NSX-T Data Center 安装指南

修改日期：2019 年 4 月 23 日

VMware NSX-T Data Center 2.3

vmware®

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

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

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

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

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

目录

NSX-T Data Center 安装指南

NSX-T Data Center 安装指南 说明了如何安装 VMware NSX-T™ Data Center 产品。本文档中的信息包括分步配置说明以及建议的最佳做法。

目标读者

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

VMware 技术出版物术语表

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

NSX-T Data Center 概述

1

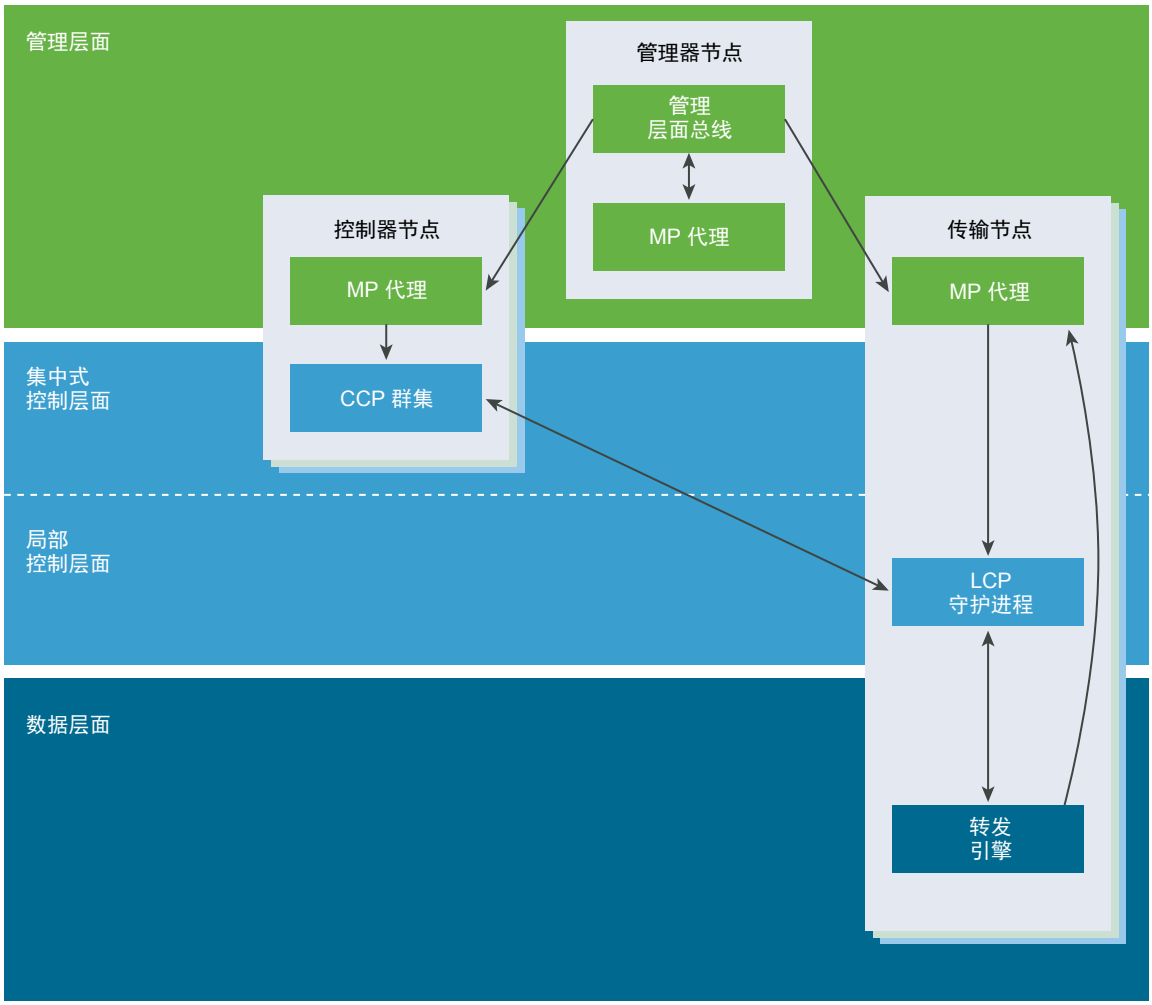
与服务器虚拟化以编程方式创建、删除和还原基于软件的虚拟机 (VM) 以及拍摄虚拟机快照的方式大致相同，NSX-T Data Center 网络虚拟化也以编程方式创建、删除和还原基于软件的虚拟网络。

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

NSX-T Data Center 的工作方式是实现三个单独但集成的层面：管理、控制和数据。这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 Data Center 安装支持单个 NSX Manager 节点。
- 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。

- 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：

- 管理层面
- 控制层面
- 数据层面
- 逻辑交换机
- 逻辑路由器
- 重要概念

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 Data Center，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 Data Center UI 进行更改。

在 NSX 中，还会在所有控制器群集和传输节点上运行管理层面代理 (Management Plane Agent, MPA)。可以在本地和远程访问 MPA。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 是一个虚拟设备，提供图形用户界面 (Graphical User Interface, GUI) 和 REST API，用于创建、配置和监控 NSX-T Data Center 组件，例如逻辑交换机和 NSX Edge 服务网关。

NSX Manager 是 NSX-T Data Center 体系的管理层面。NSX Manager 提供了聚合系统视图并且是 NSX-T Data Center 的集中式网络管理组件。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 提供了一种方法用于监控连接到 NSX-T Data Center 创建的虚拟网络的工作负载以及进行故障排除。它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 Data Center 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 Data Center 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 Policy Manager

NSX Policy Manager 是一个虚拟设备，提供基于意图的系统来简化 NSX-T Data Center 服务的使用。

NSX Policy Manager 提供图形用户界面 (GUI) 和 REST API，用于指定与网络连接、安全性和可用性相关的意图。

NSX Policy Manager 以基于树的数据模型形式接受用户意图，并配置 NSX Manager 以实现该意图。NSX Policy Manager 支持在 NSX Manager 上配置分布式防火墙的通信意图规范。

Cloud Service Manager

Cloud Service Manager (CSM) 为所有公有云构造提供了单一窗口管理端点。

CSM 是一个虚拟设备，提供了用于载入、配置和监控公有云清单的图形用户界面 (GUI) 和 REST API。

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。

控制层面在 NSX-T Data Center 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。

NSX Controller

NSX Controller 称为中央控制层面 (CCP)，是一个高级分布式状态管理系统，可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 Data Center 架构中以编程方式部署虚拟网络。NSX-T Data Center 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都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。

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。

NSX Edge

NSX Edge 为 NSX-T Data Center 部署外部的网络提供路由服务和连接。

可以将 NSX Edge 部署为裸机节点或虚拟机。

需要使用 NSX Edge 以从 NSX-T Data Center 域建立外部连接（通过 Tier-0 路由器并经由 BGP 或静态路由）。此外，如果需要在 Tier-0 或 Tier-1 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

传输区域是控制逻辑交换机可以访问哪些主机的逻辑构造。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。

传输节点不仅是运行本地控制层面守护进程的主机，还是实现 NSX-T Data Center 数据层面的转发引擎。传输节点包含一个 NSX-T Data Center 虚拟分布式交换机 (N-VDS)，它负责根据可用网络服务的配置交换数据包。

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 Data Center 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。

如果主机至少包含一个 NSX 管理的虚拟分布式交换机（N-VDS，以前称为主机交换机），那么该主机可以用作传输节点。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 Data Center 将在主机上安装一个 N-VDS。对于主机所属的每个传输区域，将安装单独的 N-VDS。N-VDS 用于将虚拟机连接到 NSX-T Data Center 逻辑交换机以及创建 NSX-T Data Center 逻辑路由器上行链路和下行链路。

逻辑交换机

NSX-T Data Center 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。

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。

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 Data Center 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。

逻辑路由器

NSX-T Data Center 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。对于东西向连接，逻辑路由器分布在主机的内核内。

通过使用 NSX-T Data Center，可以创建两层逻辑路由器拓扑：顶层逻辑路由器是 Tier-0，底层逻辑路由器是 Tier-1。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 Tier-0 路由和服务，租户管理员控制和配置 Tier-1。在物理网络的 Tier-0 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。Tier-0 的南端连接到多个 Tier-1 路由层，并从这些层中接收路由信息。为了优化资源使用率，Tier-0 不会将来自物理网络的所有路由推送到 Tier-1，而是提供默认信息。

南向 Tier-1 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 Tier-1 连接的子网，必须启用到 Tier-0 的路由重新分发。不过，不会在 Tier-1 和 Tier-0 之间运行传统路由协议（如 OSPF 或 BGP），所有路由将通过 NSX-T Data Center 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 Tier-0，而没有 Tier-1。

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

NSX-T Data Center 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。

重要概念

在文档和用户界面中使用的常见 NSX-T Data Center 概念。

计算管理器	计算管理器是一个管理资源（如主机和虚拟机）的应用程序。一个示例是 vCenter Server。
控制层面	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 Data Center 管理的物理网络或 VLAN。您可以通过 NSX Edge 将逻辑网络或覆盖网络链接到外部网络。例如，客户数据中心的物理网络或物理环境中的 VLAN。
结构层节点	已在 NSX-T Data Center 管理层面中注册并安装了 NSX-T Data Center 模块的主机。要使管理程序主机或 NSX Edge 成为 NSX-T Data Center 覆盖网络的一部分，必须将该主机添加到 NSX-T Data Center 结构层中。
逻辑端口输出	离开虚拟机或逻辑网络的出站网络流量称为输出，因为流量离开虚拟网络并进入数据中心。
逻辑端口输入	离开数据中心并进入虚拟机的入站网络流量称为输入流量。
逻辑路由器	NSX-T Data Center 路由实体。
逻辑路由器端口	可以将逻辑交换机端口或物理网络的上行链路端口连接到的逻辑网络端口。
逻辑交换机	为虚拟机接口和网关接口提供虚拟第 2 层交换的实体。逻辑交换机为租户网络管理员提供物理第 2 层交换机的逻辑等效项，从而允许他们将一组虚拟机连接到一个通用广播域。逻辑交换机是一个独立于物理管理程序基础架构的逻辑实体并跨很多管理程序，从而连接虚拟机而不考虑它们所在的物理位置。 在多租户云中，很多逻辑交换机可能在同一管理程序硬件上并列存在，并且每个第 2 层分段与其他分段隔离。可以使用逻辑路由器连接逻辑交换机，逻辑路由器可以提供连接到外部物理网络的上行链路端口。
逻辑交换机端口	用于建立到虚拟机网络接口或逻辑路由器接口的连接的逻辑交换机连接点。逻辑交换机端口报告应用的交换配置文件、端口状态和链路状态。
管理层面	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 Data Center 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。
NSX Edge 节点	功能目标是提供计算能力以提供 IP 路由和 IP 服务功能的组件。
NSX 管理的虚拟分布式交换机或 KVM Open vSwitch	在管理程序上运行并提供流量转发的软件。租户网络管理员看不到 NSX 管理的虚拟分布式交换机（N-VDS，以前称为主机交换机）或 OVS，它们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虚拟交换机配置网络流量表，它们构成了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虚拟交换机流量表。 N-VDS 有两种模式：标准和增强型数据路径。增强型数据路径 N-VDS 的性能功能支持网络功能虚拟化 (Network Functions Virtualization, NFV) 工作负载。
NSX Manager	托管 API 服务、管理层面和代理服务的节点。
NSX-T Data Center Unified Appliance	NSX-T Data Center Unified Appliance 是 NSX-T Data Center 安装软件包中包含的一个设备。您可以使用 NSX Manager、Policy Manager 或 Cloud Service Manager 角色部署该设备。当前，设备一次仅支持一个角色。
Open vSwitch (OVS)	作为 XenServer、Xen、KVM 和其他基于 Linux 的管理程序中的虚拟交换机的开源软件交换机。
覆盖逻辑网络	使用“第 3 层中的第 2 层”隧道实现的逻辑网络，将虚拟机看到的拓扑从物理网络中解耦出来。
物理接口 (pNIC)	在其中安装管理程序的物理服务器上的网络接口。
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。
传输节点	可以加入 NSX-T Data Center 覆盖网络或 NSX-T Data Center VLAN 网络的节点。对于 KVM 主机，您可以预配置 N-VDS，也可以让 NSX Manager 执行配置。对于 ESXi 主机，NSX Manager 始终配置 N-VDS。
上行链路配置文件	定义管理程序主机到 NSX-T Data Center 逻辑交换机或 NSX Edge 节点到架顶式交换机的链路策略。上行链路配置文件定义的设置可能包括绑定策略、活动/备用链路、传输 VLAN ID 以及 MTU 设置。
虚拟机接口 (vNIC)	虚拟机上的网络接口，它在虚拟客户机操作系统和标准 vSwitch 或 vSphere Distributed Switch 之间提供连接。可以将 vNIC 连接到一个逻辑端口。您可以根据其唯一 ID (UUID) 识别 vNIC。
虚拟隧道端点	允许管理程序主机加入 NSX-T Data Center 覆盖网络。NSX-T Data Center 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 层网络结构上部署第 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。

安装准备工作

2

在安装 NSX-T Data Center 之前，请确保准备您的环境。

本章讨论了以下主题：

- 系统要求
- 端口和协议
- NSX-T Data Center 安装任务概览

系统要求

NSX-T Data Center 具有有关硬件资源和软件版本的特定要求。

管理程序要求

管理程序	版本	CPU 内核	内存
vSphere	支持的 vSphere 版本	4	16 GB
RHEL KVM	7.5 和 7.4	4	16 GB
Ubuntu KVM	16.04.2 LTS	4	16 GB
CentOS KVM	7.4	4	16 GB

NSX-T Data Center 在 RHEL 7.5、RHEL 7.4、Ubuntu 16.04 和 CentOS 7.4 上支持主机准备。在 RHEL 7.5 和 CentOS 7.4 上不支持 NSX Manager 和 NSX Controller 部署。仅在 vSphere 上支持 NSX Edge 节点部署。

对于 ESXi 主机，NSX-T Data Center 在 vSphere 6.7 U1 或更高版本上支持主机配置文件和自动部署功能。

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

裸机服务器要求

操作系统	版本	CPU 内核	内存
RHEL	7.5 和 7.4	4	16 GB
Ubuntu	16.04.2 LTS	4	16 GB
CentOS	7.4	4	16 GB

NSX Manager 资源要求

精简虚拟磁盘大小为 3.1 GB，厚虚拟磁盘大小为 200 GB。

设备	内存	vCPU	存储	虚拟机硬件版本
NSX Manager 小型虚拟机	8 GB	2	200 GB	10 或更高版本
NSX Manager 中型虚拟机	16 GB	4	200 GB	10 或更高版本
NSX Manager 中大型虚拟机	24 GB	6	200 GB	10 或更高版本
NSX Manager 大型虚拟机	32 GB	8	200 GB	10 或更高版本
NSX Manager 超大型虚拟机	48 GB	12	200 GB	10 或更高版本

注　NSX Manager 小型虚拟机应该在实验室和概念证明部署中使用。

NSX Manager 资源要求适用于 NSX Policy Manager 和 Cloud Service Manager。

NSX Controller 资源要求

设备	内存	vCPU	磁盘空间	部署类型
NSX Controller 小型虚拟机	8 GB	2	120 GB	实验室和概念证明部署
NSX Controller 中型虚拟机	16 GB	4	120 GB	建议用于中型部署
NSX Controller 大型虚拟机	32 GB	8	120 GB	大规模部署所需

注　部署三个 NSX Controller 以确保高可用性并避免 NSX-T Data Center 控制层面出现任何中断。

每个 NSX Controller 群集必须在三个单独的物理管理程序主机上，才能避免影响 NSX-T Data Center 控制层面的单个物理管理程序主机故障。请参见《NSX-T Data Center 参考设计》指南。

对于没有生产工作负载的实验室和概念证明部署，可以具有单个 NSX Controller 以节省资源。

从 vSphere OVF 部署用户界面，只能部署小型和大型虚拟机规格。

NSX Edge 虚拟机资源要求

部署大小	内存	vCPU	磁盘空间	虚拟机硬件版本
小型	4 GB	2	120 GB	10 或更高版本（vSphere 5.5 或更高版本）
中等	8 GB	4	120 GB	10 或更高版本（vSphere 5.5 或更高版本）
大型	16 GB	8	120 GB	10 或更高版本（vSphere 5.5 或更高版本）

注　对于 NSX Manager 和 NSX Edge，小型设备适用于概念证明部署。中型设备适用于典型生产环境，最多可以支持 64 个管理程序。大型设备适用于具有超过 64 个管理程序的大型部署。

注　仅针对 NSX Edge 虚拟机支持 VMXNET 3 vNIC。

NSX Edge 虚拟机和裸机 NSX Edge CPU 要求

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

对于 DPDK 支持，底层平台需要满足以下要求：

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

注 由于 NSX-T Data Center 数据层面使用 Intel 的数据层面开发工具包 (Data Plane Development Kit, DPDK) 中的网络功能，仅支持基于 Intel 的 CPU。

硬件	类型
CPU	■ Xeon 56xx (Westmere-EP) ■ Xeon E7-xxxx（Westmere-EX 和更高版本 CPU） ■ Xeon E5-xxxx（Sandy Bridge 和更高版本 CPU）

裸机 NSX Edge 硬件要求

确认在该 URL https://certification.ubuntu.com/server/models/?release=16.04%20LTS&category=Server 中列出了裸机 NSX Edge 硬件。如果未列出该硬件，则在 NSX Edge 设备上存储、视频适配器或主板组件可能未正常工作。

裸机 NSX Edge 特定网卡要求

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

裸机 NSX Edge 内存、CPU 和磁盘要求

内存	CPU 内核	磁盘空间
32 GB	8	200 GB

增强型数据路径网卡驱动程序

从 My VMware 页面下载支持的网卡驱动程序。

网卡	网卡驱动程序
Intel 82599	ixgben 1.1.0.26-1OEM.670.0.0.7535516
Intel(R) Ethernet Controller X710 for 10GbE SFP+ Intel(R) Ethernet Controller XL710 for 40GbE QSFP+	i40en 1.1.3-1OEM.670.0.0.8169922

NSX Manager 浏览器支持

浏览器	Windows 10	Windows 8.1	Ubuntu 14.04	Mac OS X 10.11 和 10.12
Internet Explorer 11	是	是		
Firefox 55			是	是
Chrome 60	是	是		是
Safari 10				是
Microsoft Edge 40	是			

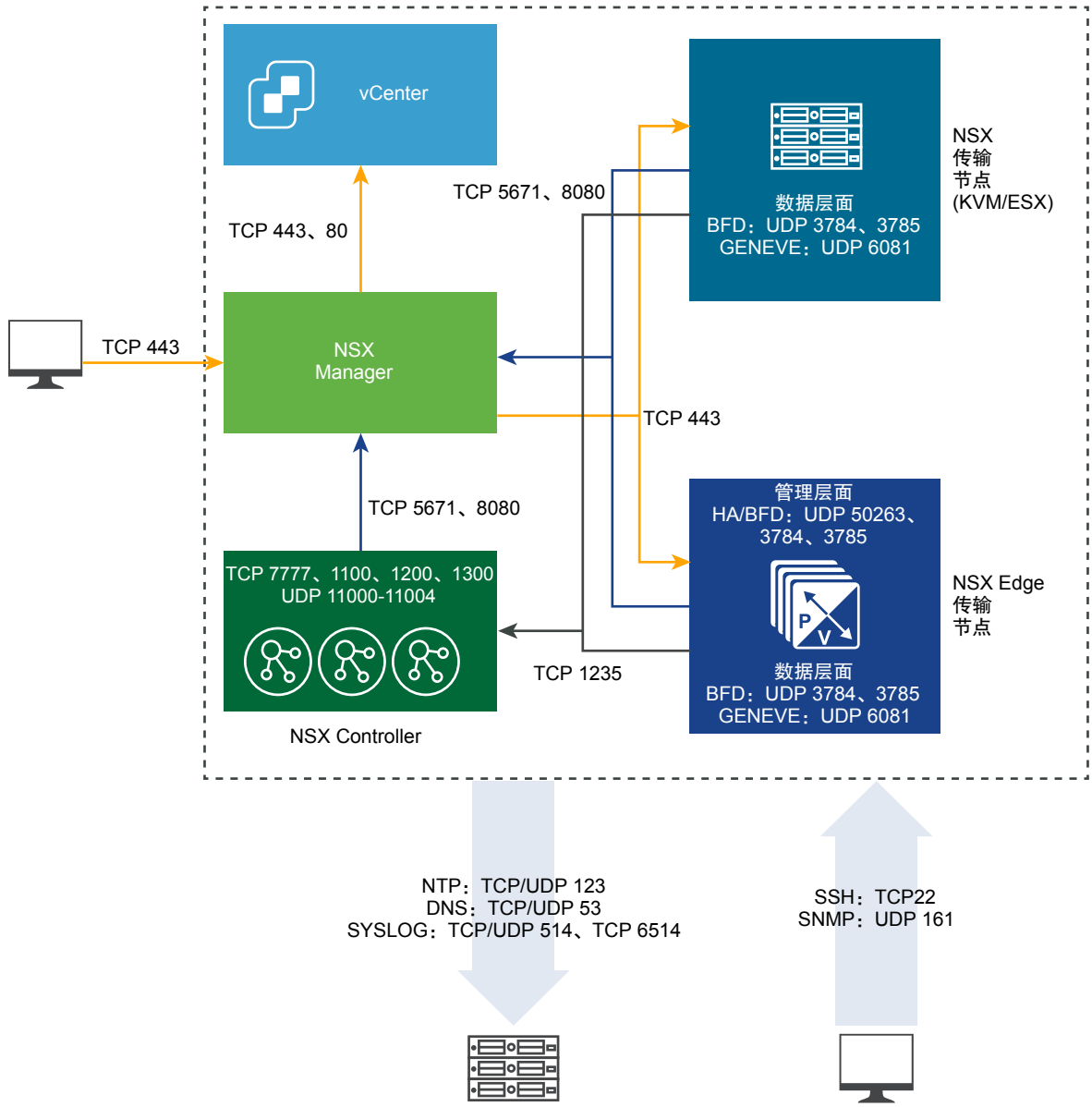
注　不支持兼容模式下的 Internet Explorer 11。

支持的浏览器最小分辨率为 1280 x 800 像素。

端口和协议

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

图 2-1. NSX-T Data Center 端口和协议



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

一些内部守护进程可以通过环回或 UNIX 域套接字进行通信：

- KVM：MPA、netcpa、nsx-agent、OVS
- 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。

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

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

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

NSX Manager 使用的 TCP 和 UDP 端口

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

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

表 2-1. NSX Manager 使用的 TCP 和 UDP 端口

源	目标	端口	协议	说明
管理客户端	NSX Manager	22	TCP	SSH（默认禁用）
NTP 服务器	NSX Manager	123	UDP	NTP
管理客户端	NSX Manager	443	TCP	NSX API 服务器
SNMP 服务器	NSX Manager	161	UDP	SNMP
NSX Controller、NSX Edge 节点、传输节点、vCenter Server	NSX Manager	8080	TCP	安装/升级 HTTP 存储库
NSX Controller、NSX Edge 节点、传输节点	NSX Manager	5671	TCP	NSX 消息传递
NSX Manager	管理 SCP 服务器	22	TCP	SSH（上载支持包、备份等）
NSX Manager	DNS 服务器	53	TCP	DNS
NSX Manager	DNS 服务器	53	UDP	DNS
NSX Manager	NTP 服务器	123	UDP	NTP
NSX Manager	SNMP 服务器	161、162	TCP	SNMP
NSX Manager	SNMP 服务器	161、162	UDP	SNMP
NSX Manager	Syslog 服务器	514	TCP	Syslog
NSX Manager	Syslog 服务器	514	UDP	Syslog
NSX Manager	Syslog 服务器	6514	TCP	Syslog
NSX Manager	Syslog 服务器	6514	UDP	Syslog
NSX Manager	LogInsight 服务器	9000	TCP	Log Insight 代理

表 2-1. NSX Manager 使用的 TCP 和 UDP 端口 （续）

源	目标	端口	协议	说明
NSX Manager	跟踪路由目标	33434 - 33523	UDP	跟踪路由
NSX Manager	vCenter Server	80	TCP	NSX Manager 与计算管理器 (vCenter Server) 通信（如果已配置）。
NSX Manager	vCenter Server	443	TCP	NSX Manager 与计算管理器 (vCenter Server) 通信（如果已配置）。

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 2-2. NSX Controller 使用的 TCP 和 UDP 端口

源	目标	端口	协议	说明
管理客户端	NSX Controller	22	TCP	SSH（默认禁用）
DNS 服务器	NSX Controller	53	UDP	DNS
NTP 服务器	NSX Controller	123	UDP	NTP
SNMP 服务器	NSX Controller	161	UDP	SNMP
NSX Controller	NSX Controller	1100	TCP	Zookeeper 仲裁数
NSX Controller	NSX Controller	1200	TCP	Zookeeper 主节点选举
NSX Controller	NSX Controller	1300	TCP	Zookeeper 服务器
NSX Edge 节点、传输节点	NSX Controller	1235	TCP	CCP-netcpa 通信
NSX Controller	NSX Controller	7777	TCP	Moot RPC
NSX Controller	NSX Controller	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。
跟踪路由目标	NSX Controller	33434 - 33523	UDP	跟踪路由
NSX Controller	SSH 目标	22	TCP	SSH（默认禁用）
NSX Controller	DNS 服务器	53	UDP	DNS
NSX Controller	DNS 服务器	53	TCP	DNS
NSX Controller	NTP 服务器	123	UDP	NTP
NSX Controller	NSX Manager	5671	TCP	NSX 消息传递
NSX Controller	LogInsight 服务器	9000	TCP	Log Insight 代理
NSX Controller	NSX Controller	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。

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

源	目标	端口	协议	说明
NSX Controller	NSX Manager	8080	TCP	NSX 升级
NSX Controller	跟踪路由目标	33434 - 33523	UDP	跟踪路由
NSX Controller	Syslog 服务器	514	UDP	Syslog
NSX Controller	Syslog 服务器	514	TCP	Syslog
NSX Controller	Syslog 服务器	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。

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 2-3. NSX Edge 使用的 TCP 和 UDP 端口

源	目标	端口	协议	说明
管理客户端	NSX Edge 节点	22	TCP	SSH（默认禁用）
NTP 服务器	NSX Edge 节点	123	UDP	NTP
SNMP 服务器	NSX Edge 节点	161	UDP	SNMP
NSX Edge 节点	NSX Edge 节点	1167	TCP	DHCP 后端
NSX Edge 节点、传输节点	NSX Edge 节点	3784、3785	UDP	数据中传输节点 TEP IP 地址之间的 BFD。
NSX 代理	NSX Edge 节点	5555	TCP	NSX Cloud - 实例上的代理与 NSX Cloud 网关通信。
NSX Edge 节点	NSX Edge 节点	6666	TCP	NSX Cloud - NSX Edge 本地通信。
NSX Edge 节点	NSX Manager	8080	TCP	NAPI、NSX-T Data Center 升级
NSX Edge 节点	NSX Edge 节点	2480	TCP	Nestdb
NSX Edge 节点	管理 SCP 或 SSH 服务器	22	TCP	SSH
NSX Edge 节点	DNS 服务器	53	UDP	DNS
NSX Edge 节点	NTP 服务器	123	UDP	NTP
NSX Edge 节点	SNMP 服务器	161、162	UDP	SNMP
NSX Edge 节点	SNMP 服务器	161、162	TCP	SNMP
NSX Edge 节点	NSX Manager	443	TCP	HTTPS
NSX Edge 节点	Syslog 服务器	514	TCP	Syslog
NSX Edge 节点	Syslog 服务器	514	UDP	Syslog
NSX Edge 节点	NSX Edge 节点	1167	TCP	DHCP 后端

表 2-3. NSX Edge 使用的 TCP 和 UDP 端口（续）

源	目标	端口	协议	说明
NSX Edge 节点	NSX Controller	1235	TCP	netcpa
NSX Edge 节点	OpenStack Nova API 服务器	3000 - 9000	TCP	元数据代理
NSX Edge 节点	NSX Manager	5671	TCP	NSX 消息传递
NSX Edge 节点	Syslog 服务器	6514	TCP	Syslog over TLS
NSX Edge 节点	跟踪路由目标	33434 - 33523	UDP	跟踪路由
NSX Edge 节点	NSX Edge 节点	50263	UDP	高可用性

由 vSphere ESXi 、KVM 主机和裸机服务器使用的 TCP 和 UDP 端口

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

表 2-4. vSphere ESXi 和 KVM 主机使用的 TCP 和 UDP 端口

源	目标	端口	协议	说明
NSX Manager	vSphere ESXi 主机	443	TCP	管理和置备连接
NSX Manager	KVM 主机	443	TCP	管理和置备连接
vSphere ESXi 主机	NSX Manager	5671	TCP	与 NSX Manager 的 AMPQ 通信通道
vSphere ESXi 主机	NSX Controller	1235	TCP	控制层面 - LCP 与 CCP 通信
KVM 主机	NSX Manager	5671	TCP	与 NSX Manager 的 AMPQ 通信通道
KVM 主机	NSX Controller	1235	TCP	控制层面 - LCP 与 CCP 通信
vSphere ESXi 主机	NSX Manager	8080	TCP	安装和升级 HTTP 存储库
KVM 主机	NSX Manager	8080	TCP	安装和升级 HTTP 存储库
GENEVE Termination End Point (TEP)	GENEVE Termination End Point (TEP)	6081	UDP	传输网络
NSX-T Data Center 传输节点	NSX-T Data Center 传输节点	3784、3785	UDP	在使用 TEP 接口的数据路径中，TEP 之间的 BFD 会话

NSX-T Data Center 安装任务概览

可以使用对照表跟踪安装进度。

请遵循建议的过程顺序。

1 安装 NSX Manager，请参见第 4 章，NSX Manager 安装。

2 安装 NSX Controller，请参见第 5 章，NSX Controller 安装和群集。

3 将 NSX Controller 加入管理层面，请参见将 NSX Controller 加入 NSX Manager。

4 创建主 NSX Controller 以初始化控制群集，请参见初始化控制群集以创建控制群集主控制器。

5 将 NSX Controller 加入控制群集，请参见将额外的 NSX Controller 加入群集主控制器。

   在添加管理程序主机后，NSX Manager 将安装 NSX-T Data Center 模块。

   注 在安装 NSX-T Data Center 模块时，将在管理程序主机上创建证书。

6 将管理程序主机加入管理层面，请参见将管理程序主机加入管理层面。

   主机将其主机证书发送到管理层面。

7 安装 NSX Edge，请参见第 6 章，NSX Edge 安装。

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

9 创建传输区域和传输节点，请参见第 8 章，传输区域和传输节点。

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

典型的安装顺序如下所示：

1 先安装 NSX Manager。

2 可以安装 NSX Controller 并加入管理层面。

3 可以在加入管理层面之前在管理程序主机上安装 NSX-T Data Center 模块，也可以使用**结构层 > 主机 > 添加** UI 同时执行这两个过程。

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

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 Data Center 逻辑实体和配置状态。

有关详细信息，请参见 NSX-T Data Center 管理指南。

使用 KVM

3

NSX-T Data Center 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。

表 3-1. 支持的 KVM 版本

要求	说明
支持的平台	■ RHEL 7.5 ■ RHEL 7.4 ■ Ubuntu 16.04.2 LTS ■ CentOS 7.4

本章讨论了以下主题：

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。

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

步骤

1 （仅限 Red Hat）打开 `/etc/yum.conf` 文件。

2 搜索行 `exclude`。

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

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

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

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

支持的 RHEL 版本是 7.4。

4 安装 KVM 和桥接实用程序。

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

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

5 检查硬件虚拟化功能。

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

输出应包含 vmx。

6 确认安装了 KVM 模块。

Linux 发布版本	命令

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

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

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

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

注 在不同的环境中，接口名称可能会有所不同。

Linux 发布版本	网络配置

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

Linux 发布版本	网络配置

	您可以使用以下命令检查桥接网络的状态：
	`virsh net-list --all`
	`Name State Autostart Persistent`
	`---`
	`bridge active yes yes`
	`default active yes yes`

RHEL	编辑 /etc/sysconfig/network-scripts/ifcfg-*management_interface*：
	`DEVICE="ens32"`
	`TYPE="Ethernet"`
	`NAME="ens32"`
	`UUID="<UUID>"`
	`BOOTPROTO="none"`
	`HWADDR="<HWADDR>"`
	`ONBOOT="yes"`
	`NM_CONTROLLED="no"`
	`BRIDGE="br0"`
	编辑 /etc/sysconfig/network-scripts/ifcfg-eth1：
	`DEVICE="eth1"`
	`TYPE="Ethernet"`
	`NAME="eth1"`
	`UUID="<UUID>"`
	`BOOTPROTO="none"`
	`HWADDR="<HWADDR>"`
	`ONBOOT="yes"`
	`NM_CONTROLLED="no"`
	编辑 /etc/sysconfig/network-scripts/ifcfg-eth2：
	`DEVICE="eth2"`
	`TYPE="Ethernet"`
	`NAME="eth2"`
	`UUID="<UUID>"`
	`BOOTPROTO="none"`
	`HWADDR="<HWADDR>"`
	`ONBOOT="yes"`
	`NM_CONTROLLED="no"`
	编辑 /etc/sysconfig/network-scripts/ifcfg-br0：
	`DEVICE="br0"`
	`BOOTPROTO="dhcp"`
	`NM_CONTROLLED="no"`
	`ONBOOT="yes"`
	`TYPE="Bridge"`

8 要将 KVM 作为传输节点，请准备网桥。

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

注 在不同的环境中，接口名称可能会有所不同。

Linux 发布版本	网络配置

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

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

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。

执行此步骤后，一旦将 KVM 主机配置为传输节点，就会创建网桥接口“nsx-vtep0.0”。在 Ubuntu 中，/etc/network/interfaces 具有如下条目：

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

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

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

9 要使网络更改生效，请重新启动网络服务 `systemctl restart network` 或重新引导 Linux 服务器。

在 KVM CLI 中管理客户机虚拟机

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

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

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)
```

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 Data Center 组件，例如，逻辑交换机、逻辑路由器和防火墙。

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

NSX-T Data Center 部署只能具有 NSX Manager 的一个实例。如果在 ESXi 主机上部署了 NSX Manager，则可以使用 vSphere High Availability (HA) 功能确保 NSX Manager 的可用性。

表 4-1. NSX Manager 部署、平台和安装要求

要求	说明
支持的部署方法	■ OVA/OVF ■ QCOW2
支持的平台	请参见系统要求。 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，以便在原始主机发生故障时在另一个主机上重新启动虚拟机。
IP 地址	NSX Manager 必须具有静态 IP 地址。您无法在安装后更改该 IP 地址。
NSX-T Data Center 设备密码	■ 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
主机名	在安装 NSX Manager 时，请指定不包含无效字符（如下划线）的主机名。如果主机名包含任何无效的字符，在部署后，主机名将设置为 **nsx-manager**。有关主机名限制的详细信息，请参阅 https://tools.ietf.org/html/rfc952 和 https://tools.ietf.org/html/rfc1123。
VMware Tools	在 ESXi 上运行的 NSX Manager 虚拟机已安装 VMTools。不要移除或升级 VMTools。
系统	■ 确认满足系统要求。请参见系统要求。 ■ 确认打开了所需的端口。请参见端口和协议。 ■ 如果还没有目标虚拟机端口组网络，请创建一个网络。建议将 NSX-T Data Center 设备放在管理虚拟机网络上。 如果具有多个管理网络，您可以添加从 NSX-T Data Center 设备到其他网络的静态路由。 ■ 计划您的 IPv4 IP 地址方案。在该 NSX-T Data Center 版本中，不支持 IPv6。

表 4-1. NSX Manager 部署、平台和安装要求（续）

要求	说明
OVF 特权	确认您具有足够的权限以在 ESXi 主机上部署 OVF 模板。 可部署 OVF 模板的管理工具，例如 vCenter Server 或 vSphere Client。OVF 部署工具必须支持配置选项以允许进行手动配置。 OVF 工具版本必须为 4.0 或更高版本。
客户端插件	必须安装客户端集成插件。

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

NSX Manager 安装方案

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

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

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

注 在设置足够复杂的密码后，设备上的核心服务才会启动。

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

本章讨论了以下主题：

- 安装 NSX Manager 和可用设备
- 使用命令行 OVF Tool 在 ESXi 上安装 NSX Manager
- 在 KVM 上安装 NSX Manager
- 登录到新创建的 NSX Manager

安装 NSX Manager 和可用设备

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

NSX Policy Manager 是用于管理策略的虚拟设备。您可以配置策略，以指定 NSX-T Data Center 组件的规则，如逻辑端口、IP 地址和虚拟机。NSX Policy Manager 规则允许您设置无需指定确切详细信息即可实施的高级别使用和资源访问规则。

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

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。请参见使用命令行 OVF Tool 在 ESXi 上安装 NSX Manager。

步骤

1 找到 NSX-T Data Center Unified Appliance 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**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。

6 为 NSX Manager 选择端口组或目标网络。

7 指定 NSX Manager 密码和 IP 设置。

8 接受 **nsx-manager** 角色。

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

注 不支持 **nsx-manager nsx-cloud-service-manager (multi-role)** 角色。

9 （可选）为了获得最佳性能，请为 NSX-T Data Center 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-T Data Center 组件具有足够的内存以高效地运行。请参见系统要求。

10 打开 NSX-T Data Center 组件控制台以跟踪引导过程。

11 在引导 NSX-T Data Center 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
  ...
```

12 确认 NSX-T Data Center 组件具有所需的连接。

确保您可以执行以下任务。

- 从另一个计算机中 ping 通 NSX-T Data Center 组件。
- NSX-T Data Center 组件可以 ping 通其默认网关。
- NSX-T Data Center 组件可以使用管理接口 ping 通位于与 NSX-T Data Center 组件相同的网络中的管理程序主机。
- NSX-T Data Center 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-T Data Center 组件。

如果未建立连接，请确保虚拟设备的网络适配器位于正确的网络或 VLAN 中。

后续步骤

通过支持的 Web 浏览器连接到 NSX Manager GUI。

URL 是 https://<NSX Manager IP 地址>。例如 https://10.16.176.10。

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 安装或使用 CLI 执行安装，您可以使用 VMware OVF Tool，这是一个命令行实用程序。

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。请参见系统要求。
- 确认打开了所需的端口。请参见端口和协议。

- 如果还没有目标虚拟机端口组网络，请创建一个网络。建议将 NSX-T Data Center 设备放在管理虚拟机网络上。

  如果具有多个管理网络，您可以添加从 NSX-T Data Center 设备到其他网络的静态路由。
- 计划您的 IPv4 IP 地址方案。在该 NSX-T Data Center 版本中，不支持 IPv6。

步骤

- 对于单独的主机，请使用相应的参数运行 `ovftool` 命令。

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-manager
--X:injectOvfEnv
--X:logFile=ovftool.log
 --allowExtraConfig
--datastore=ds1
--net="management"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_role=nsx-manager
--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
Completed successfully
```

- 对于 vCenter Server 管理的主机，请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_role=nsx-manager
--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
Completed successfully
```

- （可选）为了获得最佳性能，请为 NSX-T Data Center 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-T Data Center 组件具有足够的内存以高效地运行。请参见系统要求。

- 打开 NSX-T Data Center 组件控制台以跟踪引导过程。
- 在引导 NSX-T Data Center 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
  ...
```

- 确认 NSX-T Data Center 组件具有所需的连接。

  确保您可以执行以下任务。

  - 从另一个计算机中 ping 通 NSX-T Data Center 组件。
  - NSX-T Data Center 组件可以 ping 通其默认网关。
  - NSX-T Data Center 组件可以使用管理接口 ping 通位于与 NSX-T Data Center 组件相同的网络中的管理程序主机。
  - NSX-T Data Center 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-T Data Center 组件。

  如果未建立连接，请确保虚拟设备的网络适配器位于正确的网络或 VLAN 中。

后续步骤

通过支持的 Web 浏览器连接到 NSX Manager GUI。

URL 是 https://<NSX Manager IP 地址>。例如 https://10.16.176.10。

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。请参见设置 KVM。
- 在 KVM 主机上部署 QCOW2 映像的权限。
- 确认 guestinfo 中的密码符合密码复杂性要求，以便您可以在安装后登录。请参见第 4 章，NSX Manager 安装。

步骤

1 下载 NSX Manager QCOW2 映像，然后使用 SCP 或同步将其复制到将运行 NSX Manager 的 KVM 计算机中。

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_role" oe:value="nsx-manager"/>
         <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。

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

```
sudo guestfish --rw -i -a nsx-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 （可选）为了获得最佳性能，请为 NSX-T Data Center 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-T Data Center 组件具有足够的内存以高效地运行。请参见系统要求。

7 打开 NSX-T Data Center 组件控制台以跟踪引导过程。

8 在引导 NSX-T Data Center 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
  ...
```

9 确认 NSX-T Data Center 组件具有所需的连接。

确保您可以执行以下任务。

- 从另一个计算机中 ping 通 NSX-T Data Center 组件。
- NSX-T Data Center 组件可以 ping 通其默认网关。
- NSX-T Data Center 组件可以使用管理接口 ping 通位于与 NSX-T Data Center 组件相同的网络中的管理程序主机。
- NSX-T Data Center 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-T Data Center 组件。

如果未建立连接，请确保虚拟设备的网络适配器位于正确的网络或 VLAN 中。

10 退出 KVM 控制台。

```
control-]
```

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>。例如 https://10.16.176.10。

注 您必须使用 HTTPS。不支持 HTTP。

登录到新创建的 NSX Manager

安装 NSX Manager 后，可以使用用户界面执行其他安装任务。

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

前提条件

确认安装了 NSX Manager。

步骤

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

此时将显示 EULA。

2 滚动到 EULA 底部并接受 EULA 条款。

3 选择是否加入 VMware 客户体验提升计划 (CEIP)。

4 单击**保存**

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 Data Center 逻辑交换和路由功能。

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，例如 NSX 管理的虚拟分布式交换机（N-VDS，以前称为主机交换机）和 Open vSwitch (OVS)，它们驻留在 ESXi 和其他管理程序（例如 KVM）上。

在生产环境中，您必须有一个具有三个成员的 NSX Controller 群集，以避免 NSX 控制层面出现任何中断。每个控制器均应放在一个唯一的管理程序主机上（共有三个物理管理程序主机），以避免单个物理管理程序主机故障影响 NSX 控制层面。对于不存在任何生产工作负载的实验室和概念证明部署，为了节省资源，可以运行单个控制器。

表 5-1. NSX Controller 部署、平台和安装要求

要求	说明
支持的部署方法	■ OVA/OVF ■ QCOW2 **注** 不支持 PXE 引导部署方法。
支持的平台	请参见系统要求。 在 ESXi 上支持将 NSX Controller 作为虚拟机和 KVM。 **注** 不支持 PXE 引导部署方法。
IP 地址	NSX Controller 必须具有静态 IP 地址。您无法在安装后更改该 IP 地址。 计划您的 IPv4 IP 地址方案。在该 NSX-T Data Center 版本中，不支持 IPv6。
NSX-T Data Center 设备密码	■ 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

表 5-1. NSX Controller 部署、平台和安装要求 （续）

要求	说明
主机名	在安装 NSX Controller 时，请指定不包含无效字符（如下划线）的主机名。如果主机名包含任何无效的字符，在部署后，主机名将设置为 **localhost**。有关主机名限制的详细信息，请参阅 https://tools.ietf.org/html/rfc952 和 https://tools.ietf.org/html/rfc1123。
VMware Tools	在 ESXi 上运行的 NSX Controller 虚拟机已安装 VMTools。不要移除或升级 VMTools。
系统	确认满足系统要求。请参见系统要求。
端口	确认打开了所需的端口。请参见端口和协议。

NSX Controller 安装方案

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

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

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

注

- 请勿使用 root 权限安装守护进程或应用程序。使用 root 权限安装守护进程或应用程序可能会导致您的支持合同失效。仅当 VMware 支持团队要求时才使用 root 权限。
- 在设置足够复杂的密码后，设备上的核心服务才会启动。

  在通过 OVA 文件部署 NSX Controller 后，您无法通过关闭虚拟机电源并从 vCenter Server 中修改 OVA 设置来更改虚拟机的 IP 设置。

本章讨论了以下主题：

- 从 NSX Manager 自动安装控制器和群集
- 使用 GUI 在 ESXi 上安装 NSX Controller

- 使用命令行 OVF Tool 在 ESXi 上安装 NSX Controller
- 在 KVM 上安装 NSX Controller
- 将 NSX Controller 加入 NSX Manager
- 初始化控制群集以创建控制群集主控制器
- 将额外的 NSX Controller 加入群集主控制器

从 NSX Manager 自动安装控制器和群集

您可以将 NSX Manager 配置为在 vSphere ESXi 主机上自动安装控制器。在部署后，这些控制器将自动添加到 vCenter Server 管理的该 vSphere ESXi 主机上的控制器群集中。或者，您也可以使用 NSX Manager REST API 自动安装控制器群集。

NSX Manager 允许您将额外的控制器自动部署到手动部署的现有群集中。但是，要从该群集中删除手动添加的控制器，必须手动将它从群集中移除。

支持的用例

- 创建单节点群集
- 创建多节点群集
- 向现有群集添加节点
- 从正常运行的群集中删除自动部署的控制器

使用 NSX Manager UI 配置控制器和群集自动安装

可以将 NSX Manager 配置为在 vCenter Server 管理的 vSphere ESXi 主机上自动安装控制器。在安装后，这些控制器将自动添加到 vSphere ESXi 主机上的控制器群集中。

前提条件

- 部署 NSX Manager。
- 部署 vCenter Server 和 vSphere ESXi 主机。
- 将 vSphere ESXi 主机注册到 vCenter Server。
- vSphere ESXi 主机必须具有足够的 CPU、内存和硬盘资源以支持 12 个 vCPU、48 GB RAM 和 360 GB 存储。

步骤

1. 登录到 NSX Manager (https://*<nsxmanagerIPAddress>/*)
2. 在 NSX Manager UI 中，如果没有已经注册的 vCenter，请转至**结构层**面板，单击**计算管理器**，然后添加计算管理器。
3. 在“系统”页面上，单击**添加控制器**。
4. 在“通用属性”页面上，输入必要的值。

5 选择**计算管理器**。

6 （可选）您可以启用 SSH。

7 （可选）您可以启用 root 访问。

8 （可选）如果将节点添加到现有群集中，请启用“加入现有群集”。

9 输入并确认初始化并形成群集所需的共享密钥。

注 添加到该群集的所有控制器节点必须使用相同的共享密钥。

10 输入控制器凭据。

11 单击**下一步**。

12 在“控制器”页面上，单击**添加控制器**。

13 为控制器节点输入有效的主机名或完全限定域名。

14 选择群集。

15 （可选）选择资源池资源池仅提供用于部署控制器节点的计算资源池。分配特定的存储资源。

16 （可选）选择主机。

17 选择数据存储。

18 选择主机用于与主机本身内的其他组件进行通信的管理接口。

19 输入静态 IP 地址和端口详细信息 (*<IPAddress>*/*<PortNumber>*) 以及网络掩码。

20 可以添加多个控制器。单击 **+** 按钮，输入控制器详细信息，然后再开始部署。

21 单击**完成**。

将开始自动安装控制器。控制器首先在 NSX Manager 中注册，然后形成群集或加入现有群集。

22 验证控制器是否已在 NSX Manager 中注册。

a 登录到 NSX Manager 控制台。

b 输入 `# get management-cluster status`。

管理群集状态必须为 STABLE。

c 或者，从 NSX Manager UI 验证 Manager 连接是否处于已连接状态。

23 验证控制群集状态。

a 登录到控制器 CLI 控制台。

b 输入 `# get control-cluster status`

控制器群集状态必须为 STABLE。

c 或者，从 NSX Manager UI 验证群集连接是否处于已连接状态。

后续步骤

使用 API 将 NSX Manager 配置为自动安装控制器和群集。请参见使用 API 配置控制器和群集自动安装。

使用 API 配置控制器和群集自动安装

通过使用 API，可以将 NSX Manager 配置为在 vCenter Server 管理的 vSphere ESXi 主机上自动安装控制器。在安装控制器后，它们将自动添加到 vSphere ESXi 主机上的控制器群集中。

步骤

1 在触发自动创建控制器群集的过程之前，您必须获取所需的 vCenter Server ID、计算 ID、存储 ID 和网络 ID 以作为 POST API 负载。

2 登录到 vCenter Server。

`https://<vCenterServer_IPAddress>/mob.`

3 在“值”列中，单击**内容**。

4 在“内容属性”页面中，转到“值”列，搜索数据中心，然后单击组链接。

5 在“组属性”页面中，转到“值”列，然后单击数据中心链接。

6 在“数据中心属性”页面中，复制要用于创建控制器群集的数据存储值和网络值。

7 单击 **HostFolder** 链接。

8 在“组属性”页面上，复制要用于创建控制器群集的群集值。

9 要获取 vCenter Server ID，请转至 NSX Manager UI，然后从“计算管理器”页面复制其 ID。

10 `POST https://<nsx-manager>/api/v1/cluster/nodes/deployments`

```
REQUEST
{
  "deployment_requests": [
    {
      "roles": ["CONTROLLER"],
        "user_settings": {
        "cli_password": "CLIp4$$w4rd",
        "root_password": "ROOTp4$$w4rd"
      },
      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
        "management_network_id": "network-13",
        "hostname": "controller-0",
        "compute_id": "domain-s9",
        "storage_id": "datastore-12",
        "default_gateway_addresses":[
        "10.33.79.253"
        ],
        "management_port_subnets":[
          {
           "ip_addresses":[
           "10.33.79.64"
           ],
            "prefix_length":"22"
```

```
          }
        ]
      }
    },
    {
      "roles": ["CONTROLLER"],
        "user_settings": {
        "cli_password": "VMware$123",
        "root_password": "VMware$123"
      },

      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
        "management_network_id": "network-13",
        "hostname": "controller-1",
        "compute_id": "domain-s9",
        "storage_id": "datastore-12"
        "default_gateway_addresses":[
         "10.33.79.253"
        ],
       "management_port_subnets":[
          {
            "ip_addresses":[
              "10.33.79.65"
            ],
            "prefix_length":"22"
          }
        ]
      }
    }
  ],
                        "deployment_config": {
      "placement_type": "VsphereClusterNodeVMDeploymentConfig",
      "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
      "management_network_id": "network-13",
      "hostname": "controller-0",
      "compute_id": "domain-s9",
      "storage_id": "datastore-12",
      "default_gateway_addresses":[
      "10.33.79.253"
       ],
      "management_port_subnets":[
       {
        "ip_addresses":[
        "10.33.79.66"
         ],
        "prefix_length":"22"
          }
        ]
      }
    },

        "clustering_config": {
    "clustering_type": "ControlClusteringConfig",
```

```
    "shared_secret": "123456",
    "join_to_existing_cluster": false
  }
}

Response
{
  "result_count": 2,
  "results": [
    {
      "user_settings": {
        "cli_password": "[redacted]",
        "root_password": "[redacted]",
        "cli_username": "admin"
      },
      "vm_id": "71f02260-644f-4482-aa9a-ab8570bb49a3",
      "roles": [
        "CONTROLLER"
      ],
      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
        "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
        "management_network_id": "network-13",
        "default_gateway_addresses": [
          "10.33.79.253"
        ],
        "hostname": "controller-0",
        "compute_id": "domain-s9",
        "storage_id": "datastore-12",
        "management_port_subnets": [
          {
            "ip_addresses": [
              "10.33.79.64"
            ],
           "prefix_length": 22
          }
        ]
      },

      "form_factor": "SMALL"
    },

    {
      "user_settings": {
        "cli_password": "[redacted]",
        "root_password": "[redacted]",
        "cli_username": "admin"
      },

      "vm_id": "38029a2b-b9bc-467f-8138-aef784e802cc",
      "roles": [
        "CONTROLLER"
      ],
      "deployment_config": {
        "placement_type": "VsphereClusterNodeVMDeploymentConfig",
```

```
        "vc_id": "69874c95-51ed-4775-bba8-e0d13bdb4fed",
        "management_network_id": "network-13",
        "hostname": "controller-1",
        "compute_id": "domain-s9",
        "storage_id": "datastore-12"
      },
      "form_factor": "MEDIUM"
    }
  ]
}
```

11 您可以使用 API 调用查看部署状态。GET https://<nsx-manager>/api/v1/cluster/nodes/deployments

```
{

  "result_count": 2,
  "results": [
    {
      "user_settings": {
        "cli_password": "[redacted]",
        "root_password": "[redacted]"
      },
         "vm_id": "12f563af-af9f-48f3-848e-e9257c8740b0",
      "roles": [
      "CONTROLLER"
      ],

      "deployment_config": {
      "placement_type": "VsphereClusterNodeVMDeploymentConfig",
      "vc_id": "15145422-47a1-4c55-81da-01d953151d1f",
      "management_network_id": "network-158",
      "hostname": "controller-0",
      "compute_id": "domain-c154",
      "storage_id": "datastore-157"
      },
      "form_factor": "SMALL",
    },
    {
      "user_settings": {
      "cli_password": "[redacted]",
      "root_password": "[redacted]"
      },
      "vm_id": "cc21854c-265b-42de-af5f-05448c00777a",
      "roles": [
      "CONTROLLER"
      ],
      "deployment_config": {
      "placement_type": "VsphereClusterNodeVMDeploymentConfig",
      "vc_id": "feb17651-49a7-4ce6-88b4-41d3f624e53b",
      "management_network_id": "network-158",
      "hostname": "controller-0",
      "compute_id": "domain-c154",
      "storage_id": "datastore-157"
```

```
      },

      "form_factor": "MEDIUM",
    }
  ]

}
```

后续步骤

删除群集。请参见删除 NSX Controller。

删除 NSX Controller

从群集中删除 NSX Controller。

步骤

1 登录到 **https://<nsx-manager-ip>/**

2 单击**系统 > 组件**。

3 在“控制器群集”下面，找到 NSX Controller。

4 单击**设置**图标，然后单击**删除**。

5 单击**确认**。

NSX-T Data Center 将 NSX Controller 与群集断开连接，从 NSX Manager 中将其取消注册，关闭电源，然后删除 NSX Controller。

后续步骤

使用 GUI 在 vSphere ESXi 主机上安装 NSX Controller。请参见使用 GUI 在 ESXi 上安装 NSX Controller。

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。

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 在设置足够复杂的密码后，设备上的核心服务才会启动。

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

前提条件

- 确认满足系统要求。请参见系统要求。
- 确认打开了所需的端口。请参见端口和协议。

- 如果还没有目标虚拟机端口组网络，请创建一个网络。建议将 NSX-T Data Center 设备放在管理虚拟机网络上。

  如果具有多个管理网络，您可以添加从 NSX-T Data Center 设备到其他网络的静态路由。
- 计划您的 IPv4 IP 地址方案。在该 NSX-T Data Center 版本中，不支持 IPv6。
- 确认您具有足够的权限以在 ESXi 主机上部署 OVF 模板。
- 确认主机名不包含下划线。否则，主机名将设置为 *nsx-controller*。
- 可部署 OVF 模板的管理工具，例如，vCenter Server 或 vSphere Client。

  OVF 部署工具必须支持配置选项以允许进行手动配置。
- 必须安装客户端集成插件。

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**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。

6 为 NSX Controller 选择端口组或目标网络。

7 指定 NSX Controller 密码和 IP 设置。

8 （可选）为了获得最佳性能，请为 NSX-T Data Center 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-T Data Center 组件具有足够的内存以高效地运行。请参见系统要求。

9 打开 NSX-T Data Center 组件控制台以跟踪引导过程。

10 在引导 NSX-T Data Center 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
  ...
```

11 确认 NSX-T Data Center 组件具有所需的连接。

确保您可以执行以下任务。

- 从另一个计算机中 ping 通 NSX-T Data Center 组件。
- NSX-T Data Center 组件可以 ping 通其默认网关。
- NSX-T Data Center 组件可以使用管理接口 ping 通位于与 NSX-T Data Center 组件相同的网络中的管理程序主机。
- NSX-T Data Center 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-T Data Center 组件。

如果未建立连接，请确保虚拟设备的网络适配器位于正确的网络或 VLAN 中。

后续步骤

将 NSX Controller 加入管理层面。请参见将 NSX Controller 加入 NSX Manager。

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。请参见系统要求。
- 确认打开了所需的端口。请参见端口和协议。
- 如果还没有目标虚拟机端口组网络，请创建一个网络。建议将 NSX-T Data Center 设备放在管理虚拟机网络上。

  如果具有多个管理网络，您可以添加从 NSX-T Data Center 设备到其他网络的静态路由。
- 计划您的 IPv4 IP 地址方案。在该 NSX-T Data Center 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，请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"
--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_cli_audit_passwd_0=<password>
--prop:nsx_hostname=nsx-controller
<path/url to nsx component ova>
vi://root:<password>@192.168.110.51
```

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

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-controller
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--network="management"
--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_cli_audit_passwd_0=<password>
--prop:nsx_hostname=nsx-controller
<path/url to nsx component ova>
vi://administrator@vsphere.local:<vcenter_password>@192.168.110.24/?ip=192.168.110.51
```

- （可选）为了获得最佳性能，请为 NSX-T Data Center 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-T Data Center 组件具有足够的内存以高效地运行。请参见系统要求。

- 打开 NSX-T Data Center 组件控制台以跟踪引导过程。

- 在引导 NSX-T Data Center 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
  ...
```

- 确认 NSX-T Data Center 组件具有所需的连接。

  确保您可以执行以下任务。

  - 从另一个计算机中 ping 通 NSX-T Data Center 组件。
  - NSX-T Data Center 组件可以 ping 通其默认网关。
  - NSX-T Data Center 组件可以使用管理接口 ping 通位于与 NSX-T Data Center 组件相同的网络中的管理程序主机。
  - NSX-T Data Center 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-T Data Center 组件。

  如果未建立连接，请确保虚拟设备的网络适配器位于正确的网络或 VLAN 中。

后续步骤

将 NSX Controller 加入管理层面。请参见将 NSX Controller 加入 NSX Manager。

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。请参见设置 KVM。
- 在 KVM 主机上部署 QCOW2 映像的权限。

步骤

1 将 NSX Controller QCOW2 映像下载到 `/var/lib/libvirt/images` 目录中。

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_audit_passwd_0" oe:value="<password>"/>
         <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"/>
         <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 NSX Controller，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。

```
sudo 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
16384 --vcpus 2 --network=bridge:br0,model=e1000 --disk path=/var/lib/libvirt/images/nsx-controller-
release_version_number.qcow2,format=qcow2 --nographics --noautoconsole
```

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

6 （可选）为了获得最佳性能，请为 NSX-T Data Center 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-T Data Center 组件具有足够的内存以高效地运行。请参见系统要求。

7 打开 NSX-T Data Center 组件控制台以跟踪引导过程。

8 在引导 NSX-T Data Center 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
  ...
```

9 确认 NSX-T Data Center 组件具有所需的连接。

确保您可以执行以下任务。

- 从另一个计算机中 ping 通 NSX-T Data Center 组件。
- NSX-T Data Center 组件可以 ping 通其默认网关。
- NSX-T Data Center 组件可以使用管理接口 ping 通位于与 NSX-T Data Center 组件相同的网络中的管理程序主机。
- NSX-T Data Center 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-T Data Center 组件。

如果未建立连接，请确保虚拟设备的网络适配器位于正确的网络或 VLAN 中。

后续步骤

将 NSX Controller 加入管理层面。请参见将 NSX Controller 加入 NSX Manager。

将 NSX Controller 加入 NSX Manager

通过将 NSX Controller 加入 NSX Manager，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。
- 确认您具有登录 NSX Manager 和 NSX Controller 设备的管理员权限。

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。

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

4 在每个 NSX Controller 设备上，运行 **join management-plane** 命令。

```
NSX-Controller1> join management-plane NSX-Manager-IP-address username admin thumbprint <NSX-Manager-thumbprint>

Password for API user: <NSX-Manager-password>
Node successfully registered and controller restarted
```

在每个部署的 NSX Controller 节点上运行该命令。

提供以下信息：

- NSX Manager 的 IP 地址以及可选端口号
- NSX Manager 的用户名
- NSX Manager 的证书指纹
- NSX Manager 的密码

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

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

6 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。请参见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 Data Center 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，则控制器无法与管理程序主机进行通信。在群集中，您只需要初始化一个控制器。

前提条件

- 安装至少一个 NSX Controller。

- 将 NSX Controller 加入管理层面。
- 确认您具有登录 NSX Controller 设备的管理员权限。
- 分配一个共享密钥密码。共享密钥密码是用户定义的共享密钥密码（例如，“secret123”）。

步骤

1 为 NSX Controller 打开一个 SSH 会话。

2 运行 `set control-cluster security-model shared-secret secret <secret>` 命令，然后在出现提示时键入共享密钥。

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.
```

4 运行 `get control-cluster status verbose` 命令。

确认 `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
169.254.1.1             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=0
x8,lzxid=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=0
x21e,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=0
xc,lzxid=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=0
x49,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。请参见将额外的 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

- 至少安装三个 NSX Controller 设备。
- 确认您具有登录 NSX Controller 设备的管理员权限。
- 确保 NSX Controller 节点已加入管理层面。请参见将 NSX Controller 加入 NSX Manager。
- 初始化控制群集以创建控制群集主控制器。您只需要初始化第一个控制器。
- 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 Data Center 控制器部署到同一群集中，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 NSX Controller 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`。

6 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 NSX Controller 节点也具有一个 UUID。

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 NSX Controller 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

部署 NSX Edge。请参见第 6 章，NSX Edge 安装。

NSX Edge 安装

6

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

表 6-1. NSX Edge 部署、平台和安装要求

要求	说明
支持的部署方法	■ OVA/OVF ■ 具有 PXE 的 ISO ■ 没有 PXE 的 ISO
支持的平台	仅在 ESXi 或裸机上支持 NSX Edge。 在 KVM 上不支持 NSX Edge。
PXE 安装	对于 root 和 admin 用户密码，必须使用 sha-512 算法对密码字符串进行加密。
NSX-T Data Center 设备密码	■ 至少 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
主机名	在安装 NSX Edge 时，请指定不包含无效字符（如下划线）的主机名。如果主机名包含任何无效的字符，在部署后，主机名将设置为 **localhost**。有关主机名限制的详细信息，请参阅 https://tools.ietf.org/html/rfc952 和 https://tools.ietf.org/html/rfc1123。
VMware Tools	在 ESXi 上运行的 NSX Edge 虚拟机已安装 VMTools。不要移除或升级 VMTools。
系统	确认满足系统要求。请参见系统要求。
NSX 端口	确认打开了所需的端口。请参见端口和协议。 如果还没有目标虚拟机端口组网络，请创建一个网络。建议将 NSX-T Data Center 设备放在管理虚拟机网络上。

表 6-1. NSX Edge 部署、平台和安装要求（续）

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

NSX Edge 安装方案

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

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

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

注　在设置足够复杂的密码后，设备上的核心服务才会启动。

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

本章讨论了以下主题：

- NSX Edge 网络设置
- 从 NSX Manager 自动部署 NSX Edge 虚拟机
- 使用 vSphere GUI 在 ESXi 上安装 NSX Edge
- 使用命令行 OVF Tool 在 ESXi 上安装 NSX Edge
- 通过 ISO 文件使用 PXE 服务器安装 NSX Edge
- 将 NSX Edge 加入管理层面

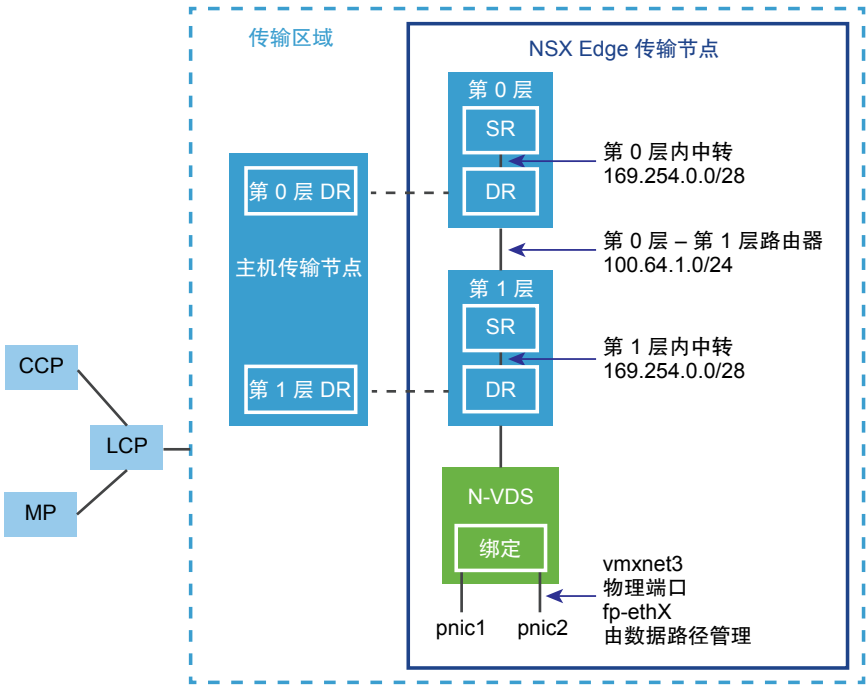
NSX Edge 网络设置

可以使用 ISO、OVA/OVF 或 PXE 启动安装 NSX Edge。无论使用什么安装方法，请确保在安装 NSX Edge 之前准备主机网络。

传输区域中的 NSX Edge 的简要视图

NSX Edge 节点是具有容量池的服务设备，专用于运行无法分发到管理程序的网络服务。在首次部署 Edge 节点时，可以将其视为空容器。

图 6-1. NSX Edge 简要概述



NSX Edge 节点是提供物理网卡以连接到物理基础架构的设备。这些功能包括：

- 到物理基础架构的连接
- NAT
- DHCP 服务器

- 元数据代理
- Edge 防火墙

如果配置了其中的一个服务，或者在逻辑路由器上定义了上行链路以连接到物理基础架构，则会在 NSX Edge 节点上实例化一个 SR。NSX Edge 节点也是一个传输节点，就像 NSX-T Data Center 中的计算节点一样；与计算节点类似，NSX Edge 可以连接到多个传输区域，一个用于覆盖网络，另一个用于与外部设备之间的南北向对等连接。在 NSX Edge 上具有两个传输区域：

覆盖网络传输区域 - 来自于加入 NSX-T Data Center 域的虚拟机的任何流量可能需要能够访问外部设备或网络。这通常描述为外部南北向流量。NSX Edge 节点负责解封从计算节点收到的覆盖网络流量，以及封装发送到计算节点的流量。

VLAN 传输区域 - 除了封装或解封流量功能以外，NSX Edge 节点还需要使用 VLAN 传输区域以提供到物理基础架构的上行链路连接。

默认情况下，SR 和 DR 之间的链路使用 169.254.0.0/28 子网。在部署 Tier-0 或 Tier-1 逻辑路由器时，将自动创建这些路由器内中转链路。您不需要配置或修改链路配置，除非在您的部署中已使用 169.254.0.0/28 子网。在 Tier-1 逻辑路由器上，只有在创建 Tier-1 逻辑路由器时选择了 NSX Edge，才会使用 SR。

为 Tier-0 到 Tier-1 的连接分配的默认地址空间为 100.64.0.0/10。将在 100.64.0.0/10 地址空间中为每个 Tier-0 到 Tier-1 的对等连接提供一个 /31 子网。在创建 Tier-1 路由器并将其连接到 Tier-0 路由器时，将自动创建该链路。您不需要在该链路上配置或修改接口，除非在您的部署中已使用 100.64.0.0/10 子网。

每个 NSX-T Data Center 部署具有一个管理层面群集 (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 Data Center 结构层节点。然后，在将结构层节点添加为传输节点时，将与主机或 NSX Edge 建立 LCP 连接。

NSX Edge 简要概述图显示了绑定在一起以提供高可用性的两个物理网卡（pNIC1 和 pNIC2）的示例。数据路径管理物理网卡。它们可以作为到外部网络的 VLAN 上行链路，或者作为到 NSX-T Data Center 管理的内部虚拟机网络的隧道端点链路。

最佳做法是，将至少两个物理链路分配给每个部署为虚拟机的 NSX Edge。或者，也可以在相同 pNIC 上叠加使用不同 VLAN ID 的端口组。找到的第一个网络链路用于管理。例如，在 NSX Edge 虚拟机上，找到的第一个链路可能是 vnic1。

在裸机安装上，找到的第一个链路可能是 eth0 或 em0。其余链路用于上行链路和隧道。例如，一个链路可能用于 NSX-T Data Center 管理的虚拟机使用的隧道端点。另一个链路可能用于 NSX Edge 到外部 TOR 的上行链路。

您可以查看 NSX Edge 的物理链路信息，以管理员身份登录到 CLI 并运行 `get interfaces` 和 `get physical-ports` 命令。在该 API 中，您可以使用 `GET fabric/nodes/<edge-node-id>/network/interfaces` API 调用。

无论将 NSX Edge 安装为虚拟机设备，还是安装在裸机上，您都可以使用多种方法进行网络配置，具体取决于您的部署。

传输区域和 N-VDS

传输区域控制 NSX-T Data Center 中的第 2 层网络的范围。N-VDS 是在传输节点上创建的软件交换机。传输节点的数据层面中涉及的主要组件是 N-VDS。N-VDS 在传输节点上运行的组件之间转发流量，例如，在虚拟机之间或在内部组件和物理网络之间转发流量。对于后一种情况，N-VDS 必须在传输节点上具有一个或多个物理接口 (pNIC)。与其他虚拟交换机一样，一个 N-VDS 不能与其他 N-VDS 共享物理接口。在使用一组单独的 pNIC 时，它可能与另一个 N-VDS 共存。

共有两种类型的传输区域：

- 用于传输节点之间内部 NSX-T Data Center 隧道的覆盖网络。
- 用于 NSX-T Data Center 外部上行链路的 VLAN。

如果您希望每个 NSX Edge 仅具有一个 N-VDS，则可以这样做。另一个设计方法是，使 NSX Edge 属于多个 VLAN 传输区域，每个上行链路一个传输区域。

最常见的设计方法是三个传输区域：一个覆盖网络传输区域和两个 VLAN 传输区域（用于冗余的上行链路）。

有关传输区域的详细信息，请参阅关于传输区域。

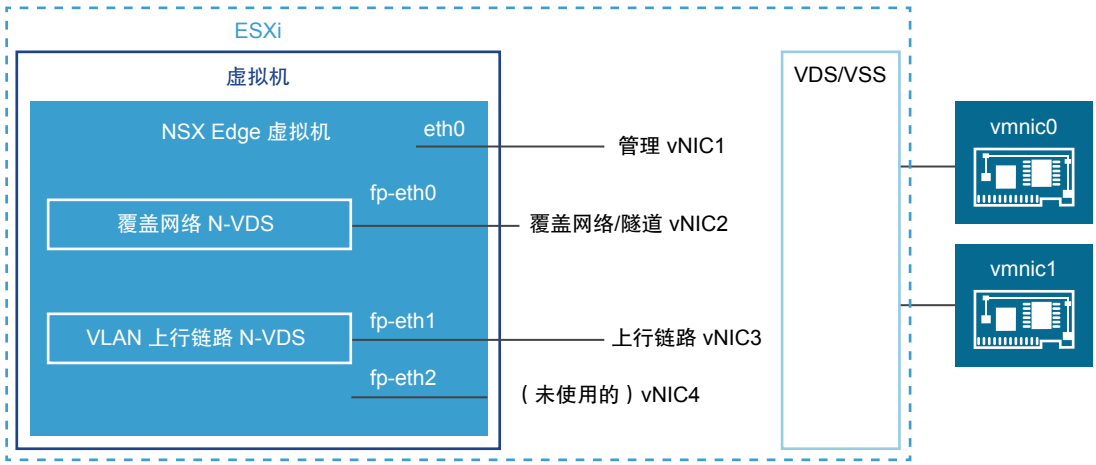
虚拟设备/虚拟机 NSX Edge 网络

NSX Edge 虚拟机具有四个内部接口：eth0、fp-eth0、fp-eth1 和 fp-eth2。eth0 是为管理预留的，而其余接口分配给 DPDK 快速路径。将为到 TOR 交换机的上行链路以及 NSX-T Data Center 覆盖网络隧道分配这些接口。可以灵活地为上行链路或覆盖网络分配接口。例如，可以为覆盖网络流量分配 fp-eth0，并为上行链路流量分配 fp-eth1 和/或 fp-eth2。

在 vSphere Distributed Switch 或 vSphere 标准交换机上，您必须为 NSX Edge 分配至少两个 vmnic 以提供冗余。

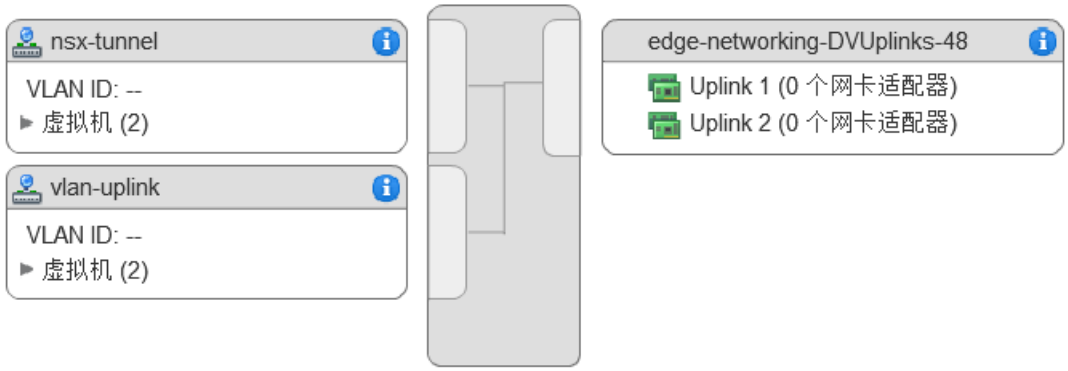
在以下示例物理拓扑中，将 eth0 用于管理网络，将 fp-eth0 用于 NSX-T Data Center 覆盖网络流量，将 fp-eth1 用于 VLAN 上行链路，并且未使用 fp-eth2。如果未使用 fp-eth2，您必须将其断开连接。

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 N-VDS（一个用于隧道，另一个用于上行链路流量）。

该屏幕截图显示虚拟机端口组 nsx-tunnel 和 vlan-uplink。



在部署期间，您必须指定与在虚拟机端口组上配置的名称匹配的网络名称。例如，如果使用 ovftool 部署 NSX Edge，要与该示例中的虚拟机端口组匹配，网络 ovftool 设置可以如下所示：

```
--net:"Network 0-Mgmt" --net:"Network 1-nsx-tunnel" --net:"Network 2=vlan-uplink"
```

此处显示的示例使用虚拟机端口组名称 Mgmt、nsx-tunnel 和 vlan-uplink。您的虚拟机端口组可以使用任意名称。

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)**。

可以在 vSphere Distributed Switch 或 vSphere 标准交换机上安装 NSX Edge 虚拟机。

可以将 NSX Edge 虚拟机安装在 NSX-T Data Center 已就绪的主机上并将其配置为传输节点。有两种部署类型：

- 使用其中的 VSS/VDS 占用主机上单独 pNIC 的 VSS/VDS 端口组可以部署 NSX Edge 虚拟机。主机传输节点占用在主机上安装的 N-VDS 的单独 pNIC。主机传输节点的 N-VDS 与 VSS 或 VDS（它们占用单独的 pNIC）共存。主机 TEP（隧道端点）和 NSX Edge TEP 可以在相同或不同的子网中。
- 在主机传输节点的 N-VDS 上使用支持 VLAN 的的逻辑交换机可以部署 NSX Edge 虚拟机。主机 TEP 和 NSX Edge TEP 必须在不同的子网中。

可以将多个 NSX Edge 虚拟机安装在单个主机上，以利用相同的管理、VLAN 和覆盖网络端口组。

对于具有 vSphere 而没有 N-VDS 的 ESXi 主机上部署的 NSX Edge 虚拟机，您必须执行以下操作：

- 为该 NSX Edge 上运行的 DHCP 服务器启用伪信号。
- 为 NSX Edge 虚拟机启用混杂模式以接收未知单播数据包，因为 MAC 学习默认处于禁用状态。vDS 6.6 或更高版本不需要这样做，因为在这些版本中，MAC 学习默认处于启用状态。

裸机 NSX Edge 网络

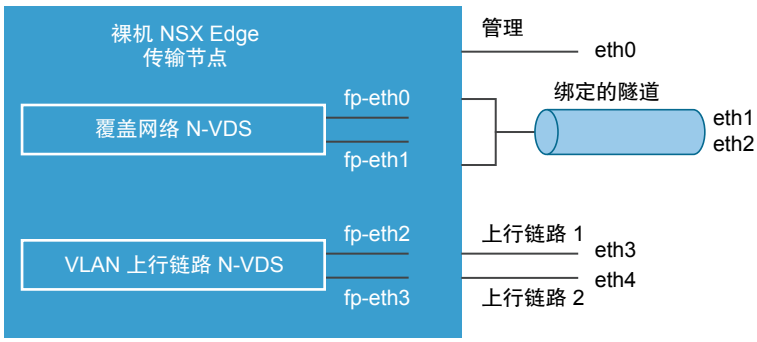
NSX-T Data Center 裸机 NSX Edge 在物理服务器上运行，并且是使用 ISO 文件或 PXE 引导安装的。建议在生产环境中使用裸机 NSX Edge，该环境需要使用 NAT、防火墙和负载平衡器等服务以及第 3 层单播转发。裸机 NSX Edge 在性能方面与虚拟机规格 NSX Edge 不同。它提供了亚秒级聚合、更快的故障切换以及更高的吞吐量。

在安装裸机 NSX Edge 节点时，将为管理保留一个专用接口。如果需要冗余，可以使用两个网卡以提供管理层面高可用性。这些管理接口也可能是 1G。

裸机 NSX Edge 节点最多支持 8 个物理网卡，以传输覆盖网络流量以及到架顶式 (TOR) 交换机的上行链路流量。对于服务器上的 8 个物理网卡，将按照命名方案“fp-ethX”分别创建一个内部接口。这些内部接口分配给 DPDK 快速路径。可以非常灵活地为覆盖网络或上行链路连接分配 fp-eth 接口。

在下面的示例物理拓扑中，fp-eth0 和 fp-eth1 绑定在一起并用于 NSX-T Data Center 覆盖网络隧道。fp-eth2 和 fp-eth3 用作到 TOR 的冗余 VLAN 上行链路。

图 6-3. 建议用于裸机 NSX Edge 网络的一种链路设置



从 NSX Manager 自动部署 NSX Edge 虚拟机

您可以在 NSX Manager UI 中配置一个 NSX Edge，并在 vCenter Server 中自动部署 NSX Edge。

前提条件

- 请参阅 NSX Edge 网络设置中的 NSX Edge 网络要求。
- 如果 vCenter Server 在 NSX-T Data Center 中注册为计算管理器，您可以使用 NSX Manager UI 将主机配置为 NSX Edge 节点并将其自动部署在 vCenter Server 上。
- 确认安装 NSX Edge 的 vCenter Server 数据存储最少具有 120GB 可用空间。
- 确认 vCenter Server 群集或主机有权访问在配置中指定的网络和数据存储。

步骤

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

2 选择**结构层 > 节点 > Edge > 添加 Edge 虚拟机**。

3 键入 NSX Edge 的名称。

4 键入 vCenter Server 的主机名称或 FQDN。

5 选择配置大小：小、中或大。

系统要求因配置大小而异。

6 为系统指定 CLI 和 root 密码。

对 root 和 CLI admin 密码的限制也适用于自动部署。

7 从下拉菜单中选择计算管理器。

计算管理器是在管理层面中注册的 vCenter Server。

8 对于计算管理器，从下拉菜单中选择一个群集或分配一个资源池。

9 选择一个数据存储以存储 NSX Edge 虚拟机文件。

10 选择要在其中部署 NSX Edge 虚拟机的群集。

建议在提供网络管理实用程序的群集中添加 NSX Edge。

11 选择主机或资源池。一次只能添加一个主机。

12 选择 IP 地址，然后键入要在其中放置 NSX Edge 接口的管理网络 IP 地址和路径。输入的 IP 地址必须采用 CIDR 格式。

管理网络必须能够访问 NSX Manager。它必须从 DHCP 服务器接收其 IP 地址。您可以在部署 NSX Edge 后更改这些网络。

13 如果管理网络 IP 地址不属于与 NSX Manager 网络相同的第 2 层，请添加一个默认网关。

确认在 NSX Manager 和 NSX Edge 管理网络之间具有第 3 层连接。

NSX Edge 部署需要 1-2 分钟才能完成。您可以在 UI 中跟踪实时部署状态。

后续步骤

如果 NSX Edge 部署失败，请导航到 `/var/log/cm-inventory/cm-inventory.log` 和 `/var/log/proton/nsxapi.log` 文件以解决该问题。

在将 NSX Edge 添加到 NSX Edge 群集或配置为传输节点之前，请确保新创建的 NSX Edge 节点显示为“节点就绪”。

使用 vSphere 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 Data Center 版本中，不支持 IPv6。

前提条件

- 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**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 vCenter Server 数据中心。

键入的名称将显示在清单中。

选定的文件夹用于将权限应用于 NSX Edge。

4 选择配置大小：小、中或大。

系统要求因配置 NSX Edge 部署大小而异。请参见系统要求。

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 Server 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。

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。

8 指定 NSX Edge 密码和 IP 设置。

9 （可选）为了获得最佳性能，请为 NSX-T Data Center 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-T Data Center 组件具有足够的内存以高效地运行。请参见系统要求。

10 打开 NSX Edge 控制台以跟踪引导过程。

如果未打开控制台窗口，请确保允许弹出窗口。

11 在 NSX Edge 启动后，使用管理员特权登录到 CLI，用户名为 **admin**，密码为 **default**。

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

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

13 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。

14 确认 NSX Edge 设备具有所需的连接。

如果已启用 SSH，请确保可以通过 SSH 访问 NSX Edge。

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

15 解决连接问题。

注 如果未建立连接，请确保虚拟机网络适配器位于正确的网络或 VLAN 中。

默认情况下，NSX Edge 数据路径声明管理网卡（具有 IP 地址和默认路由的网卡）以外的所有虚拟机网卡。如果 DHCP 将错误的网卡分配为管理网卡，请完成以下任务以纠正该问题。

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

b 键入 **`set interface eth0 dhcp plane mgmt`** 命令。

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

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

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

后续步骤

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

使用命令行 OVF Tool 在 ESXi 上安装 NSX Edge

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

在该 NSX-T Data Center 版本中，不支持 IPv6。

前提条件

- 确认满足系统要求。请参见系统要求。
- 确认打开了所需的端口。请参见端口和协议。

- 如果还没有目标虚拟机端口组网络，请创建一个网络。建议将 NSX-T Data Center 设备放在管理虚拟机网络上。

  如果具有多个管理网络，您可以添加从 NSX-T Data Center 设备到其他网络的静态路由。
- 计划您的 IPv4 IP 地址方案。在该 NSX-T Data Center 版本中，不支持 IPv6。
- 请参阅 NSX Edge 网络设置中的 NSX Edge 网络要求。
- 确认您具有足够的权限以在 ESXi 主机上部署 OVF 模板。
- 确认主机名不包含下划线。否则，主机名将设置为 *localhost*。
- OVF Tool 4.0 或更高版本。

步骤

- 对于单独的主机，请使用相应的参数运行 `ovftool` 命令。

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
<path/url to nsx component ova>
vi://root:<password>@192.168.110.51
```

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

```
Powering on VM: nsx-edge-1
Task Completed
Completed successfully
```

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

```
C:\Users\Administrator\Downloads>ovftool
--name=nsx-edge-1
--deploymentOption=medium
--X:injectOvfEnv
--X:logFile=ovftool.log
--allowExtraConfig
--datastore=ds1
--net:"Network 0=Mgmt"
--net:"Network 1=nsx-tunnel"
--net:"Network 2=vlan-uplink"
--net:"Network 3=vlan-uplink"
--acceptAllEulas
--noSSLVerify
--diskMode=thin
--powerOn
--prop:nsx_ip_0=192.168.110.37
--prop:nsx_netmask_0=255.255.255.0
--prop:nsx_gateway_0=192.168.110.1
--prop:nsx_dns1_0=192.168.110.10
--prop:nsx_domain_0=corp.local
--prop:nsx_ntp_0=192.168.110.10
--prop:nsx_isSSHEnabled=True
--prop:nsx_allowSSHRootLogin=True
--prop:nsx_passwd_0=<password>
--prop:nsx_cli_passwd_0=<password>
--prop:nsx_hostname=nsx-edge
<path/url to nsx component ova>
vi://administrator@vsphere.local:<password>@192.168.110.24/?ip=192.168.210.53
```

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

- （可选）为了获得最佳性能，请为 NSX-T Data Center 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-T Data Center 组件具有足够的内存以高效地运行。请参见系统要求。

- 打开 NSX Edge 控制台以跟踪引导过程。
- 在 NSX Edge 启动后，使用管理员特权登录到 CLI，用户名为 **admin**，密码为 **default**。
- 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。

- 确认 NSX Edge 设备具有所需的连接。

  如果已启用 SSH，请确保可以通过 SSH 访问 NSX Edge。

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

- 解决连接问题。

  注 如果未建立连接，请确保虚拟机网络适配器位于正确的网络或 VLAN 中。

  默认情况下，NSX Edge 数据路径声明管理网卡（具有 IP 地址和默认路由的网卡）以外的所有虚拟机网卡。如果 DHCP 将错误的网卡分配为管理网卡，请完成以下任务以纠正该问题。

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

  b 键入 **set interface eth0 dhcp plane mgmt** 命令。

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

  d 键入 **start service dataplane** 命令。

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

后续步骤

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

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。

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

准备 PXE 服务器以进行 NSX Edge 安装

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

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

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

前提条件

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

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

步骤

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

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

  根据指向的 PXE 服务器命名 kickstart 文件。例如：

```
nsxcli.install
```

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

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

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

  要更改 admin 用户密码，请运行以下命令：

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

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

要将 NSX Edge 加入管理层面，请运行以下命令：

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

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

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

例如：

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

7 启动 DHCP 服务。

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

8 验证 DHCP 服务是否正在运行。

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

9 安装 PXE 引导所需的 Apache、TFTP 和其他组件。

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

10 验证 TFTP 和 Apache 是否正在运行。

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

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

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

12 将下一行添加到 /etc/inetd.conf 文件中。

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

13 重新启动 TFTP 服务。

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

14 将 NSX Edge 安装程序 ISO 文件复制或下载到临时文件夹。

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

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

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

您可以使用 Linux 工具（如 mkpasswd）创建密码哈希值。

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

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

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

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

b 替换哈希字符串。

您不需要转义任何特殊字符，例如 $、'、" 或 \。

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

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

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

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

将 192.168.210.82 替换为 TFTP 服务器的 IP 地址。

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

18 将以下几行添加到 /etc/dhcp/dhcpd.conf 文件中。

将 192.168.210.82 替换为 DHCP 服务器的 IP 地址。

```
allow booting;
allow bootp;

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

19 重新启动 DHCP 服务。

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

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

后续步骤

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

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。

前提条件

- 确认系统 BIOS 模式已设置为传统 BIOS。
- 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 从磁盘中引导物理机。

3 选择**自动安装**。

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 打开 NSX Edge 控制台以跟踪引导过程。

如果未打开控制台窗口，请确保允许弹出窗口。

5 在 NSX Edge 启动后，使用管理员特权登录到 CLI，用户名为 **admin**，密码为 **default**。

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

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

7 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。

8 确认 NSX Edge 设备具有所需的连接。

如果已启用 SSH，请确保可以通过 SSH 访问 NSX Edge。

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

9 解决连接问题。

注 如果未建立连接，请确保虚拟机网络适配器位于正确的网络或 VLAN 中。

默认情况下，NSX Edge 数据路径声明管理网卡（具有 IP 地址和默认路由的网卡）以外的所有虚拟机网卡。如果 DHCP 将错误的网卡分配为管理网卡，请完成以下任务以纠正该问题。

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

b 键入 **set interface eth0 dhcp plane mgmt** 命令。

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

d 键入 **start service dataplane** 命令。

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

后续步骤

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

通过 ISO 文件将 NSX Edge 安装为虚拟设备

您可以使用 ISO 文件以手动方式安装 NSX Edge 虚拟机。

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

前提条件

- 请参阅 NSX Edge 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 Data Center 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**。

3 在 ISO 引导期间，打开虚拟机控制台并选择**自动安装**。

在按 Enter 后，可能会出现 10 秒的暂停。

在开机期间，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 在设置足够复杂的密码后，设备上的核心服务才会启动。

4 （可选）为了获得最佳性能，请为 NSX-T Data Center 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-T Data Center 组件具有足够的内存以高效地运行。请参见系统要求。

5 打开 NSX Edge 控制台以跟踪引导过程。

如果未打开控制台窗口，请确保允许弹出窗口。

6 在 NSX Edge 启动后，使用管理员特权登录到 CLI，用户名为 **admin**，密码为 **default**。

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

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

8 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。

9 确认 NSX Edge 设备具有所需的连接。

如果已启用 SSH，请确保可以通过 SSH 访问 NSX Edge。

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

10 解决连接问题。

注 如果未建立连接，请确保虚拟机网络适配器位于正确的网络或 VLAN 中。

默认情况下，NSX Edge 数据路径声明管理网卡（具有 IP 地址和默认路由的网卡）以外的所有虚拟机网卡。如果 DHCP 将错误的网卡分配为管理网卡，请完成以下任务以纠正该问题。

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

b 键入 **`set interface eth0 dhcp plane mgmt`** 命令。

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

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

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

后续步骤

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

访问并确认 NSX Edge 安装

可以登录到 NSX-T Data Center 虚拟机或 NSX-T Data Center 裸机主机，确认安装已成功，并根据需要解决任何问题。

前提条件

- 确认已为安装配置 PXE 服务器。请参见准备 PXE 服务器以进行 NSX Edge 安装。
- 确认 NSX Edge 是使用裸机或 ISO 文件安装的。请参见在裸机上安装 NSX Edge 或通过 ISO 文件将 NSX Edge 安装为虚拟设备。

步骤

1 打开 NSX-T Data Center 虚拟机或 NSX-T Data Center 裸机主机的电源。

2 在引导菜单中，选择 **nsxedge**。

将配置网络，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**。

3 （可选）为了获得最佳性能，请为 NSX-T Data Center 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-T Data Center 组件具有足够的内存以高效地运行。请参见系统要求。

4 打开 NSX Edge 控制台以跟踪引导过程。

如果未打开控制台窗口，请确保允许弹出窗口。

5 在 NSX Edge 启动后，使用管理员特权登录到 CLI，用户名为 **admin**，密码为 **default**。

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

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

7 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。

8 确认 NSX Edge 设备具有所需的连接。

如果已启用 SSH，请确保可以通过 SSH 访问 NSX Edge。

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

9 解决连接问题。

注 如果未建立连接，请确保虚拟机网络适配器位于正确的网络或 VLAN 中。

默认情况下，NSX Edge 数据路径声明管理网卡（具有 IP 地址和默认路由的网卡）以外的所有虚拟机网卡。如果 DHCP 将错误的网卡分配为管理网卡，请完成以下任务以纠正该问题。

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

b 键入 **set interface eth0 dhcp plane mgmt** 命令。

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

d 键入 **start service dataplane** 命令。

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

后续步骤

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

将 NSX Edge 加入管理层面

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

前提条件

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

步骤

1 打开到 NSX Manager 设备的 SSH 会话。

2 打开到 NSX Edge 的 SSH 会话。

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

命令输出是该 NSX Manager 特有的字母数字串。

例如：

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

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

提供以下信息：

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

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

在每个 NSX Edge 节点上重复该命令。

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，NSX Edge 显示在**结构层 > 节点 > Edge** 页面上。NSX Manager 连接应处于“已连接”状态。如果 NSX Manager 连接未处于“已连接”状态，请尝试刷新浏览器窗口。

后续步骤

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

主机准备

7

在准备管理程序主机以运行 NSX-T Data Center 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 Data Center 模块并在 NSX-T Data Center 管理层面中进行了注册。

本章讨论了以下主题：

- 在 KVM 主机或裸机服务器上安装第三方软件包
- 验证 RHEL KVM 主机上的 Open vSwitch 版本
- 将管理程序主机或裸机服务器添加到 NSX-T Data Center 结构层
- 手动安装 NSX-T Data Center 内核模块
- 将管理程序主机加入管理层面

在 KVM 主机或裸机服务器上安装第三方软件包

要准备 KVM 主机或裸机服务器以作为结构层节点，您必须安装一些第三方软件包。

前提条件

- （Red Hat 和 CentOS）在安装第三方软件包之前，请安装虚拟化软件包。在主机上运行以下命令：

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

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

- (Ubuntu) 安装第三方软件包之前，先安装虚拟化软件包。在 Ubuntu 主机上，运行以下命令：

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

- （裸机服务器）没有安装第三方软件包的虚拟化必备条件。

步骤

- 在 Ubuntu 16.04.2 LTS 上，确保在主机上安装了以下第三方软件包。

```
libunwind8
libgflags2v5
libgoogle-perftools4
traceroute
python-mako
python-simplejson
python-unittest2
python-yaml
python-netaddr
libprotobuf9v5
libboost-chrono1.58.0
libgoogle-glog0v5
dkms
libboost-date-time1.58.0
libleveldb1v5
libsnappy1v5
python-gevent
python-protobuf
ieee-data
libyaml-0-2
python-linecache2
python-traceback2
libtcmalloc-minimal4
python-greenlet
python-markupsafe
libboost-program-options1.58.0
```

  如果未在 Ubuntu 16.04.2 LTS 上安装依赖关系软件包，请运行 `apt-get install <package>` 以手动安装软件包。

- 确认注册了 Red Hat 和 CentOS 主机，并且可以访问相应的存储库。

  注 如果使用 NSX-T Data Center UI 准备主机，必须在主机上安装以下依赖项。

  在 RHEL 7.4 和 CentOS 7.4 上安装第三方软件包。

```
yum-utils
wget
redhat-lsb-core
tcpdump
boost-filesystem
PyYAML
boost-iostreams
boost-chrono
python-mako
python-netaddr
python-six
gperftools-libs
libunwind
snappy
```

```
boost-date-time
c-ares
libev
python-gevent
python-greenlet
```

在 RHEL 7.5 上安装第三方软件包。

```
PyYAML
c-ares
libev
libunwind
libyaml
python-beaker
python-gevent
python-greenlet
python-mako
python-markupsafe
python-netaddr
python-paste
python-tempita
```

- 如果手动准备已在 RHEL 或 CentOS 中注册的主机，您无需在主机上安装依赖项。如果未注册主机，请使用 `yum install <package>` 手动安装列出的依赖项。
- 在裸机服务器上安装第三方软件包。
  a 根据您的环境，安装在本主题中列出的 Ubuntu、RHEL 或 CentOS 第三方软件包。
  b 安装裸机服务器特定的第三方软件包。

  Ubuntu - `apt-get install libvirt-libs`

  RHEL 或 CentOS - `yum install libvirt-libs`

验证 RHEL KVM 主机上的 Open vSwitch 版本

如果主机上存在 OVS 软件包，必须移除现有软件包并安装支持的软件包。

受支持的 Open vSwitch 版本为 2.9.1.8614397-1。

步骤

1 确认在主机上已安装当前版本的 Open vSwitch。

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

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

a 删除以下 Open vSwitch 软件包。

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

b 从 NSX Manger 安装 NSX-T Data Center 或执行手动安装过程。

2 或者，升级 NSX-T Data Center 所需的 Open vSwitch 软件包。

a 以管理员身份登录到主机。

b 下载 nsx-lcp 文件并将其复制到 /tmp 目录中。

c 解压缩该软件包。

```
tar -zxvf nsx-lcp-<release>-rhel74_x86_64.tar.gz
```

d 导航到软件包目录。

```
cd nsx-lcp-rhel74_x86_64/
```

e 使用受支持的版本替换现有 Open vSwitch 版本。

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

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

  rpm -Uvh openvswitch-*.rpm --nodeps

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

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

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

后续步骤

将管理程序主机添加到 NSX-T Data Center 结构层。请参见将管理程序主机或裸机服务器添加到 NSX-T Data Center 结构层。

将管理程序主机或裸机服务器添加到 NSX-T Data Center 结构层

结构层节点是已在 NSX-T Data Center 管理层面中注册并安装了 NSX-T Data Center 模块的节点。要使管理程序主机或裸机服务器成为 NSX-T Data Center 覆盖网络的一部分，必须先将其添加到 NSX-T Data Center 结构层中。

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。

注 对于 RHEL 上的 KVM 主机，可以使用 **sudo** 凭据执行主机准备活动。

前提条件

- 对于打算添加到 NSX-T Data Center 结构层的每个主机，请先收集以下主机信息：
  - 主机名
  - 管理 IP 地址
  - 用户名
  - 密码
  - （可选）(KVM) SHA-256 SSL 指纹
  - （可选）(ESXi) SHA-256 SSL 指纹
- 对于 Ubuntu，确认安装了所需的第三方软件包。请参见在 KVM 主机或裸机服务器上安装第三方软件包。

步骤

1 （可选）检索管理程序指纹，以便在将主机添加到结构层时提供该指纹。

a 收集管理程序指纹信息。

使用 Linux shell。

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

使用主机中的 vSphere ESXi CLI。

```
[root@host:~] openssl x509 -in /etc/vmware/ssl/rui.crt -fingerprint -sha256 -noout
SHA256 Fingerprint=49:73:F9:A6:0B:EA:51:2A:15:57:90:DE:C0:89:CA:7F:46:8E:30:15:CA:4D:5C:
95:28:0A:9E:A2:4E:3C:C4:F4
```

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

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

2 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
```

3 从浏览器中，使用管理员权限登录到位于 `https://<nsx-manager-ip-address>` 的 NSX Manager。

4 选择**结构层 > 节点 > 主机**，然后单击**添加**。

5 输入主机名、IP 地址、用户名、密码以及可选的指纹。

例如：

对于裸机服务器，您可以从“操作系统”下拉菜单中选择 **RHEL 服务器**、**Ubuntu 服务器**或 **CentOS 服务器**。

如果未输入主机指纹，NSX-T Data Center UI 将提示您使用从主机中检索到的纯文本格式的默认指纹。

例如：

如果将主机成功添加到 NSX-T Data Center 结构层中，NSX Manager **主机**页面将显示**部署状态: 安装成功**和 **MPA 连接: 已连接**。

在将结构层节点变为传输节点后，**LCP 连接**才会可用。

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

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

在 vSphere ESXi 上，这些模块打包为 VIB。对于 RHEL 上的 KVM 或裸机服务器，这些模块打包为 RPM。对于 Ubuntu 上的 KVM 或裸机服务器，这些模块打包为 DEB。

- 在 ESXi 上，键入 `esxcli software vib list | grep nsx` 命令。

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

7 （可选）使用 `GET https://<nsx-mgr>/api/v1/fabric/nodes/<node-id>` API 调用查看结构层节点。

8 （可选）在 API 中使用 `GET https://<nsx-mgr>/api/v1/fabric/nodes/<node-id>/status` API 调用监控状态。

9 （可选）如果具有 500 个或更多管理程序，则更改某些进程的轮询间隔。

如果具有超过 500 个管理程序，NSX Manager 可能会遇到 CPU 使用率过高和性能问题。

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

b 运行位于 NSX-T Data Center 文件存储中的脚本。

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

c （可选）将轮询间隔改回到默认值。

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

后续步骤

创建传输区域。请参见关于传输区域。

手动安装 NSX-T Data Center 内核模块

作为使用 NSX-T Data Center **结构层 > 节点 > 主机 > 添加** UI 或 `POST /api/v1/fabric/nodes` API 的替代方法，您可以从管理程序命令行中手动安装 NSX-T Data Center 内核模块。

注 无法在裸机服务器上手动安装 NSX-T Data Center 内核模块。

在 ESXi 管理程序上手动安装 NSX-T Data Center 内核模块

要准备主机以加入 NSX-T Data Center 网络，您必须在 ESXi 主机上安装 NSX-T Data Center 内核模块。这样，您就可以构建 NSX-T Data Center 控制层面和管理层面结构层。在 VIB 文件中打包的 NSX-T Data Center 内核模块在管理程序内核中运行并提供一些服务，例如，分布式路由、分布式防火墙和桥接功能。

您可以手动下载 NSX-T Data Center VIB 并将其作为主机映像的一部分。每个 NSX-T Data Center 版本的下载路径可能会有所不同。请务必查看 NSX-T Data Center 下载页面以获取相应的 VIB。

步骤

1 作为 root 或具有管理权限的用户登录到主机。

2 导航到 /tmp 目录。

```
[root@host:~]: cd /tmp
```

3 下载 nsx-lcp 文件并将其复制到 /tmp 目录中。

4 运行 install 命令。

```
[root@host:/tmp]: esxcli software vib install -d /tmp/nsx-lcp-<release>.zip
Installation Result
   Message: Operation finished successfully.
   Reboot Required: false
   VIBs Installed: VMware_bootbank_nsx-aggservice_<release>, VMware_bootbank_nsx-da_<release>,
VMware_bootbank_nsx-esx-datapath_<release>, VMware_bootbank_nsx-exporter_<release>,
VMware_bootbank_nsx-host_<release>, VMware_bootbank_nsx-lldp_<release>, VMware_bootbank_nsx-
mpa_<release>, VMware_bootbank_nsx-netcpa_<release>, VMware_bootbank_nsx-python-protobuf_<release>,
VMware_bootbank_nsx-sfhc_<release>, VMware_bootbank_nsxa_<release>,
VMware_bootbank_nsxcli_<release>
   VIBs Removed:
   VIBs Skipped:
```

根据在主机上已安装的内容，可能会安装、移除或跳过一些 VIB。不需要重新引导，除非命令输出显示 `Reboot Required: true`。

将 ESXi 主机添加到 NSX-T Data Center 结构层中后，会在主机上安装以下 VIB。

- nsx-aggservice - 为 NSX-T Data Center 聚合服务提供主机端库。NSX-T Data Center 聚合服务是在管理层面节点中运行并从 NSX-T Data Center 组件中获取运行时状态的服务。
- nsx-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 Data Center 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 上通告其身份、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通告该状态。
- nsx-python-protobuf - 为协议缓冲区提供 Python 绑定。
- nsx-sfhc - 服务结构层主机组件 (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结构层主机以管理其生命周期。这会为操作提供一个通道，例如，NSX-T Data Center 升级和卸载以及监控管理程序上的 NSX-T Data Center 模块。
- nsxa - 执行主机级别配置，例如，N-VDS 创建和上行链路配置。
- nsxcli - 在管理程序主机上提供 NSX-T Data Center 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 Data Center 管理层面。请参见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 Data Center 内核模块

要准备主机以加入 NSX-T Data Center，您可以手动在 Ubuntu KVM 主机上安装 NSX-T Data Center 内核模块。这样，您就可以构建 NSX-T Data Center 控制层面和管理层面结构层。在 DEB 文件中打包的 NSX-T Data Center 内核模块在管理程序内核中运行并提供一些服务，例如，分布式路由、分布式防火墙和桥接功能。

您可以手动下载 NSX-T Data Center DEB 并将其作为主机映像的一部分。请注意，每个 NSX-T Data Center 版本的下载路径可能会有所不同。请务必查看 NSX-T Data Center 下载页面以获取相应的 DEB。

前提条件

- 确认安装了所需的第三方软件包。请参见在 KVM 主机或裸机服务器上安装第三方软件包。

步骤

1 以具有管理权限的用户身份登录到主机。

2 （可选）导航到 /tmp 目录。

```
cd /tmp
```

3 下载 nsx-lcp 文件并将其复制到 /tmp 目录中。

4 解压缩该软件包。

```
tar -xvf nsx-lcp-<release>-ubuntu-trusty_amd64.tar.gz
```

5 导航到软件包目录。

```
cd nsx-lcp-trusty_amd64/
```

6 安装该软件包。

```
sudo dpkg -i *.deb
```

7 重新加载 OVS 内核模块。

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

如果管理程序在 OVS 接口上使用 DHCP，请重新启动用于配置 DHCP 的网络接口。您可以手动停止网络接口上的旧 dhclient 进程，并在该接口上重新启动新 dhclient 进程。

8 要进行验证，可以运行 `dpkg -l | grep nsx` 命令。

```
user@host:~$ dpkg -l | grep nsx

ii  nsx-agent                            <release>     amd64        NSX Agent
ii  nsx-aggservice                       <release>     all          NSX Aggregation Service Lib
ii  nsx-cli                              <release>     all          NSX CLI
ii  nsx-da                               <release>     amd64        NSX Inventory Discovery Agent
ii  nsx-host                             <release>     all          NSX host meta package
ii  nsx-host-node-status-reporter        <release>     amd64        NSX Host Status Reporter for
Aggregation Service
ii  nsx-lldp                             <release>     amd64        NSX LLDP Daemon
ii  nsx-logical-exporter                 <release>     amd64        NSX Logical Exporter
ii  nsx-mpa                              <release>     amd64        NSX Management Plane Agent Core
ii  nsx-netcpa                           <release>     amd64        NSX Netcpa
ii  nsx-sfhc                            <release>     amd64       NSX Service Fabric Host Component
ii  nsx-transport-node-status-reporter  <release>     amd64       NSX Transport Node Status Reporter
ii  nsxa                                 <release>     amd64        NSX L2 Agent
```

任何错误很可能是由不完整的依赖项造成的。`apt-get install -f` 命令可以尝试解决依赖项问题并重新运行 NSX-T Data Center 安装。

后续步骤

将主机添加到 NSX-T Data Center 管理层面。请参见将管理程序主机加入管理层面。

在 RHEL 和 CentOS KVM 管理程序上手动安装 NSX-T Data Center 内核模块

要准备主机以加入 NSX-T Data Center，您可以手动在 RHEL 或 CentOS KVM 主机上安装 NSX-T Data Center 内核模块。

这样，您就可以构建 NSX-T Data Center 控制层面和管理层面结构层。在 RPM 文件中打包的 NSX-T Data Center 内核模块在管理程序内核中运行并提供一些服务，例如，分布式路由、分布式防火墙和桥接功能。

您可以手动下载 NSX-T Data Center RPM 并将其作为主机映像的一部分。请注意，每个 NSX-T Data Center 版本的下载路径可能会有所不同。请务必查看 NSX-T Data Center 下载页面以获取相应的 RPM。

前提条件

能够访问 RHEL 或 CentOS 存储库。

步骤

1 以管理员身份登录到主机。

2 下载 nsx-lcp 文件并将其复制到 /tmp 目录中。

3 解压缩该软件包。

```
tar -zxvf nsx-lcp-<release>-rhel7.4_x86_64.tar.gz
```

4 导航到软件包目录。

```
cd nsx-lcp-rhel74_x86_64/
```

5 安装该软件包。

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

运行 yum install 命令时，会解析任何 NSX-T Data Center 依赖项，假定 RHEL 或 CentOS 主机可以访问其各自的存储库。

6 重新加载 OVS 内核模块。

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

如果管理程序在 OVS 接口上使用 DHCP，请重新启动用于配置 DHCP 的网络接口。您可以手动停止网络接口上的旧 dhclient 进程，并在该接口上重新启动新 dhclient 进程。

7 要进行验证，可以运行 `rpm -qa | egrep 'nsx|openvswitch|nicira'` 命令。

在输出中，安装的软件包必须与 nsx-rhel74 或 nsx-centos74 目录中的软件包相匹配。

后续步骤

将主机添加到 NSX-T Data Center 管理层面。请参见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 Data Center 模块安装。

步骤

1 打开到 NSX Manager 设备的 SSH 会话。

2 使用 Administrator 凭据登录。

3 打开到管理程序主机的 SSH 会话。

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

命令输出是该 NSX Manager 特有的数字串。

例如：

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

5 在管理程序主机上，运行 **nsxcli** 命令以进入 NSX-T Data Center 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。

6 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**结构层 > 节点 > 主机**中，验证主机的 MPA 连接是否为**已连接**。

还可以使用 **GET https://<nsx-mgr>/api/v1/fabric/nodes/<fabric-node-id>/state** API 调用查看结构层主机的状态：

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

管理层面将主机证书发送到控制层面，并且控制层面将控制层面信息推送到主机。

您应该会在每个 ESXi 主机上的 `/etc/vmware/nsx/controller-info.xml` 中看到 NSX Controller 地址，或使用 `get controllers` 访问 CLI。

```
[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>
```

将启动到 NSX-T Data Center 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。请参见关于传输区域。

传输区域和传输节点

8

传输区域和传输节点是 NSX-T Data Center 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 Data Center 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 Data Center 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。

创建传输区域时，您必须指定 N-VDS 模式，可以将该模式设置为**标准**或**增强型数据路径**。将传输节点添加到传输区域时，将在该传输节点上安装与该传输区域关联的 N-VDS。每个传输区域支持单个 N-VDS。增强型数据路径 N-VDS 具有支持 NFV（网络功能虚拟化）工作负载的性能，支持 VLAN 网络和覆盖网络，并且需要支持增强型数据路径 N-VDS 的 ESXi 主机。

一个传输节点可以属于：

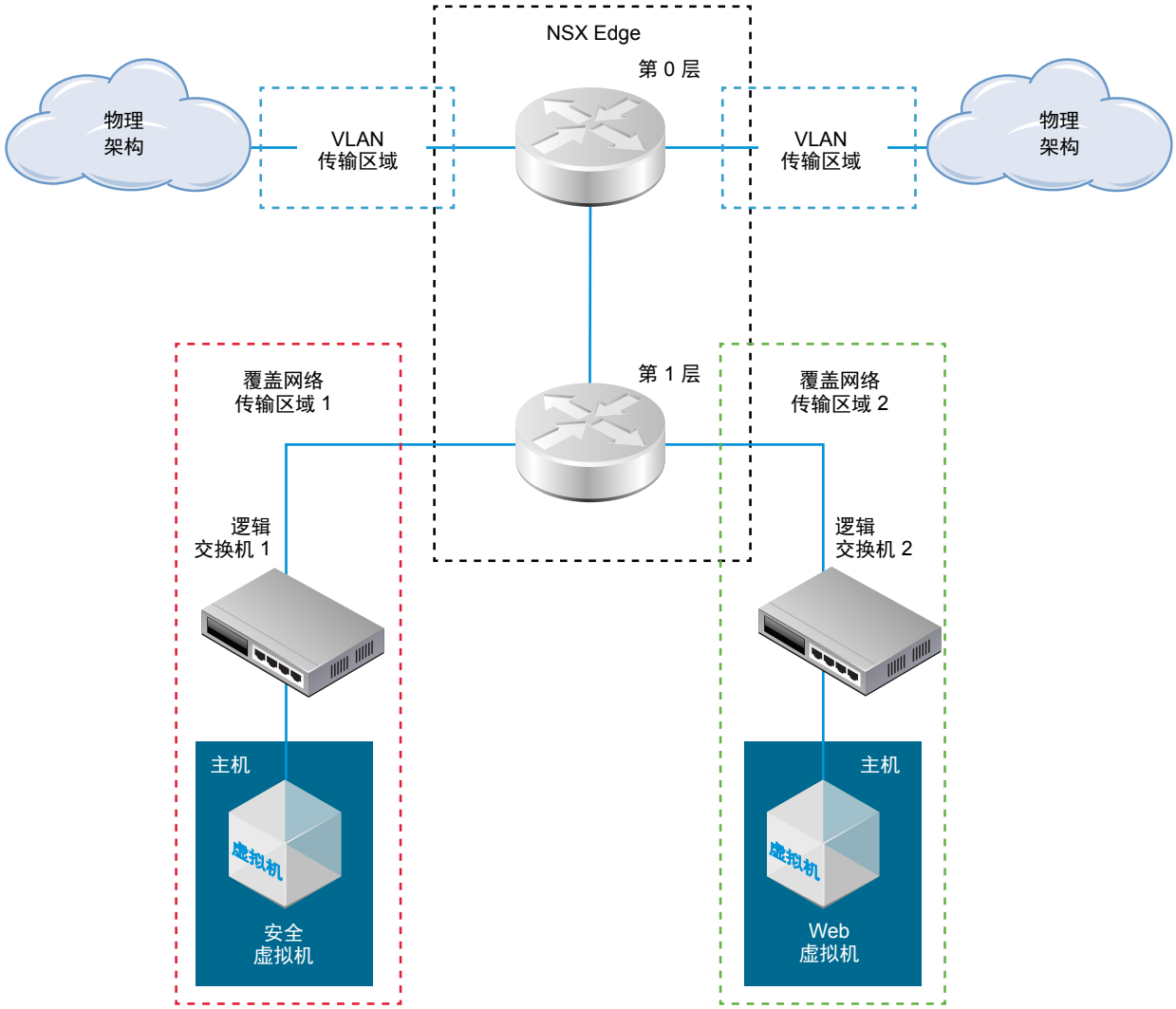
- 多个 VLAN 传输区域。
- 最多一个具有标准 N-VDS 的覆盖网络传输区域。
- 具有高级数据路径 N-VDS 的多个覆盖网络传输区域（如果传输节点正在 ESXi 主机上运行）。

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连接到也位于该传输区域中的 NSX-T Data Center 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 层底层可访问性要求，而是对可访问性施加一个限制。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 层和第 3 层（对于不同的子网）底层网络必须正常运行。

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。常规虚拟机和安全虚拟机不能位于同一传输节点上。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 Data Center 逻辑交换机。高安全性虚拟机连接到位于 secure-tz 中的 NSX-T Data Center 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。

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 Data Center 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 Data Center 传输区域



增强型数据路径

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

只能在 ESXi 主机上以增强型数据路径模式配置 N-VDS 交换机。

在增强型数据路径模式下，可以配置：

- 覆盖网络流量
- VLAN 流量

配置增强型数据路径的高级过程

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

概要步骤如下所示：

1 使用支持增强型数据路径的网卡。

请参见《VMware 兼容性指南》，了解支持增强型数据路径的网卡。

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

2 从 My VMware 页面下载并安装网卡驱动程序。

3 创建上行链路策略。

请参见创建上行链路配置文件。

4 使用增强型数据路径模式下的 N-VDS 创建传输区域。

请参见创建传输区域。

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

请参见创建主机传输节点。

负载平衡源绑定策略模式感知 NUMA

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

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

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

在以下情况下，绑定策略运行时不感知 NUMA：

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

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 Data Center 覆盖网络帧封装的管理程序主机。还可以使用 DHCP 或手动配置的 IP 池以分配隧道端点 IP 地址。

如果同时使用 ESXi 和 KVM 主机，一种设计方法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。

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

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

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

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

步骤

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

2 选择**清单 > 组 > IP 池**，然后单击**添加**。

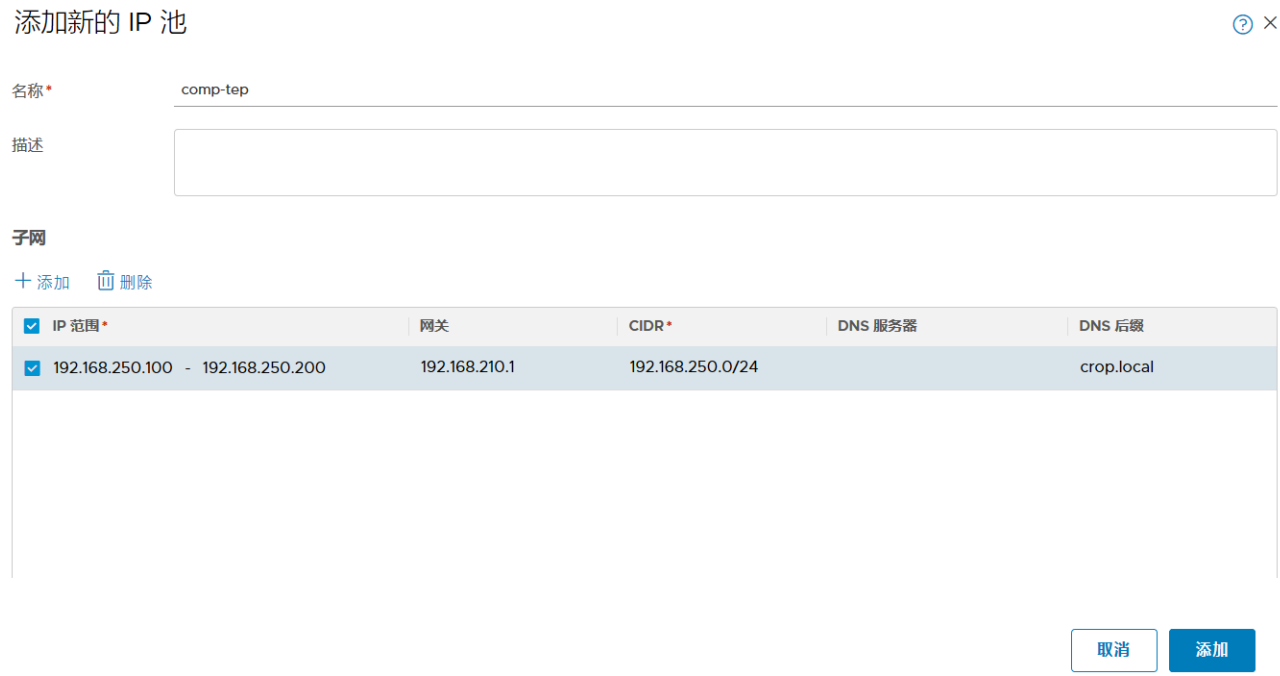
3 输入 IP 池名称、可选说明和网络设置。

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

- （可选）DNS 后缀

例如：



还可以使用 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。请参见创建上行链路配置文件。

创建上行链路配置文件

上行链路配置文件为管理程序主机到 NSX-T Data Center 逻辑交换机或 NSX Edge 节点到架顶式交换机的链路定义策略。

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 Data Center 传输节点时应用这些功能。

基于虚拟机/设备的 NSX Edge 不支持备用上行链路。将 NSX Edge 安装为虚拟设备时，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　如果为每个上行链路创建单独的 N-VDS，并且为每个 N-VDS 使用不同的 VLAN，则 NSX Edge 虚拟机允许使用多个上行链路。每个上行链路都需要单独的 VLAN 传输区域。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

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

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

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

步骤

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

2 选择**结构层 > 配置文件 > 上行链路配置文件**，然后单击**添加**。

3 填写上行链路配置文件详细信息。

选项	说明
名称	输入上行链路配置文件名称。
说明	添加可选的上行链路配置文件描述。
LAG	（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)。 **注** 对于 LACP，KVM 主机不支持多个 LAG。 添加逗号分隔的活动上行链路名称列表。 添加逗号分隔的备用上行链路名称列表。您创建的活动和备用上行链路名称可以是表示物理链路的任意文本。以后创建传输节点时，将引用这些上行链路名称。通过使用传输节点 UI/API，您可以指定与每个命名的上行链路对应的物理链路。 可能的 LAG 哈希机制选项如下所示： ■ 源 MAC 地址 ■ 目标 MAC 地址 ■ 源和目标 MAC 地址 ■ 源和目标 IP 地址及 VLAN ■ 源和目标 MAC 地址、IP 地址和 TCP/UDP 端口
绑定	在“绑定”部分中，单击**添加**，然后输入详细信息。绑定策略定义 N-VDS 如何使用其上行链路实现冗余和流量负载平衡。可通过两种绑定策略模式来配置绑定策略： ■ **故障切换顺序**：指定活动上行链路以及可选的备用上行链路列表。如果活动上行链路出现故障，备用列表中的下一个上行链路将替换该活动上行链路。该选项不会执行实际负载平衡。 ■ **负载平衡源**：指定活动上行链路列表，且传输节点上的每个接口固定到一个活动上行链路。此配置允许同时使用多个活动上行链路。 **注** 在 KVM 主机上，仅支持故障切换顺序绑定策略。不支持负载平衡源绑定策略。 （仅限 ESXi 主机）可以为传输区域定义以下策略： ■ 在交换机上配置的每个逻辑交换机的指定绑定策略。 ■ 整个交换机的默认绑定策略。 指定绑定策略：指定绑定策略意味着，可以为每个逻辑交换机定义特定的绑定策略模式和上行链路。此策略类型使您可以根据带宽要求灵活地选择上行链路。 ■ 如果定义指定绑定策略，则在连接的传输区域及主机中的逻辑交换机指定时，N-VDS 将使用该指定绑定策略。 ■ 如果未定义任何指定绑定策略，N-VDS 将使用默认绑定策略。

4 输入传输 VLAN 值。

5 输入 MTU 值。

默认值为 1600。

除了 UI 以外，还可以使用 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" : [ {
            "uplink_name" : "uplink-2",
            "uplink_type" : "PNIC"
         } ],
        "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"
      },
      "named_teamings": [
         {
          "active_list": [
         {
          "uplink_type": "PNIC",
          "uplink_name": "uplink-2"
          }
                        ],
           "standby_list": [
```

```
          {
                 "uplink_type": "PNIC",
           "uplink_name": "uplink-1"
           }
            ],
         "policy": "FAILOVER_ORDER",
          "name": "named teaming policy"
              }
             ]
                         "mtu": 1600,
       "_last_modified_time": 1457984399574,
       "_create_time": 1457984399574,
       "_last_modified_user": "admin",
       "_system_owned": false,
       "_create_user": "admin",
       "_revision": 0
     }
   ]
 }
```

后续步骤

创建传输区域。请参见创建传输区域。

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 Data Center 环境可能包含一个或多个传输区域。一个主机可以属于多个传输区域。一个逻辑交换机只能属于一个传输区域。

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

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

NSX Edge 将 VLAN 传输区域用于其 VLAN 上行链路。在将 NSX Edge 添加到 VLAN 传输区域时，将在 NSX Edge 上安装 VLAN N-VDS。

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

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

步骤

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

2 选择**结构层 > 传输区域 > 添加**。

3 输入传输区域的名称和描述（可选）。

4 输入 N-VDS 的名称。

5 选择 N-VDS 模式。

选项有**标准**和**增强型数据路径**。

6 如果 N-VDS 模式为“标准”，则选择一个流量类型。

选项有**覆盖网络**和 **VLAN**。

7 如果 N-VDS 模式为“增强型数据路径”，则选择一个流量类型。

选项有**覆盖网络**和 **VLAN**。

注 在增强型数据路径模式下，仅支持特定的网卡配置。请确保配置支持的网卡。

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

9 在**传输区域**页面上查看新传输区域。

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


```
{
  "cursor": "00369b661aed-1eaa-4567-9408-ccbcfe50b416tz-vlan",
  "result_count": 2,
  "results": [
    {
      "resource_type": "TransportZone",
      "description": "comp overlay transport zone",
      "id": "efd7f38f-c5da-437d-af03-ac598f82a9ec",
      "display_name": "tz-overlay",
      "host_switch_name": "overlay-hostswitch",
      "transport_type": "OVERLAY",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ],
      "_create_time": 1459547126454,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_last_modified_time": 1459547126454,
      "_create_user": "admin",
      "_revision": 0,
      "_schema": "/v1/schema/TransportZone"
    },
    {
      "resource_type": "TransportZone",
      "description": "comp vlan transport zone",
      "id": "9b661aed-1eaa-4567-9408-ccbcfe50b416",
      "display_name": "tz-vlan",
      "host_switch_name": "vlan-uplink-hostwitch",
      "transport_type": "VLAN",
```

```
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ],
      "_create_time": 1459547126505,
      "_last_modified_user": "admin",
      "_system_owned": false,
      "_last_modified_time": 1459547126505,
      "_create_user": "admin",
      "_revision": 0,
      "_schema": "/v1/schema/TransportZone"
    }
  ]
}
```


后续步骤

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

创建传输节点。请参见创建主机传输节点。

创建主机传输节点

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

对于 KVM 主机，您可以预配置 N-VDS，也可以让 NSX Manager 执行配置。对于 ESXi 主机，NSX Manager 始终配置 N-VDS。

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

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

单个物理网卡同时为管理接口和应用程序 IP 接口提供 IP 地址。

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

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

前提条件

- 主机必须加入管理层面，并且**结构层 > 主机**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，使用管理员权限登录到位于 `https://<nsx-manager-ip-address>` 的 NSX Manager。

2 选择**结构层 > 节点 > 传输节点 > 添加**。

3 输入传输节点的名称。

4 从下拉菜单中选择一个节点。

5 选择该传输节点所属的传输区域。

6 单击 **N-VDS** 选项卡。

7 对于 KVM 节点，选择 N-VDS 类型。

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

对于非 KVM 节点，N-VDS 类型始终为**标准**或**增强型数据路径**。

8 对于标准 N-VDS，请提供以下详细信息。

选项	说明
N-VDS 名称	必须与该节点所属传输区域的 N-VDS 名称相同。
NIOC 配置文件	从下拉菜单中选择 NIOC 配置文件。
上行链路配置文件	从下拉菜单中选择上行链路配置文件。
IP 分配	选择**使用 DHCP**、**使用 IP 池**或**使用静态 IP 列表**。 如果选择**使用静态 IP 列表**，您必须指定以逗号分隔的 IP 地址、网关和子网掩码列表。
IP 池	如果您选择**使用 IP 池**进行 IP 分配，请指定 IP 池名称。
物理网卡	确保尚未使用物理网卡（例如，标准 vSwitch 或 vSphere Distributed Switch 未使用）。否则，传输节点状态保持为**部分成功**，并且无法建立结构层节点 LCP 连接。 对于裸机服务器，请选择可配置为 uplink-1 端口的物理网卡。uplink-1 端口是在上行链路配置文件中定义的。 如果在裸机服务器中仅具有一个网络适配器，请选择该物理网卡，以便将 uplink-1 端口分配给管理和应用程序接口。

9 对于增强型数据路径 N-VDS，请提供以下详细信息。

选项	说明
N-VDS 名称	必须与该节点所属传输区域的 N-VDS 名称相同。
IP 分配	选择**使用 DHCP**、**使用 IP 池**或**使用静态 IP 列表**。 如果选择**使用静态 IP 列表**，您必须指定以逗号分隔的 IP 地址、网关和子网掩码列表。

选项	说明
IP 池	如果您选择**使用 IP 池**进行 IP 分配，请指定 IP 池名称。
物理网卡	选择支持增强型数据路径的物理网卡。确保尚未使用物理网卡（例如，标准 vSwitch 或 vSphere Distributed Switch 未使用）。否则，传输节点状态保持为**部分成功**，并且无法建立结构层节点 LCP 连接。
上行链路	从下拉菜单中选择上行链路配置文件。
CPU 配置	在“NUMA 节点索引”下拉菜单中，选择要分配给 N-VDS 交换机的 NUMA 节点。节点上存在的第一个 NUMA 节点用值 0 表示。 可以通过运行 `esxcli hardware memory get` 命令了解主机上的 NUMA 节点数。 **注** 如果要更改与 N-VDS 交换机具有关联性的 NUMA 节点数，可以更新“NUMA 节点索引”值。
	在“每个 NUMA 节点逻辑内核数”下拉菜单中，选择增强型数据路径必须使用的逻辑内核数。 可以通过运行 `esxcli network ens maxLcores get` 命令了解可在 NUMA 节点上创建的最大逻辑内核数。 **注** 如果用尽可用 NUMA 节点和逻辑内核，则无法针对 ENS 流量启用添加到传输节点的任何新交换机。

10 对于预配置的 N-VDS，请提供以下详细信息。

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

在将主机添加为传输节点后，主机与 NSX Controller 的连接将变为“已连接”状态。

11 在**传输节点**页面上查看连接状态。

12 或者，使用 CLI 命令查看连接状态。

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

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

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

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

13 （可选）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
}
```


14 将新创建的传输节点添加到传输区域中。

a 选择该传输节点。

b 选择**操作 > 添加到传输区域**。

c 从下拉菜单中选择该传输区域。

将填充所有其他字段。

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

后续步骤

将网络接口从 vSphere 标准交换机迁移到 NSX-T 虚拟分布式交换机。请参见 VMkernel 迁移到 N-VDS 交换机。

配置自动创建传输节点功能

如果具有一个 vCenter Server 群集，您可以在一个或多个群集中的所有 NSX-T Data Center 主机上自动完成安装和创建传输节点的过程，而不是手动配置这些节点。

注 仅在 vCenter Server 6.5 Update 1、6.5 Update 2 和 6.7 上支持自动创建 NSX-T Data Center 传输节点。

如果已配置传输节点，则自动创建传输节点功能不适用于该节点。

前提条件

- 主机必须是 vCenter Server 群集的一部分。
- 必须配置一个传输区域。
- 必须配置一个上行链路配置文件，也可以使用默认上行链路配置文件。
- 必须配置一个 IP 池，或者必须在网络部署中具有 DHCP。
- 必须在主机节点上具有至少一个未使用的物理网卡。
- vCenter Server 应具有至少一个群集。
- 必须配置一个计算管理器。

步骤

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

2 选择**结构层 > 节点 > 主机**。

3 从“托管主体”下拉菜单中，选择一个现有的计算管理器。

4 选择一个群集，然后单击**配置群集**。

5 填写群集配置详细信息。

选项	说明
自动安装 NSX	切换该按钮以允许在 vCenter Server 群集中的所有主机上安装 NSX-T Data Center。
自动创建传输节点	切换该按钮以允许在 vCenter Server 群集中的所有主机上创建传输节点。这是必要设置。 注 如果在群集中存在预先配置的传输节点或将其移至另一个群集，则 NSX-T Data Center 不会使用群集传输节点模板中定义的配置更新预先配置的传输节点。要确保所有节点都具有相同配置，请删除预先配置的传输节点并将该主机添加到群集。

选项	说明
传输区域	从下拉菜单中选择一个现有的传输节点。
上行链路配置文件	从下拉菜单中选择一个现有的上行链路配置文件，或者创建一个自定义上行链路配置文件。 **注** 群集中的主机必须具有相同的上行链路配置文件。 也可以使用默认上行链路配置文件。
IP 分配	从下拉菜单中选择**使用 DHCP** 或**使用 IP 池**。 如果选择**使用 IP 池**，您必须从下拉菜单中分配网络中的现有 IP 池。
物理网卡	确保尚未使用物理网卡，例如，标准 vSwitch 或 vSphere Distributed Switch 未使用该网卡。否则，传输节点状态为部分成功，并且无法建立结构层节点 LCP 连接。 您可以使用默认上行链路，或者从下拉菜单中分配一个现有的上行链路。 可以单击**添加 PNIC** 以增加配置中的网卡数。

在群集中的每个主机上安装 NSX-T Data Center 和创建传输节点是并行启动的。整个过程取决于群集中的主机数。

在将新主机添加到 vCenter Server 群集时，将自动完成安装 NSX-T Data Center 和创建传输节点的过程。

6 （可选）查看 ESXi 连接状态。

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

7 （可选）从群集上的主机中移除 NSX-T Data Center 安装和传输节点。

a 选择一个群集，然后单击**配置群集**。

b 切换“自动安装 NSX”按钮以禁用该选项。

c 选择一个或多个主机，然后单击**卸载 NSX**。

卸载最多需要 3 分钟的时间。

使用链路聚合配置 ESXi 主机传输节点

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

前提条件

- 熟悉创建上行链路配置文件的步骤。请参见创建上行链路配置文件。
- 熟悉创建主机传输节点的步骤。请参见创建主机传输节点。

步骤

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

2 选择**结构层 > 配置文件 > 上行链路配置文件**，然后单击**添加**。

3 输入名称和可选的说明。

例如，输入名称 **`uplink-profile1`**。

4 在 **LAG** 下，单击**添加**以添加链路聚合组。

例如，添加具有 2 个上行链路、名为 **lag1** 的 LAG。

5 在**绑定**下面，选择**默认绑定**条目。

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

7 单击对话框底部的**添加**。

8 输入**传输 VLAN** 和 **MTU** 的值。

9 单击窗口底部的**添加**。

10 选择**结构层 > 节点 > 传输节点 > 添加**。

11 在**常规**选项卡中输入信息。

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

13 在**物理网卡**字段中，将看到物理网卡的下拉列表以及创建上行链路配置文件时指定的上行链路的下拉列表。具体来说，将看到上行链路 **lag1-0** 和 **lag1-0**，与在步骤 4 中创建的 LAG **lag1** 相对应。选择 **lag1-0** 的物理网卡和 **lag1-1** 的物理网卡。

14 输入其他字段的信息。

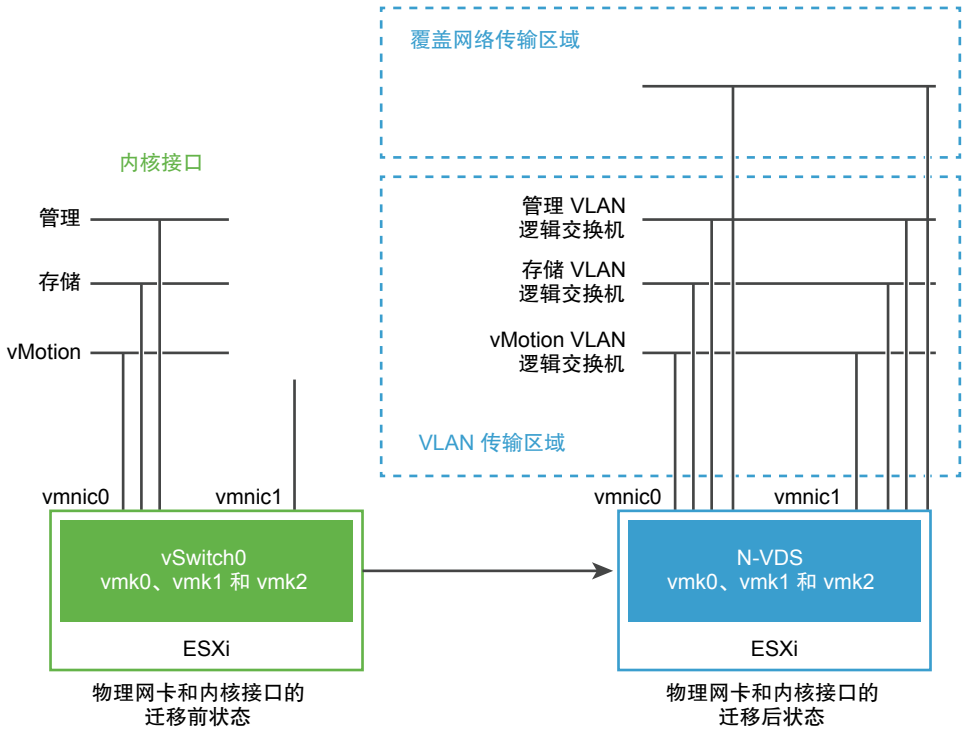
VMkernel 迁移到 N-VDS 交换机

在创建传输节点时，可能需要将物理网卡和内核接口从 vSphere 标准交换机 (VSS) 或 VDS 迁移到 NSX-T Data Center 虚拟分布式交换机 (N-VDS)。迁移后，N-VDS 处理 VLAN 网络上的流量。

物理网卡及其 VMkernel 接口最初连接到 vSphere ESXi 主机上的 VSS 或 VDS。在这些主机上定义了这些内核接口，用于提供与管理接口、存储接口和其他接口的连接。迁移后，VMkernel 接口及其关联的物理网卡连接到 N-VDS 并处理 VLAN 和覆盖网络传输区域上的流量。

在下图中，如果主机只有两个物理网卡，您可能希望将这两个网卡都分配到 N-VDS 以实现冗余。

图 8-2. 将网络接口迁移到 N-VDS 之前和之后



迁移前，vSphere ESXi 主机具有来自两个物理端口 vmnic0 和 vmnic1 的两个上行链路。此处，vmnic0 配置为活动状态并连接到 VSS 或 VDS，而不使用 vmnic1。此外，还有三个 VMkernel 接口：vmk0、vmk1 和 vmk2。

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

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

使用 NSX-T Data Center Manager UI 将 VMkernel 接口迁移到 N-VDS 交换机

通过使用 NSX-T Data Center Manager UI，您可以将所有内核接口（包括管理接口）从 VSS 或 VDS 迁移到 N-VDS 交换机。

在此示例中，请考虑具有两个物理适配器 vmnic0 和 vmnic1 的 vSphere ESXi 主机。主机上的默认 VSS 或 VDS 交换机配置了单个映射到 vmnic0 的上行链路。在 VSS 或 VDS 上还配置了 VMkernel 接口 vmk0 以在节点上运行管理流量。目的是将 vmnic0 和 vmk0 迁移到 N-VDS 交换机。

作为主机准备的一部分，创建了 VLAN 和覆盖网络传输区域以分别运行管理流量和虚拟机流量。还创建了 N-VDS 交换机，它配置有映射到 vmnic1 的上行链路。在迁移后，NSX-T Data Center 将 vmnic0 和 vmk0 从 VSS 或 VDS 交换机迁移到节点上的 N-VDS 交换机。

前提条件

- 确认物理网络基础架构向 vmnic1 和 vmnic0 提供相同的 LAN 连接。
- 确认未使用的物理网卡 vmnic1 具有与 vmnic0 的第 2 层连接。

- 确保此迁移中涉及的所有 VMkernel 接口都属于同一个网络。如果将 VMkernel 接口迁移到连接到不同网络的上行链路，则主机可能会无法访问或无法正常工作。

步骤

1 在 NSX Manager UI 上，转到**结构层 -> 配置文件 -> 上行链路配置文件**。

2 将 vmnic0 用作主动上行链路并将 vmnic1 用作被动上行链路来创建上行链路配置文件。

3 转到**结构层 -> 传输区域 -> 添加**。

4 创建覆盖网络和 VLAN 传输区域以分别处理虚拟机流量和管理流量。

> 注 VLAN 传输区域和覆盖网络传输区域中使用的 N-VDS 名称必须是相同的。

5 转到**结构层 -> 节点 -> 传输节点**。

6 将这两个传输区域添加到传输节点。

7 在 N-VDS 选项卡中，通过定义上行链路、要由 N-VDS 使用的物理适配器来添加 N-VDS。

传输节点将通过单个上行链路连接到传输区域。

8 要确保在迁移后 vmk0 和 vmnic0 连接到 VLAN 传输区域，请为相应的 VLAN 传输区域创建逻辑交换机。

9 选择传输节点，单击**操作 -> 迁移 ESX VMkernel 和物理适配器**。

10 选择**迁移到逻辑交换机**。

11 选择 N-VDS 交换机。

12 添加 VMkernel 适配器和关联的逻辑交换机。

13 添加与 VMkernel 接口相对应的物理适配器。确保在 VSS 或 VDS 交换机上保留至少一个物理适配器。

14 单击**保存**。

15 单击**继续**以开始迁移。

16 从 NSX Manager 测试到 vmnic0 和 vmk0 的连接。

17 或者，在 vCenter Server 中，确认 VMkernel 适配器与 NSX-T Data Center 交换机关联。

VMkernel 接口及其对应的物理适配器将迁移到 N-VDS。

后续步骤

您可以将 VMkernel 迁移回 VSS 或 VDS 交换机。

使用 NSX-T Data Center Manager UI 将 VMkernel 接口迁移回 VSS 或 VDS 交换机

要将 VMkernel 接口迁移回 VSS 或 VDS 交换机，请确保在 ESXi 主机上具有一个端口组。

NSX-T Data Center 需要使用端口组将 VMkernel 接口从 N-VDS 交换机迁移到 VSS 或 VDS 交换机。端口组接受将这些接口迁移到 VSS 或 VDS 交换机的网络请求。参与此迁移的端口成员根据其带宽和策略配置进行确定。

在开始将 VMkernel 迁移回 VSS 或 VDS 交换机之前，请确保 VMkernel 接口正常工作并且 N-VDS 交换机上的连接正常。

前提条件

- vSphere ESXi 服务器上存在端口组。

步骤

1. 在 NSX Manager UI 中，转到**结构层 -> 节点 -> 传输节点**。
2. 选择传输节点，单击**操作 -> 迁移 ESX VMkernel 和物理适配器**。
3. 选择**迁移到端口组**。
4. 选择 N-VDS 交换机。
5. 添加 VMkernel 适配器和关联的逻辑交换机。
6. 添加与 VMkernel 接口相对应的物理适配器。请确保至少一个物理适配器始终连接到 VSS 或 VDS 交换机。
7. 单击**保存**。
8. 单击**继续**以开始迁移。
9. 从 NSX Manager 测试到 vmnic0 和 vmk0 的连接。
10. 或者，在 vCenter Server 中，确认 VMkernel 适配器与 VSS 或 VDS 交换机相关联。

VMkernel 接口及其对应的物理适配器将迁移到 N-VDS。

后续步骤

您可能希望使用 API 迁移 VMkernel 接口。请参见使用 API 将内核接口迁移到 N-VDS。

使用 API 将内核接口迁移到 N-VDS

使用 NSX-T Data Center API 时，请确保先迁移所有内核接口再迁移管理接口。

请考虑两个上行链路连接到各自物理网卡的主机。在此过程中，可以从将存储内核接口 vmk1 迁移到 N-VDS 开始。此内核接口成功迁移到 N-VDS 后，可以迁移管理内核接口。

请参见《NSX-T Data Center API 指南》。

前提条件

- 确认物理网络基础架构向 vmnic1 和 vmnic0 提供相同的 LAN 连接。
- 确认未使用的物理网卡 vmnic1 具有与 vmnic0 的第 2 层连接。
- 确保此迁移中涉及的所有 VMkernel 接口都属于同一个网络。如果将 VMkernel 接口迁移到连接到不同网络的上行链路，则主机可能会无法访问或无法正常工作。

步骤

1. 使用覆盖网络传输区域使用的 N-VDS 的 host_switch_name 创建 VLAN 传输区域。

2 在 VLAN ID 与 VSS 或 VDS 上的 vmk1 使用的 VLAN ID 匹配的 VLAN 传输区域中创建一个支持 VLAN 的逻辑交换机。

3 将 vSphere ESXi 传输节点添加到 VLAN 传输区域。

4 检索 vSphere ESXi 传输节点配置。

```
GET /api/v1/transport-nodes/<transportnode-id>
```

其中，*<transportnode-id>* 是传输节点的 UUID。

5 将 vmk1 迁移到 N-VDS。

```
PUT https://<NSXmgr>/api/v1/transport-nodes/<transportnode-id> ?
if_id=<vmk>&esx_mgmt_if_migration_dest=<network>
```

其中，*<transportnode-id>* 是传输节点的 UUID。*<vmk>* 是 VMkernel 接口 vmk1 的名称。*<network>* 是目标逻辑交换机的 UUID。

6 确认迁移已成功完成。

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

等待迁移状态显示为成功。还可以在 vCenter Server 中验证 VMkernel 接口的迁移状态。

VMkernel 接口已从 VSS 或 VDS 迁移到 N-VDS 交换机。

后续步骤

您可以将 VSS 或 VDS 的其余 VMkernel 接口和管理内核接口迁移到 N-VDS。

使用 API 将管理内核接口从 VSS 或 VDS 迁移到 N-VDS

迁移所有其他内核接口后，继续迁移管理内核接口。在迁移管理内核接口时，您将 vmnic0 和 vmk0 从 VSS 或 VDS 移动到 N-VDS。

然后，可以在一个操作中将物理上行链路 vmnic0 和 vmk0 一起迁移到 N-VDS。修改传输节点配置，以便将 vmnic0 配置为其上行链路之一。

注 要单独迁移上行链路 vmnic0 和内核接口 vmk0，请首先迁移 vmk0，然后再迁移 vmnic0。如果先迁移 vmnic0，则 vmk0 保留在 VSS 或 VDS 上而没有任何备用上行链路，并且您与主机断开连接。

前提条件

- 确认与已迁移 vmknic 的连接。请参见使用 API 将内核接口迁移到 N-VDS。
- 如果 vmk0 和 vmk1 使用不同的 VLAN，则必须在连接到 PNIC vmnic0 和 vmnic1 的物理交换机上配置中继 VLAN，以支持这两个 VLAN。
- 确认外部设备可以访问支持 VLAN 的存储逻辑交换机上的接口 vmk1 以及支持 VLAN 的 vMotion 逻辑交换机上的 vmk2。

步骤

1 （可选）在 VSS 或 VDS 上创建第二个管理内核接口，并将该新创建的接口迁移到 N-VDS。

2 （可选）从外部设备确认与测试管理接口的连接。

3 如果 vmk0（管理接口）使用与 vmk1（存储接口）不同的 VLAN，请在 VLAN ID 与 VSS 或 VDS 上的 vmk0 使用的 VLAN ID 匹配的 VLAN 传输区域中创建一个支持 VLAN 的逻辑交换机。

4 检索 vSphere ESXi 传输节点配置。

```
GET /api/v1/transport-nodes/<transportnode-id>
```

其中，*<transportnode-id>* 是传输节点的 UUID。

5 在配置的 `host_switch_spec:host_switches` 元素中，将 vmnic0 添加到 pnic 表并将其分配给专用上行链路 uplink-2。

注 在迁移虚拟机内核接口时，我们已将 vmnic1 分配给 uplink-1。需要将管理接口 vmnic0 分配给专用上行链路，迁移才能成功，并且在迁移之后才能访问主机。

```
"pnics": [      {
                    "device_name": "vmnic0",
                    "uplink_name": "uplink-2"
                },
                {
                    "device_name": "vmnic1",
                    "uplink_name": "uplink-1"
                }
        ],
```

6 使用更新的配置将管理内核接口 vmk0 迁移到 N-VDS。

```
PUT api/v1/transport-nodes/< transportnode-
id>if_id=<vmk>&esx_mgmt_if_migration_dest=<network>
```

其中，*<transportnode-id>* 是传输节点的 UUID。*<vmk>* 是 VMkernel 管理接口 vmk0 的名称。<network> 是目标逻辑交换机的 UUID。

7 确认迁移已成功完成。

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

等待迁移状态显示为成功。在 vCenter Server 中，您可以验证内核适配器是否已配置为显示新的逻辑交换机名称。

后续步骤

您可以选择将内核接口和管理接口从 N-VDS 迁移回 VSS 或 VDS 交换机。

使用 API 将 VMkernel 接口从 N-VDS 交换机迁移回 VSS 或 VDS 交换机

在迁移 VMkernel 接口时，必须先迁移管理内核接口。然后，将其他内核接口从 N-VDS 迁移到 VSS 或 VDS 交换机。

步骤

1 确认传输节点状态为成功。

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

2 检索 vSphere ESXi 传输节点配置，以查找 "host_switch_spec":"host_switches" 元素内定义的物理网卡

```
GET /api/v1/transport-nodes/<transportnode-id>
```

```
"pnics": [
     { "device_name": "vmnic0",
       "uplink_name": "uplink-2"
        },
       { "device_name": "vmnic1",
           "uplink_name": "uplink-1"
        }
               ],
```

3 从传输节点配置的 "host_switch_spec":"host_switches" 元素中移除 vmnic0，以准备用于迁移的管理接口。

```
"pnics": [
        { "device_name": "vmnic1",
           "uplink_name": "uplink-1"
        }
               ],
```

4 使用修改的配置将管理接口 vmnic0 和 vmk0 从 N-VDS 迁移到 VSS 或 VDS。

```
PUT api/v1/transport-nodes/< transportnode-id>?
if_id=vmk0&esx_mgmt_if_migration_dest=<vmk0_port_group_name>
```

其中，*<vmk0_port_group>* 是迁移到逻辑交换机之前分配给 vmk0 的端口组名称。

5 验证迁移状态。

```
GET /api/v1/transport-nodes/<transportnode-id>/state
```

等待状态显示为“成功”。

6 检索 vSphere ESXi 传输节点配置。

```
GET /api/v1/transport-nodes/<transportnode-id>
```

7 使用上述传输节点配置将 vmk1 从 N-VDS 迁移到 VSS 或 VDS。

```
PUT api/v1/transport-nodes/< transportnode-id>?
if_id=vmk1&esx_mgmt_if_migration_dest=<vmk1_port_group>
```

其中，*<vmk1_port_group>* 是迁移到逻辑交换机之前分配给 vmk1 的端口组名称。

注 必须将 vmk0 或 vmk1 迁移到具有至少一个物理网卡的 VSS 或 VDS，因为 VSS 或 VDS 没有任何关联的物理网卡。

8 确认传输节点状态为成功。

```
GET /api/v1/transport-nodes/<transportnode-id>/state.
```

9 执行迁移后验证，以避免出现任何问题。

a 在将上行链路接口连接到 VSS 或 VDS 之前，不能迁移管理内核接口 vmk0。

b 确保 vmk0 从 vmnic0 接收其 IP 地址，否则 IP 可能会更改，并且 VC 等其他组件可能会断开通过旧 IP 与主机建立的连接。

验证传输节点状态

确保传输节点创建过程正常工作。

在创建主机传输节点后，将在主机上安装 N-VDS。

步骤

1 登录到 NSX-T Data Center。

2 转至“传输节点”页面并查看 N-VDS 状态。

3 或者，使用 `esxcli network ip interface list` 命令查看 ESXi 上的 N-VDS。

在 ESXi 上，命令输出应包含一个 vmk 接口（如 vmk10）和 VDS 名称，该名称与在配置传输区域和传输节点时使用的名称相匹配。

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

vmk10
   Name: vmk10
   MAC Address: 00:50:56:64:63:4c
   Enabled: true
   Portset: DvsPortset-1
   Portgroup: N/A
   Netstack Instance: vxlan
   VDS Name: overlay-hostswitch
   VDS UUID: 18 ae 54 04 2c 6f 46 21-b8 ae ef ff 01 0c aa c2
   VDS Port: 10
   VDS Connection: 10
   Opaque Network ID: N/A
   Opaque Network Type: N/A
   External ID: N/A
   MTU: 1600
   TSO MSS: 65535
   Port ID: 67108895

 ...
```

如果使用 vSphere Client，您可以在 UI 中选择主机**配置 > 网络适配器**查看安装的 N-VDS。

用于验证 N-VDS 安装的 KVM 命令是 `ovs-vsctl show`。请注意，在 KVM 上，N-VDS 名称为 nsx-switch.0。它与传输节点配置中的名称不匹配。这是设计问题。

```
# ovs-vsctl show
...
    Bridge "nsx-switch.0"
        Port "nsx-uplink.0"
            Interface "em2"
        Port "nsx-vtep0.0"
            tag: 0
            Interface "nsx-vtep0.0"
                type: internal
        Port "nsx-switch.0"
            Interface "nsx-switch.0"
                type: internal
    ovs_version: "2.4.1.3340774"
```

4 检查为传输节点分配的隧道端点地址。

vmk10 接口从 NSX-T Data Center IP 池或 DHCP 中接收 IP 地址，如下所示：

```
# esxcli network ip interface ipv4 get
Name   IPv4 Address    IPv4 Netmask   IPv4 Broadcast   Address Type  DHCP DNS
-----  --------------  -------------  ---------------  ------------  --------
vmk0   192.168.210.53  255.255.255.0  192.168.210.255  STATIC           false
vmk1   10.20.20.53     255.255.255.0  10.20.20.255     STATIC           false
vmk10 192.168.250.3   255.255.255.0  192.168.250.255  STATIC          false
```

在 KVM 中，您可以使用 `ifconfig` 命令验证隧道端点和 IP 分配。

```
# ifconfig
...
nsx-vtep0.0 Link encap:Ethernet  HWaddr ba:30:ae:aa:26:53
          inet addr:192.168.250.4  Bcast:192.168.250.255  Mask:255.255.255.0
          ...
```

5 检查 API 以了解状态信息。

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"
}
```

添加计算管理器

计算管理器（如 vCenter Server）是一个管理资源（如主机和虚拟机）的应用程序。NSX-T Data Center 轮询计算管理器以了解更改（如添加或移除主机或虚拟机），并相应地更新其清单。添加计算管理器是可选操作，因为 NSX-T 即使没有计算管理器也会获取清单信息，例如独立主机和虚拟机。

在该版本中，该功能支持：

- vCenter Server 版本 6.5 Update 1、6.5 Update 2 和 6.7。
- 与 vCenter Server 的 IPv6 以及 IPv4 通信。
- 最多 5 个计算管理器。

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

步骤

1. 从浏览器中，使用管理员权限登录到位于 `https://<nsx-manager-ip-address>` 的 NSX Manager。
2. 从导航面板中选择**结构层 > 计算管理器**。
3. 单击**添加**。
4. 填写计算管理器详细信息。

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

如果将指纹值保留空白，将提示您接受服务器提供的指纹。

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

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

a 选择错误消息，然后单击**解决**。一个可能的错误消息如下：

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

b 输入 vCenter Server 凭据，然后单击**解决**。

如果存在现有注册，则会替换它。

“计算管理器”面板将显示一个计算管理器列表。您可以单击管理器的名称以查看或编辑有关管理器的详细信息，或者管理适用于管理器的标记。

创建裸机服务器工作负载的应用程序接口

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

步骤

1 安装所需的第三方软件包。

请参见在 KVM 主机或裸机服务器上安装第三方软件包。

2 配置 TCP 和 UDP 端口。

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

3 将裸机服务器添加到 NSX-T Data Center 结构层。

请参见将管理程序主机或裸机服务器添加到 NSX-T Data Center 结构层。

4 创建 KVM 主机传输节点。

请参见创建主机传输节点。

5 使用 Ansible playbook 创建应用程序接口。

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

配置 Network I/O Control 配置文件

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

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

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

系统流量的带宽保证

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

系统流量的带宽分配

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

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

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

系统流量的带宽分配参数

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

系统流量的分配参数

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

注 可以预留的带宽不能超过物理网络适配器带宽的 75%。例如，如果连接到 ESXi 主机的网络适配器为 10 GbE 时，您只能将 7.5 Gbps 的带宽分配给各种流量类型。您可能会使更多容量保持未预留状态。主机可以根据份额、限制和使用情况动态分配未预留的带宽。主机仅预留足以让系统功能运行的带宽。

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

要保证 NSX-T 主机上运行的系统流量获得最小带宽，请在 NSX-T 分布式交换机上启用并配置网络资源管理。

步骤

1 登录到 NSX Manager Manager (`https://<nsx-manager-IP-address>`)。

2 导航到**结构层 > 配置文件**。

3 选择 **NIOC 配置文件**。

4 单击 **+ 添加**。

5 在“新建 NIOC 配置文件”屏幕中，输入所需详细信息。

   a 输入 NIOC 配置文件的名称。

   b 将“状态”更改为**已启用**。

   c 在“主机基础架构流量资源”部分中，选择“流量类型”，然后输入“限制”、“份额”和“预留”值。

6 单击**添加**。

   此时，新 NIOC 配置文件将添加到 NIOC 配置文件列表中。

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

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

步骤

1 查询主机以同时显示系统定义的和用户定义的主机交换机配置文件。

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

   在下面的示例响应中，显示应用于主机的 NIOC 配置文件。

```
{
  "description": "This profile is created for Network I/O Control (NIOC).",
  "extends": {
  "$ref": "BaseHostSwitchProfile"+
  },
  "id": "NiocProfile",
  "module_id": "NiocProfile",
  "polymorphic-type-descriptor": {
  "type-identifier": "NiocProfile"
  },
  "properties": {
  "_create_time": {
  "$ref": "EpochMsTimestamp"+,
  "can_sort": true,
  "description": "Timestamp of resource creation",
```

```
  "readonly": true
    },
  "_create_user": {
  "description": "ID of the user who created this resource",
  "readonly": true,
  "type": "string"
    },
  "_last_modified_time": {
  "$ref": "EpochMsTimestamp"+,
  "can_sort": true,
  "description": "Timestamp of last modification",
  "readonly": true
    },

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

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

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

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

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

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

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

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

  "display_name": {
  "can_sort": true,
  "description": "Defaults to ID if not set",
  "maxLength": 255,
  "title": "Identifier to use when displaying entity in logs or GUI",
  "type": "string"
    },

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

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

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

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

  "host_infra_traffic_res": {
  "description": "host_infra_traffic_res specifies bandwidth allocation for various traffic
resources.",
  "items": {
  "$ref": "ResourceAllocation"+
    },
```

```
  "nsx_feature": "Nioc",
  "required": false,
  "title": "Resource allocation associated with NiocProfile",
  "type": "array"
    },

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

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

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

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

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

3 如果 NIOC 配置文件不存在，则创建一个新的 NIOC 配置文件。

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

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

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

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

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

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

  },

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

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

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

```
{
    "resource_type": "TransportNode",
    "description": "Updated NSX configured Test Transport Node",
    "id": "77816de2-39c3-436c-b891-54d31f580961",
    "display_name": "NSX Configured TN",
    "host_switch_spec": {
      "resource_type": "StandardHostSwitchSpec",
      "host_switches": [
        {
        "host_switch_profile_ids": [
          {
            "value": "e331116d-f59e-4004-8cfd-c577aefe563a",
            "key": "UplinkHostSwitchProfile"
          },
        {
       "value": "9e0b4d2d-d155-4b4b-8947-fbfe5b79f7cb",
       "key": "LldpHostSwitchProfile"
        }
       {
        "value": "b0185099-8003-4678-b86f-edd47ca2c9ad",
        "key": "NiocProfile"
       }
        ],
       "host_switch_name": "nsxvswitch",
       "pnics": [
      {
       "device_name": "vmnic1",
       "uplink_name": "uplink1"
      }
      ],
      "ip_assignment_spec": {
      "resource_type": "StaticIpPoolSpec",
      "ip_pool_id": "ecddcdde-4dc5-4026-ad4f-8857995d4c92"
      }
       }
      ]
    },
     "transport_zone_endpoints": [
      {
      "transport_zone_id": "e14c6b8a-9edd-489f-b624-f9ef12afbd8f",
      "transport_zone_profile_ids": [
        {
          "profile_id": "52035bb3-ab02-4a08-9884-18631312e50a",
          "resource_type": "BfdHealthMonitoringProfile"
        }
      ]
      }
    ],

     "host_switches": [
      {
```

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

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

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

[root@ host:] net-dvs -l

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

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

6 确认主机内核中的 NIOC 配置文件。

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

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

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

```
Uplink NIOC Info
            {
    Uplink device:vmnic4
    Link Capacity in Mbps:750
    vm respool reservation:275
    link status:1
    NetSched Ready:1
    Infrastructure reservation:0
    Total VM reservation:200
    Total vnics on this uplink:1
    NIOC Version:3
    Uplink index in BitMap:0
   }
```

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

创建 NSX Edge 传输节点

传输节点是一个可以加入 NSX-T Data Center 覆盖网络或 NSX-T Data Center VLAN 网络的节点。如果任何节点包含 N-VDS，则可以将其作为传输节点。此类节点包括但不限于 NSX Edge。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**结构层 > Edge** 页面上的 MPA 连接必须为“已连接”。请参见将 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，也可以为裸机 NSX Edge 节点使用默认上行链路配置文件。
- 必须配置一个 IP 池，或者它必须在网络部署中可用。
- 必须在主机或 NSX Edge 节点上具有至少一个未使用的物理网卡。

步骤

1. 从浏览器中，使用管理员权限登录到位于 `https://<nsx-manager-ip-address>` 的 NSX Manager。
2. 选择**结构层 > 节点 > 传输节点 > 添加**。
3. 键入 NSX Edge 传输节点的名称。
4. 从下拉列表中选择一个 NSX Edge 结构层节点。
5. 选择该传输节点所属的传输区域。

   NSX Edge 传输节点属于至少两个传输区域：用于 NSX-T Data Center 连接的覆盖网络以及用于上行链路连接的 VLAN。
6. 单击 **N-VDS** 选项卡，然后提供 N-VDS 信息。

选项	说明
N-VDS 名称	必须与在创建传输区域时配置的名称相匹配。
上行链路配置文件	从下拉菜单中选择上行链路配置文件。 可用的上行链路取决于选定的上行链路配置文件中的配置。
IP 分配	为覆盖网络 N-VDS 选择**使用 IP 池**或**使用静态 IP 列表**。 如果选择**使用静态 IP 列表**，您必须指定以逗号分隔的 IP 地址、网关和子网掩码列表。
IP 池	如果您选择**使用 IP 池**进行 IP 分配，请指定 IP 池名称。
物理网卡	与主机传输节点（将 vmnicX 作为物理网卡）不同，NSX Edge 传输节点使用 fp-ethX。

7. （可选）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
}
```


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


```
{
  "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"
}
```


后续步骤

将 NSX Edge 节点添加到 NSX Edge 群集。请参见创建 NSX Edge 群集。

创建 NSX Edge 群集

具有多节点 NSX Edge 群集可以帮助确保至少一个 NSX Edge 始终可用。要使用 NAT、负载平衡器等有状态服务创建 Tier-0 逻辑路由器或 Tier-1 路由器，必须将其与 NSX Edge 群集相关联。因此，即使您只有一个 NSX Edge，它也必须属于 NSX Edge 群集才能使用。

只能将 NSX Edge 传输节点添加到一个 NSX Edge 群集中。

可以使用 NSX Edge 群集支持多个逻辑路由器。

在创建 NSX Edge 群集后，以后可以编辑该群集以添加额外的 NSX Edge。

前提条件

- 安装至少一个 NSX Edge 节点。
- 将 NSX Edge 加入管理层面。
- 将 NSX Edge 添加为传输节点。
- （可选）在**结构层 > 配置文件 > Edge 群集配置文件**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 从浏览器中，使用管理员权限登录到位于 `https://<nsx-manager-ip-address>` 的 NSX Manager。

2 导航到**结构层 > 节点 > Edge 群集 > 添加**。

3 输入 NSX Edge 群集的名称。

4 选择一个 NSX Edge 群集配置文件。

5 单击**编辑**，然后选择**物理机**或**虚拟机**。

物理机是指在裸机上安装的 NSX Edge。虚拟机是指安装为虚拟机/虚拟设备的 NSX Edge。

6 对于“虚拟机”，请从“成员类型”下拉菜单中选择“NSX Edge 节点”或**公有云网关节点**。

如果虚拟机部署在公有云环境中，请选择“公有云网关节点”，否则，选择“NSX Edge 节点”。

7 从**可用**列中，选择 NSX Edge 并单击右箭头以将其移到**选定**列中。

后续步骤

您现在可以构建逻辑网络拓扑以及配置服务。请参见 NSX-T Data Center 管理指南。

NSX Cloud 组件安装

9

NSX Cloud 通过单一窗口来管理公有云网络。

NSX Cloud 与提供商特定的网络无关，它不需要公有云中的管理程序访问权限。

它具有诸多好处：

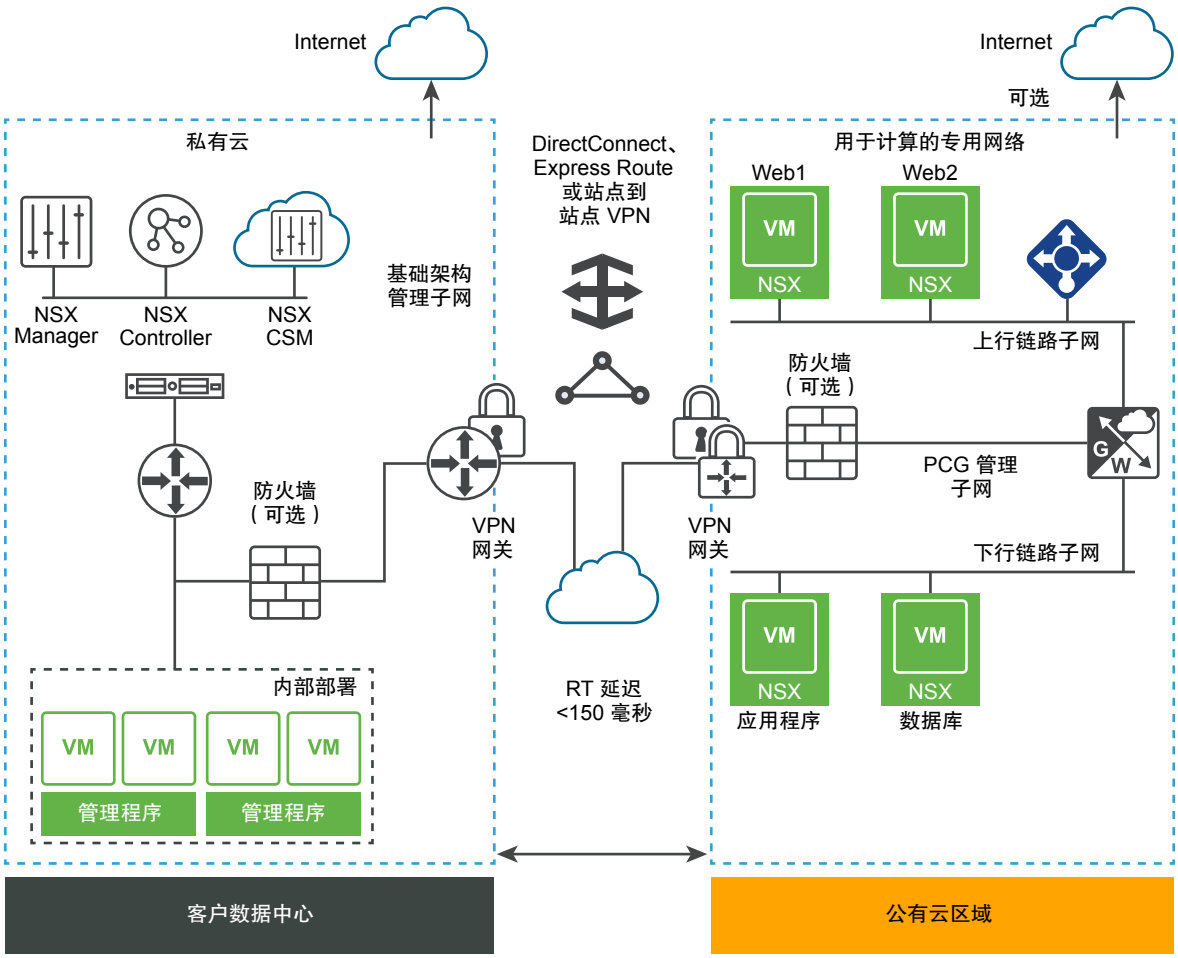
- 您可以使用生产环境中采用的相同网络和安全配置文件开发和测试应用程序。
- 开发人员在部署就绪之前，可以一直管理他们的应用程序。
- 具有灾难恢复功能，可在遇到计划外停机或公有云遭到安全威胁时进行恢复。
- 如果在公有云之间迁移工作负载，NSX Cloud 可确保对工作负载虚拟机应用类似的安全策略，而无论虚拟机的新位置在哪。

本章讨论了以下主题：

NSX Cloud 架构和组件

NSX Cloud 将 NSX-T Data Center 核心组件、NSX Manager、NSX Controller 和您的公有云相集成，以跨实施提供网络与安全性。

图 9-1. NSX Cloud 架构



NSX Cloud 核心组件有：

- NSX Manager，用于管理层面，并定义了基于角色的访问控制 (RBAC)。
- NSX Controller，用于控制层面和运行时状态。
- Cloud Service Manager，用于与 NSX Manager 集成，以向管理层面提供特定于公有云的信息。
- NSX Public Cloud Gateway，用于连接到 NSX 管理层面和控制层面、NSX Edge 网关服务，并可与公有云实体进行基于 API 的通信。
- NSX 代理功能，为工作负载虚拟机提供 NSX 管理的数据路径。

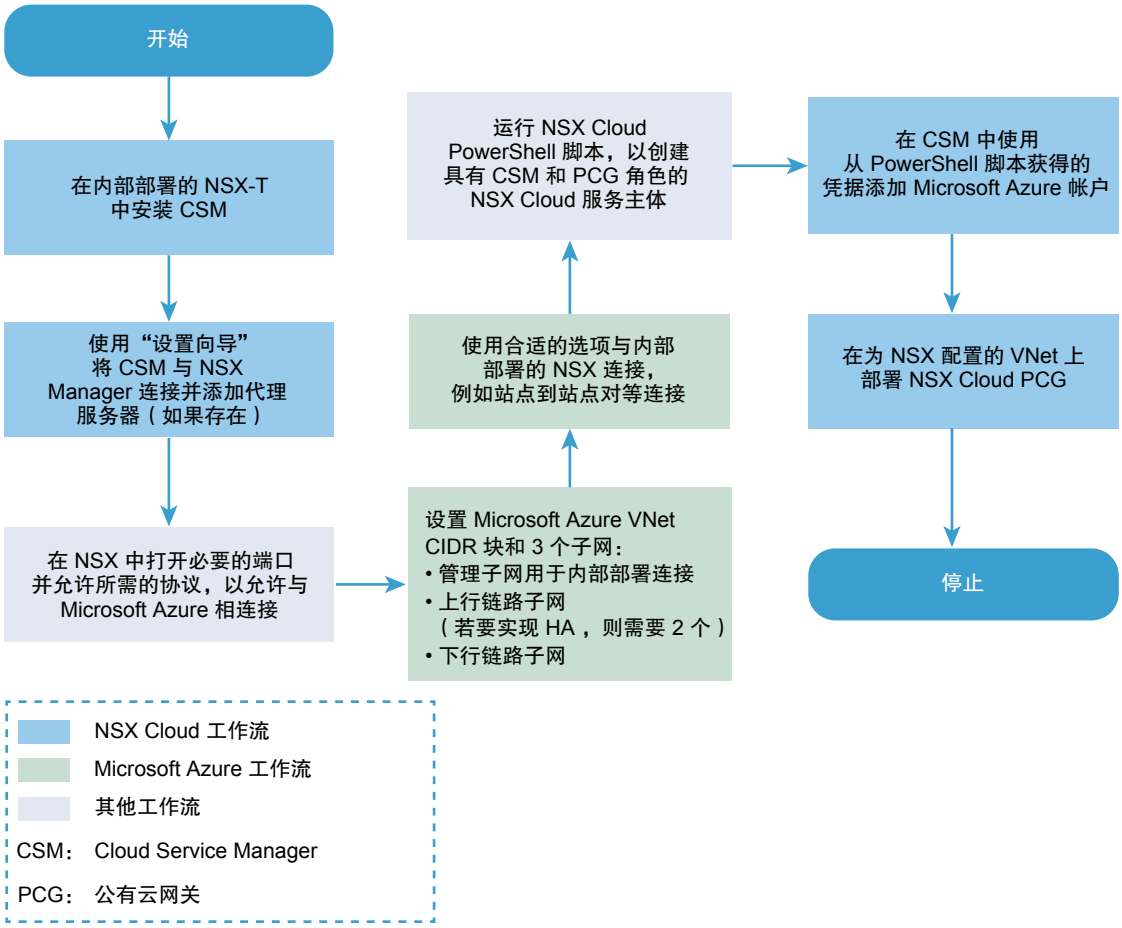
NSX Cloud 组件安装概述

请参考以下流程图，了解如何启用 NSX-T Data Center 来管理公有云中工作负载虚拟机的初始操作。

Microsoft Azure 的初始工作流

此流程图概述了将 Microsoft Azure VNet 添加到 NSX Cloud 所涉及的步骤。

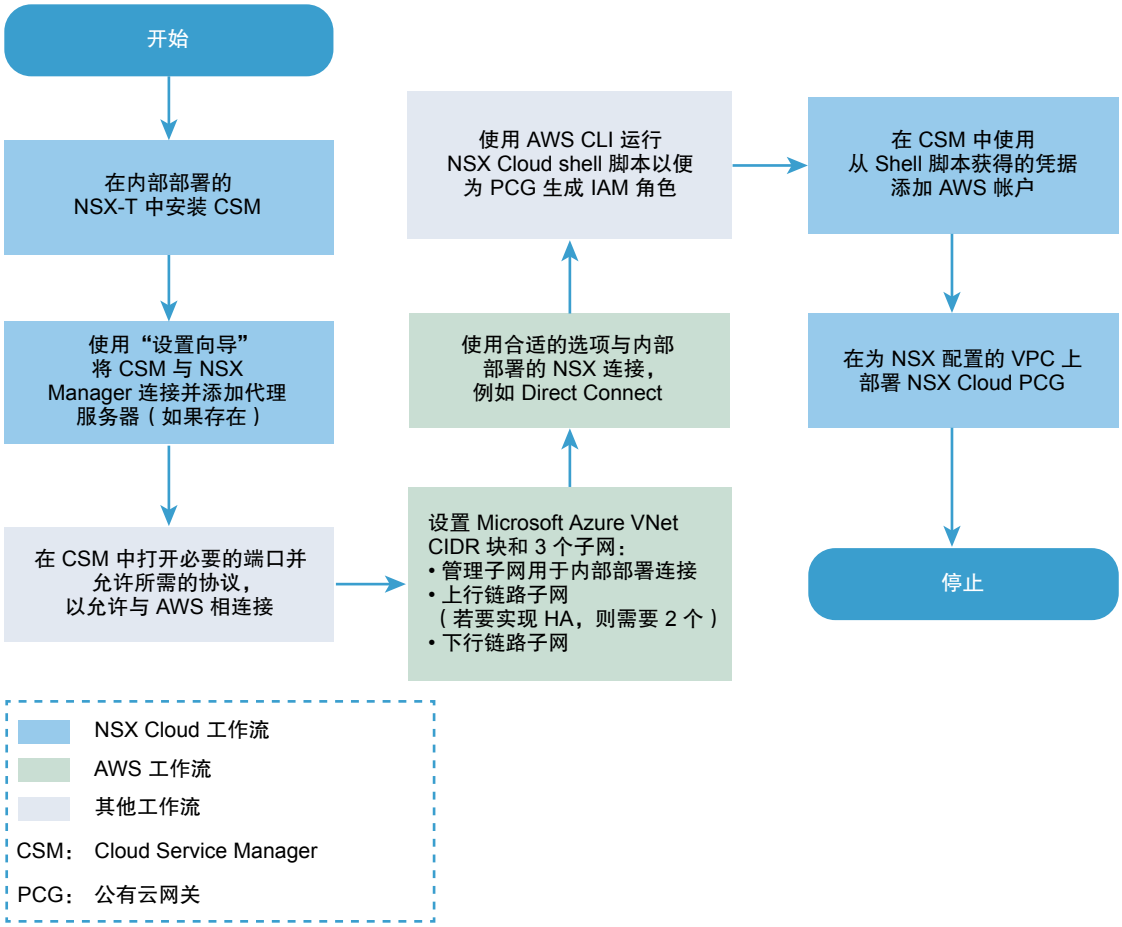
图 9-2. Microsoft Azure 的 NSX Cloud 初始工作流



AWS 的初始工作流

以下流程图概述了将 AWS VPC 添加到 NSX Cloud 时涉及的步骤。

图 9-3. AWS 的 NSX Cloud 初始工作流



安装 CSM 并与 NSX Manager 连接

使用设置向导将 NSX Manager 与 CSM 连接并设置代理服务器（如果有）。

安装 CSM

Cloud Service Manager (CSM) 是 NSX Cloud 的基本组件。

请在安装 NSX-T Data Center 核心组件后安装 CSM。

有关详细说明，请参见安装 NSX Manager 和可用设备。

发布 NSX Manager 的 FQDN

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

此外，您还必须使用 NSX-T API 启用 NSX Manager FQDN 发布。

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

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

示例响应：

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

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

将 CSM 与 NSX Manager 相连接

必须将 CSM 设备与 NSX Manager 连接，以允许这些组件互相通信。

前提条件

- 必须安装 NSX Manager，并且您必须具有管理员特权，以便登录到 NSX Manager
- 必须安装 CSM，并且您必须具有 CSM 中分配的企业管理员角色。

步骤

1 打开到 NSX Manager 的 SSH 会话。

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

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

命令输出是该 NSX Manager 特有的数字串。

3 以企业管理员角色登录到 CSM。

4 单击**系统 > 设置**。然后在标题为**关联的 NSX 节点**的面板上，单击**配置**。

注 使用首次安装 CSM 时可用的 CSM 设置向导，也可以提供这些详细信息。

5 输入 NSX Manager 的详细信息。

选项	说明
NSX Manager 主机名	输入 NSX Manager 的完全限定域名 (FQDN)（如果可用）。您还可以输入 NSX Manager 的 IP 地址。
管理员凭据	输入企业管理员角色的用户名和密码。
Manager 指纹	输入您在步骤 2 获取的 NSX Manager 的指纹值。

6 单击**连接**。

CSM 将验证 NSX Manager 指纹并建立连接。

（可选）配置代理服务器

如果要通过可靠的 HTTP 代理路由并监控 Internet 绑定的所有 HTTP/HTTPS 流量，则可以在 CSM 中配置最多五个代理服务器。

来自 PCG 和 CSM 的所有公有云通信都通过选定的代理服务器进行路由。

PCG 的代理设置独立于 CSM 的代理设置。可以选择不为 PCG 使用代理服务器或者使用不同的代理服务器。

可以选择以下级别的身份验证：

- 基于凭据的身份验证。
- 用于 HTTPS 拦截的基于证书的身份验证。
- 无身份验证。

步骤

1 单击**系统 > 设置**。然后在标题为**代理服务器**的面板上单击**配置**。

注 使用首次安装 CSM 时可用的 CSM 设置向导，也可以提供这些详细信息。

2 在“配置代理服务器”屏幕中，输入以下详细信息：

选项	说明
默认	使用此单选按钮指示默认代理服务器。
配置文件名称	提供代理服务器的配置文件名称。这是必填的。
代理服务器	输入代理服务器的 IP 地址。这是必填的。
端口	输入代理服务器的端口。这是必填的。
身份验证	可选。如果要设置其他身份验证，则选中此复选框并提供有效的用户名和密码。
用户名	如果选中“身份验证”复选框，则为必填项。
密码	如果选中“身份验证”复选框，则为必填项。
证书	可选。如果要为 HTTPS 拦截提供身份验证证书，则选中此复选框，并在出现的文本框中复制并粘贴该证书。
无代理	如果不希望使用已配置的任何代理服务器，则选中此选项。

将公有云与内部部署相连接

必须使用合适的连接选项将内部部署与公有云帐户或订阅相连接。

允许访问 CSM 上的端口和协议以实现混合连接

在 NSX Manager 上打开必要的网络端口并允许所需的协议，以启用公有云连接。

允许从公有云访问 NSX Manager

打开以下网络端口和协议，以允许与内部部署 NSX Manager 相连接：

表 9-1.

源	目标	协议/端口	说明
PCG	NSX Manager	TCP/5671	从公有云到内部部署 NSX-T Data Center 的用于管理层面通信的入站流量。
PCG	NSX Manager	TCP/8080	从公有云到内部部署 NSX-T Data Center 的用于升级的入站流量。
PCG	NSX Controller	TCP/1234、TCP/1235	从公有云到内部部署 NSX-T Data Center 的用于控制层面通信的入站流量。
PCG	DNS	UDP/53	从公有云到内部部署 NSX-T Data Center DNS 的入站流量（如果使用的是内部部署 DNS 服务器）。
CSM	PCG	TCP/7442	CSM 配置推送
任意	NSX Manager	TCP/443	NSX Manager UI
任意	CSM	TCP/443	CSM UI

重要　所有 NSX-T Data Center 基础架构通信都利用基于 SSL 的加密。请确保防火墙允许 SSL 流量通过非标准端口。

将 Microsoft Azure 网络与内部部署 NSX-T Data Center 相连接

必须在 Microsoft Azure 网络和内部部署 NSX-T Data Center 设备之间建立连接。

注　您必须已安装 NSX Manager 并将其与内部部署 CSM 相连接。

概述

- 将 Microsoft Azure 订阅与内部部署 NSX-T Data Center 相连接。
- 为 VNet 配置必要的 CIDR 块和 NSX Cloud 所需的子网。
- 将 CSM 设备上的时间与 Microsoft Azure 存储服务器或 NTP 同步。

将 Microsoft Azure 订阅与内部部署 NSX-T Data Center 相连接

每个公有云都提供了用来与内部部署连接的选项。您可以选择适合您要求的任意可用连接选项。有关详细信息，请参见 Microsoft Azure 参考文档。

注 您必须检查并实施适用的安全注意事项和 Microsoft Azure 最佳做法，例如，访问 Microsoft Azure 门户或 API 的所有特权用户帐户都应启用多重身份验证 (Multi Factor Authentication, MFA)。MFA 可确保只有合法用户才能访问该门户并降低非法合法访问的可能性，即使凭据被盗或泄漏也可以。有关详细信息和建议，请参阅“Azure Security Center Documentation”。

配置 VNet

在 Microsoft Azure 中，创建可路由 CIDR 块并设置所需的子网。

- 一个管理子网，包含至少为 /28 的建议范围，以处理：
  - 到内部部署设备的控制流量
  - 到云提供商 API 端点的 API 流量
- 一个下行链路子网，包含至少为 /24 的建议范围，用于工作负载虚拟机。
- 一个（若要实现 HA，则需要两个）上行链路子网，包含至少为 /24 的建议范围，用于路由离开或进入 VNet 的南北向流量。

将 Amazon Web Services (AWS) 网络与内部部署 NSX-T Data Center 相连接

必须在 Amazon Web Services (AWS) 网络和内部部署 NSX-T Data Center 设备之间建立连接。

注 您必须已安装 NSX Manager 并将其与内部部署 CSM 相连接。

概述

- 使用最符合您需求的任何可用选项将 AWS 帐户与内部部署 NSX Manager 设备相连接。
- 为 VPC 配置子网并根据 NSX Cloud 的其他要求进行配置。

将 AWS 帐户与内部部署 NSX-T Data Center 相连接

每个公有云都提供了用来与内部部署连接的选项。您可以选择适合您要求的任意可用连接选项。有关详细信息，请参见 AWS 参考文档。

注 您必须检查并实施适用的安全注意事项和 AWS 最佳做法；请参见 AWS 安全最佳做法。

配置 VPC

需要以下配置：

- 六个子网，用于支持具有高可用性的 PCG

- 一个 Internet 网关 (IGW)
- 一个专用和一个公用路由表
- 子网与路由表相关联
- 已启用 DNS 解析和 DNS 主机名

配置 VPC 时请遵循以下准则：

1 假设您的 VPC 使用 /16 网络，对于需要部署的每个网关，设置三个子网。

重要 如果使用高可用性，请在其他可用区中再设置三个子网。

- **管理子网**：此子网用于内部部署 NSX-T Data Center 和 PCG 之间的管理流量。建议的范围为 /28。
- **上行链路子网**：此子网用于南北向 Internet 流量。建议的范围为 /24。
- **下行链路子网**：此子网包括工作负载虚拟机的 IP 地址范围，应相应地调整大小。请注意，要进行调试，可能需要包含工作负载虚拟机上的其他接口。

注 为子网添加相应的标签，例如，**`management-subnet`**、**`uplink-subnet`**、**`downlink-subnet`**，因为在此 VPC 上部署 PCG 时需要选择子网。

2 确保您具有已连接到此 VPC 的 Internet 网关 (IGW)。

3 确保 VPC 的路由表已将**目标**设置为 **`0.0.0.0/0`** 且**目标**是连接到 VPC 的 IGW。

4 确保已为此 VPC 启用 DNS 解析和 DNS 主机名。

添加公有云帐户

要添加公有云清单，需要在公有云中创建允许访问 NSX Cloud 的角色，然后在 CSM 中添加所需信息。

使 CSM 访问 Microsoft Azure 清单

Microsoft Azure 订阅包含一个或多个希望由 NSX-T Data Center 管理的 VNet。

注 如果已将 AWS 帐户添加到 CSM，请在 **NSX Manager > 结构层 > 配置文件 > 上行链路配置文件 > PCG-Uplink-HostSwitch-Profile** 中将 MTU 更新为 1500，然后再添加 Microsoft Azure 帐户。也可以使用 NSX Manager REST API 执行此操作。

要在订阅中运行 NSX Cloud，需要创建新的服务主体以向 NSX-T Data Center 授予所需的访问权限。此外，还需要为 CSM 和 PCG 创建 MSI 角色。

NSX Cloud 提供 PowerShell 脚本以生成服务主体。

该过程分为两步：

1 使用 NSX Cloud PowerShell 脚本：

- 为 NSX Cloud 创建服务主体帐户。

- 为 CSM 创建角色并将其附加到服务主体。
- 为 PCG 创建角色并将其附加到服务主体。

2 在 CSM 中添加 Microsoft Azure 订阅。

生成所需的角色

NSX Cloud 利用 Microsoft Azure 的托管服务标识 (MSI) 功能管理身份验证，同时确保 Microsoft 凭据安全。

要使 NSX Cloud 在 Microsoft Azure 订阅中运行，需要为 CSM 和 PCG 生成 MSI 角色以及为 NSX Cloud 生成服务主体。

为此，可以运行 NSX Cloud PowerShell 脚本。此外，还需要 JSON 格式的两个文件作为参数。使用所需的参数运行 PowerShell 脚本时，会创建以下构造：

- 为 NSX Cloud 创建 Azure AD 应用程序。
- 为 NSX Cloud 应用程序创建 Azure 资源管理器服务主体。
- 为连接到服务主体帐户的 CSM 创建角色。
- 为 PCG 创建角色，以使其在公有云清单上运行。

注 首次运行脚本时，Microsoft Azure 响应时间可能会导致脚本失败。如果脚本失败，请尝试重新运行。

前提条件

- 您必须安装了包含 AzureRM 模块的 PowerShell 5.0+。
- 您必须是要运行脚本以生成 NSX Cloud 服务主体的 Microsoft Azure 订阅的所有者。

步骤

1 在 Windows 桌面或服务器上，从 NSX-T Data Center **下载页面 > 驱动程序和工具 > NSX Cloud 脚本 > Microsoft Azure** 下载名为 `CreateNSXCloudCredentials.zip` 的 ZIP 文件。

2 将 ZIP 文件的以下内容提取到 Windows 系统中：

文件名	说明
CreateNSXRoles.ps1	此 PowerShell 脚本用于生成 NSX Cloud 服务主体以及为 CSM 和 PCG 生成 MSI 角色
nsx_csm_role.json	此文件包含 Microsoft Azure 中的 CSM 角色名称和此角色的权限。这是 PowerShell 脚本的输入，必须与脚本位于同一文件夹中。
nsx_pcg_role.json	此文件包含 Microsoft Azure 中的 PCG 角色名称和此角色的权限。这是 PowerShell 脚本的输入，必须与脚本位于同一文件夹中。默认 PCG（网关）角色名称为 `nsx-pcg-role`。

注 如果要在 Microsoft Azure Active Directory 中为多个订阅创建角色，必须在相应的 JSON 文件中更改每个订阅的 CSM 和 PCG 角色名称，然后重新运行脚本。

3 运行脚本并使用您的 Microsoft Azure 订阅 ID 作为参数。参数名称为 `subscriptionId`。

例如，

```
.\CreateNSXRoles.ps1 –subscriptionId <your_subscription_ID>
```

这会为 NSX Cloud 创建服务主体以及为 CSM 和 PCG 创建具有相应特权的角色，并将 CSM 和 PCG 角色附加到 NSX Cloud 服务主体。

4 在运行 PowerShell 脚本的同一目录中查找文件。该文件的文件名类似于：`NSXCloud_ServicePrincipal_<your_subscription_ID>_<NSX_Cloud_Service_Principal_name>`。该文件包含在 CSM 中添加 Microsoft Azure 订阅所需的信息。

- 客户端 ID
- 客户端密钥
- 租户 ID
- 订阅 ID

注 有关创建 CSM 和 PCG 角色后适用于这些角色的权限列表，请参阅用于创建这些角色的 JSON 文件。

后续步骤

在 CSM 中添加 Microsoft Azure 订阅

在 CSM 中添加 Microsoft Azure 订阅

获取 NSX Cloud 服务主体以及 CSM 和 PCG 角色的详细信息后，即可在 CSM 中添加 Microsoft Azure 订阅。

前提条件

- 您必须在 NSX-T Data Center 中拥有企业管理员角色。
- 您必须拥有 PowerShell 脚本的输出和 NSX Cloud 服务主体的详细信息。
- 您必须具有运行 PowerShell 脚本以创建角色和服务主体时提供的 PCG 角色的值。

步骤

1 使用具有企业管理员角色的帐户登录到 CSM。

2 转到 **CSM > 云 > Azure**。

3 单击 **+ 添加**，然后输入以下详细信息：

选项	说明
名称	提供合适的名称以在 CSM 中标识此帐户。您可能有多个 Microsoft Azure 订阅与同一个 Microsoft Azure 租户 ID 相关联。对您的帐户命名，您可在 CSM 中使用合适的名称，例如 Azure-DevOps-Account、Azure-Finance-Account 等。
客户端 ID	从 PowerShell 脚本的输出中复制粘贴此值。
密钥	从 PowerShell 脚本的输出中复制粘贴此值。
订阅 ID	从 PowerShell 脚本的输出中复制粘贴此值。

选项	说明
租户 ID	从 PowerShell 脚本的输出中复制粘贴此值。
网关角色名称	默认值为 `nsx-pcg-role`。如果更改了默认值，可从 nsx_pcg_role.json 文件获得此值。
云标记	默认情况下，此选项处于启用状态，并允许 Microsoft Azure 标记在 NSX Manager 中可见

4 单击**保存**。

CSM 将添加该帐户，几分钟后您可在**帐户**部分中看到该帐户。

后续步骤

在 Microsoft Azure VNet 中部署 PCG

使 CSM 访问 AWS 清单

AWS 帐户包含一个或多个希望由 NSX-T Data Center 管理的计算 VPC。

该过程分为三步：

1 使用 NSX Cloud 脚本（需要 AWS CLI）执行以下操作：

- 创建 IAM 配置文件。
- 为 PCG 创建角色。

2 在 CSM 中添加 AWS 帐户。

生成所需的角色

NSX Cloud 利用 AWS IAM 生成附加到 NSX Cloud 配置文件的角色，以提供 PCG 访问 AWS 帐户所需的权限。

要使 NSX Cloud 在 AWS 帐户中运行，需要为 PCG 生成 IAM 配置文件和角色。

为此，可通过 AWS CLI 运行 NSX Cloud shell 脚本以创建以下构造：

- 为 NSX Cloud 创建 IAM 配置文件。
- 为 PCG 创建角色，以使其在公有云清单上运行。

前提条件

- 您必须使用 AWS 帐户的访问密钥和密钥来安装和配置 AWS CLI。
- 您必须选取唯一的 IAM 配置文件名来提供给脚本。网关角色名称已附加到此 IAM 配置文件
-

步骤

1 在 Linux 或者兼容的桌面或服务器上，从 NSX-T Data Center **下载页面 > 驱动程序和工具 > NSX Cloud 脚本 > AWS** 下载名为 `AWS_create_credentials.sh` 的 SHELL 脚本。

2 运行脚本，然后在出现提示时输入 IAM 配置文件的名称。例如，

```
bash AWS_create_NSXCloud_credentials.sh
```

3 脚本成功运行后，会在 AWS 帐户中为 PCG 创建该 IAM 配置文件和角色。值将保存在运行脚本时的同一目录下的输出文件中。文件名为 `aws_details.txt`。

> **注** 默认情况下，PCG（网关）角色名称为 `nsx_pcg_service`。如果要对网关角色名称使用不同的值，可以在脚本中进行更改。要在 CSM 中添加 AWS 帐户，必须提供此值，因此，如果更改了默认值，必须记下来。

后续步骤

在 CSM 中添加 AWS 帐户

在 CSM 中添加 AWS 帐户

使用脚本生成的值添加 AWS 帐户。

步骤

1 使用企业管理员角色登录到 CSM。

2 转到 **CSM > 云 > AWS**。

3 单击 **+添加**，然后使用从 NSX Cloud 脚本生成的输出文件 aws_details.txt 输入以下详细信息：

选项	说明
名称	输入此 AWS 帐户的描述性名称
访问密钥	输入帐户的访问密钥
密钥	输入帐户的密钥
云标记	默认情况下，此选项处于启用状态，并允许 AWS 标记在 NSX Manager 中可见
网关角色名称	默认值为 `nsx_pcg_service`。可以在脚本的输出文件 aws_details.txt 中找到此值。

AWS 帐户添加到了 CSM 中。

在 CSM 的“VPC”选项卡中，可以查看您 AWS 帐户中的所有 VPC。

在 CSM 的“实例”选项卡中，可以查看此 VPC 中的 EC2 实例。

后续步骤

在 AWS VPC 中部署 PCG

部署 PCG

NSX Public Cloud Gateway (PCG) 在公有云和 NSX-T Data Center 内部部署管理组件之间提供南北向连接。

必备条件

- 您的公有云帐户必须已添加到 CSM。
- 部署 PCG 的 VPC 或 VNet 必须相应调整实现高可用性所需的子网：上行链路、下行链路和管理。

PCG 部署与使用 NSX-T Data Center 组件的 FQDN 的网络寻址计划和可以解析这些 FQDN 的 DNS 服务器相一致。

注　不建议使用 PCG 连接公有云和 NSX-T Data Center 时使用 IP 地址，但是如果选择该选项，请勿更改 IP 地址。

在 Microsoft Azure VNet 中部署 PCG

请按照以下说明在 Microsoft Azure 订阅中部署 PCG。

步骤

1 使用具有企业管理员角色的帐户登录到 CSM。

2 单击**云 > Azure**，然后转到 **VNet** 选项卡。

3 单击要在其中部署 PCG 的 VNet。

4 单击**部署网关**。将打开**部署主网关**向导。

5 对于“常规属性”，请使用以下准则：

选项	说明
SSH 公钥	提供部署 PCG 时可验证的 SSH 公钥。这是每次 PCG 部署所必需的。
关联 VNet 上的隔离策略	首次部署 PCG 时，将其保留默认的**已禁用**模式。载入虚拟机后，可以更改此值。有关详细信息，请参见《NSX-T Data Center 管理指南》中的**管理隔离策略**。
本地存储帐户	向 CSM 添加 Microsoft Azure 订阅时，Microsoft Azure 存储帐户列表可用于 CSM。从下拉菜单中选择存储帐户。继续部署 PCG 时，CSM 会将 PCG 的公开可用 VHD 复制到所选区域的此存储帐户。 注　如果 VHD 映像已复制到之前的 PCG 部署对应的区域中的此存储帐户，则后续部署将使用此位置的映像，以减少整体部署时间。
VHD URL	如果要使用 VMware 公共存储库不提供的其他 PCG 映像，可在此处输入该 PCG VHD 的 URL。VHD 必须位于用来创建此 VNet 的帐户和区域中。
代理服务器	选择一个代理服务器以用于来自此 PCG 的 Internet 流量。在 CSM 中配置代理服务器。可以选择与 CSM（如果存在）相同的代理服务器，也可以选择与 CSM 不同的代理服务器，还可以选择**无代理服务器**。 有关如何在 CSM 中配置代理服务器的详细信息，请参见（可选）配置代理服务器。
高级	使用高级 DNS 设置，可以灵活地选择用于解析 NSX-T Data Center 管理组件的 DNS 服务器。

选项	说明
通过公有云提供商的 DHCP 获取	如果要使用 Microsoft Azure DNS 设置，请选择此选项。如果您未选择任一选项将其替代，则此选项是默认的 DNS 设置。
替代公有云提供商的 DNS 服务器	如果要手动提供用于解析 NSX-T Data Center 设备以及此 VNet 中的工作负载虚拟机的一个或多个 DNS 服务器的 IP 地址，请选择此选项。
仅对 NSX-T Data Center 设备使用公有云提供商的 DNS 服务器	如果要使用 Microsoft Azure DNS 服务器解析 NSX-T Data Center 管理组件，请选择此选项。选择此设置后，您可以使用两个 DNS 服务器：一个用于 PCG，以解析 NSX-T Data Center 设备；另一个用于 VNet，以解析此 VNet 中的工作负载虚拟机。

6 单击**下一步**。

7 对于**子网**，请使用以下准则：

选项	说明
为 NSX Cloud 网关启用 HA	选择此选项以启用高可用性。
子网	选择此选项以启用高可用性。
管理网卡上的公用 IP	选择**分配新 IP 地址**，以向管理网卡提供公用 IP 地址。如果要重用可用的公用 IP 地址，可以手动提供该公用 IP 地址。
上行链路网卡上的公用 IP	选择**分配新 IP 地址**，以向上行链路网卡提供公用 IP 地址。如果要重用可用的公用 IP 地址，可以手动提供该公用 IP 地址。

后续步骤

载入工作负载虚拟机。有关第 N 天工作流，请参见《NSX-T Data Center 管理指南》中的**载入并管理工作负载虚拟机**。

在 AWS VPC 中部署 PCG

请按照以下说明在 AWS 帐户中部署 PCG。

步骤

1 使用具有企业管理员角色的帐户登录到 CSM。

2 单击**云 > AWS > <AWS_account_name>**，然后转到 **VPC** 选项卡。

3 在 **VPC** 选项卡中，选择 AWS 区域名称，例如，`us-west`。AWS 区域必须是创建计算 VPC 的同一区域。

4 选择为 NSX Cloud 配置的计算 VPC。

5 单击**部署网关**。

6 填写常规网关详细信息：

选项	说明
PEM 文件	从下拉菜单中选择一个 PEM 文件。此文件必须位于部署 NSX Cloud 并创建 VPC 的同一区域。 这可唯一地标识您的 AWS 帐户。
关联 VPC 上的隔离策略	默认选择为“已启用”。对于绿地 (greenfield) 部署，建议启用。如果已在 VPC 中启动虚拟机，请禁用隔离策略。有关详细信息，请参见《NSX-T Data Center 管理指南》中的**管理隔离策略**。
代理服务器	选择一个代理服务器以用于来自此 PCG 的 Internet 流量。在 CSM 中配置代理服务器。可以选择与 CSM（如果存在）相同的代理服务器，也可以选择与 CSM 不同的代理服务器，还可以选择**无代理服务器**。 有关如何在 CSM 中配置代理服务器的详细信息，请参见（可选）配置代理服务器。
高级	高级设置提供额外选项（如果需要）。
替代 AMI ID	使用此高级功能可为 PCG 提供一个不同于 AWS 帐户所提供的 AMI ID。
通过公有云提供商的 DHCP 获取	如果要使用 AWS 设置，请选择此选项。如果您未选择任一选项将其替代，则此选项是默认的 DNS 设置。
替代公有云提供商的 DNS 服务器	如果要手动提供用于解析 NSX-T Data Center 设备以及此 VPC 中的工作负载虚拟机的一个或多个 DNS 服务器的 IP 地址，请选择此选项。
仅对 NSX-T Data Center 设备使用公有云提供商的 DNS 服务器	如果要使用 AWS DNS 服务器解析 NSX-T Data Center 管理组件，请选择此选项。选择此设置后，可以使用两个 DNS 服务器：一个用于 PCG，以解析 NSX-T Data Center 设备；另一个用于 VPC，以解析此 VPC 中的工作负载虚拟机。

7 单击**下一步**。

8 填写子网详细信息。

选项	说明
为公有云网关启用 HA	建议设置为“启用”，以设置高可用性活动/备用对，从而避免非计划停机。
主网关设置	从下拉菜单中选择一个可用区（如 `us-west-1a`）作为 HA 的主网关。 从下拉菜单中分配上行链路、下行链路和管理子网。
辅助网关设置	从下拉菜单中选择另一个可用区（如 `us-west-1b`）作为 HA 的辅助网关。 当主网关出现故障时，使用辅助网关。 从下拉菜单中分配上行链路、下行链路和管理子网。
管理网卡上的公用 IP	选择**分配新 IP 地址**，以向管理网卡提供公用 IP 地址。如果要重用可用的公用 IP 地址，可以手动提供该公用 IP 地址。
上行链路网卡上的公用 IP	选择**分配新 IP 地址**，以向上行链路网卡提供公用 IP 地址。如果要重用可用的公用 IP 地址，可以手动提供该公用 IP 地址。

单击**部署**。

9 监控主 PCG 部署（以及辅助部署，如果已选择）的状态。此过程可能需要 10-12 分钟的时间。

10 成功部署 PCG 后，单击**完成**。

后续步骤

载入工作负载虚拟机。有关第 N 天工作流，请参见《NSX-T Data Center 管理指南》中的**载入并管理工作负载虚拟机**。

部署 PCG 后创建的构造

PCG 成功部署后，会在 NSX Manager 中创建和配置必要的 NSX-T Data Center 实体，并在公有云中创建安全组。

NSX Manager 配置

在 NSX Manager 中会自动创建以下实体：

- 创建名为**公有云网关** (PCG) 的 Edge 节点。
- PCG 添加到 Edge 群集中。在高可用性部署中，有两个 PCG。
- PCG（或两个 PCG）注册为创建了两个传输区域的传输节点。
- 创建两个默认逻辑交换机。
- 创建一个第 0 层逻辑路由器。
- 创建 IP 发现配置文件。此配置文件用于覆盖网络逻辑交换机。
- 创建 DHCP 配置文件。此配置文件用于 DHCP 服务器。
- 创建名为 **PublicCloudSecurityGroup** 的默认 NS 组，其中包含以下成员：
  - 默认 VLAN 逻辑交换机
  - 逻辑端口，每个对应一个 PCG 上行链路端口（如果已启用 HA）。
  - IP 地址
- 创建三个默认的分布式防火墙规则：
  - LogicalSwitchToLogicalSwitch
  - LogicalSwitchToAnywhere
  - AnywhereToLogicalSwitch

  注 这些 DFW 规则会阻止所有流量，需要根据具体要求进行调整。

在 NSX Manager 中验证这些配置：

1 从 NSX Cloud 仪表板，单击 **NSX Manager**。

2 浏览到**结构层 > 节点 > Edge**。公有云网关应列为 Edge 节点。

3 验证部署状态、管理器连接和控制器连接是否为已连接（状态显示**已连接**并带有绿点）。

4 浏览到**结构层 > 节点 > Edge 群集**，以验证 Edge 群集和 PCG 是否已添加为此群集的一部分。

5 浏览到**结构层 > 节点 > 传输节点**，以验证 PCG 是否注册为传输节点且已连接到部署 PCG 时自动创建的两个传输区域：
   - 流量类型 VLAN -- 用于连接到 PCG 上行链路
   - 流量类型覆盖网络 -- 用于覆盖逻辑网络

6 验证是否已创建逻辑交换机和第 0 层逻辑路由器且逻辑路由器是否已添加到 Edge 群集。

重要 请勿删除任何 NSX 创建的实体。

公有云配置

在 AWS 中：

- 在 AWS VPC 中，添加名为 `nsx-gw.vmware.local` 的新类型 A 记录集。映射到此记录的 IP 地址与 PCG 的管理 IP 地址相匹配。这是由 AWS 使用 DHCP 分配的，且对于每个 VPC 会有所不同。
- 为 PCG 的上行链路接口创建一个辅助 IP。AWS 弹性 IP 与此辅助 IP 地址相关联。此配置适用于 SNAT。

在 AWS 和 Microsoft Azure 中：

gw 安全组应用于相应的 PCG 接口。

表 9-2. NSX Cloud 为 PCG 接口创建的公有云安全组

安全组名称	在 Microsoft Azure 中可用?	在 AWS 中可用?	全名
gw-mgmt-sg	是	是	网关管理安全组
gw-uplink-sg	是	是	网关上行链路安全组
gw-vtep-sg	是	是	网关下行链路安全组

表 9-3. NSX Cloud 为工作负载虚拟机创建的公有云安全组

安全组名称	在 Microsoft Azure 中可用?	在 AWS 中可用?	描述
quarantine	是	否	Microsoft Azure 隔离安全组
default	否	是	AWS 的隔离安全组
vm-underlay-sg	是	是	虚拟机非覆盖网络安全组
vm-override-sg	是	是	虚拟机替代安全组
vm-overlay-sg	是	是	虚拟机覆盖网络安全组（当前版本中未使用）
vm-outbound-bypass-sg	是	是	虚拟机出站绕过安全组（当前版本中未使用）
vm-inbound-bypass-sg	是	是	虚拟机入站绕过安全组（当前版本中未使用）

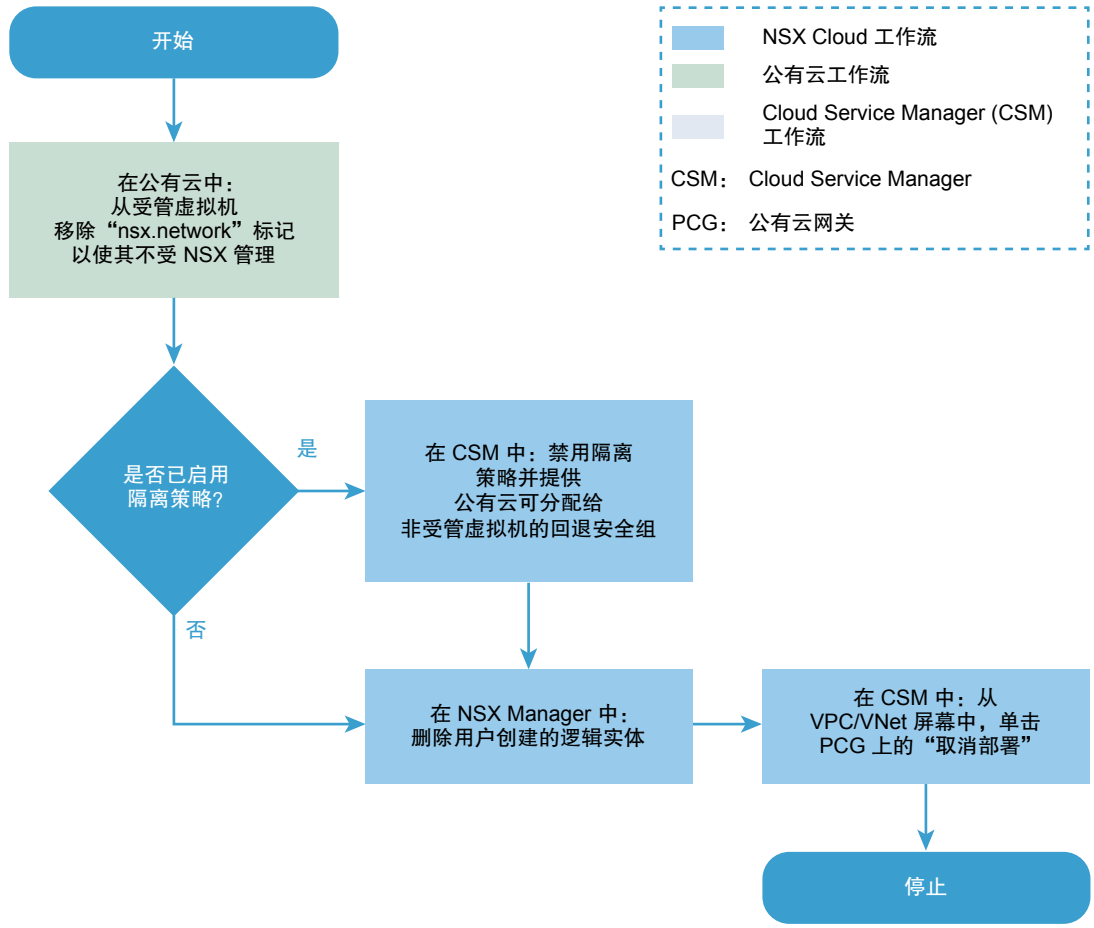
取消部署 PCG

请参阅以下流程图，了解取消部署 PCG 涉及的步骤。

- 要取消部署 PCG，必须满足以下条件：VPC 或 VNet 中的所有工作负载虚拟机都不能是 NSX 管理的虚拟机。
- 必须禁用隔离策略。

- 必须删除用户创建的且与 PCG 关联的所有逻辑实体。

图 9-4. 取消部署 PCG



1 取消标记公有云中的虚拟机

所有虚拟机必须为非受管虚拟机，才可取消部署 PCG。

2 禁用已启用的隔离策略

如果隔离策略先前已启用，必须将其禁用才能取消部署 PCG。

3 删除用户创建的逻辑实体

删除您在 NSX Manager 中创建的所有逻辑实体。

4 从 CSM 取消部署

要在满足必备条件后取消部署 PCG，请在 CSM 中，从**云 > <Public_Cloud> > <VNet/VPC>** 单击**取消部署网关**。

取消标记公有云中的虚拟机

所有虚拟机必须为非受管虚拟机，才可取消部署 PCG。

在公有云中转到 VPC 或 VNet，然后从受管虚拟机中移除 `nsx.network` 标记。

禁用已启用的隔离策略

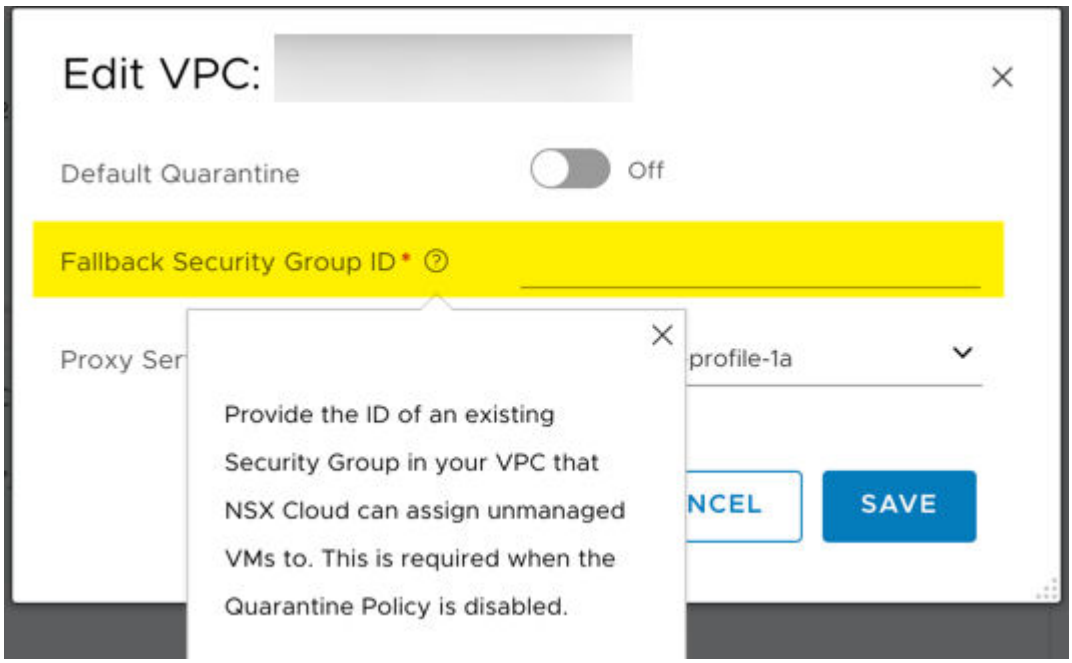
如果隔离策略先前已启用，必须将其禁用才能取消部署 PCG。

启用隔离策略时，会为虚拟机分配 NSX Cloud 定义的安全组。如果取消部署 PCG，则需要禁用隔离策略并指定将虚拟机从 NSX Cloud 安全组中移除时可将其分配到的回退安全组。

注 回退安全组必须是公有云中用户定义的现有安全组。不能使用任何 NSX Cloud 安全组作为回退安全组。有关 NSX Cloud 安全组列表，请参见部署 PCG 后创建的构造。

对要从中取消部署 PCG 的 VPC 或 VNet 禁用隔离策略：

- 在 CSM 中转到 VPC 或 VNet。
- 从**操作 > 编辑配置**，关闭**默认隔离**的设置。
- 为要将虚拟机分配到的回退安全组输入一个值。



- 此 VPC 或 VNet 中的所有非受管虚拟机或隔离虚拟机都会分配有该回退安全组。
- 如果所有虚拟机为非受管虚拟机，则将其分配到回退安全组。
- 如果禁用隔离策略时存在受管虚拟机，这些虚拟机将保留 NSX Cloud 为其分配的安全组。首次从此类虚拟机中移除 `nsx.network` 标记以使其不受 NSX 管理时，也会为其分配回退安全组。

注 有关启用和禁用隔离策略的说明以及所产生影响的详细信息，请参见 NSX-T Data Center 管理指南中的**管理隔离策略**。

删除用户创建的逻辑实体

删除您在 NSX Manager 中创建的所有逻辑实体。

请参考下面的列表，查找要删除的实体：

注 请勿删除部署 PCG 时自动创建的逻辑实体。请参见部署 PCG 后创建的构造

- 公有云 DNS 条目
- DDI：DHCP 配置文件
- 路由：SNAT 规则
- 路由：静态路由器
- 路由：逻辑路由器端口
- 路由：逻辑路由器
- 结构层-节点：Edge 群集
- 结构层-节点：传输节点
- 结构层-节点：Edge
- 结构层-配置文件：PCG-Uplink-HostSwitch-Profile
- 交换：逻辑交换机端口
- 交换：逻辑交换机
- 结构层-传输区域：传输区域
- 交换：PublicCloud-Global-SpoofGuardProfile

从 CSM 取消部署

要在满足必备条件后取消部署 PCG，请在 CSM 中，从**云 > <Public_Cloud> > <VNet/VPC>** 单击**取消部署网关**。

1 登录到 CSM 并转到公有云：
   - 如果使用的是 AWS，请转到**云 > AWS > VPC**。单击部署并运行一个或一对 PCG 的 VPC。
   - 如果使用的是 Microsoft Azure，请转到**云 > Azure > VNet**。单击部署并运行一个或一对 PCG 的 VNet。

2 单击**取消部署网关**。

取消部署 PCG 后，将自动移除 NSX Cloud 创建的默认实体。

卸载 NSX-T Data Center

10

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

本章讨论了以下主题：

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

取消配置 NSX-T Data Center 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. 登录到 vSphere Client。
2. 在虚拟机管理工具中，分离任何逻辑交换机中的所有虚拟机，然后将虚拟机连接到非 NSX-T Data Center 网络。
3. 对于 KVM 主机，通过 SSH 登录到主机并关闭虚拟机电源。

   ```
   shutdown -h now
   ```

4. 在 NSX Manager UI 或 API 中，删除所有逻辑路由器。
5. 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。
6. 在 NSX Manager UI 或 API 中，删除所有 NSX Edge，然后删除所有 NSX Edge 群集。
7. 根据需要，配置新的 NSX-T Data Center 覆盖网络。

从 NSX-T Data Center 中移除主机或完全卸载 NSX-T Data Center

如果要完全卸载 NSX-T Data Center，或者仅从 NSX-T Data Center 中移除管理程序主机以使主机脱离 NSX-T Data Center 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 Data Center。

前提条件

如果虚拟机管理工具是 vCenter Server，请将 vSphere 主机置于维护模式。

步骤

1 在 NSX Manager 中，选择**结构层 > 节点 > 传输节点**，然后删除主机传输节点。

如果删除传输节点，将导致从主机中移除 N-VDS。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
```

2 在 NSX Manager CLI 中，验证 NSX-T Data Center 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
```

3 从管理层面中卸载主机并移除 NSX-T Data Center 模块。

移除所有 NSX-T Data Center 模块可能最多需要 5 分钟的时间。

您可以使用几种方法移除 NSX-T Data Center 模块：

- 在 NSX Manager 中，选择**结构层 > 节点 > 主机 > 删除**。

  确保选中了**卸载 NSX 组件**。这会导致在主机上卸载 NSX-T Data Center 模块。

  移除 RHEL 7.4 依赖项软件包 - json_spirit、python-greenlet、libev、protobuf、leveldb、python-gevent、python-simplejson、glog。

  移除 Ubuntu 16.04.x 依赖项软件包 - nicira-ovs-hypervisor-node、openvswitch-switch、openvswitch-datapath-dkms、openvswitch-pki、python-openvswitch、openvswitch-common、libjson-spirit。

  请注意， 使用**结构层 > 节点 > 主机 > 删除**并取消选中**卸载 NSX 组件**选项并不表示用于取消注册主机。这仅作为处于错误状态的主机的一种解决方法。

- （计算管理器管理的主机）在 NSX Manager 中，选择**结构层 > 节点 > 主机 > 传输节点 > 删除主机**。

  在 NSX Manager 中，选择**结构层 > 节点 > 主机 > 计算管理器 > 配置群集管理器**，然后取消选中**自动安装 NSX**。选择节点，然后单击**卸载 NSX**。

  确保选中了**卸载 NSX 组件**。这会导致在主机上卸载 NSX-T Data Center 模块。

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

  注 此 API 不会从 nsx-lcp 包中移除依赖项软件包。

移除 RHEL 7.4 依赖项软件包 - json_spirit、python-greenlet、libev、protobuf、leveldb、python-gevent、python-simplejson、glog。

移除 Ubuntu 16.04.x 依赖项软件包 - nicira-ovs-hypervisor-node、openvswitch-switch、openvswitch-datapath-dkms、openvswitch-pki、python-openvswitch、openvswitch-common、libjson-spirit。

- 为 vSphere 使用 CLI。
  a 获取管理器指纹。

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

  b 在主机的 NSX-T Data Center 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 <ADMIN-USER> password <ADMIN-PASSWORD>
  thumbprint <MANAGER-THUMBPRINT>
  ```

  c 在主机上，运行以下命令以移除筛选器。

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

  d 在主机上，运行以下命令以停止 netcpa。

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

  e 关闭主机上虚拟机的电源，或将其迁移到另一台主机。

  f 在主机上，运行以下命令以手动卸载 NSX-T Data Center 配置和模块。在所有主机类型上均支持该命令。

  ```
  [root@host:~] clear management-plane
  ```

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 Data Center 覆盖网络。

如果要完全移除 NSX-T Data Center，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。