NSX Container Plugin 2.4.1 版本說明

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

請定期查看此文件的增補和更新。

版本說明的內容

此版本說明涵蓋下列主題：

新增功能

NSX Container Plugin (NCP) 2.4.1 具有下列新功能：

- **將單一分散式防火牆區段用於健全狀況檢查**
  對每一叢集使用單一分散式防火牆區段，以包含具備活躍性探查和整備性探查的網繭所需的所有防火牆規則。叢集中此限制的上限為具備活躍性探查或整備性探查的 1000 個網繭，因為一個分散式防火牆區段中最多可能有 1000 個規則。
- **讓 NSX 節點代理程式處理 `privsep` 精靈未預期的終止**
  已增強 NSX 節點代理程式，以處理並復原未預期的 `privsep` 精靈終止。
- **定義 Kubernetes 服務自動調整的上限**
  利用新的 NCP configMap 選項 `max_allowed_virtual_servers`，使用者可以定義在叢集內允許建立的虛擬伺服器數目上限。
- **能夠為 Kubernetes 入口指派特定 IP**
  使用者可以在 NCP configMap 中使用 `http_and_https_ingress_ip` 選項，為入口指派 IP 位址。
- **能夠為 Kubernetes 入口設定 X 轉送**
- **能夠設定 Kubernetes 入口持續性逾時**
  已新增 NCP configMap 選項 l7_persistence_timeout，以控制支援 Kubernetes 入口的第 7 層虛擬伺服器的持續性設定檔上的逾時。
- **支援類型 NodePort 的 Kubernetes 服務**
  NoderPort 允許從叢集外部存取 Kubernetes 服務。kube-proxy 會自動設定虛擬機器主機，以將流量轉送至網繭。應在虛擬機器主機上設定適當的 iptables 規則，以允許發生轉送 (例如，`iptables -I FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT`)。如果目標網繭透過 Kubernetes 網路原則隔離，管理員應設定網路原則，以允許來自主機 IP CIDR 的流量可存取網繭中的服務，使得 NCP 會自動新增相關的防火牆規則，以允許流量通過。

相容性需求

產品	版本

NCP/用於 PAS 的 NSX-T 圖標	2.4.1
NSX-T	2.3.1、2.4.0.1、2.4.1
Kubernetes	1.13、1.14
OpenShift	3.11
Kubernetes 主機虛擬機器作業系統	Ubuntu 16.04、CentOS 7.5、CentOS 7.6
OpenShift 主機虛擬機器作業系統	RHEL 7.6
OpenShift BMC	RHEL 7.6
PAS (PCF)	OpsManager 2.5 + PAS 2.5 OpsManager 2.4 + PAS 2.4

已知問題

- 問題 2118515：在大規模設定中，NCP 需要花很長時間，在 NSX-T 中建立防火牆
  在大規模設定 (例如，250 個 Kubernetes 節點、5000 個網繭、2500 個網路原則) 中，NCP 可能需要花幾分鐘時間，在 NSX-T 中建立防火牆區段和規則。

  因應措施：無。建立防火牆區段和規則後，效能應會恢復正常。

- 問題 2125755：執行 Canary 更新和階段式輪流更新時，StatefullSet 可能會中斷網路連線
  如果在 NCP 升級至目前版本之前已建立 StatefulSet，StatefullSet 可能會在執行 Canary 更新和階段式輪流更新時中斷網路連線。

  因應措施：在 NCP 升級至目前版本後建立 StatefulSet。

- 問題 2131494：將入口類別從 nginx 變更為 nsx 之後，NGINX Kubernetes 入口仍然正常運作
  當您建立 NGINX Kubernetes 入口時，NGINX 會建立流量轉送規則。如果將入口類別變更為任何其他值，即使您在變更類別後刪除 Kubernetes 入口，NGINX 也不會刪除規則，並且會繼續套用這些規則。這是 NGINX 的限制。

  因應措施：若要刪除 NGINX 所建立的規則，請在類別值為 nginx 時刪除 Kubernetes 入口。然後，重新建立 Kubernetes 入口。

- 對於類型為 ClusterIP 的 Kubernetes 服務，不支援以用戶端 IP 為基礎的工作階段相似性
  對於類型為 ClusterIP 的 Kubernetes 服務，NCP 不支援以用戶端 IP 為基礎的工作階段相似性。

  因應措施：無

- 對於類型為 ClusterIP 的 Kubernetes 服務，不支援 hairpin-mode 旗標
  對於類型為 ClusterIP 的 Kubernetes 服務，NCP 不支援 hairpin-mode 旗標。

  因應措施：無

- 問題 2193901：不支援單一 Kubernetes 網路原則規則的多個 PodSelector 或多個 NsSelector
  套用多個選取器僅允許來自特定網繭的傳入流量。

  因應措施：改為在單一 PodSelector 或 NsSelector 中搭配使用 matchLabels 和 matchExpressions。

- 問題 2194646：NCP 關閉時，不支援更新網路原則
  如果 NCP 關閉時您更新網路原則，NCP 恢復運作時，網路原則的目的地 IP 集會不正確。

  因應措施：NCP 啟動時，重新建立網路原則。

- 問題 2192489：停用 PAS 導向器組態中的「BOSH DNS 伺服器」後，Bosh DNS 伺服器 (169.254.0.2) 仍會顯示在容器的 resolve.conf 檔案中。
  在執行 PAS 2.2 的 PAS 環境中，停用 PAS 導向器組態中的「BOSH DNS 伺服器」後，Bosh DNS 伺服器 (169.254.0.2) 仍會顯示在容器的 resove.conf 檔案中。這會導致具有完整網域名稱的 Ping 命令花費很長時間。PAS 2.1 不存在此問題。

  因應措施：無。此為 PAS 問題。

- 問題 2199504：NCP 建立的 NSX-T 資源的顯示名稱限制為 80 個字元
  當 NCP 在容器環境中為資源建立 NSX-T 資源時，它會透過組合叢集名稱、命名空間或專案名稱和容器環境中的資源名稱，來產生 NSX-T 資源顯示名稱。如果顯示名稱長於 80 個字元，將被截斷為 80 個字元。

  因應措施：無

- 問題 2199778：在 NSX-T 2.2 中，不支援名稱長度超過 65 個字元的入口、服務和密碼
  在 NSX-T 2.2 中，將 `use_native_loadbalancer` 設定為 `True` 時，類型為 LoadBalancer 的入口和服務參考的入口、密碼和服務的名稱長度必須小於或等於 65 個字元。否則，入口或服務將無法正常運作。

  因應措施：設定入口、密碼或服務時，指定長度為小於或等於 65 個字元的名稱。

- 問題 2065750：安裝 NSX-T CNI 套件失敗，並顯示檔案衝突
  在安裝了 Kubernetes 的 RHEL 環境中，如果您使用 `yum localinstall` 或 `rpm -i` 安裝 NSX-T CNI 套件，會看到錯誤，指示與 kubernetes-cni 套件中的檔案衝突。

  因應措施：使用命令 `rpm -i --replacefiles nsx-cni-2.3.0.xxxxxxxx-1.x86_64.rpm` 安裝 NSX-T CNI 套件。

- 問題 2224218：刪除服務或應用程式後，需要 2 分鐘才能將 SNAT IP 釋放回 IP 集區
  如果您刪除服務或應用程式，並在 2 分鐘內重新建立，它將從 IP 集區取得新的 SNAT IP。

  因應措施：刪除服務或應用程式後，如果您想要重複使用相同的 IP，則等待 2 分鐘之後再重新建立服務或應用程式。

- 問題 2330811：在 NCP 關閉的情況下建立類型 LoadBalancer 的 Kubernetes 服務時，NCP 重新啟動時可能不會建立服務
  類型 LoadBalancer 的 Kubernetes 服務的 NSX-T 資源用盡時，您可以在刪除部分現有的服務後建立新服務。但是，如果您在 NCP 關閉時刪除並建立服務，NCP 將無法建立新服務。

  因應措施：類型 LoadBalancer 的 Kubernetes 服務的 NSX-T 資源用盡時，在 NCP 關閉時請勿執行刪除和建立作業。

- 問題 2317608：不支援多個 CNI 外掛程式
  Kubernetes 預期類型為 .conflist 的 CNI 組態檔，其中包含外掛程式組態的清單。Kubelet 將按照定義的順序逐一呼叫在此 conflist 檔案中定義的外掛程式。目前，nsx-cf-cni bosh 版本僅支援單一 CNI 外掛程式組態。任何其他 CNI 外掛程式將覆寫指定的 cni_config_dir 中現有的 CNI 組態檔 10-nsx.conf。

  因應措施：無。此問題在 NCP 2.5 中已修正。

Copyright © 2022 VMware, Inc. 保留所有權利。