

# Versionshinweise zu VMware NSX for vSphere 6.3.5

VMware NSX for vSphere 6.3.5 | Veröffentlicht am 16. November 2017 | Build 7119875

Siehe den [Revisionsverlauf](#) dieses Dokuments.

## Inhalt dieser Versionshinweise

Diese Versionshinweise decken die folgenden Themen ab:

- [Neuigkeiten in NSX 6.3.5](#)
- [Versionen, Systemanforderungen und Installation](#)
- [Eingestellte und nicht fortgeführte Funktionalität](#)
- [Upgrade-Hinweise](#)
- [FIPS-Konformität](#)
- [Revisionsverlauf](#)
- [Behobene Probleme](#)
- [Bekannte Probleme](#)

## Neuigkeiten in NSX 6.3.5

**Wichtiger Hinweis:** Wenn Sie für NSX 6.2.0, 6.2.1 oder 6.2.2 ein Upgrade auf NSX 6.3.5 durchführen, müssen Sie vor Beginn des Upgrades eine Problemumgehung durchführen. Details finden Sie im [VMware-Knowledgebase-Artikel 000051624](#).

In NSX for vSphere 6.3.5 wurden Verbesserungen in Bezug auf die Betriebsfähigkeit vorgenommen und einige von Kunden gemeldete Probleme wurden behoben. Weitere Informationen dazu finden Sie unter [Behobene Probleme](#).

- Die Guest Introspection-SVM ignoriert nun von Gast-VMs gesendete Netzwerkereignisse, es sei denn, die identitätsbasierte Firewall oder die Funktionen zur Endpunktüberwachung sind aktiviert.
- Sie können auch den Schwellenwert für Systemereignisse bezüglich der CPU- und Arbeitsspeicherauslastung mit dieser API ändern: PUT /api/2.0/endpointsecurity/usvmstats/usvmhealththresholds
- Verbesserungen in Bezug auf die L2-VPN-Betriebsfähigkeit, z. B.:
  - Ändern und/oder Aktivieren der Protokollierung im laufenden Betrieb ohne Prozessneustart
  - Optimierte Protokollierung
  - Tunnelstatus und Statistiken
  - CLI-Verbesserungen
  - Ereignisse für die Änderung des Tunnelstatus
- Weitergeleitete Syslog-Nachrichten enthalten nun zusätzliche Details, die zuvor nur im vSphere Web Client angezeigt wurden.
- Hostvorbereitung verfügt nun über eine verbesserte Fehlerbehebung einschließlich zusätzlicher Informationen für „Nicht bereit“-Fehler.

Versionshinweise für vorherige Versionen:

- NSX [6.3.4](#)

- NSX [6.3.3](#)
- NSX [6.3.2](#)
- NSX [6.3.1](#)
- NSX [6.3.0](#)

## Versionen, Systemanforderungen und Installation

### Hinweis:

- In der folgenden Tabelle sind empfohlene Versionen von VMware-Software aufgelistet. Diese Empfehlungen sind allgemeiner Natur. Umgebungsspezifische Empfehlungen haben demgegenüber Vorrang.
- Diese Informationen sind auf dem Stand des Veröffentlichungsdatums dieses Dokuments.
- Die **unterstützten Mindestversionen** von NSX und anderen VMware-Produkten entnehmen Sie der [VMware-Produkt-Interoperabilitätsmatrix](#). Die Einstufung als unterstützte Mindestversionen durch VMware erfolgt auf der Basis interner Tests.
  - **Die für NSX-Interoperabilität erforderliche unterstützte Mindestversion für vSphere unterscheidet sich für NSX 6.3.2 und NSX 6.3.3.** Ausführliche Informationen finden Sie in der [VMware-Produkt-Interoperabilitätsmatrix](#).

Produkt oder Komponente	Empfohlene Version
NSX for vSphere	<p>VMware empfiehlt die neueste NSX 6.3-Version für neue Bereitstellungen sowie zum Durchführen eines Upgrades von 6.1.x.</p> <p>Wenn Sie für vorhandene Bereitstellungen ein Upgrade durchführen möchten, lesen Sie bitte die NSX-Versionshinweise oder wenden Sie sich an einen Mitarbeiter des technischen Supports von VMware für weitere Informationen zu spezifischen Problemen, bevor Sie ein Upgrade planen.</p>
vSphere	<ul style="list-style-type: none"> <li>• vSphere 5.5U3 und höher</li> <li>• vSphere 6.0U3 und höher. vSphere 6.0U3 behebt das Problem der doppelten VTEPs in ESXi-Hosts nach dem Neustart von vCenter Server. Weitere Informationen dazu enthält der <a href="#">VMware-Knowledgebase-Artikel 2144605</a>.</li> <li>• vSphere 6.5U1 und höher. vSphere 6.5U1 behebt das Problem eines EAM-Versagens bei OutOfMemory-Fehlern. Weitere Informationen dazu enthält der <a href="#">VMware-Knowledgebase-Artikel 2135378</a>.</li> </ul>

Es werden alle Versionen von VMware Tools unterstützt. Für einige Guest Introspection-basierte Funktionen sind neuere Versionen von VMware Tools erforderlich:

#### Guest Introspection für Windows

- Verwenden Sie VMware Tools 10.0.9 und 10.0.12 für die Aktivierung der optionalen, in VMware Tools enthaltenen Thin Agent-Komponente des Netzwerk-Introspektions-Treibers.
- Führen Sie ein Upgrade auf VMware Tools 10.0.8 und höher für die Behebung des Problems verlangsamer VMs nach dem Upgrade von VMware Tools in NSX/vCloud Networking and Security durch (siehe [VMware-Knowledgebase-Artikel 2144236](#)).
- Verwenden Sie VMware Tools 10.1.0 und höher zur Unterstützung von Windows 10.
- Verwenden Sie VMware Tools 10.1.10 und höher zur Unterstützung von Windows Server 2016.

Diese NSX-Version unterstützt die folgenden Linux-Versionen:

#### Guest Introspection für Linux

- RHEL 7 GA (64 Bit)
- SLES 12 GA (64 Bit)
- Ubuntu 14.04 LTS (64 Bit)

Hinweis: VMware unterstützt aktuell nicht NSX for vSphere 6.3.x mit vRealize Networking Insight 3.2.

## Systemanforderungen und Installation

Eine vollständige Liste der NSX-Installationsvoraussetzungen finden Sie im Abschnitt [Systemvoraussetzungen für NSX](#) im *Installationshandbuch für NSX*.

Anweisungen zur Installation erhalten Sie im [Installationshandbuch für NSX](#) oder im [Installationshandbuch zu Cross-vCenter NSX](#).

## Eingestellte und nicht fortgeführte Funktionalität

### Warnungen zum Ende der Lebensdauer und des Supports

Informationen zu NSX- und anderen VMware-Produkten, für die demnächst ein Upgrade durchgeführt werden muss, finden Sie unter der [VMware-Lebenszyklus-Produktmatrix](#).

- Für NSX for vSphere 6.1.x gilt als Ende der Verfügbarkeit (EOA, End of Availability) und des allgemeinen Supports (EOGS, End of General Support) der 15. Januar 2017. (Informationen hierzu finden Sie auch im [VMware-Knowledgebase-Artikel 2144769](#).)
- NSX Data Security wurde entfernt: In der Version NSX 6.3.0 wurde die Funktion NSX Data Security aus dem Produkt entfernt.
- NSX Activity Monitoring (SAM) wird nicht mehr unterstützt: Ab NSX 6.3.0 wird Activity Monitoring nicht mehr in NSX unterstützt. Verwenden Sie stattdessen die Endpunktüberwachung. Weitere Informationen dazu finden Sie unter [Endpunktüberwachung](#) im *Administratorhandbuch für NSX*.

- **Web Access Terminal wurde entfernt:** Web Access Terminal (WAT) wurde aus NSX 6.3.0 entfernt. Sie haben nicht die Möglichkeit, Web Access SSL VPN-Plus zu konfigurieren und den Zugriff auf die öffentliche URL über NSX Edge zu aktivieren. VMware empfiehlt die Verwendung des Vollzugriffs-Clients bei SSL VPN-Bereitstellungen zur Verbesserung der Sicherheit. Wenn Sie die WAT-Funktionalität in früheren Versionen verwenden, müssen Sie diese deaktivieren, bevor Sie ein Upgrade auf 6.3.0 durchführen.
- **IS-IS wurde aus NSX Edge entfernt:** Ab der Version NSX 6.3.0 kann das IS-IS-Protokoll nicht mehr auf der Registerkarte Routing konfiguriert werden.
- **vCNS-Edges werden nicht mehr unterstützt.** Vor dem Upgrade auf NSX 6.3.x müssen Sie zuerst ein Upgrade auf ein NSX Edge durchführen.

## Entfernung von APIs und Änderungen des Verhaltens

### Änderungen in Bezug auf die API-Fehlerbehandlung

In NSX 6.3.5 werden folgende Änderungen in Bezug auf die Fehlerbehandlung eingeführt:

- Wenn eine API-Anforderung eine Datenbankausnahme auf dem NSX Manager zur Folge hat, lautet die Antwort *500 Interner Serverfehler*. Bei früheren Versionen antwortete der NSX Manager mit *200 OK*, obwohl die Anforderung fehlschlug.
- Wenn Sie eine API-Anforderung mit einem leeren Text senden, wenn ein Anforderungstext erforderlich ist, lautet die Antwort *400 Ungültige Anforderung*. Bei früheren Versionen antwortete der NSX Manager mit *500 Interner Serverfehler*.
- Wenn Sie in dieser API (GET /api/2.0/services/policy/securitygroup/{ID}/securitypolicies) eine falsche Sicherheitsgruppe angeben, lautet die Antwort *404 Nicht gefunden*. Bei früheren Versionen antwortete der NSX Manager mit *200 OK*.

### Änderungen in Bezug auf die Standardeinstellungen für die API-Sicherung und -Wiederherstellung

Seit Version 6.3.3 sind die Standardeinstellungen für zwei Sicherungs- und Wiederherstellungsparameter geändert, sodass sie den Standardeinstellungen in der Benutzeroberfläche entsprechen. Für **passiveMode** und **useEPSV** lautete die Standardeinstellung bisher *false*. Nun lautet sie *true*. Davon sind folgende APIs betroffen:

- PUT /api/1.0/appliance-management/backuprestore/backupsettings
- PUT /api/1.0/appliance-management/backuprestore/backupsettings/ftpsettings

### Löschen der Firewallkonfiguration oder des Standardabschnitts

- Seit Version 6.3.0 wird diese Anforderung abgelehnt, wenn im Standardabschnitt Folgendes angegeben ist: DELETE /api/4.0/firewall/globalroot-0/config/layer2sections|layer3sections/sectionId
- Zum Abrufen der Standardkonfiguration wurde eine neue Methode integriert. Mit der Ausgabe dieser Methode können Sie die gesamte Konfiguration oder jeden Standardabschnitt ersetzen:
  - Abrufen der Standardkonfiguration mit GET /api/4.0/firewall/globalroot-0/defaultconfig
  - Aktualisieren der gesamten Konfiguration mit PUT /api/4.0/firewall/globalroot-0/config
  - Aktualisieren eines einzelnen Abschnitts mit PUT /4.0/firewall/globalroot-0/config/layer2sections|layer3sections/{sectionId}

### defaultOriginate-Parameter:

Seit Version NSX 6.3.0 ist der Parameter „defaultOriginate“ nur aus den folgenden Methoden für NSX Edge-Appliances von logischen (verteilten) Routern entfernt:

- GET/PUT /api/4.0/edges/{edge-id}/routing/config/ospf
- GET/PUT /api/4.0/edges/{edge-id}/routing/config/bgp
- GET/PUT /api/4.0/edges/{edge-id}/routing/config

Die Festlegung von `defaultOriginate` auf „True“ für eine Edge-Appliance eines logischen (verteilten) Routers für NSX 6.3.0 oder höher schlägt fehl.

Alle IS-IS-Methoden wurden aus dem NSX Edge-Routing entfernt.

- GET/PUT/DELETE /4.0/edges/{edge-id}/routing/config/isis
- GET/PUT /4.0/edges/{edge-id}/routing/config

## Entfernungen von CLI und Änderungen des Verhaltens

Verwenden Sie keine nicht unterstützten Befehle auf NSX Controller-Knoten

Es sind nicht dokumentierte Befehle zur Konfiguration von NTP und DNS auf NSX Controller-Knoten vorhanden. Diese Befehle werden nicht unterstützt und dürfen nicht auf NSX Controller-Knoten verwendet werden. Es stehen nur diejenigen Befehle zur Verfügung, die im NSX-CLI-Handbuch dokumentiert sind.

## Upgrade-Hinweise

- [Allgemeine Upgrade-Hinweise](#)
- [Upgrade-Hinweise für NSX-Komponenten](#)
- [Upgrade-Hinweise für FIPS](#)

Hinweis: Eine Liste der bekannten Probleme, die Auswirkungen auf die Installation und auf Upgrades haben, finden Sie im Abschnitt [Bekannte Installations- und Upgrade-Probleme](#).

### Allgemeine Upgrade-Hinweise

- Für das Upgrade von NSX müssen Sie ein vollständiges NSX-Upgrade einschließlich eines Hostcluster-Upgrades durchführen (wobei die Host-VIBs aktualisiert werden). Anweisungen hierzu erhalten Sie im [Upgrade-Handbuch für NSX](#) im Abschnitt [Aktualisieren der Hostcluster](#).
- **Systemvoraussetzungen:** Die Informationen zu den Systemanforderungen für die Installation und das Upgrade von NSX werden im Abschnitt [Systemvoraussetzungen für NSX](#) der NSX-Dokumentation dargestellt.
- **Upgrade-Pfad von NSX 6.x:** Die [VMware-Produkt-Interoperabilitätsmatrix](#) bietet Details zu den Upgrade-Pfaden von VMware NSX.
- Das Upgrade für Cross-vCenter NSX wird im [Upgrade-Handbuch für NSX](#) erläutert.
- **Herabstufungen werden nicht unterstützt:**
  - Führen Sie vor der Durchführung eines Upgrades immer eine Sicherung von NSX Manager durch.
  - Nach einem erfolgreichen Upgrade von NSX ist kein Downgrade von NSX möglich.
- Zur Überprüfung, ob Ihr Upgrade auf NSX 6.3.x erfolgreich durchgeführt wurde, erhalten Sie Erläuterungen im [Knowledgebase-Artikel 2134525](#).
- Upgrades von vCloud Networking and Security auf NSX 6.3.x werden nicht unterstützt. Sie müssen zuerst ein Upgrade auf eine unterstützte 6.2.x-Version durchführen.
- **Interoperabilität:** Überprüfen Sie vor dem Upgrade die [VMware-Produkt-Interoperabilitätsmatrix](#) für alle betreffenden VMware-Produkte.
  - **Upgrade auf vSphere 6.5a oder höher:** Wenn Sie ein Upgrade von vSphere 5.5 oder 6.0 auf vSphere 6.5a oder höher durchführen möchten, müssen Sie zuerst ein Upgrade auf NSX 6.3.x durchführen.

vornehmen. Weitere Informationen dazu finden Sie unter [Upgrade von vSphere in einer NSX-Umgebung](#) im *Upgrade-Handbuch für NSX*.

Hinweis: NSX 6.2.x ist nicht mit vSphere 6.5 kompatibel.

- **Upgrade auf NSX 6.3.3 oder höher:** Die unterstützte Mindestversion für die vSphere for NSX-Interoperabilität unterscheidet sich für NSX 6.3.2 und NSX 6.3.3. Ausführliche Informationen finden Sie in der [VMware-Produkt-Interoperabilitätsmatrix](#).
- **Kompatibilität mit Partnerdiensten:** Wenn Ihre Site VMware-Partnerdienste für Guest Introspection oder für die Netzwerk-Introspektion verwendet, müssen Sie mithilfe des [VMware-Kompatibilitäts-Handbuchs](#) vor dem Upgrade prüfen, ob der Dienst Ihres Anbieters mit dieser NSX-Version kompatibel ist.
- **Networking & Security-Plug-In:** Nach dem Upgrade von NSX Manager müssen Sie sich vom vSphere Web Client abmelden und wieder bei ihm anmelden. Wenn das NSX-Plug-In nicht ordnungsgemäß angezeigt wird, löschen Sie den Browser-Cache und den Verlauf. Wenn das Networking & Security-Plug-In nicht im vSphere Web Client angezeigt wird, setzen Sie den vSphere Web Client-Server wie im [Upgrade-Handbuch für NSX](#) beschrieben zurück.
- **Zustandsfreie Umgebungen:** Bei NSX-Upgrades in einer statusfreien Hostumgebung werden die neuen VIBs während des NSX-Upgrades im Vorfeld zum Host-Image-Profil hinzugefügt. Das Verfahren von NSX-Upgrades auf statusfreien Hosts muss daher in folgender Reihenfolge durchgeführt werden:  
In Versionen vor NSX 6.2.0 wurde eine einzelne URL in NSX Manager verwendet, über die VIBs für eine bestimmte Version von ESX Host ermittelt werden konnten. (Der Administrator musste also nur eine einzige URL kennen, unabhängig von der NSX-Version.) In NSX 6.2.0 und höher sind die neuen NSX-VIBs über mehrere URLs verfügbar. Führen Sie die folgenden Schritte aus, um die richtigen VIBs zu ermitteln:
  1. Suchen Sie unter `https://<NSXManager>/bin/vdn/nwfabric.properties` nach der neuen VIB-URL.
  2. Rufen Sie die VIBs der erforderlichen ESX-Hostversion über die jeweilige URL ab.
  3. Fügen Sie sie zu einem Image-Profil hinzu.

## Upgrade-Hinweise für NSX-Komponenten

### NSX Manager-Upgrade

- **Wichtiger Hinweis:** Wenn Sie für NSX 6.2.0, 6.2.1 oder 6.2.2 ein Upgrade auf NSX 6.3.5 durchführen, müssen Sie vor Beginn des Upgrades eine Problemumgehung durchführen. Details finden Sie im [VMware-Knowledgebase-Artikel 000051624](#).
- Wenn Sie SFTP für NSX-Sicherungen verwenden, ändern Sie nach dem Upgrade auf Version 6.3.x den Sicherheitsalgorithmus auf `hmac-sha2-256`, da `hmac-sha1` nicht unterstützt wird. Eine Liste der unterstützten Sicherheitsalgorithmen in 6.3.x finden Sie im [VMware-Knowledgebase-Artikel 2149282](#).
- Wenn Sie ein Upgrade von NSX 6.3.3 auf NSX 6.3.4 oder höher durchführen möchten, müssen Sie zunächst die Anweisungen zur Problemumgehung im [VMware-Knowledgebase-Artikel 2151719](#) befolgen.

### Controller-Upgrade

- In NSX 6.3.3 wurde die NSX Controller-Appliance-Festplatte von 20 GB auf 28 GB vergrößert.
- Der NSX Controller-Cluster muss für ein Upgrade auf NSX 6.3.3 drei Controller-Knoten enthalten. Bei weniger als drei Controllern müssen Sie die entsprechende Anzahl an Controllern vor dem Start des Upgrades hinzufügen. Weitere Informationen finden Sie unter [Bereitstellen des NSX Controller-Clusters](#).

- In NSX 6.3.3 hat sich das zugrunde liegende Betriebssystem des NSX Controllers geändert. Bei einem Upgrade von NSX 6.3.2 oder früher auf NSX 6.3.3 oder höher wird deshalb nicht die vorhandene Software aktualisiert. Es werden stattdessen die bestehenden Controller einzeln nacheinander gelöscht und neue Photon OS-basierte Controller bereitgestellt, die dieselben IP-Adressen verwenden.

Wenn die Controller gelöscht werden, werden auch alle zugehörigen DRS-Anti-Affinitätsregeln gelöscht. Sie müssen neue Anti-Affinitätsregeln in vCenter erstellen, um zu verhindern, dass sich die neuen Controller-VMs auf demselben Host befinden.

Weitere Informationen zu Controller-Upgrades finden Sie unter [Upgrade von NSX Controller-Clustern](#).

## Hostcluster-Upgrade

- In NSX 6.3.3 ändern sich NSX VIB-Namen. Die esx-vxlan- und esx-vsip-VIBs werden mit esx-nsxv ersetzt, wenn Sie NSX 6.3.3 oder höher installiert haben.
- **Upgrade ohne Neustart und Deinstallation auf den Hosts:** Bei vSphere 6.0 und höher ist nach einem Upgrade auf NSX 6.3.x für alle nachfolgenden NSX-VIB-Änderungen kein Neustart erforderlich. Stattdessen müssen die Hosts in den Wartungsmodus wechseln, um die VIB-Änderung abzuschließen.

Bei den folgenden Aufgaben ist ein Neustart des Hosts nicht erforderlich:

- Upgrades von NSX 6.3.0 auf NSX 6.3.x auf ESXi 6.0 oder höher.
- Installation des NSX 6.3.x-VIB, die nach dem Upgrade für ESXi von 6.0 auf 6.5.0a oder höher erforderlich ist.

**Anmerkung:** Das ESXi-Upgrade erfordert weiterhin einen Neustart des Hosts.

- Deinstallation des NSX 6.3.x-VIB auf ESXi 6.0 oder höher.

Bei den folgenden Aufgaben ist ein Neustart des Hosts erforderlich:

- Upgrades von NSX 6.2.x oder früher auf NSX 6.3.x (alle ESXi-Versionen).
- Upgrades von NSX 6.3.0 auf NSX 6.3.x auf ESXi 5.5.
- Installation des NSX 6.3.x-VIB, die nach dem Upgrade von ESXi von 5.5 auf Version 6.0 oder höher erforderlich ist.
- Deinstallation des NSX 6.3.x-VIB auf ESXi 5.5.
- **Host bleibt eventuell im Installationsstadium hängen:** Während umfangreicher NSX-Upgrades besteht die Gefahr, dass ein Host bei der Durchführung der Installation für längere Zeit hängen bleibt. Dies kann aufgrund von Problemen bei der Deinstallation alter NSX-VIBs auftreten. In diesem Fall wird der diesem Host zugeordnete EAM-Thread in der VI Client-Aufgabenliste als „Hängend“ vermerkt.

*Problemumgehung:* Gehen Sie wie folgt vor:

- Melden Sie sich bei vCenter mithilfe des VI Client an.
- Klicken Sie mit der rechten Maustaste auf die als „Hängend“ angegebene EAM-Aufgabe und brechen Sie diese ab.
- Vom vSphere Web Client initiieren Sie einen „Auflösen“-Vorgang im Cluster. Für den hängenden Host wird nun eventuell „InProgress“ angezeigt.
- Melden Sie sich beim Host an und initiieren Sie einen Neustart, um den Abschluss des Upgrades auf diesem Host zu erzwingen.

## Upgrade von NSX Edge

- In NSX 6.3.0 wurden die Festplattengrößen der NSX Edge-Appliance geändert:
  - **Kompakt, Groß, Quad Large:** 1 Festplatte mit 584 MB + 1 Festplatte mit 512 MB
  - **Sehr groß:** 1 Festplatte mit 584 MB + 1 Festplatte mit 2 GB + 1 Festplatte mit 256 MB



- **Host-Cluster müssen vor dem Upgrade von NSX Edge-Appliances für NSX vorbereitet werden:**  
Ab 6.3.0 wird eine Kommunikation der Managementebene zwischen NSX Manager und Edge über den VIX-Kanal nicht mehr unterstützt. Es wird nur der Nachrichtenbuskanal unterstützt. Wenn Sie ein Upgrade von NSX 6.2.x oder früher auf NSX 6.3.0 oder höher durchführen, müssen Sie sicherstellen, dass die Hostcluster, auf denen NSX Edge-Appliances bereitgestellt werden, für NSX vorbereitet sind und dass für die Messaging-Infrastruktur der Status GRÜN (GREEN) gilt. Wenn die Hostcluster nicht für NSX vorbereitet sind, schlägt das Upgrade der NSX Edge-Appliance fehl. Ausführliche Informationen finden Sie unter [Upgrade von NSX Edge](#) im *Upgrade-Handbuch für NSX*.

- **Upgrade von Edge Services Gateway (ESG):**

Ab Version NSX 6.2.5 wird die Ressourcenreservierung gleichzeitig mit dem NSX Edge-Upgrade vorgenommen. Wenn vSphere HA auf einem Cluster aktiviert wird, der nicht über ausreichende Ressourcen verfügt, schlägt der Upgrade-Vorgang möglicherweise fehl, da vSphere HA-Einschränkungen verletzt werden.

Um derartige Upgrade-Fehler zu vermeiden, führen Sie die folgenden Schritte durch, bevor Sie ein ESG-Upgrade vornehmen:

Die folgenden Ressourcenreservierungen werden vom NSX Manager verwendet, sofern Sie nicht bei der Installation oder beim Upgrade ausdrücklich andere Werte festgelegt haben.

NSX Edge Formfaktor	CPU-Reservierung	Arbeitsspeicherreservierung
KOMPAKT	1000 MHz	512 MB
GROSS	2000 MHz	1024 MB
QUADLARGE	4000 MHz	2048 MB
X-LARGE	6000 MHz	8192 MB

1. Stellen Sie grundsätzlich sicher, dass Ihre Installation den Empfehlungen für vSphere HA entspricht. Erläuterungen dazu finden Sie im [VMware-Knowledgebase-Artikel 1002080](#).

2. Verwenden Sie die NSX-API für die Feinabstimmung der Konfiguration:

PUT <https://<NSXManager>/api/4.0/edgePublish/tuningConfiguration>

Stellen Sie dabei sicher, dass die Werte für `edgeVCpuReservationPercentage` und

`edgeMemoryReservationPercentage` in die verfügbaren Ressourcen für den Formfaktor passen (siehe Standardwerte in der Tabelle oben).

- **Deaktivieren Sie die Startoption für die virtuelle Maschine von vSphere, sofern vSphere HA aktiviert ist und Edges bereitgestellt sind.** Nach dem Upgrade von NSX Edges 6.2.4 oder früher auf die Version 6.2.5 oder höher müssen Sie die Startoption für die virtuelle Maschine von vSphere für jede NSX Edge-Instanz in einem Cluster deaktivieren, für den vSphere HA aktiviert ist und Edges bereitgestellt sind. Dazu müssen Sie den vSphere Web Client öffnen, den ESXi-Host ermitteln, auf dem sich die NSX Edge-VM befindet, auf „Verwalten“ > „Einstellungen“ klicken und unter „Virtuelle Maschinen“ die Option „VM starten/herunterfahren“ auswählen. Klicken Sie auf „Bearbeiten“ und stellen Sie sicher, dass sich die virtuelle Maschine im manuellen Modus befindet (d. h., sie darf nicht in der Liste „Automatisches Starten/Herunterfahren“ enthalten sein).



- Bevor Sie ein Upgrade auf NSX 6.2.5 oder höher vornehmen, stellen Sie sicher, dass alle Load-Balancer-Verschlüsselungslisten durch Doppelpunkte getrennt sind. Falls in Ihrer Verschlüsselungsliste ein anderes Trennzeichen als ein Komma verwendet wird, führen Sie einen PUT-Aufruf für

`https://nsxmgr_ip/api/4.0/edges/EdgeID/loadbalancer/config/applicationprofiles` durch und ersetzen Sie jede `<ciphers>`-Liste in `<clientSsl>` und `<serverSsl>` durch eine durch Kommas getrennte Liste. Beispielsweise kann das betreffende Segment des Anforderungstextes das im Folgenden dargestellte Aussehen haben. Wiederholen Sie diesen Vorgang für alle Anwendungsprofile:

```
<applicationProfile>
  <name>https-profile</name>
  <insertXForwardedFor>false</insertXForwardedFor>
  <sslPassthrough>false</sslPassthrough>
  <template>HTTPS</template>
  <serverSslEnabled>true</serverSslEnabled>
  <clientSsl>
    <ciphers>AES128-SHA:AES256-SHA:ECDHE-ECDSA-AES256-SHA</ciphers>
    <clientAuth>ignore</clientAuth>
    <serviceCertificate>certificate-4</serviceCertificate>
  </clientSsl>
  <serverSsl>
    <ciphers>AES128-SHA:AES256-SHA:ECDHE-ECDSA-AES256-SHA</ciphers>
    <serviceCertificate>certificate-4</serviceCertificate>
  </serverSsl>
  ...
</applicationProfile>
```

- Legen Sie die richtige Verschlüsselungsversion für Clients mit Lastausgleichsdienst auf vROPs-Versionen vor 6.2.0 fest: vROPs-Poolmitglieder auf vROPs-Versionen vor 6.2.0 verwenden TLS-Version 1.0, weshalb Sie explizit einen Wert für die Überwachungserweiterung festlegen müssen, indem Sie die Einstellung `"ssl-version=10"` in der NSX-Load-Balancer-Konfiguration festlegen. Anweisungen dazu finden Sie unter [Erstellen eines Dienstmonitors](#) im *Administratorhandbuch für NSX*.

```
{
  "expected" : null,
  "extension" : "ssl-version=10",
  "send" : null,
  "maxRetries" : 2,
  "name" : "sm_vrops",
  "url" : "/suite-api/api/deployment/node/status",
  "timeout" : 5,
  "type" : "https",
  "receive" : null,
  "interval" : 60,
  "method" : "GET"
}
```

## Upgrade für Guest Introspection

- Guest Introspection-VMs enthalten nun zusätzliche Informationen über die Hostidentität in einer XML-Datei auf der Maschine. Bei der Anmeldung bei der Guest Introspection-VM sollte die Datei „`/opt/vmware/etc/vami/ovfEnv.xml`“ Informationen über die Hostidentität enthalten.

## Upgrade-Hinweise für FIPS

Wenn Sie ein Upgrade von einer NSX-Version vor NSX 6.3.0 auf NSX 6.3.0 oder höher durchführen möchten, dürfen Sie den FIPS-Modus nicht vor dem Abschluss des Upgrades aktivieren. Wenn Sie den FIPS-Modus vor Abschluss des Upgrades aktivieren, wird die Kommunikation zwischen aktualisierten und nicht aktualisierten Komponenten unterbrochen. Weitere Informationen dazu finden Sie unter [Grundlegendes zum FIPS-Modus und zum NSX-Upgrade](#) im *Upgrade-Handbuch für NSX*.

- Auf OS X Yosemite und OS X El Capitan unterstützte Verschlüsselungen: Wenn Sie auf OS X 10.11 (El Capitan) einen SSL-VPN-Client verwenden, können Sie mit den Verschlüsselungen AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, AES256-SHA und AES128-SHA eine Verbindung herstellen. Auf OS X 10.10 (Yosemite) haben Sie nur mit den Verschlüsselungen AES256-SHA und AES128-SHA die Möglichkeit, eine Verbindung herzustellen.
- Aktivieren Sie den FIPS-Modus erst, wenn das Upgrade auf NSX 6.3.x abgeschlossen ist. Weitere Informationen dazu finden Sie unter [Grundlegendes zum FIPS-Modus und zum NSX-Upgrade](#) im *Upgrade-Handbuch für NSX*.
- Vor der Aktivierung des FIPS-Modus müssen Sie sicherstellen, dass die Partnerlösungen für den FIPS-Modus zertifiziert sind. Informationen dazu finden Sie im [VMware-Kompatibilitäts-Handbuch](#) und in der jeweiligen Partnerdokumentation.

## FIPS-Konformität

- **NSS und OpenSwan:** Das NSX Edge-IPSec-VPN verwendet das NSS-Verschlüsselungsmodul von Mozilla. Aufgrund kritischer Sicherheitsprobleme verwendet diese Version von NSX eine neuere Version von NSS, die nicht für FIPS 140-2 validiert wurde. VMware bestätigt das korrekte Funktionieren des Moduls. Es wird aber nicht mehr offiziell validiert.
- **NSS und Kennworteintrag:** Das NSX Edge-Kennwort-Hashing verwendet das NSS-Verschlüsselungsmodul von Mozilla. Aufgrund kritischer Sicherheitsprobleme verwendet diese Version von NSX eine neuere Version von NSS, die nicht für FIPS 140-2 validiert wurde. VMware bestätigt das korrekte Funktionieren des Moduls. Es wird aber nicht mehr offiziell validiert.
- **Controller und Clustering-VPN:** Der NSX Controller verwendet das IPSec-VPN zur Herstellung einer Verbindung mit Controller-Clustern. Das IPSec-VPN verwendet das VMware-Verschlüsselungsmodul für den Linux-Kernel (Photon 1-Umgebung), das gerade der CMVP-Validierung unterzogen wird.

## Revisionsverlauf der Dokumente

- 16. November 2017: Erste Auflage.
- 17. November 2017: Zweite Auflage. Bekanntes Problem 2000749 wurde hinzugefügt.
- 28. November 2017: Dritte Auflage. Upgrade-Informationen für NSX 6.2.0, 6.2.1, 6.2.2 wurden hinzugefügt.
- 1. Dezember 2017: Vierte Auflage. Die behobenen Probleme 1937124 und 1976332 wurden hinzugefügt.
- 8. Dezember 2017: Fünfte Auflage. Die behobenen Probleme 1790951 und 1935204 wurden hinzugefügt.
- 8. Januar 2018: Sechste Auflage. Behobenes Problem 1920574 wurde hinzugefügt.
- 29. März 2018: Siebte Auflage. Die behobenen Probleme 1967608 und 1947687 wurden hinzugefügt.
- 13. Mai 2019: Achte Auflage. Der Abschnitt „Hostcluster-Upgrade“ wurde aktualisiert.

## Behobene Probleme

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

- [Allgemeine behobene Probleme](#)
- [Behobene Probleme bei logischen Netzwerken und Edge](#)
- [Behobene Probleme beim NSX Manager](#)
- [Behobene Probleme bei NSX Controller](#)
- [Behobene Probleme bei Sicherheitsdiensten](#)

- **Installation und Upgrade**

## Allgemeine behobene Probleme

- **Behobenes Problem 1293896: Von 6.0.x migrierte VMs können zu einem violetten Bildschirm (PSOD, Purple Screen Of Death) führen**  
Beim Upgrade eines Clusters von 6.0.x auf 6.2.3 bis 6.2.8 oder 6.3.x kann der exportierte VM-Status beschädigt sein und zu einem PSOD-Bildschirm auf dem empfangenden Host führen.  
*Problem in 6.3.5 behoben.*
- **Behobenes Problem 1952277: GI-USVM empfängt keine IP-Adresse aus Pool**  
Die dynamische IP, die der eth0-Netzwerkkarte der GI-SVM vom Manager aus dem IP-Pool zugewiesen wurde, verursacht beim Start der GI-SVM einen Fehler, bei dem die Netzwerkkarte darauf hinweist, dass die angegebene Adresse bereits vergeben ist. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1918023: Guest Introspection-USVM belegt 100 % des Arbeitsspeichers**  
Die Guest Introspection-USVM belegt 100 % des Arbeitsspeichers, sodass eventuell die Verbindung von Gast-VMs mit der Guest Introspection-USVM getrennt wird. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1912443: Potenzielles Sicherheitsrisiko, wenn aktuelle Tomcat-Version nicht ausgeführt wird**  
Die älteren Versionen des NSX Manager Tomcat-Diensts weisen Sicherheitsschwachstellen auf.  
*Problem in 6.3.5 behoben.*
- **Behobenes Problem 1920032: SynFlood-Schutz verursacht TCP-Zeitstempelbeschädigung und führt dadurch zu Fehlern beim Klonen und bei der kalten Migration**  
Beim Initiieren einer kalten Migration von VMs zwischen zwei ESXi-Hosts oder beim Erstellen eines vollständigen Klons der VM verursacht der SynFlood-Schutz eine TCP-Zeitstempelbeschädigung.  
*Problem in 6.3.5 behoben.*
- **Behobenes Problem 1920343: Serverzertifikat kann ohne einen privaten Schlüssel erstellt werden**  
Wenn die Daten des privaten Schlüssels im Zertifikatinhalt bereitgestellt werden, wird der private Schlüssel ignoriert. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1874735: „Upgrade verfügbar“-Link wird bei Clusteralarm nicht angezeigt**  
Benutzer können die neue Dienstspezifikation nicht an den EAM weitergeben, da der Link fehlt, und es erfolgt kein Upgrade des Diensts. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1926060: Das Kontrollkästchen „Quelle ablehnen“ unter „Firewall“ > „Quelle oder Ziel angeben“ wird auch dann aktiviert, wenn Sie daneben klicken**  
Das Kontrollkästchen „Quelle ablehnen“ wird aktiviert, wenn Sie Objekte von der Liste der verfügbaren Objekte zu den ausgewählten Objekten verschieben. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1790951: Die Guest Introspection-Bereitstellung kann fehlschlagen, wenn die ersten 20 Zeichen des Clusternamens identisch sind**  
Fehler bei der gleichzeitigen Bereitstellung von Guest Introspection auf mehreren Clustern mit identischen Namen.
- **Behobenes Problem 1947687: NSX-VIB-Installation schlägt möglicherweise fehl, wenn die DVS-Konfiguration Nicht-ASCII-Zeichen enthält**  
Automatische Hostvorbereitung schlägt für Kunden mit ESX 6.5 oder höher möglicherweise fehl, wenn ihre DVS-Konfiguration (Ausgabe von „net-dvs -l“) Nicht-ASCII-Zeichen enthält.  
  
*Problemumgehung:* Vermeiden Sie die Verwendung von Nicht-ASCII-Zeichen für die DVS-Port-Namen. *Problem in 6.3.4 behoben*

## Behobene Probleme bei logischen Netzwerken und Edge

- **Problem 1967608: Kurze Unterbrechung des überbrückten Datenpfads bei Neustart des**

### **Toragent oder NSX-Controllers möglich**

In einer Umgebung, in der ein Hardware-Gateway bereitgestellt wird, tritt möglicherweise eine kurze Unterbrechung des überbrückten Datenpfads auf, wenn der Toragent oder NSX-Controller neu gestartet wird. In betroffenen Umgebungen sollten Controller nur in einem geplanten Wartungsfenster neu gestartet werden. *Problem in 6.3.5 behoben.*

- **Behobenes Problem 1976332: Der NSX Controller speichert den MAC-Eintrag der Workload-VM nicht auf dem ESXi, auf dem die aktive L2-Brücken-Kontroll-VM ausgeführt wird**  
Es treten Datenverkehrsverwerfungen bei allen Workloads auf, die auf dem Hypervisor installiert sind, auf dem die Active-Bridging-Kontroll-VM ausgeführt wird. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1937124: Der überbrückte VXLAN-VLAN-Datenverkehr wurde nach vMotion der Distributed Logical Router-Appliance (Kontroll-VM) unterbrochen**  
Wenn mehrere DLRs zur Überbrückung konfiguriert sind, führen Brücken bei vMotion oder einem Failover-Ereignis keine Aktualisierung des physischen Netzwerks mit VXLAN-VM-MACs durch. Weitere Informationen und eine Problemumgehung finden Sie im VMware-Knowledgebase-Artikel [2151647](#). *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1922967: Edge-IPsec-VPN ist nicht verfügbar, wenn die Peer-End-IP-Adressen immer wieder geändert werden.**  
Das Problem tritt bei Bereitstellungen auf, in denen VPN-Peer-IP-Adressen immer wieder geändert werden (3G-Dongle/dynamische WAN-IP-Adresse). Wenn nach der Änderung der Peer-IP der Tunnel inaktiv ist, wird die Route für das Peer-Subnetz nicht ordnungsgemäß gelöscht. Daher schlägt die IPSec-SA-Installation für das Edge fehl, wenn der Tunnel neu ausgehandelt wird. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1957065: DNS-Weiterleitungsadresse wird nach der REST-API-PUT-Konfiguration aus der ESG-Konfiguration entfernt**  
DNS-Weiterleitungsadresse wird nach der REST-API-PUT-Konfiguration aus der ESG-Konfiguration entfernt. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1916360: Hochverfügbarkeits-Failover schlägt möglicherweise aufgrund einer vollen Festplatte fehl, wenn mehr als 100 Routen installiert sind**  
Wenn mehr als 100 Routen installiert sind, übermittelt der VMware Tools-Daemon auf dem Standby-Edge alle 30 Sekunden 2 Warnprotokollmeldungen. Die Protokolle werden in einer Datei namens „/var/log/vmware-vmtoolsd.log“ gespeichert, die im Laufe der Zeit den gesamten Speicherplatz der Protokollpartition belegen kann. Die Protokollrotation ist für diese Protokolldatei nicht konfiguriert. Wenn dieses Problem auftritt, schlägt das Hochverfügbarkeits-Failover möglicherweise fehl. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1916580: Edge lässt keine Vorgänge mit der Fehlermeldung „Zertifikat xx enthält keinen Privatschlüssel“ zu**  
Beim Upgrade von NSX Manager von Version 6.2.x (bei falscher Konfiguration des Dienstzertifikats) auf Version 6.3.x kann das Edge nicht aktualisiert werden und es wird der Fehler „Zertifikat xx enthält keinen Privatschlüssel“ angezeigt. Ein Dienstzertifikat ist fälschlicherweise als CA-Zertifikat in NSX konfiguriert. (Der private Schlüssel wird als Teil des Zertifikats hinzugefügt.) *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1973130: Verlust von Nord-Süd-Datenverkehr (N-S), wenn die Kontroll-VM des Distributed Logical Routers ein Hochverfügbarkeits-Failover durchläuft, selbst wenn eine unverankerte statische Route auf dem Edge Services Gateway installiert ist**  
Der Verlust von N-S-Datenverkehr erfolgt während eines Hochverfügbarkeits-Failovers der Kontroll-VM, selbst wenn auf dem Edge Services Gateway eine unverankerte statische Route zum Distributed Logical Router installiert ist. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1972659: NSX Edge-Schnittstelle zeigt an, dass die Datenspeicher einer einzigen DLR-Appliance-Instanz sowohl null als auch gültig sind**  
Nach dem Löschen eines der Datenspeicher zeigt NSX Edge den konfigurierten Datenspeicher als "null" an. *Problem in 6.3.5 behoben.*

- **Behobenes Problem 1983497: Violetter Bildschirm wird angezeigt, wenn gleichzeitig ein Brücken-Failover und eine Brücken-Konfigurationsänderung erfolgen**  
Wenn ein Brücken-Failover und eine Brücken-Konfigurationsänderung gleichzeitig erfolgen, kann dies zu einem Deadlock und einem violetten Bildschirm führen. Die Wahrscheinlichkeit eines Deadlocks ist gering. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1897999: Datenverkehr von VTEP schlägt bei Verwendung von LACP fehl, wenn der erste Uplink in LAG ausfällt**  
Der Datenverkehr von VTEP schlägt fehl (z. B. IP-Adresse kann bei Verwendung von DHCP nicht abgerufen werden), wenn der erste Uplink in LAG ausfällt. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1888743: IPv6-Standard-Gateway kann auf NSX Edge nicht festgelegt werden, wenn in früherer NSX-Version vorhanden; Upgrade schlägt fehl**  
Bei NSX 6.3.3 und 6.3.4 können Sie kein IPv6-Standard-Gateway erstellen. Wenn Sie ein Upgrade auf NSX 6.3.3 oder NSX 6.3.4 durchführen und ein IPv6-Standard-Gateway auf einem NSX Edge festgelegt haben, schlägt das Upgrade fehl. Die Fehlermeldung „Fehler beim Ändern des statischen IPv6-Routings“ wird angezeigt. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1935204: DLR benötigt 1 bis 1,5 Sekunden für die ARP-Auflösung**  
Wenn die ARP-Unterdrückung fehlschlägt, dauert die lokale ARP-Auflösung durch den DLR für eine VM, die auf einem Remotehost ausgeführt wird, ca. 1 bis 1,5 Sekunden. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1920574: Teilschnittstellen für ein Edge können nicht konfiguriert werden**  
Das Erstellen von Teilschnittstellen auf einem Edge ist mit NSX for vSphere 6.3.2/6.3.3 nicht möglich (Teilschnittstelle mit der IP-Adresse kann nicht veröffentlicht werden).

#### Behobene Probleme beim NSX Manager

- **Behobenes Problem 1891547: NSX Manager stellt nach mehreren Neustarts der Ereignisprotokoll-Server keine Verbindung zu den Ereignisprotokoll-Servern her**  
Ein mehrmaliger Neustart des Ereignisprotokoll-Servers führt dazu, dass der NSX Manager keine Verbindung zum Ereignisprotokoll-Server mehr herstellen kann. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1931288: NSX Manager stürzt bei hoher NSX Manager-CPU-Auslastung ab**  
NSX Manager weist einen OOM-Fehler (out of memory, nicht genügend Arbeitsspeicher) auf und wird ständig neu gestartet. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1926309: NSX Manager-Plug-In kann nicht laden und zeigt die Fehlermeldung „Authentifizierungsausnahme“ an**  
In manchen Fällen kann das NSX Manager-Plug-In keine Seiten laden und es zeigt schließlich einen Zeitüberschreitungsfehler an. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1904842: NSX Manager wird nicht beim vCenter Server oder Plattform Services Controller registriert**  
NSX Manager wird nicht auf der Benutzeroberfläche angezeigt und alle an NSX Manager gesendeten REST-Aufrufe schlagen fehl.
- **Behobenes Problem 1900144: Anforderung, bestimmte Änderungen an den SGs in die Überwachungsprotokolle aufzunehmen**  
NSX Manager kann Syslog-Nachrichten nun erfolgreich an LogInsight weiterleiten, die die Details enthalten, die auf der GUI des vSphere Web Clients angezeigt werden. *Problem in 6.3.5 behoben.*

#### Behobene Probleme bei NSX Controller

- **Behobenes Problem 1898862: Hohe Controller-CPU-Auslastung aufgrund von Hardware-VTEP**  
Benutzer beobachtet Controller mit hoher CPU-Auslastung, wobei die Verbindung zwischen Controller-ToR-Manager und Switch unterbrochen ist. Bei der Überprüfung des ToR-Agentenprotokolls enthält die Protokolldatei mehrere Zeilen der folgenden Meldungen:  
2017-05-03 17:13:18,991 | DEBUG | pool-9-thread-5 | OvssdbConnectionService | Handshake status NEED\_UNWRAP. *Problem in 6.3.5 behoben.*

- **Behobenes Problem 1898937: ESXi-Host verfügt nicht über vollständige VTEP-Listen für VNIs.**  
Dies führt zu Ost-West-Konnektivitätsproblemen.  
Eine Race Condition, die nur auftritt, wenn beim Controller-Cluster Änderungen am Sharding durchgeführt wurden und der Legacy-Master-Controller die Nachricht langsamer verarbeitet als die Sitzungsnachricht, wird beendet, wenn die Statussynchronisation für den neuen Controller-Knoten abgeschlossen ist. Dies führt zu nicht synchronisierten Änderungen zwischen den Controllern für die betroffene VNI. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1965859: Speicheranstieg von NSX Controller bei Hardware-VTEP-Konfiguration führt zu hoher CPU-Auslastung**  
Bei Hardware-VTEP-Konfigurationen, die über mehrere Tage hinweg laufen, kommt es zu einem Speicheranstieg durch den Controller-Prozess. Der Speicheranstieg führt einige Zeit (einige Minuten) lang zu einer hohen CPU-Auslastung, bis der Controller den Speicher wiederhergestellt hat. Während dieser Zeit ist der Datenpfad betroffen. *Problem in 6.3.5 behoben.*

#### Behobene Probleme bei Sicherheitsdiensten

- **Behobenes Problem 1897878: ESXi-Aufgaben und -Ereignisse führen zur Anzeige der Meldung „Kommunikation mit ESX-Modul unterbrochen“**  
Wenn das ESXi-Host-Guest Introspection-Modul (EPsec Mux) nicht mehr mit dem ESX-Modul kommunizieren kann, wird die Fehlermeldung „Kommunikation mit ESX-Modul unterbrochen“ auf den ESXi-Hosts angezeigt. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1945954: Beim Upgrade wird die verteilte Firewall auf einem Cluster mit deaktivierter verteilter Firewall automatisch aktiviert**  
Bei neu hinzugefügten Hosts in einem Cluster ist die Firewall aktiviert, was zu Unterbrechungen des Datenverkehrs führt. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1951626: Ein Benutzer mit der Rolle „Auditor“ kann die verteilte Firewall auf Clusterebene auf der Registerkarte „Hostvorbereitung“ deaktivieren**  
Ein Benutzer mit der Rolle „Auditor“ sollte auf NSX nur eine Leseberechtigung besitzen und die verteilte Firewall nicht deaktivieren können. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1944599: Übersetzte IPs werden nicht zu vNIC-Filtern hinzugefügt, und aus diesem Grund blockiert die verteilte Firewall den Datenverkehr**  
Wenn neue VMs bereitgestellt werden, werden die vNIC-Filter nicht mit dem richtigen Satz an IPs aktualisiert. Aus diesem Grund blockiert die verteilte Firewall den Datenverkehr. *Problem in 6.3.5 behoben.*
- **Behobenes Problem 1958657: Dienste werden in der Dienstgruppe auf der Firewall-Benutzeroberfläche nicht angezeigt**  
Nach dem Erstellen eines Sicherheitsdiensts mit ICMP ohne Bestimmung eines Unterprotokolls werden die Dienste auf der Firewall-Benutzeroberfläche nicht angezeigt. *Problem in 6.3.5 behoben.*

#### Installation und Upgrade

- **Behobenes Problem 1789989: Im Verlauf eines Hostcluster-Upgrades kann in der Datenebene ein Paketverlust auftreten**  
Bei einem VIB-Upgrade wird die Kennwortdatei von VSFWD (vShield Firewall Daemon), die im VIB enthalten ist, entfernt, sodass VSFWD das alte Kennwort nicht für die Herstellung einer Verbindung mit NSX Manager verwenden kann. Zuerst muss deshalb das neue Kennwort aktualisiert werden. Dieser Vorgang nimmt einige Zeit nach dem Neustart des Hosts in Anspruch. Allerdings werden in einem komplett automatisierten DRS-Cluster VMs sofort verschoben, wenn der vorbereitete Host gestartet wurde. Da der VSFWD-Vorgang zu diesem Zeitpunkt noch nicht bereit ist, besteht für eine kurze Zeit die Gefahr des Paketverlustes in der Datenebene. *Problem in 6.3.5 behoben.*

## Bekannte Probleme

Die bekannten Probleme gliedern sich in folgende Gruppen.

- [Allgemeine bekannte Probleme](#)
- [Bekannte Installations- und Upgrade-Probleme](#)
- [Bekannte Probleme bei NSX Manager](#)
- [Bekannte Probleme von NSX Controller](#)
- [Probleme bei logischen Netzwerken und NSX Edge](#)
- [Bekannte Probleme bei Sicherheitsdiensten](#)
- [Bekannte Probleme bei Überwachungsdiensten](#)

### Allgemeine bekannte Probleme

- **Problem 2003765:** Der TOR Manager auf dem NSX Controller kann kein Update senden, wenn das physische TOR-Gerät zurückgesetzt/neu gestartet bzw. aus- und wieder eingeschaltet wird. Wenn TOR neu geladen wird, fehlen virtuelle Remote-Mac-Maschinen in der TOR OVSDB-Tabelle.

Problemumgehung: Starten Sie alle NSX Controller neu. Weitere Informationen dazu enthält der VMware-Knowledgebase-Artikel [52074](#).

- **Problem 1874863:** Fehler bei der Authentifizierung mit einem geänderten Kennwort nach der Deaktivierung/Aktivierung des SSL VPN-Dienstes bei einem lokalen Authentifizierungsserver. Wenn der SSL VPN-Dienst bei Verwendung einer lokalen Authentifizierung deaktiviert und dann wieder aktiviert wurde, können sich Benutzer mit geänderten Kennwörtern nicht anmelden.

Weitere Informationen dazu enthält der [VMware-Knowledgebase-Artikel 2151236](#).

- **Problem 1702339:** Bei Schwachstellenprüfungen wird möglicherweise die Quagga-Schwachstelle „bgp\_dump\_routes“ (CVE-2016-4049) gemeldet. Bei Schwachstellenprüfungen in NSX for vSphere wird möglicherweise die Quagga-Schwachstelle „bgp\_dump\_routes“ (CVE-2016-4049) gemeldet. NSX for vSphere verwendet Quagga, doch die BGP-Funktionalität (die die Schwachstelle erkennt) ist nicht aktiviert. Diese Schwachstellenwarnung kann bedenkenlos ignoriert werden.

*Problemumgehung:* Da das Produkt nicht anfällig ist, ist keine Problemumgehung erforderlich.

- **Problem 1740625, 1749975:** Probleme der Benutzeroberfläche unter Mac OS in Firefox und Safari. Wenn Sie Firefox oder Safari unter Mac OS verwenden, funktioniert die Schaltfläche „Zurück“ in NSX Edge auf der Seite „Networking & Security“ im vSphere 6.5 Web Client nicht. Manchmal friert in Firefox die Benutzeroberfläche ein.

*Problemumgehung:* Verwenden Sie Google Chrome unter Mac OS oder klicken Sie auf die Home-Schaltfläche und fahren Sie gemäß den Anweisungen fort.

- **Problem 1700980:** Bei Sicherheitspatch CVE-2016-2775 kann ein zu langer Abfragenamen zu einem Segmentierungsfehler in „lwresd“ führen. Unter NSX 6.2.4 ist BIND 9.10.4 installiert, aber die Option „lwres“ wird in *named.conf* nicht verwendet. Daher ist das Produkt nicht anfällig.

*Problemumgehung:* Da das Produkt nicht anfällig ist, ist keine Problemumgehung erforderlich.

- **Problem 1568180:** Die Funktionsliste für NSX bei der Verwendung von vCSA 5.5 (vCenter Server Appliance) ist nicht korrekt. Sie können die Funktionen einer Lizenz im vSphere Web Client durch Auswahl der Lizenz und Klicken auf **Aktionen > Funktionen anzeigen** darstellen. Wenn Sie ein Upgrade auf NSX 6.2.3 durchführen, wird für Ihre Lizenz ein Upgrade auf eine Enterprise-Lizenz durchgeführt, mit der alle Funktionen aktiviert werden. Wenn allerdings NSX Manager mit vCSA 5.5 (vCenter Server Appliance) registriert wird, führt die Auswahl von **Funktionen anzeigen** zur Darstellung der Funktionen für die Lizenz, die vor dem Upgrade verwendet wurde, und nicht für die neue Enterprise-Lizenz.



*Problemumgehung:* Alle Enterprise-Lizenzen umfassen die gleichen Funktionen, auch wenn sie im vSphere Web Client nicht korrekt dargestellt werden. Weitere Informationen finden Sie auf der [NSX-Lizenzseite](#).

## Bekannte Installations- und Upgrade-Probleme

Bevor Sie das Upgrade durchführen, lesen Sie den Abschnitt [Upgrade-Hinweise](#) weiter oben in diesem Dokument.

- **Problem 2001988:** Während eines NSX-Hostcluster-Upgrades wechselt der Installationsstatus für den gesamten Cluster auf der Registerkarte „Hostvorbereitung“ zwischen „Nicht bereit“ und „Wird installiert“, wenn jeder Host im Cluster aktualisiert wird

Während eines NSX-Upgrades wird durch Klicken auf „Upgrade verfügbar“ ein Host-Upgrade für NSX-vorbereitete Cluster ausgelöst. Bei als „DRS FULL AUTOMATIC“ konfigurierten Clustern wechselt der Installationsstatus zwischen „Wird installiert“ und „Nicht bereit“, obwohl die Hosts im Hintergrund problemlos aktualisiert werden.

*Problemumgehung:* Dieses Problem betrifft die Benutzeroberfläche und kann ignoriert werden. Warten Sie den Fortschritt des Hostcluster-Upgrades ab.

- **Problem 1932907:** Fehler beim Aktualisieren der Guest Introspection-Dienst-VM (SVM)  
Beim Versuch, die Guest Introspection-SVM zu aktualisieren, wird der Installationsstatus „Fehlgeschlagen“ für die GI-SVM ausgegeben. Dies gilt möglicherweise für die GI-SVMs auf einem oder mehreren Hosts im Cluster.

*Problemumgehung:*

1. Löschen Sie die GI-SVM von VC.
2. Klicken Sie im Bereich der Dienstbereitstellung der GI-SVM auf **Auflösen**. Damit wird die GI-SVM erneut bereitgestellt.

- **Problem 1848058:** Upgrade von ESXi-Hosts VIBs auf NSX 6.3.2 schlägt möglicherweise fehl  
In einigen Fällen wird beim Upgrade von ESXi-Host-VIBs auf NSX 6.3.2 das ältere VIB-Verzeichnis von NSX Manager gelöscht, wodurch das Upgrade nicht durchgeführt werden kann. Durch Klicken auf die Schaltfläche „Auflösen“ kann das Problem nicht behoben werden.

*Problemumgehung:* Zur Behebung dieses Problems verwenden Sie die Upgrade-API:

```
PUT https://<nsx-mgr-ip>/api/2.0/nwfabric/configure
```

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.vxlan</featureId>
  <resourceConfig>
    <resourceId>domain-cXX</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

wobei <nsx-mgr-ip> die IP-Adresse Ihres NSX Manager ist und domain-cXX die Domänen-ID des Clusters.

- **Problem 1747217:** Vorbereitung der ESXi Hosts führt zu `muxconfig.xml.bad` und Guest Introspection funktioniert nicht ordnungsgemäß

Wenn „vmx path“ in einer der VMs in `muxconfig.xml` fehlt und MUX beim Versuch, die Konfigurationsdatei zu analysieren, die Eigenschaft „xml path“ nicht findet, wird die Konfigurationsdatei in „muxconfig.xml.bad“ umbenannt, die Fehlermeldung „Fehler – MUX-Analysekonfiguration“ an die USVM gesendet und der Konfigurationskanal geschlossen.

*Problemumgehung:* Entfernen Sie die verwaisten virtuellen Maschinen aus der vCenter-Bestandsliste.

- **Problem 1859572:** Bei der Deinstallation von NSX-VIBs der Version 6.3.x auf ESXi-Hosts, die von vCenter Version 6.0.0 verwaltet werden, verbleibt der Host im Wartungsmodus  
Wenn Sie die NSX-VIBs der Version 6.3.x auf einem Cluster deinstallieren, gehört zum Workflow

das Versetzen der Hosts in den Wartungsmodus, das Deinstallieren der VIBs und das anschließende Beenden des Wartungsmodus für die Hosts durch den EAM-Dienst. Wenn jedoch solche Hosts von vCenter Server Version 6.0.0 verwaltet werden, führt dies dazu, dass die Hosts nach der Deinstallation der VIBs im Wartungsmodus verbleiben. Der für die Deinstallation der VIBs vorgesehene EAM-Dienst versetzt die Hosts in den Wartungsmodus, ist aber nicht in der Lage, den Wartungsmodus für die Hosts wieder zu deaktivieren.

*Problemumgehung:* Beenden Sie den Wartungsmodus für die Hosts manuell. Dieses Problem tritt nicht auf, wenn Hosts mit vCenter Server Version 6.5a und höher verwaltet werden.

- **Problem 1435504: HTTP/HTTPS-Systemstatusprüfung ergibt nach dem Upgrade von 6.0.x oder 6.1.x auf 6.3.x INAKTIV mit der Fehlermeldung „Rückgabecode 127 ist außerhalb des gültigen Bereichs – Plug-In fehlt möglicherweise“**

Wenn in den Versionen NSX 6.0.x und 6.1.x die URLs ohne doppelte Anführungszeichen (""") konfiguriert wurden, konnte die Systemstatusprüfung nicht durchgeführt werden. Es wurde dann folgender Fehler angezeigt: „Rückgabecode 127 ist außerhalb des gültigen Bereichs – Plug-In fehlt möglicherweise“. Als Problemumgehung wurde das Hinzufügen doppelter Anführungszeichen (""") in der eingegebenen URL empfohlen (dies war nicht für die Felder send/receive/expect erforderlich). Dieses Problem wurde in Version 6.2.0 behoben, was allerdings dazu führt, dass bei einem Upgrade von 6.0.x oder 6.1.x auf 6.3.x die Mitglieder des Pools durch die zusätzlichen doppelten Anführungszeichen in der Systemstatusprüfung als INAKTIV angezeigt werden.

*Problemumgehung:* Entfernen Sie nach dem Upgrade die doppelten Anführungszeichen (""") im URL-Feld aus allen betroffenen Konfigurationen der Systemstatusprüfung.

- **Problem 1734245: Data Security führt zum Fehler bei Upgrades auf 6.3.0**  
Upgrades auf 6.3.0 sind nicht möglich, wenn Data Security als Teil einer Dienstrichtlinie konfiguriert ist. Stellen Sie sicher, dass vor dem Upgrade Data Security von allen Dienstrichtlinien entfernt wird.
- **Problem 1801685: Filter werden auf ESXi nach dem Upgrade von Version 6.2.x auf 6.3.0 aufgrund einer fehlgeschlagenen Verbindung mit dem Host nicht angezeigt**  
Nach dem Upgrade von NSX 6.2.x auf 6.3.0 und der Cluster-VIBs auf 6.3.0-Bits weist der „Kommunikationskanalstatus“ die Verbindung von NSX Manager zum Firewallagenten und von NSX Manager zum Steuerungskomponentenagenten als inaktiv aus, auch wenn die Installation als erfolgreich und die Firewall als aktiviert angezeigt wird. Dies führt zum Scheitern der Veröffentlichung von Firewallregeln und Sicherheitsrichtlinien, und die VXLAN-Konfiguration kann nicht zu den Hosts gesendet werden.

*Problemumgehung:* Führen Sie den API-Aufruf zur Synchronisierung des Nachrichtenbus für den Cluster mithilfe folgender API durch: POST: <https://<NSX-IP>/api/2.0/nwfabric/configure?action=synchronize>.

API-Text:

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>{Cluster-MOID}</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

- **Problem 1797929: Der Nachrichtenbuskanal ist nach einem Hostcluster-Upgrade nicht verfügbar**

Nach einem Hostcluster-Upgrade wird von vCenter 6.0 (und früher) das Ereignis „Erneut verbinden“ nicht generiert. Dies führt dazu, dass NSX Manager keine Messaging-Infrastruktur auf dem Host einrichtet. Dieses Problem wurde in vCenter 6.5 behoben.

*Problemumgehung:* Synchronisieren Sie erneut die Messaging-Infrastruktur, wie im folgenden API-Aufruf dargestellt:

POST <https://<ip>:/api/2.0/nwfabric/configure?action=synchronize>

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>host-15</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

- **Problem 1768144:** Ältere NSX Edge-Appliance-Ressourcenreservierungen, die die neuen Grenzwerte überschreiten, können zu Fehlern bei Upgrades oder erneuten Bereitstellungen führen

In NSX 6.2.4 und früher konnten beliebig große Ressourcenreservierungen für eine NSX Edge-Appliance festgelegt werden. In NSX war kein Höchstwert vorgegeben. Nach dem Upgrade des NSX Managers auf Version 6.2.5 oder höher treten bei Upgrades oder erneuten Bereitstellungen des Edge Fehler auf (wodurch ein Upgrade ausgelöst wird), wenn ein vorhandenes Edge reservierte Ressourcen (insbesondere Arbeitsspeicher) aufweist, die den neuen Höchstwert für den ausgewählten Formfaktor überschreiten. Hat ein Benutzer beispielsweise eine Arbeitsspeicherreservierung in Höhe von 1000 MB auf einem LARGE Edge vor Version 6.2.5 festgelegt und ändert die Appliance-Größe nach einem Upgrade auf Version 6.2.5 in COMPACT, so überschreitet die Arbeitsspeicherreservierung den neuen Höchstwert – in diesem Fall 512 für ein COMPACT Edge – und der Vorgang scheitert.

Unter [Upgrade von Edge Services Gateway \(ESG\)](#) erhalten Sie Informationen zur empfohlenen Ressourcenzuteilung in NSX 6.2.5.

*Problemumgehung:* Verwenden Sie die Appliance-REST-API: `PUT`

`https://<NSXManager>/api/4.0/edges/<edge-Id>/appliances/` zum erneuten Konfigurieren der Arbeitsspeicherreservierung, sodass sie innerhalb der für den Formfaktor festgelegten Werte liegt, ohne weitere Appliance-Änderungen. Nach Abschluss dieses Vorgangs können Sie die Appliance-Größe ändern.

- **Problem 1600281:** Für den USVM-Installationsstatus von Guest Introspection wird in der Registerkarte „Dienstbereitstellungen“ der Wert „Fehlgeschlagen“ angegeben  
Wenn der unterstützende Datenspeicher für eine globale Guest Introspection-SVM offline geschaltet wurde oder wenn auf diesen nicht zugegriffen werden kann, muss die USVM eventuell neu gestartet oder erneut bereitgestellt werden.

*Problemumgehung:* Starten Sie die USVM zur Wiederherstellung neu oder stellen Sie diese erneut bereit.

- **Problem 1660373:** vCenter unterbindet das Hinzufügen eines Hosts zu vSphere Distributed Switch aufgrund einer abgelaufenen NSX-Lizenz

Bei vSphere 5.5 Update 3 und vSphere 6.0.x ist vSphere Distributed Switch in der NSX-Lizenz enthalten. Allerdings blockiert vCenter das Hinzufügen von ESXi-Hosts zu einem vSphere Distributed Switch, wenn die NSX-Lizenz abgelaufen ist.

*Problemumgehung:* Ihre NSX-Lizenz muss aktiv sein, damit Sie einem vSphere Distributed Switch einen Host hinzufügen können.

- **Problem 1569010/1645525:** Beim Upgrade von 6.1.x auf NSX for vSphere 6.2.3 auf einem System, das mit vCenter 5.5 verbunden ist, wird im Feld „Produkt“ des Fensters „Lizenzschlüssel zuweisen“ die NSX-Lizenz als generischer Wert „NSX for vSphere“ und nicht als eine genauer spezifizierte Version wie z. B. „NSX for vSphere - Enterprise“ dargestellt

*Problemumgehung:* Keine.

- **Problem 1636916:** In einer vCloud Air-Umgebung werden Edge-Firewall-Regeln mit dem Wert „Alle“ des Quellprotokolls in „TCP:Alle, UDP:Alle“ geändert, wenn für die NSX Edge-Version ein Upgrade von vCNS 5.5.x auf NSX 6.x durchgeführt wurde

Als Folge davon ist der ICMP-Datenverkehr blockiert und es treten eventuell Paketverwerfungen auf.

*Problemumgehung:* Vor dem Upgrade Ihrer NSX Edge-Version erstellen Sie spezifischere Edge-Firewallregeln und ersetzen Sie „Alle“ mit bestimmten Quellportwerten.

- **Problem 1474238:** Nach dem vCenter-Upgrade kann es zu einem Verbindungsabbruch zwischen vCenter und NSX kommen.

Wenn Sie das in vCenter eingebettete SSO verwenden und Sie ein Upgrade von vCenter 5.5 auf vCenter 6.0 durchführen, wird die Verbindung von vCenter zu NSX möglicherweise getrennt. Dies geschieht, wenn vCenter 5.5 bei NSX unter Verwendung des Root-Benutzernamens registriert wurde. In NSX 6.2 ist die vCenter-Registrierung mit Root veraltet.

Hinweis: Wenn Sie externes SSO verwenden, sind keine Änderungen erforderlich. Sie können denselben Benutzernamen, z. B. „admin@mybusiness.mydomain“, beibehalten. Dann wird die vCenter-Verbindung nicht getrennt.

*Problemumgehung:* Registrieren Sie vCenter mit NSX, indem Sie den administrator@vsphere.local-Benutzernamen anstelle des Root-Benutzernamens verwenden.

- **Problem 1375794:** Herunterfahren des Gastbetriebssystems für Agent-VMs (SVA) vor dem Ausschalten

Wenn ein Host in den Wartungsmodus versetzt wird, werden alle Dienstanwendungen ausgeschaltet und nicht ordnungsgemäß heruntergefahren. Dies kann zu Fehlern innerhalb von Anwendungen von Drittanbietern führen.

*Problemumgehung:* Keine.

- **Problem 1112628:** Dienst-Appliance, die mit der Ansicht „Dienstbereitstellungen“ bereitgestellt wurde, kann nicht eingeschaltet werden

*Problemumgehung:* Bevor Sie den Vorgang fortsetzen, überprüfen Sie Folgendes:

- Die Bereitstellung der virtuellen Maschine wurde abgeschlossen.
- Es werden für die virtuelle Maschine, die im Aufgabenbereich von vCenter angezeigt wird, keine in Ausführung befindlichen Aufgaben wie z. B. Klonen, Neukonfigurieren usw. angezeigt.
- Im vCenter-Ereignisfenster der virtuellen Maschine werden die folgenden Ereignisse nach der Initiierung der Bereitstellung angezeigt:

Agent-VM <VM-Name> wurde bereitgestellt.

Markieren Sie den Agenten als verfügbar, um mit dem Agent-Workflow fortzufahren.

Löschen Sie in einem solchen Fall die virtuelle Dienstmaschine. In der Dienstbereitstellungs-Benutzeroberfläche wird die Bereitstellung als „Fehlgeschlagen“ angezeigt. Durch Klicken auf das rote Symbol wird ein Alarm wegen einer nicht verfügbaren Agent-VM für den Host angezeigt. Wenn Sie den Alarm beheben, wird die virtuelle Maschine erneut bereitgestellt und eingeschaltet.

- **Problem 1497101:** Wenn in Ihrer Umgebung nicht alle Cluster und Hosts vorbereitet sind, wird die Upgrade-Meldung für die verteilte Firewall auf der Registerkarte „Hostvorbereitung“ der Installationsseite nicht angezeigt

Wenn Sie Cluster für die Netzwerkvirtualisierung vorbereiten, ist die verteilte Firewall auf diesen Clustern aktiviert. Wenn in Ihrer Umgebung nicht alle Cluster vorbereitet sind, wird die Upgrade-Meldung für die verteilte Firewall auf der Registerkarte „Hostvorbereitung“ nicht angezeigt.

*Problemumgehung:* Verwenden Sie den folgenden REST-Aufruf, um die verteilte Firewall zu aktualisieren:

PUT <https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state>

- **Problem 1413125: SSO kann nach dem Upgrade nicht neu konfiguriert werden**  
Wenn der in NSX Manager konfigurierte SSO-Server der einzige native Server in vCenter Server ist, können Sie die SSO-Einstellungen in NSX Manager nach dem Upgrade von vCenter Server auf Version 6.0 und dem Upgrade von NSX Manager auf Version 6.x nicht neu konfigurieren.

*Problemumgehung:* Keine.

- **Problem 1263858: SSL VPN sendet keine Upgrade-Benachrichtigung an den Remote-Client**  
SSL VPN-Gateway sendet keine Upgrade-Benachrichtigung an Benutzer. Der Administrator muss Remotebenutzern manuell mitteilen, dass das SSL VPN-Gateway (Server) aktualisiert wurde, und sie bitten, ihre Clients zu aktualisieren.

*Problemumgehung:* Benutzer müssen die ältere Version des Client deinstallieren und die neueste Version manuell installieren.

- **Problem 1462319: Das VIB „esx-dvfilter-switch-security“ ist nicht mehr in der Ausgabe des Befehls „esxcli software vib list | grep esx“ vorhanden.**  
Ab NSX 6.2 sind die Module „esx-dvfilter-switch-security“ innerhalb des VIB esx-vxlan enthalten. Die einzigen NSX VIBs, die für 6.2 installiert sind, sind esx-vsip und esx-vxlan. Bei einem Upgrade von NSX auf 6.2 wird das alte VIB „esx-dvfilter-switch-security“ aus den ESXi-Hosts entfernt. Ab NSX 6.2.3 wird zusätzlich zu den NSX VIBs „esx-vsip“ und „esx-vxlan“ das dritte VIB „esx-vmapi“ bereitgestellt. Bei einer erfolgreichen Installation werden alle 3 VIBs angezeigt.

*Problemumgehung:* Keine.

- **Problem 1481083: Nach dem Upgrade können logische Router, für die explizites Failover-Teaming konfiguriert ist, Pakete möglicherweise nicht ordnungsgemäß weiterleiten**  
Wenn auf den Hosts ESXi 5.5 ausgeführt wird, unterstützt die explizite Failover-Teaming-Richtlinie für NSX 6.2 nicht mehrere aktive Uplinks auf Distributed Logical Routern.

*Problemumgehung:* Ändern Sie die explizite Failover-Teaming-Richtlinie, sodass es nur einen aktiven Uplink gibt und sich die anderen Uplinks im Standby-Modus befinden.

- **Problem 1411275: vSphere Web Client zeigt die Registerkarte „Netzwerk und Sicherheit“ nach der Sicherung und Wiederherstellung in NSX for vSphere 6.2 nicht an**  
Wenn Sie nach dem Upgrade auf NSX for vSphere 6.2 eine Sicherung und Wiederherstellung durchführen, wird die Registerkarte Netzwerk und Sicherheit im vSphere Web Client nicht angezeigt.

*Problemumgehung:* Wenn eine NSX Manager-Sicherung wiederhergestellt wird, werden Sie vom Appliance Manager abgemeldet. Warten Sie ein paar Minuten, bevor Sie sich beim vSphere Web Client anmelden.

- **Problem 1764460: Nach Abschluss der Hostvorbereitung erscheinen alle Clustermitglieder als „Bereit“, aber Clusterebene wird fälschlicherweise als „Ungültig“ angezeigt**  
Nach dem Abschluss der Host-Vorbereitung erscheinen alle Cluster-Mitglieder korrekt als „Bereit“, aber das Cluster-Level wird als „Ungültig“ angegeben. Die dafür angezeigte Ursache ist ein benötigter Host-Neustart, obwohl dieser bereits durchgeführt wurde. Dieses Problem kann zweitweise bei vSphere 5.5 und 6.0 auftreten und wurde bei vSphere 6.5 behoben.

*Problemumgehung:* Im vCenter ESX Agency Manager-MOB [https://VC\\_IP/eam/mob/](https://VC_IP/eam/mob/) können Sie auf die Ihren Hostclustern zugeordneten Agencys zugreifen. Klicken Sie auf eine der Agencys und dann auf Konfiguration, um die Cluster-Details anzuzeigen. Klicken Sie bei den betroffenen Clustern auf Alle auflösen.

- **Problem 1979457: Wenn die GI-SVM während des Upgrades im Abwärtskompatibilitätsmodus gelöscht oder entfernt wird, ist die identitätsbasierte Firewall über Guest Introspection (GI) nur dann funktionsfähig, wenn der GI-Cluster aktualisiert wird.**

Die identitätsbasierte Firewall ist nicht funktionsfähig und es werden keine Protokolle im Zusammenhang mit der identitätsbasierten Firewall angezeigt. Der identitätsbasierte Firewall-Schutz ist aufgehoben, bis der Cluster aktualisiert wird.

**Problemumgehung:** Aktualisieren Sie den Cluster, damit die neuere Version der GI-SVM auf allen Hosts ausgeführt wird.

-oder-

Aktivieren Sie den Log Scraper, damit die identitätsbasierte Firewall funktioniert.

## Bekannte Probleme bei NSX Manager

- **Problem 1892999:** Die eindeutigen Auswahlkriterien können nicht geändert werden, auch wenn keine virtuellen Maschinen an ein universelles Sicherheits-Tag angehängt sind  
Wenn eine virtuelle Maschine, die an ein universelles Sicherheits-Tag angehängt ist, gelöscht wird, bleibt ein internes Objekt für die virtuelle Maschine weiterhin mit dem universellen Sicherheits-Tag verbunden. Dies führt dazu, dass die globalen Auswahlkriterien nicht geändert werden können und eine Fehlermeldung eingeblendet wird, dass die universellen Sicherheits-Tags weiterhin mit den virtuellen Maschinen verbunden sind.

**Problemumgehung:** Löschen Sie alle universellen Sicherheits-Tags und ändern Sie die globalen Auswahlkriterien.

- **Problem 1801325:** In NSX Manager mit hoher CPU- und/oder Festplattenauslastung generierte „kritische“ Systemereignisse und Protokollmeldungen  
Bei hoher Festplattenauslastung, umfangreichen Änderungen der Auftragsdaten oder einer großen Auftragswarteschlange auf NSX Manager können ein oder mehrere der folgenden Probleme auftreten:
  - „Kritische“ Systemereignisse im vSphere Web Client
  - Hohe Festplattenauslastung auf NSX Manager für die Partition /common
  - Hohe CPU-Auslastung über einen längeren Zeitraum oder in regelmäßigen Intervallen
  - Negative Auswirkungen auf die Leistung von NSX Manager

**Problemumgehung:** Wenden Sie sich an den VMware-Kundensupport. Weitere Informationen dazu enthält der [VMware-Knowledgebase-Artikel 2147907](#).

- **Problem 1806368:** Die Wiederverwendung von Controllern eines zuvor fehlgeschlagenen primären NSX Manager, der nach einem Failover wieder zum primären NSX Manager wird, führt dazu, dass die DLR-Konfiguration nicht an alle Hosts weitergegeben wird  
Fällt in einem Cross-vCenter NSX-Setup der primäre NSX Manager aus, wird ein sekundärer NSX Manager zu einem primären heraufgestuft und ein neuer Controller-Cluster für die Verwendung mit dem neu heraufgestuften sekundären (jetzt primären) NSX Manager bereitgestellt. Wenn der primäre NSX Manager wieder in Betrieb ist, wird der sekundäre NSX Manager herabgestuft und der primäre NSX Manager wiederhergestellt. In diesem Fall wird die DLR-Konfiguration nicht auf alle Hosts übertragen, wenn Sie die vorhandenen Controller wiederverwenden, die auf diesem primären NSX Manager vor dem Failover bereitgestellt wurden. Dieses Problem tritt nicht auf, wenn Sie stattdessen einen neuen Controller-Cluster erstellen.

**Problemumgehung:** Stellen Sie einen neuen Controller-Cluster für den wiederhergestellten primären NSX Manager bereit.

- **Problem 1831131:** Verbindung vom NSX Manager zu SSO schlägt bei Authentifizierung über LocalOS-Benutzer fehl  
Verbindung vom NSX Manager zu SSO schlägt bei Authentifizierung über LocalOS-Benutzer fehl und produziert folgenden Fehler: „Verbindung zum NSX Manager konnte nicht hergestellt werden. Wenden Sie sich an den Administrator.“

**Problemumgehung:** Fügen Sie die Enterprise Admin-Rolle für `nsxmanager@localos` zusätzlich zu `nsxmanager@domain` hinzu.

- **Problem 1800820: Die Aktualisierung der UDLR-Schnittstelle auf einem sekundären NSX Manager ist nicht möglich, wenn die alte UDLR-Schnittstelle bereits aus dem System gelöscht wurde**

In einem Szenario, in dem der globale Synchronisierungsdienst (Replikator) auf dem primären NSX Manager nicht mehr funktioniert, müssen Sie die UDLR- (Universal Distributed Logical Router, globaler verteilter logischer Router) und ULS-Schnittstellen (Universal Logical Switch, globaler logischer Switch) auf dem primären NSX Manager löschen, anschließend neue Schnittstellen erstellen und diese dann auf dem sekundären NSX Manager replizieren. In diesem Fall wird die UDLR-Schnittstelle auf dem sekundären NSX Manager nicht aktualisiert, da bei der Replizierung ein neuer ULS auf dem sekundären NSX Manager erstellt wird und der UDLR nicht mit dem neuen ULS verbunden ist.

*Problemumgehung:* Stellen Sie sicher, dass der Replikator ausgeführt wird, und löschen Sie die UDLR-Schnittstelle (LIF) auf dem primären NSX Manager, der über einen neu erstellten ULS als Grundlage verfügt. Erstellen Sie dann die UDLR-Schnittstelle (LIF) mit demselben zugrunde liegenden ULS erneut.

- **Problem 1772911: Die Ausführung von NSX Manager erfolgt sehr langsam, wobei die Inanspruchnahme des Festplattenspeichers sowie die Größe der Aufgaben- und Auftrags-tabelle bei fast 100%-tiger CPU-Auslastung steigt**

Die Situation stellt sich dann folgendermaßen dar:

- Die NSX Manager-CPU-Auslastung liegt bei 100 % oder nähert sich regelmäßig der 100 %-Marke, und das Hinzufügen zusätzlicher Ressourcen zur NSX Manager-Appliance bewirkt keine Änderung.
- Mit dem Befehl `show process monitor` in der NSX Manager-Befehlszeilenschnittstelle (CLI) wird der Java-Vorgang angezeigt, der die meisten CPU-Zyklen in Anspruch nimmt.
- Der Befehl `show filesystems` in der NSX Manager-CLI zeigt an, dass das Verzeichnis `/common` einen sehr hohen Nutzungsgrad aufweist, etwa über 90 %.
- Bei einigen Änderungen der Konfiguration wird die Zeit überschritten (manche dauern über 50 Minuten), und sie werden nicht wirksam.

Weitere Informationen dazu enthält der [VMware-Knowledgebase-Artikel 2147907](#).

*Problemumgehung:* Wenden Sie sich zur Behebung dieses Problems an den VMware-Kundensupport.

- **Problem 1785142: Synchronisierungsprobleme werden auf dem primären NSX Manager verzögert angezeigt, wenn die Kommunikation zwischen dem primären und dem sekundären NSX Manager blockiert ist**

Wenn die Kommunikation zwischen dem primären und dem sekundären NSX Manager blockiert ist, werden die Synchronisierungsprobleme auf dem primären NSX Manager nicht sofort angezeigt.

*Problemumgehung:* Warten Sie ca. 20 Minuten, bis die Kommunikation wieder aufgenommen wird.

- **Problem 1786066: In einer Cross-vCenter-Installation von NSX kann die Trennung eines sekundären NSX Manager dazu führen, dass NSX Manager nicht erneut als sekundärer NSX Manager verbunden werden kann**

Wenn Sie in einer Cross-vCenter-Installation von NSX die Verbindung mit einem sekundären NSX Manager trennen, können Sie später diesen NSX Manager eventuell nicht mehr als sekundären NSX Manager erneut hinzufügen. Wenn Sie in einer solchen Situation versuchen, NSX Manager erneut als sekundären NSX Manager zu verbinden, wird NSX Manager auf der Registerkarte „Verwaltung“ des vSphere Web Client zwar als „Sekundär“ angegeben, die Verbindung zum primären NSX Manager wird aber nicht hergestellt.

*Problemumgehung:*

1. Trennen Sie den sekundären NSX Manager vom primären NSX Manager.
2. Fügen Sie den sekundären NSX Manager dem primären NSX Manager erneut hinzu.

- **Problem 1715354: Verzögerte Verfügbarkeit der REST-API**

Wenn nach dem Wechsel in den FIPS-Modus oder nach dem Beenden des FIPS-Modus der NSX Manager neu gestartet wird, dauert es eine gewisse Zeit, bis die NSX Manager-API betriebsbereit



ist. Es kann dabei der Eindruck entstehen, dass die API hängt. Dies ist aber nicht der Fall. Die fehlende Betriebsbereitschaft tritt nur auf, weil die Controller Zeit benötigen, um die Verbindung mit NSX Manager wiederherzustellen. Es wird empfohlen, zu warten, bis der NSX-API-Server betriebsbereit ist. Vergewissern Sie sich, dass alle Controller verbunden sind, bevor Sie Vorgänge ausführen.

- **Problem 1441874:** Beim Upgrade eines einzelnen NSX Manager in einer vCenter-Umgebung im verknüpften Modus wird eine Fehlermeldung ausgegeben

In einer Umgebung mit mehreren VMware vCenter-Servern, die mehrere NSX Manager umfassen, wird, wenn Sie einen oder mehrere NSX Manager unter „vSphere Web Client > Netzwerk und Sicherheit > Installation > Host-Vorbereitung“ auswählen, eine Fehlermeldung ausgegeben, die sinngemäß Folgendes besagt:

„Verbindung zum NSX Manager konnte nicht hergestellt werden. Wenden Sie sich an den Administrator.“

*Problemumgehung:* Weitere Informationen dazu enthält der [VMware-Knowledgebase-Artikel 2127061](#).

- **Problem 1696750:** Beim Zuweisen einer IPv6-Adresse zu NSX Manager über PUT API ist ein Neustart erforderlich

Beim Ändern der konfigurierten Netzwerkeinstellungen für NSX Manager via <https://{NSX Manager-P-Adresse}/api/1.0/appliance-management/system/network> ist ein Systemneustart erforderlich. Bis zum Neustart werden die alten Einstellungen angezeigt.

*Problemumgehung:* Keine.

- **Problem 1529178:** Das Hochladen eines Server-Zertifikats, das keinen allgemeinen Namen enthält, führt zur Meldung „Interner Serverfehler“.

Wenn Sie ein Server-Zertifikat ohne einen allgemeinen Namen hochladen, wird die Meldung „Interner Serverfehler“ eingeblendet.

*Problemumgehung:* Verwenden Sie ein Zertifikat, das sowohl einen SubAltName als auch einen allgemeinen Namen bzw. mindestens einen allgemeinen Namen enthält

- **Problem 1655388:** Die Benutzeroberfläche von NSX Manager 6.2.3 wird in der englischen statt in der lokalen Sprache dargestellt, wenn der IE11-/Edge-Browser im Betriebssystem Windows 10 in Japanisch, Chinesisch oder Deutsch verwendet wird.

Wenn Sie NSX Manager 6.2.3 mit dem IE11-/Edge-Browser im Betriebssystem Windows 10 in Japanisch, Chinesisch und Deutsch starten, wird die Oberfläche in englischer Sprache dargestellt.

*Problemumgehung:*

1. Starten Sie den Microsoft Registrierungs-Editor (regedit.exe) und wechseln Sie zu Computer > HKEY\_CURRENT\_USER > SOFTWARE > Microsoft > Internet Explorer > International.
2. Ändern Sie den Wert von *AcceptLanguage* in die lokale Sprache. Wenn Sie beispielsweise die Benutzeroberfläche auf Deutsch darstellen möchten, ändern Sie den Wert und setzen Sie DE an die erste Position.
3. Starten Sie den Browser neu und melden Sie sich erneut beim NSX Manager an. Die entsprechende Sprache wird dann dargestellt.

- **Problem 1435996:** Im CSV-Format aus NSX Manager exportierte Protokolldateien sind mit einem Zeitstempel (Zeitraum, nicht Datum/Uhrzeit) versehen.

Protokolldateien, die als CSV aus NSX Manager mit vSphere Web Client exportiert werden, werden mit einem Zeitstempel mit der Epochenzeit in Millisekunden versehen, anstatt mit der entsprechenden Zeit basierend auf der Zeitzone.

*Problemumgehung:* Keine.

- **Problem 1644297:** Das Hinzufügen/Löschen eines Abschnitts der verteilten Firewall auf dem primären NSX erstellt zwei gespeicherte Konfigurationen der verteilten Firewall auf dem sekundären NSX

In einem Cross-vCenter-Setup werden, wenn dem primären NSX Manager ein zusätzlicher globaler

oder lokaler Abschnitt der verteilten Firewall hinzugefügt wurde, zwei Konfigurationen der verteilten Firewall auf dem sekundären NSX Manager gespeichert. Dieses Problem beeinträchtigt zwar nicht die Funktionalität, führt aber dazu, dass die Obergrenze für gespeicherte Konfigurationen schneller erreicht wird, sodass eventuell zentrale Konfigurationen überschrieben werden.

*Problemumgehung:* Keine.

- **Problem 1477138:** Der NSX Manager-Dienst wird nicht gestartet, wenn der Hostname mehr als 64 Zeichen enthält  
Bei der Erstellung eines Zertifikats über die OpenSSL-Bibliothek darf der Hostname nicht länger als 64 Zeichen sein.
- **Problem 1437664:** Die NSX Manager-Auflistung erfolgt für die Anzeige in Web Client sehr langsam  
In vSphere 6.0-Umgebungen mit mehreren NSX Managern kann es vorkommen, dass der vSphere Web Client bis zu zwei Minuten benötigt, um die Liste der NSX Manager anzuzeigen, wenn für die Validierung des angemeldeten Benutzers eine große Anzahl von AD-Gruppen verwendet wird. Beim Versuch, die NSX Manager-Liste anzuzeigen, kann es zu einem Zeitüberschreitungsfehler in Bezug auf den Datendienst kommen. Für dieses Problem gibt es keine Umgehung. Warten Sie, bis die Liste geladen ist bzw. bis Sie erneut angemeldet sind, um die NSX Manager-Liste einsehen zu können.
- **Problem 1534606:** Die Seite der Hostvorbereitung kann nicht geladen werden  
Bei der Ausführung von vCenter im verknüpften Modus müssen alle vCenter mit einem NSX Manager derselben NSX-Version verbunden sein. Sollten die NSX-Versionen nicht übereinstimmen, kann der vSphere Web Client nur mit dem NSX Manager kommunizieren, der die höhere NSX-Version ausführt. Es erscheint eine Fehlermeldung etwa in der Form „Konnte keine Verbindung zum NSX Manager herstellen. Wenden Sie sich an den Administrator“ auf der Registerkarte „Hostvorbereitung“.  
*Problemumgehung:* Es wird empfohlen, für alle NSX Manager ein Upgrade auf dieselbe NSX-Softwareversion durchzuführen.
- **Problem 1027066:** vMotion von NSX Manager zeigt möglicherweise die folgende Fehlermeldung an: „Die virtuelle Ethernet-Karte 'Netzwerkadapter 1' wird nicht unterstützt“  
Sie können diesen Fehler ignorieren. Das Netzwerk funktioniert nach vMotion ordnungsgemäß.
- **Problem 1460766:** Die NSX Manager-Benutzeroberfläche wird nach dem Ändern des Kennworts über die NSX-Befehlszeilenschnittstelle nicht automatisch abgemeldet  
Wenn Sie bei NSX Manager angemeldet sind und Ihr Kennwort über die CLI kürzlich geändert haben, können Sie mit Ihrem alten Kennwort an der NSX Manager-CLI angemeldet bleiben. Normalerweise sollten Sie vom NSX Manager-Client bei einer Zeitüberschreitung der Sitzung nach Inaktivität automatisch abgemeldet werden.  
*Problemumgehung:* Melden Sie sich bei der NSX Manager-Benutzeroberfläche ab und mit dem neuen Kennwort wieder an.
- **Problem 1966681:** Falsche Meldung von doppelter NSX Manager-IP  
Die Protokolldatei wird mit der doppelten NSX Manager-IP geflutet und die falschen Informationen über die doppelte IP im Netzwerk werden gemeldet.
- **Problem 1467382:** Hostname des Netzwerks kann nicht bearbeitet werden  
Nachdem Sie sich bei der virtuellen NSX Manager-Appliance angemeldet haben und zu Appliance Management navigiert sind, auf die Einstellungen „Appliance verwalten“ und dann auf „Netzwerk“ unter „Einstellungen“ geklickt haben, um den Hostnamen des Netzwerks zu verwalten, erhalten Sie möglicherweise einen Fehler in Bezug auf eine ungültige Domänennamenliste. Dies geschieht, wenn die im Feld „Suchdomänen“ angegebenen Domänennamen durch Leerraumzeichen anstatt durch Kommas getrennt sind. NSX Manager akzeptiert nur Domänennamen, die durch Kommas getrennt sind.

*Problemumgehung:*

1. Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
2. Klicken Sie unter Appliance-Verwaltung auf Appliance-Einstellungen verwalten.

3. Klicken Sie im Fensterbereich „Einstellungen“ auf **Netzwerk**.

4. Klicken Sie auf **Bearbeiten** neben DNS-Server.

5. Ersetzen Sie im Feld „Suchdomänen“ alle Leerraumzeichen durch Kommas.

6. Klicken Sie auf **OK**, um die Änderungen zu speichern.

- **Problem 1486193/1436953: Falsches Systemereignis wird generiert, selbst nach der erfolgreichen Wiederherstellung von NSX Manager aus einer Sicherung**

Nach der erfolgreichen Wiederherstellung des NSX Manager über eine Sicherung werden die folgenden Systemereignisse im vSphere Web Client angezeigt, wenn Sie zu **Networking & Security: NSX Manager: Überwachen: Systemereignisse** navigieren.

- Das Wiederherstellen von NSX Manager aus der Sicherung ist fehlgeschlagen (mit Schweregrad „Kritisch“).

- Das Wiederherstellen von NSX Manager wurde erfolgreich abgeschlossen (mit Schweregrad „Zur Information“).

*Problemumgehung:* Wenn die abschließende Systemereignisnachricht als erfolgreich angezeigt wird, können Sie die vom System generierten Ereignisnachrichten ignorieren.

- **Problem 1783528: Die CPU-Nutzung von NSX Manager steigt freitagnachts/samstagsmorgens stark an**

NSX fragt LDAP freitagnachts ab, um eine volle Synchronisierung durchzuführen. Es gibt keine Option zum Konfigurieren einer bestimmten Active Directory-Organisationseinheit oder eines bestimmten Containers. Deshalb ruft NSX alle Objekte ab, die mit der angegebenen Domäne in Zusammenhang stehen.

*Problemumgehung:* Erhöhen Sie die vCPU beim NSX Manager von 4 auf 6

*Problemumgehung:* Erhöhen Sie die vCPU beim NSX Manager von 4 auf 6

## **Bekannte Probleme von NSX Controller**

- **Problem 1856465: Wenn ein ESXi-Host auf einer Site in einer NSX Cross-vCenter-Umgebung ausgefallen ist, wird der CDO-Modus auf dieser Site nicht aktiviert**

Wenn ein ESXi-Host auf einer Site ausgefallen ist, wird der CDO-Modus auf dieser Site nicht vollständig deaktiviert oder aktiviert.

Wenn der Host auf einer sekundären Site ausgefallen ist, kann der Vorgang im CDO-Modus auf der primären Site erfolgreich ausgeführt werden. Der Vorgang im CDO-Modus auf der sekundären Site schlägt jedoch fehl. Dies kann zu einem inkonsistenten Verhalten führen.

*Problemumgehung:* Dieses Problem hat Auswirkungen in NSX 6.3.0 und höher.

- Stellen Sie sicher, dass alle ESXi-Hosts verfügbar sind, bevor Sie einen Vorgang im CDO-Modus durchführen.
- Für eine Wiederherstellung von einem inkonsistenten Zustand entfernen Sie den Host aus der vCenter-Bestandsliste und fügen Sie ihn erneut hinzu.

## **Probleme bei logischen Netzwerken und NSX Edge**

- **Problem 1904612: Layer 2 VPN-Tunnel zeigt „Aktiv“ auf dem L2VPN-Server an, wenn der Client ausgeschaltet ist**

Bei der Erstellung eines L2-VPN zwischen zwei NSX Edges und anschließendem Ausschalten des Client-NSX Edge wird im Server-NSX Edge weiterhin angezeigt, dass der VPN-Tunnel aktiv ist.

*Problemumgehung:* Keine.

- **Problem 1242207: Änderungen an der Router-ID während der Laufzeit werden in der OSPF-Topologie nicht wiedergegeben**

Wenn Sie versuchen, die Router-ID zu ändern, ohne OSPF zu deaktivieren, werden die neuen externen Verbindungsstatus-Ankündigungen (link-state advertisements, LSAs) mit dieser Router-ID nicht neu generiert, was zu einem Verlust von externen OSPF-Routen führt.

Deaktivieren Sie OSPF, ändern Sie die Router-ID und aktivieren Sie dann OSPF erneut.

- **Problem 1894277: PSK für IPSec-Site-Konfiguration wird nicht beibehalten, wenn das lokale Subnetz oder Peer-Subnetz geändert wird**

Wenn der maskierte PSK in der Datenbank gespeichert wird, wird aufgrund einer Nichtübereinstimmung der Kennwörter kein Tunnel zwischen den Peers aufgebaut.

*Problemumgehung:* Konfigurieren Sie die IPSec-Konfiguration mit einem gültigen Kennwort neu.

- **Problem 1492497: NSX Edge-DHCP-Datenverkehr kann nicht gefiltert werden**  
Sie können auf den DHCP-Netzwerkdatenverkehr auf einem NSX Edge keine Firewallfilter anwenden, da der DHCP-Server auf einem NSX Edge RAW-Sockets verwendet, die den TCP/IP-Stack umgehen.

*Problemumgehung:* Keine.

- **Problem 1781438: Auf den ESG- oder DLR-NSX Edge-Appliances zeigt der Routing-Dienst keine Fehlermeldungen an, wenn das BGP-Pfadattribut MULTI\_EXIT\_DISC mehr als einmal empfangen wird**  
Der Edge-Router oder der Distributed Logical Router zeigt keine Fehlermeldung an, wenn er mehr als einmal das BGP-Pfadattribut MULTI\_EXIT\_DISC empfängt. Gemäß RFC 4271 [Abschnitt 5] darf das gleiche Attribut (d. h. Attribute gleichen Typs) nur einmal im Feld „Pfadattribute“ einer bestimmten UPDATE-Meldung enthalten sein.

*Problemumgehung:* Keine.

- **Problem 1786515: Benutzer mit Sicherheitsadministratorrechten können die Load Balancer-Konfiguration nicht über die Benutzeroberfläche von vSphere Web Client bearbeiten**  
Ein Benutzer mit den Rechten eines Sicherheitsadministrators für ein bestimmtes NSX Edge kann die globale Load-Balancer-Konfiguration für dieses Edge nicht mit der Benutzeroberfläche von vSphere Web Client bearbeiten. Die folgende Fehlermeldung wird angezeigt: „Der Benutzer ist nicht berechtigt, auf das Objekt ‚Global‘ und die Funktion si.service zuzugreifen. Überprüfen Sie den Geltungsbereich für den Objektzugriff und die Funktionsberechtigungen für den Benutzer.“

*Problemumgehung:* Keine.

- **Problem 1849042/1849043: Das Administratorkonto wird gesperrt, wenn der Ablauf von Kennwörtern auf der NSX Edge-Appliance konfiguriert ist**  
Wenn für den Admin-Benutzer auf der NSX Edge-Appliance der Ablauf von Kennwörtern konfiguriert ist, wird der Benutzer nach dem Ablauf des Kennworts in einem Zeitraum von sieben Tagen zur Änderung des Kennworts aufgefordert, wenn er sich bei der Appliance anmeldet. Kommt es beim Ändern des Kennworts zu Fehlern, wird das Konto gesperrt. Wenn darüber hinaus das Kennwort zum Zeitpunkt der Anmeldung an der CLI-Eingabeaufforderung geändert wird, erfüllt das neue Kennwort eventuell nicht die Richtlinie für sichere Kennwörter, die von der Benutzeroberfläche und REST erzwungen wird.

*Problemumgehung:* Um dieses Problem zu vermeiden, müssen Sie das Administratorkennwort immer mit der Benutzeroberfläche oder der REST-API ändern, bevor das vorhandene Kennwort abläuft. Wenn das Konto gesperrt ist, können Sie mit der Benutzeroberfläche oder der REST-API auch ein neues Kennwort konfigurieren. Das Konto wird dann wieder entsperrt.

- **Problem 1711013: Synchronisierung der FIB zwischen aktivem und Standby-NSX Edge nach dem Neustart der Standby-VM dauert 15 Minuten**  
Wenn ein Standby-NSX Edge ausgeschaltet ist, wird die TCP-Sitzung zwischen dem aktiven und dem Standby-Modus nicht geschlossen. Das aktive Edge erkennt, dass der Standby-Modus nach dem Keepalive (KA-)Ausfall inaktiv ist (15 Minuten lang). Nach 15 Minuten wird eine neue Socket-

Verbindung mit dem Standby-Edge hergestellt, und die FIB wird zwischen dem aktivem Edge und dem Standby-Edge synchronisiert.

*Problemumgehung:* Keine.

- **Problem 1733282: NSX Edge unterstützt keine statischen Geräterouten mehr**  
NSX Edge unterstützt keine Konfiguration statischer Routen mit NULL-Nexthop-Adresse.

*Problemumgehung:* Keine.

- **Problem 1860583: Verwendung von Remote-Syslog-Servern als FQDN kann das Routing beeinträchtigen, wenn DNS nicht erreichbar ist**  
Wenn auf einem NSX Edge Remote-Syslog-Server mithilfe des FQDN konfiguriert sind und DNS nicht erreichbar ist, können davon die Routing-Funktionen beeinträchtigt werden. Das Problem tritt eventuell nur sporadisch auf.

*Problemumgehung:* Es wird empfohlen, IP-Adressen anstelle des FQDN zu verwenden.

- **Problem 1850773: NSX Edge NAT meldet eine ungültige Konfiguration, wenn in der Load-Balancer-Konfiguration mehrere Ports verwendet werden**  
Dieses Problem tritt jedes Mal auf, wenn Sie einen virtuellen Load-Balancer-Server mit mehr als einem Port konfigurieren. Die NAT kann bei einer solchen Konfiguration des betroffenen NSX Edge nicht mehr verwendet werden.

*Problemumgehung:* Weitere Informationen und die Problemumgehung finden Sie im [VMware-Knowledgebase-Artikel 2149942](#).

- **Problem 1764258: Der Datenverkehr geht nach einem Hochverfügbarkeits-Failover oder nach einer erzwungenen Synchronisierung auf einem NSX Edge, das mit einer Teilschnittstelle konfiguriert ist, bis zu acht Minuten verloren**  
Wenn ein Hochverfügbarkeits-Failover ausgelöst oder eine erzwungene Synchronisierung über eine Teilschnittstelle gestartet wird, geht der Datenverkehr bis zu acht Minuten lang verloren.

*Problemumgehung:* Verwenden Sie für die Hochverfügbarkeit keine Teilschnittstellen.

- **Problem 1767135: Fehler beim Versuch, auf Zertifikate und Anwendungsprofile unter Load Balancer zuzugreifen**  
Benutzer mit Security-Administrator-Rechten und Edge-Geltungsbereich können bei Verwendung des Load Balancer nicht auf Zertifikate und Anwendungsprofile zugreifen. Im vSphere Web Client werden entsprechende Fehlermeldungen angezeigt.

*Problemumgehung:* Keine.

- **Problem 1792548: NSX Controller bleibt möglicherweise mit folgender Meldung hängen: „Warten auf Verknüpfung mit Cluster“**  
NSX Controller bleibt möglicherweise mit folgender Meldung hängen: „Warten auf Verknüpfung mit Cluster“ (CLI-Befehl: `show control-cluster status`). Dieses Problem tritt auf, wenn bei der Aktivierung des Controllers für die Schnittstellen `eth0` und `breth0` dieselbe IP-Adresse konfiguriert wurde. Sie können dies mithilfe des folgenden CLI-Befehls auf dem Controller überprüfen: `show network interface`

*Problemumgehung:* Wenden Sie sich an den VMware-Kundensupport.

- **Problem 1747978: OSPF-Nachbarschaften werden mit der MD5-Authentifizierung nach einem NSX Edge-HA-Failover gelöscht**  
Wenn in einer NSX for vSphere 6.2.4-Umgebung NSX Edge für eine Hochverfügbarkeit mit OSPF ein ordnungsgemäßer Neustart konfiguriert ist und MD5 für die Authentifizierung verwendet wird, kann OSPF nicht ordnungsgemäß neu starten. Es werden nur dann Nachbarschaften gebildet, wenn der Lebensdauer-Timer auf den OSPF-Nachbarschaftsknoten abgelaufen ist.

*Problemumgehung:* Keine

- **Problem 1804116:** Der logische Router meldet einen fehlerhaften Status auf einem Host, für den keine Kommunikation mit NSX Manager möglich ist

Wenn ein logischer Router auf einem Host eingeschaltet oder erneut bereitgestellt wird, der nicht mit NSX Manager kommunizieren kann (aufgrund eines NSX-VIB-Upgrade-/Installationsfehlers oder eines Hostkommunikationsproblems), meldet der logische Router einen fehlerhaften Status, und die fortlaufende automatische Wiederherstellung über eine erzwungene Synchronisierung kann nicht durchgeführt werden.

*Problemumgehung:* Nach der Behebung des Kommunikationsproblems zwischen dem Host und NSX Manager starten Sie das NSX Edge manuell neu und warten Sie, bis alle Schnittstellen aktiv sind. Diese Problemumgehung wird nur für logische Router und nicht für das NSX Edge Services Gateway (ESG) benötigt, da die automatische Wiederherstellung über eine erzwungene Synchronisierung das NSX Edge neu startet.

- **Problem 1783065:** Bei Load Balancer ist die gemeinsame Konfiguration von UDP-Port und TCP über IPv4- und IPv6-Adressen nicht möglich

UDP unterstützt nur IPv4-IPv4, IPv6-IPv6 (Frontend-Backend). NSX Manager enthält einen Fehler. Auch wenn die IPv6-Link-Local-Adresse gelesen und als eine IP-Adresse des Gruppierungsobjekts übertragen wird, können Sie das IP-Protokoll nicht für die LB-Konfiguration verwenden.

Im Folgenden finden Sie eine beispielhafte LB-Konfiguration, die das Problem veranschaulicht:

In der Load-Balancer-Konfiguration wird der Pool „vCloud\_Connector“ mit einem Gruppierungsobjekt (vm-2681) als Poolmitglied konfiguriert. Dieses Objekt enthält sowohl IPv4- als auch IPv6-Adressen. Dies wird von der LB-L4-Engine nicht unterstützt.

```
{
    "algorithm" : {
        ...
    },
    "members" : [
        {
            ... ,
            ...
        }
    ],
    "applicationRules" : [],
    "name" : "vCloud_Connector",
    "transparent" : {
        "enable" : false
    }
}

{
    "value" : [
        "fe80::250:56ff:feb0:d6c9",
        "10.204.252.220"
    ],
    "id" : "vm-2681"
}
```

*Problemumgehung:*

- Option 1: Geben Sie unter „Poolmitglied“ die IP-Adresse des Poolmitglieds statt der Gruppierungsobjekte ein.
- Option 2: Verwenden Sie keine IPv6-Adressen in den VMs.
- **Problem 1777792:** Wenn für den Peer-Endpoint „BELIEBIG“ festgelegt wurde, kann keine

## **IPSec-Verbindung hergestellt werden**

Wenn in der IPSec-Konfiguration für NSX Edge der Remote-Peer-Endpoint auf „BELIEBIG“ festgelegt wurde, verhält sich das Edge wie ein IPSec-„Server“ und wartet auf Remote-Peers zur Initiierung von Verbindungen. Wenn allerdings der Initiator eine Anforderung zur Authentifizierung mithilfe von PSK+XAUTH sendet, wird von Edge folgende Fehlermeldung angezeigt:  
„Ursprüngliche Nachricht des Hauptmodus wurde unter XXX.XXX.XX.XX:500 empfangen, aber es wurde keine Verbindung mit der Richtlinie PSK+XAUTH autorisiert“. IPSec kann dann nicht eingerichtet werden.

*Problemumgehung:* Verwenden Sie in der IPSec-VPN-Konfiguration anstelle von „BELIEBIG“ eine ganz bestimmte IP-Adresse oder einen FQDN für den Peer-Endpoint.

- **Problem 1741158: Erstellen eines neuen, nicht konfigurierten NSX Edge und Anwenden der Konfiguration kann zu vorzeitiger Aktivierung des Edge-Dienstes führen**  
Wenn Sie die NSX API verwenden, um einen neuen, nicht konfigurierten NSX Edge zu erstellen, dann einen API-Aufruf durchführen, um einen der Edge-Dienste auf diesem Edge zu deaktivieren (also beispielsweise für „dhcp-enabled“ „false“ festlegen) und schließlich die Konfigurationsänderungen auf den deaktivierten Edge-Dienst anwenden, wird dieser umgehend aktiviert.

*Problemumgehung:* Nachdem Sie eine Konfigurationsänderung an einem Edge-Dienst vornehmen, der deaktiviert bleiben soll, führen Sie sofort einen PUT-Aufruf durch, um das Aktivierungs-Flag für diesen Dienst auf „false“ festzulegen.

- **Problem 1758500: Statische Route mit mehreren nächsten Hops wird nicht in NSX Edge-Routing- und -Weiterleitungstabellen installiert, wenn es sich bei mindestens einem der nächsten konfigurierten Hops um die vNIC-IP-Adresse des Edge handelt**  
Bei ECMP und mehreren Nächster-Hop-Adressen kann unter NSX die vNIC-IP-Adresse des Edge als nächster Hop konfiguriert werden, wenn zumindest eine der Nächster-Hop-IP-Adressen gültig ist. Dies wird ohne Fehlermeldungen und Warnungen zugelassen, aber die Netzwerkroute wird aus der Tabelle zum Edge-Routing/-Weiterleiten entfernt.

*Problemumgehung:* Konfigurieren Sie die vNIC-IP-Adresse des Edge nicht als nächsten Hop in der statischen Route, wenn Sie ECMP verwenden.

- **Problem 1716464: NSX-Load Balancer führt keine Weiterleitung zu VMs durch, die kürzlich mit einem Sicherheits-Tag versehen wurden.**  
Wenn wir zwei VMs mit einem bestimmten Tag bereitstellen und anschließend einen LB für die Weiterleitung zu dem entsprechenden Tag konfigurieren, führt der LB die Weiterleitung zu diesen beiden VMs erfolgreich durch. Falls wir jedoch eine dritte VM mit dem entsprechenden Tag bereitstellen, führt der LB die Weiterleitung nur zu den ersten beiden VMs durch.

*Problemumgehung:* Klicken Sie im LB-Pool auf „Speichern“. Dadurch werden die VMs neu geprüft und das Routing zu den neu gekennzeichneten VMs wird gestartet.

- **Problem 1753621: Wenn ein Edge mit einem privaten lokalen AS Weiterleitungen an EBGPeers sendet, werden sämtliche private AS-Pfade aus den gesendeten BGP-Routing-Aktualisierungen gelöscht.**  
NSX weist derzeit eine Beschränkung auf, die verhindert, dass der vollständige AS-Pfad für eBGP-Nachbarn freigegeben wird, wenn der AS-Pfad nur private AS-Pfade enthält. Auch wenn dies in den meisten Fällen das gewünschte Verhalten ist, gibt es Fälle, in denen der Administrator möglicherweise private AS-Pfade für einen eBGP-Nachbarn freigeben möchte.

*Problemumgehung:* Es ist keine Umgehung verfügbar, bei der der Edge alle AS-Pfade in der BGP-Aktualisierung ankündigt.

- **Problem 1461421: In der Ausgabe des Befehls „show ip bgp neighbor“ für NSX Edge wird die bisherige Anzahl an zuvor eingerichteten Verbindungen beibehalten**



Mit dem Befehl „show ip bgp neighbor“ wird angezeigt, wie oft für einen bestimmten Peer die Maschine mit dem Status „BGP“ in den Status „Eingerichtet“ übergegangen ist. Die Änderung des Kennworts einer MD5-Authentifizierung führt dazu, dass die Peer-Verbindung aufgehoben und dann erneut erstellt wird, wodurch die Zählung gelöscht wird. Dieses Problem tritt nicht mit einem Edge-DLR auf.

*Problemumgehung:* Zum Löschen der Zählung führen Sie den Befehl „clear ip bgp neighbor“ aus.

- **Problem 1656713:** Auf dem NSX Edge sind nach einem HA-Failover keine IPSec-Sicherheitsrichtlinien vorhanden. Der Datenverkehr kann nicht über den Tunnel geleitet werden.

Ein Switchover mithilfe von Standby > Aktiv ist für den über IPSec-Tunnel verlaufenden Datenverkehr nicht möglich.

*Problemumgehung:* Deaktivieren/aktivieren Sie IPSec nach dem NSX Edge-Switchover.

- **Problem 1354824:** Wenn eine Edge-VM beschädigt ist oder aus anderen Gründen wie z. B. wegen eines Stromausfalls nicht erreicht werden kann, werden Systemereignisse generiert, wenn die Systemstatusprüfung von NSX Manager scheitert  
Die Registerkarte „Systemereignisse“ zeigt Ereignisse zum Status „Edge Unreachability“ (Edge nicht erreichbar) an. In der NSX Edges-Liste wird aber möglicherweise weiterhin der Status „Bereitgestellt“ dargestellt.

*Problemumgehung:* Rufen Sie mit der folgenden API detaillierte Statusinformationen zu einem NSX Edge ab:

```
GET https://NSX-Manager-IP-Address/api/4.0/edges/edgeId/status?detailedStatus=true
```

- **Problem 1647657:** Show-Befehle auf einem ESXi-Host mit DLR (Distributed Logical Router) zeigen maximal 2000 Routen pro DLR-Instanz an

Show-Befehle auf einem ESXi-Host mit aktiviertem DLR stellen maximal 2000 Routen pro DLR-Instanz dar, auch wenn mehr Routen ausgeführt werden. Dabei handelt es sich aber nur um ein Anzeigeproblem, d. h. der Datenpfad ist für alle Routen wie vorgesehen funktionsfähig.

*Problemumgehung:* Keine.

- **Problem 1634215:** Die Ausgabe von OSPF CLI-Befehlen gibt nicht wieder, ob das Routing deaktiviert ist.  
Wenn OSPF deaktiviert ist, wird in der Ausgabe der CLI-Routing-Befehle nicht *"OSPF is disabled"* angezeigt. Die Ausgabe ist leer.

*Problemumgehung:* Der Befehl *show ip ospf* stellt den korrekten Status dar.

- **Problem 1647739:** Durch die erneute Bereitstellung einer Edge-VM nach einem vMotion-Vorgang wird das Edge oder die DLR-VM wieder im ursprünglichen Cluster platziert  
*Problemumgehung:* Um die Edge-VM in einem anderen Ressourcenpool oder in einem anderen Cluster zu platzieren, konfigurieren Sie mithilfe der NSX Manager-Benutzeroberfläche den gewünschten Speicherort.
- **Problem 1463856:** Wenn die NSX Edge-Firewall aktiviert ist, werden vorhandene TCP-Verbindungen blockiert  
TCP-Verbindungen werden über die statusorientierte Edge-Firewall blockiert, wenn der anfängliche Drei-Wege-Handshake nicht erkannt wird.

*Problemumgehung:* Gehen Sie wie folgt vor, um solche vorhandenen Flows zu steuern. Aktivieren Sie das Flag „tcpPickOngoingConnections“ in der globalen Firewall-Konfiguration mithilfe der NSX-REST-API. Dies schaltet die Firewall vom strikten Modus in den toleranten Modus um. Aktivieren Sie dann die Firewall. Nachdem die vorhandenen Verbindungen hergestellt wurden (möglicherweise erst einige Minuten nach der Aktivierung der Firewall), können Sie das Flag „tcpPickOngoingConnections“ wieder deaktivieren, um die Firewall zurück in den strikten Modus zu versetzen. (Diese Einstellung ist dauerhaft.)

```
PUT /api/4.0/edges/{edgeId}/firewall/config/global
```

```
<globalConfig>
```

```
<tcpPickOngoingConnections>true</tcpPickOngoingConnections>
```

```
</globalConfig>
```

- **Problem 1374523: Erforderlicher Neustart von ESXi oder erforderliche Ausführung von `[services.sh restart]` nach der Installation von VXLAN VIB, um die VXLAN-Befehle mit `esxcli` verfügbar zu machen**

Nach der Installation von VXLAN VIB müssen Sie ESXi neu starten oder den Befehl `[services.sh restart]` ausführen, damit die VXLAN-Befehle mit `esxcli` verfügbar sind.

*Problemumgehung:* Verwenden Sie anstelle von `esxcli` den Befehl `localcli`.

- **Problem 1525003: Die Wiederherstellung einer NSX Manager-Sicherung mit einer fehlerhaften Passphrase scheitert ohne Rückmeldung, da auf zentrale Stammordner nicht zugegriffen werden kann**

*Problemumgehung:* Keine.

- **Problem 1637639: Wenn der Windows 8 SSL VPN PHAT-Client verwendet wird, wird die virtuelle IP vom IP-Pool nicht zugewiesen**

Unter Windows 8 wird die virtuelle IP-Adresse nicht wie vorgesehen vom IP-Pool zugewiesen, wenn eine neue IP-Adresse vom Edge Services Gateway zugewiesen wurde oder wenn sich der IP-Pool ändert und einen anderen IP-Bereich verwendet.

*Problemumgehung:* Dieses Problem tritt nur unter Windows 8 auf. Um dieses Problems zu vermeiden, verwenden Sie ein anderes Windows-Betriebssystem.

- **Problem 1628220: Beobachtungen der verteilten Firewall und von NetX werden auf der Empfängerseite nicht angezeigt**

Traceflow zeigt eventuell keine Beobachtungen der verteilten Firewall und von NetX auf der Empfängerseite an, wenn der mit der Ziel-vNIC verbundene Switchport geändert wird. Dieses Problem wird für vSphere 5.5-Versionen nicht behoben. Bei vSphere 6.0 und höher tritt dieses Problem nicht auf.

*Problemumgehung:* vNIC muss aktiviert bleiben. Starten Sie die VM neu.

- **Problem 1483426: Der Dienststatus für IPSec und L2 VPN wird als ausgeschaltet angezeigt, auch wenn der Dienst nicht aktiviert ist**

In der Registerkarte „Einstellungen“ der Benutzeroberfläche wird der L2-Dienststatus als nicht aktiviert angezeigt. Die API hingegen zeigt den L2-Status als aktiviert an. Der L2 VPN- und IPSec-Dienst wird in der Registerkarte „Einstellungen“ immer als ausgeschaltet angezeigt, bis die Seite der Benutzeroberfläche aktualisiert wird.

*Problemumgehung:* Aktualisieren Sie die Seite.

- **Problem 1446327: Einige TCP-basierten Anwendungen überschreiten möglicherweise den zulässigen Zeitraum, wenn sie eine Verbindung über NSX Edge herstellen**

Der Zeitüberschreitungswert für die Inaktivität bei hergestellten TCP-Verbindungen beträgt standardmäßig 3.600 Sekunden. NSX Edge löscht jede Verbindung, die länger im Leerlauf ist, als es der Zeitüberschreitungswert für eine Inaktivität erlaubt, und trennt diese Verbindungen.

*Problemumgehung:*

1. Wenn sich die Anwendung eine relativ lange Zeit im Leerlauf befindet, aktivieren Sie die

TCP-„KeepAlives“ auf dem Host mit einem „KeepAlive“-Intervall mit weniger als 3.600 Sekunden.

2. Erhöhen Sie den Edge TCP-Zeitüberschreitungswert für die Inaktivität mithilfe der folgenden NSX-REST-API auf über zwei Stunden. So können Sie den Zeitüberschreitungswert zum Beispiel auf 9.000 Sekunden erhöhen. NSX-API-URL:

```
/api/4.0/edges/{edgeId}/systemcontrol/config PUT Method <systemControl>  
<property>sysctl.net.netfilter.nf_conntrack_tcp_timeout_established=9000</p  
roperty> </systemControl>
```

- **Problem 1089238: OSPF kann nur für einen DLR Edge-Uplink konfiguriert werden**

Es ist aktuell nicht möglich, OSPF für mehr als einen der DLR Edge-Uplinks zu konfigurieren. Diese Beschränkung ist die Folge davon, dass sich die DLR-Instanzen eine einzige Weiterleitungsadresse teilen.

*Problemumgehung:* Es handelt sich hier um eine aktuelle Systembeschränkung, für die keine Problemumgehung verfügbar ist.

- **Problem 1499978: Edge-Syslog-Meldungen erreichen den Remote-Syslog-Server nicht**  
Unmittelbar nach der Bereitstellung kann der Edge-Syslog-Server die Hostnamen für alle konfigurierten Remote-Syslog-Server nicht auflösen.

*Problemumgehung:* Konfigurieren Sie Remote-Syslog-Server unter Verwendung der entsprechenden IP-Adressen oder verwenden Sie die Benutzeroberfläche, um die Edge-Synchronisierung zu erzwingen.

- **Problem 1489829: Die Einstellungen für die Konfiguration des DNS-Clients für logische Router werden nach dem Update der REST-Edge-API nicht vollständig angewendet**

*Problemumgehung:* Wenn Sie die REST-API zum Konfigurieren der DNS-Weiterleitung (Auflöser) verwenden, führen Sie die folgenden Schritte durch:

1. Geben Sie die Einstellungen für den DNS Client XML-Server so an, dass diese der Einstellung der DNS-Weiterleitung entsprechen.
2. Aktivieren Sie die DNS-Weiterleitung und stellen Sie sicher, dass die Einstellungen für die Weiterleitung den Einstellungen für den DNS-Client-Server entsprechen, die in der XML-Konfiguration angegeben sind.

- **Problem 1243112: Validierung und Fehlermeldung für ungültigen nächsten Hop in statischer Route nicht vorhanden, ECMP-aktiviert**

Beim Versuch, eine statische Route hinzuzufügen, wenn ECMP aktiviert ist, wird keine Fehlermeldung angezeigt und die statische Route nicht installiert, wenn die Routing-Tabelle keine Standardroute enthält und es einen nicht erreichbaren nächsten Hop in der Konfiguration der statischen Route gibt.

*Problemumgehung:* Keine.

- **Problem 1281425: Wenn eine NSX Edge-VM mit einer Teilschnittstelle, die durch einen logischen Switch gesichert ist, über die Benutzeroberfläche von vCenter Web Client gelöscht wird, funktioniert der Datenpfad eventuell nicht für eine neue virtuelle Maschine, die mit demselben Port verbunden ist**

Wenn die Edge-VM über die Benutzeroberfläche von vCenter Web Client (und nicht über NSX Manager) gelöscht wird, wird der auf dvPort über einem opaken Kanal konfigurierte VXLAN-Trunk nicht zurückgesetzt. Die Trunk-Konfiguration wird nämlich von NSX Manager verwaltet.

*Problemumgehung:* Löschen Sie die VXLAN-Trunk-Konfiguration wie folgt manuell:

1. Wechseln Sie zum vCenter-MOB (Managed Object Browser), indem Sie Folgendes in einem Browserfenster eingeben:  
`https://<vc-ip>/mob?vmodl=1`
2. Klicken Sie auf **Inhalt**.
3. Rufen Sie den dvsUuid-Wert wie folgt ab:
  - a. Klicken Sie auf den Root-Ordner-Link (zum Beispiel „group-d1(Datacenters)“).
  - b. Klicken Sie auf den Datacenternamen-Link (zum Beispiel „datacenter-1“).

- c. Klicken Sie auf den networkFolder-Link (zum Beispiel group-n6).
- d. Klicken Sie auf den DVS-Namen-Link (zum Beispiel „dvs-1“).
- e. Kopieren Sie den Wert von uuid.
4. Klicken Sie auf DVSManger und dann auf updateOpaqueDataEx.
5. Fügen Sie in *selectionSet* folgendes XML-Segment hinzu.

```
<selectionSet xsi:type="DVPortSelection">
  <dvsUuid>value</dvsUuid>
  <portKey>value</portKey> <!--Portnummer der DVPD, auf der Trunk-vNIC verb
unden wurde-->
</selectionSet>
```

6. Fügen Sie in *opaqueDataSpec* folgendes XML-Segment hinzu:

```
<opaqueDataSpec>
  <operation>remove</operation>
  <opaqueData>
    <key>com.vmware.net.vxlan.trunkcfg</key>
    <opaqueData></opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

7. Setzen Sie *isRuntime* auf "false".
8. Klicken Sie auf **Methode aufrufen**.
9. Wiederholen Sie die Schritte 5 bis 8 für jeden Trunk-Port, der auf der gelöschten Edge-VM konfiguriert wurde.
- **Problem 1637939: MD5-Zertifikate werden für die Bereitstellung von Hardware-Gateways nicht unterstützt**

Beim Bereitstellen von Hardware-Gateway-Switches als VTEPs für ein logisches Bridging von L2 VLAN zu VXLAN unterstützen die physischen Switches mindestens SHA1 SSL-Zertifikate für eine OVSDB-Verbindung zwischen dem NSX Controller und dem OVSDB-Switch.

*Problemumgehung:* Keine.

- **Problem 1637943: Der Hybrid- oder Multicast-Replikationsmodus wird für VNIs, die über eine Hardware-Gateway-Bindung verfügen, nicht unterstützt.**  
Hardware-Gateway-Switches unterstützen, wenn sie als VTEPs für das L2 VXLAN-zu-VLAN Bridging verwendet werden, nur den Unicast-Replikationsmodus.

*Problemumgehung:* Verwenden Sie nur den Unicast-Replikationsmodus.

- **Problem 1995142: Host wird nach dem Entfernen aus der vCenter-Bestandsliste nicht vom Replizierungscluster entfernt**  
Wenn ein Benutzer einen Host zu einem Replizierungscluster hinzufügt und den Host dann aus der vCenter-Bestandsliste entfernt, bevor er vom Cluster entfernt wurde, verbleibt der Legacyhost im Cluster.

*Problemumgehung:* Stellen Sie beim Entfernen eines Hosts zunächst sicher, dass er ggf. bereits vom Replizierungscluster entfernt wurde.

## Bekannte Probleme bei Sicherheitsdiensten

- **Problem 2000749: Verteilte Firewall bleibt bei bestimmten Firewall-Konfigurationen im Zustand „Veröffentlichen“**  
Die verteilte Firewall bleibt im Zustand „Veröffentlichen“, wenn Sie über eine Sicherheitsgruppe verfügen, die ein IPSet mit 0.0.0.0/0 als AUSSCHLUSS-Mitglied, als EINSCHLUSS-Mitglied oder als Teil einer dynamischen Mitgliedschaft mit Schnittmenge (UND) enthält.

*Problemumgehung:* Verwenden Sie in Ihrer IPSet-Konfiguration nicht „/0“ als Subnetzmaske. Sie können „0.0.0.0/0“ als „0.0.0.0/1,128.0.0.0/1“ definieren.

- **Problem 1854661:** In einem Cross-VC-Setup zeigen die gefilterten Firewallregeln nicht den Indexwert beim Wechsel zwischen NSX Managern an  
Nach der Anwendung von Kriterien einer Filterregel auf einen NSX Manager und dem Wechsel zu einem anderen NSX Manager zeigt der Index der Regel für alle gefilterten Regeln „0“ statt der tatsächlichen Position der Regel an.

*Problemumgehung:* Löschen Sie den Filter, um die Position der Regel anzuzeigen.

- **Problem 1474650:** NetX-Benutzer sehen bei ESXi 5.5.x- und 6.x-Hosts einen violetten Diagnosebildschirm mit der Meldung **ALERT: NMI: 709: NMI IPI received**  
Wenn eine große Anzahl von Paketen von einer Dienst-VM übertragen oder empfangen wird, dominiert DVFilter weiterhin die CPU, was Taktsignalverlust und einen violetten Diagnosebildschirm zur Folge hat. Weitere Informationen dazu enthält der [VMware-Knowledgebase-Artikel 2149704](#).

*Problemumgehung:* Upgrade des ESXi-Hosts auf eine der folgenden Mindestversionen von ESXi, die für die Verwendung von NetX erforderlich sind:

- 5.5 Patch 10
  - ESXi 6.0U3
  - ESXi 6.5
- **Problem 1787680:** Globaler Firewallabschnitt kann nicht gelöscht werden, wenn sich NSX Manager im Transitmodus befindet  
Wenn Sie versuchen, einen globalen Firewallabschnitt über die Benutzeroberfläche von NSX Manager im Transitmodus zu löschen und dann eine Veröffentlichung durchzuführen, schlägt dies fehl. Sie sind dann nicht mehr in der Lage, NSX Manager in den eigenständigen Modus zu versetzen.

*Problemumgehung:* Löschen Sie den globalen Firewallabschnitt mit der REST-API zum Löschen eines einzelnen Abschnitts.

- **Problem 1689159:** Die Funktion „Regel hinzufügen“ im Flow Monitoring funktioniert nicht korrekt für ICMP-Flows  
Beim Hinzufügen einer Regel über das Flow Monitoring bleibt das Feld „Dienste“ leer, wenn es nicht explizit auf „ICMP“ festgelegt wird. Infolgedessen wird gegebenenfalls eine Regel mit dem Diensttyp „ANY“ hinzugefügt.

*Problemumgehung:* Aktualisieren Sie das Feld „Dienste“, um den ICMP-Datenverkehr widerzuspiegeln.

- **Problem 1632235:** Während der Guest Introspection-Installation wird in der Netzwerk-Dropdown-Liste nur der Eintrag „Angabe auf dem Host“ angezeigt  
Bei der Installation von Guest Introspection mit der NSX-Lizenz nur für den Virenschutz und vSphere Essential oder mit der Standardlizenz enthält die Netzwerk-Dropdown-Liste nur die vorhandene Liste der DV-Portgruppen. Diese Lizenz unterstützt nicht die DVS-Erstellung.

*Problemumgehung:* Vor der Installation von Guest Introspection auf einem vSphere-Host mit einer dieser Lizenzen geben Sie zuerst das Netzwerk im Fenster „Agent-VM-Einstellungen“ an.

- **Problem 1652155:** Das Erstellen oder Migrieren von Firewallregeln mithilfe von REST-APIs kann unter bestimmten Bedingungen nicht durchgeführt werden und ergibt dann einen HTTP 404-Fehler

Das Hinzufügen oder Migrieren von Firewallregeln mithilfe von REST-APIs wird unter folgenden Bedingungen nicht unterstützt:

- Massenerstellung von Firewallregeln, wenn „autoSaveDraft=true“ festgelegt ist.
  - Gleichzeitiges Hinzufügen von Firewallregeln in mehreren Abschnitten.

*Problemumgehung:* Legen Sie für den Parameter autoSaveDraft im API-Aufruf „false“ fest, wenn Firewallregeln als Massenvorgang erstellt oder migriert werden.

- **Problem 1509687:** Für die URL-Länge werden beim Zuweisen eines einzelnen Sicherheits-Tag

zu vielen VMs in einem API-Aufruf gleichzeitig bis zu 16000 Zeichen unterstützt  
Ein einzelnes Sicherheits-Tag kann in einem API-Aufruf nicht einer großen Anzahl an VMs gleichzeitig zugewiesen werden, wenn die URL-Länge 16000 Zeichen übersteigt.

*Problemumgehung:* Zur Optimierung der Leistung weisen Sie ein Tag in einem einzelnen Aufruf nur maximal 500 VMs zu.

- **Problem 1662020:** Eine Veröffentlichung scheitert mit der Fehlermeldung „Die letzte Veröffentlichung ist auf Host *Hostnummer* fehlgeschlagen“ in den Abschnitten „Allgemein“ und „Partnersicherheitsdienste“ der Benutzeroberfläche der verteilten Firewall  
Nach der Änderung einer Regel wird in der Benutzeroberfläche die Meldung „Die letzte Veröffentlichung ist auf Host *Hostnummer* fehlgeschlagen“ angezeigt. Die in der Benutzeroberfläche aufgeführten Hosts verfügen eventuell nicht über die korrekte Version der Firewallregeln, sodass es zu Sicherheitslücken und/oder zu einer Netzwerkunterbrechung kommt.

Das Problem tritt in der Regel in folgenden Fällen auf:

- Nach dem Upgrade einer älteren auf die neueste NSX-Version.
- Nach der Verschiebung eines Hosts aus einem Cluster und seine Verschiebung zurück in den Cluster.
- Nach der Verschiebung eines Hosts von einem Cluster in einen anderen.

*Problemumgehung:* Zur Wiederherstellung müssen Sie eine Synchronisierung der betroffenen Cluster erzwingen (nur Firewall).

- **Problem 1481522:** Die Migration von Firewallregelentwürfen von 6.1.x auf 6.2.3 wird nicht unterstützt, da die Entwürfe der beiden Versionen nicht kompatibel sind

*Problemumgehung:* Keine.

- **Problem 1628679:** Bei Verwendung einer identitätsbasierten Firewall ist die VM von entfernten Benutzern weiterhin Teil der Sicherheitsgruppe

Wenn ein Benutzer aus einer Gruppe auf dem AD-Server entfernt wird, gehört die VM, für die der Benutzer angemeldet ist, weiterhin zur Sicherheitsgruppe. Dadurch werden die Firewallrichtlinien für die VM-vNIC auf dem Hypervisor beibehalten, sodass der Benutzer über einen kompletten Zugriff auf die Dienste verfügt.

*Problemumgehung:* Keine. Dieses Verhalten entspricht dem Programm-Design.

- **Problem 1496273:** Auf der Benutzeroberfläche können Sie NSX-Firewallregeln für beide Richtungen erstellen, die nicht auf Edges angewendet werden können  
Fälschlicherweise lässt der Web Client das Erstellen einer NSX-Firewallregel zu, die auf einen oder mehrere NSX Edges angewendet wird, wenn die Regel über Datenverkehr verfügt, der in eine der beiden Richtungen gesendet wird, bzw. wenn es sich bei dem Pakettyp um IPV4 oder IPV6 handelt. Auf der Benutzeroberfläche sollte das Erstellen solcher Regeln nicht zulässig sein, da NSX diese nicht auf NSX Edges anwenden kann.

*Problemumgehung:* Keine.

- **Problem 1494718:** Es können keine neuen universellen Regeln erstellt werden und vorhandene universelle Regeln können nicht über die Benutzeroberfläche von Flow Monitoring bearbeitet werden

*Problemumgehung:* Globale Regeln können nicht über die Flow Monitoring-UI hinzugefügt oder bearbeitet werden. EditRule wird automatisch deaktiviert.

- **Problem 1066277:** Name der Sicherheitsrichtlinie darf nicht länger als 229 Zeichen sein  
In das Feld für den Namen der Sicherheitsrichtlinie auf der Registerkarte „Sicherheitsrichtlinie“ von Service Composer können bis zu 229 Zeichen eingegeben werden. Grund hierfür ist, dass den Richtlinienamen intern ein Präfix vorangestellt wird.

*Problemumgehung:* Keine.

- **Problem 1443344:** Einige Versionen der Networks-VM-Serien von Drittanbietern funktionieren

nicht mit den Standardeinstellungen von NSX Manager

Einige Komponenten von NSX 6.1.4 oder später deaktivieren SSLv3 standardmäßig. Stellen Sie vor dem Upgrade sicher, dass *keine* der in Ihre NSX-Bereitstellung eingebundenen Drittanbieterlösungen von der SSLv3-Kommunikation abhängt. Zum Beispiel erfordern einige Versionen der Lösung der Palo Alto Networks VM-Serie Unterstützung für SSLv3. Bitten Sie deshalb Ihre Anbieter um die entsprechenden Versionsanforderungen.

- **Problem 1660718:** Für den Status der Service Composer-Richtlinie wird in der Benutzeroberfläche „Vorgang läuft“ und in der API-Ausgabe „Ausstehend“ angezeigt

*Problemumgehung:* Keine.

- **Problem 1317814:** Die Synchronisierung von Service Composer geht verloren, wenn Richtlinienänderungen durchgeführt werden, während einer der Service Manager ausgefallen ist

Werden Richtlinienänderungen durchgeführt, wenn einer von mehreren Dienst-Managern inaktiv ist, können diese Änderungen nicht durchgeführt werden und Service Composer ist nicht mehr synchronisiert.

*Problemumgehung:* Stellen Sie sicher, dass der Dienst-Manager reagiert und erzwingen Sie eine Synchronisierung über den Service Composer.

- **Problem 1070905:** Entfernen und erneutes Hinzufügen eines Hosts zu einem Cluster, der durch Guest Introspection und Lösungen von Drittanbietern geschützt wird, ist nicht möglich

Wenn Sie einen Host aus einem durch Guest Introspection und Lösungen von Drittanbietern geschützten Cluster entfernen, indem Sie die Verbindung des Hosts zu vCenter Server trennen und ihn anschließend aus diesem entfernen, treten möglicherweise Probleme auf, wenn Sie versuchen, denselben Host erneut demselben Cluster hinzuzufügen.

*Problemumgehung:* Um einen Host aus einem geschützten Cluster zu entfernen, versetzen Sie den Host zunächst in den Wartungsmodus. Verschieben Sie den Host im nächsten Schritt in einen nicht geschützten Cluster oder außerhalb aller Cluster. Trennen Sie dann die Verbindung und entfernen Sie den Host.

- **Problem 1648578:** NSX erzwingt das Hinzufügen von Cluster/Netzwerk/Speicher, wenn eine neue Host-basierte NetX-Dienstinstanz erstellt wird

Wenn Sie über den vSphere Web Client eine neue Dienstinstanz für Host-basierte NetX-Dienste, beispielsweise eine Firewall, IDS und IPS, erstellen, werden Sie gezwungen, Cluster/Netzwerk/Speicher hinzuzufügen, auch wenn diese nicht erforderlich sind.

*Problemumgehung:* Beim Erstellen einer neuen Dienstinstanz können Sie beliebige Informationen für Cluster/Netzwerk/Speicher angeben, um die Felder auszufüllen. Auf diese Weise ist es Ihnen möglich, die Dienstinstanz zu erstellen und wunschgemäß fortzuführen.

## Bekannte Probleme bei Überwachungsdiensten

- **Problem 1466790:** Mit dem NSX-Tool Traceflow können keine VMs in überbrückten Netzwerken ausgewählt werden

Wenn Sie das NSX-Tool Traceflow verwenden, können Sie nur VMs auswählen, die mit einem logischen Switch verbunden sind. Das bedeutet, dass VMs in einem L2-überbrückten Netzwerk nicht mit dem VM-Namen als Quell- oder Zieladresse für die Traceflow-Untersuchung ausgewählt werden können.

*Problemumgehung:* Verwenden Sie für VMs, die an L2-überbrückte Netzwerke angeschlossen sind, die IP-Adresse oder MAC-Adresse der Schnittstelle, die Sie als Ziel in einer Traceflow-Untersuchung angeben möchten. Sie können an L2-überbrückte Netzwerke angeschlossene VMs nicht als Quelle verwenden. Weitere Informationen finden Sie im [Knowledgebase-Artikel 2129191](#).