

VMware NSX for vSphere 6.2.5 发行说明

文档更新日期：2017 年 8 月 21 日

VMware NSX for vSphere 6.2.5 | 2017 年 1 月 5 日发行 | 内部版本 4818372

发行说明内容

本发行说明包含以下主题：

- [新增功能](#)
- [推荐的最低版本、系统要求和安装说明](#)
- [已弃用和已停用的功能](#)
- [升级说明](#)
- [已知问题](#)
- [已解决的问题](#)
- [文档修订历史](#)

新增功能

请参见 NSX [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。

请参见[关于 NSX 6.2.3 的重要信息](#)。

6.2.5 中的新增功能

6.2.5 版是一个错误修复版本，该版本解决了在以下安装场景中执行某些 vMotion 操作后网络连接中断问题：一些主机运行较新版本的 NSX，其他主机运行较旧版本的 NSX。请参阅[已解决的问题](#)部分。

6.2.4 中的新增功能

6.2.4 版包含以下新增功能。此版本还修复了一系列错误，这些修复的错误列在[已解决的问题](#)部分。

- 更改了防火墙状态 API (`GET /api/4.0/firewall/globalroot-0/status`)
 - 防火墙状态 API 已得到增强，可包含防火墙规则中使用的对象更新状态：防火墙状态 API 为每个规则集显示一个生成编号 (generationNumber)，该编号可用于验证规则集中的更改是否已传播到主机。在 6.2.4 中，对象的生成编号 (generationNumberObjects) 已添加到状态 API 中。这样，您就可以验证防火墙规则中使用的对象的更改是否已传播到主机。请注意，对象生成编号可能会经常更改，并将始终大于或等于规则集生成编号。
 - 从输出中排除了未加入防火墙的集群和主机：如果在集群级别禁用 Distributed Firewall 或未准备集群（未安装 NSX VIB），则不再将集群（和集群中的主机）包含在状态输出中。在较低版本的 NSX 中，这些集群和主机包含在输出中。不过，由于没有为防火墙配置这些集群和主机，在防火墙规则发布后，其状态为“正在进行”。
- 修复了在 NSX 6.2.3 中发现的严重错误：NSX 6.2.4 为 CVE-2016-2079 提供了一个安全修补程序，这是使用

NSX SSL VPN 的站点存在的一个严重输入验证漏洞。对于使用 SSL VPN 的客户，VMware 强烈建议检查 CVE-2016-2079 并升级到 NSX 6.2.4 或更高版本。

6.2.3 中的新增功能

有关 NSX for vSphere 6.2.3 的重要信息：对于已安装 NSX 6.2.3 或 6.2.3a 的客户，VMware 建议安装 NSX 6.2.4 或更高版本以修复严重错误。

6.2.3 版本提供了安全修补程序，可解决 CVE-2016-2079 漏洞问题。CVE-2016-2079 是一个严重的输入验证漏洞，此漏洞会影响使用 NSX SSL-VPN 的站点。此版本还修复了一系列错误，这些修复的错误列在[已解决的问题](#)部分中。

NSX for vSphere 6.2.3 中引入了以下更改：

- 逻辑交换和路由
 - NSX 硬件第 2 层网关集成：通过将第三方硬件网关交换机集成到 NSX 逻辑网络中，扩展了物理连接选项
 - 在 NSX 6.2.3 及更高版本中引入了新 VXLAN 端口 4789：在 6.2.3 之前的版本中，默认 VXLAN UDP 端口号是 8472。请参见《NSX 升级指南》以了解详细信息。
- 网络连接和 Edge 服务
 - 新的 Edge DHCP 选项：DHCP 选项 121 支持静态路由选项，DHCP 服务器可通过此选项将静态路由发布到 DHCP 客户端；DHCP 选项 66、67 和 150 支持用于 PXE 引导的 DHCP 选项；以及 DHCP 选项 26 支持通过 DHCP 服务器配置 DHCP 客户端网络接口 MTU。
 - 增加了 DHCP 池中的静态绑定限制：以下是不同规格大小的新限制数量：精简：2048；中型：4096；大型：4096；及超大型：8192。
 - Edge 防火墙添加了 SYN Flood 攻击防护功能：通过为传输流量启用 SYN Flood 攻击防护，可避免服务中断。默认情况下，此功能处于禁用状态，可使用 NSX REST API 将其启用。
 - NSX Edge — 按需故障切换：使用户能够在需要时启动按需故障切换。
 - NSX Edge — 大型 (Quad Large) NSX Edge 的默认内存：已从 1 GB 增加到 2 GB。
 - NSX Edge — 资源预留：在创建期间为 NSX Edge 预留 CPU/内存。预留的 CPU/内存基于 Edge 设备规格大小。您可以使用以下 API 更改默认的 CPU 和内存资源预留百分比。将 CPU/内存百分比均设置为 0% 可禁用资源预留。

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

```
<tuningConfiguration>
  <lockUpdatesOnEdge>false</lockUpdatesOnEdge>
  <aggregatePublishing>true</aggregatePublishing>
  <edgeVMHealthCheckIntervalInMin>0</edgeVMHealthCheckIntervalInMin>
  <healthCheckCommandTimeoutInMs>120000</healthCheckCommandTimeoutInMs>
  <maxParallelVixCallsForHealthCheck>25</maxParallelVixCallsForHealthCheck>
  <publishingTimeoutInMs>1200000</publishingTimeoutInMs>
  <edgeVCpuReservationPercentage>0</edgeVCpuReservationPercentage>
  <edgeMemoryReservationPercentage>0</edgeMemoryReservationPercentage>
```

centage>

```
<megaHertzPerVCpu>1000</megaHertzPerVCpu>
</tuningConfiguration>
```

- **NSX Edge 升级行为更改：**在升级或重新部署之前将部署 NSX Edge 替换虚拟机。在升级或重新部署 Edge HA 对期间，主机必须拥有足够的资源来安装四个 NSX Edge 虚拟机。TCP 连接超时的默认值已经从之前的 3600 秒更改为 21600 秒。
- **跨 VC NSX — 通用分布式逻辑路由器 (DLR) 升级：**在主 NSX Manager 上升级之后，会自动升级辅助 NSX Manager 上的通用 DLR。
- **灵活地创建 SNAT/DNAT 规则：**不再需要 *vnictd* 作为输入参数；不再要求 DNAT 地址必须为 NSX Edge vNIC 的地址。
- **NSX Edge 虚拟机 (ESG、DLR) 现在同时显示实时位置和所需位置。**NSX Manager 和 NSX API (包括 GET api/4.0/edges//appliances) 现在除了返回当前位置之外，还返回 configuredResourcePool 和 configuredDataStore。
- **Edge 防火墙添加了 SYN Flood 攻击防护功能：**通过为传输流量启用 SYN Flood 攻击防护，可避免服务中断。默认情况下，此功能处于禁用状态，可使用 NSX REST API 将其启用。
- **NSX Manager 公开 ESXi 主机名，**在该主机上将运行第三方虚拟机系列防火墙 SVM，以改进大规模环境中的操作可管理性。
- **NAT 规则**不仅可应用于 IP 地址，现在还可以应用于 vNIC 接口。
- **新增了配置选项以设置负载均衡器会话到期时间：**此版本提供了一个新的应用程序规则命令，用于为服务器和客户端设置会话到期超时值。如果在多个虚拟服务器之间共享池，将为其设置最大值。
- **未提供 Accept 标头时，NSX API 现在默认返回 XML 输出：**从 NSX 6.2.3 开始，如果 REST API 调用中未提供 “Accept:” 标头，则 NSX API 返回值的默认格式为 XML。以前，NSX API 默认返回 JSON 格式的输出。要接收 JSON 格式的输出，API 用户在调用此功能时必须在 “Accept:” 标头中明确设置 “application/json”。
- **新增了 NSX API 以更改 NSX 分布式防火墙的自动草稿设置：**从 NSX 6.2.3 开始，可以使用以下 PUT API 更改 NSX Distributed Firewall 的自动草稿设置：

- 获取现有 GlobalConfiguration:

```
GET https://NSX-Manager-IP-
Address/api/4.0/firewall/config/globalconfiguration
```

注意：GET 将不会显示 autoDraftDisabled 字段。

- 将 autoDraftDisabled 配置属性添加到全局配置中并执行 PUT API 调用:

```
PUT https://NSX-Manager-IP-
Address/api/4.0/firewall/config/globalconfiguration
```

请求正文:

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

- 分布式防火墙 — TFTP ALG：支持各种用例，如通过网络引导虚拟机。
- 防火墙 — 细粒度规则筛选：通过根据源、目标、操作、已启用/已禁用、日志记录、名称、备注、规则 ID、标记、服务、协议，在 UI 中提供细粒度规则筛选器，简化了故障排除过程。
- 客户机侦测 — 支持 Windows 10
- SSL VPN 客户端 — 支持 Mac OS El Capitan
- 服务编排 — 性能改进：通过优化安全策略和防火墙服务之间的同步，以及默认禁用自动保存防火墙草稿的功能，提升了启动/重新引导 NSX Manager 的速度。
- 服务编排 — 状态警报：如果安全策略不同步，则会引发系统警报，并会根据警报代码采取具体操作来解决问题。
- 降低了防火墙堆内存使用率：对 IP 地址集的防火墙使用情况进行了优化，可降低堆内存使用率。

● 操作和故障排除

- NSX 仪表板：系统将 NSX 组件的总体运行状况显示在一个中央视图中，简化了故障排除过程。
- 跟踪流增强 — 网络侦测服务：通过确定数据包是否被转发到第三方网络侦测服务，以及该数据包是否从第三方服务虚拟机返回，增强了从源到目标跟踪数据包的功能。
- 支持 SNMP：为来自 NSX Manager、NSX Controller 和 Edge 的事件配置 SNMP 陷阱。
- 现在默认启用 SSL VPN 和 L2 VPN 的日志记录功能。默认日志级别为通知。
- 现在默认启用 IPsec VPN 的日志记录功能。默认日志级别设置为“警告”。如果您希望禁用日志记录或更改日志级别，请参阅《NSX 管理指南》中的“[为 IPsec VPN 启用日志记录](#)”一节。
- 防火墙规则 UI 现在显示已配置的 IP 协议和与服务相关联的 TCP/UDP 端口号。
- NSX Edge 技术支持日志已得到增强，可报告每个进程的内存消耗情况。
- 增强了通信通道运行状况监控，当服务器或集群的通道运行状况发生变化时，将报告新的事件日志消息。
- 中央 CLI 增强功能
 - 用于检查主机运行状况的中央 CLI：显示主机运行状况，一个命令可执行 30 多项检查（包括网络配置、VXLAN 配置和资源利用率等）。
 - 用于数据包捕获的中央 CLI：可捕获主机上的数据包，并将捕获文件传输到用户的远程服务器。这消除了在对逻辑网络问题进行故障排除时为网络管理员打开 Hypervisor 访问权限的需求。
- 基于每个主机的技术支持包：收集每个主机的日志，并创建一个可保存并提交给 VMware 技术支持以获取帮助的包。

● 许可增强

- 默认许可证和评估密钥分发方面的更改：默认安装的许可证是“NSX for vShield Endpoint”，此许可证只允许使用 NSX 来部署和管理 vShield Endpoint 的防病毒卸载功能。可以通过 VMware 销售人员申请评估许可证密钥。
- 许可证使用情况报告：NSX 许可证使用情况计数显示在 NSX Manager 的“摘要”UI 上，还可以通过 API 进行检索。将不再通过 vCenter 许可服务报告 NSX 许可证使用情况计数。

● 负载均衡器 (LB) 增强功能

- 可对未配置加速的 VIP 配置会话超时：可以使用应用程序规则“超时客户端 3600 秒”，将负载均衡 L7 引擎（无加速）VIP 超时配置为 5 分钟以上。
- CLI 上的统计信息增强功能：现在可通过 CLI 获取全局统计信息。此外，还可以获取特定的 VIP 和池统计信息。
- 带加速的 LB 增强功能：负载均衡 L4 引擎（启用加速）现在将始终采用运行状况检查 UDP、TCP 源 IP 哈希，并会使持久性条目无效。
- 日志调整：改进了负载均衡器日志。
- 可配置 SSL 身份验证：对于使用端到端 SSL 的 VIP，可以配置 SSL 服务器身份验证。
- 源 IP 持久性表增强功能：即使在配置发生更改后，源 IP 持久性表仍保持可用。
- 已将 NSX Edge 负载均衡器系统控制 (sysctl) `sysctl.net.ipv4.vs.expire_nodest_conn` 参数添加到 NSX Manager 白名单：`sysctl.net.ipv4.vs.expire_nodest_conn` 可用来更改持久性连接状态。
- 解决方案互操作性
 - 客户体验提升计划：NSX 通过 VMware 客户体验提升计划 (CEIP) 来支持报告系统统计信息。您可以选择是否参与此计划，具体配置在 vSphere Web Client 中进行。
 - VMware vRealize Log Insight 3.3.2 for NSX 通过监控和故障排除功能，以及用于网络虚拟化、流量分析和警示的可自定义的仪表板，为 NSX 提供智能日志分析。此版本接受为 NSX 6.2.2 以上版本颁发的 NSX 标准版/高级版/企业版许可证密钥。
 - vShield Endpoint 管理支持：NSX 支持管理 vShield Endpoint 防病毒卸载功能。如果客户购买的是带有 vShield Endpoint 的 vSphere（Essentials Plus 及更高版本），他们可以从 vSphere 下载站点下载 NSX。有关详细信息，请参阅 [VMware 知识库文章 2110078](#) 和 [VMware 知识库文章 2105558](#)。

6.2.2 中的新增功能

6.2.2 版本提供了用于解决 glibc 漏洞的安全修补程序，同时修复了一系列错误，这些修复的错误列在[已解决的问题](#)部分。此版本包含基于 6.1.4 和 6.1.5 的所有修补程序所提供的关键错误修复。对于 NSX 6.1.x 用户，NSX 6.1.6 版本中包含一组同样的修补程序修复。

此版本的主要功能包括：

- CVE-2015-7547 (glibc) 安全修补程序：该修补程序解决了 [CVE-2015-7547](#) 问题，也称为 glibc 漏洞。
- 问题 1600484：移除了对 DHCP 域名配置的限制验证 NSX 6.2.2 再次支持拥有“.local”域的 DHCP 池。请参见 [VMware 知识库文章 2144097](#)。
- 问题 1586149：增强了 DFW UI，可提供更加优质的用户体验。在以前的实施中，当用户进行更改时，表格常常滚动到网格的第一项。在修复后的实施中，只要添加规则，网格就会滚动到新添加的规则。现在，当出于任何原因刷新网格数据时（例如，在发布或恢复更改后），网格的垂直滚动位置将保持不变。
- 问题 1592562：配置新的 Edge 服务后发生行为变化。在 6.2.2 之前，配置了新的 Edge 服务后，默认将启用该服务。在 6.2.2 中，此行为发生了变化。现在，如果当前许可证支持此功能，则默认将启用此功能。否则，将禁用此功能。

6.2.1 中的新增功能

6.2.1 版本修复了许多错误，这些修复的错误列在[已解决的问题](#)部分。

- 6.1.5 修复：该版本包含与 NSX for vSphere 6.1.5 内容相同的关键修复。

- 引入了新的“show control-cluster network ipsec status”命令，用户可以使用该命令检查 Internet 协议安全 (IPSec) 状态。
- 连接状态：现在，NSX Manager 用户界面显示 NSX Controller 集群的连接状态。
- 支持适用于 NSX 的 vRealize Orchestrator 插件 1.0.3：随 NSX 6.2.1 版本引入了 NSX-vRO 插件版本 1.0.3，用于 vRealize Automation 7.0.0。该插件包含重要修复，可在 vRealize Automation 7.0 将 NSX for vSphere 6.2.1 用作网络和安全端点时提升性能。
- 从 6.2.1 版开始，NSX Manager 将查询集群中的每个控制器节点，以获取该控制器与集群中的其他控制器之间的连接信息。
此信息在 NSX REST API（“GET https://[NSX-MANAGER-IP-ADDRESS]/api/2.0/vdn/controller”命令）的输出中提供，现在会显示各控制器节点之间的对等连接状态。如果 NSX Manager 发现任何两个控制器节点之间的连接断开，则会生成系统事件以警示用户。
- 服务编排现公开一个 API，用户可以使用该 API 配置为服务编排工作流自动创建防火墙草稿。
可以使用 REST API 启用/禁用该设置，并在重新引导时保存所做的更改。如果禁用，则不会在策略工作流的 Distributed Firewall (DFW) 中创建草稿。这会限制在系统中自动创建的草稿数并提供更好的性能。

6.2.0 中的新增功能

NSX for vSphere 6.2.0 包含以下新增及改进的功能：

- 跨 vCenter 的网络和安全
 - NSX for vSphere 6.2 支持跨 vCenter 的 NSX 环境：可跨多个 vCenter 部署逻辑交换机 (LS)、分布式逻辑路由器 (DLR) 和 Distributed Firewall (DFW)，为工作负载（虚拟机）分布于多个 vCenter 或多个物理位置的应用程序提供逻辑网络连接和安全服务。
 - 多个 vCenter 使用一致的防火墙策略：现可将 NSX 中的防火墙规则区域标记为“通用”，在多个 NSX Manager 之间复制这些区域中定义的规则。这可简化跨多个 NSX 安装定义一致的防火墙策略的工作流
 - 通过 DFW 实现跨 vCenter vMotion：在“通用”区域中定义策略的虚拟机可以跨不同 vCenter 的主机进行迁移，并实施一致的安全策略。
 - 通用安全组：现在，可以在通用规则中使用基于 IP 地址、IP 集、MAC 地址和 MAC 集的 NSX 6.2 安全组，以便在多个 NSX Manager 之间同步组和组成员资格。这可提高多个 NSX Manager 之间对象组定义的一致性，并实施一致的策略。
 - 通用逻辑交换机 (ULS)：在 NSX 6.2 中，作为跨 vCenter 的 NSX 的一部分引入这一新功能，允许跨多个 vCenter 创建逻辑交换机，从而使网络管理员能够为应用程序或租户创建连续的 L2 域。
 - 通用分布式逻辑路由器 (UDLR)：在 NSX 6.2 中，作为跨 vCenter 的 NSX 的一部分引入这一新功能，允许用户跨多个 vCenter 创建分布式逻辑路由器。通用分布式逻辑路由器可在上文介绍的通用逻辑交换机之间提供路由服务。此外，NSX UDLR 能够基于工作负载的物理位置提供局部 N-S 路由。
- 操作和故障排除增强功能
 - 新的跟踪流故障排除工具：跟踪流是一个故障排除工具，可帮助确定是虚拟网络存在问题还是物理网络存在问题。它可以从源到目标跟踪数据包，有助于观察该数据包如何在虚拟网络中的各网络功能之间传递。
 - 流量监控与 IPFIX 分离：在 NSX 6.1.x 中，NSX 支持 IPFIX 报告，但只在启用 NSX Manager 的流报告时才会启用 IPFIX 报告。自 NSX 6.2.0 起，这些功能已分离。在 NSX 6.2.0 和更高版本中，您可以在 NSX Manager 上单独启用 IPFIX 和流量监控。
 - 6.2 中新增的 CLI 监控命令和故障排除命令：有关详细信息，请参见[知识库文章 2129062](#)。

- **中央 CLI:** 中央 CLI 缩短了分布式网络功能的故障排除时间。可从 NSX Manager 命令行运行命令，并从控制器、主机和 NSX Manager 检索信息。这使您能快速访问和比较来自多个源的信息。中央 CLI 提供了有关逻辑交换机、逻辑路由器、分布式防火墙和 Edge 的信息。
- **CLI ping 命令**增加了可配置的数据包大小和“不分段”标记：自 NSX 6.2.0 起，NSX CLI “ping”命令提供了指定数据包大小（不包括 ICMP 标头）和设置“不分段”标记的选项。有关详细信息，请参见 [NSX CLI 参考](#)。
- **显示通信通道的运行状况：**NSX 6.2.0 增加了监控通信通道运行状况的功能。通过 NSX Manager UI 可查看 NSX Manager 和防火墙代理之间、NSX Manager 和控制平面代理之间以及主机和 NSX Controller 之间的通道运行状况。此外，主机命令通道提供了更高的容错性。
- **独立 Edge L2 VPN 客户端 CLI：**在 NSX 6.2 之前，只能通过为虚拟中心提供的“部署 OVF”设置来配置单独的 NSX Edge L2 VPN 客户端。增加了特定于独立 NSX Edge 的命令后，可以通过命令行界面进行配置。

● 逻辑网络连接和路由

- **L2 桥接与分布式逻辑路由器的互操作性：**通过 VMware NSX for vSphere 6.2，L2 桥接现在可以加入分布式逻辑路由。网桥实例连接到的 VXLAN 网络用于将路由实例和网桥实例连接到一起。
- **根据 RFC 3021 支持在 ESG 和 DLR 接口上使用 /31 前缀。**
- **增强了 ESG DHCP 服务器对中继 DHCP 请求的支持。**
- **可以在 NSX 虚拟网络中保留 VLAN ID/标头。**
- **重新分发筛选器的精确匹配：**重新分发筛选器具有与 ACL 相同的匹配算法，因此默认执行精确的前缀匹配（除非使用了 le 或 ge 选项）。
- **支持静态路由管理距离。**
- **能够在 Edge 上启用、放宽或禁用逐个接口检查。**
- **在 CLI 命令 `show ip bgp` 中显示 AS 路径**
- **在 DLR 控制虚拟机上重新分发到路由协议时排除 HA 接口。**
- **分布式逻辑路由器 (DLR) 强制同步可避免 DLR 之间的东西向路由流量出现数据丢失。**南北向路由和桥接可能继续中断。
- **查看 HA 对中的活动 Edge：**在 NSX 6.2 Web Client 中，您可以查明 HA 对中的 NSX Edge 设备处于活动状态还是备用状态。
- **REST API 在 Edge 上支持反向路径筛选器 (rp_filter)：**使用系统控制 REST API，可以通过 UI 配置 rp_filter sysctl，还可以通过 REST API 为虚拟网卡接口及子接口公开 rp_filter sysctl。有关详细信息，请参见 [NSX API 文档](#)。
- **IP 前缀 **GE** 和 IP 前缀 **LE** BGP 路由筛选器的行为：**在 NSX 6.2 中，BGP 路由筛选器具有以下增强功能：
 - **不允许使用 LE/GE 关键字：**对于空路由网络地址（定义为 ANY 或 CIDR 格式 0.0.0.0/0），不再允许使用小于或等于 (LE) 和大于或等于 (GE) 关键字。在先前的版本中，允许使用这些关键字。
 - **现在范围 0 到 7 中的 LE 和 GE 值视为有效。**在先前的版本中，此范围无效。
 - **对于给定的路由前缀，指定的 GE 值不能大于指定的 LE 值。**

● 网络连接和 Edge 服务

- DLR 的管理接口已重命名为 HA 接口。这样做旨在强调，此接口提供 HA 传送，此接口上的流量中断会导致出现不一致 (split-brain) 的情况。
 - 改进了负载均衡器运行状况监控：提供细粒度运行状况监控，可报告有关故障的信息，跟踪上次运行状况检查和状态更改，以及报告故障原因。
 - 支持 VIP 和池端口范围：可为需要使用端口范围的应用程序提供负载均衡器支持。
 - 增加了最大虚拟 IP 地址 (VIP) 数量：支持的 VIP 数量增加到 1024。
- 安全服务增强功能
 - 虚拟机的新 IP 地址发现机制：根据虚拟机名称或其他基于 vCenter 的属性授权实施安全策略时，要求 NSX 知晓虚拟机的 IP 地址。在 NSX 6.1 及更早版本中，每个虚拟机的 IP 地址发现要求虚拟机上存在 VMware Tools (VMTools) 或需要对虚拟机 IP 地址进行手动授权。NSX 6.2 引入了一个选项，可通过从 Hypervisor 中执行发现来发现虚拟机的 IP 地址。通过这些新的发现机制，NSX 能够对未安装 VMware Tools 的虚拟机强制实施基于对象的 Distributed Firewall 规则。
 - 解决方案互操作性
 - 支持 vSphere 6.0 Platform Services Controller 拓扑：除了已支持的嵌入式 PSC 配置，NSX 现在还支持外部 Platform Services Controller (PSC)。
 - 支持适用于 NSX 的 vRealize Orchestrator 插件：NSX 6.2 支持用于集成 NSX 和 vRealize Orchestrator 的 [NSX-vRO 插件](#)。

推荐的最低版本、系统要求和安装说明

下表列出了推荐的最低 VMware 软件版本以及所需的 VMware 软件版本。此信息为截至本文档发布之日的最新信息。有关最新推荐，请参见 [VMware 知识库文章 2144295](#)

产品或组件	推荐的最低版本
NSX for vSphere	<p>6.2.2</p> <p>对于使用 SSL VPN 的客户，VMware 建议使用推荐的最低版本的 NSX for vSphere 6.2.4，并查阅 CVE-2016-2079。</p> <p>对于打算使用逻辑交换功能和 vSphere 6.0U2 的客户，VMware 建议使用推荐的最低版本的 NSX for vSphere 6.2.4，并查阅重新引导 vCenter Server 后 ESXi 主机中存在重复的 VTEP (KB 2144605)。</p>
vSphere	<p>5.5U3 或 6.0U2</p> <p>注意：vSphere 6.0 和 NSX 对象存在一个已知问题。有关详细信息，请参见 VMware 知识库文章 2144605 “重新引导 vCenter Server 后 ESXi 主机中存在重复的 VTEP”。</p>

客户机侦测

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：

- VMware Tools 10.0.8 及更高版本，可解决在 NSX / vCloud Networking and Security 中升级 VMware Tools 后虚拟机速度缓慢的问题（VMware 知识库文章 [2144236](#)）
- 支持 Windows 10 的 VMware Tools 10.0.9 及更高版本

vRealize Orchestrator

NSX-vRO 插件版本 1.0.3 或更高版本

注意：NSX 6.2.x 与 vSphere 6.5 不兼容。有关互操作性的详细信息，请参见 [VMware 产品互操作性列表](#)。

安装

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

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 将于 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 将于 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。

- **新增：**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

- **新增：**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）。
- 要升级到 NSX 6.2.4，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。
- 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](#)。
- 不支持从 NSX 6.1.6 升级到 NSX 6.2.0、6.2.1 或 6.2.2。
- 不支持从 NSX 6.1.5 升级到 NSX 6.2.0。VMware 建议从 6.1.5 升级到 6.2.4 或更高版本，以获取最新安全更新。
- 要验证是否成功升级到 NSX 6.2.x，请参见[知识库文章 2134525](#)。
- 与其他 VMware 产品一同升级：如果要在升级其他 VMware 产品（如 vCenter 和 ESXi）时一同升级 NSX，请务必按照[知识库文章 2109760](#) 中记录的所支持升级顺序进行操作。
- 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“正在进行中”。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。

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 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。

问题 1710624：如果未在 REST API 请求正文中指定 serverType，则将添加的 Windows 2008 事件日志服务器的“TYPE”设置为“WIN2K3”类型

如果您创建事件日志服务器 API 请求，则将添加的服务器的“TYPE”设置为“WIN2K3”。如果您只对 IDFW 使用事件日志服务器，IDFW 可能无法正常工作。

解决办法：将 serverType 添加到 REST API 请求正文。例如：

```
<EventlogServer>
  <domainId>1</domainId>
  <hostName>AD_server_IP</hostName>
  <enabled>true</enabled>
  <serverType>WIN2k8</serverType>
</EventlogServer>
```

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/usvmgmt/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

升级之前，请阅读本文档前文的[升级说明](#)一节。

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 1730017：从 6.2.3 到 6.2.4 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 6.2.4 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 6.2.4

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 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 1332563：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 1473537：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移除服务，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移除服务，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 1266433：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 1498376：配置分布式防火墙时，显示主机错误消息

在配置分布式防火墙时，如果您遇到与主机相关的错误消息，请检查结构层功能的状态“com.vmware.vshield.nsxmgr.messagingInfra”。如果状态为红色，请使用以下解决办法。

解决办法：使用以下 REST API 调用重置 NSX Manager 与集群中单个主机或所有主机间的通信。

POST https://<NSX Manager IP>/api/2.0/nwfabric/configure?action=synchronize

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>{HOST/CLUSTER MOID}</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

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 1479314：NSX 6.2 中已弃用 SSLv2 和 SSLv3

从 NSX 6.2 开始，SSL VPN 网关只接受 TLS 协议。NSX 升级后，您创建的任何新 NSX 6.2 客户端在建立连接时将自动使用 TLS 协议。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：在升级到 NSX 6.2 后，卸载旧的 SSL VPN 客户端并安装 NSX 6.2 版本的 SSL VPN 客户端。

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 1493777：升级至 NSX 6.2 后，NSX Manager 分配的物理内存超过了 100%

从 NSX 6.2 开始，NSX Manager 需要 16 GB 的预留内存。之前要求为 12 GB。

解决办法：将 NSX Manager 虚拟设备的预留内存增加至 16 GB。

问题 1716619：由于缺少“systemControl”功能，无法在 NSX 6.x.x Manager 上修改 NSX 5.x.x Edge 的 vNIC

由于在 vCNS (vCloud Networking and Security) Manager 上没有为 Edge 创建“systemControl”条目，无法在 NSX 6.x.x 上配置 NSX 5.x.x 的 vNIC。systemControl 功能是在 6.1.5 中引入的，不可用于 vCNS 或 vShield 5.5.x Manager。在使用 NSX 6.1.5 及更高版本或 NSX 6.2.x Manager 编辑较旧 Edge 设备（vCNS 或 vShield 5.5.x）的接口配置时，会出现此问题。

解决办法：请联系 VMware 技术支持人员。

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，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。

新增：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
需要重新引导主机，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 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-vmware-client/plugin-packages/esxtop-plugin`
`rm -R /usr/lib/vmware-vmware-vmware-client/plugin-packages/esxtop-plugin`
3. 删除 `/usr/lib/vmware-vmware-vmware-client/server/work`
`rm -R /usr/lib/vmware-vmware-vmware-client/server/work`
4. 重新启动 Web Client
`service vmware-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 1534877: 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 1537258: 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 1534622: NSX Controller 显示为已断开连接

NSX Manager 日志通过类似以下内容的消息, 报告与控制器的连接断开: “错误 http-nio-127.0.0.1-7441-exec-16908 BaseRestController:339 - 异常: 'I/O 错误: 读取已超时; 嵌套异常为 java.net.SocketTimeoutException: 读取已超时' (ERROR http-nio-127.0.0.1-7441-exec-16908 BaseRestController:339 - Exception: 'I/O error: Read timed out; nested exception is java.net.SocketTimeoutException: Read timed out')。达到闲置超时值后, 网络上的中间防火墙阻止 TCP/IP FIN 消息时, 会发生这种情况。发生这种情况时, 到 NSX Manager 的连接数将会增加。

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 1415480：还原 NSX Manager 备份后，REST 调用显示结构层功能

com.vmware.vshield.nsxmgr.messagingInfra 的状态为“红色”

还原 NSX Manager 备份后，使用 REST API 调用检查结构层功能

com.vmware.vshield.nsxmgr.messagingInfra 的状态时，其状态显示为“红色”而非“绿色”。

解决办法：使用以下 REST API 调用重置 NSX Manager 与集群中单个主机或所有主机间的通信。

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

```
<nwFabricFeatureConfig>
<featureId>com.vmware.vshield.nsxmgr.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>HOST/CLUSTER MOID</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

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 1406471：Syslog 在还原的 NSX Manager 上显示备份 NSX Manager 的主机名

如果使用与第一个 NSX Manager 相同的 IP 地址和一个唯一主机名安装第二个 NSX Manager，还原配置时将在还原后显示第一个 NSX Manager 的主机名，而在重新引导后则显示第二个 NSX Manager 的主机名。

解决办法：第二个 NSX Manager 的主机名应配置为备份 NSX Manager 的主机名。

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 1492880：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 1468613：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

问题 1833934：

在执行存储 vMotion 后，无法管理在 VIX 通信模式下运行的所有 vCNS Edge（5.5.4 版）和 NSX Edge（6.1.x 和 6.2.x）。

在消息总线通信模式下运行的 NSX Edge 不会受到影响。

解决办法：与 VMware 客户支持人员联系。

新增：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 1772004：从节点 0 到节点 1 的 Edge HA 故障切换所用的时间比预期长

在配置了 Edge HA 的环境中，从节点 0 到节点 1 的故障切换所用的时间比预期长，而从节点 1 到节点 0 的流量故障切换则是正常的。

解决办法：无。

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。

新增：问题 1726379：如果 IP 多播范围的上限值在最后三个八位字节中超过 99，VXLAN 中继端口组配置将失败。

在配置分段 ID 时，如果创建的多播 IP 范围的上限值在最后三个八位字节中超过 99（如 1.100.100.100），并且创建具有相同多播 IP 范围的多播或混合逻辑交换机，VXLAN 中继端口组配置将失败。

解决办法：在配置分段 ID 时，请在最后三个八位字节中分别使用小于 100 的多播 IP 范围（如 100.1.1.1）。

新增：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。

新增：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 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 1733146：在某些情况下，在控制虚拟机不存在时，为通用 DLR 创建或修改 LIF 失败

此问题已知会在以下情况下出现：

- ECMP 具有两个静态默认路由
- 静态路由带有本地输出标记

出现此问题是因为请求的是完全同步而不是增量更新，这就导致重复实体被拒绝和操作失败。系统将显示类似以下内容的消息：

```
2016-09-22 20:18:58.080 GMT ERROR TaskFrameworkExecutor-24 NvpRestClientManagerImpl:774 - NVP API returns error: [409] Route with the same prefix and priority already exist on router dc5e541a-d7a6-4cb9-8d8a-9334a9c51127
```

解决办法：

1. 删除通用逻辑路由器。
2. 部署新的通用逻辑路由器。启用本地输出并取消选中“部署 Edge 设备”。使用主要 DLR 上的区域设置 ID（例如，1111xxxx）通过第一个上行链路配置两个上行链路接口和一个默认网关 IP 地址。
3. 请勿通过辅助站点上使用的区域设置 ID（例如，2222xxxx）添加静态路由 0.0.0.0/0。
4. 通过预期的下一跃点 IP 地址和辅助站点的区域设置 ID（例如，222xxxx）添加以下两个静态路由。
路由 1：0.0.0.0/1
路由 2：128.0.0.0/1

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。

新增：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 1556924：L3 连接丢失，发生 VXLAN would block 错误

在主机上配置了 DLR LIF，但底层 VXLAN 没有完全准备好时，通过某些 DLR LIF 建立的连接可能会受影响。无法访问某些属于 DLR 的虚拟机。在 */var/log/vmkernel.log* 文件中可能会显示日志“VXLAN 中继状态创建失败: Would block”。

解决办法：您可以删除 LIF，然后再重新创建。另一种做法是重新引导受影响的 ESX 主机。

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 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 1604514：单击“发布”后，在未受管的 DLR 上编辑/配置默认网关失败

向未受管的 DLR 添加默认网关时，发布操作会失败，并显示错误消息“路由距离仅在已部署 NSX Edge 虚拟机的 NSX Edge 6.2.0 及更高版本上受支持” (Routing Distance is support only on NSX Edge version 6.2.0 and later with NSX Edge VMs deployed)。这是因为在 UI 上填充了默认管理距离“1”。

解决办法：移除默认填充的管理距离“1”。

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 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 1534603：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 1562767：连接到 NSX 负载均衡器时出现的延迟，导致无法在多个 VIP 上提供持续的连接

当负载均衡器配置为使用源 IP 哈希负载均衡时，已连接的客户端会话可与后端服务器建立持续的连接。对于某个已连接的特定客户端，如果相同的服务器池支持多个 VIP 的话，那么该负载均衡器还能在这些 VIP 上提供持续的连接。也就是说，当一个后端服务器服务多个 VIP 时，某个特定客户端与该后端服务器的其中一个 VIP 的连接，应确保该客户端在连接该后端服务器服务的其它 VIP 时将使用该后端服务器。某个已知问题使 NSX 负载均衡器无法在多个 VIP 上提供上述持续的连接。

问题 1553600：为接口分配 IP 地址后，在连接到 RIB 和 FIB 时出现延迟

在尝试为接口分配 IP 地址时，通常会立即更新接口信息。然而，在等待轮询事件时，您可能会在查看所分配的 IP 地址过程中出现延迟。（NSX 逻辑路由器会定期轮询，以获取接口中的更改。）

问题 1534799：关闭具有最高 IP 地址的 OSPF 区域边界路由器后，聚合缓慢

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 (ABR) 后，聚合需要花费较长时间。如果关闭或重新引导 IP 地址数值并非最高的 ABR，则流量会快速聚合到其他路径。但是，如果关闭或重新引导具有最高 IP 地址的 ABR，则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。

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 1089745：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消。

问题 1498965：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 1494025：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 1288487：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 1493611：L2 VPN 中的 VLAN ID 0 没有连接

NSX L2 VPN 配置允许用户错误地使用 VLAN ID 0 配置 L2 VPN。进行以上配置后，该 VPN 无法通过任何流量。

解决办法：解决办法：使用有效的 VLAN ID（范围为 1 到 4094）。

安全服务已知问题

新增：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。

新增：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：不要在全局规则级别使用“+”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 1707931：在服务编排中定义了服务策略时，如果在防火墙 UI 中应用筛选器来修改或发布防火墙规则，分布式防火墙规则的顺序会发生更改

从“网络和安全”>“防火墙”UI 执行一个或多个发布操作后，如果更改在服务编排中创建的服务策略的顺序，或者添加或删除服务策略，则将导致防火墙规则的顺序发生更改，还可能造成意想不到的后果。

解决办法：可用解决办法如下：

- 通过从“安全策略”选项卡的“操作”菜单中选择“同步防火墙规则”，将服务编排规则与防火墙规则进行同步。
- 使用筛选器仅查看规则集，而不更新规则集。
- 在使用筛选器之前通过 REST API `/api/4.0/firewall/globalroot-0/config PUT` 或通过 UI 更新多个区域（而不是单个区域）来执行完整发布，从而确保更改全局防火墙配置。

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、编辑或移除防火墙规则

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 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 1662020：在跨 vCenter 安装中，“常规”和“合作伙伴安全服务”选项卡的 DFW UI 上会出现错误消息“上次在主机 10.156.221.88 上发布失败” (Last publish failed on host 10.156.221.88)

当规则不存在关联的 NIC 时，系统会显示此错误消息。

解决办法：无。

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 PM GMT"
timestamp="1438816120917">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-lfd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="143" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 PM GMT"
timestamp="1438816120713">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-lfd96022-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-lfd96022-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-lfd96022-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 1505316：如果选中的服务是服务组，那么 NSX NetX 规则不会发布到主机

在 DFW 的“合作伙伴服务”选项卡中创建 L3 重定向规则时，选择“服务组”后无法正确创建规则。

解决办法：在创建规则时使用单个服务，而不是服务组。

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 1534574: SSLVPN-Plus 不支持密码 3C (SHA-256) 加密算法

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”, 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。

新增：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。

新增：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。有关详细信息，请参见[知识库文章 2129191](#)。

新增：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。

与解决方案互操作性有关的问题

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：从拥有 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

新增：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。

新增：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 6.2.4/6.2.5 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。

已解决的问题

请参见 [6.2.5](#) 或 [6.2.4 及更低版本](#) 中已解决的问题。

新增：NSX 6.2.5 中解决的问题

6.2.5 中解决的问题分为如下类别：

- [NSX 6.2.5 中解决的常规问题](#)
- [NSX 6.2.5 中解决的逻辑网络连接相关问题](#)
- [NSX 6.2.5 中解决的网络连接和 Edge 服务相关问题](#)
- [NSX 6.2.5 中解决的安全服务相关问题](#)

6.2.5 中解决的常规问题

- 已修复问题 1685375：VXLAN 网关中缺少远程 MAC
在重新加载交换机后，未发送远程 MAC 地址。极少数情况下，当硬件 VTEP 网关重新引导时，NSX Controller 可能不会再次填充 ovsdb MAC 地址表。*6.2.5 中已修复此问题。*

NSX 6.2.5 中解决的安装和升级相关问题

- 已修复问题 1685894：如果将虚拟机从安装了新版 VIB 的主机通过 DRS 迁移到具有旧版 VIB 的主机，虚拟机的网络连接将会中断
由于 NSX 不支持降级，因此不支持这种应用场景。
 - 对于已启用 DRS 的集群，请在升级期间将 DRS 模式更改为“手动”，直到集群中的所有主机都升级到较新的 NSX 版本为止。
 - 对于未启用 DRS 的集群，请不要将在具有新版 VIB 的主机中创建或关闭/打开电源的虚拟机迁移到具有旧版 VIB 的主机。

6.2.5 中已修复此问题。

NSX 6.2.5 中解决的逻辑网络连接相关问题

- 已修复问题 1663902 和 1717370：生产期间，在 ESG/DLR 上执行任何 UPDATE/PUT 操作可能会在短时间内影响流量
如果生产期间在 ESG/DLR 上执行任何 UPDATE/PUT 操作，则会在短时间内看到流量中断。*6.2.5 中已修复此问题。*
- 已修复问题 1737807 和 1703913：在启用了 DLR HA 的 NSX 中，虚拟机会断开网络连接
在使用动态路由并在 DLR 控制虚拟机上配置了高可用性 (HA) 的 NSX 环境中，当 DLR 控制虚拟机从脑裂状况中恢复时，虚拟机会断开网络连接（主要和辅助 DLR HA 节点同时保持“活动”状态）。*6.2.5 中已修复此问题。*

- 已修复问题 1717369：在 HA 模式下进行配置时，可能会在同一主机上部署活动和备用 Edge 虚拟机
出现此问题是因为，在重新部署和升级操作期间，未在 vSphere 主机上自动创建并应用反关联性规则。在现有 Edge 上启用 HA 后，将不会出现此问题。6.2.5 中已修复此问题。
- 已修复问题 1717371：在发生 vSphere HA 事件期间，NSX Edge 虚拟机不进行故障切换
在启用了 vSphere HA 的 vSphere 集群上安装或重新部署 NSX Edge 时，在 NSX Edge 部署期间，NSX Manager 为在其中部署 Edge 的 ESX 主机启用自动启动管理器。这与 vSphere HA 不兼容，因此，vSphere 不会为 Edge 虚拟机提供 HA。6.2.5 中已修复此问题。请参阅[有关自动启动管理器的升级说明](#)。
- 已修复问题 1606785 和 1736095：NSX Edge 负载均衡器可能在 `/var/log/` 分区中填充 nagios.log 文件消息
`/var/log` 分区在 NSX Edge 负载均衡器上填满。6.2.5 中已修复此问题。

NSX 6.2.5 中解决的网络连接和 Edge 服务相关问题

- 已修复问题 1770797：如果在 Edge 服务网关 DHCP 池上配置了无类别静态路由，客户端将忽略默认网关
RFC 3442 指出，如果 DHCP 服务器提供了默认路由和无类别静态路由（选项 121），DHCP 客户端将忽略默认路由。
从 NSX 6.2.5 开始，如果为 Edge 服务网关上的 DHCP 池同时配置了无类别静态路由和默认网关，则将默认网关添加为无类别静态路由。
- 已修复问题 1777121：通过 NSX L2 网桥和 LACP 进行大量 MAC 校准表更新可能会导致内存不足
当 NSX L2 网桥发现其他上行链路上的 MAC 地址时，它会通过 netcpa 进程向控制器报告 MAC 校准表变更。使用 LACP 的网络连接环境将校准多个接口上的相同 MAC 地址，从而导致校准表更新量非常大，并且可能会耗尽 netcpa 进程所需的内存来进行报告。请参阅 [VMware 知识库文章 2147181](#)。6.2.5 中已修复此问题。
- 已修复问题 1771285：在控制器同步操作过程中，不会在主机上为桥接 VXLAN 网络设置多播 IP，从而导致控制平面连接失败
在控制平面标记为“非活动”后，每当以下列任意方式触发控制器同步时，都会导致通信中断：
 - 重新部署、升级或强制同步 DLR
 - VSM 级别控制器状态同步
 - 重新引导控制器，或先断开再重新连接控制器6.2.5 中已修复此问题。
- 已修复问题 1766624：在流量通过 NSX 上的网桥 DLR 时随机丢弃数据包
在流量通过 NSX 上的网桥 DLR 并且 ping 命令显示大量“请求超时 (Request Timed Out)”消息时，会随机丢弃数据包。6.2.5 中已修复此问题。
有关详细信息，请参见 [VMware 知识库文章 2148175](#)。
- 已修复问题 1779313：重新引导 NSX Manager 后出现连接故障
重新引导 NSX Manager 后出现连接故障。发生这种情况是因为，由于部分 VDR 同步不正确，从 ESX 主机中清除了分布式逻辑路由器 (DLR) 实例。出现此错误时，通过强制同步 VXLAN/路由服务可以恢复 NSX 环境。6.2.5 中已修复此问题。
- 已修复问题 1730633：在使用分组对象时，监控状态不正确
在使用分组对象时，CLI 未正确显示监控状态。6.2.5 中已修复此问题。

- 已修复问题 1745928：在配置了 **no option http-server-close** 应用程序规则时，NTLM 身份验证失败
如果配置 **no option http-server-close** 应用程序规则，NTLM 身份验证将失败。6.2.5 中已修复此问题。
- 已修复问题 1736941：NSX Edge 防火墙 Web 客户端响应非常缓慢
在滚动查看 Edge 防火墙规则网格时，NSX Edge 防火墙 Web 客户端响应非常缓慢。6.2.5 中已修复此问题。
- 已修复问题 1729066：未应用 Edge SCSI 磁盘超时设置。
由于引导脚本文件权限不正确，未应用 Edge SCSI 磁盘超时设置。6.2.5 中已修复此问题。
- 已修复问题 1649098：DHCP 中继代理在 NSX 中无法正常工作
如果距离 DHCP 服务器超过 10 个跃点，TTL 将在传送过程中过期，并且 DHCP 数据包不会到达配置的中继服务器。6.2.5 中已修复此问题。

NSX 6.2.5 中解决的安全服务相关问题

- 已修复问题 1765744：无法将“应用对象”设置为“安全组”的 DFW 规则发布到主机
如果 DFW 规则的“应用对象”字段设置为“安全组”，则无法将该规则推送到新集群中的 ESXi 主机。6.2.5 中已修复此问题。
- 已修复问题 1760081：Netx/服务配置文件规则在发布后不显示在主机上
在大规模环境中，发布新规则或修改的规则后，Netx/服务配置文件规则集的处理需要几个小时才能在主机上生效。6.2.5 中已修复此问题。
- 已修复问题 1738421：如果虚拟机网卡地址无效，则 DFW 控制器会意外退出
在极少数情况下，vCenter 管理员可能为虚拟机的网卡设置了无效的地址，并导致 DFW 控制器进程意外退出。6.2.5 中已修复此问题。
- 已修复问题 1723946：删除的规则短暂转变为 ANY ANY 规则。
在要修改或删除规则的高并发规则置备系统中，如果某条规则在添加后随即在下一次调用中删除，可能被短暂发布为 ANY ANY 规则，直到删除操作完成。6.2.5 中已修复此问题。
- 已修复问题：1738588：某些虚拟机未添加到安全组
有时，不会将虚拟机添加到具有动态条件的安全组中，直到某种活动刷新组成员资格。6.2.5 中已修复此问题。
- 已修复问题 1733763：NSX Distributed Firewall 应用不正确的 TFTP ALG
在端口 69 上处理 TCP 会话时，NSX Distributed Firewall 应用不正确的 TFTP ALG。6.2.5 中已修复此问题。
- 已修复问题 1738419：无效的虚拟机网卡地址导致 DFW 控制器进程退出
极少数情况下，vCenter 管理员可能为虚拟机的网卡设置了无效的地址，从而导致 DFW 控制器进程意外退出。6.2.5 中已修复此问题。
- 已修复问题 1704661 和 1739613：虚拟机断开网络连接并显示以下错误：“无法恢复 PF 状态：超出限制” (Failed to restore PF state: Limit exceeded)
虚拟机断开网络连接并显示以下错误：“无法恢复 PF 状态：超出限制。” (Failed to restore PF state: Limit exceeded.)6.2.5 中已修复此问题。
- 已修复问题 1732337 和 1724222：NSX Manager 无法将防火墙规则推送到 ESXi 6.0 P03 主机
NSX Manager 无法将防火墙规则推送到 ESXi 6.0 P03 主机，并且 NSX Edge 运行状况检查失败。6.2.5 中已修复此问题。

- 已修复问题 1460363：独立 NSX Manager 错误地允许导入通用防火墙配置
在以独立模式运行的 NSX Manager 上，即使不应用通用防火墙规则，也可以导入这些规则。导入后，无法通过 API 或 Web Client 删除这些规则。而是，将这些规则保留并视为本地区域。*6.2.5 中已修复此问题。*

在以前的 6.2.x 版本中已解决以下问题：

6.2.4 及更低版本中解决的常规问题

- 已修复问题 1696192：NSX Manager 上的 NTP 同步问题
NSX 6.2.3 中引入了较新版本的 fcron。在 fcrontab 中未定义任何环境变量，这意味着不会为 fcron 运行作业初始化环境。脚本找不到 ntpdate 命令，因为 \$PATH 是空的。*6.2.4 中已修复此问题。*
- 已修复问题 1644529：提供了解决安全漏洞 CVE-2016-2079 的安全修补程序
6.2.3 版本提供了安全修补程序，可解决 [CVE-2016-2079](#) 问题。
- 已修复问题 1571156：重新启动/重新引导 vCenter 6.0 可能会导致在准备好 VXLAN 的 ESX 主机上出现重复的 VTEP
请参见 [VMware 知识库文章 2144605](#)。*NSX 6.2.3 中已修复此问题。*
- 已修复问题 1529665：当 DaaS 服务使用 2 个不同的 VIP（一个 VIP 用于 HTTP，另一个 VIP 用于 PCoIP），而这两个 VIP 必须拥有完全相同的持久性时，该服务无法使用
6.2.1 中已修复此问题。
- 已修复问题 1631261：IDFW 配置为使用日志采集器 (log scraper)，并且还安装了 GI，在卸载 GI 后，IDFW 停止工作
NSX 6.2.2 中已修复此问题。
- 已修复问题 1551773：在 VMware NSX for vSphere 6.2.0 中，Edge 安全网关 (ESG) HA vNIC 下拉选框始终为空
NSX 6.2.2 中已修复此问题。 请参见 [VMware 知识库文章 2138158](#)。
- 已修复问题 1608608：提供了解决 glibc 漏洞 CVE-2015-7547 的安全修补程序
6.2.2 版本提供了安全修补程序，可解决 [CVE-2015-7547](#) 问题。
- 已修复问题 1480581：netcpa 套接字已关闭，虚拟机无法在 VNI 和子网间通信
解决了线程不安全使用 vmacore 中的 boost::asio 问题后，此问题得以解决。*NSX 6.2.2 中已修复此问题。* 请参见 [VMware 知识库文章 2137011](#)。
- 已修复问题 1583566：规则无法推送到主机
由于 NSX Manager 的任务框架资源限制，无法调度 DFW 规则/ip 列表更新。错误消息显示无法将更改通知线程任务加入队列。*NSX 6.2.2 中已修复此问题。*
- 已修复问题 1573818：ESG 执行 HA 故障切换后，通信中断 50 秒。
如果 NSX 同步 HA NSX Edge 节点间的静态路由失败，则会出现此问题。*NSX 6.2.2 中已修复此问题。*
- 已修复问题 1570808：NSX 负载均衡器 IP_HASH 运行状况检查问题
在 IPVS 中，使用源 ip 哈希算法时，如果所选后端服务器的权重等于 0，那么即使存在运行状况良好的后端服务器，也会发送“服务不可用”回复。*NSX 6.2.2 中已修复此问题。*
- 已修复问题 1564005：在 NSX NetX 中，无法向合作伙伴设备添加流量重定向规则
客户无法向其 NetX 规则集添加流量重定向规则，因此无法将流量重定向到合作伙伴设备。这影响了使用 IP 地址集的规则。此问题是由于 NetX 规则中的 IP 范围处理不当而造成的。*NSX 6.2.2 中已修复此问题。*

- 已修复问题 1587660：DVFilterProcessSlowPathPackets 中的 NSX NetX 错误
在没有 DFW 的情况下使用 NSX NetX 将导致 DVFilter 出现错误。指示
DVFilterProcessSlowPathPackets 中 NetX 错误 PF (err=11,cr2=0x10) 的完整错误消息如下：
VSPDVFPProcessSlowPathPackets: PFFilterPacket。NSX 6.2.2 中已修复此问题。请参见 [VMware 知识库文章 2144018](#)。
- 已修复问题 1591673：向 vSphere Distributed Switch 添加 ESXi 主机失败并返回许可证错误
此错误仅针对 NSX 6.2.1，向 vSphere Distributed Switch 添加 ESXi 主机失败并出现许可证错误消息：“主机 IP 地址未获得使用 VDS 功能的许可。无法将此主机添加到 dvSwitch” (Host IP address is not licensed for the VDS feature. Cannot add this host to dvSwitch)。有关详细信息，请参见 [VMware 知识库文章 2143397](#)。NSX 6.2.2 中已修复此问题。
- 已修复问题 1590563：升级后企业许可证出错
NSX 6.2.1 升级例程允许您在没有 VMware 企业许可证的情况下升级到 6.2.1，但升级后，需要企业许可证才能使用 NSX。NSX 6.2.2 中已修复此问题。请参见 [VMware 知识库文章 2135310](#)。
- 已修复问题 1589046：向未启用 DHCP 中继的 LIF 发送数据包会导致 PSOD
如果 DHCP 单播数据包将发送至预计启用了 DHCP 中继的 LIF 的 IP，但实际接收的 LIF 未启用 DHCP 中继，那么 ESXi 主机将出现 PSOD 错误。NSX 6.2.2 中已修复此问题。请参见 [VMware 知识库文章 2144314](#)。
- 已修复问题 1593436：在 VXLAN 混合模式中，控制器连接中断会错误触发回退到多播模式
NSX 6.2.2 中已修复此问题。请参见 [VMware 知识库文章 2144457](#)。
- 已修复问题 1574995：DFW 发布错误
在筛选模式中修改和保存 DFW 规则可能导致规则无法保存和发布。NSX 6.2.2 中已修复此问题。请参见 [VMware 知识库文章 2141155](#)。
- 已修复问题 1422110：其中一个 NSX Controller 在关闭时未将主节点角色移交给其他控制器
NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。
- 已修复问题 1483728：NSX Controller 的控制平面连接失败
Controller 的控制平面连接显示为失败，netcpa 中显示与 txInProgress 相关的错误。NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。
- 已修复问题 1487910：升级 Edge 服务网关失败，并显示“等待 Edge 虚拟机时超时” (Timed out waiting for Edge vm) 消息
将 IPv6 地址应用于 NSX 管理接口会导致 NSX Manager 使用主机名。将 Edge 虚拟机连接到 NSX Manager 的 vsfwd 代理不能正确处理 FQDN，从而导致出现类似以下内容的错误：“错误 TaskFrameworkExecutor-6 AbstractEdgeApplianceManager:185 - 等待 Edge 虚拟机 {} 时超时。虚拟机引导和响应的时间过长 com.vmware.vshield.edge.exception.VshieldEdgeException” (ERROR TaskFrameworkExecutor-6 AbstractEdgeApplianceManager:185 - Timed out waiting for Edge vm {}. Vm took too long to boot and respond com.vmware.vshield.edge.exception.VshieldEdgeException)。NSX 6.2.0 中已修复此问题。
- 已修复问题 1571548：在 NSX for vSphere 6.2.0 及更高版本中，如果直接在主机上或在 VC 中更改 VTEP 的 IP 地址，会自动释放该 VTEP 的旧 IP 地址。
NSX 6.2.0 中已修复此问题。
- 已修复问题 1551164：在 NSX for vSphere 6.2.0 上，NSX 用户界面 (UI) 灰显几秒钟，并且性能有所下降
请参见 [VMware 知识库文章 2141919](#)。NSX 6.2.1 中已修复此问题。
- 已修复问题 1545840：在 VMware NSX for vSphere 6.x 中，无法禁用主机上的 NSX Distributed Firewall (DFW)
另请参见 [VMware 知识库文章 2141915](#)。NSX 6.2.1 中已修复此问题。

- 已修复问题 1528680：在 VMware NSX for vSphere 6.2.0 中使用 IP 发现时，VMware ESXi 5.x 和 6.x 显示紫色诊断屏幕 (KB 2134329)
当在 VMware NSX for vSphere 6.2.0 中的逻辑交换机上使用 IP 发现时，ESXi 5.x 和 6.x 主机会出现故障，并显示紫色诊断屏幕，如[知识库文章 2134329](#) 中所述。NSX 6.2.1 中已修复此问题。
- 已修复问题 1545885：安全标记 Portlet 上的“管理”选项默认显示为灰色
在虚拟机的摘要页面上，在用户创建新的安全标记前，安全标记 Portlet 上的“管理”超链接始终显示为灰色。NSX 6.2.1 中已修复此问题。
- 已修复问题 1476087：有些控制器日志不可用于 syslog 导出
控制器日志（包括 Zookeeper 集群日志）不是 syslog 导出的一部分。NSX 6.2.1 中已修复此问题。
- 已修复问题 1545830：如果数据大小大于 MTU 的可用数据大小，则在执行 ping 操作时，vdl2 上会发生 ESXi 6.0 PSOD
如果数据大小大于 MTU，则从连接 vmknics 的 NSX 主机交换机执行 ping 操作时，将导致主机发生 PSOD。NSX 6.2.1 中已修复此问题。
- 已修复问题 1545873：用户需要为 TCP 和 UDP 协议配置相同的 IP 地址和端口号
该版本还解决了以下问题：
 - 没有池配置的 UDP 虚拟服务器导致配置失败。
 - 在 UDP 虚拟服务器与任何池均不关联时，统计信息显示不正确的数据。

NSX 6.2.1 中已修复此问题。对于 6.2.1 版，用户可以在 TCP 和 UDP 中使用相同的 IP 地址和端口号，而无论是否具有关联的池。

6.2.4 及更低版本中解决的安装和升级相关问题

- 已修复问题 1710454：新部署的 DLR 与新升级的 DLR 之间的 HA 失效时间不一致
出现此问题的原因是，新升级的 DLR HA 失效时间会在升级期间从 15 秒明确更改为 6 秒。请参阅 [VMware 知识库文章 2146714](#)。6.2.4 中已修复此问题。
- 已修复问题 1578509：重新启动 EAM 后，客户机侦测 (GI) 服务状态为“警告”
NSX 6.2.3 中已修复此问题。
- 已修复问题 1539203：跨 vCenter 升级期间，在 NSX 升级后，NSX 插件与主 VC 断开连接
NSX 6.2.3 中已修复此问题。
- 已修复问题 1558017：在将 NSX Edge 从 6.1.x 升级到 6.2.x 之后，NSX Manager vsm.log 会显示“INVALID DHCP CONFIG”
如果您拥有配置了 IPv6 子网的接口，DHCP 会生成一个空的共享子网，并将其视为无效的操作。
- 已修复问题 1490496：NSX 升级后，客户机侦测无法与 NSX Manager 通信
从 NSX 6.0.x 升级到 NSX 6.1.x 或从 NSX 6.0.x 升级到 NSX 6.2 后，如果未升级客户机侦测服务，则 NSX Manager 无法与客户机侦测通用服务虚拟机 (USVM) 通信。NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。
- 已修复问题 1536179：无法在 Mac OS X Yosemite 及更高版本上安装 SSL VPN-Plus 客户端
支持 Mac OS X 的较早版本。NSX 6.2.1 中已修复此问题。
- 已修复问题 1393503：将 NSX for vSphere 从 6.0.7 升级到 6.1.3 以后，vSphere Web Client 在登录屏幕上崩溃
将 NSX Manager 从 6.0.7 升级到 6.1.3 以后，将会看到 vSphere Web Client UI 登录屏幕上显示异常。您将无法登录 vCenter 或 NSX Manager 并在其上执行操作。NSX 6.2.0 中已修复此问题。

- 已修复问题 1088497：客户机侦测安装失败，并出现错误
在集群中安装客户机侦测时，安装失败并出现以下错误：
VIB 模块的格式无效 (Invalid format for VIB Module)。NSX 6.2.0 中已修复此问题。
- 已修复问题 1328589：DVPor 因主机准备问题而无法启用并显示 “Would block” 错误
在启用 NSX 的 ESXi 主机上，DVPor 因主机准备问题而无法启用并显示 “Would block”。发生这种情况时，首先看到的错误消息会有所不同（例如，可能显示为 VC/hostd.log 中的 VTEP 创建失败、vmkernel.log 中的 DVPor 连接失败或客户机中的 “SIOCSIFFLAGS” 错误）。当 vCenter 推送 vSphere Distributed Switch (vDS) 属性后加载 VIB 时会发生这种情况。升级期间可能发生这种情况。请参见[知识库文章 2107951](#)。NSX 6.2.0 中已修复此问题。
- 已修复问题 1446544：在升级到 NSX 6.1.4 的环境中尝试删除现有 NSX Edge 网关失败
在从 6.1.3 升级到 6.1.4 的 NSX 安装中，升级到 6.1.4 后无法删除现有的 NSX Edge 网关。此问题不会影响升级后创建的新 Edge 网关。此问题不会影响直接从 6.1.2 或更低版本升级的安装。NSX 6.2.0 中已修复此问题。
- 已修复问题 1418836：使用第三方安全 FTP 备份执行 NSX 备份时，AES 加密不可用。NSX 6.2.0 中已修复此问题。
- 已修复问题 1410153：主机重新引导期间 NSX Manager UI 不显示用户友好的错误消息
在此 6.2 版本中，更新的 NSX Manager UI 可显示详细的错误消息，该消息介绍了主机重新引导期间可能出现的问题并提供了可能的解决方案。NSX 6.2.0 中已修复此问题。
- 已修复问题 1412133：无法完成 NSX VIB 安装
如果由于 ixgbe 驱动程序已锁定并阻止其用于安装而无法从第三方模块进行加载，则可能无法按预期安装 NSX VIB。NSX 6.2.0 中已修复此问题。
- 已修复问题 1467438：从 vCloud Networking and Security (vCNS) 5.5.3 升级后无法启动 NSX Manager 服务
将 vCloud Networking and Security (vCNS) 5.5.3 升级到 NSX 6.1.3 后，NSX Manager 服务暂停且无法成功启动。NSX 6.2.0 中已修复此问题。
- 已修复问题 1440867：重新引导 NSX Edge 后不会随机启动消息总线
重新启动 Edge 虚拟机至就绪状态后，通常不会启动消息总线，而需要再执行重新引导操作。NSX 6.2.0 中已修复此问题。

6.2.4 及更低版本中解决的 NSX Manager 相关问题

- 已修复问题 1668519：NSX Manager 的 CPU 占用率较高
当清除任务进程必须处理或清理 NSX Manager 数据库中的大量作业条目时，NSX Manager 可能会持续保持较高的 CPU 占用率，尤其是在重新引导之后。
解决办法：请联系 VMware 技术支持人员。请参见 [VMware 知识库文章 2145934](#)。6.2.4 中已修复此问题。
- 已修复问题 1603954：NSX Manager 一直显示近乎 100% 的内存占用率
重新引导 NSX Manager 会使内存占用率降低到显著低于 100%，但随着时间的推移，占用率值将重新上升到 100% 并在该级别持续显示。6.2.4 中已修复此问题。
- 已修复问题 1540187：用户无法通过 vSphere Web Client 登录，也无法使用 NSX 插件，同时显示用户/组没有权限的错误
此问题与生成 SAML 令牌时发生的超时有关。有时，在与 SSO 服务通信时请求操作没有完成，在这种情况下，NSX 无法在内部刷新解决方案注册提供程序。这会导致在发生此问题时，其他每个请求都出现空指针异常。
NSX 6.2.3 中已修复此问题，方法是避免出现空指针异常，并在需要时重新连接到 SSO 服务。

- 已修复问题 1640388：从不包含任何虚拟机的集群中卸载客户机侦测时，系统会出现“预卸载清除失败”(Pre-Uninstall cleanup failed) 错误消息，并且状态显示为“未解析”
这是客户机侦测卸载逻辑中的已知问题。
NSX 6.2.3 中已修复此问题。
- 已修复问题 1534588：NSX Manager UI 中不显示先前的备份
运行备份操作时，NSX Manager UI 中从不显示成功完成。如果目标文件夹中存储了大量备份文件，则可能会出现这些问题之一。在同一页上显示列表之前，必须检查每个备份文件的兼容性。当前文件列表处理可能会导致页面超时。
NSX 6.2.3 中已修复此问题。
- 已修复问题 1593910：不检测或阻止重复的 NSX Manager IP 地址
如果已将 NSX Manager IP 地址分配给网络上的另一设备，不会生成明确的错误或事件日志。因此，NSX Controller 和主机可能会使用不正确的 MAC 地址响应 NSX Manager，从而导致数据路径故障。**解决办法：**尝试进行判断，然后从网络中移除另一个网络设备，或为其分配其他 IP 地址。由于在网络中存在重复的 NSX Manager IP，因此，主机和控制器会使用错误的 MAC 地址响应 NSX Manager/虚拟机。这会影响 NSX Manager 与 ESX 之间，以及 NSX Manager 与 NSX Controller 之间的通信。这可能会导致数据路径故障。在这种情况下，应用程序会受到影响，直到将重复的 IP 从网络中移除，并且还原通信通道为止。
NSX 6.2.3 中已修复此问题，方法是在检测到重复的 IP 地址时添加系统事件。
- 已修复问题 1489648：使用静止快照备份 NSX Manager 后，无法从 vSphere Web Client 插件使用 NSX
请参见 [VMware 知识库文章 2142263](#)。*NSX 6.2.3 中已修复此问题。*
- 已修复问题 1440451：NSX Manager 证书替换要求重新启动 NSX Manager，并且可能要求重新启动 vSphere Web Client
替换 NSX Manager 设备证书后，必须重新启动 NSX Manager 设备。在某些情况下，vSphere Web Client 在进行证书替换后不会显示“网络和安全”选项卡。
- 已修复问题 1568861：Firefox 浏览器中的 GUI 语言为日语时，无法添加辅助 NSX Manager
使用 Firefox 浏览器在德语、日语、韩语或法语区域设置下添加辅助 NSX Manager 时，不会显示指纹对话框，从而阻止配置。
- 已修复问题 1482989/1522092：NSX “网络和安全”将所有主机显示为绿色，而将集群状态错误地显示为红色
极少数情况下，在 NSX 6.1.4 及更低版本中，NSX “网络和安全”选项卡将所有主机显示为绿色，而将集群状态错误地显示为红色（错误地指示出错状况）。NSX 6.1.5 中已修复此问题。
- 已修复问题 1515656：在将 NSX Manager 添加到 Active Directory 域后，NSX Manager CPU 占用率较高
在将 NSX Manager 添加到 Active Directory 域后，NSX Manager CPU 占用率较高在 NSX Manager 的系统日志中，发现多个 Postgres 线程在运行。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1484939：无法向 vCenter 注册 NSX Manager 6.1.4，显示错误：NSX Management Service 操作失败 (NSX Management Service operation failed)
NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。
- 已修复问题 1521710：NSX Manager Web Client 显示错误：代码 301002 (Code 301002)
描述：在导航至“NSX Manager”>“监控”>“系统事件”时，Web Client 显示以下消息：筛选器配置未应用到 vnic。代码 301002 (Filter config not applied to vnic. Code 301002)。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*

- 已修复问题 1479665：从 6.2.1 版开始，NSX Manager 将查询集群中的每个控制器节点，以获取该控制器与集群中的其他控制器之间的连接信息
此信息在 NSX REST API（“GET https://[NSX-MANAGER-IP-ADDRESS]/api/2.0/vdn/controller”命令）的输出中提供，现在会显示各控制器节点之间的对等连接状态。如果 NSX Manager 发现任何两个控制器节点之间的连接断开，则会生成系统事件以警示用户。*NSX 6.2.1 中已修复此问题。*
- 已修复问题 1525516：如果在其他设备上对管理器执行备份还原，则会中断控制器的强制同步
如果克隆和/或从备份还原 NSX Manager 设备，则对 NSX Controller 集群执行的强制同步操作将失败。从头开始部署的 NSX Manager 不会发生此问题。*NSX 6.2.1 中已修复此问题。*
- 已修复问题 1509454：未包含在 NSX 安装中的主机会发生 NSX 日志记录检测信号故障
在从 vCenter 清单中直接移除为 NSX 准备的主机时（未事先在 NSX 中取消该主机的准备），NSX 会收到意外的“主机已连接”DCN，这导致从主机中部分移除消息基础架构组件。结果，NSX 与主机之间本应移除的消息链接可能仍保持活动状态，并且 NSX 可能会对主机引发错误的“警报”系统事件。*NSX 6.2.1 中已修复此问题。NSX 6.2.1 中已修复此问题。*
- 已修复问题 1418655：运行 **write erase** 命令后 NSX Manager 无法运行
您可能会注意到，在运行 `write erase` 命令后重新启动 NSX Manager 时，NSX Manager 无法按预期工作，如访问 Linux Shell 的密码已重置、设置命令丢失等。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1366669：添加域时，使用域凭据的 LDAP 选项显示错误
在 NSX 6.1.x 中，用户尝试添加 LDAP 域时，Web Client 显示**未指定用户名**（User Name was not specified）错误，即使已在 UI 中提供用户名亦是如此。*NSX 6.2.0 中已修复此问题。NSX 6.2.0 中已修复此问题。*
- 已修复问题 1352169：CA 签名证书导入需要重新引导 NSX Manager 才能生效
导入 CA 签名的 NSX Manager 证书时，新导入的证书在 NSX Manager 重新引导后才有效。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1497113：无法将 NSX Manager 导入到 LDAPS 域
尝试将 NSX Manager 添加到 LDAPS 域时，出现以下错误消息。
无法连接到主机 <Server FQDN>
错误消息：简单绑定失败：<Server FQDN:Number> (Cannot connect to host <Server FQDN> error message: simple bind failed: <Server FQDN:Number>)。*NSX 6.2.0 中已修复此问题。*

6.2.4 及更低版本中解决的逻辑网络连接和 NSX Edge 路由相关问题

- 已修复问题 1696887：虚拟机断开逻辑分布式路由器的北向网络连接
如果虚拟机将逻辑路由器的 pMac 用作默认网关的 MAC 地址，而不是通用逻辑路由器 MAC 地址，则会断开逻辑路由器的北向连接。
解决办法：请参见 [VMware 知识库文章 2146293](#)。*6.2.4 中已修复此问题。*
- 已修复问题：已断开 NSX Controller 连接的 VNI 存在数据路径问题
出现此问题是因为，在 NSX-V 6.1.5、6.1.6、6.2、6.2.1 和 6.2.2 版本中禁用了 IPSec 重新加密功能，以避免发生其他已知的 IPSec 问题。

请参见 [VMware 知识库文章 2146973](#)。*NSX 6.2.3 中已修复此问题。*
- 已修复问题 1591582：在某些极端条件下，VDR 实例发送的 ARP 请求可能会被丢弃
在 VDR 上行链路输出处理时，VDR 向位于其他主机上的远程虚拟机发送的 ARP 请求可能会被丢弃，从而导致建立连接速度较慢。

- 已修复问题 1501900：在更改 OSPF 接口的 IP 地址后，Edge OSPF 路由器仍保持停留在 ExchangeStart 状态
由于存在争用的情况，更改 OSPF 接口的 IP 地址会导致两侧的 OSPF 邻居保持停留在 ExchangeStart 状态。在正常情况下，支持更改 OSPF 接口的 IP 地址。
NSX 6.2.3 中已修复此问题。
- 已修复问题 1498251：Edge 服务网关路由器不支持 IS-IS 路由协议

已从 NSX 6.2.3 的 UI 和 API 中移除对 IS-IS 的引用。
- 已修复问题 1492738：使用 vSphere Web Client 部署分布式逻辑路由器 (DLR) 期间，无法添加八个以上的上行链路接口
NSX 6.2.3 中已修复此问题。
- 已修复问题 1552038：间歇性丢失从 NSX Edge 到 DLR 上行链路接口的连接
导致此问题的原因是，NSX Edge 的 ARP 表中具有 DLR 控制虚拟机的 MAC 地址，而不是 DLR 的本地实例 MAC 地址。此版本添加了一个出站 ARP 筛选器，可防止 DLR 控制虚拟机生成与 DLR IP 地址相关的 ARP。
- 已修复问题 1454161：无法配置下一跃点为 /31 IP 地址的静态路由
NSX 6.2.3 中已修复此问题。
- 已修复问题 1528443：Edge 虚拟机在故障切换期间发送 GARP 时，不更新主机上的 VXLAN ARP 缓存
在某些部署中，例如，虚拟机和 Edge 位于同一 VXLAN 分段上时，在 Edge 故障切换之后，主机上的 VXLAN ARP 缓存不会更新。*NSX 6.2.3 中已修复此问题。*
- 已修复问题 1600874：部署新 Edge 虚拟机时，不移除滞留的虚拟机
升级 Edge 时，如果发布操作和回滚操作都失败，则原始 Edge 虚拟机会保留在 NSX Manager 数据库中，而 VC 却保持新 Edge 虚拟机的 ID 号。由于这种不匹配情况，重新部署 Edge 虚拟机会失败。强制同步也会失败，并显示错误“未找到虚拟机” (VM not found)。
- 已修复问题 1467774：“show ip bgp neighbor”命令的“管理距离”字段中显示错误值
从 EBGp 对等会话中发现并播发到同一 AS 中 IBGP 对等会话的路由会错误地保持前一管理距离。6.2.3 中已修复此问题。
- 已修复问题 1613383：对于在 L4 模式下运行的 NSX Edge 负载均衡器，当前连接数值错误地使用了总连接数
此版本已修复此问题，现在使用活动连接数的总和来计算当前连接数。6.2.3 中已修复此问题。
- 已修复问题 1584664：如果在手动从 vCenter 清单中移除负载均衡器池虚拟机成员之前，没有先在 NSX 中取消配置，则 NSX Manager 数据库中会残留孤立的数据库条目。NSX Manager 日志中将报告 ObjectNotFoundException。
6.2.3 中已修复此问题。
- 已修复问题 1446809：如果在 Edge 重新引导后没有发送运行状况检查恢复事件，NSX Edge 便再也无法由 vCloud Director 进行管理
NSX Manager 会在内存中保存 Edge 连接状态。当 Edge 虚拟机未能响应运行状况检查时，会引发一个错过事件；而在恢复时，会引发一个已恢复事件。如果重新启动 NSX Manager，则在重新引导后未错过任何运行状况检查时，可能不会发送恢复事件。由于 vCloud Director 依赖于这些事件，错过恢复事件可能会导致无法从 vCD 中管理 Edge 虚拟机。
- 已修复问题 1462506：无法通过配置了 CA 签名证书的 L2VPN 服务重新部署 NSX Edge
无法通过配置了 CA 签名证书或自签名证书的 L2VPN 服务重新部署 NSX Edge 或更改其大小。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*

- 已修复问题 1441319：在使用动态路由的安装中，移除逻辑接口 (LIF) 后连接丢失
使用动态路由 (OSPF 和 BGP) 时在 NSX 逻辑路由器 (Edge/DLR) 中发现一个问题，该问题会导致移除 LIF 后网络连接丢失。此问题会影响 NSX 版本 6.0.x 到 6.1.4。NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。
- 已修复问题 1399863：移除 IPsec VPN 通道的本地和远程子网中的直接汇总网络时，到对等 Edge 的间接子网的汇总路由也将消失
在 Edge 上没有默认网关的情况下，如果在配置 IPsec 的同时移除本地子网中的所有直接连接子网以及远程子网中的部分直接连接子网，其余的对等子网将无法通过 IPsec VPN 进行访问。NSX 6.2.0 中已修复此问题。
- 已修复问题 1445291：NSX Edge 上的 RADIUS 身份验证服务器配置失败
在 NSX 6.1.5 及更早版本中，RADIUS 服务器私钥字符串仅限包含 32 个字符；如果字符串超过此字符限制，RADIUS 服务器便无法与 NSX Edge 连接。现在，该限制为 64 个字符。NSX 6.2.0 中已修复此问题。
- 已修复问题 1534811：VMware NSX for vSphere 6.x Edge 的 VIO 热堆栈部署发生间歇性故障，并出现以下错误：无法分配内存 (Cannot allocate memory)
运行状况监控内存用量会随时间增加，最终导致 Edge 发生故障。NSX 6.2.1 中已修复此问题。
- 已修复问题 1500624：有效应用 BGP 筛选器大概需要 40 秒
在此期间，只会应用所有不包含筛选器的重新分发策略。此延迟仅出现在“出站”方向的 NSX 分布式逻辑路由器 (DLR) 上。NSX 6.2.0 中已修复此问题。
- 已修复问题 1484758：在 NSX Edge 子接口上，即使禁用“发送 ICMP 重定向”选项，也会发出 ICMP 重定向
默认情况下，NSX Edge 子接口已禁用“发送 ICMP 重定向”。尽管此选项已禁用，Edge 子接口仍会发送 ICMP 重定向。NSX 6.2.0 中已修复此问题。
- 已修复问题 1265605：无法在逻辑路由器的网桥或租户名称中添加非 ASCII 字符
NSX Controller API 不支持非 ASCII 字符。NSX 6.2.0 中已修复此问题。
- 已修复问题 1341784：修改 BGP 邻居筛选器规则时，现有筛选器可能在长达 40 秒的时间内无法应用
将 BGP 筛选器应用于运行 IBGP 的 NSX Edge 时，可能需要长达 40 秒的时间才能将这些筛选器应用于 IBGP 会话。在此期间，NSX Edge 可能会播发被 IBGP 对等会话 BGP 筛选器拒绝的路由。NSX 6.2.0 中已修复此问题。
- 已修复问题 1422110：其中一个 NSX Controller 在关闭时未将主节点角色移交给其他控制器
通常情况下，当承担操作主节点角色的控制器准备关闭时，会自动将主节点角色移交给其他控制器。而在这种情况下，控制器未将该角色移交给其他控制器并转变为中断状态，随后进入已断开连接模式。NSX 6.2.0 中已修复此问题。
- 已修复问题 1440790：无法通过单播或多播在主机之间传输 VXLAN 流量
虚拟机位于同一主机上时，可以通过单播或多播在 VXLAN 中进行通信，但当虚拟机位于不同主机上时则无法通信。NSX 6.2.0 中已修复此问题。
- 已修复问题 1432420：同时移除 NSX Edge/DLR 上的多个 BGP 规则导致 Web Client 崩溃。NSX 6.2.0 中已修复此问题。现在可以同时删除多个 BGP 规则。
- 已修复问题 1431716：添加边界网关协议 (BGP) 拒绝规则后短暂显示协议地址
您可能会注意到，在 NSX Edge 服务网关中添加边界网关协议 (BGP) 拒绝规则后，会短暂显示协议地址。NSX 6.2.0 中已修复此问题。

- 已修复问题 1441773：vMotion 期间虚拟机断开连接
您可能会注意到 vMotion 期间虚拟机会断开连接，或者您可能会收到虚拟机网卡断开连接的警示。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1463579：无法下载控制器快照
您可能会注意到，下载控制器快照时无法下载最后一个控制器的快照。例如，如果您有三个控制器，您可以成功下载前两个控制器的快照，但可能无法下载第三个控制器的快照。*NSX 6.2.0 中已修复此问题。*

6.2.4 及更低版本中解决的 Edge 服务相关问题

- 已修复问题 1674721：升级到 NSX 6.2.3 后，无法管理 NSX Edge
当在负载均衡器中配置了 serverSsl 或 clientSsl，但之前版本中的密码值设置为空时，会出现此问题。
解决办法：请参阅 [VMware 知识库文章 2145887](#)。6.2.4 中已修复此问题。
- 已修复问题 1698389：在通过 vSphere Web Client 更改某些路由配置后，路由配置不正确
在编辑 BGP 邻居、OSPF 区域到接口的映射、路由重新分发 - IP 前缀或 BGP 筛选器时，排序并随后编辑将导致不正确的配置。在配置大量 BGP 邻居时，滚动查看列表并随后进行编辑可能会导致不正确的配置。
解决办法：请参阅 [VMware 知识库文章 2146363](#)。6.2.4 中已修复此问题。
- 已修复问题 1633694：存储故障可能引发 NSX Manager 数据库中的 VXLAN 配置丢失
发生存储故障后，Virtual Center 可能会报告 DVS 已被删除，并且 NSX Manager 会做出响应，移除与该 DVS 关联的 VXLAN 配置。发生这种情况时，将在 NSX Manager 日志中记录类似以下内容的错误消息：“INFO DCNPool-9 VcDriver:1077 - Deleting vmknics info from host tables [host-21843 : 319]”。
NSX 6.2.3 中已修复此问题。
- 已修复问题 1456172：禁用 NSX Edge 防火墙后，NAT 不转换 IP 地址
禁用 Edge 网关防火墙后，如果 Edge 设备是 6.0 超大型设备或 6.1 和 6.2 Edge 设备，同时还会禁用所有有状态服务。*NSX 6.2.3 版本在 UI 中添加了一个警告，指出同时还会禁用其他有状态服务。*
- 已修复问题 1499601：只使用静态路由时，Edge 服务网关 (ESG) 或带有 Edge 虚拟机的 DLR 的 HA 故障切换时间延长
NSX 6.2.3 中已修复此问题。
- 已修复问题 1618289：在 VMware NSX for vSphere 6.2.x 中进行 Edge 高可用性 (HA) 故障切换时，TCP 会话发生 TCP 意外中断
出现此问题是由于在 VMware NSX for vSphere 6.2.x 中使用的内部资源库已过时。*NSX 6.2.3 中已修复此问题。*
- 已修复问题 1653484：NSX Edge 核心转储不显示函数名称
NSX 6.2.3 通过在核心文件中显示内存地址信息增强可调试性。但是，您必须仅在 VMware 技术支持要求时才启用核心转储。
NSX 6.2.3 中已修复此问题。
- 已修复问题 1604506：如果对静态路由用例使用默认网关，则无法在没有 NSX Edge 虚拟机的情况下部署分布式逻辑路由器 (DLR)

通过 Web 客户端部署新的分布式逻辑路由器 (DLR) 时，通过在配置过程中选择“配置默认网关”选项，创建 DLR 会失败，并且会在弹出式窗中显示以下错误：“[Routing] 管理距离仅在已部署 NSX Edge 虚拟机的 NSX Edge 6.2.0 版及更高版本上受支持” (*[Routing] Admin Distance is supported only on NSX Edge version 6.2.0 and later with NSX Edge VMs deployed*)。

有关详细信息，请参见 [VMware 知识库文章 2144551](#)。*NSX 6.2.3 中已修复此问题。*

- 已修复问题 1445057：在逻辑路由器 (DLR) 中未采用在 NSX Edge 服务网关 (ESG) 上配置的 OSPF 路由并丢弃受影响的数据包
在 OSPF 使用 IP_HDRINCL 选项时，将会出现该问题。在某些 Linux 内核中，如果使用该选项，则会禁止 IP 堆栈对数据包进行分段。因此，将丢弃大于接口 MTU 的任何数据包。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1406471：Syslog 在还原的 NSX Manager 上显示备份 NSX Manager 的主机名
假设第一个 NSX Manager 的主机名是 A，且为该 NSX Manager 创建了备份。现在安装了第二个 NSX Manager，并根据备份还原文档将其配置为与旧 Manager 使用相同的 IP 地址，但主机名为 B。在此 NSX Manager 上运行还原。还原的 NSX Manager 在还原完成时显示主机名 A，而在重新引导后又显示主机名 B。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1444581：ESXi 主机可能会丢失网络连接
当系统记录了类似于以下内容的多条错误消息时，ESXi 主机可能会丢失网络连接并遇到稳定性问题：
警告：检测信号：785：PCPU 63 已有 7 秒无检测信号；*可能*会被锁定 (WARNING: Heartbeat: 785: PCPU 63 didn't have a heartbeat for 7 seconds; *may* be locked up)。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1444784：vMotion 期间虚拟机断开连接
在 6.0.8 上执行 vMotion 期间虚拟机断开连接，并显示消息：VISP 堆已耗尽 (VISP heap depleted)。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1440867：重新引导 NSX Edge 后不会随机启动消息总线
重新启动 Edge 虚拟机至就绪状态后，通常不会启动消息总线，而需要再执行重新引导操作。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1548939：在配置虚拟服务器时，应用了以前选择的 IP 地址
在创建新的虚拟服务器时，您可能会注意到，IP 地址是从以前选择的 IP 池列表中自动应用的。如果以前选择一个 IP 池以获取虚拟服务器 IP，则会发生这种情况。在尝试编辑虚拟服务器 IP 池信息时，不会从 UI 中将这信息自动发送到后端，并自动应用从 IP 池中获取的先前 IP 地址。*NSX 6.2.1 中已修复此问题。*
- 已修复问题 1599706：在两个 VNI 之间通过 LDR 通信时，SYN/ACK 数据包丢失
NSX 6.2.2 中已修复此问题。
- 已修复问题 1082549：在 Edge 服务网关上启用 HA 时，将 OSPF 呼叫和停顿间隔分别配置为 30 秒和 120 秒以外的值会导致故障切换期间某些流量丢失
当主 NSX Edge 在 OSPF 正在运行且启用 HA 的情况下失败时，待机所需的时间将超过正常的重新启动超时时间，并导致 OSPF 邻居从其转发信息库 (FIB) 表中移除发现的路由。这将导致数据平面在 OSPF 重新启动聚合之前出现故障。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1403594：虚拟机无法从 Edge DHCP 服务器接收 ping
虚拟机可以对 Edge 网关执行 ping 操作，但无法通过覆盖网络从 Edge 网关中继接收 DHCP ping。Edge DHCP 服务器设置为中继端口且无法传输或接收任何流量。但是，Edge 网关和 DHCP Edge 位于相同主机上时可以相互执行 ping 操作。DHCP Edge 移动到另一台主机时，DHCP Edge 无法从 Edge 网关接收 ping。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1477176：vSphere Web Client 中未正确显示 Edge 负载均衡器状态
负载均衡器在 vSphere Web Client UI 的图表中不显示并发连接数量统计信息。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1484743：升级到 NSX 6.1.2 或更高版本后，无法通过负载均衡器传递流量
在 NSX Edge 负载均衡器上使用“插入 X-Forwarded-For”选项时，流量可能无法通过负载均衡器。*NSX 6.2.0 中已修复此问题。*

- 已修复问题 1449461：运行 `clear ip ospf neighbor` 命令时返回分段错误
NSX 6.2.0 中已修复此问题。
- 已修复问题 1418264：无法处理 Kerberos 请求
与 NSX Edge 保持均衡时，某些 Kerberos 请求失败。*NSX 6.2.0 中已修复此问题。*

6.2.4 及更低版本中解决的安全服务相关问题

- 已修复问题 1558051 和 1769174：对于 DFW 处于禁用状态的集群，不会强制执行排除列表更新，并且会基于排除列表创建筛选器。
如果某一集群的 DFW 处于禁用状态，则不会强制执行排除列表更新。出现此问题是因为 `isFirewallEnabled` API 执行严格的检查，只在所有主机都启用了 DFW 时才返回“true”。如果环境中有任何集群禁用了防火墙，都会返回“false”。
修复后，API 现在检查是否已为任何集群启用了防火墙，如果环境中有任何一个集群启用了防火墙，就会返回“true”。
此外，还会在禁用了 DFW 的主机上基于排除列表更新创建筛选器。修复后，对于每一个排除的虚拟机，API 都会获取集群，如果集群启用了防火墙，则添加该集群的系统虚拟网卡 ID 和虚拟机的虚拟网卡 ID，并发布每个集群的排除列表。通过发布虚拟机集群的排除列表，可处理将虚拟机从一个集群迁移到另一集群的过程。*6.2.4 中已修复此问题。*
- 已修复问题 1694483：在配置了 Distributed Firewall (DFW) 和安全组 (SG) 的情况下安装或升级到 NSX for vSphere 6.2.3 之后，在计算虚拟机上执行 vMotion 操作时，可能会遇到通信中断问题。
请参见 [VMware 知识库文章 2146227](#)。*6.2.4 中已修复此问题。*
- 已修复问题 1689356：通过搜索编辑安全组将从该安全组中移除所有对象
如果通过搜索静态包含的成员（如虚拟机）并随后移除该成员来编辑安全组，将导致从该安全组中移除所有静态包含的成员。*6.2.4 中已修复此问题。*
- 已修复问题 1675694：在连接中断后重新使用相同的 IP 和端口时，Distributed Firewall 会丢弃数据包
处于半关闭状态的连接不会断开，从而导致与该 IP 和端口的新连接失败。*6.2.4 中已修复此问题。*
- 已修复问题 1698863：启用 Distributed Firewall 后，在建立的 TFTP 会话中重新传输初始 TFTP 数据包可能会导致显示紫色诊断屏幕
6.2.4 中已修复此问题。
- 已修复问题 1701195：Distributed Firewall 遇到堆耗尽问题
在具有较高整合比（为每个主机置备的虚拟机数）的较大型部署中，Distributed Firewall 将会遇到堆内存耗尽问题，因为 VMkernel 中的 DFW 具有有限的可用堆内存量（在大型内存主机上最多为 1.5 GB）。*6.2.4 中已修复此问题。对于具有 96 GB 或更多内存的 ESXi 6.0 主机，最大堆大小已增加到 3 GB，支持更高的整合比。*
- 已修复问题 1712698：在尝试修改安全策略防火墙规则后，服务编排安全策略规则被删除
6.2.4 中已修复此问题。
- 已修复问题 1620109：部署第三方服务虚拟机无法按预期完成，安装状态将报告为“失败”
例如，SVM 收不到预期的 IP 地址。在 NSX Manager 日志中显示错误消息“为参数 `property.info.key` 提供的值不正确” (Value provided for parameter `property.info.key` was not correct)。

请参见 [VMware 知识库文章 2145376](#)。*NSX 6.2.3 中已修复此问题。*
- 已修复问题 1619570：对于包含数百万条规则和服务编排的大规模 DFW 配置，重新引导后规则发布可能需要几秒钟才能完成。在此期间无法发布新规则
NSX 6.2.3 只重新同步那些由于重新引导而尚未处理其最新修订的防火墙策略，从而缩短了重新引导时同步防火墙规则所需的时间。

- 已修复问题 1526781：在 NSX 6.2.x 上查询 getFirewallConfigLayer3SectionByName API 不返回 responseHeaders 字段
6.2.3 中已修复此问题，ETag 标头信息已在此 API 输出中恢复。
- 已修复问题 1599576：由于为“全局区域 ID”字段设置了空值，通用防火墙区域中经过编辑的规则可能无法发布。
不会报告任何错误消息。NSX 6.2.3 中已修复此问题。
- 已修复问题 1558501：当通用 SVM 与 NSX Manager 之间的连接失败时，可能无法安装客户机侦测
仅使用 FQDN 配置 NSX Manager 时，NSX Manager 和客户机侦测服务虚拟机之间的消息处理通道可能会出现故障。发生此问题时，客户机侦测服务状态仍保持为“警告”。USVM 上的 eventmanager.log 文件中会显示“UnknownHostException”消息。在 NSX 6.2.3 中添加了自动 DNS 支持以修复此问题。
- 已修复问题 1673068：在“服务编排策略”部分中编辑防火墙规则会导致配置不同步
如果在防火墙配置屏幕的“服务编排”策略部分中添加或编辑防火墙规则，服务编排会不同步。已将防火墙配置的“服务编排”部分更改为只读以修复此问题。通过服务编排创建的规则必须通过服务编排进行管理。NSX 6.2.3 中已修复此问题。
- 已修复问题 1639612：在 NSX for vSphere 6.2.x 中，出现 MSRPC 与 Windows 2008 及更高版本的连接问题
Windows 的更高版本支持 64 位寻址，在这些版本中，DCE/EPM 协议以 NDR64 为传输编码格式进行协商，这会导致防火墙无法解析 EPM 响应数据包，因此无法检测要打开的动态端口。请参见 [VMware 知识库文章 2145135](#)。NSX 6.2.3 中已修复此问题。
- 已修复问题 1567693：若使用 IPset 作为 NetX 规则中的源/目标，会显示错误“容器类型 IPSet 无效” (Invalid container type: IPSet)
NSX 6.2.3 中已修复此问题。
- 已修复问题 1407920：如果使用 REST API 调用删除防火墙配置，则无法加载和发布已保存的配置
删除防火墙配置时，将创建一个使用新区域 ID 的新默认区域。当您加载已保存的草稿（具有相同区域名称，但是区域 ID 较旧）时，区域名称发生冲突，并显示以下错误：
重复键值违反唯一性限制 firewall_section_name_key (Duplicate key value violates unique constraint firewall_section_name_key)。
NSX 6.2.3 中已修复此问题。
- 已修复问题 1498504：从两个重叠服务组的一个组中移除虚拟机时，该虚拟机失去防火墙保护
将服务编排工作流创建的另一个服务应用于同一虚拟机时，主机上的 NetX 筛选器（由防火墙工作流创建）被移除。例如，将一个服务配置文件应用于两个重叠的服务组时，会发生此问题。在这种情况下，如果虚拟机同时位于两个服务组中，然后从其中一个服务组中移除该虚拟机，那么该虚拟机会失去保护。6.2.3 中已修复此问题，方法是在服务配置文件中引入优先级字段。如果主机上存在重叠的 vNIC 服务组，将应用具有最高优先级的服务配置文件。
- 已修复问题 1550370：在上游数据路径故障超过 15 分钟之后，安装有 NFSv3 的 Linux 虚拟机出现操作系统挂起
请参见 [VMware 知识库文章 2133815](#)。NSX 6.2.3 中已修复此问题。
- 已修复问题 1494366：在“取消源”/“取消目标”启用的情况下复制并粘贴防火墙规则将在列出新规则时禁用“取消”选项
在“取消源”/“取消目标”选项启用的情况下复制防火墙规则时，会创建新防火墙并禁用此选项。NSX 6.2.3 中已修复此问题。

- 已修复问题 1473767：流量监控丢弃超过 200 万条（每 5 分钟）限制的流
NSX 流量监控最多可保留 200 万条流记录。如果主机在 5 分钟内生成的记录超过两百万条，则新的流将被丢弃。*NSX 6.2.3 中已修复此问题。*
请参见 [VMware 知识库文章 2091376](#)。
- 已修复问题 1611238：在 6.2.x 的 Edge 防火墙中，只显示在 Edge 范围创建的安全组（只能通过 REST 创建 Edge 范围的 SG）
在 6.2.3 中，在全局范围创建的 SG（可以在 UI 中创建这些 SG）和为相应 Edge 在 Edge 范围创建的 SG（只能通过 REST 创建这些 SG）都会显示在 Edge 防火墙中安全组列表的“源”/“目标”列下。*NSX 6.2.3 中已修复此问题。*
- 已修复问题 1516460：即使删除了防火墙规则中的应用对象逻辑交换机，防火墙规则仍被标记为有效
6.2.3 中已修复此问题。
- 已修复问题 1542157：将受保护的虚拟机通过 vMotion 操作移动到目标主机后，Distributed Firewall 功能丢失
从 VC 清单中移除已经准备好了 NSX 的主机时，会从内部防火墙表中移除该主机条目。以后再将该主机添加回 VC 清单时，不会重新创建防火墙表条目。*6.2.3 中已修复此问题。*
- 已修复问题 1592439：服务编排无法将虚拟机转换到安全组
出现此问题是由于通用服务虚拟机 (USVM) 上的 EpSecLib 中出现死锁。*6.2.3 中已修复此问题。*
- 已修复问题 1534597：NSX for vSphere 6.x 控制器间歇性断开连接
由于随 6.1.4 和更早版本提供的 StrongSWAN 软件包中存在 IPSEC 错误，在更新 IPSEC 密钥后，不会建立控制器之间的隧道。这会导致控制器之间的连接部分中断，从而导致出现很多不同的问题。有关详细信息，请参见[知识库文章 2127655](#)。*NSX 6.1.5 和 6.2.1 中已修复此问题。*
- 已修复问题 1491042：在“安全组对象选择”屏幕中，LDAP 域对象返回所需的时间太长或无法返回。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1468169：查看防火墙规则时鼠标移动延迟
在 vSphere Web Client 的 NSX “网络和安全”部分中，如果在“防火墙规则”中的行上移动鼠标，每次移动会延迟 3 秒显示结果。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1476642：NSX-v 中的一些 IP SpoofGuard 规则未正确应用
NSX-v 中的一些 IP SpoofGuard 规则未正确应用。NSX-v 中的安全组内未显示实例，需要手动将实例添加到该安全组。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1510350：在“服务编排”用户界面中执行批量删除时显示消息：**在 0 到 0 之间 (between 0 to 0)**
从 NSX 的“服务编排”用户界面中批量删除策略（100 条左右）时显示消息：应在 0 到 0 之间 (It should be between 0 to 0)。可以放心地忽略此消息。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1515656：执行策略删除的后台操作可能需要较长时间，并且 CPU 占用率很高
删除一个策略时将在后台重新评估其余的所有策略。在具有大量策略、大量安全组以及/或者每条策略有大量规则的设置中，这可能需要一个小时以上的时间。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1515630：在 20 分钟的默认超时时间之后，所有排队的可发布任务均标记为失败
队列按 NSX Edge 进行维护，可以针对不同的 Edge 并行发布。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1545879：如果重命名现有防火墙草稿，该操作将失败并在 UI 中显示“内部服务器错误”
NSX 6.2.1 中已修复此问题。

- 已修复问题 1545893：某些 DFW 集中式 CLI 显示 “ERROR output 100”
在虚拟网络适配器 (vNIC) 处于断开连接状态的某些情况下，NSX Manager 中的 vNIC 状态信息与主机之间可能会出现差异，导致集中式 CLI 中显示 “ERROR output 100”。*NSX 6.2.1 中已修复此问题。*
- 已修复问题 1545853：未对应用程序配置文件列表进行排序。
如果启用了 Service Insertion，将按未排序的方式显示 NSX Edge 中的应用程序配置文件名称列表。该版本修复了该问题以按排序的方式显示应用程序配置文件列表。*NSX 6.2.1 中已修复此问题。*
- 已修复问题 1545895：在某些设置中，针对特定 ESXi 主机运行的中央 CLI 命令会超时
NSX 6.2.1 中已修复此问题。
- 已修复问题 1491365：vsfwd.log 被大量容器更新快速覆盖
更改 SpoofGuard 策略后，NSX Manager 会立即将相应更改发送到主机，但主机需要较长时间处理该更改并更新虚拟机的 SpoofGuard 状态。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1113755：无法使用在全局范围定义的安全组或其他分组对象配置 NSX 防火墙
在 NSX Edge 范围定义的管理员用户无法访问在全局范围定义的对象。例如，如果用户 *abc* 在 Edge 范围定义，而安全组 *sg-1* 在全局范围定义，则 *abc* 将无法在 NSX Edge 的防火墙配置中使用 *sg-1*。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1425691：查看防火墙规则时鼠标移动延迟
在 vSphere Web Client 的 NSX “网络和安全” 部分中，在 “防火墙规则” 中的行上移动鼠标时会延迟 3 秒显示结果。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1352926：尽管发布成功，但是 UI 仍然显示错误消息：**防火墙发布失败 (Firewall Publish Failed)**
如果在您环境中的集群子集上启用 Distributed Firewall，且您更新了一个或多个有效防火墙规则中使用的应用程序组，则在 UI 上进行的任何发布操作都将显示错误消息，且该消息中包含未启用 NSX 防火墙的集群的主机 ID。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1295384：通过 REST 删除安全规则时显示错误
如果使用 REST API 调用删除服务编排创建的安全规则，对应的规则集实际上不会从服务配置文件缓存中删除，导致出现 `ObjectNotFoundException` 错误。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1412713：防火墙规则未反映新添加的虚拟机
将新的虚拟机添加到逻辑交换机时，防火墙规则未正确更新以包括新添加的虚拟机。更改防火墙并发布更改后，新对象将添加到策略中。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1448022：配置安全组时无法选择 Active Directory 对象
在 NSX 6.1.x 中，安全组对象选择屏幕中的 AD/LDAP 域对象在很长时间后才返回。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1473585：无法添加源/目标为逗号分隔的多个 IP 地址的防火墙规则。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1460351：无法在列表顶部移动 NSX Distributed Firewall (DFW) 部分。
使用服务编排创建安全组策略时，无法将在 DFW 表中创建的此部分添加到列表顶部。无法上下移动 DFW 部分。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1501451：将安全策略配置为端口范围导致防火墙不同步
将安全策略配置为端口范围（如 “5900-5964”）将导致防火墙不同步，并出现错误 `NumberFormatException`。*NSX 6.2.0 中已修复此问题。*

6.2.4 及更低版本中解决的监控服务相关问题

- 已修复问题 1697118：所有 IPFIX 流量都标记为新流量，而不是更新的流量，从而导致频繁更新 IPFIX 收集器
此外，发送活动流量的频率不会遵从配置的活动流量超时值。6.2.4 中已修复此问题。
- 已修复问题 1617561：vmkernel 日志文件中充满 "ALERT: vdrb: VdrArpInput:1015: CP:Malformed pkt"
当像服务器这样的网络设备使用 IEEE 802 网络 ARP 格式发送 ARP 请求时，会发生这种情况。6.2.3 中已修复此问题。
- 已修复问题 1525620：Distributed Firewall 规则中的 icmpCode 值未发送到主机。
protocolName 和 subProtocolName 值正常工作
6.2.3 中已修复此问题。
- 已修复问题 1563830：在将源或目标作为“mgmtInterface”的 DLR 设备上应用防火墙规则失败
在 NSX Manager 日志中报告类似以下内容的消息：“vShield Edge:10014:NSX Edge 虚拟机上的配置失败” (vShield Edge:10014:Configuration failed on NSX Edge vm)。6.2.3 中已修复此问题。
- 已修复问题 1474498：REST API 请求移除现有防火墙配置后，导入草稿防火墙规则失败
如果草稿是在 VMware NSX for vSphere 6.1.x 和 6.2.x 中创建并包含 *section id = null*，则会发生此问题。6.2.3 中已修复此问题。
- 已修复问题 1545888：在报告流统计信息时，索引 0（输入字节）和索引 1（输出字节）计数有时是颠倒的。
索引 0 保存起始方向的流量计数，索引 1 保存相反方向的流量计数。NSX 6.2.1 中已修复此问题。
- 已修复问题 1460085：#show interface 命令不显示 vNic_0 接口的带宽/速度
运行“#show interface”命令后，会显示全双工模式速度“0 M/s”，但不显示 NSX Edge vNic_0 接口的带宽/速度。NSX 6.2.0 中已修复此问题。
- 已修复问题 1288395：针对 Distributed Firewall 启用 IPFIX 配置时，vDS 上的 NetFlow 或 SNMP 的 ESXi 管理接口中的防火墙端口可能被移除
当针对 IPFIX 定义收集器 IP 和端口时，ESXi 管理接口的防火墙将在出站方向为指定 UDP 收集器端口打开。该操作可能会移除以下服务（如果先前已在 ESXi 主机上配置）的 ESXi 管理接口防火墙上的动态规则集配置：
 - vDS 上的 Netflow 收集器端口配置
 - SNMP 目标端口配置
 NSX 6.2.0 中已修复此问题。
- 已修复问题 1354728：无法通过 IPFIX 协议处理拒绝/阻止事件
通常，vsfwd 用户流程处理流量收集，包括丢弃/拒绝的流量并为 IPFIX 处理流量。IPFIX 收集器无法查看拒绝/阻止事件时会发生这种情况，原因是 vSIP 丢弃数据包队列过窄或被处于非活动状态的流事件封装。在此版本中，可以使用 IPFIX 协议发送拒绝/阻止事件。NSX 6.2.0 中已修复此问题。

6.2.4 及更低版本中解决的解决方案互操作性相关问题

- 已修复问题 1571170：在包含某些 vRealize 内容包版本的 NSX 6.2 中不支持某些 Log Insight 报告
最新版本的 Log Insight 内容包中已修复此问题。从 [VMware Solution Exchange](#) 下载并安装此内容包。NSX 6.2.3 中已修复此问题。
- 已修复问题 1484506：在 ESXi 升级期间显示紫色诊断屏幕
将支持 NSX 的 vSphere 5.5U2 主机升级到 vSphere 6.0 时，某些 ESXi 主机升级可能会暂停，并显示紫色诊断屏幕。请参见 [VMware 知识库文章 2137826](#)。6.2.3 中已修复此问题。

- 已修复问题 1453802：当路由遍历 NSX 负载均衡器时，无法通过 vCloud Connector 复制虚拟机。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1462006：在 VIO 部署中，一些新部署的虚拟机似乎已分配了有效的端口和 IP，但却没有访问网络的权限。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1482665：通过支持 AD 的 SSO 登录 vSphere Web Client 的 NSX 选项卡时速度缓慢
在使用 SSO 进行 AD 身份验证的 NSX for vSphere 安装中，用户首次登录 vSphere Web Client 的 NSX “网络和安全” 部分时需要较长时间。*NSX 6.1.5 和 NSX 6.2.1 中已修复此问题。*
- 已修复问题 1326669：无法设置组织网络
尝试设置组织范围的网络时，vCloud Director 失败并显示错误消息。*NSX 6.2.0 中已修复此问题。*
- 已修复问题 1497044：无法使用 VIO 设置启动多个虚拟机
使用 VMware Integrated OpenStack 的用户无法在短时间内启动大量虚拟机或发布大量防火墙规则。这将导致日志中显示 Error publishing ip for vnic 消息。*NSX 6.2.0 中已修复此问题。*

文档修订历史

2015 年 8 月 20 日：NSX 6.2.0 第一版。
2015 年 12 月 17 日：NSX 6.2.1 第一版。
2016 年 3 月 4 日：NSX 6.2.2 第一版。可解决 glibc 漏洞的安全修补程序。
2016 年 6 月 9 日：NSX 6.2.3 第一版。
2016 年 8 月 25 日：NSX 6.2.4 第一版。
2016 年 9 月 2 日：NSX 6.2.4 第二版。添加了已知问题。
2016 年 9 月 9 日：NSX 6.2.4 第三版。添加了已知问题。
2016 年 9 月 23 日：NSX 6.2.4 第四版。将两个已知问题移到了“已解决的问题”中。
2016 年 10 月 6 日：NSX 6.2.4 第五版。添加了已知问题。
2016 年 11 月 16 日：NSX 6.2.4 第六版。添加了知识库文章。
2016 年 11 月 28 日：NSX 6.2.4 第六版。更改了错误 1685894。
2017 年 1 月 5 日：NSX 6.2.5 第一版。
2017 年 1 月 10 日：NSX 6.2.5 第二版。添加了已解决的问题。
2017 年 2 月 21 日：NSX 6.2.5 第三版。添加了已知问题 1777792。
2017 年 4 月 14 日：NSX 6.2.5 第四版。添加了已知问题 1833934。
2017 年 4 月 20 日：NSX 6.2.5 第五版。添加了已解决的问题 1663902 和 1717370。
2017 年 6 月 14 日：NSX 6.2.5 第六版。添加了已解决的问题 1770797。
2017 年 8 月 21 日：NSX 6.2.5 第七版。添加了已解决的问题 1685894。