



VMware NSX-T Data Center 2.4.1 发行说明

VMware NSX-T Data Center 2.4.1 | 2019 年 5 月 21 日 | 内部版本 13716575

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](#)
- [兼容性和系统要求](#)
- [API 和 CLI 资源](#)
- [修订历史](#)
- [已解决的问题](#)
- [已知问题](#)

新增功能

VMware HCX 现在支持通过 NSX-T 将虚拟机迁移到基于 NSX-T 的内部部署。这样，客户就可以将虚拟机从 NSX Data Center for vSphere 批量迁移到 NSX-T，执行从 NSX-T 到 NSX-T 的跨站点迁移，以及从非 NSX vSphere 环境迁移到基于 NSX-T 的 SDDC 环境。

在 2.4.0 版中添加了密码策略增强功能，这会为默认密码实施 12 个字符的最小密码长度，并引入了设置密码过期时间的功能。默认情况下，密码在 90 天后过期。有关重置密码和调整密码过期时间的说明，请参见知识库文章 [70691](#)。

兼容性和系统要求

有关兼容性和系统要求信息，请参见 [《NSX-T Data Center 安装指南》](#)。

API 和 CLI 资源

请参见 code.vmware.com 以使用 NSX-T Data Center API 或 CLI 实现自动化。

可从 API 参考选项卡获取 API 文档。可从文档选项卡获取 CLI 文档。

文档修订历史

2019 年 5 月 21 日。第一版。

2019 年 6 月 3 日。第二版。添加了已解决的问题 2339832。

2019 年 6 月 20 日。第三版。添加了已知问题 2261818、2334442。

2019 年 6 月 21 日。第四版。将问题 2304571 变为已解决状态。

2019 年 8 月 23 日。第五版。添加了已知问题 2362688、2395334 和 2392093。

2019 年 11 月 12 日。第六版。将问题 2295470 变为已解决状态。

已解决的问题

- 已修复问题 2248345：安装 NSX-T Edge 后，计算机引导时显示空白黑屏。
无法在 HPE ProLiant DL380 Gen9 计算机上安装 NSX Edge。
- 已修复问题 2264386：即使传输节点是 NS 组的一部分，也会删除传输节点
即使传输节点是 NS 组的一部分，也允许删除该节点。应阻止删除。如果遇到此问题，必须重新创建 NS 组并重建与传输节点的关系。
- 已修复问题 2275869：如果 ESXi 主机上的规则包含的标记超过 31 个字符，则 ESXi 主机上的 `cfgAgent` 日志在不到 1 分钟后滚动
日志滚动频繁可能会导致丢失 `cfgAgent.log` 中用于在主机上进行调试和故障排除的有用信息。ESXi 主机上的日志位置：`/var/log/cfgAgent.log`
- 已修复问题 2288872：安装状态显示为“节点未就绪”
Edge 节点未载入。传输节点配置状态为“挂起”，因此无法添加到 Edge 集群。日志位置：`/var/log/proton/nsxapi.log`
- 已修复问题 2291267：PCM 创建的默认网关策略区域没有分配序列号，因此策略默认将其设置为 0
如果用户创建网关策略时未使用序列号或 `insert_top` 选项，则会导致策略冲突。日志位置：`/var/log/policy/policy.log`
- 已修复问题 2292995：即使所有配置的规则都已在 OVS 中编程，实现状态也设置为错误
即使 DFW 规则已在数据平面中编程，API 也呈现出一种虚假的负面印象。
- 已修复问题 2292997：对于 Linux 网络堆栈，可能无法创建某些逻辑路由器接口
对于 Linux 网络堆栈，可能无法创建某些逻辑路由器接口，并返回以下错误：错误代码 =“EDG0100002”，创建子接口操作失败：超出了最大子接口数 (`errorCode="EDG0100002", Operation failed creating sub-interface: max sub-interface exceeded`)。因此，由于缺少路由，可能会丢弃 Tier-0 服务路由器 (T0 SR) 转发的流量。
- 已修复问题 2295470 - 从 NSX for vSphere 迁移到 NSX-T 后，防火墙筛选器不存在。
如果在很多防火墙规则中使用服务，则可能导致迁移期间在服务上频繁进行更新。因此，在 ESXi 主机上未安装防火墙筛选器。这可能会导致流量中断。
- 已修复问题 2285117：不支持在 NSX 管理的虚拟机上执行内核升级
在某些 Linux Ubuntu marketplace 映像中，内核会在重新引导虚拟机时自动升级。因此，`nsx-agent` 无法按预期运行。尽管 NSX 代理可能看上去正常运行，但会有一些未实现的网络策略，这会影响 `nsx-agent`。代理一次又一次地重试实现这些策略，从而导致高 CPU 使用率。
- 已修复问题 2252776：传输节点配置文件无法应用于某个集群成员主机，即使以前在主机上发生的验证错误现在已经解决
对集群应用 TNP。但无法将 TNP 应用于一个集群成员主机，因为无法通过某个验证（例如，虚拟机已在主机上打开电源）。用户可解决此问题，但 UI 仍然显示验证且 TNP 不会自动应用于该主机。
- 已修复问题 228688：如果基于 VTI 配置 BGP，则删除基于路由的 IPsec 会话时，应先删除 BGP 邻居
如果基于 VTI 配置 BGP，则删除 IPsec 会话时，两个服务路由器将处于关闭状态，进而会阻止流量。要恢复流量，应删除为 VTI 配置的 BGP 邻居。在此场景中，仅基于 VTI 配置了 BGP。

- 已修复问题 2288509：Tier-0/Tier-1 服务接口（集中式服务端口）不支持 MTU 属性
Tier-0/Tier-1 服务接口（集中式服务端口）不支持 MTU 属性。
- 已修复问题 2266553：在 NSX 设备中，服务在首次引导时可能无法初始化
部署的节点无法处理请求，或者无法形成集群。
- 已修复问题 2267632：丢失 GI 保护配置
在策略 UI 上发布的客户机保护规则显示成功。行为中的相应变化不反映在客户机虚拟机上。同时 OpsAgent 日志显示重新启动。失去客户机虚拟机保护。
- 已修复问题 2288773：旧的 TLS 协议 API 仍然可用，但会被覆盖
NSX-T 提供了用于设置 NSX TLS 协议版本和密码套件的新 API，可更新 NSX-T 集群中的所有节点。但是，旧的 API 仍然可用。虽然可以使用，但新设置将被全局设置覆盖。
- 已修复问题 2269901：在数据包捕获 CLI 中不包含 vmk 接口
无法发出此命令。
- 已修复问题 2304571 - 在使用 VDR 运行 L3 流量时，可能会出现严重错误 (PSOD)。
在某些情况下，未正确保护挂起的 arp(ND) 条目，这可能会导致严重错误 (PSOD)。
- 已修复问题 2275985：未连接到逻辑交换机的 vNIC 列为 NS 组直接成员的选项
未连接到逻辑交换机的 vNIC 添加为 NS 组的直接成员。操作成功，但应用于该组的策略不对 vNIC 实施。
- 已修复问题 2279973：如果创建空白组并继续执行升级，则在 MP 升级后，该空白组显示为未启动
如果创建空白组并继续执行升级，将出现此问题。
- 已修复问题 2282389：如果在集群之间移动 ESX，UC 升级计划与 VC 集群成员资格不同步
将 ESX 从一个集群移至 VC 中的另一个集群时，更改不反映在 UC 升级计划中。如果用户选择跨组“并行升级”，这可能会导致多个主机同时进入维护模式。
- 已修复问题 2288921：添加旧版本的 Edge 节点时，升级状态将不同步
如果用户在 Edge 升级之后添加旧版本的 Edge 节点，升级状态将不同步。这会导致继续执行升级调用时出现问题。
- 已修复问题 2289278：策略 API 出现错误，但允许为使用相同池的多个虚拟服务器配置不同的持久性
配置文件
系统不支持为包含不同 LbVirtualServer 的相同池配置有冲突的持久性类型。但是，策略无法正确验证/拒绝有冲突的输入，并允许配置。随后，策略显示包含错误消息的警报。
- 已修复问题 2289984：即使在主机上停止 nsx-context-mux 服务之后，mux_connectivity_status 仍然显示为“已连接”
当 nsx-context-mux 或 nsx-opsagent 未在主机上运行时，系统（NSX 界面或服务实例 API）会错误地将解决方案状态和 GI 代理状态显示为正在运行且时间戳无变化。因此，客户机虚拟机可能会失去 AV 保护。
- 已修复问题 2290083：创建基于 VLAN 的分段时缺少验证
使用 VLAN ID 属性指定 VLAN 传输区域时，系统无法验证，也无法发现此错误。因此，意向将在实现过程中失败，并引发错误。
- 已修复问题 2290669：随着虚拟服务器数量的增加，每个虚拟服务器的配置时间也会增加
随着虚拟服务器数量的增加，由于需要大量验证，每个虚拟服务器的配置时间也会增加。对于前 100 个虚拟服务器，平均响应时间大约为 1 秒。250 个虚拟服务器之后，平均响应时间增加到 5-10 秒。450 个虚拟服务器之后，平均响应时间增加到约 30 秒。
- 已修复问题 2291625：升级计划同步后，PCG 升级状态从 SUCCESS 更改为 NOT_STARTED

仅当用户升级 PCG，然后尝试之后升级更多的代理/PCG时，才会遇到此问题。
在建议的工作流中，PCG 升级后，不再有需要通过 UC 接口进行升级的跨云组件。

这不会影响任何功能。以前成功完成的 PCG 升级状态在升级 UI 上显示为“无”。

- 已修复问题 2291872：在防火墙规则中使用 TFTP 服务时，日志消息显示一条警告消息
在防火墙规则中使用 TFTP 服务时，日志消息将显示无关紧要的警告消息。ESXi 节点上的日志位置：`/var/log/cfgAgent.log`。
- 已修复问题 2292096：CLI 命令“`get service router config route-maps`”返回空的输出
即使配置了 route-map，CLI 命令“`get service router config route-maps`”也返回空的输出。这只是一个显示问题。
- 已修复问题 2292526：添加主机时显示“主机无法访问 (Host not reachable)”消息
添加 ESXi 主机时，显示“主机无法访问 (Host not reachable)”消息，但不会指定原因。可能的原因是凭据不正确。
- 已修复问题 2292701：用户无法更新绑定映射中的序列号
用户无法通过更新序列号更改应用于实体的配置文件的顺序或优先级。
- 已修复问题 2293227：升级到 2.4 后，IDFW 规则不适用于运行 VMTTools 10.3.5 的虚拟机
执行 NSX-T 实时升级后，IDFW 规则不适用于运行 VMTTools 10.3.5 的虚拟机，从而导致这些虚拟机可能失去 AV 保护。
- 已修复问题 2994002：Tier-1 未列在“Tier-0/Tier-1 网关”下拉列表中，无法供创建 DNS 转发器时进行选择
在包含数千条记录的大规模部署中，Tier-1 未列在“Tier-0/Tier-1 网关”下拉列表中，无法供在 DNS 转发器创建工作流中进行选择。因此，必须使用 API 配置 DNS 转发器创建。
- 已修复问题 2294345：在包含 ESXi 托管的虚拟机和 KVM 托管的虚拟机的组上运行 Application Discovery 分类可能会失败
仅 ESXi Hypervisor 支持 Application Discovery 功能。如果组中的虚拟机所在的混合主机包含不受支持的主机，则不保证 Application Discovery 分类结果。
- 已修复问题 2294821：NSX 设备信息显示在集群监控仪表板上并出现错误“无法删除节点 (failure to delete node)”，且未提供帮助用户处理此情况的指导。
用户尝试通过界面删除自动部署的节点且关闭该节点的电源失败后，会出现此问题。如果集群丢失一个节点，必须手动添加新节点并使用下面的解决办法清理配置状态。
- 已修复问题 2281095：将部署了 svm 的主机重新添加到同一集群中时，不会从 EAM 触发回调
所有客户机虚拟机可能不受保护。NSX UI 一直显示正在进行中状态。
- 已修复问题 2295564：从 2.3 升级到 2.4 后，Edge 节点控制器连接可能会断开
这是一个影响某些南北向流量的间歇性问题。
- 已修复问题 2296888：传输节点 (TN)/传输节点配置文件 (TNP) 配置不能既在主机交换机中将“仅迁移 PNIC”标记设置为 true，又填充了“用于安装的 VMK 映射”

如果在创建期间提供不匹配的配置（在主机交换机中将“仅迁移 PNIC”标记设置为 true，并填充了“用于安装的 VMK 映射”），则会出现以下异常：

主机 b17afc36-bbdc-491a-b944-21f73cf91585 的 VMK 迁移失败并显示错误

[com.vmware.nsx.management.switching.common.exceptions.SwitchingException: 将 ESX vmk 接口 null 迁移到 [null] 期间无法更新或删除传输节点 [TransportNode/b17afc36-bbdc-491a-b944-21f73cf91585]。 (错误代码: 9418) (VMK migration for host b17afc36-bbdc-491a-b944-21f73cf91585 failed with error [com.vmware.nsx.management.switching.common.exceptions.SwitchingException: TransportNode [TransportNode/b17afc36-bbdc-491a-b944-21f73cf91585] can not be updated or deleted while migrating ESX vmk interface null to [null].]. (Error code: 9418))。

如果在更新期间提供不匹配的配置，则会出现以下异常：

常规错误 (错误代码: 400) (General error (Error code: 400))。

如果应用的 TN/TNP 配置将“仅迁移 pNIC”标记设置为 true 并包含 vmk 迁移映射，则会出现异常。

- **已修复问题 2287124：**在 Microsoft Azure VNet 上部署 PCG 后，CSM 中的 VNet 磁贴错误地报告警告
在 Microsoft Azure VNet 上部署 PCG 后，CSM 中的 VNet 报告一个警告标志（带有感叹号的黄色三角形）。如果将鼠标悬停在警告图标上，CSM 将报告 MP（管理平面）和 CCP（控制平面）的状态为“未知”。不过，连接可能不存在任何问题，而只是错误地显示警告。
- **已修复问题 2273651 -**在删除传输节点后，用户无法通过 SSH 访问主机。
在 KVM 实施中观察到该问题。用户删除一个传输节点，并收到一条消息以指示删除成功。不过，用户之后无法通过 SSH 访问同一主机。该问题可能是由于存在不是由 NSX-T 管理的开放虚拟交换机 (OVS) 造成的，该交换机可能是作为 KVM 模板的一部分预装的。
- **已修复问题 2297157 -**负载均衡 HTTPS 性能受 FIPS 模式的影响。
如果启用了默认 FIPS 模式，负载均衡性能可能会受到不利的影响。
- **已修复问题 2290688 -**在 AWS 中升级 Windows 2016 虚拟机失败。
AWS 中的多个 Windows 工作负载虚拟机升级失败。在 AWS 门户中显示的虚拟机升级状态停滞为“1/2 检查”。重试也会失败。仅在相同的 NSX-T 版本升级中观察到该问题。
- **已修复问题 2203863 -**UDP 和 ICMP 流量不支持身份防火墙规则。
身份防火墙规则不适用于 ping 测试。仅 TCP 流量支持当前功能。
- **已修复问题 2248186 -**BGP 路由器安装来自邻居的 IPv6 路由，并将自己的接口作为下一跃点。
因此，安装的路由的 IPv6 转发可能会失败并导致转发循环。
- **已修复问题 2281537 -**在迁移后，具有多 VTEP 的 ESXi 传输节点无法启动 BFD 会话。
在将 NSX-V 节点迁移到 NSX-T 后，具有多 VTEP 的 ESXi 传输节点无法在到 Edge 节点的所有 VTEP 上启动 BFD 会话。
- **已修复问题 2297918 -**从 2.3.1 升级到 2.4 后，无法从集群中移除 NSX。
将集群从 2.3.1 升级到 2.4 后，无法移除 NSX-T 并显示以下消息：“无法在集群上移除 NSX: 此 Fabric 模板存在相关的传输节点模板或传输节点集合。必须删除传输节点模板或传输节点集合，才能对此 Fabric 模板执行删除/禁用操作。” (Failed to remove NSX on the cluster: Related transport node template or transport node collection exists for this fabric template. Transport node template or transport node collection must be deleted before a delete/disable on this fabric template.)
- **已修复问题 2298499 -**如果部署没有公共 IP 的公有云网关，网关和对等主机之间的 VPN 将失败。
如果在上行链路上部署没有公共 IP 地址的公有云网关 (PCG)，则无法在 PCG 和对等主机之间建立 VPN 隧道。原因是 PCG 默认对 VPN 流量执行 SNAT。
- **已修复问题 2316831 -**即使禁用了 ECMP，也始终对 IPv6 流量进行共享负载。

从策略中禁用 ECMP 对 IPv6 单播地址系列无效（但对 IPv4 单播地址系列有效）。

- 已修复问题 2334515 - T0-T1 路由器链路端口无法使用 IPv4 链路本地范围 (169.254.0.0/16)。T0_t1 路由器链路端口无法使用 IPv4 链路本地范围 (169.254.0.0/16)。但是，T0_t1 路由器链路可以使用不是 IPv4 链路本地地址范围 (169.254.0.0/16) 的 IP 范围。
- 已修复问题 2339832：无法应用节点证书或无法使用 CA 签名证书设置集群证书。这将导致显示消息“更新证书使用情况时出错 (Error updating certificate usage)。”或“设置集群证书时出错 (An error occurred setting the cluster certificate)。”反复应用证书以及在节点证书和集群证书之间进行切换后，可能会出现此错误。将不会正确应用证书，并且通过 VIP 的 REST API 调用可能无法再正常工作。日志位置：/var/log/proton/nsxapi.log。

如果在升级到 2.4.1 之前遇到此错误，请改用自签名证书。

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](#)
- [逻辑网络已知问题](#)
- [安全服务已知问题](#)
- [负载均衡器已知问题](#)
- [解决方案互操作性已知问题](#)
- [运行和监控服务已知问题](#)
- [升级已知问题](#)
- [API 已知问题](#)
- [NSX Cloud 已知问题](#)

一般已知问题

- 问题 2239365：出现“未经授权 (Unauthorized)”错误
导致出现此错误的原因可能是用户尝试在同一类型的浏览器上打开多个身份验证会话。因此，登录将失败并显示以上错误，并且无法进行身份验证。日志位置：/var/log/proxy/reverse-proxy.log
/var/log/syslog

解决办法：关闭所有打开的身份验证窗口/选项卡，然后重新尝试执行身份验证。

- 问题 2252487：并行添加多个传输节点 (TN) 时，不会保存 BM Edge 传输节点的 TN 状态
传输节点状态在 MP UI 中显示不正确。

解决办法：

1. 重新启动 proton，所有传输节点状态会正确更新。
2. 或者，使用 API `https://<nsx-manager>/api/v1/transport-nodes/<node-id>/status?source=realtime` 查询传输节点状态。

- 问题 2256709：即时克隆虚拟机或从快照恢复的虚拟机会在 vMotion 期间短暂失去 AV 保护
恢复虚拟机快照并将虚拟机迁移到另一台主机。合作伙伴控制台不显示已迁移即时克隆虚拟机的 AV 保护。
将短暂失去 AV 保护。

解决办法：无。

- 问题 2261431：根据其他部署参数，需要筛选的数据存储列表
如果选择了不正确的选项，UI 上将显示相应的错误。客户可以删除此部署并创建新部署以从错误中恢复。

解决办法：如果创建的是集群部署，请选择共享数据存储。

- 问题 2274988：服务链不支持来自同一服务的连续服务配置文件

流量不会遍历服务链，只要链上包含两个属于同一服务的连续服务配置文件，流量就会丢弃。

解决办法：添加来自不同服务的服务配置文件，以确保没有两个连续的服务配置文件属于同一服务。或者，定义第三个服务配置文件，用于执行串连在一起的两个原始配置文件的相同操作，然后在服务链中仅使用这第三个配置文件。

- 问题 2275285：在第一个请求完成且集群稳定之前，节点发出第二个加入同一集群的请求
集群可能无法正常运行，且 CLI 命令 `get cluster status`、`get cluster config` 可能返回错误。

解决办法：在发出第一个加入请求之后，请勿在 10 分钟内发出加入同一集群的任何新的加入命令。

- 问题 2275388：环回接口/已连接的接口路由可能会在添加筛选器以拒绝路由之前重新分发
不必要的路由更新可能会导致数秒到数分钟的流量分流。

解决办法：无。

- 问题 2275708：当证书的私钥具有密码短语时，无法导入包含此私钥的证书
返回消息“收到的证书 PEM 数据无效。(错误代码: 2002) (Invalid PEM data received for certificate. (Error code: 2002))”。无法导入包含私钥的新证书。

解决办法：

1. 创建包含私钥的证书。系统出现提示时，不要输入新密码短语，而是按 Enter。
2. 选择“导入证书”，然后选择证书文件和私钥文件。

可通过打开密钥文件进行验证。如果生成密钥时输入了密码短语，文件中的第二行将显示如下类似内容：“Proc-Type: 4,ENCRYPTED”。

如果生成密钥文件时没有输入密码短语，将缺少此行。

- 问题 2277742：如果 NSX-T Manager 设备配置了完全限定域名 (FQDN) 而不仅仅是主机名，则调用
请求正文中将 `publish_fqdns` 设置为 `true` 的 PUT `https://<MGR_IP>/api/v1/configs/management`
可能会失败

如果配置了 FQDN，则无法调用 PUT `https://<MGR_IP>/api/v1/configs/management`。

解决办法：使用主机名（而非 FQDN）部署 NSX Manager。

- 问题 2279249：即时克隆虚拟机会在 vMotion 期间短暂失去 AV 保护

即时克隆虚拟机从一个主机迁移到了另一个主机。迁移后，`eicar` 文件便立即留在虚拟机上。将短暂失去 AV 保护。

解决办法：无。

- 问题 2292116：通过 IPFIX L2 页面创建组时，包含基于 CIDR 的 IP 地址组的 IPFIX L2 应用对象未在 UI 中列出

如果尝试从“应用对象”对话框创建一个 IP 地址组，则在“设置成员”对话框中输入错误的 IP 地址或 CIDR 时，这些成员不会列在组下。必须再次编辑该组以输入有效的 IP 地址。

解决办法：转到组列表生成页面，并在该组中添加 IP 地址。然后，该组会填充到“应用对象”对话框中。

- 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 2268406 - 在添加了最大数量的标记时，“标记定位点”对话框不显示所有标记。
在添加了最大数量的标记时，“标记定位点”对话框不会显示所有标记，也无法调整对话框大小或滚动查看。不过，用户仍然可以在“摘要”页面中查看所有标记。不会丢失任何数据。

解决办法：在“摘要”页面中查看标记。

- 问题 2310650 - 界面显示“请求超时” (Request timed out) 错误消息。
界面上的多个页面显示以下消息：“请求超时。在系统具有较高负载或资源不足时，可能会出现这种情况” (Request timed out. This may occur when system is under load or running low on resources)

解决办法：使用 SSH 登录到 NSX Manager 虚拟机，并运行“start search resync manager” CLI 命令。

- 问题 2320529 - 为新添加的数据存储添加第三方虚拟机后，出现“服务部署无法访问存储” (Storage not accessible for service deployment) 错误。
为新添加的数据存储添加第三方虚拟机后，即使可以从集群上的所有主机中访问存储，也会出现“服务部署无法访问存储” (Storage not accessible for service deployment) 错误。该错误状态持续长达三十分钟的时间。

解决办法：在三十分钟后重试。作为替代方法，进行以下 API 调用以更新数据存储的缓存条目：

`https://{NsxMgrIP}/api/v1/fabric/compute-collections/<CC Ext ID>/storage-resources?`

`uniform_cluster_access=true&source=realtime`

其中，NsxMgrIP 是服务部署 API 失败的 NSX Manager 的 IP 地址，CC Ext ID 是集群中正在尝试执行部署的 NSX 标识符。

- 问题 2320855 - 如果用户未单击“添加/检查”按钮，则不会创建新的虚拟机安全标记。
界面问题。如果用户将新的安全标记添加到策略对象或清单中，然后单击保存而未先单击标记范围对字段旁边的添加/检查按钮，则不会创建新的标记对。

解决办法：在单击保存之前，请务必单击添加/检查按钮。

- 问题 2328126 - 裸机问题：在 NSX 上行链路配置文件中使用时，Linux OS 绑定接口返回错误。
如果在 Linux OS 中创建一个绑定接口，然后在 NSX 上行链路配置文件中使用该接口，将会看到以下错误消息：“创建传输节点可能会失败” (Transport Node creation may fail)。出现该问题是因为，VMware 不支持 Linux OS 绑定。不过，VMware 在裸机服务器传输节点中支持 Open vSwitch (OVS) 绑定。

解决办法：如果遇到该问题，请参见知识库文章 67835 [裸机服务器在 NSX-T 传输节点配置中支持 OVS 绑定](#)。

- 问题 2334442：在重命名管理员用户后，用户没有编辑或删除创建的对象权限
在重命名管理员用户后，用户没有编辑或删除创建的对象权限。无法重命名管理员/审核员用户。

解决办法：在重命名后，执行“service nsx-policy-manager restart”命令以重新启动策略。

- 问题 2261818：从 eBGP 邻居学习的路由重新通告到同一邻居
启用 BGP 调试日志将指示正在重新接收数据包，丢弃数据包并显示错误消息。在丢弃发送到对等项的更新消息时，BGP 进程将消耗额外的 CPU 资源。如果具有大量路由和对等项，这可能会影响路由聚合。

解决办法：无。

- 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。

NSX Manager 已知问题

- 问题 2282798 - 如果尝试在 NSX Manager 中同时注册请求/主机太多，主机注册可能会失败。该问题导致 Fabric 节点处于“失败”状态。Fabric 节点状态 API 调用显示“客户端尚未对检测信号做出响应” (Client has not responded to heartbeats yet)。主机上的 /etc/vmware/nsx-mpa/mpaconfig.json 文件也是空的。

解决办法：使用以下过程从该问题中恢复。

1. 使用“解决程序”选项。
2. 从 NSX 中删除结构层节点。
3. 通过 CLI 命令“join management-plane”手动重新添加结构层节点。

NSX Edge 已知问题

- 问题 2283559：如果 Edge 的 RIB 包含 65k 多个路由且 FIB 包含 100k 多个路由，则 /routing-table 和 /forwarding-table MP API 会返回错误。如果 Edge 的 RIB 包含 65k 多个路由且 FIB 包含 100k 多个路由，从 MP 到 Edge 的请求将耗时 10 秒以上，从而导致超时。这是只读 API，仅当需要使用 API/UI 下载 RIB 中的 65k 多个路由和 FIB 中的 100k 多个路由时才会产生影响。

解决办法：获取 RIB/FIB 有两种方案可供选择。

- 这些 API 支持基于网络前缀或路由类型的筛选选项。可使用这些选项下载感兴趣的路由。
- CLI 支持需要整个 RIB/FIB 表的情况，且无超时。

- 问题 2204932 - 配置 BGP 对等连接可能会延迟 HA 故障切换恢复。

如果在与 T0 Edge 对等的路由器上配置动态 BGP 对等连接，并且在 Edge（活动-备用模式）上发生故障切换事件，可能需要长达 120 秒的时间才能建立 BGP 邻居关系。

解决办法：配置特定的 BGP 对等项以防止延迟。

- 问题 2285650 - 在 BGP 路由表中填充了不需要的路由。

如果将 allowas-in 选项作为 BGP 配置的一部分启用，将重新接收 Edge 节点通告的路由并将其安装在 BGP 路由表中。这会导致过多的内存消耗和路由计算处理。如果为过多的路由配置了较高的本地优先级，该转发循环可能会导致在某些路由器上的路由表中填充多余的路由。

例如，路由 X 来自路由器 D，将向路由器 A 和 B 通告该路由。启用了 allowas-in 的路由器 C 将与 B 对等互连，因此，它学习路由 X 并将该路由安装在其路由表中。因此，现在通过两个路径向路由器 C 通告路由 X，从而导致该问题。

解决办法：您可以配置有问题的路由器（或其对等项）以阻止重新向其通告路由，从而防止发生转发循环。

逻辑网络已知问题

- 问题 2243415：客户无法使用逻辑交换机（作为管理网络）部署 EPP 服务。在 EPP 部署屏幕上，用户在网络选择控件中看不到逻辑交换机。如果对显示为管理网络的逻辑交换机直接使用 API，用户将看到以下错误：“服务部署无法访问指定的网络 (Specified Network not accessible for service deployment)。”

解决办法：使用其他类型的交换机（如本地交换机或分布式交换机）进行部署。

- 问题 2288774：由于标记超过 30 个（错误），分段端口出现实现错误

用户输入错误地尝试应用 30 多个标记。但是，策略工作流不正确验证/拒绝用户输入，并允许配置。然后，策略显示警报，其中包含正确的错误消息，即用户不应使用 30 个以上的标记。此时，用户可以更正此问题。

解决办法：显示错误后更正配置。

- 问题 2275412：端口连接不能跨多个 TZ 工作
端口连接只能在单个 TZ 中使用。

解决办法：无。

- 问题 2320147 - 在受影响的主机上缺少 VTEP。
如果在同一事务中移除并重新添加了 LogSwitchStateMsg，并且中央控制平面在管理平面发送逻辑交换机之前处理该操作，则不会更新逻辑交换机状态。因此，流量无法流入或流出缺少的 VTEP。

解决办法：如果遇到该问题，请重新启动中央控制平面。

- 问题 2327904 - 在将预创建的 Linux 绑定接口作为上行链路后，流量不稳定或失败。
NSX-T 不支持将预创建的 Linux 绑定接口作为上行链路。

解决办法：对于上行链路，请使用上行链路配置文件中的 OVS 本机绑定配置。

- 问题 2295819 - 即使 Edge 虚拟机处于活动状态并且 PNIC 处于“已启动”状态，L2 网桥也会停滞在“已停止”状态。
即使 Edge 虚拟机处于活动状态并且支持 L2 网桥端口的 PNIC 处于“已启动”状态，L2 网桥也可能会停滞在“已停止”状态。这是因为 Edge LCP 无法在其本地缓存中更新 PNIC 状态，从而假定 PNIC 已关闭。

对客户的影响：

可通过 Edge L2 网桥端口访问的虚拟机的流量中断

解决办法：在受影响的 Edge 虚拟机上重新启动本地控制代理。

- 问题 2392093：由于 RPF 检查而丢失流量
如果流量通过 T0 下行链路环回，并且 Tier-0 和 Tier-1 路由器位于同一 Edge 节点上，则 RPF 检查可能会导致流量丢失。

解决办法：无。

安全服务已知问题

- 问题 2395334 - (Windows) 由于无状态防火墙规则连接跟踪条目导致错误丢弃数据包。
在 Windows 虚拟机上无法良好支持无状态防火墙规则。

解决办法：改为添加有状态防火墙规则。

- 问题 2458384 - NSX-T Manager 界面页面无法加载，出现 403 错误。
在发行版本 2.4.0 和 2.4.1 中发现此问题。此问题会同时影响管理员登录和 Identity Manager 登录。NSX-T Manager 的 FQDN 使用 *.SLD.TLD 格式。例如：*.co.uk、*.co.il、*.com.au 等。

解决办法：使用短名称或 IP（而不是 FQDN）访问 NSX-T Manager UI。请参见[知识库文章 71217](#)。

- 问题 2296430 - 在生成证书期间，NSX-T Manager API 不提供主体备用名称。
NSX-T Manager API 不提供主体备用名称以颁发证书，尤其是在生成 CSR 期间。

解决办法：使用支持这些扩展的外部工具创建 CSR。从证书颁发机构收到签名证书后，使用 CSR 中的密钥将其导入到 NSX-T Manager。

- 问题 2294410 - L7 防火墙检测到某些应用程序 ID。

检测到的以下 L7 应用程序 ID（基于端口而不是应用程序）：SAP、SUNRPC 和 SVN。以下 L7 应用程序 ID 不受支持：AD_BKUP、SKIP 和 AD_NSP。

解决办法：无。这对客户没有任何影响。

- 问题 2314537 - 在更新 vCenter 证书和指纹后，连接状态为“关闭”。
vCenter 中的新更新没有与 NSX 同步，并且从 vCenter 中提取数据的所有按需查询将失败。用户无法部署新的 Edge/服务虚拟机。用户无法准备在 vCenter 中添加的新集群或主机。日志位置：NSX Manager 节点上的 /var/log/cm-inventory/cm-inventory.log 和 /var/log/proton/nsxapi.log。

解决办法：登录到每个 NSX Manager 虚拟机，并切换到 root 用户。在每个 Manager 节点上运行“/etc/init.d/cm-inventory restart”命令。

负载均衡器已知问题

- 问题 2290899：IPSec VPN 不起作用，IPSec 的控制平面实现失败
如果在同一 Edge 节点的 Tier-0 上与 IPSec 服务一起启用 62 个以上的 LbServer，则 IPSec VPN（或 L2VPN）将无法启动。

解决办法：将 LbServer 数量减少到 62 以下。

- 问题 2318525 - 作为 eBGP 对等项 IP 地址的下一跃点 IPv6 路由更改为自己的 IP。
对于 eBGP IP4 会话，如果通告的 IPv4 路由将 eBGP 对等项作为下一跃点，路由的下一跃点不会在发送端更改为自己的 IP 地址。这适用于 IPv4 会话，但对于 IPv6 会话，路由的下一跃点在发送端更改为自己的 IP 地址。该行为可能会导致路由循环。

解决办法：无。

- 问题 2362688：如果负载均衡器服务中的某些池成员已关闭，则 UI 会将合并状态显示为“已启动”
当池成员已关闭时，池状态为绿色且“已启动”的策略 UI 上没有任何相应指示。

解决办法：无。

解决方案互操作性已知问题

- 问题 2289150：对 AWS 的 PCM 调用失败
如果将 CSM 上 AWS 帐户的 PCG 角色从 *old-pcg-role* 更新为 *new-pcg-role*，则 CSM 会将 AWS 上 PCG 实例的角色更新为 *new-pcg-role*。但是，PCM 不知道 PCG 角色已经更新，因此继续使用通过 *old-pcg-role* 创建的旧 AWS 客户端。这会导致 PCM AWS 云清单扫描和其他 AWS 云调用失败。

解决办法：如果遇到此问题，请在更改为新角色至少 6.5 小时内，不要立即修改/删除旧的 PCG 角色。重新启动 PCG 将使用新的角色凭据重新初始化所有 AWS 客户端。

运行和监控服务已知问题

- 问题 2316943 - 在 vMotion 期间，工作负载在短时间内未受到保护。
执行 vMotion 后，VMware Tools 需要几秒钟才能报告虚拟机的正确计算机名称。因此，执行 vMotion 后，使用计算机名称添加到 NS 组的虚拟机在几秒钟内不受保护。

解决办法：要在 DFW 规则中使用组，请使用基于虚拟机名称的条件，而不是使用基于计算机名称的条件。

- 问题 2331683 - 高级 UI 上的添加负载均衡器表单不显示 2.4 版的更新容量。
在打开添加负载均衡器表单时，高级 UI 上显示的规格容量没有根据 2.4 版进行更新。显示的容量来自于以前的版本。

解决办法：无。

升级已知问题

- 问题 2286030 - 从 NSX-T 2.3.x 及更低版本升级到 2.4.x 时，传输节点配置显示处于失败状态。
从 NSX-T 2.3.x 及更低版本升级到 2.4.x 时，由于出现空指针异常，传输节点配置进入失败状态。如果您的 ESXi 传输节点上的 VMkernel 适配器已迁移到 N-VDS VLAN 逻辑交换机，之后从 NSX-T 2.3.x 升级到 NSX-T 2.4.x，则可能会发生争用情况，从而导致 ESXi 传输节点配置状态显示为失败。但是，在升级过程中，ESXi 传输节点与 NSX Manager 和控制器的连接仍保持完好，即使节点标记为配置状态失败也是如此。

解决办法：更新或重新发送传输节点以将配置状态重置为成功。

1. 从 NSX Manager 中，编辑显示为失败的 ESXi 传输节点。
2. 在 ESXi 传输节点配置弹出窗口中，单击保存。
此操作将重置状态。您无需修改配置。

- 问题 228549：清单文件的校验和错误导致 RepoSync 失败
在最近升级到 2.4 的部署中观察到此情形。当在全部部署的管理器上备份并还原升级的设置时，数据库中存在的存储库清单校验和与实际清单文件的校验和不匹配。这会导致在备份还原之后将 RepoSync 标记为失败。

解决办法：要从此失败中恢复，请执行以下步骤：

1. 运行 CLI 命令 `get service install-upgrade`
记下结果中 “Enabled on” 的 IP。
2. 登录到在上述命令返回的 “Enabled on” 中显示的 NSX Manager IP。
3. 导航到系统 > 概览，并找到具有 IP 与返回的 “Enabled on” 相同的节点。
4. 在该节点上单击解决。
5. 上述解决操作成功后，在同一界面中的所有节点上单击解决。
所有三个节点现在将 RepoSync 状态显示为完成。

- 问题 2277543 - 在就地升级期间，主机 VIB 更新失败并显示 “在主机上安装脱机包失败” 错误。
在运行 ESXi-6.5P03（内部版本 10884925）的主机上执行从 NSX-T 2.3.x 到 2.4 的就地升级之前，在主机上执行存储 vMotion 时，可能会出现该错误。如果就在主机升级之前执行存储 vMotion，则不会移除 2.3.x 中的交换机安全模块。存储 vMotion 触发内存泄漏，从而导致交换机安全模块卸载失败。

解决办法：请参阅知识库文章 67444 [从 NSX-T 2.3.x 升级到 NSX-T 2.4.0 时，如果在主机升级之前对虚拟机进行存储 vMotion，主机 VIB 更新可能会失败。](#)

- 问题 2276398 - 在使用 NSX 升级 AV 合作伙伴服务虚拟机时，最多可能在 20 分钟内未提供保护。
在升级合作伙伴 SVM 时，将部署新的 SVM 并删除旧 SVM。可能会在主机 syslog 上显示 SolutionHandler 连接错误。

解决办法：在升级后，删除主机上的 ARP 缓存条目，然后 ping 主机上的合作伙伴控制 IP 以解决该问题。

- 问题 2330417 - 无法继续升级未升级的传输节点。
在升级时，即使未升级某些传输节点，也会将升级标记为成功。日志位置：/var/log/upgrade-coordinator/upgrade-coordinator.log。

解决办法：重新启动升级协调器服务。

API 已知问题

- 问题 2260435 - 默认情况下，API 创建无状态重定向策略/规则，东西向连接不支持该策略/规则。
默认情况下，API 创建无状态重定向策略/规则，东西向连接不支持该策略/规则。因此，不会将流量重定向到合作伙伴。

解决办法：在使用策略 API 创建重定向策略时，请创建有状态区域。

- 问题 2332397 - API 允许在不存在的域中创建 DFW 策略。
在不存在的域上创建此类策略后，当用户打开 DFW 安全选项卡时，界面变得无响应。相关的日志为 /var/log/policy/policy.log。

解决办法：使用相同的 ID 创建在其中创建策略的域。这样，验证就会成功。

NSX Cloud 已知问题

- 问题 2275232：如果 DFW 的 Connectivity_statregy 从黑名单更改为白名单，DHCP 将不适用于云中的虚拟机

请求新 DHCP 租约的所有虚拟机将丢失 IP。需要在 DFW 中针对云虚拟机明确允许 DHCP。

解决办法：在 DFW 中针对云虚拟机明确允许 DHCP。

- 问题 2277814：如果 nsx.network 标记的值无效，则虚拟机移至 vm-overlay-sg
具有无效 nsx.network 标记的虚拟机将移至 vm-overlay-sg。

解决办法：移除无效的标记。