



VMware NSX-T Data Center 2.5 发行说明

VMware NSX-T Data Center 2.5 | 2019 年 9 月 19 日 | 内部版本 14663974

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](#)
- [常规行为变化](#)
- [API 弃用和行为变化](#)
- [本地化语言](#)
- [API 和 CLI 资源](#)
- [修订历史](#)
- [已解决的问题](#)
- [已知问题](#)

新增功能

NSX-T Data Center 2.5 针对私有云、公有云和混合云的虚拟化网络和安全引入了各种新功能。新功能主要包括增强了基于意图的网络用户界面、上下文感知防火墙、客户机和网络侦测功能、IPv6 支持、高可用性集群管理、针对 vSphere 计算集群的基于配置文件的 NSX 安装，以及用于从 NSX Data Center for vSphere 迁移至 NSX-T Data Center 的迁移协调器增强功能。

NSX Intelligence

NSX-T Data Center 2.5 引入了 NSX Intelligence V1.0，这是一个全新的 NSX 分析组件。NSX Intelligence 通过 NSX Manager 中的单一管理窗格提供用户界面，并提供下列功能：

- 针对环境内工作负载的近乎实时的流量信息。
- NSX Intelligence 可将实时流量或历史流量、用户配置和工作负载清单关联在一起。
- 支持查看有关流量、用户配置和工作负载清单的以往信息。
- 通过提供防火墙规则、分组和服务建议自动执行微分段规划。

容器 API 支持

为容器清单提供了全新的 API 支持。请参见 API 文档。

L2 网络

- **对 Edge 网桥的增强功能** - Edge 网桥现在允许将同一个分段连接到多个网桥配置文件，因此能够将单个分段多次桥接到物理基础架构中的 VLAN。此新功能取代并淘汰了先前版本 NSX-T Data Center 中的原始 ESXi 网桥。注意：使用此功能的风险由您自行承担。它会将同一个分段两次桥接到物理网络中的同一个 L2 域，这可能导致出现桥接循环风险。不存在循环缓解机制。

- **MTU/VLAN 运行状况检查** - 从操作角度来看，通常难以识别因配置错误导致的网络连接问题。一种常见的情形是，虚拟网络管理员使用 NSX Manager，而物理网络管理员具有物理网络交换机的管理所有权。
 - **VLAN 运行状况检查** - 检查 N-VDS VLAN 设置与相邻物理交换机端口上的中继端口配置是否匹配。
 - **MTU 运行状况检查** - 检查基于每个 VLAN 的物理访问交换机端口 MTU 设置与 N-VDS MTU 设置是否匹配。
- **客户机 VLAN 间标记** - 增强型数据路径 N-VDS 使用户能够将客户机 VLAN 标记映射到分段。该功能克服了每个虚拟机 10 个 vNIC 的限制，允许 NSX 基础架构路由客户机 VLAN 标记的流量（已映射到不同分段）。

L3 网络

- **Edge 集群内部基于故障域的 Tier-1 放置** - 支持 NSX-T 基于用户定义的故障域自动放置 Tier-1 网关。这提高了 Tier-1 网关在不同可用性区域、机架或主机间的可靠性，即使使用自动 Tier-1 网关放置也如此。
- **ECMP 拓扑中发生路由器故障后的非对称负载共享** - 在活动/活动 Tier-0 网关上，当一个故障服务路由器停止运行，另一个路由器接管该故障路由器流量时，会导致经过此服务路由器的流量翻倍。发生路由器故障 30 分钟后，会从下一跃点列表移除故障路由器 IP 地址，从而避免额外流量进入特定路由器。
- **通过 API 获取每个 BGP 对等体已通告和已接收的路由** - 避免使用 CLI 来验证已接收及发送给 BGP 对等体的路由，从而简化 BGP 操作。
- **BGP 大型社区支持** - 提供将社区属性与 4 字节 ASN 配合使用（按 RFC8092 定义）的选项。
- **BGP 平滑重启帮助程序方式选项（按对等体）** - 为 Tier-0 网关提供相关选项，帮助针对北向物理路由器通过冗余控制平面维护路由器，而不会延长 Tier-0 路由器之间的故障转移时间。
- **批处理 API 用于创建多项 NAT 规则** - 增强现有 NAT API，以将大量 NAT 规则的创建过程绑定到单个 API 调用中。

Edge 平台

- **在裸机 Edge 节点上支持 Mellanox ConnectX-4 和 ConnectX-4 LX** - 裸机 Edge 节点现在支持 Mellanox ConnectX-4 和 ConnectX-4 LX 物理网卡 (10/25/40/50/100 Gbps)。
- **裸机 Edge PNIC 管理** - 提供选择物理网卡以用作数据平面网卡（快速路径）的选项。它还可将裸机 Edge 节点上支持的物理网卡数量从 8 个 PNIC 增加到 16 个 PNIC。

增强 IPv6 支持

NSX-T 2.5 继续增强 IPv6 路由/转发功能集。这包括对以下项的支持：

- IPv6 SLAAC（无状态地址自动配置），自动为虚拟机提供 IPv6 地址。
- IPv6 路由器通告，NSX-T 网关通过路由器通告提供 IPv6 参数。
- IPv6 DAD，NSX-T 网关可检测重复的 IPv6 地址分配。

防火墙改进

第 7 层 AppID 支持

NSX-T 2.5 为分布式防火墙和网关防火墙提供更多第 7 层功能。这包括对以下项的支持：

- KVM 上对分布式防火墙的第 7 层 AppID 支持。
- 适用于网关防火墙的第 7 层 AppID 支持。
- 单条防火墙规则中包含多种第 7 层 AppID 配置。

FQDN/URL 筛选增强功能

NSX-T 2.5 对 FQDN 筛选支持提供了少量增强功能，包括：

- 为 DNS 条目配置 TTL 定时器。
- 支持在 KVM Hypervisor 上运行的工作负载。

通过以下功能增强了防火墙操作：

- 自动保存配置和回滚功能 - 系统会在发布配置时创建配置副本。此配置可重新部署，以便回滚到现有状态。
- 手动草稿 - 用户现在可以先保存规则草稿，然后再发布这些规则集以进行实施。用户可以在手动草稿中转储规则。系统允许您让多位用户处理同一个草稿，并采用锁定机制以禁止不同用户覆盖规则。
- 会话定时器 - 用户可以为 TCP、UDP 和 ICMP 会话配置会话定时器。
- 泛洪保护 - 分布式防火墙和网关防火墙均可采用 SYN 泛洪保护。用户可以提供警示、记录和丢弃流量阈值，以生成自定义工作流程。
- 创建 NSX 负载均衡器和部署虚拟服务器时，系统会自动生成两个组。其中一组包含服务器池，而另一组包含虚拟服务器 IP。这些组可在分布式防火墙或网关防火墙上用于允许或拒绝防火墙管理员的通信。这些组可跟踪 NSX 负载均衡器配置更改。
- 按虚拟机 vNIC 检测到的 IP 地址数量已从 128 个 IP 地址增加到 256 个 IP 地址。

身份防火墙

- 在 NSX-T 2.5 中，支持在 Windows 2016 上部署的 Active Directory 服务器。
- 针对 Windows Server 工作负载支持身份防火墙，无需启用终端服务。这样允许客户严格控制管理员从一台服务器横向迁移到另一台服务器。

服务插入

- 数据包复制支持 - 除了通过服务来重定向流量外，NSX-T 现在支持网络监控用例，其中数据包副本将转发至伙伴服务虚拟机 (SVM)，从而允许在原始数据包未通过网络监控服务时检查、监控或收集统计信息。
- 基于主机的自动伙伴 SVM 部署 - 从 NSX-T 2.5 起，支持两种伙伴 SVM 部署模式，一种为集群部署，其中服务虚拟机部署在专用 vSphere（服务）集群中，另一种为基于主机的部署，其中每个服务的一个服务虚拟机部署在特定集群中的每个计算主机上。在此模式中，向集群添加新计算主机时，会自动部署相应的 SVM。
- 南北向服务插入的通知支持 - NSX-T 2.4 为东西向服务插入引入了通知框架，使伙伴服务能够在发生相关更改（例如，动态组更新）时自动接收通知。在 NSX-T 2.5 中，此通知框架已扩展至南北向服务插入。合作伙伴可以利用此机制来允许客户在合作伙伴策略中使用动态 NSX 组（即，基于标记、操作系统、虚拟机名称）。
- 其他故障排除和可视化功能 - 在 NSX-T 2.5 中，提供了多项可维护性增强功能，用于对服务插入相关问题进行更准确的故障排除。这包括验证服务实例的运行状态、通过 API 获取可用服务路径，以及在支持包中包含服务插入相关日志的功能。

端点保护（客户机侦测）

- Linux 支持 - 通过端点保护支持基于 Linux 的操作系统。请参见《NSX-T 管理指南》，了解支持客户机侦测的 Linux 操作系统。
- 端点保护仪表板 - 端点保护仪表板用于直观显示和监控受保护虚拟机和不受保护虚拟机的配置状态、主机代理和服务虚拟机问题，以及配置有文件侦测驱动程序（在 VMware Tools 安装过程中安装）的虚拟机。
- 监控仪表板 - 用于监控系统中各集群之间的伙伴服务部署状态。

负载均衡

- 用于检索负载均衡器的 Edge 容量状态的 API - 已添加新的 API 调用，以允许 admin 监控负载均衡实例方面的 Edge 容量。
- 智能选择运行状况检查 IP 地址 - 配置 SNAT IP 列表时，列表中首个 IP 地址将用于运行状况监控，而不是 Tier-1 网关的上行链路 IP 地址。此 IP 地址可与虚拟服务器 IP 地址相同。此增强功能允许负载均衡器对源 NAT 和运行状况监控使用单一 IP 地址。
- 负载均衡器日志记录增强功能 - 通过此增强功能，负载均衡器可以为每台要监控的虚拟服务器生成内容丰富的日志消息。例如，虚拟机服务器访问日志不仅包含客户端 IP 地址，还包含池成员 IP 地址。
- LB 规则中的持久增强功能 - LB 规则中引入了一项新操作，称为“持久”操作。“持久”操作支持负载均衡器基于池成员设置的 Cookie 提供应用程序持久性。
- LB 适应 - 可在小型 Edge 虚拟机中放入一个小型 LB 实例。可在中型 Edge 虚拟机中放入一个中型 LB 实例。原先，小型 Edge 虚拟机不支持负载均衡服务，因为 Edge 虚拟机的大小必须大于 LB 实例的大小。

- VS/池/成员统计信息 - 所有 LB 相关统计信息均可通过简化的界面来查看。原先此类信息只能在“高级网络和安全”界面中查看。
- 针对 SSL 终止的 ECC（椭圆曲线证书）支持 - EC 证书可用于提升 SSL 性能。
- FIPS 旋钮 - 通过 API 提供了一个全局设置，用于为负载均衡器配置 FIPS 合规性。默认情况下，将禁用该设置以提高性能。

VPN

- 对 Tier-1 网关的 IPsec VPN 支持 - 可在 Tier-1 网关上部署和终止 IPsec VPN，以实现更好的租户隔离和可扩展性。原先仅在 Tier-0 网关上受支持。
- 对 NSX 管理的 Edge 上第 2 层 VPN 的 VLAN 支持 - 通过此增强功能，可扩展支持 VLAN 的分段。原先仅第 2 层扩展支持逻辑分段。这包括 VLAN 中继支持，可在一个 Edge 接口和第 2 层 VPN 会话上扩展多个 VLAN。
- 对 IPsec VPN 的 TCP MSS 限制 - TCP MSS 限制允许 admin 强制实施所有 TCP 连接的 MSS 值以避免数据包碎片。
- 对 IPsec VPN 的 ECC（椭圆曲线证书）支持 - 需要 EC 证书才能支持各种 IPsec 合规性套件，例如，CNSA、UK Prime 等。
- 适用于合规性套件的易用按钮 - 只需在 UI 中单击或者通过单次 API 调用，即可配置 CNSA、Suite-B-GCM、Suite-B-GMAC、Prime、Foundation 和 FIPS。

自动化、OpenStack 和其他 CMP

- 扩展 OpenStack 发行版支持 - 现已包含 Stein 和 Rocky 发行版。
 - 支持策略 API 的 OpenStack Neutron 插件 - 除支持管理 API 的现有插件外，现在还提供 OpenStack Neutron 插件，此插件使用全新的 NSX-T 策略 API。此插件支持适用于第 2 层、第 3 层、防火墙和 SLAAC 的 IPv6。
 - OpenStack Neutron 路由器优化 - 此插件现在可以通过动态管理服务路由器的创建或删除来优化 OpenStack Neutron 路由器。这样客户在未配置任何服务时只能有一台分布式路由器，而在添加服务后则有另一台路由器，所有这些路由器都由该插件进行管理。
 - OpenStack Neutron 插件第 2 层网桥 - 现在，从 OpenStack 配置的第 2 层网桥在 Edge 集群上进行配置，而不是在 ESXi 集群上配置。
 - OpenStack Octavia 支持 - 除了 LBaaSv2 外，OpenStack Neutron 插件还支持采用 Octavia 作为一种支持负载均衡的方法。
- 有关更多详细信息，请参见适用于 OpenStack Neutron 的 VMware NSX-T Data Center 2.5 插件发行说明。

NSX Cloud

- 添加新操作模式 - NSX Cloud 现在具有两种操作模式，这使 NSX Cloud 正式成为市场中唯一支持有代理和无代理操作模式的混合云解决方案。
 - NSX 实施模式（有代理） - 在内部部署与任意公共云之间提供“一致”的策略框架。NSX 策略实施是使用每一项工作负载中安装的 NSX Tools 完成的。这提供了虚拟机级别的粒度，所有带标记的虚拟机都将由 NSX 来管理。此模式将克服各个公有云提供商的差异/限制，并在内部部署和公有云工作负载之间提供一致的策略框架。
 - 云原生实施模式（无代理） - 在内部部署与任意公有云之间提供“公用”的策略框架。此模式无需在工作负载中安装 NSX Tools。NSX 安全策略将转换为云原生提供商安全构造。因此，所选公有云的所有规模和功能限制都适用。在 VPC/VNET 级别控制粒度，受管 VPC/VNET 内部的每一项工作负载都将由 NSX 来管理（除非已加入白名单）。

这两种模式都将为 NSX 组成员资格条件提供动态组成员资格和一组丰富的抽象功能。
- 支持来自 NSX Cloud 的公有云原生服务的可见性和安全性 - 从此发行版开始，可以在具有本地 VPC/VNET 端点和与之关联的安全组的 Azure 和 AWS 中，对原生 SaaS 服务的安全组进行编程。主要的理念是使用用户指定的 NSX 策略相关规则来发现并保护云原生服务端点。在此发行版中，在 AWS（ELB、RDS 和 DynamoDB）和 Azure（Azure Storage、Azure LB、Azure SQL Server 和 CosmosDB）中将支持下列服务。未来 NSX-T 发行版将为更多服务添加更多支持。
- 新增操作系统支持：

- 支持 Windows Server 2019
- Windows 10 v1809
- 支持 Ubuntu 18.04
- 增强了隔离策略和虚拟机白名单 - 从 NSX 2.5 起，NSX Cloud 允许用户通过 CSM 界面将虚拟机添加到白名单中。添加到白名单后，此类虚拟机的云安全组将不受 NSX 管理，用户可自行决定将这些虚拟机放入任意云安全组中。
- 改进了 CSM 界面上的错误报告 - 加速完成故障排除。

运维

- 支持适用于一个或多个 NSX Manager 的 vSphere HA - 现在可通过 vSphere HA 来保护 NSX 管理集群。这样当运行任一 NSX 管理集群节点的主机发生故障时，就可以恢复此节点。它还支持在出现站点级别故障时，将整个 NSX 管理集群恢复到备用站点。请参见《NSX-T 安装指南》，了解有关受支持场景的详细信息。
- 容量仪表板改进 - 新增并改进了容量仪表板指标，可对照产品中支持的最大值展示客户已配置的对象数量。要获取 NSX-T Data Center 最高配置的完整列表，请参见 VMware 最高配置工具。
- 支持 vSphere 锁定模式 - 通过提供在 vSphere 锁定模式环境中安装、升级和操作 NSX-T 的功能，为客户提供更多部署选项。
- 日志记录增强功能 - 支持通过 NSX 用户空间代理的 NSX 命令行界面动态更改日志级别，从而减少故障排除期间的服务影响。
- SNMPv3 支持 - 支持为 NSX Edge 和 Manager 设备配置 SNMPv3，从而增强了安全合规性。
- 新增用于对虚拟机地址解析问题进行故障排除的流跟踪功能 - 支持通过流跟踪注入 ARP/NDP 数据包来检测连接问题，同时为 IP 目标执行地址解析。
- 升级顺序更改 - 升级到 NSX-T 2.5 时，新的升级顺序为先执行 Edge 组件升级，然后执行主机组件升级。此增强功能在升级云基础架构时作用明显，它可通过优化来缩短总体维护时间。
- Log Insight 内容包增强功能 - 通过兼容 NSX-T 2.5 的全新 NSX-T 内容包，添加了对现成日志警报的支持。

平台安全性

- FIPS - 用户现在可以生成 FIPS 合规性报告，包括能够在 FIPS 兼容模式下配置和管理其 NSX 部署。加密模块根据 FIPS 标准进行验证，从而为期望符合联邦法律或者以符合规定的 FIPS 标准的安全方式操作 NSX 的客户提供安全保障。NSX-T 2.5 中的所有加密模块均已通过 FIPS 认证（已注明例外情况）。要查看为 FIPS 验证的模块授予的证书，请参见 <https://www.vmware.com/security/certifications/fips.html>。
- 密码管理增强功能 - 用户现在可以延长自上次密码更改以来的密码到期期限（天数），即使在升级后也是如此。现在，在界面、CLI 和 syslog 中会显示三十天到期警告和密码到期通知。

支持单一集群设计

支持具有完全合并的 Edge+管理+计算虚拟机的单一集群设计，在至少有四个主机的集群中，所有这些虚拟机都由单个 N-VDS 提供支持。VxRail 和其他云提供商主机解决方案的典型参考设计要求采用含两个主机交换机的 4x10G pNIC。其中一个交换机专用于 Edge+管理 (VDS)，而另一个交换机则专用于计算虚拟机 (N-VDS)。两个主机交换机有效地将管理流量与计算流量分开。但是，随着 10G 和 25G 变得越来越经济划算，许多小型数据中心和云提供商客户正在标准化两个 pNIC 主机。通过使用此外形规格，小型数据中心和云提供商客户可以通过单个 N-VDS 构建基于 NSX-T 的解决方案，从而通过两个 pNIC 来支持所有组件。

NSX Data Center for vSphere 到 NSX-T Data Center 的迁移

- 迁移协调器增强功能 - 迁移协调器具有多种实用增强功能，可改进从 NSX Data Center for vSphere 迁移到 NSX-T Data Center 所需流程的工作流，包括改进了迁移期间提供用户反馈的功能。

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](#)》。

常规行为变化

NSX-T Data Center 系统通信端口更改

从 NSX-T Data Center 2.5 起，从所有传输节点和 Edge 节点到 NSX Manager 的 NSX 消息传递通道 TCP 端口已从端口 5671 更改为 TCP 端口 1234。对于此更改，请先确保所有 NSX-T 传输节点和 Edge 节点均可在 TCP 端口 1234 上与 NSX Manager 进行通信，并可在 TCP 端口 1235 上与 NSX Controller 进行通信，然后再升级至 NSX-T Data Center 2.5。此外，请确保在升级过程中端口 5671 保持打开状态。

L2 网络

通过增强第 2 层网桥，ESXi 网桥已被弃用。NSX-T 在一开始引入时，具有将 ESXi 主机专门用作为网桥以将覆盖网络分段扩展至 VLAN 的功能。此模型从该发行版起已被弃用，因为新的 Edge 网桥在功能方面更胜一筹，无需专用 ESXi 主机，并且可从经过优化的 Edge 节点数据路径中获益。请参见“新增功能”部分以获取更多信息。

API 弃用和行为变化

在此发行版中已弃用传输节点模板 API。建议改为使用传输节点配置文件 API。请参见 [API 指南](#)，以获取已弃用的类型和方法的列表。

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。

本地化语言

NSX-T Data Center 已本地化为多种语言：英语、德语、法语、日语、简体中文、韩语、繁体中文和西班牙语。由于 NSX-T Data Center 本地化使用浏览器语言设置，因此，请确保您的设置与期望的语言相匹配。

文档修订历史

2019 年 9 月 19 日：第一版。

2019 年 9 月 23 日：添加了已知问题 2424818 和 2419246。添加了已解决的问题 2364756、2406018 和 2383328。

2019 年 9 月 24 日：更新了“新增功能”项。

2019 年 10 月 3 日。添加了已解决的问题 2313673。

2019 年 11 月 12 日。添加了已知问题 2362688 和 2436302。更正了问题 2282798，将其移到“已解决的问题”部分。

2019 年 12 月 17 日。添加了已知问题 2444170。

2020 年 1 月 14 日。添加了已解决的问题 2399994。

2020 年 2 月 18 日。更新了已知问题 2436302，在其中包含指向知识库文章的链接。

2020 年 5 月 14 日。添加了已知问题 2467479。

2020 年 9 月 25 日。添加了已知问题 2586606。

2021 年 3 月 15 日。添加了已知问题 2730634。

已解决的问题

- 已修复问题 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。

- 已修复问题 2334442 - 在重命名 admin 用户后，用户没有编辑或删除创建的对象权限。
在重命名 admin 用户后，用户没有编辑或删除创建的对象权限。无法重命名 admin/auditor 用户。
- 已修复问题 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。
- 已修复问题 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。
- 已修复问题 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。
- 已修复问题 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://<nsx-manager>/api/v1/configs/management` 可能会失败。
如果配置了 FQDN，则无法调用 PUT `https://<nsx-manager>/api/v1/configs/management`。
- 已修复问题 2279249 - 即时克隆虚拟机在 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。
- 已修复问题 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。
- 已修复问题 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。
- 已修复问题 2282798 - 如果尝试在 NSX Manager 中同时注册的请求/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。
- 已修复问题 2383867 - 针对某一个管理平面节点，日志包收集失败。
日志收集流程在将支持包复制到远程服务器时遭遇失败。
- 已修复问题 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`。
- 已修复问题 2410818 - 升级到 2.4.2 后，NSX-T 2.3.x 中创建的虚拟服务器可能会在创建更多虚拟服务器后停止工作。
在某些部署中，在 2.3.x 中创建的虚拟服务器会在升级到 2.4.2 以及创建更多虚拟服务器后停止工作。
- 已修复问题 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)
- 已修复问题 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。

- **已修复问题 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。
- **已修复问题 2318525 - 作为 eBGP 对等体 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 对等体作为下一跃点，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。
- **已修复问题 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。
- **已修复问题 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。
- **已修复问题 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。
- **已修复问题 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。
- **已修复问题 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)。”
- **已修复问题 2364756 - 由于优先级重复，导致配置文件实现失败。**
在大规模设置中，当用户将 vRNI 与 NSX IPFIX 相关联时，将不会在管理平面上实现配置文件，而是通过解决实现错误来实现。
- **已修复问题 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。
- **已修复问题 2307551 - 将所有 pNIC 迁移到 N-VDS 时，NSX-T 主机可能会丢失管理网络连接。**
出现此问题的原因是，主机迁移重试操作会在配置了 vmk0 的 N-VDS 中移除所有 pNIC。第一次主机迁移会将所有 pNIC 和 vmk0 迁移到 N-VDS，但之后的迁移操作将失败。重试迁移时，会从 N-VDS 中移除所有 pNIC。因此，用户无法通过网络访问主机；主机中的所有虚拟机也会丢失网络连接，从而导致其服务无法访问。
- **已修复问题 2369792 - 由于 CBM 进程内存膨胀，CBM 进程反复崩溃。**
Cloud Service Manager 设备上的 CSM 和 CBM 进程无法压缩数据库。因此，CBM 进程内存膨胀，导致 CBM 进程反复崩溃。
- **已修复问题 2361892 - NSX Edge 设备出现内存泄漏，从而导致进程崩溃/重新启动。**
在一段较长的时间内，NSX Edge 设备可能会由于重复规则查找而遭遇内存泄漏，这会导致进程崩溃/重新启动。每次执行规则查找时，都会检测到内存泄漏。清除流量缓存时，不会移除 VIF 接口，从而导致内存堆积。

- 已修复问题 2364529 - 重新配置后出现负载均衡器内存泄漏。
NSX 负载均衡器可能会在发生连续/重复的配置事件时泄漏内存，从而导致 nginx 进程核心转储。
- 已修复问题 2378876 - ESXi 主机上出现 PSOD，并显示以下错误：“Usage error in dlmalloc”和“PF Exception 14 in world 3916803:VSIP PF Purg IP”。
在运行流量数天后，ESXi 会崩溃 (PSOD)。崩溃之前未观察到任何其他症状。最终在 ALG 流量 (FTP、Sunrpc、Oracle、Dcerpc、TFTP) 中发现问题，其中非原子增量计数器导致争用情况，从而破坏 ALG 树结构。
- 已修复问题 2384922 - BGPD 在 Edge 节点上的 CPU 占用率达到 100%。
NSX-T Edge 上的 BGPD 进程在具有多个使用 VTYSH 打开的会话时，可能会占用 100% CPU。
- 已修复问题 2386738 - 通过 LINKED 端口的流量会忽略 NAT 规则。
连接 Tier-0 和 Tier-1 逻辑路由器的 LINKED 路由器端口类型未启用 NAT 服务。
- 已修复问题 2363618 - VMware Identity Manager 用户无法访问 NSX Manager 仪表板中的“策略”页面。
在 VMware Identity Manager 中具有组权限角色的用户无法访问 NSX Manager 仪表板中的“策略”页面。组分配中的权限会被忽略。
- 已修复问题 2298274 - 可以通过 REST API 使用无效域名或部分域名来创建或更新策略组。
接口允许使用身份表达式创建组，其中针对单一有效内容包含无效的 Active Directory 组或者个别组成员。但是，仅当每个成员只有一个与域名关联的 LDAP 组时，该成员才有效。因此，对于在先前版本的 NSX-T 中创建的此类组，在升级过程中不会标记此错误，从而允许在后续版本中保留无效的组。在 2.5 中已修复此问题。
- 已修复问题 2317147 - 对于其成员资格取决于 IP 地址或 MAC 地址的组，用户无法看到此类组的有效虚拟机。
如果用户创建了一个组，并且该组中仅具有 IP 地址或 MAC 地址，那么从 API 调用该组的有效成员资格时不会列出任何虚拟机。这对功能没有任何影响。策略会在管理平面上正确创建 NS 组，并且 IP 地址和 MAC 地址列表会直接发送到中央控制平面。
- 已修复问题 2327201 - KVM Hypervisor 上的虚拟机更新不会立即同步。
KVM Hypervisor 上的虚拟机更新可能需要几个小时才能在 NSX-T 上完成同步。因此，KVM Hypervisor 上创建的新虚拟机无法添加到 NS 组中，无法对这些虚拟机应用任何防火墙规则，因为虚拟机电源状态未更新，所以无法升级 KVM Hypervisor。
- 已修复问题 2329443 - 由于强制同步超时，控制集群未完成初始化。
当 Ipset 中的 IPV4 范围从 0.0.0.0 开始 (例如，0.0.0.0-1.1.1.20) 时，控制集群由于强制同步超时而未初始化。此问题是由于 IPSetFullSyncMessageProvider 陷入无限循环而导致的。由于中央控制平面未初始化，用户无法部署新工作负载。
- 已修复问题 2337839 - NSX-T 备份小组件显示的字段名称不正确。
具体来说，NSX-T 备份小组件显示的备份错误数量不正确。因此，客户需要查看 NSX Manager 备份选项卡，了解备份错误的准确计数。
- 已修复问题 2341552 - 当系统包含的受支持网卡数量过多时，Edge 引导失败。
不显示任何数据路径服务或连接，数据路径服务已关闭，并且 Edge 节点处于已降级状态。这导致需要 Edge 时，部分或全部连接丢失。
- 已修复问题 2390374 - NSX Manager 响应非常慢或无响应，日志显示大量 Corfu 异常。
NSX 也可能无法启动。Corfu 异常指示 Active Directory 成员的规模过大，超出测试限制。
- 已修复问题 2371150 - 无法在裸机 Edge 节点上配置第 7 层防火墙规则。
在 NSX-T 2.5 中不支持在裸机 Edge 节点上配置第 7 层防火墙规则。存在启用此支持的内部命令，但此命令仅用于概念证明。

- 已修复问题 2361238 - 下行链路路由器与服务路由器无法配对。
在删除并重新创建曾与下行链路路由器配对的服务路由器后，NAT 规则不会对下行链路路由器产生任何影响。
- 已修复问题 2363248 - 界面上的服务实例运行状况显示为“关闭”，但 API 调用显示“已连接”。
此不一致报告可能导致虚假警报。

在[知识库文章 67165 - 《在 NSX-T 中未启动任何要保护的虚拟机时，服务实例状态显示为“关闭”》](#)中，更详细地介绍了此问题和解决方案。
- 已修复问题 2359936 - 在 ESX 主机上频繁滚动 cfgAgent 日志。
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。
- 已修复问题 2332938 - 在“泛洪保护安全性配置文件”中启用 SYN 缓存时，实际 TCP 半打开连接限制可能大于在 NSX Manager 上配置的值。
NSX-T 根据已配置的限制自动计算最优 TCP 半开连接限制。此计算限制可能大于已配置的限制，并且基于以下公式：Limit = (PwrOf2 * Depth)，其中 PwrOf2 表示 2 的幂（不小于 64），而 Depth 是整数 (<= 32)。
- 已修复问题 2376336 - 策略和 Edge 不支持路由重新分发中的地址系列。
重新分发中的地址系列未正常工作或未用于应用程序。
- 已修复问题 2412842 - 在 ESX 上将衡量指标日志限制为 40 MB，以支持具有 ramdisk 的主机。
[知识库文章 74574](#) 对此问题进行了详细讨论。
- 已修复问题 2385070 - 关于 IPv6 子网，IP 发现与 DFW 的行为相反。
IP 发现将 2001::1/64 视为主机 IP，而 DFW 则将其视为 IPv6 子网。
- 已修复问题 2394896 - 主机无法从 NSX-T Data Center 2.4.x 升级到 2.5。
主机无法从 NSX-T Data Center 2.4.0、2.4.1 和 2.4.2 升级到 2.5。这可能是由于 KCP 模块卸载失败所导致的。

[知识库文章 74674](#) 对此问题进行了更加详细的讨论。
- 已修复问题 2406018 - 如果密码将在 30 天内到期，则会触发事件/警报。
如果密码将在 30 天内到期，即使已禁用密码到期，仍会触发有关密码到期的事件/警报。
- 已修复问题 2383328 - 功能请求，请求提供实用程序来以人工可读形式呈现衡量指标数据。
NSX-T Data Center 收集衡量指标数据并将其保存为二进制格式，而用户请求了以人工可读格式查看此数据的功能。此问题会跟踪该请求。
- 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 2313673 - 基于虚拟机的 Edge 传输节点：用户无法将上行链路连接到 NSX-T 逻辑交换机/分段。
对于基于虚拟机的 Edge 传输节点，用户无法将 Edge 传输节点上行链路连接到 NSX-T 逻辑交换机/分段。他们只能将其连接到 vCenter 的 DVPG。在为基于虚拟机的 Edge 传输节点的添加/编辑流的“配置 NSX”屏幕上，仅向用户提供了使用 vCenter 的 DVPG 映射上行链路的选项。缺少用于将上行链路映射到 NSX-T 逻辑交换机/分段的选项。
- 已修复问题 2424394 - 由 NSX-T DR 中继的 DHCP 数据包无法达到距离超过 10 个跃点的位置。
当 DHCP 服务器的距离超过 10 个跃点时，中继的 DHCP 数据包将无法到达该服务器。
- 已修复问题 2399994 - 重新分配的路由会间歇性丢失。
网络流量可能会受到影响，因为到 T1 的路由有一段时间不可用。

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](#)
- [NSX Intelligence 已知问题](#)
- [运维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 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。在丢弃发送到对等体的更新消息时，BGP 进程将消耗额外的 CPU 资源。如果具有大量路由和对等体，这可能会影响路由聚合。

解决办法：无。
- **问题 2390624 - 当主机处于维护模式时，反关联性规则会阻止服务虚拟机执行 vMotion。**
如果服务虚拟机部署在恰好包含两个主机的集群中，则具有反关联性规则的 HA 对将会在执行任何维护模式任务期间阻止虚拟机对其他主机执行 vMotion。这可能会阻止主机自动进入维护模式。

解决办法：在 vCenter 上启动维护模式任务之前，关闭主机上服务虚拟机的电源。
- **问题 2329273 - 同一 Edge 节点上桥接到同一分段的 VLAN 之间没有连接。**
不支持在同一 Edge 节点上两次桥接一个分段。但是，可以将两个 VLAN 桥接到两个不同 Edge 节点上的同一分段。

解决办法：无
- **问题 2239365 - 抛出“未经授权”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 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 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 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://<nsx-manager>/api/v1/fabric/compute-collections/<CC Ext ID>/storage-resources?uniform_cluster_access=true&source=realtime`

其中 <nsx-manager> 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 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 2370555 - 用户可以删除高级界面中的某些对象，但删除不会反映在简化界面中。
具体来说，可以在“高级”界面“分布式防火墙排除列表”设置中删除作为分布式防火墙排除列表的一部分添加的组。这会导致界面中出现不一致的行为。

解决办法：使用以下过程来解决此问题：

- 在简化界面中，将某个对象添加到排除列表。

- 确认它是否显示在高级界面的分布式防火墙排除列表中。
 - 从高级界面的分布式防火墙排除列表中删除该对象。
 - 返回到简化界面，将第二个对象添加到排除列表并应用该对象。
 - 确认新对象是否显示在高级界面中。
- 问题 2377217 - 在重新引导 KVM 主机后，虚拟机之间的流量可能无法按期望方式运行。
重新引导 KVM 主机可能会导致虚拟机之间出现可访问性问题。

解决办法：重新引导主机后，使用以下命令重新启动 nsx-agent 服务：
systemctl restart nsx-agent.service
- 问题 2371251 - 导航到“备份和还原”页面时，仪表板界面闪烁
仅在 Firefox 浏览器中发现此问题，并且只有在某些部署中才会出现。

解决办法：手动刷新页面或使用其他支持的浏览器。
- 问题 2408453 - 安装 NSX 客户机侦测驱动程序时，VMware Tools 10.3.5 崩溃。
VMware Tools 10.3.5 会在 Windows 虚拟机上无规则崩溃，最明显的是在远程会话断开连接或客户机虚拟机关闭时出现崩溃。

解决办法：有关详细信息，请参见[知识库文章 70543](#)。
- 问题 2267964 - 如果移除 vCenter，那么不会向用户发出有关 vCenter 上运行的服务丢失的警告。
如果用户移除计算机管理器 (vCenter) 并且其中部署有客户机侦测之类的服务，那么不会向用户发出有关这些服务可能会丢失的通知。

解决办法：如果用户按正确过程添加新 vCenter 作为计算机管理器，就可以避免出现此问题。
- 问题 2444170：NSX CLI 命令无法卸载数据路径
del nsx 命令无法从主机卸载 NSX-T 配置和模块。这会导致 NSX-T 安装或升级失败。

解决办法：无。
- 问题 2467479 - 一旦将 SNAT 规则的“防火墙”设置为“绕过”，则在从“绕过”更改为“无”后将无法阻止该规则。
一旦将 SNAT 规则的“防火墙”设置为“绕过”，则在从“绕过”更改为“无”后将无法阻止该规则。

解决办法：删除并重新创建 SNAT 规则。
- 问题 2586606：在大量虚拟服务器中配置源 IP 持久性后，负载均衡器无法正常使用。
在负载均衡器上的大量虚拟服务器中配置源 IP 持久性后，会消耗大量内存，并且可能导致 NSX Edge 内存不足。但是，如果添加更多虚拟服务器，可能会再次出现该问题。

解决办法：禁用源 IP 持久性，或将配置了源 IP 持久性的 VIP 移至不同的 LB 服务。
- 问题 2730634：Uniscale 升级后网络组件页面显示“索引不同步” (Index out of sync) 错误。
Uniscale 升级后网络组件页面显示“索引不同步” (Index out of sync) 错误。

解决办法：使用 admin 凭据登录到 NSX Manager，然后运行“start search resync policy”命令。加载网络组件将需要几分钟时间。

安装已知问题

- 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 2378970 - 分布式防火墙的集群级别“启用/禁用”设置错误显示为“已禁用”。
简化 UI 上 IDFW 的集群级别“启用/禁用”设置可能显示为“已禁用”，即使在管理平面上已启用也如此。
从 2.4.x 升级到 2.5 后，此错误将一直保留，直至明确完成更改为止。

解决办法：手动修改简化 UI 上 IDFW 的“启用/禁用”设置，以匹配管理平面上的相同设置。

NSX Edge 已知问题

- 问题 2283559 - 当 Edge 针对 RIB 具有超过 65000 条路径且针对 FIB 具有超过 100000 条路径时，<https://<nsx-manager>/api/v1/routing-table> 和 <https://<nsx-manager>/api/v1/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 对等体以防止延迟。

- 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（或其对等体）以阻止重新向其通告路由，从而防止发生转发循环。

- 问题 2343954 - Edge 第 2 层网桥端点接口允许配置不支持的 VLAN 范围。
“Edge 第 2 层网桥和点”配置接口允许配置一个或多个 VLAN 范围，即使不支持这些范围也如此。

解决办法：针对“Edge 第 2 层网桥和点”配置，请勿配置此类 VLAN 范围。

逻辑网络已知问题

- 问题 2389993 - 使用“策略”页面或 API 修改重新分发规则后，路由映射会被移除。
对于从“管理平面”界面或 API 添加到重新分发规则的路由映射，如果随后通过“策略”页面或 API 修改了同一重新分发规则，则该路由映射可能会被移除。出现此问题的原因是，“策略”页面或 API 不支持添加路由映射。这可能会导致向 BGP 对等端通告不必要的前缀。

解决办法：您可以返回“管理平面”界面或 API 来重新将路由映射添加到同一规则，从而还原该路由映射。如果您希望在重新分发规则中包含路由映射，建议您始终使用“管理平面”界面或 API 来创建并修改该规则。

- 问题 2275412 - 在多个 TZ 之间端口连接无效。
端口连接只能在单个 TZ 中使用。

解决办法：无。

- 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 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)。

解决办法：无。

- 问题 2388158 - 用户无法在 Tier-0 逻辑路由器配置中编辑转换子网设置。创建 Tier-0 逻辑路由器后，在 NSX Manager 界面中无法修改转换子网配置。

解决办法：无。最佳选择是删除逻辑路由器，然后使用期望的转换子网配置重新创建该路由器。

安全服务已知问题

- 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 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 2366599 - 未强制实施含 IPv6 地址的虚拟机的规则。
如果虚拟机使用 IPv6 地址，但未通过 IP 发现配置文件为该 VIF 启用 IPv6 侦听，那么在数据路径中该虚拟机的规则中不会填充 IPv6 地址。因此，永远不会强制执行该规则。

解决办法：每次使用 IPv6 地址时，都验证在 VIF 或逻辑交换机上是否启用了 IP 发现配置文件中的 IPv6 选项。

- 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 2379632 - 在分类阶段命中第 7 层规则时记录多个数据包。
在分类阶段命中第 7 层规则时，会记录多个（2-3 个）数据包 (dfwpktlogs)。

解决办法：无。

- 问题 2368948 - 分布式防火墙规则：个别区域的实现状态可能并非最新。
刷新 DFW 规则视图不会更新该视图中个别区域的实现状态。因此，显示的信息可能并非最新信息。

解决办法：这仅影响手动刷新。针对实现状态将定期执行轮询，并且定期轮询将提供准确的更新。用户也可以刷新个别区域以获取准确状态。

- 问题 2380833 - 发布包含不少于 8,000 条规则的策略草稿需要大量时间。
包含不少于 8,000 条规则的策略草稿需要花费大量时间来发布。例如，包含 8,000 条规则的策略草稿可能需要花费 25 分钟来发布。

解决办法：无。

- 问题 2424818 - 在 NSX Manager 界面上未更新第 2 层和分布式防火墙状态。

逻辑导出程序在工作负载虚拟机上生成的状态信息可能不会转发到管理平面。因此，这些组件的状态未正确更新。

解决办法：无。可通过相应虚拟机上的 CLI 来访问正确的状态信息。

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 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 调用启动失败。
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。

- 问题 2401715 - 更新计算管理器时出错，指纹无效，即使提供正确的指纹也是如此。
在 NSX-T Manager 中添加 vCenter v6.7U3 作为计算管理器时发现此问题，vSphere 6.7 支持更改 PNID，其中 FQDN 或 IP 地址均可更改。NSX-T 2.5 不支持此功能，因此会出现指纹问题。

解决办法：删除先前添加的 vCenter，并使用新更改的 FQDN 添加 VC。添加注册可能失败，因为在 vCenter 上已存在先前的扩展。解决注册错误以使其成功完成注册。

NSX Intelligence 已知问题

- 问题 2410806 - 发布生成的建议失败，出现引用限制总数 500 的异常。
如果建议的组中的成员（IP 地址或虚拟机）总数超过 500，那么将生成的建议发布到策略配置中的过程将失败，并显示异常消息，如“IPAddressExpressions、MACAddressExpressions、PathExpression 中的路径和 ExternalIDExpression 中的外部标识总数不应超过 500”。

解决办法：如果出现有超过 500 个客户端正在连接到应用程序虚拟机或负载均衡器的情况，您可以创建规则以对应应用程序负载均衡器的访问权进行微分段，然后选择应用程序虚拟机以启动建议发现。或者，您可以将超过 500 个成员的组细分为多个较小的组。

- 问题 2362865 - 对于默认规则无法按规则名称筛选。
在安全规划和故障排除 > 发现并执行操作页面上发现此问题，它仅影响由连接策略创建的规则。此问题是由于缺少基于指定连接策略的默认策略所导致的。可以在管理平面上创建默认规则，但如果没有相应的默认策略，用户就无法基于该默认规则进行筛选。（流量可视化的筛选器使用规则名称按命中该规则的流量进行筛选。）

解决办法：请勿应用规则名称筛选器。改为选中“不受保护”标记。此配置将包含命中默认规则的流量，以及命中指定了“任意”源和“任意”目标的任意规则的流量。

- 问题 2368926 - 如果用户在作业进行过程中重新引导设备，那么建议作业将失败。
如果用户在建议作业正在进行时重新引导 NSX Intelligence 设备，那么此作业将进入失败状态。用户可以为一组上下文虚拟机启动建议作业。重新引导会删除上下文，因此作业将失败。

解决办法：重新引导后，对同一组虚拟机重复此建议作业。

- 问题 2385599 - 在 NSX-T Intelligence 建议中不支持静态 IP 组。

在 NSX-T 清单中无法识别的虚拟机和工作负载（如果它们具有内部网 IP 地址）可能仍作为一组静态 IP 而受到建议的影响，包括包含这些组的建议定义规则。但是，NSX Intelligence 不支持此类组，因此可视化功能会将发送给它们的流量显示为发送目标“未知”，而不是建议组。

解决办法：无。但是，建议可以正常运行。这是一个显示问题。

- 问题 2374231 - 对于 SCTP、GRE 和 ESP 协议流量，“服务”显示为“未知”，“端口”显示为 0。对于 GRE、ESP 和 SCTP 协议流量，NSX Intelligence 不支持源或目标端口解析。NSX Intelligence 可为 TCP 和 UDP 流量以及流量相关统计信息提供完整的标头解析。对于其他受支持的协议（如 GRE、ESP 和 SCTP），NSX Intelligence 只能提供不含协议特定的源或目标端口的 IP 信息。对于这些协议，源或目标端口将为零。

解决办法：无。

- 问题 2374229 - NSX Intelligence 设备的磁盘空间不足。

NSX Intelligence 设备的默认数据保留期为 30 天。如果流数据量大于 30 天内预期数据量，那么设备可能提前出现磁盘空间不足，并且导致部分或完全不可运行。

解决办法：可通过监控 NSX Intelligence 设备的磁盘使用情况来防止或缓解此问题。如果磁盘使用率较高，表明空间可能不足，那么可以修改数据保留期，缩短其天数。

1. 通过 SSH 连接到 NSX Intelligence 设备，并访问 `/opt/vmware/pace/druid-config/druid_data_retention.properties` 文件。
2. 找到 `correlated_flow` 设置，并将其更改为低于 30 天的值。例如：`correlated_flow=P14D`
3. 运行以下命令来保存该文件并应用更改：
`/opt/vmware/pace/druid-config/druid-config-data-retention.sh`
注意：物理删除数据最多可能需要两小时的时间。

- 问题 2389691 - 发布建议作业失败，并显示错误“请求负载大小超出允许的限制，每个请求最多允许 2,000 个对象。”

如果您尝试发布单个建议作业并且其中包含超过 2,000 个对象，那么该作业将失败，并显示错误“请求负载大小超出所允许的限制，每个请求允许的最大对象数为 2,000。”

解决办法：在建议作业中将对象数量降低到小于 2,000，然后重试发布。

- 问题 2376389 - 在中等规模的设置中，虚拟机被错误标记为“在过去 24 小时内”已删除。

从计算管理器断开传输节点的连接或者移除传输节点后，NSX Intelligence 将先前虚拟机显示为已删除，并使用新虚拟机取而代之。此问题是由于 NSX Intelligence 跟踪 NSX 数据库中的清单更新而导致的，此行为反应了清单是如何处理从计算管理器断开传输节点连接的。这不影响 NSX Intelligence 中的活动虚拟机总数，但在 NSX Intelligence 中会出现重复的虚拟机。

解决办法：不需要采取任何措施。根据所选时间间隔，最终会从界面中移除重复的虚拟机。

- 问题 2393240 - 发现从虚拟机到 IP 地址的额外流量。

客户会看到从虚拟机到 IP-xxxx 的额外流量。这是由于在创建流量后，来自 NSX Policy Manager 的配置数据（组、虚拟机和服务）到达 NSX Intelligence 设备而产生的。因此，先前流量无法与配置关联，因为它在流量透视图中并不存在。由于流量无法正常关联，在流量查找期间，它会默认为其虚拟机的 IP-xxxx。同步配置后即可显示实际虚拟机流量。

解决办法：修改时间范围以排除要查看的流量。

- 问题 2370660 - NSX Intelligence 针对特定虚拟机显示的数据不一致。

导致此问题的原因可能是这些虚拟机在数据中心内具有相同的 IP 地址。在 NSX-T 2.5 中，NSX Intelligence 不支持此功能。

解决办法：无。避免为数据中心内的两个虚拟机分配相同的 IP 地址。

- 问题 2372657 - 虚拟机/组关系和组/组流量关联暂时显示不正确。

如果部署 NSX Intelligence 设备时在数据中心内存在运行的流量，那么虚拟机/组关系和组/组流量关联会暂时显示不正确。具体来说，在这段时间内，以下元素可能显示不正确：

- 虚拟机错误归属于“未分类”组。
- 虚拟机错误归属于“未知”组。
- 可能会错误显示两个组之间的关联流量。

当 NSX Intelligence 设备部署时间超过用户选定的可视化时间段并完成部署后，这些错误将自行纠正。

解决办法：无。如果用户在部署 NSX Intelligence 设备期间退出可视化时间段，则不会显示该问题。

- 问题 2366630 - 部署 NSX Intelligence 设备时，传输节点删除操作可能会失败。

如果在部署 NSX Intelligence 设备时删除传输节点，那么删除可能会失败，因为 NSX-INTELLIGENCE-GROUP NSGroup 会引用该传输节点。要删除传输节点，需要在部署 NSX Intelligence 设备时使用强制删除选项。

解决办法：使用 force 选项删除传输节点。

- 问题 2357296 - 在某些规模和压力条件下，部分 ESX 主机可能不会向 NSX Intelligence 报告流量。

NSX Intelligence 界面可能不会显示来自某些主机上特定虚拟机的流量，并且无法为这些虚拟机提供防火墙规则建议。因此，可能会危及某些主机上的防火墙安全。在 vSphere 版本低于 6.7U2 和 6.5U3 的部署中，会发现此问题。该问题被标识为核心 ESX Hypervisor 虚拟机筛选器创建和删除顺序错误。

解决办法：将主机升级到版本 vSphere 6.7U2 和更高版本或 vSphere 6.5U3 和更高版本。

- 问题 2393142 - 使用 vIDM 凭据登录到 NSX Manager 可能会返回 403 未经授权的用户错误。

这仅影响以 vIDM 用户身份登录的用户，而不影响 NSX Manager 上的本地用户。与 NSX Intelligence 设备进行交互时，在 NSX-T 2.5 中不支持 vIDM 登录和集成。

解决办法：为 NSX Manager IP/FQDN 添加字符串“login.jsp?local=true”，以本地用户身份登录。

- 问题 2369802 - NSX Intelligence 设备备份排除事件数据存储备份。

在 NSX 2.5 中不支持此功能。

解决办法：无。

- 问题 2346545 - NSX Intelligence 设备：证书替换会影响新流量信息的报告。

如果用户将 NSX Intelligence 设备的主体身份证书替换为自签名证书，那么会影响新流量的处理，并且设备将不会显示后续更新信息。

解决办法：无。

- 问题 2407198 - 在 NSX Intelligence 安全状态中，虚拟机错误显示在“未分类的虚拟机”组中。

当 ESXi 主机与 vCenter 断开连接，这些主机中的虚拟机会显示在“未分类的虚拟机”组中，即使这些虚拟机属于其他组也是如此。当 ESXi 主机与 vCenter 重新连接后，这些虚拟机将显示在正确的组中。

解决办法：将主机重新连接到 vCenter。

- 问题 2410224 - 完成 NSX Intelligence 设备注册后，刷新视图可能会返回“403 已禁止”错误。

完成 NSX Intelligence 设备注册后，如果单击刷新以查看，系统可能会返回“403 已禁止”错误。这是由于 NSX Intelligence 设备访问接口所需的时间导致的临时状况。

解决办法：如果遇到此错误，请稍等片刻后重试。

- 问题 2410096 - 重新引导 NSX Intelligence 设备后，可能不显示重新引导前的最后 10 分钟内收集的流量。

由索引问题所导致。

解决办法：无。

- 问题 2436302 - 替换 NSX-T 统一设备集群证书后，无法通过 API 或 Manager 界面来访问 NSX Intelligence。

在 NSX-T Manager 界面中，转到安全规划和故障排除选项卡，然后单击发现并执行操作或建议。接口将不会加载，并最终返回一条类似以下内容的错误：无法加载所请求的应用程序。请重试，如果问题仍然存在，请联系支持部门。

解决办法：有关更多详细信息和解决办法，请参见[知识库文章 76223](#)。

运维和监控服务已知问题

- 问题 2401164 - 尽管出现 SFTP 服务器错误，备份仍错误报告为成功。

如果用于备份的 SFTP 服务器密码过期，那么 NSX-T 会报告常规错误：“备份操作未知错误”。

解决办法：确认用于访问 SFTP 服务器的凭据是最新的。

升级已知问题

- 问题 2288549 - 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。当在全新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，并找到具有的 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。

- 问题 2348994 - 在 ESXi 6.5 p03 传输节点上升级 NSX VIB 期间出现间歇性故障。

在某些 2.4.x 到 2.5 升级中发现此问题。升级 ESXi 6.5 p03 传输节点上的 NSX VIB 时，升级操作有时会失败并显示以下错误：“VI SDK 调用异常：未能从进程获取任何数据：LANG=en_US.UTF-8”。

解决办法：升级到 ESXi 5 p04。或者将主机置于维护模式，然后重新引导。重试升级，然后退出维护模式。

- 问题 2372653 - 升级到 2.5 后，用户无法在先前的 NSX-T 版本中找到基于 LogicalPort 和 LogicalSwitch 的组。

升级到 2.5 后，从先前 NSX-T 版本中的策略创建的基于 LogicalPort 和 LogicalSwitch 的组不会显示在仪表板界面中。但是，这些组仍位于 API 中。这是由于升级过程中的名称更改所致。在 2.5 中，基于 LogicalPort 和 LogicalSwitch 的组显示为基于 Segment 和 SegmentPort 的组。

解决办法：升级后，仅使用 API 来访问这些策略组。

- 问题 2408972 - 升级过程中，vSphere Update Manager 在修复最后一个主机时失败。
升级过程中，针对具有 NSX-T 逻辑交换机所支持工作负载的最后一个主机，vSphere Update Manager 修复操作失败。

解决办法：手动将所有 NSX-T 支持的工作负载虚拟机迁移到已升级的主机，然后对修复失败的主机重试升级。

- 问题 2400379 - “上下文配置文件”页面显示不支持的 APP_ID 错误消息。
“上下文配置文件”页面显示以下错误消息：“此上下文配置文件使用不支持的 APP_ID - [<APP_ID>]。请在确保任何规则中均未使用此上下文配置文件后，手动将其删除。”这是由于升级后存在六个已弃用且在数据路径上已无效的 APP_ID（AD_BKUP、SKIP、AD_NSP、SAP、SUNRPC 和 SVN）所导致的。

解决办法：确保不再使用这六个 APP_ID 后，手动删除其上下文配置文件。

- 问题 2419246 - Ubuntu KVM 升级失败。
由于 nsx-vdpi 服务未运行，导致 Ubuntu KVM 节点升级可能失败。nsx-vdpi 服务依赖于 nsx-agent，但在升级期间，尚未配置 nsx-agent。由于 vm-command-relay 组件未正确启动，因此 nsx-agent 失败。

解决办法：配置未完全安装的 nsx-agent。以下命令将重新配置所有未打包或部分配置的软件包：

```
dpkg --configure -a
```

也可以使用以下命令来仅重新配置 nsx-agent 和 nsx-vdpi：

```
dpkg --configure nsx-agent
```

```
dpkg --configure nsx-vdpi
```

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 2200856 - cloud-service-manager 服务重新启动失败。
如果用户在不等待 API 服务首次启动的情况下就尝试使用 Cloud-service-manager 服务，那么重新启动此服务可能会失败。

解决办法：请稍等几分钟时间，然后重试。

- 问题 2378752 - API 允许在分段或端口下创建多个绑定映射。
仅在 API 上发现此问题。当用户在某个分段或端口下创建多个绑定映射时，不会报告任何错误。当用户尝试同时在分段或端口上绑定多个配置文件时，会出现此问题。

解决办法：请改为使用 NSX Manager 界面执行此操作。

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。

- 问题 2355113 - 对于在 Microsoft Azure 中启用加速网络连接的 RedHat 和 CentOS 工作负载虚拟机，无法在此类虚拟机中安装 NSX Tools。

在 Microsoft Azure 中，如果在基于 RedHat（7.4 或更高版本）或 CentOS（7.4 或更高版本）的操作系统上，启用加速网络连接并在其中安装 NSX 代理，那么以太网接口不包含 IP 地址。

解决办法：在 Microsoft Azure 中启动基于 RedHat 或 CentOS 的虚拟机后，请先安装最新的 Linux Integration Services 驱动程序：<https://www.microsoft.com/en-us/download/details.aspx?id=55106> 然后再安装 NSX Tools。

- 问题 2391231 - Azure 虚拟机更改检测可能已延迟。

对云中 Azure 虚拟机更改的检测可能间歇性出现短暂延迟。这导致对应延迟可能影响虚拟机载入，以及在 NSX-T 中为虚拟机创建逻辑实体。已发现的最长延迟约为 8 分钟。

解决办法：无。延迟时间段过后，问题将自行修复。

- 问题 2424818 - 在 NSX Manager UI 上不更新 L2 和 DFW 统计信息。

由工作负载虚拟机上的逻辑导出器生成的所有统计信息都不会转发到 MP。这导致在 NSX Manager UI 上显示统计信息失败。在 NSX Manager UI 中无法显示 DFW 统计信息。逻辑交换机端口运行状态将显示为“关闭”，其对应统计信息将无效。这仅适用于云虚拟机。

解决办法：无。可以通过对应虚拟机上的 CLI 查看这些统计信息。