略和高可用性），则可以开始使用 NSX Edge 服务。

## 使用证书

NSX Edge 支持自签名证书、由证书颁发机构 (CA) 签名的证书以及由 CA 生成并签名的证书。

### 配置 CA 签名证书

您可以生成 CSR 并使其获得 CA 签名。如果在全局级别生成 CSR，则该 CSR 可用于清单中的所有 NSX Edge。

#### 步骤

- 1 执行以下操作之一。

| 选项                | 说明                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 生成全局证书            | <ol style="list-style-type: none"> <li>a 登录到 NSX Manager 虚拟设备。</li> <li>b 单击“管理”选项卡，然后单击“SSL 证书”。</li> <li>c 单击<b>生成 CSR (Generate CSR)</b>。</li> </ol>                                                                                                                                                                                                                  |
| 生成用于 NSX Edge 的证书 | <ol style="list-style-type: none"> <li>a 登录到 vSphere Web Client。</li> <li>b 单击<b>网络和安全 (Networking &amp; Security)</b>，然后单击<b>Edge 服务 (Edge Services)</b>。</li> <li>c 双击一个 NSX Edge。</li> <li>d 单击<b>管理 (Manage)</b>选项卡，然后单击<b>设置 (Settings)</b>。</li> <li>e 单击<b>证书 (Certificates)</b>链接。</li> <li>f 单击<b>操作 (Actions)</b>，然后选择<b>生成 CSR (Generate CSR)</b>。</li> </ol> |

- 2 键入组织单位和名称。
- 3 键入组织的地点、街道、省/市/自治区和国家/地区。
- 4 为主机之间的通信选择加密算法。

请注意，SSL VPN-Plus 仅支持 RSA 证书。

- 5 根据需要编辑默认密钥大小。
- 6 对于全局证书，键入证书描述。
- 7 单击**确定 (OK)**。

CSR 将生成并显示在“证书”列表中。

- 8 请在线证书颁发机构为此 CSR 签名。



## 9 导入签名证书。

- a 复制签名证书的内容。
- b 执行以下操作之一。
  - 要在全局级别导入签名证书，请在 NSX Manager Virtual Appliance 设备中单击**导入 (Import)**。
  - 要导入 NSX Edge 的签名证书，请在**证书 (Certificates)**选项卡中单击**操作 (Actions)**并选择**导入证书 (Import Certificate)**。
- c 在“导入 CSR”对话框中，粘贴签名证书的内容。
- d 单击**确定 (OK)**。

此时 CA 签名证书将显示在证书列表中。

### 添加 CA 证书

通过添加 CA 证书，您可以成为公司的临时 CA。然后，您就有权签署自己的证书。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后确保您处于**设置 (Settings)**选项卡中。
- 5 单击**证书 (Certificates)**。
- 6 单击**添加 (Add)** () 图标并选择 **CA 证书 (CA Certificate.)**。
- 7 将证书内容复制并粘贴到“证书内容”文本框中。
- 8 键入 CA 证书的描述。
- 9 单击**确定 (OK)**。

您现在可以对自己的证书进行签名。

### 配置自签名证书

可以创建、安装和管理自签名服务器证书。

#### 前提条件

确认您具有 CA 证书，以便可以签署自己的证书。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理**选项卡，然后确保您处于**设置**选项卡中。

5 单击**证书**。

6 按照以下步骤生成 CSR。

- a 单击**操作**，然后选择**生成 CSR**。
- b 在“公用名称”中，键入 NSX Manager 的 IP 地址或完全限定域名 (FQDN)。
- c 键入组织名称和单位。
- d 键入组织的地点、街道、省/市/自治区和国家/地区。
- e 为主机之间的通信选择加密算法。

请注意，SSL VPN-Plus 仅支持 RSA 证书。VMware 建议选择 RSA 以实现向后兼容性。

- f 根据需要编辑默认密钥大小。
- g 键入证书描述。
- h 单击**确定**。

CSR 将生成并显示在“证书”列表中。

7 验证是否已选中生成的证书。

8 单击**操作**，然后选择**自签名证书**。

9 键入自签名证书的有效天数。

10 单击**确定**。

## 使用客户端证书

您可以通过 CAI 命令或 REST 调用创建客户端证书。随后，您可以将此证书分发给您的远程用户，他们可以将证书安装在其 Web 浏览器上。

实施客户端证书的主要优势在于，可以存储每个远程用户各自的引用客户端证书，并对照远程用户提供的客户端证书检查该证书。为防止特定用户以后连接服务器，可以将引用证书从安全服务器的客户端证书列表中删除。删除证书即拒绝与该用户连接。

## 添加证书吊销列表

证书吊销列表 (CRL) 是订阅者及其状态的列表，由 Microsoft 提供并签名。

该列表包含以下各项：

- 已吊销证书以及吊销原因
- 证书颁发日期
- 颁发证书的实体
- 计划发行下一个版本的日期

当潜在用户尝试访问服务器时，服务器会根据该特定用户所对应的 CRL 条目允许或拒绝访问。

**步骤**

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后确保您处于**设置 (Settings)**选项卡中。
- 5 单击**证书 (Certificates)**。
- 6 单击**添加 (Add)** () 图标，然后选择 **CRL**。
- 7 在**证书内容 (Certificate contents)**中粘贴列表。
- 8 （可选）键入描述。
- 9 单击**确定 (OK)**。

**管理设备**

可以添加、编辑或删除设备。NSX Edge 实例将一直保持脱机状态，直至向其添加至少一个设备。

**添加设备**

在部署前必须向 NSX Edge 至少添加一个设备。

**步骤**

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击**设置 (Settings)**选项卡。
- 5 在 **Edge 网关设备 (Edge Gateway Appliances)**中，单击**添加 (Add)** () 图标。
- 6 为设备选择群集或资源池和数据存储。
- 7 （可选）选择设备将添加到的主机。
- 8 （可选）选择设备将添加到的 vCenter 文件夹。
- 9 单击**添加 (Add)**。

**编辑设备**

可以编辑 NSX Edge 设备。

**步骤**

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。

- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击**设置 (Settings)**选项卡。
- 5 在 **Edge 网关设备 (Edge Gateway Appliances)**中，选择要更改的设备。
- 6 单击**编辑 (Edit)** () 图标。
- 7 在“编辑 Edge 设备”对话框中，进行适当的更改。
- 8 单击**保存 (Save)**。

## 删除设备

可以删除 NSX Edge 设备。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击**设置 (Settings)**选项卡。
- 5 在 **Edge 网关设备 (Edge Gateway Appliances)**中，选择要删除的设备。
- 6 单击**删除 (Delete)** () 图标。

## 使用接口

NSX Edge 服务网关最多可以有十个内部接口、上行链路接口、或中继接口。一个 NSX Edge 路由器可以有八个上行链路接口，以及多达一千个内部接口。

一个 NSX Edge 必须至少有一个内部接口才可以对其进行部署。

## 配置接口

总体来讲，内部接口用于东西向流量，而上行链路接口则用于南北向流量。当逻辑路由器 (DLR) 连接到 Edge 服务网关 (ESG) 时，路由器上的接口为上行链路接口，而 ESG 上的接口为内部接口。NSX 中继接口适用于内部网络，而不适用于外部网络。中继接口允许中继多个内部网络 (VLAN 或 VXLAN)。

NSX Edge 服务网关 (ESG) 最多可以有十个内部接口、上行链路接口或中继接口。这些限制由 NSX Manager 强制实施。

NSX 部署可以在单个 ESXi 主机上拥有多达 1000 个分布式逻辑路由器 (DLR) 实例。在单个逻辑路由器上，您可以配置多达 8 个上行链路接口以及多达 991 个内部接口。这些限制由 NSX Manager 强制实施。有关 NSX 部署中接口扩展的详细信息，请参见 <https://communities.vmware.com/docs/DOC-27683> 上的《VMware® NSX for vSphere 网络虚拟化设计指南》。

### 步骤

- 1 登录到 vSphere Web Client。

- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击**接口 (Interfaces)**选项卡。
- 5 选择接口并单击**编辑 (Edit)** () 图标。
- 6 在“编辑 Edge 接口”对话框中，键入接口的名称。
- 7 选择**内部 (Internal)**或**上行链路 (Uplink)**以指示其是内部还是外部接口。  
在创建子接口时，选择**中继 (Trunk)**。有关详细信息，请参见[添加子接口](#)。
- 8 选择该接口应连接到的端口组或逻辑交换机。
  - a 单击**已连接到 (Connected To)**字段旁边的**选择 (Select)**。
  - b 根据要连接到接口的对象，单击**逻辑交换机 (Logical Switch)**、**标准端口组 (Standard Portgroup)**或**分布式端口组 (Distributed Portgroup)**选项卡。
  - c 选择相应的逻辑交换机或端口组。
  - d 单击**选择 (Select)**。
- 9 选择接口的连接状态。
- 10 在**配置子网 (Configure Subnets)**中，单击**添加 (Add)** () 图标，以便为接口添加子网。  
一个接口可以具有多个非重叠的子网。
- 11 在**添加子网 (Add Subnet)**中，单击**添加 (Add)** () 图标以添加 IP 地址。  
如果输入多个 IP 地址，则可以选择主 IP 地址。一个接口可以具有一个主 IP 地址和多个辅助 IP 地址。  
NSX Edge 将主 IP 地址视为本地生成的流量的源地址。  
必须将 IP 地址添加到接口，才能在所有功能配置中使用该地址。
- 12 为接口键入子网掩码，然后单击**保存 (Save)**。
- 13 根据需要更改默认 MTU。
- 14 在**选项 (Options)**中，选择所需的选项。

| 选项          | 说明                                                                       |
|-------------|--------------------------------------------------------------------------|
| 启用代理 ARP    | 支持在不同的接口之间重叠网络转发。                                                        |
| 发送 ICMP 重定向 | 将路由信息传输给主机。                                                              |
| 反向路径筛选器     | 验证正转发的数据包中源地址的可访问性。在启用模式下，必须在路由器将用来转发返回数据包的接口上接收数据包。在宽松模式下，源地址必须显示在路由表中。 |

- 15 键入防护参数，然后单击**添加 (Add)**。
- 16 单击**确定 (OK)**。

## 删除接口

可以删除 NSX Edge 接口。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击**接口 (Interfaces)**选项卡。
- 5 选择要删除的接口。
- 6 单击**删除 (Delete)** () 图标。

## 启用接口

必须为 NSX Edge 启用接口才能隔离该接口（端口组或逻辑交换机）内的虚拟机。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击**接口 (Interfaces)**选项卡。
- 5 选择要启用的接口。
- 6 单击**启用 (Enable)** () 图标。

## 禁用接口

您可以在 NSX Edge 上禁用接口。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击**接口 (Interfaces)**选项卡。
- 5 选择要禁用的接口。
- 6 单击**禁用 (Disable)**图标。

## 更改流量调整策略

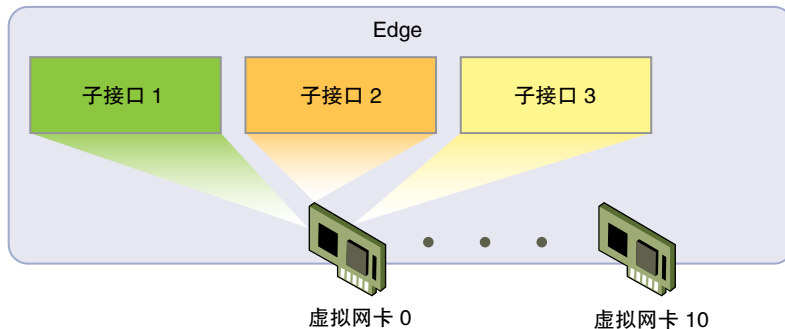
可以在 vSphere Distributed Switch 上为 NSX Edge 接口更改流量调整策略。

## 步骤

- 1 双击一个 NSX Edge，然后导航到**管理 (Manage) > 设置 (Settings) > 接口 (Interfaces)**。
- 2 选择一个接口。
- 3 单击**操作 (Actions) > 配置流量调整策略 (Configure Traffic Shaping Policy)**。
- 4 进行适当更改。  
有关选项的详细信息，请参见[流量调整策略](#)。
- 5 单击**确定 (OK)**。

## 添加子接口

可以在中继虚拟网卡上添加子接口，该接口随后可用于 NSX Edge 服务。



中继接口可以为以下类型：

- VLAN 中继是标准的，且适用于任何版本的 ESXi。它用于将标记的 VLAN 流量带入 Edge 中。
- VXLAN 中继仅适用于 NSX 版本 6.1。它用于将 VXLAN 流量带入 Edge 中。

子接口可用于以下 Edge 服务：

- DHCP
- 路由（仅 BGP）
- 负载均衡器
- IPSEC VPN
- L2 VPN

子接口不能用于 HA 或逻辑防火墙。但是，可以在防火墙规则中使用子接口的 IP 地址。

## 步骤

- 1 在 NSX Edge 的**管理 > 设置**选项卡中，单击**接口**。
- 2 选择接口并单击**编辑** (✎) 图标。
- 3 在“编辑 Edge 接口”对话框中，键入接口的名称。
- 4 在“类型”中，选择**中继**。

5 选择该接口应连接到的标准端口组或分布式端口组。

- a 单击**已连接到**字段旁边的**更改**。
- b 根据要连接到接口的对象，单击**标准端口组**或**分布式端口组**选项卡。
- c 选择相应的端口组，然后单击**确定**。
- d 单击**选择**。

6 在“子接口”中，单击**添加**图标。

7 单击**启用子接口**，然后键入子接口的名称。

8 在**隧道 ID** 中，键入一个介于 1 和 4094 之间的数字。

隧道 ID 用于连接要延伸的网络。客户端站点和服务站点上的该值必须相同。

9 在“备用类型”中，选择以下选项之一以指示支持子接口的网络。

- **VLAN**，表示 VLAN 网络。

键入子接口应使用的虚拟 LAN 的 VLAN ID。VLAN ID 的范围可以为 0 到 4094。

- **网络**，表示 VLAN 或 VXLAN 网络。

单击**选择**，然后选择分布式端口组或逻辑交换机。NSX Manager 将提取 VLAN ID，并用于中继配置。

- **无**，用于在不指定网络或 VLAN ID 的情况下创建子接口。该子接口是 NSX Edge 的内部接口，用于在延伸网络和未延伸（未标记）网络之间路由数据包。

10 要将子网添加到子接口，请单击“配置子网”区域中的**添加**图标。

11 在“添加子网”中，单击**添加**图标以添加 IP 地址。键入 IP 地址，然后单击**确定**。

如果输入多个 IP 地址，则可以选择主 IP 地址。一个接口可以具有一个主 IP 地址和多个辅助 IP 地址。NSX Edge 将主 IP 地址视为本地生成的流量的源地址。

12 键入子网前缀长度，然后单击**确定**。

13 根据需要编辑子接口的默认 MTU 值。

中继接口的默认 MTU 为 1600，而子接口的默认 MTU 为 1500。子接口的 MTU 应等于或小于 NSX Edge 的所有中继接口中的最低 MTU。

14 选择**启用发送重定向**，以将路由信息传输给主机。

15 为接口键入 MAC 地址。

由于子接口不支持 HA，仅需一个 MAC 地址。

16 根据需要编辑中继接口的默认 MTU。

17 单击**确定**。

现在即可在 Edge 服务上使用子接口。

#### 后续步骤

如果标准端口组支持添加到中继 vNic 的子接口，请配置 VLAN 中继。请参见[配置 VLAN 中继](#)。



## 配置 VLAN 中继

将子接口添加到分布式端口组支持的中继虚拟网卡时，会在中继端口上自动配置 VLAN 或 VXLAN 中继。将子接口添加到标准端口组支持的中继虚拟网卡时，仅支持 VLAN 中继。

### 前提条件

确认具有标准端口组支持的中继 vNic 的子接口可用。请参见[添加子接口](#)。


### 步骤

- 1 登录到 vCenter Web Client。
- 2 单击**网络 (Networking)**。
- 3 选择标准端口组，然后单击**编辑设置 (Edit Settings)**。
- 4 单击 **VLAN** 选项卡。
- 5 在“VLAN 类型”中，选择“VLAN 中继”，然后键入要中继的 VLAN ID。
- 6 单击**确定 (OK)**。

## 更改自动规则配置

如果已启用自动规则生成，NSX Edge 将添加防火墙、NAT 和路由，以启用对这些服务流量的控制。如果未启用自动规则生成，则必须手动添加防火墙、NAT 和路由配置，以便控制负载平衡、VPN 等 NSX Edge 服务的通道流量。

### 步骤


- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**监控**选项卡，然后单击**设置**选项卡。
- 5 单击**更多操作** () 图标并选择**更改自动规则配置**。
- 6 进行相应更改，然后单击**确定**。

## 更改 CLI 凭据

可以编辑用于登录命令行界面 (CLI) 的凭据。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。

- 4 单击**监控**选项卡，然后单击**设置**选项卡。
- 5 单击**更多操作** () 图标并选择**更改 CLI 凭据**。
- 6 进行适当编辑。
- 7 单击**确定**。

## 关于高可用性

高可用性 (HA) 确保 NSX Edge 设备提供的服务可用，即使硬件或软件故障导致单个设备不可用。NSX Edge HA 最大限度减少故障切换停机时间，而不是提供零停机时间，因为设备之间的故障切换可能需要重新启动某些服务。

例如，NSX Edge HA 同步有状态防火墙的连接跟踪器或负载均衡器保存的有状态信息。备份所有服务所需的时间不为零。已知的服务重新启动影响示例包括，在 NSX Edge 作为路由器运行时具有动态路由的非零停机时间。

有时，两个 NSX Edge HA 设备无法通信，并单方面决定变为活动状态。这是预期的行为，以便在备用 NSX Edge 不可用时保持活动 NSX Edge 服务的可用性。如果另一个设备仍然存在，在重新建立通信时，两个 NSX Edge HA 设备重新协商活动和备用状态。如果没有完成该协商，并且两个设备在重新建立连接时都宣称处于活动状态，则会观察到意外行为。观察到这种情况（称为脑裂）是由于以下环境条件造成的：

- 物理网络连接问题，包括网络分区。
- NSX Edge 上的 CPU 或内存争用。
- 可能导致至少一个 NSX Edge HA 虚拟机变得不可用的临时存储问题。

例如，从过度置备的存储中移走虚拟机时，将观察到 NSX Edge HA 稳定性和性能提高。特别是，在较大的通宵备份期间，较大的存储延迟峰值可能会影响 NSX Edge HA 稳定性。

- 数据包交换涉及的物理或虚拟网络适配器上的拥塞。

除了环境问题以外，在 HA 配置引擎变为错误状态或 HA 守护进程失败时，将会观察到裂脑情况。

## 有状态高可用性

主 NSX Edge 设备处于活动状态，辅助设备处于待机状态。NSX Edge 为备用设备复制主设备的配置，您也可以手动添加两个设备。VMware 建议您在单独的资源池和数据存储上创建主设备和辅助设备。如果将主设备和辅助设备创建在同一数据存储上，则数据存储必须在群集的所有主机间共享，以便将 HA 设备对部署在不同的 ESX 主机上。如果数据存储为本地存储器，则两个虚拟机均部署在同一主机上。

所有 NSX Edge 服务均在活动设备上运行。主设备会维护备用设备的检测信号，并通过内部接口发送服务更新。

如果未在指定的时间内（默认值为 15 秒）收到主设备的检测信号，则主设备会被声明为已停止运行。备用设备进入活动状态，接管主设备的界面配置，然后启动先前在主设备上运行的 NSX Edge 服务。发生切换时，会在“设置和报告”的**系统事件 (System Events)**选项卡中显示一个系统事件。负载均衡器和 VPN 服务需重新建立与 NSX Edge 的 TCP 连接，所以将出现短时间的服务中断。逻辑交换机连接和防火墙会话在主设备和备用设备之间进行同步，所以切换期间不会出现服务中断。

如果 NSX Edge 设备发生故障并报告错误状态，HA 将强制同步发生故障的设备以恢复该设备。恢复后，该设备具备当前活动设备的配置，并保持待机状态。如果 NSX Edge 设备已停止运行，您必须删除该设备，然后添加新设备。

NSX Edge 可确保即使在您使用 DRS 和 vMotion 之后，两个 HA NSX Edge 虚拟机也不在同一个 ESX 主机上（除非以手动方式通过 vMotion 将二者移至同一个主机）。两个虚拟机都在 vCenter 上部署，与您配置的设备处于同一资源池和数据存储中。将为 NSX Edge HA 中的 HA 虚拟机分配本地链路 IP，以便它们能够进行通信。您可以指定用于替代本地链接的管理 IP 地址。

如果配置了 syslog 服务器，则活动设备上的日志将发送到 syslog 服务器。

## vSphere High Availability

NSX Edge HA 与 vSphere HA 兼容。如果运行 NSX Edge 实例的主机停止运行，则 NSX Edge 会在备用主机上重新启动，从而确保 NSX Edge HA 对仍可以再进行一次故障切换。

如果未利用 vSphere HA，则处于活动状态的备用 NSX Edge HA 对在一次故障切换后仍将处于活动状态。但是，如果在还原第二个 HA 对之前再次出现故障切换，则将危及 NSX Edge 的可用性。

有关 vSphere HA 的详细信息，请参见《vSphere 可用性》。

## 更改高可用性配置

可以更改在安装 NSX Edge 时指定的 HA 配置。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击**设置 (Settings)**选项卡。
- 5 在**HA 配置 (HA Configuration)**面板中，单击**更改 (Change)**。
- 6 在“更改 HA 配置”对话框中，根据需要进行更改。

---

**注** 如果在启用 HA 之前此 Edge 设备上配置了 L2 VPN，则必须至少设置两个内部接口。如果在此 Edge 上配置了一个已由 L2 VPN 使用的接口，则会在 Edge 设备上禁用 HA。

---

- 7 单击**确定 (OK)**。

## 使用 NSX Manager 对 NSX Edge 执行强制同步

可以从 NSX Manager 向 NSX Edge 发送一个同步请求。

当您需要将 NSX Manager 已知的 Edge 配置同步到所有组件时，要使用强制同步。

---

**注** 对于 6.2 及更高版本，强制同步可以避免东西向路由流量的数据损失，但南北向路由和桥接可能会出现中断。

---

强制同步将导致执行以下操作：


- Edge 设备重新引导，并应用最新配置
- 与主机的连接关闭
- 如果 NSX Manager 是主 NSX Manager 或独立 NSX Manager，且 Edge 是逻辑分布式路由器，则同步控制器群集
- 将向所有相关主机发送消息，以同步分布式路由器实例

---

**重要** 在跨 vCenter NSX 环境中，您必须先在主 NSX Manager 上强制同步 NSX Edge 实例，完成后在辅助 NSX Manager 上强制同步 NSX Edge 实例。

---

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 选择一个 NSX Edge 实例。
- 4 单击**更多操作 (More Actions)** () 图标并选择**强制同步 (Force Sync)**。

## 配置远程 Syslog 服务器

您可以配置一个或两个远程 syslog 服务器。与从 NSX Edge 设备流出的防火墙事件相关联的 NSX Edge 事件和日志发送到 syslog 服务器。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击 NSX Edge。
- 4 单击**监控 (Monitor)**选项卡，然后单击**设置 (Settings)**选项卡。
- 5 在**详细信息 (Details)**面板中，单击 Syslog 服务器旁边的**更改 (Change)**。
- 6 键入这两个远程 syslog 服务器的 IP 地址并选择协议。
- 7 单击**确定 (OK)**保存配置。

## 查看 NSX Edge 的状态

状态页将显示流过所选 NSX Edge 的接口的流量的流量图，以及防火墙与负载均衡器服务的连接统计信息。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。

- 4 单击**监控 (Monitor)**选项卡。
- 5 选择要查看统计信息的时间段。

#### 后续步骤

要查看有关 NSX Edge 的详细信息，请单击**管理 (Manage)**，然后单击**设置 (Settings)**。

## 重新部署 NSX Edge

如果强制同步后 NSX Edge 服务未按预期运行，您可以重新部署 NSX Edge 实例。

---

**注** 重新部署是一种破坏性操作。建议您首先应用强制同步，如果问题没能解决，再进行重新部署。

---

重新部署 NSX Edge 实例将导致执行以下操作：

- 删除 Edge 设备，并使用应用的最新配置进行全新部署
- 从控制器中删除逻辑路由器，然后使用应用的最新配置重新创建
- 删除主机上的分布式逻辑路由器实例，然后使用应用的最新配置重新创建

如果未启用正常重新启动，将在重新部署期间撤消 OSPF 邻接。

---

**重要** 在跨 vCenter 环境中，您必须先在主 NSX Manager 上重新部署 NSX Edge 实例，然后在辅助 NSX Manager 上重新部署 NSX Edge 实例。需要重新部署主 NSX Manager 和辅助 NSX Manager。

---

#### 前提条件

确认主机在重新部署期间具有足够的资源以部署额外的 NSX Edge 服务网关设备。有关每个 NSX Edge 大小所需的资源，请参见第 1 章，**NSX 的系统要求**。

- 对于单个 NSX Edge 实例，在重新部署期间具有两个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。
- 从 NSX 6.2.3 开始，在重新部署具有 HA 的 NSX Edge 实例时，将在更换旧设备之前部署两个更换设备。这意味着，在升级给定的 NSX Edge 期间，将具有四个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。在重新部署 NSX Edge 实例后，任一 HA 设备可能会变为活动状态。
- 在 NSX 6.2.3 之前，在重新部署具有 HA 的 NSX Edge 实例时，仅在更换旧设备时部署一个更换设备。这意味着，在重新部署给定的 NSX Edge 期间，将具有三个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。在重新部署 NSX Edge 实例后，通常具有 HA 索引 0 的 NSX Edge 设备变为活动状态。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**NSX Edge (NSX Edges)**。
- 3 选择一个 NSX Edge 实例。
- 4 单击**操作 (Actions)** (  ) 图标并选择**重新部署 Edge (Redeploy Edge)**。

NSX Edge 虚拟机会替换为新的虚拟机，所有的服务都将还原。如果重新部署不起作用，请关闭 NSX Edge 虚拟机的电源，然后再次重新部署 NSX Edge。

**注** 在以下情况中重新部署可能不起作用。


- 安装有 NSX Edge 的资源池不再存在于 vCenter 清单中，或其受管对象 ID (Mold) 已更改。
- 安装有 NSX Edge 的数据存储已损坏/已卸载或不可访问。
- 连接 NSX Edge 接口的 dvportGroup 不再存在于 vCenter 清单中，或其 Mold (vCenter Server 中的标识符) 已更改。

如果发生以上任一情况，您必须使用 REST API 调用来更新资源池、数据存储或 dvPortGroup 的 Mold。请参见《NSX API 编程指南》。

## 下载 NSX Edge 的技术支持日志

可以为每个 NSX Edge 实例下载技术支持日志。如果已为 NSX Edge 实例启用高可用性，则将从两个 NSX Edge 虚拟机下载技术支持日志。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**NSX Edge (NSX Edges)**。
- 3 选择一个 NSX Edge 实例。
- 4 单击**更多操作** () 图标并选择**下载技术支持日志**。
- 5 生成技术支持日志后，单击**下载**。
- 6 在“选择下载位置”对话框中，浏览至要保存该日志文件的目录。
- 7 单击**保存**。
- 8 单击**关闭**。

## 添加静态路由

可以为目标子网或主机添加静态路由。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击**路由 (Routing)**选项卡。
- 5 从左侧面板中选择**静态路由 (Static Routes)**。
- 6 单击**添加 (Add)** () 图标。

7 采用 CIDR 表示法键入**网络 (Network)**。

8 键入**下一跃点 (Next Hop)**的 IP 地址。

路由器必须能够直接到达下一跃点。

如果启用 ECMP，可以键入多个下一跃点。

9 选择要添加静态路由的**接口 (Interface)**。

10 对于 **MTU**，编辑数据包的最大传输值（如果需要）。

该 MTU 不能高于 NSX Edge 接口上设置的 MTU。

11 如果出现提示，请键入**管理员距离 (Admin Distance)**。

选择一个介于 1 和 255 之间的值。当给定网络具有多个路由时，可根据管理员距离选择要使用的路由。管理员距离越小，就越优先选择相应路由。

**表 9-2. 默认管理员距离**

| 路由源      | 默认管理员距离 |
|----------|---------|
| 已连接      | 0       |
| 静态       | 1       |
| 外部 BGP   | 20      |
| OSPF 区域内 | 30      |
| OSPF 区域外 | 110     |
| 内部 BGP   | 200     |

如果管理距离为 255，会导致静态路由从路由表 (RIB) 和数据层面删除，从而不使用静态路由。

12 （可选）键入**区域设置 ID (Locale ID)**。

默认情况下，路由与 NSX Manager 具有相同的区域设置 ID。在此指定区域设置 ID 会将路由与此区域设置 ID 相关联。这些路由将仅发送到具有匹配区域设置 ID 的主机。有关详细信息，请参见[跨 vCenter NSX 拓扑](#)。

13 （可选）键入静态路由的**描述 (Description)**。

14 单击**确定 (OK)**。

## 在逻辑（分布式）路由器上配置 OSPF

在逻辑路由器上配置 OSPF 可以启用逻辑路由器之间的虚拟机连接，以及从逻辑路由器到 Edge 服务网关 (ESG) 的虚拟机连接。

OSPF 路由策略用于在成本相同的路由之间动态进行流量负载平衡。

一个 OSPF 网络分为多个路由区域，以优化流量并限制路由表的大小。区域是具有相同区域标识的 OSPF 网络、路由器和链路的逻辑集合。

区域由区域 ID 进行标识。



## 前提条件

必须如**示例：在逻辑（分布式）路由器上配置的 OSPF**所示配置路由器 ID。

启用路由器 ID 后，该字段会默认填充逻辑路由器的上行链路接口。

## 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击逻辑路由器。
- 4 单击**路由 (Routing)**，然后单击 **OSPF**。
- 5 启用 OSPF。
  - a 单击窗口右上角的**编辑 (Edit)**，然后单击**启用 OSPF (Enable OSPF)**
  - b 在**转发地址 (Forwarding Address)**中，键入主机中路由器数据路径模块用来转发数据路径数据包的 IP 地址。
  - c 在**协议地址 (Protocol Address)**中，键入与**转发地址 (Forwarding Address)**位于同一个子网中的唯一 IP 地址。协议地址由协议使用，以与对等方相邻。
- 6 配置 OSPF 区域。
  - a 也可以选择删除默认配置的次末节区域 (NSSA) 51。
  - b 在**区域定义 (Area Definitions)**中，单击**添加 (Add)**图标。
  - c 键入区域 ID。NSX Edge 支持 IP 地址或十进制数字形式的区域 ID。
  - d 在**类型 (Type)**中，选择**正常 (Normal)**或 **NSSA**。  
 NSSA 会阻止 AS 外部链接状态通告 (LSA) 涌入 NSSA。它们依赖于到外部目标的默认路由。因此，必须将 NSSA 放在 OSPF 路由域的边缘。NSSA 可将外部路由导入到 OSPF 路由域中，从而为未包含在 OSPF 路由域中的小型路由域提供传输服务。
- 7 （可选）选择**身份验证 (Authentication)**的类型。OSPF 在区域级执行身份验证。  
 该区域内的所有路由器都必须配置相同的身份验证和对应的密码。要使 MD5 身份验证生效，接收和传输路由器必须具有相同的 MD5 密钥。
  - a **无 (None)**：不需要身份验证（默认值）。
  - b **密码 (Password)**：在此身份验证方法中，传输的数据包中包括密码。
  - c **MD5**：此身份验证方法使用 MD5（消息摘要类型 5）加密。传输的数据包中包括 MD5 校验和。
  - d 对于**密码 (Password)**或 **MD5**类型的身份验证，键入密码或 MD5 密钥。



## 8 映射区域的接口。

- a 在**接口映射的区域 (Area to Interface Mapping)**中，单击**添加 (Add)**图标以映射属于 OSPF 区域的接口。
- b 选择要映射的接口及其要映射到的 OSPF 区域。

## 9 （可选）如有需要，编辑默认 OSPF 设置。

在大多数情况下，建议保留默认 OSPF 设置。如果不更改设置，确保 OSPF 对等方使用相同的设置。

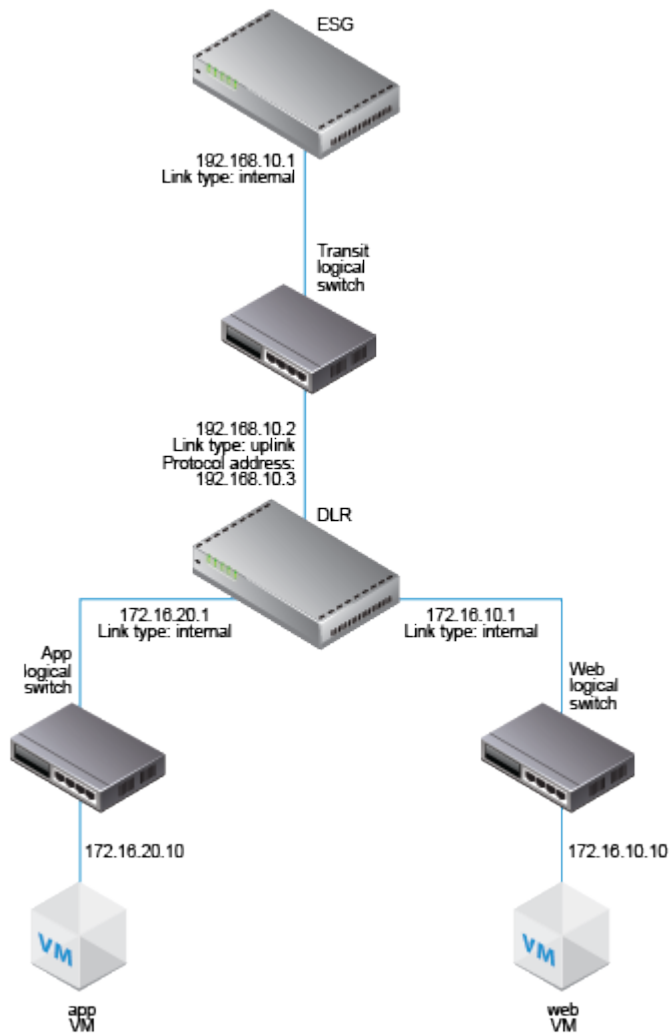
- a **通信时间间隔 (Hello Interval)**显示在接口上发送的两个通信数据包之间的默认时间间隔。
- b **失效时间间隔 (Dead Interval)**显示默认时间间隔，在该时间间隔内，路由器必须在声明邻居已关闭之前至少从该邻居接收到一个通信数据包。
- c **优先级 (Priority)**显示接口的默认优先级。优先级最高的接口是指定的路由器。
- d 接口的**成本 (Cost)**显示通过该接口发送数据包所需的默认开销。接口的成本与该接口的带宽成反比。带宽越宽，成本越低。

## 10 单击**发布更改 (Publish Changes)**。

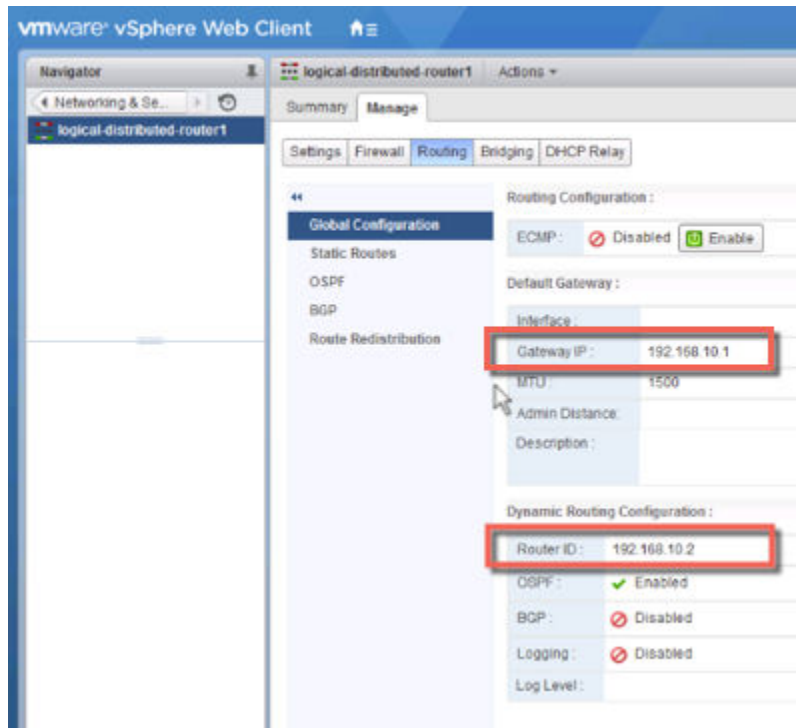
## 示例：在逻辑（分布式）路由器上配置的 OSPF

使用 OSPF 的一个简单 NSX 应用场景是当逻辑路由器 (DLR) 和 Edge 服务网关 (ESG) 是 OSPF 邻居时，如下图所示。

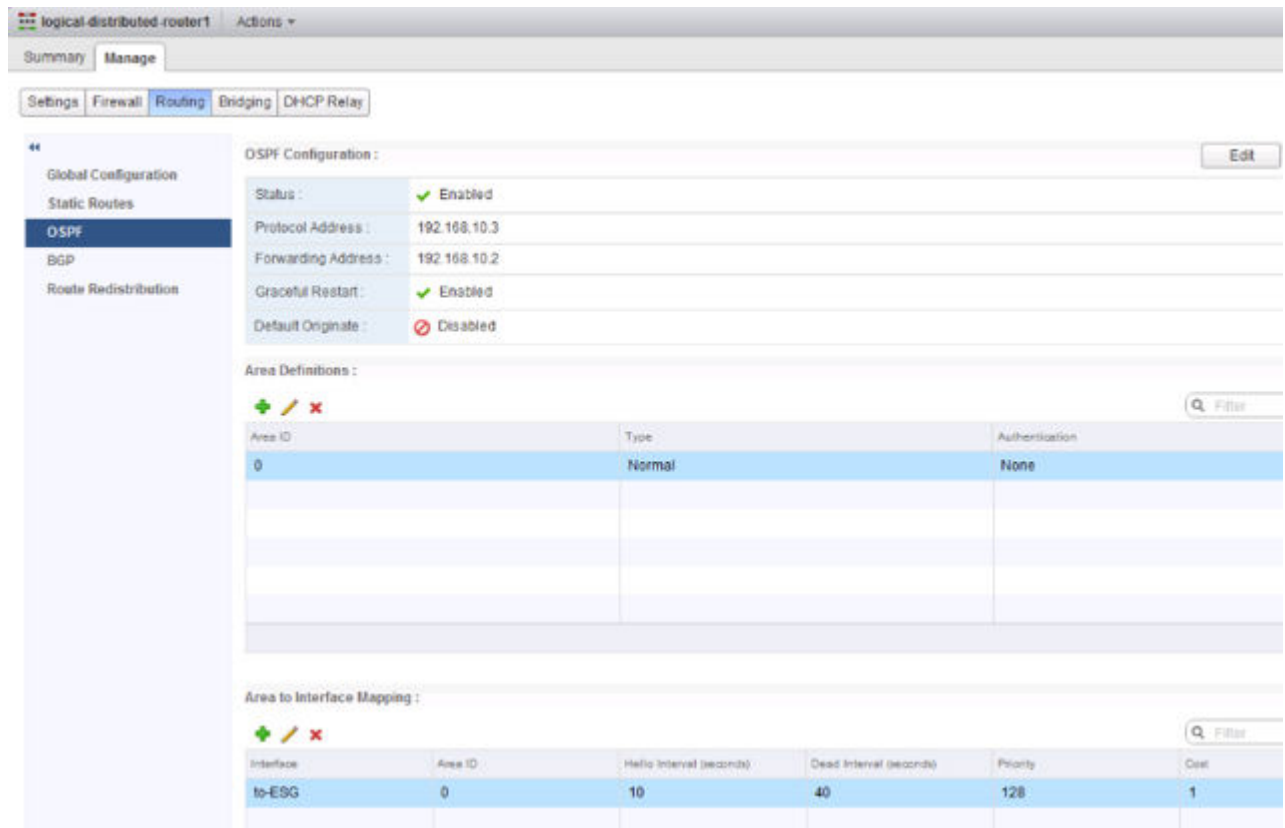
图 9-1. NSX 拓扑



在下面的屏幕中，逻辑路由器的默认网关是 ESG 的内部接口 IP 地址 (192.168.10.1)。路由器 ID 是逻辑路由器的上行链路接口，即，面向 ESG 的 IP 地址 (192.168.10.2)。



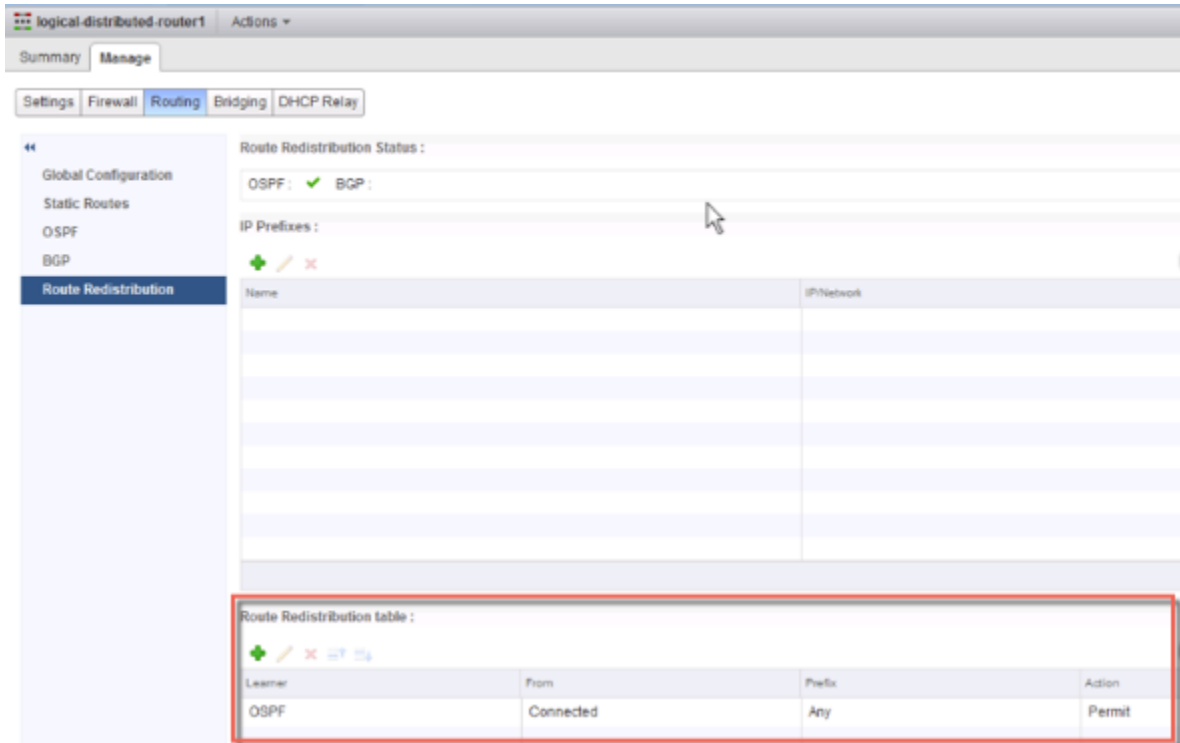
逻辑路由器配置使用 192.168.10.2 作为其转发地址。协议地址可以是位于同一个子网中并且未在其他位置使用的任何 IP 地址。在本例中，配置了 192.168.10.3。配置的区域 ID 为 0，上行链路接口（面向 ESG 的接口）映射到该区域。



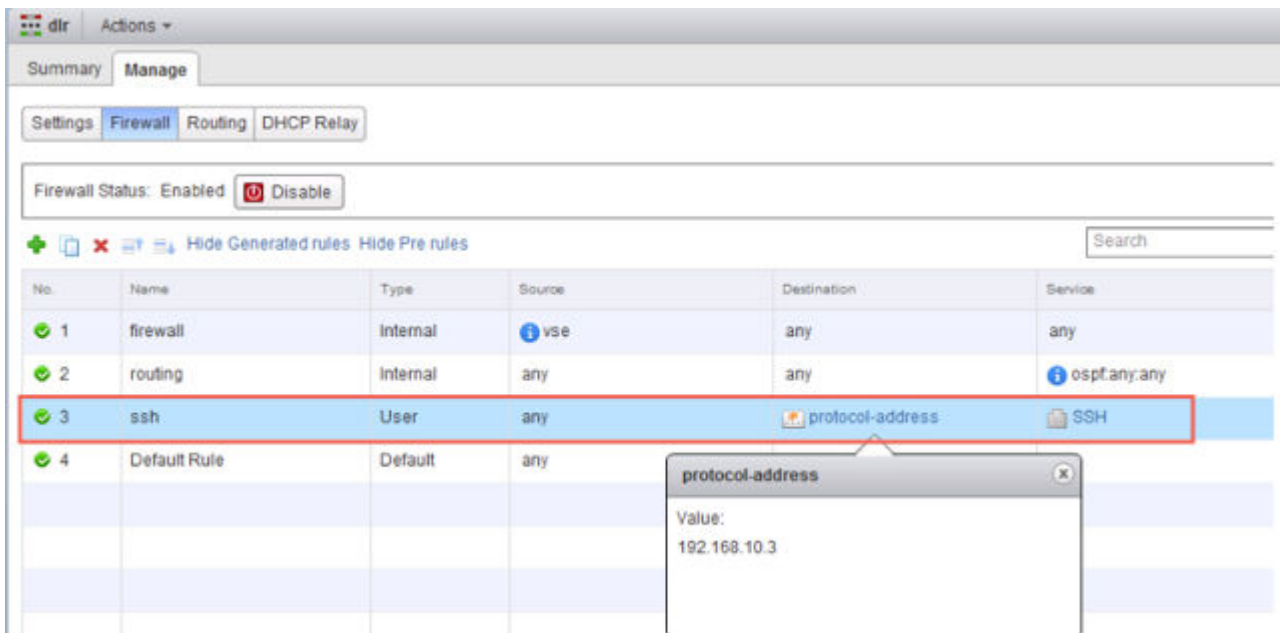
## 后续步骤

确保路由重新分布和防火墙配置允许播发正确的路由。

在本例中，逻辑路由器连接的路由（172.16.10.0/24 和 172.16.20.0/24）播发到 OSPF 中。



如果在创建逻辑路由器时启用了 SSH，还必须配置一个防火墙筛选器，以允许通过 SSH 方式连接到逻辑路由器的协议地址。例如：



## 在 Edge 服务网关上配置 OSPF

在 Edge 服务网关 (ESG) 上配置 OSPF 可以使 ESG 获知和播发路由。OSPF 在 ESG 上最常见的应用是在位于 ESG 与逻辑（分布式）路由器之间的链接上。这样 ESG 即可获知连接到逻辑路由器的逻辑接口 (LIFS)。此目标可以借助 OSPF、IS-IS、BGP 或静态路由来实现。

OSPF 路由策略用于在成本相同的路由之间动态进行流量负载平衡。

一个 OSPF 网络分为多个路由区域，以优化流量并限制路由表的大小。区域是具有相同区域标识的 OSPF 网络、路由器和链路的逻辑集合。

区域由区域 ID 进行标识。

### 前提条件

必须如**示例：在 Edge 服务网关上配置的 OSPF**所示配置路由器 ID。

启用路由器 ID 后，该字段默认填入 ESG 的上行链路接口 IP 地址。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 ESG。
- 4 单击**路由 (Routing)**，然后单击 **OSPF**。
- 5 启用 OSPF。
  - a 单击窗口右上角的**编辑 (Edit)**，然后单击**启用 OSPF (Enable OSPF)**
  - b （可选）单击**启用正常重新启动 (Enable Graceful Restart)**，确保在重新启动 OSPF 服务期间不会中断数据包转发。
  - c （可选）单击**启用默认源 (Enable Default Originate)**，允许 ESG 将其自身作为默认网关播发给其对等方。
- 6 配置 OSPF 区域。
  - a （可选）删除默认配置的次末节区域 (NSSA) 51。
  - b 在**区域定义 (Area Definitions)**中，单击**添加 (Add)**图标。
  - c 键入区域 ID。NSX Edge 支持 IP 地址或十进制数字形式的区域 ID。
  - d 在**类型 (Type)**中，选择**正常 (Normal)**或 **NSSA**。

NSSA 会阻止 AS 外部链接状态通告 (LSA) 涌入 NSSA。它们依赖于到外部目标的默认路由。因此，必须将 NSSA 放在 OSPF 路由域的边缘。NSSA 可将外部路由导入到 OSPF 路由域中，从而为未包含在 OSPF 路由域中的小型路由域提供传输服务。

## 7 （可选）选择身份验证 (Authentication) 的类型。OSPF 在区域级执行身份验证。

该区域内的所有路由器都必须配置相同的身份验证和对应的密码。要使 MD5 身份验证生效，接收和传输路由器必须具有相同的 MD5 密钥。

- a 无 (None): 不需要身份验证 (默认值)。
- b 密码 (Password): 在此身份验证方法中，传输的数据包中包括密码。
- c MD5: 此身份验证方法使用 MD5 (消息摘要类型 5) 加密。传输的数据包中包括 MD5 校验和。
- d 对于密码 (Password) 或 MD5 类型的身份验证，键入密码或 MD5 密钥。

## 8 映射区域的接口。

- a 在接口映射的区域 (Area to Interface Mapping) 中，单击添加 (Add) 图标以映射属于 OSPF 区域的接口。
- b 选择要映射的接口及其要映射到的 OSPF 区域。

## 9 （可选）编辑默认 OSPF 设置。

在大多数情况下，建议保留默认 OSPF 设置。如果不更改设置，确保 OSPF 对等方使用相同的设置。

- a 通信时间间隔 (Hello Interval) 显示在接口上发送的两个通信数据包之间的默认时间间隔。
- b 失效时间间隔 (Dead Interval) 显示默认时间间隔，在该时间间隔内，路由器必须在声明邻居已关闭之前至少从该邻居接收到一个通信数据包。
- c 优先级 (Priority) 显示接口的默认优先级。优先级最高的接口是指定的路由器。
- d 接口的成本 (Cost) 显示通过该接口发送数据包所需的默认开销。接口的成本与该接口的带宽成反比。带宽越宽，成本越低。

## 10 单击发布更改 (Publish Changes)。

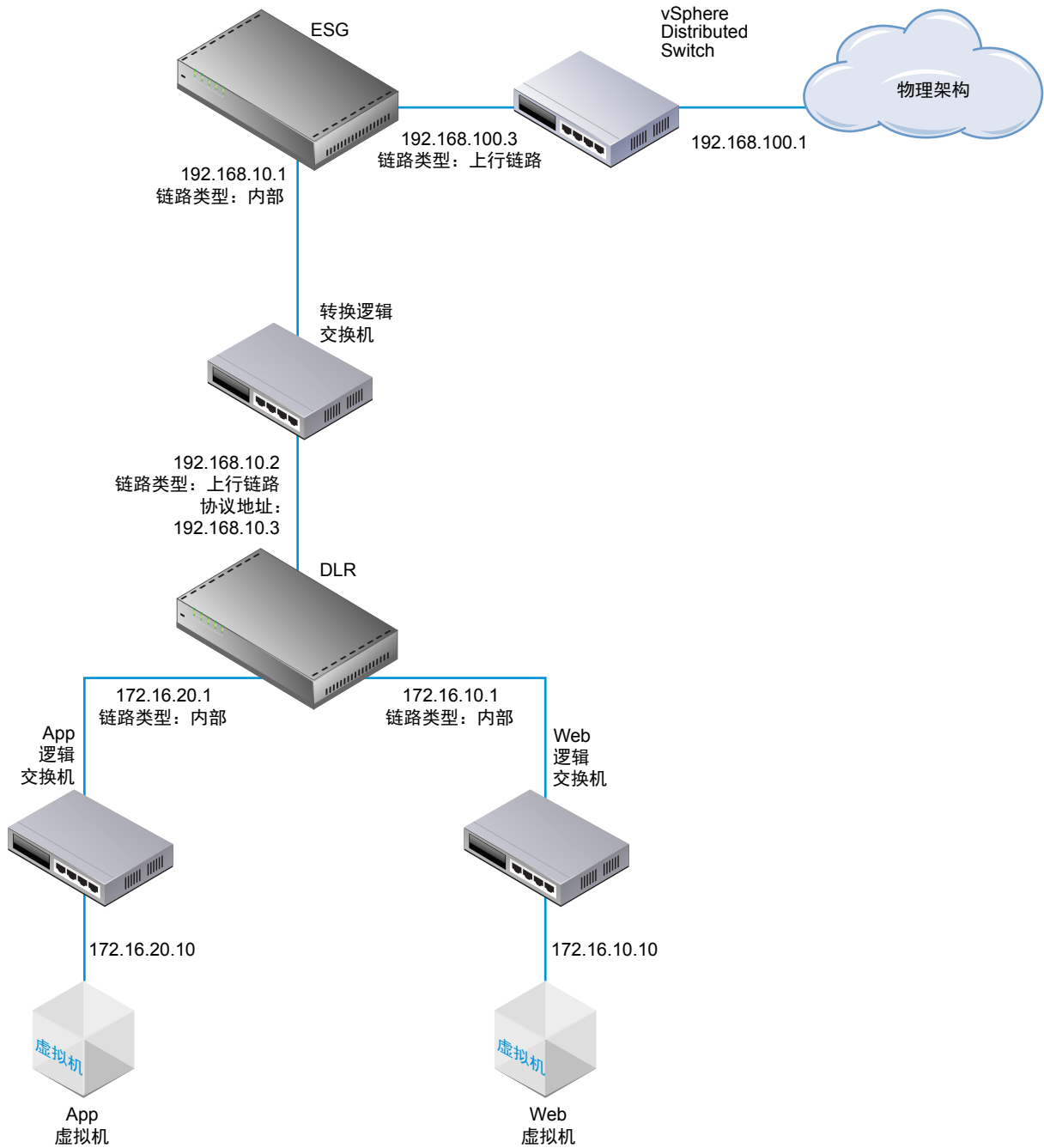
## 11 确保路由重新分布和防火墙配置允许播发正确的路由。

# 示例：在 Edge 服务网关上配置的 OSPF

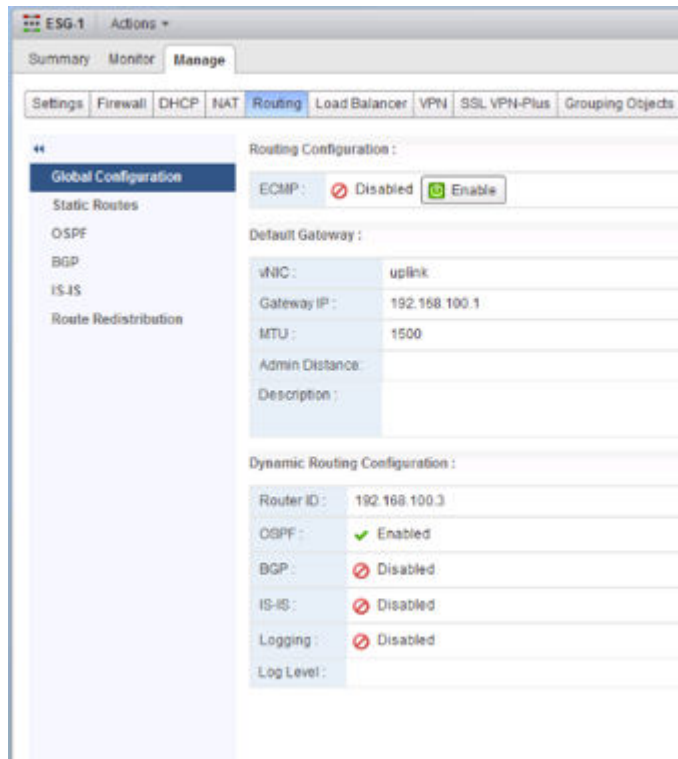
使用 OSPF 的一个简单 NSX 应用场景是当逻辑路由器 (DLR) 和 Edge 服务网关 (ESG) 是 OSPF 邻居时，如下图所示。

通过 vSphere Distributed Switch 上的上行链路端口组，ESG 可以通过桥、物理路由器（或者如下图所示）连接到外部环境。

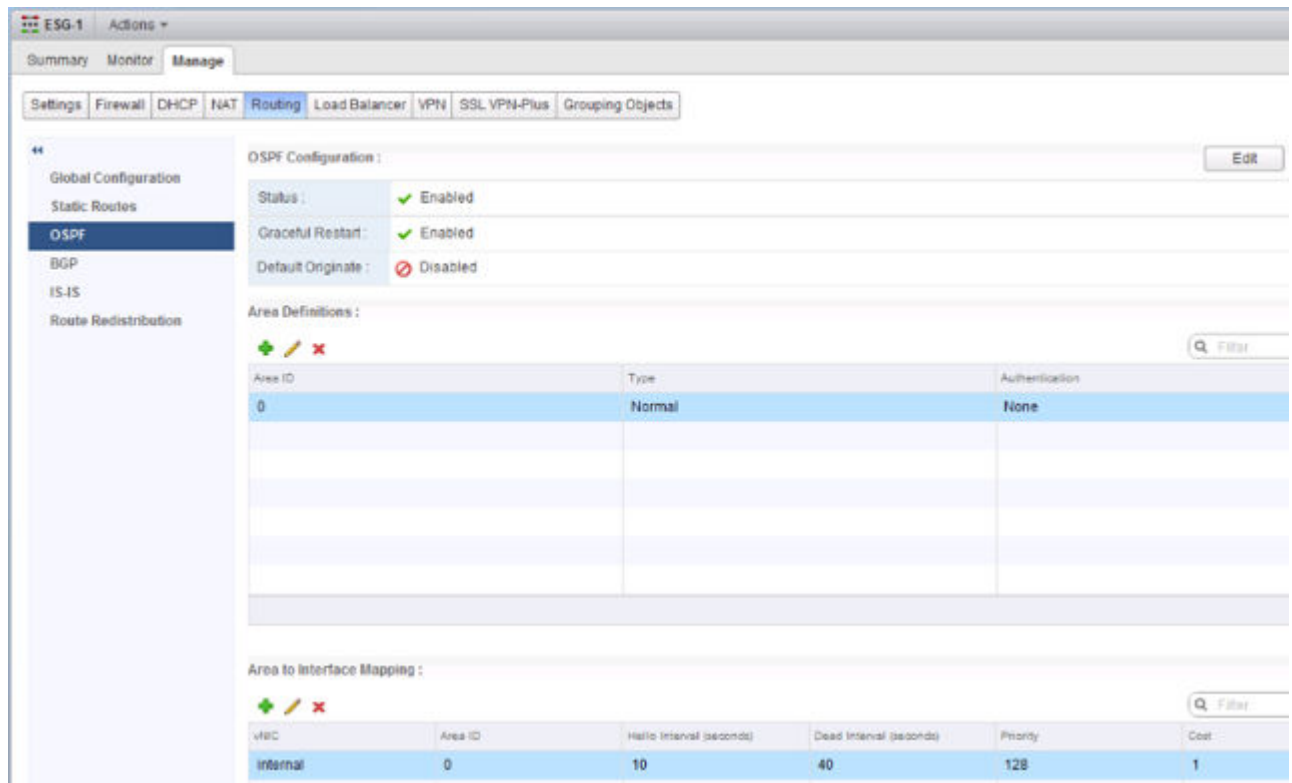
图 9-2. NSX 拓扑



在下面的屏幕中，ESG 的默认网关为连接其外部对等方的 ESG 上行链路接口。  
路由器 ID 是 ESG 的上行链路接口 IP 地址，即，面向其外部对等方的 IP 地址。



配置的区域 ID 为 0，内部接口（面向逻辑路由器的接口）映射到该区域。



连接的路由重新分布到 OSPF，以使 OSPF 邻居（逻辑路由器）可以获知 ESG 的上行链路网络的相关信息。



Summary Monitor Manage

Settings Firewall DHCP NAT **Routing** Load Balancer VPN SSL VPN-Plus Grouping Objects

Global Configuration  
Static Routes  
OSPF  
BGP  
IS-IS  
**Route Redistribution**

Route Redistribution Status:

OSPF ☒ ISIS ☐ BGP ☐

IP Prefixes:

+ - ✎ ✖

| Name | IP Network |
|------|------------|
|      |            |
|      |            |
|      |            |
|      |            |

Route Redistribution table:

+ - ✎ ✖

| Learned | From      | Prefix | Action |
|---------|-----------|--------|--------|
| OSPF    | Connected | Any    | Permit |

**注** 此外，可以在 ESG 与其外部对等路由器之间配置 OSPF，但更常见的情形是该链接使用 BGP 进行路由通告。

确保 ESG 从逻辑路由器获知 OSPF 外部路由。

```
NSX-edge-7-0> show ip route

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
M1 - OSPF NSSA external type 1, M2 - OSPF NSSA external type 2

Total number of routes: 5

S 0.0.0.0/0 [0/0] via 192.168.100.1
0 E2 172.16.10.0/24 [110/1] via 192.168.10.2
0 E2 172.16.20.0/24 [110/1] via 192.168.10.2
C 192.168.10.0/29 [0/0] via 192.168.10.1
C 192.168.100.0/24 [0/0] via 192.168.100.3
```

要验证连接，确保物理架构中的外部设备可以 ping 虚拟机。

例如：

```
PS C:\Users\Administrator> ping 172.16.10.10

Pinging 172.16.10.10 with 32 bytes of data:
Reply from 172.16.10.10: bytes=32 time=5ms TTL=61
Reply from 172.16.10.10: bytes=32 time=1ms TTL=61

Ping statistics for 172.16.10.10:
 Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 5ms, Average = 3ms
```

```
PS C:\Users\Administrator> ping 172.16.20.10

Pinging 172.16.20.10 with 32 bytes of data:
Reply from 172.16.20.10: bytes=32 time=2ms TTL=61
Reply from 172.16.20.10: bytes=32 time=1ms TTL=61

Ping statistics for 172.16.20.10:
 Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

## 配置 BGP

边界网关协议 (BGP) 可制定核心路由决策。决策包括一个由 IP 网络或前缀组成的表，这些信息指定了多个自治系统间的网络可访问性。

在交换任何路由信息之前，会先在两个 BGP 发言方 (speaker) 之间建立一个基础连接。BGP 发言方将发送“保持连接”消息，以维持这种活动状态。建立连接后，BGP 发言方将交换路由并同步其表。

## 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**路由 (Routing)**，然后单击 **BGP**。
- 5 单击**编辑 (Edit)**。
- 6 在“编辑 BGP 配置”对话框中，单击**启用 BGP (Enable BGP)**。
- 7 单击**启用正常重新启动 (Enable Graceful Restart)**，以使数据包转发在重新启动 BGP 服务期间不会中断。
- 8 单击**启用默认源 (Enable Default Originate)**以允许 NSX Edge 将其自身作为默认网关播发给其对等方。
- 9 在**本地 AS (Local AS)** 中键入路由器 ID。键入本地 AS。当 BGP 与其他自治系统 (AS) 中的路由器建立对等关系时，将播发该本地 AS。选择到达目标的最佳路径时，会将路由所遍历的 AS 路径用作一个衡量指标。
- 10 单击**确定 (OK)**。
- 11 在**邻居 (Neighbors)**中，单击**添加 (Add)**图标。
- 12 键入邻居的 IP 地址。  
配置 Edge 服务网关 (ESG) 与逻辑路由器之间的 BGP 对等关系时，使用逻辑路由器的协议 IP 地址作为 ESG 的 BGP 邻居地址。
- 13 （仅在逻辑路由器上）键入转发地址。  
转发地址是您分配给面向其 BGP 邻居的分布式逻辑路由器接口（其上行链路接口）的 IP 地址。
- 14 （仅在逻辑路由器上）键入协议地址。  
协议地址是逻辑路由器用来形成 BGP 邻居关系的 IP 地址。它可以是与转发地址位于同一子网中的任何 IP 地址（前提是未在其他位置使用）。配置 Edge 服务网关 (ESG) 与逻辑路由器之间的 BGP 对等关系时，使用逻辑路由器的协议 IP 地址作为 ESG 邻居的 IP 地址。
- 15 键入远程 AS。
- 16 根据需要编辑邻居连接的默认权重。
- 17 **按住定时器 (Hold Down Timer)**显示软件在多久未接收到保持连接消息后声明对等方失效（180 秒）。  
根据需要进行编辑。
- 18 **保持连接定时器 (Keep Alive Timer)**显示软件向其对等方发送“保持连接”消息的默认频率（60 秒）。  
根据需要进行编辑。
- 19 如果需要身份验证，键入身份验证密码。对在邻居间的连接上发送的每个数据段都会进行验证。必须配置 MD5 身份验证在两个 BGP 邻居上使用相同的密码，否则不会在二者之间建立连接。

20 要指定邻居的路由筛选，请单击 **BGP 筛选器 (Add)**区域中的**添加 (BGP Filters)**图标。



**小心** 在筛选器最后强制实行“阻止全部”规则。

21 选择方向以指示筛选流入还是流出邻居的流量。

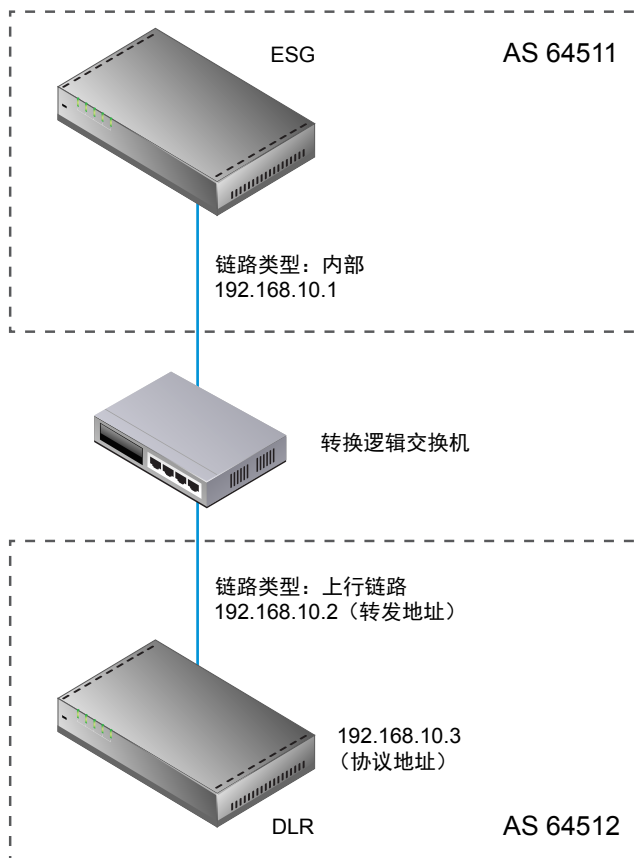
22 选择操作以指示允许还是拒绝流量。

23 以 CIDR 格式键入要筛选的连接邻居的网络。

24 键入要筛选的 IP 前缀，然后单击**确定 (OK)**。

25 单击**发布更改 (Publish Changes)**。

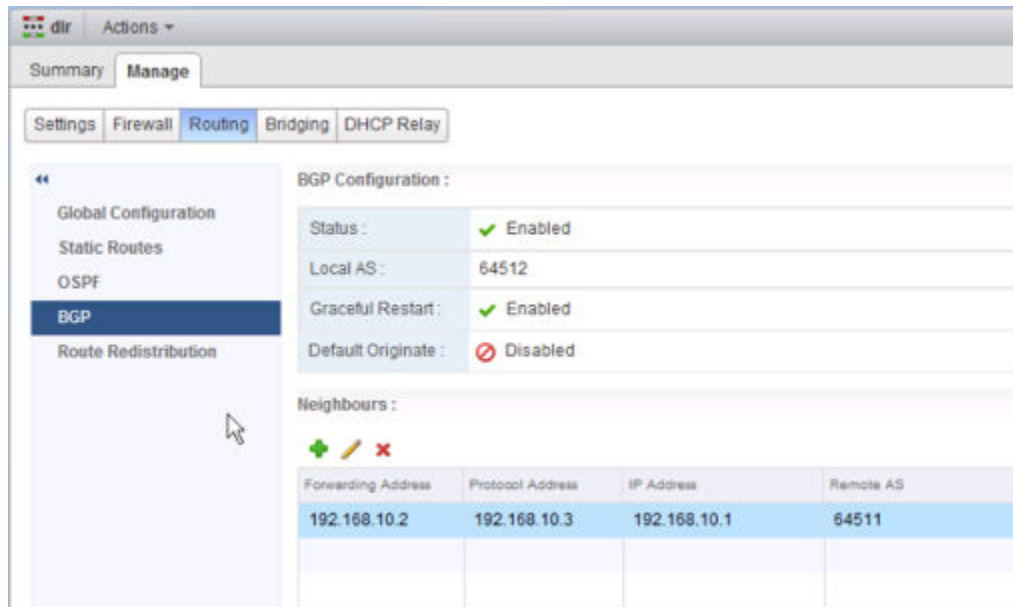
## 示例：配置 ESG 与逻辑路由器之间的 BGP



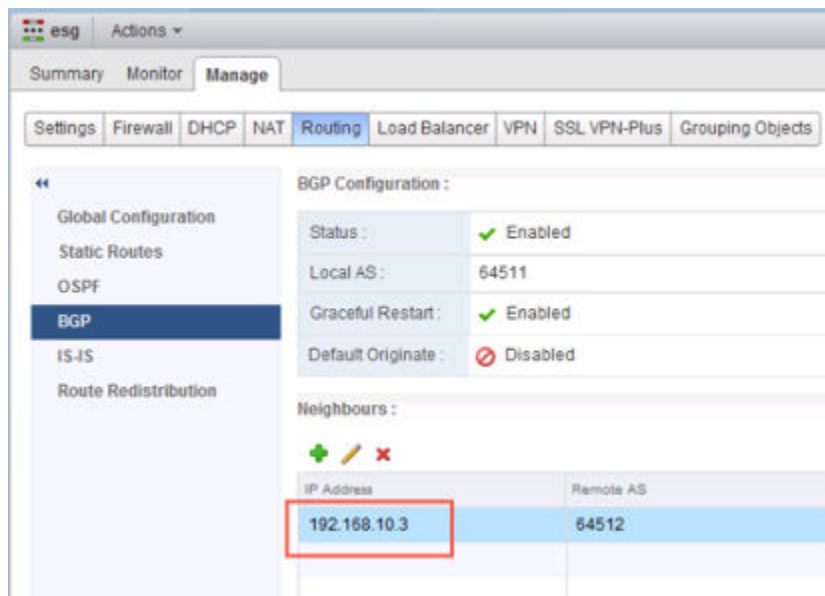
在此拓扑中，ESG 在 AS 64511 中。逻辑路由器 (DLR) 在 AS 64512 中。

逻辑路由器的转发地址为 192.168.10.2。该地址在逻辑路由器的上行链路接口上配置。逻辑路由器的协议地址为 192.168.10.3。ESG 将使用该地址与逻辑路由器形成其 BGP 对等关系。

在逻辑路由器上，如下所示配置 BGP：



在 ESG 上，如下所示配置 BGP：



ESG 的邻居地址是 192.168.10.3，它是逻辑路由器的协议地址。

在逻辑路由器上运行 `show ip bgp neighbors` 命令，并确保 BGP 状态为“已建立”。

```

NSX-edge-6-0> show ip bgp neighbors

BGP neighbor is 192.168.10.1, remote AS 64511,
BGP state = Established, up
Hold time is 180, Keep alive interval is 60 seconds
Neighbor capabilities:
 Route refresh: advertised and received
 Address family IPv4 Unicast:advertised and received
 Graceful restart Capability:advertised and received
 Restart remain time: 0
Received 120 messages, Sent 125 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
 Index 1 Identifier 0x9aa20f3c
 Route refresh request:received 0 sent 0
 Prefixes received 0 sent 0 advertised 0
Connections established 1, dropped 5
Local host: 192.168.10.3, Local port: 179
Remote host: 192.168.10.1, Remote port: 43846

```

在 ESG 上运行 show ip bgp neighbors 命令，并确保 BGP 状态为“已建立”。

```

NSX-edge-7-0> show ip bgp neighbors

BGP neighbor is 192.168.10.3, remote AS 64512,
BGP state = Established, up
Hold time is 180, Keep alive interval is 60 seconds
Neighbor capabilities:
 Route refresh: advertised and received
 Address family IPv4 Unicast:advertised and received
 Graceful restart Capability:advertised and received
 Restart remain time: 0
Received 121 messages, Sent 120 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
 Index 3 Identifier 0x40212c6c
 Route refresh request:received 0 sent 0
 Prefixes received 0 sent 0 advertised 0
Connections established 1, dropped 1
Local host: 192.168.10.1, Local port: 43846
Remote host: 192.168.10.3, Remote port: 179

```

## 配置 IS-IS 协议

中间系统到中间系统 (IS-IS) 路由协议旨在以确定通过分组交换网络的数据报的最佳路由的方式来移动信息。

使用包含两个级别的层次结构来支持大型路由域。一个大型域可分为多个区域。在某个区域内进行的路由称为 1 级路由。在区域间进行的路由称为 2 级路由。2 级中间系统 (IS) 跟踪目标区域的路径。1 级 IS 跟踪其自己区域内的路由。对于前往其他区域的数据包，1 级 IS 将该数据包发送到其自己区域内最近的 2 级 IS，而无论目标区域为何。然后该数据包通过 2 级路由传送到目标区域，在该区域可通过 1 级路由传送到目标。同时处于 1 级和 2 级的 IS 称为 1-2 级。

---

**注** IS-IS 协议的 NSX 支持目前处于实验阶段。

---

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**路由 (Routing)**，然后单击 **IS-IS**。
- 5 单击**编辑 (Edit)**，然后单击**启用 IS-IS (Enable IS-IS)**。
- 6 键入系统 ID 并选择 IS-IS 类型。

级别 1 指区域内，级别 2 指区域间，而级别 1-2 是指这两者。2 级路由器是只能与其他 2 级路由器建立关系的区域间路由器。路由信息在 1 级路由器与其他 1 级路由器之间进行交换。同样，2 级路由器仅与其他 2 级路由器交换信息。级别 1-2 路由器同时与这两个级别的路由器交换信息，并用于将区域间路由器和区域内路由器连接。

- 7 键入**域密码 (Domain Password)**和**区域密码 (Area Password)**。对于 1 级链接状态数据包，将插入区域密码并进行检查，对于 2 级链接状态数据包，将插入并检查域密码。
- 8 定义 IS-IS 区域。
  - a 在**区域 (Areas)**中单击**添加 (Add)**图标。
  - b 键入最多三个区域 IP 地址。
  - c 单击**保存 (Save)**。
- 9 配置接口映射。
  - a 在**接口映射 (Add)**中单击**添加 (Interface Mapping)**图标。
  - b 选择“电路类型”以指示是要配置 1 级、2 级还是 1-2 级相邻的接口。
  - c **通信时间间隔 (Hello Interval)**显示在接口上发送的通信数据包之间的默认时间间隔（毫秒）。如果需要可编辑默认值。
  - d **通信乘数 (Hello Multiplier)**显示在邻居声明关闭前必定会丢失的默认 IS-IS 通信数据包数量。如果需要可编辑默认值。
  - e **LSP 时间间隔 (LSP Interval)**显示连续的 IS-IS 链接状态数据包 (LSP) 传输之间的时间延迟（毫秒）。如果需要可编辑默认值。
  - f **衡量指标 (Metric)**显示接口的默认衡量指标。该指标用于计算通过网络链接从每个接口到其他目标的成本。如果需要可编辑默认值。

- g **优先级 (Priority)**显示接口的优先级。优先级最高的接口将成为指定路由器。如果需要可编辑默认值。
- h 在“网络组”中，键入用于标识此接口所属的网络组的编号。如果需要可编辑默认值。
- i 键入接口的身份验证密码并单击**确定 (OK)**。如果需要可编辑默认值。

10 单击**发布更改 (Publish Changes)**。

## 配置路由重新分发

默认情况下，路由器与运行同一协议的其他路由器共享路由。在多协议环境中，必须配置路由重新分发才能实现跨协议路由共享。

如果希望将某个接口从路由重新分发中排除出去，则可以为该网络添加拒绝条件。在 **NSX 6.2** 中，逻辑（分布式）路由器的 **HA（管理）** 接口会自动从路由重新分发中排除出去。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**路由 (Routing)**，然后单击**路由重新分发 (Route Redistribution)**。
- 5 单击**路由重新分发状态 (Route Redistribution Status)**旁边的**编辑 (Edit)**。
- 6 选择启用路由重新分发的协议，然后单击**确定 (OK)**。
- 7 添加一个 IP 前缀。

IP 前缀列表中的条目将按顺序进行处理。

- a 在 **IP 前缀 (IP Prefixes)** 中单击**添加 (Add)**图标。
- b 键入网络的名称和 IP 地址。

输入的 IP 前缀将完全匹配，但在包括小于等于 (LE) 或大于等于 (GE) 修饰符时除外。

- c 单击**确定 (OK)**。
- 8 指定 IP 前缀的重新分发条件。
    - a 在**路由重新分发表 (Route Redistribution table)**中单击**添加 (Add)**图标。
    - b 在**学习者协议 (Learner Protocol)**中，选择将从其他协议获知路由的协议。
    - c 在**允许从以下项中学习 (Allow Learning from)**中，选择应从中获知路由的协议。
    - d 单击**确定 (OK)**。
  - 9 单击**发布更改 (Publish Changes)**。



## 查看 NSX Manager 区域设置 ID

每个 NSX Manager 都有一个区域设置 ID。该 ID 默认设置为 NSX Manager 的 UUID。可以在通用逻辑路由器、群集或主机级别覆盖此设置。

### 步骤

- 1 在 vSphere Web Client 中，导航到 **网络和安全 (Networking & Security)**，然后在 **网络和安全清单 (Networking & Security Inventory)** 下单击某个 NSX Manager。
- 2 单击 **摘要 (Summary)** 选项卡。ID 字段包含 NSX Manager 的 UUID。

## 在通用逻辑（分布式）路由器上配置区域设置 ID

如果在创建通用逻辑路由器时启用了本地输出，则仅当主机的区域设置 ID 与路由所关联的区域设置 ID 相匹配时，路由才会发送到主机。您可以更改路由器上的区域设置 ID，此更新后的区域设置 ID 将与该路由器（静态和动态）上的所有路由关联。路由将发送到区域设置 ID 相匹配的主机和群集。

有关跨 vCenter NSX 环境的路由配置的信息，请参见[跨 vCenter NSX 拓扑](#)。

### 前提条件

通用逻辑（分布式）路由器必须已创建且启用了本地输出。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击通用逻辑（分布式）路由器。
- 4 单击 **路由 (Routing)** 选项卡，然后单击 **全局配置 (Global Configuration)**。
- 5 单击 **路由配置 (Routing Configuration)** 旁边的 **编辑 (Edit)**。
- 6 键入新的区域设置 ID。

---

**重要** 区域设置 ID 必须采用 UUID 格式。例如，XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX，其中每个 X 都替换为 16 进制数字 (0-F)。

---


## 在主机或群集上配置区域设置 ID

如果在创建通用逻辑路由器时启用了本地输出，则仅当主机的区域设置 ID 与路由所关联的区域设置 ID 相匹配时，路由才会发送到主机。可以通过配置主机的群集或主机上的区域设置 ID 来选择将路由发送到主机。

### 前提条件

对主机或群集执行路由的通用逻辑（分布式）路由器必须已创建且启用了本地输出。

## 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**安装 (Installation)**。
- 3 单击**主机准备 (Host Preparation)**选项卡。
- 4 选择管理需要配置的主机或群集的 NSX Manager。
- 5 选择要修改的主机或群集，需要时可展开群集以显示主机。
- 6 单击**设置 (Settings)**图标 ()，然后单击**更改区域设置 ID (Change Locale ID)**。
- 7 键入新的区域设置 ID，然后单击**确定 (OK.)**。

---

**注** 区域设置 ID 必须采用 UUID 格式。例如，XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX，其中每个 X 都替换为 16 进制数字 (0-F)。

---

通用控制器群集仅向主机发送与此新的区域设置 ID 相匹配的路由。

## 后续步骤

使用指定的区域设置 ID 配置静态路由。

## 逻辑防火墙

逻辑防火墙为动态虚拟数据中心提供安全机制，该防火墙包含两个组件，用于应对不同的部署用例。分布式防火墙侧重于东西向访问控制，而 **Edge** 防火墙侧重于租户或数据中心外围的南北向流量执行。这两个组件结合使用可满足虚拟数据中心的端对端防火墙需求。您可以选择单独部署任意一种技术，或者同时部署这两者。

本章讨论了以下主题：

- 分布式防火墙
- **Edge** 防火墙
- 使用防火墙规则区域
- 使用防火墙规则
- 从防火墙保护中排除虚拟机
- 虚拟机的 IP 发现
- 查看防火墙 CPU 和内存阈值事件
- 防火墙日志
- 使用 **NSX Edge** 防火墙规则

## 分布式防火墙

分布式防火墙是嵌入管理程序内核的防火墙，用于查看和控制虚拟化的工作负载和网络。可以基于 **VMware vCenter** 对象（如数据中心和群集）和虚拟机名称、诸如 IP 或 **IPSet** 地址、**VLAN**（**DVS** 端口组）、**VXLAN**（逻辑交换机）等网络构造、安全组以及 **Active Directory** 中的用户组标识来创建访问控制策略。防火墙规则实施在每台虚拟机的虚拟网卡上，可以提供一致的访问控制；即使虚拟机通过 **vMotion** 发生了迁移，防火墙规则也会发挥作用。由于防火墙嵌入在管理程序中的特性，因此可提供接近线速率的吞吐量，从而可在物理服务器上支持更高的工作负载整合。防火墙的分布式特性使架构具有向外扩展性，可在向数据中心添加更多主机时自动扩展防火墙功能。

对于 **L2** 数据包，分布式防火墙会创建缓存以提升性能。会按以下顺序处理 **L3** 数据包：

- 1 检查所有数据包的现有状态。也会对 **SYN** 执行此操作，以便检测出现有会话中的虚假或重新传输的 **SYN**。
- 2 如果发现状态匹配，则会处理数据包。

- 3 如果未发现状态匹配，则会通过规则处理数据包，直到发现匹配。
  - 对于 **TCP** 数据包，仅为带有 **SYN** 标记的数据包设置状态。但是，未指定协议（“任意”服务）的规则可以将 **TCP** 数据包与任何标记组合相匹配。
  - 对于 **UDP** 数据包，会从数据包中提取 5 元组详细信息。如果状态表中不存在某个状态，则会使用提取的 5 元组详细信息创建新状态。随后接收的数据包将与刚才创建的状态相匹配。
  - 对于 **ICMP** 数据包，将使用 **ICMP** 类型、代码和数据包方向来创建状态。

分布式防火墙还有助于创建基于身份的规则。管理员可以基于企业 **Active Directory** 中定义的用户组成员资格强制实施访问控制。下面是一些可使用基于标识的防火墙规则的场景：

- 用户通过笔记本电脑或移动设备访问虚拟应用程序（使用 **AD** 进行用户身份验证）
- 用户使用 **VDI** 基础架构访问虚拟应用程序（虚拟机基于 **Microsoft Windows**）

如果您的环境中部署了第三方供应商防火墙解决方案，请参见[通过逻辑防火墙将流量重定向到供应商解决方案](#)。

尚未在分布式防火墙中验证是否可以在客户机或工作负载虚拟机上运行打开的 **VMware Tools**。

## 分布式防火墙资源利用率的 ESXi 阈值参数

每个 **ESXi** 主机均配置了三个用于统计 **DFW** 资源利用率的阈值参数：**CPU**、**RAM** 和每秒连接数 (**CPS**)。如果在 200 秒的时间段内连续超过相应阈值 20 次，将发出警报。每 10 秒执行一次采样。

100% **CPU** 是指主机上的全部可用 **CPU**。

100% **RAM** 是指为分布式防火墙分配的内存（“最大大小合计”），具体取决于在主机上安装的 **RAM** 总量。

**表 10-1. 最大大小合计**

| 物理内存         | 最大大小合计 (MB) |
|--------------|-------------|
| 0 - 8GB      | 160         |
| 8GB - 32GB   | 608         |
| 32GB - 64GB  | 992         |
| 64GB - 96GB  | 1920        |
| 96GB - 128GB | 2944        |
| 128GB        | 4222        |

内存由分布式防火墙的内部数据结构使用，这些数据结构包括筛选器、规则、容器、连接状态、已发现的 IP 和丢弃的流量。您可以使用以下 **API** 调用来控制这些参数：

```
https://NSX-MGR-IP/api/4.0/firewall/stats/eventthresholds
```

Request body:

```
<eventThresholds>
 <cpu>
 <percentValue>100</percentValue>
 </cpu>
 <memory>
```

```
<percentValue>100</percentValue>
</memory>
<connectionsPerSecond>
 <value>100000</value>
</connectionsPerSecond>
</eventThresholds>
```

## Edge 防火墙

Edge 防火墙会监控南北向流量以提供外围安全功能，包括防火墙、网络地址转换 (NAT) 以及点对点 IPSec 和 SSL VPN 功能。此解决方案可用于任意虚拟机组合形式，并且可以在高可用性模式下部署。

防火墙支持仅限于逻辑路由器。只有管理接口和/或上行链路接口上的规则起作用，而内部接口上的规则不起作用。

**注** NSX-V Edge 很容易受到 SYN 洪泛攻击，在这种攻击中，攻击者发送大量 SYN 数据包以填充防火墙状态跟踪表。该 DOS/DDOS 攻击导致真正用户的服务中断。Edge 必须实施逻辑以检测并终止伪造的 TCP 连接，而不会消耗防火墙状态跟踪资源，从而抵御 SYN 洪泛攻击。默认情况下，将禁用该功能。要在高风险环境中启用该功能，请将 REST API `enableSynFloodProtection` 值设置为 “true” 以作为防火墙全局配置的一部分。

## 使用防火墙规则区域

可以添加一个区域来分隔防火墙规则。例如，您可能希望将销售部和工程部的对应规则分别置于两个单独区域中。

可以为 L2 和 L3 规则创建多个区域。

跨 vCenter NSX 环境中可以包括一个通用 L2 规则区域和一个通用 L3 规则区域。必须在主 NSX Manager 上管理通用规则，并且必须先在主 NSX Manager 上创建通用区域，才能添加通用规则。

通用区域外部的规则依然是添加规则的主 NSX Manager 和辅助 NSX Manager 的本地规则。

## 添加防火墙规则区域

您可以在防火墙表中添加一个新区域，用于组织规则，或用于创建一个要在跨 vCenter NSX 环境中使用的通用区域。

### 前提条件

确定要对其进行更改的相应 NSX Manager。

- 在独立或单个 vCenter NSX 环境中，仅有一个 NSX Manager，因此无需进行选择。
- 必须从主 NSX Manager 管理通用对象。
- 某个 NSX Manager 的本地对象必须使用该 NSX Manager 进行管理。
- 在未启用增强型链接模式的跨 vCenter NSX 环境中，您必须从链接至您想要修改的 NSX Manager 的 vCenter 中更改配置。

- 在处于增强型链接模式的跨 vCenter NSX 环境中，您可以从任意链接的 vCenter 更改任意 NSX Manager 的配置。从 NSX Manager 下拉菜单中选择相应的 NSX Manager。

#### 步骤

- 1 在 vSphere Web Client 中，导航到**网络和安全 (Networking & Security) > 防火墙 (Firewall)**。
- 2 如果有多个 NSX Manager 可用，请选择一个。必须选择主 NSX Manager，才能添加通用区域。
- 3 确保您处于**常规 (General)**选项卡中，以便为 L3 规则添加区域。单击**以太网 (Ethernet)**选项卡可为 L2 规则添加区域。
- 4 单击**添加区域 (Add Section)** () 图标。
- 5 键入区域名称并指定新区域的位置。区域名称在 NSX Manager 中必须唯一。
- 6 （可选）要创建通用区域，请选择**标记此区域待进行通用同步 (Mark this section for Universal Synchronization)**。
- 7 单击**确定 (OK)**，然后单击**发布更改 (Publish Changes)**。

#### 后续步骤


向区域添加规则。可以通过单击该区域的**编辑区域 (Edit section)** () 图标来编辑区域的名称。

## 合并防火墙规则区域

您可以合并区域以及整合这些区域内的规则。请注意，服务编排或“默认”区域无法与其他区域合并。在跨 vCenter NSX 环境中，通用区域无法与其他区域合并。

合并并整合复杂的防火墙配置有助于简化维护工作和提高可读性。

#### 步骤

- 1 在 vSphere Web Client 中，导航到**网络和安全 (Networking & Security) > 防火墙 (Firewall)**。
- 2 对于要合并的区域，请单击**合并 (Merge)** () 图标，并指定您是要将此区域与上方区域还是下方区域进行合并。  
这两个区域中的规则进行合并。新区域将保留此区域与其他区域合并前的名称。
- 3 单击**发布更改 (Publish Changes)**。

## 删除防火墙规则区域

可以删除防火墙规则区域。该区域中的所有规则都将删除。

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 在 vSphere Web Client 中，导航到**网络和安全 (Networking & Security) > 防火墙 (Firewall)**。

- 2 确保您处于**常规 (General)**选项卡中，以便删除 L3 规则的区域。单击**以太网 (Ethernet)**选项卡以删除 L2 规则的区域。
- 3 对于要删除的区域，单击**删除区域 (Delete section)** (✖) 图标。
- 4 单击**确定 (OK)**，然后单击**发布更改 (Publish Changes)**。

将删除该区域以及该区域中的所有规则。

## 使用防火墙规则

可以在“防火墙”选项卡上集中管理分布式防火墙规则和 **Edge** 防火墙规则。在多租户环境中，提供商可以在集中式防火墙用户界面上定义高级流量规则。

应先根据“防火墙”表中最上面的规则检查每个流量会话，然后才能下移至表中的后续规则。表中第一条匹配流量参数的规则会被强制实施。规则按以下顺序显示：

- 1 用户在防火墙用户界面中定义的规则具有最高优先级，按每个虚拟网卡级别的优先级顺序排列后由上到下强制实施。
- 2 自动检测到的规则（用于对 **Edge** 服务流量启用控制的规则）。
- 3 用户在 **NSX Edge** 界面中定义的规则。
- 4 服务编排规则 - 每个策略一个单独的区域。不能在防火墙表中编辑这些规则，但是可以在安全策略防火墙规则区域的顶部添加规则。如果执行了此操作，则必须在服务编排中重新同步规则。有关详细信息，请参见[第 17 章，服务编排](#)。
- 5 默认分布式防火墙规则

请注意，防火墙规则仅在已启用防火墙的群集上强制实施。有关准备群集的信息，请参见 **NSX 安装指南**。

## 编辑默认分布式防火墙规则

默认防火墙设置应用于与任何用户定义的防火墙规则均不匹配的流量。分布式防火墙默认规则在集中式防火墙用户界面中显示，并且每个 **NSX Edge** 的默认规则都在 **NSX Edge** 级别显示。

默认的分布式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，无法删除或添加。但是，您可以将规则的“操作”元素从“允许”更改为“阻止”或“拒绝”，为规则添加备注，以及指示是否应记录该规则的流量。

在跨 **vCenter NSX** 环境中，默认规则不是通用规则。对默认规则的任何更改都必须在每个 **NSX Manager** 上进行。

### 步骤

- 1 在 **vSphere Web Client** 中，导航到 **网络和安全 (Networking & Security) > 防火墙 (Firewall)**。
- 2 展开“默认区域”，进行所需更改。

仅可以编辑**操作 (Action)**和**日志 (Log)**，或者为默认规则添加备注。

## 添加防火墙规则

可以在 NSX Manager 范围添加防火墙规则。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。

可以将以下 vCenter 对象指定为防火墙规则的源或目标：

**表 10-2. 防火墙规则支持的对象**

源或目标	应用对象
<ul style="list-style-type: none"> <li>■ 群集</li> <li>■ 数据中心</li> <li>■ 分布式端口组</li> <li>■ IP 集</li> <li>■ 传统端口组</li> <li>■ 逻辑交换机</li> <li>■ 资源池</li> <li>■ 安全组</li> <li>■ vApp</li> <li>■ 虚拟机</li> <li>■ 虚拟网卡</li> <li>■ IP 地址（IPv4 或 IPv6）</li> </ul>	<ul style="list-style-type: none"> <li>■ 已安装 Distributed Firewall 的所有群集（即已完成网络虚拟化准备的所有群集）</li> <li>■ 准备好的群集上安装的所有 Edge 网关</li> <li>■ 群集</li> <li>■ 数据中心</li> <li>■ 分布式端口组</li> <li>■ Edge</li> <li>■ 传统端口组</li> <li>■ 逻辑交换机</li> <li>■ 安全组</li> <li>■ 虚拟机</li> <li>■ 虚拟网卡</li> </ul>

### 前提条件

确保 NSX Distributed Firewall 的状态未处于向后兼容模式。要检查当前状态，请使用以下 REST API 调用：  
GET https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state。如果当前状态为向后兼容模式，则可以使用以下 REST API 调用将状态更改为向前兼容：PUT https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state。当 Distributed Firewall 处于向后兼容模式时，请勿尝试发布 Distributed Firewall 规则。


如果您正在添加通用防火墙规则，请参见[添加通用防火墙规则](#)

如果您正在添加基于标识的防火墙规则，请确保：

- 已向 NSX Manager 注册了一个或多个域。NSX Manager 从向其注册的每个域获取组和用户信息以及两者之间的关系。请参见[向 NSX Manager 注册 Windows 域](#)。
- 已基于 Active Directory 对象创建了可用作规则的源或目标的安全组。请参见[创建安全组](#)。

如果您正在根据 VMware vCenter 对象添加规则，请确保在虚拟机上安装了 VMware Tools。请参见 NSX 安装指南。


### 步骤

- 1 在 vSphere Web Client 中，导航到**网络和安全 (Networking & Security) > 防火墙 (Firewall)**。
- 2 确保您处于**常规 (General)**选项卡中以添加 L3 规则。单击**以太网 (Ethernet)**选项卡可添加 L2 规则。
- 3 在添加规则的区域中，单击**添加规则 (Add rule)** () 图标。



#### 4 单击发布更改 (Publish Changes)。

任何一个允许的新规则将添加到区域的顶部。如果系统定义的规则是区域中的唯一规则，则新规则将添加到默认规则的上方。

如果要将规则添加到区域中的特定位置，请选择一个规则。在“编号”列中，单击 ，并选择**添加到上方 (Add Above)**或**添加到下方 (Add Below)**。

**Firewall**








**Configuration** Saved Configurations

NSX Manager: 10.110.8.93

This rule set has unsaved changes. Click on Publish Changes button to start deploying or click Save Changes to save this configuration.

[Publish Changes](#) [Revert Changes](#) [Save Changes](#) [Update Changes](#)

**General** **Ethernet** **Partner security services**

No.	Name	Source	Destination	Service	Action	Applied To
▼ Demo Firewall (Rule 1 - 3)						
1		* any	* any	* any	Allow	Distributed Firewall
2		* any	* any	* any	Allow	Distributed Firewall
3		NSX_Controller_55...	* any	* any	Allow	Distributed Firewall
Security Policy						
▼ Default Section Layer3 (Rule 4 - 7)						
4	ForMyTest	* any	* any	* any	Allow	NSXEdg2 Distributed Firewall
5	Default Rule NDP	* any	* any	IPv6-ICMP Neighbor... IPv6-ICMP Neighbor...	Allow	Distributed Firewall
6	Default Rule DHCP	* any	* any	DHCP-Client DHCP-Server	Allow	Distributed Firewall
7	Default Rule	* any	* any	* any	Allow	Distributed Firewall




5 指向新规则的名称 (Name) 单元，然后单击 .

6 键入新规则的名称。




## 7 指向新规则的源 (Source) 单元。将显示其他图标，如下表中所述。

选项	描述
单击 	<p>要将源指定为 IP 地址，请执行以下操作：</p> <ol style="list-style-type: none"> <li>选择 IP 地址格式。 防火墙同时支持 IPv4 和 IPv6 格式。</li> <li>键入 IP 地址。 您可以在逗号分隔列表中输入多个 IP 地址。该列表最多可以包含 255 个字符。</li> </ol>
单击 	<p>要将源指定为除特定 IP 地址以外的对象，请执行以下操作：</p> <ol style="list-style-type: none"> <li>在视图 (View) 中，选择一个产生通信的容器。 此时会显示选定容器的对象。</li> <li>选择一个或多个对象，然后单击 。 可以创建一个新的安全组或 IPSet。创建新对象后，默认情况下它将添加到“源”列。有关创建新安全组或 IPSet 的信息，请参见第 22 章，网络对象和安全对象。</li> <li>要将某个源排除在规则之外，请单击高级选项 (Advanced options)。</li> <li>选择取消源 (Negate Source)，以便将该源排除在规则之外。 如果选择取消源 (Negate Source)，则此规则将应用于来自所有源的流量，但在上一个步骤中指定的源的流量除外。 如果未选择取消源 (Negate Source)，则此规则将应用于来自在上一个步骤中指定的源的流量。</li> <li>单击确定 (OK)。</li> </ol>

## 8 指向新规则的目标 (Destination) 单元。将显示其他图标，如下表中所述。

选项	描述
单击 	<p>要将目标指定为 IP 地址，请执行以下操作：</p> <ol style="list-style-type: none"> <li>选择 IP 地址格式。 防火墙同时支持 IPv4 和 IPv6 格式。</li> <li>键入 IP 地址。 您可以在逗号分隔列表中输入多个 IP 地址。该列表最多可以包含 255 个字符。</li> </ol>
单击 	<p>要将目标指定为除特定 IP 地址以外的对象，请执行以下操作：</p> <ol style="list-style-type: none"> <li>在视图 (View) 中，选择一个通信流向的容器。 此时会显示选定容器的对象。</li> <li>选择一个或多个对象，然后单击 。 可以创建一个新的安全组或 IPSet。创建新对象后，默认情况下它将添加到“目标”列。有关创建新安全组或 IPSet 的信息，请参见第 22 章，网络对象和安全对象。</li> <li>要排除某个目标端口，请单击高级选项 (Advanced options)。</li> <li>选择取消目标 (Negate Destination)，以便将该目标排除在规则之外。 如果选择取消目标 (Negate Destination)，则此规则将应用于流向所有目标的流量，但在上一个步骤中指定的目标的流量除外。 如果未选择取消目标 (Negate Destination)，则此规则将应用于流向在上一个步骤中指定的目标的流量。</li> <li>单击确定 (OK)。</li> </ol>

## 9 指向新规则的服务 (Service) 单元。将显示其他图标，如下表中所述。


选项	描述
单击 	<p>要将服务指定为端口协议组合，请执行以下操作：</p> <ol style="list-style-type: none"> <li>选择服务协议。 Distributed Firewall 支持以下协议的 ALG（应用程序级别网关）：FTP、CIFS、ORACLE TNS、MS-RPC 和 SUN-RPC。 Edge 仅支持 FTP 的 ALG。</li> <li>键入端口号，然后单击确定 (OK)。</li> </ol>
单击 	<p>要选择预定义的服务/服务组或定义新的服务/服务组，请执行以下操作：</p> <ol style="list-style-type: none"> <li>选择一个或多个对象，然后单击 。 可以创建新的服务或服务组。创建新对象后，默认情况下它将添加到“选定的对象”列。</li> <li>单击确定 (OK)。</li> </ol>

为了保护网络免受 ACK 或 SYN 泛洪攻击，可以针对默认规则将“服务”设置为“TCP-all\_ports”或“UDP-all\_ports”，并将“操作”设置为“阻止”。有关修改默认规则的信息，请参见[编辑默认分布式防火墙规则](#)。

- 10 指向新规则的操作 (Action) 单元，然后单击 。选择下表中所描述的相应选项，然后单击确定 (OK)。

操作	结果
允许	允许来自或流向指定源、目标和服务的流量。
阻止	阻止来自或流向指定源、目标和服务的流量。
拒绝	针对不被接受的数据包发送拒绝消息。 对于 TCP 连接，发送 RST 数据包。 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。
日志	记录与此规则匹配的所有会话。启用日志记录功能可能会影响性能。
不记录	不记录会话。

- 11 在应用对象 (Applied To) 中，定义此规则适用的范围。选择下表中所描述的相应选项，然后单击确定 (OK)。

要将规则应用于	请执行以下操作
环境中准备好的所有群集	选择在已启用 Distributed Firewall 的所有群集上应用此规则 (Apply this rule on all clusters on which Distributed Firewall is enabled)。单击“确定”后，此规则的“应用对象”列将显示 Distributed Firewall。
环境中的所有 NSX Edge 网关	选择在所有的 Edge 网关上应用此规则 (Apply this rule on all Edge gateways)。单击“确定”后，此规则的“应用对象”列将显示全部 Edge (All Edges)。 如果同时选择以上选项，则“应用对象”列将显示任意 (Any)。
一个或多个群集、数据中心、分布式虚拟端口组、NSX Edge、网络、虚拟机、虚拟网卡或逻辑交换机	<ol style="list-style-type: none"> <li>在容器类型 (Container type) 中，选择相应对象。</li> <li>在“可用”列表中，选择一个或多个对象，然后单击 。</li> </ol>

如果规则的源和目标字段中包含虚拟机/虚拟网卡，则必须将源和目标虚拟机/虚拟网卡都添加到应用对象 (Applied To) 中，规则才能正常运行。

- 12 单击发布更改 (Publish Changes)。

稍等片刻，将显示一条消息指示发布操作是否成功。如果出现任何故障，将列出未应用此规则的主机。有关发布失败的其他详细信息，请导航到 **NSX Manager (NSX Managers) > NSX\_Manager\_IP\_Address > 监控 (Monitor) > 系统事件 (System Events)**。

单击发布更改 (Publish Changes) 时，将自动保存防火墙配置。有关恢复为先前配置的信息，请参见[加载防火墙配置](#)。

#### 后续步骤

- 通过单击  禁用规则，或通过单击  启用规则。

- 通过单击  并选择相应的列，显示规则表中的其他列。


列名称	显示的信息
规则 ID	系统为每个规则生成的唯一 ID
日志	记录或不记录此规则的流量
统计信息	单击  将显示与此规则相关的流量（流量包和大小）
备注	规则的备注

- 通过在“搜索”字段中键入文本来搜索规则。
- 在防火墙表中向上或向下移动规则。
- 通过单击**合并区域 (Merge section)**图标并选择与**以上区域合并 (Merge with above section)**或与**以下区域合并 (Merge with below section)**合并区域。

## 加载防火墙配置

可以加载自动保存的或导入的防火墙配置。如果当前配置包含由服务编排管理的规则，在导入后这些规则会被覆盖。

### 步骤

- 1 在 vSphere Web Client 中，导航到**网络和安全 > 防火墙**。
- 2 要加载 L3 防火墙配置，必须位于**常规**选项卡。要加载 L2 防火墙配置，请单击**以太网**选项卡。
- 3 单击**加载配置** () 图标。
- 4 选择要加载的配置，然后单击**确定**。

所选配置将替换当前配置。

### 后续步骤

如果当前配置中的服务编排规则被加载的配置覆盖，请单击服务编排中“安全策略”选项卡的**操作 > 同步防火墙规则**。

## 添加通用防火墙规则

在跨 vCenter NSX 环境中，通用规则指在通用规则区域中的主 NSX Manager 上定义的分布式防火墙规则。将在环境中的所有辅助 NSX Manager 上复制这些规则，以便您能够跨 vCenter 边界保持一致的防火墙策略。多个 vCenter Server 之间的 vMotion 不支持 Edge 防火墙规则。

主 NSX Manager 可以包含一个用于通用 L2 规则的通用区域和一个用于通用 L3 规则的通用区域。可以在辅助 NSX Manager 上查看通用区域和通用规则，但是不能进行编辑。通用区域相对于本地区域的位置不会干扰规则优先级。

表 10-3. 通用防火墙规则支持的对象

源和目标	应用对象	服务
<ul style="list-style-type: none"> <li>■ 通用 MAC 集</li> <li>■ 通用 IP 集</li> <li>■ 可包含 IP 集、MAC 集或通用安全组的通用安全组</li> <li>■ 通用逻辑交换机</li> </ul>	<ul style="list-style-type: none"> <li>■ 通用逻辑交换机</li> <li>■ 分布式防火墙 - 在已安装分布式防火墙的所有群集上应用规则</li> </ul>	<ul style="list-style-type: none"> <li>■ 预先创建的通用服务和组</li> <li>■ 用户创建的通用服务和组</li> </ul>

请注意，通用规则不支持其他 vCenter 对象。

#### 前提条件

必须先创建通用规则区域，然后才能创建通用规则。请参见[添加防火墙规则区域](#)。

#### 步骤




- 1 在 vSphere Web Client 中，导航到**网络和安全 > 防火墙**。
- 2 在 NSX Manager 中，确保选择主 NSX Manager。  
仅可在主 NSX Manager 上添加通用规则。
- 3 确保您处于**常规**选项卡中以添加 L3 通用规则。单击**以太网**选项卡可添加 L2 通用规则。
- 4 在通用区域中，单击**添加规则 (+)** 图标，然后单击**发布更改**。  
任何一个允许的新规则将添加到通用区域的顶部。
- 5 指向新规则的名称单元，并单击 。键入规则的名称。
- 6 指向新规则的源单元。将显示其他图标，如下表中所述。

选项	描述
单击 	<p>要将源指定为 IP 地址，请执行以下操作：</p> <ol style="list-style-type: none"> <li>a 选择 IP 地址格式。 防火墙同时支持 IPv4 和 IPv6 格式。</li> <li>b 键入 IP 地址。</li> </ol>
单击 	<p>要将通用 IPSet、MACSet 或安全组指定为源，请执行以下操作：</p> <ol style="list-style-type: none"> <li>a 在<b>对象类型</b>中，选择一个产生通信的容器。 此时会显示选定容器的对象。</li> <li>b 选择一个或多个对象，然后单击 。 可以创建一个新的安全组或 IPSet。创建新对象后，默认情况下它将添加到“源”列。有关创建新安全组或 IPSet 的信息，请参见<a href="#">第 22 章，网络对象和安全对象</a>。</li> <li>c 要将某个源排除在规则之外，请单击<b>高级选项</b>。</li> <li>d 选择<b>取消源</b>，以便将该源排除在规则之外。 如果选择<b>取消源</b>，则此规则将应用于来自所有源的流量，但在上一个步骤中指定的源的流量除外。 如果未选择<b>取消源</b>，则此规则将应用于来自在上一个步骤中指定的源的流量。</li> <li>e 单击<b>确定</b>。</li> </ol>

## 7 指向新规则的目标单元。将显示其他图标，如下表中所述。

选项	描述
单击 	<p>要将目标指定为 IP 地址，请执行以下操作：</p> <ol style="list-style-type: none"> <li>选择 IP 地址格式。 防火墙同时支持 IPv4 和 IPv6 格式。</li> <li>键入 IP 地址。</li> </ol>
单击 	<p>要将通用 IPSet、MACSet 或安全组指定为目标，请执行以下操作：</p> <ol style="list-style-type: none"> <li>在<b>对象类型</b>中，选择一个通信流向的容器。 此时会显示选定容器的对象。</li> <li>             选择一个或多个对象，然后单击 。             可以创建一个新的安全组或 IPSet。创建新对象后，默认情况下它将添加到“目标”列。有关创建新安全组或 IPSet 的信息，请参见第 22 章，网络对象和安全对象。         </li> <li>要将某个目标排除在规则之外，请单击<b>高级选项</b>。</li> <li>选择<b>取消目标</b>，以便将该目标排除在规则之外。             如果选择<b>取消目标</b>，则此规则将应用于流向所有目标的流量，但在上一个步骤中指定的目标的流量除外。             如果未选择<b>取消目标</b>，则此规则将应用于流向在上一个步骤中指定的目标的流量。         </li> <li>单击<b>确定</b>。</li> </ol>

## 8 指向新规则的服务单元格。将显示其他图标，如下表中所述。


选项	描述
单击 	<p>要将服务指定为端口协议组合，请执行以下操作：</p> <ol style="list-style-type: none"> <li>选择服务协议。 分布式防火墙支持以下协议的 ALG（应用程序级别网关）：FTP、CIFS、ORACLE TNS、MS-RPC 和 SUN-RPC。</li> <li>键入端口号，然后单击<b>确定</b>。</li> </ol>
单击 	<p>要选择预定义的通用服务/服务组或定义新的通用服务/服务组，请执行以下操作：</p> <ol style="list-style-type: none"> <li>             选择一个或多个对象，然后单击 。             可以创建新的服务或服务组。创建新对象后，默认情况下它将添加到“选定的对象”列。         </li> <li>单击<b>确定</b>。</li> </ol>

为了保护网络免受 ACK 或 SYN 泛洪攻击，可以针对默认规则将“服务”设置为“TCP-all\_ports”或“UDP-all\_ports”，并将“操作”设置为“阻止”。有关修改默认规则的信息，请参见[编辑默认分布式防火墙规则](#)。

## 9 指向新规则的操作单元，然后单击 。选择下表中所描述的相应选项，然后单击**确定**。

操作	结果
允许	允许来自或流向指定源、目标和服务的流量。
阻止	阻止来自或流向指定源、目标和服务的流量。

操作	结果
拒绝	<p>针对不被接受的数据包发送拒绝消息。</p> <p>对于 TCP 连接，发送 RST 数据包。</p> <p>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。</p>
日志	记录与此规则匹配的所有会话。启用日志记录功能可能会影响性能。
不记录	不记录会话。

10 在**应用对象**单元中，接受默认设置分布式防火墙以在已启用分布式防火墙的所有群集上应用此规则，或单击编辑图标  以选择将应用此规则的通用逻辑交换机。

11 单击**发布更改**。




将在所有辅助 NSX Manager 上复制此通用规则。所有 NSX 实例之间的规则 ID 保持相同。要显示规则 ID，请单击 ，然后单击“规则 ID”。

通用规则可在主 NSX Manager 上进行编辑，而在辅助 NSX Manager 上是只读的。

具有通用区域第 3 层和默认区域第 3 层的防火墙规则：

No.	Name	Source	Destination	Service	Action	Applied To
Universal Section Layer3 (Rule 1 - 2)						
1	Web Micro-Segmentation	Web USG	Web USG	* any	Block	1 Distributed Firewall
2	Allow Web Access	* any	Web USG	HTTPS SSH	Allow	1 Distributed Firewall
Default Section Layer3 (Rule 3 - 7)						
3	Web Micro-Segmentation	Web SG	Web SG	* any	Allow	1 Distributed Firewall
4	Allow Web Access	* any	Web SG	HTTPS SSH	Allow	1 Distributed Firewall
5	Default Rule NDP	* any	* any	IPv6-ICMP Neighbor ... IPv6-ICMP Neighbor ...	Allow	1 Distributed Firewall
6	Default Rule DHCP	* any	* any	DHCP-Client DHCP-Server	Allow	1 Distributed Firewall
7	Default Rule	* any	* any	* any	Block	1 Distributed Firewall

## 后续步骤

- 通过在“编号”列中单击  禁用规则，或通过单击  启用规则。
- 通过单击  并选择相应的列，显示规则表中的其他列。

列名称	显示的信息
规则 ID	系统为每个规则生成的唯一 ID
日志	记录或不记录此规则的流量
统计信息	单击  将显示与此规则相关的流量（流量包和大小）
备注	规则的备注


- 通过在“搜索”字段中键入文本来搜索规则。
- 在防火墙表中向上或向下移动规则。

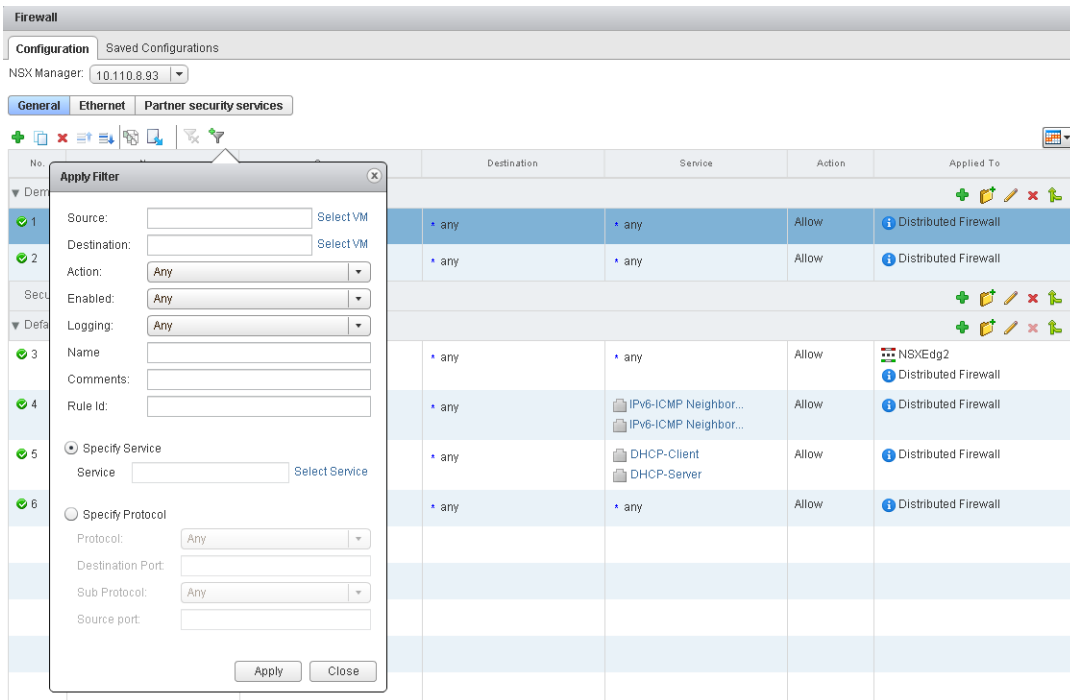


## 筛选防火墙规则

您可以使用大量条件来筛选您的规则集，从而允许进行简单的规则修改。可以按源或目标虚拟机或 IP 地址、规则操作、日志记录、规则名称、备注和规则 ID 来筛选规则。

### 步骤

- 1 在“防火墙”选项卡中，单击**应用筛选器 (Apply Filter)** (  ) 图标。



- 2 根据需要键入或选择筛选条件。

- 3 单击**应用 (Apply)**。

此时会显示匹配您的筛选条件的规则。

### 后续步骤

要重新显示所有规则，请单击**移除已应用的筛选器 (Remove applied filter)** (  ) 图标。

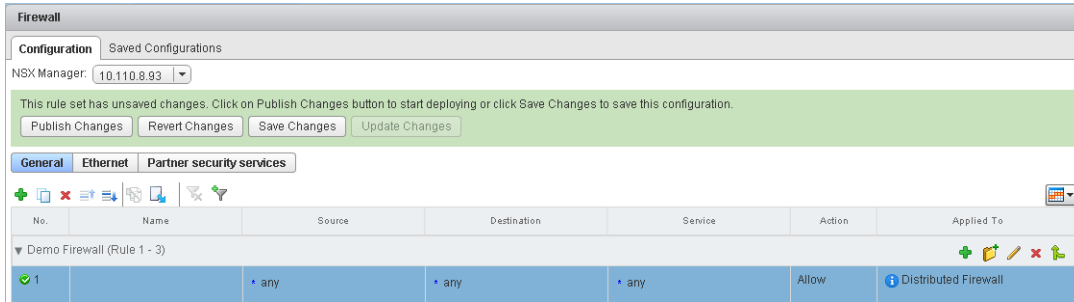
## 添加规则并稍后发布该规则

您可以添加一个规则，并在不发布该规则的情况下保存配置。稍后可以加载和发布已保存的配置。

### 步骤

- 1 添加防火墙规则。请参见[添加防火墙规则](#)。

## 2 单击保存更改。



## 3 键入配置的名称和描述，然后单击确定。

## 4 单击保留配置以保留此更改。

NSX 最多可以保存 100 项配置。超出此限制后，将保留标有保留配置的已保存配置，并会删除较旧的未保留配置，以便为保留的配置释放空间。

## 5 执行以下操作之一。

- 单击恢复更改以恢复添加规则前的配置。如果要发布刚添加的规则，请单击加载配置图标，选择第 3 步中保存的规则，然后单击确定。
- 单击更新更改可继续添加规则。

## 更改防火墙规则的顺序

防火墙规则是按照其在规则表中存在的顺序应用的。

规则按以下顺序显示（并强制执行）：

- 1 用户定义的预规则具有最高优先级，并按照由上到下的顺序强制执行，具有单个虚拟网卡级别的优先级。
- 2 自动检测到的规则。
- 3 在 NSX Edge 级别定义的本地规则。
- 4 服务编排规则 - 每个策略一个单独的区域。不能在防火墙表中编辑这些规则，但是可以在安全策略防火墙规则区域的顶部添加规则。如果执行了此操作，则必须在服务编排中重新同步规则。有关详细信息，请参见第 17 章，服务编排。
- 5 默认分布式防火墙规则

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 在防火墙 (Firewall) 选项卡中，选择要移动的规则。
- 2 单击上移规则 (Move rule up) (≡↑) 或下移规则 (Move rule down) (≡↓) 图标。
- 3 单击发布更改 (Publish Changes)。

## 删除防火墙规则

可以删除您创建的防火墙规则。但不能删除默认规则或由服务编排管理的规则。

### 步骤

- 1 在**防火墙 (Firewall)**选项卡中，选择规则。
- 2 单击位于防火墙表上方的**删除选定的规则 (Delete selected rule)** (✖) 图标。
- 3 单击**发布更改 (Publish Changes)**。

## 从防火墙保护中排除虚拟机

可以从 NSX Distributed Firewall 保护中排除一组虚拟机。

NSX Manager、NSX Controller 和 NSX Edge 虚拟机将自动从 NSX Distributed Firewall 保护中排除。此外，VMware 建议您将以下服务虚拟机放在“排除列表”中以允许流量自由流动。

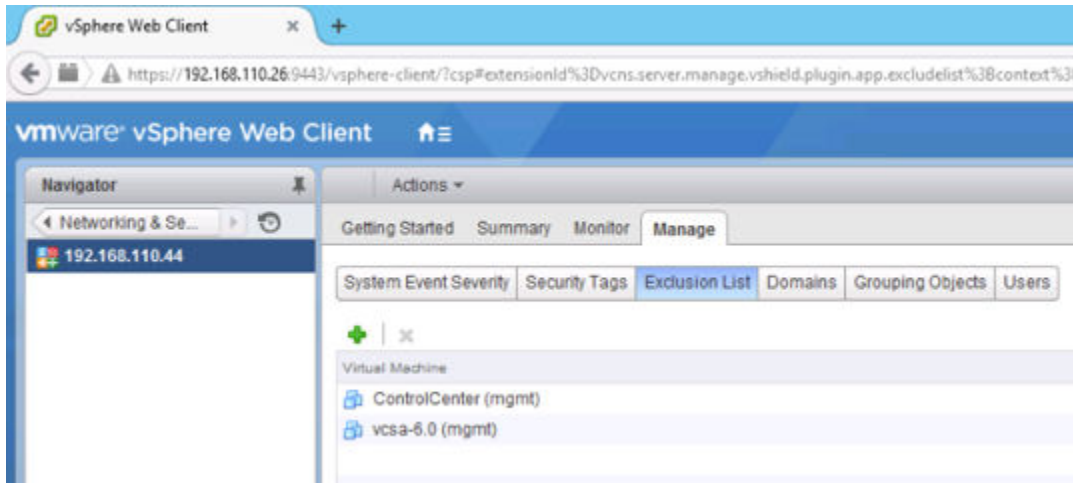
- vCenter Server。可以将其移至受 Firewall 保护的群集中，但其必须已存在于排除列表中，以避免出现连接问题。
- 合作伙伴服务虚拟机。
- 要求杂乱模式的虚拟机。如果这些虚拟机受 NSX Distributed Firewall 保护，则其性能可能会受到不利影响。
- 基于 Windows 的 vCenter 所使用的 SQL Server。
- vCenter Web Server（如果正在单独运行）。

### 步骤

- 1 在 vSphere Web Client 中，单击 **网络和安全 (Networking & Security)**。
- 2 在 **网络和安全清单 (Networking & Security Inventory)** 中，单击 **NSX Manager (NSX Managers)**。
- 3 在 **名称 (Name)** 列中，单击某个 NSX Manager。
- 4 单击 **管理 (Manage)** 选项卡，然后单击 **排除列表 (Exclusion List)** 选项卡。
- 5 单击 **添加 (Add)** (✚) 图标。

## 6 键入要排除的虚拟机的名称，然后单击**添加 (Add)**。

例如：



## 7 单击**确定 (OK)**。

如果虚拟机具有多个虚拟网卡，则它们都将从保护中排除。如果在把虚拟机添加到“排除列表”之后向虚拟机添加虚拟网卡，则会在新添加的虚拟网卡上自动部署防火墙。为了从防火墙保护中排除这些虚拟网卡，必须从“排除列表”中移除该虚拟机，然后将虚拟机重新添加到“排除列表”中。替代解决办法是重启虚拟机（关闭电源后再打开电源），但第一种方案导致的中断比较少。

## 虚拟机的 IP 发现

VMware Tools 在虚拟机上运行并提供多个服务。对于分布式防火墙而言，必不可少的一项服务是将虚拟机及其虚拟网卡与 IP 地址关联起来。在 NSX 6.2 之前，如果未在虚拟机上安装 VMware Tools，则无法获知该虚拟机的 IP 地址。在 NSX 6.2 中，您可以对群集进行配置，使其通过 DHCP 侦听或 ARP 侦听（或两者）来检测虚拟机的 IP 地址。这样，NSX 便能够在虚拟机未安装 VMware Tools 时检测 IP 地址。如果已安装，则 VMware Tools 可与 DHCP 侦听和 ARP 侦听配合工作。

VMware 建议在环境中的每个虚拟机上安装 VMware Tools。除了向 vCenter 提供虚拟机的 IP 地址之外，该工具还提供许多其他功能：

- 允许在虚拟机与主机或客户端桌面之间进行复制和粘贴
- 与主机操作系统同步时间
- 允许通过 vCenter 关闭或重新启动虚拟机
- 从虚拟机收集网络、磁盘和内存的使用情况并发送到主机
- 通过发送和收集检测信号来确定虚拟机的可用性

对于未安装 VMware Tools 的虚拟机，如果该虚拟机的群集已启用 ARP 侦听和 DHCP 侦听，则 NSX 将通过 ARP 侦听或 DHCP 侦听来获知 IP 地址。

## 更改 IP 检测类型

虚拟机的 IP 可由安装在虚拟机上的 VMware Tools 进行检测，也可以通过主机群集上启用的 DHCP 侦听和 ARP 侦听进行检测。在同一 NSX 安装中，这些 IP 发现方法可以结合使用。

### 步骤

- 1 在 vSphere Web Client 中，导航到**网络和安全 > 安装 > 主机准备**。
- 2 单击要更改的群集，然后单击**操作 (⚙️) > 更改 IP 检测类型**。
- 3 选择所需的检测类型，然后单击**确定**。

### 后续步骤

配置 SpoofGuard。

配置默认防火墙规则。

## 查看防火墙 CPU 和内存阈值事件

如果群集是为网络虚拟化而准备的，则会在该群集的所有主机上安装防火墙模块。此模块分配三个堆，一个模块堆用于存储模块参数，一个规则堆用于存储规则、容器和筛选器，一个状态堆用于存储流量。堆大小分配是由可用主机物理内存决定的。堆大小可能会随时间的推移而增大或缩小，具体取决于规则、容器集和连接的数量。管理程序中运行的防火墙模块还使用主机 CPU 来处理数据包。

了解任意指定时间的主机资源使用率可帮助您更好地整理您的服务器使用率和网络设计。

默认 CPU 阈值为 100，内存阈值为 100。可以通过 REST API 调用修改默认阈值。内存和 CPU 使用率超过阈值时，防火墙模块将生成系统事件。有关配置默认阈值的信息，请参见《NSX API 指南》中的“使用内存和 CPU 阈值”。

### 步骤

- 1 在 vSphere Web Client 中，单击**网络和安全 (Networking & Security)**，然后单击**NSX Manager (NSX Managers)**。
- 2 在**名称 (Name)**列中，单击适当的 NSX Manager 的 IP 地址。
- 3 单击**监控 (Monitor)**选项卡，然后单击**系统事件 (System Events)**。

## 防火墙日志

防火墙将生成并存储日志文件，例如审核日志、规则消息日志和系统事件日志。

防火墙将生成三种类型的日志。

- 规则消息日志包括所有访问决定，如每个规则已允许或拒绝的流量（如果已为该规则启用日志记录）。这些日志存储在每个主机的 `/var/log/dfwpktlogs.log` 中。

在以下示例中：

- 1002 是分布式防火墙规则 ID。
- domain-c7 是 vCenter Managed Object Browser (MOB) 中的群集 ID。
- 192.168.110.10/138 是源 IP 地址。
- 192.168.110.255/138 是目标 IP 地址。

```
~ # more /var/log/dfwpktlogs.log

2015-03-10T03:22:22.671Z INET match DROP domain-c7/1002 IN 242 UDP 192.168.110.10/138-
>192.168.110.255/138
```

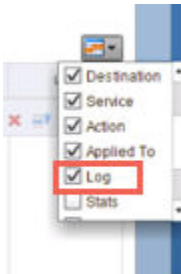
以下示例显示了从 192.168.110.10 到 172.16.10.12 的 Ping 操作的结果。

```
~ # tail -f /var/log/dfwpktlogs.log | grep 192.168.110.10

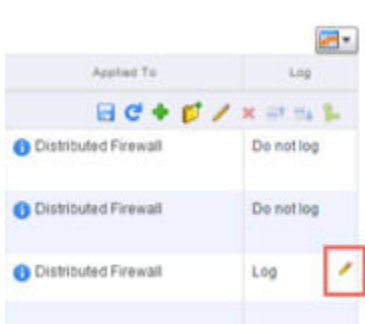
2015-03-10T03:20:31.274Z INET match DROP domain-c27/1002 IN 60 PROTO 1 192.168.110.10->172.16.10.12
2015-03-10T03:20:35.794Z INET match DROP domain-c27/1002 IN 60 PROTO 1 192.168.110.10->172.16.10.12
```

在 vSphere Web Client 6.0 中启用规则消息日志记录（vSphere 5.5 中的 UI 可能稍有不同，但步骤是相同的）：

- a 在**网络和安全 > 防火墙**页面上启用日志列。

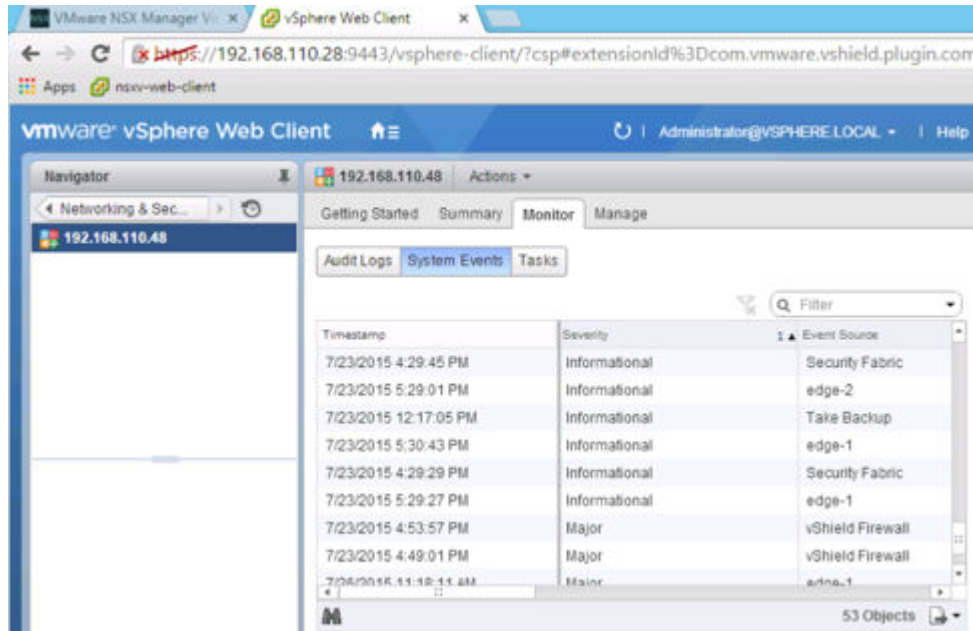


- b 要为某个规则启用日志记录，请将光标悬停在日志表单元格上并单击铅笔图标。



- 审核日志包括管理日志和分布式防火墙配置更改。这些日志存储在 `/home/secureall/secureall/logs/vsm.log` 中。
- 系统事件日志包括分布式防火墙配置已应用，筛选器已创建、删除或失败，以及虚拟机已添加到安全组等。这些日志存储在 `/home/secureall/secureall/logs/vsm.log` 中。

要在 UI 中查看审核日志和系统事件日志，请导航至**网络和安全 > 安装 > 管理**，然后双击 NSX Manager 的 IP 地址。接着选择**监控**选项卡。



有关详细信息，请参见第 23 章，**操作和管理**。

## 使用 NSX Edge 防火墙规则

您可以导航到 NSX Edge 以查看对其应用的防火墙规则。

应用于逻辑路由器的防火墙规则仅保护流入和流出逻辑路由器控制虚拟机的控制层面流量。这些规则不强制执行任何数据层面保护。要保护数据层面流量，请为东西方向保护创建逻辑防火墙规则，或者在 NSX Edge 服务网关级别为南北方向保护创建规则。

在防火墙用户界面上创建的适用于此 NSX Edge 的规则以只读模式显示。规则按以下顺序显示并强制实施：


- 1 用户在防火墙用户界面上定义的规则（只读）。
- 2 自动检测到的规则（用于对 Edge 服务流量启用控制的规则）。
- 3 用户在 NSX Edge 防火墙用户界面上定义的规则。
- 4 默认规则。

## 编辑默认的 NSX Edge 防火墙规则

默认防火墙设置应用于与任何用户定义的防火墙规则均不匹配的流量。默认的 Edge 防火墙策略会阻止所有入站流量。您可以更改默认操作和日志记录设置。

### 步骤

- 1 在 vSphere Web Client 中，导航到**网络和安全 (Networking & Security) > NSX Edge (NSX Edges)**。
- 2 双击一个 NSX Edge。

- 3 单击**管理 (Manage)**选项卡，然后单击**防火墙 (Firewall)**。
- 4 选择**默认规则 (Default Rule)**，此规则是防火墙表中的最后一个规则。
- 5 指向新规则的**操作 (Action)**单元格，然后单击 。
  - a 单击**接受 (Accept)**允许来自或流向指定源和目标的流量。
  - b 单击**记录 (Log)**以记录匹配此规则的所有会话。  
启用日志记录功能可能会影响性能。
  - c 根据需要键入备注。
  - d 单击**确定 (OK)**。
- 6 单击**发布更改 (Publish Changes)**。

## 添加 NSX Edge 防火墙规则

Edge 防火墙选项卡显示在集中式“防火墙”选项卡上采用只读模式创建的规则。您在此添加的任何规则都不显示在集中式“防火墙”选项卡上。

您可以添加多个 NSX Edge 接口和/或 IP 地址组作为防火墙规则的源和目标。

图 10-1. 适用于从 NSX Edge 接口流向 HTTP 服务器的流量的防火墙规则

No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	Traffic to HTTP server	User	vnuc-index-0: any	HTTP Address Group	For HTTP server	Accept
3	Default Rule	Default	any			Deny

HTTP Address Group  
Value:  
10.20.222.34

For HTTP server  
Value:  
TCP:8080

图 10-2. 适用于从 NSX Edge 的所有内部接口（连接到内部接口的端口组上的子网）流向 HTTP 服务器的流量的防火墙规则

No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	Traffic to HTTP server	User	internal	HTTP Address Group	For HTTP server	Accept
3	Default Rule	Default	any			Deny

HTTP Address Group  
Value:  
10.20.222.34

For HTTP server  
Value:  
TCP:8080

**注** 如果选择**内部 (internal)**作为源，则配置其他内部接口时此规则将自动更新。

图 10-3. 允许通过 SSH 方式流入内部网络 m/c 的流量防火墙规则

No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	Traffic to internal network	User	any	VM in internal netw...	Internal VM	Accept
3	Default Rule	Default	any			Deny

VM in internal network  
Value:  
192.168.0.10

Internal VM  
Value:  
TCP:22






## 步骤

- 1 在 vSphere Web Client 中，导航到 **网络和安全 (Networking & Security) > NSX Edge (NSX Edges)**。
- 2 双击一个 NSX Edge。
- 3 单击 **管理 (Manage)** 选项卡，然后单击 **防火墙 (Firewall)** 选项卡。
- 4 执行以下操作之一。

选项	描述
在防火墙表中的特定位置添加规则	<ol style="list-style-type: none"> <li>a 选择规则。</li> <li>b 在“编号”列中，单击 ，然后选择 <b>添加到上方 (Add Above)</b> 或 <b>添加到下方 (Add Below)</b>。</li> </ol> <p>任何允许的新规则将添加到选定规则的下方。如果系统定义的规则是防火墙表中的唯一规则，则新规则将添加到默认规则的上方。</p>
通过复制规则添加规则	<ol style="list-style-type: none"> <li>a 选择规则。</li> <li>b 单击“复制” () 图标。</li> <li>c 选择规则。</li> <li>d 在“编号”列中，单击  并选择 <b>在上方粘贴 (Paste Above)</b> 或 <b>在下方粘贴 (Paste Below)</b>。</li> </ol>
在防火墙表中的任意位置添加规则	<ol style="list-style-type: none"> <li>a 单击 <b>添加 (Add)</b> () 图标。</li> </ol> <p>任何允许的新规则将添加到选定规则的下方。如果系统定义的规则是防火墙表中的唯一规则，则新规则将添加到默认规则的上方。</p>

默认情况下启用新规则。

- 5 指向新规则的名称 (**Name**) 单元，然后单击 。
- 6 键入新规则的名称。
- 7 指向新规则的源 (**Source**) 单元，并单击  或 。

如果单击了 ，则键入一个 IP 地址。

- a 从下拉列表选择一个对象，然后进行相应的选择。

如果选择 **虚拟网卡组 (vNIC Group)**，然后选择 **vse**，则该规则将应用于 NSX Edge 生成的流量。如果选择 **内部 (internal)** 或 **外部 (external)**，则此规则将应用于来自所选 NSX Edge 实例的任何内部或上行链路接口的流量。当配置其他接口时，此规则将自动更新。注意，内部接口上的防火墙规则对逻辑路由器不起作用。

如果选择 **IP 集 (IP Sets)**，则可以创建新的 IP 地址组。创建新组后，它将自动添加到源列中。有关创建 IP 集的信息，请参见 [创建 IP 地址组](#)。

- b 单击 **确定 (OK)**。

## 8 指向新规则的目标 (Destination) 单元，并单击 或 .



### a 从下拉列表中选择一个对象，然后进行相应的选择。

如果选择**虚拟网卡组 (vNIC Group)**，然后选择 **vse**，则该规则将应用于 NSX Edge 生成的流量。如果选择**内部 (internal)**或**外部 (external)**，则此规则将应用于流向所选 NSX Edge 实例的任何内部或上行链路接口的流量。当配置其他接口时，此规则将自动更新。注意，内部接口上的防火墙规则对逻辑路由器不起作用。

如果选择 **IP 集 (IP Sets)**，则可以创建新的 IP 地址组。创建新组后，它将自动添加到源列中。有关创建 IP 集的信息，请参见[创建 IP 地址组](#)。

### b 单击**确定 (OK)**。

## 9 指向新规则的服务 (Service) 单元，并单击 或 .

- 如果单击了 ，则选择一个服务。要创建新服务或服务组，请单击**新建 (New)**。创建新服务后，其自动添加到“服务”列中。有关创建新服务的详细信息，请参见[创建服务](#)。
- 如果单击了 ，则选择一个协议。可以通过单击“高级”选项旁的箭头指定源端口。VMware 建议您从版本 5.1 及更高版本开始不要指定源端口。但可以为协议-端口组合创建服务。


**注** NSX Edge 仅支持使用 L3 协议定义的服务。

## 10 指向新规则的操作 (Action) 单元，然后单击 。选择下表中所描述的相应选项，然后单击**确定 (OK)**。

选定的操作	结果
允许	允许来自或流向指定源和目标的流量。
阻止	阻止来自或流向指定源和目标的流量。
拒绝	针对不被接受的数据包发送拒绝消息。 为 TCP 数据包发送 RST 数据包。 为其他数据包发送 ICMP 不可访问（管理限制）数据包。
日志	记录与此规则匹配的所有会话。启用日志记录功能可能会影响性能。
不记录	不记录会话。
备注	根据需要键入备注。
高级选项 > 转换时匹配	如果是 NAT 规则，则将该规则应用于转换后的 IP 地址和服务
启用规则方向	指出规则是入站规则还是出站规则。 VMware 建议不指定防火墙规则的方向。

## 11 单击**发布更改 (Publish Changes)**将新规则推送到 NSX Edge 实例中。

### 后续步骤

- 禁用规则，方法是单击 （位于**编号 (No.)**列中规则编号的旁边）。
- 隐藏生成的规则或预规则（在集中式“防火墙”选项卡上添加的规则），方法是单击**隐藏生成的规则 (Hide Generated rules)**或**隐藏预规则 (Hide Pre rules)**。

- 通过单击  并选择相应的列，显示规则表中的其他列。

列名称	显示的信息
规则标记	系统为每个规则生成的唯一 ID
日志	记录或不记录此规则的流量
统计信息	单击  可显示受此规则影响的流量（会话数、通信包数和大小）
备注	规则的备注

- 通过在“搜索”字段中键入文本来搜索规则。

## 编辑 NSX Edge 防火墙规则

仅可编辑已在“Edge 防火墙”选项卡中添加的用户定义的防火墙规则。无法在“Edge 防火墙”选项卡上编辑集中式“防火墙”选项卡上添加的规则。

### 步骤

- 1 在 vSphere Web Client 中，导航到 **网络和安全 > NSX Edge**。
- 2 双击一个 NSX Edge。
- 3 单击**监控**选项卡，然后单击**防火墙**选项卡。
- 4 选择要编辑的规则

**注** 您无法更改自动生成的规则或默认规则。

- 5 进行所需更改，然后单击**确定**。
- 6 单击**发布更改**。

## 更改 NSX Edge 防火墙规则的优先级

可以更改“Edge 防火墙”选项卡中添加的用户定义防火墙规则的顺序，以自定义流过 NSX Edge 的流量。例如，假设您有一条允许负载均衡器流量的规则。现在，您可以添加一条规则以拒绝来自特定 IP 地址组的负载均衡器流量，并将此规则置于 LB 允许流量规则的上方。

### 步骤

- 1 在 vSphere Web Client 中，导航到 **网络和安全 > NSX Edge**。
- 2 双击一个 NSX Edge。
- 3 单击**监控**选项卡，然后单击**防火墙**选项卡。
- 4 选择要为其更改优先级的规则。

**注** 您不能更改自动生成的规则或默认规则的优先级。

- 5 单击**上移** () 或**下移** () 图标。

- 6 单击**确定**。
- 7 单击**发布更改**。

## 删除 NSX Edge 防火墙规则

可以删除已在“NSX Edge 防火墙”选项卡中添加的用户定义的防火墙规则。无法在此处删除集中式“防火墙”选项卡上已添加的规则。

### 步骤

- 1 在 vSphere Web Client 中，导航到 **网络和安全 > NSX Edge**。
- 2 双击一个 NSX Edge。
- 3 单击**监控**选项卡，然后单击**防火墙**选项卡。
- 4 选择要删除的规则。

---

**注** 您无法删除自动生成的规则或默认规则。

---

- 5 单击**删除** (✖) 图标。

## 管理 NAT 规则

NSX Edge 提供网络地址转换 (NAT) 服务来将公共地址分配给专用网络内的计算机或计算机组。出于经济和安全目的，使用该技术可限制组织或公司必须使用的公共 IP 地址数。您必须配置 NAT 规则才能访问在专用地址的虚拟机上运行的服务。

NAT 服务配置分为源 NAT (SNAT) 和目标 NAT (DNAT) 规则。

### 添加 SNAT 规则

可以创建源 NAT (SNAT) 规则，以便将源 IP 地址从公共 IP 地址更改为专用 IP 地址或反之。

#### 前提条件

- 转换后的（公共）IP 地址必须已添加到您要在其中添加规则的 NSX Edge 接口。
- 子接口上不支持 SNAT 规则。

#### 步骤

- 1 在 vSphere Web Client 中，导航到 **网络和安全 (Networking & Security) > NSX Edge (NSX Edges)**。
- 2 双击一个 NSX Edge。
- 3 单击**管理 (Manage)**选项卡，然后单击 **NAT** 选项卡。
- 4 单击**添加 (Add)** (✚) 图标，并选择**添加 SNAT 规则 (Add SNAT Rule)**。
- 5 选择要添加规则的接口。  
子接口上不支持 SNAT 规则。

- 6 采用以下格式之一键入原始的源 IP 地址。

格式	示例
IP 地址	192.0.2.0
IP 地址范围	192.0.2.0-192.0.2.24
IP 地址/子网	192.0.2.0/24
任意	

- 7 采用以下格式之一键入转换后的（公共）源 IP 地址。

格式	示例
IP 地址	192.0.2.0
IP 地址范围	192.0.2.0-192.0.2.24
IP 地址/子网	192.0.2.0/24
任意	

- 8 选择已启用 (**Enabled**)以启用该规则。
- 9 单击启用日志记录 (**Enable logging**)以记录地址转换。
- 10 单击确定 (**OK**)添加规则。
- 11 单击发布更改 (**Publish Changes**)。


## 添加 DNAT 规则

可以创建目标 NAT (DNAT) 规则，以便将目标 IP 地址从公共 IP 地址更改为专用 IP 地址或反之。

### 前提条件

原始（公共）IP 地址必须已添加到您要在其上添加规则的 NSX Edge 接口。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击网络和安全 (**Networking & Security**)，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击管理 (**Manage**)选项卡，然后单击 **NAT** 选项卡。
- 5 单击添加 (**Add**) ( 图标，并选择添加 DNAT 规则 (**Add DNAT Rule**)。
- 6 选择要应用 DNAT 规则的接口。
- 7 采用以下格式之一键入原始（公共）IP 地址。

格式	示例
IP 地址	192.0.2.0
IP 地址范围	192.0.2.0 - 192.0.2.24

格式	示例
IP 地址/子网	192.0.2.0/24
任意	

8 键入协议。

9 键入原始端口或端口范围。

格式	示例
端口号	80
端口范围	80-85
任意	

10 采用以下格式之一键入转换后的 IP 地址。

格式	示例
IP 地址	192.0.2.0
IP 地址范围	192.0.2.0 - 192.0.2.24
IP 地址/子网	192.0.2.0/24
任意	

11 键入转换后的端口或端口范围。

格式	示例
端口号	80
端口范围	80-85
任意	

12 选择已启用 (**Enabled**)以启用该规则。

13 选择启用日志记录 (**Enable logging**)以记录地址转换。

14 单击添加 (**Add**)保存该规则。

## 身份防火墙概述

通过使用身份防火墙功能，NSX 管理员可以创建基于 **Active Directory** 用户的 DFW 规则。

IDFW 配置 workflows 简要概述首先介绍了基础架构准备。这包括管理员在每个保护的群集上安装主机准备组件和设置 **Active Directory** 同步，以便 NSX 可以使用 AD 用户和组。接下来，IDFW 必须知道 **Active Directory** 用户登录到的桌面才能应用 DFW 规则。IDFW 可以使用两种方法进行登录检测：**Guest Introspection** 和/或 **Active Directory** 事件日志采集器。**Guest Introspection** 部署在运行 IDFW 虚拟机的 ESXi 群集上。在用户生成网络事件时，在虚拟机上安装的客户机代理将信息通过 **Guest Introspection** 框架转发到 **NSX Manager**。第二种方法是使用 **Active Directory** 事件日志采集器。请在 **NSX Manager** 中配置 **Active Directory** 事件日志采集器以指向一个 **Active Directory** 域控制器实例。然后，**NSX Manager** 从 AD 安全事件日志中提取事件。您可以在环境中同时使用这两种方法，或者使用其中的一种方法。请注意，如果同时使用 AD 事件日志采集器和 **Guest Introspection**，它们是相互排斥的：如果其中的一个组件停止工作，另一个组件不会作为备用组件开始工作。

在准备基础架构后，管理员创建 **NSX** 安全组并添加新的可用 AD 组（称为目录组）。然后，管理员可以创建具有关联的防火墙规则的安全策略，并将这些策略应用于新创建的安全组。现在，在用户登录到桌面时，系统将检测该事件以及使用的 IP 地址，查找与该用户关联的防火墙策略，然后向下推送这些规则。这适用于物理桌面和虚拟桌面。对于物理桌面，还需要使用 AD 事件日志采集器以检测用户是否登录到物理桌面。

## IDFW 支持的操作系统

AD 支持的服务器

- Windows 2012
- Windows 2008
- Windows 2008 R2

支持的客户机操作系统

- Windows 2012
- Windows 2008
- Windows 2008 R2
- Windows 10
- Windows 8 32/64
- Windows 7 32/64

## 身份防火墙工作流

身份防火墙 (IDFW) 允许使用基于用户的分布式防火墙规则 (DFW)。

基于用户的分布式防火墙规则 (DFW) 是由 Active Directory (AD) 组成员的成员身份确定的。IDFW 监控 Active Directory 用户登录到的位置，并将登录名映射到 IP 地址，DFW 使用该地址以应用防火墙规则。身份防火墙需要使用 Guest Introspection 框架和/或 Active Directory 事件日志提取。

### 步骤

- 1 在 NSX 中配置 Active Directory 同步；请参见[将 Windows 域与 Active Directory 同步](#)。需要使用该功能以在服务编排中使用 Active Directory 组。
- 2 为 DFW 准备 ESXi 群集。请参见 NSX 安装指南中的“为 NSX 准备主机群集”。
- 3 配置身份防火墙登录检测选项。请注意，您必须配置下面的一个或两个选项：
  - 配置 Active Directory 事件日志访问。请参见[向 NSX Manager 注册 Windows 域](#)。
  - 安装了客户机代理的 Windows 客户机操作系统。这会提供完整的 VMware Tools™ 安装。将 Guest Introspection 服务部署到保护的群集中。请参见[安装 Guest Introspection](#)。有关 Guest Introspection 故障排除，请参见[收集 Guest Introspection 故障排除数据](#)。



## 使用 Active Directory 域

可以向 NSX Manager 及关联的 vCenter Server 注册一个或多个 Windows 域。NSX Manager 从每个注册的域中获取组 and 用户信息以及两者之间的关系。NSX Manager 还检索 Active Directory (AD) 凭据。

NSX Manager 检索到 AD 凭据后，您可以根据用户标识创建安全组、创建基于标识的防火墙规则以及运行活动监控报告。

本章讨论了以下主题：

- 向 NSX Manager 注册 Windows 域
- 将 Windows 域与 Active Directory 同步
- 编辑 Windows 域
- 在 Windows 2008 上启用安全只读日志访问
- 验证目录权限

### 向 NSX Manager 注册 Windows 域

#### 前提条件

域帐户必须具有域树中所有对象的 AD 读权限。事件日志读取器帐户必须具有安全事件日志的读权限。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Manager (NSX Managers)**。
- 3 在**名称 (Name)**列中单击 NSX Manager，然后单击**管理 (Manage)**选项卡。
- 4 单击**域 (Domain)**选项卡，然后单击**添加域 (Add domain) (+)** 图标。
- 5 在**添加域 (Add Domain)**对话框中，为域输入完全限定域名（例如 `eng.vmware.com`）和 netBIOS 名称。  
要检索域的 netBIOS 名称，可在属于域或位于域控制器上的 Windows 工作站的命令窗口中键入 `nbtstat -n`。在 NetBIOS 本地名称表中，前缀为 <00> 的条目和类型“组”是 netBIOS 名称。
- 6 在同步期间，要筛选出不再具有活动帐户的用户，请单击**忽略禁用的用户 (Ignore disabled users)**。
- 7 单击**下一步 (Next)**。

- 8 在“LDAP 选项”页面中，指定域要与之同步的域控制器，然后选择协议。
- 9 根据需要编辑端口号。
- 10 输入域帐户的用户凭据。此用户必须能够访问目录树结构。
- 11 单击下一步 (Next)。
- 12 (可选) 在“安全事件日志访问”页中，选择 **CIFS** 或 **WMI** 作为连接方法以访问指定的 AD 服务器上的安全事件日志。根据需要更改端口号。Active Directory 事件日志采集器使用该步骤。请参见[身份防火墙工作流](#)。

---

**注** 事件日志读取器从 AD 安全事件日志中查找具有以下 ID 的事件：Windows 2008/2012：4624；Windows 2003：540。事件日志服务器具有 128 MB 限制。在达到该限制时，您可能在安全日志读取器中看到事件 ID 1104。有关详细信息，请参见 <https://technet.microsoft.com/en-us/library/dd315518>。

---

- 13 选择**使用域凭据 (Use Domain Credentials)**以使用 LDAP 服务器用户凭据。要指定进行日志访问的备用域帐户，可取消选中**使用域凭据 (Use Domain Credentials)**，并指定用户名和密码。

指定的帐户必须能够读取在步骤 10 中指定的域控制器上的安全事件日志。

- 14 单击下一步 (Next)。
- 15 在“即将完成”页面上，检查输入的设置。
- 16 单击完成 (Finish)。



**注意** 如果出现的错误消息指出，实体的添加域操作由于域冲突而失败，解决方法是选择“自动合并”。

域创建完毕，其设置将显示在域列表下方。

#### 后续步骤

验证事件日志服务器上的登录事件已启用。

可以添加、编辑、删除、启用或禁用 LDAP 服务器，方法是选择域列表下方面板中的 **LDAP 服务器 (LDAP Servers)** 选项卡。可以通过选择域列表下方面板中的 **事件日志服务器 (Event Log Servers)** 选项卡对事件日志服务器执行相同的任务。添加多个 Windows 服务器（域控制器、Exchange Server 或文件服务器）作为事件日志服务器可改进用户标识关联。

---

**注** 如果使用 IDFW，则仅支持 AD 服务器。

---

## 将 Windows 域与 Active Directory 同步

默认情况下，所有注册的域每隔 3 小时自动与 Active Directory 同步一次。还可以按需同步。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Manager (NSX Managers)**。
- 3 在**名称 (Name)**列中单击 NSX Manager，然后单击**管理 (Manage)**选项卡。

- 4 选择要同步的域。
- 5 单击以下选项之一。

单击	目的
	执行增量同步，将更新上次同步事件后发生更改的本地 AD 对象
	执行完全同步，将更新所有 AD 对象的本地状态

## 编辑 Windows 域

可以编辑域的名称、netBIOS 名称、主 LDAP 服务器以及帐户凭据。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Manager (NSX Managers)**。
- 3 在**名称 (Name)**列中单击 NSX Manager，然后单击**管理 (Manage)**选项卡。
- 4 选择域，然后单击**编辑域 (Edit domain)**图标。
- 5 进行所需更改，然后单击**完成 (Finish)**。

## 在 Windows 2008 上启用安全只读日志访问

IDFW 中的事件日志采集器使用只读安全日志访问。

在创建新的用户帐户后，您必须在基于 Windows 2008 服务器的域部分中启用只读安全日志访问，以便为用户授予只读访问权限。

**注** 您必须在域、树或林的某个域控制器上执行这些步骤。

### 步骤

- 1 导航到**开始 > 管理工具 > Active Directory 用户和计算机 (Start > Administrative Tools > Active Directory Users and Computers)**。
- 2 在导航树中，展开与要启用安全日志访问的域对应的节点。
- 3 在刚展开的节点下面，选择 **Builtin** 节点。
- 4 双击组列表中的 **Event Log Readers**。
- 5 在“Event Log Readers 属性”对话框中，选择**成员 (Members)**选项卡。
- 6 单击**添加... (Add...)**按钮。  
将显示“选择用户、联系人、计算机或组”对话框。
- 7 如果以前为“AD Reader”用户创建一个组，请在“选择用户、联系人、计算机或组”对话框中选择该组。如果仅创建该用户而没有创建组，请在“选择用户、联系人、计算机或组”对话框中选择该用户。

- 8 单击**确定 (OK)**以关闭“选择用户、联系人、计算机或组”对话框。
- 9 单击**确定 (OK)**以关闭“Event Log Readers 属性”对话框。
- 10 关闭“Active Directory 用户和计算机”窗口。

#### 后续步骤

在启用安全日志访问后，请按照[验证目录权限](#)中的步骤验证目录权限。

## 验证目录权限

验证用户帐户是否具有所需的权限以读取安全日志。

在创建新帐户并启用安全日志访问后，您必须验证能否读取安全日志。

#### 前提条件

启用安全日志访问。请参见在 [Windows 2008 上启用安全只读日志访问](#)。

#### 步骤

- 1 从域包含的任何工作站中，以管理员身份登录到域。
- 2 导航到**开始 > 管理工具 > 事件查看器 (Start > Administrative Tools > Event Viewer)**。
- 3 从**操作 (Action)**菜单中选择**连接到另一台计算机... (Connect to Another Computer...)**。将显示“选择计算机”对话框。（请注意，即使已登录到打算查看事件日志的计算机，您也必须执行该操作。）
- 4 如果尚未选择，请选择**另一台计算机 (Another computer)**单选按钮。
- 5 在**另一台计算机 (Another computer)**单选按钮旁边的文本字段中，输入域控制器的名称。或者，单击**浏览... (Browse...)**按钮，然后选择域控制器。
- 6 选中**以其他用户身份连接 (Connect as another user)**复选框。
- 7 单击**设置用户... (Set User...)**按钮。将显示“事件查看器”对话框。
- 8 在**用户名 (User name)**字段中，输入您创建的用户的用户名。
- 9 在**密码 (Password)**字段中，输入您创建的用户密码。
- 10 单击**确定 (OK)**
- 11 再次单击**确定 (OK)**。
- 12 在导航树中展开**Windows 日志 (Windows Logs)**节点。
- 13 在**Windows 日志 (Windows Logs)**节点下面，选择“安全性”节点。如果您可以看见日志事件，则帐户具有所需的权限。

## 使用 SpoofGuard

与 vCenter Server 同步后，NSX Manager 会从每个虚拟机上的 VMware Tools 中收集所有 vCenter 客户机虚拟机的 IP 地址。如果虚拟机被攻击，则 IP 地址可能被假冒，恶意传输信息可能会绕过防火墙策略。

为特定网络创建 SpoofGuard 策略后，您可以授权 VMware Tools 所报告的 IP 地址，并在必要时更改这些地址以防止欺骗。SpoofGuard 本身还信任从 VMX 文件和 vSphere SDK 收集的虚拟机的 MAC 地址。可以在防火墙规则之外使用 SpoofGuard 阻止已确认为虚假的流量。

SpoofGuard 同时支持 IPv4 和 IPv6 地址。使用 IPv4 时，SpoofGuard 策略支持为虚拟网卡分配单个 IP 地址。IPv6 支持为虚拟网卡分配多个 IP 地址。SpoofGuard 策略将以下列模式之一监控和管理虚拟机所报告的 IP 地址。

<b>首次使用时自动信任 IP 分配</b>	此模式允许来自虚拟机的所有流量通过，同时还会构建一个有关虚拟网卡到 IP 地址的分配表。您可在方便时查看此表并更改 IP 地址。此模式将自动批准虚拟网卡上的所有 ipv4 和 ipv6 地址。
------------------------	--------------------------------------------------------------------------------------------------

<b>使用前手动检查和批准所有 IP 分配</b>	此模式会阻止所有流量，直到您批准所有虚拟网卡到 IP 地址分配。
---------------------------	----------------------------------

---

**注** 不管启用哪种模式，SpoofGuard 本身都会允许 DHCP 请求。不过，如果处于手动检测模式，流量将无法通过，除非 DHCP 分配的 IP 地址经过批准。

---

SpoofGuard 包括系统生成的默认策略，该策略会应用于其他 SpoofGuard 策略未涉及的端口组和逻辑网络。新添加的网络会自动添加到默认策略中，除非您将该网络添加到现有策略或为其创建新策略。

SpoofGuard 是 NSX 分布式防火墙策略用来确定虚拟机 IP 地址的方法之一。有关信息，请参见[虚拟机的 IP 发现](#)。

本章讨论了以下主题：

- [创建 SpoofGuard 策略](#)
- [批准 IP 地址](#)
- [编辑 IP 地址](#)
- [清除 IP 地址](#)

## 创建 SpoofGuard 策略

可以创建 SpoofGuard 策略，为特定网络指定操作模式。系统生成的（默认）策略适用于现有 SpoofGuard 策略未覆盖的端口组和逻辑交换机。

### 步骤

- 1 在 vSphere Web Client 中，导航到 **网络和安全 (Networking & Security) > SpoofGuard**。
- 2 单击 **添加 (Add)** 图标。
- 3 键入策略的名称。
- 4 选择 **已启用 (Enabled)** 或 **已禁用 (Disabled)** 以指示是否启用了策略。
- 5 对于 **操作模式 (Operation Mode)**，请选择以下选项之一：

选项	说明
首次使用时自动信任 IP 分配	选择此选项，可在向 NSX Manager 进行初始注册时信任分配的所有 IP。
使用前手动检查和批准所有 IP 分配	选择此选项可要求手动批准所有 IP 地址。所有发送至或发送自未经批准的 IP 地址的流量均会被阻止。

- 6 单击 **在此命名空间中，允许使用本地地址作为有效地址 (Allow local address as valid address in this namespace)**，以便在设置中允许使用本地 IP 地址。

打开虚拟机电源时，如果虚拟机无法连接到 DHCP 服务器，则会为虚拟机分配一个本地 IP 地址。仅当 SpoofGuard 模式设置为 **在此命名空间中，允许使用本地地址作为有效地址 (Allow local address as valid address in this namespace)** 时，才将此本地 IP 地址视为有效。否则，将忽略本地 IP 地址。

- 7 单击 **下一步 (Next)**。
- 8 要指定策略范围，请单击 **添加 (Add)**，然后选择应当应用此策略的网络、分布式端口组或逻辑交换机。一个端口组或逻辑交换机只能属于一个 SpoofGuard 策略。
- 9 单击 **确定 (OK)**，然后单击 **完成 (Finish)**。

### 后续步骤

可以通过单击 **编辑 (Edit)** 图标编辑策略，通过单击 **删除 (Delete)** 图标删除策略。

## 批准 IP 地址

如果将 SpoofGuard 设置为需要对分配的所有 IP 地址进行手动批准，则必须对分配的 IP 地址进行批准，才能允许来自这些虚拟机的流量通过。

### 步骤

- 1 在 **SpoofGuard** 选项卡中，选择策略。  
策略详细信息将显示在策略表下方。

- 2 在视图 (View) 中，单击其中一个选项链接。

选项	说明
活动虚拟网卡	所有经验证的 IP 地址的列表
自上次发布后的活动虚拟网卡	上次更新策略后验证的 IP 地址列表
IP 需经批准的虚拟网卡	IP 地址变更需要首先获得批准，流量方可流入/流出这些虚拟机
具有重复 IP 的虚拟网卡	IP 地址与选定数据中心内现有所分配 IP 地址重复
非活动虚拟网卡	当前 IP 地址与发布的 IP 地址不匹配的 IP 地址列表
未发布的虚拟网卡 IP	您已经编辑其 IP 地址分配但尚未发布的虚拟机列表

- 3 执行以下操作之一。

- 要批准单个 IP 地址，请单击 IP 地址旁边的**批准 (Approve)**。
- 要批准多个 IP 地址，请选择相应的虚拟网卡，然后单击**批准检测到的 IP (Approve Detected IP(s))**。

## 编辑 IP 地址

您可以编辑已分配给 MAC 地址的 IP 地址，以更正所分配的 IP 地址。

**注** SpoofGuard 可接受来自多个虚拟机的唯一 IP 地址。但是，您只能分配一次 IP 地址。经过批准的 IP 地址在 NSX 中是唯一的。不允许出现重复的经过批准的 IP 地址。

### 步骤

- 1 在 **SpoofGuard** 选项卡中，选择策略。

策略详细信息将显示在策略表下方。

- 2 在视图 (View) 中，单击其中一个选项链接。

选项	说明
活动虚拟网卡	所有经验证的 IP 地址的列表
自上次发布后的活动虚拟网卡	上次更新策略后验证的 IP 地址列表
IP 需经批准的虚拟网卡	IP 地址变更需要首先获得批准，流量方可流入/流出这些虚拟机
具有重复 IP 的虚拟网卡	IP 地址与选定数据中心内现有所分配 IP 地址重复
非活动虚拟网卡	当前 IP 地址与发布的 IP 地址不匹配的 IP 地址列表
未发布的虚拟网卡 IP	您已经编辑其 IP 地址分配但尚未发布的虚拟机列表

- 3 对于相应的虚拟网卡，单击**编辑 (Edit)**图标，然后进行适当的更改。

- 4 单击**确定 (OK)**。

## 清除 IP 地址

可清除通过 SpoofGuard 策略批准的 IP 地址分配。

## 步骤

- 1 在 **SpoofGuard** 选项卡中，选择策略。

策略详细信息将显示在策略表下方。

- 2 在**视图 (View)**中，单击其中一个选项链接。

选项	说明
活动虚拟网卡	所有经验证的 IP 地址的列表
自上次发布后的活动虚拟网卡	上次更新策略后验证的 IP 地址列表
IP 需经批准的虚拟网卡	IP 地址变更需要首先获得批准，流量方可流入/流出这些虚拟机
具有重复 IP 的虚拟网卡	IP 地址与选定数据中心内现有所分配 IP 地址重复
非活动虚拟网卡	当前 IP 地址与发布的 IP 地址不匹配的 IP 地址列表
未发布的虚拟网卡 IP	您已经编辑其 IP 地址分配但尚未发布的虚拟机列表

- 3 执行以下操作之一。

- 要清除单个 IP 地址，请单击相应 IP 地址旁边的**清除 (Clear)**。
- 要清除多个 IP 地址，请选择相应的虚拟网卡，然后单击**清除批准的 IP (Clear Approved IP(s))**。



## 虚拟专用网络 (VPN)

NSX Edge 支持多种类型的 VPN。SSL VPN-Plus 允许远程用户访问专用的企业应用程序。IPSec VPN 提供 NSX Edge 实例和远程站点之间的点对点连接。L2 VPN 允许虚拟机跨地域界限保持网络连接，从而可扩展数据中心。

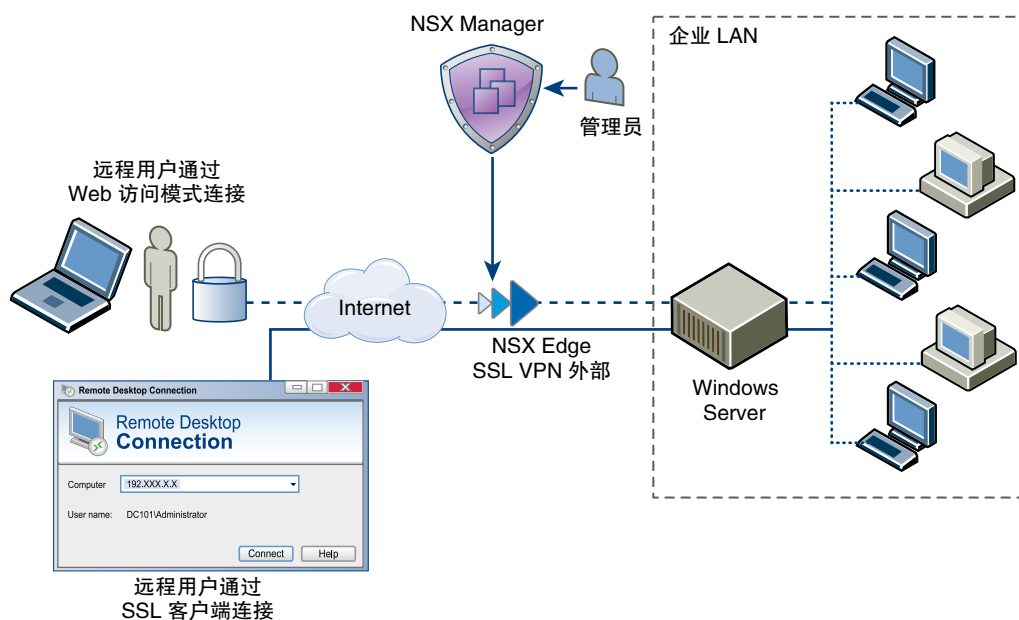
必须有正在运行的 NSX Edge 实例才能使用 VPN。有关设置 NSX Edge 的信息，请参见 [NSX Edge 配置](#)。

本章讨论了以下主题：

- [SSL VPN-Plus 概览](#)
- [IPSec VPN 概览](#)
- [L2 VPN 概述](#)

### SSL VPN-Plus 概览

使用 SSL VPN-Plus，远程用户可以安全地连接到 NSX Edge 网关后面的专用网络。远程用户可以在专用网络内访问服务器和应用程序。



支持以下客户端操作系统：

- Windows XP 及更高版本（支持 Windows 8）。

- Mac OS X Tiger、Leopard、Snow Leopard、Lion、Mountain Lion、Maverick 和 Yosemite。这些系统可以手动安装或使用 Java 安装程序安装。
  - 对于 Linux 系统，需要安装 TCL-TK 方能让 UI 正常运行。如果未提供，可以通过 CLI 使用 Linux 客户端。
- 有关 SSL VPN 故障排除的信息，请参见 <https://kb.vmware.com/kb/2126671>。

## 配置网络访问 SSL VPN-Plus

在网络访问模式中，远程用户可以在下载并安装 SSL 客户端之后访问专用网络。

### 前提条件

SSL VPN 网关要求能够从外部网络访问端口 443，而 SSL VPN 客户端要求能够从客户端系统访问 NSX Edge 网关 IP 和端口 443。

### 步骤

#### 1 添加 SSL VPN-Plus 服务器设置

必须添加 SSL VPN 服务器设置才能在 NSX Edge 接口上启用 SSL。

#### 2 添加 IP 池

从您所添加的 IP 池中为远程用户分配一个虚拟 IP 地址。

#### 3 添加专用网络

添加希望远程用户可以访问的网络。

#### 4 添加身份验证

您可以添加绑定到 SSL 网关的外部身份验证服务器（AD、LDAP、Radius 或 RSA），而不是添加本地用户。将对具有绑定的身份验证服务器上帐户的所有用户进行身份验证。

#### 5 添加安装软件包

为远程用户创建 SSL VPN-Plus 客户端的安装软件包。

#### 6 添加用户

向本地数据库添加远程用户。

#### 7 启用 SSL VPN-Plus 服务

配置 SSL VPN-Plus 服务后，请启用该服务，以便远程用户开始访问专用网络。

#### 8 添加脚本

可以添加多个登录和注销脚本。例如，可以将启动 Internet Explorer 的登录脚本与 gmail.com 绑定。当远程用户登录到 SSL 客户端时，Internet Explorer 即可打开 gmail.com。

#### 9 在远程站点安装 SSL 客户端

本节介绍了在配置 SSL VPN-Plus 后远程用户可以在他/她的桌面上执行的过程。支持 Windows、MAC 和 Linux 桌面。

## 添加 SSL VPN-Plus 服务器设置

必须添加 SSL VPN 服务器设置才能在 NSX Edge 接口上启用 SSL。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板中选择**服务器设置**。
- 2 单击**更改**。
- 3 选择 IPv4 或 IPv6 地址。
- 4 根据需要编辑端口号。配置安装软件包需要此端口号。
- 5 选择加密方法。
- 6 （可选）从“服务器证书”表中选择要添加的服务器证书。
- 7 单击**确定**。

## 添加 IP 池

从您所添加的 IP 池中为远程用户分配一个虚拟 IP 地址。


### 步骤

- 1 在 **SSL Vpn-Plus** 选项卡中，从左侧面板选择 **IP 池 (IP Pools)**。
- 2 单击**添加 (Add)** ( 图标。
- 3 键入 IP 池的开始和结束 IP 地址。
- 4 键入 IP 池的网络掩码。
- 5 键入要在 **NSX Edge** 网关中添加路由接口的 IP 地址。
- 6 （可选）键入 IP 池的描述。
- 7 选择是启用还是禁用 IP 池。
- 8 （可选）在**高级 (Advanced)**面板中，键入 DNS 名称。
- 9 （可选）键入辅助 DNS 名称。
- 10 键入特定连接的 DNS 后缀，以解析基于域的主机名。
- 11 键入 WINS 服务器地址。
- 12 单击**确定 (OK)**。

## 添加专用网络

添加希望远程用户可以访问的网络。

### 步骤

- 1 在 **SSL Vpn-Plus** 选项卡中，从左侧面板中选择**专用网络**。
- 2 单击**添加** () 图标
- 3 键入专用网络 IP 地址。
- 4 键入专用网络的网络掩码。

- 5 （可选）键入网络描述。
- 6 指定是通过已启用 SSL VPN-Plus 的 NSX Edge 发送专用网络和 Internet 流量，还是绕过 NSX Edge 直接将其发送到专用服务器。
- 7 如果选择的是**通过隧道发送流量**，请选择**启用 TCP 优化**来优化网速。

常规完全访问 SSL VPN 隧道会借助于第二个 TCP/IP 堆栈发送 TCP/IP 数据以通过 Internet 进行加密。这将导致应用程序层数据在两个单独的 TCP 流中被封装两次。丢失数据包（在最佳 Internet 条件下也会发生）时，将发生性能降级影响，称为 TCP-over-TCP 危机。从本质上讲，这是由于两个 TCP 设备正在同时更正一个 IP 数据包，这会削弱网络吞吐量，并导致连接超时。TCP 优化消除了此 TCP-over-TCP 问题，确保提供最佳性能。

- 8 如果启用了优化，请指定应进行流量优化的端口号。

该特定网络其余端口的流量将不会优化。

TCP 流量优化后，SSL VPN 服务器将代表客户端打开 TCP 连接。由于 TCP 连接由 SSL VPN 服务器打开，因此将应用自动生成的第一个规则，而此规则将允许从 Edge 打开的所有连接通过。未优化的流量将按常规 Edge 防火墙规则进行评估。默认规则是允许任何流量。

- 9 指定要启用还是禁用专用网络。

- 10 单击**确定**。

#### 后续步骤


添加相应的防火墙规则以允许专用网络流量通过。

## 添加身份验证

您可以添加绑定到 SSL 网关的外部身份验证服务器（AD、LDAP、Radius 或 RSA），而不是添加本地用户。将对具有绑定的身份验证服务器上帐户的所有用户进行身份验证。

通过 SSL VPN 进行身份验证的最长时间为 3 分钟。这是因为非身份验证超时为 3 分钟，且不是可配置属性。因此，在将 AD 身份验证超时设置为超过 3 分钟时，或在链授权中存在多个身份验证服务器且用户身份验证所用时间超过 3 分钟时，将不会对您进行身份验证。

#### 步骤

- 1 在 **SSL Vpn-Plus** 选项卡中，从左侧面板选择**身份验证 (Authentication)**。
- 2 单击**添加 (Add)** ( ) 图标。
- 3 选择身份验证服务器的类型。

#### 4 根据所选身份验证服务器类型，填写以下字段。

##### ◆ AD 身份验证服务器

表 14-1. AD 身份验证服务器选项

选项	描述
启用 SSL (Enable SSL)	如果启用 SSL，将在 Web 服务器与浏览器之间建立一个加密链接。
IP 地址 (IP Address)	身份验证服务器的 IP 地址。
端口 (Port)	显示默认端口名。根据需要进行编辑。
超时 (Timeout)	以秒为单位的时间段，AD 服务器必须在该时间段内作出响应。
状态 (Status)	选择已启用 (Enabled)或已禁用 (Disabled)以指示服务器是否处于启用状态。
搜索库 (Search base)	要搜索的部分外部目录树。该搜索库可能等同于组织、组或外部目录的域名 (AD)。
绑定的 DN (Bind DN)	外部 AD 服务器上的用户，可搜索定义的搜索库内的 AD 目录。大多数情况下，绑定的 DN 可以对整个目录进行搜索。绑定的 DN 的角色是使用 DN（标识名）的查询筛选器和搜索库查询目录，从而对 AD 用户进行身份验证。返回 DN 后，使用 DN 和密码对 AD 用户进行身份验证。
绑定的密码 (Bind Password)	验证 AD 用户身份时使用的密码。
重新键入绑定密码 (Retype Bind Password)	重新键入密码。
登录属性名称 (Login Attribute Name)	与远程用户所输入的用户 ID 相匹配的名称。对于 Active Directory，登录属性名称为 sAMAccountName。
搜索筛选器 (Search Filter)	用来限制搜索的筛选器值。搜索筛选器的格式为 <i>attribute operator value</i> 。
使用此服务器进行第二身份验证 (Use this server for secondary authentication)	如果选择该项，则此 AD 服务器将用作第二级别的身份验证。
在身份验证失败时终止会话 (Terminate Session if authentication fails)	如果选择该项，则当身份验证失败时会话将结束。

##### ◆ LDAP 身份验证服务器

表 14-2. LDAP 身份验证服务器选项

选项	描述
启用 SSL (Enable SSL)	如果启用 SSL，将在 Web 服务器与浏览器之间建立一个加密链接。
IP 地址 (IP Address)	外部服务器的 IP 地址。
端口 (Port)	显示默认端口名。根据需要进行编辑。
超时 (Timeout)	以秒为单位的时间段，AD 服务器必须在该时间段内作出响应。
状态 (Status)	选择已启用 (Enabled)或已禁用 (Disabled)以指示服务器是否处于启用状态。
搜索库 (Search base)	要搜索的部分外部目录树。该搜索库可能等同于组织、组或外部目录的域名 (AD)。
绑定的 DN (Bind DN)	外部服务器上的用户，可搜索定义的搜索库内的 AD 目录。大多数情况下，绑定的 DN 可以对整个目录进行搜索。绑定的 DN 的角色是使用 DN（标识名）的查询筛选器和搜索库查询目录，从而对 AD 用户进行身份验证。返回 DN 后，使用 DN 和密码对 AD 用户进行身份验证。
绑定的密码 (Bind Password)	验证 AD 用户身份时使用的密码。
重新键入绑定密码 (Retype Bind Password)	重新键入密码。
登录属性名称 (Login Attribute Name)	与远程用户所输入的用户 ID 相匹配的名称。对于 Active Directory，登录属性名称为 sAMAccountName。
搜索筛选器 (Search Filter)	用来限制搜索的筛选器值。搜索筛选器的格式为 <i>attribute operator value</i> 。
使用此服务器进行第二身份验证 (Use this server for secondary authentication)	如果选择该项，则此服务器将用作第二级别的身份验证。
在身份验证失败时终止会话 (Terminate Session if authentication fails)	如果选择该项，则当身份验证失败时会话将结束。

## ◆ RADIUS 身份验证服务器

表 14-3. RADIUS 身份验证服务器选项

选项	描述
IP 地址 (IP Address)	外部服务器的 IP 地址。
端口 (Port)	显示默认端口名。根据需要进行编辑。
超时 (Timeout)	以秒为单位的时间段，AD 服务器必须在该时间段内作出响应。
状态 (Status)	选择已启用 (Enabled)或已禁用 (Disabled)以指示服务器是否处于启用状态。
密钥 (Secret)	在 RSA 安全控制台中添加身份验证代理时指定的共享密钥。
重新键入密钥 (Retype secret)	重新键入共享密钥。

表 14-3. RADIUS 身份验证服务器选项（续）

选项	描述
<b>NAS IP 地址 (NAS IP Address)</b>	配置为且用作 RADIUS 属性 4 “NAS-IP-Address” 的 IP 地址，配置时无需更改 RADIUS 数据包的 IP 标头中的源 IP 地址。
<b>重试计数 (Retry Count)</b>	在身份验证失败之前，RADIUS 服务器不响应时，联系该服务器的次数。
<b>使用此服务器进行第二身份验证 (Use this server for secondary authentication)</b>	如果选择该项，则此服务器将用作第二级别的身份验证。
<b>在身份验证失败时终止会话 (Terminate Session if authentication fails)</b>	如果选择该项，则当身份验证失败时会话将结束。

## ◆ RSA-ACE 身份验证服务器

表 14-4. RSA-ACE 身份验证服务器选项

选项	描述
<b>超时 (Timeout)</b>	以秒为单位的时间段，AD 服务器必须在该时间段内作出响应。
<b>配置文件 (Configuration File)</b>	单击 <b>浏览 (Browse)</b> 以选择您从 RSA Authentication Manager 下载的 <code>sdconf.rec</code> 文件。
<b>状态 (Status)</b>	选择 <b>已启用 (Enabled)</b> 或 <b>已禁用 (Disabled)</b> 以指示服务器是否处于启用状态。
<b>源 IP 地址 (Source IP Address)</b>	NSX Edge 接口的 IP 地址，通过该地址可访问 RSA 服务器。
<b>使用此服务器进行第二身份验证 (Use this server for secondary authentication)</b>	如果选择该项，则此服务器将用作第二级别的身份验证。
<b>在身份验证失败时终止会话 (Terminate Session if authentication fails)</b>	如果选择该项，则当身份验证失败时会话将结束。

## ◆ 本地身份验证服务器

表 14-5. 本地身份验证服务器选项

选项	描述
启用密码策略 (Enable password policy)	如果选择该项，则定义密码策略。指定所需值。
启用密码策略 (Enable password policy)	<p>如果选择该项，则定义帐户锁定策略。指定所需值。</p> <ol style="list-style-type: none"> <li>1 在“重试计数”中，键入远程用户在输入错误密码后可以尝试访问其帐户的次数。</li> <li>2 在“重试持续时间”中，键入登录尝试失败后，远程用户的帐户变为锁定状态的时间段。</li> </ol> <p>例如，如果指定“重试计数”为 5，“重试持续时间”为 1 分钟，则当远程用户在 1 分钟内尝试登录 5 次均失败后，其帐户将被锁定。</p> <ol style="list-style-type: none"> <li>3 在“锁定持续时间”中，键入用户帐户将保持锁定的时间段。在此时间后，该帐户将自动解锁。</li> </ol>
状态 (Status)	选择已启用 (Enabled)或已禁用 (Disabled)以指示服务器是否处于启用状态。
使用此服务器进行第二身份验证 (Use this server for secondary authentication)	如果选择该项，则此服务器将用作第二级别的身份验证。
在身份验证失败时终止会话 (Terminate Session if authentication fails)	如果选择该项，则当身份验证失败时会话将结束。

## 添加安装软件包

为远程用户创建 SSL VPN-Plus 客户端的安装软件包。

### 步骤

- 1 在 **SSL Vpn-Plus** 选项卡中，从左侧面板选择**安装软件包**。
- 2 单击**添加 (+)** 图标。
- 3 键入安装软件包的配置文件名称。
- 4 在**网关**中，键入 NSX Edge 公共接口的 IP 地址或 FQDN。

此时该 IP 地址或 FQDN 将绑定到 SSL 客户端。安装该客户端后，此 IP 地址或 FQDN 会显示在 SSL 客户端上。

- 5 键入在服务器设置中为 SSL VPN-Plus 指定的端口号。请参见[添加 SSL VPN-Plus 服务器设置](#)。
- 6 （可选）要将其他 NSX Edge 上行链路接口绑定到 SSL 客户端，请执行以下操作：
  - a 单击**添加 (+)** 图标。
  - b 键入 IP 地址和端口号。
  - c 单击**确定**。



- 7 默认情况下，会为 Windows 操作系统创建安装软件包。选择 Linux 或 Mac，为 Linux 或 Mac 操作系统创建安装软件包。
- 8 （可选）输入安装软件包的描述。
- 9 选择**启用**，以便在“安装软件包”页面上显示安装软件包。
- 10 根据需要选择以下选项。

选项	描述
登录时启动客户端	远程用户登录至其系统时，会启动 SSL VPN 客户端。
允许记住密码	启用该选项。
启用静默模式安装	隐藏远程用户的安装命令。
隐藏 SSL 客户端网络适配器	隐藏与 SSL VPN 安装软件包一起安装在远程用户计算机上的 VMware SSL VPN-Plus 适配器。
隐藏客户端系统托盘图标	隐藏指示 VPN 连接是否处于活动状态的 SSL VPN 托盘图标。
创建桌面图标	创建图标，调用用户桌面上的 SSL 客户端。
启用静默模式操作	隐藏指示安装已完成的弹出窗口。
服务器安全证书验证	在建立安全连接前，SSL VPN 客户端会验证 SSL VPN 服务器证书。

- 11 单击**确定**。

## 添加用户

向本地数据库添加远程用户。

### 步骤


- 1 在 **SSL Vpn-Plus** 选项卡中，从左侧面板选择**用户 (Users)**。
- 2 单击**添加 (Add)** () 图标。
- 3 键入用户 ID。
- 4 键入密码。
- 5 重新键入密码。
- 6 （可选）键入用户的名字和姓氏。
- 7 （可选）键入用户的描述。
- 8 在“密码详细信息”中，选择**密码永不过期 (Password never expires)**，以便始终为用户保持相同的密码。
- 9 选择**允许更改密码 (Allow change password)**，使用户可以更改密码。
- 10 如果要使用户在下次登录时更改密码，请选择**下次登录时更改密码 (Change password on next login)**。
- 11 设置用户状态。
- 12 单击**确定 (OK)**。

## 启用 SSL VPN-Plus 服务

配置 SSL VPN-Plus 服务后，请启用该服务，以便远程用户开始访问专用网络。

### 步骤

1 在 **SSL Vpn-Plus** 选项卡中，从左侧面板中选择**仪表板 (Dashboard)**。

2 单击  **Enable** 图标。

该仪表板显示服务状态、活动 SSL VPN 会话数以及会话统计信息和数据流详细信息。单击“活动会话数”旁边的**详细信息 (Details)**，以查看关于与 NSX Edge 网关背后专用网络的并行连接的信息。


### 后续步骤

- 1 添加一个 SNAT 规则，将 NSX Edge 设备的 IP 地址转换为 VPN Edge IP 地址。
- 2 使用 Web 浏览器键入 **https://NSXEdgeIPAddress**，以导航到 NSX Edge 接口的 IP 地址。
- 3 使用您在[添加用户](#)一节创建的用户名和密码登录，并下载安装软件包。
- 4 对于[添加 SSL VPN-Plus 服务器设置](#)中使用的端口号，在路由器上启用端口转发。
- 5 启动 VN 客户端，选择 VPN 服务器，然后登录。现在即可导航到网络上的服务。SSL VPN-Plus 网关日志将发送到在 NSX Edge 设备上配置的 syslog 服务器。SSL VPN-Plus 客户端日志将存储在远程用户计算机的以下目录中：%PROGRAMFILES%/VMWARE/SSLVPN Client/。

## 添加脚本

可以添加多个登录和注销脚本。例如，可以将启动 Internet Explorer 的登录脚本与 gmail.com 绑定。当远程用户登录到 SSL 客户端时，Internet Explorer 即可打开 gmail.com。

### 步骤

- 1 在 **SSL Vpn-Plus** 选项卡中，从左侧面板选择**登录/注销脚本 (Login/Logoff Scripts)**。
- 2 单击**添加 (Add)** () 图标。
- 3 在**脚本 (Script)**中，单击**浏览 (Browse)**，然后选择要绑定到 NSX Edge 网关的脚本。
- 4 选择脚本的**类型 (Type)**。

选项	说明
登录	当远程用户登录到 SSL VPN 时，执行脚本操作。
注销	当远程用户注销 SSL VPN 时，执行脚本操作。
二者	当远程用户登录和注销 SSL VPN 时，执行脚本操作。

- 5 键入脚本描述。
- 6 选择**已启用 (Enabled)**启用脚本。
- 7 单击**确定 (OK)**。

## 在远程站点安装 SSL 客户端

本节介绍了在配置 SSL VPN-Plus 后远程用户可以在他/她的桌面上执行的过程。支持 Windows、MAC 和 Linux 桌面。

### 步骤

- 1 在客户端站点上，远程用户可以在浏览器窗口中键入 (<https://ExternalEdgeInterfaceIP/sslvpn-plus/>)，其中 *ExternalEdgeInterfaceIP* 是已启用 SSL VPN-Plus 的 Edge 外部接口的 IP 地址。

- 2 使用用户凭据登录到门户。

- 3 单击“完全访问”选项卡。

SSL 客户端已下载。

- 4 使用“用户”部分中指定的凭据登录到 SSL 客户端。

根据客户端操作系统，验证 SSL VPN 服务器证书。

#### ■ Windows 客户端

如果在创建安装软件包时已选中**服务器安全证书验证**选项，则 Windows 客户端已进行身份验证。

#### ■ Linux 客户端

在 NSX for vSphere 版本 6.1.3 及更高版本中，默认情况下，SSL VPN Linux 客户端会根据 Firefox 的证书存储验证服务器证书。如果服务器证书验证失败，则会提示您联系您的系统管理员。如果服务器证书验证成功，则会显示登录提示。

将可信 CA 添加到信任存储（如 Firefox 的证书存储）不会影响 SSL VPN 工作流。

#### ■ OS X 客户端

在 NSX for vSphere 版本 6.1.3 及更高版本中，默认情况下，SSL VPN OS X 客户端会根据 Keychain（OS X 上一种用于存储证书的数据库）验证服务器证书。如果服务器证书验证失败，则会提示您联系您的系统管理员。如果服务器证书验证成功，则会显示登录提示。

将可信 CA 添加到信任存储（如 Keychain）不会影响 SSL VPN 工作流。

远程用户现在即可访问专用网络。

## 配置 Web Access SSL VPN-Plus

在 Web Access 模式中，远程用户可以在没有硬件或软件 SSL 客户端的情况下访问专用网络。

### 步骤

- 1 创建 Web 资源

添加远程用户可以通过 Web 浏览器连接的服务器。

- 2 添加用户

向本地数据库添加远程用户。

### 3 添加身份验证

您可以添加绑定到 SSL 网关的外部身份验证服务器（AD、LDAP、Radius 或 RSA），而不是添加本地用户。将对具有绑定的身份验证服务器上帐户的所有用户进行身份验证。

### 4 添加 SSL VPN-Plus 服务器设置

必须添加 SSL VPN 服务器设置才能在 NSX Edge 接口上启用 SSL。

### 5 启用 SSL VPN-Plus 服务

配置 SSL VPN-Plus 服务后，请启用该服务，以便远程用户开始访问专用网络。

### 6 添加脚本

可以添加多个登录和注销脚本。例如，可以将启动 Internet Explorer 的登录脚本与 gmail.com 绑定。当远程用户登录到 SSL 客户端时，Internet Explorer 即可打开 gmail.com。

## 创建 Web 资源

添加远程用户可以通过 Web 浏览器连接的服务器。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理**选项卡，然后单击 **SSL VPN-Plus** 选项卡。
- 5 从左侧面板中选择 **Web 资源**。
- 6 单击**添加 (+)** 图标。
- 7 键入 Web 资源的名称。
- 8 键入希望远程用户访问的 Web 资源的 URL。
- 9 根据远程用户是要读取还是要写入 Web 资源，选择 **HTTP 方法**并键入 GET 或 POST 调用。
- 10 键入 Web 资源的描述。当远程用户访问 Web 资源时，此描述会显示在 Web 门户上。
- 11 选择**启用**以启用 Web 资源。必须启用 Web 资源，远程用户才能对其进行访问。

## 添加用户

向本地数据库添加远程用户。

#### 步骤

- 1 在 **SSL Vpn-Plus** 选项卡中，从左侧面板选择**用户 (Users)**。
- 2 单击**添加 (Add) (+)** 图标。
- 3 键入用户 ID。
- 4 键入密码。


- 5 重新键入密码。
- 6 （可选）键入用户的名字和姓氏。
- 7 （可选）键入用户的描述。
- 8 在“密码详细信息”中，选择**密码永不过期 (Password never expires)**，以便始终为用户保持相同的密码。
- 9 选择**允许更改密码 (Allow change password)**，使用户可以更改密码。
- 10 如果要使用户在下次登录时更改密码，请选择**下次登录时更改密码 (Change password on next login)**。
- 11 设置用户状态。
- 12 单击**确定 (OK)**。

## 添加身份验证

您可以添加绑定到 SSL 网关的外部身份验证服务器（AD、LDAP、Radius 或 RSA），而不是添加本地用户。将对具有绑定的身份验证服务器上帐户的所有用户进行身份验证。

通过 SSL VPN 进行身份验证的最长时间为 3 分钟。这是因为非身份验证超时为 3 分钟，且不是可配置属性。因此，在将 AD 身份验证超时设置为超过 3 分钟时，或在链授权中存在多个身份验证服务器且用户身份验证所用时间超过 3 分钟时，将不会对您进行身份验证。

### 步骤

- 1 在 **SSL Vpn-Plus** 选项卡中，从左侧面板选择**身份验证 (Authentication)**。
- 2 单击**添加 (Add)** () 图标。
- 3 选择身份验证服务器的类型。
- 4 根据所选身份验证服务器类型，填写以下字段。

#### ◆ AD 身份验证服务器

表 14-6. AD 身份验证服务器选项

选项	描述
<b>启用 SSL (Enable SSL)</b>	如果启用 SSL，将在 Web 服务器与浏览器之间建立一个加密链接。
<b>IP 地址 (IP Address)</b>	身份验证服务器的 IP 地址。
<b>端口 (Port)</b>	显示默认端口名。根据需要进行编辑。
<b>超时 (Timeout)</b>	以秒为单位的时间段，AD 服务器必须在该时间段内作出响应。
<b>状态 (Status)</b>	选择 <b>已启用 (Enabled)</b> 或 <b>已禁用 (Disabled)</b> 以指示服务器是否处于启用状态。
<b>搜索库 (Search base)</b>	要搜索的部分外部目录树。该搜索库可能等同于组织、组或外部目录的域名 (AD)。
<b>绑定的 DN (Bind DN)</b>	外部 AD 服务器上的用户，可搜索定义的搜索库内的 AD 目录。大多数情况下，绑定的 DN 可以对整个目录进行搜索。绑定的 DN 的角色是使用 DN（标识名）的查询筛选器和搜索库查询目录，从而对 AD 用户进行身份验证。返回 DN 后，使用 DN 和密码对 AD 用户进行身份验证。

表 14-6. AD 身份验证服务器选项（续）

选项	描述
绑定的密码 (Bind Password)	验证 AD 用户身份时使用的密码。
重新键入绑定密码 (Retype Bind Password)	重新键入密码。
登录属性名称 (Login Attribute Name)	与远程用户所输入的用户 ID 相匹配的名称。对于 Active Directory，登录属性名称为 <b>sAMAccountName</b> 。
搜索筛选器 (Search Filter)	用来限制搜索的筛选器值。搜索筛选器的格式为 <i>attribute operator value</i> 。
使用此服务器进行第二身份验证 (Use this server for secondary authentication)	如果选择该项，则此 AD 服务器将用作第二级别的身份验证。
在身份验证失败时终止会话 (Terminate Session if authentication fails)	如果选择该项，则当身份验证失败时会话将结束。

## ◆ LDAP 身份验证服务器

表 14-7. LDAP 身份验证服务器选项

选项	描述
启用 SSL (Enable SSL)	如果启用 SSL，将在 Web 服务器与浏览器之间建立一个加密链接。
IP 地址 (IP Address)	外部服务器的 IP 地址。
端口 (Port)	显示默认端口名。根据需要进行编辑。
超时 (Timeout)	以秒为单位的时间段，AD 服务器必须在该时间段内作出响应。
状态 (Status)	选择已启用 (Enabled)或已禁用 (Disabled)以指示服务器是否处于启用状态。
搜索库 (Search base)	要搜索的部分外部目录树。该搜索库可能等同于组织、组或外部目录的域名 (AD)。
绑定的 DN (Bind DN)	外部服务器上的用户，可搜索定义的搜索库内的 AD 目录。大多数情况下，绑定的 DN 可以对整个目录进行搜索。绑定的 DN 的角色是使用 DN（标识名）的查询筛选器和搜索库查询目录，从而对 AD 用户进行身份验证。返回 DN 后，使用 DN 和密码对 AD 用户进行身份验证。
绑定的密码 (Bind Password)	验证 AD 用户身份时使用的密码。

表 14-7. LDAP 身份验证服务器选项（续）

选项	描述
重新键入绑定密码 (Retype Bind Password)	重新键入密码。
登录属性名称 (Login Attribute Name)	与远程用户所输入的用户 ID 相匹配的名称。对于 Active Directory，登录属性名称为 <code>sAMAccountName</code> 。
搜索筛选器 (Search Filter)	用来限制搜索的筛选器值。搜索筛选器的格式为 <i>attribute operator value</i> 。
使用此服务器进行第二身份验证 (Use this server for secondary authentication)	如果选择该项，则此服务器将用作第二级别的身份验证。
在身份验证失败时终止会话 (Terminate Session if authentication fails)	如果选择该项，则当身份验证失败时会话将结束。

## ◆ RADIUS 身份验证服务器

表 14-8. RADIUS 身份验证服务器选项

选项	描述
IP 地址 (IP Address)	外部服务器的 IP 地址。
端口 (Port)	显示默认端口名。根据需要进行编辑。
超时 (Timeout)	以秒为单位的时间段，AD 服务器必须在该时间段内作出响应。
状态 (Status)	选择已启用 (Enabled)或已禁用 (Disabled)以指示服务器是否处于启用状态。
密钥 (Secret)	在 RSA 安全控制台中添加身份验证代理时指定的共享密钥。
重新键入密钥 (Retype secret)	重新键入共享密钥。
NAS IP 地址 (NAS IP Address)	配置为且用作 RADIUS 属性 4 “NAS-IP-Address” 的 IP 地址，配置时无需更改 RADIUS 数据包的 IP 标头中的源 IP 地址。
重试计数 (Retry Count)	在身份验证失败之前，RADIUS 服务器不响应时，联系该服务器的次数。

表 14-8. RADIUS 身份验证服务器选项（续）

选项	描述
使用此服务器进行第二身份验证 (Use this server for secondary authentication)	如果选择该项，则此服务器将用作第二级别的身份验证。
在身份验证失败时终止会话 (Terminate Session if authentication fails)	如果选择该项，则当身份验证失败时会话将结束。

## ◆ RSA-ACE 身份验证服务器

表 14-9. RSA-ACE 身份验证服务器选项

选项	描述
超时 (Timeout)	以秒为单位的时间段，AD 服务器必须在该时间段内作出响应。
配置文件 (Configuration File)	单击 <b>浏览 (Browse)</b> 以选择您从 RSA Authentication Manager 下载的 <code>sdconf.rec</code> 文件。
状态 (Status)	选择已启用 (Enabled)或已禁用 (Disabled)以指示服务器是否处于启用状态。
源 IP 地址 (Source IP Address)	NSX Edge 接口的 IP 地址，通过该地址可访问 RSA 服务器。
使用此服务器进行第二身份验证 (Use this server for secondary authentication)	如果选择该项，则此服务器将用作第二级别的身份验证。
在身份验证失败时终止会话 (Terminate Session if authentication fails)	如果选择该项，则当身份验证失败时会话将结束。

## ◆ 本地身份验证服务器



表 14-10. 本地身份验证服务器选项

选项	描述
启用密码策略 (Enable password policy)	如果选择该项，则定义密码策略。指定所需值。
启用密码策略 (Enable password policy)	<p>如果选择该项，则定义帐户锁定策略。指定所需值。</p> <ol style="list-style-type: none"> <li>1 在“重试计数”中，键入远程用户在输入错误密码后可以尝试访问其帐户的次数。</li> <li>2 在“重试持续时间”中，键入登录尝试失败后，远程用户的帐户变为锁定状态的时间段。</li> </ol> <p>例如，如果指定“重试计数”为 5，“重试持续时间”为 1 分钟，则当远程用户在 1 分钟内尝试登录 5 次均失败后，其帐户将被锁定。</p> <ol style="list-style-type: none"> <li>3 在“锁定持续时间”中，键入用户帐户将保持锁定的时间段。在此时间后，该帐户将自动解锁。</li> </ol>
状态 (Status)	选择已启用 (Enabled)或已禁用 (Disabled)以指示服务器是否处于启用状态。
使用此服务器进行第二身份验证 (Use this server for secondary authentication)	如果选择该项，则此服务器将用作第二级别的身份验证。
在身份验证失败时终止会话 (Terminate Session if authentication fails)	如果选择该项，则当身份验证失败时会话将结束。

## 添加 SSL VPN-Plus 服务器设置

必须添加 SSL VPN 服务器设置才能在 NSX Edge 接口上启用 SSL。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板中选择**服务器设置**。
- 2 单击**更改**。
- 3 选择 IPv4 或 IPv6 地址。
- 4 根据需要编辑端口号。配置安装软件包需要此端口号。
- 5 选择加密方法。
- 6 （可选）从“服务器证书”表中选择要添加的服务器证书。
- 7 单击**确定**。

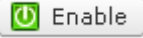
## 启用 SSL VPN-Plus 服务

配置 SSL VPN-Plus 服务后，请启用该服务，以便远程用户开始访问专用网络。

### 步骤

- 1 在 **SSL Vpn-Plus** 选项卡中，从左侧面板中选择**仪表板 (Dashboard)**。

2

单击  图标。

该仪表板显示服务状态、活动 SSL VPN 会话数以及会话统计信息和数据流详细信息。单击“活动会话数”旁边的**详细信息 (Details)**，以查看关于与 NSX Edge 网关背后专用网络的并行连接的信息。


### 后续步骤

- 1 添加一个 SNAT 规则，将 NSX Edge 设备的 IP 地址转换为 VPN Edge IP 地址。
- 2 使用 Web 浏览器键入 **https://NSXEdgeIPAddress**，以导航到 NSX Edge 接口的 IP 地址。
- 3 使用您在[添加用户](#)一节创建的用户名和密码登录，并下载安装软件包。
- 4 对于[添加 SSL VPN-Plus 服务器设置](#)中使用的端口号，在路由器上启用端口转发。
- 5 启动 VN 客户端，选择 VPN 服务器，然后登录。现在即可导航到网络上的服务。SSL VPN-Plus 网关日志将发送到在 NSX Edge 设备上配置的 syslog 服务器。SSL VPN-Plus 客户端日志将存储在远程用户计算机的以下目录中：`%PROGRAMFILES%/VMWARE/SSLVPN Client/`。

## 添加脚本

可以添加多个登录和注销脚本。例如，可以将启动 Internet Explorer 的登录脚本与 gmail.com 绑定。当远程用户登录到 SSL 客户端时，Internet Explorer 即可打开 gmail.com。

### 步骤

- 1 在 **SSL Vpn-Plus** 选项卡中，从左侧面板选择**登录/注销脚本 (Login/Logoff Scripts)**。
- 2 单击**添加 (Add)** () 图标。
- 3 在**脚本 (Script)**中，单击**浏览 (Browse)**，然后选择要绑定到 NSX Edge 网关的脚本。
- 4 选择脚本的**类型 (Type)**。

选项	说明
登录	当远程用户登录到 SSL VPN 时，执行脚本操作。
注销	当远程用户注销 SSL VPN 时，执行脚本操作。
二者	当远程用户登录和注销 SSL VPN 时，执行脚本操作。

- 5 键入脚本描述。
- 6 选择已启用 (**Enabled**)启用脚本。
- 7 单击**确定 (OK)**。

## SSL VPN-Plus 日志

SSL VPN-Plus 网关日志将发送到在 NSX Edge 设备上配置的 syslog 服务器。SSL VPN-Plus 客户端日志将存储在远程用户计算机的以下目录中：`%PROGRAMFILES%/VMWARE/SSL VPN Client/`。

## 编辑客户端配置

可以更改远程用户登录到 SSL VPN 时 SSL VPN 客户端隧道响应的方式。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板选择**客户端配置 (Client Configuration)**。
- 2 选择**隧道模式 (Tunneling Mode)**。  
在拆分隧道模式中，只有 VPN 会流过 NSX Edge 网关。在全隧道模式中，NSX Edge 网关将变为远程用户的默认网关，并且所有流量（VPN、本地和 Internet）都将流过此网关。
- 3 如果已选择了全隧道模式：
  - a 请选择**排除本地子网 (Exclude local subnets)**以便排除本地流量，使其不流过 VPN 隧道。
  - b 为远程用户系统的默认网关键入 IP 地址。
- 4 如果要使远程用户在断开连接后自动重新连接到 SSL VPN 客户端，请选择**启用自动重新连接 (Enable auto reconnect)**。
- 5 当客户端存在可用升级时，请选择**客户端升级通知 (Client upgrade notification)**以通知远程用户。远程用户随后可以选择安装升级。
- 6 单击**确定 (OK)**。

## 编辑常规设置

可以编辑默认的 VPN 设置。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板选择**常规设置**。
- 2 进行所需的选择。

选择	目的
禁止使用相同用户名进行多次登录	仅允许一个远程用户使用一个用户名登录一次。
启用压缩	启用基于 TCP 的智能数据压缩并提高数据传输速度。
启用日志记录	保留通过 SSL VPN 网关的流量日志。
强制虚拟键盘	仅允许远程用户通过虚拟键盘输入 Web 或客户端登录信息。
虚拟键盘的随机按键	使虚拟键盘按键具有随机性。
启用强制超时	指定的超时期限结束后断开远程用户的连接。键入超时期限（以分钟为单位）。
会话闲置超时	如果在指定期限内用户会话中没有活动，则在该期限结束后结束用户会话。
用户通知	输入远程用户登录后可看到的消息。
启用公共 URL 访问	允许远程用户访问管理员未配置（并且在 Web 门户上未列出）的任何站点。

- 3 单击**确定**。

## 编辑 Web 门户设计

可以编辑绑定到 SSL VPN 客户端的客户端横幅。

### 步骤

- 1 在 **NSX Edge** 选项卡中，双击 **NSX Edge**。
- 2 单击 **监控** 选项卡，然后单击 **SSL VPN-Plus** 选项卡。
- 3 从左侧面板中选择 **门户自定义**。
- 4 键入门户标题。
- 5 键入远程用户的公司名称。
- 6 在 **徽标** 中，单击 **更改**，然后为远程用户的徽标选择图像文件。
- 7 在 **颜色** 中，单击要为其更改颜色的已编号项目旁边的颜色框，然后选择所需的颜色。
- 8 如果需要，可更改客户端横幅。
- 9 单击 **确定**。

## 使用 IP 池


可以编辑或删除 IP 池。

有关添加 IP 池的信息，请参见[配置网络访问 SSL VPN-Plus](#) 或[配置 Web Access SSL VPN-Plus](#)。

### 编辑 IP 池

可以编辑 IP 池。

#### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击 **IP 池 (IP Pool)**。
- 2 选择要编辑的 IP 池。
- 3 单击 **编辑 (Edit)** ( ) 图标。  
此时将打开“编辑 IP 池”对话框。
- 4 根据需要进行编辑。
- 5 单击 **确定 (OK)**。

### 删除 IP 池

可以删除 IP 池。

#### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击 **IP 池 (IP Pool)**。

- 2 选择要删除的 IP 池。
- 3 单击删除 (Delete) (✖) 图标。  
所选的 IP 池将被删除。

## 启用 IP 池

如果要将某 IP 池中的 IP 地址分配给远程用户，您可以启用该池。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击 **IP 池 (IP Pool)**。
- 2 选择要启用的 IP 池。
- 3 单击启用 (Enable) (✓) 图标。

## 禁用 IP 池

如果不希望将某个 IP 池中的 IP 地址分配给远程用户，您可以禁用该池。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板中选择 **IP 池 (IP Pool)**。
- 2 选择要禁用的 IP 池。
- 3 单击禁用 (Disable) (⊘) 图标。

## 更改 IP 池的顺序

SSL VPN 将基于 IP 池在 IP 池表中的顺序将池中的 IP 地址分配给远程用户。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击 **IP 池 (IP Pool)**。
- 2 选择要更改顺序的 IP 池。
- 3 单击上移 (Move Up) (⇧) 或“下移” (⇩) 图标。

## 使用专用网络

可以编辑或删除远程用户可访问的专用网络。


有关添加专用网络的信息，请参见[配置网络访问 SSL VPN-Plus](#) 或[配置 Web Access SSL VPN-Plus](#)。

## 删除专用网络

可以删除专用网络。

### 步骤


- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击**专用网络 (Private Networks)**。

- 2 选择您要删除的网络，然后单击**删除 (Delete)** () 图标。

## 启用专用网络

如果启用专用网络，则远程用户可以通过 **SSL VPN-Plus** 对其进行访问。

### 步骤


- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击**专用网络 (Private Networks)**。
- 2 单击要启用的网络。
- 3 单击**启用 (Enable)**图标 ()。

所选网络将启用。

## 禁用专用网络

如果禁用专用网络，则远程用户将无法通过 **SSL VPN-Plus** 访问它。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击**专用网络 (Private Networks)**。
- 2 单击要禁用的网络。
- 3 单击**禁用 (Disable)** () 图标。




所选网络将被禁用。

## 更改专用网络顺序

通过 **SSL VPN-Plus**，远程用户可以按照专用网络在“专用网络”面板中显示的顺序对其进行访问。

如果针对某个专用网络选择**启用 TCP 优化**，则某些应用程序（如处于“活动”模式下的 **FTP**）可能无法在该子网内正常工作。要添加在“活动”模式下配置的 **FTP** 服务器，必须在禁用 **TCP 优化** 的情况下为该 **FTP** 服务器添加其他专用网络。此外，必须启用活动的 **TCP** 专用网络，并且必须将其置于子网专用网络之上。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击**专用网络**。
- 2 单击**更改顺序** () 图标。
- 3 选择要更改顺序的网络。
- 4 单击**上移** () 或**下移** () 图标。
- 5 单击**确定**。

## 使用安装软件包


可以删除或编辑 SSL 客户端的安装软件包。

有关创建安装软件包的信息，请参见[配置网络访问 SSL VPN-Plus](#) 或[配置 Web Access SSL VPN-Plus](#)。

### 编辑安装软件包

可以编辑安装软件包。


#### 步骤

- 1 在 **SSL Vpn-Plus** 选项卡中，从左側面板中选择**安装软件包 (Installation Package)**。
- 2 选择要编辑的安装软件包。
- 3 单击“编辑”() 图标。  
此时将打开“编辑安装软件包”对话框。
- 4 根据需要进行编辑。
- 5 单击**确定 (OK)**。

### 删除安装软件包

可以删除安装软件包。

#### 步骤

- 1 在 **SSL Vpn-Plus** 选项卡中，从左側面板中选择**安装软件包 (Installation Package)**。
- 2 选择要删除的安装软件包。
- 3 单击**删除 (Delete)** () 图标。

## 使用用户


可以从本地数据库编辑或删除用户。

有关添加用户的信息，请参见[配置网络访问 SSL VPN-Plus](#) 或[配置 Web Access SSL VPN-Plus](#)。

### 编辑用户

可以编辑用户的详细信息（用户 ID 除外）。

#### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左側面板单击**用户 (Users)**。
- 2 单击**编辑 (Edit)** () 图标。
- 3 根据需要进行编辑。
- 4 单击**确定 (OK)**。

## 删除用户

可以删除用户。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击**用户 (Users)**。
- 2 用户 (Users)在**配置 (Configure)**面板中，单击**用户 (Users)**。
- 3 选择要删除的用户，然后单击**删除 (Delete)** () 图标。

## 更改用户的密码

可以更改用户的密码。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击**用户 (Users)**。
- 2 单击**更改密码 (Change Password)**图标。
- 3 键入新密码，然后重新键入一次。
- 4 单击“下次登录时更改密码”，以使用户下次登录到系统时更改密码。
- 5 单击**确定 (OK)**。


## 使用登录和注销脚本

可以将登录或注销脚本绑定到 NSX Edge 网关。

## 编辑脚本

可以编辑绑定到 NSX Edge 网关的登录或注销脚本的类型、描述和状态。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击**登录/注销脚本 (Login/Logoff Scripts)**。
- 2 选择脚本并单击**编辑 (Edit)** () 图标。
- 3 进行适当更改。
- 4 单击**确定 (OK)**。

## 删除脚本

可以删除登录或注销脚本。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击**登录/注销脚本 (Login/Logoff Scripts)**。



- 2 选择脚本并单击删除 (Delete) (✖) 图标。

## 启用脚本

必须启用脚本才能使脚本运行。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击登录/注销脚本 (Login/Logoff Scripts)。
- 2 选择脚本并单击启用 (Enable) (✓) 图标。

## 禁用脚本

可以禁用登录/注销脚本。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击登录/注销脚本 (Login/Logoff Scripts)。
- 2 选择脚本并单击禁用 (Disable) (⛔) 图标。

## 更改脚本的顺序

可以更改脚本的顺序。例如，假设您在 Internet Explorer 中将打开 gmail.com 的登录脚本放置在打开 yahoo.com 的登录脚本之上，则当远程用户登录到 SSL VPN 时，gmail.com 会显示在 yahoo.com 之前。如果现在互换登录脚本的顺序，则 yahoo.com 将显示在 gmail.com 之前。

### 步骤

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击登录/注销脚本 (Login/Logoff Scripts)。
- 2 选择要更改顺序的脚本，然后单击上移 (Move Up) (⇧) 或下移 (Move Down) (⇩) 图标。
- 3 单击确定 (OK)。

## IPSec VPN 概览

NSX Edge 支持在 NSX Edge 实例与远程站点之间实施点对点 IPSec VPN。在 NSX Edge 实例与远程 VPN 路由器之间，支持证书身份验证、预共享密钥模式、IP 单播通信和非动态路由协议。

在每个远程 VPN 路由器后面，您可以将多个子网配置为通过 IPSec 通道连接到位于 NSX Edge 后面的内部网络。

---

**注** 子网和位于 NSX Edge 后面的内部网络的地址范围不能重叠。

---

如果通过 IPsec VPN 连接的本地网络和远程对等子网具有重叠的 IP 地址，则跨通道转发的流量可能不连贯，具体取决于是否存在本地连接的路由和自动检测到的路由。

可以在 NAT 设备后面部署 NSX Edge 代理。在此部署中，NAT 设备将 NSX Edge 实例的 VPN 地址转换为面向 Internet 的公开访问地址。远程 VPN 路由器可使用此公共地址访问 NSX Edge 实例。

您也可以将远程 VPN 路由器置于 NAT 设备的后面。您必须同时提供 VPN 本地地址和 VPN 网关 ID 以设置隧道。在通道两端，VPN 地址需要静态一对一 NAT。

所需的通道数量由本地子网数量乘以对等子网数量计算而得。例如，如果有 10 个本地子网和 10 个对等子网，则需要 100 个通道。支持的最大通道数量由 ESG 大小决定，如下所示。

**表 14-11. 每个 ESG 的 IPSec 通道数量**

ESG	IPSec 通道数量
精简	512
中型	1600
大型	4096
超大型	6000

支持以下 IPSec VPN 算法：

- AES (AES128-CBC)
- AES256 (AES256-CBC)
- 三重 DES (3DES192-CBC)
- AES-GCM (AES128-GCM)
- DH-2 (Diffie – Hellman group 2)
- DH-5 (Diffie – Hellman group 5)

有关 IPSec VPN 配置示例，请参见第 24 章，NSX Edge VPN 配置示例。

有关 IPSec VPN 故障排除，请参见 <https://kb.vmware.com/kb/2123580>。

## 配置 IPSec VPN 服务

可以在本地子网与对等子网之间设置一个 NSX Edge 隧道。

**注** 如果通过 IPSec VPN 连接到远程站点，则该站点的 IP 地址无法由 Edge 上行链路中的动态路由所获知。

### 1 启用 IPSec VPN 服务

必须启用 IPSec VPN 服务，以便流量从本地子网流向对等子网。

### 2 使用 OpenSSL 为 IPSec VPN 生成 CA 签名证书

要为 IPSec 启用证书身份验证，您必须导入服务器证书和相应的 CA 签名证书。或者，您也可以使用诸如 OpenSSL 等开源命令行工具生成 CA 签名证书。

### 3 指定全局 IPSec VPN 配置

该操作将在 NSX Edge 实例上启用 IPSec VPN。

### 4 为 IPSec VPN 启用日志记录

可以对所有 IPSec VPN 流量启用日志记录。

## 5 配置 IPsec VPN 参数

必须在 NSX Edge 上至少配置一个外部 IP 地址才能提供 IPsec VPN 服务。

### 启用 IPsec VPN 服务

必须启用 IPsec VPN 服务，以便流量从本地子网流向对等子网。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击 **VPN** 选项卡。
- 5 单击 **IPsec VPN**。
- 6 单击**启用 (Enable)**。

### 使用 OpenSSL 为 IPsec VPN 生成 CA 签名证书

要为 IPsec 启用证书身份验证，您必须导入服务器证书和相应的 CA 签名证书。或者，您也可以使用诸如 OpenSSL 等开源命令行工具生成 CA 签名证书。

#### 前提条件

必须安装 OpenSSL。

#### 步骤

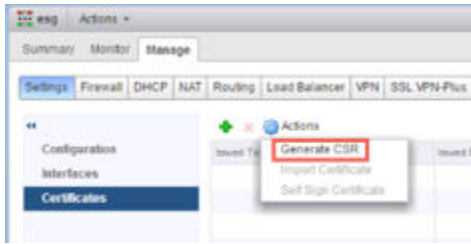
- 1 在安装了 OpenSSL 的 Linux 或 Mac 计算机上，打开以下文件：`/opt/local/etc/openssl/openssl.cnf` 或 `/System/Library/OpenSSL/openssl.cnf`。
- 2 确保 `dir = ..`。
- 3 运行以下命令：

```
mkdir newcerts
mkdir certs
mkdir req
mkdir private
echo "01" > serial
touch index.txt
```

- 4 运行以下命令生成 CA 签名证书：

```
openssl req -new -x509 -newkey rsa:2048 -keyout private/cakey.pem -out cacert.pem -days 3650
```

- 5 在 NSX Edge1 上，生成 CSR，复制隐私增强邮件 (PEM) 文件内容，然后将其保存到 req/edge1.req 目录下的文件中。



请参见配置 [CA 签名证书](#)。

- 6 运行以下命令对 CSR 进行签名：

```
sudo openssl ca -policy policy_anything -out certs/edge1.pem -in req/edge1.req
```

- 7 在 NSX Edge2 上，生成 CSR，复制 PEM 文件内容，然后将其保存到 req/edge2.req 目录下的文件中。

- 8 运行以下命令对 CSR 进行签名：

```
sudo openssl ca -policy policy_anything -out certs/edge2.pem -in req/edge2.req
```

- 9 将 certs/edge1.pem 文件结尾处的 PEM 证书上载到 Edge1。
- 10 将 certs/edge2.pem 文件结尾处的 PEM 证书上载到 Edge2。
- 11 将 cacert.pem 文件中的 CA 证书作为 CA 签名证书上载到 Edge1 和 Edge2。
- 12 在 Edge1 和 Edge2 的 IPsec 全局配置中，选择已上载的 PEM 证书和 CA 证书并保存配置。
- 13 在证书 (Certificate) 选项卡上，单击已上载的证书并记录 DN 字符串。
- 14 将 DN 字符串反转为 C=IN,ST=ka,L=b1r,O=bmware,OU=vmware,CN=edge2.eng.vmware.com 格式，并为 Edge1 和 Edge2 保存该字符串。
- 15 在 Edge1 和 Edge2 上创建 IPsec VPN 站点，并使用指定格式的本地 ID 和对等 ID 作为标识名 (DN) 字符串。

通过单击显示 IPsec 统计信息 (Show IPsec Statistics) 检查状态。单击通道可查看隧道状态。通道和隧道的状态都应为绿色。

## 指定全局 IPsec VPN 配置

该操作将在 NSX Edge 实例上启用 IPsec VPN。

### 前提条件

要启用证书身份验证，您必须导入服务器证书和相应的 CA 签名证书。或者，您也可以使用诸如 OpenSSL 等开源命令行工具生成 CA 签名证书。

自签名证书不能用于 IPsec VPN，只能用于负载均衡和 SSL VPN。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击 **VPN** 选项卡。
- 5 单击 **IPSec VPN**。
- 6 单击“全局配置状态”旁边的**更改 (Change)**。
- 7 为对等端点设置为“任意”的站点键入全局预共享密钥，然后选择**显示共享密钥 (Display shared key)**以显示该密钥。
- 8 选择“启用证书身份验证”，然后选择相应的证书。
- 9 单击**确定 (OK)**。

## 为 IPSec VPN 启用日志记录

可以对所有 IPSec VPN 流量启用日志记录。

默认情况下，将启用日志记录并设置为警告级别。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理**选项卡，然后单击 **VPN** 选项卡。
- 5 单击 **IPSec VPN**。
- 6 单击**日志记录策略**旁边的 ，然后单击**启用日志记录**以记录在本地子网和对等子网之间流动的流量，再选择日志记录级别。
- 7 选择日志级别，然后单击**发布更改**。

## 配置 IPSec VPN 参数

必须在 NSX Edge 上至少配置一个外部 IP 地址才能提供 IPSec VPN 服务。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**监控 (Monitor)**选项卡，然后单击 **VPN** 选项卡。
- 5 单击 **IPSec VPN**。

- 6 单击**添加 (Add)** () 图标。
- 7 键入 IPSec VPN 的名称。
- 8 在**本地 ID (Local Id)** 中键入 NSX Edge 实例的 IP 地址。此 ID 将成为远程站点上的对等 ID。
- 9 键入本地端点的 IP 地址。  
如果您使用预共享密钥将一个 IP 添加到 IP 隧道，则本地 ID 和本地端点 IP 可能相同。
- 10 采用 CIDR 格式键入要在站点之间共享的子网。使用逗号分隔符键入多个子网。
- 11 键入“对等 ID”以唯一标识对等站点。对于使用证书身份验证的对等站点，此 ID 必须是对等站点证书中的公用名称。对于 PSK 对等站点，此 ID 可以是任何字符串。VMware 建议将 VPN 的公共 IP 地址或 VPN 服务的 FQDN 用作对等 ID。
- 12 在“对等端点”中键入对等站点的 IP 地址。如果将其留空，则 NSX Edge 会等待对等设备请求连接。
- 13 采用 CIDR 格式键入对等子网的内部 IP 地址。使用逗号分隔符键入多个子网。
- 14 选择“加密算法”。
- 15 在“身份验证方法”中，选择下列选项之一：

选项	描述
PSK (预共享密钥)	表示将使用在 NSX Edge 与对等站点之间共享的密钥进行身份验证。密钥可以是最大长度为 128 字节的字符串。
证书	表示将使用在全局级别定义的证书进行身份验证。

- 16 如果匿名站点将连接至 VPN 服务，则键入共享密钥。
- 17 单击**显示共享密钥 (Display Shared Key)**，以便在对等站点上显示该密钥。
- 18 在 Diffie-Hellman (DH) Group 中，选择将允许对等站点和 NSX Edge 通过非安全通信通道建立共享密钥的加密方案。
- 19 在 Extension 中，键入以下内容之一：
  - `securelocaltrafficbyip=IPAddress` 通过 IPSec VPN 隧道重定向 Edge 的本地流量。这是默认值。
  - `passthroughSubnets=PeerSubnetIPAddress` 支持重叠子网。
- 20 单击**确定 (OK)**。  
NSX Edge 创建从本地子网到对等子网的隧道。

#### 后续步骤

启用 IPSec VPN 服务。

## 编辑 IPSec VPN 服务

可以编辑 IPSec VPN 服务。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**监控**选项卡，然后单击 **VPN** 选项卡。
- 5 单击 **IPSec VPN**。
- 6 选择要编辑的 IPSec 服务。
- 7 单击**编辑** (✎) 图标。
- 8 进行适当编辑。
- 9 单击**确定**。

## 禁用 IPSec 服务

可以禁用 IPSec 服务。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**监控**选项卡，然后单击 **VPN** 选项卡。
- 5 单击 **IPSec VPN**。
- 6 选择要禁用的 IPSec 服务。
- 7 单击**禁用** (🚫) 图标。

## 删除 IPSec 服务

可以删除 IPSec 服务。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**监控**选项卡，然后单击 **VPN** 选项卡。
- 5 单击 **IPSec VPN**。
- 6 选择您要删除的 IPSec 服务。

- 7 单击删除 (✖) 图标。

## L2 VPN 概述

L2 VPN 允许您配置两个站点之间的隧道。虚拟机仍保留在同一子网中，但可以在这些站点之间移动，这样您就可以扩展数据中心。一个站点上的 NSX Edge 可以向另一站点上的虚拟机提供所有服务。

要创建 L2 VPN 隧道，需要配置 L2 VPN 服务器和 L2 VPN 客户端。

## 配置 L2 VPN

要使用 L2 VPN 延伸网络，可以配置 L2 VPN 服务器（目标 Edge）和 L2 VPN 客户端（源 Edge）。然后必须在服务器和客户端上均启用 L2 VPN 服务。

### 前提条件

在 NSX Edge 的中继接口上必须已添加子接口。请参见[添加子接口](#)。

### 步骤

#### 1 L2 VPN 最佳做法

根据最佳做法配置 L2 VPN 可以避免发生问题，例如循环和重复的 ping 操作和响应。

#### 2 配置 L2 VPN 服务器

L2 VPN 服务器是客户端将连接到的目标 NSX Edge。

#### 3 添加对等站点

可以将多个站点连接到 L2 VPN 服务器。

#### 4 在服务器上启用 L2 VPN 服务

必须在 L2 VPN 服务器（目标 NSX Edge）上启用 L2 VPN 服务。如果在此 Edge 设备上已配置 HA，请确保 Edge 在其上已配置多个内部接口。如果只存在一个接口，并且该接口已由 HA 使用，则同一内部接口上的 L2 VPN 配置将失败。

#### 5 配置 L2 VPN 客户端

L2 VPN 客户端是源 NSX Edge，可发起与目标 Edge（L2 VPN 服务器）之间的通信。

#### 6 在客户端上启用 L2 VPN 服务

必须在 L2 VPN 客户端（源 NSX Edge）上启用 L2 VPN 服务。

## L2 VPN 最佳做法

根据最佳做法配置 L2 VPN 可以避免发生问题，例如循环和重复的 ping 操作和响应。



## 用于缓解循环的 L2VPN 选项

以下两个选项可用于缓解循环。NSX Edge 和虚拟机可以位于不同的 ESXi 主机上，也可以位于同一 ESXi 主机上。

- 选项 1: 将 L2VPN Edge 和虚拟机的各自 ESXi 主机分开
  - a 将 Edge 和虚拟机部署在单独的 ESXi 主机上。
  - b 为与 Edge 的中继虚拟网卡关联的分布式端口组配置成组策略和故障切换策略，如下所示：
    - 1 以“基于源虚拟端口的路由”方式开展负载平衡。
    - 2 仅将一个上行链路配置为“活动”，而将另一个上行链路配置为“备用”。
  - c 为与虚拟机关联的分布式端口组配置成组策略和故障切换策略，如下所示：
    - 1 任何成组策略均可。
    - 2 可以配置多个活动上行链路。
  - d 将 Edge 配置为使用池端口模式，并在中继虚拟网卡上禁用混杂模式。
- 选项 2: Edge 和虚拟机位于同一 ESXi 主机上
  - a 为与 Edge 的中继虚拟网卡关联的分布式端口组配置成组策略和故障切换策略，如下所示：
    - 1 以“基于源虚拟端口的路由”方式开展负载平衡。
    - 2 将一个上行链路配置为“活动”，而将另一个上行链路配置为“备用”。
  - b 为与虚拟机关联的分布式端口组配置成组策略和故障切换策略，如下所示：
    - 1 任何成组策略均可。
    - 2 只能有一个上行链路处于活动状态。
    - 3 虚拟机分布式端口组和 Edge 中继虚拟网卡分布式端口组的活动/备用上行链路的顺序必须相同。
  - c 将客户端侧的独立 Edge 配置为使用池端口模式，并在中继虚拟网卡上禁用混杂模式。

## 配置池端口

如果将 NSX 管理的 NSX Edge 设置为 L2 VPN 客户端，NSX 会自动完成一些配置。如果将独立的 NSX Edge 设置为 L2 VPN 客户端时，这些配置步骤必须手动完成。

如果某个 VPN 站点没有部署 NSX，您可以在该站点中部署单独的 NSX Edge 以配置 L2 VPN。单独的 Edge 是使用 OVF 文件部署的，它表示 Edge 网关以作为在 NSX 未管理的主机上部署的 L2 VPN 客户端。

如果单独的 Edge 中继虚拟网卡连接到 vSphere Distributed Switch，那么需要混杂模式或池端口才能使用 L2 VPN 功能。使用混杂模式会导致出现重复的 Ping 操作和响应。因此，建议在 L2 VPN 独立 NSX Edge 配置中使用池端口模式。

## 前提条件

您需要单独的 Edge 的中继虚拟网卡的端口号。

## 步骤

### 1 检索 dvsUuid 值:

- a 转到 vCenter MOB UI: <https://<vc-ip>/mob?vmodl=1>。
- b 单击 **内容 (content)**。
- c 单击与 **rootFolder** 关联的链接 (例如 group-d1 (Datacenters))。
- d 单击与 **childEntity** 关联的链接 (例如 datacenter-1)。
- e 单击与 **networkFolder** 关联的链接 (例如 group-n6)。
- f 单击与 NSX Edge 关联的 vSphere Distributed Switch 的 DVS 名称链接 (例如 dvs-1 (Mgmt\_VDS))。
- g 复制 uuid 字符串的值。

### 2 在 vCenter Managed Object Browser (MOB) 中修改 selectionSet。

- a 登录到 vCenter MOB UI: <https://<vc-ip>/mob?vmodl=1>。
- b 单击 **内容 (content)**。
- c 单击 **DVSManager**。
- d 单击 **updateOpaqueDataEx**。
- e 在 **selectionSet** 值框中, 粘贴以下 XML 块:

```
<selectionSet xsi:type="DVPortSelection">
 <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!--example only-->
 <portKey>393</portKey> <!--port number of the DVPG where SINK to be set-->
</selectionSet>
```

使用从 vCenter MOB 检索到的 dvsUuid 值。

- f 在“opaqueDataSpec”值框中，粘贴以下 XML 块之一：

要启用池端口，请执行以下操作：

```
<opaqueDataSpec>
 <operation>edit</operation>
 <opaqueData>
 <key>com.vmware.etherswitch.port.extraEthFRP</key>
 <opaqueData
 xsi:type="vmodl.Binary">AAABAA
AA
AA
AAAAAA=</opaqueData>
 </opaqueData>
 </opaqueDataSpec>
```

要禁用池端口，请执行以下操作：

```
<opaqueDataSpec>
 <operation>edit</operation>
 <opaqueData>
 <key>com.vmware.etherswitch.port.extraEthFRP</key>
 <opaqueData
 xsi:type="vmodl.Binary">AA
AA
AA
AAAAAA=</opaqueData>
 </opaqueData>
 </opaqueDataSpec>
```

- g 将 isRuntime 布尔值设置为 **false**。
- h 单击调用方法 (Invoke Method)。

## 配置 L2 VPN 服务器

L2 VPN 服务器是客户端将连接到的目标 NSX Edge。

### 步骤

- 1 在 **L2 VPN** 选项卡中，选择**服务器 (Server)**，然后单击**更改 (Change)**。
- 2 在**侦听器 IP (Listener IP)** 中，键入 NSX Edge 外部接口的主 IP 地址或辅助 IP 地址。
- 3 L2 VPN 服务的默认端口是 **443**。根据需要编辑此端口。
- 4 为服务器与客户端之间的通信选择加密算法。
- 5 选择要绑定到 SSL VPN 服务器的证书。
- 6 单击**确定 (OK)**。

## 添加对等站点

可以将多个站点连接到 L2 VPN 服务器。

---

**注** 更改站点配置设置将导致 NSX Edge 断开并重新连接所有现有的连接。

---

### 步骤

- 1 在“L2 VPN”选项卡中，确保 **L2 VPN 模式 (L2 VPN Mode)** 为 **服务器 (Server)**。
- 2 在 **站点配置详细信息 (Site Configuration Details)** 中，单击 **添加 (Add)** 图标。
- 3 为对等站点键入唯一名称。
- 4 键入对等站点进行身份验证所需使用的用户名和密码。对等站点上的用户凭据应与客户端上的用户凭据相同。
- 5 在 **延伸的接口 (Stretched Interfaces)** 中，单击 **选择子接口 (Select Sub Interfaces)** 以选择要使用客户端延伸的子接口。
  - a 在“选择对象”中，选择 Edge 的中继接口。  
此时将显示中继虚拟网卡上配置的子接口。
  - b 双击要延伸的子接口。
  - c 单击 **确定 (OK)**。
- 6 如果两个站点上虚拟机的默认网关相同，请在 **输出优化网关地址 (Egress Optimization Gateway Address)** 中键入应在本地路由其流量或要通过隧道阻止其流量的网关 IP 地址。
- 7 单击 **确定 (OK)**，然后单击 **发布更改 (Publish Changes)**。

## 在服务器上启用 L2 VPN 服务

必须在 L2 VPN 服务器（目标 NSX Edge）上启用 L2 VPN 服务。如果在此 Edge 设备上已配置 HA，请确保 Edge 在其上已配置多个内部接口。如果只存在一个接口，并且该接口已由 HA 使用，则同一内部接口上的 L2 VPN 配置将失败。

### 步骤

- 1 对于目标 NSX Edge，导航到 **管理 (Manage) > VPN > L2 VPN**。
- 2 在 **L2VPN 服务配置 (L2VPN Service Configuration)** 中，单击 **启用 (Enable)**。

### 后续步骤

在面向 Internet 的防火墙端创建 NAT 或防火墙规则，以使客户端与服务器相互连接。

## 配置 L2 VPN 客户端

L2 VPN 客户端是源 NSX Edge，可发起与目标 Edge（L2 VPN 服务器）之间的通信。

也可以将独立的 Edge 配置为 L2 VPN 客户端。请参见 [将独立 Edge 配置为 L2 VPN 客户端](#)。

**步骤**

- 1 在“L2 VPN”选项卡中，将 **L2 VPN 模式 (L2 VPN Mode)** 设置为 **客户端 (Client)**，然后单击 **更改 (Change)**。
- 2 键入此客户端所要连接的 L2 VPN 服务器的地址。地址可以是主机名或 IP 地址。
- 3 根据需要编辑 L2 VPN 客户端应连接的默认端口。
- 4 选择与服务器通信所用的加密算法。
- 5 在 **延伸的接口 (Stretched Interfaces)** 中，单击 **选择子接口 (Select Sub Interfaces)** 以选择要延伸到服务器的子接口。
  - a 在 **选择对象 (Select Object)** 中，选择 Edge 的中继接口。  
此时将显示中继虚拟网卡上配置的子接口。
  - b 双击要延伸的子接口。
  - c 单击 **确定 (OK)**。
- 6 键入描述。
- 7 在 **输出优化网关地址 (Egress Optimization Gateway Address)** 中，键入子接口的网关 IP 地址或者流量不应通过隧道所流向的 IP 地址。
- 8 在 **用户详细信息 (User Details)** 中，键入在服务器进行身份验证的用户凭据。
- 9 单击 **高级 (Advanced)** 选项卡。  
如果客户端 NSX Edge 不能直接访问 Internet，并需要通过代理服务器访问源（服务器）NSX Edge，请指定 **代理设置 (Proxy Settings)**。
- 10 要启用仅允许安全代理连接，请选择 **启用安全代理 (Enable Secure Proxy)**。
- 11 键入代理服务器地址、端口、用户名和密码。
- 12 要启用服务器证书验证，请选择 **验证服务器证书 (Validate Server Certificate)**，然后选择相应的 CA 证书。
- 13 单击 **确定 (OK)**，然后单击 **发布更改 (Publish Changes)**。

**后续步骤**

确保面向防火墙的 Internet 允许流量从 L2 VPN Edge 流向 Internet。目标端口为 443。

**在客户端上启用 L2 VPN 服务**

必须在 L2 VPN 客户端（源 NSX Edge）上启用 L2 VPN 服务。

**步骤**

- 1 对于源 NSX Edge，导航到 **管理 (Manage) > VPN > L2 VPN**。
- 2 在 **L2VPN 服务配置 (L2VPN Service Configuration)** 中，单击 **启用 (Enable)**。

## 后续步骤

- 在面向 Internet 的防火墙端创建 NAT 或防火墙规则，以使客户端与服务器相互连接。
- 如果正在延伸标准端口组所支持的中继虚拟网卡，请通过以下步骤手动启用 L2 VPN 流量：
  - a 将**混杂模式 (Promiscuous mode)**设置为**接受 (Accept)**。
  - b 将**伪传输 (Forged Transmits)**设置为**接受 (Accept)**。

有关详细信息，请参见《ESXi 和 vCenter Server 5.5 文档》。

## 将独立 Edge 配置为 L2 VPN 客户端

如果您要延伸的某个站点不受 NSX 支持，则可以在该站点上部署一个独立 Edge 作为 L2 VPN 客户端。

### 前提条件

您已为要连接的独立 Edge 的中继接口创建了一个中继端口组。该端口组需要一些手动配置：

- 如果中继端口组在 vSphere 标准交换机上，您必须执行以下操作：
  - 启用伪传输
  - 启用混杂模式
 请参见《vSphere 网络连接指南》。
- 如果中继端口组在 vSphere Distributed Switch 上，您必须执行以下操作：
  - 启用伪传输。请参见《vSphere 网络连接指南》。
  - 为中继虚拟网卡启用池端口，或启用混杂模式。启用池端口是推荐的最佳做法。

池端口配置必须在部署独立 Edge 后才能完成，因为您需要更改连接到 Edge 中继虚拟网卡的端口的配置。

### 步骤

- 1 使用 vSphere Web Client 登录到管理非 NSX 环境的 vCenter Server。
- 2 选择**主机和群集**，并展开群集以显示可用主机。
- 3 右键单击要安装独立 Edge 的主机，然后选择**部署 OVF 模板**。
- 4 输入 URL 以从 Internet 下载并安装 OVF 文件，或单击**浏览**找到计算机中独立 Edge OVF 文件所在的文件夹，然后单击**下一步**。
- 5 在“OVF 模板详细信息”页面上，验证模板详细信息并单击**下一步**。
- 6 在“选择名称和文件夹”页面上，键入独立 Edge 的名称，并选择要在其中执行部署操作的文件夹或数据中心。然后，单击**下一步**。
- 7 在“选择存储器”页面上，选择要存储已部署模板文件的位置。
- 8 在“选择网络”页面上，配置已部署模板应使用的网络。单击**下一步**。
  - 公共接口为上行链路接口。
  - 中继接口用于为将要延伸的网络创建子接口。将此接口连接到您所创建的中继端口组。

9 在“自定义模板”页面上，指定以下值。

- a 键入并再次键入 CLI 管理员密码。
- b 键入并再次键入 CLI 启用密码。
- c 键入并再次键入 CLI 根密码。
- d 键入上行链路 IP 地址和前缀长度，默认网关和 DNS IP 地址为可选项。
- e 选择要在身份验证中使用的密码。这应与 L2VPN 服务器上使用的密码相一致。
- f 要启用“输出优化”，键入应本地路由流量的网关 IP 地址或要通过隧道阻止流量的网关 IP 地址。
- g 键入 L2 VPN 服务器的地址和端口。
- h 输入对等站点完成身份验证操作所需的用户名和密码。
- i 在子接口 VLAN（隧道 ID）中，键入要延伸的网络的 VLAN ID。可以采用逗号分隔列表或者范围的形式列出 VLAN ID。例如，2,3,10-20。  
  
如果要在将网络延伸到独立 Edge 站点之前更改网络的 VLAN ID，可以键入网络的 VLAN ID，然后在括号中键入隧道 ID。例如，2(100),3(200)。隧道 ID 用于映射要延伸的网络。但您无法用范围的方式指定隧道 ID。因此不允许采用：10(100)-14(104)。需将其改写为 10(100),11(101),12(102),13(103),14(104)。
- j 如果独立 NSX Edge 无法直接访问 Internet 并需要通过代理服务器访问源（服务器）NSX Edge，则键入代理地址、端口、用户名和密码。
- k 如果根 CA 可用，您可以将它粘贴到“证书”部分。
- l 单击下一步。

10 在“即将完成”页面上，检查独立 Edge 设置，然后单击完成。

#### 后续步骤

打开独立 Edge 虚拟机的电源。

记下中继虚拟网卡的端口号，并配置池端口。请参见[配置池端口](#)。

使用独立 Edge 命令行界面对配置进行进一步的更改。请参见 NSX 命令行界面参考。

## 查看 L2 VPN 统计信息

您可以查看源和目标 NSX Edge 的 L2 VPN 统计信息，例如通道状态、发送和接收的字节数等。

#### 步骤

- 1 在“L2 VPN”选项卡中，确保 **L2 VPN 模式 (L2 VPN Mode)** 为客户端 (Client)。
- 2 单击 **获取状态 (Fetch Status)**，然后展开 **隧道状态 (Tunnel Status)**。

如果 L2 VPN 服务器具有多个对等站点，则将显示所有对等站点的统计信息。

## 后续步骤

要查看在中继接口上配置的网络，请导航到 Edge 的 **管理 (Manage) > 设置 (Settings) > 接口 (Interfaces)**，然后单击“类型”列中的 **中继 (Trunk)**。



## 逻辑负载均衡器

NSX Edge 负载均衡器启用高可用性服务，并在多个服务器之间分配网络流量负载。它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。这样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。NSX Edge 最多可对第 7 层提供负载均衡。

将外部或公共 IP 地址映射到一组内部服务器以进行负载均衡。负载均衡器可接受外部 IP 地址上的 TCP、UDP、HTTP 或 HTTPS 请求，并确定要使用的内部服务器。端口 80 是 HTTP 的默认端口，端口 443 是 HTTPS 的默认端口。

必须具有工作 NSX Edge 实例才可以执行负载均衡。有关设置 NSX Edge 的信息，请参见 [NSX Edge 配置](#)。

有关配置 NSX Edge 证书的信息，请参见[使用证书](#)。

本章讨论了以下主题：

- [设置负载均衡](#)
- [管理应用程序配置文件](#)
- [管理服务监控器](#)
- [管理服务器池](#)
- [管理虚拟服务器](#)
- [管理应用程序规则](#)
- [对使用 NTLM 身份验证的 Web 服务器进行负载均衡](#)
- [NSX 负载均衡器配置场景](#)

### 设置负载均衡

NSX Edge 负载均衡器在多个服务器之间分配网络流量，以实现最佳资源使用率。

NSX 负载均衡器支持第 4 层和第 7 层负载均衡引擎。第 4 层负载均衡器基于数据包，第 7 层负载均衡器基于套接字。

基于数据包的负载均衡是在 TCP 和 UDP 层上实现的。基于数据包的负载均衡不会停止连接或缓冲整个请求，而是在处理数据包后将数据包直接发送到选定的服务器。将在负载均衡器中保持 TCP 和 UDP 会话，以便将单个会话的数据包定向到相同的服务器。您可以在全局配置和相关的虚拟服务器配置中选择“启用加速”以启用基于数据包的负载均衡。

基于套接字的负载平衡是在套接字接口上面实现的。将为单个请求建立两个连接：面向客户端的连接和面向服务器的连接。在选择服务器后，将建立面向服务器的连接。对于基于 HTTP 套接字的实现，将在发送到具有可选 L7 处理的选定服务器之前接收整个请求。对于基于 HTTPS 套接字的实现，将在面向客户端的连接或面向服务器的连接上交换身份验证信息。基于套接字的负载平衡是 TCP、HTTP 和 HTTPS 虚拟服务器的默认模式。

NSX 负载平衡器的重要概念包括虚拟服务器、服务器池、服务器池成员和服务监控器。

<b>虚拟服务器</b>	应用程序服务的抽象形式，它是由 IP、端口和协议（如 TCP 或 UDP）的唯一组合表示的。
<b>服务器池</b>	后端服务器组。
<b>服务器池成员</b>	将后端服务器表示为池中的成员。
<b>服务监控器</b>	定义如何探查后端服务器的运行状态。

首先，请设置负载平衡器的全局选项。现在，请创建由后端服务器成员组成的服务器池，并将服务监控器与该池关联，以便有效地管理和共享后端服务器。

然后，创建一个应用程序配置文件以定义负载平衡器中的常见应用程序行为，如客户端 SSL、服务器 SSL、x-forwarded-for 或持久性。持久性发送具有类似特性的后续请求（例如，需要将源 IP 或 cookie 发送到相同的池成员），而无需运行负载平衡算法。可以在虚拟服务器中重复使用应用程序配置文件。

然后，创建一个可选的应用程序规则，以便为流量处理（如匹配某个 URL 或主机名）配置应用程序特定的设置，以便由不同的池处理不同的请求。接下来，请创建服务监控器以定义负载平衡器的运行状况检查参数。

在虚拟服务器收到请求时，负载平衡算法将考虑池成员配置和运行时状态。然后，该算法计算相应的池以分配包含一个或多个成员的流量。池成员配置包括一些设置，例如，权重、最大连接数和条件状态。运行时状态包括当前连接、响应时间以及运行状况检查状态信息。计算方法可能是循环、加权循环、最少连接或源 IP 哈希。

每个池都由相关联的服务监控器监控。当负载平衡器检测到池成员出现问题时，会将其标记为关闭。从服务器池中选择池成员时，仅会选择已启动的服务器。如果服务器池未配置服务监控器，则将所有池成员视为已启动。

#### ■ 配置负载平衡器服务

可以指定全局负载平衡器配置参数。

#### ■ 创建服务监控器

可创建服务监控器以便为特定类型的网络流量定义运行状况检查参数。将服务监控器与池关联后，将根据服务监控器参数对池成员进行监控

#### ■ 添加服务器池

可以添加服务器池，以灵活高效地管理和共享后端服务器。池可管理负载平衡器分配方法，并且具有一个附加的服务监控器，可提供运行状况检查参数。

#### ■ 创建应用程序配置文件

通过创建应用程序配置文件可以定义特定类型的网络流量的行为。设置配置文件后，可以将此配置文件与虚拟服务器关联。然后，该虚拟服务器会根据配置文件中指定的值处理流量。使用配置文件可以加强对网络流量管理的控制，使流量管理任务更简单高效。

## ■ 添加应用程序规则

您可以编写一个应用程序规则，以便直接处理和管理应用程序流量。

## ■ 添加虚拟服务器

将 NSX Edge 内部或上行链路接口作为虚拟服务器进行添加。

## 配置负载均衡器服务

可以指定全局负载均衡器配置参数。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**，然后单击**负载均衡器 (Load Balancer)**选项卡。
- 5 单击**编辑 (Edit)**。
- 6 选中要启用的选项旁边的复选框。

选项	描述
启用负载均衡器	允许 NSX Edge 负载均衡器将流量分布到内部服务器以实现负载均衡。
启用加速	<p>在全局启用后，每个虚拟 IP 使用更快的 L4 LB 引擎，而不是 L7 LB 引擎。</p> <p>L4 TCP VIP 在 Edge 防火墙之前处理，因此不需要“允许”防火墙规则。L7 HTTP/HTTPS VIP 在 Edge 防火墙之后处理。</p> <p>如果选择了“启用加速”，Edge 防火墙规则必须允许访问 L7 HTTP/HTTPS VIP。</p> <p>如果为 L4 TCP VIP 选择了“启用加速”标记，并且服务器池处于非透明模式，则会添加一个 SNAT 规则。因此，请确保在 NSX Edge 上启用防火墙。</p> <p>如果为 L4 TCP VIP 取消选择“启用加速”标记并且启用了防火墙，Edge 防火墙规则必须允许访问 L7 HTTP/HTTPS VIP。</p>
日志记录	<p>NSX Edge 负载均衡器收集流量日志。</p> <p>您可以从下拉菜单中选择日志级别。这些日志将导出到配置的 syslog 服务器。您还可以使用 <code>show log follow</code> 命令列出负载均衡日志。</p> <p>“调试”和“信息”选项记录最终用户请求。“警告”、“错误”和“严重”选项不记录最终用户请求。</p>
启用 Service Insertion	<p>允许负载均衡器使用第三方供应商服务。</p> <p>如果在环境中部署了第三方供应商负载均衡器服务，请参见<a href="#">使用合作伙伴负载均衡器</a>。</p>

- 7 单击**确定 (OK)**。

## 创建服务监控器

可创建服务监控器以便为特定类型的网络流量定义运行状况检查参数。将服务监控器与池关联后，将根据服务监控器参数对池成员进行监控

## 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**，然后单击**负载均衡器 (Load Balancer)**选项卡。
- 5 在左侧导航面板中，单击**服务监控 (Service Monitoring)**。
- 6 单击**添加 (Add)** () 图标。
- 7 输入服务监控器的名称。
- 8 输入对服务器执行 ping 命令的时间间隔（秒）。
- 9 输入在声明服务器出现故障之前必须对服务器执行 ping 命令的次数。
- 10 输入最长的时间（秒），在该时间内必须从服务器接收到响应。
- 11 从下拉菜单中选择将运行状况检查请求发送到服务器的方式。
- 12 对于 HTTP 和 HTTPS 流量，请执行以下步骤。
  - a 在“预期”部分中输入监控器要求与 HTTP 响应状态行匹配的字符串。  
例如，200,301,302,401。
  - b 从下拉菜单中选择检测服务器状态的方法。
  - c 输入要在请求示例中使用的 URL。
  - d 如果选择 POST 方法，请输入要发送的数据。
- 13 在“接收”部分中输入与响应内容匹配的字符串。  
如果“预期”部分中的字符串不匹配，则监控器不会尝试与“接收”内容匹配。
- 14 在“扩展”部分中，以“键=值”对形式输入高级监控器参数。  
示例扩展 **warning=10** 表示，如果服务器未在 10 秒内响应，则将状态设置为警告。  
所有扩展项都应使用回车符分隔。

```
<extension>eregi="(OK1|OK2)"</extension>
```

请参阅支持的协议扩展表。

**表 15-1. TCP 协议的扩展**

监控扩展	描述
escape	可以在发送或退出字符串中使用 \n、\r、\t 或 \。必须在发送或退出选项之前使用。默认：发送选项中不添加任何内容，\r\n 添加到退出末尾。
all	所有预期字符串都需要在服务器响应中出现。默认为 any。
quit=STRING	发送到服务器的字符串，启动完全关闭连接。

表 15-1. TCP 协议的扩展（续）

监控扩展	描述
refuse=ok warn crit	接受状态为 <b>ok</b> 、 <b>warn</b> 或 <b>crit</b> 的 TCP 拒绝，默认为 <b>crit</b> 。
mismatch=ok warn crit	接受预期字符串与状态 <b>ok</b> 、 <b>warn</b> 或 <b>crit</b> 不匹配。默认为 <b>warn</b> 。
jail	从 TCP 套接字隐藏输出。
maxbytes= <i>INTEGER</i>	接收的字节数比指定的字节数多时关闭连接。
delay= <i>INTEGER</i>	发送字符串与轮询响应之间所等待的秒数。
certificate= <i>INTEGER</i> [, <i>INTEGER</i> ]	证书必须有效的最短天数。第一个值是警告天数，第二个值用于严重级别（如果未指定，则为 0）。
ssl-version=3	使用 <b>sslv3</b> 强制实施 SSL 握手。 默认情况下，将在运行状况检查选项中禁用 <b>sslv3</b> 和 <b>tlsv1</b> 。
ssl-version=10	使用 <b>tls 1.0</b> 强制实施 SSL 握手。
ssl-version=11	使用 <b>tls 1.1</b> 强制实施 SSL 握手。
ssl-version=12	使用 <b>tls 1.2</b> 强制实施 SSL 握手。
ciphers='ECDHE-RSA-AES256-GCM-SHA384'	显示在 HTTPS 运行状况检查中使用的密码。
warning=DOUBLE	响应时间（秒）：在此范围内不反应则发出警告。
critical=DOUBLE	响应时间（秒）：在此范围内不反应则变成严重状态。

表 15-2. HTTP/HTTPS 协议的扩展

监控扩展	描述
no-body	不等待文档正文：停止读取标头后的内容。注意，这仍然是 HTTP GET 或 POST，而不是 HEAD。
max-age= <i>SECONDS</i>	如果文档存在时间超过 <b>SECONDS</b> ，则发出警告。该数字还可以采用 <b>10m</b> （表示分钟）、 <b>10h</b> （表示小时）或 <b>10d</b> （表示天数）的形式。
content-type= <i>STRING</i>	指定 POST 调用中的 <b>Content-Type</b> 标头介质类型。
linespan	允许正则表达式跨新行（前面必须加上 <b>-r</b> 或 <b>-R</b> ）。
regex= <i>STRING</i> 或 <i>ereg=STRING</i>	在页面中搜索正则表达式 <b>STRING</b> 。
eregi= <i>STRING</i>	在页面中搜索不区分大小写的正则表达式 <b>STRING</b> 。
invert-regex	找到则返回 <b>CRITICAL</b> ，否则返回 <b>OK</b> 。
proxy-authorization= <i>AUTH_PAIR</i>	代理服务器上完成基本身份验证所需的用户名和密码。
useragent= <i>STRING</i>	要在 HTTP 标头中作为 <b>User Agent</b> 发送的字符串。
header= <i>STRING</i>	要在 HTTP 标头中发送的任何其他标记。对其他标头使用多次。
onredirect=ok warning critical follow sticky stickyport	如何处理重定向后的页面。 <b>sticky</b> 类似于 <b>follow</b> 但遵循指定的 IP 地址。 <b>stickyport</b> 还确保端口保持不变。
pagesize= <i>INTEGER</i> : <i>INTEGER</i>	所需页面大小最小值（字节）：所需页面大小最大值（字节）。
warning=DOUBLE	响应时间（秒）：在此范围内不反应则发出警告。
critical=DOUBLE	响应时间（秒）：在此范围内不反应则变成严重状态。

表 15-3. HTTPS 协议的扩展

监控扩展	描述
sni	启用 SSL/TLS 主机名扩展支持 (SNI)。
certificate= <i>INTEGER</i>	证书必须有效的最短天数。端口默认为 443。如果使用该选项，则不检查 URL。
authorization=AUTH_PAIR	使用基本身份验证的站点上的用户名和密码。

15 单击**确定 (OK)**。

#### 后续步骤

将服务监控器与池关联。

## 添加服务器池

可以添加服务器池，以灵活高效地管理和共享后端服务器。池可管理负载均衡器分配方法，并且具有一个附加的服务监控器，可提供运行状况检查参数。

#### 步骤


- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**，然后单击**负载均衡器 (Load Balancer)**选项卡。
- 5 在左侧导航面板中，单击**池 (Pools)**。
- 6 单击**添加 (Add) (+)** 图标。
- 7 键入负载均衡器池的名称和描述。
- 8 为每个启用的服务选择算法平衡方法。

选项	描述
<b>IP-HASH</b>	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。 将为该选项禁用算法参数。
<b>LEASTCONN</b>	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。 将为该选项禁用算法参数。
<b>ROUND_ROBIN</b>	根据每个服务器分配到的权重，依次使用各服务器。 当服务器的处理时间保持均匀分布时，这是最顺畅、最公平的算法。 将为该选项禁用算法参数。

选项	描述
URI	<p>对 URI 左侧部分（问号之前）进行哈希并除以运行的服务器的总权重。</p> <p>结果指定接收请求的服务器。这样可以确保只要没有服务器启动或关闭，URI 将始终定向到同一服务器。</p> <p>URI 算法参数具有两个选项：uriLength=&lt;len&gt; 和 uriDepth=&lt;dep&gt;。长度参数范围应该为 1&lt;=len&lt;256。深度参数范围应该为 1&lt;=dep&lt;10。</p> <p>长度和深度参数后跟一个正整数。这些选项可以仅根据 URI 开头平衡服务器。长度参数指示算法只应考虑在 URI 开头定义的字符以计算哈希值。</p> <p>深度参数指示用于计算哈希值的最大目录深度。将为请求中的每个斜杠计入一个级别。如果指定了两个参数，在到达任一参数时，计算将停止。</p>
HTTPHEADER	<p>在每个 HTTP 请求中查找 HTTP 标头名称。</p> <p>圆括号中的标头名称不区分大小写，这类似于 ACL 函数“hdr()”。如果标头不存在或不包含任何值，将应用循环算法。</p> <p>HTTPHEADER 算法参数具有一个选项：headerName=&lt;name&gt;。例如，可以将 host 作为 HTTPHEADER 算法参数。</p>
URL	<p>在每个 HTTP GET 请求的查询字符串中查找参数中指定的 URL 参数。</p> <p>如果参数后跟等号 = 和一个值，则对该值进行哈希并除以运行的服务器的总权重。结果指定接收请求的服务器。该过程用于跟踪请求中的用户标识符，并确保始终将相同的用户 ID 发送到相同的服务器，但前提是没有启动或关闭服务器。</p> <p>如果找不到任何值或参数，则应用循环算法。</p> <p>URL 算法参数具有一个选项：urlParam=&lt;url&gt;。</p>

9 （可选）从**监控器 (Monitors)**下拉菜单中选择一个现有的默认或自定义监控器。

10 向池添加成员。

- a 单击**添加 (Add)** ( ) 图标。
- b 输入服务器成员的名称和 IP 地址，或者单击**选择 (Select)**以分配分组对象。  
分组对象可以是 vCenter 或 NSX。
- c 输入成员在其上接收流量的端口和成员在其上接收运行状况监控 ping 的监控端口。  
如果相关的虚拟服务器配置了端口范围，则端口值应该为 null。
- d 在“权重”部分中输入该成员处理的流量比例。
- e 输入成员可以处理的最大并行连接数。  
如果传入请求数高于最大数，它们将排队等待释放连接。
- f 输入成员必须始终接受的最小并行连接数。
- g 单击**确定 (OK)**。

11 选中**透明 (Transparent)**以使客户端 IP 地址对后端服务器可见。

如果未选中“透明”（默认值），则后端服务器会将流量源 IP 地址看作负载平衡器内部 IP 地址。如果选中了“透明”，则源 IP 地址是真正的客户端 IP 地址，并且必须将 NSX Edge 设置为默认网关以确保返回数据包通过 NSX Edge 设备。

12 单击**确定 (OK)**。



## 创建应用程序配置文件

通过创建应用程序配置文件可以定义特定类型的网络流量的行为。设置配置文件后，可以将此配置文件与虚拟服务器关联。然后，该虚拟服务器会根据配置文件中指定的值处理流量。使用配置文件可以加强对网络流量管理的控制，使流量管理任务更简单高效。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**，然后单击**负载均衡器 (Load Balancer)**选项卡。
- 5 在左侧导航面板中，单击**应用程序配置文件 (Application Profiles)**。
- 6 单击**添加 (Add)** () 图标。
- 7 键入配置文件的名称，然后从下拉菜单中选择要创建配置文件的流量类型。

流量类型	支持的持久性方法
TCP	源 IP、MSRDP
HTTP	cookie、源 IP
HTTPS	cookie、SSL 会话 ID（已启用 SSL 直通）、源 IP
UDP	源 IP

- 8 键入 HTTP 流量要重定向到的 URL。

例如，可以将流量从 `http://myweb.com` 定向到 `https://myweb.com`。

- 9 从下拉菜单中为配置文件指定持久性类型。

持久性配置文件可跟踪和存储会话数据，例如服务于客户端请求的特定池成员。通过使用持久性，客户端请求在整个会话期间或后续会话期间定向到同一个池成员。

- 选择 **Cookie** 持久性以插入唯一的 **cookie**，以便在客户端首次访问站点时标识会话。

将在后续请求中引用该 **cookie**，以永久保留到相应服务器的连接。

- 选择**源 IP (Source IP)** 持久性以根据源 IP 地址跟踪会话。

客户端请求连接到支持源地址关联性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个池成员。

- 选择 **Microsoft 远程桌面协议 (MSRDP)** 持久性以在运行 **Microsoft 远程桌面协议 (RDP)** 服务的 **Windows** 客户端和服务器之间保持持久性会话。

启用 MSRDP 持久性的推荐方案是创建由运行 **Windows Server 2003** 或 **Windows Server 2008** 的成员所组成的负载均衡池，其中所有成员均属于一个 **Windows** 群集并加入 **Windows** 会话目录。



**10** 键入 cookie 名称并选择插入 cookie 应采用的模式。

选项	描述
插入	NSX Edge 发送一个 cookie。 如果服务器发送一个或多个 cookie，客户端将收到一个额外的 cookie（服务器 cookie + Edge cookie）。如果服务器不发送 cookie，客户端将收到 Edge cookie。
前缀	如果客户端不支持多个 cookie，则选择该选项。  <b>注</b> 所有浏览器均接受多个 cookie。如果具有专用应用程序使用仅支持一个 cookie 的专用客户端，Web 服务器正常发送其 cookie。NSX Edge 在服务器 cookie 值中注入（作为前缀）其 cookie。此添加了 cookie 的信息在 NSX Edge 将其发送到服务器时删除。
App 会话	服务器不发送 cookie，而是将用户会话信息作为 URL 发送。 例如， http://mysite.com/admin/UpdateUserServlet;jsessionid=OI24B9ASD7BSSD，其中 jsessionid 是用户会话信息并用于持久性。无法查看 App 会话持久性表进行故障排除。

**11** 输入持久性到期时间（秒）。

持久性默认值为 5 分钟。

对于 L7 负载平衡 TCP 源 IP 持久性方案，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。

**12** （可选）为 HTTPS 流量创建一个应用程序配置文件。

支持的 HTTPS 流量模式。

- SSL 卸载 -> 客户端 -> HTTPS -> LB (终止 SSL) -> HTTP -> 服务器
  - SSL 代理 -> 客户端 -> HTTPS -> LB (终止 SSL) -> HTTPS -> 服务器
  - SSL 直通 -> 客户端 -> HTTPS -> LB (SSL 直通) -> HTTPS -> 服务器
  - 客户端 -> HTTP -> LB -> HTTP -> 服务器
- a （可选）选中**插入 X-Forwarded-For HTTP 标头 (Insert X-Forwarded-For HTTP header)**，以标识通过负载均衡器连接到 Web 服务器的客户端的源 IP 地址。
- b 选中**配置服务证书 (Configure Service Certificate)**，以便在**虚拟服务器证书 (Virtual Server Certificates)**选项卡中选择适用的服务证书、CA 证书和 CRL 以用于在负载均衡器上终止客户端的 HTTPS 流量。

仅当“客户端 -> LB”连接为 HTTPS 连接时，才需要执行此操作。

- c （可选）选中**启用池端 SSL (Enable Pool Side SSL)** 以在负载均衡器和后端服务器之间启用 HTTPS 通信。

您可以使用池端 SSL 配置端到端 SSL。

- d （可选）选中**配置服务证书 (Configure Service Certificate)**，以便在**池证书 (Pool Certificates)** 选项卡中选择适用的服务证书、CA 证书和 CRL 以用于验证服务器端的负载均衡器。

仅当模式为“客户端 -> HTTPS -> LB -> HTTPS -> 服务器”时，才需要执行此操作。

如果 NSX Edge 负载均衡器已配置 CA 证书和 CRL，并且需要从后端服务器中验证服务证书，您可以配置服务证书。如果后端服务器需要验证负载均衡器端服务证书，也可以使用该选项为后端服务器提供负载均衡器证书。

- 13 输入在 SSL/TLS 握手期间协商的密码算法（或密码套件）。

例如，您可以仅允许使用 3DES 密码套件。

- 14 从下拉菜单中指定是忽略还是要求使用客户端身份验证。

如果选择“要求”，则客户端必须在请求或握手中止后提供证书。

- 15 单击**确定 (OK)**。

## 添加应用程序规则

您可以编写一个应用程序规则，以便直接处理和管理应用程序流量。

有关应用程序规则示例，请参见[应用程序规则示例](#)。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**，然后单击**负载均衡器 (Load Balancer)**选项卡。
- 5 在左侧的导航面板中，单击**应用程序规则 (Application Rules)**。
- 6 单击**添加 (Add)** () 图标。
- 7 键入规则的名称和脚本。  
有关应用程序规则语法的信息，请参见 <http://cbonte.github.io/haproxy-dconv/configuration-1.5.html>。
- 8 单击**确定 (OK)**。

## 应用程序规则示例

## 基于条件的 HTTP/HTTPS 重定向

通过应用程序配置文件可指定 HTTP/HTTPS 重定向，无论请求 URL 是什么，始终可重定向流量。您还可以灵活指定在什么条件下可以重定向 HTTP/HTTPS 流量。

```
move the login URL only to HTTPS.
acl clear dst_port 80
acl secure dst_port 8080
acl login_page url_beg /login
acl logout url_beg /logout
acl uid_given url_reg /login?userid=[^&]+
acl cookie_set hdr_sub(cookie) SEEN=1
redirect prefix https://mysite.com set-cookie SEEN=1 if !cookie_set
redirect prefix https://mysite.com if login_page !secure
redirect prefix http://mysite.com drop-query if login_page !uid_given
redirect location http://mysite.com/ if !login_page secure
redirect location / clear-cookie USERID= if logout
```

## 按域名进行路由

可以创建应用程序规则，以便根据域名将请求定向到特定的负载均衡器池。以下规则将发送到 **foo.com** 的请求定向到 **pool\_1**，将发送到 **bar.com** 的请求定向到 **pool\_2**。

```
acl is_foo hdr_dom(host) -i foo
acl is_bar hdr_dom(host) -i bar
use_backend pool_1 if is_foo
use_backend pool_2 if is_bar
```

## Microsoft RDP 负载均衡和保护

在以下示例方案中，负载均衡器将新用户平衡到负载较少的服务器并恢复中断的会话。此方案的 NSX Edge 内部接口 IP 地址是 10.0.0.18，内部接口 IP 地址是 192.168.1.1，虚拟服务器是 192.168.1.100、192.168.1.101 和 192.168.1.102。

- 1 为 TCP 流量创建包含 MSRDP 持久性的应用程序配置文件。
- 2 创建 TCP 运行状况监控 (tcp\_monitor)。
- 3 创建名为 rdp-pool 的池，其中包含成员 192.168.1.100:3389、192.168.1.101:3389 和 192.168.1.102:3389。
- 4 将 tcp\_monitor 与 dp-pool 相关联。
- 5 创建以下应用程序规则。

```
tcp-request content track-sc1 rdp_cookie(msthash) table rdp-pool
tcp-request content track-sc2 src table ipv4_ip_table

each single IP can have up to 2 connections on the VDI infrastructure
tcp-request content reject if { sc2_conn_cur ge 2 }

each single IP can try up to 5 connections in a single minute
tcp-request content reject if { sc2_conn_rate ge 10 }
```

```
Each user is supposed to get a single active connection at a time, block the second one
tcp-request content reject if { sc1_conn_cur ge 2 }

if a user tried to get connected at least 10 times over the last minute,
it could be a brute force
tcp-request content reject if { sc1_conn_rate ge 10 }
```

6 创建名为 **rdp-vs** 的虚拟服务器。

7 将应用程序配置文件关联到此虚拟服务器，并添加第 4 步中创建的应用程序规则。

在虚拟服务器上新应用的应用程序规则将保护 RDP 服务器。

## 高级日志记录

默认情况下，**NSX** 负载均衡器支持基本日志记录。您可以按如下方式创建应用程序规则，以便查看详细的日志记录消息以进行故障排除。

```
log the name of the virtual server
capture request header Host len 32

log the amount of data uploaded during a POST
capture request header Content-Length len 10
log the beginning of the referrer
capture request header Referer len 20

server name (useful for outgoing proxies only)
capture response header Server len 20

logging the content-length is useful with "option logasap"
capture response header Content-Length len 10

log the expected cache behaviour on the response
capture response header Cache-Control len 8

the Via header will report the next proxy's name
capture response header Via len 20

log the URL location during a redirection
capture response header Location len 20
```

将应用程序规则关联到虚拟服务器后，日志将包含如下所示的详细消息。

```
2013-04-25T09:18:17+00:00 edge-187 loadbalancer[18498]: [org1]: 10.117.7.117 -- [25/Apr/2013:09:18:16
+0000] "GET /favicon.ico HTTP/1.1" 404 1440 "" "" 51656 856 "vip-http-complete"
"pool-http-complete" "m2" 145 0 1 26 172 --NI 1 1 0 0 0 0 "" "" "10.117.35.187" "Mozilla/5.0 (Windows
NT 6.1; WOW64) AppleWebKit/537.31
(KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31" "Apache/2.2.15 (Linux" ""

2013-04-25T09:18:17+00:00 edge-187 loadbalancer[18498]: [org1]: 10.117.7.117 -- [25/Apr/2013:09:18:16
```

```
+0000] "GET /favicon.ico HTTP/1.1" 404 1440 "" "" 51657 856 "vip-http-complete"
"pool-http-complete" "m2" 412 0 0 2 414 --NI 0 0 0 0 0 0 0 "" "" "10.117.35.187" "Mozilla/5.0 (Windows
NT 6.1; WOW64) AppleWebKit/537.31
(KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31" "Apache/2.2.15 (Linux" ""
```

要排除 HTTPS 流量故障，可能需要添加更多的规则。大多数的 Web 应用程序使用带位置标头的 301/302 响应以将客户端重定向到页面（大多数情况下是在登录或 POST 调用后），还需要应用程序 cookie。所以应用程序服务器可能无法获取客户端连接信息，从而无法做出正确的响应，这甚至可能会使应用程序停止工作。

要使 Web 应用程序支持 SSL 卸载，请添加以下规则。

```
See clearly in the log if the application is setting up response for HTTP or HTTPS
capture response header Location len 32
capture response header Set-Cookie len 32

Provide client side connection info to application server over HTTP header
http-request set-header X-Forwarded-Proto https if { ssl_fc }
http-request set-header X-Forwarded-Proto http if !{ ssl_
```

通过 SSL 建立连接后，负载均衡器将插入以下标头。

```
X-Forwarded-Proto: https
```

通过 HTTP 建立连接后，负载均衡器将插入以下标头。

```
X-Forwarded-Proto: http
```

## 阻止特定的 URL

您可以阻止在 URL 中包含特定关键字的请求。以下示例规则检查请求是否以 `/private` 或 `/finance` 开头，并阻止包含这些内容的请求。

```
acl block_url_list path_beg -i /private /finance
block if block_url_list
```

## 没有 cookie 时的身份验证 HTTP 重定向

您可以重定向没有 cookie 的客户端请求以进行身份验证。以下示例规则检查 HTTP 请求是否是真实的并在标头中具有 cookie。如果请求没有 cookie，则规则将请求重定向到 `/authent.php` 以进行身份验证。

```
acl authent_url url /authent.php
acl cookie_present hdr_sub(cookie) cookie1=
redirect prefix /authent.php if !authent_url !cookie_present
```

## 默认页面重定向

您可以将客户端请求 / 重定向到默认页面。以下示例规则检查 HTTP 请求是否为 /，并将请求重定向到默认登录页面。

```
acl default_url url /
redirect prefix /login.php if default_url
```

## 重定向到维护网站

在主池发生故障时，您可以使用维护服务器池并将 URL 重定向到维护网站。

```
redirect location http://maintenance.xyz.com/maintenance.htm
```

## NT LAN 管理器 (NTLM) 身份验证

如果不希望在每个请求后关闭服务器会话，您可以将服务器会话保持活动状态并使用 NTLM 协议保护会话安全。

```
no option http-server-close
```

## 替换服务器标头

您可以删除现有的响应服务器标头，并将其替换为另一个服务器。以下示例规则删除服务器标头，并将其替换为可作为 HTTP、HTTPS、SMTP、POP3 和 IMAP 协议、HTTP 缓存和负载均衡器的反向代理服务器的 NGINX Web 服务器。

```
rspidel Server
rspadd Server:\ nginx
```

## 重写重定向

您可以将位置标头从 HTTP 重写为 HTTPS。以下示例规则指定位置标头并将 HTTP 替换为 HTTPS。

```
rspirep ^Location:\ http://(.*) Location:\ https://\1
```

## 根据主机选择特定的池

您可以将具有特定主机的请求重定向到定义的池。以下示例规则检查特定主机 app1.xyz.com、app2.xyz.com 和 host\_any\_app3 的请求，并将这些请求分别重定向到定义的池 pool\_app1、pool\_app2 和 pool\_app3。所有其他请求将重定向到虚拟服务器中定义的现有池。

```
acl host_app1 hdr(Host) -i app1.xyz.com
acl host_app2 hdr(Host) -i app2.xyz.com
acl host_any_app3 hdr_beg(host) -i app3

use_backend pool_app1 if host_app1
use_backend pool_app2 if host_app2
use_backend pool_app3 if host_any_app3
```

## 根据 URL 选择特定的池

您可以将具有 URL 关键字的请求重定向到特定的池。以下示例规则检查请求是否以 `/private` 或 `/finance` 开头，并将这些请求重定向到定义的池 `pool_private` 或 `pool_finance`。所有其他请求将重定向到虚拟服务器中定义的现有池。

```
acl site_private path_beg -i /private
acl site_finance path_beg -i /finance
use_backend pool_private if site_private
use_backend pool_finance if site_finance
```

## 在主池发生故障时重定向

如果主池中的服务器发生故障，您可以重定向用户以使用辅助池中的服务器。以下示例规则检查 `pool_production` 是否发生故障，并将用户转移到 `pool_sorry_server`。

```
acl pool_production_down nbsrv(pool_production) eq 0
use_backend pool_sorry_server if pool_production_down
```

## 白名单 TCP 连接

您可以阻止客户端 IP 地址访问您的服务器。如果定义的 IP 地址不在白名单中，以下示例规则阻止这些 IP 地址并停止连接。

```
acl whitelist src 10.10.10.0 20.20.20.0
tcp-request connection reject if !whitelist
```

## 启用 sslv3 和 tlsv1

默认情况下，服务监控器扩展禁用 `sslv3` 和 `tlsv1`。您可以使用以下应用程序规则启用它们。

```
sslv3 enable
tlsv1 enable
```

## 配置客户端会话超时

会话超时是客户端的最大连接闲置时间。在客户端需要确认或发送数据时，将应用闲置超时。在 HTTP 模式下，在第一阶段（客户端发送请求）和响应期间（客户端读取服务器发送的数据），该超时是特别重要的。默认超时值为 5 分钟。

以下示例规则将超时时间设置为 100 秒。

```
timeout client 100s
```

时间可以设置为以毫秒、秒、分钟、小时或天为单位的整数。

## 添加虚拟服务器

将 NSX Edge 内部或上行链路接口作为虚拟服务器进行添加。

## 前提条件

- 确认应用程序配置文件可用。请参见[创建应用程序配置文件](#)。
- 如果将应用程序规则与虚拟服务器相关联，请参见[创建应用程序配置文件](#)。
- 如果启用加速以使用更快的负载均衡器，应在配置负载均衡器时启用加速。请参见[配置负载均衡器服务](#)。

## 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**，然后单击**负载均衡器 (Load Balancer)**选项卡。
- 5 在左侧导航面板中，单击**虚拟服务器 (Virtual Servers)**。
- 6 单击**添加 (Add)** () 图标。
- 7 选中**启用虚拟服务器 (Enable Virtual Server)**以使该虚拟服务器可用。
- 8 (可选) 选中**启用加速 (Enable Acceleration)**以使 NSX Edge 负载均衡器使用更快的 L4 负载均衡器引擎，而不是 L7 负载均衡器引擎。  
  
如果虚拟服务器配置（如应用程序规则、HTTP 类型或 cookie 持久性）使用 L7 负载均衡器引擎，即使启用了加速，也会使用 L7 负载均衡器引擎。  
  
您可以使用 **show service load balancer virt** CLI 命令确认正在使用的负载均衡器引擎。
- 9 选择要与虚拟服务器相关联的应用程序配置文件。  
  
您只能关联与所添加的虚拟服务器具有相同协议的应用程序配置文件。此时将显示选定的池所支持的服务。
- 10 输入虚拟服务器的名称和描述。
- 11 单击**选择 IP 地址 (Select IP Address)**，以设置负载均衡器正在侦听的 IP 地址，然后键入虚拟服务器将处理的协议。  
  
“选择 IP 地址”对话框仅显示主 IP 地址。如果使用辅助 IP 地址创建 VIP，请手动输入该地址。
- 12 从下拉菜单中选择虚拟服务器处理的协议。
- 13 输入负载均衡器侦听的端口号。  
  
也可以设置端口范围（如 80,8001-8004,443）以共享虚拟服务器配置，例如，服务器池、应用程序配置文件和应用程序规则。  
  
要使用 FTP，必须为 TCP 协议分配端口 21。
- 14 选择应用程序规则。
- 15 在“连接限制”部分中，输入虚拟服务器可以处理的最大并发连接数。
- 16 在“连接速率限制”部分中，输入每秒的最大传入新连接请求数。
- 17 (可选) 单击**高级 (Advanced)**选项卡，然后添加应用程序规则以将其与虚拟服务器相关联。



18 单击**确定 (OK)**。

## 管理应用程序配置文件

在创建应用程序配置文件并将其与虚拟服务器关联后，您可以更新现有的配置文件或将其删除以节省系统资源。

### 编辑应用程序配置文件

可以编辑应用程序配置文件。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**监控 (Monitor)**选项卡，然后单击**负载均衡器 (Load Balancer)**选项卡。
- 5 在左侧导航面板中，单击**应用程序配置文件 (Application Profiles)**。
- 6 选择一个配置文件，然后单击**编辑 (Edit)** (✎) 图标。
- 7 对流量、持久性、证书或密码配置进行相应的更改，然后单击**完成 (Finish)**。

### 为负载均衡器配置 SSL 终止

如果未配置 SSL 终止，则不会检查 HTTP 请求。负载均衡器可以看到源和目标 IP 地址以及加密的数据。如果要检查 HTTP 请求，您可以在负载均衡器上终止 SSL 会话，然后创建到单元池的新 SSL 会话。

#### 前提条件

转到**管理 > 设置 > 证书 (Manage > Settings > Certificates)**以确保具有有效的证书。

#### 步骤

- 1 在**管理 > 负载均衡器 > 应用程序配置文件 (Manage > Load Balancer > Application Profiles)**的应用程序配置文件中：
- 2 从下拉菜单中选择 **HTTPS** 类型。
- 3 验证是否取消选中了**启用 SSL 直通 (Enable SSL Passthrough)**。
- 4 验证是否选中了**配置服务证书 (Configure Service Certificate)**。

- 5 从列表中选择相应的证书。

**Edit Profile**

Name:

Type:

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence:

Cookie Name:

Mode:

Expires in (Seconds):

☐ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

**Virtual Server Certificates** **Pool Certificates**

**Service Certificates** **CA Certificates** **CRL**

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu

## 删除应用程序配置文件

您可以删除应用程序配置文件。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**，然后单击**负载均衡器 (Load Balancer)**选项卡。
- 5 在左侧导航面板中，单击**应用程序配置文件 (Application Profiles)**。
- 6 选择配置文件，然后单击**删除 (Delete)**图标。

## 管理服务监控器

在创建服务监控器以便为网络流量定义运行状况检查参数并将其与一个池关联后，您可以更新现有的服务监控器或将其删除以节省系统资源。

## 编辑服务监控器

您可以编辑服务监控器。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**，然后单击**负载均衡器 (Load Balancer)**选项卡。
- 5 在左侧导航面板中，单击**服务监控器 (Service Monitoring)**。
- 6 选择服务监控器，然后单击**编辑 (Edit)**图标。
- 7 进行相应更改，然后单击**确定 (OK)**。

## 删除服务监控器

可以删除服务监控器。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**，然后单击**负载均衡器 (Load Balancer)**选项卡。
- 5 在左侧导航面板中，单击**服务监控器 (Service Monitoring)**。
- 6 选择服务监控器并单击**删除 (Delete)**图标。

## 管理服务器池

在添加服务器池以管理负载均衡器分配后，您可以更新现有的池或将其删除以节省系统资源。

## 编辑服务器池

可以编辑服务器池。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**监控**选项卡，然后单击**负载均衡器**选项卡。

- 5 确保您处于“池”选项卡中。
- 6 选择要编辑的池。
- 7 单击编辑 (✎) 图标。
- 8 进行适当更改，然后单击完成。

## 将负载均衡器配置为使用透明模式

“透明”表示客户端 IP 地址对后端服务器可见。如果未选中“透明”（默认值），则后端服务器会将流量源 IP 看作负载均衡器内部 IP。如果选择了“透明”，则源 IP 是真正的客户端 IP，并且 NSX Edge 必须位于服务器响应路径中。典型的设计是将 NSX Edge 作为服务器默认网关。

### 步骤

- ◆ 在**管理 > 负载均衡器 > 池 (Manage > Load Balancer > Pools)**的服务器池配置中，启用透明模式。

**Edit Pool**

Name: \* Web-Tier-Pool-01

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default\_https\_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	web-01a	172.16.1...	1	443	443	0	0
✓	web-02a	172.16.1...	1	443	443	0	0

☒ Transparent

OK Cancel

## 删除服务器池

可以删除服务器池。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**监控**选项卡，然后单击**负载均衡器**选项卡。
- 5 确保您处于“池”选项卡中。

- 6 选择要删除的池
- 7 单击删除 (✖) 图标。

## 管理虚拟服务器

在添加虚拟服务器后，您可以更新或删除现有的虚拟服务器配置。

### 编辑虚拟服务器

可以编辑虚拟服务器。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**监控**选项卡，然后单击**负载均衡器**选项卡。
- 5 单击**虚拟服务器**选项卡。
- 6 选择要编辑的虚拟服务器。
- 7 单击编辑 (✎) 图标。
- 8 进行适当更改，然后单击**完成**。

### 删除虚拟服务器

可以删除虚拟服务器。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**监控**选项卡，然后单击**负载均衡器**选项卡。
- 5 单击**虚拟服务器**选项卡。
- 6 选择要删除的虚拟服务器。
- 7 单击删除 (✖) 图标。

## 管理应用程序规则

在创建应用程序规则以配置应用程序流量后，您可以编辑或删除现有的规则。

## 编辑应用程序规则

可以编辑应用程序规则。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**，然后单击**负载均衡器 (Load Balancer)**选项卡。
- 5 在左侧的导航面板中，单击**应用程序规则 (Application Rules)**。
- 6 选择规则并单击**编辑 (Edit)**图标。
- 7 进行相应更改，然后单击**确定 (OK)**。

## 删除应用程序规则

可以删除应用程序规则。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**，然后单击**负载均衡器 (Load Balancer)**选项卡。
- 5 在左侧导航面板中，单击**应用程序配置文件 (Application Profiles)**。
- 6 选择配置文件，然后单击**删除 (Delete)**图标。

## 对使用 NTLM 身份验证的 Web 服务器进行负载均衡

默认情况下，NSX 负载均衡器会在每个客户端请求后关闭服务器 TCP 连接。NTLM 身份验证在同一个 TCP 会话中需要多个 HTTP 请求，因此通过 NSX 负载均衡器进行的身份验证中断。

### 前提条件

要解决此问题，请在对使用 NTLM 身份验证的 Web 服务器进行负载均衡的 VIP 上添加以下应用程序规则：

```
add # NTLM authentication and keep the server connection open between requests
no option http-server-close
```

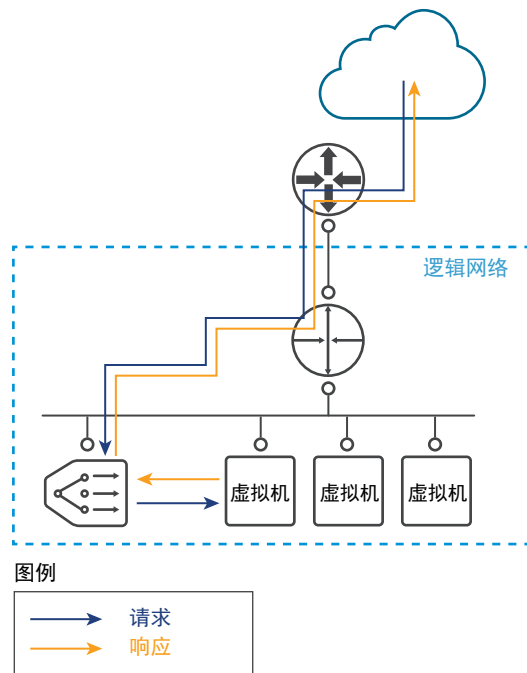
该应用程序规则在请求之间将服务器连接保持打开状态。

## NSX 负载均衡器配置场景

您可以使用 NSX 负载均衡器配置场景了解所需的端到端工作流。

### 场景：配置单臂负载均衡器

可以将 Edge 服务网关 (ESG) 视为传入客户端流量的代理。



在代理模式下，负载均衡器将自己的 IP 地址作为源地址，以将请求发送到后端服务器。后端服务器查看从负载均衡器中发送的所有流量，并直接响应负载均衡器。这种模式也称为 **SNAT** 模式或非透明模式。

典型的 **NSX** 单臂负载均衡器部署在具有其后端服务器的相同子网上，与逻辑路由器分开。**NSX** 负载均衡器虚拟服务器侦听虚拟 IP 以查找来自客户端的传入请求，并将这些请求发送到后端服务器。对于返回流量，需要使用反向 **NAT** 以将源 IP 地址从后端服务器更改为虚拟 IP (**VIP**) 地址，然后将虚拟 IP 地址发送到客户端。如果不执行该操作，到客户端的连接将中断。

在 **ESG** 收到流量后，它执行两个操作：目标网络地址转换 (**DNAT**) 以将 **VIP** 地址更改为某个负载均衡计算机的 IP 地址；以及源网络地址转换 (**SNAT**) 以将客户端 IP 地址与 **ESG** IP 地址调换。

然后，**ESG** 服务器将流量发送到负载均衡服务器，负载均衡服务器将响应发送回 **ESG**，然后发送回客户端。该选项比内嵌模式容易配置得多，但具有两个潜在问题。第一个问题是，该模式需要使用专用的 **ESG** 服务器，第二个问题是，负载均衡器服务器不知道原始客户端 IP 地址。**HTTP/HTTPS** 应用程序的一种解决方法是，在 **HTTP** 应用程序配置文件中启用“插入 **X-Forwarded-For**”，以便在发送到后端服务器的请求的 **X-Forwarded-For** **HTTP** 标头中包含客户端 IP 地址。

如果 HTTP/HTTPS 以外的应用程序要求在后端服务器上看到客户端 IP 地址，您可以将 IP 池配置为透明的。如果客户端没有位于与后端服务器相同的子网上，建议使用内嵌模式。否则，您必须将负载均衡器 IP 地址作为后端服务器的默认网关。

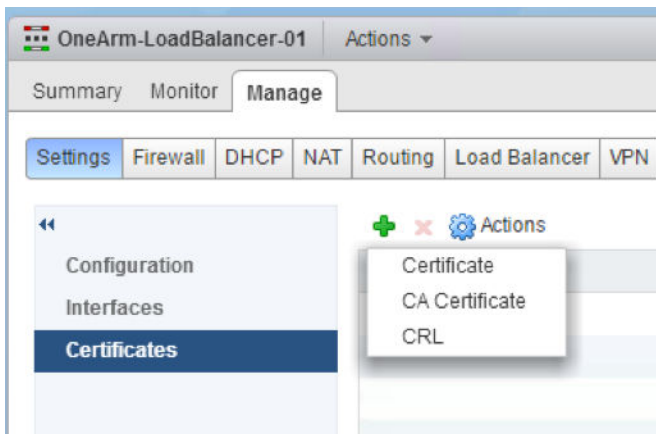
**注** 通常，可以使用两种方法确保连接完整性：

- SNAT/代理/非透明模式（如上所述）
- 直接服务器返回 (DSR)

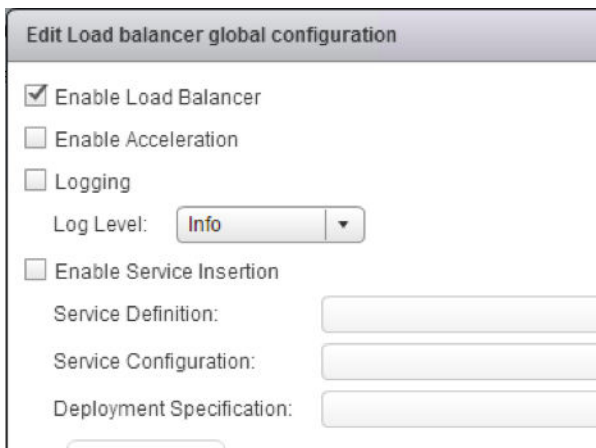
在 DSR 模式下，后端服务器直接响应客户端。目前，NSX 负载均衡器不支持 DSR。

## 步骤

- 1 双击 Edge，然后选择**管理 > 设置 > 证书 (Manage > Settings > Certificate)**以创建一个证书。



- 2 选择**管理 > 负载均衡器 > 全局配置 > 编辑 (Manage > Load Balancer > Global Configuration > Edit)**以启用负载均衡器服务。





- 3 选择**管理 > 负载均衡器 > 应用程序配置文件 (Manage > Load Balancer > Application Profiles)**以创建一个 HTTPS 应用程序配置文件。

**New Profile**

Name: Web-SSL-Profile

Type: HTTPS

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence: None

Cookie Name:

Mode:

Expires in (Seconds):

☐ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

Virtual Server Certifica... Pool Certificates

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu

**注** 上面的屏幕截图使用自签名证书以仅用于说明目的。

- 4 （可选）单击**管理 > 负载均衡器 > 服务监控 (Manage > Load Balancer > Service Monitoring)**，然后编辑默认服务监控以将其从基本 HTTP/HTTPS 更改为特定的 URL/URI（如果需要）。

5 选择**管理 > 负载均衡器 > 池 (Manage > Load Balancer > Pools)**以创建服务器池。

要使用 SNAT 模式，请在池配置中取消选中**透明 (Transparent)**复选框。

**Edit Pool**

Name: \* Web-Tier-Pool-01

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default\_https\_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connections
✓	web-01a	172.16.10.11	1	443	443	0	0
✓	web-02a	172.16.10.12	1	443	443	0	0

☐ Transparent

OK Cancel

确保已列出并启用虚拟机。

6 （可选）单击**管理 > 负载均衡器 > 池 > 显示池统计信息 (Manage > Load Balancer > Pools > Show Pool Statistics)**以检查状态。

确保成员处于已启动状态。

- 7 选择**管理 > 负载均衡器 > 虚拟服务器 (Manage > Load Balancer > Virtual Servers)**以创建一个虚拟服务器。

如果要将 L4 负载均衡器用于 UDP 或更高性能的 TCP，请选中**启用加速 (Enable Acceleration)**。如果选中**启用加速 (Enable Acceleration)**，请确保负载均衡器 NSX Edge 上的防火墙状态为已启用 (**Enabled**)，因为 L4 SNAT 需要使用防火墙。

The screenshot shows the 'General' tab of the Virtual Server configuration. The 'Enable Virtual Server' checkbox is checked. The 'Application Profile' is set to 'OneArmWeb-01'. The 'Name' is 'Web-Tier-VIP-01'. The 'IP Address' is '172.16.10.10'. The 'Protocol' is 'HTTPS'. The 'Port' is '443'. The 'Default Pool' is 'Web-Tier-Pool-01'. The 'Connection Limit' is '0'. The 'Connection Rate Limit' is '0 (CPS)'.

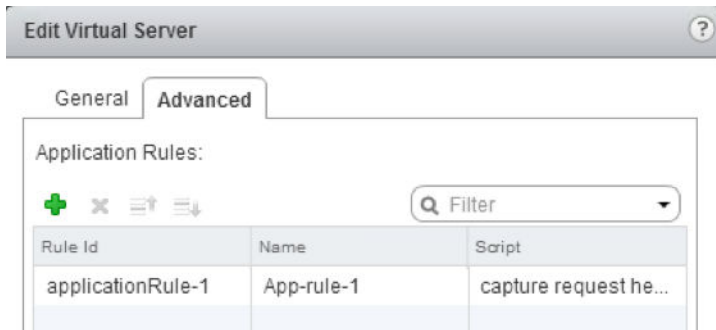
确保 IP 地址绑定到服务器池。

- 8 (可选) 如果使用一个应用程序规则，请在**管理 > 负载均衡器 > 应用程序规则 (Manage > Load Balancer > Application Rules)**中检查配置。

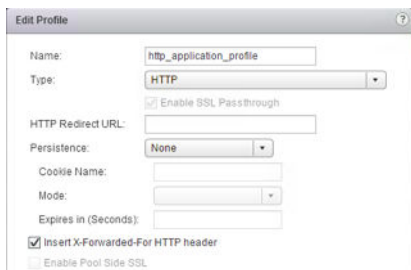
The screenshot shows the 'Add Application Rule' dialog. The 'Name' is 'App-Rule-1'. The 'Script' contains the text: '# A sample application rule to log the name of the virtual server' and 'capture request header Host len 32'.

- 9 如果使用一个应用程序规则，请在**管理 > 负载均衡器 > 虚拟服务器 > 高级 (Manage > Load Balancer > Virtual Servers > Advanced)**中确保该应用程序规则与虚拟服务器相关联。

有关支持的示例，请参见：<https://communities.vmware.com/docs/DOC-31772>。



在非透明模式下，后端服务器无法看到客户端 IP，但可以看到负载均衡器内部 IP 地址。作为 HTTP/HTTPS 流量的解决方法，请选中**插入 X-Forwarded-For HTTP 标头 (Insert X-Forwarded-For HTTP header)**。如果选中该选项，Edge 负载均衡器将添加 “X-Forwarded-For” 标头并且值为客户端源 IP 地址。



## 场景：为平台服务控制器配置 NSX 负载均衡器

平台服务控制器 (PSC) 提供基础架构安全功能，例如，vCenter Single Sign-On、许可、证书管理和服务器预留。

在配置 NSX 负载均衡器后，您可以为 vCenter Single Sign-On 提供 NSX Edge 设备上行链路接口 IP 地址。

### 前提条件

- 执行知识库中列出的 PSC 高可用性准备任务。请参见 <http://kb.vmware.com/kb/2113315>。
- 从第一个 PSC 节点中保存 /ha/lb.crt 和 /ha/lb\_rsa.key 以配置证书。
- 确认配置了 NSX Edge 设备。
- 确认至少具有一个上行链路以配置 VIP，并将一个接口连接到内部逻辑交换机。

### 步骤

- 1 将 PSC CA 证书添加到 NSX Edge 中。
  - a 保存 OpenSSL 命令生成的 PSC root.cer 和证书、RSA 和密码短语。
  - b 双击 Edge，然后选择**管理 (Manage) > 设置 (Settings) > 证书 (Certificate)**。

- c 将保存的内容 `root.cer` 文件添加到 CA 证书内容中。
  - d 将保存的密码短语添加到私钥部分中。
- 2 启用负载均衡器服务。
  - a 选择**管理 (Manage) > 负载均衡器 (Load Balancer) > 编辑 (Edit)**。
  - b 选中**启用负载均衡 (Enable Load Balancing)**和**日志记录 (Logging)**选项。

### 3 创建具有 TCP 和 HTTPS 协议的应用程序配置文件。

- a 选择**管理 (Manage) > 负载均衡器 (Load Balancer) > 应用程序配置文件 (Application Profiles)**。
- b 创建一个 TCP 应用程序配置文件。

The 'New Profile' dialog box is shown with the following configuration:

- Name:** sso\_tcp\_profile
- Type:** TCP
- Enable SSL Passthrough:** ☐
- HTTP Redirect URL:** (empty)
- Persistence:** Source IP
- Cookie Name:** (empty)
- Mode:** (empty)
- Expires in (Seconds):** (empty)
- Insert X-Forwarded-For HTTP header:** ☐
- Enable Pool Side SSL:** ☐
- Virtual Server Certificates:** (selected tab)
- Service Certificates:** (selected sub-tab)
- Configure Service Certificate:** ☐
- Cipher:** (empty)
- Client Authentication:** Ignore

The 'Virtual Server Certificates' section contains a table with the following data:

Common Name	Issuer	Validity
NSX-ESG-1-0.system	CA	Thu Jul 30 2015 - Thu

Buttons: OK, Cancel

- c 创建一个 HTTPS 应用程序配置文件。

The 'New Profile' dialog box is shown with the following configuration:

- Name:** sso\_https\_profile
- Type:** HTTPS
- Enable SSL Passthrough:** ☐
- HTTP Redirect URL:** (empty)
- Persistence:** Source IP
- Cookie Name:** (empty)
- Mode:** (empty)
- Expires in (Seconds):** (empty)
- Insert X-Forwarded-For HTTP header:** ☐
- Enable Pool Side SSL:** ☒
- Virtual Server Certificates:** (selected tab)
- Service Certificates:** (selected sub-tab)
- Configure Service Certificate:** ☒
- Cipher:** (empty)
- Client Authentication:** Ignore

The 'Virtual Server Certificates' section contains a table with the following data:

Common Name	Issuer	Validity
NSX-ESG-1-0.system	CA	Thu Jul 30 2015 - Thu

Buttons: OK, Cancel

- 4 创建应用程序池以添加成员 PSC 节点。
- 选择**管理 (Manage) > 负载均衡器 (Load Balancer) > 池 (Pools)**。
  - 创建两个具有监控端口 **443** 的应用程序池。

使用 PSC 节点 IP 地址。

**Edit Pool**

Name: \* sso\_tcp\_pool1

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default\_tcp\_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	PSC01	192.168.1.1	1	443		0	0
✓	PSC02	192.168.1.2	1	443		0	0

☐ Transparent

OK Cancel

- 创建两个具有监控端口 **389** 的应用程序池。
- 使用 PSC 节点 IP 地址。

**New Pool**

Name: \* sso\_tcp\_pool2

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default\_tcp\_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	PSC01	192.168.1.1	1	389		0	0
✓	PSC02	192.168.1.2	1	389		0	0

☐ Transparent

OK Cancel

## 5 为 TCP 和 HTTPS 协议创建虚拟服务器。

- a 选择**管理 (Manage) > 负载均衡器 (Load Balancer) > 虚拟服务器 (Virtual Servers)**。
- b 为 TCP VIP 创建一个虚拟服务器。

The screenshot shows the 'New Virtual Server' dialog box with the 'General' tab selected. The 'Enable Virtual Server' checkbox is checked. The 'Application Profile' is set to 'sso\_tcp\_profile'. The 'Name' is 'sso\_tcp\_vip'. The 'IP Address' is '10.156.209.158' with a 'Select IP Address' link. The 'Protocol' is 'TCP'. The 'Port' is '389,636,2012,2014,2020'. The 'Default Pool' is 'sso\_tcp\_pool2'. The 'Connection Limit' and 'Connection Rate Limit' fields are empty. The 'OK' and 'Cancel' buttons are at the bottom right.

- c 为 HTTPS VIP 创建一个虚拟服务器。

The screenshot shows the 'New Virtual Server' dialog box with the 'General' tab selected. The 'Enable Virtual Server' checkbox is checked. The 'Application Profile' is set to 'sso\_https\_profile'. The 'Name' is 'sso\_https\_vip'. The 'IP Address' is '10.156.209.158' with a 'Select IP Address' link. The 'Protocol' is 'HTTPS'. The 'Port' is '443'. The 'Default Pool' is 'sso\_tcp\_pool1'. The 'Connection Limit' and 'Connection Rate Limit' fields are empty. The 'OK' and 'Cancel' buttons are at the bottom right.



## 其他 Edge 服务

NSX Services 网关提供 IP 地址池和一对一的静态 IP 地址分配以及外部 DNS 服务器配置。

必须具有工作 NSX Edge 实例才能使用上述的任一服务。有关设置 NSX Edge 的信息，请参见 [NSX Edge 配置](#)。

本章讨论了以下主题：

- [管理 DHCP 服务](#)
- [配置 DHCP 中继](#)
- [配置 DNS 服务器](#)

### 管理 DHCP 服务

NSX Edge 支持 IP 地址池和一对一的静态 IP 地址分配。静态 IP 地址绑定基于请求客户端的 vCenter 托管对象 ID 和接口 ID。

NSX Edge DHCP 服务遵循以下准则：

- 侦听 NSX Edge 内部接口以发现 DHCP。
- 将 NSX Edge 上内部接口的 IP 地址作为所有客户端的默认网关地址（非直接连接的池除外），并将内部接口的广播和子网掩码值用于容器网络。

在下列情形下，您必须在客户端虚拟机上重新启动 DHCP 服务：

- 您更改或删除了一个 DHCP 池、默认网关或 DNS 服务器。
- 您更改了 NSX Edge 实例的内部 IP 地址。

### 添加 DHCP IP 池

DHCP 服务需要一个 IP 地址池。IP 池是网络中连续的 IP 地址范围。该池中的 IP 地址将会分配给未绑定任何地址的受 NSX Edge 保护的虚拟机。IP 池的范围不得互相交叉，因此一个 IP 地址只能属于一个 IP 池。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。

- 4 单击**管理**选项卡，然后单击 **DHCP** 选项卡。
- 5 单击**添加 (+)** 图标。
- 6 配置池。

选项	操作
自动配置 DNS	选择为 DHCP 绑定使用 DNS 服务配置。
租约永不过期	选择将地址永久绑定到虚拟机的 MAC 地址。如果选择此选项，将会禁用租约时间。
起始 IP	键入池的起始 IP 地址。
结束 IP	键入池的结束 IP 地址。
域名	键入 DNS 服务器的域名。此选项为可选选项。
主名称服务器	如果未选择自动配置 DNS，请键入 DNS 服务的主名称服务器。您必须输入 DNS 服务器的 IP 地址用于进行主机名到 IP 地址的解析。此选项为可选选项。
辅助名称服务器	如果未选择自动配置 DNS，请键入 DNS 服务的辅助名称服务器。您必须输入 DNS 服务器的 IP 地址用于进行主机名到 IP 地址的解析。此选项为可选选项。
默认网关	键入默认网关地址。如果未指定默认网关 IP 地址，则会将 NSX Edge 实例的内部接口作为默认网关。此选项为可选选项。
子网掩码	指定子网掩码。对于分布式路由器，该子网掩码必须与 Edge 接口或 DHCP 中继的子网掩码相同。
租约时间	选择是以默认时间（1 天）将地址租给客户端，还是键入一个值（以秒为单位）。如果选择了租约永不过期，则将无法指定租约时间。此选项为可选选项。

- 7 单击**确定**。

## 启用 DHCP 服务

启用 DHCP 服务以允许 NSX Edge 自动将已定义 IP 池中的某个 IP 地址分配给虚拟机。

### 前提条件

必须已添加 DHCP IP 池。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理**选项卡，然后单击 **DHCP** 选项卡。
- 5 单击**启用**。
- 6 如果需要，选择**启用日志记录**，并选择日志级别。
- 7 单击**发布更改**。

### 后续步骤

创建 IP 池和绑定。

## 编辑 DHCP IP 池

您可以编辑 DHCP IP 池以添加或移除 IP 地址。


### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击 **DHCP** 选项卡。
- 5 选择 DHCP 池并单击**编辑 (Edit)**图标。
- 6 进行相应更改，然后单击**确定 (OK)**。

## 添加 DHCP 静态绑定

如果虚拟机上有正在运行的服务，并且您不希望更改 IP 地址，则可将 IP 地址绑定到虚拟机的 MAC 地址。绑定的 IP 地址不得与 IP 池重叠。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击 **DHCP** 选项卡。
- 5 从左侧面板中选择**绑定 (Bindings)**。
- 6 单击**添加 (Add)** () 图标。
- 7 配置绑定。

选项	操作
自动配置 DNS (Auto Configure DNS)	选择为 DHCP 绑定使用 DNS 服务配置。
租约永不过期 (Lease never expires)	选择将地址永久绑定到虚拟机的 MAC 地址。
接口 (Interface)	选择要绑定的 NSX Edge 接口。
虚拟机名称 (VM Name)	选择要绑定的虚拟机。
虚拟机虚拟网卡索引 (VM vNIC Index)	选择要绑定到 IP 地址的虚拟机网卡。
主机名称 (Host Name)	键入 DHCP 客户端虚拟机的主机名称。
IP 地址 (IP Address)	键入要与选定虚拟机的 MAC 地址绑定的地址。
子网掩码 (Subnet Mask)	指定子网掩码。对于分布式路由器，该子网掩码应与 Edge 接口或 DHCP 中继的子网掩码相同。
域名 (Domain Name)	键入 DNS 服务器的域名。

选项	操作
主名称服务器 (Primary Name Server)	如果未选择 <b>自动配置 DNS (Auto Configure DNS)</b> ，请键入 DNS 服务的主名称服务器 (Primary Nameserver)。您必须输入 DNS 服务器的 IP 地址用于进行主机名到 IP 地址的解析。
辅助名称服务器 (Secondary Name Server)	如果未选择 <b>自动配置 DNS (Auto Configure DNS)</b> ，请键入 DNS 服务的辅助名称服务器 (Secondary Nameserver)。您必须输入 DNS 服务器的 IP 地址用于进行主机名到 IP 地址的解析。
默认网关 (Default Gateway)	键入默认网关地址。如果未指定默认网关 IP 地址，则会将 NSX Edge 实例的内部接口作为默认网关。
租约时间 (Lease Time)	如果未选择 <b>租约永不过期 (Lease never expires)</b> ，请选择是以默认时间（1 天）将地址租给客户端，还是键入一个值（以秒为单位）。

8 单击**添加 (Add)**。

9 单击**发布更改 (Publish Changes)**。

## 编辑 DHCP 绑定

您可以分配绑定到虚拟机 MAC 地址的不同静态 IP 地址。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击 **DHCP** 选项卡。
- 5 从左侧面板中选择**绑定 (Bindings)**，然后单击绑定进行编辑。
- 6 单击“编辑”图标。
- 7 进行相应更改，然后单击**确定 (OK)**。

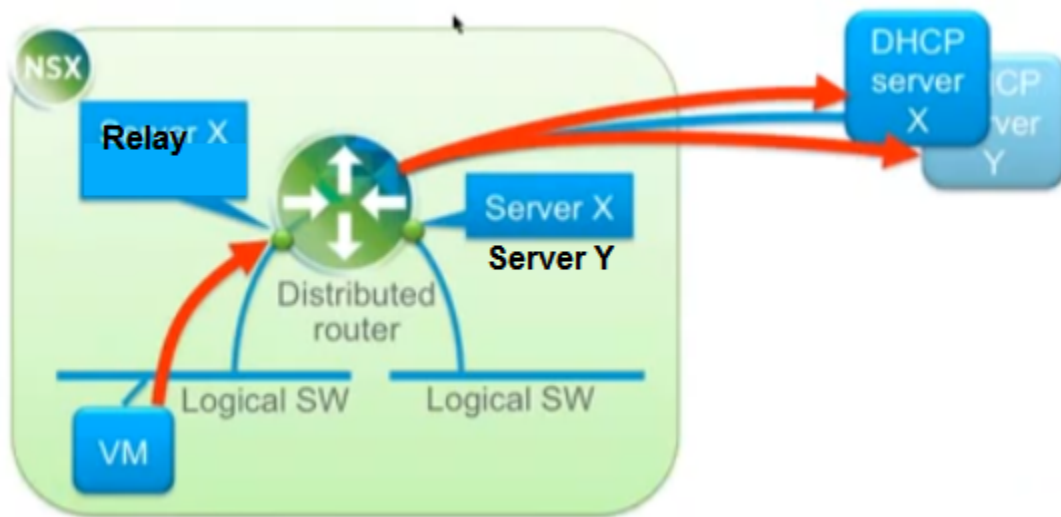
## 配置 DHCP 中继

动态主机配置协议 (DHCP) 中继可使您利用 NSX 中现有的 DHCP 基础架构，而不会对您环境中的 IP 地址管理造成任何中断。在物理环境中将 DHCP 消息从虚拟机中继到指定的 DHCP 服务器。这可使 NSX 中的 IP 地址继续与其他环境中的 IP 地址同步。

DHCP 配置已应用于逻辑路由器端口，并且可以列出多个 DHCP 服务器。会向所有列出的服务器发送请求。中继来自客户端的 DHCP 请求时，中继会添加该请求的网关 IP 地址。外部 DHCP 服务器使用此网关地址来匹配池以及为该请求分配 IP 地址。该网关地址必须属于中继正在运行的 NSX 端口的子网。

可以为每个逻辑交换机指定不同的 DHCP 服务器，并且可以在每个逻辑路由器上配置多个 DHCP 服务器，从而为多个 IP 域提供支持。

在 DHCP 服务器上配置池和绑定时，请确保中继查询的池/绑定的子网掩码与 DHCP 中继的接口相同。当 DLR 用作虚拟机与提供 DHCP 服务的 Edge 之间的 DHCP 中继时，您必须在 API 中提供子网掩码信息。此子网掩码应与 DLR 中虚拟机的网关接口上配置的子网掩码匹配。



### 注

- DHCP 中继不支持重叠的 IP 地址空间（选项 82）。
- DHCP 中继和 DHCP 服务无法同时在端口/虚拟网卡上运行。如果已在端口上配置中继代理，则无法在该端口的子网中配置 DHCP 池。

## 添加 DHCP 中继服务器

添加您希望将 DHCP 消息转发到的外部中继服务器。中继服务器可以是 IP 集、IP 地址块、域或以上所有项的组合。消息将会转发到列出的每个 DHCP 服务器。

### 步骤

- 1 在 vSphere Web Client 中，导航到**网络和安全 (Networking & Security) > NSX Edge (NSX Edges)**。
- 2 双击相应的 Edge，并确保您处于**管理 (Manage) > DHCP** 选项卡中。
- 3 单击 **DHCP 中继全局配置 (DHCP Relay Global Configuration)** 旁边的 **编辑 (Edit)**。
- 4 要将 IP 集作为服务器添加，请执行以下操作：
  - a 单击**添加 (Add)**，然后选择 IP 集。
  - b 通过单击  图标将选定的 IP 集移至“选定的对象”列表中。
  - c 单击**确定 (OK)**。
- 5 要添加 IP 地址或域名，请在相应区域中键入地址或名称。
- 6 单击**确定 (OK)**。

## 添加中继代理

添加用于将 DHCP 消息中继到外部 DHCP 中继服务器的 Edge 接口。

### 步骤

1 在 **DHCP 中继代理 (DHCP Relay Agents)** 区域中，单击 **添加 (Add)** 图标。

2 在 **虚拟网卡 (vNIC)** 中，确保选择了内部虚拟网卡。

**网关 IP 地址 (Gateway IP Address)** 显示所选虚拟网卡的主 IP 地址。

3 单击 **确定 (OK)**。

## 配置 DNS 服务器

您可以配置外部 DNS 服务器，NSX Edge 可向该服务器中继来自客户端的名称解析请求。NSX Edge 将向 DNS 服务器中继客户端应用程序请求，以便完全解析网络名称并缓存来自服务器的响应。

### 步骤

1 登录到 vSphere Web Client。

2 单击 **网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。

3 双击 NSX Edge。

4 单击 **管理 (Manage)** 选项卡，然后单击 **设置 (Settings)** 选项卡。

5 在 **DNS 配置 (DNS Configuration)** 面板中，单击 **更改 (Change)**。

6 单击 **启用 DNS 服务 (Enable DNS Service)** 以启用 DNS 服务。

7 键入两台 DNS 服务器的 IP 地址。

8 如果需要，更改默认缓存大小。

9 单击 **启用日志记录 (Enable Logging)** 以记录 DNS 流量并选择日志级别。

生成的日志发送到 syslog 服务器。

10 单击 **确定 (OK)**。

## 服务编排

服务编排有助于置备网络和安全服务并将其分配给虚拟基础架构中的应用程序。您可以将这些服务映射到安全组，这些服务即会应用到安全组中的虚拟机。

### 安全组

首先创建安全组来定义要保护的资产。安全组可以是静态的（包含特定虚拟机），也可以是动态的，其中的成员资格可以通过以下一种或多种方式来定义：

- vCenter 容器（群集、端口组或数据中心）
- 安全标记、IPset、MACset 或甚至其他安全组。例如，您可以加入一个条件，将使用指定安全标记（例如 AntiVirus.virusFound）进行标记的所有成员添加到安全组中。
- 目录组（如果已向 Active Directory 注册 NSX Manager）
- 正则表达式，如名称为 VM1 的虚拟机

请注意，安全组成员资格经常发生变化。例如，以 AntiVirus.virusFound 标记进行标记的虚拟机移到隔离安全组中。清除病毒并从虚拟机中删除此标记后，该虚拟机再次移出隔离安全组。

### 安全策略

安全策略是以下服务配置的集合。

**表 17-1. 包含在安全策略中的安全服务**

服务	描述	适用对象
防火墙规则	定义允许流向安全组、从安全组流出以及在安全组内流动的流量的规则。	虚拟网卡
Endpoint 服务	数据安全或第三方解决方案提供商服务，如防病毒或漏洞管理服务。	虚拟机
网络自检服务	监控网络的服务，如 IPS。	虚拟机

在 NSX 中部署服务期间，第三方供应商可选择正在部署的服务的服务类别。系统会为每个供应商模板创建一个默认服务配置文件。

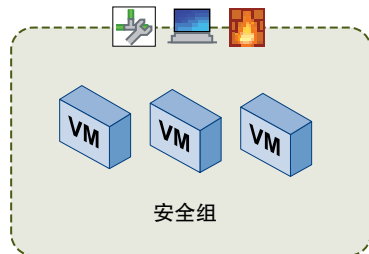
将第三方供应商服务升级到 NSX 6.1 时，系统会为正在升级的供应商模板创建默认服务配置文件。包含 Guest Introspection 规则的现有服务策略将更新为引用在升级过程中创建的服务配置文件。

### 将安全策略映射到安全组

可以将安全策略（如 **SP1**）映射到安全组（如 **SG1**）。针对 **SP1** 配置的服务应用于所有属于 **SG1** 的虚拟机。

**注** 当您需要将大量安全组连接到同一安全策略时，请创建一个可以包含所有这些子安全组的伞安全组，并将通用安全策略应用于该伞安全组。此举将确保 **NSX** 分布式防火墙可以高效地利用 **ESXi** 主机内存。

图 17-1. 服务编排概述



如果一个虚拟机属于多个安全组，则应用于该虚拟机的服务将取决于映射到这些安全组的安全策略的优先级。

服务编排配置文件可以作为备份导出和导入，或者在其他环境中使用。这种管理网络和安全服务的方法有助于实现可操作和可重复的安全策略管理。

本章讨论了以下主题：

- [使用服务编排](#)
- [服务编排的图形视图](#)
- [使用安全标记](#)
- [查看有效服务](#)
- [使用安全策略](#)
- [编辑安全组](#)
- [服务编排场景](#)

## 使用服务编排

服务编排可帮助您轻松地使用安全服务。

让我们浏览一个示例，该示例显示了服务编排如何以端到端方式来帮助保护您的网络。让我们假设您的环境中定义了以下安全策略：

- 包括漏洞扫描服务的初始状态安全策略 (**InitStatePolicy**)
- 除防火墙规则和防病毒服务以外，还包括网络 **IPS** 服务的修复安全策略 (**RemPolicy**)

确保 **RemPolicy** 的权重（优先级）高于 **InitStatePolicy**。

您还拥有以下准备就绪的安全组：

- 应用程序资产组 (**AssetGroup**)，其中包括您的环境中的关键业务应用程序
- 名为 **RemGroup** 的修复安全组，此安全组由表示虚拟机易受攻击的标记 (**VULNERABILITY\_MGMT.VulnerabilityFound.threat=medium**) 定义

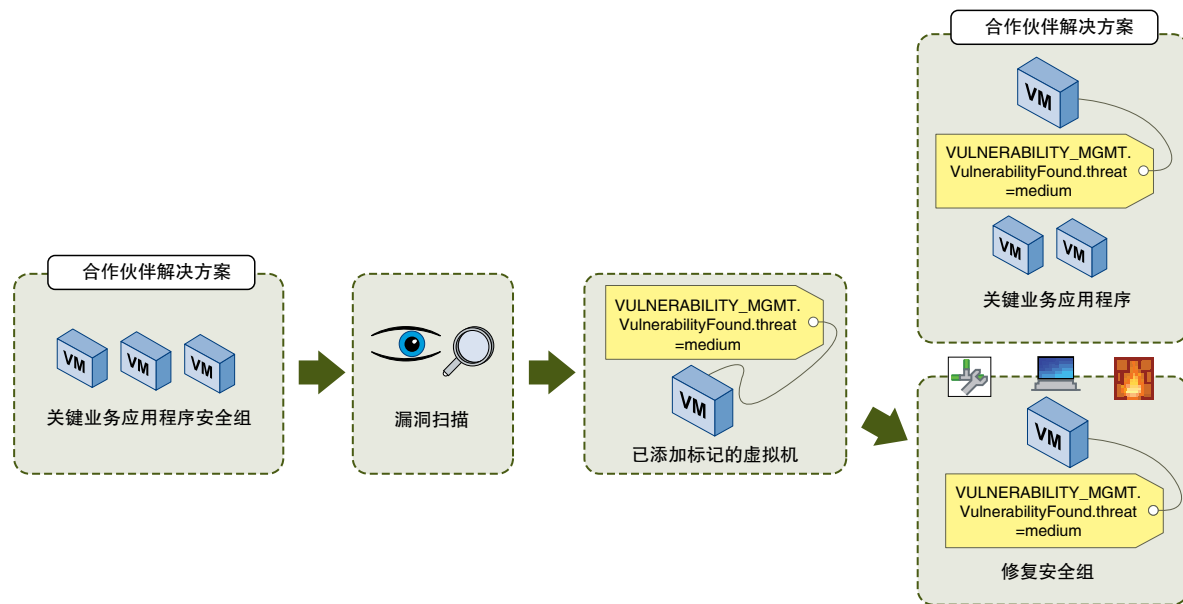


现在，将 `InitStatePolicy` 映射到 `AssetGroup` 以保护您的环境中的所有关键业务应用程序。还要将 `RemPolicy` 映射到 `RemGroup` 以保护易受攻击的虚拟机。

启动漏洞扫描后，将扫描 `AssetGroup` 中的所有虚拟机。如果扫描发现存在漏洞的虚拟机，则会将 `VULNERABILITY_MGMT.VulnerabilityFound.threat=medium` 标记应用于该虚拟机。

服务编排会立即将已标记的该虚拟机添加到 `RemGroup`，其中网络 IPS 解决方案已准备就绪，可保护该易受攻击的虚拟机。

图 17-2. 运行中的服务编排



现在，本主题将指导您完成使用服务编排提供的安全服务所需的步骤。

### 1 在服务编排中创建安全组

可以在 **NSX Manager** 级别创建安全组。

### 2 创建安全策略

安全策略是可以应用于安全组的一组 **Guest Introspection**、防火墙和网络自检服务。安全策略的显示顺序由与此策略相关联的权重决定。默认情况下，新策略分配有最高权重，因此位于表的顶部。但您可以修改建议的默认权重，以更改变分配给新策略的顺序。

### 3 将安全策略应用于安全组

您可以将安全策略应用到安全组，以保护您的虚拟桌面、关键业务应用程序以及两者之间的连接。您还可以查看未应用的服务的列表以及无法应用的原因。

## 在服务编排中创建安全组

可以在 **NSX Manager** 级别创建安全组。

### 步骤

#### 1 登录到 vSphere Web Client。

- 2 单击**网络和安全 (Networking & Security)**，然后单击**服务编排 (Service Composer)**。
- 3 单击**安全组**选项卡，然后单击**添加安全组**图标。
- 4 键入安全组的名称和描述，然后单击**下一步**。
- 5 在“动态成员资格”页面上，定义对象要添加到所创建安全组所需具备的条件。

例如，您可以加入一个条件，将使用指定安全标记（例如 **AntiVirus.virusFound**）进行标记的所有成员添加到安全组中。安全标记区分大小写。

**注** 如果通过应用了特定安全标记的虚拟机来定义安全组，则可以创建动态或条件工作流。该标记应用于虚拟机时，该虚拟机将自动添加到相应安全组中。

或者，可以将所有包含名称 **w2008** 的虚拟机以及位于逻辑交换机 **global\_wire** 中的虚拟机添加到安全组中。

- 6 单击**下一步**。
- 7 在“选择要包括的对象”页面上，从下拉列表中选择对象类型。
- 8 双击要添加到包括列表中的对象。可以在安全组中包括以下对象。
  - 其他安全组（可以嵌入正在创建的安全组）。
  - 群集
  - 逻辑交换机
  - 网络
  - 虚拟应用程序
  - 数据中心
  - IP 集
  - AD 组

**注** NSX 安全组的 AD 配置不同于 vSphere SSO 的 AD 配置。NSX AD 组配置用于访问客户机虚拟机的最终用户，而 vSphere SSO 的 AD 配置适用于使用 vSphere 和 NSX 的管理员。

- MAC 集
- 安全标记
- 虚拟网卡

- 虚拟机
- 资源池
- 分布式虚拟端口组

无论此处选定的对象是否满足动态条件，都将始终包含在安全组中。

将资源添加到安全组时，将自动添加所有关联的资源。例如，选择虚拟机后，关联的虚拟网卡将自动添加到安全组中。

## 9 单击下一步，然后双击要从安全组中排除的对象。

此处选定的对象始终都将从安全组中排除，即使这些对象满足动态条件或者已在包括列表中选定时亦如此。

## 10 单击完成。

将按下列方式确定安全组的成员资格：

{表达式结果（来自第 5 步）+ 包括（在第 8 步指定} - 排除（在第 9 步指定）

这表示包括项先添加到表达式结果中。然后，将从组合结果中减去排除项。

## 创建安全策略


安全策略是可以应用于安全组的一组 **Guest Introspection**、防火墙和网络自检服务。安全策略的显示顺序由与此策略相关联的权重决定。默认情况下，新策略分配有最高权重，因此位于表的顶部。但您可以修改建议的默认权重，以更改分配给新策略的顺序。

### 前提条件

请确保：

- 安装了所需的 VMware 内置服务（例如分布式防火墙、数据安全和 Guest Introspection）。
- 已向 NSX Manager 注册了所需的合作伙伴服务。
- 为服务编排防火墙规则设置了所需的默认应用对象值。请参见[编辑服务编排防火墙应用对象设置](#)。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**服务编排 (Service Composer)**。
- 3 单击**安全策略**选项卡。
- 4 单击**创建安全策略** () 图标。
- 5 在“添加安全策略”对话框中，键入安全策略的名称。
- 6 键入安全策略的描述。

NSX 会向策略分配默认权重（最高权重 + 1000）。例如，如果现有策略中的最高权重为 1200，则分配给新策略的权重为 2200。

将根据安全策略的权重来应用安全策略 - 权重较高的策略优先于权重较低的策略。

- 7 如果您希望所创建的策略接收来自其他安全策略的服务，则选择**从指定策略继承安全策略**。选择父策略。新策略将继承来自父策略的所有服务。

8 单击**下一步**。

- 9 在“Guest Introspection 服务”页面中，单击**添加 Guest Introspection 服务 (+)** 图标。

a 在“添加 Guest Introspection 服务”对话框中，键入服务的名称和描述。

b 指定要应用服务还是阻止服务。

继承安全策略后，可以选择阻止来自父策略的服务。

如果应用服务，必须选择服务和服务配置文件。如果阻止服务，必须选择要阻止的服务的类型。

c 如果选择阻止服务，则要选择服务类型。

如果选择数据安全，则必须具有合适的数据安全策略。请参见第 19 章，[数据安全](#)。

d 如果选择应用 Guest Introspection 服务，将选择服务名称。

将显示所选服务的默认服务配置文件，其中包括关联的供应商模板所支持的服务功能类型的相关信息。

e 在**状态**中，指定要启用还是禁用选定的 Guest Introspection 服务。

您可以添加 Guest Introspection 服务作为要在稍后启用的服务的占位符。此操作在需要按需应用服务的情况下尤其有用（例如，新应用程序）。

f 选择是否要强制执行 Guest Introspection 服务（即，不能覆盖此服务）。如果所选服务配置文件支持多个服务功能类型，则其默认设置为**强制**，且无法更改。

如果在安全策略中强制执行 Guest Introspection 服务，则继承此安全策略的其他策略将要求在应用其他子策略之前应用此策略。如果未强制执行此服务，则继承选择会在应用子策略之后添加父策略。

g 单击**确定**。

可按照上述步骤操作添加更多 Guest Introspection 服务。可通过服务表上方的图标来管理 Guest Introspection 服务。

可以在该页面上导出或复制服务，方法是单击位于“Guest Introspection 服务”页面右下方的  图标。

10 单击**下一步**。

- 11 在“防火墙”页面上，单击**添加防火墙规则 (+)** 图标。

可以在此处为将应用此安全策略的安全组定义防火墙规则。

a 键入所添加的防火墙规则的名称和描述。

b 选择**允许**或**阻止**以指示规则需要允许还是阻止流向选定目标的流量。

c 为该规则选择源。默认情况下，此规则应用于来自应用此策略的安全组的流量。要更改默认源，请单击**更改**，然后选择合适的安全组。

- d 为该规则选择目标。

---

**注** “源”或“目标”（或两者）必须是应用此策略的安全组。

---


假设您使用默认源创建规则，则将“目标”指定为“工资单”，然后选择**取消目标**。然后将此安全策略应用到“工程部”安全组。此操作将使“工程部”能够访问除“工资单”服务器以外的任何位置。

- e 选择将应用此规则的服务和/或服务组。
- f 选择**已启用**或**已禁用**，以指定规则状态。
- g 选择**日志**以记录与此规则相匹配的会话。

启用日志记录功能可能会影响性能。

- h 单击**确定**。

可按照上述步骤操作添加更多防火墙规则。可通过防火墙表上方的图标来管理防火墙规则。

可以导出或复制此页面上的规则，方法是单击位于“防火墙”页面右下方的  图标。

您在此处添加的防火墙规则将显示在“防火墙”表中。VMware 建议您不要编辑防火墙表中的服务编排规则。如果在进行紧急故障排除时必须编辑，则必须从“安全策略”选项卡的**操作**菜单中选择**同步防火墙规则**，将服务编排规则与防火墙规则重新同步。


## 12 单击下一步。

“网络自检服务”页面将显示已与您的 VMware 虚拟环境相集成的 NetX 服务。

## 13 单击**添加网络自检服务 (+)**图标。

- a 在“添加网络自检服务”对话框中，键入所添加的服务的名称和描述。
- b 选择是否重定向到服务。
- c 选择服务名称和配置文件。
- d 选择源和目标
- e 选择要添加的网络服务。
- f 选择是启用还是禁用服务。
- g 选择“日志”以记录与此规则相匹配的会话。
- h 单击**确定**。

可按照上述步骤操作添加更多网络自检服务。可通过服务表上方的图标来管理网络自检服务。

可以在该页面上导出或复制服务，方法是单击位于“网络自检服务”页面右下方的  图标。

---

**注** 为服务编排策略中使用的服务配置文件手动创建的绑定将被覆盖。

---

## 14 单击完成。

安全策略添加到策略表中。可以单击策略名称并选择相应的选项卡，以查看与该策略关联的服务摘要、查看服务错误或编辑服务。

### 后续步骤

将安全策略映射到安全组。

## 编辑服务编排防火墙应用对象设置

您可以将通过服务编排创建的所有防火墙规则的应用对象设置设为“分布式防火墙”或“策略的安全组”。默认情况下，应用对象设置为“分布式防火墙”。

在服务编排防火墙规则将应用对象设置设为“分布式防火墙”时，这些规则将应用于安装了分布式防火墙的所有群集。如果将防火墙规则设置为应用于策略的安全组，您可以对防火墙规则进行更精细的控制，但可能需要使用多个安全策略或防火墙规则以获得所需的结果。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，单击**服务编排 (Service Composer)**，然后单击**安全策略 (Security Policies)**选项卡。
- 3 单击**操作 (Actions) > 编辑防火墙策略设置 (Edit Firewall Policy Settings)**。选择默认“应用对象”设置，然后单击“确定”。

选项	说明
分布式防火墙	将防火墙规则应用于安装了分布式防火墙的所有群集。
策略的安全组	将防火墙规则应用于应用了安全策略的安全组。

也可以通过 API 查看和更改默认“应用对象”设置。请参见 [NSX API 指南](#)。

### 示例：应用对象行为

在该示例场景中，默认防火墙规则操作设置为阻止。您具有两个包含虚拟机的安全组：**web-servers** 和 **app-servers**。您创建包含以下防火墙规则的安全策略 **allow-ssh-from-web**，然后将其应用于安全组 **app-servers**。

- 名称：allow-ssh-from-web
- 源：web-servers
- 目标：策略的安全组
- 服务：ssh
- 操作：允许

如果防火墙规则应用于分布式防火墙，您可以通过 **ssh** 从安全组 **web-servers** 中的虚拟机访问安全组 **app-servers** 中的虚拟机。

如果防火墙规则应用于策略的安全组，您无法通过 `ssh` 进行访问，因为阻止流量到达 `app-servers`。您需要创建额外的安全策略以允许通过 `ssh` 访问 `app-servers`，并将该策略应用于安全组 `web-servers`。

- 名称: `allow-ssh-to-app`
- 源: 策略的安全组
- 目标: `app-servers`
- 服务: `ssh`
- 操作: 允许

## 将安全策略应用于安全组

您可以将安全策略应用到安全组，以保护您的虚拟桌面、关键业务应用程序以及两者之间的连接。您还可以查看未应用的服务的列表以及无法应用的原因。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全 (Networking & Security)**，然后单击 **服务编排 (Service Composer)**。
- 3 单击 **安全策略 (Security Policy)** 选项卡。
- 4 选择安全策略，然后单击 **应用安全策略 (Apply Security Policy)** ( 图标)。
- 5 选择您要对其应用该策略的安全组。

如果选择应用了特定安全标记的虚拟机所定义的一个安全组，则可以创建动态或条件工作流。该标记应用于虚拟机时，该虚拟机将自动添加到相应安全组中。

与该策略关联的网络自检规则和 **Endpoint** 规则对包含 **IPSet** 和/或 **MacSet** 成员的安全组无效。

- 6 单击 **预览服务状态 (Preview Service Status)** 图标可查看无法应用于选定安全组的服务以及失败原因。  
例如，安全组可能包括属于尚未安装策略服务之一的群集的虚拟机。您必须在相应的群集上安装该服务，以使安全策略按预期生效。
- 7 单击 **确定 (OK)**。

## 服务编排的图形视图

服务编排提供了一个画布视图，其中显示所选 **NSX Manager** 中的所有安全组。此视图还显示一些详细信息，例如每个安全组的成员以及应用的安全策略。

本主题通过演示特定配置的系统介绍服务编排，以画布视图直观显示安全组和安全组级别之间的大致映射关系。

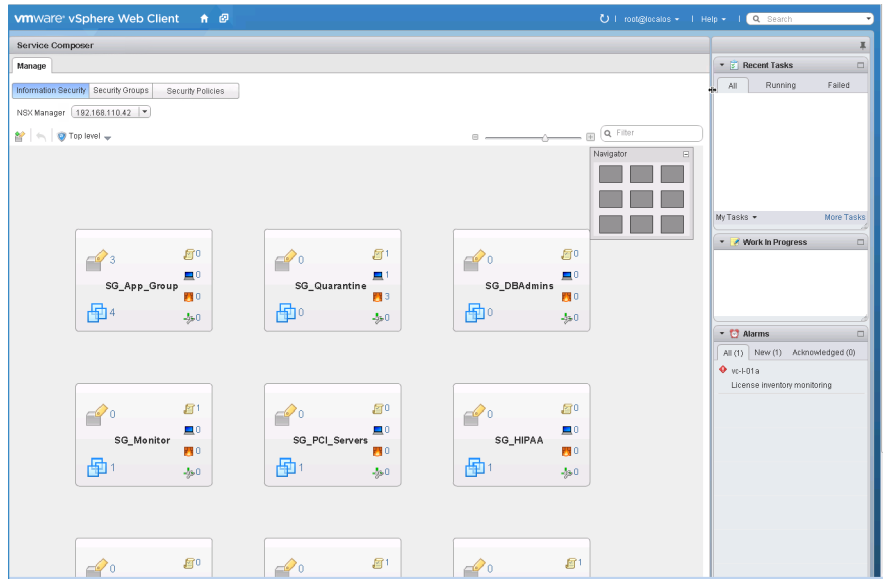
### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全 (Networking & Security)**，然后单击 **服务编排 (Service Composer)**。

### 3 单击画布选项卡。

所选 NSX Manager 中的所有安全组（不包含在其他安全组中）都将与其应用的策略一起显示。**NSX Manager** 下拉菜单中列出了当前登录的用户在其上分配有角色的所有 NSX Manager。

图 17-3. 服务编排画布顶层视图



画布中的每个矩形框都代表一个安全组，该矩形框中的图标代表安全组成员以及映射到该安全组的安全策略的详细信息。


图 17-4. 安全组



每个图标旁边的数字表示实例数目 - 例如， 1 表示有 1 个安全策略映射到了该安全组。

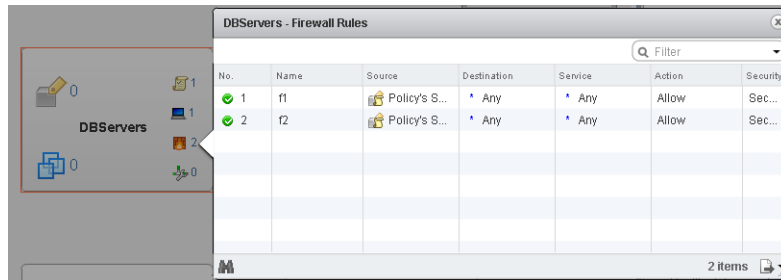
图标	单击显示
	嵌套在主安全组中的安全组。
	当前包含在主安全组以及嵌套安全组中的虚拟机。单击“错误”选项卡可查看出现服务错误的虚拟机。
	映射到安全组的有效安全策略。 <ul style="list-style-type: none"> <li>通过单击<b>创建安全策略</b> () 图标，您可以创建新的安全策略。新创建的安全策略对象自动映射到安全组。</li> <li>通过单击<b>应用安全策略</b> () 图标将其他安全策略映射到安全组。</li> </ul>



图标	单击显示
	与映射到安全组的安全策略相关联的有效 <b>Endpoint</b> 服务。假设有两个策略应用到一个安全组，并且每个策略都配置了相同类别的 <b>Endpoint</b> 服务。此示例中的有效服务计数为 1（因为优先级较低的第二个服务被覆盖）。 <b>Endpoint</b> 服务故障由警示图标指示（如果有）。单击此图标可显示错误。
	与映射到安全组的安全策略相关联的有效防火墙规则。 服务故障由警示图标指示（如果有）。单击此图标可显示错误。
	与映射到安全组的安全策略相关联的有效网络自检服务。 服务故障由警示图标指示（如果有）。单击此图标可显示错误。

单击图标可显示带有相应详细信息的对话框。

图 17-5. 单击安全组中的图标时显示的详细信息



您可以根据名称搜索安全组。例如，如果在画布视图的右上角的搜索字段中键入 **PCI**，则仅显示名称中包含 **PCI** 的安全组。

要查看安全组层次结构，请单击窗口左上方的**顶级** (▼) 图标，然后选择要显示的安全组。如果安全组包含嵌套的安全组，请单击 ► 以显示嵌套的组。顶部一栏中将显示父安全组的名称，此栏中的图标显示应用于该父组的安全策略、**Endpoint** 服务、防火墙服务和网络自检服务的总数。您可以向上导航回到顶层，方法是单击窗口左上方的**转至上一级** (↶) 图标。

通过移动窗口右上角的缩放滑块，您可以顺利地放大和缩小画布视图。“导航器”框显示整个画布的缩小视图。如果画布大小远远超出适合您的屏幕的大小，则将在实际可视的区域周围显示一个框，您可以移动此框来更改所显示的画布部分。

## 后续步骤

既然我们已了解安全组和安全策略间映射的工作原理，就可以开始创建安全策略来定义您要应用于安全组的安全服务。

## 将安全组映射到安全策略

可以将选定的安全组映射到某个安全策略。

### 步骤

- 1 选择您要应用于该安全组的安全策略。
- 2 要创建新策略，请选择“新建安全组”。

请参见 [创建安全策略](#)。

### 3 单击保存 (Save)。

## 使用安全标记

您可以查看应用于虚拟机的安全标记或创建用户定义的安全标记。

### 查看应用的安全标记

您可以查看应用到环境中虚拟机的安全标记。

#### 前提条件

必须已运行过数据安全扫描或防病毒扫描，并且在相应的虚拟机中应用了标记。

---

**注** 有关第三方解决方案所应用的标记的详细信息，请参见第三方解决方案文档。

---

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Manager (NSX Managers)**。
- 3 在**名称 (Name)**列中单击 NSX Manager，然后单击**管理 (Manage)**选项卡。
- 4 单击**安全标记**选项卡。

此时将显示您环境中应用的标记的列表，以及有关已应用这些标记的虚拟机的详细信息。如果您计划添加安全组以包括带有特定标记的虚拟机，请记下准确的标记名称。

- 5 单击**虚拟机计数**列中的数字以查看已应用该行中的标记的虚拟机。

### 添加安全标记

可以手动添加安全标记并将其应用到虚拟机。在以下情况中，此操作特别有用：您在环境中使用非 NETX 解决方案，因此无法向 NSX Manager 注册解决方案标记。

#### 前提条件

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Manager (NSX Managers)**。
- 3 在**名称 (Name)**列中单击 NSX Manager，然后单击**管理 (Manage)**选项卡。
- 4 单击**安全标记 (Security Tags)**选项卡。
- 5 单击**新建安全标记 (New Security Tag)** (  ) 图标。
- 6 键入标记的名称和描述，然后单击**确定 (OK)**。

## 分配安全标记

除了通过基于动态成员资格的安全标记创建条件 workflows 外，还可以手动将安全标记分配给虚拟机。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Manager (NSX Managers)**。
- 3 在**名称 (Name)**列中单击 NSX Manager，然后单击**管理 (Manage)**选项卡。
- 4 单击**安全标记 (Security Tags)**选项卡。
- 5 选择一个安全标记，然后单击**分配安全标记 (Assign Security Tag)** () 图标。
- 6 选择一个或多个虚拟机，然后单击**确定 (OK)**。

## 编辑安全标记

可以编辑用户定义的安全标记。如果安全组基于您正在编辑的标记，则对该标记进行更改可能会影响安全组的成员资格。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Manager (NSX Managers)**。
- 3 在**名称 (Name)**列中单击 NSX Manager，然后单击**管理 (Manage)**选项卡。
- 4 单击**安全标记 (Security Tags)**选项卡。
- 5 选择安全标记并单击**编辑安全标记 (Edit Security Tag)** () 图标。
- 6 进行相应更改，然后单击**确定 (OK)**。

## 删除安全标记

您可以删除用户定义的安全标记。如果安全组基于您正在删除的标记，则对该标记进行更改可能会影响安全组的成员资格。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Manager (NSX Managers)**。
- 3 在**名称 (Name)**列中单击 NSX Manager，然后单击**管理 (Manage)**选项卡。
- 4 单击**安全标记 (Security Tags)**选项卡。
- 5 选择安全标记，然后单击**删除安全标记 (Delete Security Tag)** () 图标。

## 查看有效服务

可以查看安全策略对象或虚拟机的有效服务。

### 查看安全策略中的有效服务

可以查看安全策略上有效的服务，包括继承自父策略的服务。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**服务编排 (Service Composer)**。
- 3 单击**安全策略 (Security Policies)**选项卡。
- 4 单击**名称 (Name)**列中的一个安全策略。
- 5 确保您处于**管理 (Manage) > 信息安全 (Information Security)**选项卡中。

这三个选项卡（**Endpoint 服务 (Endpoint Services)**、**防火墙 (Firewall)**和**网络自检服务 (Network Introspection Services)**）中的每个选项卡都会显示安全策略的相应服务。

无效的服务将变灰。**已覆盖 (Overridden)**列显示实际应用于安全策略的服务，而**继承自 (Inherited from)**列显示从其继承服务的安全策略。

### 查看安全策略的服务故障

可以查看与安全策略（此安全策略无法应用到与该策略映射的安全组）相关联的服务。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**服务编排 (Service Composer)**。
- 3 单击**安全策略 (Security Policies)**选项卡。
- 4 单击**名称 (Name)**列中的一个安全策略。
- 5 确保您位于**监控 (Monitor) > 服务错误 (Service Errors)**选项卡中。

单击**状态 (Status)**列中的链接可进入“服务部署”页面，可在其中更正服务错误。

### 查看虚拟机上的有效服务

可以查看虚拟机上的有效服务。如果对虚拟机应用了多个安全策略（例如虚拟机属于多个有对应策略的安全组），则该视图将列出所有这些策略的所有有效服务（按照应用策略的顺序）。服务状态列显示每项服务的状态。

#### 步骤

- 1 登录到 vSphere Web Client。

- 2 单击 **vCenter**，然后单击**虚拟机 (Virtual Machines)**。
- 3 单击**名称 (Name)**列中的一个虚拟机。
- 4 确保您位于**监控 (Monitor) > 服务编排 (Service Composer)**选项卡中。

## 使用安全策略

安全策略是一组网络和安全服务。

以下网络和安全服务可以组成一个安全策略：




- Endpoint 服务 - 数据安全、防病毒和漏洞管理
- 分布式防火墙规则
- 网络自检服务 - 网络 IPS 和网络取证

## 管理安全策略优先级

可以根据安全策略的权重应用安全策略 - 安全策略的权重越高，其优先级越高。在表中上移或下移策略时，其权重也相应调整。

可能会对虚拟机应用多个安全策略，原因是包含该虚拟机的安全组与多个策略相关联，或者该虚拟机属于与不同策略相关联的多个安全组的一部分。如果通过每个策略分组的服务相冲突，策略的权重将决定要对虚拟机应用的服务。例如，假设策略 1 阻止 Internet 访问，其权重值为 1000，而策略 2 允许 Internet 访问，其权重值为 2000。在此特定情况下，策略 2 的权重较高，因此将允许虚拟机执行 Internet 访问。

### 步骤


- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**服务编排 (Service Composer)**。
- 3 单击**安全策略 (Security Policies)**选项卡。
- 4 单击**管理优先级 (Manage Precedence)** ( 图标。
- 5 在“管理优先级”对话框中，选择要更改优先级的安全策略，然后单击**上移 (Move Up)** () 或**下移 (Move Down)** () 图标。
- 6 单击**确定 (OK)**。

## 编辑安全策略

您可以编辑安全策略的名称或描述，以及关联的服务和规则。

### 步骤


- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**服务编排 (Service Composer)**。
- 3 单击**安全策略 (Security Policies)**选项卡。

- 4 选择要编辑的安全策略，然后单击**编辑安全策略 (Edit Security Policy)** () 图标。
- 5 在“编辑安全策略”对话框中，进行适当的更改，然后单击**完成 (Finish)**。

## 删除安全策略

您可以删除安全策略。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**服务编排 (Service Composer)**。
- 3 单击**安全策略 (Security Policies)**选项卡。
- 4 选择要删除的安全策略，然后单击**删除安全策略 (Delete Security Policy)** () 图标。

## 编辑安全组

可以编辑安全组。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**服务编排 (Service Composer)**。
- 3 单击**安全组**选项卡。
- 4 选择要编辑的安全组，然后单击**编辑安全组**图标。
- 5 进行相应更改，然后单击**确定**。

## 服务编排场景

此部分介绍了服务编排的一些假设场景。在每个用例中，假设已创建安全管理员角色并分配给了管理员。

### 隔离受感染的计算机的场景

服务编排可以利用第三方防病毒解决方案识别出网络中受感染的系统，并将这些系统隔离，以防止病毒进一步爆发。

我们的示例场景说明如何为您的桌面提供端到端保护。

图 17-6. 配置服务编排

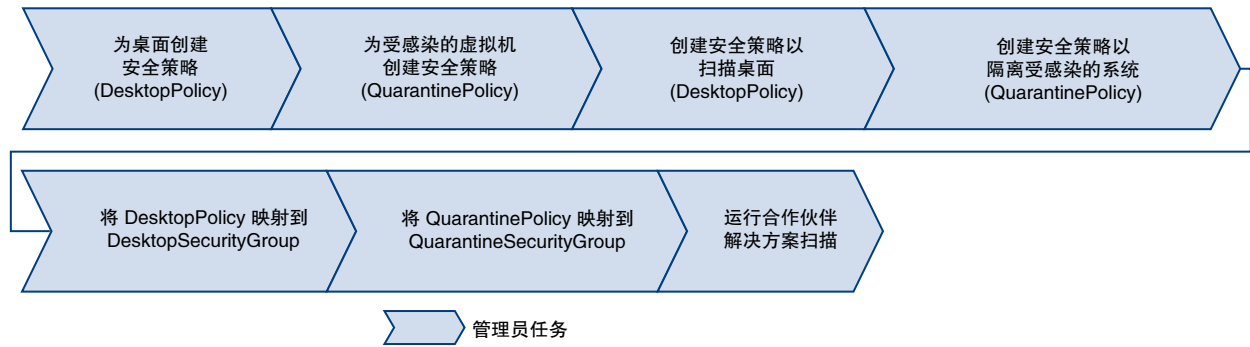
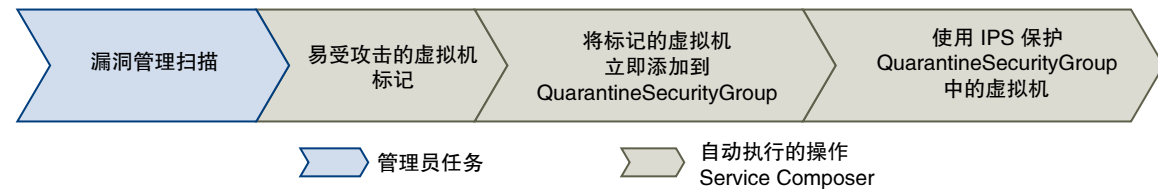


图 17-7. 服务编排条件 workflow



#### 前提条件

我们发现，Symantec 用 **AntiVirus.virusFound** 标记受感染的虚拟机。

#### 步骤

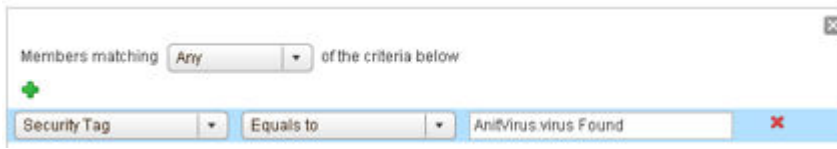
- 1 安装、注册和部署 Symantec Antimalware 解决方案。
- 2 为桌面创建安全策略。
  - a 单击**安全策略 (Security Policies)**选项卡，然后单击**添加安全策略 (Add Security Policy)**图标。
  - b 在**名称 (Name)**中，键入 **DesktopPolicy**。
  - c 在**描述 (Description)**中，键入 **Antivirus scan for all desktops**。
  - d 将权重值改为 51000。将策略优先级设置为非常高，以确保优先于其他所有策略强制实施。
  - e 单击**下一步 (Next)**。
  - f 在“添加 Endpoint 服务”页面上，单击 **+** 并填入以下值。

选项	值
操作 (Action)	请勿修改默认值
服务类型 (Service Type)	防病毒
服务名称 (Service Name)	Symantec Antimalware
服务配置 (Service Configuration)	银级
状态 (State)	请勿修改默认值
强制实施 (Enforce)	请勿修改默认值
名称 (Name)	Desktop AV
描述 (Description)	要在所有桌面应用的强制策略

- g 单击**确定 (OK)**。
  - h 请勿添加任何防火墙或网络自检服务，然后单击**完成 (Finish)**。
- 3 为受感染的虚拟机创建安全策略。
- a 单击**安全策略 (Security Policies)**选项卡，然后单击**添加安全策略 (Add Security Policy)**图标。
  - b 在“名称”中，键入 **QuarantinePolicy**。
  - c 在“描述”中，键入 **Policy to be applied to all infected systems**。
  - d 不要更改默认权重。
  - e 单击**下一步 (Next)**。
  - f 在“添加 Endpoint 服务”页面，不要执行任何操作，单击**下一步 (Next)**。
  - g 在“防火墙”中，添加三个规则，其中一个规则用于阻止所有出站流量，第二个规则用于阻止组的所有流量，最后一个规则仅允许来自修复工具的入站流量。
  - h 不要添加任何网络自检服务，单击**完成 (Finish)**。
- 4 将 **QuarantinePolicy** 移至安全策略表的顶部，以确保该策略在所有其他策略之前强制执行。
- a 单击**管理优先级 (Manage Priority)**图标。
  - b 选择 **QuarantinePolicy** 并单击**上移 (Move Up)**图标。
- 5 为您环境中的所有桌面创建一个安全组。
- a 登录到 vSphere Web Client。
  - b 单击**网络和安全 (Networking & Security)**，然后单击**服务编排 (Service Composer)**。
  - c 单击**安全组 (Security Groups)**选项卡，然后单击**添加安全组 (Add Security Group)**图标。
  - d 在“名称”中，键入 **DesktopSecurityGroup**。
  - e 在“描述”中，键入 **All desktops**。
  - f 在接下来的两个页面上单击**下一步 (Next)**。
  - g 查看“即将完成”页面上的选择，然后单击**完成 (Finish)**。
- 6 创建用来放置受感染的虚拟机的隔离安全组。
- a 单击**安全组 (Security Groups)**选项卡，然后单击**添加安全组 (Add Security Group)**图标。
  - b 在**名称 (Name)**中，键入 **QuarantineSecurityGroup**。
  - c 在**描述 (Description)**中，键入 **Dynamic group membership based on infected VMs identified by the antivirus scan**。



- d 在“定义成员资格条件”页面上，单击  并添加以下条件。



- e 在“选择要包括的对象”或“选择要排除的对象”页面上，不要执行任何操作，并单击下一步 (Next)。
- f 查看“即将完成”页面上的选择，然后单击完成 (Finish)。

## 7 将 DesktopPolicy 策略映射到 DesktopSecurityGroup 安全组。

- a 在“安全策略”选项卡上，确保选择 DesktopPolicy 策略。
- b 单击应用安全策略 (Apply Security Policy) () 图标，并选择 SG\_Desktops 组。
- c 单击确定 (OK)。

此映射可确保在触发防病毒扫描时扫描所有桌面（包含在 DesktopSecurityGroup 中）。

## 8 导航到画布视图以确认 QuarantineSecurityGroup 不包含任何虚拟机。

- a 单击信息安全 (Information Security) 选项卡。
- b

确认组中没有任何虚拟机 ()

## 9 将 QuarantinePolicy 映射到 QuarantineSecurityGroup。

此映射可确保没有任何流量流向受感染的系统。

## 10 从 Symantec Antimalware 控制台触发网络扫描。

扫描将发现受感染的虚拟机，并使用安全标记 AntiVirus.virusFound 对这些虚拟机进行标记。这些已标记的虚拟机将立即添加到 QuarantineSecurityGroup 中。QuarantinePolicy 不允许流量流入/流出受感染的系统。

# 备份安全配置

服务编排可高效备份安全配置并在以后按需还原。

### 步骤

- 1 安装、注册并部署 Rapid 7 Vulnerability Management 解决方案。
- 2 为共享点应用程序的第一层（Web 服务器）创建安全组。
  - a 登录到 vSphere Web Client。
  - b 单击网络和安全，然后单击服务编排。
  - c 单击安全组选项卡，然后单击添加安全组图标。
  - d 在名称中，键入 SG\_Web。

- e 在**描述**中，键入 **Security group for application tier**。
  - f 请勿在“定义成员资格条件”页面上执行任何操作，然后单击**下一步**。
  - g 在“选择要包括的对象”页面上，选择 **Web 服务器虚拟机**。
  - h 请勿在“选择要排除的对象”页面上执行任何操作，然后单击**下一步**。
  - i 查看“即将完成”页面上的选择，然后单击**完成**。
- 3 现在，为您的数据库和共享点服务器各创建一个安全组，并分别将其命名为 **SG\_Database** 和 **SG\_Server\_SharePoint**。在每组中包括合适的对象。
  - 4 为您的应用程序层创建一个顶层安全组，并将其命名为 **SG\_App\_Group**。将 **SG\_Web**、**SG\_Database** 和 **SG\_Server\_SharePoint** 添加到该组。
  - 5 为您的 **Web 服务器** 创建安全策略。
    - a 单击“安全策略”选项卡，然后单击“添加安全策略”图标。
    - b 在“名称”中，键入 **SP\_App**。
    - c 在“描述”中，键入 **SP for application web servers**。
    - d 将权重值改为 **50000**。将策略优先级设置为非常高的值，以确保优先于大多数其他策略（隔离为例外情况）强制实施。
    - e 单击“下一步”。
    - f 在“Endpoint 服务”页面上，单击  并填写以下值。

选项	值
操作	请勿修改默认值
服务类型	Vulnerability Management
服务名称	Rapid 7
服务配置	银级
状态	请勿修改默认值
强制实施	请勿修改默认值

- g 请勿添加任何防火墙或网络自检服务，然后单击**完成**。
- 6 将 **SP\_App** 映射到 **SG\_App\_Group**。
  - 7 导航到画布视图以确认已将 **SP\_App** 映射到 **SG\_App\_Group**。
    - a 单击“信息安全”选项卡。
    - b 单击  图标旁边的数字可看到 **SP\_App** 已映射。
  - 8 导出 **SP\_App** 策略。
    - a 单击“安全策略”选项卡，然后单击**导出 Blueprint** () 图标。
    - b 在**名称**中，键入 **Template\_ App\_**，在**前缀**中，键入 **FromAppArchitect**。

- c 单击“下一步”。
- d 选择 **SP\_App** 策略，然后单击“下一步”。
- e 检查做出的选择，然后单击“完成”。
- f 在计算机上选择导出文件下载到的目录，然后单击“保存”。

此时将导出安全策略以及已应用此策略的所有安全组（在我们的示例中，即应用程序安全组以及嵌套其中的三个安全组）。

**9** 要演示导出策略的工作原理，请删除 **SP\_App** 策略。

**10** 现在，我们将还原在步骤 7 中导出的 **Template\_App\_DevTest** 策略。

- a 单击**操作**，然后单击**导入服务配置**图标。
- b 在桌面上选择 **FromAppArchitect\_Template\_App** 文件（在步骤 7 中保存的文件）。
- c 单击**下一步**。
- d “即将完成”页面将显示要导入的安全策略及其关联对象（应用这些安全策略的安全组，以及 **Endpoint** 服务、防火墙规则和网络自检服务）。
- e 单击**完成**。

配置和关联的对象将被导入 **vCenter** 清单，并且可在画布视图中查看。

# Guest Introspection

**Guest Introspection** 可将防病毒和防恶意软件代理处理任务卸载到 VMware 合作伙伴所提供的专用安全虚拟设备上。由于安全虚拟设备（与客户机虚拟机不同）不会脱机，因此可以不断地更新防病毒特征码，从而为主机上的虚拟机提供持续保护。另外，还可以在新虚拟机（或处于脱机状态的现有虚拟机）联机时，立即使用最新的防病毒特征码来保护这些虚拟机。

**Guest Introspection** 运行状况将通过 vCenter Server 控制台中红色显示的警报进行体现。此外，还可通过查看事件日志来收集更多状况信息。

---

**重要** 必须针对 **Guest Introspection** 安全正确配置 vCenter Server:

- 并非所有客户机操作系统都受 **Guest Introspection** 支持。使用不支持的操作系统的虚拟机不受安全解决方案保护。
  - 包含受保护虚拟机的资源池中的所有主机必须针对 **Guest Introspection** 设置好，以确保虚拟机通过 vMotion 从资源池中的一台 ESX 主机迁移到另一台时仍可受保护。
- 

本章讨论了以下主题：

- [安装 Guest Introspection](#)
- [查看 Guest Introspection 状态](#)
- [Guest Introspection 警报](#)
- [Guest Introspection 事件](#)
- [Guest Introspection 审核消息](#)
- [收集 Guest Introspection 故障排除数据](#)
- [卸载 Guest Introspection 模块](#)

## 安装 Guest Introspection

安装 **Guest Introspection** 会在群集中的每个主机上自动安装新的 VIB 和服务虚拟机。NSX 数据安全、活动监控和多个第三方安全解决方案需要 **Guest Introspection**。

对于无状态主机上的自动部署设置，您必须在 ESXi 主机重新引导后人工重新启动 VMware NSX for vSphere 6.x Service Virtual Machines (SVM)。有关详细信息，请参见知识库文章 <http://kb.vmware.com/kb/2120649>。



**小心** 在 VMware NSX for vSphere 6.x 环境中，在迁移服务虚拟机 (SVM) (vMotion/SvMotion) 时，可能会出现以下症状：

- 服务虚拟机 (SVM) 为其提供数据的服务（工作负载虚拟机）中断
- ESXi 主机发生故障并显示紫色诊断屏幕，其中包含类似下面的回溯追踪：

```
@BlueScreen: #PF Exception 14 in world www:WorldName IP 0xffffffff addr 0x0
PTes:0xffffffff;0xffffffff;0x0;
0xffffffff: [0xffffffff]VmMemPin_DecCount@vmkernel#nover+0x1b
0xffffffff: [0xffffffff]VmMemPinUnpinPages@vmkernel#nover+0x65
0xffffffff: [0xffffffff]VmMemPin_ReleaseMainMemRange@vmkernel#nover+0x6
0xffffffff: [0xffffffff]P2MCache_ReleasePages@vmkernel#nover+0x2a
0xffffffff: [0xffffffff]DVFilterVmciUnmapGuestPage@com.vmware.vmkapi#v2_2_0_0+0x34
```

这是一个影响 VMware ESXi 5.5.x 和 6.x 主机的已知问题。要解决该问题，请不要将服务虚拟机 (SVM) (vMotion/SvMotion) 手动迁移到群集中的另一个 ESXi 主机。要将 SVM 迁移到另一个数据存储 (svMotion)，VMware 建议关闭 SVM 并将其迁移到另一个数据存储以执行冷迁移。

#### 前提条件

以下安装说明假定您拥有以下系统：

- 群集中每个主机上均安装了具有受支持版本的 vCenter Server 和 ESXi 的数据中心。
- 如果群集中的主机已从 vCenter Server 版本 5.0 升级到 5.5，则必须在这些主机上打开端口 80 和 443。
- 为 NSX 准备了群集中要安装 Guest Introspection 的主机。请参见 NSX 安装指南中的“为 NSX 准备主机群集”。不能将 Guest Introspection 安装在单独的主机上。如果使用 NSX 部署和管理 Guest Introspection 以仅提供防病毒卸载功能，您不需要为 NSX 准备主机，并且 NSX for vShield Endpoint 许可证不允许使用该功能。
- 已安装 NSX Manager 6.2 并且正在运行。
- 确保将运行 Guest Introspection 服务的 NSX Manager 和准备好的主机链接到相同的 NTP 服务器，且时间同步。无法完成此操作可能会导致防病毒服务无法保护虚拟机，但群集的状态将对 Guest Introspection 和任意第三方服务显示为绿色。


如果添加了 NTP 服务器，VMware 建议您重新部署 Guest Introspection 和任意第三方服务。

如果要将 IP 池中的某个 IP 地址分配给 NSX Guest Introspection 服务虚拟机，请先创建 IP 池，然后再安装 NSX Guest Introspection。请参见《NSX 管理指南》中的“使用 IP 池”。

vSphere Fault Tolerance 无法与 Guest Introspection 一起使用。

#### 步骤

- 1 在**安装 (Installation)**选项卡上，单击**服务部署 (Service Deployments)**。

- 2 单击**新建服务部署 (New Service Deployment)** ( ) 图标。
- 3 在“部署网络和安全服务”对话框中，选择 **Guest Introspection**。
- 4 在**指定调度 (Specify schedule)**（在该对话框的底部）中，选择**立即部署 (Deploy now)**以便在安装 Guest Introspection 后立即对其进行部署，或者选择部署日期和时间。
- 5 单击**下一步 (Next)**。
- 6 选择要安装 Guest Introspection 的数据中心和群集，然后单击**下一步 (Next)**。
- 7 在“选择存储和管理网络”页面上，选择要添加服务虚拟机存储器的数据存储，或者选择**已在主机上指定 (Specified on host)**。建议使用共享数据存储和网络而不是“已在主机上指定”，以便自动化部署工作流。

选定的数据存储在选定群集的所有主机上都必须可用。

如果选择了**已在主机上指定 (Specified on host)**，请对群集中的每个主机执行下列步骤。

- a 在 vSphere Web Client 主页上，单击 **vCenter**，然后单击**主机 (Hosts)**。
  - b 在**名称 (Name)**列中单击一个主机，然后单击**管理 (Manage)**选项卡。
  - c 单击**代理虚拟机设置 (Agent VM Settings)**，然后单击**编辑 (Edit)**。
  - d 选择数据存储，然后单击**确定 (OK)**。
- 8 选择用于承载管理接口的分布式虚拟端口组。如果数据存储设置为**已在主机上指定 (Specified on host)**，则网络必须也为**已在主机上指定 (Specified on host)**。

选定的端口组必须能够访问 NSX Manager 的端口组，并且在选定群集的所有主机上都可用。

如果选择了**已在主机上指定 (Specified on host)**，请按照第 7 步中的子步骤在主机上选择一个网络。将一个主机（或多个主机）添加到群集中时，必须先设置数据存储和网络，再将每个主机添加到群集中。

- 9 在“IP 分配”中，选择以下其中的一项：

选择	目的
DHCP	通过动态主机配置协议 (DHCP) 将 IP 地址分配给 NSX Guest Introspection 服务虚拟机。如果主机位于不同子网，请选择此选项。
IP 池	将选定 IP 池中的某个 IP 地址分配给 NSX Guest Introspection 服务虚拟机。

- 10 单击**下一步 (Next)**，然后在“即将完成”页面上单击**完成 (Finish)**。
- 11 监控该部署，直至**安装状态 (Installation Status)**列显示**成功 (Succeeded)**。
- 12 如果**安装状态 (Installation Status)**列显示**失败 (Failed)**，则单击“失败”旁边的图标。将显示所有部署错误。单击**解决 (Resolve)**修复这些错误。在某些情况下，解决这些错误时会显示其他错误。执行所需操作，然后重新单击**解决办法 (Resolve)**。

## 后续步骤

在客户机虚拟机上安装 VMware Tools。

## 在客户机虚拟机上安装 VMware Tools

VMware Tools 包含必须安装在要受保护的每台客户机虚拟机上的 NSX 瘦代理。在安装了安全解决方案的 ESX 主机上启动已安装 VMware Tools 的虚拟机后，所启动的虚拟机会自动得到保护。这意味着受保护的虚拟机在关机和重启后仍可以得到安全保护，当通过 vMotion 迁移到另一个安装了安全解决方案的 ESX 主机时也不例外。

### 前提条件

确保客户机虚拟机安装了 ESX 5.1 或更高版本以及支持的 Windows 版本。NSX Guest Introspection 支持以下 Windows 操作系统：

- Windows Vista（32 位）
- Windows 7（32/64 位）
- Windows XP SP3 及更高版本（32 位）
- Windows 2003 SP2 及更高版本（32/64 位）
- Windows 2003 R2（32/64 位）
- Windows 2008（32/64 位）
- Windows 2008 R2（64 位）
- Windows 8 (32/64) - vSphere 5.5 及更高版本
- Win2012 (64) - vSphere 5.5 及更高版本
- Windows 8.1 (32/64) - vSphere 5.5 Patch 2 及更高版本
- Win2012 R2 (64) - vSphere 5.5 Patch 2 及更高版本

### 步骤

- 1 按照“在 Windows 虚拟机中手动安装或升级 VMware Tools”过程进行操作  
[http://pubs.vmware.com/vsphere-55/topic/com.vmware.vsphere.vm\\_admin.doc/GUID-391BE4BF-89A9-4DC3-85E7-3D45F5124BC7.html](http://pubs.vmware.com/vsphere-55/topic/com.vmware.vsphere.vm_admin.doc/GUID-391BE4BF-89A9-4DC3-85E7-3D45F5124BC7.html)。
- 2 在第 7 步中选择自定义 (Custom) 安装后，展开 **VMCI 驱动程序 (VMCI Driver)** 部分，选择 **vShield 驱动程序 (vShield Drivers)**，然后选择 **将在本地硬盘上安装此功能 (This feature will be installed on the local hard drive)**。
- 3 按照此过程中的剩余步骤进行操作。

## 查看 Guest Introspection 状态

对 Guest Introspection 实例的监控包括检查来自各 Guest Introspection 组件的状态：安全虚拟机 (SVM)、ESX 主机所驻留的 Guest Introspection 模块以及受保护的虚拟机所驻留的瘦代理。

### 步骤

- 1 在 vSphere Web Client 中，单击 **vCenter**，然后单击 **数据中心 (Datacenters)**。

- 2 在**名称 (Name)**列中，单击某个数据中心。
- 3 单击**监控 (Monitor)**，然后单击 **Endpoint**。

Guest Introspection “运行状况和警报”页面会显示所选的数据中心下对象的运行状况以及活动警报。运行状况变化会在触发该变化的事件实际发生后的一分钟内反映。

## Guest Introspection 警报

警报用信号通知 vCenter Server 管理员存在需要特别注意的 Guest Introspection 事件。如果警报状态不再存在，这些警报便会自动取消。

vCenter Server 警报可在未安装自定义 vSphere 插件的情况下显示。请参见《vCenter Server 管理指南》了解有关事件和警报的信息。

注册为 vCenter Server 扩展组件后，NSX Manager 会定义规则，以便基于来自以下三个 Guest Introspection 组件的事件来创建和移除警报：SVM、Guest Introspection 模块和瘦代理。规则可进行自定义。有关如何为警报创建新的自定义规则的说明，请参见 vCenter Server 文档。在某些情况下，导致出现警报的可能原因有很多种。下文的表格列出了可能的原因以及修复问题所需采取的相应操作。

### 主机警报

主机警报由影响 Guest Introspection 模块的运行状态的事件生成。

表 18-1. 错误（标记为红色）

可能的原因	操作
Guest Introspection 模块已安装在主机上，但不再向 NSX Manager 报告状态。	<ol style="list-style-type: none"> <li>1 通过登录主机并键入命令 <code>/etc/init.d/vShield-Endpoint-Mux start</code> 确保 Guest Introspection 正在运行。</li> <li>2 确保网络配置正确，以便 Guest Introspection 可以连接到 NSX Manager。</li> <li>3 重新引导 NSX Manager。</li> </ol>

### SVM 警报

SVM 警报是由影响 SVM 运行状况的事件生成的。

表 18-2. 红色 SVM 警报

问题	操作
协议版本与 Guest Introspection 模块不匹配	确保 Guest Introspection 模块和 SVM 具有相互兼容的协议。
Guest Introspection 无法建立与 SVM 的连接	确保已打开 SVM 电源并正确配置了网络。
即使连接了客户机，SVM 也不会报告其状况。	内部错误。请联系您的 VMware 技术支持代表。

## Guest Introspection 事件

事件用于记录和审核基于 Guest Introspection 的安全系统中的各种情况。



事件可在未安装自定义 vSphere 插件的情况下显示。请参见《vCenter Server 管理指南》了解有关事件和警报的信息。

事件是生成警报的基础。注册为 vCenter Server 扩展组件后，NSX Manager 会定义创建和移除警报的规则。

所有事件的通用参数是事件时间戳和 NSX Manager event\_id。

下表列出了 SVM 和 NSX Manager 报告的 Guest Introspection 事件。

**表 18-3. Guest Introspection 事件**

描述	严重性	VC 参数
已启用 Guest Introspection 解决方案 <i>SolutionName</i> 。支持 <i>versionNumber</i> 版本的 VFile 协议。	信息	时间戳
ESX 模块已启用。	信息	时间戳
ESX 模块已卸载。	信息	时间戳
NSX Manager 已丢失与 ESX 模块的连接。	信息	时间戳
不兼容版本的 ESX 模块联系了 Guest Introspection 解决方案 <i>SolutionName</i> 。	错误	时间戳、解决方案版本、ESX 模块版本
ESX 模块与 <i>SolutionName</i> 之间的连接失败。	错误	时间戳、ESX 模块版本、解决方案版本
Guest Introspection 无法连接到 SVM。	错误	时间戳
Guest Introspection 丢失与 SVM 的连接。	错误	时间戳

## Guest Introspection 审核消息

审核消息包含致命错误及其他重要的审核信息，这些信息记录在 `vmware.log` 中。

以下情况将记录为审核消息：

- 瘦代理初始化成功（版本号）。
- 瘦代理初始化失败。
- 首次建立了与 SVM 的通信。
- 无法与 SVM 建立通信（当这种情况首次出现时）。

生成的每个日志消息的起始处包含以下子字符串：vf-AUDIT、vf-ERROR、vf-WARN、vf-INFO、vf-DEBUG。

## 收集 Guest Introspection 故障排除数据

VMware 技术支持部门会定期收集诊断信息或支持包（如果处理支持请求）。该诊断信息包含您的虚拟机的日志和配置文件。

### 身份防火墙故障排除数据

如果基于身份标识的防火墙环境使用 Guest Introspection，请在以下知识库文章中查找诊断信息：“排除 vShield Endpoint/NSX Guest Introspection 故障” (<https://kb.vmware.com/kb/2094261>) 和“在 VMware NSX for vSphere 6.x Guest Introspection 通用服务虚拟机中收集日志” (<https://kb.vmware.com/kb/2144624>)。

## 卸载 Guest Introspection 模块

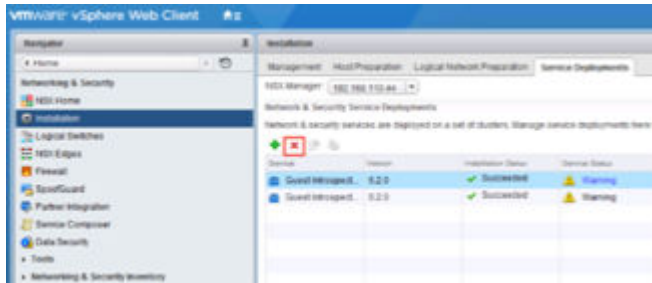
卸载 Guest Introspection 会从群集上的主机中移除 VIB，并从群集上的每台主机中移除服务虚拟机。NSX 数据安全、活动监控和多种第三方安全解决方案需要 Guest Introspection。卸载 Guest Introspection 会产生多种影响。



**小心** 从群集中卸载 Guest Introspection 模块之前，必须先从该群集上的主机中卸载使用 Guest Introspection 的所有第三方产品。请按照解决方案提供商提供的说明进行操作。

要卸载 Guest Introspection，请执行以下操作：

- 1 在 vCenter 中，导航到主页 > 网络和安全 > 安装，然后选择**服务部署**选项卡。
- 2 选择一个 Guest Introspection 实例，然后单击删除图标。
- 3 可以立即删除，也可以安排以后删除。



## 数据安全

可通过 **NSX** 数据安全查看存储在组织的虚拟化环境和云环境中的敏感数据。基于 **NSX** 数据安全所报告的违规情况，您可以确保敏感数据受到充分保护，并能评估是否符合周围环境的法规。

---

**注** 从 **NSX 6.2.3** 开始，**NSX** 数据安全功能将被弃用。在 **NSX 6.2.3** 中，您可以自行决定继续使用该功能，但要注意，在将来的 **NSX** 版本中将移除该功能。

---

要开始使用 **NSX** 数据安全，请创建一个策略，该策略定义适用于组织中的数据安全的法规，并指定待扫描的环境区域和文件。法规由识别待检测敏感内容的内容滤片组成。**NSX** 仅支持 **PCI**、**PHI** 和 **PII** 相关的法规。

启动数据安全扫描后，**NSX** 将分析 **vSphere** 清单中虚拟机上的数据，并报告检测到的违规数量和违反策略的文件。

本章讨论了以下主题：

- 安装 **NSX** 数据安全
- **NSX** 数据安全用户角色
- 定义数据安全策略
- 运行数据安全扫描
- 查看和下载报告
- 创建正则表达式
- 卸载 **NSX** 数据安全

## 安装 **NSX** 数据安全

---

**注** 从 **NSX 6.2.3** 开始，**NSX** 数据安全功能将被弃用。在 **NSX 6.2.3** 中，您可以自行决定继续使用该功能，但要注意，在将来的 **NSX** 版本中将移除该功能。

---

### 前提条件

必须在要安装数据安全的群集上安装 **NSX Guest Introspection**。

如果要将 **IP** 池中的某个 **IP** 地址分配给数据安全服务虚拟机，请先创建 **IP** 池，然后再安装数据安全。请参见《**NSX** 管理指南》中的“分组对象”。

## 步骤

- 1 在**安装 (Installation)**选项卡中，单击**服务部署 (Service Deployments)**。
- 2 单击**新建服务部署 (New Service Deployment)** () 图标。
- 3 在“部署网络和安全服务”对话框中，选择**数据安全 (Data Security)**，然后单击**下一步 (Next)**。
- 4 在**指定调度 (Specify schedule)**（在该对话框的底部）中，选择**立即部署 (Deploy now)**以便在安装数据安全后立即对其进行部署，或者选择部署日期和时间。
- 5 单击**下一步 (Next)**。
- 6 选择要安装数据安全的数据中心和群集，然后单击**下一步 (Next)**。
- 7 在“选择存储和管理网络”页面上，选择要添加服务虚拟机存储器的数据存储，或者选择**已在主机上指定 (Specified on host)**。

选定的数据存储在选定群集的所有主机上都必须可用。

如果选择了**已在主机上指定 (Specified on host)**，则在将数据存储添加到群集中之前，必须在主机的**AgentVM 设置 (AgentVM Settings)**中指定 ESX 主机的数据存储。请参见《vSphere API/SDK 文档》。

- 8 选择用于承载管理接口的分布式虚拟端口组。该端口组必须能够访问 NSX Manager 的端口组。

如果数据存储设置为**已在主机上指定 (Specified on host)**，则必须在群集内每个主机的 **agentVmNetwork** 属性中指定要使用的网络。请参见《vSphere API/SDK 文档》。

将主机添加到群集时，必须在将该主机添加到群集之前设置其 **agentVmNetwork** 属性。

选定的端口组必须在选定群集的所有主机上都可用。

- 9 在“IP 分配”中，选择以下其中的一项：

选择	目的
<b>DHCP</b>	通过动态主机配置协议 (DHCP) 将 IP 地址分配给数据安全服务虚拟机。
<b>IP 池</b>	将选定 IP 池中的某个 IP 地址分配给数据安全服务虚拟机。

请注意，不支持静态 IP 地址。

- 10 单击**下一步 (Next)**，然后在“即将完成”页面上单击**完成 (Finish)**。
- 11 监控该部署，直至**安装状态 (Installation Status)**列显示**成功 (Succeeded)**。
- 12 如果**安装状态 (Installation Status)**列显示**失败 (Failed)**，则单击“失败”旁边的图标。将显示所有部署错误。单击**解决 (Resolve)**修复这些错误。在某些情况下，解决这些错误时会显示其他错误。执行所需操作，然后重新单击**解决办法 (Resolve)**。

## NSX 数据安全用户角色

用户的角色确定了该用户可以执行的操作。

角色	允许的操作
安全管理员	创建和发布策略，并查看违规报告。无法启动或停止数据安全扫描。
NSX 管理员	启动和停止数据安全扫描。
审核员	查看配置的策略和违规报告。

## 定义数据安全策略

要在环境中检测敏感数据，必须创建数据安全策略。您必须是安全管理员才可创建策略。

要定义策略，必须指定以下内容：

<b>法规</b>	法规是数据隐私法，用于保护 <b>PCI</b> （支付卡行业）、 <b>PHI</b> （受保护的健康信息）和 <b>PII</b> （个人身份信息）信息。可以选择您的公司需要遵守的法规。运行扫描时，数据安全会识别违反策略中法规并且对组织来说比较敏感的数据。
<b>文件筛选器</b>	可以创建筛选器以限制要扫描的数据，并从扫描中排除不可能包含敏感数据的文件类型。

## 选择法规

选择完公司数据需要遵守的法规后，**NSX** 即可识别哪些文件中包含违反这些特定法规的信息。

### 前提条件

您必须已获得安全管理员角色。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking and Security)**，然后单击**数据安全 (Data Security)**。
- 3 单击**管理 (Manage)**选项卡。
- 4 单击**编辑 (Edit)**，然后单击**全部 (All)**以显示所有可用法规。
- 5 选择要检测其合规性的法规。

**注** 有关可用的法规的信息，请参见《数据安全参考》指南。

某些法规需要 **NSX** 数据安全的其他信息才能识别敏感数据。如果选择的法规可监控团体保险编号、患者标识号、医疗记录编号、健康计划受益人编号、美国银行帐号、自定义帐户或学生标识号，请指定正则表达式模式以标识该数据。

- 6 检查正则表达式的准确性。

指定错误的正则表达式会减慢发现过程。有关正则表达式的详细信息，请参见[创建正则表达式](#)。

- 7 单击**下一步 (Next)**。
- 8 单击**完成 (Finish)**。

9 单击**发布更改 (Publish Changes)**应用该策略。

## 指定文件筛选器

可以根据大小、上次修改日期或文件扩展名限制要监控的文件。

### 前提条件

您必须已获得安全管理员角色。

### 步骤

- 1 在数据安全面板的**管理 (Manage)**选项卡中，单击**要扫描的文件 (Files to scan)**旁边的**编辑 (Edit)**。
- 2 可以选择监控清单中虚拟机上的所有文件，也可以选择要应用的限制。

选项	描述
监控客户机虚拟机上的所有文件	NSX 数据安全将扫描所有文件。
仅监控满足以下条件的文件	<p>根据需要选择以下选项。</p> <ul style="list-style-type: none"> <li>■ <b>大小 (Size)</b>指示 NSX 数据安全应仅扫描小于指定大小的文件。</li> <li>■ <b>上次修改日期 (Last Modified Date)</b>指示 NSX 数据安全应仅扫描在指定日期之间修改的文件。</li> <li>■ <b>类型 (Types):</b> 选择仅具有以下扩展名的文件 (<b>Only files with the following extensions</b>)以输入要扫描的文件类型。选择<b>除具有以下扩展名的文件以外的所有文件 (All files, except those with extensions)</b>以输入要从扫描中排除的文件类型。</li> </ul>

有关 NSX 数据安全可以检测的文件格式的信息，请参见《数据安全参考》指南。

- 3 单击**保存 (Save)**。
- 4 单击**发布更改 (Publish Changes)**应用该策略。

## 运行数据安全扫描

运行数据安全扫描可识别虚拟环境中违反策略的数据。

### 前提条件

只有 NSX 管理员才能启动、暂停或停止数据安全扫描。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking and Security)**，然后单击**数据安全 (Data Security)**。
- 3 单击**管理 (Manage)**选项卡。
- 4 单击“扫描”旁边的**开始 (Start)**。

**注** 如果虚拟机已关闭电源，则只能在其打开电源后才可以进行扫描。

如果正在进行扫描，则可用选项包括**暂停 (Pause)**和**停止 (Stop)**。

如果数据安全是服务编排策略的一部分，在扫描过程中会将映射到该服务编排策略的安全组中的虚拟机都扫描一遍。如果运行扫描时编辑和发布了策略，则扫描将重新启动。重新扫描可确保所有虚拟机符合已编辑的策略。可通过发布已编辑的策略触发重新扫描，而不是通过虚拟机上的数据更新。

如果在扫描数据安全时将虚拟机移动到排除的群集或资源池，则不会扫描该虚拟机上的文件。如果通过 vMotion 将虚拟机移至其他主机，则扫描会在第二台主机上继续运行。该虚拟机位于之前的主机上时已扫描的文件不会重新扫描。

数据安全引擎开始扫描虚拟机时，它会记录扫描的开始时间。扫描结束时，它将记录扫描的结束时间。通过选择**任务和事件 (Tasks and Events)**选项卡，可以查看群集、主机或虚拟机的扫描开始时间和结束时间。

NSX 数据安全会限制主机上每次同时扫描的虚拟机数，从而最大程度地降低对性能的影响。VMware 建议您在正常工作时间暂停扫描以避免任何性能开销。

## 查看和下载报告

启动安全扫描后，NSX 会显示每次扫描的开始时间和结束时间、扫描的虚拟机数以及检测到的冲突数。

### 前提条件

您被分配了安全管理员角色或审核员角色。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全 (Networking and Security)**，然后单击**数据安全 (Data Security)**。
- 3 单击**报告 (Reports)**选项卡。
- 4 指定冲突计数报告或冲突文件报告。

## 创建正则表达式

正则表达式是一种用于描述特定文本字符（也称为字符串）序列的模式。可使用正则表达式在文本正文中搜索或匹配特定的字符串或字符串类。

使用正则表达式类似于执行通配符搜索，但是正则表达式的功能更强大。正则表达式既可以非常简单，也可以非常复杂。正则表达式的一个简单示例是 *cat*。

它会在应用该正则表达式的任何文本正文中查找字母序列 *cat* 的第一个实例。如果要确保只查找单词 *cat*，而不查找 *cats* 或 *hepcat* 等其他字符串，则可使用以下稍复杂一些的正则表达式：*\bcat\b*。

此表达式包括特殊字符，确保仅当 *cat* 序列的两端均断字时才匹配。再举一个例子，要执行几乎等效于典型通配符搜索字符串 *c+t* 的搜索，可以使用以下正则表达式：*\bclw+tlb*。

这表示查找这样的单词：边界 (*\b*) 为 *c*，后跟一个或多个非空格字符、非标点符号字符 (*w+*)，最后以 *t* 作为单词边界 (*\b*)。此表达式将查找 *cot*、*cat*、*croat*，但不查找 *crate*。

表达式可以非常复杂。以下表达式可查找任何有效的电子邮件地址。

```
\b[A-Za-z0-9._%~]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}\b
```

有关创建正则表达式的详细信息，请参见 <http://userguide.icu-project.org/strings/regexp>。

## 卸载 NSX 数据安全

如果您不再使用 NSX 数据安全或要升级 NSX Manager，需要卸载 NSX 数据安全。NSX 数据安全不支持直接升级。在升级 NSX Manager 之前，请务必先卸载 NSX 数据安全，并在升级完成后再重新安装。

从 NSX 6.2.3 开始，NSX 数据安全功能将被弃用。在 NSX 6.2.3 中，您可以自行决定继续使用该功能，但要注意，在将来的 NSX 版本中将移除该功能。

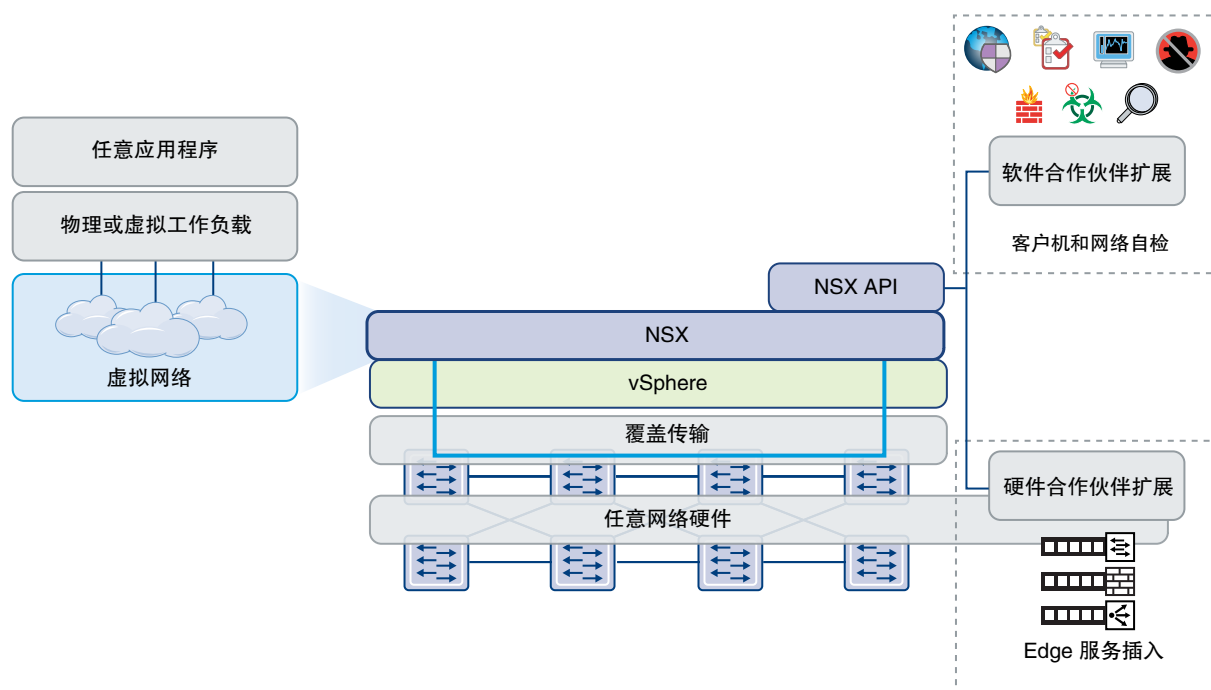
### 步骤

- 1 在**安装 (Installation)**选项卡中，单击**服务部署 (Service Deployments)**。
- 2 选择 NSX 数据安全服务，然后单击**删除服务部署 (Delete Service Deployment)** (✖) 图标。
- 3 在“确认删除”对话框中，单击**立即删除 (Delete now)**，或者选择删除生效的日期和时间。
- 4 单击**确定 (OK)**。



## 网络可扩展性

数据中心网络通常涉及范围广泛的网络服务，包括交换、路由、防火墙、负载平衡等。在大多数情况下，这些服务由不同供应商提供。在物理环境中，在网络中连接这些服务是一项复杂的活动，包括搭架和堆叠物理网络设备、建立物理连接以及分别管理这些服务。**NSX** 可简化按照正确的流量路径连接正确服务的过程，并且可帮助您在单个 **ESX Server** 主机中或跨多个 **ESX Server** 主机构建复杂的网络，以用于生产、测试或开发目的。



有各种部署方法可用于向 **NSX** 插入第三方服务。

本章讨论了以下主题：

- 分布式服务插入
- 基于 **Edge** 的服务插入
- 集成第三方服务
- 部署合作伙伴服务
- 通过服务编排使用供应商服务

- [通过逻辑防火墙将流量重定向到供应商解决方案](#)
- [使用合作伙伴负载均衡器](#)
- [移除第三方集成](#)

## 分布式服务插入

在分布式服务插入中，单台主机拥有单台物理机上的所有服务模块、内核模块和虚拟机实施。系统的所有组件均可与物理主机内的组件进行交互。这样可以实现更快的模块到模块通信以及精简型部署模型。同一配置可以复制到网络中的其他物理系统上以实现扩展，同时，服务模块和 **vmkernel** 之间的控制层面与数据层面流量在同一物理系统上处理。在受保护虚拟机的 **vMotion** 操作期间，合作伙伴安全计算机会将虚拟机状态从源主机移至目标主机。

利用此类型服务插入的供应商解决方案包括入侵防御服务 (IPS)/入侵检测服务 (IDS)、防火墙、防病毒、File Identity Monitoring (FIM) 和漏洞管理。

## 基于 Edge 的服务插入

将 NSX Edge 与其他网络服务一起在 Edge 服务群集中部署为虚拟机。NSX Edge 具有将特定流量重定向到第三方网络服务的功能。

利用此类型的服务插入的供应商解决方案包括 ADC/负载均衡器设备。

## 集成第三方服务

这是一个用来将第三方服务插入到 NSX 平台中的高级通用工作流。

### 步骤

- 1 在供应商控制台上向 NSX Manager 注册第三方服务。

需要 NSX 登录凭据才能注册该服务。有关详细信息，请参见供应商文档。

- 2 在 NSX 中部署该服务。请参见[部署合作伙伴服务](#)。

在部署后，该第三方服务会在 NSX “服务定义” 窗口中显示，并且已准备就绪，可以使用。在 NSX 中使用该服务的过程取决于所插入的服务的类型。

例如，通过在服务编排中创建安全策略或创建将流量重定向到该服务的防火墙规则，可以启用基于主机的防火墙服务。请参见[通过服务编排使用供应商服务](#)或[通过逻辑防火墙将流量重定向到供应商解决方案](#)。

有关使用基于 Edge 的服务的信息，请参见[使用合作伙伴负载均衡器](#)。

## 部署合作伙伴服务

如果合作伙伴解决方案包含主机中驻留的虚拟设备，则可以先部署服务，然后向 NSX Manager 注册解决方案。

## 前提条件

请确保：

- 向 NSX Manager 注册合作伙伴解决方案。
- NSX Manager 可访问合作伙伴解决方案的管理控制台。

## 步骤

- 1 单击**网络和安全**，然后单击**安装**。
- 2 单击**服务部署**选项卡，然后单击**新建服务部署 (+)** 图标。
- 3 在“部署网络和安全服务”对话框中，选择相应的解决方案。
- 4 在**指定调度**（在对话框的底部）中，选择**立即部署**以立即部署解决方案，或者选择部署日期和时间。
- 5 单击**下一步**。

- 6 选择要部署解决方案的数据中心和群集，然后单击**下一步**。

- 7 选择要添加解决方案服务虚拟机存储器的数据存储，或者选择**已在主机上指定**。

选定的数据存储在选定群集的所有主机上都必须可用。

如果选择了**已在主机上指定**，则在将数据存储添加到群集中之前，必须在主机的 **AgentVM 设置** 中指定 ESX 主机的数据存储。请参见《vSphere API/SDK 文档》。

- 8 选择用于承载管理接口的分布式虚拟端口组。该端口组必须能够访问 NSX Manager 的端口组。

如果网络设置为**已在主机上指定**，则必须在群集内每个主机的**代理虚拟机设置 > 网络**属性中指定要使用的网络。请参见《vSphere API/SDK 文档》。

您必须先在主机上设置代理虚拟机网络属性，然后再将其添加到群集中。导航到**管理 > 设置 > 代理虚拟机设置 > 网络**，然后单击**编辑**以设置代理虚拟机网络。

选定的端口组必须在选定群集的所有主机上都可用。

- 9 在“IP 分配”中，选择以下其中的一项：

选择	目的
<b>DHCP</b>	通过动态主机配置协议 (DHCP) 将 IP 地址分配给服务虚拟机。
<b>IP 池</b>	将选定 IP 池中的某个 IP 地址分配给服务虚拟机。

- 10 单击**下一步**，然后在“即将完成”页面上单击**完成**。

- 11 监控部署，直到**安装状态**显示“成功”。如果状态显示“失败”，请单击“失败”旁边的图标并采取措施解决该错误。

## 后续步骤

现在可以通过 NSX UI 或 NSX API 使用合作伙伴服务。

## 通过服务编排使用供应商服务

第三方供应商服务包括流量重定向、负载均衡器以及数据丢失防护、防病毒等客户机安全服务。通过服务编排，您可以对一组 vCenter 对象应用这些服务。

安全组是指一组 vCenter 对象，例如群集、虚拟机、虚拟网卡和逻辑交换机。安全策略是指一组 Guest Introspection 服务、防火墙规则和网络自检服务。

将安全策略映射到安全组时，将基于适当的第三方供应商服务配置文件创建重定向规则。当流量从属于该安全组的虚拟机中流出时，将被重定向到确定如何处理该流量的注册第三方供应商服务。有关服务编排的详细信息，请参见[使用服务编排](#)。

## 通过逻辑防火墙将流量重定向到供应商解决方案

您可以添加防火墙，以将流量重定向到已注册的供应商解决方案。重定向的流量之后会由供应商服务处理。

### 前提条件

- 必须向 NSX Manager 注册第三方服务，且必须在 NSX 中部署注册的服务。
- 如果默认防火墙规则操作设置为“阻止”，则必须添加一条允许流量重定向的规则。

### 步骤

- 1 在 vSphere Web Client 中，导航到 **网络和安全 (Networking & Security) > 防火墙 (Firewall)**。
- 2 单击 **合作伙伴安全服务 (Partner security services)** 选项卡。
- 3 在要添加规则的区域中，单击 **添加规则 (Add rule)** ( 图标。  
任何一个允许的新规则将添加到区域的顶部。
- 4 指向新规则的名称 (Name) 单元格，单击 ，然后键入规则名称。
- 5 指定规则的 **源 (Source)**、**目标 (Destination)** 和 **服务 (Service)**。有关详细信息，请参见[添加防火墙规则](#)。
- 6 指向新规则的操作 (Action) 单元格，然后单击 。
  - a 在 **操作 (Action)** 中选择 **重定向 (Redirect.)**。
  - b 在 **重定向到 (Redirect To)** 中，选择服务配置文件和要向其绑定服务配置文件的逻辑交换机或安全组。  
该服务配置文件应用到连接所选逻辑虚拟机或安全组或其中包含的虚拟机。
  - c 指明是否要将重定向的流量记入日志，并键入注释（如有）。
  - d 单击 **确定 (OK)**。  
所选的服务配置文件在 **操作 (Action)** 列中显示为链接。单击该服务链接可显示服务配置文件绑定。
- 7 单击 **发布更改 (Publish Changes)**。

## 使用合作伙伴负载均衡器

可以使用第三方负载均衡器来平衡特定 NSX Edge 的流量。

### 前提条件

第三方负载均衡器必须向 NSX Manager 注册，并且必须在 NSX 中部署。

### 步骤

- 1 在 vSphere Web Client 中，导航到**网络和安全 (Networking & Security) > NSX Edge (NSX Edges)**。
- 2 双击一个 NSX Edge。
- 3 单击**管理 (Manage)**，然后单击**负载均衡器 (Load Balancer)**选项卡。
- 4 单击负载均衡器全局配置旁边的**编辑 (Edit)**。
- 5 选择**启用负载均衡器 (Enable Load Balancer)**和**启用服务插入 (Enable Service Insertion)**。
- 6 在**服务定义 (Service Definition)**中，选择适当的合作伙伴负载均衡器。
- 7 在**服务配置 (Service Configuration)**中，选择适当的服务配置。
- 8 填写其余字段，完成负载均衡器设置，包括添加服务监控器、服务器池、应用程序配置文件、应用程序规则和虚拟服务器。添加虚拟服务器时，请选择供应商提供的模板。有关详细信息，请参见[设置负载均衡](#)。

指定 Edge 的流量将通过第三方供应商的管理控制台进行负载均衡。

## 移除第三方集成

本示例介绍如何从 NSX 中移除第三方集成解决方案。

移除任何第三方软件解决方案时，都应遵循正确的顺序。

### 步骤

- 1 在 vSphere Web Client 中，导航至**网络和安全 > 服务编排 (Networking & Security > Service Composer)**，然后删除将流量重定向到第三方解决方案的规则（或安全策略）。
- 2 导航至**服务定义 (Service Definitions)**，然后双击第三方解决方案的名称。
- 3 单击**相关对象 (Related Objects)**，然后删除相关对象。
- 4 导航至**安装 > 服务部署 (Installation > Service Deployments)**，然后删除第三方部署。  
此操作将卸载关联的虚拟机。
- 5 返回到**服务定义 (Service Definitions)**，然后删除定义的任何子组件。
- 6 在服务实例中，删除服务配置文件。
- 7 删除服务实例。
- 8 删除服务定义。

第三方集成解决方案现已从 **NSX** 中移除。

### 后续步骤

记下配置设置，然后从第三方解决方案中移除 **NSX**。例如，您可能需要删除引用其他对象的规则，然后删除这些对象。

## 用户管理

在许多组织中，网络连接和安全操作由不同的小组或成员处理。此类组织可能需要某种方法来限制只有特定用户可以执行某些操作。本主题介绍了 NSX 提供的一些用于配置此类访问控制的选项。

NSX 还支持 Single Sign On (SSO)，通过 SSO，NSX 可借此功能对来自其他身份服务（如 Active Directory、NIS 和 LDAP）的用户进行身份验证。

vSphere Web Client 中的用户管理与任何 NSX 组件的 CLI 中的用户管理都是分开的。

本章讨论了以下主题：

- [NSX 用户和各功能访问权限](#)
- [配置 Single Sign On](#)
- [管理用户权限](#)
- [管理默认用户帐户](#)
- [将角色分配给 vCenter 用户](#)
- [编辑用户帐户](#)
- [更改用户角色](#)
- [禁用或启用用户帐户](#)
- [删除用户帐户](#)

### NSX 用户和各功能访问权限

要部署并管理 NSX，需要具有某些 vCenter 权限。NSX 为各种用户和角色提供广泛的读取权限和读/写权限。

#### 角色定义

可用角色如下：

角色 = system\_write、system\_urm、super\_user、vshield\_admin、security\_admin、auditor、dlp\_svm、epsec\_host、enterprise\_admin、component\_manager\_user、replicator

本地用户角色 = system\_write、system\_urm、super\_user、security\_admin、auditor、dlp\_svm、epsec\_host、component\_manager\_user、replicator

系统角色 = system\_write、system\_urm、dlp\_svm、epsec\_host、replicator

## 权限类型

权限类型分为读取权限和写入权限。

## 角色访问权限定义

角色访问权限定义确定一个角色拥有读取权限还是读/写权限。

`super_user.object_permission = 读、写`

`vshield_admin.object_permission = 读、写`

`security_admin.object_permission = 读、写`

`auditor.object_permission = 读`

`system_write.object_permission = 读、写`

`system_urm.object_permission = 读`

`dlp_svm.object_permission = 读、写`

`epsec_host.object_permission = 读、写`

`enterprise_admin.object_permission = 读、写`

`replicator.object_permission = 读、写`

## 根定义

根定义说明超级用户角色。

`super_user.superuser = true`

`system_write.superuser = true`

## 全局范围内角色对对象的访问权限

`vshield_admin.object_access_scope.global = true`

`super_user.object_access_scope.global = true`

`system_write.object_access_scope.global = true`

`system_urm.object_access_scope.global = true`

`dlp_svm.object_access_scope.global = true`

`epsec_host.object_access_scope.global = true`

`enterprise_admin.object_access_scope.global = true`



## 通用范围内角色对对象的访问权限

replicator.object\_access\_scope.universal=true

system\_write.object\_access\_scope.universal=true

## 服务

以下服务在 NSX 中可用：

administration、urm、edge、app、namespace、spoofguard、dlp、epsec、library、install、vdn、eam、si、truststore、component\_manager、ipam、secfabric、security\_policy、messaging、replicator

## 功能定义

每种服务中的功能定义如下所示：

administration.featurelist = administration.configuration, administration.update, administration.system\_events, administration.audit\_logs, administration.debug

urm.featurelist = urm.user\_account\_management, urm.object\_access\_control, urm.feature\_access\_control

edge.featurelist = edge.system, edge.nat, edge.firewall, edge.dhcp, edge.loadbalancer, edge.vpn, edge.syslog, edge.support, edge.routing, edge.certificate, edge.appliance, edge.highavailability, edge.dns, edge.vnic, edge.ssh, edge.autoplumbing, edge.statistics, edge.bridging, edge.systemcontrol

app.featurelist = app.config, app.firewall, app.flow, app.forcesync, app.syslog, app.techsupport

pgi.featurelist = pgi.switch, pgi.portgroup, pgi.lkm

namespace.featurelist = namespace.config

spoofguard.featurelist = spoofguard.config

dlp.featurelist = dlp.scan\_scheduling, dlp.reports, dlp.policy, dlp.svm\_interaction

epsec.featurelist = epsec.registration, epsec.health\_monitoring, epsec.manager, epsec.policy, epsec.svm\_priv, epsec.scan, epsec.reports

library.featurelist = library.grouping, library.host\_preparation, library.tagging

install.featurelist = install.app, install.epsec, install.dlp

vdn.featurelist = vdn.config\_nsm, vdn.provision

eam.featurelist = eam.install

si.featurelist = si.service, si.serviceprofile

truststore.featurelist = truststore.trustentity\_management

component\_manager.featurelist = healthstatus

ipam.featurelist = ipam.configuration, ipam.ipallocation

```
secfabric.featurelist = secfabric.deploy, secfabric.alarms
```

```
security_policy.featurelist = security_policy.configuration, security_policy.security_group_binding
```

```
blueprint_sam.featurelist = blueprint_sam.reports, blueprint_sam.ad_config,
blueprint_sam.control_data_collection, blueprint_sam.techsupport, blueprint_sam.db_maintain
```

```
messaging.featurelist = messaging.messaging
```

```
replicator.featurelist = replicator.configuration
```

## 功能访问权限定义

对于每个功能和角色组合，功能访问权限定义指定用户拥有只读权限还是读/写权限。

若功能和角色组合未列出，这意味着拥有该角色的用户无权使用此功能。

例如：

```
auditor.app.firewall = 读
```

```
security_admin.app.firewall = 读、写
```

这表示 `app.firewall` 功能上的 `auditor` 角色拥有只读权限，而 `app.firewall` 功能上的 `security_admin` 角色拥有读/写权限。

## 功能访问权限定义 - system\_urm

```
system_urm.urm.user_account_management = 读
```

## 功能访问权限定义 - vshield\_admin

```
vshield_admin.administration.configuration = 读、写
```

```
vshield_admin.administration.update = 读、写
```

```
vshield_admin.administration.system_events = 读、写
```

```
vshield_admin.administration.audit_logs = 读
```

```
vshield_admin.urm.user_account_management = 读、写
```

```
vshield_admin.urm.object_access_control = 读
```

```
vshield_admin.urm.feature_access_control = 读
```

```
vshield_admin.edge.system = 读、写
```

```
vshield_admin.edge.appliance = 读、写
```

```
vshield_admin.edge.highavailability = 读、写
```

```
vshield_admin.edge.vnic = 读、写
```

```
vshield_admin.edge.dns = 读
```

```
vshield_admin.edge.ssh = 读、写
```

vshield\_admin.edge.autoplumbing = 读  
vshield\_admin.edge.statistics = 读  
vshield\_admin.edge.nat = 读  
vshield\_admin.edge.dhcp = 读  
vshield\_admin.edge.loadbalancer = 读  
vshield\_admin.edge.vpn = 读  
vshield\_admin.edge.syslog = 读、写  
vshield\_admin.edge.support = 读、写  
vshield\_admin.edge.routing = 读  
vshield\_admin.edge.firewall = 读  
vshield\_admin.edge.bridging = 读  
vshield\_admin.edge.certificate = 读  
vshield\_admin.edge.systemcontrol = 读、写  
vshield\_admin.library.grouping = 读  
vshield\_admin.app.config = 读、写  
vshield\_admin.app.forcesync = 读、写  
vshield\_admin.app.syslog = 读、写  
vshield\_admin.app.techsupport = 读、写  
vshield\_admin.namespace.config = 读、写  
vshield\_admin.dlp.scan\_scheduling = 读、写  
vshield\_admin.epsec.reports = 读、写  
vshield\_admin.epsec.registration = 读、写  
vshield\_admin.epsec.health\_monitoring = 读  
vshield\_admin.epsec.policy = 读、写  
vshield\_admin.epsec.scan\_scheduling = 读、写  
vshield\_admin.library.host\_preparation = 读、写  
vshield\_admin.library.tagging = 读  
vshield\_admin.install.app = 读、写  
vshield\_admin.install.epsec = 读、写  
vshield\_admin.install.dlp = 读、写  
vshield\_admin.vdn.config\_nsm = 读、写

vshield\_admin.vdn.provision = 读、写  
 vshield\_admin.eam.install = 读、写  
 vshield\_admin.si.service = 读、写  
 vshield\_admin.si.serviceprofile = 读、写  
 vshield\_admin.truststore.trustentity\_management = 读、写  
 vshield\_admin.ipam.configuration = 读、写  
 vshield\_admin.ipam.ipallocation = 读、写  
 vshield\_admin.secfabric.deploy = 读、写  
 vshield\_admin.secfabric.alarms = 读、写  
 vshield\_admin.blueprint\_sam.ad\_config = 读、写  
 vshield\_admin.blueprint\_sam.control\_data\_collection = 读、写  
 vshield\_admin.blueprint\_sam.techsupport = 读、写  
 vshield\_admin.blueprint\_sam.db\_maintain = 读、写  
 vshield\_admin.messaging.messaging = 读、写  
 vshield\_admin.replicator.configuration = 读、写

## 功能访问权限定义 - security\_admin

security\_admin.administration.system\_events = 读、写  
 security\_admin.administration.audit\_logs = 读  
 security\_admin.edge.system = 读  
 security\_admin.edge.appliance = 读  
 security\_admin.edge.highavailability = 读  
 security\_admin.edge.vnic = 读、写  
 security\_admin.edge.dns = 读、写  
 security\_admin.edge.ssh = 读、写  
 security\_admin.edge.autoplumbing = 读、写  
 security\_admin.edge.statistics = 读  
 security\_admin.edge.nat = 读、写  
 security\_admin.edge.dhcp = 读、写  
 security\_admin.edge.loadbalancer = 读、写  
 security\_admin.edge.vpn = 读、写

security\_admin.edge.syslog = 读、写  
security\_admin.edge.support = 读、写  
security\_admin.edge.routing = 读、写  
security\_admin.edge.firewall = 读、写  
security\_admin.edge.bridging = 读、写  
security\_admin.edge.certificate = 读、写  
security\_admin.edge.systemcontrol = 读、写  
security\_admin.app.firewall = 读、写  
security\_admin.app.flow = 读、写  
security\_admin.app.forcesync = 读  
security\_admin.app.syslog = 读  
security\_admin.namespace.config = 读  
security\_admin.spoofguard.config = 读、写  
security\_admin.dlp.reports = 读、写  
security\_admin.dlp.policy = 读、写  
security\_admin.epsec.policy = 读、写  
security\_admin.epsec.reports = 读  
security\_admin.epsec.health\_monitoring = 读  
security\_admin.library.grouping = 读、写  
security\_admin.library.tagging = 读、写  
security\_admin.install.app = 读  
security\_admin.install.epsec = 读  
security\_admin.install.dlp = 读  
security\_admin.vdn.config\_nsm = 读  
security\_admin.vdn.provision = 读  
security\_admin.eam.install = 读  
security\_admin.si.service = 读、写  
security\_admin.si.serviceprofile = 读  
security\_admin.truststore.trustentity\_management = 读、写  
security\_admin.ipam.configuration = 读、写  
security\_admin.ipam.ipallocation = 读、写

security\_admin.secfabric.alarms = 读  
security\_admin.secfabric.deploy = 读  
security\_admin.security\_policy.configuration = 读、写  
security\_admin.security\_policy.security\_group\_binding = 读、写  
security\_admin.blueprint\_sam.reports = 读  
security\_admin.blueprint\_sam.ad\_config = 读  
security\_admin.blueprint\_sam.control\_data\_collection = 读  
security\_admin.blueprint\_sam.db\_maintain = 读  
security\_admin.messaging.messaging = 读、写  
security\_admin.replicator.configuration = 读

## 功能访问权限定义 - auditor

auditor.administration.system\_events = 读  
auditor.administration.audit\_logs = 读  
auditor.edge.appliance = 读  
auditor.edge.highavailability = 读  
auditor.edge.vnic = 读  
auditor.edge.dns = 读  
auditor.edge.ssh = 读  
auditor.edge.autoplumbing = 读  
auditor.edge.statistics = 读  
auditor.edge.nat = 读  
auditor.edge.dhcp = 读  
auditor.edge.loadbalancer = 读  
auditor.edge.vpn = 读  
auditor.edge.syslog = 读  
auditor.edge.routing = 读  
auditor.edge.firewall = 读  
auditor.edge.bridging = 读  
auditor.edge.system = 读  
auditor.edge.certificate = 读

auditor.edge.systemcontrol = 读  
auditor.app.firewall = 读  
auditor.app.flow = 读  
auditor.app.forcesync = 读  
auditor.app.syslog = 读  
auditor.namespace.config = 读  
auditor.spoofguard.config = 读  
auditor.dlp.scan\_scheduling = 读  
auditor.dlp.policy = 读  
auditor.dlp.reports = 读  
auditor.library.grouping = 读  
auditor.epsec\_host.health\_monitoring = 读  
auditor.epsec.policy = 读  
auditor.epsec.reports = 读  
auditor.epsec.registration = 读  
auditor.vdn.config\_nsm = 读  
auditor.epsec.scan\_scheduling = 读  
auditor.vdn.provision = 读  
auditor.si.service = 读  
auditor.si.serviceprofile = 读  
auditor.truststore.trustentity\_management = 读  
auditor.secfabric.alarms = 读  
auditor.secfabric.deploy = 读  
auditor.security\_policy.configuration = 读  
auditor.security\_policy.security\_group\_binding = 读  
auditor.blueprint\_sam.reports = 读  
auditor.blueprint\_sam.ad\_config = 读  
auditor.blueprint\_sam.control\_data\_collection = 读  
auditor.blueprint\_sam.db\_maintain = 读  
auditor.library.tagging = 读  
auditor.ipam.configuration = 读

auditor.ipam.ipallocation = 读

auditor.messaging.messaging = 读

auditor.replicator.configuration = 读

## 功能访问权限定义 - dlp\_svm

dlp\_svm.dlp.svm\_interaction = 读、写

dlp\_svm.epsec.svm\_priv = 读、写

dlp\_svm.epsec.registration = 读

dlp\_svm.epsec.policy = 读

dlp\_svm.epsec.scan\_scheduling = 读

dlp\_svm.library.host\_preparation = 读、写

dlp\_svm.library.tagging = 读、写

## 功能访问权限定义 - epsec\_host

epsec\_host.epsec.registration = 读

epsec\_host.epsec.health\_monitoring = 写

## 功能访问权限定义 - enterprise\_admin

enterprise\_admin.administration.configuration = 读、写

enterprise\_admin.administration.update = 读、写

enterprise\_admin.administration.system\_events = 读、写

enterprise\_admin.administration.audit\_logs = 读

enterprise\_admin.urm.user\_account\_management = 读、写

enterprise\_admin.urm.object\_access\_control = 读

enterprise\_admin.urm.feature\_access\_control = 读

enterprise\_admin.edge.system = 读、写

enterprise\_admin.edge.appliance = 读、写

enterprise\_admin.edge.highavailability = 读、写

enterprise\_admin.edge.vnic = 读、写

enterprise\_admin.edge.dns = 读、写

enterprise\_admin.edge.ssh = 读、写

enterprise\_admin.edge.autoplumbing = 读、写



enterprise\_admin.edge.statistics = 读、写  
enterprise\_admin.edge.nat = 读、写  
enterprise\_admin.edge.dhcp = 读、写  
enterprise\_admin.edge.loadbalancer = 读、写  
enterprise\_admin.edge.vpn = 读、写  
enterprise\_admin.edge.syslog = 读、写  
enterprise\_admin.edge.support = 读、写  
enterprise\_admin.edge.routing = 读、写  
enterprise\_admin.edge.firewall = 读、写  
enterprise\_admin.edge.bridging = 读、写  
enterprise\_admin.edge.certificate = 读、写  
enterprise\_admin.edge.systemcontrol = 读、写  
enterprise\_admin.library.grouping = 读、写  
enterprise\_admin.library.host\_preparation = 读、写  
enterprise\_admin.library.tagging = 读、写  
enterprise\_admin.app.config = 读、写  
enterprise\_admin.app.forcesync = 读、写  
enterprise\_admin.app.syslog = 读、写  
enterprise\_admin.app.techsupport = 读、写  
enterprise\_admin.app.firewall = 读、写  
enterprise\_admin.app.flow = 读、写  
enterprise\_admin.namespace.config = 读、写  
enterprise\_admin.dlp.scan\_scheduling = 读、写  
enterprise\_admin.dlp.reports = 读、写  
enterprise\_admin.dlp.policy = 读、写  
enterprise\_admin.epsec.registration = 读、写  
enterprise\_admin.epsec.health\_monitoring = 读  
enterprise\_admin.epsec.scan\_scheduling = 读、写  
enterprise\_admin.epsec.reports = 读、写  
enterprise\_admin.epsec.policy = 读、写  
enterprise\_admin.install.app = 读、写

enterprise\_admin.install.epsec = 读、写

enterprise\_admin.install.dlp = 读、写

enterprise\_admin.eam.install = 读、写

enterprise\_admin.spoofguard.config = 读、写

enterprise\_admin.vdn.config\_nsm = 读、写

enterprise\_admin.vdn.provision = 读、写

enterprise\_admin.si.service = 读、写

enterprise\_admin.si.serviceprofile = 读、写

enterprise\_admin.truststore.trustentity\_management = 读、写

enterprise\_admin.ipam.configuration = 读、写

enterprise\_admin.ipam.ipallocation = 读、写

enterprise\_admin.secfabric.deploy = 读、写

enterprise\_admin.secfabric.alarms = 读、写

enterprise\_admin.security\_policy.configuration = 读、写

enterprise\_admin.security\_policy.security\_group\_binding = 读、写

enterprise\_admin.blueprint\_sam.reports = 读

enterprise\_admin.blueprint\_sam.ad\_config = 读、写

enterprise\_admin.blueprint\_sam.control\_data\_collection = 读、写

enterprise\_admin.blueprint\_sam.techsupport = 读、写

enterprise\_admin.blueprint\_sam.db\_maintain = 读、写

enterprise\_admin.messaging.messaging = 读、写

enterprise\_admin.replicator.configuration = 读、写

## 功能访问权限定义 - component\_manager\_user

component\_manager\_user.component\_manager.healthstatus = 读

## 功能访问权限定义 - replicator

replicator.administration.configuration = 读、写

replicator.administration.update = 读、写

replicator.administration.system\_events = 读、写

replicator.administration.audit\_logs = 读

replicator.urm.user\_account\_management = 读、写

replicator.urm.object\_access\_control = 读  
replicator.urm.feature\_access\_control = 读  
replicator.edge.system = 读、写  
replicator.edge.appliance = 读、写  
replicator.edge.highavailability = 读  
replicator.edge.vnic = 读、写  
replicator.edge.dns = 读  
replicator.edge.ssh = 读  
replicator.edge.autoplumbing = 读、写  
replicator.edge.statistics = 读  
replicator.edge.nat = 读  
replicator.edge.dhcp = 读、写  
replicator.edge.loadbalancer = 读  
replicator.edge.vpn = 读  
replicator.edge.syslog = 读  
replicator.edge.support = 读  
replicator.edge.routing = 读、写  
replicator.edge.firewall = 读  
replicator.edge.bridging = 读  
replicator.edge.certificate = 读  
replicator.edge.systemcontrol = 读  
replicator.library.grouping = 读、写  
replicator.library.host\_preparation = 读、写  
replicator.library.tagging = 读、写  
replicator.app.config = 读、写  
replicator.app.forcesync = 读、写  
replicator.app.syslog = 读、写  
replicator.app.techsupport = 读、写  
replicator.app.firewall = 读、写  
replicator.app.flow = 读、写  
replicator.namespace.config = 读、写

replicator.dlp.scan\_scheduling = 读、写  
replicator.dlp.reports = 读、写  
replicator.dlp.policy = 读、写  
replicator.epsec.registration = 读、写  
replicator.epsec.health\_monitoring = 读  
replicator.epsec.scan\_scheduling = 读、写  
replicator.epsec.reports = 读、写  
replicator.epsec.policy = 读、写  
replicator.install.app = 读、写  
replicator.install.epsec = 读、写  
replicator.install.dlp = 读、写  
replicator.eam.install = 读、写  
replicator.spoofguard.config = 读、写  
replicator.vdn.config\_nsm = 读、写  
replicator.vdn.provision = 读、写  
replicator.si.service = 读、写  
replicator.si.serviceprofile = 读、写  
replicator.truststore.trustentity\_management = 读、写  
replicator.ipam.configuration = 读、写  
replicator.ipam.ipallocation = 读、写  
replicator.secfabric.deploy = 读、写  
replicator.secfabric.alarms = 读、写  
replicator.security\_policy.configuration = 读、写  
replicator.security\_policy.security\_group\_binding = 读、写  
replicator.blueprint\_sam.reports = 读  
replicator.blueprint\_sam.ad\_config = 读、写  
replicator.blueprint\_sam.control\_data\_collection = 读、写  
replicator.blueprint\_sam.techsupport = 读、写  
replicator.blueprint\_sam.db\_maintain = 读、写  
replicator.messaging.messaging = 读、写  
replicator.replicator.configuration = 读、写

## 辅助节点上对通用对象的覆盖角色功能权限

secondary.super\_user.edge.highavailability = 读、写

secondary.enterprise\_admin.edge.highavailability = 读、写

secondary.vshield\_admin.edge.highavailability = 读、写

secondary.super\_user.edge.ssh = 读、写

secondary.enterprise\_admin.edge.ssh = 读、写

secondary.security\_admin.edge.ssh = 读、写

secondary.vshield\_admin.edge.ssh = 读、写

secondary.super\_user.edge.syslog = 读、写

secondary.enterprise\_admin.edge.syslog = 读、写

secondary.security\_admin.edge.syslog = 读、写

secondary.vshield\_admin.edge.syslog = 读、写

secondary.super\_user.edge.support = 读、写

secondary.enterprise\_admin.edge.support = 读、写

secondary.security\_admin.edge.support = 读、写

secondary.vshield\_admin.edge.support = 读、写

secondary.super\_user.edge.routing = 读、写

secondary.security\_admin.edge.routing = 读、写

secondary.enterprise\_admin.edge.routing = 读、写

secondary.super\_user.edge.appliance = 读、写

secondary.vshield\_admin.edge.appliance = 读、写

secondary.enterprise\_admin.edge.appliance = 读、写

secondary.super\_user.edge.vnic = 读、写

secondary.vshield\_admin.edge.vnic = 读、写

secondary.enterprise\_admin.edge.vnic = 读、写

secondary.super\_user.edge.firewall = 读、写

secondary.vshield\_admin.edge.firewall = 读、写

secondary.enterprise\_admin.edge.firewall = 读、写

## 配置 Single Sign On

SSO 可提高 vSphere 和 NSX 的安全性，它允许各个组件通过安全的令牌交换机制彼此进行通信，而不要求每个组件单独对用户进行身份验证。可以在 NSX Manager 上配置 Lookup Service，并提供 SSO 管理员凭据以便以 SSO 用户的身份注册 NSX Management Service。将 Single Sign On (SSO) 服务与 NSX 集成在一起可提高 vCenter 用户进行用户身份验证的安全性，并使 NSX 可以通过诸如 AD、NIS 和 LDAP 等其他标识服务对用户进行身份验证。

借助 SSO，NSX 可支持通过 REST API 调用使用受信任源的已验证安全断言标记语言 (SAML) 令牌来进行身份验证。NSX Manager 还可以获取身份验证 SAML 令牌供其他 VMware 解决方案使用。

SSO 用户的 NSX 缓存组信息。对组成员资格进行的更改最多将花费 60 分钟的时间从标识提供程序（例如 Active Directory）传播到 NSX。

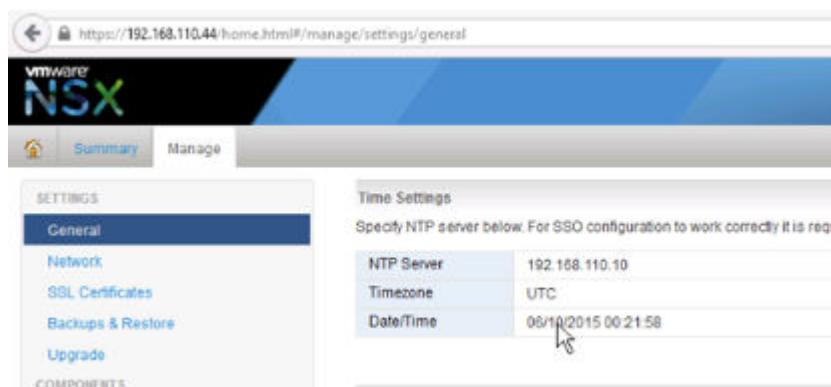
### 前提条件

- 要在 NSX Manager 上使用 SSO，您必须拥有 vCenter Server 5.5 或更高版本，并且必须在 vCenter Server 上安装 Single Sign On (SSO) 身份验证服务。请注意，这是针对嵌入式 SSO。您的部署可能使用外部集中式 SSO 服务器。

有关 vSphere 提供的 SSO 服务的信息，请参见 <http://kb.vmware.com/kb/2072435> 和 <http://kb.vmware.com/kb/2113115>。

- 必须指定 NTP 服务器，以使 SSO 服务器上的时间与 NSX Manager 上的时间保持同步。

例如：



### 步骤

- 1 登录到 NSX Manager 虚拟设备。

在 Web 浏览器中，导航到 NSX Manager 设备 GUI（位于 <https://<nsx-manager-ip>> 或 <https://<nsx-manager-hostname>>），然后以管理员身份使用您在 NSX Manager 安装期间配置的密码登录。

- 2 单击 **管理 (Manage)** 选项卡，然后单击 **NSX Management Service**。

- 3 键入装有 Lookup Service 的主机的名称或 IP 地址。

如果使用 vCenter 执行 Lookup Service，请输入 vCenter Server 的 IP 地址或主机名，并输入 vCenter Server 用户名和密码。

#### 4 键入端口号。

如果使用 vSphere 6.0 则输入端口 443。对于 vSphere 5.5，使用端口号 7444。

系统将根据指定的主机和端口显示 Lookup Service URL。

例如：

Lookup Service

For vCenter versions 5.1 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Management Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly.

Lookup Service IP:	192.168.110.26
Lookup Service Port:	443
Lookup Service:	https://192.168.110.26:443/lookupservice/sdk
SSO Administrator User Name:	administrator@vsphere.local
Password:	*****

OK Cancel

#### 5 检查证书指纹是否与 vCenter Server 的证书匹配。

如果在 CA 服务器上安装了 CA 签名证书，您将获得该 CA 签名证书的指纹。否则，您将获得自签名证书。

#### 6 确认 Lookup Service 状态为已连接 (Connected)。

例如：

Lookup Service

For vCenter versions 5.1 and above, you may configure Lookup Service and provide the SSO administrator credentials to register NSX Management Service as a solution user. It is also recommended to set the NTP server for SSO configuration to work correctly.

Lookup Service:	https://192.168.110.26:443/lookupservice/sdk
SSO Administrator User Name:	administrator@vsphere.local
Status:	● Connected ↻

#### 后续步骤

为该 SSO 用户分配一个角色。

## 管理用户权限

用户角色指定了用户可以对给定资源执行的操作。角色确定用户获得授权可对给定资源执行的活动，从而确保用户只能执行完成适当操作必需的功能。这样可以实现对特定资源的域控制，如果您的权限没有限制，还可实现系统范围的控制。

强制执行下列规则：

- 一个用户只能拥有一个角色。
- 不能将角色添加到用户或从用户中移除分配的角色。但可以更改用户的分配角色。

表 21-1. NSX Manager 用户角色

权限	权限
企业管理员	NSX 操作和安全。
NSX 管理员	NSX 操作仅包括以下内容：例如，安装虚拟设备、配置端口组。
安全管理员	NSX 安全仅包括以下内容：例如，定义数据安全策略、创建端口组、创建 NSX 模块的报告。
审核员	只读。

只能为 vCenter 用户分配企业管理员和 NSX 管理员角色。

## 管理默认用户帐户

NSX Manager 用户界面包含一个用户帐户，此帐户具有对所有资源的访问权限。您不能编辑此用户的权限或删除此用户。默认用户名是 **admin**，默认密码是 **default** 或您在 NSX Manager 安装期间指定的密码。

仅可以通过 CLI 命令管理 NSX Manager 设备的 **admin** 用户。

## 将角色分配给 vCenter 用户

将角色分配给 SSO 用户时，vCenter 通过在 SSO 服务器上配置的身份服务对该用户进行身份验证。如果 SSO 服务器未配置或不可用，则用户在本地进行身份验证或基于 vCenter 配置通过 Active Directory 进行身份验证。

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全**，然后单击 **NSX Manager**。
- 3 在“名称”列中单击 **NSX Manager**，然后单击**管理**选项卡。
- 4 单击**用户**。
- 5 单击**添加**。

此时将打开“分配角色”窗口。

- 6 单击**指定 vCenter 用户**或**指定 vCenter 组**。
- 7 键入用户的 vCenter 用户名称或组名称。

有关详细信息，请参见以下示例。

域名：corp.vmware.com

别名：corp

组名称：group1@corp.vmware.com

用户名：user1@corp.vmware.com

如果在 NSX Manager 中为某个组分配一个角色，该组中的任何用户都可以登录到 NSX Manager 用户界面。

将角色分配给用户时，键入用户别名。例如，user1@corp。



- 8 单击**下一步**。
- 9 为用户选择角色，然后单击**下一步**。有关可用角色的详细信息，请参见[管理用户权限](#)。
- 10 单击**完成**。

用户帐户将显示在“用户”表中。

## 了解基于组的角色分配

组织创建用户组以进行适当的用户管理。与 SSO 集成后，NSX Manager 可以获得用户所属组的详细信息。NSX Manager 可以将角色分配给组，而无需将角色分配给同一组中的各个用户。以下场景说明了 NSX Manager 如何分配角色。

### 示例：基于角色的访问控制场景

此场景为 IT 网络工程师 (Sally Moore) 提供了对以下环境中 NSX 组件的访问权限。

AD 域: corp.local, vCenter 组: neteng@corp.local, 用户名: smoore@corp.local

必备条件: 已向 NSX Manager 注册了 vCenter Server, 且已配置 SSO。

- 1 向 Sally 分配角色。
  - a 登录到 vSphere Web Client。
  - b 单击**网络和安全**，然后单击 **NSX Manager**。
  - c 在“名称”列中单击 **NSX Manager**，然后单击**管理**选项卡。
  - d 单击**用户**，然后单击**添加**。  
此时将打开“分配角色”窗口。
  - e 单击**指定 vCenter 组**，然后在**组**中键入 neteng@corp.local。
  - f 单击**下一步**。
  - g 在“选择角色”中，单击 **NSX 管理员**，然后单击**下一步**。
- 2 向 Sally 授予数据中心权限。
  - a 单击“主页”图标，然后单击 **vCenter 主页 > 数据中心**。
  - b 选择数据中心，然后单击**操作 > 所有 vCenter 操作 > 添加权限**。
  - c 单击**添加**，然后选择域 **CORP**。
  - d 在**用户和组**中，选择**先显示组**。
  - e 选择 **NetEng**，然后单击**确定**。
  - f 在**分配的角色**中，选择**只读**并取消选择**传播到子项**，然后单击**确定**。
- 3 注销 vSphere Web Client，然后重新以 smoore@corp.local 身份登录。  
Sally 仅可执行 NSX 操作。例如，安装虚拟设备、创建逻辑交换机等。

## 示例：通过用户组成员资格继承权限的场景

组选项	值
名称	G1
分配的角色	审核员（只读）
资源	全局根

用户选项	值
名称	John
属于组	G1
分配的角色	无

John 属于组 G1，该组已被分配审核员角色。John 继承了组角色和资源权限。

## 示例：用户成员属于多个组的场景

组选项	值
名称	G1
分配的角色	审核员（只读）
资源	全局根

组选项	值
名称	G2
分配的角色	安全管理员（读和写）
资源	Datacenter1

用户选项	值
名称	Joseph
属于组	G1、G2
分配的角色	无

Joseph 属于组 G1 和 G2，并且继承了审核员和安全管理员角色的组合权限。例如，John 拥有以下权限：

- 对 Datacenter1 的读、写（安全管理员角色）权限
- 对全局根的只读（审核员）权限

## 示例：用户成员具有多个角色的场景

组选项	值
名称	G1
分配的角色	企业管理员
资源	全局根

用户选项	值
名称	Bob
属于组	G1
分配的角色	安全管理员（读和写）
资源	Datacenter1

Bob 已被分配安全管理员角色，因此他未继承组角色权限。Bob 拥有以下权限

- 对 Datacenter1 及其子资源的读、写（安全管理员角色）权限
- Datacenter1 上的企业管理员角色

## 编辑用户帐户

可以编辑用户帐户来更改角色或范围。但不能编辑 **admin** 帐户。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在“名称”列中单击 **NSX Manager**，然后单击**管理 (Manage)**选项卡。
- 4 单击**用户 (Users)**。
- 5 选择要编辑的用户。
- 6 单击**编辑 (Edit)**。
- 7 根据需要进行更改。
- 8 单击**完成 (Finish)**保存更改。

## 更改用户角色

可以为除 **admin** 用户之外的所有用户更改角色分配。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。

- 3 在“名称”列中单击 **NSX Manager**，然后单击**管理 (Manage)**选项卡。
- 4 单击**用户 (Users)**。
- 5 选择要为其更改角色的用户。
- 6 单击**更改角色 (Change Role)**。
- 7 根据需要进行更改。
- 8 单击**完成 (Finish)**保存更改。

## 禁用或启用用户帐户

可以禁用某个用户帐户，以阻止该用户登录到 **NSX Manager**。无法禁用 **admin** 用户或当前已登录到 **NSX Manager** 的用户。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在“名称”列中单击 **NSX Manager**，然后单击**管理 (Manage)**选项卡。
- 4 单击**用户 (Users)**。
- 5 选择用户帐户。
- 6 单击**启用 (Enable)**或**禁用 (Disable)**图标。

## 删除用户帐户

您可以删除创建的任何用户帐户。但是，不能删除 **admin** 帐户。已删除用户的审核记录会保留在数据库中，并可以在审核日志报告中引用。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在“名称”列中单击 **NSX Manager**，然后单击**管理 (Manage)**选项卡。
- 4 单击**用户 (Users)**。
- 5 选择用户帐户。
- 6 单击**删除 (Delete)**。
- 7 单击**确定 (OK)**确认删除。

如果删除 vCenter 用户帐户，则仅会删除 **NSX Manager** 的角色分配。不会删除 vCenter 上的用户帐户。

## 网络对象和安全对象

本节介绍了自定义网络和安全容器。这些容器可在分布式防火墙和服务编排中使用。在跨 vCenter NSX 环境中，您可以创建要在通用分布式防火墙规则中使用的通用网络和安全容器。您无法在服务编排中使用通用网络和安全对象。

本章讨论了以下主题：

- 使用 IP 地址组
- 使用 MAC 地址组
- 使用 IP 池
- 使用安全组
- 使用服务和服务组

### 使用 IP 地址组

#### 创建 IP 地址组

可以创建一个 IP 地址组，然后将该组作为源或目标添加到防火墙规则中。该规则可帮助保护物理机不受虚拟机的影响，反之亦然。

##### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单** 下的 **NSX Manager**。
- 3 在 **名称** 列中单击 **NSX Manager**，然后单击 **管理** 选项卡。
  - ◆ 如果需要管理通用 IP 地址组，必须选择主 NSX Manager。
- 4 单击 **分组对象** 选项卡，然后单击 **IP 集**。
- 5 单击 **添加 (+)** 图标。
- 6 键入地址组名称。
- 7 （可选）键入地址组描述。
- 8 键入要包含在组中的 IP 地址。

- 9 （可选）选择**启用继承**以便可在基础范围内可见。
- 10 （可选）选择**标记此对象待进行通用同步**以创建通用 IP 地址组。
- 11 单击**确定**。

## 编辑 IP 地址组

### 前提条件

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称**列中单击 **NSX Manager**，然后单击**管理**选项卡。
  - ◆ 如果需要管理通用 IP 地址组，必须选择主 NSX Manager。
- 4 单击**分组对象**选项卡，然后单击 **IP 集**。
- 5 选择要编辑的组，然后单击**编辑 (Edit)** () 图标。
- 6 在“编辑 IP 集”对话框中，进行适当的更改。
- 7 单击**确定 (OK)**。

## 删除 IP 地址组

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称**列中单击 **NSX Manager**，然后单击**管理**选项卡。
  - ◆ 如果需要管理通用 IP 地址组，必须选择主 NSX Manager。
- 4 单击**分组对象 (Grouping Objects)**选项卡，然后单击 **IP 集 (IP Sets)**。
- 5 选择要删除的组，然后单击**删除 (Delete)** () 图标。

## 使用 MAC 地址组

### 创建 MAC 地址组

可以创建由一系列 MAC 地址组成的 MAC 地址组，然后在分布式防火墙规则中将该组作为源或目标添加。该规则可帮助保护物理机不受虚拟机的影响，反之亦然。

### 步骤

- 1 登录到 vSphere Web Client。

- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称**列中单击 **NSX Manager**，然后单击**管理**选项卡。
  - ◆ 如果需要管理通用 MAC 地址组，必须选择主 NSX Manager。
- 4 单击**分组对象 (Grouping Objects)**选项卡，然后单击 **MAC 集 (MAC Sets)**。
- 5 单击**添加 (+)** 图标。
- 6 键入地址组名称。
- 7 （可选）键入地址组描述。
- 8 键入要包含在组中的 MAC 地址。
- 9 （可选）选择**启用继承**以便可在**基础范围**内可见。
- 10 （可选）选择**标记此对象待进行通用同步**以创建通用 MAC 地址组。
- 11 单击**确定 (OK)**。

## 编辑 MAC 地址组

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称**列中单击 **NSX Manager**，然后单击**管理**选项卡。
  - ◆ 如果需要管理通用 MAC 地址组，必须选择主 NSX Manager。
- 4 单击**分组对象 (Grouping Objects)**选项卡，然后单击 **MAC 集 (MAC Sets)**。
- 5 选择要编辑的组，然后单击**编辑 (Edit) (✎)** 图标。
- 6 在“编辑 MAC 集”对话框中，进行适当的更改。
- 7 单击**确定 (OK)**。

## 删除 MAC 地址组

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称**列中单击 **NSX Manager**，然后单击**管理**选项卡。
  - ◆ 如果需要管理通用 MAC 地址组，必须选择主 NSX Manager。
- 4 单击**分组对象 (Grouping Objects)**选项卡，然后单击 **MAC 集 (MAC Sets)**。
- 5 选择要删除的组，然后单击**删除 (Delete) (✖)** 图标。

## 使用 IP 池

可以编辑或删除 IP 池。

有关添加 IP 池的信息，请参见[配置网络访问 SSL VPN-Plus](#) 或[配置 Web Access SSL VPN-Plus](#)。

## 创建 IP 池

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称列**中单击 **NSX Manager**，然后单击**管理**选项卡。
- 4 单击**分组对象 (Grouping Objects)**选项卡，然后单击 **IP 池 (IP Pool)**。
- 5 单击**添加新的 IP 池 (Add New IP Pool)**图标。
- 6 键入 IP 池的名称并键入默认网关和前缀长度。
- 7 （可选）键入主要 DNS、辅助 DNS 以及 DNS 后缀。
- 8 键入要包含在池中的 IP 地址范围，然后单击**确定 (OK)**。

## 编辑 IP 池

可以编辑 IP 池，但不能编辑 CIDR 和网关。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称列**中单击 **NSX Manager**，然后单击**管理**选项卡。
- 4 单击**分组对象 (Grouping Objects)**选项卡，然后单击 **IP 池 (IP Pools)**。
- 5 选择 IP 池并单击**编辑 (Edit)**图标。
- 6 进行相应更改，然后单击**确定 (OK)**。

## 删除 IP 池

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称列**中单击 **NSX Manager**，然后单击**管理**选项卡。
- 4 单击**分组对象 (Grouping Objects)**选项卡，然后单击 **IP 池 (IP Pool)**。



- 5 选择要删除的 IP 池，然后单击**删除 (Delete)**图标。

## 使用安全组

安全组是 vSphere 清单中的资产或分组对象的集合。

### 创建安全组

可以在 NSX Manager 级别创建安全组。

#### 前提条件

如果您正在根据 Active Directory 组对象创建安全组，请确保已向 NSX Manager 注册了一个或多个域。NSX Manager 从向其注册的每个域获取组 and 用户信息以及两者之间的关系。请参见[向 NSX Manager 注册 Windows 域](#)。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称**列中单击 NSX Manager，然后单击**管理**选项卡。
  - ◆ 如果需要管理通用安全组，必须选择主 NSX Manager。
- 4 依次单击**分组对象 (Grouping Objects)**选项卡、**安全组 (Security Group)**和**添加安全组 (Add Security Group)**图标。
- 5 键入此安全组的名称和描述（可选）。
- 6 （可选）如果需要创建通用安全组，请选择**标记此对象待进行通用同步 (Mark this object for universal synchronization)**。
- 7 单击**下一步 (Next)**。
- 8 在“动态成员资格”页面上，定义对象要添加到所创建安全组所需具备的条件。这样，您可以通过使用支持的大量参数定义筛选条件以匹配搜索条件来包含虚拟机。

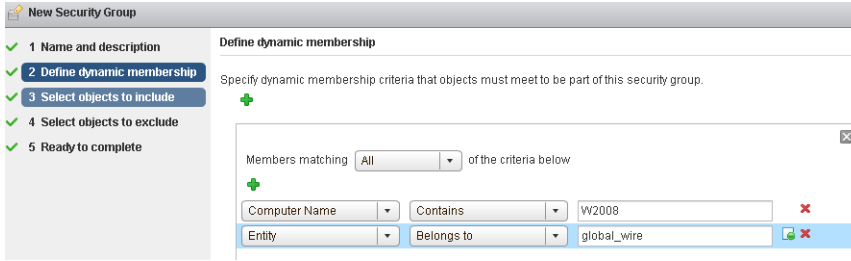
---

**注** 如果您正在创建通用安全组，则**定义动态成员资格**步骤不可用。

---

例如，您可以加入一个条件，将标记有指定安全标记（如 AntiVirus.virusFound）的所有虚拟机添加到安全组中。安全标记区分大小写。

或者，可以将所有包含名称 w2008 的虚拟机以及位于逻辑交换机 global\_wire 中的虚拟机添加到安全组中。



9 单击下一步 (Next)。

10 在“选择要包括的对象”页面上，选择要添加的资源所对应的选项卡，并选择一个或多个要添加到安全组中的资源。可以在安全组中包括以下对象。

表 22-1. 安全组和通用安全组中可以包括的对象。

安全组	通用安全组
<ul style="list-style-type: none"> <li>其他安全组（可以嵌入正在创建的安全组）。</li> <li>群集</li> <li>逻辑交换机</li> <li>网络</li> <li>虚拟应用程序</li> <li>数据中心</li> <li>IP 集</li> <li>目录组</li> </ul>	<ul style="list-style-type: none"> <li>其他通用安全组（可以嵌入正在创建的通用安全组）。</li> <li>通用 IP 集</li> <li>通用 MAC 集</li> </ul>
<p><b>注</b> NSX 安全组的 Active Directory 配置不同于 vSphere SSO 的 AD 配置。NSX AD 组配置用于供最终用户访问客户机虚拟机，而 vSphere SSO 用于供管理员使用 vSphere 和 NSX。要使用这些目录组，您必须与 Active Directory 进行同步。请参见第 11 章，身份防火墙概述。</p>	
<ul style="list-style-type: none"> <li>MAC 集</li> <li>安全标记</li> <li>虚拟网卡</li> <li>虚拟机</li> <li>资源池</li> <li>分布式虚拟端口组</li> </ul>	

此处选定的对象无论是否满足第 8 步 中的条件，都将包含在安全组中。

将资源添加到安全组时，将自动添加所有关联的资源。例如，选择虚拟机后，关联的虚拟网卡将自动添加到安全组中。

11 单击下一步 (Next)，然后选择要从安全组中排除的对象。

**注** 如果您正在创建通用安全组，则选择要排除的对象 步骤不可用。

此处选定的对象无论是否满足动态条件，都将从安全组中排除。

12 单击完成 (Finish)。

将按下列方式确定安全组的成员资格：

{表达式结果（源自第 8 步）+ 包含项（在第 10 步中指定）}- 排除项（在第 11 步中指定）

这意味着，首先会将包含项与表达式结果相加。然后，将从组合结果中减去排除项。

## 编辑安全组

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称**列中单击 **NSX Manager**，然后单击**管理**选项卡。
  - ◆ 如果需要管理通用安全组，必须选择主 **NSX Manager**。
- 4 单击**分组对象**选项卡，然后单击**安全组**。
- 5 选择要编辑的组，然后单击**编辑** (✎) 图标。
- 6 在“编辑安全组”对话框中，进行适当的更改。
- 7 单击**确定**。

## 删除安全组

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称**列中单击 **NSX Manager**，然后单击**管理**选项卡。
  - ◆ 如果需要管理通用安全组，必须选择主 **NSX Manager**。
- 4 单击**分组对象 (Grouping Objects)**选项卡，然后单击**安全组 (Security Group)**。
- 5 选择要删除的组，然后单击**删除 (Delete)** (✖) 图标。

## 使用服务和服务组

服务是协议-端口组合，服务组是由服务或其他服务组构成的组。

## 创建服务

可以创建一个服务，然后为该服务定义规则。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。

- 3 在**名称**列中单击 **NSX Manager**，然后单击**管理**选项卡。
  - ◆ 如果需要管理通用服务，必须选择主 **NSX Manager**。
- 4 单击**分组对象 (Grouping Objects)**选项卡，然后单击**服务 (Service)**。
- 5 单击**添加 (+)**图标。
- 6 键入用来标识该服务的**名称 (Name)**。
- 7 （可选）键入对服务的**描述 (Description)**。
- 8 选择**协议 (Protocol)**。
  - a 视所选协议而定，系统可能提示您输入更多信息，如目标端口。
- 9 （可选）选择**启用继承**以便可在**基础范围内**可见。
- 10 （可选）选择**标记此对象待进行通用同步**以创建通用服务。
- 11 单击**确定 (OK)**。

该服务会显示在“服务”表中。

## 创建服务组

您可以创建服务组，然后为该服务组定义规则。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称**列中单击 **NSX Manager**，然后单击**管理**选项卡。
  - ◆ 如果需要管理通用服务组，必须选择主 **NSX Manager**。
- 4 单击**分组对象 (Grouping Objects)**选项卡，然后单击**服务组 (Service Groups)**。
- 5 单击**添加 (Add)**图标。
- 6 键入用来标识服务组的**名称 (Name)**。
- 7 （可选）键入服务组的**描述 (Description)**。
- 8 （可选）选择**标记此对象待进行通用同步**以创建通用服务组。
- 9 在“成员”中，选择要添加到组中的服务或服务组。
- 10 （可选）选择**启用继承**以便可在**基础范围内**可见。
- 11 单击**确定 (OK)**。

## 编辑服务或服务组

您可以编辑服务和服务组。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称**列中单击 **NSX Manager**，然后单击**管理**选项卡。
  - ◆ 如果需要管理通用服务或服务组，必须选择主 NSX Manager。
- 4 单击**分组对象 (Grouping Objects)**选项卡，然后单击**服务 (Service)**或**服务组 (Service Groups)**。
- 5 选择自定义服务或服务组，然后单击**编辑 (Edit)** () 图标。
- 6 进行适当更改。
- 7 单击**确定 (OK)**。

## 删除服务或服务组

您可以删除服务或服务组。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称**列中单击 **NSX Manager**，然后单击**管理**选项卡。
  - ◆ 如果需要管理通用服务或服务组，必须选择主 NSX Manager。
- 4 单击**分组对象 (Grouping Objects)**选项卡，然后单击**服务 (Service)**或**服务组 (Service Groups)**。
- 5 选择自定义服务或服务组，然后单击**删除 (Delete)** () 图标。
- 6 单击**是 (Yes)**。

该服务或服务组将被删除。

## 操作和管理

本章讨论了以下主题：

- 更改控制器密码
- 从 NSX Controller 故障恢复
- 更改 VXLAN 端口
- 检查通信通道运行状况
- 客户体验改进计划
- 系统事件和审核日志
- 管理系统设置
- 使用 SNMP 陷阱
- NSX 备份和还原
- 流量监控
- 活动监控
- 跟踪流

### 更改控制器密码

为确保数据安全，您可以更改 NSX Controller 的密码。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全**，然后单击**安装**。
- 3 在“管理”下，选择要更改其密码的控制器。
- 4 单击**操作**，然后单击**更改控制器群集密码**。
- 5 键入新密码，然后单击**确定**。

控制器密码现已更改。

## 从 NSX Controller 故障恢复

当出现 NSX Controller 故障时，可能仍有两个控制器正在工作。此时保持着群集多数，并且控制层面仍继续正常工作。尽管如此，您也必须将三个控制器全部删除并添加新的控制器，以便维护完全正常工作的三节点群集。

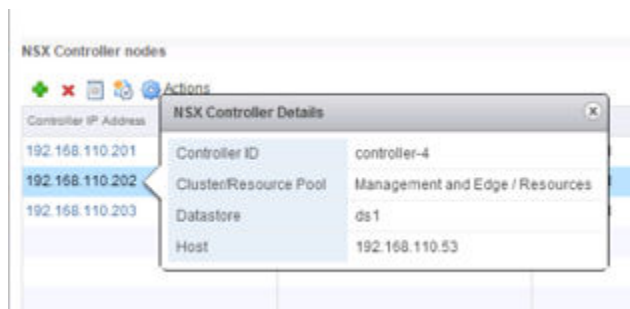
当一个或多个控制器遇到不可恢复的灾难性错误，或者一个或多个控制器虚拟机变为无法访问并且无法修复时，建议删除控制器群集。

在这种情况下，虽然部分控制器看似运行良好，我们也建议删除所有控制器。建议的过程是先创建新的控制器群集，然后在 NSX Manager 上使用“更新控制器状态”机制将状态同步到控制器。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 从 **网络和安全** 中，单击**安装 > 管理**。
- 3 在“NSX Controller 节点”部分中，单击每个控制器并获取详细信息屏幕的屏幕截图/打印屏幕，或者记下配置信息以供将来参考。

例如：

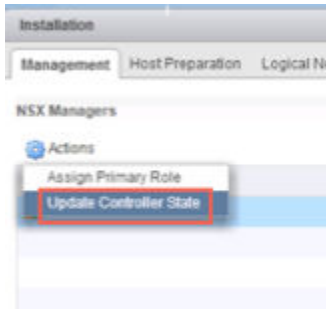


- 4 在“NSX Controller 节点”部分中，将三个节点全部删除，方法是选择每个节点并单击**删除节点 (x)** 图标。

当系统中不存在任何控制器时，主机将在所谓的“无头”模式下工作。新虚拟机或已执行 vMotion 操作的虚拟机将遇到网络问题，直至部署了新的控制器并且同步已完成为止。

- 5 部署三个新的 NSX Controller 节点，方法是单击**添加节点 (+)** 图标。
- 6 在“添加控制器”对话框中，选择要添加节点的数据中心，然后配置控制器设置。
  - a 选择适当的群集。
  - b 在群集和存储中选择一个主机。
  - c 选择分布式端口组。
  - d 选择要将其中的 IP 地址分配给节点的 IP 池。
  - e 单击**确定**，等待安装完成，并确保所有节点的状态均为“正常”。

7 重新同步控制器状态，方法是单击**操作 > 更新控制器状态**。



更新控制器状态将当前 VXLAN 和分布式逻辑路由器配置（包括跨 VC NSX 部署中的通用对象）从 NSX Manager 推送到控制器群集。

## 更改 VXLAN 端口

您可以更改用于 VXLAN 流量的端口。

从 NSX 6.2.3 开始，默认 VXLAN 端口为 4789，这是 IANA 分配的标准端口。在 NSX 6.2.3 之前，默认 VXLAN UDP 端口号为 8472。

任何新的 NSX 安装将 UDP 端口 4789 用于 VXLAN。

如果升级到 NSX 6.2.3，并且安装在升级之前使用旧默认值 (8472) 或自定义端口号（如 8888），将在升级后继续使用该端口，除非您对其进行了更改。

如果您的升级安装使用或将使用硬件 VTEP 网关（ToR 网关），则必须切换到 VXLAN 端口 4789。

跨 vCenter NSX 不要求将 4789 用于 VXLAN 端口，但必须将跨 vCenter NSX 环境中的所有主机配置为使用相同的 VXLAN 端口。如果切换到端口 4789，这会确保添加到跨 vCenter NSX 环境中的任何新 NSX 安装使用与现有 NSX 部署相同的端口。

更改 VXLAN 端口是通过一个包含三个阶段的过程完成的，并且不会中断 VXLAN 流量。在跨 vCenter NSX 环境中，更改将传播到跨 vCenter NSX 环境中的所有 NSX Manager 设备和所有主机。

### 前提条件

- 确认防火墙未阻止要用于 VXLAN 的端口。
- 确认在更改 VXLAN 端口时未同时运行主机准备。

### 步骤

- 1 单击**逻辑网络准备 (Logical Network Preparation)**选项卡，然后单击**VXLAN 传输 (VXLAN Transport)**。
- 2 在“VXLAN 端口”面板中，单击**更改 (Change)**按钮。输入要切换到的端口。4789 是 IANA 为 VXLAN 分配的端口。

将端口更改传播到所有主机需要很短的时间。



- 3 （可选）使用 GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus API 请求检查端口更改进度。

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
 <prevPort>8472</prevPort>
 <targetPort>4789</targetPort>
 <taskPhase>PHASE_TW0</taskPhase>
 <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

...

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
 <prevPort>8472</prevPort>
 <targetPort>4789</targetPort>
 <taskPhase>FINISHED</taskPhase>
 <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

## 检查通信通道运行状况

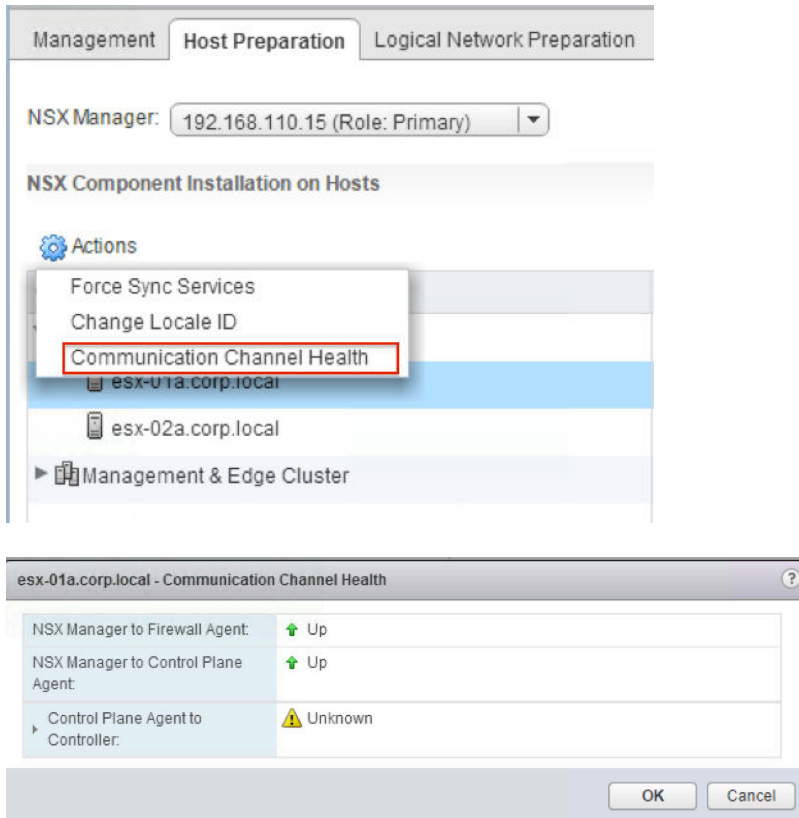
NSX 会检查 NSX Manager 和防火墙代理、NSX Manager 和控制层面代理以及控制层面代理和控制器之间的通信状态。

### 步骤

- 1 在 vSphere Web Client 中，导航到**网络和安全 (Networking & Security) > 安装 (Installation) > 主机准备 (Host Preparation)**。

- 2 选择群集或展开群集，并选择主机。单击**操作 (Actions)** (⚙️)，然后单击**通信通道运行状况 (Communication Channel Health)**。

随即显示通信通道运行状况信息。



## 客户体验改进计划

NSX 参与 VMware 的客户体验改进计划 (CEIP)。

有关通过 CEIP 收集的数据以及 VMware 使用该数据的用途的详情，请参见 Trust & Assurance Center 中的规定：<http://www.vmware.com/trustvmware/ceip.html>。

要加入或退出 NSX CEIP 或编辑计划设置，请参见[编辑客户体验改进计划选项](#)。

## 编辑客户体验改进计划选项

在安装或升级 NSX Manager 时，您可以选择加入 CEIP。您可以在以后加入或退出 CEIP。您还可以定义收集信息的频率和日期。

### 前提条件

- 确认连接了 NSX Manager 并且可以与 vCenter Server 同步。
- 确认在 NSX Manager 上配置了 DNS。
- 确认将 NSX 连接到公共网络以上载数据。

## 步骤

- 1 登录到 vSphere Web Client。
- 2 选择**网络和安全 (Networking & Security)**。
- 3 在“网络和安全清单”中，选择 **NSX Manager (NSX Managers)**。
- 4 双击要修改的 NSX Manager。
- 5 单击**摘要 (Summary)**选项卡。
- 6 在“客户体验改进计划”对话框中，单击**编辑 (Edit)**。
- 7 选择或取消选择**加入 VMware 客户体验改进计划 (Join the VMware Customer Experience Improvement Program)**选项。
- 8 （可选）配置重复周期设置。
- 9 单击**确定 (OK)**。

## 系统事件和审核日志

系统事件指与 NSX 操作有关的事件。引入系统事件可详细说明每个操作事件。这些事件可能与基本操作（信息事件）或重要错误（重要事件）相关。

借助 NSX 票证记录器功能，您可以使用票证 ID 跟踪所做的更改。对于用票证跟踪的操作，审核日志中将包含票证 ID。

## 关于 NSX 日志

本节介绍如何配置 syslog 服务器并查看每个 NSX 组件的技术支持日志。管理层面日志可通过 NSX Manager 获取，而数据层面日志可通过 vCenter Server 获取。因此，建议您为 NSX 组件和 vCenter Server 指定同一 syslog 服务器，以便在查看 syslog 服务器上的日志时获得完整的信息。

有关配置 vCenter Server 中托管主机的 syslog 的详细信息，请参见 VMware vSphere ESXi 和 vCenter Server 5.5 文档。

---

**注** 用于收集日志和访问 NSX 分布式逻辑路由器 (DLR) 控制虚拟机的 syslog 或跳转服务器不能位于直接连接到该 DLR 的逻辑接口的逻辑交换机上。

---

### NSX Manager

要指定 syslog 服务器，请参见[指定 syslog 服务器](#)。

要下载技术支持日志，请参见[下载 NSX 的技术支持日志](#)。

### NSX Edge

要指定 syslog 服务器，请参见[配置远程 Syslog 服务器](#)。

要下载技术支持日志，请参见[下载 NSX Edge 的技术支持日志](#)。

## 防火墙

必须为每个启用了防火墙的群集配置远程 **syslog** 服务器。远程 **syslog** 服务器在 **Syslog.global.logHost** 属性中指定。请参见《ESXi 和 vCenter Server 5.5 文档》。

以下是主机日志文件中的示例行。

```
2013-10-02T05:41:12.670Z cpu11:1000046503)vsip_pkt: INET, match, PASS, Rule 0/3, Ruleset domain-c7, Rule ID 100, OUT, Len 60, SRC 10.24.106.96, DST 10.24.106.52, TCP SPORT 59692, DPORT 22 S
```

其中包含三个部分：

**表 23-1. 日志文件条目中的各部分**

	示例中的值
VMKernel 常见日志部分包含日期、时间、CPU 和 WorldID	2013-10-02T05:41:12.670Z cpu11:1000046503)
标识符	vsip_pkt
防火墙特定部分	INET, match, PASS, Rule 0/3, Ruleset domain-c7, Rule ID 100, OUT, Len 60, SRC 10.24.106.96, DST 10.24.106.52, TCP SPORT 59692, DPORT 22 S

**表 23-2. 日志文件条目的防火墙特定部分**

实体	可能值
AF 值	INET、INET6
原因	可能值：match、bad-offset、fragment、short、normalize、memory、bad-timestamp、congestion、ip-option、proto-cksum、state-mismatch、state-insert、state-limit、src-limit、synproxy 和 spoofguard
操作	PASS、DROP、SCRUB、NOSCRUB、NAT、NONAT、BINAT、NOBINAT、RDR、NORDR、SYNPROXY_DROP、PUNT、REDIRECT 和 COPY
规则标识符	<i>Identifier</i>
规则值	规则集 ID 和规则位置（内部详细信息）
规则集标识符	<i>Identifier</i>
规则集值	规则集名称
规则 ID 标识符	<i>Identifier</i>
规则 ID	匹配的 ID
方向	ROUT、IN
长度标识符	“Len” 后跟变量
长度值	数据包长度
源标识符	SRC
源 IP 地址	<i>IP address</i>
目标标识符	<i>IP address</i>
协议	TCP、UDP 和 PROTO
源端口标识符	SPORT

表 23-2. 日志文件条目的防火墙特定部分（续）

实体	可能值
源端口	TDP 和 UDP 的源端口号
源端口标识符	目标端口标识符
目标端口	TDP 和 UDP 的目标端口号
标记	TCP 的标记

## 使用 NSX 票证记录器

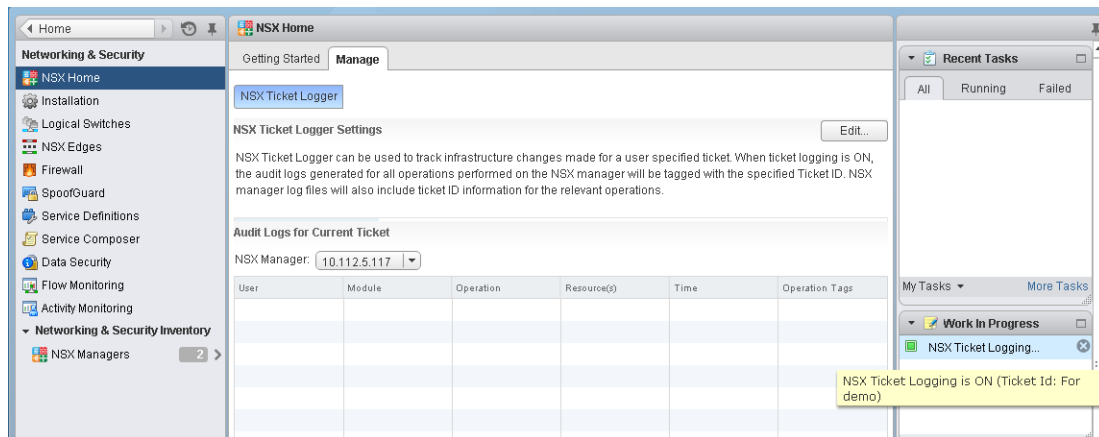
NSX 票证记录器允许您跟踪对基础架构所做的更改。所有操作都将使用指定的票证 ID 进行标记，并且这些操作的审核日志将包括该票证 ID。这些操作的日志文件都将使用相同的票证 ID 进行标记。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**管理 (Manage)**选项卡。
- 3 单击 **NSX 票证记录器设置 (NSX Ticket Logger Settings)**旁边的**编辑 (Edit)**。
- 4 键入一个票证 ID，然后单击**打开 (Turn On)**。

此时在 vSphere Web Client 窗口的右侧将显示“NSX 票证记录”窗格。在当前 UI 会话中执行的操作的审核日志中，将在**操作标记 (Operation Tags)**列中包含该票证 ID。

图 23-1. “NSX 票证记录器”窗格



如果 vSphere Web Client 管理了多个 vCenter Server，则该票证 ID 用于登录所有适用的 NSX Manager。

### 后续步骤

票证记录基于会话。如果您在启用票证记录的情况下注销或者会话丢失，则当您重新登录 UI 时，将默认关闭票证记录。完成票证的操作后，重复第 2 步和第 3 步并单击**关闭 (Turn Off)**来关闭记录。

## 查看系统事件报告

从 vSphere Web Client 中，您可以查看由 NSX Manager 管理的所有组件的系统事件。

**步骤**

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单** 下的 **NSX Manager**。
- 3 在 **名称** 列中单击 **NSX Manager**，然后单击 **监控** 选项卡。
- 4 单击 **系统事件** 选项卡。

您可以单击列标题中的箭头对事件进行排序，也可以使用**筛选器**文本框筛选事件。

## NSX Manager 虚拟设备事件

以下事件特定于 NSX Manager 虚拟设备。

**表 23-3. NSX Manager 虚拟设备事件**

	关闭电源	打开电源	界面关闭	界面启动
本地 CLI	运行 show log follow 命令。	运行 show log follow 命令。	运行 show log follow 命令。	运行 show log follow 命令。
GUI	不适用	不适用	不适用	不适用

**表 23-4. NSX Manager 虚拟设备事件**

	CPU	内存	存储器
本地 CLI	运行 show process monitor 命令。	运行 show system memory 命令。	运行 show filesystem 命令。
GUI	不适用	不适用	不适用

## 关于 Syslog 格式

syslog 中记录的系统事件消息的结构如下。

```
syslog header (timestamp + hostname + sysmgr/)
Timestamp (from the service)
Name/value pairs
Name and value separated by delimiter ':' (double colons)
Each name/value pair separated by delimiter ';' (double semi-colons)
```

系统事件的字段和类型包含以下信息。

```
Event ID :: 32 bit unsigned integer
Timestamp :: 32 bit unsigned integer
Application Name :: string
Application Submodule :: string
Application Profile :: string
Event Code :: integer (possible values: 10007 10016 10043 20019)
Severity :: string (possible values: INFORMATION LOW MEDIUM HIGH CRITICAL)
Message ::
```

## 查看审核日志

审核日志提供的视图中列出所有 NSX Manager 用户执行操作。NSX Manager 最多保留 1,000,000 条审核日志。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称**列中，单击某个 NSX 服务器，然后单击**监控**选项卡。
- 4 单击**审核日志**选项卡。
- 5 如果该审核日志有详细信息，则可以单击**操作**列中该日志所对应的文本。要查看某一审核日志的详细信息，请单击**操作**列中的文本。
- 6 在**审核日志更改详细信息**中，选择**已更改的行**可以仅显示因该审核日志操作而值发生变化的属性。

## 管理系统设置

您可以编辑 vCenter Server、DNS 和 NTP 服务器，以及在初始登录过程中指定的查询服务器。NSX Manager 需要与 vCenter Server 和服务（例如 DNS 和 NTP）进行通信，以提供有关 VMware Infrastructure 清单的详细信息。

## 登录到 NSX Manager 虚拟设备

安装和配置 NSX Manager 虚拟机后，登录 NSX Manager 虚拟设备以查看安装期间指定的设置。

### 步骤

- 1 打开 Web 浏览器窗口并键入分配给 NSX Manager 的 IP 地址。例如，**https://192.168.110.42**。  
NSX Manager 用户界面将使用 SSL 在 Web 浏览器窗口中打开。
- 2 接受安全证书。

---

**注** 可以使用 SSL 证书进行身份验证。

---

此时将显示 NSX Manager 登录屏幕。

- 3 使用用户名 **admin** 和安装期间设置的密码登录到 NSX Manager 虚拟设备。
- 4 单击**登录 (Log In)**。

## 编辑 NSX Manager 日期和时间

您可以更改在首次登录期间指定的 NTP 服务器。

### 步骤

- 1 登录到 NSX Manager 虚拟设备。

- 2 在设备管理 (Appliance Management) 下面，单击管理设备设置 (Manage Appliance Settings)。
- 3 单击时间设置 (Time Settings) 旁边的编辑 (Edit)。
- 4 进行适当更改。
- 5 单击确定 (OK)。
- 6 重新引导 NSX Manager。

## 指定 syslog 服务器

如果指定了 syslog 服务器，则 NSX Manager 会将所有审核日志和系统事件发送至 syslog 服务器。

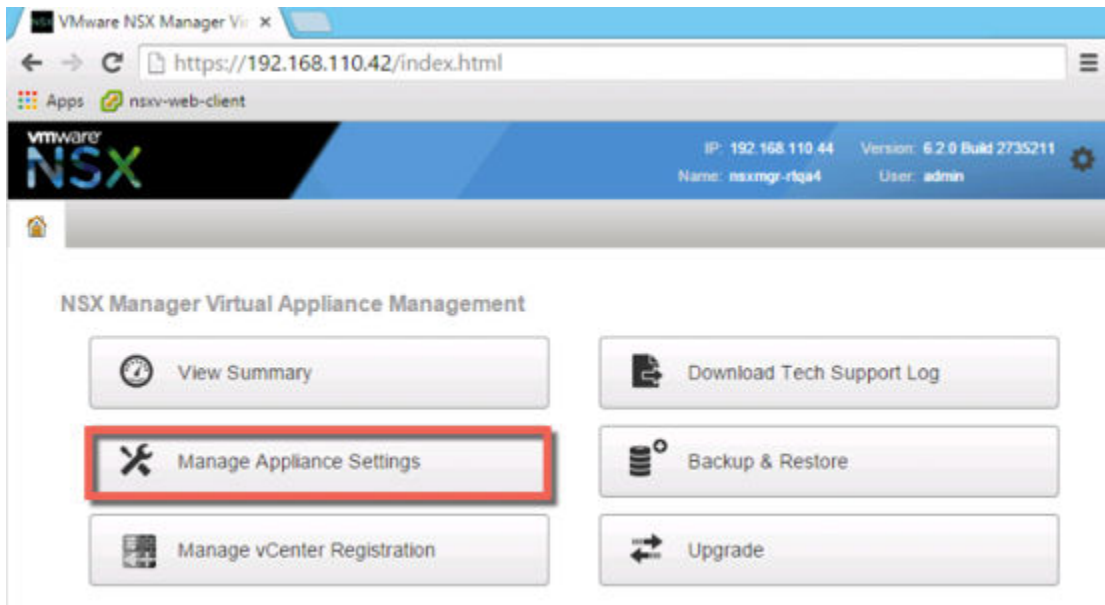
syslog 数据有助于进行故障排除以及查看安装和配置期间记录的数据。

NSX Edge 支持两个 syslog 服务器。NSX Manager 和 NSX Controller 支持一个 syslog 服务器。

### 步骤

- 1 在 Web 浏览器中，导航到 NSX Manager 设备 GUI: <https://<nsx-manager-ip>> 或 <https://<nsx-manager-hostname>>。
- 2 使用在 NSX Manager 安装期间配置的 admin 和密码登录。
- 3 单击管理设备设置 (Manage Appliance Settings)。

例如：



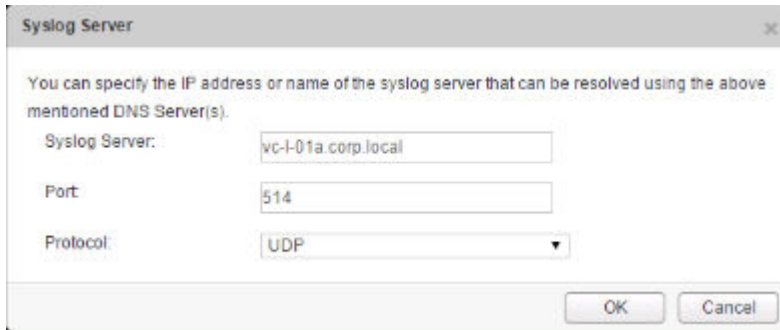
- 4 在“设置”面板中，单击常规 (General)。
- 5 单击 Syslog 服务器 (Syslog Server) 旁边的编辑 (Edit)。



- 键入 **syslog** 服务器的 IP 地址或主机名、端口和协议。

如果不指定端口，则会使用 **syslog** 服务器的 IP 地址/主机名的默认 UDP 端口。

例如：



- 单击 **确定 (OK)**。

vCenter Server 远程日志记录已启用，并且日志存储在单独的 **syslog** 服务器中。

## 编辑 DNS 服务器

可以更改在 Manager 安装期间指定的 DNS 服务器。

### 步骤

- 登录到 NSX Manager 虚拟设备。
- 在 **设备管理 (Appliance Management)** 下面，单击 **管理设备设置 (Manage Appliance Settings)**。
- 在“设置”面板中，单击 **网络 (Network)**。
- 单击 **DNS 服务器 (DNS Servers)** 旁边的 **编辑 (Edit)**。
- 进行适当更改。
- 单击 **确定 (OK)**。

## 编辑 Lookup Service 详细信息

您可以更改在首次登录期间指定的 Lookup Service 详细信息。

### 步骤

- 登录到 NSX Manager 虚拟设备。
- 在 **设备管理 (Appliance Management)** 下面，单击 **管理设备设置 (Manage Appliance Settings)**。
- 在“设置”面板中，单击 **NSX 管理服务 (NSX Management Service)**。
- 单击 **Lookup Service** 旁的 **编辑 (Edit)**。
- 进行适当更改。
- 单击 **确定 (OK)**。

## 编辑 vCenter Server

您可以更改安装过程中向其注册 NSX Manager 的 vCenter Server。仅在更改当前 vCenter Server 的 IP 地址时才应进行该操作。

### 步骤

- 1 如果已登录到 vSphere Web Client，请注销。
- 2 登录到 NSX Manager 虚拟设备。
- 3 在**设备管理 (Appliance Management)**下面，单击**管理设备设置 (Manage Appliance Settings)**。
- 4 在“设置”面板中，单击 **NSX 管理服务 (NSX Management Service)**。
- 5 单击 **vCenter Server (Edit)** 旁的**编辑 (vCenter Server)**。
- 6 进行适当更改。
- 7 单击**确定 (OK)**。

## 下载 NSX 的技术支持日志

可以将 NSX Manager 系统日志和 Web Manager 日志下载到桌面。

### 步骤

- 1 登录到 NSX Manager 虚拟设备。
- 2 在“设备管理”下方，单击**管理设备设置**。
- 3 单击 ，然后单击**下载技术支持日志**。
- 4 单击**下载**。
- 5 日志准备就绪后，单击**保存**将日志下载到桌面上。

该日志已压缩，其文件扩展名为 **.gz**。

### 后续步骤

您可以在保存文件的目录中浏览查找**所有文件**，然后使用解压缩实用程序打开该日志。

## NSX Manager SSL 证书

NSX Manager 需要使用已签名证书来验证 NSX Manager Web 服务的身份以及对发送到 NSX Manager Web 服务器的信息进行加密。此过程的必要步骤包括：生成证书签名请求 (CSR)，将该请求提交给 CA 进行签署以及将已签名的 SSL 证书导入到 NSX Manager 中。作为安全方面的最佳实践，您应该使用生成证书选项生成私钥和公钥，其中私钥应保存到 NSX Manager。

要获取 NSX Manager 证书，您可以使用 NSX Manager 的内置 CSR 生成器，也可以使用诸如 OpenSSL 等其他工具。

使用 NSX Manager 的内置 CSR 生成器生成的 CSR 无法包含诸如主题备用名称 (SAN) 等扩展属性。如果要包含扩展属性，您必须使用其他 CSR 生成工具。如果要使用诸如 OpenSSL 等其他工具生成 CSR，则过程如下：1) 生成 CSR，2) 提交该请求以进行签署，3) 继续执行[将 NSX Manager 证书文件转换为 PKCS#12 格式](#)一节所述的步骤。

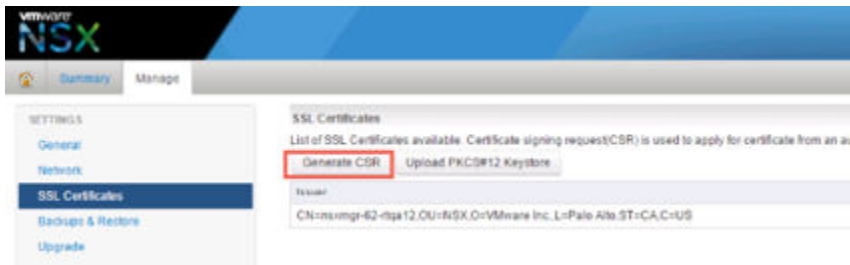
## 使用内置 CSR 生成器

为 NSX Manager 获取 SSL 证书的方法之一是使用内置 CSR 生成器。

此方法的局限是 CSR 无法包含诸如主题备用名称 (SAN) 等扩展属性。如果要包含扩展属性，您必须使用其他 CSR 生成工具。如果您使用的是其他 CSR 生成工具，请跳过此过程。

### 步骤

- 1 登录到 NSX Manager 虚拟设备。
- 2 单击**管理设备设置 (Manage Appliance Settings)**。
- 3 在“设置”面板中，单击**SSL 证书 (SSL Certificates)**。
- 4 单击**生成 CSR (Generate CSR)**。



- 5 通过填充以下字段填写表单：

选项	操作
密钥大小 (Key Size)	选择在选定算法中使用的密钥长度。
公用名称 (Common Name)	键入 NSX Manager 的 IP 地址或完全限定域名 (FQDN)。VMware 建议您输入 FQDN。
组织单位 (Organization Unit)	输入订购该证书的公司部门。
组织名称 (Organization Name)	输入公司的法定全称。
城市名称 (City Name)	输入公司所在城市的全称。
省/自治区/直辖市名称 (State Name)	输入公司所在省/市/自治区的全称。
国家/地区代码 (Country Code)	输入代表您所在国家/地区的两位数代码。例如，美国的代码为 US。

- 6 单击**确定 (OK)**。
- 7 将 CSR 发送给 CA 进行签名。
  - a 通过单击**下载 CSR (Download CSR)** 下载生成的请求。  
通过使用此方法，NSX Manager 永远不会丢失私钥。
  - b 将此请求提交到 CA。

- c 获取已签名证书和根 CA 证书以及任何 PEM 格式的中间 CA 证书。
- d 使用以下 OpenSSL 命令将 CER/DER 格式的证书转换为 PEM 格式：

```
openssl x509 -inform der -in Cert.cer -out 4-nsx_signed.pem
```

- e 将所有证书（服务器证书、中间证书和根证书）联接在文本文件中。
- f 在 NSX Manager UI 中，单击**导入 (Import)**，然后浏览至包含所有证书的文本文件。
- g 导入成功后，服务器证书和所有 CA 证书将显示在“SSL 证书”页面上。

#### 后续步骤

将已签名 SSL 证书导入到 NSX Manager 中。

### 将 NSX Manager 证书文件转换为 PKCS#12 格式

如果已使用其他工具（例如 OpenSSL）获取 NSX Manager 证书，请确保证书和私钥为 PKCS#12 格式。如果 NSX Manager 证书和私钥不是 PKCS#12 格式，则必须先转换才能将其导入到 NSX Manager 中。

#### 前提条件

验证系统上是否已安装 OpenSSL。您可以从 <http://www.openssl.org> 下载 openssl。

#### 步骤

- ◆ 从授权签名机构收到签名证书后，使用 OpenSSL 并根据证书文件和私钥生成 PKCS#12（.pfx 或 .p12）密钥库文件。

例如：

```
openssl pkcs12 -export -out server.p12 -inkey server.key -in server.crt -certfile CACert.crt
```

在此示例中，CACert.crt 是证书颁发机构返回的根证书的名称。

#### 后续步骤

将已签名 SSL 证书导入到 NSX Manager 中。

### 导入 SSL 证书

您可以导入预先存在的或由 CA 签署的 SSL 证书以供 NSX Manager 使用。

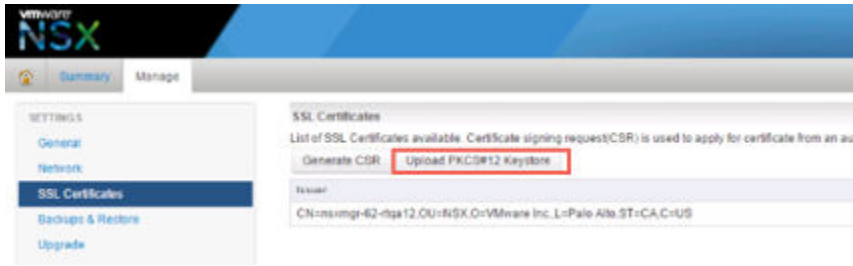
#### 前提条件

在 NSX Manager 上安装证书时，仅支持 PKCS#12 密钥库格式，而且该证书必须包含单个私钥及其相应的已签名证书或证书链。

#### 步骤

- 1 登录到 NSX Manager 虚拟设备。
- 2 单击**管理设备设置 (Manage Appliance Settings)**。

- 3 在“设置”面板中，单击 **SSL 证书 (SSL Certificates)**。
- 4 单击**上载 PKCS#12 密钥库 (Upload PKCS#12 Keystore)**。



- 5 单击**选择文件 (Choose File)**来查找文件。
- 6 单击**导入 (Import)**。
- 7 要应用证书，请重新引导 NSX Manager 设备。

证书将存储在 NSX Manager 中。

## 使用 SNMP 陷阱

NSX Manager 从 NSX Edge 和管理程序等接收信息、警告和严重系统事件。SNMP 代理将具有 OID 的 SNMP 陷阱转发到 SNMP 接收方。

SNMP 陷阱必须具有 SNMPv2c 版本。陷阱必须与管理信息库 (MIB) 相关联，以便 SNMP 接收方可以处理具有对象标识符 (OID) 的陷阱。

默认情况下，将禁用 SNMP 陷阱机制。启用 SNMP 陷阱仅激活严重和高严重性通知，以便 SNMP 管理器不会收到大量的通知。IP 地址或主机名定义了陷阱目标。要将主机名用于陷阱目标，必须设置设备以查询域名系统 (DNS) 服务器。

在启用 SNMP 服务时，将首次发出具有 OID 1.3.6.1.6.3.1.1.5.1 的 coldStart 陷阱。然后，在每次停止-开始时将具有 OID 1.3.6.1.6.3.1.1.5.2 的 warmStart 陷阱发出到配置的 SNMP 接收方。

如果将 SNMP 服务保持启用状态，将每隔 5 分钟发出一个具有 OID 1.3.6.1.4.1.6876.4.190.0.401 的 heartbeat 陷阱。在禁用该服务时，将发出具有 OID 1.3.6.1.4.1.6876.90.1.2.1.0.1 的 vmwNsxMSnmpDisabled 陷阱。该过程停止运行 vmwHbHeartbeat 陷阱并禁用该服务。

在添加、修改或删除 SNMP 接收方值时，将向一组新的或更新的 SNMP 接收方发送具有 OID 1.3.6.1.6.3.1.1.5.2 的 warmStart 陷阱和具有 OID 1.3.6.1.4.1.6876.90.1.2.1.0.2 的 vmwNsxMSnmpManagerConfigUpdated 陷阱。

---

**注** 不支持 SNMP 轮询。

---

## 配置 SNMP 设置

您可以启用 SNMP 设置，并配置目标接收方以发送严重、高或信息陷阱。

### 前提条件

- 熟悉 SNMP 陷阱机制。请参见[使用 SNMP 陷阱](#)。
- 确认配置了 SNMP 接收方。
- 为 NSX Manager 下载并安装 MIB 模块，以使 SNMP 接收方可以处理具有 OID 的陷阱。请参见<http://kb.vmware.com/kb/1013445>。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 选择**网络和安全 (Networking & Security) > 网络和安全清单 (Networking & Security Inventory) > NSX Manager (NSX Managers)**。
- 3 选择一个 NSX Manager IP 地址。
- 4 选择**管理 (Manage) > 系统事件 (System Events)**选项卡。
- 5 单击**编辑 (Edit)**以配置 SNMP 设置。

选项	说明
服务	发出 SNMP 陷阱。 默认情况下，将禁用该选项。
组通知	为某些系统事件预定义的组集合，用于聚合引发的事件。默认情况下，将启用该选项。 例如，如果系统事件属于某个组，将阻止这些分组事件的陷阱。每 5 分钟发出一个陷阱，以详细说明从 NSX Manager 收到的系统事件数。发出较少的陷阱可以节省 SNMP 接收方资源。
接收方	配置最多四个将陷阱发出到的接收方。 在添加 SNMP 接收方时，您必须填写以下部分。 接收方地址 - 接收方主机的 IP 地址或完全限定域名。 接收方端口 - SNMP 接收方的默认 UDP 端口为 162。 团体字符串 - 作为通知陷阱的一部分发出的信息。 已启用 - 指示该接收方是否发送陷阱。

- 6 单击**确定 (OK)**。

将启用 SNMP 服务并将陷阱发出到接收方。

### 后续步骤

检查 SNMP 配置是否正常工作。请参阅[验证 SNMP 陷阱配置](#)。

## 验证 SNMP 陷阱配置

在开始编辑现有的系统陷阱之前，您必须检查新启用的 SNMP 服务或更新的 SNMP 是否正常工作。

### 前提条件

确认配置了 SNMP。请参见[配置 SNMP 设置](#)。

## 步骤

### 1 验证 SNMP 配置和接收方连接。

- a 选择**管理 (Manage) > 系统事件 (System Events)**选项卡。
- b 单击**编辑 (Edit)**以配置 SNMP 设置。  
不要更改对话框中的设置。
- c 单击**确定 (OK)**。

将向所有 SNMP 接收方发出具有 OID 1.3.6.1.6.3.1.1.5.2 的 warmStart 陷阱。

### 2 调试 SNMP 配置或接收方问题。

- a 如果 SNMP 接收方未收到陷阱，请验证 SNMP 接收方是否在配置的端口上运行。
- b 在“SNMP 设置”部分中，检查接收方详细信息是否准确。
- c 如果 SNMP 接收方每隔 5 分钟停止接收具有 OID 1.3.6.1.4.1.6876.4.190.0.401 的 vmwHbHeartbeat 陷阱，请检查 NSX Manager 设备或 NSX Manager SNMP 代理是否正常工作。
- d 如果 Heartbeat 陷阱停止，请检查是否禁用了 SNMP 服务，或者测试 NSX Manager 和 SNMP 接收方之间的网络连接是否正常工作。

## 编辑系统陷阱

您可以编辑系统陷阱以提高或降低陷阱严重性和启用状态，以便将陷阱发出到接收方或阻止陷阱。

如果模块、SNMP OID 或 SNMP 陷阱“已启用”列值显示为 --，这意味着尚未为这些事件分配陷阱 OID。因此，不会发出这些事件的陷阱。

系统陷阱具有几个列，它们列出系统事件的不同特性。

选项	说明
事件代码	与事件关联的静态事件代码。
说明	描述事件的摘要。
模块	触发事件的子组件。
严重性	事件级别可以是信息、低、中、主要、严重或高。 默认情况下，如果启用了 SNMP 服务，则仅发出严重和高严重性事件的陷阱以强调需要立即引起注意的陷阱。
SNMP OID	表示单个 OID，将在引发系统事件时发出该 OID。 默认情况下，将启用组通知。如果启用了组通知，该组中的事件或陷阱显示事件或陷阱所属的组的 OID。 例如，划分到配置组的组通知 OID 具有 OID 1.3.6.1.4.1.6876.90.1.2.0.1.0.1。
SNMP 陷阱已启用	显示是允许还是禁止发出该事件的陷阱。 您可以将图标分别切换到事件或陷阱启用状态。如果启用了组通知，则无法切换陷阱启用状态。
筛选器	用于筛选系统陷阱的搜索项。

### 前提条件

确认 SNMP 设置可用。请参见[配置 SNMP 设置](#)。

## 步骤

- 1 登录到 vSphere Web Client。
- 2 选择**网络和安全 (Networking & Security) > 网络和安全清单 (Networking & Security Inventory) > NSX Manager (NSX Managers)**。
- 3 选择一个 NSX Manager IP 地址。
- 4 选择**管理 (Manage) > 系统事件 (System Events)**选项卡。
- 5 在“系统陷阱”部分中选择一个系统事件。
- 6 单击**编辑 (Edit)** () 图标。  
如果启用了组通知，则不允许编辑陷阱启用状态。您可以更改不属于组的陷阱的启用状态。
- 7 从下拉菜单中更改系统事件的严重性。
- 8 如果将严重性从“信息”更改为“严重”，请选中**启用为 SNMP 陷阱 (Enable as SNMP Trap)**复选框。
- 9 单击**确定 (OK)**。
- 10 (可选) 单击标题中的**启用 (Enable)** () 图标或**禁用 (Disable)** () 图标，以允许或禁止发送系统陷阱。
- 11 (可选) 单击**复制 (Copy)** () 图标以将一个或多个事件行复制到剪贴板中。

## NSX 备份和还原

要在出现故障时将系统还原到工作状态，就必须正确备份所有 NSX 组件，这点至关重要。

NSX Manager 备份包含所有 NSX 配置，包括控制器、逻辑交换和路由实体、安全性、防火墙规则以及在 NSX Manager UI 或 API 中配置的任何其他内容。需要单独备份 vCenter 数据库和相关的元素（如虚拟交换机）。

建议至少定期备份 NSX Manager 和 vCenter。备份频率和计划可能因业务需求和运行流程而异。建议在配置频繁更改时经常执行 NSX 备份。

NSX Manager 备份可以按需执行，也可以按每小时、每日或每周的频率执行。

建议在以下情况下执行备份：

- 执行 NSX 或 vCenter 升级之前。
- 执行 NSX 或 vCenter 升级之后。
- 执行 NSX 组件零日部署和初始配置之后，例如，创建 NSX Controller、逻辑交换机、逻辑路由器、Edge 服务网关、安全策略和防火墙策略之后。
- 基础架构或拓扑更改之后。
- 执行重大第 2 日更改之后。

要将整个系统回滚到指定时间的状态，建议将 NSX 组件备份（如 NSX Manager）与其他交互组件（如 vCenter、云管理系统和运行工具等）的备份计划保持同步。



## 备份 NSX Manager 数据

您可以通过执行按需备份或调度备份来备份 NSX Manager 数据。

您可以通过 NSX Manager 虚拟设备 Web 界面或 NSX Manager API 配置 NSX Manager 备份和还原。备份频率可以调度为每小时、每日或每周。

备份文件保存到 NSX Manager 可访问的远程 FTP 或 SFTP 位置。NSX Manager 数据包括配置表、事件表和审核日志表。配置表包含在每个备份中。

仅支持在版本与备份版本相同的 NSX Manager 上执行还原。因此，请务必在执行 NSX 升级前后创建新的备份文件，即一个备份用于旧版本，另一个用于新版本。

### 步骤

- 1 登录到 NSX Manager 虚拟设备。
- 2 在“设备管理”下方，单击**备份和还原**。
- 3 要指定备份位置，请单击“FTP 服务器设置”旁边的**更改**。
  - a 键入备份系统的 IP 地址或主机名。
  - b 根据目标支持的内容，从**传输协议**下拉菜单中选择 **SFTP** 或 **FTP**。
  - c 根据需要编辑默认端口。
  - d 键入登录到备份系统所需的用户名和密码。
  - e 在**备份目录**字段中，键入用于存储备份的绝对路径。

要确定绝对路径，您可以登录到 FTP 服务器，导航到要使用的目录，然后运行 `present working directory` 命令 (`pwd`)。例如：

```
PS C:\Users\Administrator> ftp 192.168.110.60
Connected to 192.168.110.60.
220 server-nfs FTP server ready.
User (192.168.110.60:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> ls
200 PORT command successful.
150 Opening BINARY mode data connection for 'file list'.
datastore-01
226 Transfer complete.
ftp: 22 bytes received in 0.00Seconds 22000.00Kbytes/sec.
ftp> cd datastore-01
250 CWD command successful.
ftp> pwd
257 "/datastore-01" is current directory.
```

- f 在**文件名前缀**中键入一个文本字符串。

此文本将被预置到每个备份文件名中，以便在备份系统中识别这些备份文件。例如，如果键入 **ppdb**，则生成的备份的名称为 **ppdbHH\_MM\_SS\_DayDDMonYYYY**。

- g 键入密码短语以确保备份安全。

您需要此密码才能还原备份。

- h 单击**确定**。

例如：

- 4 对于按需备份，请单击**备份**。

新文件将添加到**备份历史记录**下。

- 5 对于调度备份，请单击“调度”旁边的**更改**。

- a 从**备份频率**下拉菜单中，选择**按小时**、**按天**或**按周**。系统将根据所选的频率禁用“一周中的某天”、“每日时间”和“分钟”下拉菜单。例如，如果您选择“按天”，则将禁用“一周中的某天”下拉菜单，因为此字段不适用于每天频率。

- b 对于按周备份，选择应该在一周中的哪一天备份数据。

- c 对于按周备份或按天备份，选择开始备份的小时。

- d 选择开始备份的分钟，然后单击**调度**。

- 6 要从备份中排除日志和流量数据，请单击“排除”旁边的**更改**。

- a 选择要从备份中排除的项目。

- b 单击**确定**。

7 保存 FTP 服务器的 IP/主机名、凭据、目录详细信息和密码。您需要此信息才能还原备份。

## 还原 NSX Manager 备份

还原 NSX Manager 会使备份文件加载到 NSX Manager 设备上。备份文件必须保存到 NSX Manager 可以访问的远程 FTP 或 SFTP 位置。NSX Manager 数据包括配置表、事件表和审核日志表。

---

**重要** 在还原备份文件前，请对您的当前数据进行备份。

---

### 前提条件

还原 NSX Manager 数据之前，建议重新安装 NSX Manager 设备。您或许也可以在现有 NSX Manager 设备上运行还原操作，但此操作未获得官方支持。前提是现有 NSX Manager 已失败，从而部署了新的 NSX Manager 设备。

最佳做法是捕获旧的 NSX Manager 设备的当前设置的屏幕截图或记下这些设置，以便可以使用这些设置来指定新部署的 NSX Manager 设备的 IP 信息和备份位置信息。

### 步骤

1 捕获屏幕截图或记下现有 NSX Manager 设备上的所有设置。

2 部署新的 NSX Manager 设备。

版本必须与已备份的 NSX Manager 设备相同。

3 登录到新的 NSX Manager 设备。

4 在“设备管理”下方，单击**备份和还原 (Backups & Restore)**。

5 在“FTP 服务器设置”中，单击**更改 (Change)**并添加设置。

“备份位置”屏幕中的主机 IP 地址 (Host IP Address)、用户名 (User Name)、密码 (Password)、备份目录 (Backup Directory)、文件名前缀 (Filename Prefix)和密码短语 (Pass Phrase)字段必须标识要还原的备份的位置。

6 在“备份历史记录”部分中，选中要还原的备份所对应的复选框，然后单击**还原 (Restore)**。

## 备份 NSX Edge

所有 NSX Edge 配置（逻辑路由器和 Edge 服务网关）都会在备份 NSX Manager 数据的过程中进行备份。

如果您设置了完整的 NSX Manager 配置，可以通过重新部署 NSX Edge（在 vSphere Web Client 中单击**重新部署 NSX Edge** 图标）来重新创建一个不可访问或失效的 Edge 设备虚拟机。

不支持创建单独的 NSX Edge 备份。

## 备份 vSphere Distributed Switch

可以将 vSphere Distributed Switch 和分布式端口组配置导出到文件。

该文件保留有效的网络配置，使这些配置能够分发到其他部署。

该功能仅在 vSphere Web Client 5.1 或更高版本中可用。VDS 设置和端口组设置将作为导入内容的一部分进行导入。

最佳做法是在针对 VXLAN 为群集做好准备之前导出 VDS 配置。有关详细说明，请参见 <http://kb.vmware.com/kb/2034602>。

## 备份 vCenter

为保护 NSX 部署，请务必备份 vCenter 数据库并生成虚拟机快照。

请参考您使用的 vCenter 版本对应的 vCenter 文档，了解 vCenter 备份和还原步骤以及最佳做法。

有关虚拟机快照，请参见 <http://kb.vmware.com/kb/1015180>。

与 vCenter 5.5 有关的有用链接：

- <http://kb.vmware.com/kb/2057353>
- <http://kb.vmware.com/kb/2034505>
- <http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf>

与 vCenter 6.0 有关的有用链接：

- <https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html>
- <http://kb.vmware.com/kb/2110294>

## 流量监控

流量监控是一种流量分析工具，提供流入/流出受保护虚拟机的流量详细视图。启用流量监控后，其输出定义哪些计算机正通过哪些应用程序交换数据。此数据中包括会话数和每个会话传输的数据包数。会话详细信息包括源、目标、应用程序和正在使用的端口。可以使用会话详细信息来创建防火墙以允许或阻止规则。

您可以查看多种类型协议的流量数据，包括 TCP、UDP、ARP 和 ICMP 等。此外，您还可以查看选定虚拟网卡的入站/出站 TCP 和 UDP 连接。还可以通过指定筛选器排除流量。

因此，可将流量监控作为取证工具来检测恶意服务和检查出站会话。

## 查看流量监控数据

可以查看虚拟机上指定时间范围内的流量会话。默认情况下将显示过去 24 小时的数据，最短时间段为一小时，最长时间段为两周。

### 前提条件

只有群集中已安装网络虚拟化组件并启用了防火墙的虚拟机才提供流量监控数据。请参见 NSX 安装指南。

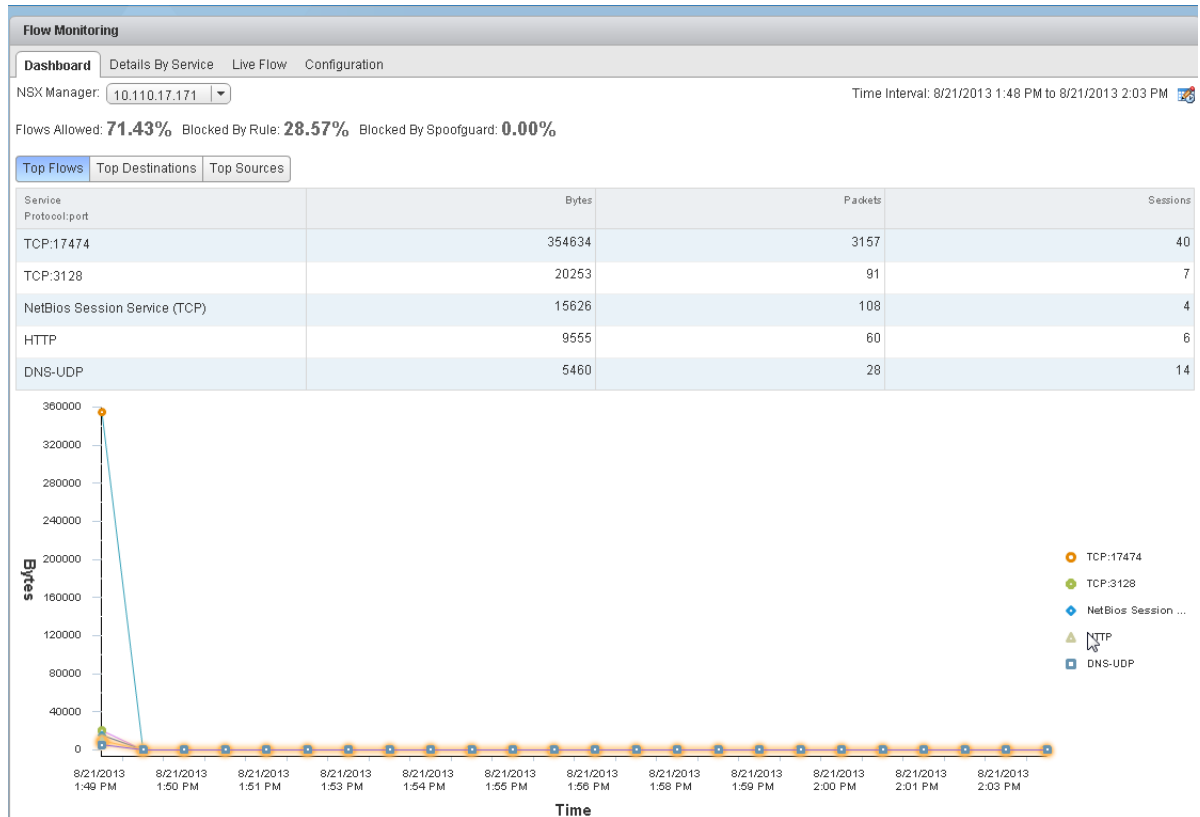
### 步骤

- 1 登录到 vSphere Web Client。
- 2 从左侧导航窗格中选择**网络和安全 (Networking & Security)**，然后选择**流量监控 (Flow Monitoring)**。

3 确保您处于**仪表板 (Dashboard)**选项卡中。

4 单击**流量监控 (Flow Monitoring)**。

加载此页面可能需要几秒钟的时间。页面顶部将显示允许的流量、防火墙规则阻止的流量和 SpoofGuard 阻止的流量的相应百分比。多线图将显示环境中每项服务的数据流。当您指向图例区域中的某项服务时，该项服务的图形将突出显示。



以下三个选项卡将显示流量统计信息：

- **最高流量 (Top Flows)**显示指定时间段内每项服务的进站和出站总流量（基于总字节值，而非会话数/数据包数）。此处将显示流量最高的前五项服务。计算最高流量时不考虑受阻的通信流。
- **流量最高的目标 (Top Destinations)**显示指定时间段内每个目标的进站流量。此处将显示流量最高的前五个目标。
- **流量最高的源 (Top Sources)**显示指定时间段内每个源的出站流量。此处将显示流量最高的前五个源。

## 5 单击按服务列出详细信息 (Details by Service) 选项卡。

此处将显示有关所选服务的所有流量的详细信息。**允许的流量 (Allowed Flows)** 选项卡显示允许的流量会话，**阻止的流量 (Blocked Flows)** 选项卡显示阻止的流量。

您可以使用服务名称进行搜索。

**Flow Monitoring**

Dashboard **Details By Service** Live Flow Configuration

NSX Manager: 10.110.17.171 Time Interval: 8/23/2013 6:10 AM to 8/23/2013 6:25 AM

Allowed Flows Blocked Flows

Type	Service	Bytes	Sessions
UDP	DHCP-Server	4954	6
TCP	TCP:17474	2224	1
OTHER	IPv6-ICMP:0	1872	18
OTHER	ARP	1196	26
OTHER	0xffff	162	2
UDP	NTP Time Server	152	1

Find 6 items

Rule Id	Time Stamp	Source	Source User(s)	Destination	Packets	Actions
1021	8/23/2013 6:15 AM	10.112.243.233	Unknown	10.112.192.5	2	Add Rule Edit Rule
1021	8/23/2013 6:15 AM	DB_server	Unknown	10.112.192.5	2	Add Rule Edit Rule
1021	8/23/2013 6:15 AM	win32rdclone	Unknown	10.112.192.6	2	Add Rule Edit Rule
1021	8/23/2013 6:14 AM	10.112.243.214	Unknown	10.112.192.6	2	Add Rule Edit Rule
1021	8/23/2013 6:12 AM	win32rdclone	Unknown	10.112.192.5	2	Add Rule Edit Rule
1021	8/23/2013 6:11 AM	10.112.243.229	Unknown	10.112.192.6	2	Add Rule Edit Rule
1021	8/23/2013 6:13 AM	win32rdclone	Unknown	10.113.60.150	12	Add Rule Edit Rule

## 6 单击表中的某一项可显示允许或阻止该流量的规则。

## 7 单击某个规则的规则 ID (Rule Id) 可显示该规则的详细信息。

# 更改流量监控图表的日期范围

可以针对“仪表板”和“详细信息”选项卡更改流量监控数据的日期范围。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 从左侧导航窗格中选择**网络和安全 (Networking & Security)**，然后选择**流量监控 (Flow Monitoring)**。
- 3 单击**时间间隔 (Time interval)**旁边的
- 4 选择时间段或键入新的开始日期和结束日期。  
可以查看流量数据的最大时间段为前两周。
- 5 单击**确定 (OK)**。

## 在流量监控报告中添加或编辑防火墙规则

通过对流量数据进行深入查看，可以评估资源使用情况，并将会话信息发送至分布式防火墙，以在任意级别创建新的允许规则或阻止规则。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 从左侧导航窗格中选择**网络和安全 (Networking & Security)**，然后选择**流量监控 (Flow Monitoring)**。
- 3 单击**按服务列出详细信息 (Details by Service)**选项卡。
- 4 单击某个服务以查看其流量。  
根据选定的选项卡，将显示此服务允许或拒绝流量的规则。
- 5 单击某个规则 ID 以查看规则详细信息。
- 6 执行以下操作之一：

- 要编辑规则，请执行以下操作：
  - 1 单击**操作 (Actions)**列中的**编辑规则 (Edit Rule)**。
  - 2 更改规则的名称、操作或备注。
  - 3 单击“确定”。
- 要添加规则，请执行以下操作：
  - 1 单击**操作 (Actions)**列中的**添加规则 (Add Rule)**。
  - 2 完成表单以添加规则。有关完成防火墙规则表单的信息，请参见[添加防火墙规则](#)。
  - 3 单击**确定 (OK)**。

此时规则将添加到防火墙规则区域的顶部。

## 查看实时流量

可以查看选定虚拟网卡的出站/入站 UDP 和 TCP 连接。要查看两台虚拟机之间的流量，可以在一台计算机上查看其中一台虚拟机的实时流量，在另一台计算机上查看第二台虚拟机的实时流量。每台主机最多可查看两个虚拟网卡的流量，每个基础架构最多可查看 5 个虚拟网卡的流量。

查看实时流量会影响 NSX Manager 和相应虚拟机的性能。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 从左侧导航窗格中选择**网络和安全 (Networking & Security)**，然后选择**流量监控 (Flow Monitoring)**。
- 3 单击**实时流量 (Live Flow)**选项卡。
- 4 单击**浏览 (Browse)**并选择一个虚拟网卡。

## 5 单击启动 (Start)以开始查看实时流量。

此页面将每 5 秒刷新一次。可以从**刷新速率 (Refresh Rate)**下拉菜单中选择其他频率。

RuleId	Direction	Flow Type	Protocol	Source IP	Source Port	Destination IP	Destination Port	state	Incoming Bytes	Incoming Packets	Outgoing Bytes	Outgoing Packets
1026	OUT	Active	TCP	172.16.40.121	49099	172.16.40.131	3306	FINWAIT2	747	11	2077	9
1026	OUT	Inactive	TCP	172.16.40.121	49098	172.16.40.131	3306	FINWAIT2	747	11	2077	9

## 6 完成调试或故障排除后，请单击停止 (Stop)以避免影响 NSX Manager 或所选虚拟机的性能。

## 配置流量监控数据收集

查看并筛选要收集的流量监控数据后，您可以配置数据收集。可以通过指定排除条件筛选要显示的数据。例如，您可能想要排除一个代理服务器以避免看到重复的流量。或者，如果在清单中的虚拟机上运行 Nessus 扫描，可能不希望收集扫描流量。您可以配置 IPFix，使特定流量的信息直接从防火墙导出到流量收集器。流量监控图中不包括 IPFix 流量。IPFix 流量显示在 IPFix 收集器的界面上。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 从左侧导航窗格中选择**网络和安全 (Networking & Security)**，然后选择**流量监控 (Flow Monitoring)**。
- 3 选择**配置 (Configuration)**选项卡。
- 4 确保**全局流量收集状态 (Global Flow Collection Status)**为已启用 (Enabled)。

将在整个清单（**排除设置 (Exclusion Settings)**中指定的对象除外）中收集所有防火墙相关的流量。



## 5 要指定筛选条件，请单击**流量排除 (Flow Exclusion)**，并按以下步骤操作。

### a 单击要排除的流量对应的选项卡。

**Flow Monitoring**

Dashboard Details By Service Live Flow **Configuration**

NSX Manager: 10.110.8.93

Global Flow Collection Status: **Enabled** **Disable**

**Flow Exclusion** IPFix

**Exclusion Settings**  
System will not collect flows that match the specified condition

Filter	
Collect Blocked Flows	Yes
Collect Layer2 Flows	Yes
Source	
Destination	system-generated-broadcast-macset, 224.0.0.0/24, 255.255.255.255
Destination ports	138,137
Service	

System is configured to collect all firewall related flows except those that match the conditions specified below

**Detail Collection Policy:** (Click Save to commit changes to settings)

Collect Blocked Flows:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Collect Layer2 Flows:	<input checked="" type="radio"/> Yes <input type="radio"/> No

Save

### b 指定所需信息。

如果选择	指定以下信息
收集阻止的流量	选择“否”排除阻止的流量。
收集第 2 层流量	选择“否”排除第 2 层流量。
源	不为指定的源收集流量。 <ol style="list-style-type: none"> <li>单击<b>添加 (Add)</b>图标。</li> <li>在“查看”中，选择相应的容器。</li> <li>选择要排除的对象。</li> </ol>
目标	不为指定的目标收集流量。 <ol style="list-style-type: none"> <li>单击<b>添加 (Add)</b>图标。</li> <li>在“查看”中，选择相应的容器。</li> <li>选择要排除的对象。</li> </ol>
目标端口	排除流向指定端口的流量。 键入要排除的端口号。
服务	排除指定服务和/或服务组的流量。 <ol style="list-style-type: none"> <li>单击<b>添加 (Add)</b>图标。</li> <li>选择相应的服务和/或服务组。</li> </ol>

### c 单击**保存 (Save)**。

6 要配置流量收集，请单击 **IPFix**，并按照以下步骤操作。

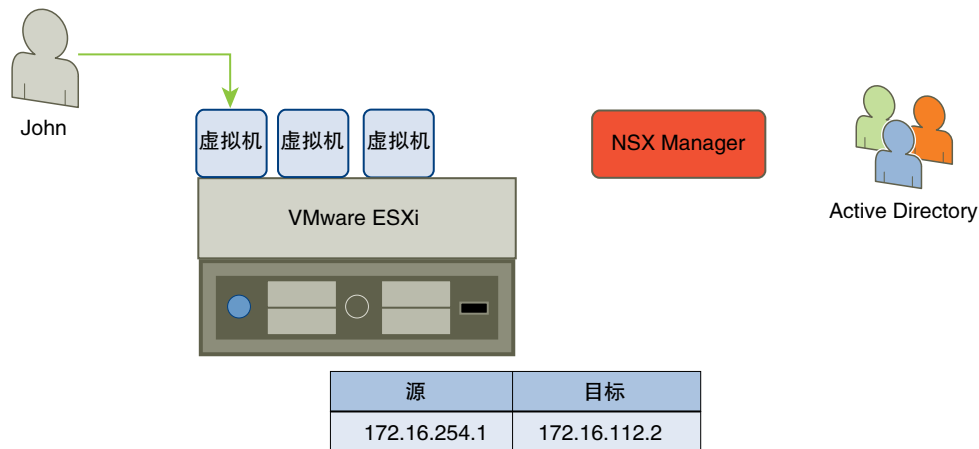
- a 单击“IPFix 配置”旁的**编辑 (Edit)**，然后单击**启用 IPFix 配置 (Enable IPFix Configuration)**。
- b 在**观察 DomainID (Observation DomainID)** 中，键入可标识导出到流量收集器的防火墙的 32 位标识符。
- c 在**活动流导出超时 (Active Flow Export Timeout)**中键入一个时间（以分钟为单位），在经过这段时间之后，活动流将导出到流量收集器。默认值为 5。例如，如果流量持续 30 分钟处于活动状态，并且导出超时为 5 分钟，则该流量将在其生命周期内导出 7 次。创建和删除各一次，活动期间 5 次。
- d 在**收集器 IP (Collector IPs)** 中，单击“添加” (+) 图标，并键入流量收集器的 IP 地址和 UDP 端口。
- e 单击**确定 (OK)**。

## 活动监控

使用活动监控可以查看由 vCenter 管理的 Windows 桌面虚拟机正在使用的应用程序。此可见性有助于确保组织的安全策略得到正确执行。

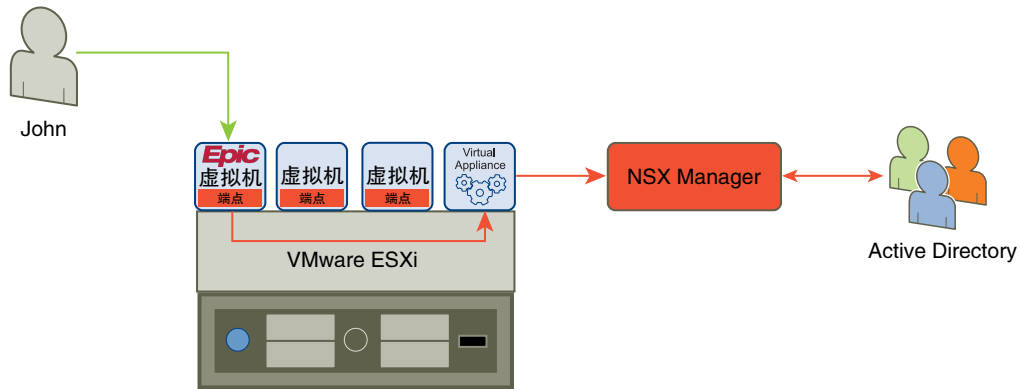
安全策略可能规定了哪些人员可以访问哪些应用程序。云管理员可生成活动监控报告，以了解所设置的基于 IP 的防火墙规则是否正按预期工作。通过提供用户和应用程序级别详细信息，活动监控可以将高级别安全策略转换成基于 IP 地址和网络的低级别实施。

图 23-2. 当前的虚拟环境



为活动监控 启用数据收集后，可以运行报告以查看入站流量（如用户访问的虚拟机）以及出站流量（资源利用率、清单容器间的交互以及访问了服务器的 AD 组）。

图 23-3. 使用 活动监控 的虚拟环境



用户	AD 组	应用程序名称	源虚拟机名称	目标虚拟机名称	源 IP	目标 IP
John	医师	Epic.exe	DoctorsWS13	EpicSVR3	172.16.254.1	172.16.112.2

**重要** 在 Linux 虚拟机上不支持活动监控。

## 设置活动监控

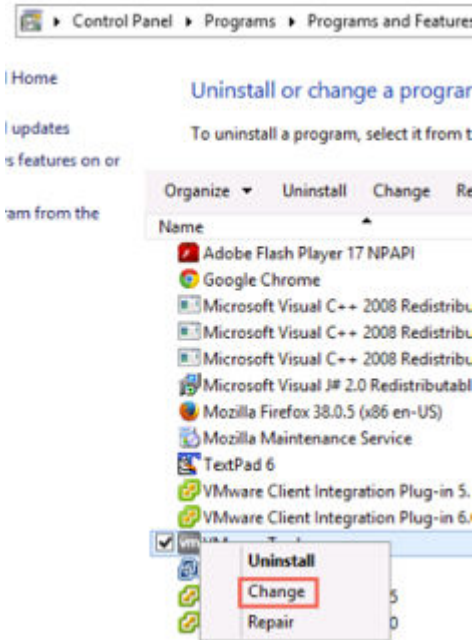
要使活动监控正常工作，您必须执行几项必要步骤，包括安装 **Guest Introspection** 驱动程序和 **Guest Introspection** 虚拟机以及启用 **NSX** 活动监控。或者，您也可以使用服务编排来控制要监控的虚拟机。

### 前提条件

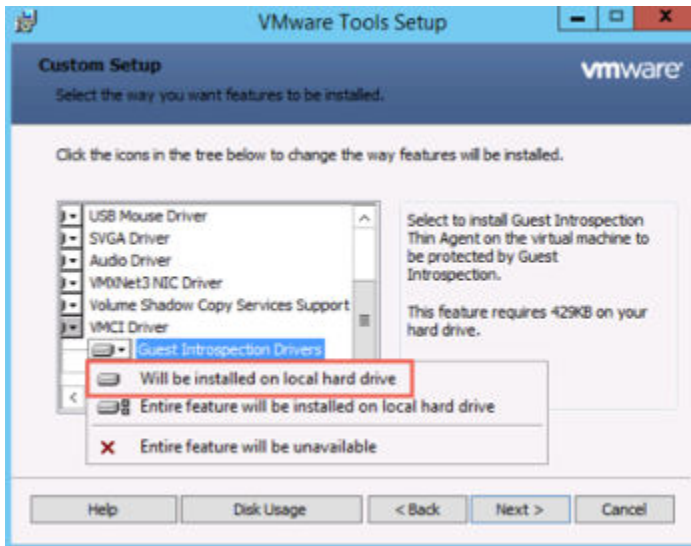
- **NSX** 必须已安装并且正常运行。
- **NSX Manager** 必须与 **AD** 服务器链接起来，因为 **Windows** 虚拟机用户将与从该服务器获取的组进行匹配。
- **vCenter** 清单必须包含一个或多个 **Windows** 桌面虚拟机。
- **VMware Tools** 必须正在 **Windows** 桌面虚拟机上运行且为最新版本。

## 步骤

- 1 在 vCenter 清单中的 Windows 虚拟机上，安装 Guest Introspection 驱动程序（如果尚未安装）。
  - a 导航至**控制面板\程序\程序和功能 (Control Panel\Programs\Programs and Features)**，右键单击 **VMware Tools** 并选择**更改 (Change)**。



- b 选择**修改 (Modify)**。
  - c 在 **VMCI 驱动程序 (VMCI Driver)** 下面，单击 **Guest Introspection 驱动程序 > 此功能将安装到本地硬盘上 (Guest Introspection Drivers > Will be installed on local hard drive)**。



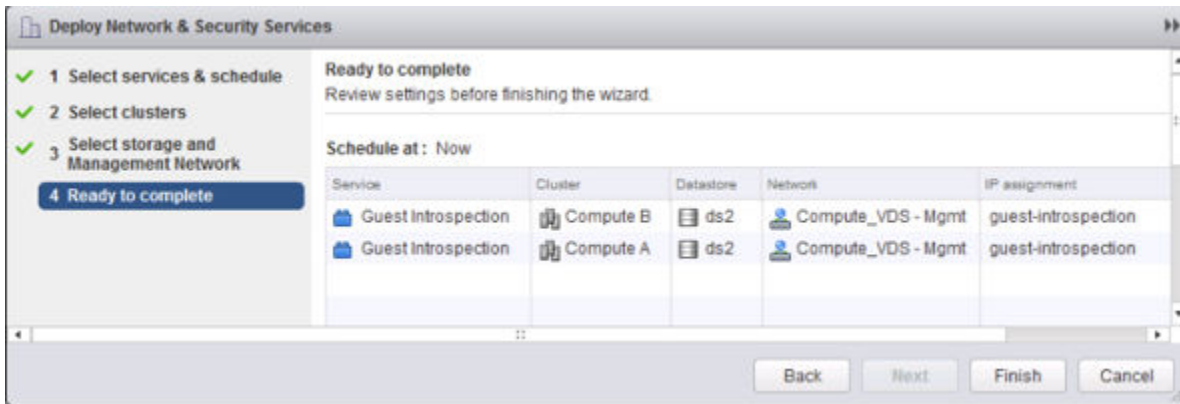
Guest Introspection 驱动程序会检测正在每个 Windows 虚拟机上运行的应用程序，并将此信息发送到 Guest Introspection 虚拟机。

## 2 安装 Guest Introspection 虚拟机。

首次启动 VMware Tools 安装时，请选择自定义 (Custom) 选项。在 VMCI 文件夹中，选择 **Guest Introspection 驱动程序 (Guest Introspection Driver)**。默认情况下，该驱动程序处于未选中状态。

要在安装 VMware Tools 后添加驱动程序，请执行以下操作：

- 在 vCenter Web Client 中，导航至 **网络和安全 > 安装 > 服务部署 (Networking & Security > Installation > Service Deployments)**。
- 添加新的服务部署。
- 选择 **Guest Introspection**。
- 选择包含 Windows 虚拟机的主机群集。
- 选择相应的数据存储、网络和 IP 寻址机制。如果未对 Guest Introspection 虚拟机使用 DHCP，请创建并分配 IP 池。

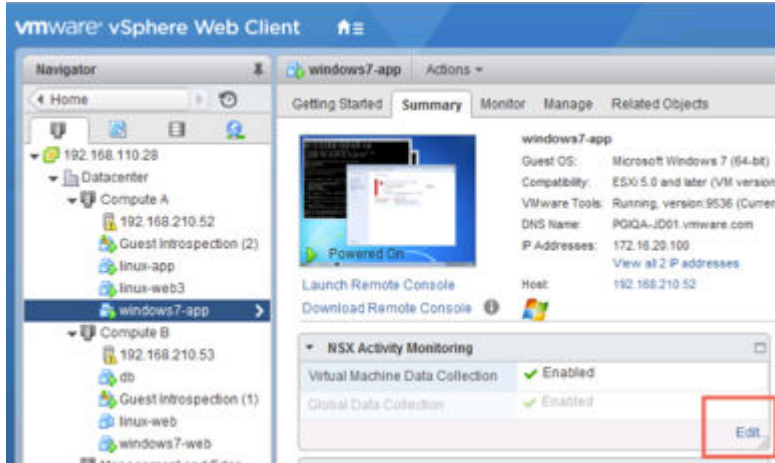


现已安装两个 Guest Introspection 虚拟机，每个群集内的每个主机上各安装一个。



### 3 在 Windows 虚拟机上启用活动监控。

- a 在**主机和群集 (Hosts and Clusters)**视图中，选择 Windows 虚拟机，然后选择**摘要 (Summary)**选项卡。
- b 在 NSX 活动监控中，单击**编辑 (Edit)**，然后单击**是 (Yes)**。



对所有要监控的 Windows 虚拟机重复此步骤。

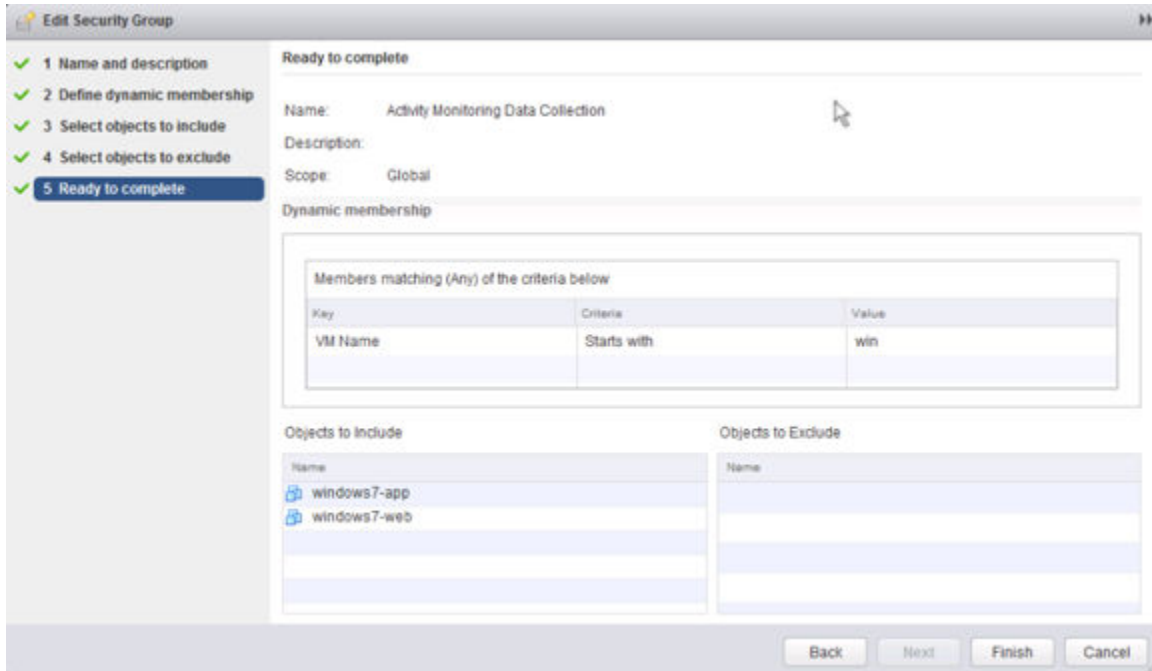
### 4 （可选）修改受监控的 vCenter 对象的列表，或定义动态成员资格规则。

- a 在 vCenter Web Client 中，导航至**网络和安全 > 服务编排 (Networking & Security > Service Composer)**。
- b 编辑**活动监控数据收集 (Activity Monitoring Data Collection)**安全组。

- c 定义动态成员资格规则，以便向群集添加新的 **Windows** 虚拟机时，这些虚拟机自动受监控。
- d 选择要包含到活动监控安全组或从中排除的 **vCenter** 对象。

已启用活动监控的虚拟机将自动包含到活动监控安全组。

在以下示例中，所有名称以“win”开头的虚拟机将自动添加到活动监控安全组。这意味着这些虚拟机将自动启用活动监控。



## 活动监控场景

本节介绍活动监控的某些假设场景。

### 对应用程序的用户访问权限

在假想的 **ACME Enterprise** 公司中，仅允许经过批准的用户访问企业资产上的特定应用程序。

其安全策略授权如下：

- 仅允许授权用户访问关键业务应用程序
- 仅允许授权应用程序放置在公司服务器上
- 仅允许从特定网络访问必需的端口

根据以上授权，公司需要根据用户身份控制员工的访问权限，保护公司资产。开始时，**ACME Enterprise** 的安全操作员需要能够确认仅管理员可以访问 **MS SQL Server**。

### 步骤

- 1 登录到 **vSphere Web Client**。
- 2 单击 **网络和安全 (Networking & Security)**，然后单击 **活动监控 (Activity Monitoring)**。

3 单击**进站活动 (Inbound Activity)**选项卡。

4 在**出站自 (Outbound from)**中，将值保留为**所有已发现的 AD 组 (All Observed AD Groups)**，以查看来自所有员工的访问。

5 在**目标虚拟机位置 (Where destination virtual machine)**中，选择**包括 (includes)**，并保持选中**所有已发现的目标虚拟机 (all observed destination virtual machines)**。

6 在**目标应用程序位置 (And where destination application)**中，选择**包括 (includes)**，然后单击**所有已发现的目标应用程序 (all observed destination applications)**并选择 Microsoft SQL Server。

7 单击**搜索 (Search)**。

搜索结果显示仅管理用户在访问 MS SQL Server。请注意，没有组（例如财务或 HR）在访问这些服务器。

8 现在可以通过将**出站自 (Outbound from)**值设置为 HR 和财务 AD 组来反转此查询。

9 单击**搜索 (Search)**。

未显示任何记录，这就可以确认这些组的用户都无法访问 MS SQL Server。

## 数据中心内的应用程序

作为安全策略的一部分，ACME Enterprise 需要查看数据中心的所有应用程序。这有助于识别捕获机密信息或将敏感数据提取到外部源的恶意应用程序。

John 是 ACME Enterprise 的云管理员，他想要确认只能通过 Internet Explorer 访问 SharePoint 服务器，并且没有恶意应用程序（例如 FTP 或 RDP）可以访问此服务器。

### 步骤

1 登录到 vSphere Web Client。

2 单击**网络和安全 (Networking & Security)**，然后单击**活动监控 (Activity Monitoring)**。

3 单击**虚拟机活动 (VM Activity)**选项卡。

4 在**源虚拟机位置 (Where source VM)**中，选择**包括 (includes)**并选中**所有已发现的虚拟机 (All observed virtual machines)**，以捕获来自数据中心内所有虚拟机的流量。

5 在**目标虚拟机位置 (Where destination VM)**中，选择**包括 (includes)**，单击**所有已发现的虚拟机 (All observed virtual machines)**，然后选择 SharePoint 服务器。

6 单击**搜索 (Search)**。

搜索结果中的**出站 App 产品名称 (Outbound App Product Name)**列显示只通过 Internet Explorer 对 SharePoint 服务器进行了访问。这些相对同类的搜索结果表明，该 SharePoint 服务器应用了某个防火墙规则，此规则阻止了其他所有访问方法。

同时请注意，搜索结果显示了观测流量的源用户，而非源组。单击搜索结果中的箭头将显示有关源用户（例如用户所属的 AD 组）的详细信息。



## 验证打开的端口

管理员 John 了解到只有授权的应用程序才能访问 ACME Enterprise 共享点服务器后，他可以确保公司可基于预期使用率只打开必需的端口。

### 前提条件


在[数据中心内的应用程序](#)场景中，管理员 John 已观察了 ACME Enterprise 共享点服务器的流量。现在，他要确保所有从共享点服务器到 MSSQL Server 的访问都是通过预期的协议和应用程序进行的。

### 步骤

- 1 单击**转到主页 (Go Home)**图标。
- 2 单击 **vCenter 主页 (vCenter Home)**，然后单击**虚拟机 (Virtual Machines)**。
- 3 选择 **win\_sharepoint**，然后单击**监控 (Monitor)**选项卡。
- 4 单击**活动监控 (Activity Monitoring)**。
- 5 在**目标位置 (Where destination)**中，选择 **win2K-MSSQL**。
- 6 单击**搜索 (Search)**。

搜索结果将显示从共享点服务器到 MSSQL Server 的流量。**用户 (User)**和**出站 App (Outbound App)** 列将显示只有系统进程连接到 MSSQL Server，这也是 John 预期看到的结果。

**进站端口 (Inbound Port)**和 **App** 列将显示所有访问都是针对在目标服务器上运行的 MSSQL Server。

由于搜索结果中的记录过多，John 无法在 Web 浏览器中进行分析，但是他可以导出所有的完整结果集，并通过单击页面右下方的  图标以 CSV 格式保存文件。

## 启用数据收集

在运行 **活动监控** 报告之前，必须为 vCenter Server 上的一个或多个虚拟机启用数据收集。在运行该报告之前，应确保启用的虚拟机处于活动状态，并且正在产生网络流量。

您还应该向 AD 域控制器注册 NSX Manager。请参见[向 NSX Manager 注册 Windows 域](#)。

请注意，活动监控仅跟踪活动连接。虚拟网卡级别下的防火墙规则所阻止的虚拟机流量不会反映在报告中。

### 在一个虚拟机上启用数据收集

必须在启用数据收集至少五分钟之后，才可以运行 **活动监控** 报告。

### 前提条件

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **vCenter**，然后单击**虚拟机和模板 (VMs and Templates)**。
- 3 在左侧清单面板中选择虚拟机。

- 4 单击**管理 (Manage)**选项卡，然后单击**设置 (Settings)**选项卡。
- 5 在左侧面板中单击 **NSX 活动监控 (NSX Activity Monitoring)**。
- 6 单击**编辑 (Edit)**。
- 7 在“编辑 NSX 活动监控数据收集设置”对话框中，单击**是 (Yes)**。

## 为多个虚拟机启用数据收集

活动监控数据收集安全组是预定义的安全组。可以一次将多个虚拟机添加到该安全组，并且在所有这些虚拟机上启用数据收集。

必须在启用数据收集至少五分钟之后，才可以运行 活动监控 报告。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**服务编排 (Service Composer)**。
- 3 单击**安全组 (Security Groups)**选项卡。
- 4 选择“活动监控数据收集”安全组，然后单击**编辑 (Edit)** (✎) 图标。
- 5 按照向导提示将虚拟机添加到安全组。

数据收集在您添加到该安全组的所有虚拟机上处于启用状态，而在排除在该安全组以外的任何虚拟机上处于禁用状态。

## 查看虚拟机活动报告

您可以查看环境中一个虚拟机或一组虚拟机的出入流量。

可以通过单击**搜索 (Search)**使用默认搜索条件执行快速查询，或者根据您的要求自定义查询。

### 前提条件

- 必须在环境中安装 Guest Introspection。
- 必须向 NSX Manager 注册一个域。有关域注册的信息，请参见[向 NSX Manager 注册 Windows 域](#)。
- 必须在一个或多个虚拟机上启用数据收集。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**活动监控 (Activity Monitoring)**。
- 3 单击**虚拟机活动 (VM Activity)**选项卡。
- 4 单击**源位置 (Where source)**旁边的链接。选择要查看其出站流量的虚拟机。指示要将所选虚拟机包括在报告中还是排除在报告之外。
- 5 单击**目标位置 (Where destination)**旁边的链接。选择要查看其入站流量的虚拟机。指示要将所选虚拟机包括在报告中还是排除在报告之外。

6 单击**期间 (During period)** (📅) 图标，然后选择搜索的时间段。

7 单击**搜索 (Search)**。

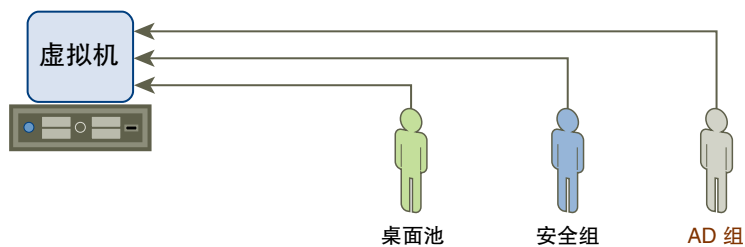
此时将显示按指定条件筛选的搜索结果。单击某行可查看该行用户的详细信息。

可以通过单击页面右下方的 📄 图标导出此页面上的特定记录或所有记录，将其以 .csv 格式保存到某个目录中。

## 查看入站活动

您可以按照桌面池、安全组或 AD 组查看服务器的所有入站活动。

图 23-4. 查看入站活动




可以通过单击**搜索 (Search)**使用默认搜索条件执行快速查询，或者根据您的要求自定义查询。

### 前提条件


- 必须在环境中安装 Guest Introspection。
- 必须向 NSX Manager 注册一个域。有关域注册的信息，请参见[向 NSX Manager 注册 Windows 域](#)。
- 必须在一个或多个虚拟机上启用数据收集。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**活动监控 (Activity Monitoring)**。
- 3 单击**入站活动 (Inbound Activity)**选项卡。
- 4 单击**来源 (Originating from)**旁边的链接。
- 5 选择要查看活动的用户组的类型。
- 6 在**筛选器类型 (Filter type)**中，选择一个或多个组，然后单击“确定”。
- 7 在**目标虚拟机位置 (Where destination virtual machine)**中，选择**包括 (includes)**或**排除 (excludes)**以指示应在搜索中包括还是排除所选虚拟机。
- 8 单击**目标虚拟机位置 (And where destination virtual machine)**旁边的链接。
- 9 选择一个或多个虚拟机，然后单击**确定 (OK)**。
- 10 在**目标应用程序位置 (And where destination application)**中，选择**包括 (includes)**或**排除 (excludes)**以指示应在搜索中包括还是排除所选应用程序。

- 11 单击**目标应用程序位置 (And where destination application)**旁边的链接。
- 12 选择一个或多个应用程序，然后单击**确定 (OK)**。
- 13 单击**期间 (During period)** () 图标，然后选择搜索的时间段。
- 14 单击**搜索 (Search)**。

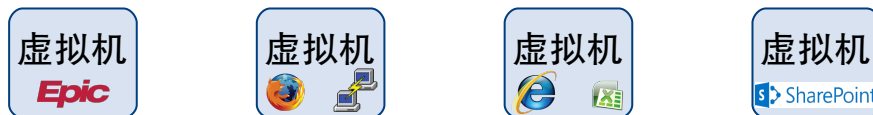
此时将显示按指定条件筛选的搜索结果。单击结果表的任意位置，查看有关访问指定虚拟机和应用程序的用户的信息。

可以通过单击页面右下方的  图标导出此页面上的特定记录或所有记录，将其以 .csv 格式保存到某个目录中。

## 查看出站活动

可以查看安全组或桌面池正在运行的应用程序，然后详细查看报告以查明哪些客户端应用程序正由一组特定的用户建立出站连接。还可以发现正在访问特定应用程序的所有用户组 and 用户，这可以帮助您确定是否需要调整环境中的用户身份防火墙。

图 23-5. 查看出站活动



### 前提条件


- 必须在环境中安装 Guest Introspection。
- 必须向 NSX Manager 注册一个域。有关域注册的信息，请参见[向 NSX Manager 注册 Windows 域](#)。
- 必须在一个或多个虚拟机上启用数据收集。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**活动监控 (Activity Monitoring)**。
- 3 确保左侧窗格中的**出站活动 (Outbound Activity)**选项卡处于选中状态。
- 4 单击**来源 (Originating from)**旁边的链接。  
此时将显示通过 Guest Introspection 发现的所有组。
- 5 选择您要查看资源利用率的用户组的类型。
- 6 在**筛选器 (Filter)**中，选择一个或多个组，然后单击**确定 (OK)**。
- 7 在**应用程序位置 (Where application)**中，选择**包括 (includes)**或**排除 (excludes)**以指示搜索时应包括还是排除所选应用程序。
- 8 单击**应用程序位置 (Where application)**旁边的链接。
- 9 选择一个或多个应用程序，然后单击**确定 (OK)**。

- 10 在**目标位置 (And where destination)**中，选择**包括 (includes)**或**排除 (excludes)**以指示搜索时应包括还是排除所选虚拟机。
- 11 单击**目标位置 (And where destination)**旁边的链接。
- 12 选择一个或多个虚拟机，然后单击**确定 (OK)**。
- 13 单击**期间 (During period)** (📅) 图标，然后选择搜索的时间段。
- 14 单击**搜索 (Search)**。  
滚动到右侧以查看显示的所有信息。

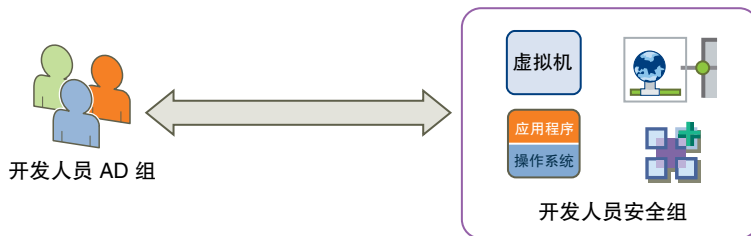
此时将显示按指定条件筛选的搜索结果。单击某个行可查看与该 AD 组中使用指定应用程序访问指定虚拟机的用户有关的信息。

可以通过单击页面右下方的  图标导出此页面上的特定记录或所有记录，将其以 .csv 格式保存到某个目录中。

## 查看清单容器间的交互

您可以查看所定义容器（例如 AD 组、安全组和/或桌面池）之间通过的流量。这可以帮助您确定并配置共享服务的访问权限，并解决清单容器定义、桌面池和 AD 组之间关系的配置错误。

图 23-6. 容器间交互



可以通过单击**搜索 (Search)**使用默认搜索条件执行快速查询，或者根据您的要求自定义查询。


### 前提条件

- 必须在环境中安装 Guest Introspection。
- 必须向 NSX Manager 注册一个域。有关域注册的信息，请参见[向 NSX Manager 注册 Windows 域](#)。
- 必须在一个或多个虚拟机上启用数据收集。


### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**活动监控 (Activity Monitoring)**。
- 3 在左侧窗格中选择**容器间交互 (Inter Container Interaction)**选项卡。
- 4 单击**来源 (Originating from)**旁边的链接。

此时将显示通过 Guest Introspection 发现的所有组。

- 5 选择您要查看资源利用率的用户组的类型。
- 6 在**筛选器 (Filter)**中，选择一个或多个组，然后单击**确定 (OK)**。
- 7 在**目标位置 (Where the destination is)**中，选择**是 (is)**或**不是 (is not)**以指示应在搜索中包括选定组还是排除选定组。
- 8 单击**目标位置 (Where the destination is)**旁边的链接。
- 9 选择组类型。
- 10 在**筛选器 (Filter)**中，选择一个或多个组，然后单击**确定 (OK)**。
- 11 单击**期间 (During period)** () 图标，然后选择搜索的时间段。
- 12 单击**搜索 (Search)**。

此时将显示按指定条件筛选的搜索结果。单击某一行可查看有关访问指定容器的用户的信息。

可以通过单击页面右下方的  图标导出此页面上的特定记录或所有记录，将其以 .csv 格式保存到某个目录中。

## 示例：清单容器查询间的交互

### ■ 验证允许的通信

如果已经在 vCenter 清单中定义了容器，然后添加了允许这些容器之间进行通信的规则，则可以通过对**源自 (Originating from)**和**目标位置 (Where the destination is)**字段中指定的两个容器运行此查询来验证该规则是否生效。

### ■ 验证拒绝的通信

如果已经在 vCenter 清单中定义了容器，然后添加了拒绝这些容器之间进行通信的规则，则可以通过对**源自 (Originating from)**和**目标位置 (Where the destination is)**字段中指定的两个容器运行此查询来验证该规则是否生效。

### ■ 验证拒绝的容器内部通信

如果已实施了不允许同一容器的成员间相互通信的策略，则可以运行此查询以验证该策略是否生效。同时在**源自 (Originating from)**和**目标位置 (Where the destination is)**字段中选择容器。

### ■ 去除不必要的访问权限

假设您已在 vCenter 清单中定义了容器，然后添加了一条允许这些容器之间相互通信的规则。则完全不与其他容器交互的任一容器中可能存在一些成员。您可以选择从相应容器中移除这些成员，以优化安全控制。要检索此类列表，请同时从**源自 (Originating from)**和**目标位置 (Where the destination is)**字段中选择相应的容器。选择**目标位置 (Where the destination is)**字段旁边的**不是 (is not)**。

## 查看出站 AD 组活动

您可以查看已定义的 Active Directory 组的成员之间的流量，并使用该数据优化防火墙规则。

可以通过单击**搜索 (Search)**使用默认搜索条件执行快速查询，或者根据您的要求自定义查询。


### 前提条件

- 必须在环境中安装 Guest Introspection。
- 必须向 NSX Manager 注册一个域。有关域注册的信息，请参见[向 NSX Manager 注册 Windows 域](#)。
- 必须在一个或多个虚拟机上启用数据收集。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**活动监控 (Activity Monitoring)**。
- 3 选择左侧窗格中的**AD 组和容器 (AD Groups & Containers)**选项卡。
- 4 单击**来源 (Originating from)**旁边的链接。  
此时将显示通过 Guest Introspection 发现的所有组。
- 5 选择要包括在搜索中的用户组的类型。
- 6 在**筛选器 (Filter)**中，选择一个或多个组，然后单击**确定 (OK)**。
- 7 在**AD 组位置 (Where AD Group)**中，选择**包括 (includes)**或**排除 (excludes)**以指示应在搜索中包括还是排除所选 AD 组。
- 8 单击**AD 组位置 (Where AD Group)**旁边的链接。
- 9 选择一个或多个 AD 组，然后单击**确定 (OK)**。
- 10 单击**期间 (During period)** ( ) 图标，然后选择搜索的时间段。
- 11 单击**搜索 (Search)**。

此时将显示按指定条件筛选的搜索结果。单击某一行可查看从指定安全组或桌面池访问网络资源的指定 AD 组成员的相关信息。

可以通过单击页面右下方的  图标导出此页面上的特定记录或所有记录，将其以 .csv 格式保存到某个目录中。

## 替代数据收集

在紧急情况下（如网络过载），您可以在全局级别关闭数据收集。此操作会替代所有其他数据收集设置。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**活动监控 (Activity Monitoring)**。
- 3 单击**设置 (Settings)**选项卡。
- 4 选择要覆盖数据收集的 vCenter Server。
- 5 单击**编辑 (Edit)**。



6 取消选中**收集报告数据 (Collect reporting data)**。

7 单击**确定 (OK)**。

## 跟踪流

跟踪流是一个故障排除工具，能够插入数据包并在数据包通过物理网络和逻辑网络时观察该数据包出现的位置。通过观察，可以确定网络的相关信息，例如识别已关闭的节点或阻止数据包被目标接收的防火墙规则。

## 关于跟踪流

当数据包通过覆盖网络和底层网络中的物理及逻辑实体（如 ESXi 主机、逻辑交换机和逻辑路由器）时，跟踪流会将数据包注入到 **vSphere Distributed Switch (VDS)** 端口，并沿着数据包的路径提供各个观察点。这样，您就可以标识数据包到达其目标所经过的一个或多个路径，或者反过来，标识数据包沿着哪个路径时被丢弃。每个实体都会报告输入和输出上的数据包处理，因此您可以确定接收数据包或转发数据包时是否出现问题。

请记住，跟踪流与在客户机虚拟机堆栈之间传送的 **ping** 请求/响应不同。跟踪流执行的操作是在标记的数据包通过覆盖网络时观察这些数据包。在每个数据包通过覆盖网络时，将监视该数据包，直至到达并可传输到目标客户机虚拟机。不过，绝不会将注入的跟踪流数据包实际传输到目标客户机虚拟机。这意味着即使客户机虚拟机电源关闭，跟踪流仍能够成功。

跟踪流支持以下流量类型：

- 第 2 层单播
- 第 3 层单播
- 第 2 层广播
- 第 2 层多播

您可以使用自定义标头字段和数据包大小构造数据包。跟踪流的源始终为虚拟机的虚拟网卡 (vNIC)。目标端点可以是 **NSX** 覆盖或底层中的任何设备。不过，您无法选择位于 **NSX Edge** 服务网关 (ESG) 北部的目标。目标必须位于相同的子网上，或者必须能够通过 **NSX** 分布式逻辑路由器访问目标。

如果源和目标虚拟网卡位于同一第 2 层域中，跟踪流操作将被视为第 2 层。在 **NSX** 中，这意味着它们位于同一 **VXLAN** 网络标识符 (VNI 或分段 ID) 上。例如，当两个虚拟机连接到同一逻辑交换机时，会发生这种情况。

如果配置了 **NSX** 桥接，未知第 2 层数据包将始终发送到网桥。通常，网桥会将这些数据包转发到 **VLAN** 并将跟踪流数据包报告为“已传送”。报告为“已递送”的数据包不一定表示跟踪数据包已传送到指定的目标。

对于第 3 层跟踪流单播流量，两个端点位于不同的逻辑交换机上，且具有连接到分布式逻辑路由器 (DLR) 的不同 VNI。

对于多播流量，源为虚拟机的虚拟网卡，目标为多播组地址。



跟踪流观察可能包括广播的跟踪流数据包观察。如果不知道目标主机的 MAC 地址，ESXi 主机将广播跟踪流数据包。对于广播流量，源为虚拟机的虚拟网卡。广播流量的第 2 层目标 MAC 地址为 FF:FF:FF:FF:FF:FF。要为防火墙检测创建有效的数据包，广播跟踪流操作需要子网前缀长度。子网掩码使 NSX 可以计算数据包的 IP 网络地址。



**小心** 根据部署中逻辑端口的数量，多播和广播跟踪流操作可能会生成大量流量。

使用跟踪流的方式有两种：通过 API 和通过 GUI。API 即为 GUI 使用的 API，但是 API 允许您在数据包中指定确切设置，而 GUI 具有的设置更有限。

GUI 允许您设置以下值：

- 协议---TCP、UDP、ICMP。
- 活动时间 (TTL)。默认值为 64 个跃点。
- TCP 和 UDP 源及目标端口号。默认值为 0。
- TCP 标记。
- ICMP ID 和序列号。两者的默认值均为 0。
- 跟踪流操作的过期超时，以毫秒 (ms) 为单位。默认值为 10,000 ms。
- 以太网帧大小。默认值为每帧 128 字节。最大帧大小为每帧 1000 字节。
- 负载编码。默认值为 Base64。
- 负载值。

## 使用跟踪流进行故障排除

跟踪流在多种场景中非常有用。

跟踪流在以下场景下有用：

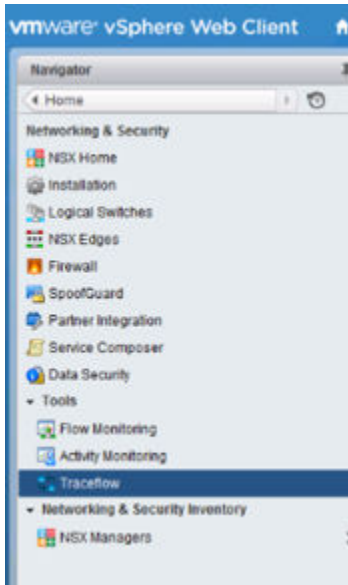
- 排除网络故障以查看流量流经的准确路径
- 监控性能以了解链接使用率
- 规划网络以了解网络在生产环境中的运行方式

### 前提条件

- 跟踪流操作要求 vCenter、NSX Manager、NSX Controller 群集以及主机上的 netcpa 用户环境代理之间能够通信。
- 要使跟踪流按预期工作，请确保控制器群集已连接且处于正常状态。

## 步骤

- 1 在 vCenter Web Client 中，导航到主页 > 网络和安全 > 跟踪流 (Home > Networking & Security > Traceflow)。



- 2 选择流量类型：单播、广播或多播。
- 3 选择源虚拟机的虚拟网卡。

如果虚拟机托管于运行跟踪流的 vCenter Server 中，则可以从列表中选择虚拟机和虚拟网卡。

- 4 对于单播跟踪流，请输入目标虚拟网卡的信息。

目标可以是 NSX 覆盖网络或底层网络中任意设备的虚拟网卡，例如主机、虚拟机、逻辑路由器或 Edge 服务网关。如果目标是运行 VMware Tools 的虚拟机，并且该虚拟机在从中运行跟踪流的同一 vCenter Server 中进行管理，则可以从列表中选择虚拟机和虚拟网卡。

否则，必须输入目标 IP 地址（对于单播第 2 层跟踪流，还需输入 MAC 地址）。可以在设备控制台或 SSH 会话中从设备自身收集此信息。例如，如果目标是 Linux 虚拟机，则可以通过在 Linux 终端中运行 `ifconfig` 命令来获取其 IP 和 MAC 地址。对于逻辑路由器或 Edge 服务网关，可以通过 `show interface` CLI 命令收集信息。

- 5 对于第 2 层广播跟踪流，请输入子网前缀的长度。

数据包仅基于 MAC 地址进行交换。目标 MAC 地址为 FF:FF:FF:FF:FF:FF。

需要提供源和目标 IP 地址，才能使 IP 数据包对防火墙监测有效。

- 6 对于第 2 层多播跟踪流，请输入多播组地址。

数据包仅基于 MAC 地址进行交换。

需要提供源和目标 IP 地址，才能使 IP 数据包有效。在多播情况下，MAC 地址是根据 IP 地址推导出来的。

- 7 配置其他必选和可选设置。

8 单击跟踪 (Trace)。

示例：场景

下例展示的第 2 层跟踪流涉及在同一台 ESXi 主机上运行的两个虚拟机。这两个虚拟机连接到同一个逻辑交换机。

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: web-01a - Network adapter 1 Change...  
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: web-02a - Network adapter 1 Change...  
IP: 172.16.10.12, MAC: 00:50:56:ae:f8:6b

Advanced Options

Protocol: TCP

Source Port: 0

Destination Port: 0

TCP Flags: ☐ FIN ☒ SYN ☐ RST

Timeout (ms): 10000

Frame Size: 128

TTL: 64

Trace

Trace Result: Traceflow delivered observation(s) reported

1 Delivered

Sequence	Observation Type	Host	Component Type	Component Name
0	Injected	esx-01a.corp.local	vNIC	vNIC
1	Received	esx-01a.corp.local	Firewall	Firewall
2	Forwarded	esx-01a.corp.local	Firewall	Firewall
3	Received	esx-01a.corp.local	Firewall	Firewall
4	Forwarded	esx-01a.corp.local	Firewall	Firewall
5	Delivered	esx-01a.corp.local	vNIC	vNIC

下例展示的第 2 层跟踪流涉及分别在两台不同的 ESXi 主机上运行的两个虚拟机。这两个虚拟机连接到同一个逻辑交换机。

**Traceflow**

NSX Manager: 192.168.110.15 (Role: Primary)

**Trace Parameters**

Traffic Type: **Unicast**

Source: web-01a - Network adapter 1 Change...  
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: web-03a - Network adapter 1 Change...  
IP: 172.17.10.11, MAC: 00:50:56:ae:cf:88

▼ Advanced Options

Protocol: **TCP**

Source Port: 0

Destination Port: 0

TCP Flags: ☐ FIN ☒ SYN ☐ RST

Timeout (ms): 10000

Frame Size: 128

TTL: 64

**Trace**

**Trace Result:** Traceflow delivered observation(s) reported

**1 Delivered**

Sequence	Observation Type	Host	Component Type	Component Name
0	Injected	esx-01a.corp.local	vNIC	vNIC
1	Received	esx-01a.corp.local	Firewall	Firewall
2	Forwarded	esx-01a.corp.local	Firewall	Firewall
3	Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
3	Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esx-02a.corp.local	Physical	esx-02a.corp.local
4	Received	esx-02a.corp.local	Physical	esx-02a.corp.local
5	Received	esx-02a.corp.local	Firewall	Firewall
6	Forwarded	esx-02a.corp.local	Firewall	Firewall
7	Delivered	esx-02a.corp.local	vNIC	vNIC

下例展示了一个第 3 层跟踪流。其中的两个虚拟机分别连接到由逻辑路由器分隔的两个不同逻辑交换机。

**Traceflow**

NSX Manager: 192.168.110.15 (Role: Primary)

**Trace Parameters**

Traffic Type: Unicast

Source: \* web-01a - Network adapter 1 Change...  
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: \* db-01a - Network adapter 1 Change...  
IP: 172.16.30.11, MAC: 00:50:56:ae:d4:2b

► Advanced Options

Trace

**Trace Result:** Traceflow delivered observation(s) reported

**1 Delivered**

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-01a.corp.local	vNIC	vNIC
1		Received	esx-01a.corp.local	Firewall	Firewall
2		Forwarded	esx-01a.corp.local	Firewall	Firewall
3		Forwarded	esx-01a.corp.local	Logical Switch	Web-Tier-01
4		Received	esx-01a.corp.local	Logical Router	Local-Distributed-Router
5		Forwarded	esx-01a.corp.local	Logical Router	Local-Distributed-Router
6		Received	esx-01a.corp.local	Logical Switch	DB-Tier-01
7		Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
8		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
8		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
9		Received	esx-02a.corp.local	Firewall	Firewall
10		Forwarded	esx-02a.corp.local	Firewall	Firewall
11		Delivered	esx-02a.corp.local	vNIC	vNIC

下例展示了三个虚拟机连接到同一个逻辑交换机的部署中的广播跟踪流。其中的两个虚拟机位于一个主机 (esx-01a) 上，第三个虚拟机位于另一个主机 (esx-02a) 上。广播是从主机 192.168.210.53 上的其中一个虚拟机发送的。

**Traceflow**

NSX Manager: 192.168.110.15 (Role: Primary)

**Trace Parameters**

Traffic Type: **L2 Broadcast** High volume of traffic may get generated for this traffic type.

Source: web-01a - Network adapter 1 [Change...](#) Subnet Prefix Length: 24

IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d IP: 172.16.10.255, MAC: FF:FF:FF:FF:FF:FF

► Advanced Options

**Trace**

Trace Result: Traceflow delivered observation(s) reported

**3 Delivered**

Sequence	Observation Type	Host	Component Type	Component Name
0	Injected	esx-01a.corp.local	vNIC	vNIC
1	Received	esx-01a.corp.local	Firewall	Firewall
2	Forwarded	esx-01a.corp.local	Firewall	Firewall
3	Forwarded	esx-01a.corp.local	Logical Switch	Web-Tier-01
3	Received	esx-01a.corp.local	Firewall	Firewall
3	Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
3	Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4	Forwarded	esx-01a.corp.local	Firewall	Firewall
4	Received	esx-02a.corp.local	Physical	esx-02a.corp.local
4	Received	esx-02a.corp.local	Physical	esx-02a.corp.local
5	Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5	Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5	Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5	Forwarded	esxmgt-02a.corp.local	Logical Switch	Web-Tier-01
5	Delivered	esxmgt-02a.corp.local	vNIC	vNIC
5	Delivered	esx-01a.corp.local	vNIC	vNIC
5	Forwarded	esx-02a.corp.local	Logical Switch	Web-Tier-01
5	Forwarded	esx-02a.corp.local	Logical Switch	Web-Tier-01
5	Received	esx-02a.corp.local	Firewall	Firewall
6	Forwarded	esx-02a.corp.local	Firewall	Firewall
7	Delivered	esx-02a.corp.local	vNIC	vNIC

下例显示了在配置多播的部署中发送多播流量时会出现的情况。

**Traceflow**

NSX Manager: 192.168.110.15 (Role: Primary)

**Trace Parameters**

Traffic Type: L2 Multicast High volume of traffic may get generated for this traffic type.

Source: web-01a - Network adapter 1 Change...  
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination IP: 239.0.0.1 e.g. 239.0.0.1  
IP: 239.0.0.1, MAC: 01:00:5e:00:00:01

► Advanced Options

**Trace**

Trace Result: Traceflow delivered observation(s) reported

**3 Delivered**

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-01a.corp.local	vNIC	vNIC
1		Received	esx-01a.corp.local	Firewall	Firewall
2		Forwarded	esx-01a.corp.local	Firewall	Firewall
3		Received	esx-01a.corp.local	Firewall	Firewall
3		Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
3		Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Received	esxmgt-02a.corp.local	Physical	esxmgt-02a.corp.local
4		Forwarded	esx-01a.corp.local	Firewall	Firewall
4		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
4		Received	esx-02a.corp.local	Physical	esx-02a.corp.local
5		Delivered	esxmgt-02a.corp.local	vNIC	vNIC
5		Delivered	esx-01a.corp.local	vNIC	vNIC
5		Received	esx-02a.corp.local	Firewall	Firewall
6		Forwarded	esx-02a.corp.local	Firewall	Firewall
7		Delivered	esx-02a.corp.local	vNIC	vNIC

下例显示了因应用阻止将 ICMP 流量发送到目标地址的分布式防火墙规则而丢弃跟踪流时出现的情况。请注意，流量永远不会离开原始主机，即使目标虚拟机位于另一个主机上也是如此。

**Traceflow**

NSX Manager: 192.168.110.15 (Role: Primary)

**Trace Parameters**

Traffic Type: Unicast

Source: web-02a - Network adapter 1 Change...  
IP: 172.16.10.12, MAC: 00:50:56:ae:f8:6b

Destination: web-03a - Network adapter 1 Change...  
IP: 172.17.10.11, MAC: 00:50:56:ae:cf:88

► Advanced Options

**Trace**

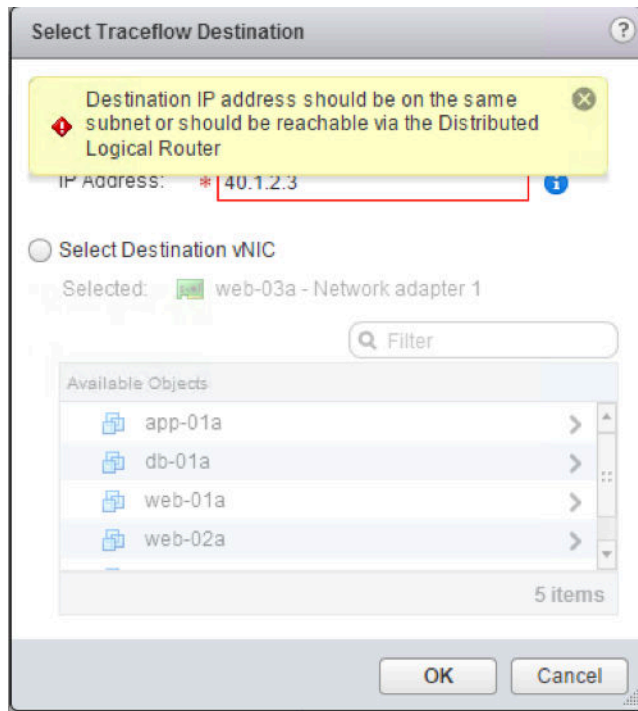
Trace Result: Traceflow dropped observation(s) reported

**1 Dropped**

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-01a.corp.local	vNIC	vNIC
1		Received	esx-01a.corp.local	Firewall	Firewall
2		Dropped	esx-01a.corp.local	Firewall	Firewall (Rule - 1013)



下例显示了跟踪流目标位于 **Edge** 服务网关的另一端时出现的情况，例如 **Internet** 或必须通过 **Edge** 服务网关路由的任何内部目标上的 **IP** 地址。从设计上不允许使用跟踪流，因为仅位于同一子网上或可通过分布式逻辑路由器 (DLR) 访问的目标支持跟踪流。



下例显示了跟踪流目标是位于另一个子网中已关闭电源的虚拟机时出现的情况。

**Traceflow**

NSX Manager: 192.168.110.15 (Role: Primary)

**Trace Parameters**

Traffic Type: Unicast

Source: \* app-01a - Network adapter 1 Change...  
IP: 172.16.20.11, MAC: 00:50:56:ae:23:b9

Destination: \* db-01a - Network adapter 1 Change...  
IP: 172.16.30.11, MAC: 00:50:56:ae:d...

Advanced Options

Trace

**Trace Result:** No delivered or dropped observations reported

Sequence	1 ▲	Observation Type	Host	Component Type	Component Name
0		Injected	esx-02a.corp.local	vNIC	vNIC
1		Received	esx-02a.corp.local	Firewall	Firewall
2		Forwarded	esx-02a.corp.local	Firewall	Firewall
3		Forwarded	esx-02a.corp.local	Logical Switch	App-Tier-01
4		Received	esx-02a.corp.local	Logical Router	Local-Distributed-Router
5		Forwarded	esx-02a.corp.local	Logical Router	Local-Distributed-Router
6		Received	esx-02a.corp.local	Logical Switch	DB-Tier-01



## NSX Edge VPN 配置示例

此方案包含 NSX Edge 与另一端的 Cisco 或 WatchGuard VPN 之间的基本点对点 IPSEC VPN 连接的配置示例。

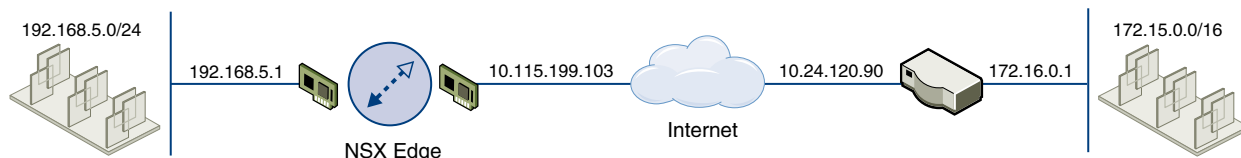
对于此方案，NSX Edge 会将内部网络 192.0.2.0/24 连接到 Internet。NSX Edge 接口配置如下：

- 上行链路接口：198.51.100.1
- 内部接口：192.0.2.1

远程网关会将 172.16.0.0/16 内部网络连接到 Internet。远程网关接口将按如下方式进行配置：

- 上行链路接口：10.24.120.90/24
- 内部接口：172.16.0.1/16

图 24-1. 连接到远程 VPN 网关的 NSX Edge



**注** 对于从 NSX Edge 到 NSX Edge 的 IPSEC 隧道，可以通过将第二个 NSX Edge 设置为远程网关的方式来使用同一个方案。

本章讨论了以下主题：

- [术语](#)
- [IKE 阶段 1 和阶段 2](#)
- [配置 IPsec VPN 服务示例](#)
- [使用 Cisco 2821 集成服务路由器](#)
- [使用 Cisco ASA 5510](#)
- [配置 WatchGuard Firebox X500](#)
- [NSX Edge 配置故障排除示例](#)

## 术语

IPSec 是开放式标准的框架。大量的技术术语可参阅下列日志：**NSX Edge** 日志及其他 VPN 设备（用于对 IPSEC VPN 进行故障排除）的日志。

您可能会遇到以下标准：

- ISAKMP（Internet 安全关联和密钥管理协议）是一个由 RFC 2408 定义的协议，用于在 Internet 环境中建立安全关联 (SA) 和加密密钥。ISAKMP 仅为身份验证和密钥交换提供一个框架，与密钥交换无关。
- Oakley 是一个密钥协商协议，允许完成身份验证的双方采用 Diffie-Hellman 密钥交换算法越过不安全的网络连接交换加密密钥。
- IKE（Internet 密钥交换）是 ISAKMP 框架和 Oakley 的组合。NSX Edge 提供 IKEv1。
- Diffie-Hellman (DH) 私钥交换是一个加密协议，允许互不认识的双方通过不安全的通信通道共建一个共享密钥。VSE 支持 DH 组 2（1024 位）和组 5（1536 位）。

## IKE 阶段 1 和阶段 2

IKE 是用于排列已通过身份验证的安全通信的标准方法。

### 阶段 1 参数

阶段 1 设置对等站点的双向身份验证，协商加密参数，并创建会话密钥。NSX Edge 使用的阶段 1 参数如下：

- 主模式
- TripleDES/AES [可配置]
- SHA-1
- MODP 组 2（1024 位）
- 预共享密钥 [可配置]
- SA 生命周期为 28800 秒（8 个小时），未重新加密千字节
- ISAKMP 激进模式已禁用

### 阶段 2 参数

IKE 阶段 2 通过创建要供 IPSec 使用的加密材料来协商 IPSec 隧道（通过将 IKE 阶段 1 密钥用作基准或执行新密钥交换）。NSX Edge 支持的 IKE 阶段 2 参数如下：

- TripleDES/AES [将与阶段 1 设置相匹配]
- SHA-1
- ESP 隧道模式
- MODP 组 2（1024 位）

- 用于重新加密的完全向前保密
- SA 生命周期为 3600 秒（1 个小时），未重新加密千字节
- 用于两个使用 IPv4 子网的网络之间所有 IP 协议和所有端口的选择器

## 事务模式示例

NSX Edge 支持阶段 1 的“主模式”和阶段 2 的“快速模式”。

NSX Edge 建议使用需要 PSK、3DES/AES128、sha1 和 DH Group 2/5 的策略。对等站点必须接受该策略；否则，协商阶段将失败。

### 阶段 1：主模式事务

此示例显示从 NSX Edge 启动的阶段 1 协商到 Cisco 设备的交换。

以下事务按顺序发生在处于“主模式”状态下的 NSX Edge 和 Cisco VPN 设备之间。

#### 1 NSX Edge 到 Cisco

- 建议：加密 3des-cbc、sha、psk、group5(group2)
- DPD 已启用

#### 2 Cisco 到 NSX Edge

- 包含 Cisco 选择的建议
- 如果 Cisco 设备不接受 NSX Edge 在第一步中发送的任何参数，则 Cisco 设备将发送带有标记 NO\_PROPOSAL\_CHOSEN 的消息并终止协商。

#### 3 NSX Edge 到 Cisco

- DH 密钥和当前值

#### 4 Cisco 到 NSX Edge

- DH 密钥和当前值

#### 5 NSX Edge 到 Cisco（已加密）

- 包括 ID (PSK)

#### 6 Cisco 到 NSX Edge（已加密）

- 包括 ID (PSK)
- 如果 Cisco 设备发现 PSK 不匹配，则 Cisco 设备将发送带有标记 INVALID\_ID\_INFORMATION 的消息，阶段 1 失败。

### 阶段 2：快速模式事务

以下事务按顺序发生在处于“快速模式”状态下的 NSX Edge 和 Cisco VPN 设备之间。

#### 1 NSX Edge 到 Cisco

NSX Edge 建议针对对等站点使用阶段 2 策略。例如：

```
Aug 26 12:16:09 weiqing-desktop
ipsec[5789]:
"s1-c1" #2: initiating Quick Mode
PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
{using isakmp#1 msgid:d20849ac
proposal=3DES(3)_192-SHA1(2)_160
pfsgroup=OAKLEY_GROUP_MODP1024}
```

## 2 Cisco 到 NSX Edge

如果 Cisco 设备未发现任何与建议相匹配的策略，它将发送回 NO\_PROPOSAL\_CHOSEN。否则，Cisco 设备将发送已选择的一组参数。

## 3 NSX Edge 到 Cisco

为方便调试，可以在 NSX Edge 上启用 IPsec 日志记录，并在 Cisco 上启用加密调试 (debug crypto isakmp <level>)。

# 配置 IPsec VPN 服务示例

必须配置 VPN 参数，然后才能启用 IPSEC 服务。

### 步骤

#### 1 配置 NSX Edge VPN 参数示例

必须在 NSX Edge 上配置至少一个外部 IP 地址才能提供 IPsec VPN 服务。

#### 2 启用 IPsec VPN 服务示例

必须启用 IPsec VPN 服务，以便流量从本地子网流向对等子网。

# 配置 NSX Edge VPN 参数示例

必须在 NSX Edge 上配置至少一个外部 IP 地址才能提供 IPsec VPN 服务。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**监控**选项卡，然后单击 **VPN** 选项卡。
- 5 单击 **IPsec VPN**。
- 6 单击**添加 (+)** 图标。
- 7 键入 IPsec VPN 的名称。
- 8 在**本地 ID** 中键入 NSX Edge 实例的 IP 地址。此 ID 将成为远程站点上的对等 ID。

**9** 键入本地端点的 IP 地址。

如果您使用预共享密钥将一个 IP 添加到 IP 隧道，则本地 ID 和本地端点 IP 可能相同。

**10** 采用 CIDR 格式键入要在站点之间共享的子网。使用逗号分隔符键入多个子网。**11** 键入“对等 ID”以唯一标识对等站点。对于使用证书身份验证的对等站点，此 ID 必须是对等站点证书中的公用名称。对于 PSK 对等站点，此 ID 可以是任何字符串。VMware 建议您使用 VPN 的公用 IP 地址或 VPN 服务的 FQDN 作为对等 ID。**12** 在“对等端点”中键入对等站点的 IP 地址。如果将其留空，则 NSX Edge 会等待对等设备请求连接。**13** 采用 CIDR 格式键入对等子网的内部 IP 地址。使用逗号分隔符键入多个子网。**14** 选择“加密算法”。**15** 在“身份验证方法”中，选择下列选项之一：

选项	描述
PSK (预共享密钥)	表示将使用在 NSX Edge 与对等站点之间共享的密钥进行身份验证。密钥可以是最大长度为 128 字节的字符串。
证书	表示将使用在全局级别定义的证书进行身份验证。

**16** 如果匿名站点将连接至 VPN 服务，则键入共享密钥。**17** 单击**显示共享密钥**，以便在对等站点上显示该密钥。**18** 在 Diffie-Hellman (DH) Group 中，选择将允许对等站点和 NSX Edge 通过非安全通信通道建立共享密钥的加密方案。**19** 根据需要更改 MTU 阈值。**20** 选择是启用还是禁用“完全向前保密 (PFS)”阈值。在 IPsec 协商中，完全向前保密 (PFS) 可确保每个新加密密钥都与之前的任何密钥无关。**21** 单击**确定**。

NSX Edge 创建从本地子网到对等子网的隧道。

**后续步骤**

启用 IPsec VPN 服务。

**启用 IPsec VPN 服务示例**

必须启用 IPsec VPN 服务，以便流量从本地子网流向对等子网。

**步骤****1** 登录到 vSphere Web Client。**2** 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。**3** 双击一个 NSX Edge。**4** 单击**监控**选项卡，然后单击 **VPN** 选项卡。

5 单击 **IPSec VPN**。

6 单击 **启用**。

#### 后续步骤

单击 **启用日志记录**，以记录在本地子网和对等子网之间流动的流量。

## 使用 Cisco 2821 集成服务路由器

以下介绍了使用 Cisco IOS 执行的配置。

#### 步骤

##### 1 配置界面和默认路由

```
interface GigabitEthernet0/0
ip address 10.24.120.90 255.255.252.0
duplex auto
speed auto
crypto map MYVPN
!
interface GigabitEthernet0/1
ip address 172.16.0.1 255.255.0.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 10.24.123.253
```

##### 2 配置 IKE 策略

```
Router# config term
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# encryption 3des
Router(config-isakmp)# group 2
Router(config-isakmp)# hash sha
Router(config-isakmp)# lifetime 28800
Router(config-isakmp)# authentication
pre-share
Router(config-isakmp)# exit
```

##### 3 将每个对等设备与其预共享密钥进行匹配

```
Router# config term
Router(config)# crypto isakmp key vshield
address 10.115.199.103
Router(config-isakmp)# exit
```

#### 4 定义 IPSEC 转换

```
Router# config term
Router(config)# crypto ipsec transform-set
 myset esp-3des esp-sha-hmac
Router(config-isakmp)# exit
```

#### 5 创建 IPSEC 访问列表

```
Router# config term
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# access-list 101 permit ip
 172.16.0.0 0.0.255.255 192.168.5.0 0.0.0.255
Router(config)# exit
```

#### 6 将策略与加密映射绑定并对其进行标记

在下例中，该加密映射标记为 MYVPN

```
Router# config term
Router(config)# crypto map MYVPN 1
 ipsec-isakmp
% NOTE: This new crypto map will remain
disabled until a peer and a valid
access list have been configured.
Router(config-crypto-map)# set transform-set
 myset
Router(config-crypto-map)# set pfs group1
Router(config-crypto-map)# set peer
 10.115.199.103
Router(config-crypto-map)# match address 101
Router(config-crypto-map)# exit
```

### 示例：配置

```
router2821#show running-config output
Building configuration...

Current configuration : 1263 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2821
!
boot-start-marker
boot-end-marker
!
! card type command needed for slot 0
```

```

! card type command needed for slot 1
enable password cisco
!
no aaa new-model
!
resource policy
!
ip subnet-zero
!
ip cef
!no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key vshield address 10.115.199.103
!
crypto ipsec transform-set myset esp-3des
 esp-sha-hmac
!
crypto map MYVPN 1 ipsec-isakmp
set peer 10.115.199.103
set transform-set myset
set pfs group1
match address 101
!
interface GigabitEthernet0/0
ip address 10.24.120.90 255.255.252.0
duplex auto
speed auto
crypto map MYVPN
!
interface GigabitEthernet0/1
ip address 172.16.0.1 255.255.0.0
duplex auto
speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.24.123.253
!
ip http server
no ip http secure-server
!
access-list 101 permit ip 172.16.0.0
 0.0.255.255 192.168.5.0 0.0.0.255
!
control-plane
!
line con 0
line aux 0
line vty 0 4

```



```

password cisco
login
line vty 5 15
password cisco
login
!
scheduler allocate 20000 1000
!
end

```

## 使用 Cisco ASA 5510

使用以下输出配置 Cisco ASA 5510。

```

ciscoasa# show running-config output
: Saved
:
ASA Version 8.2(1)18
!
hostname ciscoasa
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
nameif untrusted
security-level 100
ip address 10.24.120.90 255.255.252.0
!
interface Ethernet0/1
nameif trusted
security-level 90
ip address 172.16.0.1 255.255.0.0
!
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
boot system disk0:/asa821-18-k8.bin

```

```

ftp mode passive
access-list ACL1 extended permit ip 172.16.0.0 255.255.0.0
 192.168.5.0 255.255.255.0
access-list ACL1 extended permit ip 192.168.5.0 255.255.255.0
 172.16.0.0 255.255.0.0
access-list 101 extended permit icmp any any
pager lines 24
mtu untrusted 1500
mtu trusted 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any untrusted
icmp permit any trusted
no asdm history enable
arp timeout 14400
access-group 101 in interface untrusted
access-group 101 out interface untrusted
access-group 101 in interface trusted
access-group 101 out interface trusted
route untrusted 10.115.0.0 255.255.0.0 10.24.123.253 1
route untrusted 192.168.5.0 255.255.255.0 10.115.199.103 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00
 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
crypto ipsec transform-set MYSET esp-3des esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto map MYVPN 1 match address ACL1
crypto map MYVPN 1 set pfs
crypto map MYVPN 1 set peer 10.115.199.103
crypto map MYVPN 1 set transform-set MYSET
crypto map MYVPN interface untrusted
crypto isakmp enable untrusted
crypto isakmp policy 1
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
telnet 10.0.0.0 255.0.0.0 untrusted
telnet timeout 5
ssh timeout 5
console timeout 0
no threat-detection basic-threat
no threat-detection statistics access-list
no threat-detection statistics tcp-intercept

```

```
username admin password f3UhLvUj1QsXsuK7 encrypted
tunnel-group 10.115.199.103 type ipsec-l2l
tunnel-group 10.115.199.103 ipsec-attributes
pre-shared-key *
!
!
prompt hostname context
Cryptochecksum:29c3cc49460831ff6c070671098085a9
: end
```

## 配置 WatchGuard Firebox X500

可以将 WatchGuard Firebox X500 配置为远程网关。

**注** 有关详细步骤，请参见 WatchGuard Firebox 文档。

### 步骤

- 1 在 Firebox System Manager 中，选择工具 (Tools) > 策略管理器 (Policy Manager) >。
- 2 在“策略管理器”中，选择网络 (Network) > 配置 (Configuration)。
- 3 配置此界面并单击确定 (OK)。
- 4 （可选）选择网络 (Network) > 路由 (Routes) 以配置默认路由。
- 5 选择网络 (Network) > 分支机构 VPN (Branch Office VPN) > 手动 IPsec (Manual IPsec) 以配置远程网关。
- 6 在“IPsec 配置”对话框中，单击网关 (Gateways) 以配置 IPSEC 远程网关。
- 7 在“IPsec 配置”对话框中，单击隧道 (Tunnels) 以配置隧道。
- 8 在“IPsec 配置”对话框中，单击添加 (Add) 以添加路由策略。
- 9 单击关闭 (Close)。
- 10 确认该隧道已打开。

## NSX Edge 配置故障排除示例

使用此处的信息可帮助您解决设置中的协商问题。

### 成功协商（阶段 1 和阶段 2）

下例显示了 NSX Edge 和 Cisco 设备之间一次成功协商的结果。

## NSX Edge

在 NSX Edge 命令行界面（`ipsec auto -status`，即 `show service ipsec` 命令的一部分）中：

```
000 #2: "s1-c1":500 STATE_QUICK_I2 (sent QI2, IPsec SA established);
 EVENT_SA_REPLACE in 2430s; newest IPSEC; eroute owner; isakmp#1; idle;
 import:admin initiate
000 #2: "s1-c1" esp.f5f6877d@10.20.131.62 esp.7aaf335f@10.20.129.80
 tun.0@10.20.131.62 tun.0@10.20.129.80 ref=0 refhim=4294901761
000 #1: "s1-c1":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in
 27623s; newest ISAKMP; lastdpd=0s(seq in:0 out:0); idle;
 import:admin initiate
```

## Cisco

```
ciscoasa# show crypto isakmp sa detail

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

IKE Peer: 10.20.129.80
Type : L2L Role : responder
Rekey : no State : MM_ACTIVE
Encrypt : 3des Hash : SHA
Auth : preshared Lifetime: 28800
Lifetime Remaining: 28379
```

## 阶段 1 策略不匹配

下面列出了阶段 1 策略不匹配错误日志。

## NSX Edge

NSX Edge 在 `STATE_MAIN_I1` 状态下挂起。在 `/var/log/messages` 中查找显示对等站点返回包含“`NO_PROPOSAL_CHOSEN`”集的 IKE 消息的信息。

```
000 #1: "s1-c1":500 STATE_MAIN_I1 (sent MI1,
 expecting MR1); EVENT_RETRANSMIT in 7s; nodpd; idle;
 import:admin initiate
000 #1: pending Phase 2 for "s1-c1" replacing #0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
 | got payload 0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
 | ***parse ISAKMP Notification Payload:
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
 | next payload type: ISAKMP_NEXT_NONE
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: | length: 96
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
 | DOI: ISAKMP_DOI_IPSEC
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: | protocol ID: 0
```

```
Aug 26 12:31:25 weiqing-desktop ipsec[6569]: | SPI size: 0
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
| Notify Message Type: NO_PROPOSAL_CHOSEN
Aug 26 12:31:25 weiqing-desktop ipsec[6569]:
"s1-c1" #1: ignoring informational payload,
type NO_PROPOSAL_CHOSEN msgid=00000000
```

## Cisco

如果已启用调试加密，则会打印错误消息以显示未接受任何建议。

```
ciscoasa# Aug 26 18:17:27 [IKEv1]:
IP = 10.20.129.80, IKE_DECODE RECEIVED
Message (msgid=0) with payloads : HDR + SA (1)
+ VENDOR (13) + VENDOR (13) + NONE (0) total length : 148
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
processing SA payload
Aug 26 18:17:27 [IKEv1]: Phase 1 failure: Mismatched attribute
types for class Group Description: Rcv'd: Group 5
Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: Phase 1 failure: Mismatched attribute
types for class Group Description: Rcv'd: Group 5
Cfg'd: Group 2
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
Message (msgid=0) with payloads : HDR + NOTIFY (11)
+ NONE (0) total length : 124
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80,
All SA proposals found unacceptable
Aug 26 18:17:27 [IKEv1]: IP = 10.20.129.80, Error processing
payload: Payload ID: 1
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE MM Responder
FSM error history (struct &0xd8355a60) <state>, <event>:
MM_DONE, EV_ERROR-->MM_START, EV_RCV_MSG-->MM_START,
EV_START_MM-->MM_START, EV_START_MM-->MM_START,
EV_START_MM-->MM_START, EV_START_MM-->MM_START,
EV_START_MM-->MM_START, EV_START_MM
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, IKE SA
MM:9e0e4511 terminating: flags 0x01000002, refcnt 0,
tuncnt 0
Aug 26 18:17:27 [IKEv1 DEBUG]: IP = 10.20.129.80, sending
delete/delete with reason message
```

## 阶段 2 不匹配

下面列出了阶段 2 策略不匹配错误日志。

## NSX Edge

NSX Edge 在 STATE\_QUICK\_I1 状态下挂起。日志消息显示对等站点发送了一条 NO\_PROPOSAL\_CHOSEN 消息。

```
000 #2: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
 QR1); EVENT_RETRANSMIT in 11s; lastdpd=-1s(seq in:0 out:0);
 idle; import:admin initiate
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | got payload
 0x800(ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | ***parse
 ISAKMP Notification Payload:
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | next payload
 type: ISAKMP_NEXT_NONE
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | length: 32
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: |
 | DOI: ISAKMP_DOI_IPSEC
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | protocol ID: 3
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | SPI size: 16
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: | Notify Message
 Type: NO_PROPOSAL_CHOSEN
Aug 26 12:33:54 weiqing-desktop ipsec[6933]: "s1-c1" #3:
 ignoring informational payload, type NO_PROPOSAL_CHOSEN
 msgid=00000000
```

## Cisco

调试消息显示阶段 1 已完成，但阶段 2 因为策略协商失败而失败。

```
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80,
 IP = 10.20.129.80, PHASE 1 COMPLETED
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, Keep-alive type
 for this connection: DPD
Aug 26 16:03:49 [IKEv1 DEBUG]: Group = 10.20.129.80,
 IP = 10.20.129.80, Starting P1 rekey timer: 21600 seconds
Aug 26 16:03:49 [IKEv1]: IP = 10.20.129.80, IKE_DECODE RECEIVED
 Message (msgid=b2cdcb13) with payloads : HDR + HASH (8)
 + SA (1) + NONCE (10) + KE (4) + ID (5) + ID (5) + NONE (0)
 total length : 288
.
.
.
Aug 26 16:03:49 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
 Session is being torn down. Reason: Phase 2 Mismatch
```

## PFS 不匹配

下面列出了 PFS 不匹配错误日志。

## NSX Edge

PFS 协商为阶段 2 的一部分。如果 PFS 不匹配，则该行为类似于[阶段 2 不匹配](#)中所述的失败案例。

```
000 #4: "s1-c1":500 STATE_QUICK_I1 (sent QI1, expecting
 QR1); EVENT_RETRANSMIT in 8s; lastdpd=-1s(seq in:0 out:0);
 idle; import:admin initiate
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | got payload 0x800
 (ISAKMP_NEXT_N) needed: 0x0 opt: 0x0
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
 | ***parse ISAKMP Notification Payload:
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | next payload
 type: ISAKMP_NEXT_NONE
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | length: 32
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
 | DOI: ISAKMP_DOI_IPSEC
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | protocol ID: 3
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | SPI size: 16
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | Notify Message
 Type: NO_PROPOSAL_CHOSEN
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: "s1-c1" #1: ignoring
 informational payload, type NO_PROPOSAL_CHOSEN
 msgid=00000000
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info: fa 16 b3 e5
 91 a9 b0 02 a3 30 e1 d9 6e 5a 13 d4
Aug 26 12:35:52 weiqing-desktop ipsec[7312]: | info: 93 e5 e4 d7
Aug 26 12:35:52 weiqing-desktop ipsec[7312]:
 | processing informational NO_PROPOSAL_CHOSEN (14)
```

## Cisco

```
<BS>Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
 IP = 10.20.129.80, sending delete/delete with
 reason message
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
 IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
 IP = 10.20.129.80, constructing blank hash payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
 IP = 10.20.129.80, constructing IKE delete payload
Aug 26 19:00:26 [IKEv1 DEBUG]: Group = 10.20.129.80,
 IP = 10.20.129.80, constructing qm hash payload
Aug 26 19:00:26 [IKEv1]: IP = 10.20.129.80, IKE_DECODE SENDING
 Message (msgid=19eb1e59) with payloads : HDR + HASH (8)
 + DELETE (12) + NONE (0) total length : 80
Aug 26 19:00:26 [IKEv1]: Group = 10.20.129.80, IP = 10.20.129.80,
 Session is being torn down. Reason: Phase 2 Mismatch
```

## PSK 不匹配

下面列出了 PSK 不匹配错误日志

### NSX Edge

在阶段 1 的最后一轮中协商 PSK。如果 PSK 协商失败，则 NSX Edge 状态为 STATE\_MAIN\_I4。对等站点将发送包含 INVALID\_ID\_INFORMATION 的消息。

```
Aug 26 11:55:55 weiqing-desktop ipsec[3855]:
 "s1-c1" #1: transition from state STATE_MAIN_I3 to
 state STATE_MAIN_I4
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
 STATE_MAIN_I4: ISAKMP SA established
 {auth=OAKLEY_PRESHARED_KEY
 cipher=oakley_3des_cbc_192 prf=oakley_sha group=modp1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1: Dead Peer
 Detection (RFC 3706): enabled
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #2:
 initiating Quick Mode PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
 {using isakmp#1 msgid:e8add10e proposal=3DES(3)_192-SHA1(2)_160
 pfsgroup=OAKLEY_GROUP_MODP1024}
Aug 26 11:55:55 weiqing-desktop ipsec[3855]: "s1-c1" #1:
 ignoring informational payload, type INVALID_ID_INFORMATION
 msgid=00000000
```

### Cisco

```
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191,
 IKE_DECODE SENDING Message (msgid=0) with payloads : HDR
 + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13)
 + VENDOR (13) + VENDOR (13) + NAT-D (130) + NAT-D (130)
 + NONE (0) total length : 304
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
 IP = 10.115.199.191, Received encrypted Oakley Main Mode
 packet with invalid payloads, MessID = 0
Aug 26 15:27:07 [IKEv1]: IP = 10.115.199.191, IKE_DECODE SENDING
 Message (msgid=0) with payloads : HDR + NOTIFY (11)
 + NONE (0) total length : 80
Aug 26 15:27:07 [IKEv1]: Group = 10.115.199.191,
 IP = 10.115.199.191, ERROR, had problems decrypting
 packet, probably due to mismatched pre-shared key.
 Aborting
```



## 成功协商的数据包捕获

下面列出了 NSX Edge 和 Cisco 设备之间成功协商的数据包捕获会话。

```
No. Time Source Destination Protocol Info
9203 768.394800 10.20.129.80 10.20.131.62 ISAKMP Identity Protection
 (Main Mode)

Frame 9203 (190 bytes on wire, 190 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
 Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
 Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 0000000000000000
 Next payload: Security Association (1)
 Version: 1.0
 Exchange type: Identity Protection (Main Mode) (2)
 Flags: 0x00
 Message ID: 0x00000000
 Length: 148
 Security Association payload
 Next payload: Vendor ID (13)
 Payload length: 84
 Domain of interpretation: IPSEC (1)
 Situation: IDENTITY (1)
 Proposal payload # 0
 Next payload: NONE (0)
 Payload length: 72
 Proposal number: 0
 Protocol ID: ISAKMP (1)
 SPI Size: 0
 Proposal transforms: 2
 Transform payload # 0
 Next payload: Transform (3)
 Payload length: 32
 Transform number: 0
 Transform ID: KEY_IKE (1)
 Life-Type (11): Seconds (1)
 Life-Duration (12): Duration-Value (28800)
 Encryption-Algorithm (1): 3DES-CBC (5)
 Hash-Algorithm (2): SHA (2)
 Authentication-Method (3): PSK (1)
 Group-Description (4): 1536 bit MODP group (5)
 Transform payload # 1
 Next payload: NONE (0)
 Payload length: 32
 Transform number: 1
 Transform ID: KEY_IKE (1)
 Life-Type (11): Seconds (1)
 Life-Duration (12): Duration-Value (28800)
 Encryption-Algorithm (1): 3DES-CBC (5)
```

```

 Hash-Algorithm (2): SHA (2)
 Authentication-Method (3): PSK (1)
 Group-Description (4): Alternate 1024-bit MODP group (2)
Vendor ID: 4F456C6A405D72544D42754D
 Next payload: Vendor ID (13)
 Payload length: 16
 Vendor ID: 4F456C6A405D72544D42754D
Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)
 Next payload: NONE (0)
 Payload length: 20
 Vendor ID: RFC 3706 Detecting Dead IKE Peers (DPD)

```

No.	Time	Source	Destination	Protocol Info
9204	768.395550	10.20.131.62	10.20.129.80	ISAKMP Identity Protection (Main Mode)

```

Frame 9204 (146 bytes on wire, 146 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
 Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
 Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Security Association (1)
 Version: 1.0
 Exchange type: Identity Protection (Main Mode) (2)
 Flags: 0x00
 Message ID: 0x00000000
 Length: 104
 Security Association payload
 Next payload: Vendor ID (13)
 Payload length: 52
 Domain of interpretation: IPSEC (1)
 Situation: IDENTITY (1)
 Proposal payload # 1
 Next payload: NONE (0)
 Payload length: 40
 Proposal number: 1
 Protocol ID: ISAKMP (1)
 SPI Size: 0
 Proposal transforms: 1
 Transform payload # 1
 Next payload: NONE (0)
 Payload length: 32
 Transform number: 1
 Transform ID: KEY_IKE (1)
 Encryption-Algorithm (1): 3DES-CBC (5)
 Hash-Algorithm (2): SHA (2)
 Group-Description (4): Alternate 1024-bit MODP group (2)
 Authentication-Method (3): PSK (1)
 Life-Type (11): Seconds (1)
 Life-Duration (12): Duration-Value (28800)
 Vendor ID: Microsoft L2TP/IPSec VPN Client

```

Next payload: NONE (0)  
 Payload length: 24  
 Vendor ID: Microsoft L2TP/IPSec VPN Client

No.	Time	Source	Destination	Protocol Info
9205	768.399599	10.20.129.80	10.20.131.62	ISAKMP Identity Protection (Main Mode)

Frame 9205 (222 bytes on wire, 222 bytes captured)  
 Ethernet II, Src: Vmware\_9d:2c:dd (00:50:56:9d:2c:dd),  
 Dst: Cisco\_80:70:f5 (00:13:c4:80:70:f5)  
 Internet Protocol, Src: 10.20.129.80 (10.20.129.80),  
 Dst: 10.20.131.62 (10.20.131.62)  
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)  
 Internet Security Association and Key Management Protocol  
 Initiator cookie: 92585D2D797E9C52  
 Responder cookie: 34704CFC8C8DBD09  
 Next payload: Key Exchange (4)  
 Version: 1.0  
 Exchange type: Identity Protection (Main Mode) (2)  
 Flags: 0x00  
 Message ID: 0x00000000  
 Length: 180  
 Key Exchange payload  
 Next payload: Nonce (10)  
 Payload length: 132  
 Key Exchange Data (128 bytes / 1024 bits)  
 Nonce payload  
 Next payload: NONE (0)  
 Payload length: 20  
 Nonce Data

No.	Time	Source	Destination	Protocol Info
9206	768.401192	10.20.131.62	10.20.129.80	ISAKMP Identity Protection (Main Mode)

Frame 9206 (298 bytes on wire, 298 bytes captured)  
 Ethernet II, Src: Cisco\_80:70:f5 (00:13:c4:80:70:f5),  
 Dst: Vmware\_9d:2c:dd (00:50:56:9d:2c:dd)  
 Internet Protocol, Src: 10.20.131.62 (10.20.131.62),  
 Dst: 10.20.129.80 (10.20.129.80)  
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)  
 Internet Security Association and Key Management Protocol  
 Initiator cookie: 92585D2D797E9C52  
 Responder cookie: 34704CFC8C8DBD09  
 Next payload: Key Exchange (4)  
 Version: 1.0  
 Exchange type: Identity Protection (Main Mode) (2)  
 Flags: 0x00  
 Message ID: 0x00000000  
 Length: 256  
 Key Exchange payload  
 Next payload: Nonce (10)  
 Payload length: 132  
 Key Exchange Data (128 bytes / 1024 bits)

```

Nonce payload
 Next payload: Vendor ID (13)
 Payload length: 24
 Nonce Data
Vendor ID: CISCO-UNITY-1.0
 Next payload: Vendor ID (13)
 Payload length: 20
 Vendor ID: CISCO-UNITY-1.0
Vendor ID: draft-beaulieu-ike-xauth-02.txt
 Next payload: Vendor ID (13)
 Payload length: 12
 Vendor ID: draft-beaulieu-ike-xauth-02.txt
Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
 Next payload: Vendor ID (13)
 Payload length: 20
 Vendor ID: C1B7EBE18C8CBD099E89695E2CB16A4A
Vendor ID: CISCO-CONCENTRATOR
 Next payload: NONE (0)
 Payload length: 20
 Vendor ID: CISCO-CONCENTRATOR

```

No.	Time	Source	Destination	Protocol	Info
9207	768.404990	10.20.129.80	10.20.131.62	ISAKMP	Identity Protection (Main Mode)

```

Frame 9207 (110 bytes on wire, 110 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
 Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
 Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Identification (5)
 Version: 1.0
 Exchange type: Identity Protection (Main Mode) (2)
 Flags: 0x01
 Message ID: 0x00000000
 Length: 68
 Encrypted payload (40 bytes)

```

No.	Time	Source	Destination	Protocol	Info
9208	768.405921	10.20.131.62	10.20.129.80	ISAKMP	Identity Protection (Main Mode)

```

Frame 9208 (126 bytes on wire, 126 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
 Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
 Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Identification (5)

```

```

Version: 1.0
Exchange type: Identity Protection (Main Mode) (2)
Flags: 0x01
Message ID: 0x00000000
Length: 84
Encrypted payload (56 bytes)

```

No.	Time	Source	Destination	Protocol	Info
9209	768.409799	10.20.129.80	10.20.131.62	ISAKMP	Quick Mode

```

Frame 9209 (334 bytes on wire, 334 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
 Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
 Dst: 10.20.131.62 (10.20.131.62)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Hash (8)
 Version: 1.0
 Exchange type: Quick Mode (32)
 Flags: 0x01
 Message ID: 0x79a63fb1
 Length: 292
 Encrypted payload (264 bytes)

```

No.	Time	Source	Destination	Protocol	Info
9210	768.411797	10.20.131.62	10.20.129.80	ISAKMP	Quick Mode

```

Frame 9210 (334 bytes on wire, 334 bytes captured)
Ethernet II, Src: Cisco_80:70:f5 (00:13:c4:80:70:f5),
 Dst: Vmware_9d:2c:dd (00:50:56:9d:2c:dd)
Internet Protocol, Src: 10.20.131.62 (10.20.131.62),
 Dst: 10.20.129.80 (10.20.129.80)
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Hash (8)
 Version: 1.0
 Exchange type: Quick Mode (32)
 Flags: 0x01
 Message ID: 0x79a63fb1
 Length: 292
 Encrypted payload (264 bytes)

```

No.	Time	Source	Destination	Protocol	Info
9211	768.437057	10.20.129.80	10.20.131.62	ISAKMP	Quick Mode

```

Frame 9211 (94 bytes on wire, 94 bytes captured)
Ethernet II, Src: Vmware_9d:2c:dd (00:50:56:9d:2c:dd),
 Dst: Cisco_80:70:f5 (00:13:c4:80:70:f5)
Internet Protocol, Src: 10.20.129.80 (10.20.129.80),
 Dst: 10.20.131.62 (10.20.131.62)

```

```
User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
Internet Security Association and Key Management Protocol
 Initiator cookie: 92585D2D797E9C52
 Responder cookie: 34704CFC8C8DBD09
 Next payload: Hash (8)
 Version: 1.0
 Exchange type: Quick Mode (32)
 Flags: 0x01
 Message ID: 0x79a63fb1
 Length: 52
 Encrypted payload (24 bytes)
```