Upgrade-Handbuch für NSX

Update 9
Geändert am 16. November 2017
VMware NSX for vSphere 6.3

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

https://docs.vmware.com/de/

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Upgrade-Handbuch für NSX

Im *Upgrade-Handbuch für NSX* wird das Durchführen von Upgrades für das VMware NSX® for vSphere®-System mithilfe der NSX Manager-Benutzeroberfläche und des vSphere Web Client beschrieben. Zu den bereitgestellten Informationen gehören schrittweise Anleitungen für das Upgrade sowie empfohlene Vorgehensweisen.

Zielgruppe

Dieses Handbuch ist für alle Benutzer gedacht, die NSX in einer VMware vCenter-Umgebung aktualisieren oder verwenden möchten. Die Informationen in diesem Handbuch sind für erfahrene Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und dem Betrieb virtueller Datencenter vertraut sind. Dieses Handbuch setzt voraus, mit VMware vSphere, einschließlich VMware ESXi, vCenter Server und dem vSphere Web Client vertraut zu sein.

VMware Technical Publications – Glossar

VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter http://www.vmware.com/support/pubs.

Lesen der unterstützenden Dokumente

Zusätzlich zu diesem Upgrade-Handbuch veröffentlicht VMware zahlreiche weitere Dokumente über den Upgrade-Vorgang.

Versionshinweise

Lesen Sie die Versionshinweise, bevor Sie mit dem Upgrade beginnen. Bekannte Probleme bei Upgrades und entsprechende Umgehungen sind in den Versionshinweisen zu NSX dokumentiert. Wenn Sie die Upgrade-Probleme durchlesen, bevor Sie mit dem Upgrade-Vorgang beginnen, können Sie Zeit und Mühe sparen. Weitere Informationen dazu finden Sie unter https://www.vmware.com/support/pubs/nsx_pubs.html.

Produkt-Interoperabilitätsmatrix

Stellen Sie die Interoperabilität mit anderen VMware-Produkten wie z. B. vCenter sicher. Weitere Erläuterungen finden Sie in der VMware-Produkt-Interoperabilitätsmatrix unter http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php in der Registerkarte **Interoperabilität (Interoperability)**.

Stellen Sie sicher, dass der Upgrade-Pfad von Ihrer aktuellen NSX-Version auf die Version, auf die Sie ein Upgrade durchführen möchten, unterstützt wird. Wählen Sie auf der Registerkarte **Upgrade-Pfad (Upgrade Path)** im Produktmenü die Option **VMware NSX** aus.

Kompatibilitätshandbuch

Überprüfen Sie die Kompatibilität der Partnerlösungen mit NSX im VMware Kompatibilitätshandbuch unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.

Systemvoraussetzungen für NSX

Bevor Sie NSX installieren oder aktualisieren, prüfen Sie Ihre Netzwerkkonfiguration und -ressourcen. Sie können einen NSX Manager pro vCenter Server, eine Guest Introspection-Instanz pro ESXi™-Host und mehrere NSX Edge-Instanzen pro Datencenter installieren.

Hardware

Diese Tabelle enthält die Hardwareanforderungen für NSX-Appliances.

Tabelle 1. Hardwareanforderungen für Appliances

Appliance	Arbeitsspeicher	vCPU	Festplattenspeicher
NSX Manager	16 GB (24 GB für größere NSX-Bereitstellungen)	4 (8 für größere NSX-Bereitstellungen)	60 GB
NSX Controller	4 GB	4	28 GB

Tabelle 1. Hardwareanforderungen für Appliances (Fortsetzung)

Appliance	Arbeitsspeicher	vCPU	Festplattenspeicher
NSX Edge	■ Kompakt: 512 MB ■ Groß: 1 GB ■ Quad Large: 2 GB ■ Sehr groß: 8 GB	■ Kompakt: 1 ■ Groß: 2 ■ Quad Large: 4 ■ Sehr groß: 6	■ Kompakt, Groß, Quad Large: 1 Datenträger 584 MB + 1 Datenträger 512 MB ■ Sehr groß: 1 Datenträger 584 MB + 1 Datenträger 2 GB + 1 Datenträger 256 MB
Guest Introspection	2 GB	2	5 GB (bereitgestellter Speicherplatz: 6,26 GB)

Als allgemeine Richtlinie gilt: Erhöhen Sie die NSX Manager-Ressourcen auf 8 vCPU und 24 GB RAM, wenn Ihre von NSX verwaltete Umgebung mehr als 256 Hypervisoren oder mehr als 2.000 VMs umfasst.

Um spezifische Details zur Größe zu erhalten, wenden Sie sich an den Support von VMware.

Informationen zur Erhöhung der Arbeitsspeicher- und vCPU-Zuteilung für Ihre virtuellen Appliances finden Sie unter „Zuteilen von Arbeitsspeicherressourcen“ und „Ändern der Anzahl virtueller CPUs “ in der Dokumentation *Verwaltung virtueller vSphere-Maschinen*.

Der bereitgestellte Speicherplatz für eine Guest Introspection-Appliance zeigt 6,26 GB für Guest Introspection an. Dies liegt daran, dass vSphere ESX Agent Manager einen Snapshot von der Dienst-VM erstellt, um schnelle Klone zu erstellen, wenn mehrere Hosts in einem Cluster Speicher gemeinsam nutzen. Weitere Informationen zum Deaktivieren dieser Option über ESX Agent Manager finden Sie in der *ESX Agent Manager*-Dokumentation.

Software

Die neuesten Interoperabilitätsinformationen finden Sie in den Produkt-Interoperabilitätsmatrizen unter http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Informationen zu den empfohlenen Versionen von NSX, vCenter Server und ESXi finden Sie in den Versionshinweisen unter https://www.vmware.com/support/pubs/nsx_pubs.html und https://kb.vmware.com/kb/2144295.

Beachten Sie, dass die folgenden Bedingungen erfüllt sein müssen, damit ein NSX Manager in einer Cross-vCenter NSX-Bereitstellung teilnehmen kann:

Komponente	Version
NSX Manager	6.2 oder höher
NSX Controller	6.2 oder höher
vCenter Server	6.0 oder höher
ESXi	■ ESXi 6.0 oder höher ■ Mit NSX 6.2 oder späteren VIBs vorbereitete Hostcluster

Um alle NSX Manager in einer Cross-vCenter NSX-Bereitstellung von einem einzigen vSphere Web Client aus verwalten zu können, müssen Sie Ihre vCenter Server-Instanzen im erweiterten verknüpften Modus verbinden. Erläuterungen dazu finden Sie unter „Verwenden des erweiterten verknüpften Modus“ in der Dokumentation *vCenter Server und Hostverwaltung*.

Informationen zur Überprüfung der Kompatibilität von Partnerlösungen mit NSX finden Sie im „VMware Kompatibilitätshandbuch für Networking & Security“ unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.

Client- und Benutzerzugriff

- Wenn Sie ESXi-Hosts nach Namen zur vSphere-Bestandsliste hinzugefügt haben, stellen Sie sicher, dass die Namensauflösung vorwärts und rückwärts funktioniert. Andernfalls kann NSX Manager die IP-Adressen nicht auflösen.
- Berechtigungen zum Hinzufügen und Einschalten von virtuellen Maschinen
- Zugriff auf den Datenspeicher, in dem Dateien für virtuelle Maschinen gespeichert werden, sowie Kontoberechtigungen zum Kopieren von Dateien in diesen Datenspeicher
- Cookies in Ihrem Webbrowser aktiviert, um auf die NSX Manager-Benutzeroberfläche zugreifen zu können
- Stellen Sie in NSX Manager sicher, dass die ESXi-Hosts, vCenter Server und die bereitzustellenden NSX-Appliances auf Port 443 zugreifen können. Dieser Port wird zum Herunterladen der OVF-Datei auf dem ESXi-Host für die Bereitstellung benötigt.
- Ein für die von Ihnen verwendete Version von vSphere Web Client unterstützter Webbrowser. Ausführliche Informationen erhalten Sie unter „Verwenden des vSphere Web Client“ in der Dokumentation *vCenter Server und Hostverwaltung*.

Für NSX erforderliche Ports und Protokolle

Für einen ordnungsgemäßen Betrieb von NSX müssen die folgenden Ports geöffnet sein.

Tabelle 2. Für NSX erforderliche Ports und Protokolle

Quelle	Ziel	Port	Protokoll	Zweck	Sensibel	TLS	Authentifizierung
Client-PC	NSX Manager	443	TCP	Verwaltungsschnittstelle von NSX Manager	Nein	Ja	PAM-Authentifizierung
Client-PC	NSX Manager	80	TCP	VIB-Zugang für NSX Manager	Nein	Nein	PAM-Authentifizierung
ESXi-Host	vCenter Server	443	TCP	Vorbereitung des ESXi-Hosts	Nein	Nein	
vCenter Server	ESXi-Host	443	TCP	Vorbereitung des ESXi-Hosts	Nein	Nein	
ESXi-Host	NSX Manager	5671	TCP	RabbitMQ	Nein	Ja	RabbitMQ-Benutzer/Kennwort

Tabelle 2. Für NSX erforderliche Ports und Protokolle (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Zweck	Sensibel	TLS	Authentifizierung
ESXi-Host	NSX Controller	1234	TCP	UWAC (User World Agent Connection)	Nein	Ja	
NSX Controller	NSX Controller	2878, 2888, 3888	TCP	Controller-Cluster – Statussynchronisierung	Nein	Ja	IPsec
NSX Controller	NSX Controller	7777	TCP	RPC-Port für die Kommunikation zwischen Controllern	Nein	Ja	IPsec
NSX Controller	NSX Controller	30865	TCP	Controller-Cluster – Statussynchronisierung	Nein	Ja	IPsec
NSX Manager	NSX Controller	443	TCP	Kommunikation zwischen Controller und Manager	Nein	Ja	Benutzer/Kennwort
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	Nein	Ja	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	Nein	Ja	
NSX Manager	ESXi-Host	443	TCP	Verwaltungs- und Bereitstellungsverbindung	Nein	Ja	
NSX Manager	ESXi-Host	902	TCP	Verwaltungs- und Bereitstellungsverbindung	Nein	Ja	
NSX Manager	DNS-Server	53	TCP	DNS-Client-Verbindung	Nein	Nein	
NSX Manager	DNS-Server	53	UDP	DNS-Client-Verbindung	Nein	Nein	
NSX Manager	Syslog-Server	514	TCP	Syslog-Verbindung	Nein	Nein	
NSX Manager	Syslog-Server	514	UDP	Syslog-Verbindung	Nein	Nein	
NSX Manager	NTP-Zeitserver	123	TCP	NTP-Client-Verbindung	Nein	Ja	
NSX Manager	NTP-Zeitserver	123	UDP	NTP-Client-Verbindung	Nein	Ja	
vCenter Server	NSX Manager	80	TCP	Hostvorbereitung	Nein	Ja	
REST-Client	NSX Manager	443	TCP	NSX Manager-REST-API	Nein	Ja	Benutzer/Kennwort

Tabelle 2. Für NSX erforderliche Ports und Protokolle (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Zweck	Sensibel	TLS	Authentifizierung
VXLAN Tunnel End Point (VTEP)	VXLAN Tunnel End Point (VTEP)	8472 (Standard vor NSX 6.2.3) oder 4789 (Standard in neuen Installationen von NSX 6.2.3 und höher)	UDP	Transportnetzwerk-Kapselung zwischen VTEPs	Nein	Ja	
ESXi-Host	ESXi-Host	6999	UDP	ARP auf VLAN-LIFs	Nein	Ja	
ESXi-Host	NSX Manager	8301, 8302	UDP	DVS-Synchronisierung	Nein	Ja	
NSX Manager	ESXi-Host	8301, 8302	UDP	DVS-Synchronisierung	Nein	Ja	
Guest Introspection-VM	NSX Manager	5671	TCP	RabbitMQ	Nein	Ja	RabbitMQ-Benutzer/Kennwort
Primärer NSX Manager	Sekundärer NSX Manager	443	TCP	Globaler Synchronisierungsdienst für Cross-vCenter NSX	Nein	Ja	
Primärer NSX Manager	vCenter Server	443	TCP	vSphere-API	Nein	Ja	
Sekundärer NSX Manager	vCenter Server	443	TCP	vSphere-API	Nein	Ja	
Primärer NSX Manager	Globaler NSX Controller-Cluster	443	TCP	NSX Controller-REST-API	Nein	Ja	Benutzer/Kennwort
Sekundärer NSX Manager	Globaler NSX Controller-Cluster	443	TCP	NSX Controller-REST-API	Nein	Ja	Benutzer/Kennwort
ESXi-Host	Globaler NSX Controller-Cluster	1234	TCP	Protokoll der NSX-Steuerungskomponente	Nein	Ja	

Tabelle 2. Für NSX erforderliche Ports und Protokolle (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Zweck	Sensibel	TLS	Authentifizierung
ESXi-Host	Primärer NSX Manager	5671	TCP	RabbitMQ	Nein	Ja	RabbitMQ-Benutzer/Kennwort
ESXi-Host	Sekundärer NSX Manager	5671	TCP	RabbitMQ	Nein	Ja	RabbitMQ-Benutzer/Kennwort

Ports für Cross-vCenter NSX und den erweiterten verknüpften Modus

Wenn Sie über eine Cross-vCenter NSX-Umgebung verfügen und Ihre vCenter Server-Systeme sich im erweiterten verknüpften Modus befinden, muss jede NSX Manager-Appliance über die erforderliche Konnektivität mit den vCenter Server-Systemen in der Umgebung verfügen, um alle NSX Manager aus beliebigen vCenter Server-Systemen verwalten zu können.

Aktualisieren von NSX

1

Dieses Kapitel behandelt die folgenden Themen:

- Vorbereiten des NSX-Upgrades
- Upgrade auf NSX 6.3.x
- Upgrade auf NSX 6.3.x mit Cross-vCenter NSX

Vorbereiten des NSX-Upgrades

Um ein erfolgreiches NSX-Upgrade sicherzustellen, überprüfen Sie die Versionshinweise auf Upgrade-Probleme, stellen Sie sicher, dass Sie die korrekte Upgrade-Reihenfolge einhalten, und stellen Sie zudem sicher, dass die Infrastruktur ordnungsgemäß für das Upgrade vorbereitet ist.

Vorsicht Herabstufungen werden nicht unterstützt:

- Führen Sie vor der Durchführung eines Upgrades immer eine Sicherung von NSX Manager durch.
- Nach einem erfolgreichen Upgrade von NSX Manager kann NSX nicht herabgestuft werden.

VMware empfiehlt, die Upgrade-Tätigkeiten in einem von Ihrem Unternehmen definierten Wartungsfenster durchzuführen.

Die folgenden Richtlinien können als eine Vor-Upgrade-Checkliste verwendet werden.

1. Stellen Sie sicher, dass vCenter die Systemanforderungen für NSX erfüllt. Siehe Systemvoraussetzungen für NSX.
2. Wenn Guest Introspection-Partnerdienste oder Partnerdienste zur Netzwerkerweiterbarkeit bereitgestellt wurden, müssen Sie vor dem Upgrade die Kompatibilität überprüfen:
   - Unter den meisten Umständen kann ein NSX-Upgrade ohne Einfluss auf Partnerlösungen durchgeführt werden. Wenn Ihre Partnerlösung jedoch nicht mit der NSX-Version kompatibel ist, auf die Sie das Upgrade durchführen, müssen Sie vor dem NSX-Upgrade ein Upgrade der Partnerlösung auf eine kompatible Version durchführen.
   - Informieren Sie sich im VMware-Kompatibilitätshandbuch für Networking and Security. Weitere Informationen dazu finden Sie unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.

- Informieren Sie sich über Kompatibilitäts- und Upgrade-Details in der Partnerdokumentation.

3 Wenn Data Security in Ihrer Umgebung vorhanden ist, deinstallieren Sie diese Komponente, bevor Sie ein NSX-Upgrade durchführen. Data Security wird in NSX 6.3.x nicht unterstützt. Siehe Deinstallieren von NSX Data Security.

4 Wenn in Ihrer Umgebung ein Hardware-Gateway (Hardware-VTEP) installiert ist, kann kein Upgrade auf NSX 6.3.0 und 6.3.1 durchgeführt werden. Wenden Sie sich an VMware, um mit dem Upgrade fortzufahren. Weitere Informationen hierzu finden Sie unter https://kb.vmware.com/kb/2148511. Ein Upgrade auf NSX 6.3.2 ist zulässig.

5 Wenn Sie über NSX Edge-Appliances der Version NSX 5.5 oder früher verfügen, müssen Sie dafür ein Upgrade auf NSX 6.x durchführen, bevor Sie ein Upgrade auf NSX 6.3.x vornehmen.

6 Wenn Sie ein Upgrade auf NSX 6.3.3 durchführen, muss der NSX Controller-Cluster drei Controllerknoten enthalten. Sind weniger als drei vorhanden, müssen Sie vor Beginn des Upgrades weitere Knoten hinzufügen. Schritte zum Hinzufügen von Controllerknoten finden Sie unter „Bereitstellen von NSX Controller-Clustern“ im *Installationshandbuch für NSX*.

7 Planen Sie ein Upgrade für alle NSX Manager, die mit vCenter Server-Systemen verbunden sind, die den gleichen SSO-Server für dasselbe Wartungsfenster (einschließlich vCenter Server-Systemen im erweiterten verknüpften Modus), verwenden. Wenn das nicht möglich ist, finden Sie dafür unter https://kb.vmware.com/kb/2127061 eine Problemumgehung.

8 Stellen Sie sicher, dass Sie über eine aktuelle Sicherung der NSX Manager vCenter- und anderen NSX-Komponenten verfügen. Weitere Informationen dazu finden Sie unter Sichern und Wiederherstellen von NSX.

9 Erstellen Sie ein Tech-Support-Paket.

10 Stellen Sie sicher, dass die Auflösung des Domänennamens mit dem Befehl nslookup vorwärts und rückwärts funktioniert.

11 Wenn VUM in dieser Umgebung verwendet wird, stellen Sie sicher, dass das Flag bypassVumEnabled in vCenter auf „Wahr“ gesetzt ist. Diese Einstellung konfiguriert den EAM so, dass die VIBs direkt auf den ESXi-Hosts installiert werden, auch wenn der VUM installiert und/oder nicht verfügbar ist. Siehe http://kb.vmware.com/kb/2053782.

12 Laden Sie das Upgrade-Paket herunter, stellen Sie es bereit und überprüfen Sie es mit md5sum. Weitere Informationen dazu finden Sie unter Herunterladen des NSX-Upgrade-Pakets und Überprüfen der MD5-Prüfsumme.

13 Es wird empfohlen, alle Operationen in der Umgebung einzustellen, bis alle Abschnitte des Upgrades vollständig ausgeführt sind.

14 Schalten Sie keine NSX-Komponenten oder -Appliances aus und löschen Sie diese nicht, bevor Sie dazu aufgefordert werden.

Überprüfen der Lizenzanforderungen beim Upgrade von NSX

NSX hat im Mai 2016 ein neues Lizenzmodell eingeführt.

Wenn Sie ein Upgrade von NSX 6.2.2 oder früher auf NSX 6.2.3. oder höher durchführen und über einen gültigen Support-Vertrag verfügen, wird Ihre vorhandene Lizenz in eine NSX-Enterprise-Lizenz umgewandelt. Es steht Ihnen dann dieselbe Funktionalität wie beim Enterprise-Angebot zur Verfügung.

Informationen zu den NSX-Lizenzierungseditionen und zugehörigen Funktionen finden Sie unterhttps://kb.vmware.com/kb/2145269.

Operative Auswirkungen von NSX-Upgrades

Der Upgrade-Vorgang für NSX kann einige Zeit in Anspruch nehmen. Es ist wichtig, den Betriebszustand von NSX-Komponenten bei einem Upgrade zu kennen, z. B. wenn einige, aber nicht alle Hosts aktualisiert wurden oder wenn NSX Edges noch nicht aktualisiert wurden.

VMware empfiehlt, dass Sie das Upgrade aller NSX-Komponenten in einem einzelnen Ausfallfenster durchführen, um die Ausfallzeit zu minimieren und Irritationen unter den NSX-Benutzern zu vermeiden, die während des Upgrades nicht auf bestimmte NSX-Verwaltungsfunktionen zugreifen können. Wenn Ihre Standortanforderungen Sie allerdings daran hindern, das Upgrade in einem einzelnen Ausfallfenster durchzuführen, können die nachfolgenden Informationen dazu beitragen, dass Ihre NSX-Benutzer verstehen, welche Funktionen während des Upgrades zur Verfügung stehen.

Ein NSX-Bereitstellungs-Upgrade läuft wie folgt ab:

NSX Manager —> NSX Controller Cluster —> NSX-Hostcluster —> Verteilte (logische) Router —> Guest Introspection

Edge Services Gateways können jederzeit nach dem Upgrade von NSX Manager aktualisiert werden.

Wichtig Lesen Sie vor dem Start des Upgrades Vorbereiten des NSX-Upgrades und *Versionshinweise zu NSX for vSphere* für detaillierte Informationen zu den Upgrade-Voraussetzungen und bekannten Upgrade-Problemen.

NSX Manager-Upgrade

Planen des NSX Manager-Upgrades:

- In einer Cross-vCenter NSX-Umgebung sollten Sie zunächst ein Upgrade für den primären NSX Manager und anschließend für die sekundären NSX Manager durchführen.
- In einer Cross-vCenter NSX-Umgebung müssen alle NSX Manager in demselben Wartungsfenster aktualisiert werden.
- Wenn Sie ein Upgrade von NSX 6.1.x auf NSX 6.2.x oder höher durchführen, müssen Sie NSX Manager und den NSX Controller-Cluster im selben Wartungsfenster aktualisieren.

Auswirkungen während des NSX Manager-Upgrades:

- Die NSX Manager-Konfiguration mithilfe von vSphere Web Client und API ist blockiert.

- Die vorhandene VM-Kommunikation funktioniert weiter einwandfrei.
- Die neue VM-Bereitstellung funktioniert weiter in vSphere, aber die neuen virtuellen Maschinen können während des NSX Manager-Upgrades nicht mit NSX verbunden oder von logischen Switches getrennt werden.
- Bei einem Upgrade von NSX Manager in einer Cross-vCenter NSX-Umgebung dürfen Sie keine Änderungen an globalen Objekten vornehmen, bis der primäre NSX Manager und alle sekundären NSX Manager aktualisiert sind. Dazu gehört das Erstellen, Aktualisieren oder Löschen von globalen Objekten und Vorgänge, die globale Objekte betreffen (z. B. das Anwenden eines globalen Sicherheits-Tags für eine virtuelle Maschine).

Nach dem NSX Manager-Upgrade:

- Alle NSX-Konfigurationsänderungen sind zulässig.
- Wenn in dieser Phase neue NSX Controller-Appliances bereitgestellt werden, erfolgt deren Bereitstellung mit der Version des vorhandenen NSX Controller-Clusters, bis ein Upgrade des NSX Controller-Clusters erfolgt.
- Änderungen an der vorhandenen NSX-Konfiguration sind zulässig. Neue logische Switches, logische Router und Edge-Service-Gateways können bereitgestellt werden.
- Wenn bei einer verteilten Firewall neue Funktionen nach dem Upgrade eingeführt werden, können diese in der Benutzeroberfläche erst dann konfiguriert werden (sie werden abgeblendet dargestellt), wenn alle Hosts aktualisiert wurden.
- Je nach NSX Manager-Version wird nach dem Upgrade von NSX der Systemzustand des Kommunikationskanals für die Steuerungskomponente als unbekannt angezeigt. Sie müssen die Upgrades für Controller und Host abschließen, damit der Status „Aktiv“ angezeigt wird.

NSX Controller-Cluster-Upgrade

Planen des NSX Controller-Upgrades:

- Sie können das NSX Controller-Cluster nach einem Upgrade von NSX Manager aktualisieren.
- In einer Cross-vCenter NSX-Umgebung müssen Sie vor dem Upgrade des NSX Controller-Clusters ein Upgrade für alle NSX Manager durchführen.
- VMware empfiehlt dringend, das Upgrade des NSX Controller-Clusters in demselben Wartungsfenster wie das NSX Manager-Upgrade durchzuführen.
- Wenn Sie ein Upgrade von NSX 6.1.x auf NSX 6.2.x oder höher durchführen, müssen Sie NSX Manager und den NSX Controller-Cluster im selben Wartungsfenster aktualisieren.

Auswirkungen während des NSX Controller-Upgrades:

- Das Erstellen von logischen Netzwerken und Änderungen daran werden während des Upgrade-Vorgangs blockiert. Nehmen Sie keine Konfigurationsänderungen an logischen Netzwerken vor, während das NSX Controller-Cluster-Upgrade durchgeführt wird.

- Stellen Sie während dieses Vorgangs keine neuen VMs bereit. Verschieben Sie während des Upgrades keine virtuellen Maschinen bzw. lassen Sie nicht zu, dass DRS während des Upgrades virtuelle Maschinen verschiebt.
- Wenn während des Upgrades vorübergehend ein Nicht-Mehrheitszustand eintritt, geht für vorhandene virtuelle Maschinen die Netzwerkverbindung nicht verloren.
- Lassen Sie nicht zu, dass während des Upgrades dynamische Routen geändert werden.

Nach dem NSX Controller-Upgrade:

- Konfigurationsänderungen sind zulässig.

NSX Host-Upgrade

Planen des NSX-Hostcluster-Upgrades:

- Sie können Hostcluster aktualisieren, nachdem Sie ein Upgrade der NSX Manager und NSX Controller-Cluster durchgeführt haben.
- Sie können die Hostcluster in einem separaten Wartungsfenster der NSX Manager- und NSX Controller-Cluster-Upgrades aktualisieren.
- Sie müssen nicht alle Hostcluster in demselben Wartungsfenster aktualisieren.
- Die neuen Funktionen der unter NSX Manager installierten NSX-Version werden zwar im vSphere Web Client und der API angezeigt, sie funktionieren jedoch möglicherweise erst nach dem VIB-Upgrade.
- Um alle neuen Funktionen einer NSX-Version nutzen zu können, führen Sie ein Upgrade der Hostcluster durch, sodass die Host-VIBs mit der NSX Manager-Version übereinstimmen.

Auswirkungen während des NSX-Hostcluster-Upgrades:

- Konfigurationsänderungen werden in NSX Manager nicht blockiert.
- Die Kommunikation von Controller zu Host ist abwärtskompatibel. Dies bedeutet, dass aktualisierte Controller mit nicht aktualisierten Hosts kommunizieren können.
- Das Upgrade wird pro Cluster durchgeführt. Wenn DRS auf dem Cluster aktiviert ist, verwaltet DRS die Upgradereihenfolge der Hosts.
- Momentan aktualisierte Hosts müssen in den Wartungsmodus versetzt werden. Dies bedeutet, dass virtuelle Maschinen ausgeschaltet oder auf andere Hosts evakuiert werden müssen. Dies kann mit DRS oder manuell durchgeführt werden.
- Hinzufügungen zu und Änderungen an logischen Netzwerken sind zulässig.
- Die Bereitstellung neuer virtueller Maschinen funktioniert weiter auf Hosts, die sich zurzeit nicht im Wartungsmodus befinden.

Upgrade von NSX Edge

Planen des NSX Edge-Upgrades:

- Sie können NSX Edges in separaten Wartungsfenstern von anderen NSX-Komponenten aktualisieren.
- Sie können logische Router aktualisieren, nachdem Sie ein Upgrade der NSX Manager, des NSX Controller-Clusters und der Hostcluster durchgeführt haben.
- Sie können ein Edge Services Gateway selbst dann aktualisieren, wenn Sie die NSX Controller- oder die Hostcluster noch nicht aktualisiert haben.
- Sie müssen nicht alle NSX Edges in demselben Wartungsfenster aktualisieren.
- Wenn ein Upgrade für NSX Edge verfügbar ist, Sie jedoch kein Upgrade durchgeführt haben, werden Größenänderungen, Ressourcen, Datenspeicher, Aktivierung des erweiterten Debuggens und die HA-Aktivierung auf der Appliance bis zu einem NSX Edge-Upgrade blockiert.

Auswirkungen während des NSX Edge-Upgrades:

- Auf dem aktuell aktualisierten NSX Edge-Gerät werden Konfigurationsänderungen blockiert. Es können Elemente zu logischen Switches hinzugefügt werden und Änderungen daran vorgenommen werden. Die Bereitstellung neuer virtueller Maschinen funktioniert weiterhin einwandfrei.
- Die Paketweiterleitung ist vorübergehend unterbrochen.
- In NSX Edge 6.0 und höher sind die OSPF-Nachbarschaften vom Upgrade ausgenommen, wenn Graceful Restart nicht aktiviert wurde.

Nach dem NSX Edge-Upgrade:

- Konfigurationsänderungen werden nicht blockiert. Durch das NSX-Upgrade eingeführte neue Funktionen für Edge Services Gateway sind erst dann konfigurierbar, wenn alle NSX Controller und alle Hostcluster aktualisiert wurden.

Upgrade für Guest Introspection

Planen des Guest Introspection-Upgrades:

- Sie können Guest Introspection aktualisieren, nachdem Sie ein Upgrade der NSX Manager, des NSX Controller-Clusters und der Hostcluster durchgeführt haben.
- Informationen zu einem Upgrade von Partnerlösungen finden Sie in der Partnerdokumentation.

Auswirkungen während des Guest Introspection-Upgrades:

- Die VMs im NSX-Cluster sind bei Änderungen, etwa bei VM-Hinzufügungen, vMotion-Vorgängen oder Löschvorgängen, nicht geschützt.

Nach dem Guest Introspection-Upgrade:

- Die VMs sind bei VM-Hinzufügungen, vMotion-Vorgängen und Löschvorgängen geschützt.

Informationen zum Verständnis des FIPS-Modus und NSX-Upgrades

Ab NSX 6.3.0 können Sie den FIPS-Modus aktivieren. Dies führt zur Aktivierung der FIPS-konformen Verschlüsselungs-Suiten.

Vorsicht Wenn Sie ein Upgrade von einer NSX-Version vor NSX 6.3.0 auf NSX 6.3.0 oder höher ausführen, dürfen Sie den FIPS-Modus erst nach Abschluss des Upgrades aktivieren. Wenn Sie den FIPS-Modus vor Abschluss des Upgrades aktivieren, wird die Kommunikation zwischen aktualisierten und nicht aktualisierten Komponenten unterbrochen.

NSX-Upgrade und FIPS-Status

Tabelle 1-1. Status des FIPS-Modus in NSX-Komponenten nach einem Upgrade auf NSX 6.3.x.

NSX-Komponente	Status des FIPS-Modus
NSX Manager	Nach einem Upgrade auf 6.3.x ist der FIPS-Modus für NSX Manager-Appliances verfügbar und deaktiviert. Aktivieren Sie FIPS erst nach Abschluss des Upgrades aller NSX-Komponenten und nachdem FIPS auf allen NSX Edge-Appliances aktiviert wurde.
NSX Controller-Cluster	Nach einem Upgrade auf 6.3.x ist das NSX Controller-Cluster FIPS-konform. Dies ist nicht konfigurierbar.
NSX Host-Cluster	Nach einem Upgrade auf 6.3.x sind NSX Host-Cluster FIPS-konform. Dies ist nicht konfigurierbar.
NSX Edge	Nach einem Upgrade auf 6.3.x ist der FIPS-Modus für NSX Edge-Appliances verfügbar und deaktiviert. Aktivieren Sie FIPS erst, nachdem das Upgrade aller NSX-Komponenten abgeschlossen ist.
Guest Introspection-Dienst-VM	Nach einem Upgrade auf 6.3.x ist die virtuelle Maschine für den Guest Introspection-Dienst FIPS-konform. Dies ist nicht konfigurierbar.

FIPS aktivieren

Wenn Sie ein Upgrade auf NSX 6.3.x ausführen und FIPS aktivieren möchten, müssen Sie die folgenden Schritte durchführen:

1. Stellen Sie sicher, dass Partnerlösungen für den FIPS-Modus zertifiziert sind. Weitere Informationen finden Sie im VMware-Kompatibilitätshandbuch unter http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security. Schlagen Sie Informationen in der Partnerdokumentation nach.
2. Führen Sie ein Upgrade von NSX Manager auf NSX 6.3.0 oder höher durch.
3. Führen Sie ein Upgrade des NSX Controller-Clusters NSX 6.3.0 oder höher durch.
4. Führen Sie für alle Host-Cluster, auf denen NSX-Arbeitslasten ausgeführt werden, ein Upgrade auf NSX 6.3.0 oder höher durch.
5. Führen Sie ein Upgrade aller NSX Edge-Appliances auf NSX 6.3.0 oder höher durch.

6 Sofern installiert, führen Sie auf allen Host-Clustern ein Upgrade von Guest Introspection auf NSX 6.3.0 oder höher durch.

7 Aktivieren Sie den FIPS-Modus auf NSX Edge-Appliances. Siehe „Ändern des FIPS-Modus in NSX Edge“ im *Administratorhandbuch für NSX*.

8 Aktivieren Sie den FIPS-Modus auf den NSX Manager-Appliances. Siehe „Ändern des FIPS-Modus und der TLS-Einstellungen für NSX Manager“ im *Administratorhandbuch für NSX*.

Überprüfen des NSX-Arbeitszustands

Bevor Sie mit dem Upgrade beginnen, ist es wichtig, dass Sie den NSX-Arbeitszustand testen. Anderenfalls sind Sie nicht in der Lage zu ermitteln, ob der Upgrade-Vorgang irgendwelche auftretenden Probleme verursacht hat oder ob diese bereits vor dem Upgrade-Vorgang existierten.

Gehen Sie vor dem Upgrade der NSX-Infrastruktur nicht davon aus, dass alles problemlos funktioniert. Nehmen Sie zuvor einige Überprüfungen vor.

Vorgehensweise

1 Merken Sie sich die aktuellen Versionen von NSX Manager, vCenter Server, ESXi und NSX Edges.

2 Ermitteln Sie die administrativen Benutzer-IDs und Kennwörter.

3 Stellen Sie sicher, dass Sie sich bei den folgenden Komponenten anmelden können:

- vCenter Server
- NSX Manager-Web-UI
- Edge Services Gateway-Appliances
- Verteilte logische Router-Appliances
- NSX Controller-Appliances

4 Stellen Sie sicher, dass die VXLAN-Segmente funktionsfähig sind.

Stellen Sie sicher, dass die Paketgröße korrekt festgelegt und das Nicht-Fragmentieren-Bit berücksichtigt wird.

- Senden Sie einen Ping-Befehl zwischen zwei virtuellen Maschinen, die sich auf demselben logischen Switch, aber auf zwei unterschiedlichen Hosts befinden.
  - Von einer Windows-VM: ping -l 1472 –f <dest VM>
  - Von einer Linux-VM: ping -s 1472 –M do <dest VM>
- Ping-Befehl zwischen den VTEP-Schnittstellen zweier Hosts.
  - ping ++netstack=vxlan -d -s 1572 <dest VTEP IP>

  Hinweis Um die VTEP-IP eines Hosts zu ermitteln, suchen Sie auf der Seite **Verwalten > Netzwerk > Virtuelle Switches (Manage > Networking > Virtual Switches)** des Hosts nach der IP-Adresse von vmknicPG.

5 Validieren Sie die Nord-Süd-Verbindung, indem Sie von einer virtuellen Maschine aus pingen.

6 Inspizieren Sie die NSX-Umgebung visuell, um sicherzustellen, dass alle Statusanzeigen grün/normal/bereitgestellt sind.

- Wählen Sie **Installation > Verwaltung (Installation > Management)**.
- Wählen Sie **Installation > Hostvorbereitung (Installation > Host Preparation)**.
- Wählen Sie **Installation > Vorbereitung des logischen Netzwerks > VXLAN-Transport (Installation > Logical Network Preparation > VXLAN Transport)**.
- Wählen Sie **Logische Switches (Logical Switches)**.
- Wählen Sie **NSX Edges**.

7 Zeichnen Sie die BGP- und OSPF-Zustände auf den NSX Edge-Geräten auf.

- `show ip ospf neighbor`
- `show ip bgp neighbor`
- `show ip route`

8 Stellen Sie sicher, dass syslog konfiguriert ist.

Weitere Informationen hierzu finden Sie unter Angeben eines Syslog-Servers.

9 Erstellen Sie, wenn möglich, in der Vor-Upgrade-Umgebung einige neue Komponenten und testen Sie deren Funktionalität.

- Erstellen Sie einen neuen logischen Switch.
- Erstellen Sie ein neues Edge Services Gateway und einen neuen verteilten logischen Router.
- Verbinden Sie eine virtuelle Maschine mit dem neuen logischen Switch und testen Sie die Funktionalität.

10 Validieren Sie die Verbindungen von netcpad und vsfwd user-world agent (UWA).

- Führen Sie auf einem ESXi-Host `esxcli network vswitch dvs vmware vxlan network list --vds-name=<VDS_name>` aus und überprüfen Sie den Zustand der Controller-Verbindung.
- Führen Sie auf NSX Manager den Befehl `show tech-support save session` aus und suchen Sie nach „5671“, um sicherzustellen, dass alle Hosts mit NSX Manager verbunden sind.

11 (Optional) Wenn eine Testumgebung vorhanden ist, testen Sie die Upgrade- und die Nach-Upgrade-Funktionalität, bevor Sie ein Upgrade der Produktionsumgebung durchführen.

Deinstallieren von NSX Data Security

NSX Data Security war in NSX 6.2.3 veraltet und wurde aus NSX 6.3.0 entfernt. Sie müssen NSX Data Security deinstallieren, bevor Sie ein Upgrade auf NSX 6.3.x ausführen.

Vorgehensweise

1 Klicken Sie auf der Registerkarte **Installation** auf **Dienstbereitstellungen (Service Deployments)**.

2 Wählen Sie einen NSX Data Security-Dienst aus und klicken Sie auf das Symbol **Dienstbereitstellung löschen (Delete Service Deployment)** (✖).

3 Klicken Sie im Dialogfeld „Löschen bestätigen“ auf **Jetzt löschen (Delete now)** oder wählen Sie ein Datum und eine Uhrzeit aus, wann der Löschvorgang ausgeführt werden soll.

4 Klicken Sie auf **OK**.

Sichern und Wiederherstellen von NSX

Die ordnungsgemäße Sicherung aller NSX-Komponenten ist entscheidend, um bei einem Ausfall das System in einem funktionsfähigen Zustand wiederherzustellen.

Die NSX Manager-Sicherung enthält die gesamte NSX-Konfiguration, inklusive logische Switches und Routing-Entitäten, Sicherheits- und Firewallregeln sowie alle anderen Festlegungen zur Konfiguration mit der NSX Manager-Benutzeroberfläche oder -API. Die vCenter-Datenbank sowie zugehörige Elemente wie die virtuellen Switches müssen gesondert gesichert werden.

Es wird empfohlen, zumindest von NSX Manager und vCenter regelmäßig Sicherungskopien zu erstellen. Je nach geschäftlichen Anforderungen und operativen Verfahren können die Sicherungshäufigkeit und der Zeitplan variieren. Es wird empfohlen, in Zeiten häufiger Konfigurationsänderungen NSX häufig zu sichern.

Sicherungen von NSX Manager können bei Bedarf stündlich, täglich oder wöchentlich vorgenommen werden.

Es wird empfohlen, in den folgenden Szenarios Sicherungskopien zu erstellen:

- Vor der Durchführung eines Upgrades von NSX oder vCenter.
- Nach der Durchführung eines Upgrades von NSX oder vCenter.
- Nach der Bereitstellung von Day Zero und der Erstkonfiguration der NSX-Komponenten, z. B. nach dem Erstellen der NSX-Controller, logischen Switches, logischen Router, Edge Services Gateways, Sicherheit und der Firewallrichtlinien.
- Nach Änderungen an der Infrastruktur oder der Topologie.
- Nach jeder größeren Tag 2-Änderung.

Damit Sie ein Rollback auf den gesamten Systemzustand zu einem bestimmten Zeitpunkt vornehmen können, wird empfohlen, Sicherungen von NSX-Komponenten (z. B. NSX Manager) mit Ihrem Sicherungszeitplan für andere interagierende Komponenten, z. B. vCenter, Cloud-Managementsysteme, operative Tools usw., zu synchronisieren.

Sichern und Wiederherstellen von NSX Manager

Die Sicherung und Wiederherstellung von NSX Manager-Daten kann über die Webschnittstelle der virtuellen Appliance von NSX Manager oder über die NSX Manager-API konfiguriert werden. Stündliche, tägliche oder wöchentliche Backups können geplant werden.

Die Sicherungsdatei wird an einem Remote-FTP- oder -SFTP-Speicherort gespeichert, auf den NSX Manager zugreifen kann. Zu den NSX Manager-Daten gehören die Konfiguration, Ereignisse und Audit-Protokolltabellen. Konfigurationstabellen sind in jeder Sicherung enthalten.

Die Wiederherstellung wird nur unterstützt, wenn die Version von NSX Manager mit der Sicherungsversion identisch ist. Aus diesem Grund ist es wichtig, eine neue Sicherungsdatei vor und nach dem Durchführen eines Upgrades von NSX zu erstellen: eine Datensicherung für die alte Version und eine weitere Datensicherung für die neue Version.

Sichern von NSX Manager-Daten

Sie können NSX Manager-Daten sichern, indem Sie eine bedarfsbasierte oder eine geplante Sicherung durchführen.

Vorgehensweise

1. Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
2. Klicken Sie unter „Appliance-Verwaltung“ auf **Sicherung und Wiederherstellung (Backups & Restore)**.
3. Um den Sicherungsspeicherort anzugeben, klicken Sie neben den FTP-Server-Einstellungen auf **Ändern (Change)**.
   a. Geben Sie die IP-Adresse oder den Hostnamen des Sicherungssystems ein.
   b. Wählen Sie im Dropdown-Menü **Übertragungsprotokoll (Transfer Protocol)** basierend auf der Unterstützung durch das Zielsystem entweder das Protokoll **SFTP** oder das Protokoll **FTP** aus.
   c. Bearbeiten Sie den Standardport, falls erforderlich.
   d. Geben Sie den Benutzernamen und das Kennwort ein, die zur Anmeldung beim Sicherungssystem erforderlich sind.

e Geben Sie im Feld **Sicherungsverzeichnis (Backup Directory)** den absoluten Pfad zu dem Verzeichnis ein, in dem die Sicherungen gespeichert werden sollen.

Um den absoluten Pfad festzustellen, melden Sie sich auf dem FTP-Server an, wechseln Sie in das Verzeichnis, das Sie verwenden möchten, und führen Sie den Befehl zum Anzeigen des aktuellen Arbeitsverzeichnisses (`pwd`) aus. Beispiel:

```
PS C:\Users\Administrator> ftp 192.168.110.60
Connected to 192.168.110.60.
220 server-nfs FTP server ready.
User (192.168.110.60:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> ls
200 PORT command successful.
150 Opening BINARY mode data connection for 'file list'.
datastore-01
226 Transfer complete.
ftp: 22 bytes received in 0.00Seconds 22000.00Kbytes/sec.
ftp> cd datastore-01
250 CWD command successful.
ftp> pwd
257 "/datastore-01" is current directory.
```

f Geben Sie in das Feld **Präfix des Dateinamens (Filename Prefix)** eine Textzeichenfolge als Präfix für den Dateinamen ein.

Dieser Text wird jedem Sicherungsdateinamen vorangestellt, um eine leichte Identifizierung auf dem Sicherungssystem zu ermöglichen. Wenn Sie beispielsweise **ppdb** als Präfix verwenden, lautet der Sicherungsname *ppdbHH_MM_SS_TagTTMonJJJJ*.

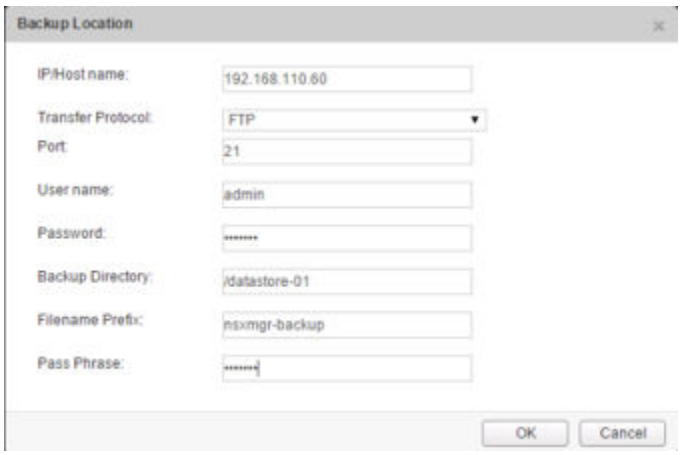
Hinweis Dateien im Backup-Verzeichnis müssen auf 100 begrenzt werden. Wenn die Anzahl der Dateien im Verzeichnis den Grenzwert überschreitet, erhalten Sie eine Warnmeldung.

g Geben Sie zum Sichern der Sicherungsdatei einen Kennwortsatz ein.

Sie benötigen diese Passphrase, um die Sicherung wiederherzustellen.

h Klicken Sie auf **OK**.

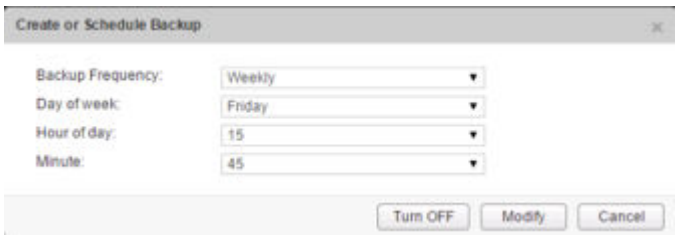
Beispiel:



4 Klicken Sie für eine bedarfsbasierte Sicherung auf **Sichern (Backup)**.

Unter **Sicherungsverlauf (Backup History)** wird eine neue Datei hinzugefügt.

5 Klicken Sie für geplante Sicherungen neben „Zeitplan“ auf **Ändern (Change)**.



a Wählen Sie im Dropdown-Menü **Häufigkeit der Sicherungsvorgänge (Backup Frequency)** die Option **Stündlich (Hourly)**, **Täglich (Daily)** oder **Wöchentlich (Weekly)** aus. Je nach ausgewählter Häufigkeit werden die Dropdown-Menüs „Wochentag“, „Stunde des Tages“ und „Minute“ deaktiviert. Wenn Sie beispielsweise „Täglich“ auswählen, wird das Dropdown-Menü „Wochentag“ deaktiviert, da dieses Feld bei einer täglichen Sicherung nicht zum Tragen kommt.

b Wählen Sie für eine wöchentliche Sicherung den Wochentag aus, an dem die Daten gesichert werden sollen.

c Wählen Sie für eine wöchentliche oder tägliche Sicherung die Stunde aus, zu der die Sicherung beginnen soll.

d Wählen Sie die Minute aus, zu der die Sicherung beginnen soll, und klicken Sie auf **Zeitplan (Schedule)**.

6 Um Protokolle und Flussdaten von der Sicherung auszuschließen, klicken Sie neben „Ausschließen“ auf **Ändern (Change)**.

   a Wählen Sie die Objekte aus, die Sie von der Sicherung ausschließen möchten.

   b Klicken Sie auf **OK**.

7 Bewahren Sie die IP-Adresse bzw. den Hostnamen Ihres FTP-Servers, die Anmeldedaten, die Verzeichnisdetails und die Passphrase auf. Diese Informationen werden benötigt, um die Sicherung wiederherzustellen.

Wiederherstellen eines NSX Manager-Backups

Durch das Wiederherstellen von NSX Manager wird eine Sicherungsdatei auf eine NSX Manager-Appliance geladen. Die Sicherungsdatei muss in einem Remote-FTP- oder SFTP-Speicherort gespeichert werden, auf den NSX Manager zugreifen kann. Zu den NSX Manager-Daten gehören die Konfiguration, Ereignisse und Audit-Protokolltabellen.

Wichtig Sichern Sie Ihre aktuellen Daten, bevor Sie eine Sicherungsdatei wiederherstellen.

Voraussetzungen

Bevor Sie NSX Manager-Daten wiederherstellen, sollten Sie die NSX Manager-Appliance neu installieren. Das Ausführen des Wiederherstellungsvorgangs auf einer vorhandenen NSX Manager-Appliance kann zwar gelingen, wird jedoch nicht unterstützt. Es wird davon ausgegangen, dass der bestehende NSX Manager ausgefallen ist. Daher wird eine neue NSX Manager-Appliance bereitgestellt.

Gemäß Best Practice notieren Sie die aktuellen Einstellungen der alten NSX Manager-Appliance, damit sie für die Angabe von Informationen zu IP-Adressen und zum Sicherungsspeicherort für die neu bereitgestellte NSX Manager-Appliance verfügbar sind.

Vorgehensweise

1 Notieren Sie alle Einstellungen auf der vorhandenen NSX Manager-Appliance. Notieren Sie auch die FTP-Servereinstellungen.

2 Stellen Sie eine neue NSX Manager-Appliance bereit.

   Die Version muss mit der gesicherten NSX Manager-Appliance identisch sein.

3 Melden Sie sich bei der neuen NSX Manager-Appliance an.

4 Klicken Sie unter „Appliance-Verwaltung“ auf **Sicherung und Wiederherstellung (Backups & Restore)**.

5 Klicken Sie in den FTP-Servereinstellungen auf **Ändern (Change)** und fügen Sie die FTP-Servereinstellungen hinzu.

   Die Felder **Host-IP-Adresse (Host IP Address)**, **Benutzername (User Name)**, **Kennwort (Password)**, **Sicherungsverzeichnis (Backup Directory)**, **Präfix des Dateinamens (Filename Prefix)** und **Kennwortsatz (Pass Phrase)** im Bildschirm „Sicherungsspeicherort“ müssen den Speicherort der wiederherzustellenden Sicherungsdatei identifizieren.

   Im Abschnitt **Sicherungsverlauf (Backup History)** wird der Sicherungsordner angezeigt.

   Hinweis Wenn der Sicherungsordner im Abschnitt **Sicherungsverlauf (Backup History)** nicht enthalten ist, überprüfen Sie die FTP-Servereinstellungen. Prüfen Sie, ob Sie eine Verbindung mit dem FTP-Server herstellen können, und zeigen Sie den Sicherungsordner an.

6 Wählen Sie im Abschnitt **Sicherungsverlauf (Backup History)** den erforderlichen Sicherungsordner für die Wiederherstellung aus und klicken Sie auf **Wiederherstellen (Restore)**.

   Die Wiederherstellung der NSX Manager-Daten wird gestartet.

Die NSX-Konfiguration wird für den NSX Manager wiederhergestellt.

Vorsicht Nach der Wiederherstellung einer NSX Manager-Sicherung müssen Sie möglicherweise zusätzliche Maßnahmen für den ordnungsgemäßen Betrieb der NSX Edge-Appliances und der logischen Switches durchführen. Siehe Wiederherstellen von NSX Edges und Auflösen von Synchronisationsfehlern auf logischen Switches.

Wiederherstellen von NSX Edges

Alle NSX Edge-Konfigurationen (logische Router und Gateways für Edge-Dienste) werden als Teil der NSX Manager-Datensicherung gesichert.

Individuelle Sicherungen von NSX Edge werden nicht unterstützt.

Wenn Sie über eine intakte NSX Manager-Konfiguration verfügen, können Sie eine Edge-Appliance-VM, auf die nicht zugegriffen werden kann oder auf der ein Fehler aufgetreten ist, durch erneutes Bereitstellen des NSX Edge neu erstellen (klicken Sie auf **NSX Edge erneut bereitstellen (Redeploy NSX Edge)(**  **)** in vSphere Web Client). Weitere Informationen finden Sie unter „Erneutes Bereitstellen von NSX Edge“ im Dokument *Administratorhandbuch für NSX*.

Vorsicht Nach der Wiederherstellung einer NSX-Manager-Sicherung müssen Sie möglicherweise zusätzliche Maßnahmen für den ordnungsgemäßen Betrieb der NSX Edge-Appliances durchführen.

- Edge-Appliances, die nach der letzten Sicherung erstellt wurden, werden bei der Wiederherstellung nicht entfernt. Sie müssen die virtuelle Maschine manuell löschen.
- Edge-Appliances, die nach der letzten Sicherung gelöscht wurden, werden nicht wiederhergestellt, solange sie nicht erneut bereitgestellt werden.
- Wenn bei der Wiederherstellung einer Sicherung sowohl die konfigurierten wie die aktuellen Speicherorte einer in der Sicherung gespeicherten NSX Edge-Appliance nicht mehr vorhanden sind, können Vorgänge wie das erneute Bereitstellen, das Migrieren oder das Aktivieren/Deaktivieren der Hochverfügbarkeit nicht durchgeführt werden. Sie müssen die Appliance-Konfiguration bearbeiten und gültige Speicherortinformationen zur Verfügung stellen. Bearbeiten Sie mit `PUT /api/4.0/edges/{edgeId}/appliances` die Konfiguration des Appliance-Speicherorts (*resourcePoolId*, *datastoreId*, *hostId* und *vmFolderId* wie erforderlich). Informationen dazu finden Sie unter „Arbeiten mit der NSX Edge-Appliance-Konfiguration“ im Dokument *Handbuch zu NSX-API*.

Wenn eine der im Folgenden aufgeführten Änderungen seit der letzten NSX Manager-Sicherung vorgenommen wurden, unterscheiden sich die wiederhergestellte NSX Manager-Konfiguration und die Konfiguration auf der NSX Edge-Appliance. Sie müssen die Option **Synchronisierung erzwingen (Force Sync)** für das NSX Edge ausführen, um diese Änderungen für die Appliance rückgängig zu machen und den ordnungsgemäßen Betrieb des NSX Edge zu gewährleisten. Informationen dazu finden Sie unter „Erzwingen der Synchronisierung von NSX Edge mit NSX Manager“ im Dokument *Administratorhandbuch für NSX*.

- Änderungen, die über die Verteilte Firewall für vordefinierte Regeln für die NSX Edge-Firewall vorgenommen wurden.
- Änderungen bei der Mitgliedschaft gruppierter Objekte.

Wenn eine der im Folgenden aufgeführten Änderungen seit der letzten NSX Manager-Sicherung vorgenommen wurden, unterscheiden sich die wiederhergestellte NSX Manager-Konfiguration und die Konfiguration auf der NSX Edge-Appliance. Sie müssen die Option **Erneut bereitstellen (Redeploy)** für NSX Edge aufrufen, um diese Änderungen für die Appliance wiederherzustellen und den ordnungsgemäßen Betrieb des NSX Edge zu gewährleisten. Weitere Informationen finden Sie unter „Erneutes Bereitstellen von NSX Edge“ im Dokument *Administratorhandbuch für NSX*.

- Änderungen der Edge-Appliance-Einstellungen:
  - HA aktiviert oder deaktiviert
  - Status der Appliance von „Bereitgestellt“ zu „Nicht bereitgestellt“ geändert
  - Status der Appliance von „Nicht bereitgestellt“ zu „Bereitgestellt“ geändert
  - Einstellungen für die Ressourcenreservierung geändert
- Änderungen der vNIC-Einstellungen der Edge-Appliance:
  - Hinzufügen, Entfernen oder Trennen der vNIC
  - Portgruppen
  - Trunk-Ports
  - Fence-Parameter
  - Shaping-Richtlinie

Auflösen von Synchronisationsfehlern auf logischen Switches

Wenn zwischen dem Zeitpunkt der Sicherung und Wiederherstellung von NSX Manager auf logischen Switches Änderungen aufgetreten sind, melden die logischen Switches möglicherweise, dass sie nicht synchron laufen.

Vorgehensweise

1. Melden Sie sich beim vSphere Web Client an.
2. Navigieren Sie zu **Networking & Security > Logische Switches (Logical Switches)**.
3. Falls vorhanden, klicken Sie auf den Link **+++Nicht synchron+++ (Out of sync)** in der Spalte „Status“, um Details zu dem Fehler anzuzeigen.
4. Klicken Sie auf **Auflösen (Resolve)**, um fehlende Backing-Portgruppen für den logischen Switch neu zu erstellen.

Sichern von vSphere Distributed Switches

Sie können Konfigurationen von vSphere Distributed Switches und verteilten Portgruppen in eine Datei exportieren.

Die Datei behält gültige Netzwerkkonfigurationen bei, sodass die Verteilung dieser Konfigurationen an andere Bereitstellungen möglich ist.

vSphere Distributed Switch- und Portgruppeneinstellungen werden im Rahmen des Importvorgangs importiert.

Best Practice ist, die vSphere Distributed Switch-Konfiguration zu exportieren, bevor Sie den Cluster für VXLAN vorbereiten. Eine detaillierte Anleitung finden Sie unter http://kb.vmware.com/kb/2034602.

Sichern von vCenter

Zum Sichern Ihrer NSX-Bereitstellung ist es wichtig, ein Backup der vCenter-Datenbank und Snapshots der virtuellen Maschinen zu erstellen.

Weitere Informationen zu den vCenter-Sicherungs- und -Wiederherstellungsverfahren sowie zu den Best Practices finden Sie in der vCenter-Dokumentation.

Weitere Informationen zu VM-Snapshots finden Sie unter http://kb.vmware.com/kb/1015180.

Nützliche Links für vCenter 5.5:

- http://kb.vmware.com/kb/2057353
- http://kb.vmware.com/kb/2034505
- http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf

Nützliche Links für vCenter 6.0:

- https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html
- http://kb.vmware.com/kb/2110294

Herunterladen des NSX-Upgrade-Pakets und Überprüfen der MD5-Prüfsumme

Das NSX-Upgrade-Paket enthält alle Dateien, die für das Upgrade der NSX-Infrastruktur erforderlich sind. Bevor Sie ein Upgrade von NSX Manager durchführen, müssen Sie zuerst das Upgrade-Paket für die Version herunterladen, die Sie aktualisieren möchten.

Voraussetzungen

Ein MD5-Prüfsummentool.

Vorgehensweise

1 Laden Sie das NSX-Upgrade-Paket an einen Speicherort herunter, auf den NSX Manager zugreifen kann. Der Name der Upgrade-Paket-Datei entspricht in etwa dem Format `VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz`.

2 Stellen Sie sicher, dass der Dateiname für das NSX Manager-Upgrade mit tar.gz endet.

Einige Browser ändern möglicherweise die Dateierweiterung. Wenn beispielsweise der Download-Dateiname wie folgt lautet:

VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx.gz

Ändern Sie ihn in:

VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx.tar.gz

Andernfalls wird nach dem Hochladen des Upgrade-Pakets folgende Fehlermeldung angezeigt: „Ungültige Upgrade-Paket-Datei VMware-NSX-Manager-upgrade-bundle-6.x.x-xxxxx.gz, Upgrade-Dateiname hat die Erweiterung tar.gz.“

3 Verwenden Sie ein MD5-Prüfsummentool zum Vergleichen der auf der VMware-Website angegebenen offiziellen MD5-Summe des Upgrade-Pakets mit der vom Prüfsummentool berechneten MD5-Summe.

a Navigieren Sie im MD5-Prüfsummentool zum Upgrade-Paket.

b Verwenden Sie das Tool zum Berechnen der Prüfsumme des Pakets.

c Fügen Sie die Prüfsumme ein, die auf der VMware-Website aufgelistet ist.

d Verwenden Sie das Tool zum Vergleichen der beiden Prüfsummen.

Sollten die zwei Prüfsummen nicht übereinstimmen, laden Sie das Upgrade-Paket erneut herunter.

Upgrade auf NSX 6.3.x

Um ein Upgrade auf NSX 6.3.x durchzuführen, müssen Sie die NSX-Komponenten in der Reihenfolge aktualisieren wie in diesem Handbuch dokumentiert.

Die NSX-Komponenten müssen in der folgenden Reihenfolge aktualisiert werden:

1 NSX Manager-Appliance

2 NSX Controller-Cluster

3 Host-Cluster

4 NSX Edge (siehe Hinweis)

5 Guest Introspection

Hinweis Edge Services Gateways können jederzeit nach dem Upgrade von NSX Manager aktualisiert werden. Für logische Router kann jedoch erst ein Upgrade erfolgen, nachdem das NSX Controller-Cluster und die Host-Cluster aktualisiert wurden. Weitere Informationen zu den Upgrade-Abhängigkeiten finden Sie unter Operative Auswirkungen von NSX-Upgrades.

Der Upgrade-Vorgang wird von NSX Manager verwaltet. Falls das Upgrade einer Komponente fehlschlägt oder unterbrochen wird und Sie das Upgrade wiederholen oder neu starten müssen, wird der Vorgang von dem Punkt aus fortgesetzt, an dem er unterbrochen wurde. Er startet nicht wieder von vorne.

Der Upgrade-Status wird für jeden Knoten und auf Clusterebene aktualisiert.

Upgrade von NSX Manager

Der erste Schritt beim Upgrade der NSX-Infrastruktur ist das Upgrade der NSX Manager-Appliance.

Beim Upgrade können Sie auswählen, ob Sie am „Programm zur Verbesserung der Benutzerfreundlichkeit“ (CEIP, Customer Experience Improvement Program) für NSX teilnehmen möchten. Unter „Programm zur Verbesserung der Benutzerfreundlichkeit im *Administratorhandbuch für NSX*“ finden Sie weitere Informationen dazu, inklusive Informationen, wie Sie sich daran beteiligen und wieder abmelden können.

Wenn Sie ein Upgrade von NSX 6.1.x auf NSX 6.2.x oder höher durchführen, müssen Sie NSX Manager und den NSX Controller-Cluster im selben Wartungsfenster aktualisieren.

Voraussetzungen

- Überprüfen Sie die NSX Manager-Nutzung des Dateisystems und führen Sie eine Bereinigung durch, wenn die Nutzung bei 100 Prozent liegt.
  a Melden Sie sich bei NSX Manager an und führen Sie `show filesystems` aus, um die Nutzung des Dateisystems anzuzeigen.
  b Wenn die Nutzung bei 100 Prozent liegt, führen Sie die Befehle `purge log manager` und `purge log system` aus.
  c Starten Sie die NSX Manager-Appliance neu, damit die Protokollbereinigung wirksam wird.
- Stellen Sie vor dem Upgrade sicher, dass der reservierte Arbeitsspeicher der virtuellen Appliance für NSX Manager die Systemanforderungen erfüllt.

  Weitere Informationen dazu finden Sie unter Systemvoraussetzungen für NSX.
- Wenn sich Data Security in Ihrer Umgebung befindet, deinstallieren Sie es, bevor Sie NSX Manager aktualisieren. Weitere Informationen dazu finden Sie unter Deinstallieren von NSX Data Security. Data Security wurde aus NSX 6.3.x entfernt.

- Sichern Sie Ihre aktuelle Konfiguration und laden Sie die Protokolle des technischen Supports herunter, bevor Sie mit dem Upgrade beginnen. Weitere Informationen dazu finden Sie unter Sichern und Wiederherstellen von NSX.
- Laden Sie das NSX-Upgrade-Paket herunter und überprüfen Sie die MD5-Prüfsumme. Weitere Informationen dazu finden Sie unter Herunterladen des NSX-Upgrade-Pakets und Überprüfen der MD5-Prüfsumme.
- Informieren Sie sich über die operativen Auswirkungen des NSX Manager-Upgrades, während das Upgrade läuft. Weitere Informationen dazu finden Sie unter Operative Auswirkungen von NSX-Upgrades.
- Sie müssen alle NSX Manager in einer Cross-vCenter NSX-Umgebung im selben Wartungsfenster aktualisieren.
- Planen Sie ein Upgrade für alle NSX Manager, die mit vCenter Server-Systemen verbunden sind, die den gleichen SSO-Server für dasselbe Wartungsfenster (einschließlich vCenter Server-Systemen im erweiterten verknüpften Modus), verwenden. Wenn das nicht möglich ist, finden Sie dafür unter https://kb.vmware.com/kb/2127061 eine Problemumgehung.

Vorgehensweise

1. Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
2. Klicken Sie auf der Startseite auf **Upgrade**.
3. Klicken Sie auf **Upgrade durchführen (Upgrade)**, anschließend auf **Datei auswählen (Choose File)** und rufen Sie die Datei `VMware-NSX-Manager-upgrade-bundle-`*releaseNumber-NSXbuild-Number*`.tar.gz` auf. Klicken Sie auf **Fortsetzen (Continue)**, um das Hochladen zu starten.

   Der Upload-Status wird im Browserfenster angezeigt.
4. Im Dialogfeld „Upgrade“ legen Sie fest, ob SSH aktiviert werden soll, und ob Sie am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teilnehmen möchten. Klicken Sie auf **Upgrade durchführen (Upgrade)**, um das Upgrade zu starten.

   Der Upgrade-Status wird im Browserfenster angezeigt.

   Warten Sie, bis der Upgrade-Vorgang abgeschlossen ist und die NSX Manager-Anmeldeseite angezeigt wird.
5. Melden Sie sich erneut bei der virtuellen Appliance für NSX Manager an und klicken Sie auf der Startseite auf **Upgrade**. Bestätigen Sie, dass der Upgrade-Status **Abgeschlossen (Complete)** lautet und dass die Version- und Build-Nummer oben rechts mit dem geraden installierten Upgrade-Paket übereinstimmt.

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 korrekt in vSphere Web Client angezeigt wird, löschen Sie den Zwischenspeicher und den Verlauf Ihres Browsers. Wird dieser Schritt nicht durchgeführt, wird möglicherweise eine Fehlermeldung in der Art „Es ist ein interner Fehler aufgetreten – Fehler #1009“ angezeigt, wenn in vSphere Web Client Änderungen an der NSX-Konfiguration vorgenommen werden.

Wenn die Registerkarte „Networking & Security“ im vSphere Web Client nicht angezeigt wird, setzen Sie den vSphere Web Client-Server zurück:

- Öffnen Sie in vCenter 5.5 „https://<vcenter-ip>: 5480“ und starten Sie den Web-Client-Server neu.
- Melden Sie sich in der vCenter Server Appliance 6.0 bei der vCenter Server-Shell als Root-Benutzer an und führen Sie die folgenden Befehle aus:

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- Führen Sie dazu in vCenter Server 6.0 auf Windows die nachfolgend aufgeführten Befehle aus.

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

Es wird empfohlen, unterschiedliche Webclients zum Verwalten der vCenter Server zu verwenden, die unterschiedliche Versionen von NSX Manager ausführen. Dadurch werden unerwartete Fehler vermieden, wenn unterschiedliche Versionen von NSX-Plug-Ins ausgeführt werden.

Erstellen Sie nach dem Upgrade von NSX Manager eine neue NSX Manager-Sicherungsdatei. Weitere Informationen dazu finden Sie unter Sichern und Wiederherstellen von NSX. Die vorherige NSX Manager-Sicherung gilt nur für die vorherige Version.

Weiter

Führen Sie ein Upgrade des NSX Controller-Clusters durch.

Upgrade von NSX Controller-Clustern

Die Controller in Ihrer Umgebung werden auf Clusterebene aktualisiert. Wenn für einen Controller-Knoten ein Upgrade zur Verfügung steht, wird in NSX Manager ein Upgrade-Link angezeigt.

Es wird empfohlen, die Controller während eines Wartungsfensters zu aktualisieren.

Das NSX Controller-Upgrade führt dazu, dass auf jeden Controller-Knoten eine Upgrade-Datei heruntergeladen wird. Die Controller werden nacheinander aktualisiert. Wenn ein Upgrade durchgeführt wird, ist der Link **Upgrade verfügbar (Upgrade Available)** nicht anklickbar und API-Aufrufe zum Aktualisieren des Controller-Clusters werden so lange blockiert, bis das Upgrade abgeschlossen ist.

Wenn Sie neue Controller bereitstellen, bevor vorhandene Controller aktualisiert wurden, werden die neuen Controller in der alten Version bereitgestellt. Um einem Cluster beitreten zu können, müssen die Controller-Knoten dieselbe Version haben.

Wichtig In NSX 6.3.3 ändert sich das zugrunde liegende Betriebssystem des NSX Controllers. 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.

Beim Löschen der Controller 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.

Voraussetzungen

- Stellen Sie sicher, dass sich alle Controller im normalen Zustand befinden. Ein Upgrade ist nicht möglich, wenn sich ein oder mehrere Controller im Zustand „Getrennt“ befinden. Um einen getrennten Controller neu zu verbinden, versuchen Sie, die virtuelle Controller-Appliance zurückzusetzen. Klicken Sie in der Ansicht **Hosts und Cluster (Hosts and Clusters)** mit der rechten Maustaste auf den Controller und wählen Sie **Stromversorgung > Zurücksetzen (Power > Reset)**.
- Ein gültiger NSX Controller-Cluster enthält drei Controller-Knoten. Melden Sie sich bei den drei Controller-Knoten an und führen Sie den Befehl **show control-cluster status** aus.

```
controller-node# show control-cluster status

Type                Status                                          Since
--------------------------------------------------------------------------------
Join status:        Join complete                                   05/04 02:36:03
Majority status:    Connected to cluster majority                   05/19 23:57:23
Restart status:     This controller can be safely restarted         05/19 23:57:12
Cluster ID:         ff3ebaeb-de68-4455-a3ca-4824e31863a8
Node UUID:          ff3ebaeb-de68-4455-a3ca-4824e31863a8

Role                Configured status   Active status
--------------------------------------------------------------------------------
api_provider        enabled             activated
persistence_server  enabled             activated
switch_manager      enabled             activated
logical_manager     enabled             activated
directory_server    enabled             activated
```

  - Überprüfen Sie unter „Join Status“, ob der Controller-Knoten „Join Complete“ meldet.
  - Überprüfen Sie unter „Majority Status“, ob der Controller mit der „Cluster Majority“ verbunden ist.
  - Unter „Cluster ID“ sollten alle Controller-Knoten eines Clusters dieselbe Cluster-ID besitzen.
  - Überprüfen Sie unter „Configured status“ und „Active status“, ob alle Controller-Rollen bereitstehen und aktiviert sind.

- Machen Sie sich mit den operativen Auswirkungen des NSX Controller-Upgrades vertraut, während das Upgrade durchgeführt wird. Weitere Informationen dazu finden Sie unter Operative Auswirkungen von NSX-Upgrades.
- Wenn Sie ein Upgrade auf NSX 6.3.3 durchführen, muss der NSX Controller-Cluster drei Controllerknoten enthalten. Sind weniger als drei vorhanden, müssen Sie vor Beginn des Upgrades weitere Knoten hinzufügen. Schritte zum Hinzufügen von Controllerknoten finden Sie unter „Bereitstellen von NSX Controller-Clustern“ im *Installationshandbuch für NSX*.

Vorgehensweise

- Navigieren Sie zu **Startseite > Networking & Security > Installation (Home > Networking & Security > Installation)**, wählen Sie die Registerkarte **Verwaltung (Management)** aus und klicken Sie auf **Upgrade verfügbar (Upgrade Available)** in der Spalte **Status des Controller-Clusters (Controller Cluster Status)**.

  Die Controller in Ihrer Umgebung werden nacheinander aktualisiert und neu gestartet. Nachdem Sie das Upgrade gestartet haben, lädt das System die Upgrade-Datei herunter, aktualisiert jeden Controller, startet jeden Controller neu und aktualisiert den Upgrade-Status eines jeden Controllers. Die folgenden Felder zeigen den Controller-Status an:

  - Die Spalte **Status des Controller-Clusters (Controller Cluster Status)** im NSX Manager-Abschnitt zeigt den Upgrade-Status des Clusters an. Wenn das Upgrade beginnt, lautet der Status **Upgrade-Datei wird heruntergeladen (Downloading upgrade file)**. Wenn die Upgrade-Datei auf alle Controller im Cluster heruntergeladen wurde, ändert sich der Status in **Vorgang läuft (In progress)**. Wenn alle Controller im Cluster aktualisiert wurden, lautet der angezeigte Status **Vollständig (Complete)** und diese Spalte wird nicht mehr angezeigt.
  - In der Spalte **Status** im Abschnitt für die NSX Controller-Knoten wird der Status der einzelnen Controller angezeigt. Er lautet je nach NSX-Originalversion vor dem Upgrade **Verbunden (Connected)** oder **Normal**. Wenn die Controller-Dienste heruntergefahren werden und der Controller neu gestartet wird, ändert sich der Status in **Getrennt (Disconnected)**. Nach dem Abschluss des Upgrades für diesen Controller lautet der Status **Verbunden (Connected)**.
  - Die Spalte **Upgrade-Status (Upgrade Status)** im Bereich der NSX Controller-Knoten zeigt den Upgrade-Status für jeden Controller an. Der Status lautet anfangs **Upgrade-Datei wird heruntergeladen (Downloading upgrade file)**, dann **Upgrade läuft (Upgrade in progress)** und danach **Neustarten (Rebooting)**. Nach Abschluss des Controller-Upgrades lautet der Status **Aktualisiert (Upgraded)**.

    Hinweis Wenn Sie ein Upgrade von NSX 6.3.2 oder früher auf NSX 6.3.3 oder höher durchführen, wird der Status **Upgrade-Datei wird heruntergeladen (Downloading upgrade file)** durch **In Warteschlange für Upgrade (Queued For Upgrade)** ersetzt.

Wenn das Upgrade abgeschlossen ist, wird in der Spalte **Softwareversion (Software Version)** im Bereich der NSX Controller-Knoten für jeden Controller **6.3.***buildNumber* angezeigt. Führen Sie den Befehl **show control-cluster status** erneut aus, um sicherzustellen, dass die Controller eine Mehrheit herstellen können. Wenn die NSX Controller-Cluster-Mehrheit nicht neu gebildet werden kann, überprüfen Sie die Controller- und NSX Manager-Protokolle.

Die durchschnittliche Dauer eines Upgrades beträgt 6-8 Minuten. Wenn das Upgrade nicht innerhalb des Zeitlimits (30 Minuten) abgeschlossen ist, wird in der Spalte **Upgrade-Status (Upgrade Status)** der Status **Fehlgeschlagen (Failed)** angezeigt. Klicken Sie im NSX Manager-Abschnitt erneut auf **Upgrade verfügbar (Upgrade Available)**, um den Upgrade-Vorgang von dem Punkt aus fortzusetzen, wo er angehalten wurde.

Wenn Netzwerkprobleme ein erfolgreiches Upgrade innerhalb des 30-minütigen Zeitlimits verhindern, müssen Sie ein längeres Zeitlimit konfigurieren. Erstellen Sie zusammen mit dem VMware-Support eine Diagnose, beheben Sie die zugrunde liegenden Probleme und konfigurieren Sie, falls erforderlich, ein längeres Zeitlimit.

Falls das Controller-Upgrade fehlschlägt, überprüfen Sie die Verbindung zwischen den Controllern und NSX Manager.

Es gibt ein Szenario, in dem der erste Controller erfolgreich aktualisiert werden kann, der zweite aber nicht. Angenommen es befinden sich drei Controller in einem Cluster. Der erste Controller wurde erfolgreich auf die neue Version aktualisiert und der zweite Controller wird gerade aktualisiert. Falls das Upgrade des zweiten Controllers fehlschlägt, verbleibt dieser möglicherweise in nicht verbundenem Zustand. Zudem verfügen der erste und der dritte Controller nun über zwei unterschiedliche Versionen (eine aktualisiert, die andere nicht), weshalb keine Mehrheit gebildet werden kann. An diesem Punkt kann das Upgrade nicht neu gestartet werden. Erstellen Sie einen anderen Controller, um dieses Szenario zu umgehen. Der neu erstellte Controller verfügt über die ältere Version, die mit der des dritten Controllers übereinstimmt. Diese können daher zusammen eine Mehrheit bilden. Zu diesem Zeitpunkt kann der Upgrade-Vorgang neu gestartet werden. Anweisungen zum Erstellen eines weiteren Controllers finden Sie unter dem Abschnitt zum erneuten Bereitstellen von NSX Controller im *Fehlerbehebungshandbuch zu NSX*.

Weiter

Führen Sie ein Upgrade der Host-Cluster durch.

Aktualisieren von Hostclustern

Nach dem Upgrade von NSX Manager und der NSX Controller können Sie die entsprechenden Cluster in Ihrer Umgebung aktualisieren.

Beim Upgrade von Hostclustern wird auch ein Upgrade der NSX-VIBs ausgeführt.

Wenn Sie ein Upgrade von NSX 6.2.x oder früher oder von NSX 6.3.0 oder höher mit ESXi 5.5 durchführen, müssen die Hosts für den Abschluss des Upgrades neu gestartet werden.

- Wenn der Cluster DRS-fähig ist, versucht DRS nach dem Klicken auf **Alle auflösen (Resolve all)**, die Hosts auf kontrollierte Weise neu zu starten, damit die VMs weiterhin ausgeführt werden können. Die VMs werden auf andere Hosts im Cluster verschoben. Die Hosts wechseln in den Wartungsmodus und werden neu gestartet werden.

- Wenn der Cluster nicht DRS-fähig ist, müssen Sie die virtuellen Maschinen ausschalten oder manuell einen vMotion-Vorgang für sie ausführen, bevor Sie mit dem Upgrade starten. Wenn Sie auf **Alle auflösen (Resolve all)** klicken, wechseln die Hosts in den Wartungsmodus und werden neu gestartet.

Wenn Sie ein Upgrade von NSX 6.3.0 oder höher mit ESXi 6.0 oder höher durchführen, müssen die Hosts für den Abschluss des Upgrades in den Wartungsmodus wechseln. Es ist kein Neustart erforderlich.

- Wenn der Cluster DRS-fähig ist, versucht DRS nach dem Klicken auf **Alle auflösen (Resolve all)**, die Hosts auf kontrollierte Weise in den Wartungsmodus zu versetzen, damit die VMs weiterhin ausgeführt werden können. Die VMs werden auf andere Hosts im Cluster verschoben, und die Hosts wechseln in den Wartungsmodus.
- Wenn der Cluster nicht DRS-fähig ist, müssen Sie die virtuellen Maschinen ausschalten oder manuell einen vMotion-Vorgang für sie ausführen, bevor Sie mit dem Upgrade starten. Sie müssen die Hosts für den Abschluss des Upgrades manuell in den Wartungsmodus versetzen.

Bei NSX 6.3.5 oder höher sehen Sie den EAM-Status auf der Registerkarte **Hostvorbereitung (Host Preparation)**.

Voraussetzungen

- Führen Sie ein Upgrade von NSX Manager und des NSX Controller-Clusters durch.
- Melden Sie sich beim vSphere Web Client ab und wieder an, nachdem Sie NSX Manager aktualisiert haben und bevor Sie die Host-Cluster aktualisieren.
- Machen Sie sich während der Durchführung des Upgrades mit den operativen Auswirkungen eines Hostcluster-Upgrades vertraut. Weitere Informationen dazu finden Sie unter Operative Auswirkungen von NSX-Upgrades.
- Stellen Sie sicher, dass die vollqualifizierten Domänennamen (FQDNs) all Ihrer Hosts aufgelöst werden können.
- Wenn DRS deaktiviert ist, schalten Sie die VMs aus oder verschieben Sie sie mit vMotion manuell, bevor Sie das Upgrade starten.
- Wenn DRS aktiviert ist, werden die gestarteten VMs während des Hostcluster-Upgrades automatisch verschoben. Stellen Sie vor dem Starten des Upgrades sicher, dass DRS in Ihrer Umgebung funktioniert.
  - Stellen Sie sicher, dass DRS auf den Hostclustern aktiviert ist.
  - Stellen Sie sicher, dass vMotion ordnungsgemäß funktioniert.
  - Überprüfen Sie den Zustand der Hostverbindung mit vCenter.
  - Stellen Sie sicher, dass sich mindestens drei ESXi-Hosts in jedem Hostcluster befinden. Bei einem NSX-Upgrade ist die Wahrscheinlichkeit größer, dass bei einem Hostcluster mit nur einem oder zwei Hosts Probleme bei der DRS-Zugangssteuerung auftreten. Für ein erfolgreiches NSX-Upgrade empfiehlt VMware, dass jeder Hostcluster über mindestens drei Hosts verfügt. Wenn ein Cluster weniger als drei Hosts enthält, wird empfohlen, die Hosts manuell zu evakuieren.

- Wenn sich in einem kleinen Cluster nur zwei oder drei Hosts befinden und Sie Anti-Affinitätsregeln definiert haben, die besagen, dass sich bestimmte VMs auf separaten Hosts befinden müssen, verhindern diese Regeln möglicherweise, dass DRS die VMs während des Upgrades verschiebt. Fügen Sie entweder weitere Hosts zum Cluster hinzu oder deaktivieren Sie die Anti-Affinitätsregeln während des Upgrades und aktivieren Sie sie wieder, nachdem das Upgrade abgeschlossen ist. Navigieren Sie zum Deaktivieren einer Anti-Affinitätsregel zu **Hosts und Cluster (Hosts and Clusters) > *Cluster* > Einstellungen (Manage) > verwalten (Settings) > VM-/Host-Regeln (VM/Host Rules)**. Bearbeiten Sie die Regel und deaktivieren Sie die Option **Regel aktivieren (Enable rule)**.

- Melden Sie sich bei einem der Hosts im Cluster an und führen Sie den Befehl `esxcli software vib list` aus.

  Welche VIBs vorhanden sind, hängt von den ESXi- und NSX-Versionen ab und kann sich daher beim Upgrade ändern. Beachten Sie die aktuelle Version der installierten VIBs:

ESXi-Version	NSX-Version	Installierte VIBs
5.5	6.1.x, 6.2.x oder 6.3.x	■ esx-vsip ■ esx-vxlan
6.0 oder höher	6.3.2 oder früher	■ esx-vsip ■ esx-vxlan
6.0 oder höher	6.3.3 oder höher	■ esx-nsxv

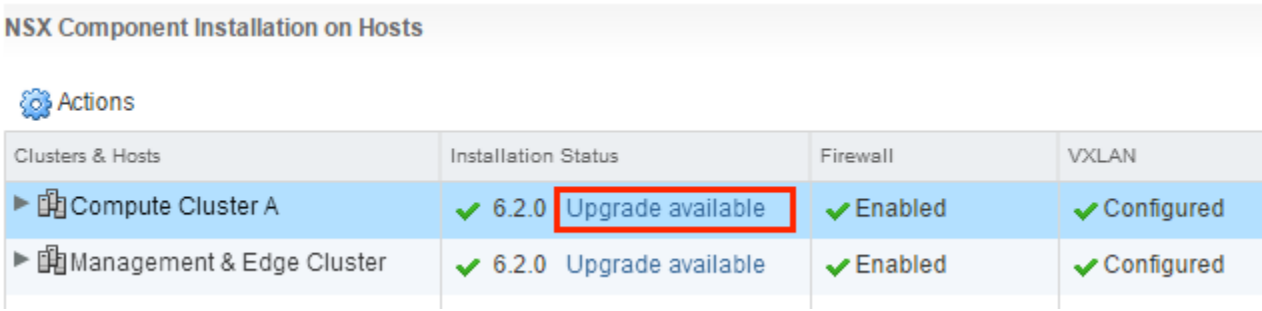
  Hinweis Einige Versionen von NSX haben zusätzliche VIBs, die während des Upgrades entfernt werden.

  - Wenn Sie das Upgrade von einer NSX-Version vor NSX 6.2 ausführen, weisen die vorbereiteten Hosts ein zusätzliches VIB auf, „esx-dvfilter-switch-security“.
  - Wenn Sie ein Upgrade von NSX 6.2.x auf Version NSX 6.2.4 oder höher durchführen, weisen die vorbereiteten Hosts ein zusätzliches „esx-vdpi“-VIB auf.

Vorgehensweise

1 Navigieren Sie im vSphere Web Client zu **Start > Networking & Security > Installation (Home > Networking & Security > Installation)** und wählen Sie die Registerkarte **Hostvorbereitung (Host Preparation)** aus.

2 Klicken Sie für jeden Cluster, für den Sie ein Upgrade durchführen möchten, auf **Upgrade verfügbar (Upgrade available)**.



Für den Installationsstatus wird `Wird installiert` angezeigt.

3 Für den Installationsstatus des Clusters wird `Nicht bereit` angezeigt. Klicken Sie auf **Nicht bereit (Not Ready)**, um weitere Informationen anzuzeigen. Klicken Sie auf **Alle auflösen (Resolve all)**, um zu versuchen, die VIB-Installation abzuschließen.

Die Hosts werden für den Abschluss des Upgrades in den Wartungsmodus versetzt und, falls erforderlich, neu gestartet.

In der Spalte „Installationsstatus“ wird `Wird installiert` angezeigt. Nach dem Abschluss des Upgrades ist in der Spalte „Installationsstatus“ ein grünes Häkchen und die aktualisierte NSX-Version enthalten.

4 Wenn die Aktion **Auflösen (Resolve)** bei aktiviertem DRS nicht durchgeführt werden kann, müssen die Hosts eventuell manuell in den Wartungsmodus versetzt werden (z. B. aufgrund von Hochverfügbarkeitsanforderungen oder DRS-Regeln). Der Upgrade-Vorgang wird angehalten und für den Installationsstatus des Clusters wird erneut `Nicht bereit` angezeigt. Klicken Sie auf **Nicht bereit (Not Ready)**, um weitere Informationen anzuzeigen. Überprüfen Sie die Hosts in der Ansicht **Hosts & Cluster (Hosts and Clusters)** und stellen Sie sicher, dass die Hosts eingeschaltet und verbunden sind und keine gestarteten VMs enthalten. Führen Sie die Aktion **Auflösen (Resolve)** dann erneut aus.

In der Spalte „Installationsstatus“ wird `Wird installiert` angezeigt. Nach dem Abschluss des Upgrades ist in der Spalte „Installationsstatus“ ein grünes Häkchen und die aktualisierte NSX-Version enthalten.

5 Wenn die Aktion **Auflösen (Resolve)** bei deaktiviertem DRS nicht durchgeführt werden kann und Sie ein Upgrade von NSX 6.3.0 oder höher mit ESXi 6.0 oder höher durchführen, müssen Sie die Hosts für den Abschluss des Upgrades manuell in den Wartungsmodus versetzen.

   a Versetzen Sie die evakuierten Hosts in den Wartungsmodus.

   b Navigieren Sie zu **Networking & Security > Installation > Hostvorbereitung (Host Preparation)**.

      Das Upgrade wird automatisch gestartet, wenn die Hosts in den Wartungsmodus wechseln. In der Spalte „Installationsstatus“ wird `Wird installiert` angezeigt. Wenn der `Installationsstatus` nicht angezeigt wird, aktualisieren Sie die Seite.

      Nach dem Abschluss des Upgrades ist in der Spalte „Installationsstatus“ ein grünes Häkchen und die aktualisierte NSX-Version enthalten.

   c Heben Sie den Wartungsmodus für die Hosts auf.

Um das Host-Update zu bestätigen, melden Sie sich bei einem der Hosts im Cluster an und führen Sie den Befehl `esxcli software vib list` aus. Stellen Sie sicher, dass die entsprechenden VIBs auf die erwartete Version aktualisiert wurden.

Wenn ein Host nicht aktualisiert werden kann, führen Sie die folgenden Fehlerbehebungsschritte durch:

- Überprüfen Sie den ESX Agent Manager auf vCenter und suchen Sie nach Warnungen und Fehlern.
- Melden Sie sich beim Host an, überprüfen Sie die Protokolldatei `/var/log/esxupdate.log` und suchen Sie nach neuen Warnungen und Fehlern.
- Stellen Sie sicher, dass DNS und NTP auf dem Host konfiguriert sind.

Informationen zu weiteren Fehlerbehebungsschritten finden Sie unter „Hostvorbereitung“ im *Fehlerbehebungshandbuch zu NSX*.

Weiter

Upgrade von NSX Edge

Upgrade von NSX Edge

Während des Upgrade-Vorgangs wird eine neue virtuelle Edge-Appliance neben der bereits vorhandenen bereitgestellt.

Wenn das neue Edge bereit ist, werden die vNICs des alten Edge getrennt und die vNICs des neuen Edge verbunden. Das neue Edge sendet dann einige ARP-Pakete (GARP), um den ARP-Cache verbundener Switches zu aktualisieren. Wenn HA bereitgestellt ist, wird der Upgrade-Vorgang zwei Mal durchgeführt.

Dieser Vorgang kann vorübergehend die Paketweiterleitung beeinträchtigen. Sie können die Auswirkungen minimieren, indem Sie das Edge so konfigurieren, dass es im ECMP-Modus funktioniert.

OSPF-Nachbarschaften sind vom Upgrade ausgenommen, wenn Graceful Restart nicht aktiviert wurde.

Voraussetzungen

- Vergewissern Sie sich, dass für NSX Manager ein Upgrade durchgeführt wurde.
- Stellen Sie sicher, dass für den NSX Controller-Cluster und die Hostvorbereitung ein Upgrade durchgeführt wurde, bevor die logischen Router aktualisiert werden.
- Stellen Sie sicher, dass ein lokaler Segment-ID-Pool vorhanden ist, auch wenn Sie nicht vorhaben, logische NSX-Switches zu erstellen.
- Stellen Sie sicher, dass die Hosts über ausreichend Ressourcen zur Bereitstellung zusätzlicher NSX Edge Services Gateway-Appliances im Rahmen des Upgrades verfügen. Das ist vor allem dann wichtig, wenn Sie ein Upgrade für mehrere NSX Edge-Appliances gleichzeitig durchführen. Unter Systemvoraussetzungen für NSX werden die für jede NSX Edge-Größe erforderlichen Ressourcen dargestellt.
  - Für eine einzelne NSX Edge-Instanz befinden sich während des Upgrades zwei NSX Edge-Appliances der geeigneten Größe im eingeschalteten Status.
  - Für eine NSX Edge-Instanz mit Hochverfügbarkeit (HA, High Availability) werden beide Ersetzungs-Appliances bereitgestellt, bevor die alten Appliances ersetzt werden. Das bedeutet, dass sich während des Upgrades einer bestimmten NSX Edge vier NSX Edge-Appliances der geeigneten Größe im eingeschalteten Status befinden. Nach dem Upgrade der NSX Edge-Instanz kann jede HA-Appliance aktiv werden.
- Stellen Sie sicher, dass die Hostcluster, die im konfigurierten und aktuellen Speicherort für die NSX Edge-Appliance aufgeführt sind, für NSX vorbereitet sind und dass für deren Messaging-Infrastruktur der Status `GREEN` (GRÜN) gilt. Wenn der konfigurierte Speicherort nicht verfügbar ist, etwa weil der Cluster nach der Erstellung der NSX Edge-Appliance entfernt wurde, überprüfen Sie nur den aktuellen Speicherort.
  - Suchen Sie die ID des ursprünglich konfigurierten Speicherorts (*configuredResourcePool* > *Id*) und des aktuellen Speicherorts (*resourcePoolId*) mit der `GET https://NSX-Manager-IP-Address/api/4.0/edges/{edgeId}/appliances`-API-Anforderung.
  - Ermitteln Sie mit der `GET https://NSX-Manager-IP-Address/api/2.0/nwfabric/status?resource={resourceId}`-API-Anforderung den Status der Hostvorbereitung und der Messaging-Infrastruktur für diese Cluster, wobei *resourceId* die ID des konfigurierten und des aktuellen Speicherorts der NSX Edge-Appliances darstellt, die zuvor gefunden wurden.
    - Suchen Sie im Antworttext nach dem Status, der der *featureId* von `com.vmware.vshield.vsm.nwfabric.hostPrep` entspricht: Der Status muss `GREEN` (GRÜN) lauten.

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.nwfabric.hostPrep</featureId>
  <featureVersion>6.3.1.5124716</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
  <installed>true</installed>
  <enabled>true</enabled>
  <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

- Suchen Sie im Antworttext nach dem Status, der der *featureId* von `com.vmware.vshield.vsm.messagingInfra` entspricht: Der Status muss `GREEN` (GRÜN) lauten.

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

- Machen Sie sich während der Durchführung des Upgrades mit den operativen Auswirkungen des NSX Edge-Upgrades vertraut. Siehe „Operative Auswirkungen von NSX-Upgrades“ im *Upgrade-Handbuch für NSX*.
- Wenn Sie ein Upgrade von NSX 6.0.x durchführen und L2 VPN auf einem NSX Edge aktiviert ist, müssen Sie vor dem Upgrade die L2 VPN-Konfiguration löschen. Nach dem Upgrade können Sie L2 VPN neu konfigurieren. Weitere Informationen finden Sie im Dokument *Installationshandbuch für NSX* unter „Überblick über L2 VPN“.

Vorgehensweise

1. Wählen Sie im vSphere Web Client **Networking & Security > NSX Edges** aus.
2. Wählen Sie für jede NSX Edge-Instanz die Option **Upgrade-Version (Upgrade Version)** aus dem Menü **Aktionen (Actions) ( )** aus.

   Falls das Upgrade mit der Fehlermeldung „Fehler beim Bereitstellen der Edge-Appliance“ fehlschlägt, stellen Sie sicher, dass der Host, auf dem die NSX Edge-Appliance bereitgestellt wird, verbunden ist und sich nicht im Wartungsmodus befindet.

Nach dem erfolgreichen Upgrade des NSX Edge lautet der **Status** „Bereitgestellt“ und in der Spalte **Version** wird die neue NSX-Version angezeigt.

Falls das Upgrade eines Edge fehlschlägt und kein Rollback auf die alte Version erfolgt, klicken Sie auf das Symbol **NSX Edge erneut bereitstellen (Redeploy NSX Edge)** und führen Sie dann das Upgrade erneut aus.

Weiter

Nach dem Upgrade von NSX Edges 6.2.4 oder früher auf die Version 6.2.5 oder höher müssen Sie den Start der virtuellen Maschine von vSphere für jede NSX Edge-Instanz in einem Cluster deaktivieren, für den vSphere HA aktiviert ist und Edges bereitgestellt sind. Öffnen Sie dazu den vSphere Web Client und suchen Sie nach dem ESXi-Host, auf dem sich die virtuelle NSX Edge-Maschine befindet: Klicken Sie auf **Verwalten (Manage) > Einstellungen (Settings)** und wählen Sie unter „Virtuelle Maschinen“ die Option „Starten/Herunterfahren von virtuellen Maschinen“ aus. Klicken Sie auf **Bearbeiten (Edit)** und vergewissern Sie sich, dass für die virtuelle Maschine der Modus „Manuell“ festgelegt ist (d. h., dass sie sich nicht in der Liste für ein automatisches Starten/Herunterfahren befindet).

Upgrade von Guest Introspection

Es ist wichtig, Guest Introspection zu aktualisieren, damit es auf die NSX Manager-Version abgestimmt ist.

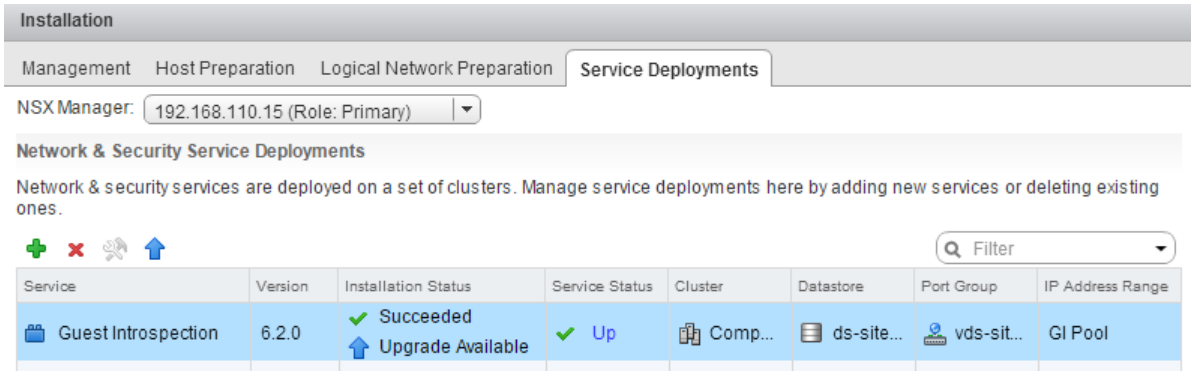
Hinweis Für die Guest Introspection-Dienst-VMs kann ein Upgrade über vSphere Web Client durchgeführt werden. Sie müssen die Dienst-VM für deren Upgrade nach dem Upgrade von NSX Manager nicht löschen. Wenn Sie die Dienst-VM löschen, wird für den Dienststatus `Fehlgeschlagen` angezeigt, da die Agenten-VM fehlt. Klicken Sie auf **Auflösen (Resolve)**, um eine neue Dienst-VM bereitzustellen, und klicken Sie dann auf **Upgrade verfügbar (Upgrade Available)**, um die neueste Guest Introspection-Dienst-VM bereitzustellen.

Voraussetzungen

Führen Sie ein Upgrade von NSX Manager, Controllern, vorbereiteten Host-Clustern und NSX Edges durch.

Vorgehensweise

1 Klicken Sie auf der Registerkarte **Installation** auf **Dienstbereitstellungen (Service Deployments)**.

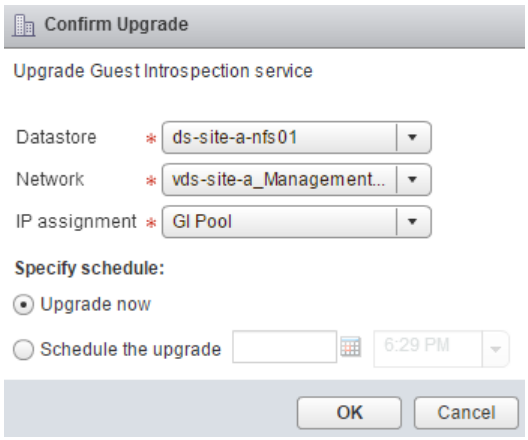


Die Spalte **Installationsstatus (Installation Status)** enthält den Wert **Upgrade verfügbar (Upgrade Available)**.

2 Wählen Sie die Guest Introspection-Bereitstellung aus, die Sie aktualisieren möchten.

Das Symbol **Upgrade** (⬆) in der Symbolleiste über der Tabelle „Dienste“ ist aktiviert.

3 Klicken Sie auf das Symbol **Upgrade** (⬆) und folgen Sie den Eingabeaufforderungen.



Nach dem Upgrade von Guest Introspection lautet der Installationsstatus `Erfolg` und der Dienststatus `Aktiv`. Virtuelle Maschinen des Guest Introspection-Dienstes werden in der vCenter Server-Bestandsliste angezeigt.

Nach dem Upgrade von Guest Introspection für einen bestimmten Cluster können Sie für jede Partnerlösung ein Upgrade durchführen. Wenn Sie Partnerlösungen aktiviert haben, finden Sie entsprechende Erläuterungen in der Upgrade-Dokumentation des Partners. Partnerlösungen bleiben geschützt, auch wenn für sie kein Upgrade durchgeführt wird.

NSX Services, die kein direktes Upgrade unterstützen

Einige NSX Services unterstützen kein direktes Upgrade. In diesen Fällen müssen Sie die Dienste deinstallieren und neu installieren.

Virtuelle Appliances für VMware-Partnersicherheit

Lesen Sie in der Partnerdokumentation nach, ob die virtuelle Appliance für die Partnersicherheit aktualisiert werden kann.

NSX SSL VPN

Ab NSX 6.2 akzeptiert das SSL VPN-Gateway nur das TLS-Protokoll. Nach einem Upgrade auf NSX 6.2 oder höher verwenden automatisch erstellte Clients jedoch automatisch das TLS-Protokoll beim Verbindungsaufbau. Darüber hinaus wird ab der Version NSX 6.2.3 TLS 1.0 nicht mehr unterstützt.

Aufgrund der Protokolländerung scheitert der Verbindungsaufbau beim SSL-Handshake-Schritt, wenn ein NSX 6.0.x-Client versucht, eine Verbindung mit einem NSX 6.2.x-Gateway oder höher herzustellen.

Nach dem Upgrade von NSX 6.0.x deinstallieren Sie die alten SSL VPN-Clients und installieren Sie die Version NSX 6.3.x der SSL VPN-Clients. Diese „Installieren des SSL-Clients auf der Remote-Site“ im *Administratorhandbuch für NSX*.

NSX L2 VPN

NSX Edge-Upgrades werden nicht unterstützt, wenn L2 VPN auf einem NSX Edge mit installiertem NSX 6.0.x installiert ist. Alle L2 VPN-Konfigurationen müssen vor dem Upgrade des NSX Edge gelöscht werden.

Checkliste nach dem Upgrade

Wenn das Upgrade abgeschlossen ist, führen Sie die nachfolgend aufgeführten Schritte aus.

Vorgehensweise

1 Erstellen Sie nach dem Upgrade eine Sicherung des aktuellen Stands des NSX Manager.

2 Stellen Sie sicher, dass VIBs auf den Hosts installiert sind.

NSX installiert diese VIBs:

```
esxcli software vib get --vibname esx-vxlan
esxcli software vib get --vibname esx-vsip
```

Überprüfen Sie, wenn Guest Introspection installiert wurde, auch, ob dieses VIB auf den Hosts vorhanden ist:

```
esxcli software vib get --vibname epsec-mux
```

3 Synchronisieren Sie den Hostnachrichtenbus erneut. VMware empfiehlt allen Kunden die erneute Synchronisierung nach einem Upgrade.

Mit dem nachfolgend aufgeführten API-Aufruf können Sie die erneute Synchronisierung auf jedem Host durchführen.

```
URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
HTTP Method : POST

Headers:

Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
```

Upgrade auf NSX 6.3.x mit Cross-vCenter NSX

Um in einer Cross-vCenter-Umgebung ein Upgrade auf NSX 6.3.x durchzuführen, müssen Sie die NSX-Komponenten in der Reihenfolge aktualisieren wie in diesem Handbuch dokumentiert.

Die NSX-Komponenten müssen in der folgenden Reihenfolge aktualisiert werden:

1 Primäre NSX Manager-Appliance

2 Alle sekundären NSX Manager-Appliances

3 NSX Controller-Cluster

4 Host-Cluster

5 NSX Edge

6 Guest Introspection

Der Upgrade-Vorgang wird von NSX Manager verwaltet. Falls das Upgrade einer Komponente fehlschlägt oder unterbrochen wird und Sie das Upgrade wiederholen oder neu starten müssen, wird der Vorgang von dem Punkt aus fortgesetzt, an dem er unterbrochen wurde. Er startet nicht wieder von vorne.

Der Upgrade-Status wird für jeden Knoten und auf Clusterebene aktualisiert.

Upgrade des primären NSX Manager in Cross-vCenter NSX

Der erste Schritt beim Upgrade der NSX-Infrastruktur besteht im Upgrade der primären NSX Manager-Appliance.

Vorsicht Die Ausführung von NSX Manager-Appliances verschiedener Versionen wird in einer Cross-vCenter NSX-Umgebung nicht unterstützt. Wenn Sie die primäre NSX Manager-Appliance aktualisieren, müssen Sie auch die sekundären NSX Manager-Appliances aktualisieren.

Bei einem Upgrade von NSX Manager in einer Cross-vCenter NSX-Umgebung dürfen Sie keine Änderungen an globalen Objekten vornehmen, bis der primäre NSX Manager und alle sekundären NSX Manager aktualisiert sind. Dazu gehört das Erstellen, Aktualisieren oder Löschen von globalen Objekten und Vorgänge, die globale Objekte betreffen (z. B. das Anwenden eines globalen Sicherheits-Tags für eine virtuelle Maschine).

Beim Upgrade können Sie auswählen, ob Sie am „Programm zur Verbesserung der Benutzerfreundlichkeit“ (CEIP, Customer Experience Improvement Program) für NSX teilnehmen möchten. Unter „Programm zur Verbesserung der Benutzerfreundlichkeit im *Administratorhandbuch für NSX*“ finden Sie weitere Informationen dazu, inklusive Informationen, wie Sie sich daran beteiligen und wieder abmelden können.

Voraussetzungen

- Überprüfen Sie die NSX Manager-Nutzung des Dateisystems und führen Sie eine Bereinigung durch, wenn die Nutzung bei 100 Prozent liegt.
  a Melden Sie sich bei NSX Manager an und führen Sie `show filesystems` aus, um die Nutzung des Dateisystems anzuzeigen.

b Wenn die Nutzung bei 100 Prozent liegt, führen Sie die Befehle `purge log manager` und `purge log system` aus.

c Starten Sie die NSX Manager-Appliance neu, damit die Protokollbereinigung wirksam wird.

- Stellen Sie vor dem Upgrade sicher, dass der reservierte Arbeitsspeicher der virtuellen Appliance für NSX Manager die Systemanforderungen erfüllt.

  Weitere Informationen dazu finden Sie unter Systemvoraussetzungen für NSX.

- Wenn sich Data Security in Ihrer Umgebung befindet, deinstallieren Sie es, bevor Sie NSX Manager aktualisieren. Weitere Informationen dazu finden Sie unter Deinstallieren von NSX Data Security. Data Security wurde aus NSX 6.3.x entfernt.
- Sichern Sie Ihre aktuelle Konfiguration und laden Sie die Protokolle des technischen Supports herunter, bevor Sie mit dem Upgrade beginnen. Weitere Informationen dazu finden Sie unter Sichern und Wiederherstellen von NSX.
- Laden Sie das NSX-Upgrade-Paket herunter und überprüfen Sie die MD5-Prüfsumme. Weitere Informationen dazu finden Sie unter Herunterladen des NSX-Upgrade-Pakets und Überprüfen der MD5-Prüfsumme.
- Informieren Sie sich über die operativen Auswirkungen des NSX Manager-Upgrades, während das Upgrade läuft. Weitere Informationen dazu finden Sie unter Operative Auswirkungen von NSX-Upgrades.
- Sie müssen alle NSX Manager in einer Cross-vCenter NSX-Umgebung im selben Wartungsfenster aktualisieren.
- Planen Sie ein Upgrade für alle NSX Manager, die mit vCenter Server-Systemen verbunden sind, die den gleichen SSO-Server für dasselbe Wartungsfenster (einschließlich vCenter Server-Systemen im erweiterten verknüpften Modus), verwenden. Wenn das nicht möglich ist, finden Sie dafür unter https://kb.vmware.com/kb/2127061 eine Problemumgehung.

Vorgehensweise

1. Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
2. Klicken Sie auf der Startseite auf **Upgrade**.
3. Klicken Sie auf **Upgrade durchführen (Upgrade)**, anschließend auf **Datei auswählen (Choose File)** und rufen Sie die Datei `VMware-NSX-Manager-upgrade-bundle-`*releaseNumber-NSXbuild-Number*`.tar.gz` auf. Klicken Sie auf **Fortsetzen (Continue)**, um das Hochladen zu starten.

   Der Upload-Status wird im Browserfenster angezeigt.

4 Im Dialogfeld „Upgrade“ legen Sie fest, ob SSH aktiviert werden soll, und ob Sie am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teilnehmen möchten. Klicken Sie auf **Upgrade durchführen (Upgrade)**, um das Upgrade zu starten.

   Der Upgrade-Status wird im Browserfenster angezeigt.

   Warten Sie, bis der Upgrade-Vorgang abgeschlossen ist und die NSX Manager-Anmeldeseite angezeigt wird.

5 Melden Sie sich erneut bei der virtuellen Appliance für NSX Manager an und klicken Sie auf der Startseite auf **Upgrade**. Bestätigen Sie, dass der Upgrade-Status **Abgeschlossen (Complete)** lautet und dass die Version- und Build-Nummer oben rechts mit dem geraden installierten Upgrade-Paket übereinstimmt.

Wenn Sie während des Upgrades beim vSphere Web Client angemeldet sind, werden auf der Seite **Networking & Security (Networking and Security) > Installation > Management** Warnungen zu Synchronisierungsfehlern angezeigt. Dies ist darauf zurückzuführen, dass NSX Manager-Appliances mit verschiedenen Versionen von NSX ausgeführt werden. Sie müssen ein Upgrade für die sekundären NSX Manager-Appliances durchführen, bevor Sie das Upgrade fortsetzen.

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 korrekt in vSphere Web Client angezeigt wird, löschen Sie den Zwischenspeicher und den Verlauf Ihres Browsers. Wird dieser Schritt nicht durchgeführt, wird möglicherweise eine Fehlermeldung in der Art „Es ist ein interner Fehler aufgetreten – Fehler #1009“ angezeigt, wenn in vSphere Web Client Änderungen an der NSX-Konfiguration vorgenommen werden.

Wenn die Registerkarte „Networking & Security“ im vSphere Web Client nicht angezeigt wird, setzen Sie den vSphere Web Client-Server zurück:

- Öffnen Sie in vCenter 5.5 „https://<vcenter-ip>: 5480“ und starten Sie den Web-Client-Server neu.
- Melden Sie sich in der vCenter Server Appliance 6.0 bei der vCenter Server-Shell als Root-Benutzer an und führen Sie die folgenden Befehle aus:

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- Führen Sie dazu in vCenter Server 6.0 auf Windows die nachfolgend aufgeführten Befehle aus.

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

Es wird empfohlen, unterschiedliche Webclients zum Verwalten der vCenter Server zu verwenden, die unterschiedliche Versionen von NSX Manager ausführen. Dadurch werden unerwartete Fehler vermieden, wenn unterschiedliche Versionen von NSX-Plug-Ins ausgeführt werden.

Erstellen Sie nach dem Upgrade von NSX Manager eine neue NSX Manager-Sicherungsdatei. Weitere Informationen dazu finden Sie unter Sichern und Wiederherstellen von NSX. Die vorherige NSX Manager-Sicherung gilt nur für die vorherige Version.

Weiter

Aktualisieren Sie alle sekundären NSX Manager-Appliances

Upgrade aller sekundären NSX Manager-Appliances in Cross-vCenter NSX

Sie müssen alle sekundären NSX Manager-Appliances aktualisieren, bevor Sie andere NSX-Komponenten aktualisieren.

Führen Sie die folgenden Schritte zum Aktualisieren einer sekundären NSX Manager-Appliance aus. Wiederholen Sie diese Schritte für alle sekundären NSX Manager-Appliances in der Cross-vCenter NSX-Umgebung.

Bei einem Upgrade von NSX Manager in einer Cross-vCenter NSX-Umgebung dürfen Sie keine Änderungen an globalen Objekten vornehmen, bis der primäre NSX Manager und alle sekundären NSX Manager aktualisiert sind. Dazu gehört das Erstellen, Aktualisieren oder Löschen von globalen Objekten und Vorgänge, die globale Objekte betreffen (z. B. das Anwenden eines globalen Sicherheits-Tags für eine virtuelle Maschine).

Beim Upgrade können Sie auswählen, ob Sie am „Programm zur Verbesserung der Benutzerfreundlichkeit“ (CEIP, Customer Experience Improvement Program) für NSX teilnehmen möchten. Unter „Programm zur Verbesserung der Benutzerfreundlichkeit im *Administratorhandbuch für NSX*“ finden Sie weitere Informationen dazu, inklusive Informationen, wie Sie sich daran beteiligen und wieder abmelden können.

Voraussetzungen

- Stellen Sie sicher, dass die primäre NSX Manager-Appliance aktualisiert wird.
- Überprüfen Sie die NSX Manager-Nutzung des Dateisystems und führen Sie eine Bereinigung durch, wenn die Nutzung bei 100 Prozent liegt.
  a. Melden Sie sich bei NSX Manager an und führen Sie `show filesystems` aus, um die Nutzung des Dateisystems anzuzeigen.
  b. Wenn die Nutzung bei 100 Prozent liegt, führen Sie die Befehle `purge log manager` und `purge log system` aus.
  c. Starten Sie die NSX Manager-Appliance neu, damit die Protokollbereinigung wirksam wird.
- Stellen Sie vor dem Upgrade sicher, dass der reservierte Arbeitsspeicher der virtuellen Appliance für NSX Manager die Systemanforderungen erfüllt.

  Weitere Informationen dazu finden Sie unter Systemvoraussetzungen für NSX.

- Wenn sich Data Security in Ihrer Umgebung befindet, deinstallieren Sie es, bevor Sie NSX Manager aktualisieren. Weitere Informationen dazu finden Sie unter Deinstallieren von NSX Data Security. Data Security wurde aus NSX 6.3.x entfernt.
- Sichern Sie Ihre aktuelle Konfiguration und laden Sie die Protokolle des technischen Supports herunter, bevor Sie mit dem Upgrade beginnen. Weitere Informationen dazu finden Sie unter Sichern und Wiederherstellen von NSX.
- Laden Sie das NSX-Upgrade-Paket herunter und überprüfen Sie die MD5-Prüfsumme. Weitere Informationen dazu finden Sie unter Herunterladen des NSX-Upgrade-Pakets und Überprüfen der MD5-Prüfsumme.
- Informieren Sie sich über die operativen Auswirkungen des NSX Manager-Upgrades, während das Upgrade läuft. Weitere Informationen dazu finden Sie unter Operative Auswirkungen von NSX-Upgrades.
- Sie müssen alle NSX Manager in einer Cross-vCenter NSX-Umgebung im selben Wartungsfenster aktualisieren.
- Planen Sie ein Upgrade für alle NSX Manager, die mit vCenter Server-Systemen verbunden sind, die den gleichen SSO-Server für dasselbe Wartungsfenster (einschließlich vCenter Server-Systemen im erweiterten verknüpften Modus), verwenden. Wenn das nicht möglich ist, finden Sie dafür unter https://kb.vmware.com/kb/2127061 eine Problemumgehung.

Vorgehensweise

1. Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
2. Klicken Sie auf der Startseite auf **Upgrade**.
3. Klicken Sie auf **Upgrade durchführen (Upgrade)**, anschließend auf **Datei auswählen (Choose File)** und rufen Sie die Datei `VMware-NSX-Manager-upgrade-bundle-`*releaseNumber-NSXbuild-Number*`.tar.gz` auf. Klicken Sie auf **Fortsetzen (Continue)**, um das Hochladen zu starten.

   Der Upload-Status wird im Browserfenster angezeigt.
4. Im Dialogfeld „Upgrade“ legen Sie fest, ob SSH aktiviert werden soll, und ob Sie am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teilnehmen möchten. Klicken Sie auf **Upgrade durchführen (Upgrade)**, um das Upgrade zu starten.

   Der Upgrade-Status wird im Browserfenster angezeigt.

   Warten Sie, bis der Upgrade-Vorgang abgeschlossen ist und die NSX Manager-Anmeldeseite angezeigt wird.
5. Melden Sie sich erneut bei der virtuellen Appliance für NSX Manager an und klicken Sie auf der Startseite auf **Upgrade**. Bestätigen Sie, dass der Upgrade-Status **Abgeschlossen (Complete)** lautet und dass die Version- und Build-Nummer oben rechts mit dem geraden installierten Upgrade-Paket übereinstimmt.

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 korrekt in vSphere Web Client angezeigt wird, löschen Sie den Zwischenspeicher und den Verlauf Ihres Browsers. Wird dieser Schritt nicht durchgeführt, wird möglicherweise eine Fehlermeldung in der Art „Es ist ein interner Fehler aufgetreten – Fehler #1009“ angezeigt, wenn in vSphere Web Client Änderungen an der NSX-Konfiguration vorgenommen werden.

Wenn die Registerkarte „Networking & Security“ im vSphere Web Client nicht angezeigt wird, setzen Sie den vSphere Web Client-Server zurück:

- Öffnen Sie in vCenter 5.5 „https://<vcenter-ip>: 5480“ und starten Sie den Web-Client-Server neu.
- Melden Sie sich in der vCenter Server Appliance 6.0 bei der vCenter Server-Shell als Root-Benutzer an und führen Sie die folgenden Befehle aus:

```
Command> shell.set --enabled True
Command> shell
localhost:~ # cd /bin
localhost:~ # service-control --stop vsphere-client
localhost:~ # service-control --start vsphere-client
```

- Führen Sie dazu in vCenter Server 6.0 auf Windows die nachfolgend aufgeführten Befehle aus.

```
cd C:\Program Files\VMware\vCenter Server\bin
service-control --stop vspherewebclientsvc
service-control --start vspherewebclientsvc
```

Es wird empfohlen, unterschiedliche Webclients zum Verwalten der vCenter Server zu verwenden, die unterschiedliche Versionen von NSX Manager ausführen. Dadurch werden unerwartete Fehler vermieden, wenn unterschiedliche Versionen von NSX-Plug-Ins ausgeführt werden.

Erstellen Sie nach dem Upgrade von NSX Manager eine neue NSX Manager-Sicherungsdatei. Weitere Informationen dazu finden Sie unter Sichern und Wiederherstellen von NSX. Die vorherige NSX Manager-Sicherung gilt nur für die vorherige Version.

Weiter

Upgrade des NSX Controller-Clusters in Cross-vCenter NSX

Upgrade des NSX Controller-Clusters in Cross-vCenter NSX

Die Controller in Ihrer Umgebung werden auf Clusterebene aktualisiert. Wenn für den NSX Controller-Cluster ein Upgrade verfügbar ist, wird im Bereich **Networking & Security > Installation > Management** neben dem primären NSX Manager ein Upgrade-Link dargestellt.

Es wird empfohlen, die Controller während eines Wartungsfensters zu aktualisieren.

Das NSX Controller-Upgrade führt dazu, dass auf jeden Controller-Knoten eine Upgrade-Datei heruntergeladen wird. Die Controller werden nacheinander aktualisiert. Wenn ein Upgrade durchgeführt wird, ist der Link **Upgrade verfügbar (Upgrade Available)** nicht anklickbar und API-Aufrufe zum Aktualisieren des Controller-Clusters werden so lange blockiert, bis das Upgrade abgeschlossen ist.

Wenn Sie neue Controller bereitstellen, bevor vorhandene Controller aktualisiert wurden, werden die neuen Controller in der alten Version bereitgestellt. Um einem Cluster beitreten zu können, müssen die Controller-Knoten dieselbe Version haben.

Wichtig In NSX 6.3.3 ändert sich das zugrunde liegende Betriebssystem des NSX Controllers. 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.

Beim Löschen der Controller 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.

Voraussetzungen

- Stellen Sie sicher, dass sich alle Controller im normalen Zustand befinden. Ein Upgrade ist nicht möglich, wenn sich ein oder mehrere Controller im Zustand „Getrennt“ befinden. Um einen getrennten Controller neu zu verbinden, versuchen Sie, die virtuelle Controller-Appliance zurückzusetzen. Klicken Sie in der Ansicht **Hosts und Cluster (Hosts and Clusters)** mit der rechten Maustaste auf den Controller und wählen Sie **Stromversorgung > Zurücksetzen (Power > Reset)**.
- Ein gültiger NSX Controller-Cluster enthält drei Controller-Knoten. Melden Sie sich bei den drei Controller-Knoten an und führen Sie den Befehl **show control-cluster status** aus.

```
controller-node# show control-cluster status

Type                Status                                          Since
--------------------------------------------------------------------------------
Join status:        Join complete                                   05/04 02:36:03
Majority status:    Connected to cluster majority                   05/19 23:57:23
Restart status:     This controller can be safely restarted         05/19 23:57:12
Cluster ID:         ff3ebaeb-de68-4455-a3ca-4824e31863a8
Node UUID:          ff3ebaeb-de68-4455-a3ca-4824e31863a8

Role                Configured status   Active status
--------------------------------------------------------------------------------
api_provider        enabled             activated
persistence_server  enabled             activated
switch_manager      enabled             activated
logical_manager     enabled             activated
directory_server    enabled             activated
```

  - Überprüfen Sie unter „Join Status“, ob der Controller-Knoten „Join Complete“ meldet.
  - Überprüfen Sie unter „Majority Status“, ob der Controller mit der „Cluster Majority“ verbunden ist.
  - Unter „Cluster ID“ sollten alle Controller-Knoten eines Clusters dieselbe Cluster-ID besitzen.
  - Überprüfen Sie unter „Configured status“ und „Active status“, ob alle Controller-Rollen bereitstehen und aktiviert sind.

- Machen Sie sich mit den operativen Auswirkungen des NSX Controller-Upgrades vertraut, während das Upgrade durchgeführt wird. Weitere Informationen dazu finden Sie unter Operative Auswirkungen von NSX-Upgrades.
- Wenn Sie ein Upgrade auf NSX 6.3.3 durchführen, muss der NSX Controller-Cluster drei Controllerknoten enthalten. Sind weniger als drei vorhanden, müssen Sie vor Beginn des Upgrades weitere Knoten hinzufügen. Schritte zum Hinzufügen von Controllerknoten finden Sie unter „Bereitstellen von NSX Controller-Clustern“ im *Installationshandbuch für NSX*.

Vorgehensweise

- Navigieren Sie zu **Startseite > Networking & Security > Installation (Home > Networking & Security > Installation)**, wählen Sie die Registerkarte **Verwaltung (Management)** aus und klicken Sie auf **Upgrade verfügbar (Upgrade Available)** in der Spalte **Status des Controller-Clusters (Controller Cluster Status)**.

  Die Controller in Ihrer Umgebung werden nacheinander aktualisiert und neu gestartet. Nachdem Sie das Upgrade gestartet haben, lädt das System die Upgrade-Datei herunter, aktualisiert jeden Controller, startet jeden Controller neu und aktualisiert den Upgrade-Status eines jeden Controllers. Die folgenden Felder zeigen den Controller-Status an:

  - Die Spalte **Status des Controller-Clusters (Controller Cluster Status)** im NSX Manager-Abschnitt zeigt den Upgrade-Status des Clusters an. Wenn das Upgrade beginnt, lautet der Status **Upgrade-Datei wird heruntergeladen (Downloading upgrade file)**. Wenn die Upgrade-Datei auf alle Controller im Cluster heruntergeladen wurde, ändert sich der Status in **Vorgang läuft (In progress)**. Wenn alle Controller im Cluster aktualisiert wurden, lautet der angezeigte Status **Vollständig (Complete)** und diese Spalte wird nicht mehr angezeigt.
  - In der Spalte **Status** im Abschnitt für die NSX Controller-Knoten wird der Status der einzelnen Controller angezeigt. Er lautet je nach NSX-Originalversion vor dem Upgrade **Verbunden (Connected)** oder **Normal**. Wenn die Controller-Dienste heruntergefahren werden und der Controller neu gestartet wird, ändert sich der Status in **Getrennt (Disconnected)**. Nach dem Abschluss des Upgrades für diesen Controller lautet der Status **Verbunden (Connected)**.
  - Die Spalte **Upgrade-Status (Upgrade Status)** im Bereich der NSX Controller-Knoten zeigt den Upgrade-Status für jeden Controller an. Der Status lautet anfangs **Upgrade-Datei wird heruntergeladen (Downloading upgrade file)**, dann **Upgrade läuft (Upgrade in progress)** und danach **Neustarten (Rebooting)**. Nach Abschluss des Controller-Upgrades lautet der Status **Aktualisiert (Upgraded)**.

    Hinweis Wenn Sie ein Upgrade von NSX 6.3.2 oder früher auf NSX 6.3.3 oder höher durchführen, wird der Status **Upgrade-Datei wird heruntergeladen (Downloading upgrade file)** durch **In Warteschlange für Upgrade (Queued For Upgrade)** ersetzt.

Wenn das Upgrade abgeschlossen ist, wird in der Spalte **Softwareversion (Software Version)** im Bereich der NSX Controller-Knoten für jeden Controller **6.3.***buildNumber* angezeigt. Führen Sie den Befehl **show control-cluster status** erneut aus, um sicherzustellen, dass die Controller eine Mehrheit herstellen können. Wenn die NSX Controller-Cluster-Mehrheit nicht neu gebildet werden kann, überprüfen Sie die Controller- und NSX Manager-Protokolle.

Nach dem Upgrade der Controller wird eventuell einem oder mehreren Controller-Knoten eine neue Controller-ID zugewiesen. Dies ist ein erwartetes Verhalten, das davon abhängig ist, wann der sekundäre NSX Manager die Knoten abruft.

Die durchschnittliche Dauer eines Upgrades beträgt 6-8 Minuten. Wenn das Upgrade nicht innerhalb des Zeitlimits (30 Minuten) abgeschlossen ist, wird in der Spalte **Upgrade-Status (Upgrade Status)** der Status **Fehlgeschlagen (Failed)** angezeigt. Klicken Sie im NSX Manager-Abschnitt erneut auf **Upgrade verfügbar (Upgrade Available)**, um den Upgrade-Vorgang von dem Punkt aus fortzusetzen, wo er angehalten wurde.

Wenn Netzwerkprobleme ein erfolgreiches Upgrade innerhalb des 30-minütigen Zeitlimits verhindern, müssen Sie ein längeres Zeitlimit konfigurieren. Erstellen Sie zusammen mit dem VMware-Support eine Diagnose, beheben Sie die zugrunde liegenden Probleme und konfigurieren Sie, falls erforderlich, ein längeres Zeitlimit.

Falls das Controller-Upgrade fehlschlägt, überprüfen Sie die Verbindung zwischen den Controllern und NSX Manager.

Es gibt ein Szenario, in dem der erste Controller erfolgreich aktualisiert werden kann, der zweite aber nicht. Angenommen es befinden sich drei Controller in einem Cluster. Der erste Controller wurde erfolgreich auf die neue Version aktualisiert und der zweite Controller wird gerade aktualisiert. Falls das Upgrade des zweiten Controllers fehlschlägt, verbleibt dieser möglicherweise in nicht verbundenem Zustand. Zudem verfügen der erste und der dritte Controller nun über zwei unterschiedliche Versionen (eine aktualisiert, die andere nicht), weshalb keine Mehrheit gebildet werden kann. An diesem Punkt kann das Upgrade nicht neu gestartet werden. Erstellen Sie einen anderen Controller, um dieses Szenario zu umgehen. Der neu erstellte Controller verfügt über die ältere Version, die mit der des dritten Controllers übereinstimmt. Diese können daher zusammen eine Mehrheit bilden. Zu diesem Zeitpunkt kann der Upgrade-Vorgang neu gestartet werden. Anweisungen zum Erstellen eines weiteren Controllers finden Sie unter dem Abschnitt zum erneuten Bereitstellen von NSX Controller im *Fehlerbehebungshandbuch zu NSX*.

Weiter

Upgrade von Hostclustern in Cross-vCenter NSX.

Upgrade von Hostclustern in Cross-vCenter NSX

Nach dem Upgrade aller NSX Manager-Appliances und des NSX Controller-Clusters müssen Sie alle Hostcluster in der Cross-vCenter NSX-Umgebung aktualisieren.

Beim Upgrade von Hostclustern wird auch ein Upgrade der NSX-VIBs ausgeführt.

Wenn Sie ein Upgrade von NSX 6.2.x oder früher oder von NSX 6.3.0 oder höher mit ESXi 5.5 durchführen, müssen die Hosts für den Abschluss des Upgrades neu gestartet werden.

- Wenn der Cluster DRS-fähig ist, versucht DRS nach dem Klicken auf **Alle auflösen (Resolve all)**, die Hosts auf kontrollierte Weise neu zu starten, damit die VMs weiterhin ausgeführt werden können. Die VMs werden auf andere Hosts im Cluster verschoben. Die Hosts wechseln in den Wartungsmodus und werden neu gestartet werden.
- Wenn der Cluster nicht DRS-fähig ist, müssen Sie die virtuellen Maschinen ausschalten oder manuell einen vMotion-Vorgang für sie ausführen, bevor Sie mit dem Upgrade starten. Wenn Sie auf **Alle auflösen (Resolve all)** klicken, wechseln die Hosts in den Wartungsmodus und werden neu gestartet.

Wenn Sie ein Upgrade von NSX 6.3.0 oder höher mit ESXi 6.0 oder höher durchführen, müssen die Hosts für den Abschluss des Upgrades in den Wartungsmodus wechseln. Es ist kein Neustart erforderlich.

- Wenn der Cluster DRS-fähig ist, versucht DRS nach dem Klicken auf **Alle auflösen (Resolve all)**, die Hosts auf kontrollierte Weise in den Wartungsmodus zu versetzen, damit die VMs weiterhin ausgeführt werden können. Die VMs werden auf andere Hosts im Cluster verschoben, und die Hosts wechseln in den Wartungsmodus.
- Wenn der Cluster nicht DRS-fähig ist, müssen Sie die virtuellen Maschinen ausschalten oder manuell einen vMotion-Vorgang für sie ausführen, bevor Sie mit dem Upgrade starten. Sie müssen die Hosts für den Abschluss des Upgrades manuell in den Wartungsmodus versetzen.

Bei NSX 6.3.5 oder höher sehen Sie den EAM-Status auf der Registerkarte **Hostvorbereitung (Host Preparation)**.

Voraussetzungen

- Führen Sie ein Upgrade von NSX Manager und des NSX Controller-Clusters durch.
- Melden Sie sich beim vSphere Web Client ab und wieder an, nachdem Sie NSX Manager aktualisiert haben und bevor Sie die Host-Cluster aktualisieren.
- Machen Sie sich während der Durchführung des Upgrades mit den operativen Auswirkungen eines Hostcluster-Upgrades vertraut. Weitere Informationen dazu finden Sie unter Operative Auswirkungen von NSX-Upgrades.
- Stellen Sie sicher, dass die vollqualifizierten Domänennamen (FQDNs) all Ihrer Hosts aufgelöst werden können.
- Wenn DRS deaktiviert ist, schalten Sie die VMs aus oder verschieben Sie sie mit vMotion manuell, bevor Sie das Upgrade starten.
- Wenn DRS aktiviert ist, werden die gestarteten VMs während des Hostcluster-Upgrades automatisch verschoben. Stellen Sie vor dem Starten des Upgrades sicher, dass DRS in Ihrer Umgebung funktioniert.
  - Stellen Sie sicher, dass DRS auf den Hostclustern aktiviert ist.
  - Stellen Sie sicher, dass vMotion ordnungsgemäß funktioniert.

- Überprüfen Sie den Zustand der Hostverbindung mit vCenter.
- Stellen Sie sicher, dass sich mindestens drei ESXi-Hosts in jedem Hostcluster befinden. Bei einem NSX-Upgrade ist die Wahrscheinlichkeit größer, dass bei einem Hostcluster mit nur einem oder zwei Hosts Probleme bei der DRS-Zugangssteuerung auftreten. Für ein erfolgreiches NSX-Upgrade empfiehlt VMware, dass jeder Hostcluster über mindestens drei Hosts verfügt. Wenn ein Cluster weniger als drei Hosts enthält, wird empfohlen, die Hosts manuell zu evakuieren.
- Wenn sich in einem kleinen Cluster nur zwei oder drei Hosts befinden und Sie Anti-Affinitätsregeln definiert haben, die besagen, dass sich bestimmte VMs auf separaten Hosts befinden müssen, verhindern diese Regeln möglicherweise, dass DRS die VMs während des Upgrades verschiebt. Fügen Sie entweder weitere Hosts zum Cluster hinzu oder deaktivieren Sie die Anti-Affinitätsregeln während des Upgrades und aktivieren Sie sie wieder, nachdem das Upgrade abgeschlossen ist. Navigieren Sie zum Deaktivieren einer Anti-Affinitätsregel zu **Hosts und Cluster (Hosts and Clusters) > *Cluster* > Einstellungen (Manage) > verwalten (Settings) > VM-/Host-Regeln (VM/Host Rules)**. Bearbeiten Sie die Regel und deaktivieren Sie die Option **Regel aktivieren (Enable rule)**.

- Melden Sie sich bei einem der Hosts im Cluster an und führen Sie den Befehl `esxcli software vib list` aus.

  Welche VIBs vorhanden sind, hängt von den ESXi- und NSX-Versionen ab und kann sich daher beim Upgrade ändern. Beachten Sie die aktuelle Version der installierten VIBs:

ESXi-Version	NSX-Version	Installierte VIBs
5.5	6.1.x, 6.2.x oder 6.3.x	■ esx-vsip ■ esx-vxlan
6.0 oder höher	6.3.2 oder früher	■ esx-vsip ■ esx-vxlan
6.0 oder höher	6.3.3 oder höher	■ esx-nsxv

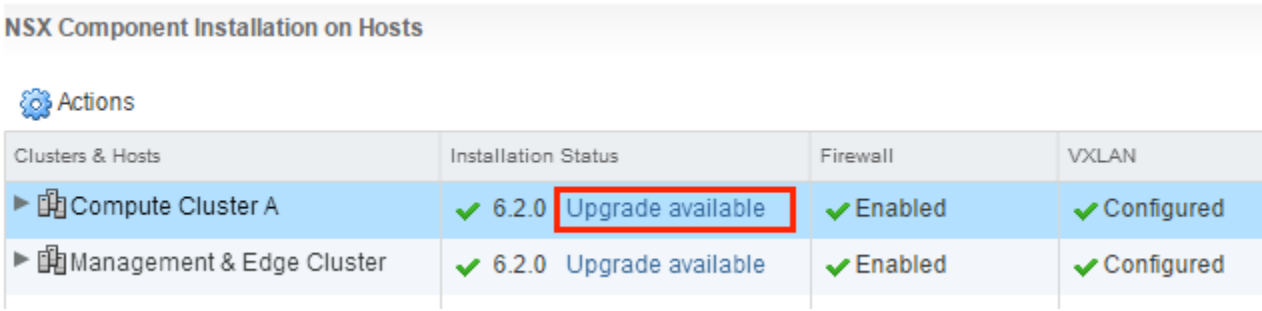
  Hinweis Einige Versionen von NSX haben zusätzliche VIBs, die während des Upgrades entfernt werden.

  - Wenn Sie das Upgrade von einer NSX-Version vor NSX 6.2 ausführen, weisen die vorbereiteten Hosts ein zusätzliches VIB auf, „esx-dvfilter-switch-security“.
  - Wenn Sie ein Upgrade von NSX 6.2.x auf Version NSX 6.2.4 oder höher durchführen, weisen die vorbereiteten Hosts ein zusätzliches „esx-vdpi“-VIB auf.

Vorgehensweise

1 Navigieren Sie im vSphere Web Client zu **Start > Networking & Security > Installation (Home > Networking & Security > Installation)** und wählen Sie die Registerkarte **Hostvorbereitung (Host Preparation)** aus.

2 Klicken Sie für jeden Cluster, für den Sie ein Upgrade durchführen möchten, auf **Upgrade verfügbar (Upgrade available)**.



Für den Installationsstatus wird `Wird installiert` angezeigt.

3 Für den Installationsstatus des Clusters wird `Nicht bereit` angezeigt. Klicken Sie auf **Nicht bereit (Not Ready)**, um weitere Informationen anzuzeigen. Klicken Sie auf **Alle auflösen (Resolve all)**, um zu versuchen, die VIB-Installation abzuschließen.

Die Hosts werden für den Abschluss des Upgrades in den Wartungsmodus versetzt und, falls erforderlich, neu gestartet.

In der Spalte „Installationsstatus“ wird `Wird installiert` angezeigt. Nach dem Abschluss des Upgrades ist in der Spalte „Installationsstatus“ ein grünes Häkchen und die aktualisierte NSX-Version enthalten.

4 Wenn die Aktion **Auflösen (Resolve)** bei aktiviertem DRS nicht durchgeführt werden kann, müssen die Hosts eventuell manuell in den Wartungsmodus versetzt werden (z. B. aufgrund von Hochverfügbarkeitsanforderungen oder DRS-Regeln). Der Upgrade-Vorgang wird angehalten und für den Installationsstatus des Clusters wird erneut `Nicht bereit` angezeigt. Klicken Sie auf **Nicht bereit (Not Ready)**, um weitere Informationen anzuzeigen. Überprüfen Sie die Hosts in der Ansicht **Hosts & Cluster (Hosts and Clusters)** und stellen Sie sicher, dass die Hosts eingeschaltet und verbunden sind und keine gestarteten VMs enthalten. Führen Sie die Aktion **Auflösen (Resolve)** dann erneut aus.

In der Spalte „Installationsstatus“ wird `Wird installiert` angezeigt. Nach dem Abschluss des Upgrades ist in der Spalte „Installationsstatus“ ein grünes Häkchen und die aktualisierte NSX-Version enthalten.

5 Wenn die Aktion **Auflösen (Resolve)** bei deaktiviertem DRS nicht durchgeführt werden kann und Sie ein Upgrade von NSX 6.3.0 oder höher mit ESXi 6.0 oder höher durchführen, müssen Sie die Hosts für den Abschluss des Upgrades manuell in den Wartungsmodus versetzen.

   a Versetzen Sie die evakuierten Hosts in den Wartungsmodus.

   b Navigieren Sie zu **Networking & Security > Installation > Hostvorbereitung (Host Preparation)**.

   Das Upgrade wird automatisch gestartet, wenn die Hosts in den Wartungsmodus wechseln. In der Spalte „Installationsstatus“ wird `Wird installiert` angezeigt. Wenn der `Installationsstatus` nicht angezeigt wird, aktualisieren Sie die Seite.

   Nach dem Abschluss des Upgrades ist in der Spalte „Installationsstatus“ ein grünes Häkchen und die aktualisierte NSX-Version enthalten.

   c Heben Sie den Wartungsmodus für die Hosts auf.

Um das Host-Update zu bestätigen, melden Sie sich bei einem der Hosts im Cluster an und führen Sie den Befehl `esxcli software vib list` aus. Stellen Sie sicher, dass die entsprechenden VIBs auf die erwartete Version aktualisiert wurden.

Wenn ein Host nicht aktualisiert werden kann, führen Sie die folgenden Fehlerbehebungsschritte durch:

- Überprüfen Sie den ESX Agent Manager auf vCenter und suchen Sie nach Warnungen und Fehlern.
- Melden Sie sich beim Host an, überprüfen Sie die Protokolldatei `/var/log/esxupdate.log` und suchen Sie nach neuen Warnungen und Fehlern.
- Stellen Sie sicher, dass DNS und NTP auf dem Host konfiguriert sind.

Informationen zu weiteren Fehlerbehebungsschritten finden Sie unter „Hostvorbereitung“ im *Fehlerbehebungshandbuch zu NSX*.

Weiter

Upgrade von NSX Edge in Cross-vCenter NSX

Upgrade von NSX Edge in Cross-vCenter NSX

Während des Upgrade-Vorgangs wird eine neue virtuelle Edge-Appliance neben der bereits vorhandenen bereitgestellt.

Wenn das neue Edge bereit ist, werden die vNICs des alten Edge getrennt und die vNICs des neuen Edge verbunden. Das neue Edge sendet dann einige ARP-Pakete (GARP), um den ARP-Cache verbundener Switches zu aktualisieren. Wenn HA bereitgestellt ist, wird der Upgrade-Vorgang zwei Mal durchgeführt.

Dieser Vorgang kann vorübergehend die Paketweiterleitung beeinträchtigen. Sie können die Auswirkungen minimieren, indem Sie das Edge so konfigurieren, dass es im ECMP-Modus funktioniert.

OSPF-Nachbarschaften sind vom Upgrade ausgenommen, wenn Graceful Restart nicht aktiviert wurde.

Führen Sie ein Upgrade für die NSX Edges in allen NSX-Installationen der Cross-vCenter NSX-Umgebung durch.

Voraussetzungen

- Vergewissern Sie sich, dass für NSX Manager ein Upgrade durchgeführt wurde.
- Stellen Sie sicher, dass für den NSX Controller-Cluster und die Hostvorbereitung ein Upgrade durchgeführt wurde, bevor die logischen Router aktualisiert werden.
- Stellen Sie sicher, dass ein lokaler Segment-ID-Pool vorhanden ist, auch wenn Sie nicht vorhaben, logische NSX-Switches zu erstellen.
- Stellen Sie sicher, dass die Hosts über ausreichend Ressourcen zur Bereitstellung zusätzlicher NSX Edge Services Gateway-Appliances im Rahmen des Upgrades verfügen. Das ist vor allem dann wichtig, wenn Sie ein Upgrade für mehrere NSX Edge-Appliances gleichzeitig durchführen. Unter Systemvoraussetzungen für NSX werden die für jede NSX Edge-Größe erforderlichen Ressourcen dargestellt.
  - Für eine einzelne NSX Edge-Instanz befinden sich während des Upgrades zwei NSX Edge-Appliances der geeigneten Größe im eingeschalteten Status.
  - Für eine NSX Edge-Instanz mit Hochverfügbarkeit (HA, High Availability) werden beide Ersetzungs-Appliances bereitgestellt, bevor die alten Appliances ersetzt werden. Das bedeutet, dass sich während des Upgrades einer bestimmten NSX Edge vier NSX Edge-Appliances der geeigneten Größe im eingeschalteten Status befinden. Nach dem Upgrade der NSX Edge-Instanz kann jede HA-Appliance aktiv werden.
- Stellen Sie sicher, dass die Hostcluster, die im konfigurierten und aktuellen Speicherort für die NSX Edge-Appliance aufgeführt sind, für NSX vorbereitet sind und dass für deren Messaging-Infrastruktur der Status `GREEN` (GRÜN) gilt. Wenn der konfigurierte Speicherort nicht verfügbar ist, etwa weil der Cluster nach der Erstellung der NSX Edge-Appliance entfernt wurde, überprüfen Sie nur den aktuellen Speicherort.
  - Suchen Sie die ID des ursprünglich konfigurierten Speicherorts (*configuredResourcePool* > *Id*) und des aktuellen Speicherorts (*resourcePoolId*) mit der `GET https://NSX-Manager-IP-Address/api/4.0/edges/{edgeId}/appliances`-API-Anforderung.
  - Ermitteln Sie mit der `GET https://NSX-Manager-IP-Address/api/2.0/nwfabric/status?resource={resourceId}`-API-Anforderung den Status der Hostvorbereitung und der Messaging-Infrastruktur für diese Cluster, wobei *resourceId* die ID des konfigurierten und des aktuellen Speicherorts der NSX Edge-Appliances darstellt, die zuvor gefunden wurden.
    - Suchen Sie im Antworttext nach dem Status, der der *featureId* von `com.vmware.vshield.vsm.nwfabric.hostPrep` entspricht: Der Status muss `GREEN` (GRÜN) lauten.

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.nwfabric.hostPrep</featureId>
  <featureVersion>6.3.1.5124716</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>GREEN</status>
```

```
  <installed>true</installed>
  <enabled>true</enabled>
  <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

- Suchen Sie im Antworttext nach dem Status, der der *featureId* von `com.vmware.vshield.vsm.messagingInfra` entspricht: Der Status muss `GREEN` (GRÜN) lauten.

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

- Machen Sie sich während der Durchführung des Upgrades mit den operativen Auswirkungen des NSX Edge-Upgrades vertraut. Siehe „Operative Auswirkungen von NSX-Upgrades“ im *Upgrade-Handbuch für NSX*.
- Wenn Sie ein Upgrade von NSX 6.0.x durchführen und L2 VPN auf einem NSX Edge aktiviert ist, müssen Sie vor dem Upgrade die L2 VPN-Konfiguration löschen. Nach dem Upgrade können Sie L2 VPN neu konfigurieren. Weitere Informationen finden Sie im Dokument *Installationshandbuch für NSX* unter „Überblick über L2 VPN“.

Vorgehensweise

1. Wählen Sie im vSphere Web Client **Networking & Security > NSX Edges** aus.
2. Wählen Sie für jede NSX Edge-Instanz die Option **Upgrade-Version (Upgrade Version)** aus dem Menü **Aktionen (Actions) (** **)** aus.

   Falls das Upgrade mit der Fehlermeldung „Fehler beim Bereitstellen der Edge-Appliance“ fehlschlägt, stellen Sie sicher, dass der Host, auf dem die NSX Edge-Appliance bereitgestellt wird, verbunden ist und sich nicht im Wartungsmodus befindet.

Nach dem erfolgreichen Upgrade des NSX Edge lautet der **Status** „Bereitgestellt“ und in der Spalte **Version** wird die neue NSX-Version angezeigt.

Falls das Upgrade eines Edge fehlschlägt und kein Rollback auf die alte Version erfolgt, klicken Sie auf das Symbol **NSX Edge erneut bereitstellen (Redeploy NSX Edge)** und führen Sie dann das Upgrade erneut aus.

Weiter

Nach dem Upgrade von NSX Edges 6.2.4 oder früher auf die Version 6.2.5 oder höher müssen Sie den Start der virtuellen Maschine von vSphere für jede NSX Edge-Instanz in einem Cluster deaktivieren, für den vSphere HA aktiviert ist und Edges bereitgestellt sind. Öffnen Sie dazu den vSphere Web Client und suchen Sie nach dem ESXi-Host, auf dem sich die virtuelle NSX Edge-Maschine befindet: Klicken Sie auf

Verwalten (Manage) > Einstellungen (Settings) und wählen Sie unter „Virtuelle Maschinen“ die Option „Starten/Herunterfahren von virtuellen Maschinen“ aus. Klicken Sie auf **Bearbeiten (Edit)** und vergewissern Sie sich, dass für die virtuelle Maschine der Modus „Manuell“ festgelegt ist (d. h., dass sie sich nicht in der Liste für ein automatisches Starten/Herunterfahren befindet).

Upgrade von Guest Introspection in Cross-vCenter NSX

Upgrade von Guest Introspection in Cross-vCenter NSX

Es ist wichtig, Guest Introspection zu aktualisieren, damit es auf die NSX Manager-Version abgestimmt ist.

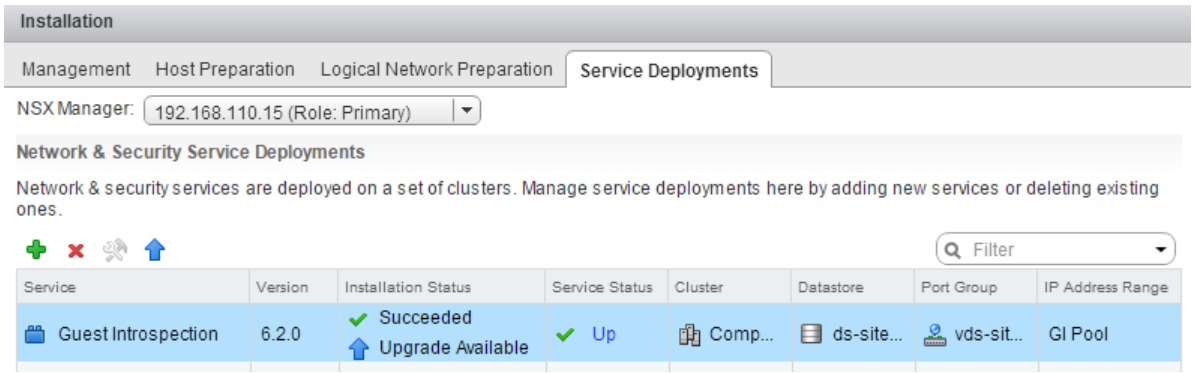
Hinweis Für die Guest Introspection-Dienst-VMs kann ein Upgrade über vSphere Web Client durchgeführt werden. Sie müssen die Dienst-VM für deren Upgrade nach dem Upgrade von NSX Manager nicht löschen. Wenn Sie die Dienst-VM löschen, wird für den Dienststatus `Fehlgeschlagen` angezeigt, da die Agenten-VM fehlt. Klicken Sie auf **Auflösen (Resolve)**, um eine neue Dienst-VM bereitzustellen, und klicken Sie dann auf **Upgrade verfügbar (Upgrade Available)**, um die neueste Guest Introspection-Dienst-VM bereitzustellen.

Voraussetzungen

Führen Sie ein Upgrade von NSX Manager, Controllern, vorbereiteten Host-Clustern und NSX Edges durch.

Vorgehensweise

1 Klicken Sie auf der Registerkarte **Installation** auf **Dienstbereitstellungen (Service Deployments)**.

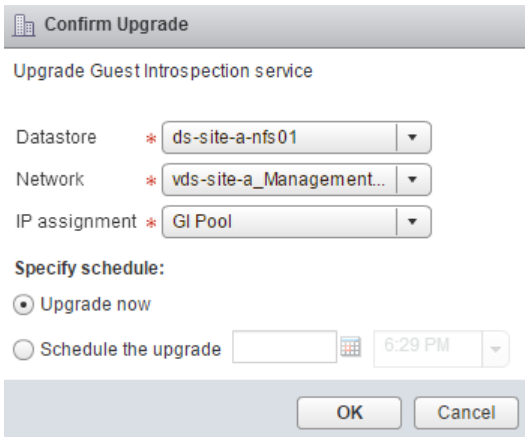


Die Spalte **Installationsstatus (Installation Status)** enthält den Wert **Upgrade verfügbar (Upgrade Available)**.

2 Wählen Sie die Guest Introspection-Bereitstellung aus, die Sie aktualisieren möchten.

Das Symbol **Upgrade** (⇧) in der Symbolleiste über der Tabelle „Dienste“ ist aktiviert.

3 Klicken Sie auf das Symbol **Upgrade** (⬆) und folgen Sie den Eingabeaufforderungen.



Nach dem Upgrade von Guest Introspection lautet der Installationsstatus `Erfolg` und der Dienststatus `Aktiv`. Virtuelle Maschinen des Guest Introspection-Dienstes werden in der vCenter Server-Bestandsliste angezeigt.

Weiter

Nach dem Upgrade von Guest Introspection für einen bestimmten Cluster können Sie für jede Partnerlösung ein Upgrade durchführen. Wenn Sie Partnerlösungen aktiviert haben, finden Sie entsprechende Erläuterungen in der Upgrade-Dokumentation des Partners. Partnerlösungen bleiben geschützt, auch wenn für sie kein Upgrade durchgeführt wird.

NSX Services, die kein direktes Upgrade unterstützen

Einige NSX Services unterstützen kein direktes Upgrade. In diesen Fällen müssen Sie die Dienste deinstallieren und neu installieren.

Virtuelle Appliances für VMware-Partnersicherheit

Lesen Sie in der Partnerdokumentation nach, ob die virtuelle Appliance für die Partnersicherheit aktualisiert werden kann.

NSX SSL VPN

Ab NSX 6.2 akzeptiert das SSL VPN-Gateway nur das TLS-Protokoll. Nach einem Upgrade auf NSX 6.2 oder höher verwenden automatisch erstellte Clients jedoch automatisch das TLS-Protokoll beim Verbindungsaufbau. Darüber hinaus wird ab der Version NSX 6.2.3 TLS 1.0 nicht mehr unterstützt.

Aufgrund der Protokolländerung scheitert der Verbindungsaufbau beim SSL-Handshake-Schritt, wenn ein NSX 6.0.x-Client versucht, eine Verbindung mit einem NSX 6.2.x-Gateway oder höher herzustellen.

Nach dem Upgrade von NSX 6.0.x deinstallieren Sie die alten SSL VPN-Clients und installieren Sie die Version NSX 6.3.x der SSL VPN-Clients. Diese „Installieren des SSL-Clients auf der Remote-Site“ im *Administratorhandbuch für NSX*.

NSX L2 VPN

NSX Edge-Upgrades werden nicht unterstützt, wenn L2 VPN auf einem NSX Edge mit installiertem NSX 6.0.x installiert ist. Alle L2 VPN-Konfigurationen müssen vor dem Upgrade des NSX Edge gelöscht werden.

Checkliste nach dem Upgrade

Wenn das Upgrade abgeschlossen ist, führen Sie die nachfolgend aufgeführten Schritte aus.

Vorgehensweise

1 Erstellen Sie nach dem Upgrade eine Sicherung des aktuellen Stands des NSX Manager.

2 Stellen Sie sicher, dass VIBs auf den Hosts installiert sind.

NSX installiert diese VIBs:

```
esxcli software vib get --vibname esx-vxlan
esxcli software vib get --vibname esx-vsip
```

Überprüfen Sie, wenn Guest Introspection installiert wurde, auch, ob dieses VIB auf den Hosts vorhanden ist:

```
esxcli software vib get --vibname epsec-mux
```

3 Synchronisieren Sie den Hostnachrichtenbus erneut. VMware empfiehlt allen Kunden die erneute Synchronisierung nach einem Upgrade.

Mit dem nachfolgend aufgeführten API-Aufruf können Sie die erneute Synchronisierung auf jedem Host durchführen.

```
URL : https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>
HTTP Method : POST

Headers:

Authorization : base64encoded value of username password
Accept : application/xml
Content-Type : application/xml
```

Upgrade von vSphere in einer NSX-Umgebung

2

Wenn Sie ein Upgrade für NSX und vSphere durchführen müssen, empfiehlt VMware, zunächst das NSX-Upgrade und anschließend das vSphere-Upgrade vorzunehmen.

Prüfen Sie anhand der VMware-Produkt-Interoperabilitätsmatrix, welche Versionen von vSphere und ESXi mit Ihrer NSX-Installation kompatibel sind. Weitere Informationen dazu finden Sie unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Detaillierte Anweisungen zu einem Upgrade von vSphere, einschließlich *vSphere-Upgrade-Handbuch* und *Handbuch zum Installieren und Verwalten von VMware vSphere Update Manager*, finden Sie in der entsprechenden Version der vSphere-Dokumentation.

Wenn Sie ein Upgrade für ESXi auf einem Host durchführen, müssen Sie auch neue NSX-VIBs auf dem Host installieren, um die Kompatibilität mit der neuen ESXi-Version sicherzustellen. NSX-Arbeitslasten können nicht auf dem aktualisierten Host ausgeführt werden, solange die NSX-VIBs nicht aktualisiert sind.

Der ESXi-Upgrade-Vorgang bei installiertem NSX 6.3.x unterscheidet sich je nach der ESXi-Version, auf die bzw. für die Sie das Upgrade durchführen.

Tabelle 2-1. Vorgehensweise für ein ESXi-Upgrade bei installiertem NSX 6.3.x

Host-Upgrade-Typ	Anforderungen für den Wartungsmodus des Hosts	Anforderungen für den Neustart des Hosts
ESXi 5.5 auf ESXi 6.0. Weitere Informationen dazu finden Sie unter Upgrade auf ESXi 6.0 in einer NSX-Umgebung.	Der Host muss im Wartungsmodus verbleiben, bis das ESXi-Upgrade und das nachfolgende NSX-VIB-Upgrade abgeschlossen sind.	Für das ESXi-Upgrade ist ein Neustart erforderlich. Auch für das nachfolgende NSX-VIB-Upgrade ist ein Neustart notwendig.
ESXi 5.5 auf ESXi 6.5. Weitere Informationen dazu finden Sie unter Upgrade auf ESXi 6.5 in einer NSX-Umgebung.	Für den Host kann der Wartungsmodus nach dem Abschluss des ESXi-Upgrades beendet werden. Eine vMotion-Verschiebung von VMs auf VXLAN-vorbereitete vSphere Distributed Switches auf dem aktualisierten Host wird blockiert, bis das nachfolgende NSX-VIB-Upgrade abgeschlossen ist.	Für das ESXi-Upgrade ist ein Neustart erforderlich. Auch für das nachfolgende NSX-VIB-Upgrade ist ein Neustart notwendig.
ESXi 6.0 auf ESXi 6.5 Weitere Informationen dazu finden Sie unter Upgrade auf ESXi 6.5 in einer NSX-Umgebung.	Für den Host kann der Wartungsmodus nach dem Abschluss des ESXi-Upgrades beendet werden. Eine vMotion-Verschiebung von VMs auf VXLAN-vorbereitete vSphere Distributed Switches auf dem aktualisierten Host wird blockiert, bis das nachfolgende NSX-VIB-Upgrade abgeschlossen ist.	Für das ESXi-Upgrade ist ein Neustart erforderlich. Für das nachfolgende NSX-VIB-Upgrade ist kein Neustart notwendig.

Dieses Kapitel behandelt die folgenden Themen:

- Upgrade auf ESXi 6.0 in einer NSX-Umgebung
- Upgrade auf ESXi 6.5 in einer NSX-Umgebung
- Erneutes Bereitstellen von Guest Introspection nach dem ESXi-Upgrade

Upgrade auf ESXi 6.0 in einer NSX-Umgebung

NSX-VIBs sind spezifisch für die auf dem Host installierte ESXi-Version. Bei einem ESXi-Upgrade müssen Sie die neuen entsprechenden NSX-VIBs für die neue ESXi-Version installieren.

Die installierten NSX-VIBs hängen von der ESXi- und NSX-Version ab. Wenn NSX 6.3.3 oder höher installiert ist und Sie eine Upgrade von ESXi 5.5 auf 6.0 ausführen, werden die VIBs „esx-vsip“ und „esx-vxlan“ entfernt und durch „esx-nsxv“ ersetzt.

ESXi-Version	NSX-Version	Installierte VIBs
5.5	Alle 6.3.x	■ esx-vsip ■ esx-vxlan
6.0 oder höher	6.3.2 oder früher	■ esx-vsip ■ esx-vxlan
6.0 oder höher	6.3.3 oder höher	■ esx-nsxv

Wichtig Sie müssen sicherstellen, dass der Host während des gesamten Upgrade-Prozesses im Wartungsmodus bleibt. Damit wird verhindert, dass VMs durch DRS oder vMotion auf den Host verschoben werden, bevor das Upgrade abgeschlossen ist.

Voraussetzungen

- Prüfen Sie anhand der VMware-Produkt-Interoperabilitätsmatrix, welche Versionen von vSphere und ESXi mit Ihrer NSX-Installation kompatibel sind. Weitere Informationen dazu finden Sie unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- Detaillierte Anweisungen zu einem Upgrade von vSphere, einschließlich *vSphere-Upgrade-Handbuch* und *Handbuch zum Installieren und Verwalten von VMware vSphere Update Manager*, finden Sie in der entsprechenden Version der vSphere-Dokumentation.
- Stellen Sie sicher, dass für die Platform Services Controller- und vCenter Server-Systeme ein Upgrade auf die neue vSphere-Version erfolgt ist.
- Stellen Sie sicher, dass die vollqualifizierten Domänennamen (FQDNs) all Ihrer Hosts aufgelöst werden können.
- Wenn DRS deaktiviert ist, schalten Sie die VMs aus oder verschieben Sie sie mit vMotion manuell, bevor Sie das Upgrade starten.
- Wenn DRS aktiviert ist, werden die gestarteten VMs während des Hostcluster-Upgrades automatisch verschoben. Stellen Sie vor dem Starten des Upgrades sicher, dass DRS in Ihrer Umgebung funktioniert.
  - Stellen Sie sicher, dass DRS auf den Hostclustern aktiviert ist.
  - Stellen Sie sicher, dass vMotion ordnungsgemäß funktioniert.
  - Überprüfen Sie den Zustand der Hostverbindung mit vCenter.
  - Stellen Sie sicher, dass sich mindestens drei ESXi-Hosts in jedem Hostcluster befinden. Bei einem NSX-Upgrade ist die Wahrscheinlichkeit größer, dass bei einem Hostcluster mit nur einem oder zwei Hosts Probleme bei der DRS-Zugangssteuerung auftreten. Für ein erfolgreiches NSX-Upgrade empfiehlt VMware, dass jeder Hostcluster über mindestens drei Hosts verfügt. Wenn ein Cluster weniger als drei Hosts enthält, wird empfohlen, die Hosts manuell zu evakuieren.
  - Wenn sich in einem kleinen Cluster nur zwei oder drei Hosts befinden und Sie Anti-Affinitätsregeln definiert haben, die besagen, dass sich bestimmte VMs auf separaten Hosts befinden müssen, verhindern diese Regeln möglicherweise, dass DRS die VMs während des Upgrades verschiebt. Fügen Sie entweder weitere Hosts zum Cluster hinzu oder deaktivieren Sie die Anti-Affi-

nitätsregeln während des Upgrades und aktivieren Sie sie wieder, nachdem das Upgrade abgeschlossen ist. Navigieren Sie zum Deaktivieren einer Anti-Affinitätsregel zu **Hosts und Cluster (Hosts and Clusters) > *Cluster* > Einstellungen (Manage) > verwalten (Settings) > VM-/Host-Regeln (VM/Host Rules)**. Bearbeiten Sie die Regel und deaktivieren Sie die Option **Regel aktivieren (Enable rule)**.

Vorgehensweise

- Führen Sie für jeden zu aktualisierenden Host die folgenden Schritte durch.
  a. Versetzen Sie den Host in den Wartungsmodus.

     Wenn DRS für das Cluster aktiviert ist, versucht DRS, VMs auf andere Hosts zu verschieben. Wenn DRS aus irgendeinem Grund ausfällt, müssen Sie die VMs möglicherweise manuell verschieben und den Host anschließend in den Wartungsmodus versetzen.

  b. Führen Sie das ESXi-Upgrade auf dem Host durch.

     Starten Sie den Host nach Abschluss des ESXi-Upgrades neu.

  c. Wenn der Host nach dem Neustart den Status `Nicht verbunden` aufweist, stellen Sie eine Verbindung mit dem Host her. Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Verbindung (Connection) > Verbinden (Connect)** aus.

  d. Navigieren Sie zu **Networking & Security > Installation > Hostvorbereitung (Host Preparation)**.

  e. Wählen Sie den Host aus, auf dem Sie das ESXi-Upgrade durchgeführt haben. Für den Installationsstatus wird **Nicht bereit (Not Ready)** angezeigt.

  f. Klicken Sie auf **Aktionen (Actions) > Auflösen (Resolve)**, um die NSX-VIB-Aktualisierung abzuschließen.

     NSX-VIBs werden auf dem Host aktualisiert, und der Host wird neu gestartet.

  g. Wenn der Neustart für den Host abgeschlossen ist, beenden Sie den Wartungsmodus.

Sie können sicherstellen, dass die VIBs aktualisiert wurden, indem Sie eine Verbindung mit der Befehlszeile herstellen und den Befehl `esxcli software vib list` ausgeben. Im ersten Teil der VIB-Version wird die ESXi-Version für den VIB angezeigt.

Beispiel: Nach dem Upgrade auf ESXi 6.0 mit NSX 6.3.2 oder früher:

```
[root@host-1:~] esxcli software vib list
...
esx-vsip    6.0.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-01-23
esx-vxlan   6.0.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-01-23
...
```

Nach dem Upgrade auf ESXi 6.0 mit NSX 6.3.3 oder höher:

```
[root@host-2:~] esxcli software vib list
...
esx-nsxv    6.0.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-08-10
...
```

Upgrade auf ESXi 6.5 in einer NSX-Umgebung

NSX-VIBs sind spezifisch für die auf dem Host installierte ESXi-Version. Bei einem ESXi-Upgrade müssen Sie die neuen entsprechenden NSX-VIBs für die neue ESXi-Version installieren.

Wenn Sie ein Upgrade auf ESXi 6.5 durchführen, während NSX 6.3.x installiert ist, sind VM-vMotion-Verschiebungen auf VXLAN-vorbereitete vSphere Distributed Switches für den aktualisierten Host bis zur Installation der neuen NSX-VIBs blockiert.

VMware empfiehlt, mit vSphere Upgrade Manager ein Upgrade für die Hosts auf ESXi 6.5 in einer NSX 6.3.x-Umgebung durchzuführen.

Ganz gleich, welche Methode Sie für das ESXi-Upgrade anwenden, Sie sollten den folgenden Workflow befolgen. Gehen Sie auf einem Host jeweils wie folgt vor:

1 Upgrade von ESXi durchführen

   Nach Abschluss des ESXi-Upgrades beendet der Host den Wartungsmodus. Sie können die mit logischen Switches verbundenen VMs jedoch erst verschieben, wenn der nächste Schritt durchgeführt wurde.

2 Upgrade der NSX-VIBs

   Nachdem ein Upgrade der VIBs erfolgt ist und sich der Host nicht mehr im Wartungsmodus befindet, können Sie die mit logischen Switches verbundenen VMs auf den Host verschieben.

Wichtig Die Hostupgrades müssen jeweils einzeln erfolgen. Wählen Sie kein Cluster oder Datencenter für die Standardisierung aus, wenn Sie ein ESXi-Upgrade durchführen.

Die installierten NSX-VIBs hängen von der ESXi- und NSX-Version ab. Wenn NSX 6.3.3 oder höher installiert ist und Sie eine Upgrade von ESXi 5.5 auf 6.5 ausführen, werden die VIBs „esx-vsip“ und „esx-vxlan“ entfernt und durch „esx-nsxv“ ersetzt.

ESXi-Version	NSX-Version	Installierte VIBs
5.5	Alle 6.3.x	■ esx-vsip ■ esx-vxlan
6.0 oder höher	6.3.2 oder früher	■ esx-vsip ■ esx-vxlan
6.0 oder höher	6.3.3 oder höher	■ esx-nsxv

Voraussetzungen

- Stellen Sie sicher, dass NSX 6.3.x installiert ist.
- Prüfen Sie anhand der VMware-Produkt-Interoperabilitätsmatrix, welche Versionen von vSphere und ESXi mit Ihrer NSX-Installation kompatibel sind. Weitere Informationen dazu finden Sie unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

  Wichtig NSX 6.3.x ist nicht mit der ersten Version von ESXi 6.5 kompatibel. Sie müssen ein Upgrade auf ESXi 6.5.0a oder höher durchführen, um die Kompatibilität mit NSX 6.3.0 zu gewährleisten. Aktuelle Informationen zur Interoperabilität finden Sie in der Interoperabilitätsmatrix.

- Detaillierte Anweisungen zu einem Upgrade von vSphere, einschließlich *vSphere-Upgrade-Handbuch* und *Handbuch zum Installieren und Verwalten von VMware vSphere Update Manager*, finden Sie in der entsprechenden Version der vSphere-Dokumentation.
- Stellen Sie sicher, dass für die Platform Services Controller- und vCenter Server-Systeme ein Upgrade auf die neue vSphere-Version erfolgt ist.
- Stellen Sie sicher, dass vSphere Update Manager installiert und konfiguriert ist.
- Stellen Sie sicher, dass die vollqualifizierten Domänennamen (FQDNs) all Ihrer Hosts aufgelöst werden können.
- Wenn DRS deaktiviert ist, schalten Sie die VMs aus oder verschieben Sie sie mit vMotion manuell, bevor Sie das Upgrade starten.
- Wenn DRS aktiviert ist, werden die gestarteten VMs während des Hostcluster-Upgrades automatisch verschoben. Stellen Sie vor dem Starten des Upgrades sicher, dass DRS in Ihrer Umgebung funktioniert.
  - Stellen Sie sicher, dass DRS auf den Hostclustern aktiviert ist.
  - Stellen Sie sicher, dass vMotion ordnungsgemäß funktioniert.
  - Überprüfen Sie den Zustand der Hostverbindung mit vCenter.
  - Stellen Sie sicher, dass sich mindestens drei ESXi-Hosts in jedem Hostcluster befinden. Bei einem NSX-Upgrade ist die Wahrscheinlichkeit größer, dass bei einem Hostcluster mit nur einem oder zwei Hosts Probleme bei der DRS-Zugangssteuerung auftreten. Für ein erfolgreiches NSX-Upgrade empfiehlt VMware, dass jeder Hostcluster über mindestens drei Hosts verfügt. Wenn ein Cluster weniger als drei Hosts enthält, wird empfohlen, die Hosts manuell zu evakuieren.

- Wenn sich in einem kleinen Cluster nur zwei oder drei Hosts befinden und Sie Anti-Affinitätsregeln definiert haben, die besagen, dass sich bestimmte VMs auf separaten Hosts befinden müssen, verhindern diese Regeln möglicherweise, dass DRS die VMs während des Upgrades verschiebt. Fügen Sie entweder weitere Hosts zum Cluster hinzu oder deaktivieren Sie die Anti-Affinitätsregeln während des Upgrades und aktivieren Sie sie wieder, nachdem das Upgrade abgeschlossen ist. Navigieren Sie zum Deaktivieren einer Anti-Affinitätsregel zu **Hosts und Cluster (Hosts and Clusters) > *Cluster* > Einstellungen (Manage) > verwalten (Settings) > VM-/Host-Regeln (VM/Host Rules)**. Bearbeiten Sie die Regel und deaktivieren Sie die Option **Regel aktivieren (Enable rule)**.

Vorgehensweise

1. Navigieren Sie im vSphere Web Client zu **Update Manager > *Update Manager-Objekt* (*Update Manager Object*) > Verwalten (Manage)**.
2. Befolgen Sie die Anweisungen unter *Importieren von Host-Upgrade-Images und Erstellen von Host-Upgrade-Baselines*, um ein Upgrade-Image für den Host zu importieren und eine Host-Upgrade-Baseline zu erstellen.
   a. Klicken Sie auf die Registerkarte **ESXi-Images (ESXi Images)**, klicken Sie auf **ESXi-Image importieren (Import ESXi Image)** und navigieren Sie zu dem Image, das Sie hochladen möchten.
   b. Klicken Sie auf die Registerkarte **Host-Baselines (Host Baselines)** und auf **Neue Baseline (New Baseline)**. Erstellen Sie mithilfe des Assistenten für neue Baselines eine neue Baseline, und wählen Sie **Host-Upgrade (Host Upgrade)** für den Baseline-Typ aus.
3. Führen Sie die Hostupgrades einzeln durch. Wiederholen Sie diese Schritte für alle Hosts.
   a. Navigieren Sie zu **Hosts und Cluster (Hosts and Clusters)**, und wählen Sie einen Host für das Upgrade aus. Wählen Sie kein Cluster oder Datencenter aus.
   b. Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Update Manager > Baseline anhängen... (Attach Baseline...)** aus. Wählen Sie mithilfe des Assistenten zum Anhängen einer Baseline oder des Baseline-Gruppenassistenten eine Baseline aus. Vollständige Anweisungen finden Sie unter *Anhängen von Baselines und Baseline-Gruppen an Objekte* in der vSphere-Dokumentation.
   c. Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Update Manager > Standardisieren... (Remediate...)** aus. Wählen Sie mithilfe des Assistenten zum Standardisieren eine Baseline aus. Vollständige Anweisungen finden Sie unter *Standardisieren von Hosts für eine Upgrade-Baseline* in der vSphere-Dokumentation.
   d. Wenn der Host nach dem Neustart den Status `Nicht verbunden` aufweist, stellen Sie eine Verbindung mit dem Host her. Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Verbindung (Connection) > Verbinden (Connect)** aus.

e Wenn Sie sicherstellen möchten, dass das Upgrade abgeschlossen ist, klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Update Manager > Auf Updates prüfen... (Scan for Updates...)** aus. Aktivieren Sie das Kontrollkästchen **Upgrades**, um die Upgrade-Übereinstimmung zu prüfen. Wenn der Übereinstimmungsstatus „Konform“ lautet, ist das Upgrade abgeschlossen.

   Vollständige Anweisungen finden Sie unter *Manuelles Initiieren einer Prüfung der ESXi-Hosts* in der vSphere-Dokumentation.

f Navigieren Sie zu **Networking & Security > Installation > Hostvorbereitung (Host Preparation)**.

g Suchen Sie den Host, auf dem Sie das ESXi-Upgrade durchgeführt haben. Für den Installationsstatus wird **Nicht bereit (Not Ready)** angezeigt.

Klicken Sie auf **Nicht bereit (Not Ready)**, um weitere Informationen anzuzeigen.

h Wählen Sie den Host aus und klicken Sie auf **Aktionen (Actions) > Auflösen (Resolve)**, um die NSX-VIB-Installation zu starten.

Wenn Sie ein Upgrade von ESXi 5.5 durchführen und der Cluster DRS-fähig ist, versucht DRS, den Host auf kontrollierte Weise neu zu starten, damit die VMs weiterhin ausgeführt werden können. Wenn der DRS aus irgendeinem Grund fehlschlägt, wird die Aktion **Auflösen (Resolve)** gestoppt. In diesem Fall müssen Sie die virtuellen Maschinen gegebenenfalls manuell verschieben und dann versuchen, die Aktion **Auflösen (Resolve)** erneut auszuführen. Alternativ können Sie den Host manuell in den Wartungsmodus versetzen und neu starten.

Wenn Sie ein Upgrade von ESXi 6.0 durchführen und der Cluster DRS-fähig ist, versucht DRS, den Host auf kontrollierte Weise in den Wartungsmodus zu versetzen, damit die VMs weiterhin ausgeführt werden können. Wenn der DRS aus irgendeinem Grund fehlschlägt, wird die Aktion **Auflösen (Resolve)** gestoppt. In diesem Fall müssen Sie die virtuellen Maschinen gegebenenfalls manuell verschieben und dann versuchen, die Aktion **Auflösen (Resolve)** erneut auszuführen. Alternativ können Sie den Host manuell in den Wartungsmodus setzen.

Wichtig Wenn Sie ein Upgrade von ESXi 6.0 durchführen und einen Host manuell in den Wartungsmodus versetzen, um die Host-VIBs zu installieren, müssen Sie sicherstellen, dass die Installation der Host-VIBs abgeschlossen ist, bevor Sie den Wartungsmodus für den Host beenden. Unter **Hostvorbereitung (Host Preparation)** wird der Installationsstatus `Wird installiert` angezeigt, auch wenn die Installation bereits abgeschlossen ist.

1 Stellen Sie im Bereich „Aktuelle Aufgaben“ von vSphere Web Client sicher, dass alle Installationsaufgaben abgeschlossen sind.

2 Stellen Sie eine Verbindung mit der Host-Befehlszeile her und führen Sie den Befehl `esxcli software vib list` aus. Im ersten Teil der VIB-Version wird die ESXi-Version für den VIB angezeigt.

Beispiel: Nach dem Upgrade auf ESXi 6.5 mit NSX 6.3.2 oder früher:

```
[root@host-1:~] esxcli software vib list
...
esx-vsip    6.5.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-01-23
esx-vxlan   6.5.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-01-23
...
```

Nach dem Upgrade auf ESXi 6.5 mit NSX 6.3.3 oder höher:

```
[root@host-2:~] esxcli software vib list
...
esx-nsxv    6.5.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-08-10
...
```

Erneutes Bereitstellen von Guest Introspection nach dem ESXi-Upgrade

Wenn Sie für ESXi ein Upgrade auf einem Cluster durchführen, auf dem Guest Introspection bereitgestellt wird, müssen Sie auf der Registerkarte „Dienstbereitstellungen“ prüfen, ob Guest Introspection erneut bereitgestellt werden muss.

Wichtig Sie müssen das ESXi-Upgrade und das damit verbundene NSX-VIB-Upgrade abschließen, bevor Sie Guest Introspection erneut bereitstellen.

Voraussetzungen

- Schließen Sie das ESXi-Upgrade ab.
- Schließen Sie das (Hostvorbereitungs-)Upgrade für NSX-VIBs nach dem Upgrade von ESXi ab.

Vorgehensweise

1. Melden Sie sich beim vSphere Web Client an.
2. Klicken Sie auf **Networking & Security** und anschließend auf **Installation**.
3. Klicken Sie auf die Registerkarte **Dienstbereitstellungen (Service Deployments)**.
4. Wenn in der Spalte „Installationsstatus“ der Eintrag `Erfolg` angezeigt wird, ist eine erneute Bereitstellung nicht erforderlich.
5. Wenn in der Spalte „Installationsstatus“ der Eintrag „Nicht bereit“ angezeigt wird, klicken Sie auf den Link **Nicht bereit (Not Ready)**. Klicken Sie auf **Alle auflösen (Resolve all)**, um Guest Introspection erneut bereitzustellen.