

# Versionshinweise zu VMware NSX for vSphere 6.3.0

VMware NSX for vSphere 6.3.0 | Freigegeben am 2. Februar 2017 | Build 5007049

## Inhalt dieser Versionshinweise

Diese Versionshinweise decken die folgenden Themen ab:

- [Neuigkeiten](#)
- [Versionen, Systemanforderungen und Installation](#)
- [Eingestellte und nicht fortgeführte Funktionalität](#)
- [Upgrade-Hinweise](#)
- [Bekannte Probleme](#)
- [Behobene Probleme](#)
- [Revisionsverlauf der Dokumente](#)

## Neuigkeiten

Die neuen Funktionen in NSX 6.3.0 sind in folgende Kategorien aufgeschlüsselt:

- [Plattform- und Übereinstimmungsfunktionen](#)
- [Verbesserungen im Betrieb](#)
- [Dienst- und Routing-Verbesserungen](#)
- [Sicherheitsverbesserungen](#)
- [CMP und Partnerintegration](#)
- [Installation und Upgrade](#)
- [Sichern und Wiederherstellen](#)

### Plattform- und Übereinstimmungsfunktionen

- Plattformfunktionen:
  - **Verbesserungen der Cross-vCenter NSX-Aktiv/Standby-DFW:** NSX 6.3.0 verfügt über folgende Verbesserungen:
    - Es werden nun mehrere globale DFW-Abschnitte unterstützt. Sowohl globale wie lokale Regeln können globale Sicherheitsgruppen in den Feldern **Quelle**, **Ziel** und **AppliedTo** nutzen.
    - **Universelle Sicherheitsgruppen:** Die Mitgliedschaft in globalen Sicherheitsgruppen kann statisch oder dynamisch definiert werden. Eine statische Mitgliedschaft entsteht durch manuelles Hinzufügen eines globalen Sicherheits-Tags zu jeder VM. Eine dynamische Mitgliedschaft wird durch Hinzufügen von VMs als Mitglieder auf der Basis dynamischer Kriterien (VM-Name) erstellt.

- **Universelle Sicherheits-Tags:** Sie haben jetzt die Möglichkeit, globale Sicherheits-Tags auf dem primären NSX Manager zu definieren und für eine globale Synchronisierung mit sekundären NSX Managern zu kennzeichnen. Globale Sicherheits-Tags können VMs statisch auf der Basis einer ausgewählten eindeutigen Kennung oder dynamisch auf der Basis von Kriterien wie Antivirenschans oder Prüfungen auf Schwachstellen zugewiesen werden.
- **Auswahlkriterien für eindeutige Kennung:** In früheren Version von NSX waren Sicherheits-Tags nur lokal für einen NSX Manager verfügbar. Sie wurden VMs mithilfe der Objekt-ID der verwalteten VM zugeordnet. In einer Aktiv/Standby-Umgebung ist die Objekt-ID für eine bestimmte verwaltete VM nicht immer mit jener in den aktiven und Standby-Datenzentern identisch. NSX 6.3.x ermöglicht die Konfiguration von Auswahlkriterien für eine eindeutige Kennung auf dem primären NSX Manager für die Ermittlung von VMs beim Anfügen an globale Sicherheits-Tags: VM-Instanz-UUID, VM-BIOS-UUID, VM-Name oder eine Kombination dieser Optionen. Weitere Informationen dazu finden Sie unter [Auswahl einer eindeutigen Kennung](#) im *NSX Administratorhandbuch für NSX*.

- **Automatische Wiederherstellung des Agenten der Kontrollebene (netcpa)** Mit einem verbesserten Mechanismus zur automatischen Wiederherstellung für den netcpa-Vorgang wird eine fortlaufende Datenpfadkommunikation sichergestellt. Der automatische netcpa-Überwachungsvorgang startet auch automatisch neu, wenn Probleme auftreten, und übermittelt Warnungen über den Syslog-Server. Zusammenfassung der Verbesserungen:
  - Automatische Überwachung des netcpa-Vorgangs
  - Durchführung eines automatischen Neustarts bei Problemen, z. B. wenn das System hängt
  - Automatische Generierung einer Kerndatei für das Debugging
  - Warnungen über Syslog für das Ereignis des automatischen Neustarts
- **vSphere 6.5-Kompatibilität:** Ab Version NSX 6.3.0 wird vSphere 6.5a und höher unterstützt. NSX 6.3.0 ist dabei weiterhin mit vSphere 5.5 und 6.0 kompatibel.
- **Tech-Preview:** Modus für den Betrieb mit getrenntem Controller (Controller Disconnected Operation, CDO): Der CDO-Modus (Controller Disconnected Operation, Betrieb mit getrenntem Controller) wurde als Tech-Preview-Funktion integriert. In diesem Modus ist sichergestellt, dass die Datenebenenkonnektivität nicht beeinträchtigt wird, wenn die Verbindung von Hosts zum Controller verloren geht. Erläuterungen dazu finden Sie im Abschnitt [Modus für den Betrieb mit getrenntem Controller \(Controller Disconnected Operation, CDO\)](#): im *Administratorhandbuch für NSX*. Siehe auch das Problem 1803220.

• **Übereinstimmungsfunktionen:**

- **FIPS:** NSX 6.3.0 verfügt über einen FIPS-Modus, der nur jene Verschlüsselungs-Suiten verwendet, die mit FIPS übereinstimmen. Der FIPS-Modus von NSX Manager und NSX Edge kann über den vSphere Web Client oder über die NSX-REST-API aktiviert werden. Eine Liste der Funktionen, die vom FIPS-Modus betroffen sind, finden Sie unter [Unterschiede der Funktionalität zwischen dem FIPS-Modus und dem Nicht-FIPS-Modus](#) im *Administratorhandbuch für NSX*.

**Hinweis:** VMware-Entwicklungspartner durchlaufen eine Zertifizierung von neuen, FIPS-konformen Partnerlösungen für die Verwendung in NSX. Ausgehende NSX 6.3.0-Verbindungen benötigen TLS 1.1 oder höher und verwenden nur FIPS-konforme Verschlüsselungs-Suiten. Das bedeutet, dass Partner-Appliances, die Callbacks erhalten, sichere Web-Listener konfigurieren müssen, um sicherere Verschlüsselungs-Suiten zu ermöglichen. Im Folgenden sind die Verschlüsselungen für den Standardmodus und den FIPS-Modus aufgeführt:

■ **Verschlüsselungen für den Standardmodus: (FIPS-Modus deaktiviert)**

```
[TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA,
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA, TLS_EMPTY_RENEGOTIATION_INFO_SCSV]
```

■ **Verschlüsselungen für den FIPS-Modus:** [TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA, TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA]

Sowohl der Standard- wie der FIPS-Modus unterstützen das TLS 1.1- und das TLS 1.2-Protokoll. Um festzustellen, ob Partnerlösungen für den FIPS-Modus zertifiziert sind, lesen Sie die entsprechenden Informationen im [VMware-Kompatibilitäts-Handbuch](#) nach.

- **Common Criteria:** Für eine Übereinstimmung mit Common Criteria wurde NSX auf eine Übereinstimmung mit dem EAL2+-Vertrauensgrad getestet. Die Durchführung einer Common Criteria-konformen NSX-Installation erfordert die Konfiguration von NSX, wie im Dokument [Konfigurieren von NSX für Common Criteria](#) im *Administratorhandbuch für NSX* beschrieben.
- **ICSA:** Hier handelt es sich um eine branchenweit anerkannte Standardzertifizierung, mit der Produkte wie Antiviren-, Firewall-, IPSec VPN-, Kryptografie-, SSL VPN-, Netzwerk-IPS-, Antispyware- und PC-Firewallprodukte getestet und zertifiziert werden. Sowohl die verteilte Firewall wie die Edge-Firewall werden auf der Basis der ICSA-Corporate-Firewall-Kriterien zertifiziert.
- **Änderung des Protokollformats des DFW-Pakets aufgrund der Anforderungen der ICSA-Zertifizierung:** Ab NSX 6.3.0 gelten Änderungen für die DFW-Paketprotokolle. In 6.3.0 und höher wurde der ICMP-Typ und -Code hinzugefügt, um die Anforderungen der ICSA-Zertifizierung zu erfüllen.

Protokolle vor 6.3.0 hatten ohne ICMP-Code und -Typ folgendes Aussehen:

```
2016-09-29T20:52:21.983Z 6673 INET6 match PASS domain-c27/1001 IN 96 ICMP
```

fe80:0:0:0:21d:b502:f984:c601->ff02:0:0:0:0:0:0:1

In 6.3.0 und höher lauten die Protokolleintragungen mit ICMP-Code und -Typ wie im Folgenden dargestellt. In folgendem Beispiel steht 8 für den Code und 0 für den Typ:

```
2016-09-29T20:54:16.051Z 42991 INET match PASS domain-c27/1001 IN 84 ICMP 8
0 10.113.226.5->10.28.79.55
```

## Verbesserungen im Betrieb

- **Fehlerbehebung für Dashboard:** NSX Dashboard wurde in NSX 6.3.0 aktualisiert und enthält nun weitere Funktionen wie den Status der Dienstbereitstellung, den Sicherheitsstatus für NSX Manager und Edge-Appliance-Benachrichtigungen.
- **Sicherheits-Tagging:** Mit dieser Funktion können Sie über API-Aufrufe mehrere Tags für eine bestimmte VM zuweisen und löschen.
- **Verbesserungen für Syslog:** Eine neue Syslog-Aktualisierung ist speziell für Load Balancer verfügbar.
- **Log Insight-Inhaltspaket:** Dieses Paket wurde für Load Balancer aktualisiert. Es enthält nun ein zentrales Dashboard, eine End-to-End-Überwachung und eine verbesserte Kapazitätsplanung über die Benutzeroberfläche.
- **Rollenbasierte Zugriffssteuerung:** Diese Funktion beschränkt die Benutzerverwaltung auf Enterprise-Administratoren. NSX-Administratoren haben dann nicht mehr die Berechtigung, neue Benutzer anzulegen oder neuen Benutzern Rollen zuzuweisen. Vom Standpunkt der Sicherheit aus lässt sich damit eine eindeutige Trennlinie zwischen diesen beiden Administratorrollen ziehen.
- **Status „Ausgleichen“ für Load-Balancer-Poolmitglieder:** Sie haben die Möglichkeit, Poolmitglieder in den Status *Ausgleichen* zu versetzen, in dem das kontrollierte Herunterfahren für Wartungszwecke erzwungen wird. Die Festlegung des Status „Ausgleichen“ für ein Poolmitglied entfernt den Backend-Server aus dem Load Balancing. Der Server kann aber weiterhin neue dauerhafte Verbindungen eingehen.

## Dienst- und Routing-Verbesserungen

- **4-Byte-ASN-Unterstützung für BGP:** In Verbindung mit der Rückwärtskompatibilität für bereits vorhandene 2-Byte-ASN-BGP-Peers ist die BGP-Konfiguration nun mit 4-Byte-ASN-Unterstützung verfügbar.
- **NAT-Verbesserung für 5-Tupel-Übereinstimmung:** Für eine detaillierte Konfiguration und eine größere Flexibilität von NAT-Regeln wird in NSX 6.3.0 die 5-Tupel-Übereinstimmung unterstützt:
  - Die Übereinstimmungskriterien basieren auf fünf Parametern: Protokoll, Quell-IP, Quellport, Ziel-IP und Zielport.
  - Die Benutzeroberfläche wurde geändert, um die Festlegung von SNAT-/DNAT-Konfigurationen zu vereinfachen. In früheren Edge-Versionen wurden die Fenster nach der Änderung von SNAT-/DNAT-Konfigurationen immer noch im alten Stil angezeigt.
  - Die NSX-REST-API verfügt über die Möglichkeit, Felder für die neuen Parameter hinzuzufügen:

```
<natRules>
  <natRule>
    {...}

<!-- Neue, für DNAT anwendbare Felder -->
    <dnatMatchSourceAddress>Beliebig</dnatMatchSourceAddress>
    <dnatMatchSourcePort>Beliebig</dnatMatchSourcePort>
  </natRule>
```

```

    <natRule>
    {...}
    <!-- Neue, für SNAT anwendbare Felder -->
    <snatMatchDestinationAddress>Beliebig</snatMatchDestinationAddress>
ess>
    <snatMatchDestinationPort>Beliebig</snatMatchDestinationPort>
    </natRule>
</natRules>

```

- **Verbesserte Schicht-2-VPN-Leistung:** Die Leistung eines Schicht-2-VPN wurde verbessert. Dies ermöglicht einer einzelnen Edge-Appliance die Unterstützung eines Durchsatzes von bis zu 1,5 GB/s gegenüber 750 MB/s der vorherigen Versionen.
- **Verbesserte Konfigurierbarkeit für OSPF:** Bei der Konfiguration von OSPF auf einem Edge Services Gateway (ESG) lassen sich mit NSSA alle Typ-7-LSAs in Typ-5-LSAs konvertieren.

## Sicherheitsverbesserungen

Für die verteilte Firewall sind verschiedene Verbesserungen vorgenommen worden:

- **DFW-Timer:** NSX 6.3.0 verfügt nun über Sitzungstimer, die definieren, wie lange eine Sitzung nach der Inaktivität an der Firewall beibehalten wird. Wenn die Sitzungszeitüberschreitung für das Protokoll abläuft, wird die Sitzung geschlossen. Für die Firewall können Sie Zeitüberschreitungen für TCP-, UDP- und ICMP-Sitzungen definieren und diese auf benutzerdefinierte Sätze von VMs oder vNICs anwenden. Weitere Erläuterungen dazu finden Sie unter [Sitzungs-Timer](#) im *Administratorhandbuch für NSX*.
- **Neue Funktionen zur Unterstützung der Mikrosegmentierung:** Zur Unterstützung der Mikrosegmentierung in Bezug auf Sichtbarkeit und Planungstools wurden zwei neue Funktionen implementiert:
  - Der Application Rule Manager vereinfacht das Erstellen von Sicherheitsgruppen und Firewallregeln mit Positivlisten für vorhandene Anwendungen.
  - Die Endpunktüberwachung gibt dem Besitzer einer Anwendung die Möglichkeit, seine Anwendung zu überprüfen und die Vorgänge zu ermitteln, die Netzwerkverbindungen herstellen.
- **Linux-Unterstützung für Guest Introspection:** NSX 6.3.0 ermöglicht die Anwendung der Guest Introspection für Linux-VMs. Auf Linux-basierten Gast-VMs nutzt die NSX Guest Introspection-Funktion die vom Linux-Kernel bereitgestellten Module `fanotify` und `inotify`. Weitere Informationen dazu finden Sie unter [Installieren von Guest Introspection für Linux](#) im *Administratorhandbuch für NSX*. Unter [Versionen](#) finden Sie eine Liste von Linux-Versionen, die von NSX unterstützt werden.
- **Veröffentlichungsstatus für Service Composer:** Es ist nun der Veröffentlichungsstatus für Service Composer verfügbar, damit Sie prüfen können, ob eine Richtlinie synchronisiert wurde. Dies erhöht die Transparenz der Übersetzung von Sicherheitsrichtlinien in DFW-Regeln auf dem Host.

## Cloud Management Platform (CMP) und Partnerintegration

- Durch eine verbesserte Interoperabilität zwischen vCloud Director 8.20 und NSX 6.3.0 können Dienstanbieter ihren Mandanten erweiterte Netzwerk- und Sicherheitsdienste liefern. vCloud Director 8.20 mit NSX 6.3.0 bietet eine native NSX-Funktionalität zur Unterstützung mehrerer Mandanten und eines Mandanten-Self-Service.
- NSX 6.3.0 unterstützt die neue vRO-Plug-in-Version 1.1, die nicht nur vRA unterstützt, sondern auch Nicht-vRA-Anwendungen.

- NSX NetX 6.3.0 bietet Verbesserungen in Sachen Skalierung und Leistung in Bezug auf Service Insertion.

## Installation und Upgrade

- **NSX-Kernelmodule sind jetzt nicht mehr von der ESXi-Version abhängig:** Ab der Version NSX 6.3.0 verwenden NSX-Kernelmodule nur die öffentlich verfügbare VMKAPI, sodass die Schnittstellen zwischen Versionen sichergestellt sind. Durch diese Verbesserung wird die Gefahr des Scheiterns von Host-Upgrades aufgrund falscher Versionen des Kernelmoduls reduziert. In früheren Versionen waren für jedes ESXi-Upgrade in einer NSX-Umgebung mindestens zwei Neustarts erforderlich, um sicherzustellen, dass die NSX-Funktionalität weiterhin funktioniert (da neue Kernelmodule für jede neue ESXi-Version weitergegeben werden müssen).
- NSX 6.3.0 überprüft auch, ob NSX bereit ist, bevor für einen Host der Wartungsmodus beendet wird. Damit wird sichergestellt, dass DRS nur dann Arbeitslasten auf einen Host überträgt, wenn NSX bereit ist. Dies verhindert die Trennung der Netzwerkverbindung für einige Arbeitslast-VMs.
- **OVF-Parameters sind nun kommasetrennt:** Die folgenden OVF-Parameter werden nicht mehr durch Leerzeichen, sondern durch Kommas getrennt:
  - DNS-Serverliste (vsm\_dns1\_0)
  - Domänensuchliste (vsm\_domain\_0)
  - NTP-Serverliste (vsm\_ntp\_0)

## Sichern und Wiederherstellen

Ab NSX 6.3.0 werden die folgenden Verschlüsselungen für die SFTP-Sicherung unterstützt:

- **Verschlüsselung:** aes128-cbc, aes128-ctr, aes192-cbc, aes192-ctr, aes256-cbc, aes256-ctr
- **Nachrichtenauthentifizierung (Mac):** hmac-sha2-256
- **Schlüsselaustausch:** diffie-hellman-group-exchange-sha256

**Hinweis:** Es ist keine Unterstützung für `Hmac-sha1` verfügbar, es wird nur `Hmac-sha2-256` unterstützt. Wenn Sie für die Sicherung SFTP verwenden, ändern Sie nach dem Upgrade auf 6.3.0 den Wert in `Hmac-sha2-256`. Weitere Informationen dazu enthält der [VMware-Knowledgebase-Artikel 2149282](#).

## 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.

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>
Guest Introspection für Windows	<p>Es werden alle Versionen von VMware Tools unterstützt. Für einige Guest Introspection-basierte Funktionen sind neuere Versionen von VMware Tools erforderlich:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Führen Sie ein Upgrade auf VMware Tools 10.0.8 und höher für die Behebung des Problems verlangsamter VMs nach dem Upgrade von VMware Tools in NSX/vCloud Networking and Security durch (siehe <a href="#">VMware-Knowledgebase-Artikel 2144236</a>).</li> <li>• Verwenden Sie VMware Tools 10.1.0 und höher zur Unterstützung von Windows 10.</li> </ul>
Guest Introspection für Linux	<p>Diese NSX-Version unterstützt die folgenden Linux-Versionen:</p> <ul style="list-style-type: none"> <li>• RHEL 7 GA (64 Bit)</li> <li>• SLES 12 GA (64 Bit)</li> <li>• Ubuntu 14.04 LTS (64 Bit)</li> </ul>
vRealize Orchestrator	NSX-vRO-Plug-In 1.1.0 oder höher

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](#).

- **NSX for vSphere 6.1.x:** Für NSX for vSphere 6.1.x wurden am 15. Januar 2017 der EOA-Zeitpunkt (End of Availability, Ende der Verfügbarkeit) und der EOGS-Zeitpunkt (End of General Support, Ende des allgemeinen Supports) erreicht. (Informationen hierzu finden Sie auch im [VMware-Knowledgebase-Artikel 2144769](#).)
- **NeuNSX Data Security wurde entfernt:** In der Version NSX 6.3.0 wurde die Funktion NSX Data Security aus dem Produkt entfernt.
- **NeuNSX 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*.
- **NeuWeb 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.
- **NeuIS-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.
- **NeuvCNS-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

Löschen der Firewallkonfiguration oder des Standardabschnitts:

- Die Anforderung zum Löschen eines Firewallabschnitts wird jetzt abgelehnt, wenn der Standardabschnitt angegeben wurde: `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 /api/4.0/firewall/globalroot-0/config/layer2sections|layer3sections/{sectionId}`

Der Parameter `defaultOriginate` wurde aus den folgenden Methoden nur 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

## Upgrade-Hinweise

- [Upgrade-Hinweise zu NSX und vSphere](#)
- [Upgrade-Hinweise zu NSX-Komponenten](#)
- [Upgrade-Hinweise zu FIPS](#)

Hinweis: Wenn Sie SFTP für NSX-Sicherungen verwenden, finden Sie unter [Sicherung und Wiederherstellung](#) eine Liste der ab 6.3.x unterstützten Sicherheitsalgorithmen.

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

### Upgrade-Hinweise zu NSX und vSphere

- 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.

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
- **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 6.3.0 werden nicht unterstützt. Sie müssen zuerst ein Upgrade auf eine unterstützte 6.2.x-Version durchführen.
- **Upgrade auf vSphere 6.5a:** Wenn Sie ein Upgrade von vSphere 5.5 oder 6.0 auf vSphere 6.5a durchführen möchten, müssen Sie zuerst ein Upgrade auf NSX 6.3.0 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.

- **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.
- Wenn in Ihrer Umgebung ein Hardware-Gateway (Hardware-VTEP) installiert ist, kann kein Upgrade auf NSX 6.3.0 durchgeführt werden. Um mit dem Upgrade fortfahren zu können, müssen Sie Kontakt mit dem VMware-Support aufnehmen. Weitere Informationen dazu enthält der [VMware-Knowledgebase-Artikel 2148511](#).
- **Setzen Sie den vSphere Web Client zurück:** Nach dem Upgrade von NSX Manager müssen Sie den vSphere Web Client-Server wie in der [Dokumentation zum NSX-Upgrade](#) erläutert zurücksetzen. Bevor Sie diesen Schritt ausführen, wird die Registerkarte **Netzwerk und Sicherheit** im vSphere Web Client möglicherweise nicht angezeigt. Eventuell müssen Sie auch Ihren Browser-Cache oder Ihren Browser-Verlauf löschen.
- **Zustandsfreie Umgebungen:** Für NSX-Upgrades in einer statusfreien Hostumgebung werden neue VIB-URLs verwendet: 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:

1. Laden Sie die aktuellen NSX-VIBs vom NSX Manager über eine feste URL herunter.
2. Fügen Sie die VIBs zum Host-Image-Profil hinzu.

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:

- Suchen Sie die neue VIB-URL über `https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties`.
- Rufen Sie die VIBs der erforderlichen ESX-Hostversion über die jeweilige URL ab.
- Fügen Sie sie zu einem Image-Profil hinzu.

## Upgrade-Hinweise zu NSX-Komponenten

- **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:

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 nachfolgender Tabelle).

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

- **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*.

Führen Sie die folgenden Schritte aus, um sicherzustellen, dass für die Messaging-Infrastruktur der Hosts, auf denen NSX Edge bereitgestellt wird, der Status GRÜN (GREEN) gilt:

- Verwenden Sie die API-Methode `GET /api/2.0/nwfabric/status?resource={resourceId}`, wobei `resourceId` für die Objekt-ID (z. B. `domain-c33` oder `host-21`) des mit vCenter verwalteten Host- oder Cluster-Objekts steht. Anweisungen zur Ermittlung von Ressourcen-IDs für Cluster und Hosts finden Sie unter „Suchen von vCenter-Objekt-IDs“ im *API-Handbuch zu NSX*.
- Suchen Sie im Antworttext nach dem Status, der der `featureId` von `com.vmware.vshield.vsm.messagingInfra` entspricht:

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
  <installed>true</installed>
  <enabled>true</enabled>
  <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

- **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).
- **Controller-Festplattenlayout:** Upgrades von 6.2.2 und früher erhalten nicht das neue, in 6.2.3 eingeführte Festplattenlayout, das separate Festplattenpartitionen für Daten und Protokolle zur Verbesserung der Controller-Stabilität ermöglicht.

- **Bevor Sie ein Upgrade auf NSX 6.2.5 oder höher vornehmen, stellen Sie sicher, dass alle Load-Balancer-Verschlüsselungslisten durch Doppelpunkte getrennt sind.** Wenn in Ihrer Verschlüsselungsliste ein anderes Trennzeichen (z. B. das 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>` mit einer Liste mit Doppelpunkttrennung. 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"
}
```

- **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-Hinweise zu 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-SHA38, 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 6.3.0 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.

## Bekannte Probleme

Bekannte Probleme gliedern sich wie folgt:

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

### Allgemeine bekannte Probleme

**Neu** 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 1558285:** Das Löschen von Clustern von vCenter mithilfe von Guest Introspection führt zu einer Nullzeiger-Ausnahme

Bevor ein Cluster von vCenter entfernt werden kann, müssen Dienste wie Guest Introspection entfernt werden.

*Problemumgehung:* Löschen Sie die EAM-Agency für die Dienstbereitstellung ohne zugeordneten Cluster.

**Problem 1629030:** Für die Befehle der zentralen CLI zur Paketerfassung (debug packet capture und show packet capture) ist vSphere 5.5U3 oder höher erforderlich

Diese Befehle werden von früheren Versionen von vSphere 5.5 nicht unterstützt.

*Problemumgehung:* VMware empfiehlt allen NSX-Kunden die Verwendung von vSphere 5.5U3 oder höher.

**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.

**Neu**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.

**Neu**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>
```

**NeuProblem 1808478:** Der vsfwd-Dienst kann nicht gestartet werden, wenn der vmvisor-Arbeitsspeicher nach dem Upgrade von NSX 6.2.x auf NSX 6.3.0 nicht zugeteilt werden kann  
Der vsfwd-Dienst kann nicht gestartet werden, wenn der vmvisor-Arbeitsspeicher nach dem Upgrade von NSX 6.2.x auf NSX 6.3.0 nicht zugeteilt werden kann. Weitere Informationen enthält der [VMware-Knowledgebase-Artikel 2148974](#).

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

**NeuProblem 1818257:** Es werden keine VTEP-Informationen an die Controller übergeben, wenn für VXLAN nach dem Host-Upgrade von NSX 6.2.x auf NSX 6.3.0 mit ESXi 6.0 das erweiterte LACP-Protokoll verwendet wird  
Beim Upgrade von NSX 6.2.x auf 6.3.0 mit ESXi 6.0 werden nach dem Hostupgrade die VTEP-Informationen nicht an die Controller übergeben, wenn das erweiterte LACP-Protokoll verwendet wird. Weitere Informationen enthält der [VMware-Knowledgebase-Artikel 2149210](#).

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

**NeuProblem 1791371:** Wenn beim Upgrade von ESXi-Hosts auf vSphere 6.5a die Guest Introspection- und VXLAN-VIBs zeitgleich aktualisiert werden, wird ein Alarm ausgelöst  
Die Guest Introspection- und VXLAN-VIBs unterscheiden sich bei vSphere 6.5a. Wenn Sie diese Komponenten zeitgleich aktualisieren, wird vom VXLAN-VIB-Upgrade ein Alarm ausgelöst, der einen Neustart des Hosts verlangt.

*Problemumgehung:* Installieren Sie zuerst die VXLAN-VIBs und anschließend die Guest Introspection-VIBs, wenn Sie ein Upgrade auf vSphere 6.5a durchführen.

**NeuProblem 1805983:** Wenn Sie ein Upgrade auf NSX 6.2.5, 6.2.6 oder 6.3.0 durchführen, funktionieren virtuelle Server ohne einen Serverpool nicht  
Virtuelle Server ohne Serverpool unterstützen nur die HTTP/HTTPS-Umleitung. Alle anderen Funktionen sind nicht verfügbar.

*Problemumgehung:* Erstellen Sie einen Pseudopool ohne Mitglieder und weisen Sie diesen dem virtuellen Server zu.

**NeuProblem 1797307:** Bei NSX Edge kann nach einem Upgrade oder einer erneuten Bereitstellung ein Split Brain auftreten  
Für ein Standby-NSX Edge wird vom CLI-Befehl „show service highavailability“ der Hochverfügbarkeitsstatus als „Standby“ ausgegeben, der Status für „config engine“ aber als „Aktiv“.

*Problemumgehung:* Starten Sie das NSX Edge im Standbymodus neu.

**NeuProblem 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.

*Problemumgehung:* Statt das Failback sofort nach dem Neustart des Hosts durchzuführen, führen Sie das Failback auf den neu vorbereiteten Host dieser VMs später durch.

**NeuProblem 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>
```

### **NeuProblem 1802688: Upgrade von NSX 6.2.x auf 6.3.0 übernimmt nicht den aktualisierten DFW-Aktivierungsstatus**

Wenn Sie dem aktualisierten Cluster nach einem Upgrade von NSX von 6.2.x auf 6.3.0 und von Cluster-VIBs auf 6.3.0-Bits einen neuen Host hinzufügen, ist der bisherige Firewallstatus des betreffenden Hosts und Clusters weiterhin gültig und wird nicht aktualisiert, auch wenn die neuen VIBs auf dem neuen Host installiert wurden.

**Problemumgehung:** Gehen Sie wie folgt vor:

1. Führen Sie den API-Aufruf zur Synchronisierung des Nachrichtenbusses für den Host mit folgender API durch: POST <https://<NSX-IP>/api/2.0/nwfabric/configure?action=synchronize>. Der Firewallstatus für diesen Host und Cluster wird dadurch auf „Deaktiviert“ gesetzt.

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

2. Aktivieren Sie jetzt über die Benutzeroberfläche die Firewall für diesen Cluster auf der Seite „Installation“ > „Hostvorbereitung“. Damit sollte für alle Hosts in diesem Cluster der Modus der aktivierten DFW gelten.

### **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 1660355:** Bei VMs, die von 6.1.5 auf 6.2.3 und höher migriert wurden, wird TFTP-ALG nicht unterstützt

Auch wenn der Host aktiviert ist, wird für VMs, die von 6.1.5 auf 6.2.3 und höher migriert wurden, kein TFTP-ALG unterstützt.

*Problemumgehung:* Fügen Sie die VM hinzu und entfernen Sie diese von der Ausschlussliste oder starten Sie die VM neu, damit der neue Filter für 6.2.3 (und höher) erstellt wird, der ein TFTP-ALG unterstützt.

**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 1332563:** 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 1473537: 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.

Wenn in Ihrer Umgebung nicht alle Cluster 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 1215460: Wenn eine Dienstgruppe nach dem Upgrade geändert wird und Dienste hinzugefügt oder entfernt werden, werden diese Änderungen nicht in der Firewall-Tabelle widerspiegelt.**

Von Benutzern erstellte Dienstgruppen werden in der Edge-Firewall-Tabelle beim Upgrade erweitert, d. h., in der Spalte „Service“ in der Firewall-Tabelle werden alle Dienste innerhalb der Dienstgruppe angezeigt. Wenn die Dienstgruppe nach dem Upgrade zum Hinzufügen oder Entfernen von Diensten modifiziert wird, werden diese Änderungen nicht in der Firewall-Tabelle widerspiegelt.

*Problemumgehung:* Erstellen Sie eine neue Dienstgruppe mit einem anderen Namen und verwenden Sie dann diese Dienstgruppe in der Firewallregel.

**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 1266433: 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 neuste Version manuell installieren.

### Problem 1474066: Der NSX-REST-API-Aufruf zur Aktivierung bzw. Deaktivierung der IP-Erkennung scheint keine Auswirkungen zu haben

Wenn die Clustervorbereitung auf dem Host noch nicht abgeschlossen ist, hat der NSX-REST-API-Aufruf zum Aktivieren bzw. Deaktivieren der IP-Erkennung (<https://<nsxmgr-ip>/api/2.0/xvs/networks/universalwire-5/features>) keine Auswirkungen.

**Problemumgehung:** Stellen Sie vor dem Erteilen dieses API-Aufrufs sicher, dass die Hostclustervorbereitung abgeschlossen ist.

### Problem 1459032: Fehler beim Konfigurieren eines VXLAN-Gateways

Wenn beim Konfigurieren von VXLAN mit einem statischen IP-Pool (unter Networking & Security > Installation > Hostvorbereitung > VXLAN konfigurieren) keine Gateway-IP für den IP-Pool auf dem VTEP festgelegt werden kann (weil das Gateway nicht ordnungsgemäß konfiguriert oder nicht erreichbar ist), wechselt der Status der VXLAN-Konfiguration für den Host-Cluster in den Fehlerstatus (ROT).

Die Fehlermeldung lautet `VXLAN-Gateway kann auf Host nicht festgelegt werden` und der Fehlerstatus ist `VXLAN_GATEWAY_SETUP_FAILURE`. Im REST-API-Aufruf `GET https://<nsxmgr-ip>/api/2.0/nwfabric/status?resource=<cluster-moid>` lautet der VXLAN-Status wie folgt:

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.nsxmgr.vxlan</featureId>
  <featureVersion>5.5</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>RED</status>
  <message>VXLAN Gateway cannot be set on host</message>
  <installed>true</installed>
  <enabled>true</enabled>
  <errorStatus>VXLAN_GATEWAY_SETUP_FAILURE</errorStatus>
</nwFabricFeatureStatus>
```

**Problemumgehung:** Es gibt zwei Optionen, den Fehler zu beheben.

- Option 1: Entfernen Sie die VXLAN-Konfiguration für den Host-Cluster, korrigieren Sie das zugrunde liegende Gateway-Setup im IP-Pool, indem Sie sicherstellen, dass das Gateway ordnungsgemäß konfiguriert ist, und konfigurieren Sie VXLAN für den Host-Cluster anschließend neu.
- Option 2: Führen Sie die folgenden Schritte aus.
  1. Korrigieren Sie das zugrunde liegende Gateway-Setup im IP-Pool, indem Sie sicherstellen, dass das Gateway ordnungsgemäß konfiguriert und erreichbar ist.
  2. Versetzen Sie den Host (oder Hosts) in den Wartungsmodus, um sicherzustellen, dass auf dem Host kein VM-Datenverkehr aktiv ist.
  3. Löschen Sie die VXLAN VTEPs aus dem Host.
  4. Deaktivieren Sie den Wartungsmodus für den Host. Durch das Deaktivieren des Wartungsmodus für den Host wird der VXLAN VTEP-Erstellungsvorgang auf NSX Manager ausgelöst. NSX Manager versucht, die erforderlichen VTEPs auf dem Host erneut zu erstellen.

### 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-vdpi“ 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 1485862:** Das Deinstallieren von NSX aus einem Hostcluster führt manchmal zu einem Fehlerzustand

Bei Verwendung der Aktion "Deinstallieren" auf der Registerkarte Installation: Hostvorbereitung kann ein Fehler auftreten, bei dem die Nachricht `eam.issue.OrphanedAgency` in den EAM-Protokollen für die Hosts angezeigt wird. Nach Verwendung der Aktion „Beheben“ und dem Neustart der Hosts bleibt der Fehlerzustand bestehen, selbst wenn die NSX-VIBs erfolgreich deinstalliert wurden.

*Problemumgehung:* Löschen Sie die verwaiste Agency auf dem vSphere ESX Agent Manager (Verwaltung: vCenter Server-Erweiterungen: vSphere ESX Agent Manager).

**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.

Die Dienst-VM, die über die Registerkarte "Dienstbereitstellungen" auf der Installationsseite bereitgestellt wurde, wird nicht eingeschaltet

*Problemumgehung:* Befolgen Sie die unten beschriebenen Schritte.

1. Entfernen Sie die Dienst-VM manuell vom `ESX Agent`-Ressourcenpool im Cluster.
2. Klicken Sie auf **Networking and Security** und anschließend auf **Installation**.
3. Klicken Sie auf die Registerkarte **Dienstbereitstellungen**.
4. Wählen Sie den entsprechenden Dienst aus und klicken Sie auf das Symbol **Auflösen**.  
Die Dienst-VM wird neu bereitgestellt.

**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.

*Problemumgehung:* Klicken Sie auf das rote Warnsymbol und wählen Sie „Lösen“.

## Bekannte Probleme bei NSX Manager

**Neu** 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 Replikator auf dem primären NSX Manager nicht mehr funktioniert, müssen Sie die UDLR- (Universal Distributed Logical Router, universeller 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.

**Neu**Problem 1770436: Es werden Warnungen generiert, auch wenn keine doppelte IP-Adresse vorhanden ist

Manchmal meldet der Befehl `Arping`, dass die NSX Manager-IP-Adresse im Netzwerk dupliziert wurde, obwohl dies nicht der Fall ist. Dadurch wird eine Falschmeldung zu diesem Ereignis generiert.

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

**Neu**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.

**Neu**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.

**Neu**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:* Gehen Sie wie folgt vor:

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

**Neu**Problem 1713669: NSX Manager schlägt wegen einer vollen Festplatte fehl, wenn die Datenbank-tabelle `ai_useripmap` zu groß geworden ist

Die zu große Datenbank führt zu einer vollen Festplatte der NSX Manager-Appliance und zum entsprechenden NSX Manager-Fehler. Der postgres-Vorgang kann nach einem Neustart nicht gestartet werden. Die Partition `„/common“` ist voll. Dieses Problem tritt meist auf Sites mit einer großen Arbeitslast auf dem Ereignisprotokollserver (ELS, Event Log Server) und auf Sites mit hohem Guest Introspection-Datenverkehrsvolumen auf. Häufig sind davon Sites betroffen, die die identitätsbasierte Firewall (IDFW) verwenden. Weitere Informationen dazu enthält der [VMware-Knowledgebase-Artikel 2148341](#).

*Problemumgehung:* Kontaktieren Sie den VMware-Kundensupport, der Ihnen bei der Behebung dieses Problems weiterhelfen kann.

**Problem 1787542: Ausnahmen im Protokoll der sekundären NSX Manager nach einer DB-Wiederherstellung auf dem primären NSX Manager**

Nach der Wiederherstellung der DB auf dem primären NSX Manager werden wiedereingesetzte globale DFW-Abschnitte für die sekundären NSX Manager nicht angezeigt.

*Problemumgehung:* Keine. Starten Sie den betreffenden sekundären NSX Manager erneut für die Wiederherstellung.

**Neu 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:*

Führen Sie die folgenden Schritte aus:

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 1534877:** 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 1537258:** 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 1386874:** Registerkarte „Networking & Security“ wird im vSphere Web Client nicht angezeigt

Nach dem Upgrade von vSphere auf Version 6.0 wird die Registerkarte „Networking & Security“ nicht angezeigt, wenn Sie sich mit dem Root-Benutzernamen beim vSphere Web Client anmelden.

*Problemumgehung:* Melden Sie sich als „administrator@vsphere.local“ oder als beliebiger anderer vCenter-Benutzer an, der vor dem Upgrade in vCenter Server vorhanden war und dessen Rolle in NSX Manager definiert war.

**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 1477041: Auf der Übersichtsseite der virtuellen NSX Manager-Appliance wird kein DNS-Name angezeigt**

Beim Anmelden bei der virtuellen NSX Manager-Appliance weist die Zusammenfassungsseite ein Feld für den DNS-Namen auf. Dieses Feld bleibt leer, selbst wenn ein DNS-Name für die NSX Manager-Appliance festgelegt wurde.

*Problemumgehung:* Sie können den NSX Manager-Hostnamen und die Suchdomänen auf der Seite "Verwalten: Netzwerk" anzeigen.

**Problem 1492880: 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 1468613: 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:* Führen Sie die folgenden Schritte aus:

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 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 1489768: Änderung im Verhalten des NSX REST-API-Aufrufs zum Hinzufügen eines Namespace in einem Datacenter

In NSX 6.2 gibt der Aufruf `POST https://<nsxmgr-ip>/api/2.0/namespace/datacenter/REST API` eine URL mit einem absoluten Pfad zurück, zum Beispiel:

`http://198.51.100.3/api/2.0/namespace/api/2.0/namespace/datacenter/datacenter-1628/2.`

In früheren Versionen von NSX hat dieser API-Aufruf eine URL mit einem relativen Pfad zurückgegeben.

Beispiel: `/api/2.0/namespace/datacenter/datacenter-1628/2.`

*Problemumgehung:* Keine.

## Bekannte Probleme bei logischen Netzwerken und bekannte Probleme bei NSX Edge

**Neu**Problem 1825416: vApps mit Fencing schlagen in vCloud Director 8.20 nach dem Upgrade auf NSX for vSphere 6.3.x fehl

Nach dem Upgrade auf NSX 6.3.x und von NSX Edge-Gateways auf 6.3.x in vCloud Director 8.20 schlagen vApps mit Fencing fehl, und die virtuellen Maschinen in einem Netzwerk mit Fencing können nicht mit ihrem Gateway kommunizieren. Weitere Informationen dazu enthält der [VMware-Knowledgebase-Artikel 2150010](#).

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

**Neu**Problem 1781438: Auf der ESG- oder DLR-NSX Edge-Appliance zeigt der Routing-Dienst keine Fehlermeldung 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.

**Neu**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.

**Neu**Problem 1791264: Durch Doppelklicken auf eine Transportzone kann der CDO-Modus nicht aktiviert/deaktiviert werden.

Wenn Sie versuchen, den CDO-Modus auf der Seite „Übersicht“, die durch Doppelklicken auf eine Transportzone im vSphere Web Client aufgerufen wird, zu aktivieren oder zu deaktivieren, hat dies keine Auswirkungen.

*Problemumgehung:* Gehen Sie wie folgt vor:

1. Wechseln Sie mit **Installation > Vorbereitung des logischen Netzwerks > Transportzonen** zurück zur Seite mit den Transportzonen und wählen Sie die gewünschte Transportzone aus.
2. Wählen Sie aus dem Dropdown-Menü **Aktionen** die Option **CDO aktivieren/deaktivieren** aus.
3. Die ausgewählte Aktion wird wirksam.

**Neu**Problem 1773500: Ungültige Route (0.0.0.0/32) führt zum Absturz von NSX

Wenn Sie die Route 0.0.0.0/32 auf dem NSX-DLR weitergeben, wird diese Route nicht unterstützt und zurückgewiesen. Dies führt jedoch weiterhin zu einem Absturz mit violettem Diagnosebildschirm (Purple Screen of Death, PSOD), wenn die zugehörige logische Schnittstelle gelöscht und erneut mit einer IP-Adresse desselben Subnetzes hinzugefügt wird.

*Problemumgehung:* 0.0.0.0/32 ist keine gültige Route. Konfigurieren Sie diese nicht oder verwenden Sie eine Routemap, um sie zurückzuweisen.

**NeuProblem 1769941: Die L2VPN-Bridge-Tabelle wird wegen eines DLR-pMAC mit doppelter ARP-Antwort funktionsunfähig**

Der VXLAN-Trunk-Port des L2VPN-Servers auf dem Host verwirft nicht die ARP-Antwort von der virtuellen Client-Maschine mit einem pMAC als Ziel-MAC, wodurch die MAC-Tabelle der Bridge nicht mehr funktionsfähig ist, sodass der Datenverkehr verworfen wird.

*Problemumgehung:* Um dieses Problem zu umgehen, fügen Sie einen Datenverkehrsfilter für den VXLAN-Trunk-Dvport hinzu, um die ARP-Antwort für den pMAC zu verwerfen.

So fügen Sie einen Bezeichner für den Datenverkehr hinzu:

1. Wechseln Sie zum Dvport, mit dem NSX Edge verbunden ist.
2. Wechseln Sie zu „Einstellungen bearbeiten“ > „Filtern und Markieren des Datenverkehrs“.
3. Fügen Sie einen MAC-Bezeichner mit dem pMAC als Ziel hinzu.

**NeuProblem 1782321: Bei einigen NSX Edges können Split-Brain-Szenarien auftreten, auch wenn ihr Hochverfügbarkeitsstatus ordnungsgemäß angezeigt wird.**

Aufgrund einer Race Condition im Hochverfügbarkeits-Mechanismus können bei einigen NSX Edges, die auf NSX 6.2.5 oder höher aktualisiert wurden, Split-Brain-Szenarien auftreten, auch wenn ihr Hochverfügbarkeitsstatus ordnungsgemäß angezeigt wird. Dies kann auch nach der erneuten Bereitstellung des Edge auftreten.

*Problemumgehung:* Starten Sie das NSX Edge im Standbymodus neu.

**NeuProblem 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.

**NeuProblem 1771760: SNMP-Antwortpakete mit einem OID vom Typ „Counter64“ werden durch das NSX Edge verworfen, wenn NAT nicht aktiviert ist.**

Das SNMP-ALG in NSX Edge kann keine Counter64-Typen von einem SNMP-Antwortpaket verarbeiten. Das Paket wird deshalb verworfen. Als Ergebnis erhält der Client keine Antwort für die Anforderung.

*Problemumgehung:* Wenn dieses Problem auftritt, wenden Sie sich an den VMware-Kundensupport.

**NeuProblem 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.

**NeuProblem 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.

**NeuProblem 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*

**NeuProblem 1803220: VXLAN-Konnektivität mit Hosts, für die der CDO-Modus aktiviert ist, geht verloren, wenn die Verbindung von Controller zu Host nicht verfügbar ist**

Die CDO-Funktion (Controller Disconnected Operation, Betrieb mit getrenntem Controller) stellt die VXLAN-Konnektivität sicher, wenn der gesamte Controller-Cluster nicht aktiv oder nicht erreichbar ist. Wenn allerdings der Controller-Cluster aktiv ist und ein Host die Konnektivität mit ihm verliert, bleibt der Datenverkehr der Datenebene zu diesem Host von anderen Hosts, die mit dem Controller verbunden sind, eventuell weiterhin unterbrochen. In diesem Fall wurde der Host aus der VTEP-pro-VNI-Liste entfernt und die vom Remotehost gesendeten ARPs werden verworfen. Für Datenverkehr ausgehend von dem Host, der die Konnektivität mit dem Controller verloren hat, stellt die CDO-Funktion sicher, dass er das richtige Ziel erreicht.

**NeuProblem 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.

**NeuProblem 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.

**Neu**Problem 1773127: Bei Setups mit einer erheblichen Anzahl an Hosts und logischen Switches wird der Bildschirm, der die Hosts eines bestimmten logischen Switch anzeigt, nicht korrekt geladen. Wenn Sie „Logischer Switch“ > „Zugehörige Objekte“ > „Hosts“ aus Ihrem Setup mit einer erheblichen Anzahl an Hosts auswählen, kann der vSphere Web Client nach einer Wartezeit von einigen Minuten nicht geladen werden. Es wird folgende Fehlermeldung angezeigt: Für den Datendienst wurde eine Zeitüberschreitung festgestellt, da eine Backend-Aufgabe mehr als 120 Sekunden in Anspruch genommen hat. Dieses Problem tritt auf, weil der Remote-API-Aufruf für NSX Manager zu lange für die Rückgabe benötigt.

**Problemumgehung:** Sie können dieses Problem auf zweifache Weise umgehen:

- Erste Möglichkeit: Erhöhen Sie den Grenzwert für die API-Zeitüberschreitung wie im [VMware-Knowledgebase-Artikel 2040626](#) beschrieben. Nach der Erhöhung dieses Wertes müssen Sie eventuell den vSphere Web Client neu starten. Die Wahrscheinlichkeit ist hoch, dass nach der Erhöhung des Grenzwertes für die Zeitüberschreitung kein Fehler mehr auftritt. Sie müssen aber etwa zwei bis vier Minuten warten, bis die Seite erneut geladen wird.
- Zweite Möglichkeit: Wenn Sie nur die zugehörigen Hosts korrekt anzeigen möchten, wechseln Sie zu „Home“ > „Netzwerk“ > „Portgruppe“ > „Zugehörige Objekte“ > „Hosts“, um die Liste der Hosts aufzurufen, die dem logischen Switch zugeordnet sind.

**Neu**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.

**Neu**Problem 1770114: Fehlermeldung auf Clusterebene wird nach erfolgreicher Hostvorbereitung nicht gelöscht

Wenn Sie einem Cluster einen IP-Pool zuweisen, der nicht über ausreichend IP-Adressen verfügt, und dann versuchen, diesem Cluster einen Host hinzuzufügen, erhalten Sie die Fehlermeldung „Unzureichende IP-Adressen“. Auch wenn Sie dann diesem Pool zusätzliche IP-Adressen hinzufügen und dieser Cluster daraufhin weitere Hosts erhalten kann, verbleibt die Fehlermeldung auf der Clusterebene.

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

**Problem 1789088: NSX Edge bleibt hängen, wenn in der Befehlszeile die Eingabeaufforderung `grub` eingegeben wird**

NSX Edge kann eventuell nicht gestartet werden und bleibt eventuell bei der `grub`-Eingabeaufforderung der Befehlszeile hängen.

*Problemumgehung:*

- Untersuchen Sie als Erstes Folgendes:
  1. Prüfen Sie mit dem Befehl `set` die vorhandene Umgebung.
  2. Ermitteln Sie mit den Befehlen `ls` und `cat` die Datei `/boot/grub/grub.cfg` und entfernen Sie diese.
- Als Nächstes starten Sie NSX Edge manuell. Gehen Sie in der Reihenfolge vor, wie im Folgenden beschrieben (führen Sie den jeweils folgenden Schritt nur dann aus, wenn das Edge mit dem Schritt zuvor nicht startet):

```
grub> ls /boot
grub> ls /boot/grub
grub> cat /boot/grub/grub.cfg
```

3. Erfassen Sie die Hostprotokolle zu diesem Zeitpunkt (möglichst nah am Auftreten des Problems). Einige NFS-Protokolle zeigen eventuell ein NFS-Speicherproblem an.

1. Starten Sie die Edge-VM mithilfe der Option „Power-Neustart“ im vSphere Web Client neu.
2. ODER geben Sie die grub-Konfigurationsdatei erneut an. Damit soll das Menü geladen werden, wodurch das Edge sofort gestartet werden kann.  
Führen Sie bei der grub-Eingabeaufforderung den folgenden Befehl aus:

```
grub> configfile /boot/grub/grub.cfg
```

3. ODER führen Sie bei der grub-Eingabeaufforderung die folgenden Befehle aus:

```
grub> insmod ext2
grub> set root=(hd0,1)
grub> linux /boot/vmlinuz loglevel=3 root=/dev/sda1
grub> boot
```

**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 EBGP-Peers 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 1676085:** Eine Aktivierung der Edge-HA ist nicht möglich, wenn keine Ressourcenreservierung durchgeführt werden kann

Ab der Version NSX for vSphere 6.2.3 scheitert die Aktivierung der Hochverfügbarkeit (High Availability, HA) auf einem vorhandenen Edge, wenn nicht ausreichend Ressourcen für eine zweite Edge-VM-Appliance reserviert werden können. Die Konfiguration wird auf die letzte bekannte brauchbare Konfiguration zurückgesetzt. In vorherigen Versionen wird die Edge-VM, wenn die HA nach dem Scheitern der Edge-Bereitstellung und der Ressourcenreservierung aktiviert wird, trotzdem erstellt.

*Problemumgehung:* Dies ist eine erwartete Änderung des Verhaltens.

**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:* Verwenden Sie die API <https://NSX-Manager-IP-Address/api/4.0/edges/edgeld/status> mit `detailedStatus=true`.

**Problem 1556924: Der L3-Konnektivitätsverlust mit VXLAN führt zu einem „Würde blockieren“-Fehler**

Wenn die DLR-LIFs auf dem Host konfiguriert sind, der zugrunde liegende VXLAN-Layer aber nicht komplett vorbereitet wurde, kann die Konnektivität einiger DLR-LIFs beeinträchtigt sein. Einige VMs des DLR sind nicht erreichbar. Möglicherweise sind Protokolleinträge in der Art „*Failed to Create VXLAN trunk status: Would block*“ (VXLAN-Trunk-Status kann nicht erstellt werden: Würde blockieren) in der Datei `/var/log/vmkernel.log` vorhanden.

*Problemumgehung:* Sie können die LIFs löschen und dann erneut erstellen. Eine andere Möglichkeit ist ein Neustart der betroffenen ESXi-Hosts.

**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 1604514: Die Bearbeitung und Konfiguration des Standard-Gateway auf einem nicht verwalteten DLR scheitert nach dem Klicken auf „Veröffentlichen“**

Wenn ein Standard-Gateway einem nicht verwalteten DLR hinzugefügt wird, scheitert die Veröffentlichung mit der Fehlermeldung „Routing Distance wird nur von NSX Edge Version 6.2.0 und später mit bereitgestellten NSX Edge-VMs unterstützt“. Die Ursache dafür ist der Standardwert „1“ für Admin Distance in der Benutzeroberfläche.

*Problemumgehung:* Entfernen Sie den Wert „1“ für Admin Distance, der standardmäßig eingestellt ist.

**Problem 1642087: Nach der Änderung des Parameters securelocaltrafficbyip in der IPSec-VPN-Erweiterung scheitert die Weiterleitung zum Zielnetzwerk**

Bei der Verwendung eines NSX Edge Services Gateway tritt folgendes Problem auf:

- Nach der Änderung des Wertes securelocaltrafficbyip in der NSX-Benutzeroberfläche (Bildschirm „IPSec-VPN bearbeiten“) auf 0 funktioniert die Weiterleitung zu einem Remotesubnetz des IPSec-VPN-Tunnels nicht mehr
- Nach der Änderung dieses Parameters werden die korrekten Informationen für ein Remotesubnetz nicht mehr in der IP-Routing-Tabelle angezeigt

*Problemumgehung:* Deaktivieren Sie den IPSec-VPN-Dienst und aktivieren Sie ihn dann erneut. Anschließend prüfen Sie, ob die erwarteten Routing-Informationen in der Befehlszeilenschnittstelle (CLI) und in der Benutzeroberfläche angezeigt werden.

**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 1534603: 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 1534799: Langsame Konvergenz beim Herunterfahren des OSPF Area Border Router mit der höchsten IP-Adresse**

Die Konvergenz dauert sehr lang, wenn der NSX-basierte OSPF Area Border Router (ABR) mit der höchsten IP-Adresse heruntergefahren oder neu gestartet wird. Wenn ein ABR, der nicht über die numerisch höchste IP-Adresse verfügt, heruntergefahren oder neu gestartet wird, konvergiert der Datenverkehr schnell auf einen anderen Pfad. Wird jedoch der ABR mit der höchsten IP-Adresse heruntergefahren oder neu gestartet, so nimmt die erneute Konvergenz einen Zeitraum von mehreren Minuten in Anspruch. Der OSPF-Vorgang kann manuell bereinigt werden, um die Konvergenzzeit zu verringern.

**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</property>  
</systemControl>
```

**Problem 1089745: 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 1498965: 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 1494025: 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 Fehlernachricht 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 1288487:** 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 **DVSManager** 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 DVPG, auf der Trunk-vNIC verbunden 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.

## Bekannte Probleme bei Sicherheitsdiensten

**Neu**Problem 1847753: Hosts schlagen beim Abrufen von Flows für ALG-fähige Protokolle mit einem violetten Diagnosebildschirm fehl.

Nach dem Upgrade von NSX for vSphere 6.2.4 auf 6.3.0 oder 6.3.1 mit in der Umgebung aktiviertem Flow Monitoring wird für den ESXi-Host ein violetter Diagnosebildschirm angezeigt. Weitere Informationen und die Problemumgehung finden Sie im [VMware-Knowledgebase-Artikel 2149908](#).

**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

**Neu**Problem 1676043: VM wird aus der Ausschlussliste entfernt, wenn sie zweimal gleichzeitig hinzugefügt wird

Wird einer Ausschlussliste eine bestimmte VM von zwei Benutzern gleichzeitig hinzugefügt, ohne dass die Benutzeroberfläche aktualisiert wird, werden die bereits hinzugefügten VMs aus der Ausschlussliste entfernt.

*Problemumgehung:* Aktualisieren Sie die vSphere Web Client-Benutzeroberfläche, bevor Sie die virtuelle Maschine der Ausschlussliste hinzufügen.

**Neu**Problem 1770259: Im Feld `appliedTo` der DFW-Regel können nicht mehrere `appliedTo`-Objekte angegeben werden

Wenn Sie die DFW-Regel auf einen Satz von vNICs oder VMs oder auf Cluster oder Datacenter anwenden, diese veröffentlichen und dann später durch Hinzufügen zusätzlicher Objekte zum Feld `appliedTo` verändern möchten, werden die Änderungen nicht wirksam, auch wenn die Veröffentlichung durchgeführt werden kann.

*Problemumgehung:* Keine.

**Neu**Problem 1798779: Nach dem Upgrade von NSX von 6.2.x auf 6.3.0 ermöglicht die Benutzeroberfläche des vSphere Web Client irrtümlicherweise das Hinzufügen eines globalen Sicherheits-Tags

In NSX 6.3.0 wurden globale Sicherheits-Tags eingeführt. Wenn Sie versuchen einer globalen Sicherheitsgruppe, die mit der Version 6.2.x vor dem Upgrade auf NSX 6.3.0 erstellt wurde, ein solches globales Sicherheits-Tag hinzuzufügen, scheitert dieser Vorgang mit der Fehlermeldung „Das angeforderte Mitglied ist kein gültiges Mitglied“. Diese Meldung ist korrekt und weist darauf hin, dass es nicht möglich ist, einer globalen NSX 6.2.x-Sicherheitsgruppe ein globales Sicherheits-Tag hinzuzufügen. Die Benutzeroberfläche ist hier irreführend.

*Problemumgehung:* Erstellen Sie nach dem Upgrade eine globale NSX 6.3.0-Sicherheitsgruppe und fügen Sie dieser die globalen Sicherheits-Tags hinzu.

**NeuProblem 1799543:** Nach dem Upgrade von NSX 6.2.x auf NSX 6.3.0 zeigt der vSphere Web Client irrtümlicherweise globale NSX 6.2.x-Sicherheitsgruppen sowie globale Nicht-Aktiv/Standby-Sicherheitsgruppen an und ermöglicht deren Auswahl, wenn Sie die erste globale Aktiv/Standby-Sicherheitsgruppe erstellen

Wenn Sie die allererste globale Aktiv/Standby-Sicherheitsgruppe erstellen, wird in der Benutzeroberfläche des vSphere Web Client eine globale Sicherheitsgruppe angezeigt, die mit NSX 6.2.x erstellt wurde, und die auch hinzugefügt werden kann. Dieser Vorgang scheitert mit der Fehlermeldung „Das angeforderte Mitglied ist kein gültiges Mitglied“.

*Problemumgehung:* Erstellen Sie mindestens eine globale Aktiv/Standby-Sicherheitsgruppe. Das Problem wird nicht mehr auftreten, wenn Sie die nächste globale Aktiv/Standby-Sicherheitsgruppe anlegen.

**NeuProblem 1786780:** Das Neuordnen und Verschieben von Richtlinien mit der Benutzeroberfläche von Service Composer dauert sehr lange, und die CPU-Auslastung ist hoch. Wenn Sie mit der Benutzeroberfläche von Service Composer Richtlinien neu anordnen oder neu positionieren, kann dies eine sehr lange Zeit in Anspruch nehmen, und die CPU-Auslastung ist hoch.

*Problemumgehung:* Führen Sie zur Lösung des Problems die folgenden Schritte durch:

- Geben Sie der Richtlinie bei der Erstellung die passende Priorität (Gewichtung), damit diese schon im ersten Versuch an der richtigen Stelle platziert wird, sodass Sie die Richtlinien dann nicht mehr erneut anordnen müssen.
- Wenn Sie eine Richtlinie an eine andere Position verschieben müssen, bearbeiten Sie die betreffende Richtlinie und ändern Sie die Priorität (Gewichtung) in einen geeigneten Wert. So wird eine einzelne Richtlinie geändert und die Rangfolge schnell angepasst.

**NeuProblem 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 1741844:** Die Adressermittlung einer vNIC mit mehreren IP-Adressen mithilfe von ARP-Snooping führt zu einer CPU-Auslastung von 100 %.

Dieses Problem tritt auf, wenn die vNIC einer virtuellen Maschine mit mehreren IP-Adressen konfiguriert wurde und ARP-Snooping für die IP-Erkennung aktiviert wurde. Das Modul für die IP-Erkennung sendet weiter ständig vNIC-IP-Aktualisierungen an den NSX Manager, um die vNIC-IP-Zuordnung für alle VMs zu ändern, die mit mehreren IP-Adressen konfiguriert wurden.

*Problemumgehung:* Für dieses Problem gibt es keine Umgehung. Zurzeit unterstützt die Funktion für das ARP-Snooping nur eine IP-Adresse pro vNIC. Weitere Informationen finden Sie im Abschnitt [IP-Erkennung für virtuelle Maschinen](#) im *Administratorhandbuch für NSX*.

**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 1462027:** In übergreifenden vCenter NSX-Bereitstellungen werden mehrere Versionen von gespeicherten Firewallkonfigurationen auf sekundäre NSX Manager kopiert

Bei der globalen Synchronisierung werden mehrere Kopien von globalen Konfigurationen auf sekundären NSX Managern gespeichert. Die Liste der gespeicherten Konfigurationen enthält mehrere Entwürfe, die während der Synchronisierung für NSX Manager mit demselben Namen und derselben Zeit oder mit einer Zeitdifferenz von 1 Sekunde erstellt wurden.

**Problemumgehung:** Führen Sie den API-Aufruf aus, um doppelte Entwürfe zu löschen.

DELETE : <https://<nsxmgr-ip>/api/4.0/firewall/config/drafts/>

Suchen Sie die zu löschenden Entwürfe, indem Sie alle Entwürfe anzeigen:

GET: <https://<nsxmgr-ip>/api/4.0/firewall/config/drafts>

In der folgenden Beispielausgabe weisen die Entwürfe 143 und 144 denselben Namen auf und sie wurden zur selben Zeit erstellt. Sie stellen daher Duplikate dar. Ebenso weisen die Entwürfe 127 und 128 denselben Namen auf, jedoch mit einer Sekunde Zeitdifferenz. Sie stellen daher auch Duplikate dar.

```
<firewallDrafts>
  <firewallDraft id="144" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 PM GMT"
timestamp="1438816120917">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-lfd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="143" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 PM GMT"
timestamp="1438816120713">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-lfd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="128" name="AutoSaved_Wednesday, August 5, 2015 9:08:02 PM GMT"
timestamp="1438808882608">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-lfd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="127" name="AutoSaved_Wednesday, August 5, 2015 9:08:01 PM GMT"
timestamp="1438808881750">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-lfd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
</firewallDrafts>
```

**Problem 1449611:** Wenn eine Firewallrichtlinie im Service Composer aufgrund einer gelöschten Sicherheitsgruppe nicht synchronisiert ist, kann die Firewallregel nicht auf der Benutzeroberfläche korrigiert werden.

*Problemumgehung:* Auf der Benutzeroberfläche können Sie die ungültige Firewallregel löschen und sie anschließend erneut hinzufügen. Sie können auch in der API die Firewallregel korrigieren, indem Sie die ungültige Sicherheitsgruppe löschen. Synchronisieren Sie anschließend die Firewallkonfiguration: Wählen Sie **Service Composer: Sicherheitsrichtlinien** aus und klicken Sie für jede Sicherheitsrichtlinie mit verbundenen Firewallregeln auf **Aktionen** und wählen Sie **Firewallkonfiguration synchronisieren** aus. Um dieses Problem zu vermeiden, verändern Sie die Firewallregeln so, dass sie sich nicht auf Sicherheitsgruppen beziehen, bevor Sie die Sicherheitsgruppen löschen.

**Problem 1557880:** Es sind eventuell keine Schicht 2-Regeln (L2, Layer 2) vorhanden, wenn die MAC-Adresse einer virtuellen Maschine in den Regeln verändert wurde

Da die L2-Regeloptimierung standardmäßig AKTIVIERT ist, werden L2-Regeln, wenn Quell- und Zielfelder angegeben sind (keine Auswahl von „Beliebig“), nur für vNICs (oder Filter) angewendet, wenn die vNIC-MAC-Adresse mit der Quell- oder Ziel-MAC-Adressliste übereinstimmt. Für Hosts mit virtuellen Maschinen, die nicht den Quell- oder Ziel-MAC-Adressen entsprechen, werden diese L2-Regeln nicht angewendet.

*Problemumgehung:* Damit L2-Regeln auf alle vNICs (oder Filter) angewendet werden können, muss für die Quell- oder Zielfelder die Option „Beliebig“ ausgewählt werden.

**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 1557924:** Der globale logische Switch ist für die Verwendung im Feld „AppliedTo“ einer lokalen Regel der verteilten Firewall zulässig

Wenn ein globaler logischer Switch als Mitglied einer Sicherheitsgruppe benutzt wird, kann die Regel der verteilten Firewall diese Sicherheitsgruppe im Feld „AppliedTo“ verwenden. Dadurch wird indirekt die Regel auf den globalen logischen Switch angewendet. Dies sollte nicht erlaubt sein, da es zu einem nicht vorhersehbaren Verhalten dieser Regeln führen kann.

*Problemumgehung:* Keine.

**Problem 1559971:** Eine Firewall-Ausschlussliste von Cross-vCenter NSX wird nicht veröffentlicht, wenn die Firewall auf einem Cluster deaktiviert wurde

In Cross-vCenter NSX wird für alle Cluster keine Firewall-Ausschlussliste veröffentlicht, wenn die Firewall auf einem Cluster deaktiviert wurde.

*Problemumgehung:* Führen Sie eine Synchronisierung der betroffenen NSX-Edges durch.

**Problem 1407920:** Nach der Verwendung von DELETE API schlägt das erneute Veröffentlichen einer Firewallregel fehl

Wenn Sie die gesamte Firewallkonfiguration mithilfe der Methode DELETE API löschen und dann versuchen, alle Regeln erneut anhand eines zuvor gespeicherten Entwurfs der Firewallregeln zu veröffentlichen, schlägt die Regelveröffentlichung fehl.

**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 1442379: Firewallkonfiguration für Service Composer nicht synchronisiert**

Wenn in NSX Service Composer eine Firewallrichtlinie ungültig ist (z. B. wenn Sie eine Sicherheitsgruppe gelöscht haben, die aktuell in einer Firewallregel verwendet wurde), wird durch das Löschen oder Ändern einer anderen Firewallrichtlinie bewirkt, dass Service Composer nicht mehr synchronisiert ist. Es wird die Fehlermeldung `Firewallkonfiguration nicht synchronisiert` angezeigt.

*Problemumgehung:* Löschen Sie ungültige Firewallregeln und synchronisieren Sie anschließend die Firewallkonfiguration. Wählen Sie **Service Composer: Sicherheitsrichtlinien** aus und klicken Sie für jede Sicherheitsrichtlinie mit verbundenen Firewallregeln auf **Aktionen** und wählen Sie **Firewallkonfiguration synchronisieren** aus. Um dieses Problem zu vermeiden, korrigieren oder löschen Sie immer ungültige Firewallkonfigurationen, bevor Sie weitere Änderungen an der Firewallkonfiguration vornehmen.

#### **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 1620491: Der Synchronisierungsstatus auf Richtlinienenebene in Service Composer zeigt nicht den Veröffentlichungsstatus der Regeln einer Richtlinie an**

Wenn eine Richtlinie erstellt oder geändert wird, zeigt Service Composer den Status „Erfolg“ an, der sich aber nur auf den Persistenzstatus bezieht. Dieser Status sagt nichts darüber aus, ob die Regeln auf dem Host erfolgreich bereitgestellt wurden.

*Problemumgehung:* Verwenden Sie die Firewall-Benutzeroberfläche zur Anzeige des Veröffentlichungsstatus.

#### **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 fortfahren.

**Problem 1772504: Service Composer unterstützt keine Sicherheitsgruppen mit MAC Set**

Service Composer erlaubt die Verwendung von Sicherheitsgruppen in Richtlinienkonfigurationen. Für den Fall, dass eine Sicherheitsgruppe einen MAC Set enthält, akzeptiert Service Composer die entsprechende Sicherheitsgruppe ohne Warnung, es können jedoch keine Regeln für den entsprechenden MAC Set erzwungen werden. Dies ist darauf zurückzuführen, dass Service Composer auf Layer3 arbeitet und keine Layer2-Konstrukte unterstützt. Beachten Sie, dass falls eine Sicherheitsgruppe sowohl einen IP Set als auch einen MAC Set enthält, der IP Set nach wie vor wirksam ist, wohingegen der MAC Set ignoriert wird. Es kann nicht schaden, eine Sicherheitsgruppe, die einen MAC Set enthält, zu referenzieren – der Benutzer muss sich bewusst sein, dass der MAC Set ignoriert wird.

*Problemumgehung:* Falls der Benutzer beabsichtigt, Firewallregeln mithilfe eines MAC Sets zu erstellen, sollte er die Layer2-/Ethernetkonfiguration der verteilten Firewall anstelle von Service Composer verwenden.

**Problem 1718726: Synchronisation von Service Composer kann nicht erzwungen werden, wenn ein Benutzer den Abschnitt „Service Composer-Richtlinie“ mithilfe der REST-API der verteilten Firewall manuell gelöscht hat**

In einer cross-vCenter NSX-Umgebung wird jeder Versuch eines Benutzers, die Synchronisation der NSX Service Composer-Konfiguration zu erzwingen, fehlschlagen, wenn es nur einen Richtlinienabschnitt gab und dieser Richtlinienabschnitt (der über den Service Composer verwaltete Richtlinienabschnitt) zu einem früheren Zeitpunkt mit einem REST API-Aufruf gelöscht wurde.

*Problemumgehung:* Löschen Sie den über den Service Composer verwalteten Richtlinienabschnitt nicht mit einem REST API-Aufruf. (Bitte beachten Sie, dass bereits die UI das Löschen dieses Abschnittes verhindert.)

## **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](#).

**Problem 1626233: Wenn die NetX-Dienst-VM (SVM) Pakete verwirft, generiert Traceflow keine entsprechende Beobachtung**

Die Traceflow-Sitzung wird nach dem Senden des Pakets an die NetX-Dienst-VM (SVM) beendet. Wenn die SVM Pakete verwirft, generiert Traceflow keine entsprechende Beobachtung.

*Problemumgehung:* Für dieses Problem gibt es keine Umgehung. Wird das Traceflow-Paket nicht wieder eingefügt, ist davon auszugehen, dass die SVM das Paket verworfen hat.

## Bekannte Probleme bei der Lösungsinteroperabilität

**Problem 1568861:** Die NSX Edge-Bereitstellung scheitert im Zuge jeder Edge-Bereitstellung von einer vCloud Director-Zelle aus, zu welcher der vCenter-Listener nicht gehört.

Die NSX Edge-Bereitstellung scheitert im Zuge jeder Edge-Bereitstellung von einer vCloud Director-Zelle aus, zu welcher der vCenter-Listener nicht gehört. Darüber hinaus scheitern alle NSX Edge-Aktionen vom vCloud Director, inklusive einer erneuten Bereitstellung.

*Problemumgehung:* Stellen Sie ein NSX Edge von der vCloud Director-Zelle aus bereit, zu welcher der vCenter-Listener gehört.

## Bekannte Probleme von NSX Controller

**Problem 1765354:** <deployType> ist eine erforderliche Eigenschaft, wird aber nicht verwendet  
<deployType> ist eine erforderliche Eigenschaft, wird aber nicht verwendet und hat keine Bedeutung.

**Problem 1516207:** Controller werden eventuell isoliert, wenn die IPsec-Kommunikation für NSX Controller-Cluster erneut aktiviert wird

Wenn für einen NSX-Controller-Cluster die unverschlüsselte Controller-zu-Controller-Kommunikation zulässig ist (IPSec ist deaktiviert) und die IPSec-basierte Kommunikation später erneut aktiviert wird, kann es vorkommen, dass ein oder mehrere Controller aufgrund eines nicht übereinstimmenden, zuvor vereinbarten Schlüssels (Pre-Shared Key, PSK) von einem Großteil des Clusters isoliert werden. In diesem Fall ist es der NSX-API eventuell nicht mehr möglich, die IPSec-Einstellungen der Controller zu ändern.

*Problemumgehung:*

Führen Sie zur Behebung dieses Problems folgende Schritte durch:

1. Deaktivieren Sie IPSec mithilfe der NSX-API.

```
PUT /2.0/vdn/controller/node

<controllerNodeConfig>
  <ipSecEnabled>false</ipSecEnabled>
</controllerNodeConfig>
```

2. Aktivieren Sie IPSec mithilfe der NSX-API erneut.

```
PUT /2.0/vdn/controller/node

<controllerNodeConfig>
  <ipSecEnabled>true</ipSecEnabled>
</controllerNodeConfig>
```

Um dieses Problem zu vermeiden, beachten Sie die nachfolgenden Empfehlungen:

- Verwenden Sie für die Deaktivierung von IPSec immer die NSX-API. Die Verwendung der NSX Controller-CLI zur Deaktivierung von IPSec wird nicht unterstützt.
- Stellen Sie immer sicher, dass alle Controller aktiv sind, bevor Sie mit der API die IPSec-Einstellung ändern.

**Problem 1306408:** NSX Controller-Protokolle müssen nacheinander heruntergeladen werden  
NSX Controller-Protokolle können nicht alle gleichzeitig heruntergeladen werden. Selbst wenn der Download über mehrere Controller stattfindet, muss der Download über den aktuellen Controller abgeschlossen sein, bevor Sie den Download über den nächsten Controller starten. Beachten Sie, dass Sie den Download eines Protokolls nicht abbrechen können, nachdem er gestartet wurde.

*Problemumgehung:* Warten Sie, bis der Download über den aktuellen Controller abgeschlossen ist, bevor Sie den Download eines weiteren Protokolls starten.

## Behobene Probleme

### NeuIn NSX 6.3.0 behobene Probleme

Die behobenen Probleme in NSX 6.3.0 gliedern sich wie folgt:

- [In NSX 6.3.0 behobene allgemeine Probleme](#)
- [In NSX 6.3.0 behobene Probleme bei Installation und Upgrades](#)
- [In NSX 6.3.0 behobene Probleme bei NSX Manager](#)
- [In NSX 6.3.0 behobene Netzwerk- und Edge-Dienste-Probleme](#)
- [In NSX 6.3.0 behobene Probleme der Sicherheitsdienste](#)
- [In NSX 6.3.0 behobene Probleme der Lösungsinteroperabilität](#)

### In NSX 6.3.0 behobene allgemeine Probleme

**Behobenes Problem 1497389:** Benutzer mit NSX-Administratorrechten können ihre Rechte in „Enterprise-Administrator“ ändern, die eine höhere Benutzerrolle darstellt. Ab NSX 6.3.0 können Benutzer mit NSX-Administratorrechten keine Benutzer mehr verwalten. Dies ist nur Benutzern mit Enterprise-Administrator-Rechten möglich. *Problem in 6.3.0 behoben.*

**Behobene Probleme 1575342, 1719402:** Wenn in einer NSX for vSphere 6.x-Umgebung eine Dienst-VM (Service VM, SVM) migriert wird (vMotion/SvMotion), kann es zu einer Unterbrechung des Dienstes kommen oder der ESXi-Host kann abstürzen

Ab der Version 6.3.0 können Sie eine SVM nicht mehr mithilfe von vMotion/SvMotion migrieren. Die Dienst-VMs müssen für eine korrekte Ausführung auf dem Host verbleiben, auf dem sie bereitgestellt wurden.

Bisher war eine Migration auf einen anderen Host möglich. Sie wurde aber nicht unterstützt und führte zu einer Unterbrechung des Dienstes und zu Problemen mit dem Host.

Weitere Informationen dazu enthält der [VMware-Knowledgebase-Artikel 2141410](#). *Problem in 6.3.0 behoben.*

**Behobenes Problem 1708769:** Erhöhte Latenz bei SVM (Dienst-VM) nach Snapshot in NSX

Dieses Problem tritt auf, weil durch die Ausführung eines Snapshots eines Dienst-VMs (SVM) zusätzliche Netzwerklatenz verursacht werden kann. Ein Snapshot wird mitunter durch in der Umgebung ausgeführte Sicherungsanwendungen aufgerufen. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1760102:** Nach dem Löschen und erneuten Bereitstellen eines NSX Controllers zur Wiederherstellung nach einem Speicherausfall können virtuelle Maschinen gegebenenfalls nicht kommunizieren.

Im Falle eines Speicherausfalls wird ein NSX Controller für die vSphere 6.2.4/6.2.5-Umgebung gegebenenfalls in den schreibgeschützten Modus versetzt. Wenn Sie den Controller löschen und erneut bereitstellen, um diesen Zustand aufzuheben, können einige VMs unter Umständen nicht kommunizieren. Bei einem Speicherausfall eines Controllers sollte er sich nach einem Neustart nicht mehr im schreibgeschützten Modus befinden. Aktuell ist dies aber in NSX nicht der Fall. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1662842:** Guest Introspection: Die Verbindung zwischen MUX und USVM wird bei dem Versuch getrennt, nicht auflösbare Windows-SIDs aufzulösen

Der Guest Introspection-Dienst befindet sich dann im Status „Warnung“, wobei der Status jedes Guest Introspection-Modul den Status „Warnung“ abwechselnd annimmt und wieder verliert.

Netzwerkereignisse werden erst wieder an den NSX Manager übermittelt, wenn die Verbindung mit der Guest Introspection-VM wiederhergestellt wurde. Dies hat Auswirkungen sowohl auf Activity Monitoring als auch auf die ID-Firewall, wenn über den Guest Introspection-Pfad Anmeldeereignisse erkannt werden. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1752051:** Für Guest Introspection wird als Dienststatus „Nicht bereit“ gemeldet, wenn die Zeit für die Kommunikation von NSX Manager mit der USVM überschritten wird

Wenn die vorgesehene Kennwortänderung mit NSX Manager auf dem internen Nachrichtenbus (RabbitMQ) nicht durchgeführt werden kann, wird für die globale Guest Introspection-SVM eventuell eine Fehlermeldung in der Art „PLAIN-Anmeldung zurückgewiesen: Benutzer ‚usvm-admin-host-14‘ - ungültige Anmeldedaten“ angezeigt. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1716328:** Entfernen eines Host im Wartungsmodus kann später zu einem Fehler in der Clustervorbereitung führen

Wenn ein Administrator einen NSX-aktivierten ESXi-Host in den Wartungsmodus versetzt und dann aus einem vorbereiteten NSX-Cluster entfernt, kann NSX die ID-Nummer des entfernten Host nicht löschen. Nachdem die Installation in diesem Zustand ist, schlägt die Clustervorbereitung für dieses Cluster fehl, wenn in einem anderen Cluster ein anderer Host mit derselben ID vorhanden ist oder dieser Host einem anderen Cluster hinzugefügt wird. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1710624:** Ereignisprotokollserver von Windows 2008 wird als „TYPE“ von „WIN2K3“ hinzugefügt, falls serverType nicht im REST-API-Anforderungstext angegeben ist

Wenn Sie eine API-Anforderung für den EventLog-Server erstellen, wird der Server als „TYPE“ von „WIN2K3“ hinzugefügt. Wenn Sie den EventLog-Server nur für IDFW verwenden, funktioniert IDFW eventuell nicht korrekt. *Problem in 6.3.0 behoben.*

## In NSX 6.3.0 behobene Probleme bei Installation und Upgrades

**Behobenes Problem 1463767:** In einer übergreifenden vCenter-Bereitstellung befindet sich unterhalb eines lokalen Konfigurationsabschnitts möglicherweise ein globaler Konfigurationsabschnitt für die Firewall.

Wenn Sie einen sekundären NSX Manager in den eigenständigen Status (Transit) versetzen und anschließend wieder in den sekundären Status wechseln, werden alle lokalen Konfigurationsänderungen, die Sie vorgenommen haben, als sich der NSX Manager vorübergehend im eigenständigen Status befunden hat, über den Abschnitten der replizierten globalen Konfiguration aufgelistet, die vom primären NSX Manager vererbt wurden. Dies führt zur Ausgabe der Fehlermeldung `Der universelle Abschnitt muss sich oberhalb aller anderen Abschnitte auf den sekundären NSX Managern befinden.` *Problem in 6.3.0 behoben.*

**Behobenes Problem 1402307:** Wird vCenter während des NSX for vSphere-Upgradevorgangs neu gestartet, wird ein falscher Clusterstatus angezeigt

Wenn Sie während eines Upgrades eine Hostvorbereitung in einer Umgebung mit mehreren für NSX vorbereiteten Clustern durchführen und der vCenter Server neu gestartet wird, nachdem mindestens ein Cluster vorbereitet wurde, wird für die übrigen Cluster möglicherweise statt eines Updatelinks der Clusterstatus „Nicht bereit“ angezeigt. Für die Hosts in vCenter wird möglicherweise zudem „Neustart erforderlich“ angezeigt.

*Problem in 6.3.0 behoben.*

**Behobenes Problem 1495307:** Während eines Upgrades werden die L2- und L3-Firewallregeln nicht für Hosts veröffentlicht

Nach dem Veröffentlichen einer Änderung an der Konfiguration der verteilten Firewall lautet der Status sowohl auf der Benutzeroberfläche als auch in der API permanent `InProgress` und der Datei „vsfwd.log“ wird kein Protokoll für L2- oder L3-Regeln hinzugefügt. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1491820:** Im NSX Manager-Protokoll werden nach dem Upgrade auf NSX 6.2 Meldungen mit dem Text `WARN messagingTaskExecutor-7` angezeigt

Nach dem Upgrade von NSX 6.1.x auf NSX 6.2 wird das NSX Manager-Protokoll mit so oder ähnlich lautenden Meldungen überflutet: `WARN messagingTaskExecutor-7 ControllerInfoHandler:48 - Host ist unbekannt: host-15 gibt leere Liste zurück.` Dies wirkt sich nicht auf die Funktionsfähigkeit aus. *Problem in 6.3.0 behoben.*

## In NSX 6.3.0 behobene Probleme bei NSX Manager

**Behobenes Problem 1671067:** Das NSX-Plug-In wird nicht im vCenter Web Client angezeigt, wenn das ESXTOP-Plug-In ebenfalls installiert ist

Nach der Bereitstellung von NSX und einer erfolgreichen Registrierung mit vCenter wird das NSX-Plug-In im vCenter Web Client nicht angezeigt. Dieses Problem entsteht aufgrund eines Konflikts zwischen dem NSX-Plug-In und dem ESXTOP-Plug-In. *Problem in 6.3.0 behoben.*

## In NSX 6.3.0 behobene Netzwerk- und Edge-Dienste-Probleme

**Behobenes Problem 1740231:** IP-Adresse kann der Hochverfügbarkeits(HA)-Schnittstelle nicht hinzugefügt werden

Ab 6.3.0 können Sie IP-Adressen für die DLR-HA-Schnittstelle hinzufügen. Diese Funktionalität war in einigen älteren NSX-Versionen nicht verfügbar. Sie wurde wieder hinzugefügt, um die Kompatibilität mit dem API-Verhalten der DLR-HA-Verwaltungsschnittstelle zu gewährleisten. *Problem in 6.3.0 behoben*

**Behobenes Problem 1716333:** Durch die Änderung der Größe der Edge-VM oder eines Platzierungsparameters bei der Aktivierung oder Deaktivierung der Edge-Hochverfügbarkeit werden eventuell zusätzliche Edge-VMs erstellt

Wenn die Größe der Edge-VM oder eines Platzierungsparameters (wie z. B. ein Datenspeicher oder ein Ressourcenpool) geändert und gleichzeitig die Edge-Hochverfügbarkeit aktiviert oder deaktiviert wird, kann die NSX-Datenbank der verwalteten Objekte beschädigt werden, sodass Edge-VMs nicht mehr verwendet werden können. Darüber hinaus werden in einer Umgebung mit Cross-vCenter die verbleibenden Edge-VMs auf die sekundäre Site repliziert. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1717369:** Bei einer Konfiguration im HA-Modus können sowohl aktive als auch Standby-Edge-VMs auf demselben Host bereitgestellt werden

Dieses Problem kommt zustande, weil bei Vorgängen zur erneuten Bereitstellung und bei Upgrade-Vorgängen keine Anti-Affinitätsregeln erstellt und automatisch auf die vSphere-Hosts angewendet werden. Bei einer HA-Aktivierung auf einem vorhandenen Edge tritt dieses Problem nicht auf.

*Problem in 6.3.0 behoben.* Das folgende Verhalten ist das erwartete Verhalten:

- Wenn vSphere HA aktiviert ist, werden bei der erneuten Bereitstellung und bei Upgrades Anti-Affinitätsregeln für Edge-VMs eines HA-Paares erstellt.
- Wenn vSphere HA deaktiviert ist, werden keine Anti-Affinitätsregeln für Edge-VMs eines HA-Paares erstellt.

**Behobenes Problem 1675659:** Unverankerte statische Routen werden gegenüber dynamischen Routen (OSPF) bevorzugt

Eine unverankerte statische Route zur Sicherung wird falsch in die Routing-Tabelle eines Edges eingegeben, wenn die Route Redistribution aktiviert ist, auch wenn eine OSPF-Route verfügbar ist.

*Problem in 6.3.0 behoben.*

**Behobenes Problem 1733165:** IPsec verursacht u. U. das Entfernen dynamischer Routen aus der NSX Edge-Tabelle zum Weiterleiten

Wird ein über die dynamische Route erreichbares Subnetz als Remotesubnetz für die IPsec-Konfiguration verwendet, wird dieses Subnetz von NSX Edge aus der Tabelle zum Weiterleiten entfernt und nicht erneut installiert, auch nicht, nachdem dieses Subnetz aus der IPsec-Konfiguration entfernt wurde. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1663902:** Das Umbenennen einer NSX Edge-VM unterbricht den Datenverkehr durch das Edge

Das Umbenennen einer NSX Edge-VM unterbricht den Datenverkehr durch das Edge. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1624663:** Nach dem Klicken auf „Erweitertes Debugging konfigurieren“ wird die vCenter-Benutzeroberfläche aktualisiert und die Änderung wird nicht beibehalten

Nach dem Klicken auf „<Spezifische Edge-ID>“ > „Konfiguration“ > „Aktion“ > „Erweitertes Debugging konfigurieren“ wird die vCenter-Benutzeroberfläche aktualisiert und die Änderung wird nicht beibehalten. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1706429:** Kommunikationsprobleme beim Aktivieren der Hochverfügbarkeit (HA) nach der anfänglichen Bereitstellung eines logischen (verteilten) Routers können dazu führen, dass beide logischen Router-Appliances aktiv sind.

Wenn Sie einen logischen Router ohne HA bereitstellen und HA später aktivieren (durch Bereitstellen einer neuen logischen Router-Apliance) oder wenn Sie HA deaktivieren und dann wieder aktivieren, fehlt einer der logischen Router-Apliances eine verbundene Route zur HA-Schnittstelle. Dies führt dazu, dass sich beide Appliances im Zustand „aktiv“ befinden. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1542416:** Der Datenpfad funktioniert nach erneuter Bereitstellung des Edge und HA-Failover bei Teilschnittstellen 5 Minuten lang nicht

Nach erneuter Bereitstellung oder HA-Failover entsteht ein fünf Minuten langer Ausfall, wenn Teilschnittstellen verwendet werden. Das Problem wurde bei Schnittstellen nicht beobachtet. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1492547:** Die Konvergenz dauert mitunter sehr lange, wenn der NSX-basierte OSPF-Area-Border-Router mit der höchsten IP-Adresse heruntergefahren oder neu gestartet wird. Wenn ein NSSA-Area-Border-Router, der nicht über die höchste IP-Adresse verfügt, heruntergefahren oder neu gestartet wird, konvergiert der Datenverkehr schnell auf einen anderen Pfad. Wird ein NSSA-Area-Border-Router mit der höchsten IP-Adresse heruntergefahren oder neu gestartet, so nimmt die erneute Konvergenz mitunter einen Zeitraum von mehreren Minuten in Anspruch. Der OSPF-Vorgang kann manuell bereinigt werden, um die Konvergenzzeit zu verringern. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1510724:** Nach der Universal Distributed Logical Router(UDLR)-Erstellung werden die Standardrouten auf den Hosts nicht aufgefüllt

Nach einer Änderung von NSX Manager vom eigenständigen in den primären Modus zum Konfigurieren von Cross-vCenter in NSX for vSphere 6.2.x treten möglicherweise die folgenden Symptome auf:

- Beim Erstellen eines neuen UDLR werden die Standardrouten auf der Hostinstanz nicht aufgefüllt.
- Die Routen werden zwar auf dem UDLR-Kontroll-VM, aber nicht auf der Hostinstanz aufgefüllt.
- Beim Ausführen des Befehls *show logical-router host host-ID dlr Edge-ID route* werden keine Standardrouten angezeigt.

*Problem in 6.3.0 behoben.*

**Behobenes Problem 1704540:** Hohes Volumen an Aktualisierungen der MAC-Lerntabelle mit NSX L2 Bridge und LACP kann dazu führen, dass nicht genügend Arbeitsspeicher verfügbar ist

Wenn eine NSX L2 Bridge eine MAC-Adresse unter einem anderen Uplink erkennt, meldet sie den Controllern über den netcpa-Prozess eine Änderung der MAC-Lerntabelle. Netzwerkumgebungen mit LACP lernen dieselbe MAC-Adresse an mehreren Schnittstellen, was zu einem sehr hohen Volumen an Tabellenaktualisierungen und zu einer potenziellen Erschöpfung des Arbeitsspeichers führt, der vom netcpa-Prozess für die Meldung benötigt wird. Informationen hierzu finden Sie im [VMware-Knowledgebase-Artikel 2147181](#). *Problem in 6.3.0 behoben.*

**Behobenes Problem 1716545:** Eine Änderung der Appliance-Größe von Edge hat keinen Einfluss auf die CPU- und Arbeitsspeicherreservierung von Standby-Edges

Die Reservierungseinstellungen werden nur der ersten Edge-VM als Teil eines HA-Paares zugewiesen.

**Behobenes Problem 1772004:** Edge HA-Failover von Knoten 0 auf Knoten 1 nimmt mehr Zeit in Anspruch als erwartet

Ein Failover von Knoten 0 auf Knoten 1 nimmt in Edge HA-konfigurierten Umgebungen mehr Zeit in Anspruch als erwartet, der Datenverkehr-Failover von Knoten 0 auf Knoten 1 verläuft hingegen normal. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1726379:** Wenn der IP-Multicast-Bereich in den letzten drei Oktetten einen oberen Grenzwert aufweist, der 99 überschreitet, schlägt die VXLAN-Trunk-Portgruppen-Konfiguration fehl.

Wenn Sie beim Konfigurieren der Segment-ID einen Multicast-IP-Bereich erstellen, der einen oberen Grenzwert aufweist, der in den letzten drei Oktetten über 99 hinausgeht, beispielsweise 1.100.100.100, und zudem einen Multicast- oder hybriden logischen Switch mit demselben Multicast-IP-Bereich erstellen, schlägt die VXLAN-Trunk-Portgruppen-Konfiguration fehl. *Problem in 6.3.0 behoben.*

## **In NSX 6.3.0 behobene Probleme der Sicherheitsdienste**

**Behobenes Problem 1767402:** DFW-Regeln, für die „Angewendet auf“ auf eine Sicherheitsgruppe festgelegt wurde, werden nicht auf Hosts veröffentlicht.

DFW-Regeln, bei denen das Feld „Angewendet auf“ auf eine Sicherheitsgruppe festgelegt wurde, werden nicht auf ESXi-Hosts in einem neuen Cluster veröffentlicht. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1743366:** Die NSX-Schwellenwertüberwachung ist standardmäßig deaktiviert, um einen potenziellen Absturz zu vermeiden

Wenn das Firewallmodul ausgeführt wird, deaktiviert NSX die Schwellenwertüberwachung für den Arbeitsspeicher, um einen potenziellen Absturz zu vermeiden. Wenn auf dem Host ESX 6.5P01 oder ESX 6.0U3 oder höher ausgeführt wird, wird die Schwellenwertüberwachung für den Arbeitsspeicher automatisch aktiviert. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1491046:** IPv4-IP-Adresse wird nicht automatisch genehmigt

Die IPv4-IP-Adresse wird nicht automatisch genehmigt, wenn die SpoofGuard-Richtlinie in VMware NSX for vSphere 6.2.x auf „Vertrauen bei erster Nutzung“ (Trust On First Use, TOFU) festgelegt ist. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1686036:** Firewallregeln können nicht hinzugefügt, bearbeitet oder entfernt werden, wenn der Standardabschnitt gelöscht wird

Wenn der Layer2- oder Layer3-Standardabschnitt gelöscht wird, kann das Veröffentlichen einer Firewallregel fehlschlagen. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1717994:** Status-API-Abfrage für die verteilte Firewall meldet zwischenzeitlich den internen Serverfehler 500

Wird die Status-API-Abfrage für die verteilte Firewall ausgeführt, während ein neuer Host einem vorbereiteten Hostcluster hinzugefügt wird, schlägt die API-Abfrage bei einigen Versuchen mit einem internen Serverfehler 500 fehl und liefert erst dann wieder die korrekte Antwort, wenn auf dem Host mit der Installation von VIBs begonnen wird. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1717635:** Der Firewallkonfigurationsvorgang schlägt fehl, wenn mehrere Cluster in einer Umgebung vorhanden sind und parallel Änderungen vorgenommen werden

Wenn in einer Umgebung mit mehreren Clustern zwei oder mehr Benutzer dauerhaft die Firewallkonfiguration in einer engen Schleife ändern, (z. B. Hinzufügen/Löschen von Abschnitten oder Regeln), schlagen einige Vorgänge fehl, und dem Benutzer wird eine API-Antwort angezeigt, die der Folgenden ähnelt: `org.hibernate.exception.GenericJDBCException: Could not execute JDBC batch update; nested exception is javax.persistence.PersistenceException: org.hibernate.exception.GenericJDBCException: Could not execute JDBC batch update`  
*Problem in 6.3.0 behoben.*

**Behobenes Problem 1707931:** Die Reihenfolge von Distributed Firewall-Regeln ändert sich, wenn in Service Composer definierte Dienstrichtlinien vorhanden sind und wenn eine Firewallregel geändert oder mit in der Firewall-UI angewandtem Filter veröffentlicht wird

Beim Ändern der Reihenfolge, Hinzufügen oder Löschen von in Service Composer erstellten Dienstrichtlinien, nachdem unter „Networking & Security“ > „Firewall“ mindestens ein Veröffentlichungsvorgang durchgeführt wurde, ändert sich die Reihenfolge der Firewallregeln. Dies kann nicht beabsichtigte Folgen haben. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1682552:** Schwellenwertereignisse für CPU/Speicher/CPS für die verteilte Firewall werden nicht gemeldet

Selbst wenn für die Schwellenwerte der verteilten Firewall für CPU/Speicher/CPS die entsprechende Einstellung vorgenommen wurde, werden Schwellenwertereignisse beim Überschreiten von Schwellenwerten nicht gemeldet. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1620460:** NSX kann nicht verhindern, dass Benutzer im Regelabschnitt von Service Composer Regeln erstellen

Im vSphere Web Client kann die Schnittstelle der Firewall für Netzwerk und Sicherheit nicht verhindern, dass Benutzer im Service Composer-Regelabschnitt Regeln hinzufügen. Das Hinzufügen von Regeln über/unter dem Service Composer-Abschnitt durch die Benutzer sollte zulässig sein, jedoch nicht innerhalb dieses Abschnitts. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1445897:** In VMware NSX for vSphere 6.1.x und 6.2.x können Distributed-Firewall(DFW)-Regeln nicht veröffentlicht werden, nachdem das Objekt, auf das verwiesen wird, gelöscht wurde. *Problem in 6.2.3 behoben.*

**Behobenes Problem 1704661, 1739613:** Verlust der VM-Netzwerkverbindung mit folgendem Fehler: „Failed to restore PF state: Limit exceeded.“ (PF-Status konnte nicht wiederhergestellt werden. Grenzwert überschritten.)

Verlust der VM-Netzwerkverbindung mit folgendem Fehler: „Failed to restore PF state: Limit exceeded.“ (PF-Status konnte nicht wiederhergestellt werden. Grenzwert überschritten.) *Problem in 6.3.0 behoben.*

## In NSX 6.3.0 behobene Probleme der Lösungsinteroperabilität

**Behobenes Problem 1527402:** Windows-VM mit einem NSX-Netzwerk-Introspektions-Treiber verliert TCP-Konnektivität

In einer VMware NSX for vSphere 6.x-Umgebung verliert die Windows-VM mit einem NSX-Netzwerk-Introspektions-Treiber (vnetflt.sys), die mit einer USVM (Guest Introspection-SVM) verbunden ist, zeitweilig die TCP-Netzwerk-Konnektivität. *Problem in 6.3.0 behoben.*

**Behobenes Problem 1530360:** Nach einem Failover für eine NSX Manager-VM wird für Site Recovery Manager (SRM) fälschlicherweise ein Zeitüberschreitungsfehler angezeigt.

Nach einem Failover für eine NSX Manager-VM wird von SRM fälschlicherweise ein Zeitüberschreitungsfehler beim Warten auf VMware Tools angezeigt. In diesem Fall wird VMware Tools tatsächlich innerhalb eines Zeitüberschreitungsintervalls von 300 Sekunden ausgeführt. *Problem in 6.3.0 behoben.*

## Revisionsverlauf der Dokumente

2. Februar 2017: Erste Auflage für NSX 6.3.0.

3. Februar 2017: Zweite Auflage für NSX 6.3.0. Bekanntes Problem 1799543 wurde hinzugefügt.

22. Februar 2017: Dritte Auflage für NSX 6.3.0. Aktualisierte CDO-Info

27. Februar 2017: Vierte Auflage für NSX 6.3.0. Die bekannten Probleme 1808478 und 1818257 wurden hinzugefügt.

30. März 2017: Fünfte Auflage für NSX 6.3.0. Die bekannten Probleme 1474650 und 1782321 wurden hinzugefügt.

10. April 2017: Sechste Auflage für NSX 6.3.0. Der Abschnitt „Upgrade-Hinweise“ wurde ergänzt.

3. Mai 2017: Siebte Auflage für NSX 6.3.0. Informationen zur Einstellung der vCNS-Edges und von VIX wurden hinzugefügt.

2. Juni 2017: Achte Auflage für NSX 6.3.0. Die bekannten Probleme 1860583, 1781438 und 1825416 wurden hinzugefügt.

22. Juni 2017: Neunte Auflage für NSX 6.3.0. Bekanntes Problem 1847753 wurde hinzugefügt.

21. August 2017: Zehnte Auflage für NSX 6.3.0. Behobenes Problem 1463767 wurde hinzugefügt und einige frühere Probleme wurden gelöscht.

2. Oktober 2017: Elfte Auflage für NSX 6.3.0. Empfohlene Mindestversionen wurden aktualisiert.

