



# VMware NSX for vSphere 6.2.8 发行说明

VMware NSX for vSphere 6.2.8 | 2017 年 7 月 6 日发行 | 内部版本 5901733

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：

- [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](#)
- [修订历史](#)
- [已解决的问题](#)
- [已知问题](#)

## 新增功能

严重错误修复：该版本包含一些严重错误修复和安全更新。此外，还改进了与 VTEP 相关的日志记录信息。有关详细信息，请参见[已解决的问题](#)部分。

请参见 NSX [6.2.7](#)、[6.2.6](#)、[6.2.5](#)、[6.2.4](#)、[6.2.3](#)、[6.2.2](#)、[6.2.1](#) 和 [6.2.0](#) 中的新增及改进的功能。

## 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。

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 for vSphere 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> <ul style="list-style-type: none"> <li>• NSX for vSphere 6.2.4 解决了已知的 SSL VPN 问题。有关详细信息，请参见 <a href="#">CVE-2016-2079</a>。强烈建议运行 6.2.2 或更低版本的客户进行升级。</li> <li>• NSX for vSphere 6.2.4 与 vSphere 6.0U3 的互操作运行解决了在重新引导 vCenter Server 后 ESXi 主机中出现的重复 VTEP 问题。有关详细信息，请参见 <a href="#">VMware 知识库文章 2144605</a>。</li> </ul>
vSphere	<p>VMware 建议在 NSX 环境中最低运行 5.5U3 和 6.0U3。另请参见 <a href="#">VMware 产品互操作性列表</a> 以了解互操作性信息。</p> <p>注意：</p> <ul style="list-style-type: none"> <li>• NSX 6.2.x 与 vSphere 6.5 不兼容。</li> <li>• NSX for vSphere 6.2.4 与 vSphere 6.0U3 的互操作运行解决了在重新引导 vCenter Server 后 ESXi 主机中出现的重复 VTEP 问题。有关详细信息，请参见 <a href="#">VMware 知识库文章 2144605</a>。</li> <li>• 对于分布式服务插入，建议使用 ESXi 版本 5.5 Patch 10 以及 ESXi 6.0U3 或更高版本。有关详细信息，请参见 <a href="#">VMware 知识库文章 2149704</a>。</li> </ul>
客户机侦测	<p>NSX 中基于客户机侦测的功能与特定的 VMware Tools (VMTools) 版本兼容。要启用 VMware Tools 随附的可选 Thin Agent 网络侦测驱动程序组件，您必须升级到以下任一版本：</p> <ul style="list-style-type: none"> <li>• VMware Tools 10.0.8 和更高版本；可以解决在 NSX/vCloud Networking and Security 中升级 VMware Tools 后出现的虚拟机速度缓慢问题。请参见 <a href="#">VMware 知识库文章 2144236</a>。</li> <li>• 支持 Windows 10 的 VMware Tools 10.0.9 及更高版本</li> </ul>
vRealize Orchestrator	NSX-vRO 插件版本 1.0.3 或更高版本
VMware Integrated Openstack (VIO)	VIO 2.5.1 或更高版本
vCloud Director (vCD)	<ul style="list-style-type: none"> <li>• vCD 8.0 或更高版本（如果从 vCNS 迁移到 NSX）</li> <li>• vCD 8.10.1 或更高版本（如果已运行在 NSX 上）</li> </ul>

## 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](#)。即将终止支持的产品包括：

- vCloud Networking and Security 已于 2016 年 9 月 19 日终止提供 (EOA) 和终止支持 (EOGS)。（另请参见 [VMware 知识库文章 2144733](#)。）（另请参见 [VMware 知识库文章 2144620](#)。）
- NSX for vSphere 6.1.x 已于 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](#)。）
- 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。
- Web 访问终端 (WAT) 即将被弃用，因此将不会包含在未来的维护版本中。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。

## 不再显示不支持的控制器命令

有关支持的命令的完整列表，请查阅 CLI 指南。您应该仅使用此指南中列出的命令。NSX for vSphere 不支持 join control-cluster 命令。另请参见 [VMware 知识库文章 2135280](#)。

## 自 NSX 6.2.3 起已不再支持 TLS 1.0

在 NSX VPN、IPsec 和负载均衡器密码套件中，从 NSX 6.2.3 起已不再支持 TLS 1.0。有关密码支持变化的信息，请参见 [VMware 知识库文章 2147293](#)。

# 升级说明

- 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。
- 要升级到 NSX 6.2.4 或更高版本，您必须执行完整的 NSX 升级，包括主机集群升级（将主机 VIB 升级到 6.2.4）。有关说明，请参见 [《NSX 升级指南》](#)，其中包括[将主机集群升级至 NSX 6.2](#)一节。
- 最低内存要求为 8GB：在内存少于 8 GB 的主机上，可能无法升级到 NSX 6.2.3 或更高版本。
- 升级 Edge 服务网关 (ESG)：
  - 从 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：

1. 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（请参见下表以了解默认值）。

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

- 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。如果您的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，并将 `<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>
```

- 控制器磁盘布局：新安装 NSX 6.2.3 或更高版本时，将使用更新的磁盘分区部署 NSX Controller 设备，增强了集群弹性。在以前的版本中，控制器磁盘上的日志溢出可能会影响控制器的稳定性。除了添加日志管理增强功能来防止溢出之外，NSX Controller 设备还为数据和日志提供了单独的磁盘分区，以防止发生这些事件。如果是升级到 NSX 6.2.3 或更高版本，NSX Controller 设备将保留它们的原始磁盘布局。
- 升级途径：
  - 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](#)》中讲述了跨 vCenter NSX 升级过程。
  - 从 vCNS 5.5.x 升级的途径：

- 您可以使用 NSX 升级包，直接从 VMware vCloud Networking and Security (vCNS) 5.5.x 升级到 NSX 6.2.x。有关说明，请参见《NSX 升级指南》中的[将 vCloud Networking and Security 升级到 NSX](#) 一节。本节还包含有关在 vCloud Director 环境中将 vCNS 5.5.x 升级到 NSX 的说明。如果您只是将 vShield Endpoint 用于防病毒保护，请参见单独的指南《[NSX for vShield Endpoint 升级指南](#)》，其中包含有关将 vCNS 5.5.x 升级到 NSX 6.2.x 的说明。
- 如果您的环境中具有虚拟线路，则必须更新主机集群。更新完成后，虚拟线路即会被重命名为逻辑交换机。有关说明，请参见[更新主机集群](#)。
- 要验证是否成功升级到 NSX 6.2.x，请参见[知识库文章 2134525](#)。
- 合作伙伴服务兼容性：如果您的站点使用 VMware 合作伙伴服务来实施客户机侦测或网络侦测，则在升级之前，必须查阅《[VMware 兼容性指南](#)》，以确认供应商的服务与此版本的 NSX 兼容。
- 影响升级的已知问题：有关与升级相关的已知问题的列表，请参见本文档后文的[安装和升级已知问题](#) 一节。
- 新系统要求：有关在安装和升级 NSX Manager 时的内存和 CPU 要求，请参阅 NSX 6.2 文档中的[NSX 的系统要求](#) 一节。
- 为使用 TLS 1.0 的负载均衡客户端设置正确的密码版本：这会影响使用 TLS 1.0 版的 vROPs 池成员。如果要进行流量负载均衡的服务器使用该版本，您必须在 NSX 负载均衡器中使用“ssl-version=10”明确设置监控扩展值。请参见《[NSX 管理指南](#)》。

```
{
    "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"
}
```

- **最大 NAT 规则数量：**对于 6.2 之前的 NSX Edge 版本，用户可以分别配置 2048 个 SNAT 规则和 2048 个 DNAT 规则，规则总数限制为 4096 个。自 NSX Edge 版本 6.2 起，将根据 NSX Edge 设备大小来强制实施允许的最大 NAT 规则数限制：

对于精简 (COMPACT) Edge，可以分别配置 1024 个 SNAT 规则和 1024 个 DNAT 规则，规则总数限制为 2048 个。

对于中型 Edge 和大型 (QUADLARGE) Edge，可以分别配置 2048 个 SNAT 规则和 2048 个 DNAT 规则，规则总数限制为 4096 个。

对于超大型 (XLARGE) Edge，可以分别配置 4096 个 SNAT 规则和 4096 个 DNAT 规则，规则总数限制为 8192 个。

在将 NSX Edge 升级到版本 6.2 期间，NAT 规则总数（SNAT 规则和 DNAT 规则的数量总和）超过上限 2048 个的任何现有精简 (COMPACT) Edge 都将无法通过验证，从而导致升级失败。在这种情况下，用户需要将设备大小更改为中型和大型，然后重新尝试升级。

- 分布式逻辑路由器和 Edge 服务网关上的重新分发筛选器中的行为更改：从 6.2 版开始，DLR 和 ESG 中的重新分发规则仅作为 ACL 运行。即，如果规则是精确匹配，则执行相应操作。
- **VXLAN 隧道 ID：**升级到 NSX 6.2.x 之前，必须确保您的安装未在任何隧道上使用 VXLAN 隧道 ID 4094。VXLAN 隧道 ID 4094 不再可用。要评估并解决此问题，请遵循以下步骤：

1. 在 vCenter 中，导航到主页 > 网络和安全 > 安装，然后选择主机准备选项卡。

2. 在 VXLAN 列中单击配置。

3. 在“配置 VXLAN 网络”窗口中，将 VLAN ID 设置为介于 1 到 4093 之间的值。

- **重置 vSphere Web Client：**升级 NSX Manager 后，必须按照 [NSX 升级文档](#) 中的说明重置 vSphere Web Client 服务器。如未执行此操作，网络和安全选项卡可能不会在 vSphere Web Client 中显示。您可能还需要清除浏览器缓存或历史记录。
- **无状态环境：**无状态主机环境中的 NSX 升级使用新的 VIB URL：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：
  1. 通过 NSX Manager 从固定 URL 手动下载最新 NSX VIB。
  2. 将 VIB 添加到主机映像配置文件。

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：

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

- **自动保存草稿和服务编排：**在 NSX 6.2.3 及更高版本中，可以通过将 `autoDraftDisabled` 设置为 True 来禁用自动保存草稿功能。在升级过程中会保留手动配置的设置。在对防火墙规则进行大量更改之前禁用自动保存草稿功能可以提高性能，还会防止以前保存的草稿被覆盖。您可以使用以下 API 调用将全局配置中的属性 `autoDraftDisabled` 设置为 True：

1. 获取现有全局防火墙配置 (GlobalConfiguration)：

```
GET https://NSX-Manager-IP-
```

```
Address/api/4.0/firewall/config/globalconfiguration
```

请注意，GET 将不会显示 `autoDraftDisabled` 字段。

2. 使用 PUT 调用将全局配置中的属性 `autoDraftDisabled` 设置为 True：

```
PUT https://NSX-Manager-IP-
```

```
Address/api/4.0/firewall/config/globalconfiguration
```

请求正文中包含：

```
<globalConfiguration>
  <layer3RuleOptimize>...</layer3RuleOptimize>
  <layer2RuleOptimize>...</layer2RuleOptimize>
  <tcpStrictOption>...</tcpStrictOption>
  <autoDraftDisabled>true</autoDraftDisabled>
</globalConfiguration>
```

- **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：**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。

## 文档修订历史



2017 年 7 月 6 日：第一版。

2017 年 8 月 21 日：第二版。添加了 1904842、1878081、1910593。

2017 年 10 月 2 日：第三版。更新了建议的最低 NSX 版本。

## 已解决的问题

已解决的问题分为以下几类。

- [NSX 6.2.8 中解决的安装和升级相关问题](#)
- [NSX 6.2.8 中解决的网络连接和 Edge 服务相关问题](#)
- [NSX 6.2.8 中解决的 NSX Manager 问题](#)
- [NSX 6.2.8 中解决的安全服务问题](#)
- [NSX 6.2.8 中解决的解决方案互操作性问题](#)

### NSX 6.2.8 中解决的安装和升级相关问题

- 已修复问题 1854519：在从 VLAN 迁移到桥接的 VXLAN 后，虚拟机丢失南北向连接  
在 DLR 上将虚拟机网络从 VLAN 切换到桥接的 VXLAN 后，到虚拟机的输入流量将会立即丢失。*6.2.8 中已修复此问题。*

### NSX 6.2.8 中解决的网络连接和 Edge 服务相关问题

- 已修复问题 1849037：在与 NSX Edge 的通信链路中断时，NSX Manager API 线程耗尽  
如果 NSX Manager 和 NSX Edge 虚拟机之间的通信通道中断，到 Edge 虚拟机的状态/统计信息请求将挂起并阻止 API 线程。多个此类请求可能会最终耗尽所有 API 线程。*6.2.8 中已修复此问题。*
- 已修复问题 1865394：未从 dvPortGroup 端口中删除流量调整策略  
在配置连接到 NSX Edge vNIC 的 dvPortGroup 端口时，将在该端口上设置流量调整策略 (TSP)。预期行为是，在将 vNIC 从该端口断开连接时，将删除（清除）TSP。NSX Manager 触发的以下情况导致更改/断开连接到 NSX Edge vNIC 的 dvPortGroup 端口：
  - 重新部署 NSX Edge
  - 升级 NSX Edge
  - 断开并重新连接 NSX Edge
  - 更改 NSX Edge 设备大小
  - 删除 NSX Edge 接口
  - 删除 NSX Edge*6.2.8 中已修复此问题。*
- 已修复问题 1704940：如果 pCPU 计数超过 256 个，则可能会在 ESXi 主机上显示紫色诊断屏幕  
对于每个 pCPU，NSX DLR 具有一个流量表，并且 pCPU 数限制为 256 个。如果 pCPU 计数超过 256 个，这会导致崩溃。*6.2.8 中已修复此问题。*
- 已修复问题 1892265：在每次发布后，不会从 `/common/tmp` 目录中删除 NSX Edge 文件包，从而导致 `/common` 目录填满  
`/common` 目录填满并且 NSX Manager 空间不足，因为不会从 `/common/tmp` 中删除 NSX Edge 文件包 (sslvpn-plus config)。*6.2.8 中已修复此问题。*
- 已修复问题 1681063：在 vCloud Director 中未准确反映某些 Edge 网关的 VPN 隧道状态  
vCloud Director (vCD) 和 NSX 显示不同的 IPSec VPN 隧道状态。甚至在 IPSec 隧道已启动并传送流量时，vCD 也会将其显示为关闭。*6.2.8 中已修复此问题。*
- 已修复问题 1849760：如果通过 IBGP 网络发现某些前缀使下一跃点属于前缀子网，路由进程可能会独占 CPU

如果 DLR 控制虚拟机与 IBGP 中的 ESG 配对使用，而 ESG 通过 EBGP 与物理路由器配对使用，则会在此设置中出现该问题。此外，DLR 控制虚拟机正在运行 HA。BGP 会话正在使用激进定时器。如果底层网络开始出现抖动，从而导致 BGP 邻居出现抖动，DLR 控制虚拟机还会重新发现抖动邻居的前缀并需要解析这些前缀。如果发现的前缀子网涵盖下一跃点的 IP（例如 10.0.0.0/8 覆盖 10.1.1.2），则路由进程可能会进入递归循环。*6.2.8 中已修复此问题。*

## NSX 6.2.8 中解决的 NSX Manager 问题

- 已修复问题 1892208：NSX Manager 数据库仅显示一个数据存储（vmx 文件位置），但 UI 显示两个数据存储（当前数据存储和配置的数据存储）。*6.2.8 中已修复此问题。*
- 已修复问题 1861785：在具有 vCloud Director (vCD) 和 vRealize Operations (vROps) 部署的 NSX Manager 上观察到 100% CPU 使用率  
如果您的数据库在 `system_event_message_params` 和 `system_event_event_metadata` 表中具有大量孤立记录，API 需要较长的时间响应来自 vCD 的请求，同时将 vCD 客户端断开连接，从而导致再次调用相同的 API。这将导致较高的 CPU 使用率。移除孤立记录将会解决该问题。*6.2.8 中已修复此问题。*
- 已修复问题 1760940：很多同时进行的 vMotion 任务触发 NSX Manager 高 CPU 使用率  
DFW 配置了动态安全组，这些组具有基于虚拟机名称或虚拟机客户机操作系统的条件。有关详细信息，请参阅 [VMware 知识库文章 2150668](#)。*6.2.8 中已修复此问题。*

## NSX 6.2.8 中解决的安全服务问题

- 已修复问题 1836322：在编辑 NSX 防火墙规则时出现“Flash 错误”  
有时，在编辑安全组时，vSphere Web Client UI 显示与 Flash 插件相关的错误。*6.2.8 中已修复此问题。*
- 已修复问题 1832912：在将主机置于维护模式时，该主机中的某些虚拟机丢失以前应用的防火墙规则  
如果将主机置于维护模式并且 DRS 将所有虚拟机移到另一个主机，该主机中的某些虚拟机将丢失以前应用的防火墙规则。解决办法是，避免使用基于计算机名称或计算机操作系统名称的动态条件创建安全组。*6.2.8 中已修复此问题。*
- 已修复问题 1818550：在具有大量虚拟机和嵌套安全组的主机上，分组对象更新延迟  
在具有大量虚拟机和嵌套安全组的主机上，单个清单更改将导致分组对象更新刷新，从而导致主机的分组对象更新延迟很长时间。*6.2.8 中已修复此问题。*
- 已修复问题 1798537：ESXi 上的 DFW 控制器进程 (vsfwd) 可能会出现内存不足问题  
如果环境中的 DFW 配置具有大量规则或大型安全组，ESXi 上的 DFW 控制器进程 (vsfwd) 可能会出现内存不足问题，而无法将规则发布到数据路径。*6.2.8 中已修复此问题。*
- 已修复问题 1853106：在 PSK 模式下，取消选中证书或修改 IPsec VPN 的某些 IPsec 配置时，用户界面上会显示错误  
对于基于证书进行身份验证的 IPsec VPN，在 PSK 模式下取消选中证书或修改某些配置时，将会在“全局配置”选项卡上看到错误“无法读取证书和密钥: 002 忘记密钥” (Failed to read certs & secrets: 002 forgetting secrets)。*6.2.8 中已修复此问题。*

## NSX 6.2.8 中解决的解决方案互操作性问题

- 已修复问题 1838742：NSX Edge UI/API 版本可能与在 VCD 环境中部署的版本不同  
将 vCNS 升级到 NSX 期间，在升级 NSX Manager 后，必须明确升级或重新部署所有 vCNS Edge，然后再在 vCloud Director 上执行任何其他编辑操作。如果未启动升级，在 UI 和 API 中显示的 NSX Edge 版本可能与部署的版本不同。*6.2.8 中已修复此问题。*

# 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](#)
- [逻辑网络已知问题和 NSX Edge 已知问题](#)
- [安全服务已知问题](#)
- [监控服务已知问题](#)
- [解决方案互操作性已知问题](#)
- [NSX Controller 已知问题](#)

## 一般已知问题

- **问题 1708769:** 在 NSX 中运行 SVM (服务虚拟机) 快照后, SVM 延迟增加  
出现该问题的原因是, 运行服务虚拟机 (SVM) 快照可能导致网络延迟增加。快照有时会被环境中运行的备份应用程序调用。

*解决办法:* 请参阅 [VMware 知识库文章 2146769](#)。

- **问题 1716328:** 移除处于维护模式的主机可能会导致之后的集群准备失败。  
如果管理员将启用了 NSX 的 ESXi 主机置于维护模式, 然后将该主机从准备好 NSX 的集群中移除, NSX 将无法删除所移除主机的 ID 号记录。安装处于此状态中后, 如果另一个集群中还有另一个使用相同 ID 的主机, 或者如果该主机将被添加到另一个集群, 则该集群的准备过程将失败。

*解决办法:* 重新启动 NSX Manager 或运行以下 API 以删除多余的条目。执行 API 方法中的 PUT:

`https://nsx-manager-address/api/internal/firewall/updatestatus`

- **问题 1659043:** 当 NSX Manager 与 USVM 的通信超时, 客户机侦测的服务状态报告为“未就绪”  
当通过 NSX Manager 在内部消息总线 (rabbit MQ) 上执行预期的密码更改流程失败时, 系统可能会对 客户机侦测通用 SVM 报告类似以下内容的错误消息: “拒绝明文登录: 用户 ‘usvm-admin-host-14’ - 无效的凭据” (PLAIN login refused: user 'usvm-admin-host-14' - invalid credentials)。

*解决办法:* 要在 USVM 和 NSX Manager 之间重新建立连接, 请重新启动 USVM, 或者手动将其删除, 然后选择服务编排 UI 上的“解决”按钮, 以便仅为受影响的主机重新部署 USVM。

- **问题 1662842:** 客户机侦测: 尝试解析不可解析的 Windows SID 时, MUX 和 USVM 之间的连接丢失  
随着每个客户机侦测进入和退出警告状态, 客户机侦测服务将进入警告状态。在客户机侦测虚拟机重新连接之前, 网络事件将不会被递送到 NSX Manager。当通过客户机侦测路径检测到登录事件时, 这会同时影响活动监控和 ID 防火墙。

*解决办法:* 要使客户机侦测返回到稳定状态, 必须将客户机侦测虚拟机配置为忽略对这些已知 SID 的查找。要实现此操作, 请更新每个客户机侦测虚拟机上的配置文件, 然后重新启动此服务。此外, 还可以使用 Active Directory 日志采集功能作为解决办法来检测 ID 防火墙的登录事件。

对不可解析的 SID 忽略 SID 查找的步骤:

1. 登录到客户机侦测虚拟机。
2. 编辑位于 /usr/local/usvmmgmt/config/ignore-sids.lst 的文件。
3. 附加以下 2 行:  
S-1-18-1  
S-1-18-2
4. 保存并关闭该文件。
5. 使用以下命令重新启动客户机侦测服务:  
rcusvm restart。

- **问题 1558285:** 从 Virtual Center 中删除部署了客户机侦测的集群时会导致空指针异常  
在从 VC 中移除集群之前, 必须首先移除客户机侦测等服务

*解决办法:* 对于没有与任何集群关联的服务部署, 删除其 EAM 代理机构。

- **问题 1629030:** 数据包捕获中央 CLI (调试数据包捕获和显示数据包捕获) 需要 vSphere 5.5U3 或更

## 高版本

较早的 vSphere 5.5 版本不支持这些命令。

*解决办法：*VMware 建议所有 NSX 客户运行 vSphere 5.5U3 或更高版本。

- **问题 1568180：**使用 vCenter Server Appliance (vCSA) 5.5 时，NSX 的功能列表不正确

您可以通过在 vSphere Web Client 中选择许可证，然后单击操作 > 查看功能来查看该许可证的功能。如果您升级到 NSX 6.2.3，您的许可证会升级到企业许可证，这将启用所有功能。然而，如果 NSX Manager 已经在 vCenter Server Appliance (vCSA) 5.5 中注册，那么，选择“查看功能”将会显示升级之前所使用的许可证功能列表，而不是新的企业许可证。

*解决办法：*所有企业许可证都有相同的功能，即使它们未正确显示在 vSphere Web Client 中也是如此。有关详细信息，请参见 [NSX 许可页面](#)。

- **问题 1477280：**未部署控制器时，无法创建硬件网关实例

必须先部署控制器，然后才能配置硬件网关实例。如果不先部署控制器，会显示错误消息“无法在控制器上执行操作” (Failed to do the Operation on the Controller)。

*解决办法：*无。

- **问题 1491275：**在某些情况下 NSX API 返回 JSON 而非 XML

有时，API 请求导致向用户返回的是 JSON 而非 XML。

*解决办法：*在请求标头中添加 Accept: application/xml。

## 安装和升级已知问题

- **新增：**问题 1905064：在主机升级期间，集群中的某些主机与 NSX Manager 和控制器的 TCP 连接中断

如果 ESXi 主机与 NSX Manager 的 TCP 连接在升级期间中断，则该主机无法获取控制器信息。这会禁止控制器将与 NSX 相关的配置推送到该主机，从而导致该主机中的所有虚拟机断开连接。

*解决办法：*重新引导受影响的主机。

- **新增：**问题 1910593：应答参数在 NSX Manager 升级 API 中区分大小写

如果使用 NSX API 升级 NSX Manager，并且要启用 SSH 或加入 VMware CEIP 计划，您必须为应答参数指定“Yes”（而不是“YES”）。

*解决办法：*有关使用 API 进行升级的详细信息，请参见 NSX API 指南。

- **问题 1838229：**在升级到 NSX 6.1.5 或更高版本后，NSX 负载均衡器上的 HTTP/HTTPS 事务失败。  
从 NSX 6.1.5 开始，在启用 x-forwarded-for 时，HTTP 连接模式已从被动关闭 (option httpclose) 更改为默认 HTTP 服务器关闭 (option http-server-close) 模式，从而在从服务器收到响应后关闭面向服务器的连接时将面向客户端的连接保持打开状态。这会导致某些应用程序出现问题，因为在低于 6.1.5 的 NSX 版本中，负载均衡器不会主动关闭连接，而是在两个方向上插入“Connection:close”标头以指示客户端或服务器关闭连接。

*解决办法：*使用 option httpclose 脚本添加一个应用程序规则，并将其与虚拟服务器相关联。

- **问题 1820723：**从 6.2.x 升级到 6.2.7 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 6.2.7 并将集群 VIB 升级到 6.2.7 后，即使安装状态显示成功并启用了防火墙，通信通道运行状况也会将 NSX Manager 到防火墙代理的连接以及 NSX Manager 到控制平面代理的连接显示为关闭。这会导致防火墙规则发布和安全策略发布失败，并且不会将 VXLAN 配置向下发送到主机。

*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 1435504：从 6.0.x 或 6.1.x 升级到 6.2.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 6.2.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 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 或更高版本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 1730017：从 6.2.3 到 6.2.7 的升级不显示客户机侦测的版本变化  
由于 6.2.3 的客户机侦测模块已经是最新版本，因此其版本在升级到 6.2.7 后会保持不变。请注意，从较低的 NSX 版本升级可能会显示版本更改为 6.2.7

**解决办法：**此问题不会影响任何功能。

- 问题 1683879：在内存低于 8 GB 的主机上，可能无法升级到 NSX 6.2.3 或更高版本  
NSX 6.2.3 及更高版本要求准备好的运行网络和安全服务的主机上至少具有 8 GB 内存。ESXi 6.0 的最低内存要求 (4 GB) 不足以运行 NSX。

**解决办法：**无。

- 问题 1673626：从 vCloud Networking and Security 升级到 NSX 后，不允许通过 `/api/3.0/edges` 修改 tcpLoose

从 vCloud Networking and Security 升级到 NSX 后，如果尝试在以下 API 请求中修改 tcpLoose 设置，您将会看到错误：`/api/3.0/edges`

**解决办法：**在 API 请求 `/api/4.0/firewall/config` 的 globalConfig 部分中改用 tcpPickOngoingConnections 设置。

- 问题 1658720：在从 vCNS 升级到 NSX 时，如果集群在 vCNS 部署中安装了 VXLAN，但未安装 vShield App（或在升级之前已将其移除），则将无法为给定的集群启用 DFW  
出现此问题是由于在升级主机时未调用集群同步状态。

**解决办法：**重新启动 NSX Manager。

- **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 Virtual Center 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 1465249：即使主机处于脱机状态，客户机侦测的安装状态也会显示“成功”**  
在有一个主机处于脱机状态的集群上安装客户机侦测后，处于脱机状态的主机将“安装状态”显示为“成功”，而将“状态”显示为“未知”。  
**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 1660355：从 6.1.5 迁移到 6.2.3 的虚拟机将不支持 TFTP ALG**  
即使已启用主机，从 6.1.5 迁移到 6.2.3 的虚拟机也不支持 TFTP ALG。  
**解决办法：**在排除列表中添加并移除该虚拟机，或重新启动该虚拟机，以便创建将支持 TFTP ALG 的新 6.2.3 筛选器。
- **问题 1394287：在虚拟线路中添加或移除虚拟机不会更新 vShieldApp 规则中的 IP 地址集**  
如果现有 vCNS vShield App 防火墙安装未在增强模式下升级到 NSX 分布式防火墙，则防火墙规则基于虚拟线路的新虚拟机将不会更新 IP 地址。因此，这些虚拟机将不受 NSX 防火墙的保护。此问题仅在以下场景中出现：
  - 将 Manager 从 vCNS 升级到 NSX 后，没有切换到 DFW 增强模式。
  - 如果将新虚拟机添加到 virtualWire 时，将 vShield App 规则设置为使用这些 virtualWire，那么，这些规则将不会为新虚拟机设置新的 IP 地址。  
这将导致新虚拟机不受 vShieldApp 保护。**解决办法：**再次发布规则将设置新地址。
- **问题 1386874：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。
- 虚拟机的 VC 任务窗格中没有显示克隆和重新配置等任务正在进行。
- 在虚拟机的 VC 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。

- 如果未准备好环境中的所有集群，则分布式防火墙的升级消息不会显示在“安装”页面的“主机准备”选项卡上

为网络虚拟化准备集群时，会在这些集群上启用分布式防火墙。如果未准备好环境中的所有集群，则分布式防火墙的升级消息不会显示在“主机准备”选项卡上。

*解决办法：*使用以下 REST 调用升级分布式防火墙：

```
PUT https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state
```

- 问题 1215460：如果在升级后修改服务组以添加或删除服务，则这些更改不会反映在防火墙表中  
在升级过程中，Edge 防火墙表中用户创建的服务组展开，例如，防火墙表中的“服务”列显示服务组内的所有服务。如果在升级后修改服务组以添加或删除服务，则这些更改不会反映在防火墙表中。

*解决办法：*使用其他名称新建一个服务组，并在防火墙规则中使用此服务组。

- 问题 1088913：vSphere Distributed Switch MTU 无法更新

在准备集群时，如果指定的 MTU 值低于 vSphere Distributed Switch 的 MTU 值，则 vSphere Distributed Switch 不会更新此值。这是为了确保不会意外丢弃具有较高帧大小的现有流量。

*解决办法：*确保在准备集群时指定的 MTU 高于或匹配 vSphere Distributed Switch 的当前 MTU。VXLAN 所需的最低 MTU 为 1550。

- 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 1288506：从 vCloud Networking and Security 5.5.3 升级到 NSX for vSphere 6.0.5 或更高版本以后，如果使用 DSA-1024 密钥大小的 SSL 证书，NSX Manager 不会启动

DSA-1024 密钥大小的 SSL 证书在 NSX for vSphere 6.0.5 或更高版本中不受支持，因此未能成功升级。

*解决办法：*在开始升级之前，导入密钥大小受支持的新 SSL 证书。

- 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 1402307：如果 vCenter 在 NSX for vSphere 升级过程中重新引导，将显示错误的集群状态

对于具有多个准备好 NSX 部署的集群，如果在升级过程中进行主机准备，并且 vCenter Server 在至少准备了一个集群后重新引导，其他集群的“集群状态”可能会显示为“未就绪”，而不是“更新”链接。此外，vCenter 中的主机可能会显示“需要重新引导”。

*解决办法：*不要在主机准备过程中重新引导 vCenter。

- 问题 1487752：升级期间短暂失去第三方防病毒防护



从 NSX 6.0.x 升级到 NSX 6.1.x 或 6.2.x 时，您可能会遇到虚拟机短暂失去第三方防病毒防护的问题。从 NSX 6.1.x 升级到 NSX 6.2 时，不会受此问题影响。

**解决办法：**无。

- **问题 1491820：**升级到 NSX 6.2 后，NSX Manager 日志收集到 **WARN messagingTaskExecutor-7** 消息

从 NSX 6.1.x 升级到 NSX 6.2 后，NSX Manager 日志中充满类似以下内容的消息：WARN

```
messagingTaskExecutor-7 ControllerInfoHandler:48 - host is unknown: host-15  
return empty list.这对操作并无影响。
```

**解决办法：**无。

- **问题 1284735：**从 vCNS 升级后，无法将新分组对象放在某些升级的分组对象中  
vCNS 5.x 支持在 GlobalRoot 以下的范围（低于 NSX 范围）创建分组对象。例如，在 vCNS 5.x 中，您可以在 DC 或 PG 级别创建一个分组对象。与此不同，NSX 6.x 用户界面在 GlobalRoot 中创建这些对象，这些新创建的分组对象无法添加到在升级前的 vCNS 安装中以较低范围（DC 或 PG）创建的现有分组对象中。

**解决办法：**请参见 [VMware 知识库文章 2117821](#)。

- **问题 1495969：**从 vCNS 5.5.4 升级到 NSX 6.2.x 后，“主机准备”选项卡上的防火墙保持禁用状态  
从 vCNS 5.5.x 升级到 NSX 6.2.x 并升级所有集群后，“主机准备”选项卡上的防火墙保持禁用状态。此外，UI 中不显示升级防火墙的选项。仅当数据中心存在不属于任何已准备集群的主机时才会发生此情况，原因是 VIB 不会安装在这些主机上。

**解决办法：**要解决此问题，请将主机移动到已准备好 NSX 6.2 部署的集群。

- **问题 1495307：**升级过程中，L2 和 L3 防火墙规则未发布到主机  
将更改发布到分布式防火墙配置后，UI 和 API 中无限期保持**正在进行中**状态，且 L2 或 L3 规则的日志均未写入到 vsfwd.log 文件中。

**解决办法：**在 NSX 升级过程中，不要将更改发布到 Distributed Firewall 配置。要退出**正在进行中**状态并解决此问题，请重新引导 NSX Manager 虚拟设备。

- **问题 1474066：**启用或禁用 IP 检测的 NSX REST API 调用似乎不起作用

如果主机集群准备尚未完成，则启用或禁用 IP 检测的 NSX REST API 调用 (<https://<nsxmgr-ip>/api/2.0/xvs/networks/universalwire-5/features>) 将不起作用。

**解决办法：**发出 API 调用之前，请确保主机集群准备已完成。

- **问题 1479314：**NSX 6.0.7 SSL VPN 客户端无法连接到 NSX 6.2 SSL VPN 网关

在 NSX 6.2 SSL VPN 网关中，已禁用 SSLv2 和 SSLv3 协议。这意味着 SSL VPN 网关只接受 TLS 协议。SSL VPN 6.2 客户端已升级，建立连接时默认使用 TLS 协议。在 NSX 6.0.7 中，SSL VPN 客户端使用较旧版本的 OpenSSL 库和 SSLv3 协议建立连接。NSX 6.0.x 客户端尝试连接到 NSX 6.2 网关时，连接建立在 SSL 握手阶段失败。

**解决办法：**升级至 NSX 6.2 后，将 SSL VPN 客户端升级至 NSX 6.2。有关升级说明，请参见 [NSX 升级文档](#)。

- **问题 1434909：**必须为新的或已升级逻辑路由器创建一个分段 ID 池

在 NSX 6.2 中，必须存在一个具有可用分段 ID 的分段 ID 池，然后才能将逻辑路由器升级至 6.2 或创建新的 6.2 逻辑路由器。即使未计划在部署中使用 NSX 逻辑交换机也是如此。

**解决办法：**如果 NSX 部署没有本地分段 ID 池，则创建一个本地分段 ID 池，这是升级或安装 NSX 逻辑路由器的先决条件。

- **问题 1459032：**配置 VXLAN 网关时出错

使用静态 IP 池配置 VXLAN（网络和安全 > 安装 > 主机准备 > 配置 VXLAN）且配置无法在 VTEP 上设置 IP 池网关 IP（因为网关未正确配置或不可访问）时，主机集群的 VXLAN 配置会进入“错误 (红色)”状态。

错误消息为：**无法在主机上设置 VXLAN 网关** (VXLAN Gateway cannot be set on host)，错误状态为：VXLAN\_GATEWAY\_SETUP\_FAILURE。在 REST API 调用 GET <https://<nsxmgr-ip>/api/2.0/nwfabric/status?resource=<cluster-moid>> 中，VXLAN 的状态如下所示：



```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.nsxmgr.vxlan</featureId>
  <featureVersion>5.5</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>RED</status>
  <message>VXLAN Gateway cannot be set on host</message>
  <installed>true</installed>
  <enabled>true</enabled>
  <errorStatus>VXLAN_GATEWAY_SETUP_FAILURE</errorStatus>
</nwFabricFeatureStatus>
```

**解决办法：**要解决此错误，有两种办法。

- 方法 1：移除主机集群的 VXLAN 配置，通过确保网关配置正确且可访问来修复 IP 池中的基础网关设置，然后为主机集群重新配置 VXLAN。
- 方法 2：执行以下步骤。
  1. 通过确保网关配置正确且可访问来修复 IP 池中的基础网关设置。
  2. 将主机置于维护模式，确保主机上没有任何活动的虚拟机流量。
  3. 从主机中删除 VXLAN VTEP。
  4. 使主机退出维护模式。使主机退出维护模式会触发 NSX Manager 上的 VXLAN VTEP 创建过程。NSX Manager 将尝试在主机上重新创建所需 VTEP。

- 问题 1463767：在跨 vCenter 部署中，通用防火墙配置区域可能位于本地配置区域下（从属于本地配置区域）  
如果将辅助 NSX Manager 置于独立（过渡）状态，然后将其更改回辅助状态，则会在复制的继承自主 NSX Manager 的通用配置区域上方列出临时处于独立状态时所做的任何本地配置更改。这会产生错误状况：**辅助 NSX Manager 上的通用区域应该在所有其他区域顶部** (universal section has to be on top of all other sections on secondary NSX Managers)。

**解决办法：**使用 UI 选项向上或向下移动区域，使本地区域位于通用区域下方。

- 问题 1289348：升级后，防火墙规则和网络侦测服务可能与 NSX Manager 不同步  
从 NSX 6.0 升级至 NSX 6.1 或 6.2 后，NSX Firewall 配置会显示错误消息：**同步失败 / 不同步** (synchronization failed / out of sync)。使用**强制同步服务 > 防火墙**操作无法解决该问题。  
**解决办法：**在 NSX 6.1 和 NSX 6.2 中，安全组或 dvPortgroup 可以绑定到服务配置文件，但两者不能同时绑定。要解决此问题，请修改服务配置文件。
- 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-vdpi。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 1485862：从主机集群卸载 NSX 有时会导致出现错误状况

使用安装 > 主机准备 选项卡上的“卸载”操作时，可能会发生错误并在主机的 EAM 日志中显示 eam.issue.OrphanedAgency 消息。使用“解决”操作并重新引导主机后，即使已成功卸载 NSX VIB，还是会显示错误状态。

**解决办法：**从 vSphere ESX Agent Manager 中删除孤立的代理机构（系统管理 > vCenter Server 扩展 > vSphere ESX Agent Manager）。

- **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 1393889：**即使未建立 IP 连接，数据安全服务状态仍显示为“运行”

数据安全设备可能未收到 DHCP 的 IP 地址或连接了错误的端口组。

**解决办法：**确保数据安全设备从 DHCP/IP 池获取 IP，且可从管理网络进行访问。从 NSX/ESX 检查对数据安全设备进行的 ping 是否成功。

- 使用“安装”页面上的“服务部署”选项卡部署的服务虚拟机无法开机

**解决办法：**按照下面的步骤执行操作。

1. 从集群中的 ESX 代理资源池中手动移除服务虚拟机。
2. 单击网络和安全，然后单击安装。
3. 单击服务部署选项卡。
4. 选择相应的服务并单击解决图标。  
将重新部署服务虚拟机。

- **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。

**解决办法：**单击红色的警告图标，然后选择“解决办法”。

## NSX Manager 已知问题

- **新增：**问题 1904842：未在 vCenter 或 Platform Service Controller 中注册 NSX Manager  
NSX Manager 未显示在 UI 中，并且对 NSX Manager 的任何 REST 调用均失败。

**解决办法：**重新启动 NSX 管理服务或重新引导 NSX Manager 设备。

- **新增：**问题 1826225：合作伙伴服务虚拟机的服务状态在 NSX Manager 中报告为“未知”  
合作伙伴服务虚拟机的服务状态在 NSX Manager 中报告为“未知”。在合作伙伴虚拟机具有过期的数据库条目时，将会出现该问题。

**解决办法：**与 VMware 客户支持人员联系。

- **新增：**问题 1713669：NSX Manager 磁盘已装满 IDFW 数据

无论是否使用 IDFW 规则，客户机侦测和事件日志服务器检测到的登录事件都会存储在 NSX Manager 数据库中，并在这些事件过期后在该数据库中保留 30 天。在具有大量登录活动的环境中，该数据库可能会增大并影响 NSX Manager 磁盘上的空间。

**解决办法：**没有解决办法。如果遇到此问题，请与 VMware 支持人员联系。

- **问题 1806368：**对于跨 VC 故障切换，如果在以前发生故障的主 NSX Manager（在故障切换后再次变为主 NSX Manager）中重新使用旧控制器，则不会将 DLR 配置推送到所有主机。

在跨 VC 设置中，当主 NSX Manager 发生故障时，将升级辅助 NSX Manager 作为主 NSX Manager，并部署

新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 1772911：**NSX Manager 磁盘空间消耗量迅速增加，任务和作业表大小增加，并且 CPU 使用率较高

NSX Manager CPU 持续处于 100% 或其峰值经常达到 100%。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。磁盘空间消耗快速增长，DB 大小也随之增加，从而导致 NSX Manager 的性能下降。

**解决办法：**请联系 VMware 技术支持人员。

- **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  
如果环境中的多个 VMware vCenter Server 具有多个 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 1671067：**同时安装了 ESXTOP 插件时，NSX 插件不会显示在 vCenter Web Client 中  
在部署 NSX 并在 vCenter 中成功注册之后，NSX 插件不会显示在 vCenter Web Client 中。此问题是由于 NSX 插件和 ESXTOP 插件之间存在冲突所导致。

**解决办法：**通过以下过程移除 ESXTOP 插件：

1. 确保最近对 vCenter 虚拟机进行了 vCenter 快照备份（不使用静默方式）
2. 删除 `/usr/lib/vmware-vmware-vsphere-client/plugin-packages/esxtop-plugin`  
`rm -R /usr/lib/vmware-vmware-vsphere-client/plugin-packages/esxtop-plugin`
3. 删除 `/usr/lib/vmware-vmware-vsphere-client/server/work`  
`rm -R /usr/lib/vmware-vmware-vsphere-client/server/work`
4. 重新启动 Web Client  
`service vmware-vsphere-client restart`
5. （可选）确保以下命令不输出任何内容：`"tail -f /var/log/vmware/vsphere-client/logs/eventlog.log | grep esx"`
6. 如果整合 vCenter 快照是回滚选项的首选方法，请确保执行此操作

- **问题 1486403：**NSX Manager 不接受带有空格分隔符的 DNS 搜索字符串  
NSX Manager 不接受带有空格分隔符的 DNS 搜索字符串。只能使用逗号作为分隔符。例如，如果 DHCP 服务器为 DNS 搜索列表播发 `eng.sample.com` 和 `sample.com`，则 NSX Manager 会配置 `eng.sample.com sample.com`。

**解决办法：**使用逗号分隔符。NSX Manager 只接受在 DNS 搜索字符串中使用逗号分隔符。

- **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：**

执行下列步骤：

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 1534606：**“主机准备”页面加载失败

当在链接模式下运行 Virtual Center 时，每个 VC 必须连接到所运行的 NSX 版本相同的 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：**应当将所有 NSX Manager 都升级到相同的 NSX 软件版本。

- **问题 1386874：**vSphere Web Client 中不显示“网络和安全”选项卡

vSphere 升级到 6.0 后，使用 root 用户名登录到 vSphere Web Client 时，看不到“网络和安全”选项卡。

**解决办法：**使用 administrator@vsphere.local 登录，或使用升级前 vCenter Server 上其角色已在 NSX Manager 中定义的任何其他 vCenter 用户登录。

- **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 1477041：**NSX Manager 虚拟设备摘要页面不显示 DNS 名称

登录到 NSX Manager 虚拟设备时，“摘要”页面显示 DNS 名称字段。即使为 NSX Manager 设备定义了 DNS 名称，此字段仍为空。

**解决办法：**您可以在“管理”>“网络”页面上查看 NSX Manager 的主机名和搜索域。

- **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 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：**执行下列步骤：

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 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 1489768：在数据中心添加命名空间的 NSX REST API 调用的行为更改**

在 NSX 6.2 中，POST `https://<nsxmgr-ip>/api/2.0/namespace/datacenter/` REST API 调用返回包含绝对路径的 URL，例如

`http://198.51.100.3/api/2.0/namespace/api/2.0/namespace/datacenter/datacenter-1628/2`。在先前版本的 NSX 中，此 API 调用返回包含相对路径的 URL，例如：`/api/2.0/namespace/datacenter/datacenter-1628/2`。

**解决办法：**无。

## 逻辑网络已知问题和 NSX Edge 已知问题

- **新增：**问题 1878081：某些路由是从 Edge 服务网关上的转发表中刷新获得在极少数情况下，某些路由是从转发表中刷新获得。这会导致流量中断。

**解决办法：**重新引导 Edge 节点。

- 问题 1798847：在跨 VC NSX 设置中，VXLAN UDP 端口更新可能会一直处于停滞状态。如果主 NSX Manager 没有配置任何辅助 NSX Manager，VXLAN UDP 端口更新将会一直挂起。

**解决办法：**使用 NSX Manager API 在主 NSX Manager 上恢复端口更新工作流。

- 问题 1698286：跨 vCenter NSX 环境中仅在主 NSX Manager 上支持硬件 VTEP

跨 vCenter NSX 环境中，仅在主 NSX Manager 上支持硬件网关交换机配置和操作。硬件网关交换机必须绑定到非通用逻辑交换机。辅助 NSX Manager 不支持硬件网关配置。

**解决办法：**跨 vCenter NSX 环境中，建议使用 L2 桥接将逻辑交换机连接到物理网络。

- **问题 1844966：NSX Edge 文件系统变为只读**

如果 Edge 所在的位置出现任何存储连接问题，Edge 文件系统可能会进入只读状态以保护操作系统文件系统。这是 Linux 服务器中的预期行为。有关详细信息，请参阅 [VMware 知识库文章 2146870](#)。

**解决办法：**执行以下操作：

1. 重新部署 Edge。
2. 重新引导 Edge（HA 对中的两个 Edge）。
3. 强制同步 Edge。

- **问题 1799261：NSX Edge 在升级或重新部署后可能陷入脑裂状况**

在备用 NSX Edge 上，`show service highavailability` CLI 命令将高可用性状态显示为“备用”，但将配置引擎状态显示为“活动”。

**解决办法：**重新引导备用 NSX Edge。

- **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，当启动程序使用 PSK 和 XAUTH 发送身份验证请求时，Edge 会显示以下错误消息：“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 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 1733165：IPsec 可能会导致从 NSX Edge 转发表中移除动态路由**

如果使用可通过动态路由访问的子网作为 IPsec 配置的远程子网，则 NSX Edge 会从转发表中移除该子网，并且即使在从 IPsec 配置中删除该子网后，也不会重新安装该子网。

**解决办法：**启用/禁用路由协议或清除路由邻居关系。

- **问题 1675659：优先使用浮动静态路由而不是 OSPF 动态路由**

如果启用了路由重新分发，则在 Edge 的路由表中错误地输入备用浮动静态路由，即使 OSPF 路由可用也是如此。

**解决办法：**要解决该问题，请禁止将静态路由重新分发到 OSPF。

**注意：**该问题不会影响数据路径。请参见 [VMware 知识库文章 2147998](#)。

- **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 1776073：**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 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 eBGP 邻居共享专用 AS 路径。

**解决办法：**没有解决办法可以使 Edge 在 BGP 更新中声明所有 AS 路径。

- **问题 1716545：**更改 Edge 的设备大小不更改备用 Edge 的 CPU 和内存预留

只有作为 HA 对的一部分创建的第一个 Edge 虚拟机才分配有预留设置。

要在两个 Edge 虚拟机上配置相同的 CPU/内存预留，请执行以下操作：

- 使用 PUT API <https://<NSXManager>/api/4.0/edgePublish/tuningConfiguration> 为两个 Edge 虚拟机设置明确的值。
- 或
- 禁用 Edge HA 后再将其重新启用，这将删除第二个 Edge 虚拟机，并使用默认预留设置重新部署新的 Edge 虚拟机。

**解决办法：**无。

- **问题 1510724：**创建新通用分布式逻辑路由器 (UDLR) 后，不在主机上填充默认路由

将 NSX Manager 从“独立”模式更改为“主”模式以在 NSX for vSphere 6.2.x 中进行跨 vCenter 配置后，您可能会遇到以下症状：

- 创建新 UDLR 时，不在主机实例上填充默认路由。
- 在 UDLR 控制虚拟机上填充路由，而不在主机实例上填充。
- 运行 `show logical-router host host-ID dlr Edge-ID route` 命令时，未能显示默认路由。

**解决办法：**要从此问题中恢复，请参阅 [VMware 知识库文章 2145959](#)。

- **问题 1492547：**关闭或重新引导具有最高 IP 地址的基于 NSX 的 OSPF 区域边界路由器后，聚合时间延长

如果关闭或重新引导 IP 地址并非最高的 NSSA 区域边界路由器，流量会快速聚合到其他路径。如果关闭或重新引导具有最高 IP 地址的 NSSA 区域边界路由器，重新聚合需要花费数分钟时间。可以手动清除 OSPF 进程以缩短聚合时间。

**解决办法：**请参见 [VMware 知识库文章 2127369](#)。

- **问题 1542416：**使用子接口进行 Edge 重新部署和 HA 故障切换后，数据路径会有 5 分钟时间无法工作

如果使用子接口，执行重新部署或 HA 故障切换操作后，将出现五分钟的故障时间。接口中未发现问题。

**解决办法：**没有解决办法。

- **问题 1706429：**初次部署逻辑（分布式）路由器后，在启用高可用性 (HA) 时出现的通信问题可能会导致两个逻辑路由器设备均处于活动状态。

如果在不启用 HA 的情况下部署一个逻辑路由器，然后再启用 HA（部署一个新的逻辑路由器设备），或者，如果先禁用 HA，然后再重新启用 HA，有时其中一个逻辑路由器设备会缺失到 HA 接口的连接路由。这会导致两个设备都处于活动状态。

**解决办法：**在缺失 HA 接口连接路由的逻辑路由器设备上，要么先断开逻辑路由器设备的 vNIC，然后再重新连接，要么重新引导逻辑路由器设备。

- **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 1676085：如果资源预留失败，将无法启用 Edge HA

从 NSX for vSphere 6.2.3 开始，如果无法为第二个 Edge 虚拟机设备预留足够的资源，在现有 Edge 上启用高可用性将失败。配置将回滚到上一个已知正常的配置。在以前的版本中，如果在 Edge 部署和资源预留失败后启用 HA，仍会创建 Edge 虚拟机。

**解决办法：**这是预期的行为更改。

- 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 1624663：单击“配置高级调试”后，系统会刷新 VC UI，但更改未保留  
在单击特定的 Edge ID > “配置” > “操作” > “配置高级调试”后，系统会刷新 VC UI，但更改未保留。

**解决办法：**直接转到 Edge 列表菜单，突出显示相应的 Edge，然后单击“操作” > “配置高级调试”以继续进行更改。

- 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 `https://NSX-Manager-IP-Address/api/4.0/edges/edgeId/status` API 并设置 `detailedStatus=true`。

- 问题 1647657：在使用 VDR 的 ESXi 主机上，显示命令只能为每个 VDR 实例最多显示 2000 个路由

在启用 VDR 的 ESXi 主机上，显示命令只能为每个 VDR 实例最多显示 2000 个路由，尽管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：**没有解决办法。

- 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 1663902：重命名 NSX Edge 虚拟机会中断流经 Edge 的流量

- 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 1642087：修改 IPsec VPN 扩展中的 securelocaltrafficbyip 参数值后，转发到目标网络失败使用 NSX Edge 服务网关时，您会遇到以下症状：
  - 在 NSX UI（“编辑 IPsec VPN”屏幕）中，将 securelocaltrafficbyip 值改为 0 后，无法再转发到 IPsec VPN 隧道的远程子网
  - 更改此参数后，您再也看不到 IP 路由表中远程子网的正确信息

*解决办法*：禁用后重新启用 IPsec VPN 服务。然后，验证 CLI 和 UI 中是否显示预期的路由信息。

- 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 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 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 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</property> </systemControl>
```

- 问题 1534602：UI 不显示 Edge 管理平面模式 (VIX/MSGBUS)，并且不提供从 VIX 更改为 MSGBUS 的选项  
当 Edge 设备处于 VIX 模式时，无法选择该设备以使其包含在 DFW 中，并且与 MSGBUS 模式相比，在 VIX 模式下运行集中式 CLI 命令所需的时间更长。  
*解决办法*：确保部署 Edge 的集群已为 NSX 做好准备，并且其“NSX Manager 到防火墙代理”处于“启动”状态，然后重新部署 Edge。

- 问题 1498243：当 BGP 邻居筛选器设置为“拒绝、任意、流出”时，分布式逻辑路由器为默认路由播发不正确的下一跃点  
如果在 NSX 分布式逻辑路由器 (DLR) 上启用了“默认源”，则将该 DLR 上的 BGP 邻居筛选器设置为“拒绝、任意、流出”会导致 DLR 为默认路由播发不正确的下一跃点地址。此错误仅在为 BGP 邻居筛选器添加

了以下属性时发生：

- 操作：拒绝
- 网络：任意
- 方向：流出

**解决办法：**无。

- **问题 1471561：使用直接连接的路由器无法建立 BGP/OSPF 邻居关系**  
使用直接连接的路由器时，如果该直接连接的网络存在 ECMP 路由，则动态路由无法按预期工作。  
**解决办法：**重新引导 Edge，或者删除关联的 vNIC 接口，然后再重新创建该接口。
- **问题 1089238：即使逻辑路由器 OSPF 已禁用，上游 Edge 服务网关依然播发逻辑路由器 LIF 路由**  
即使逻辑路由器 OSPF 已禁用，上游 Edge 服务网关也将继续播发从连接逻辑路由器的接口发现的 OSPF 外部 LSA。  
**解决办法：**禁用将连接的路由手动重新分发到 OSPF 并在禁用 OSPF 协议之前发布。这可确保路由被正确撤销。
- **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?vmob=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 DVPD 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。

## 安全服务已知问题

- 问题 1800196: 如果大量具有广播 MAC 地址的 IP 数据包与分布式防火墙拒绝规则匹配, VMkernel 日志记录将停止

分布式防火墙仅将拒绝数据包发送到单播 MAC 地址。在具有广播 MAC 地址的 IP 数据包与拒绝规则匹配时, 不会发送任何拒绝数据包。但在 vmkernel.log 中记录该事件。如果在网络中具有大量该流量, vmkernel.log 将由于日志负载太大而丢弃消息并停止日志记录。现在, 只有在启用了调试时, 才会记录拒绝具有广播 MAC 地址的数据包的情况。

*解决办法*: 将 DFW 防火墙规则中的“操作”从“拒绝”更改为“阻止”。

- 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](#)。

- 问题 1741844: 使用 ARP 侦听功能检测具有多个 IP 地址的 vNIC 的地址时, 导致 100% CPU 消耗  
当虚拟机的 vNIC 配置有多个 IP 地址, 并且启用了 ARP 侦听功能来进行 IP 检测时, 会出现此问题。IP 发现模块会持续不断地将 vNIC-IP 更新发送到 NSX Manager, 以更改配置有多个 IP 地址的所有虚拟机的 vNIC-IP 映射。

*解决办法*: 没有解决办法。ARP 侦听功能当前仅支持每个 vNIC 具有一个 IP 地址的情况。有关详细信息, 请参见《NSX 管理指南》中的“[虚拟机的 IP 发现](#)”一节。

- 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 1620460: NSX 无法阻止用户在服务编排规则区域创建规则

在 vSphere Web Client 中, “网络和安全: 防火墙”界面无法阻止用户向服务编排规则区域添加规则。应允

许用户在服务编排区域的上方/下方添加规则，但不应允许在此区域内部添加规则。

**解决办法：**不要在全球规则级别使用“+”按钮向服务编排规则区域添加规则。

- **问题 1682552：不报告分布式防火墙 (DFW) 的 CPU/内存/CPS 的阈值事件**  
即使设置为报告 CPU/内存/CPS 的 DFW 阈值，超过阈值时也不会报告阈值事件。

**解决办法：**

- 登录到每个 ESXi 主机，通过运行以下命令来重新启动 DFW 控制平面流程：  
`/etc/init.d/vShield_Stateful_Firewall restart`
- 使用以下命令验证状态：  
`/etc/init.d/vShield_Stateful_Firewall status`
- 将显示类似以下内容的结果：  
*“vShield-Stateful-Firewall 正在运行” (vShield-Stateful-Firewall is running)*

**注意：**您在执行此操作时应小心谨慎，因为此操作会将所有 DFW 规则再次推送到所有筛选器。如果规则很多，可能需要一些时间才能对所有筛选器强制实施这些规则。

- **问题 1717635：如果环境中存在多个集群，并且同时进行更改，则防火墙配置操作会失败**  
在具有多个集群的环境中，如果两个或更多用户接连不断地修改防火墙配置（例如，添加/删除区域或规则），有些操作会失败，并且用户将看到类似以下内容的 API 响应：  

```
<?xml version="1.0" encoding="UTF-8"?>
neutron-server.log.1:70282:2016-08-23 17:58:23.429 30787 ERROR vmware_nsx.plugins.nsx_v.plugin
<error>
<details> org.hibernate.exception.GenericJDBCException: Could not execute JDBC batch update; nested
exception is javax.persistence.PersistenceException: org.hibernate.exception.GenericJDBCException:
Could not execute JDBC batch update </details>
<errorCode>258
</errorCode>
</error>
```

**解决办法：**避免同时修改防火墙配置。

- **问题 1717994：分布式防火墙 (DFW) 状态 API 查询间歇性报告“500 内部服务器错误”**  
如果在向准备好主机的集群中添加新主机时发出 DFW 状态 API 查询，有些 API 查询尝试会失败，并显示“500 内部服务器错误”，然后在主机开始安装 VIB 后返回正确的响应。  
**解决办法：**在成功准备新主机之前，请勿使用 DFW 状态 API 查询。

- **问题 1686036：删除默认部分后，无法添加、编辑或删除防火墙规则**  
如果删除了默认的第 2 层或第 3 层部分，发布防火墙规则可能会失败。  
**解决办法：**请勿删除默认规则。如果在草稿中保存了使用默认规则的配置，请执行以下步骤：

1. 使用以下 DELETE API 调用彻底删除防火墙配置。  
`https://<NSX Manager IP>/api/4.0/firewall/globalroot-0/config`  
这将还原防火墙上的默认部分。
2. 将带有默认部分的已保存防火墙规则草稿加载到防火墙。

- **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 1626233：在 NetX 服务虚拟机 (SVM) 丢弃数据包时，跟踪流不生成已丢弃观察数**  
在将数据包发送到 NetX 服务虚拟机 (SVM) 后，跟踪流会话将退出。在 SVM 丢弃数据包时，跟踪流不会生成已丢弃观察数。

**解决办法：**没有解决办法。如果未注回跟踪流数据包，则可以认为 SVM 已丢弃数据包。



- 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 1491046：在 VMware NSX for vSphere 6.2.x 中，将 SpoofGuard 策略设置为“首次使用时信任” (TOFU) 时，IPv4 IP 地址不会自动获得批准

*解决办法：*请参见 [VMware 知识库文章 2144649](#)。

- 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 1462027：在跨 vCenter NSX 部署中，已保存防火墙配置的多个版本被复制到辅助 NSX Manager

通用同步将在辅助 NSX Manager 上保存通用配置的多个副本。已保存配置的列表包含在 NSX Manager 之间进行同步而创建的多个草稿，这些草稿具有相同名称且在同一时间创建或时间相差 1 秒。

*解决办法：*运行 API 调用删除重复的草稿。

DELETE : <https://<nsxmgr-ip>/api/4.0/firewall/config/drafts/>

查看所有草稿，找到要删除的草稿：

GET: https://<nsxmgr-ip>/api/4.0/firewall/config/drafts

在以下示例输出中，草稿 143 和 144 的名称和创建时间均相同，因此这两个草稿是重复的。同样，草稿 127 和 128 的名称相同且创建时间相差 1 秒，因此也是重复的。

```
<firewallDrafts>
  <firewallDraft id="144" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 P
M GMT" timestamp="1438816120917">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="143" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 P
M GMT" timestamp="1438816120713">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="128" name="AutoSaved_Wednesday, August 5, 2015 9:08:02 PM
GMT" timestamp="1438808882608">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="127" name="AutoSaved_Wednesday, August 5, 2015 9:08:01 PM
GMT" timestamp="1438808881750">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
</firewallDrafts>
```

- 问题 1449611：当服务编排中的防火墙策略因删除了安全组而不同步时，无法在 UI 中修复该防火墙规则  
*解决办法：*在 UI 中，您可以删除无效的防火墙规则，然后重新添加。或者，在 API 中，您可以通过删除无效的安全组来修复防火墙规则。然后同步防火墙配置：选择服务编排 > 安全策略，然后对具有关联防火墙规则的每个安全策略，单击操作并选择同步防火墙配置。为防止出现此问题，请修改防火墙规则，以便在删除安全组之前防火墙规则不会引用安全组。
- 问题 1557880：如果规则中使用的虚拟机 MAC 地址被修改，第 2 层 (L2) 规则可能会缺失  
由于 L2 规则优化在默认情况下处于启用状态，因此只有在 vNIC MAC 地址与源或目标 MAC 地址列表相匹配的情况下，同时指定了“源”和“目标”字段（非“任意”）的 L2 规则才会应用于 vNIC（或筛选器）。如果虚拟机与源或目标 MAC 地址不匹配，主机将不会应用这些 L2 规则。  
*解决办法：*要让 L2 规则应用于所有 vNIC（或筛选器），请将“源”或“目标”字段中的一个设置为“任意”。
- 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 1557924：在本地 DFW 规则的“应用对象”字段中允许使用通用逻辑交换机  
当通用逻辑交换机用作安全组成员时，DFW 规则可在“应用对象”字段中使用该安全组。这会间接在通用逻辑交换机上应用该规则，而此操作应该是禁止的，因为它可能会导致这些规则出现未知的行为。

解决办法：无。

- 问题 1559971：如果一个集群上的防火墙被禁用，不发布跨 vCenter NSX 防火墙排除列表  
在跨 vCenter NSX 中，当一个集群上的防火墙被禁用时，不会向任何集群发布防火墙排除列表。

解决办法：强制同步受影响的 NSX Edge。

- 问题 1407920：使用 DELETE API 后，重新发布防火墙规则失败  
如果您通过 DELETE API 方法删除整个防火墙配置，然后尝试从以前保存的防火墙规则草稿重新发布所有规则，则规则发布操作将失败。
- 问题 1534585：在 VMware NSX for vSphere 6.1.x 和 VMware NSX for vSphere 6.2.x 中删除引用的对象后，发布 Distributed Firewall (DFW) 规则会失败  
解决办法：如果发生这种情况，请参见[知识库文章 2126275](#)。

- 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 1442379：服务编排防火墙配置不同步

在 NSX 服务编排中，任何防火墙策略无效时（例如，您删除了防火墙规则中当前使用的安全组），删除或修改其他防火墙策略都会导致服务编排不同步，并显示错误消息：**防火墙配置不同步** (Firewall configuration is not in sync)。

解决办法：删除任何无效的防火墙规则，然后同步防火墙配置。选择服务编排 > 安全策略，然后对具有关联防火墙规则的每个安全策略，单击操作并选择同步防火墙配置。为防止出现此问题，请始终修复或删除无效的防火墙配置，然后再进一步更改防火墙配置。

- 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“正在进行中”，在 API 输出中显示为“挂起”

解决办法：无。

- 问题 1620491：服务编排中策略级别的同步状态不显示策略中规则的发布状态

创建或修改策略后，服务编排将显示成功状态，该状态仅表示持久性状态，而不反映是否已将规则成功发布到主机。

解决办法：使用防火墙 UI 查看发布状态。

- 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。

- **问题 1772504：**服务编排不支持具有 MAC 集的安全组  
服务编排允许在策略配置中使用安全组。如果具有的安全组包含 MAC 集，服务编排将直接接受该安全组，但无法为该特定 MAC 集强制实施规则。这是因为服务编排在第 3 层上工作，而不支持第 2 层结构。请注意，如果安全组同时具有 IP 集和 MAC 集，则 IP 集将仍然有效，但会忽略 MAC 集。引用包含 MAC 集的安全组没有什么坏处，但用户必须知道 MAC 集会被忽略。

**解决办法：**如果用户打算使用 MAC 集创建防火墙规则，用户应使用 DFW 第 2 层/以太网配置，而不是服务编排。

- **问题 1718726：**用户使用 DFW REST API 手动删除服务编排的策略部分后，无法强制同步服务编排在跨 vCenter NSX 环境中，如果只有一个策略部分，而该策略部分（服务编排管理的策略部分）之前已通过调用 REST API 删除，则用户尝试强制同步 NSX 服务编排配置将会失败。

**解决办法：**请勿通过调用 REST API 来删除服务编排管理的策略部分。（请注意，UI 已经阻止删除这部分。）

## 监控服务已知问题

- **问题 1655593：**以审核员或安全管理员角色登录时，NSX 仪表板上的状态缺失  
以审核员或安全管理员身份查看 NSX 仪表板时，显示错误消息“未授权用户访问对象...和功能...，请查看用户的对象访问范围和功能权限”（User is not authorized to access object ... and feature ... Please check object access scope and feature permissions for the user）。例如，审核员可能无法从仪表板查看“逻辑交换机状态”。

**解决办法：**无。

- **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。

## 解决方案互操作性已知问题

- **问题 1840744：**虚拟机陷入重新引导循环后，VMware ESXi 6.0.0 主机显示紫色诊断屏幕  
出现该问题是因为陷入重新引导循环的虚拟机生成的 dvfilter 创建/销毁事件中存在争用情况。有关详细信息，请参见 [VMware 知识库文章 2149782](#)。

**解决办法：**在 VMware ESXi 6.0 Patch 03 和更高版本中已解决该问题，可以从 VMware 网站中下载这些版本。

如果不希望通过升级来解决该问题，请关闭受影响的虚拟机电源。

- **问题 1568861：**从没有 VC 侦听器的 vCD 单元部署任何 Edge 期间，NSX Edge 部署会失败

从没有 VC 侦听器的 vCD 单元部署任何 Edge 期间，NSX Edge 部署会失败。此外，从 vCD 中执行的 NSX Edge 操作（包括重新部署）也会失败。

*解决办法：*从具有 VC 侦听器的 vCD 单元中部署 NSX Edge。

- 问题 1530360：NSX Manager 虚拟机进行故障切换后，Site Recovery Manager (SRM) 错误地报告超时错误

NSX Manager 虚拟机进行故障转移后，SRM 错误地报告超时错误，等待 VMware Tools。在这种情况下，VMware Tools 实际已在 300 秒超时内启动并运行。

*解决办法：*无。

## NSX Controller 已知问题

- 问题 1845087：如果磁盘延迟较高，NSX Controller API 将会受到不利影响  
如果 NSX Controller 使用的存储的 I/O 延迟太高，NSX Controller API 可能不会在 NSX Manager 的时间限制内响应。这可能会进而影响 NSX Controller 的升级和其他功能。如果严重性超过特定限制，vSphere Web Client 的网络和安全插件将显示“较高的控制器磁盘延迟” (High controller disk latency) 错误。

*解决办法：*要解决该问题，VMware 建议使用专用的本地硬盘驱动器和 SSD。

- 问题 1765354：<deployType> 是必需属性，但并未使用该属性  
<deployType> 是必需属性，但并未使用该属性，而且该属性没有任何意义。
- 问题 1760102：在删除 NSX Controller 并重新部署以从存储故障中恢复后，虚拟机可能无法通信  
出现存储故障时，适用于 vSphere 的 NSX Controller 6.2.x 环境可能会进入只读模式。如果先删除再重新部署控制器以从该状态中恢复，则某些虚拟机可能无法通信。控制器上出现存储故障时，预期行为是重新引导控制器应会将其从只读模式中恢复，但当前在 NSX 中并未实现此预期行为。

*解决办法：*重新启动 NSX 管理服务。

- 问题 1516207：在 NSX Controller 集群中重新启用 IPsec 通信后，控制器可能会被隔离  
如果 NSX Controller 集群设置为允许控制器之间以明文形式进行通信（禁用 IPsec），并在稍后重新启用基于 IPsec 的通信，则一个或多个控制器可能会由于预共享密钥 (PSK) 不匹配而导致与集群主体隔离。出现此情况时，NSX API 可能无法更改控制器的 IPsec 设置。

*解决办法：*

按照以下步骤进行操作以解决此问题：

1. 使用 NSX API 禁用 IPsec。

```
PUT /2.0/vdn/controller/node

<controllerNodeConfig>
  <ipSecEnabled>false</ipSecEnabled>
</controllerNodeConfig>
```

2. 使用 NSX API 重新启用 IPsec。

```
PUT /2.0/vdn/controller/node

<controllerNodeConfig>
  <ipSecEnabled>true</ipSecEnabled>
</controllerNodeConfig>
```

按照以下最佳做法进行操作可避免此问题：

- 始终使用 NSX API 来禁用 IPSec。不支持使用 NSX Controller CLI 来禁用 IPSec。
  - 在使用此 API 来更改 IPSec 设置之前，始终确认所有控制器都处于活动状态。
- **问题 1306408：必须按顺序下载 NSX Controller 日志**

不能同时下载多个 NSX Controller 日志。即使从多个控制器下载，您也必须等待从当前控制器下载完成后，再开始从下一个控制器下载。另请注意，开始日志下载后便无法取消。

*解决办法：*等待当前控制器日志下载完成，然后再开始其他日志下载。