

# Versionshinweise für VMware NSX-T Data Center 2.4

VMware NSX-T Data Center 2.4 | 28. Februar 2019 | Build 12456646

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

## Inhalt dieser Versionshinweise

Diese Versionshinweise decken die folgenden Themen ab:

- [Neuigkeiten](#)
- [Kompatibilität und Systemvoraussetzungen](#)
- [API und CLI-Ressourcen](#)
- [Revisionsverlauf](#)
- [Behobene Probleme](#)
- [Bekannte Probleme](#)

## Neuigkeiten

NSX-T Data Center 2.4 bietet verschiedene neue Funktionen für virtualisierte Netzwerke und Sicherheit für Private Cloud, Public Cloud und Hybrid Cloud. Zu den wichtigsten neuen Funktionen gehören eine neue Intent-basierte Netzwerkbenutzeroberfläche, eine kontextbezogene Firewall, Gast- und Netzwerk-Introspektionsfunktionen, IPv6, hochverfügbare geclusterte Verwaltung, profilbasierte NSX-Installation für vSphere-Computing-Cluster, Wartungs-Upgrade-Modus ohne Neustart von NSX for vSphere-Computing, ein neuer Modus „Direktes Upgrade“ für vSphere-Computing und ein Migrations-Koordinator für das Migrieren von NSX Data Center for vSphere zu NSX-T Data Center.

Die folgenden neuen Funktionen und Verbesserungen sind in der Version NSX-T Data Center 2.4 verfügbar.

### Verwaltungscluster

NSX-T Data Center 2.4 unterstützt jetzt die Möglichkeit, einen Cluster von Managern für die Hochverfügbarkeit der Benutzeroberfläche und der API zu erstellen. Dieses Clustering unterstützt sowohl externe Ausgleichsdienste für Redundanz und Lastverteilung als auch eine von NSX bereitgestellte virtuelle IP für Redundanz. Darüber hinaus wurden die Funktionen „Management Plane“ und „Zentrale Control Plane“ in diesem neuen Verwaltungscluster zusammengefasst, um die Anzahl virtueller Appliances zu reduzieren, die von der NSX-Administration bereitgestellt und verwaltet werden müssen. Die NSX Manager-Appliance ist in drei verschiedenen Größen für unterschiedliche Bereitstellungsszenarien verfügbar. Eine kleine Appliance für Bereitstellungen für Tests oder Machbarkeitsstudien. Eine mittlere Appliance für Bereitstellungen für 64 Hosts und eine große Appliance für Kunden, die eine Bereitstellung für eine große Umgebung durchführen. Details zur Konfiguration von Maximalwerten finden Sie im VMware-Tool für die Konfiguration von Maximalwerten unter: <https://configmax.vmware.com>

Unterstützung für ein Design mit einem einzelnen Cluster

Unterstützung für ein Design mit einem einzelnen Cluster, in dem Edge- + Management- + Computing-VMs, die alle von einem einzelnen N-VDS auf einem einzelnen physischen Host betrieben werden, zusammengefasst sind. Für typische Referenzdesigns für VCF-SP-Kunden sind 4 x 10G-pNICs mit zwei Host-Switches vorgegeben: einer für Edge- + Management- und ein weiterer für Computing-VMs. Dadurch wird die Kommunikation zwischen der Edge-VM und der Computing-VM effektiv isoliert, weshalb der Datenverkehr den Host verlässt und zurückkommt. Durch die mit 25G-Netzwerkkarten möglichen Einsparungen wird 2 x 25G-NIC-Hosts jedoch zunehmend zum Standard für VCF-SP-Kunden und sie können mit diesem Design zu einem einzelnen N-VDS wechseln, der einen Host mit 2 pNICs versorgt. Bei diesem Design können die Edge-VM und die Computing-VM, die zum selben Subnetz gehören, miteinander kommunizieren, ohne dass Datenverkehr die Host-Uplinks verlässt und wieder zurückkehrt.

## Richtlinie und Benutzeroberfläche

### NSX-Verwaltung und Automatisierung

- **Deklarative Richtlinienverwaltung** – Vereinfachen und automatisieren Sie Netzwerk- und Sicherheitskonfigurationen über ergebnisorientierte Richtlinienanweisungen. Diese neue deklarative Richtlinien-API reduziert die Anzahl an Konfigurationsschritten, indem sie zulässt, dass Benutzer gewünschte Endziele beschreiben, während sie zugleich vom System ermitteln lässt, wie diese am besten erreicht werden können. Definieren Sie eine vollständige Netzwerktopologie und stellen Sie alles in einem Zug bereit, und zwar in einer von der Reihenfolge unabhängigen präskriptiven Art und Weise.

### Verbesserungen der Benutzeroberfläche

- **Verbesserungen bei Navigation und Seitenlayout:** Verbesserungen bei der Navigationsleiste und dem Seitenlayout zum Verringern der Anzahl an Klicks für den Zugriff auf kritische Informationen.
- **Internationalisierung:** Verbesserungen bei der Handhabung von Gebietsschema-spezifischen Elementen, wie etwa das Format für Datum und Uhrzeit, das Zahlenformat und die Zeitzone.

**Hinweis:** Die Funktion zur Visualisierung der Netzwerktopologie für NSX Policy Manager, die in Version 2.3 eingeführt wurde, ist in dieser Version veraltet.

## Firewall

Verteilte Firewall und Gateway-Firewalls unterstützen das Filtern von IPv6-Datenverkehr von NSX-T Data Center 2.4. Darüber hinaus wurden dem Produkt verschiedene Betriebsfunktionen hinzugefügt, wie in der nachstehenden Liste aufgeführt:

### Schaltfläche „Veröffentlichen/Wiederherstellen“

Eine einzige Veröffentlichungsschaltfläche ist verfügbar für die gesamte Firewalltabelle. Dies ist sowohl für verteilte als auch für Gateway-Firewalls verfügbar. Vor NSX-T Data Center 2.4 gab es für jeden Abschnitt eine eigene Veröffentlichungsschaltfläche. Dies ist über API verfügbar. Darüber hinaus haben Sie die Möglichkeit, Ihre Änderungen zurückzusetzen. Sie haben auch die Möglichkeit, Abschnitte zu sperren, wenn Änderungen aktualisiert werden.

### Regelstatistiken

Jede Regel weist Angaben zu Anzahl der Treffer, Paketanzahl, Sitzungsanzahl, Byteanzahl und Beliebtheitsindex auf. Sie enthält auch eine Gegenüberstellung der aufgetretenen Maximalwerte und der aktuellen Anzahl der Treffer. Diese Statistiken können über eine Schaltfläche zurückgesetzt werden.

### Verbesserungen bei der Gruppierung

Zusätzliche Gruppierungskriterien basierend auf Betriebssystemen für die VM- und Active Directory-Gruppen sind verfügbar.

### Sichtbarkeit von Regeln pro VM

Eine Liste von Firewallregeln für eine bestimmte VM ist verfügbar, indem Sie sich den für jede virtuelle Maschine zugeordneten Port für den logischen Switch ansehen.

## **IP Discovery für virtuelle Maschinen**

Das standardmäßige IP Discovery-Profil wird derzeit aktualisiert, damit es zusätzlich zu ARP-Snooping und DHCP-Snooping eine VMTools-basierte IP Discovery umfasst. Bestehende Kunden, die ein Upgrade von früheren Versionen durchführen, müssen das IP Discovery-Profil aktualisieren, um eine VMTools-basierte Erkennung zu ermöglichen. Darüber hinaus wird die Erstellung eines globalen IP Discovery-Profiles in Verbindung mit NSX-T 2.4 unterstützt. Außerdem gibt es folgende Änderungen:

1. Auf DHCPv6 basierende IPv6 IP Discovery und Nachbarermittlungsmechanismen sind verfügbar.
2. Die IPv6-Ermittlung ist standardmäßig deaktiviert.
3. Automatisch ermittelte IP-Bindungen können entweder manuell in die Whitelist aufgenommen oder der Liste der ignorierten Bindungen hinzugefügt werden.
4. Local Link-IPv4-Adressen werden standardmäßig ignoriert.

## **Identitätsbasierte Firewall**

Mit NSX-T Data Center 2.4 werden identitätsbasierte (Benutzer-ID) Regeln für die verteilte Firewall eingeführt. Firewalladministratoren können jetzt verteilte Regeln auf virtuellen Maschinen in Active Directory-basierten Gruppen konfigurieren. Mit dieser Funktion können Firewalladministratoren Firewallregeln basierend auf den bei den virtuellen Maschinen angemeldeten Benutzern bereitstellen. NSX erkennt angemeldete/abgemeldete Benutzer automatisch, und dementsprechend werden bestimmte Regeln für die Benutzer aktiviert. Eine identitätsbasierte Firewall kann Regeln für einen einzelnen Benutzer pro VM erkennen und durchsetzen oder sogar mehrere Benutzer mit jeweils eigenen Sitzungen in derselben VM nachverfolgen. Firewalladministratoren erstellen NSX-T-Gruppen mithilfe von Active Directory-Gruppen als Kriterium. NSX-T Manager ruft automatisch eine Liste der Active Directory-Gruppen von den angegebenen Domänen-Controllern ab. Firewalladministratoren können Ost-West-Zugriff von Benutzern insbesondere in Umgebungen mit virtuellem Desktop oder Sitzungen mit Remote-Desktop mit aktivierten Terminaldiensten steuern.

## **L7-Anwendungssignaturen für kontextbezogene verteilte Firewall**

NSX-T Data Center 2.4 bietet die Möglichkeit von L7-basierten Anwendungssignaturen in Regeln für verteilte Firewalls. Benutzer können entweder eine Kombination von L3-/L4-Regeln mit L7-Anwendungssignaturen verwenden oder nur auf L7-Anwendungssignaturen basierende Regeln erstellen. Derzeit werden Anwendungssignaturen mit verschiedenen Unterattributen nur für die Server-Server- oder Client-Server-Kommunikation unterstützt. In NSX-T Data Center 2.4 ist dies nur für ESXi-basierte Transportknoten verfügbar.

## **FQDN-/URL-Whitelisting für kontextbezogene verteilte Firewall**

Mit NSX-T Data Center 2.4 werden auf URL-/FQDN-Whitelisting basierende Regeln für die verteilte Firewall eingeführt. In NSX-T Data Center wird eine Neuerung eingeführt, bei der Verteiltes DNS-Snooping verwendet wird, damit jede Verbindung von jeder VM ihre eigene URL-/FQDN-Auflösung hat. Firewalladministratoren können im Voraus gescannte URL-Domänen verwenden und dies auf Regeln in der verteilten Firewall anwenden. Anwendungen, die hybrider Natur sind und auf SaaS- oder cloudbasierte Dienste zugreifen, können basierend auf den URLs, auf die sie zugegriffen haben, eine Mikrosegmentierung durchführen. Clientanwendungen oder Browsern, die auf SaaS-Anwendungen zugreifen, kann granularitätsbasierter Zugriff gewährt werden. In NSX-T Data Center 2.4 ist dies nur für ESXi-basierte Transportknoten verfügbar.

## **Service Insertion**

Mit NSX-T Data Center 2.4 wird eine große Bandbreite an nativen Sicherheitsfunktionen eingeführt, wie etwa Layer-7-Anwendungsidentität, FQDN-Whitelisting und identitätsbasierte Firewall, wodurch eine noch feiner granulierte Mikrosegmentierung ermöglicht wird. Zusätzlich zu der nativen Sicherheitssteuerung durch die verteilte und die Gateway-Firewall lässt das NSX Service Insertion Framework zu, dass verschiedene Typen von Partnerdiensten, wie etwa IDS/IPS, NGFW und Netzwerküberwachungslösungen, transparent in den Datenpfad eingefügt und aus NSX heraus verbraucht werden, ohne dass Änderungen an der Topologie vorgenommen werden müssen.

In NSX-T Data Center 2.4 unterstützt Service Insertion nun Ost-West-Datenverkehr (d. h. Datenverkehr zwischen den VMs und dem Data Center). Sämtlicher Datenverkehr zwischen VMs und dem Datacenter kann an eine dynamische Kette von Partnerdiensten weitergeleitet werden.

Die Ost-West-Dienstebene stellt ihren eigenen Weiterleitungsmechanismus bereit, der eine richtlinienbasierte Umleitung von Datenverkehr über Dienstketten zulässt. Die Weiterleitung entlang der Dienstebene wird vollständig von der Plattform automatisiert: Fehler werden erkannt, und vorhandene/neue Flows werden nach Bedarf umgeleitet. Flow-Pinning wird zur Unterstützung von statusbehafteten Diensten durchgeführt, und Richtlinien für die Mehrfachpfadauswahl sind zur Optimierung für Durchsatz/Latenz oder Dichte verfügbar.

## Guest Introspection

Mit NSX-T Data Center 2.4 wird die Guest Introspection-Dienstplattform für VMware-Partner eingeführt, um richtlinienbasierte Agent-lose Antivirus- und Anti-Malware-Offload-Funktionen für Windows-basierte Gast-VM-Arbeitslasten auf vSphere ESXi-Hypervisoren bereitzustellen.

In NSX-T Data Center 2.4 bietet die Guest Introspection-Plattform Folgendes:

- Vereinfachte Bereitstellung und Lebenszyklusverwaltung durch Konsolidierung der Guest Introspection-Bereitstellung in der NSX-Agent-Hostvorbereitungs-Installation, wobei eine globale Guest Introspection-Dienst-VM nicht mehr auf jedem ESXi-Hypervisor bereitgestellt werden muss.
- Konsistente richtlinienbasierte Dienste über mehrere vCenter hinweg.
- VMware-Partner skalieren Verbesserungen über die Größenanpassung der Partner-SVM (d. h. die Größen „Klein“, „Mittel“ und „Groß“ für Partner-Appliances).

## L2-Netzwerk

### Mehrere N-VDS pro Host

Diese neue Funktion zur Unterstützung mehrerer N-VDS pro Host bietet außer Flexibilität zum Organisieren von VM-Datenverkehr Einhaltung von PCI-Bestimmungen, bei denen eine strikte Isolierung für den VM-Datenverkehr erforderlich ist.

Mit der Hinzufügung dieser Funktion können nun ENS-Uplinks von Nicht-ENS-Uplinks getrennt werden. Dies ist eine nützliche Funktion, da ENS derzeit nicht über denselben Funktionsumfang wie N-VDS verfügt, sodass ENS-Arbeitslasten schnelle Pfade, aber einen geringen Funktionsumfang aufweisen.

### N-VDS-Visualisierung

Diese Funktion bietet die Möglichkeit, den N-VDS als eigenständiges Objekt mit Drilldown-Fähigkeit zum Anzeigen verbundener Hosts usw. zu verwalten. Beim Betrachten eines bestimmten Hosts kann ein UI-Raster angezeigt werden, das zeigt, wie er mit dem N-VDS verbunden ist. Logische Schnittstellen wie VM-Kernel-Schnittstellen sind ebenfalls als Teil des N-VDS sichtbar. Dies ist eine deutliche Verbesserung gegenüber der Hostansicht. Es wird eine Liste der Schnittstellen angezeigt, die alle physischen Netzwerkkarten, VM-Kernel-Schnittstellen und alle OVS-Ports in einer Ansicht enthält.

### LLDP-Unterstützung für physische Netzwerkkarten

Mit dieser Funktion werden Lücken in der LLDP-Implementierung für NSX geschlossen. Sie bietet Debug-Fähigkeit für die Konnektivität physischer Switches. Die Fähigkeit, zu ermitteln, welche physischen Ports mit welchen Schnittstellen auf einem Host verbunden sind, bietet eine einfache Fehlerbehebung bei Problemen mit der Kabelführung. Der Geltungsbereich dieser Funktion gilt für alle physischen Hosts (ESXi, KVM, Baremetal-Linux-Hosts und Baremetal-Edge), die Teil der NSX-Datenebene sind.

### Unterstützung für Proxy-ARP auf Edge-Knoten

Wenn externe Clients auf Dienste wie LB, IKE usw. mit denselben Subnetzadressen zugreifen, treffen Sie auf Geräte-Routing. Sie senden ARP-Abfragen für diese an Loopback-Ports gebundene Adressen. Die LR-Loopback-Ports verfügen jedoch nicht über die MAC-Adressen und reagieren deshalb nicht auf diese ARP-Abfragen. Dies führt zu Zugriffsproblemen.

Derzeit besteht die Problemumgehung darin, in diesen Clients ein /32-Routing zu konfigurieren, wie etwa „Loopback IP/32 → uplink/CSP“, damit der Datenverkehr an uplink/CSP-Ports weitergeleitet werden kann und anschließend zum korrekten Loopback-Port gelangt. ARP-Proxy ist die richtige Lösung zur Überwindung dieses Nachteils.

## L3-Netzwerk

### Verbesserungen bei der MTU-Konfiguration

NSX-T 2.4 bietet zwei neue globale MTU-Parameter:

- „Global Physical Uplink MTU“, der die MTU für alle N-VDS-Instanzen in der NSX-Domäne konfiguriert. Dies kann als die maximale Frames-Größe für die GENEVE-gekapselten Frames oder TEP-MTU übersetzt werden.
  - Uplink-Profil-MTU kann den globalen physischen Uplink-Parameter auf einem bestimmten Host überschreiben.
- „Global Logical Interface MTU“, der die MTU für alle logischen Router-Schnittstellen konfiguriert.
  - Die Uplink-MTU des logischen Routers und die CSP-Port-MTU können bei Bedarf die globale MTU der logischen Schnittstelle an einem bestimmten Port überschreiben.

Dies ermöglicht End-to-End-Kommunikationen für VMs, die mit einer MTU mit einer Größe von mehr als 1500 Byte für Ost-West- und Nord-Süd-Datenverkehr konfiguriert sind.

### Inter-SR-Routing

Logische Tier-0 Router im Modus „Aktiv/Aktiv“ können jetzt für alle Dienstrouter (Service Routers, SR), die Teil eines vorgegebenen logischen Tier-0 Routers sind, automatisch vollständig vermaschte iBGP-Peerings einrichten. Hierdurch wird verhindert, dass der Datenverkehr im Fall von mit mehreren Uplinks konfigurierten SRs und bei einem Fehler bei nur einem davon zurückgeht. Ein SR in diesem Fehlerszenario leitet jetzt den Datenverkehr an einen anderen SR weiter, wenn das Ziel auf seinen eigenen Uplinks nicht verfügbar ist.

### Verbesserungen bei der DNS-Weiterleitung

- Die DNS-Weiterleitungsfunktion kann nun aktiviert oder deaktiviert werden, ohne dass ihre aktuelle Konfiguration verloren geht.
- Die DNS-Weiterleitungsfunktion zeigt auch Statistiken, Ereignisse und Alarmer über die API und die Benutzeroberfläche an.

### Unterstützung von SNAT von Uplink zu Uplink

Mit NSX-T 2.4 wird die Unterstützung von SNAT (Source Network Address Translation) für Datenverkehr, der bei einem logischen Tier-0-Router über einen Uplink eingeht und denselben logischen Router über einen anderen Uplink verlässt, eingeführt. Diese Funktion ist nützlich, wenn mehrere logische Tier-0 Router miteinander verbunden sind.

### Unterstützung für Proxy-ARP auf einem logischen Tier-0 Router

Mit NSX-T 2.4 wird die Unterstützung für Proxy-ARP auf Uplinks von logischen Tier-0 Routern eingeführt. Hierdurch kann die Bereitstellung von NSX-T in Umgebungen ermöglicht werden, in denen Routing auf den Northbound-Routern des logischen Tier-0 Routers nicht konfiguriert werden kann. Mit dieser Funktion können NAT-, LB-, oder beliebige statusbehaftete Dienste mit IP-Adressen konfiguriert werden, die zum Netzwerk des Tier-0-Uplinks gehören.

### Verbesserungen des Edge-Knotens

- Mit NSX-T 2.4 wird die Option auf dem Bare Metal Edge-Knoten eingeführt, mit der die Verwaltung auf den Fast Path-Netzwerkkarten unterstützt wird, sodass eine dedizierte Verwaltungs-NIC nicht mehr erforderlich ist.
- Der Bare Metal Edge-Knoten unterstützt auch Intel-Netzwerkkarten des Typs XXV710 mit 25 GBit/s.
- Der Edge-Knoten unterstützt Mehrfach-GENEVE-Tunnel-EndPoint (TEP). Dies ermöglicht, dass die Verwendung von LAG für Hochverfügbarkeit des Overlay-Datenverkehrs durch Edge-Knoten nicht erzwungen wird.

### BGP-Verbesserungen

- Ab NSX-T 2.4 unterstützen logische Tier-0 Router iBGP-Peering mit physischen Northbound-Routern.
- Mit NSX-T 2.4 wird die Option eingeführt, mit der ECMP über alle eBGP-Peers in einem anderen ASN (AS-Pfad-Multipath Relax) aktiviert werden kann, und es wird auch unterstützt, dass der logische Tier-0 Router sein eigenes ASN im AS-Pfad (eingehendes AS zulassen) zulässt.

## IPv6

Mit NSX-T 2.4 wird IPv6-Routing/-Weiterleitung und -Sicherheit eingeführt. Dies schließt die Unterstützung für Folgendes ein:

- Statisches IPv6-Routing
- IPv6-Nachbarermittlung
- DHCPv6-Relay
- Verteilte IPv6-Firewall (Distributed Firewall, DFW)
- IPv6-Edge-Firewall
- IPv6-Adressfamilie für MP-BGP und zugehörige Präfixliste/Routenzuordnung
- IPv6-Switch-Sicherheit
- IPv6-Adressermittlung
- IPv6-Ops-Tools

## Betrieb

### Traceflow-Verbesserungen

Traceflow fügt Unterstützung für noch mehr Fehlerbehebungs- und Visualisierungsfunktionen hinzu. In NSX-T 2.4 bietet Traceflow Beobachtungen für zentrale Dienste wie Edge-Firewall, Load Balancer, NAT und routenbasiertes VPN.

### Verbesserungen bei der Installation

- NSX ermöglicht vereinfachte Bereitstellungen mithilfe einer neuen profilbasierten Installation von NSX-Komponenten für vSphere-Computing-Cluster. Mit dieser Funktion werden schnellere Bereitstellungen ermöglicht, die Konfigurationskonsistenz gefördert und Fehler durch manuelle Eingabe vermieden. Darüber hinaus bietet sie eine Möglichkeit, einmal eine Definition vorzunehmen und diese mehrfach wiederzuverwenden.
- Unterstützung für automatisierte Installation und automatisiertes Clustering von NSX Manager-Knoten über die Benutzeroberfläche.
- Unterstützung für mehrere Bereitstellungskonfigurationen, die mehrere N-VDS-Switches erstellen sowie VMKernel-Ports und physische Adapter über Profile migrieren können.

## Verbesserungen beim Upgrade

- Die Verbesserungen dienen der Bereitstellung von vollständig orchestrierten Upgrades von ESXi-Hosts, ohne dass die Kosten eines Hostneustarts mithilfe des standardmäßigen Wartungsmodus „NSX-Upgrade“ entstehen.
- Es wurde ein neuer NSX-Upgrade-Modus mit dem Namen „Direktes Upgrade“ eingeführt. Diese Funktion bietet eine einfache Handhabung und ermöglicht schnellere Upgrades. Bei Verwendung dieses Modus werden Upgrades der NSX-Komponenten auf den ESXi-Hosts durchgeführt, ohne dass Arbeitslasten abgebrochen oder auf einen anderen Hypervisor migriert werden müssen.
- Es wurde ein neues Framework eingeführt und es werden einsatzbereite Tests zum Durchführen von Vorabprüfungen und Nachprüfungen während des NSX-Upgrades bereitgestellt, bei denen zugrunde liegende noch nicht erkannte Probleme zum Vorschein kommen können, bevor Sie mit dem eigentlichen Upgrade beginnen oder unmittelbar nachdem Sie das Upgrade durchgeführt haben.

## NSX-Sicherung bei Erkennung von Änderung

Die Notfallwiederherstellungslösung von NSX wurde verbessert, indem die Möglichkeit der Erkennung von Konfigurationsänderungen und der proaktiven Sicherung in einem sicheren Speicher bereitgestellt wird. Mit dieser Funktion erhalten Kunden ein besseres SLA für die Konfiguration von Sicherungen, ohne dass die Kosten einer Sicherung von unnötigen Daten auf dem Speicherserver entstehen.

## NFV

Der N-VDS-Switch unterstützt jetzt die folgenden Verbesserungen im EDP-Modus.

- verteilte Firewall
- IP Discovery
- Spoof Guard
- IPFIX
- IPv6
- Verbesserte Leistung für die Edge-VM, die jetzt bis zu fünf Mal mehr Durchsatz im EDP-Modus bietet.
- Pfadredundanz für mehrfach vernetzte Anwendungen. Die Funktion zum Pinnen einer VM an einen bestimmten Uplink ermöglicht heute die Konstruktion eines mehrfach vernetzten redundanten Pfads auf NSX mit VTEPs.

## Betrieb – AAA/RBAC und Plattformsicherheit

### Betrieb

- **Verbesserungen bei der Prinzipalidentität:** Prinzipalidentitätsbenutzer können damit NSX-Komponenten registrieren und installieren. Es wurde UI-Unterstützung für die Erstellung von Prinzipalidentitätsbenutzern und die Rollenzuweisung hinzugefügt.
- **Verbesserungen bei der Kennwortrichtlinie** Für Standardkennwörter wird eine Kennwortmindestlänge von 12 Zeichen erzwungen. Es wird die Möglichkeit, Kennwortablaufzeiten festzulegen, eingeführt, und es werden Alarme generiert, wenn das Kennwort demnächst abläuft. Standardmäßig laufen Kennwörter nach 90 Tagen ab. Anweisungen zum Zurücksetzen von Kennwörtern und zum Anpassen des Kennwortablaufs finden Sie im Knowledgebase-Artikel [70691](#).
- **Zertifikatsverwaltung:** Bietet die zusätzliche Möglichkeit, den Sperrstatus des Zertifikats zu überprüfen.

## VPN

In NSX-T 2.4 wurden die folgenden Funktionen für VPN-Dienste hinzugefügt:

- Richtlinien-API und -GUI sind sowohl für L3-VPN- als auch für L2-VPN-Dienste verfügbar.
- L3-VPN-Dienste unterstützen zertifikatsbasierte Authentifizierung für eine bessere

Sicherheitsverwaltung.

- Der L2-VPN-Client-Modus ist zur Unterstützung der L2-Erweiterung von NSX-T-SDDC zu NSX-T-SDDC verfügbar.
- Die DH-Gruppen 19, 20 und 21 sind zur Erfüllung hoher Sicherheitsanforderungen verfügbar.

## Load Balancing

In NSX-T 2.4 wurden die folgenden Funktionen für Load Balancing-Dienste hinzugefügt:

- Eine Richtlinien-API und eine neue GUI sind verfügbar. Die alte Load Balancer-GUI ist noch auf der Registerkarte „Netzwerk und Sicherheit – Erweitert“ verfügbar.
- VIPs auf eigenständigem SR können zum selben Subnetz gehören wie der zentrale Dienstport oder CSP. Wenn Sie vor dieser Version eine VIP im selben Subnetz erstellen wollten, in dem sich das CSP-Netzwerk befand, musste die CSP-IP-Adresse für die VIP verwendet werden. Andernfalls mussten Sie die VIP in einem anderen Netzwerk erstellen.
- DNAT und Edge-Firewall werden für Load Balancer-Datenverkehrsflüsse auf demselben Tier-1-Gateway unterstützt. Vor dieser Version umgingen Load Balancer-Datenverkehrsflüsse die Edge-Firewall.
- LB-Regeln unterstützen HTTP-Header, die mit „\_“ (Unterstrich) beginnen. Mit dieser Erweiterung kann NSX Load Balancer für vDM und AirWatch bereitgestellt werden.
- Eine VIP kann als Quell-IP-Adresse für LB-SNAT verwendet werden.
- Der HTTP-Antwort-Header kann mit einer Maximalgröße von bis zu 64 KB konfiguriert werden. Die Standardgröße bleibt mit 4 KB dieselbe wie in der vorherigen Version.
- Eine große Edge-VM unterstützt eine große LB-Instanz. Vor dieser Version unterstützte die große Edge-VM höchstens eine mittlere LB-Instanz.

## Migration von NSX Data Center for vSphere zu NSX-T Data Center

NSX-T 2.4 verfügt jetzt über einen Migrations-Koordinator, der zur Unterstützung bei der Migration von NSX Data Center for vSphere zu NSX-T Data Center verwendet werden kann. Diese Funktion ist dafür vorgesehen, bestehende Hosts ohne Verwendung von vMotion zu migrieren. Der Migrations-Koordinator unterstützt die Migration von Layer-2-Netzwerk, Layer-3-Netzwerk, Firewall, Load Balancing und VPN. Der *NSX-T Data Center Migration Coordinator Guide* enthält Details zu diesem Tool.

Über die Bereitstellung von NSX-T Managern und Edge-Knoten hinaus sind keine weiteren Computing-Ressourcen erforderlich. Sobald die Migration abgeschlossen ist, kann ein Kunde NSX for vSphere und die zugehörigen Manager, Controller und Edges deinstallieren. Beachten Sie, dass sich diese Migration auf Data Plane-Verkehr auswirkt und dafür konfiguriert ist, dass er in einem einzigen Änderungsfenster abgeschlossen wird.

## Automatisierung, OpenStack und anderer CMP

Mit NSX-T 2.4 werden die folgenden Funktionen für OpenStack-Verbrauch über das zugehörige Neutron-Plug-In eingeführt:

- Unterstützung von Rocky und Queens
- Unterstützung von Clustering auf der Management Plane  
Das OpenStack Neutron-Plug-In nutzt die neue Möglichkeit, über einen Cluster von Managern zu verfügen. Es kann die REST-API-Endpoints der drei Manager verbrauchen, und dies ohne eine externe VIP für zusätzliche Leistung und höhere Verfügbarkeit.
- Unterstützung für Barbican  
Das OpenStack Neutron-Plug-In unterstützt jetzt Barbican. Barbican ist eine REST-API, die für das sichere Speichern, Bereitstellen und Verwalten von geheimen Schlüsseln wie Kennwörtern, Verschlüsselungsschlüsseln und X.509-Zertifikaten vorgesehen ist. Dies ermöglicht die Verwaltung von Zertifikaten für den Load Balancer als Dienst für die HTTPS-Beendigung. Diese Funktion wird derzeit ausschließlich in einer VIO-Umgebung unterstützt.



Mit dem Terraform-Anbieter von NSX-T werden die folgenden Funktionen in NSX-T 2.4 zu den bereits vorhandenen (Erstellung logischer Switches, Router, Firewallregeln usw.) hinzugefügt:

- Möglichkeit der Unterstützung von CRUD im Load Balancer und in der Load Balancer-Konfiguration (Überwachung, Pool usw.)
- Möglichkeit der Unterstützung von CRUD auf DHCP-Servern
- Möglichkeit der Unterstützung von CRUD bei NSX-T-IPAM (IP-Block, IP-Pool)

## NSX Cloud

NSX-T 2.4 für NSX Cloud weist viele neue Funktionen auf, um die Akzeptanz durch bzw. die Bereitstellung für einen Kunden zu erleichtern, dem Kunden mehr Optionen für Service Insertion, VPN-Beendigung und die Verwaltung seiner VDI-Umgebungen zu bieten und damit eine wirklich multiregionale, Multi-Cloud-fähige hybride Bereitstellung zu verwalten.

Nachstehend sind einige der Schlüsselfunktionen in NSX Cloud mit NSX-T 2.4 aufgeführt:

- Gemeinsames Gateway in Transit-VPC/-VNET für vereinfachtes, schnelleres Onboarding und die zugehörige Konsolidierung
- VPN für Backhaul-Datenverkehr zurück zum lokalen Datacenter
- Selektive Nord-Süd-Service Insertion und -Partnerintegration
- Mikrosegmentierung auf Horizon Cloud für Azure
- Intent-basierte Richtlinie für hybride Arbeitslasten

**Vereinfachte Architektur für Transit-VPC/-VNET:** Ab Version 2.4 können Kunden ein einzelnes NSX Cloud-Gateway auf einer Transit-VPC/VNET installieren und bis zu 10 Computing-VPCs/VNETs verwalten. Dies vereinfacht die Hub-and-Spoke-Transit-/Computing-Architektur und aktiviert das transitive Routing zwischen Computing-VPCs, auch wenn diese keine Peering-Verbindung besitzen. Mit NSX-Overlay-Tunneling kann Datenverkehr zwischen VPCs jetzt über einen Overlay-Tunnel gesendet werden. Weiterleitungsrichtlinien können direkt auf VM-Ebene eingerichtet werden, um vorzugeben, ob Datenverkehr GENEVE-gekapselt im Overlay oder im Underlay-Netzwerk des Public-Cloud-Anbieters gesendet werden soll. Alle diese Funktionen bieten mehr Flexibilität im Hinblick darauf, wie Benutzer Daten innerhalb und außerhalb Ihres Public Cloud-Netzwerks weiterleiten können.

**VPN für Backhaul-Datenverkehr:** NSX Cloud bietet nun integrierte Unterstützung für VPN-Tunnel zum Rückholen (Backhaul) von Datenverkehr von der Public Cloud zum lokalen Datacenter. VPNs von einem lokalen Datacenter können nun direkt am NSX Cloud-Gateway in der Public Cloud beendet werden. Die Kunden benötigen das von Public Cloud-Anbietern bereitgestellte VGW nicht, und dies spart Kosten. Auch der Verwaltungsaufwand wird reduziert, da das NSX Cloud-Gateway die Routen automatisch über BGP weitergibt. In Bezug auf die Bandbreite bietet NSX Cloud auch bezüglich der Kapazität einen großen Fortschritt: Inter-VPC-Datenverkehr kann bei 5 GBit/s über Peering-VPCs fließen, im Gegensatz zu 1 GBit/s über VGW.

**Selektive Nord-Süd-Service Insertion und -Partnerintegration:** Kunden können den Partnerdienst direkt über den Public Cloud-Marketplace in der Architektur für gemeinsam genutzte Dienste/Transitarchitektur bereitstellen. Das im Transit-VPC/-VNET vorhandene NSX Cloud-Gateway kann so programmiert werden, dass es den Datenverkehr basierend auf NSX-Richtlinien selektiv an Partnerdienst-Appliances weiterleitet. Dies kann für Kunden enorme Kosteneinsparungen mit sich bringen, da sie nicht gezwungen sind, sämtlichen Datenverkehr über eine virtuelle, für die Public Cloud erworbene L7-Firewall-Appliance zu leiten, deren Kosten auf dem durchgeleiteten Datenverkehr basieren. Doch damit nicht genug: Service Insertion mit NSX Cloud erfordert keine VPNs zu Computing-VPCs/-VNETs. Dies bedeutet weitere Kosteneinsparungen und geringere Betriebskosten.

**Mikrosegmentierung auf Horizon Cloud für Azure:** NSX Cloud weist jetzt eine kombinierte Lösung mit Horizon Cloud für Azure auf. Für Kunden, die eine in Azure bereitgestellte Horizon-VDI-Umgebung wünschen, bietet NSX Cloud die erforderliche Mikrosegmentierung und sorgt für eine sichere VDI-Umgebung.

**Intent-basierte Richtlinie für hybride Arbeitslasten:** Der Cloud Service Manager (CSM) ist jetzt in NSX Manager integriert. Kunden können jetzt eine einzelne Intent-basierte Richtlinie vom Richtlinien-Manager definieren, ohne sich darum kümmern zu müssen, wo die Arbeitslasten bereitgestellt oder wohin sie in Zukunft verschoben werden. NSX Cloud realisiert diese Richtlinie durchgängig im lokalen Datencenter, in Azure und AWS.

## Kompatibilität und Systemvoraussetzungen

Informationen zur Kompatibilität und zu den Systemvoraussetzungen finden Sie im [Installationshandbuch für NSX-T Data Center](#).

## API und CLI-Ressourcen

Informationen zur Verwendung der NSX-T Data Center-APIs oder -CLIs für die Automation finden Sie unter [code.vmware.com](https://code.vmware.com).

Die API-Dokumentation ist über die Registerkarte **API-Referenz** verfügbar. Die CLI-Dokumentation ist über die Registerkarte **Dokumentation** verfügbar.

## Revisionsverlauf der Dokumente

28. Februar 2019. Erste Auflage.

2. April 2019. Zweite Auflage. Hinzugefügte bekannte Probleme: 2273651, 2279326, 2281095 und 2296888. Hinzugefügtes behobenes Problem: 2199785.

10. April 2019. Dritte Auflage. Hinzugefügte bekannte Probleme: 2203863, 2248186, 2252738, 2277543, 2276398, 2279326, 2281537, 2287124, 2290688, 2294178, 2295592, 2296430, 2297157, 2297918 und 2298499. Der Abschnitt „Neuigkeiten“ wurde um „Unterstützung für ein Design mit einem einzelnen Cluster“ ergänzt.

20. Juni 2019. Vierte Auflage. Bekanntes Problem 2261818 wurde hinzugefügt. Behobenes Problem 2182745 wurde hinzugefügt.

23. August 2019. Fünfte Auflage. Die bekannten Probleme 2362688, 2395334 und 2392093 wurden hinzugefügt.

## Behobene Probleme

- **Behobenes Problem 1842511: Multihop-BFD wird für statische Routen nicht unterstützt**  
In NSX-T 2.0 kann BFD (Bidirectional Forwarding Detection, bidirektionale Weiterleitungserkennung) für einen Multihop-BGP-Nachbarn (MH-BGP) aktiviert werden. Eine statische Multihop-Route kann in NSX-T 2.0 nicht mit BFD konfiguriert werden. Nur BGP ist konfigurierbar. Beachten Sie: Wenn Sie einen Multihop-BGP-Nachbarn mit BFD konfiguriert haben und eine entsprechende statische Multihop-Route mit demselben Nexthop als BGP-Nachbarn konfigurieren, hat der BFD-Sitzungsstatus Auswirkungen sowohl auf die BGP-Sitzung wie auf die statische Route.
- **Behobenes Problem 2279326: Beim Erstellen eines IPFIX L2-Collectors mit mehr als 4 IP:PORT-Kombinationen wird kein Fehler angezeigt**

Für die maximal zulässige Anzahl von IP:Port-Kombinationen wird keine Fehlermeldung angezeigt. Dies ist kein Problem, da die Benutzeroberfläche die Tag-Erstellung beschränkt, sobald die Obergrenze überschritten wird.

- **Behobenes Problem 1931707:** Für die automatische Transportknoten-Funktion müssen alle Hosts im Cluster über dieselbe pNIC-Einrichtung verfügen.  
Wenn die automatische TN-Funktion für ein Cluster aktiviert ist, wird eine Vorlage für einen Transportknoten erstellt, die für alle Hosts in diesem Cluster angewendet wird. Alle pNICs in der Vorlage müssen auf allen Hosts für die Transportknotenkonfiguration frei sein, da andernfalls die Transportknotenkonfiguration auf Hosts fehlschlagen kann, deren pNICs fehlen oder besetzt sind.
- **Behobenes Problem 1909703:** NSX-Administrator kann neue statische Routen, NAT-Regeln und Ports in einem Router erstellen, der direkt vom Back-End von OpenStack erstellt wurde  
Im Rahmen der RBAC-Funktion in NSX-T 2.0 können Ressourcen, wie z. B. Switches, Router oder Sicherheitsgruppen, die vom OpenStack-Plug-In erstellt wurden, nicht direkt vom NSX-Administrator über die NSX-Benutzeroberfläche/API gelöscht oder geändert werden. Diese Ressourcen können nur durch die APIs, die durch das OpenStack-Plug-In gesendet wurden, geändert/gelöscht werden. Es besteht eine Einschränkung in dieser Funktion. Der NSX-Administrator kann keine von OpenStack erstellten Ressourcen löschen/ändern. Der Admin ist jedoch berechtigt, neue Ressourcen wie statische Routen und NAT-Regeln innerhalb der von OpenStack erstellten vorhandenen Ressourcen zu erstellen.
- **Behobenes Problem 1989407:** vIDM-Benutzer mit der Rolle „Enterprise-Administrator“ können den Objektschutz nicht außer Kraft setzen  
Ein vIDM-Benutzer mit der Rolle „Enterprise-Administrator“ kann den Objektschutz nicht außer Kraft setzen und keine Prinzipalidentitäten erstellen oder löschen.
- **Behobenes Problem 2030784:** Die Anmeldung beim NSX Manager mit einem Remotebenutzernamen, der ASCII-fremde Zeichen enthält, ist nicht möglich  
Sie können sich nicht bei der NSX Manager-Appliance als Remotebenutzer mit einem Benutzernamen anmelden, der ASCII-fremde Zeichen enthält.
- **Behobenes Problem 2111047:** Anwendungserkennung wird auf VMware vSphere 6.7-Hosts in der Version NSX-T 2.2 nicht unterstützt.  
Die Ausführung von Anwendungserkennung in einer Sicherheitsgruppe mit VMs, die auf einem vSphere 6.7-Host ausgeführt werden, hat zur Folge, dass die Erkennungssitzung fehlschlägt.
- **Behobenes Problem 2157370:** Bei der Konfiguration von L3 Switched Port Analyzer (SPAN) mit Trunkierung verwirft ein spezifischer physischer Switch gespiegelte Pakete  
Bei der Konfiguration von L3 SPAN, einschließlich GRE/ERSPAN mit Trunkierung, werden trunkierte gespiegelte Pakete aufgrund der Richtlinie zu physischen Switches verworfen. Eine mögliche Ursache ist unter Umständen, dass der Port Pakete empfängt, bei denen die Anzahl der Bytes in der Nutzlast nicht gleich dem Typlängenfeld ist.
- **Behobenes Problem 2174583:** Im Assistenten „Erste Schritte“ funktioniert die Schaltfläche „Transportknoten einrichten“ im Microsoft Edge-Browser nicht ordnungsgemäß  
Nachdem Sie im Assistenten „Erste Schritte“ auf die Schaltfläche „Transportknoten einrichten“ geklickt haben, stürzt der Microsoft Edge-Webbrowser ab und ein JavaScript-Fehler wird ausgegeben.
- **Behobenes Problem 2114756:** In bestimmten Fällen werden VIBs nicht entfernt, wenn ein Host aus dem vorbereiteten NSX-T-Cluster entfernt wird  
Wenn ein Host aus dem vorbereiteten NSX-T-Cluster entfernt wird, verbleiben unter Umständen bestimmte VIBs auf dem Host.
- **Behobenes Problem 2059414:** Die RHEL LCP-Paket-Installation schlägt aufgrund einer älteren Version von python-gevent RPM fehl

Wenn ein RHEL-Host eine neuere Version von python-gevent RPM enthält, schlägt die RHEL LCP-Paket-Installation fehl, da der NSX-T Data Center RPM eine ältere Version von python-gevent RPM enthält.

- **Behobenes Problem 2142755: Die Installation der OVS-Kernel-Module schlägt fehl, je nachdem, welche Unterversion von RHEL 7.4 Kernel-Version ausgeführt wird.**  
OVS-Kernel-Module lassen sich möglicherweise nicht auf einem RHEL 7.4-Host mit einer Kernel-Unterversion 17.1 oder höher installieren. Der Installationsfehler führt dazu, dass die Datenpfade des Kernels nicht mehr länger funktionieren, wodurch die Appliance-Verwaltungskonsole nicht länger verfügbar ist.
- **Behobenes Problem 2125725: Nach der Wiederherstellung umfangreicher Topologiebereitstellungen sind die Suchdaten nicht mehr synchron und mehrere NSX Manager-Seiten reagieren nicht mehr.**  
Nach dem Wiederherstellen von NSX Manager mit umfangreichen Topologiebereitstellungen sind die Suchdaten nicht mehr synchron und auf mehreren NSX Manager-Seiten wird folgende Fehlermeldung angezeigt: Ein nicht behebbarer Fehler ist aufgetreten.
- **Behobenes Problem 2187888: Das über die NSX Manager-Benutzeroberfläche bereitgestellte NSX Edge verbleibt auf unbestimmte Zeit im Status „Registrierung ausstehend“**  
Das über die NSX Manager-Benutzeroberfläche bereitgestellte NSX Edge verbleibt auf unbestimmte Zeit im Status „Registrierung ausstehend“. Dieser Zustand führt dazu, dass NSX Edge zur weiteren Konfiguration nicht mehr verfügbar ist.
- **Behobenes Problem 2077145: Erzwungenes Löschen des Transportknotens hat in bestimmten Fällen verwaiste Transportknoten zur Folge**  
Beim Versuch, den Transportknoten mit einem API-Aufruf zwangsweise zu löschen, wenn beispielsweise ein Hardwarefehler vorliegt oder die Hosts nicht mehr abgerufen werden können, wird der Status des Transportknotens in „Verwaist“ geändert.
- **Behobenes Problem 2099530: Eine Änderung der VTEP-IP-Adresse des Bridge-Knotens führt zu Ausfällen beim Datenverkehr**  
Bei einer Änderung der VTEP-IP-Adresse des Bridge-Knotens wird die MAC-Tabelle vom VLAN zum Overlay auf den Remote-Hypervisoren nicht aktualisiert, was zu Datenverkehrsausfällen von bis zu 10 Minuten führt.
- **Behobenes Problem 2106176: Die automatische Installation des NSX Controllers stagniert während des Installationsschritts zum Warten auf die Registrierung**  
Während der automatischen Installation von NSX Controllern mithilfe der NSX Manager-API oder -Benutzeroberfläche stagniert der Fortschritt eines der ausgeführten NSX Controller und wird dauerhaft als „Warten auf Registrierung“ angezeigt.
- **Behobenes Problem 2125514: Nach dem Failover der Schicht-2-Bridge führt der logische Switch auf bestimmten NSX Edge-VMs so lange eine BUM-Replikation jedes einzelnen Pakets durch, bis die MAC-Adresse erneut bekannt ist.**  
Nach dem Failover der Schicht-2-Bridge führt der logische Switch auf bestimmten NSX Edge-VMs so lange (etwa 10 Minuten) eine BUM-Replikation jedes einzelnen Pakets durch, bis die MAC-Adresse für den Endpunkt erneut bekannt ist. Das System stellt sich selbst wieder her, nachdem die Endpunkte das nächste ARP erzeugt haben.
- **Behobenes Problem 2183549: Bei der Bearbeitung eines zentralen Dienstports kann ein neu erstellter logischer VLAN-Switch nicht angezeigt werden**  
Nachdem Sie auf der Manager-Benutzeroberfläche einen zentralen Dienstport und einen logischen VLAN-Switch erstellt haben, können Sie, wenn Sie den zentralen Dienstport bearbeiten, den neu erstellten logischen VLAN-Switch nicht mehr sehen.
- **Behobenes Problem 2186040: Wenn ein Transportknoten im System nicht unter den Top 250 Uplink-Profilen im System ist, wird das Uplink-Dropdown-Menü der physischen Netzwerkkarten auf der Benutzeroberfläche deaktiviert**

Wenn ein Transportknoten im System nicht unter den Top 250 Uplink-Profilen im System ist, wird das Uplink-Dropdown-Menü der physischen Netzwerkkarten auf der Benutzeroberfläche deaktiviert. Das Speichern des Transportknotens führt zum Entfernen des Uplink-Namens vom Transportknoten.

- **Behobenes Problem 2106635: Während der Erstellung statischer Routen führt das Ändern des Admin-Abstands der NULL-Routen dazu, dass die NULL-Einstellung für den nächsten Hop von der Benutzeroberfläche verschwindet**  
Wenn Sie den nächsten Hop beim Anlegen der statischen Routen auf NULL festlegen und dann den Admin-Abstand der NULL-Routen ändern, verschwindet die NULL-Einstellung des nächsten Hop von der Benutzeroberfläche.
- **Behobenes Problem 1928376: Controller-Cluster-Mitgliedsknoten hat fehlerhaften Status nach Wiederherstellung von NSX Manager**  
Der Controller-Cluster-Mitgliedsknoten kann möglicherweise instabil werden und einen herabgestuften Systemzustand melden, wenn NSX Manager mit einem Sicherungs-Image wiederhergestellt wird, das vor der Trennung dieses Mitgliedsknotens vom Cluster erstellt wurde.
- **Behobenes Problem 2128361: CLI-Befehl zum Setzen der Protokollebene des NSX Managers auf den Debug-Modus wird nicht ordnungsgemäß ausgeführt**  
Bei Verwendung des CLI-Befehls „set service manager logging-level debug“ zum Setzen der Protokollebene des NSX Managers auf den Debug-Modus werden keine Debugging-Protokollinformationen gesammelt.
- **Behobenes Problem 1940046: Wenn dieselbe statische Route in mehreren logischen Tier-1-Routern hinzugefügt und angekündigt wird, schlägt der Ost-West-Datenverkehr fehl**  
Wenn dieselbe statische Route in mehreren logischen Tier-1-Routern hinzugefügt und angekündigt wird, schlägt der Ost-West-Datenverkehr fehl.
- **Behobenes Problem 2160634: Durch das Ändern der IP-Adresse auf einem Loopback kann die IP-Adresse der Router-ID auf einem Uplink geändert werden.**  
Wenn die IP-Adresse auf dem Loopback geändert wird, wählt der NSX Edge die IP-Adresse auf dem Uplink als Router-ID. Die IP-Adresse des Uplinks, die als Router-ID zugewiesen ist, kann nicht geändert werden.
- **Behobenes Problem 2199785: Nginx-Kern-Problem, wenn die Integritätsüberwachung (ohne Portnummer) zum dynamischen Pool (mit Portnummer) hinzugefügt wird**  
Wenn Load Balancing mit einem Serverpool mit dynamischen Mitgliedern (mit Portnummer) konfiguriert ist und anschließend versucht wird, eine Integritätsüberwachung zuzuordnen, für die kein Überwachungsport konfiguriert ist, kann Nginx abstürzen.
- **Behobenes Problem 2182745: Zuvor wurden le/ge in Neuverteilungsregeln im Manager nicht validiert und funktionierten nicht ordnungsgemäß.**  
Neuverteilungsregeln unterstützen le/ge in Präfixlisten.

## Bekannte Probleme

Die bekannten Probleme gliedern sich in folgende Gruppen.

- [Allgemeine bekannte Probleme](#)
- [Bekannte Installationsprobleme](#)
- [Bekannte Probleme bei NSX Manager](#)
- [Bekannte Probleme bei NSX Edge](#)
- [Bekannte Probleme bei logischen Netzwerken](#)
- [Bekannte Probleme bei Sicherheitsdiensten](#)
- [Bekannte Probleme bei KVM-Netzwerken](#)
- [Bekannte Probleme beim Load Balancer](#)
- [Bekannte Probleme bei der Lösungsinteroperabilität](#)

- [Bekannte Probleme bei Betriebs- und Überwachungsdiensten](#)
- [Bekannte Upgradeprobleme](#)
- [Bekannte Probleme mit APIs](#)
- [Bekannte Probleme beim NSX Policy Manager](#)
- [Bekannte Probleme bei NSX Cloud](#)

## Allgemeine bekannte Probleme

- **Problem 2239365: „Nicht autorisiert“-Fehler wird ausgelöst**  
Möglicherweise kommt es zu diesem Fehler, weil der Benutzer versucht, mehrere Authentifizierungssitzungen im selben Browsertyp zu öffnen. Dies führt dazu, dass die Anmeldung mit dem oben angegebenen Fehler fehlschlägt und die Authentifizierung nicht möglich ist.  
Speicherort des Protokolls: `/var/log/proxy/reverse-proxy.log/var/log/syslog`  
  
Problemumgehung: Schließen Sie alle offenen Authentifizierungsfenster/-registerkarten und versuchen Sie die Authentifizierung erneut.
- **Problem 2287482: Eine Tabelle mit automatisch ermittelten Bindungen enthält möglicherweise Bindungen, die derzeit nicht ermittelt wurden**  
Bindungen, die in der Tabelle mit den automatisch ermittelten Bindungen als „doppelt“ gekennzeichnet sind, werden möglicherweise nicht mehr ermittelt.  
  
Problemumgehung: Keine.
- **Problem 2278142: Das globale Switch-IPFIX-Profil kann nicht bearbeitet werden**  
Wenn im System globale Profile verfügbar sind, können Sie sie nicht über die Schnittstelle ändern oder löschen, da es keinen Workflow für globale Profile gibt.  
  
Problemumgehung: Löschen Sie diese globalen Profile mithilfe der API.
- **Problem 2292222: Auf dem Bildschirm „Fehler beheben“ wird der Benutzer nicht benachrichtigt, wenn der Fingerabdruck falsch ist**  
Wenn der Hostvorbereitungsvorgang fehlschlägt, kann der Benutzer das Problem beheben, indem er auf „NSX-Installation fehlgeschlagen“ klickt. In diesem Fall muss er einen Benutzernamen, ein Kennwort und einen Fingerabdruck des Hosts angeben. Wenn der Benutzer einen falschen Fingerabdruck angibt, wird der Benutzer nicht von den Systemen benachrichtigt und das Problem bleibt ungelöst.  
  
Es gibt keine eindeutige Möglichkeit, in Erfahrung zu bringen, ob der Fingerabdruck falsch war. Überprüfen Sie das Protokoll, in dem diese `ThumbPrintValidationFailedException`-Ausnahme protokolliert ist.  
  
Problemumgehung: Geben Sie den korrekten Fingerabdruck an.
- **Problem 2252487: Der Transportknotenstatus wird für einen BM-Edge-Transportknoten nicht gespeichert, wenn mehrere Transportknoten gleichzeitig hinzugefügt werden**  
Der Transportknotenstatus wird auf der MP-Benutzeroberfläche nicht korrekt angezeigt.  
  
Problemumgehung:
  1. Starten Sie den Proton neu, dann werden alle Transportknotenstatus korrekt aktualisiert.
  2. Verwenden Sie alternativ die API „`https://<nsx-manager>/api/v1/transport-nodes/<node-id>/status?source=realtime`“, um den Transportknotenstatus abzufragen.
- **Problem 2285117: Kernel-Upgrade auf NSX-verwalteten VMs wird nicht unterstützt**  
Auf einigen Linux Ubuntu-Marketplace-Images führt der Kernel beim Neustart der VM automatisch für sich selbst ein Upgrade durch. Dies führt dazu, dass NSX-Agent nicht erwartungsgemäß funktioniert. Auch wenn es so aussehen kann, als ob der NSX-Agent funktionierte, sind einige nicht realisierte Netzwerkrichtlinien vorhanden, die sich auf den NSX-Agent auswirken. Der Agent versucht die Realisierung dieser Richtlinien immer wieder erneut, was zu einer hohen CPU-Auslastung führt.

Problemumgehung: Wenn ein Kernel-Upgrade erforderlich ist, müssen die geeigneten Linux-Header für diesen neuen Kernel zuerst heruntergeladen werden und das dkms-Paket des openvswitch-Datenpfads muss erneut kompiliert werden.

- **Problem 2285544: MD5-Hashes werden beim Aufrufen von NSX APIs, die die Angabe eines ssh\_fingerprint-Werts erfordern, nicht mehr unterstützt**  
NSX-T 2.4 unterstützt Nicht-FIPS-Verschlüsselungsalgorithmen, Hashes usw. nicht mehr, die das Aufrufen der NSX APIs für Sichern/Wiederherstellen, „file-store“ und Support-Pakete und die Angabe eines MD5-Hash für den ssh\_fingerprint-Wert beinhalten. Als Folge werden MD5-Hashes nicht mehr unterstützt.

Problemumgehung: Geben Sie einen anderen Hash an, der mit einem anderen Hashing-Algorithmus berechnet wird, beispielsweise SHA256.

- **Problem 2256709: Eine Instant Clone-VM oder eine aus einem Snapshot wiederhergestellte VM verliert während vMotion kurzzeitig den AV-Schutz**  
Der Snapshot einer VM wird wiederhergestellt, und die VM wird auf einen anderen Host migriert. Die Partnerkonsole zeigt keinen AV-Schutz für die migrierte Instant Clone-VM an. Es tritt ein kurzzeitiger Verlust des AV-Schutzes auf.

Problemumgehung: Keine.

- **Problem 2261431: Abhängig von den anderen Bereitstellungsparametern ist eine gefilterte Liste von Datenspeichern erforderlich**  
Entsprechender Fehler wird auf der Benutzeroberfläche angezeigt, wenn die falsche Option ausgewählt wurde. Der Kunde kann zur Behebung dieses Fehlers diese Bereitstellung löschen und eine neue erstellen.

Problemumgehung: Wählen Sie einen gemeinsam genutzten Datenspeicher aus, wenn Sie eine geclusterte Bereitstellung erstellen.

- **Problem 2266553: In der NSX-Appliance schlägt die Initialisierung eines Diensts möglicherweise beim ersten Starten fehl**  
Der bereitgestellte Knoten kann keine Anforderungen bedienen oder keinen Cluster bilden.

Problemumgehung: Versuchen Sie, den fehlgeschlagenen Dienst neu zu starten.

- **Problem 2267632: Verlust von GI-Schutzkonfiguration**  
Eine auf der Richtlinien-Benutzeroberfläche veröffentlichte Gastschutzregel zeigt ERFOLGREICH an. Die entsprechende Änderung im Verhalten wird auf der Gast-VM nicht widerspiegelt. Gleichzeitige OpsAgent-Protokolle zeigen Neustart an. Verlust des Gast-VM-Schutzes.

Problemumgehung: Wiederholen Sie die Konfigurationsänderung manuell.

- **Problem 2269901: Die vmk-Schnittstelle ist nicht in der Paketerfassung-CLI enthalten**  
Dieser Befehl kann nicht ausgegeben werden.

Problemumgehung: Verwenden Sie zum selben Zweck die Paketerfassungs-UW.

- **Problem 2274988: Dienstketten unterstützen aufeinander folgende Dienstprofile vom selben Dienst nicht**  
Der Datenverkehr durchläuft keine Dienstkette und wird immer dann verworfen, wenn die Kette zwei aufeinander folgende und zum selben Dienst gehörende Dienstprofile aufweist.

Problemumgehung: Fügen Sie ein Dienstprofil von einem anderen Dienst hinzu, um sicherzustellen, dass keine zwei aufeinander folgenden Dienstprofile zum selben Dienst gehören. Definieren Sie alternativ dazu ein drittes Dienstprofil, das dieselben Vorgänge der ursprünglichen zwei Dienstprofile verkettet durchführt. Verwenden Sie dann dieses dritte Profil allein in der Dienstkette.

- **Problem 2275285: Ein Knoten stellt eine zweite Anforderung, um demselben Cluster beizutreten, bevor die erste Anforderung abgeschlossen und der Cluster stabilisiert wurde**

Der Cluster funktioniert möglicherweise nicht ordnungsgemäß und die CLI-Befehle zum Abrufen des Clusterstatus und zum Abrufen der Clusterkonfiguration geben möglicherweise einen Fehler zurück.

Problemumgehung: Geben Sie nach der ersten Beitrittsanforderung für einen Zeitraum von 10 Minuten keinen weiteren Beitrittsbefehl für den Beitritt zum selben Cluster aus.

- **Problem 2275388:** Routen über eine Loopback-Schnittstelle/verbundene Schnittstelle werden möglicherweise neu verteilt, bevor Filter zum Verweigern der Routen hinzugefügt werden. Unnötige Updates von Routen können für einen Zeitraum zwischen wenigen Sekunden und einer Minute zur Umleitung von Datenverkehr führen.

Problemumgehung: Keine.

- **Problem 2275708:** Ein Zertifikat mit seinem privaten Schlüssel kann nicht importiert werden, wenn der private Schlüssel eine Passphrase aufweist. Die zurückgegebene Meldung lautet „Ungültige PEM-Daten für Zertifikat empfangen. (Fehlercode: 2002)“. Das Importieren eines neuen Zertifikats mit privatem Schlüssel ist nicht möglich.

Problemumgehung:

1. Erstellen Sie ein Zertifikat mit privatem Schlüssel. Geben Sie bei entsprechender Aufforderung keine neue Passphrase ein und drücken Sie stattdessen die Eingabetaste.
2. Wählen Sie „Zertifikat importieren“ und wählen Sie anschließend die Zertifikatsdatei und die Privatschlüsseldatei aus.

Überprüfen Sie den Vorgang, indem Sie die Schlüsseldatei öffnen. Wenn beim Generieren des Schlüssels eine Passphrase eingegeben wurde, steht in der zweiten Zeile der Datei etwas wie „Proc-Type: 4,ENCRYPTED“.

Diese Zeile fehlt, wenn die Schlüsseldatei ohne Passphrase generiert wurde.

- **Problem 2275985:** Nicht mit einem logischen Switch verbundene VNICs werden als Optionen für direkte NSGroup-Mitglieder aufgeführt. Eine nicht mit einem logischen Switch verbundene VNIC wird als direktes Mitglied der NSGroup hinzugefügt. Der Vorgang ist erfolgreich, aber die für diese Gruppe angewendeten Richtlinien werden auf der VNIC nicht durchgesetzt.

Problemumgehung: Keine.

Prüfen Sie, ob eine VNIC mit einem logischen Switch verbunden ist, bevor Sie sie als direktes Mitglied einer NSGroup hinzufügen.

- **Problem 2277742:** Der Aufruf von „PUT https://<MGR\_IP>/api/v1/configs/management“ mit einem Anforderungstext, in dem „publish\_fqdns“ auf „true“ festgelegt ist, kann fehlschlagen, wenn die NSX-T Manager-Appliance mit einem vollqualifizierten Domännennamen (FQDN) anstatt nur mit einem Hostnamen konfiguriert ist. „PUT https://<MGR\_IP>/api/v1/configs/management“ kann nicht aufgerufen werden, wenn ein FQDN konfiguriert ist.

Problemumgehung: Stellen Sie den NSX Manager mit einem Hostnamen anstatt mit einem FQDN bereit.

- **Problem 2279249:** Eine Instant Clone-VM verliert während vMotion kurzzeitig den AV-Schutz. Von einem Host zu einem anderen migrierte Instant Clone-VM. Unmittelbar nach der Migration bleibt eine eicar-Datei auf der VM zurück. Kurzzeitiger Verlust des AV-Schutzes.

Problemumgehung: Keine.

- **Problem 2290669:** Mit zunehmender Anzahl an virtuellen Servern steigt die Konfigurationszeit für jeden dieser Server an.



Aufgrund einer großen Anzahl an Validierungen steigt mit zunehmender Anzahl an virtuellen Servern die Konfigurationszeit für jeden dieser Server an. Bei den ersten 100 virtuellen Servern beträgt die durchschnittliche Reaktionszeit ca. 1 Sekunde. Nach 250 virtuellen Servern steigt die durchschnittliche Reaktionszeit auf 5–10 Sekunden an. Nach 450 virtuellen Servern steigt die durchschnittliche Reaktionszeit auf ca. 30 Sekunden an.

Problemumgehung: Keine. Sie können virtuelle Server abhängig von der Topologie möglicherweise als Mehrfach-LbServices konfigurieren. Andernfalls sind beim Konfigurieren großer Setups mit virtuellen Servern längere Antwortzeiten zu erwarten.

- **Problem 2292116: IPFIX L2-Funktion „Angewendet auf“ mit CIDR-basierter Gruppe von IP-Adressen, die nicht auf der Benutzeroberfläche aufgeführt werden, wenn die Gruppe über die Seite „IPFIX L2“ erstellt wird**

Wenn Sie versuchen, über das Dialogfeld „Angewendet auf“ eine Gruppe von IP-Adressen zu erstellen, und im Dialogfeld „Mitglieder festlegen“ eine falsche IP-Adresse oder CIDR eingeben, werden diese Mitglieder nicht unter den Gruppen aufgeführt. Sie müssen diese Gruppe erneut bearbeiten, um gültige IP-Adressen einzugeben.

Problemumgehung: Wechseln Sie zur Seite mit der Auflistung der Gruppen und fügen Sie IP-Adressen in der betreffenden Gruppe hinzu. Danach kann das Auffüllen der Gruppe im Dialogfeld „Angewendet auf“ beginnen.

- **Problem 2294821: NSX-Appliance-Informationen werden im Cluster-Überwachungs-Dashboard mit dem Fehler „Fehler beim Löschen des Knotens“ und ohne Hinweise an den Benutzer zur Handhabung der Situation angezeigt**

Dieses Problem wurde beobachtet, nachdem der Benutzer versuchte, den automatisch bereitgestellten Knoten über die Schnittstelle zu löschen, und das Ausschalten des Knotens fehlschlug. Wenn der Cluster einen Knoten verliert, müssen Sie manuell einen neuen Knoten hinzufügen und die Konfigurationszustände mithilfe der Problemumgehung unten bereinigen.

Problemumgehung: Sobald die Löschung der Appliance über API/Benutzeroberfläche fehlgeschlagen ist, löschen Sie die Appliance wie folgt mithilfe der force-delete-API manuell:  
`POST api/v1/cluster/nodes/deployments/467a102d-472f-4f43-a93c-08b992b9f471?action=delete&force_delete=true`  
Löschen Sie anschließend die VM aus dem vCenter.

- **Problem 2281095: Wenn der Host, auf dem die SVM bereitgestellt ist, dem selben Cluster erneut hinzugefügt wird, wird kein Callback von EAM ausgelöst**  
Alle Gast-VMs sind möglicherweise ungeschützt. Die NSX-Benutzeroberfläche bleibt im Status „In Bearbeitung“ hängen.

Problemumgehung: Entfernen Sie die SVM vom Host und fügen Sie sie dann dem Cluster hinzu.

- **Problem 1957072: Das Uplink-Profil für den Bridge-Knoten muss für mehrere Uplinks immer eine LAG verwenden**  
Wenn Sie mehrere Uplinks verwenden, die keine Linkzusammenfassungsvergruppe (Link Aggregation Group, LAG) bilden, findet für den Datenverkehr kein Lastausgleich statt, sodass der Datenverkehr möglicherweise nicht richtig funktioniert.

Problemumgehung: Verwenden Sie für mehrere Uplinks auf Bridge-Knoten eine LAG.

- **Problem 1970750: N-VDS-Profil des Transportknotens, das LACP mit schnellen Timern verwendet, wird nicht auf vSphere ESXi-Hosts angewendet**

Wenn ein LACP-Uplink-Profil mit schnellen Raten auf einen vSphere ESXi-Transportknoten auf NSX Manager angewendet wird, zeigt der NSX Manager an, dass das Profil erfolgreich angewendet wird, aber der vSphere ESXi-Host verwendet den standardmäßigen langsamen LACP-Timer. Auf dem vSphere Hypervisor können Sie den Effekt des lacp-timeout-Werts (SLOW/FAST) nicht sehen, wenn das Profil des verwalteten LACP-NSX-Distributed Switch (N-VDS) über den NSX Manager auf dem Transportknoten verwendet wird.

Problemumgehung: Keine.

- **Problem 2261818: Von eBGP-Nachbarn erlernte Routen werden an denselben Nachbarn zurückgegeben.**

Durch das Aktivieren von BGP-Debug-Protokollen werden Pakete angezeigt, die erneut empfangen werden, und das Paket wird mit einer Fehlermeldung verworfen. Der BGP-Prozess nutzt zusätzliche CPU-Ressourcen, um die an Peers gesendeten Updatemeldungen zu verwerfen. Wenn viele Routen und Peers vorhanden sind, kann dies Auswirkungen auf die Routenkonvergenz haben.

Problemumgehung: Keine.

## Bekannte Installationsprobleme

- **Problem 2238093: Fehlerbehebung (Resolver) wird nicht unterstützt, wenn das Entfernen der NSX-Pakete erzwungen wird**

Zum Deinstallieren von NSX vom Host wird das Entfernen der NSX-Pakete erzwungen. Dies kann zu einem zu beschädigten NSX-Paket führen. Die Fehlerbehebung (Resolver) für die NSX-Paketinstallation ist möglicherweise nicht erfolgreich, wenn vor der Fehlerbehebung das Entfernen der NSX-Pakete erzwungen wird. Speicherort des Protokolls: `/var/log/proton/nsxapi.log`

Problemumgehung: Keine.

Erzwingen Sie das Entfernen der NSX-Pakete nicht. Deinstallieren Sie die NSX-Komponenten entsprechend der in der NSX-Dokumentation beschriebenen Standardschritte.

- **Problem 2288872: Installationsstatus wird als „Knoten nicht bereit“ angezeigt**  
Der Edge-Knoten wird nicht integriert. Der Konfigurationszustand des Transportknotens lautet „Ausstehend“, und der Knoten kann daher nicht einem Edge-Cluster hinzugefügt werden.  
Speicherort des Protokolls: `/var/log/proton/nsxapi.log`

Problemumgehung: Versuchen Sie die Registrierung des Edge-Knotens erneut. Alternativ dazu können Sie den Edge-Knoten ausschalten. Wenn er gestartet wird, stellt er den MP-MPA-Kanal her.

- **Problem 2252776: Ein Transportknotenprofil kann auf einem der Mitgliederhosts des Clusters nicht angewendet werden, obwohl der zuvor aufgetretene Validierungsfehler jetzt behoben ist**  
Das Transportknotenprofil wird auf dem Cluster angewendet. Aber es kann auf einem der Mitgliederhosts des Clusters nicht angewendet werden, weil eine der Validierungen nicht bestanden wurde (z. B. sind VMs auf dem Host eingeschaltet). Der Benutzer behebt dieses Problem, aber die Validierung wird weiterhin auf der Benutzeroberfläche angezeigt, und das Transportknotenprofil wird nicht automatisch auf diesem Host angewendet.

Problemumgehung: Verschieben Sie den Host aus dem Cluster heraus und fügen Sie ihn dem Cluster erneut hinzu. Dies führt dazu, dass die Aktivität zum Anwenden des Transportknotenprofils auf dem Host ausgelöst wird.

- **Problem 2284683: Eine automatisch bereitgestellte Appliance kann nicht gelöscht werden, wenn ein registrierter Compute Manager gelöscht und erneut hinzugefügt wird**  
Die Löschung der Appliance ist mit dem Fehler „Fehler beim Ausschalten“ fehlgeschlagen, und es wird gemeldet, dass der Compute Manager nicht gefunden wurde.

Problemumgehung: Sobald die Löschung der Appliance über API/Benutzeroberfläche fehlgeschlagen ist, löschen Sie die Appliance wie folgt mithilfe der force-delete-API manuell: `POST api/v1/cluster/nodes/deployments/<node-id>?action=delete&force_delete=true`. Löschen Sie die VM aus dem VC.

- **Problem 1957059: Das Aufheben der Hostvorbereitung schlägt fehl, wenn dabei dem Cluster ein Host mit vorhandenen VIBs hinzugefügt wird**  
Wenn die VIBs vor dem Hinzufügen der Hosts zum Cluster nicht vollständig entfernt wurden, kann die Hostvorbereitung nicht aufgehoben werden.

Problemumgehung: Stellen Sie sicher, dass die VIBs auf den Hosts vollständig entfernt werden und starten Sie den Host neu.

- **Problem 2296888: Für die Konfiguration von Transportknoten (TN)/Transportknotenprofil (TNP) können nicht sowohl das Flag für die Migration nur von PNIC auf „true“ gesetzt als auch VMK-Zuordnungen für die Installation für alle Host-Switches festgelegt werden**  
Wenn mit einer falschen Konfiguration (sowohl PNIC-Migrations-Flag auf „true“ festgelegt als auch VMK-Zuordnungen für die Installation, die für alle Host-Switches angegeben wurden) CREATE ausgeführt wird, kommt es zur folgenden Ausnahme:

VMK-Migration für Host b17afc36-bbdc-491a-b944-21f73cf91585 ist mit Fehler  
[com.vmware.nsx.management.switching.common.exceptions.SwitchingException: TransportNode [TransportNode/b17afc36-bbdc-491a-b944-21f73cf91585] kann während der Migration der ESX-vmk-Schnittstelle null auf [null] nicht aktualisiert oder gelöscht werden.] fehlgeschlagen.  
(Fehlercode: 9418)

Wenn mit einer falschen Konfiguration ein UPDATE-Befehl ausgeführt wird, kommt es zur folgenden Ausnahme:

Allgemeiner Fehler (Fehlercode: 400)

Eine Ausnahme tritt auf, wenn die TN/TNP-Konfiguration angewendet wird, in der sowohl das Flag für die Migration nur von PNIC auf „true“ als auch die VMK-Migrationszuordnung festgelegt ist.

Problemumgehung: In jeder an den Host gesendeten Konfiguration darf entweder das Flag für die Migration nur von PNIC auf „true“ festgelegt oder die VMK-Zuordnungen für die Installation aufgefüllt sein, aber nicht beides.

1. Senden Sie die TN-Konfiguration mit den Host-Switches, für die die Migration nur von PNIC auf „true“ festgelegt sein muss.
  2. Aktualisieren Sie die TN-Konfiguration, indem Sie alle Flags für die Migration nur von PNIC auf „false“ setzen, und füllen Sie die VMK-Zuordnungen für die Installation nach Bedarf auf. Anders ausgedrückt: Stellen Sie sicher, dass für die an den TN gesendete Konfiguration entweder das Flag für die Migration nur von PNIC auf „true“ festgelegt ist oder die VMK-Zuordnungen für die Installation auf allen Host-Switches aufgefüllt sind. Für Konfigurationen, die beide erfordern, müssen zwei getrennte Konfigurationsaufrufe durchgeführt werden.
- **Problem 2273651 – nach dem Löschen des Transportknotens kann der Benutzer kein SSH in den Host ausführen.**  
In KVM-Implementierungen beobachtet. Der Benutzer löscht einen Transportknoten und erhält eine Meldung, dass der Löschvorgang erfolgreich war. Danach kann der Benutzer jedoch nicht mehr über SSH auf denselben Host zugreifen. Das Problem wird wahrscheinlich durch das Vorhandensein eines Open Virtual Switchs (OVS) verursacht, der nicht von NSX-T verwaltet wird und wahrscheinlich als Teil der KVM-Vorlage vorab installiert wurde.

Problemumgehung: Identifizieren Sie den problematischen OVS, bevor Sie den Transportknoten löschen.

1. Führen Sie `ovs-vsctl show` aus, um den OVS zu identifizieren.
2. Migrieren Sie alle Workload-VM-Schnittstellen vom OVS zur Linux-Bridge.
3. Löschen Sie den Transportknoten wie folgt:

`DELETE api/v1/transport-nodes/<uuid>`

- **Problem 2281537 – Nach der Migration kann der ESXi-Transportknoten mit Multi-VTEP die BFD-Sitzung nicht starten.**  
Nach der Migration eines NSX-V-Knotens zu NSX-T kann der ESXi-Transportknoten mit Multi-VTEP auf allen VTEPs zu Edge-Knoten keine BFD-Sitzung starten.

Problemumgehung: Starten Sie den netcpa-Dienst neu.

#### Bekannte Probleme bei NSX Manager

- **Problem 2285306: Der Dienstbereitstellungsstatus für Guest Introspection-Dienste bleibt „Unbekannt“, bis die Dienst-VM eingeschaltet wird**  
Nach dem Erstellen einer Dienstbereitstellung und ihrer Auflistung in der Tabelle „Dienstbereitstellung“ wird der Status möglicherweise nicht sofort als „In Bearbeitung“ angezeigt und bleibt „Unbekannt“, bis die Tabelle aktualisiert wird.

Problemumgehung: Keine. Aktualisieren Sie die Seite nach zehn Sekunden. Der Status sollte aktualisiert werden.

- **Problem 2292526: Beim Hinzufügen eines Hosts wird die Meldung „Host nicht erreichbar“ angezeigt**  
Beim Hinzufügen eines ESXi-Hosts wird die Meldung „Host nicht erreichbar“ angezeigt, es wird jedoch kein Grund angezeigt. Der wahrscheinliche Grund dafür liegt in falschen Anmeldedaten.

Problemumgehung: Überprüfen Sie die Hostkonfiguration, geben Sie die Anmeldedaten erneut ein und versuchen Sie das Hinzufügen des Hosts erneut.

- **Problem 2292701: Der Benutzer kann die Sequenznummer in einer Bindungszuordnung nicht aktualisieren**  
Der Benutzer kann die Reihenfolge oder Rangfolge von Profilen, die auf eine Einheit angewendet werden, nicht durch Aktualisieren der Sequenznummer ändern.

Problemumgehung: Löschen Sie die Bindungszuordnung und erstellen Sie sie mit der gewünschten neuen Sequenznummer.

- **Problem 2294345: Das Ausführen einer Anwendungserkennungs-Klassifizierung für eine Gruppe mit sowohl ESXi- als auch KVM-gehosteten VMs kann fehlschlagen**  
Die Funktion der Anwendungserkennung wird nur auf ESXi-Hypervisoren unterstützt. Für Gruppen von VMs, die sich auf verschiedenen Hosts befinden, die nicht unterstützte Hosts umfassen, wird für die Ergebnisse der Anwendungserkennungs-Klassifizierung keine Garantie übernommen.

Problemumgehung: Keine.

#### Bekannte Probleme bei NSX Edge

- **Problem 2248345: Nach der Installation des NSX-T Edge wird die Maschine mit einem leeren schwarzen Bildschirm gestartet.**  
NSX-T Edge kann nicht auf einer Maschine des Typs HPE ProLiant DL380 Gen9 installiert werden.

Problemumgehung: Verwenden Sie eine andere Maschine oder stellen Sie NSX-T Edge als VM auf einem Hypervisor bereit.

- **Problem 2283559: Die MP-APIs „/routing-table“ und „/forwarding-table“ geben einen Fehler zurück, wenn der Edge mehr als 65.000 Routen für RIB und mehr als 100.000 Routen für FIB aufweist**  
Wenn der Edge mehr als 65.000 Routen für RIB und mehr als 100.000 Routen für FIB aufweist, nimmt die Anforderung von MP an den Edge mehr als 10 Sekunden in Anspruch, und dies führt zu einer Zeitüberschreitung. Dies ist eine schreibgeschützte API und wirkt sich nur dann aus, wenn die mehr als 65.000 Routen für RIB und mehr als 100.000 Routen für FIB mithilfe der API/UI heruntergeladen werden müssen.

Problemumgehung: Es gibt zwei Optionen zum Abrufen von RIB/FIB.

- Diese APIs unterstützen Filteroptionen, die auf Netzwerkpräfixen oder Routentypen beruhen. Verwenden Sie diese Optionen zum Herunterladen der gewünschten Routen.
- Wenn die gesamte RIB-/FIB-Tabelle erforderlich ist, ist eine CLI-Unterstützung erforderlich, und in diesem Fall tritt keine Zeitüberschreitung auf.

## Bekannte Probleme bei logischen Netzwerken

- **Problem 2243415: Der Kunde kann den NXGI-Dienst mithilfe des logischen Switches (als Verwaltungsnetzwerk) nicht bereitstellen**

Auf dem NXGI-Bereitstellungsbildschirm kann der Benutzer im Steuerelement für die Netzwerkauswahl keinen logischen Switch sehen. Wenn die API direkt mit dem als Verwaltungsnetzwerk erwähnten logischen Switch verwendet wird, wird dem Benutzer der folgende Fehler angezeigt: „Dienstbereitstellung kann nicht auf angegebenes Netzwerk zugreifen.“

Problemumgehung: Führen Sie die Bereitstellung mit einem anderen Switch-Typ wie etwa einem lokalen oder verteilten Switch durch.

- **Problem 2264386: Die Löschung des Transportknotens findet statt, obwohl der Transportknoten Teil einer NS-Gruppe ist**

Die Löschung des Transportknotens ist zulässig, selbst wenn der Knoten Teil einer NS-Gruppe ist. Die Löschung sollte vermieden werden. Wenn dieses Problem auftritt, müssen Sie die NS-Gruppen neu erstellen und die Beziehungen mit ihren Transportknoten erneut herstellen.

Problemumgehung: Überprüfen Sie zur Vermeidung dieses Problems manuell, ob ein Transportknoten NS-Gruppen zugeordnet ist. Navigieren Sie in der Schnittstelle der Management Plane zu Netzwerk und Sicherheit – Erweitert > Bestand > Gruppen oder zu System > Knoten > Transportknoten > Zugehörig > NSGroup.

- **Problem 2292997: Bestimmte logische Routerschnittstellen können möglicherweise für Linux-Netzwerk-Stack nicht erstellt werden**

Bestimmte logische Routerschnittstellen können für Linux-Netzwerk-Stack möglicherweise nicht erstellt werden und geben den folgenden Fehler zurück: `errorCode="EDG0100002", Operation failed creating sub-interface: max sub-interface exceeded`. Dies kann dazu führen, dass von einem Tier0-Dienstrouter (TO SR) weitergeleiteter Datenverkehr aufgrund fehlender Routen verworfen wird.

Problemumgehung: Starten Sie den betroffenen Edge-Knoten neu.

- **Problem 228688: Der BGP-Nachbar muss beim Löschen einer IPsec-Routen-Basis Sitzung zuerst gelöscht werden, wenn BGP über VTI konfiguriert ist**

Wenn BGP über VTI konfiguriert ist und Sie die IPsec-Sitzung löschen, sind beide SR inaktiv, und dies blockiert wiederum den Datenverkehr. Um den Datenverkehr wiederaufzunehmen, muss der für VTI konfigurierte BGP-Nachbar gelöscht werden. In diesem Szenario ist nur BGP über VTI konfiguriert.

Problemumgehung: Löschen Sie den BGP-Nachbarn, bevor Sie die IPsec-Sitzung löschen.

- **Problem 2288509: Eigenschaft MTU wird für Tier0-/Tier1-Dienstschnittstelle (zentraler Dienstport) nicht unterstützt**

Die Eigenschaft MTU wird für die Tier0-/Tier1-Dienstschnittstelle (zentraler Dienstport) nicht unterstützt.

Problemumgehung: Konfigurieren Sie MTU mithilfe der Management Plane-API, selbst wenn der CSP-Port vom Richtlinien-Workflow erstellt wird.

- **Problem 2288774: Segment-Port gibt einen Realisierungsfehler aus, weil die Anzahl der Tags (fälschlicherweise) 30 überschreitet**

Bei der Benutzereingabe wird fälschlicherweise versucht, mehr als 30 Tags anzuwenden. Der Richtlinien-Workflow validiert/verweigert jedoch die Benutzereingabe nicht ordnungsgemäß und lässt die Konfiguration zu. Die Richtlinie zeigt dann einen Alarm mit der korrekten Fehlermeldung an, dass der Benutzer nicht mehr als 30 Tags verwenden darf. An diesem Punkt kann der Benutzer das Problem beheben.

Problemumgehung: Korrigieren Sie die Konfiguration, nachdem der Fehler angezeigt wurde.

- **Problem 2275412: Die Portverbindung funktioniert nicht über mehrere Transportzonen hinweg**  
Die Portverbindung kann nicht nur in einer einzelnen Transportzone verwendet werden.

Problemumgehung: Keine.

- **Problem 2290083: Beim Erstellen eines VLAN-basierten Segments fehlt die Validierung**  
Wenn Sie eine VLAN-Transportzone mit einer VLAN-ID-Eigenschaft angeben, kann der Fehler vom System nicht validiert und identifiziert werden. Dies führt dazu, dass der Intent während der Realisierung fehlschlägt und einen Fehler auslöst.

Problemumgehung: Anweisungen zum Korrigieren der Eingabe finden Sie in den Fehlerdetails des Realisierungsalarms.

- **Problem 2292096: Der CLI-Befehl „get service router config route-maps“ gibt eine leere Ausgabe zurück**  
Der CLI-Befehl „get service router config route-maps“ gibt selbst dann eine leere Ausgabe zurück, wenn „route-maps“ konfiguriert ist. Dieses Problem betrifft nur die Anzeige.

Problemumgehung: Verwenden Sie den CLI-Befehl `get service router config`, der eine route-map-Konfiguration als Teil der gesamten Ausgabe zurückgibt.

- **Problem 2994002: Bei der DNS-Weiterleitungserstellung wird Tier1 in der Dropdown-Liste der Tier0-/Tier1-Gateways nicht zur Auswahl angeboten**  
In einer großen Bereitstellung mit Tausenden von Datensätzen wird im Workflow zur DNS-Weiterleitungserstellung Tier1 in der Dropdown-Liste der Tier0-/Tier1-Gateways nicht zur Auswahl angeboten. Sie müssen deshalb zum Konfigurieren der DNS-Weiterleitungserstellung die API verwenden.

Problemumgehung: Führen Sie die Konfiguration mithilfe der API durch.

- **Problem 2298499 – VPN zwischen Public Cloud-Gateway und Peer-Host schlägt fehl, wenn das Gateway nicht mit öffentlicher IP bereitgestellt wurde.**  
Der VPN-Tunnel zwischen dem Public Cloud-Gateway (PCG) und dem Peer-Host kann nicht hergestellt werden, wenn das PCG ohne öffentliche IP-Adresse auf dem Uplink bereitgestellt wurde. Dies passiert, weil das PCG für den VPN-Datenverkehr standardmäßig SNAT ausführt.

Problemumgehung: Aktivieren Sie bei der Bereitstellung des Public Cloud-Gateways die öffentliche IP-Adresse für die Uplink-Schnittstelle.

- **Problem 2392093: Datenverkehr sinkt aufgrund der RPF-Prüfung**  
Die RPF-Prüfung kann zu einem verworfenen Datenverkehr führen, wenn der Datenverkehr über einen TO-Downlink angeheftet wird und sich die Tier0- und Tier1-Router auf demselben Edge-Knoten befinden.

Problemumgehung: Keine.

## Bekannte Probleme bei Sicherheitsdiensten

- **Problem 2288523: Das Entladen des NSX Guest Introspection-Treibers kann zu Sicherheitsproblemen führen**  
IDFW stützt sich auf Benutzeridentitätsinformationen aus dem NSX Guest Introspection-Treiber. Das Entladen des Treibers kann für Benutzer, die über den bestimmten Gast angemeldet sind, zu Sicherheitsproblemen führen. Dabei treten die folgenden Symptome auf:

- Nicht erzwungene Firewallregeln für Benutzer, die über bestimmte Gast-VMs angemeldet sind, auf denen der Guest Introspection-Treiber entladen ist.
- In der IDFW-Komponente Details nicht angemeldeter Benutzer für Benutzer, die sich über bestimmte Gast-VMs anmelden, auf denen der Guest Introspection-Treiber entladen ist.
- MUX-Protokolle zeigen keine Verbindungen von diesen Gast-VMs an, obwohl IDFW auf dem Host aktiviert ist.
- MUX-Protokolle zeigen keine Netzwerkereignisse von diesen Gast-VMs an, obwohl IDFW auf dem Host aktiviert ist.

Dies führt dazu, dass die Regel „Standardeinstellung – Alle ablehnen“ den Zugriff für Benutzer blockieren kann, die über Gast-VMs angemeldet sind, auf denen der Guest Introspection-Treiber entladen ist.

Problemumgehung: Keine. Der IT-Administrator muss die Best Practices für die Sicherheit befolgen, um sicherzustellen, dass keinem Benutzer Rechte zum Entladen von Guest Introspection-Treibern innerhalb von Gast-VMs gewährt werden.

- **Problem 2288773: Die noch verfügbare alte TLS-Protokoll-API wird überschrieben**  
NSX-T verfügt über eine neue API zum Einstellen der NSX-TLS-Protokollversionen und -Verschlüsselungs-Suites, was zu einem Update aller Knoten in einem NSX-T-Cluster führt. Die alte API ist jedoch immer noch verfügbar. Diese kann verwendet werden, aber die neuen Einstellungen werden von den globalen Einstellungen überschrieben.

Problemumgehung: Verwenden Sie die neue API.

- **Problem 2291872: Eine Protokollmeldung zeigt eine Warnmeldung an, wenn der TFTP-Dienst in einer Firewallregel verwendet wird**

Eine Protokollmeldung zeigt eine irrelevante Warnmeldung an, wenn der TFTP-Dienst in einer Firewallregel verwendet wird. Protokollspeicherort auf dem ESXi-Knoten:

`/var/log/cfgAgent.log.`

Problemumgehung: Erstellen Sie einen neuen Dienst für TFTP als L4PortSet-Dienst und verwenden Sie diesen in der Firewallregel.

- **Problem 2203863 – Identitäts-Firewallregeln werden für UDP-und ICMP-Datenverkehr nicht unterstützt.**

Identitäts-Firewallregeln funktionieren nicht mit Ping-Tests. Die aktuelle Funktionalität wird nur für TCP-Datenverkehr unterstützt.

Problemumgehung: Nutzen Sie TCP, um Identitäts-Firewallregeln zu testen. Bei der Konfiguration von Identitäts-Firewallregeln in der Spalte „Service“ niemals ANY/UDP/ICMP festlegen

- **Problem 2296430 – Die NSX-T Manager-API stellt bei der Zertifikatgenerierung keine alternativen Antragstellernamen (SANs) bereit.**

Die NSX-T Manager-API stellt keine alternativen Antragstellernamen für das Ausstellen von Zertifikaten bereit, insbesondere während der CSR-Generierung.

Problemumgehung: Erstellen Sie den CSR mit einem externen Tool, das die Erweiterungen unterstützt. Nachdem das signierte Zertifikat von der Zertifizierungsstelle empfangen wurde, importieren Sie es mit dem Schlüssel vom CSR in NSX-T Manager.

- **Problem 2252738 – Regeln für vollqualifizierte Domännennamen (FQDN) erlauben, dass ein Paket, das nicht mit der Regel übereinstimmt, das Ziel erreicht.**

Wenn eine bestimmte FQDN-Regel erstellt wird, wird der mit einer IP-Adresse verknüpfte Domänenname zur entsprechenden Regel der Firewall-Datenbank hinzugefügt. Pakete, die an diesen Domännennamen gesendet werden, dürfen den Server erreichen. Wenn jedoch ein Benutzer den Domännennamen ändert, der mit dieser IP-Adresse auf dem Domännennamenserver verknüpft ist, wird der Eintrag für den Domännennamen in der Firewall-Datenbank nicht aktualisiert (es sei denn, es sind andere FQDN-Regeln vorhanden, die mit dem neuen Domännennamen übereinstimmen). Infolgedessen werden Pakete auch dann an den neuen Domännennamen gesendet, wenn sie durch die FQDN-Regel verworfen werden müssten.

Problemumgehung: Keine.

- **Problem 2395334 – (Windows)-Pakete wurden fälschlicherweise aufgrund eines Contrack-Eintrags für Stateless Firewall-Regeln verworfen.**  
Stateless Firewall-Regeln werden auf Windows-VMs nicht gut unterstützt.

Problemumgehung: Fügen Sie stattdessen eine statusbehaftete Firewallregel hinzu.

- **Problem 2458384 – Seiten der NSX-T Manager-Schnittstelle können nicht geladen werden (Fehler 403).**  
Trat in den Herausgabeverionen 2.4.0 und 2.4.1 auf. Dieses Problem betrifft sowohl Admin- als auch Identity Manager-Anmeldungen. Der FQDN des NSX-T Manager verwendet das Format „\*.SLD.TLD“. Beispiel: \*.co.uk, \*.co.il, \*.com.au.

Problemumgehung: Greifen Sie auf die NSX-T Manager-Benutzeroberfläche zu, indem Sie anstelle des FQDN einen Kurznamen oder eine IP verwenden. Weitere Informationen hierzu finden Sie unter <https://kb.vmware.com/s/article/71217>.

#### Bekannte Probleme bei KVM-Netzwerken

- **Problem 2292995: Der Realisierungsstatus ist auf „Fehler“ festgelegt, obwohl alle konfigurierten Regeln in OVS programmiert sind**  
Die API vermittelt fälschlicherweise einen negativen Eindruck, selbst wenn die DFW-Regeln in der Data Plane programmiert sind.

Problemumgehung: Ein Update einer beliebigen DFW-Regel behebt diese Fehlerbedingung. Indem Sie beispielsweise einfach die Regelprotokollierung umschalten, erzwingen Sie, dass das KVM-DFW-Modul diese Fehlerbedingung behebt.

#### Bekannte Probleme beim Load Balancer

- **Problem 2290899: IPSec-VPN funktioniert nicht, und die Realisierung der Control Plane für IPSec schlägt fehl**  
IPSec-VPN (oder L2VPN) wird nicht aktiviert, wenn zusammen mit dem IPSec-Dienst auf Tier-0 mehr als 62 LbServers auf demselben Edge-Knoten aktiviert sind.

Problemumgehung: Verringern Sie die Anzahl an LbServers auf weniger als 62.

- **Problem 2297157 – Die HTTPS-Leistung des Load Balancing wird vom FIPS-Modus beeinflusst.**  
Die Leistung des Load Balancing kann beeinträchtigt werden, wenn der standardmäßige FIPS-Modus aktiviert ist.

Problemumgehung: Eine Problemumgehung finden Sie im Knowledgebase-Artikel 67400 [NSX-T 2.4.0 Load Balance Service may observe low performance on HTTPs](#).

- **Problem 2362688: Wenn einige Pool-Mitglieder in einem Load Balancer inaktiv sind, zeigt die Benutzeroberfläche den konsolidierten Status als aktiv an.**  
Wenn ein Pool-Mitglied ausgefallen ist, gibt es keine Hinweise auf der Benutzeroberfläche der Richtlinie, bei der der Pool-Status grün und aktiv ist.

Problemumgehung: Keine.



## Bekannte Probleme bei der Lösungsinteroperabilität

- **Problem 2289150: PCM-Aufrufe an AWS beginnen fehlschlagen**  
Wenn Sie die PCG-Rolle für ein AWS-Konto in CSM von *old-pcg-role* in *new-pcg-role* ändern, aktualisiert CSM die Rolle für die PCG-Instanz auf AWS auf *new-pcg-role*. Der PCM weiß jedoch nicht, dass die PCG-Rolle aktualisiert wurde, und verwendet daher weiterhin die alten AWS-Clients, die er unter Verwendung der Rolle *old-pcg-role* erstellt hat. Dies führt dazu, dass die Prüfung der AWS-Cloud-Bestandsliste des PCM und andere AWS-Cloud-Aufrufe fehlschlagen.

Problemumgehung: Wenn dieses Problem auftritt, ändern/löschen Sie nach dem Wechsel zu der neuen Rolle die alte PCG-Rolle für mindestens 6,5 Stunden nicht. Beim Neustarten des PCG werden alle AWS-Clients mit den Anmeldedaten der neuen Rolle neu gestartet.

## Bekannte Probleme bei Betriebs- und Überwachungsdiensten

- **Problem 2275869: Rollover des cfgAgent-Protokolls in weniger als 1 Minute auf dem ESXi-Host, wenn Regeln auf dem Host Tags mit einer Länge von mehr als 31 Zeichen aufweisen**  
Häufige Protokoll-Rollover können zum Verlust nützlicher Informationen im Protokoll „cfgAgent.log“ für Debugging und Fehlerbehebung auf dem Host führen. Protokollspeicherort auf dem ESXi-Host: `/var/log/cfgAgent.log`

Problemumgehung: Keine.

- **Problem 2289984: „mux\_connectivity\_status“ wird selbst nach dem Beenden des nsx-context-mux-Diensts auf dem Host als CONNECTED angezeigt**  
Wenn „nsx-context-mux“ oder „nsx-opsagent“ nicht auf dem Host ausgeführt wird, zeigt das System (NSX-Schnittstellen- oder -Dienstinstanz-API) fälschlicherweise den Lösungsstatus und den GI-Agent-Status als „Wird ausgeführt“ mit einem unveränderten Zeitstempel an. Dies führt dazu, dass der AV-Schutz der Gast-VMs möglicherweise verloren geht.

Problemumgehung: Versuchen Sie, „mux“ und „opsagent“ auf dem Host manuell zu starten, wenn sie nicht bereits ausgeführt werden.

1. Melden Sie sich beim Host als „root“ an und führen Sie die folgenden Befehle aus:  
`/etc/init.d/nsx-opsagent start`  
`/etc/init.d/nsx-context-mux start`
2. Warten Sie nach dem Starten der Agents einige Minuten und vergewissern Sie sich, dass der Integritäts-Zeitstempel auf der Benutzeroberfläche aktualisiert wurde.

## Bekannte Upgradeprobleme

- **Problem 2273737: Nach dem Upgrade von NSX-T 2.3 auf 2.4 fehlen Details zum vIDM-Server**  
Wenn vIDM-Benutzer verwendet werden, wobei der vIDM-Server nur auf der NSX-Policy-Appliance konfiguriert ist, wird der vIDM-Server innerhalb des Upgrades migriert, aber der vIDM-Server fehlt in der konvergierten Appliance.

Problemumgehung: Je nach dem Zeitpunkt, zu dem das Problem beim Kunden auftritt, gibt es zwei Optionen:

- Vor dem Upgrade von Version 2.3 auf 2.4:  
Konfigurieren Sie dieselben vIDM-Serverdetails auf der NSX-Policy-Appliance und der NSX Manager-VM.
- Nach dem Upgrade von Version 2.3 auf 2.4:  
Konfigurieren Sie dieselben vIDM-Serverdetails erneut auf der konvergierten Appliance.

- **Problem 2288549: RepoSync schlägt mit einem Prüfsummenfehler in der Manifestdatei fehl**

Dies wurde bei Bereitstellungen beobachtet, für die kürzlich ein Upgrade auf Version 2.4 durchgeführt wurde. Wenn ein aktualisiertes Setup gesichert und auf einem neu bereitgestellten Manager wiederhergestellt wird, stimmen die Prüfsumme der Repository-Manifestdatei und die Prüfsumme der tatsächlichen Manifestdatei nicht überein. Dies führt dazu, dass RepoSync nach der Wiederherstellung der Sicherung als „Fehlgeschlagen“ markiert wird.

Problemumgehung: Um diesen Fehler zu beheben, führen Sie die folgenden Schritte aus:

1. Führen Sie den CLI-Befehl `get service install-upgrade` aus.  
Beachten Sie die IP von „Aktiviert auf“ in den Ergebnissen.
2. Melden Sie sich bei der NSX Manager-IP an, die in der „Aktiviert auf“-Rückgabe des oben angegebenen Befehls ausgegeben wird.
3. Navigieren Sie zu **System > Übersicht** und suchen Sie den Knoten mit der in der „Aktiviert auf“-Rückgabe angegebenen IP.
4. Klicken Sie für diesen Knoten auf **Beheben**.
5. Klicken Sie, nachdem die oben angegebene Behebung erfolgreich war, für alle Knoten derselben Schnittstelle auf **Beheben**.

Für alle drei Knoten wird jetzt der RepoSync-Status als **Abgeschlossen** angezeigt.

- **Problem 2279973: Wenn eine leere Gruppe erstellt und das Upgrade fortgesetzt wird, wird nach dem MP-Upgrade diese leere Gruppe nicht als „Gestartet“ angezeigt**  
Dies tritt auf, wenn eine leere Gruppe erstellt und das Upgrade fortgesetzt wird.

Problemumgehung: Erstellen Sie keine leere Gruppe.

Führen Sie einen der folgenden Schritte aus, um fortzufahren:

- Löschen Sie die leere Gruppe.
- Klicken Sie auf eine Schaltfläche zum Fortsetzen, um das Upgrade abzuschließen.
- Setzen Sie den Plan zurück.
- **Problem 2282389: Der UC-Upgrade-Plan ist nicht mit der VC-Cluster-Mitgliedschaft synchronisiert, wenn ESX über Cluster hinweg verschoben wird**  
Wenn ESX im VC von einem Cluster in einen anderen verschoben wird, spiegelt sich die Änderung nicht im UC-Upgrade-Plan wider. Dies kann dazu führen, dass mehr als ein HOST gleichzeitig in den Wartungsmodus wechselt, wenn der Benutzer über Gruppen hinweg „Paralleles Upgrade“ ausgewählt hat.

Problemumgehung: Klicken Sie auf der Seite „Host-Upgrade“ auf die Option „Zurücksetzen“, um den Plan so neu zu erstellen, dass der UC-Upgrade-Plan mit den VC-Clustern synchronisiert ist.

- **Problem 2288921: Der Upgrade-Status ist nicht mehr synchronisiert, wenn Edge-Knoten mit einer alten Version hinzugefügt werden**  
Der Upgrade-Status ist nicht mehr synchronisiert, wenn der Benutzer nach einem Edge-Upgrade Edge-Knoten einer älteren Version hinzufügt. Dies führt zu Problemen beim Fortsetzen des Upgrade-Aufrufs.

Problemumgehung: Vermeiden Sie zunächst, dass Edge-Knoten mit einer alten Version hinzugefügt werden. Wenn das Problem dennoch auftritt, starten Sie den UC-Dienst neu.

- **Problem 2291625: Nach der Synchronisierung des Upgrade-Plans wird der PCG-Upgrade-Status von SUCCESS in NOT\_STARTED geändert**  
Dieses Problem tritt nur dann auf, wenn der Benutzer ein Upgrade des PCG durchführt und dann versucht, nachträglich ein Upgrade weiterer Agents/PCGs durchzuführen.  
Im empfohlenen Workflow sind nach dem PCG-Upgrade keine weiteren Cross-Cloud-Komponenten mehr vorhanden, für die ein Upgrade über die UC-Schnittstelle durchgeführt werden soll.

Dies wirkt sich auf keine der Funktionen aus. Der Status des zuvor erfolgreich abgeschlossenen PCG-Upgrades wird auf der Upgrade-Benutzeroberfläche als „Keine“ angezeigt.

Problemumgehung: Keine. Die Funktionalität sollte hiervon nicht betroffen sein.

- **Problem 2293227:** Nach dem Upgrade auf Version 2.4 werden für VMs, auf denen VMTools 10.3.5 ausgeführt wird, keine IDFW-Regeln angewendet  
Nach dem Durchführen eines Live-NSX-T-Upgrades werden für VMs, auf denen VMTools 10.3.5 ausgeführt wird, keine IDFW-Regeln angewendet. Dies kann zu einem Verlust des AV-Schutzes für diese VMs führen.

Problemumgehung: Starten Sie die betroffenen VMs neu.

- **Problem 2295564:** Die Konnektivität des Edge-Knoten-Controllers geht möglicherweise nach dem Upgrade von 2.3 auf 2.4 verloren  
Dies ist ein Problem, das zeitweilig auftritt und sich teilweise auf den Nord-Süd-Datenverkehr auswirkt.

Problemumgehung: Aktivieren und deaktivieren Sie den Wartungsmodus auf demselben Edge-Knoten.

- **Problem 2294178 – Das Host-VIB-Update schlägt während des Upgrades von 2.3.1 auf 2.4 fehl.**  
Der Upgrade-Vorgang von Version 2.3.1 auf 2.4 kann mit der Fehlermeldung „Installieren von Offline-Paket auf dem Host“ fehlschlagen. Genau genommen schlägt das Host-VIB-Update fehl, weil das Switch-Sicherheitsmodul nicht entladen werden kann. Das Problem tritt bekanntermaßen auf, wenn die IP Discovery-Funktion im Switching-Profil aktiviert ist und wenn ein direktes Upgrade von NSX-T 2.3.1 auf NSX-T 2.4 mit einem Host durchgeführt wird, auf dem ESXi-6.7EP06 (Build 11675023) ausgeführt wird.

Problemumgehung: Eine Problemumgehung finden Sie im Knowledgebase-Artikel 67445 [With IP Discovery enabled, host VIB update may fail when upgrading from NSX-T 2.3.1 to NSX-T 2.4](#).

- **Problem 2277543 – Das Host-VIB-Update schlägt während des direkten Upgrades mit der Fehlermeldung „Installieren von Offline-Paket auf dem Host fehlgeschlagen“ fehl.**  
Dieser Fehler kann auftreten, wenn vor einem direkten Upgrade von NSX-T 2.3.x auf 2.4 Storage vMotion auf dem Host ausgeführt wurde und wenn auf dem Host ESXi-6.5P03 (Build 10884925) ausgeführt wird. Das Switch-Sicherheitsmodul von 2.3.x wird nicht entfernt, wenn kurz vor dem Host-Upgrade Storage vMotion ausgeführt wurde. Storage vMotion löst einen Arbeitsspeicherverlust aus, der dazu führt, dass das Entladen des Switch-Sicherheitsmoduls fehlschlägt.

Problemumgehung: Weitere Informationen finden Sie im Knowledgebase-Artikel 67444 [Host VIB update may fail when upgrading from NSX-T 2.3.x to NSX-T 2.4.0 if VMs are storage vMotioned before host upgrade](#).

- **Problem 2276398 – Wenn eine AV-Partnerdienst-VM mithilfe von NSX aktualisiert wird, kann es zu einem bis zu zwanzig Minuten dauernden Verlust des Schutzes kommen.**  
Wenn eine Partner-SVM aktualisiert wird, wird die neue SVM bereitgestellt und die alte SVM wird gelöscht. Im Host-Syslog werden möglicherweise SolutionHandler-Verbindungsfehler angezeigt.

Problemumgehung: Löschen Sie nach dem Upgrade den ARP-Cache-Eintrag auf dem Host und pingen Sie dann die Partnersteuerungs-IP auf dem Host, um dieses Problem zu beheben.

- **Problem 2297918 – Nach dem Upgrade von 2.3.1 auf 2.4 kann NSX nicht auf dem Cluster entfernt werden.**  
Nach dem Upgrade eines Clusters von 2.3.1 auf 2.4 kann NSX-T nicht entfernt werden und schlägt mit der folgenden Meldung fehl: „Fehler beim Entfernen von NSX auf dem Cluster: Für diese Fabric-Vorlage existiert eine zugehörige Transportknotenvorlage oder Transportknotensammlung. Die Transportknotenvorlage oder Transportknotensammlung muss vor dem Löschen/Deaktivieren auf dieser Fabric-Vorlage gelöscht werden.“

Problemumgehung: Trennen Sie das Transportknotenprofil vom betroffenen Cluster und führen Sie dann den Workflow „NSX entfernen“ aus.

- **Problem 2286030 – Die Transportknotenkonfiguration wird als fehlgeschlagen angezeigt, wenn**

ein Upgrade von NSX-T 2.3.x und früher auf 2.4.x durchgeführt wird.

Die Transportknotenkonfiguration geht bei einem Upgrade von NSX-T 2.3.x und früher auf 2.4.x aufgrund einer Nullzeiger-Ausnahme in den Fehlerzustand über. Wenn Sie über einen ESXi-Transportknoten mit vmkernel-Adaptoren verfügen, die auf N-VDS VLAN logical-switch migriert wurden, und ein Upgrade von NSX-T 2.3.x auf NSX-T 2.4.x durchführen, kann eine Wettlaufsituation dazu führen, dass der Konfigurationsstatus des ESXi-Transportknotens als fehlgeschlagen angezeigt wird. Die Konnektivität des ESXi-Transportknotens mit NSX Manager und Controllern ist jedoch während des Upgrades intakt, auch wenn der Knoten für den Konfigurationsstatus fehlgeschlagen ist.

Problemumgehung: Aktualisieren oder senden Sie den Transportknoten erneut, um den Konfigurationsstatus auf „Erfolgreich“ zurückzusetzen.

1. Bearbeiten Sie im NSX Manager den ESXi-Transportknoten, der als fehlgeschlagen angezeigt wird.
2. Klicken Sie im Pop-up-Fenster für die Konfiguration des ESXi-Transportknotens auf **Speichern**.  
Diese Aktion setzt den Status zurück. Sie müssen die Konfiguration nicht ändern.

## Bekannte Probleme mit APIs

### Bekannte Probleme beim NSX Policy Manager

- **Problem 2291267:** Einem vom PCM erstellten Standard-Gateway-Richtlinienabschnitt ist keine Sequenznummer zugewiesen, sodass die Richtlinie diese standardmäßig auf 0 festlegt  
Wenn ein Benutzer Gateway-Richtlinien ohne Sequenznummern oder insert\_top-Optionen erstellt, führt dies zu einem Richtlinienkonflikt. Speicherort des Protokolls: `/var/log/policy/policy.log`

Problemumgehung: Vermeiden Sie dieses Problem, indem Sie immer Richtlinien mit geeigneten `sequence_numbers` oder unter Verwendung des URL-Parameters `action=revise&operation=insert_top` erstellen.

- **Problem 2289278:** Die Richtlinien-API löst einen Fehler aus, lässt jedoch die Konfiguration von mehreren virtuellen Servern mit demselben Pool und mit unterschiedlichem Persistenzprofil zu  
Das System unterstützt die Konfiguration von widersprüchlichen Persistenztypen für denselben Pool und für unterschiedliche LbVirtualServers nicht. Die Richtlinie validiert/verweigert jedoch die widersprüchliche Eingabe nicht ordnungsgemäß und lässt die Konfiguration zu. In der Folge zeigt die Richtlinie einen Alarm mit der entsprechenden Fehlermeldung an.

Problemumgehung: Wenn dieses Problem auftritt, können Sie es korrigieren, indem Sie die Gruppeneinstellung auf dem LbVirtualServer ändern.

- **Problem 2248186 – Der BGP-Router installiert IPv6-Routen von seinem Nachbarn mit seiner eigenen Schnittstelle als nächstem Hop.**  
Infolgedessen kann die IPv6-Weiterleitung für die installierte Route fehlschlagen und zu einer Weiterleitungsschleife führen.

Problemumgehung: Um dieses Problem zu vermeiden, konfigurieren Sie eine Route Map, um die mit IPv6 verbundenen Adressen als nächsten Hop in den BGP-Updates zu filtern.

### Bekannte Probleme bei NSX Cloud

- **Problem 2287884:** Bestimmte Centos-Marketplace-Images werden für NSX Cloud nicht unterstützt  
Nur die Centos-Marketplace-Images, deren Verteilung mit ihren erwarteten Kernel-Unterversionen übereinstimmen, werden für NSX Cloud unterstützt.  
Beispiel: Die Verteilungsversionen und ihre entsprechenden Kernel-Versionen sollten erwartungsgemäß wie folgt lauten:

- RHEL 7.5 3.10.0-862

- RHEL 7.4 3.10.0-693
- RHEL 7.3 3.10.0-514

Problemumgehung: Verwenden Sie ausschließlich in der Dokumentation empfohlene Centos-Verteilungen.

- **Problem 2275232: DHCP funktioniert nicht für VMs in der Cloud, wenn Connectivity\_statregy für DFWs von BLACKLIST in WHITELIST geändert wird**

Alle VMs, die neue DHCP-Leases anfordern, verlieren die IPs. DHCP muss in DFW explizit für Cloud-VMs zugelassen werden.

Problemumgehung: Lassen Sie in DFW DHCP explizit für Cloud-VMs zu.

- **Problem 2277814: Eine VM wird aufgrund eines ungültigen Werts für das nsx.network-Tag zu „vm-overlay-sg“ verschoben**

Eine VM, die mit einem ungültigen nsx.network-Tag versehen ist, wird zu „vm-overlay-sg“ verschoben.

Problemumgehung: Entfernen Sie das ungültige Tag.

- **Problem 2280663: Paralleles Offboarding von mehreren VPCs kann in seltenen Fällen zu Fehlern führen**

Das Offboarding einer der Compute-VPCs schlägt fehl.

Problemumgehung: Bereinigen Sie die VPC und die entsprechenden Gruppen in der Richtlinie manuell.

- **Behobenes Problem 2287124: Nach der Bereitstellung des PCG in einem Microsoft Azure-VNET wird auf der VNET-Kachel in CSM fälschlicherweise eine Warnung angezeigt**

Nach der Bereitstellung des PCG in einem Microsoft Azure-VNET zeigt VNET in CSM ein Warnsignal (gelbes Dreieck mit Ausrufezeichen). Wenn Sie den Mauszeiger über das Warnsymbol bewegen, meldet CSM, dass der Status von MP (Management Plane) und CCP (Control Plane) unbekannt ist. Es liegt jedoch möglicherweise kein Problem mit der Konnektivität vor und die Warnung wird fälschlicherweise angezeigt.

- **Problem 2290688 – Das Upgrade von Windows 2016-VMs in AWS schlägt fehl.**

Upgrade mehrerer Windows-Workload-VMs schlägt in AWS fehl. Der Status der VM-Aktualisierung bleibt im AWS-Portal bei der ersten von zwei Überprüfungen stehen. Ein erneuter Versuch schlägt ebenfalls fehl. Dieses Problem tritt nur bei Upgrades derselben NSX-T-Version auf.

Problemumgehung: Um dieses Problem zu beheben, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass das PCG auf den betroffenen Hosts aktualisiert wurde, damit die VM die neuesten Host-Komponenten herunterladen kann.
2. Starten Sie die VM neu, um sie in einen ordnungsgemäßen Zustand zu versetzen.
3. Führen Sie den uninstall-Befehl manuell aus.
4. Führen Sie den install-Befehl manuell aus.