

Versionshinweise zu NSX Container Plug-In 2.4.1

VMware NSX Container Plugin 2.4.1 | 9. Mai 2019

Überprüfen Sie regelmäßig, ob Erweiterungen und Updates für dieses Dokument zur Verfügung stehen.

Inhalt dieser Versionshinweise

Diese Versionshinweise decken die folgenden Themen ab:

- [Neuigkeiten](#)
- [Kompatibilitätsanforderungen](#)
- [Behobene Probleme](#)
- [Bekannte Probleme](#)

Neuigkeiten

NSX Container Plug-In (NCP) 2.4.1 weist folgende neuen Funktionen auf:

- Verwendung eines einzelnen Abschnitts der verteilten Firewall für die Integritätsprüfung
Verwenden Sie einen einzelnen Abschnitt der verteilten Firewall pro Cluster, um alle Firewallregeln anzugeben, die für Pods mit Aktivitäts- und Bereitschaftsprüfung erforderlich sind. Der Grenzwert liegt bei maximal 1.000 Pods mit Aktivitäts- oder Bereitschaftsprüfung in einem Cluster, da ein Abschnitt der verteilten Firewall höchstens 1.000 Regeln enthalten kann.
- Festlegen der Behandlung der unerwarteten Beendigung des `privsep`-Daemons durch den NSX-Knotenagent
Der NSX-Knotenagent wurde dahingehend verbessert, dass er jetzt eine unerwartete Beendigung des `privsep`-Daemons behandelt und den Daemon wiederherstellt.
- Definieren einer Obergrenze für die automatische Skalierung des Kubernetes-Dienstes
Mit der neuen NCP-ConfigMap-Option `max_allowed_virtual_servers` können Benutzer die maximale Anzahl virtueller Server definieren, die im Cluster erstellt werden dürfen.
- Kubernetes-Ingress kann eine bestimmte IP zugewiesen werden
Mit der Option `http_and_https_ingress_ip` können Benutzer Dateneingängen in der NCP-ConfigMap eine IP-Adresse zuweisen.
- Für Kubernetes-Ingress kann X-Forwarded-For festgelegt werden
- Für Kubernetes-Ingress kann eine Persistenz-Zeitüberschreitung festgelegt werden
Die NCP-ConfigMap-Option „`l7_persistence_timeout`“ wurde hinzugefügt, um eine Zeitüberschreitung des Persistenzprofils für virtuelle Server der Schicht 7 zu steuern, die Kubernetes-Ingress unterstützen.
- Unterstützung für Kubernetes-Dienst des Typs „NodePort“
NodePort ermöglicht den Zugriff auf einen Kubernetes-Dienst von außerhalb des Clusters. Kube-Proxy konfiguriert automatisch den VM-Host, damit der Datenverkehr an den Pod weitergeleitet wird. Auf dem VM-Host muss die richtige iptables-Regel konfiguriert werden, damit die Weiterleitung erfolgt (z. B. `iptables -I FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT`). Falls die Ziel-Pods durch die Kubernetes-Netzwerkrichtlinie isoliert sind, muss der Administrator die Netzwerkrichtlinie so konfigurieren, dass sie Host-IP-CIDR-Datenverkehr den Zugriff auf den Dienst im Pod erlaubt. NCP fügt dann automatisch die

entsprechenden Firewallregeln hinzu, damit der Datenverkehr weitergeleitet werden kann.

Kompatibilitätsanforderungen

Produkt	Version
NCP/NSX-T-Kachel für 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-Host-VM-Betriebssystem	Ubuntu 16.04, CentOS 7.5, CentOS 7.6
OpenShift-Host-VM-Betriebssystem	RHEL 7.6
OpenShift BMC	RHEL 7.6
PAS (PCF)	OpsManager 2.5 + PAS 2.5 OpsManager 2.4 + PAS 2.4

Bekannte Probleme

- **Problem 2118515:** In einem umfangreichen Setup benötigt NCP viel Zeit für die Erstellung von Firewalls auf NSX-T
In einem großen Setup (z. B. 250 Kubernetes-Knoten, 5.000 Pods, 2.500 Netzwerkrichtlinien) kann es einige Minuten dauern, bis NCP die Firewallabschnitte und -regeln in NSX-T erstellt hat.

Probleumgehung: Keine. Nachdem die Firewallabschnitte und -regeln erstellt wurden, sollte die Leistung wieder das normale Niveau erreichen.

- **Problem 2125755:** Ein StatefullSet könnte die Netzwerkkonnektivität verlieren, wenn Canary-Updates und gestaffelte fortlaufende Updates durchgeführt werden
Wenn ein StatefullSet erstellt wurde, bevor NCP auf die aktuelle Version aktualisiert wurde, könnte das StatefullSet die Netzwerkkonnektivität verlieren, wenn Canary-Updates und gestaffelte fortlaufende Updates durchgeführt werden.

Probleumgehung: Erstellen Sie ein StatefullSet, nachdem NCP auf die aktuelle Version aktualisiert wurde.

- **Problem 2131494:** NGINX-Kubernetes-Ingress funktioniert weiterhin nach der Änderung der Ingress-Klasse von „nginx“ in „nsx“
Bei der Erstellung eines NGINX-Kubernetes-Ingress erstellt NGINX Regeln für die Weiterleitung des Datenverkehrs. Wenn Sie die Ingress-Klasse in einen anderen Wert ändern, werden die Regeln von NGINX nicht gelöscht und weiterhin angewendet, selbst wenn Sie den Kubernetes Ingress nach der Änderung der Klasse löschen. Dies ist eine Einschränkung von NGINX.

Probleumgehung: Um die von NGINX erstellten Regeln zu löschen, löschen Sie den Kubernetes-Ingress, wenn der Klassenwert „nginx“ lautet. Erstellen Sie dann den Kubernetes-Ingress neu.

- **Für einen Kubernetes-Dienst des Typs „ClusterIP“ wird die Client-IP-basierte Sitzungsaffinität nicht unterstützt**
NCP unterstützt keine Client-IP-basierte Sitzungsaffinität für einen Kubernetes-Dienst des Typs „ClusterIP“.

Probleumgehung: Keine

- Für einen Kubernetes-Dienst des Typs „ClusterIP“ wird das Hairpin-Modus-Flag nicht unterstützt
NCP unterstützt das Hairpin-Modus-Flag für einen Kubernetes-Dienst des Typs „ClusterIP“ nicht.

Problemumgehung: Keine

- **Problem 2193901: Mehrere PodSelectors oder mehrere NsSelectors für eine einzelne Kubernetes-Netzwerkregel wird nicht unterstützt**
Beim Anwenden mehrerer Selektoren ist nur eingehender Datenverkehr von bestimmten Pods möglich.

Problemumgehung: Verwenden Sie stattdessen MatchLabels mit MatchExpressions in einem einzelnen PodSelector oder NsSelector.

- **Problem 2194646: Das Aktualisieren von Netzwerkrichtlinien, wenn NCP heruntergefahren ist, wird nicht unterstützt**
Wenn Sie eine Netzwerkrichtlinie aktualisieren, wenn NCP heruntergefahren ist, ist das Ziel-IPset für die Netzwerkrichtlinie falsch, wenn NCP wieder hochgefahren wird.

Problemumgehung: Erstellen Sie die Netzwerkrichtlinie neu, wenn NCP hochgefahren ist.

- **Problem 2192489: Nach dem Deaktivieren des „BOSH DNS-Servers“ in der PAS Director-Konfiguration wird der Bosh DNS-Server (169.254.0.2) auch weiterhin in der resolve.conf Datei angezeigt.**

In einer PAS-Umgebung, in der PAS 2.2 ausgeführt wird, wird der Bosh DNS-Server (169.254.0.2) nach dem Deaktivieren des „BOSH DNS-Servers“ in der PAS Director-Konfiguration weiterhin in der in der resolve.conf-Datei des Containers angezeigt. Dadurch nimmt ein Ping-Befehl mit einem vollqualifizierten Domännennamen viel Zeit in Anspruch. Dieses Problem liegt bei PAS 2.1 nicht vor.

Problemumgehung: Keine. Hierbei handelt es sich um ein PAS-Problem.

- **Problem 2199504: Der Anzeigename der vom NCP generierten NSX-T Ressourcen ist auf 80 Zeichen begrenzt**
Wenn das NCP eine NSX-T Ressource für eine Ressource in der Container-Umgebung erstellt, generiert es den Anzeigenamen der NSX-T Ressource durch eine Kombination aus Clusternamen, Namespace oder Projektnamen sowie dem Namen der Ressource in der Container-Umgebung. Wenn der Anzeigename länger als 80 Zeichen ist, wird er auf 80 Zeichen abgeschnitten (trunkiert).

Problemumgehung: Keine

- **Problem 2199778: Mit NSX-T 2.2 werden Ingress, Dienste und Secrets mit Namen, die länger sind als 65 Zeichen, nicht unterstützt**
Wenn bei NSX-T 2.2 `use_native_loadbalancer` auf `True` (Wahr) eingestellt ist, dürfen die Namen des eingehenden Datenverkehrs (Ingress), der Secrets und Dienste, auf die vom eingehenden Datenverkehr (Ingress) und Diensten vom Typ LoadBalancer verwiesen wird, max. 65 Zeichen lang sein. Andernfalls funktionieren der eingehende Datenverkehr (Ingress) oder der Dienst nicht ordnungsgemäß.

Problemumgehung: Geben Sie beim Konfigurieren eines eingehenden Datenverkehrs (Ingress), eines Secrets oder Dienstes einen Namen mit max. 65 Zeichen ein.

- **Problem 2065750: Das Installieren des NSX-T CNI-Pakets schlägt mit einem Dateikonflikt fehl**
Wenn in einer Umgebung mit RHEL, in der Kubernetes installiert ist, das NSX-T CNI-Paket mit den Befehlen `yum localinstall` oder `rpm -i` installiert wird, wird ein Fehler angezeigt, der auf einen Konflikt mit einer Datei aus dem Kubernetes-CNI-Paket verweist.

Problemumgehung: Installieren Sie das NSX-T CNI-Paket mit dem Befehl `rpm -i --replacefiles nsx-cni-2.3.0.xxxxxxxx-1.x86_64.rpm`.

- **Problem 2224218: Nach dem Löschen eines Diensts oder einer App dauert es 2 Minuten, bis die**

SNAT-IP wieder im IP-Pool freigegeben wird

Wenn Sie einen Dienst oder eine App löschen und sie innerhalb von 2 Minuten erneut erstellen, erhält er bzw. sie eine neue SNAT IP aus dem IP-Pool.

Problemumgehung: Warten Sie nach dem Löschen eines Diensts oder einer App 2 Minuten, bevor Sie ihn bzw. sie neu erstellen, wenn Sie dieselbe IP wiederverwenden möchten.

- **Problem 2330811: Wenn Kubernetes-Dienste des Typs „LoadBalancer“ erstellt werden, während NCP inaktiv ist, können die Dienste möglicherweise nicht erstellt werden, wenn NCP neu gestartet wird**

Wenn NSX-T-Ressourcen für Kubernetes-Dienste des Typs „LoadBalancer“ ausgeschöpft sind, können Sie neue Dienste erstellen, nachdem einige der vorhandenen Dienste gelöscht wurden. Wenn Sie die Dienste jedoch löschen und erstellen während NCP inaktiv ist, kann NCP die neuen Dienste nicht erstellen.

Problemumgehung: Wenn NSX-T-Ressourcen für Kubernetes-Dienste des Typs LoadBalancer ausgeschöpft sind, dürfen Sie weder das Löschen noch das Erstellen ausführen, während NCP inaktiv ist.

- **Problem 2317608: Mehrere CNI-Plug-Ins werden nicht unterstützt**

Kubernetes erwartet eine CNI-Konfigurationsdatei vom Typ „conflist“, die eine Liste der Plug-In-Konfigurationen enthält. Das Kubelet ruft die in dieser .conflist-Datei definierten Plug-Ins in der angegebenen Reihenfolge nacheinander auf. Derzeit unterstützt die Bosh-Version „nsx-cf-cni“ nur eine einzelne CNI-Plug-In-Konfiguration. Jedes zusätzliche CNI-Plug-In überschreibt die vorhandene CNI-Konfigurationsdatei „10-nsx.conf“ im angegebenen Verzeichnis „cni_config_dir“.

Problemumgehung: Keine. Dieses Problem wurde in NCP 2.5 behoben.