

# 跨 vCenter 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](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://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](http://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](http://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](http://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

<b>1</b>	<b>跨 vCenter 安装指南</b>	<b>5</b>
<b>2</b>	<b>NSX for vSphere 概述</b>	<b>6</b>
	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
<b>3</b>	<b>跨 vCenter 网络和安全概述</b>	<b>14</b>
	跨 vCenter NSX 的优点	14
	跨 vCenter NSX 的工作方式	15
	跨 vCenter NSX 中支持的 NSX Services 列表	16
	通用控制器群集	17
	通用传输区域	17
	通用逻辑交换机	18
	通用逻辑（分布式）路由器	18
	通用防火墙规则	18
	通用网络和安全对象	19
	跨 vCenter NSX 拓扑	19
	多站点和单站点跨 vCenter NSX	19
	本地输出	21
	修改 NSX Manager 角色	22
<b>4</b>	<b>安装准备工作</b>	<b>24</b>
	NSX 的系统要求	24
	NSX for vSphere 所需的端口和协议	26
	NSX 和 vSphere Distributed Switch	28
	示例：使用 vSphere Distributed Switch	30
	NSX 安装工作流程和示例拓扑	37
	跨 vCenter NSX 和增强型链接模式	38
<b>5</b>	<b>针对主/辅助 NSX Manager 的任务</b>	<b>40</b>
	安装 NSX Manager 虚拟设备	40
	配置 Single Sign On	44

- 在 NSX Manager 中注册 vCenter Server 46
- 为 NSX Manager 配置 syslog 服务器 47
- 安装和分配 NSX for vSphere 许可证 48
- 从防火墙保护中排除虚拟机 50

## 6 配置主 NSX Manager 51

- 在主 NSX Manager 上部署 NSX Controller 51
- 准备主 NSX Manager 上的主机 54
- 从主 NSX Manager 配置 VXLAN 58
- 为主 NSX Manager 分配分段 ID 池和多播地址 61
- 将主要角色分配给 NSX Manager 62
- 在主 NSX Manager 上分配通用分段 ID 池和通用多播地址 63
- 在主 NSX Manager 上添加通用传输区域 65
- 在主 NSX Manager 上添加通用逻辑交换机 66
- 将虚拟机连接到逻辑交换机 68
- 在主 NSX Manager 上添加通用逻辑（分布式）路由器 68

## 7 配置辅助 NSX Manager 79

- 添加辅助 NSX Manager 79
- 准备辅助 NSX Manager 上的主机 81
- 从辅助 NSX Manager 配置 VXLAN 82
- 为辅助 NSX Manager 分配分段 ID 池和多播地址 84
- 向通用传输区域添加群集 84

## 8 配置主 NSX Manager 和辅助 NSX Manager 之后 86

## 9 卸载 NSX 组件 87

- 从准备 NSX 部署的群集中移除主机 87
- 卸载 NSX Edge 服务网关或分布式逻辑路由器 88
- 卸载逻辑交换机 88
- 从主机群集中卸载 NSX 89
- 安全移除 NSX 安装 90

# 跨 vCenter 安装指南

# 1

本手册介绍了如何在跨 vCenter NSX 环境中安装 VMware NSX<sup>®</sup> for vSphere<sup>®</sup>。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

本手册适用于要在跨 vCenter NSX 环境中安装 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

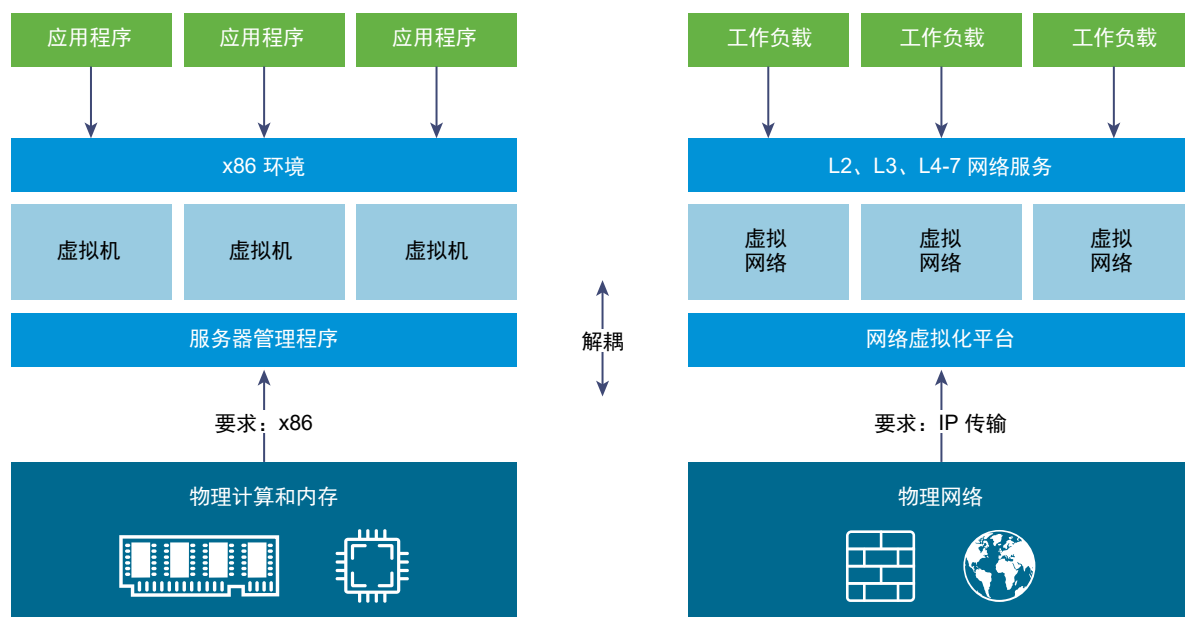
VMware 技术出版物提供了一个术语表，其中包含一些您可能不熟悉的术语。有关 VMware 技术文档中使用的术语的定义，请访问 <http://www.vmware.com/support/pubs>。

# NSX for vSphere 概述

## 2

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。

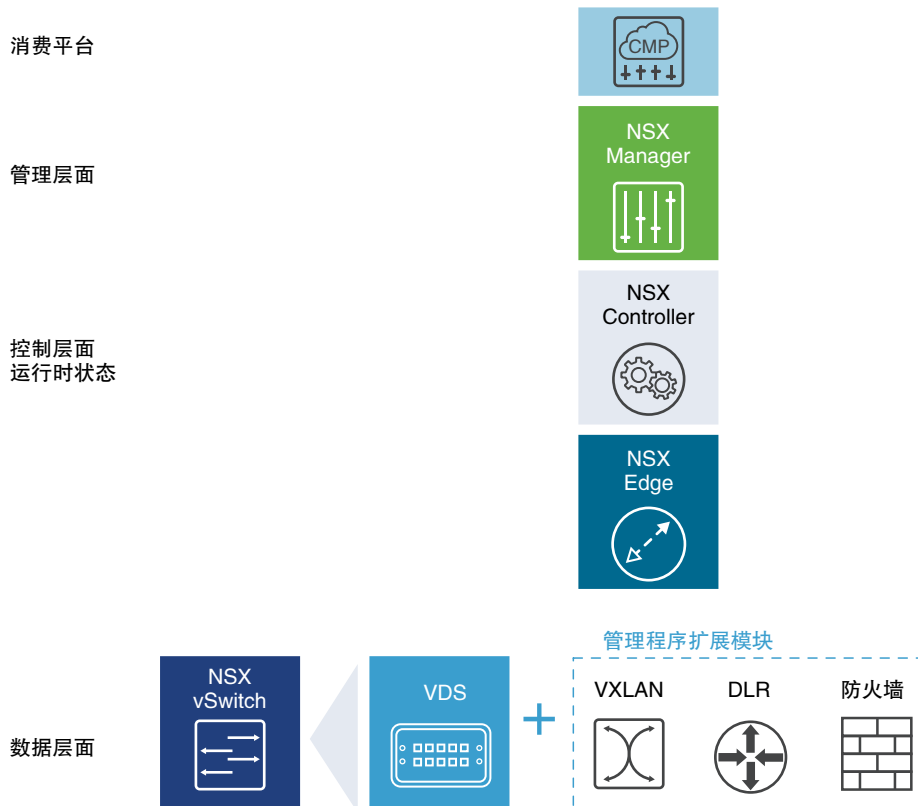
可通过 vSphere Web Client、命令行界面 (Command-Line Interface, CLI) 和 REST API 配置 NSX for vSphere。

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

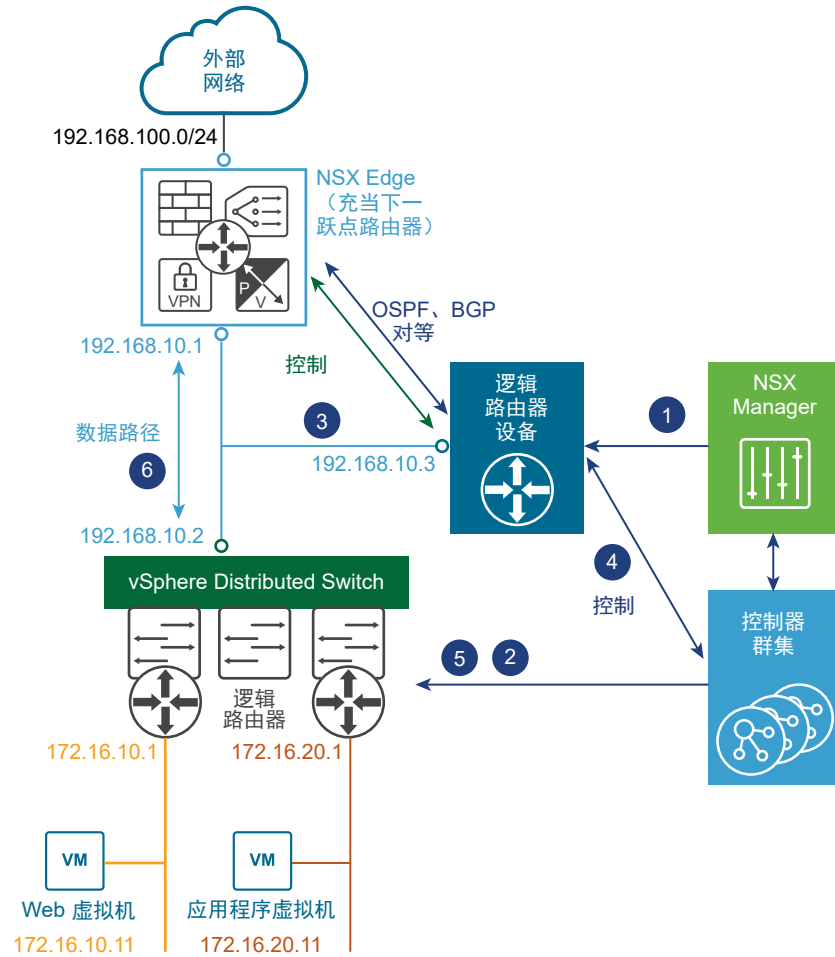
DLR 提供东西向分布式路由，可实现租户 IP 地址空间和数据路径隔离。位于不同子网中同一台主机上的虚拟机或工作负载可以彼此通信，而无需遍历传统的路由接口。

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 2-1. 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。

# 跨 vCenter 网络和安全概述

# 3

NSX 6.2 和更高版本允许从单个主 NSX Manager 中管理多个 vCenter NSX 环境。

本章讨论了以下主题：

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

## 跨 vCenter NSX 的优点

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

需要多个 vCenter Server 系统的原因可能有许多种，例如：

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

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

跨 vCenter NSX 包含以下功能：

- 增加了 NSX 逻辑网络的跨度。同一逻辑网络在整个 vCenter NSX 环境中可用，因此，位于任何 vCenter Server 系统上的任何群集中的虚拟机都可以连接到同一逻辑网络。
- 集中式安全策略管理。防火墙规则可从一个中央位置进行管理，并且应用到虚拟机，不受位置和 vCenter Server 系统影响。
- vSphere 6 中支持新的移动性边界，包括跨 vCenter 和跨多个逻辑交换机的远距离 vMotion。
- 增强了对多站点环境的支持，从城域距离到 150 毫秒 RTT。这包括主动-主动数据中心和主动-被动数据中心。

跨 vCenter NSX 环境具有许多优点：

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

---

**注** vSphere 6.0 和更高版本支持 跨 vCenter NSX 功能。

---

## 跨 vCenter NSX 的工作方式

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

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

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

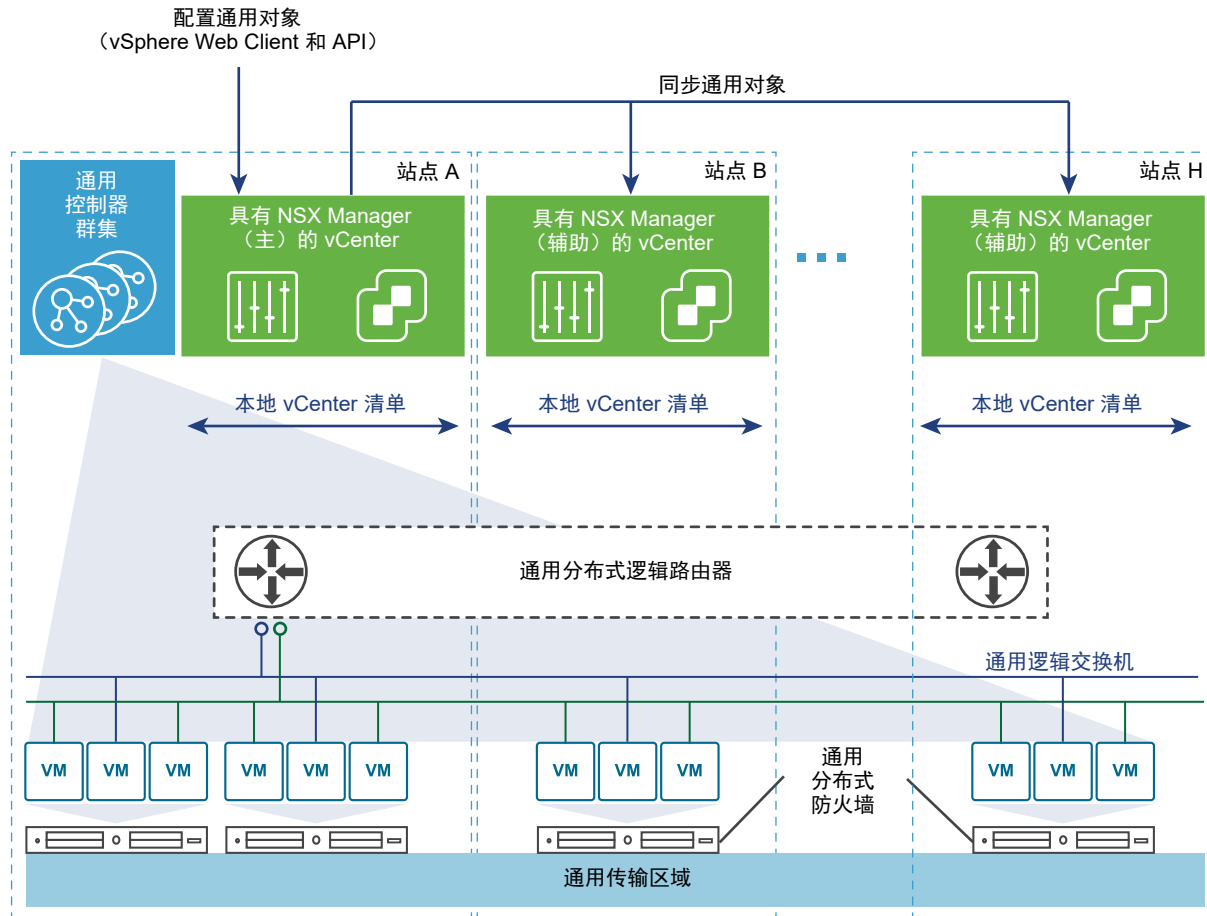
在主和辅助 NSX Manager 中，可以创建特定 vCenter NSX 环境的本地对象，如逻辑交换机和逻辑（分布式）路由器。这些对象仅存在于创建它们的 vCenter NSX 环境中。这些对象在跨 vCenter NSX 环境中的其他 NSX Manager 中将不可见。

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

---

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

---



## 跨 vCenter NSX 中支持的 NSX Services 列表

NSX Services 的子集适用于跨 vCenter NSX 中的通用同步。对于不适用于通用同步的服务，可将其配置为在 NSX Manager 本地使用。

表 3-1. 跨 vCenter NSX 中 NSX Services 的支持列表

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



表 3-1. 跨 vCenter NSX 中 NSX Services 的支持列表（续）

NSX Service	详细信息	是否支持跨 vCenter NSX 同步?
	排除列表	否
	SpoofGuard	否
	汇总流的流量监控	否
	网络服务插入	否
	Edge 防火墙	否
VPN		否
逻辑负载均衡器		否
其他 Edge 服务		否
服务编排		否
网络可扩展性		否
网络对象和安全对象	IP 地址组（IP 集）	是
	MAC 地址组（MAC 集）	是
	IP 池	否
	安全组	是，但成员资格配置不同于非通用安全组成员资格。有关详细信息，请参见 NSX 管理指南中的“创建安全组”。
	服务	是
	服务组	是
安全标记		是
硬件网关（也称为“硬件 VTEP”）		否。有关详细信息，请参见 NSX 管理指南中的“硬件网关示例配置”。

## 通用控制器群集

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

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

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

## 通用传输区域

在跨 vCenter NSX 环境中，只能存在一个通用传输区域。

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

## 通用逻辑交换机

通用逻辑交换机允许第 2 层网络跨多个站点。

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

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

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

## 通用逻辑（分布式）路由器

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

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

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

- 通用逻辑路由器
- 群集
- ESXi 主机

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

## 通用防火墙规则

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

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

在主 NSX Manager 中，您可以创建标记为用于通用同步的分布式防火墙规则区域。您可以创建多个通用 L2 规则区域和多个通用 L3 规则区域。通用区域始终列在主和辅助 NSX Manager 列表的顶部。这些区域及其规则都同步到环境中的所有辅助 NSX Manager。其他区域中的规则保持为相应的 NSX Manager 的本地规则。

以下分布式防火墙功能在跨 vCenter NSX 环境中不受支持：

- 排除列表
- SpoofGuard
- 汇总流的流量监控
- 网络服务插入
- Edge 防火墙

服务编排不支持通用同步，因此，您无法在通用区域中使用服务编排创建分布式防火墙规则。

## 通用网络和安全对象

可以创建自定义网络和安全对象，以在通用区域中的分布式防火墙规则中使用。

通用安全组 (Universal Security Group, USG) 可以包含以下内容：

- 通用 IP 集
- 通用 MAC 集
- 通用安全组
- 通用安全标记
- 动态条件

通用网络和安全对象只能在主 NSX Manager 上创建、删除和更新，但可以在辅助 NSX Manager 上读取。通用同步服务会立即同步 vCenter 上的所有通用对象，并根据需要使用强制同步。

通用安全组可用于两种类型的部署：多个活动的跨 vCenter NSX 环境和跨 vCenter NSX 活动/备用部署（其中一个站点在给定的时间内处于活动状态，而其他站点处于备用状态）。仅活动备用部署中的通用安全组可以具有基于虚拟机名称的动态成员资格以及基于通用安全标记的静态成员资格。一旦选择了某个通用安全组，便无法对它进行编辑以针对活动/备用部署场景功能启用或禁用它。成员资格只由包含的对象定义，您不能使用已排除的对象。

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

## 跨 vCenter NSX 拓扑

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

### 多站点和单站点跨 vCenter NSX

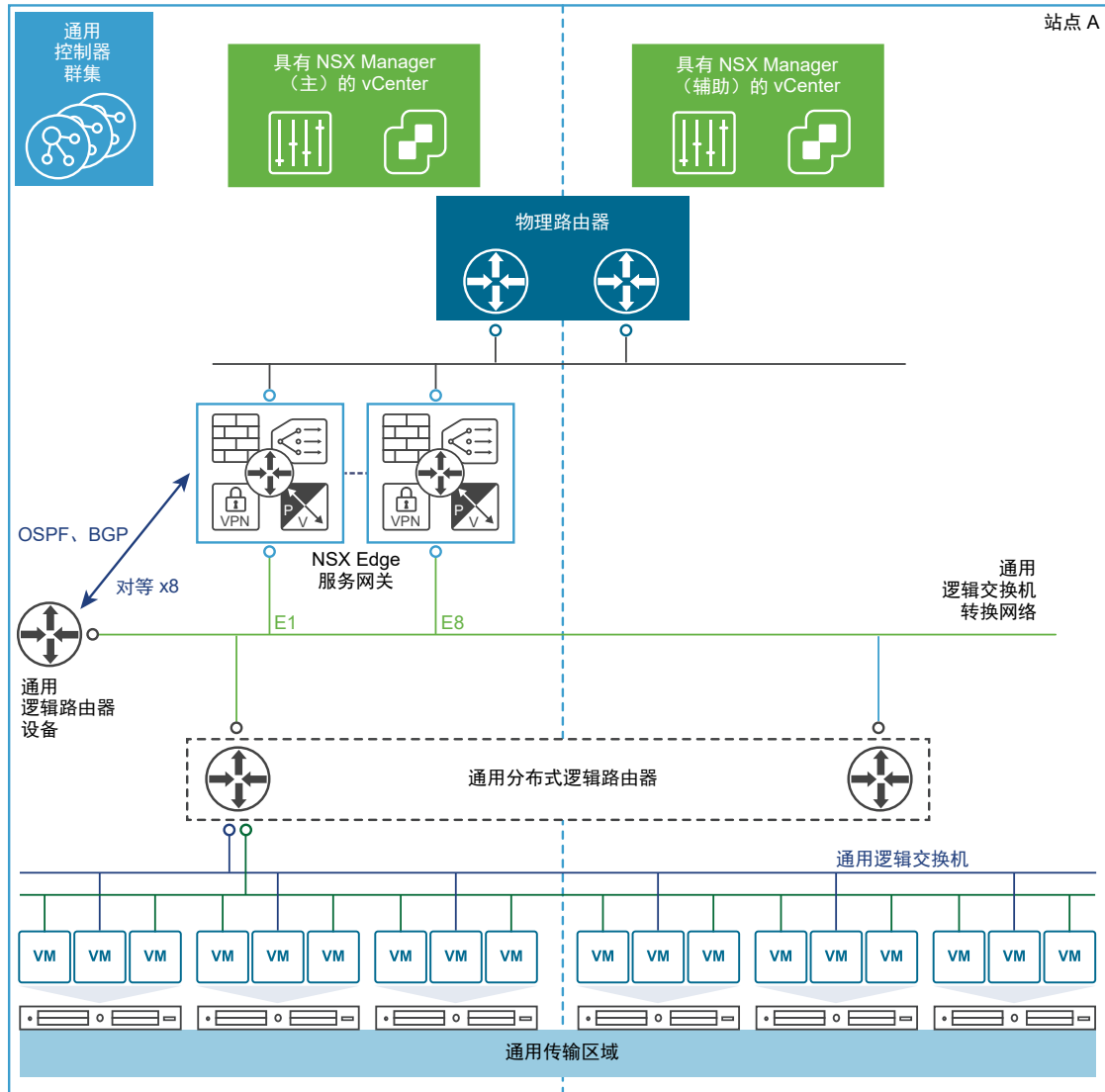
通过跨 vCenter NSX 环境，您可以在多个 vCenter NSX 设置中使用同一逻辑交换机和其他网络对象。多个 vCenter 可以位于同一站点，也可以位于不同的站点。

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

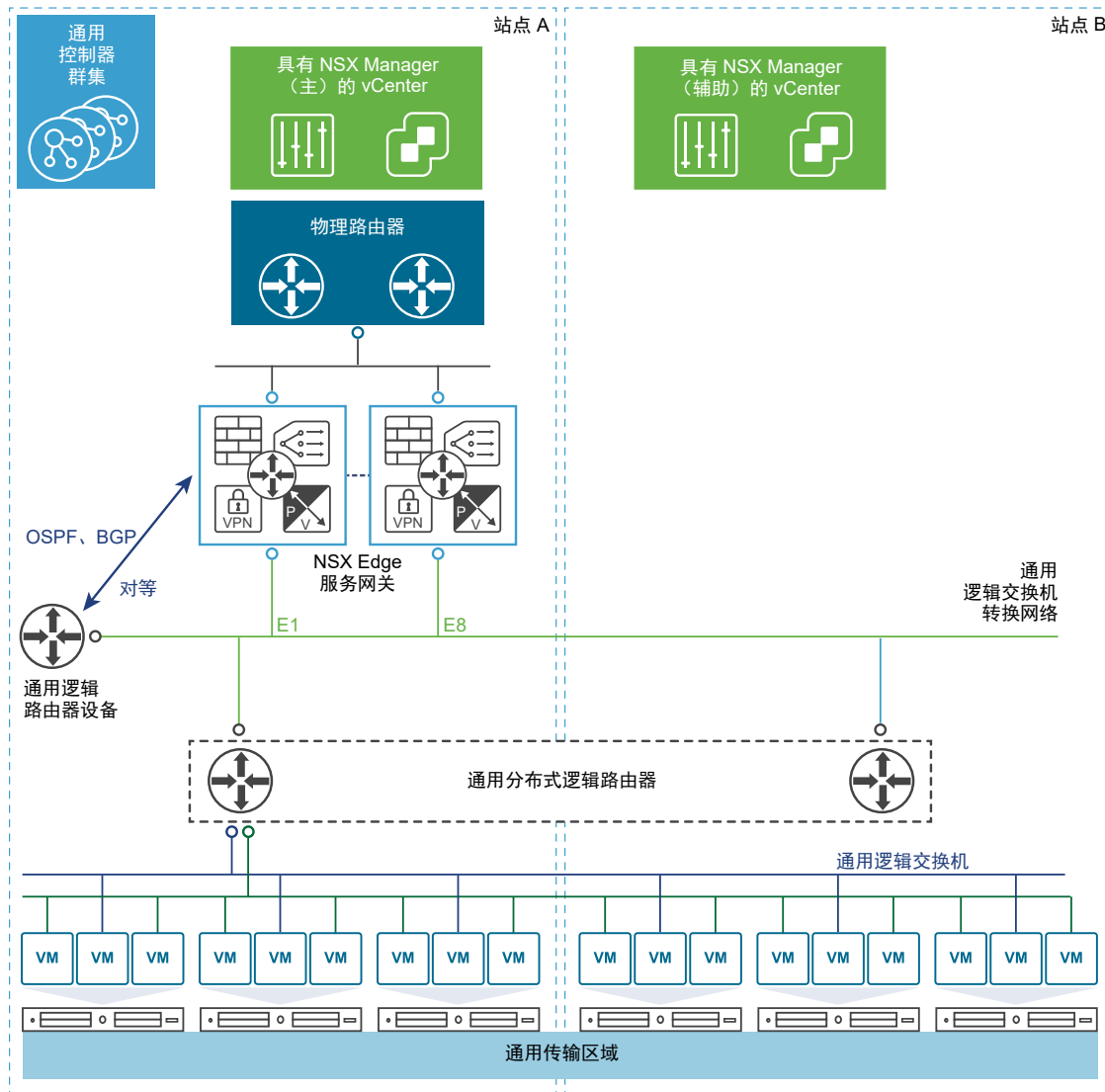
- 一个通用传输区域，其中的所有群集包含于单个或多个站点。

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

图 3-1. 位于单个站点中的跨 vCenter NSX



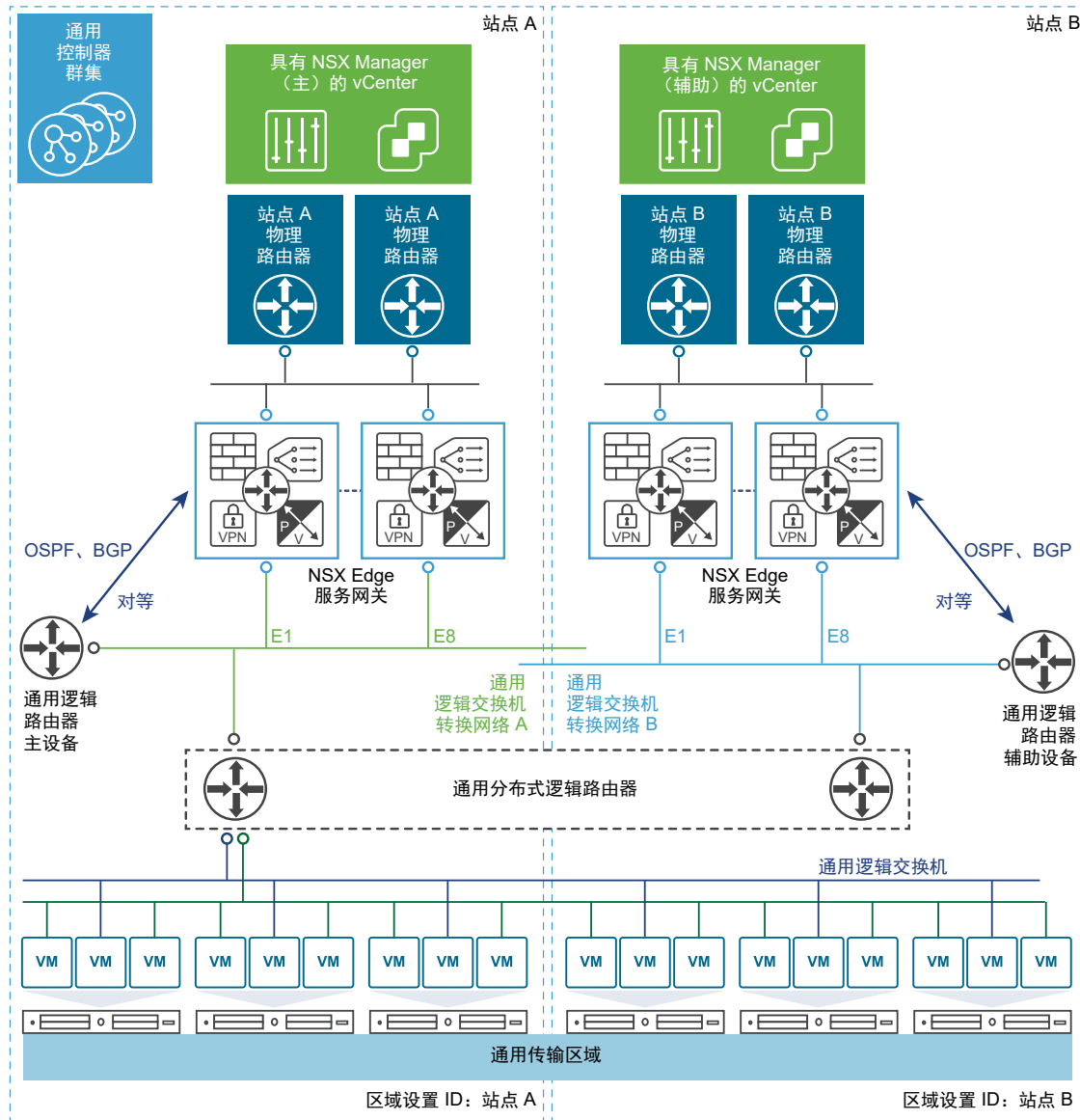
### 图 3-2. 跨两个站点的跨 vCenter NSX



## 本地输出

多站点跨 vCenter NSX 环境中的所有站点都可以使用同一物理路由器来处理输出流量。但是，如果需要自定义输出路由，则您必须在创建通用逻辑路由器时启用本地输出功能。

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



## 修改 NSX Manager 角色

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

您必须了解更改 NSX Manager 的角色时产生的影响。

### 设置为主角色

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

### 设置为独立角色（从辅助角色切换）

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

## 设置为独立角色（从主角色切换）

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

## 从主角色断开连接

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

# 安装准备工作

# 4

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
- 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 4-1. 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
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 4-2. 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](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"> <li>■ ESXi 6.0 或更高版本</li> <li>■ 为 NSX 6.2 或更高版本的 VIB 准备的主机群集</li> </ul>

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 4-3. 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	
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

表 4-3. 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
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
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	

表 4-3. 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
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

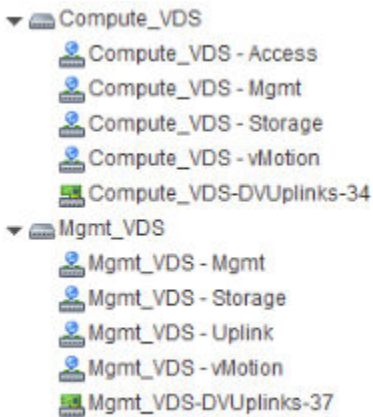
下面的屏幕截图显示这些群集在 vCenter 中的显示方式。



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。

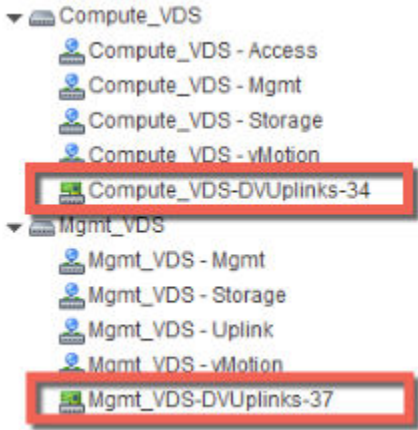
例如，下面的屏幕截图显示这些 **Distributed Switch** 和端口在 vCenter 中的显示方式。



或者，每个端口组也可以用 **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>）。

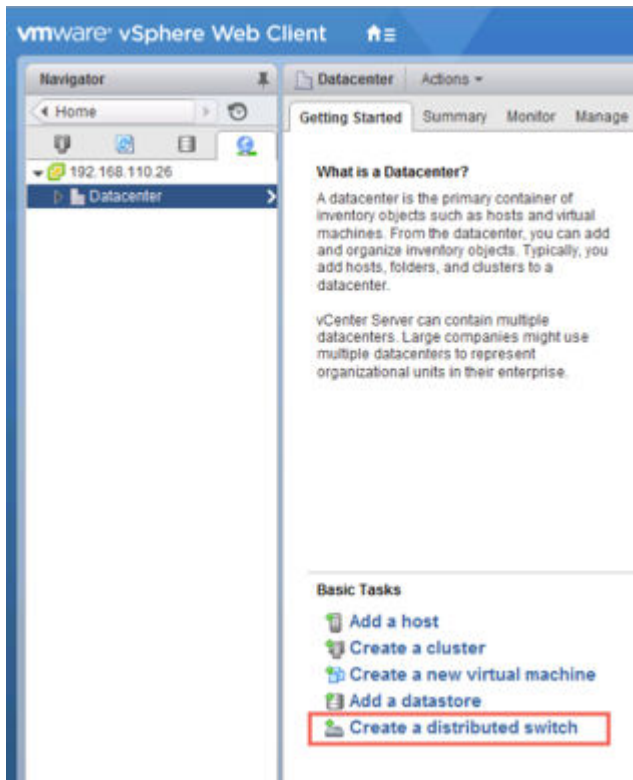
### 前提条件

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)。



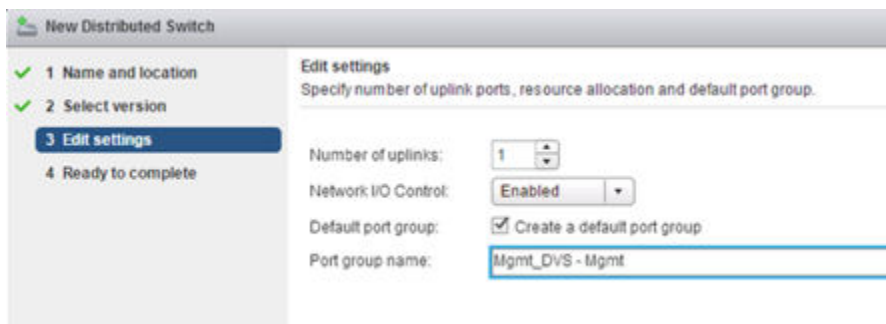
- 3 根据将与交换机关联的主机群集为此交换机指定体现其意义的名称。

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。

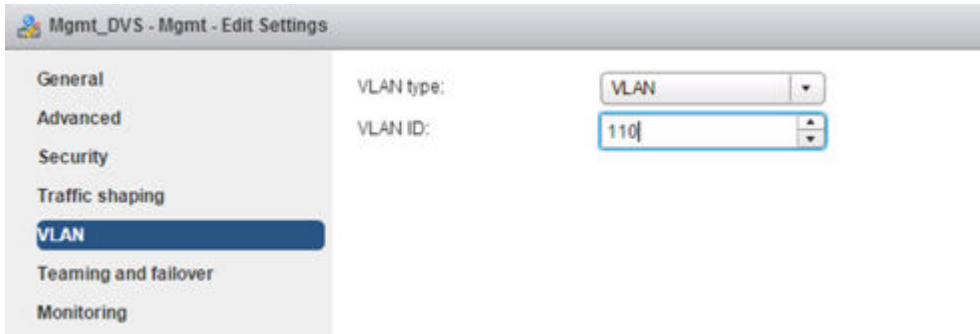


默认端口组正是此交换机将包含的端口组之一。创建交换机后，您将可以添加不同流量类型的端口组。或者，在创建新 **VDS** 时，您也可以取消勾选 **创建默认端口组 (Create a default port group)** 选项。这种做法实际上可能是最佳实践：最好在创建端口组时明确。



- 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。

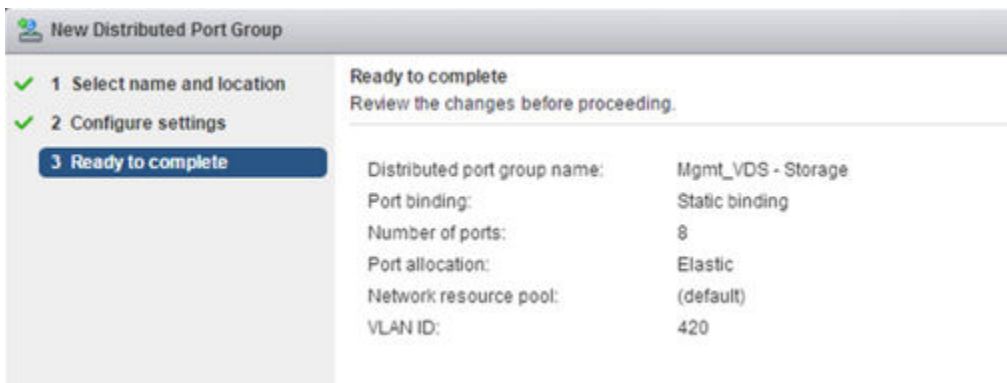
例如，如果您的主机管理接口在 VLAN 110 中，则将默认端口组置于 VLAN 110 中。如果您的主机管理接口未在 VLAN 中，请跳过此步骤。



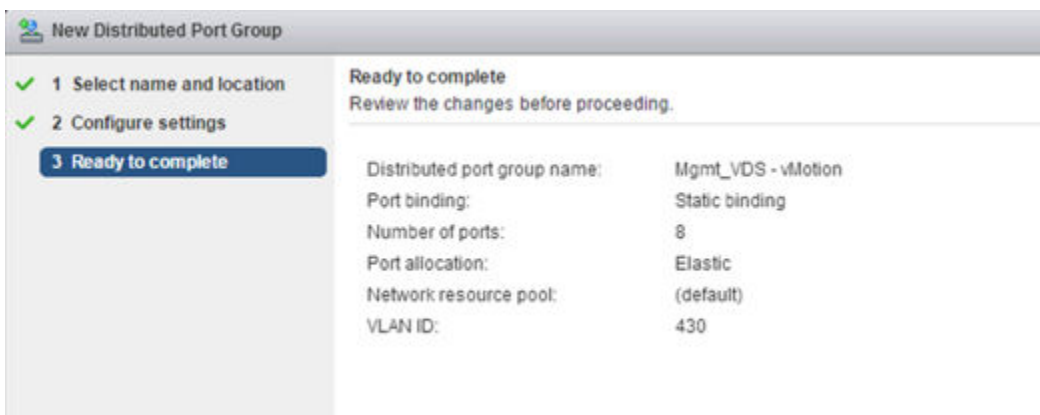
- 6 完成“新建 Distributed Switch”向导之后，右键单击该 Distributed Switch，然后选择**新建 Distributed Switch 端口组 (New Distributed Port Group)**。

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。

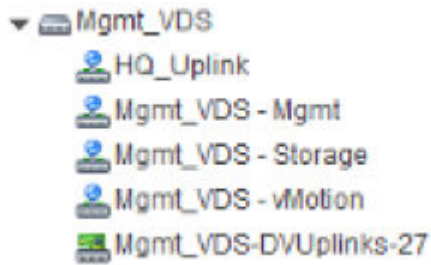


vMotion 流量的示例组设置。



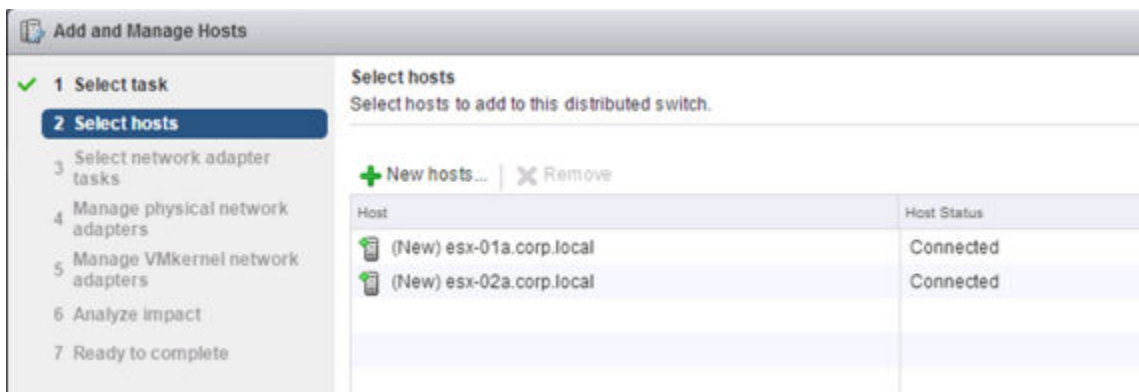
完成的 Distributed Switch 和端口组如下所示。



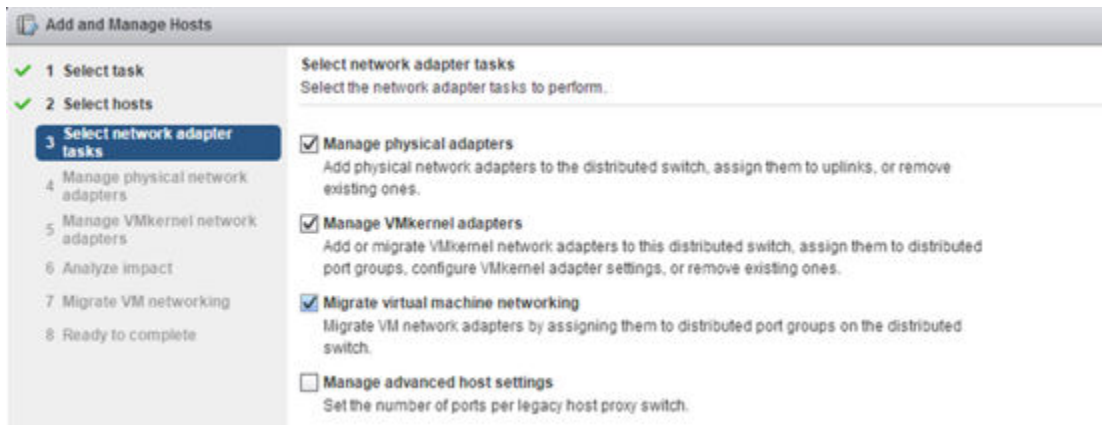


- 7 右键单击 Distributed Switch，选择**添加和管理主机 (Add and Manage Hosts)**，然后选择**添加主机 (Add Hosts)**。

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。

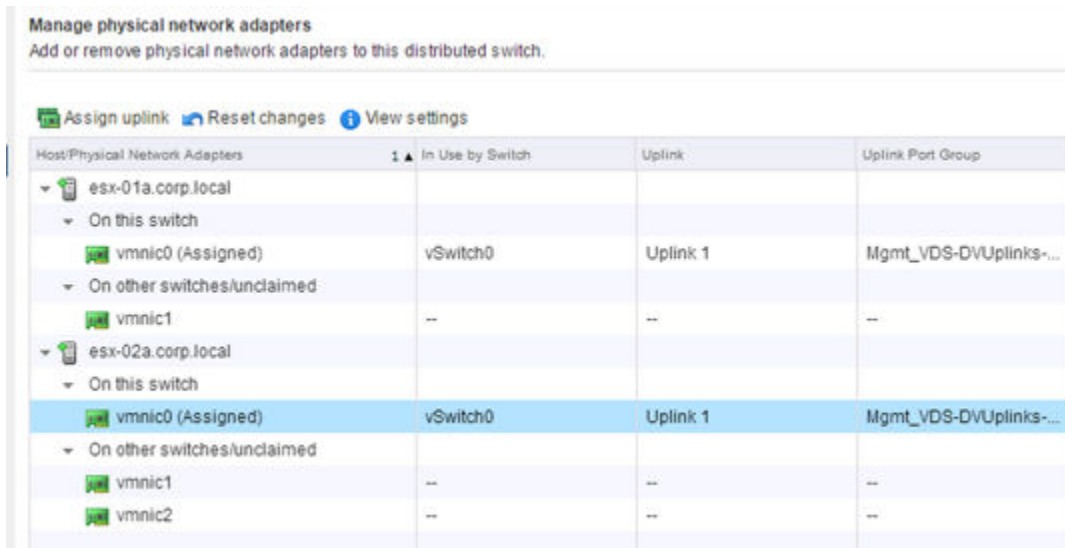


- 8 选择各选项以迁移物理适配器、VMkernel 适配器和虚拟机网络连接。



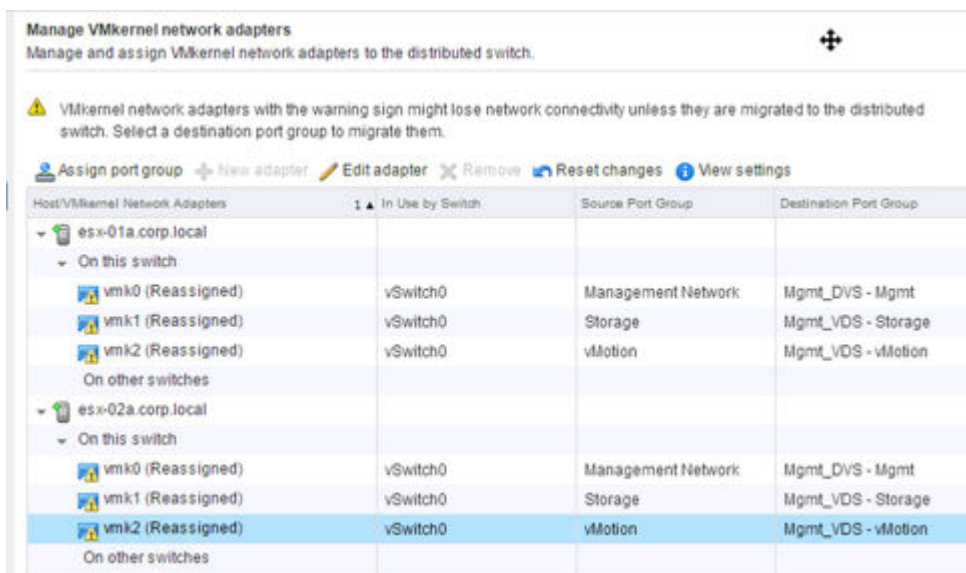
- 9 选择一个 vmnic 并单击**分配上行链路 (Assign uplink)**，将 vmnic 从标准 vSwitch 迁移至 Distributed Switch。为连接到分布式 vSwitch 的每个主机重复此步骤。

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。



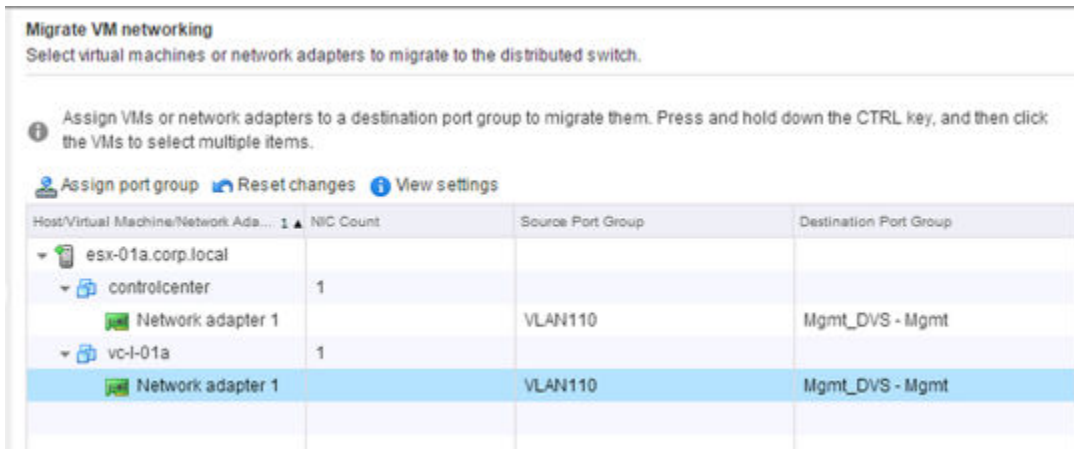
- 10 选择一个 VMKernel 网络适配器，然后单击**分配端口组 (Assign port group)**。为连接到分布式 vSwitch 的所有主机上的所有网络适配器重复此步骤。

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

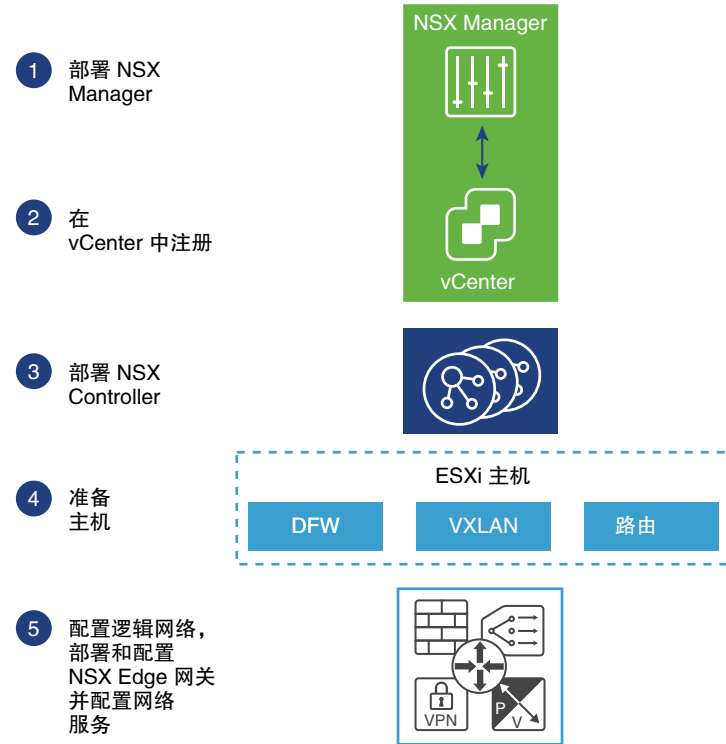
```

## 后续步骤

为所有 vSphere Distributed Switch 重复迁移流程。

## NSX 安装工作流程和示例拓扑

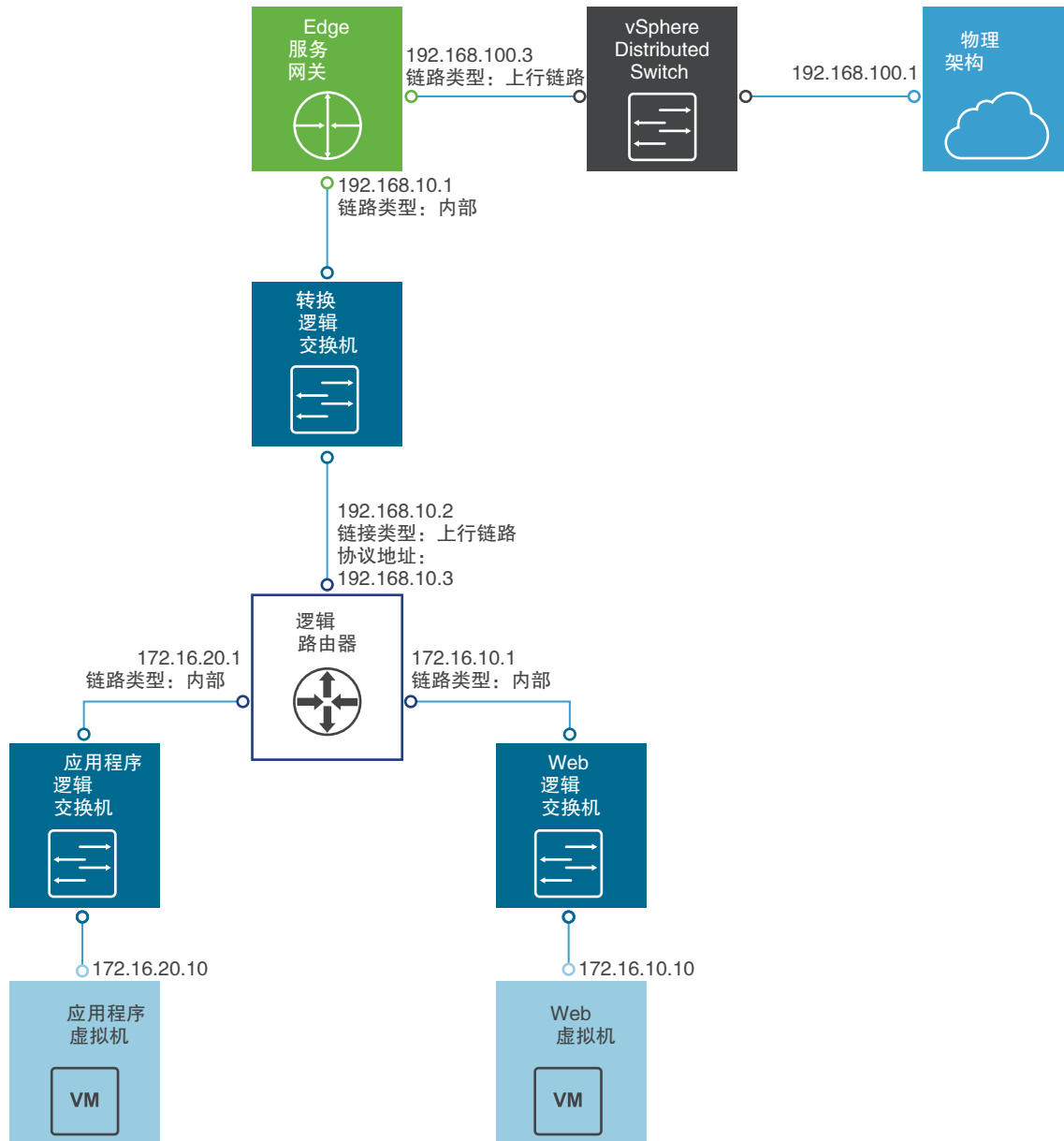
NSX 安装流程包括部署多个虚拟设备，完成一些 ESX 主机准备，并进行一些配置以便所有物理和虚拟设备能够相互通信。



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。

# 针对主/辅助 NSX Manager 的任务

# 5

在跨 vCenter 环境中，可以同时存在一个主 NSX Manager 和多达七个辅助 NSX Manager。在每个 NSX Manager 上执行一些设置任务，无论它将成为主 NSX Manager，还是辅助 NSX Manager。

本章讨论了以下主题：

- 安装 NSX Manager 虚拟设备
- 配置 Single Sign On
- 在 NSX Manager 中注册 vCenter Server
- 为 NSX Manager 配置 syslog 服务器
- 安装和分配 NSX for vSphere 许可证
- 从防火墙保护中排除虚拟机

## 安装 NSX Manager 虚拟设备

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。

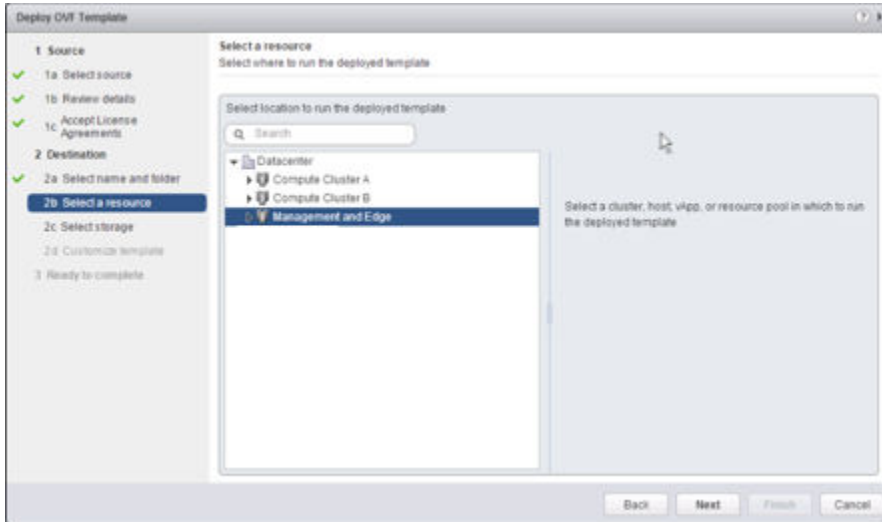
- 6 接受 VMware 许可协议。
- 7 编辑 NSX Manager 名称（如果需要）。选择已部署的 NSX Manager 所在的位置。

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。

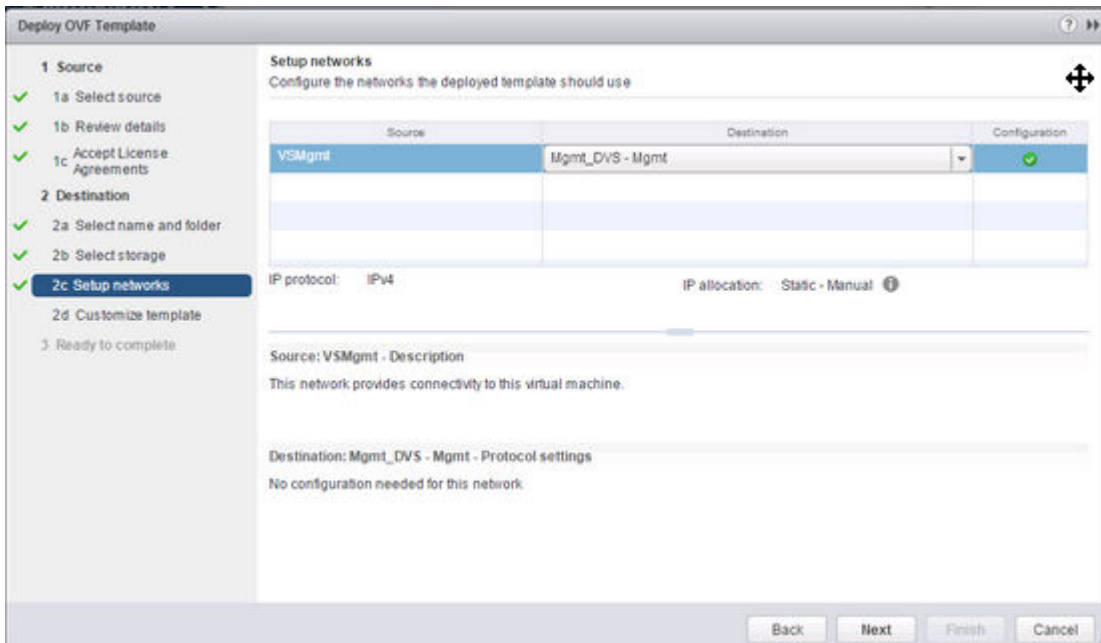
例如：



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。

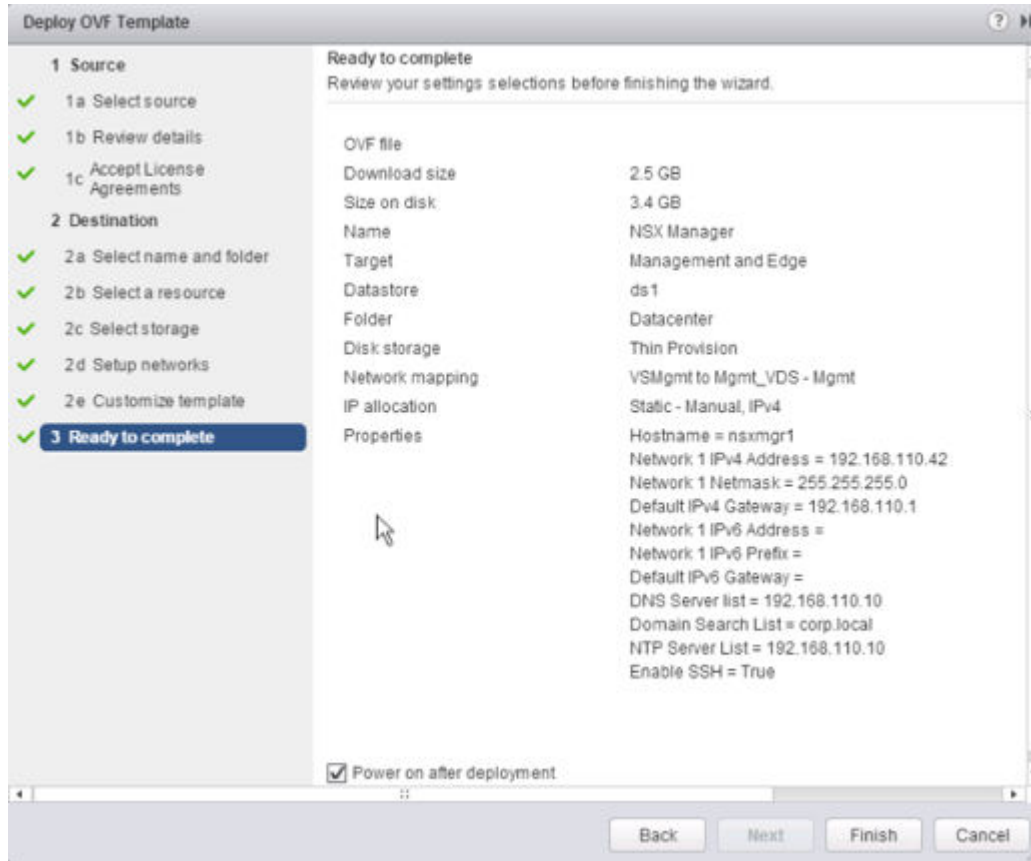
例如，下面的屏幕截图显示 Mgmt\_DVS - Mgmt 端口组选择。



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。

## 配置 Single Sign On

SSO 可提高 vSphere 和 NSX 的安全性，它允许各个组件通过安全的令牌交换机制彼此进行通信，而不要求每个组件单独对用户进行身份验证。

可以在 NSX Manager 上配置 Lookup Service，并提供 SSO 管理员凭据以便以 SSO 用户的身份注册 NSX Management Service。将 Single Sign On (SSO) 服务与 NSX 集成在一起可提高 vCenter 用户进行用户身份验证的安全性，并使 NSX 可以通过诸如 AD、NIS 和 LDAP 等其他标识服务对用户进行身份验证。借助 SSO，NSX 可支持通过 REST API 调用使用受信任源的已验证安全断言标记语言 (SAML) 令牌来进行身份验证。NSX Manager 还可以获取身份验证 SAML 令牌供其他 VMware 解决方案使用。

SSO 用户的 NSX 缓存组信息。对组成员资格进行的更改最多将花费 60 分钟的时间从标识提供程序（例如 Active Directory）传播到 NSX。

#### 前提条件

- 要在 NSX Manager 上使用 SSO，您必须拥有 vCenter Server 5.5 或更高版本，并且必须在 vCenter Server 上安装 Single Sign On (SSO) 身份验证服务。请注意，这是针对嵌入式 SSO。您的部署可能使用外部集中式 SSO 服务器。

有关 vSphere 提供的 SSO 服务的信息，请参见 <http://kb.vmware.com/kb/2072435> 和 <http://kb.vmware.com/kb/2113115>。

- 必须指定 NTP 服务器，以使 SSO 服务器上的时间与 NSX Manager 上的时间保持同步。

例如：

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（位于 <https://<nsx-manager-ip>> 或 <https://<nsx-manager-hostname>>），然后以管理员身份使用您在 NSX Manager 安装期间配置的密码登录。

- 2 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”。

## 在 NSX Manager 中注册 vCenter Server

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，甚至在跨 vCenter NSX 环境中。

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，必须先移除所有 NSX 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，以便在新的 vCenter Server 系统中进行注册。

### 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（位于 <https://<nsx-manager-ip>> 或 <https://<nsx-manager-hostname>>），然后以管理员身份使用您在 NSX Manager 安装期间配置的密码登录。

- 2 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。

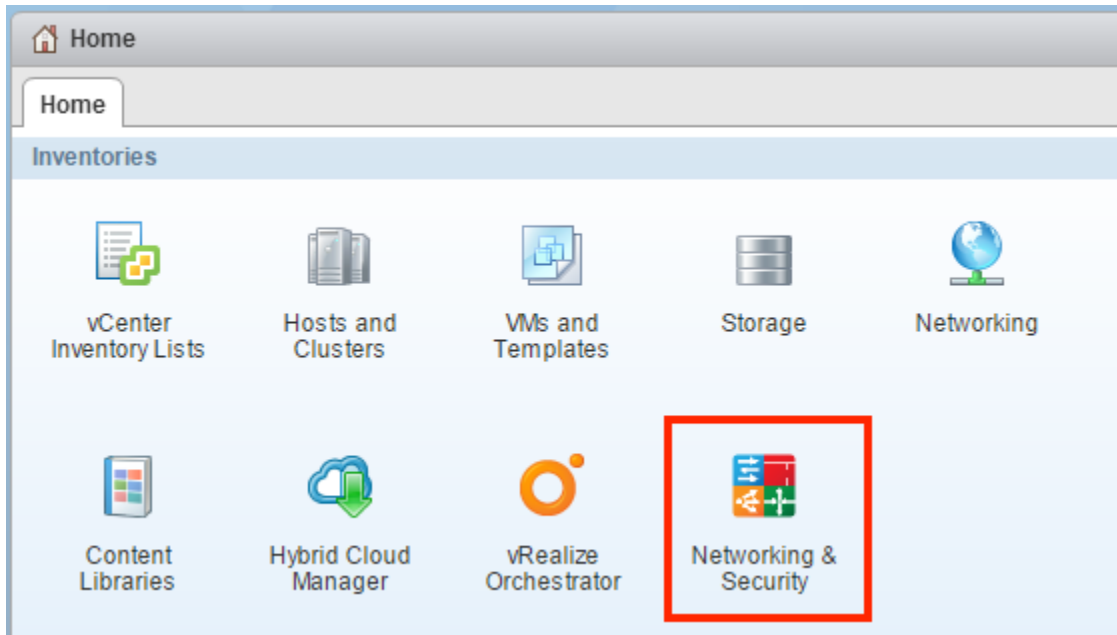
- 5 不要选中**修改插件脚本下载位置 (Modify plugin script download location)**，除非 NSX Manager 位于屏蔽设备类型的防火墙后面。

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。

## 为 NSX Manager 配置 syslog 服务器

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。



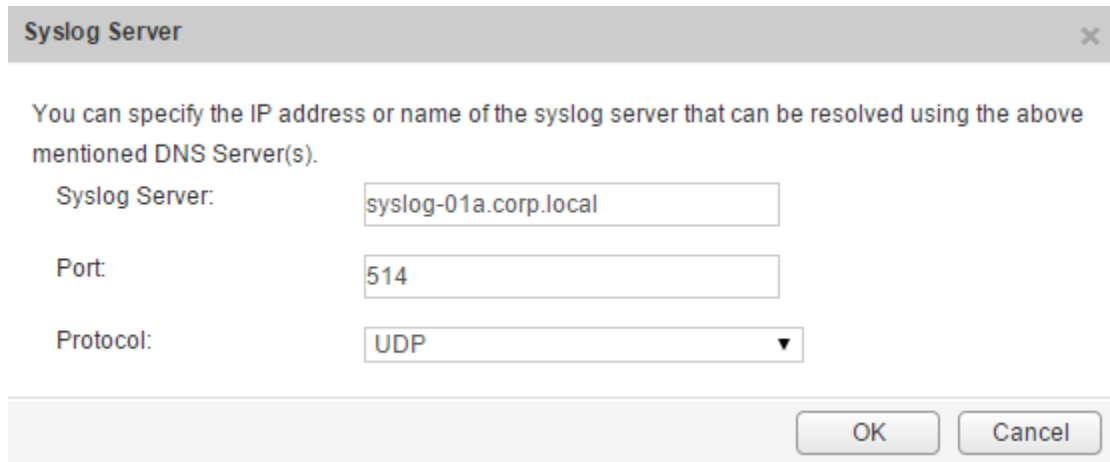
## 步骤

- 1 登录到 NSX Manager 虚拟设备。

在 Web 浏览器中，导航到 NSX Manager 设备 GUI（位于 <https://<nsx-manager-ip>> 或 <https://<nsx-manager-hostname>>），然后以管理员身份使用您在 NSX Manager 安装期间配置的密码登录。

- 2 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：



- 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>。

## 从防火墙保护中排除虚拟机

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。

# 配置主 NSX Manager

# 6

跨 vCenter NSX 环境中只有一个主 NSX Manager。选择将作为您的主 NSX Manager 的 NSX Manager，并完成配置任务，以完成 NSX 的安装，向 NSX Manager 分配主角色，并创建通用对象。

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

本章讨论了以下主题：

- 在主 NSX Manager 上部署 NSX Controller
- 准备主 NSX Manager 上的主机
- 从主 NSX Manager 配置 VXLAN
- 为主 NSX Manager 分配分段 ID 池和多播地址
- 将主要角色分配给 NSX Manager
- 在主 NSX Manager 上分配通用分段 ID 池和通用多播地址
- 在主 NSX Manager 上添加通用传输区域
- 在主 NSX Manager 上添加通用逻辑交换机
- 将虚拟机连接到逻辑交换机
- 在主 NSX Manager 上添加通用逻辑（分布式）路由器

## 在主 NSX Manager 上部署 NSX Controller

NSX Controller 是一个高级分布式状态管理系统，可以提供控制层面功能以实现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。在跨 vCenter NSX 中，一旦为 NSX Manager 分配了主要角色，其控制器群集就会变为用于整个跨 vCenter NSX 环境的通用控制器群集。

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。

## 前提条件

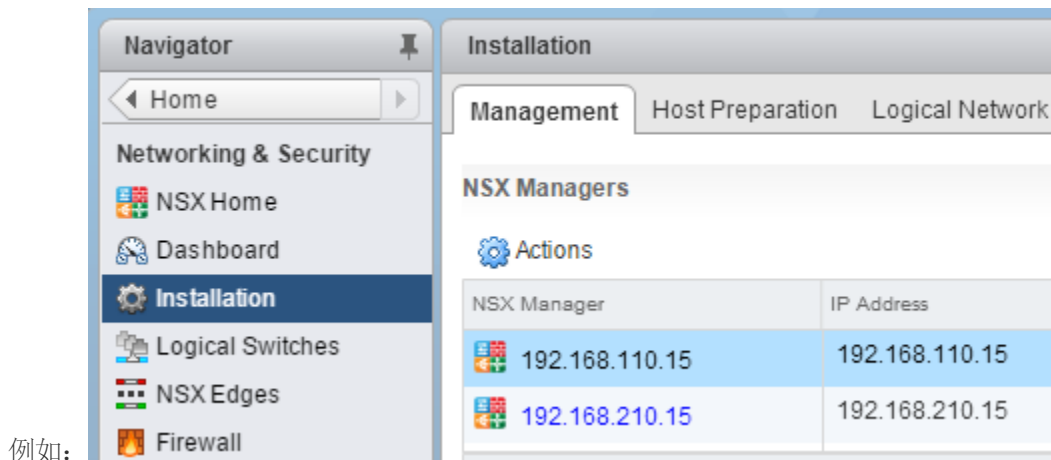
- 在部署 NSX Controller 之前，必须部署 NSX Manager 设备并向 NSX Manager 注册 vCenter。
- 确定控制器群集的 IP 池设置，包括网关和 IP 地址范围。DNS 设置是可选设置。NSX Controller IP 网络必须具有与 NSX Manager 以及 ESXi 主机上的管理接口的连接。

## 步骤

- 1 通过使用 vSphere Web Client，登录到在将变为主 NSX Manager 的 NSX Manager 中注册的 vCenter Server 系统。

如果跨 vCenter NSX 环境中的 vCenter Server 系统处于增强型链接模式，您可以从任何链接的 vCenter Server 系统中访问任何关联的 NSX Manager，方法是从 **NSX Manager** 下拉菜单中选择该 NSX Manager。

- 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。



如果 vCenter Server 系统处于增强型链接模式，将会看到此处列出的所有关联的 NSX Manager。

- 3 在 NSX Manager 部分中，选择将成为主 NSX Manager 的 NSX Manager。
- 4 在“NSX Controller 节点”部分，单击**添加节点 (Add Node)** (+) 图标。
- 5 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: \* controller-1

NSX Manager: \* 192.168.110.15

Datacenter: \* Datacenter Site A

Cluster/Resource Pool: \* Management & Edge Cl...

Datastore: \* ds-site-a-nfs01

Host: esxmgmt-01a.corp.local

Folder: NSX Controllers

Connected To: \* vds-mgt\_Managem Change Remove

IP Pool: \* controller-pool Select

Password: \* \*\*\*\*\*

Confirm password: \* \*\*\*\*\*

OK Cancel

- 6 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：

**Add Static IP Pool**

Name: \* controller-pool

Gateway: \* 192.168.110.1  
A gateway can be any IPv4 or IPv6 address.

Prefix Length: \* 24

Primary DNS:

Secondary DNS:

DNS Suffix:

Static IP Pool: \* 192.168.110.31-192.168.110.35

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

OK Cancel

7 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

8 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”。

## 准备主 NSX Manager 上的主机

主机准备是 NSX Manager 中执行的一个流程，即 1) 在 vCenter 群集成员的 ESXi 主机上安装 NSX 内核模块并 2) 构建 NSX 控制层面和管理层面结构。封装在 VIB 文件中的 NSX 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

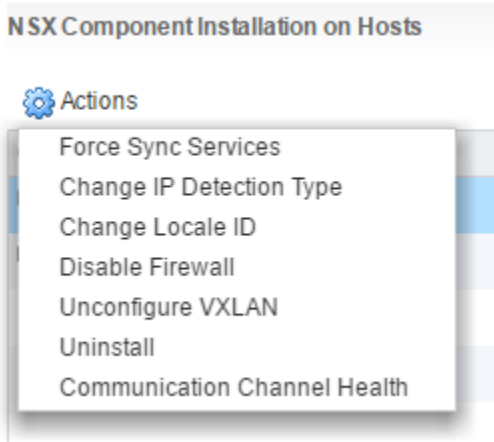
Name: nsxmgr-l-01a.corp.local
Address: 192.168.110.42
```

- 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。

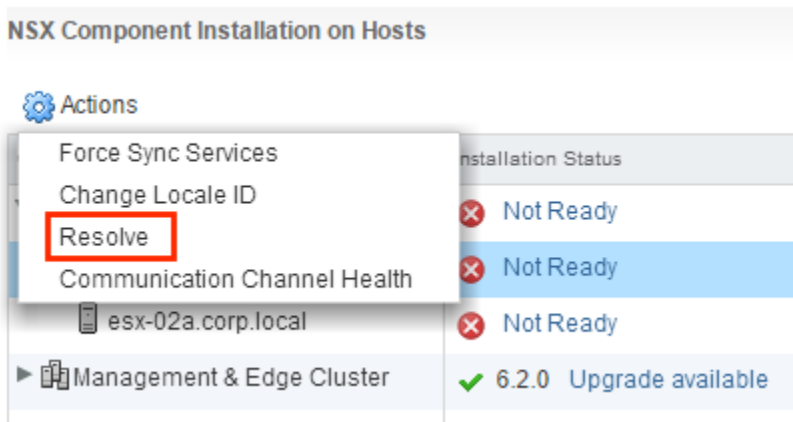
- 如果您的环境中具有 vSphere Update Manager (VUM)，您必须在准备进行网络虚拟化的群集之前将其禁用。有关如何确认 VUM 是否启用及如何在必要时禁用的信息，请参见 <http://kb.vmware.com/kb/2053782>。
- 开始 NSX 主机准备流程之前，务必要确保群集处于已解决状态—这意味着群集的操作 (Actions) 列表中不显示解决 (Resolve) 选项。

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 通过使用 vSphere Web Client，登录到在将变为主 NSX Manager 的 NSX Manager 中注册的 vCenter Server 系统。

如果跨 vCenter NSX 环境中的 vCenter Server 系统处于增强型链接模式，您可以从任何链接的 vCenter Server 系统中访问任何关联的 NSX Manager，方法是从 **NSX Manager** 下拉菜单中选择该 NSX Manager。

- 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。

## 从主 NSX Manager 配置 VXLAN

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。

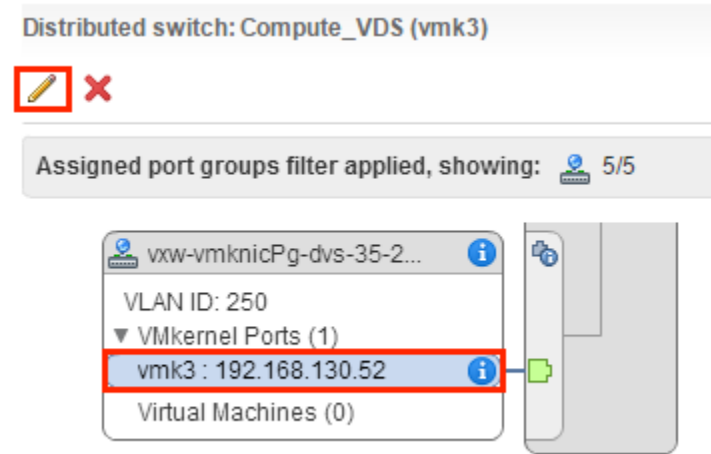
基于 IP 哈希的绑定（以太网通道、LACPv1 或 LACPv2）的最佳做法是在组中使用 vSphere Distributed Switch 上的所有上行链路，而不是在该 vSphere Distributed Switch 上的端口组中使用不同的绑定策略。有关详细信息和更多指导，请参见 <https://communities.vmware.com/docs/DOC-27683> 上的《VMware® NSX for vSphere 网络虚拟化设计指南》。

- 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。

如果要为特定的 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

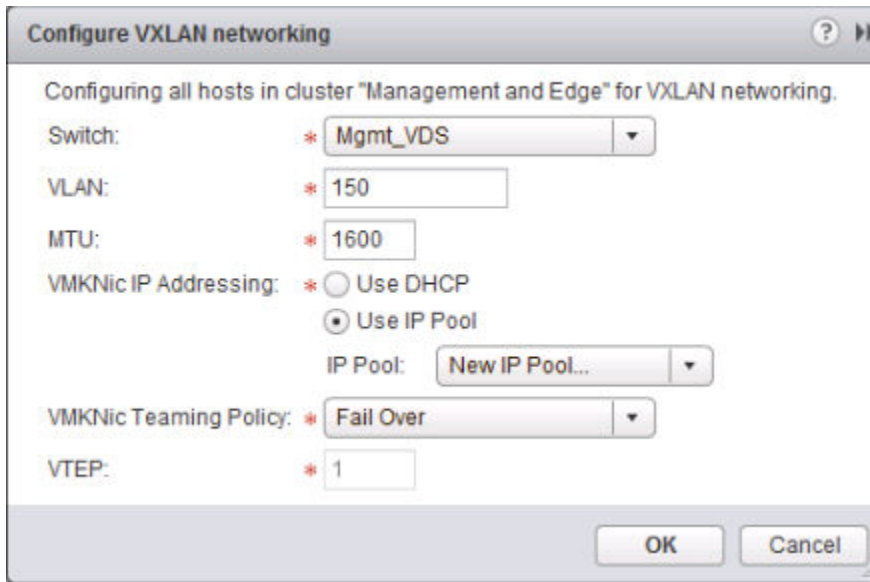
- 1 通过使用 vSphere Web Client，登录到在将变为主 NSX Manager 的 NSX Manager 中注册的 vCenter Server 系统。

如果跨 vCenter NSX 环境中的 vCenter Server 系统处于增强型链接模式，您可以从任何链接的 vCenter Server 系统中访问任何关联的 NSX Manager，方法是从 **NSX Manager** 下拉菜单中选择该 NSX Manager。

- 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 验证是否在 **NSX Manager** 下拉菜单中选择了正确的 NSX Manager。
- 4 在 **VXLAN** 列中单击未配置 (Not Configured)。
- 5 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

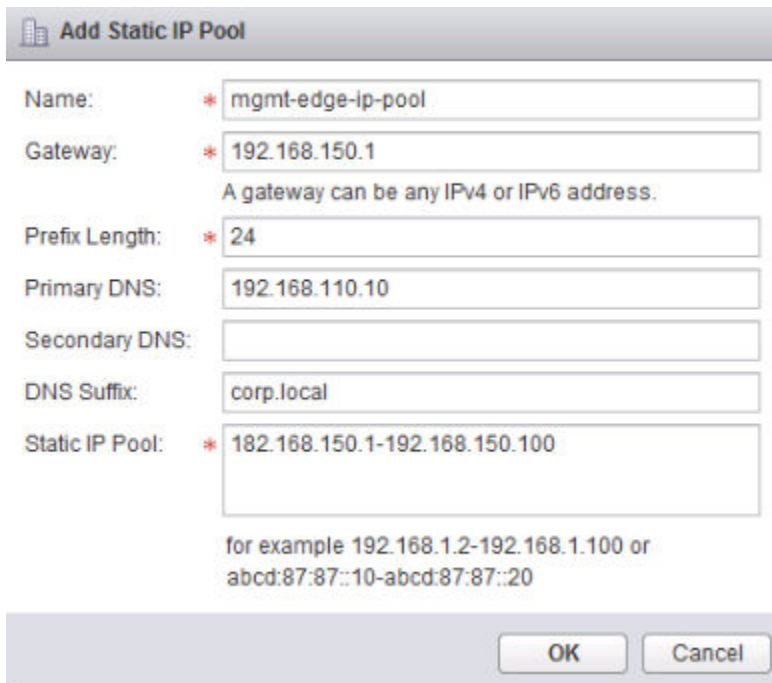
IP Pool: New IP Pool...

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

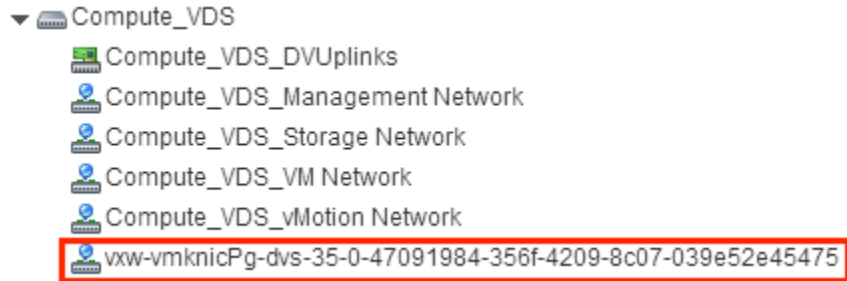
OK Cancel

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。

## 为主 NSX Manager 分配分段 ID 池和多播地址

VXLAN 分段构建于 VXLAN 隧道端点 (VTEP) 之间。每个 VXLAN 隧道都具有一个分段 ID。必须为主 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 的小型子集。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。

跨 vCenter NSX 环境中的 NSX Manager 必须全部使用非重叠的分段 ID 池。此外，通用分段 ID 池不应与跨 vCenter NSX 环境中的任何分段 ID 池重叠。单个 NSX Manager 和 vCenter 环境中会自动实施非重叠 VNI。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 NSX 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。

您必须确保指定的多播地址或地址范围与跨 vCenter NSX 环境中的任何 NSX Manager 上分配的其他多播地址不存在冲突。

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 通过使用 vSphere Web Client，登录到在将变为主 NSX Manager 的 NSX Manager 中注册的 vCenter Server 系统。

如果跨 vCenter NSX 环境中的 vCenter Server 系统处于增强型链接模式，您可以从任何链接的 vCenter Server 系统中访问任何关联的 NSX Manager，方法是从 **NSX Manager** 下拉菜单中选择该 NSX Manager。

- 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 验证是否在 **NSX Manager** 下拉菜单中选择了正确的 NSX Manager。
- 4 单击分段 ID > 编辑 (Segment ID > Edit)。
- 5 输入一个分段 ID 范围，例如，5000–5999。
- 6 （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。

## 将主要角色分配给 NSX Manager

主 NSX Manager 运行控制器群集。其他 NSX Manager 是辅助的。由主 NSX Manager 部署的控制器群集是一个共享对象，可称为通用控制器群集。辅助 NSX Manager 会自动导入通用控制器群集。跨 vCenter NSX 环境中有一个主 NSX Manager 和最多 7 个辅助 NSX Manager。

NSX Manager 可以拥有以下四个角色中的一个：

- 主
- 辅助
- 独立
- 转换

要查看 NSX Manager 的角色，请登录到链接至该 NSX Manager 的 vCenter，并导航到主页 (Home) > 网络和安全 (Networking & Security) > 安装 (Installation)，并选择管理 (Management) 选项卡。角色显示在 NSX Manager 部分的“角色”列中。如果未显示“角色”列，则 NSX Manager 拥有独立角色。



## 前提条件

- NSX Manager（主 NSX Manager 和要为其分配辅助角色的 NSX Manager）的版本必须相匹配。
- 主 NSX Manager 和要为其分配辅助角色的 NSX Manager 必须具有节点 ID 且节点 ID 不能相同。从 OVA 文件部署的 NSX Manager 实例均有唯一的节点 ID。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 具有相同的节点 ID，并且这两个 NSX Manager 不能在同一个跨 vCenter NSX 安装中使用。

**注** 您可以使用以下 REST API 调用查看 NSX Manager 节点 ID：

```
GET https://NSX-Manager-IP-Address/api/2.0/services/vsmconfig
```

- 必须在单独的唯一 vCenter Server 系统中注册每个 NSX Manager。
- 对于所有 NSX Manager，用于 VXLAN 的 UDP 端口都必须相同。

**注** 您可以使用 vSphere Web Client 中的**网络和安全 (Networking & Security) > 安装 (Installation) > 逻辑网络准备 (Logical Network Preparation)**查看和更改 VXLAN 端口。请参阅《NSX 管理指南》中的“更改 VXLAN 端口”。

- 在为某个 NSX Manager 分配辅助角色时，链接到该 NSX Manager 的 vCenter Server 系统不能具有任何部署的 NSX Controller。
- 分配有辅助角色的 NSX Manager 的分段 ID 池不得与主 NSX Manager 的分段 ID 池或任何其他辅助 NSX Manager 的分段 ID 池重叠。
- 分配有辅助角色的 NSX Manager 必须为独立或转换角色。

## 步骤

- 1 使用 vSphere Web Client 登录到与主 NSX Manager 链接的 vCenter。
- 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。
- 3 选择您要分配主要角色的 NSX Manager，单击**操作 (Actions)**，然后单击**分配主要角色 (Assign Primary Role)**。

已为选定的 NSX Manager 分配主要角色。跨 vCenter NSX 环境中的其他 NSX Manager 现在显示独立角色。

## 在主 NSX Manager 上分配通用分段 ID 池和通用多播地址

通用分段 ID 池指定构建逻辑网络分段时所使用的范围。跨 vCenter NSX 部署使用唯一的通用分段 ID 池，以确保通用逻辑交换机 VXLAN 网络标识符 (VNI) 在所有辅助 NSX Manager 中是一致的。

通用分段 ID 池在主 NSX Manager 上定义一次，随后将其同步到辅助 NSX Manager。请注意，分段 ID 范围在您计划用于跨 vCenter NSX 部署中的任何 NSX Manager 中都必须唯一。以下示例使用较大范围以在将来提供可扩展性。

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 的小型子集。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。

您必须确保指定的多播地址或地址范围与跨 vCenter NSX 环境中的任何 NSX Manager 上分配的其他多播地址不存在冲突。

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 通过使用 vSphere Web Client，登录到在将变为主 NSX Manager 的 NSX Manager 中注册的 vCenter Server 系统。

如果跨 vCenter NSX 环境中的 vCenter Server 系统处于增强型链接模式，您可以从任何链接的 vCenter Server 系统中访问任何关联的 NSX Manager，方法是从 **NSX Manager** 下拉菜单中选择该 NSX Manager。

- 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 验证是否在 **NSX Manager** 下拉菜单中选择了正确的 NSX Manager。
- 4 单击分段 ID > 编辑 (Segment ID > Edit)。



- 5 输入通用分段 ID 的范围，如 900000-909999。

**小心** 确认该范围与在跨 vCenter NSX 环境中的任何 NSX Manager 上分配的任何其他范围不重叠。

- 6 （可选）如果任何传输区域将使用多播或混合复制模式，请选中**启用通用多播寻址 (Enable Universal multicast addressing)**，并输入一个通用多播地址或通用多播地址范围。

**小心** 确认指定的多播地址与跨 vCenter NSX 环境中任何 NSX Manager 上分配的任何其他多播地址不存在冲突。

## 结果

然后，在配置通用逻辑交换机后，每个通用逻辑交换机都会从该池接收到通用分段 ID。

## 在主 NSX Manager 上添加通用传输区域

通用传输区域控制通用逻辑交换机可以访问的主机。通用传输区域由 NSX Manager 创建，并会复制到辅助 NSX Manager。通用传输区域可跨跨 vCenter NSX 环境中的一个或多个 vSphere 群集。

创建后，通用传输区域在跨 vCenter NSX 环境中的所有辅助 NSX Manager 上可用。只能有一个通用传输区域。

### 前提条件

在创建主 NSX Manager 后配置通用传输区域。

### 步骤

- 1 通过使用 vSphere Web Client，登录到在主 NSX Manager 中注册的 vCenter Server 系统。  
如果跨 vCenter NSX 环境中的 vCenter Server 系统处于增强型链接模式，您可以从任何链接的 vCenter Server 系统中访问任何关联的 NSX Manager，方法是从 **NSX Manager** 下拉菜单中选择该 NSX Manager。
- 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 验证是否在 **NSX Manager** 下拉菜单中选择了正确的 NSX Manager。
- 4 单击**传输区域 (Transport Zones)**，然后单击**新建传输区域 (New Transport Zone)** ( 图标)。
- 5 选择**标记此对象待进行通用同步 (Mark this object for universal synchronization)**。  
该传输区域将与辅助 NSX Manager 进行同步。
- 6 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。

## 7 选择要添加到传输区域的群集。

### 结果

通用传输区域在跨 vCenter NSX 环境中的所有 NSX Manager 上可用。

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

### 后续步骤

接下来，创建通用逻辑交换机。

## 在主 NSX Manager 上添加通用逻辑交换机

在跨 vCenter NSX 部署中，您可以创建跨所有 vCenter 的通用逻辑交换机。传输区域类型确定新交换机是逻辑交换机还是通用逻辑交换机。当您向通用传输区域添加逻辑交换机时，逻辑交换机是通用的。

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。

**注** 在创建通用逻辑交换机时，您无法禁用 IP 发现。在创建通用逻辑交换机后，您可以通过 API 禁用 IP 发现。该设置是在每个 NSX Manager 上单独管理的。请参阅《NSX API 指南》。


**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。如果您的虚拟机具有多个 MAC 地址或使用中继 VLAN 的虚拟网卡，您可能希望启用 MAC 发现。

### 前提条件

表 6-1. 创建逻辑交换机或通用逻辑交换机的必备条件

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

**步骤**

- 1 导航到主页 > 网络和安全 > 逻辑交换机 (Home > Networking & Security > Logical Switches)。
- 2 选择主 NSX Manager。
- 3 单击**新建逻辑交换机 (New Logical Switch)** () 图标。
- 4 键入逻辑交换机的名称和可选描述。
- 5 在“传输区域”部分中，单击**更改 (Change)**以选择一个传输区域。选择要创建通用逻辑交换机的通用传输区域。

**重要事项** 如果创建一个通用逻辑交换机并选择混合作为复制模式，则必须确保使用的多播地址与跨 vCenter NSX 环境中的任何 NSX Manager 上分配的其他多播地址不存在冲突。

- 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 **MAC 发现 (Enable MAC learning)**。

**示例：逻辑交换机和通用逻辑交换机**

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

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

逻辑交换机和通用逻辑交换机的分段 ID 来自于不同的分段 ID 池。

       Actions					
Virtual Wire ID	Segment ID	Name	1 ▲	Status	Transport Zone
 virtualwire-1	5000	 App		 Normal	 Transport-Zone
 universalwire-2	900000	 Universal-App		 Normal	 Universal-Transport-Zone

**后续步骤**


向通用逻辑交换机添加虚拟机。

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

## 将虚拟机连接到逻辑交换机

您可以将虚拟机连接到逻辑交换机或通用逻辑交换机。

### 步骤

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

## 在主 NSX Manager 上添加通用逻辑（分布式）路由器

主机中的逻辑路由器内核模块在 VXLAN 网络之间以及虚拟和物理网络之间执行路由。如果需要，NSX Edge 设备可提供动态路由功能。通用逻辑路由器可提供通用逻辑交换机之间的东西向路由。

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>。

**重要事项** 如果您在跨 vCenter NSX 环境中的 NSX Edge 上启用高可用性，则活动和备用 NSX Edge 设备必须位于同一个 vCenter Server 中。如果您将 NSX Edge HA 对的其中一个成员迁移到其他 vCenter Server 系统中，则两个 HA 设备将不再作为 HA 对运行，而且您可能会遇到流量中断问题。

#### 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”。
- 确定是否需要启用本地输出。本地输出允许您选择性地向主机发送路由。如果 NSX 部署跨多个站点，您可能需要此功能。有关详细信息，请参见 [跨 vCenter NSX 拓扑](#)。无法在创建通用逻辑路由器后启用本地输出。

#### 步骤

- 1 在 vSphere Web Client 中，导航到主页 > 网络和安全 > NSX Edge (Home > Networking & Security > NSX Edges)。
- 2 选择要添加通用逻辑路由器的主 NSX Manager。
- 3 单击添加 (Add) ( 图标。
- 4 选择通用逻辑 (分布式) 路由器 (Universal Logical (Distributed) Router)。
- 5 (可选) 启用本地输出。
- 6 键入设备的名称。

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

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

此外，还可以输入描述和租户。

#### 7 （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。

#### 8 （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。

#### 9 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

#### 10 （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。

#### 11 （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*

## 12 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:  ▼



### 13 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

+ ✎ ✕

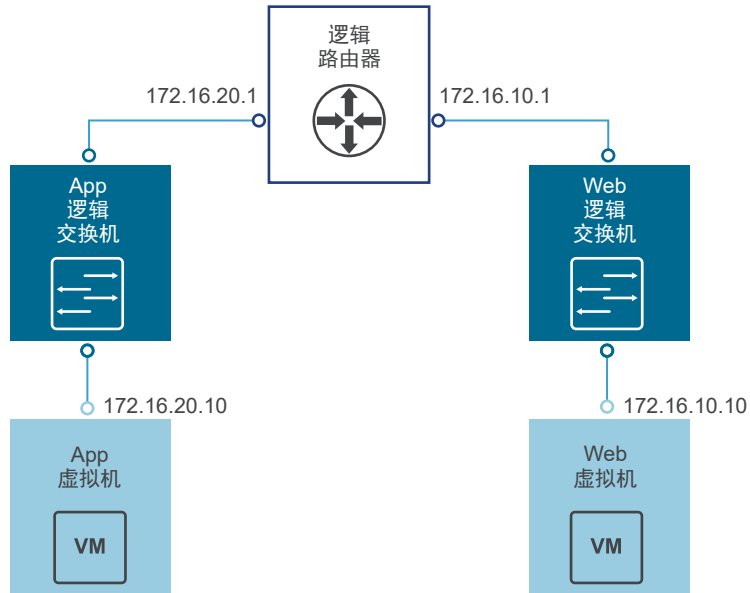
Name	IP Address	Subnet Prefix Length	Connected To
app	172.16.20.1*	24	app
web	172.16.10.1*	24	web
to-ESG	192.168.10.2*	29	transit

Back Next Finish Cancel

**14** 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	vxl	0x1389	172.16.10.1/24
13880000000a	vxl	0x1388	172.16.20.1/24
138800000002	vxl	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。

# 配置辅助 NSX Manager

# 7

在配置主 跨 vCenter NSX Manager 后，您可以配置您的辅助 NSX Manager。辅助 NSX Manager 使用主 NSX Manager 部署的相同通用控制群集。一个 跨 vCenter NSX 环境中可以存在七个辅助 NSX Manager。一旦为 NSX Manager 分配了辅助角色，它就可以使用通用逻辑交换机等通用对象。

在 跨 vCenter NSX 环境中，完成每个辅助 NSX Manager 的配置任务。

## 添加辅助 NSX Manager

在一个跨 vCenter NSX 环境中，最多可以添加七个辅助 NSX Manager。主 NSX Manager 上配置的通用对象将会同步到辅助 NSX Manager。

NSX Manager 可以拥有以下四个角色中的一个：

- 主
- 辅助
- 独立
- 转换

要查看 NSX Manager 的角色，请登录到链接至该 NSX Manager 的 vCenter，并导航到**主页 (Home) > 网络和安全 (Networking & Security) > 安装 (Installation)**，并选择**管理 (Management)**选项卡。角色显示在 NSX Manager 部分的“角色”列中。如果未显示“角色”列，则 NSX Manager 拥有独立角色。

### 前提条件

- 应该至少有两个 NSX Manager，一个担任主要角色，另一个担任独立或转换角色。
- NSX Manager（主 NSX Manager 和要为其分配辅助角色的 NSX Manager）的版本必须相匹配。
- 主 NSX Manager 和要为其分配辅助角色的 NSX Manager 必须具有节点 ID 且节点 ID 不能相同。从 OVA 文件部署的 NSX Manager 实例均有唯一的节点 ID。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 具有相同的节点 ID，并且这两个 NSX Manager 不能在同一个跨 vCenter NSX 安装中使用。

**注** 您可以使用以下 REST API 调用查看 NSX Manager 节点 ID：

```
GET https://NSX-Manager-IP-Address/api/2.0/services/vsmconfig
```

- 必须在单独的唯一 vCenter Server 系统中注册每个 NSX Manager。
- 对于所有 NSX Manager，用于 VXLAN 的 UDP 端口都必须相同。

**注** 您可以使用 vSphere Web Client 中的**网络和安全 (Networking & Security) > 安装 (Installation) > 逻辑网络准备 (Logical Network Preparation)**查看和更改 VXLAN 端口。请参阅《NSX 管理指南》中的“更改 VXLAN 端口”。

- 在为某个 NSX Manager 分配辅助角色时，链接到该 NSX Manager 的 vCenter Server 系统不能具有任何部署的 NSX Controller。
- 分配有辅助角色的 NSX Manager 的分段 ID 池不得与主 NSX Manager 的分段 ID 池或任何其他辅助 NSX Manager 的分段 ID 池重叠。
- 分配有辅助角色的 NSX Manager 必须为独立或转换角色。
- 主和辅助 NSX Manager 必须使用相同的 TLS 版本，才能正常执行通用同步。

确认辅助 NSX Manager 已配置为至少使用主 NSX Manager 上配置的一个 TLS 版本。请参见 NSX 管理指南中的“在 NSX Manager 上更改 FIPS 模式和 TLS 设置”。





#### 步骤

- 1 登录到与主 NSX Manager 链接的 vCenter。
- 2 导航到主页 (Home) > 网络和安全 (Networking & Security) > 安装 (Installation)，然后选择**管理 (Management)**选项卡。
- 3 选择主 NSX Manager。然后选择**操作 (Actions) > 添加辅助 NSX Manager (Add Secondary NSX Manager)**。
- 4 输入辅助 NSX Manager 的 IP 地址、用户名和密码。

**注** 如果主 NSX Manager 使用的是 IPv6 地址，则应使用主机名来配置辅助 NSX Manager。

- 5 单击**确定 (OK)**。
- 6 检查证书指纹是否与辅助 NSX Manager 的证书匹配。
- 7 在注册成功后，角色将从“独立”更改为“辅助”。

如果您的 vCenter Server 系统处于增强型链接模式，您可以从**主页 (Home) > 网络和安全 (Networking & Security) > 安装 (Installation)**选项卡中看到与这些 vCenter Server 系统关联的所有 NSX Manager 的角色。

NSX Manager	Role	1 ▲ IP Address	vCenter
 192.168.110.15	Primary	192.168.110.15	 vcsa-01a.corp.local
 192.168.210.15	Secondary	192.168.210.15	 vcsa-01b.corp.local

如果您的环境未采用增强型链接模式，则登录到与辅助 NSX Manager 链接的 vCenter 查看 NSX Manager 的角色。



如果未显示 NSX Manager 角色变化，请注销 vSphere Web Client 并重新登录。

**注** 最初，控制器状态可能显示为“已断开连接”。等待几秒钟，然后刷新 vSphere Web Client，此时状态应更改为“正常”。

## 准备辅助 NSX Manager 上的主机

在主机准备期间，辅助 NSX Manager 会在是 vCenter 群集成员的 ESXi 主机上安装 NSX 内核模块，并构建 NSX 控制层面和管理层面结构。封装在 VIB 文件中的 NSX 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。

### 前提条件

有关主机准备的先决条件的详细信息，请参见[准备主 NSX Manager 上的主机](#)

### 步骤

- 1 通过使用 vSphere Web Client，登录到在要修改的 NSX Manager 中注册的 vCenter Server 系统。  
如果跨 vCenter NSX 环境中的 vCenter Server 系统处于增强型链接模式，您可以从任何链接的 vCenter Server 系统中访问任何关联的 NSX Manager，方法是从 **NSX Manager** 下拉菜单中选择该 NSX Manager。
- 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 验证是否在 **NSX Manager** 下拉菜单中选择了正确的 NSX Manager。
- 4 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。

- 5 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。

## 从辅助 NSX Manager 配置 VXLAN

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。

### 前提条件

有关先决条件的详细信息，请参见[从主 NSX Manager 配置 VXLAN](#)

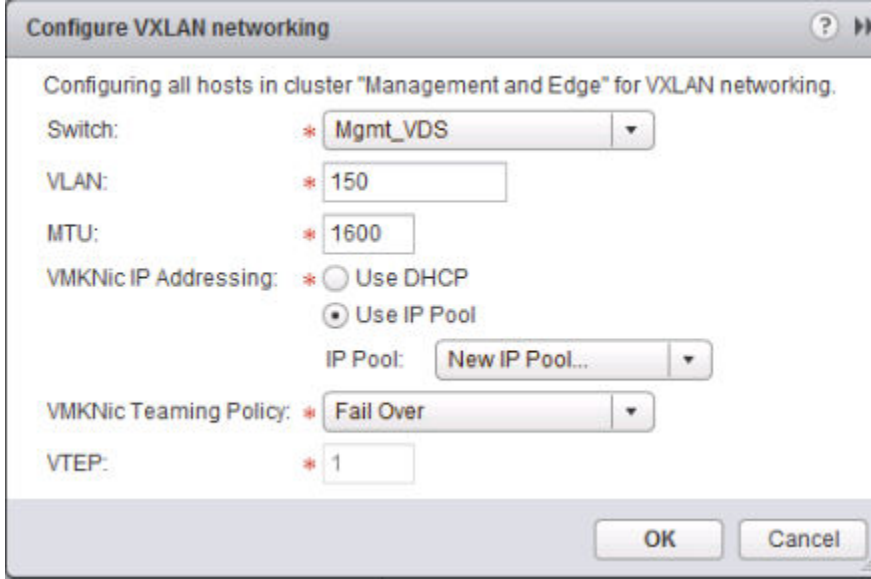
### 步骤

- 1 通过使用 vSphere Web Client，登录到在要修改的 NSX Manager 中注册的 vCenter Server 系统。  
如果跨 vCenter NSX 环境中的 vCenter Server 系统处于增强型链接模式，您可以从任何链接的 vCenter Server 系统中访问任何关联的 NSX Manager，方法是从 **NSX Manager** 下拉菜单中选择该 NSX Manager。
- 2 导航到主页 (Home) > 网络和安全 (Networking & Security) > 安装 (Installation)，然后选择主机准备 (Host Preparation) 选项卡。
- 3 验证是否在 **NSX Manager** 下拉菜单中选择了正确的 NSX Manager。
- 4 在 **VXLAN** 列中单击**未配置 (Not Configured)**。

## 5 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

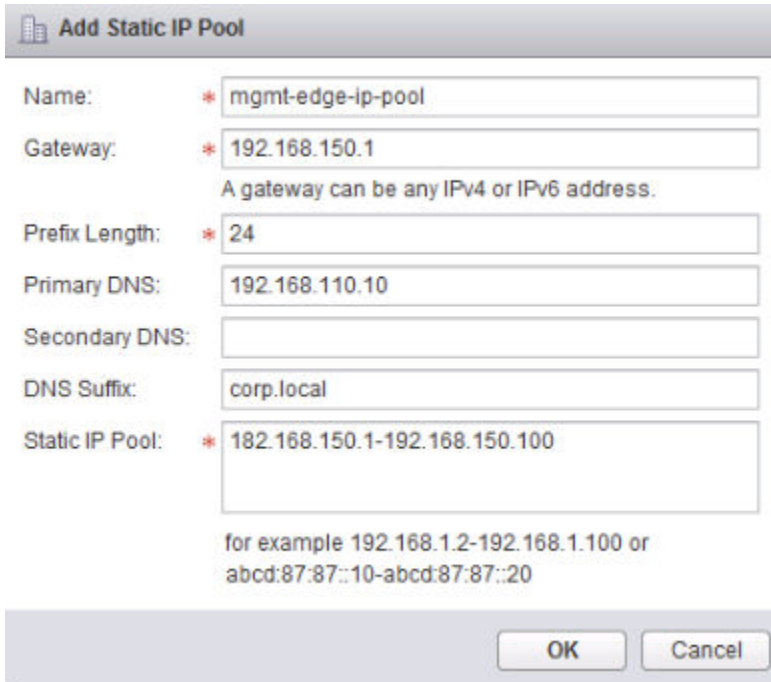
IP Pool: New IP Pool...

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。

## 为辅助 NSX Manager 分配分段 ID 池和多播地址

辅助 NSX Manager 显示通用分段 ID 池，该池是从主 NSX Manager 中同步的。此外，您还可以创建辅助 NSX Manager 的本地分段 ID 池，它用于创建该 NSX Manager 的本地逻辑交换机。如果仅创建通用逻辑交换机，则不需要添加辅助 NSX Manager 的本地分段 ID 池。

### 前提条件

有关规划分段 ID 池和多播地址的先决条件和指导的详细信息，请参阅 [为主 NSX Manager 分配分段 ID 池和多播地址](#)。

### 步骤

- 1 通过使用 vSphere Web Client，登录到在要修改的 NSX Manager 中注册的 vCenter Server 系统。  
如果跨 vCenter NSX 环境中的 vCenter Server 系统处于增强型链接模式，您可以从任何链接的 vCenter Server 系统中访问任何关联的 NSX Manager，方法是从 **NSX Manager** 下拉菜单中选择该 NSX Manager。
- 2 导航到主页 (Home) > 网络和安全 (Networking & Security) > 安装 (Installation) > 逻辑网络准备 (Logical Network Preparation)，然后选择分段 ID (Segment ID) 选项卡。
- 3 验证是否在 **NSX Manager** 下拉菜单中选择了正确的 NSX Manager。
- 4 输入本地分段 ID 的范围，如 **20000–29999**。

---

**小心** 为本地和通用分段 ID 指定的范围不能重叠。

---

- 5 （可选）如果任何传输区域将使用多播或混合复制模式，请选中**启用多播寻址 (Enable multicast addressing)**，并输入一个多播地址或多播地址范围。

---

**小心** 确认指定的多播地址与跨 vCenter NSX 环境中任何 NSX Manager 上分配的任何其他多播地址不存在冲突。

---

### 结果

辅助 NSX Manager 现在拥有导入的由主 NSX Manager 提供的通用分段 ID 以及本地分段 ID。

## 向通用传输区域添加群集

您必须将与辅助 NSX Manager 关联的群集添加到通用传输区域中。这样，您就可以将这些群集上的虚拟机连接到通用逻辑交换机。

### 步骤

- 1 通过使用 vSphere Web Client，登录到在要修改的 NSX Manager 中注册的 vCenter Server 系统。  
如果跨 vCenter NSX 环境中的 vCenter Server 系统处于增强型链接模式，您可以从任何链接的 vCenter Server 系统中访问任何关联的 NSX Manager，方法是从 **NSX Manager** 下拉菜单中选择该 NSX Manager。

- 2 导航到主页 (Home) > 网络和安全 (Networking & Security) > 安装 (Installation) > 逻辑网络准备 (Logical Network Preparation)，然后选择传输区域 (Transport Zones) 选项卡。
- 3 验证是否在 **NSX Manager** 下拉菜单中选择了正确的 NSX Manager。
- 4 选择通用传输区域，并单击操作 (Actions) () > 连接群集 (Connect Clusters)。选择要添加到通用传输区域的群集并单击“确定”。

# 配置主 NSX Manager 和辅助 NSX Manager 之后

## 8

您现在拥有了一个已配置的主 NSX Manager 和至少一个辅助 NSX Manager。除了从主 NSX Manager 中创建通用对象以外，您还可以创建该特定 vCenter NSX 环境的本地对象，如逻辑交换机、逻辑（分布式）路由器和 Edge 服务网关。这些路由器可以在主 NSX Manager 或辅助 NSX Manager 上创建。这些对象仅存在于创建它们的 vCenter NSX 环境中。这些对象在跨 vCenter NSX 环境中的其他 NSX Manager 上将不可见。另外，您可以在群集中添加或移除主机。

有关您可能想要完成的其他管理任务的信息，请参见 NSX 管理指南。

# 卸载 NSX 组件

# 9

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：

- 从准备 NSX 部署的群集中移除主机
- 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

## 从准备 NSX 部署的群集中移除主机

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`

## 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。在跨 vCenter NSX 环境中，您必须从所有 NSX Manager 上的通用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)**。

如果要卸载通用逻辑交换机，主和辅助 NSX Manager 上的通用逻辑交换机可能连接了虚拟机。对于跨 vCenter NSX 环境中的所有 NSX Manager，重复这些步骤以从通用逻辑交换机中移除所有虚拟机。

- 3 选择逻辑交换机之后，请单击**删除 (Delete)** (  ) 图标。

如果要卸载通用逻辑交换机，您必须从主 NSX Manager 中删除该交换机。

## 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[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，这样可以使虚拟机继续运行。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

完全卸载 NSX 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 创建的设备，例如 NSX Edge 设备。请务必使用 vSphere Web Client 的“网络和安全”选项卡管理和移除这些设备。

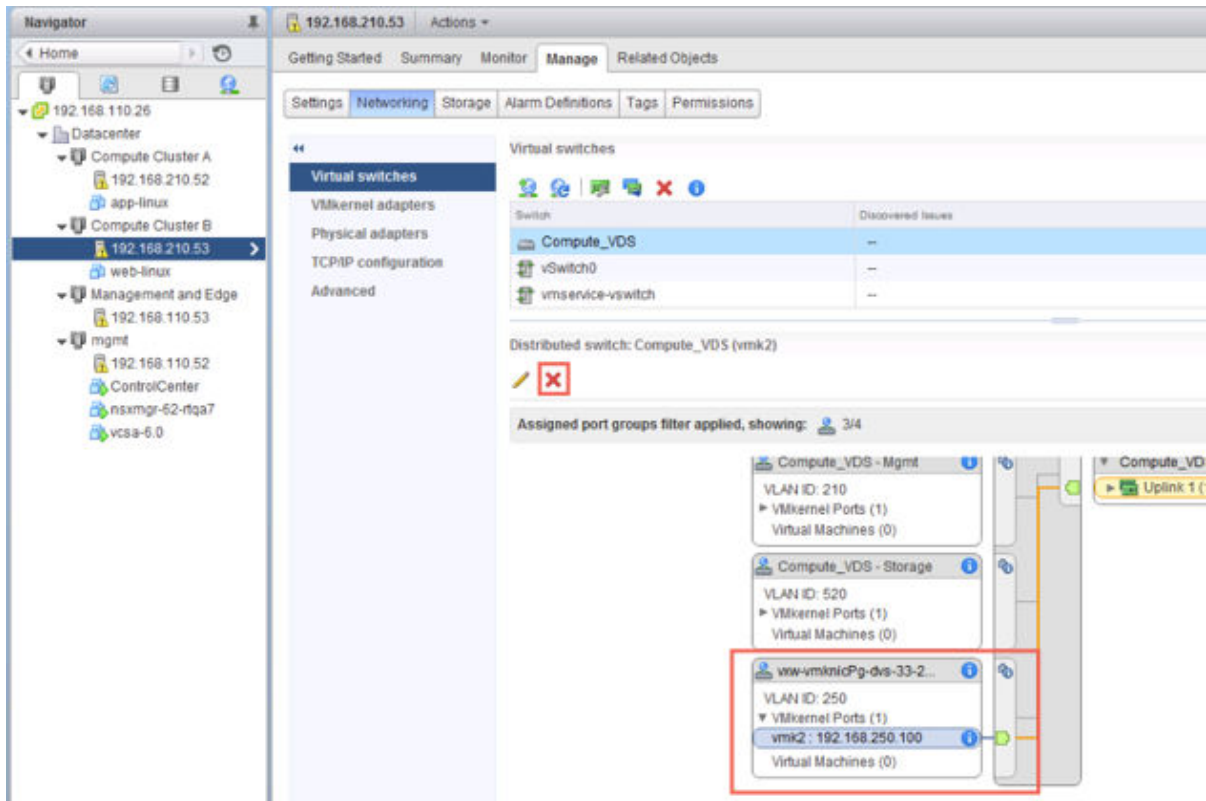
### 前提条件

- 您必须已获得企业管理员或 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。

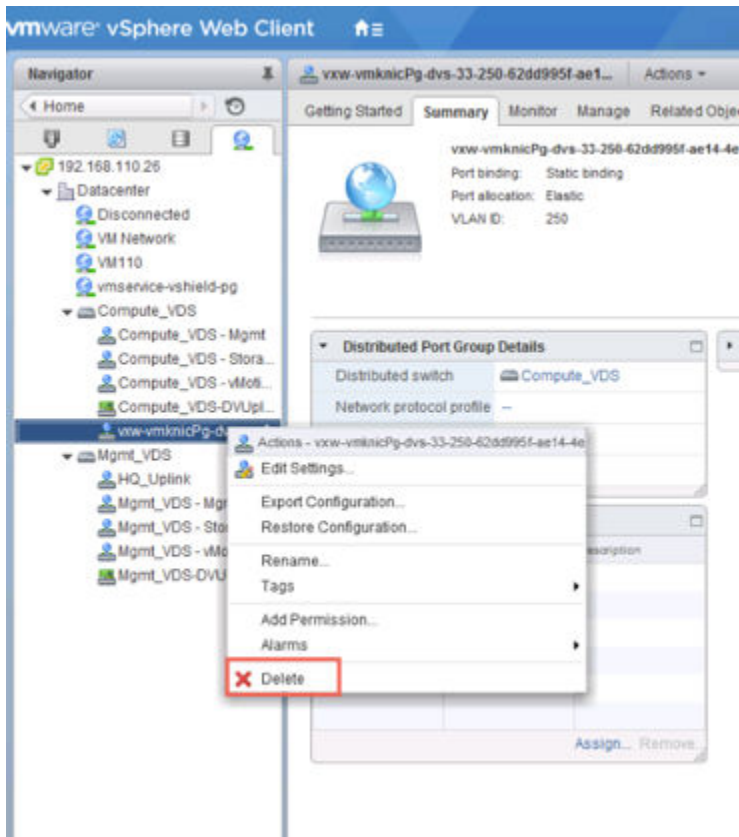
例如：



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。

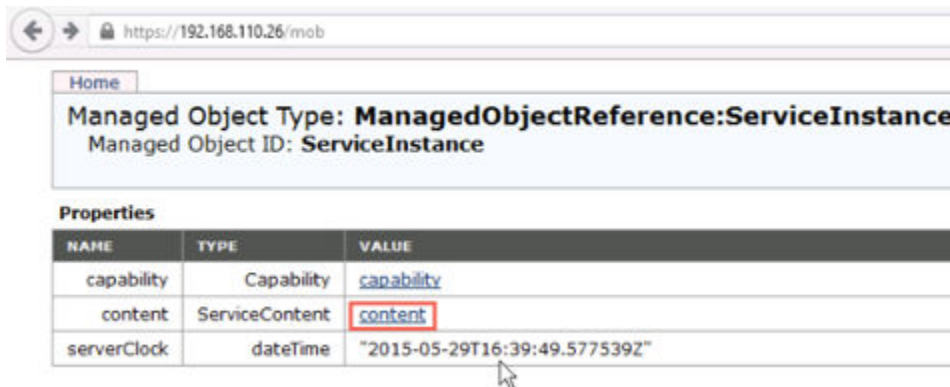
例如：



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="#">DVSManager</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="#">questOperationsManager</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**

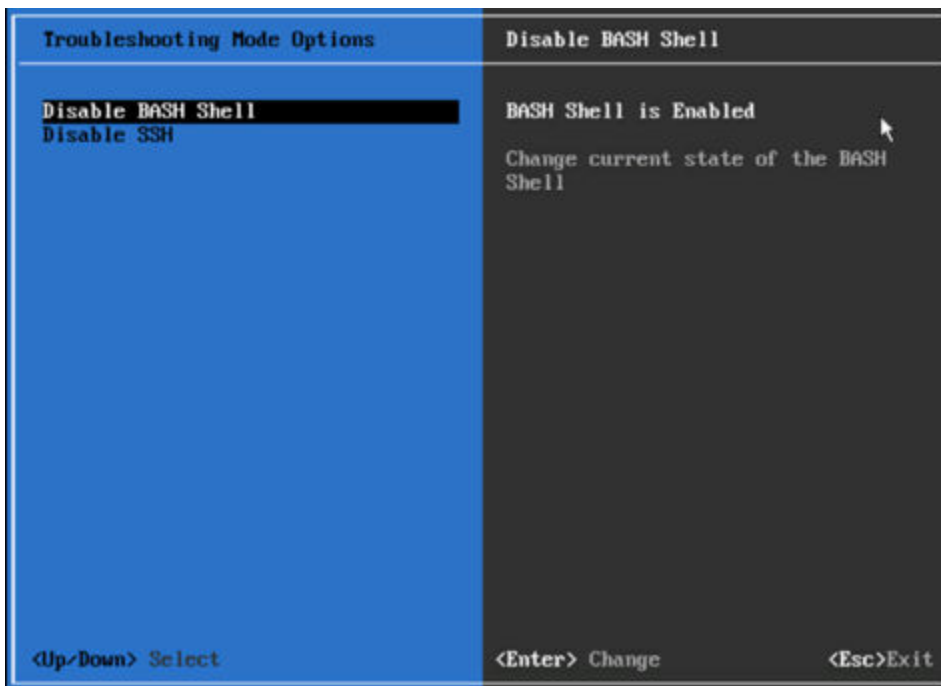
**void UnregisterExtension**

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：

- vCenter Server 5.x
  - Windows 2003 - %ALLUSERSPROFILE%\Application Data\VMware\vSphere Web Client\vc-packages\vsphere-client-serenity\

- Windows 2008/2012 - %ALLUSERSPROFILE%\VMware\vsphere Web Client\vc-packages\vsphere-client-serenity\
  - VMware vCenter Server Appliance - /var/lib/vmware/vsphere-client/vc-packages/vsphere-client-serenity/
- vCenter Server 6.0.x
  - Windows 2008/2012 - 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/

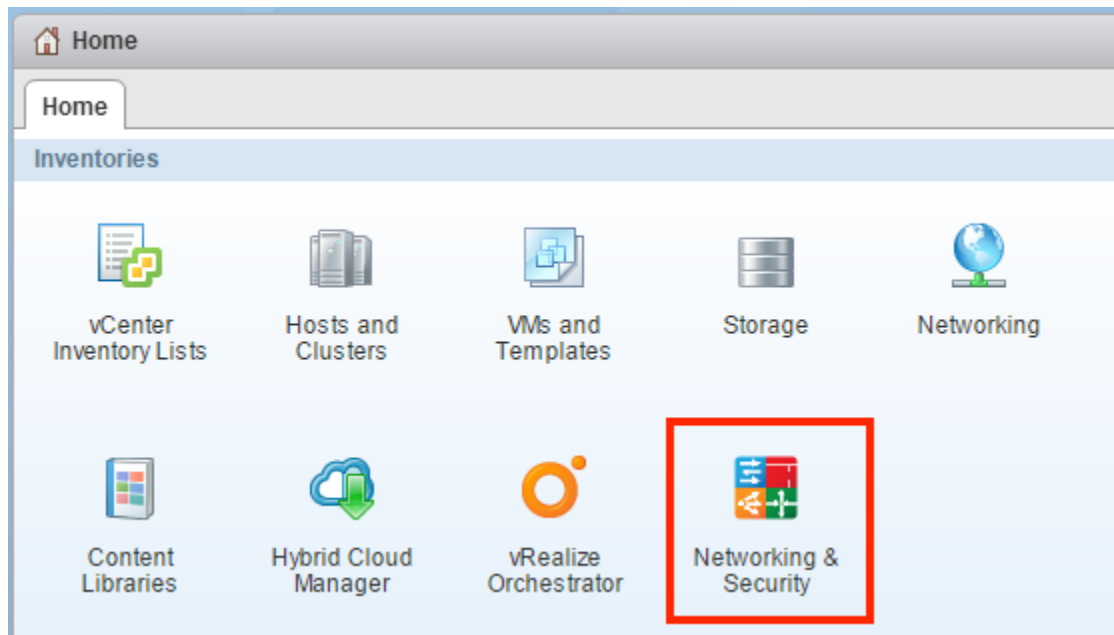
对于 vCenter Server Appliance, 请在设备 shell 中运行 `service vsphere-client restart` 命令。

对于基于 Windows 的 vCenter, 请运行 `services.msc`, 右键单击 **vSphere Web Client**, 然后单击 **启动 (Start)**。

## 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)**。



