NSX Container Plugin 2.4 发行说明

VMware NSX Container Plugin 2.4 | 2019 年 3 月 7 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

新增功能

NSX Container Plugin (NCP) 2.4 具有以下新增功能：

- VMware-NSX-T tile 包的 Foundation 名称现在是可选的。如果未指定，则设置为 PAS 部署的名称。
- NCP HA 在 Kubernetes 上默认处于启用状态。
- NCP/nsx_node_agent 将在后端连接失败时退出。
  增加了 connect_retry_timeout 配置选项。可使用此选项配置 NCP/nsx_node_agent 在退出之前恢复与 NSX Manager、容器协调器适配器或 Hyperbus 的连接所需的时间（以秒为单位）。
- 支持 LoadBalancer 类型服务的会话关联性。
  除了 configMap 选项 l4_persistence，NCP 现在支持在 LoadBalancer 类型服务的服务规范上配置 SessionAffinity。如果 l4_persistence 设置为“无”，则服务规范上的 sessionAffinity 配置将仅确定持久性效果。否则，将为所有 LoadBalancer 类型的服务启用会话关联性，并且用户可以使用服务规范上的 sessionAffinity 配置来控制持久性超时。
- 如果在 LoadBalancer 类型的 Kubernetes 服务的 loadBalancerIP 规范中提供 IP 地址，则该服务将在此 IP 地址上对外公开。
- 支持 NSX Manager 集群。

注意：NCP 将忽略具有 SSL 直通和重新加密终止的 OpenShift 路由。

兼容性要求

产品	版本
NCP/NSX-T Tile for PAS	2.4
NSX-T	2.3、2.3.1、2.4
Kubernetes	1.12、1.13
OpenShift	3.10、3.11
Kubernetes 主机虚拟机操作系统	Ubuntu 16.04，RHEL 7.5、7.6，CentOS 7.4、7.5

OpenShift 主机虚拟机操作系统	RHEL 7.4、7.5、7.6，CentOS 7.4、7.5
PAS (PCF)	OpsManager 2.3.x + PAS 2.3.x OpsManager 2.4.x（2.4.0 除外）+ PAS 2.4.x（2.4.0 除外）

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，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。

- 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 2194367：NSX-T Tile 当前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 2218008：将不同的 Kubernetes 集群配置为使用相同的 IP 块会导致连接问题
  如果将不同的 Kubernetes 集群配置为使用相同的 IP 块，某些 pod 将不能与其他 pod 或外部网络进行通信。

  解决办法：不要将不同的 Kubernetes 集群配置为使用相同的 IP 块。

- 问题 2263536：NodePort 类型的 Kubernetes 服务无法转发流量
  对于 NodePort 类型的服务，Kubernetes 节点就像一个路由器，可将流量从集群外部转发至 pod。设置此类节点时，有时 iptables 中的规则未正确配置为允许流量通过。

  解决办法：运行以下命令，手动向 iptables 中添加规则：

  ```
  iptables -I FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
  ```

  请注意，此方法仅适用于具有“externalTrafficPolicy: Cluster”的 NodePort 服务，而不适用于具有“externalTrafficPolicy: Local”的 NodePort 服务。