



VMware NSX for vSphere 6.3.7 发行说明

VMware NSX for vSphere 6.3.7 | 2018 年 11 月 15 日发行 | 内部版本 10667122

请参见本文的[修订历史](#)。

发行说明内容

本发行说明包含以下主题：

- [NSX 6.3.7 的新增功能](#)
- [版本、系统要求和安装说明](#)
- [已弃用和已停用的功能](#)
- [升级说明](#)
- [FIPS 合规性](#)
- [修订历史](#)
- [已解决的问题](#)
- [已知问题](#)

NSX 6.3.7 的新增功能

NSX for vSphere 6.3.7 解决了一些特定的客户问题。有关详细信息，请参见[已解决的问题](#)。

查看以前版本的发行说明：

- [NSX 6.3.6](#)
- [NSX 6.3.5](#)
- [NSX 6.3.4](#)
- [NSX 6.3.3](#)
- [NSX 6.3.2](#)
- [NSX 6.3.1](#)
- [NSX 6.3.0](#)

版本、系统要求和安装说明

注意：

- 下表列出了建议的 VMware 软件版本。这些建议只是常规建议，具体应考虑特定的环境需求。
- 此信息为截至本文档发布之日的最新信息。
- 有关 NSX 和其他 VMware 产品的最低支持版本，请参见 [VMware 产品互操作性列表](#)。VMware 的最低支持版本声明基于内部测试。
 - [满足 NSX 互操作性所需的 vSphere 的最低支持版本在 NSX 6.3.2 和 NSX 6.3.3 之间发生变化](#)。有关详细信息，请参见 [VMware 产品互操作性列表](#)。

产品或组件	建议的版本
NSX for vSphere	<p>对于新部署，VMware 建议使用最新的 NSX 版本。</p> <p>在升级现有部署时，请在计划升级之前参考 NSX 发行说明，或者与 VMware 技术支持代表联系以了解某些特定问题的详细信息。</p>
vSphere	<ul style="list-style-type: none"> • vSphere 5.5U3 和更高版本 • vSphere 6.0U3 和更高版本。vSphere 6.0U3 解决了在重新引导 vCenter Server 后在 ESXi 主机中出现的重复 VTEP 问题。有关详细信息，请参见 VMware 知识库文章 2144605。 • vSphere 6.5U1 和更高版本。vSphere 6.5U1 解决了 EAM 由于内存不足而失败的问题。有关详细信息，请参见 VMware 知识库文章 2135378。
适用于 Windows 的客户机侦测	<p>支持所有版本的 VMware Tools。某些基于客户机侦测的功能需要使用较新的 VMware Tools 版本：</p> <ul style="list-style-type: none"> • 使用 VMware Tools 10.0.9 和 10.0.12 启用 VMware Tools 附带的可选瘦代理网络侦测驱动程序组件。 • 升级到 VMware Tools 10.0.8 和更高版本，以解决在 NSX/vCloud Networking and Security 中升级 VMware Tools 后虚拟机速度缓慢问题（请参见 VMware 知识库文章 2144236）。 • 使用 VMware Tools 10.1.0 和更高版本以支持 Windows 10。 • 使用 VMware Tools 10.1.10 和更高版本以支持 Windows Server 2016。
适用于 Linux 的客户机侦测	<p>该 NSX 版本支持以下 Linux 版本：</p> <ul style="list-style-type: none"> • RHEL 7 GA（64 位） • SLES 12 GA（64 位） • Ubuntu 14.04 LTS（64 位）

系统要求和安装说明

有关 NSX 安装必备条件的完整列表，请参见《NSX 安装指南》中的 [NSX 的系统要求](#) 一节。

有关安装说明，请参见 [《NSX 安装指南》](#) 或 [《跨 vCenter NSX 安装指南》](#)。

已弃用和已停用的功能

产品周期终止和支持期终止警告

有关必须尽快升级的 NSX 和其他 VMware 产品的信息，请参见 [VMware 生命周期产品列表](#)。

- NSX for vSphere 6.1.x 于 2017 年 1 月 15 日终止提供 (EOA) 和终止支持 (EOGS)。（另请参见 [VMware 知识库文章 2144769](#)。）
- NSX for vSphere 6.2.x 将于 2018 年 8 月 20 日终止支持 (EOGS)。
- 已移除 NSX 数据安全：从 NSX 6.3.0 开始，已从产品中移除 NSX 数据安全功能。
- 已弃用 NSX 活动监控 (SAM)：从 NSX 6.3.0 开始，活动监控不再是受支持的 NSX 功能。作为替代，请使用端点监控。有关详细信息，请参见《NSX 管理指南》中的“[端点监控](#)”。
- 已移除 Web Access 终端：Web Access 终端 (WAT) 已从 NSX 6.3.0 中移除。您无法配置 Web Access SSL VPN-Plus 并启用通过 NSX Edge 的公共 URL 访问。VMware 建议在 SSL VPN 部署中使用完全访问权限客户端以提高安全性。如果在早期版本中使用 WAT 功能，您必须在升级到 6.3.0 之前将其禁用。
- 已从 NSX Edge 中移除 IS-IS：从 NSX 6.3.0 开始，您无法从路由选项卡中配置 IS-IS 协议。
- 不再支持 vCNS Edge。在升级到 NSX 6.3.x 之前，您必须先升级到 NSX Edge。

常规行为变化

如果具有多个 vSphere Distributed Switch，并在其中的一个 vSphere Distributed Switch 上配置了 VXLAN，您必须将任何分布式逻辑路由器接口连接到该 vSphere Distributed Switch 上的端口组。从 NSX 6.3.6 开始，将在 UI 和 API 中实施该配置。在早期版本中，不会禁止您创建无效的配置。

API 移除和行为变化

API 错误处理变化

NSX 6.3.5 引入了以下错误处理变化：

- 如果 API 请求导致在 NSX Manager 上发生数据库异常，则响应为“500 内部服务器错误” (*500 Internal Server Error*)。在以前的版本中，NSX Manager 响应为 *200 OK*，即使请求失败也是如此。
- 在需要提供请求正文时，如果发送的 API 请求正文为空，则响应为“400 请求错误” (*400 Bad request*)。在以前的版本中，NSX Manager 响应为“500 内部服务器错误” (*500 Internal server error*)。
- 如果在 API GET /api/2.0/services/policy/securitygroup/{ID}/securitypolicies 中指定不正确的安全组，则响应为“404 未找到” (*404 Not found*)。在以前的版本中，NSX Manager 响应为 *200 OK*。

备份和还原 API 默认值变化

从 6.3.3 开始，更改了两个备份和还原参数的默认值，以便与 UI 中的默认值相匹配。以前，`passiveMode` 和 `useEPSV` 默认为 *false*，现在默认为 *true*。这会影响以下 API：

- PUT /api/1.0/appliance-management/backuprestore/backupsettings
- PUT /api/1.0/appliance-management/backuprestore/backupsettings/ftpsettings

删除防火墙配置或默认区域

- 从 6.3.0 开始，如果指定默认区域，则会拒绝以下请求：DELETE /api/4.0/firewall/globalroot-0/config/layer2sections|layer3sections/sectionId
- 引入了一个新方法以获取默认配置。请使用该方法的输出替换整个配置或任何默认区域：
 - 使用 GET /api/4.0/firewall/globalroot-0/defaultconfig 获取默认配置
 - 使用 PUT /api/4.0/firewall/globalroot-0/config 更新整个配置
 - 使用 PUT /4.0/firewall/globalroot-0/config/layer2sections|layer3sections/{sectionId} 更新单个区域

defaultOriginate 参数：

从 NSX 6.3.0 开始，仅从逻辑（分布式）路由器 NSX Edge 设备的以下方法中移除 defaultOriginate 参数：

- GET/PUT /api/4.0/edges/{edge-id}/routing/config/ospf
- GET/PUT /api/4.0/edges/{edge-id}/routing/config/bgp
- GET/PUT /api/4.0/edges/{edge-id}/routing/config

若在 NSX 6.3.0 或更高版本中将 defaultOriginate 设为 true，逻辑（分布式）路由器 Edge 设备将失败。

从 NSX Edge 路由中移除了所有 IS-IS 方法。

- GET/PUT/DELETE /4.0/edges/{edge-id}/routing/config/isis
- GET/PUT /4.0/edges/{edge-id}/routing/config

CLI 移除和行为变化

不要在 NSX Controller 节点上使用不支持的命令

不要使用未列出的命令在 NSX Controller 节点上配置 NTP 和 DNS。这些命令不受支持，不要在 NSX Controller 节点上使用这些命令。请仅使用 NSX CLI 指南中列出的命令。

升级说明

- [常规升级说明](#)
- [NSX 组件的升级说明](#)
- [FIPS 的升级说明](#)

注意：有关影响安装和升级的已知问题列表，请参见[安装和升级已知问题](#)一节。

常规升级说明

- 要升级 NSX，您必须执行完整的 NSX 升级，包括主机集群升级（将升级主机 VIB）。有关说明，请参见《[NSX 升级指南](#)》，包括“[升级主机集群](#)”部分。
- 系统要求：有关安装和升级 NSX 时的系统要求信息，请参见 NSX 文档中的 [NSX 的系统要求](#) 部分。
- 从 NSX 6.x 升级的途径：[VMware 产品互操作性列表](#) 提供了有关从 VMware NSX 升级的途径的详细信息。
- 在《[NSX 升级指南](#)》中介绍了跨 vCenter NSX 升级。
- 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 后，无法对 NSX 进行降级。
- 要验证是否成功升级到 NSX 6.3.x，请参见[知识库文章 2134525](#)。
- 不支持从 vCloud Networking and Security 升级到 NSX 6.3.x。您必须先升级到支持的 6.2.x 版。
- 互操作性：在升级之前，请检查 [VMware 产品互操作性列表](#) 以了解所有相关的 VMware 产品。
 - 升级到 vSphere 6.5a 或更高版本：从 vSphere 5.5 或 6.0 升级到 vSphere 6.5a 或更高版本时，您必须先升级到 NSX 6.3.x。请参见《[NSX 升级指南](#)》中的“[在 NSX 环境中升级 vSphere](#)”。
 - 注意：NSX 6.2.x 与 vSphere 6.5 不兼容。
 - 升级到 NSX 6.3.3 或更高版本：满足 NSX 互操作性所需的 vSphere 的最低支持版本在 NSX 6.3.2 和 NSX 6.3.3 之间发生变化。有关详细信息，请参见 [VMware 产品互操作性列表](#)。
- 合作伙伴服务兼容性：如果您的站点使用 VMware 合作伙伴服务实施客户机侦测或网络侦测，您必须在升

级之前查阅《[VMware 兼容性指南](#)》以确认供应商的服务与此版本的 NSX 兼容。

- **Networking and Security 插件**：在升级 NSX Manager 后，您必须注销并重新登录到 vSphere Web Client。如果未正确显示 NSX 插件，请清除浏览器缓存和历史记录。如果 Networking and Security 插件未显示在 vSphere Web Client 中，请重置 vSphere Web Client 服务器，如《[NSX 升级指南](#)》中所述。
- **无状态环境**：在无状态主机环境中执行 NSX 升级时，新的 VIB 将在 NSX 升级过程中预先添加到主机映像配置文件。因此，无状态主机上的 NSX 升级过程遵循以下顺序：
在 NSX 6.2.0 之前，您只能在 NSX Manager 上通过单个 URL 找到适用于特定版本的 ESX 主机的 VIB。（这意味着管理员只需知道一个 URL，而不管使用的是哪种 NSX 版本。）在 NSX 6.2.0 和更高版本中，新的 NSX VIB 通过不同的 URL 提供。要找到合适的 VIB，您必须执行以下步骤：

1. 从 `https://<NSXManager>/bin/vdn/nwfabric.properties` 中找到新的 VIB URL。
2. 从相应的 URL 获取所需 ESX 主机版本的 VIB。
3. 将这些 VIB 添加到主机映像配置文件。

NSX 组件的升级说明

NSX Manager 升级

- **重要信息**：如果将 NSX 6.2.0、6.2.1 或 6.2.2 升级到 NSX 6.3.5 或更高版本，您必须在开始升级之前按照解决办法进行操作。有关详细信息，请参见 [VMware 知识库文章 000051624](#)。
- 如果使用 SFTP 进行 NSX 备份，请在升级到 6.3.x 后更改为 `hmac-sha2-256`，因为不支持 `hmac-sha1`。有关 6.3.x 中支持的安全算法列表，请参见 [VMware 知识库文章 2149282](#)。
- 如果要从 NSX 6.3.3 升级到 NSX 6.3.4 或更高版本，必须先按照 [VMware 知识库文章 2151719](#) 中的解决办法说明进行操作。
- 在将 NSX Manager 升级到 NSX 6.3.6 或更高版本时，将在升级过程中自动创建备份并保存在本地。有关详细信息，请参见[升级 NSX Manager](#)。

控制器升级

- 在 NSX 6.3.3 中，NSX Controller 设备磁盘大小从 20GB 变为 28GB。
- NSX Controller 集群必须包含三个控制器节点才能升级到 NSX 6.3.3。如果少于三个控制器，您必须在开始升级之前添加控制器。请参见[部署 NSX Controller 集群](#)以了解相应的说明。
- 在 NSX 6.3.3 中，NSX Controller 的底层操作系统发生变化。这意味着，从 NSX 6.3.2 或更低版本升级到 NSX 6.3.3 或更高版本而不是执行就地软件升级时，将每次删除一个现有的控制器，并使用相同的 IP 地址部署基于 Photon OS 的新控制器。

在删除控制器时，还会删除任何关联的 DRS 反关联性规则。您必须在 vCenter 中创建新的反关联性规则，以防止新的控制器虚拟机位于同一主机上。

有关控制器升级的详细信息，请参见[升级 NSX Controller 集群](#)。

主机集群升级

- 在 NSX 6.3.3 中，NSX VIB 名称发生了变化。如果安装了 NSX 6.3.3 或更高版本，`esx-vxlan` 和 `esx-vsip` VIB 将替换为 `esx-nsxv`。
- **主机上无重新引导的升级和卸载**：在 vSphere 6.0 和更高版本上，升级到 NSX 6.3.x 后，任何后续的 NSX VIB 更改都不需要重新引导，但主机必须进入维护模式才能完成 VIB 更改。

在执行以下任务期间，不需要重新引导主机：

- 在 ESXi 6.0 或更高版本上从 NSX 6.3.0 升级到 NSX 6.3.x。

- 在将 ESXi 从 6.0 升级到 6.5.0a 或更高版本之后安装必须的 NSX 6.3.x VIB。

注意：ESXi 升级仍需要重新引导主机。

- 在 ESXi 6.0 或更高版本上卸载 NSX 6.3.x VIB。

在执行以下任务期间，需要重新引导主机：

- 从 NSX 6.2.x 或更低版本升级到 NSX 6.3.x（任何 ESXi 版本）。
- 在 ESXi 5.5 上从 NSX 6.3.0 升级到 NSX 6.3.x。
- 在将 ESXi 从 5.5 升级到 6.0 或更高版本之后安装必须的 NSX 6.3.x VIB。
- 在 ESXi 5.5 上卸载 NSX 6.3.x VIB。
- 主机可能会停滞在正在安装状态：在大规模的 NSX 升级过程中，主机可能会长时间停滞在正在安装状态。出现这种情况可能是由于卸载旧 NSX VIB 的过程中出现问题。在这种情况下，与此主机关联的 EAM 线程将在 VI Client 任务列表中被报告为停滞。

解决办法：执行以下操作：

- 使用 VI Client 登录到 vCenter。
- 右键单击停滞的 EAM 任务并将其取消。
- 从 vSphere Web Client 中，对集群执行“解决”操作。停滞的主机现在可能显示为“正在进行”。
- 登录到主机，然后执行重新引导以强制完成该主机上的升级操作。

NSX Edge 升级

- 在 NSX 6.3.0 中，已更改 NSX Edge 设备磁盘大小：
 - 精简、中型、大型：1 个磁盘 584 MB + 1 个磁盘 512 MB
 - 超大型：1 个磁盘 584 MB + 1 个磁盘 2 GB + 1 个磁盘 256 MB
- 在升级 NSX Edge 设备之前，必须为 NSX 准备主机集群：从 6.3.0 开始，不再支持通过 VIX 通道在 NSX Manager 和 Edge 之间进行的管理平面通信。仅支持消息总线通道。从 NSX 6.2.x 或更低版本升级到 NSX 6.3.0 或更高版本时，您必须确认为 NSX 准备了部署 NSX Edge 设备的主机集群，并且消息基础架构状态为绿色。如果没有为 NSX 准备主机集群，NSX Edge 设备升级将失败。有关详细信息，请参见《NSX 升级指南》中的[升级 NSX Edge](#)。

- 升级 Edge 服务网关 (ESG)：

从 NSX 6.2.5 开始，将在升级 NSX Edge 时执行资源预留。如果在资源不足的集群上启用 vSphere HA，由于违反 vSphere HA 限制，升级操作可能会失败。

为了避免此类升级失败，请在升级 ESG 之前执行以下步骤：

如果在安装或升级时没有明确设置值，NSX Manager 将使用以下资源预留。

NSX Edge 规格大小	CPU 预留	内存预留
精简	1000MHz	512 MB
中型	2000MHz	1024 MB
大型	4000MHz	2048 MB
超大型	6000MHz	8192 MB

- 始终确保您的安装遵循为 vSphere HA 建议的最佳做法。请参见 [VMware 知识库文章 1002080](#) 文档。

2. 使用 NSX 优化配置 API:

PUT <https://<NSXManager>/api/4.0/edgePublish/tuningConfiguration>

确保 `edgeVCpuReservationPercentage` 和 `edgeMemoryReservationPercentage` 值在相应规格大小的可用资源范围内（请参见上表以了解默认值）。

- 在启用 vSphere HA 并部署 Edge 时，请禁用 vSphere 的虚拟机启动选项。在将 6.2.4 或更低版本的 NSX Edge 升级到 6.2.5 或更高版本后，您必须为已启用 vSphere HA 并部署 Edge 的集群中的每个 NSX Edge 禁用 vSphere 虚拟机启动选项。为此，请打开 vSphere Web Client，找到 NSX Edge 虚拟机所在的 ESXi 主机，单击“管理”>“设置”并在“虚拟机”下面选择“虚拟机启动/关机”，单击“编辑”并确保该虚拟机处于手动模式（即，确保该虚拟机未添加到自动启动/关机列表中）。
- 在升级到 NSX 6.2.5 或更高版本之前，确保所有的负载均衡器密码列表均以冒号分隔。如果密码列表使用逗号等其他分隔符，请对

https://nsxmgr_ip/api/4.0/edges/EdgeID/loadbalancer/config/applicationprofiles 执行 PUT 调用，将 `<clientSsl>` 和 `<serverSsl>` 中的每个 `<ciphers>` 列表替换为以冒号分隔的列表。例如，请求正文中的相关分段可能类似于以下内容。对所有的应用程序配置文件重复此过程：

```
<applicationProfile>
  <name>https-profile</name>
  <insertXForwardedFor>false</insertXForwardedFor>
  <sslPassthrough>false</sslPassthrough>
  <template>HTTPS</template>
  <serverSslEnabled>true</serverSslEnabled>
  <clientSsl>
    <ciphers>AES128-SHA:AES256-SHA:ECDHE-ECDSA-AES256-SHA</ciphers>
    <clientAuth>ignore</clientAuth>
    <serviceCertificate>certificate-4</serviceCertificate>
  </clientSsl>
  <serverSsl>
    <ciphers>AES128-SHA:AES256-SHA:ECDHE-ECDSA-AES256-SHA</ciphers>
    <serviceCertificate>certificate-4</serviceCertificate>
  </serverSsl>
  ...
</applicationProfile>
```

- 在早于 6.2.0 的 vROPs 版本中为负载均衡的客户端设置正确的密码版本：早于 6.2.0 的 vROPs 版本中的 vROPs 池成员使用 TLS 版本 1.0，因此，您必须在 NSX 负载均衡器配置中设置 `"ssl-version=10"` 以显式设置监控扩展值。请参见《NSX 管理指南》中的“[创建服务监控器](#)”以了解相应的说明。

```
{
  "expected" : null,
  "extension" : "ssl-version=10",
  "send" : null,
  "maxRetries" : 2,
  "name" : "sm_vrops",
  "url" : "/suite-api/api/deployment/node/status",
  "timeout" : 5,
  "type" : "https",
  "receive" : null,
  "interval" : 60,
  "method" : "GET"
}
```

- 现在，客户机侦测虚拟机在计算机上的 XML 文件中包含额外的主机标识信息。在登录到客户机侦测虚拟机时，“/opt/vmware/etc/vami/ovfEnv.xml” 文件应包含主机标识信息。

FIPS 的升级说明

从 NSX 6.3.0 之前的 NSX 版本升级到 NSX 6.3.0 或更高版本时，不能在完成升级之前启用 FIPS 模式。如果在完成升级之前启用 FIPS 模式，将中断升级的组件和未升级的组件之间的通信。有关详细信息，请参见《NSX 升级指南》中的“[了解 FIPS 模式和 NSX 升级](#)”。

- 在 OS X Yosemite 和 OS X El Capitan 上支持的密码：如果在 OS X 10.11 (El Capitan) 上使用 SSL VPN 客户端，您可以使用 AES128-GCM-SHA256、ECDHE-RSA-AES128-GCM-SHA256、ECDHE-RSA-AES256-GCM-SHA38、AES256-SHA 和 AES128-SHA 密码进行连接，使用 OS X 10.10 (Yosemite) 的客户端只能使用 AES256-SHA 和 AES128-SHA 进行连接。
- 在完成到 NSX 6.3.x 的升级之前，不要启用 FIPS。有关详细信息，请参见《NSX 升级指南》中的“[了解 FIPS 模式和 NSX 升级](#)”。
- 在启用 FIPS 之前，请确认任何合作伙伴解决方案都已通过 FIPS 模式认证。请参见《[VMware 兼容性指南](#)》和相关的合作伙伴文档。

FIPS 合规性

- NSS 和 OpenSwan: NSX Edge IPsec VPN 使用 Mozilla NSS 加密模块。由于严重的安全问题，该版本的 NSX 使用尚未进行 FIPS 140-2 验证的较新 NSS 版本。VMware 确认该模块正常工作，但不再正式进行验证。
- NSS 和密码输入: NSX Edge 密码哈希处理使用 Mozilla NSS 加密模块。由于严重的安全问题，该版本的 NSX 使用尚未进行 FIPS 140-2 验证的较新 NSS 版本。VMware 确认该模块正常工作，但不再正式进行验证。
- 控制器和集群 VPN: NSX Controller 使用 IPsec VPN 连接控制器集群。IPsec VPN 使用 VMware Linux 内核加密模块（Photon 1 环境），目前正在对该模块进行 CMVP 验证。

文档修订历史

2018 年 11 月 15 日：第一版。

2019 年 3 月 3 日：第二版。添加了已解决的问题 2249307。

2019 年 5 月 13 日：第三版。更新了“主机集群升级”部分。

已解决的问题

已解决的问题分为以下几类。

- [已解决的逻辑网络和 NSX Edge 问题](#)
- [已解决的一般问题](#)
- [已解决的 NSX Controller 问题](#)
- [已解决的 NSX Manager 问题](#)
- [已解决的安装和升级问题](#)
- [已解决的安全服务问题](#)

已解决的逻辑网络和 NSX Edge 问题

- 已修复问题 2207483：东西向和南北向路由流量均具有较高的延迟
生成路由流量的虚拟机 TxWorld 占用 100% 的 CPU，从而导致较高的延迟。
- 已修复问题 2188666：无法使用 SSLVPN Linux 客户端 CLI 连接到端口号为 5 位数的网关

需要使用 Linux 上的 SSLVPN 客户端 GUI 来连接到端口号为 5 位数的网关，这种方法适用于 GUI，而 SSLVPN Linux CLI 最多只能用于连接端口号为 4 位数的网关。

- **已修复问题 2185457：桥接工作负载的网络延迟增加**
桥接网络上具有高流量 (pps) 的工作负载可能会导致 VLAN 和 VXLAN 之间出现延迟。
- **已修复问题 2182874：如果站点之间存在重叠的 VDR ID，则无法使用 VDR ID**
当尝试将某个站点纳入多 VC 中时，如果多个站点的分段范围存在重叠，则必须更改该站点的分段范围。
- **已修复问题 2181650：在发送 ARP 请求以刷新 ARP 条目时，接受将 GARP 作为有效的回复**
某些旧设备将 GARP 作为 ARP 请求回复发送。
- **已修复问题 2181435：在 ESX 5.5 中，hostd 在统计信息轮询期间发生崩溃**
在 ESX 5.5 中，hostd 在统计信息轮询期间发生崩溃。需要重新启动 hostd。
- **已修复问题 2179054：避免在 NSX 安装和升级过程中重新启动 IXGBE 驱动程序**
主机上的服务会出现 5-10 秒的网络中断。
- **已修复问题 2178950：启用 HA 后，流量中断，或者同一 Edge 在 vCenter 中有两个以上的虚拟机**
启用 HA 后，流量发生中断，或者同一 Edge 在 vCenter 中有两个以上的虚拟机。通过编辑设备设置或者更改设备位置来执行还原操作，会导致虚拟机滞留，从而导致网络中断。
- **已修复问题 2177514：在某些情况下，DaD ping 会被转发回来，从而导致 DaD 进程检测到重复的 IP 地址**
系统事件报告虚假的检测到重复 IP 的信息。
- **已修复问题 2176316：防火墙规则中的 Edge 名称未更新**
从 Edge UI 中更改 Edge 名称之后，防火墙 UI 继续显示旧的 Edge 名称
- **已修复问题 2172005：发出“show ip bgp”CLI 命令时，BGP 邻居关系出现抖动**
当 BGP 获知路由 AS_PATH 超过 126 个字符，且发出“show ip bgp”命令时，路由堆栈会重新启动。在 BGP 重新汇聚之前，路由会出现振荡，可能发生流量中断。
- **已修复问题 2171616：如果无法解析 ESG 主机名，SSL VPN Windows 客户端进程会崩溃**
当配置了 HTTP 代理，且无法解析 ESG 主机名时，客户端进程会崩溃。
- **已修复问题 2167176：对于启用了 HA 的 DLR Edge，tmpfs 分区变满**
启用 HA 之后，/var/run 目录 (tmpfs) 会完全填满。如果此目录被填满，会导致任何配置都无法正常工作。
- **已修复问题 2164068：启用 HA 一段时间后，Edge 的 tmpfs 分区变满**
使用 rsync 在 HA 对中的 Edge 虚拟机之间同步文件。由于 rsync 的编译方式，每次定期调用 rsync 都会生成一个错误日志消息，该消息保存在 tmpfs 分区上的日志文件中。一段时间后，分区会逐渐变满，这会严重影响 Edge 的正常操作。
- **已修复问题 2156094：无法使用 SSL VPN Linux 客户端 CLI 连接到端口号为五位数的网关**
需要使用 Linux 上的 SSL VPN 客户端 GUI 来连接到端口号为五位数的网关，这种方法适用于 GUI，而 SSL VPN Linux CLI 最多只能用于连接端口号为四位数的网关。
- **已修复问题 2152060：Edge 上的监控服务引擎 (Nagios) 存在内存泄漏**
当负载均衡器的配置使用的是无内存监控服务时，负载均衡器将无法正常工作。
- **已修复问题 2140512：升级到 6.3.x 或更高版本之后，如果 MP 数据库中缺少传输区域 (vdnscope) 条目，会导致 VXLAN 和逻辑网络出现错误**
为 NSX 准备的集群上出现 VXLAN 和逻辑网络错误。
- **已修复问题 2134760：已成功完成 SSL VPN Mac 客户端安装，但无法运行该应用程序**
即使已成功安装客户端，也无法将其打开。

- 已修复问题 2100704：在某些情况下，NSX Edge 可能会丢失与 NSX Manager 的 VMCI 连接 Edge 变得无法管理，从而导致无法向 Edge 推送配置。
- 已修复问题 2092516：多个监控工作线程同时更新池成员状态
负载均衡器无法正常工作，从而某些流量会缓慢发送到不正常的服务器上，或者正常服务器没有任何可以处理的流量。
- 已修复问题 2078866：主机重新引导时，refreshHostdNetstackCache() 中的 nsxv-vib 失败
VXLAN Rx 吞吐量性能可能会下降。
- 已修复问题 2028337：当 Edge CPU 占用率超过 90% 时，不显示前五个 CPU 消耗最大的进程
当 Edge CPU 占用率超过 90% 时，系统会向管理器发送一份通知，其中将显示自 Edge 启动以来前五个 CPU 消耗最大的进程列表。该列表很可能不显示此刻前五个 CPU 消耗最大的进程，从而很难诊断 CPU 使用情况问题。
- 已修复问题 1983497：如果在网桥进行故障切换的同时更改网桥配置，将显示紫色屏幕
如果在网桥进行故障切换的同时更改网桥配置，可能会导致死锁并显示紫色屏幕。产生死锁的可能性很小。
- 已修复问题 2181633：针对客户机虚拟机子接口 IP 地址的 ARP 抑制失败。
第一次对这些接口进行 ARP 解析比平时所需的时间（1 秒）要稍长一些。
- 已修复问题 2170329：DNS 配置无法应用于 SSLVPN Windows 客户端接口
DNS 查询失败，从而影响访问。

已解决的一般问题

- 已修复问题 2183198：从没有端口的 ToR 交换机检索端口时，UI 显示错误消息
如果硬件网关的物理交换机没有端口，当尝试从该交换机获取端口时，NSX UI 会弹出错误。尝试检索端口信息时，UI 中显示“无法获取清单信息”(Unable to fetch inventory information) 错误。
- 已修复问题 2176000：管理平面发送的消息与主机预期接收的消息之间的编码差异，导致 DVS 的上行链路端口无效，进而致使 MAC 解析失败
DLR 无法解析不同 ESXi 主机上虚拟机的 MAC 地址。
- 已修复问题 2170413：API /api/3.0/ai/directorygroup 无法正常工作
后端抛出 NullPointerException 异常，并且 API 返回错误。无法自动执行工作流。
- 已修复问题 2170395：domain_object 与 ai_group 表不同步
加载“服务编排”页面时，包含空组 ID 列表的 SQL 会引发 SQLGrammarException。
- 已修复问题 2131680：多播数据包命中拒绝防火墙规则时，导致在 VMkernel 日志中记录过多的日志。
VMkernel 日志中的日志记录过多会导致主机停止日志记录。
- 已修复问题 2129177：如果升级过程中在向后兼容模式下删除或移除了 GI-SVM，通过客户机侦测 (GI) 的身份防火墙将无法正常工作，除非升级了 GI 集群
身份防火墙将无法正常工作，并且不显示与身份防火墙相关的任何日志。身份防火墙保护将挂起，除非升级了集群。
- 已修复问题 2105632：USVM 尝试与 Google（外部）NTP 服务器同步时间
已修改时间同步服务以防止出现该行为。
- 已修复问题 2003396：如果配置了大量路由，则在重新引导后或者在新主机加入后，DLR LIF/路由将丢失。
路由不会按照配置原样显示。
- 问题 1960383：在很短的时间内删除大量清单对象时，网络创建由于超时而失败
发生网络创建超时是因为，在 NSX 中创建 DVPG 出现延迟。

- 已修复问题 2058770：vCenter 上发生的登录事件过多，vCenter SSO 服务器出现高负载情况
当 vCenter SSO 用户在短时间内发出大量 NSX API 请求时，vCenter SSO 服务器会遇到登录事件过多和高负载问题。这可能会导致行为迟缓。
- 已修复问题 2046427：更改 vmknics 或 LS dvs 端口组绑定策略会导致 DP 中断
在主机准备 (VXLAN) 过程中，如果用户设置 vmknics 绑定策略，会相应地设置 DVS 上的上行链路绑定策略。所创建的新逻辑交换机 dvs pg 也会收到此绑定策略。
- 已修复问题 2178339：rsyslog 8.15.0-7.ph1 移除了 systemd 服务文件中的 ExecReload 行，导致 /var/log/syslog 和 /var/log/messages 无法妥善地轮换日志文件
这会导致 /var/log 分区占用 100% 的磁盘空间，进而导致新日志无法写入。
- 已修复问题 2146879：在独立设置中，强制同步不会同步 ToR 和 ToR 绑定
在独立设置中，如果管理平面和控制器之间的 HW 绑定或 HW 传输节点配置不同步，则强制同步无法同步配置。如果 ToR 绑定不同步，则无法将 ToR 配置同步到控制器。
- 已修复问题 2146749：ESXi 主机重新引导后会丢失区域 ID 配置
主机接收错误的 localeId 并刷新相应的路由。
- 已修复问题 2200396：故障切换后，在辅助站点中的 ESXi 主机上重新创建 VDR 实例
故障切换后约 40 秒，会出现通信中断和网络中断。
- 已修复问题 2100296：在 vCenter/PSC 上禁用 SSL/TLS1.0 之后，NSX 6.3.5 Web 客户端插件不显示任何 NSX Manager
在 vCenter 上禁用 SSL/TLS1.0，NSX 会中断与 vCenter、NSX 或 ESX 的通信。vCenter 应用程序将无法与 NSX Manager 通信。
- 已修复问题 2077492：NSX Manager 为已存在的 ipsec 站点自动创建 ipsecsite ID
 - NSX Manager 为已存在的 ipsec 站点自动创建 ipsecsite ID。
 - NSX for vSphere 从 6.2.x 升级到 6.3.5 或 6.4.0a 可能会为 IPSec 站点引入重复的 siteID。
 - 引入了重复 siteID 之后，下一个 IPSec 配置会失败。
 - 您会看到类似于以下内容的错误消息：[13646] [Ipsec] 找到重复的 Ipsec 站点 ID ipsecsite-id ([13646] [Ipsec] Duplicate Ipsec site Ids ipsecsite-id found)。
- 已修复问题 2177097：使用 API 调用 /api/2.0/vdn/config/segments 创建具有 1 个分段 ID 的池时，创建过程会失败并显示错误消息“分段 ID 超出范围，有效范围为 5000-16777215” (Segment id is out of range, valid range is 5000-16777215)
在使用 API 调用 /api/2.0/vdn/config/segments 时，如果您提供的开始值和结束值相同，则创建过程会失败并显示错误消息。
- 已修复问题 2172267：在主机无响应时删除 NSX Edge 会导致 vCenter 中出现孤立对象
NSX Manager 上的 Edge 实例被删除，但 Edge 设备仍然显示在 vCenter 中并提供数据路径，直到 NSX Manager 将此 Edge 标记为孤立并在删除清理过程中将其删除。无法从 NSX Manager 中删除 Edge 设备。
- 已修复问题 2097255：在 NSX Manager 设备上启用 FIPS 后，不会发送 SNMP 陷阱
未收到 SNMP 陷阱。

已解决的 NSX Controller 问题

- 已修复问题 2181306：控制器内存不足，无法正常提供服务
控制器支持通过 SSH 接口查询集群成员资格和状态。如果客户端访问此接口并且未关闭会话，则控制器会将这些会话一直保持为活动状态。有足够多的会话处于打开状态时，控制器会出现内存不足问题。

已解决的 NSX Manager 问题

- 已修复问题 2171653：NSX Manager 上的安全扫描报告“未检测到 HTTP 安全标头”
安全扫描报告该问题。可能发生了点击劫持 (Clickjacking)。

- 已修复问题 2161066：处理 API 响应时，连接 Usage Meter 与 NSX Manager 失败或出现无效 XML 字符错误
连接 Usage Meter 与 NSX Manager 失败并出现错误。
- 已修复问题 2145195：NSX Manager 发出所有 USVM 的检测信号警示并显示高 CPU 占用率
NSX Manager 发出警示，指出所有 USVM 均未响应检测信号。Postgres 会话导致 CPU 占用率较高。
- 已修复问题 2144825：由于 nsx-tcserver-wrapper.log 文件过多，Manager 根分区已满
NSX UI 无法访问，并且许多其他服务由于空间不足而停止工作。
- 已修复问题 2141490：NSX Manager 和 Controller 上的 ToR 绑定不同步
无法修改逻辑交换机上的 HW 绑定或删除配置。UI 显示以下错误：“未能在控制器上执行该操作。{0}” (Failed to do operation on the Controller. {0})
- 已修复问题 2066631：使用安全管理员用户角色登录并选择虚拟机时，会显示错误消息弹出窗口
显示错误消息弹出窗口“无权访问全局对象和函数 library.tagging。请确认函数和对象访问权限范围” (There is no authority to access object global and function library.tagging. Confirm the authority of the function and object access scope)。
- 已修复问题 2189810：当第三方服务插入解决方案向 NSX Manager 发出 API 调用，以检索在服务插入中配置的所有安全组/IPSet 时，受 PAN 保护的客户机虚拟机将丢弃流量
NSX Manager 为 IPSet 或包含 IPSet 的安全组返回空配置。因此，给第三方管理器的 IPSet 或包含 IPSet 的安全组报告为空。因为没有规则匹配且命中默认的拒绝规则，受 PAN 或其他第三方防火墙设备保护的客户机虚拟机会丢弃流量。运行 API 调用 https://NSXMGR_IP/api/2.0/si/serviceprofile/serviceprofile-10/containeraset 不会返回 IPSet 或包含 IPSet 的安全组的任何 IP。

因为没有规则匹配且命中默认的拒绝规则，受 PAN 或其他第三方防火墙设备保护的所有客户机虚拟机会丢弃流量。

- 已修复问题 2178700：如果任一 VDR LIF 正在使用已删除的虚拟线路，则 NSX Manager 无法将 VDR LIF 信息同步到控制器
VDR LIF 操作失败，导致用户无法修改 LIF 配置。
- 已修复问题 2249307：在 ESXi 主机重新连接到 NSX Manager 时，ESXi 主机上的区域设置 ID 重置为默认值
缺少 DLR 路由。DLR 不再路由流量。主机收到错误的区域设置 ID，并且不保留预期的 DLR 路由。

已解决的安装和升级问题

- 已修复问题 2133143：NSX 数据库中存在失效的集群条目
从 6.2.2 升级到 6.2.9 之后，NSX 数据库中存在一些失效的集群条目。
- 已修复问题 2112773：控制器升级失败
控制器在从 6.2.4 到 6.3.6 的升级期间失败。

已解决的安全服务问题

- 已修复问题 2098645：安全组引用已删除的 AD 组时出现空指针异常
如果删除一个 AD 组 (ai_group)，并且某个安全组引用此删除的 AD 组，安全组->虚拟机转换将引发空指针异常。“服务编排”页面将不会正确加载。
- 已修复问题 2032988、2032990、2032991：CVE-2017-5753、CVE-2017-5715 (Specter) 和 CVE-2017-5754 (Meltdown) 带来的安全漏洞
因 CVE-2017-5753、CVE-2017-5715 (Specter) 和 CVE-2017-5754 (Meltdown) 漏洞而造成的潜在安全问题。

已知问题

已知问题分为以下几类。

- [安装和升级已知问题](#)
- [一般已知问题](#)

安装和升级已知问题

- 问题 2001988：在 NSX 主机集群升级期间，在升级集群中的每个主机时，“主机准备”选项卡中的“安装状态”为整个集群交替显示“未就绪”和“正在安装”
在 NSX 升级期间，为 NSX 准备的集群单击“可升级”将触发主机升级。对于配置了 DRS 全自动的集群，“安装状态”交替显示“正在安装”和“未就绪”，即使在后台正常升级了主机也是如此。

解决办法：这是一个用户界面问题，可以将其忽略。等待继续执行主机集群升级。

一般已知问题

- 问题 2158182：如果 DHCP 服务和使用本地链路 IP 的 HA 共享同一 vNic，则会导致 DHCP 更新数据包被丢弃
如果 HA 地址是本地链路地址 (169.x.x.x)，DR 可能会将 DHCP 更新单播数据包丢弃到该本地链路地址，这可能导致 DHCP 客户端更新失败。

解决办法：选择不带 DHCP 服务的 vNic 作为 HA 接口，或使用可路由的 IP 地址作为 HA 接口，例如 192.168.x.x

- 问题 1467382：无法编辑网络主机名
登录到 NSX Manager 虚拟设备并导航到“设备管理”后，单击“管理设备设置”，然后单击“设置”下的“网络”以编辑网络主机名，您可能会收到无效域名列表的错误。“搜索域”字段中指定的域名以空白字符而非逗号分隔时会发生此情况。NSX Manager 只接受以逗号分隔的域名。

解决办法：

1. 登录到 NSX Manager 虚拟设备。
2. 在“设备管理”下方，单击“管理设备设置”。
3. 在“设置”面板中，单击“网络”。
4. 单击 DNS 服务器旁边的“编辑”。
5. 在“搜索域”字段中，将所有空白字符替换为逗号。
6. 单击“确定”保存更改。

- 问题 1849042/1849043：在 NSX Edge 设备上配置密码时效后，管理员帐户锁定
如果在 NSX Edge 设备上为管理员用户配置了密码时效，在密码过期后的 7 天内，将在用户登录到设备时要求其更改密码。如果未更改密码，将导致锁定该帐户。此外，如果在登录时在 CLI 提示符下更改密码，新密码可能不符合 UI 和 REST 实施的强密码策略。

解决办法：为避免出现该问题，请始终在现有密码过期之前使用 UI 或 REST API 更改管理员密码。如果已锁定该帐户，也要使用 UI 或 REST API 配置新密码并对该帐户解除锁定。

- 问题 2204383：对于使用 sql cert9.db 的 Linux 版本，SSLVPN Linux 客户端无法验证其服务器证书
服务器验证失败，并显示内部错误消息。

解决办法：无。