

# Versionshinweise zu NSX Container Plug-In 2.4

VMware NSX Container Plug-In 2.4 | 7. März 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

### Neuigkeiten

NSX Container Plug-In (NCP) 2.4 weist folgende neuen Funktionen auf:

- Der Foundation-Name der VMware-NSX-T-Kachel ist jetzt optional. Wenn nicht angegeben, wird er auf den Namen der PAS-Bereitstellung festgelegt.
- NCP-Hochverfügbarkeit ist standardmäßig auf Kubernetes aktiviert.
- „NCP/nsx\_node\_agent“ wird bei Backend-Verbindungsfehler beendet.  
Die Konfigurationsoption „connect\_retry\_timeout“ wurde hinzugefügt. Mit dieser Option kann die Zeit in Sekunden angegeben werden, die „NCP/nsx\_node\_agent“ für die Wiederherstellung der Verbindung zum NSX Manager, zum Container-Orchestrator-Adapter oder Hyperbus verwenden darf, bevor der Vorgang beendet wird.
- Unterstützung für Sitzungsaffinität für einen Dienst des Typs LoadBalancer.  
Zusätzlich zur configMap-Option „l4\_persistence“ unterstützt NCP jetzt die sessionAffinity-Konfiguration in der Dienstspezifikation für Dienste des Typs LoadBalancer. Wenn „l4\_persistence“ auf „Keine“ festgelegt ist, legt die sessionAffinity-Konfiguration in der Dienstspezifikation lediglich den Persistenzeffekt fest. Andernfalls ist die Sitzungsaffinität für alle Dienste des Typs LoadBalancer aktiviert, und der Benutzer kann die sessionAffinity-Konfiguration in der Dienstspezifikation verwenden, um die Persistenzzeitüberschreitung zu steuern.
- Wenn in der loadBalancerIP-Spezifikation eines Kubernetes-Diensts des Typs LoadBalancer eine IP-Adresse bereitgestellt wird, wird der Dienst extern unter dieser IP-Adresse verfügbar gemacht.
- Unterstützung für NSX Manager-Cluster.

Hinweis: NCP ignoriert OpenShift-Routen mit SSL-Passthrough und Neuverschlüsselungs-Beendigungen.

## Kompatibilitätsanforderungen

Produkt	Version
NCP/NSX-T-Kachel für PAS	2.4
NSX-T	2.3, 2.3.1, 2.4

Kubernetes	1.12, 1.13
OpenShift	3.10, 3.11
Kubernetes-Host-VM-Betriebssystem	Ubuntu 16.04, RHEL 7.5, 7.6, CentOS 7.4, 7.5
OpenShift-Host-VM-Betriebssystem	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 (außer 2.4.0) + PAS 2.4.x (außer 2.4.0)

## 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.

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

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

Problemumgehung: Erstellen Sie ein StatefulSet, 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.

Problemumgehung: 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“.

Problemumgehung: 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 2194367: Die NSX-T Kachel unterstützt derzeit keine PAS-Isolationssegmente, die ihre eigenen Router bereitstellen**

Die NSX-T Kachel funktioniert nicht mit PAS (Pivotal Application Service)-Isolationssegmenten, die ihre eigenen GoRouter und TCPRouter bereitstellen. Der Grund dafür ist, dass NCP die IP-Adressen der Router-VMs nicht abrufen und keine NSX-Firewall-Regeln erstellen kann, welche einen Datenverkehr von den Routern zu den PAS-App-Containern ermöglichen.

Problemumgehung: Keine.

- **Problem 2199504: Der Anzeigenamen 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 Anzeigenamen 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 2218008: Das Konfigurieren verschiedener Kubernetes-Cluster, damit sie denselben IP-Block verwenden, führt zu Konnektivitätsproblemen**

Wenn Sie verschiedene Kubernetes-Cluster so konfigurieren, dass sie denselben IP-Block verwenden, können einige Pods nicht mehr mit anderen Pods oder externen Netzwerken kommunizieren.

Problemumgehung: Konfigurieren Sie verschiedene Kubernetes-Cluster nicht so, dass sie denselben IP-Block verwenden.

- **Problem 2263536: Kubernetes-Dienst des Typs NodePort kann Datenverkehr nicht weiterleiten**

Mit einem Dienst des Typs NodePort fungiert ein Kubernetes-Knoten wie ein Router, der Datenverkehr von außerhalb des Clusters zu den Pods weiterleitet. Bei der Einrichtung solcher Knoten sind manchmal die Regeln in iptables nicht ordnungsgemäß zum Durchlassen von Datenverkehr konfiguriert.

Problemumgehung: Führen Sie den folgenden Befehl aus, um iptables manuell eine Regel hinzuzufügen:

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

Beachten Sie, dass dies nur für einen NodePort-Dienst mit „externalTrafficPolicy: Cluster“ funktioniert. Es funktioniert nicht für „externalTrafficPolicy: Local“.