

VMware NSX for vSphere 6.3.6 发行说明

VMware NSX for vSphere 6.3.6 | 2018 年 3 月 29 日发行 | 内部版本 8085122

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 6.3.6 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 6.3.6 的新增功能

NSX for vSphere 6.3.6 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 6.3.5](#)
- [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 /api/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 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 3 月 29 日：第一版。

2018 年 5 月 2 日：第二版。添加了已解决的问题 1993384。

2018 年 6 月 4 日：第三版。添加了已解决的问题 2058770。

2018 年 7 月 25 日：第四版。添加了已解决的问题 2019124 和 2021080。

2018 年 9 月 5 日：第五版。添加了已知问题 2186968。

2019 年 5 月 13 日：第六版。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。

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

已解决的一般问题

- 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 2003765：重置/重新引导或重新启动物理 TOR 设备后，NSX Controller 上的 TOR 管理器无法发送更新
如果重新加载 TOR，TOR OVSDDB 表中的虚拟机远程 MAC 会丢失。

解决办法：重新引导所有 NSX Controller。有关详细信息，请参见 VMware 知识库文章 [52074](#)。

- 已修复问题 2014220：不应直接在“init”中运行 netcpa 监控进程
在升级到 6.5 Update 1 后，主机处于无响应状态。请在“netcpa”而不是“init”组中运行 netcpa 监控进程。
- 已修复问题 2023494：如果在装有 Dell 插件的环境中部署 NSX 插件，则会在 vSphere Web Client 上显示“没有 NSX Manager” (No NSX manager) 错误。
在升级后，在 vSphere Web Client 上显示“没有可用的 NSX Manager” (No NSX Managers available) 错误。
- 已修复问题 2073125：将防病毒合作伙伴解决方案部署到集群失败，服务虚拟机一直处于“未知”状态
服务虚拟机一直处于“未知”状态，但 Eicar 检测正常工作，如果应用了安全组中的安全策略，则主机上运行的代理按预期方式保护环境。
- 已修复问题 2021080：由于 HostFirewallRuleset 错误，主机重新启动失败
主机与 vCenter 之间的连接中断，且无法重新连接。无法对主机执行操作。

已解决的安装和升级问题

- 已修复问题 2035026：在 Edge 升级时，发现网络中断大约 40-50 秒
在 Edge 升级期间，大约中断 40-50 秒。
- 已修复问题 2058636：在升级到 6.3.5 后，DLR 和 ESG 之间的路由环路在某些 BGP 配置中导致连接问题。
路由环路导致连接问题。
- 已修复问题 1977797：从 NSX 6.2.2 升级到 NSX 6.3.x 导致在 vSphere Web Client 中出现错误，并且主机显示错误
在将 NSX Manager 从 NSX 6.2.2 升级到 NSX 6.3.x 后，vSphere Web Client 显示“内部服务器错误” (Internal Server Error)，并且主机集群显示错误。

已解决的 NSX Manager 问题

- 已修复问题 2012045：由于 Edge 处于只读文件系统模式，NSX Manager CPU 使用率较高。
由于 NSX Manager 保持 100% CPU 使用率，并从 Edge 收到大量只读文件系统事件，因此响应速度较慢。
- 已修复问题 1995891：在主 NSX Manager 上进行的更改未同步到辅助 NSX Manager。
如果从主 NSX Manager 中移除辅助 NSX Manager（辅助 NSX Manager 仍具有辅助角色），在辅助 NSX Manager 上没有任何迹象表明未接收任何更新。
- 已修复问题 1983902：在大型设置环境中，在 NSX Manager 重新引导后，netcpad 不会立即连接到 vsfwd。
在大型设置环境中，在 NSX Manager 重新引导后，netcpad 不会立即连接到 vsfwd。这对数据路径没有任何影响。系统会在 13 分钟后恢复，而无需进行干预。

已解决的 NSX Controller 问题

- 已修复问题 2003453：控制器日志包含大量网桥“无法添加/删除不存在的网桥实例的 MAC 记录 MacRecord” (Fail to add/delete a mac record MacRecord for non-existing bridge instance) 错

误。

在分片发生变化时，网桥无法将“加入”命令发送到控制器。

已解决的逻辑网络和 NSX Edge 问题

- 已修复问题 1753621：在具有专用本地 AS 的 Edge 将路由发送到 EBGP 对等项时，将从发送的 BGP 路由更新中删除所有专用 AS 路径
NSX for vSphere 目前存在一个限制，即，在 AS 路径仅包含专用 AS 路径时，无法与 eBGP 邻居共享完整 AS 路径。虽然这在大多数情况下是预期行为，但在某些情况下，管理员可能希望与外部 BGP 邻居共享专用 AS 路径。此项修复允许您更改外部 BGP 对等项的“专用 AS 路径”行为。此功能的默认行为是“移除专用 ASN”，这与之前版本的 NSX for vSphere 是一致的。
- 已修复问题 2014400：在禁用 Edge 上的防火墙功能后，备用 NSX Edge 开始响应 IPv6 流量。
在 NSX Edge 上启用了 IPv6 的情况下，如果触发故障切换，将使用备用 Edge 的 MAC 更新上游设备，因此，南北向流量可能会转发到不正确的 Edge。
- 已修复问题 2018810：在启用了 IPv6 的情况下，在启动 NSX Edge HA 故障切换后，不会发送邻居请求消息，从而导致丢弃流量。
来自南向虚拟机的流量停止。
- 已修复问题 2055195：在 NSX Edge 上尝试设置 IPv6 静态路由时，如果路由包含 /128 前缀，则可能不会在转发表中显示路由。
如果具有 /128 前缀，则可能无法正常重新配置 IPv6 静态路由。
- 已修复问题 2069428：在 NSX Edge 上禁用 IPv6 接口或子接口导致 Edge 重新引导。
在禁用 IPv6 接口和子接口（在 NSX Edge 中的静态路由上配置的下一跃点范围内）后，Edge 重新引导。
NSX Edge 不支持 IPv6 路由递归。

解决办法：移除下一跃点在分配给 vNIC 或子接口的 IPv6 地址范围内的静态路由，然后重试该操作。

- 已修复问题 1976378：在从 vCNS Edge 5.5.4 升级到 NSX 6.3.6 后，客户无法配置运行状况检查监控端口，也无法直接从 vCD 中进行任何更改。
客户无法配置运行状况检查监控端口，也无法直接从 vCD 中进行任何更改。

*解决办法：*使用 API 4.0 获取池成员 XML 配置，从 Edge 中删除该旧池配置，然后将 API 4.0 XML 配置重新添加到 Edge 中。

- 已修复问题 1967402：在 Edge 设备中使用易受攻击的旧 tcpdump 版本。
Edge 上的数据包捕获 CLI 使用 tcpdump 软件包捕获和显示数据包。使用的 tcpdump 软件包 (v4.9.0) 包含很多在更高版本中才修复的漏洞。因此，在使用数据包捕获 CLI 时，CLI 用户可能容易受到攻击。
- 已修复问题 1993384：SSLVPN 客户端无法从 IP 池获取 IP
客户端无法连接到专用网络，因为客户端自动重新连接到服务器时，不会从 IP 池分配任何 IP。而且不会清理从 IP 池分配给客户端的旧 IP。
- 已修复问题 2019124：进入被动模式后，Edge FTP 负载均衡器会丢弃数据包
FTP 被动模式适用于处于非透明模式的池，但不适用于处于透明模式的池。

已解决的安全服务问题

- 已修复问题 2000749：在特定的防火墙配置下，分布式防火墙停留在“正在发布”状态
如果您拥有的安全组所包含的 IPSet 中使用 0.0.0.0/0 作为排除成员、包含成员，或作为“包含交集 (AND) 的动态成员资格”的一部分，则分布式防火墙将停留在“正在发布”状态。
*解决办法：*在 IPSet 配置中使用 /0 以外的子网掩码。您可以将 0.0.0.0/0 定义为“0.0.0.0/1,128.0.0.0/1”。
- 已修复问题 2063415：在配置 L2 VPN 防火墙规则时，在 NSX Edge 日志中包含有关 --physdev-out 的警告消息

日志消息指出“在未桥接的流量的 OUTPUT、FORWARD 和 POSTROUTING 链中不再支持使用 --physdev-out” (using --physdev-out in the OUTPUT, FORWARD and POSTROUTING chains for non-bridged traffic is not supported anymore)。包含该消息是因为，Linux 内核 2.6.20 中移除了一个功能（延迟输出）。

- 已修复问题 2040064：将虚拟机作为静态成员添加到安全组需要很长时间。
如果以静态方式将虚拟机添加到一个安全组，并且该安全组连接到大量其他安全组，则添加速度较慢。
- 已修复问题 2029693：在 DFW 大型环境（具有 65K+ 个规则）中，用户可能花费更长的时间发布 DFW 规则。
在发布 10-15 分钟后，防火墙规则才会生效。

已知问题

已知问题分为以下几类。

- [一般已知问题](#)
- [安装和升级已知问题](#)
- [NSX Manager 已知问题](#)
- [NSX Controller 已知问题](#)
- [逻辑网络和 NSX Edge 已知问题](#)
- [安全服务已知问题](#)
- [监控服务已知问题](#)

一般已知问题

- 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。如果在很短的时间内删除大量清单对象，清单线程则需要较长时间来处理删除操作，这会导致在 NSX 上创建 DVPG 超时，网络创建失败。

解决办法：在未执行删除操作或执行较少的删除操作时创建网络。在未执行删除操作或执行较少的删除操作时重试失败的网络创建。

- 问题 1874863：在本地身份验证服务器上禁用/启用 sslvpn 服务后，无法使用更改的密码进行身份验证
在禁用并重新启用 SSL VPN 服务以及使用本地身份验证时，用户无法使用更改的密码登录。

有关详细信息，请参见 [VMware 知识库文章 2151236](#)。

- 问题 1702339：漏洞扫描程序可能会报告 Quagga bgp_dump_routes 漏洞 CVE-2016-4049
漏洞扫描程序可能会在 NSX for vSphere 中报告 Quagga bgp_dump_routes 漏洞 CVE-2016-4049。NSX for vSphere 使用 Quagga，但未启用 BGP 功能（包括漏洞）。可以放心地忽略该漏洞警示。

解决办法：由于该产品不存在漏洞，因此，不需要解决办法。

- 问题 1740625、1749975：Mac OS 上 Firefox 和 Safari 中的 UI 问题
如果在 Mac OS 中使用 Firefox 或 Safari，则“返回”导航按钮在 vSphere 6.5 Web Client 的“网络和安全”页面中的 NSX Edge 上无法正常工作，并且 UI 有时在 Firefox 中冻结。

解决办法：在 Mac OS 上使用 Google Chrome，或者单击“主页”按钮，然后根据需要继续操作。

- 问题 1700980：对于 CVE-2016-2775 漏洞安全修补程序，查询名称过长会导致在 lwresd 中出现段错误
NSX 6.2.4 随产品一起安装了 BIND 9.10.4，但它在 *named.conf* 中不使用 lwres 选项，因此，该产品不存在漏洞。

解决办法：由于该产品不存在漏洞，因此，不需要解决办法。

安装和升级已知问题

升级之前，请阅读本文档前文的[升级说明](#)一节。

- **问题 2072696：**如果存在某种无效的配置，将分布式逻辑路由器升级到 NSX 6.3.6 将失败
在 NSX 6.3.6 中添加了验证步骤，这是为了确保在配置了 VXLAN 并具有多个 vSphere Distributed Switch 的环境中，只能将分布式逻辑路由器接口连接到配置了 VXLAN 的 vSphere Distributed Switch。如果在环境中将 DLR 接口连接到未配置 VXLAN 的 vSphere Distributed Switch，则将 DLR 升级到 NSX 6.3.6 会失败。UI 不再显示不支持的 vSphere Distributed Switch。

解决办法：如果 DLR 升级由于该无效配置而失败，请使用 API 将任何未正确配置的接口连接到配置了 VXLAN 的 vSphere Distributed Switch 上的端口组。在有效配置后，再次尝试进行升级。使用 PUT `/api/4.0/edges/{edgeId}` 或 PUT `/api/4.0/edges/{edgeId}/interfaces/{index}` 更改接口配置。有关详细信息，请参见《*NSX API 指南*》。

- **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。

- **问题 1932907：**客户机侦测 SVM 升级失败
在尝试升级客户机侦测 SVM 时，GI SVM 的安装状态为“失败”。这可能适用于集群中的一个或多个主机的 GI-SVM。

解决办法：

1. 从 VC 中删除 GI-SVM。
2. 在 GI-SVM 服务部署窗格中单击**解决**。这会重新部署 GI-SVM。

- **问题 1747217：**准备 ESXi 主机导致 **muxconfig.xml.bad** 并且客户机侦测无法正常工作
如果某个虚拟机在 `muxconfig.xml` 中缺少“vmx path”，在 MUX 尝试分析该配置文件并且找不到“xml path”属性时，它将该配置文件重命名为“muxconfig.xml.bad”，并将错误“错误 - MUX 分析配置” (Error - MUX Parsing config) 发送到 USVM，同时关闭配置通道。

解决办法：从 vCenter 清单中移除孤立的虚拟机。

- **问题 1859572：**在 vCenter 6.0.0 版管理的 ESXi 主机上卸载 NSX VIB 6.3.x 版期间，主机继续处于维护模式
如果在集群上卸载 NSX VIB 6.3.x 版，工作流包括将主机置于维护模式，卸载 VIB 以及 EAM 服务将主机退出维护模式。不过，如果此类主机由 vCenter Server 6.0.0 版进行管理，则会导致在卸载 VIB 后主机停滞在维护模式。负责卸载 VIB 的 EAM 服务将主机置于维护模式，但无法将主机退出维护模式。

解决办法：手动将主机退出维护模式。如果主机由 vCenter Server 6.5a 及更高版本进行管理，则不会出现该问题。

- **问题 1435504：**从 6.0.x 或 6.1.x 升级到 6.3.x 后，HTTP/HTTPS 运行状况检查显示“关闭”，并且失败原因为“返回代码 127 超出范围 - 插件可能丢失” (Return code of 127 is out of bounds - plugin may be missing)
在 NSX 6.0.x 和 6.1.x 版本中，如果配置的 URL 没有双引号 ("")，将导致运行状况检查失败并显示以下错误：“返回代码 127 超出范围 - 插件可能丢失” (Return code of 127 is out of bounds - plugin may be missing)。该问题的解决办法是，在输入 URL 中添加双引号 ("")（对于 send/receive/expect 字段，不需要添加双引号）。不过，在 6.2.0 中修复了该问题，因此，如果从 6.0.x 或 6.1.x 升级到 6.3.x，额外的双引号将导致池成员在运行状况检查中显示为“关闭”。

解决办法：在升级后，从所有相关的运行状况检查配置的 URL 字段中移除双引号 ("")。

- **问题 1734245：“数据安全”导致升级到 6.3.0 的操作失败**
如果将“数据安全”配置为服务策略的一部分，则升级到 6.3.0 的操作将会失败。确保在升级之前从所有服务策略中移除“数据安全”。
- **问题 1801685：从 6.2.x 升级到 6.3.0 后因无法连接到主机而看不到 ESXi 上的筛选器**
在从 NSX 6.2.x 升级到 6.3.0 并将集群 VIB 升级到 6.3.0 之后，即使安装状态显示成功并且启用了防火墙，“通信通道运行状况”也会将“NSX Manager 到防火墙代理”连接和“NSX Manager 到控制平面代理”连接显示为关闭。这将导致防火墙规则发布和安全策略发布失败，以及 VXLAN 配置无法发送到主机。

解决办法：使用 API POST `https://<NSX-IP>/api/2.0/nwfabric/configure?action=synchronize` 对集群运行消息总线同步 API 调用。

API 正文：

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>{Cluster-MOId}</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

- **问题 1797929：消息总线通道在主机集群升级后出现故障**
在主机集群升级后，vCenter 6.0（和更低版本）不会生成事件“重新连接”，因此，NSX Manager 也不会主机上设置消息基础架构。vCenter 6.5 中已修复此问题。

解决办法：重新同步消息基础架构，如下所示：

POST `https://<ip>:/api/2.0/nwfabric/configure?action=synchronize`

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>host-15</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

- **问题 1768144：在升级或重新部署过程中，超出新限制的旧 NSX Edge 设备资源预留可能会导致失败**
在 NSX 6.2.4 及更低版本中，可以为 NSX Edge 设备指定任意大小的资源预留。NSX 不会强制实施最大值。
☒ 在将 NSX Manager 升级到 6.2.5 或更高版本后，如果现有 Edge 的预留资源（特别是内存）超过为所选规格大小新强制实施的最大值，则在 Edge 升级或重新部署（将会触发升级）过程中会失败。例如，如果用户在 6.2.5 以前版本的中型 Edge 上将内存预留指定为 1000 MB，并在升级到 6.2.5 后将设备大小更改为“精简”，则用户指定的内存预留将超过新强制实施的最大值（在此示例中，精简 Edge 的最大值为 512 MB），并且操作会失败。

有关从 NSX 6.2.5 开始的建议资源分配的信息，请参见[升级 Edge 服务网关 \(ESG\)](#)。

解决办法：使用设备 REST API PUT `https://<NSXManager>/api/4.0/edges/<edge-Id>/appliances/` 重新配置内存预留，使其值不超过为该规格大小指定的值，除此之外，无需进行任何其他设备更改。您可以在此操作完成后更改设备大小。

- **问题 1600281：客户机侦测的 USVM 安装状态在“服务部署”选项卡中显示为“失败”**
如果客户机侦测通用 SVM 的备用数据存储脱机或变得无法访问，可能需要重新引导或重新部署 USVM 才能恢复。

解决办法：重新引导或重新部署 USVM 以进行恢复。

- **问题 1660373：vCenter 强制实施已过期的 NSX 许可证**
从 vSphere 5.5 Update 3 或 vSphere 6.0.x 开始，vSphere Distributed Switch 包含在 NSX 许可证中。然而，如果 NSX 许可证已过期，vCenter 不允许将 ESX 主机添加到 vSphere Distributed Switch。

*解决办法：*您的 NSX 许可证必须处于活动状态，才能将主机添加到 vSphere Distributed Switch。

- 问题 1569010/1645525：在连接到 vCenter 5.5 的系统上，从 6.1.x 升级到 NSX for vSphere 6.2.3 时，“分配许可证密钥”窗口中的“产品”字段将 NSX 许可证显示为通用值“NSX for vSphere”，而不是比较具体的版本，如“NSX for vSphere - Enterprise”。

*解决办法：*无。

- 问题 1636916：在 vCloud Air 环境中，当 NSX Edge 版本从 vCNS 5.5.x 升级到 NSX 6.x 时，源协议值为“any”的 Edge 防火墙规则更改为“tcp:any, udp:any”
因此，ICMP 流量会被阻止，并且可能会出现丢弃数据包的情况。

*解决办法：*在升级您的 NSX Edge 版本之前，创建更加具体的 Edge 防火墙规则，并将“any”替换为具体的源端口值。

- 问题 1474238：执行 vCenter 升级后，vCenter 可能会与 NSX 断开连接
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 NSX 的连接。如果您已使用 root 用户名向 NSX 注册 vCenter 5.5，则会出现这种情况。在 NSX 6.2 中，使用 root 进行 vCenter 注册的做法已弃用。
注意：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。

*解决办法：*使用 administrator@vsphere.local 用户名向 NSX 注册 vCenter，而不要使用 root。

- 问题 1375794：关闭电源之前关闭代理虚拟机 (SVA) 的客户机操作系统
将主机置于维护模式时，会关闭所有服务设备的电源，而不是正常关闭。这可能会导致第三方设备出现错误。

*解决办法：*无。

- 问题 1112628：无法打开使用“服务部署”视图部署的服务设备的电源

*解决办法：*在继续操作之前，请确认以下事项：

- 虚拟机部署已完成。
- vCenter 任务窗格中不显示虚拟机的克隆和重新配置等正在进行的任务。
- 在虚拟机的 vCenter 事件窗格中，启动部署后会显示以下事件：

代理虚拟机 <vm name> 已置备。

将代理标记为可用，以继续执行代理工作流。

在这种情况下，删除服务虚拟机。在服务部署 UI 中，部署显示为“失败”。单击红色图标后，主机上将显示代理虚拟机不可用的警报。解决警报后，将重新部署和启动虚拟机。

- 问题 1413125：升级后无法重新配置 SSO
如果在 NSX Manager 上配置的 SSO 服务器是 vCenter Server 上的本机服务器，则在 vCenter Server 升级到 6.0 版本且 NSX Manager 升级到 6.x 版本后，无法在 NSX Manager 上重新配置 SSO 设置。

*解决办法：*无。

- 问题 1263858：SSL VPN 不向远程客户端发送升级通知
SSL VPN 网关不向用户发送升级通知。管理员必须手动通知远程用户 SSL VPN 网关（服务器）已更新，并通知用户必须更新其客户端。

*解决办法：*用户需要手动卸载旧版本的客户端并安装最新版本。

- 问题 1462319: “esxcli software vib list | grep esx” 命令输出不再包含 esx-dvfilter-switch-security VIB。
从 NSX 6.2 开始, esx-dvfilter-switch-security 模块包含在 esx-vxlan VIB 中。为 6.2 安装的 NSX VIB 只有 esx-vsip 和 esx-vxlan。在 NSX 升级至 6.2 的过程中, 已从 ESXi 主机中移除旧的 esx-dvfilter-switch-security VIB。
从 NSX 6.2.3 开始, 将随 esx-vsip 和 esx-vxlan NSX VIB 一起提供第三个 VIB esx-vmk。成功安装后将显示全部 3 个 VIB。

解决办法: 无。

- 问题 1481083: 升级后, 配置了明确故障切换绑定的逻辑路由器可能无法正确转发数据包
主机运行 ESXi 5.5 时, 明确故障切换 NSX 6.2 绑定策略不支持分布式逻辑路由器上的多个活动上行链路。

解决办法: 更改明确故障切换绑定策略, 以便只有一个活动上行链路, 其他上行链路处于待机模式。

- 问题 1411275: 在 NSX for vSphere 6.2 中进行备份和还原后, vSphere Web Client 不显示“网络和安全”选项卡
在升级到 NSX for vSphere 6.2 后, 当您执行备份和还原操作时, vSphere Web Client 不显示网络和安全选项卡。

解决办法: 还原 NSX Manager 备份后, 您将从 NSX Manager 虚拟设备管理门户注销。请等待几分钟, 然后再登录 vSphere Web Client。

- 问题 1764460: 完成主机准备后, 所有集群成员都显示处于“就绪”状态, 但集群级别错误地显示为“无效”
完成主机准备后, 所有集群成员都正确地显示处于“就绪”状态, 但集群级别显示为“无效”, 对此显示的原因是重新引导主机, 即使该主机已重新引导也是如此。在 vSphere 5.5 和 6.0 中, 可能会间歇性出现该问题, 在 vSphere 6.5 中修复了该问题。

解决办法: 在 vCenter ESX Agency Manager MOB https://VC_IP/eam/mob/ 中, 您可以访问与主机集群关联的代理。单击某个代理, 然后单击配置以查看集群详细信息。对于受影响的集群, 请单击解决所有。

- 问题 1979457: 如果在升级过程中以向后兼容模式删除或移除了 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。

解决办法: 升级集群, 以便所有主机运行新版本的 GI-SVM。

或

启用日志采集器以使身份防火墙正常工作。

NSX Manager 已知问题

- 问题 1892999: 无法修改唯一选择条件, 即使未将任何虚拟机附加到通用安全标记
如果删除了附加到通用安全标记的虚拟机, 表示虚拟机的内部对象仍会附加到通用安全标记。这会导致通用选择条件更改失败, 并出现“通用安全标记仍附加到虚拟机”错误。

解决办法: 删除所有通用安全标记, 然后更改通用选择条件。

- 问题 1801325: 由于较高的 CPU 和/或磁盘使用率, 在 NSX Manager 中生成“严重”系统事件和日志记录

如果在 NSX Manager 上具有较高的磁盘空间使用率、较高的作业数据改动量或较高的作业队列大小, 您可能会遇到一个或多个以下问题:

- 在 vSphere Web Client 中存在“严重”系统事件

- NSX Manager 上的 /common 分区具有较高的磁盘使用率
- 较长时间或每隔一段时间存在较高的 CPU 使用率
- 对 NSX Manager 性能造成不利影响

解决办法：与 VMware 客户支持人员联系。有关详细信息，请参见 [VMware 知识库文章 2147907](#)。

- **问题 1806368：**如果重用以前发生故障的主 NSX Manager（在故障切换后再次变为主 NSX Manager）中的控制器，将导致不会将 DLR 配置推送到所有主机

在跨 vCenter NSX 设置中，当主 NSX Manager 发生故障时，将升级辅助 NSX Manager 为主 NSX Manager，并部署新的控制器集群以用于新升级的辅助 NSX Manager（现在为主 NSX Manager）。当主 NSX Manager 恢复启动时，将辅助 NSX Manager 降级并还原主 NSX Manager。在这种情况下，如果重用在故障切换之前在该主 NSX Manager 上部署的现有控制器，则不会将 DLR 配置推送到所有主机。如果创建新的控制器集群，则不会出现该问题。

解决办法：为还原的主 NSX Manager 部署新的控制器集群。

- **问题 1831131：**在使用 LocalOS 用户进行身份验证时，无法从 NSX Manager 连接到 SSO

在使用 LocalOS 用户进行身份验证时，无法从 NSX Manager 连接到 SSO 并出现以下错误：“无法与 NSX Manager 建立通信。请联系管理员。” (Could not establish communication with NSX Manager. Please contact administrator.)

解决办法：除了 nsxmanager@domain 以外，还要为 nsxmanager@localos 添加企业管理员角色。

- **问题 1800820：**如果已从系统中删除旧 UDLR 接口，辅助 NSX Manager 上的 UDLR 接口更新将失败。如果通用同步服务（复制程序）在主 NSX Manager 上停止工作，您必须删除主 NSX Manager 上的 UDLR（通用分布式逻辑路由器）和 ULS（通用逻辑交换机）接口并创建新的接口，然后在辅助 NSX Manager 上复制这些更改。在这种情况下，不会在辅助 NSX Manager 中更新 UDLR 接口，因为复制期间在辅助 NSX Manager 上创建了新的 ULS 而 UDLR 未连接到新 ULS。

解决办法：确保复制程序正在运行，删除主 NSX Manager 上连接新建 ULS 的 UDLR 接口 (LIF)，然后重新创建 UDLR 接口 (LIF) 并连接相同的 ULS。

- **问题 1772911：**NSX Manager 的执行速度因磁盘空间消耗变得异常缓慢，任务和作业表大小不断增加，CPU 使用率接近 100%

您将遇到以下问题：

- NSX Manager CPU 使用率达 100%，或其峰值经常达到 100%，即使向 NSX Manager 设备添加额外资源也不起作用。
- 在 NSX Manager 命令行界面 (CLI) 中运行 `show process monitor` 命令，将显示 CPU 周期消耗最高的 Java 进程。
- 在 NSX Manager CLI 中运行 `show filesystems` 命令会显示 /common 目录，因为它达到了非常高的使用百分比，如超过 90%。
- 某些配置更改超时（有时长达 50 分钟以上）并且没有效果。

有关详细信息，请参见 [VMware 知识库文章 2147907](#)。

解决办法：与 VMware 客户支持人员联系以解决该问题。

- **问题 1785142：**在阻止主和辅助 NSX Manager 之间的通信时，主 NSX Manager 上延迟显示“同步问题”。

在主和辅助 NSX Manager 之间的通信被阻止时，您将不会立即在主 NSX Manager 上看到“同步问题”。

解决办法：等候大约 20 分钟以使通信重新建立连接。

- **问题 1786066：**在跨 vCenter NSX 安装中，断开辅助 NSX Manager 的连接可能会使 NSX Manager 无法作为辅助 NSX Manager 重新连接

在跨 vCenter NSX 安装中，如果断开辅助 NSX Manager 的连接，以后可能无法将该 NSX Manager 重新添加为辅助 NSX Manager。尝试作为辅助 NSX Manager 重新连接 NSX Manager 时，此 NSX Manager 将会在

vSphere Web Client 的“管理”选项卡中被列为“辅助”，但不会建立与主 NSX Manager 的连接。
解决办法：

1. 断开辅助 NSX Manager 与主 NSX Manager 的连接。
2. 再次将辅助 NSX Manager 添加到主 NSX Manager。

- **问题 1715354：REST API 可用性延迟**

在切换 FIPS 模式时，在 NSX Manager 重新启动后，NSX Manager API 需要一些时间才会启动并运行。该 API 似乎已挂起，但发生这种情况是因为，控制器需要一些时间以重新建立与 NSX Manager 的连接。建议您等待 NSX API 服务器启动并运行，并确保所有控制器处于已连接状态，然后再执行任何操作。

- **问题 1441874：在 vCenter 链接模式环境中升级单个 NSX Manager 时显示错误消息**

如果环境中具有多个 VMware vCenter Server 和多个 NSX Manager，从 vSphere Web Client 的“网络和安全” > “安装” > “主机准备”中选择一个或多个 NSX Manager 时，将会看到以下错误：

“无法与 NSX Manager 建立通信。请联系管理员。” (Could not establish communication with NSX Manager. Please contact administrator.)

*解决办法：*有关详细信息，请参见 [VMware 知识库文章 2127061](#)。

- **问题 1696750：通过 PUT API 为 NSX Manager 分配 IPv6 地址需要重新引导才能生效**

通过 <https://{NSX Manager IP address}/api/1.0/appliance-management/system/network> 更改为 NSX Manager 配置的网络设置需要重新引导系统才能生效。在重新引导之前，将显示先前存在的设置。

*解决办法：*无。

- **问题 1529178：上载不包含常用名称的服务器证书会返回消息“内部服务器错误” (internal server error)**

如果上载的服务器证书不包含常用名称，会显示消息“内部服务器错误” (internal server error)。

*解决办法：*使用同时包含 SubAltName 和常用名称的服务器证书，或者使用至少包含一个常用名称的服务器证书。

- **问题 1655388：在日语、简体中文和德语版本的 Windows 10 操作系统上使用 IE11/Edge 浏览器时，NSX Manager 6.2.3 UI 显示英语，而不是本地语言。**

在日语、简体中文和德语版本的 Windows 10 操作系统上使用 IE11/Edge 浏览器启动 NSX Manager 6.2.3 时，显示英语。

解决办法：

1. 启动 Microsoft 注册表编辑器 (regedit.exe)，然后转到计算机 > HKEY_CURRENT_USER > SOFTWARE > Microsoft > Internet Explorer > International。
2. 将 *AcceptLanguage* 文件的值改为本地语言。例如，如果希望将语言改为德语，请更改该文件的值，让 DE 显示在最前面。
3. 重新启动浏览器，然后再次登录 NSX Manager。此时将显示相应的语言。

- **问题 1435996：从 NSX Manager 导出为 CSV 的日志文件使用 Epoch（而不是日期时间）作为时间戳**
使用 vSphere Web Client 从 NSX Manager 导出的 CSV 格式的日志文件，其时间戳标记为 Epoch 时间（以毫秒为单位），而不是基于时区的相应时间。

*解决办法：*无。

- **问题 1644297：主 NSX 上任何 DFW 部分的添加/删除操作都会在辅助 NSX 上创建两个已保存的 DFW 配置**

在跨 vCenter 安装中，将其他通用或本地 DFW 部分添加到主 NSX Manager 后，会在辅助 NSX Manager 上保存两个 DFW 配置。尽管这个问题并不影响任何功能，但它将导致更快地达到已保存的配置限制，同时还可能会覆盖重要配置。

*解决办法：*无。

- **问题 1477138：如果主机名的长度超过 64 个字符，不会启动 NSX 管理服务**

要通过 OpenSSL 库创建证书，需要使用少于或等于 64 个字符的主机名。

- **问题 1437664：NSX Manager 列表在 Web Client 中显示缓慢**
在拥有多个 NSX Manager 的 vSphere 6.0 环境中，当通过大型 AD 组集对登录用户进行验证时，vSphere Web Client 可能需要多达两分钟才能显示 NSX Manager 列表。在尝试显示 NSX Manager 列表时，可能会出现数据服务超时错误。没有解决办法。必须等待列表加载/重新登录后，才能看到 NSX Manager 列表。
- **问题 1534606：“主机准备”页面加载失败**
当在链接模式下运行 vCenter 时，每个 vCenter 都必须连接到相同 NSX 版本的 NSX Manager。如果 NSX 版本不同，vSphere Web Client 将只能与运行较高 NSX 版本的 NSX Manager 通信。“主机准备”选项卡将显示类似以下内容的错误：“无法与 NSX Manager 建立通信。请联系管理员” (Could not establish communication with NSX Manager. Please contact administrator)。
*解决办法：*应将所有 NSX Manager 升级到相同的 NSX 软件版本。
- **问题 1027066：对 NSX Manager 执行 vMotion 操作可能会显示以下错误消息：“虚拟以太网卡网络适配器 1 不受支持 (Virtual ethernet card Network adapter 1 is not supported)”**
可以忽略此错误。在执行该 vMotion 操作后，网络将正常工作。
- **问题 1460766：使用 NSX 命令行界面更改密码后，NSX Manager UI 不会自动注销**
登录到 NSX Manager 且最近使用 CLI 更改了密码后，可能仍会使用旧密码在 NSX Manager UI 中保持登录状态。通常，如果会话处于不活动状态导致超时，NSX Manager 客户端应自动将您注销。
*解决办法：*从 NSX Manager UI 注销并使用新密码重新登录。
- **问题 1966681：错误地报告重复的 NSX Manager IP**
日志文件包含大量重复的 NSX Manager IP，并错误地报告有关网络中的重复 IP 的信息。
- **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. 在设备管理下面，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 1486193/1436953：即使成功从备份还原 NSX Manager，也会生成错误的系统事件**
成功从备份还原 NSX Manager 后，当您导航到网络和安全 > NSX Manager > 监控 > 系统事件时，vSphere Web Client 中会显示以下系统事件。
 - **无法从备份还原 NSX Manager (严重性=严重)** (Restore of NSX Manager from backup failed (with Severity=Critical))。
 - **已成功还原 NSX Manager (严重性=信息)** (Restore of NSX Manager successfully completed (with Severity=Informational))。*解决办法：*如果最后的系统事件消息显示为成功，您可以忽略系统生成的事件消息。
- **问题 1783528：NSX Manager CPU 占用率在每个星期五晚上/星期六早上达到峰值**
在每个星期五晚上，NSX 轮询 LDAP 以执行完全同步。没有配置特定 Active Directory 组织单位或容器的选项，因此，NSX 会同步与提供的域相关的所有对象。
*解决办法：*将 NSX Manager vCPU 从 4 增加到 6

NSX Controller 已知问题

- 问题 1856465：如果 ESXi 主机在 NSX 跨 vCenter 环境中的某个站点上关闭，则不会在该站点上启用 CDO 模式

如果 ESXi 主机在某个站点上关闭，则无法在该站点上完全成功启用或禁用 CDO 模式。

如果主机在某个辅助站点上关闭，CDO 模式操作将在主站点上成功完成。但 CDO 模式操作在辅助站点上失败。这可能会导致不一致的行为。

*解决办法：*该问题影响 NSX 6.3.0 和更高版本。

- 确保在执行任何 CDO 操作之前已启动所有 ESXi 主机。
- 要从不一致的状态中恢复，请从 vCenter 清单中移除主机，然后重新添加。

逻辑网络和 NSX Edge 已知问题

- 问题 2071666：对配有 L2VPN 的 Edge 执行 vMotion 后，通过 L2VPN 隧道中的延伸网络与远程虚拟机的流量传输中断

对配有 L2VPN 的 Edge（受管和单独 Edge）执行 vMotion 后，通过 L2VPN 隧道中的延伸网络与远程虚拟机的流量传输中断，直到远程虚拟机 MAC 的物理网络 MAC 表条目过期，手动清除或重新发现这些条目（如果在执行 vMotion 后生成来自远程虚拟机的流量）后恢复。

*解决办法：*为配有 L2VPN 的 Edge 禁用 DRS 以防止不受控制的 vMotion。如果在未禁用 DRS 的情况下执行 vMotion，则在执行 vMotion 后，清除远程虚拟机 MAC 的 MAC 表条目，并生成来自远程虚拟机的流量。

- 问题 1904612：在关闭客户端电源后，第 2 层 VPN 隧道在 L2VPN 服务器上显示“已启动”
如果在两个 NSX Edge 之间创建 L2 VPN，然后关闭客户端 NSX Edge 电源，服务器 NSX Edge 仍会显示 VPN 隧道已启动。

*解决办法：*无。

- 问题 1242207：在 OSPF 拓扑中未反映在运行时更改的路由器 ID
如果尝试更改路由器 ID 而不禁用 OSPF，不会使用该路由器 ID 重新生成新的外部链接状态通告 (LSA)，从而导致 OSPF 外部路由丢失。

*解决办法：*禁用 OSPF，更改路由器 ID，然后再次启用 OSPF。

- 问题 1894277：在更改本地或对等子网时，不保留 IPSec 站点配置 PSK
在数据库中保存遮蔽的 PSK 时，由于密码不匹配，对等方之间的隧道不会启动。

*解决办法：*使用有效的密码重新配置 IPSec 设置。

- 问题 1492497：无法筛选 NSX Edge DHCP 流量
您无法将任何防火墙筛选器应用于 NSX Edge 上的 DHCP 流量，因为 NSX Edge 上的 DHCP 服务器使用绕过 TCP/IP 堆栈的原始套接字。

*解决办法：*无。

- 问题 1781438：在 ESG 或 DLR NSX Edge 设备上，如果多次收到 BGP 路径属性 MULTI_EXIT_DISC，路由服务不会发送错误消息。
如果多次收到 BGP 路径属性 MULTI_EXIT_DISC，Edge 路由器或分布式逻辑路由器不会发送错误消息。根据 RFC 4271 [第 5 节]，相同的属性（具有相同类型的属性）不能在特定更新消息的“路径属性”字段中多次出现。

*解决办法：*无。

- 问题 1786515：具有“安全管理员”特权的用户无法通过 vSphere Web Client UI 编辑负载均衡器配置。

具有特定 NSX Edge 的“安全管理员”特权的用户无法使用 vSphere Web Client UI 编辑该 Edge 的全局负载均衡器配置。将显示以下错误消息：“未授权用户访问对象 Global 和功能 si.service, 请查看用户的对象访问范围和功能权限。(User is not authorized to access object Global and feature si.service, please check object access scope and feature permissions for the user.)”

*解决办法：*无。

- 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 1711013：在重新引导备用虚拟机后，大约需要 15 分钟在活动/备用 NSX Edge 之间同步 FIB。
在关闭备用 NSX Edge 电源后，不会在活动 and 备用模式之间关闭 TCP 会话。在发生保持连接 (KA) 故障后（15 分钟），活动 Edge 才会检测到备用 Edge 已关闭。在 15 分钟后，将与备用 Edge 之间建立新的套接字连接并在活动/备用 Edge 之间同步 FIB。

*解决办法：*无。

- 问题 1733282：NSX Edge 不再支持静态设备路由
NSX Edge 不支持配置下一跃点地址为空的静态路由。

*解决办法：*无。

- 问题 1860583：如果无法访问 DNS，应避免将远程系统日志记录程序作为 FQDN。
在 NSX Edge 上，如果使用 FQDN 配置远程系统日志记录程序并且无法访问 DNS，则路由功能可能会受到影响。可能不会持续出现该问题。

*解决办法：*建议使用 IP 地址而不是 FQDN。

- 问题 1850773：在负载均衡器配置中使用多个端口时，NSX Edge NAT 报告无效的配置
每次为负载均衡器虚拟服务器配置多个端口时，都会出现该问题。因此，在受影响的 NSX Edge 存在该配置状态时，无法管理 NAT。

*解决办法：*有关详细信息和解决办法，请参见 [VMware 知识库文章 2149942](#)。

- 问题 1764258：在配置了子接口的 NSX Edge 上进行 HA 故障切换或强制同步后，流量产生黑洞长达八分钟之久
如果通过子接口触发 HA 故障切换或启动强制同步，流量会产生黑洞长达八分钟之久。

*解决办法：*不要对 HA 使用子接口。

- 问题 1767135：在尝试访问负载均衡器中的证书和应用程序配置文件时出错
具有安全管理员权限和 Edge 范围的用户无法访问负载均衡器中的证书和应用程序配置文件。vSphere Web Client 将显示错误消息。

*解决办法：*无。

- 问题 1792548：NSX Controller 可能会停滞并显示以下消息：“正在等待加入集群” (Waiting to join cluster)

NSX Controller 可能会停滞并显示以下消息：“正在等待加入集群” (Waiting to join cluster) (CLI 命令：show control-cluster status)。出现该问题是因为，在控制器启动时，为控制器的 eth0 和 breth0 接口配置了相同的 IP 地址。您可以在控制器上使用以下命令验证是否存在这种情况：show network interface

*解决办法：*与 VMware 客户支持人员联系。

- 问题 1747978：在 NSX Edge HA 故障切换后，删除了具有 MD5 身份验证的 OSPF 邻接。在为 NSX Edge 配置了 HA、配置了 OSPF 正常重新启动并使用 MD5 进行身份验证的 NSX for vSphere 6.2.4 环境中，OSPF 无法正常启动。只有在失效定时器在 OSPF 邻居节点上到期后，才会形成邻接。

*解决办法：*无

- 问题 1804116：在与 NSX Manager 通信中断的主机上，逻辑路由器进入错误状态。如果在与 NSX Manager 通信中断的主机（因 NSX VIB 升级/安装失败或主机通信问题所致）上打开或重新部署逻辑路由器，此逻辑路由器将进入错误状态，而且通过强制同步执行的持续自动恢复操作将失败。

*解决办法：*在解决了主机和 NSX Manager 通信问题后，手动重新引导 NSX Edge 并等待显示所有界面。此解决办法仅适用于逻辑路由器，而不适用于 NSX Edge 服务网关 (ESG)，因为通过强制同步执行的自动恢复进程会重新引导 NSX Edge。

- 问题 1783065：无法同时使用 IPv4 和 IPv6 地址来针对 UDP 端口及 TCP 配置负载均衡器。UDP 仅支持 ipv4-ipv4、ipv6-ipv6（前端-后端）。NSX Manager 中存在一个错误，即使将 IPv6 链路本地地址以分组对象 IP 地址的形式读取和推送，您也无法选择要在 LB 配置中使用的 IP 协议。

以下是一个用于展示此问题的示例 LB 配置：

在负载均衡器配置中，池“vCloud_Connector”将分组对象 (vm-2681) 配置为池成员，并且此对象同时包含 IPv4 和 IPv6 地址，LB L4 引擎不支持这种情况。

```
{
  "algorithm" : {
    ...
  },
  "members" : [
    {
      ... ,
      ...
    }
  ],
  "applicationRules" : [],
  "name" : "vCloud_Connector",
  "transparent" : {
    "enable" : false
  }
}

{
  "value" : [
    "fe80::250:56ff:feb0:d6c9",
    "10.204.252.220"
  ],
  "id" : "vm-2681"
}
```

解决办法：

- 方法 1：输入池成员的 IP 地址，而不是池成员中分组对象的 IP 地址。
- 方法 2：请不要在虚拟机中使用 IPv6。

- 问题 1777792：设置为“ANY”的对等端点导致 IPsec 连接失败

当 NSX Edge 上的 IPsec 配置将远程对等端点设置为“ANY”时，Edge 将充当 IPsec “服务器”，并等待远程对等端点启动连接。但是，如果启动程序使用 PSK 和 XAUTH 发送身份验证请求，则 Edge 显示以下错误消息：“在 XXX.XXX.XX.XX:500 上收到初始主模式消息，但是连接没有通过 policy=PSK+XAUTH 进行授权”(initial Main Mode message received on XXX.XXX.XX.XX:500 but no connection has been authorized with policy=PSK+XAUTH)，并且无法建立 IPsec。

*解决办法：*在 IPsec VPN 配置中使用特定的对等端点 IP 地址或 FQDN，而不是“ANY”。

- 问题 1741158：如果创建新 NSX Edge 而未进行配置，则应用配置可能会导致 Edge 服务过早激活。如果使用 NSX API 创建新 NSX Edge 而未进行配置，然后执行 API 调用以禁用该 Edge 上的某个 Edge 服务（例如，将 dhcp-enabled 设置为“false”），最后将配置更改应用到禁用的 Edge 服务，则该服务将会被立即激活。

*解决办法：*在对希望保持禁用状态的 Edge 服务进行配置更改后，立即执行 PUT 调用以将该服务的 enabled 标记设置为“false”。

- 问题 1758500：对于具有多个下一跃点的静态路由，如果配置的下一跃点中至少有一个是 Edge 的 vNIC IP 地址，则该静态路由将不会安装在 NSX Edge 路由表和转发表中。在使用 ECMP 和多个下一跃点地址时，如果下一跃点 IP 地址中至少有一个有效，则 NSX 便允许将 Edge 的 vNIC IP 地址配置为下一跃点。系统会接受配置而不出现任何错误或警告，但该网络的路由会从 Edge 的路由表/转发表中移除。

*解决办法：*使用 ECMP 时，不要将 Edge 本身的 vNIC IP 地址配置为静态路由中的下一跃点。

- 问题 1716464：NSX 负载均衡器不会路由到使用安全标记新标记的虚拟机。如果我们部署两个具有给定标记的虚拟机，然后配置一个 LB 以路由到该标记，该 LB 将成功路由到这两个虚拟机。但是，如果我们随后部署第三个具有该标记的虚拟机，该 LB 仅路由到前两个虚拟机。

*解决办法：*在 LB 池上单击“保存”。这会重新扫描虚拟机，并开始路由到新标记的虚拟机。

- 问题 1461421：NSX Edge 的“show ip bgp neighbor”命令输出保留以前建立连接的历史计数。“show ip bgp neighbor”命令显示 BGP 状态计算机在给定对等连接中转换到“已建立”状态的次数。更改基于 MD5 身份验证的密码会导致对等连接被损毁并重新创建，这转而将清除计数器。Edge DLR 不会发生此问题。

*解决办法：*要清除计数器，请执行“clear ip bgp neighbor”命令。

- 问题 1656713：HA 故障切换之后 NSX Edge 上缺少 IPsec 安全策略 (SP)，流量无法流过隧道。待机 > 活动切换对于 IPsec 隧道上的流量无效。

*解决办法：*在切换 NSX Edge 后禁用/启用 IPsec。

- 问题 1354824：Edge 虚拟机由于电源故障等原因被损坏或无法访问时，如果 NSX Manager 中的运行状况检查失败，会引发系统事件。“系统事件”选项卡将报告事件“Edge 不可访问”(Edge Unreachability)。NSX Edge 列表可能会继续报告“已部署”状态。

*解决办法：*使用以下 API 获取有关 NSX Edge 的详细状态信息：

```
GET https://NSX-Manager-IP-Address/api/4.0/edges/edgeId/status?detailedStatus=true
```

- 问题 1647657：在启用 DLR（分布式逻辑路由器）的 ESXi 主机上，显示命令只能为每个 DLR 实例最多显示 2000 个路由

在启用 DLR 的 ESXi 主机上，显示命令只能为每个 DLR 实例最多显示 2000 个路由，即使正在运行的路由数量超出此最大限制也是如此。这是一个显示问题，数据路径对所有路由都将按预期工作。

解决办法：无。

- 问题 1634215：OSPF CLI 命令输出不指示是否已禁用路由
禁用 OSPF 后，路由 CLI 命令输出不显示任何指示“OSPF 已禁用”(*OSPF is disabled*) 的消息。输出为空。

解决办法：*show ip ospf* 命令将显示正确的状态。

- 问题 1647739：执行 vMotion 操作之后重新部署 Edge 虚拟机会导致 Edge 或 DLR 虚拟机被放回原始集群。

解决办法：要将 Edge 虚拟机放到其他资源池或集群，请使用 NSX Manager UI 来配置所需的位置。

- 问题 1463856：启用 NSX Edge 防火墙后，现有 TCP 连接会被阻止

由于看不到最初的三次握手，因此会通过 Edge 状态防火墙阻止 TCP 连接。

解决办法：要处理此类现有流量，请执行以下操作。使用 NSX REST API 在防火墙全局配置中启用“tcpPickOngoingConnections”标记。这会将防火墙从严格模式切换到宽松模式。接下来，启用防火墙。现有连接正常工作（在启用防火墙后执行此操作可能需要几分钟时间）后，将“tcpPickOngoingConnections”标记重新设置为 false，以将防火墙返回到严格模式。（这是持久性设置。）

```
PUT /api/4.0/edges/{edgeId}/firewall/config/global
```

```
<globalConfig>
```

```
<tcpPickOngoingConnections>true</tcpPickOngoingConnections>
```

```
</globalConfig>
```

- 问题 1374523：在安装 VXLAN VIB 后需要重新引导 ESXi 或运行 *[services.sh restart]*，才能通过 esxcli 使用 VXLAN 命令

在安装 VXLAN VIB 后，您必须重新引导 ESXi 或运行 *[services.sh restart]* 命令，之后才能通过 esxcli 使用 VXLAN 命令。

解决办法：使用 localcli，而不是 esxcli。

- 问题 1525003：使用不正确的密码短语还原 NSX Manager 备份时将会静默失败，因为无法访问关键引导文件夹

解决办法：无。

- 问题 1483426：即使未启用 IPSec 和 L2 VPN 服务，其状态也显示为关闭

在 UI 中的“设置”选项卡下，L2 服务状态显示为关闭，而 API 将 L2 服务状态显示为启动。L2 VPN 和 IPSec 服务在“设置”选项卡中始终显示为关闭，除非刷新 UI 页面。

解决办法：刷新页面。

- 问题 1637639：使用 Windows 8 SSL VPN PHAT 客户端时，不会从 IP 池分配虚拟 IP。

在 Windows 8 上，当由 Edge 服务网关分配新 IP 地址，或者 IP 池改为使用不同的 IP 范围时，不会按预期从 IP 池中分配虚拟 IP 地址。

解决办法：此问题仅在 Windows 8 上出现。使用其他 Windows 操作系统可避免遇到此问题。

- 问题 1628220：在接收器侧看不到 DFW 或 NetX 观察。

如果与目标 vNIC 关联的交换机端口发生更改，跟踪流可能不在接收器侧显示 DFW 和 NetX 观察。将不为 vSphere 5.5 版本修复此问题。vSphere 6.0 及更高版本不存在此问题。

解决办法：不要禁用 vNIC。重新引导虚拟机。

- 问题 1446327：通过 NSX Edge 连接时，某些基于 TCP 的应用程序可能会超时

TCP 建立连接的默认非活动状态超时为 3600 秒。NSX Edge 会删除闲置时间超过非活动状态超时的任何连接，并丢弃这些连接。

解决办法：

1. 如果应用程序处于非活动状态的时间相对较长，请在主机上启用 TCP Keepalive，并将 `keep_alive_interval` 设置为少于 3600 秒。
2. 使用以下 NSX REST API，将 Edge TCP 非活动状态超时延长为大于 2 小时。例如，将非活动状态超时延长为 9000 秒。NSX API URL：

```
/api/4.0/edges/{edgeId}/systemcontrol/config PUT Method <systemControl>  
<property>sysctl.net.netfilter.nf_conntrack_tcp_timeout_established=9000</p  
roperty> </systemControl>
```

- 问题 1089238：无法在多个 DLR Edge 上行链路上配置 OSPF

目前，无法在多个 DLR Edge 上行链路（共 8 个）上配置 OSPF。该限制是由于每个 DLR 实例共享单个转发地址造成的。

解决办法：这是当前的系统限制，没有解决办法。

- 问题 1499978：Edge syslog 消息无法到达远程 syslog 服务器

Edge syslog 服务器无法在部署后立即解析任何已配置的远程 syslog 服务器的主机名。

解决办法：使用 IP 地址配置远程 syslog 服务器，或通过 UI 强制同步 Edge。

- 问题 1489829：更新 REST Edge API 后，逻辑路由器的 DNS 客户端配置设置未完全应用

解决办法：使用 REST API 配置 DNS 转发器（解析程序）时，请执行以下步骤：

1. 指定 DNS 客户端 XML 服务器的设置，以便使其与 DNS 转发器设置相匹配。
2. 启用 DNS 转发器，并确保转发器设置与 XML 配置中指定的 DNS 客户端服务器设置相同。

- 问题 1243112：启用了 ECMP 的静态路由中无效的下一跃点未显示验证和错误消息

尝试添加启用了 ECMP 的静态路由时，如果路由表不包含默认路由且静态路由配置中存在无法访问的下一跃点，将不会显示任何错误消息且不会安装静态路由。

解决办法：无。

- 问题 1281425：如果通过 vCenter Web Client 用户界面删除一个子接口受逻辑交换机支持的 NSX Edge 虚拟机，数据路径可能不适用于连接至同一端口的新虚拟机

当通过 vCenter Web Client 用户界面（而非 NSX Manager）删除 Edge 虚拟机时，在 dvPort 上通过不透明通道配置的 VXLAN 中继不会重置。这是因为中继配置由 NSX Manager 管理。

解决办法：按照下面的步骤手动删除 VXLAN 中继配置：

1. 通过在浏览器窗口中键入以下内容导航至 vCenter Managed Object Browser：

```
https://<vc-ip>/mob?vmodl=1
```

2. 单击内容。
3. 按照下面的步骤检索 dvsUuid 值。
 - a. 单击 rootFolder 链接（例如，group-d1(Datacenters)）。
 - b. 单击数据中心名称链接（例如，datacenter-1）。
 - c. 单击 networkFolder 链接（例如，group-n6）。
 - d. 单击 DVS 名称链接（例如，dvs-1）。
 - e. 复制 uuid 的值。
4. 单击 DVSManger，然后单击 updateOpaqueDataEx。
5. 在 `selectionSet` 中，添加以下 XML。

```
<selectionSet xsi:type="DVPortSelection">  
  <dvsUuid>value</dvsUuid>  
  <portKey>value</portKey> <!--port number of the DVPG where trunk vnic got  
  connected-->  
</selectionSet>
```

6. 在 `opaqueDataSpec` 中，添加以下 XML

```

<opaqueDataSpec>
  <operation>remove</operation>
  <opaqueData>
    <key>com.vmware.net.vxlan.trunkcfg</key>
    <opaqueData></opaqueData>
  </opaqueData>
</opaqueDataSpec>

```

7. 将 isRuntime 设置为 false。

8. 单击调用方法。

9. 为在已删除 Edge 虚拟机上配置的每个中继端口重复步骤 5 至 8。

- 问题 1637939：在部署硬件网关时，不支持 MD5 证书

将硬件网关交换机部署为用于逻辑 L2 VLAN 到 VXLAN 之间桥接的 VTEP 时，物理交换机应至少支持用于在 NSX Controller 和 OVSDB 交换机之间建立 OVSDB 连接的 SHA1 SSL 证书。

*解决办法：*无。

- 问题 1637943：对于具有硬件网关绑定的 VNI，不支持混合或多播复制模式

硬件网关交换机在用作 L2 VXLAN 到 VLAN 之间桥接的 VTEP 时，只支持单播复制模式。

*解决办法：*只使用单播复制模式。

- 问题 1995142：从 VC 清单中移除主机后，没有将其从复制集群中移除

如果用户将主机添加到复制集群中，然后在将主机从集群中移除之前先将其从 VC 清单中移除，旧版主机将保留在集群中。

*解决办法：*每次移除主机时，请先确保已将其从复制集群中移除（如果有）。

- 问题 2085286：如果所有桥接接口具有路由 LIF，在移除所有这些桥接接口后，将从主机中移除 VDR。

如果 VDR 包含 n 个 LIF，具有 n 个逻辑 vWire，并且同一 VDR 上的所有 vWire 用于桥接，则删除所有网桥会出现该问题。

不要使用用作路由 LIF 的所有 vWire 进行桥接。如果将所有路由 LIF 进行桥接，则不应同时删除所有网桥。

安全服务已知问题

- 问题 2186968：静态 IPset 未报告给 containerset API 调用

如果有服务设备，则 NSX 可能会在与合作伙伴服务管理器通信时忽略 IP 集。这可能会导致合作伙伴防火墙错误地允许或拒绝连接。

*解决办法：*有关解决办法，请与 VMware 客户支持联系。有关详细信息，请参见 [VMware 知识库文章 57834](#)。

- 问题 1854661：在跨 VC 设置中，在 NSX Manager 之间切换时，筛选的防火墙规则不显示索引值

如果将规则筛选条件应用于某个 NSX Manager，然后切换到不同的 NSX Manager，所有筛选的规则索引显示为“0”，而不是显示实际的规则位置。

*解决办法：*清除筛选器以查看规则位置。

- 问题 1474650：对于 NetX 用户，ESXi 5.5.x 和 6.x 主机显示紫色诊断屏幕，警示用户 **ALERT: NMI: 709: NMI IPI received**

在服务虚拟机发送或收到大量数据包时，DVFilter 持续占用 CPU，从而导致检测信号丢失并显示紫色诊断屏幕。有关详细信息，请参见 [VMware 知识库文章 2149704](#)。

*解决办法：*将 ESXi 主机升级到使用 NetX 所需的任何以下最低 ESXi 版本：

- 5.5 Patch 10

- ESXi 6.0U3
- ESXi 6.5

- 问题 1787680：在 NSX Manager 处于转换模式时，删除通用防火墙区域失败
在尝试从处于转换模式的 NSX Manager 的 UI 中删除通用防火墙区域并进行发布时，发布将失败，因而无法将 NSX Manager 设置为独立模式。

解决办法：使用单个删除区域 REST API 删除通用防火墙区域。

- 问题 1689159：“流量监控”中的“添加规则”功能无法正常用于 ICMP 流量。
在从“流量监控”中添加规则时，如果未明确将“服务”字段设置为“ICMP”，则该字段将保留为空，结果，您最终可能会添加服务类型为“ANY”的规则。

解决办法：更新“服务”字段以反映 ICMP 流量。

- 问题 1632235：在客户机侦测安装过程中，网络下拉列表仅显示“已在主机上指定”
使用 NSX 仅防病毒许可证和 vSphere Essential 或 vSphere Standard 许可证安装客户机侦测时，网络下拉列表将仅显示现有的 DV 端口组列表。此类许可证不支持创建 DVS。
解决办法：在 vSphere 主机上使用其中一种许可证安装客户机侦测之前，先在“代理虚拟机设置”窗口中指定网络。

- 问题 1652155：在某些情况下，使用 REST API 创建或迁移防火墙规则可能会失败，并报告 HTTP 404 错误

以下情况不支持使用 REST API 添加或迁移防火墙规则：

- 设置 autosavedraft=true 时通过批量操作创建防火墙规则。
- 在多个部分同时添加防火墙规则。

解决办法：执行防火墙规则批量创建或迁移时，在 API 调用中将 autoSaveDraft 参数设置为 false。

- 问题 1509687：在一次 API 调用中，一次将一个安全标记分配给多个虚拟机时，URL 长度最多支持 16000 个字符

如果 URL 长度超过 16,000 个字符，则无法在一次 API 调用中将一个安全标记同时分配给大量虚拟机。

解决办法：为了优化性能，请在一次调用中最多标记 500 个虚拟机。

- 问题 1662020：发布操作失败导致在 DFW UI 的“常规”和“合作伙伴安全服务”部分中显示错误消息“上次在主机 *host number* 上发布失败” (Last publish failed on host *host number*)
更改任何规则后，UI 都会显示“上次在主机 *host number* 上发布失败” (Last publish failed on host *host number*)。UI 上所列主机的防火墙规则版本可能不正确，从而导致安全性缺乏和/或网络中断。

通常在以下场景中会出现此问题：

- 从旧版 NSX 升级到最新版本之后。
- 将主机移出集群后再将其移回时。
- 将主机从一个集群移动到另一个集群时。

解决办法：要解决此问题，您必须强制同步受影响的集群（仅限防火墙）。

- 问题 1481522：不支持从 6.1.x 向 6.2.3 迁移防火墙规则草稿，因为这些草稿在这两个版本之间不兼容

解决办法：无。

- 问题 1628679：使用基于身份标识的防火墙时，已移除用户的虚拟机会继续保持在安全组中

将用户从 AD 服务器上的组中移除后，该用户登录的虚拟机继续保持在这个安全组中。这会在 Hypervisor 上保留虚拟机虚拟网卡的防火墙策略，因此，会授予用户对服务的完全访问权限。

解决办法：无。这是设计的预期行为。

- 问题 1496273：UI 允许创建无法应用到 Edge 的入站/出站 NSX 防火墙规则

当 NSX 防火墙规则包含按“入站”或“出站”方向传输的流量并且数据包类型为 IPV4 或 IPV6 时，Web Client 错误地允许创建该规则并将其应用到一个或多个 NSX Edge。UI 不应允许创建此类规则，因为 NSX 无法将其应用到 NSX Edge。

*解决办法：*无。

- 问题 1494718：无法创建新的通用规则，且无法从流量监控 UI 编辑现有通用规则

*解决办法：*无法通过流量监控 UI 添加或编辑通用规则。EditRule 将自动禁用。

- 问题 1066277：安全策略名称不允许超过 229 个字符

服务编排的“安全策略”选项卡中的安全策略名称字段最多允许 229 个字符。这是因为策略名称在内部预置了前缀。

*解决办法：*无。

- 问题 1443344：第三方网络虚拟机系列的某些版本无法使用 NSX Manager 默认设置

默认情况下，某些 NSX 6.1.4 或更高版本的组件会禁用 SSLv3。升级前，请确保所有与 NSX 部署集成的第三方解决方案均不依赖于 SSLv3 通信。例如，Palo Alto Networks 虚拟机系列解决方案的某些版本需要 SSLv3 支持，所以请向您的供应商确认其版本要求。

- 问题 1660718：服务编排策略状态在 UI 中显示为“正在进行”，在 API 输出中显示为“挂起”

*解决办法：*无。

- 问题 1317814：如果在一个 Service Manager 关闭的情况下进行策略更改，服务编排将不同步

如果在多个 Service Manager 中有一个关闭的情况下进行策略更改，则更改将失败，并且服务编排将不同步。

*解决办法：*确保 Service Manager 有响应，然后从服务编排执行强制同步。

- 问题 1070905：无法从受客户机侦测和第三方安全解决方案保护的集群中移除主机并重新添加

如果通过断开主机连接然后将其从 vCenter Server 中移除，从受客户机侦测和第三方安全解决方案保护的集群中移除主机，则在将同一主机重新添加到同一集群时可能会遇到一些问题。

*解决办法：*要从受保护的集群中移除主机，请先将该主机置于维护模式。接下来，将该主机移动到不受保护的集群中或置于所有集群之外，然后断开连接并移除该主机。

- 问题 1648578：在创建基于 NetX 主机的新服务实例时，NSX 强制添加集群/网络/存储

从 vSphere Web Client 中为基于 NetX 主机的服务（例如，防火墙、IDS 和 IPS）创建新的服务实例时，将强制添加集群/网络/存储，即使不需要使用这些集群/网络/存储也是如此。

*解决办法：*在创建新的服务实例时，您可以为集群/网络/存储添加任何信息以填写这些字段。这样，就可以创建服务实例了，并且您可以根据需要继续操作。

监控服务已知问题

- 问题 1466790：无法使用 NSX 跟踪流工具选择桥接网络上的虚拟机

无法使用 NSX 跟踪流工具选择未连接到逻辑交换机的虚拟机。这意味着无法按虚拟机名称选择 L2 桥接网络上的虚拟机来作为跟踪流检测的源或目标地址。

*解决办法：*对于连接到 L2 桥接网络的虚拟机，请使用要作为跟踪流检测目标的接口的 IP 地址或 MAC 地址。您无法选择将连接到 L2 桥接网络的虚拟机作为源。