# VMware NSX-T Data Center 2.3 发行说明

VMware NSX-T Data Center 2.3 | 2018 年 9 月 18 日 | 内部版本 10085361

请定期查看以了解本发行说明的新增内容和更新。

## 发行说明内容

本发行说明包含以下主题：



## 新增功能

**NSX-T Data Center 2.3 是增量升级版本，增强了针对云和容器提供的全新多 Hypervisor 平台。**

**NSX-T Data Center 2.3 版本提供了以下新功能和增强功能。**

针对裸机主机引入 NSX-T Data Center 支持

裸机支持包括裸机服务器上运行的基于 Linux 的工作负载以及无 Hypervisor 的裸机服务器上运行的容器。NSX-T Data Center 利用 Open vSwitch 可使任何 Linux 主机成为 NSX-T Data Center 传输节点。

- **裸机服务器支持：**包括运行 RHEL 7.4、CentOS 7.4 和 Ubuntu 16.0.4 操作系统的本机计算工作负载，以允许用户通过 VLAN（覆盖网络连接）连接裸机计算工作负载，并为虚拟到物理以及物理到物理的通信流量实施微分段策略（有状态第 4 层实施）。
- **裸机 Linux 容器支持：**在具有 RHEL 7.4 或 RHEL 7.5 的裸机 Linux 主机上使用 RedHat OpenShift 容器平台运行 Docker 容器。

NSX Cloud 增强功能

- **支持 AWS 部署：**NSX Cloud 支持 AWS 工作负载。
- **在 Azure VNET 中自动置备 NSX 代理**
- **内部部署到公有云之间的 VPN 支持：**包括使用 API 的 NSX Cloud 公有云网关中的内置 VPN 功能。可以使用 VPN 功能在以下对象之间创建 IPSEC 链接：
  - 受管计算 Amazon VPC/Azure VNet 和传输 Amazon VPC/Azure VNet 中的第三方服务虚拟机
  - 受管 Amazon VPC/Azure VNET 和内部部署 VPN 设备
- **扩展了对 NSX Cloud 代理的操作系统支持：**NSX Cloud 支持公有云中的 RHEL 7.5 操作系统。

安全服务支持

在路由层引入服务插入

- **第 0 层和第 1 层路由器上的服务插入支持：**包括第三方安全解决方案上线，在第 0 层或第 1 层上或同时在两层上部署高可用性第三方安全解决方案以及通过重定向策略插入第三方安全解决方案。
  查看《VMware 兼容性指南》– NSX-T Data Center 上的第三方解决方案的最新认证状态的网络和安全性。

分布式防火墙增强功能

- **NSX Edge 防火墙中的多个区域支持：**在 NSX Edge 防火墙中添加多个区域以便于管理
- **防火墙规则命中计数和规则热门指数：**监控规则使用情况并快速识别未使用的规则以进行清理
- **防火墙区域锁定：**允许多个安全管理员同时对防火墙执行操作
- **分组对象：**如果某个对象与所有五个指定标记（之前是两个标记）匹配，则支持将该对象添加到组
- **标记长度：**将标记长度值从 65 增加到 256 并将标记范围从 20 增加到 128
- **应用程序发现：**发现并分类（用户也可自定义分类）在客户机虚拟机内安装的应用程序。应用程序将包含有关可执行文件、哈希、发布者信息和安装日期的详细信息。

网络和 NSX Edge 服务支持

- **对 N-VDS 增强型数据路径模式的覆盖网络支持：**与 vSphere 6.7 配合使用，NSX-T Data Center 2.3 的 N-VDS 增强型数据路径模式支持需要高性能数据路径的 NFV 样式工作负载。
- **支持集中式服务端口上的有状态 NAT 和防火墙服务**
- **用于清除 DNS 转发器上所有 DNS 条目的 API 支持：**可在单个 API 调用中清除给定 DNS 转发器上所有 DNS 缓存条目。如果 DNS 服务器给出错误答案并希望避免在 DNS 服务器修复后等待 DNS 条目超时，此命令非常有用。
- **负载均衡器增强功能**
  - **支持预定义的密码列表：** HTTPS VIP 的预定义 SSL 配置文件可提高安全性或性能。
  - **负载均衡器规则增强功能：**新建负载均衡器规则、删除标头操作、SSL 匹配条件以及条件匹配时分配变量。
  - **独立服务路由器上的负载均衡器支持：**可在没有路由器端口的服务路由器上部署负载均衡服务。

用户界面增强功能

- **新语言支持：**用户界面现在提供英语、德语、法语、日语、简体中文、韩语、繁体中文和西班牙语版本。
- **增强型导航和主页：**新主页中突出显示搜索和系统摘要一览。
- **增强型搜索：**搜索包含提前键入的建议，可从主页访问这些建议。
- **网络拓扑可视化：**可在 NSX Policy Manager 中监控组到组、虚拟机到虚拟机以及进程到进程的通信。可以可视化网络对象（如逻辑交换机、端口、路由器和 NSX Edge）之间的关系。

操作和故障排除支持

- **安装和升级增强功能**
  - **无状态 vSphere 环境中的 NSX-T Data Center：**通过对使用 vSphere Auto Deploy 和主机配置文件的无状态 ESXi 主机提供支持，启用其他部署选项。功能支持需要 vSphere 6.7 U1 或更高版本。
  - **支持 NSX Edge 虚拟机和裸机共存于同一个 NSX Edge 集群中：**NSX Edge 节点虚拟机和裸机现在可以存在于同一个 NSX Edge 集群中，以便简化 NSX Edge 节点上托管的服务（如负载均衡器）的扩展。
  - **NSX-T Data Center 模块化升级：**包括对升级协调器中的模块化升级的支持。可以仅升级新发行版本中已更改的 NSX-T Data Center 组件。此新增功能可减少修补 NSX-T Data Center 版本的运维开销。
- **监控和故障排除**
  - **用于 KVM Hypervisor 的 ERSPAN：**包括对 KVM – ERSPAN 类型 II 和 III 上端口镜像的支持。
  - **使用往返 Tier-0 逻辑路由器上行链路的流跟踪：**可从 Tier-0 逻辑路由器上行链路生成“流跟踪”流量并报告在 Tier-0 逻辑路由器上行链路上接收流跟踪数据包以简化故障排除操作，从而将 NSX Edge 节点的北向接口包括在流跟踪报告中。
  - **用于关闭裸机 Edge 节点上的 DPDK 端口的 CLI 支持：**可关闭裸机 NSX Edge 节点上 DPDK 声明的端口，以便在安装和故障排除操作期间简化端口隔离。

OpenStack Neutron 插件支持
自 OpenStack Upstream Queens 版本起，支持以下功能。

- **Neutron 插件能够置备增强型数据路径支持的覆盖网络逻辑交换机：**NSX Neutron 插件可利用覆盖网络（以前通常仅使用 VLAN）的增强型数据路径模式。通过此支持，可以利用除 OpenStack 环境（例如，用于 NFV 相关工作负载）以外的增强型数据路径性能。
- **支持 NSX 产品与 OpenStack 共存：**NSX Neutron 插件现在支持同时管理 NSX Data Center for vSphere 和 NSX-T Data Center 以便于 OpenStack 实现。
- **支持使用 OpenStack 中的 VPN 即服务功能：**支持 OpenStack 中引入 VPN 功能集的 Neutron 扩展 OpenStack VPNaaS。

NSX Container Plug-in (NCP) 支持

- 用于安装 NSX-T Data Center 的 Concourse 管道
- **负载均衡器 SNAT IP 注释：**负载均衡器的 SNAT IP 已在类型为 LoadBalancer 的 Kubernetes 服务中注明，`ncp/internal_ip_for_policy: <SNAT IP>`，并添加到服务状态，`status.loadbalancer.ingress.ip: [<SNAT IP>, <Virtual IP>]`。此 IP 可用于创建允许此 IP CIDR 的网络策略。
- **Kubernetes 网络策略增强功能：**可使用 Kubernetes 网络策略规则从不同命名空间中选择 pod。
- Kubernetes 负载均衡器/SNAT 注释改进
  - 如果 NCP 无法为某个服务配置负载均衡器，则该服务将使用 `ncp/error.loadbalancer` 进行注释。
  - 如果 NCP 无法为某个服务配置 SNAT IP，则该服务将使用 `ncp/error.snat` 进行注释。
- 用于 Kubernetes Ingress 和 OpenShift 路由的 NSX-T Date Center 负载均衡器的会话持久性
- 清理脚本增强功能

# 兼容性和系统要求

有关兼容性和系统要求信息，请参阅《NSX-T Data Center 安装指南》。

无状态 vSphere 环境中的 NSX-T Data Center - 对于使用 vSphere Auto Deploy 和主机配置文件的无状态 ESXi 主机，要求使用 vSphere 6.7 U1 或更高版本。

NCP 兼容性要求：

| 产品 | 版本 |
| --- | --- |
| NCP/NSX-T Data Center Tile for PAS | 2.3.0 |
| NSX-T Data Center | 2.2、2.3 |
| Kubernetes | 1.10、1.11 |
| OpenShift | 3.9、3.10 |
| Kubernetes 主机虚拟机操作系统 | Ubuntu 16.04、RHEL 7.4、RHEL 7.5 |
| OpenShift 主机虚拟机操作系统 | RHEL 7.4、RHEL 7.5 |
| PAS (PCF) | OpsManager 2.1.x + PAS 2.1.x（不包括 PAS 2.1.0）<br>OpsManager 2.2.0 + PAS 2.2.0 |

# 常规行为变化

第 1 层逻辑路由器的默认 HA 模式从主动变为非主动

创建第 1 层逻辑路由器时，默认 HA 模式为主动，当首选 NSX Edge 节点重新联机时会导致流量减慢。新的默认 HA 模式设置为非主动后，新创建的第 1 层逻辑路由器不会出现此流量减慢问题。现有的第 1 层逻辑路由器不会受此变化影响。

传输节点到 NSX Controller 的通信更改

由于传输节点到 NSX Controller 的通信发生更改，您现在必须为 NSX-T 2.2 及更高版本打开 TCP 端口 1235。请参见《NSX-T 安装指南》。

从 NSX-T 2.1 升级到更高版本时，必须打开 TCP 端口 1234 和 1235。升级完成后，TCP 端口 1235 正在使用中。

# API 参考信息

请参见已弃用的 NSX-T Data Center 和 NSX 策略 API 调用和属性。

NSX-T Data Canter 产品信息中提供了最新的 API 参考。

# 已解决的问题

已解决的问题分为以下几类。

- 已解决的一般问题
- 已解决的安装问题
- 已解决的 NSX Manager 问题
- 已解决的 NSX Edge 问题
- 已解决的逻辑网络连接问题
- 已解决的安全服务问题
- 已解决的负载均衡器问题
- 已解决的解决方案互操作性问题
- 已解决的运行和监控服务问题
- 已解决的升级问题
- 已解决的 API 问题
- 已解决的 NSX Container Plug-in (NCP) 问题

已解决的一般问题

- 问题 1775315：从 Web 浏览器打开 Postman 客户端后，会发生 CSRF 攻击
  对于使用 Postman、CURL 或其他 REST 客户端执行的 API 调用，您必须明确提供 XSRF TOKEN 标头及其值。使用远程身份验证的第一个 API 调用或 /api/session/create（本地身份验证）调用在响应对象中携带 XSRF-Token。后续 API 调用在请求中携带 XSRF-TOKEN 标头的令牌值。

- 问题 1989412：连接恢复后，未反映 NSX Manager 无法访问时的域删除操作
  如果在 NSX Manager 无法访问时从策略中删除域，则恢复连接到 NSX Manager 后，被删除域的防火墙以及相应规则仍然存在。

- 问题 2018478：尝试从仪表板中移除小组件会导致崩溃，并显示堆栈跟踪错误
  自定义仪表板用户界面更改（例如，从多个小组件中移除一个小组件）会导致用户界面崩溃，并显示堆栈跟踪错误。

- 问题 1959647：如果使用数据库服务器别名创建 DSN，则可能导致 vCenter Server 安装失败
  如果使用数据库服务器别名创建 DSN，则安装使用外部 Microsoft SQL 数据库的 vCenter Server 的操作将失败。安装 Inventory Service 期间出现以下错误：启动 invsvc 期间出现错误 (An error occurred while starting invsvc)。

已解决的安装问题

- 问题 1739120：重新启动管理平面或管理平面中的 Proton 服务后，Fabric 节点的部署状态变得停滞
  使用主机凭据在 Fabric 页面上添加新的受支持主机时，状态更改为**正在进行安装**。在管理平面重新启动管理平面或 Proton 服务后，主机部署状态始终显示**正在进行安装**或**正在进行卸载**。

- 问题 1944669：在 KVM 上部署 NSX-T Data Center 设备时需要指定确切的内存大小
  在 ESX 上部署 NSX-T**Data Center** 设备时，您可以部署具有不同 RAM 配置的小型、中型和大型设备。但是，在 KVM 上部署 NSX-T**Data Center** 设备时，必须明确配置 RAM 分配。

- 问题 1944678：部署 NSX-T Unified Appliance 时需要有效的角色类型
  在 KVM 中部署 NSX-T Unified Appliance 时，如果未指定任何角色或角色类型无效，则部署后的配置将启用所有角色且不受支持。

- 问题 1958308：在主机处于锁定模式时，主机准备或传输节点创建失败
  在主机处于锁定模式时，主机准备或传输节点创建失败。将显示以下错误消息：执**行**该**操作的**权**限被拒**绝 `(Permission to perform this operation was denied)`。

已解决的 NSX Manager 问题

- 问题 1954923：在管理平面升级过程中，通过 vMotion 移动连接到逻辑交换机的虚拟机失败
  在升级管理平面时，如果尝试通过 vMotion 移动连接到逻辑交换机的虚拟机，vMotion 操作将失败。

- 问题 1954927：完成了 NSX Manager 还原，在 NSX Manager 中注册了新的非 VC 管理的 ESX 主机，并将其虚拟机连接到现有的逻辑交换机后，ESX 主机的 MOB 中的虚拟机 MAC 地址将为空白
  完成了 NSX Manager 还原，在 NSX Manager 中注册了新的非 VC 管理的 ESX 主机，并将其虚拟机连接到现有的逻辑交换机后，ESX 主机的 MOB 中的虚拟机 MAC 地址将为空白。

- 问题 1978104：使用 Internet Explorer 11 时，NSX Manager 用户界面中的某些页面不可访问
  在 Windows 计算机上使用 Internet Explorer 时，NSX Manager 用户界面中的仪表板、开始工作流和负载均衡器页面不可访问。

- 问题 1954986：从 UI 中删除许可证密钥后，在日志中显示该密钥
  NSX 许可证密钥显示在 /var/log/syslog 中，如下所示：

  ```
  <182>1 2017-03-24T05:03:47.008Z bb-mgr-221 NSX - SYSTEM [nsx@6876 audit="true"
  comp="nsx-manager" reqId="3d146f2b-fa34-460f-8ac3-56e3c7326015"
  subcomp="manager"] UserName:'admin', ModuleName:'License',
  Operation:'DeleteLicense, Operation status:'success', New value: ["
  <license_key>"] <182>1 2017-03-24T05:03:47.009Z bb-mgr-221 NSX - - [nsx@6876
  audit="true" comp="nsx-manager" subcomp="manager"] UserName:'admin',
  ModuleName:'Batch', Operation:'RegisterBatchRequest, Operation status:'success',
  New value: [{"atomic":false} {"request":
  [{"method":"DELETE","uri":"/v1/licenses/<license_key>"}]}]
  ```

  如果设备配置为将日志发送到外部日志收集器，则外部日志收集器上的任何授权用户都可以看见密钥值。

- 问题 1956055：在管理平面数据存储关闭时，本地管理员用户无法从 UI 中访问技术支持包
  管理平面数据存储不可访问时，本地管理员用户无法从 UI 中访问技术支持包。

- 问题 1957165：加载包含 10,040 条或更多条记录的搜索结果集中的最后一页时导致出错
  在可能为搜索查询返回 10,040 条或更多对象的大型环境中，尝试加载结果集中的最后几条记录时，您可能会看到错误。

已解决的 NSX Edge 问题

- 问题 1762064：如果在重新引导 NSX Edge 后立即配置 NSX Edge VTEP IP 池和上行链路配置文件，将导致 VTEP BFD 会话变得无法访问
  在重新引导 NSX Edge 后，代理需要一些时间以重置 NSX Edge 连接。

已解决的逻辑网络连接问题

- 问题 1966641：添加一个主机并将其配置为传输节点后，如果节点不是逻辑交换机的一部分，则其状态将显示为“关闭”
  添加一个新主机并将其配置为传输节点或配置升级到 NSX-T 2.1 的升级计划时，如果传输节点不是逻辑交换机的一部分，则其在用户界面中显示为“关闭”状态。

- 问题 2015445：活动服务路由器上的防火墙状态可能不会复制到新的活动服务路由器
  租户逻辑路由器 (TLR) 可能有多个从 NSX Edge1 到 NSX Edge2 以及从 NSX Edge2 到 NSX Edge1 的故障切换。防火墙或 NAT 流量状态在活动/备用 TLR 服务路由器之间同步。在非主动故障切换模式下配置 TLR 时，同步在第一次故障切换之前执行，但不会在第一次故障切换和后续故障切换之间执行。因此，第二次故障切换时，TCP 流量可能会超时。在主动模式下配置 TLR 时不会出现此问题。

- 问题 2016629：迁移后，RSPAN_SRC 镜像会话失败
  将连接到为 RSPAN_SRC 镜像会话分配的端口的虚拟机迁移到另一个 Hypervisor ，且目标 Hypervisor 的目标网络上没有所需的 pNic 时，在该端口上配置 RSPAN_SRC 镜像会话将失败。此问题会导致端口连接失败，但 vMotion 迁移过程会成功。

- 问题 1620144：NSX-T Data Center CLI **`get logical-switches`** 会列出具有 UP 状态的逻辑交换机，即使传输节点已被删除也会列出
  该 CLI 可能会让用户误以为存在正常工作的逻辑交换机。即使看到逻辑交换机，它们也不会正常工作。在删除传输节点时，将禁用不透明交换机，因而不会传输任何流量。

- 问题 1590888：需要显示一条警告以指出，在“以太网”部分中选择的逻辑端口仅在同一 L2 网络中适用
  对于分布式防火墙，在“以太网”部分的源/目标部分中输入任何逻辑端口或 MAC 地址时，应该显示一条警告以指出 MAC 地址或逻辑端口应属于同一 L2 网络中的虚拟机端口（连接到同一逻辑交换机）。目前，没有任何警告消息。

- 问题 1763576：允许将 Hypervisor 作为传输节点移除，即使它们在 NSX-T Data Center 网络上具有虚拟机
  NSX-T Data Center 不会禁止删除传输节点，即使该节点上的虚拟机是 NSX-T Data Center 网络的一部分。在删除该传输节点后，将断开连接这些虚拟机。

- 问题 1780798：在大型环境中，某些主机可能会进入故障状态
  在具有 200 个或更多主机节点的大型环境中，在运行一段时间后，某些主机可能会与 NSX Manager 断开连接，并且日志包含如下错误消息：
  ```
  2016-12-09T00:57:58Z mpa: [nsx@6876 comp="nsx-esx" subcomp="mpa" level="WARN"]
  Unknown routing key: com.vmware.nsx.tz.*
  ```

- 问题 1954997：在删除传输节点时，如果传输节点上的虚拟机连接到逻辑交换机，删除将失败
  1. 创建 Fabric 节点和传输节点。
  2. 将 VIF 连接到逻辑交换机。
  3. 删除传输节点而不移除 VIF 到逻辑交换机的连接，删除将失败。
- 问题 1958041：在 ESX Hypervisor 具有多个上行链路时，并且其处于不同的二层物理分段，BUM 流量可能无法跨越三层网络
  如果满足所有以下条件，来自逻辑路由器中的源 Hypervisor 的 BUM 流量无法到达目标 Hypervisor。
  - ESX 具有多个上行链路
  - 源和目标虚拟机通过逻辑路由器进行连接
  - 源和目标 Hypervisor 位于不同的物理分段上

    - 目标逻辑网络使用 MTEP 复制

  出现该问题是因为 BFD 模块可能尚未创建会话，这意味着可能还没有为目标逻辑网络选择 MTEP。

已解决的安全服务问题

- 问题 1520694：在 RHEL 7.1 内核 3.10.0-229 和更早版本中，FTP ALG 无法在数据通道上打开协商的端口
  对于 FTP 会话，如果客户端和服务器位于同一 Hypervisor 上的虚拟机中，FTP 应用程序级别网关 (ALG) 不会为数据通道打开协商的端口。该问题是 Red Hat 特有的，在 RHEL 7.1 内核 3.10.0-229 中存在该问题。不会影响以后的 RHEL 内核。

- 问题 2008882：要确保 Application Discovery 正常工作，请不要创建跨多个主机的安全组
  如果安全组具有跨多个主机的虚拟机，则 Application Discovery 会话可能会失败。

已解决的负载均衡器问题

- 问题 1995228：加权循环和加权最少连接算法配置更改并重新加载后可能无法正确分配流量
  加权循环或加权最少连接配置更改并重新加载后，服务器会断开连接。断开连接后，不会保留历史流量分配信息，导致流量分配不合理。

- 问题 2018629：运行状况检查表不显示 NS 组池的更新监视器类型
  使用一个监视器类型创建具有相同成员的静态和动态 NS 组池并更改动态池中的监视器类型后，动态池运行状况检查不会显示在运行状况检查表中。

- 问题 2020372：达到最大失败计数后，被动运行状况检查不会将池成员标为无法访问
  被动运行状况检查需要比配置计数更高的值才会将池成员标为无法访问。

已解决的解决方案互操作性问题

- 问题：2025624：加载时 Splunk 仪表板停滞或仪表板上的图形为空
  由于 HTML 模板错误地指向查询脚本的以前路径，因此 Splunk 将获取 *nsx_splunk_app* 的旧版本。于是，仪表板将执行旧查询，其中包含 *vmw_nsxt_comp*、*vmw_nsxt_subcomp* 和 *vmw_nsxt_errorcode* 等字段，而这些字段在查询脚本的新版本中以不同的方式命名。由此一来，查询将返回空结果，仪表板将为空。

已解决的运行和监控服务问题

- 问题 1957092：无法初始化 NSX Controller 集群，因为在加载 docker 映像时出错
  `initialize control-cluster` 命令失败并显示错误消息“**控制集群激活超**时。请**重**试 `(Control cluster activation timed out. Please try again)`。”此外，syslog 中还显示以下日志信息：`<30>1 2017-08-03T22:52:41.258925+00:00 localhost load-zookeeper-image 1183 - - grpc: the connection is unavailable.`

已解决的升级问题

- 问题 1847884：管理平面升级过程完成之前，不要进行 NSX-T Data Center 相关更改
  在管理平面升级期间执行任何更改（如创建、更新或删除传输区域、传输节点或逻辑交换机）可能会损坏管理平面，导致 NSX Edge、主机和数据路径连接失败。

- 问题 2005709：使用 NSX Manager FQDN 时，升级协调器页面变为不可访问

使用 NSX Manager FQDN 打开 NSX Manager 用户界面时，升级协调器页面中将显示以下错误消息：此页面仅在运行升级协调器的 NSX Manager 上可用。要启用该服务，请在 NSX Manager 上运行命令“set service install-upgrade enabled”。如果已启用 install-upgrade 服务，请尝试使用“clear service install-upgrade enabled”将其禁用，然后再重新启用 (This page is only available on the NSX Manager where Upgrade Coordinator is running. To enable the service, run the command "set service install-upgrade enabled" on the NSX Manager. If the install-upgrade service is already enabled, try disabling it using "clear service install-upgrade enabled" and then enable it again)。

- 问题 2022609：受管主机在升级协调器中视为非受管主机
  如果环境中的受管主机超过 128 台，则在升级过程中，属于某集群的主机将显示在未受管 ESXi 组中。
- 问题 1944731：如果第二个 NSX Edge 升级期间第一个已升级的 NSX Edge 处理了许多请求，则 DHCP 租约可能会出现冲突记录
  如果第二个 NSX Edge 升级期间第一个已升级的 NSX Edge 处理了许多请求，则 DHCP 租约可能会出现冲突记录。

已解决的 API 问题

- 问题 1619450：轮询频率配置 API **GET /api/v1/hpm/features** 返回垂直测试功能
  GET /api/v1/hpm/features 返回可以配置轮询频率的所有功能的列表。该 API 返回一些内部仅用于测试目的的功能。除了额外的噪声之外，对用户功能没有任何影响。
- 问题 1781225：API **GET https://<NSX-Manager>/api/v1/fabric/nodes/<node-id>/modules** 不适用于 Ubuntu
  API GET https://<NSX-Manager>/api/v1/fabric/nodes/<node-id>/modules 适用于 ESXi 和 RHEL，但不适用于 Ubuntu。
- 问题 1954990：返回不准确的实现 API 状态
  如果使用实现 API 检查在屏障点之前执行的所有 API 的实现状态，实现 API 返回的状态可能具有误导性（相对于实际状态）。由于在管理平面中执行 DFW 非常复杂，DFW API 可能会迟于应遵循的屏障点，从而导致这种不准确性问题。

已解决的 NSX Container Plug-in (NCP) 问题

- 问题 2167491：如果 NSX-T 负载均衡器已达到最大虚拟服务器数，则 NCP 无法启动
  在适用于 NCP 的 ConfigMap 中，您可以将 NSX-T 负载均衡器大小设置为小型、中型或大型。小型负载均衡器的最大虚拟服务器数为 10，中型为 100，大型为 1000。如果负载均衡器已达到最大虚拟服务器数，则 NCP 不会启动。要查看负载均衡器是否已达到最大虚拟服务器数，请从 NSX-T Manager GUI 中找到负载均衡器（具有包含集群名称的标记），并计算虚拟服务器的数量。
- 问题 2160806：不支持在 NCP 未运行时更新活动 Ingress 的 TLS 规范
  如果 NCP 为 Ingress 资源分配了外部 IP，并且在 NCP 未运行时更新了 Ingress 的 TLS 规范，例如，移除或更改参数 secretName，则 NCP 将不会知晓这些更改。当 NCP 再次运行时，与旧密钥对应的证书仍存在且不会被删除。

# 已知问题

已知问题分为以下几类。

- 一般已知问题
- 安装已知问题
- NSX Manager 已知问题
- NSX Edge 已知问题

一般已知问题

- 问题 1842511：不支持静态路由的多跳 BFD
  在 NSX-T 2.0 中，可以为多跳 BGP (MH-BGP) 邻居启用 BFD（双向转发检测）。无法在 NSX-T 2.0 中配置多跳静态路由的 BFD 功能，而只能针对 BGP 配置。请注意，如果配置了支持 BFD 的多跳 BGP 邻居，然后为相应多跳静态路由配置与 BGP 邻居相同的下一跃点，BFD 会话状态影响 BGP 会话以及静态路由。

  解决办法：无。

- 问题 1931707：自动 TN 功能要求集群中的所有主机具有相同的 pnic 设置
  在为集群启用自动 TN 功能时，将创建一个传输节点模板以应用于该集群中的所有主机。该模板中的所有 pnic 必须在 TN 配置的所有主机上可用，否则，TN 配置可能会在缺少或已占用 pnic 的那些主机上失败。

  解决办法：如果 TN 配置失败，请重新配置各个传输节点以进行纠正。

- 问题 1909703：允许 NSX 管理员直接从后端在 OpenStack 创建的路由器中创建新的静态路由、NAT 规则和端口
  作为 NSX-T 2.0 中的 RBAC 功能的一部分，NSX 管理员无法直接从 NSX UI/API 中删除或修改 OpenStack 插件创建的资源（如交换机、路由器和安全组）。只能使用通过 OpenStack 插件发送的 API 修改/删除这些资源。该功能存在一些限制。目前，仅阻止 NSX 管理员删除/修改 OpenStack 创建的资源，但允许管理员在 OpenStack 创建的现有资源中创建新的资源（如静态路由和 NAT 规则）。

  解决办法：无。

- 问题 1957072：对于多个上行链路，网桥节点的上行链路配置文件应始终使用 LAG
  在使用多个未组成 LAG 的上行链路时，不会对流量进行负载均衡并且可能无法正常工作。

  解决办法：对于网桥节点上的多个上行链路，请使用 LAG。

- 问题 1970750：使用具有快速定时器的 LACP 的传输节点 N-VDS 配置文件不适用于 vSphere ESXi 主机
  配置速率较快的 LACP 上行链路配置文件并将其应用于 NSX Manager 上的 vSphere ESXi 传输节点时，NSX Manager 显示配置文件已成功应用，但 vSphere ESXi 主机仍使用默认的 LACP 慢速计时器。

  在 vSphere Hypervisor 中，当 NSX Manager 的传输节点上使用 LACP NSX 受管分布式交换机 (N-VDS) 配置文件时，无法查看 lacp-timeout 值 (SLOW/FAST) 的影响。

  解决办法：无。

- 问题 1989407：具有企业管理员角色的 vIDM 用户无法覆盖对象保护
  具有企业管理员角色的 vIDM 用户无法覆盖对象保护且无法创建或删除主体身份。

  解决办法：使用管理员特权登录。

- 问题 2030784：无法使用包含非 ASCII 字符的远程用户名登录到 NSX Manager。
  无法以用户名中包含非 ASCII 字符的远程用户身份登录到 NSX Manager 设备。

  解决办法：登录到 NSX Manager 设备时，远程用户名应包含 ASCII 字符。
  如果在 Active Directory 服务器中使用非 ASCII 字符设置远程用户名，则可以使用非 ASCII 字符。

- 问题 2111047：NSX-T 2.2 版本不支持在 VMware vSphere 6.7 主机上使用 Application Discovery 功能
  如果安全组包含运行在 vSphere 6.7 主机上的虚拟机，则在此安全组上运行 Application Discovery 会导致发现会话失败。

  解决办法：无

- 问题 2157370：配置 L3 交换端口分析器 (SPAN) 截断时，特定物理交换机会丢弃镜像数据包
  配置包括 GRE/ERSPAN 的 L3 SPAN 截断时，会因物理交换机策略而丢弃截断的镜像数据包。可能的原因是端口正在接收的数据包的负载字节数与类型长度字段不符。

  解决办法：移除 L3 SPAN 截断配置。

- 问题 216992：vSphere ESXi 上行链路会丢弃其他主机中目标 MAC 地址为 02:50:56:56:44:52 的镜像数据包
  当主机从其他主机接收目标 MAC 地址为 02:50:56:56:44:52 的镜像数据包时，vSphere ESXi 上行链路会丢弃这些镜像数据包。

  解决办法：无

- 问题 2174583：在“快速入门”向导中，“设置传输节点”按钮在 Microsoft Edge 浏览器上无法正常工作
  在“快速入门”向导中，单击**设置传输节点**按钮后，Microsoft Edge Web 浏览器显示 JavaScript 错误。

  解决办法：改为使用 Firefox 或 Google Chrome 浏览器。

安装已知问题

- 问题 1617459：Ubuntu 的主机配置不支持获取接口配置文件
  如果 pnic 接口没有位于 /etc/network/interfaces 文件中，则不会在网络配置文件中正确配置 MTU。因此，在每次重新引导后，传输网桥上的 MTU 配置将会丢失。

  解决办法：将 pnic 接口配置移到 /etc/network/interfaces 中。

- 问题 1906410：尝试从 UI 删除主机时未首先删除传输节点，导致主机进入不一致状态
  尝试从 UI 删除主机时未首先删除传输节点，导致主机进入不一致状态。如果尝试删除传输节点时主机处于不一致状态，UI 将不允许删除此主机。

  解决办法：

  1. 删除传输节点之前，关闭此传输节点上部署的所有租户虚拟机的电源。
  2. 从传输节点中移除传输区域。
  3. 删除传输节点。
  4. 成功删除传输节点后，删除相应的主机。

  如果传输节点删除失败，请完成知识库文章 https://kb.vmware.com/s/article/52068 中的步骤。

- 问题 1957059：如果在尝试取消准备时将当前具有 vib 的主机添加到集群，主机取消准备将失败
  如果在将主机添加到集群之前未完全移除 vib，主机取消准备操作将失败。

  解决办法：确保完全移除主机上的 vib 并重新启动主机。

- 问题 2106956：将同一集群的两个 NSX Controller 加入到两个不同的 NSX Manager 会导致出现未定

义的数据路径问题
将同一 NSX Controller 集群的两个 NSX Controller 加入到两个不同的 NSX Manager 会导致出现未定义的数据路径问题。

解决办法：在 NSX Manager 上使用 detach CLI 命令从 NSX Controller 集群中移除 NSX Controller。重新配置 NSX Controller 集群，以便集群中的所有 NSX Controller 都在同一个 NSX Manager 中注册。

请参见《NSX-TData Center安装指南》中的“NSX Controller 安装和建立集群”部分。

- 问题 2106973：在所有 NSX Controller 上初始化 NSX Controller 集群会导致每个 NSX Controller 成为单节点 NSX Controller 集群，从而导致出现未定义的数据路径连接问题
  避免在所有 NSX Controller 上初始化 NSX Controller 集群，因为这样做会导致每个 NSX Controller 成为单节点 NSX Controller 集群，从而导致出现未定义的数据路径连接问题。仅在第一个 NSX Controller 上初始化 NSX Controller 集群，然后在第一个 NSX Controller 上运行 `join control-cluster` CLI 命令将其他 NSX 控制器加入集群。

  解决办法：重新配置 NSX Controller 集群，如《NSX-TData Center安装指南》中的“NSX Controller 安装和建立集群”部分。

- 问题 2114756：在某些情况下，从 NSX-T Data Center 就绪集群中移除主机时不会移除 VIB
  从 NSX-TData Center就绪集群中移除主机时，某些 VIB 可能会保留在主机上。

  解决办法：从主机中手动卸载 VIB。

- 问题 2059414：由于 python-gevent RPM 版本较旧，RHEL LCP 包安装失败
  RHEL 主机包含较新版本的 python-gevent RPM 时，RHEL LCP 包安装会失败，因为 NSX-T Data Center RPM 包含较旧版本的 python-gevent RPM。

  解决办法：如果主机包含最新版本的 python-gevent RPM，请在 RHEL 主机上手动安装 LCP 包。

  完成以下步骤：

  1. 提取 RHEL LCP 包。
  2. 导航到 LCP 包文件夹。
  3. 从 LCP 文件夹中删除 libev、python-greenlet 和 python-gevent RPM。
  4. 安装其余的 RPM。请参见《NSX-T Data Center 安装指南》。
- 问题 2142755：OVS 内核模块安装失败，具体取决于正在运行哪些次要 RHEL 7.4 内核版本
  OVS 内核模块在运行次要内核版本 17.1 或更高版本的 RHEL 7.4 主机上安装失败。安装失败会导致内核数据路径停止工作，从而导致设备管理控制台变得不可用。

  解决办法：升级 RHEL 7.4 内核版本。使用管理员特权在主机上运行脚本 `/usr/share/openvswitch/scripts/ovs-kmod-manage.sh` 并重新加载 OVS 内核模块。

NSX Manager 已知问题

- 问题 1950583：在系统升级到 NSX-T 2.0.0 后，NSX Manager 计划备份可能会失败
  从以前版本的 NSX-T 升级到 2.0.0 后，某些 NSX-T 环境无法执行计划备份。 该问题是由于 SSH 指纹格式与以前版本不同所致。

  解决办法：重新配置计划备份。

- 问题 1576112：如果 KVM Hypervisor 位于不同的第 2 层分段中，则它们需要手动配置网关
  如果在 NSX Manager 上配置一个 IP 池并使用该 IP 池创建传输节点，则 Ubuntu KVM 框不会显示在 IP 池配置中配置的网关的路由。因此，位于不同 L2 分段中的 Hypervisor 上的虚拟机之间的覆盖流量将失败，因为底层结构层主机不知道如何访问远程分段中的结构层节点。

  解决办法：为网关添加一个路由，以便它可以将流量路由到位于不同分段中的其他 Hypervisor。如果该配置不是手动完成的，覆盖流量将失败，因为结构层节点不知道如何访问远程结构层节点。

- 问题 1710152：在兼容性模式下，NSX Manager GUI 在 Internet Explorer 11 上无法正常工作

  解决办法：转到**工具 > 兼容性视图设置**，并验证 Internet Explorer 是否在兼容性模式下不显示 NSX Manager GUI。

- 问题 2128476：对包含 500 多个主机、1000 多个虚拟机和 10000 多个 VIF 的清单执行大规模设置时，硬性重新引导后可能需要约 30 分钟才能完成完全同步
  重新引导 NSX Manager 后，每个主机都会与 NSX Manager 同步，以便 NSX Manager 接收主机上的最新数据，其中包括有关主机上的虚拟机以及虚拟机上的 VIF 的信息。对包含 500 多个主机、1000 多个虚拟机和 10000 多个 VIF 的清单执行大规模设置时，完全同步需要大约 30 分钟的时间才能完成。

  解决办法：硬性重新引导后，等待 NSX Manager 中显示最新信息。

  使用 API `api/v1/fabric/nodes/<nodeid>/status` 检查 last_sync_time 属性，该属性指明了特定节点的最新同步时间。

- 问题 1928376：在还原 NSX Manager 后，控制器集群成员节点处于性能下降状态
  如果将 NSX Manager 还原为在将控制器集群成员节点从集群中分离之前创建的备份映像，该成员节点可能会变得不稳定并报告性能下降运行状况。

  解决办法：如果集群成员发生变化，请确保创建新的 NSX Manager 备份。

- 问题 1956088：在防火墙 UI 视图中的规则集应用筛选时，如果在保存到 Manager 之前取消了筛选器，对该视图的更改可能会丢失
  在防火墙 UI 视图中的规则集应用筛选时，如果在保存到 Manager 之前取消了筛选器，对该视图的更改可能会丢失

  解决办法：无。

- 问题 1928447：在管理平面节点 syslog 中未记录具有重复虚拟隧道端点 IP 地址的 Hypervisor
  在管理平面节点 syslog 中未记录具有重复虚拟隧道端点 IP 地址的 Hypervisor。确保为 Hypervisor 的虚拟隧道端点和 NSX Edge 节点的上行链路接口分配唯一的 IP 地址。

  解决办法： 无。

- 问题 2125725：还原大型拓扑部署后，搜索数据变得不同步且多个 NSX Manager 页面无响应
  还原具有大型拓扑部署的 NSX Manager 时，搜索数据变得不同步且多个 NSX Manager 页面显示错误消息“发**生不可恢复的**错误 `(An unrecoverable error has occurred)`”。

  解决办法：完成以下步骤：

  1. 以管理员身份登录到 NSX Manager CLI。
  2. 重新启动搜索服务。
     `restart service search`
     至少等待 15 分钟，以便搜索服务在后台完成数据差异修复。

- 问题 2128361：用于将 NSX Manager 日志级别设置为调试模式的 CLI 命令不能正常工作
  使用 CLI 命令 `set service manager logging-level debug` 将 NSX Manager 的日志级别设置为调试模式时，不会收集调试日志信息。

解决办法：完成以下步骤：

1. 以管理员身份登录到 NSX Manager CLI。
2. 运行命令 `st e` 以切换为 root 用户。
3. 复制 log4j2.xml.default 和 log4j2.xml 文件。
   `cp /opt/vmware/proton-tomcat/conf/log4j2.xml.default /opt/vmware/proton-tomcat/conf/log4j2.xml`
4. 更改 log4j2.xml 文件的所有权。
   `chown uproton:uproton /opt/vmware/proton-tomcat/conf/log4j2.xml`

- 问题 1964681：即使已删除主机，Manager UI 中的“主机”选项卡仍会显示传输节点主机的状态为“正在删除”
  在 Manager UI 的“Fabric”>“节点”>“传输节点”选项卡中，成功删除传输节点主机后，“主机”选项卡仍会将主机的状态显示为“正在删除”。

  解决办法：刷新浏览器。

- 问题 2169998：使用 Chrome 浏览器登录到 NSX Manger 后清除浏览数据会导致 Manager UI 停止工作
  使用 Chrome 浏览器登录到 NSX Manager 后，如果转到浏览器设置并清除所有浏览数据（包括所有基本数据和高级数据），该浏览器将丢失与 NSX Manager 的连接。

  解决办法：登录到 NSX Manager 后不要清除浏览数据。

NSX Edge 已知问题

- 问题 1765087：NSX Edge 创建的内核接口（用于将数据包从数据路径传输到 Linux 内核）最多仅支持 1600 的 MTU
  数据路径和内核之间的内核接口不支持巨型帧。BGP 守护进程将截断和丢弃大小超过 1600 的 BGP 数据包。将截断大小超过 1600 的 SPAN 数据包，并且数据包捕获实用程序显示一条警告。不会截断负载，负载仍保持有效。

  解决办法：无。

- 问题 1738960：如果将 DHCP 服务器配置文件 NSX Edge 节点替换为另一个集群中的 NSX Edge 节点，DHCP 服务器为虚拟机分配的 IP 地址将发生变化
  该问题是由替换的节点和新节点之间缺少协调造成的。

  解决办法：无。

- 问题 1629542：在单个 NSX Edge 节点上设置转发延迟将导致显示不正确的路由状态
  在将 NSX Edge 作为单个 NSX Edge 节点（不在 HA 对中）运行时，配置转发延迟可能会导致错误地报告路由状态。在配置转发延迟后，路由状态错误地显示为 DOWN，直到转发定时器到期。如果路由器聚合已完成，但转发延迟定时器尚未到期，则从南到北的数据路径继续按预期方式传输数据，即使路由状态报告为 DOWN。您可以安全地忽略该警告。

- 问题 1601425：无法克隆已在 NSX Manager 集群中注册的 NSX Edge 虚拟机
  在 NSX Manager 集群中注册 NSX Edge 虚拟机后，不支持克隆该虚拟机，应部署全新的映像。

  解决办法：无。

- 问题 1585575：无法编辑连接到第 0 层路由器的第 1 层路由器上的 NSX Edge 集群详细信息
  如果已在第 1 层逻辑路由器上启用 NAT，必须先指定一个 NSX Edge 节点或 NSX Edge 集群，然后再将第 1 层路由器连接到第 0 层路由器。NSX 不支持编辑已连接到第 0 层路由器的第 1 层路由器上的 NSX Edge 集群详细信息。

  解决办法：要编辑已连接到第 0 层路由器的第 1 层路由器上的 NSX Edge 集群详细信息，请将第 1 层路由器与第 0 层路由器断开连接，进行更改，然后重新连接。

- 问题 1955830：在 NSX Edge 集群名称包含高位或非 ASCII 字符时，从 NSX-T 1.1 升级到 NSX-T 2.0 失败
  如果在 NSX-T 1.1 设置中使用高位或非 ASCII 字符命名 NSX Edge 集群，从 NSX-T 1.1 升级到 NSX-T 2.0 将失败并出现无限循环错误。

  解决办法：在升级之前，在 NSX-T 1.1 设置实例上重命名 NSX Edge 集群以移除高位或非 ASCII 字符。

- 问题 2122332：在某些情况下，无法通过 SSH 登录到裸机 Edge
  有些情况下，无法通过 SSH 登录到裸机 Edge。

  解决办法：打开命令提示符并导航到 iLO 驱动程序。重新启动 Edge SSH 服务。

- 问题 2187888：从 NSX Manager 用户界面自动部署的 NSX Edge 始终保持“注册挂起”状态
  从 NSX Manager 用户界面自动部署的 NSX Edge 始终保持“注册挂起”状态。此状态会导致 NSX Edge 无法进行进一步配置。

  解决办法：使用 CLI 向 NSX Manager 手动注册 NSX Edge。

逻辑网络已知问题

- 问题 1769922：NSX Controller 集群层面可能在 vSphere Client 上显示内部 IP 地址 172.17.0.1，而不是实际 IP 地址
  在 vSphere Client 上，NSX Controller 的 IP 地址错误地显示为 172.17.0.1 而不是实际 IP 地址。对于 NSX Manager，将正确显示 IP 地址。

  解决办法：不需要采取任何措施。这种表面问题不会影响任何功能。

- 问题 1771626：不支持更改 NSX Controller 节点的 IP 地址

  解决办法：重新部署 NSX Controller 集群。

- 问题 1940046：在多个 Tier-1 逻辑路由器上添加和通告相同的静态路由时，东西向流量会失败
  如果在多个 Tier-1 逻辑路由器上添加和通告相同的静态路由，则东西向流量会失败。

  解决办法：如果前缀在第 1 层分布式路由器的已连接网络后面，应仅从原始第 1 层逻辑路由器通告静态路由。

- 问题 1753468：在桥接的 VLAN 上启用生成树协议 (STP) 将导致网桥集群状态显示为关闭
  如果在用于与 LACP 绑定桥接的 VLAN 上启用 STP，将阻止物理交换机端口通道，从而导致 ESX 主机上的网桥集群显示为关闭。

  解决办法：禁用 STP 或启用 BPDU 筛选器和 BPDU 防护。

- 问题 1753468：第 0 层逻辑路由器不聚合路由，而是单独重新分发这些路由
  如果某个前缀未涵盖连接到它的所有子前缀，则第 0 层逻辑路由器不会为该前缀执行路由聚合，而是单独分发这些路由。

  解决办法：无。

- 问题 1536251：不支持将虚拟机从一个 ESX 主机复制到连接到同一逻辑交换机的另一个 ESX 主机
  如果从一个 ESX 主机中复制虚拟机并在另一个 ESX 主机上注册了同一虚拟机，第 2 层网络将失败。

  解决办法：如果 ESX 主机是 Virtual Center 的一部分，请使用虚拟机克隆。
  如果要在 ESX 主机之间复制虚拟机，外部 ID 在虚拟机 .vmx 文件中必须是唯一的，第 2 层网络才能正常工作。

- 问题 1747485：从 LAG 接口中移除任何上行链路将导致所有 BFD 协议关闭并且 BGP 路由出现抖动
  从配置的 LAG 接口中删除任何接口时，将导致所有 BFD 协议关闭并且 BGP 路由出现抖动，从而影响流量流。

  解决办法：无。

- 问题 1741929：在 KVM 环境中，如果配置了端口镜像并启用了截断，将以分段形式发送来自源的巨型数据包，但在镜像目标中重新组合这些数据包

  解决办法：不需要任何解决办法，因为重新组合是由目标虚拟机 vNIC 驱动程序执行的。

- 问题 1619838：将逻辑路由器的传输区域连接更改为一组不同的逻辑交换机失败，并显示不匹配错误
  对于下行链路端口，逻辑路由器仅支持单个覆盖传输区域。因此，在未删除现有的下行链路或路由器链路端口的情况下，无法将传输区域连接更改为一组不同的逻辑交换机。

  解决办法：完成以下步骤。

  1. 删除所有现有的下行链路或路由器链路端口。
  2. 等待一段时间以使系统进行更新。
  3. 再次尝试将传输区域连接更改为一组不同的逻辑交换机。

- 问题 1625360：在创建逻辑交换机后，NSX Controller 可能不会显示新创建的逻辑交换机信息

  解决办法：在创建逻辑交换机后，等待 60 秒以检查 NSX Controller 上的逻辑交换机信息。

- 问题 1581649：在创建和删除逻辑交换机后，无法缩减 VNI 池范围
  范围缩减失败，因为在删除逻辑交换机后不会立即释放 VNI。将在 6 小时后释放 VNI。这是为了防止在创建另一个逻辑交换机时重新使用 VNI。因此，在删除逻辑交换机后，您在 6 小时内无法缩减或修改范围。

  解决办法：要修改从中为逻辑交换机分配 VNI 的范围，请在删除逻辑交换机后等待 6 小时。也可以使用 VNI 池中的其他范围，或者重新使用相同的范围而不缩减或删除该范围。

- 问题 1516253：Intel 82599 网卡对队列接收的字节数计数器 (QBRC) 具有硬件限制，从而导致在收到的总字节数超过 0xFFFFFFFFF 后发生溢出
  由于硬件限制，`get dataplane physical-port stats` 的 CLI 输出与发生溢出时的实际数字不匹配。

  解决办法：运行一次 CLI 以重置该计数器，然后在较短的时间内再次运行该 CLI。

- 问题 2075246：不支持在第 0 层逻辑路由器之间移动第 1 层逻辑路由器。
  在第 0 层逻辑路由器之间移动第 1 层逻辑路由器会导致第 1 层逻辑路由器断开下行链路端口路由连接。

  解决办法：完成以下步骤：

1. 断开第 0 层逻辑路由器与第 1 层逻辑路由器的连接。
2. 等待大约 20 分钟，以便第 1 层逻辑路由器完全与第 0 层逻辑路由器断开连接。
3. 将第 1 层逻辑路由器连接到另一个第 0 层逻辑路由器。
   下行链路端口路由连接恢复。

- 问题 2077145：在某些情况下，尝试强制删除传输节点可能会导致出现孤立的传输节点
  在某些情况下（例如，存在硬件故障、主机变得无法检索），尝试使用 API 调用强制删除传输节点时，传输节点状态会变为“孤立”。

  解决办法：删除包含孤立传输节点的 Fabric 节点。

- 问题 2099530：更改网桥节点的 VTEP IP 地址会导致流量中断
  更改网桥节点的 VTEP IP 地址时，VLAN 到覆盖网络的 MAC 表在远程 Hypervisor 上不会更新，从而导致流量中断长达 10 分钟。

  解决办法：从 VLAN 进行流量更改，确保 Hypervisor 上的覆盖网络 MAC 表会刷新。

- 问题 2106176：NSX Controller 自动安装过程在“等待注册”安装步骤停滞
  使用 NSX Manager API 或 UI 自动安装 NSX Controller 期间，一个正在进行的 NSX Controller 的状态停滞，一直显示**等待注册**。

  解决办法：完成以下步骤：

  1. 发送 API 请求以查找与已停滞 NSX Controller 关联的虚拟机 ID。

     ```
     https://<nsx-mgr>/api/v1/cluster/nodes/deployments
     ```

  2. 发送 API 请求以删除已停滞 NSX Controller。

     ```
     https://<nsx-mgr>/api/v1/cluster/nodes/deployments/<Controller id>?action=delete
     ```

- 问题 2112459：替换网桥集群中的单个节点导致流量丢失
  替换网桥集群中的单个节点时，桥接流量流向旧节点，这会导致流量丢失，直到远程 Hypervisor 中的转发条目更新或过期后才恢复正常。

  解决办法：完成以下步骤：

  1. 将替换节点置于网桥集群中。
  2. 允许建立 HA。
  3. 移除旧节点。

- 问题 216992：使用自定义逻辑端口 MTU 设置可能会导致丢包
  在逻辑端口（例如，逻辑路由器上行链路端口）上使用自定义 MTU 设置时，不合规的值或第 0 层和第 1 层逻辑路由器的某些配置可能会导致丢包。默认 MTU 设置为 1500。

  解决办法：使用默认 MTU 设置。

  否则，在不同逻辑端口上应用的 MTU 必须符合以下关系：

  1. 将第 0 层逻辑路由器上行链路 MTU 设置为 8900。
  2. 将 NSX Edge VTEP MTU 设置为 9000。
  3. 将虚拟机 MTU 设置为 8900。

  第 0 层逻辑路由器以及连接到第 0 层逻辑路由器的所有第 1 层逻辑路由器必须分配到相同的 NSX Edge 节点上。

- 问题 2125514：第 2 层网桥故障切换后，某些 NSX Edge 虚拟机上的逻辑交换机可能会对每个数据包执行 BUM 复制，直到重新学习 MAC 为止

第 2 层网桥故障切换后，某些 NSX Edge 虚拟机上的逻辑交换机可能会对每个数据包执行 BUM 复制，持续时间约为 10 分钟，直到重新学习端点的 MAC 为止。端点生成下一个 ARP 后，系统恢复正常。

解决办法：无

- 问题 2113769：NSX Edge VLAN 第 2 层桥接不支持 DHCP 中继
  通过 NSX Edge 上的第 2 层桥接端口将 VLAN 主机连接到逻辑交换机 VNI 会导致逻辑路由器端口上的 DHCP 中继代理不向该 VLAN 主机提供 IP 地址。

  解决办法：完成以下步骤：

  1. 手动配置 VLAN 主机。
  2. 将第 2 层桥接端口移至 ESXi 主机。
- 问题 2183549：编辑集中式服务端口时，无法查看新创建的 VLAN 逻辑交换机
  在 Manager UI 中，创建集中式服务端口和新的 VLAN 逻辑交换机后，编辑集中式服务端口时无法查看新创建的 VLAN 逻辑交换机。

  解决办法：使用 API 编辑端口。

- 问题 2160634：更改环回的 IP 地址可以更改上行链路上路由器 ID 的 IP 地址
  如果更改了环回的 IP 地址，则 NSX Edge 会选择上行链路的 IP 地址作为路由器 ID。分配为路由器 ID 的上行链路 IP 地址无法更改。

  *对客户的影响*：1.路由器 ID 的预期负面影响是所有 BGP 会话都会出现抖动。
  2.实际影响是路由器 ID 的变更，这样会使调试 BGP 变得更加困难，并且可能会导致混淆。

  解决办法：禁用 BGP 配置并更改环回的 IP 地址。

- 问题 2186040：如果传输节点不在系统的前 250 个上行链路配置文件中，则将在用户界面中禁用物理网卡的上行链路下拉菜单
  如果传输节点不在系统的前 250 个上行链路配置文件中，则将在用户界面中禁用物理网卡的上行链路下拉菜单。保存传输节点会导致从传输节点中移除上行链路名称。

  解决办法：重新选择该传输节点的上行链路配置文件和上行链路名称。

- 问题 2106635：在静态路由创建期间，更改 NULL 路由的管理距离会导致下一跃点 NULL 设置从用户界面中消失
  在静态路由创建期间，如果将下一跃点设置为 NULL，则更改 NULL 路由的管理距离时，下一跃点 NULL 设置将从用户界面中消失。

  解决办法：重新选择下一跃点。

安全服务已知问题

- 问题 1680128：未加密客户端和服务器之间的 DHCP 通信

  解决办法：使用 IPSEC 提高通信的安全性。

- 问题 1711221：通过网络以明文形式发送 IPFIX 数据
  默认情况下，将禁用收集 IPFIX 流量的选项。

  解决办法：无。

- 问题 1726081：在 KVM 中拒绝 Geneve 隧道流量 (UDP)

  解决办法：完成以下步骤：
  如果 KVM 使用 firewalld，请使用以下命令在防火墙中打开一个缺口：
  ```
  # firewall-cmd --zone=public --permanent --add-port=6081/udp
  ```
  如果 KVM 直接使用 IPtables，请使用以下命令打开一个缺口：
  ```
  # iptables -A INPUT -p udp --dport 6081 -j ACCEPT
  ```
  如果 KVM 使用 UFW，请使用以下命令打开一个缺口：
  ```
  # ufw allow 6081/udp
  ```

- 在客户端位于不同的网络并且由客户机虚拟机提供路由服务时，DHCP 释放和更新数据包无法到达 DHCP 服务器
  NSX-T 无法识别虚拟机是否用作路由器，因此，可能会丢弃使用路由器虚拟机路由的单播 DHCP 数据包，因为数据包中的 CHADDR 字段与源 MAC 不匹配。CHADDR 具有 DHCP 客户端虚拟机的 MAC，而源 MAC 是路由器接口的 MAC。

  解决办法：如果虚拟机起到类似于路由器的作用，请在应用于路由器虚拟机的所有 VIF 的交换机安全配置文件中禁用 DHCP 服务器阻止。

- 问题 2108290：作为传输节点的裸机服务器不能保证 NSX-T Data Center 安全功能
  裸机服务器作为一种新型传输节点不能提供与其他 Hypervisor 工作负载相同级别的安全保证，例如微分段。这是因为，应用程序工作负载和 NSX 代理之间不会强制实施可靠的信任边界。

  解决办法：为了安全起见，请勿为租户虚拟机分配裸机服务器的根特权或以 root 用户身份运行应用程序。如果租户虚拟机具有此类访问权限，则受影响的租户帐户或应用程序可能会对裸机服务器执行恶意活动，并在 NSX-T Data Center 网络中引发问题。

- 问题 2162722：热度指数不适用于 DROP 或 REJECT 规则以及无状态规则
  通信遇到具有 DROP/REJECT 操作的规则或无状态规则时，规则的会话计数不会递增，因为“会话”仅适用于有状态 ALLOW 规则。热度指数将会话计数用作关键参数，因此不会因此类规则而更改。

  解决办法：无

- 问题 2170512：如果界面中的规则超过 1,000 个，则用于获取防火墙规则的 CLI 命令将失败
  如果界面中的规则超过 1,000 个，则 CLI 命令 `get firewall <VIF_ID> ruleset rules` 将返回空字符串。

  解决办法：有下面两种解决方法：

  - 改为运行“nsxcli -c get firewall <VIF_ID> ruleset rules | json”。
  - 运行以下原始 CLI 命令：将显示包含结果的文件的名称。
    ```
    ovs-appctl -t /var/run/vmware/nsx-agent/nsxa-ctl dfw/rules
    ```

KVM 网络连接已知问题

- 问题 1775916：在无法将 KVM 主机添加到结构层后，解决方案 API **`POST /api/v1/error-resolver?action=resolve_error`** 没有解决这些错误
  在无法将 RHEL KVM 主机添加到结构层并且 NSX Manager 用户界面显示失败安装状态后，将运行解决方案 API `POST /api/v1/error-resolver?action=resolve_error` 以解决这些错误。不过，再次将该主机添加到结构层将显示以下错误消息：
  **无法在主机上安装**软**件。**`Un-handled deployment plug-in perform-action. Install command failed.`

  解决办法：完成以下步骤。

  1. 手动移除以下软件包。
     ```
     rpm -e glog-0.3.1-1nn5.x86_64
     rpm -e json_spirit-v4.06-1.el6.x86_64
     rpm -e kmod-openvswitch-2.6.0.4557686-1.el7.x86_64
     rpm -e nicira-ovs-hypervisor-node-2.6.0.4557686-1.x86_64
     rpm -e nsx-agent-1.1.0.0.0.4690847-1.el7.x86_64
     rpm -e nsx-aggservice-1.1.0.0.0.4690845-1.el7.x86_64
     rpm -e nsx-cli-1.1.0.0.0.4690892-1.el6.x86_64
     rpm -e nsx-da-1.1.0.0.0.4690845-1.el7.x86_64
     rpm -e nsx-host-1.1.0.0.0.4690932-1.x86_64 rpm -e nsx-
     host_node_status_reporter-1.1.0.0.0.4690845-1.el7.x86_64
     rpm -e nsx-lldp-1.1.0.0.0.4690845-1.el7.x86_64
     rpm -e nsx-logical_exporter-1.1.0.0.0.4690845-1.el7.x86_64
     rpm -e nsx-mpa-1.1.0.0.0.4690845-1.el7.x86_64
     rpm -e nsx-netcpa-1.1.0.0.0.4690924-1.el7.x86_64 rpm -e nsx-sfhc-
     1.1.0.0.0.4690845-1.el7.x86_64
     rpm -e nsx-support-bundle-client-1.1.0.0.0.4690845-1.el7.x86_64
     rpm -e nsx-transport_node_status-1.1.0.0.0.4690845-1.el7.x86_64
     rpm -e nsxa-1.1.0.0.0.4690845-1.el7.x86_64
     rpm -e openvswitch-2.6.0.4557686-1.x86_64
     rpm -e openvswitch-selinux-policy-2.6.0.4557686-1.noarch
     rpm -e python-simplejson-3.3.3-1.el7.x86_64
     ```
     如果在运行 `rpm -e` 命令时出现任何错误，请在该命令中添加 `--noscripts` 标记。
  2. 运行解决方案 API `POST /api/v1/error-resolver?action=resolve_error`。
  3. 再次将 KVM 主机添加到结构层中。

- 问题 1602470：在 KVM 上不支持负载均衡绑定

- 问题 1611154：一个 KVM 传输节点中的虚拟机无法访问位于另一个传输节点中的虚拟机
  在将多个 IP 池用于属于不同网络的 VTEP 时，KVM 主机上的虚拟机可能无法访问在具有不同 IP 池中的 VTEP IP 地址的其他主机上部署的虚拟机。

  解决办法：添加路由，以便 KVM 传输节点可以访问用于其他传输节点上的 VTEP 的所有网络。
  例如，如果具有两个网络（25.10.10.0/24 和 35.10.10.0/24），并且本地 VTEP 具有 IP 地址 25.10.10.20 和网关 25.10.10.1，则可以使用以下命令为另一个网络添加路由：
  ```
  ip route add dev nsx-vtep0.0 35.10.10.0/24 via 25.10.10.1
  ```

- 问题 1654999：底层流量的连接跟踪将减少可用内存
  在虚拟机之间建立大量连接时，可能会出现以下症状。
  在 /var/log/syslog 或 /var/log/messages 文件中，将会看到类似下面的条目：
  ```
  Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.950872] net_ratelimit: 239 callbacks suppressed
  Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.950875] nf_conntrack: table full, dropping packet
  Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.958436] nf_conntrack: table full, dropping packet
  ```
  如果已配置默认防火墙规则，就会出现该问题。如果未配置防火墙规则，则不会出现该问题（例如：将逻辑交换机放在防火墙排除列表中）。
  **注意**：前面的日志摘录仅作为示例。日期、时间和环境变量可能因您的环境而异。

  解决办法：添加一个防火墙规则以在底层设备中的端口 6081 上禁用 UDP 连接跟踪。
  下面是一个示例命令：
  ```
  # iptables -A PREROUTING -t raw -p udp --dport 6081 -j CT --notrack
  ```
  应该将其配置为在引导期间运行。如果平台还启用了防火墙管理器（Ubuntu：UFW；RHEL：firewalld），应通过防火墙管理器配置等效的规则。请参见相关知识库文章 2145463。

- 问题 2002353：不支持使用 Linux 网络管理器管理 KVM 主机上行链路
  NSX-TData Center管理用于 N-VDS 的 KVM 主机上的所有网卡。再为这些上行链路启用网络管理器时，会发生配置错误。

  解决办法：对于 Ubuntu 主机，从网络管理器中排除要用于 NSX-TData Center的网卡。

  在 Red Hat 主机上启用 NSX-TData Center 之前，将 /etc/sysconfig/network-scripts 中的网卡配置脚本修改为 `NM_CONTROLLED="no"`。如果已为主机启用了 NSX-TData Center ，请进行相同的脚本修改，然后重新启动主机的网络连接。

- 问题 2186045：在 KVM 上，默认情况下每天而不是每分钟运行 logrotate
  在 KVM 上，如果日志文件的大小在一天内超过其基于大小的轮换策略中定义的大小限制，则在运行 logrotate 当天结束之前不会进行轮换。因此，日志文件的大小可能会大于定义的大小限制。

  解决办法：执行下列步骤：

  1. 创建新目录 /etc/cron.minutes。
  2. 使用以下内容创建 /etc/cron.minutes/logrotate 脚本：
     ```
     #!/bin/sh
     /usr/sbin/logrotate /etc/logrotate.conf
     ```
  3. 更改 /etc/cron.minutes/logrotate 的权限：
     ```
     chmod 755 /etc/cron.minutes/logrotate
     ```
  4. 附加 cron.minutes 作为 /etc/crontab 中的条目：
     ```
     echo "* * * * * root cd / && run-parts --report /etc/cron.minutes" >>/etc/crontab
     ```

负载均衡器已知问题

- 问题 2010428：负载均衡器规则创建和应用限制
  在用户界面中，您只能从虚拟服务器创建负载均衡器规则。使用 REST API 创建的负载均衡器规则不能在用户界面中附加到虚拟服务器。

  解决办法：如果您使用 REST API 创建了一个负载均衡器规则，请使用 REST API 将该负载均衡器规则附加到虚拟服务器。使用 REST API 创建的规则随即将显示在用户界面的虚拟服务器中。

- 问题 2016489：选择服务器名称指示后，LCP 无法配置默认证书
  在服务器名称指示 (SNI) 中使用多个证书 ID 时，应首先在证书列表中设置默认证书 ID，以避免 LCP 忽略默认证书。

  解决办法：默认证书应位于 SNI 证书列表首位。

- 问题 2115545：启用负载均衡器运行状况检查后，直接连接到后端服务器池成员可能会失败
  如果负载均衡器连接到逻辑路由器，则可使用逻辑路由器的上行链路访问池成员时，连接到逻辑路由器下行链路的客户端无法使用与运行状况检查相同的协议访问池成员。

  例如，如果负载均衡器连接到逻辑路由器 LR1 并启用 ICMP 运行状况检查以通过 LR1 上行链路访问池成员，则 LR1 下行链路上的客户端无法直接对这些池成员执行 ping 操作。但是，同一个客户端可以使用 SSH 或 HTTP 等其他协议与服务器通信。

  解决办法：在负载均衡器上使用不同的运行状况检查类型。例如，要对后端服务器执行 ping 操作，请使用 TCP 或 UDP 运行状况检查，而不是 ICMP 运行状况检查。

- 问题 2128560：配置负载均衡器 SNAT 自动映射和运行状况检查可能会导致偶尔执行运行状况检查失败或出现连接故障
  为同一个服务器池配置负载均衡器 SNAT 自动映射和运行状况检查（例如，TCP、HTTP、HTTPS 或 UDP）可能会导致该服务器池偶尔执行运行状况检查失败或出现连接故障。

  解决办法：使用 SNAT IP 列表，而非 SNAT 自动映射。

  注意：SNAT IP 列表模式中指定的 SNAT IP 地址不应包含逻辑路由器上行链路 IP 地址。

  例如，如果负载均衡器连接到第 1 层逻辑路由器 LR1，则配置的 SNAT IP 范围不应包含 LR1 上行链路 IP 地址。

解决方案互操作性已知问题

- 问题 1588682：将 ESXi 主机置于锁定模式将禁用用户 nsx-user
  在将 ESXi 主机置于锁定模式时，用户 vpxuser 是可以在主机中进行身份验证或运行任何命令的唯一用户，NSX-TData Center依赖另一个用户（nsx 用户）在主机上执行所有与 NSX-TData Center相关的任务。

  解决办法：不要使用锁定模式。请参阅 vSphere 文档中的锁定模式。

运行和监控服务已知问题

- 问题 1749078：在删除 ESXi 主机和相应主机传输节点上的租户虚拟机后，删除 ESXi 主机将失败
  删除主机节点涉及重新配置各种对象，可能需要几分钟或更长的时间。

  解决办法：等待几分钟，然后重试删除操作。如有必要，请重复该操作。

- 问题 1761955：注册虚拟机后，无法将虚拟机的 vNIC 连接到 NSX-T Data Center 逻辑交换机
  如果使用现有的 vmx 文件在 ESXi 主机上注册虚拟机，注册操作将忽略以下 vNIC 特定的错误：

  - 为 vNIC 配置的网络支持无效。
  - 连接到 NSX-T 逻辑交换机的 vNIC 的 VIF 连接失败。

  解决办法：完成以下步骤。
  1. 在标准 vSwitch 上创建一个临时端口组。
  2. 将处于断开连接状态的 vNIC 连接到新端口组，并将其标记为已连接。
  3. 将这些 vNIC 连接到有效的 NSX-TData Center逻辑交换机。

- 问题 1774858：在极少数情况下，NSX Controller 集群在运行数天后变为非活动状态
  在 NSX Controller 集群变为非活动状态时，所有传输和 NSX Edge 节点将与 NSX Controller 断开连接，并且无法对配置进行更改。不过，数据流量不会受到影响。

  解决办法：完成以下步骤。

  - 修复磁盘延迟问题（如果存在）。
  - 在所有 NSX Controller 上重新启动 cluster-mgmt 服务。

- 问题 1576304：在端口状态和统计信息报告中不包含丢弃的字节数
  在使用 /api/v1/logical-ports/<lport-id>/statistics 或 NSX Manager 查看逻辑端口状态和统计信息时，丢弃的数据包数值为 0。该值不准确。无论丢弃的数据包数是多少，此处显示的数字始终是空白的。

  解决办法：无。

- 问题 1955822：许可证使用情况报告 csv 文件还应包含 CPU 和虚拟机授权以及实际使用情况
  在查询许可证使用情况报告（通过 API/UI）时，数据仅包含当前使用情况。

  解决办法：通过 UI 或 REST API 查询当前许可证允许的使用情况限制：
  方法：GET；URI：/api/v1/licenses

- 问题 2081979：传输节点主机无法连接到任何控制器
  NSX 代理日志显示以下内容。预期显示“证书验证”消息，但未显示。

  ```
  TCP connection started: 10.171.0.73:0::3a4de8a2-3bc1-41ea-a94d-c1427d8cd757:1234
  Doing SSL handshake
  TCP connection established: 10.171.0.73:0::3a4de8a2-3bc1-41ea-a94d-c1427d8cd757,
  local addr: 10.171.0.59:36048, remote addr: 10.171.0.73
  ```

  解决办法：以管理员身份登录到控制器并运行以下命令：

  ```
  set debug
  get mediator forcesync
  ```

升级已知问题

- 问题 1930705：在管理平面升级过程中，通过 vMotion 移动连接到逻辑交换机的虚拟机失败
  在管理平面升级过程中，尝试通过 vMotion 移动连接到逻辑交换机的虚拟机失败。

  解决办法：等到管理平面升级完成，然后重试 vMotion 过程。

- 问题 2005423：从以前版本的 NSX-T 升级的 KVM 节点不会自动更改为使用 balance-tcp
  NSX-T 不会自动将已升级的 KVM 主机上行链路的绑定模式从 active-backup 修改为 balance-tcp。

  解决办法：编辑传输节点以更正模式设置，即使没有任何配置更改也是如此。

- 问题 2101728：有些情况下，一个 NSX Edge 组成功升级后，NSX Edge 升级过程会暂停
  一个 NSX Edge 组升级成功，但是，在第二个 NSX Edge 组升级期间，升级过程暂停。

  解决办法：单击**继续**以继续升级 NSX Edge 组。

- 问题 2106257：从 NSX-T 2.1 升级到 NSX-T 2.2 后，EULA API 接受工作流发生变化
  更新升级处理协调器之后以及升级现有主机之前，应调用 EULA API 接受操作。

  解决办法：无

- 问题 2108649：如果将执行升级的分区中有文件或目录处于打开状态，则升级将失败

避免打开将升级的分区（例如，NSX Manager 或 NSX Controller）中的文件或目录，因为这会导致升级过程失败。

解决办法：重新引导发生故障的设备并重新启动升级过程。

- 问题 2116020：从 NSX-T 2.1 升级到 NSX-T 2.2 后，不会移除某些 Ubuntu KVM 弃用的软件包
从 NSX-T 2.1 升级到 NSX-T 2.2 后，不会移除以下 Ubuntu KVM 弃用的软件包。
    - nsx-host-node-status-reporter
    - nsx-lldp
    - nsx-logical-exporter
    - nsx-netcpa
    - nsx-support-bundle-client
    - nsx-transport-node-status-reporter
    - nsxa

解决办法：完成以下步骤。

1. 在 /etc/vmware/nsxa/ 目录中创建临时文件。
   `cd /etc/vmware/nsxa`
   `touch temp.txt`
2. 列出所有 nsxa 软件包目录和文件。
   `dpkg -L nsxa`
   `/etc/vmware/nsxa# ls`
3. 移除以下软件包。
   a) `dpkg --purge nsx-lldp`
   b) `dpkg --purge nsx-support-bundle-client`
   c) `dpkg --purge nsx-transport-node-status-reporter`
   d) `dpkg --purge nsx-logical-exporter`
   e) `dpkg --purge nsx-netcpa`
   f) `dpkg --purge nsxa`
   g) `dpkg --purge nsx-host-node-status-reporter`
4. 确认以下目录可用。
   `/etc/vmware/nsxa/`
5. 从 /etc/vmware/nsxa/ 目录中移除 temp.txt 文件。
   `rm -f temp.txt`

- 问题 2164930：如果包含空的主机升级单元组，则管理平面升级完成后显示“已暂停”状态
包含空的主机升级单元组时，总体管理平面升级状态显示为已暂停，且主机升级状态未标记为 100%。

  *对客户的影响*：如果在升级期间客户具有空的主机组，则在 MP 升级完成后，升级状态将显示为已暂停。

  解决办法：升级管理平面之前，请删除空的主机升级单元组。
  如果已升级管理平面，请删除空的主机升级单元组并使用 CLI 重新启动 `install-upgrade service`。

- 问题 2097094：不支持在升级期间取消升级包上载
正在上载升级包 .mub 文件时，无法取消上载操作。

  解决办法：等待升级包 .mub 文件完成上载。

- 问题 2122242：将 Ubuntu KVM 主机从 NSX-T 2.1 升级到 2.2 或 NSX-T Data Center 2.3 不会移除 nsx-support-bundle-client 软件包
将 Ubuntu KVM 主机从 NSX-T 2.1 版本升级到较新版本（NSX-T 2.2 或 NSX-TData Center2.3）时，仍会安装 nsx-support-bundle-client 软件包，即使该软件包不再使用也是如此。用户通过调用 `/usr/bin/dpkg -l` 等命令可看到仍会安装软件包。

解决办法：以 root 用户身份登录并运行以下命令手动移除该软件包：

```
# /usr/bin/dpkg --purge nsx-support-bundle-client
```

- 问题 2186957：ESXi 主机在升级后未退出维护模式
  如果集群只有一个主机且如果升级协调器以前尝试将其置于维护模式失败，则 ESXi 主机在升级后不会退出维护模式。

  解决办法：手动使主机退出维护模式，或者确保主机可以进入维护模式（每个集群必须至少有 2 个主机）。

- 问题 2166207：从 NSX-T Data Center 2.2 升级到具有 500 个 Hypervisor 的 NSX-T Data Center 2.3 期间，整体升级过程可能会始终处于 IN_PROGRESS 状态
  从 NSX-T Data Center 2.2 升级到具有 500 个 Hypervisor 的 NSX-T Data Center 2.3 期间，单击“暂停”再多次刷新 Web 浏览器后，整体升级过程可能会始终处于 IN_PROGRESS 状态。

  解决办法：在 NSX Manager 上登录到 NSX-T Data Center CLI。键入命令 `install-upgrade` 以重新启动服务。

- 问题 2113681：如果 KVM 主机在 NSX Edge 升级后变得无法访问并出现故障，则升级协调器会尝试升级出现故障的主机，而不是继续升级 NSX Controller 节点
  升级 KVM 主机和 NSX Edge 并卸载主机上的新 RPM、安装旧 RPM 后，主机在升级协调器中将变得不可用。因此，升级协调器会尝试升级 KVM 主机，而不是继续升级 NSX Controller 节点。

  解决办法：刷新升级协调器用户界面，单击**主机**选项卡，然后尝试升级 KVM 主机。

  也可以跳过 KVM 主机升级，打开命令提示符并键入命令 `curl -i -k -u admin -X POST https://<nsx-manager-ip-address>/api/v1/upgrade/plan?action=continue\&skip=true`

API 已知问题

- 问题 1605461：syslog 中的 NSX-T API 日志显示系统内部 API 调用。NSX-T 将用户调用的 API 调用以及系统调用的 API 调用记录到 syslog 中
  在 syslog 中记录 API 调用事件并不表明用户直接调用 NSX-T API。您可以在日志中看到 NSX Controller 和 NSX Edge API 调用，即使这些 NSX-T 设备没有公开的 API 服务。这些专用的 API 服务是由其他 NSX-T 服务使用的，例如，NSX-T CLI。

  解决办法：无。

- 问题 1641035：对 **`POST/hpm/features/<feature-stack-name?action=reset_collection_frequency>`** 的 REST 调用不会还原覆盖统计信息的 collection_frequency
  如果尝试使用该 REST 调用将收集频率重置为默认值，并不会重置该频率。
  解决办法：使用 `PUT /hpm/features/<feature-stack-name>` 并将 collection_frequency 设置为新的值。

- 问题 1648571：按需状态和统计信息请求可能会间歇性失败。HTTP 故障代码不一致
  在某些情况下，按需请求失败。有时，这些请求失败并显示 HTTP 500 错误，而不是 HTTP 503 错误，即使 API 调用在重试时成功。
  对于统计信息 API，超时情况可能会导致虚假的消息路由错误日志。发生这些情况是因为，在超时期限到期后返回响应。
  例如，可能会出现如下错误：`java.lang.IllegalArgumentException: Unknown message handler for type com.vmware.nsx.management.agg.messaging.AggService$OnDemandStatsResponseMsg.`
  对于状态 API，超时情况（在超时后返回响应）可能会导致过早更新缓存。

  解决办法：重试 API 请求。

- 问题 1963850：GET API 显示以区分大小写的方式存储的项目
  GET API 返回按显示名称排序的项目时，排序区分大小写。

  解决办法：无。

- 问题 2070136：可处理大量数据的分布式防火墙 API 失败
  必须创建或更新超过 100 MB 数据的分布式防火墙 API 失败并显示错误代码 500 和指示失败事务的消息。API 通常涉及具有 1000 个以上规则的区域，其中每个规则包含多个源、目标和适用对象。

  解决办法：以递增方式创建或更新规则。

- 问题 1895497：API 中的负载均衡器算法 SRCDESTMACIPPORT 无法正常工作
  调用 API 以使用包含源和目标 MAC 地址、IP 地址及 TCP/UDP 端口的 LAG 创建传输节点的上行链路配置文件将失败。

  解决办法：无

NSX Policy Manager 已知问题

- 问题 2057616：NSX Policy Manager 从 NSX-T 2.1 升级到 NSX-T 2.2 期间，不会传输不受支持的 NS 服务和 NS 组
  NSX Policy Manager 从 NSX-T 2.1 升级到 NSX-T 2.2 期间，不会传输具有以太网类型的不受支持的 NS 服务以及具有 MAC 集和逻辑端口成员资格条件的 NS 组。

  解决办法：完成以下步骤。

  1. 在 NSX-T 2.1 中，移除和修改任何通信条目中使用的以太网类型的 NS 服务。
  2. 移除和修改任何通信条目中使用的具有 MAC 集和逻辑端口成员资格条件的 NS 组。
  3. 将 NSX Manager 从 NSX-T 2.1 升级到 NSX-T 2.2。
  4. 使用 CLI 升级 NSX Policy Manager。
- 问题 2116117：UI 中的 NSX Policy Manager 拓扑选项卡显示“数据连接失败”
  UI 中的 NSX Policy Manager 拓扑选项卡显示数据连接失败，因为策略域中的组包含 ESXi 6.7 版本托管的虚拟机，而这不受支持。

  解决办法：无

- 问题 2126647：同时更新 NSX Policy Manager 分布式防火墙会导致覆盖
  当两个用户同时编辑 NSX Policy Manager 分布式防火墙区域时，后一用户所做的更改将覆盖另一用户之前所做的编辑。

  解决办法：恢复第一位用户所做的分布式防火墙更改。保存所做的更改后，第二位用户可以进行更改。

NSX Cloud 已知问题

- 问题 2112947：在 Cloud Service Manager (CSM) 中升级 NSX 代理时，一些实例可能会显示为“失败”
  在 CSM 中升级 NSX 代理时，一些实例可能会由于用户界面无响应而显示为“失败”。

  *解决办法：* 刷新用户界面。

- 问题 2111262：部署 PCG 时，可能会看到以下错误：“网关部署失败: [错误代码: 60609] 异步操作失败，置备状态为: 失败 (Gateway deployment failed: [Errorcode: 60609] Async operation failed with provisioning state: Failed)”。或者“无法使用名称 nsx-gw 创建网关虚拟机，网关部署失败 (Failed to create gateway virtual machine with name nsx-gw, Gateway deployment failed)”。
  此类事件很少发生，是 Microsoft Azure 基础架构所致。

  *解决办法：* 重新部署失败的公有云网关 (PCG)。

- 问题 2110728：如果您使用 HA，但通过使用 --gateway 选项仅指定一个 PCG DNS 名称在虚拟机上安装了 NSX 代理，则无法故障切换到辅助 PCG。
  故障切换后，工作负载虚拟机无法连接到 PCG，因此 PCG 无法实施/实现虚拟机上的任何逻辑状态。

  *解决办法：* 在工作负载虚拟机上安装代理时，不要使用 `--gateway` 选项。使用来自 VPC 或 VNet 的网关屏幕的值。有关详细信息，请参阅《NSX-T Data Center 管理指南》中的**安装 NSX 代理**。

- 问题 2071374：在某些 Linux 虚拟机实例上安装 NSX 代理时，可能会显示有关“nscd”的无害错误消息
  描述：在运行“nscd”的虚拟机上，安装 NSX 代理时，您可能会看到类似以下内容的错误消息：“已发送 invalidate(passwd) 请求，正在退出 (sent invalidate(passwd) request, exiting)”。运行 Ubuntu 14.04 或 16.04 的虚拟机上将出现该问题

  *解决办法：* 由于 Linux 发布版本中的已知错误，会显示此类消息。这些消息没有危害性，不会影响 NSX 代理的安装。

- 问题 2010739：两个公有云网关 (PCG) 都显示为待机
  如果主 PCG 在网关接入期间无法连接到控制器，则主网关和辅助网关都将处于待机模式，直到恢复控制器和网关之间的连接。

- 问题 2121686：CSM 显示异常“服务器无法对请求进行身份验证 (Server failed to authenticate the request)”。
  CSM 中可能会显示此错误，这是因为 CSM 设备时间与 Microsoft Azure 存储服务器或 NTP 不同步。在这种情况下，Microsoft Azure 会抛出异常“服务器无法对请求进行身份验证 (Server failed to authenticate the request)”。此错误不够明确，但 CSM 中也显示了相同的错误。

  *解决办法：* 将 CSM 设备时间与 NTP 或 Microsoft Azure 存储服务器时间同步。

- 问题 2092378：在 HA 模式下部署 PCG 时会显示两个 PCG 都处于备用模式，而云同步显示主 PCG 为活动状态
  在专用网络中通过 CSM 针对 PCG 执行 HA 部署后，部署的 PCG 上显示备用/备用或活动/活动状态，时间长达 1 小时。在此时段内，对于用户而言，似乎部署的 PCG 存在一些问题且状态不够明确，无法继续操作。

  *解决办法：* 执行以下操作：

  1. 部署 PCG 后从 UI 重新同步帐户，CSM 可以获取最新数据并显示在 CSM 中。
  2. 如果重新同步后 CSM 仍显示 PCG 处于错误状态，请在 NSX Manager 中检查 PCG 的连接状态。
  3. 如果连接显示为“已连接”，但状态仍不正确，请继续调试 PCG。
- 问题 2119726： 在 Microsoft Azure VNet 中部署 PCG 时，先前与虚拟机关联的公共 IP 可能会被错误地列为可用。
  如果先前分配了公共 IP 的虚拟机现在已关闭电源，则它们不再与这些公共 IP 关联。这是因为，虚拟机关闭电源后，Microsoft Azure 会在一段时间内解除关联与这些虚拟机关联的公共 IP。Microsoft Azure 未专门定义此时间段。

*解决办法：*请勿关闭 VNet 中 PCG 的电源。这可以防止公共 IP 与主 PCG 的上行链路接口解除关联。如果必须关闭 PCG 电源，请确保未重用与 PCG 关联的 PIP，这样只要 PCG 重新打开电源，便会获得相同的 PIP。

- 问题 2165915：NSX Cloud 对包含 kmod.x86_64 0:20-15.el7_4.6 的 Red Hat Enterprise Linux 7.4 的支持
  NSX Cloud 不支持虚拟机实例运行包含 `kmod-20-15.el7_4.6` 的 Red Hat Enterprise Linux 7.4。该问题是由 Red Hat 报告的错误造成的：https://bugzilla.redhat.com/show_bug.cgi?id=1522994。

  *解决办法：*更新到已修复此错误的 kmod 版本，以便成功安装 NSX 代理。

- 问题 2102828：在 Microsoft Azure 部署中，从 NSX-T 2.2 升级到 NSX-T Data Center 2.3 期间或之后，公有云网关 (PCG) 可能无法正常工作。
  在系统已从 NSX-T 2.2 升级到 NSX-T Data Center 2.3 的 Microsoft Azure 部署中，在极少数情况下，公有云网关 (PCG) 可能会无法获取其接口上的 IP 地址。执行 PCG 升级步骤时，如果 PCG 升级过程似乎挂起，则可能会出现该问题。如果管理员从 Microsoft Azure 门户重新启动 PCG 设备，此问题也可能会显示为 PCG 无法正常工作。首次安装 NSX-T Data Center 2.3 的新系统不会出现该问题。

  *解决办法：*从 Microsoft Azure 门户重新启动正在升级的 PCG，然后在 Cloud Service Manager (CSM) 中验证 PCG 和虚拟机实例的状态是否有效。

- 问题 2180531：具有内核 4.14 及更低版本的 Ubuntu 16.04 虚拟机实例支持 NSX 代理
  具有内核 4.14 及更低版本的 Ubuntu 16.04 虚拟机实例支持 NSX 代理。NSX 代理不适用于具有内核 4.15 及更高版本的 Ubuntu 16.04 虚拟机实例。

  此问题没有解决办法

- 问题 2170445：将 PCG 从 NSX-T Data Center 2.2 升级到 NSX-T Data Center 2.3 后，Microsoft Azure PCG 的 PCG HA 状态将不会正确设置
  将 Microsoft Azure PCG 从 NSX-T 2.2 升级到 NSX-T Data Center 2.3 后，PCG HA 状态不会按预期变为“活动-备用”。首选 PCG HA 状态显示为“同步”，非首选 PCG HA 状态显示为“活动”。因此，如果在升级后发生 HA 故障切换，则只有一个 PCG 具有有效状态。

  *解决办法：*在 NSX-T 2.2 中，先将 PCG 的上行链路主机交换机配置文件中的 MTU 更新为 1500，然后再开始升级到 NSX-T Data Center 2.3。
  可以使用 NSX Manager UI 或 NSX Manager REST API 实现。

  通过 UI，执行以下操作：

  1. 转到Fabric > 配置文件
  2. 选择名称为“PCG-Uplink-HostSwitch-Profile”、描述为“PublicCloudGateway Uplink HostSwitch Profile”的配置文件
  3. 单击**编辑**，将 MTU 值修改为 1500，然后单击**保存**
  4. 开始从 NSX-T 2.2 升级到 NSX-T Data Center 2.3。

  通过 REST API，执行以下操作：

  1.使用以下命令获取所有主机交换机配置文件：

```
curl -X GET \
  https://<NSX-Manager-URL>/api/v1/host-switch-profiles \
  -H 'authorization: Basic <AUTH ID>' \
  -H 'content-type: application/json'
```

2.标识名称为“PCG-Uplink-HostSwitch-Profile”、描述为“PublicCloudGateway Uplink HostSwitch Profile”的主机交换机配置文件，然后获取该配置文件的 ID：

```
curl -X PUT \
  https://<NSX-Manager-URL>/api/v1/host-switch-profiles/<host-switch-profile-id>
 \
  -H 'authorization: Basic <AUTH ID>' \
  -H 'content-type: application/json' \
  -d '{
            "resource_type": "UplinkHostSwitchProfile",
            "description": "PublicCloudGateway Uplink HostSwitch Profile",
            "id": "<host-switch-profile-id>",
            "display_name": "PCG-Uplink-HostSwitch-Profile",
            "tags": [
                {
                    "scope": "CrossCloud",
                    "tag": "public-cloud-manager"
                },
                {
                    "scope": "PcmId",
                    "tag": "<Existing PCM ID>"
                },
                {
                    "scope": "EntityType",
                    "tag": "default"
                },
                {
                    "scope": "CloudScope",
                    "tag": "<Existing VPC/VNET name>"
                },
                {
                    "scope": "CloudType",
                    "tag": "<Existing cloud type>"
                },
                {
                    "scope": "CloudVpcId",
                    "tag": "<Existing Vpc/Vnet id>"
                }
            ],
            "transport_vlan": 0,
            "teaming": {
                "active_list": [
                    {
                        "uplink_type": "PNIC",
                        "uplink_name": "uplink-1"
                    }
                ],
                "policy": "FAILOVER_ORDER"
            },
            "overlay_encap": "GENEVE",
            "mtu": 1500,
```

```
        "_revision": 1
    }'
```

- 问题 2174725：部署了 PCG 的受管 VPC/VNet 在 CSM 中显示为非受管。
  部署了 PCG 的受管 AWS VPC 或 Microsoft Azure VNet 在 CSM 中显示为非受管。

  *解决办法：*重新启动 CSM 应该能解决该问题。

- 问题 2162856：Azure PCG 的 HA 状态无效（均为活动或均为备用）
  在 AWS 中部署一对 PCG，然后为 Azure 部署另一对 PCG 后，Azure PCG 将具有无效的 HA 状态（均为活动或均为备用）。

  解决办法：先将 PCM 创建的 PCG 上行链路主机交换机配置文件中的 MTU 更新为 1500，然后再开始跨云升级到 NSX-T Data Center 2.3。从 Manager UI 执行以下步骤：

  - 转到“Fabric”>“配置文件”。
  - 选择名称为“PCG-Uplink-HostSwitch-Profile”、描述为“PublicCloudGateway Uplink HostSwitch Profile”的配置文件。
  - 单击“编辑”，将“MTU”值修改为 1500，然后单击“保存”。
  - 启动升级工作流。
- 问题 2102321：在高流量时段内，某些 NSX Cloud 操作在 Microsoft Azure 上可能会较慢。
  NSX Cloud 依赖 Microsoft Azure ARM API 执行某些操作，如管理虚拟机或退出 NSX 管理；或者对虚拟机采取隔离操作。在高峰时段内，Microsoft Azure 可能会达到给定订阅的 API 限制，在这种情况下，将开始终止该订阅的所有 API 请求。在此期间，上述 NSX 操作可能无法及时完成。最终会在 Microsoft Azure 停止终止请求时完成这些操作。公有云网关上的 PCM 日志将具有类似以下内容的日志，指示当前发生终止情况：“*Azure Resource Manager read/write per hour limit reached.Will retry in: x seconds*”

  *解决办法：* 等待 Microsoft Azure 终止停止。

- 问题 2189738：为已加载的 VPC 禁用之前启用的隔离策略后，无法访问 AWS 工作负载虚拟机。
  如果部署了已启用隔离策略的 PCG，并且之后如果禁用隔离模式，则此 VPC 中的某些 NSX 受管 AWS 工作负载虚拟机无法与 PCG 进行通信。

  *解决办法：*将以下入站规则添加到 AWS VPC 中的 NSX Cloud 安全组：gw-mgmt-sg：
  **注意**：出于安全原因再次启用隔离策略时，请移除这些规则。

| 类型 | 协议 | 端口 | 源 |
|---|---|---|---|
| CUSTOM-TCP | TCP | 8080 | VPC-CIDR |
| CUSTOM-TCP | TCP | 5555 | VPC-CIDR |

- 问题 2188950：使用 API 检索 PCG 列表时，您会看到以下错误：“找不到指定 ID 的 VNet (No VNet found for specified ID)”。
  如果从 CSM 中删除与 PCG 部署关联的帐户，您会看到此错误。

  *解决办法：*在部署了 PCG 的 CSM 中添加 Microsoft Azure 帐户。

- 问题 2191571：如果 PCG 部署的 SSH 公钥未以电子邮件 ID 为结尾，则 PCG 部署不会启动。
  SSH 公钥必须以电子邮件 ID 为结尾，否则 PCG 部署将不会启动并显示错误。

  *解决办法：*确保 SSH 密钥以电子邮件 ID 为结尾。

- 问题 2092073：在 Windows 工作负载虚拟机上，未正确收到 IPFIX 模板。

在 Windows 工作负载虚拟机上，在与虚拟机相同的子网上配置 IPFIX 收集器后未立即发送逻辑交换机和防火墙 IPFIX 模板。这是因为在发送 UDP 数据包之前，Windows 套接字需要 IPFIX 收集器的 IP 地址的 ARP 条目。如果缺少 ARP 条目，则将以静默方式丢弃所有 UDP 数据包（最后一个数据包除外）。因此，在 IPFIX 收集器上，将收到不含模板信息的数据包。

*解决办法：*执行以下操作之一：

- 使用以下命令添加 IPFIX 收集器的静态 ARP 条目：

```
netsh interface ipv4 add neighbors "<Interface name>" <collector IP> <physical address of collector>
```

例如：

```
netsh interface ipv4 add neighbors "Ethernet 3" 172.26.15.7 12-34-56-78-9a-bc
```

- 在与工作负载虚拟机不同的子网上配置 IPFIX 收集器。

- **问题 2210490：如果在 CSM 中添加代理配置文件，密码将对分配有以下任意角色的所有 CSM API 用户可见： 云服务审核员或云服务管理员。**
  如果在 CSM 中创建代理配置文件并提供用户名和密码，即使您不能在 CSM UI 中查看密码，密码也会显示在以下 API 响应中：
  - /csm/proxy-server-profiles
  - /csm/proxy-server-profiles/<profile-id>
- **问题 2039804：PCG 部署失败，但 PCG 实例在 AWS 中不终止。**
  如果部署 PCG 时部署失败，仍会看到 AWS VPC 中的 PCG 实例和 NSX Manager 中自动创建的逻辑实体。

  *解决办法：*手动删除自动创建的 NSX Manager 实体，并终止 AWS VPC 中的 PCG 实例。

NSX Container Plug-in (NCP) 已知问题

- PAS 2.1.0 CNI 更改
  由于 PAS 2.1.0 中的 CNI 插件发生更改，因此无论哪种版本的 NSX-T Tile 都不会使用 PAS 2.1.0。PAS 2.1.1 中已修复此问题。

- **问题 2118515：在大型设置中，NCP 需要很长时间才能在 NSX-T 上创建防火墙**
  在大型设置（例如，250 个 Kubernetes 节点、5000 个 pod、2500 个网络策略）中，NCP 可能需要数分钟才能在 NSX-T 中创建防火墙区域和规则。

  解决办法：无。创建防火墙区域和规则后，性能应恢复正常。

- **问题 2125755：执行 canary 更新和分阶段滚动更新时，StatefullSet 可能会断开网络连接**
  如果将 NCP 升级到当前版本之前已创建 StatefulSet，则执行 canary 更新和分阶段滚动更新时，StatefullSet 可能会断开网络连接。

  解决办法：将 NCP 升级到当前版本之后再创建 StatefulSet。

- **问题 2131494：将 NGINX Kubernetes Ingress 类从 nginx 更改为 nsx 后，该 Ingress 仍起作用**
  创建 NGINX Kubernetes Ingress 时，NGINX 会创建流量转发规则。将 Ingress 类更改为其他任何值后，NGINX 不会删除规则并继续应用这些规则，即使在更改类后删除 Kubernetes Ingress 也是如此。这是 NGINX 的一个缺陷。

  解决办法：要删除 NGINX 创建的规则，请在类值为 nginx 时删除 Kubernetes Ingress。然后重新创建 Kubernetes Ingress。

- **问题 2194845：不支持 PAS Cloud Foundry V3 API 功能“每个应用程序多个进程”**

使用 PAS Cloud Foundry V3 API `v3-push` 推送具有多个进程的应用程序时，NCP 不会为默认进程以外的其他进程创建逻辑交换机端口。NCP 2.3.0 和更低版本中存在此问题。

解决办法：无

- 问题 2193901：单个 Kubernetes 网络策略规则不支持使用多个 PodSelector 或多个 NsSelector
  应用多个选择器仅允许来自特定 pod 的入站流量。

  解决办法：在单个 PodSelector 或 NsSelector 中改为结合使用 matchLabels 和 matchExpressions。

- 问题 2194646：不支持在 NCP 关闭时更新网络策略
  如果在 NCP 关闭时更新网络策略，则在 NCP 恢复运行后，网络策略的目标 IPset 将不正确。

  解决办法：NCP 启动后，重新创建网络策略。

- 问题 2192489：在 PAS Director 配置中禁用“BOSH DNS 服务器”后，Bosh DNS 服务器 (169.254.0.2) 仍显示在容器的 resolve.conf 文件中。
  在运行 PAS 2.2 的 PAS 环境中，在 PAS Director 配置中禁用“BOSH DNS 服务器”后，Bosh DNS 服务器 (169.254.0.2) 仍显示在容器的 resolve.conf 文件中。这将导致需要较长时间来执行具有完全限定域名的 ping 命令。PAS 2.1 不存在此问题。

  解决办法：无。这是 PAS 问题。

- 问题 2194367：NSX-T Tile 不支持自行部署路由器的 PAS 隔离分段
  NSX-T Tile 不支持自行部署 Go 路由器和 TCP 路由器的 Pivotal Application Service (PAS) 隔离分段。这是因为 NCP 无法获取路由器虚拟机的 IP 地址和创建 NSX 防火墙规则以允许从路由器到 PAS 应用程序容器的流量。

  解决办法：无。

- 问题 2199504：NCP 创建的 NSX-T 资源的显示名称限定为 80 个字符
  当 NCP 为容器环境中的资源创建 NSX-T 资源时，会通过组合集群名称、命名空间或项目名称和容器环境中的资源的名称来生成 NSX-T 资源的显示名称。如果显示名称长度超过 80 个字符，则会截断为 80 个字符。

  解决办法：无

- 问题 2199778：对于 NSX-T 2.2，不支持名称超过 65 个字符的 Ingress、Service 和 Secret
  对于 NSX-T 2.2，当 `use_native_loadbalancer` 设置为 `True` 时，Ingress 及其引用的 Secret/Service 的名称，以及 LoadBalancer 类型 Service 的名称不得超过 65 个字符。否则，Ingress 或 Service 将无法正常工作。

  解决办法：配置 Ingress、Secret 和 Service 时，指定不超过 65 个字符的名称。

- 问题 2065750：安装 NSX-T CNI 软件包失败并发生文件冲突
  在安装了 kubernetes 的 RHEL 环境中，如果使用 `yum localinstall` 或 `rpm-i` 安装 NSX-T CNI 软件包，则会显示错误，指示 kubernetes-cni 软件包中的文件发生冲突。

  解决办法：使用命令 `rpm -i --replacefiles nsx-cni-2.3.0.xxxxxxxx-1.x86_64.rpm` 安装 NSX-T CNI 软件包。

- 对于 ClusterIP 类型的 Kubernetes 服务，不支持基于 Client-IP 的会话关联性
  NCP 不支持 ClusterIP 类型的 Kubernetes 服务的基于 Client-IP 的会话关联性。

  解决办法：无

- 对于 ClusterIP 类型的 Kubernetes 服务，不支持发卡模式标记
  NCP 不支持 ClusterIP 类型的 Kubernetes 服务的发卡模式标记。

解决办法：无

## 文档勘误和增补

- 问题 1372211：在同一子网上具有两个接口
  如果隧道端点位于与管理接口相同的子网上，隧道流量可能会泄漏到管理接口。发生这种情况是因为，隧道数据包可能会经由管理接口。请确保管理接口位于与隧道端点接口不同的子网上。