

NSX 安装指南

Update 9

修改日期：2020 年 2 月 21 日

VMware NSX Data Center for vSphere 6.3



vmware®

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

如果您对本文档有任何意见或建议, 请将反馈信息发送至:

docfeedback@vmware.com

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

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

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

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

版权所有 © 2010 - 2020 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

目录

NSX 安装指南 5

1 NSX for vSphere 概述 6

NSX for vSphere 组件 7

数据层面 8

控制层面 8

管理层面 9

消费平台 9

NSX Edge 10

NSX Services 12

2 安装准备工作 14

NSX 的系统要求 14

NSX for vSphere 所需的端口和协议 16

NSX 和 vSphere Distributed Switch 19

示例：使用 vSphere Distributed Switch 21

了解复制模式 27

NSX 安装工作流程和示例拓扑 29

跨 vCenter NSX 和增强型链接模式 31

3 安装 NSX Manager 虚拟设备 33

4 在 NSX Manager 中注册 vCenter Server 38

5 配置 Single Sign On 40

6 为 NSX Manager 配置 syslog 服务器 42

7 安装和分配 NSX for vSphere 许可证 43

8 部署 NSX Controller 群集 45

9 从防火墙保护中排除虚拟机 49

10 为 NSX 准备主机群集 51

11 向准备好的群集添加主机 55

- 12** 从准备 NSX 部署的群集中移除主机 56
- 13** 配置 VXLAN 传输参数 57
- 14** 分配分段 ID 池和多播地址范围 61
- 15** 添加传输区域 63
- 16** 添加逻辑交换机 67
- 17** 添加分布式逻辑路由器 73
- 18** 添加 Edge 服务网关 85
- 19** 在逻辑（分布式）路由器上配置 OSPF 95
- 20** 在 Edge 服务网关上配置 OSPF 100
- 21** 在主机群集上安装 Guest Introspection 106
- 22** 卸载 NSX 组件 108
 - 卸载 Guest Introspection 模块 108
 - 卸载 NSX Edge 服务网关或分布式逻辑路由器 109
 - 卸载逻辑交换机 109
 - 从主机群集中卸载 NSX 110
 - 安全移除 NSX 安装 111

NSX 安装指南

本手册《NSX 安装指南》介绍了如何使用 NSX Manager 用户界面和 vSphere Web Client 安装 VMware NSX[®] for vSphere[®] 系统。本文档中的信息包括分步配置说明以及建议的最佳做法。

目标读者

本手册适用于要在 VMware vCenter 环境中安装或使用 NSX 的用户。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 vSphere，包括 VMware ESXi、vCenter Server 和 vSphere Web Client。

VMware 技术出版物术语表

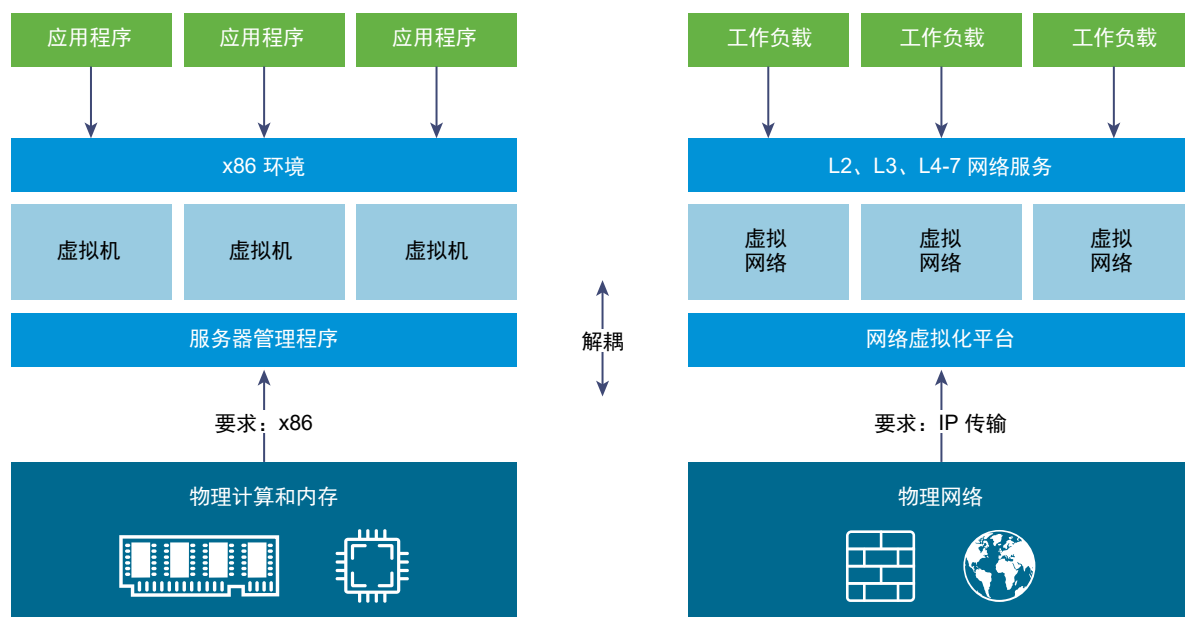
VMware 技术出版物提供了一个术语表，其中包含一些您可能不熟悉的术语。有关 VMware 技术文档中使用的术语的定义，请访问 <http://www.vmware.com/support/pubs>。

NSX for vSphere 概述

1

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。**NSX for vSphere** 是 SDDC 架构中的关键产品。使用 **NSX for vSphere** 可以实现网络虚拟化，正如计算和存储虚拟化交付。与服务器虚拟化以编程方式创建、删除和还原基于软件的虚拟机 (Virtual Machine, VM) 以及拍摄虚拟机快照的方式大致相同，**NSX for vSphere** 网络虚拟化也是以编程方式创建、删除和还原基于软件的虚拟网络以及拍摄虚拟网络快照。这使得联网方式发生了变革，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 for vSphere** 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网络架构，它为您提供了一个无中断的解决方案。事实上，使用 **NSX for vSphere**，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 和负载平衡）。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。

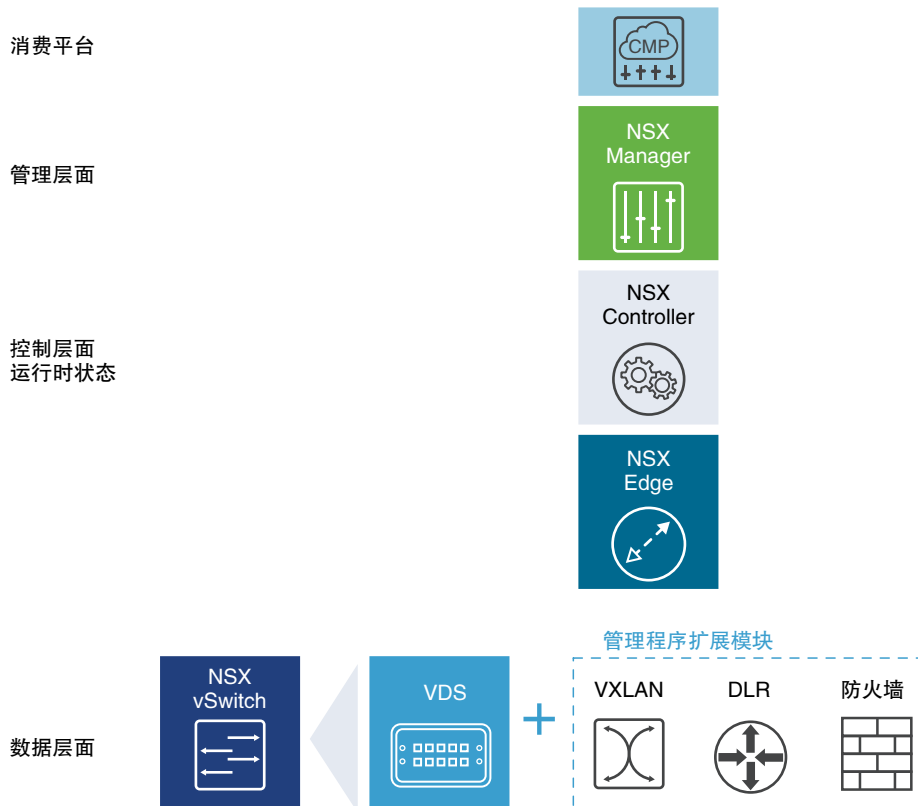
可通过 vSphere Web Client、命令行界面 (Command-Line Interface, CLI) 和 REST API 配置 NSX for vSphere。

本章讨论了以下主题：

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

NSX for vSphere 组件

本节介绍了 NSX for vSphere 解决方案的各个组件。



请注意，云管理平台 (Cloud Management Platform, CMP) 不是 NSX for vSphere 的组件，但 NSX for vSphere 可提供通过 REST API 与几乎所有 CMP 的集成，以及与 VMware CMP 的即时可用集成。

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)。

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。您可以在一个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

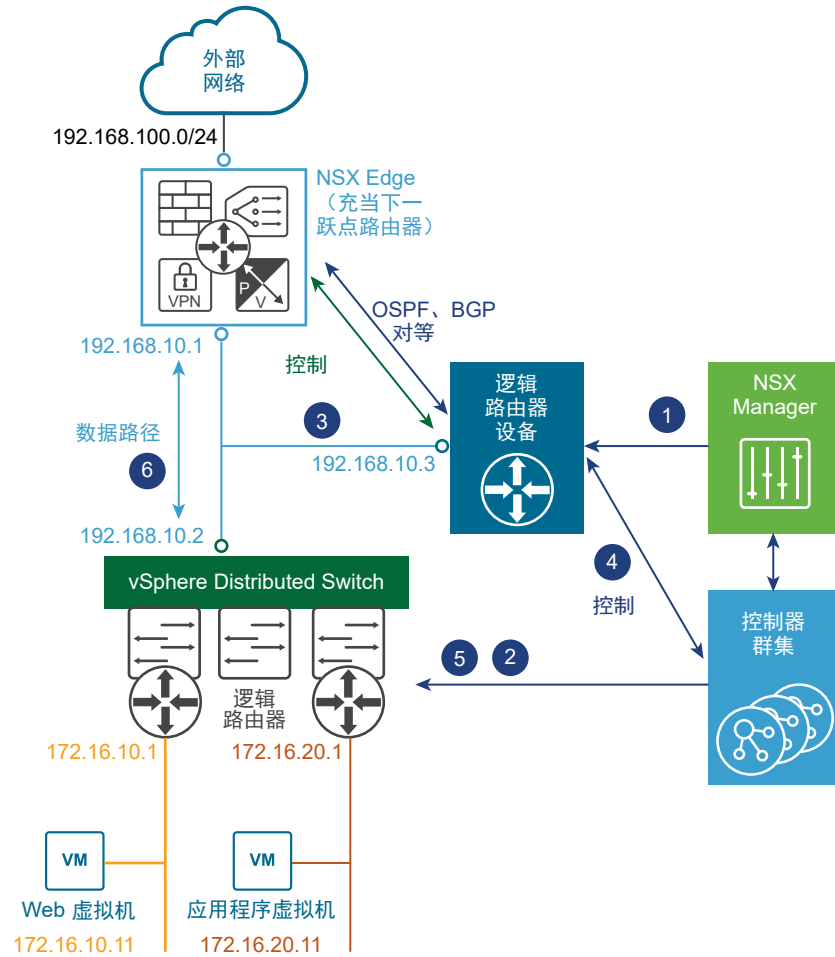
DLR 提供东西向分布式路由，可实现租户 IP 地址空间和数据路径隔离。位于不同子网中同一台主机上的虚拟机或工作负载可以彼此通信，而无需遍历传统的路由接口。

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 ESXi 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 1-1. 逻辑路由组件



- 1 DLR 实例已使用 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 使用控制层面和 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。结果是其将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”，而后者则为“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。

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。

安装准备工作

2

本节介绍 NSX for vSphere 的系统要求以及必须打开的端口。

本章讨论了以下主题：

- [NSX 的系统要求](#)
- [NSX for vSphere 所需的端口和协议](#)
- [NSX 和 vSphere Distributed Switch](#)
- [示例：使用 vSphere Distributed Switch](#)
- [了解复制模式](#)
- [NSX 安装工作流程和示例拓扑](#)
- [跨 vCenter NSX 和增强型链接模式](#)

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 实例，并在每个数据中心安装多个 NSX Edge 实例。

硬件

下表列出了 NSX 设备的硬件要求。

表 2-1. 设备的硬件要求

设备	内存	vCPU	磁盘空间
NSX Manager	16 GB（更大的 NSX 部署为 24 GB）	4（更大的 NSX 部署为 8）	60 GB
NSX Controller	4 GB	4	28 GB

表 2-1. 设备的硬件要求（续）

设备	内存	vCPU	磁盘空间
NSX Edge	精简：512 MB 中型：1 GB 大型：2 GB 超大型：8 GB	精简：1 中型：2 大型：4 超大型：6	精简、中型：1 个 584 MB 磁盘 + 1 个 512 MB 磁盘 大型：1 个 584 MB 磁盘 + 2 个 512 MB 磁盘 超大型：1 个 584 MB 磁盘 + 1 个 2 GB 磁盘 + 1 个 512 MB 磁盘
Guest Introspection	2 GB	2	5 GB（置备的空间为 6.26 GB）

作为一般准则，如果您的 NSX 受管环境包含超过 256 个管理程序或超过 2000 个虚拟机，需将 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”。

为 Guest Introspection 设备置备的空间显示 Guest introspection 为 6.26 GB。这是因为在群集中的多个主机共享存储时，vSphere ESX Agent Manager 创建服务虚拟机快照以创建快速克隆。有关如何通过 ESX Agent Manager 禁用该选项的详细信息，请参阅 *ESX Agent Manager* 文档。

网络延迟

您应确保组件之间的网络延迟等于或短于所述的最长延迟。

表 2-2. 组件之间的最长网络延迟

组件	最长延迟
NSX Manager 和 NSX Controller	150 毫秒 RTT
NSX Manager 和 ESXi 主机	150 毫秒 RTT
NSX Manager 和 vCenter Server 系统	150 毫秒 RTT
跨 vCenter NSX 环境中的 NSX Manager 和 NSX Manager	150 毫秒 RTT
NSX Controller 和 ESXi 主机	150 毫秒 RTT

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 NSX、vCenter Server 和 ESXi 的建议版本，请参见您将升级到的 NSX 版本的发行说明。发行说明可在以下 NSX for vSphere 文档站点中获取：<https://docs.vmware.com/cn/VMware-NSX-for-vSphere/index.html>。

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”。

要验证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

要管理您的 NSX 环境，需要具备以下各项：

- 正向和反向名称解析。如果您已按名称将 ESXi 主机添加到 vSphere 清单中，则需要具备此功能，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
- 必须在 Web 浏览器上启用 Cookie，才能访问 NSX Manager 用户界面。
- 必须在 NSX Manager 与要部署的 ESXi 主机、vCenter Server 和 NSX 设备之间打开端口 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 for vSphere 所需的端口和协议

以下端口必须处于打开状态才能使 NSX for vSphere 正常工作。

注 如果您具有跨 vCenter NSX 环境并且您的 vCenter Server 系统处于增强型链接模式，则每个 NSX Manager 设备必须具有与环境中每个 vCenter Server 系统的所需连接，才能从任何 vCenter Server 系统管理任何 NSX Manager。

表 2-3. NSX for vSphere 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	443	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	

表 2-3. NSX for vSphere 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
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	
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

表 2-3. NSX for vSphere 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
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	
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

NSX 和 vSphere Distributed Switch

在 NSX 域中，NSX vSwitch 是在服务器管理程序中运行以在服务器与物理网络之间形成软件抽象层的软件。

NSX vSwitch 基于 vSphere Distributed Switch (VDS)，用于提供主机连接到柜顶式 (ToR) 物理交换机的上行链路。作为最佳实践，VMware 建议您在安装 NSX for vSphere 之前规划并准备 vSphere Distributed Switch。

NSX Services 在 vSphere Standard Switch 上不受支持。虚拟机工作负载必须连接到 vSphere Distributed Switch 才能使用 NSX 服务和功能。

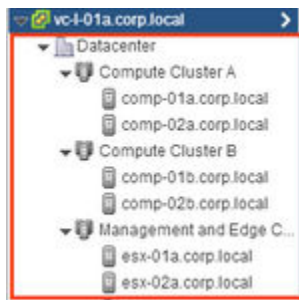
一个主机可以连接到多个 VDS。一个 VDS 可以跨多个群集中的多个主机。对于将参与 NSX 的每个主机群集，该群集中的所有主机都必须连接到一个通用 VDS。

例如，假如您有一个包含 Host1 和 Host2 的群集。Host1 连接到 VDS1 和 VDS2。Host2 连接到 VDS1 和 VDS3。为 NSX 准备群集时，您只能将 NSX 与群集中的 VDS1 相关联。如果向该群集添加另一个主机 (Host3) 且 Host3 未连接到 VDS1，则配置无效，而且 Host3 将无法用于 NSX 功能。

通常，为了简化部署，主机的每个群集仅与一个 VDS 相关联，即使一些 VDS 跨多个群集亦如此。例如，假设您的 vCenter 包含以下主机群集：

- 应用程序层主机的计算群集 A
- Web 层主机的计算群集 B
- 管理和 Edge 主机的管理和 Edge 群集

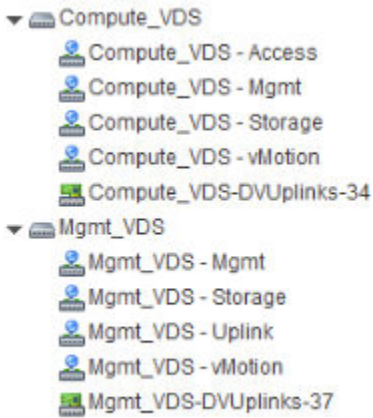
下面的屏幕截图显示这些群集在 vCenter 中的显示方式。



对于此类群集设计，您可能具有两个分别名为 Compute_VDS 和 Mgmt_VDS 的 VDS。Compute_VDS 跨两个计算群集，而 Mgmt_VDS 仅与管理 Edge 群集关联。

每个 VDS 都包含需要承载的不同流量类型的分布式端口组。典型流量类型包括管理、存储和 vMotion。上行链路和访问端口通常也为必需项。正常情况下，每个 VDS 上会针对每种流量创建一个端口组。

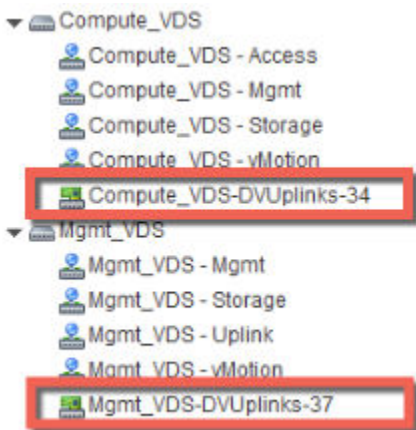
例如，下面的屏幕截图显示这些 Distributed Switch 和端口在 vCenter 中的显示方式。



或者，每个端口组也可以用一个 **VLAN ID** 进行配置。以下列表显示 **VLAN** 如何与分布式端口组关联以在不同流量类型之间提供逻辑隔离的示例：

- Compute_VDS - Access---VLAN 130
- Compute_VDS - Mgmt---VLAN 210
- Compute_VDS - Storage---VLAN 520
- Compute_VDS - vMotion---VLAN 530
- Mgmt_VDS - Uplink---VLAN 100
- Mgmt_VDS - Mgmt---VLAN 110
- Mgmt_VDS - Storage---VLAN 420
- Mgmt_VDS - vMotion---VLAN 430

DVUplinks 端口组是在创建 VDS 时自动创建的 **VLAN** 中继。作为一个中继端口，它发送和接收标记的帧。默认情况下，它将携带所有 **VLAN ID (0-4094)**。这意味着带有任何 **VLAN ID** 的流量均可通过与 DVUplink 插槽关联的 vmnic 网络适配器，并由管理程序主机进行筛选，因为 **Distributed Switch** 确定了应接收流量的端口组。



如果现有 vCenter 环境不包含 **Distributed Switch**，而是包含标准 **vSwitch**，则您可以将主机迁移至 **Distributed Switch**。

示例：使用 vSphere Distributed Switch

本例展示了如何创建新的 vSphere Distributed Switch (VDS)；如何针对管理、存储和 vMotion 流量类型添加端口组；如何将标准 vSwitch 上的主机迁移至新的 Distributed Switch。

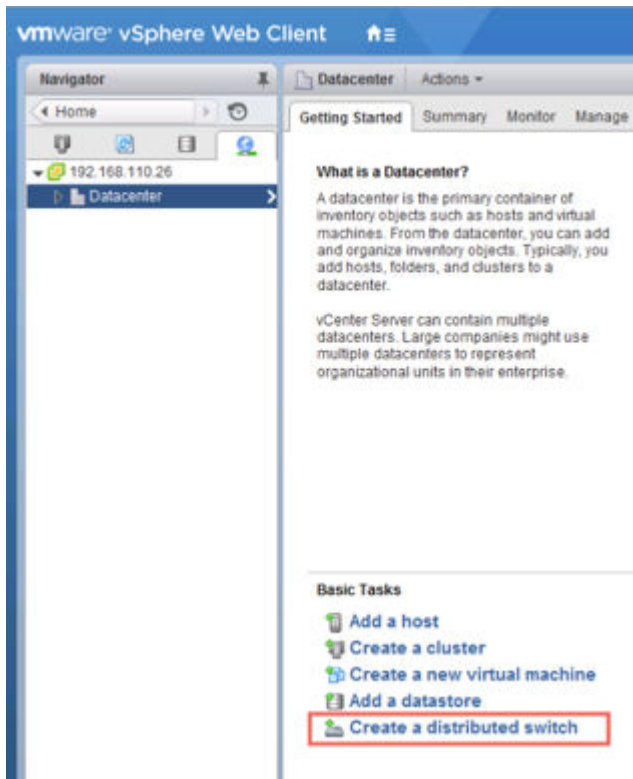
请注意，本例的目的仅为展示操作过程。有关详细的 VDS 物理和逻辑上行链路注意事项，请参见《VMware NSX for vSphere 网络虚拟化设计指南》（网址为：<https://communities.vmware.com/docs/DOC-27683>）。

前提条件

本例假设要连接到 vSphere Distributed Switch 的每个 ESX 主机至少具有一个到物理交换机的连接（一个 vmnic 上行链路）。此上行链路可用于 Distributed Switch 和 NSX VXLAN 流量。

步骤

- 1 在 vSphere Web Client 中，导航到数据中心。
- 2 单击**创建 Distributed Switch (Create a Distributed Switch)**。



- 3 根据将与交换机关联的主机群集为此交换机指定体现其意义的名称。

例如，如果一个 Distributed Switch 将与一组数据中心管理主机相关联，您可以将该交换机命名为 VDS_Mgmt。

- 4 请至少提供一个该 **Distributed Switch** 的上行链路，保持启用 **IO 控制**，并为默认端口组提供体现其意义的名称。请注意，您不一定需要创建默认端口组，可在以后手动创建该端口组。

默认情况下，系统会创建四个上行链路。调整上行链路数量以体现您的 **VDS** 设计。所需的上行链路数通常等于分配给 **VDS** 的物理网卡数。

下面的屏幕截图显示管理主机群集上管理流量的示例设置。

默认端口组正是此交换机将包含的端口组之一。创建交换机后，您将可以添加不同流量类型的端口组。或者，在创建新 **VDS** 时，您也可以取消勾选 **创建默认端口组 (Create a default port group)** 选项。这种做法实际上可能是最佳实践：最好在创建端口组时明确。

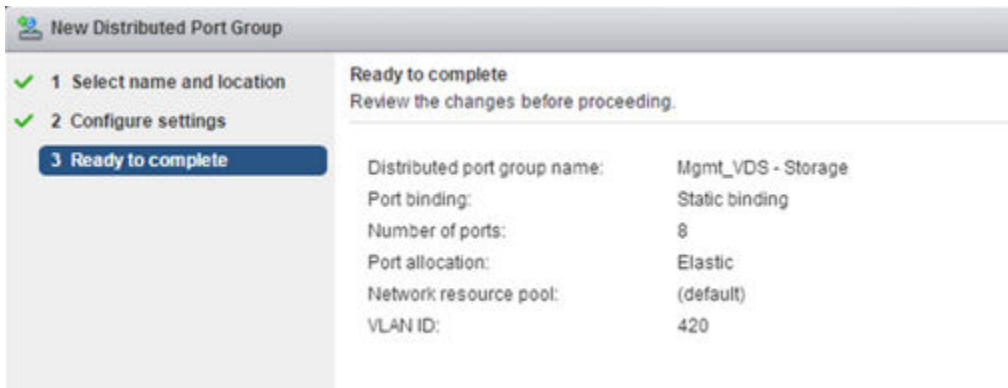
- 5 （可选）完成“新建 **Distributed Switch**”向导之后，编辑默认端口组的设置，以将其置于正确的管理流量 **VLAN** 中。

例如，如果您的主机管理接口在 **VLAN 110** 中，则将默认端口组置于 **VLAN 110** 中。如果您的主机管理接口未在 **VLAN** 中，请跳过此步骤。

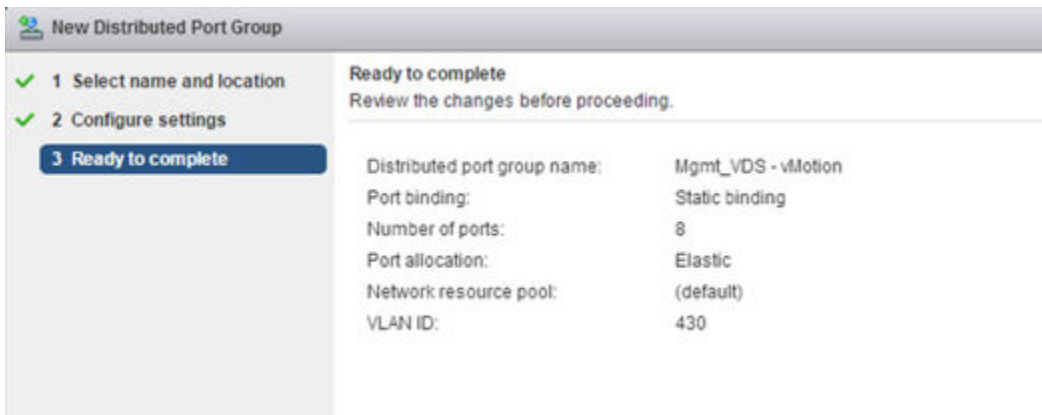
- 6 完成“新建 **Distributed Switch**”向导之后，右键单击该 **Distributed Switch**，然后选择**新建 Distributed Switch 端口组 (New Distributed Port Group)**。

为每种流量重复此步骤，确保提供体现每个端口组意义的名称，并确保根据您的部署的流量隔离要求配置正确的 **VLAN ID**。

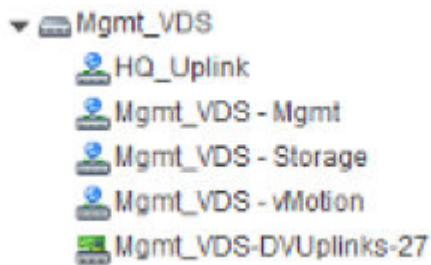
存储的示例组设置。



vMotion 流量的示例组设置。

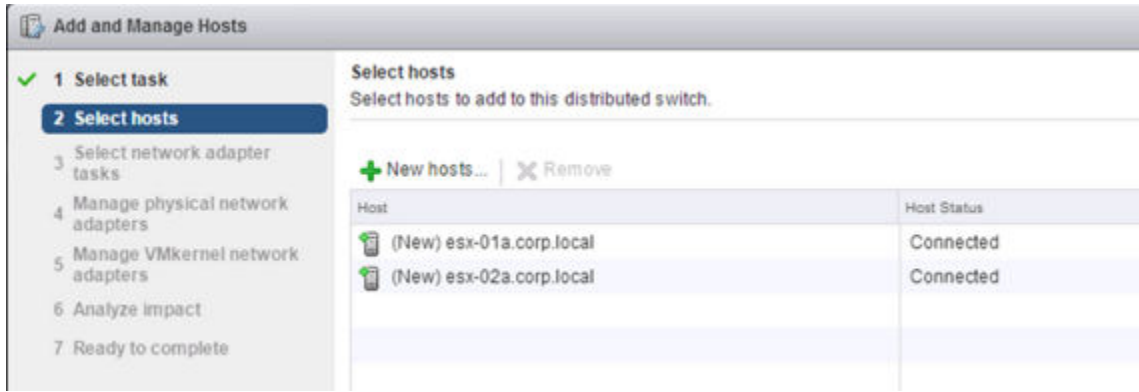


完成的 Distributed Switch 和端口组如下所示。

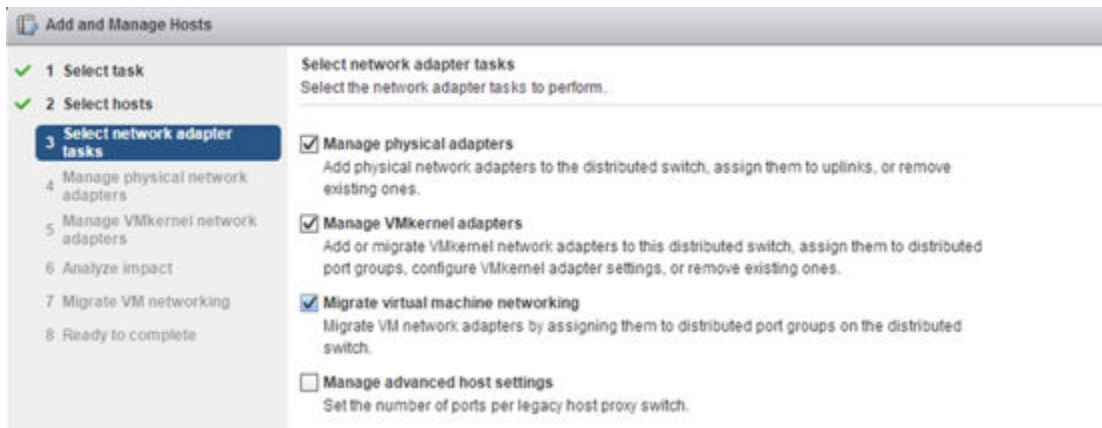


- 7 右键单击 Distributed Switch，选择**添加和管理主机 (Add and Manage Hosts)**，然后选择**添加主机 (Add Hosts)**。

连接位于关联群集中的所有主机。例如，如果该交换机用于管理主机，则选择位于管理群集中的所有主机。

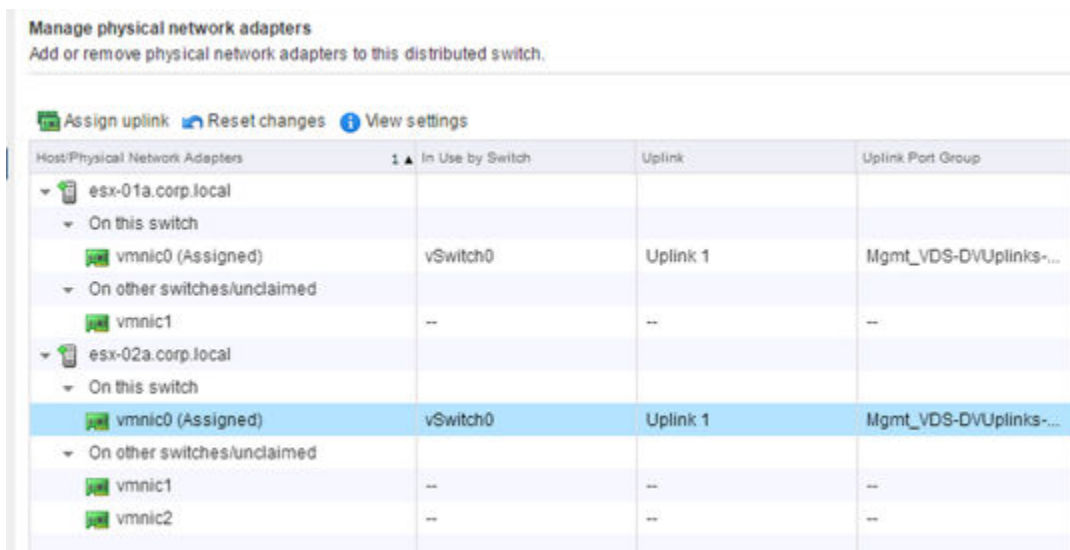


- 8 选择各选项以迁移物理适配器、VMkernel 适配器和虚拟机网络连接。



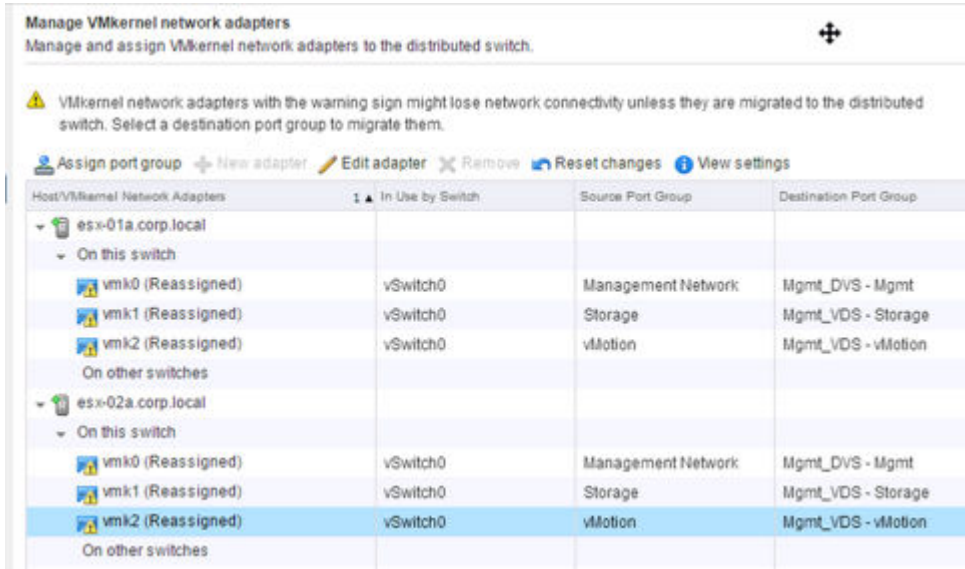
- 9 选择一个 vmnic 并单击分配上行链路 (Assign uplink)，将 vmnic 从标准 vSwitch 迁移至 Distributed Switch。为连接到分布式 vSwitch 的每个主机重复此步骤。

例如，下面的屏幕截图显示两个配置了 vmnic0 上行链路的主机从各自的标准 vSwitch 迁移至分布式 Mgmt_VDS-DVUplink 端口组，该端口组是可带有任何 VLAN ID 的中继端口。



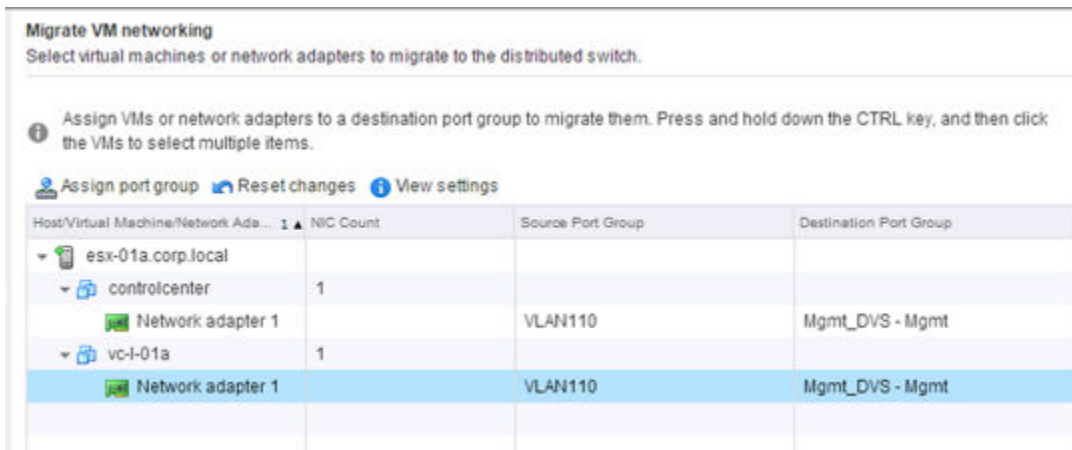
- 10 选择一个 VMKernel 网络适配器，然后单击**分配端口组 (Assign port group)**。为连接到分布式 vSwitch 的所有主机上的所有网络适配器重复此步骤。

例如，下面的屏幕截图显示两个主机上的三个 vmk 网络适配器配置为从标准端口组迁移至新的分布式端口组。



- 11 将主机上的任何虚拟机全部移至分布式端口组。

例如，下面的屏幕截图显示一个主机上的两个虚拟机配置为从标准端口组迁移至新的分布式端口组。



结果

此操作过程完成后，您可以在主机 CLI 中通过运行以下命令来验证结果：

- ```
~ # esxcli network vswitch dvs vmware list
Mgmt_VDS
 Name: Mgmt_VDS
 VDS ID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
 Class: etherswitch
 Num Ports: 1862
 Used Ports: 5
```

```

Configured Ports: 512
MTU: 1600
CDP Status: listen
Beacon Timeout: -1
Uplinks: vmnic0
VMware Branded: true
DVPort:
 Client: vmnic0
 DVPortgroup ID: dvportgroup-306
 In Use: true
 Port ID: 24

 Client: vmk0
 DVPortgroup ID: dvportgroup-307
 In Use: true
 Port ID: 0

 Client: vmk2
 DVPortgroup ID: dvportgroup-309
 In Use: true
 Port ID: 17

 Client: vmk1
 DVPortgroup ID: dvportgroup-308
 In Use: true
 Port ID: 9

```

```

■ ~ # esxcli network ip interface list
vmk2
 Name: vmk2
 MAC Address: 00:50:56:6f:2f:26
 Enabled: true
 Portset: DvsPortset-0
 Portgroup: N/A
 Netstack Instance: defaultTcpipStack
 VDS Name: Mgmt_VDS
 VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
 VDS Port: 16
 VDS Connection: 1235399406
 MTU: 1500
 TSO MSS: 65535
 Port ID: 50331650

vmk0
 Name: vmk0
 MAC Address: 54:9f:35:0b:dd:1a
 Enabled: true
 Portset: DvsPortset-0
 Portgroup: N/A
 Netstack Instance: defaultTcpipStack
 VDS Name: Mgmt_VDS
 VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
 VDS Port: 2
 VDS Connection: 1235725173
 MTU: 1500

```

```

TSO MSS: 65535
Port ID: 50331651

vmk1
Name: vmk1
MAC Address: 00:50:56:6e:a4:53
Enabled: true
Portset: DvsPortset-0
Portgroup: N/A
Netstack Instance: defaultTcpipStack
VDS Name: Mgmt_VDS
VDS UUID: 89 78 26 50 98 bb f5 1e-a5 07 b5 29 ff 86 e2 ac
VDS Port: 8
VDS Connection: 1236595869
MTU: 1500
TSO MSS: 65535
Port ID: 50331652

```

### 后续步骤

为所有 vSphere Distributed Switch 重复迁移流程。

## 了解复制模式

创建传输区域或逻辑交换机时，必须选择一种复制模式。了解不同的模式可以帮助您确定哪种模式最适合您的环境。

为 NSX 准备的每个 ESXi 主机都配置了 VXLAN 隧道端点 (VTEP)。每个 VXLAN 隧道端点具有一个 IP 地址。这些 IP 地址可以位于同一子网中，也可以位于不同子网中。

在不同 ESXi 主机上的两个虚拟机直接通信时，将在两个 VTEP IP 地址之间传输单播封装流量，而无需进行泛洪。不过，与任何第 2 层网络一样，有时来自某个虚拟机的流量必须进行泛洪操作，或者发送到属于同一逻辑交换机的所有其他虚拟机。第 2 层广播、未知单播和多播流量统称为 BUM 流量。必须将来自特定主机上的某个虚拟机的 BUM 流量复制到将虚拟机连接到同一个逻辑交换机的所有其他主机。NSX for vSphere 支持三种不同的复制模式：

- 单播复制模式
- 多播复制模式
- 混合复制模式

## 复制模式摘要

表 2-4. 复制模式摘要

| 复制模式 | 将 BUM 复制到同一子网上 VTEP 的方法 | 将 BUM 复制到不同子网上 VTEP 的方法 | 物理网络要求                                                                                                                                    |
|------|-------------------------|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 单播   | 单播                      | 单播                      | <ul style="list-style-type: none"> <li>■ VTEP 子网之间的路由</li> </ul>                                                                          |
| 多播   | 第 2 层多播                 | 第 3 层多播                 | <ul style="list-style-type: none"> <li>■ VTEP 子网之间的路由</li> <li>■ 第 2 层多播, IGMP</li> <li>■ 第 3 层多播, PIM</li> <li>■ 将多播组分配给逻辑交换机</li> </ul> |
| 混合   | 第 2 层多播                 | 单播                      | <ul style="list-style-type: none"> <li>■ VTEP 子网之间的路由</li> <li>■ 第 2 层多播, IGMP</li> </ul>                                                 |

### 单播复制模式

单播复制模式无需物理网络支持第 2 层或第 3 层多播来处理逻辑交换机内的 BUM 流量。使用单播模式可以将逻辑交换机从物理网络中完全分离出来。单播模式会将所有 BUM 流量复制到源主机本地，并通过单播数据包将这些 BUM 流量转发给远程主机。在单播模式下，可以将所有 VTEP 放在一个子网中，也可以放在多个子网中。

一个子网的情况：当所有主机 VTEP 接口都属于一个子网时，源 VTEP 会将 BUM 流量转发给所有远程 VTEP。这种复制称为头端复制。头端复制可能会导致不必要的主机开销和更高的带宽使用。具体影响取决于 BUM 流量多少以及子网内的主机和 VTEP 数量。

多个子网的情况：如果主机 VTEP 接口分布到多个 IP 子网，源主机将分两部分处理 BUM 流量。源 VTEP 将 BUM 流量转发到同一子网中的每个 VTEP（与一个子网的情况相同）。对于远程子网中的 VTEP，源 VTEP 会将 BUM 流量转发给每个远程 VTEP 子网中的一个主机，并设置复制位以将此数据包标记为本地复制。远程子网中的主机在收到此数据包并找到所设置的复制位后，会将数据包发送到其子网中逻辑交换机所在的所有其他 VTEP。

因此，在具有许多 VTEP IP 子网的网络架构中，单播复制模式具有良好的可扩展性，因为负载在多个主机之间进行分发。

### 多播复制模式

多播复制模式需要在物理基础架构中同时启用第 3 层和第 2 层多播。要配置多播模式下，网络管理员需要将每个逻辑交换机与 IP 多播组关联起来。对于在特定逻辑交换机上托管虚拟机的 ESXi 主机，其相关联的 VTEP 会使用 IGMP 加入多播组 G。路由器会跟踪 IGMP 联接情况并使用多播路由协议在 IGMP 联接之间创建多播分发树。

当主机将 BUM 流量复制到位于同一 IP 子网的 VTEP 时，它们使用第 2 层多播。当主机将 BUM 流量复制到位于不同 IP 子网的 VTEP 时，它们使用第 3 层多播。在这两种情况下，由物理基础架构来处理到远程 VTEP 的 BUM 流量复制。

尽管 IP 多播是一项众所周知的技术，但由于各种技术、运营或管理原因，在数据中心中部署 IP 多播通常被视为一大难题。网络管理员必须密切关注物理基础架构支持的最大多播状态，以便在逻辑交换机与多播组之间启用一对一映射。虚拟化的一个好处是，允许在不将其他状态公开到物理基础架构的情况下扩展虚拟基础架构。将逻辑交换机映射到“物理”多播组会破坏此模型。

**注** 在多播复制模式下，NSX Controller 群集不用于逻辑交换。

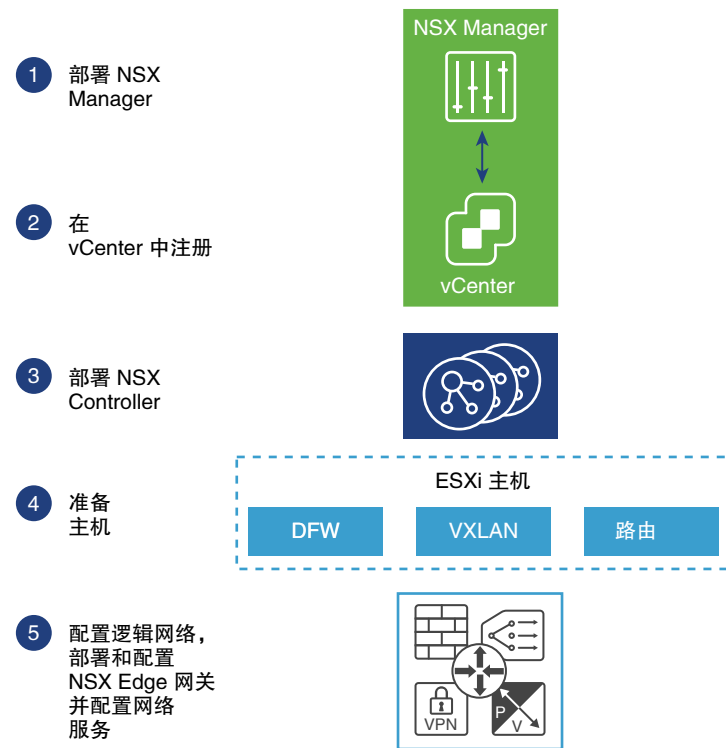
## 混合复制模式

混合模式是单播和多播复制模式的组合。在混合复制模式中，主机 VTEP 使用第 2 层多播将 BUM 流量分发到位于同一子网的对等 VTEP。当主机 VTEP 将 BUM 流量复制到位于不同子网中的 VTEP 时，它们会以单播数据包形式将这些流量转发给每个 VTEP 子网中的一个主机。然后，接收流量的主机使用第 2 层多播将数据包发送给子网中的其他 VTEP。

在客户网络中，第 2 层多播比第 3 层多播更常用，因为第 2 层多播通常可以轻松部署。将 BUM 流量复制到位于同一子网中的不同 VTEP 通常在物理网络中进行。如果同一子网中有多个对等 VTEP，则混合复制可以有效缓解源主机的 BUM 流量。使用混合复制，您可以扩展至分段很少或不含分段的高密度环境。

## NSX 安装工作流程和示例拓扑

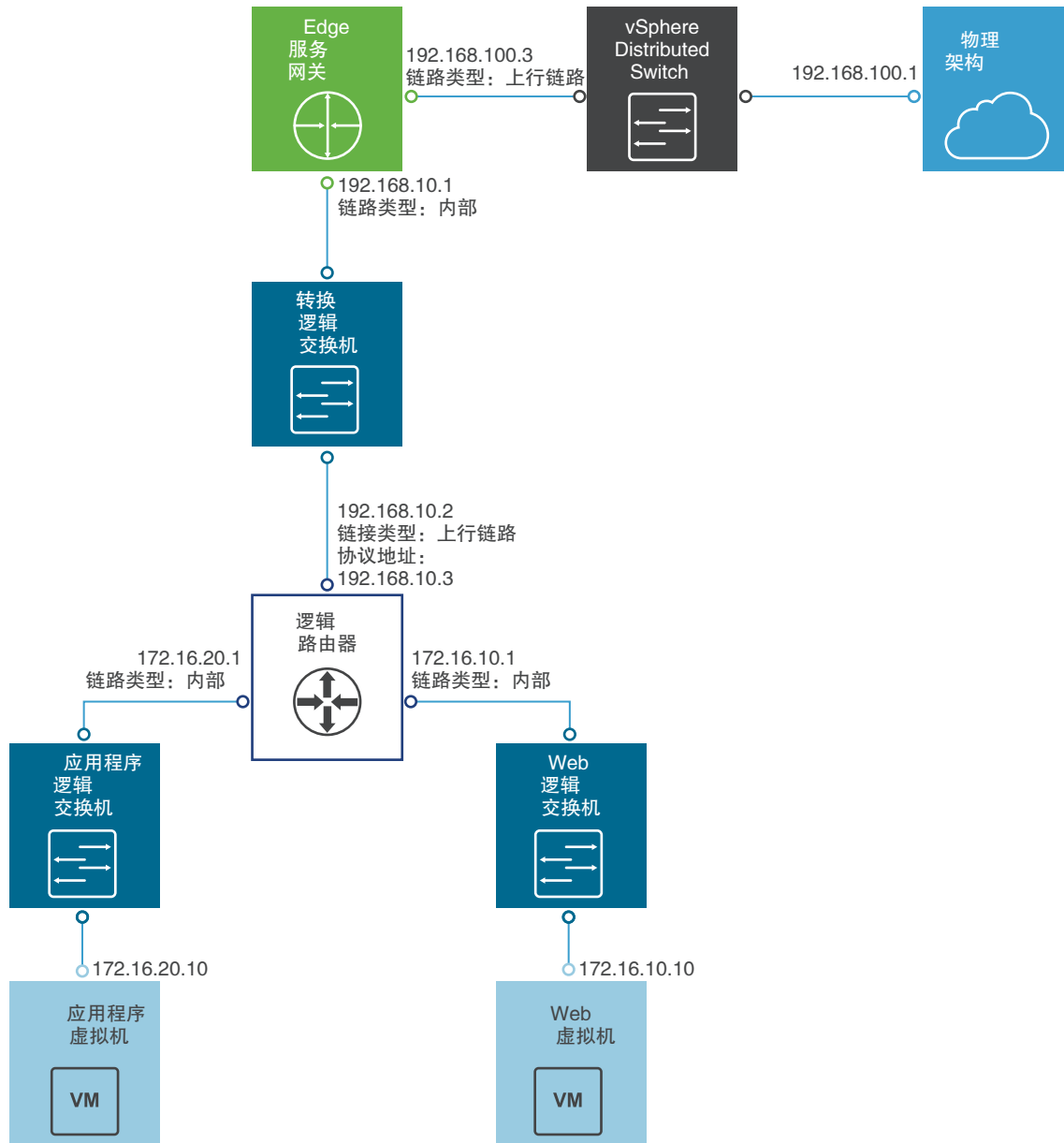
NSX 安装流程包括部署多个虚拟设备，完成一些 ESX 主机准备，并进行一些配置以便所有物理和虚拟设备能够相互通信。



此流程首先应部署 **NSX Manager OVF/OVA** 模板，确保 **NSX Manager** 完全连接到它将管理的 **ESX** 主机的管理接口。接下来，需要通过注册流程将 **NSX Manager** 与一个 **vCenter** 实例彼此链接。然后，就可以部署 **NSX Controller** 群集了。与 **NSX Manager** 一样，**NSX Controller** 在 **ESX** 主机上作为虚拟设备运行。下一步是为 **NSX** 准备 **ESX** 主机，您需要在主机上安装多个 **VIB**。这些 **VIB** 支持第 2 层 **VXLAN** 功能、分布式路由和分布式防火墙。配置 **VXLAN**、指定虚拟网络接口 (**VNI**) 范围并创建传输区域之后，您就可以开始构建自己的 **NSX** 覆盖拓扑。

本安装向导详细介绍该流程中的每一步。

本向导不仅适用于所有 **NSX** 部署，而且还可指导您创建一个示例 **NSX** 覆盖拓扑，您可以利用该示例拓扑进行练习、做为指导或参考。示例覆盖有一个 **NSX** 逻辑分布式路由器（有时被称为 **DLR**）、一个 **Edge** 服务网关 (**ESG**) 和一个连接两个 **NSX** 路由设备的 **NSX** 逻辑转换交换机。示例拓扑还包括底层元素，其中包括两个示例虚拟机。这两个虚拟机均分别连接到一个独立的 **NSX** 逻辑交换机，允许通过 **NSX** 逻辑路由器 (**DLR**) 进行连接。



## 跨 vCenter NSX 和增强型链接模式

vSphere 6.0 引入了增强型链接模式，它使用一个或多个 Platform Services Controller 链接多个 vCenter Server 系统。这使您可以查看和搜索 vSphere Web Client 内所有已链接的 vCenter Server 系统的清单。在跨 vCenter NSX 环境中，增强型链接模式允许您从一个 vSphere Web Client 管理所有 NSX Manager。在存在多个 vCenter Server 的中型部署中，您可以对 vCenter 组合使用跨 vCenter NSX 和增强型链接模式。这两项功能是互补的，但彼此又相互独立。

## 组合使用跨 vCenter NSX 和增强型链接模式

在跨 vCenter NSX 中，您有一个主 NSX Manager 和多个辅助 NSX Manager。它们中的每个 NSX Manager 都链接到独立的 vCenter Server。在主 NSX Manager 上，您可以创建能够辅助 NSX Manager 查看的通用 NSX 组件（例如交换机和路由器）。

当使用增强型链接模式部署每个 vCenter Server 时，可从一个 vCenter Server（有时称为一个窗口）查看和管理所有 vCenter Server。

因此，当对 vCenter 组合使用跨 vCenter NSX 与增强型链接模式时，您可以从任何链接的 vCenter Server 查看和管理任意 NSX Manager 以及所有通用 NSX 组件。

## 在不启用增强型链接模式的情况下使用跨 vCenter NSX

对于跨 vCenter NSX，增强型链接模式并不是必要条件或要求。如果不启用增强型链接模式，您仍可以创建跨 vCenter 的通用传输区域、通用交换机、通用路由器和通用防火墙规则。但是，在不启用增强型链接模式的情况下，您必须登录到各个 vCenter Server，才能访问每个 NSX Manager 实例。

## 有关 vSphere 和增强型链接模式的详细信息

如果您决定使用增强型链接模式，请参见《vSphere 安装和设置指南》或《vSphere 升级指南》以了解 vSphere 和增强型链接模式的最新要求。



# 安装 NSX Manager 虚拟设备

## 3

NSX Manager 可作为虚拟设备安装在 vCenter 环境中的任意 ESX 主机上。

NSX Manager 提供了图形用户界面 (GUI) 和 REST API 以创建、配置和监控 NSX 组件，如控制器、逻辑交换机和 Edge 服务网关。NSX Manager 提供了一个聚合系统视图，它是 NSX 的集中式网络管理组件。NSX Manager 虚拟机打包为 OVA 文件，允许您使用 vSphere Web Client 将 NSX Manager 导入数据存储和虚拟机清单。

为了实现高可用性，VMware 建议在配置了 HA 和 DRS 的群集中部署 NSX Manager。或者，您也可以在其他不与 NSX Manager 进行互操作的 vCenter 中安装 NSX Manager。一个 NSX Manager 服务于一个 vCenter Server 环境。

在跨 vCenter NSX 安装中，确保每个 NSX Manager 都有一个唯一的 UUID。从 OVA 文件部署的 NSX Manager 实例均有唯一的 UUID。从模板部署的 NSX Manager（如同将虚拟机转换为模板）将与用于创建模板的原始 NSX Manager 具有相同的 UUID，并且这两个 NSX Manager 不能在同一个跨 vCenter NSX 安装中使用。换言之，对于每个 NSX Manager，您应按照本过程所述重新安装一个新设备。

NSX Manager 虚拟机安装将包含 VMware Tools。请勿尝试在 NSX Manager 上升级或安装 VMware Tools。

在安装期间，您可以选择加入 NSX 客户体验改进计划 (CEIP)。有关该计划的详细信息（包括如何加入或退出该计划），请参见 NSX 管理指南中的“客户体验改进计划”。

### 前提条件

- 安装 NSX Manager 前，确保所需端口处于打开状态。请参见 [NSX for vSphere 所需的端口和协议](#)。
- 确保数据存储已配置且可在目标 ESX 主机上访问。建议使用共享存储。HA 需要使用共享存储，以便可以在原始主机出现故障的情况下在其他主机上重新启动 NSX Manager 设备。
- 确保知道 NSX Manager 将使用的 IP 地址和网关、DNS 服务器 IP 地址、域搜索列表和 NTP 服务器 IP 地址。
- 确定 NSX Manager 是只进行 IPv4 寻址或只进行 IPv6 寻址，还是具有双堆栈网络配置。NSX Manager 的主机名将由其他实体使用。因此，NSX Manager 主机名必须映射到该网络中使用的 DNS 服务器中的正确 IP 地址。

- 准备 NSX Manager 将在其上通信的管理流量分布式端口组。请参阅[示例：使用 vSphere Distributed Switch](#)。NSX Manager 管理接口、vCenter Server 和 ESXi 主机管理接口必须可由 NSX Guest Introspection 实例访问。
- 必须安装客户端集成插件。“部署 OVF 模板”向导在 Firefox Web 浏览器中性能最佳。在 Chrome Web 浏览器中运行时，有时会显示一条有关安装客户端集成插件的错误消息，即使已成功安装该插件也会显示此消息。安装客户端集成插件：
  - a 打开 Web 浏览器，然后键入 vSphere Web Client 的 URL。
  - b 在 vSphere Web Client 登录页面底部，单击“下载客户端集成插件”。

如果客户端集成插件已安装在系统上，则您不会看到该插件的下载链接。如果卸载客户端集成插件，则该插件的下载链接将显示在 vSphere Web Client 登录页面上。

## 步骤

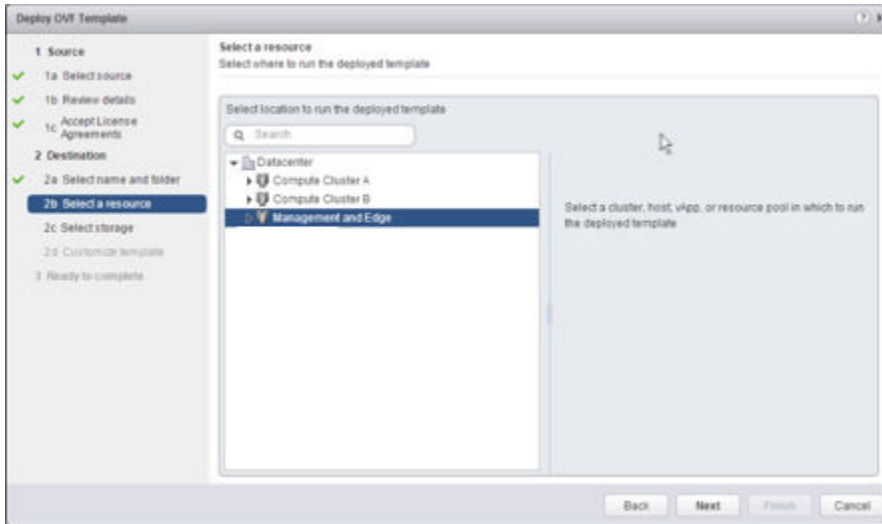
- 1 找到 NSX Manager 开放虚拟化设备 (OVA) 文件。  
将下载 URL 复制到计算机或下载 OVA 文件到计算机。
- 2 在 Firefox 中，打开 vCenter。
- 3 选择**虚拟机和模板 (VMs and Templates)**，右键单击您的数据中心，然后选择**部署 OVF 模板 (Deploy OVF Template)**。
- 4 粘贴下载 URL，或单击**浏览 (Browse)**选择计算机上的文件。

---

**注** 如果安装失败并显示操作超时错误，请检查存储和网络设备是否出现任何连接问题。在物理基础架构出现问题（例如，到存储设备的连接中断或物理网卡或交换机出现连接问题）时，将会出现该问题。

---

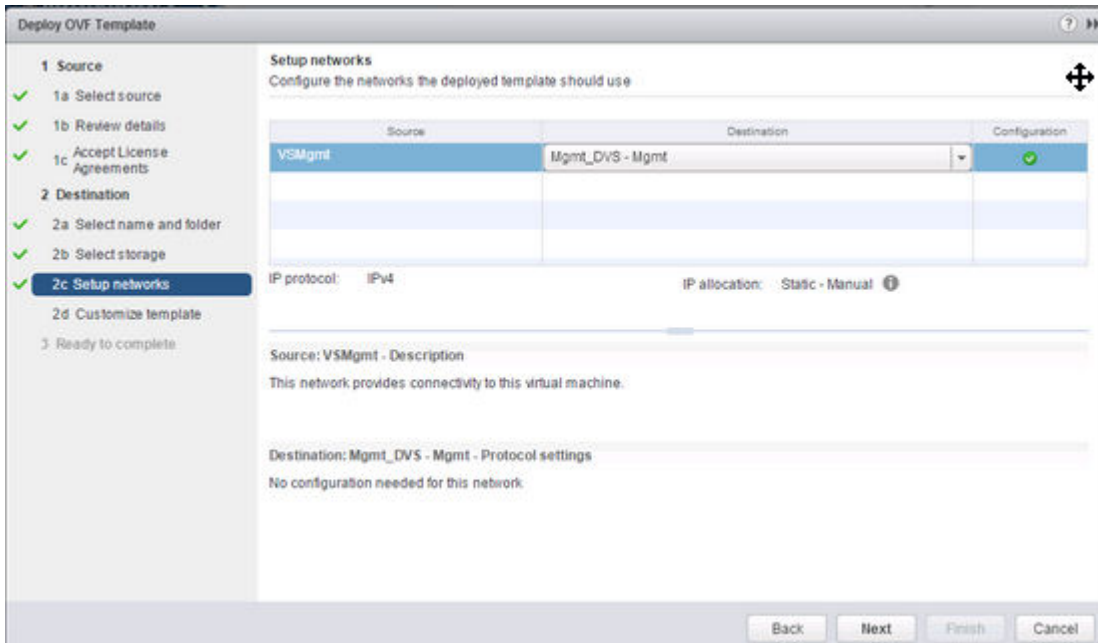
- 5 勾选复选框**接受其他配置选项 (Accept extra configuration options)**。  
这允许您在安装过程中设置 IPv4 和 IPv6 地址、默认网关、DNS、NTP 和 SSH 属性，而不是在安装后手动配置这些设置。
- 6 接受 VMware 许可协议。
- 7 编辑 NSX Manager 名称（如果需要）。选择已部署的 NSX Manager 所在的位置。  
您键入的名称将显示在 vCenter 清单中。  
所选文件夹将用于向 NSX Manager 应用权限。
- 8 选择要在其上部署 NSX Manager 设备的主机或群集。  
例如：



9 将虚拟磁盘格式更改为**厚置备 (Thick Provision)**，并为虚拟机配置文件和虚拟磁盘选择目标数据存储。

10 选择 NSX Manager 的端口组。

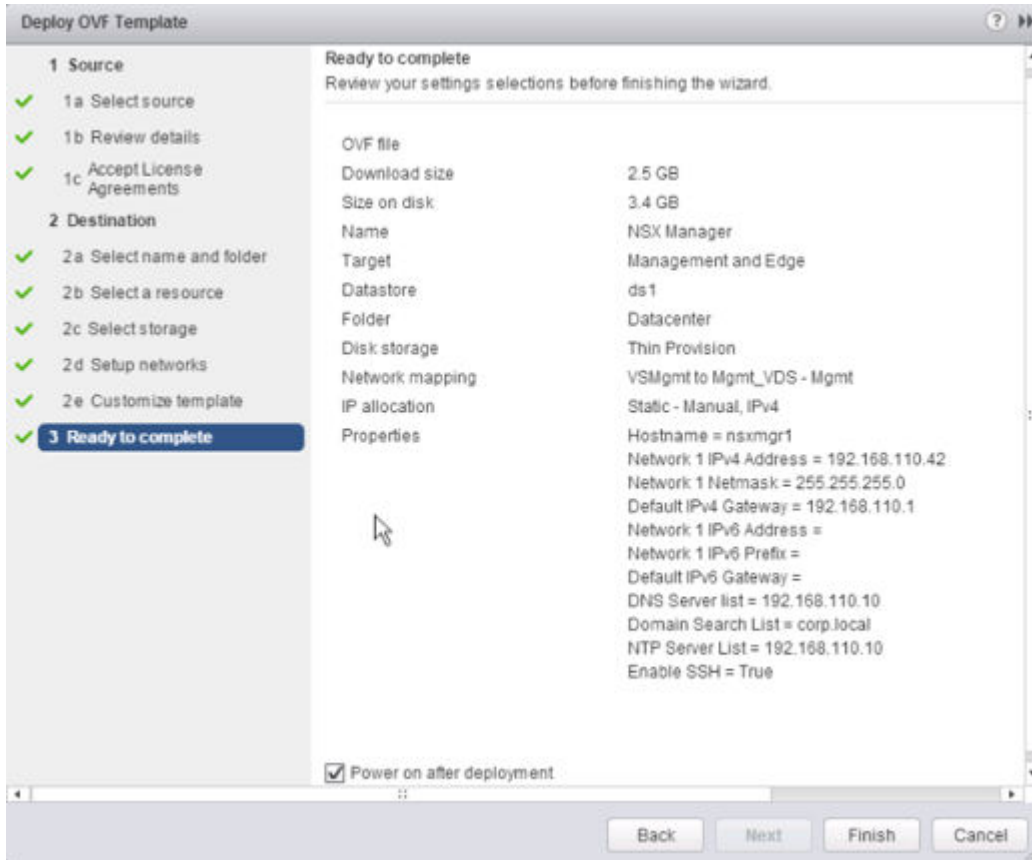
例如，下面的屏幕截图显示 **Mgmt\_DVS - Mgmt** 端口组选择。



11 （可选）选中**加入客户体验改进计划 (Join the Customer Experience Improvement Program)**复选框。

12 设置 NSX Manager 其他配置选项。

例如，下面的屏幕截图显示在仅使用 IPv4 的部署中配置完所有选项之后的最终查看屏幕。



## 结果

打开 NSX Manager 的控制台以跟踪引导流程。

完成 NSX Manager 的引导后，登录 CLI 并运行 `show interface` 命令，以验证 IP 地址已按预期应用。

```
nsxmgr1> show interface
Interface mgmt is up, line protocol is up
index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
HWaddr: 00:50:56:8e:c7:fa
inet 192.168.110.42/24 broadcast 192.168.110.255
inet6 fe80::250:56ff:fe8e:c7fa/64
Full-duplex, 0Mb/s
input packets 1370858, bytes 389455808, dropped 50, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 1309779, bytes 2205704550, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
```

确保 NSX Manager 可以对其默认网关、其 NTP 服务器、vCenter Server 和它将管理的所有管理程序主机上的管理接口的 IP 地址执行 ping 操作。

打开 Web 浏览器并导航到 NSX Manager IP 地址或主机名，以连接到 NSX Manager 设备 GUI。

在使用安装期间设置的密码以 **admin** 身份登录后，请从“主页”中单击[查看摘要 \(View Summary\)](#)并确保以下服务正在运行：

- vPostgres
- RabbitMQ
- NSX 管理服务

为获得最佳性能，VMware 建议为 **NSX Manager** 虚拟设备预留内存。即使内存过量使用，内存预留也能保证主机为虚拟机预留的物理内存量下限。将预留内存设置为可确保 **NSX Manager** 内存足以高效运行的级别。

#### 后续步骤

向 **NSX Manager** 注册 vCenter Server。

# 在 NSX Manager 中注册 vCenter Server

## 4

NSX Manager 和 vCenter Server 具有一一对应关系。每个 NSX Manager 实例具有一个 vCenter Server，即使是在跨 vCenter NSX 环境中也是如此。

只能在 vCenter Server 系统中注册一个 NSX Manager。不支持更改已配置的 NSX Manager 的 vCenter 注册。

如果要更改现有 NSX Manager 的 vCenter 注册，您必须先移除所有 NSX for vSphere 配置，然后从 vCenter Server 系统中移除 NSX Manager 插件。有关说明，请参见[安全移除 NSX 安装](#)。或者，您可以部署新的 NSX Manager 设备以在新的 vCenter Server 系统中进行注册。

如果需要，您可以更改用于在 NSX Manager 中注册的 vCenter Server 用户帐户。用于注册的 vCenter Server 用户帐户必须是 vCenter Single Sign-On **管理员组**的成员。

### 前提条件

- NSX 管理服务必须正在运行。在 NSX Manager Web 界面 (<https://<nsx-manager-ip>>) 中，单击**主页 (Home) > 查看摘要 (View Summary)**以查看服务状态。
- 您必须使用作为 vCenter Single Sign-On **管理员组**成员的 vCenter Server 用户帐户将 NSX Manager 与 vCenter Server 系统进行同步。如果帐户密码包含非 ASCII 字符，您必须先更改该密码，然后再将 NSX Manager 与 vCenter Server 系统进行同步。不要使用 root 帐户。

请参见《Platform Services Controller 管理》文档中的“管理 vCenter Single Sign-On 用户和组”，了解有关如何添加用户的信息。

- 确认正向和反向名称解析工作正常并且以下系统可解析彼此的 DNS 名称：
  - NSX Manager 设备
  - vCenter Server 系统
  - Platform Services Controller 系统
  - ESXi 主机

### 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（网址为 <https://<nsx-manager-ip>> 或 <https://<nsx-manager-hostname>>），然后以**管理员**身份或使用具有**企业管理员**角色的帐户登录。

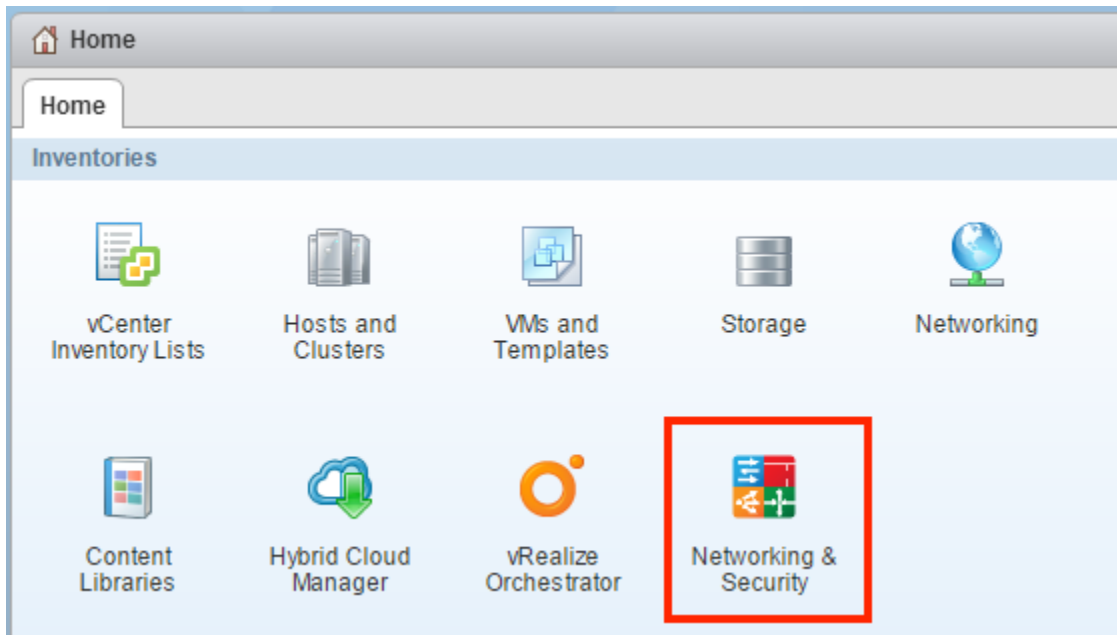
- 2 从主页中，单击**管理 vCenter 注册 (Manage vCenter Registration)**。
- 3 编辑 vCenter Server 元素以指向 vCenter Server 系统的 IP 地址或主机名，并输入 vCenter Server 系统的用户名和密码。
- 4 检查证书指纹是否与 vCenter Server 系统的证书匹配。

如果在 vCenter Server 系统上安装了 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。
- 5 不要选中**修改插件脚本下载位置 (Modify plugin script download location)**，除非 NSX Manager 位于屏蔽设备类型的防火墙后面。

此选项可允许您输入 NSX Manager 的备用 IP 地址。不建议将 NSX Manager 置于此类型防火墙的保护之下。
- 6 确认 vCenter Server 系统状态为**已连接 (Connected)**。
- 7 如果 vSphere Web Client 已打开，请注销并使用用于在 vCenter Server 中注册 NSX Manager 的帐户重新登录。

如果未注销并重新登录，则 vSphere Web Client 不会在**主页 (Home)**选项卡上显示**网络和安全 (Networking & Security)**图标。

单击**网络和安全 (Networking & Security)**图标，并确认您可以看到新部署的 NSX Manager。



#### 后续步骤

安装 NSX Manager 之后立即计划备份 NSX Manager 数据。请参阅《NSX 管理指南》中的“NSX 备份和还原”。

如果您拥有 NSX for vSphere 合作伙伴解决方案，请参考合作伙伴文档以了解在 NSX Manager 中注册合作伙伴控制台的相关信息。

现在即可安装和配置 NSX for vSphere 组件。

# 配置 Single Sign On

## 5

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：

Time Settings

Unconfigure NTP Servers

Edit

Specify NTP server below. For SSO configuration to work correctly it is required that the time on this virtual appliance and NTP server should be in sync. It is recommended to use the same NTP server used by the SSO server.

|            |                     |
|------------|---------------------|
| NTP Server | 192.168.110.10      |
| Timezone   | UTC                 |
| Date/Time  | 12/28/2016 21:31:49 |



**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（网址为 <https://<nsx-manager-ip>> 或 <https://<nsx-manager-hostname>>），然后以**管理员**身份或使用具有**企业管理员**角色的帐户登录。

- 2 登录到 NSX Manager 虚拟设备。

- 3 从主页中，单击**管理设备设置 (Manage Appliance Settings) > NSX 管理服务 (NSX Management Service)**。

- 4 在 Lookup Service URL 部分单击**编辑 (Edit)**。

- 5 输入装有 Lookup Service 的主机的名称或 IP 地址。

- 6 输入端口号。

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。

- 7 输入 SSO 管理员用户名和密码，然后单击**确定 (OK)**。


将显示 SSO 服务器的证书指纹。

- 8 检查证书指纹是否与 SSO 服务器的证书匹配。

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。

- 9 确认 Lookup Service 状态为**已连接 (Connected)**。

例如：

|                              |                                                                                                                                    |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Lookup Service URL:          | <a href="https://psc-01a.corp.local:443/lookupservice/sdk">https://psc-01a.corp.local:443/lookupservice/sdk</a>                    |
| SSO Administrator User Name: | administrator@vsphere.local                                                                                                        |
| Status:                      | <span style="color: green;">●</span> Connected  |

**后续步骤**

请参见 NSX 管理指南中的“将角色分配给 vCenter 用户”。

# 为 NSX Manager 配置 syslog 服务

## 6

如果指定了 syslog 服务器，则 NSX Manager 将所有审核日志和系统事件发送到 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 登录到 NSX Manager 虚拟设备。

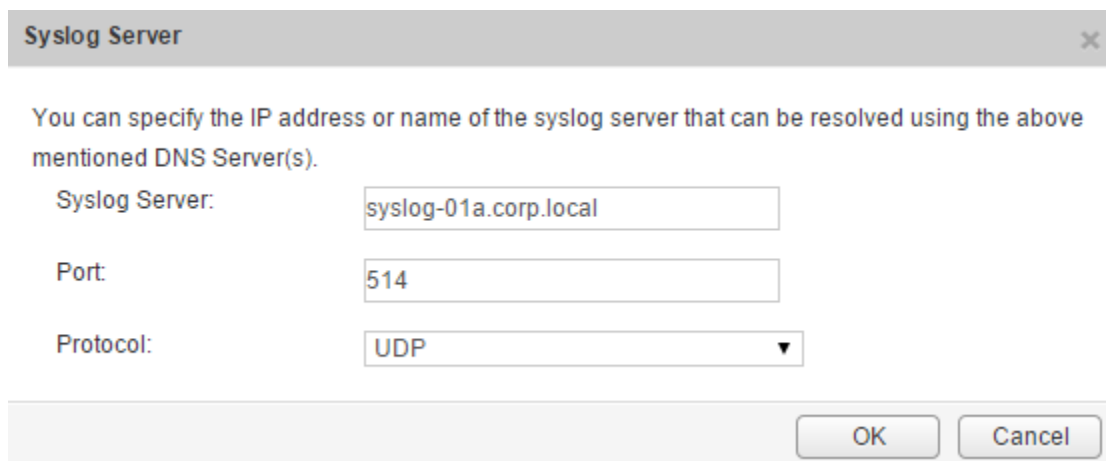
在 Web 浏览器中，导航到 NSX Manager 设备 GUI（网址为 <https://<nsx-manager-ip>> 或 <https://<nsx-manager-hostname>>），然后以管理员身份或使用具有企业管理员角色的帐户登录。

- 2 从主页中，单击**管理设备设置 (Manage Appliance Settings) > 常规 (General)**。

- 3 单击 **Syslog 服务器 (Syslog Server)** 旁边的**编辑 (Edit)**。

- 4 键入 syslog 服务器的 IP 地址或主机名、端口和协议。

例如：



Syslog Server

You can specify the IP address or name of the syslog server that can be resolved using the above mentioned DNS Server(s).

Syslog Server:

Port:

Protocol:

OK Cancel

- 5 单击**确定 (OK)**。

### 结果

将启用 NSX Manager 远程日志记录，并在单独的 syslog 服务器中存储日志。

# 安装和分配 NSX for vSphere 许可证



安装完 NSX Manager 后，可以使用 vSphere Web Client 安装和分配 NSX for vSphere 许可证。

从 NSX 6.2.3 开始，安装后的默认许可证是 NSX for vShield Endpoint。该许可证允许使用 NSX 部署和管理 vShield Endpoint 以仅提供防病毒卸载功能，并具有硬实施功能以限制使用 VXLAN、防火墙和 Edge 服务（通过阻止主机准备和 NSX Edge 创建）。

如果需要使用其他 NSX 功能（包括逻辑交换机、逻辑路由器、分布式防火墙或 NSX Edge），您必须购买 NSX 许可证以使用这些功能，或者申请评估许可证以短期评估这些功能。

有关 NSX 许可版本及相关功能的信息，请参见 <https://kb.vmware.com/kb/2145269>。

## 步骤

- ◆ 在 vSphere 5.5 中，完成以下步骤以添加 NSX 许可证。
  - a 登录到 vSphere Web Client。
  - b 单击**系统管理 (Administration)**，然后单击许可证 (**Licenses**)。
  - c 单击**解决方案 (Solutions)**选项卡。
  - d 在“解决方案”列表中，选择 NSX for vSphere。单击**分配许可证密钥 (Assign a license key)**。
  - e 从下拉菜单中选择**分配新的许可证密钥 (Assign a new license key)**。
  - f 键入许可证密钥和新密钥的可选标签。
  - g 单击**解码 (Decode)**。

对许可证密钥进行解码，以验证其格式是否正确，以及是否具有足够的容量来对资产进行授权。
  - h 单击**确定 (OK)**。
- ◆ 在 vSphere 6.0 中，完成以下步骤以添加 NSX 许可证。
  - a 登录到 vSphere Web Client。
  - b 单击**系统管理 (Administration)**，然后单击许可证 (**Licenses**)。
  - c 单击**资产 (Assets)**选项卡，然后单击**解决方案 (Solutions)**选项卡。
  - d 在“解决方案”列表中，选择 NSX for vSphere。从**所有操作 (All Actions)**下拉菜单中，选择**分配许可证... (Assign license...)**。

- e 单击**添加 (Add) (+)** 图标。输入许可证密钥，然后单击**下一步 (Next)**。添加许可证名称，然后单击**下一步 (Next)**。单击**完成 (Finish)**以添加许可证。
- f 选择新许可证。
- g (可选) 单击**View 功能 (View Features)**图标以查看使用该许可证启用的功能。查看**容量 (Capacity)**列以查看许可证的容量。
- h 单击**确定 (OK)**以将新许可证分配给 NSX。

#### 后续步骤

有关 NSX 许可的更多信息，请参见 <http://www.vmware.com/files/pdf/vmware-product-guide.pdf>。

# 部署 NSX Controller 群集

## 8

**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。它充当网络内所有逻辑交换机的中央控制点，并维护所有主机、逻辑交换机 (VXLAN) 和分布式逻辑路由器的相关信息。如果您计划部署 1) 分布式逻辑路由器或 2) 单播或混合模式下的 VXLAN，则需要控制器。

无论 **NSX** 部署的大小如何，**VMware** 都要求每个 **NSX Controller** 群集包含三个控制器节点。其他的控制器节点数量不受支持。

群集要求每个控制器的磁盘存储系统的峰值写入延迟少于 300 ms，平均写入延迟少于 100 ms。如果存储系统不满足这些要求，则群集可能变得不稳定，并且导致系统停机时间。

---

**小心** 当控制器状态为**正在部署 (Deploying)**时，请勿在您的环境中添加或修改逻辑交换机或分布式路由。另外，不要继续进行主机准备过程。在向控制器群集添加新的控制器后，所有控制器都将在短时间（不超过 5 分钟）内处于非活动状态。在此停机期间，任何与控制器相关的操作（例如，主机准备）都可能导致出现意外结果。即使主机准备可能看上去成功完成，但 **SSL** 证书可能无法正确建立，因此会导致 **VXLAN** 网络中出现问题。

---

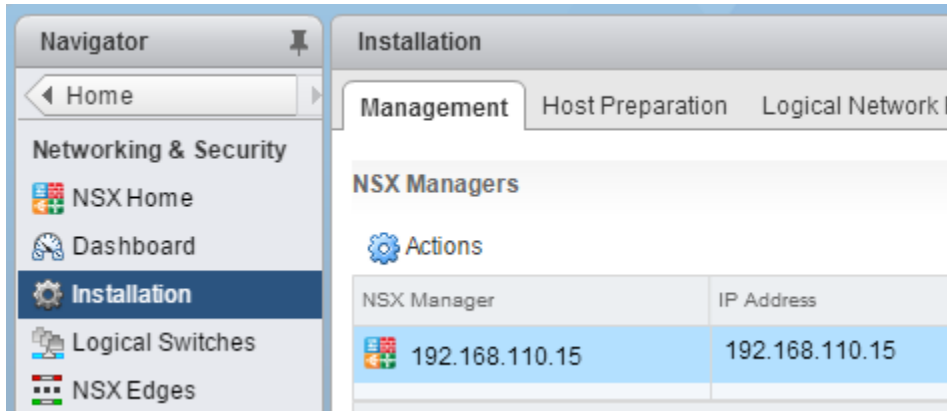
### 前提条件

- 在部署 **NSX Controller** 之前，必须部署 **NSX Manager** 设备并向 **NSX Manager** 注册 **vCenter**。
- 确定控制器群集的 IP 池设置，包括网关和 IP 地址范围。DNS 设置是可选设置。**NSX Controller** IP 网络必须具有与 **NSX Manager** 以及 **ESXi** 主机上的管理接口的连接。

### 步骤

- 1 登录到 **vSphere Web Client**。
- 2 导航到主页 > 网络和安全 > 安装 (**Home > Networking & Security > Installation**)，然后选择**管理 (Management)**选项卡。

例如：



- 3 在“NSX Controller 节点”部分，单击**添加节点 (Add Node)** (+) 图标。
- 4 输入适用于您环境的 NSX Controller 设置。

应将 NSX Controller 部署到不基于 VXLAN 并连接到 NSX Manager、其他控制器和主机（通过 IPv4）的 vSphere 标准交换机或 vSphere Distributed Switch 端口组。

例如：

**Add Controller**
?

Name: \*

NSX Manager: \*  ▼

Datacenter: \*  ▼

Cluster/Resource Pool: \*  ▼

Datastore: \*  ▼

Host:  ▼

Folder:  ▼

Connected To: \*  Change Remove

IP Pool: \*  Select

Password: \*

Confirm password: \*

- 5 如果尚未为您的控制器群集配置 IP 池，请立即通过单击**新建 IP 池 (New IP Pool)**配置一个。  
如果需要，单个控制器可以位于单独的 IP 子网中。

例如：

## 6 键入并再次键入控制器的密码。

**注** 密码中不得包含用户名作为子字符串。任何字符不得连续重复 3 次或以上。

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

## 7 在完全部署第一个控制器后，部署其他两个控制器。

必须具有三个控制器。我们建议配置 DRS 反关联性规则以防止控制器位于相同的主机上。

### 结果

在成功部署后，控制器将处于**已连接 (Connected)**状态并显示绿色对勾。

如果部署失败，请参阅《NSX 故障排除指南》中的“部署 NSX Controller”。

在第一次部署 NSX Controller 节点的主机上，NSX 会启用自动虚拟机启动/关机。如果控制器节点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)。

## 示例



# 从防火墙保护中排除虚拟机

## 9

可以从 NSX 分布式防火墙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 分布式防火墙保护中排除。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。

---

**注** 在将允许任何流量的默认规则从允许更改为阻止之前，请务必将 **vCenter Server** 添加到排除列表中。如果不执行该操作，在创建“拒绝全部”规则（或将默认规则修改为阻止操作）后，将会导致 **vCenter Server** 访问被阻止。如果出现此问题，请运行以下 API 命令，将 DFW 回滚到默认防火墙规则集：[https://NSX\\_Manager\\_IP/api/4.0/firewall/globalroot-0/config](https://NSX_Manager_IP/api/4.0/firewall/globalroot-0/config)。请求必须返回状态 204。这将还原 DFW 的默认策略（其默认规则为允许），并重新启用对 **vCenter Server** 和 **vSphere Web Client** 的访问。

---

- 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 分布式防火墙保护，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 选择您要排除的虚拟机，然后单击 **添加 (Add)**。
- 7 单击 **确定 (OK)**。

## 结果

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。

# 为 NSX 准备主机群集

# 10

主机准备是 NSX Manager 执行的一个流程，即 1) 在 vCenter 群集成员的 ESXi 主机上安装内核模块，以及 2) 构建控制层面和管理层面结构。封装在 VIB 文件中的 NSX for vSphere 内核模块在管理程序内核中运行，并提供分布式路由、分布式防火墙等服务以及 VXLAN 桥接功能。

要准备进行网络虚拟化的环境，必须在所需的每个 vCenter server 的每个群集上安装网络基础架构组件。这是在群集中的所有主机上部署所需软件。将新主机添加到此群集时，所需软件将自动安装在新添加的主机上。

如果在无状态模式下使用 ESXi（意味着 ESXi 在重新引导期间不会主动保留其状态），您必须手动下载 NSX VIB 并让它们成为主机图像的一部分。NSX VIB 的下载路径详见以下页面：[https://<NSX\\_MANAGER\\_IP>/bin/vdn/nwfabric.properties](https://<NSX_MANAGER_IP>/bin/vdn/nwfabric.properties)。请注意，每个 NSX 版本的下载路径均有可能变化。请务必查看 [https://<NSX\\_MANAGER\\_IP>/bin/vdn/nwfabric.properties](https://<NSX_MANAGER_IP>/bin/vdn/nwfabric.properties) 页面以获取相应的 VIB。有关详细信息，请参见“通过 Auto Deploy 部署 VXLAN (<https://kb.vmware.com/kb/2041972>)”。

## 前提条件

- 在 NSX Manager 中注册 vCenter Server 并部署 NSX Controller。
- 确认 DNS 反向查找在查询 NSX Manager 的 IP 地址时返回完全限定域名。例如：

```
C:\Users\Administrator>nslookup 192.168.110.42
Server: localhost
Address: 127.0.0.1

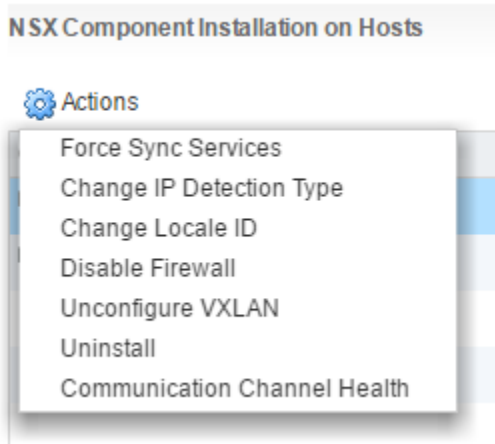
Name: nsxmgr-l-01a.corp.local
Address: 192.168.110.42
```

- 确认主机可以解析 vCenter Server 的 DNS 名称。
- 确认主机可以通过端口 80 连接到 vCenter Server。
- 确认 vCenter Server 和 ESXi 主机上的网络时间已同步。
- 对于加入 NSX 的每个主机群集，确认群集中的主机连接到一个通用 vSphere Distributed Switch (VDS)。

例如，假如您有一个包含 Host1 和 Host2 的群集。Host1 连接到 VDS1 和 VDS2。Host2 连接到 VDS1 和 VDS3。为 NSX 准备群集时，您只能将 NSX 与群集中的 VDS1 相关联。如果向该群集添加另一个主机 (Host3) 且 Host3 未连接到 VDS1，则配置无效，而且 Host3 将无法用于 NSX 功能。

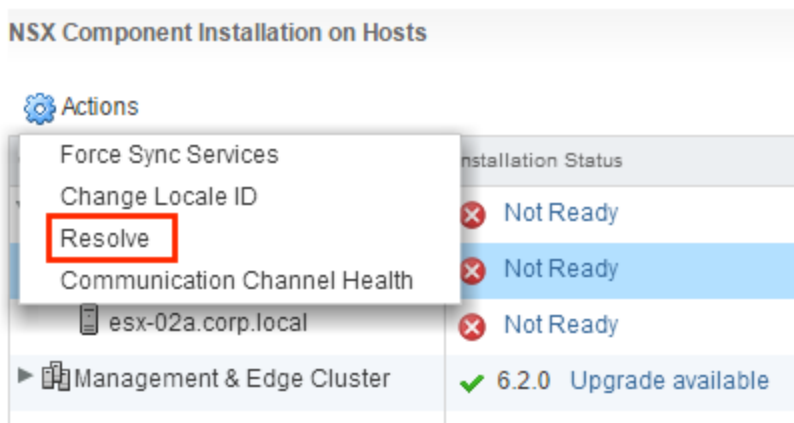
- 如果您的环境中具有 vSphere Update Manager (VUM)，您必须在准备进行网络虚拟化的群集之前将其禁用。有关如何确认 VUM 是否启用及如何在必要时禁用的信息，请参见 <http://kb.vmware.com/kb/2053782>。
- 开始 NSX 主机准备流程之前，务必要确保群集处于已解决状态—这意味着群集的操作 (Actions) 列表中不显示解决 (Resolve) 选项。

例如：



解决 (Resolve) 选项有时会在群集中的一个或多个主机需要引导的情况下显示。

但解决 (Resolve) 选项多数会在存在需要解决的错误状态时显示。单击未就绪 (Not Ready) 进行链接以查看错误。如果可以，请清除错误状态。如果无法清除群集上的错误状态，可以采用一种解决办法，即将主机移至新群集或其他群集并删除旧群集。



如果解决 (Resolve) 选项无法修复该问题，请参阅 NSX 故障排除指南。要查看解决 (Resolve) 选项解决的问题列表，请参阅 NSX 日志记录和系统事件。

## 步骤

- 1 登录到 vSphere Web Client。
- 2 导航到主页 > 网络和安全 > 安装 (Home > Networking & Security > Installation)，然后选择主机准备 (Host Preparation) 选项卡。
- 3 对于需要使用 NSX 逻辑交换、路由和防火墙的所有群集，单击操作 (Actions) (⚙️)，然后单击安装 (Install)。

计算群集（也被称为“有效负载群集”）是使用应用程序虚拟机（Web、数据库等）的群集。如果一个计算群集将具备 NSX 交换、路由或防火墙功能，您必须针对该计算群集单击安装 (Install)。

在共享的“管理和 Edge”群集（如示例中所示）中，NSX Manager 和控制器虚拟机共享包含 Edge 设备的群集，Edge 设备包括分布式逻辑路由器 (DLR) 和 Edge 服务网关 (ESG) 等。在此情况下，务必要针对该共享群集单击安装 (Install)。

相反，如果管理和 Edge 分别具有一个专用的非共享群集（建议在生产环境中使用），请为 Edge 群集单击安装 (Install)，但不要为管理群集单击该按钮。

**注** 正在进行安装时，不要部署、升级或卸载任何服务或组件。

- 4 监控安装，直到安装状态 (Installation Status) 列显示绿色对勾。

如果安装状态 (Installation Status) 列显示红色警告图标并显示未就绪 (Not Ready)，请单击解决 (Resolve)。单击解决 (Resolve) 可能导致主机重新引导。如果安装仍不成功，请单击警告图标。此时会显示所有错误。执行所需操作，然后重新单击解决办法 (Resolve)。

在安装完成后，安装状态 (Installation Status) 列将显示安装的 NSX 版本和内部版本，并且防火墙 (Firewall) 列显示已启用 (Enabled)。这两列均有一个绿色对勾。如果在安装状态 (Installation Status) 列中看到“解决”，请单击“解决”，然后刷新浏览器窗口。

## 结果

将在准备的群集内的所有主机中安装并注册 VIB。安装的 VIB 因安装的 NSX 和 ESXi 版本而异。

| ESXi 版本   | NSX 版本      | 安装的 VIB                                                                           |
|-----------|-------------|-----------------------------------------------------------------------------------|
| 5.5       | 任何 6.3.x    | <ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul> |
| 6.0 或更高版本 | 6.3.2 或更低版本 | <ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul> |
| 6.0 或更高版本 | 6.3.3 或更高版本 | <ul style="list-style-type: none"> <li>■ esx-nsxv</li> </ul>                      |

要进行验证，请通过 SSH 连接到每个主机，然后运行 `esxcli software vib list` 命令并检查相关的 VIB。除了显示 VIB 之外，此命令还可显示已安装 VIB 的版本。

```
[root@host:~] esxcli software vib list | grep esx
esx-XXXX 6.0.0-0.0.XXXXXXX VMware VMwareCertified 2016-12-29
```

如果将主机添加到准备好的群集，NSX VIB 会自动安装在该主机上。

如果将主机移至未准备好的群集，NSX VIB 将从该主机中自动卸载 NSX VIB。

# 向准备好的群集添加主机

# 11

本部分介绍如何向为网络虚拟化准备的群集添加主机。

## 步骤

- 1 将主机作为独立主机添加到 vCenter Server。  
请参阅《ESXi 和 vCenter Server 文档》。
- 2 将主机添加到 vSphere Distributed Switch，后者需已映射至该主机要加入的群集。  
该群集中的所有主机都必须位于 NSX 正利用的 vSphere Distributed Switch 中。
- 3 右键单击目标主机，然后选择**维护模式 (Maintenance Mode) > 进入维护模式 (Enter Maintenance Mode)**。
- 4 将目标主机拖放到启用了 NSX 的现有群集中。  
由于这是已准备好的群集，新添加的主机将会自动安装需要的软件。
- 5 右键单击主机，然后选择**维护模式 (Maintenance Mode) > 退出维护模式 (Exit Maintenance Mode)**。  
DRS 会在该主机上放置虚拟机以确保平衡。

# 从准备 NSX 部署的群集中移除主机

# 12

本节介绍如何从为网络虚拟化准备的群集中移除主机。例如，如果您决定不让主机加入 **NSX**，则可能需要移除主机。

**重要事项** 如果主机具有 **NSX 6.3.0** 或更高版本和 **ESXi 6.0** 或更高版本，则不需要重新引导主机以卸载 **VIB**。在更低版本的 **NSX** 和 **ESXi** 中，需要重新引导才能完成 **VIB** 卸载。

## 步骤

- 1 将主机置于维护模式，并等待 **DRS** 撤出主机，或者通过 **vMotion** 手动迁移主机中正在运行的虚拟机。
- 2 将主机从已准备就绪的群集移至未准备就绪的群集，或者将其设置为任意群集外部的独立主机，从而移除主机

**NSX** 从主机中卸载网络虚拟化组件和服务虚拟机。

- 3 如果主机安装了 **NSX 6.2.x** 或更低版本或安装了 **ESXi 5.5**，请重新引导主机。
- 4 确认 **VIB** 卸载已完成。
  - a 检查 **vSphere Web Client** 中的“近期任务”窗格。
  - b 在**主机准备 (Host Preparation)**选项卡中，查看从中移除了主机的群集的安装状态，确定它是否具有绿色对勾。

如果安装状态为正在安装，则表明卸载仍在进行。

- 5 在卸载完成后，从维护模式中移除主机。

## 结果

**NSX VIB** 将从主机中移除。要进行验证，请运行 **SSH** 命令以连接到主机，然后运行 **esxcli software vib list | grep esx** 命令。请确保以下 **VIB** 不在主机上：

- **esx-vsip**
- **esx-vxlan**

如果 **VIB** 仍位于主机上，您可以查看日志，以确定自动执行的 **VIB** 移除操作失效的原因。

可以通过运行以下命令手动移除 **VIB**：

- **esxcli software vib remove --vibname=esx-vxlan**
- **esxcli software vib remove --vibname=esx-vsip**



# 配置 VXLAN 传输参数

# 13

VXLAN 网络可用于主机之间的第 2 层逻辑交换，可能跨越多个底层第 3 层域。在每个群集的基础上配置 VXLAN，在该配置中可将要加入 NSX 的每个群集映射到 vSphere Distributed Switch (VDS)。将群集映射到 Distributed Switch 时，将为逻辑交换机启用该群集中的每个主机。此处所选设置将用于创建 VMkernel 接口。

如果需要进行逻辑路由和交换，则主机上安装有 NSX VIB 的所有群集还应配置 VXLAN 传输参数。如果计划仅部署分布式防火墙，则无需配置 VXLAN 传输参数。

在配置 VXLAN 网络时，您必须提供 vSphere Distributed Switch、VLAN ID、MTU 大小、IP 寻址机制（DHCP 或 IP 池）和网卡绑定策略。

每个交换机的 MTU 都必须设置为 1550 或更高值。默认情况下，该值设置为 1600。如果 vSphere Distributed Switch MTU 大于 VXLAN MTU，则不会下调 vSphere Distributed Switch MTU。如果该值设置较低，将会对其进行调整以匹配 VXLAN MTU。例如，如果 vSphere Distributed Switch MTU 设置为 2000，并且您接受默认 VXLAN MTU 值 1600，则不会对 vSphere Distributed Switch MTU 进行更改。如果 vSphere Distributed Switch MTU 是 1500，并且 VXLAN MTU 是 1600，vSphere Distributed Switch MTU 将更改为 1600。

VTEP 具有关联的 VLAN ID。但是，您可以为 VTEP 指定 VLAN ID = 0，这意味着将不标记帧。

您可能需要在管理群集和计算群集中使用不同的 IP 地址设置。这取决于物理网络的设计方式，而在小型部署中，很可能不是这种情况。

## 前提条件

- 群集中的所有主机必须连接到一个通用 vSphere Distributed Switch。
- 必须安装 NSX Manager。
- 必须安装 NSX Controller，除非您使用的是控制层面的多播复制模式。
- 计划您的网卡绑定策略。您的网卡绑定策略确定 vSphere Distributed Switch 的负载平衡和故障切换设置。

不要在 vSphere Distributed Switch 上的不同端口组中混用不同的绑定策略，有些端口组使用以太网通道、LACPv1 或 LACPv2，而其他端口组使用不同的绑定策略。如果这些不同的绑定策略共享上行链路，通信将会中断。如果存在逻辑路由器，将出现路由问题。此类配置不受支持，您应避免使用。

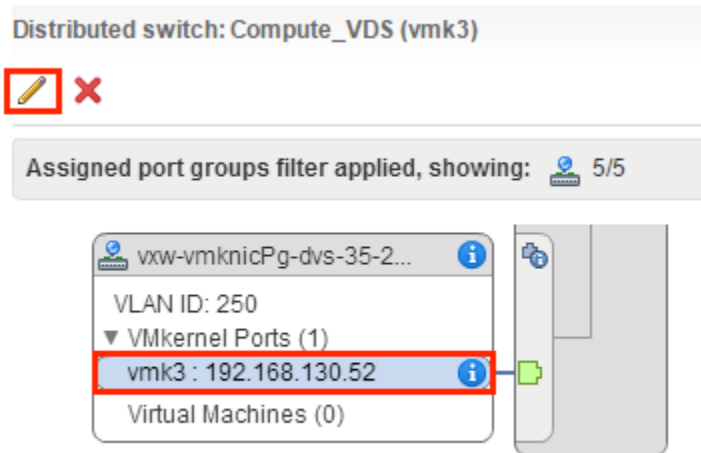
基于 IP 哈希的绑定（以太网通道、LACPv1 或 LACPv2）的最佳做法是在组中使用 vSphere Distributed Switch 上的所有上行链路，而不是在该 vSphere Distributed Switch 上的端口组中使用不同的绑定策略。有关详细信息和更多指导，请参见 <https://communities.vmware.com/docs/DOC-27683> 上的《VMware® NSX for vSphere 网络虚拟化设计指南》。

- 为 VXLAN 隧道终端 (VTEP) 计划 IP 寻址方案。VTEP 是在外部 IP 标头中使用的源和目标 IP 地址，可唯一标识发出和终止 VXLAN 帧封装的 ESX 主机。您可以使用 DHCP 或手动为 VTEP IP 地址配置的 IP 池。

如果要将特定的 IP 地址分配给 VTEP，您可以 1) 使用将 MAC 地址映射到 DHCP 服务器中的特定 IP 地址的 DHCP 固定地址或预留，或者 2) 使用 IP 池并在 **主机和群集 (Hosts and Clusters) > 主机 (host) > 管理 (Manage) > 网络 (Networking) > 虚拟交换机 (Virtual Switches)** 中手动编辑分配给 vmknics 的 VTEP IP 地址。

**注** 如果您手动编辑 IP 地址，请确保 IP 地址与原始 IP 池范围不相似。

例如：



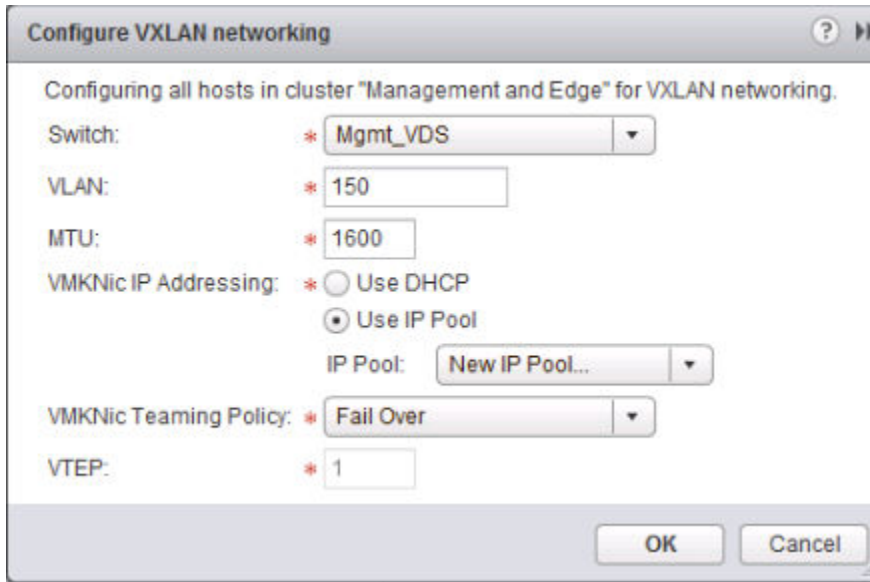
- 对于为相同 VDS 成员的群集，VTEP 的 VLAN ID 和网卡绑定必须相同。
- 最佳做法是，在为 VXLAN 准备群集之前导出 vSphere Distributed Switch 配置。请参见 <http://kb.vmware.com/kb/2034602>。

#### 步骤

- 1 登录到 vSphere Web Client。
- 2 导航到 **主页 > 网络和安全 > 安装 (Home > Networking & Security > Installation)**，然后选择 **主机准备 (Host Preparation)** 选项卡。
- 3 在 **VXLAN** 列中单击 **未配置 (Not Configured)**。
- 4 设置逻辑网络。

这包括选择 vSphere Distributed Switch、VLAN ID、MTU 大小、IP 寻址机制和网卡绑定策略。

以下示例屏幕显示了以下管理群集配置：VLAN 150 所支持的 IP 池地址范围为 182.168.150.1-192.168.150.100 且使用故障切换网卡绑定策略。



**Configure VXLAN networking**

Configuring all hosts in cluster "Management and Edge" for VXLAN networking.

Switch: \* Mgmt\_VDS

VLAN: \* 150

MTU: \* 1600

VMKNic IP Addressing: \* ☐ Use DHCP ☒ Use IP Pool

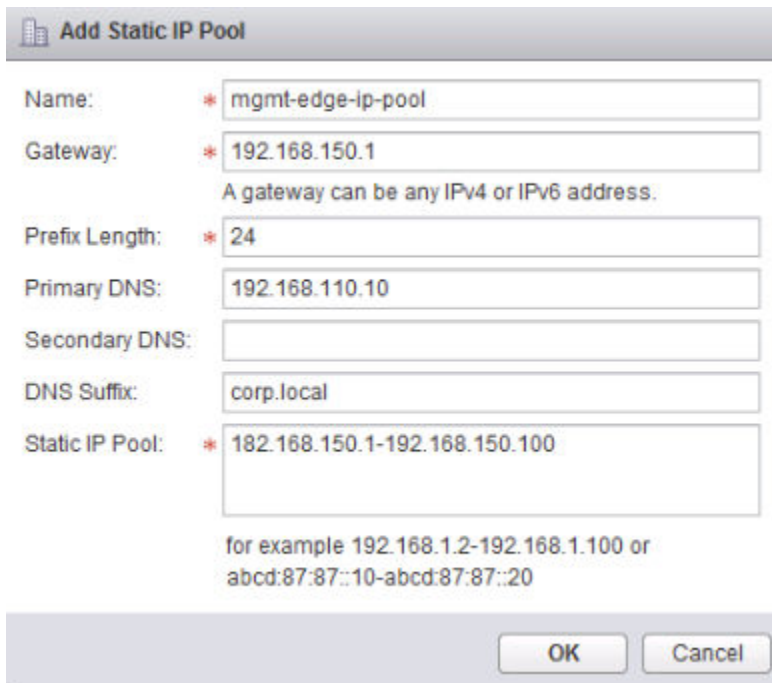
IP Pool: New IP Pool...

VMKNic Teaming Policy: \* Fail Over

VTEP: \* 1

OK Cancel

在该 UI 中，VTEP 的数量不可编辑。VTEP 数量已设置为匹配正在准备的 vSphere Distributed Switch 上的 dvUplink 数量。



**Add Static IP Pool**

Name: \* mgmt-edge-ip-pool

Gateway: \* 192.168.150.1

A gateway can be any IPv4 or IPv6 address.

Prefix Length: \* 24

Primary DNS: 192.168.110.10

Secondary DNS:

DNS Suffix: corp.local

Static IP Pool: \* 182.168.150.1-192.168.150.100

for example 192.168.1.2-192.168.1.100 or  
abcd:87:87::10-abcd:87:87::20

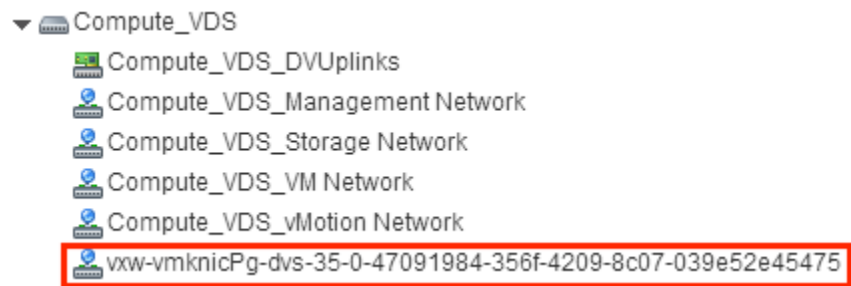
OK Cancel

对于计算群集，您可能希望使用其他 IP 地址设置（例如，使用 VLAN 250 的 192.168.250.0/24）。这取决于物理网络的设计方式，而在小型部署中，很可能不是这种情况。

## 结果

配置 VXLAN 将导致在指定的 vSphere Distributed Switch 中创建新的分布式端口组。

例如：



有关排除 VXLAN 故障的详细信息，请参阅 [NSX 故障排除指南](#)。

# 分配分段 ID 池和多播地址范围

# 14

VXLAN 分段构建于 VXLAN 隧道端点 (VTEP) 之间。虚拟化管理程序主机是一个典型的 VTEP 示例。每个 VXLAN 隧道都具有一个分段 ID。必须为每个 NSX Manager 指定一个分段 ID 池来隔离网络流量。如果您的环境中未部署 NSX Controller，则还必须添加一个多播地址范围以帮助将流量分散到网络中，从而避免单个多播地址过载。

在确定每个分段 ID 池的大小时，请记住，分段 ID 池范围控制可以创建的逻辑交换机的数量。选择 1600 万潜在 VNI 的小性子集。单个 vCenter 中不应配置超过 10,000 个 VNI，因为 vCenter 将 dvPortgroup 的数量限制为 10,000。

如果 VXLAN 位于其他 NSX 部署中，请考虑哪些 VNI 已在使用并避免重叠 VNI。单个 NSX Manager 和 vCenter 环境中会自动实施非重叠 VNI。本地 VNI 范围不可重叠。但重要的是，您应确保 VNI 在单独的 NSX 部署中不会重叠。非重叠 VNI 对跟踪很有用，并且有助于确保您的部署已针对跨 vCenter 环境做好了准备。

如果任何传输区域将使用多播或混合复制模式，您必须添加一个多播地址或一定范围的多播地址。

如果具有多个多播地址，则可将流量分散到网络中，防止单个多播地址超载，并能更好地包含 BUM 复制。

请勿使用 239.0.0.0/24 或 239.128.0.0/24 作为多播地址范围，因为这些网络用于本地子网控制，这意味着物理交换机会使所有使用这些地址的流量泛洪。有关不可用多播地址的详细信息，请参见 <https://tools.ietf.org/html/draft-ietf-mboned-ipv4-mcast-unusable-01>。

如果 VXLAN 多播和混合复制模式配置正确且运行正常，则只会将多播流量的副本传送给已发送 IGMP 加入消息的主机。否则，物理网络会把所有多播流量泛洪到同一广播域中的所有主机。要避免此类泛洪，必须：

- 确保为底层物理交换机配置的 MTU 大于或等于 1600。
- 确保底层物理交换机配置正确，在承载 VTEP 流量的网络分段中启用了 IGMP 侦听和 IGMP 查询器功能。
- 确保为传输区域配置了建议的多播地址范围。建议的多播地址范围从 239.0.1.0/24 开始，并排除 239.128.0.0/24。

在 vSphere Web Client 界面中，您可以配置单个分段 ID 范围以及单个多播地址或多播地址范围。如果要配置多个分段 ID 范围或多个多播地址值，您可以使用 NSX API 执行该操作。请参阅《NSX API 指南》以了解详细信息。

## 步骤

- 1 登录到 vSphere Web Client。
- 2 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。
- 3 单击分段 ID > 编辑 (Segment ID > Edit)。
- 4 输入一个分段 ID 范围，例如，**5000–5999**。
- 5 （可选） 如果任何传输区域将使用多播或混合复制模式，您必须添加一个多播地址或一定范围的多播地址。
  - a 选中启用多播寻址 (Enable Multicast addressing) 复选框。
  - b 输入一个多播地址或多播地址范围，例如，**239.0.0.0–239.255.255.255**。

## 结果

配置逻辑交换机时，每个逻辑交换机都会接收来自该池的分段 ID。

## 添加传输区域

# 15

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。

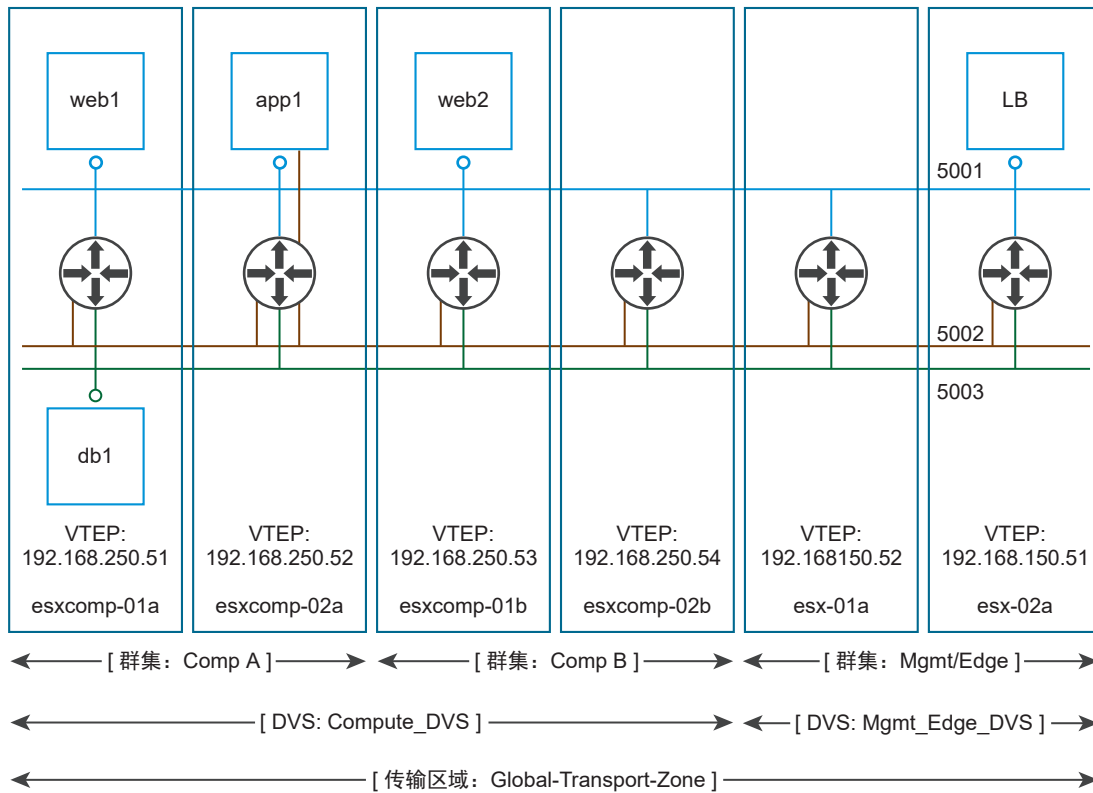
**NSX** 环境可以根据您的需要包含一个或多个传输区域。一个主机群集可以属于多个传输区域。一个逻辑交换机只能属于一个传输区域。

**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。

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。

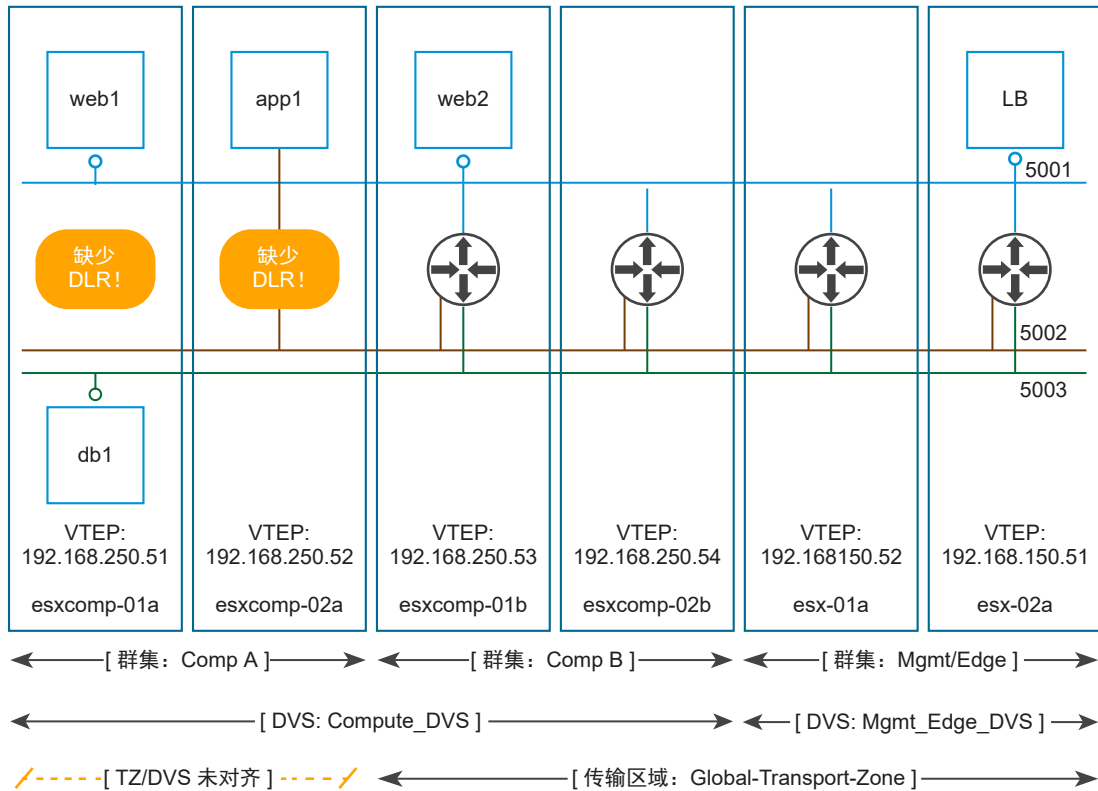
下图显示了一个与 **VDS** 边界正确对齐的传输区域。



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)。

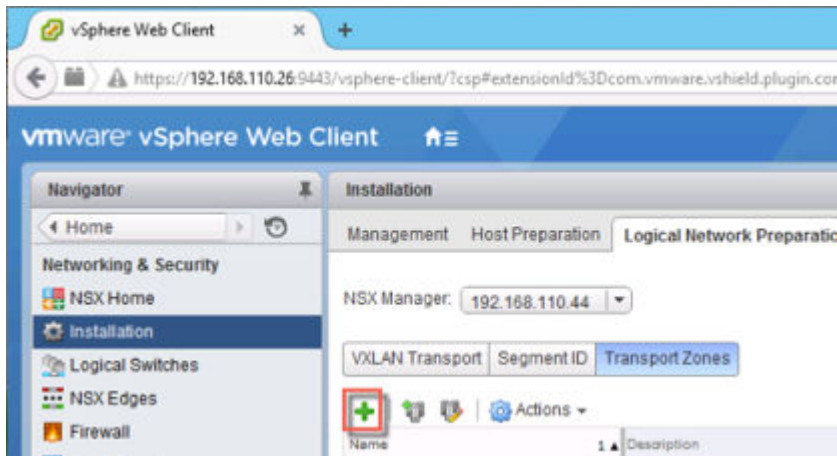




## 步骤

- 1 登录到 vSphere Web Client。
- 2 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。
- 3 单击传输区域 (Transport Zones)，然后单击新建传输区域 (New Transport Zone) (+) 图标。

例如：



- 4 在“新建传输区域”对话框中，键入传输区域的名称和可选描述。

5 根据您的环境中是否有控制器节点或是否要使用多播地址，选择控制层面模式。

- **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。

6 选择要添加到传输区域的群集。

例如：

**New Transport Zone**

Name:

Description:

Replication mode:

- ☐ Multicast  
*Multicast on Physical network used for VXLAN control plane.*
- ☒ Unicast  
*VXLAN control plane handled by NSX Controller Cluster.*
- ☐ Hybrid  
*Optimized Unicast mode. Offloads local traffic replication to physical network.*

Select clusters that will be part of the Transport Zone

|                                     | Name                         | NSX vSwitch | Status |
|-------------------------------------|------------------------------|-------------|--------|
| <input checked="" type="checkbox"/> | Compute Cluster A            | Compute_DVS | Normal |
| <input checked="" type="checkbox"/> | Compute Cluster B            | Compute_DVS | Normal |
| <input checked="" type="checkbox"/> | Management and Edge Clust... | Mgmt_VDS    | Normal |

OK Cancel

#### 后续步骤

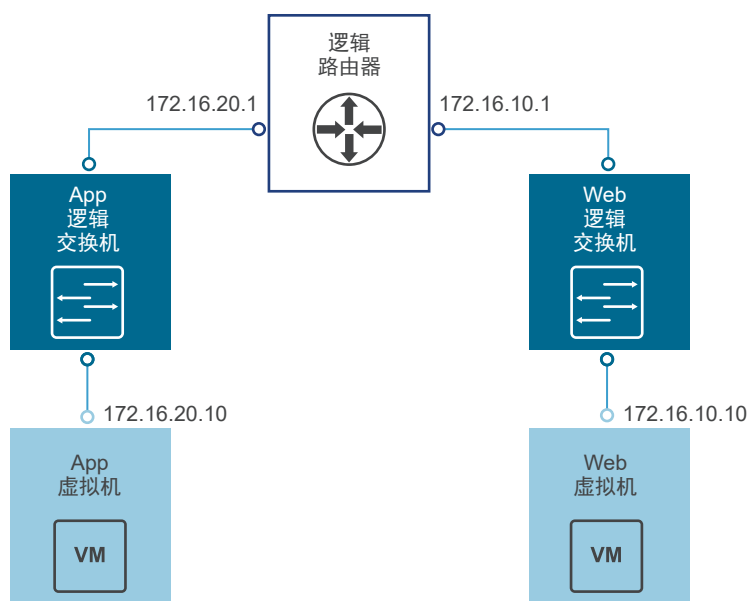
您已经拥有传输区域，现在可以添加逻辑交换机了。

## 添加逻辑交换机

# 16

NSX for vSphere 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。如果将这些虚拟机连接到同一逻辑交换机，它们就可以通过 VXLAN 相互通信。每个逻辑交换机都有一个类似 VLAN ID 的分段 ID。但与 VLAN ID 不同的是，分段 ID 的数量可能多达 1600 万个。

添加逻辑交换机时，务必记住您正在构建的特定拓扑。例如，以下简单拓扑显示了两个连接到一个分布式逻辑路由器 (DLR) 的逻辑交换机。在此图中，每个逻辑交换机都连接到一个虚拟机。两个虚拟机可以位于不同主机群集或同一主机群集中的不同主机或同一主机上。如果 DLR 未将这些虚拟机分离开来，则虚拟机上配置的底层 IP 地址可能位于同一子网中。如果 DLR 将这些虚拟机分离开来，则虚拟机上的 IP 地址必须位于不同子网中（如示例中所示）。



在创建逻辑交换机时，除了选择传输区域和复制模式以外，您还会配置两个选项：IP 发现和 MAC 发现。

IP 发现最大限度减少各个 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，将启用 IP 发现。

MAC 发现在每个 vNIC 上构建一个 VLAN/MAC 对发现表。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。如果正在使用中继 VLAN 的虚拟网卡，您可能希望启用 MAC 发现。

## 前提条件

- 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。

## 步骤



- 1 登录到 vSphere Web Client。
- 2 导航到主页 > 网络和安全 > 逻辑交换机 (Home > Networking & Security > Logical Switches)。
- 3 单击**新建逻辑交换机 (New Logical Switch)** ()。
- 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。

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。

- 6 (可选) 覆盖传输区域确定的复制模式。

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。

所创建的逻辑交换机在其将承载的 BUM 流量方面具有明显不同的特点时，您可能希望替代单个逻辑交换机所继承传输区域的控制层面复制模式。在这种情况下，您可以创建一个以单播模式使用的传输区域，并对此单个逻辑交换机使用混合或多播模式。

- 7 (可选) 单击**启用 IP 发现 (Enable IP Discovery)**以启用 ARP 禁止功能。
- 8 (可选) 单击**启用 MAC 发现 (Enable MAC learning)**。
- 9 选择逻辑交换机并单击**添加虚拟机 (Add Virtual Machine)** () 以将虚拟机连接到该交换机。
- 10 选择一个或多个虚拟机，然后单击向右箭头按钮 ()。

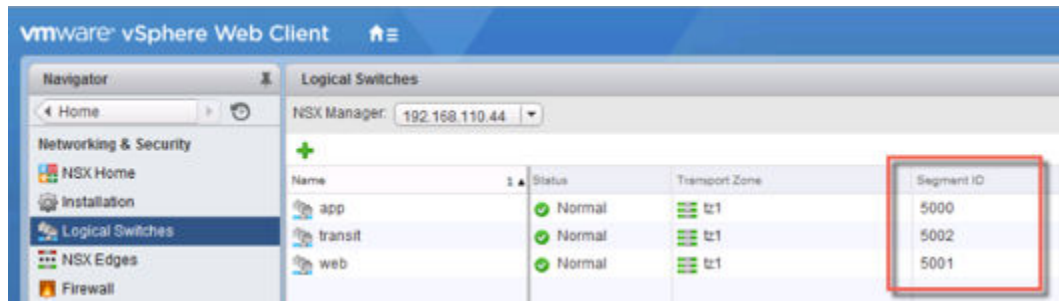
虚拟机将从“可用对象”移到“选定对象”中。

- 11 单击**下一步 (Next)**，然后为每个虚拟机选择一个 vNIC。单击**完成 (Finish)**。

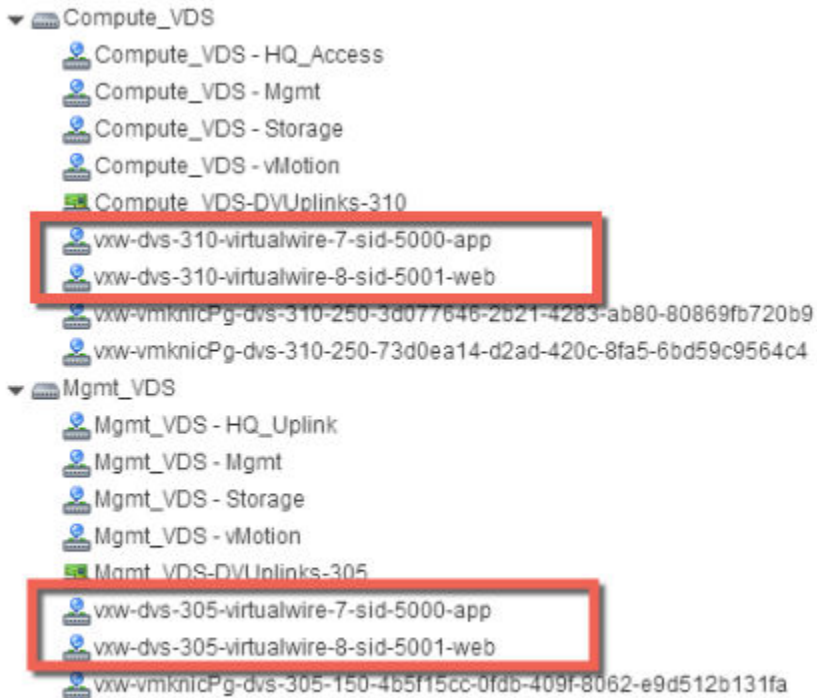
## 结果

您创建的每个逻辑交换机都将从分段 ID 池收到一个 ID，且将创建一个虚拟线路。虚拟线路是在每个 vSphere Distributed Switch 上创建的 dvPortgroup。虚拟线路描述符包含逻辑交换机的名称和分段 ID。分配的分段 ID 将显示在多个位置，如以下示例中所示。

在主页 > 网络和安全 > 逻辑交换机 (Home > Networking & Security > Logical Switches)中：

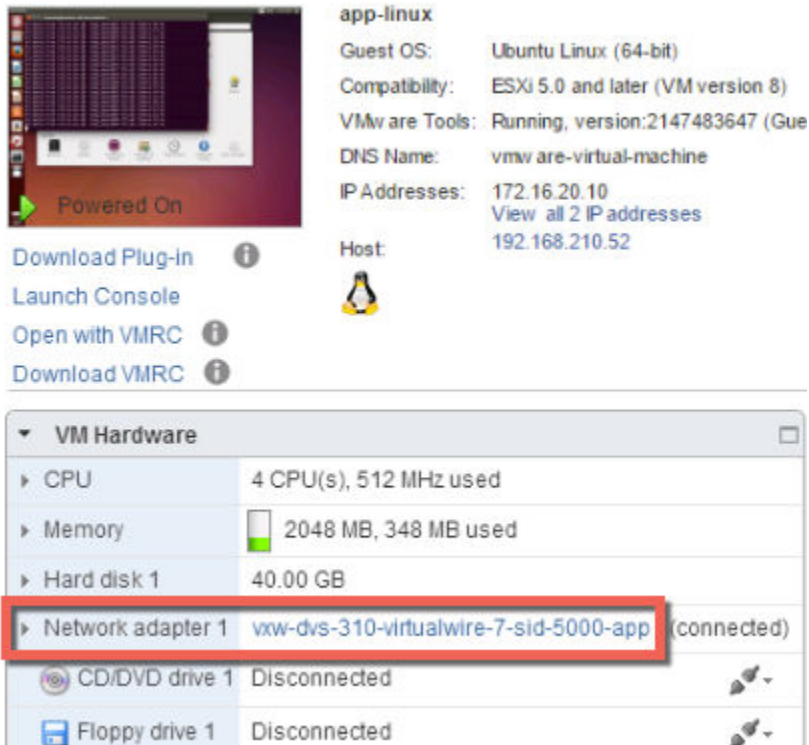


在主页 > 网络 (Home > Networking)中:



请注意，在两个 vSphere Distributed Switch (Compute\_VDS 和 Mgmt\_VDS) 上都会创建虚拟线路。这是因为这两个 vSphere Distributed Switch 都是与 Web 和应用程序逻辑交换机关联的传输区域的成员。

在主页 > 主机和群集 > 虚拟机 > 摘要 (Home > Hosts and Clusters > VM > Summary)中:



在运行连接到逻辑交换机的虚拟机的主机上，进行登录并执行以下命令，以查看逻辑 **VXLAN** 配置和状态信息。

- 显示主机特定的 **VXLAN** 详细信息。

```
~ # esxcli network vswitch dvs vmware vxlan list
```

| VDS ID                                                            | VDS Name    | MTU  | Segment ID    | Gateway IP    |
|-------------------------------------------------------------------|-------------|------|---------------|---------------|
| 88 eb 0e 50 96 af 1d f1-36 fe c1 ef a1 51 51 49 ff:ff:ff:ff:ff:ff | Compute_VDS | 1600 | 192.168.250.0 | 192.168.250.1 |

**注** 如果 `esxcli network vswitch dvs vmware vxlan` 命令生成“未知命令或命名空间 (Unknown command or namespace)”错误消息，请在主机上运行 `/etc/init.d/hostd restart` 命令，然后重试。

“VDS 名称”显示主机连接到的 vSphere Distributed Switch。

“分段 ID”是 VXLAN 使用的 IP 网络。

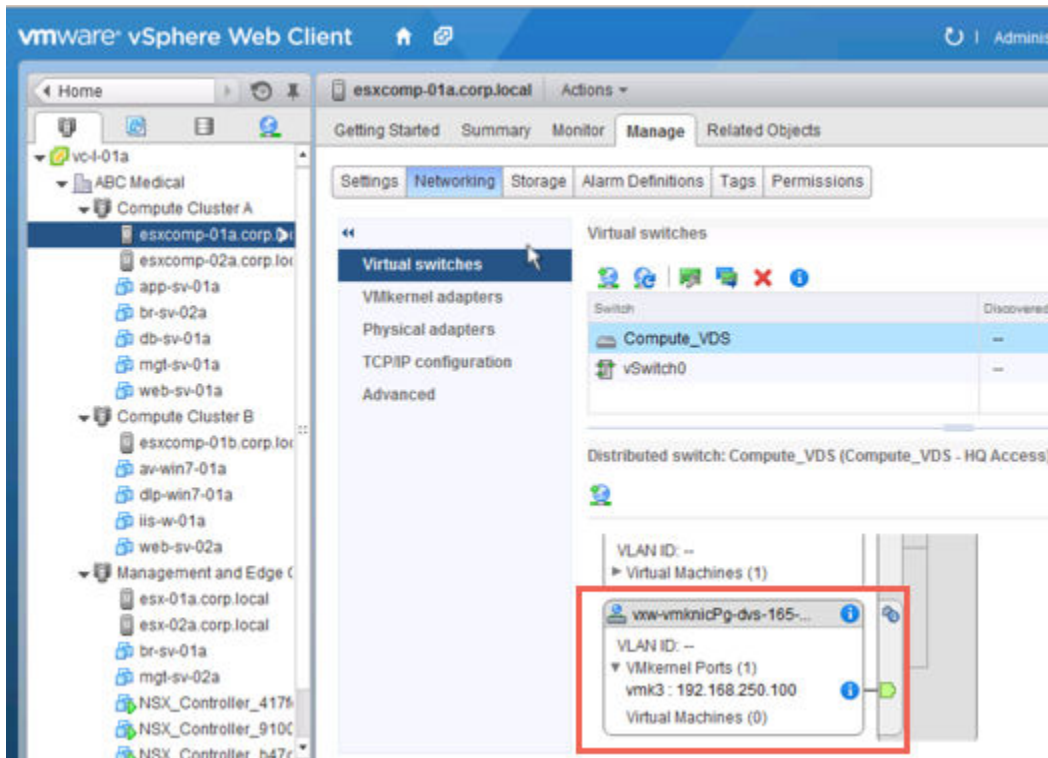
“网关 IP”是 VXLAN 使用的网关 IP 地址。

网关 MAC 地址保持为 `ff:ff:ff:ff:ff:ff`。

“网络计数”保持为 0，除非 DLR 连接到逻辑交换机。

Vmknics 计数应与连接到逻辑交换机的虚拟机数相匹配。

- 测试 IP VTEP 接口连接，并确认 MTU 已增加，可支持 VXLAN 封装。Ping vmknic 接口 IP 地址，该地址可在 vCenter Web Client 中主机的管理 > 网络 > 虚拟交换机 (Manage > Networking > Virtual switches)页面上找到。



-d 标记用于设置 IPv4 数据包上的不分段 (DF) 位。-s 标记用于设置数据包大小。

```
root@esxcomp-02a ~ # vmkping ++netstack=vxlan -d -s 1570 192.168.250.100
PING 192.168.250.100 (192.168.250.100): 1570 data bytes
1578 bytes from 192.168.250.100: icmp_seq=0 ttl=64 time=1.294 ms
1578 bytes from 192.168.250.100: icmp_seq=1 ttl=64 time=0.686 ms
1578 bytes from 192.168.250.100: icmp_seq=2 ttl=64 time=0.758 ms
```

```
--- 192.168.250.100 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.686/0.913/1.294 ms
~ #
```

```
root@esxcomp-01a ~ # vmkping ++netstack=vxlan -d -s 1570 192.168.250.101
PING 192.168.250.101 (192.168.250.101): 1570 data bytes
1578 bytes from 192.168.250.101: icmp_seq=0 ttl=64 time=0.065 ms
1578 bytes from 192.168.250.101: icmp_seq=1 ttl=64 time=0.118 ms
```

```
--- 192.168.250.101 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.065/0.091/0.118 ms
```

## 后续步骤

创建一个逻辑（分布式）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。



# 添加分布式逻辑路由器

# 17

分布式逻辑路由器 (DLR) 是一个包含控制层面和数据层面的虚拟设备，控制层面用于管理路由，而数据层面则从内部模块分发到各个虚拟机管理程序主机。DLR 控制层面功能依靠 NSX Controller 群集将路由更新推送到内核模块。

在部署新的逻辑路由器时，请考虑以下事项：

- NSX 6.2 和更高版本允许将逻辑路由器路由的逻辑接口 (LIF) 连接到 VLAN 桥接的 VXLAN。
- 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。
- 如果逻辑路由器已连接到跨多个 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。这是为了确保逻辑路由器实例与主机中的逻辑交换机 dvPortgroup 正确对齐。
- 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。
- 如果配置了 VXLAN，则必须将逻辑路由器接口连接到配置了 VXLAN 的 vSphere Distributed Switch 上的分布式端口组。请不要将逻辑路由器接口连接到其他 vSphere Distributed Switch 上的端口组。

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《管理接口指南：DLR 控制虚拟机 - NSX》，网址为 <http://kb.vmware.com/kb/2122060>。

## 前提条件

- 必须已为您分配**企业管理员**或 **NSX 管理员**角色。
- 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。

- 在创建或更改逻辑路由器配置之前，请确保控制器群集已启动且可用。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。
- 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管理程序主机都可以在 **UDP 端口 6999** 上相互访问。要使基于逻辑路由器 **VLAN** 的 **ARP** 代理能够正常工作，需要在此端口上通信。
- 确定在何处部署逻辑路由器设备。
  - 目标主机必须属于与连接到新逻辑路由器接口的逻辑交换机相同的传输区域。
  - 如果在 **ECMP** 设置中使用 **ESG**，应避免将逻辑路由器设备放在与它的一个或多个上游 **ESG** 相同的主机上。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》。
- 确认已为 **NSX** 准备好安装逻辑路由器设备的主机群集。请参见 **NSX 安装指南** 中的“为 **NSX** 准备主机群集”。

## 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 单击添加 (**Add**) () 图标。
- 3 选择**逻辑 (分布式) 路由器 (Logical (Distributed) Router)**，然后键入设备的名称。

该名称会显示在 **vCenter** 清单中。请使用在单个租户内的所有逻辑路由器中均唯一的名称。

此外，还可以输入主机名。该名称会显示在 **CLI** 中。如果未输入主机名，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。

例如：

## Name and description

Install Type: ☐ Edge Services Gateway  
*Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.*

☒ Logical (Distributed) Router  
*Provides Distributed Routing and Bridging capabilities.*

Name: \*

Hostname:

Description:

Tenant:

☒ Deploy Edge Appliance  
*Deploys NSX Edge Appliance to support Firewall and Dynamic routing.*

☐ Enable High Availability  
*Enable HA, for enabling and configuring High Availability.*

## 4 （可选）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。

## 5 （可选）启用高可用性。

默认情况下，**启用高可用性 (Enable High Availability)**处于未选中状态。选中**启用高可用性 (Enable High Availability)**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。

## 6 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

## 7 （可选）启用 SSH。

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。您必须手动调整逻辑路由器防火墙配置，才能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。

## 8 （可选）启用 FIPS 模式并设置日志级别。

默认情况下，将禁用 FIPS 模式。选中**启用 FIPS 模式 (Enable FIPS mode)**复选框以启用 FIPS 模式。在启用 FIPS 模式时，与 NSX Edge 之间的任何安全通信将使用 FIPS 允许的加密算法或协议。

默认情况下，日志级别为紧急。

例如：

**Settings**

---

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 FIPS mode

Edge Control Level Logging  ▼

*Set the Edge Control Level Logging*

## 9 配置部署。

- ◆ 如果未选择**部署 Edge 设备 (Deploy Edge Appliance)**，则**添加 (Add)** (🟢) 图标为灰显状态。单击**下一步 (Next)**继续配置。
- ◆ 如果您选择了**部署 Edge 设备 (Deploy Edge Appliance)**，请输入逻辑路由器虚拟设备的设置。

例如：

**Add NSX Edge Appliance**

---

Specify placement parameters for the NSX Edge appliance.

Cluster/Resource Pool: \*  ▼

Datastore: \*  ▼

Host:  ▼

Folder:  ▼

## 10 配置接口。在逻辑路由器上，仅支持 IPv4 寻址。

### a 配置 HA 接口连接以及可选的 IP 地址。

如果您选择了**部署 Edge 设备 (Deploy Edge Appliance)**，则必须将 HA 接口连接到分布式端口组或逻辑交换机。如果您仅将该接口作为 HA 接口，请使用逻辑交换机。将从链路本地范围 169.254.0.0/16 中分配一个 /30 子网，用于为两个 NSX Edge 设备分别提供一个 IP 地址。

（可选）如果要使用该接口连接到 NSX Edge，您可以为 HA 接口指定一个额外的 IP 地址和前缀。

---

**注** 在 NSX 6.2 之前，HA 接口称为管理接口。对于任何与 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，但这不利于实现高可用性。对于 SSH 访问，您也可以使用逻辑路由器的协议地址，这是以后在配置动态路由时配置的。

在 NSX 6.2 和更高版本中，自动从路由重新分发中排除逻辑路由器的 HA 接口。

---

### b 配置此 NSX Edge 的接口。

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 Edge 服务网关或第三方路由器虚拟机。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      |
|        |               |                      |              |
|        |               |                      |              |

Back

Next

Finish

Cancel

## 11 配置默认网关。

例如：

The screenshot shows the 'New NSX Edge' configuration wizard. On the left, a progress bar indicates the current step is '5 Default gateway settings'. The main area is titled 'Default gateway settings' and contains the following fields:

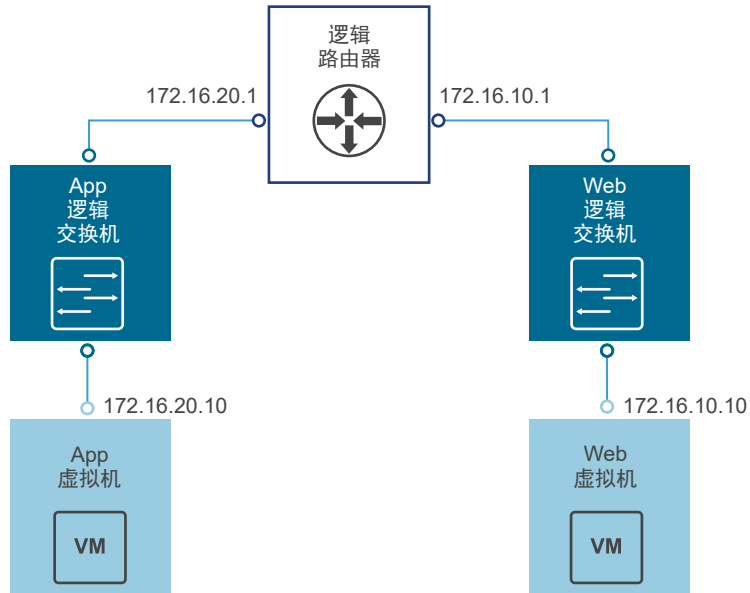
- ☒ Configure Default Gateway
- vNIC: \* to-ESG (dropdown menu)
- Gateway IP: \* 192.168.10.1 (text input field)
- MTU: 1500 (text input field)

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

**12** 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。

### 结果

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



使用 SSH 或控制台连接到 NSX Manager，并运行以下命令：

- 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。

```

nsx-mgr-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。此输出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，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@app-vm$ ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=64 time=2.605 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=64 time=1.490 ms
64 bytes from 172.16.10.10: icmp_req=3 ttl=64 time=2.422 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。与 ESXi 主机上不同，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。

- 列出连接到该控制器的所有逻辑路由器。

```
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 | vxlan | 0x1389 | 172.16.10.1/24  |
| 13880000000a | vxlan | 0x1388 | 172.16.20.1/24  |
| 138800000002 | vxlan | 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 6.0 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 是指 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

如果在群集上禁用了 vSphere HA，在安装 NSX Edge 设备时，NSX 将在主机上启用自动虚拟机启动/关闭。如果以后将设备虚拟机迁移到群集中的其他主机，新主机可能不会启用自动虚拟机启动/关闭。因此，在已禁用 vSphere HA 的群集上安装 NSX Edge 设备时，VMware 建议您应检查群集中的所有主机以确保启用了自动虚拟机启动/关闭。请参见《vSphere 虚拟机管理》中的“编辑虚拟机启动和关闭设置”。

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。

# 添加 Edge 服务网关

# 18

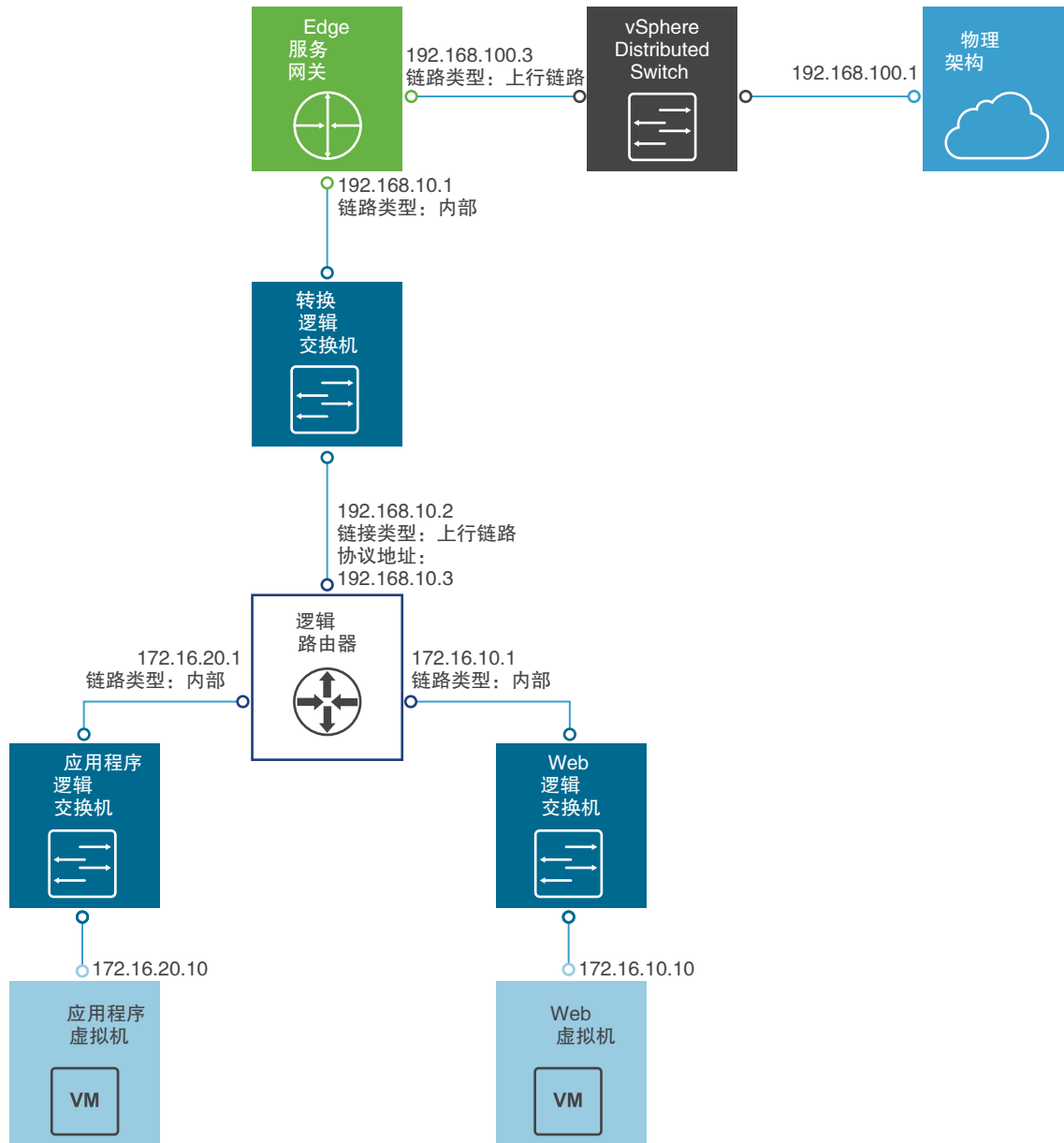
您可以在一个数据中心中安装多个 **NSX Edge** 服务网关虚拟设备。每个 **NSX Edge** 虚拟设备总共可以有十个上行链路和内部网络接口。内部接口连接至安全的端口组，并充当端口组中所有受保护虚拟机的网关。分配给内部接口的子网可以是公开路由的 IP 地址空间，或者是采用 NAT/路由的 **RFC 1918** 专用空间。会对接口之间的流量实施防火墙规则和其他 **NSX Edge** 服务。

**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。



可以为负载均衡、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 [NSX 的系统要求](#)。
- 确认为 NSX 准备了将在其中安装 NSX Edge 设备的主机群集。请参见 NSX 安装指南中的“为 NSX 准备主机群集”。

#### 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 is a sidebar with 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. Navigation buttons 'Back', 'Next', 'Finish', and 'Cancel' are at the bottom right.

## 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、自动规则生成和 FIPS 模式，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（包括负载均衡和 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，将禁用 FIPS 模式。

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, 6 Firewall and HA, and 7 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 FIPS mode
- ☒ Enable auto rule generation
- Enable auto rule generation, to automatically generate service rules to allow flow of control traffic.
- Edge Control Level Logging:
- 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 适合具有负载均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 [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。

如果以后使用 API 调用更改 MAC 地址，则在更改 MAC 地址后必须重新部署 Edge。

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：

**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

**Default gateway settings**

☒ Configure Default Gateway

vNIC: \* uplink

Gateway IP: \* 192.168.100.2

MTU: 1500

Back Next Finish Cancel

## 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** 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

## 结果

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

如果在群集上禁用了 vSphere HA，在安装 NSX Edge 设备时，NSX 将在主机上启用自动虚拟机启动/关闭。如果以后将设备虚拟机迁移到群集中的其他主机，新主机可能不会启用自动虚拟机启动/关闭。因此，在已禁用 vSphere HA 的群集上安装 NSX Edge 设备时，VMware 建议您应检查群集中的所有主机以确保启用了自动虚拟机启动/关闭。请参见《vSphere 虚拟机管理》中的“编辑虚拟机启动和关闭设置”。

现在，便可配置路由以允许外部设备到虚拟机的连接。

# 在逻辑（分布式）路由器上配置 OSPF

# 19

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 支持十进制数字形式的区域 ID。有效值为 0 – 4294967295。
- 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。

### 重要事项

- 如果为 NSX Edge 配置了 HA，启用了 OSPF 正常重新启动并使用 MD5 进行身份验证，则 OSPF 无法正常重新启动。只有在 OSPF 帮助程序节点上的宽限期到期后，才会形成邻接。
- 在启用 FIPS 模式时，无法配置 MD5 身份验证。
- NSX for vSphere 始终使用密钥 ID 值 1。对于任何设备，如果不受与 Edge 服务网关或逻辑分布式路由器建立对等关系的 NSX for vSphere 管理，则在使用 MD5 身份验证时，必须配置为使用密钥 ID 值 1。否则，将无法建立 OSPF 会话。

## 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。

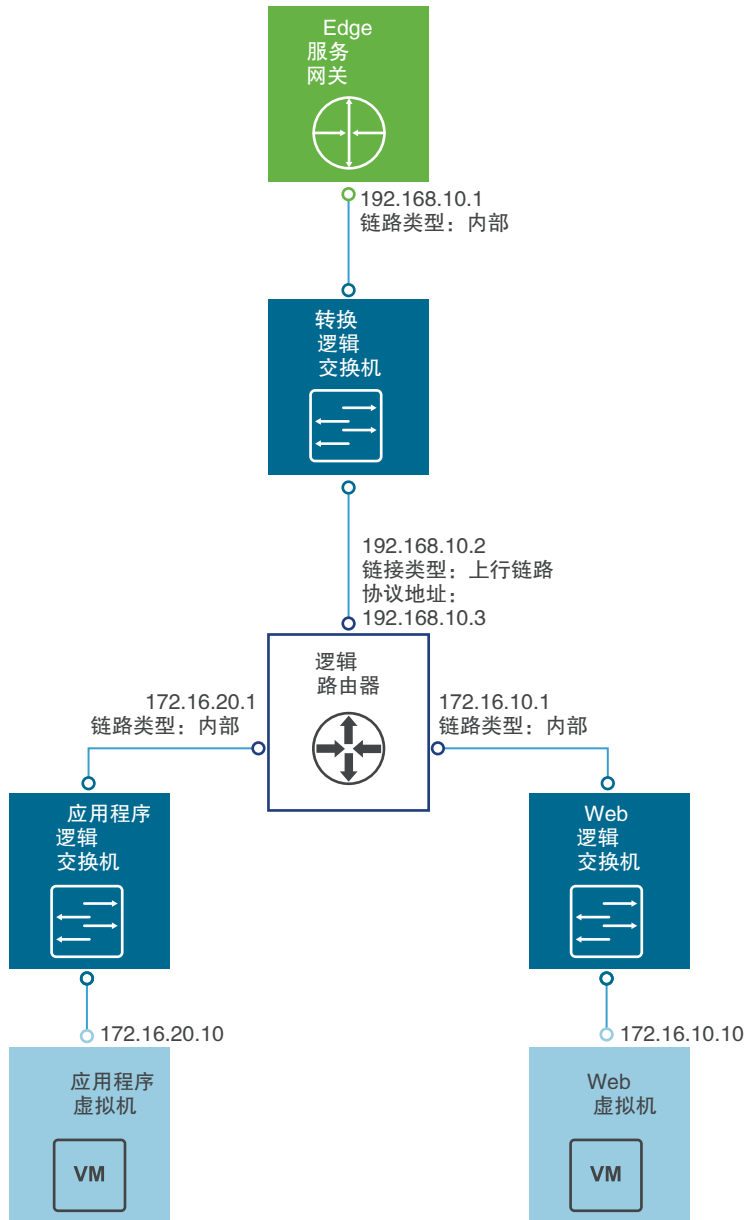
## 10 单击**发布更改 (Publish Changes)**。



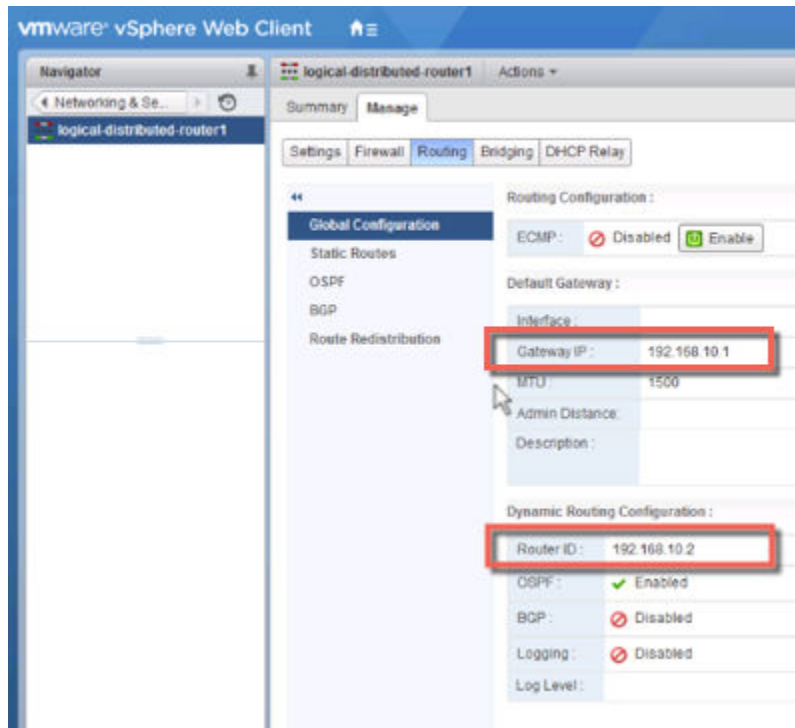
## 示例：在逻辑（分布式）路由器上配置的 OSPF

使用 OSPF 的一个简单 NSX for vSphere 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。

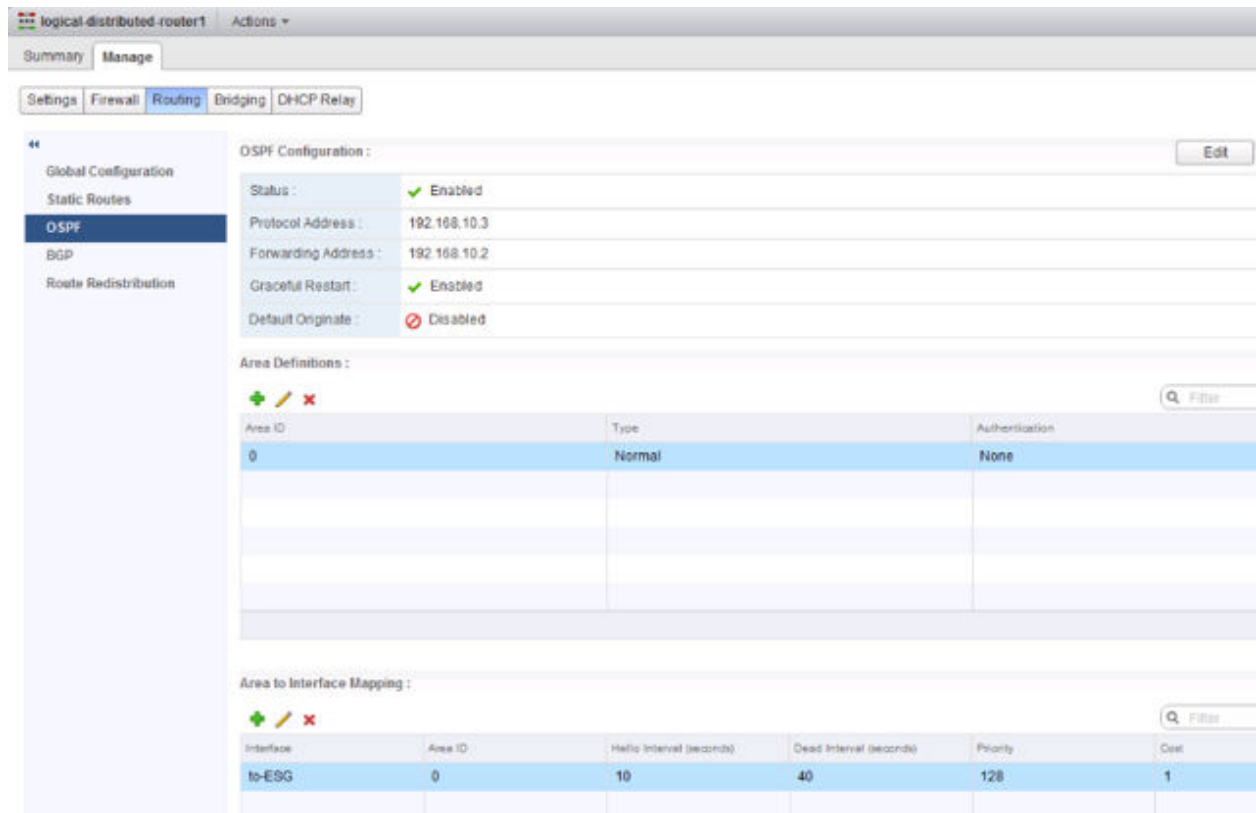
图 19-1. NSX for vSphere 拓扑



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)。



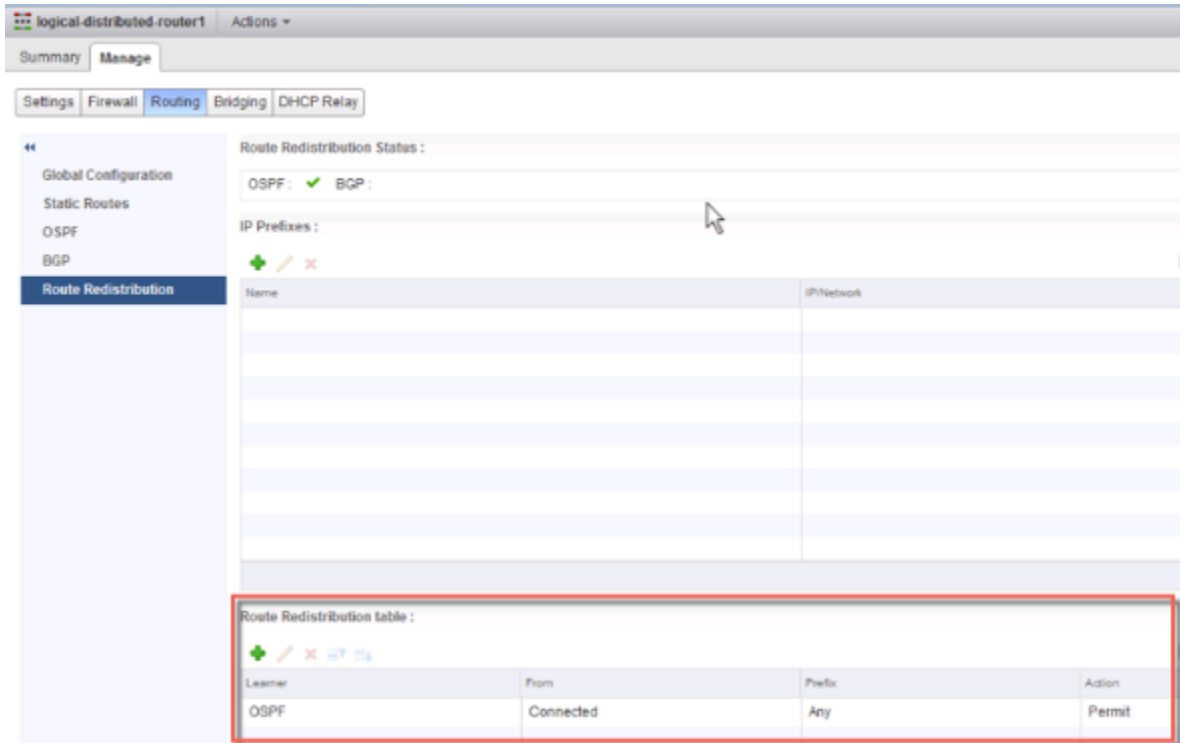
逻辑路由器配置使用 192.168.10.2 作为其转发地址。协议地址可以是位于同一个子网中并且未在其他位置使用的任何 IP 地址。在本例中，配置了 192.168.10.3。配置的区域 ID 为 0，上行链路接口（面向 ESG 的接口）映射到该区域。



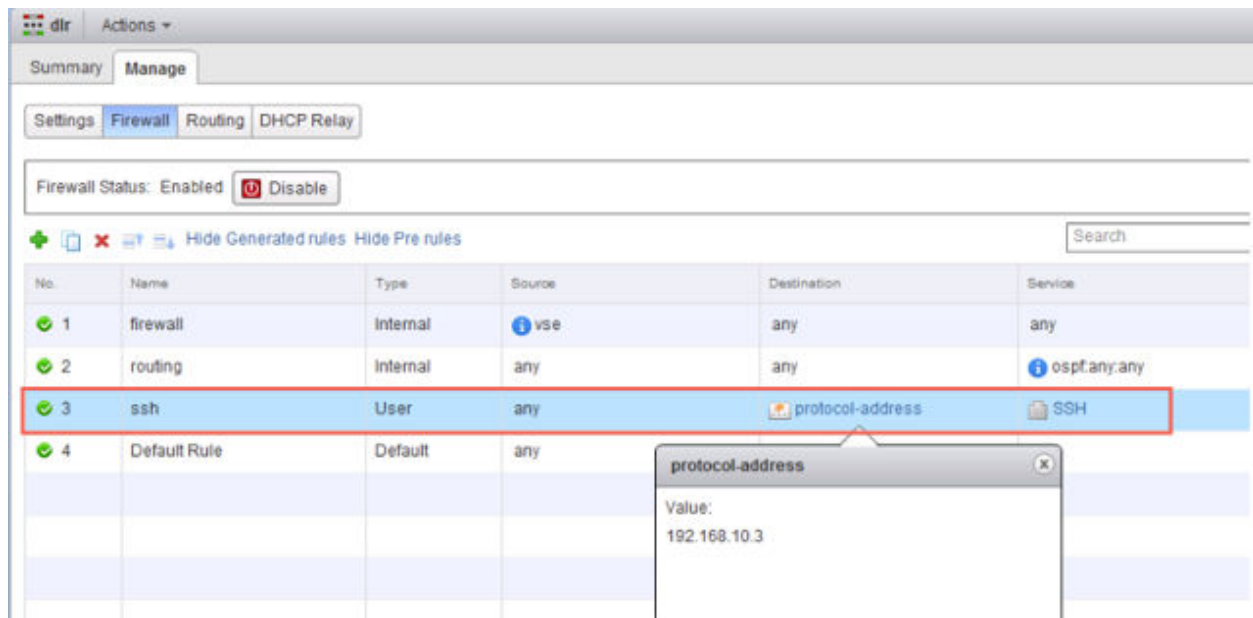
## 后续步骤

确保路由重新分发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

# 20

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) 如果在“类型”中选择 **NSSA**，则将显示 **NSSA 转换器角色 (NSSA Translator Role)** 字段。选中**始终 (Always)**复选框以将 7 类 LSA 转换为 5 类 LSA。所有 7 类 LSA 将由 NSSA 转换为 5 类 LSA。
- 8 (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。

#### 注

- 在启用 FIPS 模式时，无法配置 **MD5** 身份验证。
- NSX 始终使用密钥 ID 值 1。在使用 MD5 身份验证时，必须将 NSX Edge 或逻辑分布式路由器的任何非 NSX 设备对等项配置为使用密钥 ID 值 1，否则，无法建立 OSPF 会话。

- 9 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。
- 10 (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。

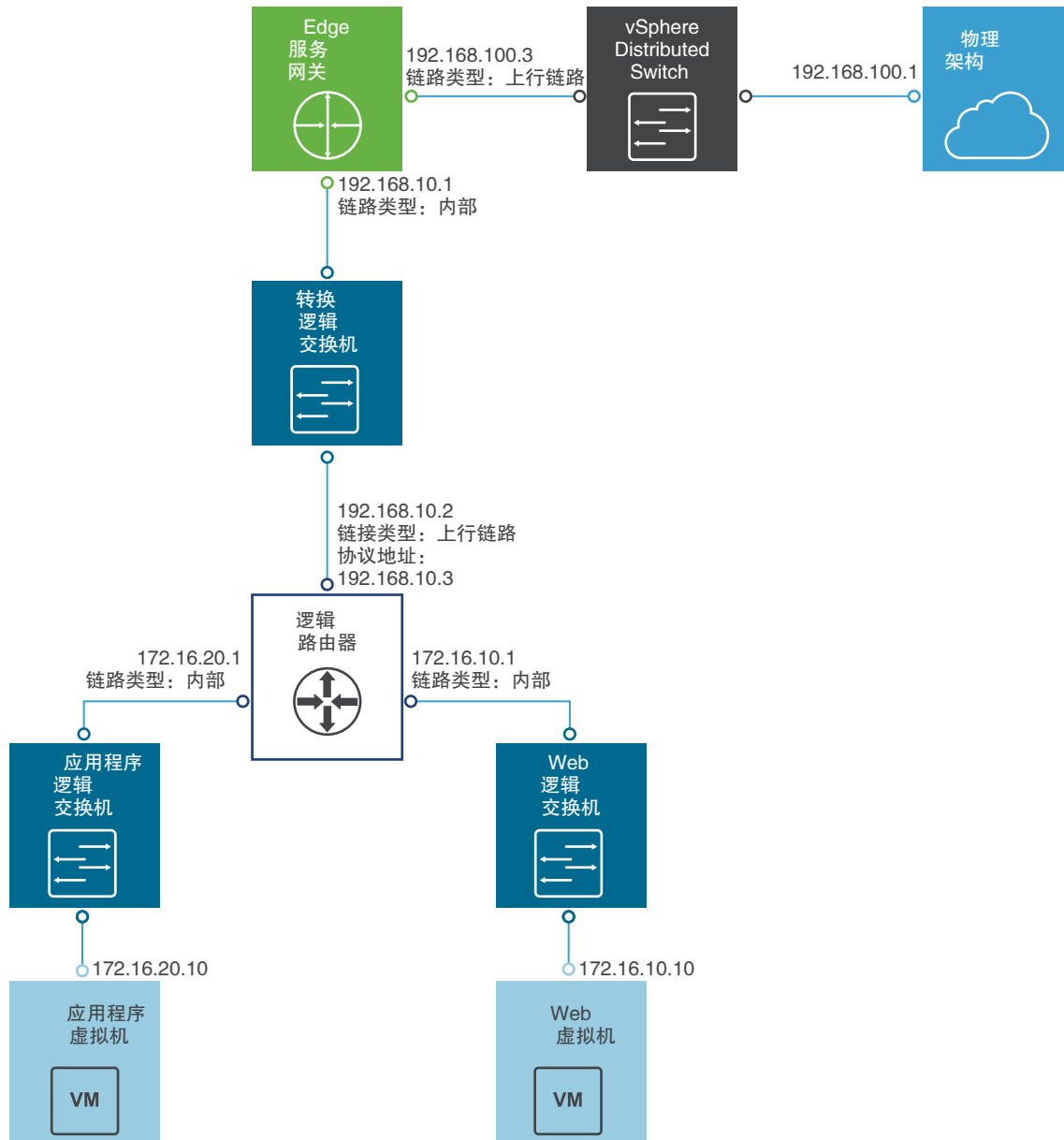
- 11 单击**发布更改 (Publish Changes)**。
- 12 确保路由重新分发和防火墙配置允许播发正确的路由。

## 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。

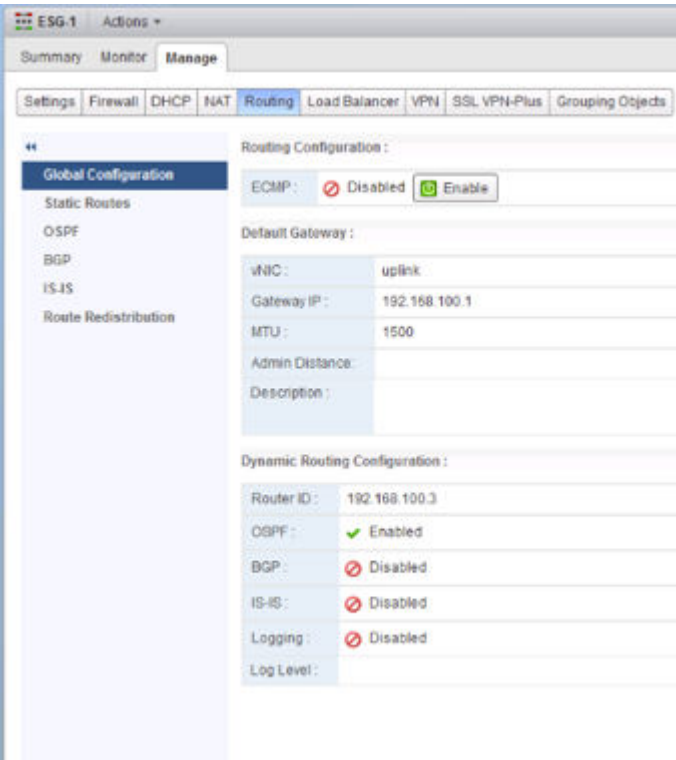
通过 vSphere Distributed Switch 上的上行链路端口组，ESG 可以通过桥、物理路由器（或者如下图所示）连接到外部环境。

图 20-1. NSX 拓扑

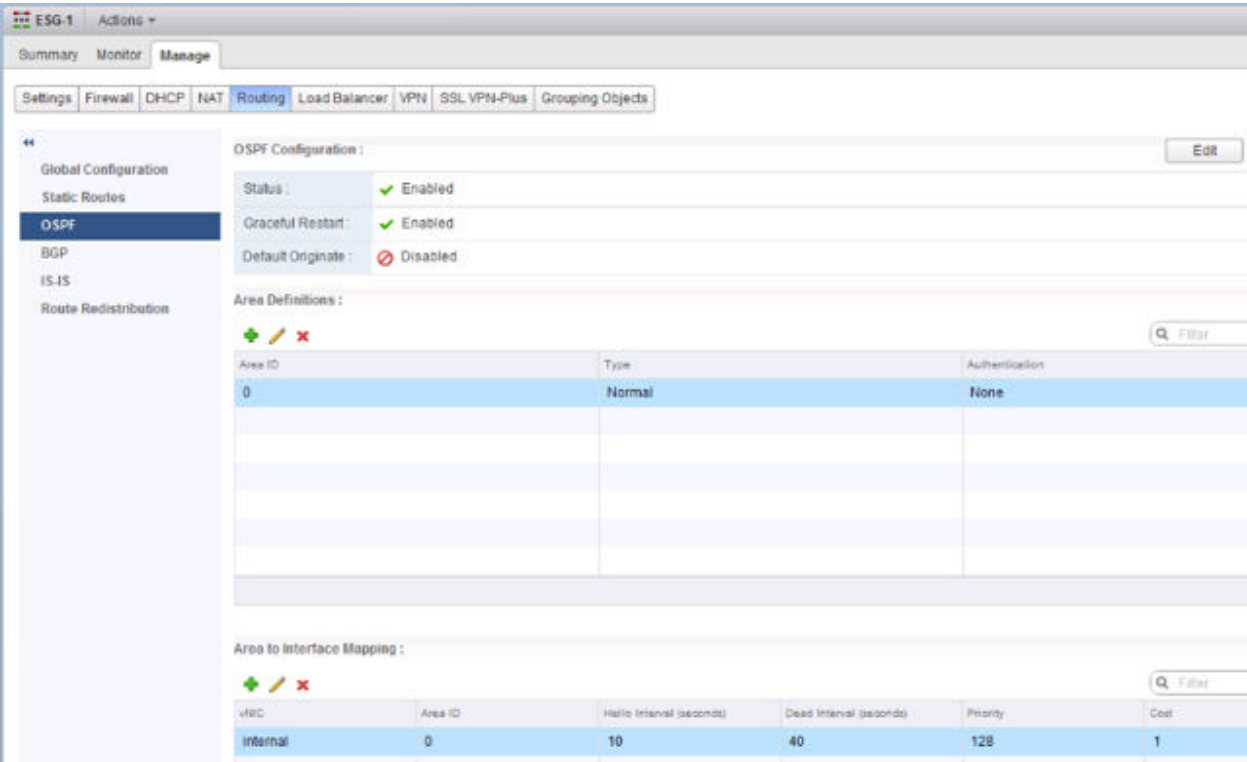


在下面的屏幕中，ESG 的默认网关为连接其外部对等方的 ESG 上行链路接口。

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。



连接的路由重新分发到 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: O - 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,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 5

S 0.0.0.0/0 [0/0] via 192.168.100.1
O E2 172.16.10.0/24 [110/1] via 192.168.10.2
O 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
```

# 在主机群集上安装 Guest Introspection

# 21

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。活动监控和多个第三方安全解决方案需要 Guest Introspection。

---

**注** 无法使用 vMotion/SvMotion 迁移服务虚拟机 (SVM)。SVM 必须位于所部署的主机上才能正常运行。

---

## 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。请参阅 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 并正在运行。
- 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”。


---

**小心** Guest Introspection 使用 169.254.x.x 子网在内部为 GI 服务分配 IP 地址。如果将 IP 地址 169.254.1.1 分配给 ESXi 主机的任何 VMkernel 接口，则 Guest Introspection 安装将失败。GI 服务使用此 IP 地址进行内部通信。

---

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 (Agent VMs)**，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   | 目标                                                                            |
|------|-------------------------------------------------------------------------------|
| 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)**。

# 卸载 NSX 组件

# 22

本章将详细介绍从 vCenter 清单中卸载 NSX 组件所需的步骤。

**注** 不要直接从 vCenter 中移除 NSX 部署的任何设备（如控制器和 Edge）。请务必使用 vSphere Web Client 的**网络和安全 (Networking & Security)**选项卡管理和移除 NSX 设备。

本章讨论了以下主题：

- 卸载 Guest Introspection 模块
- 卸载 NSX Edge 服务网关或分布式逻辑路由器
- 卸载逻辑交换机
- 从主机群集中卸载 NSX
- 安全移除 NSX 安装

## 卸载 Guest Introspection 模块

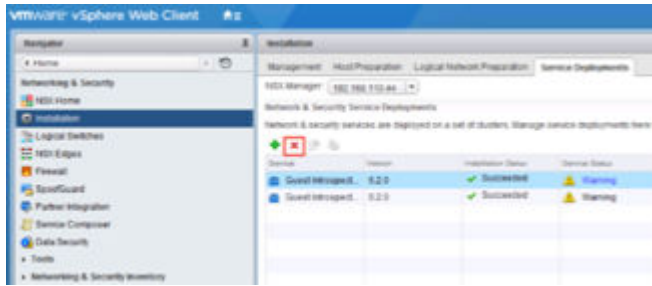
卸载 Guest Introspection 会从群集上的主机中移除 VIB，并从群集上的每台主机中移除服务虚拟机。身份防火墙、端点监控以及一些第三方安全解决方案需要使用 Guest Introspection。卸载 Guest Introspection 会产生多种影响。

**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。

NSX 群集中的虚拟机将不再受到保护。在卸载之前，您必须通过 vMotion 将虚拟机从群集中移出。

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 (Home > Networking & Security > Installation)**，然后选择**服务部署 (Service Deployments)**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。



## 卸载 NSX Edge 服务网关或分布式逻辑路由器

您可以使用 vSphere Web Client 卸载 NSX Edge。

### 前提条件

您必须已获得企业管理员或 NSX 管理员角色。

### 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 NSX Edge，然后单击**删除 (Delete) (✖)** 图标。

## 卸载逻辑交换机

在卸载逻辑交换机之前，必须从该逻辑交换机中移除所有虚拟机。

### 前提条件

您必须已获得企业管理员或 NSX 管理员角色。

### 步骤

- 1 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)**。
- 2 从一个逻辑交换机中移除所有虚拟机。
  - a 选择一个逻辑交换机，然后单击“移除虚拟机”图标 (🗑️)。
  - b 将所有虚拟机从“可用对象”移到“选定对象”中，然后单击**确定 (OK)**。
- 3 选择逻辑交换机之后，请单击**删除 (Delete) (✖)** 图标。

## 从主机群集中卸载 NSX

您可以从群集的所有主机中卸载 NSX。

如果要从各个主机中（而非从整个群集中）移除 NSX，请参见第 12 章 [从准备 NSX 部署的群集中移除主机](#)。

### 前提条件

- 断开群集中虚拟机与逻辑交换机的连接。

### 步骤

- 1 从传输区域中移除群集。

转至**逻辑网络准备 > 传输区域 (Logical Network Preparation > Transport Zones)**，然后断开群集与传输区域的连接。

如果群集显示为灰色，并且您无法断开其与传输区域的连接，这可能是因为：1) 群集中的主机已断开连接或未打开电源，或者 2) 群集中可能包含一台或多台未附加到传输区域的虚拟机或设备。例如，如果主机位于管理群集中，并且上面安装了 NSX Controller，请先移除或移动这些控制器。

- 2 卸载 NSX VIB。在 vCenter Web Client 中，转至**网络和安全 > 安装 > 主机准备 (Networking & Security > Installation > Host Preparation)**。选择群集，然后单击**操作 (Actions)** (⚙️) 并选择**卸载 (Uninstall)**。

“安装状态”将显示**未就绪 (Not Ready)**。如果单击**未就绪 (Not Ready)**，对话框将显示以下消息：必须将主机置于维护模式才能完成代理 VIB 安装 (Host must be put into maintenance mode to complete agent VIB installation)。

- 3 选择群集并单击**解决 (Resolve)**操作以完成卸载。

- 如果主机具有 NSX 6.2.x 或更低版本或 ESXi 5.5 版，则需要重新引导才能完成卸载。如果群集启用了 DRS，DRS 将尝试以受控方式重新引导主机，这样可以让虚拟机继续运行。如果 DRS 因任何原因失败，**解决 (Resolve)**操作将暂停。在这种情况下，您可能需要先手动移除虚拟机，然后再重试**解决 (Resolve)**操作，或者手动重新引导主机。
- 对于具有 NSX 6.3.0 或更高版本以及 ESXi 6.0 或更高版本的主机，必须将主机置于维护模式才能完成卸载。如果群集启用了 DRS，DRS 将尝试以受控方式将主机置于维护模式，这样可以让虚拟机继续运行。如果 DRS 因任何原因失败，**解决 (Resolve)**操作将暂停。在这种情况下，您可能需要先手动移除虚拟机，然后再重试**解决 (Resolve)**操作，或者手动将主机置于维护模式。

---

**重要事项** 如果您手动将主机置于维护模式，则在将主机退出维护模式之前，必须验证主机 VIB 卸载是否已经完成。

- a 检查 vSphere Web Client 中的“近期任务”窗格。
- b 在**主机准备 (Host Preparation)**选项卡中，查看从中移除了主机的群集的安装状态，确定它是否具有绿色对勾。

如果安装状态为正在安装，则表明卸载仍在进行。

---

## 安全移除 NSX 安装

如果完全卸载 NSX，则会移除主机 VIB、NSX Manager、控制器、所有 VXLAN 配置、逻辑交换机、逻辑路由器、NSX 防火墙、Guest Introspection 和 vCenter NSX 插件。请务必对群集中的所有主机遵循以下步骤。VMware 建议您先从群集中卸载网络虚拟化组件，然后再从 vCenter Server 中移除 NSX 插件。

---

**注** 不要直接从 vCenter 中移除 NSX 部署的任何设备（如控制器和 Edge）。请务必使用 vSphere Web Client 的**网络和安全 (Networking & Security)**选项卡管理和移除 NSX 设备。

---

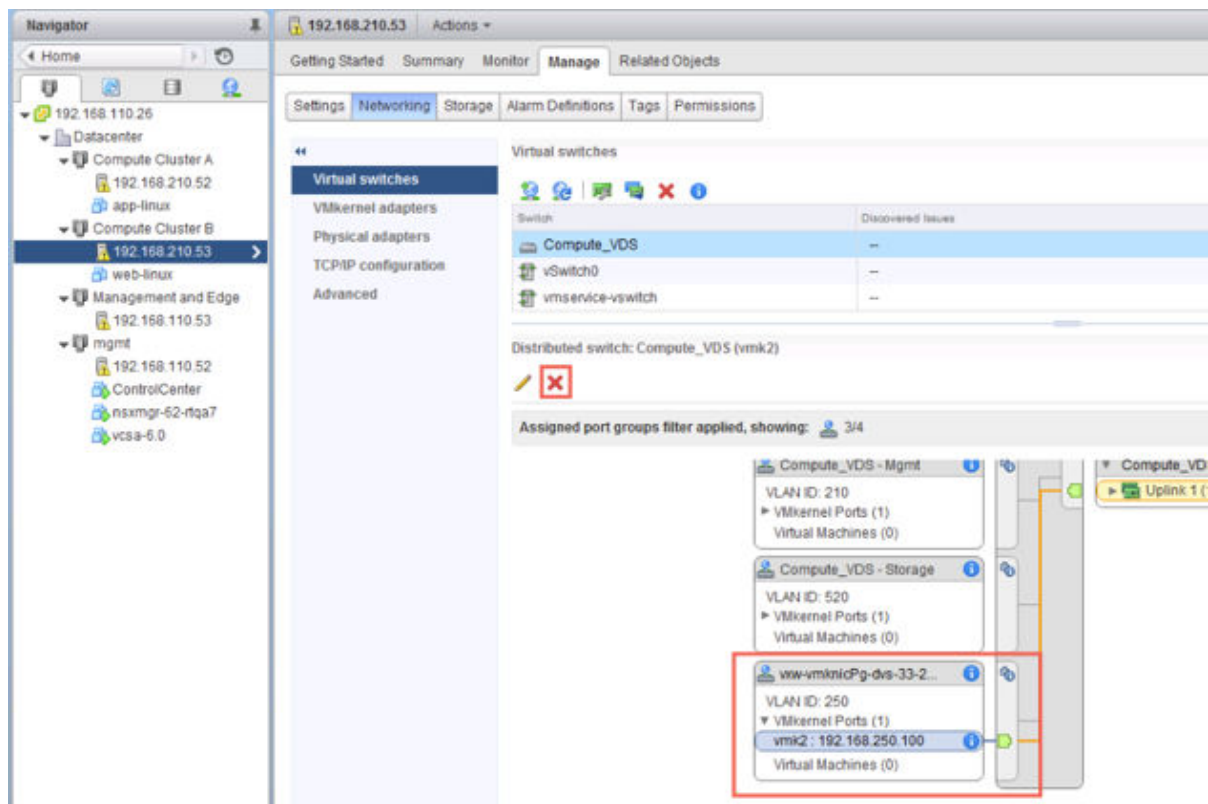
### 前提条件

- 必须已为您分配企业管理员或 NSX 管理员角色。
- 取消主机准备之前，先移除已注册的所有合作伙伴解决方案以及端点服务，以便能够正常移除群集中的服务虚拟机。
- 删除所有 NSX Edge。请参见[卸载 NSX Edge 服务网关或分布式逻辑路由器](#)。
- 将传输区域中的虚拟机与逻辑交换机分离并删除这些逻辑交换机。请参见[卸载逻辑交换机](#)。
- 从主机群集中卸载 NSX。请参见[从主机群集中卸载 NSX](#)。

### 步骤

- 1 删除传输区域。
- 2 从磁盘中删除 NSX Manager 设备和所有 NSX Controller 设备虚拟机。
- 3 移除所有遗留的 VTEP vmkernel 接口。

例如：

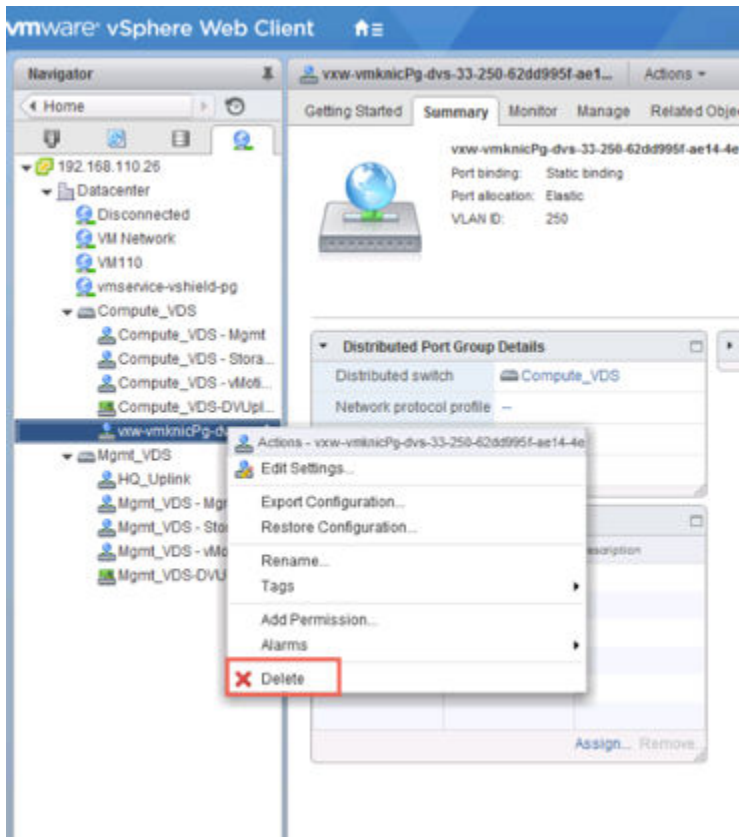


通常情况下，VTEP vmkernel 接口已随前面的卸载操作删除。

#### 4 移除遗留的所有用于 VTEP 的 dvPortgroup。

例如：

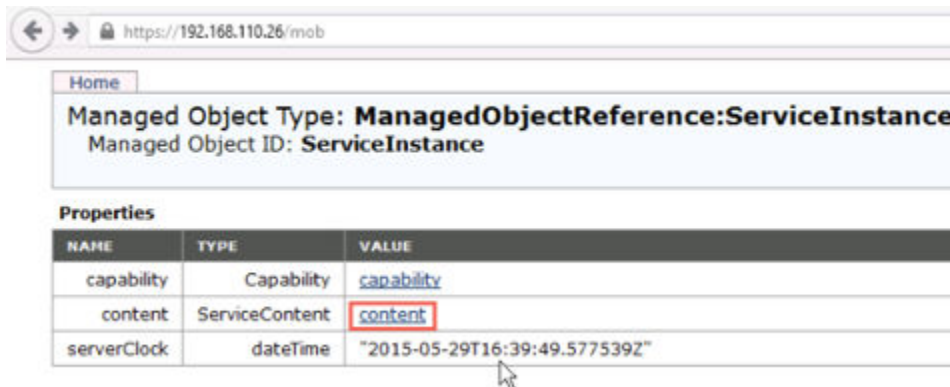




通常情况下，用于 VTEP 的 dvPortgroup 已随前面的卸载操作删除。

- 5 如果移除了 VTEP vmkernel 接口或 dvPortgroup，请重新引导主机。
- 6 对于要从中移除 NSX Manager 插件的 vCenter，通过 [https://your\\_vc\\_server/mob](https://your_vc_server/mob) 登录到 Managed Object Browser。
- 7 单击内容 (Content)。

例如：



8 单击 **ExtensionManager**。

← → https://192.168.110.26/mob/?moid=ServiceInstance&doPath=content

Home

**Data Object Type: ServiceContent**  
Parent Managed Object ID: **ServiceInstance**  
Property Path: **content**

**Properties**

| NAME                      | TYPE                                                   | VALUE                                     |
|---------------------------|--------------------------------------------------------|-------------------------------------------|
| about                     | AboutInfo                                              | <a href="#">about</a>                     |
| accountManager            | ManagedObjectReference:HostLocalAccountManager         | Unset                                     |
| alarmManager              | ManagedObjectReference:AlarmManager                    | <a href="#">AlarmManager</a>              |
| authorizationManager      | ManagedObjectReference:AuthorizationManager            | <a href="#">AuthorizationManager</a>      |
| certificateManager        | ManagedObjectReference:CertificateManager              | <a href="#">certificateManager</a>        |
| clusterProfileManager     | ManagedObjectReference:ClusterProfileManager           | <a href="#">ClusterProfileManager</a>     |
| complianceManager         | ManagedObjectReference:ProfileComplianceManager        | <a href="#">MoComplianceManager</a>       |
| customFieldsManager       | ManagedObjectReference:CustomFieldsManager             | <a href="#">CustomFieldsManager</a>       |
| customizationSpecManager  | ManagedObjectReference:CustomizationSpecManager        | <a href="#">CustomizationSpecManager</a>  |
| datastoreNamespaceManager | ManagedObjectReference:DatastoreNamespaceManager       | <a href="#">DatastoreNamespaceManager</a> |
| diagnosticManager         | ManagedObjectReference:DiagnosticManager               | <a href="#">DiagMgr</a>                   |
| dvSwitchManager           | ManagedObjectReference:DistributedVirtualSwitchManager | <a href="#">DVSwitchManager</a>           |
| eventManager              | ManagedObjectReference:EventManager                    | <a href="#">EventManager</a>              |
| extensionManager          | ManagedObjectReference:ExtensionManager                | <a href="#">ExtensionManager</a>          |
| fileManager               | ManagedObjectReference:FileManager                     | <a href="#">FileManager</a>               |
| guestOperationsManager    | ManagedObjectReference:GuestOperationsManager          | <a href="#">guestOperationsManager</a>    |
| hostProfileManager        | ManagedObjectReference:HostProfileManager              | <a href="#">HostProfileManager</a>        |

9 单击 **UnregisterExtension**。

**Methods**

| RETURN TYPE                            | NAME                                            |
|----------------------------------------|-------------------------------------------------|
| Extension                              | <a href="#">FindExtension</a>                   |
| string                                 | <a href="#">GetPublicKey</a>                    |
| ExtensionManagerIpAllocationUsage[]    | <a href="#">QueryExtensionIpAllocationUsage</a> |
| ManagedObjectReference:ManagedEntity[] | <a href="#">QueryManagedBy</a>                  |
| void                                   | <a href="#">RegisterExtension</a>               |
| void                                   | <a href="#">SetExtensionCertificate</a>         |
| void                                   | <a href="#">SetPublicKey</a>                    |
| void                                   | <a href="#">UnregisterExtension</a>             |
| void                                   | <a href="#">UpdateExtension</a>                 |

- 10 输入字符串 `com.vmware.vShieldManager`，然后单击调用方法 (Invoke Method)。

Managed Object Type:  
**ManagedObjectReference:ExtensionManager**  
Managed Object ID: **ExtensionManager**  
Method: **UnregisterExtension**

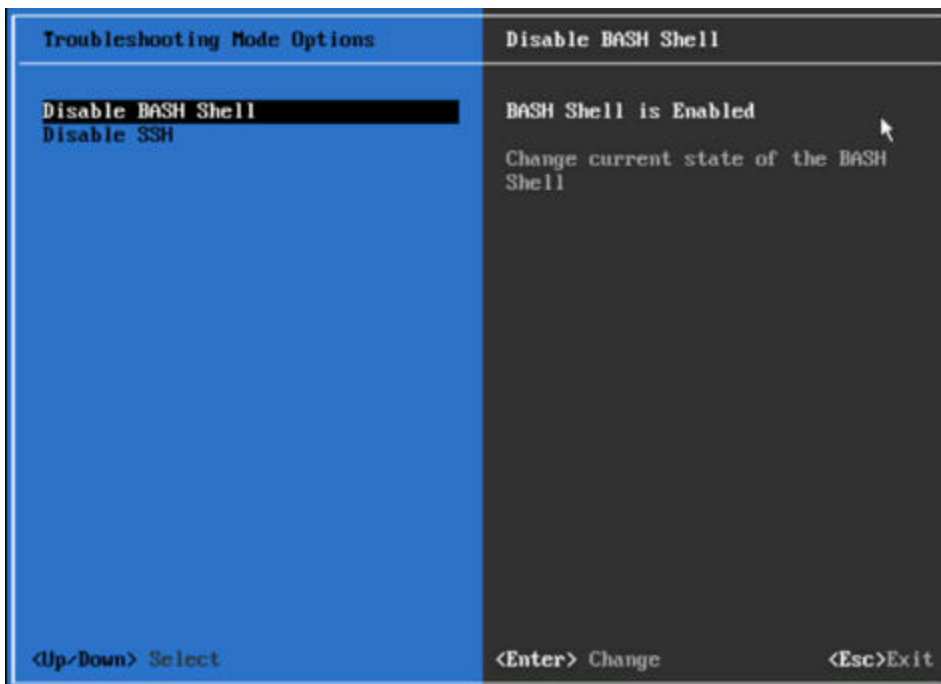
**void UnregisterExtension**

Parameters

| NAME                           | TYPE   | VALUE                                  |
|--------------------------------|--------|----------------------------------------|
| <b>extensionKey (required)</b> | string | <code>com.vmware.vShieldManager</code> |

[Invoke Method](#)

- 11 如果您正在运行 vSphere 6 vCenter Appliance，请启动控制台并在故障排除模式选项 (Troubleshooting Mode Options) 下启用 BASH shell。



另一种启用 BASH shell 的方法是作为 root 用户身份登录，并运行 `shell.set --enabled true` 命令。

- 12 删除 NSX 的 vSphere Web Client 目录，然后重新启动 Web Client 服务。

NSX 的 vSphere Web Client 目录名为 `com.vmware.vShieldManager.**`，其位置如下：

- 适用于 Windows 的 VMware vCenter Server - `C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity\`
- VMware vCenter Server Appliance - `/etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity/`

重新启动 vCenter Server Appliance:

- 在 vCenter Server Appliance 6.0 中, 以 root 用户身份登录到 vCenter Server shell, 然后运行以下命令:

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

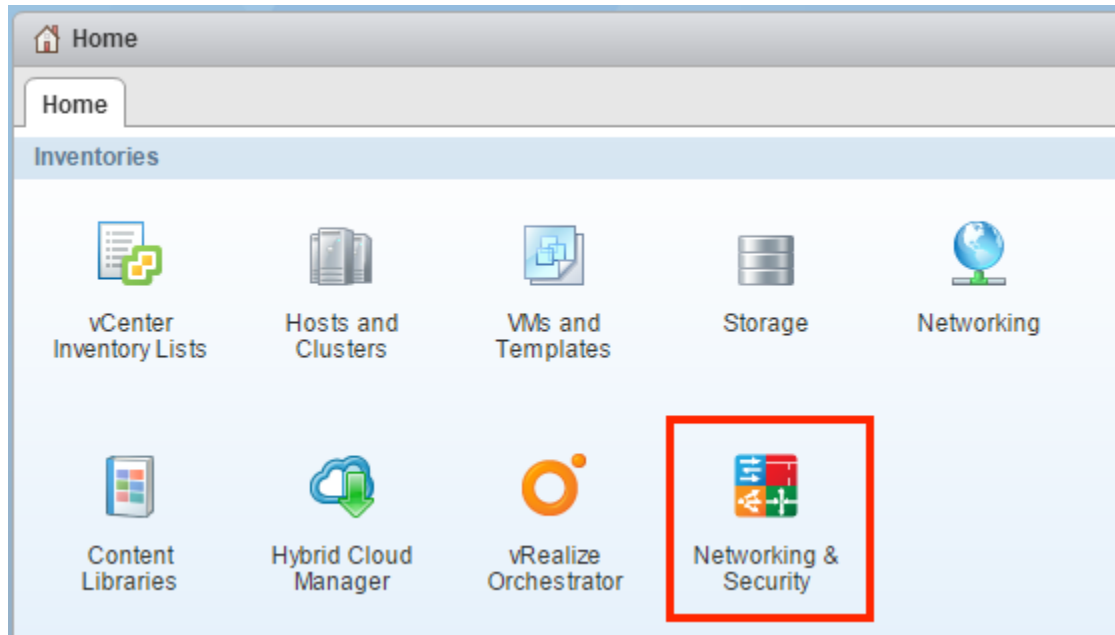
- 在 Windows 上的 vCenter Server 6.0 中, 您可以通过运行以下命令来执行该操作。

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

## 结果

NSX Manager 插件将从 vCenter 中移除。要确认, 请注销 vCenter, 然后重新登录。

NSX Manager 插件的 **网络和安全 (Networking & Security)** 图标不再显示在 vCenter Web Client 的主屏幕上。



转到 **系统管理 > 客户端插件 (Administration > Client Plug-Ins)**, 并确认插件列表中不包含 **NSX 用户界面插件 (NSX User Interface plugin)**。

