NSX-T Data Center 安装指南

修改日期：2020 年 2 月 28 日
VMware NSX-T Data Center 2.4

vmware®

您可以从 VMware 网站下载最新的技术文档：

https://docs.vmware.com/cn/。

如果您对本文档有任何意见或建议，请将反馈信息发送至：

docfeedback@vmware.com

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

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

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

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

目录

NSX-T Data Center 安装指南

NSX-T Data Center 安装指南 说明了如何安装 VMware NSX-T™ Data Center 产品。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

本文档中的信息适用于要安装使用 NSX-T Data Center 的用户。这些信息是为熟悉虚拟机技术和网络虚拟化概念且经验丰富的系统管理员编写的。

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-T Data Center 概述

1

与服务器虚拟化以编程方式创建和管理虚拟机的方式相同，NSX-T Data Center 网络虚拟化也以编程方式创建和管理基于软件的虚拟网络。

通过网络虚拟化，与网络管理程序功能等效的组件以软件形式再现一整套第 2 层至第 7 层网络服务（例如，交换、路由、访问控制、防火墙和 QoS）。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。

NSX-T Data Center 的工作方式是实现三个单独但集成的层面：管理、控制和数据。这些层面是作为位于两种类型的节点上的一组进程、模块和代理实现的：NSX Manager 和传输节点。

- 每个节点托管一个管理平面代理。
- NSX Manager 节点托管 API 服务和管理平面集群守护进程。
- NSX Controller 节点托管中央控制平面集群守护进程。
- 传输节点托管本地控制平面守护进程和转发引擎。

NSX Manager 提供了三节点集群支持，在节点集群上合并了策略管理器、管理和中央控制服务。NSX Manager 集群提供用户界面和 API 的高可用性。管理和控制平面节点的融合减少了必须由 NSX-T Data Center 管理员部署和管理的虚拟设备数。

针对不同的部署方案，NSX Manager 设备以三种不同的大小提供。用于实验室或概念证明部署的小型设备。最多可部署 64 个主机的中型设备，以及针对部署到大型环境的客户的大型设备。请参见 NSX Manager 虚拟机系统要求和配置最大值工具。

本章讨论了以下主题：

重要概念

在文档和用户界面中使用的常见 NSX-T Data Center 概念。

计算管理器	计算管理器是一个管理资源（如主机和虚拟机）的应用程序。一个示例是 vCenter Server。
控制平面	根据管理平面中的配置计算运行时状态。控制平面传播数据平面元素报告的拓扑信息，并将无状态配置推送到转发引擎。
数据平面	根据控制平面填充的表执行无状态数据包转发或转换。数据平面向控制平面报告拓扑信息以及维护数据包级别统计信息。
外部网络	不是由 NSX-T Data Center 管理的物理网络或 VLAN。您可以通过 NSX Edge 将逻辑网络或覆盖网络链接到外部网络。例如，客户数据中心的物理网络或物理环境中的 VLAN。
Fabric 节点	已在 NSX-T Data Center 管理平面中注册并安装了 NSX-T Data Center 模块的主机。要使管理程序主机或 NSX Edge 成为 NSX-T Data Center 覆盖网络的一部分，必须将该主机添加到 NSX-T Data Center Fabric 中。
逻辑端口输出	离开虚拟机或逻辑网络的出站网络流量称为输出，因为流量离开虚拟网络并进入数据中心。
逻辑端口输入	离开数据中心并进入虚拟机的入站网络流量称为输入流量。
逻辑路由器	NSX-T Data Center 路由实体。
逻辑路由器端口	可以将逻辑交换机端口或物理网络的上行链路端口连接到的逻辑网络端口。
逻辑交换机	为虚拟机接口和网关接口提供虚拟第 2 层交换的实体。逻辑交换机为租户网络管理员提供物理第 2 层交换机的逻辑等效项，从而允许他们将一组虚拟机连接到一个通用广播域。逻辑交换机是一个独立于物理管理程序基础架构的逻辑实体并跨很多管理程序，从而连接虚拟机而不考虑它们所在的物理位置。 在多租户云中，很多逻辑交换机可能在同一管理程序硬件上并列存在，并且每个第 2 层分段与其他分段隔离。可以使用逻辑路由器连接逻辑交换机，逻辑路由器可以提供连接到外部物理网络的上行链路端口。
逻辑交换机端口	用于建立到虚拟机网络接口或逻辑路由器接口的连接的逻辑交换机连接点。逻辑交换机端口报告应用的交换配置文件、端口状态和链路状态。
管理平面	提供系统的单个 API 入口点，永久保留用户配置，处理用户查询以及在系统中的所有管理、控制和数据平面节点上执行操作任务。管理平面还负责查询、修改和永久保留用户配置。
NSX Edge 集群	具有与高可用性监控中涉及的协议相同的设置的 NSX Edge 节点设备集合。
NSX Edge 节点	功能目标是提供计算能力以提供 IP 路由和 IP 服务功能的组件。

NSX 管理的虚拟分布式交换机或 KVM Open vSwitch	NSX 管理的虚拟分布式交换机（N-VDS，以前称为主机交换机）或 OVS 用于共享 NSX Edge 和计算集群。覆盖网络流量配置需要 N-VDS。 N-VDS 有两种模式：标准和增强型数据路径。增强型数据路径 N-VDS 的性能功能支持网络功能虚拟化 (Network Functions Virtualization, NFV) 工作负载。
NSX Manager	托管 API 服务、管理平面和代理服务的节点。NSX Manager 是 NSX-T Data Center 安装软件包中包含的一个设备。可以使用 nsx-manager、nsx-controller 或 nsx-cloud-service-manager 角色部署该设备。当前，设备一次仅支持一个角色。
NSX Manager 集群	可以提供高可用性的 NSX Manager 的集群。
Open vSwitch (OVS)	作为 XenServer、Xen、KVM 和其他基于 Linux 的管理程序中的虚拟交换机的开源软件交换机。
覆盖逻辑网络	使用“第 3 层中的第 2 层”隧道实现的逻辑网络，将虚拟机看到的拓扑从物理网络中解耦出来。
物理接口 (pNIC)	在其中安装管理程序的物理服务器上的网络接口。
分段	为虚拟机接口和网关接口提供虚拟第 2 层交换的实体。分段为租户网络管理员提供物理第 2 层交换机的逻辑等效项，从而允许他们将一组虚拟机连接到一个通用广播域。分段是一个独立于物理管理程序基础架构的逻辑实体并跨很多管理程序，从而连接虚拟机而不考虑它们所在的物理位置。分段也称为逻辑交换机。 在多租户云中，很多分段可能在同一管理程序硬件上并列存在，并且每个第 2 层分段与其他分段隔离。分段可以使用网关（可提供到外部物理网络的连接）进行连接。
Tier-0 网关或 Tier-0 逻辑路由器	Tier-0 网关在**高级网络和安全**选项卡中称为“Tier-0 逻辑路由器”。它与物理网络连接，且可以作为活动-活动或活动-备用集群实现。Tier-0 网关运行 BGP 并作为物理路由器的对等项。在活动-备用模式下，该网关还可以提供有状态服务。
Tier-1 网关或 Tier-1 逻辑路由器	Tier-1 网关在**高级网络和安全**选项卡中称为“Tier-1 逻辑路由器”。它连接到一个 Tier-0 网关以建立北向连接，并连接到一个或多个覆盖网络以建立南向连接。Tier-1 网关可以是提供有状态服务的活动-备用集群。
传输区域	定义逻辑交换机的最大范围的传输节点集合。传输区域表示一组以类似方式置备的管理程序以及连接这些管理程序上的虚拟机的逻辑交换机。
传输节点	可以加入 NSX-T Data Center 覆盖网络或 NSX-T Data Center VLAN 网络的节点。对于 KVM 主机，您可以预配置 N-VDS，也可以让 NSX Manager 执行配置。对于 ESXi 主机，NSX Manager 始终配置 N-VDS。
上行链路配置文件	定义管理程序主机到 NSX-T Data Center 逻辑交换机或 NSX Edge 节点到架顶式交换机的链路策略。上行链路配置文件定义的设置可能包括绑定策略、

	活动/备用链路、传输 VLAN ID 以及 MTU 设置。上行链路配置文件中设置的传输 VLAN 仅标记覆盖网络流量，并且 VLAN ID 由 TEP 端点使用。
虚拟机接口 (vNIC)	虚拟机上的网络接口，它在虚拟客户机操作系统和标准 vSwitch 或 vSphere Distributed Switch 之间提供连接。可以将 vNIC 连接到一个逻辑端口。您可以根据其唯一 ID (UUID) 识别 vNIC。
虚拟隧道端点	每个管理程序具有一个虚拟隧道端点 (Virtual Tunnel Endpoint, VTEP)，负责将虚拟机流量封装在 VLAN 标头中，并将数据包路由到目标 VTEP 以进行进一步的处理。可以将流量路由到其他主机或 NSX Edge 网关上的其他 VTEP 以访问物理网络。

NSX Manager 概览

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

NSX Manager Web 界面提供了两种配置资源的方法。

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

何时使用“策略”或“高级”界面

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

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

表 1-1. 何时使用”策略“或”高级“界面

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

表 1-1. 何时使用“策略”或“高级”界面 （续）

“策略”界面	“高级”界面
仅在“策略”界面中提供的网络连接功能： ■ DNS 服务和 DNS 区域 ■ VPN ■ NSX Cloud 转发策略	仅在“高级”界面中提供的网络连接功能： ■ IPv4 和 IPv6 第 3 层转发 ■ 转发启动定时器 ■ 更改内部转换网络 IP ■ Tier-0 上的 VIP HA 支持 ■ 备用重新放置 ■ 根据 Tier-1 上的前缀列表进行路由通告筛选 ■ 环回创建 ■ BGP 多跃点 ■ BGP 源地址 ■ 以 BFD 和接口作为下一跃点的静态路由 ■ 元数据代理 ■ 连接到隔离分段和静态绑定的 DHCP 服务器
仅在“策略”界面中提供的安全功能： ■ 端点保护 ■ 网络侦测（东西向服务插入） ■ 上下文配置文件 ■ L7 应用程序 ■ FQDN ■ 新的分布式防火墙和网关防火墙布局 ■ 类别 ■ 自动服务规则	仅在“高级”界面中提供的安全功能： ■ 启用或禁用分布式防火墙、身份防火墙和网关防火墙的功能 ■ 分布式防火墙会话定时器 ■ 排除列表 ■ CPU 和内存阈值 ■ 无状态规则的部分 ■ 网桥防火墙 ■ 区域锁定 ■ 分布式防火墙规则 ID ■ 基于源和目标中的 IP 的分布式防火墙规则

使用“策略”界面

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

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

在何处可以找到“策略”界面和“高级”界面

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

表 1-2. “策略”界面和“高级”界面

“策略”界面	“高级”界面
■ **网络**选项卡 ■ **安全** 选项卡 ■ **清单**选项卡 ■ **安全规划和故障排除**选项卡	**高级网络和安全**选项卡
以 `/policy/api` 开头的 API URI	以 `/api` 开头的 API URI

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

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

在“策略”界面和“高级”界面中所创建的对象的名称

您创建的对象具有不同的名称，具体取决于创建这些对象时所使用的界面。

表 1-3. 对象名称

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

NSX-T Data Center 安装工作流

2

您可以在 vSphere 或 KVM 主机上安装 NSX-T Data Center。还可以配置要使用 NSX-T Data Center 的裸机服务器。

要安装或配置任何虚拟化管理程序或裸机，请遵循工作流中的建议任务。

本章讨论了以下主题：

- vSphere 的 NSX-T Data Center 工作流
- KVM 的 NSX-T Data Center 安装工作流
- 裸机服务器的 NSX-T Data Center 配置工作流

vSphere 的 NSX-T Data Center 工作流

在 vSphere 主机上使用对照表跟踪安装进度。

请遵循建议的过程顺序。

1 查看 NSX Manager 安装要求。请参见 NSX Manager 安装。

2 配置必要的端口和协议。请参见 端口和协议。

3 安装 NSX Manager。请参见安装 NSX Manager 和可用设备。

4 登录到新创建的 NSX Manager。请参见登录到新创建的 NSX Manager 。

5 配置计算管理器。请参见添加计算管理器。

6 部署其他 NSX Manager 设备以形成群集。请参见从 UI 部署 NSX Manager 节点以形成群集。

7 查看 NSX Edge 安装要求。请参见 NSX Edge 安装。

8 安装 NSX Edge。请参见使用 vSphere GUI 在 ESXi 上安装 NSX Edge。

9 创建 NSX Edge 群集。请参见创建 NSX Edge 群集。

10 创建传输区域。请参见创建传输区域。

11 创建主机传输节点。请参见 创建独立主机或裸机服务器传输节点或配置受管主机传输节点。

   在每个主机上创建虚拟交换机。管理层面将主机证书发送到控制层面，并且管理层面将控制层面信息推送到主机。每个主机通过 SSL 连接到控制层面以提供其证书。控制层面根据管理层面提供的主机证书验证该证书。在成功验证后，控制器将接受该连接。

安装后

如果主机是传输节点，您可以随时通过 NSX Manager UI 或 API 创建传输区域、逻辑交换机、逻辑路由器和其他网络组件。在 NSX Edge 和主机加入管理层面时，将自动向 NSX Edge 和主机推送 NSX-T Data Center 逻辑实体和配置状态。

有关详细信息，请参见 NSX-T Data Center 管理指南。

KVM 的 NSX-T Data Center 安装工作流

在 KVM 主机上使用对照表跟踪安装进度。

请遵循建议的过程顺序。

1 准备 KVM 环境。请参见设置 KVM。

2 查看 NSX Manager 安装要求。请参见 NSX Manager 安装。

3 配置必要的端口和协议。请参见 端口和协议。

4 安装 NSX Manager。请参见在 KVM 上安装 NSX Manager 。

5 登录到新创建的 NSX Manager。请参见登录到新创建的 NSX Manager 。

6 在 KVM 主机上配置第三方软件包。请参见在 KVM 主机上安装第三方软件包。

7 部署其他 NSX Manager 设备以形成群集。请参见使用 CLI 部署 NSX Manager 节点以形成群集 。

8 查看 NSX Edge 安装要求。请参见 NSX Edge 安装。

9 安装 NSX Edge。请参见使用 ISO 文件或 PXE 安装 NSX Edge。

10 创建 NSX Edge 群集。请参见创建 NSX Edge 群集。

11 创建传输区域。请参见创建传输区域。

12 创建主机传输节点。请参见 创建独立主机或裸机服务器传输节点。

   在每个主机上创建虚拟交换机。管理层面将主机证书发送到控制层面，并且管理层面将控制层面信息推送到主机。每个主机通过 SSL 连接到控制层面以提供其证书。控制层面根据管理层面提供的主机证书验证该证书。在成功验证后，控制器将接受该连接。

安装后

如果主机是传输节点，您可以随时通过 NSX Manager UI 或 API 创建传输区域、逻辑交换机、逻辑路由器和其他网络组件。在 NSX Edge 和主机加入管理层面时，将自动向 NSX Edge 和主机推送 NSX-T Data Center 逻辑实体和配置状态。

有关详细信息，请参见 NSX-T Data Center 管理指南。

裸机服务器的 NSX-T Data Center 配置工作流

将裸机服务器配置为使用 NSX-T Data Center 时，使用对照表跟踪进度。

请遵循建议的过程顺序。

1 查看裸机要求。请参见裸机服务器系统要求。

2 配置必要的端口和协议。请参见 端口和协议。

3 安装 NSX Manager。请参见在 KVM 上安装 NSX Manager 。

4 在裸机服务器上配置第三方软件包。请参见在裸机服务器上安装第三方软件包。

5 创建主机传输节点。请参见 创建独立主机或裸机服务器传输节点。

   在每个主机上创建虚拟交换机。管理层面将主机证书发送到控制层面，并且管理层面将控制层面信息推送到主机。每个主机通过 SSL 连接到控制层面以提供其证书。控制层面根据管理层面提供的主机证书验证该证书。在成功验证后，控制器将接受该连接。

6 创建裸机服务器工作负载的应用程序接口。请参见创建裸机服务器工作负载的应用程序接口。

安装准备工作

3

在安装 NSX-T Data Center 之前，请确保准备您的环境。

本章讨论了以下主题：

- 系统要求
- 端口和协议
- 安装 NSX-T Data Center 组件

系统要求

在安装 NSX-T Data Center 之前，您的环境必须满足特定的硬件和资源要求。

NSX Manager 虚拟机系统要求

在安装 NSX Manager 之前，请确保您的环境满足支持的要求。

传输节点的管理程序主机要求

管理程序	版本	CPU 内核	内存
vSphere	支持的 vSphere 版本	4	16 GB
CentOS Linux KVM	7.4	4	16 GB
Red Hat Enterprise Linux (RHEL) KVM	7.6、7.5 和 7.4	4	16 GB
SUSE Linux Enterprise Server KVM	12 SP3、SP4	4	16 GB
Ubuntu KVM	18.04 和 16.04.2 LTS	4	16 GB

表 3-1. NSX Manager 支持的主机

支持说明	管理程序
ESXi	有关支持的主机，请参见 VMware 产品互操作性列表。
KVM	RHEL 7.4 和 Ubuntu 16.04 LTS

对于 ESXi 主机，NSX-T Data Center 支持 vSphere 6.7 U1 或更高版本上的主机配置文件和自动部署功能。有关详细信息，请参见《VMware ESXi 安装和设置》文档中的了解 vSphere Auto Deploy。

小心 在 RHEL 上，`yum update` 命令可能会更新内核版本并破坏与 NSX-T Data Center 的兼容性。运行 `yum update` 时，禁用自动内核更新。此外，运行 `yum install` 后，确认 NSX-T Data Center 支持内核版本。

管理程序主机网络要求

运行 NSX-T Data Center 的管理程序主机需要具有兼容的网卡。有关支持的网卡，请参见《VMware 兼容性指南》。

提示 要快速识别该兼容性指南中提及的兼容网卡，请应用以下条件：

- 在 **I/O 设备类型**下方，选择**网络**。
- （可选）要使用支持的 GENEVE 封装，请在**功能**下方选择 GENEVE 选项。
- （可选）要使用增强型数据路径，请选择 **N–VDS 增强型数据路径**。

增强型数据路径网卡驱动程序

从 My VMware 页面下载支持的网卡驱动程序。

网卡	网卡驱动程序
Intel 82599	ixgben 1.1.0.26-1OEM.670.0.0.7535516
Intel(R) Ethernet Controller X710 for 10GbE SFP+ Intel(R) Ethernet Controller XL710 for 40GbE QSFP+	i40en 1.2.0.0-1OEM.670.0.0.8169922

NSX Manager 虚拟机资源要求

精简虚拟磁盘大小为 3.8 GB，厚虚拟磁盘大小为 200 GB。

设备大小	内存	vCPU	磁盘空间	虚拟机硬件版本
NSX Manager 超小型	8 GB	2	200 GB	10 或更高版本
NSX Manager 小型虚拟机	16 GB	4	200 GB	10 或更高版本

设备大小	内存	vCPU	磁盘空间	虚拟机硬件版本
NSX Manager 中型虚拟机	24 GB	6	200 GB	10 或更高版本
NSX Manager 大型虚拟机	48 GB	12	200 GB	10 或更高版本

注 从 NSX-T 2.4 开始，NSX Manager 提供了多个以前需要使用单独设备的角色。这包括策略角色、管理平面角色和中央控制平面角色。中央控制平面角色以前是由 NSX Controller 设备提供的。

- NSX Manager 超小型虚拟机资源要求仅适用于 Cloud Service Manager。
- NSX Manager 小型虚拟机设备大小适用于实验室和概念证明部署，而不能在生产中使用。
- NSX Manager 中型虚拟机设备大小适用于典型生产环境，最多可以支持 64 个管理程序。
- NSX Manager 大型虚拟机设备大小适用于具有超过 64 个管理程序的大型部署。

有关使用 NSX Manager 大型虚拟机设备大小的最大规模，请转到 VMware 最高配置工具 (https://configmax.vmware.com/guest)，然后从产品列表中选择 NSX-T Data Center。

NSX Manager 浏览器支持

建议在使用 NSX Manager 时使用以下浏览器。

浏览器	Windows 10	Mac OS X 10.13、10.14	Ubuntu 18.04
Google Chrome 76	是	是	是
Mozilla Firefox 68	是	是	是
Microsoft Edge 44	是		
Apple Safari 12		是	

注

- 不支持 Internet Explorer。
- 支持的浏览器最小分辨率为 1280 x 800 像素。
- 语言支持：NSX Manager 已本地化为多种语言：英语、德语、法语、日语、简体中文、韩语、繁体中文和西班牙语。但是，由于 NSX Manager 本地化使用浏览器的语言设置，因此，请确保您的设置与所需的语言相匹配。NSX Manager 界面本身没有语言首选项设置。

网络延迟要求

NSX Manager 集群中各 NSX Manager 之间的最大网络延迟为 10 毫秒。

NSX Manager 和传输节点之间的最大网络延迟为 150 毫秒。

存储要求

- 最大磁盘访问延迟低于 10 毫秒。
- 建议将 NSX Manager 放在共享存储上。

- 存储应具有高可用性以避免存储中断，从而导致在发生存储故障时将所有 NSX Manager 文件系统置于只读模式。

  有关如何以最佳方式设计高可用性存储解决方案的信息，请参阅您的存储技术文档。

NSX Edge 虚拟机系统要求

在安装 NSX Edge 之前，请确保您的环境满足支持的要求。

仅在具有基于 Intel 的芯片组的基于 ESXi 的主机上支持 NSX Edge 节点。否则，vSphere EVC 模式可能会禁止启动 NSX Edge 节点，并在控制台中显示错误消息。

注 NSX Edge 虚拟机仅支持 VMXNET 3 vNIC。

NSX Cloud 注意 如果使用 NSX Cloud，请注意，将按照每个受支持公有云的单一默认大小部署 NSX Public Cloud Gateway(PCG)。有关详细信息，请参见部署或链接 NSX Public Cloud Gateway。

NSX Edge 虚拟机资源要求

设备大小	内存	vCPU	磁盘空间	虚拟机硬件版本
NSX Edge 小型	4 GB	2	200 GB	11 或更高版本（vSphere 6.0 或更高版本）
NSX Edge 中型	8 GB	4	200 GB	11 或更高版本（vSphere 6.0 或更高版本）
NSX Edge 大型	32 GB	8	200 GB	11 或更高版本（vSphere 6.0 或更高版本）

注

- NSX Edge 小型虚拟机设备大小适用于实验室和概念证明部署。
- NSX Edge 中型设备大小适用于典型生产环境。
- NSX Edge 大型设备大小适用于具有负载均衡功能的环境。请参见《NSX-T Data Center 管理指南》中的“缩放负载均衡器资源”。

NSX Edge 虚拟机 CPU 要求

对于 DPDK 支持，底层平台需要满足以下要求：

- CPU 必须具有 AESNI 功能。
- CPU 必须具有 1 GB 巨大页面支持。

硬件	类型
CPU	■ Intel Xeon E7-xxxx（Westmere-EX 和更高版本 CPU） ■ Intel Xeon 56xx (Westmere-EP) ■ Intel Xeon E5-xxxx（Sandy Bridge 和更高版本 CPU） ■ Intel Xeon Platinum（所有版本） ■ Intel Xeon Gold（所有版本） ■ Intel Xeon Silver（所有版本） ■ Intel Xeon Bronze（所有版本）

NSX Edge 裸机要求

在配置 NSX Edge 裸机之前，请确保您的环境满足支持的要求。

仅在具有基于 Intel 的芯片组的基于 ESXi 的主机上支持 NSX Edge 节点。否则，vSphere EVC 模式可能会禁止启动 Edge 节点，并在控制台中显示错误消息。

NSX Edge 裸机内存、CPU 和磁盘要求

内存	CPU 内核	磁盘空间
32 GB	8	200 GB

NSX Edge 裸机 DPDK CPU 要求

对于 DPDK 支持，底层平台需要满足以下要求：

- CPU 必须具有 AES-NI 功能。
- CPU 必须具有 1 GB 巨大页面支持。

硬件	类型
CPU	■ Intel Xeon E7-xxxx（Westmere-EX 和更高版本 CPU） ■ Intel Xeon 56xx (Westmere-EP) ■ Intel Xeon E5-xxxx（Sandy Bridge 和更高版本 CPU） ■ Intel Xeon Platinum（所有版本） ■ Intel Xeon Gold（所有版本） ■ Intel Xeon Silver（所有版本） ■ Intel Xeon Bronze（所有版本）

NSX Edge 裸机硬件要求

确认在此 URL https://certification.ubuntu.com/server/models/?release=18.04%20LTS&category=Server 中列出了裸机 NSX Edge 硬件。如果未列出该硬件，则在 NSX Edge 设备上存储、视频适配器或主板组件可能未正常工作。

NSX Edge 裸机网卡要求

网卡类型	说明	PCI 设备 ID
Intel XXV710	I40E_DEV_ID_25G_B	0x158A
	I40E_DEV_ID_25G_SFP28	0x158B
Intel X520/Intel 82599	IXGBE_DEV_ID_82599_KX4	0x10F7
	IXGBE_DEV_ID_82599_KX4_MEZZ	0x1514
	IXGBE_DEV_ID_82599_KR	0x1517
	IXGBE_DEV_ID_82599_COMBO_BACKPLANE	0x10F8
		0x000C
	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ	0x10F9
		0x10FB
	IXGBE_DEV_ID_82599_CX4	0x11A9
	IXGBE_DEV_ID_82599_SFP	0x1F72
	IXGBE_SUBDEV_ID_82599_SFP	0x17D0
	IXGBE_SUBDEV_ID_82599_RNDC	0x0470
	IXGBE_SUBDEV_ID_82599_560FLR	0x1507
	IXGBE_SUBDEV_ID_82599_ECNA_DP	0x154D
	IXGBE_DEV_ID_82599_SFP_EM	0x154A
	IXGBE_DEV_ID_82599_SFP_SF2	0x1558
	IXGBE_DEV_ID_82599_SFP_SF_QP	0x1557
	IXGBE_DEV_ID_82599_QSFP_SF_QP	0x10FC
	IXGBE_DEV_ID_82599EN_SFP	0x151C
	IXGBE_DEV_ID_82599_XAUI_LOM	
	IXGBE_DEV_ID_82599_T3_LOM	
Intel X540	IXGBE_DEV_ID_X540T	0x1528
	IXGBE_DEV_ID_X540T1	0x1560
Intel X550	IXGBE_DEV_ID_X550T	0x1563
	IXGBE_DEV_ID_X550T1	0x15D1
Intel X710	I40E_DEV_ID_SFP_X710	0x1572
	I40E_DEV_ID_KX_C	0x1581
	I40E_DEV_ID_10G_BASE_T	0x1586
Intel XL710	I40E_DEV_ID_KX_B	0x1580
	I40E_DEV_ID_QSFP_A	0x1583
	I40E_DEV_ID_QSFP_B	0x1584
	I40E_DEV_ID_QSFP_C	0x1585
Cisco VIC 1387	Cisco UCS 虚拟接口卡 1387	0x0043

裸机服务器系统要求

在配置裸机服务器之前，请确保服务器满足支持的要求。

重要事项 执行安装的用户可能需要具有 sudo 命令权限以执行某些过程。请参见在裸机服务器上安装第三方软件包。

裸机服务器要求

操作系统	版本	CPU 内核	内存
CentOS Linux	7.4	4	16 GB
Red Hat Enterprise Linux (RHEL)	7.5 和 7.4	4	16 GB
SUSE Linux Enterprise Server	12 SP3	4	16 GB
Ubuntu	18.04 和 16.04.2 LTS	4	16 GB

裸机 Linux 容器要求

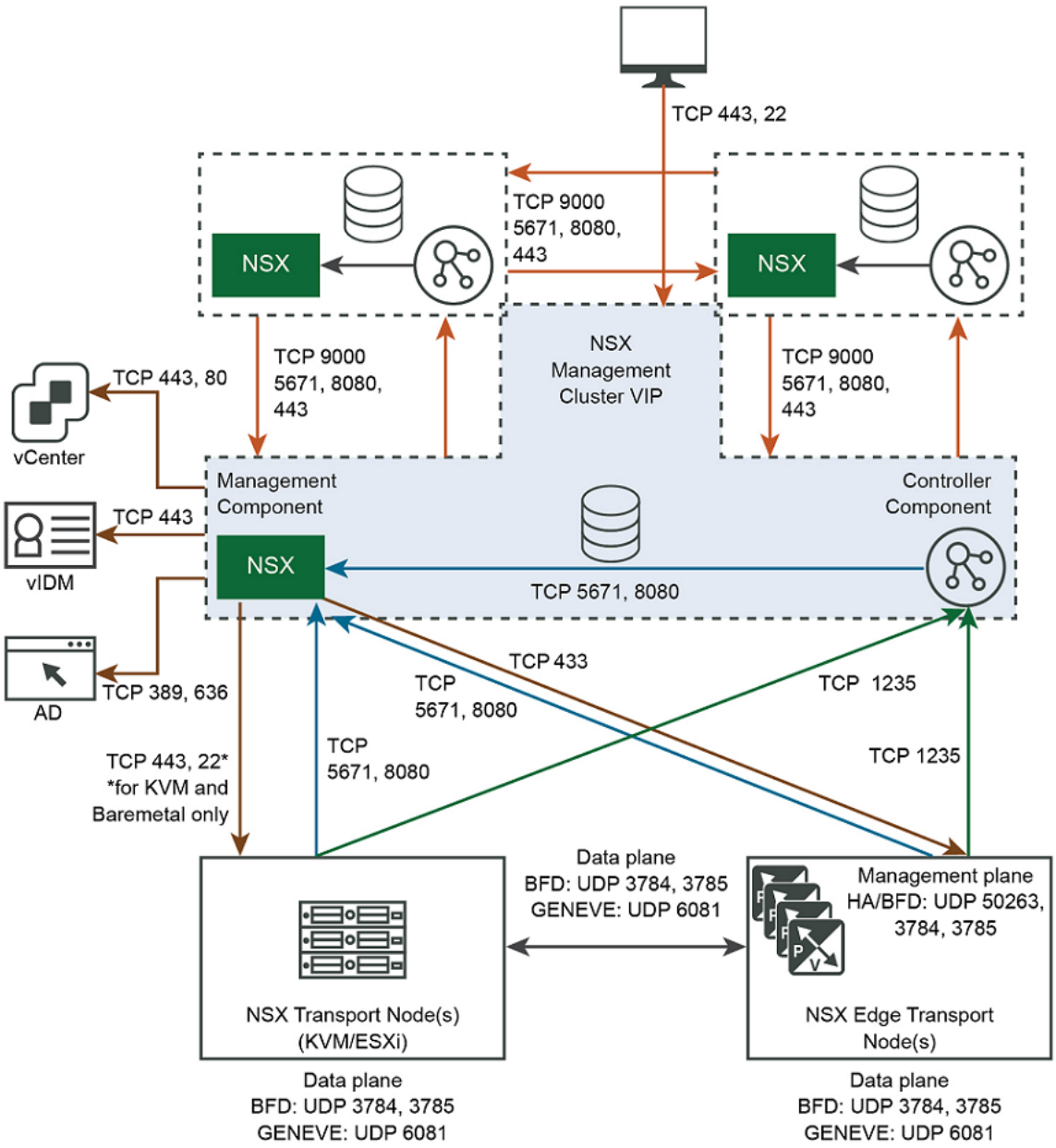
有关裸机 Linux 容器要求，请参阅《适用于 OpenShift 的 NSX Container Plug-in - 安装和管理指南》。

端口和协议

在 NSX-T Data Center 中，端口和协议允许节点到节点通信路径，保护这些路径并对其进行身份验证，并且使用凭据的存储位置建立双向身份验证。

注　必须在物理和主机管理程序防火墙上打开所需的端口和协议。

图 3-1. NSX-T Data Center 端口和协议



默认情况下，所有证书是自签名证书。CA 签名的证书可以替换北向 GUI 和 API 证书和私钥。

一些内部守护进程可以通过环回或 UNIX 域套接字进行通信：

- KVM：MPA、netcpa、nsx-agent、OVS

- ESXi：netcpa、ESX-DP（在内核中）

注 要获取对 NSX-T Data Center 节点的访问权限，必须在这些节点上启用 SSH。

NSX Cloud 说明 有关部署 NSX Cloud 所需端口的列表，请参见允许访问 CSM 上的端口和协议以实现混合连接。

NSX Manager 使用的 TCP 和 UDP 端口

NSX Manager 使用特定的 TCP 和 UDP 端口与其他组件和产品通信。必须在防火墙中打开这些端口。

您可以使用 API 调用或 CLI 命令来指定用于进行以下操作的自定义端口：传输文件（默认端口为 22）和导出 Syslog 数据（默认端口为 514 和 6514）。如果配置自定义端口，则需要对防火墙进行相应的配置。

表 3-2. NSX Manager 使用的 TCP 和 UDP 端口

源	目标	端口	协议	说明
NSX Manager	Active Directory	389	TCP	Active Directory
NSX Controller、NSX Edge 节点、传输节点	NSX Manager	5671	TCP	NSX 消息传递
NSX Controller、NSX Edge 节点、传输节点、vCenter Server	NSX Manager	8080	TCP	安装/升级 HTTP 存储库
NSX Manager	NSX Manager	9000	TCP	内部数据存储访问
NSX Manager	DNS 服务器	53	TCP	DNS
NSX Manager	DNS 服务器	53	UDP	DNS
NSX Manager	NSX Edge	443	TCP	HTTPS
NSX Manager	管理 SCP 服务器	22	TCP	SSH（上载支持包、备份等）
NSX Manager	NTP 服务器	123	UDP	NTP
NSX Manager	SNMP 服务器	161、162	TCP	SNMP
NSX Manager	SNMP 服务器	161、162	UDP	SNMP
NSX Manager	Syslog 服务器	514	TCP	Syslog
NSX Manager	Syslog 服务器	514	UDP	Syslog
NSX Manager	Syslog 服务器	6514	TCP	Syslog
NSX Manager	Syslog 服务器	6514	UDP	Syslog
NSX Manager	跟踪路由目标	33434 - 33523	UDP	跟踪路由
NSX Manager	vCenter Server	80	TCP	NSX Manager 与计算管理器 (vCenter Server) 通信（如果已配置）。

表 3-2. NSX Manager 使用的 TCP 和 UDP 端口 （续）

源	目标	端口	协议	说明
NSX Manager	vCenter Server	443	TCP	NSX Manager 与计算管理器 (vCenter Server) 通信（如果已配置）。
NSX Manager	vIDM	443	TCP	vIDM
NSX Manager	NSX Manager	443	TCP	NSX Manager 与 NSX Manager 通信
管理客户端	NSX Manager	22	TCP	SSH（默认禁用）
管理客户端	NSX Manager	443	TCP	NSX API 服务器
SNMP 服务器	NSX Manager	161	UDP	SNMP

NSX Edge 使用的 TCP 和 UDP 端口

NSX Edge 使用特定的 TCP 和 UDP 端口与其他组件和产品通信。必须在防火墙中打开这些端口。

您可以使用 API 调用或 CLI 命令来指定用于进行以下操作的自定义端口：传输文件（默认端口为 22）和导出 Syslog 数据（默认端口为 514 和 6514）。如果配置自定义端口，则需要对防火墙进行相应的配置。

表 3-3. NSX Edge 使用的 TCP 和 UDP 端口

源	目标	端口	协议	说明
管理客户端	NSX Edge 节点	22	TCP	SSH（默认禁用）
NSX 代理	NSX Edge 节点	5555	TCP	NSX Cloud - 实例上的代理与 NSX Cloud 网关通信。
NSX Edge 节点	DNS 服务器	53	UDP	DNS
NSX Edge 节点	管理 SCP 或 SSH 服务器	22	TCP	SSH（上载支持包、备份等）
NSX Edge 节点	NSX Controller 节点	1235	TCP	netcpa
NSX Edge 节点	NSX Edge 节点	1167	TCP	DHCP 后端
NSX Edge 节点	NSX Edge 节点	2480	TCP	Nestdb
NSX Edge 节点	NSX Edge 节点	6666	TCP	NSX Cloud - NSX Edge 本地通信。
NSX Edge 节点	NSX Edge 节点	50263	UDP	高可用性
NSX Edge 节点	NSX Manager 节点	443	TCP	HTTPS
NSX Edge 节点	NSX Manager 节点	5671	TCP	NSX 消息传递
NSX Edge 节点	NSX Manager 节点	8080	TCP	NAPI、NSX-T Data Center 升级

表 3-3. NSX Edge 使用的 TCP 和 UDP 端口 （续）

源	目标	端口	协议	说明
NSX Edge 节点	NTP 服务器	123	UDP	NTP
NSX Edge 节点	OpenStack Nova API 服务器	3000 - 9000	TCP	元数据代理
NSX Edge 节点	SNMP 服务器	161、162	TCP	SNMP
NSX Edge 节点	SNMP 服务器	161、162	UDP	SNMP
NSX Edge 节点	Syslog 服务器	514	TCP	Syslog
NSX Edge 节点	Syslog 服务器	514	UDP	Syslog
NSX Edge 节点	Syslog 服务器	6514	TCP	Syslog
NSX Edge 节点	Syslog 服务器	6514	UDP	Syslog
NSX Edge 节点	跟踪路由目标	33434 - 33523	UDP	跟踪路由
NSX Edge 节点、传输节点	NSX Edge 节点	3784、3785	UDP	数据中传输节点 TEP IP 地址之间的 BFD。
SNMP 服务器	NSX Edge 节点	161	UDP	SNMP

由 ESXi、KVM 主机和裸机服务器使用的 TCP 和 UDP 端口

ESXi、KVM 主机和裸机服务器用作传输节点时要求某些 TCP 和 UDP 端口可用。

表 3-4. ESXi 和 KVM 主机使用的 TCP 和 UDP 端口

源	目标	端口	协议	说明
ESXi 主机	NSX Controller	1235	TCP	控制平面 - LCP 与 CCP 通信
ESXi 主机	NSX Manager	5671	TCP	与 NSX Manager 的 AMPQ 通信通道
ESXi 主机	NSX Manager	8080	TCP	安装和升级 HTTP 存储库
ESXi 和 KVM 主机	NSX Manager	443	TCP	管理和置备连接
ESXi 和 KVM 主机	NSX Manager	443	TCP	安装和升级 HTTP 存储库
GENEVE Termination End Point (TEP)	GENEVE Termination End Point (TEP)	6081	UDP	传输网络
KVM 主机	NSX Manager	5671	TCP	与 NSX Manager 的 AMPQ 通信通道
KVM 主机	NSX Controller	1235	TCP	控制平面 - LCP 与 CCP 通信

表 3-4. ESXi 和 KVM 主机使用的 TCP 和 UDP 端口 （续）

源	目标	端口	协议	说明
KVM 主机	NSX Manager	8080	TCP	安装和升级 HTTP 存储库
NSX Manager	ESXi 主机	443	TCP	管理和置备连接
NSX Manager	KVM 主机	443	TCP	管理和置备连接
ESXi 和 KVM 主机	Syslog 服务器	514	TCP	Syslog
ESXi 和 KVM 主机	Syslog 服务器	514	UDP	Syslog
ESXi 和 KVM 主机	Syslog 服务器	6514	TCP	Syslog
ESXi 和 KVM 主机	Syslog 服务器	6514	UDP	Syslog
NSX-T Data Center 传输节点	NSX-T Data Center 传输节点	3784、3785	UDP	在使用 TEP 接口的数据路径中，TEP 之间的 BFD 会话

安装 NSX-T Data Center 组件

必须安装 NSX Manager 和 NSX Edge 核心组件才能使用 NSX-T Data Center。

NSX Manager 安装

NSX Manager 提供了图形用户界面 (GUI) 和 REST API 以创建、配置和监控 NSX-T Data Center 组件，例如，逻辑交换机、逻辑路由器和防火墙。

NSX Manager 提供了系统视图并且是 NSX-T Data Center 的管理组件。

为了获得高可用性，NSX-T Data Center 支持三个 NSX Manager 的管理集群。对于生产环境，建议部署管理集群。对于概念证明环境，可以部署单个 NSX Manager。

NSX Manager 部署、平台和安装要求

下表详细说明了 NSX Manager 部署、平台和安装要求

要求	说明
支持的部署方法	■ OVA/OVF ■ QCOW2
支持的平台	请参见 NSX Manager 虚拟机系统要求。 在 ESXi 上，建议将 NSX Manager 设备安装在共享存储上。
IP 地址	NSX Manager 必须具有静态 IP 地址。您无法在安装后更改该 IP 地址。

要求	说明
NSX-T Data Center 设备密码	■ 至少 12 个字符 ■ 至少一个小写字母 ■ 至少一个大写字母 ■ 至少一个数字 ■ 至少一个特殊字符 ■ 至少 5 个不同的字符 ■ 没有字典词语 ■ 没有回文 ■ 不允许使用超过四个单调字符的序列
主机名	在安装 NSX Manager 时，请指定不包含无效字符（如下划线）的主机名。如果主机名包含任何无效的字符，在部署后，主机名将设置为 **nsx-manager**。 有关主机名限制的详细信息，请参阅 https://tools.ietf.org/html/rfc952 和 https://tools.ietf.org/html/rfc1123。
VMware Tools	在 ESXi 上运行的 NSX Manager 虚拟机已安装 VMTools。不要移除或升级 VMTools。
系统	■ 确认满足系统要求。请参见系统要求。 ■ 确认打开了所需的端口。请参见 端口和协议。 ■ 确认配置了一个数据存储，并且可以在 ESXi 主机上访问该数据存储。 ■ 确认具有供 NSX Manager 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。 ■ 如果还没有目标虚拟机端口组网络，请创建一个网络。将 NSX-T Data Center 设备放在管理虚拟机网络上。 如果具有多个管理网络，您可以添加从 NSX-T Data Center 设备到其他网络的静态路由。 ■ 规划 NSX Manager IPv4 或 IPv6 IP 寻址方案。
OVF 特权	确认您具有足够的权限以在 ESXi 主机上部署 OVF 模板。 可部署 OVF 模板的管理工具，例如 vCenter Server 或 vSphere Client。OVF 部署工具必须支持配置选项以允许进行手动配置。 OVF 工具版本必须为 4.0 或更高版本。
客户端插件	必须安装客户端集成插件。

注 在 NSX Manager 全新安装或重新引导时，或者在首次登录出现提示时更改 **admin** 密码后，NSX Manager 可能需要几分钟的时间才会启动。

NSX Manager 安装方案

重要事项 从 vSphere Client 或命令行中通过 OVA 或 OVF 文件安装 NSX Manager 时，在打开虚拟机电源之前，不会验证 OVA/OVF 属性值（如用户名、密码或 IP 地址）。

- 如果为 **admin** 或 **audit** 用户指定用户名，该名称必须是唯一的。如果指定相同的名称，则会忽略该名称并使用默认名称（**admin** 和 **audit**）。
- 如果 **admin** 用户的密码不符合复杂性要求，您必须通过 SSH 或控制台以 **admin** 用户身份（使用密码 **default**）登录到 NSX Manager。将提示您更改密码。

- 如果 **audit** 用户的密码不符合复杂性要求，则会禁用该用户帐户。要启用该帐户，请通过 SSH 或控制台以 **admin** 用户身份登录到 NSX Manager，然后运行 **set user audit** 命令以设置 **audit** 用户的密码（当前密码为空字符串）。
- 如果 **root** 用户的密码不符合复杂性要求，您必须通过 SSH 或控制台以 **root** 身份（使用密码 **vmware**）登录到 NSX Manager。将提示您更改密码。

小心 以 **root** 用户凭据登录时对 NSX-T Data Center 进行的更改可能会导致系统出现故障，且可能会影响您的网络。只能在 Vmware 技术支持团队的指导下使用 **root** 用户凭据进行更改。

注 在设置足够复杂的密码后，设备上的核心服务才会启动。

从 OVA 文件部署 NSX Manager 后，您无法通过关闭虚拟机电源，然后从 vCenter Server 中修改 OVA 设置来更改虚拟机的 IP 设置。

配置 NSX Manager 以通过 DNS 服务器访问

默认情况下，传输节点根据 IP 地址访问 NSX Manager。不过，也可以根据 NSX Manager 的 DNS 名称进行访问。

通过在 NSX Manager 上允许使用 FQDN (DNS)，可以更改 Manager 的 IP 地址而不会影响传输节点。

您可以发布 NSX Manager 的 FQDN 以允许使用 FQDN。

注 多站点 Lite 和 NSX 以及 NSX Cloud 部署需要在 NSX Manager 上允许使用 FQDN (DNS)。（对于所有其他部署类型，这是可选的。）请参见《NSX-T Data Center 管理指南》中的 NSX-T Data Center 的多站点部署以及本指南中的第 11 章 安装 NSX Cloud 组件 。

发布 NSX Manager 的 FQDN

安装 NSX-T Data Center 核心组件和 CSM 后，要通过 FQDN 启用 NAT，您需要在部署的 NSX-T DNS 服务器中设置查找和反向查找的条目。

此外，您还必须允许使用 NSX-T API 发布 NSX Manager FQDN。

示例请求：`PUT https://<nsx-mgr>/api/v1/configs/management`

```
{
  "publish_fqdns": true,
  "_revision": 0
}
```

示例响应：

```
{
  "publish_fqdns": true,
  "_revision": 1
}
```

请参阅《《NSX-T Data Center API 指南》》以了解详细信息。

注 在发布 FQDN 后，请验证传输节点进行的访问，如下一节中所述。

验证传输节点通过 FQDN 进行的访问

在发布 NSX Manager 的 FQDN 后，请验证传输节点是否可以成功访问 NSX Manager。

使用 SSH 登录到一个传输节点（如管理程序或 Edge 节点），然后运行 `get controllers` CLI 命令。

示例响应：

```
Controller IP    Port  SSL     Status       Is Physical Master   Session State    Controller FQDN
192.168.60.5     1235  enabled  connected   true                 up               nsxmgr.corp.com
```

NSX Edge 安装

NSX Edge 为 NSX-T Data Center 部署外部的网络 NSX Edge 提供路由服务和连接。如果要使用网络地址转换 (NAT)、VPN 等有状态服务部署 Tier-0 路由器或 Tier-1 路由器，则需要使用 NSX Edge。

注 每个 NSX Edge 节点只能具有一个 Tier-0 路由器。不过，可以在一个 NSX Edge 节点上托管多个 Tier-1 负载路由器。可以在同一群集中组合使用不同大小的 NSX Edge 虚拟机，但不建议这样做。

表 3-5. NSX Edge 部署、平台和安装要求

要求	说明
支持的部署方法	■ OVA/OVF ■ 具有 PXE 的 ISO ■ 没有 PXE 的 ISO
支持的平台	仅在 ESXi 或裸机上支持 NSX Edge。 在 KVM 上不支持 NSX Edge。
PXE 安装	对于 root 和 admin 用户密码，必须使用 sha-512 算法对密码字符串进行加密。
NSX-T Data Center 设备密码	■ 至少 12 个字符 ■ 至少一个小写字母 ■ 至少一个大写字母 ■ 至少一个数字 ■ 至少一个特殊字符 ■ 至少 5 个不同的字符 ■ 没有字典词语 ■ 没有回文 ■ 不允许使用超过四个单调字符的序列
主机名	在安装 NSX Edge 时，请指定不包含无效字符（如下划线）的主机名。如果主机名包含任何无效的字符，在部署后，主机名将设置为 **localhost**。有关主机名限制的详细信息，请参阅 https://tools.ietf.org/html/rfc952 和 https://tools.ietf.org/html/rfc1123。
VMware Tools	在 ESXi 上运行的 NSX Edge 虚拟机已安装 VMTools。不要移除或升级 VMTools。

表 3-5. NSX Edge 部署、平台和安装要求 （续）

要求	说明
系统	确认满足系统要求。请参见 NSX Edge 虚拟机系统要求。
端口	确认打开了所需的端口。请参见 端口和协议。
IP 地址	如果具有多个管理网络，您可以添加从 NSX-T Data Center 设备到其他网络的静态路由。 规划 NSX Edge IPv4 或 IPv6 IP 寻址方案。
OVF 模板	■ 确认您具有足够的权限以在 ESXi 主机上部署 OVF 模板。 ■ 确认主机名不包含下划线。否则，主机名将设置为 *nsx-manager*。 ■ 可部署 OVF 模板的管理工具，例如，vCenter Server 或 vSphere Client。 OVF 部署工具必须支持配置选项以允许进行手动配置。 ■ 必须安装客户端集成插件。
NTP 服务器	必须在 Edge 群集中的所有 NSX Edge 服务器上配置相同的 NTP 服务器。

NSX Edge 安装方案

重要事项 从 vSphere Web Client 或命令行中通过 OVA 或 OVF 文件安装 NSX Edge 时，在打开虚拟机电源之前，不会验证 OVA/OVF 属性值（如用户名、密码或 IP 地址）。

- 如果为 **admin** 或 **audit** 用户指定用户名，该名称必须是唯一的。如果指定相同的名称，则会忽略该名称并使用默认名称（**admin** 和 **audit**）。
- 如果 **admin** 用户的密码不符合复杂性要求，您必须通过 SSH 或控制台以 **admin** 用户身份（使用密码 **default**）登录到 NSX Edge。将提示您更改密码。
- 如果 **audit** 用户的密码不符合复杂性要求，则会禁用该用户帐户。要启用该帐户，请通过 SSH 或控制台以 **admin** 用户身份登录到 NSX Edge，然后运行 **set user audit** 命令以设置 **audit** 用户的密码（当前密码为空字符串）。
- 如果 **root** 用户的密码不符合复杂性要求，您必须通过 SSH 或控制台以 **root** 身份（使用密码 **vmware**）登录到 NSX Edge。将提示您更改密码。

小心 以 **root** 用户凭据登录时对 NSX-T Data Center 进行的更改可能会导致系统出现故障，且可能会影响您的网络。只能在 Vmware 技术支持团队的指导下使用 **root** 用户凭据进行更改。

注 在设置足够复杂的密码后，设备上的核心服务才会启动。

从 OVA 文件部署 NSX Edge 后，您无法通过关闭虚拟机电源，然后从 vCenter Server 中修改 OVA 设置来更改虚拟机的 IP 设置。

将 NSX Edge 加入管理层面

通过将 NSX Edge 加入管理层面，可以确保 NSX Manager 和 NSX Edge 可以相互通信。

前提条件

确认您具有登录 NSX Edge 和 NSX Manager 设备的管理员权限。

步骤

1 打开到 NSX Manager 设备的 SSH 会话。

2 打开到 NSX Edge 的 SSH 会话。

3 在 NSX Manager 设备上，运行 `get certificate api thumbprint` 命令。

命令输出是该 NSX Manager 特有的字母数字串。

例如：

```
NSX-Manager1> get certificate api thumbprint
...
```

4 在 NSX Edge 上，运行 **join management-plane** 命令。

提供以下信息：

- NSX Manager 的主机名或 IP 地址以及可选的端口号
- NSX Manager 的用户名
- NSX Manager 的证书指纹
- NSX Manager 的密码

```
NSX-Edge1> join management-plane NSX-Manager1 username admin thumbprint <NSX-Manager1's-
thumbprint>
Password for API user: <NSX-Manager1's-password>
Node successfully registered and Edge restarted
```

在每个 NSX Edge 节点上重复该命令。

5 在 NSX Edge 上运行 `get managers` 命令以验证结果。

```
nsx-edge-1> get managers
- 192.168.110.47   Connected
```

6 在 NSX Manager UI 中，选择**系统 > 结构层 > 节点 > Edge 传输节点**页面。

NSX Manager 连接应处于“已启动”状态。如果 NSX Manager 连接未处于“已启动”状态，请尝试刷新浏览器窗口。

后续步骤

将 NSX Edge 添加为传输节点。请参见创建 NSX Edge 传输节点。

在 vSphere 上安装 NSX-T Data Center

4

可以使用 UI 或 CLI 安装 NSX-T Data Center 组件、NSX Manager 和 NSX Edge。

请确保具有支持的 vSphere 版本。请参见 vSphere 支持。

本章讨论了以下主题：

- 安装 NSX Manager 和可用设备
- 使用 vSphere GUI 在 ESXi 上安装 NSX Edge

安装 NSX Manager 和可用设备

可以使用 vSphere Client 将 NSX Manager 或 Cloud Service Manager 部署为虚拟设备。

Cloud Service Manager 是使用 NSX-T Data Center 组件并将其与公有云相集成的虚拟设备。

前提条件

- 确认满足系统要求。请参见系统要求。
- 确认打开了所需的端口。请参见 端口和协议。
- 确认配置了一个数据存储，并且可以在 ESXi 主机上访问该数据存储。
- 确认具有供 NSX Manager 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。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。将 NSX-T Data Center 设备放在管理虚拟机网络上。

  如果具有多个管理网络，您可以添加从 NSX-T Data Center 设备到其他网络的静态路由。
- 规划 NSX Manager IPv4 或 IPv6 IP 寻址方案。

步骤

1 在 VMware 下载门户上找到 NSX-T Data Center OVA 文件。

  将下载 URL 复制到计算机或下载 OVA 文件。

2 在 vSphere Client 中，选择要在其上安装 NSX-T Data Center 的主机。

3 单击鼠标右键并选择**部署 OVF 模板**以启动安装向导。

4 输入下载 OVA URL 或导航到 OVA 文件。

5 输入 NSX Manager 虚拟机的名称。

输入的名称将显示在 vSphere 清单中。

6 选择 NSX Manager 设备的计算资源。

- 要在 vCenter 管理的 ESXi 主机上安装，请选择要在其上部署 NSX Manager 设备的主机。
- 要在独立 ESXi 主机上安装，请选择要在其上部署 NSX Manager 设备的主机。

7 确认 OVF 模板详细信息。

8 为了获得最佳性能，请为 NSX Manager 设备预留内存。

将预留内存设置为可确保 NSX Manager 足以高效运行。请参见 NSX Manager 虚拟机系统要求。

9 选择一个数据存储以存储 NSX Manager 设备文件。

10 为每个源网络选择目标网络。

11 为 NSX Manager 选择端口组或目标网络。

12 输入 NSX Manager 系统 root、CLI admin 和 audit 密码。

您的密码必须符合密码强度限制。

- 至少 12 个字符
- 至少一个小写字母
- 至少一个大写字母
- 至少一个数字
- 至少一个特殊字符
- 至少 5 个不同的字符
- 没有字典词语
- 没有回文
- 不允许使用超过四个单调字符的序列

13 输入 NSX Manager 的主机名。

注 主机名必须是有效的域名。请确保以点分隔的主机名（域/子域）的每个部分都必须以字母字符开头。

14 接受虚拟机的默认 **NSX Manager** 角色。

从下拉菜单中选择 **nsx-cloud-service-manager** 角色以安装 NSX Cloud 设备。

15 输入默认网关、管理网络 IPv4、管理网络的网络掩码、DNS 和 NTP IP 地址。

16 启用 SSH，并允许以 root 身份通过 SSH 登录到 NSX Manager 命令行。

默认情况下，出于安全考虑禁用这些选项。

17 确认所有的自定义 OVF 模板规范都是准确的，然后单击**完成**以启动安装。

该安装可能需要 7-8 分钟的时间。

18 从 vSphere Client 中，打开 NSX Manager 虚拟机控制台以跟踪引导过程。

19 在引导 NSX Manager 后，以 admin 身份登录到 CLI 并运行 `get interface eth0` 命令以确认 IP 地址已按预期应用。

20 输入 `get services` 命令以确认所有服务都正在运行。

如果服务未运行，则等待所有服务开始运行。

注 默认情况下，不会运行以下服务：liagent、migration-coordinator 和 snmp。您可以按以下方式启动这些服务：

- `start service liagent`
- `start service migration-coordinator`
- 对于 SNMP：

```
set snmp community <community-string>
start service snmp
```

21 确认 NSX Manager 具有所需的连接。

确保您可以执行以下任务。

- 从另一个计算机中 ping 通 NSX Manager。
- NSX Manager 可以 ping 通其默认网关。
- NSX Manager 可以使用管理接口 ping 通位于与 NSX Manager 相同的网络中的管理程序主机。
- NSX Manager 可以 ping 通其 DNS 服务器和 NTP 服务器。
- 如果已启用 SSH，请确保可以通过 SSH 访问 NSX Manager。

如果未建立连接，请确保虚拟设备的网络适配器位于正确的网络或 VLAN 中。

后续步骤

从支持的 Web 浏览器登录到 NSX Manager。请参见 登录到新创建的 NSX Manager 。

使用命令行 OVF Tool 在 ESXi 上安装 NSX Manager

如果希望自动完成 NSX Manager 安装或使用 CLI 执行安装，您可以使用 VMware OVF Tool，这是一个命令行实用程序。

默认情况下，出于安全原因，将禁用 `nsx_isSSHEnabled` 和 `nsx_allowSSHRootLogin`。如果禁用，则无法通过 SSH 访问或登录到 NSX Manager 命令行。如果启用 `nsx_isSSHEnabled` 但未启用 `nsx_allowSSHRootLogin`，您可以通过 SSH 访问 NSX Manager，但无法以 root 身份登录。

前提条件

- 确认满足系统要求。请参见系统要求。
- 确认打开了所需的端口。请参见 端口和协议。
- 确认配置了一个数据存储，并且可以在 ESXi 主机上访问该数据存储。
- 确认具有供 NSX Manager 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。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。将 NSX-T Data Center 设备放在管理虚拟机网络上。

  如果具有多个管理网络，您可以添加从 NSX-T Data Center 设备到其他网络的静态路由。
- 规划 NSX Manager IPv4 或 IPv6 IP 寻址方案。

步骤

1 使用相应的参数运行 `ovftool` 命令。

  该过程取决于主机是单独的，还是由 vCenter Server 管理的。

  - 对于单独的主机：
    - Windows 示例：

```
C:\Program Files\VMware\VMware OVF Tool>ovftool \
--sourceType=OVA \
--name=nsx-manager \
--X:injectOvfEnv \
--X:logFile=<filepath>\nsxovftool.log \
--allowExtraConfig \
--datastore=<datastore name> \
--network=<network name> \
--acceptAllEulas \
--noSSLVerify \
--diskMode=thin \
--powerOn \
--prop:"nsx_role=nsx-manager nsx-controller" \
--prop:"nsx_ip_0=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--prop:"nsx_isSSHEnabled=<True|False>" \
--prop:"nsx_allowSSHRootLogin=<True|False>" \
--prop:"nsx_passwd_0=<password>" \
--prop:"nsx_cli_passwd_0=<password>" \
```

```
--prop:"nsx_cli_audit-passwd_0=<password>" \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://root:<password>@10.168.110.51
```

注 上面的 Windows 代码块使用反斜杠 (\) 表示命令行续行。在实际使用中，请省略反斜杠并将整个命令放在一行中。

注 在上面的示例中，10.168.110.51 是要在其中部署 NSX Manager 的主机的 IP 地址。

- Linux 示例：

```
mgrformfactor="small"
ipAllocationPolicy="fixedPolicy"
mgrdatastore="QNAP-Share-VMs"
mgrnetwork="Management-VLAN-210"

mgrname01="nsx-manager-01"
mgrhostname01="nsx-manager-01"
mgrip01="192.168.210.121"

mgrnetmask="255.255.255.0"
mgrgw="192.168.210.254"
mgrdns="192.168.110.10"
mgrntp="192.168.210.254"
mgrpasswd="<password>"
mgrssh="<True|False>"
mgrroot="<True|False>"
logLevel="trivia"

mgresxhost01="192.168.110.113"

ovftool --noSSLVerify --skipManifestCheck --powerOn \
--deploymentOption=$mgrformfactor \
--diskMode=thin \
--acceptAllEulas \
--allowExtraConfig \
--ipProtocol=IPv4 \
--ipAllocationPolicy=$ipAllocationPolicy \
--datastore=$mgrdatastore \
--network=$mgrnetwork \
--name=$mgrname01 \
--prop:nsx_hostname=$mgrhostname01 \
--prop:nsx_role="nsx-manager nsx-controller" \
--prop:nsx_ip_0=$mgrip01 \
--prop:nsx_netmask_0=$mgrnetmask \
--prop:nsx_gateway_0=$mgrgw \
--prop:nsx_dns1_0=$mgrdns \
--prop:nsx_ntp_0=$mgrntp \
--prop:nsx_passwd_0=$mgrpasswd \
--prop:nsx_cli_passwd_0=$mgrpasswd \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:nsx_isSSHEnabled=$mgrssh \
--prop:nsx_allowSSHRootLogin=$mgrroot \
```

```
--X:logFile=nsxt-manager-ovf.log \
--X:logLevel=$logLevel \
/home/<user/nsxt-autodeploy/<nsx-unified-appliance-release>.ova \
vi://root:<password>@$mgresxhost01
```

结果应如下所示：

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://root:<password>@10.168.110.51
Deploying to VI: vi://root:<password>@10.168.110.51
Transfer Completed
Powering on VM: nsx-manager nsx-controller
Task Completed
Completed successfully
```

- 对于 vCenter Server 管理的主机：
  - Windows 示例：

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-manager \
--X:injectOvfEnv \
--X:logFile=ovftool.log \
 --allowExtraConfig \
--datastore=ds1 \
--network="management" \
--acceptAllEulas \
--noSSLVerify \
--diskMode=thin \
--powerOn \
--prop:"nsx_role=nsx-manager nsx-controller" \
--prop:"nsx_ip_0=10.168.110.75" \
--prop:"nsx_netmask_0=255.255.255.0" \
--prop:"nsx_gateway_0=10.168.110.1" \
--prop:"nsx_dns1_0=10.168.110.10" \
--prop:"nsx_domain_0=corp.local" \
--prop:"nsx_ntp_0=10.168.110.10" \
--prop:"nsx_isSSHEnabled=<True|False>" \
--prop:"nsx_allowSSHRootLogin=<True|False>" \
--prop:"nsx_passwd_0=<password>" \
--prop:"nsx_cli_passwd_0=<password>" \
--prop:"nsx_hostname=nsx-manager" \
<nsx-unified-appliance-release>.ova \
vi://administrator@vsphere.local:<password>@10.168.110.24/?ip=10.168.110.51
```

注 上面的 Windows 代码块使用反斜杠 (\) 表示命令行续行。在实际使用中，请省略反斜杠并将整个命令放在一行中。

- Linux 示例：

```
mgrformfactor="small"
ipAllocationPolicy="fixedPolicy"
mgrdatastore="QNAP-Share-VMs"
mgrnetwork="Management-VLAN-210"

mgrname01="nsx-manager-01"
mgrhostname01="nsx-manager-01"
mgrip01="192.168.210.121"

mgrnetmask="255.255.255.0"
mgrgw="192.168.210.254"
mgrdns="192.168.110.10"
mgrntp="192.168.210.254"
mgrpasswd="<password>"
mgrssh="<True|False>"
mgrroot="<True|False>"
logLevel="trivia"

vcadmin="administrator@vsphere.local"
vcpass="<password>"
vcip="192.168.110.151"
mgresxhost01="192.168.110.113"

ovftool --noSSLVerify --skipManifestCheck --powerOn \
--deploymentOption=$mgrformfactor \
--diskMode=thin \
--acceptAllEulas \
--allowExtraConfig \
--ipProtocol=IPv4 \
--ipAllocationPolicy=$ipAllocationPolicy \
--datastore=$mgrdatastore \
--network=$mgrnetwork \
--name=$mgrname01 \
--prop:nsx_hostname=$mgrhostname01 \
--prop:nsx_role="nsx-manager nsx-controller" \
--prop:nsx_ip_0=$mgrip01 \
--prop:nsx_netmask_0=$mgrnetmask \
--prop:nsx_gateway_0=$mgrgw \
--prop:nsx_dns1_0=$mgrdns \
--prop:nsx_ntp_0=$mgrntp \
--prop:nsx_passwd_0=$mgrpasswd \
--prop:nsx_cli_passwd_0=$mgrpasswd \
--prop:nsx_cli_audit_passwd_0=$mgrpasswd \
--prop:nsx_isSSHEnabled=$mgrssh \
--prop:nsx_allowSSHRootLogin=$mgrroot \
--X:logFile=nsxt-manager-ovf.log \
--X:logLevel=$logLevel \
/home/<user/nsxt-autodeploy/<nsx-unified-appliance-release>.ova \
vi://$vcadmin:$vcpass@$vcip/?ip=$mgresxhost01
```

结果应如下所示：

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator@vsphere.local@10.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@10.168.110.24:443/
Transfer Completed
Powering on VM: nsx-manager nsx-controller
Task Completed
Completed successfully
```

2 为了获得最佳性能，请为 NSX Manager 设备预留内存。

将预留内存设置为可确保 NSX Manager 足以高效运行。请参见 NSX Manager 虚拟机系统要求。

3 从 vSphere Client 中，打开 NSX Manager 虚拟机控制台以跟踪引导过程。

4 在引导 NSX Manager 后，以 admin 身份登录到 CLI 并运行 `get interface eth0` 命令以确认 IP 地址已按预期应用。

5 确认 NSX Manager 具有所需的连接。

确保您可以执行以下任务。

- 从另一个计算机中 ping 通 NSX Manager。
- NSX Manager 可以 ping 通其默认网关。
- NSX Manager 可以使用管理接口 ping 通位于与 NSX Manager 相同的网络中的管理程序主机。
- NSX Manager 可以 ping 通其 DNS 服务器和 NTP 服务器。
- 如果已启用 SSH，请确保可以通过 SSH 访问 NSX Manager。

如果未建立连接，请确保虚拟设备的网络适配器位于正确的网络或 VLAN 中。

后续步骤

从支持的 Web 浏览器登录到 NSX Manager。请参见登录到新创建的 NSX Manager 。

将 NSX-T Data Center 配置为在引导时显示 GRUB 菜单

需要将 NSX-T Data Center 设备配置为在引导时显示 GRUB 菜单，才能重置 NSX-T Data Center 设备的 root 密码。

重要事项 如果部署设备后未执行配置并且忘记 root、管理员或审核密码，则无法重置审核密码。

步骤

1 以 root 身份登录到虚拟机。

2 在 `/etc/default/grub` 文件中更改参数 `GRUB_HIDDEN_TIMEOUT` 的值。

```
GRUB_HIDDEN_TIMEOUT=2
```

3 （可选）在 /etc/grub.d/40_custom 文件中更改 GRUB 密码。

默认密码为 VMware1。

4 更新 GRUB 配置。

```
update-grub
```

登录到新创建的 NSX Manager

安装 NSX Manager 后，可以使用用户界面执行其他安装任务。

安装 NSX Manager 后，可以加入 NSX-T Data Center 的客户体验提升计划 (CEIP)。有关该计划的详细信息（包括如何稍后加入或退出该计划），请参见 NSX-T Data Center 管理指南中的“客户体验提升计划”。

前提条件

确认安装了 NSX Manager。请参见安装 NSX Manager 和可用设备。

步骤

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

此时将显示 EULA。

2 阅读并接受 EULA 条款。

3 选择是否加入 VMware 客户体验提升计划 (CEIP)。

4 单击**保存**

添加计算管理器

计算管理器（如 vCenter Server）是一个管理资源（如主机和虚拟机）的应用程序。

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

在添加 vCenter Server 计算管理器时，您必须提供 vCenter Server 用户的凭据。您可以提供 vCenter Server 管理员的凭据，或者专门为 NSX-T Data Center 创建一个角色和用户并提供该用户的凭据。该角色必须具有以下 vCenter Server 权限：

Extension.Register extension
Extension.Unregister extension
Extension.Update extension
Sessions.Message
Sessions.Validate session
Sessions.View and stop sessions
Host.Configuration.Maintenance

Host.Local Operations.Create virtual machine
Host.Local Operations.Delete virtual machine
Host.Local Operations.Reconfigure virtual machine
Tasks
Scheduled task
Global.Cancel task
Permissions.Reassign role permissions
Resource.Assign vApp to resource pool
Resource.Assign virtual machine to resource pool
Virtual Machine.Configuration
Virtual Machine.Guest Operations
Virtual Machine.Provisioning
Virtual Machine.Inventory
Network.Assign network
vApp

有关 vCenter Server 角色和权限的详细信息，请参见《vSphere 安全性》文档。

前提条件

- 确认使用支持的 vSphere 版本。请参见支持的 vSphere 版本
- 与 vCenter Server 的 IPv6 和 IPv4 通信。
- 确认使用建议数量的计算管理器。请参见 https://configmax.vmware.com/home。

> **注** NSX-T Data Center 不支持在多个 NSX Manager 中注册相同的 vCenter Server。

步骤

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

2 选择**系统 > 结构层 > 计算管理器 > 添加**。

3 填写计算管理器详细信息。

选项	说明
名称和说明	键入名称以标识 vCenter Server。 您可以选择描述任何特殊详细信息，如 vCenter Server 中的群集数。
域名/IP 地址	键入 vCenter Server 的 IP 地址。
类型	保留默认选项。
用户名和密码	键入 vCenter Server 登录凭据。
指纹	键入 vCenter Server SHA-256 指纹算法值。

如果将指纹值保留空白，将提示您接受服务器提供的指纹。

在接受该指纹后，需要几秒钟 NSX-T Data Center 才能发现并注册 vCenter Server 资源。

4 如果进度图标从**正在进行中**更改为**未注册**，请执行以下步骤解决错误。

a 选择错误消息，然后单击**解决**。一个可能的错误消息如下：

```
Extension already registered at CM <vCenter Server name> with id <extension ID>
```

b 输入 vCenter Server 凭据，然后单击**解决**。

如果存在现有注册，则会替换它。

结果

向 vCenter Server 注册计算管理器且连接状态显示为已启动需要一些时间。

可以单击计算管理器的名称，以查看详细信息、编辑计算管理器或者管理适用于计算管理器的标记。

从 UI 部署 NSX Manager 节点以形成群集

可以部署多个 NSX Manager 节点以提供高可用性和可靠性。

部署新节点后，这些节点将连接到 NSX Manager 节点以形成群集。建议形成群集的 NSX Manager 节点数为 3。

注 仅在 vCenter Server 管理的 ESXi 主机上才支持使用 UI 部署多个 NSX Manager 节点。

第一个部署的 NSX Manager 节点的所有存储库详细信息和密码将与群集中新部署的节点进行同步。

前提条件

- 确认已安装 NSX Manager 节点。请参见安装 NSX Manager 和可用设备。
- 确认配置了计算管理器。请参见添加计算管理器。
- 确认满足系统要求。请参见系统要求。
- 确认打开了所需的端口。请参见 端口和协议。
- 确认配置了一个数据存储，并且可以在 ESXi 主机上访问该数据存储。
- 确认具有供 NSX Manager 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。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。将 NSX-T Data Center 设备放在管理虚拟机网络上。

  如果具有多个管理网络，您可以添加从 NSX-T Data Center 设备到其他网络的静态路由。

步骤

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

2 选择**系统 > 设备 > 概览 > 添加节点**。

3 输入 NSX Manager 常见属性详细信息。

选项	说明
计算管理器	会填充已注册的资源计算管理器。
启用 SSH	切换该按钮以允许通过 SSH 登录到新的 NSX Manager 节点。
启用 root 访问权限	切换该按钮以允许对新的 NSX Manager 节点进行根访问。
CLI 用户名和密码确认	为新节点设置 CLI 密码和密码确认。 您的密码必须符合密码强度限制。 ■ 至少 12 个字符 ■ 至少一个小写字母 ■ 至少一个大写字母 ■ 至少一个数字 ■ 至少一个特殊字符 ■ 至少 5 个不同的字符 ■ 没有字典词语 ■ 没有回文 ■ 不允许使用超过四个单调字符的序列 CLI 用户名已设置为 admin。
Root 密码和密码确认	为新节点设置 root 密码和密码确认。 您的密码必须符合密码强度限制。 ■ 至少 12 个字符 ■ 至少一个小写字母 ■ 至少一个大写字母 ■ 至少一个数字 ■ 至少一个特殊字符 ■ 至少 5 个不同的字符 ■ 没有字典词语 ■ 没有回文 ■ 不允许使用超过四个单调字符的序列
DNS 服务器	输入 vCenter Server 中可用的 DNS 服务器 IP 地址。
NTP 服务器	输入 NTP 服务器的 IP 地址。

4 输入 NSX Manager 节点详细信息。

选项	说明
名称	输入 NSX Manager 节点的名称。
群集	从下拉菜单中指定节点要加入的群集。
资源池或主机	从下拉菜单中为节点分配资源池或主机。
数据存储	从下拉菜单中选择节点文件的数据存储。
网络	在下拉菜单中分配网络。
管理 IP/网络掩码	输入 IP 地址和网络掩码。
管理网关	输入网关 IP 地址。

5 （可选）单击**新建节点**并配置另一个节点。

重复步骤 3-4。

6 单击**完成**。

将部署新节点。可以在**系统 > 设备 > 概览**页面或 vCenter Server 上跟踪部署过程。

7 等待 10-15 分钟，以便部署、群集形成和存储库同步完成。

第一个部署的 NSX Manager 节点的所有存储库详细信息和密码将与群集中新部署的节点进行同步。

8 在引导 NSX Manager 后，以 admin 身份登录到 CLI 并运行 `get interface eth0` 命令以确认 IP 地址已按预期应用。

9 输入 `get services` 命令以确认所有服务都正在运行。

如果服务未运行，则等待所有服务开始运行。

注 默认情况下，不会运行以下服务：liagent、migration-coordinator 和 snmp。您可以按以下方式启动这些服务：

- `start service liagent`
- `start service migration-coordinator`
- 对于 SNMP：

```
set snmp community <community-string>
start service snmp
```

10 登录到第一个部署的 NSX Manager 节点，然后输入 `get cluster status` 命令以确认节点已成功添加到群集。

11 确认 NSX Manager 具有所需的连接。

确保您可以执行以下任务。

- 从另一个计算机中 ping 通 NSX Manager。
- NSX Manager 可以 ping 通其默认网关。
- NSX Manager 可以使用管理接口 ping 通位于与 NSX Manager 相同的网络中的管理程序主机。
- NSX Manager 可以 ping 通其 DNS 服务器和 NTP 服务器。
- 如果已启用 SSH，请确保可以通过 SSH 访问 NSX Manager。

如果未建立连接，请确保虚拟设备的网络适配器位于正确的网络或 VLAN 中。

后续步骤

配置 NSX Edge。请参见使用 vSphere GUI 在 ESXi 上安装 NSX Edge。

使用 CLI 部署 NSX Manager 节点以形成群集

使用 CLI 将 NSX Manager 加入以形成群集可确保群集中的所有 NSX Manager 节点都可以相互通信。

前提条件

必须完成 NSX-T Data Center 组件的安装。

步骤

1 打开与第一个部署的 NSX Manager 节点的 SSH 会话。

2 使用管理员凭据登录。

3 在 NSX Manager 设备上，运行 `get certificate api thumbprint` 命令。

命令输出是该 NSX Manager 特有的数字串。

4 运行 `get cluster config` 命令以获取第一个部署的 NSX Manager 群集 ID。

5 将 NSX Manager 节点添加到群集。

> **注** 必须在新部署的 NSX Manager 节点上运行 join 命令。

提供以下 NSX Manager 信息：

- 要加入的节点的主机名或 IP 地址
- Cluster ID
- 用户名
- 密码
- 证书指纹

可以使用 CLI 命令或 API 调用。

- CLI 命令

```
host> join <NSX-Manager-IP> cluster-id <cluster-id> username<NSX-Manager-username>
password<NSX-Manager-password> thumbprint <NSX-Manager1's-thumbprint>
```

- API 调用 `POST https://<nsx-mgr>/api/v1/cluster?action=join_cluster`

加入和群集稳定过程可能需要 10-15 分钟的时间。

6 将第三个 NSX Manager 节点添加到群集。

重复步骤 5。

7 在主机上运行 `get cluster status` 命令以确认群集状态。

8 选择 **系统 > 设备 > 概览**并确认群集连接。

后续步骤

创建传输区域。请参见 创建独立主机或裸机服务器传输节点。

配置集群的虚拟 IP (VIP) 地址

要为 NSX Manager 节点提供容错和高可用性，需为 NSX-T 集群成员分配虚拟 IP (Virtual IP, VIP) 地址。

集群的 NSX Manager 将成为 HTTPS 组的一部分，用于处理 API 和 UI 请求。集群的主节点拥有集群的集合 VIP 的所有权以处理任何 API 和 UI 请求。来自客户端的任何 API 和 UI 请求将传送到主节点。

注 分配虚拟 IP 时，必须在同一子网中配置集群中的所有 NSX Manager 虚拟机。

如果拥有 VIP 的主节点变得不可用，NSX-T 将选择新的主节点。新的主节点将拥有 VIP。它会发出一个免费 ARP 数据包，通告新 VIP 到 MAC 地址的映射。选择新的主节点后，新 API 和 UI 请求将被发送到该新的主节点。

在将 VIP 故障切换到集群的新主节点时，主节点可能需要几分钟的时间才能正常工作。如果由于以前的主节点变得不可用而将 VIP 故障切换到新的主节点，请重新验证凭据，以便将 API 请求传送到新的主节点。

注 VIP 不能用作负载均衡器，如果从**系统 > 用户 > 配置**中启用 vIDM **外部负载均衡器集成**，则无法使用该 VIP。如果要从 vIDM 中使用外部负载均衡器，请不要设置 VIP。有关更多详细信息，请参见《NSX-T Data Center 管理指南》中的配置 VMware Identity Manager 集成。

步骤

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

2 转到**系统 > 概览**。

3 在“虚拟 IP”字段中，单击**编辑**。

4 输入集群的 VIP。确保 VIP 属于与其他管理节点相同的子网。

5 单击**保存**。

6 要验证 HTTPS 组的集群状态和主 API，请在 NSX Manager 控制台中或通过 SSH 输入 NSX Manager CLI 命令 `get cluster status verbose`。

下面是以粗体标记的主 API 的示例输出。

```
Group Type: HTTPS
Group Status: STABLE

Members:
    UUID                                     FQDN                 IP
STATUS
    cdb93642-ccba-fdf4-8819-90bf018cd727     nsx-manager      192.196.197.84
UP
    51a13642-929b-8dfc-3455-109e6cc2a7ae     nsx-manager      192.196.198.156
UP
    d0de3642-d03f-c909-9cca-312fd22e486b     nsx-manager      192.196.198.54
UP
```

```
Leaders:
    SERVICE                                 LEADER                                  LEASE
VERSION
    api                                     cdb93642-ccba-fdf4-8819-90bf018cd727    8
```

7 要对 VIP 进行故障排除，请在 NSX Manager CLI 中检查反向代理日志 (`/var/log/proxy/reverse-proxy.log`) 和集群管理器日志 (`/var/log/cbm/cbm.log`)。

结果

发送到 NSX-T 的任何 API 请求将重定向到集群的虚拟 IP 地址（主节点拥有该地址）。然后，主节点将请求向前路由到设备的其他组件。

使用 vSphere GUI 在 ESXi 上安装 NSX Edge

如果首选交互式 NSX Edge 安装，则可以使用 vSphere Web 客户端。

重要事项 在 NSX-T 中，NSX Edge 虚拟机不支持 vMotion。

前提条件

请参见 NSX Edge 安装。

步骤

1 在 VMware 下载门户上找到 NSX Edge 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 vSphere Client 中，选择要在其上安装 NSX Edge 设备的主机。

3 单击鼠标右键并选择**部署 OVF 模板**以启动安装向导。

4 输入下载 OVA URL 或导航到已保存的 OVA 文件。

5 输入 NSX Edge 虚拟机的名称。

键入的名称将显示在清单中。

6 选择 NSX Edge 设备的计算资源。

7 为了获得最佳性能，请为 NSX Edge 设备预留内存。

将预留内存设置为可确保 NSX Edge 足以高效运行。请参见 NSX Edge 虚拟机系统要求。

8 确认 OVF 模板详细信息。

9 选择一个数据存储以存储 NSX Edge 设备文件。

10 接受默认的源和目标网络接口。

可以接受其余网络的默认网络目标，并在部署 NSX Edge 后更改网络配置。

11 从下拉菜单中选择 IP 分配。

12 输入 NSX Edge 系统 root、CLI admin 和 audit 密码。

您的密码必须符合密码强度限制。

- 至少 12 个字符
- 至少一个小写字母
- 至少一个大写字母
- 至少一个数字
- 至少一个特殊字符
- 至少 5 个不同的字符
- 没有字典词语
- 没有回文
- 不允许使用超过四个单调字符的序列

13 输入默认网关、管理网络 IPv4、管理网络的网络掩码、DNS 和 NTP IP 地址。

14 （可选） 如果具有可用的 NSX Manager，则向管理层面注册 NSX Edge。

a 输入 NSX Manager 父节点的 IP 地址和指纹。

b 运行 API 调用 `POST https://<nsx-manager>/api/v1/aaa/registration-token` 以检索 NSX Manager 令牌。

15 输入 NSX Edge 虚拟机的主机名。

16 启用 SSH，并允许以 root 身份通过 SSH 登录到 NSX Edge 命令行。

默认情况下，出于安全考虑禁用这些选项。

17 确认所有的自定义 OVA 模板规范都是准确的，然后单击**完成**以启动安装。

该安装可能需要 7-8 分钟的时间。

18 打开 NSX Edge 控制台以跟踪引导过程。

如果未打开控制台窗口，请确保允许弹出窗口。

19 在 NSX Edge 启动后，使用管理员凭据登录到 CLI。

注 在 NSX Edge 启动后，如果第一次不使用管理员凭据进行登录，则不会在 NSX Edge 上自动启动数据层面服务。

20 运行 `get interface eth0.<vlan_ID>` 命令以验证是否按预期方式应用了 IP 地址。

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
  Address: 192.168.110.37/24
  MAC address: 00:50:56:86:62:4d
```

```
MTU: 1500
Default gateway: 192.168.110.1
Broadcast address: 192.168.110.255
...
```

注 在 NSX 未管理的主机上启动 NSX Edge 虚拟机时，请确认在数据网卡的物理主机交换机上将 MTU 设置设为 1600（而不是 1500）。

21 运行 `get managers` 命令以确认已注册 NSX Edge。

```
- 10.29.14.136 Standby
- 10.29.14.135 Standby
- 10.29.14.134 Connected
```

22 确认 NSX Edge 设备具有所需的连接。

如果已启用 SSH，请确保可以通过 SSH 访问 NSX Edge。

- 您可以 ping 通 NSX Edge。
- NSX Edge 可以 ping 通其默认网关。
- NSX Edge 可以 ping 通位于与 NSX Edge 相同的网络中的管理程序主机。
- NSX Edge 可以 ping 通其 DNS 服务器和 NTP 服务器。

23 解决连接问题。

注 如果未建立连接，请确保虚拟机网络适配器位于正确的网络或 VLAN 中。

默认情况下，NSX Edge 数据路径声明管理网卡（具有 IP 地址和默认路由的网卡）以外的所有虚拟机网卡。如果错误地将一个网卡分配为管理接口，请按照以下步骤使用 DHCP 将管理 IP 地址分配给正确的网卡。

a 登录到 CLI，然后键入 **`stop service dataplane`** 命令。

b 键入 **`set interface`** ***`interface`*** **`dhcp plane mgmt`** 命令。

c 将 *interface* 放入 DHCP 网络中，并等待为该 *interface* 分配一个 IP 地址。

d 键入 **`start service dataplane`** 命令。

将在 NSX Edge 上的 **get interfaces** 和 **get physical-port** 命令中显示用于 VLAN 上行链路和隧道覆盖网络的数据路径 fp-ethX 端口。

后续步骤

将 NSX Edge 加入管理层面。请参见将 NSX Edge 加入管理层面。

使用命令行 OVF Tool 在 ESXi 上安装 NSX Edge

如果希望自动完成 NSX Edge 安装，您可以使用 VMware OVF Tool，这是一个命令行实用程序。

前提条件

- 确认满足系统要求。请参见系统要求。
- 确认打开了所需的端口。请参见 端口和协议。
- 确认配置了一个数据存储，并且可以在 ESXi 主机上访问该数据存储。
- 确认具有供 NSX Manager 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。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。将 NSX-T Data Center 设备放在管理虚拟机网络上。

  如果具有多个管理网络，您可以添加从 NSX-T Data Center 设备到其他网络的静态路由。
- 规划 NSX Manager IPv4 或 IPv6 IP 寻址方案。
- 请参阅 NSX Edge 安装中的 NSX Edge 网络要求。
- 确认您具有足够的权限以在 ESXi 主机上部署 OVF 模板。
- 确认主机名不包含下划线。否则，主机名将设置为 *localhost*。
- OVF Tool 4.3 或更高版本。

步骤

- 对于单独的主机，请使用相应的参数运行 `ovftool` 命令。

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
```

```
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
<path/url to nsx component ova>
vi://root:<password>@192.168.110.51
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://root@192.168.110.24
Deploying to VI: vi://root@192.168.110.24
Transfer Completed
Powering on VM: nsx-edge-1
Task Completed
Completed successfully
```

- 对于 vCenter Server 管理的主机，请使用相应的参数运行 `ovftool` 命令。

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
```

```
--prop:nsx_hostname=nsx-edge
<path/url to nsx component ova>
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.210.53
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator@vsphere.local@192.168.110.24:443/
Deploying to VI: vi://administrator@vsphere.local@192.168.110.24:443/
Transfer Completed
Powering on VM: nsx-edge-1
Task Completed
Completed successfully
```

- 为了获得最佳性能，请为 NSX Manager 设备预留内存。

  将预留内存设置为可确保 NSX Manager 足以高效运行。请参见 NSX Manager 虚拟机系统要求。

- 打开 NSX Edge 控制台以跟踪引导过程。
- 在 NSX Edge 启动后，使用管理员凭据登录到 CLI。
- 运行 `get interface eth0.<vlan_ID>` 命令以验证是否按预期方式应用了 IP 地址。

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
  Address: 192.168.110.37/24
  MAC address: 00:50:56:86:62:4d
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

注 在 NSX 未管理的主机上启动 NSX Edge 虚拟机时，请确认在数据网卡的物理主机交换机上将 MTU 设置设为 1600（而不是 1500）。

- 确认 NSX Edge 设备具有所需的连接。

  如果已启用 SSH，请确保可以通过 SSH 访问 NSX Edge。

  - 您可以 ping 通 NSX Edge。
  - NSX Edge 可以 ping 通其默认网关。
  - NSX Edge 可以 ping 通位于与 NSX Edge 相同的网络中的管理程序主机。
  - NSX Edge 可以 ping 通其 DNS 服务器和 NTP 服务器。

- 解决连接问题。

注 如果未建立连接，请确保虚拟机网络适配器位于正确的网络或 VLAN 中。

默认情况下，NSX Edge 数据路径声明管理网卡（具有 IP 地址和默认路由的网卡）以外的所有虚拟机网卡。如果错误地将一个网卡分配为管理接口，请按照以下步骤使用 DHCP 将管理 IP 地址分配给正确的网卡。

a 登录到 CLI，然后键入 **`stop service dataplane`** 命令。

b 键入 **`set interface`** ***`interface`*** **`dhcp plane mgmt`** 命令。

c 将 *interface* 放入 DHCP 网络中，并等待为该 *interface* 分配一个 IP 地址。

d 键入 **`start service dataplane`** 命令。

将在 NSX Edge 上的 **get interfaces** 和 **get physical-port** 命令中显示用于 VLAN 上行链路和隧道覆盖网络的数据路径 fp-ethX 端口。

后续步骤

将 NSX Edge 加入管理层面。请参见将 NSX Edge 加入管理层面。

在 KVM 上安装 NSX-T Data Center 5

NSX-T Data Center 以两种方式支持 KVM：作为主机传输节点和作为 NSX Manager 的主机。

请确保具有支持的 KVM 版本。请参见 NSX Manager 虚拟机系统要求。

本章讨论了以下主题：

- 设置 KVM
- 在 KVM CLI 中管理客户机虚拟机
- 在 KVM 上安装 NSX Manager
- 登录到新创建的 NSX Manager
- 在 KVM 主机上安装第三方软件包
- 验证 RHEL KVM 主机上的 Open vSwitch 版本
- 使用 CLI 部署 NSX Manager 节点以形成群集
- 使用 ISO 文件或 PXE 安装 NSX Edge

设置 KVM

如果计划将 KVM 用作传输节点或 NSX Manager 客户机虚拟机的主机，但尚未设置 KVM，您可以使用此处介绍的过程。

注 Geneve 封装协议使用 UDP 端口 6081。您必须在 KVM 主机上的防火墙中允许该端口访问。

步骤

1 （仅限 RHEL）打开 `/etc/yum.conf` 文件。

2 搜索行 `exclude`。

3 添加行 `"kernel* redhat-release*"` 以配置 YUM 来避免任何不受支持的 RHEL 升级。

```
exclude=[existing list] kernel* redhat-release*
```

如果计划运行具有特定兼容性要求的 NSX-T Data Center Container Plug-in，还要排除容器相关模块。

```
exclude=[existing list] kernel* redhat-release* kubelet-* kubeadm-* kubectl-* docker-*
```

受支持的 RHEL 版本是 7.4 和 7.5。

4 安装 KVM 和桥接实用程序。

Linux 发布版本	命令
Ubuntu	`apt-get install -y qemu-kvm libvirt-bin ubuntu-vm-builder bridge-utils virtinst virt-manager virt-viewer libguestfs-tools`

RHEL 或 CentOS Linux	`yum groupinstall "Virtualization Hypervisor"`
	`yum groupinstall "Virtualization Client"`
	`yum groupinstall "Virtualization Platform"`
	`yum groupinstall "Virtualization Tools"`

SUSE Linux Enterprise Server	启动 YaSt，然后选择 **Virtualization (虚拟化) > Install Hypervisor and Tools (安装管理程序和工具)**。 通过使用 YaSt，您可以自动启用和配置网桥。

5 确认硬件虚拟化功能。

```
cat /proc/cpuinfo | egrep "vmx|svm"
```

输出必须包含 vmx。

6 确认安装了 KVM 模块。

Linux 发布版本	命令

Ubuntu	`kvm-ok`
	
	`INFO: /dev/kvm exists`
	`KVM acceleration can be used`

RHEL 或 CentOS Linux	`lsmod | grep kvm`
	
	`kvm_intel   53484  6`
	`kvm         316506  1 kvm_intel`

SUSE Linux Enterprise Server	

7 对于要用作 NSX Manager 的主机的 KVM，准备桥接网络、管理接口和网卡接口。

在以下示例中，使用第一个以太网接口（eth0 或 ens32）以连接到 Linux 计算机本身。根据您的部署环境，该接口可以使用 DHCP 或静态 IP 设置。向 NSX-T Data Center 主机分配上行链路接口之前，请确保已配置这些上行链路使用的接口脚本。如果在系统上没有这些接口文件，将无法成功创建主机传输节点。

注 在不同的环境中，接口名称可能会有所不同。

Linux 发布版本	网络配置

Ubuntu	编辑 /etc/network/interfaces：
	`auto lo`
	`iface lo inet loopback`
	
	`auto eth0`
	`iface eth0 inet manual`
	
	`auto br0`
	`iface br0 inet static`
	`address 192.168.110.51`
	`netmask 255.255.255.0`
	`network 192.168.110.0`
	`broadcast 192.168.110.255`
	`gateway 192.168.110.1`
	`dns-nameservers 192.168.3.45`
	`dns-search example.com`
	`bridge_ports eth0`
	`bridge_stp off`
	`bridge_fd 0`
	`bridge_maxwait 0`
	
	为网桥创建一个网络定义 XML 文件。例如，创建包含以下行的 /tmp/bridge.xml：
	`<network>`
	`<name>bridge</name>`
	`<forward mode='bridge'/>`
	`<bridge name='br0'/>`
	`</network>`
	
	使用以下命令定义并启动桥接网络：
	`virsh net-define`
	`bridge.xml`
	`virsh net-start bridge`
	`virsh net-autostart bridge`
	
	使用以下命令确认桥接网络的状态：
	`virsh net-list --all`
	
	`Name State Autostart Persistent`
	`----------------------------------------------------------`
	`bridge active yes yes`
	`default active yes yes`

RHEL 或 CentOS Linux	编辑 /etc/sysconfig/network-scripts/ifcfg-*management_interface*：
	`DEVICE="ens32"`
	`TYPE="Ethernet"`
	`NAME="ens32"`
	`UUID="<UUID>"`
	`BOOTPROTO="none"`
	`HWADDR="<HWADDR>"`

Linux 发布版本	网络配置
	ONBOOT="yes" NM_CONTROLLED="no" BRIDGE="br0" 编辑 /etc/sysconfig/network-scripts/ifcfg-eth1： DEVICE="eth1" TYPE="Ethernet" NAME="eth1" UUID="<*UUID*>" BOOTPROTO="none" HWADDR="<*HWADDR*>" ONBOOT="yes" NM_CONTROLLED="no" 编辑 /etc/sysconfig/network-scripts/ifcfg-eth2： DEVICE="eth2" TYPE="Ethernet" NAME="eth2" UUID="<*UUID*>" BOOTPROTO="none" HWADDR="<*HWADDR*>" ONBOOT="yes" NM_CONTROLLED="no" 编辑 /etc/sysconfig/network-scripts/ifcfg-br0： DEVICE="br0" BOOTPROTO="dhcp" NM_CONTROLLED="no" ONBOOT="yes" TYPE="Bridge"
SUSE Linux Enterprise Server	

8 要将 KVM 作为传输节点，请准备网桥。

在以下示例中，使用第一个以太网接口（eth0 或 ens32）以连接到 Linux 计算机本身。根据您的部署环境，该接口可以使用 DHCP 或静态 IP 设置。

注 在不同的环境中，接口名称可能会有所不同。

Linux 发布版本	网络配置

Ubuntu	编辑 /etc/network/interfaces：
	`auto lo`
	`iface lo inet loopback`
	
	`auto eth0`
	`iface eth0 inet manual`
	
	`auto eth1`
	`iface eth1 inet manual`
	
	`auto br0`
	`iface br0 inet dhcp`
	`  bridge_ports eth0`

RHEL 或 CentOS Linux	编辑 /etc/sysconfig/network-scripts/ifcfg-ens32：
	`DEVICE="ens32"`
	`  TYPE="Ethernet"`
	`  NAME="ens32"`
	`  UUID="<something>"`
	`  BOOTPROTO="none"`
	`  HWADDR="<something>"`
	`  ONBOOT="yes"`
	`  NM_CONTROLLED="no"`
	`  BRIDGE="br0"`
	
	编辑 /etc/sysconfig/network-scripts/ifcfg-ens33：
	`DEVICE="ens33"`
	`  TYPE="Ethernet"`
	`  NAME="ens33"`
	`  UUID="<something>"`
	`  BOOTPROTO="none"`
	`  HWADDR="<something>"`
	`  ONBOOT="yes"`
	`  NM_CONTROLLED="no"`
	
	编辑 /etc/sysconfig/network-scripts/ifcfg-br0：
	`DEVICE="br0"`
	`   BOOTPROTO="dhcp"`
	`   NM_CONTROLLED="no"`
	`   ONBOOT="yes"`
	`   TYPE="Bridge"`

SUSE Linux Enterprise Server	

重要事项 对于 Ubuntu，必须在 /etc/network/interfaces 中指定所有网络配置。不要创建单独的网络配置文件（如 /etc/network/ifcfg-eth1），这可能会导致传输节点创建失败。

在将 KVM 主机配置为传输节点后，将创建网桥接口“nsx-vtep0.0”。在 Ubuntu 中， `/etc/network/interfaces` 具有如下条目：

```
iface nsx-vtep0.0 inet static
pre-up ip addr flush dev nsx-vtep0.0
address <IP_pool_address>
netmask <subnet_mask>
mtu 1600
down ifconfig nsx-vtep0.0 down
up ifconfig nsx-vtep0.0 up
```

在 RHEL 中，主机 NSX 代理 (nsxa) 会创建一个名为 ifcfg-nsx-vtep0.0 的配置文件，其中包含如下条目：

```
DEVICE=nsx-vtep0.0
BOOTPROTO=static
NETMASK=<IP address>
IPADDR=<subnet mask>
MTU=1600
ONBOOT=yes
USERCTL=no
NM_CONTROLLED=no
```

在 SUSE 中，

9 重新启动网络连接服务 `systemctl restart network`，或者重新引导 Linux 服务器，以使网络连接更改生效。

在 KVM CLI 中管理客户机虚拟机

可以将 NSX Manager 安装为 KVM 虚拟机。此外，还可以将 KVM 作为 NSX-T Data Center 传输节点的管理程序。

KVM 客户机虚拟机管理超出本指南的范围。不过，此处提供了一些简单的 KVM CLI 命令供您快速入门。

要在 KVM CLI 中管理客户机虚拟机，请使用 `virsh` 命令。下面是一些常见的 `virsh` 命令。请参阅 KVM 文档了解其他信息。

```
# List running
virsh list

# List all
virsh list --all

# Control instances
virsh start <instance>
virsh shutdown <instance>
virsh destroy <instance>
virsh undefine <instance>
virsh suspend <instance>
```

```
virsh resume <instance>

# Access an instance's CLI
virsh console <instance>
```

在 Linux CLI 中，`ifconfig` 命令显示 vnetX 接口，它表示为客户机虚拟机创建的接口。如果添加额外的客户机虚拟机，则会添加额外的 vnetX 接口。

```
ifconfig
...

vnet0     Link encap:Ethernet  HWaddr fe:54:00:b0:a0:6d
          inet6 addr: fe80::fc54:ff:feb0:a06d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13183 errors:0 dropped:0 overruns:0 frame:0
          TX packets:181524 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:4984832 (4.9 MB)  TX bytes:29498709 (29.4 MB)
```

在 KVM 上安装 NSX Manager

可以在 KVM 主机上将 NSX Manager 安装为虚拟设备。

QCOW2 安装过程使用 guestfish（Linux 命令行工具）将虚拟机设置写入到 QCOW2 文件中。

前提条件

- 设置了 KVM。请参见设置 KVM。
- 在 KVM 主机上部署 QCOW2 映像的权限。
- 确认 guestinfo 中的密码符合密码复杂性要求，以便您可以在安装后登录。请参见 NSX Manager 安装。
- 熟悉 NSX Manager 资源要求。请参见 NSX Manager 虚拟机系统要求。
- 如果您计划安装 Ubuntu OS，则建议在 KVM 主机上安装 NSX Manager 之前，安装 Ubuntu 版本 18.04。

步骤

1 从 **nsx-unified-appliance > exports > kvm** 文件夹下载 NSX Manager QCOW2 映像。

2 将其复制到要使用 SCP 或同步运行 NSX Manager 的 KVM 计算机。

3 （仅限 Ubuntu）将当前登录的用户添加为 libvirtd 用户：

```
adduser $USER libvirtd
```

4 在保存 QCOW2 映像的同一目录中，创建一个名为 guestinfo.xml 的文件，然后使用 NSX Manager 虚拟机的属性填充该文件。

属性	说明
■ **nsx_cli_passwd_0** ■ **nsx_cli_audit_passwd_0** ■ **nsx_passwd_0**	您的密码必须符合密码强度限制。 ■ 至少 12 个字符 ■ 至少一个小写字母 ■ 至少一个大写字母 ■ 至少一个数字 ■ 至少一个特殊字符 ■ 至少 5 个不同的字符 ■ 没有字典词语 ■ 没有回文 ■ 不允许使用超过四个单调字符的序列
nsx_hostname	输入 NSX Manager 的主机名。主机名必须是有效的域名。请确保主机名的各个部分（域/子域，用点分隔）都必须以字母字符开头。
nsx_role	■ *nsx manager*：必需。该角色名称将安装 NSX Manager 设备。 ■ *nsx-cloud-service-manager*：可选。安装 NSX Manager 后，使用此角色名称为 NSX Cloud 安装 Cloud Service Manager 设备。
nsx_isSSHEnabled	您可以启用或禁用此属性。如果启用，则可以使用 SSH 登录到 NSX Manager。
nsx_allowSSHRootLogin	您可以启用或禁用此属性。如果启用，则可以使用 SSH 以 root 用户的身份登录到 NSX Manager。为了能够使用此属性，必须启用 `nsx_isSSHEnabled`。
■ **nsx_dns1_0** ■ **nsx_ntp_0** ■ **nsx_domain_0** ■ **nsx_gateway_0** ■ **nsx_netmask_0** ■ **nsx_ip_0**	输入默认网关的 IP 地址、管理网络 IPv4、管理网络的网络掩码、DNS 和 NTP IP 地址。

例如：

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment
     xmlns="http://schemas.dmtf.org/ovf/environment/1"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xmlns:oe="http://schemas.dmtf.org/ovf/environment/1">
   <PropertySection>
    <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_cli_audit_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_passwd_0" oe:value="<password>"/>
    <Property oe:key="nsx_hostname" oe:value="nsx-manager1"/>
    <Property oe:key="nsx_role" oe:value="nsx-manager"/>
    <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
    <Property oe:key="nsx_allowSSHRootLogin" oe:value="True"/>
    <Property oe:key="nsx_dns1_0" oe:value="10.168.110.10"/>
    <Property oe:key="nsx_ntp_0" oe:value="10.168.110.10"/>
```

```
    <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
    <Property oe:key="nsx_gateway_0" oe:value="10.168.110.83"/>
    <Property oe:key="nsx_netmask_0" oe:value="255.255.252.0"/>
    <Property oe:key="nsx_ip_0" oe:value="10.168.110.19"/>
   </PropertySection>
</Environment>
```

注 在该示例中，启用了 nsx_isSSHEnabled 和 nsx_allowSSHRootLogin。如果禁用，则无法通过 SSH 访问或登录到 NSX Manager 命令行。如果启用 nsx_isSSHEnabled 但未启用 nsx_allowSSHRootLogin，您可以通过 SSH 访问 NSX Manager，但无法以 root 身份登录。

5 使用 guestfish 将 guestinfo.xml 文件写入到 QCOW2 映像中。

注 在将 guestinfo 信息写入到 QCOW2 映像后，无法覆盖该信息。

```
sudo guestfish --rw -i -a nsx-unified-appliance-<BuildNumber>.qcow2 upload guestinfo /config/
guestinfo
```

6 使用 virt-install 命令部署 QCOW2 映像。

vCPU 和 RAM 值适用于大型虚拟机。网络名称和端口组名称特定于您的环境。模型必须为 virtio。

```
sudo virt-install \
--import \
--ram 48000 \
--vcpus 12 \
--name <manager-name> \
--disk path=<manager-qcow2-file-path>,bus=virtio,cache=none \
--network network=<network-name>,portgroup=<portgroup-name>,model=virtio \
--noautoconsole              \
--cpu mode=host-passthrough,cache.mode=passthrough

Starting install...
Domain installation still in progress. Waiting for installation to complete.
```

7 确认部署了 NSX Manager。

```
virsh list --all

Id    Name             State
----------------------------------
18    nsx-manager1     running
```

8 打开 NSX Manager 控制台并登录。

```
virsh console 18
Connected to domain nsx-manager1
```

```
Escape character is ^]

nsx-manager1 login: admin
Password:
```

9 在引导 NSX Manager 后，以 admin 身份登录到 CLI 并运行 `get interface eth0` 命令以确认 IP 地址已按预期应用。

10 运行 `get services` 以确认服务正在运行。

11 确认 NSX Manager 具有所需的连接。

确保您可以执行以下任务。

- 从另一个计算机中 ping 通 NSX Manager。
- NSX Manager 可以 ping 通其默认网关。
- NSX Manager 可以使用管理接口 ping 通位于与 NSX Manager 相同的网络中的管理程序主机。
- NSX Manager 可以 ping 通其 DNS 服务器和 NTP 服务器。
- 如果已启用 SSH，请确保可以通过 SSH 访问 NSX Manager。

如果未建立连接，请确保虚拟设备的网络适配器位于正确的网络或 VLAN 中。

12 退出 KVM 控制台。

```
control-]
```

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

登录到新创建的 NSX Manager

安装 NSX Manager 后，可以使用用户界面执行其他安装任务。

安装 NSX Manager 后，可以加入 NSX-T Data Center 的客户体验提升计划 (CEIP)。有关该计划的详细信息（包括如何稍后加入或退出该计划），请参见 NSX-T Data Center 管理指南中的“客户体验提升计划”。

前提条件

确认安装了 NSX Manager。请参见安装 NSX Manager 和可用设备。

步骤

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

此时将显示 EULA。

2 阅读并接受 EULA 条款。

3 选择是否加入 VMware 客户体验提升计划 (CEIP)。

4 单击**保存**

在 KVM 主机上安装第三方软件包

要准备 KVM 主机以作为 Fabric 节点，您必须安装一些第三方软件包。

前提条件

- （RHEL 和 CentOS Linux）在安装第三方软件包之前，请运行以下命令以安装虚拟化软件包。

```
yum groupinstall “Virtualization Hypervisor”
yum groupinstall “Virtualization Client”
yum groupinstall "Virtualization Platform"
yum groupinstall "Virtualization Tools"
```

  如果无法安装软件包，可以在新安装上使用命令 `yum install glibc.i686 nspr` 手动安装它们。

- (Ubuntu) 在安装第三方软件包之前，请运行以下命令以安装虚拟化软件包。

```
apt install -y \
qemu-kvm \
libvirt-bin \
virtinst \
virt-manager \
virt-viewer \
ubuntu-vm-builder \
bridge-utils
```

- (SUSE Linux Enterprise Server) 在安装第三方软件包之前，请运行以下命令以安装虚拟化软件包。

```
libcap-progs
```

步骤

- 在 Ubuntu 上，运行 `apt-get install <package_name>` 以手动安装第三方软件包。

Ubuntu 18.04 软件包	Ubuntu 16.04 软件包
traceroute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl dkms make	libboost-chrono1.58.0 libboost-filesystem1.58.0 libgoogle-glog0v5 libgoogle-perftools4 libprotobuf9v5 traceroute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl libboost-date-time1.58.0 libleveldb1v5 python-gevent python-protobuf libboost-program-options1.58.0 dkms

- 在 RHEL 和 CentOS Linux 上，运行 `yum install <package_name>` 以手动安装第三方软件包。

  如果手动准备已注册到 RHEL 或 CentOS 的主机，则无需在主机上安装第三方软件包。

RHEL 7.6、7.5 和 7.4	CentOS Linux 7.5 和 7.4
wget PyYAML libunwind python-gevent python-mako python-netaddr redhat-lsb-core tcpdump	wget PyYAML libunwind python-gevent python-mako python-netaddr redhat-lsb-core tcpdump

- 在 SUSE 上，运行 `zypper install <package_name>` 以手动安装第三方软件包。

SUSE Linux Enterprise Server 12.0
python-simplejson python-PyYAML python-netaddr lsb-release

验证 RHEL KVM 主机上的 Open vSwitch 版本

如果 RHEL 主机上存在 OVS 软件包，必须移除现有软件包并安装支持的软件包。

受支持的 Open vSwitch 版本为 2.9.1.8614397-1。

步骤

1 确认在主机上已安装当前版本的 Open vSwitch。

```
ovs-vswitchd --version
```

如果您有 Open vSwitch 的较新或较旧版本，则必须将该 Open vSwitch 版本替换为受支持的版本。

2 打开 Open vSwitch 文件夹。

3 删除以下 Open vSwitch 软件包。

- kmod-openvswitch
- openvswitch
- openvswitch-selinux-policy

4 或者，添加 NSX-T Data Center 所需的 Open vSwitch 软件包。

a 以管理员身份登录到主机。

b 下载 nsx-lcp 文件并将其复制到 /tmp 目录中。

c 解压缩该软件包。

```
tar -zxvf nsx-lcp-<release>-rhel75_x86_64.tar.gz
```

d 导航到软件包目录。

```
cd nsx-lcp-rhel75_x86_64/
```

e 使用受支持的版本替换现有 Open vSwitch 版本。

- 对于较新的 Open vSwitch 版本，请使用 `--nodeps` 命令。

  例如，rpm -Uvh kmod-openvswitch-<new version>.e17.x86_64.rpm --nodeps

  rpm -Uvh openvswitch-*.rpm --nodeps

- 对于较旧的 Open vSwitch 版本，请使用 `--force` 命令。

  例如，rpm -Uvh kmod-openvswitch-<new version>.e17.x86_64.rpm --nodeps --force

  rpm -Uvh openvswitch-*.rpm --nodeps --force

使用 CLI 部署 NSX Manager 节点以形成群集

使用 CLI 将 NSX Manager 加入以形成群集可确保群集中的所有 NSX Manager 节点都可以相互通信。

前提条件

必须完成 NSX-T Data Center 组件的安装。

步骤

1 打开与第一个部署的 NSX Manager 节点的 SSH 会话。

2 使用管理员凭据登录。

3 在 NSX Manager 设备上，运行 `get certificate api thumbprint` 命令。

命令输出是该 NSX Manager 特有的数字串。

4 运行 `get cluster config` 命令以获取第一个部署的 NSX Manager 群集 ID。

5 将 NSX Manager 节点添加到群集。

> 注 必须在新部署的 NSX Manager 节点上运行 join 命令。

提供以下 NSX Manager 信息：

- 要加入的节点的主机名或 IP 地址
- Cluster ID
- 用户名
- 密码
- 证书指纹

可以使用 CLI 命令或 API 调用。

- CLI 命令

```
host> join <NSX-Manager-IP> cluster-id <cluster-id> username<NSX-Manager-username>
password<NSX-Manager-password> thumbprint <NSX-Manager1's-thumbprint>
```

- API 调用 `POST https://<nsx-mgr>/api/v1/cluster?action=join_cluster`

加入和群集稳定过程可能需要 10-15 分钟的时间。

6 将第三个 NSX Manager 节点添加到群集。

重复步骤 5。

7 在主机上运行 `get cluster status` 命令以确认群集状态。

8 选择 **系统 > 设备 > 概览**并确认群集连接。

后续步骤

创建传输区域。请参见 创建独立主机或裸机服务器传输节点。

使用 ISO 文件或 PXE 安装 NSX Edge

您可以使用 PXE 以自动方式在裸机上安装 NSX Edge 设备或安装为虚拟机。

注 NSX Manager 不支持 PXE 引导安装。您也无法配置网络设置，例如，IP 地址、网关、网络掩码、NTP 和 DNS。

通过 ISO 文件将 NSX Edge 安装为虚拟设备

您可以使用 ISO 文件以手动方式安装 NSX Edge 虚拟机。

重要事项 NSX-T Data Center 组件虚拟机安装包括 VMware Tools。NSX-T Data Center 设备不支持移除或升级 VMware Tools。

前提条件

- 请参阅 NSX Edge 安装中的 NSX Edge 网络要求。

步骤

1 转到您的 MyVMware 帐户 (myvmware.com)，然后导航到 **VMware NSX-T Data Center > 下载**。

2 找到并下载 NSX Edge 的 ISO 文件。

3 在 vSphere Client 中，选择主机数据存储。

4 选择**文件 > 上载文件 > 将文件上载到数据存储**，浏览到 ISO 文件，然后上载。

如果使用的是自签名证书，请在浏览器中打开 IP 地址并接受证书，然后重新上载 ISO 文件。

5 在 vSphere Client 清单中，选择上载 ISO 文件的主机。或者在 vSphere Client 中，

6 右键单击并选择**新建虚拟机**。

7 选择 NSX Edge 设备的计算资源。

8 选择一个数据存储以存储 NSX Edge 设备文件。

9 接受您的 NSX Edge 虚拟机的默认兼容性。

10 选择您的 NSX Edge 虚拟机支持的 ESXi 操作系统。

11 配置虚拟硬件。

- 新硬盘 - **200 GB**
- 新网络 - **虚拟机网络**
- 新 CD/DVD 驱动器 - **数据存储 ISO 文件**

  您必须单击**连接**将 NSX Edge ISO 文件绑定到虚拟机。

12 打开新 NSX Edge 虚拟机的电源。

13 在 ISO 引导期间，打开虚拟机控制台并选择**自动安装**。

在按 Enter 后，可能会出现 10 秒的暂停。

在安装期间，安装程序将提示您输入管理接口的 VLAN ID。选择**是**，然后输入一个 VLAN ID，以便为网络接口创建一个 VLAN 子接口。如果您不希望在数据包上配置 VLAN 标记，请选择**否**。

在开机期间，虚拟机通过 DHCP 请求网络配置。如果 DHCP 在您的环境中不可用，安装程序将提示您输入 IP 设置。

默认情况下，root 登录密码为 **vmware**，admin 登录密码为 **default**。

在首次登录时，将提示您更改密码。这种密码更改方法具有严格的复杂性规则，包括以下内容：

- 至少 12 个字符
- 至少一个小写字母
- 至少一个大写字母
- 至少一个数字
- 至少一个特殊字符
- 至少 5 个不同的字符
- 没有字典词语
- 没有回文
- 不允许使用超过四个单调字符的序列

重要事项 在设置足够复杂的密码后，设备上的核心服务才会启动。

14 为了获得最佳性能，请为 NSX Edge 设备预留内存。

将预留内存设置为可确保 NSX Edge 足以高效运行。请参见 NSX Edge 虚拟机系统要求。

15 在 NSX Edge 启动后，使用管理员凭据登录到 CLI。

注 在 NSX Edge 启动后，如果第一次不使用管理员凭据进行登录，则不会在 NSX Edge 上自动启动数据层面服务。

16 可以使用三种方法配置管理接口。

- 未标记的接口。该接口类型创建一个带外管理接口。

  (DHCP) `set interface eth0 dhcp plane mgmt`

  （静态） `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt`

- 标记的接口。

  `set interface eth0 vlan <vlan_ID> plane mgmt`

  (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

  （静态）`set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

- 带内接口。

  `set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt`

  (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

  （静态） `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

17 （可选）启动 SSH 服务。运行 `start service ssh`。

18 运行 `get interface eth0.<vlan_ID>` 命令以验证是否按预期方式应用了 IP 地址。

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
  Address: 192.168.110.37/24
  MAC address: 00:50:56:86:62:4d
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

注 在 NSX 未管理的主机上启动 NSX Edge 虚拟机时，请确认在数据网卡的物理主机交换机上将 MTU 设置设为 1600（而不是 1500）。

19 （标记的接口和带内接口）在创建新的 VLAN 管理接口之前，必须清除任何现有的 VLAN 管理接口。

`Clear interface eth0.<vlan_ID>`

要设置新接口，请参阅步骤 15。

20 确认 NSX Edge 设备具有所需的连接。

如果已启用 SSH，请确保可以通过 SSH 访问 NSX Edge。

- 您可以 ping 通 NSX Edge。
- NSX Edge 可以 ping 通其默认网关。
- NSX Edge 可以 ping 通位于与 NSX Edge 相同的网络中的管理程序主机。
- NSX Edge 可以 ping 通其 DNS 服务器和 NTP 服务器。

21 解决连接问题。

注 如果未建立连接，请确保虚拟机网络适配器位于正确的网络或 VLAN 中。

默认情况下，NSX Edge 数据路径声明管理网卡（具有 IP 地址和默认路由的网卡）以外的所有虚拟机网卡。如果错误地将一个网卡分配为管理接口，请按照以下步骤使用 DHCP 将管理 IP 地址分配给正确的网卡。

a 登录到 CLI，然后键入 **`stop service dataplane`** 命令。

b 键入 **`set interface`** ***`interface`*** **`dhcp plane mgmt`** 命令。

c 将 *interface* 放入 DHCP 网络中，并等待为该 *interface* 分配一个 IP 地址。

d 键入 **`start service dataplane`** 命令。

将在 NSX Edge 上的 **get interfaces** 和 **get physical-port** 命令中显示用于 VLAN 上行链路和隧道覆盖网络的数据路径 fp-ethX 端口。

后续步骤

如果未将 NSX Edge 加入管理层面，请参见将 NSX Edge 加入管理层面。

在裸机上通过 ISO 文件安装 NSX Edge

您可以使用 ISO 文件以手动方式在裸机上安装 NSX Edge 设备。这包括配置网络设置，例如，IP 地址、网关、网络掩码、NTP 和 DNS。

前提条件

- 确认系统 BIOS 模式已设置为传统 BIOS。
- 请参阅 NSX Edge 安装中的 NSX Edge 网络要求。

步骤

1 在 **nsx-edgenode > publish > xenial_amd64** 文件夹中，找到 NSX Edge 设备 ISO 文件。

将 ISO 文件下载到计算机上。

2 登录到裸机的 ILO。

3 单击虚拟控制台预览中的**启动**。

4 选择**虚拟介质 > 连接虚拟介质**。

等待几秒钟以供虚拟介质连接。

5 选择**虚拟介质 > 映射 CD/DVD** 并浏览到 ISO 文件。

6 选择**下次引导 > 虚拟 CD/DVD/ISO**。

7 选择**电源 > 重置系统 (热引导)**。

安装持续时间取决于裸机环境。

8 选择**自动安装**。

在按 Enter 后，可能会出现 10 秒的暂停。

9 选择适用的主网络接口。

在开机期间，安装程序通过 DHCP 请求网络配置。如果 DHCP 在您的环境中不可用，安装程序将提示您输入 IP 设置。

默认情况下，root 登录密码为 **vmware**，admin 登录密码为 **default**。

10 打开 NSX Edge 控制台以跟踪引导过程。

如果未打开控制台窗口，请确保允许弹出窗口。

11 在 NSX Edge 启动后，使用管理员凭据登录到 CLI。

注 在 NSX Edge 启动后，如果第一次不使用管理员凭据进行登录，则不会在 NSX Edge 上自动启动数据层面服务。

12 重新引导后，可以使用管理员凭据或 root 凭据进行登录。默认 root 密码为 **vmware**。

13 可以使用三种方法配置管理接口。

- 未标记的接口。该接口类型创建一个带外管理接口。

  (DHCP) `set interface eth0 dhcp plane mgmt`

  （静态） `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt`

- 标记的接口。

  `set interface eth0 vlan <vlan_ID> plane mgmt`

  (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

  （静态）`set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

- 带内接口。

  `set interface mac <mac_address> vlan <vlan_ID> in-band plane mgmt`

  (DHCP) `set interface eth0.<vlan_ID> dhcp plane mgmt`

  （静态） `set interface eth0.<vlan_ID> ip <CIDR> gateway <gateway-ip> plane mgmt`

14 运行 `get interface eth0.<vlan_ID>` 命令以验证是否按预期方式应用了 IP 地址。

```
nsx-edge-1> get interface eth0.100

Interface: eth0.100
  Address: 192.168.110.37/24
  MAC address: 00:50:56:86:62:4d
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

注 在 NSX 未管理的主机上启动 NSX Edge 虚拟机时，请确认在数据网卡的物理主机交换机上将 MTU 设置设为 1600（而不是 1500）。

15 （标记的接口和带内接口）在创建新的 VLAN 管理接口之前，必须清除任何现有的 VLAN 管理接口。

`clear interface eth0.<vlan_ID>`

要设置新接口，请参阅步骤 13。

16 确认 NSX Edge 设备具有所需的连接。

如果已启用 SSH，请确保可以通过 SSH 访问 NSX Edge。

- 您可以 ping 通 NSX Edge。
- NSX Edge 可以 ping 通其默认网关。
- NSX Edge 可以 ping 通位于与 NSX Edge 相同的网络中的管理程序主机。
- NSX Edge 可以 ping 通其 DNS 服务器和 NTP 服务器。

17 解决连接问题。

注 如果未建立连接，请确保虚拟机网络适配器位于正确的网络或 VLAN 中。

默认情况下，NSX Edge 数据路径声明管理网卡（具有 IP 地址和默认路由的网卡）以外的所有虚拟机网卡。如果错误地将一个网卡分配为管理接口，请按照以下步骤使用 DHCP 将管理 IP 地址分配给正确的网卡。

a 登录到 CLI，然后键入 **`stop service dataplane`** 命令。

b 键入 **`set interface`** ***`interface`*** **`dhcp plane mgmt`** 命令。

c 将 *interface* 放入 DHCP 网络中，并等待为该 *interface* 分配一个 IP 地址。

d 键入 **`start service dataplane`** 命令。

将在 NSX Edge 上的 **get interfaces** 和 **get physical-port** 命令中显示用于 VLAN 上行链路和隧道覆盖网络的数据路径 fp-ethX 端口。

后续步骤

将 NSX Edge 加入管理层面。请参见将 NSX Edge 加入管理层面。

在 PXE 服务器上安装 NSX Edge

PXE 由几个组件组成：DHCP、HTTP 和 TFTP。该过程说明了如何在 Ubuntu 上设置 PXE 服务器。

DHCP 将 IP 设置动态分配给 NSX-T Data Center 组件，例如，NSX Edge。在 PXE 环境中，DHCP 服务器允许 NSX Edge 自动请求和接收 IP 地址。

TFTP 是一种文件传输协议。TFTP 服务器始终侦听网络上的 PXE 客户端。检测到任何网络 PXE 客户端请求 PXE 服务时，它会提供 NSX-T Data Center 组件 ISO 文件以及 preseed 文件中包含的安装设置。

前提条件

- 必须在您的部署环境中具有 PXE 服务器。可以在任何 Linux 发布版本上设置 PXE 服务器。PXE 服务器必须具有两个接口，一个接口用于外部通信，另一个接口用于提供 DHCP IP 和 TFTP 服务。

  如果具有多个管理网络，您可以添加从 NSX-T Data Center 设备到其他网络的静态路由。
- 确认预植入的配置文件中 -- 后设置的参数 net.ifnames=0 和 biosdevname=0 在重新引导后继续存在。
- 请参阅 NSX Edge 安装中的 NSX Edge 网络要求。

步骤

1 （可选） 使用 kickstart 文件在 Ubuntu 服务器上设置新的 TFTP 或 DHCP 服务。

  kickstart 文件是一个文本文件，其中包含在首次引导后在设备上运行的 CLI 命令。

  根据指向的 PXE 服务器命名 kickstart 文件。例如：

```
nsxcli.install
```

  该文件必须复制到 Web 服务器，例如，在 `/var/www/html/nsx-edge/nsxcli.install` 中。

  在 kickstart 文件中，您可以添加 CLI 命令。例如，要配置管理接口的 IP 地址，请运行以下命令：

```
stop dataplane
set interface eth0 <ip-cidr-format> plane mgmt
start dataplane
```

  要更改 admin 用户密码，请运行以下命令：

```
set user admin password <new_password> old-password <old-password>
```

  如果在 preseed.cfg 文件中指定一个密码，请在 kickstart 文件中使用相同的密码。否则，将使用默认密码“default”。

  要将 NSX Edge 加入管理层面，请运行以下命令：

```
join management-plane <manager-ip> thumbprint <manager-thumbprint> username <manager-username>
password <manager password>
```

2 创建两个接口，一个接口用于管理，另一个接口用于 DHCP 和 TFTP 服务。

  确保 DHCP/TFTP 接口位于 NSX Edge 所在的同一子网中。

例如，如果 NSX Edge 管理接口位于 192.168.210.0/24 子网中，请将 eth1 放在该相同子网中。

```
# The loopback network interface
auto lo
iface lo inet loopback

# PXE server's management interface
auto eth0
iface eth0 inet static
  address 192.168.110.81
  gateway 192.168.110.1
  netmask 255.255.255.0
  dns-nameservers 192.168.110.10

# PXE server's DHCP/TFTP interface
auto eth1
iface eth1 inet static
  address 192.168.210.82
  gateway 192.168.210.1
  netmask 255.255.255.0
  dns-nameservers 192.168.110.10
```

3 安装 DHCP 服务器软件。

```
sudo apt-get install isc-dhcp-server -y
```

4 编辑 `/etc/default/isc-dhcp-server` 文件，并添加提供 DHCP 服务的接口。

```
INTERFACES="eth1"
```

5 （可选） 如果要将该 DHCP 服务器作为本地网络的正式 DHCP 服务器，请在 `/etc/dhcp/dhcpd.conf` 文件中取消注释 **authoritative;** 行。

```
...
authoritative;
...
```

6 在 `/etc/dhcp/dhcpd.conf` 文件中，为 PXE 网络定义 DHCP 设置。

例如：

```
subnet 192.168.210.0 netmask 255.255.255.0 {
   range 192.168.210.90 192.168.210.95;
   option subnet-mask 255.255.255.0;
   option domain-name-servers 192.168.110.10;
   option routers 192.168.210.1;
   option broadcast-address 192.168.210.255;
   default-lease-time 600;
   max-lease-time 7200;
}
```

7 启动 DHCP 服务。

```
sudo service isc-dhcp-server start
```

8 验证 DHCP 服务是否正在运行。

```
service --status-all | grep dhcp
```

9 安装 PXE 引导所需的 Apache、TFTP 和其他组件。

```
sudo apt-get install apache2 tftpd-hpa inetutils-inetd
```

10 验证 TFTP 和 Apache 是否正在运行。

```
service --status-all | grep tftpd-hpa
service --status-all | grep apache2
```

11 将以下几行添加到 /etc/default/tftpd-hpa 文件中。

```
RUN_DAEMON="yes"
OPTIONS="-l -s /var/lib/tftpboot"
```

12 将下一行添加到 /etc/inetd.conf 文件中。

```
tftp    dgram   udp    wait    root    /usr/sbin/in.tftpd /usr/sbin/in.tftpd -s /var/lib/tftpboot
```

13 重新启动 TFTP 服务。

```
sudo /etc/init.d/tftpd-hpa restart
```

14 将 NSX Edge 安装程序 ISO 文件复制或下载到临时文件夹。

15 挂载 ISO 文件，并将安装组件复制到 TFTP 服务器和 Apache 服务器中。

```
            sudo mount -o loop ~/nsx-edge.<build>.iso /mnt
            cd /mnt
sudo cp -fr install/netboot/* /var/lib/tftpboot/
sudo mkdir /var/www/html/nsx-edge
sudo cp -fr /mnt/* /var/www/html/nsx-edge/
```

16 （可选） 编辑 /var/www/html/nsx-edge/preseed.cfg 文件以修改加密的密码。

您可以使用 Linux 工具（如 mkpasswd）创建密码哈希值。

```
sudo apt-get install whoissudo mkpasswd -m sha-512

Password:
$6$SUFGqs[...]FcoHLijOuFD
```

a 修改 root 密码，编辑 /var/www/html/nsx-edge/preseed.cfg 并搜索下一行：

```
d-i passwd/root-password-crypted password $6$tgmLNLMp$9BuAHhN...
```

b 替换哈希字符串。

您不需要转义任何特殊字符，例如 $、'、" 或 \。

c 在 preseed.cfg 中添加 usermod 命令以设置 root 和/或 admin 密码。

例如，搜索 echo 'VMware NSX Edge' 行并添加以下命令。

```
usermod --password '\$6\$VS3exId0aKmzW\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00bO2hUF8u/' root; \
usermod --password '\$6\$VS3exId0aKmzW\$U3g0V7BF0DXlmRI.LR0v/VgloxVotEDp00bO2hUF8u/' admin; \
```

哈希字符串是一个示例。您必须转义所有特殊字符。第一个 usermod 命令中的 root 密码替换在 d-i passwd/root-password-crypted password 6tgm... 中设置的密码。

如果使用 usermod 命令设置密码，则在首次登录时不会提示用户更改密码。否则，用户必须在首次登录时更改密码。

17 将以下几行添加到 /var/lib/tftpboot/pxelinux.cfg/default 文件中。

将 192.168.210.82 替换为 TFTP 服务器的 IP 地址。

```
label nsxedge
    kernel ubuntu-installer/amd64/linux
    ipappend 2
    append netcfg/dhcp_timeout=60 auto=true priority=critical vga=normal partman-lvm/
device_remove_lvm=true netcfg/choose_interface=auto debian-installer/allow_unauthenticated=true
preseed/url=http://192.168.210.82/nsx-edge/preseed.cfg mirror/country=manual mirror/http/
hostname=192.168.210.82 nsx-kickstart/url=http://192.168.210.82/nsx-edge/nsxcli.install mirror/
http/directory=/nsx-edge initrd=ubuntu-installer/amd64/initrd.gz mirror/suite=xenial --
```

18 将以下几行添加到 /etc/dhcp/dhcpd.conf 文件中。

将 192.168.210.82 替换为 DHCP 服务器的 IP 地址。

```
allow booting;
allow bootp;

next-server 192.168.210.82; #Replace this IP address
filename "pxelinux.0";
```

19 重新启动 DHCP 服务。

```
sudo service isc-dhcp-server restart
```

注 如果返回错误（例如：“stop: Unknown instance: start: Job failed to start”），请运行 `sudo /etc/init.d/isc-dhcp-server stop`，然后运行 `sudo /etc/init.d/isc-dhcp-server start`。`sudo /etc/init.d/isc-dhcp-server start` 命令返回有关错误来源的信息。

后续步骤

使用 ISO 文件在裸机上安装 NSX Edge。请参见在裸机上通过 ISO 文件安装 NSX Edge 或通过 ISO 文件将 NSX Edge 安装为虚拟设备。

将裸机服务器配置为使用 NSX-T Data Center

6

要在裸机服务器上使用 NSX-T Data Center，必须安装支持的第三方软件包。

NSX-T Data Center 通过以下两种方式支持裸机服务器：作为主机传输节点和作为 NSX Manager 的主机。

请确保具有支持的裸机服务器版本。请参见裸机服务器系统要求。

注 如果 NSX Edge 采用虚拟机规格，并且您打算使用 NSX DHCP 服务（部署在基于 VLAN 的逻辑交换机上），您必须在部署了 NSX Edge 的裸机主机上将“伪传输”选项设置为“接受”。请参见 vSphere 产品文档中的“伪传输”。

本章讨论了以下主题：

在裸机服务器上安装第三方软件包

要准备裸机服务器作为结构层节点，您必须安装一些第三方软件包。

前提条件

- 确认执行安装的用户具有管理权限以执行以下操作，其中的一些操作可能需要具有 sudo 权限：
  - 下载并解压缩包。
  - 运行 dpkg 或 rpm 命令以安装/卸载 NSX 组件。
  - 执行 nsxcli 命令以执行加入管理层面命令。
- 确认已安装虚拟化软件包。
  - Redhat 或 CentOS - `yum install libvirt-libs`
  - Ubuntu - `apt-get install libvirt0`
  - SUSE - `zypper install libvirt-libs`

步骤

- 在 Ubuntu 上，运行 `apt-get install <package_name>` 安装第三方软件包。

Ubuntu18.04	Ubuntu16.04
traceroute python-mako python-netaddr python-simplejson python-unittest2 python-yaml python-openssl dkms libvirt0	libunwind8 libgflags2v5 libgoogle-perftools4 traceroute python-mako python-simplejson python-unittest2 python-yaml python-netaddr libboost-filesystem1.58.0 libboost-chrono1.58.0 libgoogle-glog0v5 dkms libboost-date-time1.58.0 python-protobuf python-gevent libsnappy1v5 libleveldb1v5 libboost-program-options1.58.0 libboost-thread1.58.0 libboost-iostreams1.58.0 libvirt0

- 在 RHEL 或 CentOS 上，运行 `yum install` 安装第三方软件包。

RHEL 7.4、7.5 和 7.6	CentOS 7.4、7.5 和 7.6
tcpdump boost-filesystem PyYAML boost-iostreams boost-chrono python-mako python-netaddr python-six gperftools-libs libunwind snappy boost-date-time c-ares redhat-lsb-core wget net-tools yum-utils lsof python-gevent libev python-greenlet libvirt-libs	tcpdump boost-filesystem PyYAML boost-iostreams boost-chrono python-mako python-netaddr python-six gperftools-libs libunwind snappy boost-date-time c-ares redhat-lsb-core wget net-tools yum-utils lsof python-gevent libev python-greenlet libvirt-libs

- 在 SUSE 上，运行 `zypper install <package_name>` 以手动安装第三方软件包。

  SUSE 12.0

  ```
  net-tools
  tcpdump
  python-simplejson
  python-netaddr
  python-PyYAML
  python-six
  libunwind
  wget
  lsof
  libcap-progs
  libvirt-libs
  ```

创建裸机服务器工作负载的应用程序接口

创建或迁移裸机服务器工作负载的应用程序接口之前，必须配置 NSX-T Data Center 并安装 Linux 第三方软件包。

NSX-T Data Center 不支持 Linux OS 接口绑定。您必须在裸机服务器传输节点中使用 Open vSwitch (OVS) 绑定。请参见知识库文章 67835 裸机服务器在 NSX-T 传输节点配置中支持 OVS 绑定。

步骤

1. 安装所需的第三方软件包。

   请参见在裸机服务器上安装第三方软件包。

2. 配置 TCP 和 UDP 端口。

   请参见由 ESXi、KVM 主机和裸机服务器使用的 TCP 和 UDP 端口。

3. 将裸机服务器添加到 NSX-T Data Center 结构层并创建传输节点。

   请参见 创建独立主机或裸机服务器传输节点。

4. 使用 Ansible playbook 创建应用程序接口。

   请参见 https://github.com/vmware/bare-metal-server-integration-with-nsxt。

配置 NSX Manager 群集

7

以下小节介绍了如何配置 NSX Manager 群集，详细说明了群集要求，并为特定站点部署提供了建议。此外，还介绍了如何将 vSphere HA 与 NSX-T Data Center 一起使用，以便在运行 NSX Manager 节点的主机发生故障时快速进行恢复。

本章讨论了以下主题：

- NSX Manager 群集要求
- 单站点、双站点及多站点的 NSX Manager 群集要求

NSX Manager 群集要求

以下要求适用于 NSX Manager 群集配置：

- 在生产环境中，NSX Manager 群集必须具有三个成员，以避免管理和控制层面发生中断。

  每个群集成员应放在唯一的管理程序主机上（共有三个物理管理程序主机）。这是避免单个物理管理程序主机故障影响 NSX 控制层面所必需的。建议您应用反关联性规则，以确保所有三个群集成员在不同的主机上运行。

  正常生产运行状态是三节点 NSX Manager 群集。不过，您可以添加额外的临时 NSX Manager 节点以允许更改 IP 地址。

  重要事项 从 NSX-T Data Center 2.4 开始，NSX Manager 包含 NSX 中央控制层面进程。该服务对于 NSX 正常运行至关重要。如果 NSX Manager 完全丢失，或者群集从 3 个 NSX Manager 减少到 1 个 NSX Manager，则无法对环境的拓扑进行更改，并且依赖于 NSX 的计算机的 vMotion 将失败。

- 对于没有生产工作负载的实验室和概念证明部署，您可以运行单个 NSX Manager 以节省资源。NSX Manager 节点可以部署在 ESXi 或 KVM 上。不过，不支持在 ESXi 和 KVM 上进行 Manager 混合部署。

重要事项 NSX-T Data Center 部署中的站点数会影响这些要求。请参见 单站点、双站点及多站点的 NSX Manager 群集要求。

单站点、双站点及多站点的 NSX Manager 群集要求

根据您的部署是单站点、双站点还是多站点部署，您的 NSX Manager 群集配置会有所不同。

您可以将 vSphere HA 与 NSX-T Data Center 一起使用，以便在运行 NSX Manager 节点的主机发生故障时快速进行恢复。

注 请参见 vSphere 产品文档中的创建和使用 vSphere HA 群集。

单站点要求和建议

以下建议适用于单站点 NSX-T Data Center 部署。

- 建议您将 NSX Manager 放置在不同的主机上，以避免一个主机发生故障时影响多个管理器。
- 各 NSX Manager 之间的最大延迟为 10 毫秒。
- 您可以将 NSX Manager 放置在不同的 vSphere 群集或一个共同的 vSphere 群集中。
- 建议您将 NSX Manager 放置在不同的管理子网或一个共享管理子网中。在使用 vSphere HA 时，建议使用一个共享管理子网，这样由 vSphere 恢复的 NSX Manager 便可以保留其 IP 地址。
- 此外，还建议您将 NSX Manager 放置在共享存储上。对于 vSphere HA，请查看该解决方案的要求。

您也可以将 vSphere HA 与 NSX-T 一起使用，以便在运行 NSX Manager 的主机发生故障时，恢复丢失的 NSX Manager。

场景示例：

- 一个 vSphere 群集，其中部署了所有三个 NSX Manager。
- 该 vSphere 群集包含四个或更多主机：
  - 部署了 nsxmgr-01 的 Host-01
  - 部署了 nsxmgr-02 的 Host-02
  - 部署了 nsxmgr-03 的 Host-03
  - 未部署任何 NSX Manager 的 Host-04
- vSphere HA 配置为将任意主机（例如，Host-01）中丢失的任意 NSX Manager（例如，nsxmgr-01）恢复到 Host-04。

因此，如果运行 NSX Manager 的任意主机丢失，vSphere 将在 Host-04 上恢复丢失的 NSX Manager。

双站点要求和建议

以下建议适用于双站点（站点 A/站点 B）NSX-T Data Center 部署。

- 如果没有 vSphere HA，则不建议在双站点场景中部署 NSX Manager。在此场景中，一个站点需要部署两个 NSX Manager，并且该站点丢失时将影响 NSX-T Data Center 的运行。
- 如果具有 vSphere HA，则可以在双站点场景中部署 NSX Manager，且在部署时应考虑以下事项：
  - 一个延伸的 vSphere 群集包含 NSX Manager 的所有主机。

- 所有三个 NSX Manager 均部署到一个共同的管理子网/VLAN，以便在恢复丢失的 NSX Manager 时保留 IP 地址。
- 有关各站点之间的延迟，请参见存储产品要求。

场景示例：

- 一个 vSphere 群集，其中部署了所有三个 NSX Manager。
- 该 vSphere 群集包含六个或更多主机，其中站点 A 中有三个主机，站点 B 中有三个主机。
- 三个 NSX Manager 部署到不同的主机，其他主机则用于放置恢复的 NSX Manager：

  站点 A：

  - 部署了 nsxmgr-01 的 Host-01
  - 部署了 nsxmgr-02 的 Host-02
  - 部署了 nsxmgr-03 的 Host-03

  站点 B：

  - 未部署任何 NSX Manager 的 Host-04
  - 未部署任何 NSX Manager 的 Host-05
  - 未部署任何 NSX Manager 的 Host-06
- vSphere HA 配置为将站点 A 内的任意主机（例如，Host-01）中丢失的任意 NSX Manager（例如，nsxmgr-01）恢复到站点 B 内的一个主机。

因此，当站点 A 发生故障时，vSphere HA 会将所有 NSX Manager 恢复到站点 B 内的主机。

重要事项 您必须正确配置反关联性规则，以防止将 NSX Manager 恢复到同一个主机。

多站点（三个或更多）要求和建议

以下建议适用于多站点（站点 A/站点 B/站点 C）NSX-T Data Center 部署。

在具有三个或更多站点的场景中，不论是否具有 vSphere HA，您都可以部署 NSX Manager。

如果在没有 vSphere HA 的情况下部署：

- 建议每个站点使用单独的管理子网或 VLAN。
- 各 NSX Manager 之间的最大延迟为 10 毫秒。

场景示例（三个站点）：

- 三个独立的 vSphere 群集，每个站点一个。
- 每个站点至少有一个主机在运行 NSX Manager：
  - 部署了 nsxmgr-01 的 Host-01
  - 部署了 nsxmgr-02 的 Host-02
  - 部署了 nsxmgr-03 的 Host-03

故障场景：

- 单个站点故障：其他站点中的其余两个 NSX Manager 继续运行。NSX-T Data Center 处于已降级状态，但仍可正常运行。建议您手动部署第三个 NSX Manager，以取代丢失的群集成员。
- 两个站点故障：无法形成仲裁机制，因此影响 NSX-T Data Center 运行。

根据环境条件（如 CPU 速度、磁盘性能和其他部署因素），恢复 NSX Manager 可能需要长达 20 分钟时间。

传输区域和传输节点

8

传输区域和传输节点是 NSX-T Data Center 中的重要概念。

本章讨论了以下主题：

- 创建传输区域
- 创建 IP 池以分配隧道端点 IP 地址
- 增强型数据路径
- 对配置文件进行配置
- 创建独立主机或裸机服务器传输节点
- 手动安装 NSX-T Data Center 内核模块
- NSX Edge 网络设置
- 创建 NSX Edge 传输节点
- 创建 NSX Edge 群集

创建传输区域

传输区域确定哪些主机可以参与使用特定的网络，进而确定哪些虚拟机可以参与使用该网络。传输区域限制可以“看到”某个逻辑交换机的主机（从而限制可以连接到该逻辑交换机的虚拟机）以实现该目的。传输区域可以跨一个或多个主机群集。

根据您的要求，NSX-T Data Center 环境可能包含一个或多个传输区域。一个主机可以属于多个传输区域。一个逻辑交换机只能属于一个传输区域。

NSX-T Data Center 不允许连接位于第 2 层网络中的不同传输区域的虚拟机。逻辑交换机的跨度仅限于一个传输区域，因此不同传输区域中的虚拟机不能位于同一第 2 层网络。

主机传输节点和 NSX Edge 均使用覆盖网络传输区域。在将主机或 NSX Edge 传输节点添加到覆盖网络传输区域时，将在主机或 NSX Edge 上安装 N-VDS。

NSX Edge 和主机传输节点将 VLAN 传输区域用于其 VLAN 上行链路。在将 NSX Edge 添加到 VLAN 传输区域时，将在 NSX Edge 上安装 VLAN N-VDS。

N-VDS 将逻辑路由器上行链路和下行链路绑定到物理网卡以支持虚拟到物理数据包流量。

在创建传输区域时，您必须提供 N-VDS 的名称，以后在该传输区域中添加传输节点时，将在这些节点上安装 N-VDS。N-VDS 名称可以是所需的任意名称。

步骤

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

2 选择**系统 > 结构层 > 传输区域 > 添加**。

3 输入传输区域的名称和描述（可选）。

4 输入 N-VDS 的名称。

5 选择 N-VDS 模式。

- 适用于所有受支持主机的**标准**模式。
- **增强型数据路径**是仅适用于传输区域中可属于 ESXi 主机版本 6.7 和更高版本类型的传输节点的网络连接堆栈模式。

6 如果 N-VDS 模式设置为“标准”，则选择流量类型。

选项有**覆盖网络**和 **VLAN**。

7 如果 N-VDS 模式设置为“增强型数据路径”，则选择流量类型。

选项有**覆盖网络**和 **VLAN**。

注 在增强型数据路径模式下，仅支持特定的网卡配置。请确保配置支持的网卡。

8 输入一个或多个上行链路绑定策略名称。这些命名绑定策略可供连接到传输区域的逻辑交换机使用。如果逻辑交换机未找到匹配的命名绑定策略，则使用默认的上行链路绑定策略。

9 在**传输区域**页面上查看新传输区域。

10 （可选） 还可以使用 `GET https://<nsx-mgr>/api/v1/transport-zones` API 调用查看新传输区域。


```
{
  "cursor": "00369b661aed-1eaa-4567-9408-ccbcfe50b416tz-vlan",
  "result_count": 2,
  "results": [
    {
      "resource_type": "TransportZone",
      "description": "comp overlay transport zone",
      "id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "display_name": "tz-overlay",
      "host_switch_name": "overlay-hostswitch",
      "transport_type": "OVERLAY",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ],
      "_create_time": 1459547126454,
      "_last_modified_user": "admin",
```

```
      "_system_owned": false,
      "_last_modified_time": 1459547126454,
      "_create_user": "admin",
      "_revision": 0,
      "_schema": "/v1/schema/TransportZone"
    },
    {
      "resource_type": "TransportZone",
      "description": "comp vlan transport zone",
      "id": "9b661aed-1eaa-4567-9408-ccbcfe50b416",
      "display_name": "tz-vlan",
      "host_switch_name": "vlan-uplink-hostwitch",
      "transport_type": "VLAN",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ],
      "_create_time": 1459547126505,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_last_modified_time": 1459547126505,
      "_create_user": "admin",
      "_revision": 0,
      "_schema": "/v1/schema/TransportZone"
    }
  ]
}
```


后续步骤

（可选）创建一个自定义传输区域配置文件并将其绑定到传输区域。您可以使用 `POST /api/v1/transportzone-profiles` API 创建自定义传输区域配置文件。没有用于创建传输区域配置文件的 UI 工作流。在创建传输区域配置文件后，您可以使用 `PUT /api/v1/transport-zones/<transport-zone-id>` API 将其绑定到传输区域。

创建传输节点。请参见 创建独立主机或裸机服务器传输节点。

创建 IP 池以分配隧道端点 IP 地址

您可以使用 IP 池以分配隧道端点地址。隧道端点是在外部 IP 标头中使用的源和目标 IP 地址，以便标识发出和结束 NSX-T Data Center 覆盖网络帧封装的管理程序主机。还可以使用 DHCP 或手动配置的 IP 池以分配隧道端点 IP 地址。

如果同时使用 ESXi 和 KVM 主机，一种设计方法可能是将两个不同的子网用于 ESXi 隧道端点 IP 池 (sub_a) 和 KVM 隧道端点 IP 池 (sub_b)。在这种情况下，必须在 KVM 主机上添加具有专用默认网关的 sub_a 静态路由。

在 Ubuntu 主机上生成的路由表的示例，其中 sub_a = 192.168.140.0，sub_b = 192.168.150.0。（例如，管理子网可能是 192.168.130.0）。

内核 IP 路由表：

```
Destination          Gateway          Genmask          Iface
0.0.0.0              192.168.130.1    0.0.0.0          eth0
192.168.122.0        0.0.0.0          255.255.255.0    virbr0
192.168.130.0        0.0.0.0          255.255.255.0    eth0
192.168.140.0        192.168.150.1    255.255.255.0    nsx-vtep0.0
192.168.150.0        0.0.0.0          255.255.255.0    nsx-vtep0.0
```

可以使用至少两种不同的方法添加路由。在这两种方法中，仅当通过编辑接口添加路由时才能在主机重新引导后保持该路由。使用 route add 命令添加路由在主机重新引导后不会保持。

```
route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.150.1 dev nsx-vtep0.0
```

在 /etc/network/interfaces 中的“up ifconfig nsx-vtep0.0 up”前面添加以下静态路由：

```
post-up route add -net 192.168.140.0 netmask 255.255.255.0 gw 192.168.150.1
```

步骤

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

2 选择**高级网络和安全 > 清单 > 组 > IP 池 > 添加**。

3 输入 IP 池详细信息。

选项	参数示例
名称和说明	输入 IP 池和可选说明。
IP 范围	IP 分配范围 192.168.200.100 - 192.168.200.115
网关	192.168.200.1
CIDR	采用 CIDR 表示法的网络地址 192.168.200.0/24
DNS 服务器	以逗号分隔的 DNS 服务器列表 192.168.66.10
DNS 后缀	corp.local

结果

IPv4 或 IPv6 地址池将在 IP 池页面上列出。

也可以使用 `GET https://<nsx-mgr>/api/v1/pools/ip-pools` API 调用查看 IP 池列表。

后续步骤

创建上行链路配置文件。请参见创建上行链路配置文件。

增强型数据路径

增强型数据路径是一种网络堆栈模式，配置后可提供卓越的网络性能。它主要用于 NFV 工作负载，这些工作负载需要此模式提供的性能优势。

只能在 ESXi 主机上以增强型数据路径模式配置 N-VDS 交换机。ENS 还支持流经 Edge 虚拟机的流量。

在增强型数据路径模式下，可以配置：

- 覆盖网络流量
- VLAN 流量

受支持的 VMkernel 网卡

对于支持多个 ENS 主机交换机的 NSX-T Data Center，每个主机支持的 VMkernel 网卡最大数为 32。

配置增强型数据路径的高级过程

作为网络管理员，创建支持增强型数据路径模式 N-VDS 的传输区域之前，必须使用支持的网卡和驱动程序准备网络。要提高网络性能，可以使负载平衡源绑定策略成为 NUMA 节点感知的绑定策略。

概要步骤如下所示：

1 使用支持增强型数据路径的网卡。

请参见《VMware 兼容性指南》，了解支持增强型数据路径的网卡。

在“VMware 兼容性指南”页面上的 **IO 设备**类别下，选择 **ESXi 6.7**，选择**网络**作为“IO 设备类型”并选择 **N-VDS 增强型数据路径**作为“功能”。

2 从 My VMware 页面中下载并安装最新的网卡驱动程序。

a 转到**驱动程序和工具 > 驱动程序 CD**。

b 下载网卡驱动程序：

适用于 `Intel 以太网控制器 82599、x520、x540、x550 和 x552 系列的 VMware ESXi 6.7 ixgben-ens 1.1.3` 网卡驱动程序

适用于 `Intel 以太网控制器 X710、XL710、XXV710 和 X722 系列的 VMware ESXi 6.7 i40en-ens 1.1.3` 网卡驱动程序

3 创建上行链路策略。

请参见创建上行链路配置文件。

4 使用增强型数据路径模式下的 N-VDS 创建传输区域。

请参见创建传输区域。

注 为覆盖网络流量配置的 ENS 传输区域：对于运行低于 11.0.0 的 VMware Tools 版本的 Microsoft Windows 虚拟机，如果 vNIC 类型为 `VMXNET3`，请确保将 MTU 设置为 1500。对于运行 vSphere 6.7 U1 和 VMware Tools 11.0.0 和更高版本的 Microsoft Windows 虚拟机，请确保将 MTU 设置为小于 8900 的值。对于运行其他支持的操作系统的虚拟机，请确保将虚拟机 MTU 设置为小于 8900 的值。

5 创建主机传输节点。为增强型数据路径 N-VDS 配置逻辑内核和 NUMA 节点。

请参见 创建独立主机或裸机服务器传输节点。

负载平衡源绑定策略模式感知 NUMA

满足以下条件时，为增强型数据路径 N-VDS 定义的负载平衡源绑定策略模式会感知 NUMA：

- 虚拟机上的**延迟敏感度**为**高**。
- 使用的网络适配器类型为 VMXNET3。

如果虚拟机或物理网卡的 NUMA 节点位置不可用，则负载平衡源绑定策略不考虑 NUMA 感知性以与虚拟机和网卡一致。

在以下情况下，绑定策略运行时不感知 NUMA：

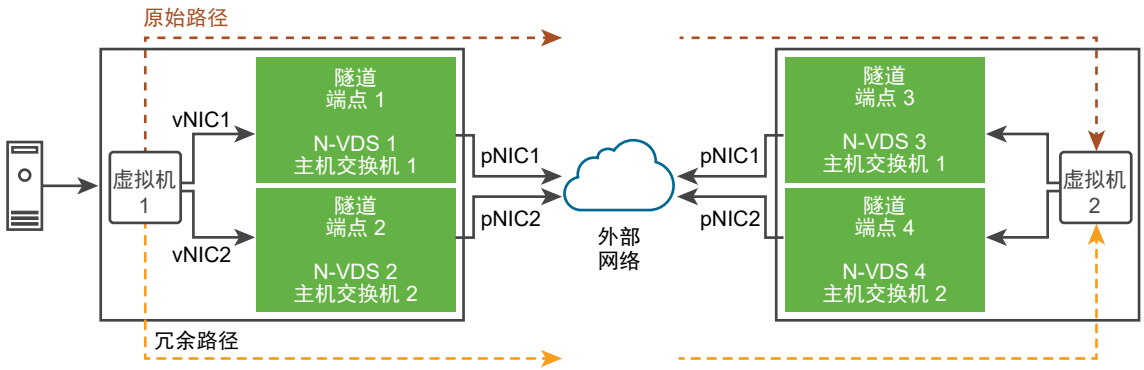
- LAG 上行链路配置有多个 NUMA 节点的物理链路。
- 虚拟机具有与多个 NUMA 节点的关联性。
- ESXi 主机无法定义虚拟机或物理链路的 NUMA 信息。

对 SCTP 应用程序的 ENS 支持

在 SCTP 环境中，NFV 工作负载使用多宿主和冗余功能来提高对在应用程序上运行的流量的弹性和可靠性。多宿主是支持从源虚拟机到目标虚拟机的冗余路径的功能。

根据要用作覆盖网络或 VLAN 网络的上行链路的可用物理网卡数，那些多个冗余网络路径可供虚拟机用于向目标虚拟机发送流量。固定到逻辑交换机的 pNIC 出现故障时，会使用冗余路径。因此，增强型数据路径 N-VDS 为通过 SCTP 协议路由的流量提供冗余网络路径。

图 8-1. 在 SCTP 应用程序上运行的 ENS 流量



高级任务如下：

1 将主机准备为 NSX-T Data Center 传输节点。

2 在增强型数据路径模式下，准备具有两个 N-VDS 交换机的 VLAN 或覆盖网络传输区域。

3 在 N-VDS 1 上，将第一个物理网卡固定到交换机。

4 在 N-VDS 2 上，将第二个物理网卡固定到交换机。

处于增强型数据路径模式的 N-VDS 确保 pNIC1 变得不可用时，通过冗余路径路由来自虚拟机 1 的流量：vNIC 1 → 隧道端点 2 → pNIC 2 → 虚拟机 2。请注意，虚拟机 1 和虚拟机 2 的 vNIC1 在一个子网上。同样，虚拟机 1 和虚拟机 2 的 vNIC2 在另一个子网上。

对配置文件进行配置

通过使用配置文件，您可以始终为多个主机或节点之间的网络适配器配置完全相同的功能。

配置文件是一些容器，其中包含您希望网络适配器具有的属性或功能。并非为每个网络适配器配置单独的属性或功能，您可以在配置文件中指定功能，以后可以在多个主机或节点之间应用这些功能。

创建上行链路配置文件

上行链路是从 NSX Edge 节点到机架顶部交换机或 NSX-T Data Center 逻辑交换机的链路。链路是从 NSX Edge 节点上的物理网络接口到交换机。

上行链路配置文件可定义上行链路的策略。上行链路配置文件所定义的设置可能包括绑定策略、活动链路及备用链路、传输 VLAN ID 以及 MTU 设置。

为基于虚拟机设备的 NSX Edge 节点和主机传输节点配置上行链路：

- 如果为上行链路配置文件配置了“故障切换”绑定策略，则只能在该绑定策略中配置单个活动上行链路。不支持备用上行链路，并且不得在“故障切换”绑定策略中配置备用上行链路。将 NSX Edge 作为虚拟设备或主机传输节点安装时，请使用默认上行链路配置文件。
- 如果为上行链路配置文件配置了“负载均衡源”绑定策略，则可以在同一个 N-VDS 上配置多个活动上行链路。每个上行链路都与一个具有不同名称和 IP 地址的物理网卡相关联。分配给上行链路端点的 IP 地址可使用 N-VDS 的 IP 分配进行配置。

您必须使用**负载均衡源**绑定策略进行流量负载均衡。

前提条件

- 请参阅 NSX Edge 安装中的 NSX Edge 网络要求。
- 上行链路配置文件中的每个上行链路必须对应于管理程序主机或 NSX Edge 节点上的已连接且可用的物理链路。

  例如，管理程序主机具有两个已连接的物理链路：vmnic0 和 vmnic1。假定将 vmnic0 用于管理和存储网络，而 vmnic1 未使用。这可能意味着，可以将 vmnic1 用作 NSX-T Data Center 上行链路，但不能将 vmnic0 用作上行链路。要进行链路绑定，您必须具有两个未使用的物理链路，例如，vmnic1 和 vmnic2。

  对于 NSX Edge，隧道端点和 VLAN 上行链路可以使用相同的物理链路。例如，可能会将 vmnic0/eth0/em0 用于管理网络，而将 vmnic1/eth1/em1 用于 fp-ethX 链路。

步骤

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

2 选择**系统 > 结构层 > 配置文件 > 上行链路配置文件 > 添加**。

3 填写上行链路配置文件详细信息。

选项	说明
名称和说明	输入上行链路配置文件名称。 添加可选的上行链路配置文件描述。
LAG	（可选）在 LAG 部分中，对于将链路聚合控制协议 (LACP) 用于传输网络的链路聚合组 (LAG)，单击**添加**。 注 对于 LACP，KVM 主机不支持多个 LAG。 您创建的活动和备用上行链路名称可以是表示物理链路的任意文本。以后创建传输节点时，将引用这些上行链路名称。通过使用传输节点 UI/API，您可以指定与每个命名的上行链路对应的物理链路。 可能的 LAG 哈希机制选项如下所示： ■ 源 MAC 地址 ■ 目标 MAC 地址 ■ 源和目标 MAC 地址 ■ 源和目标 IP 地址及 VLAN ■ 源和目标 MAC 地址、IP 地址和 TCP/UDP 端口
绑定	在“绑定”部分中，您可以输入默认绑定策略，也可以选择输入命名的绑定策略。单击**添加**以添加一个命名的绑定策略。绑定策略可定义 N-VDS 如何使用其上行链路实现冗余和流量负载均衡。您可以在以下模式下配置一个绑定策略： ■ **故障切换顺序**：指定活动上行链路以及可选的备用上行链路列表。如果活动上行链路出现故障，备用列表中的下一个上行链路将替换该活动上行链路。该选项不会执行实际负载均衡。 ■ **负载均衡源**：指定一个活动上行链路列表，并且传输节点上的每个接口固定到一个活动上行链路。此配置允许同时使用多个活动上行链路。 注 ■ 在 KVM 主机上：仅支持“故障切换顺序”绑定策略，而不支持“负载均衡源”和“负载均衡源 MAC”绑定策略。 ■ 在 NSX Edge 上：对于默认绑定策略，支持“负载均衡源”和“故障切换顺序”绑定策略。对于命名的绑定策略，仅支持“故障切换顺序”策略。 ■ 在 ESXi 主机上：支持“负载均衡源 MAC”、“负载均衡源”和“故障切换顺序”绑定策略。 （ESXi 主机和 NSX Edge）您可以为传输区域定义以下策略： ■ 每个基于 VLAN 的逻辑交换机或分段的命名绑定策略。 ■ 整个 N-VDS 的默认绑定策略。 命名的绑定策略：命名的绑定策略意味着，可以为每个基于 VLAN 的逻辑交换机或分段定义特定的绑定策略模式和上行链路名称。此策略类型使您可以根据流量控制策略灵活地选择特定的上行链路，例如，根据带宽要求进行选择。 ■ 如果定义了命名的绑定策略，则在 N-VDS 连接到基于 VLAN 的传输区域并最终为主机中基于 VLAN 的特定逻辑交换机或分段选择 N-VDS 时，它将使用该命名的绑定策略。 ■ 如果未定义任何指定绑定策略，N-VDS 将使用默认绑定策略。

4 输入传输 VLAN 值。上行链路配置文件中设置的传输 VLAN 仅标记覆盖网络流量，并且 VLAN ID 由 TEP 端点使用。

5 输入 MTU 值。

上行链路配置文件 MTU 默认值为 1600。

全局物理上行链路 MTU 为 NSX-T Data Center 域中的所有 N-VDS 实例配置 MTU 值。如果未指定全局物理上行链路 MTU 值，则从上行链路配置文件 MTU（如果已配置）中推断 MTU 值或使用默认值 1600。上行链路配置文件 MTU 值可能会覆盖特定主机上的全局物理上行链路 MTU 值。

全局逻辑接口 MTU 为所有逻辑路由器接口配置 MTU 值。如果未指定全局逻辑接口 MTU 值，则从 Tier-0 逻辑路由器中推断 MTU 值。逻辑路由器上行链路 MTU 值可能会覆盖特定端口上的全局逻辑接口 MTU 值。

结果

除了 UI 以外，还可以使用 API 调用 `GET /api/v1/host-switch-profiles` 查看上行链路配置文件。

后续步骤

创建传输区域。请参见创建传输区域。

配置 Network I/O Control 配置文件

使用 Network I/O Control (NIOC) 配置文件可向关键业务应用程序分配网络带宽以及解决多种流量争用通用资源的情况。

NIOC 配置文件引入了一种基于主机上物理适配器的容量为系统流量预留带宽的机制。Network I/O Control 版本 3 的功能改进了整个交换机上的网络资源预留和分配。

NSX-T Data Center 的 Network I/O Control 版本 3 支持对与虚拟机和基础架构服务（例如 vSphere Fault Tolerance）相关的系统流量进行资源管理。系统流量与 ESXi 主机紧密相关。

系统流量的带宽保证

Network I/O Control 版本 3 使用份额、预留和限制构成为虚拟机的网络适配器置备带宽。可以在 NSX-T Data Center Manager UI 中定义这些构成。虚拟机流量的带宽预留也用在准入控制中。当您打开虚拟机电源时，准入控制实用程序将验证是否有足够的带宽，然后才会在可提供资源容量的主机上放置虚拟机。

系统流量的带宽分配

您可以配置 Network I/O Control，以便为 vSphere Fault Tolerance、vSphere vMotion、虚拟机等生成的流量分配一定量的带宽。

- 管理流量：是用于主机管理的流量。
- Fault Tolerance (FT) 流量：是用于故障切换和恢复的流量。
- NFS 流量：是与网络文件系统中的文件传输相关的流量。
- vSAN 流量：是虚拟存储区域网络生成的流量。
- vMotion 流量：是用于计算资源迁移的流量。
- vSphere Replication 流量：是用于复制的流量。
- vSphere Data Protection 备份流量：是数据备份生成的流量。

- 虚拟机流量：是虚拟机生成的流量。
- iSCSI 流量：是用于 Internet 小型计算机系统接口的流量。

vCenter Server 将分布式交换机的分配传播到连接到该交换机的主机上的每个物理适配器。

系统流量的带宽分配参数

通过使用多个配置参数，Network I/O Control 服务可以将带宽分配给基本 vSphere 系统功能的流量。系统流量的分配参数。

系统流量的分配参数

- 份额：份额从 1 到 100，反映某个系统流量类型对于同一物理适配器上活动的其他系统流量类型的相对优先级。分配给系统流量类型的相对份额以及其他系统功能传输的数据量将确定该系统流量类型的可用带宽。
- 预留：单个物理适配器上必须保证的带宽最小值 (Mbps)。为所有系统流量类型预留的总带宽不得超过容量最低的物理网络适配器所能提供的带宽的 75%。未使用的预留带宽可用于其他类型的系统流量。但是，Network I/O Control 不会重新分配系统流量未用于虚拟机放置的容量。
- 限制：系统流量类型在单个物理适配器上可消耗的带宽最大值（Mbps 或 Gbps）。

注 可以预留的带宽不能超过物理网络适配器带宽的 75%。

例如，如果连接到 ESXi 主机的网络适配器为 10 GbE 时，您只能将 7.5 Gbps 的带宽分配给各种流量类型。您可能会使更多容量保持未预留状态。主机可以根据份额、限制和使用情况动态分配未预留的带宽。主机仅预留足以让系统功能运行的带宽。

为 N-VDS 上的系统流量配置 Network I/O Control 和带宽分配

要保证 NSX-T Data Center 主机上运行的系统流量获得最小带宽，请在 N-VDS 上启用并配置网络资源管理。

步骤

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

2 选择**系统 > 结构层 > 配置文件 > NIOC 配置文件 > 添加**。

3 输入 NIOC 配置文件详细信息。

选项	说明
名称和说明	输入 NIOC 配置文件名称。 您可以选择输入配置文件详细信息，例如启用的流量类型。
状态	切换以启用流量资源中列出的带宽分配。
主机基础架构流量资源	您可以接受列出的默认流量资源。 单击**添加**，然后输入您的流量资源以自定义 NIOC 配置文件。 （可选）选择现有流量类型，然后单击**删除**从 NIOC 配置文件中移除资源。

新 NIOC 配置文件将添加到 NIOC 配置文件列表中。

使用 API 为 N-VDS 上的系统流量配置 Network I/O Control 和带宽分配

可以使用 NSX-T Data Center API 为主机上运行的应用程序配置网络和带宽。

步骤

1 查询主机以同时显示系统定义的和用户定义的主机交换机配置文件。

2 `GET https://<nsx-mgr>/api/v1/host-switch-profiles?include_system_owned=true`。

示例响应显示应用于主机的 NIOC 配置文件。

```
{
  "description": "This profile is created for Network I/O Control (NIOC).",
  "extends": {
  "$ref": "BaseHostSwitchProfile"+
  },
  "id": "NiocProfile",
  "module_id": "NiocProfile",
  "polymorphic-type-descriptor": {
  "type-identifier": "NiocProfile"
  },
  "properties": {
  "_create_time": {
  "$ref": "EpochMsTimestamp"+,
  "can_sort": true,
  "description": "Timestamp of resource creation",
  "readonly": true
    },
  "_create_user": {
  "description": "ID of the user who created this resource",
  "readonly": true,
  "type": "string"
    },
  "_last_modified_time": {
  "$ref": "EpochMsTimestamp"+,
  "can_sort": true,
  "description": "Timestamp of last modification",
  "readonly": true
    },

  "_last_modified_user": {
  "description": "ID of the user who last modified this resource",
  "readonly": true,
  "type": "string"
    },

  "_links": {
  "description": "The server will populate this field when returning the resource. Ignored on PUT
and POST.",
  "items": {
  "$ref": "ResourceLink"+
    },

  "readonly": true,
```

```
  "title": "References related to this resource",
  "type": "array"
    },
  "_protection": {
  "description": "Protection status is one of the following:
     PROTECTED - the client who retrieved the entity is not allowed to modify it.
     NOT_PROTECTED - the client who retrieved the entity is allowed to modify it
     REQUIRE_OVERRIDE - the client who retrieved the entity is a super user and can modify it,
     but only when providing the request header X-Allow-Overwrite=true.
     UNKNOWN - the _protection field could not be determined for this entity.",
  "readonly": true,
  "title": "Indicates protection status of this resource",
  "type": "string"
    },

  "_revision": {
  "description": "The _revision property describes the current revision of the resource.
    To prevent clients from overwriting each other's changes, PUT operations must include the
             current _revision of the resource,
    which clients should obtain by issuing a GET operation.
                If the _revision provided in a PUT request is missing or stale, the operation
will be rejected.",
  "readonly": true,
  "title": "Generation of this resource config",
  "type": "int"
    },

  "_schema": {
  "readonly": true,
  "title": "Schema for this resource",
  "type": "string"
    },

  "_self": {
  "$ref": "SelfResourceLink"+,
  "readonly": true,
  "title": "Link to this resource"
    },

  "_system_owned": {
  "description": "Indicates system owned resource",
  "readonly": true,
  "type": "boolean"
    },

  "description": {
  "can_sort": true,
  "maxLength": 1024,
  "title": "Description of this resource",
  "type": "string"
    },

  "display_name": {
  "can_sort": true,
  "description": "Defaults to ID if not set",
```

```
  "maxLength": 255,
  "title": "Identifier to use when displaying entity in logs or GUI",
  "type": "string"
    },

  "enabled": {
  "default": true,
  "description": "The enabled property specifies the status of NIOC feature.

  When enabled is set to true, NIOC feature is turned on and the bandwidth allocations
     specified for the traffic resources are enforced.
  When enabled is set to false, NIOC feature is turned off and no bandwidth allocation is
guaranteed.

  By default, enabled will be set to true.",

  "nsx_feature": "Nioc",
  "required": false,
  "title": "Enabled status of NIOC feature",
  "type": "boolean"
    },

  "host_infra_traffic_res": {
  "description": "host_infra_traffic_res specifies bandwidth allocation for various traffic
resources.",
  "items": {
  "$ref": "ResourceAllocation"+
    },
  "nsx_feature": "Nioc",
  "required": false,
  "title": "Resource allocation associated with NiocProfile",
  "type": "array"
    },

  "id": {
  "can_sort": true,
  "readonly": true,
  "title": "Unique identifier of this resource",
  "type": "string"
    },

  "required_capabilities": {
  "help_summary":
                            "List of capabilities required on the fabric node if this profile is
used.
          The required capabilities is determined by whether specific features are enabled in the
profile.",
  "items": {
  "type": "string"
    },
  "readonly": true,
  "required": false,
  "type": "array"
    },
```

```
  "resource_type": {
  "$ref": "HostSwitchProfileType"+,
  "required": true
    },

  "tags": {
  "items": {
  "$ref": "Tag"+
      },

  "maxItems": 30,
  "title": "Opaque identifiers meaningful to the API user",
  "type": "array"
    }
  },
  "title": "Profile for Nioc",
  "type": "object"
  }
```

3 如果 NIOC 配置文件不存在，则创建一个 NIOC 配置文件。

```
POST https://<nsx-mgr>/api/v1/host-switch-profiles
```

```
{
  "description": "Specify limit, shares and reservation for all kinds of traffic.
   Values for limit and reservation are expressed in percentage. And for shares,
   the value is expressed as a number between 1-100.\nThe overall reservation among all traffic
types should not exceed 75%.
   Otherwise, the API request will be rejected.",

  "id": "ResourceAllocation",
  "module_id": "NiocProfile",
  "nsx_feature": "Nioc",
  "properties": {
    "limit": {
      "default": -1.0,
      "description": "The limit property specifies the maximum bandwidth allocation for a given
      traffic type and is expressed in percentage. The default value for this
      field is set to -1 which means the traffic is unbounded for the traffic
      type. All other negative values for this property is not supported\nand will be rejected by
the API.",
      "maximum": 100,
      "minimum": -1,
      "required": true,
      "title": "Maximum bandwidth percentage",
      "type": "number"
    },

    "reservation": {
      "default": 0.0,
      "maximum": 75,
      "minimum": 0,
      "required": true,
      "title": "Minimum guaranteed bandwidth percentage",
      "type": "number"
```

```
    },

    "shares": {
      "default": 50,
      "maximum": 100,
      "minimum": 1,
      "required": true,
      "title": "Shares",
      "type": "int"
    },

    "traffic_type": {
      "$ref": "HostInfraTrafficType"+,
      "required": true,
      "title": "Resource allocation traffic type"
    }

  },

  "title": "Resource allocation information for a host infrastructure traffic type",
  "type": "object"
```

4 使用新创建的 NIOC 配置文件的 NIOC 配置文件 ID，更新传输节点配置。

```
PUT https://<nsx-mgr>/api/v1/transport-nodes/<TN-id>
```

```
{
    "resource_type": "TransportNode",
    "description": "Updated NSX configured Test Transport Node",
    "id": "77816de2-39c3-436c-b891-54d31f580961",
    "display_name": "NSX Configured TN",
    "host_switch_spec": {
      "resource_type": "StandardHostSwitchSpec",
      "host_switches": [
        {
        "host_switch_profile_ids": [
          {
            "value": "e331116d-f59e-4004-8cfd-c577aefe563a",
            "key": "UplinkHostSwitchProfile"
          },
        {
       "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
       "key": "LldpHostSwitchProfile"
        }
       {
        "value": "b0185099-8003-4678-b86f-edd47ca2c9ad",
        "key": "NiocProfile"
       }
        ],
       "host_switch_name": "nsxvswitch",
       "pnics": [
      {
       "device_name": "vmnic1",
       "uplink_name": "uplink1"
      }
```

```
      ],
      "ip_assignment_spec": {
      "resource_type": "StaticIpPoolSpec",
      "ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
      }
       }
      ]
    },
     "transport_zone_endpoints": [
      {
      "transport_zone_id": "e14c6b8a-9edd-489f-b624-f9ef12afbd8f",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ]
      }
    ],

     "host_switches": [
      {
        "host_switch_profile_ids": [
          {
          "value": "e331116d-f59e-4004-8cfd-c577aefe563a",
          "key": "UplinkHostSwitchProfile"
         },
          {
          "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
          "key": "LldpHostSwitchProfile"
          }
        ],

        "host_switch_name": "nsxvswitch",
        "pnics": [
        {
          "device_name": "vmnic1",
          "uplink_name": "uplink1"
          }
        ],
        "static_ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
      }
    ],
    "node_id": "41a4eebd-d6b9-11e6-b722-875041b9955d",
    "_revision": 0
  }
```

5 确认在 com.vmware.common.respools.cfg 文件中已更新 NIOC 配置文件参数。

[root@ host:] net-dvs -l

```
           switch 1d 73 f5 58 99 7a 46 6a-9c cc d0 93 17 bb 2a 48 (vswitch)
   max ports: 2560
   global properties:
```

```
   com.vmware.common.opaqueDvs = true ,     propType = CONFIG
   com.vmware.nsx.kcp.enable = true ,     propType = CONFIG
   com.vmware.common.alias = nsxvswitch ,     propType = CONFIG
   com.vmware.common.uplinkPorts: uplink1   propType = CONFIG
   com.vmware.common.portset.mtu = 1600, propType = CONFIG
   com.vmware.etherswitch.cdp = LLDP, listen  propType = CONFIG
   com.vmware.common.respools.version = version3,   propType = CONFIG
   com.vmware.common.respools.cfg:
   netsched.pools.persist.ft:0:50:-1:255
   netsched.pools.persist.hbr:0:50:-1:255
   netsched.pools.persist.vmotion:0:50:-1:255
   netsched.pools.persist.vm:0:100:-1:255
   netsched.pools.persist.iscsi:0:50:-1:255
   netsched.pools.persist.nfs:0:50:-1:255
   netsched.pools.persist.mgmt:0:50:-1:255
   netsched.pools.persist.vdp:0:50:-1:255
   netsched.pools.persist.vsan:0:50:-1:255
   propType = CONFIG
```

6 确认主机内核中的 NIOC 配置文件。

[root@ host:] /get /net/portsets/DvsPortset-1/ports/50335755/niocVnicInfo

```
Vnic NIOC Info
                    {
      Uplink reserved on:vmnic4
      Reservation in Mbps:200
      Shares:50
      Limit in Mbps:4294967295
      World ID:1001400726
      vNIC Index:0
      Respool Tag:0
      NIOC Version:3
      Active Uplink Bit Map:15
      Parent Respool ID:netsched.pools.persist.vm
     }
```

7 确认 NIOC 配置文件信息。

[root@ host:] /get /net/portsets/DvsPortset-1/uplinks/vmnic4/niocInfo

```
Uplink NIOC Info
            {
    Uplink device:vmnic4
    Link Capacity in Mbps:750
    vm respool reservation:275
    link status:1
    NetSched Ready:1
    Infrastructure reservation:0
    Total VM reservation:200
```

```
    Total vnics on this uplink:1
    NIOC Version:3
    Uplink index in BitMap:0
   }
```

结果

NIOC 配置文件将配置有 NSX-T Data Center 主机上运行的应用程序的预定义带宽分配。

添加 NSX Edge 群集配置文件

NSX Edge 群集配置文件定义 NSX Edge 传输节点的策略。

前提条件

确认 NSX Edge 群集可用。

步骤

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

2 选择**系统 > 结构层 > 配置文件 > Edge 集群配置文件 > 添加**。

3 输入 NSX Edge 群集配置文件详细信息。

选项	说明
名称和说明	输入 NSX Edge 群集配置文件名称。 可以选择输入配置文件详细信息，如双向转发检测 (BFD) 设置。
BFD 探测间隔	接受默认设置。 BFD 是用于识别转发路径故障的检测协议。可以设置 BFD 检测转发路径故障的间隔时间。
BFD 允许的跃点	接受默认设置。 可以设置为配置文件允许的多跃点 BFD 会话数。
BFD 声明失效倍数	接受默认设置。 可以设置会话标记为关闭之前未收到 BFD 数据包的次数。
备用重定位阈值	接受默认设置。

添加 NSX Edge 网桥配置文件

NSX Edge 网桥配置文件定义 ESXi 网桥群集的策略。

网桥群集是 ESXi 主机传输节点的集合。

前提条件

- 确认 NSX Edge 群集可用。
- 确认 ESXi 网桥群集可用。

步骤

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

2 选择**系统 > 结构层 > 配置文件 > Edge 网桥配置文件 > 添加**。

3 输入 NSX Edge 群集配置文件详细信息。

选项	说明
名称和说明	输入 NSX Edge 网桥群集配置文件名称。 可以选择输入配置文件详细信息，如主节点和备份节点详细信息。
Edge 群集	选择要使用的 NSX Edge 群集。
主节点	从群集中指定首选 NSX Edge 节点。
备份节点	指定主节点出现故障时的备份 NSX Edge 节点。
故障切换模式	选择**先行性**或**非先行性**模式。 默认 HA 模式为先行性，首选 NSX Edge 节点恢复联机时它可减慢流量。非先行性模式不会导致任何流量减慢。

添加传输节点配置文件

传输节点配置文件捕获创建传输节点所需的配置。传输节点配置文件可应用于现有 vCenter Server 集群为成员主机创建传输节点。传输节点配置文件定义传输区域、成员主机、N-VDS 交换机配置（包括上行链路配置文件、IP 分配、物理网卡到上行链路虚拟接口的映射等）。

在传输节点配置文件应用于 vCenter Server 集群时，开始创建传输节点。NSX Manager 准备集群中的主机，并在所有主机上安装 NSX-T Data Center 组件。主机的传输节点基于在传输节点配置文件中指定的配置进行创建。

要删除传输节点配置文件，必须先从关联的集群中分离配置文件。现有的传输节点不受影响。添加到集群的新主机将不再自动转换为传输节点。

创建传输节点配置文件的注意事项如下：

- 您最多可以为每种配置添加四个 N-VDS 交换机：为 VLAN 传输区域创建的增强型 N-VDS、为覆盖网络传输区域创建的标准 N-VDS、为覆盖网络传输区域创建的增强型 N-VDS。
- 为 VLAN 传输区域创建的标准 N-VDS 交换机没有数量限制。
- 在同一主机上运行多个标准覆盖网络 N-VDS 交换机和 Edge 虚拟机的单个主机集群拓扑中，NSX-T Data Center 提供了流量隔离以便通过第一个 N-VDS 的流量与通过第二个 N-VDS 的流量隔离，以此类推。每个 N-VDS 上的物理网卡必须映射到主机上的 Edge 虚拟机，以允许与外界的南北向流量连接。从第一个传输区域上的虚拟机移出的数据包必须通过外部路由器或外部虚拟机路由到第二个传输区域上的虚拟机。
- 每个 N-VDS 交换机的名称都必须唯一。NSX-T Data Center 不允许使用重复的交换机名称。
- 每个传输区域 ID 都必须唯一。NSX-T Data Center 不允许使用重复的 ID。
- 传输节点配置文件中最多可以添加 1000 个传输区域。
- 要添加传输区域，必须由传输节点配置文件中存在的任何 N-VDS 实现它。

前提条件

- 确认主机是 vCenter Server 集群的一部分。

  vCenter Server 必须至少具有一个集群。
- 确认配置了一个传输区域。请参见创建传输区域。
- 确认具有一个可用集群。请参见从 UI 部署 NSX Manager 节点以形成群集。
- 确认配置了一个 IP 池，或者 DHCP 在网络部署中必须可用。请参见创建 IP 池以分配隧道端点 IP 地址。
- 确认配置了一个计算管理器。请参见添加计算管理器。

步骤

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

2 选择**系统 > 结构层 > 配置文件 > 传输节点配置文件 > 添加**。

3 输入一个名称以标识传输节点配置文件。

  可以选择添加有关传输节点配置文件的说明。

4 选择可用的传输区域，然后单击 **>** 按钮将传输区域包括在传输节点配置文件中。

  注 可以添加多个传输区域。

5 单击 **N-VDS** 选项卡，然后输入交换机详细信息。

选项	说明
N-VDS 名称	如果传输节点连接到传输区域，请确保为 N-VDS 输入的名称与在传输区域中指定的 N-VDS 名称相同。可以创建传输节点而不将其连接到传输区域。
关联的传输区域	显示由关联的主机交换机实现的传输区域。如果传输区域未由传输节点配置文件中的任何 N-VDS 实现，则无法添加。
NIOC 配置文件	从下拉菜单中选择 NIOC 配置文件。 将强制实施在流量资源的配置文件中指定的带宽分配。
上行链路配置文件	从下拉菜单中选择一个现有的上行链路配置文件，或者创建一个自定义上行链路配置文件。 注 集群中的主机必须具有相同的上行链路配置文件。 也可以使用默认上行链路配置文件。
LLDP 配置文件	默认情况下，NSX-T 仅接收来自 LLDP 邻居的 LLDP 数据包。 但是，可以将 NSX-T 设置为与 LLDP 邻居之间收发 LLDP 数据包。
IP 分配	选择**使用 DHCP**、**使用 IP 池**或**使用静态 IP 列表**以将 IP 地址分配给传输节点的虚拟隧道端点 (VTEP)。 如果选择**使用静态 IP 列表**，您必须指定以逗号分隔的 IP 地址、网关和子网掩码列表。传输节点的所有 VTEP 都必须在同一子网中，否则将不建立双向流 (BFD) 会话。
IP 池	如果您选择**使用 IP 池**进行 IP 分配，请指定 IP 池名称。

选项	说明
物理网卡	将物理网卡添加到传输节点。您可以使用默认上行链路，或者从下拉菜单中分配一个现有的上行链路。 单击**添加 PNIC** 为传输节点配置其他物理网卡。 **注** 在此字段中添加的物理网卡的迁移取决于配置**仅迁移 PNIC**、**用于安装的网络映射**和**用于卸载的网络映射**的方式。 ■ 要迁移没有关联 VMkernel 映射的已用物理网卡（例如，通过标准 vSwitch 或 vSphere Distributed Switch），请确保已启用**仅迁移 PNIC**。否则，传输节点状态保持为**部分成功**，并且无法建立 Fabric 节点 LCP 连接。 ■ 要迁移具有关联 VMkernel 网络映射的已用物理网卡，请禁用**仅迁移 PNIC** 并配置 VMkernel 网络映射。 ■ 要迁移可用物理网卡，请启用**仅迁移 PNIC**。
仅迁移 PNIC	在设置此字段之前，请考虑以下几点： ■ 了解定义的物理网卡是已用网卡还是可用网卡。 ■ 确定主机的 VMkernel 接口是否需要与物理网卡一起迁移。 设置以下字段： ■ 如果仅希望将物理网卡从 VSS 或 DVS 交换机迁移到 N-VDS 交换机，则启用**仅迁移 PNIC**。 ■ 如果要迁移已用的物理网卡及其关联的 VMkernel 接口映射，则禁用**仅迁移 PNIC**。指定 VMkernel 接口迁移映射时，可用物理网卡将连接到 N-VDS 交换机。 在具有多个主机交换机的主机上： ■ 如果所有主机交换机都仅迁移 PNIC，则可以在单个操作中迁移 PNIC。 ■ 如果一些主机交换机要迁移 VMkernel 接口，而其余的主机交换机要仅迁移 PNIC： 1 在第一个操作中，仅迁移 PNIC。 2 在第二个操作中，迁移 VMkernel 接口。请确保已禁用**仅迁移 PNIC**。 不支持同时在多个主机中执行仅迁移 PNIC 和 VMkernel 接口迁移。 **注** 要迁移管理网络网卡，请配置其关联的 VMkernel 网络映射并使**仅迁移 PNIC** 保持禁用状态。如果仅迁移管理网卡，则主机将失去连接。 有关详细信息，请参见 VMkernel 迁移到 N-VDS 交换机。

选项	说明
用于安装的网络映射	要在安装期间将 VMkernel 迁移到 N-VDS 交换机，请将 VMkernel 映射到现有逻辑交换机。NSX Manager 将 VMkernel 迁移到 N-VDS 上的映射逻辑交换机。 小心 确保管理网卡和管理 VMkernel 接口迁移到的逻辑交换机连接到迁移前管理网卡所连接的同一 VLAN。如果 vmnic<*n*> 和 VMkernel<*n*> 迁移到不同的 VLAN，则将失去与主机的连接。 小心 对于固定的物理网卡，请确保物理网卡到 VMkernel 接口的主机交换机映射与在传输节点配置文件中指定的配置匹配。在验证过程中，NSX-T Data Center 将确认映射，以及验证通过后 VMkernel 接口是否成功迁移到 N-VDS 交换机。还必须为卸载配置网络映射，因为将 VMkernel 接口迁移到 N-VDS 交换机后 NSX-T Data Center 不会存储主机交换机的映射配置。如果未配置映射，则迁移回 VSS 或 VDS 交换机后，可能会失去与服务（如 vSAN）的连接。 有关详细信息，请参见 VMkernel 迁移到 N-VDS 交换机。
用于卸载的网络映射	要在卸载期间恢复 VMkernel 的迁移，请将 VMkernel 映射到 VSS 或 DVS 上的端口组，以便 NSX Manager 知道必须将 VMkernel 迁移回 VSS 或 DVS 上的哪个端口组。对于 DVS 交换机，请确保端口组的类型为临时。 小心 对于固定的物理网卡，请确保物理网卡到 VMkernel 接口的传输节点配置文件映射与在主机交换机中指定的配置匹配。必须为卸载配置网络映射，因为将 VMkernel 接口迁移到 N-VDS 交换机后 NSX-T Data Center 不会存储主机交换机的映射配置。如果未配置映射，则迁移回 VSS 或 VDS 交换机后，可能会失去与服务（如 vSAN）的连接。 有关详细信息，请参见 VMkernel 迁移到 N-VDS 交换机。

6 要添加另一个 N-VDS 交换机，请单击 **+ 添加 N-VDS**。

7 单击**保存**以完成配置。

后续步骤

将传输节点配置文件应用于现有的 vSphere 集群。请参见配置受管主机传输节点。

VMkernel 迁移到 N-VDS 交换机

要在群集级别将 VMkernel 接口从 VSS 或 DVS 交换机迁移到 N-VDS 交换机，请使用迁移所需的网络映射详细信息（将 VMkernel 接口映射到逻辑交换机）配置传输节点配置文件。同样，要迁移主机节点上的 VMkernel 接口，请配置传输节点配置。要将 VMkernel 接口迁移回 VSS 或 DVS 交换机，请在要在卸载过程中实现的传输节点配置文件中配置卸载网络映射（将逻辑端口映射到 VMkernel 接口）。

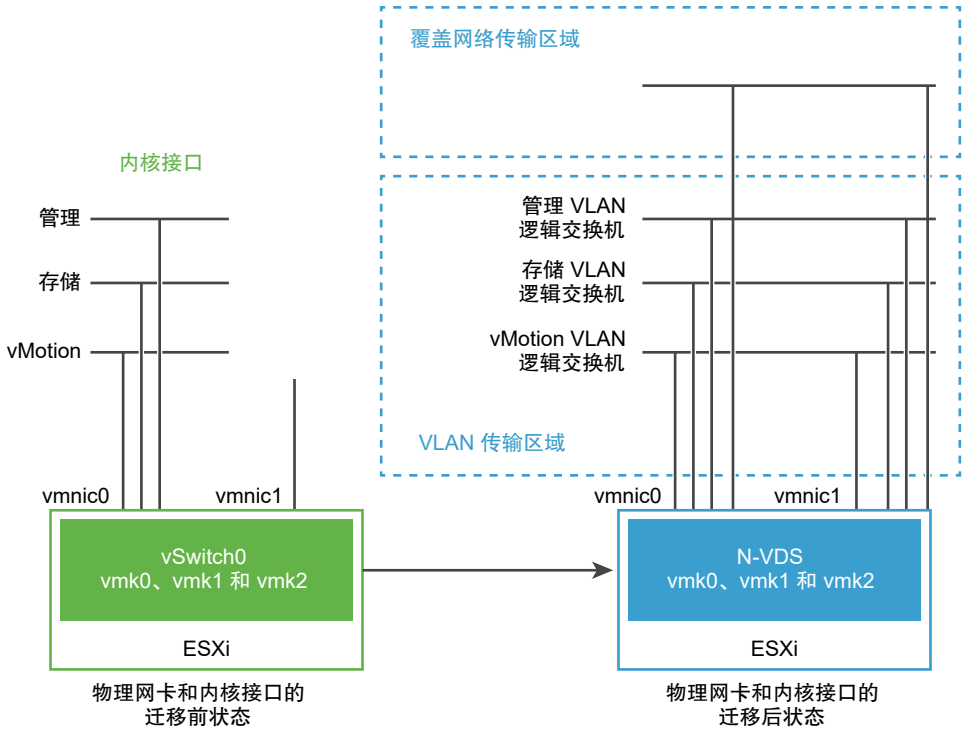
在迁移期间，当前正在使用的物理网卡将迁移到 N-VDS 交换机，而可用或空闲物理网卡则在迁移后连接到 N-VDS 交换机。

注 传输节点配置文件应用到群集的所有成员主机。但是，如果您希望在特定主机上限制 VMkernel 接口的迁移，您可以直接配置主机。迁移后，N-VDS 将为连接到 N-VDS 交换机的那些接口处理 VLAN 和覆盖网络上的流量。

重要事项 各个主机已完成的配置将标记已替代标记。对传输节点配置文件的任何进一步更新均不会应用于这些已替代的主机。卸载 NSX-T Data Center 之前，这些主机将保持已替代状态。

在下图中，如果主机只有两个物理网卡，您可能希望将这两个网卡及其关联的 VMkernel 接口分配给 N-VDS 以实现冗余，并且这些接口不会失去与主机的连接。

图 8-2. 将网络接口迁移到 N-VDS 之前和之后



迁移前， ESXi 主机具有来自两个物理端口 vmnic0 和 vmnic1 的两个上行链路。此处，vmnic0 配置为处于活动状态且连接到 VSS，而 vmnic1 未使用。此外，还有三个 VMkernel 接口：vmk0、vmk1 和 vmk2。

可以使用 NSX-T Data Center Manager UI 或 NSX-T Data Center API 迁移 VMkernel 接口。请参见《NSX-T Data Center API 指南》。

迁移后，vmnic0、vmnic1 及其 VMkernel 接口将迁移到 N-VDS 交换机。vmnic0 和 vmnic1 通过 VLAN 和覆盖网络传输区域进行连接。

VMkernel 迁移的注意事项

- 物理网卡和 VMkernel 迁移：将固定物理网卡和关联的 VMkernel 接口迁移到 N-VDS 交换机之前，请记下主机交换机上的网络映射（物理网卡到端口组映射）。
- 仅物理网卡迁移：如果您打算仅迁移物理网卡，请确保不要迁移已连接到管理 VMkernel 接口的管理物理网卡。这会导致失去与主机的连接。有关更多详细信息，请参见添加传输节点配置文件中的**仅迁移 PNIC** 字段。
- 恢复迁移：计划将 VMkernel 接口迁移回固定物理网卡的 VSS 或 DVS 主机交换机之前，请确保记下主机交换机上的网络映射（物理网卡到端口组映射）。这是使用**卸载的网络映射**字段中的主机交换机映射配置传输节点配置文件的必备条件。如果没有此映射，NSX-T Data Center 不知道必须将 VMkernel 接口迁移回哪些端口组。这种情况可能会导致失去与 vSAN 网络的连接。

- 在迁移前注册 vCenter Server：如果计划迁移连接到 DVS 交换机的 VMkernel 或物理网卡，请确保向 NSX Manager 注册 vCenter Server。
- 匹配 VLAN ID：迁移后，管理网卡和管理 VMkernel 接口必须位于管理网卡迁移前所连接的同一个 VLAN 上。如果 vmnic0 和 vmk0 已连接到管理网络并迁移到不同的 VLAN，那么将失去与主机的连接。
- 迁移到 VSS 交换机：无法将两个 VMkernel 接口迁移回 VSS 交换机的同一个端口组。
- vMotion：在 VMkernel 和/或 PNIC 迁移之前，执行 vMotion 以将虚拟机工作负载移动到另一个主机。如果迁移失败，则工作负载虚拟机不会受到影响。
- vSAN：如果正在主机上运行 vSAN 流量，请通过 vCenter Server 将主机置于维护模式，并在 VMkernel 和/或 PNIC 迁移之前使用 vMotion 功能将虚拟机从主机中移出。
- 迁移：如果 VMkernel 已连接到目标交换机，则仍然可以选择该 VMkernel 以迁移到同一交换机。该属性允许执行幂等 VMK 和/或 PNIC 迁移操作。如果您希望仅将 PNIC 迁移到目标交换机，这是非常有用的。由于迁移始终需要至少一个 VMkernel 和一个 PNIC，因此，在仅将 PNIC 迁移到目标交换机时，您可以选择已迁移到目标交换机的 VMkernel。如果不需要迁移任何 VMkernel，请通过 vCenter Server 在源交换机或目标交换机中创建一个临时 VMkernel。然后，将其与 PNIC 一起迁移，并在迁移完成后通过 vCenter Server 删除临时 VMkernel。
- MAC 共享：如果 VMkernel 接口和 PNIC 具有相同的 MAC 并且它们位于同一交换机中，则必须将它们一起迁移到同一目标交换机（如果在迁移后使用它们）。请始终将 vmk0 和 vmnic0 保留在同一交换机中。

  可以运行以下命令，以检查主机中的所有 VMK 和 PNIC 使用的 MAC：

  ```
  esxcfg-vmknic -l
  ```

  ```
  esxcfg-nics -l
  ```
- 在迁移后创建的 VIF 逻辑端口：在将 VMkernel 从 VSS 或 DVS 交换机迁移到 N-VDS 交换机后，将在 NSX Manager 上创建 VIF 类型的逻辑交换机端口。您不能在这些 VIF 逻辑交换机端口上创建分布式防火墙规则。

将 VMkernel 接口迁移到 N-VDS 交换机

将 VMkernel 接口迁移到 N-VDS 交换机的汇总工作流：

1 如果需要，创建逻辑交换机。

2 在要将 VMkernel 接口和物理网卡迁移到 N-VDS 交换机的主机上关闭虚拟机的电源。

3 使用创建传输节点时用于迁移 VMkernel 接口的网络映射配置传输节点配置文件。网络映射意味着将 VMkernel 接口映射到逻辑交换机。

  有关更多详细信息，请参见添加传输节点配置文件。

4 确认 vCenter Server 中的网络适配器映射反映了 VMkernel 交换机与 N-VDS 交换机的新关联。如果是固定物理网卡，请确认 NSX-T Data Center 中的映射反映了固定到 vCenter Server 中的物理网卡的任何 VMkernel。

5 在 NSX Manager 中，转到**高级网络和安全性 > 网络 > 切换**。在**交换机**页面上，确认 VMkernel 接口已通过新创建的逻辑端口连接到逻辑交换机。

6 转到**系统 > 节点 > 主机传输节点**。对于每个传输节点，确认**节点状态**列上的状态为“成功”，以确认已成功验证传输节点配置。

7 在**主机传输节点**页面上，确认**配置状态**上的状态为“成功”，以确认已成功使用指定的配置实现主机。

在使用 NSX-T UI 或传输节点 API 将 VMkernel 接口和 PNIC 从 VDS 迁移到 N-VDS 交换机后，vCenter Server 将为 VDS 显示警告。如果主机需要连接到 VDS，请从 VDS 中移除主机。vCenter Server 将不再为 VDS 显示任何警告。

有关在迁移期间可能会遇到的错误的详细信息，请参见 VMkernel 迁移错误

将 VMkernel 接口迁移回 VSS 或 DVS 交换机

卸载 NSX-T Data Center 时将 VMkernel 接口从 N-VDS 交换机迁移回 VSS 或 DVS 交换机的汇总工作流：

1 在 ESXi 主机上，迁移后关闭连接到托管 VMkernel 接口的逻辑端口的虚拟机的电源。

2 使用在卸载过程中用于迁移 VMkernel 接口的网络映射配置传输节点配置文件。卸载期间的网络映射将 VMkernel 接口映射到 ESXi 主机上的 VSS 或 DVS 交换机上的端口组。

> **注** 将 VMkernel 迁移回 DVS 交换机上的端口组时，请确保将端口组类型设置为临时。

有关更多详细信息，请参见添加传输节点配置文件。

3 确认 vCenter Server 中的网络适配器映射反映了 VMkernel 交换机与 VSS 或 DVS 交换机的端口组的新关联。

4 在 NSX Manager 中，转到**高级网络和安全性 > 网络 > 切换**。在**交换机**页面上，确认已删除包含 VMkernel 接口的逻辑交换机。

有关在迁移期间可能会遇到的错误的详细信息，请参见 VMkernel 迁移错误

更新主机交换机映射

重要事项

- 有状态主机：支持添加和更新操作。要更新现有映射，您可以向网络映射配置中添加新的 VMkernel 接口条目。如果更新已迁移到 N-VDS 交换机的 VMkernel 接口的网络映射配置，则在主机上不会实现更新的网络映射。
- 无状态主机：支持添加、更新和移除操作。在主机重新引导后，将实现对网络映射配置所做的任何更改。

  要将 VMkernel 接口更新到新的逻辑交换机，您可以编辑传输节点配置文件以在群集级别应用网络映射。如果只希望将更新应用于单个主机，请使用主机级 API 配置传输节点。

注 更新单个主机的传输节点配置后，通过传输节点配置文件应用的任何新更新均不会应用到该主机。主机状态将变为已替代。

1 要更新群集中的所有主机，请编辑**安装期间的网络映射**字段以更新 VMkernel 到逻辑交换机的映射。

  有关更多详细信息，请参见添加传输节点配置文件。

2 保存更改。对传输节点配置文件所做的更改将自动应用于群集的所有成员主机，但标记有已替代状态的主机除外。

3 同样，要更新单个主机，请编辑传输节点配置中的 VMkernel 映射。

注 如果您使用新的 VMkernel 映射更新**安装期间的网络映射**字段，那么必须将同一 VMkernel 接口添加到**卸载期间的网络映射**字段。

有关在迁移期间可能会遇到的错误的详细信息，请参见 VMkernel 迁移错误

迁移无状态群集上的 VMkernel 接口

1 使用传输节点 API 准备将主机配置为引用主机。

2 从引用主机提取主机配置文件。

3 在 vCenter Server 中，将主机配置文件应用于无状态群集。

4 在 NSX-T Data Center 中，将传输节点配置文件应用于无状态群集。

5 重新引导群集的每个主机。

群集主机可能需要几分钟时间才能实现更新的状态。

迁移故障情形

- 如果迁移由于某种原因失败，主机将尝试迁移物理网卡和 VMkernel 接口三次。
- 如果迁移仍失败，主机将通过保留与管理物理网卡 vmnic0 的 VMkernel 连接执行到之前配置的回滚。
- 如果回滚也失败，导致配置到管理物理网卡的 VMkernel 丢失，您必须重置主机。

不支持的迁移场景

不支持以下场景：

- 同时迁移来自两个不同 VSS 或 DVS 交换机的 VMkernel 接口。
- 在有状态主机上，更新网络映射以将 VMkernel 接口映射到另一个逻辑交换机。例如，在迁移之前，先将 VMkernel 映射到逻辑交换机 1，将 VMkernel 接口映射到逻辑交换机 2。

VMkernel 迁移错误

将 VMkernel 接口和物理网卡从 VSS 或 DVS 交换机迁移到 N-VDS 交换机，或者将接口迁移回 VSS 或 DVS 主机交换机时，可能会遇到错误。

表 8-1. VMkernel 迁移错误

错误代码	问题	原因	解决方案
8224	找不到传输节点配置指定的主机交换机。	找不到主机交换机 ID。	■ 请确保使用主机交换机名称创建传输区域，然后创建传输节点。 ■ 请确保在传输节点配置中使用有效的主机交换机。
8225	VMkernel 迁移正在进行中。	迁移正在进行中。	等待迁移完成后再执行其他操作。
8226	VMkernel 迁移仅在 ESXi 主机上受支持。	迁移仅对 ESXi 主机有效。	请确保在启动迁移之前该主机为 ESXi 主机。
8227	主机交换机名称未附加 VMkernel 接口。	在具有多个主机交换机的主机上，NSX-T Data Center 无法识别每个 VMkernel 接口与其主机交换机的关联。	如果主机具有多个 N-VDS 主机交换机，请确保主机所连接的 N-VDS 的主机交换机名称附加 VMkernel 接口。 例如，卸载具有 N-VDS 主机交换机名称 nsxvswitch1 和 VMkernel1 以及另一个 N-VDS 主机交换机名称 nsxvswitch2 和 VMkernel2 的主机的网络映射必须进行如下定义：`device_name: VMkernel1@nsxvswitch1, destination_network: DPortGroup`。
8228	在主机上未找到在 `device_name` 字段中使用的主机交换机。	主机交换机名称不正确。	输入正确的主机交换机名称。
8229	传输节点未指定逻辑交换机的传输区域。	未添加传输区域。	将传输区域添加到传输节点配置。
8230	主机交换机上没有物理网卡。	主机交换机上必须至少有一个物理网卡。	至少为上行链路配置文件指定一个物理网卡，并为逻辑交换机指定 VMkernel 网络映射配置。
8231	主机交换机名称不匹配。	如果在 `vmk1@host_switch` 中使用的主机交换机名称与接口的目标逻辑交换机使用的主机交换机名称不匹配。	请确保在网络映射配置中指定的主机交换机名称与接口的逻辑交换机使用的名称匹配。
8232	在主机上未实现逻辑交换机。	在主机上实现逻辑交换机不成功。	将主机与 NSX Manager 同步。

表 8-1. VMkernel 迁移错误 （续）

错误代码	问题	原因	解决方案
8233	在网络接口映射中出现意外的逻辑交换机。	用于安装和卸载的网络接口映射同时列出了逻辑交换机和端口组。	用于安装的网络映射必须仅包含逻辑交换机作为目标。同样，用于卸载的网络映射必须仅包含端口组作为目标。
8294	逻辑交换机未存在于网络接口映射中。	未指定逻辑交换机。	请确保在网络接口映射配置中指定了逻辑交换机。
8296	主机交换机不匹配。	用于卸载的网络接口映射配置有不正确的主机交换机名称。	请确保映射配置中使用的主机交换机名称与在 VMkernel 接口所驻留的主机交换机上输入的名称匹配。
8297	重复的 VMkernel。	为迁移指定了重复的 VMkernel。	请确保在安装或卸载映射配置中未指定重复的 VMkernel 接口。
8298	VMkernel 接口和目标数量不匹配。	配置不正确。	请确保每个 VMkernel 接口都具有在配置中指定的对应目标。
8299	无法删除传输节点，因为 VMkernel 接口正在使用 N-VDS 上的端口。	VMkernel 接口正在使用 N-VDS 交换机中的端口。	将所有 VMkernel 接口从 N-VDS 交换机迁移回 VSS/DVS 交换机。然后尝试删除传输节点。
9412	VMkernel 无法从一个 N-VDS 迁移到另一个 N-VDS。	不支持此操作。	将 VMkernel 接口迁移回 VSS 或 DVS 交换机。然后，可以将 VMkernel 接口迁移到另一个 N-VDS 交换机。
9413	无法将 VMkernel 接口迁移到不同的逻辑交换机。	在有状态主机上，无法将连接到逻辑交换机的 VMkernel 迁移到另一个逻辑交换机。	将 VMkernel 从逻辑交换机迁移回 VSS/DVS 交换机。然后，将 VMkernel 迁移到 N-VDS 上的另一个逻辑交换机。
9414	重复的 VMkernel 接口。	在安装和卸载映射配置中映射了重复的 VMkernel 接口。	请确保每个 VMkernel 接口在安装和卸载映射中都是唯一的。
9415	在主机上已打开虚拟机电源。	对于已打开电源的虚拟机，迁移无法进行。	在启动 VMkernel 接口的迁移之前，在主机上关闭虚拟机电源。
9416	在主机上找不到 VMkernel。	在网络映射配置中未指定存在于主机上的 VMkernel。	指定存在于网络映射配置中的 VMkernel。
9417	未找到端口组。	在网络映射配置中未指定存在于主机上的端口组。	指定存在于网络映射配置中的端口组。
9419	在迁移过程中未找到逻辑交换机。	未找到在网络接口映射配置中定义的逻辑交换机。	指定存在于网络接口映射配置中的逻辑交换机。
9420	在迁移过程中未找到逻辑端口。	在迁移过程中，NSX-T Data Center 未找到在逻辑交换机上创建的端口。	请确保未从逻辑交换机中删除逻辑端口，这样迁移才能成功。
9421	缺少主机信息，无法验证迁移过程。	无法从清单中检索主机信息。	重试迁移过程。
9423	固定到 VMkernel 接口的物理网卡未迁移到正确的主机交换机。	在环境中找到了固定的物理网卡，但是未将 VMkernel 和物理网卡迁移到同一主机交换机。	与 VMkernel 接口固定的物理网卡必须具有在同一主机交换机上将物理网卡与 VMkernel 映射的传输节点配置。

表 8-1. VMkernel 迁移错误 （续）

错误代码	问题	原因	解决方案
600	找不到对象。	逻辑交换机使用的指定传输区域不存在。 找不到在 VMK 映射目标中发现的逻辑交换机。	■ 指定存在于环境中的传输区域。 ■ 创建所需的逻辑交换机，或者使用现有的 VLAN 逻辑交换机。
8310	逻辑交换机类型不正确。	逻辑交换机类型为“覆盖网络”。	创建一个 VLAN 逻辑交换机。
9424	如果为安装或卸载设置同时配置了“仅迁移 PNIC”和“网络映射”，则无法迁移。	仅当配置其中一个设置时，迁移才会进行。	请确保为安装或卸载设置配置“仅迁移 PNIC”或“网络映射”。

创建独立主机或裸机服务器传输节点

必须先将 ESXi 主机、KVM 主机或裸机服务器添加到 NSX-T Data Center Fabric，然后配置传输节点。

Fabric 节点是已在 NSX-T Data Center 管理平面中注册并安装了 NSX-T Data Center 模块的节点。要使主机或裸机服务器成为 NSX-T Data Center 覆盖网络的一部分，必须先将其添加到 NSX-T Data Center Fabric。

传输节点是一个加入 NSX-T Data Center 覆盖网络或 NSX-T Data Center VLAN 网络的节点。

对于 KVM 主机或裸机服务器，您可以预配置 N-VDS，也可以让 NSX Manager 执行配置。对于 ESXi 主机，NSX Manager 始终配置 N-VDS。

注 如果打算从模板虚拟机中创建传输节点，请确保在主机上的 `/etc/vmware/nsx/` 中没有任何证书。如果证书存在，则 netcpa 代理不会创建该证书。

裸机服务器支持覆盖网络和 VLAN 传输区域。可以使用管理接口管理裸机服务器。应用程序接口允许您访问裸机服务器上的应用程序。

单个物理网卡同时为管理接口和应用程序 IP 接口提供 IP 地址。

双物理网卡为管理接口提供物理网卡和唯一 IP 地址。双物理网卡还为应用程序接口提供物理网卡和唯一 IP 地址。

绑定配置中的多个物理网卡为管理接口提供双物理网卡和唯一 IP 地址。绑定配置中的多个物理网卡还为应用程序接口提供双物理网卡和唯一 IP 地址。

最多可以为每个配置添加四个 N-VDS 交换机：为 VLAN 传输区域创建的标准 N-VDS、为 VLAN 传输区域创建的增强型 N-VDS、为覆盖网络传输区域创建的标准 N-VDS、为覆盖网络传输区域创建的增强型 N-VDS。

在同一主机上运行多个标准覆盖网络 N-VDS 交换机和 Edge 虚拟机的单个主机集群拓扑中，NSX-T Data Center 提供了流量隔离以便通过第一个 N-VDS 的流量与通过第二个 N-VDS 的流量隔离，以此类推。每个 N-VDS 上的物理网卡必须映射到主机上的 Edge 虚拟机，以允许与外界的南北向流量连接。从第一个传输区域上的虚拟机移出的数据包必须通过外部路由器或外部虚拟机路由到第二个传输区域上的虚拟机。

前提条件

- 主机必须已加入管理平面，且连接必须已启动。
- 必须配置一个传输区域。
- 必须配置一个上行链路配置文件，也可以使用默认上行链路配置文件。
- 必须配置一个 IP 池，或者必须在网络部署中具有 DHCP。
- 必须在主机节点上具有至少一个未使用的物理网卡。
- 主机名
- 管理 IP 地址
- 用户名
- 密码
- （可选）(KVM) SHA-256 SSL 指纹
- （可选）(ESXi) SHA-256 SSL 指纹
- 确认安装了所需的第三方软件包。请参见在 KVM 主机上安装第三方软件包。

步骤

1 （可选） 检索管理程序指纹，以便在将主机添加到 Fabric 时提供该指纹。

a 收集管理程序指纹信息。

使用 Linux shell。

```
# echo -n | openssl s_client -connect <esxi-ip-address>:443 2>/dev/null | openssl x509 -noout
-fingerprint -sha256
```

使用主机中的 ESXi CLI。

```
[root@host:~] openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha256 -noout
SHA256
Fingerprint=49:73:F9:A6:0B:EA:51:2A:15:57:90:DE:C0:89:CA:7F:46:8E:30:15:CA:4D:5C:95:28:0A:9E:A
2:4E:3C:C4:F4
```

b 从 KVM 管理程序中检索 SHA-256 指纹，在 KVM 主机中运行该命令。

```
# awk '{print $2}' /etc/ssh/ssh_host_rsa_key.pub | base64 -d | sha256sum -b | sed 's/ .*$//'
| xxd -r -p | base64
```

2 选择**系统 > 结构层 > 节点 > 主机传输节点**。

3 从“托管主体”字段中，选择**独立主机**，然后单击 **+ 添加**。

4 输入要添加到 Fabric 的独立主机或裸机服务器详细信息。

选项	说明
名称和说明	输入名称以标识独立主机或裸机服务器。 可以选择添加用于主机或裸机服务器的操作系统说明。
IP 地址	输入主机或裸机服务器的 IP 地址。
操作系统	从下拉菜单中选择操作系统。 根据主机或裸机服务器，可以选择支持的任何操作系统。请参见系统要求。
用户名和密码	输入主机的用户名和密码。
SHA-256 指纹	输入主机指纹值以进行身份验证。 如果将指纹值留空，将提示您接受服务器提供的指纹。NSX-T Data Center 发现主机并对其进行身份验证需要几秒钟的时间。

5 （必选） 对于 KVM 主机或裸机服务器，选择 N-VDS 类型。

选项	说明
NSX 已创建	NSX Manager 创建 N-VDS。 默认情况下，将选择该选项。
预配置	已配置 N-VDS。

对于 ESXi 主机，N-VDS 类型始终设置为 **NSX 已创建**。

6 输入标准 N-VDS 详细信息。可以在单个主机上配置多个 N-VDS 交换机。

选项	说明
传输区域	从下拉菜单中选择此传输节点所属的传输区域。
N-VDS 名称	必须与该节点所属传输区域的 N-VDS 名称相同。
NIOC 配置文件	对于 ESXi 主机，从下拉菜单中选择 NIOC 配置文件。
上行链路配置文件	从下拉菜单中选择一个现有的上行链路配置文件，或者创建一个自定义上行链路配置文件。 也可以使用默认上行链路配置文件。
LLDP 配置文件	默认情况下，NSX-T 仅接收来自 LLDP 邻居的 LLDP 数据包。 但是，可以将 NSX-T 设置为与 LLDP 邻居传输 LLDP 数据包。
IP 分配	选择**使用 DHCP**、**使用 IP 池**或**使用静态 IP 列表**。 如果选择**使用静态 IP 列表**，您必须指定以逗号分隔的 IP 地址、网关和子网掩码列表。
IP 池	如果您选择**使用 IP 池**进行 IP 分配，请指定 IP 池名称。

选项	说明
物理网卡	将物理网卡添加到传输节点。您可以使用默认上行链路，或者从下拉菜单中分配一个现有的上行链路。 单击**添加 PNIC** 为传输节点配置其他物理网卡。 **注** 在此字段中添加的物理网卡的迁移取决于配置**仅迁移 PNIC**、**用于安装的网络映射**和**用于卸载的网络映射**的方式。 ■ 要迁移没有关联 VMkernel 映射的已用物理网卡（例如，通过标准 vSwitch 或 vSphere Distributed Switch），请确保已启用**仅迁移 PNIC**。否则，传输节点状态保持为**部分成功**，并且无法建立 Fabric 节点 LCP 连接。 ■ 要迁移具有关联 VMkernel 网络映射的已用物理网卡，请禁用**仅迁移 PNIC** 并配置 VMkernel 网络映射。 ■ 要迁移可用物理网卡，请启用**仅迁移 PNIC**。
仅迁移 PNIC	在设置此字段之前，请考虑以下几点： ■ 了解定义的物理网卡是已用网卡还是可用网卡。 ■ 确定主机的 VMkernel 接口是否需要与物理网卡一起迁移。 设置以下字段： ■ 如果仅希望将物理网卡从 VSS 或 DVS 交换机迁移到 N-VDS 交换机，则启用**仅迁移 PNIC**。 ■ 如果要迁移已用的物理网卡及其关联的 VMkernel 接口映射，则禁用**仅迁移 PNIC**。指定 VMkernel 接口迁移映射时，可用物理网卡将连接到 N-VDS 交换机。 在具有多个主机交换机的主机上： ■ 如果所有主机交换机都仅迁移 PNIC，则可以在单个操作中迁移 PNIC。 ■ 如果一些主机交换机要迁移 VMkernel 接口，而其余的主机交换机要仅迁移 PNIC： 1 在第一个操作中，仅迁移 PNIC。 2 在第二个操作中，迁移 VMkernel 接口。请确保已禁用**仅迁移 PNIC**。 不支持同时在多个主机中执行仅迁移 PNIC 和 VMkernel 接口迁移。 **注** 要迁移管理网络网卡，请配置其关联的 VMkernel 网络映射并使**仅迁移 PNIC** 保持禁用状态。如果仅迁移管理网卡，则主机将失去连接。 有关详细信息，请参见 VMkernel 迁移到 N-VDS 交换机。

选项	说明
用于安装的网络映射	要在安装期间将 VMkernel 迁移到 N-VDS 交换机，请将 VMkernel 映射到现有逻辑交换机。NSX Manager 将 VMkernel 迁移到 N-VDS 上的映射逻辑交换机。 小心　确保管理网卡和管理 VMkernel 接口迁移到的逻辑交换机连接到迁移前管理网卡所连接的同一 VLAN。如果 vmnic<*n*> 和 VMkernel<*n*> 迁移到不同的 VLAN，则将失去与主机的连接。 小心　对于固定的物理网卡，请确保物理网卡到 VMkernel 接口的主机交换机映射与在传输节点配置文件中指定的配置匹配。在验证过程中，NSX-T Data Center 将检查映射，以及验证通过后 VMkernel 接口是否成功迁移到 N-VDS 交换机。同时，必须为卸载配置网络映射，因为将 VMkernel 接口迁移到 N-VDS 交换机后，NSX-T Data Center 不会存储主机交换机的映射配置。如果未配置映射，则迁移回 VSS 或 VDS 交换机后，可能会失去与服务（如 vSAN）的连接。 有关详细信息，请参见 VMkernel 迁移到 N-VDS 交换机。
用于卸载的网络映射	要在卸载期间恢复 VMkernel 的迁移，请将 VMkernel 映射到 VSS 或 DVS 上的端口组，以便 NSX Manager 知道必须将 VMkernel 迁移回 VSS 或 DVS 上的哪个端口组。对于 DVS 交换机，请确保端口组的类型为临时。 小心　对于固定的物理网卡，请确保物理网卡到 VMkernel 接口的传输节点配置文件映射与在主机交换机中指定的配置匹配。必须为卸载配置网络映射，因为将 VMkernel 接口迁移到 N-VDS 交换机后 NSX-T Data Center 不会存储主机交换机的映射配置。如果未配置映射，则迁移回 VSS 或 VDS 交换机后，可能会失去与服务（如 vSAN）的连接。 有关详细信息，请参见 VMkernel 迁移到 N-VDS 交换机。

7　输入增强型数据路径 N-VDS 详细信息。可以在单个主机上配置多个 N-VDS 交换机。

选项	说明
N-VDS 名称	必须与该节点所属传输区域的 N-VDS 名称相同。
IP 分配	选择**使用 DHCP**、**使用 IP 池**或**使用静态 IP 列表**。 如果选择**使用静态 IP 列表**，您必须指定以逗号分隔的 IP 地址、网关和子网掩码列表。
IP 池	如果您选择**使用 IP 池**进行 IP 分配，请指定 IP 池名称。
物理网卡	将物理网卡添加到传输节点。您可以使用默认上行链路，或者从下拉菜单中分配一个现有的上行链路。 单击**添加 PNIC** 为传输节点配置其他物理网卡。 注　在此字段中添加的物理网卡的迁移取决于配置**仅迁移 PNIC**、**用于安装的网络映射**和**用于卸载的网络映射**的方式。 ■ 要迁移没有关联 VMkernel 映射的已用物理网卡（例如，通过标准 vSwitch 或 vSphere Distributed Switch），请确保已启用**仅迁移 PNIC**。否则，传输节点状态保持为**部分成功**，并且无法建立 Fabric 节点 LCP 连接。 ■ 要迁移具有关联 VMkernel 网络映射的已用物理网卡，请禁用**仅迁移 PNIC** 并配置 VMkernel 网络映射。 ■ 要迁移可用物理网卡，请启用**仅迁移 PNIC**。
上行链路	从下拉菜单中选择上行链路配置文件。

选项	说明
CPU 配置	在“NUMA 节点索引”下拉菜单中，选择要分配给 N-VDS 交换机的 NUMA 节点。节点上存在的第一个 NUMA 节点用值 0 表示。 可以通过运行 `esxcli hardware memory get` 命令了解主机上的 NUMA 节点数。 **注** 如果要更改与 N-VDS 交换机具有关联性的 NUMA 节点数，可以更新“NUMA 节点索引”值。
	在“每个 NUMA 节点逻辑内核数”下拉菜单中，选择增强型数据路径必须使用的逻辑内核数。 可以通过运行 `esxcli network ens maxLcores get` 命令了解可在 NUMA 节点上创建的最大逻辑内核数。 **注** 如果用尽可用 NUMA 节点和逻辑内核，则无法针对 ENS 流量启用添加到传输节点的任何新交换机。

8 对于预配置的 N-VDS，请提供以下详细信息。

选项	说明
N-VDS 外部 ID	必须与该节点所属传输区域的 N-VDS 名称相同。
VTEP	虚拟隧道端点名称。

9 在**主机传输节点**页面上查看连接状态。

将主机或裸机服务器添加为传输节点后，到 NSX Manager 的连接在 3-4 分钟后将变为“已启动”状态。

10 或者，使用 CLI 命令查看连接状态。

- 对于 ESXi，请键入 `esxcli network ip connection list | grep 1234` 命令。

```
# esxcli network ip connection list | grep 1234
tcp   0   0  192.168.210.53:20514  192.168.110.34:1234   ESTABLISHED  1000144459  newreno
netcpa
```

- 对于 KVM，请键入 `netstat –anp ––tcp | grep 1234` 命令。

```
user@host:~$ netstat –anp ––tcp | grep 1234
tcp  0   0 192.168.210.54:57794  192.168.110.34:1234   ESTABLISHED –
```

11 确认在主机或裸机服务器上已安装 NSX-T Data Center 模块。

将主机或裸机服务器添加到 NSX-T Data Center Fabric 后，将在主机或裸机服务器上安装 NSX-T Data Center 模块的集合。

将打包不同主机上的模块，如下所示：

- RHEL 或 CentOS 上的 KVM - RPM。

- Ubuntu 上的 KVM - DEB
- 在 ESXi 上，输入命令 `esxcli software vib list | grep nsx`。

  日期为执行安装的日期。
- 在 RHEL 或 CentOS 上，输入命令 `yum list installed` 或 `rpm -qa`。
- 在 Ubuntu 上，输入命令 `dpkg --get-selections`。

12 （可选） 如果具有 500 个或更多管理程序，则更改某些进程的轮询间隔。

如果具有 500 多个管理程序，则 NSX Manager 可能会遇到 CPU 使用过高和性能问题。

a 使用 NSX-T Data Center CLI 命令 `copy file` 或 API `POST /api/v1/node/file-store/<file-name>?action=copy_to_remote_file` 将 `aggsvc_change_intervals.py` 脚本复制到主机。

b 运行位于 NSX-T Data Center 文件存储中的脚本。

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -i
900
```

c （可选） 将轮询间隔改回到默认值。

```
python aggsvc_change_intervals.py -m '<NSX ManagerIPAddress>' -u 'admin' -p '<password>' -r
```

结果

注 对于 NSX-T Data Center 创建的 N-VDS，创建传输节点后，如果要更改配置，例如，隧道端点的 IP 分配，必须通过 NSX Manager GUI 而不是主机上的 CLI 执行此操作。

后续步骤

将网络接口从 vSphere 标准交换机迁移到 N-VDS。请参见 VMkernel 迁移到 N-VDS 交换机。

配置受管主机传输节点

如果具有一个 vCenter Server，您可以在所有 NSX-T Data Center 主机上自动完成安装和创建传输节点的过程，而不是手动配置这些节点。

如果已配置传输节点，则自动创建传输节点功能不适用于该节点。

前提条件

- 确认 vCenter Server 中的所有主机都已打开电源。
- 确认满足系统要求。请参见系统要求。
- 确认一个传输区域可用。请参见创建传输区域。
- 确认配置了一个传输节点配置文件。请参见添加传输节点配置文件。

步骤

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

2 选择**系统 > 结构层 > 节点 > 主机传输节点**。

3 从“托管主体”下拉菜单中，选择一个现有的 vCenter Server。

该页面会列出所选 vCenter Server 中的可用 vSphere 集群和/或 ESXi 主机。您可能需要展开集群才能查看 ESXi 主机。

4 从列表中选择一个主机，然后单击**配置 NSX**。

此时会打开“配置 NSX”对话框。

a 在“主机详细信息”面板中验证主机名。您可以选择添加描述。

b 单击**下一步**以移动到**配置 NSX** 面板。

c 选择可用的传输区域，然后单击 **>** 按钮将传输区域包括在传输节点配置文件中。

5 在“主机详细信息”面板中验证主机名，然后单击**下一步**。

您可以选择添加描述。

6 在**配置 NSX** 面板中，选择所需的传输区域。

您可以选择多个传输区域。

7 （可选） 查看 ESXi 连接状态。

```
# esxcli network ip connection list | grep 1235
tcp   0   0  192.168.210.53:20514  192.168.110.34:1234   ESTABLISHED  1000144459  newreno  netcpa
```

8 从“主机传输节点”页面中，确认集群中主机的 NSX Manager 连接状态为“已启动”且 NSX-T Data Center 配置状态为“成功”。

也可以看到，传输区域已应用于集群中的主机。

9 （可选） 从传输区域内的主机中移除 NSX-T Data Center 安装和传输节点。

a 选择一个或多个主机，然后单击**操作 > 移除 NSX**。

卸载最多需要 3 分钟的时间。卸载 NSX-T Data Center 将移除主机上的传输节点配置，且主机从传输区域和 N-VDS 交换机中分离。在将传输节点配置文件重新应用于集群之前，不会自动配置添加到 vCenter Server 集群的任何新主机。

10 （可选） 从传输区域中移除传输节点。

a 选择一个传输节点，然后单击**操作 > 从传输区域中移除**。

后续步骤

创建逻辑交换机并分配逻辑端口。请参见 NSX-T Data Center 管理指南中的“高级交换”部分。

使用链路聚合配置 ESXi 主机传输节点

此过程介绍如何创建已配置链路聚合组的上行链路配置文件，以及如何将 ESXi 主机传输节点配置为使用该上行链路配置文件。

前提条件

- 熟悉创建上行链路配置文件的步骤。请参见创建上行链路配置文件。
- 熟悉创建主机传输节点的步骤。请参见 创建独立主机或裸机服务器传输节点。

步骤

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

2 选择**系统 > 结构层 > 配置文件 > 上行链路配置文件 > 添加**。

3 输入名称和可选的说明。

例如，输入名称 **uplink-profile1**。

4 在 **LAG** 下，单击**添加**以添加链路聚合组。

例如，添加具有 2 个上行链路、名为 **lag1** 的 LAG。

5 在**绑定**下面，选择**默认绑定**。

6 在**活动上行链路**字段中，输入在步骤 4 中添加的 LAG 的名称。在此示例中，名称为 **lag1**。

7 输入**传输 VLAN** 和 **MTU** 的值。

8 单击对话框底部的**添加**。

9 在**绑定**下，单击**添加**为链路聚合添加一个条目。

10 选择**结构层 > 节点 > 主机传输节点 > 添加**。

11 在**主机详细信息**选项卡中，输入主机的 IP 地址、操作系统名称、管理员凭据和 SHA-256 指纹。

12 在 **N-VDS** 选项卡中，选择在步骤 3 中创建的上行链路配置文件 **uplink-profile1**。

13 在**物理网卡**字段中，物理网卡和上行链路下拉列表将反映新的网卡和上行链路配置文件。具体来说，将显示上行链路 **lag1-0** 和 **lag1-1**（与步骤 4 中创建的 LAG **lag1** 相对应）。选择 **lag1-0** 的物理网卡和 **lag1-1** 的物理网卡。

14 输入其他字段的信息。

完全合并的单一 vSphere 集群 NSX-T 部署

配置 NSX Manager 和主机传输节点，以便在单个集群上运行工作负载虚拟机和 NSX Edge 虚拟机。集群中的每个主机都提供了两个为 NSX-T 配置的物理网卡。

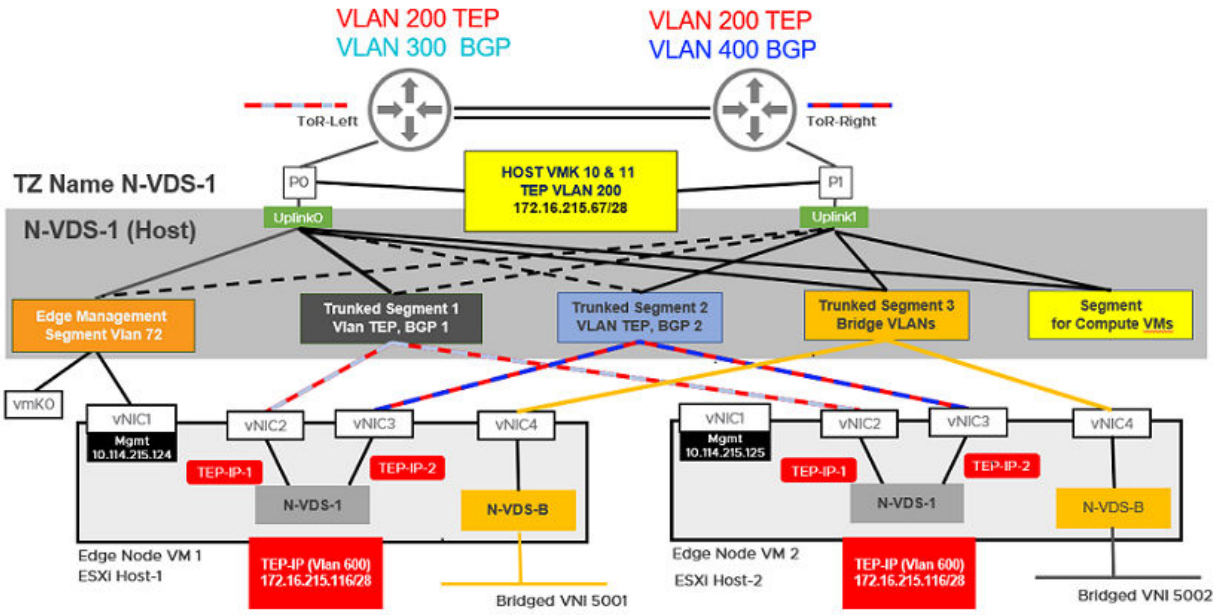
重要事项 从 NSX-T 2.4.2 或 2.5 版本开始，可部署完全合并的单一 vSphere 集群拓扑。

此过程中引用的拓扑将使用：

- 通过集群中的主机来配置的 vSAN。

- 每个主机中的至少两个物理网卡。
- vMotion 和 Management VMkernel 接口。

图 8-3. 拓扑：单个 N-VDS 交换机，用于管理主机与 NSX Edge 和客户机虚拟机之间的通信



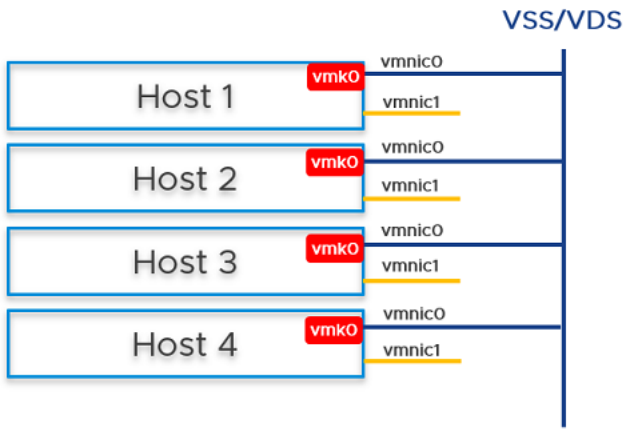
注 即使主机有四个物理网卡，也只能使用两个网卡来部署完全合并的单一拓扑。此过程将主机上的物理网卡称为 vmnic0 和 vmnic1。

前提条件

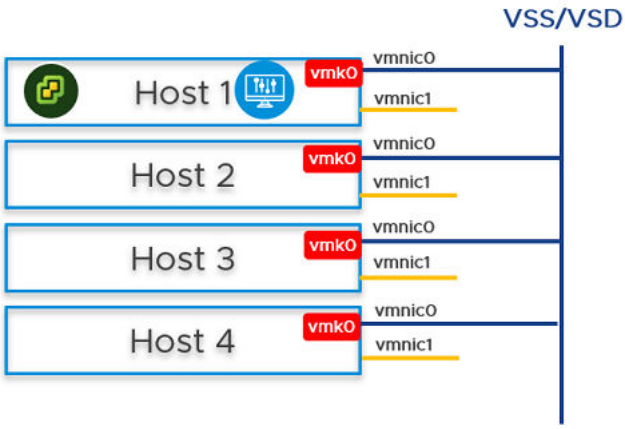
- 所有主机必须属于同一个 vSphere 集群。
- 每个主机都启用了两个物理网卡。
- 向 vCenter Server 注册所有主机。
- 在 vCenter Server 上确认共享存储器可供这些主机使用。
- 确保用于 NSX Edge TEP 和主机 TEP 的 VLAN ID 不同。

步骤

1 准备四个 ESXi 主机，vmnic0 位于 vSS 或 vDS 上，vmnic1 处于空闲状态。



2 在主机 1 上，安装 vCenter Server，配置 vSS/vDS 端口组，然后在主机上创建的端口组中安装 NSX Manager。



3 准备要用作传输节点的 ESXi 主机 1、2、3 和 4。

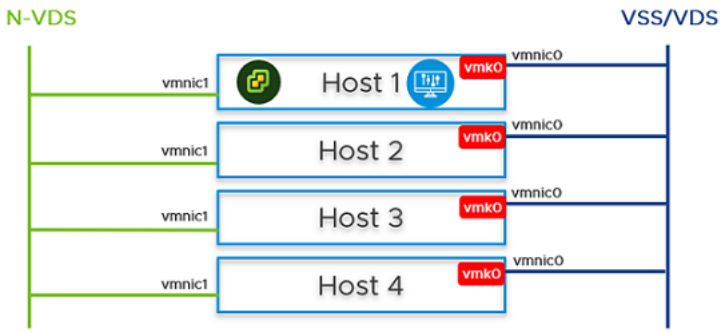
a 创建包含指定绑定策略的 VLAN 传输区域。请参见创建传输区域。

b 为主机的隧道端点 IP 地址创建一个 IP 池或 DHCP。请参见创建 IP 池以分配隧道端点 IP 地址。

c 为 Edge 节点的隧道端点 IP 地址创建一个 IP 池或 DHCP。请参见创建 IP 池以分配隧道端点 IP 地址。

d 创建包含指定绑定策略的上行链路配置文件。请参见创建上行链路配置文件。

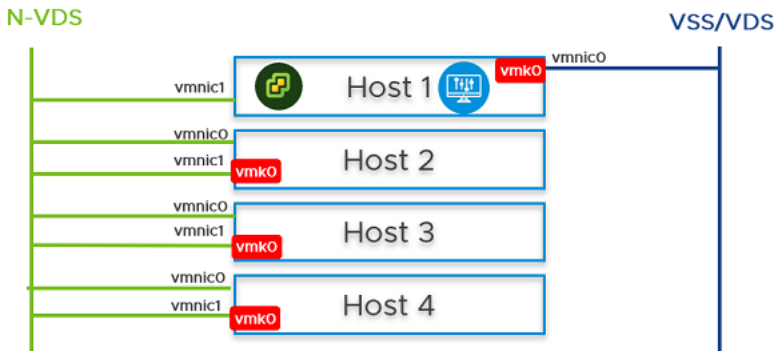
e 通过应用传输节点配置文件来将主机配置为传输节点。在此步骤中，传输节点配置文件仅将 vmnic1（未使用的物理网卡）迁移到 N-VDS 交换机。在将传输节点配置文件应用于集群主机后，将创建 N-VDS 交换机，并将 vmnic1 连接到 N-VDS 交换机。请参见添加传输节点配置文件。



所有主机上的 vmnic1 都会添加到 N-VDS 交换机。因此，在两个物理网卡中，有一个会迁移到 N-VDS 交换机。vmnic0 接口仍会连接到 vSS 或 vDS 交换机，这可确保到主机的连接可用。

4 在 NSX Manager 用户界面中，为 NSX Manager、vCenter Server 和 NSX Edge 创建支持 VLAN 的分段。请确保为每个支持 VLAN 的分段选择正确的绑定策略。

5 在主机 2、主机 3 和主机 4 上，必须将 vmk0 适配器和 vmnic0 一起从 VSS/VDS 迁移到 N-VDS 交换机。更新每个主机上的 NSX-T 配置。迁移时，请确保 vmnic0 已映射到活动上行链路。

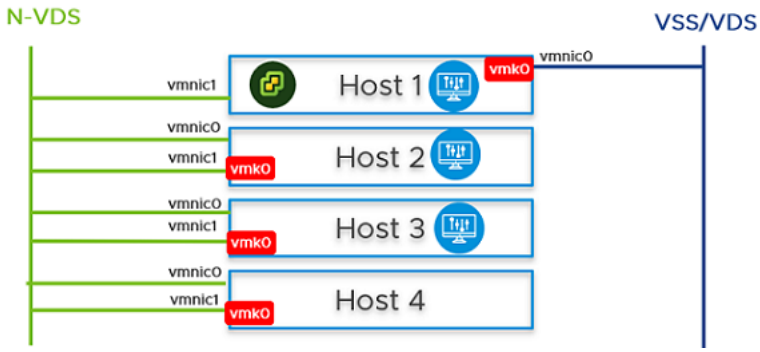


6 在 vCenter Server 中，转至主机 2、主机 3 和主机 4，同时确认 vmk0 适配器已连接到 N-VDS 上的 vmnic0 物理网卡且必须可访问。

7 在 NSX Manager 用户界面中，转至主机 2、主机 3 和主机 4，并确认这两个物理网卡都位于 N-VDS 交换机上。

8 创建逻辑分段，并将 NSX Manager 连接到该逻辑分段。等待大约 10 分钟以形成集群，并验证集群是否已形成。

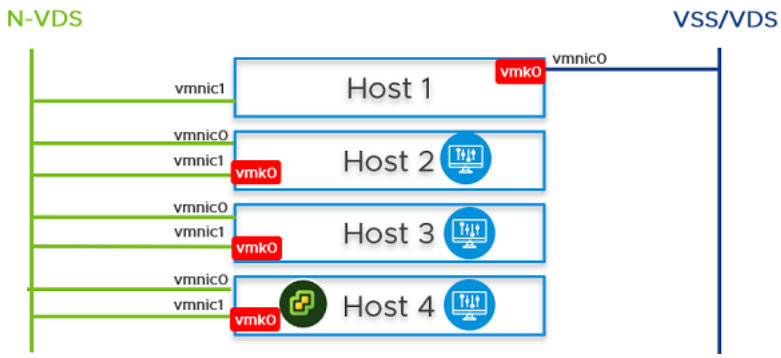
9 在主机 2 和主机 3 上，从 NSX Manager 用户界面中安装 NSX Manager。



10 关闭第一个 NSX Manager 节点的电源。等待大约 10 分钟。

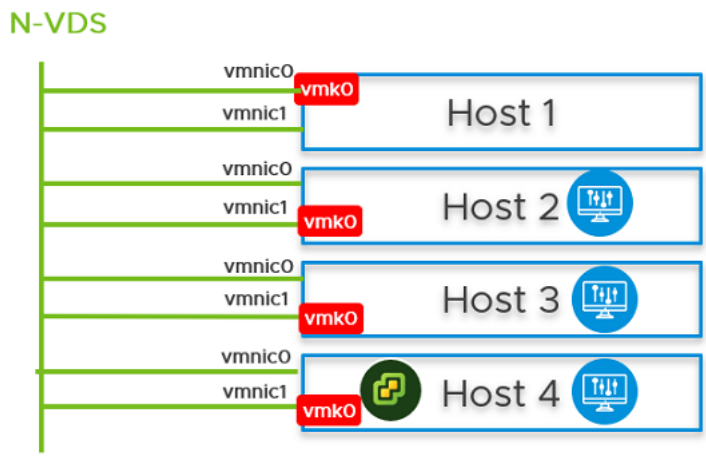
11 将 NSX Manager 和 vCenter Server 重新连接到先前创建的逻辑交换机。在主机 4 上，打开 NSX Manager 的电源。等待大约 10 分钟，然后验证集群是否处于稳定状态。在第一个 NSX Manager 关闭电源后，执行冷 vMotion 以将 NSX Manager 和 vCenter Server 从主机 1 迁移到主机 4。

有关 vMotion 限制的信息，请参见 https://kb.vmware.com/s/article/56991。



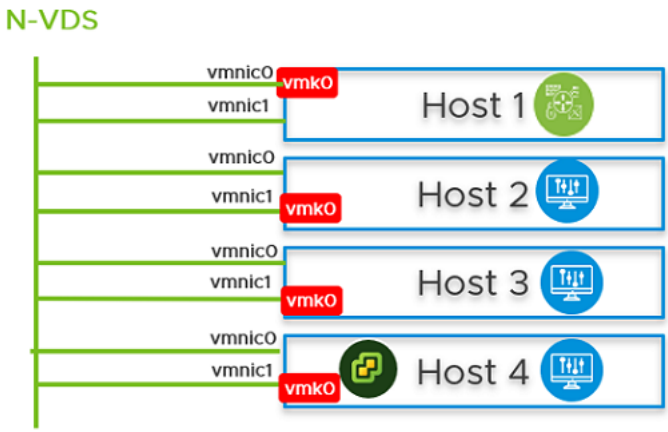
12 从 NSX Manager 用户界面中，转至主机 1，将 vmk0 和 vmnic0 一起从 VSS 迁移到 N-VDS 交换机。

13 在**用于安装的网络映射**字段中，确保 vmk0 适配器已映射到 N-VDS 交换机上的管理逻辑分段。



14 在主机 1 上，通过 NSX Manager UI 安装 NSX Edge 虚拟机。

请参见创建 NSX Edge 传输节点。



15 将 NSX Edge 虚拟机加入管理平面。

请参见将 NSX Edge 加入管理层面。

16 要建立南北向流量连接，请为 NSX Edge 虚拟机配置一个外部路由器。

17 验证 NSX Edge 虚拟机与外部路由器之间的南北向流量连接。

18 设置并验证 NSX Manager 和 NSX Edge 虚拟机之间的 BFD 连接。

19 如果出现了要重新引导整个集群的电源故障，则 NSX-T 管理组件可能无法启动并与 N-VDS 通信。为了避免出现这种情况，请执行以下步骤：

小心 错误地运行任何 API 命令都会导致与 NSX Manager 的连接中断。

注 在单集群配置中，管理组件将作为虚拟机托管在 N-VDS 交换机上。出于安全考虑，管理组件默认情况下连接到的 N-VDS 端口会初始化为已阻止的端口。如果出现了需要重新引导所有四个主机（建议的最低配置）的电源故障，则在默认重新引导状态下，管理虚拟机端口将处于已阻止状态。为避免出现循环依赖关系，建议在 N-VDS 上创建处于未阻止状态的端口。未阻止的端口可确保在集群重新引导时，NSX-T 管理组件可以与 N-VDS 通信以恢复正常功能。

在该子任务结束时，迁移命令会采用以下信息：

- NSX Manager 所在主机节点的 UUID。
- NSX Manager 虚拟机的 UUID，并且会将其迁移到处于未阻止状态的静态逻辑端口。

如果所有主机都已关闭电源或都已打开电源，或者如果 NSX Manager 虚拟机移至另一台主机，则 NSX Manager 在恢复后会连接到未阻止的端口，从而防止与 NSX-T 管理组件的连接中断。

a 转至**高级网络和安全** → **交换**，选择 MGMT-VLAN-Segment。在**概览**选项卡中，找到并复制 UUID。此示例中使用的 UUID 为 *c3fd8e1b-5b89-478e-abb5-d55603f04452*。

b 要创建初始化为 **UNBLOCKED_VLAN** 状态的逻辑端口，请创建四个 JSON 文件，其中三个文件用于 NSX Manager，还有一个则用于 vCenter Server Appliance (VCSA)。将 `logical_switch_id` 的值替换为先前创建的 MGMT-VLAN-Segment 分段的 UUID。

```
mgrhost.json
{
"admin_state": "UP",
"attachment": {
"attachment_type": "VIF",
"id": "nsxmgr-port-147"
},
"display_name": "NSX Manager Node 147 Port",
"init_state": "UNBLOCKED_VLAN",
"logical_switch_id": "c3fd8e1b-5b89-478e-abb5-d55603f04452"
}
```

c 通过 API 客户端或使用 curl 命令为管理器创建逻辑端口。

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -X POST -k -u
'<username>:<password>' -H 'Content-Type:application/json' -d @mgr.json https://
localhost/api/v1/logical-ports
{
  "logical_switch_id" : "c3fd8e1b-5b89-478e-abb5-d55603f04452",
  "attachment" : {
    "attachment_type" : "VIF",
    "id" : "nsxmgr-port-147"
  },
  "admin_state" : "UP",
  "address_bindings" : [ ],
  "switching_profile_ids" : [ {
    "key" : "SwitchSecuritySwitchingProfile",
    "value" : "fbc4fb17-83d9-4b53-a286-ccdf04301888"
  }, {
    "key" : "SpoofGuardSwitchingProfile",
    "value" : "fad98876-d7ff-11e4-b9d6-1681e6b88ec1"
  }, {
    "key" : "IpDiscoverySwitchingProfile",
    "value" : "0c403bc9-7773-4680-a5cc-847ed0f9f52e"
  }, {
    "key" : "MacManagementSwitchingProfile",
    "value" : "1e7101c8-cfef-415a-9c8c-ce3d8dd078fb"
  }, {
    "key" : "PortMirroringSwitchingProfile",
    "value" : "93b4b7e8-f116-415d-a50c-3364611b5d09"
  }, {
    "key" : "QosSwitchingProfile",
    "value" : "f313290b-eba8-4262-bd93-fab5026e9495"
  } ],
  "init_state" : "UNBLOCKED_VLAN",
  "ignore_address_bindings" : [ ],
  "resource_type" : "LogicalPort",
  "id" : "02e0d76f-83fa-4839-a525-855b47ecb647",
  "display_name" : "NSX Manager Node 147 Port",
  "_create_user" : "admin",
  "_create_time" : 1574716624192,
  "_last_modified_user" : "admin",
  "_last_modified_time" : 1574716624192,
  "_system_owned" : false,
  "_protection" : "NOT_PROTECTED",
  "_revision" : 0
```

d 将 NSX Manager 移到采用静态方式创建的逻辑端口。

e 要复制 NSX Manager 虚拟机实例 ID，请转至“高级网络和安全 → 清单 → 虚拟机”。选择 NSX Manager 虚拟机。在**概览**选项卡中，找到并复制 ID。此示例中使用的 ID 为 *5028d756-d36f-719e-3db5-7ae24aa1d6f3*。

f 要查找安装了 NSX Manager 的主机 ID，请转至**系统 -> Fabric -> 节点 -> 主机传输节点**。选择主机，然后单击**概览**选项卡。查找并复制主机 ID。此示例中使用的 ID 为 *11161331-11f8-45c7-8747-34e7218b687f*。

g 将 NSX Manager 从虚拟机网络迁移到先前在 MGMT-VLAN-Segment 上创建的逻辑端口。`vnic_migration_dest` 值是先前为 NSX Manager 创建的端口的连接 ID。

```
root@nsx-mgr-147:/var/CollapsedCluster# curl -k -X PUT -u '<username>:<password>' -H
'Content-Type:application/json' -d @mgrhost.json
'https://localhost/api/v1/transport-nodes/11161331-11f8-45c7-8747-34e7218b687f?
vnic_migration_dest=nsxmgr-port-147'
```

h 在 NSX Manager 用户界面中，确保采用静态方式创建的逻辑端口已启动。

i 对集群中的每个 NSX Manager 重复上述步骤。

验证传输节点状态

确保传输节点创建过程正常工作。

在创建主机传输节点后，将在主机上安装 N-VDS。

步骤

1 登录到 NSX-T Data Center。

2 导航到“传输节点”页面并查看 N-VDS 状态。

3 或者，使用 `esxcli network ip interface list` 命令查看 ESXi 上的 N-VDS。

在 ESXi 上，命令输出应包含一个 vmk 接口（如 vmk10）和 VDS 名称，该名称与在配置传输区域和传输节点时使用的名称相匹配。

```
# esxcli network ip interface list
...

vmk10
   Name: vmk10
```

```
   MAC Address: 00:50:56:64:63:4c
   Enabled: true
   Portset: DvsPortset-1
   Portgroup: N/A
   Netstack Instance: vxlan
   VDS Name: overlay-hostswitch
   VDS UUID: 18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2
   VDS Port: 10
   VDS Connection: 10
   Opaque Network ID: N/A
   Opaque Network Type: N/A
   External ID: N/A
   MTU: 1600
   TSO MSS: 65535
   Port ID: 67108895

 ...
```

如果使用 vSphere Client，可以在 UI 中选择主机**配置 > 网络适配器**查看安装的 N-VDS。

用于验证 N-VDS 安装的 KVM 命令是 `ovs-vsctl show`。请注意，在 KVM 上，N-VDS 名称为 nsx-switch.0。它与传输节点配置中的名称不匹配。这是设计问题。

```
# ovs-vsctl show
...
    Bridge "nsx-switch.0"
        Port "nsx-uplink.0"
            Interface "em2"
        Port "nsx-vtep0.0"
            tag: 0
            Interface "nsx-vtep0.0"
                type: internal
        Port "nsx-switch.0"
            Interface "nsx-switch.0"
                type: internal
    ovs_version: "2.4.1.3340774"
```

4 检查为传输节点分配的隧道端点地址。

vmk10 接口从 NSX-T Data Center IP 池或 DHCP 中接收 IP 地址，如下所示：

```
# esxcli network ip interface ipv4 get
Name   IPv4 Address    IPv4 Netmask   IPv4 Broadcast   Address Type  DHCP DNS
-----  --------------  -------------  ---------------  ------------  --------
vmk0   192.168.210.53  255.255.255.0  192.168.210.255  STATIC           false
vmk1   10.20.20.53     255.255.255.0  10.20.20.255     STATIC           false
vmk10 192.168.250.3   255.255.255.0  192.168.250.255  STATIC          false
```

在 KVM 中，您可以使用 `ifconfig` 命令验证隧道端点和 IP 分配。

```
# ifconfig
...
nsx-vtep0.0 Link encap:Ethernet  HWaddr ba:30:ae:aa:26:53
          inet addr:192.168.250.4  Bcast:192.168.250.255  Mask:255.255.255.0
          ...
```

5 检查 API 以了解传输节点状态信息。

使用 `GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/state` API 调用。例如：

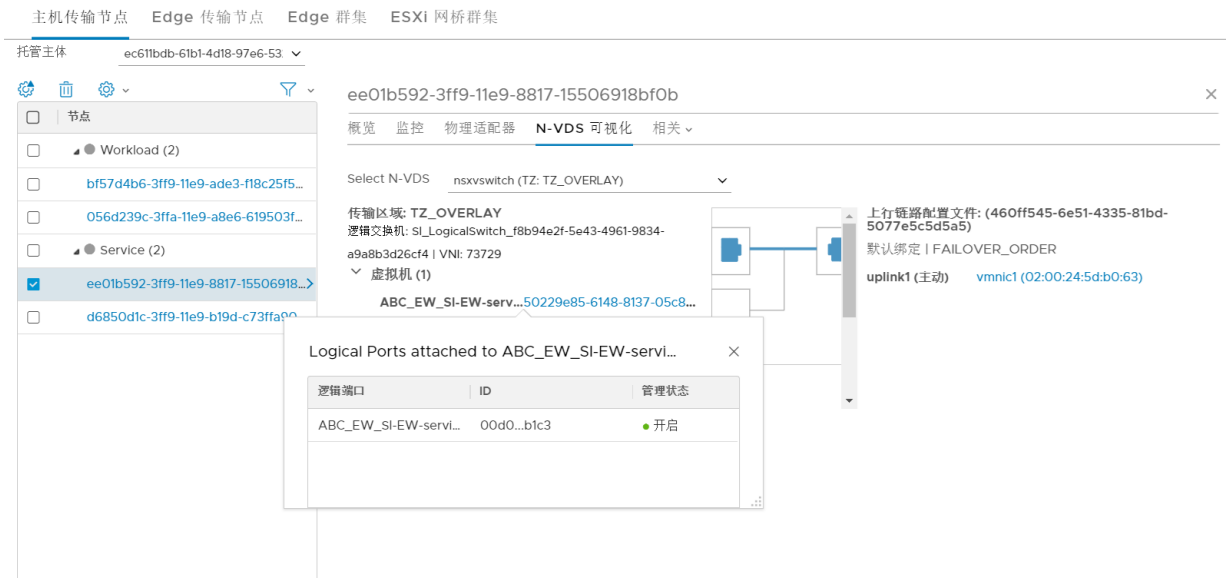
```
{
  "state": "success",
  "host_switch_states": [
    {
      "endpoints": [
        {
          "default_gateway": "192.168.250.1",
          "device_name": "vmk10",
          "ip": "192.168.250.104",
          "subnet_mask": "255.255.255.0",
          "label": 69633
        }
      ],
      "transport_zone_ids": [
        "efd7f38f-c5da-437d-af03-ac598f82a9ec"
      ],
      "host_switch_name": "overlay-hostswitch",
      "host_switch_id": "18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2"
    }
  ],
  "transport_node_id": "2d030569-5769-4a13-8918-0c309c63fdb9"
}
```

N-VDS 的可视表示

在单个主机级别上获取 N-VDS 的精确度视图。NSX-T Data Center 提供了 N-VDS 的上行链路和与传输区域关联的虚拟机之间连接状态的可视表示。以可视方式表示的对象包括绑定策略 - 提供与虚拟机的连接的上行链路和物理网卡。以可视方式表示的另一组对象是虚拟机、关联的逻辑端口和交换机以及虚拟机的状态。可视表示使管理 N-VDS 变得更容易。

注 只有 ESXi 主机才支持 N-VDS 对象的可视化。

图 8-4. N-VDS 可视化



步骤

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

2 选择**系统 > 结构层 > 节点 > 主机传输节点**。

3 从“托管主体”字段中，选择**独立主机**或*计算管理器*。

4 选择主机。

5 单击 **N-VDS 可视化**选项卡。

6 选择一个 N-VDS。

NSX-T 以可视方式表示连接到虚拟机的上行链路配置文件、与虚拟机关联的逻辑端口、连接到传输区域的逻辑交换机。

7 要查看连接到虚拟机的上行链路配置文件和虚拟机连接到的逻辑端口，请选择虚拟机。

NSX-T 以可视方式表示虚拟机和上行链路配置文件之间的连接。

8 要查看哪些虚拟机已连接到上行链路配置文件，请选择上行链路配置文件。

9 要查看与虚拟机关联的逻辑端口，请展开逻辑交换机，单击该虚拟机。

将在一个单独的对话框中显示逻辑端口详细信息。

> **注** 在对话框上显示逻辑端口的管理状态。如果操作状态为“关闭”，则在对话框上不显示它。

手动安装 NSX-T Data Center 内核模块

作为使用 NSX-T Data Center **结构层 > 节点 > 主机 > 添加** UI 或 `POST /api/v1/fabric/nodes` API 的替代方法，您可以从管理程序命令行中手动安装 NSX-T Data Center 内核模块。

注 无法在裸机服务器上手动安装 NSX-T Data Center 内核模块。

在 ESXi 管理程序上手动安装 NSX-T Data Center 内核模块

要准备主机以加入 NSX-T Data Center 网络，您必须在 ESXi 主机上安装 NSX-T Data Center 内核模块。这样，您就可以构建 NSX-T Data Center 控制平面和管理平面 Fabric。在 VIB 文件中打包的 NSX-T Data Center 内核模块在管理程序内核中运行并提供一些服务，例如，分布式路由、分布式防火墙和桥接功能。

您可以手动下载 NSX-T Data Center VIB 并将其作为主机映像的一部分。每个 NSX-T Data Center 版本的下载路径可能会有所不同。请务必查看 NSX-T Data Center 下载页面以获取相应的 VIB。

步骤

1 作为 root 或具有管理权限的用户登录到主机。

2 导航到 /tmp 目录。

```
[root@host:~]: cd /tmp
```

3 下载 nsx-lcp 文件并将其复制到 /tmp 目录中。

4 运行 install 命令。

```
[root@host:/tmp]: esxcli software vib install –d /tmp/nsx–lcp–<release>.zip
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: VMware_bootbank_nsx–aggservice_<release>, VMware_bootbank_nsx–da_<release>,
VMware_bootbank_nsx–esx–datapath_<release>, VMware_bootbank_nsx–exporter_<release>,
VMware_bootbank_nsx–host_<release>, VMware_bootbank_nsx–lldp_<release>, VMware_bootbank_nsx–
mpa_<release>, VMware_bootbank_nsx–netcpa_<release>, VMware_bootbank_nsx–python–
protobuf_<release>, VMware_bootbank_nsx–sfhc_<release>, VMware_bootbank_nsxa_<release>,
VMware_bootbank_nsxcli_<release>
   VIBs Removed:
   VIBs Skipped:
```

根据在主机上已安装的内容，可能会安装、移除或跳过一些 VIB。不需要重新引导，除非命令输出显示 `Reboot Required: true`。

结果

将 ESXi 主机添加到 NSX-T Data Center Fabric 中后，会在主机上安装以下 VIB。

nsx-adf	（自动诊断框架）收集并分析性能数据，以生成对性能问题的本地（主机）和中心（跨数据中心）诊断。
nsx-aggservice	为 NSX-T Data Center 聚合服务提供主机端库。NSX-T Data Center 聚合服务是在管理平面节点中运行并从 NSX-T Data Center 组件中获取运行时状态的服务。
nsx-cli-libs	在管理程序主机上提供 NSX-T Data Center CLI。
nsx-common-libs	提供一些实用程序类，例如 AES、SHA-1、UUID 和位图等。
nsx-context-mux	提供 NSX 客户机侦测中继功能。允许 VMware Tools 客户机代理将客户机上下文中继到内部设备和已注册的第三方合作伙伴设备。
nsx-esx-datapath	提供 NSX-T Data Center 数据平面数据包处理功能。
nsx-exporter	提供主机代理以便向在管理平面中运行的聚合服务报告运行时状态。
nsx-host	为在主机上安装的 VIB 包提供元数据。
nsx-metrics-libs	提供用于收集守护进程衡量指标的衡量指标实用程序类。
nsx-mpa	在 NSX Manager 和管理程序主机之间提供通信。
nsx-nestdb-libs	NestDB 是一个用来存储与主机相关的 NSX 配置（所需/运行时状态等）的数据库。
nsx-netcpa	在中央控制平面和管理程序之间提供通信。从中央控制平面中接收逻辑网络状态，并以编程方式在数据平面中通告该状态。
nsx-opsagent	向管理平面传达操作代理执行情况（传输节点实现、链路层发现协议 (LLDP)、流跟踪、数据包捕获等）。
nsx-platform-client	为集中式 CLI 和审核日志收集提供了一个通用 CLI 执行代理。
nsx-profiling-libs	提供基于用于守护进程分析的 gpeftool 的分析功能。
nsx-proxy	提供仅与中央控制平面和管理平面通信的北向联络点代理。
nsx-python-gevent	包含 Python Gevent。
nsx-python-greenlet	包含 Python Greenlet 库（第三方库）。
nsx-python-logging	包含 Python 日志。
nsx-python-protobuf	为协议缓冲区提供 Python 绑定。
nsx-rpc-libs	此库提供了 nsx-rpc 功能。
nsx-sfhc	服务 Fabric 主机组件 (Service Fabric Host Component, SFHC)。提供主机代理，以便将管理程序作为管理平面清单中的 Fabric 主机以管理其生命周

	期。这会为操作提供一个通道，例如，NSX-T Data Center 升级和卸载以及监控管理程序上的 NSX-T Data Center 模块。
nsx-shared-libs	包含共享的 NSX 库。
nsx-upm-libs	为拼合客户端配置和避免重复数据传输提供统一的配置文件管理功能。
nsx-vdpi	为 NSX-T Data Center 分布式防火墙提供深层数据包检查功能。
nsxcli	在管理程序主机上提供 NSX-T Data Center CLI。
vsipfwlib	提供分布式防火墙功能。

要进行验证，您可以在 ESXi 主机上运行 `esxcli software vib list | grep nsx` 和 `esxcli software vib list | grep vsipfwlib` 命令。或者，您也可以运行 `esxcli software vib list | grep <yyyy-mm-dd>` 命令，其中的日期是执行安装的日期。

后续步骤

将主机添加到 NSX-T Data Center 管理平面。请参见使用 CLI 部署 NSX Manager 节点以形成群集 。

在 Ubuntu KVM 管理程序上手动安装 NSX-T Data Center 内核模块

要准备主机以加入 NSX-T Data Center，您可以手动在 Ubuntu KVM 主机上安装 NSX-T Data Center 内核模块。这样，您就可以构建 NSX-T Data Center 控制层面和管理层面结构层。在 DEB 文件中打包的 NSX-T Data Center 内核模块在管理程序内核中运行并提供一些服务，例如，分布式路由、分布式防火墙和桥接功能。

您可以手动下载 NSX-T Data Center DEB 并将其作为主机映像的一部分。请注意，每个 NSX-T Data Center 版本的下载路径可能会有所不同。请务必查看 NSX-T Data Center 下载页面以获取相应的 DEB。

前提条件

- 确认安装了所需的第三方软件包。请参见在 KVM 主机上安装第三方软件包。

步骤

1. 以具有管理权限的用户身份登录到主机。
2. （可选） 导航到 /tmp 目录。

```
cd /tmp
```

3. 下载 nsx-lcp 文件并将其复制到 /tmp 目录中。
4. 解压缩该软件包。

```
tar -xvf nsx-lcp-<release>-ubuntu-trusty_amd64.tar.gz
```

5 导航到软件包目录。

```
cd nsx-lcp-trusty_amd64/
```

6 安装该软件包。

```
sudo dpkg -i *.deb
```

7 重新加载 OVS 内核模块。

```
/etc/init.d/openvswitch-switch force-reload-kmod
```

如果管理程序在 OVS 接口上使用 DHCP，请重新启动用于配置 DHCP 的网络接口。您可以手动停止网络接口上的旧 dhclient 进程，并在该接口上重新启动新 dhclient 进程。

8 要进行验证，可以运行 `dpkg -l | grep nsx` 命令。

```
user@host:~$ dpkg -l | grep nsx

ii  nsx-agent                          <release>     amd64        NSX Agent
ii  nsx-aggservice                     <release>     all          NSX Aggregation Service Lib
ii  nsx-cli                            <release>     all          NSX CLI
ii  nsx-da                             <release>     amd64        NSX Inventory Discovery Agent
ii  nsx-host                           <release>     all          NSX host meta package
ii  nsx-host-node-status-reporter      <release>     amd64        NSX Host Status Reporter for
Aggregation Service
ii  nsx-lldp                           <release>     amd64        NSX LLDP Daemon
ii  nsx-logical-exporter               <release>     amd64        NSX Logical Exporter
ii  nsx-mpa                            <release>     amd64        NSX Management Plane Agent Core
ii  nsx-netcpa                         <release>     amd64        NSX Netcpa
ii  nsx-sfhc                           <release>     amd64        NSX Service Fabric Host
Component
ii  nsx-transport-node-status-reporter  <release>     amd64        NSX Transport Node Status
Reporter
ii  nsxa                               <release>     amd64        NSX L2 Agent
```

任何错误很可能是由不完整的依赖项造成的。`apt-get install -f` 命令可以尝试解决依赖项问题并重新运行 NSX-T Data Center 安装。

后续步骤

将主机添加到 NSX-T Data Center 管理层面。请参见使用 CLI 部署 NSX Manager 节点以形成群集 。

在 RHEL 和 CentOS KVM 管理程序上手动安装 NSX-T Data Center 内核模块

要准备主机以加入 NSX-T Data Center，您可以手动在 RHEL 或 CentOS KVM 主机上安装 NSX-T Data Center 内核模块。

这样，您就可以构建 NSX-T Data Center 控制层面和管理层面结构层。在 RPM 文件中打包的 NSX-T Data Center 内核模块在管理程序内核中运行并提供一些服务，例如，分布式路由、分布式防火墙和桥接功能。

您可以手动下载 NSX-T Data Center RPM 并将其作为主机映像的一部分。请注意，每个 NSX-T Data Center 版本的下载路径可能会有所不同。请务必查看 NSX-T Data Center 下载页面以获取相应的 RPM。

前提条件

能够访问 RHEL 或 CentOS 存储库。

步骤

1 以管理员身份登录到主机。

2 下载 nsx-lcp 文件并将其复制到 /tmp 目录中。

3 解压缩该软件包。

```
tar -zxvf nsx-lcp-<release>-rhel7.4_x86_64.tar.gz
```

4 导航到软件包目录。

```
cd nsx-lcp-rhel74_x86_64/
```

5 安装该软件包。

```
sudo yum install *.rpm
```

运行 yum install 命令时，会解析任何 NSX-T Data Center 依赖项，假定 RHEL 或 CentOS 主机可以访问其各自的存储库。

6 重新加载 OVS 内核模块。

```
/etc/init.d/openvswitch force-reload-kmod
```

如果管理程序在 OVS 接口上使用 DHCP，请重新启动用于配置 DHCP 的网络接口。您可以手动停止网络接口上的旧 dhclient 进程，并在该接口上重新启动新 dhclient 进程。

7 要进行验证，可以运行 `rpm -qa | egrep 'nsx|openvswitch|nicira'` 命令。

在输出中，安装的软件包必须与 nsx-rhel74 或 nsx-centos74 目录中的软件包相匹配。

后续步骤

将主机添加到 NSX-T Data Center 管理层面。请参见使用 CLI 部署 NSX Manager 节点以形成群集 。

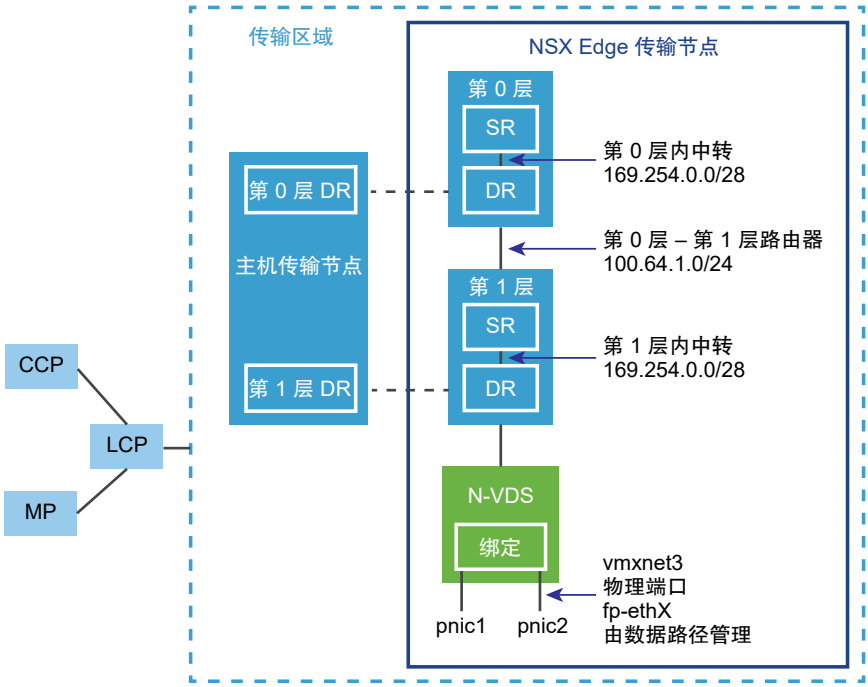
NSX Edge 网络设置

可以使用 ISO、OVA/OVF 或 PXE 启动安装 NSX Edge。无论使用什么安装方法，请确保在安装 NSX Edge 之前准备主机网络。

传输区域中的 NSX Edge 的简要视图

NSX-T Data Center 的简要视图显示传输区域中的两个传输节点。一个传输节点是主机。另一个传输节点是 NSX Edge。

图 8-5. NSX Edge 简要概述



在首次部署 NSX Edge 时，您可以将其视为空容器。在创建逻辑路由器后，NSX Edge 才会执行任何操作。NSX Edge 为 Tier-0 和 Tier-1 逻辑路由器提供计算支持。每个逻辑路由器包含一个服务路由器 (SR) 和一个分布式路由器 (DR)。在我们谈到路由器是分布式路由器时，我们是指在属于同一传输区域的所有传输节点上复制该路由器。在该图中，主机传输节点包含在 Tier-0 和 Tier-1 路由器上包含的同一 DR。如果要配置逻辑路由器以执行服务（如 NAT），则需要使用服务路由器。所有 Tier-0 逻辑路由器都具有服务路由器。如果需要，Tier-1 路由器可以根据设计要求使用服务路由器。

默认情况下，SR 和 DR 之间的链路使用 169.254.0.0/28 子网。在部署 Tier-0 或 Tier-1 逻辑路由器时，将自动创建这些路由器内中转链路。您不需要配置或修改链路配置，除非在您的部署中已使用 169.254.0.0/28 子网。在 Tier-1 逻辑路由器上，只有在创建 Tier-1 逻辑路由器时选择了 NSX Edge 集群，才会使用 SR。

为 Tier-0 到 Tier-1 的连接分配的默认地址空间为 100.64.0.0/10。将在 100.64.0.0/10 地址空间中为每个 Tier-0 到 Tier-1 的对等连接提供一个 /31 子网。在创建 Tier-1 路由器并将其连接到 Tier-0 路由器时，将自动创建该链路。您不需要在该链路上配置或修改接口，除非在您的部署中已使用 100.64.0.0/10 子网。

每个 NSX-T Data Center 部署具有一个管理平面集群 (MP) 和一个控制平面集群 (CCP)。MP 和 CCP 将配置推送到每个传输区域的本地控制平面 (LCP)。在主机或 NSX Edge 加入管理平面时，管理平面代理 (MPA) 将与主机或 NSX Edge 建立连接，并且主机或 NSX Edge 变为 NSX-T Data Center Fabric 节点。然后，在将 Fabric 节点添加为传输节点时，将与主机或 NSX Edge 建立 LCP 连接。

最后，该图显示了绑定在一起以提供高可用性的两个物理网卡（pNIC1 和 pNIC2）的示例。数据路径管理物理网卡。它们可以作为到外部网络的 VLAN 上行链路，或者作为到 NSX-T Data Center 管理的内部虚拟机网络的隧道端点链路。

最佳做法是向部署为虚拟机的每个 NSX Edge 至少分配两个物理链路。或者，也可以在相同 pNIC 上叠加使用不同 VLAN ID 的端口组。找到的第一个网络链路用于管理。例如，在 NSX Edge 虚拟机上，找到的第一个链路可能是 vnic1。在裸机安装上，找到的第一个链路可能是 eth0 或 em0。其余链路用于上行链路和隧道。例如，一个链路可能用于 NSX-T Data Center 管理的虚拟机使用的隧道端点。另一个链路可能用于 NSX Edge 到外部 TOR 的上行链路。

您可以通过以管理员身份登录到 CLI 并运行 `get interfaces` 和 `get physical-ports` 命令来查看 NSX Edge 的物理链路信息。在该 API 中，您可以使用 `GET fabric/nodes/<edge-node-id>/network/interfaces` API 调用。将在下一节中更详细地讨论物理链路。

无论将 NSX Edge 安装为虚拟机设备，还是安装在裸机上，您都可以使用多种方法进行网络配置，具体取决于您的部署。

传输区域和 N-VDS

要了解 NSX Edge 网络，您必须了解有关传输区域和 N-VDS 的内容。传输区域控制 NSX-T Data Center 中的第 2 层网络的范围。N-VDS 是在传输节点上创建的软件交换机。N-VDS 的用途是，将逻辑路由器上行链路和下行链路绑定到物理网卡。对于 NSX Edge 所属的每个传输区域，将在 NSX Edge 上安装单个 N-VDS。

共有两种类型的传输区域：

- 用于传输节点之间内部 NSX-T Data Center 隧道的覆盖网络。
- 用于 NSX-T Data Center 外部上行链路的 VLAN。

NSX Edge 可以属于零个或多个 VLAN 传输区域。对于零个 VLAN 传输区域，NSX Edge 可能仍然具有上行链路，因为 NSX Edge 上行链路可以使用为覆盖网络传输区域安装的相同 N-VDS。如果您希望每个 NSX Edge 仅具有一个 N-VDS，则可以这样做。另一个设计方法是，使 NSX Edge 属于多个 VLAN 传输区域，每个上行链路一个传输区域。

最常见的设计方法是三个传输区域：一个覆盖网络传输区域和两个 VLAN 传输区域（用于冗余的上行链路）。

要将同一 VLAN ID 用于覆盖网络流量的传输网络和 VLAN 流量的其他网络（如 VLAN 上行链路），请在两个不同的 N-VDS（一个用于 VLAN，另一个用于覆盖网络）上配置 ID。

虚拟设备/虚拟机 NSX Edge 网络

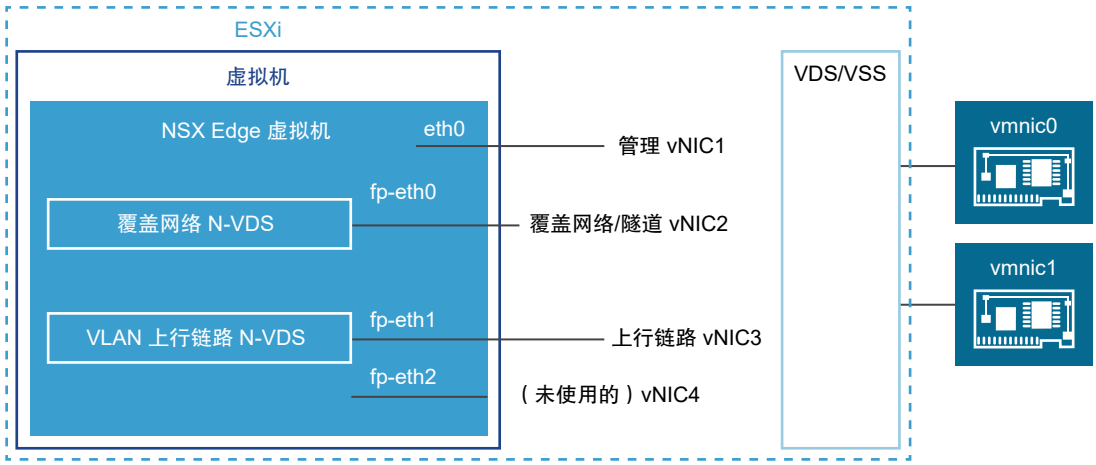
在将 NSX Edge 安装为虚拟设备或虚拟机时，将创建名为 fp-ethX 的内部接口，其中 X 为 0、1、2 和 3。将为到架顶式 (Top-Of-Rack, ToR) 交换机的上行链路和 NSX-T Data Center 覆盖网络隧道分配这些接口。

在创建 NSX Edge 传输节点时，您可以选择 fp-ethX 接口，以便与上行链路和覆盖网络隧道相关联。您可以决定如何使用 fp-ethX 接口。

在 vSphere Distributed Switch 或 vSphere 标准交换机上，您必须为 NSX Edge 分配至少两个 vmnic：一个用于 NSX Edge 管理，一个用于上行链路和隧道。

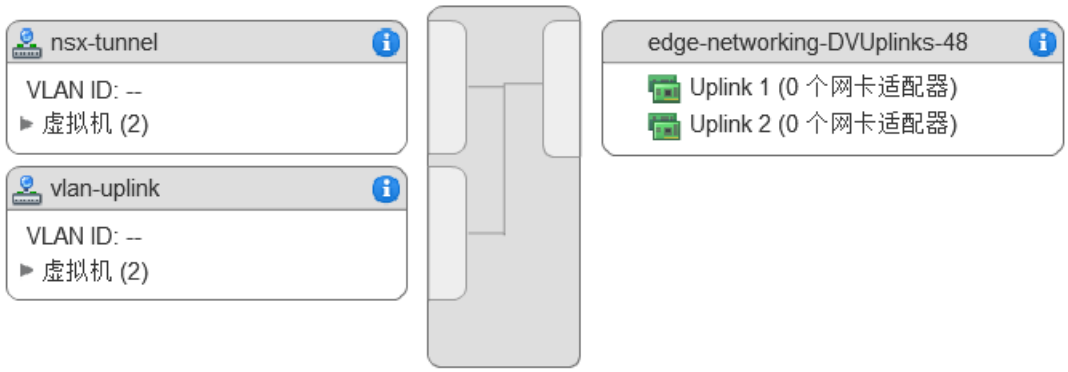
在下面的示例物理拓扑中，fp-eth0 用于 NSX-T Data Center 覆盖网络隧道。fp-eth1 用于 VLAN 上行链路。未使用 fp-eth2 和 fp-eth3。vNIC1 分配给管理网络。

图 8-6. 建议用于 NSX Edge 虚拟机网络的一种链路设置



该示例中显示的 NSX Edge 属于两个传输区域（一个是覆盖网络，另一个是 VLAN），因此，具有两个 N-VDS（一个用于隧道，另一个用于上行链路流量）。

该屏幕截图显示虚拟机端口组 nsx-tunnel 和 vlan-uplink。



在部署期间，您必须指定与在虚拟机端口组上配置的名称匹配的网络名称。例如，如果使用 ovftool 部署 NSX Edge，要与该示例中的虚拟机端口组匹配，网络 ovftool 设置可以如下所示：

```
--net:"Network 0-Mgmt" --net:"Network 1-nsx-tunnel" --net:"Network 2=vlan-uplink"
```

此处显示的示例使用虚拟机端口组名称 Mgmt、nsx-tunnel 和 vlan-uplink。您的虚拟机端口组可以使用任意名称。

为 NSX Edge 配置的隧道和上行链路虚拟机端口组不需要与 VMkernel 端口或给定的 IP 地址相关联。这是因为，它们仅在第 2 层中使用。如果您的部署使用 DHCP 为管理接口提供地址，请确保仅将一个网卡分配给管理网络。

请注意，VLAN 和隧道端口组配置为中继端口。这是必需的。例如，在标准 vSwitch 上，您可以按以下方式配置中继端口：**主机 > 配置 > 网络 > 添加网络 > 虚拟机 > 所有 VLAN ID (4095)**。

如果使用基于设备或虚拟机 NSX Edge，您可以使用标准 vSwitch 或 vSphere Distributed Switch。

可以将 NSX Edge 虚拟机安装在 NSX-T Data Center 已就绪的主机上并将其配置为传输节点。有两种部署类型：

- 使用其中的 VSS/VDS 占用主机上单独 pNIC 的 VSS/VDS 端口组可以部署 NSX Edge 虚拟机。主机传输节点占用在主机上安装的 N-VDS 的单独 pNIC。主机传输节点的 N-VDS 与 VSS 或 VDS（它们占用单独的 pNIC）共存。主机 TEP（隧道端点）和 NSX Edge TEP 可以在相同或不同的子网中。
- 在主机传输节点的 N-VDS 上使用支持 VLAN 的的逻辑交换机可以部署 NSX Edge 虚拟机。主机 TEP 和 NSX Edge TEP 必须在不同的子网中。

或者，也可以在单个主机上安装多个 NSX Edge 设备/虚拟机，所有安装的 NSX Edge 可以使用相同的管理、VLAN 和隧道端点端口组。

在连接了底层物理链路并配置了虚拟机端口组的情况下，您可以安装 NSX Edge。

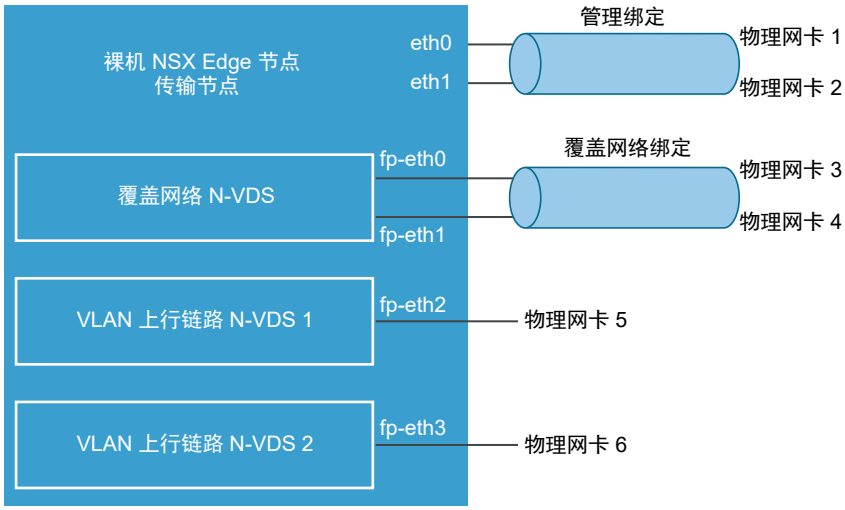
裸机 NSX Edge 网络

裸机 NSX Edge 包含名为 fp-ethX 的内部接口，其中 X 为 0、1、2、3 或 4。创建的 fp-ethX 接口数取决于裸机 NSX Edge 具有多少个物理网卡。最多可以为到架顶式 (ToR) 交换机和 NSX-T Data Center 覆盖网络隧道的上行链路分配其中的 4 个接口。

在创建 NSX Edge 传输节点时，您可以选择 fp-ethX 接口，以便与上行链路和覆盖网络隧道相关联。

您可以决定如何使用 fp-ethX 接口。在下面的示例物理拓扑中，fp-eth0 和 fp-eth1 绑定在一起并用于 NSX-T Data Center 覆盖网络隧道。fp-eth2 和 fp-eth3 用作到 TOR 的冗余 VLAN 上行链路。

图 8-7. 建议用于裸机 NSX Edge 网络的一种链路设置



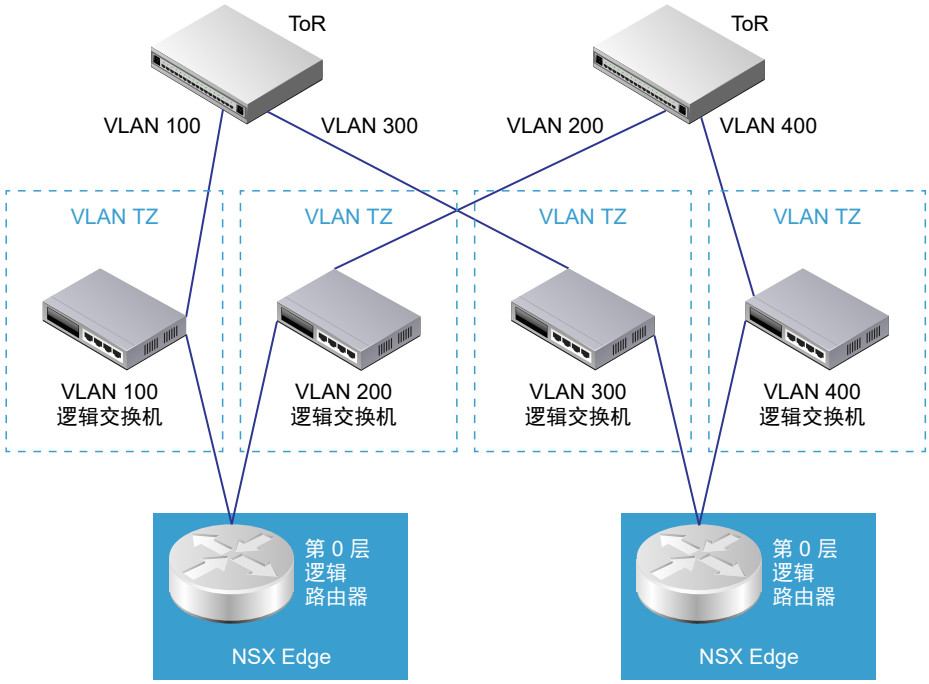
NSX Edge 上行链路冗余

NSX Edge 上行链路冗余允许在 NSX Edge 到外部 TOR 的网络连接上使用两个 VLAN 等价多路径 (Equal-Cost MultiPath, ECMP) 上行链路。

在具有两个 ECMP VLAN 上行链路时，您还必须使用两个 TOR 交换机以实现高可用性和全网格连接。每个 VLAN 逻辑交换机具有一个关联的 VLAN ID。

在将 NSX Edge 添加到 VLAN 传输区域时，将安装新的 N-VDS。例如，如果将 NSX Edge 节点添加到四个 VLAN 传输区域（如图中所示），则会在 NSX Edge 上安装四个 N-VDS。

图 8-8. 建议用于 NSX Edge 到 TOR 的一种 ECMP VLAN 设置



注　对于具有 vSphere Distributed Switch (vDS) 而非 N-VDS 的 ESXi 主机上部署的 Edge 虚拟机，必须执行以下操作：

- 启用伪信号以便 dhcp 工作。
- 启用混杂模式以便 Edge 虚拟机接收未知单播数据包，因为 MAC 学习默认处于禁用状态。vDS 6.6 或更高版本不需要这样做，因为在这些版本中，MAC 学习默认处于启用状态。

创建 NSX Edge 传输节点

可以将 NSX Edge 添加到 NSX-T Data Center Fabric，并继续将 NSX Edge 配置为传输节点。

传输节点是一个可以加入 NSX-T Data Center 覆盖网络或 NSX-T Data Center VLAN 网络的节点。如果任何节点包含 N-VDS，则可以将其作为传输节点。此类节点包括但不限于 NSX Edge。

NSX Edge 可以属于一个覆盖网络传输区域和多个 VLAN 传输区域。如果虚拟机需要访问外界，NSX Edge 必须属于虚拟机的逻辑交换机所属的同一传输区域。通常，NSX Edge 属于至少一个 VLAN 传输区域以提供上行链路访问。

注 如果打算从模板虚拟机中创建传输节点，请确保在主机上的 `/etc/vmware/nsx/` 中没有任何证书。如果证书已存在，则 netcpa 代理不会创建该证书。

前提条件

- 必须配置传输区域。
- 确认配置了计算管理器。请参见添加计算管理器。
- 必须配置一个上行链路配置文件，也可以为裸机 NSX Edge 节点使用默认上行链路配置文件。
- 必须配置一个 IP 池，或者它必须在网络部署中可用。
- 必须在主机或 NSX Edge 节点上具有至少一个未使用的物理网卡。

步骤

1. 从浏览器中，使用管理员权限登录到 https://<nsx-manager-ip-address> 中的 NSX Manager。
2. 选择**系统 > 结构层 > 节点 > Edge 传输节点 > 添加 Edge 虚拟机**。
3. 键入 NSX Edge 的名称。
4. 键入 vCenter Server 的主机名称或 FQDN。
5. 为了获得最佳性能，请为 NSX Edge 设备预留内存。

   将预留内存设置为可确保 NSX Edge 足以高效运行。请参见 NSX Edge 虚拟机系统要求。
6. 为 NSX Edge 指定 CLI 和 root 密码。

   您的密码必须符合密码强度限制。
   - 至少 12 个字符
   - 至少一个小写字母
   - 至少一个大写字母
   - 至少一个数字
   - 至少一个特殊字符
   - 至少 5 个不同的字符
   - 没有字典词语
   - 没有回文
   - 不允许使用超过四个单调字符的序列

7 输入 NSX Edge 详细信息。

选项	说明
计算管理器	从下拉菜单中选择计算管理器。 计算管理器是在管理平面中注册的 vCenter Server。
集群	从下拉菜单中指定 NSX Edge 要加入的集群。
资源池或主机	从下拉菜单中为 NSX Edge 分配资源池或特定主机。
数据存储	从下拉菜单中选择 NSX Edge 文件的数据存储。

8 输入 NSX Edge 接口详细信息。

选项	说明
IP 分配	选择 **DHCP** 或**静态** IP。 如果选择**静态**，您必须指定以逗号分隔的 IP 地址、网关和子网掩码列表。
管理接口	从下拉菜单中选择虚拟机网络接口。

9 选择该传输节点所属的传输区域。

NSX Edge 传输节点属于至少两个传输区域：用于 NSX-T Data Center 连接的覆盖网络以及用于上行链路连接的 VLAN。

注 传输区域中的多个 VTEP 必须配置为相同的网络分段。如果将传输区域中的 VTEP 配置为不同的网络分段，则无法在 VTEP 之间建立 BFD 会话。

10 输入 N-VDS 信息。

选项	说明
Edge 交换机名称	从下拉菜单中选择覆盖网络交换机。
上行链路配置文件	从下拉菜单中选择上行链路配置文件。 可用的上行链路取决于选定的上行链路配置文件中的配置。
IP 分配	为覆盖网络 N-VDS 选择**使用 IP 池**或**使用静态 IP 列表**。 如果选择**使用静态 IP 列表**，您必须指定以逗号分隔的 IP 地址、网关和子网掩码列表。
IP 池	如果您选择**使用 IP 池**进行 IP 分配，请指定 IP 池名称。
数据路径接口	选择上行链路接口的数据路径接口名称。

注 NSX Edge 虚拟机设备不支持 LLDP 配置文件。

11 在**传输节点**页面上查看连接状态。

将 NSX Edge 添加为传输节点后，连接状态将在 10-12 分钟后变为“已启动”。

12 （可选） 使用 `GET https://<nsx-manager>/api/v1/transport-nodes/<transport-node-id>` API 调用查看传输节点。

13 （可选）有关状态信息，请使用 `GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status` API 调用。

后续步骤

将 NSX Edge 节点添加到 NSX Edge 集群。请参见创建 NSX Edge 群集。

创建 NSX Edge 群集

具有多节点 NSX Edge 群集可以帮助确保至少一个 NSX Edge 始终可用。

要使用 NAT、负载平衡器等有状态服务创建 Tier-0 逻辑路由器或 Tier-1 路由器，必须将其与 NSX Edge 群集相关联。因此，即使您只有一个 NSX Edge，它也必须属于 NSX Edge 群集才能使用。

只能将 NSX Edge 传输节点添加到一个 NSX Edge 群集中。

可以使用 NSX Edge 群集支持多个逻辑路由器。

在创建 NSX Edge 群集后，以后可以编辑该群集以添加额外的 NSX Edge。

前提条件

- 安装至少一个 NSX Edge 节点。
- 将 NSX Edge 加入管理层面。
- 将 NSX Edge 添加为传输节点。
- （可选）为高可用性 (HA) 创建 NSX Edge 群集配置文件。也可以使用默认 NSX Edge 群集配置文件。

步骤

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

2 选择**系统 > 结构层 > 节点 > Edge 集群 > 添加**。

3 输入 NSX Edge 群集的名称。

4 从下拉菜单中选择 NSX Edge 群集配置文件。

5 从“成员类型”下拉菜单中选择任一 NSX Edge 节点。

如果虚拟机部署在公有云环境中，请选择“公有云网关节点”，否则，选择“NSX Edge 节点”。

6 从**可用**列中，选择 NSX Edge 并单击右箭头以将其移到**选定**列中。

后续步骤

您现在可以构建逻辑网络拓扑以及配置服务。请参见 NSX-T Data Center 管理指南。

自动部署无状态群集

9

无状态主机不会保留配置，因此，它们需要一个自动部署服务器，以便在主机打开电源时提供所需的启动文件。

本节可帮助您使用 vSphere Auto Deploy 和 NSX-T 传输节点配置文件来设置无状态群集，以使用包含不同版本的 ESXi 和 NSX-T 的新映像配置文件来重新置备主机。为 vSphere Auto Deploy 设置的主机可使用自动部署服务器和 vSphere 主机配置文件来自定义主机。还可以为 NSX-T 传输节点配置文件设置这些主机，以便在主机上配置 NSX-T。

因此，可以为 vSphere Auto Deploy 和 NSX-T 传输节点配置文件设置无状态主机，以使用自定义 ESXi 和 NSX-T 版本来重新置备主机。

本章讨论了以下主题：

自动部署无状态群集的高级别任务

自动部署无状态群集的高级别任务。

设置自动部署无状态群集的高级别任务包括：

1 必备条件和支持的版本。请参见必备条件和支持的版本。

2 （引用主机）创建自定义映像配置文件。请参见为无状态主机创建自定义映像配置文件。

3 （引用主机和目标主机）关联自定义映像配置文件。请参见将自定义映像与引用主机和目标主机相关联。

4 （引用主机）在 ESXi 中设置网络配置。请参见在引用主机上设置网络配置。

5 （引用主机）在 NSX 中配置为传输节点。请参见将引用主机配置为 NSX-T 中的传输节点。

6 （引用主机）提取并验证主机配置文件。请参见提取并验证主机配置文件。

7 （引用主机和目标主机）验证主机配置文件与无状态群集的关联。请参见验证主机配置文件与无状态群集的关联。

8 （引用主机）更新主机自定义。请参见更新主机自定义。

9 （目标主机）触发自动部署。请参见在目标主机上触发自动部署。

   a 应用传输节点配置文件之前。请参见应用 TNP 之前重新引导主机。

   b 应用传输节点配置文件。请参见对无状态群集应用 TNP。

   c 应用传输节点配置文件之后。请参见应用 TNP 后重新引导主机。

10 对主机配置文件和传输节点配置文件进行故障排除。请参见对主机配置文件和传输节点配置文件进行故障排除。

必备条件和支持的版本

必备条件和支持的 ESXi 和 NSX-T 版本。

支持的工作流

- 具有映像配置文件和主机配置文件

必备条件

- 仅支持同类集群（集群内的所有主机必须都是无状态主机或都是有状态主机）。
- 必须启用 Image Builder 服务。
- 必须启用自动部署服务。

支持的 NSX 和 ESXi 版本

支持的 EXSi 版本	ESXi 67ep6	ESXi 67u2	ESXi 67u3	ESXi 67ep7
NSX-T Data Center 2.4	是	是	否	否
NSX-T Data Center 2.4.1	是	是	否	否
NSX-T Data Center 2.4.2	是	是	否	否
NSX-T Data Center 2.4.3	是	是	否	否
NSX-T Data Center 2.5	是	是	是	是

为无状态主机创建自定义映像配置文件

在数据中心内，确定准备用作引用主机的主机。

引用主机首次启动时， ESXi 会将默认规则与引用主机关联。在此过程中，我们将添加自定义映像配置文件（ ESXi 和 NSX VIB），并将引用主机与新的自定义映像关联。包含 NSX-T 映像的映像配置文件可显著缩短安装时间。同一自定义映像可与无状态群集中的多个目标主机相关联。

注 或者，您可以只将一个 ESXi 映像配置文件添加到引用和目标无状态群集。对无状态群集应用传输节点配置文件时，将下载 NSX-T VIB。请参见添加软件库。

前提条件

确保已启用自动部署服务和 Image Builder 服务。请参见使用 vSphere Auto Deploy 重新置备主机。

步骤

1 要导入 NSX-T 软件包，请创建软件库。

2 下载 `nsx-lcp` 软件包。

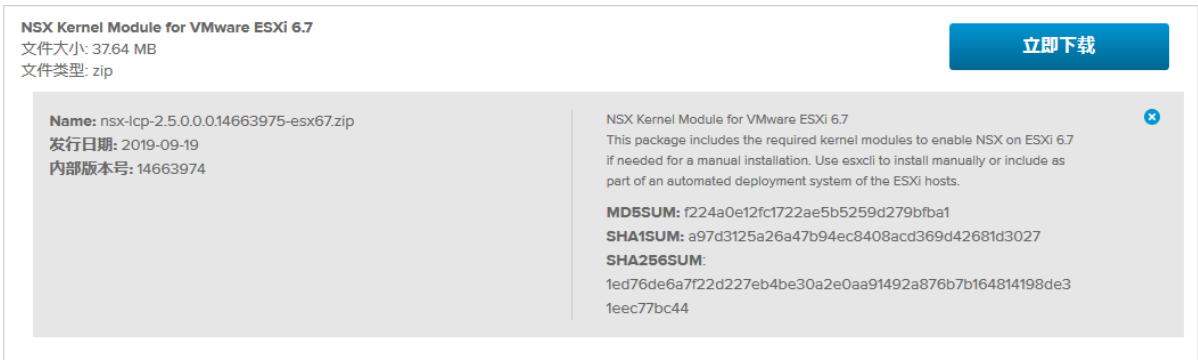
a 登录到 `https://my.vmware.com`。

b 在“下载 VMware NSX-T Data Center”页面上，选择 NSX-T 版本。

c 在“产品下载”页面中，搜索适用于特定 VMware ESXi 版本的 NSX-T 内核模块。

d 单击**立即下载**以开始下载 `nsx-lcp` 软件包。

e 将 `nsx-lcp` 软件包导入到软件库。



3 创建另一个软件库以导入 ESXi 软件包。

vSphere Web Client 将显示引用主机上创建的两个软件库。

4 创建一个自定义软件库以克隆先前导入的 ESXi 映像和 `nsx-lcp` 软件包。

a 从前面步骤中创建的 ESXi 软件库中选择 ESXi 映像配置文件。

b 单击**克隆**。

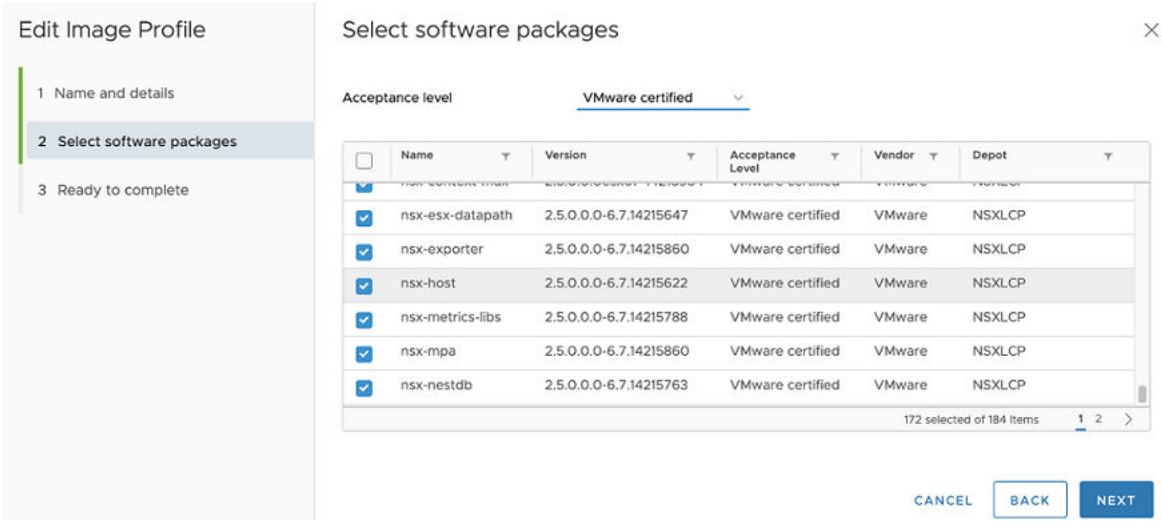
c 在“克隆映像配置文件”向导中，输入要创建的自定义映像的名称。

d 选择自定义软件库，其中克隆映像 (ESXi) 必须可用。

e 在“选择软件包”窗口中，将“接受级别”选择为 **VMware 认证**。已预先选择 ESXi VIB。

f 在软件包列表中手动标识并选择 NSX-T 软件包，然后单击**下一步**。

g 在“即将完成”屏幕中，确认详细信息，然后单击**完成**以在自定义软件库中创建包含 ESXi 和 NSX-T 软件包的克隆映像。



后续步骤

将自定义映像与引用主机和目标主机关联。请参见将自定义映像与引用主机和目标主机相关联。

将自定义映像与引用主机和目标主机相关联

要使用包含“ ESXi 和 NSX 软件包的新自定义映像”启动引用主机和目标主机，请关联该自定义映像配置文件。

此时，该自定义映像仅与引用主机和目标主机相关联，但不会安装 NSX。

重要事项 在引用主机和目标主机上执行此自定义映像关联过程。

前提条件

步骤

1 在 ESXi 主机上，导航到**菜单 > 自动部署 > 已部署的主机**。

2 要将自定义映像配置文件与主机相关联，请选择自定义映像。

3 单击**编辑映像配置文件关联**。

4 在“编辑映像配置文件关联”向导中，单击**浏览**并选择自定义软件库，然后选择自定义映像配置文件。

5 启用**跳过映像配置文件签名检查**。

6 单击**确定**。

结果

后续步骤

在引用主机上设置网络配置。请参见在引用主机上设置网络配置。

在引用主机上设置网络配置

在引用主机上，创建一个具有 VMkernel 适配器的标准交换机，以在 ESXi 上设置网络配置。

此网络配置将在从引用主机提取的主机配置文件中捕获。在无状态部署期间，主机配置文件将在每个目标主机上复制此网络配置设置。

步骤

1 在 ESXi 主机上，通过添加 VMkernel 适配器来配置 vSphere 标准交换机 (vSphere Standard Switch, VSS) 或分布式虚拟交换机 (Distributed Virtual switch, DVS)。

2 确认新添加的 VSS/DVS 交换机显示在“VMkernel 适配器”页面中。

后续步骤

将引用主机配置为 NSX-T 中的传输节点。请参见将引用主机配置为 NSX-T 中的传输节点。

将引用主机配置为 NSX-T 中的传输节点

在将引用主机与自定义映像配置文件相关联并配置了 VSS 交换机后，将引用主机设置为 NSX-T 中的传输节点。

步骤

1 从浏览器中，登录到 https://<NSXManager_IPaddress> 中的 NSX-T。

2 要找到引用主机，请导航到**系统 -> 节点 -> 主机传输节点**。

3 创建 VLAN 传输区域以定义虚拟网络的范围。可通过将 N-VDS 交换机连接到传输区域来定义该范围。根据此连接，N-VDS 可以访问传输区域内定义的分段。请参见创建传输区域。

4 在传输区域中创建 VLAN 分段。创建的分段将显示为逻辑交换机。

   a 导航到**网络 -> 分段**。

   b 选择要连接分段的传输区域。

   c 输入 VLAN ID。

   d 单击**保存**。

5 为引用主机创建上行链路配置文件，以定义 N-VDS 连接到物理网络的方式。请参见创建上行链路配置文件。

6 将引用主机配置为传输节点请参见配置受管主机传输节点。

   a 在“主机传输节点”页面中，选择引用主机。

   b 单击“配置 NSX”，然后选择之前创建的传输区域、N-VDS 和上行链路配置文件。

7 在“用于安装的网络映射”部分中，单击**添加映射**以添加 VMkernel 到分段/逻辑交换机的映射。

8 单击**完成**，开始在引用主机上安装 NSX-T。

在安装过程中，VMkernel 适配器和物理网卡将从 VSS 或 DVS 交换机迁移到 N-VDS 交换机。安装后，引用主机的配置状态将显示为成功。

注 引用主机将在“其他主机”下列出。

9 在 vCenter Server 中，请确认 VSS 交换机上的 PNIC 和 VMkernel 适配器已经迁移，并且已连接到 N-VDS 交换机。

后续步骤

提取并验证主机配置文件。请参见提取并验证主机配置文件。

提取并验证主机配置文件

从引用主机提取主机配置文件后，请验证在主机配置文件中提取的 NSX-T 配置。它包含应用于目标主机的 ESXi 和 NSX-T 配置。

步骤

1 要提取主机配置文件，请从引用主机提取并配置主机配置文件。

2 验证提取的主机配置文件中的 NSX 配置。

结果

主机配置文件包含与 ESXi 和 NSX 相关的配置，因为主机是为这两种环境准备的。

后续步骤

验证主机配置文件与无状态群集的关联。请参见验证主机配置文件与无状态群集的关联。

验证主机配置文件与无状态群集的关联

要使用 ESXi 和 NSX 配置准备目标无状态群集，请将从引用主机提取的主机配置文件与目标无状态群集关联。

如果没有与无状态群集关联的主机配置文件，则无法使用 ESXi 和 NSX VIB 自动部署加入群集的新节点。

步骤

1 将主机配置文件与无状态群集连接或断开连接。请参见在主机配置文件中附加或分离实体。

2 在“已部署的主机”选项卡中，确认现有无状态主机已与正确的映像关联，并与主机配置文件关联。

3 如果缺少主机配置文件关联，请选择目标主机，然后单击“修复主机关联”以强制将映像和主机配置文件更新到目标主机。

后续步骤

更新主机自定义。请参见更新主机自定义。

更新主机自定义

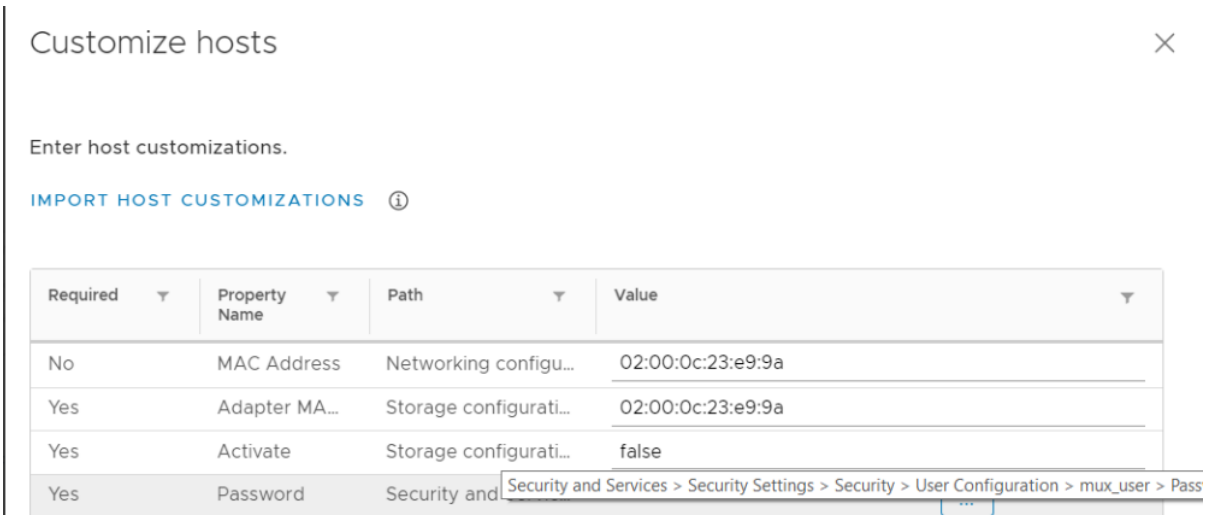
将主机配置文件连接到目标群集后，可能需要在主机上添加其他自定义条目，才能成功自动部署 ESXi 和 NSX-T 软件包。

步骤

1 将主机配置文件连接到目标群集后，如果未使用自定义值对主机进行更新，则系统将显示以下消息。

2 要更新主机自定义，请导航到主机配置文件，单击**操作 -> 编辑主机自定义**。

3 对于 ESXi 版本 67ep6、67ep7、67u2，请输入 MUX 用户密码。



4 确认所有必填字段均已使用相应的值进行了更新。

后续步骤

在目标主机上触发自动部署。请参见在目标主机上触发自动部署。

在目标主机上触发自动部署

将新节点添加到群集时，需要手动重新引导该节点，以便配置 ESXi 和 NSX-T VIB。

注 仅适用于无状态主机。

可通过两种方法来准备主机以触发自动部署要配置的 ESXi 和 NSX-T VIB 的过程。

- 将 TNP 应用到无状态群集之前重新引导主机。
- 将 TNP 应用到无状态群集之后重新引导主机。

如果要在主机上安装 NSX-T 时迁移 VMkernel 适配器，请参见：

- 无状态主机位于目标群集时的场景
- 无状态主机不在目标群集中时的场景

后续步骤

将 TNP 应用到无状态群集之前重新引导主机。请参见应用 TNP 之前重新引导主机。

应用 TNP 之前重新引导主机

仅适用于无状态主机。在此场景中，传输节点配置文件不会应用于无状态群集，这意味着不会在目标主机上安装和配置 NSX-T。

步骤

1 重新引导主机。

使用 ESXi 映像启动目标主机。启动后，目标主机将一直处于维护模式，直到将 TNP 配置文件应用于目标主机并且 NSX-T 安装完成为止。配置文件将按以下顺序应用于主机：

配置文件将按以下顺序应用于主机。

- 将映像配置文件应用于主机。
- 将主机配置文件配置应用于主机。
- 将 NSX-T 配置应用于主机。

2 在 ESXi 主机上，VMkernel 适配器连接到一个名为 <N-LogicalSegment> 的临时分段，因为该主机还不是传输节点。安装 NSX-T 后，临时交换机将替换为实际的 N-VDS 交换机和逻辑分段。

将 ESXi VIB 应用于所有重新引导的主机。 ESXi 主机中的临时 NSX 交换机。将 TNP 应用于主机后，临时交换机将替换为实际的 NSX-T 交换机。

后续步骤

将 TNP 应用于无状态群集。请参见对无状态群集应用 TNP。

对无状态群集应用 TNP

只有在将 TNP 应用于群集时，才会在目标主机上进行 NSX-T 配置和安装。

步骤

1 请记下从引用主机的主机配置文件中提取的设置。TNP 配置文件中的相应实体必须具有相同的值。例如，主机配置文件和 TNP 中使用的 N-VDS 名称必须相同。

有关提取的主机配置文件设置的更多信息，请参见提取并验证主机配置文件。

2 添加 TNP。请参见添加传输节点配置文件。

3 请确保新的 TNP 配置文件和现有的主机配置文件中以下参数的值相同。

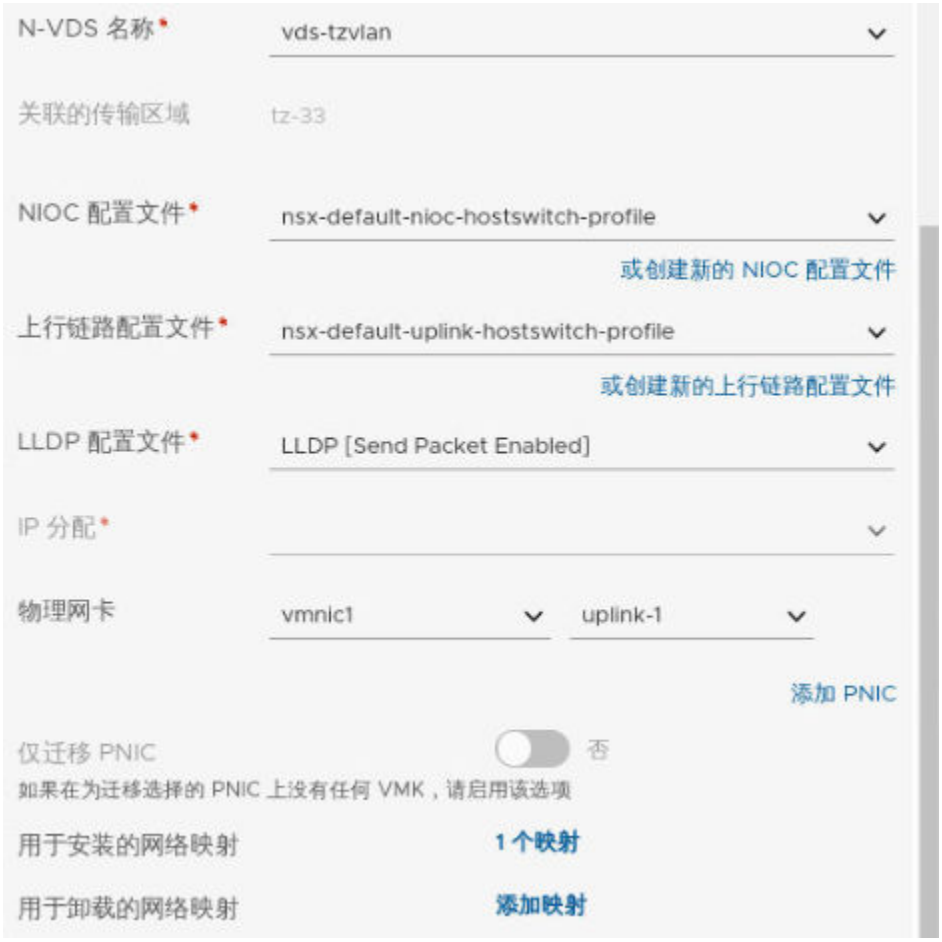
- N-VDS 名称：确保主机配置文件和 TNP 中引用的 N-VDS 名称相同。
- 上行链路配置文件：确保主机配置文件和 TNP 中引用的上行链路配置文件相同。
- PNIC：在将物理网卡映射到上行链路配置文件时，请先验证主机配置文件中使用的网卡，然后再将该物理网卡映射到上行链路配置文件。
- 用于安装的网络映射：在安装期间映射网络时，请先验证主机配置文件上 VMkernel 到分段的映射，然后在 TNP 中添加相同的映射。
- 用于卸载的网络映射：在卸载期间映射网络时，请先验证主机配置文件上 VMkernel 到 VSS/DVS 交换机的映射，然后在 TNP 中添加相同的映射。

4 通过输入所有必填字段来添加 TNP。请参见添加传输节点配置文件。

请确保新的 TNP 配置文件和现有的主机配置文件中以下参数的值相同。

- 传输区域：确保主机配置文件和 TNP 中引用的传输区域相同。
- N-VDS 名称：确保主机配置文件和 TNP 中引用的 N-VDS 名称相同。

- 上行链路配置文件：确保主机配置文件和 TNP 中引用的上行链路配置文件相同。
- PNIC：在将物理网卡映射到上行链路配置文件时，请先验证主机配置文件中使用的网卡，然后再将该物理网卡映射到上行链路配置文件。
- 用于安装的网络映射：在安装期间映射网络时，请先验证主机配置文件上 VMkernel 到逻辑交换机的映射，然后在 TNP 中添加相同的映射。
- 用于卸载的网络映射：在卸载期间映射网络时，请先验证主机配置文件上 VMkernel 到 VSS/DVS 交换机的映射，然后在 TNP 中添加相同的映射。



对目标节点应用 TNP 后，如果 TNP 配置与主机配置文件配置不匹配，则节点可能会因为合规性错误而无法启动。

5 确认已成功创建 TNP 配置文件。

6 将 TNP 配置文件应用于目标群集，然后单击**保存**。

7 确认 TNP 配置文件已成功应用于目标群集。这意味着已在群集的所有节点上成功配置 NSX。

8 在 vSphere 中，确认物理网卡或 VMkernel 适配器已连接到 N-VDS 交换机。

9 在 NSX 中，确认已将 ESXi 主机成功配置为传输节点。

后续步骤

或者，可以在将 TNP 应用于群集后重新引导目标主机。请参见应用 TNP 后重新引导主机。

应用 TNP 后重新引导主机

仅适用于无状态主机。将新节点添加到群集时，请手动重新引导节点，以便在该节点上配置 ESXi 和 NSX-T 软件包。

步骤

1 将 TNP 应用于已准备好主机配置文件的无状态群集。请参见创建 TNP 并将其应用于无状态群集。

2 重新引导主机

将 TNP 配置文件应用到无状态群集后，在重新引导加入群集的任何新节点时，将在主机上自动为该节点配置 NSX-T。

后续步骤

确保重新引导加入群集的任何新节点，以在重新引导的节点上自动部署并配置 ESXi 和 NSX-T。

要对在配置自动部署时出现的与主机配置文件和传输节点配置文件相关的问题进行故障排除，请参见对主机配置文件和传输节点配置文件进行故障排除。

无状态主机位于目标群集时的场景

本节讨论无状态主机存在于目标群集中时的用例。

重要事项 在无状态目标主机上：

- NSX-T 2.4 和 NSX-T 2.4.1 不支持将 vmk0 适配器从 VSS/DVS 迁移到 N-VDS。
- NSX-T 2.5 支持将 vmk0 适配器从 VSS/DVS 迁移到 N-VDS。

目标主机	引用主机配置	自动部署目标主机的步骤
目标主机已配置了 vmk0 适配器。	从引用主机提取的主机配置文件在 N-VDS 交换机上配置了 vmk0。 在 NSX-T 中，TNP 只配置了 vmk0 迁移映射。	1 将主机配置文件连接到目标主机。 将 vmk0 适配器连接到 vSwitch。 2 根据需要更新主机自定义。 3 重新引导主机。将主机配置文件应用于主机。将 vmk0 连接到临时交换机。 4 应用 TNP。 vmk0 适配器将迁移到 N-VDS。 已使用 ESXi 和 NSX-T VIB 成功部署了目标主机。
目标主机已配置了 vmk0 适配器。	从引用主机提取的主机配置文件在 vSwitch 上配置了 vmk0，在 N-VDS 交换机上配置了 vmk1。 在 NSX-T 中，TNP 只配置了 vmk1 迁移映射。	1 将主机配置文件连接到目标主机。 已将 vmk0 适配器连接到 vSwitch，但未在任何交换机上实现 vmk1。 2 根据需要更新主机自定义。 3 重新引导主机。 vmk0 将连接到 vSwitch，并且 vmk1 将连接到临时 NSX 交换机。 4 应用 TNP。 vmk1 适配器将迁移到 N-VDS。 5 （可选）如果主机保持与主机配置文件不兼容，请重新引导主机以使主机合规。 已使用 ESXi 和 NSX-T VIB 成功部署了目标主机。
目标主机已配置了 vmk0 适配器。	从引用主机提取的主机配置文件在 vSwitch 上配置了 vmk0，在 N-VDS 交换机上配置了 vmk1。 在 NSX-T 中，TNP 配置了 vmk0 和 vmk1 迁移映射。	1 将主机配置文件连接到目标主机。 已将 vmk0 适配器连接到 vSwitch，但未在任何交换机上实现 vmk1。 2 根据需要更新主机自定义。 3 重新引导主机。 vmk0 适配器将连接到 vSwitch，并且 vmk1 将连接到临时 NSX 交换机。 4 应用 TNP。 5 （可选）如果主机保持与主机配置文件不兼容，请重新引导主机以使主机合规。 已使用 ESXi 和 NSX-T VIB 成功部署了目标主机。

目标主机	引用主机配置	自动部署目标主机的步骤
目标主机已配置了 vmk0 和 vmk1 适配器。	从引用主机提取的主机配置文件在 vSwitch 上配置了 vmk0，并且在 N-VDS 交换机上配置了 vmk1。 在 NSX-T 中，TNP 配置了 vmk1 迁移映射。	1 将主机配置文件连接到目标主机。 vmk0 和 vmk1 适配器将连接到 vSwitch。 2 根据需要更新主机自定义。 3 重新引导主机。 4 应用 TNP。 vmk0 适配器将连接到 vSwitch，并且 vmk1 将连接到 N-VDS 交换机。 5 （可选）如果主机保持与主机配置文件不兼容，请重新引导主机以使主机合规。 已使用 ESXi 和 NSX-T VIB 成功部署了目标主机。
目标主机已配置了 vmk0 和 vmk1 适配器。	从引用主机提取的主机配置文件在 N-VDS 交换机上配置了 vmk0 和 vmk1。 在 NSX-T 中，TNP 配置了 vmk0 和 vmk1 迁移映射。	1 将主机配置文件连接到目标主机。 vmk0 和 vmk1 适配器将连接到 vSwitch。 2 根据需要更新主机自定义。 3 重新引导主机。 4 应用 TNP。 vmk0 和 vmk1 将迁移到 N-VDS 交换机。 已使用 ESXi 和 NSX-T VIB 成功部署了目标主机。

无状态主机不在目标群集中时的场景

本节讨论无状态主机不在目标群集中时的用例。

重要事项 在无状态主机上：

- NSX-T 2.4 和 NSX-T 2.4.1 不支持将 vmk0 适配器从 VSS/DVS 迁移到 N-VDS。
- NSX-T 2.5 支持将 vmk0 适配器从 VSS/DVS 迁移到 N-VDS。

。

目标主机状态	引用主机配置	自动部署目标主机的步骤
主机处于电源关闭状态（首次启动时）。稍后会将其添加到群集中。 为目标群集配置默认的自动部署规则，并将其与主机配置文件关联。 对群集应用 TNP。	从引用主机提取的主机配置文件在 vSwitch 上配置了 VMkernel 适配器 0 (vmk0)，并且在 N-VDS 交换机上配置了 VMkernel 适配器 1 (vmk1)。 在 NSX-T 中，TNP 只配置了 vmk1 迁移映射。	1 打开该主机电源。 打开主机电源后。 ■ 主机会添加到群集。 ■ 将主机配置文件应用于目标主机。 ■ vmk0 适配器位于 vSwitch 上，而 vmk1 适配器位于临时交换机上。 ■ 触发 TNP。 ■ 将 TNP 应用于群集后，vmk0 适配器将位于 vSwitch 上，而 vmk1 将被迁移到 N-VDS 交换机。 2 （可选）如果主机保持与主机配置文件不兼容，请重新引导主机以使主机合规。 已使用 ESXi 和 NSX-T VIB 成功部署了主机。
主机处于电源关闭状态（首次启动时）。稍后会将其添加到群集中。 为目标群集配置默认的自动部署规则，并将其与主机配置文件关联。 对群集应用 TNP。	从引用主机提取的主机配置文件在 N-VDS 交换机上配置了 VMkernel 适配器 0 (vmk0) 和 VMkernel 适配器 1 (vmk1)。 在 NSX-T 中，TNP 配置了 vmk0 和 vmk1 迁移。	1 打开该主机电源。 打开主机电源后。 ■ 主机会添加到群集。 ■ 将主机配置文件应用于目标主机。 ■ vmk0 和 vmk1 适配器位于临时交换机上。 ■ 触发 TNP。 ■ 将 TNP 应用于群集后，vmk0 和 vmk1 将被迁移到 N-VDS 交换机。 已使用 ESXi 和 NSX-T VIB 成功部署了主机。
主机处于电源打开状态。稍后会将其添加到群集中。 为目标群集配置默认的自动部署规则，并将其与主机配置文件关联。 目标主机上只配置了 vmk0 适配器。	从引用主机提取的主机配置文件在 vSwitch 上配置了 VMkernel 适配器 0 (vmk0)，并且在 N-VDS 交换机上配置了 VMkernel 适配器 1 (vmk1)。 在 NSX-T 中，TNP 配置了 vmk1 迁移映射。	1 移动主机，使其成为群集的一部分。 2 重新引导主机。 重新引导主机后，主机配置文件将应用于目标主机。 ■ vmk0 适配器将连接到 vSwitch，而 vmk1 适配器将连接到临时 NSX 交换机。 ■ 触发 TNP。 ■ vmk1 将被迁移到 N-VDS 交换机。 3 （可选）如果主机保持与主机配置文件不兼容，请重新引导主机以使主机合规。 已使用 ESXi 和 NSX-T VIB 成功部署了主机。
主机处于电源打开状态。稍后会将其添加到群集中。 为目标群集配置默认的自动部署规则，并将其与主机配置文件关联。 目标主机上只配置了 vmk0 适配器。	从引用主机提取的主机配置文件在 N-VDS 上配置了 VMkernel 适配器 0 (vmk0) 和 VMkernel 适配器 1 (vmk1)。 在 NSX-T 中，TNP 配置了 vmk0 和 vmk1 迁移。	1 移动主机，使其成为群集的一部分。 2 重新引导主机。 重新引导主机后，主机配置文件将应用于目标主机。 ■ vmk0 和 vmk1 适配器将连接到临时 NSX 交换机。 ■ 触发 TNP。 ■ vmk0 和 vmk1 将连接到 N-VDS 交换机。 已使用 ESXi 和 NSX-T VIB 成功部署了主机。

目标主机状态	引用主机配置	自动部署目标主机的步骤
主机处于电源打开状态。稍后会将其添加到群集中。 为目标群集配置默认的自动部署规则，并将其与主机配置文件关联。 目标主机已配置了 vmk0 和 vmk1 网络映射。	从引用主机提取的主机配置文件在 vSwitch 上配置了 VMkernel 适配器 0 (vmk0)，并且在 N-VDS 交换机上配置了 VMkernel 适配器 1 (vmk1)。 在 NSX-T 中，TNP 配置了 vmk1 迁移。	1 移动主机，使其成为群集的一部分。 2 重新引导主机。 重新引导主机后，主机配置文件将应用于目标主机。 ■ Vmk0 适配器将连接到 vSwitch，而 vmk1 适配器将连接到临时 NSX 交换机。 ■ 触发 TNP。 ■ vmk1 将被迁移到 N-VDS 交换机。 3 （可选）如果主机保持与主机配置文件不兼容，请重新引导主机以使主机合规。 已使用 ESXi 和 NSX-T VIB 成功部署了主机。
主机处于电源打开状态。稍后会将其添加到群集中。 为目标群集配置默认的自动部署规则，并将其与主机配置文件关联。 主机已配置了 vmk0 和 vmk1 网络映射。	在引用主机中，主机配置文件在 N-VDS 交换机上配置了 VMkernel 适配器 0 (vmk0) 和 VMkernel 适配器 1 (vmk1)。 在 NSX-T 中，TNP 配置了 vmk0 和 vmk1 迁移。	1 移动主机，使其成为群集的一部分。 2 重新引导主机。 重新引导主机后，主机配置文件将应用于目标主机。 ■ vmk0 和 vmk1 适配器将连接到临时 NSX 交换机。 ■ 触发 TNP。 ■ vmk0 和 vmk1 适配器将迁移到 N-VDS 交换机。 已使用 ESXi 和 NSX-T VIB 成功部署了主机。

对主机配置文件和传输节点配置文件进行故障排除

对使用主机配置文件和 TNP 自动部署无状态群集时它们存在的问题进行故障排除。

场景	说明
主机配置文件不可移植。	问题：任何 vCenter Server 都不能使用包含 NSX-T 配置的主机配置文件。 解决办法：无。
自动部署规则引擎	问题：无法在自动部署规则中使用主机配置文件来部署新群集。如果部署了新群集，则主机将使用基本网络连接进行部署，并将保持维护模式。 解决办法：从 NSX-T GUI 中准备每个群集。请参见对无状态群集应用 TNP。
检查合规性错误。	问题：主机配置文件修复无法修复与 NSX-T 配置相关的合规性错误。 ■ 主机配置文件和 TNP 上配置的物理网卡不同。 ■ vNIC 到 LS 映射之间的映射。主机配置文件发现逻辑交换机中到 vNIC 的映射与 TNP 配置文件不匹配。 ■ 主机配置文件和 TNP 上连接到 N-VDS 的 VMkernel 不匹配。 ■ 主机配置文件和 TNP 上的 Opaque 交换机不匹配。 解决办法：确保主机配置文件和 TNP 上的 NSX-T 配置匹配。重新引导主机以实现配置更改。主机将启动。

场景	说明
修复	问题：如果存在任何 NSX-T 特定的合规性错误，则会阻止该群集上的主机配置文件修复。 配置不正确： ■ vNIC 到 LS 映射之间的映射 ■ 物理网卡的映射 解决办法：确保主机配置文件和 TNP 上的 NSX-T 配置匹配。重新引导主机以实现配置更改。主机将启动。
连接	问题：在配置了 NSX-T 的群集中，无法在主机级别连接主机配置文件。 解决办法：无。
断开连接	问题：在配置了 NSX-T 的群集中断开连接和连接新的主机配置文件时，不会移除 NSX-T 配置。即使群集与新连接的主机配置文件兼容，它仍会包含先前配置文件中的 NSX-T 配置。 解决办法：无。
更新	问题：如果用户更改了群集中的 NSX-T 配置，则会提取新的主机配置文件。对于丢失的所有设置，需要手动更新主机配置文件。 解决办法：无。
主机级别的传输节点配置	问题：自动部署 anportsport 节点后，它将充当单个实体。对该传输节点的任何更新都可能与 TNP 不匹配。 解决办法：更新群集。独立传输节点中的任何更新都无法保留其迁移规范。迁移可能无法发布重新引导。
无法应用主机配置文件，因为 mux_user 密码策略和密码未重置。	问题：仅在运行 vSphere 6.7 U3 之前版本的主机上出现此问题。主机上的主机修复和主机配置文件应用程序可能会失败，除非重置 **mux_user** 密码。 解决办法：在“策略和配置文件”下，编辑主机配置文件以修改 mux_user 密码策略并重置 **mux_user** 密码。
选定用于迁移到 NVDS 交换机的 VMkernel 适配器不支持 PeerDNS 配置。	问题：如果选定用于迁移到 NVDS 的 VMkernel 适配器启用对等 DNS，则主机配置文件应用程序会失败。 解决办法：通过在必须迁移到 NVDS 交换机的 VMkernel 适配器上禁用对等 DNS 设置，编辑提取的主机配置文件。或者，确保不要将启用了对等 DNS 的 VMkernel 适配器迁移到 NVDS 交换机。
不会保留 VMkernel 网卡地址的 DHCP 地址	问题：如果引用主机是有状态主机，则对于使用从有状态引用主机提取的配置文件的任何无状态主机，都无法保留其源自 PXE 启动的 MAC 的 VMkernel 管理 MAC 地址。这会导致 DHCP 寻址问题。 解决办法：编辑从有状态主机提取的主机配置文件，并将“**确定应如何决定 vmknic 的 MAC 地址**”修改为“**使用 PXE 用于启动系统的 MAC 地址**”。
vCenter 中的主机配置文件应用程序故障可能会导致主机上出现 NSX 配置错误。	问题：如果 vCenter 中的主机配置文件应用程序出现故障，则 NSX 配置可能也会失败。 解决办法：在 vCenter 中，确认已成功应用主机配置文件。修复错误，然后重试
无状态 ESXi 主机不支持 LAG。	问题：由 vCenter Server 管理或者在 NSX 中管理的无状态 ESXi 主机不支持配置为 NSX 中 LAG 的上行链路配置文件。 解决办法：无。

从主机传输节点中卸载 NSX-T Data Center

10

从主机传输节点中卸载 NSX-T Data Center 的步骤因主机类型和主机配置方式而异。

- 验证用于卸载的主机网络映射

  从 ESXi 主机中卸载 NSX-T Data Center 之前，请确认您已配置用于卸载的相应网络映射。如果 ESXi 主机具有已连接到 N-VDS 的 VMkernel 接口，则需要该映射。

- 从 vSphere 集群中卸载 NSX-T Data Center

  如果您使用传输节点配置文件在 vSphere 集群上安装了 NSX-T Data Center，则可以按照以下说明从该集群内的所有主机中卸载 NSX-T Data Center。

- 从 vSphere 集群内的主机中卸载 NSX-T Data Center

  您可以从由 vCenter Server 管理的单个主机中卸载 NSX-T Data Center。集群内的其他主机将不受影响。

- 从独立主机中卸载 NSX-T Data Center

  您可以从独立主机中卸载 NSX-T Data Center。独立主机可以是 ESXi 或 KVM。

验证用于卸载的主机网络映射

从 ESXi 主机中卸载 NSX-T Data Center 之前，请确认您已配置用于卸载的相应网络映射。如果 ESXi 主机具有已连接到 N-VDS 的 VMkernel 接口，则需要该映射。

卸载映射确定卸载后接口所连接到的位置。物理接口 (vmnicX) 和 VMkernel 接口 (vmkX) 都有卸载映射。卸载时，VMkernel 接口将从其当前连接移到在卸载映射中指定的端口组。如果卸载映射中包含物理接口，则物理接口将根据 VMkernel 接口的目标端口组，连接到相应的 vSphere 分布式交换机或 vSphere 标准交换机。

小心 如果物理接口或 VMkernel 接口已连接到 N-VDS，则从 ESXi 主机中卸载 NSX-T Data Center 会具有破坏性。如果主机或集群加入其他应用程序（如 vSAN），则这些应用程序可能会受到卸载的影响。

您可以在两个位置配置用于卸载的网络映射。

- 在应用于该主机的传输节点配置中。
- 在传输节点配置文件配置（随后可将该配置应用于集群）中。

  注 必须将计算管理器配置为将传输节点配置文件应用于集群。

如果配置了计算管理器，则主机可以同时具有传输节点配置和传输节点配置文件配置。如果两者都存在，则传输节点配置将处于活动状态。请确认在活动的配置中正确配置了用于卸载的网络映射。

在此示例中，对集群 cluster-1 应用了传输节点配置文件 TNP-1。主机 tn-1 显示“配置不匹配 (Configuration Mismatch)”。此不匹配消息表示对 tn-1 应用了不同的配置。不匹配问题会持续存在，直到传输节点配置与传输节点配置文件配置相匹配为止。传输节点 tn-2 使用传输节点配置文件中的网络映射，而传输节点 tn-1 则使用其自身的配置。

前提条件

- 确认您已配置要在卸载映射中使用的相应端口组。您必须使用 vSphere 分布式交换机临时端口组或 vSphere 标准交换机端口组。
- 如果要在独立 ESXi 主机的卸载映射中使用 vSphere 分布式交换机端口组，则配置计算管理器。请参见添加计算管理器。如果未配置任何计算管理器，则必须使用 vSphere 标准交换机端口组。

步骤

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

2 选择**系统 > 结构层 > 节点 > 主机传输节点**。

3 对于要卸载的每个主机，验证用于卸载的网络映射中是否为 N-VDS 上的每个 VMkernel 接口都包含一个端口组。添加任何缺少的映射。

重要事项 用于卸载的网络映射中的端口组必须是 vSphere 分布式交换机临时端口组或 vSphere 标准交换机端口组。

a 要查看 VMkernel 接口，请登录 vCenter Server，选择主机，然后单击**配置 > VMkernel 适配器**。

b 如果传输节点配置为活动配置，请选择主机，然后单击**编辑**（对于独立主机）或**配置 NSX**（对于受管主机）。单击**下一步**，然后单击**用于卸载的网络映射**。查看 **VMKNic 映射**和**物理网卡映射**选项卡中的映射。

c 如果传输节点配置文件为活动配置，请单击 **NSX 配置**列中集群的传输节点配置文件的名称，然后单击**编辑**。在 **N-VDS** 选项卡中，单击**用于卸载的网络映射**。查看 **VMKNic 映射**和**物理网卡映射**选项卡中的映射。

从 vSphere 集群中卸载 NSX-T Data Center

如果您使用传输节点配置文件在 vSphere 集群上安装了 NSX-T Data Center，则可以按照以下说明从该集群内的所有主机中卸载 NSX-T Data Center。

有关传输节点配置文件的详细信息，请参见添加传输节点配置文件。

小心 如果物理接口或 VMkernel 接口已连接到 N-VDS，则从 ESXi 主机中卸载 NSX-T Data Center 会具有破坏性。如果主机或集群加入其他应用程序（如 vSAN），则这些应用程序可能会受到卸载的影响。

如果您未使用传输节点配置文件安装 NSX-T Data Center，或者如果您要从集群内的部分主机中移除 NSX-T Data Center，请参见从 vSphere 集群内的主机中卸载 NSX-T Data Center。

注 从集群中移除主机不会卸载 NSX-T Data Center。请按照以下说明从集群内的主机中卸载 NSX-T Data Center：从 vSphere 集群内的主机中卸载 NSX-T Data Center。

前提条件

- 确认要卸载的主机已配置网络卸载映射。请参见验证用于卸载的主机网络映射。
- 确认要卸载的主机在 vSphere 中处于维护模式。

步骤

1. 从浏览器中，使用管理员权限登录到 https://<nsx-manager-ip-address> 中的 NSX Manager。
2. 选择**系统 > 结构层 > 节点 > 主机传输节点**。
3. 从**托管主体**下拉菜单中，选择 vCenter Server。
4. 选择要卸载的集群，然后单击**移除 NSX**。
5. 确认已从主机中移除 NSX-T Data Center 软件。
   a. 以 root 用户身份登录到主机的命令行界面。
   b. 运行以下命令以检查 NSX-T Data Center VIB

   ```
   esxcli software vib list | grep -E 'nsx|vsipfwlib'
   ```

   如果 NSX-T Data Center 软件已成功移除，则不会列出任何 VIB。如果主机上仍留有任何 NSX VIB，请联系 VMware 技术支持团队。

从 vSphere 集群内的主机中卸载 NSX-T Data Center

您可以从由 vCenter Server 管理的单个主机中卸载 NSX-T Data Center。集群内的其他主机将不受影响。

小心 如果物理接口或 VMkernel 接口已连接到 N-VDS，则从 ESXi 主机中卸载 NSX-T Data Center 会具有破坏性。如果主机或集群加入其他应用程序（如 vSAN），则这些应用程序可能会受到卸载的影响。

前提条件

- 确认要卸载的主机已配置网络卸载映射。请参见验证用于卸载的主机网络映射。
- 确认要卸载的主机在 vSphere 中处于维护模式。

步骤

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

2 选择**系统 > 结构层 > 节点 > 主机传输节点**。

3 从**托管主体**下拉菜单中，选择 vCenter Server。

4 如果集群应用了传输节点配置文件，请选择该集群，然后单击**操作 > 断开连接 TN 配置文件**。

如果集群应用了传输节点配置文件，该集群对应的 **NSX 配置**列会显示配置文件名称。

5 选择主机，然后单击**移除 NSX**。

6 确认已从主机中移除 NSX-T Data Center 软件。

a 以 root 用户身份登录到主机的命令行界面。

b 运行以下命令以检查 NSX-T Data Center VIB

```
esxcli software vib list | grep -E 'nsx|vsipfwlib'
```

如果 NSX-T Data Center 软件已成功移除，则不会列出任何 VIB。如果主机上仍留有任何 NSX VIB，请联系 VMware 技术支持团队。

7 如果集群应用了传输节点配置文件，并且您想要重新应用该配置文件，请选择该集群，单击**配置 NSX**，然后从**选择部署配置文件**下拉菜单中选择该配置文件。

从独立主机中卸载 NSX-T Data Center

您可以从独立主机中卸载 NSX-T Data Center。独立主机可以是 ESXi 或 KVM。

小心 如果物理接口或 VMkernel 接口已连接到 N-VDS，则从 ESXi 主机中卸载 NSX-T Data Center 会具有破坏性。如果主机或集群加入其他应用程序（如 vSAN），则这些应用程序可能会受到卸载的影响。

前提条件

如果要从独立的 ESXi 主机中卸载 NSX-T Data Center，请确认以下设置：

- 确认要卸载的主机已配置网络卸载映射。请参见验证用于卸载的主机网络映射。
- 确认要卸载的主机在 vSphere 中处于维护模式。

步骤

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

2 选择**系统 > 结构层 > 节点 > 主机传输节点**。

3 从**托管主体**下拉菜单中，选择**无: 独立主机**。

4 选择主机，然后单击**删除**。在显示的确认对话框中，确保选择**卸载 NSX 组件**，并取消选择**强制删除**。单击**删除**。

此时会从主机中移除 NSX-T Data Center 软件。移除所有 NSX-T Data Center 软件可能最多需要 5 分钟。

5 如果卸载失败，请选择主机，然后再次单击**删除**。在确认对话框中，取消选择**卸载 NSX 组件**，并选择**强制删除**。

此时会从管理平面中删除主机传输节点，但主机上可能仍装有 NSX-T Data Center 软件。

6 确认已从主机中移除 NSX-T Data Center 软件。

a 以 root 用户身份登录到主机的命令行界面。

b 运行相应的命令以检查 NSX-T Data Center 软件包。

表 10-1. 软件包列表命令

主机操作系统	命令
ESXi	`esxcli software vib list | grep -E 'nsx|vsipfwlib'`
Red Hat Enterprise Linux 和 CentOS Linux	`rpm -qa | grep -E 'nsx|vsipfwlib'`
Ubuntu	`dpkg -l | grep -E 'nsx|vsipfwlib'`
SUSE Linux Enterprise Server	`zypper packages --installed-only | grep -E 'nsx|vsipfwlib'`

如果 NSX-T Data Center 软件已成功移除，则不会列出任何软件包。如果主机上仍留有任何 NSX 软件包，请联系 VMware 技术支持团队。

安装 NSX Cloud 组件

11

NSX Cloud 通过单一窗口来管理公有云网络。

NSX Cloud 与提供商特定的网络无关，它不需要公有云中的管理程序访问权限。

它具有诸多好处：

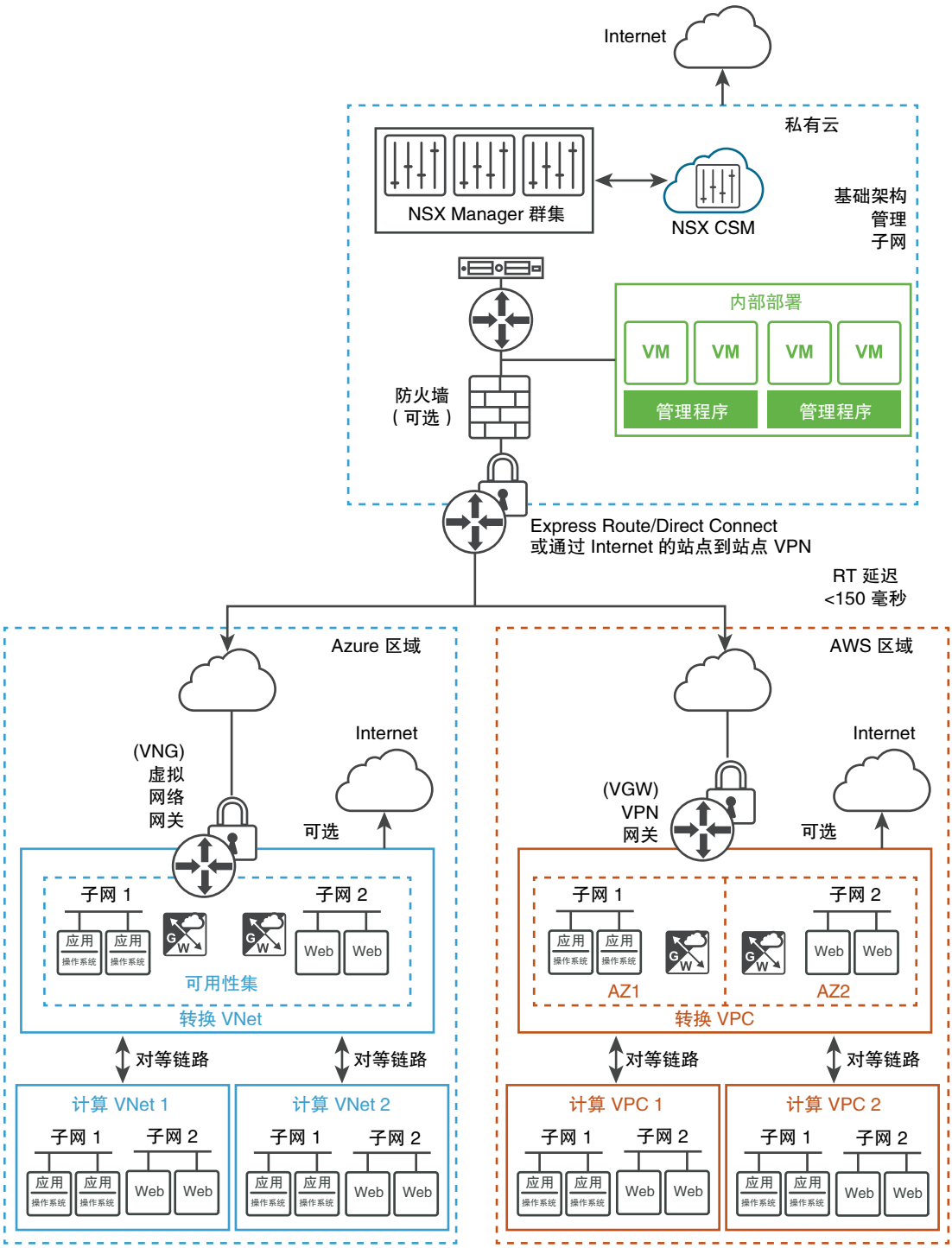
- 您可以使用生产环境中采用的相同网络和安全配置文件开发和测试应用程序。
- 开发人员在部署就绪之前，可以一直管理他们的应用程序。
- 具有灾难恢复功能，可在遇到计划外停机或公有云遭到安全威胁时进行恢复。
- 如果在公有云之间迁移工作负载，NSX Cloud 可确保对工作负载虚拟机应用类似的安全策略，而无论虚拟机的新位置在哪。

本章讨论了以下主题：

NSX Cloud 架构和组件

NSX Cloud 将 NSX-T Data Center 核心组件与公有云集成在一起，以便在您的实施中提供网络和安全功能。

图 11-1. NSX Cloud 架构



核心组件

NSX Cloud 核心组件有：

- NSX Manager 用于管理层面，并定义了基于策略的路由、基于角色的访问控制 (RBAC)、控制层面和运行时状态。
- Cloud Service Manager (CSM)，可与 NSX Manager 集成以向管理层面提供特定于公有云的信息。
- NSX Public Cloud Gateway (PCG)，用于连接到 NSX 管理层面和控制层面、NSX Edge 网关服务，并与公有云实体进行基于 API 的通信。请参见部署或链接 NSX Public Cloud Gateway 以了解详细信息。
- NSX 代理功能，为工作负载虚拟机提供 NSX 管理的数据路径。

部署模式

NSX Public Cloud Gateway 可以是独立网关设备，或者在公有云 VPC 或 VNet 之间共享以实现中心辐射型拓扑。

自我管理 VPC 或 VNet 充当转换 VPC：在 VPC 或 VNet 中部署 PCG 时，可确保 VPC 或 Vnet 能够自我管理，即由 NSX 管理此 VPC 或 VNet 中托管的虚拟机。此 VPC 或 VNet 还可以作为转换 VPC 或 VNet，因为可以使用其上部署的 PCG 载入其他 VPC 或 VNet 中托管的虚拟机。

计算 VPC 或 VNet 链接到转换 VPC 或 VNet：未部署 PCG 但链接到转换 VPC 或 VNet 的 VPC 或 VNet 称为计算 VPC 或 VNet。

为公有云安装和配置 NSX Cloud 组件的概述

请参阅检查表，以简要了解启用 NSX-T Data Center 以管理公有云中的工作负载虚拟机所涉及的步骤。

用于将 NSX Cloud 与公有云连接的初始工作流

此工作流概述了开始使用公有云的 NSX Cloud 所需的步骤。

注　在规划部署时，请确保在内部部署 NSX-T Data Center 设备和公有云中部署的 PCG 之间具有正确的连接。此外，转换 VPC/VNet 必须位于与计算 VPC/VNet 相同的区域中。

表 11-1. 用于将 NSX Cloud 与公有云连接的初始工作流

任务	说明
❑ 安装 CSM 并与 NSX Manager 连接。	请参见安装 CSM 并与 NSX Manager 连接。
❑ 在 CSM 中添加一个或多个公有云帐户。	请参见添加公有云帐户。
❑ 在转换 VPC 或 VNet 中部署 PCG 并链接到计算 VPC 或 VNet。	请参见部署或链接 NSX Public Cloud Gateway。
❑ 通过在公有云中进行标记，并在其上安装 NSX 代理，载入工作负载虚拟机。	按照 NSX-T Data Center 管理指南中“载入工作负载虚拟机”的说明操作。

安装 CSM 并与 NSX Manager 连接

使用设置向导将 NSX Manager 与 CSM 连接并设置代理服务器（如果有）。

安装 CSM

Cloud Service Manager (CSM) 是 NSX Cloud 的基本组件。

请在安装 NSX-T Data Center 核心组件后安装 CSM。

有关详细说明，请参见安装 NSX Manager 和可用设备。

注 要安装 NSX Cloud，您需要在 NSX Manager 上允许使用 FQDN (DNS)。请参见发布 NSX Manager 的 FQDN。

将 CSM 与 NSX Manager 相连接

必须将 CSM 设备与 NSX Manager 连接，以允许这些组件互相通信。

前提条件

- 必须安装 NSX Manager 且您必须具有 admin 帐户的用户名和密码才能登录到 NSX Manager
- 必须安装 CSM，并且您必须具有 CSM 中分配的企业管理员角色。

步骤

1 从浏览器中，登录到 CSM。

2 设置向导中出现提示时，单击**开始设置**。

3 在“NSX Manager 凭据”屏幕中输入以下详细信息：

选项	说明
NSX Manager 主机名	输入 NSX Manager 的完全限定域名 (FQDN)（如果可用）。您还可以输入 NSX Manager 的 IP 地址。
管理员凭据	为 NSX Manager 输入企业管理员用户名和密码。
Manager 指纹	（可选）输入 NSX Manager 的指纹值。如果将此字段留空，则系统将识别指纹并在下一个屏幕中显示它。

4 （可选） 如果未提供 NSX Manager 的指纹值，或者值不正确，则将显示**验证指纹**屏幕。选中复选框以接受系统发现的指纹。

5 单击**连接**。

注 如果在设置向导中错过此设置，或者要更改关联的 NSX Manager，则登录到 CSM，单击**系统 > 设置**，然后在标题为**关联的 NSX 节点**的面板上单击**配置**。

CSM 将验证 NSX Manager 指纹并建立连接。

6 （可选） 设置代理服务器。请参见（可选）配置代理服务器中的说明。

（可选）配置代理服务器

如果要通过可靠的 HTTP 代理路由并监控 Internet 绑定的所有 HTTP/HTTPS 流量，则可以在 CSM 中配置最多五个代理服务器。

来自 PCG 和 CSM 的所有公有云通信都通过选定的代理服务器进行路由。

PCG 的代理设置独立于 CSM 的代理设置。可以选择不为 PCG 使用代理服务器或者使用不同的代理服务器。

可以选择以下级别的身份验证：

- 基于凭据的身份验证。
- 用于 HTTPS 拦截的基于证书的身份验证。
- 无身份验证。

步骤

1 单击**系统 > 设置**。然后在标题为**代理服务器**的面板上单击**配置**。

注 使用首次安装 CSM 时可用的 CSM 设置向导，也可以提供这些详细信息。

2 在“配置代理服务器”屏幕中，输入以下详细信息：

选项	说明
默认	使用此单选按钮指示默认代理服务器。
配置文件名称	提供代理服务器的配置文件名称。这是必填的。
代理服务器	输入代理服务器的 IP 地址。这是必填的。
端口	输入代理服务器的端口。这是必填的。
身份验证	可选。如果要设置其他身份验证，则选中此复选框并提供有效的用户名和密码。
用户名	如果选中“身份验证”复选框，则为必填项。
密码	如果选中“身份验证”复选框，则为必填项。
证书	可选。如果要为 HTTPS 拦截提供身份验证证书，则选中此复选框，并在出现的文本框中复制并粘贴该证书。
无代理	如果不希望使用已配置的任何代理服务器，则选中此选项。

（可选）为 Cloud Service Manager 设置 vIDM

如果使用 VMware Identity Manager，您可以将其设置为从 NSX Manager 中访问 CSM。

步骤

1 为 NSX Manager 和 CSM 配置 vIDM。请参见《NSX-T Data Center 管理指南》的“配置 VMware Identity Manager 集成”部分中的说明。

2 为 NSX Manager 和 CSM 的 vIDM 用户分配相同的角色，例如，为名为 **vIDM_admin** 的用户分配**企业管理员**角色。您必须分别登录到 NSX Manager 和 CSM，并为同一用户名分配相同的角色。有关详细说明，请参见《NSX-T Data Center 管理指南》中的“添加角色分配或主体身份”。

3 登录到 NSX Manager。您将重定向到 vIDM 登录。

4 输入 vIDM 用户的凭据。在登录后，您可以单击应用程序图标以在 NSX Manager 和 CSM 之间进行切换。

将公有云与内部部署相连接

必须使用合适的连接选项将内部部署与公有云帐户或订阅相连接。

允许访问 CSM 上的端口和协议以实现混合连接

在 NSX Manager 上打开必要的网络端口并允许所需的协议，以启用公有云连接。

允许从公有云访问 NSX Manager

打开以下网络端口和协议，以允许与内部部署 NSX Manager 相连接：

表 11-2.

源	目标	协议/端口	说明
PCG	NSX Manager	TCP/5671	公有云到内部部署 NSX-T Data Center 的入站流量，用于管理层面通信。
PCG	NSX Manager	TCP/8080	公有云到内部部署 NSX-T Data Center 的入站流量，用于访问 HTTP 存储库以便升级 NSX Cloud 组件。
PCG	NSX Controller	TCP/1234、TCP/1235	公有云到内部部署 NSX-T Data Center 的入站流量，用于控制层面通信。
PCG	DNS	UDP/53	从公有云到内部部署 NSX-T Data Center DNS 的入站流量（如果使用的是内部部署 DNS 服务器）。
CSM	PCG	TCP/7442	CSM 配置推送

表 11-2.（续）

源	目标	协议/端口	说明
任意	NSX Manager	TCP/443	NSX Manager UI
任意	CSM	TCP/443	CSM UI。

重要事项 所有 NSX-T Data Center 基础架构通信都利用基于 SSL 的加密。请确保防火墙允许 SSL 流量通过非标准端口。

将 Microsoft Azure 网络与内部部署 NSX-T Data Center 相连接

必须在 Microsoft Azure 网络和内部部署 NSX-T Data Center 设备之间建立连接。

注 您必须已安装 NSX Manager 并将其与内部部署 CSM 相连接。

概述

- 将 Microsoft Azure 订阅与内部部署 NSX-T Data Center 相连接。
- 为 VNet 配置必要的 CIDR 块和 NSX Cloud 所需的子网。
- 将 CSM 设备上的时间与 Microsoft Azure 存储服务器或 NTP 同步。

将 Microsoft Azure 订阅与内部部署 NSX-T Data Center 相连接

每个公有云都提供了用来与内部部署连接的选项。您可以选择适合您要求的任意可用连接选项。有关详细信息，请参见 Microsoft Azure 参考文档。

注 您必须检查并实施适用的安全注意事项和 Microsoft Azure 最佳做法，例如，访问 Microsoft Azure 门户或 API 的所有特权用户帐户都应启用多重身份验证 (Multi Factor Authentication, MFA)。MFA 可确保只有合法用户才能访问该门户并降低非法合法访问的可能性，即使凭据被盗或泄漏也可以。有关详细信息和建议，请参阅“Azure Security Center Documentation”。

配置 VNet

在 Microsoft Azure 中，创建可路由 CIDR 块并设置所需的子网。

- 一个管理子网，包含至少为 /28 的建议范围，以处理：
  - 到内部部署设备的控制流量
  - 到云提供商 API 端点的 API 流量
- 一个下行链路子网，包含至少为 /24 的建议范围，用于工作负载虚拟机。
- 一个（若要实现 HA，则需要两个）上行链路子网，包含至少为 /24 的建议范围，用于路由离开或进入 VNet 的南北向流量。

有关如何使用这些子网的详细信息，请参见部署或链接 NSX Public Cloud Gateway。

将 Amazon Web Services (AWS) 网络与内部部署 NSX-T Data Center 相连接

必须在 Amazon Web Services (AWS) 网络和内部部署 NSX-T Data Center 设备之间建立连接。

注　您必须已安装 NSX Manager 并将其与内部部署 CSM 相连接。

概述

- 使用最符合您需求的任何可用选项将 AWS 帐户与内部部署 NSX Manager 设备相连接。
- 为 VPC 配置子网并根据 NSX Cloud 的其他要求进行配置。

将 AWS 帐户与内部部署 NSX-T Data Center 相连接

每个公有云都提供了用来与内部部署连接的选项。您可以选择适合您要求的任意可用连接选项。有关详细信息，请参见 AWS 参考文档。

注　您必须检查并实施适用的安全注意事项和 AWS 最佳做法；请参见 AWS 安全最佳做法。

配置 VPC

需要以下配置：

- 六个子网，用于支持具有高可用性的 PCG
- 一个 Internet 网关 (IGW)
- 一个专用和一个公用路由表
- 子网与路由表相关联
- 已启用 DNS 解析和 DNS 主机名

配置 VPC 时请遵循以下准则：

1　假设您的 VPC 使用 /16 网络，对于需要部署的每个网关，设置三个子网。

重要事项　如果使用高可用性，请在其他可用区中再设置三个子网。

- **管理子网**：此子网用于内部部署 NSX-T Data Center 和 PCG 之间的管理流量。建议的范围为 /28。
- **上行链路子网**：此子网用于南北向 Internet 流量。建议的范围为 /24。
- **下行链路子网**：此子网包括工作负载虚拟机的 IP 地址范围，应相应地调整大小。请注意，要进行调试，可能需要包含工作负载虚拟机上的其他接口。

注　为子网添加相应的标签，例如，`management-subnet`、`uplink-subnet`、`downlink-subnet`，因为在此 VPC 上部署 PCG 时需要选择子网。

请参见部署或链接 NSX Public Cloud Gateway 以了解详细信息。

2 确保您具有已连接到此 VPC 的 Internet 网关 (IGW)。

3 确保 VPC 的路由表已将**目标**设置为 **0.0.0.0/0** 且**目标**是连接到 VPC 的 IGW。

4 确保已为此 VPC 启用 DNS 解析和 DNS 主机名。

添加公有云帐户

要添加公有云清单，需要在公有云中创建允许访问 NSX Cloud 的角色，然后在 CSM 中添加所需信息。

设置对 Microsoft Azure 清单的安全访问

要让 NSX Cloud 在订阅中运行，请创建一个服务主体以基于 Microsoft Azure 功能为 CSM 和 PCG 授予所需权限和角色以便管理 Azure 资源的身份。

注 如果已将 AWS 帐户添加到 CSM，请在 **NSX Manager > 结构层 > 配置文件 > 上行链路配置文件 > PCG-Uplink-HostSwitch-Profile** 中将 MTU 更新为 1500，然后再添加 Microsoft Azure 帐户。也可以使用 NSX Manager REST API 执行此操作。

概览：

- Microsoft Azure 订阅包含一个或多个希望由 NSX-T Data Center 管理的 VNet。VNet 可能处于转换模式或计算模式。转换 VNet 是部署 PCG 的 VNet。可以将其他 VNet 链接到转换 VNet 并载入其中托管的工作负载虚拟机。VNet 链接到转换 VNet 时称为计算 VNet。
- NSX Cloud 提供了 PowerShell 脚本以生成服务主体和角色（使用 Microsoft Azure 的受管身份功能来管理身份验证，同时确保您的 Microsoft Azure 凭据安全）。也可以使用此脚本在一个服务主体下包括多个订阅。
- 可以选择将服务主体重用于所有的订阅，或者根据需要创建新的服务主体。如果要为其他订阅创建单独的服务主体，可以使用其他脚本。
- 对于多个订阅（不管将单个服务主体用于所有订阅，还是使用多个服务主体），必须更新 CSM 和 PCG 角色的 JSON 文件，才能在部分 *AssignableScopes* 下添加每个额外订阅的名称。
- 如果在 VNet 中已具有 NSX Cloud 服务主体，则可以通过再次运行脚本，并从参数中省略服务主体名称来进行更新。
- 服务主体名称对于 Microsoft Azure Active Directory 必须是唯一的。可以在同一 Active Directory 域下的不同订阅中使用相同的服务主体，或者每个订阅使用不同的服务主体。但是不能创建两个同名的服务主体。
- 必须是所有者，或者具有在所有 Microsoft Azure 订阅中创建和分配角色的权限。
- 支持以下场景：
  - **场景 1**：具有要通过 NSX Cloud 启用的单个 Microsoft Azure 订阅。
  - **场景 2**：在要通过 NSX Cloud 启用的同一 Microsoft Azure 目录下具有多个 Microsoft Azure 订阅，但要在所有订阅中使用一个 NSX Cloud 服务主体。

- **场景 3**：在要通过 NSX Cloud 启用的同一 Microsoft Azure 目录下具有多个 Microsoft Azure 订阅，但不同的订阅要使用不同的 NSX Cloud 服务主体名称。

以下是过程概要：

1 使用 NSX Cloud PowerShell 脚本：
   - 为 NSX Cloud 创建服务主体帐户。
   - 为 CSM 创建角色。
   - 为 PCG 创建角色。
2 （可选）为要链接的其他订阅创建服务主体。
3 在 CSM 中添加 Microsoft Azure 订阅。

> 注 如果使用多个订阅，则不管是使用相同的还是不同的服务主体，都必须在 CSM 中单独添加每个订阅。

生成服务主体和角色

NSX Cloud 提供了 PowerShell 脚本，可帮助您为一个或多个订阅生成所需的服务主体和角色。

前提条件

- 必须安装有包含 AzureRM 模块的 PowerShell 5.0+。
- 必须是所有者，或者具有在所有 Microsoft Azure 订阅中创建和分配角色的权限。

注 首次运行脚本时，Microsoft Azure 响应时间可能会导致脚本失败。如果脚本失败，请尝试重新运行。

步骤

1 在 Windows 桌面或服务器上，从 NSX-T Data Center **下载页面 > 驱动程序和工具 > NSX Cloud 脚本 > Microsoft Azure** 下载名为 `CreateNSXCloudCredentials.zip` 的 ZIP 文件。

2 将 ZIP 文件的以下内容提取到 Windows 系统中：

脚本/文件	说明
CreateNSXRoles.ps1	此 PowerShell 脚本用于生成 NSX Cloud 服务主体以及为 CSM 和 PCG 生成受管身份角色。此脚本采用以下参数： ■ `–subscriptionId <the Transit_VNet's_Azure_subscription_ID>` ■ （可选）`–servicePrincipalName <Service_Principal_Name>` ■ （可选）`–useOneServicePrincipal`
AddServicePrincipal.ps1	如果要添加多个订阅并且为每个订阅分配不同的服务主体，则需要此可选脚本。请参见以下步骤中的**场景 3**。此脚本采用以下参数： ■ `–computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID>` ■ `–transitSubscriptionId <the Transit_VNet's_Azure_Subscription_ID>` ■ `–csmRoleName <CSM_Role_Name>` ■ `–servicePrincipalName <Service_Principal_Name>`
nsx_csm_role.json	针对 CSM 角色名称和权限提供的一个 JSON 模板。需要此文件作为 PowerShell 脚本的输入，并且它必须与脚本位于同一文件夹中。
nsx_pcg_role.json	针对 PCG 角色名称和权限提供的一个 JSON 模板。需要此文件作为 PowerShell 脚本的输入，并且它必须与脚本位于同一文件夹中。 **注** 默认 PCG（网关）角色名称为 `nsx–pcg–role`。在 CSM 中添加您的订阅时，需要提供此值。

3 **场景 1**：具有要通过 NSX Cloud 启用的单个 Microsoft Azure 订阅。

a 从 PowerShell 实例中，转到下载了 Microsoft Azure 脚本和 JSON 文件的目录。

b 使用参数 -SubscriptionId 运行名为 CreateNSXRoles.ps1 的脚本，如下所示：

```
.\CreateNSXRoles.ps1 –subscriptionId <the_single_Azure_subscription_ID>
```

注 如果要替代 `nsx–service–admin` 的默认服务主体名称，也可以使用参数 `-servicePrincipalName`。服务主体名称在 Microsoft Azure Active Directory 中必须是唯一的。

4 **场景 2**：在要通过 NSX Cloud 启用的同一 Microsoft Azure 目录下具有多个 Microsoft Azure 订阅，但要在所有订阅中使用一个 NSX Cloud 服务主体。

a 从 PowerShell 实例中，转到下载了 Microsoft Azure 脚本和 JSON 文件的目录。

b 编辑每个 JSON 文件以在标题为 *"AssignableScopes"* 的部分下添加其他订阅 ID 的列表，例如：

```
"AssignableScopes": [

"/subscriptions/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",

"/subscriptions/aaaaaaaa-bbbb-cccc-dddd-ffffffffffff",

"/subscriptions/aaaaaaaa-bbbb-cccc-dddd-000000000000"
```

注 必须使用示例中显示的格式来添加订阅 ID： `"/subscriptions/<Subscription_ID>"`

c 运行带参数 `-subscriptionID` 和 `-useOneServicePrincipal` 的名为 `CreateNSXRoles.ps1` 的脚本：

```
.\CreateNSXRoles.ps1 -subscriptionId <the_Transit_VNet's_Azure_subscription_ID> -
useOneServicePrincipal
```

注 如果要使用默认名称 `nsx-service-admin`，请在此处省略服务主体名称。如果该服务主体名称已存在于 Microsoft Azure Active Directory 中，则不带服务主体名称运行此脚本将更新该服务主体。

5 **场景 3**：在要通过 NSX Cloud 启用的同一 Microsoft Azure 目录下具有多个 Microsoft Azure 订阅，但不同的订阅要使用不同的 NSX Cloud 服务主体名称。

a 从 PowerShell 实例中，转到下载了 Microsoft Azure 脚本和 JSON 文件的目录。

b 按照场景 2 中的步骤 **b** 和 **c**，将多个订阅添加到每个 JSON 文件的 *AssignableScopes* 部分。

c 运行带参数 -subscriptionID 的名为 CreateNSXRoles.ps1 的脚本：

```
.\CreateNSXRoles.ps1 –subscriptionId <One of the subscription_IDs>
```

注 如果要使用默认名称 nsx-service-admin，请在此处省略服务主体名称。如果该服务主体名称存在于 Microsoft Azure Active Directory 中，则不带服务主体名称运行此脚本将更新该服务主体。

d 运行带以下参数的名为 AddServicePrincipal.ps1 的脚本：

参数	值
–computeSubscriptionId	Compute_VNet 的 Azure 订阅 ID
–transitSubscriptionId	转换 VNet 的 Azure 订阅 ID
–csmRoleName	从文件 nsx_csm_role.JSON 中获取此值。
–servicePrincipalName	新服务主体名称

```
./AddServicePrincipal.ps1 –computeSubscriptionId <the_Compute_VNet's_Azure_subscription_ID>
 –transitSubscriptionId <the_Tranist_VNet's_Azure_Subscription_ID>
–csmRoleName <CSM_Role_Name>
–servicePrincipalName <new_Service_Principal_Name>”
```

6 在运行 PowerShell 脚本的同一目录中查找文件。该文件的文件名类似于：NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name>。该文件包含在 CSM 中添加 Microsoft Azure 订阅所需的信息。

- 客户端 ID
- 客户端密钥
- 租户 ID
- 订阅 ID

结果

将创建以下结构：

- 为 NSX Cloud 创建 Azure AD 应用程序。
- 为 NSX Cloud 应用程序创建 Azure 资源管理器服务主体。
- 为连接到服务主体帐户的 CSM 创建角色。
- 为 PCG 创建角色，以使其在公有云清单上运行。
- 在运行 PowerShell 脚本的同一目录中创建名称类似 NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name> 的文件。该文件包含在 CSM 中添加 Microsoft Azure 订阅所需的信息。

注 有关创建 CSM 和 PCG 角色后适用于这些角色的权限列表，请参阅用于创建这些角色的 JSON 文件。

后续步骤

在 CSM 中添加 Microsoft Azure 订阅

注 为多个订阅启用 NSX Cloud 时，必须将每个单独的订阅分别添加到 CSM，例如，如果共有五个订阅，则必须在 CSM 中添加五个 Microsoft Azure 帐户，所有其他值相同，但订阅 ID 不同。

在 CSM 中添加 Microsoft Azure 订阅

获取 NSX Cloud 服务主体以及 CSM 和 PCG 角色的详细信息后，即可在 CSM 中添加 Microsoft Azure 订阅。

前提条件

- 您必须在 NSX-T Data Center 中拥有企业管理员角色。
- 您必须拥有 PowerShell 脚本的输出和 NSX Cloud 服务主体的详细信息。
- 您必须具有运行 PowerShell 脚本以创建角色和服务主体时提供的 PCG 角色的值。默认值为 `nsx-pcg-role`。

步骤

1 使用具有企业管理员角色的帐户登录到 CSM。

2 转到 **CSM > 云 > Azure**。

3 单击 **+ 添加**，然后输入以下详细信息：

选项	说明
名称	提供合适的名称以在 CSM 中标识此帐户。您可能有多个 Microsoft Azure 订阅与同一个 Microsoft Azure 租户 ID 相关联。对您的帐户命名，您可在 CSM 中使用合适的名称，例如 Azure-DevOps-Account、Azure-Finance-Account 等。
客户端 ID	从 PowerShell 脚本的输出中复制粘贴此值。
密钥	从 PowerShell 脚本的输出中复制粘贴此值。
订阅 ID	从 PowerShell 脚本的输出中复制粘贴此值。
租户 ID	从 PowerShell 脚本的输出中复制粘贴此值。
网关角色名称	默认值为 `nsx-pcg-role`。如果更改了默认值，可从 nsx_pcg_role.json 文件获得此值。
云标记	默认情况下，此选项处于启用状态，并允许 Microsoft Azure 标记在 NSX Manager 中可见

4 单击**保存**。

CSM 将添加该帐户，三分钟内可在**帐户**部分中看到该帐户。

后续步骤

在自我管理或转换 VNet 中部署 PCG

设置对 AWS 清单的安全访问

可能有一个或多个包含希望由 NSX-T Data Center 管理的 VPC 和工作负载虚拟机的 AWS 帐户。

概览：

- 在一个 VPC 中，可以使用部署 PCG 的转换/计算 VPC 拓扑，使其成为转换 VPC 并将其他 VPC（称为计算 VPC）与之链接。
- NSX Cloud 提供了 Shell 脚本，可以从 AWS 帐户的 AWS CLI 运行该脚本，以便创建 IAM 配置文件和角色，并为转换和计算 VPC 创建信任关系。
- 支持以下场景：
  - **场景 1**：将单个 AWS 帐户与 NSX Cloud 一起使用。
  - **场景 2**：在由主 AWS 帐户管理的 AWS 中使用多个子帐户。
  - **场景 3**：将多个 AWS 帐户与 NSX Cloud 一起使用。

以下是过程概要：

1 使用 NSX Cloud Shell 脚本（需要 AWS CLI）执行以下操作：
   - 创建 IAM 配置文件。
   - 为 PCG 创建角色。
   - （可选）在托管转换 VPC 的 AWS 帐户和托管计算 VPC 的 AWS 帐户之间创建信任关系。

2 在 CSM 中添加 AWS 帐户。

生成 IAM 配置文件和 PCG 角色

NSX Cloud 提供了 SHELL 脚本以帮助设置一个或多个 AWS 帐户，方法是针对附加到为您的 AWS 帐户提供必要权限的配置文件的 PCG 生成 IAM 配置文件和角色。

如果计划在两个不同的 AWS 帐户中托管链接到多个计算 VPC 的转换 VPC，则可以使用脚本在这些帐户之间创建信任关系。

注 默认情况下，PCG（网关）角色名称为 `nsx_pcg_service`。如果要为网关角色名称使用不同的值，则可以在脚本中更改它，但请记下此值，因为在 CSM 中添加 AWS 帐户时需要该值。

前提条件

运行脚本之前，必须在 Linux 或兼容系统上安装并配置以下项：

- AWS CLI
- `jq`（JSON 解析器）
- `openssl`

注 如果使用多个 AWS 帐户，则必须使用合适的方法使其处于对等状态。

步骤

1 在 Linux 或兼容的桌面或服务器上，从 NSX-T Data Center 下载页面 > 驱动程序和工具 > NSX Cloud 脚本 > AWS 下载 SHELL 脚本 `nsx_csm_iam_script.sh`。

2 **场景 1**：将单个 AWS 帐户与 NSX Cloud 一起使用。

a 运行该脚本，例如：

```
bash nsx_csm_iam_script.sh
```

b 系统提示问题 `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]` 时，输入 `yes`

c 系统询问 `What do you want to name the IAM User?` 时，输入 IAM 用户的名称

注 IAM 用户名在 AWS 帐户中必须是唯一的。

d 系统询问 `Do you want to add trust relationship for any Transit VPC account? [yes/no]` 时，输入 `no`

脚本成功运行后，会在 AWS 帐户中为 PCG 创建该 IAM 配置文件和角色。值将保存在运行脚本的同一目录下名为 `aws_details.txt` 的输出文件中。接下来，依次按照在 CSM 中添加 AWS 帐户和在自我管理或转换 VPC 中部署 PCG 中的说明操作，完成转换或自我管理 VPC 的设置过程。

3 **场景 2**：在由一个主 AWS 帐户管理的 AWS 中使用多个子帐户。

a 从 AWS 主帐户运行脚本。

```
bash nsx_csm_iam_script.sh
```

b 系统提示问题 `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]` 时，输入 `yes`

c 系统询问 `What do you want to name the IAM User?` 时，输入 IAM 用户的名称

注 IAM 用户名在 AWS 帐户中必须是唯一的。

d 系统询问 `Do you want to add trust relationship for any Transit VPC account? [yes/no]` 时，输入 `no`

注 对于主 AWS 帐户，如果您的转换 VPC 具有查看子帐户中计算 VPC 的权限，则不需要与子帐户建立信任关系。如果没有，则按照**场景 3** 的步骤设置多个帐户。

成功运行脚本后，会在 AWS 主帐户中为 PCG 创建 IAM 配置文件和角色。值将保存在运行脚本时的同一目录下的输出文件中。文件名为 `aws_details.txt`。接下来，依次按照在 CSM 中添加 AWS 帐户和在自我管理或转换 VPC 中部署 PCG 中的说明操作，完成转换或自我管理 VPC 的设置过程。

4 **场景 3**：将多个 AWS 帐户与 NSX Cloud 一起使用。

注 验证 AWS 帐户是否处于对等状态，然后再继续。

a 记下要托管转换 VPC 的 12 位 AWS 帐号。

b 按照场景 1 中步骤 a 到 d 在 AWS 帐户中设置转换 VPC，并完成在 CSM 中添加帐户以及部署 PCG 的过程。

c 在要托管计算 VPC 的其他 AWS 帐户中，从 Linux 或兼容系统下载并运行 NSX Cloud 脚本。

注 或者，可以将 AWS 配置文件与不同的帐户凭据一起使用，以便使用同一系统对其他 AWS 帐户再次运行脚本。

d 系统询问 `Do you want to create an IAM user for CSM and an IAM role for PCG? [yes/no]` 时，输入 `yes`

注 如果已将此 AWS 帐户添加到 CSM 中，并且希望重用脚本以连接到不同的 AWS 帐户，则可以输入 `no` 并跳过创建 IAM 用户。

e 系统询问 `What do you want to name the IAM User?` 时，输入 IAM 用户的名称

注 IAM 用户名在 AWS 帐户中必须是唯一的。

f 系统询问 `Do you want to add trust relationship for any Transit VPC account? [yes/no]` 时，输入 `yes`

g 系统询问 `What is the Transit VPC account number?` 时，输入或复制并粘贴在步骤 1 中记录的 12 位 AWS 帐号

在两个 AWS 帐户之间建立了 IAM 信任关系，外部 ID 由脚本生成。

成功运行脚本后，会在 AWS 主帐户中为 PCG 创建 IAM 配置文件和角色。值将保存在运行脚本时的同一目录下的输出文件中。文件名为 `aws_details.txt`。接下来，依次按照在 CSM 中添加 AWS 帐户和链接到转换 VPC 或 VNet 中的说明完成链接到转换 VPC 的过程。

在 CSM 中添加 AWS 帐户

使用脚本生成的值添加 AWS 帐户。

步骤

1 使用企业管理员角色登录到 CSM。

2 转到 **CSM > 云 > AWS**。

3 单击 **+添加**，然后使用从 NSX Cloud 脚本生成的输出文件 aws_details.txt 输入以下详细信息：

选项	说明
名称	输入此 AWS 帐户的描述性名称
访问密钥	输入帐户的访问密钥

选项	说明
密钥	输入帐户的密钥
云标记	默认情况下，此选项处于启用状态，并允许 AWS 标记在 NSX Manager 中可见
网关角色名称	默认值为 `nsx_pcg_service`。可以在脚本的输出文件 aws_details.txt 中找到此值。

结果

AWS 帐户添加到了 CSM 中。

在 CSM 的“VPC”选项卡中，可以查看您 AWS 帐户中的所有 VPC。

在 CSM 的“实例”选项卡中，可以查看此 VPC 中的 EC2 实例。

后续步骤

在自我管理或转换 VPC 中部署 PCG

部署或链接 NSX Public Cloud Gateway

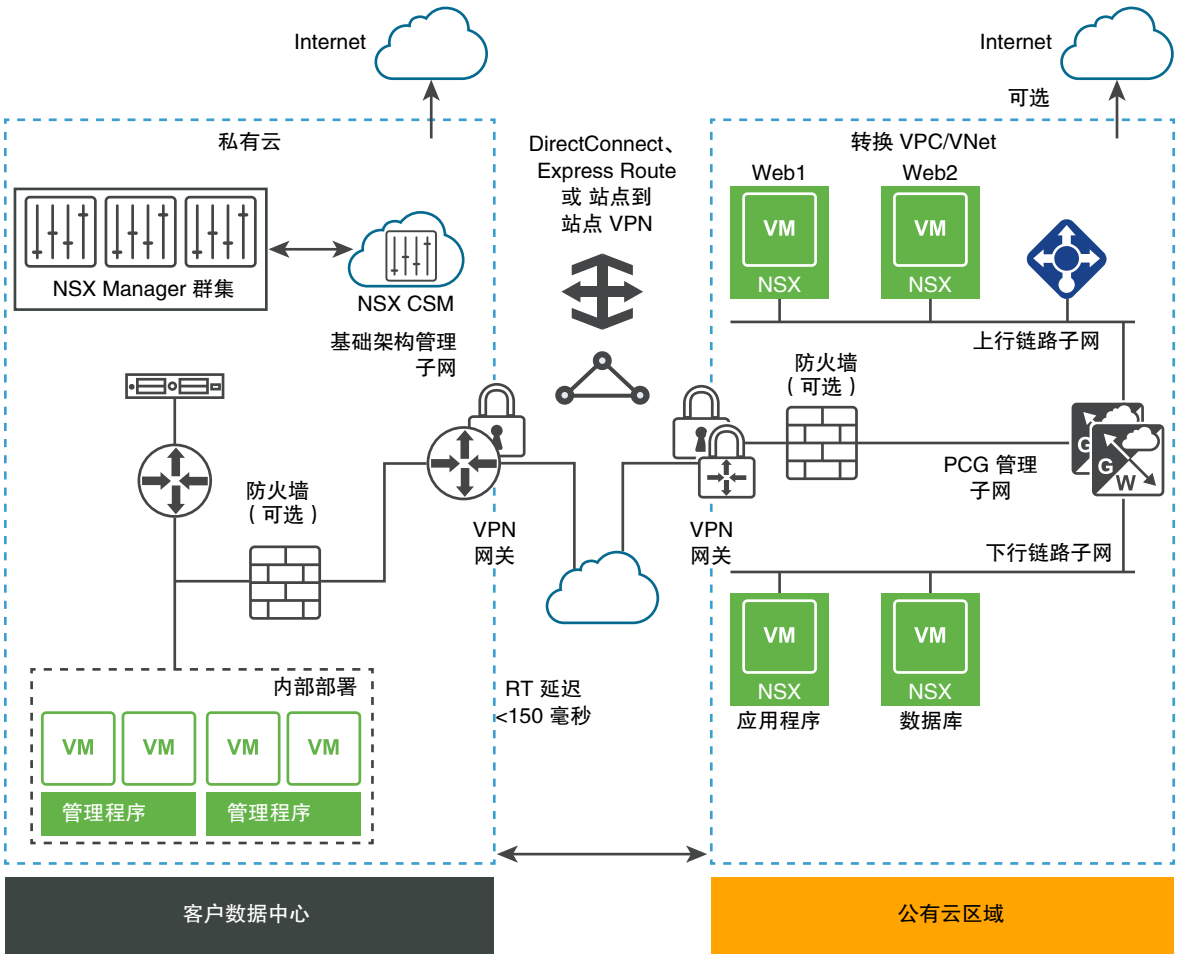
NSX Public Cloud Gateway (PCG) 在公有云和 NSX-T Data Center 的内部部署管理组件之间提供南北向连接。

PCG 可以是独立网关设备，或者在公有云 VPC 或 VNet 之间共享以实现中心辐射型拓扑。

注　将按照每个受支持公有云的单一默认大小来部署 PCG：

公有云	PCG 实例类型
AWS	C4.xlarge 注　某些区域可能不支持 C4.xlarge 实例类型。有关详细信息，请参阅 AWS 文档。
Microsoft Azure	Standard DS3 v.2

图 11-2. NSX Public Cloud Gateway 架构



转换或自我管理 VPC 或 VNet：在 VPC 或 VNet 中部署 PCG 时，可确保 VPC 或 VNet 能够自我管理，即由 NSX 管理此 VPC 或 VNet 中托管的虚拟机。此 VPC 或 VNet 还可以作为转换 VPC 或 VNet，因为可以使用其上部署的 PCG 载入其他 VPC 或 VNet 中托管的虚拟机。PCG 利用在 VPC/VNet 中设置的以下子网。请参见将 Microsoft Azure 网络与内部部署 NSX-T Data Center 相连接或将 Amazon Web Services (AWS) 网络与内部部署 NSX-T Data Center 相连接。

- **管理子网**：此子网用于内部部署 NSX-T Data Center 和 PCG 之间的管理流量。建议的范围为 /28。
- **上行链路子网**：此子网用于南北向 Internet 流量。建议的范围为 /24。
- **下行链路子网**：此子网包括工作负载虚拟机的 IP 地址范围，应相应地调整大小。请注意，要进行调试，可能需要包含工作负载虚拟机上的其他接口。

计算 VPC 或 VNet：未部署 PCG 但链接到转换 VPC 或 VNet 的 VPC 或 VNet 称为计算 VPC 或 VNet。

PCG 部署与使用 NSX-T Data Center 组件的 FQDN 的网络寻址计划和可以解析这些 FQDN 的 DNS 服务器相一致。

注　不建议使用 PCG 连接公有云和 NSX-T Data Center 时使用 IP 地址，但是如果选择该选项，请勿更改 IP 地址。

在自我管理或转换 VNet 中部署 PCG

按照以下说明在 Microsoft Azure VNet 中部署 PCG。

部署 PCG 的 VNet 可以充当其他 VNet 可以连接的转换 VNet（称为计算 VNet）。此 VNet 也可以管理虚拟机，并充当自我管理 VNet。

按照以下说明部署 PCG。如果要链接到现有的转换 VNet，请参见链接到转换 VPC 或 VNet 。

前提条件

- 您的公有云帐户必须已添加到 CSM。
- 部署 PCG 的 VNet 必须相应调整所需子网以实现高可用性：上行链路、下行链路和管理。

步骤

1 使用具有企业管理员角色的帐户登录到 CSM。

2 单击**云 > Azure**，然后转到 **VNet** 选项卡。

3 单击要在其中部署 PCG 的 VNet。

4 单击**部署网关**。将打开**部署主网关**向导。

5 对于“常规属性”，请使用以下准则：

选项	说明
SSH 公钥	提供部署 PCG 时可验证的 SSH 公钥。这是每次 PCG 部署所必需的。
关联 VNet 上的隔离策略	首次部署 PCG 时，将其保留默认的**已禁用**模式。载入虚拟机后，可以更改此值。有关详细信息，请参见《NSX-T Data Center 管理指南》中的**管理隔离策略**。
本地存储帐户	向 CSM 添加 Microsoft Azure 订阅时，Microsoft Azure 存储帐户列表可用于 CSM。从下拉菜单中选择存储帐户。继续部署 PCG 时，CSM 会将 PCG 的公开可用 VHD 复制到所选区域的此存储帐户。 **注** 如果 VHD 映像已复制到之前的 PCG 部署对应的区域中的此存储帐户，则后续部署将使用此位置的映像，以减少整体部署时间。
VHD URL	如果要使用 VMware 公共存储库不提供的其他 PCG 映像，可在此处输入该 PCG VHD 的 URL。VHD 必须位于用来创建此 VNet 的帐户和区域中。 **注** VHD 必须采用正确的 URL 格式。我们建议您在 Microsoft Azure 中使用**单击以复制**选项。
代理服务器	选择一个代理服务器以用于来自此 PCG 的 Internet 流量。在 CSM 中配置代理服务器。可以选择与 CSM（如果存在）相同的代理服务器，也可以选择与 CSM 不同的代理服务器，还可以选择**无代理服务器**。 有关如何在 CSM 中配置代理服务器的详细信息，请参见（可选）配置代理服务器。
高级	使用高级 DNS 设置，可以灵活地选择用于解析 NSX-T Data Center 管理组件的 DNS 服务器。
通过公有云提供商的 DHCP 获取	如果要使用 Microsoft Azure DNS 设置，请选择此选项。如果您未选择任一选项将其替代，则此选项是默认的 DNS 设置。

选项	说明
替代公有云提供商的 DNS 服务器	如果要手动提供用于解析 NSX-T Data Center 设备以及此 VNet 中的工作负载虚拟机的一个或多个 DNS 服务器的 IP 地址，请选择此选项。
仅对 NSX-T Data Center 设备使用公有云提供商的 DNS 服务器	如果要使用 Microsoft Azure DNS 服务器解析 NSX-T Data Center 管理组件，请选择此选项。选择此设置后，您可以使用两个 DNS 服务器：一个用于 PCG，以解析 NSX-T Data Center 设备；另一个用于 VNet，以解析此 VNet 中的工作负载虚拟机。

6 单击**下一步**。

7 对于**子网**，请使用以下准则：

选项	说明
为 NSX Cloud 网关启用 HA	选择此选项以启用高可用性。
子网	选择此选项以启用高可用性。
管理网卡上的公用 IP	选择**分配新 IP 地址**，以向管理网卡提供公用 IP 地址。如果要重用可用的公用 IP 地址，可以手动提供该公用 IP 地址。
上行链路网卡上的公用 IP	选择**分配新 IP 地址**，以向上行链路网卡提供公用 IP 地址。如果要重用可用的公用 IP 地址，可以手动提供该公用 IP 地址。

后续步骤

载入工作负载虚拟机。有关第 N 天工作流，请参见《NSX-T Data Center 管理指南》中的**载入并管理工作负载虚拟机**。

在自我管理或转换 VPC 中部署 PCG

请按照以下说明在 AWS VPC 中部署 PCG。

部署 PCG 的 VPC 可以充当其他 VPC 可以连接的转换 VPC（称为计算 VPC）。此 VPC 也可以管理虚拟机，并充当自我管理 VPC。

按照以下说明部署 PCG。如果要链接到现有的转换 VPC，请参见链接到转换 VPC 或 VNet 。

前提条件

- 您的公有云帐户必须已添加到 CSM。
- 部署 PCG 的 VPC 必须相应调整所需子网以实现高可用性：上行链路、下行链路和管理。
- VPC 的网络 ACL 配置必须包括允许入站规则。

步骤

1 使用具有企业管理员角色的帐户登录到 CSM。

2 单击**云 > AWS > <AWS_account_name>**，然后转到 **VPC** 选项卡。

3 在 **VPC** 选项卡中，选择 AWS 区域名称，例如，`us-west`。AWS 区域必须是创建计算 VPC 的同一区域。

4 选择为 NSX Cloud 配置的计算 VPC。

5 单击部署网关。

6 填写常规网关详细信息：

选项	说明
PEM 文件	从下拉菜单中选择一个 PEM 文件。此文件必须位于部署 NSX Cloud 并创建 VPC 的同一区域。 这可唯一地标识您的 AWS 帐户。
关联 VPC 上的隔离策略	首次部署 PCG 时，将其保留默认的**已禁用**模式。载入虚拟机后，可以更改此值。有关详细信息，请参见《NSX-T Data Center 管理指南》中的**管理隔离策略**。
代理服务器	选择一个代理服务器以用于来自此 PCG 的 Internet 流量。在 CSM 中配置代理服务器。可以选择与 CSM（如果存在）相同的代理服务器，也可以选择与 CSM 不同的代理服务器，还可以选择**无代理服务器**。 有关如何在 CSM 中配置代理服务器的详细信息，请参见（可选）配置代理服务器。
高级	高级设置提供额外选项（如果需要）。
替代 AMI ID	使用此高级功能可为 PCG 提供一个不同于 AWS 帐户所提供的 AMI ID。
通过公有云提供商的 DHCP 获取	如果要使用 AWS 设置，请选择此选项。如果您未选择任一选项将其替代，则此选项是默认的 DNS 设置。
替代公有云提供商的 DNS 服务器	如果要手动提供用于解析 NSX-T Data Center 设备以及此 VPC 中的工作负载虚拟机的一个或多个 DNS 服务器的 IP 地址，请选择此选项。
仅对 NSX-T Data Center 设备使用公有云提供商的 DNS 服务器	如果要使用 AWS DNS 服务器解析 NSX-T Data Center 管理组件，请选择此选项。选择此设置后，可以使用两个 DNS 服务器：一个用于 PCG，以解析 NSX-T Data Center 设备；另一个用于 VPC，以解析此 VPC 中的工作负载虚拟机。

7 单击下一步。

8 填写子网详细信息。

选项	说明
为公有云网关启用 HA	建议设置为“启用”，以设置高可用性活动/备用对，从而避免非计划停机。
主网关设置	从下拉菜单中选择一个可用区（如 `us-west-1a`）作为 HA 的主网关。 从下拉菜单中分配上行链路、下行链路和管理子网。
辅助网关设置	从下拉菜单中选择另一个可用区（如 `us-west-1b`）作为 HA 的辅助网关。 当主网关出现故障时，使用辅助网关。 从下拉菜单中分配上行链路、下行链路和管理子网。
管理网卡上的公用 IP	选择**分配新 IP 地址**，以向管理网卡提供公用 IP 地址。如果要重用可用的公用 IP 地址，可以手动提供该公用 IP 地址。
上行链路网卡上的公用 IP	选择**分配新 IP 地址**，以向上行链路网卡提供公用 IP 地址。如果要重用可用的公用 IP 地址，可以手动提供该公用 IP 地址。

单击部署。

9 监控主 PCG 部署（以及辅助部署，如果已选择）的状态。此过程可能需要 10-12 分钟的时间。

10 成功部署 PCG 后，单击完成。

后续步骤

载入工作负载虚拟机。有关第 N 天工作流，请参见《NSX-T Data Center 管理指南》中的**载入并管理工作负载虚拟机**。

链接到转换 VPC 或 VNet

可以将一个或多个计算 VPC 或 VNet 链接到转换 VPC 或 VNet。

前提条件

- 确认您具有 PCG 处于**已启动**状态的转换 VPC 或 VNet。
- 确认要链接的 VPC/VNet 通过 VPN 或对等互连连接到转换 VPC 或 VNet。
- 确认转换 VPC/VNet 位于与计算 VPC/VNet 相同的区域中。

注　在基于路由的 IPSec VPN 配置中，您必须指定虚拟隧道接口 (Virtual Tunnel Interface, VTI) 端口的 IP 地址。该 IP 必须位于与工作负载虚拟机不同的子网中。这可防止将工作负载虚拟机入站流量传送到 VTI 端口，将在此处丢弃流量。

注　在公有云中，每个安全组的入站/出站规则数具有默认限制，NSX Cloud 将创建默认安全组。这会影响可以链接到转换 VPC/VNet 的计算 VPC/VNet 数。假设每个 VPC/VNet 具有 1 个 CIDR 块，NSX Cloud 在每个转换 VPC/VNet 中支持 10 个计算 VPC/VNet。如果在任何计算 VPC/VNet 中具有多个 CIDR，则每个转换 VPC/VNet 支持的计算 VPC/VNet 数将会减少。您可以与公有云提供商联系以调整默认限制。

步骤

1. 使用具有企业管理员角色的帐户登录到 CSM。
2. 单击**云 > AWS/Azure > <public cloud_account_name>**，然后转到 **VPC/VNet** 选项卡。
3. 在 **VPC** 或 **VNet** 选项卡中，选择要托管一个或多个计算 VPC 或 VNet 的区域名称。
4. 选择为 NSX Cloud 配置的计算 VPC 或 VNet。
5. 单击**链接到转换 VPC** 或**链接到转换 VNET**
6. 完成**链接转换 VPC 或 VNet** 窗口中的选项：

选项	说明
转换 VPC 或 VNet	从下拉菜单中选择转换 VPC 或 VNet。选择的转换 VPC 或 VNet 必须已通过 VPN 或对等互连与此 VPC 链接。 注　如果连接到转换 VNet，则必须在该 VNet 中已配置 DNS 转发器。请参见 Microsoft Azure 文档以了解详细信息。
默认隔离策略	首次部署 PCG 时，将其保留默认的**已禁用**模式。载入虚拟机后，可以更改此值。有关详细信息，请参见《NSX-T Data Center 管理指南》中的**管理隔离策略**。

后续步骤

载入工作负载虚拟机。有关第 N 天工作流，请参见《NSX-T Data Center 管理指南》中的**载入并管理工作负载虚拟机**。

自动创建的逻辑实体和云原生安全组

转换 VPC/VNet 中 PCG 的部署以及向其链接计算 VPC/VNet 会触发 NSX-T Data Center 和公有云中的必要配置。

自动创建的 NSX-T 逻辑实体

在 NSX-T Data Center 中，会创建一组逻辑实体。

重要事项 请勿删除任何这些自动创建的实体。

系统实体

可以在**系统**下看到以下实体：

表 11-3. 自动创建的系统实体

逻辑系统实体	已创建多少个？	术语	范围
传输区域	为每个转换 VPC/VNet 创建两个传输区域	■ TZ-<VPC/VNet-ID>-OVERLAY ■ TZ-<VPC/VNet-ID>-VLAN	范围：全局
Edge 传输节点	为每个已部署的 PCG 创建一个 Edge 传输节点，如果在高可用性模式下部署，则创建两个。	■ PublicCloudGatewayTN-<VPC/VNET-ID> ■ PublicCloudGatewayTN-<VPC/VNET-ID>-preferred	范围：全局
Edge 群集	为每个已部署的 PCG 创建一个 Edge 群集，在高可用性模式下则创建两个。	PCG-cluster-<VPC/VNet-ID>	范围：全局

清单实体

在**清单**下面创建了以下实体：

表 11-4. 自动创建的清单实体

逻辑清单实体	已创建多少个？	术语	范围
域 注 域对象是 NSX-T Data Center 2.4 中的一个实验性功能，并在用户界面中显示自动创建的域。不过，在 NSX-T Data Center 2.4.1 用户界面中不再显示这些域。	每个转换 VPC/VNet 一个	cloud-<Transit VPC/VNet-ID>	范围：在所有 PCG 之间共享。
组	默认域下的两个组 注 在 NSX-T Data Center 中，您可以看到默认域。不过，在 NSX-T Data Center 2.4.1 中不显示域对象。	■ cloud-default-route ■ Cloud-metadata 服务	范围：在所有 PCG 之间共享
组	一个组 对于在计算 VPC/VNet 级别上创建的各个分段，在转换 VPC/VNet 级别上创建为父组。	cloud-<Transit VPC/VNet ID>-all-segments	范围：在所有计算 VPC/VNet 之间共享
组	两个组： ■ 计算 VPC/VNet 的所有 CIDR 的网络 CIDR 组 ■ 计算 VPC/VNet 中所有受管分段的本地分段组	■ cloud-<Compute VPC/VNet ID>-cidr ■ cloud-<Compute VPC/VNet ID>-local-segments	范围：在所有计算 VPC/VNet 之间共享

安全实体

表 11-5. 自动创建的安全实体

逻辑安全实体	已创建多少个？	术语	范围
分布式防火墙（东西向）	每个转换 VPC/VNet 两个： ■ 无状态 ■ 有状态	■ cloud-stateless-<VPC/VNet ID> ■ cloud-stateful-<VPC/VNet ID>	■ 允许本地受管分段中的流量的有状态规则 ■ 拒绝来自非受管虚拟机的流量的有状态规则
网关防火墙（南北向）	每个转换 VPC/VNet 一个	cloud-<Transit VPC/VNet ID>	

网络实体

在不同载入阶段创建以下实体：

图 11-3. 部署 PCG 后自动创建的 NSX-T Data Center 网络实体

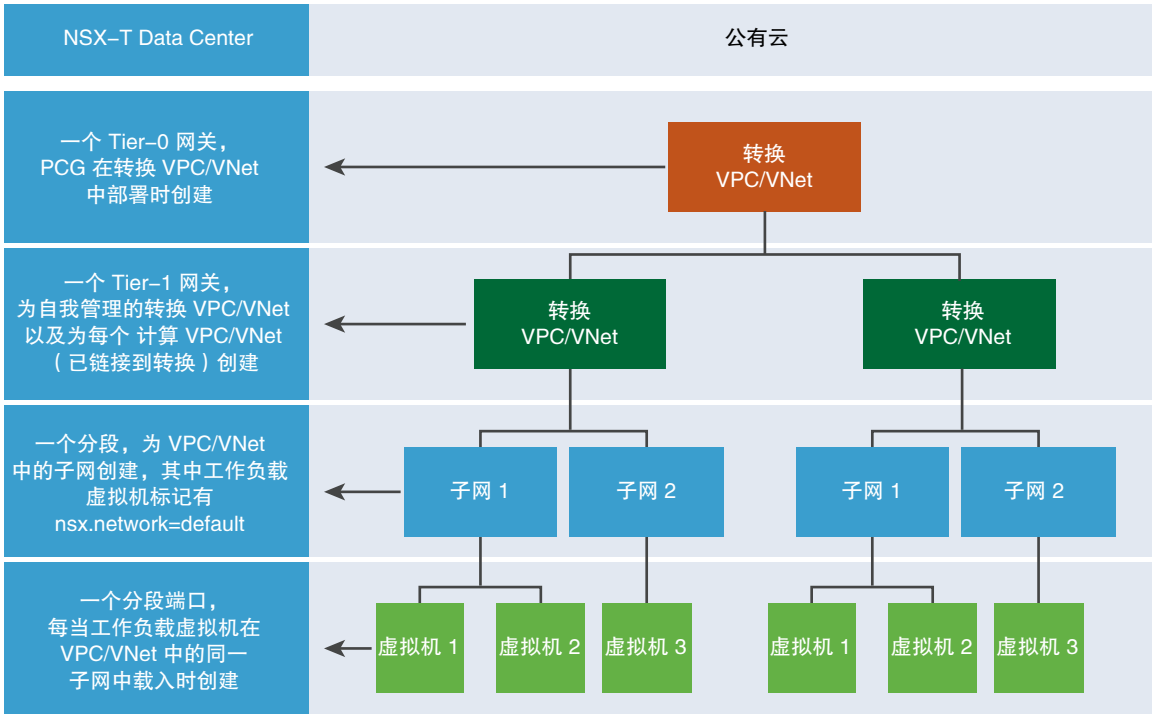


表 11-6. 自动创建的网络实体

载入任务	在 NSX-T Data Center 中创建的逻辑实体
在转换 VPC/VNet 上部署的 PCG	■ Tier-0 网关 ■ 基础架构分段（默认 VLAN 交换机） ■ Tier-1 路由器
链接到转换 VPC/VNet 的计算 VPC 或 VNet	■ Tier-1 路由器
安装有 NSX 代理的工作负载虚拟机在计算或自我管理 VPC/VNet 的子网中标记有“nsx.network:default”键:值	■ 为计算或自我管理 VPC 或 Vnet 的此特定子网创建分段 ■ 为安装有 NSX 代理的每个已标记工作负载虚拟机创建混合端口
在计算或自我管理 VPC/VNet 的同一子网中标记多个工作负载虚拟机	■ 为安装有 NSX 代理的每个已标记工作负载虚拟机创建混合端口

转发策略

为计算 VPC/VNet（包括自我管理转换 VPC/VNet）设置以下三个转发规则：

- 通过公有云网络（底层网络）访问同一计算 VPC 的任何 CIDR
- 通过公有云网络（底层网络）路由与公有云元数据服务有关的流量

- 通过 NSX-T Data Center 网络（覆盖网络），路由不在计算 VPC/VNet 的 CIDR 块中的所有内容或者已知服务

自动创建的云原生安全组

在公有云中，会创建云原生安全组。

公有云配置

在 AWS 中：

- 在 AWS VPC 中，新的 A 型记录集使用名称 `nsx-gw.vmware.local` 添加到 Amazon Route 53 中的私有托管区域中。映射到此记录的 IP 地址与 AWS 使用 DHCP 分配的 PCG 的管理 IP 地址匹配，且对于每个 VPC 都是不同的。Amazon Route 53 中私有托管区域中的此 DNS 条目由 NSX Cloud 用于解析 PCG 的 IP 地址。

  注 使用在 Amazon Route 53 中私有托管区域中定义的自定义 DNS 域名时，对于 AWS 中的 VPC 设置，**DNS 解析**和 **DNS 主机名**属性必须设置为**是**。

- 为 PCG 的上行链路接口创建一个辅助 IP。AWS 弹性 IP 与此辅助 IP 地址相关联。此配置适用于 SNAT。

在 AWS 和 Microsoft Azure 中：

gw 安全组应用于相应的 PCG 接口。

表 11-7. NSX Cloud 为 PCG 接口创建的公有云安全组

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

表 11-8. NSX Cloud 为工作负载虚拟机创建的公有云安全组

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

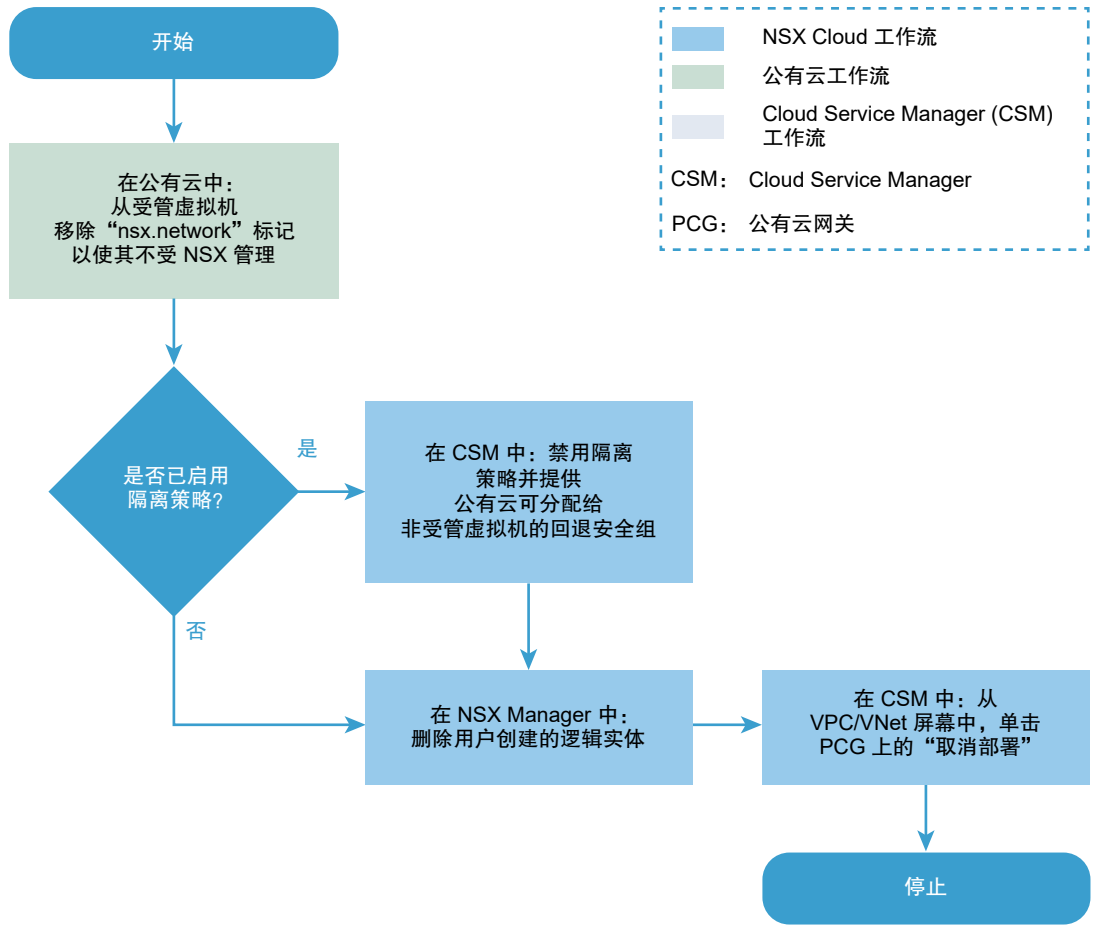
取消部署 PCG

请参阅以下流程图，了解取消部署 PCG 涉及的步骤。

取消部署 PCG 之前，必须执行以下操作：

- 确保 VPC 或 VNet 中的工作负载虚拟机不受 NSX 管理。
- 禁用隔离策略。
- 删除用户创建的且与 PCG 关联的所有逻辑实体。

图 11-4. 取消部署 PCG



步骤

1 取消标记公有云中的虚拟机

所有虚拟机必须为非受管虚拟机，才可取消部署 PCG。

2 禁用已启用的隔离策略

如果隔离策略先前已启用，必须将其禁用才能取消部署 PCG。

3 删除用户创建的逻辑实体

必须删除用户创建的且与 PCG 关联的所有逻辑实体。

4 从 CSM 取消部署

要在满足必备条件后取消部署 PCG，请在 CSM 中，从**云 > <Public_Cloud> > <VNet/VPC>** 单击取消部署网关。

取消标记公有云中的虚拟机

所有虚拟机必须为非受管虚拟机，才可取消部署 PCG。

在公有云中转到 VPC 或 VNet，然后从受管虚拟机中移除 `nsx.network` 标记。

禁用已启用的隔离策略

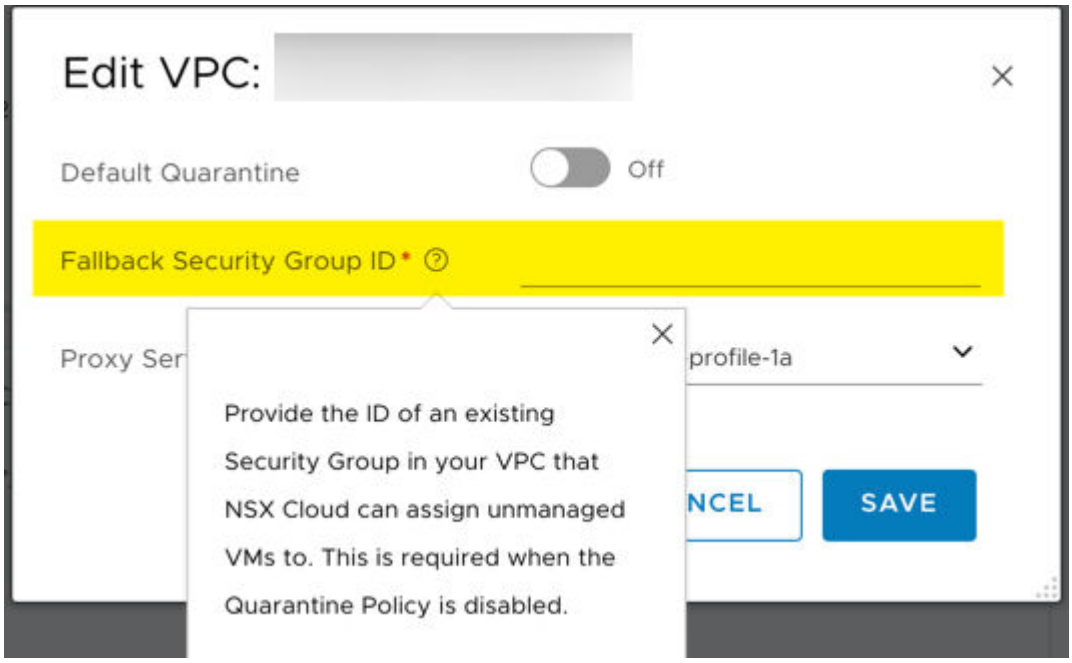
如果隔离策略先前已启用，必须将其禁用才能取消部署 PCG。

启用隔离策略时，会为虚拟机分配 NSX Cloud 定义的安全组。如果取消部署 PCG，则需要禁用隔离策略并指定将虚拟机从 NSX Cloud 安全组中移除时可将其分配到的回退安全组。

注 回退安全组必须是公有云中用户定义的现有安全组。不能使用任何 NSX Cloud 安全组作为回退安全组。有关 NSX Cloud 安全组列表，请参见自动创建的逻辑实体和云原生安全组。

对要从中取消部署 PCG 的 VPC 或 VNet 禁用隔离策略：

- 在 CSM 中转到 VPC 或 VNet。
- 从**操作 > 编辑配置**，关闭**默认隔离**的设置。
- 为要将虚拟机分配到的回退安全组输入一个值。



- 此 VPC 或 VNet 中的所有非受管虚拟机或隔离虚拟机都会分配有该回退安全组。
- 如果所有虚拟机为非受管虚拟机，则将其分配到回退安全组。

- 如果禁用隔离策略时存在受管虚拟机，这些虚拟机将保留 NSX Cloud 为其分配的安全组。首次从此类虚拟机中移除 `nsx.network` 标记以使其不受 NSX 管理时，也会为其分配回退安全组。

注 有关启用和禁用隔离策略的说明以及所产生影响的详细信息，请参见 NSX-T Data Center 管理指南中的**管理隔离策略**。

删除用户创建的逻辑实体

必须删除用户创建的且与 PCG 关联的所有逻辑实体。

识别与 PCG 关联的实体并将其删除。

注 请勿删除自动创建的逻辑实体。从 CSM 单击**取消部署网关**后，会自动删除它们。有关自动创建的逻辑实体列表，请参见自动创建的逻辑实体和云原生安全组。

从 CSM 取消部署

要在满足必备条件后取消部署 PCG，请在 CSM 中，从**云 > <Public_Cloud> > <VNet/VPC>** 单击取消部署网关。

1 登录到 CSM 并转到公有云：
   - 如果使用的是 AWS，请转到**云 > AWS > VPC**。单击部署并运行一个或一对 PCG 的 VPC。
   - 如果使用的是 Microsoft Azure，请转到**云 > Azure > VNet**。单击部署并运行一个或一对 PCG 的 VNet。
2 单击取消部署网关。

取消部署 PCG 后，将自动移除 NSX Cloud 创建的默认实体。