



NSX Container Plugin 2.4.1 发行说明

VMware NSX Container Plugin 2.4.1 | 2019 年 5 月 9 日

请定期查看以了解本文档的新增内容和更新。

发行说明内容

本发行说明包含以下主题：

- [新增功能](#)
- [兼容性要求](#)
- [已解决的问题](#)
- [已知问题](#)

新增功能

NSX Container Plugin (NCP) 2.4.1 具有以下新功能：

- 使用单个分布式防火墙区域进行运行状况检查
在每个集群中使用单个分布式防火墙区域，以包含具有活动状态探测和就绪状态探测的 pod 所需的所有防火墙规则。限制为在一个集群中最多包含 1000 个具有活动状态探测或就绪状态探测的 pod，因为在一个分布式防火墙区域中最多可以具有 1000 个规则。
- 让 NSX 节点代理处理 `privsep` 守护进程意外终止
已增强 NSX 节点代理以处理 `privsep` 守护进程意外终止并从中恢复。
- 定义 Kubernetes 服务自动缩放的最大限制
通过使用新的 NCP configMap 选项 `max_allowed_virtual_servers`，用户可以定义允许在集群中创建的最大虚拟服务器数。
- 能够为 Kubernetes Ingress 分配特定的 IP
用户可以使用 NCP configMap 中的 `http_and_https_ingress_ip` 选项为 Ingress 分配 IP 地址。
- 能够为 Kubernetes Ingress 设置 X-Forwarded-For
- 能够设置 Kubernetes Ingress 持久性超时
添加了 NCP configMap 选项 `l7_persistence_timeout`，以在支持 Kubernetes Ingress 的第 7 层虚拟服务器的持久性配置文件中控制超时。
- 支持 NodePort 类型的 Kubernetes 服务
NodePort 允许从集群外部访问 Kubernetes 服务。kube-proxy 自动配置虚拟机主机以将流量中继到 pod。应在虚拟机主机上配置正确的 iptables 规则以允许进行转发（例如，`iptables -I FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT`）。如果 Kubernetes 网络策略隔离了目标 pod，管理员应配置网络策略以允许来自主机 IP CIDR 的流量访问 pod 中的服务，然后 NCP 自动添加相应的防火墙规则以允许流量通过。

兼容性要求

产品	版本
----	----

NCP/NSX-T Tile for PAS	2.4.1
NSX-T	2.3.1、2.4.0.1、2.4.1
Kubernetes	1.13、1.14
OpenShift	3.11
Kubernetes 主机虚拟机操作系统	Ubuntu 16.04、CentOS 7.5、CentOS 7.6
OpenShift 主机虚拟机操作系统	RHEL 7.6
OpenShift BMC	RHEL 7.6
PAS (PCF)	OpsManager 2.5 + PAS 2.5 OpsManager 2.4 + PAS 2.4

已知问题

- **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，StatefulSet 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，StatefulSet 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。

- **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

- **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 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
在安装有 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 软件包中的文件产生冲突。

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。

- 问题 2224218：删除服务或应用程序后，需要 2 分钟的时间才会将 SNAT IP 释放回 IP 池
如果删除服务或应用程序并在 2 分钟内重新创建，将从 IP 池中获取新的 SNAT IP。

解决办法：删除服务或应用程序后，如果要重用相同的 IP，请等待 2 分钟然后再重新创建。

- 问题 2330811：如果在 NCP 关闭时创建 LoadBalancer 类型的 Kubernetes 服务，可能在重新启动 NCP 后无法创建这些服务
在 LoadBalancer 类型的 Kubernetes 服务耗尽 NSX-T 资源时，您可以在删除一些现有的服务后创建新的服务。不过，如果在 NCP 关闭时删除并创建服务，NCP 将无法创建新服务。

解决办法：在 LoadBalancer 类型的 Kubernetes 服务耗尽 NSX-T 资源时，请勿在 NCP 关闭时执行删除和创建操作。

- 问题 2317608：不支持安装多个 CNI 插件
Kubernetes 需要一个包含插件配置列表的 `.conflist` 类型的 CNI 配置文件。Kubelet 将按定义的顺序逐个调用在此 `conflist` 文件中定义的插件。目前，`nsx-cf-cni bosh` 版本仅支持单个 CNI 插件配置。任何其他 CNI 插件都将覆盖指定 `cni_config_dir` 中的现有 CNI 配置文件 `10-nsx`。

解决办法：无。NCP 2.5 中已修复此问题。