

NSX 升级指南

Update 5

修改日期：2017 年 11 月 20 日

VMware NSX Data Center for vSphere 6.2



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 升级指南 4

[阅读支持文档 4](#)

[NSX 的系统要求 5](#)

[NSX 所需的端口和协议 6](#)

1 vCloud Networking and Security 到 NSX 升级 9

[准备 vCloud Networking and Security 到 NSX 升级 9](#)

[从 vCloud Networking and Security 5.5.x 升级到 NSX 6.2.x 19](#)

[在 vCloud Director 环境中从 vCloud Networking and Security 5.5.x 升级到 NSX 37](#)

2 NSX 升级 54

[准备 NSX 升级 54](#)

[从 NSX 6.1.x 或 6.2.x 升级到 NSX 6.2.x 65](#)

[在跨 vCenter NSX 中升级到 NSX 6.2.x 78](#)

3 在 NSX 环境中升级 vSphere 94

[在 NSX 环境中升级 ESXi 94](#)

[在 ESXi 升级后重新部署 Guest Introspection 96](#)

NSX 升级指南

本手册（《NSX 升级指南》）介绍了如何使用 vSphere Web Client 升级 VMware® NSX™ 系统。此信息包括分步升级说明以及建议的最佳做法。

目标读者

本手册专供要在 VMware vCenter 环境中安装或使用 NSX 的用户使用。本手册的目标读者为熟悉虚拟机技术和虚拟数据中心操作且经验丰富的系统管理员。本手册假定您熟悉 VMware vSphere 5.5 或 6.0，包括 VMware ESXi、vCenter Server 和 vSphere Web Client。

VMware 技术出版物术语表

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

阅读支持文档

除了本升级指南之外，VMware 还发布了其他多本提供升级过程支持的文档。

发行说明

在开始升级之前，请查看发行说明。NSX 发行说明中介绍了已知升级问题和解决办法。在开始升级过程之前阅读升级问题可节省时间和精力。请参阅 <https://docs.vmware.com/cn/VMware-NSX-for-vSphere/index.html>。

产品互操作性列表

验证与其他 VMware 产品的互操作性，例如，vCenter。请参见 VMware 产品互操作性列表 (http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php) 中的互操作性 (Interoperability) 选项卡。

验证是否支持从当前 NSX 版本到目标版本的升级途径。在升级途径 (Upgrade Path) 选项卡中，从产品菜单中选择 VMware NSX。

兼容性指南

验证合作伙伴解决方案与 NSX 的兼容性，请参见《VMware 兼容性指南》，网址为 <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>。

NSX 的系统要求

在安装或升级 NSX 之前，请考虑您的网络配置和资源。您可以在每个 vCenter Server 中安装一个 NSX Manager，在每个 ESXi™ 主机上安装一个 Guest Introspection 和数据安全实例，并在每个数据中心安装多个 NSX Edge 实例。

硬件

表 1. 硬件要求

设备	内存	vCPU	磁盘空间
NSX Manager	16 GB (某些 NSX 部署规模为 24 GB*)	4 (某些 NSX 部署规模为 8*)	60 GB
NSX Controller	4 GB	4	20 GB
NSX Edge	<ul style="list-style-type: none"> ■ 精简: 512 MB ■ 中型: 1 GB ■ 大型: 1 GB ■ 超大型: 8 GB 	<ul style="list-style-type: none"> ■ 精简: 1 ■ 中型: 2 ■ 大型: 4 ■ 超大型: 6 	<ul style="list-style-type: none"> ■ 精简: 1 磁盘 500 MB ■ 中型: 1 磁盘 500 MB + 1 磁盘 512 MB ■ 大型: 1 磁盘 500 MB + 1 磁盘 512 MB ■ 超大型: 1 磁盘 500 MB + 1 磁盘 2 GB
Guest Introspection	1 GB	2	4 GB
NSX 数据安全	512 MB	1	每个 ESXi 主机 6 GB

作为一般准则，如果您的 NSX 受管环境包含超过 256 个管理程序或 2000 个虚拟机，您应该将 NSX Manager 资源增加到 8 个 vCPU 和 24 GB RAM。

有关特定规模的详细信息，请联系 VMware 支持人员。

有关为虚拟设备增加内存和 vCPU 分配的信息，请参见《vSphere 虚拟机管理》中的“分配内存资源”和“更改虚拟 CPU 数目”。

软件

有关互操作性的最新信息，请参见产品互操作性列表，网址为 http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php。

有关建议的 NSX、vCenter Server 和 ESXi 版本，请参见位于 <https://docs.vmware.com/cn/VMware-NSX-for-vSphere/index.html> 的发行说明。

注意，要让 NSX Manager 加入跨 vCenter NSX 部署，需要满足以下条件：

组件	版本
NSX Manager	6.2 或更高版本
NSX Controller	6.2 或更高版本

组件	版本
vCenter Server	6.0 或更高版本
ESXi	<ul style="list-style-type: none"> ESXi 6.0 或更高版本 为 NSX 6.2 或更高版本的 VIB 准备的主机群集

要从单个 vSphere Web Client 管理跨 vCenter NSX 部署中的所有 NSX Manager，必须在增强型链接模式下连接 vCenter Server。请参见《vCenter Server 和主机管理》中的“使用增强型链接模式”。

要检查合作伙伴解决方案与 NSX 的兼容性，请参见《VMware Networking and Security 兼容性指南》，网址为 <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>。

客户端和用户访问权限

- 如果按名称将 ESXi 主机添加到 vSphere 清单中，请确保正向和反向名称解析正常工作。否则，NSX Manager 将无法解析 IP 地址。
- 添加和打开虚拟机电源的权限
- 访问存储虚拟机文件的数据存储的权限，以及将文件复制到该数据存储的帐户权限
- 在 Web 浏览器中启用 cookie 以访问 NSX Manager 用户界面
- 从 NSX Manager 中，确保可以从要部署的 ESXi 主机、vCenter Server 和 NSX 设备中访问端口 443。需要使用该端口在 ESXi 主机上下载 OVF 文件以进行部署。
- 使用的 vSphere Web Client 版本支持的 Web 浏览器。请参见《vCenter Server 和主机管理》文档中的“使用 vSphere Web Client”以了解详细信息。

NSX 所需的端口和协议

以下端口必须处于打开状态才能使 NSX 正常工作。

表 2. NSX 所需的端口和协议

源	目标	端口	协议	用途	敏感	TLS	身份验证
客户端 PC	NSX Manager	443	TCP	NSX Manager 管理接口	否	是	PAM 身份验证
客户端 PC	NSX Manager	80	TCP	NSX Manager VIB 访问	否	否	PAM 身份验证
ESXi 主机	vCenter Server	443	TCP	ESXi 主机准备	否	否	
vCenter Server	ESXi 主机	443	TCP	ESXi 主机准备	否	否	
ESXi 主机	NSX Manager	5671	TCP	RabbitMQ	否	是	RabbitMQ 用户/密码
ESXi 主机	NSX Controller	1234	TCP	用户方代理连接	否	是	
NSX Controller	NSX Controller	2878、2888、3888	TCP	控制器群集 - 状态同步	否	是	IPsec

表 2. NSX 所需的端口和协议 (续)

源	目标	端口	协议	用途	敏感	TLS	身份验证
NSX Controller	NSX Controller	7777	TCP	内部控制器 RPC 端口	否	是	IPsec
NSX Controller	NSX Controller	30865	TCP	控制器群集 - 状态同步	否	是	IPsec
NSX Manager	NSX Controller	443	TCP	控制器与 Manager 通信	否	是	用户/密码
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	否	是	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	否	是	
NSX Manager	ESXi 主机	443	TCP	管理和置备连接	否	是	
NSX Manager	ESXi 主机	902	TCP	管理和置备连接	否	是	
NSX Manager	DNS 服务器	53	TCP	DNS 客户端连接	否	否	
NSX Manager	DNS 服务器	53	UDP	DNS 客户端连接	否	否	
NSX Manager	Syslog 服务器	514	TCP	Syslog 连接	否	否	
NSX Manager	Syslog 服务器	514	UDP	Syslog 连接	否	否	
NSX Manager	NTP Time Server	123	TCP	NTP 客户端连接	否	是	
NSX Manager	NTP Time Server	123	UDP	NTP 客户端连接	否	是	
vCenter Server	NSX Manager	80	TCP	主机准备	否	是	
REST 客户端	NSX Manager	443	TCP	NSX Manager REST API	否	是	用户/密码
VXLAN 隧道端点 (VTEP)	VXLAN 隧道端点 (VTEP)	8472 (NSX 6.2.3 之前的默认值) 或 4789 (新安装的 NSX 6.2.3 及更高版本中的默认值)	UDP	VTEP 之间的传输网络封装	否	是	
ESXi 主机	ESXi 主机	6999	UDP	防止 VLAN LIF 上的 ARP	否	是	
ESXi 主机	NSX Manager	8301、8302	UDP	DVS 同步	否	是	

表 2. NSX 所需的端口和协议（续）

源	目标	端口	协议	用途	敏感	TLS	身份验证
NSX Manager	ESXi 主机	8301、8302	UDP	DVS 同步	否	是	
Guest Introspection 虚拟机	NSX Manager	5671	TCP	RabbitMQ	否	是	RabbitMQ 用户/密码
主 NSX Manager	辅助 NSX Manager	443	TCP	跨 vCenter NSX 通用同步服务	否	是	
主 NSX Manager	vCenter Server	443	TCP	vSphere API	否	是	
辅助 NSX Manager	vCenter Server	443	TCP	vSphere API	否	是	
主 NSX Manager	NSX 通用控制器群集	443	TCP	NSX Controller REST API	否	是	用户/密码
辅助 NSX Manager	NSX 通用控制器群集	443	TCP	NSX Controller REST API	否	是	用户/密码
ESXi 主机	NSX 通用控制器群集	1234	TCP	NSX 控制层面协议	否	是	
ESXi 主机	主 NSX Manager	5671	TCP	RabbitMQ	否	是	RabbitMQ 用户/密码
ESXi 主机	辅助 NSX Manager	5671	TCP	RabbitMQ	否	是	RabbitMQ 用户/密码

跨 vCenter NSX 和增强型链接模式的端口

如果您有一个跨 vCenter NSX 环境，并且 vCenter Server 系统处于增强型链接模式，则要从任何 vCenter Server 系统中管理任何 NSX Manager，每个 NSX Manager 设备必须具有到该环境中每个 vCenter Server 系统的所需连接。

vCloud Networking and Security 到 NSX 升级

1

本章讨论了以下主题：

- 准备 vCloud Networking and Security 到 NSX 升级
- 从 vCloud Networking and Security 5.5.x 升级到 NSX 6.2.x
- 在 vCloud Director 环境中从 vCloud Networking and Security 5.5.x 升级到 NSX

准备 vCloud Networking and Security 到 NSX 升级

为确保 NSX 升级成功，请务必查看发行说明以了解升级问题，确保使用正确的升级顺序，以及确保基础架构为升级工作做好了恰当准备。以下准则可用作升级前对照表。



小心 不支持降级：

- 请务必先备份 NSX Manager，然后再执行升级。
- 成功升级 NSX Manager 后，无法对 NSX 进行降级。

VMware 建议在您的公司定义的维护期限内完成升级工作。

以下准则可用作升级前对照表。

- 1 验证 vCloud Networking and Security 是否为 5.5 版。如果不是，请参见《vShield 安装和升级指南》5.5 版以了解升级说明。
- 2 验证是否打开了所需的所有端口。请参见 [NSX 所需的端口和协议](#)。
- 3 验证是否可以检索 vSphere Distributed Switch 的上行链路端口名称信息。请参见 <https://kb.vmware.com/kb/2129200>。
- 4 如果部署了任何 vShield Endpoint 合作伙伴服务，请在升级之前验证兼容性：
 - 在大多数情况下，可以将 vCloud Networking and Security 升级到 NSX 而不影响合作伙伴解决方案。但是，如果您的合作伙伴解决方案与要升级到的 NSX 版本不兼容，则在升级到 NSX 之前，您需要将合作伙伴解决方案升级到兼容版本。
 - 请参阅《VMware Networking and Security 兼容性指南》。请参见 <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>。
 - 请参阅合作伙伴文档以了解兼容性和升级详细信息。

- 5 如果在环境中安装了数据安全，请在升级 vShield Manager 之前将其卸载。请参见[卸载 vShield Data Security](#)。
- 6 如果将 Cisco Nexus 1000V 作为外部交换机提供程序，您必须在升级到 NSX 之前将这些网络迁移到 vSphere Distributed Switch。在安装 NSX 后，您可以将 vSphere Distributed Switch 迁移到逻辑交换机。
- 7 验证您是否具有 vShield Manager、vCenter 和其他 vCloud Networking and Security 组件的最新备份。请参见[vCloud Networking and Security 备份和还原](#)。
- 8 创建一个技术支持包。
- 9 使用 nslookup 命令确保正向和反向域名解析正常工作。
- 10 如果正在环境中使用 VUM，请确保在 vCenter 中将 bypassVumEnabled 标记设置为 true。该设置配置 EAM 以将 VIB 直接安装到 ESXi 主机中，即使安装了 VUM 以及/或者 VUM 不可用。请参见<http://kb.vmware.com/kb/2053782>。
- 11 下载并暂存升级包，并使用 md5sum 进行验证。请参见[下载 vShield Manager 到 NSX 升级包并检查 MD5](#)。
- 12 最佳做法是，保持环境中的所有操作为静默模式，直到完成了升级的所有部分。
- 13 不要关闭或删除任何 vCloud Networking and Security 组件或设备，除非要求这样做。

在将 vCloud Networking and Security 升级到 NSX 之前评估许可证需求

从 vCloud Networking and Security 升级到 NSX 时，现有的许可证将转换为 NSX for vShield Endpoint 许可证。

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

如果已部署 vCloud Networking and Security 功能（包括准备的主机、虚拟线路、vShield App 或 vShield Edge），这些功能将继续正常工作，但无法将其升级到 NSX 并且无法对其进行任何更改。

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

请参见 NSX 许可证常见问题解答 (<https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf>)。

vCloud Networking and Security 升级对运行产生的影响

vCloud Networking and Security 升级过程需要一些时间，尤其是升级 ESXi 主机时，因为此过程必须重新引导主机。您必须了解 vCloud Networking and Security 组件在升级过程中的运行状况，例如，升级部分而非全部主机时或尚未升级 NSX Edge 时的状况。

要将 vCloud Networking and Security 升级到 NSX 6.2.x，您必须按以下顺序升级 NSX 组件：

- vShield Manager
- 主机群集和虚拟线路

- vShield App
- vShield Edge
- vShield Endpoint

VMware 建议在单个中断时段内运行升级，以尽可能缩短停机时间并避免由于某些 vCloud Networking and Security 管理功能在升级过程中无法访问而给 vCloud Networking and Security 用户带来混乱。但是，如果您的站点要求导致无法在单个中断时段内完成升级，以下信息可帮助 vCloud Networking and Security 用户了解哪些功能在升级过程中可用。

vCenter 升级

如果您正在使用 vCenter 嵌入式 SSO 并且想要将 vCenter 5.5 升级到 vCenter 6.0，则 vCenter 可能会断开与 vShield Manager 的连接。如果您已使用 root 用户名向 vShield 注册 vCenter 5.5，则会出现这种情况。从 NSX 6.2 开始，使用 root 进行 vCenter 注册的做法已弃用。要解决此问题，请使用 administrator@vsphere.local 用户名重新向 vShield 注册 vCenter，而不要使用 root。

如果您正在使用外部 SSO，则不需要进行任何更改。您可以保留相同的用户名（例如 admin@mybusiness.mydomain），而且 vCenter 不会断开连接。

vShield Manager 升级

升级过程中：

- vShield Manager 配置受到阻止。vShield API 服务不可用。您不能对 vShield 配置进行任何更改。现有虚拟机通信将继续工作。新虚拟机置备操作可在 vSphere 中继续进行，但新虚拟机在 vShield Manager 升级过程中无法连接到 vShield 虚拟线路。

升级后：

- 您可以进行所有 vShield 配置更改。

主机群集升级和虚拟线路

在主机群集升级期间，将在主机上安装新的 VIB。

在 NSX 中，虚拟线路重命名为逻辑交换机。

升级过程中：

- 不会阻止 NSX Manager 上的配置更改。
- 升级针对每个群集逐一执行。如果在群集上启用了 DRS，则 DRS 会管理主机的升级顺序。

当群集中的部分 NSX 主机已升级而其他主机未升级时：

- NSX Manager 配置更改不会受到阻止。可以添加和更改逻辑网络。您可以继续在当前未进行升级的主机上置备新虚拟机。当前正在进行升级的主机将进入维护模式，因此您必须关闭虚拟机的电源或将虚拟机撤出至其他主机。您可以使用 DRS 执行此操作，也可以手动执行。

vShield App 迁移到 NSX 分布式防火墙

在主机群集升级期间，vShield App 配置将迁移到分布式防火墙。

升级过程中：

- 在进行迁移时，现有的筛选器继续正常工作。
- 在进行迁移时，不要添加或更改筛选器。

升级后：

- 检查每个已迁移的部分，以确保其按预期工作。
- 在迁移后，通过 NSX 中的“服务部署”页移除 vShield App。

vShield Edge 升级

vShield Edge 升级与主机升级不存在任何依赖关系。即使尚未升级主机，您也可以升级 vShield Edge。



小心 如果使用的 vCloud Director 版本早于 8.10，请不要升级 NSX Edge。请参见[确定是否在 vCloud Director 环境中升级 vShield Edge](#)。

升级过程中：

- 在当前正在进行升级的 vShield Edge 设备上，配置更改会受到阻止。
- 数据包转发将暂时中断。
- 可以添加和更改逻辑交换机。
- 可以继续置备新虚拟机。

升级后：

- 配置更改不会受到阻止。任何在 NSX 升级过程中引入的新功能将不可配置，直至安装了 NSX Controller 并且所有主机群集都已升级到 NSX 6.2.x 版为止。
- 在升级后，必须重新配置 L2 VPN。
- 在升级后，必须重新安装 SSL VPN 客户端。

vShield Endpoint 迁移到 Guest Introspection

在 NSX 6.x 中，vShield Endpoint 重命名为 Guest Introspection。在升级 NSX Manager 后，如果导航到**网络和安全 > 安装 > 服务部署**，Guest Introspection 服务将显示[升级](#)链接。从 vCloud Networking and Security 升级到 NSX 时，将在启用 Guest Introspection 的群集中的每个主机上部署 Guest Introspection 虚拟设备和 Guest Introspection 主机代理。

升级过程中：

- 在虚拟机发生变化（如添加虚拟机、执行 vMotion 或删除虚拟机）时，NSX 群集中的虚拟机将失去保护。

升级后：

- 在添加虚拟机、执行 vMotion 或删除虚拟机期间，将保护虚拟机。

验证 vCloud Networking and Security 工作状态

开始升级之前，请务必测试 vCloud Networking and Security 工作状态。否则，一旦升级后出现问题，您将无法确定这些问题是由升级过程导致的还是在升级过程之前便已经存在。

开始升级 vCloud Networking and Security 基础架构之前，请勿假定一切正常。请务必先进行检查。您可以将以下过程作为升级前检查表。

步骤

- 1 确定管理用户 ID 和密码。
- 2 验证所有组件的正向和反向名称解析是否正常工作。
- 3 验证您是否可以登录到所有 vSphere 和 vShield 组件。
- 4 记下 vShield Manager、vCenter Server、ESXi 和 vShield Edge 的当前版本。
- 5 验证 VXLAN 分段是否正常工作。

请务必正确设置数据包大小并包含“不分段”位。

- 在两个虚拟机（处于同一虚拟线路上，但位于两个不同的主机）之间执行 Ping 操作。
 - 从 Windows 虚拟机中：ping -l 1472 -f <dest VM>
 - 从 Linux 虚拟机中：ping -s 1472 -M do <dest VM>
- 在两个主机的 VTEP 接口之间执行 Ping 操作。
 - ping ++netstack=vxlan -d -s 1572 <dest VTEP IP>

注 要获取主机的 VTEP IP，请在该主机的**管理 > 网络 > 虚拟交换机 (Manage > Networking > Virtual Switches)**页面上查找 vmknics IP 地址。

- 6 通过从虚拟机向外执行 Ping 操作来验证南北连接。
- 7 记录 NSX Edge 设备上的 BGP 状态和 OSPF 状态。
- 8 目视检查 vShield 环境，确保所有状态指示灯均显示为绿色、正常或已部署。
- 9 验证是否已配置 syslog。
- 10 如果可能，请在升级前环境中创建一些新组件并测试其功能。
- 11 验证 netcpad 和 vsfwd 用户环境代理 (UWA) 连接。
 - 在 ESXi 主机上，运行 `esxcli network vswitch dvs vmware vxlan network list --vds-name=<VDS_name>`，并检查控制器的连接状态。
 - 在 vShield Manager 上，运行 `show tech-support save session` 命令，并搜索“5671”以确保所有主机都已连接到 vShield Manager。
- 12 （可选）如果拥有测试环境，请在升级生产环境之前测试升级和升级后功能。

将本地管理员用户迁移到 CLI 管理员用户

在 NSX 6.x 系列之前，用户管理员是本地数据库用户。自 NSX 6.0 起，用户管理员已成为 CLI 用户。为实现向后兼容性，您可以采取一些步骤来迁移管理员用户。

对于 vCloud Networking and Security 5.x 系列，CLI 中的管理员用户和 UI (VSM) 中的管理员用户是两个不同的用户。CLI 管理员用户的密码由操作系统管理，而 VSM 用户的密码由用户的本地数据库管理。更改 CLI 管理员用户的密码时，该更改不会影响 VSM 管理员用户的密码。同样，更改 VSM 管理员用户的密码时，该更改也不会影响 CLI 管理员用户的密码。

对于 NSX 6.x 系列，VSM 用户数据库已弃用。CLI 用户可以直接登录到 NSX Manager。

在升级方案中，为实现向后兼容性，管理员用户同时存在于 CLI 数据库和 Web UI 数据库中。在这种情况下，如果 CLI 用户的密码已更改，该更改不会反映在 UI 或 REST API 调用中。在 NSX 6.x 系列之前，CLI 用户无法登录到 UI 或 REST API。

在 NSX 6.x 系列的全新（首次）部署中，CLI 用户和 NSX Manager（UI 或 REST）是相同的，并且凭据也相同。

如果希望升级后的 NSX 部署像 NSX 6.x 的全新部署一样工作，您有以下两个选项可选择。

- 选项 1 - 更改管理员数据库用户的密码。

您可以使用以下 REST API 更改密码。此选项要求您知道旧密码。

PUT URI /api/2.0/services/usermgmt/user/local/<userId>

```
<userInfo>
  <userId></userId>
  <password></password>
  <fullname></fullname>
  <email></email>
  <accessControlEntry>
    <role></role>
    <resource>
      <resourceId></resourceId>
      ...
    </resource>
  </accessControlEntry>
</userInfo>
```

例如，使用 curl：

```
curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X PUT
https://<vsm-ip>/api/2.0/services/usermgmt/user/local/admin -d
'<userInfo><userId>admin</userId><password>123</password><fullname>admin</fullname><email>admin@com
pany.com</email><accessControlEntry><role>security_admin</role><resource><resourceId>datacenter-312
</resourceId></resource></accessControlEntry></userInfo>'
```

该 API 可用于更新本地用户帐户和密码。如果未提供密码，则保留现有密码。URI 中的 userId 变量应与 XML 中指定的用户 ID 相同。

- 选项 2 - 移除 Web UI 管理员用户并向 CLI 管理员用户添加一个角色。完成此更改后，您可以使用 CLI 用户凭据登录到 NSX Manager，而且对 CLI 管理员用户进行的密码更改会反映在 NSX Manager 管理员用户上。

由于 Web UI 管理员用户是 `super_user`，因此您需要先添加另一个具有 `super_user` 特权的用户才能删除 Web UI 管理员用户。

- 添加具有 `super_user` 角色的新用户 `tempadmin`。

例如，使用 `curl`：

```
curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X PUT https://<vsm-ip>/api/2.0/services/usermgmt/user/local/admin -d '<userInfo><userId>tempadmin</userId><password>123</password><fullName>tempadmin</fullName><email>tempadmin@company.com</email><accessControlEntry><role>super_user</role><resource><resourceId>datacenter-312</resourceId></resource></accessControlEntry></userInfo>'
```

- 使用 `tempadmin` 删除 Web UI 管理员用户。

例如，使用 `curl`：

```
curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X DELETE https://<vsm-ip>/api/2.0/services/usermgmt/user/admin
```

- 向 CLI 管理员用户添加 `super_user` 角色。

例如，使用 `curl`：

```
curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X POST https://<nsx-ip>/api/2.0/services/usermgmt/role/admin?isCli=true -d '<accessControlEntry><role>super_user</role></accessControlEntry>'
```

卸载 vShield Data Security

如果在环境中安装了 Data Security，请在升级到 NSX 之前将其卸载。

从 NSX 6.2.3 开始，NSX 数据安全功能将被弃用。在 NSX 6.2.3 中，您可以自行决定继续使用该功能，但要注意，在将来的 NSX 版本中将移除该功能。

步骤

- 1 从 vShield Manager 5.5 清单面板中，展开 **数据中心 (Datacenters)** 文件夹，然后导航到安装了 vShield Data Security 的主机。
- 2 在安装了 vShield Data Security 的每个主机上，完成以下步骤以将其卸载。
 - a 单击该主机，然后在“vShield 主机准备”窗格的 **摘要 (Summary)** 选项卡中单击 vShield Data Security 的 **卸载 (Uninstall)** 链接。
 - b 在“选择要卸载的服务”窗格中，确认选择了 vShield Data Security，然后单击 **卸载 (Uninstall)** 按钮。

将卸载 vShield Data Security，并且“vShield 主机准备”窗格将状态显示为未安装。

vCloud Networking and Security 备份和还原

要在出现故障时将系统还原到工作状态，就必须正确备份所有 vCloud Networking and Security 组件，这点至关重要。

vShield Manager 备份包含所有 vShield 配置，包括虚拟线路和路由实体、安全性、vApp 规则以及在 vShield Manager UI 或 API 中配置的任何其他内容。需要单独备份 vCenter 数据库和相关的元素（如虚拟交换机）。

建议至少定期备份 vShield Manager 和 vCenter。备份频率和计划可能因业务需求和运行流程而异。建议在配置频繁更改时经常执行 vCloud Networking and Security 备份。

vShield Manager 备份可以按需执行，也可以按每小时、每日或每周的频率执行。

建议在以下情况下执行备份：

- 在 vCloud Networking and Security 或 vCenter 升级之前。
- 在 vCloud Networking and Security 或 vCenter 升级之后。
- 在执行 vCloud Networking and Security 组件零日部署和初始配置后，例如，在创建虚拟交换机、Edge、安全性和防火墙策略后。
- 基础架构或拓扑更改之后。
- 执行重大第 2 日更改之后。

要将整个系统回滚到指定时间的状态，建议将 vCloud Networking and Security 组件备份与其他交互组件（如 vCenter、云管理系统和运行工具等）的备份计划保持同步。

按需备份 vShield Manager 数据

您可以随时执行按需备份以备份 vShield Manager 数据。

步骤

- 1 从 vShield Manager 清单面板中，单击**设置和报告 (Settings & Reports)**。
- 2 单击**配置 (Configuration)**选项卡。
- 3 单击**备份 (Backups)**。
- 4 （可选）如果不希望备份系统事件表，请选中**排除系统事件 (Exclude System Events)**复选框。
- 5 （可选）如果不希望备份审核日志表，请选中**排除审核日志 (Exclude Audit Logs)**复选框。
- 6 键入保存备份的系统的主机 IP 地址 (**Host IP Address**)。
- 7 键入备份系统的主机名称 (**Host Name**)。
- 8 键入登录到备份系统所需的用户名 (**User Name**)。
- 9 键入与备份系统的用户名关联的密码 (**Password**)。
- 10 在**备份目录 (Backup Directory)**字段中，键入存储备份的绝对路径。

11 在文件名前缀 (Filename Prefix) 中键入一个文本字符串。

此文本将被预置到备份文件名中，以便在备份系统中识别这些备份文件。例如，如果键入 **ppdb**，则生成的备份的名称为 **ppdbHH_MM_SS_DayDDMonYYYY**。

12 输入密码短语 (Pass Phrase) 以确保备份文件安全。

在 vCloud Networking and Security 中，密码短语是可选的。在 NSX 中，密码短语是必需的。

13 从传输协议 (Transfer Protocol) 下拉菜单中，选择 SFTP 或 FTP。**14 单击备份 (Backup)。**

在完成后，备份将显示在该表单下方的表中。

15 单击保存设置 (Save Settings) 以保存配置。

请注意，如果所有备份保存在单个目录中，您可能在查看备份时遇到问题。最佳做法是，时常将备份文件移动到存档文件夹中。

备份 vSphere Distributed Switch

可以将 vSphere Distributed Switch 和分布式端口组配置导出到文件。

该文件保留有效的网络配置，使这些配置能够分发到其他部署。

该功能仅在 vSphere Web Client 5.1 或更高版本中可用。VDS 设置和端口组设置将作为导入内容的一部分进行导入。

最佳做法是在针对 VXLAN 为群集做好准备之前导出 VDS 配置。有关详细说明，请参见 <http://kb.vmware.com/kb/2034602>。

备份 vCenter

为保护 NSX 部署，请务必备份 vCenter 数据库并生成虚拟机快照。

请参考您使用的 vCenter 版本对应的 vCenter 文档，了解 vCenter 备份和还原步骤以及最佳做法。

有关虚拟机快照，请参见 <http://kb.vmware.com/kb/1015180>。

与 vCenter 5.5 有关的有用链接：

- <http://kb.vmware.com/kb/2057353>
- <http://kb.vmware.com/kb/2034505>
- <http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf>

与 vCenter 6.0 有关的有用链接：

- <https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html>
- <http://kb.vmware.com/kb/2110294>

下载 vShield Manager 到 NSX 升级包并检查 MD5

vShield Manager 到 NSX 升级包包含有升级 NSX 基础架构所需的所有文件。在升级 vShield Manager 之前，您需要先下载适用于要升级到的版本的升级包。

前提条件

一个 MD5 校验和工具。

步骤

- 1 将 vShield Manager 到 NSX 升级包下载到 vShield Manager 可浏览到的位置。升级包文件名称具有类似于 `VMware-vShield-Manager-upgrade-bundle-to-NSX-releaseNumber-NSXbuildNumber.tar.gz` 的格式。

- 2 验证升级文件名是否以 `tar.gz` 结尾。

部分浏览器可能会更改文件扩展名。例如，如果下载文件的名称是：

`VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.gz`

则将其更改为：

`VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.tar.gz`

否则，在上载升级包后，将显示以下错误消息：“升级包文件 `VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.gz` 无效，升级文件名称的扩展名应为 `tar.gz`”。

- 3 使用 MD5 校验和工具将 VMware 网站上显示的升级包官方 MD5 校验和与该校验和工具计算而得的 MD5 校验和相比较。
 - a 在 MD5 校验和工具中，浏览到该升级包。
 - b 使用该工具计算升级包的校验和。
 - c 粘贴 VMware 网站上列出的校验和。
 - d 使用该工具比较两个校验和。

如果两个校验和不匹配，请重复升级包下载过程。

vCloud Director 环境的其他升级准备步骤

NSX 支持 vCloud Director 网络隔离 (VCDNI)，但这是已弃用的技术。

在广泛采用 VXLAN 之前，vCloud Director 依靠 vCloud 网络隔离技术提供逻辑网络覆盖。仍然支持这种 MAC 中的 MAC 专有封装技术，但现在已停止支持该技术。与 VXLAN 逻辑网络不同，VCDNI 逻辑网络是 vCloud Director 直接创建的，vCloud Director 通过在 VMkernel 中运行的 vCloud Agent 与 ESXi 主机进行通信。因此，vCloud Networking and Security 升级对 VCDNI 网络没有任何影响，并且对将其与 NSX 一起使用没有任何限制。

不过，建议您使用 VXLAN 技术，因为 VCDNI 是已弃用的技术，仅在传统部署中支持该技术。

从 vCloud Networking and Security 5.5.x 升级到 NSX 6.2.x

要升级到 NSX 6.2.x，您必须按照本指南中介绍的顺序升级 vCloud Networking and Security 组件。

必须按照以下顺序将 vCloud Networking and Security 组件升级到 NSX：

- 1 将 vShield Manager 升级到 NSX Manager
- 2 部署 NSX Controller 群集 - 可选，对逻辑（分布式）路由器以及将控制层面模式更改为混合或单播时是必需的
- 3 更新主机群集
- 4 更新传输区域 - 可选；如果部署了 NSX Controller 群集，则可以将控制层面模式更改为混合或单播
- 5 将 vShield App 升级到 NSX 分布式防火墙
- 6 将 vShield Edge 升级到 NSX Edge
- 7 将 vShield Endpoint 升级到 NSX Guest Introspection

升级过程由 vShield Manager 管理。如果某个组件升级失败或升级中断，并且您需要重复或重新启动升级，则升级过程会从停止的位置开始，而不会从头开始。

重要 升级到 NSX Manager 后，如果您的环境中存在虚拟线路，您必须更新主机群集。

将 vShield Manager 升级到 NSX Manager

NSX 基础架构升级过程的第一步是升级 NSX Manager 设备。



小心 请不要卸载已部署的 vShield Manager 设备实例。

前提条件

- 确认已完成[准备 vCloud Networking and Security 到 NSX 升级](#)中所述的所有升级准备任务，包括检查系统要求和执行备份。
- 确认 vShield Manager 具有足够的磁盘空间以升级到 NSX Manager。请参见[NSX 的系统要求](#)。
- 在升级到 NSX 6.2.x 之前，将 vShield Manager 虚拟设备的预留内存增加到至少 16 GB 并分配 4 个 vCPU。

请参见[NSX 的系统要求](#)。

- 确认 5.5 版之前的 vShield Edge 实例（如果有）已升级到 vShield 5.5 版。

在将 vShield Manager 升级到 NSX Manager 后，无法管理或删除 5.5 之前的 vShield Edge 实例。

步骤

- 1 将 NSX 升级包下载到 vShield Manager 可以浏览到的位置。升级包文件的名称类似于 `VMware-vShield-Manager-upgrade-bundle-to-NSX-release-buildNumber.tar.gz`。

- 2 从 vShield Manager 5.5 清单面板中，单击**设置和报告**。
- 3 单击**更新**选项卡，然后单击**上载升级包**。
- 4 单击**选择文件**，选择 `VMware-vShield-Manager-upgrade-bundle-to-NSX-release-buildNumber.tar.gz` 文件，然后单击**打开**。
- 5 单击**上载文件**。
上载文件需要几分钟时间。
- 6 单击**安装**以开始升级过程。
- 7 单击**确认安装**。升级过程将重新引导 vShield Manager，因此您可能会失去与 vShield Manager 用户界面的连接。不会重新引导其他任何 vShield 组件。
- 8 在重新引导后，打开 Web 浏览器窗口并键入 IP 地址以登录到 NSX Manager 虚拟设备，例如，`https://10.10.10.10`。升级的 NSX Manager 具有与 vShield Manager 相同的 IP 地址。
“摘要”选项卡将显示刚安装的 NSX Manager 的版本。
- 9 导航到**主页 > 管理 vCenter 注册**，并确认 vCenter Server 状态为已连接。
- 10 关闭任何正在访问 vSphere Web Client 的现存浏览器会话。等待几分钟，清除浏览器缓存，然后重新登录到 vSphere Web Client。
- 11 如果已在 vShield Manager 上启用 SSH，则升级后必须也在 NSX Manager 上启用 SSH。登录到 NSX Manager 虚拟设备，然后单击**查看摘要**。在系统级别组件中，为 SSH 服务单击**开始**。

重要 从 vCloud Networking and Security 5.x 升级到 NSX 6.x 后，您必须使用 CLI 管理登录凭据登录到 NSX Manager。以前，在 vCloud Networking and Security 中需要使用两个密码，一个用于 CLI，另一个用于 UI。从 NSX 6.x 开始，只需要使用一个密码。例如：

vCloud Networking and Security 中的密码

- mypassword#123 用于 CLI
- mypassword#456 用于 UI

升级到 NSX 后的密码

- mypassword#123 用于 CLI
- mypassword#123 用于 UI

在升级 NSX Manager 后，您必须注销并重新登录到 vSphere Web Client。

如果在 vSphere Web Client 中未正确显示 NSX 插件，请清除浏览器的缓存和历史记录。如果未执行此步骤，则当您在 vSphere Web Client 中对 NSX 配置进行更改时，可能会看到类似以下内容的错误：“出现内部错误 - 错误 #1009 (An internal error has occurred - Error #1009)”。

如果在 vSphere Web Client 中不显示“网络和安全”选项卡，请重置 vSphere Web Client 服务器：

- 在 vCenter 5.5 中，打开 `https://<vcenter-ip>:5480`，然后重新启动 Web Client 服务器。

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

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

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

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

建议使用不同的 Web Client 管理运行不同 NSX Manager 版本的 vCenter Server，以避免运行不同版本的 NSX 插件时发生意外错误。

升级 NSX Manager 后，请创建新的 NSX Manager 备份文件。请参见 [NSX 备份和还原](#)。以前的 NSX Manager 备份仅对先前版本有效。

后续步骤

安装和分配 [NSX 许可证](#)。

安装和分配 NSX 许可证

在完成 NSX Manager 升级后，可以使用 vSphere Web Client 安装和分配 NSX for vSphere 许可证。

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

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

请参见 NSX 许可证常见问题解答 (<https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf>)。

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

步骤

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

- f 键入许可证密钥和新密钥的可选标签。
- g 单击**解码 (Decode)**。
对许可证密钥进行解码，以验证其格式是否正确，以及是否具有足够的容量来对资产进行授权。
- h 单击**确定 (OK)**。
- 在 vSphere 6.0 中，完成以下步骤以添加 NSX 许可证。
 - a 登录到 vSphere Web Client。
 - b 单击**系统管理 (Administration)**，然后单击**许可证 (Licenses)**。
 - c 单击**资产 (Assets)**选项卡，然后单击**解决方案 (Solutions)**选项卡。
 - d 在“解决方案”列表中，选择 NSX for vSphere。从**所有操作 (All Actions)**下拉菜单中，选择**分配许可证... (Assign license...)**。
 - e 单击**添加 (Add) (+)** 图标。输入许可证密钥，然后单击**下一步 (Next)**。添加许可证名称，然后单击**下一步 (Next)**。单击**完成 (Finish)**以添加许可证。
 - f 选择新许可证。
 - g （可选）单击**View 功能 (View Features)**图标以查看使用该许可证启用的功能。查看**容量 (Capacity)**列以查看许可证的容量。
 - h 单击**确定 (OK)**以将新许可证分配给 NSX。

后续步骤

部署 [NSX Controller 群集](#)。

如果未部署控制器，请[更新主机群集](#)。

部署 NSX Controller 群集

NSX Controller 是一个高级分布式状态管理系统，它提供了控制层面功能以实现 NSX 逻辑交换和路由功能。它充当网络内所有逻辑交换机的中央控制点，并维护所有主机、逻辑交换机 (VXLAN) 和分布式逻辑路由器的相关信息。如果您计划部署 1) 分布式逻辑路由器或 2) 单播或混合模式下的 VXLAN，则需要控制器。

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

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

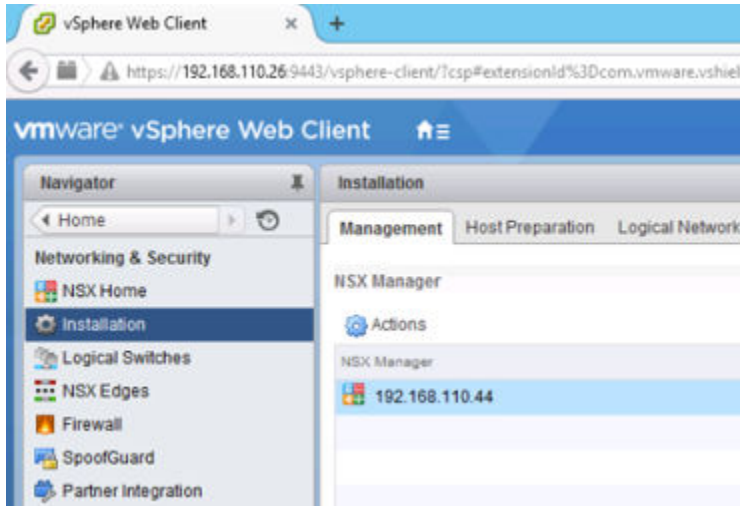
前提条件

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

步骤

- 1 在 vCenter 中，导航到主页 > 网络和安全 > 安装，然后选择管理选项卡。

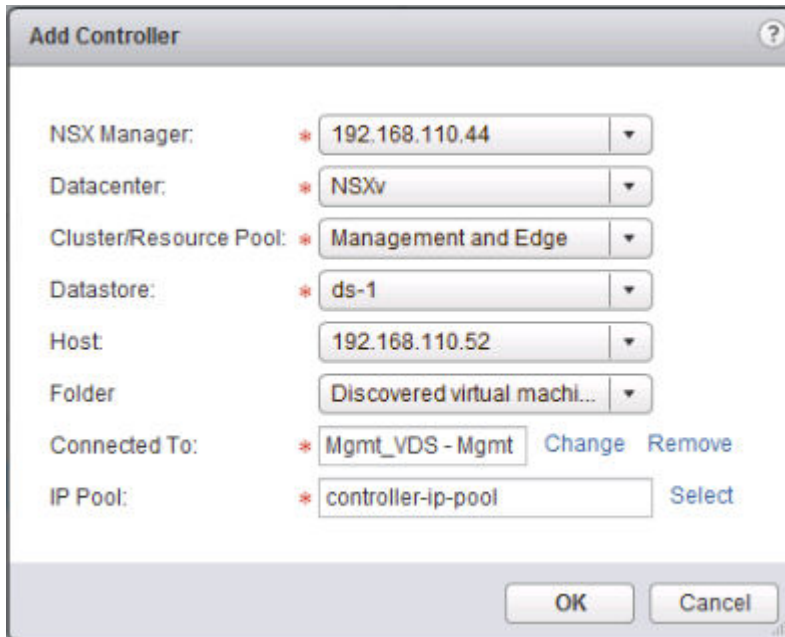
例如：



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

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

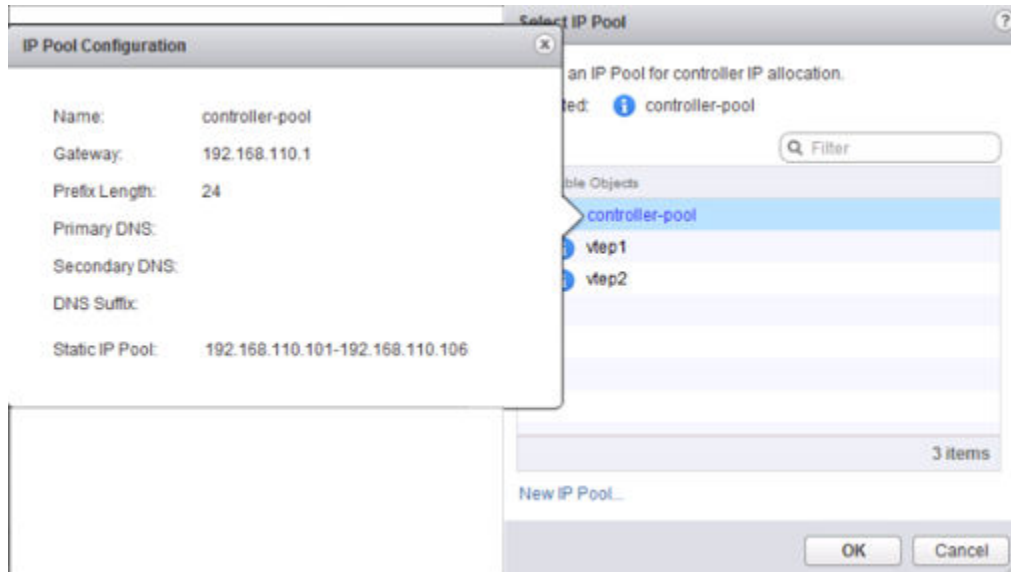
例如：



- 4 如果尚未为您的控制器群集配置 IP 池，请立即通过单击**新建 IP 池**配置一个。

如果需要，单个控制器可以位于单独的 IP 子网中。

例如：



- 5 键入并再次键入控制器的密码。

注 密码中不得包含用户名作为子字符串。任何字符不得连续重复 3 次或以上。

该密码必须至少为 12 个字符，且必须遵循以下 4 个规则中的 3 个：

- 至少一个大写字母
- 至少一个小写字母
- 至少一个数字
- 至少一个特殊字符

- 6 在完全部署第一个控制器后，部署其他两个控制器。

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

后续步骤

更新主机群集

更新主机群集

您必须在每个群集级别为每个 vCenter Server 安装网络基础架构组件，以便准备环境以进行网络虚拟化。这会在群集中的所有主机上部署所需的软件，并将虚拟线路重命名为 NSX 逻辑交换机。在此过程中，群集中的每个主机会接收软件更新，然后重新引导。

如果在您的环境中具有虚拟线路，在升级到 NSX Manager 后，您必须更新主机群集。

建议您在数据中心维护时段更新主机群集。

如果启用了 DRS，请监控主机撤出、主机进入维护模式和主机重新引导进度。如果禁用了 DRS 或处于手动模式，必须手动完成主机撤出和重新引导。在主机准备期间，可能会出现警告，可以单击警告图标以进行查看，并在必要时单击**解决办法 (Resolve)**。

当升级正在进行时，不要部署、升级或者卸载任何服务或组件。

注 在 vCloud Networking and Security 中创建的 VTEP 使用 DHCP 或手动分配的 IP 地址，而不是 IP 池。

前提条件

- 确认 vShield Manager 已升级到 NSX Manager。
- 确认“主机准备”选项卡中的“VXLAN”列显示**已启用 (Enabled)**。
- 确认所有主机的完全限定域名 (FQDN) 均可解析。
- 如果 DRS 已禁用，请先关闭虚拟机的电源或手动对虚拟机执行 vMotion 操作，然后再开始升级。
- 如果 DRS 已启用，则正在运行的虚拟机在主机群集升级过程中会自动移动。开始升级之前，请确保 DRS 可以在您的环境中工作。
 - 确认在主机群集上启用了 DRS。
 - 确认 vMotion 正常工作。
 - 验证主机与 vCenter 的连接状态。
 - 确认每个主机群集包含至少三个 ESXi 主机。在 NSX 升级过程中，仅包含一个或两个主机的主机群集更可能出现 DRS 接入控制方面的问题。为确保 NSX 升级成功，VMware 建议每个主机群集包含至少三个主机。如果一个群集包含的主机少于三个，则建议手动撤出这些主机。

步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**安装 (Installation)**。
- 3 单击**主机准备 (Host Preparation)**选项卡。

将显示基础架构中的所有群集。

如果您在 5.5 环境中具有虚拟线路，则**安装状态 (Installation Status)**列将显示**旧版 (legacy)**、**更新 (Update)**和**卸载 (Uninstall)**。

图 1-1. 当您在 5.5 环境中具有虚拟线路时，“安装状态”将显示“更新”

Clusters & Hosts	Installation Status	Firewall	VXLAN
CL-5.5	legacy Update Uninstall	Not Enabled	Enabled
CL-5.1	legacy Update Uninstall	Not Enabled	Enabled

如果您在 5.5 环境中不具有虚拟线路，则安装状态 (Installation Status) 列将显示安装 (Install)。

图 1-2. 当您在 5.5 环境中不具有虚拟线路时，“安装状态”将显示“安装”

Clusters & Hosts	Installation Status	Firewall	VXLAN
CL-5.5	Install	Not Enabled	Enabled
CL-5.1	Install	Not Enabled	Enabled

- 对于每个群集，在“安装状态”列中选择**更新 (Update)**或**安装 (Install)**。

群集中的每个主机都会接收到此新的逻辑交换机软件。

主机升级会启动主机扫描。旧 VIB 会移除（但它们在重新引导后才完全删除）。新 VIB 会安装在备选引导分区上。要在尚未重新引导的主机上查看新 VIB，您可以运行 `esxcli software vib list --rebooting-image | grep esx` 命令。

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

如果群集启用了 DRS，DRS 将尝试以受控方式重新引导主机，这样可以让虚拟机继续运行。vMotion 会将正在运行的虚拟机移到群集中的其他主机，并将该主机置入维护模式。

如果需要手动干预才能使主机进入维护模式（例如，因为 HA 要求或 DRS 规则），则升级过程将停止，并且群集的**安装状态 (Installation Status)**将显示**未就绪 (Not Ready)**。单击 以显示错误。

手动撤出主机后，选择群集并单击**解决 (Resolve)**操作。**解决 (Resolve)**操作将尝试完成升级并重新引导群集中的所有主机。如果主机因任何原因而重新引导失败，**解决 (Resolve)**操作将暂停。在**主机和群集 (Hosts and Clusters)**视图中检查主机，确保主机已打开电源并且已连接，并确保主机不包含正在运行的虚拟机。然后重试**解决 (Resolve)**操作。

5.5 基础架构中的所有虚拟线路都会重命名 NSX 逻辑交换机，并且群集的“VXLAN”列显示已启用 (Enabled)。

确保“主机准备”选项卡中的“VXLAN”列显示已启用 (Enabled)。

当群集已更新时，**安装状态 (Installation Status)**列将显示已更新到的软件版本。

要确认主机是否已更新，请登录到群集中的主机之一并运行 `esxcli software vib list | grep esx` 命令。确保以下 VIB 已更新到预期版本。

- `esx-vsip`
- `esx-vxlan`

注 在 NSX 6.2 中，`esx-dvfilter-switch-security` VIB 包含在 `esx-vxlan` VIB 中。

如果主机升级失败，请执行以下故障排除步骤：

- 在 vCenter 上检查 ESX Agent Manager，并查找警示和错误。
- 登录到主机，检查 `/var/log/esxupdate.log` 日志文件，然后查找最近的警示和错误。
- 确保已在主机上配置了 DNS 和 NTP。

后续步骤

更改 VXLAN 端口

更改 VXLAN 端口

您可以更改用于 VXLAN 流量的端口。

在 NSX 6.2.3 及更新版本中，默认 VXLAN 端口为 4789，这是 IANA 分配的标准端口。在 NSX 6.2.3 之前，默认 VXLAN UDP 端口号为 8472。

任何新的 NSX 安装将 UDP 端口 4789 用于 VXLAN。

如果是从 NSX 6.2.2 或更早版本升级到 NSX 6.2.3 或更新版本，并且安装在升级之前使用旧的默认端口号 (8472) 或自定义端口号（如 8888），则在升级后将继续使用该端口，除非您对其进行了更改。

如果您的升级安装使用或将使用硬件 VTEP 网关（ToR 网关），则必须切换到 VXLAN 端口 4789。

跨 vCenter NSX 不要求将 4789 用于 VXLAN 端口，但必须将跨 vCenter NSX 环境中的所有主机配置为使用相同的 VXLAN 端口。如果切换到端口 4789，这会确保添加到跨 vCenter NSX 环境中的任何新 NSX 安装使用与现有 NSX 部署相同的端口。

更改 VXLAN 端口是通过一个包含三个阶段的过程完成的，并且不会中断 VXLAN 流量。

- 1 NSX Manager 将所有主机配置为同时侦听新旧端口上的 VXLAN 流量。主机继续在旧端口上发送 VXLAN 流量。
- 2 NSX Manager 将所有主机配置为在新端口上发送流量。
- 3 NSX Manager 将所有主机配置为停止侦听旧端口，所有流量均通过新端口发送和接收。

在跨 vCenter NSX 环境中，您必须在主 NSX Manager 上启动端口更改。对于每个阶段，在对跨 vCenter NSX 环境中的所有主机进行配置更改之后，才会继续下一阶段的操作。

前提条件

- 确认防火墙未阻止要用于 XLAN 的端口。
- 确认在更改 VXLAN 端口时未同时运行主机准备。

步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**安装 (Installation)**。
- 3 单击**逻辑网络准备 (Logical Network Preparation)**选项卡，然后单击 **VXLAN 传输 (VXLAN Transport)**。
- 4 在“VXLAN 端口”面板中，单击**更改 (Change)**按钮。输入要切换到的端口。4789 是 IANA 为 VXLAN 分配的端口。

将端口更改传播到所有主机需要很短的时间。

- 5 （可选）使用 GET `/api/2.0/vdn/config/vxlan/udp/port/taskStatus` API 请求检查端口更改进度。

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>PHASE_TW0</taskPhase>
  <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

...

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>FINISHED</taskPhase>
  <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

后续步骤

[更新传输区域和逻辑交换机。](#)

更新传输区域和逻辑交换机

如果部署 NSX Controller 群集，您不需要在逻辑网络中依靠多播功能。您可以将传输区域和逻辑交换机上的控制层面模式更新为单播或混合。

更改控制层面模式和迁移现有的逻辑交换机对网络数据层面流量没有任何影响。

步骤

- 1 在 vSphere Web Client 中，导航到主页 (**Home**) > **网络和安全 (Networking & Security)** > **安装 (Installation)** > **逻辑网络准备 (Logical Network Preparation)** > **传输区域 (Transport Zones)**。

2 选择您的传输区域，然后单击**操作 (Actions) > 编辑设置 (Edit Settings)**。选择所需的复制模式。

- **多播 (Multicast)**: 物理网络中的多播 IP 地址用于控制层面。仅在您从较旧的 VXLAN 部署升级时才推荐使用该模式。在物理网络中需要 PIM/IGMP。
- **单播 (Unicast)**: 控制层面由 NSX Controller 处理。所有单播流量都利用优化的头端复制。不需要任何多播 IP 地址或特殊的网络配置。
- **混合 (Hybrid)**: 将本地流量复制卸载到物理网络 (L2 多播)。这在第一个跃点交换机上需要 IGMP 侦听，并且需要在每个 VTEP 子网中访问 IGMP 查询器，但是不需要 PIM。第一个跃点交换机将处理该子网的流量复制。

3 选中**将现有逻辑交换机迁移到新控制层面模式 (Migrate existing Logical Switches to the new control plane mode)**复选框，然后单击**确定 (OK)**。

后续步骤

将 [vShield App](#) 升级到 [Distributed Firewall](#)。

将 vShield App 升级到 Distributed Firewall

您只能从 vShield App 5.5 版升级到 Distributed Firewall。如果在基础架构中具有以前版本的 vShield App，必须先升级到 5.5 版，然后再升级到 6.2.x 版。有关升级到 5.5 版的信息，请参见《vShield 安装和升级指南》5.5 版。

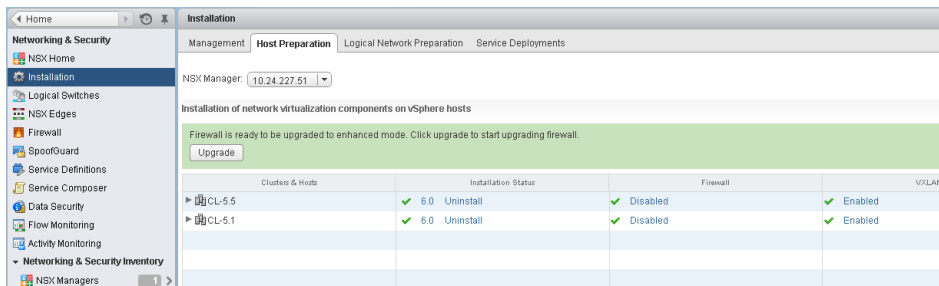
以下过程的持续时间取决于环境中的规则数。从 vShield App 迁移到 NSX Distributed Firewall（增强模式）时，将迁移并推送这些规则。这会导致流量中断。应在维护时段内完成该工作。

前提条件

- vShield Manager 已升级到 NSX Manager。
- 虚拟线路已升级到 NSX 逻辑交换机。对于非 VXLAN 用户，已安装网络虚拟化组件。
- 如果要将 vShield App 5.5 规则迁移到 Distributed Firewall，请在升级到 Distributed Firewall 之前不要删除 vShield App 设备。

步骤

1 在环境中为网络虚拟化组件准备所有群集后，将显示一条消息以指示已准备好升级 Firewall。



2 单击升级 (Upgrade)。

vShield App 5.5 规则将通过以下方式迁移到 NSX：

- a 在中央防火墙表中为 vShield App 5.5 版中配置的每个命名空间（数据中心和虚拟线路）创建新的部分。每个部分包含相应的防火墙规则。
- b 各个部分中的所有规则在 **AppliedTo** 中都具有相同的值 - 数据中心 ID 用于数据中心命名空间，虚拟线路 ID 用于虚拟线路命名空间，而端口组 ID 用于基于端口组的命名空间。
- c 在不同命名空间级别创建的容器将移动到全局级别。
- d 部分顺序如下所示，以确保更新后的防火墙规则保持相同：

```

Section_Namespace_Portgroup-1
.....
Section_Namespace_Portgroup-N
Section_Namespace_VirtualWire-1
.....
Section_Namespace_VirtualWire-N
Section_Namespace_Datacenter_1
.....
Section_Namespace_Datacenter_N
Default_Section_DefaultRule
  
```

完成升级后，“防火墙”列显示已启用 (Enabled)。

- 3 单击**主页 (Home) > 主机和群集 (Hosts and Clusters)**，然后导航到运行 vShield App 服务虚拟机的主机。关闭旧版 vShield App 服务虚拟机。
- 4 导航到**网络和安全 (Networking & Security) > 防火墙 (Firewall)**，检查每个升级的部分和规则并测试其是否按预期工作。
- 5 导航到**安装 (Installation) > 服务部署 (Service Deployments)**选项卡，并确保已解决所有警报并且旧版 vShield App 服务状态显示**成功 (Succeeded)**。
- 6 如果规则正常工作，请从**服务部署 (Service Deployments)**选项卡中选择 vShield App，然后单击**删除服务部署 (Delete Service Deployment) (✖)**以删除旧版 vShield App 服务虚拟机。

后续步骤

将 [vShield Edge](#) 升级到 [NSX Edge](#)

将 vShield Edge 升级到 NSX Edge

您只能从 vShield 5.5 版升级到 NSX Edge 6.2.x。如果在基础架构中具有以前版本的 vShield Edge，必须先升级到 5.5 版，然后再升级到 6.2.x 版。有关升级到 5.5 版的信息，请参见《vShield 安装和升级指南》5.5 版。

在升级过程中，新的 Edge 虚拟设备会与现有虚拟设备部署在一起。当新的 Edge 准备就绪时，旧的 Edge 的 vNIC 会断开连接，而新的 Edge 的 vNIC 会建立连接。然后，新的 Edge 会发送无故 ARP (GARP) 数据包，更新已连接的交换机的 ARP 缓存。当部署了 HA 时，升级过程将执行两次。

此过程会暂时影响数据包转发。您可以通过将 Edge 配置为以 ECMP 模式工作来最大程度地减小该影响。

如果未启用正常重新启动，将在升级期间撤消 OSPF 邻接。

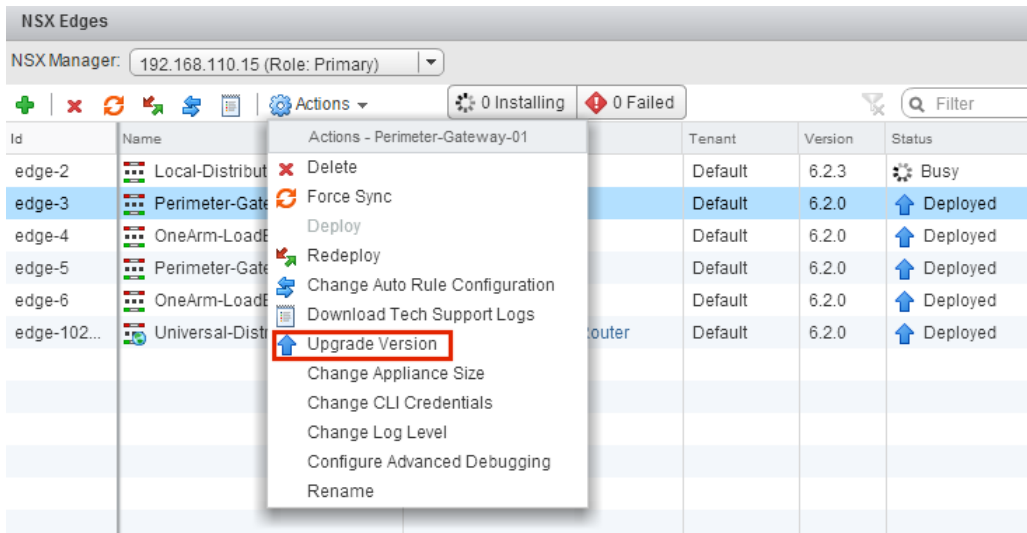
前提条件

- 确认 vShield Manager 已升级到 NSX Manager。
- 了解在进行 NSX Edge 升级时对运行产生的影响。请参见 [vCloud Networking and Security 升级对运行产生的影响](#)。
- 确认具有本地分段 ID 池，即使不打算创建 NSX 逻辑交换机。
- 确认主机具有足够的资源以在升级期间部署额外的 NSX Edge 服务网关设备，特别是在并行升级多个 NSX Edge 设备时。有关每个 NSX Edge 大小所需的资源，请参见 [NSX 的系统要求](#)。
 - 对于单个 NSX Edge 实例，在升级期间具有两个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。
 - 从 NSX 6.2.3 开始，在升级具有高可用性的 NSX Edge 实例时，将在更换旧设备之前部署两个更换设备。这意味着，在升级给定的 NSX Edge 期间，将具有四个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。在升级 NSX Edge 实例后，任一 HA 设备可能会变为活动状态。
 - 在 NSX 6.2.3 之前，在升级具有高可用性的 NSX Edge 实例时，仅在更换旧设备时部署一个更换设备。这意味着，在升级给定的 NSX Edge 期间，将具有三个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。在升级 NSX Edge 实例后，通常具有 HA 索引 0 的 NSX Edge 设备变为活动状态。
- 不支持升级启用了 L2 VPN 的 NSX Edge 版本 5.5 或 6.0。在升级之前，您必须删除 L2 VPN 配置。在升级后，您可以重新配置 L2 VPN。请参见 NSX 安装指南中的“L2 VPN 概述”。

步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。

3 对于每个 NSX Edge 实例，请在操作 (Actions) 菜单中选择升级版本 (Upgrade Version)。



如果升级失败并显示错误消息“无法部署 Edge 设备”，请确保 NSX Edge 设备部署到的主机已连接并且未处于维护模式。

在成功升级 NSX Edge 后，状态 (Status) 为“已部署”，并且版本 (Version) 列显示新的 NSX 版本。

如果 Edge 升级失败并且未回滚到旧版本，请单击重新部署 NSX Edge (Redeploy NSX Edge) 图标，然后重试升级。

NSX Edge 防火墙规则不支持 sourcePort，因此，在升级期间将按如下方式修改包含 sourcePort 的 vShield Edge 5.5 版规则。

- 如果在规则中未使用 application，将使用以下参数创建服务：protocol=any、port=any 和 sourcePort=asDefinedInTheRule。
- 如果在规则中使用了 application 或 applicationGroup，则添加 sourcePort 以复制这些分组对象。因此，将在升级后更改防火墙规则中使用的 groupingObjectId。

NSX Edge 6.x 中的用户防火墙规则不会根据 REST API 输入生成内部 IPSet 和 applicationSet，而是将它们保留原始格式。在升级期间，将使用内部生成的 IPSet 和 applicationSet 通过原始数据创建规则。内部 groupingObject 不再显示在用户 firewallRules 中。

后续步骤

如果需要，请重新配置任何 L2 VPN 配置。请参见 NSX 安装指南中的“L2 VPN 概述”。

升级 Guest Introspection

将 vShield Endpoint 升级到 NSX Guest Introspection

请务必升级 Guest Introspection 以便与 NSX Manager 版本相匹配。

注 可以从 vSphere Web Client 中升级 Guest Introspection 服务虚拟机。在升级 NSX Manager 后，您不需要删除服务虚拟机以进行升级。如果删除了服务虚拟机，服务状态将显示为失败，因为代理虚拟机丢失。单击**解决 (Resolve)**以部署新的服务虚拟机，然后单击**可升级 (Upgrade Available)**以部署最新的 Guest Introspection 服务虚拟机。

前提条件

NSX Manager、控制器、准备的主机群集和 NSX Edge 必须已升级到 6.2.x。

步骤

- 1 在**安装 (Installation)**选项卡中，单击**服务部署 (Service Deployments)**。

Installation

Management Host Preparation Logical Network Preparation **Service Deployments**

NSX Manager: 192.168.110.15 (Role: Primary)

Network & Security Service Deployments

Network & security services are deployed on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.

+ × ↺ ⬆

Filter

Service	Version	Installation Status	Service Status	Cluster	Datastore	Port Group	IP Address Range
Guest Introspection	6.2.0	Succeeded Upgrade Available	Up	Comp...	ds-site...	vds-sit...	GI Pool

安装状态 (Installation Status)列显示可升级 (Upgrade Available)。

- 2 选择要升级的 Guest Introspection 部署。

将启用服务表上方的工具栏中的**升级 (Upgrade)** (⬆) 图标。

3 单击升级 (Upgrade) (↑) 图标并按照 UI 提示进行操作。

Confirm Upgrade

Upgrade Guest Introspection service

Datastore * ds-site-a-nfs01 ▼

Network * vds-site-a_Management... ▼

IP assignment * GI Pool ▼

Specify schedule:

☒ Upgrade now

☐ Schedule the upgrade 6:29 PM ▼

OK Cancel

在升级 Guest Introspection 后，安装状态为成功，服务状态为已连接。将在 vCenter Server 清单中显示 Guest Introspection 服务虚拟机。

后续步骤

在为特定群集升级 Guest Introspection 后，您可以升级任何合作伙伴解决方案。如果启用了合作伙伴解决方案，请参阅合作伙伴提供的升级文档。即使未升级合作伙伴解决方案，也会继续提供保护。

如果将合作伙伴解决方案升级到通过 NSX 认证的版本，您必须使用服务编排以根据合作伙伴解决方案创建策略以提供保护。请参见 NSX 管理指南中的“使用服务编排”。

不支持直接升级的 NSX 服务

某些 NSX 服务（如 VMware 合作伙伴安全虚拟设备）不支持直接升级。在这些情况下，您必须卸载并重新安装这些服务。

VMware 合作伙伴安全虚拟设备

请查看合作伙伴文档，以验证合作伙伴安全虚拟设备是否可以升级。

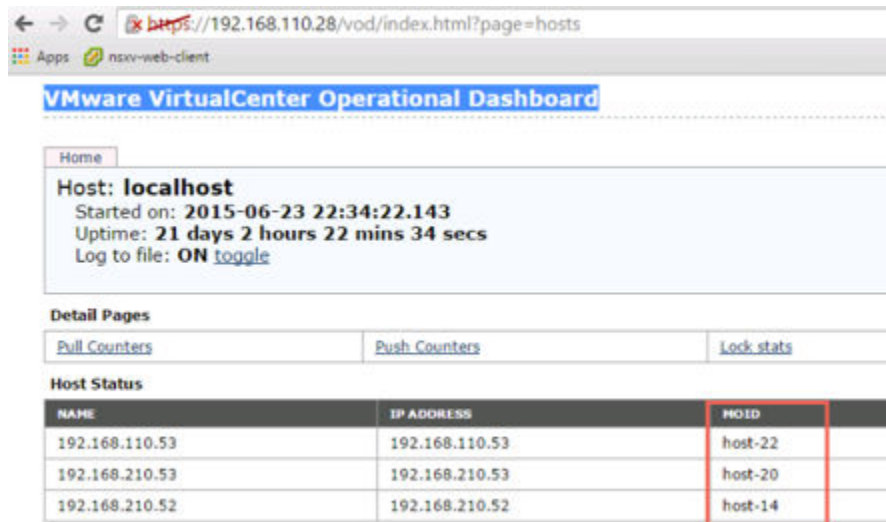
NSX 数据安全

您应该在升级 NSX 之前卸载 NSX 数据安全，并在 NSX 升级完成后重新安装 NSX 数据安全。如果您已在未先卸载 NSX 数据安全的情况下升级了 NSX，必须使用 REST API 调用卸载数据安全。

发出下面的 API 调用：

```
DELETE https://<nsx-manager-ip>/api/1.0/vshield/<host-id>/vsds
```

host-id 是 ESXi 主机的 MOID。要检索 MOID，请打开 VMware VirtualCenter 操作仪表板：<https://<vcenter-ip>/vod/index.html?page=hosts>。



对于 vCenter Server 192.168.110.28 上 MOID 为 “host-22” 的 ESXi 主机，API 调用的格式如下所示：

DELETE <https://192.168.110.28/api/1.0/vshield/host-22/vsds>

请务必在所有 ESXi 主机上发出该 API 调用。

卸载数据安全后，您可以安装新版本。请参见[安装 NSX 数据安全](#)。

NSX SSL VPN

从 NSX 6.2 开始，SSL VPN 网关只接受 TLS 协议。不过，在升级到 NSX 6.2 或更高版本后，创建的任何新客户端在建立连接期间会自动使用 TLS 协议。此外，从 NSX 6.2.3 开始，TLS 1.0 已弃用。

由于协议发生变化，在 NSX 6.0.x 客户端尝试连接到 NSX 6.2 或更高版本网关时，连接建立会在 SSL 握手阶段失败。

从 NSX 6.0.x 升级后，卸载旧 SSL VPN 客户端并安装 NSX 6.2.x 版本的 SSL VPN 客户端。请参见《NSX 管理指南》中的“在远程站点上安装 SSL 客户端”。

NSX L2 VPN

如果在 NSX Edge 版本 5.5.x 或 6.0.x 上安装了 L2 VPN，则不支持升级 NSX Edge。必须先删除任何 L2 VPN 配置，然后才能升级 NSX Edge。

安装 NSX 数据安全

注 从 NSX 6.2.3 开始，NSX 数据安全功能将被弃用。在 NSX 6.2.3 中，您可以自行决定继续使用该功能，但要注意，在将来的 NSX 版本中将移除该功能。

前提条件

必须在要安装数据安全群集的群集上安装 NSX Guest Introspection。

如果要将 IP 池中的某个 IP 地址分配给数据安全服务虚拟机，请先创建 IP 池，然后再安装数据安全。请参见《NSX 管理指南》中的“分组对象”。

步骤

- 1 在**安装 (Installation)**选项卡中，单击**服务部署 (Service Deployments)**。
- 2 单击**新建服务部署 (New Service Deployment)** (+) 图标。
- 3 在“部署网络和安全服务”对话框中，选择**数据安全 (Data Security)**，然后单击**下一步 (Next)**。
- 4 在**指定调度 (Specify schedule)**（在该对话框的底部）中，选择**立即部署 (Deploy now)**以便在安装数据安全后立即对其进行部署，或者选择部署日期和时间。
- 5 单击**下一步 (Next)**。
- 6 选择要安装数据安全的数据中心和群集，然后单击**下一步 (Next)**。
- 7 在“选择存储和管理网络”页面上，选择要添加服务虚拟机存储器的数据存储，或者选择**已在主机上指定 (Specified on host)**。

选定的数据存储在选定群集的所有主机上都必须可用。

如果选择了**已在主机上指定 (Specified on host)**，则在将数据存储添加到群集中之前，必须在主机的 **AgentVM 设置 (AgentVM Settings)** 中指定 ESX 主机的数据存储。请参见《vSphere API/SDK 文档》。

- 8 选择用于承载管理接口的分布式虚拟端口组。该端口组必须能够访问 NSX Manager 的端口组。

如果数据存储设置为**已在主机上指定 (Specified on host)**，则必须在群集内每个主机的 **agentVmNetwork** 属性中指定要使用的网络。请参见《vSphere API/SDK 文档》。

将主机添加到群集时，必须在将该主机添加到群集之前设置其 **agentVmNetwork** 属性。

选定的端口组必须在选定群集的所有主机上都可用。

- 9 在“IP 分配”中，选择以下其中的一项：

选择	目的
DHCP	通过动态主机配置协议 (DHCP) 将 IP 地址分配给数据安全服务虚拟机。
IP 池	将选定 IP 池中的某个 IP 地址分配给数据安全服务虚拟机。

请注意，不支持静态 IP 地址。

- 10 单击**下一步 (Next)**，然后在“即将完成”页面上单击**完成 (Finish)**。
- 11 监控该部署，直至**安装状态 (Installation Status)**列显示**成功 (Succeeded)**。
- 12 如果**安装状态 (Installation Status)**列显示**失败 (Failed)**，则单击“失败”旁边的图标。将显示所有部署错误。单击**解决 (Resolve)**修复这些错误。在某些情况下，解决这些错误时会显示其他错误。执行所需操作，然后重新单击**解决办法 (Resolve)**。

升级后对照表

在完成升级后，请执行以下步骤。

步骤

- 1 在升级后，创建 NSX Manager 的当前备份。
- 2 检查是否在主机上安装了 VIB。

NSX 使用以下命令安装这些 VIB：

```
esxcli software vib get --vibname esx-vxlan
esxcli software vib get --vibname esx-vsip
```

如果已安装 Guest Introspection，还要检查该 VIB 在主机上是否存在：

```
esxcli software vib get --vibname epsec-mux
```

- 3 重新同步主机消息总线。VMware 建议所有客户在升级后执行重新同步。

您可以使用以下 API 调用在每个主机上执行重新同步。

```
URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
HTTP Method : POST
```

Headers:

```
Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
```

在 vCloud Director 环境中从 vCloud Networking and Security 5.5.x 升级到 NSX

vCloud Director 版本决定了可升级到的 NSX 版本。VMware 建议升级到与环境中的其他解决方案和工具兼容的最新支持的 NSX 版本。

请参见 https://www.vmware.com/resources/compatibility/sim/interop_matrix.php 上的《VMware 产品互操作性列表》。

要升级到 NSX，您必须按照本指南中介绍的顺序升级 vCloud Networking and Security 组件。

vCloud Networking and Security 组件必须按照以下顺序进行升级：

- 1 将 vShield Manager 升级到 NSX Manager
- 2 部署 NSX Controller 群集 - 可选，对逻辑（分布式）路由器以及将控制层面模式更改为混合或单播时是必需的

- 3 更新主机群集
- 4 更新传输区域 - 可选；如果部署了 NSX Controller 群集，则可以将控制层面模式更改为混合或单播
- 5 NSX Edge - 只有在使用 vCloud Director 8.10 或更高版本时，升级到 NSX Edge。

重要 升级到 NSX Manager 后，如果您的环境中存在虚拟线路，您必须更新主机群集。

可选的 vCloud Networking and Security 组件没有与 vCloud Director 集成在一起：

- 1 vShield App - 请参见[将 vShield App 升级到 Distributed Firewall](#)。
- 2 vShield Endpoint - 请参见[将 vShield Endpoint 升级到 NSX Guest Introspection](#)。
- 3 vShield Data Security - 不支持升级。请参见[卸载说明不支持直接升级的 NSX 服务](#)和[安装说明安装 NSX 数据安全](#)。

在 vCloud Director 环境中将 vShield Manager 升级到 NSX Manager

NSX 基础架构升级过程的第一步是升级 NSX Manager 设备。



小心 请不要卸载已部署的 vShield Manager 设备实例。

前提条件

- 确认已完成[准备 vCloud Networking and Security 到 NSX 升级](#)中所述的所有升级准备任务，包括检查系统要求和执行备份。
- 确认 vShield Manager 具有足够的磁盘空间以升级到 NSX Manager。请参见[NSX 的系统要求](#)。
- 在升级到 NSX 6.2.x 之前，将 vShield Manager 虚拟设备的预留内存增加到至少 16 GB 并分配 4 个 vCPU。
请参见[NSX 的系统要求](#)。
- 确认 5.5 版之前的 vShield Edge 实例（如果有）已升级到 vShield 5.5 版。

在将 vShield Manager 升级到 NSX Manager 后，无法管理或删除 5.5 之前的 vShield Edge 实例。

步骤

- 1 将 NSX 升级包下载到 vShield Manager 可以浏览到的位置。升级包文件的名称类似于 VMware-vShield-Manager-upgrade-bundle-to-NSX-release-buildNumber.tar.gz。
- 2 从 vShield Manager 5.5 清单面板中，单击[设置和报告](#)。
- 3 单击[更新](#)选项卡，然后单击[上载升级包](#)。
- 4 单击[选择文件](#)，选择 VMware-vShield-Manager-upgrade-bundle-to-NSX-release-buildNumber.tar.gz 文件，然后单击[打开](#)。
- 5 单击[上载文件](#)。

上载文件需要几分钟时间。

- 6 单击**安装**以开始升级过程。
- 7 单击**确认安装**。升级过程将重新引导 vShield Manager，因此您可能会失去与 vShield Manager 用户界面的连接。不会重新引导其他任何 vShield 组件。
- 8 在重新引导后，打开 Web 浏览器窗口并键入 IP 地址以登录到 NSX Manager 虚拟设备，例如，<https://10.10.10.10>。升级的 NSX Manager 具有与 vShield Manager 相同的 IP 地址。
“摘要”选项卡将显示刚安装的 NSX Manager 的版本。
- 9 导航到**主页 > 管理 vCenter 注册**，并确认 vCenter Server 状态为已连接。
- 10 关闭任何正在访问 vSphere Web Client 的现存浏览器会话。等待几分钟，清除浏览器缓存，然后重新登录到 vSphere Web Client。
- 11 如果已在 vShield Manager 上启用 SSH，则升级后必须也在 NSX Manager 上启用 SSH。登录到 NSX Manager 虚拟设备，然后单击**查看摘要**。在系统级别组件中，为 SSH 服务单击**开始**。

重要 从 vCloud Networking and Security 5.x 升级到 NSX 6.x 后，您必须使用 CLI 管理登录凭据登录到 NSX Manager。以前，在 vCloud Networking and Security 中需要使用两个密码，一个用于 CLI，另一个用于 UI。从 NSX 6.x 开始，只需要使用一个密码。例如：

vCloud Networking and Security 中的密码

- mypassword#123 用于 CLI
- mypassword#456 用于 UI

升级到 NSX 后的密码

- mypassword#123 用于 CLI
- mypassword#123 用于 UI

在升级 NSX Manager 后，您必须注销并重新登录到 vSphere Web Client。

如果在 vSphere Web Client 中未正确显示 NSX 插件，请清除浏览器的缓存和历史记录。如果未执行此步骤，则当您在 vSphere Web Client 中对 NSX 配置进行更改时，可能会看到类似以下内容的错误：“出现内部错误 - 错误 #1009 (An internal error has occurred - Error #1009)”。

如果在 vSphere Web Client 中不显示“网络和安全”选项卡，请重置 vSphere Web Client 服务器：

- 在 vCenter 5.5 中，打开 <https://<vcenter-ip>:5480>，然后重新启动 Web Client 服务器。
- 在 vCenter Server Appliance 6.0 中，以 root 用户身份登录到 vCenter Server shell，然后运行以下命令：

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


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

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

建议使用不同的 Web Client 管理运行不同 NSX Manager 版本的 vCenter Server，以避免运行不同版本的 NSX 插件时发生意外错误。

升级 NSX Manager 后，请创建新的 NSX Manager 备份文件。请参见 [NSX 备份和还原](#)。以前的 NSX Manager 备份仅对先前版本有效。

后续步骤

在 vCloud Director 环境中安装和分配 NSX 许可证

在 vCloud Director 环境中安装和分配 NSX 许可证

在完成 NSX Manager 升级后，可以使用 vSphere Web Client 安装和分配 NSX for vSphere 许可证。

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

要将 NSX 与 vCloud Director 一起使用，您必须购买 NSX 许可证以涵盖所需的额外 NSX 功能，包括 NSX Edge。

请参见 NSX 许可证常见问题解答 (<https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf>)。

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

步骤

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

对许可证密钥进行解码，以验证其格式是否正确，以及是否具有足够的容量来对资产进行授权。
 - h 单击**确定 (OK)**。

- 在 vSphere 6.0 中，完成以下步骤以添加 NSX 许可证。
 - a 登录到 vSphere Web Client。
 - b 单击**系统管理 (Administration)**，然后单击许可证 (**Licenses**)。
 - c 单击**资产 (Assets)**选项卡，然后单击**解决方案 (Solutions)**选项卡。
 - d 在“解决方案”列表中，选择 NSX for vSphere。从**所有操作 (All Actions)**下拉菜单中，选择**分配许可证... (Assign license...)**。
 - e 单击**添加 (Add)** () 图标。输入许可证密钥，然后单击**下一步 (Next)**。添加许可证名称，然后单击**下一步 (Next)**。单击**完成 (Finish)**以添加许可证。
 - f 选择新许可证。
 - g （可选）单击**View 功能 (View Features)**图标以查看使用该许可证启用的功能。查看**容量 (Capacity)**列以查看许可证的容量。
 - h 单击**确定 (OK)**以将新许可证分配给 NSX。

后续步骤

在 vCloud Director 环境中为 NSX 部署 NSX Controller 群集（可选，允许您选择多播以外的控制层面模式）。

如果未部署控制器，请在 vCloud Director 环境中将主机群集从 vCNS 更新为 NSX。

在 vCloud Director 环境中为 NSX 部署 NSX Controller 群集

NSX Controller 是一个高级分布式状态管理系统，它提供了控制层面功能以实现 NSX 逻辑交换和路由功能。它充当网络内所有逻辑交换机的中央控制点，并维护所有主机、逻辑交换机 (VXLAN) 和分布式逻辑路由器的相关信息。如果您计划部署 1) 分布式逻辑路由器或 2) 单播或混合模式下的 VXLAN，则需要控制器。

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

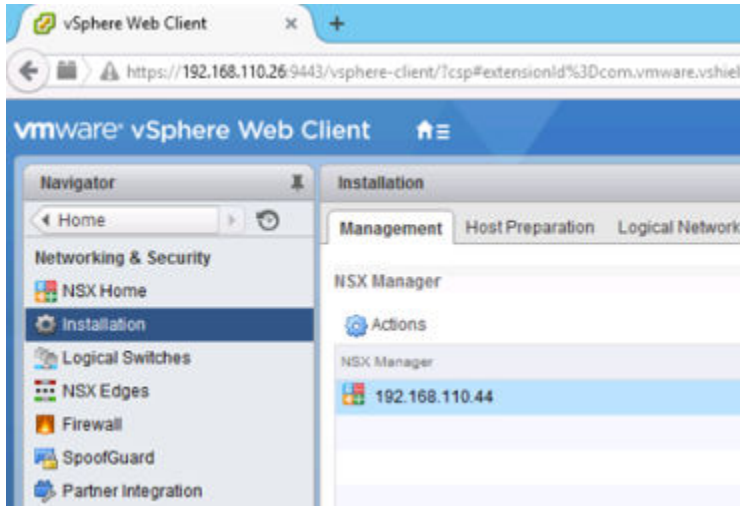
前提条件

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

步骤

- 1 在 vCenter 中，导航到主页 > 网络和安全 > 安装，然后选择管理选项卡。

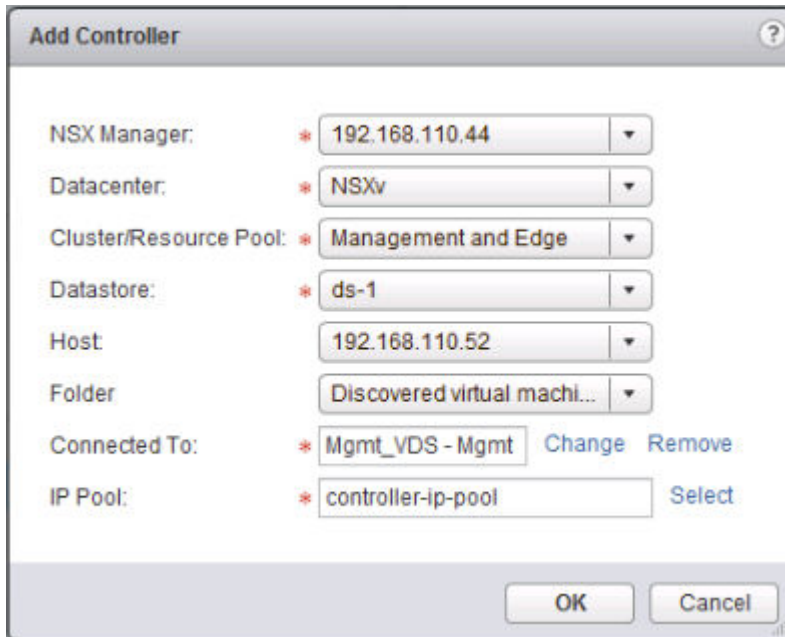
例如：



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

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

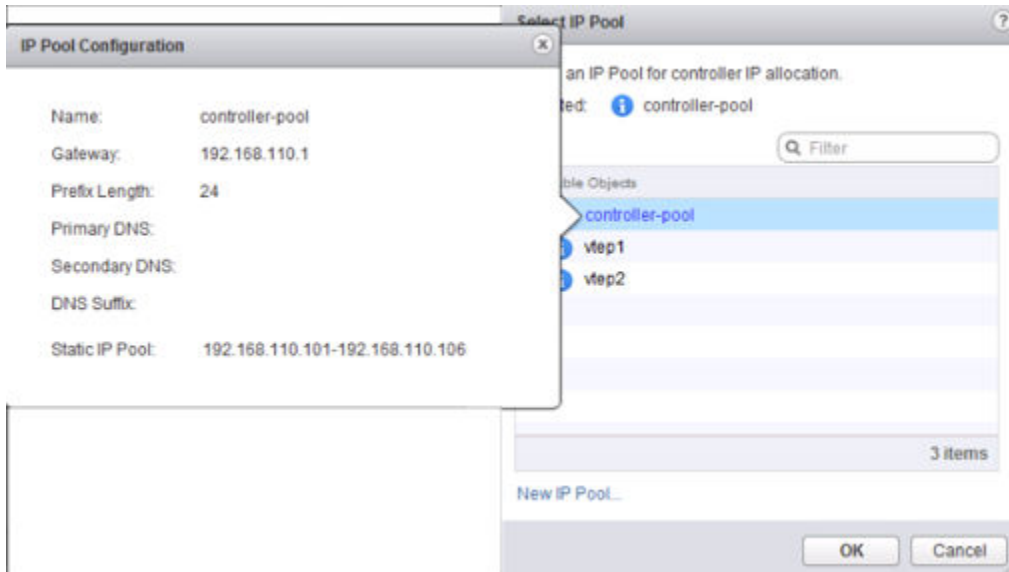
例如：



- 4 如果尚未为您的控制器群集配置 IP 池，请立即通过单击**新建 IP 池**配置一个。

如果需要，单个控制器可以位于单独的 IP 子网中。

例如：



- 5 键入并再次键入控制器的密码。

注 密码中不得包含用户名作为子字符串。任何字符不得连续重复 3 次或以上。

该密码必须至少为 12 个字符，且必须遵循以下 4 个规则中的 3 个：

- 至少一个大写字母
- 至少一个小写字母
- 至少一个数字
- 至少一个特殊字符

- 6 在完全部署第一个控制器后，部署其他两个控制器。

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

成功部署后，控制器将处于**正常**状态并显示绿色选中标记。

通过 SSH 连接到每个控制器，并确保可以 ping 主机管理接口 IP 地址。如果 ping 操作失败，请确保所有控制器都具有正确的默认网关。要查看控制器路由表，请运行 **show network routes** 命令。要更改控制器默认网关，请运行 **clear network routes** 命令，随后运行 **add network default-route <IP-address>** 命令。

运行以下命令以验证控制器群集是否按预期运行。

- **show control-cluster status**

Type	Status	Since
Join status:	Join complete	05/04 02:36:03
Majority status:	Connected to cluster majority	05/19 23:57:23

```
Restart status: This controller can be safely restarted 05/19 23:57:12
Cluster ID: ff3ebaeb-de68-4455-a3ca-4824e31863a8
Node UUID: ff3ebaeb-de68-4455-a3ca-4824e31863a8
```

Role	Configured status	Active status
api_provider	enabled	activated
persistence_server	enabled	activated
switch_manager	enabled	activated
logical_manager	enabled	activated
directory_server	enabled	activated

对于“加入”状态，请验证控制器节点是否正在报告“加入完成”。

对于“多数”状态，请验证控制器是否已连接到群集中的多数节点。

对于群集 ID，群集中的所有控制器节点应具有相同的群集 ID。

对于“已配置”状态和“活动”状态，请验证是否所有控制器角色均已启用并激活。

■ show control-cluster roles

	Listen-IP	Master?	Last-Changed	Count
api_provider	Not configured	Yes	06/02 08:49:31	4
persistence_server	N/A	Yes	06/02 08:49:31	4
switch_manager	127.0.0.1	Yes	06/02 08:49:31	4
logical_manager	N/A	Yes	06/02 08:49:31	4
directory_server	N/A	Yes	06/02 08:49:31	4

一个控制器节点将为每个角色的主节点。在此示例中，一个节点为所有角色的主节点。

如果某个角色的主 NSX Controller 实例失败，则群集会从可用的 NSX Controller 实例中为该角色选择一个新的主实例。

NSX Controller 实例位于控制层面上，因此 NSX Controller 故障不会影响数据层面流量。

■ show control-cluster connections

role	port	listening	open conns
api_provider	api/443	Y	2
persistence_server	server/2878	Y	2
	client/2888	Y	1
	election/3888	Y	0
switch_manager	ovsmgmt/6632	Y	0
	openflow/6633	Y	0
system	cluster/7777	Y	0

此命令显示群集内部的通信状态。

控制器群集多数前导者会侦听端口 2878（如“listening”列中的“Y”所示）。其他控制器节点在端口 2878 的“listening”列中将显示短划线 (-)。

在所有 3 个控制器节点上，会侦听所有其他端口。

“open conns”列显示控制器节点与其他控制器节点之间打开的连接的数量。在 3 节点控制器群集中，控制器节点最多只有 2 个打开的连接。

后续步骤



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

如果您需要删除部署的控制器，请参见 NSX 管理指南中的“从 NSX Controller 故障恢复”。

在第一次部署 NSX Controller 节点的主机上，NSX 会启用自动虚拟机启动/关机。如果控制器节点虚拟机后来被迁移到其他主机，则新的主机可能不会启用自动虚拟机启动/关机。因此，VMware 建议您检查群集中的所有主机，以确保启用了自动虚拟机启动/关机。请参见

http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-5FE08AC7-4486-438E-AF88-80D6C7928810.html。

在 vCloud Director 环境中将主机群集从 vCNS 更新为 NSX

您必须在每个群集级别为每个 vCenter Server 安装网络基础架构组件，以便准备环境以进行网络虚拟化。这会在群集中的所有主机上部署所需的软件，并将虚拟线路重命名为 NSX 逻辑交换机。在此过程中，群集中的每个主机会接收软件更新，然后重新引导。

如果在您的环境中具有虚拟线路，在升级到 NSX Manager 后，您必须更新主机群集。

建议您在数据中心维护时段更新主机群集。

当升级正在进行时，不要部署、升级或者卸载任何服务或组件。

在安装或升级 NSX 时，它自动尝试将每个主机置于维护模式，然后重新引导该主机。在 vCloud Director 环境中，不建议这样做。

您应该在每个群集上升级 VIB，但不要单击**解决 (Resolve)**。在进入维护模式并重新引导之前，您必须在 vCloud Director 中禁用主机。

注 在 vCloud Networking and Security 中创建的 VTEP 使用 DHCP 或手动分配的 IP 地址，而不是 IP 池。

步骤

1 在 vCloud Director 环境中升级主机上的 VIB

在 vCloud Director 环境中，您必须在群集上升级 VIB 之前将 DRS 设置为“手动”，否则，NSX 尝试将主机置于维护模式。

2 在 vCloud Director 环境中安装 VIB 后手动重新引导主机

必须重新引导主机以使安装的 NSX VIB 生效。在重新引导之前，您必须在 vCloud Director 中禁用主机。这可防止 vCloud Director 在重新引导期间尝试使用这些主机。

在 vCloud Director 环境中升级主机上的 VIB

在 vCloud Director 环境中，您必须在群集上升级 VIB 之前将 DRS 设置为“手动”，否则，NSX 尝试将主机置于维护模式。

前提条件

- 确认 vShield Manager 已升级到 NSX Manager。
- 确认“主机准备”选项卡中的“VXLAN”列显示已启用 (Enabled)。
- 确认所有主机的完全限定域名 (FQDN) 均可解析。
- 开始升级之前，请确保 DRS 可以在您的环境中工作。
 - 确认在主机群集上启用了 DRS。
 - 确认 vMotion 正常工作。
 - 验证主机与 vCenter 的连接状态。
- 确认每个主机群集包含至少三个 ESXi 主机。在 NSX 升级过程中，仅包含一个或两个主机的主机群集更可能出现 DRS 接入控制方面的问题。为确保 NSX 升级成功，VMware 建议每个主机群集包含至少三个主机。如果一个群集包含的主机少于三个，则建议手动撤出这些主机。
- 如果 DRS 已启用，则正在运行的虚拟机在主机群集升级过程中会自动移动。开始升级之前，请确保 DRS 可以在您的环境中工作。
 - 确认在主机群集上启用了 DRS。
 - 确认 vMotion 正常工作。
 - 验证主机与 vCenter 的连接状态。
- 确认每个主机群集包含至少三个 ESXi 主机。在 NSX 升级过程中，仅包含一个或两个主机的主机群集更可能出现 DRS 接入控制方面的问题。为确保 NSX 升级成功，VMware 建议每个主机群集包含至少三个主机。如果一个群集包含的主机少于三个，则建议手动撤出这些主机。

步骤

- 1 在 vSphere Web Client 中，导航到主页 (Home) > 主机和群集 (Hosts and Clusters)。

- 在主机群集上将 DRS 设置为“手动”。对于安装了 vCloud Networking and Security 的所有群集，重复这些步骤。



小心 不要禁用 DRS。禁用 DRS 将会删除资源池并损坏 vCloud Director 安装。

- 选择一个群集，然后导航到**管理 (Manage) > 设置 (Settings) > vSphere DRS**。
 - 记下当前 **DRS 自动化 (DRS Automation)** 设置，因为以后将恢复该更改。
 - 单击**编辑 (Edit)**。在 **DRS 自动化 (DRS Automation)** 部分中，选择**手动 (Manual)**，然后单击**确定 (OK)**。
- 导航到**主页 (Home) > 网络和安全 (Networking & Security) > 安装 (Installation)**。
 - 单击**主机准备 (Host Preparation)** 选项卡。

将显示基础架构中的所有群集。

如果您在 5.5 环境中具有虚拟线路，则**安装状态 (Installation Status)** 列将显示旧版 (**legacy**)、更新 (**Update**) 和卸载 (**Uninstall**)。

图 1-3. 当您在 5.5 环境中具有虚拟线路时，“安装状态”将显示“更新”

Clusters & Hosts	Installation Status	Firewall	VXLAN
CL-5.5	legacy Update Uninstall	Not Enabled	Enabled
CL-5.1	legacy Update Uninstall	Not Enabled	Enabled

如果您在 5.5 环境中不具有虚拟线路，则**安装状态 (Installation Status)** 列将显示**安装 (Install)**。

图 1-4. 当您在 5.5 环境中不具有虚拟线路时，“安装状态”将显示“安装”

Clusters & Hosts	Installation Status	Firewall	VXLAN
CL-5.5	Install	Not Enabled	Enabled
CL-5.1	Install	Not Enabled	Enabled

- 对于每个群集，在“安装状态”列中选择**更新 (Update)**或**安装 (Install)**。

群集中的每个主机都会接收到此新的逻辑交换机软件。

主机升级会启动主机扫描。旧 VIB 会移除（但它们在重新引导后才完全删除）。新 VIB 会安装在备选引导分区上。要在尚未重新引导的主机上查看新 VIB，您可以运行 `esxcli software vib list --rebooting-image | grep esx` 命令。

- 监控该安装，直至**安装状态 (Installation Status)**列显示**未就绪 (Not Ready)**。

不要单击**解决 (Resolve)**。

- 导航到**主页 (Home) > 主机和群集 (Hosts and Clusters)**。

- 在主机群集上恢复 DRS 更改。对于安装了 NSX 的所有群集，重复这些步骤。

- 选择一个群集，然后导航到**管理 (Manage) > 设置 (Settings)**。
- 选择 **vSphere DRS**，然后单击**编辑 (Edit)**。在 **DRS 自动化 (DRS Automation)**部分中，选择原始 DRS 设置，然后单击**确定 (OK)**。

后续步骤

在 [vCloud Director 环境中安装 VIB](#) 后手动重新引导主机。

在 vCloud Director 环境中安装 VIB 后手动重新引导主机

必须重新引导主机以使安装的 NSX VIB 生效。在重新引导之前，您必须在 vCloud Director 中禁用主机。这可防止 vCloud Director 在重新引导期间尝试使用这些主机。

前提条件

- 确认所有主机处于**未就绪 (Not Ready)**状态。
- 确认每个 vSphere 群集具有足够的容量以暂时运行，而没有一个主机。
- 确认已启用 DRS 并且未设置为“手动”。

步骤

- 在 vCloud Director 中，禁用主机。
 - 导航到**管理和监控 (Manage & Monitor) > 主机 (Hosts)**。
 - 右键单击一个主机，然后选择**禁用主机 (Disable Host)**。
- 在 vSphere Web Client 中，导航到**主页 (Home) > 主机和群集 (Hosts and Clusters)**。
- 右键单击在 vCloud Director 中禁用的主机，然后选择**进入维护模式 (Enter Maintenance Mode)**。在“确认维护模式”对话框中，选择**将关闭电源和挂起的虚拟机移动到群集中的其他主机 (Move powered-off and suspended virtual machines to other hosts in the cluster)**，然后单击**确定 (OK)**。
- 如果并非将所有虚拟机都移动到其他主机，请手动移动这些虚拟机。
- 在主机处于维护模式后，右键单击主机，然后选择**重新引导 (Reboot)**。输入重新引导原因，然后单击**确定 (OK)**。

- 6 在备份主机后，右键单击主机，然后选择**退出维护模式 (Exit Maintenance Mode)**。
- 7 在 vCloud Director 中，启用主机。
 - a 导航到**管理和监控 (Manage & Monitor) > 主机 (Hosts)**。
 - b 右键单击主机，然后选择**启用主机 (Enable Host)**。
- 8 在 vCloud Director 中启用主机后，为下一个主机重复这些步骤。

5.5 基础架构中的所有虚拟线路都会重命名 NSX 逻辑交换机，并且群集的“VXLAN”列显示已启用 (Enabled)。

已启用 (Enabled)

当群集已更新时，**安装状态 (Installation Status)**列将显示已更新到的软件版本。

要确认主机是否已更新，请登录到群集中的主机之一并运行 `esxcli software vib list | grep esx` 命令。确保以下 VIB 已更新到预期版本。

- esx-vsip
- esx-vxlan

注 在 NSX 6.2 中，esx-dvfilter-switch-security VIB 包含在 esx-vxlan VIB 中。

如果主机升级失败，请执行以下故障排除步骤：

- 在 vCenter 上检查 ESX Agent Manager，并查找警示和错误。
- 登录到主机，检查 `/var/log/esxupdate.log` 日志文件，然后查找最近的警示和错误。
- 确保已在主机上配置了 DNS 和 NTP。

后续步骤

如果已部署 NSX Controller 群集，您可以选择更改控制层面模式：[在 vCloud Director 环境中更新传输区域和逻辑交换机](#)。

否则，[确定是否在 vCloud Director 环境中升级 vShield Edge](#)。

在 vCloud Director 环境中更新传输区域和逻辑交换机

如果部署 NSX Controller 群集，您不需要在逻辑网络中依靠多播功能。您可以将传输区域和逻辑交换机上的控制层面模式更新为单播或混合。

更改控制层面模式和迁移现有的逻辑交换机对网络数据层面流量没有任何影响。

步骤

- 1 在 vSphere Web Client 中，导航到主页 (Home) > 网络和安全 (Networking & Security) > 安装 (Installation) > 逻辑网络准备 (Logical Network Preparation) > 传输区域 (Transport Zones)。

2 选择您的传输区域，然后单击**操作 (Actions) > 编辑设置 (Edit Settings)**。选择所需的复制模式。

- **多播 (Multicast)**: 物理网络中的多播 IP 地址用于控制层面。仅在您从较旧的 VXLAN 部署升级时才推荐使用该模式。在物理网络中需要 PIM/IGMP。
- **单播 (Unicast)**: 控制层面由 NSX Controller 处理。所有单播流量都利用优化的头端复制。不需要任何多播 IP 地址或特殊的网络配置。
- **混合 (Hybrid)**: 将本地流量复制卸载到物理网络 (L2 多播)。这在第一个跃点交换机上需要 IGMP 侦听，并且需要在每个 VTEP 子网中访问 IGMP 查询器，但是不需要 PIM。第一个跃点交换机将处理该子网的流量复制。

3 选中**将现有逻辑交换机迁移到新控制层面模式 (Migrate existing Logical Switches to the new control plane mode)**复选框，然后单击**确定 (OK)**。

后续步骤

确定是否在 vCloud Director 环境中升级 vShield Edge

确定是否在 vCloud Director 环境中升级 vShield Edge

vCloud Director 版本决定了是否应升级 vShield Edge。

如果使用的 vCloud Director 版本早于 8.10，则不能升级 vShield Edge。

此外，如果使用 vCloud Director 5.x，您必须在 vCloud Director 数据库中进行配置更改以防止 vCloud Director 在重新部署时升级 Edge。请参见在 [vCloud Director 环境中禁止重新部署旧版 vShield Edge](#)。

从 vCloud Director 8.10 开始，支持 NSX Edge 6.x，您可以将 vShield Edge 升级到 NSX Edge 6.x。请参见在 [vCloud Director 环境中将 vShield Edge 升级到 NSX Edge](#)。

在 vCloud Director 环境中禁止重新部署旧版 vShield Edge

如果使用 vCloud Director 5.x，在升级到 NSX 后，您必须对数据库进行更改以防止将旧版 vShield Edge 设备部署为 NSX Edge 设备。

一定不要将旧版 Edge 服务网关升级到 VMware NSX 6.x，因为这会破坏 vCloud Director 兼容性。在重新部署 vCloud Director 上的 Edge 时，vCloud Director 5.x 将升级该 Edge。为了防止这种行为，必须在 vCloud Network and Security 迁移之前进行以下 vCloud Director 数据库更改。

有关详细信息，请参见以下 VMware 知识库文章：<http://kb.vmware.com/kb/2096351> 和 <http://kb.vmware.com/kb/2108913>。

步骤

1 登录到 vCloud Director SQL Server 数据库。

2 将以下行添加到配置表中。

```
INSERT INTO config (cat, name, value, sortorder) VALUES
('vcloud','networking.edge_version_for_vsm6.2', '5.5', 0);
```

注 如果使用 NSX 6.1，请使用 `networking.edge_version_for_vsm6.1`；如果使用 NSX 6.0，请使用 `networking.edge_version_for_vsm6.0`。

在 vCloud Director 环境中将 vShield Edge 升级到 NSX Edge

vCloud Director 8.10 支持 NSX Edge 6.x，它允许将 vShield Edge 升级到 NSX Edge。如果使用早期版本的 vCloud Director，则不支持 NSX Edge 6.x，并且不应升级 NSX Edge。

您可以使用两种方法将 vShield Edge 升级到 NSX Edge：NSX 或 vCloud Director。

要使用 vCloud Director 升级 Edge，请参见《vCloud Director 安装和升级指南》中的“升级 vCenter Server 系统、主机和 NSX Edge”。



注意 如果使用的 vCloud Director 版本早于 8.10，请不要升级 NSX Edge。

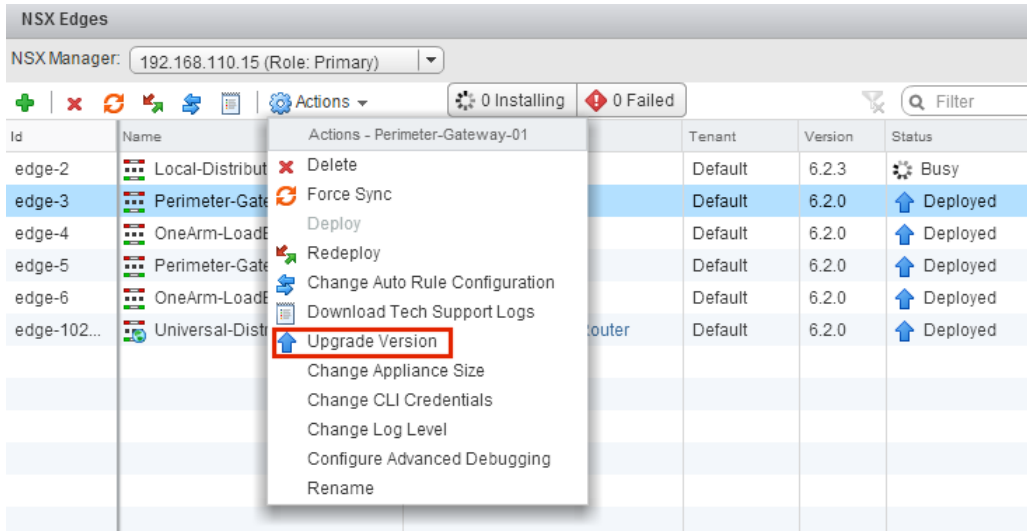
前提条件

- 确认 vShield Manager 已升级到 NSX Manager。
- 了解在进行 NSX Edge 升级时对运行产生的影响。请参见 [vCloud Networking and Security 升级对运行产生的影响](#)。
- 确认具有本地分段 ID 池，即使不打算创建 NSX 逻辑交换机。
- 确认主机具有足够的资源以在升级期间部署额外的 NSX Edge 服务网关设备，特别是在并行升级多个 NSX Edge 设备时。有关每个 NSX Edge 大小所需的资源，请参见 [NSX 的系统要求](#)。
 - 对于单个 NSX Edge 实例，在升级期间具有两个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。
 - 从 NSX 6.2.3 开始，在升级具有高可用性的 NSX Edge 实例时，将在更换旧设备之前部署两个更换设备。这意味着，在升级给定的 NSX Edge 期间，将具有四个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。在升级 NSX Edge 实例后，任一 HA 设备可能会变为活动状态。
 - 在 NSX 6.2.3 之前，在升级具有高可用性的 NSX Edge 实例时，仅在更换旧设备时部署一个更换设备。这意味着，在升级给定的 NSX Edge 期间，将具有三个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。在升级 NSX Edge 实例后，通常具有 HA 索引 0 的 NSX Edge 设备变为活动状态。
- 不支持升级启用了 L2 VPN 的 NSX Edge 版本 5.5 或 6.0。在升级之前，您必须删除 L2 VPN 配置。在升级后，您可以重新配置 L2 VPN。请参见 NSX 安装指南中的“L2 VPN 概述”。

步骤

- 1 登录到 vSphere Web Client。

- 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 对于每个 NSX Edge 实例，请在**操作 (Actions)**菜单中选择**升级版本 (Upgrade Version)**。



如果升级失败并显示错误消息“无法部署 Edge 设备”，请确保 NSX Edge 设备部署到的主机已连接并且未处于维护模式。

在成功升级 NSX Edge 后，**状态 (Status)**为“已部署”，并且**版本 (Version)**列显示新的 NSX 版本。

如果 Edge 升级失败并且未回滚到旧版本，请单击**重新部署 NSX Edge (Redeploy NSX Edge)** 图标，然后重试升级。

NSX Edge 防火墙规则不支持 **sourcePort**，因此，在升级期间将按如下方式修改包含 **sourcePort** 的 vShield Edge 5.5 版规则。

- 如果在规则中未使用 **application**，将使用以下参数创建服务：**protocol=any**、**port=any** 和 **sourcePort=asDefinedInTheRule**。
- 如果在规则中使用了 **application** 或 **applicationGroup**，则添加 **sourcePort** 以复制这些分组对象。因此，将在升级后更改防火墙规则中使用的 **groupingObjectId**。

NSX Edge 6.x 中的用户防火墙规则不会根据 REST API 输入生成内部 **IPSet** 和 **applicationSet**，而是将它们保留原始格式。在升级期间，将使用内部生成的 **IPSet** 和 **applicationSet** 通过原始数据创建规则。内部 **groupingObject** 不再显示在用户 **firewallRules** 中。

后续步骤

如果需要，请重新配置任何 L2 VPN 配置。请参见 NSX 安装指南中的“L2 VPN 概述”。

升级后对照表

在完成升级后，请执行以下步骤。

步骤

- 在升级后，创建 NSX Manager 的当前备份。

2 检查是否在主机上安装了 VIB。

NSX 使用以下命令安装这些 VIB:

```
esxcli software vib get --vibname esx-vxlan  
esxcli software vib get --vibname esx-vsip
```

如果已安装 **Guest Introspection**，还要检查该 VIB 在主机上是否存在:

```
esxcli software vib get --vibname epsec-mux
```

3 重新同步主机消息总线。VMware 建议所有客户在升级后执行重新同步。

您可以使用以下 API 调用在每个主机上执行重新同步。

```
URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>  
HTTP Method : POST
```

Headers:

```
Authorization : base64encoded value of username password  
Accept : application/xml  
Content-Type : application/xml
```

NSX 升级

本章讨论了以下主题：

- 准备 NSX 升级
- 从 NSX 6.1.x 或 6.2.x 升级到 NSX 6.2.x
- 在跨 vCenter NSX 中升级到 NSX 6.2.x

准备 NSX 升级

为确保 NSX 升级成功，请务必查看发行说明以了解升级问题，确保使用正确的升级顺序，以及确保基础架构为升级工作做好了恰当准备。



小心 不支持降级：

- 请务必先备份 NSX Manager，然后再执行升级。
- 成功升级 NSX Manager 后，无法对 NSX 进行降级。

VMware 建议在您的公司定义的维护期限内完成升级工作。

以下准则可用作升级前对照表。

- 1 验证 vCenter 是否满足 NSX 系统要求。请参见 [NSX 的系统要求](#)。
- 2 如果部署了任何 Guest Introspection 或网络可扩展性合作伙伴服务，请在升级之前验证兼容性：
 - 在大多数情况下，可以升级 NSX 而不影响合作伙伴解决方案。但是，如果您的合作伙伴解决方案与要升级到的 NSX 版本不兼容，则在升级 NSX 之前，您需要将合作伙伴解决方案升级到兼容版本。
 - 请参阅《VMware Networking and Security 兼容性指南》。请参见 <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>。
 - 请参阅合作伙伴文档以了解兼容性和升级详细信息。
- 3 如果您的环境中已安装数据安全，请在升级 NSX Manager 之前将其卸载。请参见[卸载 NSX 数据安全](#)。
- 4 计划升级使用相同 SSO 服务器的 vCenter Server 系统（包括处于增强型链接模式的 vCenter Server 系统）连接的所有 NSX Manager。如果无法升级，请参见 <https://kb.vmware.com/kb/2127061> 以了解解决办法。

- 5 验证您是否具有 NSX Manager、vCenter 和其他 NSX 组件的最新备份。请参见 [NSX 备份和还原](#)。
- 6 创建一个技术支持包。
- 7 使用 nslookup 命令确保正向和反向域名解析正常工作。
- 8 如果正在环境中使用 VUM，请确保在 vCenter 中将 bypassVumEnabled 标记设置为 true。该设置配置 EAM 以将 VIB 直接安装到 ESXi 主机中，即使安装了 VUM 以及/或者 VUM 不可用。请参见 <http://kb.vmware.com/kb/2053782>。
- 9 下载并暂存升级包，并使用 md5sum 进行验证。请参见 [下载 NSX 升级包并检查 MD5](#)。
- 10 最佳做法是，保持环境中的所有操作为静默模式，直到完成了升级的所有部分。
- 11 不要关闭或删除任何 NSX 组件或设备，除非要求这样做。

在升级 NSX 时评估许可证需求

2016 年 5 月，NSX 推出了新的许可模式。

如果具有活动支持合同，在将早期版本的 NSX 升级到 NSX 6.2.3 时，现有的许可证将转换为 NSX Enterprise 许可证，并授权您使用 Enterprise 产品中的相同功能。

请参见 NSX 许可证常见问题解答 (<https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf>)。

NSX 升级对运行产生的影响

NSX 升级过程需要一些时间，尤其是升级 ESXi 主机时，因为此过程必须重新引导主机。您必须了解 NSX 组件在升级过程中的运行状况，例如，升级部分而非全部主机时或尚未升级 NSX Edge 时的状况。

VMware 建议在单个中断时段内升级所有 NSX 组件，以尽可能缩短停机时间并避免由于某些 NSX 管理功能在升级过程中无法访问而给 NSX 用户带来混乱。但是，如果您的站点要求导致无法在单个中断时段内完成升级，以下信息可帮助 NSX 用户了解哪些功能在升级过程中可用。

NSX 部署的升级顺序如下所示：

NSX Manager —> NSX Controller 群集 —> NSX 主机群集 —> 分布式（逻辑）路由器 —> Guest Introspection

在升级 NSX Manager 后，可以随时升级 Edge 服务网关。

重要 在开始升级之前，请阅读[准备 NSX 升级](#)和《NSX for vSphere 发行说明》以了解升级必备条件和升级已知问题的详细信息。

NSX Manager 升级

NSX Manager 升级计划：

- 在跨 vCenter NSX 环境中，必须先升级主 NSX Manager，然后再升级辅助 NSX Manager。
- 在跨 vCenter NSX 环境中，必须在同一个维护时段内升级所有 NSX Manager。
- 如果从 NSX 6.1.x 升级到 NSX 6.2.x 或更高版本，您必须在相同维护时段内升级 NSX Manager 和 NSX Controller 群集。

升级 NSX Manager 过程中产生的影响：

- 使用 vSphere Web Client 和 API 的 NSX Manager 配置受到阻止。
- 现有虚拟机通信将继续工作。
- 新虚拟机置备操作可在 vSphere 中继续进行，但新虚拟机在 NSX Manager 升级过程中无法连接到 NSX 或断开与逻辑交换机的连接。
- 在跨 vCenter NSX 环境中升级 NSX Manager 时，如果主 NSX Manager 和所有辅助 NSX Manager 未完成升级，不要对通用对象进行任何更改。这包括创建、更新或删除通用对象，以及涉及通用对象的各种操作（例如，将通用安全标记应用到虚拟机）。

升级 NSX Manager 后：

- 您可以进行所有 NSX 配置更改。
- 在此阶段，如果部署了任何新的 NSX Controller 设备，它们都将使用与现有 NSX Controller 群集相匹配的版本进行部署，直到 NSX Controller 群集已升级时为止。
- 您可以对现有 NSX 配置进行更改。可以部署新的逻辑交换机、逻辑路由器和 Edge 服务网关。
- 对于分布式防火墙，如果在升级后引入了新功能，您将无法在用户界面中配置这些功能（灰显），直至所有主机都已升级为止。
- 根据 NSX 版本，在升级 NSX Manager 后，控制层面的通信通道运行状况将显示为“未知”。您必须完成控制器和主机升级才能看到“已启动”状态。

NSX Controller 群集升级

NSX Controller 升级计划：

- 您可以在升级 NSX Manager 之后升级 NSX Controller 群集。
- 在跨 vCenter NSX 环境中，必须先升级所有 NSX Manager，然后再升级 NSX Controller 群集。
- VMware 强烈建议您在升级 NSX Manager 的同一维护时段内升级 NSX Controller 群集。
- 如果从 NSX 6.1.x 升级到 NSX 6.2.x 或更高版本，您必须在相同维护时段内升级 NSX Manager 和 NSX Controller 群集。

升级 NSX Controller 过程中产生的影响：

- 逻辑网络创建和修改在升级过程中受到阻止。当 NSX Controller 群集升级正在进行时，请勿进行逻辑网络配置更改。
- 请勿在此过程中置备新虚拟机。此外，请勿在升级过程中移动虚拟机或允许 DRS 移动虚拟机。
- 在升级过程中，当出现临时的非多数状态时，现有虚拟机不会断开网络连接。
- 请勿允许在升级过程中更改动态路由。

升级 NSX Controller 后：

- 您可以进行配置更改。

NSX 主机升级

NSX 主机群集升级计划：

- 您可以在升级 NSX Manager 和 NSX Controller 群集之后升级主机群集。
- 您可以在与升级 NSX Manager 和 NSX Controller 群集不同的维护时段内升级主机群集。
- 您无需在同一个维护时段内升级所有主机群集。
- 在 NSX Manager 上安装的 NSX 版本的新功能会显示在 vSphere Web Client 和 API 中，但这些功能可能要在升级 VIB 后才可使用。
- 要利用 NSX 发行版的所有新功能，请升级主机群集，以便主机 VIB 与 NSX Manager 版本相匹配。

升级 NSX 主机群集过程中产生的影响：

- NSX Manager 上的配置更改不会受到阻止。
- 控制器到主机通信具有向后兼容性，这意味着已升级的控制器可以与未升级的主机通信。
- 升级针对每个群集逐一执行。如果在群集上启用了 DRS，则 DRS 会管理主机的升级顺序。
- 当前正在进行升级的主机必须进入维护模式，因此您必须关闭虚拟机的电源或将虚拟机撤出至其他主机。您可以使用 DRS 执行此操作，也可以手动执行。
- 可以添加和更改逻辑网络。
- 您可以继续在当前未处于维护模式的主机上置备新虚拟机。

NSX Edge 升级

NSX Edge 升级计划：

- 您可以在与其他 NSX 组件不同的维护时段内升级 NSX Edge。
- 您可以在升级 NSX Manager、NSX Controller 群集和主机群集之后升级逻辑路由器。
- 即使尚未升级 NSX Controller 群集或主机群集，也可以升级 Edge 服务网关。
- 您无需在同一个维护时段内升级所有 NSX Edge。
- 如果可以升级 NSX Edge，但尚未进行升级，则在完成 NSX Edge 升级前，将阻止在设备上执行以下操作：更改大小、资源和数据存储在，启用高级调试，以及启用 HA。

升级 NSX Edge 过程中产生的影响：

- 在当前正在进行升级的 NSX Edge 设备上，配置更改会受到阻止。可以添加和更改逻辑交换机。可以继续置备新虚拟机。
- 数据包转发将暂时中断。
- 在 NSX Edge 6.0 和更高版本中，如果未启用正常重新启动，将在升级期间撤消 OSPF 邻接。

升级 NSX Edge 后：

- 配置更改不会受到阻止。任何在 NSX 升级过程中为 Edge 服务网关引入的新功能将不可配置，直至升级所有 NSX Controller 和所有主机群集为止。

Guest Introspection 升级

Guest Introspection 升级计划：

- 您可以在升级 NSX Manager、NSX Controller 群集和主机群集后升级 Guest Introspection。
- 参见合作伙伴文档以了解合作伙伴解决方案升级信息。

升级 Guest Introspection 过程中产生的影响：

- 在虚拟机发生变化（如添加虚拟机、执行 vMotion 或删除虚拟机）时，NSX 群集中的虚拟机将失去保护。

升级 Guest Introspection 后：

- 在添加虚拟机、执行 vMotion 或删除虚拟机期间，将保护虚拟机。

验证 NSX 工作状态

开始升级之前，请务必测试 NSX 工作状态。否则，一旦升级后出现问题，您将无法确定这些问题是由升级过程导致的还是在升级过程之前便已经存在。

开始升级 NSX 基础架构之前，请勿假定一切正常。请务必先进行检查。

步骤

- 1 记下 NSX Manager、vCenter Server、ESXi 和 NSX Edge 的当前版本。
- 2 确定管理用户 ID 和密码。
- 3 验证是否可以登录到以下组件：

- vCenter Server
- NSX Manager Web UI
- Edge 服务网关设备
- 分布式逻辑路由器设备
- NSX Controller 设备

- 4 验证 VXLAN 分段是否正常工作。

请务必正确设置数据包大小并包含“不分段”位。

- 在两个虚拟机（处于同一逻辑交换机上，但位于两个不同的主机）之间执行 Ping 操作。
 - 从 Windows 虚拟机中：ping -l 1472 -f <dest VM>
 - 从 Linux 虚拟机中：ping -s 1472 -M do <dest VM>
- 在两个主机的 VTEP 接口之间执行 Ping 操作。
 - ping ++netstack=vxlan -d -s 1572 <dest VTEP IP>

注 要获取主机的 VTEP IP，请在该主机的**管理 > 网络 > 虚拟交换机 (Manage > Networking > Virtual Switches)**页面上查找 vmknics IP 地址。

- 5 通过从虚拟机向外执行 Ping 操作来验证南北连接。
- 6 目视检查 NSX 环境，确保所有状态指示灯均显示为绿色/正常/已部署。
 - 检查安装 > 管理 (Installation > Management)。
 - 检查安装 > 主机准备 (Installation > Host Preparation)。
 - 检查安装 > 逻辑网络准备 > VXLAN 传输 (Installation > Logical Network Preparation > VXLAN Transport)。
 - 检查逻辑交换机 (Logical Switches)。
 - 检查 NSX Edge (NSX Edges)。
- 7 记录 NSX Edge 设备上的 BGP 状态和 OSPF 状态。
 - `show ip ospf neighbor`
 - `show ip bgp neighbor`
 - `show ip route`
- 8 验证是否已配置 syslog。

请参见[指定 Syslog 服务器](#)。
- 9 如果可能，请在升级前环境中创建一些新组件并测试其功能。
 - 创建新的逻辑交换机。
 - 创建一个新的 Edge 服务网关和一个新的分布式逻辑路由器。
 - 将虚拟机连接到新的逻辑交换机并测试其功能。
- 10 验证 netcpad 和 vsfwd 用户环境代理 (UWA) 连接。
 - 在 ESXi 主机上，运行 `esxcli network vswitch dvs vmware vxlan network list --vds-name=<VDS_name>`，并检查控制器的连接状态。
 - 在 NSX Manager 上，运行 `show tech-support save session` 命令，并搜索“5671”以确保所有主机都已连接到 NSX Manager。
- 11 （可选）如果拥有测试环境，请在升级生产环境之前测试升级和升级后功能。

卸载 NSX 数据安全

如果您不再使用 NSX 数据安全或要升级 NSX Manager，需要卸载 NSX 数据安全。NSX 数据安全不支持直接升级。在升级 NSX Manager 之前，请务必先卸载 NSX 数据安全，并在升级完成后再重新安装。

从 NSX 6.2.3 开始，NSX 数据安全功能将被弃用。在 NSX 6.2.3 中，您可以自行决定继续使用该功能，但要注意，在将来的 NSX 版本中将移除该功能。

步骤

- 1 在**安装 (Installation)**选项卡中，单击**服务部署 (Service Deployments)**。
- 2 选择 NSX 数据安全服务，然后单击**删除服务部署 (Delete Service Deployment)** (✖) 图标。

- 3 在“确认删除”对话框中，单击**立即删除 (Delete now)**，或者选择删除生效的日期和时间。
- 4 单击**确定 (OK)**。

NSX 备份和还原

要在出现故障时将系统还原到工作状态，就必须正确备份所有 NSX 组件，这点至关重要。

NSX Manager 备份包含所有 NSX 配置，包括控制器、逻辑交换和路由实体、安全性、防火墙规则以及在 NSX Manager UI 或 API 中配置的任何其他内容。需要单独备份 vCenter 数据库和相关的元素（如虚拟交换机）。

建议至少定期备份 NSX Manager 和 vCenter。备份频率和计划可能因业务需求和运行流程而异。建议在配置频繁更改时经常执行 NSX 备份。

NSX Manager 备份可以按需执行，也可以按每小时、每日或每周的频率执行。

建议在以下情况下执行备份：

- 执行 NSX 或 vCenter 升级之前。
- 执行 NSX 或 vCenter 升级之后。
- 执行 NSX 组件零日部署和初始配置之后，例如，创建 NSX Controller、逻辑交换机、逻辑路由器、Edge 服务网关、安全策略和防火墙策略之后。
- 基础架构或拓扑更改之后。
- 执行重大第 2 日更改之后。

要将整个系统回滚到指定时间的状态，建议将 NSX 组件备份（如 NSX Manager）与其他交互组件（如 vCenter、云管理系统和运行工具等）的备份计划保持同步。

备份 NSX Manager 数据

您可以通过执行按需备份或调度备份来备份 NSX Manager 数据。

您可以通过 NSX Manager 虚拟设备 Web 界面或 NSX Manager API 配置 NSX Manager 备份和还原。备份频率可以调度为每小时、每日或每周。

备份文件保存到 NSX Manager 可访问的远程 FTP 或 SFTP 位置。NSX Manager 数据包括配置表、事件表和审核日志表。配置表包含在每个备份中。

仅支持在版本与备份版本相同的 NSX Manager 上执行还原。因此，请务必在执行 NSX 升级前后创建新的备份文件，即一个备份用于旧版本，另一个用于新版本。

步骤

- 1 登录到 NSX Manager 虚拟设备。
- 2 在“设备管理”下方，单击**备份和还原**。

3 要指定备份位置，请单击“FTP 服务器设置”旁边的**更改**。

- a 键入备份系统的 IP 地址或主机名。
- b 根据目标支持的内容，从**传输协议**下拉菜单中选择 **SFTP** 或 **FTP**。
- c 根据需要编辑默认端口。
- d 键入登录到备份系统所需的用户名和密码。
- e 在**备份目录**字段中，键入用于存储备份的绝对路径。

要确定绝对路径，您可以登录到 FTP 服务器，导航到要使用的目录，然后运行 `present working directory` 命令 (`pwd`)。例如：

```
PS C:\Users\Administrator> ftp 192.168.110.60
Connected to 192.168.110.60.
220 server-nfs FTP server ready.
User (192.168.110.60:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> ls
200 PORT command successful.
150 Opening BINARY mode data connection for 'file list'.
datastore-01
226 Transfer complete.
ftp: 22 bytes received in 0.00Seconds 22000.00Kbytes/sec.
ftp> cd datastore-01
250 CWD command successful.
ftp> pwd
257 "/datastore-01" is current directory.
```

- f 在**文件名前缀**中键入一个文本字符串。

此文本将被预置到每个备份文件名中，以便在备份系统中识别这些备份文件。例如，如果键入 **ppdb**，则生成的备份的名称为 **ppdbHH_MM_SS_DayDDMonYYYY**。

g 键入密码短语以确保备份安全。

您需要此密码才能还原备份。

h 单击**确定**。

例如：

4 对于按需备份，请单击**备份**。

新文件将添加到**备份历史记录**下。

5 对于调度备份，请单击“调度”旁边的**更改**。

a 从**备份频率**下拉菜单中，选择**按小时**、**按天**或**按周**。系统将根据所选的频率禁用“一周中的某天”、“每日时间”和“分钟”下拉菜单。例如，如果您选择“按天”，则将禁用“一周中的某天”下拉菜单，因为此字段不适用于每天频率。

b 对于按周备份，选择应该在一周中的哪一天备份数据。

c 对于按周备份或按天备份，选择开始备份的小时。

d 选择开始备份的分钟，然后单击**调度**。

6 要从备份中排除日志和流量数据，请单击“排除”旁边的**更改**。

a 选择要从备份中排除的项目。

b 单击**确定**。

7 保存 FTP 服务器的 IP/主机名、凭据、目录详细信息和密码。您需要此信息才能还原备份。

还原 NSX Manager 备份

还原 NSX Manager 会使备份文件加载到 NSX Manager 设备上。备份文件必须保存到 NSX Manager 可以访问的远程 FTP 或 SFTP 位置。NSX Manager 数据包括配置表、事件表和审核日志表。

重要 在还原备份文件前，请对您的当前数据进行备份。

前提条件

还原 NSX Manager 数据之前，建议重新安装 NSX Manager 设备。您或许也可以在现有 NSX Manager 设备上运行还原操作，但此操作未获得官方支持。前提是现有 NSX Manager 已失败，从而部署了新的 NSX Manager 设备。

最佳做法是捕获旧的 NSX Manager 设备的当前设置的屏幕截图或记下这些设置，以便可以使用这些设置来指定新部署的 NSX Manager 设备的 IP 信息和备份位置信息。

步骤

- 1 捕获屏幕截图或记下现有 NSX Manager 设备上的所有设置。
- 2 部署新的 NSX Manager 设备。
版本必须与已备份的 NSX Manager 设备相同。
- 3 登录到新的 NSX Manager 设备。
- 4 在“设备管理”下方，单击**备份和还原 (Backups & Restore)**。
- 5 在“FTP 服务器设置”中，单击**更改 (Change)**并添加设置。
“备份位置”屏幕中的**主机 IP 地址 (Host IP Address)**、**用户名 (User Name)**、**密码 (Password)**、**备份目录 (Backup Directory)**、**文件名前缀 (Filename Prefix)**和**密码短语 (Pass Phrase)**字段必须标识要还原的备份的位置。
- 6 在“备份历史记录”部分中，选中要还原的备份所对应的复选框，然后单击**还原 (Restore)**。

备份 NSX Edge

所有 NSX Edge 配置（逻辑路由器和 Edge 服务网关）都会在备份 NSX Manager 数据的过程中进行备份。

如果您设置了完整的 NSX Manager 配置，可以通过重新部署 NSX Edge（在 vSphere Web Client 中单击**重新部署 NSX Edge** 图标）来重新创建一个不可访问或失效的 Edge 设备虚拟机。

不支持创建单独的 NSX Edge 备份。

备份 vSphere Distributed Switch

可以将 vSphere Distributed Switch 和分布式端口组配置导出到文件。

该文件保留有效的网络配置，使这些配置能够分发到其他部署。

该功能仅在 vSphere Web Client 5.1 或更高版本中可用。VDS 设置和端口组设置将作为导入内容的一部分进行导入。

最佳做法是在针对 VXLAN 为群集做好准备之前导出 VDS 配置。有关详细说明，请参见 <http://kb.vmware.com/kb/2034602>。

备份 vCenter

为保护 NSX 部署，请务必备份 vCenter 数据库并生成虚拟机快照。

请参考您使用的 vCenter 版本对应的 vCenter 文档，了解 vCenter 备份和还原步骤以及最佳做法。

有关虚拟机快照，请参见 <http://kb.vmware.com/kb/1015180>。

与 vCenter 5.5 有关的有用链接：

- <http://kb.vmware.com/kb/2057353>
- <http://kb.vmware.com/kb/2034505>
- <http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf>

与 vCenter 6.0 有关的有用链接：

- <https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html>
- <http://kb.vmware.com/kb/2110294>

下载 NSX 升级包并检查 MD5

NSX 升级包包含有升级 NSX 基础架构所需的所有文件。升级 NSX Manager 之前，您需要先下载适用于要升级到的版本的升级包。

前提条件

一个 MD5 校验和工具。

步骤

- 1 将 NSX 升级包下载到 NSX Manager 可浏览到的位置。升级包文件名称具有类似于 VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz 的格式。
- 2 验证 NSX Manager 升级文件名是否以 tar.gz 结尾。

部分浏览器可能会更改文件扩展名。例如，如果下载文件的名称是：

VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx.gz

则将其更改为：

VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx.tar.gz

否则，在上载升级包后，将显示以下错误消息：“升级包文件 VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx.gz 无效，升级文件名称的扩展名应为 tar.gz”。

- 3 使用 MD5 校验和工具将 VMware 网站上显示的升级包官方 MD5 校验和与该校验和工具计算而得的 MD5 校验和相比较。
 - a 在 MD5 校验和工具中，浏览到该升级包。
 - b 使用该工具计算升级包的校验和。
 - c 粘贴 VMware 网站上列出的校验和。
 - d 使用该工具比较两个校验和。

如果两个校验和不匹配，请重复升级包下载过程。

从 NSX 6.1.x 或 6.2.x 升级到 NSX 6.2.x

要升级到 NSX 6.2.x，您必须按照本指南中介绍的顺序升级 NSX 组件。

NSX 组件必须按照以下顺序进行升级：

- 1 NSX Manager 设备
- 2 NSX Controller 群集
- 3 主机群集
- 4 NSX Edge
- 5 Guest Introspection

升级过程是由 NSX Manager 管理的。如果某个组件升级失败或升级中断，并且您需要重复或重新启动升级，则升级过程会从停止的位置开始，而不会从头开始。

每个节点的升级状态都会更新，并按群集级别显示。

升级 NSX Manager

NSX 基础架构升级过程的第一步是升级 NSX Manager 设备。

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

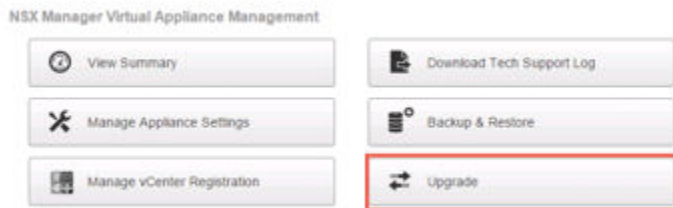
前提条件

- 验证 NSX Manager 文件系统使用率，并在文件系统使用率达到 100% 时执行清理。
 - a 登录到 NSX Manager 并运行 `show filesystems` 以显示 `/dev/sda2` 文件系统使用率。
 - b 如果使用率达到 100%，请运行 `purge log manager` 和 `purge log system` 命令。
 - c 重新引导 NSX Manager 设备以使日志清理生效。
- 在升级 NSX 6.2.x 之前，将 NSX Manager 虚拟设备的预留内存增加至 16 GB。
请参见 [NSX 的系统要求](#)。
- 如果您的环境中已安装数据安全，请在升级 NSX Manager 之前将其卸载。请参见[卸载 NSX 数据安全](#)。
- 升级之前，请备份当前配置并下载技术支持日志。请参见 [NSX 备份和还原](#)。

- 下载升级包并检查 MD5。请参见[下载 NSX 升级包并检查 MD5](#)。
- 确保您了解执行 NSX Manager 升级时升级对运行产生的影响。请参见[NSX 升级对运行产生的影响](#)。

步骤

- 1 登录到 NSX Manager 虚拟设备。
- 2 在 NSX Manager 主页上，单击**升级**。



- 3 单击**升级**，然后单击**选择文件**并浏览到 `VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz` 文件。单击**继续**以开始上载。

上载状态会显示在浏览器窗口中。

- 4 在“升级”对话框中，指定是否要启用 SSH 以及是否要参加 VMware 的客户体验改善计划（“CEIP”）。单击**升级**以开始进行升级。

将在浏览器窗口中显示升级状态。

等待升级过程完成，随后将显示 NSX Manager 登录页面。

- 5 再次登录到 NSX Manager 虚拟设备，确认升级状态是否为**完成**，并确认右上角的版本号和内部版本号是否与刚安装的升级包匹配。

在升级 NSX Manager 后，您必须注销并重新登录到 vSphere Web Client。

如果在 vSphere Web Client 中未正确显示 NSX 插件，请清除浏览器的缓存和历史记录。如果未执行此步骤，则当您在 vSphere Web Client 中对 NSX 配置进行更改时，可能会看到类似以下内容的错误：“出现内部错误 - 错误 #1009 (An internal error has occurred - Error #1009)”。

如果在 vSphere Web Client 中不显示“网络和安全”选项卡，请重置 vSphere Web Client 服务器：

- 在 vCenter 5.5 中，打开 `https://<vcenter-ip>:5480`，然后重新启动 Web Client 服务器。
- 在 vCenter Server Appliance 6.0 中，以 root 用户身份登录到 vCenter Server shell，然后运行以下命令：

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

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

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

建议使用不同的 Web Client 管理运行不同 NSX Manager 版本的 vCenter Server，以避免运行不同版本的 NSX 插件时发生意外错误。

升级 NSX Manager 后，请创建新的 NSX Manager 备份文件。请参见 [NSX 备份和还原](#)。以前的 NSX Manager 备份仅对先前版本有效。

后续步骤

升级 NSX Controller 群集。

升级 NSX Controller 群集

环境中的控制器在群集级别进行升级。如果某个控制器节点可升级，则 NSX Manager 中会显示升级链接。

建议在维护期限内升级控制器。

执行 NSX Controller 升级时，升级文件会下载到每个控制器节点。控制器会逐个进行升级。升级期间，**可升级**链接不可单击，而且系统会阻止升级控制器群集的 API 调用，直至升级已完成。

如果您在升级现有控制器之前部署新的控制器，则新的控制器会部署为旧版本。控制器节点必须具有相同版本才能加入群集。

前提条件

- 确保所有控制器都处于正常状态。当一个或多个控制器处于断开连接状态时，升级无法进行。要重新连接已断开连接的控制器，请尝试重置控制器虚拟设备。在**主机**和**群集**视图中，右键单击控制器并选择**电源 > 重置**。
- 有效的 NSX Controller 群集包含三个控制器节点。登录到这三个控制器节点，然后运行 **show controller-cluster status** 命令。

```
controller-node# show control-cluster status
```

Type	Status	Since
Join status:	Join complete	05/04 02:36:03
Majority status:	Connected to cluster majority	05/19 23:57:23
Restart status:	This controller can be safely restarted	05/19 23:57:12
Cluster ID:	ff3ebaeb-de68-4455-a3ca-4824e31863a8	
Node UUID:	ff3ebaeb-de68-4455-a3ca-4824e31863a8	
Role	Configured status	Active status
api_provider	enabled	activated

persistence_server	enabled	activated
switch_manager	enabled	activated
logical_manager	enabled	activated
directory_server	enabled	activated

- 对于“加入”状态，请验证控制器节点是否正在报告“加入完成”。
- 对于“多数”状态，请验证控制器是否已连接到群集中的多数节点。
- 对于群集 ID，群集中的所有控制器节点应具有相同的群集 ID。
- 对于“已配置”状态和“活动”状态，请验证是否所有控制器角色均已启用并激活。
- 确保您了解执行 NSX Controller 升级时升级对运行产生的影响。请参见 [NSX 升级对运行产生的影响](#)。

步骤

- ◆ 在 vSphere Web Client 中，导航至主页 > 网络和安全 > 安装，选择管理选项卡，然后单击**控制器群集**状态列中的可升级。

The screenshot shows the vSphere Web Client interface for NSX installation. The 'Management' tab is selected. Under 'NSX Managers', there is a table with one entry: IP Address 192.168.110.44, vCenter 192.168.110.28, Version 6.2.0.2860153, and Controller Cluster Status 'Upgrade Available'. Below this, the 'NSX Controller nodes' section shows a table with three nodes, all with a status of 'Normal' and 'Upgrade Status' of 'Not Started'.

NSX Manager	IP Address	vCenter	Version	Controller Cluster Status
192.168.110.44	192.168.110.44	192.168.110.28	6.2.0.2860153	Upgrade Available

Controller IP Address	ID	Status	Upgrade Status	Software Version	NSX Manager
192.168.110.201	controller-1	Normal	Not Started	6.2.4.1894	192.168.110.44
192.168.110.202	controller-2	Normal	Not Started	6.2.4.1894	192.168.110.44
192.168.110.203	controller-3	Normal	Not Started	6.2.4.1894	192.168.110.44

环境中的控制器会逐个进行升级和重新引导。启动升级后，系统首先会下载升级文件，然后升级每个控制器，接着重新引导每个控制器，最后更新每个控制器的升级状态。以下字段显示各个控制器状态：

- NSX Manager 区域中的**控制器群集状态**列显示群集的升级状态。当升级已开始时，状态显示为**正在下载升级文件**。当升级文件已下载到群集中的所有控制器时，状态会变为**正在进行中**。当群集中的所有控制器都已升级后，显示的状态是**完成**，然后此列将不再显示。
- “NSX Controller 节点”部分中的**状态**列显示每个控制器的状态，而且此状态最初显示为**正常**。当控制器服务关闭并且控制器重新引导时，状态会变为**已断开连接**。当控制器升级完成后，状态会再次变为**正常**。
- “NSX Controller 节点”部分中的**升级状态**列显示每个控制器的升级状态。状态最初显示**正在下载升级文件**，接着显示**升级正在进行中**，然后显示**正在重新引导**。控制器升级后，状态将显示**已升级**。

当升级已完成时，“NSX Controller 节点”部分中的**软件版本**列将为每个控制器显示 **6.2.buildNumber**。重新运行 **show controller-cluster status** 命令，以确保控制器能够形成多数。如果未重新形成 NSX Controller 群集多数，请查看控制器日志和 NSX Manager 日志。

每次升级的平均升级时间是 6 到 8 分钟。如果升级无法在超时期限（30 分钟）内完成，则**升级状态**列会显示**失败**。再次单击 NSX Manager 区域中的**可升级**，以从停止的位置恢复升级过程。

如果网络问题导致无法在 30 分钟的超时期限内成功完成升级，您可能需要配置更长的超时期限。与 VMWARE 支持合作，诊断并解决任何基础问题，并根据需要配置更长的超时期限。

如果控制器升级失败，请检查控制器与 NSX Manager 之间的连接。

升级时会存在以下情况，即第一个控制器升级成功，而第二个控制器升级不成功。假设某个群集包含三个控制器，并且第一个控制器已成功升级到新版本，而第二个控制器正在升级。如果第二个控制器升级失败，则该控制器可能会停留在断开连接状态。同时，第一个和第三个控制器现在具有两种不同版本（一个已升级，另一个未升级），从而无法形成多数。此时，升级无法重新启动。要解决此情况，请创建另一个控制器。新创建的控制器将具有较旧版本（与第三个控制器匹配），从而与第三个控制器形成多数。此时，您可以重新启动升级过程。

后续步骤

升级主机群集。

升级主机群集

将 NSX Manager 和 NSX Controller 升级到版本 6.2.x 后，您可以更新环境中相应的群集。在此过程中，群集中的每个主机会接收软件更新，然后重新引导。

升级主机群集会升级 NSX VIB：esx-vsip 和 esx-vxlan。

- 如果您从早于 NSX 6.2 的 NSX 版本升级，则准备好的主机将具有一个额外的 VIB：esx-dvfilter-switch-security。在 NSX 6.2 和更高版本中，esx-dvfilter-switch-security 包含在 esx-vxlan VIB 中。
- 如果您从 NSX 6.2.x（版本为 NSX 6.2.4 或更高版本）升级，则准备好的主机将具有一个额外的 VIB：esx-vgpi。

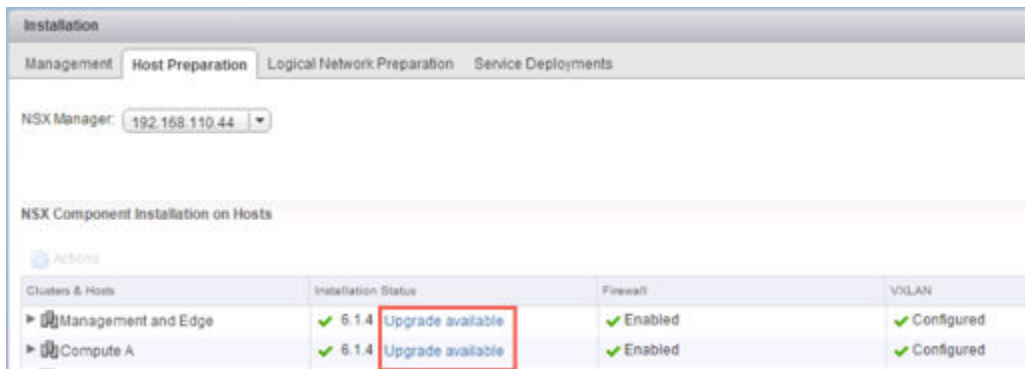
前提条件

- 确保所有主机的完全限定域名 (FQDN) 均可解析。
- 登录到群集中的主机之一，并运行 **esxcli software vib list** 命令。记录以下 VIB 的当前版本：
 - esx-vsip
 - esx-vxlan
- 升级 NSX Manager 和 NSX Controller 群集。
- 确保您了解执行主机群集升级时升级对运行产生的影响。请参阅 [NSX 升级对运行产生的影响](#)。
- 如果 DRS 已禁用，请先关闭虚拟机的电源或手动对虚拟机执行 vMotion 操作，然后再开始升级。

- 如果 DRS 已启用，则正在运行的虚拟机在主机群集升级过程中会自动移动。开始升级之前，请确保 DRS 可以在您的环境中工作。
 - 确保在主机群集上启用了 DRS。
 - 确保 vMotion 正常工作。
 - 检查主机与 vCenter 的连接状态。
- 检查每个主机群集是否包含至少三个 ESXi 主机。在 NSX 升级过程中，仅包含一个或两个主机的主机群集更可能出现 DRS 接入控制方面的问题。为确保 NSX 升级成功，VMware 建议每个主机群集包含至少三个主机。如果一个群集包含的主机少于三个，则建议手动撤出这些主机。
- 在仅包含两个或三个主机的小型群集中，如果您已创建声明某些虚拟机必须驻留在单独的主机上的反关联性规则，则这些规则可能会导致 DRS 无法在升级过程中移动虚拟机。在此情况下，请向群集添加更多主机，或者在升级过程中禁用反关联性规则，并在升级完成后重新启用这些规则。要禁用反关联性规则，请导航到**主机和群集 (Hosts and Clusters) > Cluster > 管理 (Manage) > 设置 (Settings) > 虚拟机/主机规则 (VM/Host Rules)**。编辑该规则并取消选择**启用规则 (Enable rule)**。

步骤

- 1 在 vSphere Web Client 中，导航至**主页 > 网络和安全 > 安装 (Home > Networking & Security > Installation)**，然后选择**主机准备 (Host Preparation)**选项卡。
- 2 对每个要升级的群集单击**可升级 (Upgrade available)**。



“安装状态”显示正在安装。

- 3 群集的“安装状态”显示未就绪。单击**未就绪 (Not Ready)**以显示详细信息。单击**解决所有 (Resolve all)**以尝试完成 VIB 安装。

主机将被置于维护模式并重新引导（如果需要）以完成升级。

“安装状态”列显示正在安装。在升级完成后，“安装状态”列将显示绿色对勾和升级后的 NSX 版本。

- 4 如果在启用 DRS 后**解决 (Resolve)**操作失败，主机可能需要手动干预以进入维护模式（例如，由于 HA 要求或 DRS 规则），升级过程停止，并且群集的“安装状态”再次显示未就绪。单击**未就绪 (Not Ready)**以显示详细信息。在**主机和群集 (Hosts and Clusters)**视图中检查主机，确保主机已打开电源并且已连接，并确保主机不包含正在运行的虚拟机。然后重试**解决 (Resolve)**操作。

“安装状态”列显示正在安装。在升级完成后，“安装状态”列将显示绿色对勾和升级后的 NSX 版本。

要确认主机是否已更新，请登录到群集中的主机之一并运行 `esxcli software vib list | grep esx` 命令。确保以下 VIB 已更新到预期版本。

- `esx-vsip`
- `esx-vxlan`

如果主机升级失败，请执行以下故障排除步骤：

- 在 vCenter 上检查 ESX Agent Manager，并查找警示和错误。
- 登录到主机，检查 `/var/log/esxupdate.log` 日志文件，然后查找最近的警示和错误。
- 确保已在主机上配置了 DNS 和 NTP。

有关更多故障排除步骤，请参见 NSX 故障排除指南中的“主机准备”。

后续步骤

更改 VXLAN 端口

更改 VXLAN 端口

您可以更改用于 VXLAN 流量的端口。

在 NSX 6.2.3 及更新版本中，默认 VXLAN 端口为 4789，这是 IANA 分配的标准端口。在 NSX 6.2.3 之前，默认 VXLAN UDP 端口号为 8472。

任何新的 NSX 安装将 UDP 端口 4789 用于 VXLAN。

如果是从 NSX 6.2.2 或更早版本升级到 NSX 6.2.3 或更新版本，并且安装在升级之前使用旧的默认端口号 (8472) 或自定义端口号（如 8888），则在升级后将继续使用该端口，除非您对其进行了更改。

如果您的升级安装使用或将使用硬件 VTEP 网关（ToR 网关），则必须切换到 VXLAN 端口 4789。

跨 vCenter NSX 不要求将 4789 用于 VXLAN 端口，但必须将跨 vCenter NSX 环境中的所有主机配置为使用相同的 VXLAN 端口。如果切换到端口 4789，这会确保添加到跨 vCenter NSX 环境中的任何新 NSX 安装使用与现有 NSX 部署相同的端口。

更改 VXLAN 端口是通过一个包含三个阶段的过程完成的，并且不会中断 VXLAN 流量。

- 1 NSX Manager 将所有主机配置为同时侦听新旧端口上的 VXLAN 流量。主机继续在旧端口上发送 VXLAN 流量。
- 2 NSX Manager 将所有主机配置为在新端口上发送流量。
- 3 NSX Manager 将所有主机配置为停止侦听旧端口，所有流量均通过新端口发送和接收。

在跨 vCenter NSX 环境中，您必须在主 NSX Manager 上启动端口更改。对于每个阶段，在对跨 vCenter NSX 环境中的所有主机进行配置更改之后，才会继续下一阶段的操作。

前提条件

- 确认防火墙未阻止要用于 XLAN 的端口。
- 确认在更改 VXLAN 端口时未同时运行主机准备。

步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**安装 (Installation)**。
- 3 单击**逻辑网络准备 (Logical Network Preparation)**选项卡，然后单击 **VXLAN 传输 (VXLAN Transport)**。
- 4 在“VXLAN 端口”面板中，单击**更改 (Change)**按钮。输入要切换到的端口。4789 是 IANA 为 VXLAN 分配的端口。

将端口更改传播到所有主机需要很短的时间。

- 5 （可选）使用 GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus API 请求检查端口更改进度。

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>PHASE_TW0</taskPhase>
  <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

...

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>FINISHED</taskPhase>
  <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

后续步骤

升级 NSX Edge

升级 NSX Edge

NSX Edge 升级与 NSX Controller 群集升级或主机群集升级不存在任何依赖关系。即使尚未升级 NSX Controller 群集或主机群集，您也可以升级 NSX Edge。

在升级过程中，新的 Edge 虚拟设备会与现有虚拟设备部署在一起。当新的 Edge 准备就绪时，旧的 Edge 的 vNIC 会断开连接，而新的 Edge 的 vNIC 会建立连接。然后，新的 Edge 会发送无故 ARP (GARP) 数据包，更新已连接的交换机的 ARP 缓存。当部署了 HA 时，升级过程将执行两次。

此过程会暂时影响数据包转发。您可以通过将 Edge 配置为以 ECMP 模式工作来最大程度地减小该影响。

如果未启用正常重新启动，将在升级期间撤消 OSPF 邻接。

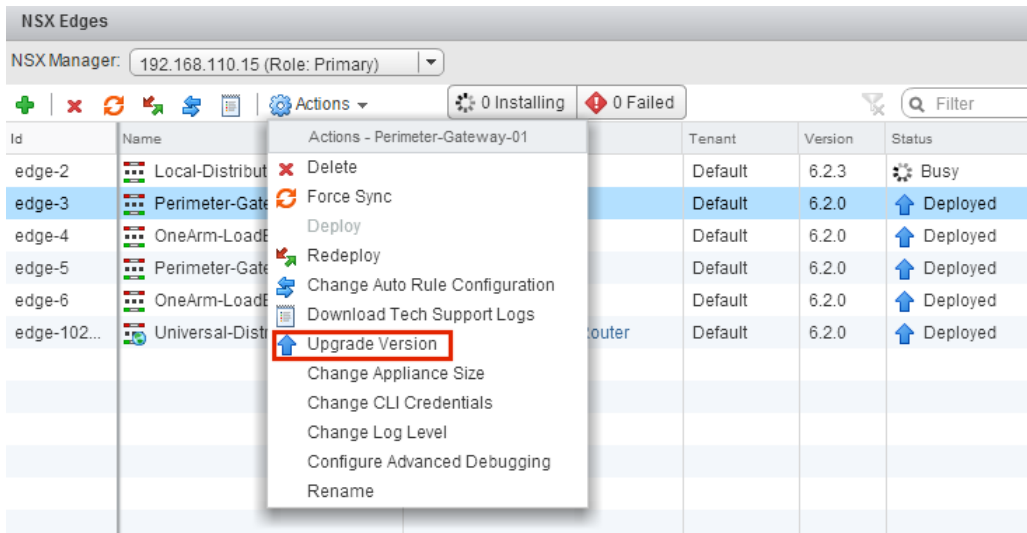
前提条件

- 确认 NSX Manager 已升级到 6.2.x。
- 确认具有本地分段 ID 池，即使不打算创建 NSX 逻辑交换机。
- 确认主机具有足够的资源以在升级期间部署额外的 NSX Edge 服务网关设备，特别是在并行升级多个 NSX Edge 设备时。有关每个 NSX Edge 大小所需的资源，请参见 [NSX 的系统要求](#)。
 - 对于单个 NSX Edge 实例，在升级期间具有两个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。
 - 从 NSX 6.2.3 开始，在升级具有高可用性的 NSX Edge 实例时，将在更换旧设备之前部署两个更换设备。这意味着，在升级给定的 NSX Edge 期间，将具有四个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。在升级 NSX Edge 实例后，任一 HA 设备可能会变为活动状态。
 - 在 NSX 6.2.3 之前，在升级具有高可用性的 NSX Edge 实例时，仅在更换旧设备时部署一个更换设备。这意味着，在升级给定的 NSX Edge 期间，将具有三个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。在升级 NSX Edge 实例后，通常具有 HA 索引 0 的 NSX Edge 设备变为活动状态。
- 了解在进行 NSX Edge 升级时对运行产生的影响。请参见 [NSX 升级对运行产生的影响](#)。
- 不支持升级启用了 L2 VPN 的 NSX Edge 版本 5.5 或 6.0。在升级之前，您必须删除 L2 VPN 配置。在升级后，您可以重新配置 L2 VPN。请参见 NSX 安装指南中的“L2 VPN 概述”。
- 如果从 NSX 6.2.x 升级到 NSX 6.2.3 并且配置了负载均衡器，请参见以下知识库文章以避免出现升级问题：<https://kb.vmware.com/kb/2145887>。

步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。

- 3 对于每个 NSX Edge 实例，请在**操作 (Actions)**菜单中选择**升级版本 (Upgrade Version)**。



如果升级失败并显示错误消息“无法部署 Edge 设备”，请确保 NSX Edge 设备部署到的主机已连接并且未处于维护模式。

在成功升级 NSX Edge 后，**状态 (Status)**为“已部署”，并且**版本 (Version)**列显示新的 NSX 版本。

如果 Edge 升级失败并且未回滚到旧版本，请单击**重新部署 NSX Edge (Redeploy NSX Edge)** 图标，然后重试升级。

后续步骤

如果需要，请重新配置任何 L2 VPN 配置。请参见 NSX 安装指南中的“L2 VPN 概述”。

升级 Guest Introspection

请务必升级 Guest Introspection 以便与 NSX Manager 版本相匹配。

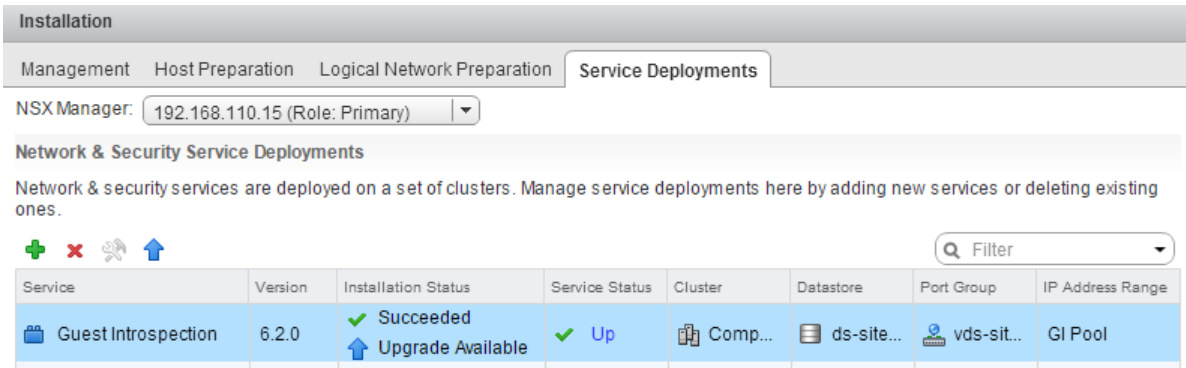
注 可以从 vSphere Web Client 中升级 Guest Introspection 服务虚拟机。在升级 NSX Manager 后，您不需要删除服务虚拟机以进行升级。如果删除了服务虚拟机，服务状态将显示为失败，因为代理虚拟机丢失。单击**解决 (Resolve)**以部署新的服务虚拟机，然后单击**可升级 (Upgrade Available)**以部署最新的 Guest Introspection 服务虚拟机。

前提条件

NSX Manager、控制器、准备的主机群集和 NSX Edge 必须已升级到 6.2.x。

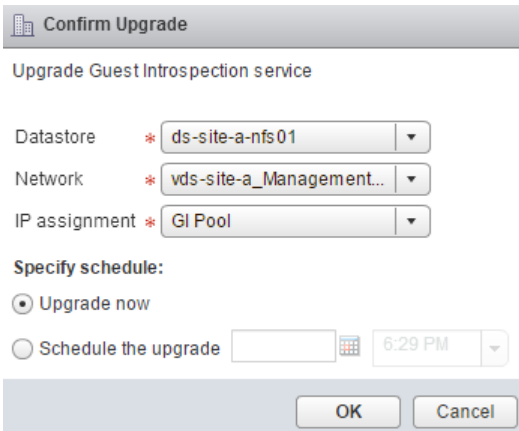
步骤

- 1 在**安装 (Installation)**选项卡中，单击**服务部署 (Service Deployments)**。



安装状态 (Installation Status)列显示可升级 (Upgrade Available)。

- 2 选择要升级的 Guest Introspection 部署。
将启用服务表上方的工具栏中的**升级 (Upgrade)** (⬆) 图标。
- 3 单击**升级 (Upgrade)** (⬆) 图标并按照 UI 提示进行操作。



在升级 Guest Introspection 后，安装状态为成功，服务状态为已连接。将在 vCenter Server 清单中显示 Guest Introspection 服务虚拟机。

在为特定群集升级 Guest Introspection 后，您可以升级任何合作伙伴解决方案。如果启用了合作伙伴解决方案，请参阅合作伙伴提供的升级文档。即使未升级合作伙伴解决方案，也会继续提供保护。

不支持直接升级的 NSX 服务

某些 NSX 服务（如 VMware 合作伙伴安全虚拟设备）不支持直接升级。在这些情况下，您必须卸载并重新安装这些服务。

VMware 合作伙伴安全虚拟设备

请查看合作伙伴文档，以验证合作伙伴安全虚拟设备是否可以升级。

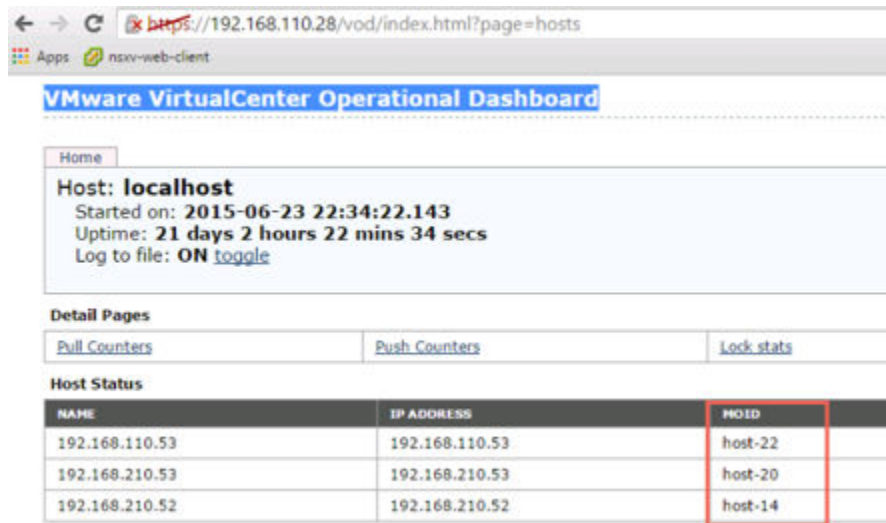
NSX 数据安全

您应该在升级 NSX 之前卸载 NSX 数据安全，并在 NSX 升级完成后重新安装 NSX 数据安全。如果您已在未先卸载 NSX 数据安全的情况下升级了 NSX，必须使用 REST API 调用卸载数据安全。

发出下面的 API 调用：

DELETE `https://<nsx-manager-ip>/api/1.0/vshield/<host-id>/vsds`

host-id 是 ESXi 主机的 MOID。要检索 MOID，请打开 VMware VirtualCenter 操作仪表板：`https://<vcenter-ip>/vod/index.html?page=hosts`。



对于 vCenter Server 192.168.110.28 上 MOID 为 “host-22” 的 ESXi 主机，API 调用的格式如下所示：

DELETE `https://192.168.110.28/api/1.0/vshield/host-22/vsds`

请务必在所有 ESXi 主机上发出该 API 调用。

卸载数据安全后，您可以安装新版本。请参见[安装 NSX 数据安全](#)。

NSX SSL VPN

从 NSX 6.2 开始，SSL VPN 网关只接受 TLS 协议。不过，在升级到 NSX 6.2 或更高版本后，创建的任何新客户端在建立连接期间会自动使用 TLS 协议。此外，从 NSX 6.2.3 开始，TLS 1.0 已弃用。

由于协议发生变化，在 NSX 6.0.x 客户端尝试连接到 NSX 6.2 或更高版本网关时，连接建立会在 SSL 握手阶段失败。

从 NSX 6.0.x 升级后，卸载旧 SSL VPN 客户端并安装 NSX 6.2.x 版本的 SSL VPN 客户端。请参见《NSX 管理指南》中的“在远程站点上安装 SSL 客户端”。

NSX L2 VPN

如果在 NSX Edge 版本 5.5.x 或 6.0.x 上安装了 L2 VPN，则不支持升级 NSX Edge。必须先删除任何 L2 VPN 配置，然后才能升级 NSX Edge。

安装 NSX 数据安全

注 从 NSX 6.2.3 开始，NSX 数据安全功能将被弃用。在 NSX 6.2.3 中，您可以自行决定继续使用该功能，但要注意，在将来的 NSX 版本中将移除该功能。

前提条件

必须在要安装数据安全的数据中心上安装 NSX Guest Introspection。

如果要将 IP 池中的某个 IP 地址分配给数据安全服务虚拟机，请先创建 IP 池，然后再安装数据安全。请参见《NSX 管理指南》中的“分组对象”。

步骤

- 1 在**安装 (Installation)**选项卡中，单击**服务部署 (Service Deployments)**。
- 2 单击**新建服务部署 (New Service Deployment)** () 图标。
- 3 在“部署网络和安全服务”对话框中，选择**数据安全 (Data Security)**，然后单击**下一步 (Next)**。
- 4 在**指定调度 (Specify schedule)** (在该对话框的底部) 中，选择**立即部署 (Deploy now)**以便在安装数据安全后立即对其进行部署，或者选择部署日期和时间。
- 5 单击**下一步 (Next)**。
- 6 选择要安装数据安全的数据中心和群集，然后单击**下一步 (Next)**。
- 7 在“选择存储和管理网络”页面上，选择要添加服务虚拟机存储器的数据存储，或者选择**已在主机上指定 (Specified on host)**。

选定的数据存储在选定群集的所有主机上都必须可用。

如果选择了**已在主机上指定 (Specified on host)**，则在将数据存储添加到群集中之前，必须在主机的 **AgentVM 设置 (AgentVM Settings)** 中指定 ESX 主机的数据存储。请参见《vSphere API/SDK 文档》。

- 8 选择用于承载管理接口的分布式虚拟端口组。该端口组必须能够访问 NSX Manager 的端口组。

如果数据存储设置为**已在主机上指定 (Specified on host)**，则必须在群集内每个主机的 **agentVmNetwork** 属性中指定要使用的网络。请参见《vSphere API/SDK 文档》。

将主机添加到群集时，必须在将该主机添加到群集之前设置其 **agentVmNetwork** 属性。

选定的端口组必须在选定群集的所有主机上都可用。

- 9 在“IP 分配”中，选择以下其中的一项：

选择	目的
DHCP	通过动态主机配置协议 (DHCP) 将 IP 地址分配给数据安全服务虚拟机。
IP 池	将选定 IP 池中的某个 IP 地址分配给数据安全服务虚拟机。

请注意，不支持静态 IP 地址。

- 10 单击**下一步 (Next)**，然后在“即将完成”页面上单击**完成 (Finish)**。

- 11 监控该部署，直至**安装状态 (Installation Status)**列显示**成功 (Succeeded)**。
- 12 如果**安装状态 (Installation Status)**列显示**失败 (Failed)**，则单击“失败”旁边的图标。将显示所有部署错误。单击**解决 (Resolve)**修复这些错误。在某些情况下，解决这些错误时会显示其他错误。执行所需操作，然后重新单击**解决办法 (Resolve)**。

升级后对照表

在完成升级后，请执行以下步骤。

步骤

- 1 在升级后，创建 NSX Manager 的当前备份。
- 2 检查是否在主机上安装了 VIB。

NSX 使用以下命令安装这些 VIB：

```
esxcli software vib get --vibname esx-vxlan
esxcli software vib get --vibname esx-vsip
```

如果已安装 Guest Introspection，还要检查该 VIB 在主机上是否存在：

```
esxcli software vib get --vibname epsec-mux
```

- 3 重新同步主机消息总线。VMware 建议所有客户在升级后执行重新同步。
- 您可以使用以下 API 调用在每个主机上执行重新同步。

```
URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
HTTP Method : POST

Headers:

Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
```

在跨 vCenter NSX 中升级到 NSX 6.2.x

要在跨 vCenter 环境中升级到 NSX 6.2.x，您必须按照本指南中介绍的顺序升级 NSX 组件。

NSX 组件必须按照以下顺序进行升级：

- 1 主 NSX Manager 设备
- 2 所有辅助 NSX Manager 设备
- 3 NSX Controller 群集

4 主机群集

5 NSX Edge

6 Guest Introspection

升级过程是由 **NSX Manager** 管理的。如果某个组件升级失败或升级中断，并且您需要重复或重新启动升级，则升级过程会从停止的位置开始，而不会从头开始。

每个节点的升级状态都会更新，并按群集级别显示。

在跨 vCenter NSX 中升级主 NSX Manager

NSX 基础架构升级过程的第一步是升级主 NSX Manager 设备。

在升级期间，您可以选择加入 **NSX 客户体验改善计划 (CEIP)**。有关该计划的详细信息（包括如何加入或退出该计划），请参见 **NSX 管理指南** 中的“客户体验改善计划”。



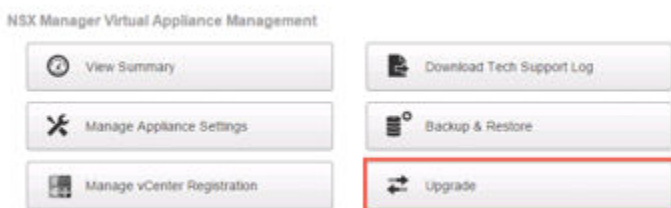
小心 不支持在跨 vCenter NSX 环境中运行不同版本的 NSX Manager 设备。在升级主 NSX Manager 设备后，您必须升级辅助 NSX Manager 设备。

前提条件

- 验证 **NSX Manager** 文件系统使用率，并在文件系统使用率达到 100% 时执行清理。
 - a 登录到 **NSX Manager** 并运行 `show filesystems` 以显示 `/dev/sda2` 文件系统使用率。
 - b 如果使用率达到 100%，请运行 `purge log manager` 和 `purge log system` 命令。
 - c 重新引导 **NSX Manager** 设备以使日志清理生效。
- 在升级 **NSX 6.2.x** 之前，将 **NSX Manager** 虚拟设备的预留内存增加至 16 GB。
请参见 [NSX 的系统要求](#)。
- 如果您的环境中已安装数据安全，请在升级 **NSX Manager** 之前将其卸载。请参见[卸载 NSX 数据安全](#)。
- 升级之前，请备份当前配置并下载技术支持日志。请参见 [NSX 备份和还原](#)。
- 下载升级包并检查 MD5。请参见[下载 NSX 升级包并检查 MD5](#)。
- 确保您了解执行 **NSX Manager** 升级时升级对运行产生的影响。请参见 [NSX 升级对运行产生的影响](#)。

步骤

- 1 登录到 **NSX Manager** 虚拟设备。
- 2 在 **NSX Manager** 主页上，单击**升级**。



- 3 单击**升级**，然后单击**选择文件**并浏览到 `VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz` 文件。单击**继续**以开始上载。

上载状态会显示在浏览器窗口中。

- 4 在“升级”对话框中，指定是否要启用 SSH 以及是否要参加 VMware 的客户体验改善计划（“CEIP”）。单击**升级**以开始进行升级。

将在浏览器窗口中显示升级状态。

等待升级过程完成，随后将显示 NSX Manager 登录页面。

- 5 再次登录到 NSX Manager 虚拟设备，确认升级状态是否为**完成**，并确认右上角的版本号和内部版本号是否与刚安装的升级包匹配。

如果在升级期间登录到 vSphere Web Client，将会在**网络和安全 > 安装 > 管理**页上看到同步问题警告。这是因为 NSX Manager 设备具有不同版本的 NSX。您必须先升级辅助 NSX Manager 设备，然后再执行升级的任何其他部分。

在升级 NSX Manager 后，您必须注销并重新登录到 vSphere Web Client。

如果在 vSphere Web Client 中未正确显示 NSX 插件，请清除浏览器的缓存和历史记录。如果未执行此步骤，则当您在 vSphere Web Client 中对 NSX 配置进行更改时，可能会看到类似以下内容的错误：“出现内部错误 - 错误 #1009 (An internal error has occurred - Error #1009)”。

如果在 vSphere Web Client 中不显示“网络和安全”选项卡，请重置 vSphere Web Client 服务器：

- 在 vCenter 5.5 中，打开 `https://<vcenter-ip>:5480`，然后重新启动 Web Client 服务器。
- 在 vCenter Server Appliance 6.0 中，以 root 用户身份登录到 vCenter Server shell，然后运行以下命令：

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

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

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

建议使用不同的 Web Client 管理运行不同 NSX Manager 版本的 vCenter Server，以避免运行不同版本的 NSX 插件时发生意外错误。

升级 NSX Manager 后，请创建新的 NSX Manager 备份文件。请参见 [NSX 备份和还原](#)。以前的 NSX Manager 备份仅对先前版本有效。

后续步骤

升级所有辅助 NSX Manager 设备。

在跨 vCenter NSX 中升级所有辅助 NSX Manager 设备

您必须先升级所有辅助 NSX Manager 设备，然后再升级任何其他 NSX 组件。

完成以下步骤以升级辅助 NSX Manager 设备。在跨 vCenter NSX 环境中，为所有辅助 NSX Manager 设备重复这些步骤。

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

前提条件

- 确认升级了主 NSX Manager。
- 验证 NSX Manager 文件系统使用率，并在文件系统使用率达到 100% 时执行清理。
 - a 登录到 NSX Manager 并运行 `show filesystems` 以显示 `/dev/sda2` 文件系统使用率。
 - b 如果使用率达到 100%，请运行 `purge log manager` 和 `purge log system` 命令。
 - c 重新引导 NSX Manager 设备以使日志清理生效。
- 在升级 NSX 6.2.x 之前，将 NSX Manager 虚拟设备的预留内存增加至 16 GB。
请参见 [NSX 的系统要求](#)。
- 如果您的环境中已安装数据安全，请在升级 NSX Manager 之前将其卸载。请参见[卸载 NSX 数据安全](#)。
- 升级之前，请备份当前配置并下载技术支持日志。请参见 [NSX 备份和还原](#)。
- 下载升级包并检查 MD5。请参见[下载 NSX 升级包并检查 MD5](#)。
- 确保您了解执行 NSX Manager 升级时升级对运行产生的影响。请参见 [NSX 升级对运行产生的影响](#)。

步骤

- 1 单击**升级**，然后单击**选择文件**并浏览到 `VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz` 文件。单击**继续**以开始上载。
上载状态会显示在浏览器窗口中。
- 2 在“升级”对话框中，指定是否要启用 SSH 以及是否要参加 VMware 的客户体验改善计划（“CEIP”）。单击**升级**以开始进行升级。
将在浏览器窗口中显示升级状态。
等待升级过程完成，随后将显示 NSX Manager 登录页面。
- 3 再次登录到 NSX Manager 虚拟设备，确认升级状态是否为**完成**，并确认右上角的版本号和内部版本号是否与刚安装的升级包匹配。

在升级 NSX Manager 后，您必须注销并重新登录到 vSphere Web Client。

如果在 vSphere Web Client 中未正确显示 NSX 插件，请清除浏览器的缓存和历史记录。如果未执行此步骤，则当您在 vSphere Web Client 中对 NSX 配置进行更改时，可能会看到类似以下内容的错误：“出现内部错误 - 错误 #1009 (An internal error has occurred - Error #1009)”。

如果在 vSphere Web Client 中不显示“网络和安全”选项卡，请重置 vSphere Web Client 服务器：

- 在 vCenter 5.5 中，打开 <https://<vcenter-ip>:5480>，然后重新启动 Web Client 服务器。
- 在 vCenter Server Appliance 6.0 中，以 root 用户身份登录到 vCenter Server shell，然后运行以下命令：

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

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

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

建议使用不同的 Web Client 管理运行不同 NSX Manager 版本的 vCenter Server，以避免运行不同版本的 NSX 插件时发生意外错误。

升级 NSX Manager 后，请创建新的 NSX Manager 备份文件。请参见 [NSX 备份和还原](#)。以前的 NSX Manager 备份仅对先前版本有效。

后续步骤

[在跨 vCenter NSX 中升级 NSX Controller 群集](#)

在跨 vCenter NSX 中升级 NSX Controller 群集

环境中的控制器在群集级别进行升级。如果可以升级 NSX Controller 群集，则会在**网络和安全 (Networking & Security) > 安装 (Installation) > 管理 (Management)**面板中的主 NSX Manager 旁边显示升级链接。

建议在维护期限内升级控制器。

执行 NSX Controller 升级时，升级文件会下载到每个控制器节点。控制器会逐个进行升级。升级期间，**可升级**链接不可单击，而且系统会阻止升级控制器群集的 API 调用，直至升级已完成。

如果您在升级现有控制器之前部署新的控制器，则新的控制器会部署为旧版本。控制器节点必须具有相同版本才能加入群集。

前提条件

- 确保所有控制器都处于正常状态。当一个或多个控制器处于断开连接状态时，升级无法进行。要重新连接已断开连接的控制器，请尝试重置控制器虚拟设备。在**主机和群集**视图中，右键单击控制器并选择**电源 > 重置**。

- 有效的 NSX Controller 群集包含三个控制器节点。登录到这三个控制器节点，然后运行 **show controller-cluster status** 命令。

```
controller-node# show control-cluster status
```

Type	Status	Since
Join status:	Join complete	05/04 02:36:03
Majority status:	Connected to cluster majority	05/19 23:57:23
Restart status:	This controller can be safely restarted	05/19 23:57:12
Cluster ID:	ff3ebaeb-de68-4455-a3ca-4824e31863a8	
Node UUID:	ff3ebaeb-de68-4455-a3ca-4824e31863a8	
Role	Configured status	Active status
api_provider	enabled	activated
persistence_server	enabled	activated
switch_manager	enabled	activated
logical_manager	enabled	activated
directory_server	enabled	activated

- 对于“加入”状态，请验证控制器节点是否正在报告“加入完成”。
- 对于“多数”状态，请验证控制器是否已连接到群集中的多数节点。
- 对于群集 ID，群集中的所有控制器节点应具有相同的群集 ID。
- 对于“已配置”状态和“活动”状态，请验证是否所有控制器角色均已启用并激活。
- 确保您了解执行 NSX Controller 升级时升级对运行产生的影响。请参见 [NSX 升级对运行产生的影响](#)。

步骤

- 在 vSphere Web Client 中，导航至主页 > 网络和安全 > 安装，选择管理选项卡，然后单击控制器群集状态列中的可升级。

The screenshot shows the 'Installation' page in the vSphere Web Client. The 'Management' tab is selected. Under 'NSX Managers', there is a table with the following data:

NSX Manager	IP Address	vCenter	Version	Controller Cluster Status
192.168.110.44	192.168.110.44	192.168.110.28	6.2.0.2860153	Upgrade Available

Below this, the 'NSX Controller nodes' section shows a table with three controller nodes:

Controller IP Address	ID	Status	Upgrade Status	Software Version	NSX Manager
192.168.110.201	controller-1	Normal	Not Started	6.2.4.1894	192.168.110.44
192.168.110.202	controller-2	Normal	Not Started	6.2.4.1894	192.168.110.44
192.168.110.203	controller-3	Normal	Not Started	6.2.4.1894	192.168.110.44

环境中的控制器会逐个进行升级和重新引导。启动升级后，系统首先会下载升级文件，然后升级每个控制器，接着重新引导每个控制器，最后更新每个控制器的升级状态。以下字段显示各个控制器状态：

- NSX Manager 区域中的**控制器群集状态**列显示群集的升级状态。当升级已开始时，状态显示为**正在下载升级文件**。当升级文件已下载到群集中的所有控制器时，状态会变为**正在进行中**。当群集中的所有控制器都已升级后，显示的状态是**完成**，然后此列将不再显示。
- “NSX Controller 节点”部分中的**状态**列显示每个控制器的状态，而且此状态最初显示为**正常**。当控制器服务关闭并且控制器重新引导时，状态会变为**已断开连接**。当控制器升级完成后，状态会再次变为**正常**。
- “NSX Controller 节点”部分中的**升级状态**列显示每个控制器的升级状态。状态最初显示**正在下载升级文件**，接着显示**升级正在进行中**，然后显示**正在重新引导**。控制器升级后，状态将显示**已升级**。

当升级已完成时，“NSX Controller 节点”部分中的**软件版本**列将为每个控制器显示 **6.2.buildNumber**。重新运行 **show controller-cluster status** 命令，以确保控制器能够形成多数。如果未重新形成 NSX Controller 群集多数，请查看控制器日志和 NSX Manager 日志。

在升级控制器后，可能会为一个或多个控制器节点分配新的控制器 ID。这是预期的行为，这取决于辅助 NSX Manager 何时轮询节点。

每次升级的平均升级时间是 6 到 8 分钟。如果升级无法在超时期限（30 分钟）内完成，则**升级状态**列会显示**失败**。再次单击 NSX Manager 区域中的**可升级**，以从停止的位置恢复升级过程。

如果网络问题导致无法在 30 分钟的超时期限内成功完成升级，您可能需要配置更长的超时期限。与 VMware 支持合作，诊断并解决任何基础问题，并根据需要配置更长的超时期限。

如果控制器升级失败，请检查控制器与 NSX Manager 之间的连接。

升级时会存在以下情况，即第一个控制器升级成功，而第二个控制器升级不成功。假设某个群集包含三个控制器，并且第一个控制器已成功升级到新版本，而第二个控制器正在升级。如果第二个控制器升级失败，则该控制器可能会停留在断开连接状态。同时，第一个和第三个控制器现在具有两种不同版本（一个已升级，另一个未升级），从而无法形成多数。此时，升级无法重新启动。要解决此情况，请创建另一个控制器。新创建的控制器将具有较旧版本（与第三个控制器匹配），从而与第三个控制器形成多数。此时，您可以重新启动升级过程。

后续步骤

在跨 vCenter NSX 中升级主机群集。

在跨 vCenter NSX 中升级主机群集

在将所有 NSX Manager 设备和 NSX Controller 群集升级到 NSX 6.2.x 后，您应该在跨 vCenter NSX 环境中更新所有主机群集。在此过程中，群集中的每个主机会接收软件更新，然后重新引导。

升级主机群集会升级 NSX VIB：esx-vsip 和 esx-vxlan。

- 如果您从早于 NSX 6.2 的 NSX 版本升级，则准备好的主机将具有一个额外的 VIB：esx-dvfilter-switch-security。在 NSX 6.2 和更高版本中，esx-dvfilter-switch-security 包含在 esx-vxlan VIB 中。
- 如果您从 NSX 6.2.x（版本为 NSX 6.2.4 或更高版本）升级，则准备好的主机将具有一个额外的 VIB：esx-vdpi。

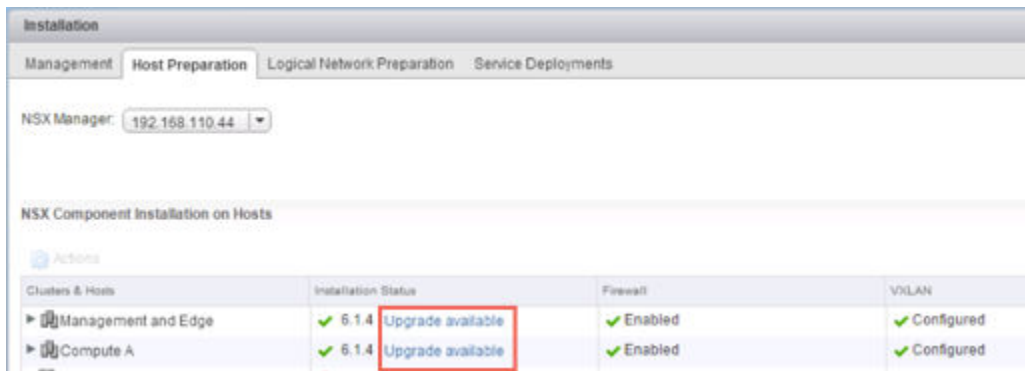
前提条件

- 确保所有主机的完全限定域名 (FQDN) 均可解析。
- 登录到群集中的主机之一，并运行 `esxcli software vib list` 命令。记录以下 VIB 的当前版本：
 - esx-vsip
 - esx-vxlan
- 升级 NSX Manager 和 NSX Controller 群集。
- 确保您了解执行主机群集升级时升级对运行产生的影响。请参阅 [NSX 升级对运行产生的影响](#)。
- 如果 DRS 已禁用，请先关闭虚拟机的电源或手动对虚拟机执行 vMotion 操作，然后再开始升级。
- 如果 DRS 已启用，则正在运行的虚拟机在主机群集升级过程中会自动移动。开始升级之前，请确保 DRS 可以在您的环境中工作。
 - 确保在主机群集上启用了 DRS。
 - 确保 vMotion 正常工作。
 - 检查主机与 vCenter 的连接状态。
 - 检查每个主机群集是否包含至少三个 ESXi 主机。在 NSX 升级过程中，仅包含一个或两个主机的主机群集更可能出现 DRS 接入控制方面的问题。为确保 NSX 升级成功，VMware 建议每个主机群集包含至少三个主机。如果一个群集包含的主机少于三个，则建议手动撤出这些主机。

- 在仅包含两个或三个主机的小型群集中，如果您已创建声明某些虚拟机必须驻留在单独的主机上的反关联性规则，则这些规则可能会导致 DRS 无法在升级过程中移动虚拟机。在此情况下，请向群集添加更多主机，或者在升级过程中禁用反关联性规则，并在升级完成后重新启用这些规则。要禁用反关联性规则，请导航到**主机和群集 (Hosts and Clusters) > Cluster > 管理 (Manage) > 设置 (Settings) > 虚拟机/主机规则 (VM/Host Rules)**。编辑该规则并取消选择**启用规则 (Enable rule)**。

步骤

- 1 在 vSphere Web Client 中，导航至主页 > 网络和安全 > 安装 (Home > Networking & Security > Installation)，然后选择**主机准备 (Host Preparation)**选项卡。
- 2 对每个要升级的群集单击**可升级 (Upgrade available)**。



“安装状态”显示正在安装。

- 3 群集的“安装状态”显示未就绪。单击**未就绪 (Not Ready)**以显示详细信息。单击**解决所有 (Resolve all)**以尝试完成 VIB 安装。

主机将被置于维护模式并重新引导（如果需要）以完成升级。

“安装状态”列显示正在安装。在升级完成后，“安装状态”列将显示绿色对勾和升级后的 NSX 版本。

- 4 如果在启用 DRS 后**解决 (Resolve)**操作失败，主机可能需要手动干预以进入维护模式（例如，由于 HA 要求或 DRS 规则），升级过程停止，并且群集的“安装状态”再次显示未就绪。单击**未就绪 (Not Ready)**以显示详细信息。在**主机和群集 (Hosts and Clusters)**视图中检查主机，确保主机已打开电源并且已连接，并确保主机不包含正在运行的虚拟机。然后重试**解决 (Resolve)**操作。

“安装状态”列显示正在安装。在升级完成后，“安装状态”列将显示绿色对勾和升级后的 NSX 版本。

要确认主机是否已更新，请登录到群集中的主机之一并运行 `esxcli software vib list | grep esx` 命令。确保以下 VIB 已更新到预期版本。

- esx-vmip
- esx-vxlan

如果主机升级失败，请执行以下故障排除步骤：

- 在 vCenter 上检查 ESX Agent Manager，并查找警示和错误。
- 登录到主机，检查 `/var/log/esxupdate.log` 日志文件，然后查找最近的警示和错误。

- 确保已在主机上配置了 DNS 和 NTP。

有关更多故障排除步骤，请参见 NSX 故障排除指南中的“主机准备”。

在跨 vCenter NSX 中更改 VXLAN 端口

您可以更改用于 VXLAN 流量的端口。

在 NSX 6.2.3 及更新版本中，默认 VXLAN 端口为 4789，这是 IANA 分配的标准端口。在 NSX 6.2.3 之前，默认 VXLAN UDP 端口号为 8472。

任何新的 NSX 安装将 UDP 端口 4789 用于 VXLAN。

如果是从 NSX 6.2.2 或更早版本升级到 NSX 6.2.3 或更新版本，并且安装在升级之前使用旧的默认端口号 (8472) 或自定义端口号（如 8888），则在升级后将继续使用该端口，除非您对其进行了更改。

如果您的升级安装使用或将使用硬件 VTEP 网关（ToR 网关），则必须切换到 VXLAN 端口 4789。

跨 vCenter NSX 不要求将 4789 用于 VXLAN 端口，但必须将跨 vCenter NSX 环境中的所有主机配置为使用相同的 VXLAN 端口。如果切换到端口 4789，这会确保添加到跨 vCenter NSX 环境中的任何新 NSX 安装使用与现有 NSX 部署相同的端口。

更改 VXLAN 端口是通过一个包含三个阶段的过程完成的，并且不会中断 VXLAN 流量。

- 1 NSX Manager 将所有主机配置为同时侦听新旧端口上的 VXLAN 流量。主机继续在旧端口上发送 VXLAN 流量。
- 2 NSX Manager 将所有主机配置为在新端口上发送流量。
- 3 NSX Manager 将所有主机配置为停止侦听旧端口，所有流量均通过新端口发送和接收。

在跨 vCenter NSX 环境中，您必须在主 NSX Manager 上启动端口更改。对于每个阶段，在对跨 vCenter NSX 环境中的所有主机进行配置更改之后，才会继续下一阶段的操作。

前提条件

- 确认防火墙未阻止要用于 XLAN 的端口。
- 确认在更改 VXLAN 端口时未同时运行主机准备。

步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**安装 (Installation)**。
- 3 单击**逻辑网络准备 (Logical Network Preparation)**选项卡，然后单击**VXLAN 传输 (VXLAN Transport)**。
- 4 在“VXLAN 端口”面板中，单击**更改 (Change)**按钮。输入要切换到的端口。4789 是 IANA 为 VXLAN 分配的端口。

将端口更改传播到所有主机需要很短的时间。

- 5 （可选）使用 GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus API 请求检查端口更改进度。

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>PHASE_TWO</taskPhase>
  <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

...

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
  <prevPort>8472</prevPort>
  <targetPort>4789</targetPort>
  <taskPhase>FINISHED</taskPhase>
  <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

后续步骤

在跨 vCenter NSX 中升级 NSX Edge

在跨 vCenter NSX 中升级 NSX Edge

NSX Edge 升级与 NSX Controller 群集升级或主机群集升级不存在任何依赖关系。即使尚未升级 NSX Controller 群集或主机群集，您也可以升级 NSX Edge。请在跨 vCenter NSX 环境的所有 NSX 安装中升级 NSX Edge。

在升级过程中，新的 Edge 虚拟设备会与现有虚拟设备部署在一起。当新的 Edge 准备就绪时，旧的 Edge 的 vNIC 会断开连接，而新的 Edge 的 vNIC 会建立连接。然后，新的 Edge 会发送无故 ARP (GARP) 数据包，更新已连接的交换机的 ARP 缓存。当部署了 HA 时，升级过程将执行两次。

此过程会暂时影响数据包转发。您可以通过将 Edge 配置为以 ECMP 模式工作来最大程度地减小该影响。

如果未启用正常重新启动，将在升级期间撤消 OSPF 邻接。

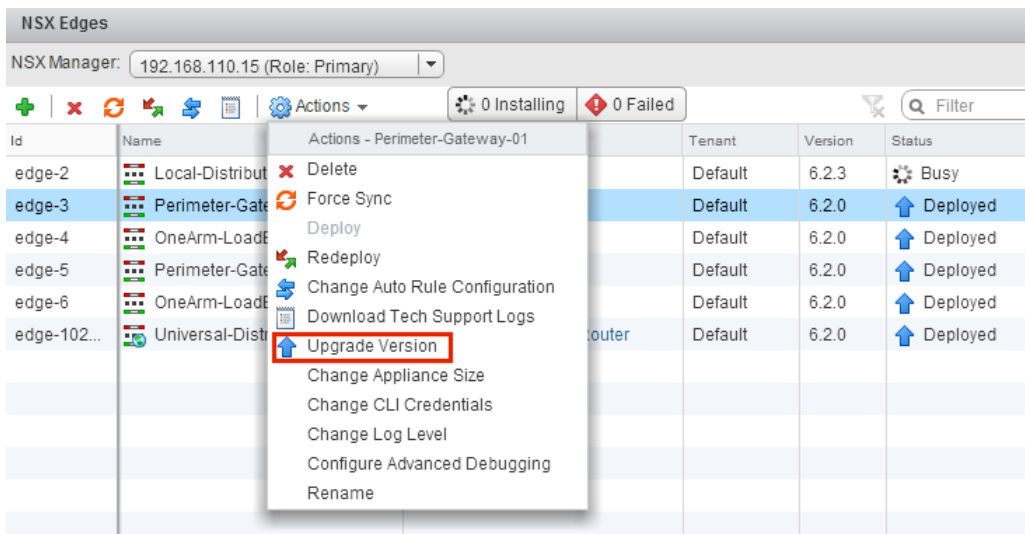
前提条件

- 确认 NSX Manager 已升级到 6.2.x。
- 确认具有本地分段 ID 池，即使不打算创建 NSX 逻辑交换机。
- 确认主机具有足够的资源以在升级期间部署额外的 NSX Edge 服务网关设备，特别是在并行升级多个 NSX Edge 设备时。有关每个 NSX Edge 大小所需的资源，请参见 [NSX 的系统要求](#)。
 - 对于单个 NSX Edge 实例，在升级期间具有两个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。

- 从 NSX 6.2.3 开始，在升级具有高可用性的 NSX Edge 实例时，将在更换旧设备之前部署两个更换设备。这意味着，在升级给定的 NSX Edge 期间，将具有四个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。在升级 NSX Edge 实例后，任一 HA 设备可能会变为活动状态。
- 在 NSX 6.2.3 之前，在升级具有高可用性的 NSX Edge 实例时，仅在更换旧设备时部署一个更换设备。这意味着，在升级给定的 NSX Edge 期间，将具有三个处于“已打开电源”状态并具有相应大小的 NSX Edge 设备。在升级 NSX Edge 实例后，通常具有 HA 索引 0 的 NSX Edge 设备变为活动状态。
- 了解在进行 NSX Edge 升级时对运行产生的影响。请参见 [NSX 升级对运行产生的影响](#)。
- 不支持升级启用了 L2 VPN 的 NSX Edge 版本 5.5 或 6.0。在升级之前，您必须删除 L2 VPN 配置。在升级后，您可以重新配置 L2 VPN。请参见 NSX 安装指南中的“L2 VPN 概述”。
- 如果从 NSX 6.2.x 升级到 NSX 6.2.3 并且配置了负载平衡器，请参见以下知识库文章以避免出现升级问题：<https://kb.vmware.com/kb/2145887>。

步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 对于每个 NSX Edge 实例，请在**操作 (Actions)**菜单中选择**升级版本 (Upgrade Version)**。



如果升级失败并显示错误消息“无法部署 Edge 设备”，请确保 NSX Edge 设备部署到的主机已连接并且未处于维护模式。

在成功升级 NSX Edge 后，**状态 (Status)**为“已部署”，并且**版本 (Version)**列显示新的 NSX 版本。

如果 Edge 升级失败并且未回滚到旧版本，请单击**重新部署 NSX Edge (Redeploy NSX Edge)** 图标，然后重试升级。

后续步骤

如果需要，请重新配置任何 L2 VPN 配置。请参见 NSX 安装指南中的“L2 VPN 概述”。

在跨 vCenter NSX 中升级 Guest Introspection

在跨 vCenter NSX 中升级 Guest Introspection

请务必升级 Guest Introspection 以便与 NSX Manager 版本相匹配。

注 可以从 vSphere Web Client 中升级 Guest Introspection 服务虚拟机。在升级 NSX Manager 后，您不需要删除服务虚拟机以进行升级。如果删除了服务虚拟机，服务状态将显示为失败，因为代理虚拟机丢失。单击**解决 (Resolve)**以部署新的服务虚拟机，然后单击**可升级 (Upgrade Available)**以部署最新的 Guest Introspection 服务虚拟机。

前提条件

NSX Manager、控制器、准备的主机群集和 NSX Edge 必须已升级到 6.2.x。

步骤

- 1 在**安装 (Installation)**选项卡中，单击**服务部署 (Service Deployments)**。

The screenshot shows the 'Service Deployments' tab in the vSphere Web Client. At the top, there are tabs for 'Installation', 'Management', 'Host Preparation', 'Logical Network Preparation', and 'Service Deployments'. Below these, the 'NSX Manager' is listed as '192.168.110.15 (Role: Primary)'. The main section is titled 'Network & Security Service Deployments' and contains a table of services.

Service	Version	Installation Status	Service Status	Cluster	Datastore	Port Group	IP Address Range
Guest Introspection	6.2.0	<div>✓ Succeeded</div> <div>⬆ Upgrade Available</div>	<div>✓ Up</div>	Comp...	ds-site...	vds-sit...	GI Pool

安装状态 (Installation Status)列显示可升级 (Upgrade Available)。

- 2 选择要升级的 Guest Introspection 部署。

将启用服务表上方的工具栏中的**升级 (Upgrade)** (⬆) 图标。

3 单击升级 (Upgrade) (↑) 图标并按照 UI 提示进行操作。

Confirm Upgrade

Upgrade Guest Introspection service

Datastore * ds-site-a-nfs01 ▼

Network * vds-site-a_Management... ▼

IP assignment * GI Pool ▼

Specify schedule:

☒ Upgrade now

☐ Schedule the upgrade 6:29 PM ▼

OK Cancel

在升级 Guest Introspection 后，安装状态为成功，服务状态为已连接。将在 vCenter Server 清单中显示 Guest Introspection 服务虚拟机。

后续步骤

在为特定群集升级 Guest Introspection 后，您可以升级任何合作伙伴解决方案。如果启用了合作伙伴解决方案，请参阅合作伙伴提供的升级文档。即使未升级合作伙伴解决方案，也会继续提供保护。

不支持直接升级的 NSX 服务

某些 NSX 服务（如 VMware 合作伙伴安全虚拟设备）不支持直接升级。在这些情况下，您必须卸载并重新安装这些服务。

VMware 合作伙伴安全虚拟设备

请查看合作伙伴文档，以验证合作伙伴安全虚拟设备是否可以升级。

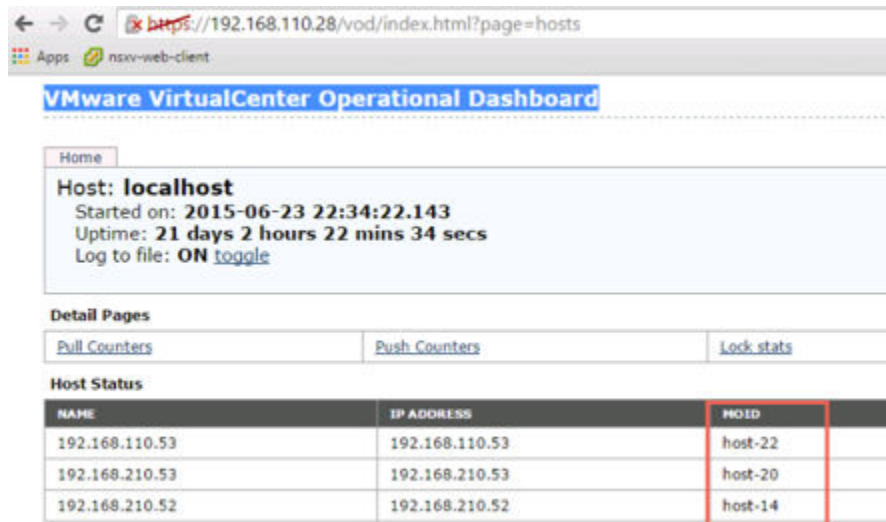
NSX 数据安全

您应该在升级 NSX 之前卸载 NSX 数据安全，并在 NSX 升级完成后重新安装 NSX 数据安全。如果您已在未先卸载 NSX 数据安全的情况下升级了 NSX，必须使用 REST API 调用卸载数据安全。

发出下面的 API 调用：

```
DELETE https://<nsx-manager-ip>/api/1.0/vshield/<host-id>/vsds
```

host-id 是 ESXi 主机的 MOID。要检索 MOID，请打开 VMware VirtualCenter 操作仪表板：<https://<vcenter-ip>/vod/index.html?page=hosts>。



对于 vCenter Server 192.168.110.28 上 MOID 为 “host-22” 的 ESXi 主机，API 调用的格式如下所示：

DELETE <https://192.168.110.28/api/1.0/vshield/host-22/vsds>

请务必在所有 ESXi 主机上发出该 API 调用。

卸载数据安全后，您可以安装新版本。请参见[安装 NSX 数据安全](#)。

NSX SSL VPN

从 NSX 6.2 开始，SSL VPN 网关只接受 TLS 协议。不过，在升级到 NSX 6.2 或更高版本后，创建的任何新客户端在建立连接期间会自动使用 TLS 协议。此外，从 NSX 6.2.3 开始，TLS 1.0 已弃用。

由于协议发生变化，在 NSX 6.0.x 客户端尝试连接到 NSX 6.2 或更高版本网关时，连接建立会在 SSL 握手阶段失败。

从 NSX 6.0.x 升级后，卸载旧 SSL VPN 客户端并安装 NSX 6.2.x 版本的 SSL VPN 客户端。请参见《NSX 管理指南》中的“在远程站点上安装 SSL 客户端”。

NSX L2 VPN

如果在 NSX Edge 版本 5.5.x 或 6.0.x 上安装了 L2 VPN，则不支持升级 NSX Edge。必须先删除任何 L2 VPN 配置，然后才能升级 NSX Edge。

升级后对照表

在完成升级后，请执行以下步骤。

步骤

- 1 在升级后，创建 NSX Manager 的当前备份。

2 检查是否在主机上安装了 VIB。

NSX 使用以下命令安装这些 VIB:

```
esxcli software vib get --vibname esx-vxlan  
esxcli software vib get --vibname esx-vsip
```

如果已安装 **Guest Introspection**，还要检查该 VIB 在主机上是否存在:

```
esxcli software vib get --vibname epsec-mux
```

3 重新同步主机消息总线。VMware 建议所有客户在升级后执行重新同步。

您可以使用以下 API 调用在每个主机上执行重新同步。

```
URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>  
HTTP Method : POST
```

Headers:

```
Authorization : base64encoded value of username password  
Accept : application/xml  
Content-Type : application/xml
```

在 NSX 环境中升级 vSphere

在 NSX 环境中升级 vSphere 时，您必须确保 NSX 和 vSphere 版本兼容。

查看“VMware 产品互操作性列表”，验证哪些 vSphere 和 ESXi 版本与您的 NSX 安装兼容。请参阅 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php。

参见 vSphere 相应版本的文档，了解有关升级 vSphere 的详细说明，其中包括《vSphere 升级指南》和《安装和管理 VMware vSphere Update Manager 指南》。

在主机上升级 ESXi 时，您还必须在主机上安装新的 NSX VIB，以便与新的 ESXi 版本兼容。在更新 NSX VIB 后，NSX 工作负载才能在升级的主机上运行。

本章讨论了以下主题：

- 在 NSX 环境中升级 ESXi
- 在 ESXi 升级后重新部署 Guest Introspection

在 NSX 环境中升级 ESXi

NSX VIB 特定于主机上安装的 ESXi 版本。如果您升级 ESXi，则必须安装适合新 ESXi 版本的新 NSX VIB。

重要 您必须确保主机在整个升级过程中都保持维护模式，以避免 DRS 或 vMotion 在升级完成之前将虚拟机移到主机。

前提条件

- 查看“VMware 产品互操作性列表”，验证哪些 vSphere 和 ESXi 版本与您的 NSX 安装兼容。请参阅 http://www.vmware.com/resources/compatibility/sim/interop_matrix.php。
- 阅读 vSphere 相应版本的文档，了解有关升级 vSphere 的详细说明，其中包括《vSphere 升级指南》和《安装和管理 VMware vSphere Update Manager 指南》。
- 确认 Platform Services Controller 和 vCenter Server 系统已升级到新的 vSphere 版本。
- 确保所有主机的完全限定域名 (FQDN) 均可解析。
- 如果 DRS 已禁用，请先关闭虚拟机的电源或手动对虚拟机执行 vMotion 操作，然后再开始升级。

- 如果 DRS 已启用，则正在运行的虚拟机在主机群集升级过程中会自动移动。开始升级之前，请确保 DRS 可以在您的环境中工作。
 - 确保在主机群集上启用了 DRS。
 - 确保 vMotion 正常工作。
 - 检查主机与 vCenter 的连接状态。
 - 检查每个主机群集是否包含至少三个 ESXi 主机。在 NSX 升级过程中，仅包含一个或两个主机的主机群集更可能出现 DRS 接入控制方面的问题。为确保 NSX 升级成功，VMware 建议每个主机群集包含至少三个主机。如果一个群集包含的主机少于三个，则建议手动撤出这些主机。
 - 在仅包含两个或三个主机的小型群集中，如果您已创建声明某些虚拟机必须驻留在单独的主机上的反关联性规则，则这些规则可能会导致 DRS 无法在升级过程中移动虚拟机。在此情况下，请向群集添加更多主机，或者在升级过程中禁用反关联性规则，并在升级完成后重新启用这些规则。要禁用反关联性规则，请导航到**主机和群集 (Hosts and Clusters) > Cluster > 管理 (Manage) > 设置 (Settings) > 虚拟机/主机规则 (VM/Host Rules)**。编辑该规则并取消选择**启用规则 (Enable rule)**。

步骤

- ◆ 对于每个必须升级的主机，请完成以下步骤。
 - a 将主机置于维护模式。

如果群集启用了 DRS，则 DRS 将尝试把虚拟机移至其他主机。如果 DRS 因任何原因而失败，您可能需要手动移动虚拟机，然后将主机置于维护模式。
 - b 在主机上升级 ESXi。

在 ESXi 升级完成后重新引导主机。
 - c 如果在重新引导后主机的状态为未连接，请连接主机。右键单击主机，然后选择**连接 (Connection) > 连接 (Connect)**。
 - d 导航至**网络和安全 (Networking & Security) > 安装 (Installation) > 主机准备 (Host Preparation)**。
 - e 选择已升级 ESXi 的主机。“安装状态”将显示**未就绪 (Not Ready)**。
 - f 单击**操作 (Actions) > 解决 (Resolve)**以完成 NSX VIB 更新。

将在主机上更新 NSX VIB 并重新引导主机。
 - g 在主机完成重新引导后，退出维护模式。

您可以通过连接到主机命令行并发出 `esxcli software vib list | grep esx-v` 命令来验证 VIB 是否更新。VIB 版本的第一部分显示适用于 VIB 的 ESXi 版本。例如，在从 ESXi 5.5 升级到 ESXi 6.0 之前。

```
[root@host-1:~] esxcli software vib list | grep esx-v
esx-vsip    5.5.0-0.0.XXXXXXX  VMware  VMwareCertified  2017-01-23
esx-vxlan   5.5.0-0.0.XXXXXXX  VMware  VMwareCertified  2017-01-23
```

在升级到 ESXi 6.0 之后：

```
[root@host-1:~] esxcli software vib list | grep esx-v
esx-vsip      6.0.0-0.0.XXXXXXX  VMware  VMwareCertified  2017-01-23
esx-vxlan     6.0.0-0.0.XXXXXXX  VMware  VMwareCertified  2017-01-23
```

在 ESXi 升级后重新部署 Guest Introspection

如果在部署了 Guest Introspection 的群集上升级 ESXi，您应该选中“服务部署”选项卡以查看是否需要重新部署 Guest Introspection。

重要 您必须先完成 ESXi 升级和关联的 NSX VIB 升级，然后再重新部署 Guest Introspection。

前提条件

- 完成 ESXi 升级。
- 在 ESXi 升级后，完成 NSX VIB（主机准备）升级。

步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击**安装 (Installation)**。
- 3 单击**服务部署 (Service Deployments)**选项卡。
- 4 如果“安装状态”列显示成功，则不需要重新进行部署。
- 5 如果“安装状态”列显示“未就绪”，请单击**未就绪 (Not Ready)**链接。单击**解决所有 (Resolve all)**以重新部署 Guest Introspection。