

VMware NSX for vSphere 6.2.0 发行说明

VMware NSX for vSphere 6.2.0 | 2015 年 8 月 20 日 | 内部版本 2986609 | 文档更新日期：2015 年 11 月 22 日

发行说明内容

本发行说明包含以下主题：

- [新增功能](#)
- [系统要求和安装说明](#)
- [升级说明](#)
- [已知问题](#)
- [已解决的问题](#)
- [文档修订历史](#)

新增功能

NSX for vSphere 6.2 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：现可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，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](#)。
- 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，此功能可检测来自 NSX Manager 的配置消息是否未应用到主机便已丢失，并在发生此类消息故障时指示主机重新加载其 NSX 配置。
- 独立 Edge L2 VPN 客户端 CLI：在 NSX 6.2 之前，独立 NSX Edge L2 VPN 客户端只能通过 OVF 参数进行配置。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。OVF 现在仅用于初始配置。

• 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。
- 能够在 VXLAN 上保留 VLAN 标记。
- 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 提供了一个使用 DHCP 侦听或 ARP 侦听发现虚拟机 IP 地址的选项。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 IP 地址的安全规则。

- 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 1.0.2：为支持 NSX 6.2 版本，vRealize Automation (vRA) 中引入了 NSX-vRO 插件 v1.0.2。

系统要求和安装说明

NSX 中基于客户机侦测和网络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 NSX 网络侦测驱动程序组件，请将 VMware Tools 升级到以下版本：

- VMware Tools 5.1 P07 和更高版本
- VMware Tools 5.5 P04 和更高版本
- VMware Tools 6.0

有关 NSX 安装必备条件的完整列表，请参见“NSX 6.2 安装”中的 [NSX 的系统要求](#) 一节。

升级说明

- [VMware 产品互操作性列表](#) 提供有关支持的 VMware NSX 升级途径的详细信息。
- 不支持从 NSX 6.1.5 升级到 NSX 6.2.0。而是必须从 NSX 6.1.5 升级到 NSX 6.2.1 或更高版本。
- 在包含其他 VMware 产品（如 vCenter 和 ESXi）升级的环境中升级 NSX 时，请务必按照此 [知识库文章](#) 中记录的所支持升级顺序进行操作。

- 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。
- 安装和升级 NSX Manager 的内存要求及 CPU 要求已更改。请参见“NSX 6.2 安装”或“NSX 6.2 升级”文档中的[NSX 的系统要求](#)。
- 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。
- 升级到 NSX 6.2.0 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。
- 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。
- 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。（这意味着无论使用的是哪种 NSX 版本，管理员只需知道一个 URL。）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。
- 将 VMware vCloud Network and Security 5.x 升级到 VMware NSX for vSphere 6.2 之前：如果计划从 VMware vCloud Network and Security 5.5.x 升级到 VMware NSX for vSphere 6.2，请运行以下 REST API 调用，验证表中是否缺少上行链路端口名称信息：

```
GET https://<nsxmgr-IP>/api/2.0/vdn/switches
```

在输出中，查找 `uplinkPortName` 字段。例如：

```
<?xml version="1.0" encoding="UTF-8"?>
<vdsContexts>
  <vdsContext>
    <switch>
      <objectId>dvs-22</objectId>
      <objectTypeName>VmwareDistributedVirtualSwitch</objectTypeName>
      <nsxmgrUuid>4236F6CA-3B1A-56BE-4B55-1EF82B8CA12D</nsxmgrUuid>
      <revision>2</revision>
      <type>
        <typeName>VmwareDistributedVirtualSwitch</typeName>
      </type>
      <name>1-vds-20</name>
      <scope>
        <id>datacenter-3</id>
        <objectTypeName>Datacenter</objectTypeName>
```

```
<name>datacenter-1</name>
</scope>
<clientHandle />
<extendedAttributes />
</switch>
<mtu>1600</mtu>
<teaming>FAILOVER_ORDER</teaming>
<uplinkPortName>uplink2</uplinkPortName>
<promiscuousMode>>false</promiscuousMode>
</vdsContext>
</vdsContexts>
```

对于每个 vSphere Distributed Switch，如果此命令的输出包含至少一个上行链路端口名称，则您可以继续执行升级。如果输出中缺少上行链路端口名称，请参见[知识库文章](#)。

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](#)
- [网络连接和 Edge 服务已知问题](#)
- [安全服务已知问题](#)
- [监控服务已知问题](#)

一般已知问题

分布式逻辑路由器出现问题并显示 **Would block** 错误

在主机配置发生更改后，NSX 分布式逻辑路由器可能会出现这个问题。当 vSphere 无法在主机上创建所需的 VDR 端口时就会发生这种情况。此错误可显示为 vmkernel.log 中的 DVPort 连接故障，或客户机中的 SIOCSIFFLAGS 错误。当 vCenter 推送 vSphere Distributed Switch (vDS) 属性后加载 VIB 时可能会发生这种情况。

解决办法：请参见 [VMware 知识库文章 2107951](#)。

使用 IP 发现时，VMware ESXi 5.x 和 6.x 会显示紫色诊断屏幕

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。

解决办法：请参见 <http://kb.vmware.com/kb/2134329> 了解相关说明。

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允许应用到一个或多个 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。

用户必须按顺序下载 NSX Controller 日志

故障排除时可以下载 NSX Controller 日志。由于某个已知问题，您无法同时下载多个控制器的日志。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。

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 将日志文件导出为 CSV 时，您可能会注意到日志文件使用 Epoch 时间（以毫秒为单位）作为时间戳，而不使用基于时区的相应时间作为时间戳。

解决办法：无。

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](#)。

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。

解决办法：无。

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。

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。

在跨 vCenter 的 NSX 部署中，已保存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-1fd96022-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-1fd96022-db14-434d-811d-31912b1cb907</user>
<mode>autosaved</mode>
</firewallDraft>
<firewallDraft id="128" name="AutoSaved_Wednesday, August 5, 2015 9:08:02 PM GMT"
timestamp="1438808882608">
  <description>Auto saved configuration</description>
  <preserve>false</preserve>
  <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
  <mode>autosaved</mode>
</firewallDraft>
<firewallDraft id="127" name="AutoSaved_Wednesday, August 5, 2015 9:08:01 PM GMT"
timestamp="1438808881750">
  <description>Auto saved configuration</description>
  <preserve>false</preserve>
  <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
  <mode>autosaved</mode>
</firewallDraft>
</firewallDrafts>
```

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。

无法打开客户机虚拟机电源

打开客户机虚拟机电源时，可能显示错误消息：**当前未部署所需的所有代理虚拟机** (All required agent virtual machines are not currently deployed)。

解决办法：执行下列步骤：

1. 在 vSphere Web Client 中，单击主页，然后单击系统管理。
2. 在“解决方案”中，选择 vCenter Server 扩展。
3. 单击 vSphere ESX Agent Manager，然后单击管理选项卡。
4. 单击解决。

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。

DVPort 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，DVPort 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 DVPort 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。

解决办法：在 NSX 6.1.4 及更低版本中，要在使用 NSX 逻辑路由器的站点中处理此类 DVPort 故障，必须额外进行一次重新引导。在 NSX 6.2.0 中，NSX 软件提供了一种缓解方法。对于大多数情况，这种缓解方法都可以帮助避免再次重新引导。其根本原因是 vSphere 中的一个已知问题。有关详细信息，请参见 [VMware 知识库文章 2107951](#)。请注意，对于运行 NSX 6.1.x 的客户，此缓解方法也适用于 NSX 6.1.5 及更高版本。

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。如果出现这种情况，请遵循下面的解决办法。

解决办法：重新启动 NSX Manager 设备，然后重新启动 vSphere Web Client。

要重新启动 NSX Manager，请执行以下步骤：

1. 登录到 NSX Manager CLI。
2. 通过键入 `en` 切换到启用/特权模式。
3. 通过键入 `no web-manager` 停止 Web Manager 服务。等待显示“确定”以确认该服务已停止。
4. 通过键入 `web-manager` 启动 NSX Manager。等待显示“确定”以确认 NSX Manager 已重新启动。
5. 要重新启动 vSphere Web Client，请在 vCenter 5.5 中打开 `https://{vcenter-ip}:5480`，然后重新启动 Web Client 服务器。
6. 在 vCenter 6.0 设备中，以 root 用户身份登录到 vCenter Server shell 并运行以下命令：

```
shell.set --enabled True

shell

localhost:~ # cd /bin

localhost:~ # service-control --stop vsphere-client

localhost:~ # service-control --start vsphere-client
```

7. 在 vCenter Server 6.0 中运行以下命令：

```
cd C:\Program Files\VMware\vCenter Server\bin

service-control --stop vsphere-client

service-control --start vsphere-client
```

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。

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。

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 任务窗格中显示的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
```

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。

使用“安装”页面上的“服务部署”选项卡部署的服务虚拟机无法开机

解决办法：按照下面的步骤执行操作。

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

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。

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。

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。

SSL VPN 不向远程客户端发送升级通知

SSL VPN 网关不会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。

将 NSX 从 6.0 版升级到 6.0.x 或 6.1 后，NSX Edge 未列在 UI 中

从 NSX 6.0 升级到 NSX 6.0.x 或 6.1 后，vSphere Web Client 插件可能无法正常升级。这可能会导致 UI 显示问题，如缺少 NSX Edge。

如果从 NSX 6.0.1 或更高版本进行升级，则不会出现此问题。

解决办法：按照下面的步骤执行操作。

1. 在 vCenter MOB 中，单击内容。
2. 在“值”列中，单击 ExtensionManager。
3. 查找 extensionList 属性值(例如 com.vmware.vShieldManager)并复制字符串。
4. 在“方法”区域，单击 UnregisterExtension。
5. 在“值”字段中，粘贴步骤 3 中复制的字符串。
6. 单击调用方法。

这样可以确保部署最新的插件包。

如果在 Edge 上启用 L2 VPN，则 NSX Edge 升级失败

不支持将 L2 VPN 配置从 5.x 或 6.0.x 更新到 6.1。因此，如果已在 Edge 上配置 L2 VPN，Edge 会升级失败。

解决办法：需要先删除 L2 VPN 配置，再升级 NSX Edge。升级后，重新配置 L2 VPN。

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。

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 6.2.0 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。

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”，请执行以下解决办法。

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>
```

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

如果在“取消源/目标”选项启用的情况下复制并粘贴防火墙规则，则会在粘贴操作完成后列出新的防火墙规则，但此时“取消源/目标”选项已禁用。

解决办法：无。

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。

从 vCNS 5.5.4 升级到 NSX 6.2.0 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 6.2.0 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。

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 Distributed Firewall 配置后，UI 和 API 中都无限期保持“正在进行”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”状态并解决此问题，请重新引导 NSX Manager 虚拟设备。

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。

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](#)。

ESXi 升级过程中发生 PSOD

将支持 NSX 的 vSphere 5.5U2 环境升级到 vSphere 6.0 时，部分 ESXi 主机升级可能会暂停，并显示紫色诊断屏幕（也称为 PSOD）。

解决办法：重新引导 ESXi 主机，然后继续升级。

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。

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。

在跨 vCenter 部署中，通用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。

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。

“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。

解决办法：无。

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。

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）。

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。

在 NSX for vSphere 6.2 中进行备份和还原后，vSphere Web Client 不显示“Networking & Security”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。

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。

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 Manager 与客户机侦测之间的通信丢失会导致当虚拟机发生更改（如虚拟机添加、执行 vMotion 或删除）时，NSX 集群中的虚拟机将失去保护。NSX 的“安装”>服务部署选项卡显示客户机侦测的当前版本。存在此问题时，“服务状态”列显示警告。警告消息包括受影响主机的列表和错误消息：**客户机侦测尚未就绪** (Guest Introspection is not ready)。

解决办法：要解决该问题，请按照 [NSX 升级文档](#) 中的过程升级客户机侦测。

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。

NSX Manager 已知问题

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。

这与注册的多个服务/Service Manager 实例和创建的引用这些服务的策略相关。如果在其中一个 Service Manager 关闭的情况下，在服务编排中对此类策略进行更改，由于到已关闭 Service Manager 的回调失败，更改将失败。因此，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。

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。

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://<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>
```

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。

对 NSX Manager 执行 vMotion 操作可能会显示以下错误：“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。

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。

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。

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。

使用 NSX 命令行界面更改密码后，NSX Manager UI 不会自动注销用户

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。

独立 NSX Manager 错误地允许导入通用防火墙配置

通常，在独立角色下运行的 NSX Manager 应该只允许导入本地防火墙规则。从 NSX 6.2 开始，NSX Manager 可以在独立角色（管理一个 vCenter 的网络）或跨 vCenter 模式下运行，这会错误地允许将通用防火墙规则导入到在独立角色下运行的 NSX Manager 环境。导入后，您无法通过 REST API 或 vSphere Web Client 删除通用防火墙规则，因为 NSX Manager 当前正在独立角色下运行，其中通用区域被视为本地区域。

解决办法：如果在独立角色下运行 NSX Manager，请不要导入包含通用规则的防火墙配置。如果已将通用防火墙规则导入独立 NSX Manager，请通过导入已保存的不包含通用规则的防火墙配置文件来修复此问题，并通过将该配置文件加载到防火墙表中来发布该文件。

执行下列步骤：

1. 登录到 vSphere Web Client。
2. 单击网络和安全性，然后单击防火墙。
3. 单击防火墙选项卡。
4. 单击已保存的配置选项卡。

5. 单击导入配置（导入）图标。

6. 单击浏览，然后选择包含要导入的配置的文件。

规则将按照规则名称顺序导入。在导入期间，防火墙将确保环境中存在规则所引用的每个对象。如果未找到某个对象，则会将规则标记为无效。如果规则引用了动态安全组，则导入时会在 NSX Manager 中创建该组。

7. 重新添加节点作为辅助节点。在 NSX Manager 之间进行同步会自动正确地同步通用区域，并执行任何必需的清理。

成功发布配置文件后，规则将推送至主机并影响数据路径。系统会按预期运行。

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。

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。

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。

NSX Edge 和逻辑路由已知问题

当 BGP 邻居筛选器设置为“任意、流出、拒绝”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“任意、流出、拒绝”会导致 DLR 为默认路由播发不正确的下一跃点。此错误仅在为 BGP 邻居筛选器添加了以下属性时发生：

- 方向: 流出
- 操作: 拒绝
- 网络: 任意

解决办法: 无。

在 NSX Edge 上禁用路由协议可能会导致数据流量暂时丢失

如果在 NSX Edge 上禁用路由协议, 则不会向对等设备发送路由撤销请求, 从而使流量在抑制计时器/失效计时器到期之前出现黑洞。

解决办法: 无。

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逻辑路由器连接的接口发现的 OSPF 外部 LSA。

解决办法: 禁用将连接的路由手动重新分发到 OSPF 并在禁用 OSPF 协议之前发布。这可确保路由被正确撤销。

ESG syslog 无法发送到远程服务器并表示它无法解析主机名, 但 DNS 解析程序正在工作

部署 Edge 后, syslog 无法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。此问题首次在 6.2 中出现。

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. 指定与 DNS 转发器设置相同的 DNS 客户端 XML 服务器设置。
2. 启用 DNS 转发器, 并确保转发器设置与 XML 中指定的 DNS 客户端服务器设置相同。

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。

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。

安全服务已知问题

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。

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。

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。

Palo Alto Networks 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 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。

在已升级的 NSX 安装中，发布防火墙规则可能导致 Web Client 中出现空指针异常

在已升级的 NSX 安装中，发布防火墙规则可能导致 UI 中出现空指针异常。将保存规则更改。这只是一个显示问题。

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约束 firewall_section_name_key (Duplicate key value violates
unique constraint firewall_section_name_key)
```

解决办法：执行以下操作之一：

- 加载保存的配置后重命名当前的默认防火墙区域。
- 发布之前，重命名加载的已保存配置上的默认区域。

监控服务已知问题

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

*解决办法：*等待 DLR 部署完成，然后将其他接口添加到分布式逻辑路由器。

已解决的问题

6.2.0 版本中已解决下列问题：

已解决问题分为如下类别：

- [已解决的安装和升级问题](#)
- [已解决的 NSX Manager 问题](#)
- [与逻辑网络连接有关的已解决问题](#)
- [与网络连接和 Edge 服务有关的已解决问题](#)
- [已解决的安全服务问题](#)
- [与监控服务有关的已解决问题](#)
- [与解决方案互操作性有关的已解决问题](#)

与安装和升级有关的已解决问题

- 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。

- 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。

- 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。

- 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。

- 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。

- 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。

- 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。

- 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。

已解决的 NSX Manager 问题

- 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。

- 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。

- 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。

- 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。

与逻辑网络连接有关的已解决问题

- 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。

- 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。

- 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。

- 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。

- 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。

- 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。

- 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。

- 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。

- 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。

- 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。

与网络连接和 Edge 服务有关的已解决问题

- 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。

- 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。

- 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。

- 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。

- 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。

- 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。

- 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。

已解决的安全服务问题

- 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。

- 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。

- 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。

- 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。
尽管出现错误消息，规则仍将成功发布，且会在启用了 Distributed Firewall 的主机上强制使用。

NSX 6.2.0 中已修复此问题。

- 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。

- 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。

- 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。

- 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。

- 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。

- 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。

与监控服务有关的已解决问题

- **#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。

- 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。

- 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。

与解决方案互操作性有关的已解决问题

- 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。

- 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 9 月 4 日：NSX 6.2.0 第二版。移除了不需要的升级警告。

2015 年 11 月 22 日：NSX 6.2.0 第三版。将 [would-block 问题 \(1328589\)](#) 从已解决的问题列表中移到了已知问题列表。在 vSphere 中提供解决办法之前，此问题将保留为已知问题。在 NSX 6.1.5 和 6.2.0 中，NSX 增加了针对此问题的缓解方法。