VMware NSX-T Data Center 2.4 发行说明

VMware NSX-T Data Center 2.4 | 2019 年 2 月 28 日 | 内部版本 12456646

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 2.4 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。新功能主要包括基于意向的全新网络用户界面、上下文感知的防火墙、客户机和网络侦测功能、IPv6、高度可用的集群管理、针对 vSphere 计算集群的基于配置文件的 NSX 安装、适用于 NSX for vSphere 计算的无重新引导维护升级模式、适用于 vSphere 计算的全新就地升级模式以及用于从 NSX Data Center for vSphere 迁移到 NSX-T Data Center 的迁移协调器。

NSX-T Data Center 2.4 版本提供了以下新功能和增强功能。

管理集群

NSX-T Data Center 2.4 现在支持创建管理器集群以实现用户界面和 API 的高可用性。此集群支持使用两个外部均衡器实现冗余和分布负载，也支持通过 NSX 提供的虚拟 IP 实现冗余。此外，管理平面功能和中央控制平面功能已合并到这一全新管理集群，减少了需要通过 NSX 管理来部署和管理的虚拟设备的数量。NSX Manager 设备提供三种不同的规模，分别适用于不同的部署方案。小型设备适用于实验室或概念证明部署。中型设备适用于 64 个主机的部署环境，而大型设备适用于部署到大型环境的客户。有关最高配置的详细信息，请参见 VMware 最高配置工具，网址为：https://configmax.vmware.com

支持单一集群设计

支持具有合并的 Edge+管理+计算虚拟机的单一集群设计，所有这些虚拟机由单个物理主机中的单个 N-VDS 提供支持。VCF SP 客户的典型参考设计要求使用 4 个 10G pNIC 以及两个主机交换机；一个交换机用于 Edge+管理虚拟机，另一个交换机用于计算虚拟机。这有效地隔离了 Edge 虚拟机和计算虚拟机之间的通信，因此，流量离开并返回到主机。不过，随着 25G 网卡变得越来越经济划算，VCF SP 客户正在标准化双 25G 网卡主机；通过采用这种设计，他们可以转向支持具有 2 个 pNIC 的主机的单一 N-VDS。在该设计中，属于同一子网的 Edge 虚拟机和计算虚拟机可以相互通信，流量不会离开并返回到主机上行链路。

策略和 UI

NSX 管理和自动化

- **声明式策略管理** - 通过结果导向的策略语句简化并自动化网络和安全配置。这一新的声明式策略 API 允许用户描述所需的最终目标，由系统推荐最佳的实现方式，从而简化配置步骤。定义整个网络拓扑，并以规范化方式和任意次序进行一次性部署。

用户界面增强功能

- **增强型导航和页面布局：**改进了导航栏和页面布局，减少了访问关键信息所需的单击次数。
- **国际化：**改进了对区域设置特定项目的处理，例如，日期/时间格式、数字格式、时区。

注意：在该版本中已弃用 2.3 版引入的 NSX Policy Manager 网络拓扑可视化功能。

防火墙

分布式防火墙和网关防火墙将支持筛选从 NSX-T Data Center 2.4 传出的 IPv6 流量。此外，此产品还增加了各种操作功能，如下所示：

发布/恢复按钮

整个防火墙表使用一个发布按钮。可用于分布式防火墙和网关防火墙。在 NSX-T Data Center 2.4 之前，每个区域单独有一个发布按钮。将通过 API 实现。此外，也可以选择恢复所做的更改。更改更新时，还可以选择锁定区域。

规则统计信息

每个规则都将包含命中计数、数据包计数、会话计数、字节计数和热度指数。此外，还包含显示的最大值与当前命中计数对比情况。此统计信息可通过按钮重置。

分组增强功能

增加了基于虚拟机操作系统和 Active Directory 组的分组条件。

每个虚拟机的规则可见性

可以通过查看每个虚拟机的逻辑交换机端口关联，获得特定虚拟机的防火墙规则列表。

虚拟机的 IP 发现

默认 IP 发现配置文件正在更新，除包含 ARP 侦听和 DHCP 侦听之外，还将包含基于 VMTools 的 IP 发现。从早期版本升级的现有客户必须更新 IP 发现配置文件才可启用基于 VMTools 的检测。此外，NSX-T 2.4 还支持创建全局 IP 发现配置文件。另外，还进行了以下更改：

1. 提供基于 DHCPv6 的 IPv6 IP 发现和邻居发现机制。
2. 默认情况下，IPv6 发现处于禁用状态。
3. 可以将自动发现的 IP 绑定手动列入白名单或放入忽略列表。
4. 默认情况下，将忽略本地链路 IPv4 地址。

身份防火墙

NSX-T Data Center 2.4 针对分布式防火墙引入了基于身份（用户 ID）的规则。防火墙管理员现在可以根据基于 Active Directory 的组在虚拟机上配置分布式规则。防火墙管理员可以利用此功能根据登录到虚拟机的用户提供防火墙规则。NSX 将自动检测登录/注销的用户，然后相应地为用户启用特定的规则。基于身份的防火墙可以按虚拟机针对单个用户检测并实施规则，甚至跟踪同一虚拟机中具有特定会话的多个用户。防火墙管理员将使用 Active Directory 组作为条件创建 NSX-T 组。NSX-T Manager 将自动从提供的域控制器检索 Active Directory 组列表。防火墙管理员可以控制用户的东西向访问，尤其是在启用终端服务的虚拟桌面环境或远程桌面会话中。

针对上下文感知分布式防火墙实现 L7 应用程序签名

NSX-T Data Center 2.4 能够在分布式防火墙规则中实现基于 L7 的应用程序签名。用户可以结合使用 L3/L4 规则和 L7 应用程序签名，也可以只创建基于 L7 应用程序签名的规则。我们当前仅对服务器-服务器或客户端-服务器通信支持包含各种子属性的应用程序签名。在 NSX-T Data Center 2.4 中，这仅适用于基于 ESXi 的传输节点。

针对上下文感知分布式防火墙实现 FQDN/URL 白名单

NSX-T Data Center 2.4 在分布式防火墙中引入了基于 URL/FQDN 白名单的规则。NSX-T Data Center 引入了使用分布式 DNS 侦听的创新功能，允许来自每个虚拟机的每个连接都拥有自己的 URL/FQDN 解析。防火墙管理员可以使用固有 URL 域，并将其应用于分布式防火墙中的规则。本质上混合访问 SaaS 服务或云端服务的应用程序可以基于访问的 URL 微分段。可以为客户端应用程序或访问 SaaS 应用程序的浏览器细粒度授予访问权限。在 NSX-T Data Center 2.4 中，这仅适用于基于 ESXi 的传输节点。

服务插入

NSX-T Data Center 2.4 引入了广泛的原生安全功能，如第 7 层应用程序标识、FQDN 白名单和身份防火墙，这些功能可实现更精细的微分段。除了分布式防火墙和网关防火墙提供的原生安全控制，NSX 服务插入框架还支持将 IDS/IP、NGFW 和网络监控解决方案等各种类型的合作伙伴服务以透明方式插入到数据路径并从 NSX 内使用，而无需对拓扑进行更改。

在 NSX-T Data Center 2.4 中，服务插入现在支持东西向流量（即，数据中心内虚拟机之间的流量）。数据中心内虚拟机之间的所有流量都可以重定向到一个动态合作伙伴服务链。

东西向服务层面提供自己的转发机制，从而允许基于策略重定向沿着服务链传输的流量。沿着服务层面转发完全由平台自动完成：检测故障并根据需要重定向现有/新流量，执行流量抑制以支持有状态服务，以及可使用多个路径选择策略优化吞吐量/延迟或密度。

客户机侦测

NSX-T Data Center 2.4 为 VMware 合作伙伴引入了客户机侦测服务平台，可帮助他们为 vSphere ESXi Hypervisor 上基于 Windows 的客户机虚拟机工作负载提供基于策略的无代理防病毒和防恶意软件卸载功能。

在 NSX-T Data Center 2.4 中，客户机侦测平台具备以下优势：

- 简化部署和生命周期管理，可将客户机侦测部署合并到 NSX 代理主机准备安装中，无需在每个 ESXi Hypervisor 上部署客户机侦测通用服务虚拟机。
- 跨多个 vCenter 实施基于策略的一致服务。
- 通过合作伙伴 SVM 分级（即，“小型”、“中型”、“大型”合作伙伴设备）增强 VMware 合作伙伴规模。

L2 网络

每个主机多个 N-VDS

除了能够灵活地组织虚拟机流量之外，这种支持每个主机多个 N-VDS 的新功能还有助于遵守 PCI 法规，其中规定虚拟机流量需要严格隔离。

增加此功能后，现在可以将 ENS 上行链路与非 ENS 上行链路分开；这是一个非常有用的功能，因为 ENS 目前还没有与 N-VDS 同等的功能，所以 ENS 支持的工作负载将获得快速路径，但在功能上却较低。

N-VDS 可视化

此功能支持将 N-VDS 作为独立对象进行管理，同时支持细分以深入查看连接的主机等。用户查看特定主机时，会看到 UI 网格视图，其中显示了该主机连接到 N-VDS 的方式。虚拟机内核接口等逻辑接口也显示为 N-VDS 的一部分。相比于主机视图，这是一个巨大改进，可在一个视图中显示接口列表，其中包含所有物理网卡、虚拟机内核接口和所有 OVS 端口。

针对物理网卡支持 LLDP

此功能有助于弥补针对 NSX 实施 LLDP 的不足。它为物理交换机连接提供了可调试性。辨识哪个物理端口连接到主机上哪个接口的功能有助于轻松地对布线问题进行故障排除。此功能适用范围广泛，可适用于加入 NSX 数据平面的所有物理主机（ESXi、KVM、裸机 Linux 主机和裸机 Edge）。

在 Edge 节点上支持代理 ARP

当外部客户端访问具有相同子网地址的服务（例如 LB、IKE 等）时，会触发设备路由。它们会发送 ARP 查询以查询绑定到环回端口的地址，然而，LR 环回端口没有 MAC 地址，因此不响应这些 ARP 查询。这会导致访问问题。

当前的解决办法是，在这些客户端中配置 /32 路由，如环回 IP/32 → 上行链路/CSP，以便可以将流量转发到上行链路/CSP 端口，然后可以转至正确的环回端口。使用 ARP 代理可以帮助克服这一缺点。

L3 网络

MTU 配置增强功能

NSX-T 2.4 提供了两个全新的 MTU 全局参数：

- 全局物理上行链路 MTU，可为 NSX 域中的所有 N-VDS 实例配置 MTU。这可以转换为 GENEVE 封装帧的最大帧大小或 TEP MTU。
    - 上行链路配置文件 MTU 可以替代特定主机上的全局物理上行链路参数。
- 全局逻辑接口 MTU，可为所有逻辑路由器接口配置 MTU。
    - 如果需要，逻辑路由器上行链路 MTU 和 CSP 端口 MTU 可以替代特定端口上的全局逻辑接口 MTU。

这样，在东西向和南北向流量上配置了大于 1500 字节 MTU 的虚拟机可进行端到端通信。

服务路由器间路由

活动/活动模式下的 Tier-0 逻辑路由器现在可以在给定的 Tier-0 逻辑路由器的所有服务路由器 (SR) 部分之间自动建立全网状 iBGP 对等连接。这可以防止配置有多个上行链路的服务路由器中的一个发生故障时导致流量下降。现在，如果目标在其自己的上行链路上不可用，则位于此故障场景中的服务路由器会将流量转发到另一个服务路由器。

DNS 转发器增强功能

- DNS 转发器功能现在可以启用或禁用，而不会丢失其当前配置。
- DNS 转发器功能还通过 API 和 UI 公开统计信息、事件和警报。

支持上行链路间实现 SNAT

NSX-T 2.4 引入了 SNAT（源地址转换）支持，可对通过一个上行链路进入 Tier-0 逻辑路由器并通过另一上行链路离开同一逻辑路由器的流量执行 SNAT。多个 Tier-0 逻辑路由器互连时，此功能非常有用。

在 Tier-0 逻辑路由器上支持代理 ARP

NSX-T 2.4 在 Tier-0 逻辑路由器上行链路上引入了代理 ARP 支持。这样，对于无法在 Tier-0 逻辑路由器的北向路由器上配置路由的环境，可以在其中部署 NSX-T。使用此功能，可以为 NAT、LB 或任何有状态服务配置属于 Tier-0 上行链路网络的 IP 地址。

Edge 节点增强功能

- NSX-T 2.4 在裸机 Edge 节点上引入了支持在快速路径网卡上进行管理的选项，从而不再需要专用的管理网卡。
- 裸机 Edge 节点还支持 25 Gbps Intel 网卡 XXV710。
- Edge 节点支持多个 GENEVE 隧道端点 (TEP)。这使得 Edge 节点不必为实现覆盖网络流量的高可用性而被迫使用 LAG。

BGP 增强功能

- 从 NSX-T 2.4 开始，Tier-0 逻辑路由器支持与北向物理路由器的 iBGP 对等连接。
- NSX-T 2.4 引入了这样一个选项：跨不同 ASN 中的 eBGP 对等项启用 ECMP（AS 路径多路径负载分担），同时支持 Tier-0 逻辑路由器在 AS 路径中允许自己的 ASN（允许 AS 进入）。

IPv6

NSX-T 2.4 引入了 IPv6 路由/转发和安全性。这包括对以下项的支持：

- IPv6 静态路由
- IPv6 邻居发现
- DHCPv6 中继
- IPv6 分布式防火墙 (DFW)
- IPv6 Edge 防火墙
- MP-BGP 的 IPv6 地址系列及关联的前缀列表/路由映射
- IPv6 交换机安全
- IPv6 地址发现
- IPv6 运维工具

运维

流跟踪增强功能

流跟踪增加了对更多故障排除和可视化功能的支持。在 NSX-T 2.4 中，可通过流跟踪了解集中式服务的运行状况，如 Edge 防火墙、负载均衡器、NAT 和基于路由的 VPN。

安装增强功能

- NSX 对 vSphere 计算集群的 NSX 组件使用基于配置文件的新型安装，从而简化了部署。此功能有助于加快部署，确保配置一致性以及避免手动错误，并提供了“一次定义，多次重用”的方法。
- 支持从 UI 进行自动安装并建立 NSX Manager 节点集群。
- 支持更多部署配置，可创建多个 N-VDS 交换机，并通过配置文件迁移 VMKernel 端口和物理适配器。

升级增强功能

- 增强了 ESXi 主机的全面协调升级，无需重新引导主机，而使用默认的维护模式 NSX 升级时需要支持此操作。
- 引入了全新 NSX 升级模式，即“就地”升级。此功能有助于简化操作并加快升级。如果使用此模式，升级 ESXi 主机上的 NSX 组件时不必关闭工作负载的电源或将其迁移到不同的 Hypervisor。
- 引入了一个新的框架并提供了即时可用的测试，可在 NSX 升级期间执行预检查和后期检查，从而有助于在开始实际升级之前或升级之后立即揭示隐匿的底层问题。

NSX 在检测到更改时进行备份

NSX 增强了其灾难恢复解决方案，它能够检测到配置更改并主动将其备份到安全存储。此功能使客户能够更好地满足配置备份 SLA 要求，而无需将不必要的文件备份到存储服务器。

NFV

现在，N-VDS 交换机在 EDP 模式下支持以下增强功能。

- 分布式防火墙
- IP 发现
- SpoofGuard
- IPFIX
- IPv6
- 增强 Edge 虚拟机的性能，现在，在 EDP 模式下，吞吐量提高了 5 倍之多

- 针对多宿主应用程序实现路径冗余。现在，将虚拟机固定到某特定上行链路的功能允许在具有 VTEP 的 NSX 上构建多宿主冗余路径。

运维 - AAA/RBAC 和平台安全性

运维

- **主体身份增强功能：**支持主体身份用户注册并安装 NSX 组件。增加了通过 UI 创建主体身份用户并分配角色的支持。
- **密码策略增强功能：**强制默认密码的最小密码长度为 12 个字符。引入了设置密码过期时间和在密码即将过期时生成警报的功能。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。

- **证书管理：**增加了检查证书吊销状态的功能。

VPN

NSX-T 2.4 针对 VPN 服务增加了以下功能：

- 策略 API 和 GUI 可用于 L3 VPN 和 L2 VPN 服务。
- L3 VPN 服务支持基于证书的身份验证，提高了安全管理。
- L2 VPN 客户端模式支持从 NSX-T SDDC 到 NSX-T SDDC 的 L2 扩展。
- DH 组 19、20 和 21 可用于满足高安全性要求。

负载均衡

NSX-T 2.4 针对负载均衡服务增加了以下功能：

- 提供策略 API 和新型 GUI。仍可在“高级网络和安全”选项卡下使用旧的负载均衡器 GUI。
- 独立服务路由器上的 VIP 可以与集中式服务端口（即 CSP）属于同一子网。在此版本之前，如果要在与 CSP 网络相同的子网上创建 VIP，则必须对此 VIP 使用 CSP IP 地址。否则，必须在不同的网络上创建 VIP。
- 同一 Tier-1 网关上的负载均衡器传输流支持 DNAT 和 Edge 防火墙。在此版本之前，负载均衡器传输流绕过 Edge 防火墙。
- LB 规则支持以“_”开头的 HTTP 标头。通过此增强功能，可以为 vIDM 和 AirWatch 部署 NSX 负载均衡器。
- VIP 可以用作 LB SNAT 的源 IP 地址。
- HTTP 响应标头的最大大小可以配置为 64K 字节。默认大小保持不变，与以前版本一样，为 4K 字节。
- 大型 Edge 虚拟机支持大型 LB 实例。在此版本之前，大型 Edge 虚拟机最多支持中型 LB 实例。

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

NSX-T 2.4 现在提供了迁移协调器，可用于帮助从 NSX Data Center for vSphere 到 NSX-T Data Center 的迁移。此功能设计用于在不使用 vMotion 的情况下迁移现有主机。迁移协调器支持迁移第 2 层网络、第 3 层网络、防火墙、负载均衡和 VPN。《NSX-T Data Center 迁移协调器指南》详细介绍了此工具。

除了部署 NSX-T Manager 和 Edge 节点外，不需要其他计算资源。迁移完成后，客户便可以卸载 NSX for vSphere 以及关联的管理器、控制器和 Edge。请注意，此迁移会影响数据平面流量，且设计为在单个更改窗口中完成。

自动化、OpenStack 和其他 CMP

NSX-T 2.4 通过 Neutron 插件针对 OpenStack 使用引入了以下功能：

- 支持 Rocky 和 Queens
- 支持管理平面集群
  OpenStack Neutron 插件利用建立管理器集群的新功能。它可以在没有外部 VIP 的情况下使用三管理器 REST API 端点，从而提高了性能和可用性。

- 支持 Barbican
  OpenStack Neutron 插件现在支持 Barbican。Barbican 是一个用于安全存储、置备和管理密钥（例如密码、加密密钥和 X.509 证书）的 REST API。这样，可以将负载均衡器的证书作为服务进行管理，以便执行 HTTPS 终止。当前，仅 VIO 环境支持此功能。

NSX-T Terraform 提供程序在 NSX-T 2.4 中为那些既有设置（创建逻辑交换机、路由器、防火墙规则等）增加了以下功能：

- 在负载均衡器和负载均衡器配置（监控器、池等）上支持 CRUD
- 在 DHCP 服务器上支持 CRUD
- 在 NSX-T IPAM（IP 块、IP 池）上支持 CRUD

NSX Cloud

适用于 NSX Cloud 的 NSX-T 2.4 提供了许多新功能，不仅简化了客户的采用/部署流程，在客户执行服务插入和 VPN 终止以及管理其 VDI 环境方面也提供了更多选项，确保客户可以管理真正的多区域、多云混合部署。
以下是 NSX-T 2.4 在 NSX Cloud 中提供的一些主要功能：

- 在转换 VPC/VNET 中共享网关，从而简化并加快了载入和整合
- 通过 VPN 将反向流量传输回内部部署数据中心
- 选择性南北向服务插入和合作伙伴集成
- 在适用于 Azure 的 Horizon Cloud 上进行微分段
- 针对混合工作负载实现基于意向的策略

简化转换 VPC/VNET 架构：从 2.4 开始，客户可以在转换 VPC/VNET 上安装单个 NSX Cloud 网关，并管理最多 10 个计算 VPC/VNET。这简化了中心和分支转换/计算架构，即使计算 VPC 没有对等连接，也会在它们之间启用转换路由。通过使用 NSX 覆盖网络隧道功能，现在可以在覆盖网络隧道中发送 VPC 之间的流量。可以直接在虚拟机级别设置转发策略，以指示应使用 Geneve 封装流量并在覆盖网络中发送，还是在公有云提供商的底层网络中发送流量。通过使用所有这些功能，用户可以更加灵活地在公有云网络内部和外部路由流量。

通过 VPN 传输反向流量：NSX Cloud 现在内置通过 VPN 隧道将流量从公有云反向传输至内部部署数据中心的支持。源自内部部署数据中心的 VPN 现在可以直接在公有云中的 NSX Cloud 网关终止。客户无需公有云供应商提供的 VGW，从而减少了成本。此外，也降低了管理开销，因为 NSX Cloud 网关将自动通过 BGP 传播路由。从 BW 的角度讲，NSX Cloud 在容量上也实现了很大的提升：VPC 间的传输流通过对等 VPC 可以达到 5 Gbps，而通过 VGW 仅为 1 Gbps。

选择性南北向服务插入和合作伙伴集成：客户可以在共享服务/转换架构中直接从公有云商城部署合作伙伴服务。可以对转换 VPC/VNET 中存在的 NSX Cloud 网关进行编程，以根据 NSX 策略选择性地将流量路由到合作伙伴服务设备。对于客户而言，这可以节省大量成本，因为他们不必将所有流量定向通过虚拟 L7 防火墙设备，而此设备是他们为使用公有云购买的，并按照所通过的流量收费。另外，NSX Cloud 中的服务插入不需要通往 VPC/VNET 的 VPN。成本节省更多，操作更少。

在适用于 Azure 的 Horizon Cloud 上进行微分段：NSX Cloud 现在提供了一个与适用于 Azure 的 Horizon Cloud 相结合的解决方案。对于选择在 Azure 中部署 Horizon VDI 环境的客户，NSX Cloud 将提供必要的微分段并保护 VDI 环境的安全。

针对混合工作负载实现基于意向的策略：Cloud Service Manager (CSM) 现与 NSX Manager 集成在一起。客户现在可以从 Policy Manager 定义一个基于意向的策略，而不必担心工作负载的部署位置或者未来将移至的位置。NSX Cloud 将在内部部署数据中心、Azure 和 AWS 之间以一致的方式实施该策略。

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 2 月 28 日。第一版。
2019 年 4 月 2 日。第二版。添加了已知问题：2273651、2279326、2281095 和 2296888。添加了已修复的问题：2199785。
2019 年 4 月 10 日。第三版。添加了已知问题：2203863、2248186、2252738、2277543、2276398、2279326、2281537、2287124、2290688、2294178、2295592、2296430、2297157、2297918 和 2298499。更新了“新增功能”部分以包含“支持单一集群设计”。
2019 年 6 月 20 日。第四版。添加了已知问题 2261818。添加了已修复的问题 2182745。
2019 年 8 月 23 日。第五版。添加了已知问题 2362688、2395334 和 2392093。

已解决的问题

- 已修复问题 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。

- 已修复问题 2279326：在创建具有超过 4 个 IP:端口组合的 IPFIX L2 收集器时，不会显示任何错误
  不会为允许的最大 IP:端口组合数显示错误消息。这没有任何害处，因为如果超过了最大限制，UI 将限制创建标记。

- 已修复问题 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。

- 已修复问题 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）。

- 已修复问题 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。

- 已修复问题 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。

- 已修复问题 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。

- 已修复问题 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。

- 已修复问题 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。

- 已修复问题 2114756：在某些情况下，从 NSX-T 就绪集群中移除主机时不会移除 VIB
  从 NSX-T 就绪集群中移除主机时，某些 VIB 可能仍位于主机上。

- 已修复问题 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。

- 已修复问题 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。

- 已修复问题 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)”。

- 已修复问题 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。

- 已修复问题 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”。

- 已修复问题 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。

- 已修复问题 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”。

- 已修复问题 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。

- 已修复问题 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。

- 已修复问题 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。

- 已修复问题 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。

- 已修复问题 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。

- 已修复问题 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。

- 已修复问题 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。

- 已修复问题 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。

- 已修复问题 2199785：在将运行状况监控器（没有端口号）添加到动态池（具有端口号）时，观察到 nginx 核心转储
  如果使用具有动态成员（具有端口号）的服务器池配置负载均衡，然后尝试关联未配置任何监控端口的运行状况监控器，nginx 可能会崩溃。

- 已修复问题 2182745：以前，在管理器中不验证重新分发规则中的 LE/GE，并且这些值无法正常工作
  重新分发规则在前缀列表中支持 LE/GE。

已知问题

已知问题分为以下几类。

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 2287482：自动发现绑定表可能包括当前未发现的绑定
  在自动发现绑定表中标记为“重复”的绑定可能不再被发现。

  解决办法：无。

- 问题 2278142：交换机 IPFIX 全局配置文件不可编辑
  如果全局配置文件在系统中可用，则无法通过界面对其进行修改或删除，因为没有与全局配置文件对应的工作流。

  解决办法：使用 API 删除此类全局配置文件。

- 问题 2292222：在“解决错误”屏幕上，指纹不正确时不会通知用户
  如果主机准备操作失败，用户可通过单击“NSX 安装失败”解决该问题，但在这种情况下，他们需要提供主机的用户名、密码和指纹。如果用户提供的指纹不正确，系统不会通知用户，问题仍得不到解决。

  没有一种明确的方法知道指纹不正确。请查看记录此 ThumbPrintValidationFailedException 的日志。

  解决办法：提供正确的指纹。

- 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 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。

  解决办法：如果需要内核升级，则必须首先下载新版本内核的适当 Linux 头，并且需要重新编译 openvswitch 数据路径 dkms 软件包。

- 问题 2285544：调用需要指定 ssh_fingerprint 值的 NSX API 时，不再支持 MD5 哈希值
  NSX-T 2.4 不再支持非 FIPS 加密算法、哈希等，其中包括调用备份/还原、file-store 和支持包 NSX API 以及为 ssh_fingerprint 值指定 MD5 哈希值。因此，不再支持 MD5 哈希值。

  解决办法：指定使用不同的哈希算法（例如，SHA256）计算的不同哈希值。

- 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 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。

  解决办法：尝试重新启动失败的服务。

- 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。

  解决办法：手动重放配置更改。

- 问题 2269901：数据包捕获 CLI 中不包含 vmk 接口

无法发出此命令。

解决办法：使用数据包捕获 uw 实现此目的。

- 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 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。

  解决办法：无。

  在将 vNIC 添加为 NS 组的直接成员之前，检查该 vNIC 是否连接到逻辑交换机。

- 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 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。

解决办法：无。您也许可以根据拓扑将虚拟服务器配置为多个 LbService，否则在配置包含虚拟服务器的大规模设置时，响应时间会变长。

- 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 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。

  解决办法：通过 API/UI 删除设备失败后，请使用 force-delete API 手动删除该设备，如下所示：
  `POST api/v1/cluster/nodes/deployments/467a102d-472f-4f43-a93c-08b992b9f471?action=delete&force_delete=true`
  之后，从 vCenter 销毁虚拟机。

- 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。

  解决办法：从主机中移除 SVM，然后再将其添加到集群。

- 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 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。

安装已知问题

- 问题 2238093：如果强制移除 NSX 软件包，则不支持解决程序
  从主机卸载 NSX 时，将强制移除 NSX 软件包。这可能会导致 NSX 软件包处于损坏状态。如果在应用解决程序之前强制删除了 NSX 软件包，则安装 NSX 软件包的解决程序可能无法成功运行。日志位置：`/var/log/proton/nsxapi.log`

  解决办法：无。

  不要强制移除 NSX 软件包。通过 NSX 文档中所述的标准步骤卸载 NSX 组件。

- 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`

解决办法：重新尝试注册 Edge 节点。或者，关闭 Edge 节点的电源。启动时，将建立 MP-MPA 通道。

- 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。

  解决办法：将主机移出集群后再将其重新添加。这会触发对主机应用传输节点配置文件的活动。

- 问题 2284683：当删除并重新添加已注册的计算管理器时，无法删除自动部署的设备
  删除设备失败并显示错误“无法关闭电源 (Failed to power-off)”，并指明找不到计算管理器。

  解决办法：通过 API/UI 删除设备失败后，请使用 force-delete API 手动删除该设备，如下所示：POST api/v1/cluster/nodes/deployments/<node-id>?action=delete&force_delete=true。从 VC 销毁虚拟机。

- 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 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。

  解决办法：发送到主机的每个配置可以将“仅迁移 pNIC”标记设置为 true，或填充“用于安装的 VMK 映射”，但不能同时指定两者。

  1. 使用要求将“仅迁移 pNIC”设置为 true 的主机交换机发送 TN 配置。
  2. 将所有“仅迁移 pNIC”标记设置为 false 以更新 TN 配置，并根据需要填充“用于安装的 VMK 映射”。换句话说，确保发送到 TN 的配置仅在所有主机交换机中将“仅迁移 pNIC”标记设置为 true 或填充“用于安装的 VMK 映射”。必须为需要两者的任何配置进行两次单独的配置调用。

- 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。

  解决办法：在删除传输节点之前，找出有问题的 OVS。

  1. 运行 `ovs-vsctl` show 以找出该 OVS。

2. 将任何工作负载虚拟机接口从 OVS 迁移到 Linux 网桥。
3. 按以下方式删除传输节点：

```
DELETE api/v1/transport-nodes/<uuid>
```

- 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。

  解决办法：重新启动 netcpa 服务。

NSX Manager 已知问题

- 问题 2285306：客户机侦测服务的服务部署状态可能保持“未知”状态，直到服务虚拟机打开电源
  创建服务部署并在“服务部署”网格视图中列出后，状态可能不会立即显示为“正在进行中”，可能仍保持“未知”状态直至网格视图刷新。

  解决办法：无。十秒钟后刷新页面。状态应更新。

- 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。

  解决办法：检查主机配置，重新生成凭据，然后重新尝试添加主机。

- 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。

  解决办法：删除绑定映射并使用所需的新序列号重新创建。

- 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。

  解决办法：无。

NSX Edge 已知问题

- 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。

  解决办法：使用其他计算机或将 NSX-T Edge 部署为 Hypervisor 上的虚拟机。

- 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。

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 NXGI 服务

在 NXGI 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 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。

  解决办法：要防止出现此问题，请手动验证传输节点是否与任何 NS 组相关联。在“管理平面”界面中，导航到**高级网络和安全 > 清单 > 组**或**系统 > 节点 > 传输节点 > 相关 > NS 组**。

- 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。

  解决办法：重新引导受影响的 Edge 节点。

- 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。

  解决办法：先删除 BGP 邻居，然后再删除 IPsec 会话。

- 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。

  解决办法：使用管理平面 API 配置 MTU，即使 CSP 端口是通过策略工作流创建的。

- 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 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。

  解决办法：有关修复输入的说明，请参见实现警报错误详细信息。

- 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。

  解决办法：使用 CLI 命令 `get service router config`，该命令会将 route-map 配置作为整个输出的一部分返回。

- 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。

解决办法：使用 API 执行配置。

- 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。

  解决办法：在部署公有云网关时，为上行链路接口启用公共 IP。

- 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 2288523：卸载 NSX 客户机侦测驱动程序可能会导致安全问题
IDFW 需要 NSX 客户机侦测驱动程序中的用户身份信息。卸载该驱动程序可能会导致从特定客户机登录的用户出现安全问题。这将显示为以下症状：
  - 对于从卸载了客户机侦测驱动程序的某些客户机虚拟机登录的用户，不实施防火墙规则。
  - 对于从卸载了客户机侦测驱动程序的某些客户机虚拟机登录的用户，用户详细信息中未记录 IDFW 组件。
  - 即使主机上已启用 IDFW，MUX 日志也不会显示来自这些客户机虚拟机的任何连接。
  - 即使主机上已启用 IDFW，MUX 日志也不会显示来自这些客户机虚拟机的任何网络事件。

  因此，默认全部拒绝规则会阻止从卸载了客户机侦测驱动程序的客户机虚拟机登录的用户进行访问。

  解决办法：无。IT 管理员应遵循安全最佳做法，以确保没有用户有权卸载客户机虚拟机内的客户机侦测驱动程序。

- 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。

  解决办法：使用新 API。

- 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`。

  解决办法：以 L4PortSet 服务的形式为 TFTP 创建新服务并在防火墙规则中使用。

- 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。

  解决办法：使用 TCP 测试身份防火墙规则。在配置身份防火墙规则时，切勿在服务列中设置 ANY/UDP/ICMP

- 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 2252738 - 对于完全限定域名 (FQDN) 规则，允许将与规则不匹配的数据包传送到目标。

在创建特定的 FQDN 规则时，将在防火墙数据库匹配规则中添加与一个 IP 地址关联的域名，并允许将发送到该域名的数据包传送到服务器。不过，如果用户在域名服务器上更改与该 IP 地址关联的域名，则不会在防火墙数据库中更新该域名条目（除非存在另一个与新域名匹配的 FQDN 规则）。因此，即使 FQDN 规则应丢弃数据包，也会将数据包发送到新域名。

解决办法：无。

- 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 https://kb.vmware.com/s/article/71217。

KVM 网络连接已知问题

- 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。

  解决办法：任何 DFW 规则的更新可清除此错误情况。例如，只切换规则日志记录，KVM DFW 模块就会清除此错误情况。

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 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。

  解决办法：有关解决办法，请参阅知识库文章 67400 NSX-T 2.4.0 负载均衡服务可能会在 HTTPs 上观察到性能下降。

- 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 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

会在不到 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`

解决办法：无。

- 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。

  解决办法：如果主机上的 mux 和 opsagent 尚未运行，请尝试将其手动启动。

  1. 以 root 用户身份登录到主机并执行以下命令：
     `/etc/init.d/nsx-opsagent start`
     `/etc/init.d/nsx-context-mux start`
  2. 启动代理后，等待几分钟并确认 UI 上的运行状况时间戳已更新。

升级已知问题

- 问题 2273737：从 NSX-T 2.3 升级到 2.4 后，vIDM 服务器详细信息缺失
如果使用 vIDM，即仅在 NSX 策略设备上配置 vIDM 服务器，则在升级中迁移 vIDM 服务器，但融合设备中将缺少 vIDM 服务器。

  解决办法：有两种方案可供选择，具体取决于客户何时遇到此问题：

  - 从版本 2.3 升级到 2.4 之前：
    在 NSX 策略设备和 NSX Manager 虚拟机上配置相同的 vIDM 服务器详细信息。
  - 从版本 2.3 升级到 2.4 之后：
    在融合设备上重新配置相同的 vIDM 服务器详细信息。

- 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 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。

  解决办法：不用创建空白组。

  要继续进行，请执行以下操作之一：

  - 删除空白组
  - 单击恢复按钮以完成升级
  - 重置计划
- 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。

解决办法：在“主机升级”页面上，单击“重置”选项，重建计划，以便 UC 升级计划与 VC 集群同步。

- 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。

  解决办法：首先，避免添加旧版本的 Edge 节点。如果遇到此问题，请重新启动 UC 服务。

- 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”。

  解决办法：无。功能应不受影响。

- 问题 2293227：升级到 2.4 后，IDFW 规则不适用于运行 VMTools 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 VMTools 10.3.5 的虚拟机，从而导致这些虚拟机可能失去 AV 保护。

  解决办法：重新启动受影响的虚拟机。

- 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。

  解决办法：在同一 Edge 节点上启用和禁用维护模式。

- 问题 2294178 - 从 2.3.1 升级到 2.4 期间，主机 VIB 更新失败。
  从 2.3.1 到 2.4 版的升级过程可能会失败，并显示“在主机上安装脱机包失败”错误。更具体地说，主机 VIB 更新失败，因为无法卸载交换机安全模块。如果在交换配置文件中启用了 IP 发现功能，在运行 ESXi-6.7EP06（内部版本 11675023）的主机上执行从 NSX-T 2.3.1 到 NSX-T 2.4 的就地升级时，已知会出现该问题。

  解决办法：有关解决办法，请参阅知识库文章 67445 在启用 IP 发现的情况下，从 NSX-T 2.3.1 升级到 NSX-T 2.4 时，主机 VIB 更新可能会失败。

- 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 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.)

解决办法：从受影响的集群中分离传输节点配置文件，然后使用“移除 NSX”工作流。

- 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。

API 已知问题

NSX Policy Manager 已知问题

- 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`

  解决办法：要防止出现此问题，请在创建策略时始终使用 sequence_number 或 url 参数 `action=revise&operation=insert_top`

- 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。

  解决办法：如果遇到此问题，可以通过更改 LbVirtualServer 上的组设置进行更正。

- 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。

  解决办法：要避免该问题，请配置路由映射以将 IPv6 连接的地址在 BGP 更新中作为下一跃点进行筛选。

NSX Cloud 已知问题

- 问题 2287884：NSX Cloud 不支持某些 Centos marketplace 映像
  NSX Cloud 只支持发行版与预期的次要内核版本匹配的 Centos marketplace 映像。
  例如，发行版及其相应的内核版本应如下所示：
  - RHEL 7.5 3.10.0-862
  - RHEL 7.4 3.10.0-693
  - RHEL 7.3 3.10.0-514

  解决办法：仅使用文档中建议的 Centos 发行版。

- 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 2280663：在少数情况下，并行卸载多个 VPC 可能会导致失败
  卸载某个计算 VPC 会失败。

  解决办法：手动清理 VPC 和策略上的相应组。

- 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。

- 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。

  解决办法：要从该问题中恢复，请执行以下步骤：

  1. 确保在受影响的主机上升级 PCG，以便虚拟机可以下载最新的主机组件。
  2. 重新引导虚拟机以进入正常状态。
  3. 手动运行卸载 cmd。
  4. 手动运行安装 cmd。

版权所有 © 2022 VMware, Inc. 保留所有权利。