NSX-T 安装指南

VMware NSX-T Data Center 1.1

vmware®

您可以从 VMware 网站下载最新的技术文档：
https://docs.vmware.com/cn/。
VMware 网站还提供了最近的产品更新。
如果您对本文档有任何意见或建议，请将反馈信息发送至：
docfeedback@vmware.com

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

北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

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

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

版权所有 © 2017 VMware, Inc. 保留所有权利。 版权和商标信息。

目录

VMware, Inc. 保留所有权利。

VMware, Inc. 保留所有权利。

NSX-T 安装指南

NSX-T 安装指南 说明了如何安装 VMware NSX-T ® 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 的用户。本文档中的信息是为熟悉虚拟机技术和虚拟数据中心操作且经验丰富的系统管理员编写的。本手册假定您熟悉虚拟机管理服务（如 VMware vSphere 5.5 或 6.0，包括 VMware ESX、vCenter Server 和 vSphere Web Client、VMware OVF Tool）或具有基于内核的虚拟机 (Kernel-Based Virtual Machine, KVM) 的其他虚拟机管理服务。

VMware 技术出版物术语表

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

VMware, Inc. 保留所有权利。

NSX-T 概述

1

与服务器虚拟化以编程方式创建、删除和还原基于软件的虚拟机 (VM) 以及拍摄虚拟机快照的方式大致相同，NSX-T 网络虚拟化也是以编程方式创建、删除和还原基于软件的虚拟网络以及拍摄虚拟网络快照。

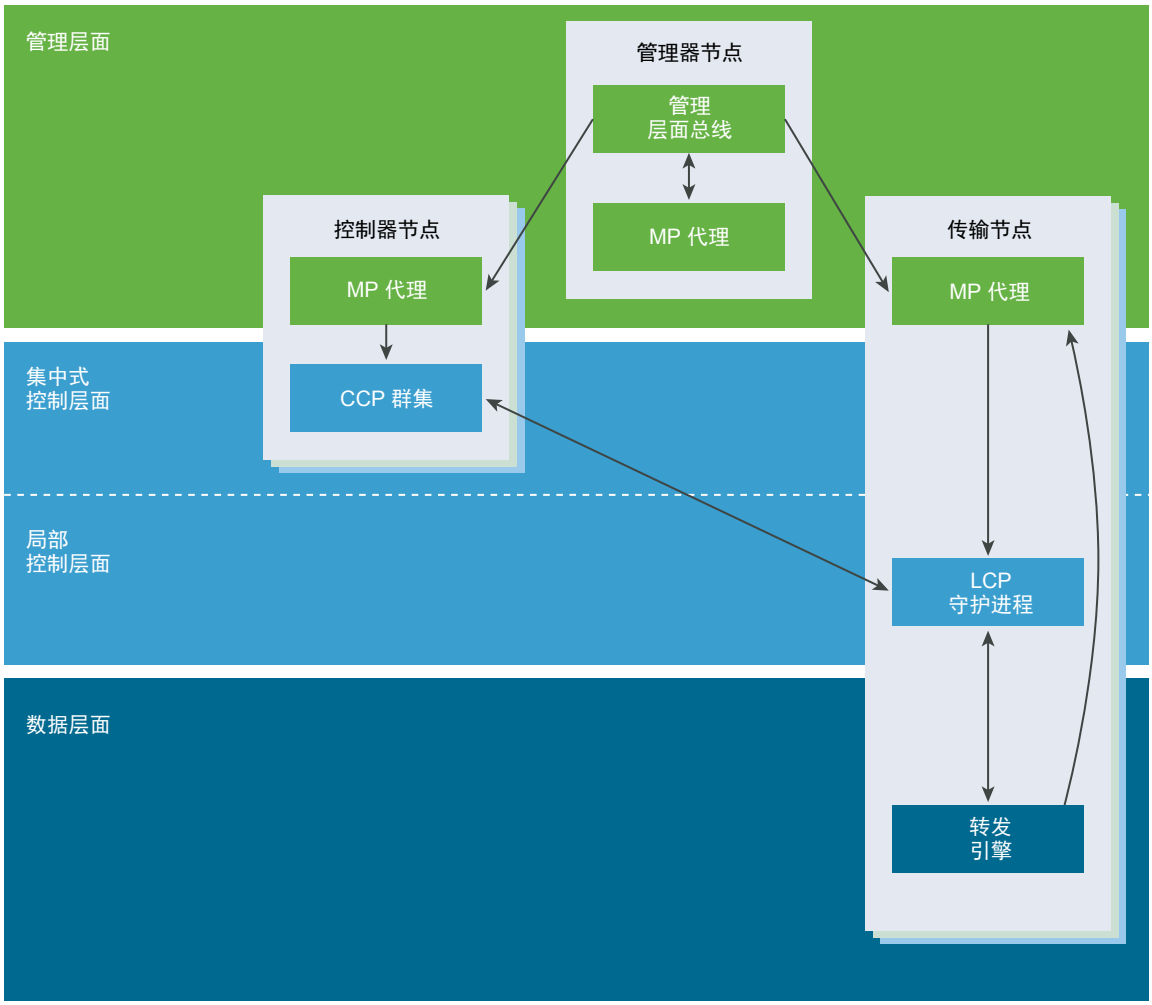
通过网络虚拟化，与网络管理程序功能等效的组件以软件形式再现一整套第 2 层至第 7 层网络服务（例如，交换、路由、访问控制、防火墙和 QoS）。因此，可通过编程方式任意组合这些服务，只需短短数秒，即可生成独一无二的独立虚拟网络。

NSX-T 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。这三个层面是作为位于三种类型的节点上的一组进程、模块和代理实现的：管理器、控制器和传输节点。

- 每个节点托管一个管理层面代理。
- NSX Manager 节点托管 API 服务。每个 NSX-T 安装支持单个 NSX Manager 节点，而不支持 NSX Manager 群集。
- NSX Controller 节点托管中央控制层面群集守护进程。
- 可以在同一物理服务器上托管 NSX Manager 和 NSX Controller 节点。

VMware, Inc. 保留所有权利。

- 传输节点托管本地控制层面守护进程和转发引擎。



本章讨论了以下主题：

- 数据层面
- 控制层面
- 管理层面
- NSX Manager
- NSX Controller
- 逻辑交换机
- 逻辑路由器
- NSX Edge
- 传输区域
- 重要概念

数据层面

根据控制层面填充的表执行无状态数据包转发/转换，向控制层面报告拓扑信息以及维护数据包级别统计信息。

数据层面是物理拓扑和状态的真实数据源，例如，VIF 位置、隧道状态，等等。如果要将数据包从一个位置移动到另一个位置，则需要位于数据层面。数据层面还维护多个链路/隧道的状态并处理它们之间的故障切换。每个数据包的性能是至关重要的，并具有非常严格的延迟或抖动要求。数据层面并不一定完全包含在内核、驱动程序、用户空间甚至特定用户空间进程中。数据层面限制为基于控制层面填充的表/规则的完全无状态转发。

数据层面可能还具有维护一定数量的功能状态（如 TCP 终止）的组件。这与控制层面管理的状态（如 MAC:IP 隧道映射）不同，因为控制层面管理的状态与如何转发数据包有关，而数据层面管理的状态仅限于如何处理负载。

控制层面

根据管理层面中的配置计算所有瞬间运行时状态，传播数据层面元素报告的拓扑信息以及将无状态配置推送到转发引擎。

有时，将控制层面描述为网络信令。如果要处置处理消息以便将数据层面保持静态用户配置，则需要位于控制层面（例如，控制层面负责响应虚拟机 (VM) 的 vMotion，而管理层面负责将虚拟机连接到逻辑网络）。通常，控制层面作为在数据层面元素之间映射拓扑信息的反射器，例如，VTEP 的 MAC/隧道映射。在其他情况下，控制层面处理从某些数据层面元素中收到的数据以配置（或重新配置）某些数据层面元素，例如，使用 VIF 定位器计算和确定正确的隧道子集网格。

控制层面处理的对象集包括 VIF、逻辑网络、逻辑端口、逻辑路由器、IP 地址，等等。

控制层面在 NSX-T 中拆分成两个部分：中央控制层面 (Central Control Plane, CCP) 和本地控制层面 (Local Control Plane, LCP)，前者在 NSX Controller 群集节点上运行，后者在它控制的数据层面的相邻传输节点上运行。中央控制层面根据管理层面中的配置计算某种瞬间运行时状态，并通过本地控制层面传播数据层面元素报告的信息。本地控制层面监控本地链路状态，根据数据层面和 CCP 中的更新计算最新的运行时状态，并将无状态配置推送到转发引擎。LCP 与托管它的数据层面元素存在相同的风险。

管理层面

管理层面提供系统的单个 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、控制和数据层面节点上执行操作任务。

对于 NSX-T，管理层面负责处理查询、修改和永久保留用户配置，而控制层面负责将该配置向下传播到正确的数据层面元素子集。这意味着，某些数据属于多个层面，具体取决于它处于哪个阶段。管理层面还处理从控制层面中查询最近的状态和统计信息，有时直接从数据层面中进行查询。

管理层面是配置的（逻辑）系统的唯一真实数据源，这是用户通过配置管理的。可以使用 REST API 或 NSX-T UI 进行更改。

VMware, Inc. 保留所有权利。

在 NSX 中，还会在所有群集和传输节点上运行管理层面代理 (Management Plane Agent, MPA)。引导配置就是一个示例用例，例如，中央管理节点地址凭据、软件包、统计信息和状态。MPA 可以相对独立于控制层面和数据层面运行，在其进程崩溃或停滞时可单独重新启动，但它们有时存在相同的风险，因为它们在相同的主机上运行。可以在本地和远程访问 MPA。MPA 在传输节点、控制节点和管理节点上运行以管理节点。在传输节点上，它还可以执行与数据层面相关的任务。

在管理层面上执行的任务包括：

- 永久保留配置（所需的逻辑状态）
- 输入验证
- 用户管理 - 角色分配
- 策略管理
- 后台任务跟踪

NSX Manager

NSX Manager 提供了图形用户界面 (Graphical User Interface, GUI) 和 REST API 以创建、配置和监控 NSX-T 组件，例如，控制器、逻辑交换机和 Edge 服务网关。

NSX Manager 是 NSX-T 体系的管理层面。NSX Manager 提供了聚合系统视图并且是 NSX-T 的集中式网络管理组件。它提供了一种方法以监控连接到 NSX-T 创建的虚拟网络的工作负载以及进行故障排除。它提供了以下内容的配置和编排：

- 逻辑网络组件 - 逻辑交换和路由
- 网络和 Edge 服务
- 安全服务和分布式防火墙 - NSX Manager 的内置组件或集成的第三方供应商可以提供 Edge 服务和安全服务。

NSX Manager 允许无缝编排内置和外部服务。所有安全服务（无论是内置还是第三方服务）都是由 NSX-T 管理层面部署和配置的。管理层面提供了单个窗口以查看服务可用性。它还简化了基于策略的服务链、上下文共享和服务间事件处理。这会简化安全状态审核，简化了应用基于身份的控制（例如，AD 和移动性配置文件）。

NSX Manager 还提供 REST API 入口点以供自动化使用。这种灵活的架构允许通过任何云管理平台、安全供应商平台或自动化框架自动完成所有配置和监控操作。

NSX-T 管理层面代理 (MPA) 是位于每个和所有节点（管理程序）上的 NSX Manager 组件。MPA 负责永久保留所需的系统状态，以及在传输节点和管理层面之间传送非流量控制 (Non-Flow-Controlling, NFC) 消息，例如，配置、统计信息、状态和实时数据。

NSX Controller

NSX Controller 是一种高级分布式状态管理系统，它控制虚拟网络和覆盖网络传输隧道。

NSX Controller 部署为一组高可用性的虚拟设备，它们负责在整个 NSX-T 架构中以编程方式部署虚拟网络。NSX-T 中央控制层面 (CCP) 在逻辑上与所有数据层面流量隔离，这意味着，控制层面中的任何故障不会影响现有的数据层面操作。流量不通过控制器传输；控制器负责为其他 NSX Controller 组件提供配置（如逻辑交换机、逻辑路由器和 Edge 配置）。数据传输的稳定性和可靠性是网络的核心问题。为了进一步提高高可用性和可扩展性，将在包含三个实例的群集中部署 NSX Controller。

逻辑交换机

NSX Edge 平台中的逻辑交换功能可以启动隔离的逻辑 L2 网络并提供虚拟机具有的相同灵活性和敏捷性。

虚拟数据中心的云部署具有跨多个租户的多种应用程序。出于安全和故障隔离的目的以及避免重叠的 IP 寻址问题，这些应用程序和租户需要互相隔离。端点（虚拟和物理）可以连接到逻辑分段并建立连接，而与它们在数据中心网络中的物理位置无关。这是通过将网络基础结构与 NSX-T 网络虚拟化提供的逻辑网络分离（即，将底层网络与覆盖网络分离）实现的。

逻辑交换机为第 2 层交换连接的多个主机提供了第 3 层 IP 访问能力。如果打算将某些逻辑网络限制为一组有限的主机，或者具有自定义连接要求，您可能会发现需要创建额外的逻辑交换机。

逻辑路由器

NSX-T 逻辑路由器提供南北向连接以允许租户访问公用网络，并在这些相同租户中的不同网络之间提供东西向连接。

逻辑路由器是为传统网络硬件路由器配置的一个分区。它复制硬件的功能，可在单个路由器中创建多个路由域。逻辑路由器执行物理路由器可以处理的一部分任务，每个逻辑路由器可以包含多个路由实例和路由表。使用逻辑路由器是一种有效的方法以最大限度提高路由器使用率，因为单个物理路由器中的一组逻辑路由器可以执行以前由很多设备执行的操作。

通过使用 NSX-T，可以创建两层逻辑路由器拓扑：顶层逻辑路由器是第 0 层，底层逻辑路由器是第 1 层。这种结构允许提供商管理员和租户管理员完全控制其服务和策略。提供商管理员控制和配置第 0 层路由和服务，租户管理员控制和配置第 1 层。在物理网络的第 0 层接口的北端，可以配置动态路由协议以便与物理路由器交换路由信息。第 0 层的南端连接到多个第 1 层路由层，并从这些层中接收路由信息。为了优化资源使用率，第 0 层不会将来自物理网络的所有路由推送到第 1 层，而是提供默认信息。

南向第 1 层路由层提供与租户管理员定义的逻辑交换机的接口，并在这些交换机之间提供单跃点路由功能。要从物理网络中访问第 1 层连接的子网，必须启用到第 0 层的路由重新分发。不过，不会在第 1 层和第 0 层之间运行传统路由协议（如 OSPF 或 BGP），所有路由将通过 NSX-T 控制层面。请注意，两层路由拓扑不是强制性的，如果不需要隔离提供商和租户，则可以创建单层拓扑，在这种情况下，逻辑交换机直接连接到第 0 层，而没有第 1 层。

逻辑路由器由两个可选的部分组成：一个分布式路由器 (Distributed Router, DR) 和一个或多个服务路由器 (Service Router, SR)。

DR 将跨虚拟机连接到该逻辑路由器的管理程序以及该逻辑路由器绑定到的 Edge 节点。从功能上讲，DR 负责连接到该逻辑路由器的逻辑交换机和/或逻辑路由器之间的单跃点分布式路由。SR 负责提供当前未以分布式方式实现的服务（如有状态 NAT）。

逻辑路由器始终具有 DR；如果满足任何以下条件，则还具有 SR：

- 逻辑路由器是第 0 层路由器，即使未配置有状态服务
- 逻辑路由器是链接到第 0 层路由器的第 1 层路由器，并且配置了没有分布式实现的服务（如 NAT、LB、DHCP）。

NSX-T 管理层面 (Management Plane, MP) 负责自动创建将服务路由器连接到分布式路由器的结构。MP 创建一个中转逻辑交换机并为其分配一个 VNI，然后在每个 SR 和 DR 上创建一个端口，将它们连接到中转逻辑交换机，并为 SR 和 DR 分配 IP 地址。

NSX Edge

NSX Edge 为 NSX-T 部署外部的网络提供路由服务和连接。

通过使用 NSX Edge，位于不同子网中的同一主机上的虚拟机或工作负载可以相互通信，而无需通过传统路由接口。

需要使用 NSX Edge 以从 NSX-T 域建立外部连接（通过第 0 层路由器并经由 BGP 或静态路由）。此外，如果需要在第 0 层或第 1 层逻辑路由器中使用网络地址转换 (NAT) 服务，则必须部署 NSX Edge。

NSX Edge 提供了常见的网关服务（如 NAT）和动态路由以将隔离的末端网络连接到共享（上行链路）网络。DMZ 和多租户云环境中包含常见的 NSX Edge 部署，其中 NSX Edge 为每个租户创建虚拟边界。

传输区域

传输区域控制逻辑交换机可以访问的主机。它可以跨一个或多个主机群集。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。

传输区域定义了一组可以通过物理网络基础结构相互通信的主机。该通信是通过一个或多个定义为虚拟隧道端点 (Virtual Tunnel Endpoint, VTEP) 的接口完成的。

如果两个传输节点位于相同的传输区域中，在这些传输节点上托管的虚拟机可以“看到”也位于该传输区域中的 NSX-T 逻辑交换机，从而可以连接到这些逻辑交换机。虚拟机可以通过该连接相互通信，并假定虚拟机具有第 2 层/第 3 层可访问性。如果虚拟机连接到位于不同传输区域中的交换机，则虚拟机无法相互通信。传输区域没有取代第 2 层/第 3 层可访问性要求，而是对该可访问性施加了一个限制。换句话说，属于同一传输区域是连接的一个必备条件。在满足该必备条件后，可以进行访问，但不会自动进行。要实现实际可访问性，第 2 层和（对于不同的子网）第 3 层网络必须正常运行。

如果某个节点包含至少一个主机交换机，则可以将其作为传输节点。在创建主机传输节点并随后将该节点添加到传输区域时，NSX-T 将在主机上安装一个主机交换机。对于主机所属的每个传输区域，将安装单独的主机交换机。主机交换机用于将虚拟机连接到 NSX-T 逻辑交换机以及创建 NSX-T 逻辑路由器上行链路和下行链路。

VMware, Inc. 保留所有权利。

重要概念

在文档和用户界面中使用的常见 NSX-T 概念。

控制层面	根据管理层面中的配置计算运行时状态。控制层面传播数据层面元素报告的拓扑信息，并将无状态配置推送到转发引擎。
数据层面	根据控制层面填充的表执行无状态数据包转发或转换。数据层面向控制层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 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。
架构节点	已在 NSX-T 管理层面中注册并安装了 NSX-T 模块的节点。要使管理程序主机或 NSX Edge 成为 NSX-T 覆盖网络的一部分，必须将该主机添加到 NSX-T 架构中。
架构配置文件	表示可以与 NSX Edge 群集关联的特定配置。例如，架构配置文件可能包含隧道属性以检测失效的对等项。
逻辑端口输出	到虚拟机或逻辑网络的入站网络流量称为输出，因为流量离开数据中心网络并进入虚拟空间。
逻辑端口输入	从虚拟机到数据中心网络的出站网络流量称为输入，因为流量进入物理网络。
逻辑路由器	NSX-T 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 API 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。这样，就可以迁移虚拟机，而不要求租户网络管理员进行重新配置。 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。
管理层面	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、控制和数据层面节点上执行操作任务。管理层面还负责查询、修改和永久保留用户配置。
NSX Controller 群集	部署为一组高可用性的虚拟设备，它们负责在整个 NSX-T 架构中以编程方式部署虚拟网络。
NSX Edge 群集	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。

VMware, Inc. 保留所有权利。

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-T 主机交换机或 KVM Open vSwitch	在管理程序上运行并提供物理流量转发的软件。主机交换机或 OVS 对租户网络管理员不可见，并提供每个逻辑交换机依赖的底层转发服务。要实现网络虚拟化，网络控制器必须为管理程序主机交换机配置网络流量表，它们构成租户管理员在创建和配置其逻辑交换机时定义的逻辑广播域。 每个逻辑广播域是使用隧道封装机制 Geneve 通过隧道传输虚拟机之间的流量以及虚拟机到逻辑路由器的流量实现的。网络控制器具有数据中心的全局视图，并确保在创建、移动或移除虚拟机时更新管理程序主机交换机流量表。
NSX Manager	托管 API 服务、管理层面和代理服务的节点。
Open vSwitch (OVS)	作为 XenServer、Xen、KVM 和其他基于 Linux 的管理程序中的管理程序主机交换机的开源软件交换机。NSX Edge 交换组件基于 OVS。
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。
第 0 层逻辑路由器	提供商逻辑路由器也称为物理网络的第 0 层逻辑路由器接口。第 0 层逻辑路由器是顶层路由器，可以实现为活动-活动或活动-备用服务路由器群集。该逻辑路由器运行 BGP 并作为物理路由器的对等项。在活动-备用模式下，该逻辑路由器还可以提供有状态服务。
第 1 层逻辑路由器	第 1 层逻辑路由器是第二层路由器，它连接到一个第 0 层逻辑路由器以建立北向连接，并连接到一个或多个覆盖网络以建立南向连接。第 1 层逻辑路由器可以是提供有状态服务的活动-备用服务路由器群集。
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。NSX-T 可以将所需的支持软件包部署到主机中，因为它知道在逻辑交换机上启用了哪些功能。
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。
VTEP	虚拟隧道端点。管理程序主机可以通过隧道端点加入 NSX-T 覆盖网络。NSX-T 覆盖网络将帧封装到数据包中并通过底层传输网络传输数据包，从而在现有的第 3 层网络架构上部署第 2 层网络。底层传输网络可以是另一个第 2 层网络，也可以跨第 3 层边界。VTEP 是进行封装和解封的连接点。

VMware, Inc. 保留所有权利。

安装准备工作

2

在安装 NSX-T 之前，请确保准备您的环境。

本章讨论了以下主题：

系统要求

NSX-T 具有有关硬件资源和软件版本的特定要求。

管理程序

表 2-1. 管理程序要求

管理程序	版本	CPU 内核	内存
ESXi	■ 6.5 ■ 6.0 修补程序版本 P04	4	16 GB
RHEL KVM	7.1（仅限 3.10.0-229 内核）、7.2（仅限 3.10.0-327 内核）	4	16 GB
Ubuntu KVM	14.04.x（3.13 或 4.4 内核）、16.04.x（仅限 4.4 内核）	4	16 GB

对于 ESXi，NSX-T 不支持主机配置文件和 Auto Deploy 功能。

小心 在 RHEL 上，`yum update` 命令可能会更新内核版本并破坏与 NSX-T 的兼容性。在运行 `yum update` 时，请务必禁用内核更新。此外，在运行 `yum install` 后，还要确认 NSX-T 支持内核版本。

VMware, Inc. 保留所有权利。

NSX Manager 和 NSX Controller

表 2-2. NSX Manager 和 NSX Controller 资源要求

设备	内存	vCPU	磁盘空间
NSX Manager	16 GB	2	140 GB
NSX Controller	16 GB	2	120 GB

在 vSphere ESXi 5.5 和更高版本上支持 NSX Manager 和 NSX Controller 虚拟机。

NSX Edge

表 2-3. NSX Edge 资源要求

部署大小	内存	vCPU	磁盘空间
小型	4 GB	2	120 GB
中型	8 GB	4	120 GB
大型	16 GB	8	120 GB

表 2-4. NSX Edge 物理硬件要求

硬件	类型
CPU	■ Xeon 56xx (Westmere-EP) ■ Xeon E7-xxxx (Westmere-EX) ■ Xeon E5-xxxx (Sandy Bridge)
网卡	■ Intel 82599 ■ Intel X540

裸机 NSX Edge 系统要求

产品代码

- X520QDA1
- E10G42BT (X520-T2)
- E10G42BTDA (X520-DA2)
- E10G42BTDABLK
- X520DA1OCP
- X520DA2OCP
- E10G41BFSR (X520-SR1)
- E10G41BFSRBLK
- E10G42BFSR (X520-SR2)
- E10G42BFSRBLK

VMware, Inc. 保留所有权利。

- E10G41BFLR (X520-LR1)
- E10G41BFLRBL

网卡 PCI 设备 ID	说明
0x10F7	IXGBE_DEV_ID_82599_KX4
0x1514	IXGBE_DEV_ID_82599_KX4_MEZZ
0x1517	IXGBE_DEV_ID_82599_KR
0x10F8	IXGBE_DEV_ID_82599_COMBO_BACKPLANE
0x000C	IXGBE_SUBDEV_ID_82599_KX4_KR_MEZZ
0x10F9	IXGBE_DEV_ID_82599_CX4
0x10FB	IXGBE_DEV_ID_82599_SFP
0x11A9	IXGBE_SUBDEV_ID_82599_SFP
0x1F72	IXGBE_SUBDEV_ID_82599_RNDC
0x17D0	IXGBE_SUBDEV_ID_82599_560FLR
0x0470	IXGBE_SUBDEV_ID_82599_ECNA_DP
0x152A	IXGBE_DEV_ID_82599_BACKPLANE_FCOE
0x1529	IXGBE_DEV_ID_82599_SFP_FCOE
0x1507	IXGBE_DEV_ID_82599_SFP_EM
0x154D	IXGBE_DEV_ID_82599_SFP_SF2
0x154A	IXGBE_DEV_ID_82599_SFP_SF_QP
0x1558	IXGBE_DEV_ID_82599_QSFP_SF_QP
0x1557	IXGBE_DEV_ID_82599EN_SFP
0x10FC	IXGBE_DEV_ID_82599_XAUI_LOM
0x151C	IXGBE_DEV_ID_82599_T3_LOM
0x1528	IXGBE_DEV_ID_X540T
0x1560	IXGBE_DEV_ID_X540T1

NSX Manager 浏览器支持

表 2-5. NSX Manager 浏览器支持

浏览器	Windows 10	Windows 8.1	Windows 7	Ubuntu 12、14.04	Max OSX 10.9、10.10、10.11
Internet Explorer 11		是	是		
Firefox 50		是	是	是	是
Chrome 54	是	是	是	是	是
Safari 9					是
Microsoft Edge 25	是				

端口和协议

下图说明了 NSX-T 中的所有节点到节点通信路径，如何保护和验证这些路径以及用于建立相互身份验证的凭据的存储位置。

箭头指示启动通信的代理。默认情况下，所有证书是自签名证书。可以替换北向 API 证书和私钥。

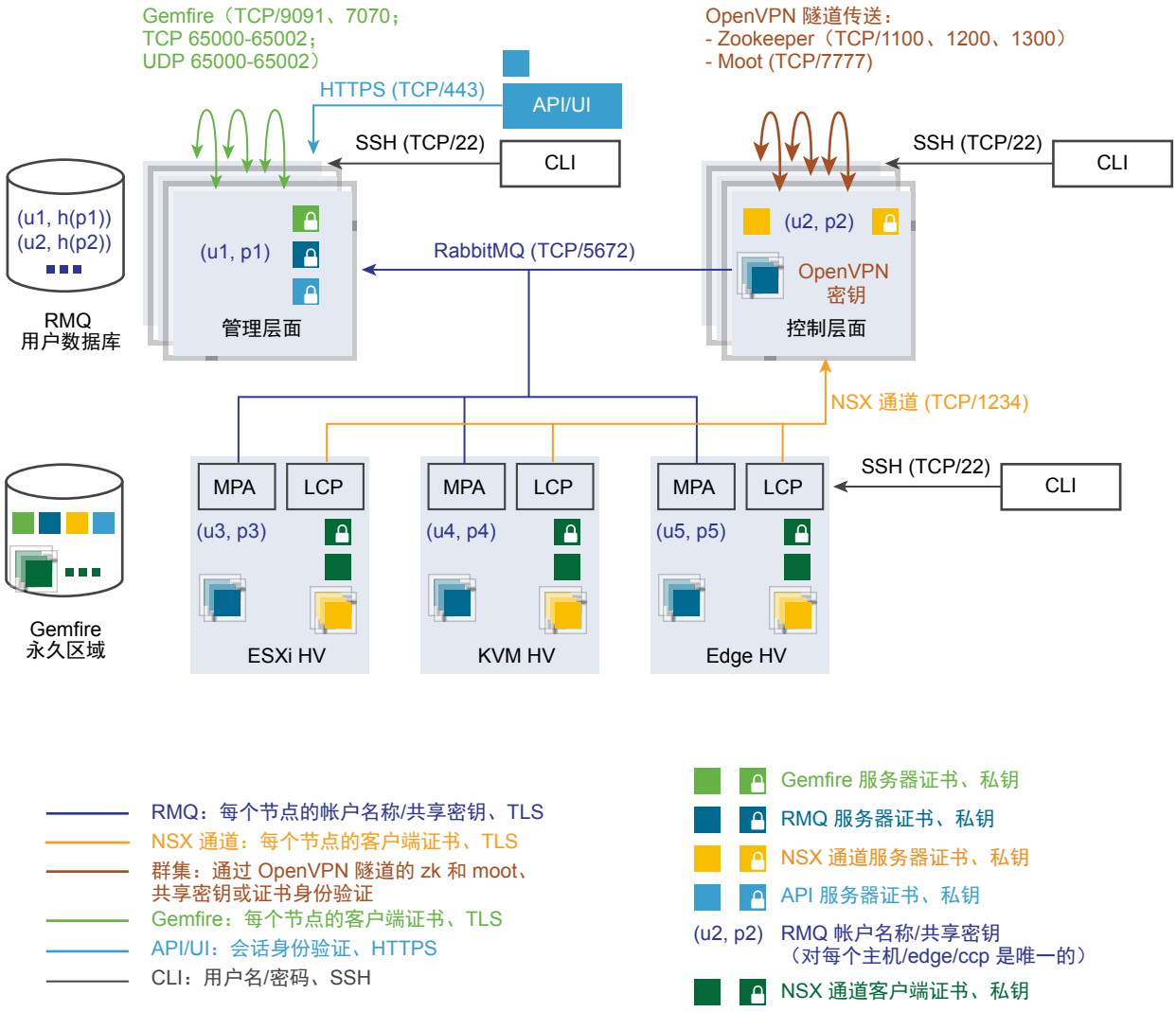
一些内部守护进程可以通过环回或 UNIX 域套接字进行通信：

- KVM：MPA、netcpa、nsx-agent、OVS
- ESX：netcpa、ESX-DP（在内核中）

在 RMQ 用户数据库 (db) 中，密码是使用不可逆的哈希函数进行哈希处理的。因此，h(p1) 是密码 p1 的哈希值。

右上角带有锁图标的彩色方块表示私钥。没有锁图标的方块是公用密钥。

VMware, Inc. 保留所有权利。



CCP	中央控制层面
LCP	本地控制层面
MP	管理层面
MPA	管理层面代理

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 2-6. NSX Manager 使用的 TCP 和 UDP 端口

源	目标	端口	协议	说明
任意	NSX Manager	22	TCP	SSH
任意	NSX Manager	123	UDP	NTP
任意	NSX Manager	443	TCP	NSX API 服务器
任意	NSX Manager	161	UDP	SNMP
任意	NSX Manager	8080	TCP	安装/升级 HTTP 存储库
任意	NSX Manager	5671	TCP	NSX 消息传递
NSX Manager	任意	22	TCP	SSH（上载支持包、备份等）
NSX Manager	任意	53	TCP	DNS
NSX Manager	任意	53	UDP	DNS
NSX Manager	任意	123	UDP	NTP
NSX Manager	任意	161、162	TCP	SNMP
NSX Manager	任意	161、162	UDP	SNMP
NSX Manager	任意	514	TCP	Syslog
NSX Manager	任意	514	UDP	Syslog
NSX Manager	任意	6514	TCP	Syslog
NSX Manager	任意	6514	UDP	Syslog
NSX Manager	任意	9000	TCP	Log Insight 代理
NSX Manager	任意	33434 - 33523	UDP	跟踪路由

NSX Controller 使用的 TCP 和 UDP 端口

NSX Controller 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 2-7. NSX Controller 使用的 TCP 和 UDP 端口

源	目标	端口	协议	说明
任意	控制器	22	TCP	SSH
任意	控制器	53	UDP	DNS
任意	控制器	123	UDP	NTP
任意	控制器	161	UDP	SNMP
任意	控制器	1100	TCP	Zookeeper 仲裁数
任意	控制器	1200	TCP	Zookeeper 主节点选举
任意	控制器	1300	TCP	Zookeeper 服务器
任意	控制器	1234	TCP	CCP-netcpa 通信
任意	控制器	7777	TCP	Moot RPC
任意	控制器	11000 - 11004	UDP	到其他群集节点的隧道。如果群集有 5 个以上结点，必须打开更多端口。
任意	控制器	33434 - 33523	UDP	跟踪路由
控制器	任意	22	TCP	SSH
控制器	任意	53	UDP	DNS
控制器	任意	53	TCP	DNS
控制器	任意	80	TCP	HTTP
控制器	任意	123	UDP	NTP
控制器	任意	5671	TCP	NSX 消息传递
控制器	任意	7777	TCP	Moot RPC
控制器	任意	9000	TCP	Log Insight 代理
控制器	任意	11000 - 11004	TCP	到其他群集节点的隧道。如果群集有 5 个以上结点，必须打开更多端口。
控制器	任意	8080	TCP	NSX 升级
控制器	任意	33434 - 33523	UDP	跟踪路由
控制器	任意	514	UDP	Syslog
控制器	任意	514	TCP	Syslog
控制器	任意	6514	TCP	Syslog

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。

VMware, Inc. 保留所有权利。

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 2-8. NSX Edge 使用的 TCP 和 UDP 端口

源	目标	端口	协议	说明
任意	Edge	22	TCP	SSH
任意	Edge	123	UDP	NTP
任意	Edge	161	UDP	SNMP
任意	Edge	67、68	UDP	DHCP
任意	Edge	1167	TCP	DHCP 后端
任意	Edge	3784、3785	UDP	BFD
任意	Edge	5555	TCP	公有云
任意	Edge	6666	TCP	公有云
任意	Edge	8080	TCP	NAPI、NSX 升级
任意	Edge	2480	TCP	Nestdb
Edge	任意	22	TCP	SSH
Edge	任意	53	UDP	DNS
Edge	任意	80	TCP	HTTP
Edge	任意	123	UDP	NTP
Edge	任意	161、162	UDP	SNMP
Edge	任意	161、162	TCP	SNMP
Edge	任意	179	TCP	BGP
Edge	任意	443	TCP	HTTPS
Edge	任意	514	TCP	Syslog
Edge	任意	514	UDP	Syslog
Edge	任意	1167	TCP	DHCP 后端
Edge	任意	1234	TCP	netcpa
Edge	任意	3000 - 9000	TCP	元数据代理
Edge	任意	5671	TCP	NSX 消息传递
Edge	任意	6514	TCP	Syslog over TLS
Edge	任意	33434 - 33523	UDP	跟踪路由

密钥管理器使用的 TCP 端口

密钥管理器使用特定的 TCP 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。

表 2-9. 密钥管理器使用的 TCP 端口

源	目标	端口	协议	说明
任意	密钥管理器	22	TCP	SSH
MP	密钥管理器	8992	TCP	管理层面与密钥管理器间的通信
管理程序	密钥管理器	8443	TCP	管理程序与密钥管理器间的通信
密钥管理器	任意	22	TCP	SSH

安装概述

通常，对于初始安装，过程顺序如下所示：

1 安装 NSX Manager。

2 安装 NSX Controller。

3 将 NSX Controller 加入管理层面。

4 初始化控制群集以创建主控制器。

即使在您的环境中只有一个 NSX Controller，也需要执行该步骤。

5 将 NSX Controller 加入控制群集。

6 在管理程序主机上安装 NSX-T 模块。

在安装 NSX-T 模块时，将在管理程序主机上创建证书。

7 将管理程序主机加入管理层面。

这会导致主机将其主机证书发送到管理层面。

8 安装 NSX Edge。

9 将 NSX Edge 加入管理层面。

10 创建传输区域和传输节点。

这会导致在每个主机上创建 NSX-T 主机交换机。此时，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。

这是建议的顺序，但该顺序不是必需的。

可以随时安装 NSX Manager。

可以随时安装 NSX Controller 并加入管理层面。

可以在加入管理层面之前在管理程序主机上安装 NSX-T 模块，也可以使用**架构 > 主机 > 添加 (Fabric > Hosts > Add)** UI 或 `POST fabric/nodes` API 同时执行这两个过程。

NSX Controller、NSX Edge 和具有 NSX-T 模块的主机可以随时加入管理层面。

VMware, Inc. 保留所有权利。

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 Controller、NSX Edge 和主机加入管理层面时，将自动向 NSX Controller、NSX Edge 和主机推送 NSX-T 逻辑实体和配置状态。

有关详细信息，请参阅《 NSX-T 管理指南》。

VMware, Inc. 保留所有权利。

使用 KVM

3

NSX-T 以两种方式支持 KVM：1) 作为主机传输节点以及 2) 作为 NSX Manager 和 NSX Controller 的主机。

本章讨论了以下主题：

- 设置 KVM
- 在 KVM CLI 中管理客户机虚拟机

设置 KVM

如果打算将 KVM 作为传输节点或 NSX Manager 和 NSX Controller 客户机虚拟机主机，但尚未设置 KVM，您可以使用此处介绍的过程。

步骤

1 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`

RHEL	`yum groupinstall "Virtualization Hypervisor"`
	`yum groupinstall "Virtualization Client"`
	`yum groupinstall "Virtualization Platform"`
	`yum groupinstall "Virtualization Tools"`

2 检查硬件虚拟化功能。

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

输出应包含 vmx。

3 确保安装了 KVM 模块。

Linux 发布版本	命令

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

RHEL	`lsmod | grep kvm`
	
	`kvm_intel  53484  6`
	`kvm  316506  1 kvm_intel`

4 （要将 KVM 作为 NSX Manager 或 NSX Controller 主机）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 文件：
	
	`auto lo`
	`iface lo inet loopback`
	
	`auto eth0`
	`iface eth0 inet manual`
	
	`auto br0`
	`iface br0 inet dhcp`
	`  bridge_ports eth0`

RHEL	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-br0 文件：
	
	`DEVICE="br0"`
	`  BOOTPROTO="dhcp"`
	`  NM_CONTROLLED="no"`
	`  ONBOOT="yes"`
	`  TYPE="Bridge"`

5 （要将 KVM 作为传输节点）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。

配置的接口比上一步多一个。

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 文件：
	`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	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 文件：
	`DEVICE="br0"`
	`  BOOTPROTO="dhcp"`
	`  NM_CONTROLLED="no"`
	`  ONBOOT="yes"`
	`  TYPE="Bridge"`

重要 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，将自动创建网桥接口“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 address>
netmask <subnet mask>
mtu 1600
down ifconfig nsx-vtep0.0 down
up ifconfig nsx-vtep0.0 up
```

在 RHEL 中，nsxa 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
```

6 要使网络更改生效，请重新启动网络或重新引导 Linux 服务器。

7 准备主机以进行核心转储。

Linux 发布版本	准备以进行核心转储

RHEL	运行以下命令：
	`mkdir /var/cores`
	`chmod 1777 /var/cores`
	`echo "kernel.core_pattern = /var/cores/core.%e.%t.%p" >> /etc/sysctl.conf`
	`sysctl –p`
	在 /etc/security/limits.conf 中添加以下几行：
	`* soft core unlimited`
	`* hard core unlimited`
	`root soft core unlimited`
	`root hard core unlimited`

在 KVM CLI 中管理客户机虚拟机

可以将 NSX Manger 和 NSX Controller 安装为 KVM 虚拟机。此外，还可以将 KVM 作为 NSX 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 命令以快速入门。

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

```
# 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)
```

VMware, Inc. 保留所有权利。

NSX Manager 安装

4

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 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 的管理组件。

在 vSphere ESXi 或 KVM 上支持 NSX Manager。您只能安装一个 NSX Manager 实例。可以使用 vSphere vSphere High Availability (HA) 功能确保 NSX Manager 的可用性。在 ESXi 上，建议将 NSX Manager 设备安装在共享存储上。vSphere HA 需要使用共享存储，以便可以在原始主机出现故障的情况下在其他主机上重新启动 NSX Manager 设备。

NSX Manager 支持以下部署方法：

- OVA/OVF
- QCOW2

NSX Manager 必须具有静态 IP 地址。您无法在安装后更改该 IP 地址。

NSX-T 设备具有以下密码复杂性要求：

- 至少 8 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

VMware, Inc. 保留所有权利。

即使密码不符合复杂性要求，安装也会成功。如果在部署期间没有为 **admin** 用户指定足够复杂的密码，您必须在部署后以 **admin** 身份登录并响应提示以更改密码。如果 **root** 用户也没有足够复杂的密码，请在以 **admin** 身份登录时使用以下命令更改密码：

```
set user root password <password>
```

注 在管理器全新安装时，在重新引导时，或者在首次登录出现提示时更改 **admin** 密码后，管理器可能需要几分钟的时间才会启动。

在设置了足够复杂的密码后，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。

在安装 NSX Manager 时，请选择不包含下划线的主机名。如果指定包含下划线的主机名，在部署后，设备将使用默认主机名，如 nsx-manager。

重要 NSX 组件虚拟机安装包括 VMware Tools。NSX 设备不支持移除或升级 VMware Tools。

本章讨论了以下主题：

- 使用 vSphere Web Client 在 ESXi 上安装 NSX Manager
- 使用命令行 OVF Tool 在 ESXi 上安装 NSX Manager
- 在 KVM 上安装 NSX Manager

使用 vSphere Web Client 在 ESXi 上安装 NSX Manager

您可以使用 vSphere Web Client 将 NSX Manager 部署为虚拟设备。

注 建议您使用 vSphere Web Client 而不是 vSphere Client。如果在您的环境中没有 vCenter Server，请使用 `ovftool` 部署 NSX Manager。请参阅使用命令行 OVF Tool 在 ESXi 上安装 NSX Manager。

前提条件

- 确认满足系统要求。请参阅系统要求。
- 确认打开了所需的端口。请参阅端口和协议。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。大多数部署将 NSX 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 设备到其他网络的静态路由。准备 NSX 设备进行通信时使用的管理虚拟机端口组。
- 计划您的 IPv4 IP 地址方案。在该 NSX-T 版本中，不支持 IPv6。

步骤

1 找到 NSX Manager OVA 或 OVF 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 Web Client 中，启动**部署 OVF 模板 (Deploy OVF template)**向导并导航或链接到 .ova 文件。

3 输入 NSX Manager 的名称，然后选择一个文件夹或数据中心。

键入的名称将显示在清单中。

将使用选定的文件夹将权限应用于 NSX Manager。

4 选择一个数据存储以存储 NSX Manager 虚拟设备文件。

5 如果在 vCenter 中进行安装，请选择一个主机或群集以在其中部署 NSX Manager 设备。

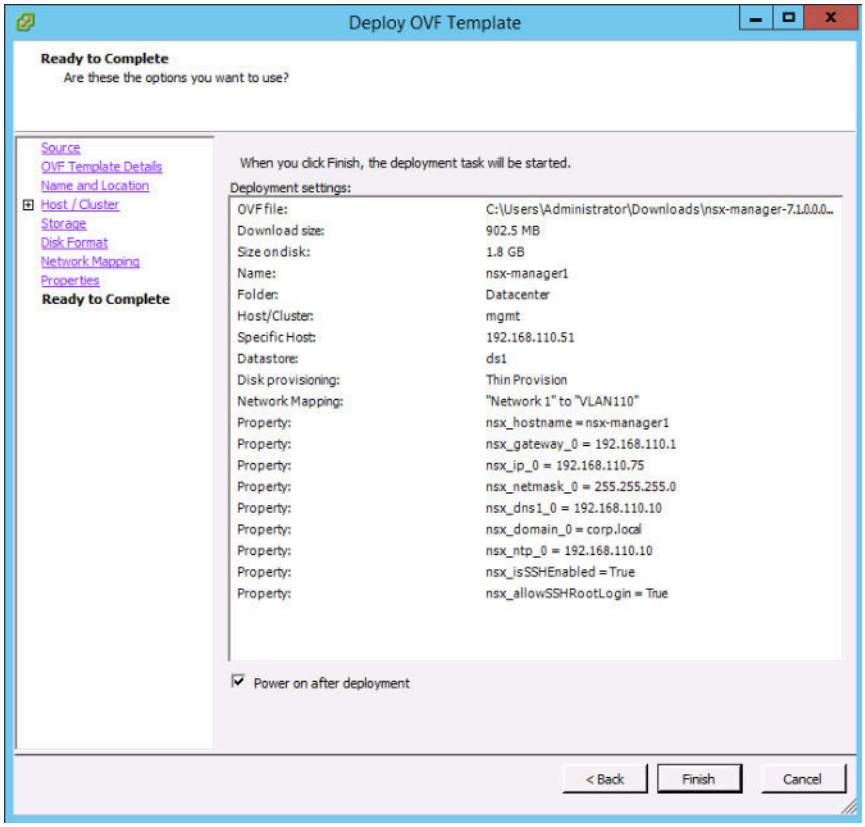
通常，应将 NSX Manager 放在提供网络管理实用程序的群集中。

6 为 NSX Manager 选择端口组或目标网络。

例如，如果使用 vSphere Distributed Switch，您可以将 NSX Manager 放在名为 Mgmt_VDS - Mgm 的端口组上。

7 设置 NSX Manager 密码和 IP 设置。

例如，在配置所有选项后，该屏幕显示最终检查屏幕。



8 为了获得最佳性能，请为 NSX 组件预留内存。

即使内存过量使用，内存预留也能保证主机为虚拟机预留的物理内存量下限。将预留设置为某个级别，以确保 NSX 组件具有足够的内存以高效地运行。请参阅系统要求。

打开 NSX 组件控制台以跟踪引导过程。

在完全引导 NSX 组件后，以 admin 身份登录到 CLI 并运行 `get interface eth0` 命令以验证是否按预期方式应用了 IP 地址。

```
nsx-component> get interface eth0
Interface: eth0
  Address: 192.168.110.25/24
  MAC address: 00:50:56:86:7b:1b
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

确保 NSX 组件具有所需的连接。

- 确保您可以 ping 通 NSX 组件。
- 确保 NSX 组件可以 ping 通其默认网关。
- 确保 NSX 组件可以 ping 通位于与 NSX 组件相同的网络中的管理程序主机。
- 确保 NSX 组件可以 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 组件。

如果未建立连接，请确保网络适配器位于正确的网络或 VLAN 中。

后续步骤

通过支持的 Web 浏览器连接到 NSX Manager GUI。URL 是 https://<NSX Manager IP 地址或主机名>。例如：https://192.168.110.75。

注 您必须使用 HTTPS。不支持 HTTP。

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，您可以使用 VMware OVF Tool，这是一个命令行实用程序。

为了安全起见，将默认禁用 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 但不启用 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。请参阅系统要求。
- 确认打开了所需的端口。请参阅端口和协议。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。大多数部署将 NSX 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 设备到其他网络的静态路由。准备 NSX 设备进行通信时使用的管理虚拟机端口组。
- 计划您的 IPv4 IP 地址方案。在该 NSX-T 版本中，不支持 IPv6。

步骤

- （对于单独的主机）使用相应的参数运行 ovftool 命令。例如，

```
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_ip_0=192.168.110.75
--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|False>
--prop:nsx_allowSSHRootLogin=<True|False>
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-manager
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:<password>@192.168.110.51
Deploying to VI: vi://root:<password>@192.168.110.51
Transfer Completed
Powering on VM: nsx-manager
Task Completed
Warning:
 - No manifest entry found for: 'nsx-<component>.ovf'.
 - File is missing from the manifest: 'nsx-<component>.ovf'.
 - ExtraConfig options exists in source.
 - Skipping monitor as the --X:waitForIp option is not given.
Completed successfully
```

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

```
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_ip_0=192.168.110.75
--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|False>
--prop:nsx_allowSSHRootLogin=<True|False>
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-manager
nsx-<component>.ova
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.110.51
```

```
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-manager
Task Completed
Warning:
 - No manifest entry found for: 'nsx-<component>.ovf'.
 - File is missing from the manifest: 'nsx-<component>.ovf'.
 - ExtraConfig options exists in source.
 - Skipping monitor as the --X:waitForIp option is not given.
Completed successfully
```

- 为了获得最佳性能，请为 NSX 组件预留内存。

  即使内存过量使用，内存预留也能保证主机为虚拟机预留的物理内存量下限。将预留设置为某个级别，以确保 NSX 组件具有足够的内存以高效地运行。请参阅系统要求。

打开 NSX 组件控制台以跟踪引导过程。

在完全引导 NSX 组件后，以 admin 身份登录到 CLI 并运行 `get interface eth0` 命令以验证是否按预期方式应用了 IP 地址。

```
nsx-component> get interface eth0
Interface: eth0
  Address: 192.168.110.25/24
  MAC address: 00:50:56:86:7b:1b
```

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

确保 NSX 组件具有所需的连接。

- 确保您可以 ping 通 NSX 组件。
- 确保 NSX 组件可以 ping 通其默认网关。
- 确保 NSX 组件可以 ping 通位于与 NSX 组件相同的网络中的管理程序主机。
- 确保 NSX 组件可以 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 组件。

如果未建立连接，请确保网络适配器位于正确的网络或 VLAN 中。

后续步骤

通过支持的 Web 浏览器连接到 NSX Manager GUI。URL 是 https://<NSX Manager IP 地址或主机名>。例如：https://192.168.110.75。

注 您必须使用 HTTPS。不支持 HTTP。

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。请参阅设置 KVM。
- 在 KVM 主机上部署 QCOW2 映像的权限。
- 确认满足系统要求。请参阅系统要求。
- 确认打开了所需的端口。请参阅端口和协议。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。大多数部署将 NSX 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 设备到其他网络的静态路由。准备 NSX 设备进行通信时使用的管理虚拟机端口组。
- 计划您的 IPv4 IP 地址方案。在该 NSX-T 版本中，不支持 IPv6。

步骤

1 下载 NSX Manager QCOW2 映像，然后将其复制到所需的位置。

2 （仅限 Ubuntu）将当前登录的用户添加为 libvirtd 用户：

```
adduser $USER libvirtd
```

3 在保存 QCOW2 映像的同一目录中，创建一个名为 guestinfo 的文件（无文件扩展名），然后使用 NSX Manager 虚拟机的属性填充该文件。

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_allowSSHRootLogin" oe:value="True"/>
         <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
         <Property oe:key="nsx_dns1_0" oe:value="192.168.110.10"/>
         <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
         <Property oe:key="nsx_gateway_0" oe:value="192.168.110.1"/>
         <Property oe:key="nsx_hostname" oe:value="nsx-manager1"/>
         <Property oe:key="nsx_ip_0" oe:value="192.168.110.19"/>
         <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
         <Property oe:key="nsx_netmask_0" oe:value="255.255.255.0"/>
         <Property oe:key="nsx_ntp_0" oe:value="192.168.110.10"/>
         <Property oe:key="nsx_passwd_0" oe:value="<password>"/>
   </PropertySection>
</Environment>
```

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 但不启用 nsx_allowSSHRootLogin，您可以通过 SSH 访问 NSX Manager，但无法以 root 身份登录。

4 使用 guestfish 将 guestinfo 文件写入到 QCOW2 映像中。

如果要创建多个管理器，请为每个管理器创建单独的 QCOW2 映像副本。在将 guestinfo 信息写入到 QCOW2 映像后，无法覆盖该信息。

```
guestfish --rw -i -a nsx-manager1-build.qcow2 upload guestinfo /config/guestinfo
```

5 使用 virt-install 命令部署 QCOW2 映像。

```
user@ubuntu1604:/var/lib/libvirt/images$ sudo virt-install --import --name nsx-manager1 --ram 16348
--vcpus 4 --network=bridge:br0,model=e1000 --disk path=/var/lib/libvirt/images/nsx-
manager-1.1.0.0.0.4446302.qcow2,format=qcow2 --nographics

Starting install...
Creating domain...       |    0 B     00:01
Connected to domain nsx-manager1
```

```
Escape character is ^]

nsx-manager1 login:
```

在 NSX Manager 引导后，将显示 NSX Manager 控制台。

6 为了获得最佳性能，请为 NSX 组件预留内存。

即使内存过量使用，内存预留也能保证主机为虚拟机预留的物理内存量下限。将预留设置为某个级别，以确保 NSX 组件具有足够的内存以高效地运行。请参阅系统要求。

打开 NSX 组件控制台以跟踪引导过程。

在完全引导 NSX 组件后，等待 3 分钟，然后以 admin 身份登录到 CLI。将显示 EULA 屏幕。接受 EULA。然后，运行 `get interface eth0` 命令以验证是否按预期方式应用了 IP 地址。

```
nsx-component> get interface eth0
Interface: eth0
  Address: 192.168.110.25/24
  MAC address: 00:50:56:86:7b:1b
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

确保 NSX 组件具有所需的连接。

- 确保您可以 ping 通 NSX 组件。
- 确保 NSX 组件可以 ping 通其默认网关。
- 确保 NSX 组件可以 ping 通位于与 NSX 组件相同的网络中的管理程序主机。
- 确保 NSX 组件可以 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 组件。

如果未建立连接，请确保网络适配器位于正确的网络或 VLAN 中。

后续步骤

通过支持的 Web 浏览器连接到 NSX Manager GUI。URL 是 https://<NSX Manager IP 地址或主机名>。例如：https://192.168.110.75。

注 您必须使用 HTTPS。不支持 HTTP。

NSX Controller 安装和群集

5

NSX Controller 是一个高级分布式状态管理系统，它提供了控制层面功能以实现 NSX-T 逻辑交换和路由功能。它作为网络中的所有逻辑交换机的中央控制点，并维护有关所有主机、逻辑交换机和逻辑路由器的信息。NSX Controller 控制执行数据包转发的设备。这些转发设备称为虚拟交换机。虚拟交换机（如 NSX-T 主机交换机或 Open vSwitch (OVS)）位于 ESX 和其他管理程序（如 KVM）中。

NSX Controller 具有以下支持的部署方法：

- OVA/OVF
- QCOW2

在 ESX 或 KVM 上支持 NSX Controller。

不支持通过 PXE 引导的 NSX Controller 安装。

NSX Controller 必须具有静态 IP 地址。您无法在安装后更改该 IP 地址。

NSX-T 设备具有以下密码复杂性要求：

- 至少 8 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

即使密码不符合复杂性要求，安装也会成功。但在首次登录时，将提示您更改密码。

注　在设置了足够复杂的密码后，设备上的核心服务才会启动。

从 OVA 文件部署 NSX Controller 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。

在安装 NSX Manager 时，请选择不包含下划线的主机名。否则，主机名将设置为 localhost。

重要　NSX 组件虚拟机安装包括 VMware Tools。NSX 设备不支持移除或升级 VMware Tools。

VMware, Inc. 保留所有权利。

本章讨论了以下主题：

使用 GUI 在 ESXi 上安装 NSX Controller

如果希望进行交互式 NSX Controller 安装，您可以使用基于 UI 的虚拟机管理工具，例如，连接到 vCenter Server 的 vSphere Client。

要支持备份和还原，NSX Controller 设备必须具有静态管理 IP 地址。不支持使用 DHCP 分配管理 IP 地址。不支持更改管理 IP 地址。有关备份和还原信息，请参阅《 NSX-T 管理指南》。

您的密码必须符合密码强度限制。NSX-T 设备强制实施以下复杂性规则：

- 至少 8 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

对于 PXE 安装，您必须为 root 和 admin 用户密码提供使用 sha-512 算法加密的密码字符串。

如果密码不符合要求，安装也会成功。但在首次登录时，将提示您更改密码。

重要 在设置了足够复杂的密码后，设备上的核心服务才会启动。

重要 NSX 组件虚拟机安装包括 VMware Tools。NSX 设备不支持移除或升级 VMware Tools。

前提条件

- 确认满足系统要求。请参阅系统要求。
- 确认打开了所需的端口。请参阅端口和协议。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。大多数部署将 NSX 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 设备到其他网络的静态路由。准备 NSX 设备进行通信时使用的管理虚拟机端口组。

- 计划您的 IPv4 IP 地址方案。在该 NSX-T 版本中，不支持 IPv6。
- 用于在 ESXi 主机上部署 OVF 模板的权限。
- 选择不包含下划线的主机名。否则，主机名将设置为 *nsx-manager*。
- 可以部署 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。

步骤

1 找到 NSX Controller OVA 或 OVF 文件。

  将下载 URL 复制到计算机或下载 OVA 文件到计算机。

2 在管理工具中，启动**部署 OVF 模板 (Deploy OVF template)**向导并导航或链接到 .ova 文件。

3 输入 NSX Controller 的名称，然后选择一个文件夹或数据中心。

  键入的名称将显示在清单中。

  将使用选定的文件夹将权限应用于 NSX Controller。

4 选择一个数据存储以存储 NSX Controller 虚拟设备文件。

5 如果使用 vCenter，请选择一个主机或群集以在其中部署 NSX Controller 设备。

  通常，应将 NSX Controller 放在提供网络管理实用程序的群集中。

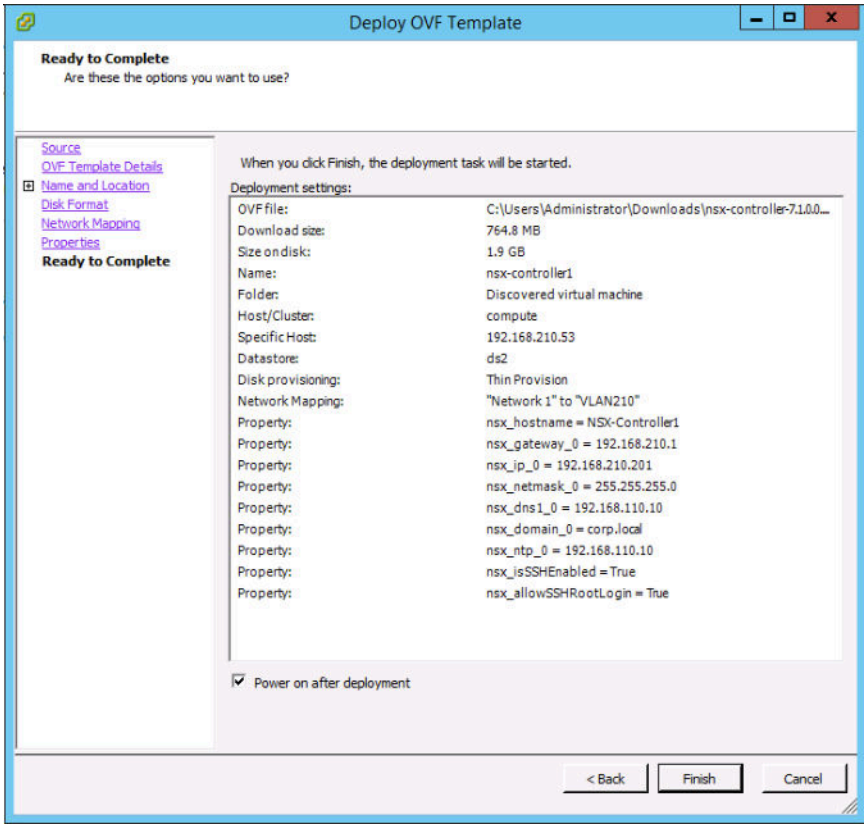
6 为 NSX Controller 选择端口组或目标网络。

  例如，如果使用 vSphere Distributed Switch，您可以将 NSX Controller 放在名为 Mgmt_VDS - Mgm 的端口组上。

VMware, Inc. 保留所有权利。

7 设置 NSX Controller 密码和 IP 设置。

例如，在配置所有选项后，该屏幕显示最终检查屏幕。



8 为了获得最佳性能，请为 NSX 组件预留内存。

即使内存过量使用，内存预留也能保证主机为虚拟机预留的物理内存量下限。将预留设置为某个级别，以确保 NSX 组件具有足够的内存以高效地运行。请参阅系统要求。

打开 NSX 组件控制台以跟踪引导过程。

在完全引导 NSX 组件后，以 admin 身份登录到 CLI 并运行 `get interface eth0` 命令以验证是否按预期方式应用了 IP 地址。

```
nsx-component> get interface eth0
Interface: eth0
  Address: 192.168.110.25/24
  MAC address: 00:50:56:86:7b:1b
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

确保 NSX 组件具有所需的连接。

- 确保您可以 ping 通 NSX 组件。
- 确保 NSX 组件可以 ping 通其默认网关。

- 确保 NSX 组件可以 ping 通位于与 NSX 组件相同的网络中的管理程序主机。
- 确保 NSX 组件可以 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 组件。

如果未建立连接，请确保网络适配器位于正确的网络或 VLAN 中。

后续步骤

将 NSX Controller 加入管理层面。请参阅将 NSX Controller 加入管理层面。

使用命令行 OVF Tool 在 ESXi 上安装 NSX Controller

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

为了安全起见，将默认禁用 nsx_isSSHEnabled 和 nsx_allowSSHRootLogin。如果禁用，则无法通过 SSH 访问或登录到 NSX Controller 命令行。如果启用 nsx_isSSHEnabled 但不启用 nsx_allowSSHRootLogin，您可以通过 SSH 访问 NSX Controller，但无法以 root 身份登录。

前提条件

- 确认满足系统要求。请参阅系统要求。
- 确认打开了所需的端口。请参阅端口和协议。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。大多数部署将 NSX 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 设备到其他网络的静态路由。准备 NSX 设备进行通信时使用的管理虚拟机端口组。
- 计划您的 IPv4 IP 地址方案。在该 NSX-T 版本中，不支持 IPv6。
- OVF Tool 4.0 或更高版本。

步骤

- （对于单独的主机）使用相应的参数运行 `ovftool` 命令。

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-controller
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--network="management"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.210
--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|False>
--prop:nsx_allowSSHRootLogin=<True|False>
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-controller
<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-controller
Task Completed
Warning:
 - No manifest entry found for: 'nsx-<component>.ovf'.
 - File is missing from the manifest: 'nsx-<component>.ovf'.
 - ExtraConfig options exists in source.
 - Skipping monitor as the --X:waitForIp option is not given.
Completed successfully
```

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

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-controller
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--network="management"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.210
--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|False>
--prop:nsx_allowSSHRootLogin=<True|False>
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
```

VMware, Inc. 保留所有权利。

```
--prop:nsx_hostname=nsx-controller
<path/url to nsx component ova>
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.110.51
```

```
Opening OVA source: nsx-<component>.ova
The manifest validates
Source is signed and the certificate validates
Opening VI target: vi://administrator%40vsphere.local@192.168.110.24:443/
Deploying to VI: vi://administrator%40vsphere.local@192.168.110.24:443/
Transfer Completed
Powering on VM: nsx-controller
Task Completed
Warning:
 - No manifest entry found for: 'nsx-<component>.ovf'.
 - File is missing from the manifest: 'nsx-<component>.ovf'.
 - ExtraConfig options exists in source.
 - Skipping monitor as the --X:waitForIp option is not given.
Completed successfully
```

- 为了获得最佳性能，请为 NSX 组件预留内存。

  即使内存过量使用，内存预留也能保证主机为虚拟机预留的物理内存量下限。将预留设置为某个级别，以确保 NSX 组件具有足够的内存以高效地运行。请参阅系统要求。

打开 NSX 组件控制台以跟踪引导过程。

在完全引导 NSX 组件后，以 admin 身份登录到 CLI 并运行 `get interface eth0` 命令以验证是否按预期方式应用了 IP 地址。

```
nsx-component> get interface eth0
Interface: eth0
  Address: 192.168.110.25/24
  MAC address: 00:50:56:86:7b:1b
  MTU: 1500
  Default gateway: 192.168.110.1
  Broadcast address: 192.168.110.255
  ...
```

确保 NSX 组件具有所需的连接。

- 确保您可以 ping 通 NSX 组件。
- 确保 NSX 组件可以 ping 通其默认网关。
- 确保 NSX 组件可以 ping 通位于与 NSX 组件相同的网络中的管理程序主机。
- 确保 NSX 组件可以 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 组件。

如果未建立连接，请确保网络适配器位于正确的网络或 VLAN 中。

VMware, Inc. 保留所有权利。

后续步骤

将 NSX Controller 加入管理层面。请参阅将 NSX Controller 加入管理层面。

在 KVM 上安装 NSX Controller

NSX Controller 作为网络中的所有逻辑交换机的中央控制点，并维护有关所有主机、逻辑交换机和分布式逻辑路由器的信息。

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。请参阅设置 KVM。
- 在 KVM 主机上部署 QCOW2 映像的权限。
- 确认满足系统要求。请参阅系统要求。
- 确认打开了所需的端口。请参阅端口和协议。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。大多数部署将 NSX 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 设备到其他网络的静态路由。准备 NSX 设备进行通信时使用的管理虚拟机端口组。
- 计划您的 IPv4 IP 地址方案。在该 NSX-T 版本中，不支持 IPv6。

步骤

1 下载 NSX Controller QCOW2 映像。

2 （仅限 Ubuntu）将当前登录的用户添加为 libvirtd 用户：

```
adduser $USER libvirtd
```

3 在保存 QCOW2 映像的同一目录中，创建一个名为 `guestinfo` 的文件（无文件扩展名），然后使用 NSX Controller 虚拟机的属性填充该文件。

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_allowSSHRootLogin" oe:value="True"/>
         <Property oe:key="nsx_cli_passwd_0" oe:value="<password>"/>
         <Property oe:key="nsx_dns1_0" oe:value="192.168.110.10"/>
         <Property oe:key="nsx_domain_0" oe:value="corp.local"/>
         <Property oe:key="nsx_gateway_0" oe:value="192.168.110.1"/>
         <Property oe:key="nsx_hostname" oe:value="nsx-Controller1"/>
         <Property oe:key="nsx_ip_0" oe:value="192.168.110.34"/>
```

VMware, Inc. 保留所有权利。

```
          <Property oe:key="nsx_isSSHEnabled" oe:value="True"/>
          <Property oe:key="nsx_netmask_0" oe:value="255.255.255.0"/>
          <Property oe:key="nsx_ntp_0" oe:value="192.168.110.10"/>
          <Property oe:key="nsx_passwd_0" oe:value="<password>"/>
   </PropertySection>
</Environment>
```

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 Controller 命令行。如果启用 nsx_isSSHEnabled 但不启用 nsx_allowSSHRootLogin，您可以通过 SSH 访问 NSX Controller，但无法以 root 身份登录。

4 使用 guestfish 将 `guestinfo` 文件写入到 QCOW2 映像中。

如果要创建多个控制器，请为每个控制器创建单独的 QCOW2 映像副本。在将 `guestinfo` 信息写入到 QCOW2 映像后，无法覆盖该信息。

```
guestfish --rw -i -a nsx-Controller1-build.qcow2 upload guestinfo /config/guestinfo
```

5 使用 `virt-install` 命令部署 QCOW2 映像。

```
user@ubuntu1604:/var/lib/libvirt/images$ sudo virt-install --import --name nsx-controller1 --ram
16348 --vcpus 4 --network=bridge:br0,model=e1000 --disk path=/var/lib/libvirt/images/nsx-
manager-1.1.0.0.0.4446302.qcow2,format=qcow2 --nographics

Starting install...
Creating domain...            |    0 B     00:01
Connected to domain nsx-Controller1
Escape character is ^]

nsx-Controller1 login:
```

在 NSX Controller 引导后，将显示 NSX Controller 控制台。

6 为了获得最佳性能，请为 NSX 组件预留内存。

即使内存过量使用，内存预留也能保证主机为虚拟机预留的物理内存量下限。将预留设置为某个级别，以确保 NSX 组件具有足够的内存以高效地运行。请参阅系统要求。

打开 NSX 组件控制台以跟踪引导过程。

在完全引导 NSX 组件后，以 admin 身份登录到 CLI 并运行 `get interface eth0` 命令以验证是否按预期方式应用了 IP 地址。

```
nsx-component> get interface eth0
Interface: eth0
  Address: 192.168.110.25/24
  MAC address: 00:50:56:86:7b:1b
```

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

确保 NSX 组件具有所需的连接。

- 确保您可以 ping 通 NSX 组件。
- 确保 NSX 组件可以 ping 通其默认网关。
- 确保 NSX 组件可以 ping 通位于与 NSX 组件相同的网络中的管理程序主机。
- 确保 NSX 组件可以 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 组件。

如果未建立连接，请确保网络适配器位于正确的网络或 VLAN 中。

后续步骤

将 NSX Controller 加入管理层面。请参阅将 NSX Controller 加入管理层面。

将 NSX Controller 加入管理层面

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

前提条件

确认安装了 NSX Manager。

步骤

1 打开到 NSX Manager 的 SSH 会话。

2 打开到每个 NSX Controller 设备的 SSH 会话。

例如，NSX-Controller1、NSX-Controller2 和 NSX-Controller3。

3 在 NSX Manager 上，运行 `get certificate api thumbprint` 命令。例如，

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

4 在每个 NSX Controller 设备上，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

VMware, Inc. 保留所有权利。

- NSX Manager 的密码

```
NSX-Controller1> join management-plane NSX-Manager username admin thumbprint <NSX-Manager's-
thumbprint>
Password for API user: <NSX-Manager's-password>
Node successfully registered and controller restarted
```

在每个控制器节点上运行该命令。

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

```
NSX-Controller1> get managers
- 192.168.110.47   Connected
```

在 NSX Manager 设备上，运行 `get management-cluster status` 命令并确保列出了 NSX Controller。

```
NSX-Manager> get management-cluster status
Number of nodes in management cluster: 1
- 192.168.110.47 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086) Online

Management cluster status: STABLE

Number of nodes in control cluster: 3
- 192.168.110.201 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.202 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
- 192.168.110.203 (UUID 45A8869B-BB90-495D-8A01-69B5FCC56086)
```

后续步骤

初始化控制群集。请参阅初始化控制群集以创建控制群集主控制器。

初始化控制群集以创建控制群集主控制器

在 NSX-T 部署中安装第一个 NSX Controller 后，您可以初始化控制群集。即使设置仅包含一个控制器节点的较小概念证明环境，也需要初始化控制群集。如果未初始化控制群集，则任何控制器都无法与管理程序主机进行通信。

前提条件

- 安装至少一个 NSX Controller。
- 将 NSX Controller 加入管理层面。
- 选择一个共享密钥密码。共享密钥密码是用户定义的共享密钥密码（例如，“secret123”）。对于群集中的三个节点，该密码必须是相同的。

步骤

1. 为 NSX Controller 打开一个 SSH 会话。
2. 运行 `set control-cluster security-model shared-secret` 命令，然后在出现提示时输入共享密钥密码。

3 运行 initialize control-cluster 命令。

该命令将该控制器指定为控制群集主控制器。

例如：

```
NSX-Controller1> initialize control-cluster
Control cluster initialization successful.
```

运行 get control-cluster status verbose 命令并确保 is master 和 in majority 为 true，status 为 active 以及 Zookeeper Server IP 为 reachable, ok。

```
nsx-controller1> get control-cluster status verbose
NSX Controller Status:

uuid: 78d5b561-4f66-488d-9e53-089735eac1c1
is master: true
in majority: true
uuid                                 address              status
78d5b561-4f66-488d-9e53-089735eac1c1 192.168.110.34       active

Cluster Management Server Status:

uuid                                 rpc address          rpc port             global id            vpn
address          status
557a911f-41fd-4977-9c58-f3ef55b3efe7 192.168.110.34       7777                 1
10.0.0.1             connected

Zookeeper Ensemble Status:

Zookeeper Server IP: 10.0.0.1, reachable, ok
Zookeeper version: 3.5.1-alpha--1, built on 03/08/2016 01:18 GMT
Latency min/avg/max: 0/0/1841
Received: 212095
Sent: 212125
Connections: 5
Outstanding: 0
Zxid: 0x10000017a
Mode: leader
Node count: 33
Connections: /10.0.0.1:51726[1]
(queued=0,recved=60324,sent=60324,sid=0x100000f14a10003,lop=PING,est=1459376913497,to=30000,lcxid=0x8,l
zxid=0x10000017a,lresp=604617273,llat=0,minlat=0,avglat=0,maxlat=1088)
 /10.0.0.1:35462[0](queued=0,recved=1,sent=0)
 /10.0.0.1:51724[1]
(queued=0,recved=45786,sent=45803,sid=0x100000f14a10001,lop=GETC,est=1459376911226,to=40000,lcxid=0x21e
,lzxid=0x10000017a,lresp=604620658,llat=0,minlat=0,avglat=0,maxlat=1841)
 /10.0.0.1:51725[1]
(queued=0,recved=60328,sent=60333,sid=0x100000f14a10002,lop=PING,est=1459376913455,to=30000,lcxid=0xc,l
zxid=0x10000017a,lresp=604618294,llat=0,minlat=0,avglat=0,maxlat=1356)
 /10.0.0.1:51730[1]
(queued=0,recved=45315,sent=45324,sid=0x100000f14a10006,lop=PING,est=1459376914516,to=40000,lcxid=0x49,
lzxid=0x10000017a,lresp=604623243,llat=0,minlat=0,avglat=0,maxlat=1630)
```

后续步骤

将额外的 NSX Controller 添加到控制群集。请参阅将额外的 NSX Controller 加入群集主控制器。

将额外的 NSX Controller 加入群集主控制器

具有多节点 NSX Controller 群集可以帮助确保至少一个 NSX Controller 始终可用。

前提条件

- 安装三个 NSX Controller 设备。
- 确保 NSX Controller 节点已加入管理层面。请参阅将 NSX Controller 加入管理层面。
- 初始化控制群集以创建控制群集主控制器。
- 在 `join control-cluster` 命令中，您必须使用 IP 地址而不是域名。
- 如果使用 vCenter 并将 NSX-T 组件部署到同一群集中，请确保配置 DRS 反关联性规则。反关联性规则禁止 DRS 将多个节点迁移到单个主机。

步骤

1 为每个 NSX Controller 设备打开一个 SSH 会话。

例如，NSX-Controller1、NSX-Controller2 和 NSX-Controller3。在该示例中，NSX-Controller1 已初始化控制群集，并且是控制群集主控制器。

2 在非主 NSX Controller 上，使用共享密钥密码运行 `set control-cluster security-model` 命令。为 NSX-Controller2 和 NSX-Controller3 输入的共享密钥密码必须与在 NSX-Controller1 上输入的共享密钥密码相匹配。

例如：

```
NSX-Controller2> set control-cluster security-model shared-secret secret <NSX-Controller1' s-shared-secret-password>

Security secret successfully set on the node.
```

```
NSX-Controller3> set control-cluster security-model shared-secret secret <NSX-Controller1' s-shared-secret-password>

Security secret successfully set on the node.
```

3 在非主 NSX Controller 上，运行 `get control-cluster certificate thumbprint` 命令。

命令输出是每个 NSX Controller 特有的数字串。

例如：

```
NSX-Controller2> get control-cluster certificate thumbprint
...
```

```
NSX-Controller3> get control-cluster certificate thumbprint
...
```

4 在主 NSX Controller 上，运行 **join control-cluster** 命令。

提供以下信息：

- 非主 NSX Controller（本示例中的 NSX-Controller2 和 NSX-Controller3）的 IP 地址以及可选的端口号
- 非主 NSX Controller 的证书指纹

不要在多个控制器上并行运行 `join` 命令。确保在加入完一个控制器后，再加入另一个控制器。

```
NSX-Controller1> join control-cluster <NSX-Controller2-IP> thumbprint <nsx-controller2's-thumbprint>
Node 192.168.210.48 has successfully joined the control cluster.
Please run 'activate control-cluster' command on the new node.
```

确保运行 `get control-cluster status` 命令以将 NSX-Controller2 加入群集。

```
NSX-Controller1> join control-cluster <NSX-Controller3-IP> thumbprint <nsx-controller3's-thumbprint>
Node 192.168.210.49 has successfully joined the control cluster.
Please run 'activate control-cluster' command on the new node.
```

确保运行 `get control-cluster status` 命令以将 NSX-Controller3 加入群集。

5 在已加入控制群集主控制器的两个 NSX Controller 节点上，运行 `activate control-cluster` 命令。

注 不要在多个控制器上并行运行 `activate` 命令。确保在激活完一个控制器后，再激活另一个控制器。

例如：

```
NSX-Controller2> activate control-cluster
Control cluster activation successful.
```

在 NSX-Controller2 上运行 `get control-cluster status verbose` 命令，并确保 `Zookeeper Server IP` 为 `reachable, ok`。

```
NSX-Controller3> activate control-cluster
Control cluster activation successful.
```

在 NSX-Controller3 上运行 `get control-cluster status verbose` 命令，并确保 `Zookeeper Server IP` 为 `reachable, ok`。

VMware, Inc. 保留所有权利。

运行 `get control-cluster status` 命令以验证结果。

```
NSX-Controller1> get control-cluster status
uuid: db4aa77a-4397-4d65-ad33-9fde79ac3c5c
is master: true
in majority: true
uuid                                   address              status
0cfe232e-6c28-4fea-8aa4-b3518baef00d 192.168.210.47       active
bd257108-b94e-4e6d-8b19-7fa6c012961d 192.168.210.48       active
538be554-1240-40e4-8e94-1497e963a2aa 192.168.210.49       active
```

列出的第一个 UUID 用于整个控制群集。每个控制器节点也具有一个 UUID。

注 如果尝试将控制器加入群集并且 `set control-cluster security-model` 或 `join control-cluster` 命令失败，则群集配置文件可能处于不一致的状态。要解决该问题，请执行以下步骤：

- 在尝试加入群集的控制器上，运行 `deactivate control-cluster` 命令。
- 在主控制器上，如果 `get control-cluster status` 或 `get control-cluster status verbose` 命令显示有关失败的控制器的信息，请运行 `detach control-cluster <IP address of failed controller>` 命令。

后续步骤

将管理程序主机添加到 NSX-T 架构。请参阅第 7 章，主机准备。

NSX Edge 安装

6

NSX Edge 为 NSX-T 部署外部的网络提供路由服务和连接。如果要部署具有网络地址转换 (Network Address Translation, NAT) 的第 0 层路由器或第 1 层路由器，则需要使用 NSX Edge。

NSX Edge 具有以下支持的部署方法：

- OVA/OVF
- 具有 PXE 的 ISO
- 没有 PXE 的 ISO

仅在 ESXi 或裸机上支持 NSX Edge。在 KVM 上不支持 NSX Edge。

对于 PXE 安装，您必须为 root 和 admin 用户密码提供使用 sha-512 算法加密的密码字符串。

NSX-T 设备具有以下密码复杂性要求：

- 至少 8 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

即使密码不符合复杂性要求，安装也会成功。但在首次登录时，将提示您更改密码。

注 在设置了足够复杂的密码后，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。

在安装 NSX Manager 时，请选择不包含下划线的主机名。如果指定包含下划线的主机名，在部署后，设备将使用默认主机名，如 nsx-manager。

重要 NSX 组件虚拟机安装包括 VMware Tools。NSX 设备不支持移除或升级 VMware Tools。

VMware, Inc. 保留所有权利。

本章讨论了以下主题：

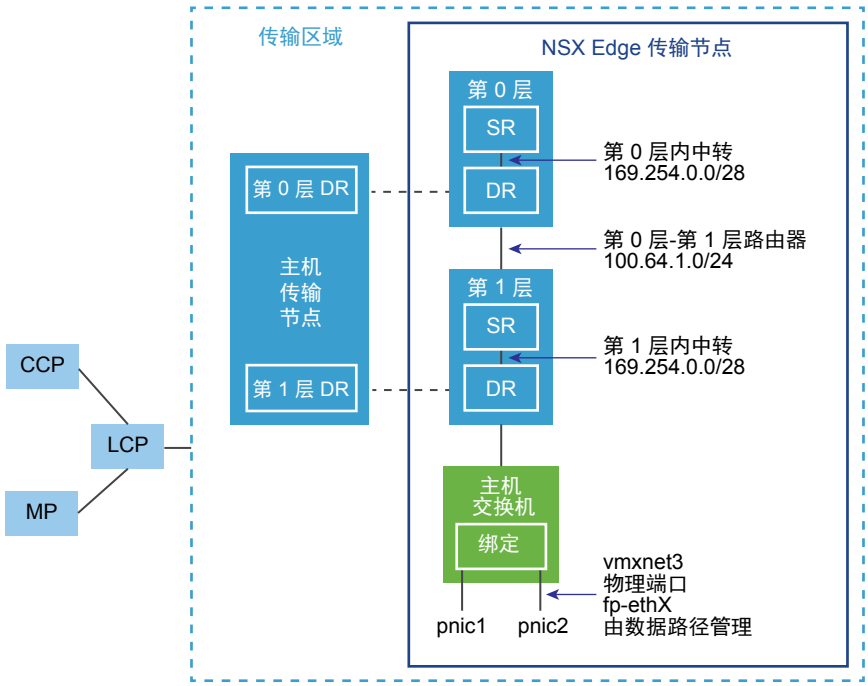
NSX Edge 网络设置

可以通过 ISO、OVA/OVF 或 PXE 引导安装 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 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 6-1. NSX Edge 的简要视图



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 为第 0 层和第 1 层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第 0 层和第 1 层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。所有第 0 层逻辑路由器都具有服务路由器。如果需要，第 1 层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。在部署第 0 层或第 1 层逻辑路由器时，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。请注意，在第 1 层逻辑路由器上，只有在创建第 1 层逻辑路由器时选择了 NSX Edge 群集，才会使用 SR。

为第 0 层到第 1 层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 地址空间中为每个第 0 层到第 1 层的对等连接提供一个 /31 子网。在创建第 1 层路由器并将其连接到第 0 层路由器时，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 部署具有一个管理层面群集 (MP) 和一个控制层面群集 (CCP)。MP 和 CCP 将配置推送到每个传输区域的本地控制层面 (LCP)。在主机或 NSX Edge 加入管理层面时，管理层面代理 (MPA) 将与主机或 NSX Edge 建立连接，并且主机或 NSX Edge 变为 NSX-T 架构节点。然后，在将架构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。这些物理网卡是由数据路径管理的。它们可以作为到外部网络的 VLAN 上行链路，或者作为到 NSX-T 管理的内部虚拟机网络的隧道端点链路。

最佳做法是为每个 NSX Edge 分配至少两个物理链路。或者，也可以在相同物理网卡上叠加使用不同 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 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。

您可以在 NSX Edge CLI 中运行 `get interfaces` 和 `get physical-ports` 命令以查看物理链路信息。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。

传输区域和主机交换机

要了解 NSX Edge 网络，您必须了解有关传输区域和主机交换机的内容。传输区域控制 NSX-T 中的第 2 层网络的范围。主机交换机是在传输节点上创建的软件交换机。主机交换机的用途是，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 上安装单个主机交换机。

共有两种类型的传输区域：

- 传输节点之间的内部 NSX-T 隧道的覆盖网络 - NSX Edge 只能属于一个覆盖网络传输区域。
- NSX-T 外部的上行链路的 VLAN - 对 NSX Edge 所属的 VLAN 传输区域数量没有限制。

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主机交换机。如果您希望每个 NSX Edge 仅具有一个主机交换机，则应该这样做。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）。

请注意，如果您需要在用于覆盖网络流量和其他 VLAN 流量（如 VLAN 上行链路）的传输网络中使用相同的 VLAN ID，则必须在两个不同的主机交换机上配置这些传输区域，一个用于 VLAN，另一个用于覆盖网络。

有关传输区域的详细信息，请参阅关于传输区域。

虚拟设备/虚拟机 NSX Edge 网络

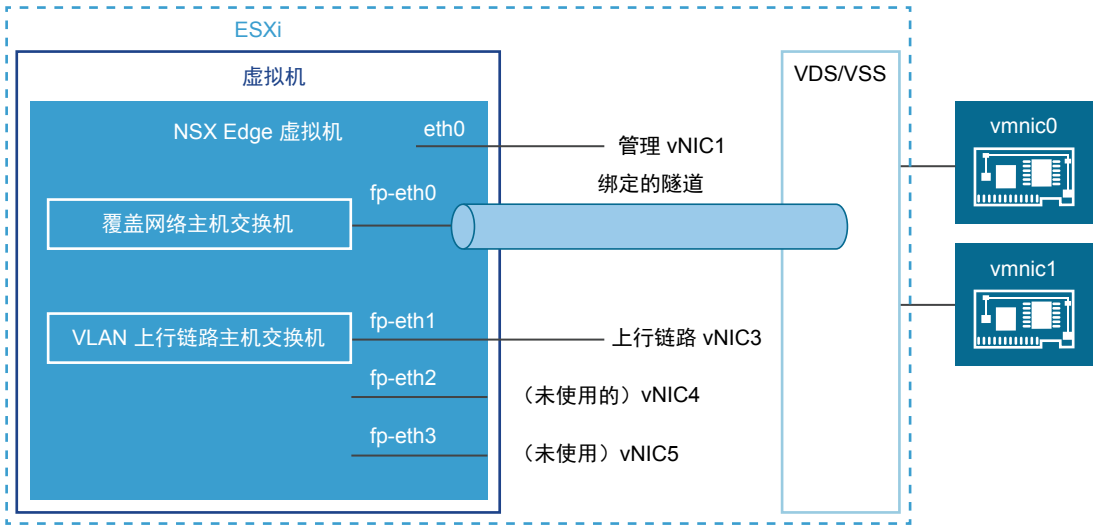
在将 NSX Edge 安装为虚拟设备或虚拟机时，将创建名为 fp-ethX 的内部接口，其中 X 为 0、1、2 和 3。将为到架顶式 (Top-Of-Rack, ToR) 交换机的上行链路和 NSX-T 覆盖网络隧道分配这些接口。

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，您应该为 NSX Edge 分配至少两个 vmnic：一个 vmnic 用于 NSX Edge 管理，一个 vmnic 用于上行链路和隧道。

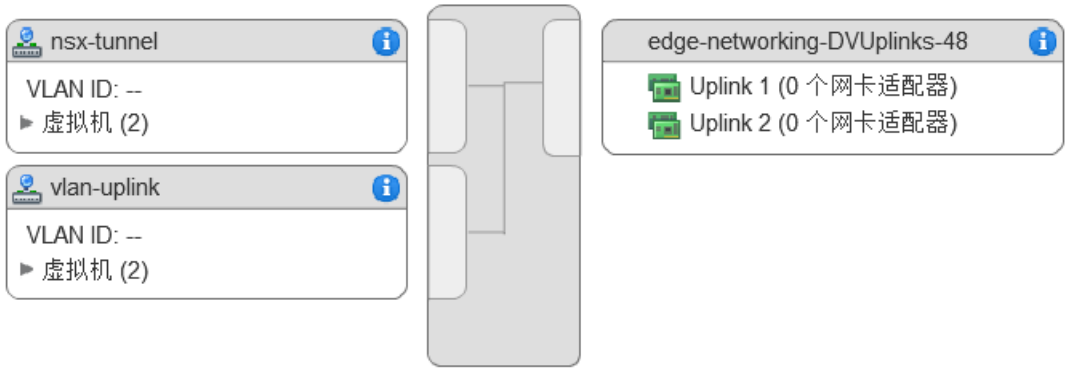
在下面的示例物理拓扑中，fp-eth0 用于 NSX-T 覆盖网络隧道。fp-eth1 用于 VLAN 上行链路。未使用 fp-eth2 和 fp-eth3。

图 6-2. 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，具有两个主机交换机（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 设置应如下所示：

```
--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。这只是一个示例。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) (Host > Configuration > Networking > Add Networking > Virtual Machine > VLAN ID All (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。

可以在相同的管理程序上部署 NSX Edge 和主机传输节点。

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

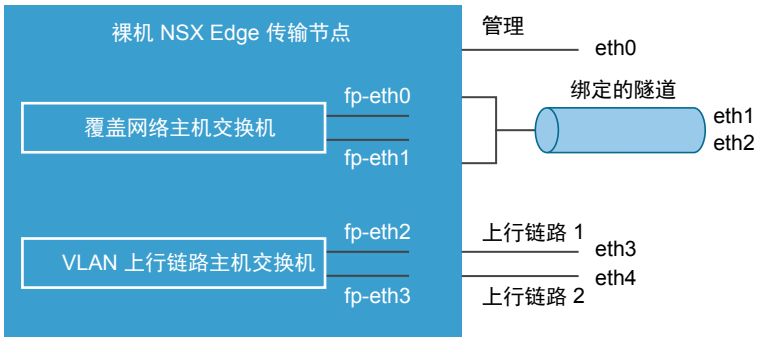
裸机 NSX Edge 包含名为 fp-ethX 的内部接口，其中 X 为 0、1、2、3 等。创建的 fp-ethX 接口数取决于裸机 NSX Edge 具有多少个物理网卡。可以为到架顶式 (ToR) 交换机和 NSX-T 覆盖网络隧道的上行链路分配所有这些接口或一部分接口。

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。

VMware, Inc. 保留所有权利。

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 覆盖网络隧道。fp-eth2 和 fp-eth3 用作到 TOR 的冗余 VLAN 上行链路。

图 6-3. 建议用于裸机 NSX Edge 网络的一种链路设置



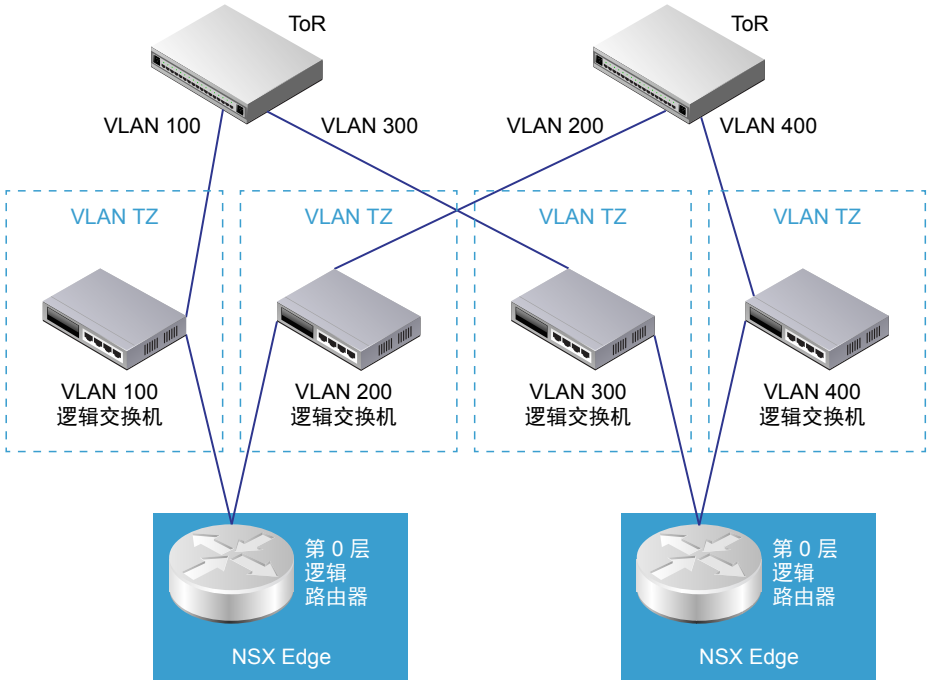
NSX Edge 上行链路冗余

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，您还应该使用两个 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，将安装新的主机交换机。例如，如果将 NSX Edge 节点添加到四个 VLAN 传输区域中（如图中所示），则会在 NSX Edge 上安装四个主机交换机。

图 6-4. 建议用于 NSX Edge 到 TOR 的一种 ECMP VLAN 设置



使用 GUI 在 ESXi 上安装 NSX Edge

如果希望进行交互式 NSX Edge 安装，您可以使用基于 UI 的虚拟机管理工具，例如，连接到 vCenter Server 的 vSphere Client。

在该 NSX-T 版本中，不支持 IPv6。

前提条件

- 确认满足系统要求。请参阅系统要求。
- 确认打开了所需的端口。请参阅端口和协议。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。大多数部署将 NSX 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 设备到其他网络的静态路由。准备 NSX 设备进行通信时使用的管理虚拟机端口组。
- 计划您的 IPv4 IP 地址方案。在该 NSX-T 版本中，不支持 IPv6。
- 用于在 ESXi 主机上部署 OVF 模板的权限。
- 选择不包含下划线的主机名。否则，主机名将设置为 *localhost*。
- 可以部署 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。
- 请参阅 NSX Edge 网络设置中的 NSX Edge 网络要求。

步骤

1 找到 NSX Edge OVA 或 OVF 文件。

  将下载 URL 复制到计算机或下载 OVA 文件到计算机。

2 在管理工具中，启动**部署 OVF 模板 (Deploy OVF template)**向导并导航或链接到 .ova 文件。

3 输入 NSX Edge 的名称，然后选择一个文件夹或数据中心。

  键入的名称将显示在清单中。

  将使用选定的文件夹将权限应用于 NSX Edge。

4 选择配置大小：小、中或大。

  系统要求因配置大小而异。请参阅《 NSX-T 发行说明》。

5 选择一个数据存储以存储 NSX Edge 虚拟设备文件。

6 如果在 vCenter 中进行安装，请选择一个主机或群集以在其中部署 NSX Edge 设备。

  通常，应将 NSX Edge 放在提供网络管理实用程序的群集中。

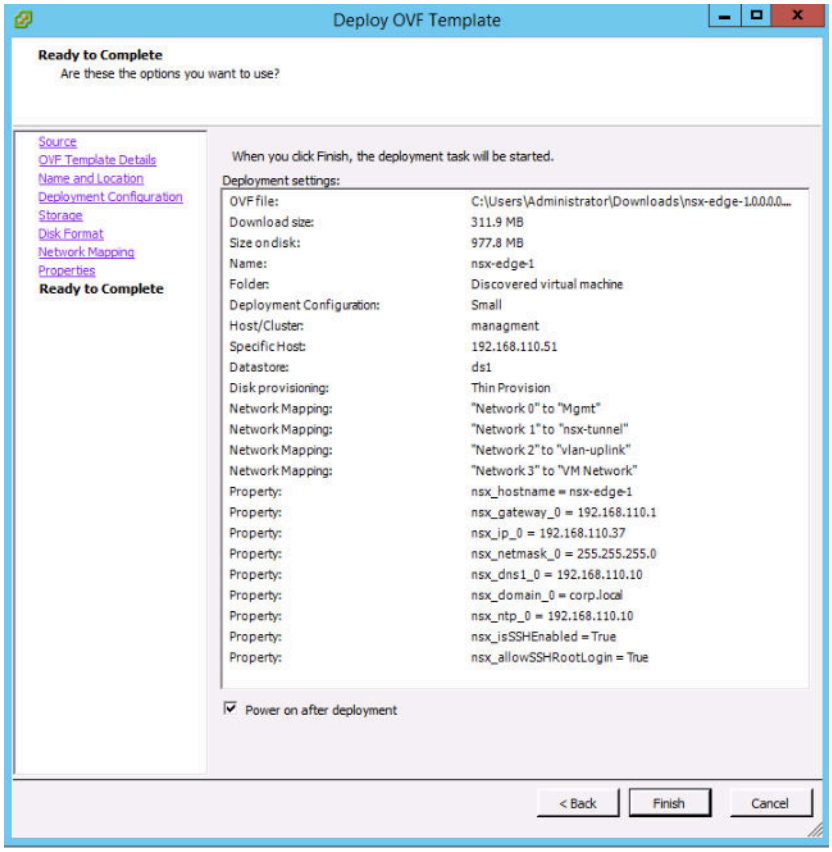
7 选择要在其中放置 NSX Edge 接口的网络。

  您可以在部署 NSX Edge 后更改这些网络。

VMware, Inc. 保留所有权利。

8 设置 NSX Edge 密码和 IP 设置。

例如，在配置所有选项后，该屏幕显示最终检查屏幕。



9 为了获得最佳性能，请为 NSX 组件预留内存。

即使内存过量使用，内存预留也能保证主机为虚拟机预留的物理内存量下限。将预留设置为某个级别，以确保 NSX 组件具有足够的内存以高效地运行。请参阅系统要求。

打开 NSX Edge 控制台以跟踪引导过程。如果未打开该窗口，请确保允许弹出窗口。

在完全引导 NSX Edge 后，登录到 CLI 并运行 `get interface eth0` 命令以验证是否按预期方式应用了 IP 地址。

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

Interface: eth0
  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
  ...
```

如果需要，请运行 `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` 命令以更新管理接口。或者，也可以使用 `start service ssh` 命令启动 SSH 服务。

确保 NSX Edge 设备具有所需的连接。

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

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 DHCP 将错误的网卡分配为管理网卡，您可以按以下方式纠正该问题：

1 `stop service dataplane`

2 `set interface eth0 dhcp plane mgmt`

3 将 eth0 放到 DHCP 网络中，并等待为 eth0 分配 IP 地址。

4 `start service dataplane`

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。请参阅将 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。

在该 NSX-T 版本中，不支持 IPv6。

前提条件

- 确认满足系统要求。请参阅系统要求。
- 确认打开了所需的端口。请参阅端口和协议。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。大多数部署将 NSX 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 设备到其他网络的静态路由。准备 NSX 设备进行通信时使用的管理虚拟机端口组。
- 计划您的 IPv4 IP 地址方案。在该 NSX-T 版本中，不支持 IPv6。
- 请参阅 NSX Edge 网络设置中的 NSX Edge 网络要求。
- 用于在 ESXi 主机上部署 OVF 模板的权限。
- 选择不包含下划线的主机名。否则，主机名将设置为 *localhost*。
- OVF Tool 4.0 或更高版本。

步骤

- （对于单独的主机）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
Warning:
 - No manifest entry found for: 'nsx-<component>.ovf'.
 - File is missing from the manifest: 'nsx-<component>.ovf'.
 - ExtraConfig options exists in source.
 - Skipping monitor as the --X:waitForIp option is not given.
Completed successfully
```

VMware, Inc. 保留所有权利。

- （对于 vCenter Server 管理的主机）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
Warning:
 - No manifest entry found for: 'nsx-<component>.ovf'.
 - File is missing from the manifest: 'nsx-<component>.ovf'.
 - ExtraConfig options exists in source.
 - Skipping monitor as the --X:waitForIp option is not given.
Completed successfully
```

- 为了获得最佳性能，请为 NSX 组件预留内存。

  即使内存过量使用，内存预留也能保证主机为虚拟机预留的物理内存量下限。将预留设置为某个级别，以确保 NSX 组件具有足够的内存以高效地运行。请参阅系统要求。

打开 NSX Edge 控制台以跟踪引导过程。如果未打开该窗口，请确保允许弹出窗口。

在完全引导 NSX Edge 后，登录到 CLI 并运行 `get interface eth0` 命令以验证是否按预期方式应用了 IP 地址。

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

Interface: eth0
  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
  ...
```

如果需要，请运行 `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` 命令以更新管理接口。或者，也可以使用 `start service ssh` 命令启动 SSH 服务。

确保 NSX Edge 设备具有所需的连接。

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

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 DHCP 将错误的网卡分配为管理网卡，您可以按以下方式纠正该问题：

1 `stop service dataplane`

2 `set interface eth0 dhcp plane mgmt`

3 将 eth0 放到 DHCP 网络中，并等待为 eth0 分配 IP 地址。

4 `start service dataplane`

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。请参阅将 NSX Edge 加入管理层面。

通过 ISO 文件使用 PXE 服务器安装 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。请注意，NSX Manager 和 NSX Controller 不支持 PXE 引导安装。这包括自动配置网络设置，例如，IP 地址、网关、网络掩码、NTP 和 DNS。

该过程说明了如何在 Ubuntu 上设置 PXE 服务器。PXE 由两个组件组成：DHCP 和 TFTP。

DHCP 将 IP 设置动态分配给 NSX-T 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 组件 ISO 文件以及 preseed 文件中包含的安装设置。

在 PXE 服务器准备就绪后，该过程说明如何使用 preseed 配置文件安装 NSX Edge。

前提条件

- 确认满足系统要求。请参阅系统要求。
- 确认打开了所需的端口。请参阅端口和协议。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。大多数部署将 NSX 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 设备到其他网络的静态路由。准备 NSX 设备进行通信时使用的管理虚拟机端口组。
- 计划您的 IPv4 IP 地址方案。在该 NSX-T 版本中，不支持 IPv6。
- 请参阅 NSX Edge 网络设置中的 NSX Edge 网络要求。
- 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。

步骤

1 （可选）创建一个 kickstart 文件。

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

  必须将 kickstart 文件命名为

```
nsxcli.install
```

  并复制到 Web 服务器中，例如，在 `/var/www/html/nsx-edge/nsxcli.install` 中。

  在 kickstart 文件中，您可以添加所需的 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 <password>
```

请注意，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 <mgr-ip> thumbprint <mgr-thumbprint> username <mgr-username> password <mgr
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）如果希望将该 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 中，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 确保 DHCP 服务正在运行。

```
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 确保 TFTP 和 Apache 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 文件复制或下载到所需的位置。

VMware, Inc. 保留所有权利。

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 whois
sudo mkpasswd -m sha-512

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

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

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

替换哈希字符串。您不需要转义任何特殊字符，例如 $、'、" 或 \。

也可以在 `preseed.cfg` 中添加 `usermod` 命令以设置 root 和/或 admin 密码。例如，您可以添加以下两行：

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

哈希字符串只是一个示例。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 $6$tgm...` 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。

务必将 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=trusty --
```

VMware, Inc. 保留所有权利。

18 将以下几行添加到 /etc/dhcp/dhcpd.conf 文件中。

务必将 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。

20 按照裸机安装说明或 ISO 安装说明完成安装。

- 在裸机上安装 NSX Edge
- 通过 ISO 文件将 NSX Edge 安装为虚拟设备

21 打开虚拟机电源。

22 在引导菜单中，选择 **nsxedge**。

将自动配置网络，创建分区并安装 NSX Edge 组件。

在显示 NSX Edge 登录提示时，您可以作为 admin 或 root 登录。

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

23 为了获得最佳性能，请为 NSX 组件预留内存。

即使内存过量使用，内存预留也能保证主机为虚拟机预留的物理内存量下限。将预留设置为某个级别，以确保 NSX 组件具有足够的内存以高效地运行。请参阅系统要求。

打开 NSX Edge 控制台以跟踪引导过程。如果未打开该窗口，请确保允许弹出窗口。

在完全引导 NSX Edge 后，登录到 CLI 并运行 get interface eth0 命令以验证是否按预期方式应用了 IP 地址。

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

Interface: eth0
  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
  ...
```

如果需要，请运行 `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` 命令以更新管理接口。或者，也可以使用 `start service ssh` 命令启动 SSH 服务。

确保 NSX Edge 设备具有所需的连接。

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

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 DHCP 将错误的网卡分配为管理网卡，您可以按以下方式纠正该问题：

1 `stop service dataplane`

2 `set interface eth0 dhcp plane mgmt`

3 将 eth0 放到 DHCP 网络中，并等待为 eth0 分配 IP 地址。

4 `start service dataplane`

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。请参阅将 NSX Edge 加入管理层面。

在裸机上安装 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。通常在无法访问 PXE 服务器的概念证明 (Proof Of Concept, POC) 实验室中使用这种安装方法。

前提条件

- 确认满足系统要求。请参阅系统要求。
- 确认打开了所需的端口。请参阅端口和协议。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。大多数部署将 NSX 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 设备到其他网络的静态路由。准备 NSX 设备进行通信时使用的管理虚拟机端口组。
- 计划您的 IPv4 IP 地址方案。在该 NSX-T 版本中，不支持 IPv6。
- 请参阅 NSX Edge 网络设置中的 NSX Edge 网络要求。

步骤

1 创建一个可引导磁盘并在其中包含 NSX Edge ISO 文件。

2 从磁盘中引导主机。

3 选择**自动安装 (Automated installation)**。

在按 Enter 后，可能会出现 10 秒的暂停。

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**。

4 为了获得最佳性能，请为 NSX 组件预留内存。

即使内存过量使用，内存预留也能保证主机为虚拟机预留的物理内存量下限。将预留设置为某个级别，以确保 NSX 组件具有足够的内存以高效地运行。请参阅系统要求。

打开 NSX Edge 控制台以跟踪引导过程。如果未打开该窗口，请确保允许弹出窗口。

在完全引导 NSX Edge 后，登录到 CLI 并运行 `get interface eth0` 命令以验证是否按预期方式应用了 IP 地址。

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

Interface: eth0
  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
  ...
```

如果需要，请运行 `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` 命令以更新管理接口。或者，也可以使用 `start service ssh` 命令启动 SSH 服务。

确保 NSX Edge 设备具有所需的连接。

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

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 DHCP 将错误的网卡分配为管理网卡，您可以按以下方式纠正该问题：

1 `stop service dataplane`

2 `set interface eth0 dhcp plane mgmt`

3 将 eth0 放到 DHCP 网络中，并等待为 eth0 分配 IP 地址。

4 `start service dataplane`

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。请参阅将 NSX Edge 加入管理层面。

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 设备。通常在无法访问 PXE 服务器的概念证明 (Proof Of Concept, POC) 实验室中使用这种安装方法。

重要 NSX 组件虚拟机安装包括 VMware Tools。NSX 设备不支持移除或升级 VMware Tools。

前提条件

- 确认满足系统要求。请参阅系统要求。
- 确认打开了所需的端口。请参阅端口和协议。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。大多数部署将 NSX 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 设备到其他网络的静态路由。准备 NSX 设备进行通信时使用的管理虚拟机端口组。
- 计划您的 IPv4 IP 地址方案。在该 NSX-T 版本中，不支持 IPv6。
- 请参阅 NSX Edge 网络设置中的 NSX Edge 网络要求。

步骤

1 在单独主机上或 vCenter Web Client 中，创建一个虚拟机并分配以下资源：
   - 客户机操作系统：其他（64 位）。
   - 3 个 VMXNET3 网卡。NSX Edge 不支持 e1000 网卡驱动程序。
   - NSX-T 部署所需的相应系统资源。

2 将 NSX Edge ISO 文件绑定到虚拟机。

确保 CD/DVD 驱动器设备状态设置为**启动时连接 (Connect at power on)**。

3 在 ISO 引导期间，打开虚拟机控制台并选择**自动安装 (Automated installation)**。

在按 Enter 后，可能会出现 10 秒的暂停。

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 8 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

重要 在设置了足够复杂的密码后，设备上的核心服务才会启动。

4 为了获得最佳性能，请为 NSX 组件预留内存。

即使内存过量使用，内存预留也能保证主机为虚拟机预留的物理内存量下限。将预留设置为某个级别，以确保 NSX 组件具有足够的内存以高效地运行。请参阅系统要求。

打开 NSX Edge 控制台以跟踪引导过程。如果未打开该窗口，请确保允许弹出窗口。

在完全引导 NSX Edge 后，登录到 CLI 并运行 `get interface eth0` 命令以验证是否按预期方式应用了 IP 地址。

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

Interface: eth0
  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
  ...
```

如果需要，请运行 `set interface eth0 ip <CIDR> gateway <gateway-ip> plane mgmt` 命令以更新管理接口。或者，也可以使用 `start service ssh` 命令启动 SSH 服务。

确保 NSX Edge 设备具有所需的连接。

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

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 DHCP 将错误的网卡分配为管理网卡，您可以按以下方式纠正该问题：

1 `stop service dataplane`

2 `set interface eth0 dhcp plane mgmt`

3 将 eth0 放到 DHCP 网络中，并等待为 eth0 分配 IP 地址。

4 `start service dataplane`

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。请参阅将 NSX Edge 加入管理层面。

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。

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。

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
```

在 NSX Manager UI 中，将在**架构 > Edge (Fabric > Edges)** 页面上显示 NSX Edge。MPA 连接应处于“已连接”状态。如果 MPA 连接未处于“已连接”状态，请尝试刷新浏览器屏幕。

后续步骤

将 NSX Edge 添加为传输节点。请参阅创建 NSX Edge 传输节点。

VMware, Inc. 保留所有权利。

主机准备

7

在准备管理程序主机以运行 NSX-T 时，这些主机称为结构层节点。作为结构层节点的主机安装了 NSX-T 模块并在 NSX-T 管理层面中进行了注册。

本章讨论了以下主题：

- 在 KVM 主机上安装第三方软件包
- 将管理程序主机添加到 NSX-T 架构
- 手动安装 NSX-T 内核模块
- 将管理程序主机加入管理层面

在 KVM 主机上安装第三方软件包

要准备 KVM 主机以作为架构节点，您必须安装一些第三方软件包。

步骤

- 对于 Ubuntu 14.04，请运行以下命令：

```
apt-get install libunwind8 libgflags2 libgoogle-perftools4 traceroute
apt-get install python-mako python-simplejson python-support python-unittest2 python-yaml python-
netaddr
apt-get install libprotobuf8
apt-get install libboost-filesystem1.54.0 libboost-chrono1.54.0
apt-get install dkms
```

- 对于 Ubuntu 16.04，请运行以下命令：

```
apt-get install libunwind8 libgflags2v5 libgoogle-perftools4 traceroute
apt-get install python-mako python-simplejson python-unittest2 python-yaml python-netaddr
apt-get install libprotobuf9v5
apt-get install libboost-filesystem1.58.0 libboost-chrono1.58.0 libgoogle-glog0v5
apt-get install dkms
```

- 对于 RHEL 7.2，请运行以下命令：

```
yum groupinstall “Virtualization Hypervisor”
yum groupinstall “Virtualization Client”
yum groupinstall "Virtualization Platform"
yum groupinstall "Virtualization Tools"
yum install boost-filesystem PyYAML boost-iostreams boost-chrono python-mako python-netaddr python-six gperftools-libs libunwind yum-utils wget net-tools redhat-lsb-core tcpdump wget
```

将管理程序主机添加到 NSX-T 架构

架构节点是已在 NSX-T 管理层面中注册并安装了 NSX-T 模块的节点。要使管理程序主机成为 NSX-T 覆盖网络的一部分，必须先将该主机添加到 NSX-T 架构中。

注 如果在主机上已手动安装这些模块并使用 CLI 将主机加入管理层面，则可以跳过该过程。

前提条件

- 对于打算添加到 NSX-T 架构的每个主机，请先收集以下主机信息：
  - 主机名
  - 管理 IP 地址
  - 用户名
  - 密码
  - (KVM) SHA-256 SSL 指纹
  - (ESXi) SHA-256 SSL 指纹
- （可选）检索管理程序指纹，以便在将主机添加到架构时提供该指纹。
  - 一种自行收集该信息的方法是，在 Linux shell 中运行以下命令：

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

  - 另一种方法是，使用 ESXi CLI：

```
[root@host:~] openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha256 -noout
```

  - 要从 KVM 管理程序中检索 SHA-256 指纹，请运行以下命令：

```
# ssh-keyscan -t rsa hostname > hostname.pub
# awk '{print $3}' hostname.pub | base64 -d | sha256sum -b | sed 's/ .*$//' | xxd -r -p | base64

where hostname is the hypervisor’ s hostname or IP address.
```

- 对于 Ubuntu，确认安装了所需的第三方软件包。请参阅在 KVM 主机上安装第三方软件包。

步骤

1 在 NSX Manager CLI 中，验证 install-upgrade 服务是否正在运行。

```
nsx-manager-1> get service install-upgrade

Service name: install-upgrade
Service state: running
Enabled: True
```

2 从浏览器中，登录到 `https://<nsx-mgr>` 中的 NSX Manager。

3 选择**架构 (Fabric) > 节点 (Nodes) > 主机 (Hosts)**，然后单击**添加 (Add)**。

VMware, Inc. 保留所有权利。

4 输入主机名、IP 地址、用户名、密码以及可选的指纹。

例如：

如果未输入主机指纹，NSX-T UI 将提示您使用从主机中检索的默认指纹。

例如：

在将主机成功添加到 NSX-T 架构后，NSX Manager **架构 > 节点 > 主机 (Fabric > Nodes > Hosts)** UI 将显示**部署状态: 安装成功 (Deployment Status: Installation Successful)**和 **MPA 连接: 已连接 (MPA Connectivity: Up)**。在将架构节点变为传输节点后，**LCP 连接 (LCP Connectivity)**才会可用。

由于将主机添加到 NSX-T 架构中后，将在该主机上安装一组 NSX-T 模块。在 ESXi 上，这些模块将打包为 VIB。对于 RHEL 上的 KVM，这些模块将打包为 RPM。对于 Ubuntu 上的 KVM，这些模块将打包为 DEB。

要在 ESXi 上进行验证，您可以运行 `esxcli software vib list | grep nsx` 命令，其中的日期是执行安装的日期。

要在 RHEL 上进行验证，请运行 `yum list installed` 或 `rpm –qa` 命令。

要在 Ubuntu 上进行验证，请运行 `dpkg ––get-selections` 命令。

您可以使用 `GET https://<nsx-mgr>/api/v1/fabric/nodes/<node-id>` API 调用查看架构节点：

```
{
  "resource_type" : "HostNode",
  "id" : "f36d5a79-233c-47c9-9c17-9adc9f8ec466",
  "display_name" : "10.143.1.177",
  "fqdn" : "w1-mvpcloud-177.eng.vmware.com",
  "ip_addresses" : [ "10.143.1.177" ],
  "external_id" : "f36d5a79-233c-47c9-9c17-9adc9f8ec466",
  "discovered_ip_addresses" : [ "192.168.150.104", "10.143.1.177" ],
  "os_type" : "ESXI",
  "os_version" : "6.5.0",
  "managed_by_server" : "",
  "_create_time" : 1480369243245,
  "_last_modified_user" : "admin",
  "_last_modified_time" : 1480369243245,
  "_create_user" : "admin",
  "_revision" : 0
}
```

您可以在 API 中使用 `GET https://<nsx-mgr>/api/v1/fabric/nodes/<node-id>/status` API 调用监控状态。

```
{
  "lcp_connectivity_status" : "UP",
  "mpa_connectivity_status" : "UP",
  "last_sync_time" : 1480370899198,
  "mpa_connectivity_status_details" : "Client is responding to heartbeats",
  "lcp_connectivity_status_details" : [ {
    "control_node_ip" : "10.143.1.47",
    "status" : "UP"
  } ],
  "inventory_sync_paused" : false,
  "last_heartbeat_timestamp" : 1480369333415,
  "system_status" : {
    "mem_used" : 2577732,
    "system_time" : 1480370897000,
    "file_systems" : [ {
      "file_system" : "root",
```

```
      "total" : 32768,
      "used" : 5440,
      "type" : "ramdisk",
      "mount" : "/"
    }, {
      "file_system" : "etc",
      "total" : 28672,
      "used" : 264,
      "type" : "ramdisk",
      "mount" : "/etc"
    }, {
      "file_system" : "opt",
      "total" : 32768,
      "used" : 20,
      "type" : "ramdisk",
      "mount" : "/opt"
    }, {
      "file_system" : "var",
      "total" : 49152,
      "used" : 2812,
      "type" : "ramdisk",
      "mount" : "/var"
    }, {
      "file_system" : "tmp",
      "total" : 262144,
      "used" : 21728,
      "type" : "ramdisk",
      "mount" : "/tmp"
    }, {
      "file_system" : "iofilters",
      "total" : 32768,
      "used" : 0,
      "type" : "ramdisk",
      "mount" : "/var/run/iofilters"
    }, {
      "file_system" : "hostdstats",
      "total" : 116736,
      "used" : 2024,
      "type" : "ramdisk",
      "mount" : "/var/lib/vmware/hostd/stats"
    } ],
    "load_average" : [ 0.03999999910593033, 0.03999999910593033, 0.05000000074505806 ],
    "swap_total" : 0,
    "mem_cache" : 0,
    "cpu_cores" : 2,
    "source" : "cached",
    "mem_total" : 8386740,
    "swap_used" : 0,
    "uptime" : 3983605000
  },
  "software_version" : "1.1.0.0.0.4649755",
  "host_node_deployment_status" : "INSTALL_SUCCESSFUL"
}
```

后续步骤

如果具有大量管理程序（例如，500 个或更多），NSX Manager 可能会出现较高的 CPU 使用率和性能问题。您可以运行 `aggsvc_change_intervals.py` 脚本（位于 NSX 文件存储中）以避免该问题。（您可以使用 NSX CLI 命令 `copy file` 或 API `POST /api/v1/node/file-store/<file-name>?action=copy_to_remote_file` 将该脚本复制到主机中。）该脚本更改某些进程的轮询间隔。请按以下方式运行该脚本：

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

要将轮询间隔改回到默认值，请运行以下命令：

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

创建传输区域。请参阅关于传输区域。

手动安装 NSX-T 内核模块

作为使用 NSX-T **架构 > 节点 > 主机 > 添加 (Fabric > Nodes > Hosts > Add)** 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 内核模块。

在 ESXi 管理程序上手动安装 NSX-T 内核模块

要准备主机以加入 NSX-T 网络，您必须在 ESXi 主机上安装 NSX-T 内核模块。这样，您就可以构建 NSX-T 控制层面和管理层面架构。在 VIB 文件中打包的 NSX-T 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 VIB 并将其作为主机映像的一部分。请注意，每个 NSX-T 版本的下载路径可能会有所不同。请务必查看 NSX-T 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, Inc. 保留所有权利。

```
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`。

将 ESXi 主机添加到 NSX-T 架构中后，会在主机上安装以下 VIB。

- nsx-aggservice - 为 NSX-T 聚合服务提供主机端库。NSX-T 聚合服务是在管理层面节点中运行并从 NSX-T 组件中获取运行时状态的服务。
- nsx-da - 收集有关管理程序操作系统版本、虚拟机和网络接口的发现代理 (Discovery Agent, DA) 数据。向管理层面提供数据以便在故障排除工具中使用。
- nsx-esx-datapath - 提供 NSX-T 数据层面数据包处理功能。
- nsx-exporter - 提供主机代理以便向在管理层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-lldp - 为链路层发现协议 (Link Layer Discovery Protocol, LLDP) 提供支持，这是网络设备在 LAN 上播发其身份、功能和邻居时使用的链路层协议。
- nsx-mpa - 在 NSX Manager 和管理程序主机之间提供通信。
- nsx-netcpa - 在中央控制层面和管理程序之间提供通信。从中央控制层面中接收逻辑网络状态，并以编程方式在数据层面中播发该状态。
- nsx-python-protobuf - 为协议缓冲区提供 Python 绑定。
- nsx-sfhc - 服务架构主机组件 (Service Fabric Host Component, SFHC)。提供主机代理，以便将管理程序作为管理层面清单中的架构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 升级和卸载以及监控管理程序上的 NSX-T 模块。
- nsxa - 执行主机级别配置，例如，主机交换机创建和上行链路配置。
- nsxcli - 在管理程序主机上提供 NSX-T CLI。
- nsx-support-bundle-client - 提供收集支持包的功能。

要进行验证，您可以在 ESXi 主机上运行 **esxcli software vib list | grep nsx** 或 **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 管理层面。请参阅将管理程序主机加入管理层面。

在 Ubuntu KVM 管理程序上手动安装 NSX-T 内核模块

要准备主机以加入 NSX-T 网络，您必须在 Ubuntu KVM 主机上安装 NSX-T 内核模块。这样，您就可以构建 NSX-T 控制层面和管理层面架构。在 DEB 文件中打包的 NSX-T 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 DEB 并将其作为主机映像的一部分。请注意，每个 NSX-T 版本的下载路径可能会有所不同。请务必查看 NSX-T 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。请参阅在 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
```

要进行验证，您可以运行 **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` 命令将尝试解决依赖项问题并重新运行 NSX-T 安装。

后续步骤

将主机添加到 NSX-T 管理层面。请参阅将管理程序主机加入管理层面。

在 RHEL KVM 管理程序上手动安装 NSX-T 内核模块

要准备主机以加入 NSX-T 网络，您必须在 RHEL KVM 主机上安装 NSX-T 内核模块。这样，您就可以构建 NSX-T 控制层面和管理层面架构。在 RPM 文件中打包的 NSX-T 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 RPM 并将其作为主机映像的一部分。请注意，每个 NSX-T 版本的下载路径可能会有所不同。请务必查看 NSX-T 下载页面以获取相应的 RPM。

前提条件

- 能够访问 RHEL 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 -xvf nsx-lcp-<release>-rhel71_x86_64.tar.gz
```

4 导航到软件包目录。

```
cd nsx-lcp-rhel71_x86_64/
```

5 安装该软件包。

```
sudo yum install *.rpm
```

在运行 yum install 命令时，将解决任何 NSX-T 依赖项问题，并假定 RHEL 计算机可以访问 RHEL 存储库。

6 重新加载 OVS 内核模块。

```
/etc/init.d/openvswitch force-reload-kmod
```

要进行验证，您可以运行 **rpm -qa | grep nsx** 命令。

```
user@host:~$ rpm -qa | grep nsx

nsxa-<release>.el7.x86_64.rpm
nsx-agent-<release>.el7.x86_64.rpm
nsx-aggservice-<release>.el7.x86_64.rpm
nsx-cli-<release>.x86_64.rpm
nsx-da-<release>.el7.x86_64.rpm
nsx-host-<release>.x86_64.rpm
```

VMware, Inc. 保留所有权利。

```
nsx-host_node_status_reporter-<release>.el7.x86_64.rpm
nsx-lldp-<release>.el7.x86_64.rpm
nsx-logical_exporter-<release>.el7.x86_64.rpm
nsx-mpa-<release>.el7.x86_64.rpm
nsx-netcpa-<release>.el7.x86_64.rpm
nsx-sfhc-<release>.el7.x86_64.rpm
nsx-transport_node_status-<release>.el7.x86_64.rpm
```

后续步骤

将主机添加到 NSX-T 管理层面。请参阅将管理程序主机加入管理层面。

将管理程序主机加入管理层面

通过将管理程序主机加入管理层面，可以确保 NSX Manager 和主机可以相互通信。

前提条件

必须完成 NSX-T 模块安装。

步骤

1 打开到 NSX Manager 设备的 SSH 会话。

2 打开到管理程序主机的 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 特有的数字串。

例如：

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

4 在管理程序主机上，运行 **/opt/vmware/nsx-cli/bin/scripts/nsxcli** 命令以进入 NSX-T CLI。

注 对于 KVM，请以超级用户 (sudo) 身份运行该命令。

```
[user@host:~] nsxcli
host>
```

提示符将发生变化。

5 在管理程序主机上，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

```
host> join management-plane NSX-Manager1 username admin thumbprint <NSX-Manager1's-thumbprint>
Password for API user: <NSX-Manager1's-password>
Node successfully joined
```

在主机上运行 `get managers` 命令以验证结果。

```
host> get managers
- 192.168.110.47   Connected
```

在 NSX Manager UI 的**架构 > 节点 > 主机 (Fabric > Node > Hosts)**中，验证主机的 MPA 连接是否为**已连接 (Up)**。

您可以使用 **GET https://<nsx-mgr>/api/v1/fabric/nodes/<fabric-node-id>/state** API 调用查看架构主机的状态：

```
{
  "details": [],
  "state": "success"
}
```

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。

将会在每个 ESXi 主机上的 `/etc/vmware/nsx/controller-info.xml` 中看到 NSX Controller 地址。

```
[root@host:~] cat /etc/vmware/nsx/controller-info.xml
<?xml version="1.0" encoding="utf-8"?>
<config>
  <connectionList>
    <connection id="0">
        <server>10.143.1.47</server>
        <port>1234</port>
        <sslEnabled>true</sslEnabled>
        <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
    <connection id="1">
        <server>10.143.1.45</server>
        <port>1234</port>
        <sslEnabled>true</sslEnabled>
        <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
    <connection id="2">
        <server>10.143.1.46</server>
        <port>1234</port>
        <sslEnabled>true</sslEnabled>
        <pemKey>-----BEGIN CERTIFICATE-----...-----END CERTIFICATE-----</pemKey>
    </connection>
  </connectionList>
</config>
```

VMware, Inc. 保留所有权利。

将启动到 NSX-T 的主机连接并处于“CLOSE_WAIT”状态，直到将主机升级为传输节点。您可以使用 **esxcli network ip connection list | grep 1234** 命令查看该内容。

```
# esxcli network ip connection list | grep 1234
tcp        0      0  192.168.210.53:45823       192.168.110.34:1234  CLOSE_WAIT   37256  newreno  netcpa
```

对于 KVM，该命令是 `netstat -anp --tcp | grep 1234`。

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

后续步骤

创建传输区域。请参阅关于传输区域。

传输区域和传输节点

8

传输区域和传输节点是 NSX-T 中的重要概念。

本章讨论了以下主题：

关于传输区域

传输区域是一个容器，它定义了传输节点的潜在范围。传输节点是加入 NSX-T 覆盖网络的管理程序主机和 NSX Edge。对于管理程序主机，这意味着，它托管通过 NSX-T 逻辑交换机进行通信的虚拟机。对于 NSX Edge，这意味着，它具有逻辑路由器上行链路和下行链路。

如果两个传输节点位于相同的传输区域中，在这些传输节点上托管的虚拟机可以“看到”也位于该传输区域中的 NSX-T 逻辑交换机，从而可以连接到这些逻辑交换机。虚拟机可以通过该连接相互通信，并假定虚拟机具有第 2 层/第 3 层可访问性。如果虚拟机连接到位于不同传输区域中的交换机，则虚拟机无法相互通信。传输区域没有取代第 2 层/第 3 层可访问性要求，而是对该可访问性施加了一个限制。换句话说，属于同一传输区域是连接的一个必备条件。在满足该必备条件后，可以进行访问，但不会自动进行。要实现实际可访问性，第 2 层和（对于不同的子网）第 3 层网络必须正常运行。

传输节点可能是管理程序主机或 NSX Edge。NSX Edge 可以属于多个传输区域。管理程序主机（和 NSX-T 逻辑交换机）只能属于一个传输区域。

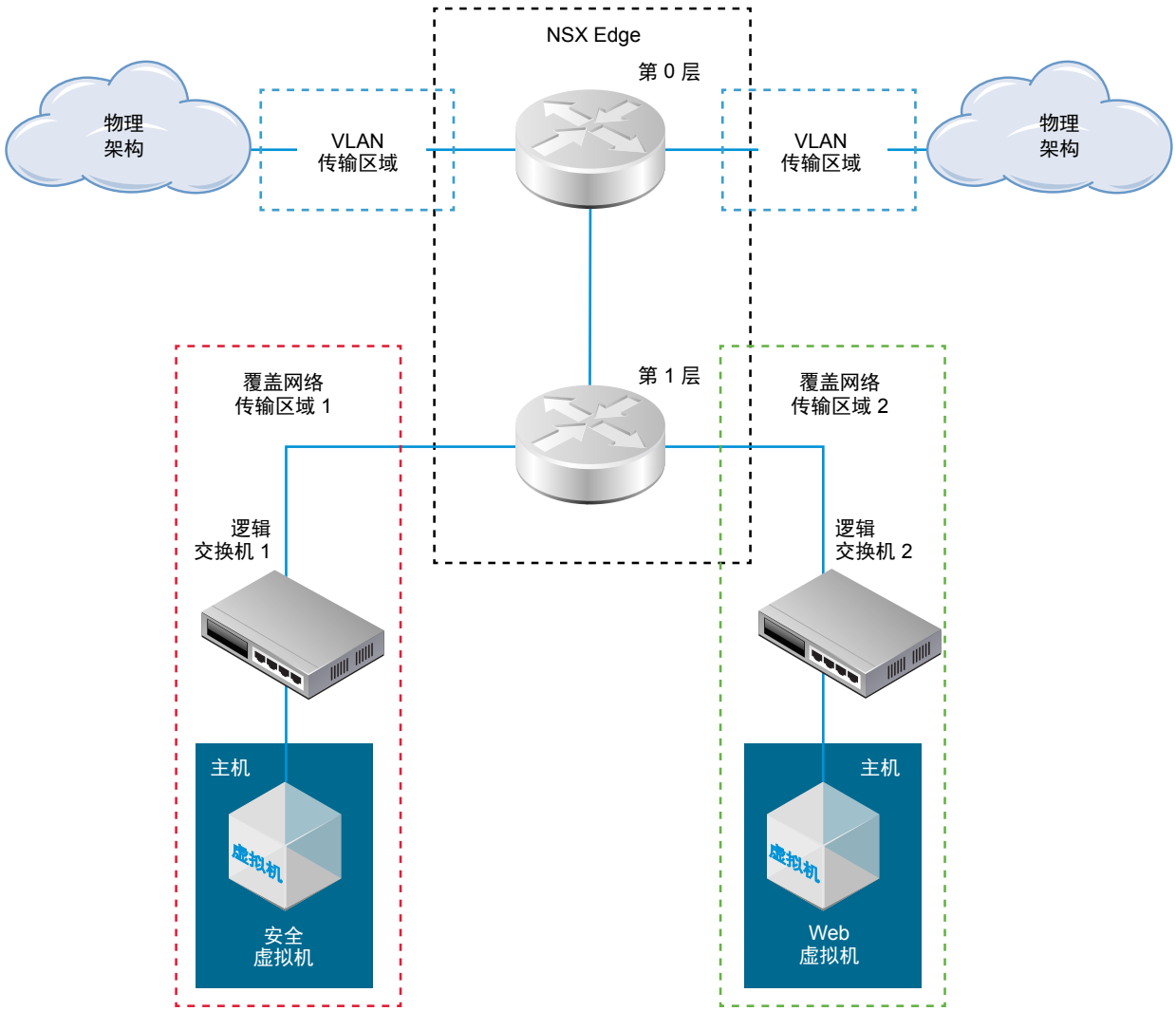
假定单个传输节点包含常规虚拟机和高安全性虚拟机。在您的网络设计中，常规虚拟机应该能够相互访问，但无法访问高安全性虚拟机。要实现该目标，您可以将安全虚拟机放在属于一个名为 secure-tz 的传输区域的主机上。常规虚拟机将位于名为 general-tz 的不同传输区域上。常规虚拟机连接到也位于 general-tz 中的 NSX-T 逻辑交换机。高安全性虚拟机连接到位于 secure-tz 中的 NSX-T 逻辑交换机。不同传输区域中的虚拟机无法相互通信，即使它们位于同一子网中。虚拟机到逻辑交换机的连接最终控制虚拟机可访问性。因此，由于两个逻辑交换机位于单独的传输区域中，因此，“Web 虚拟机”和“安全虚拟机”无法相互访问。

VMware, Inc. 保留所有权利。

NSX Edge 传输节点可以属于多个传输区域：一个覆盖网络传输区域和多个 VLAN 传输区域。VLAN 传输区域用于到外界的 VLAN 上行链路。

例如，下图显示了属于三个传输区域的 NSX Edge：两个 VLAN 传输区域和覆盖网络传输区域 2。覆盖网络传输区域 1 包含一个主机、一个 NSX-T 逻辑交换机和一个安全虚拟机。由于 NSX Edge 不属于覆盖网络传输区域 1，安全虚拟机无法与物理架构相互访问。相反，覆盖网络传输区域 2 中的 Web 虚拟机可以与物理架构通信，因为 NSX Edge 属于覆盖网络传输区域 2。

图 8-1. NSX-T 传输区域



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，以便唯一地标识发出和终止 NSX-T 帧封装的管理程序主机。您可以使用 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，需要在 KVM 主机上添加具有专用默认网关的 sub_a 静态路由。

VMware, Inc. 保留所有权利。

下面是在 Ubuntu 主机上生成的示例路由表，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。

```
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，登录到 `https://<nsx-mgr>` 中的 NSX Manager。

2 选择**清单 > IP 池 (Inventory > IP Pools)**，然后单击**添加 (Add)**。

3 输入 IP 池名称、可选说明和网络设置。

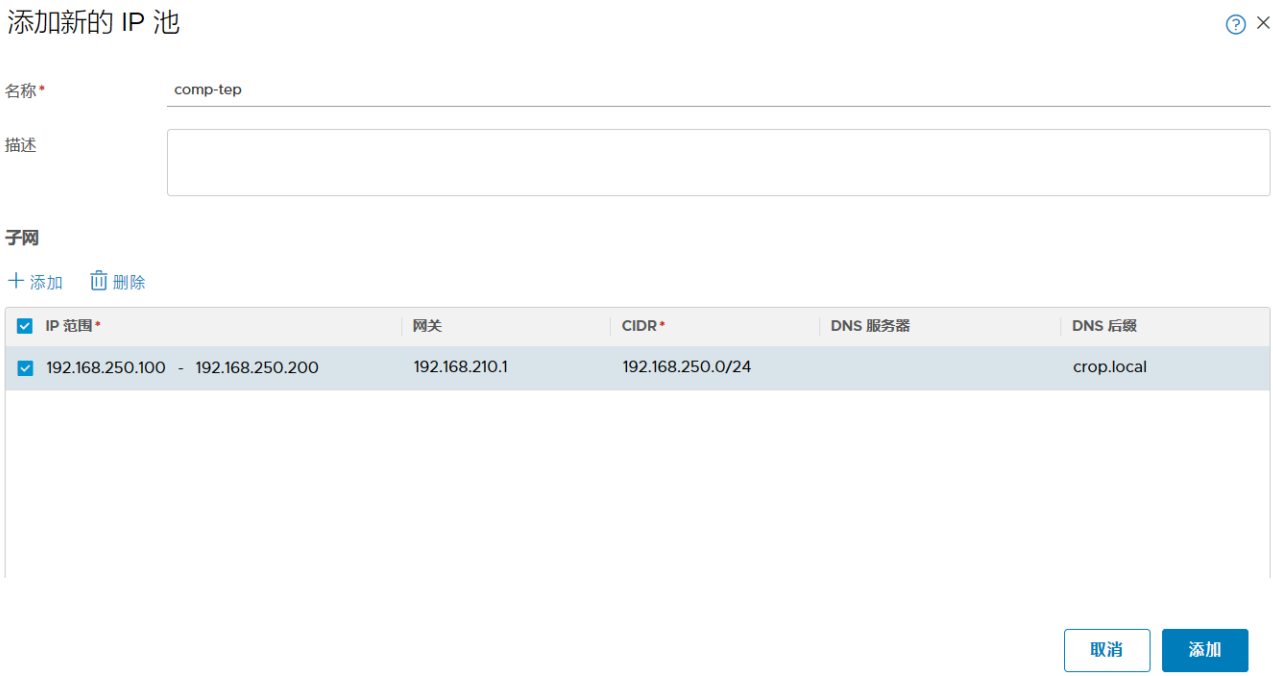
网络设置包括：

- IP 地址范围
- 网关
- 采用 CIDR 表示法的网络地址
- （可选）以逗号分隔的 DNS 服务器列表

VMware, Inc. 保留所有权利。

- （可选）DNS 后缀

例如：



您可以使用 GET https://<nsx-mgr>/api/v1/pools/ip-pools API 调用查看 IP 池：

```
{
  "cursor": "0036e2d8c2e8-f6d7-498e-821b-b7e44d2650a9ip-pool-1",
  "sort_by": "displayName",
  "sort_ascending": true,
  "result_count": 1,
  "results": [
    {
      "id": "e2d8c2e8-f6d7-498e-821b-b7e44d2650a9",
      "display_name": "comp-tep",
      "resource_type": "IpPool",
      "subnets": [
        {
          "dns_nameservers": [
            "192.168.110.10"
          ],
          "allocation_ranges": [
            {
              "start": "192.168.250.100",
              "end": "192.168.250.200"
            }
          ],
          "gateway_ip": "192.168.250.1",
          "cidr": "192.168.250.0/24",
          "dns_suffix": "corp.local"
        }
      ],
```

```
      "_last_modified_user": "admin",
      "_last_modified_time": 1443649891178,
      "_create_time": 1443649891178,
      "_system_owned": false,
      "_create_user": "admin",
      "_revision": 0
    }
  ]
}
```

后续步骤

创建上行链路配置文件。请参阅创建上行链路配置文件。

创建上行链路配置文件

上行链路配置文件是一个主机交换机配置文件，这意味着，它为从管理程序主机到 NSX-T 逻辑交换机或从 NSX Edge 节点到架顶式交换机的链路定义策略。

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。

通过使用上行链路配置文件，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。上行链路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，您可以在上行链路配置文件中指定功能，以后可以在创建 NSX-T 传输节点时应用这些功能。

如果在裸机上安装了 NSX Edge，您可以使用默认上行链路配置文件。默认上行链路配置文件要求具有一个活动上行链路和一个被动备用上行链路。基于虚拟机/设备的 NSX Edge 不支持备用上行链路。在将 NSX Edge 安装为虚拟设备时，您必须创建自定义上行链路配置文件，而不是使用默认上行链路配置文件。对于为基于虚拟机的 NSX Edge 创建的每个上行链路配置文件，该配置文件只能指定一个活动上行链路，而不能指定备用上行链路。

注　尽管如此，如果为每个上行链路创建单独的主机交换机，并且每个主机交换机使用不同的 VLAN，则 NSX Edge 虚拟机允许使用多个上行链路。这是为了支持连接到多个 TOR 交换机的单个 NSX Edge 节点。

前提条件

确保您了解 NSX Edge 网络。请参阅 NSX Edge 网络设置。

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，假定管理程序主机具有两个已连接的物理链路：vmnic0 和 vmnic1。假定当前将 vmnic0 用于管理和存储网络，而当前未使用 vmnic1。这意味着，可以将 vmnic1 作为 NSX-T 上行链路，但不能将 vmnic0 作为上行链路。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，可以将 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，登录到 `https://<nsx-mgr>` 中的 NSX Manager。

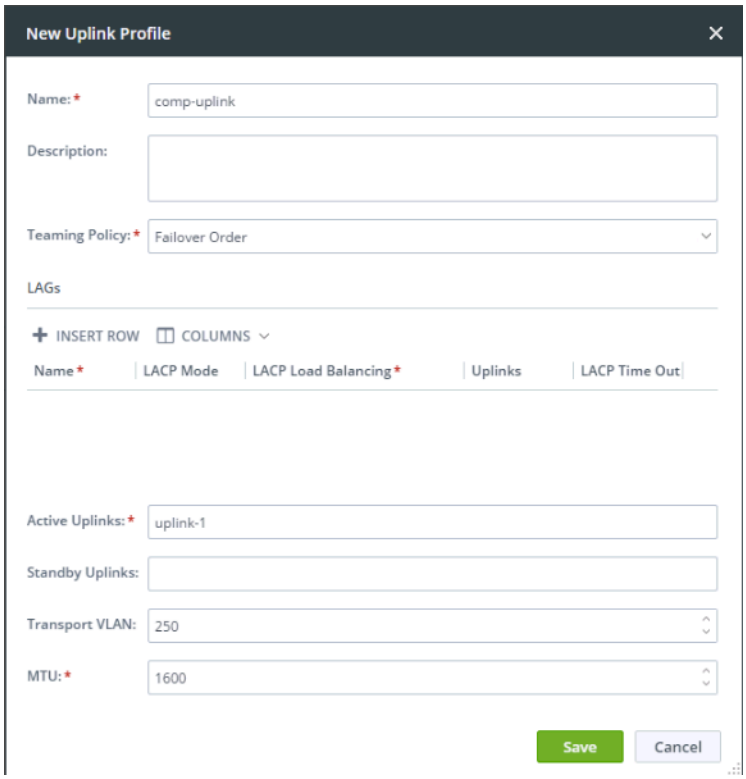
2　选择**架构 > 配置文件 > 上行链路配置文件 (Fabric > Profiles > Uplink Profiles)**，然后单击**添加 (Add)**。

3 输入以下信息：

- 上行链路配置文件名称
- （可选）说明
- 绑定策略：故障切换顺序或负载平衡源（默认为故障切换顺序）
  - 故障切换顺序 - 从活动适配器列表中，始终使用满足故障切换检测条件的最高顺序的上行链路。该选项不会执行实际负载平衡。
  - 负载平衡源 - 根据源以太网 MAC 地址的哈希值选择上行链路。
- （可选）将链路聚合控制协议 (Link Aggregation Control Protocol, LACP) 用于传输网络的链路聚合组 (Link Aggregation Group, LAG)
- 以逗号分隔的活动上行链路名称列表
- （可选）以逗号分隔的备用上行链路名称列表

  在此处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。以后在创建传输节点时，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。
- （可选）传输 VLAN
- MTU（默认值为 1600）

例如：



您可以使用 GET /api/v1/host-switch-profiles API 调用查看上行链路配置文件：


```
{
  "result_count": 2,
  "results": [
    {
      "resource_type": "UplinkHostSwitchProfile",
      "id": "16146a24-122b-4274-b5dd-98b635e4d52d",
      "display_name": "comp-uplink",
      "transport_vlan": 250,
      "teaming": {
        "active_list": [
          {
            "uplink_type": "PNIC",
            "uplink_name": "uplink-1"
          }
        ],
        "standby_list": [],
        "policy": "FAILOVER_ORDER"
      },
      "mtu": 1600,
      "_last_modified_time": 1457984399526,
      "_create_time": 1457984399526,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_create_user": "admin",
      "_revision": 0
    },
    {
      "resource_type": "UplinkHostSwitchProfile",
      "id": "c9e35cec-e9d9-4c51-b52e-17a5c1bd9a38",
      "display_name": "vlan-uplink",
      "transport_vlan": 100,
      "teaming": {
        "active_list": [
          {
            "uplink_type": "PNIC",
            "uplink_name": "uplink-1"
          }
        ],
        "standby_list": [],
        "policy": "FAILOVER_ORDER"
      },
      "mtu": 1600,
      "_last_modified_time": 1457984399574,
      "_create_time": 1457984399574,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_create_user": "admin",
      "_revision": 0
    }
  ]
}
```


VMware, Inc. 保留所有权利。

后续步骤

创建传输区域。请参阅创建传输区域。

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

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 NSX-T 主机交换机。

NSX Edge 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 主机交换机。

主机交换机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，您必须提供主机交换机的名称，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该交换机。主机交换机名称可以是所需的任意名称。

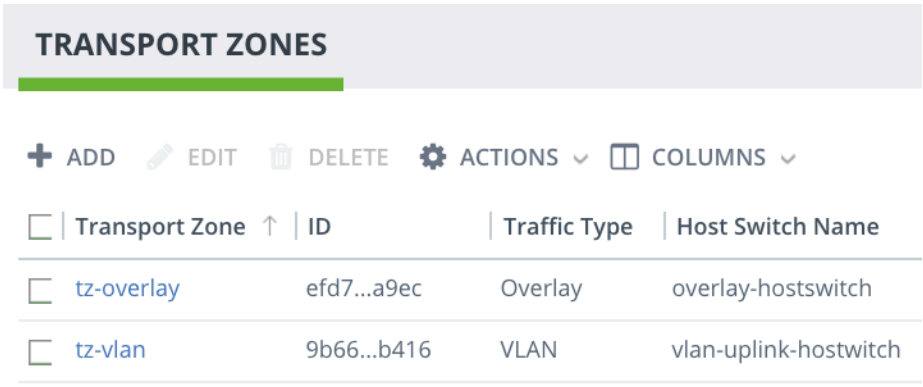
步骤

1 从浏览器中，登录到 `https://<nsx-mgr>` 中的 NSX Manager。

2 选择**架构 > 传输区域 (Fabric > Transport Zones)**，然后单击**添加 (Add)**。

3 输入传输区域名称、主机交换机名称和流量类型（覆盖网络或 VLAN）。

例如：



您可以使用 GET https://<nsx-mgr>/api/v1/transport-zones API 调用查看新的传输区域：


```
{
  "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。请参阅创建主机传输节点。

创建主机传输节点

传输节点是一个可以加入 NSX-T 覆盖网络或 NSX-T VLAN 网络的节点。

对于 KVM 主机，您可以预配置主机交换机，也可以让 NSX Manager 执行配置。对于 ESXi 主机，NSX Manager 始终配置主机交换机。

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 代理不会创建新的证书。

前提条件

- 主机必须加入管理层面，并且**架构 > 主机 (Fabric > Hosts)**页面上的 MPA 连接必须为“已连接”。
- 必须配置一个传输区域。
- 必须配置一个上行链路配置文件（也称为主机交换机配置文件），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。

步骤

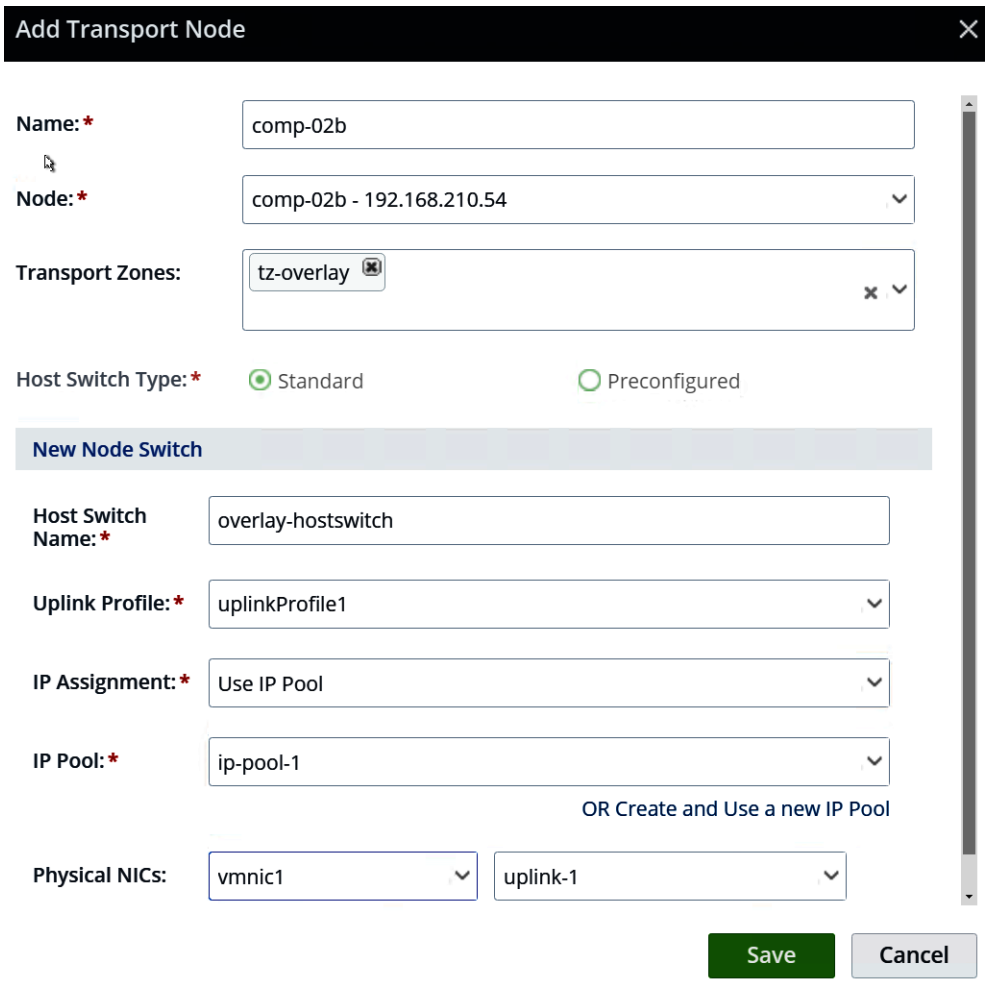
1. 从浏览器中，登录到 `https://<nsx-mgr>` 中的 NSX Manager。
2. 选择**架构 > 节点 > 传输节点 (Fabric > Nodes > Transport Nodes)**，然后单击**添加 (Add)**。
3. 输入传输节点的名称。
4. 从下拉菜单中选择一个节点。
5. （可选）从下拉菜单中选择一个传输区域。
6. （可选）对于 KVM 节点，请选择一种主机交换机类型。

选项	说明
标准	NSX Manager 创建主机交换机。默认情况下，将选择该选项。
预配置	已配置主机交换机。

   对于非 KVM 节点，主机交换机类型始终为**标准 (Standard)**。
7. 对于标准主机交换机，请输入或选择以下主机交换机信息：
   - 主机交换机名称。该名称必须与该节点所属的传输区域的主机交换机名称相同。

- 上行链路配置文件。
- IP 分配。您可以选择**使用 DHCP (Use DHCP)**、**使用 IP 池 (Use IP Pool)**或**使用静态 IP 列表 (Use Static IP List)**。如果选择**使用静态 IP 列表 (Use Static IP List)**，您必须指定以逗号分隔的 IP 地址、网关和子网掩码列表。
- 物理网卡信息

  重要 确保尚未使用物理网卡（例如，标准 vSwitch 或 vSphere Distributed Switch 未使用）。否则，传输节点状态为**部分成功 (partial success)**，并且无法建立架构节点 LCP 连接。



8 对于预配置的主机交换机，请输入以下主机交换机信息：

- 主机交换机外部 ID。该 ID 必须与该节点所属的传输区域的主机交换机名称相同。
- VTEP 名称。

在将主机添加为传输节点后，到 NSX Controller 的主机连接将从“CLOSE_WAIT”状态变为“Established”状态。您可以使用 esxcli network ip connection list | grep 1234 命令查看该状态。

```
# 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，该命令是 netstat –anp ––tcp | grep 1234。

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

您可以使用 GET https://<nsx–mgr>/api/v1/transport–nodes/<node–id> API 调用查看传输节点：

```
{
  "resource_type": "TransportNode",
  "description": "",
  "id": "95c8ce77–f895–43de–adc4–03a3ae2565e2",
  "display_name": "node–comp–01b",
  "tags": [],
  "transport_zone_endpoints": [
    {
      "transport_zone_id": "efd7f38f–c5da–437d–af03–ac598f82a9ec",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3–ab02–4a08–9884–18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ]
    }
  ],
  "host_switches": [
    {
      "host_switch_profile_ids": [
        {
          "value": "8abdb6c0–db83–4e69–8b99–6cd85bfcc61d",
          "key": "UplinkHostSwitchProfile"
        },
        {
          "value": "9e0b4d2d–d155–4b4b–8947–fbfe5b79f7cb",
          "key": "LldpHostSwitchProfile"
        }
      ],
      "host_switch_name": "overlay–hostswitch",
      "pnics": [
        {
          "device_name": "vmnic1",
          "uplink_name": "uplink–1"
        }
      ],
      "static_ip_pool_id": "c78ac522–2a50–43fe–816a–c459a210127e"
```

```
    }
  ],
  "node_id": "c551290a-f682-11e5-ae84-9f8726e1de65",
  "_create_time": 1460051753373,
  "_last_modified_user": "admin",
  "_system_owned": false,
  "_last_modified_time": 1460051753373,
  "_create_user": "admin",
  "_revision": 0
}
```

在成功创建传输节点后，**架构 > 节点 > 主机 (Fabric > Nodes > Hosts)**上的 **LCP 连接 (LCP Connectivity)** 将变为**已连接 (Up)**。要查看更改，请刷新浏览器屏幕。

后续步骤

创建 NSX Edge 传输节点。请参阅创建 NSX Edge 传输节点。

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 NSX-T 主机交换机。

步骤

1 使用 `esxcli network ip interface list` 命令查看 ESXi 上的 NSX-T 主机交换机。

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。

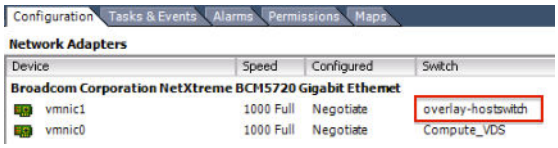
```
# esxcli network ip interface list
...

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，您可以在 UI 中选择主机**配置 > 网络适配器 (Configuration > Network Adapters)**以查看安装的主机交换机。



用于验证 NSX-T 主机交换机安装的 KVM 命令是 `ovs-vsctl show`。请注意，在 KVM 上，主机交换机名称为 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"
```

2 检查为传输节点分配的隧道端点地址。

vmk10 接口从 NSX-T 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
         ...
```

3 检查 API 以了解状态信息。

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"
}
```


创建 NSX Edge 传输节点

传输节点是一个可以加入 NSX-T 覆盖网络或 NSX-T VLAN 网络的节点。如果任何节点包含主机交换机，则可以将其作为传输节点。此类节点包括但不限于 NSX Edge。该过程说明了如何将 NSX Edge 添加为传输节点。

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 代理不会创建新的证书。

前提条件

- NSX Edge 必须加入管理层面，并且**架构 > Edge (Fabric > Edges)** 页面上的 MPA 连接必须为“已连接”。请参阅将 NSX Edge 加入管理层面。
- 必须配置传输区域。
- 必须配置一个上行链路配置文件（主机交换机配置文件），也可以在裸机 NSX Edge 节点中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。

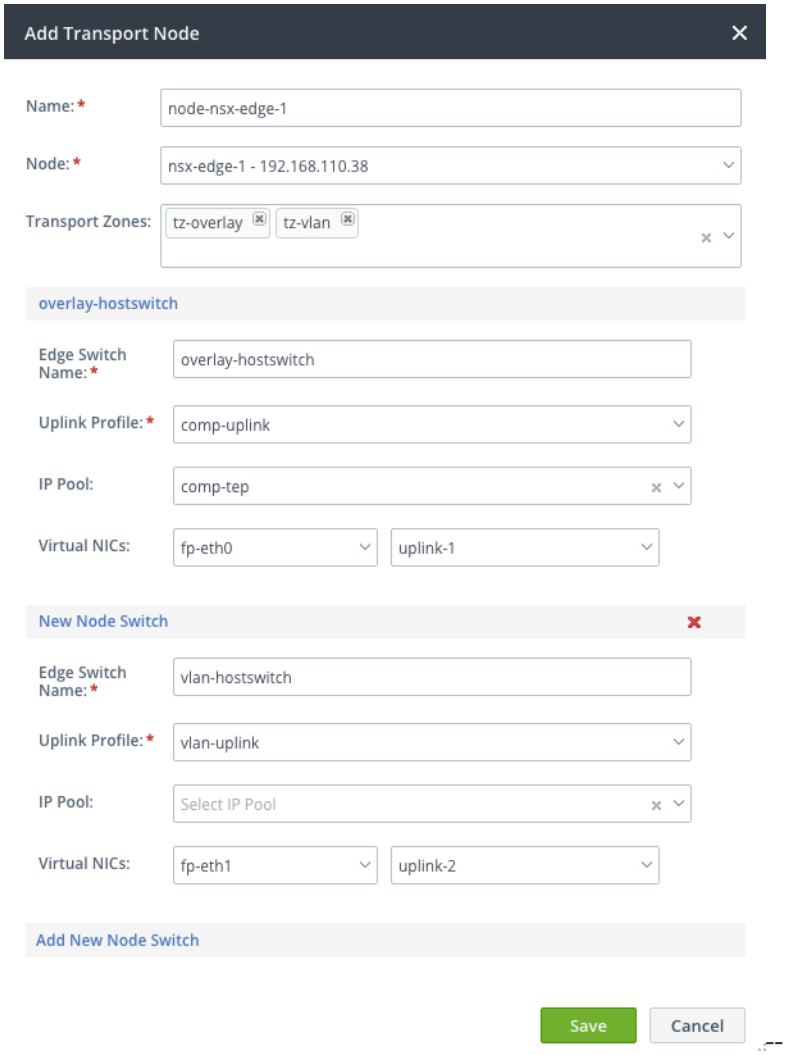
步骤

1. 从浏览器中，登录到 `https://<nsx-mgr>` 中的 NSX Manager。
2. 选择**架构 > 节点 > 传输节点 (Fabric > Nodes > Transport Nodes)**，然后单击**添加 (Add)**。
3. 输入以下信息：IP 地址、主机交换机名称、上行链路配置文件、IP 池（或选择 DHCP）以及物理网卡信息。
   - 输入 NSX Edge 传输节点的名称。
   - 从下拉列表中选择一个 NSX Edge 架构节点。
   - 选择传输区域。通常，NSX Edge 传输节点属于至少两个传输区域：1) 用于 NSX-T 连接的覆盖网络以及 2) 用于上行链路连接的 VLAN。
   - 输入主机交换机的名称。Edge 交换机名称（有时称为主机交换机名称）。Edge 交换机名称必须与在创建传输区域时配置的名称相匹配。
   - 选择上行链路配置文件。
   - 为覆盖网络主机交换机选择一个 IP 池。对于 VLAN 主机交换机，请将“IP 池”字段保留空白。不需要使用覆盖网络隧道端点 IP 地址，因为覆盖网络主机交换机仅用于上行链路 VLAN 流量。
   - 选择虚拟网卡和上行链路。请注意，与主机传输节点不同（它将 vmnicX 作为物理网卡），NSX Edge 传输节点使用 fp-ethX。

VMware, Inc. 保留所有权利。

- 选择上行链路。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。

例如：



4 单击**保存 (Save)**以退出。

您可以使用 `GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>` API 调用查看传输节点：

```
GET https://<nsx-mgr>/api/v1/transport-nodes/78a03020-a3db-44c4-a8fa-f68ad4be6a0c

{
  "resource_type": "TransportNode",
  "id": "78a03020-a3db-44c4-a8fa-f68ad4be6a0c",
  "display_name": "node-comp-01b",
  "transport_zone_endpoints": [
    {
      "transport_zone_id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
```

```
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ]
    }
  ],
  "host_switches": [
    {
      "host_switch_profile_ids": [
        {
          "value": "8abdb6c0-db83-4e69-8b99-6cd85bfcc61d",
          "key": "UplinkHostSwitchProfile"
        },
        {
          "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
          "key": "LldpHostSwitchProfile"
        }
      ],
      "host_switch_name": "overlay-hostswitch",
      "pnics": [
        {
          "device_name": "vmnic1",
          "uplink_name": "uplink-1"
        }
      ],
      "static_ip_pool_id": "c78ac522-2a50-43fe-816a-c459a210127e"
    }
  ],
  "node_id": "c551290a-f682-11e5-ae84-9f8726e1de65",
  "_create_time": 1459547122893,
  "_last_modified_user": "admin",
  "_last_modified_time": 1459547126740,
  "_create_user": "admin",
  "_revision": 1
}
```

有关状态信息，请使用 `GET https://<nsx-mgr>/api/v1/transport-nodes/<transport-node-id>/status` API 调用。例如：

```
{
  "control_connection_status": {
    "degraded_count": 0,
    "down_count": 0,
    "up_count": 1,
    "status": "UP"
  },
  "tunnel_status": {
    "down_count": 0,
    "up_count": 0,
    "status": "UNKNOWN",
    "bfd_status": {
      "bfd_admin_down_count": 0,
      "bfd_up_count": 0,
```

```
        "bfd_init_count": 0,
        "bfd_down_count": 0
      },
      "bfd_diagnostic": {
        "echo_function_failed_count": 0,
        "no_diagnostic_count": 0,
        "path_down_count": 0,
        "administratively_down_count": 0,
        "control_detection_time_expired_count": 0,
        "forwarding_plane_reset_count": 0,
        "reverse_concatenated_path_down_count": 0,
        "neighbor_signaled_session_down_count": 0,
        "concatenated_path_down_count": 0
      }
    },
    "pnic_status": {
      "degraded_count": 0,
      "down_count": 0,
      "up_count": 4,
      "status": "UP"
    },
    "mgmt_connection_status": "UP",
    "node_uuid": "cd4a8501-0ffc-44cf-99cd-55980d3d8aa6",
    "status": "UNKNOWN"
}
```


在成功创建传输节点后，**架构 > 节点 > Edge (Fabric > Nodes > Edges)** 上的 **LCP 连接 (LCP Connectivity)** 将变为**已连接 (Up)**。您可能需要重新加载浏览器屏幕才能看到该更改。

后续步骤

将 NSX Edge 节点添加到 Edge 群集。请参阅创建 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。要创建具有 NAT 的第 0 层逻辑路由器或第 1 层路由器，您必须将其与一个 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）在**架构 > 配置文件 > Edge 群集配置文件 (Fabric > Profiles > Edge Cluster Profiles)**中创建一个 NSX Edge 群集配置文件以实现高可用性 (High Availability, HA)。也可以使用默认 NSX Edge 群集配置文件。

步骤

1. 在 NSX Manager UI 中，导航到**架构 > 节点 > Edge 群集 (Fabric > Nodes > Edge Clusters)**。
2. 输入 NSX Edge 群集的名称。
3. 选择一个 NSX Edge 群集配置文件。
4. 单击**编辑 (Edit)**，然后选择**物理 (Physical)**或**虚拟 (Virtual)**。

   “物理”是指在裸机上安装的 NSX Edge。“虚拟”是指安装为虚拟机/设备的 NSX Edge。
5. 从**可用 (Available)**列中，选择 NSX Edge 并单击右箭头以将其移到**已选定 (Selected)**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。请参阅《 NSX-T 管理指南》。

卸载 NSX-T

9

您可以移除 NSX-T 覆盖网络元素，从 NSX-T 中移除管理程序主机或完全卸载 NSX-T。

本章讨论了以下主题：

- 取消配置 NSX-T 覆盖网络
- 从 NSX-T 中移除主机或完全卸载 NSX-T

取消配置 NSX-T 覆盖网络

如果要删除一个覆盖网络，但保留您的传输节点，请执行以下步骤。

步骤

1 在虚拟机管理工具中，将所有虚拟机与任何逻辑交换机断开连接。

2 在 NSX Manager UI 或 API 中，删除所有逻辑路由器。

3 在 NSX Manager UI 或 API 中，删除所有逻辑交换机端口，然后删除所有逻辑交换机。

4 在 NSX Manager UI 或 API 中，删除所有 NSX Edge，然后删除所有 NSX Edge 群集。

5 根据需要，配置新的 NSX-T 覆盖网络。

从 NSX-T 中移除主机或完全卸载 NSX-T

如果要完全卸载 NSX-T，或者仅从 NSX-T 中移除管理程序主机以使主机脱离 NSX-T 覆盖网络，请执行以下步骤。

以下过程说明了如何彻底卸载 NSX-T。

步骤

1 在虚拟机管理工具中，将主机上的所有虚拟机与任何 NSX-T 逻辑交换机断开连接。

2 在 NSX Manager 中，使用**架构 > 节点 > 传输节点 (Fabric > Nodes > Transport Nodes)** UI 或 `DELETE /api/v1/transport-node/<node-id>` API 删除主机传输节点。

如果删除传输节点，将导致从主机中移除 NSX-T 主机交换机。您可以运行以下命令以进行确认。

```
[root@host:~] esxcli network vswitch dvs vmware list
```

在 KVM 上，该命令是：

```
ovs-vsctl show
```

3 在 NSX Manager CLI 中，启用并启动 NSX-T install-upgrade 服务。

```
nsx-manager-1> set service install-upgrade enable
nsx-manager-1> start service install-upgrade
```

4 从管理层面中取消注册主机并移除 NSX-T 模块。

移除所有 NSX-T 模块可能需要 10 分钟的时间。

您可以使用几种方法移除 NSX-T 模块：

- 在 NSX Manager 中，使用**架构 > 节点 > 主机 > 删除 (Fabric > Nodes > Hosts > Delete)** UI。

  在 UI 中，确保选中**卸载 NSX 组件 (Uninstall NSX Components)**。这会导致在主机上卸载 NSX-T 模块。请注意， 不应在处于正常状态的主机上使用**架构 > 节点 > 主机 > 删除 (Fabric > Nodes > Hosts > Delete)**并取消选中**卸载 NSX 组件 (Uninstall NSX Components)**选项。这仅作为处于错误状态的主机的一种解决方法。

- 使用 `DELETE /api/v1/fabric/nodes/<node-id>` API。

- 使用 CLI。

  1 获取管理器指纹。

  ```
  manager> get certificate api thumbprint
  ```

  2 在主机的 NSX-T CLI 上，运行以下命令，将主机与管理层面断开连接。

  ```
  host> detach management-plane <MANAGER> username <MANAGER-USERNAME> password <MANAGER-PASSWORD> thumbprint <MANAGER-THUMBPRINT>
  ```

  3 在主机上，运行以下命令以移除筛选器。

  ```
  [root@host:~] vsipioctl clearallfilters
  ```

  4 在主机上，运行以下命令以停止 netcpa。

  ```
  [root@host:~] /etc/init.d/netcpad stop
  ```

  5 关闭主机上的虚拟机电源。

  6 从主机中手动卸载 NSX-T 模块。

  请注意，不支持移除单个模块。您必须在一个命令中移除所有模块。

  ```
  esxcli software vib remove -n nsx-aggservice -n nsx-da -n nsx-esx-datapath -n nsx-exporter -n nsx-host -n nsx-lldp -n nsx-mpa -n nsx-netcpa -n nsx-python-protobuf -n nsx-sfhc -n nsx-support-bundle-client -n nsxa -n nsxcli
  ```

在 RHEL 上，使用 `sudo yum remove <package-name>` 命令。在 Ubuntu 上，使用 `apt-get remove <package-name>` 命令。

在这两种情况下，请使用通配符以选择 NSX-T 模块。

还要移除以下模块：

- 在 Ubuntu 上：tcpdump-ovs、nicira-ovs-hypervisor-node、python-openvswitch、openvswitch-*、libgoogle-glog0、libjson-spirit
- 在 RHEL 上：tcpdump-ovs、openvswitch、kmod-openvswitch、glog、json_spirit

后续步骤

在进行该更改后，将从管理层面中移除主机以脱离 NSX-T 覆盖网络。

如果要完全移除 NSX-T，请在虚拟机管理工具中关闭 NSX Manager、NSX Controller 和 NSX Edge，然后将其从磁盘中删除。