



# Versionshinweise für VMware NSX-T Data Center 2.3.1 und NSX Container Plug-in 2.3.1

VMware NSX-T Data Center 2.3.1 | 20. Dezember 2018

VMware NSX Container Plug-in 2.3.1 | 8. November 2018

Überprüfen Sie regelmäßig, ob Erweiterungen und Updates für diese Versionshinweise zur Verfügung stehen.

## Inhalt dieser Versionshinweise

Diese Versionshinweise decken die folgenden Themen ab:

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

## Neuigkeiten

### Neuigkeiten in NSX-T Data Center 2.3.1

NSX-T Data Center 2.3.1 ist eine Wartungsversion, die eine Reihe von Problemen behebt, die in früheren Versionen gefunden wurden. Neue Funktionen in NSX-T Data Center 2.3 sowie bekannte und behobene Probleme, die sich auf NSX-T Data Center 2.3.1 beziehen, finden Sie unter [Versionshinweise für NSX-T Data Center 2.3](#).

### Neuigkeiten in NSX Container Plug-in 2.3.1

NSX Container Plug-in (NCP) 2.3.1 ist eine Wartungsversion, die eine Reihe von Problemen, die in früheren Versionen gefunden wurden, behebt und die folgende neue Funktion aufweist:

- Automatisches Skalieren von NSX-T Load Balancern für Kubernetes-LoadBalancer-Dienste. Wenn ein Kubernetes-LoadBalancer-Dienst zusätzliche virtuelle Server erfordert, wird bei Bedarf ein neuer NSX-T Load Balancer erstellt.

## Empfohlene ESXi-Versionen für NSX-T Data Center 2.3.1

- ESXi 6.5 P03 Build 10884925
- ESXi 6.7 U1 Build 10302608

## Kompatibilitätsanforderungen für NCP 2.3.1

Produkt	Version
---------	---------

NCP/NSX-T-Kachel für PAS	2.3.1
NSX-T	2.2, 2.3, 2.3.1
Kubernetes	1.11, 1.12
OpenShift	3.10, 3.11
Kubernetes-Host-VM-Betriebssystem	Ubuntu 16.04, RHEL 7.4, 7.5
OpenShift-Host-VM-Betriebssystem	RHEL 7.4, 7.5
PAS (PCF)	OpsManager 2.2.0 + PAS 2.2.0 OpsManager 2.3.x + PAS 2.3.x

## Behobene Probleme

Die behobenen Probleme werden in die im Folgenden aufgeführten Kategorien unterteilt.

- [Behobene Probleme in NSX-T Data Center 2.3.1](#)
- [Behobene Probleme in NCP 2.3.1](#)

### Behobene Probleme in NSX-T Data Center 2.3.1

- **Problem 2238957: Veraltete Hyperbus-Ports werden nach dem Neustart eines ESXi-Hosts nicht bereinigt**  
Wenn Sie einen ESXi-Host neu starten, ohne die auf dem Host ausgeführten Container-VMs auszuschalten, werden Hyperbus-Ports nicht wie erwartet bereinigt.
- **Problem 2226523: CLI-Befehl „get debug bgp“ funktioniert nicht**  
Bei der Ausführung des CLI-Befehls „get debug bgp“ wird keine Ausgabe erzeugt.
- **Problem 2241365: Während eines Upgrades von NSX-T Data Center 2.2 auf 2.3 verlieren Firewall-geschützte VMs mit ALG (Application Level Gateway)-Datenverkehr Netzwerkkonnektivität**  
Während eines Upgrades von NSX-T Data Center 2.2 auf 2.3 werden VMs von Hosts, auf denen NSX-T Data Center 2.2 ausgeführt wird, auf Hosts migriert, auf denen NSX-T Data Center 2.3 ausgeführt wird. Eine virtuelle Maschine, die durch eine Firewall geschützt ist und ALG-Datenverkehr aufweist, verliert nach der Migration die Netzwerkkonnektivität.
- **Problem 2241378: VPN-Tunnel sind nicht dauerhaft bereit, und Datenverkehr wird verworfen**  
VPN-Tunnel, für die eine Firewall-Drop-Regel konfiguriert ist und die fragmentierten Datenverkehr aufweisen, sind nicht dauerhaft bereit, und Datenverkehr wird verworfen.
- **Problem 2232034: ESXi-Host stürzt beim Erstellen eines Support-Pakets ab, wenn der Host über eine DLR-Bridge mit mehr als 1024 MAC-Adressen verfügt**  
Die Ausführung von vm-support oder des Befehls „net-bridge --mac-address-table \$bridgeName“ führt zu einem Pufferüberlauf, wenn es eine große Zahl von Bridge-Weiterleitungseinträgen gibt.
- **Problem 2216746: Bei einem vMotion-Vorgang oder beim Einschalten wird die Netzwerkkarte einer VM getrennt, und die virtuelle Maschine verfügt über keine Netzwerkkonnektivität**  
Wenn eine große Anzahl von VMs gleichzeitig eingeschaltet oder mit vMotion migriert wird, werden möglicherweise die Netzwerkkarten einiger VMs getrennt, und sie haben keine Netzwerkkonnektivität.
- **Problem 2216747: vMotion-Vorgang für virtuelle Maschine führt zur Trennung ihrer Ports**  
Wenn sich der Speicher einer virtuellen Maschine auf NFS befindet und für sie ein vMotion-Vorgang durchgeführt wird (der von HA ausgelöst werden kann), verliert die virtuelle Maschine die Netzwerkkonnektivität.

- **Problem 2229210: Wiederholte Vorgänge zum Erstellen und Löschen logischer Switch-Ports führen zu Arbeitsspeicherverlust im NSX Controller**  
Dieses Problem wird durch Spoof Guard-Domänenobjekte verursacht, die nicht gelöscht werden, wenn logische Switch Ports gelöscht werden.
- **Problem 2220560: Übermäßige Systemereignisprotokolle in metricRegistry können zu Arbeitsspeicherverlust im NSX Controller führen**  
Nachdem eine große Anzahl von Transaktionen vom NSX Controller verarbeitet wurde, kann die umfangreiche Protokollierung einen Arbeitsspeicherverlust verursachen.
- **Problem 2221286: ARP-Einträge laufen ab, kurz nachdem die VM-Verbindung ausfällt**  
Dieses Problem kann dazu führen, dass VMs für eine bestimmte Zeit nicht erreichbar sind.
- **Problem 2227882: Richtlinienbasiertes VPN fällt mit dem Fehler „No active IPsec SA, deleting childless IKE SA“ aus**  
Der Fehler führt zu einer Neuverhandlung und zum Verwerfen von Datenverkehr.
- **Probleme 2227885 und 2227879: Speicherverlust in IPsec-VPN auf Edge-Knoten mit bestimmten Datenverkehrsmustern beobachtet**  
Wenn UDP-gekapselter ESP-Datenverkehr (Pakete mit Ziel-Port 4500) mit Ziel-IP-Adresse im Besitz von Edge während der folgenden Fenster eingeht:
  - PBR-Redirect-Regeln (genutzt von HCX) werden nach der FIB-Programmierung der umgeleiteten IP-Adresse auf den Loopback-Port programmiert
  - Fehlende Quelladresse für VPN-Tunnel (z. B. bei falschem Verhalten oder Coredump von iked)
- **Problem 2227890: VLAN-ID wird nicht geändert, nachdem die Tunnel-ID in der logischen Port-Konfiguration geändert wurde**  
Wenn Sie einen API-Aufruf für die Änderung der Tunnel-ID eines logischen Ports vornehmen, wird die VLAN-ID nicht geändert.
- **Problem 2230277: Leeren der Laufzeitdaten von Ports während vMotion**  
Bei ESXi 6.5 werden aufgrund eines Problems während der Ausführung von Storage vMotion die Laufzeitdaten auf einem Port geleert, bevor das vMotion-Framework die Daten speichern kann.
- **Problem 2236206: ESXi-Transportknoten verlieren möglicherweise aufgrund eines Arbeitsspeicherverlusts Netzwerkzugriff**  
Dieses Problem kann dazu führen, dass ein ESXi-Transportknoten in einer PKS-Umgebung Netzwerkkonnektivität verliert.

#### Behobene Probleme in NCP 2.3.1

- **Problem 2216781: Die maximale Länge eines Tag-Werts ist in NCP 2.2.x auf 65 Zeichen und in NCP 2.3.0 auf 256 begrenzt**  
NCP 2.3.1 unterstützt für die folgenden Load Balancer-bezogenen Kubernetes-Ressourcen Namen, die die Begrenzung für den Tag-Wert überschreiten:
  - LoadBalancer-Dienst
  - Ingress
  - In einer Ingress-Spezifikation angegebener geheimer Schlüssel
  - In einer Ingress-Spezifikation angegebener Dienst
- **Problem: 2217051: Die IP des virtuellen Servers wird nach Änderung des loadBalancerIP-Werts eines LoadBalancer-Diensts nicht aktualisiert**  
Wenn Sie nach dem Erstellen eines LoadBalancer-Diensts den loadBalancerIP-Wert des Diensts ändern, spiegelt sich die Änderung nicht in der IP des virtuellen Servers des NSX-T Load Balancers wider.
- **Problem 2216085: Nach dem Löschen eines Namespace werden NSX-T Load Balancer-Regeln und -Pools nicht gelöscht**

Wenn Sie Ingress-Ressourcen und NSX-T-Load Balancing konfigurieren, werden virtuelle Server, Pools und Regeln für NSX-T erstellt. Wenn Sie den Namespace löschen, in dem sich die Ingress-Ressourcen befinden, werden einige Regeln und Pools nicht aus NSX-T gelöscht.

## Bekannte Probleme

Die bekannten Probleme gliedern sich in folgende Gruppen.

- [Bekannte Probleme in NSX-T Data Center 2.3.1](#)
- [Bekannte Probleme in NCP 2.3.1](#)

### Bekannte Probleme in NSX-T Data Center 2.3.1

- **Problem 2235834: RDP- und HTTPS-Datenverkehrsproblem, wenn flow-cache aktiviert ist**  
Wenn flow-cache aktiviert ist, können Probleme mit RDP- und HTTPS-Datenverkehr auftreten.

Problemumgehung: Führen Sie auf dem Edge-Knoten die folgenden Befehle aus, um flow-cache zu deaktivieren:

- set dataplane flow-cache disabled
- restart service dataplane
- **Problem 2227975: Zeitweiliger Verlust des TCP-Datenverkehrs über einen Edge-Knoten**  
TCP-Datenverkehr über einen Edge-Knoten wird zeitweilig verworfen. ICMP-Datenverkehr ist nicht betroffen.

Problemumgehung: Deaktivieren Sie auf dem Edge-Knoten flow-cache mit den folgenden Befehlen:

- set dataplane flow-cache disabled
- restart service dataplane

### Bekannte Probleme in NCP 2.3.1

- **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 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.

Problemumgehung: 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.

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 2194845: Die PAS Cloud Foundry-V3-API-Funktion „Mehrere Prozesse pro App“ wird nicht unterstützt  
Wenn Sie die PAS Cloud Foundry V3 API `v3-push` verwenden, um eine App mit mehreren Prozessen zu pushen, erstellt NCP keine logischen Switch-Ports für die Prozesse, mit Ausnahme des Standard-Ports. Das Problem tritt in NCP 2.3.0 und früheren Versionen auf.

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 `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 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 `use_native_loadbalancer` bei NSX-T 2.2 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.