

Versionshinweise zu VMware NSX for vSphere 6.3.7

VMware NSX for vSphere 6.3.7 | Veröffentlicht am 15. November 2018 | Build 10667122

Siehe den [Revisionsverlauf](#) dieses Dokuments.

Inhalt dieser Versionshinweise

Diese Versionshinweise decken die folgenden Themen ab:

- [Neuigkeiten in NSX 6.3.7](#)
- [Versionen, Systemanforderungen und Installation](#)
- [Eingestellte und nicht fortgeführte Funktionalität](#)
- [Upgrade-Hinweise](#)
- [FIPS-Konformität](#)
- [Revisionsverlauf](#)
- [Behobene Probleme](#)
- [Bekannte Probleme](#)

Neuigkeiten in NSX 6.3.7

In NSX for vSphere 6.3.7 wurden einige von Kunden gemeldete Fehler behoben. Weitere Informationen dazu finden Sie unter [Behobene Probleme](#).

Versionshinweise für vorherige Versionen:

- NSX [6.3.6](#)
- NSX [6.3.5](#)
- NSX [6.3.4](#)
- NSX [6.3.3](#)
- NSX [6.3.2](#)
- NSX [6.3.1](#)
- NSX [6.3.0](#)

Versionen, Systemanforderungen und Installation

Hinweis:

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

- Die für NSX-Interoperabilität erforderliche unterstützte Mindestversion für vSphere unterscheidet sich für NSX 6.3.2 und NSX 6.3.3. Ausführliche Informationen finden Sie in der [VMware-Produkt-Interoperabilitätsmatrix](#).

| Produkt oder Komponente | Empfohlene Version |
|---------------------------------|--|
| NSX for vSphere | <p>VMware empfiehlt die neueste NSX-Version für neue Bereitstellungen.</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"> • vSphere 5.5U3 und höher • 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 VMware-Knowledgebase-Artikel 2144605. • vSphere 6.5U1 und höher. vSphere 6.5U1 behebt das Problem eines EAM-Versagens bei OutOfMemory-Fehlern. Weitere Informationen dazu enthält der VMware-Knowledgebase-Artikel 2135378. |
| 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"> • Verwenden Sie VMware Tools 10.0.9 und 10.0.12 für die Aktivierung der optionalen, in VMware Tools enthaltenen Thin Agent-Komponente des Netzwerk-Introspektions-Treibers. • Führen Sie ein Upgrade auf VMware Tools 10.0.8 und höher für die Behebung des Problems verlangsamer VMs nach dem Upgrade von VMware Tools in NSX/vCloud Networking and Security durch (siehe VMware-Knowledgebase-Artikel 2144236). • Verwenden Sie VMware Tools 10.1.0 und höher zur Unterstützung von Windows 10. • Verwenden Sie VMware Tools 10.1.10 und höher zur Unterstützung von Windows Server 2016. |
| Guest Introspection für Linux | <p>Diese NSX-Version unterstützt die folgenden Linux-Versionen:</p> <ul style="list-style-type: none"> • RHEL 7 GA (64 Bit) • SLES 12 GA (64 Bit) • Ubuntu 14.04 LTS (64 Bit) |

Systemanforderungen und Installation

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

Anweisungen zur Installation erhalten Sie im *Installationshandbuch für NSX* oder im *Installationshandbuch zu Cross-vCenter NSX*.

Eingestellte und nicht fortgeführte Funktionalität

Warnungen zum Ende der Lebensdauer und des Supports

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

- Für NSX for vSphere 6.1.x gilt als Ende der Verfügbarkeit (EOA, End of Availability) und des allgemeinen Supports (EOGS, End of General Support) der 15. Januar 2017. (Informationen hierzu finden Sie auch im [VMware-Knowledgebase-Artikel 2144769](#).)
- NSX for vSphere 6.2.x erreicht das Ende des allgemeinen Supports (End of General Support, EOGS) am 20. August 2018.
- NSX Data Security wurde entfernt: In der Version NSX 6.3.0 wurde die Funktion NSX Data Security aus dem Produkt entfernt.
- NSX Activity Monitoring (SAM) wird nicht mehr unterstützt: Ab NSX 6.3.0 wird Activity Monitoring nicht mehr in NSX unterstützt. Verwenden Sie stattdessen die Endpunktüberwachung. Weitere Informationen dazu finden Sie unter [Endpunktüberwachung](#) im *Administratorhandbuch für NSX*.
- Web Access Terminal wurde entfernt: Web Access Terminal (WAT) wurde aus NSX 6.3.0 entfernt. Sie haben nicht die Möglichkeit, Web Access SSL VPN-Plus zu konfigurieren und den Zugriff auf die öffentliche URL über NSX Edge zu aktivieren. VMware empfiehlt die Verwendung des Vollzugriffs-Clients bei SSL VPN-Bereitstellungen zur Verbesserung der Sicherheit. Wenn Sie die WAT-Funktionalität in früheren Versionen verwenden, müssen Sie diese deaktivieren, bevor Sie ein Upgrade auf 6.3.0 durchführen.
- IS-IS wurde aus NSX Edge entfernt: Ab der Version NSX 6.3.0 kann das IS-IS-Protokoll nicht mehr auf der Registerkarte Routing konfiguriert werden.
- vCNS-Edges werden nicht mehr unterstützt. Vor dem Upgrade auf NSX 6.3.x müssen Sie zuerst ein Upgrade auf ein NSX Edge durchführen.

Allgemeine Änderungen des Verhaltens

Wenn Sie über mehr als einen vSphere Distributed Switch verfügen und wenn VXLAN auf einem von ihnen konfiguriert ist, müssen Sie alle Distributed Logical Router-Schnittstellen mit Portgruppen auf diesem vSphere Distributed Switch verbinden. Ab der Version NSX 6.3.6 wird diese Konfiguration in der Benutzeroberfläche und API erzwungen. In früheren Versionen wurden Sie nicht daran gehindert, eine ungültige Konfiguration zu erstellen.

Entfernung von APIs und Änderungen des Verhaltens

Änderungen in Bezug auf die API-Fehlerbehandlung

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

- Wenn eine API-Anforderung eine Datenbankausnahme auf dem NSX Manager zur Folge hat, lautet die Antwort *500 Internal Serverfehler*. Bei früheren Versionen antwortete der NSX Manager mit *200 OK*, obwohl die Anforderung fehlschlug.
- Wenn Sie eine API-Anforderung mit einem leeren Text senden, wenn ein Anforderungstext

erforderlich ist, lautet die Antwort *400 Ungültige Anforderung*. Bei früheren Versionen antwortete der NSX Manager mit *500 Interner Serverfehler*.

- Wenn Sie in dieser API (GET /api/2.0/services/policy/securitygroup/{ID}/securitypolicies) eine falsche Sicherheitsgruppe angeben, lautet die Antwort *404 Nicht gefunden*. Bei früheren Versionen antwortete der NSX Manager mit *200 OK*.

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

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

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

Löschen der Firewallkonfiguration oder des Standardabschnitts

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

defaultOriginate-Parameter:

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

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

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

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

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

Entfernungen von CLI und Änderungen des Verhaltens

Verwenden Sie keine nicht unterstützten Befehle auf NSX Controller-Knoten

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

Upgrade-Hinweise

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

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

Allgemeine Upgrade-Hinweise

- Für das Upgrade von NSX müssen Sie ein vollständiges NSX-Upgrade einschließlich eines Hostcluster-Upgrades durchführen (wobei die Host-VIBs aktualisiert werden). Anweisungen hierzu erhalten Sie im [Upgrade-Handbuch für NSX](#) im Abschnitt [Aktualisieren der Hostcluster](#).
- **Systemvoraussetzungen:** Die Informationen zu den Systemanforderungen für die Installation und das Upgrade von NSX werden im Abschnitt [Systemvoraussetzungen für NSX](#) der NSX-Dokumentation dargestellt.
- **Upgrade-Pfad von NSX 6.x:** Die [VMware-Produkt-Interoperabilitätsmatrix](#) bietet Details zu den Upgrade-Pfaden von VMware NSX.
- Das Upgrade für Cross-vCenter NSX wird im [Upgrade-Handbuch für NSX](#) erläutert.
- **Herabstufungen werden nicht unterstützt:**
 - Führen Sie vor der Durchführung eines Upgrades immer eine Sicherung von NSX Manager durch.
 - Nach einem erfolgreichen Upgrade von NSX ist kein Downgrade von NSX möglich.
- **Zur Überprüfung, ob Ihr Upgrade auf NSX 6.3.x erfolgreich durchgeführt wurde,** erhalten Sie Erläuterungen im [Knowledgebase-Artikel 2134525](#).
- Upgrades von vCloud Networking and Security auf NSX 6.3.x werden nicht unterstützt. Sie müssen zuerst ein Upgrade auf eine unterstützte 6.2.x-Version durchführen.
- **Interoperabilität:** Überprüfen Sie vor dem Upgrade die [VMware-Produkt-Interoperabilitätsmatrix](#) für alle betreffenden VMware-Produkte.
 - **Upgrade auf vSphere 6.5a oder höher:** Wenn Sie ein Upgrade von vSphere 5.5 oder 6.0 auf vSphere 6.5a oder höher durchführen möchten, müssen Sie zuerst ein Upgrade auf NSX 6.3.x vornehmen. Weitere Informationen dazu finden Sie unter [Upgrade von vSphere in einer NSX-Umgebung](#) im [Upgrade-Handbuch für NSX](#).
Hinweis: NSX 6.2.x ist nicht mit vSphere 6.5 kompatibel.
 - **Upgrade auf NSX 6.3.3 oder höher:** Die unterstützte Mindestversion für die vSphere for NSX-Interoperabilität unterscheidet sich für NSX 6.3.2 und NSX 6.3.3. Ausführliche Informationen finden Sie in der [VMware-Produkt-Interoperabilitätsmatrix](#).
- **Kompatibilität mit Partnerdiensten:** Wenn Ihre Site VMware-Partnerdienste für Guest Introspection oder für die Netzwerk-Introspektion verwendet, müssen Sie mithilfe des [VMware-Kompatibilitäts-Handbuchs](#) vor dem Upgrade prüfen, ob der Dienst Ihres Anbieters mit dieser NSX-Version kompatibel ist.
- **Networking & Security-Plug-In:** Nach dem Upgrade von NSX Manager müssen Sie sich vom vSphere Web Client abmelden und wieder bei ihm anmelden. Wenn das NSX-Plug-In nicht ordnungsgemäß angezeigt wird, löschen Sie den Browser-Cache und den Verlauf. Wenn das Networking & Security-Plug-In nicht im vSphere Web Client angezeigt wird, setzen Sie den vSphere Web Client-Server wie im [Upgrade-Handbuch für NSX](#) beschrieben zurück.
- **Zustandsfreie Umgebungen:** Bei NSX-Updates in einer statusfreien Hostumgebung werden die neuen VIBs während des NSX-Upgrades im Vorfeld zum Host-Image-Profil hinzugefügt. Das Verfahren von NSX-Updates auf statusfreien Hosts muss daher in folgender Reihenfolge durchgeführt werden:

In Versionen vor NSX 6.2.0 wurde eine einzelne URL in NSX Manager verwendet, über die VIBs für eine bestimmte Version von ESX Host ermittelt werden konnten. (Der Administrator musste also nur eine einzige URL kennen, unabhängig von der NSX-Version.) In NSX 6.2.0 und höher sind die neuen NSX-VIBs über mehrere URLs verfügbar. Führen Sie die folgenden Schritte aus, um die richtigen VIBs zu ermitteln:

1. Suchen Sie unter `https://<NSXManager>/bin/vdn/nwfabric.properties` nach der neuen VIB-URL.
2. Rufen Sie die VIBs der erforderlichen ESX-Hostversion über die jeweilige URL ab.
3. Fügen Sie sie zu einem Image-Profil hinzu.

Upgrade-Hinweise für NSX-Komponenten

NSX Manager-Upgrade

- **Wichtiger Hinweis:** Wenn Sie ein Upgrade von NSX 6.2.0, 6.2.1 oder 6.2.2 auf NSX 6.3.5 oder höher durchführen, müssen Sie vor Beginn des Upgrades eine Problemumgehung durchführen. Details finden Sie im [VMware-Knowledgebase-Artikel 000051624](#).
- Wenn Sie SFTP für NSX-Sicherungen verwenden, ändern Sie nach dem Upgrade auf Version 6.3.x den Sicherheitsalgorithmus auf `hmac-sha2-256`, da `hmac-sha1` nicht unterstützt wird. Eine Liste der unterstützten Sicherheitsalgorithmen in 6.3.x finden Sie im [VMware-Knowledgebase-Artikel 2149282](#).
- Wenn Sie ein Upgrade von NSX 6.3.3 auf NSX 6.3.4 oder höher durchführen möchten, müssen Sie zunächst die Anweisungen zur Problemumgehung im [VMware-Knowledgebase-Artikel 2151719](#) befolgen.
- Beim Upgrade von NSX Manager auf NSX 6.3.6 oder höher wird automatisch eine Sicherung erstellt und als Teil des Upgrade-Vorgangs lokal gespeichert. Weitere Informationen finden Sie unter [NSX Manager-Upgrade](#).

Controller-Upgrade

- In NSX 6.3.3 wurde die NSX Controller-Appliance-Festplatte von 20 GB auf 28 GB vergrößert.
- Der NSX Controller-Cluster muss für ein Upgrade auf NSX 6.3.3 drei Controller-Knoten enthalten. Bei weniger als drei Controllern müssen Sie die entsprechende Anzahl an Controllern vor dem Start des Upgrades hinzufügen. Weitere Informationen finden Sie unter [Bereitstellen des NSX Controller-Clusters](#).
- In NSX 6.3.3 hat sich das zugrunde liegende Betriebssystem des NSX Controllers geändert. Bei einem Upgrade von NSX 6.3.2 oder früher auf NSX 6.3.3 oder höher wird deshalb nicht die vorhandene Software aktualisiert. Es werden stattdessen die bestehenden Controller einzeln nacheinander gelöscht und neue Photon OS-basierte Controller bereitgestellt, die dieselben IP-Adressen verwenden.

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

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

Hostcluster-Upgrade

- In NSX 6.3.3 ändern sich NSX VIB-Namen. Die `esx-vxlan`- und `esx-vsip`-VIBs werden mit `esx-nsxv` ersetzt, wenn Sie NSX 6.3.3 oder höher installiert haben.

- **Upgrade ohne Neustart und Deinstallation auf den Hosts:** Bei vSphere 6.0 und höher ist nach einem Upgrade auf NSX 6.3.x für alle nachfolgenden NSX-VIB-Änderungen kein Neustart erforderlich. Stattdessen müssen die Hosts in den Wartungsmodus wechseln, um die VIB-Änderung abzuschließen.

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

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

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

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

Bei den folgenden Aufgaben ist ein Neustart des Hosts erforderlich:

- Upgrades von NSX 6.2.x oder früher auf NSX 6.3.x (alle ESXi-Versionen).
- Upgrades von NSX 6.3.0 auf NSX 6.3.x auf ESXi 5.5.
- Installation des NSX 6.3.x-VIB, die nach dem Upgrade von ESXi von 5.5 auf Version 6.0 oder höher erforderlich ist.
- Deinstallation des NSX 6.3.x-VIB auf ESXi 5.5.

- **Host bleibt eventuell im Installationsstadium hängen:** Während umfangreicher NSX-Upgrades besteht die Gefahr, dass ein Host bei der Durchführung der Installation für längere Zeit hängen bleibt. Dies kann aufgrund von Problemen bei der Deinstallation alter NSX-VIBs auftreten. In diesem Fall wird der diesem Host zugeordnete EAM-Thread in der VI Client-Aufgabenliste als „Hängend“ vermerkt.

Problemumgehung: Gehen Sie wie folgt vor:

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

Upgrade von NSX Edge

- In NSX 6.3.0 wurden die Festplattengrößen der NSX Edge-Appliance geändert:
 - **Kompakt, Groß, Quad Large:** 1 Festplatte mit 584 MB + 1 Festplatte mit 512 MB
 - **Sehr groß:** 1 Festplatte mit 584 MB + 1 Festplatte mit 2 GB + 1 Festplatte mit 256 MB
- **Host-Cluster müssen vor dem Upgrade von NSX Edge-Appliances für NSX vorbereitet werden:** Ab 6.3.0 wird eine Kommunikation der Managementebene zwischen NSX Manager und Edge über den VIX-Kanal nicht mehr unterstützt. Es wird nur der Nachrichtenbuskanal unterstützt. Wenn Sie ein Upgrade von NSX 6.2.x oder früher auf NSX 6.3.0 oder höher durchführen, müssen Sie sicherstellen, dass die Hostcluster, auf denen NSX Edge-Appliances bereitgestellt werden, für NSX vorbereitet sind und dass für die Messaging-Infrastruktur der Status GRÜN (GREEN) gilt. Wenn die Hostcluster nicht für NSX vorbereitet sind, schlägt das Upgrade der NSX Edge-Appliance fehl. Ausführliche Informationen finden Sie unter [Upgrade von NSX Edge](#) im *Upgrade-Handbuch für NSX*.
- **Upgrade von Edge Services Gateway (ESG):** Ab Version NSX 6.2.5 wird die Ressourcenreservierung gleichzeitig mit dem NSX Edge-Upgrade vorgenommen. Wenn vSphere HA auf einem Cluster aktiviert wird, der nicht über ausreichende Ressourcen verfügt, schlägt der Upgrade-Vorgang möglicherweise fehl, da vSphere HA-Einschränkungen verletzt werden. Um derartige Upgrade-Fehler zu vermeiden, führen Sie die folgenden Schritte durch, bevor Sie ein ESG-Upgrade vornehmen:

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

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

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

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

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

Stellen Sie dabei sicher, dass die Werte für `edgeVCpuReservationPercentage` und `edgeMemoryReservationPercentage` in die verfügbaren Ressourcen für den Formfaktor passen (siehe Standardwerte in der Tabelle oben).

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

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

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

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



```
...
</applicationProfile>
```

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

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

Upgrade für Guest Introspection

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

Upgrade-Hinweise für FIPS

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

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

FIPS-Konformität

- **NSS und OpenSwan:** Das NSX Edge-IPSec-VPN verwendet das NSS-Verschlüsselungsmodul von Mozilla. Aufgrund kritischer Sicherheitsprobleme verwendet diese Version von NSX eine neuere Version von NSS, die nicht für FIPS 140-2 validiert wurde. VMware bestätigt das korrekte Funktionieren des Moduls. Es wird aber nicht mehr offiziell validiert.

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

Revisionsverlauf der Dokumente

15. November 2018: Erste Auflage.

3. März 2019: Zweite Auflage. Behobenes Problem 2249307 wurde hinzugefügt.

13. Mai 2019: Dritte Auflage. Der Abschnitt „Hostcluster-Upgrade“ wurde aktualisiert.

Behobene Probleme

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

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

Behobene Probleme bei logischen Netzwerken und NSX Edge

- **Behobenes Problem 2207483: Hohe Latenz sowohl für gerouteten O-W- als auch für gerouteten N-S-Datenverkehr**
Die Generierung von geroutetem Datenverkehr mit TxWorld von VM erfordert 100 % CPU, was zu hoher Latenz führt.
- **Behobenes Problem 2188666: Mit der SSL-VPN-Linux-Client-CLI kann keine Verbindung zu einem Gateway mit 5-stelliger Portnummer hergestellt werden**
Für die Verbindungsherstellung zu einem Gateway mit 5-stelliger Portnummer muss die SSL-VPN-Client-GUI auf Linux verwendet werden, da diese mit der GUI funktioniert. Bei bis zu 4-stelligen Portnummern funktioniert die SSL-VPN-Linux-CLI allerdings.
- **Behobenes Problem 2185457: Zunahme der Netzwerklatenz für überbrückte Arbeitslasten**
Arbeitslasten mit hohem Datenverkehr (pps) in überbrückten Netzwerken können zu einer Latenz zwischen VLAN und VXLAN führen.
- **Behobenes Problem 2182874: VDR-ID nicht möglich, wenn für Sites überlappende VDR-IDs vorhanden sind**
Der Segmentbereich einer Site musste geändert werden, wenn es beim Versuch, die Site zu Multi-vC zu überführen, bei mehr als einer Site zu einer Überlappung des Segmentbereichs kam.
- **Behobenes Problem 2181650: GARP wird beim Senden einer ARP-Anforderung zur Aktualisierung des ARP-Eintrags als gültige Antwort akzeptiert**
Einige alte Geräte senden GARP als Antwort auf eine ARP-Anforderung.
- **Behobenes Problem 2181435: In ESX 5.5 stürzt Hostd bei Statistikabfragen ab**
In ESX 5.5 stürzt Hostd bei Statistikabfragen ab. Hostd muss neu gestartet werden.
- **Behobenes Problem 2179054: Vermeiden eines IXGBE-Treiberneustarts bei NSX-Installation und -Upgrades**
Für die Dienste auf dem Host besteht ein Netzwerkausfall von 5 bis 10 Sekunden.

- **Behobenes Problem 2178950: Unterbrechung des Datenverkehrs oder mehr als zwei VMs in vCenter für denselben Edge bei Aktivierung von HA**
Unterbrechung des Datenverkehrs oder mehr als zwei VMs in vCenter für denselben Edge bei Aktivierung von HA. Wiederherstellung per Bearbeitungs-Appliances oder Änderung der Appliance-Platzierung führt zu isolierten VMs mit Netzwerkunterbrechung.
- **Behobenes Problem 2177514: In einigen Fällen kam es bei DaD zu einer Ping-Zurückleitung, sodass der DaD-Prozess doppelte IP-Adressen erkannte.**
Systemereignis meldet fälschlicherweise das Erkennen einer doppelten IP.
- **Behobenes Problem 2176316: Edge-Name wird in Firewallregel nicht aktualisiert**
Nach Ändern des Edge-Namens in der Edge-Benutzeroberfläche wird in der Benutzeroberfläche der Firewall weiter der alte Edge-Name angezeigt
- **Behobenes Problem 2172005: Die BGP-Nachbarschaft ist instabil, wenn der CLI-Befehl „show ip bgp“ ausgegeben wird**
Wenn BGP über Lernrouten mit einem AS_PATH verfügt, der länger als 126 Zeichen ist, und der Befehl „show ip bgp“ ausgegeben wird, wird der Routing-Stack neu gestartet. Routenänderung und möglicher Ausfall des Datenverkehrs, bis BGP wieder zusammengeführt wird.
- **Behobenes Problem 2171616: Vorgang mit SSL-VPN-Windows-Client stürzt ab, wenn der ESG-Hostname nicht aufgelöst werden kann**
Wenn HTTP-Proxy konfiguriert ist und der ESG-Hostname nicht aufgelöst werden kann, stürzt der Client-Vorgang ab.
- **Behobenes Problem 2167176: Bei DLR-Edges mit aktivierter HA läuft die tmpfs-Partition voll**
Das /var/run-Verzeichnis (tmpfs) läuft bei aktivierter HA komplett voll. Bei vollem Verzeichnis funktioniert keine Konfiguration mehr.
- **Behobenes Problem 2164068: tmpfs-Partition läuft bei aktivierter HA nach gewisser Zeit voll**
rsync wird verwendet, um Dateien zwischen Edge-VMs in einem HA-Paar zu synchronisieren. Aufgrund der rsync-Kompilierungsart wurden bei allen periodischen Aufrufen von rsync Fehlerprotokollbenachrichtigungen generiert, die in einer Protokolldatei auf der tmpfs-Partition gespeichert wurden. Nach einer gewissen Zeit läuft die Partition voll. Dies beeinträchtigt den regulären Edge-Betrieb signifikant.
- **Behobenes Problem 2156094: Mit der SSL-VPN-Linux-Client-CLI kann keine Verbindung zu einem Gateway mit 5-stelliger Portnummer hergestellt werden**
Für die Verbindungsherstellung zu einem Gateway mit 5-stelliger Portnummer muss die SSL-VPN-Client-GUI auf Linux verwendet werden, da diese mit der GUI funktioniert. Bei bis zu 4-stelligen Portnummern funktioniert die SSL-VPN-Linux-CLI allerdings.
- **Behobenes Problem 2152060: Speicherverlust bei Monitoring-Service-Engine (Nagios) auf Edge**
Der Lastausgleich funktioniert nicht gut, wenn die Konfiguration einen Monitoring-Service nutzt, da es zu Speicherproblemen kommt.
- **Behobenes Problem 2140512: Nach dem Upgrade auf 6.3.x oder höher führen fehlende TransportZone (vdscope)-Einträge in der MP-Datenbank zu Fehlern bei VXLAN und logischen Netzwerken**
Fehler bei VXLAN und logischen Netzwerken auf für NSX vorbereiteten Clustern.
- **Behobenes Problem 2134760: Die Installation des SSL-VPN-Mac-Clients wird erfolgreich abgeschlossen, aber die App kann nicht ausgeführt werden**
Der Client kann auch nach erfolgreicher Installation nicht geöffnet werden.
- **Behobenes Problem 2100704: NSX Edge kann in bestimmten Szenarien VMCI-Verbindungen zu NSX Manager verlieren**
Edges können nicht mehr verwaltet werden, sodass keine Konfigurationen mehr an die Edges weitergegeben werden können.

- **Behobenes Problem 2092516: Mehrere Monitoring-Mitarbeiter aktualisieren Poolmitgliedsstatus gleichzeitig**
Der Lastausgleich funktioniert nicht gut, da ein Teil des Datenverkehrs nur langsam an fehlerhaften Server versendet wird oder ein fehlerfreier Server keinen Datenverkehr zur Verarbeitung erhält.
- **Behobenes Problem 2078866: Beim Neustart des Hosts schlägt nsxv-vib in refreshHostdNetstackCache() fehl**
Der VXLAN-Rx-Durchsatz kann geringer ausfallen.
- **Behobenes Problem 2028337: Die fünf Vorgänge mit dem höchsten CPU-Verbrauch werden nicht angezeigt, wenn die Edge-CPU-Auslastung über 90 % liegt**
Wenn die Edge-CPU-Auslastung über 90 % liegt, wird eine Benachrichtigung an den Manager gesendet. Diese enthält eine Liste, die fünf Vorgänge mit dem höchsten CPU-Verbrauch seit dem Edge-Start ausweist. Diese Liste zeigt höchstwahrscheinlich nicht die fünf aktuellen Top-CPU-Benutzer, sodass die Diagnose von CPU-Auslastungsproblemen nur schwer möglich ist.
- **Behobenes Problem 1983497: Violetter Bildschirm wird angezeigt, wenn gleichzeitig ein Brücken-Failover und eine Brücken-Konfigurationsänderung erfolgen**
Wenn ein Brücken-Failover und eine Brücken-Konfigurationsänderung gleichzeitig erfolgen, kann dies zu einem Deadlock und einem violetten Bildschirm führen. Die Wahrscheinlichkeit eines Deadlocks ist gering.
- **Behobenes Problem 2181633: ARP-Unterdrückung der Teilschnittstellen-IP-Adressen von Gast-VMs schlägt fehl.**
Die ARP-Auflösung dieser Schnittstellen dauert beim ersten Mal etwas länger als üblich (1 Sekunde).
- **Behobenes Problem 2170329: DNS-Konfiguration wird nicht auf SSL-VPN-Windows-Client-Schnittstelle angewendet**
DNS-Abfrage schlägt fehl, was den Zugriff beeinträchtigt.

Allgemeine behobene Probleme

- **Behobenes Problem 2183198: Benutzeroberfläche zeigt beim Abrufen eines Ports von einem ToR-Switch ohne Port einen Fehler an**
Wenn ein physischer Switch auf einem Hardware-Gateway keinen Port hat, löst die NSX-Benutzeroberfläche einen Fehler aus, wenn der Port vom Switch aus abgerufen werden soll. In der Benutzeroberfläche wird beim Versuch, die Portinformationen abzurufen, die Fehlermeldung „Abrufen von Bestandsinformationen nicht möglich“ angezeigt.
- **Behobenes Problem 2176000: Kodierungsunterschied in von der Verwaltungsebene gesendeten und vom Host erwarteten Nachrichten führte zu ungültigen Uplink-Port-Namen von DVS und infolgedessen zu fehlerhafter MAC-Auflösung**
DLR kann Mac-Adressen von VMs auf unterschiedlichen ESXi-Hosts nicht auflösen.
- **Behobenes Problem 2170413: API /api/3.0/ai/directorygroup funktioniert nicht**
Null-Pointer-Ausnahme (NullPointerException) wird von Backend ausgelöst, und API gibt einen Fehler zurück. Workflow kann nicht automatisiert werden.
- **Behobenes Problem 2170395: domain_object ist nicht mit ai_group-Tabelle synchron**
Wenn die Service Composer-Seite geladen wird, wird die SQLGrammarException ausgelöst, da SQL eine leere Liste mit Gruppen-IDs enthält.
- **Behobenes Problem 2131680: Multicast-Pakete, die von einer Firewall-Ablehnungsregel betroffen sind, führen zu übermäßiger Protokollierung im VMkernel-Protokoll**
Bei übermäßiger Protokollierung im VMkernel-Protokoll stellt der Host die Protokollierung ein.
- **Behobenes Problem 2129177: Wenn die GI-SVM während des Upgrades im Abwärtskompatibilitätsmodus gelöscht oder entfernt wird, ist die identitätsbasierte Firewall über Guest Introspection (GI) nur funktionsfähig, wenn der GI-Cluster aktualisiert wird**

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

- **Behobenes Problem 2105632: USVMs versuchen eine Zeitsynchronisierung mit Google-NTP-Servern (extern).**
Der Dienst für die Zeitsynchronisierung wurde geändert, um dieses Verhalten zu verhindern.
- **Behobenes Problem 2003396: DLR-LIFs/Routen funktionieren nach Neustart oder Beitritt eines neuen Hosts nicht, wenn eine große Anzahl an Routen konfiguriert wird**
Die Routen werden nicht wie konfiguriert angezeigt.
- **Problem 1960383: Fehler bei der Netzwerkerstellung aufgrund einer Zeitüberschreitung, wenn eine hohe Anzahl von Bestandslistenobjekten innerhalb eines kurzen Zeitraums gelöscht werden**
Die Zeitüberschreitung bei der Netzwerkerstellung tritt aufgrund einer Verzögerung bei der DVPG-Erstellung in NSX auf.
- **Behobenes Problem 2058770: Übermäßige Anmeldeereignisse werden am vCenter ausgelöst und beim vCenter SSO-Server tritt eine hohe Last auf**
Beim vCenter SSO-Server treten übermäßig viele Anmeldeereignisse sowie eine hohe Last auf, wenn vCenter SSO-Benutzer viele NSX-API-Anforderungen in einem kurzen Zeitraum stellen. Dies kann zu schwerfälligem Verhalten führen.
- **Behobenes Problem 2046427: Änderung von Gruppierungsrichtlinie für Vmknic oder LS-DVS-Portgruppe kann zu DP-Ausfall führen**
Wenn der Benutzer während der Hostvorbereitung (VXLAN) die Gruppierungsrichtlinie für Vmknic festlegt, dann wird die Uplink-Gruppierungsrichtlinie für DVS entsprechend festgelegt. Jede neue DVS-PG eines logischen Switches, die erstellt wird, erhält auch diese Gruppierungsrichtlinie.
- **Behobenes Problem 2178339: rsyslog 8.15.0-7.ph1 hat ExecReload-Zeile in systemd-Dienstdatei entfernt, sodass die Protokollrotation für /var/log/syslog und /var/log/messages nicht ordnungsgemäß ausgeführt wird**
Dies führt dazu, dass die /var/log-Partition den Festplattenspeicher zu 100 % beansprucht, sodass keine neuen Protokolle mehr erstellt werden können.
- **Behobenes Problem 2146879: In einem eigenständigen Setup werden ToR und ToR-Bindungen bei erzwungener Synchronisierung nicht synchronisiert**
Wenn HW-Bindung oder HW-Transportknotenkonfiguration auf Verwaltungsebene und Controller nicht synchron sind, kann die Konfiguration bei einer erzwungenen Synchronisierung nicht synchronisiert werden. ToR-Konfigurationen können nicht mit dem Controller synchronisiert werden, wenn ToR-Bindungen nicht synchron sind.
- **Behobenes Problem 2146749: ESXi-Host verliert Gebietsschema-ID-Konfiguration nach dem Neustart**
Der Host erhält die falsche Gebietsschema-ID, und die entsprechenden Routen werden gelöscht.
- **Behobenes Problem 2200396: VDR-Instanzen werden nach Failover auf ESXi-Host auf sekundärer Site neu erstellt**
Unterbrechung des Datenverkehrs und Netzwerkausfall von ca. 40 Sekunden nach dem Failover.
- **Behobenes Problem 2100296: Web Client-Plug-In für NSX 6.3.5 zeigt nach Deaktivierung von SSL/TLS 1.0 auf den vCentern/PSCs keinen NSX Manager an**
Bei einer Deaktivierung von SSL/TLS 1.0 auf den vCentern unterbricht NSX die Kommunikation mit vCentern, NSX oder ESX. Die vCenter-Anwendung kommuniziert nicht mit NSX Manager.
- **Behobenes Problem 2077492: NSX Manager erstellt automatisch Ipsec-Site-ID für bereits vorhandene Ipsec-Sites**
 - NSX Manager erstellt automatisch Ipsec-Site-ID für bereits vorhandene Ipsec-Sites.
 - Bei einem NSX for vSphere-Upgrade von Version 6.2.x auf 6.3.5 oder 6.4.0a kann es zu einer

Duplizierung von Site-IDs für Ipsec-Sites kommen.

- Wenn duplizierte Site-IDs vorhanden sind, schlägt die nächste Ipsec-Konfiguration fehl.
- Es wird ein Fehler ähnlich dem Folgenden angezeigt: [13646] [Ipsec] Doppelte IDs der Ipsec-Site ipsecsite-id gefunden.
- **Behobenes Problem 2177097:** Die Verwendung des API-Aufrufs /api/2.0/vdn/config/segments zum Erstellen eines Pools mit einer Segment-ID schlägt fehl. Die Fehlermeldung „Segment-ID liegt außerhalb des Bereichs. Gültiger Bereich ist 5000 bis 16777215“ wird angezeigt
Wenn Sie die API /api/2.0/vdn/config/segments verwenden und bei der Erstellung eines Segments mit nur einem Wert denselben Start- und Endwert angeben, schlägt dies mit einer Fehlermeldung fehl.
- **Behobenes Problem 2172267:** Wenn Sie NSX Edge löschen, wenn der Host gerade nicht reaktionsfähig ist, entstehen im vCenter verwaiste Objekte
Die Edge-Instanz auf NSX Manager wird gelöscht, aber die Edge-Appliance ist nach wie vor im vCenter vorhanden und dient als Datenpfad, bis NSX Manager diesen Edge als verwaist markiert und den Edge im Rahmen eines Bereinigungsprozesses löscht. Es gibt keine Möglichkeit, die Edge-Appliance aus NSX Manager zu löschen.
- **Behobenes Problem 2097255:** SNMP-Traps werden nicht gesendet, wenn FIPS auf der NSX Manager-Appliance aktiviert ist
Es werden keine SNMP-Traps empfangen.

Behobene Probleme bei NSX Controller

- **Behobenes Problem 2181306:** Controller verfügt nicht über ausreichend Arbeitsspeicher und kann den Dienst nicht normal bereitstellen
Der Controller unterstützt eine ssh-Schnittstelle zum Abfragen von Clustermitgliedschaft und -status. Wenn ein Client darauf zugreift und die Sitzungen nicht schließt, bleiben die Sitzungen auf dem Controller unbefristet aktiv. Wenn zu viele Sitzungen geöffnet sind, verfügt der Controller nicht mehr über ausreichend Arbeitsspeicher.

Behobene Probleme beim NSX Manager

- **Behobenes Problem 2171653:** Sicherheitsprüfung auf NSX Manager meldet: „HTTP Security Header Not Detected“
Sicherheitsprüfung meldet dieses Problem. Es kann zu Clickjacking-Angriffen kommen.
- **Behobenes Problem 2161066:** Herstellen einer Verbindung zwischen Nutzungsmessung und NSX Manager schlägt fehl oder es kommt zu einem Fehler mit ungültigen XML-Zeichen, wenn eine API-Antwort verarbeitet wird
Herstellen einer Verbindung zwischen Nutzungsmessung und NSX Manager schlägt mit Fehlermeldung fehl.
- **Behobenes Problem 2145195:** Taktsignalwarnung für alle USVMs und hohe CPU-Auslastung auf NSX Manager
NSX Manager warnt, dass alle USVMs nicht auf Taktsignal reagiert haben. Die CPU-Auslastung ist hoch, was von einer postgres-Sitzung verursacht wird.
- **Behobenes Problem 2144825:** Manager-Stammpartition aufgrund zahlreicher nsx-tcserver-wrapper.log-Dateien belegt
Ein Zugriff auf die NSX-Benutzeroberfläche ist nicht möglich, und viele andere Dienste funktionieren nicht mehr, weil kein ausreichender Speicherplatz verfügbar ist.
- **Behobenes Problem 2141490:** ToR-Bindung auf NSX Manager und Controller nicht synchron
Ändern der HW-Bindung auf einem logischer Switch oder Löschen der Konfiguration nicht möglich. Benutzeroberfläche zeigt folgende Fehlermeldung an: „Der Vorgang konnte auf dem Controller nicht ausgeführt werden. {}“
- **Behobenes Problem 2066631:** Popup mit Fehlermeldung wird angezeigt, wenn eine Anmeldung als Security Administrator erfolgt und eine VM ausgewählt wird

Die Fehlermeldung „There is no authority to access object global and function library.tagging. Confirm the authority of the function and object access scope” wird als Popup angezeigt.

- **Behobenes Problem 2189810:** Mit PAN geschützte Gast-VMs verwerfen Datenverkehr, wenn von der Service Insertion-Lösung eines Drittanbieters ein API-Aufruf an NSX Manager erfolgt, alle im Rahmen der Service Insertion konfigurierten Sicherheitsgruppen/IP-Sätze abzurufen. NSX Manager gibt eine leere Konfiguration für IP-Sätze oder Sicherheitsgruppen mit IP-Sätzen zurück. Infolgedessen werden IP-Sätze oder Sicherheitsgruppen mit IP-Sätzen dem Manager des Drittanbieters als leer gemeldet. Die von PAN oder anderen Drittanbieter-Firewallgeräten geschützten Gast-VMs würden den Datenverkehr verwerfen, da keinerlei Regeln übereinstimmen, und eine Standard-Ablehnungsregel auslösen. Das Ausführen des API-Aufrufs https://NSXMgr_IP/api/2.0/si/serviceprofile/serviceprofile-10/containerset gibt keinerlei IPs für IP-Sätze oder Sicherheitsgruppen mit IP-Sätzen zurück.

Alle von PAN oder anderen Drittanbieter-Firewallgeräten geschützten Gast-VMs würden den Datenverkehr verwerfen, da keinerlei Regeln übereinstimmen, und eine Standard-Ablehnungsregel auslösen.

- **Behobenes Problem 2178700:** NSX Manager kann keinerlei VDR LIF-Informationen mit dem Controller synchronisieren, wenn eine der VDR-LIFs einen gelöschten VirtualWire verwendet. VDR LIF-Vorgänge schlagen fehl, sodass der Benutzer die LIF-Konfiguration nicht anpassen kann.
- **Behobenes Problem 2249307:** Die Gebietsschema-ID auf dem ESXi-Host wird auf den Standardwert zurückgesetzt, wenn der ESXi-Host wieder eine Verbindung zu NSX Manager herstellt.
Fehlende DLR-Routen. DLR leitet keinen Datenverkehr mehr weiter. Der Host empfängt die falsche Gebietsschema-ID, und die beabsichtigten DLR-Routen werden nicht beibehalten.

Behobene Installations- und Upgrade-Probleme

- **Behobenes Problem 2133143:** Veraltete Clustereinträge in NSX-DB
Nach einem Upgrade von 6.2.2 auf bis zu 6.2.9 sind einige veraltete Clustereinträge in der NSX-DB vorhanden.
- **Behobenes Problem 2112773:** Controller-Upgrade fehlgeschlagen
Beim Upgrade von 6.2.4 auf 6.3.6 ist ein Controller fehlgeschlagen.

Behobene Probleme bei Sicherheitsdiensten

- **Behobenes Problem 2098645:** Nullzeigerausnahme, wenn Sicherheitsgruppe über Referenz zu gelöschter AD-Gruppe verfügt
Wenn eine AD-Gruppe (ai_group) gelöscht wird und eine Sicherheitsgruppe mit Referenz auf die gelöschte AD-Gruppe vorhanden ist, gibt die Übersetzung SG->VM eine Nullzeigerausnahme aus. Die Service Composer-Seite wird nicht ordnungsgemäß geladen.
- **Behobene Probleme 2032988, 2032990 und 2032991:** Schwachstelle aufgrund von CVE-2017-5753, CVE-2017-5715 (Specter) und CVE-2017-5754 (Meltdown)
Potenzielles Sicherheitsrisiko aufgrund der folgenden Schwachstellen: CVE-2017-5753, CVE-2017-5715 (Specter) und CVE-2017-5754 (Meltdown)

Bekannte Probleme

Die bekannten Probleme gliedern sich in folgende Gruppen.

- [Bekannte Installations- und Upgrade-Probleme](#)
- [Allgemeine bekannte Probleme](#)

Bekannte Installations- und Upgrade-Probleme

- **Problem 2001988:** Während eines NSX-Hostcluster-Upgrades wechselt der Installationsstatus für den gesamten Cluster auf der Registerkarte „Hostvorbereitung“ zwischen „Nicht bereit“ und „Wird installiert“, wenn jeder Host im Cluster aktualisiert wird
Während eines NSX-Upgrades wird durch Klicken auf „Upgrade verfügbar“ ein Host-Upgrade für NSX-vorbereitete Cluster ausgelöst. Bei als „DRS FULL AUTOMATIC“ konfigurierten Clustern wechselt der Installationsstatus zwischen „Wird installiert“ und „Nicht bereit“, obwohl die Hosts im Hintergrund problemlos aktualisiert werden.

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

Allgemeine bekannte Probleme

- **Problem 2158182:** DHCP-Dienst und HA mit verbindungslokaler IP-Adresse teilen dieselbe vNic, was zu einem Verwerfen des DHCP-Erneuerungspakets führt
Wenn es sich bei der HA-Adresse um eine verbindungslokale Adresse (169.x.x.x) handelt, kann der DR ein DHCP-Unicast-Erneuerungspaket für diese verbindungslokale Adresse verwerfen. Der DHCP-Client kann die Erneuerung dann möglicherweise nicht ausführen.

Problemumgehung: Wählen Sie eine vNic ohne DHCP-Dienst als HA-Schnittstelle aus oder verwenden Sie eine routingfähige IP-Adresse als HA-Schnittstellen-IP, z. B. 192.168.x.x.

- **Problem 1467382:** Hostname des Netzwerks kann nicht bearbeitet werden
Nachdem Sie sich bei der virtuellen NSX Manager-Appliance angemeldet haben und zu Appliance Management navigiert sind, auf die Einstellungen „Appliance verwalten“ und dann auf „Netzwerk“ unter „Einstellungen“ geklickt haben, um den Hostnamen des Netzwerks zu verwalten, erhalten Sie möglicherweise einen Fehler in Bezug auf eine ungültige Domänennamenliste. Dies geschieht, wenn die im Feld „Suchdomänen“ angegebenen Domänennamen durch Leerraumzeichen anstatt durch Kommas getrennt sind. NSX Manager akzeptiert nur Domänennamen, die durch Kommas getrennt sind.

Problemumgehung:

1. Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
 2. Klicken Sie unter „Appliance-Verwaltung“ auf „Appliance-Einstellungen verwalten“.
 3. Klicken Sie im Fensterbereich „Einstellungen“ auf „Netzwerk“.
 4. Klicken Sie neben „DNS-Server“ auf „Bearbeiten“.
 5. Ersetzen Sie im Feld „Suchdomänen“ alle Leerraumzeichen durch Kommas.
 6. Klicken Sie auf „OK“, um die Änderungen zu speichern.
- **Problem 1849042/1849043:** Das Administratorkonto wird gesperrt, wenn der Ablauf von Kennwörtern auf der NSX Edge-Appliance konfiguriert ist
Wenn für den Admin-Benutzer auf der NSX Edge-Appliance der Ablauf von Kennwörtern konfiguriert ist, wird der Benutzer nach dem Ablauf des Kennworts in einem Zeitraum von sieben Tagen zur Änderung des Kennworts aufgefordert, wenn er sich bei der Appliance anmeldet. Kommt es beim Ändern des Kennworts zu Fehlern, wird das Konto gesperrt. Wenn darüber hinaus das Kennwort zum Zeitpunkt der Anmeldung an der CLI-Eingabeaufforderung geändert wird, erfüllt das neue Kennwort eventuell nicht die Richtlinie für sichere Kennwörter, die von der Benutzeroberfläche und REST erzwungen wird.

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

- **Problem 2204383:** SSL-VPN-Linux-Client kann Serverzertifikat für Linux-Versionen mit sql cert9.db nicht verifizieren
Servervalidierung schlägt mit internem Fehler fehl.

Problemumgehung: Keine.

