Upgrade-Handbuch für NSX

Update 5
Geändert am 20. November 2017
VMware NSX for vSphere 6.2

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

Dieses Handbuch, das *Upgrade-Handbuch für NSX*, beschreibt, wie das VMware® NSX™-System mit dem vSphere Web Client aktualisiert werden kann. 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 installieren 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. In diesem Handbuch wird vorausgesetzt, dass Sie mit VMware vSphere 5.5 oder 6.0, einschließlich VMware ESXi, vCenter Server und vSphere Web Client, vertraut sind.

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://docs.vmware.com/en/VMware-NSX-for-vSphere/index.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 Instanz von Guest Introspection und Data Security pro ESXi™-Host und mehrere NSX Edge-Instanzen pro Datencenter installieren.

Hardware

Tabelle 1. Hardwareanforderungen

Appliance	Arbeitsspeicher	vCPU	Festplattenspeicher
NSX Manager	16 GB (24 GB mit bestimmten NSX-Bereitstellungsgrößen*)	4 (8 mit bestimmten NSX-Bereitstellungsgrößen*)	60 GB
NSX Controller	4 GB	4	20 GB
NSX Edge	■ Kompakt: 512 MB ■ Groß: 1 GB ■ Quad Large: 1 GB ■ Sehr groß: 8 GB	■ Kompakt: 1 ■ Groß: 2 ■ Quad Large: 4 ■ Sehr groß: 6	■ Kompakt: 1 Festplatte mit 500 MB ■ Groß: 1 Festplatte mit 500 MB + 1 Festplatte mit 512 MB ■ Quad Large: 1 Festplatte mit 500 MB + 1 Festplatte mit 512 MB ■ Sehr groß: 1 Festplatte mit 500 MB + 1 Festplatte mit 2 GB
Guest Introspection	1 GB	2	4 GB
NSX Data Security	512 MB	1	6 GB pro ESXi-Host

Als allgemeine Richtlinie gilt, dass Sie die Ressourcen von NSX Manager auf 8 vCPU und 24 GB RAM erhöhen sollten, wenn Ihre mit 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*.

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://docs.vmware.com/en/VMware-NSX-for-vSphere/index.html.

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
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	

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

Quelle	Ziel	Port	Protokoll	Zweck	Sensibel	TLS	Authentifizierung
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
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	

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

Quelle	Ziel	Port	Protokoll	Zweck	Sensibel	TLS	Authentifizierung
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	
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.

Upgrade von vCloud Networking and Security auf NSX

1

Dieses Kapitel behandelt die folgenden Themen:

- Vorbereiten des Upgrades von vCloud Networking and Security auf NSX
- Upgrade von vCloud Networking and Security 5.5.x auf NSX 6.2.x
- Upgrade von vCloud Networking and Security 5.5.x auf NSX in einer vCloud Director-Umgebung

Vorbereiten des Upgrades von vCloud Networking and Security auf NSX

Um ein erfolgreiches Upgrade auf NSX 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. Die folgenden Richtlinien können als eine Vor-Upgrade-Checkliste verwendet werden.

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 vCloud Networking and Security in der Version 5.5 vorliegt. Ist dies nicht der Fall, finden Sie im *vShield Installations- und Upgrade-Handbuch* entsprechende Upgrade-Anleitungen für die Version 5.5.
2. Stellen Sie sicher, dass alle erforderlichen Ports geöffnet sind. Siehe Für NSX erforderliche Ports und Protokolle.
3. Stellen Sie sicher, dass Sie den Uplink-Portnamen für vSphere Distributed Switches abrufen können. Siehe https://kb.vmware.com/kb/2129200.

4 Wenn vShield Endpoint-Partnerdienste bereitgestellt wurden, müssen Sie vor dem Upgrade die Kompatibilität überprüfen:

   - Unter den meisten Umständen kann vCloud Networking and Securityohne Einfluss auf Partnerlösungen auf NSX aktualisiert werden. Wenn Ihre Partnerlösung jedoch nicht mit der NSX-Version kompatibel ist, auf die Sie das Upgrade durchführen, müssen Sie vor dem Upgrade auf NSX ein Upgrade der Partnerlösung auf eine kompatible Version durchführen.
   - Informieren Sie sich im „VMware Kompatibilitätshandbuch für Networking & Security“. Siehe http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.
   - Informieren Sie sich über Kompatibilitäts- und Upgrade-Details in der Partnerdokumentation.

5 Wenn Sie über Data Security in Ihrer Umgebung verfügen, deinstallieren Sie es, bevor Sie ein Upgrade auf vShield Manager durchführen. Siehe Deinstallieren von vShield Data Security.

6 Wenn Sie Cisco Nexus 1000V als externen Switch-Anbieter verwenden, müssen Sie diese Netzwerke auf vSphere Distributed Switch migrieren, ehe Sie das Upgrade auf NSX durchführen. Nachdem NSX installiert ist, können Sie die vSphere Distributed Switches auf logische Switches migrieren.

7 Stellen Sie sicher, dass Sie über eine aktuelle Sicherung von vShield Manager, vCenter und anderen vCloud Networking and Security-Komponenten verfügen. Siehe Sichern und Wiederherstellen von vCloud Networking and Security.

8 Erstellen Sie ein Tech-Support-Paket.

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

10 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.

11 Laden Sie das Upgrade-Paket herunter, stellen Sie es bereit und überprüfen Sie es mit md5sum. Siehe Herunterladen des Pakets für das Upgrade von vShield Manager auf NSX und Überprüfen der MD5-Prüfsumme.

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

13 Schalten Sie keine vCloud Networking and Security-Komponenten oder -Appliances aus und löschen Sie diese nicht, bevor Sie dazu aufgefordert werden.

Überprüfen der Lizenzanforderungen vor dem Upgrade von vCloud Networking and Security auf NSX

Wenn Sie ein Upgrade von vCloud Networking and Security auf NSX durchführen, wird Ihre vorhandene Lizenz in eine NSX for vShield Endpoint-Lizenz umgewandelt.

Ab der Version NSX 6.2.3 wird als Standardlizenz diejenige für NSX für vShield Endpoint installiert. Mit dieser Lizenz können Benutzer mit NSX vShield Endpoint nur für die Antivirenfunktion bereitstellen und verwalten. Außerdem wird die Nutzung von VXLAN, Firewall und Edge-Diensten durch Blockierung der Hostvorbereitung und der Erstellung von Edges stark eingeschränkt.

Wenn Sie bereits vCloud Networking and Security-Funktionen inklusive vorbereitete Hosts, virtuelle Leitungen, vShield App oder vShield Edge bereitgestellt haben, sind diese weiterhin funktionsfähig. Sie können für diese aber kein Upgrade auf NSX und keine Änderungen durchführen.

Wenn Sie andere NSX-Funktionen benötigen, z. B. logische Switches, logische Router, Distributed Firewall oder NSX Edge, müssen Sie entweder eine NSX-Lizenz für die Verwendung dieser Funktionen erwerben oder eine Evaluierungslizenz für einen befristeten Test der Funktionen anfordern.

Weitere Informationen finden Sie in der NSX-Lizenz-FAQ unter https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf

Operative Auswirkungen von Upgrades für vCloud Networking and Security

Der vCloud Networking and Security-Upgrade-Vorgang kann einige Zeit in Anspruch nehmen, insbesondere dann, wenn Upgrades für ESXi-Hosts durchgeführt werden, da die Hosts neu gestartet werden müssen. Es ist wichtig, den Betriebszustand von vCloud Networking and Security-Komponenten bei einem Upgrade zu kennen, z. B. wenn einige, aber nicht alle Hosts aktualisiert wurden oder wenn NSX Edges noch nicht aktualisiert wurden.

Für das Upgrade von vCloud Networking and Security auf NSX 6.2.x müssen Sie die NSX-Komponenten in der folgenden Reihenfolge aktualisieren:

- vShield Manager
- Host-Cluster und virtuelle Leitungen
- vShield App
- vShield Edge
- vShield Endpoint

VMware empfiehlt, dass Sie das Upgrade in einem einzelnen Ausfallfenster durchführen, um die Ausfallzeit zu minimieren und Irritationen unter den vCloud Networking and Security-Benutzern zu vermeiden, die während des Upgrades nicht auf bestimmte vCloud Networking and Security-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 vCloud Networking and Security-Benutzer verstehen, welche Funktionen während des Upgrades zur Verfügung stehen.

vCenter-Upgrade

Wenn Sie das in vCenter eingebettete SSO verwenden und Sie ein Upgrade von vCenter 5.5 auf vCenter 6.0 durchführen, wird die Verbindung von vCenter zu vShield Manager möglicherweise getrennt. Dies geschieht, wenn vCenter 5.5 bei vShield unter Verwendung des Root-Benutzernamens registriert wurde. Ab der Version NSX 6.2 ist die vCenter-Registrierung mit Root veraltet. Als Problemumgehung registrieren Sie vCenter bei vShield mithilfe des Benutzernamens „administrator@vsphere.local“ anstelle von „root“ neu.

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

vShield Manager -Upgrade

Während des Vorgangs gilt Folgendes:

- Die vShield Manager-Konfiguration ist gesperrt. Der vShield-API-Dienst ist nicht verfügbar. An der vShield-Konfiguration können keine Änderungen vorgenommen werden. Die vorhandene VM-Kommunikation funktioniert weiter einwandfrei. Die neue VM-Bereitstellung funktioniert weiter in vSphere, aber die neuen virtuellen Maschinen können während des vShield Manager-Upgrades nicht mit virtuellen vShield-Leitungen verbunden werden.

Nach dem Vorgang gilt Folgendes:

- Alle vShield-Konfigurationsänderungen sind zulässig.

Host-Cluster-Upgrade und virtuelle Leitungen

In Verbindung mit dem Host-Cluster-Upgrade werden neue VIBs auf den Hosts installiert.

In NSX wurden virtuelle Leitungen in logische Switches umbenannt.

Während des Vorgangs gilt Folgendes:

- Konfigurationsänderungen werden auf NSX Manager nicht blockiert.
- Das Upgrade wird pro Cluster durchgeführt. Wenn DRS auf dem Cluster aktiviert ist, verwaltet DRS die Upgrade-Reihenfolge der Hosts.

Wenn einige NSX-Hosts eines Clusters aktualisiert werden und andere nicht:

- Konfigurationsänderungen am NSX Manager werden nicht blockiert. Es können Elemente zu logischen Netzwerken hinzugefügt werden und Änderungen daran vorgenommen werden. Die Bereitstellung neuer virtueller Maschinen funktioniert weiter auf Hosts, die zurzeit nicht aktualisiert werden. Hosts, die zurzeit aktualisiert werden, werden in den Wartungsmodus versetzt. Dies bedeutet, dass virtuelle Maschinen ausgeschaltet oder auf andere Hosts evakuiert werden müssen. Dies kann mit DRS oder manuell durchgeführt werden.

Migration von vShield App auf NSX Distributed Firewall

In Verbindung mit dem Host-Cluster-Upgrade wird die vShield App-Konfiguration auf die Distributed Firewall migriert.

Während des Vorgangs gilt Folgendes:

- Während der Durchführung der Migration werden vorhandene Filter weiter angewandt.
- Fügen Sie während der Durchführung der Migration keine Filter hinzu und ändern Sie diese nicht.

Nach dem Vorgang gilt Folgendes:

- Überprüfen Sie alle migrierten Bereiche, um sicherzustellen, dass sie wie vorgesehen funktionieren.
- Nach der Migration entfernen Sie vShield App über die Seite „Dienstbereitstellung“ in NSX.

Upgrade von vShield Edge

vShield Edges können unabhängig von Host-Upgrades aktualisiert werden. Sie können eine vShield Edge selbst dann aktualisieren, wenn Sie die Hosts noch nicht aktualisiert haben.

Vorsicht Wenn Sie eine vCloud Director-Version vor 8.10 verwenden, ist kein Upgrade von NSX Edge möglich. Siehe Prüfen eines Upgrades von vShield Edge in einer vCloud Director-Umgebung.

Während des Vorgangs gilt Folgendes:

- Auf dem aktuell aktualisierten vShield Edge-Gerät werden Konfigurationsänderungen blockiert.
- Die Paketweiterleitung ist vorübergehend unterbrochen.
- Es können Elemente zu logischen Switches hinzugefügt werden und Änderungen daran vorgenommen werden.
- Die Bereitstellung neuer virtueller Maschinen funktioniert weiterhin einwandfrei.

Nach dem Vorgang gilt Folgendes:

- Konfigurationsänderungen werden nicht blockiert. Durch das Upgrade auf NSX eingeführte neue Funktionen sind erst dann konfigurierbar, wenn alle NSX Controller installiert und alle Host-Cluster auf NSX Version 6.2.x aktualisiert wurden.
- L2 VPN muss nach dem Upgrade neu konfiguriert werden.
- SSL-VPN-Clients müssen nach dem Upgrade neu installiert werden.

Migration von vShield Endpoint auf Guest Introspection

In NSX 6.x wurde vShield Endpoint in Guest Introspection umbenannt. Nach dem Upgrade von NSX Manager zeigt der Guest Introspection-Dienst einen **Upgrade**-Link an, wenn Sie zu **Networking & Security > Installation > Dienstbereitstellungen** wechseln. Wenn Sie ein Upgrade von vCloud Networking and Security auf NSX durchführen, werden die virtuelle Appliance Guest Introspection und der Hostagent für Guest Introspection auf jedem Host im Cluster bereitgestellt, auf dem Guest Introspection aktiviert ist.

Während des Vorgangs gilt Folgendes:

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

Nach dem Vorgang gilt Folgendes:

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

Überprüfen des Arbeitszustands von vCloud Networking and Security

Bevor Sie mit dem Upgrade beginnen, ist es wichtig, den Arbeitszustand von vCloud Networking and Security zu 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 vCloud Networking and Security-Infrastruktur nicht davon aus, dass alles problemlos funktioniert. Nehmen Sie zuvor einige Überprüfungen vor.

Die nachfolgend aufgeführte Vorgehensweise lässt sich als Checkliste vor dem Upgrade verwenden.

Vorgehensweise

1. Ermitteln Sie die administrativen Benutzer-IDs und Kennwörter.
2. Stellen Sie sicher, dass die Namensauflösung vorwärts und rückwärts für alle Komponenten funktioniert.
3. Stellen Sie sicher, dass Sie sich bei allen vSphere- und vShield-Komponenten anmelden können.
4. Merken Sie sich die aktuellen Versionen von vShield Manager, vCenter Server, ESXi und vShield Edges.
5. 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 derselben virtuellen Leitung, 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.
6. Validieren Sie die Nord-Süd-Verbindung, indem Sie von einer virtuellen Maschine aus pingen.

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

8 Inspizieren Sie die vShield -Umgebung visuell, um sicherzustellen, dass alle Statusanzeigen grün, normal oder bereitgestellt lauten.

9 Stellen Sie sicher, dass syslog konfiguriert ist.

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

11 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 vShield Manager den Befehl `show tech-support save session` aus und suchen Sie nach „5671“, um sicherzustellen, dass alle Hosts mit vShield Manager verbunden sind.

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

Migrieren des lokalen Admin-Benutzers in den CLI-Admin-Benutzer

Vor der NSX 6.x-Serie war der Benutzeradministrator ein lokaler Datenbankbenutzer. Ab NSX 6.0 ist der Benutzeradministrator ein CLI-Benutzer. Zum Zwecke der Abwärtskompatibilität gibt es Schritte zum Migrieren des Admin-Benutzers.

In der vCloud Networking and Security 5.x-Serie waren der Admin-Benutzer der Befehlszeilenschnittstelle (CLI) und der Admin-Benutzer der Benutzerschnittstelle (VSM) zwei unterschiedliche Benutzer. Das Admin-Kennwort des CLI-Benutzers wurde vom Betriebssystem verwaltet und das Kennwort des VSM-Benutzers wurde von der lokalen Datenbank der Benutzer verwaltet. Wenn Sie das Kennwort des CLI-Admin-Benutzers änderten, wirkte sich dies nicht auf das Kennwort des VSM-Admin-Benutzers aus. Wenn Sie wiederum das Kennwort des VSM-Admin-Benutzers änderten, wirkte sich dies nicht auf das Kennwort des CLI-Admin-Benutzers aus.

Für die NSX 6.x-Serie ist die VSM-Benutzerdatenbank veraltet. Der CLI-Benutzer kann sich direkt beim NSX Manager anmelden.

In einem Upgrade-Szenario ist der Admin-Benutzer zum Zwecke der Abwärtskompatibilität sowohl in der CLI- als auch in der Web UI-Datenbank vorhanden. Wenn in diesem Fall das Kennwort des CLI-Benutzers geändert wird, wirkt sich diese Änderung nicht in der Benutzeroberfläche oder in den REST API-Aufrufen aus. Vor der NSX 6.x-Serie konnte sich der CLI-Benutzer nicht bei der Benutzeroberfläche oder der REST API anmelden.

Bei neuen Bereitstellungen der NSX 6.x-Serie (grünes Feld) sind der CLI-Benutzer und NSX Manager (UI oder REST) sowie die Anmeldedaten identisch.

Wenn Sie möchten, dass sich Ihre aktualisierte NSX-Bereitstellung wie eine neue Bereitstellung von NSX 6.x verhält, haben Sie zwei Optionen.

- Option 1 – Ändern Sie das Kennwort des Admin-Datenbankbenutzers.

Sie können die folgende REST API verwenden, um das Kennwort zu ändern. Bei Nutzung dieser Option müssen Sie das alte Kennwort kennen.

PUT URI /api/2.0/services/usermgmt/user/local/<userId>

```
<userInfo>
      <userId></userId>
      <password></password>
      <fullname></fullname>
      <email></email>
      <accessControlEntry>
         <role></role>
         <resource>
             <resourceId></resourceId>
             ...
         </resource>
      </accessControlEntry>
</userInfo>
```

Beispielsweise unter Verwendung von curl:

```
curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X PUT
https://<vsm-ip>/api/2.0/services/usermgmt/user/local/admin -d '<userInfo><userId>admin</use-
rId><password>123</password><fullname>admin</fullname><email>admin@company.com</email><accessCont-
rolEntry><role>security_admin</role><resource><resourceId>datacenter-312</resourceId></resour-
ce></accessControlEntry></userInfo>'
```

Mit der API können Sie ein lokales Benutzerkonto einschließlich des Kennworts aktualisieren. Wenn kein Kennwort angegeben wird, wird das vorhandene Kennwort beibehalten. Die userId-Variable in der URI muss der in XML angegebenen Variablen entsprechen.

- Option 2 – Anstatt den Web UI-Admin-Benutzer beizubehalten, können Sie ihn entfernen und dem CLI-Admin-Benutzer eine Rolle zuweisen. Nach dieser Änderung können Sie sich beim NSX Manager mit den Anmeldedaten des CLI-Benutzers anmelden. Eine Änderung des Kennworts des CLI-Admin-Benutzers spiegelt sich im NSX Manager-Admin-Benutzer wider.

  Da der Web UI-Admin-Benutzer der „super_user“ ist, müssen Sie einen anderen Benutzer mit super_user-Rechten hinzufügen, bevor Sie den Web UI-Admin-Benutzer löschen können.

  - Fügen Sie einen neuen Benutzer-Tempadmin mit der Rolle „super_user“ hinzu.

    Beispielsweise unter Verwendung von curl:

    ```
    curl -k -H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' -H 'Content-Type: application/xml' -X
    PUT https://<vsm-ip>/api/2.0/services/usermgmt/user/local/admin -d '<userInfo><userId>tempad-
    min</userId><password>123</password><fullname>tempadmin</fullname><email>tempadmin@compa-
    ny.com</email><accessControlEntry><role>super_user</role><resource><resourceId>datacen-
    ter-312</resourceId></resource></accessControlEntry></userInfo>'
    ```

- Lassen Sie den Tempadmin den Web UI-Benutzeradministrator löschen.

  Beispielsweise unter Verwendung von curl:

  ```
  curl –k –H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' –H 'Content–Type: application/xml' –X
  DELETE https://<vsm–ip>/api/2.0/services/usermgmt/user/admin
  ```

- Fügen Sie dem CLI-Benutzer-Admin die Rolle „super_user“ hinzu.

  Beispielsweise unter Verwendung von curl:

  ```
  curl –k –H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' –H 'Content–Type: application/xml' –X
  POST https://<nsx–ip>/api/2.0/services/usermgmt/role/admin?isCli=true –d '<accessControlEnt–
  ry><role>super_user</role></accessControlEntry>'
  ```

Deinstallieren von vShield Data Security

Wenn Data Security in Ihrer Umgebung vorhanden ist, deinstallieren Sie diese Komponente, bevor Sie ein Upgrade auf NSX durchführen.

Ab der Version NSX 6.2.3 wird die NSX Data Security-Funktion eingestellt. In NSX 6.2.3 können Sie diese Funktion noch auf eigene Verantwortung weiter benutzen. In künftigen NSX-Versionen ist diese Funktion jedoch nicht mehr enthalten.

Vorgehensweise

1. Erweitern Sie im Bestandslistenbereich von vShield Manager 5.5 den Ordner **Datacenters** und navigieren Sie zu einem Host, auf dem vShield Data Security installiert ist.
2. Führen Sie die nachfolgend aufgeführten Schritte auf jedem Host aus, auf dem vShield Data Security installiert ist, um diese Komponente zu deinstallieren.
   a. Klicken Sie auf den Host und klicken Sie auf der Registerkarte **Übersicht (Summary)** im vShield-Fensterbereich „Hostvorbereitung“ auf den Link **Deinstallieren (Uninstall)** für vShield Data Security.
   b. Stellen Sie im Fensterbereich „Dienste für die Deinstallation auswählen“ sicher, dass vShield Data Security ausgewählt ist, und klicken Sie auf die Schaltfläche **Deinstallieren (Uninstall)**.

      vShield Data Security wird deinstalliert und im vShield-Fensterbereich „Hostvorbereitung“ wird der Status `Nicht installiert` angezeigt.

Sichern und Wiederherstellen von vCloud Networking and Security

Die ordnungsgemäße Sicherung aller Komponenten von vCloud Networking and Security ist die Voraussetzung dafür, das System bei einem Ausfall in einem funktionsfähigen Zustand wiederherstellen zu können.

Die vShield Manager-Sicherung enthält die gesamte vShield-Konfiguration, inklusive virtuelle Leitungen und Routing-Entitäten, Sicherheit, vApp-Regeln und alle anderen Konfigurationen mit der vShield Manager-Benutzeroberfläche oder -API. Die vCenter-Datenbank sowie zugehörige Elemente wie die virtuellen Switches müssen gesondert gesichert werden.

Es wird empfohlen, zumindest von vShield Manager und vCenter regelmäßig Sicherungskopien zu erstellen. Je nach geschäftlichen Anforderungen und operativen Verfahren können die Sicherungshäufigkeit und der Zeitplan variieren. Es wird empfohlen, im Fall häufiger Konfigurationsänderungen vCloud Networking and Security auch häufiger zu sichern.

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

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

- Vor einem Upgrade von vCloud Networking and Security oder vCenter.
- Nach einem Upgrade von vCloud Networking and Security oder vCenter.
- Nach der Bereitstellung von Day Zero und der Erstkonfiguration der Komponenten von vCloud Networking and Security, z. B. nach dem Erstellen von virtuellen Switches, Edges, Sicherheit und 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 der Komponenten von vCloud Networking and Security mit Ihrem Sicherungszeitplan für andere interaktive Komponenten, z. B. vCenter, Cloud-Managementsysteme, operative Tools usw., zu synchronisieren.

Sichern von vShield Manager-Daten nach Bedarf

Sie können vShield Manager-Daten jederzeit sichern, indem Sie eine bedarfsorientierte Sicherung durchführen.

Vorgehensweise

1. Klicken Sie im vShield Manager-Bestandslistenbereich auf **Einstellungen und Berichte (Settings & Reports)**.
2. Klicken Sie auf die Registerkarte **Konfiguration (Configuration)**.
3. Klicken Sie auf **Sicherungen (Backups)**.

4 (Optional) Aktivieren Sie das Kontrollkästchen **Systemereignisse ausschließen (Exclude System Events)**, wenn Sie die Systemereignistabellen nicht sichern möchten.

5 (Optional) Aktivieren Sie das Kontrollkästchen **Überwachungsprotokolle ausschließen (Exclude Audit Logs)**, wenn Sie die Überwachungsprotokolltabellen nicht sichern möchten.

6 Geben Sie in das Feld **Host-IP-Adresse (Host IP Address)** die Host-IP-Adresse des Systems ein, auf dem die Sicherung gespeichert wird.

7 Geben Sie in das Feld **Hostname (Host Name)** den Hostnamen des Sicherungssystems ein.

8 Geben Sie in das Feld **Benutzername (User Name)** den zur Anmeldung beim Sicherungssystem erforderlichen Benutzernamen ein.

9 Geben Sie in das Feld **Kennwort (Password)** das dem Benutzernamen für das Sicherungssystem zugeordnete Kennwort ein.

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

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

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

12 Geben Sie zum Sichern der Sicherungsdatei einen **Kennwortsatz (Pass Phrase)** ein.

    In vCloud Networking and Security war der Kennwortsatz optional. In NSX ist er erforderlich.

13 Wählen Sie im Dropdown-Menü **Übertragungsprotokoll (Transfer Protocol)** entweder das Protokoll **SFTP** oder das Protokoll **FTP** aus.

14 Klicken Sie auf **Sicherung (Backup)**.

    Nach Abschluss der Sicherung wird diese in einer Tabelle unterhalb dieses Formulars angezeigt.

15 Klicken Sie auf **Einstellungen speichern (Save Settings)**, um die Konfiguration zu speichern.

Achtung: Wenn Sie alle Sicherungen in ein- und demselben Verzeichnis abspeichern, kann es bei der Anzeige der Sicherungen zu Problemen kommen. Es wird empfohlen, die Sicherungsdateien gelegentlich in einen Archivordner zu verschieben.

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.

Diese Funktionen sind nur für vSphere Web Client 5.1 oder höher verfügbar. VDS-Einstellungen und Portgruppeneinstellungen werden im Rahmen des Importvorgangs importiert.

Best Practice ist, die VDS-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 Pakets für das Upgrade von vShield Manager auf NSX und Überprüfen der MD5-Prüfsumme

Das Paket für das Upgrade von vShield Manager auf NSX enthält alle Dateien, die für das Upgrade der NSX-Infrastruktur erforderlich sind. Bevor Sie ein Upgrade von vShield 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 Paket für das Upgrade von vShield Manager auf NSX an einen Speicherort herunter, auf den vShield Manager zugreifen kann. Der Name der Upgrade-Paket-Datei entspricht in etwa dem Format `VMware-vShield-Manager-upgrade-bundle-to-NSX-releaseNumber-NSXbuildNumber.tar.gz`.
2. Stellen Sie sicher, dass der Dateiname für das Upgrade mit tar.gz endet.

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

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

Ändern Sie ihn in:

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

Andernfalls wird nach dem Hochladen des Upgrade-Pakets folgende Fehlermeldung angezeigt: „Ungültige Upgrade-Paket-Datei VMware-vShield-Manager-upgrade-bundle-to-NSX-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.

Zusätzliche Vorbereitungsschritte zum Upgrade für vCloud Director-Umgebungen

vCloud Director Network Isolation (VCDNI) wird mit NSX unterstützt, ist aber eine veraltete Technologie.

Ehe VXLAN auf breiter Ebene eingeführt wurde, war vCloud Director auf die vCloud-Netzwerk-Isolationstechnologie angewiesen, um ein logisches Netzwerk-Overlay anbieten zu können. Diese proprietäre MAC-in-MAC-Kapselungstechnologie wird zwar nach wie vor unterstützt, die Unterstützung dieser Technologie ist aber nun veraltet. Anders als die logischen VXLAN-Netzwerke, werden die logischen VCDNI-Netzwerke direkt von vCloud Director erstellt, das mit den ESXi Hosts über den vCloud Agent kommuniziert, der im VMkernel ausgeführt wird. Aus diesem Grund hat ein Upgrade von vCloud Networking and Security keine Auswirkungen auf VCDNI-Netzwerke und es gibt keine Beschränkung für deren gemeinsame Verwendung mit NSX.

Dennoch sollten Sie die VXLAN-Technologie verwenden, da VCDNI eine veraltete Technologie ist, die nur für bereits vorhandene Installationen unterstützt wird.

Upgrade von vCloud Networking and Security 5.5.x auf NSX 6.2.x

Um ein Upgrade auf NSX 6.2.x durchzuführen, müssen Sie die vCloud Networking and Security-Komponenten in der Reihenfolge aktualisieren wie in diesem Handbuch dokumentiert.

Für die vCloud Networking and Security-Komponenten muss in der folgenden Reihenfolge ein Upgrade auf NSX durchgeführt werden:

1 Upgrade von vShield Manager auf NSX Manager

2 Bereitstellen von NSX Controller-Clustern (optional); dies ist für logische (verteilte) Router und die Änderung des Steuerungskomponenten-Modus auf „Hybrid“ oder „Unicast“ erforderlich

3 Aktualisieren von Host-Clustern

4 Aktualisieren der Transportzone (optional); wenn der NSX Controller-Cluster bereitgestellt wurde, können Sie den Steuerungskomponenten-Modus von „Hybrid“ auf „Unicast“ ändern

5 Upgrade von vShield App auf die verteilte Firewall von NSX

6 Upgrade von vShield Edge auf NSX Edge

7 Upgrade von vShield Endpoint auf NSX Guest Introspection

Der Upgrade-Vorgang wird von vShield 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.

Wichtig Wenn in Ihrer Umgebung virtuelle Leitungen vorliegen, müssen Sie nach dem Upgrade auf NSX Manager Ihre Host-Cluster aktualisieren.

Upgrade von vShield Manager auf NSX Manager

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

Vorsicht Deinstallieren Sie keine bereitgestellte Instanz der vShield Manager-Appliance.

Voraussetzungen

- Vergewissern Sie sich, dass alle in Vorbereiten des Upgrades von vCloud Networking and Security auf NSX beschriebenen Aufgaben zur Upgrade-Vorbereitung abgeschlossen sind, inklusive der Überprüfung der Systemanforderungen und der Durchführung von Sicherungen.
- Stellen Sie sicher, dass vShield Manager über genügend Festplattenspeicher für das Upgrade auf NSX Manager verfügt. Siehe Systemvoraussetzungen für NSX.
- Erhöhen Sie den reservierten Arbeitsspeicher der virtuellen vShield Manager-Appliance auf mindestens 16 GB und teilen Sie 4 vCPUs zu, ehe Sie das Upgrade auf NSX 6.2.x durchführen.

  Siehe Systemvoraussetzungen für NSX.
- Stellen Sie sicher, dass vShield Edge-Instanzen, die älter als Version 5.5 sind, auf Version vShield 5.5 aktualisiert wurden.

  vShield Edge-Instanzen, die älter als 5.5 sind, können nicht mehr verwaltet oder gelöscht werden, nachdem für vShield Manager ein Upgrade auf NSX Manager durchgeführt wurde.

Vorgehensweise

1 Laden Sie das NSX-Upgrade-Paket an einen Speicherort herunter, auf den vShield Manager zugreifen kann. Der Name der Upgrade-Paket-Datei lautet in etwa `VMware-vShield-Manager-upgrade-bundle-to-NSX-`*`release-buildNumber`*`.tar.gz`.

2 Klicken Sie im Bestandslistenbereich von vShield Manager 5.5 auf **Einstellungen und Berichte**.

3 Klicken Sie auf die Registerkarte **Updates** und dann auf **Upgrade-Paket hochladen**.

4 Klicken Sie auf **Datei auswählen**, wählen Sie die Datei `VMware-vShield-Manager-upgrade-bundle-to-NSX-`*`release-buildNumber`*`.tar.gz` aus und klicken Sie auf **Öffnen**.

5 Klicken Sie auf **Datei hochladen**.

Das Hochladen der Dateien dauert einige Minuten.

6 Klicken Sie auf **Installieren**, um mit dem Upgrade zu beginnen.

7 Klicken Sie auf **Installation bestätigen**. Der Upgrade-Vorgang startet vShield Manager neu, d. h., die Verbindung zur vShield Manager-Benutzeroberfläche geht möglicherweise verloren. Keine der anderen vShield-Komponenten wird neu gestartet.

8 Nach dem Neustart melden Sie sich bei der virtuellen NSX Manager-Appliance durch Öffnen eines Webbrowser-Fensters und Eingabe der IP-Adresse (z. B https://10.10.10.10) an. Der NSX Manager verfügt nach dem Upgrade über die gleiche IP-Adresse wie der vShield Manager.

Die Registerkarte „Übersicht“ zeigt die Version von NSX-Manager an, die Sie gerade installiert haben.

9 Wechseln Sie zu **Home > vCenter-Registrierung verwalten** und stellen Sie sicher, dass für den vCenter Server-Status `Verbunden` gilt.

10 Schließen Sie alle vorhandenen Browser-Sitzungen, die auf vSphere Web Client zugreifen. Warten Sie einige Minuten und löschen Sie den Browser-Cache, bevor Sie sich am vSphere Web Client anmelden.

11 Wenn SSH auf vShield Manager aktiviert war, müssen Sie es nach der Durchführung des Upgrades auf NSX-Manager aktivieren. Melden Sie sich an der virtuellen NSX-Manager-Appliance an und klicken Sie auf **Übersicht anzeigen**. Klicken Sie in den Komponenten auf Systemebene für den SSH-Dienst auf **Start**.

Wichtig Nach dem Upgrade von vCloud Networking and Security 5.x auf NSX 6.x müssen Sie sich mit Ihren CLI-Administratoranmeldedaten beim NSX Manager anmelden. Bisher waren für vCloud Networking and Security zwei Kennwörter erforderlich, eines für die Befehlszeilenschnittstelle (CLI) und ein anderes für die Benutzeroberfläche. Ab der Version NSX 6.x wird nur mehr ein Kennwort benötigt. Beispiel:

Kennwörter in vCloud Networking and Security

- mypassword#123 für die Befehlszeilenschnittstelle (CLI)
- mypassword#456 für die Benutzeroberfläche

Kennwörter nach dem Upgrade auf NSX

- mypassword#123 für die Befehlszeilenschnittstelle (CLI)
- mypassword#123 für die Benutzeroberfläche

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. Siehe Sichern und Wiederherstellen von NSX. Die vorherige NSX Manager-Sicherung gilt nur für die vorherige Version.

Weiter

Installieren und Zuweisen einer NSX-Lizenz.

Installieren und Zuweisen einer NSX-Lizenz

Sie können, nachdem das Upgrade des NSX Manager abgeschlossen ist, eine Lizenz von NSX for vSphere installieren und zuweisen, indem Sie vSphere Web Client verwenden.

Ab der Version NSX 6.2.3 wird als Standardlizenz diejenige für NSX für vShield Endpoint installiert. Mit dieser Lizenz können Benutzer mit NSX vShield Endpoint nur für die Antivirenfunktion bereitstellen und verwalten. Außerdem wird die Nutzung von VXLAN, Firewall und Edge-Diensten durch Blockierung der Hostvorbereitung und der Erstellung von Edges stark eingeschränkt.

Wenn Sie andere NSX-Funktionen benötigen, z. B. logische Switches, logische Router, Distributed Firewall oder NSX Edge, müssen Sie entweder eine NSX-Lizenz für die Verwendung dieser Funktionen erwerben oder eine Evaluierungslizenz für einen befristeten Test der Funktionen anfordern.

Weitere Informationen finden Sie in der NSX-Lizenz-FAQ unter https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf

Weitere Informationen zur NSX-Lizenzierung finden Sie unter http://www.vmware.com/files/pdf/vmware-product-guide.pdf.

Vorgehensweise

- In vSphere 5.5 führen Sie die im Folgenden aufgeführten Schritte zum Hinzufügen einer Lizenz für NSX durch.
  a. Melden Sie sich beim vSphere Web Client an.
  b. Klicken Sie auf **Verwaltung (Administration)** und dann auf **Lizenzen (Licenses)**.
  c. Klicken Sie auf die Registerkarte **Lösungen (Solutions)**.
  d. Wählen Sie in der Liste „Lösungen“ die Option „NSX for vSphere“ aus. Klicken Sie auf **Lizenzschlüssel zuweisen (Assign a license key)**.
  e. Wählen Sie im Dropdown-Menü **Neuen Lizenzschlüssel zuweisen (Assign a new license key)** aus.
  f. Geben Sie den Lizenzschlüssel und eine optionale Bezeichnung für den neuen Schlüssel ein.
  g. Klicken Sie auf **Entschlüsseln (Decode)**.

     Entschlüsseln Sie den Lizenzschlüssel, um sicherzustellen, dass er das richtige Format aufweist und über genügend Kapazität verfügt, um die Assets zu lizenzieren.
  h. Klicken Sie auf **OK**.
- In vSphere 6.0 führen Sie die im Folgenden aufgeführten Schritte zum Hinzufügen einer Lizenz für NSX durch.
  a. Melden Sie sich beim vSphere Web Client an.
  b. Klicken Sie auf **Verwaltung (Administration)** und dann auf **Lizenzen (Licenses)**.
  c. Klicken Sie auf die Registerkarte **Assets** und dann auf die Registerkarte **Lösungen (Solutions)**.
  d. Wählen Sie in der Liste „Lösungen“ die Option „NSX for vSphere“ aus. Im Dropdown-Menü **Alle Aktionen (All Actions)** wählen Sie **Lizenz zuweisen... (Assign license...)** aus.
  e. Klicken Sie auf das Symbol **Hinzufügen (Add)** (). Geben Sie einen Lizenzschlüssel ein und klicken Sie auf **Weiter (Next)**. Fügen Sie einen Namen für die Lizenz hinzu und klicken Sie auf **Weiter (Next)**. Klicken Sie zum Hinzufügen der Lizenz auf **Beenden (Finish)**.
  f. Wählen Sie die neue Lizenz aus.
  g. (Optional) Klicken Sie auf das Symbol **Funktionen anzeigen (View Features)**, um darzustellen, welche Funktionen mit dieser Lizenz aktiviert sind. In der Spalte **Kapazität (Capacity)** wird der Leistungsumfang der Lizenz angegeben.
  h. Klicken Sie auf **OK**, um NSX die neue Lizenz zuzuweisen.

Weiter

Bereitstellen des NSX Controller-Clusters.

Wenn Sie keine Controller bereitstellen, finden Sie Erläuterungen unter Aktualisieren von Host-Clustern.

Bereitstellen des NSX Controller-Clusters

NSX Controller ist ein erweitertes, verteiltes Zustandsverwaltungssystem, das Steuerungskomponenten-funktionen für logische Switching- und Routing-Funktionen für NSX bereitstellt. Das System fungiert als zentraler Kontrollpunkt für alle logischen Switches innerhalb eines Netzwerks und pflegt Informationen zu allen Hosts, logischen Switches (VXLANs) und Distributed Logical Routern. Controller sind erforderlich, wenn Sie Distributed Logical Router oder VXLAN im Unicast-oder Hybrid-Modus bereitstellen möchten.

Unabhängig von der Größe der NSX-Bereitstellung ist es für VMware erforderlich, dass jeder NSX Controller-Cluster drei Controller-Knoten enthält. Eine andere Anzahl an Controller-Knoten wird nicht unterstützt.

Für den Cluster ist es erforderlich, dass das Datenspeichersystem jedes Controllers über eine Spitzenschreiblatenz von weniger als 300 ms und eine durchschnittliche Schreiblatenz von weniger als 100 ms verfügt. Erfüllt das Speichersystem diesen Anforderungen nicht, kann der Cluster instabil werden und zu einem Systemausfall führen.

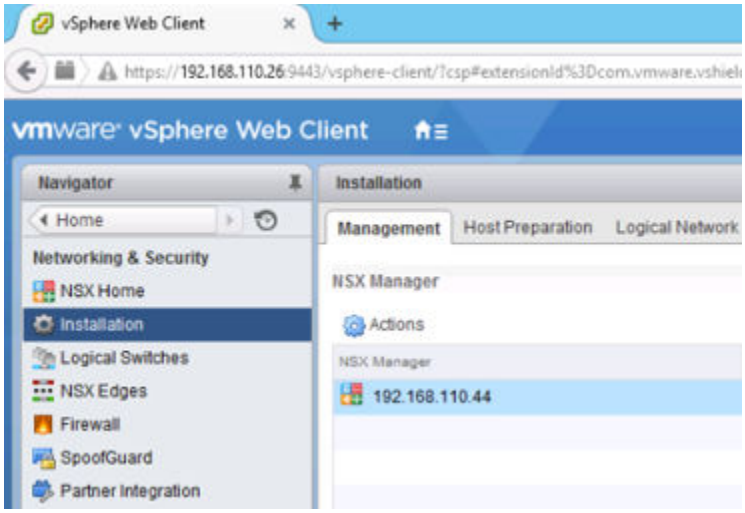
Voraussetzungen

- Bevor Sie NSX Controller bereitstellen, müssen Sie eine NSX Manager-Appliance bereitstellen und vCenter bei NSX Manager registrieren.
- Legen Sie die IP-Pool-Einstellungen für Ihren Controller-Cluster, einschließlich des Gateways und des IP-Adressbereichs, fest. DNS-Einstellungen sind optional. Das IP-Netzwerk des NSX Controllers muss mit dem NSX Manager und den Verwaltungsschnittstellen auf den ESXi-Hosts verbunden sein.

Vorgehensweise

1 Gehen Sie in vCenter zu **Home> Networking & Security > Installation** und wählen Sie die Registerkarte **Management** aus.

Beispiel:

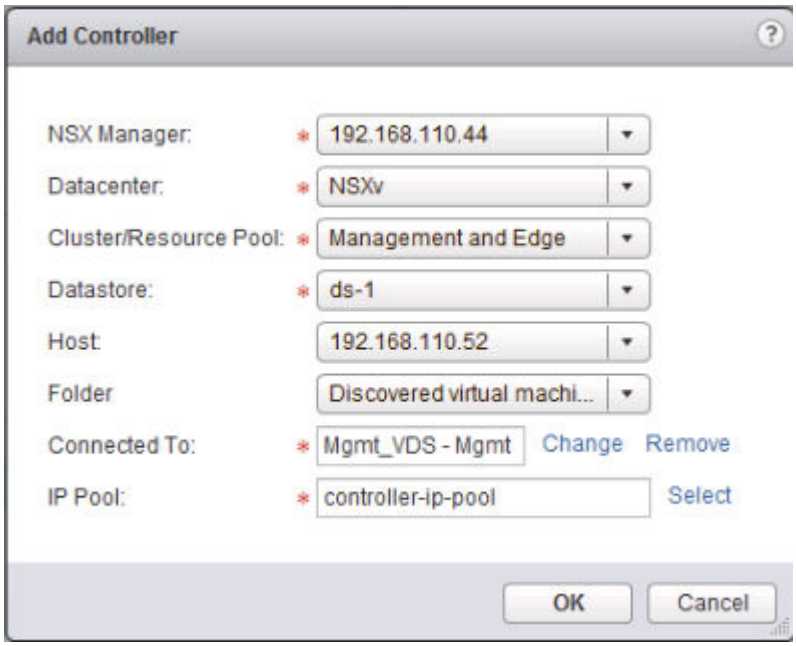


2 Klicken Sie im Bereich der NSX Controller-Knoten auf das Symbol **Knoten hinzufügen** ( ).

3 Geben Sie die für Ihre Umgebung geeigneten NSX Controller-Einstellungen ein.

NSX Controller müssen für eine vSphere Standard Switch- oder vSphere Distributed Switch-Portgruppe bereitgestellt werden, die nicht auf VXLAN basiert und die über eine Konnektivität zum NSX Manager, zu anderen Controllern und zu Hosts über IPv4 verfügt.

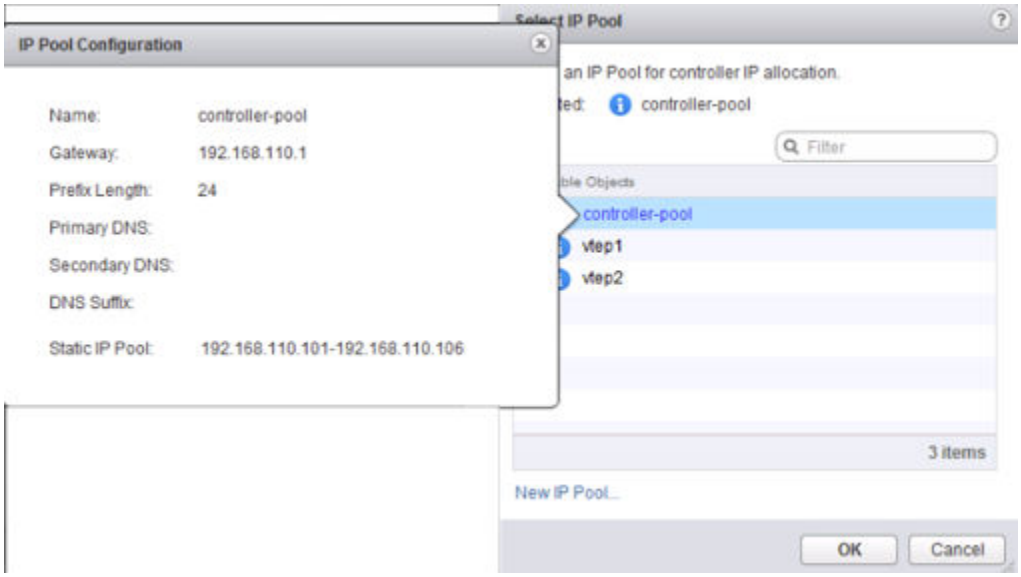
Beispiel:



4 Wenn Sie noch keinen IP-Pool für Ihren Controller-Cluster konfiguriert haben, tun Sie dies jetzt, indem Sie auf **Neuer IP-Pool** klicken.

Falls erforderlich, können einzelne Controller sich in separaten IP-Subnetzen befinden.

Beispiel:



5 Geben Sie ein Kennwort für den Controller einmal und dann erneut ein.

Hinweis Der Benutzername darf nicht als Teilzeichenfolge im Kennwort enthalten sein. Zeichen dürfen maximal zweimal hintereinander wiederholt werden.

Das Kennwort muss mindestens 12 Zeichen lang sein und 3 der 4 folgenden Regeln folgen:

- mindestens ein Großbuchstabe
- mindestens ein Kleinbuchstabe
- mindestens eine Zahl
- mindestens ein Sonderzeichen

6 Stellen Sie nach der vollständigen Bereitstellung des ersten Controllers zwei weitere Controller bereit.

Es müssen drei Controller vorhanden sein. Es wird empfohlen, eine DRS-Anti-Affinitätsregel zu konfigurieren, mit der verhindert wird, dass sich die Controller auf demselben Host befinden.

Weiter

Aktualisieren von Host-Clustern

Aktualisieren von Host-Clustern

Sie müssen Ihre Umgebung auf die Netzwerkvirtualisierung vorbereiten, indem Sie auf Clusterebene Netzwerkinfrastrukturkomponenten für jeden vCenter Server installieren. Dadurch wird die erforderliche Software auf allen Hosts im Cluster installiert und die virtuellen Leitungen werden in logische NSX-Switches umbenannt. Bei diesem Vorgang erhält jeder Host im Cluster ein Software-Update und wird dann neu gestartet.

Wenn in Ihrer Umgebung virtuelle Leitungen vorliegen, müssen Sie nach dem Upgrade auf NSX Manager Ihre Host-Cluster aktualisieren.

Es wird empfohlen, dass Sie Host-Cluster in einem Datencenterwartungsfenster aktualisieren.

Wenn DRS aktiviert ist, überwachen Sie den Verlauf der Hostevakuierung, die Hosts, die in den Wartungsmodus wechseln, und den Hostneustart. Wenn DRS deaktiviert oder der manuelle Modus aktiviert ist, müssen Hostevakuierungen und -neustarts manuell durchgeführt werden. Während der Hostvorbereitung können Warnungen auftreten und durch Klicken auf das Warnsymbol eingeblendet werden. Klicken Sie auf **Auflösen (Resolve)**, wenn erforderlich.

Führen Sie während des Upgrades keine anderen Upgrades aus, stellen Sie keine Dienste oder Komponenten bereit und deinstallieren Sie keine Dienste oder Komponenten.

Hinweis In vCloud Networking and Security erstellte VTEPs verwenden DHCP oder manuell zugewiesene IP-Adressen und keine IP-Pools.

Voraussetzungen

- Stellen Sie sicher, dass vShield Manager auf NSX Manager aktualisiert wurde.
- Stellen Sie sicher, dass die Spalte „VXLAN“ der Registerkarte „Hostvorbereitung“ den Eintrag **Aktiviert (Enabled)** enthält.
- 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 Host-Clustern aktiviert ist.
  - Stellen Sie sicher, dass vMotion korrekt funktioniert.
  - Überprüfen Sie den Zustand der Hostverbindung mit vCenter.

- Stellen Sie sicher, dass sich mindestens drei ESXi-Hosts in jedem Host-Cluster 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.

Vorgehensweise

1 Melden Sie sich beim vSphere Web Client an.

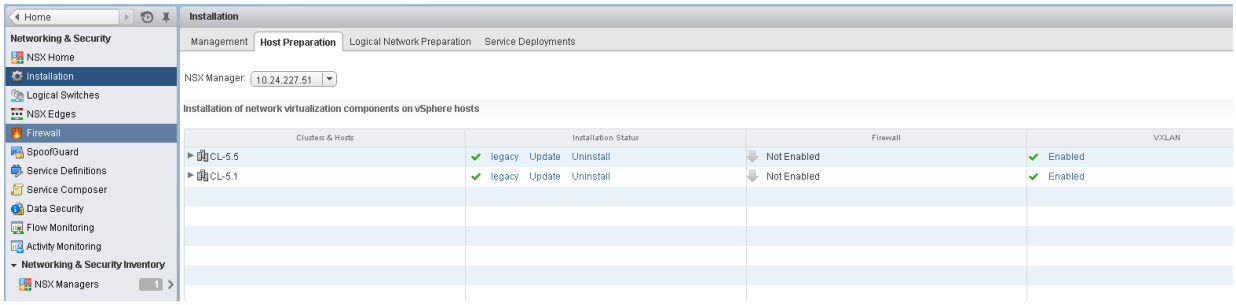
2 Klicken Sie auf **Networking & Security** und anschließend auf **Installation**.

3 Klicken Sie auf die Registerkarte **Hostvorbereitung (Host Preparation)**.

Alle Cluster in Ihrer Infrastruktur werden angezeigt.

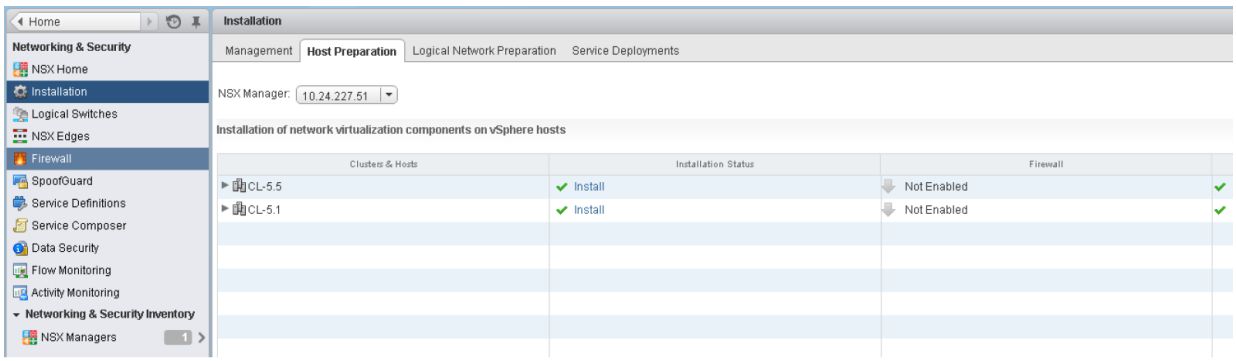
Wenn Sie virtuelle Leitungen in Ihrer 5.5-Umgebung hatten, zeigt die Spalte **Installationsstatus (Installation Status) Legacy**, **Aktualisieren (Update)** und **Deinstallieren (Uninstall)** an.

Abbildung 1-1. Der Installationsstatus zeigt „Aktualisieren“ an, wenn Sie virtuelle Leitungen in Ihrer 5.5-Umgebung haben



Wenn Sie keine virtuellen Leitungen in Ihrer 5.5-Umgebung hatten, zeigt die Spalte **Installationsstatus (Installation Status) Installieren (Install)** an.

Abbildung 1-2. Der Installationsstatus zeigt „Installieren“ an, wenn Sie virtuelle Leitungen in Ihrer 5.5-Umgebung haben



4 Klicken Sie für jeden Cluster in der Spalte „Installationsstatus“ auf **Aktualisieren (Update)** oder **Installieren (Install)**.

   Jeder Host im Cluster erhält die neue logische Switch-Software.

   Das Host-Upgrade initiiert eine Hostprüfung. Die alten VIBs werden entfernt (sie werden aber erst nach dem Neustart vollständig gelöscht). Neue VIBs werden auf der altboot-Partition installiert. Zum Anzeigen der neuen VIBs auf einem Host, der noch nicht neu gestartet wurde, können Sie den Befehl `esxcli software vib list ––rebooting–image | grep esx` ausführen.

5 Überwachen Sie die Installation, bis in der Spalte **Installationsstatus (Installation Status)** ein grünes Häkchen angezeigt wird.

   Wenn der Cluster DRS-fähig ist, versucht DRS, die Hosts auf kontrollierte Weise neu zu starten, sodass die VMs weiterhin ausgeführt werden können. vMotion verschiebt die gestarteten VMs auf andere Hosts im Cluster und versetzt den Host in den Wartungsmodus.

   Wenn Hosts manuell in den Wartungsmodus versetzt werden müssen (beispielsweise aufgrund von HA-Anforderungen oder DRS-Regeln), wird der Upgrade-Vorgang angehalten und als **Installationsstatus (Installation Status)** wird für den Cluster **Nicht bereit (Not Ready)** angezeigt. Klicken Sie auf ⚠, um die Fehler anzuzeigen.

   Nachdem Sie die Hosts manuell evakuiert haben, wählen Sie den Cluster aus und klicken Sie auf die Aktion **Auflösen (Resolve)**. Die Aktion **Auflösen (Resolve)** versucht, das Upgrade abzuschließen und alle Hosts im Cluster neu zu starten. Falls der Neustart der Hosts aus irgendeinem Grund fehlschlägt, wird die Aktion **Auflösen (Resolve)** angehalten. 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.

Alle virtuellen Leitungen Ihrer 5.5-Infrastruktur wurden in logische NSX-Switches umbenannt, und die Spalte VXLAN zeigt **Aktiviert (Enabled)** an.

Stellen Sie sicher, dass die Spalte „VXLAN“ der Registerkarte „Hostvorbereitung“ den Eintrag **Aktiviert (Enabled)** enthält.

Wenn der Cluster aktualisiert ist, wird in der Spalte **Installationsstatus (Installation Status)** die Softwareversion angezeigt, auf die Sie aktualisiert haben.

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 | grep esx` aus. Stellen Sie sicher, dass die folgenden VIBs auf die erwartete Version aktualisiert wurden.

- esx-vsip
- esx-vxlan

Hinweis In NSX 6.2 ist das „esx-dvfilter-switch-security“-VIB im „esx-vxlan“-VIB enthalten.

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.

Weiter

Ändern des VXLAN-Ports

Ändern des VXLAN-Ports

Sie können den für den VXLAN-Datenverkehr verwendeten Port ändern.

In NSX 6.2.3 und höher lautet der von IANA zugewiesene Standard-VXLAN-Port 4789. Vor NSX 6.2.3 lautete die Standard-VXLAN-UDP-Portnummer 8472.

Alle neuen NSX-Installationen verwenden jetzt den UDP-Port 4789 für VXLAN.

Wenn Sie von NSX 6.2.2 oder früher ein Upgrade auf NSX 6.2.3 oder höher durchführen und für Ihre Installation vor dem Upgrade die alte Standardnummer (8472) oder eine benutzerdefinierte Portnummer verwendet wurde (z. B. 8888), wird dieser Port so lange nach dem Upgrade weiter benutzt, bis Sie diesen ändern.

Wenn die Installation, für die ein Upgrade durchgeführt wurde, Hardware-VTEP-Gateways („ToR-Gateways“) verwendet oder verwenden soll, müssen Sie zum VXLAN-Port 4789 wechseln.

Cross-vCenter NSX erfordert nicht die Verwendung von 4789 für den VXLAN-Port. Allerdings muss für alle Hosts in einer Cross-vCenter NSX-Umgebung die Verwendung desselben VXLAN-Ports konfiguriert werden. Dadurch wird bei einem Wechsel zu Port 4789 sichergestellt, dass neue der Cross-vCenter NSX-Umgebung hinzugefügte NSX-Installationen denselben Port wie vorhandene NSX-Bereitstellungen verwenden.

Die Änderung des VXLAN-Ports erfolgt in drei Stufen und führt nicht zur Unterbrechung des VXLAN-Datenverkehrs.

1. NSX Manager konfiguriert alle Hosts, die auf VXLAN-Datenverkehr sowohl auf den alten wie auf den neuen Ports überwacht werden sollen. Hosts senden weiterhin VXLAN-Datenverkehr auf den alten Port.
2. NSX Manager konfiguriert alle Hosts für das Senden des Datenverkehrs auf den neuen Port.
3. NSX Manager konfiguriert alle Hosts für das Beenden der Überwachung auf dem alten Port. Der gesamte Datenverkehr wird auf dem neuen Port gesendet und empfangen.

In einer Cross-vCenter NSX-Umgebung müssen Sie die Änderung des Ports auf dem primären NSX Manager initiieren. In jeder Phase werden die Konfigurationsänderungen auf allen Hosts in der Cross-vCenter NSX-Umgebung durchgeführt, bevor mit der nächsten Phase fortgesetzt wird.

Voraussetzungen

- Stellen Sie sicher, dass der Port, den Sie für VXLAN verwenden möchten, nicht durch eine Firewall blockiert ist.

- Stellen Sie sicher, dass die Hostvorbereitung nicht zur gleichen Zeit ausgeführt wird wie die Änderung des VXLAN-Ports.

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 **Vorbereitung des logischen Netzwerks (Logical Network Preparation)** und dann auf **VXLAN-Transport (VXLAN Transport)**.
4. Klicken Sie im VXLAN-Portbereich auf die Schaltfläche **Ändern (Change)**. Geben Sie den Port ein, zu dem Sie wechseln möchten. 4789 ist der Port, der von IANA für VXLAN zugewiesen wurde.

   Es dauert einen Moment, bis die Portänderung an alle Hosts übermittelt wird.
5. (Optional) Sie können den Fortschritt der Portänderung mit der API-Anforderung `GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus` überprüfen.

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
    <prevPort>8472</prevPort>
    <targetPort>4789</targetPort>
    <taskPhase>PHASE_TWO</taskPhase>
    <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

...

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
    <prevPort>8472</prevPort>
    <targetPort>4789</targetPort>
    <taskPhase>FINISHED</taskPhase>
    <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

Weiter

Aktualisieren von Transportzonen und logischen Switches.

Aktualisieren von Transportzonen und logischen Switches

Wenn Sie einen NSX Controller-Cluster bereitstellen, sind Sie für logische Netzwerke nicht mehr von Multicast abhängig. Sie können den Steuerungskomponenten-Modus in Ihren Transportzonen und logischen Switches für die Verwendung von Unicast oder Hybrid aktualisieren.

Die Änderung des Steuerungskomponenten-Modus und die Migration von vorhandenen logischen Switches hat keine Auswirkungen auf den Datenverkehr der Netzwerkdatenebene.

Vorgehensweise

1. In vSphere Web Client navigieren Sie zu **Home > Networking & Security > Installation > Vorbereitung des logischen Netzwerks (Logical Network Preparation) > Transportzonen (Transport Zones)**.
2. Wählen Sie Ihre Transportzone aus und klicken Sie auf **Aktionen (Actions) > Einstellungen bearbeiten (Edit Settings)**. Wählen Sie den gewünschten Replizierungs-Modus aus:
   - **Multicast**: Multicast-IP-Adressen auf dem physischen Netzwerk werden für die Steuerungskomponente verwendet. Dieser Modus wird nur empfohlen, wenn Sie Upgrades von älteren VXLAN-Bereitstellungen aus durchführen wollen. Erfordert PIM/IGMP im physischen Netzwerk.
   - **Unicast**: Die Steuerungskomponente wird von einem NSX Controller verwendet. Der komplette Unicast-Datenverkehr verwendet die optimierte Kopfendereplikation. Es sind keine Multicast-IP-Adressen oder bestimmte Netzwerkkonfigurationen erforderlich.
   - **Hybrid**: Lagert eine Replizierung des lokalen Datenverkehrs auf das physische Netzwerk aus (L2 Multicast). Erfordert IGMP-Snooping auf dem ersten Hop-Switch und Zugriff auf einen IGMP-Abfrager in jedem VTEP-Subnetz, aber keinen PIM. Der erste Hop-Switch steuert die Datenverkehrsreplizierung für das Subnetz.
3. Aktivieren Sie das Kontrollkästchen **Migrieren Sie vorhandene logische Switches auf den neuen Steuerungskomponenten-Modus (Migrate existing Logical Switches to the new control plane mode)** und klicken Sie auf **OK**.

Weiter

Upgrade von vShield App auf Distributed Firewall.

Upgrade von vShield App auf Distributed Firewall

Sie können nur von vShield App Version 5.5 ein Upgrade auf Distributed Firewall durchführen. Wenn Ihre Infrastruktur eine Vorgängerversion von vShield App enthält, müssen Sie diese auf Version 5.5 aktualisieren, bevor Sie das Upgrade auf Version 6.2.x durchführen. Weitere Informationen zum Upgrade auf Version 5.5 finden Sie im *vShield Installations- und Upgrade-Handbuch* Version 5.5.

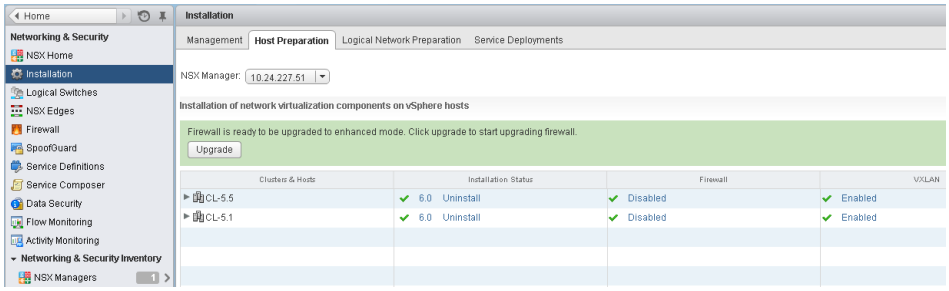
Die Dauer des nachfolgend aufgeführten Vorgangs hängt von der Anzahl der Regeln in Ihrer Umgebung ab. Wenn Sie von vShield App auf die NSX Distributed Firewall (erweiterter Modus) migrieren, werden die Regeln migriert und übertragen. Dies führt zur Unterbrechung des Datenverkehrs. Dieser Schritt sollte deshalb in einem Wartungsfenster durchgeführt werden.

Voraussetzungen

- vShield Manager wurde auf NSX Manager aktualisiert.
- Die virtuellen Leitungen wurden auf logische NSX-Switches aktualisiert. Für Benutzer, die kein VXLAN verwenden, wurden Netzwerkvirtualisierungskomponenten installiert.
- Wenn Sie vShield App 5.5-Regeln auf die Distributed Firewall migrieren möchten, dürfen Sie die vShield App-Appliances vor dem Upgrade auf die Distributed Firewall nicht löschen.

Vorgehensweise

1 Nach der Vorbereitung aller Cluster in Ihrer Umgebung für die Komponenten der Netzwerkvirtualisierung zeigt eine Meldung an, dass das Upgrade für die Firewall durchgeführt werden kann.



2 Klicken Sie auf **Upgrade durchführen (Upgrade)**.

Die vShield App 5.5-Regeln werden in folgender Weise auf NSX migriert:

a In der zentralen Firewalltabelle wird für jeden Namespace (Datencenter und virtuelle Leitung), der in vShield App Version 5.5 konfiguriert wurde, ein neuer Bereich erstellt. Jeder Bereich verfügt über die entsprechenden Firewallregeln.

b Alle Regeln in jedem Bereich haben denselben Wert im Feld **Angewendet auf (AppliedTo)**: Datencenter-ID für Datencenter-Namespace, virtuelle Leitungs-ID für virtuellen Leitungs-Namespace und Portgruppen-ID für portgruppenbasierten Namespace.

c Container, die auf verschiedenen Ebenen des Namespace erstellt wurden, werden auf die globale Ebene verschoben.

d Die Bereichsreihenfolge bleibt wie unten angegeben, um sicherzustellen, dass das Firewallverhalten nach der Durchführung des Upgrades gleich bleibt:

Section_Namespace_Portgroup-1

.....

Section_Namespace_Portgroup-N

Section_Namespace_VirtualWire-1

.....

Section_Namespace_VirtualWire-N

Section_Namespace_Datacenter_1

.....

Section_Namespace_Datacenter_N

Default_Section_DefaultRule

Nachdem das Upgrade abgeschlossen ist, zeigt die Spalte „Firewall“ **Aktiviert (Enabled)** an.

3 Klicken Sie auf **Home > Hosts und Cluster (Hosts and Clusters)** und wechseln Sie zu den Hosts, auf denen vShield App-Dienst-VMs ausgeführt werden. Fahren Sie die Legacy vShield App-Dienst-VMs herunter.

4 Wechseln Sie zu **Networking & Security > Firewall** und überprüfen Sie jeden aktualisierten Abschnitt bzw. jede aktualisierte Regel und testen Sie, ob sie wie vorgesehen funktionieren.

5 Wechseln Sie zur Registerkarte **Installation > Dienstbereitstellungen (Service Deployments)** und stellen Sie sicher, dass alle Alarme aufgelöst wurden und dass als Dienststatus für die Legacy vShield App **Erfolg (Succeeded)** angezeigt wird.

6 Wenn die Regeln korrekt funktionieren, wählen Sie in der Registerkarte **Dienstbereitstellungen (Service Deployments)** „vShield App“ aus und klicken Sie auf **Dienstbereitstellung löschen (Delete Service Deployment) (✖)**, um die Legacy vShield App-Dienst-VMs zu entfernen.

Weiter

Upgrade von vShield Edge auf NSX Edge

Upgrade von vShield Edge auf NSX Edge

Sie können nur von vShield 5.5 ein Upgrade auf NSX Edge 6.2.x durchführen. Wenn Ihre Infrastruktur eine Vorgängerversion von vShield Edge enthält, müssen Sie diese auf Version 5.5 aktualisieren, bevor Sie das Upgrade auf Version 6.2.x durchführen. Weitere Informationen zum Upgrade auf Version 5.5 finden Sie im *vShield Installations- und Upgrade-Handbuch* Version 5.5.

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.

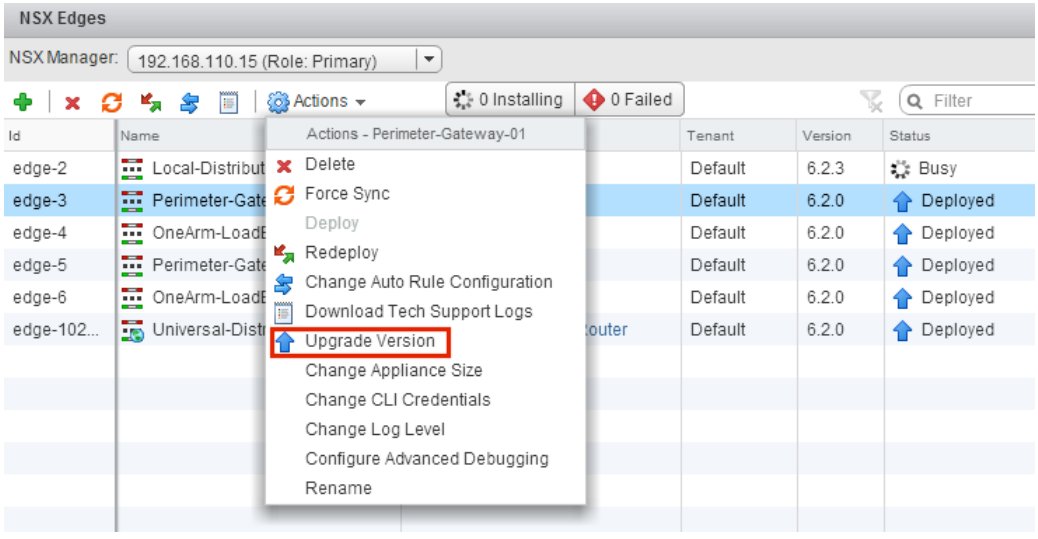
Voraussetzungen

- Stellen Sie sicher, dass vShield Manager auf NSX Manager aktualisiert wurde.
- Machen Sie sich während der Durchführung des Upgrades mit den operativen Auswirkungen des NSX Edge-Upgrades vertraut. Siehe Operative Auswirkungen von Upgrades für vCloud Networking and Security.
- 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.
  - Ab der Version NSX 6.2.3 werden, wenn für eine NSX Edge-Instanz mit Hochverfügbarkeit (HA, High Availability) ein Upgrade durchgeführt wird, 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.
  - Vor der Version NSX 6.2.3 wird, wenn für eine NSX Edge-Instanz mit Hochverfügbarkeit ein Upgrade durchgeführt wird, jeweils nur eine Ersetzungs-Appliance bereitgestellt, während die alten Appliances ersetzt werden. Es befinden sich dann während des Upgrades einer bestimmten NSX Edge drei NSX Edge-Appliances der geeigneten Größe im eingeschalteten Status. Nach dem Upgrade der NSX Edge-Instanz wird in der Regel die NSX Edge-Appliance mit dem HA-Index 0 aktiv.
- Das Durchführen eines Upgrades für einen NSX Edge mit Version 5.5 oder 6.0 mit aktiviertem L2 VPN wird nicht unterstützt. Sie müssen die L2 VPN-Konfiguration löschen, bevor Sie ein Upgrade durchführen. 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. Melden Sie sich beim vSphere Web Client an.
2. Klicken Sie auf **Networking & Security** und anschließend auf **NSX Edges**.
3. Wählen Sie für jede NSX Edge-Instanz die Option **Upgrade der Version durchführen (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.

In NSX Edge-Firewallregeln wird „sourcePort“ nicht unterstützt. Daher müssen die Regeln von vShield Edge Version 5.5, die „sourcePort“ enthalten, während des Upgrades wie folgt geändert werden.

- Wenn in der Regel keine applications-Einträge verwendet werden, wird ein Dienst mit den Einstellungen „protocol=any“, „port=any“ und „sourcePort=asDefinedInTheRule“ erstellt.
- Wenn die Regel Einträge für „applications“ oder „applicationsGroups“ aufweist, werden diese Gruppierungsobjekte dupliziert, indem ihnen „sourcePort“ hinzugefügt wird. Deswegen sind die in der Firewallregel verwendeten groupingObjectIds nach dem Upgrade verändert.

Benutzerfirewallregeln in NSX Edge 6.x generieren keine internen IPSets und applicationSets auf der Basis einer Eingabe von REST-APIs. Stattdessen werden sie in einem nicht formatierten Format beibehalten. Während des Upgrades werden mit den intern generierten IPSets und applicationSets Regeln mit nicht formatierten Daten erstellt. Die internen gruppierten Objekte sind nicht mehr in den Benutzerfirewallregeln enthalten

Weiter

Konfigurieren Sie bei Bedarf alle L2 VPN-Konfigurationen neu. Weitere Informationen finden Sie im *Installationshandbuch für NSX* unter „Überblick über L2 VPN“.

Upgrade von Guest Introspection

Upgrade von vShield Endpoint auf NSX Guest Introspection

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

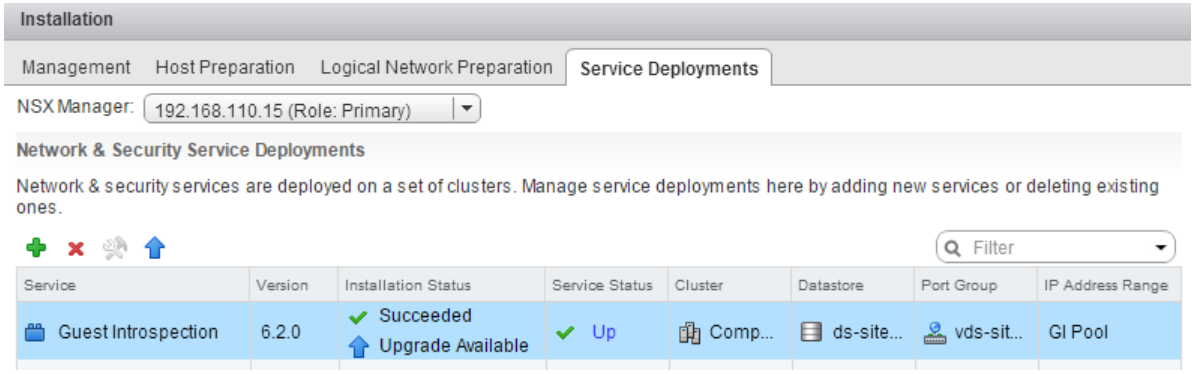
Hinweis Für die Guest Introspection-Dienst-VMs kann ein Upgrade über vSphere Web Client durchgeführt werden. Sie müssen die Dienst-VM für deren Upgrade nach dem Upgrade von NSX Manager nicht löschen. Wenn Sie die Dienst-VM löschen, wird für den Dienststatus `Fehlgeschlagen` angezeigt, da die Agenten-VM 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

Voraussetzung dafür ist das Upgrade von NSX Manager, Controllern, vorbereiteten Host-Clustern und NSX Edges auf Version 6.2.x.

Vorgehensweise

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

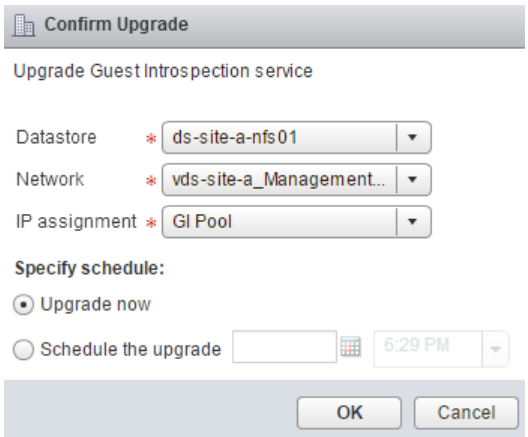


Die Spalte **Installationsstatus (Installation Status)** enthält den Wert **Upgrade verfügbar (Upgrade available)**.

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.

Wenn Sie für eine Partnerlösung ein Upgrade auf eine NSX-zertifizierte Version durchführen, müssen Sie mit Service Composer Richtlinien auf der Basis der Partnerlösungen erstellen, damit diese geschützt bleiben. Weitere Informationen erhalten Sie im *Administratorhandbuch für NSX* unter „Verwenden des Service Composer“.

NSX Services, die kein direktes Upgrade unterstützen

Einige NSX Services, wie virtuelle Sicherheits-Appliances von VMware-Partnern 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.

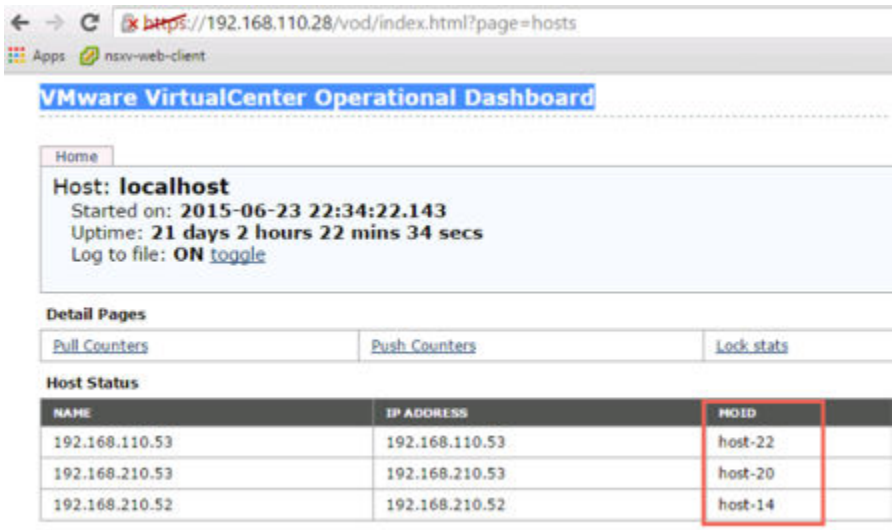
NSX Data Security

Sie sollten NSX Data Security vor dem Upgrade von NSX deinstallieren und nach Abschluss des NSX-Upgrades neu installieren. Wenn Sie NSX bereits aktualisiert haben, ohne NSX Data Security vorher zu deinstallieren, müssen Sie Data Security mithilfe eines REST-API-Aufrufs deinstallieren.

Geben Sie den folgenden API-Aufruf aus:

```
DELETE https://<nsx-manager-ip>/api/1.0/vshield/<host-id>/vsds
```

Die Host-ID ist die MOID des ESXi-Hosts. Um die MOID abzurufen, öffnen Sie das VMware VirtualCenter Operational Dashboard: https://<vcenter-ip>/vod/index.html?page=hosts.



Für den ESXi-Host mit der MOID „host-22“ auf vCenter Server 192.168.110.28 würde der API-Aufruf folgendes Format aufweisen:

```
DELETE https://192.168.110.28/api/1.0/vshield/host-22/vsds
```

Stellen Sie sicher, dass Sie den API-Aufruf auf allen Ihren ESXi-Hosts ausführen.

Nach der Deinstallation von Data Security können Sie die neue Version installieren. Weitere Informationen dazu finden Sie unter Installieren von NSX Data Security.

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 6.2.x der SSL VPN-Clients. Diese „Installieren des SSL-Clients auf der Remote-Site“ im *Administratorhandbuch für NSX*.

NSX L2 VPN

Das Durchführen eines Upgrades für NSX Edge wird nicht unterstützt, wenn Sie L2 VPN auf einem NSX Edge mit Version 5.5.x oder 6.0.x installiert haben. Alle L2 VPN-Konfigurationen müssen vor dem Upgrade von NSX Edge gelöscht werden.

Installieren von NSX Data Security

Hinweis Ab der Version NSX 6.2.3 wird die NSX Data Security-Funktion eingestellt. In NSX 6.2.3 können Sie diese Funktion noch auf eigene Verantwortung weiter benutzen. In künftigen NSX-Versionen ist diese Funktion jedoch nicht mehr enthalten.

Voraussetzungen

NSX Guest Introspection muss auf dem Cluster installiert sein, auf dem Sie Data Security installieren.

Wenn Sie der VM des Data Security-Diensts eine IP-Adresse aus einem IP-Pool zuweisen möchten, erstellen Sie den IP-Pool, bevor Sie Data Security installieren. Siehe „Gruppieren von Objekten“ im *Administratorhandbuch für NSX*.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Installation** auf **Dienstbereitstellungen (Service Deployments)**.
2. Klicken Sie auf das Symbol **Neue Dienstbereitstellung (New Service Deployment)** ( ).
3. Wählen Sie im Dialogfeld „Netzwerk- und Sicherheitsdienste bereitstellen“ **Data Security** und klicken Sie auf **Weiter (Next)**.
4. Wählen Sie in **Zeitplan angeben (Specify schedule)** (unten im Dialogfeld) **Jetzt bereitstellen (Deploy now)**, um Data Security bereitzustellen, sobald es installiert ist, oder wählen Sie ein Datum und eine Uhrzeit für die Bereitstellung aus.
5. Klicken Sie auf **Weiter (Next)**.

6 Wählen Sie das Datencenter und die Cluster dort aus, wo Sie Data Security installieren wollen, und klicken Sie auf **Weiter (Next)**.

7 Wählen Sie auf der Seite „Speicher- und Verwaltungsnetzwerk auswählen“ den Datenspeicher aus, auf dem Sie den VM-Speicher für den Dienst hinzufügen möchten, oder wählen Sie die Option **Angegeben auf dem Host (Specified on host)** aus.

   Der ausgewählte Datenspeicher muss auf allen Hosts im ausgewählten Cluster verfügbar sein.

   Wenn Sie **Angegeben auf dem Host (Specified on host)** ausgewählt haben, muss der Datenspeicher für den ESX-Host in den **Agent-VM-Einstellungen (AgentVM Settings)** des Hosts angegeben werden, bevor dieser zum Cluster hinzugefügt wird. Weitere Informationen hierzu finden Sie in der *vSphere-API/SDK-Dokumentation*.

8 Wählen Sie die verteilte virtuelle Portgruppe aus, in der die Verwaltungsschnittstelle gehostet werden soll. Diese Portgruppe muss in der Lage sein, die Portgruppe des NSX Managers zu erreichen.

   Wenn der Datenspeicher auf **Angegeben auf dem Host (Specified on host)** festgelegt ist, muss das zu verwendende Netzwerk in der Eigenschaft **agentVmNetwork** jedes Hosts im Cluster angegeben werden. Weitere Informationen hierzu finden Sie in der *vSphere-API/SDK-Dokumentation*.

   Die Eigenschaft **agentVmNetwork** muss für alle Hosts, die Sie zum Cluster hinzufügen möchten, vorher festgelegt werden.

   Die ausgewählte Portgruppe muss auf allen Hosts im ausgewählten Cluster verfügbar sein.

9 Wählen Sie unter „IP-Zuweisungen“ eine der folgenden Optionen aus:

Option	Zweck
DHCP	Weisen Sie der VM des Data Security-Diensts eine IP-Adresse über Dynamic Host Configuration Protocol (DHCP) zu.
Einen IP-Pool	Weisen Sie der VM des Data Security-Diensts eine IP-Adresse aus dem ausgewählten IP-Pool zu.

   Beachten Sie, dass statische IP-Adressen nicht unterstützt werden.

10 Klicken Sie auf der Seite „Bereit zum Abschließen“ auf **Weiter (Next)** und anschließend auf **Beenden (Finish)**.

11 Überwachen Sie die Bereitstellung, bis **Erfolg (Succeeded)** für die Spalte **Installationsstatus (Installation Status)** angezeigt wird.

12 Wenn **Fehlgeschlagen (Failed)** für die Spalte **Installationsstatus (Installation Status)** angezeigt wird, klicken Sie auf das Symbol neben „Fehlgeschlagen“. Es werden alle Bereitstellungsfehler angezeigt. Klicken Sie auf **Auflösen (Resolve)**, um die Fehler zu beheben. In einigen Fällen werden beim Auflösen der Fehler zusätzliche Fehlermeldungen angezeigt. Führen Sie die nötige(n) Aktion(en) aus und klicken Sie wieder auf **Auflösen (Resolve)**.

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 vCloud Networking and Security 5.5.x auf NSX in einer vCloud Director-Umgebung

Von der vCloud Director-Version hängt die Version von NSX ab, auf die Sie ein Upgrade durchführen können. VMware empfiehlt ein Upgrade auf die zuletzt unterstützte NSX-Version, die mit den anderen Lösungen und Tools in Ihrer Umgebung kompatibel ist.

Weitere Informationen hierzu finden Sie in der VMware-Produkt-Interoperabilitätsmatrix unter https://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Um ein Upgrade auf NSX durchzuführen, müssen Sie die vCloud Networking and Security-Komponenten in der Reihenfolge aktualisieren wie in diesem Handbuch dokumentiert.

Die vCloud Networking and Security-Komponenten müssen in der folgenden Reihenfolge aktualisiert werden:

1 Upgrade von vShield Manager auf NSX Manager

2 Bereitstellen von NSX Controller-Clustern (optional); dies ist für logische (verteilte) Router und die Änderung des Steuerungskomponenten-Modus auf „Hybrid“ oder „Unicast“ erforderlich

3 Aktualisieren von Host-Clustern

4 Aktualisieren der Transportzone (optional); wenn der NSX Controller-Cluster bereitgestellt wurde, können Sie den Steuerungskomponenten-Modus von „Hybrid“ auf „Unicast“ ändern

5 NSX Edge – ein Upgrade auf NSX Edge ist nur möglich, wenn Sie vCloud Director 8.10 oder höher verwenden.

Wichtig Wenn in Ihrer Umgebung virtuelle Leitungen vorliegen, müssen Sie nach dem Upgrade auf NSX Manager Ihre Host-Cluster aktualisieren.

Optionale vCloud Networking and Security-Komponenten, die nicht in vCloud Director integriert sind:

1 vShield App – siehe Upgrade von vShield App auf Distributed Firewall

2 vShield Endpoint – siehe Upgrade von vShield Endpoint auf NSX Guest Introspection.

3 vShield Data Security – es wird kein Upgrade unterstützt. Anleitungen zur Deinstallation finden Sie unter NSX Services, die kein direktes Upgrade unterstützen und zur Installation unter Installieren von NSX Data Security.

Upgrade von vShield Manager auf NSX Manager in einer vCloud Director-Umgebung

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

Vorsicht Deinstallieren Sie keine bereitgestellte Instanz der vShield Manager-Appliance.

Voraussetzungen

- Vergewissern Sie sich, dass alle in Vorbereiten des Upgrades von vCloud Networking and Security auf NSX beschriebenen Aufgaben zur Upgrade-Vorbereitung abgeschlossen sind, inklusive der Überprüfung der Systemanforderungen und der Durchführung von Sicherungen.
- Stellen Sie sicher, dass vShield Manager über genügend Festplattenspeicher für das Upgrade auf NSX Manager verfügt. Siehe Systemvoraussetzungen für NSX.
- Erhöhen Sie den reservierten Arbeitsspeicher der virtuellen vShield Manager-Appliance auf mindestens 16 GB und teilen Sie 4 vCPUs zu, ehe Sie das Upgrade auf NSX 6.2.x durchführen.

  Siehe Systemvoraussetzungen für NSX.

- Stellen Sie sicher, dass vShield Edge-Instanzen, die älter als Version 5.5 sind, auf Version vShield 5.5 aktualisiert wurden.

  vShield Edge-Instanzen, die älter als 5.5 sind, können nicht mehr verwaltet oder gelöscht werden, nachdem für vShield Manager ein Upgrade auf NSX Manager durchgeführt wurde.

Vorgehensweise

1. Laden Sie das NSX-Upgrade-Paket an einen Speicherort herunter, auf den vShield Manager zugreifen kann. Der Name der Upgrade-Paket-Datei lautet in etwa `VMware-vShield-Manager-upgrade-bundle-to-NSX-`*`release-buildNumber`*`.tar.gz`.
2. Klicken Sie im Bestandslistenbereich von vShield Manager 5.5 auf **Einstellungen und Berichte**.
3. Klicken Sie auf die Registerkarte **Updates** und dann auf **Upgrade-Paket hochladen**.
4. Klicken Sie auf **Datei auswählen**, wählen Sie die Datei `VMware-vShield-Manager-upgrade-bundle-to-NSX-`*`release-buildNumber`*`.tar.gz` aus und klicken Sie auf **Öffnen**.
5. Klicken Sie auf **Datei hochladen**.

   Das Hochladen der Dateien dauert einige Minuten.
6. Klicken Sie auf **Installieren**, um mit dem Upgrade zu beginnen.
7. Klicken Sie auf **Installation bestätigen**. Der Upgrade-Vorgang startet vShield Manager neu, d. h., die Verbindung zur vShield Manager-Benutzeroberfläche geht möglicherweise verloren. Keine der anderen vShield-Komponenten wird neu gestartet.
8. Nach dem Neustart melden Sie sich bei der virtuellen NSX Manager-Appliance durch Öffnen eines Webbrowser-Fensters und Eingabe der IP-Adresse (z. B https://10.10.10.10) an. Der NSX Manager verfügt nach dem Upgrade über die gleiche IP-Adresse wie der vShield Manager.

   Die Registerkarte „Übersicht“ zeigt die Version von NSX-Manager an, die Sie gerade installiert haben.
9. Wechseln Sie zu **Home > vCenter-Registrierung verwalten** und stellen Sie sicher, dass für den vCenter Server-Status `Verbunden` gilt.
10. Schließen Sie alle vorhandenen Browser-Sitzungen, die auf vSphere Web Client zugreifen. Warten Sie einige Minuten und löschen Sie den Browser-Cache, bevor Sie sich am vSphere Web Client anmelden.
11. Wenn SSH auf vShield Manager aktiviert war, müssen Sie es nach der Durchführung des Upgrades auf NSX-Manager aktivieren. Melden Sie sich an der virtuellen NSX-Manager-Appliance an und klicken Sie auf **Übersicht anzeigen**. Klicken Sie in den Komponenten auf Systemebene für den SSH-Dienst auf **Start**.

Wichtig Nach dem Upgrade von vCloud Networking and Security 5.x auf NSX 6.x müssen Sie sich mit Ihren CLI-Administratoranmeldedaten beim NSX Manager anmelden. Bisher waren für vCloud Networking and Security zwei Kennwörter erforderlich, eines für die Befehlszeilenschnittstelle (CLI) und ein anderes für die Benutzeroberfläche. Ab der Version NSX 6.x wird nur mehr ein Kennwort benötigt. Beispiel:

Kennwörter in vCloud Networking and Security

- mypassword#123 für die Befehlszeilenschnittstelle (CLI)
- mypassword#456 für die Benutzeroberfläche

Kennwörter nach dem Upgrade auf NSX

- mypassword#123 für die Befehlszeilenschnittstelle (CLI)
- mypassword#123 für die Benutzeroberfläche

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. Siehe Sichern und Wiederherstellen von NSX. Die vorherige NSX Manager-Sicherung gilt nur für die vorherige Version.

Weiter

Installieren und Zuweisen einer NSX-Lizenz in einer vCloud Director-Umgebung

Installieren und Zuweisen einer NSX-Lizenz in einer vCloud Director-Umgebung

Sie können, nachdem das Upgrade des NSX Manager abgeschlossen ist, eine Lizenz von NSX for vSphere installieren und zuweisen, indem Sie vSphere Web Client verwenden.

Ab der Version NSX 6.2.3 wird als Standardlizenz diejenige für NSX für vShield Endpoint installiert. Mit dieser Lizenz können Benutzer mit NSX vShield Endpoint nur für die Antivirenfunktion bereitstellen und verwalten. Außerdem wird die Nutzung von VXLAN, Firewall und Edge-Diensten durch Blockierung der Hostvorbereitung und der Erstellung von Edges stark eingeschränkt.

Um NSX mit vCloud Director verwenden zu können, müssen Sie eine NSX-Lizenz, die die zusätzlich erforderlichen NSX-Funktionen inklusive NSX Edge umfasst, erwerben.

Weitere Informationen finden Sie in der NSX-Lizenz-FAQ unter https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf

Weitere Informationen zur NSX-Lizenzierung finden Sie unter http://www.vmware.com/files/pdf/vmware-product-guide.pdf.

Vorgehensweise

- In vSphere 5.5 führen Sie die im Folgenden aufgeführten Schritte zum Hinzufügen einer Lizenz für NSX durch.
  a. Melden Sie sich beim vSphere Web Client an.
  b. Klicken Sie auf **Verwaltung (Administration)** und dann auf **Lizenzen (Licenses)**.
  c. Klicken Sie auf die Registerkarte **Lösungen (Solutions)**.
  d. Wählen Sie in der Liste „Lösungen“ die Option „NSX for vSphere“ aus. Klicken Sie auf **Lizenzschlüssel zuweisen (Assign a license key)**.
  e. Wählen Sie im Dropdown-Menü **Neuen Lizenzschlüssel zuweisen (Assign a new license key)** aus.
  f. Geben Sie den Lizenzschlüssel und eine optionale Bezeichnung für den neuen Schlüssel ein.
  g. Klicken Sie auf **Entschlüsseln (Decode)**.

     Entschlüsseln Sie den Lizenzschlüssel, um sicherzustellen, dass er das richtige Format aufweist und über genügend Kapazität verfügt, um die Assets zu lizenzieren.
  h. Klicken Sie auf **OK**.

- In vSphere 6.0 führen Sie die im Folgenden aufgeführten Schritte zum Hinzufügen einer Lizenz für NSX durch.
  a Melden Sie sich beim vSphere Web Client an.
  b Klicken Sie auf **Verwaltung (Administration)** und dann auf **Lizenzen (Licenses)**.
  c Klicken Sie auf die Registerkarte **Assets** und dann auf die Registerkarte **Lösungen (Solutions)**.
  d Wählen Sie in der Liste „Lösungen“ die Option „NSX for vSphere“ aus. Im Dropdown-Menü **Alle Aktionen (All Actions)** wählen Sie **Lizenz zuweisen... (Assign license...)** aus.
  e Klicken Sie auf das Symbol **Hinzufügen (Add)** (). Geben Sie einen Lizenzschlüssel ein und klicken Sie auf **Weiter (Next)**. Fügen Sie einen Namen für die Lizenz hinzu und klicken Sie auf **Weiter (Next)**. Klicken Sie zum Hinzufügen der Lizenz auf **Beenden (Finish)**.
  f Wählen Sie die neue Lizenz aus.
  g (Optional) Klicken Sie auf das Symbol **Funktionen anzeigen (View Features)**, um darzustellen, welche Funktionen mit dieser Lizenz aktiviert sind. In der Spalte **Kapazität (Capacity)** wird der Leistungsumfang der Lizenz angegeben.
  h Klicken Sie auf **OK**, um NSX die neue Lizenz zuzuweisen.

Weiter

Bereitstellen des NSX Controller-Clusters für NSX in einer vCloud Director-Umgebung (optional; ermöglicht die Auswahl von Steuerungskomponenten-Modi über Multicast hinaus).

Wenn Sie keine Controller bereitstellen, finden Sie Erläuterungen unter Aktualisieren von Host-Clustern von vCNS auf NSX in einer vCloud Director-Umgebung.

Bereitstellen des NSX Controller-Clusters für NSX in einer vCloud Director-Umgebung

NSX Controller ist ein erweitertes, verteiltes Zustandsverwaltungssystem, das Steuerungskomponentenfunktionen für logische Switching- und Routing-Funktionen für NSX bereitstellt. Das System fungiert als zentraler Kontrollpunkt für alle logischen Switches innerhalb eines Netzwerks und pflegt Informationen zu allen Hosts, logischen Switches (VXLANs) und Distributed Logical Routern. Controller sind erforderlich, wenn Sie Distributed Logical Router oder VXLAN im Unicast-oder Hybrid-Modus bereitstellen möchten.

Unabhängig von der Größe der NSX-Bereitstellung ist es für VMware erforderlich, dass jeder NSX Controller-Cluster drei Controller-Knoten enthält. Eine andere Anzahl an Controller-Knoten wird nicht unterstützt.

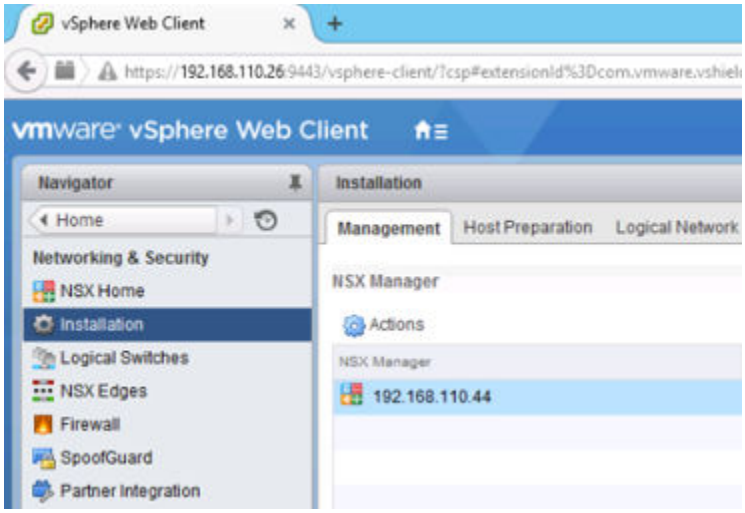
Voraussetzungen

- Bevor Sie NSX Controller bereitstellen, müssen Sie eine NSX Manager-Appliance bereitstellen und vCenter bei NSX Manager registrieren.
- Legen Sie die IP-Pool-Einstellungen für Ihren Controller-Cluster, einschließlich des Gateways und des IP-Adressbereichs, fest. DNS-Einstellungen sind optional. Das IP-Netzwerk des NSX Controllers muss mit dem NSX Manager und den Verwaltungsschnittstellen auf den ESXi-Hosts verbunden sein.

Vorgehensweise

1 Gehen Sie in vCenter zu **Home> Networking & Security > Installation** und wählen Sie die Registerkarte **Management** aus.

Beispiel:

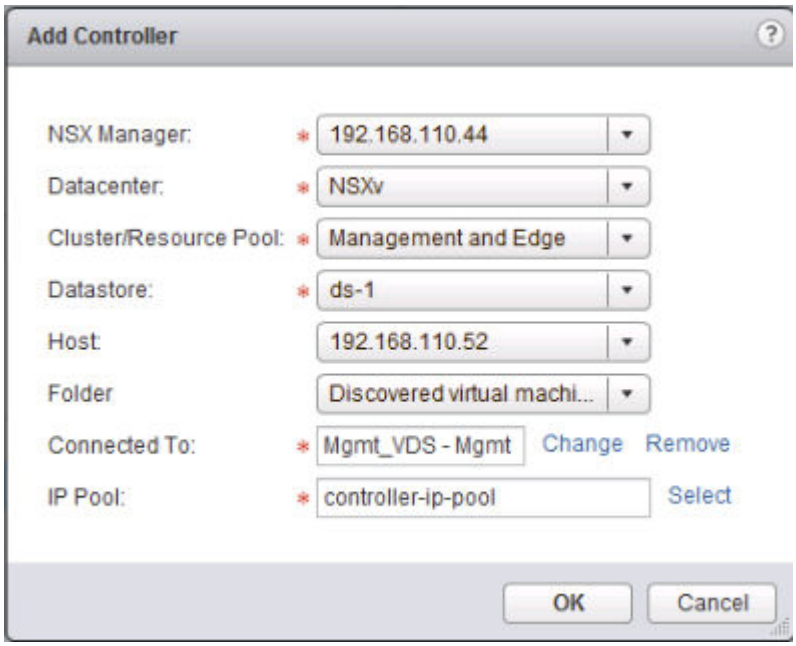


2 Klicken Sie im Bereich der NSX Controller-Knoten auf das Symbol **Knoten hinzufügen** ( ).

3 Geben Sie die für Ihre Umgebung geeigneten NSX Controller-Einstellungen ein.

NSX Controller müssen für eine vSphere Standard Switch- oder vSphere Distributed Switch-Portgruppe bereitgestellt werden, die nicht auf VXLAN basiert und die über eine Konnektivität zum NSX Manager, zu anderen Controllern und zu Hosts über IPv4 verfügt.

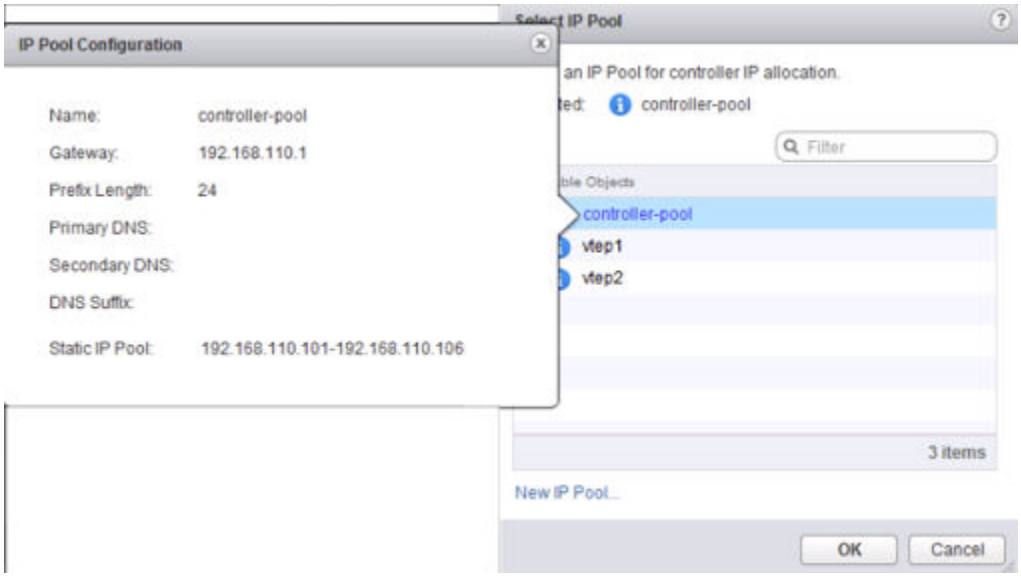
Beispiel:



4 Wenn Sie noch keinen IP-Pool für Ihren Controller-Cluster konfiguriert haben, tun Sie dies jetzt, indem Sie auf **Neuer IP-Pool** klicken.

Falls erforderlich, können einzelne Controller sich in separaten IP-Subnetzen befinden.

Beispiel:



5 Geben Sie ein Kennwort für den Controller einmal und dann erneut ein.

Hinweis Der Benutzername darf nicht als Teilzeichenfolge im Kennwort enthalten sein. Zeichen dürfen maximal zweimal hintereinander wiederholt werden.

Das Kennwort muss mindestens 12 Zeichen lang sein und 3 der 4 folgenden Regeln folgen:

- mindestens ein Großbuchstabe
- mindestens ein Kleinbuchstabe
- mindestens eine Zahl
- mindestens ein Sonderzeichen

6 Stellen Sie nach der vollständigen Bereitstellung des ersten Controllers zwei weitere Controller bereit.

Es müssen drei Controller vorhanden sein. Es wird empfohlen, eine DRS-Anti-Affinitätsregel zu konfigurieren, mit der verhindert wird, dass sich die Controller auf demselben Host befinden.

Nach erfolgreicher Bereitstellung wird für die Controller der Status **Normal** und ein grünes Häkchen angezeigt.

Verbinden Sie sich per SSH mit den einzelnen Controllern und vergewissern Sie sich, dass diese die IP-Adressen der Host-Verwaltungsschnittstelle anpingen können. Sollte das Anpingen fehlschlagen, überprüfen Sie, ob alle Controller über das richtige Standard-Gateway verfügen. Führen Sie zur Ansicht der Routing-Tabelle eines Controllers den Befehl **Netzwerkrouten anzeigen** aus. Führen Sie zum Ändern des Standard-Gateways eines Controllers den Befehl **Netzwerkrouten löschen** und anschließend den Befehl **Standard-Netzwerkroute hinzufügen <IP-address>** aus.

Führen Sie folgende Befehle aus, um zu überprüfen, ob der Controller-Cluster sich erwartungsgemäß verhält.

- `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.

- `show control-cluster roles`

```
                          Listen-IP  Master?    Last-Changed  Count
api_provider         Not configured      Yes  06/02 08:49:31      4
persistence_server              N/A      Yes  06/02 08:49:31      4
switch_manager            127.0.0.1      Yes  06/02 08:49:31      4
logical_manager                 N/A      Yes  06/02 08:49:31      4
directory_server                N/A      Yes  06/02 08:49:31      4
```

  Für jede Rolle ist ein Controller-Knoten der Master. In diesem Beispiel ist ein einzelner Knoten der Master für alle Rollen.

  Wenn eine NSX Controller-Masterinstanz für eine Rolle ausfällt, wählt der Cluster aus den verfügbaren NSX Controller-Instanzen einen neuen Master für diese Rolle aus.

  NSX Controller-Instanzen befinden sich auf der Steuerungsebene, damit der Ausfall eines NSX Controllers nicht den Datenverkehr auf der Datenebene beeinträchtigt.

- `show control-cluster connections`

```
role                server            listening open conns
------------------------------------------------------------
api_provider        api/443           Y         2
------------------------------------------------------------
persistence_server  server/2878       Y         2
                    client/2888       Y         1
                    election/3888     Y         0
------------------------------------------------------------
switch_manager      ovsmgmt/6632      Y         0
                    openflow/6633     Y         0
------------------------------------------------------------
system              cluster/7777      Y         0
```

  Mit diesem Befehl wird der Kommunikationsstatus innerhalb des Clusters angezeigt.

  Der „Mehrheitsführer“ des Controller-Clusters überwacht Port 2878 (durch das „Y“ in der Spalte „Listening“ dargestellt). Bei den anderen Controller-Knoten steht in der Spalte „Listening“ unter Port 2878 ein Bindestrich (-).

  Alle anderen Ports sollten alle drei Controller-Knoten überwachen.

  In der Spalte „Open conns“ wird die Anzahl der offenen Verbindungen angezeigt, die zwischen dem Controller-Knoten und anderen Controller-Knoten vorhanden sind. In einem Controller-Cluster mit 3 Knoten sollte der Controller-Knoten maximal zwei offene Verbindungen haben.

Weiter

Vorsicht Während ein Controller-Status **Wird bereitgestellt** anzeigt, dürfen Sie in Ihrer Umgebung keine logischen Switches oder verteiltes Routing hinzufügen oder ändern. Fahren Sie auch nicht mit dem Verfahren zur Hostvorbereitung fort. Nachdem der neue Controller zum Controller-Cluster hinzugefügt wurde, sind alle Controller eine kurze Zeit lang inaktiv (maximal 5 Minuten). Während dieser Downtime können alle Vorgänge im Zusammenhang mit Controllern (z. B. die Hostvorbereitung) zu unerwarteten Ergebnissen führen. Obwohl die Hostvorbereitung vollständig erfolgreich zu sein gewesen scheint, kann das SSL-Zertifikat möglicherweise nicht korrekt eingerichtet werden, was zu Problemen im VXLAN-Netzwerk führt.

Erläuterungen zum Löschen eines bereitgestellten Controllers finden Sie unter „Wiederherstellen nach dem Ausfall eines NSX Controllers“ im Handbuch *Administratorhandbuch für NSX*.

Auf den Hosts, auf denen die NSX Controller-Knoten zuerst bereitgestellt werden, aktiviert NSX automatisch das Starten/Herunterfahren von virtuellen Maschinen. Wenn die Controller-Knoten-VMs später zu anderen Hosts migriert werden, ist auf dem neuen Hosts das automatische Starten/Herunterfahren von virtuellen Maschinen möglicherweise nicht aktiviert. Aus diesem Grund empfiehlt VMware, dass Sie alle Hosts im Cluster überprüfen, um sicherzustellen, dass das automatische Starten/Herunterfahren von virtuellen Maschinen aktiviert ist. Siehe http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-5FE08AC7-4486-438E-AF88-80D6C7928810.html.

Aktualisieren von Host-Clustern von vCNS auf NSX in einer vCloud Director-Umgebung

Sie müssen Ihre Umgebung auf die Netzwerkvirtualisierung vorbereiten, indem Sie auf Clusterebene Netzwerkinfrastrukturkomponenten für jeden vCenter Server installieren. Dadurch wird die erforderliche Software auf allen Hosts im Cluster installiert und die virtuellen Leitungen werden in logische NSX-Switches umbenannt. Bei diesem Vorgang erhält jeder Host im Cluster ein Software-Update und wird dann neu gestartet.

Wenn in Ihrer Umgebung virtuelle Leitungen vorliegen, müssen Sie nach dem Upgrade auf NSX Manager Ihre Host-Cluster aktualisieren.

Es wird empfohlen, dass Sie Host-Cluster in einem Datencenterwartungsfenster aktualisieren.

Führen Sie während des Upgrades keine anderen Upgrades aus, stellen Sie keine Dienste oder Komponenten bereit und deinstallieren Sie keine Dienste oder Komponenten.

Bei der Installation oder Aktualisierung von NSX wird automatisch versucht, jeden Host in den Wartungsmodus zu versetzen und neu zu starten. In vCloud Director-Umgebungen ist dies nicht empfehlenswert.

Stattdessen sollten Sie die VIBs in jedem Cluster aktualisieren, jedoch ohne auf **Auflösen (Resolve)** zu klicken. Sie müssen, bevor Sie in den Wartungsmodus wechseln und neu starten, den Host in vCloud Director deaktivieren.

Hinweis In vCloud Networking and Security erstellte VTEPs verwenden DHCP oder manuell zugewiesene IP-Adressen und keine IP-Pools.

Vorgehensweise

1 Upgrade von VIBs auf Hosts in einer vCloud Director-Umgebung

   In einer vCloud Director-Umgebung müssen Sie vor dem Upgrade von VIBs auf den Clustern für DRS „Manuell“ festlegen. Andernfalls versucht NSX, die Hosts in den Wartungsmodus zu versetzen.

2 Manuelles Neustarten von Hosts nach einer VIB-Installation in einer vCloud Director-Umgebung

   Die Hosts müssen neu gestartet werden, damit die installierten NSX-VIBs wirksam werden können. Sie müssen die Hosts in vCloud Director deaktivieren, bevor Sie diese neu starten. Dadurch wird verhindert, dass vCloud Director die Hosts beim Neustart verwendet.

Upgrade von VIBs auf Hosts in einer vCloud Director-Umgebung

In einer vCloud Director-Umgebung müssen Sie vor dem Upgrade von VIBs auf den Clustern für DRS „Manuell“ festlegen. Andernfalls versucht NSX, die Hosts in den Wartungsmodus zu versetzen.

Voraussetzungen

- Stellen Sie sicher, dass vShield Manager auf NSX Manager aktualisiert wurde.
- Stellen Sie sicher, dass die Spalte „VXLAN“ der Registerkarte „Hostvorbereitung“ den Eintrag **Aktiviert (Enabled)** enthält.

- Stellen Sie sicher, dass die vollqualifizierten Domänennamen (FQDNs) all Ihrer Hosts aufgelöst werden können.
- Stellen Sie vor dem Starten des Upgrades sicher, dass DRS in Ihrer Umgebung funktioniert.
  - Stellen Sie sicher, dass DRS auf den Host-Clustern aktiviert ist.
  - Stellen Sie sicher, dass vMotion korrekt funktioniert.
  - Überprüfen Sie den Zustand der Hostverbindung mit vCenter.
  - Stellen Sie sicher, dass sich mindestens drei ESXi-Hosts in jedem Host-Cluster 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 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 Host-Clustern aktiviert ist.
  - Stellen Sie sicher, dass vMotion korrekt funktioniert.
  - Überprüfen Sie den Zustand der Hostverbindung mit vCenter.
  - Stellen Sie sicher, dass sich mindestens drei ESXi-Hosts in jedem Host-Cluster 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.

Vorgehensweise

1. In vSphere Web Client navigieren Sie zu **Home > Hosts und Cluster (Hosts and Clusters)**.
2. Legen Sie auf den Host-Clustern für DRS „Manuell“ fest. Wiederholen Sie diese Schritte für alle Cluster, auf denen vCloud Networking and Security installiert ist.

   Vorsicht DRS muss aktiviert bleiben. Eine Deaktivierung von DRS löscht Ihre Ressourcenpools und beschädigt Ihre vCloud Director-Installation.

   a. Wählen Sie einen Cluster aus und navigieren Sie dann zu **Verwalten (Manage) > Einstellungen (Settings) > vSphere-DRS (vSphere DRS)**.

   b. Achten Sie auf die Einstellung **DRS-Automation (DRS Automation)**. Diese werden Sie später ändern.

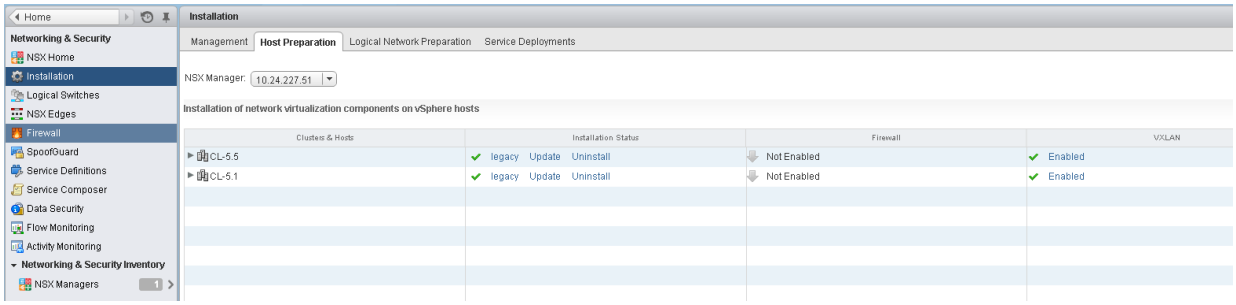
   c. Klicken Sie auf **Bearbeiten (Edit)**. Wählen Sie im Abschnitt **DRS-Automation (DRS Automation)** die Option **Manuell (Manual)** aus und klicken Sie auf **OK**.
3. Navigieren Sie zu **Home > Networking & Security > Installation**.

4 Klicken Sie auf die Registerkarte **Hostvorbereitung (Host Preparation)**.

Alle Cluster in Ihrer Infrastruktur werden angezeigt.

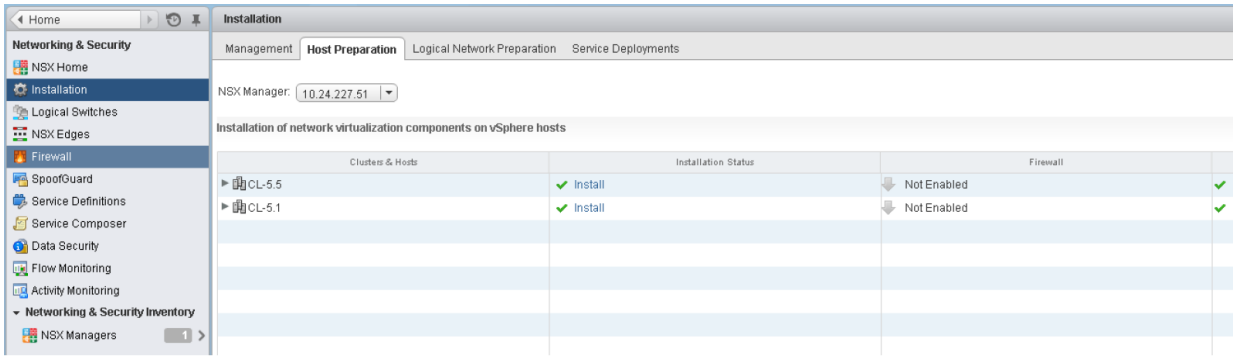
Wenn Sie virtuelle Leitungen in Ihrer 5.5-Umgebung hatten, zeigt die Spalte **Installationsstatus (Installation Status) Legacy**, **Aktualisieren (Update)** und **Deinstallieren (Uninstall)** an.

Abbildung 1-3. Der Installationsstatus zeigt „Aktualisieren“ an, wenn Sie virtuelle Leitungen in Ihrer 5.5-Umgebung haben



Wenn Sie keine virtuellen Leitungen in Ihrer 5.5-Umgebung hatten, zeigt die Spalte **Installationsstatus (Installation Status) Installieren (Install)** an.

Abbildung 1-4. Der Installationsstatus zeigt „Installieren“ an, wenn Sie virtuelle Leitungen in Ihrer 5.5-Umgebung haben



5 Klicken Sie für jeden Cluster in der Spalte „Installationsstatus“ auf **Aktualisieren (Update)** oder **Installieren (Install)**.

Jeder Host im Cluster erhält die neue logische Switch-Software.

Das Host-Upgrade initiiert eine Hostprüfung. Die alten VIBs werden entfernt (sie werden aber erst nach dem Neustart vollständig gelöscht). Neue VIBs werden auf der altboot-Partition installiert. Zum Anzeigen der neuen VIBs auf einem Host, der noch nicht neu gestartet wurde, können Sie den Befehl `esxcli software vib list --rebooting-image | grep esx` ausführen.

6 Überwachen Sie die Installation, bis **Nicht bereit (Not Ready)** für die Spalte **Installationsstatus (Installation Status)** angezeigt wird.

Klicken Sie nicht auf **Auflösen (Resolve)**.

7 Navigieren Sie zu **Home > Hosts und Cluster (Hosts and Clusters)**.

8 Machen Sie die DRS-Änderungen auf den Host-Clustern rückgängig. Wiederholen Sie diese Schritte für alle Cluster, auf denen NSX installiert ist.

   a Wählen Sie einen Cluster aus und navigieren Sie dann zu **Verwalten (Manage) > Einstellungen (Settings)**.

   b Wählen Sie **vSphere-DRS (vSphere DRS)** aus und klicken Sie auf **Bearbeiten (Edit)**. Im Abschnitt **DRS-Automation (DRS Automation)** wählen Sie Ihre ursprüngliche DRS-Einstellung aus und klicken Sie auf **OK**.

Weiter

Manuelles Neustarten von Hosts nach einer VIB-Installation in einer vCloud Director-Umgebung.

Manuelles Neustarten von Hosts nach einer VIB-Installation in einer vCloud Director-Umgebung

Die Hosts müssen neu gestartet werden, damit die installierten NSX-VIBs wirksam werden können. Sie müssen die Hosts in vCloud Director deaktivieren, bevor Sie diese neu starten. Dadurch wird verhindert, dass vCloud Director die Hosts beim Neustart verwendet.

Voraussetzungen

- Stellen Sie sicher, dass sich alle Hosts im Status **Nicht bereit (Not Ready)** befinden.
- Stellen Sie sicher, dass die Kapazität eines jeden vSphere-Clusters für die temporäre Ausführung ohne einen Host ausreicht.
- Stellen Sie sicher, dass DRS aktiviert und nicht auf „Manuell“ gesetzt ist.

Vorgehensweise

1 In vCloud Director deaktivieren Sie den Host.

   a Navigieren Sie zu **Verwalten und Überwachen (Manage & Monitor) > Hosts.**.

   b Klicken Sie einen Host mit der rechten Maustaste an und wählen Sie **Host deaktivieren (Disable Host)** aus.

2 In vSphere Web Client navigieren Sie zu **Home > Hosts und Cluster (Hosts and Clusters)**.

3 Klicken Sie mit der rechten Maustaste auf den in vCloud Director deaktivierten Host und wählen Sie **Wechseln in den Wartungsmodus (Enter Maintenance Mode)** aus. Im Dialogfeld „Wartungsmodus bestätigen“ wählen Sie **Ausgeschaltete und angehaltene virtuelle Maschinen auf andere Hosts im Cluster verschieben (Move powered-off and suspended virtual machines to other hosts in the cluster)** aus und klicken Sie auf **OK**.

4 Wenn nicht alle virtuellen Maschinen auf andere Hosts verschoben wurden, verschieben Sie diese manuell.

5 Wenn sich der Host im Wartungsmodus befindet, klicken Sie den Host mit der rechten Maustaste an und wählen Sie **Neu starten (Reboot)** aus. Geben Sie einen Grund für den Neustart ein und klicken Sie auf **OK**.

6 Wenn der Host wieder hochgefahren ist, klicken Sie den Host mit der rechten Maustaste an und wählen Sie **Wartungsmodus beenden (Exit Maintenance Mode)** aus.

7 In vCloud Director aktivieren Sie den Host.

   a Navigieren Sie zu **Verwalten und Überwachen (Manage & Monitor) > Hosts.**.

   b Klicken Sie den Host mit der rechten Maustaste an und wählen Sie **Host aktivieren (Enable Host)** aus.

8 Wenn der Host in vCloud Director aktiviert ist, wiederholen Sie diese Schritte für den nächsten Host.

Alle virtuellen Leitungen Ihrer 5.5-Infrastruktur wurden in logische NSX-Switches umbenannt, und die Spalte VXLAN zeigt **Aktiviert (Enabled)** an.

Aktiviert (Enabled)

Wenn der Cluster aktualisiert ist, wird in der Spalte **Installationsstatus (Installation Status)** die Softwareversion angezeigt, auf die Sie aktualisiert haben.

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 | grep esx` aus. Stellen Sie sicher, dass die folgenden VIBs auf die erwartete Version aktualisiert wurden.

- esx-vsip
- esx-vxlan

Hinweis In NSX 6.2 ist das „esx-dvfilter-switch-security“-VIB im „esx-vxlan“-VIB enthalten.

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.

Weiter

Wenn Sie einen NSX Controller-Cluster bereitgestellt haben, können Sie optional den Steuerungskomponenten-Modus ändern: Aktualisieren von Transportzonen und logischen Switches in einer vCloud Director-Umgebung.

Andernfalls finden Sie Erläuterungen unter Prüfen eines Upgrades von vShield Edge in einer vCloud Director-Umgebung

Aktualisieren von Transportzonen und logischen Switches in einer vCloud Director-Umgebung

Wenn Sie einen NSX Controller-Cluster bereitstellen, sind Sie für logische Netzwerke nicht mehr von Multicast abhängig. Sie können den Steuerungskomponenten-Modus in Ihren Transportzonen und logischen Switches für die Verwendung von Unicast oder Hybrid aktualisieren.

Die Änderung des Steuerungskomponenten-Modus und die Migration von vorhandenen logischen Switches hat keine Auswirkungen auf den Datenverkehr der Netzwerkdatenebene.

Vorgehensweise

1. In vSphere Web Client navigieren Sie zu **Home > Networking & Security > Installation > Vorbereitung des logischen Netzwerks (Logical Network Preparation) > Transportzonen (Transport Zones)**.
2. Wählen Sie Ihre Transportzone aus und klicken Sie auf **Aktionen (Actions) > Einstellungen bearbeiten (Edit Settings)**. Wählen Sie den gewünschten Replizierungs-Modus aus:
   - **Multicast**: Multicast-IP-Adressen auf dem physischen Netzwerk werden für die Steuerungskomponente verwendet. Dieser Modus wird nur empfohlen, wenn Sie Upgrades von älteren VXLAN-Bereitstellungen aus durchführen wollen. Erfordert PIM/IGMP im physischen Netzwerk.
   - **Unicast**: Die Steuerungskomponente wird von einem NSX Controller verwendet. Der komplette Unicast-Datenverkehr verwendet die optimierte Kopfendereplikation. Es sind keine Multicast-IP-Adressen oder bestimmte Netzwerkkonfigurationen erforderlich.
   - **Hybrid**: Lagert eine Replizierung des lokalen Datenverkehrs auf das physische Netzwerk aus (L2 Multicast). Erfordert IGMP-Snooping auf dem ersten Hop-Switch und Zugriff auf einen IGMP-Abfrager in jedem VTEP-Subnetz, aber keinen PIM. Der erste Hop-Switch steuert die Datenverkehrsreplizierung für das Subnetz.
3. Aktivieren Sie das Kontrollkästchen **Migrieren Sie vorhandene logische Switches auf den neuen Steuerungskomponenten-Modus (Migrate existing Logical Switches to the new control plane mode)** und klicken Sie auf **OK**.

Weiter

Prüfen eines Upgrades von vShield Edge in einer vCloud Director-Umgebung

Prüfen eines Upgrades von vShield Edge in einer vCloud Director-Umgebung

Ob ein Upgrade von vShield Edge durchgeführt muss, hängt von der Version von vCloud Director ab.

Wenn Sie vCloud Director mit einer Version vor 8.10 verwenden, ist kein Upgrade von vShield Edge erforderlich.

Dabei müssen Sie bei der Verwendung von vCloud Director 5.x die Konfiguration in der vCloud Director-Datenbank ändern, um zu verhindern, dass vCloud Director für die Edges bei der erneuten Bereitstellung ein Upgrade durchführt. Weitere Informationen dazu finden Sie unter Verhindern der erneuten Bereitstellung des Legacy vShield Edge in einer vCloud Director-Umgebung.

Ab der Version vCloud Director 8.10 wird NSX Edge 6.x unterstützt und Sie können für vShield Edge ein Upgrade auf NSX Edge 6.x durchführen. Siehe Upgrade von vShield Edge auf NSX Edge in einer vCloud Director-Umgebung

Verhindern der erneuten Bereitstellung des Legacy vShield Edge in einer vCloud Director-Umgebung

Wenn Sie vCloud Director 5.x verwenden, müssen Sie nach dem Upgrade auf NSX eine Datenbankänderung vornehmen, um zu verhindern, dass Legacy vShield Edge-Appliances als NSX Edge-Appliances bereitgestellt werden.

Beachten Sie, dass das Upgrade der Legacy Edge Services Gateways nicht auf VMware NSX 6.x durchgeführt werden darf, da dies die vCloud Director-Kompatibilität außer Kraft setzt. Mit vCloud Director 5.x wird das Upgrade für ein Edge auf vCloud Director durchgeführt, wenn ein Edge erneut bereitgestellt wird. Dieses Verhalten lässt sich vermeiden, wenn Sie vor der Migration auf vCloud Network and Security die nachfolgend aufgeführten Datenbankänderungen in vCloud Director vornehmen.

Weitere Informationen dazu finden Sie in den folgenden VMware Knowledgebase-Artikeln: http://kb.vmware.com/kb/2096351 und http://kb.vmware.com/kb/2108913.

Vorgehensweise

1 Melden Sie sich bei der vCloud Director-SQL Server-Datenbank an.

2 Fügen Sie diese Zeile der Konfigurationstabelle hinzu.

```
INSERT INTO config (cat, name, value, sortorder) VALUES ('vcloud','networking.edge_versi-
on_for_vsm6.2', '5.5', 0);
```

Hinweis Verwenden Sie `networking.edge_version_for_vsm6.1` für NSX 6.1 oder `networking.edge_version_for_vsm6.0` für NSX 6.0.

Upgrade von vShield Edge auf NSX Edge in einer vCloud Director-Umgebung

vCloud Director 8.10 unterstützt NSX Edge 6.x, sodass Sie ein Upgrade von vShield Edge auf NSX Edge durchführen können. Wenn Sie ein frühere Version von vCloud Director verwenden, wird NSX Edge 6.x nicht unterstützt, d. h., Sie können kein Upgrade für NSX Edge durchführen.

Sie können auf zweifache Weise ein Upgrade von vShield Edge auf NSX Edge durchführen: entweder mithilfe von NSX oder mit vCloud Director.

Erläuterungen zum Upgrade von Edge mithilfe von vCloud Director finden Sie unter „Upgrade von vCenter Server-Systemen, Hosts und NSX Edges“ im *vCloud DirectorInstallations- und Upgrade-Handbuch*.

Achtung Wenn Sie vCloud Director mit einer Version vor 8.10 verwenden, ist kein Upgrade von NSX Edge möglich.

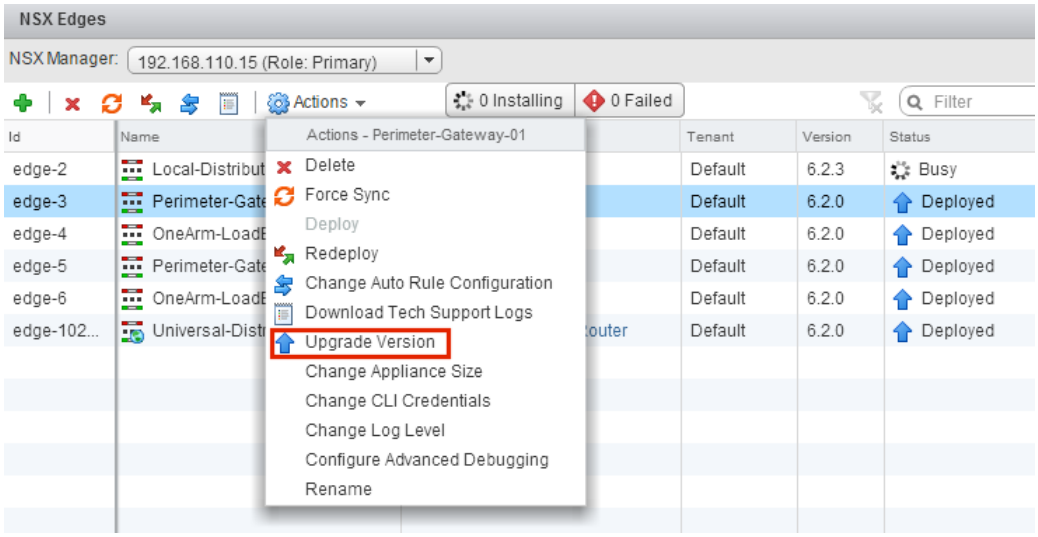
Voraussetzungen

- Stellen Sie sicher, dass vShield Manager auf NSX Manager aktualisiert wurde.
- Machen Sie sich während der Durchführung des Upgrades mit den operativen Auswirkungen des NSX Edge-Upgrades vertraut. Siehe Operative Auswirkungen von Upgrades für vCloud Networking and Security.
- 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.
  - Ab der Version NSX 6.2.3 werden, wenn für eine NSX Edge-Instanz mit Hochverfügbarkeit (HA, High Availability) ein Upgrade durchgeführt wird, 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.
  - Vor der Version NSX 6.2.3 wird, wenn für eine NSX Edge-Instanz mit Hochverfügbarkeit ein Upgrade durchgeführt wird, jeweils nur eine Ersetzungs-Appliance bereitgestellt, während die alten Appliances ersetzt werden. Es befinden sich dann während des Upgrades einer bestimmten NSX Edge drei NSX Edge-Appliances der geeigneten Größe im eingeschalteten Status. Nach dem Upgrade der NSX Edge-Instanz wird in der Regel die NSX Edge-Appliance mit dem HA-Index 0 aktiv.
- Das Durchführen eines Upgrades für einen NSX Edge mit Version 5.5 oder 6.0 mit aktiviertem L2 VPN wird nicht unterstützt. Sie müssen die L2 VPN-Konfiguration löschen, bevor Sie ein Upgrade durchführen. 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. Melden Sie sich beim vSphere Web Client an.
2. Klicken Sie auf **Networking & Security** und anschließend auf **NSX Edges**.

3 Wählen Sie für jede NSX Edge-Instanz die Option **Upgrade der Version durchführen (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.

In NSX Edge-Firewallregeln wird „sourcePort“ nicht unterstützt. Daher müssen die Regeln von vShield Edge Version 5.5, die „sourcePort“ enthalten, während des Upgrades wie folgt geändert werden.

- Wenn in der Regel keine applications-Einträge verwendet werden, wird ein Dienst mit den Einstellungen „protocol=any“, „port=any“ und „sourcePort=asDefinedInTheRule“ erstellt.
- Wenn die Regel Einträge für „applications“ oder „applicationsGroups“ aufweist, werden diese Gruppierungsobjekte dupliziert, indem ihnen „sourcePort“ hinzugefügt wird. Deswegen sind die in der Firewallregel verwendeten groupingObjectIds nach dem Upgrade verändert.

Benutzerfirewallregeln in NSX Edge 6.x generieren keine internen IPSets und applicationSets auf der Basis einer Eingabe von REST-APIs. Stattdessen werden sie in einem nicht formatierten Format beibehalten. Während des Upgrades werden mit den intern generierten IPSets und applicationSets Regeln mit nicht formatierten Daten erstellt. Die internen gruppierten Objekte sind nicht mehr in den Benutzerfirewallregeln enthalten

Weiter

Konfigurieren Sie bei Bedarf alle L2 VPN-Konfigurationen neu. Weitere Informationen finden Sie im *Installationshandbuch für NSX* unter „Überblick über L2 VPN“.

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
```

NSX-Upgrade

2

Dieses Kapitel behandelt die folgenden Themen:

- Vorbereiten des NSX-Upgrades
- Upgrade von NSX 6.1.x oder 6.2.x auf NSX 6.2.x
- Upgrade auf NSX 6.2.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. Weitere Informationen dazu finden Sie unter 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 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.

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

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

6 Erstellen Sie ein Tech-Support-Paket.

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

8 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.

9 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.

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

11 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 für eine frühere Version von NSX auf NSX 6.2.3 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.

Weitere Informationen finden Sie in der NSX-Lizenz-FAQ unter https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf

Operative Auswirkungen von NSX-Upgrades

Der NSX-Upgrade-Vorgang kann einige Zeit dauern, insbesondere dann, wenn Upgrades von ESXi-Hosts durchgeführt werden, da die Hosts neu gestartet werden müssen. Es ist wichtig, den Betriebszustand von NSX-Komponenten bei einem Upgrade zu verstehen, 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.

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

Deinstallieren Sie NSX Data Security entweder, weil Sie es nicht mehr verwenden oder weil Sie ein Upgrade von NSX Manager ausführen. NSX Data Security unterstützt kein direktes Upgrade. Bevor Sie NSX Manager aktualisieren, müssen Sie unbedingt zuerst NSX Data Security deinstallieren. Nach dem Upgrade können Sie es dann erneut installieren.

Ab der Version NSX 6.2.3 wird die NSX Data Security-Funktion eingestellt. In NSX 6.2.3 können Sie diese Funktion noch auf eigene Verantwortung weiter benutzen. In künftigen NSX-Versionen ist diese Funktion jedoch nicht mehr enthalten.

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 von NSX Manager-Daten

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

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.

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.

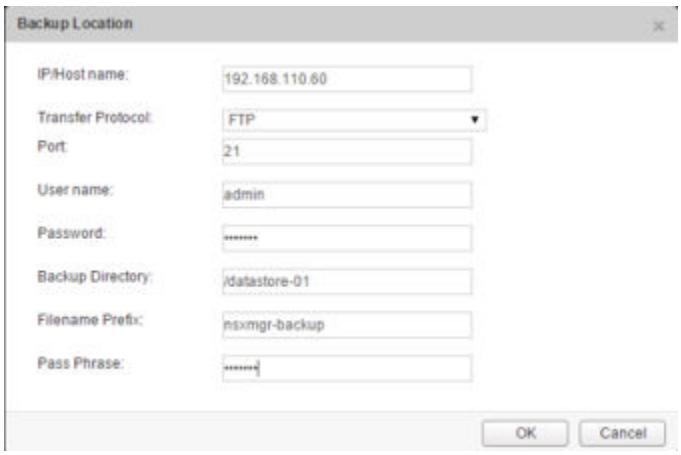
Dieser Text wird jedem Sicherungsdateinamen vorangestellt, um eine leichte Identifizierung auf dem Sicherungssystem zu ermöglichen. Wenn Sie beispielsweise **ppdb** als Präfix verwenden, lautet der Sicherungsname `ppdbHH_MM_SS_DayDDMonYYYY`.

g Geben Sie zum Sichern der Sicherungsdatei einen Kennwortsatz ein.

Sie benötigen diese Passphrase, um die Sicherung wiederherzustellen.

h Klicken Sie auf **OK**.

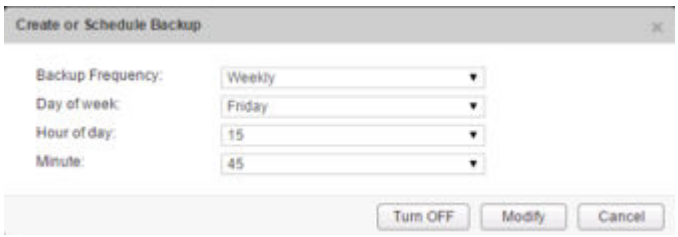
Beispiel:



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 offiziell nicht unterstützt. Es wird davon ausgegangen, dass der bestehende NSX Manager ausgefallen ist. Daher wird eine neue NSX Manager-Appliance bereitgestellt.

Gemäß Best Practice werden Screenshots der aktuellen Einstellungen der altern NSX Manager-Appliance erstellt bzw. diese Einstellungen notiert, damit sie zum Angeben von Informationen zu IP-Adressen und zum Sicherungsspeicherort für die neu bereitgestellte NSX Manager-Appliance verwendet werden können.

Vorgehensweise

1 Erstellen Sie Screenshots von allen Einstellungen auf der vorhandenen NSX Manager-Appliance bzw. notieren Sie sie.

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-Server-Einstellungen auf **Ändern (Change)** und fügen Sie die Einstellungen 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.

6 Aktivieren Sie im Abschnitt „Sicherungsverlauf“ das Kontrollkästchen für die wiederherzustellende Datensicherung und klicken Sie auf **Wiederherstellen (Restore)**.

Sichern von NSX Edges

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

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 das Symbol **NSX Edge erneut bereitstellen (Redeploy NSX Edge)** in vSphere Web Client).

Individuelle Sicherungen von NSX Edge werden nicht unterstützt.

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.

Diese Funktionen sind nur für vSphere Web Client 5.1 oder höher verfügbar. VDS-Einstellungen und Portgruppeneinstellungen werden im Rahmen des Importvorgangs importiert.

Best Practice ist, die VDS-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 von NSX 6.1.x oder 6.2.x auf NSX 6.2.x

Um ein Upgrade auf NSX 6.2.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

5 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 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.

Voraussetzungen

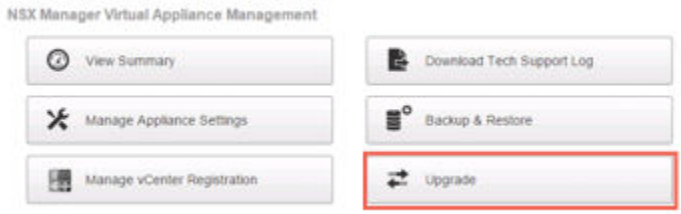
- Überprüfen Sie die NSX Manager-Nutzung des Dateisystems und führen Sie eine Bereinigung durch, wenn die Nutzung bei 100 Prozent liegt.
  a Melden Sie sich bei NSX Manager an und führen Sie `show filesystems` aus, um die /dev/sda2-Nutzung des Dateisystems anzuzeigen.
  b Wenn die Nutzung bei 100 Prozent 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.
- Vergrößern Sie den reservierten Arbeitsspeicher der virtuellen NSX Manager-Appliance vor dem Upgrade für NSX 6.2.x auf mindestens 16 GB.

  Siehe Systemvoraussetzungen für NSX.
- Wenn sich Data Security in Ihrer Umgebung befindet, deinstallieren Sie es, bevor Sie NSX Manager aktualisieren. Siehe Deinstallieren von NSX Data Security.
- Sichern Sie Ihre aktuelle Konfiguration und laden Sie die Protokolle des technischen Supports herunter, bevor Sie mit dem Upgrade beginnen. Siehe Sichern und Wiederherstellen von NSX.
- Laden Sie das NSX-Upgrade-Paket herunter und überprüfen Sie die MD5-Prüfsumme. Siehe 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. Siehe Operative Auswirkungen von NSX-Upgrades.

Vorgehensweise

1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.

2 Auf der Homepage von NSX Manager klicken Sie auf **Upgrade**.



3 Klicken Sie auf **Upgrade durchführen**, anschließend auf **Datei auswählen** und rufen Sie die Datei `VMware-NSX-Manager-upgrade-bundle-`*releaseNumber-NSXbuildNumber*`.tar.gz` auf. Klicken Sie auf **Fortsetzen**, 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**, 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 virtuelle NSX Manager-Appliance an und bestätigen Sie, dass der Upgrade-Zustand **Vollständig** lautet und die Version und Build-Nummer oben rechts mit denen des Upgrade-Pakets übereinstimmen, das Sie gerade installiert haben.

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. Siehe 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** 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.

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** mit der rechten Maustaste auf den Controller und wählen Sie **Stromversorgung > Zurücksetzen**.

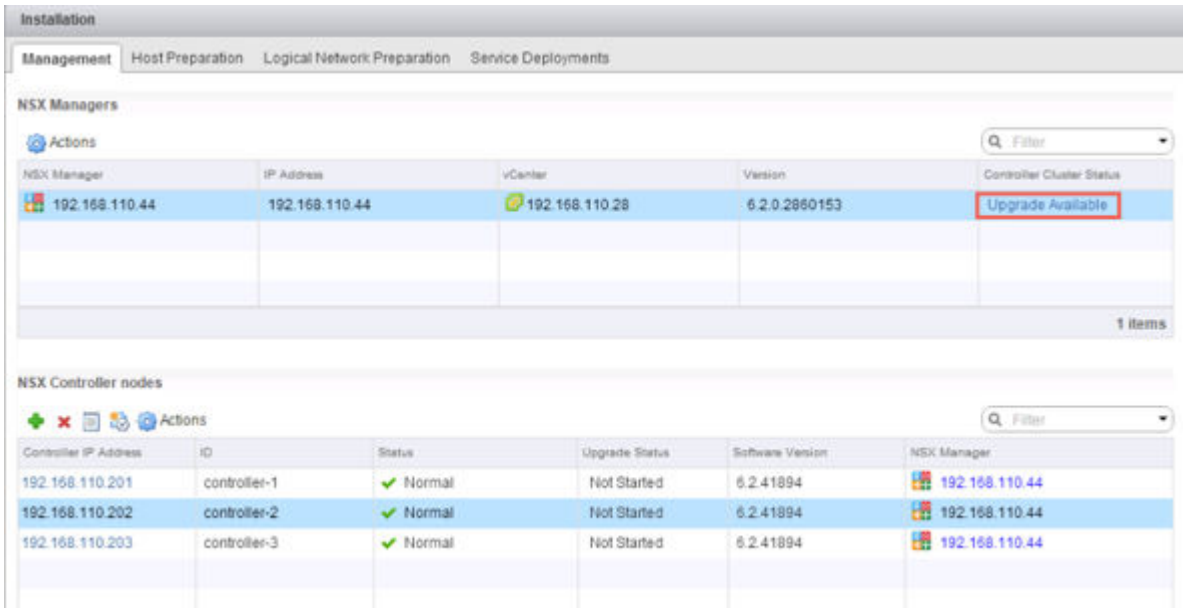
- Ein gültiger NSX Controller-Cluster enthält drei Controller-Knoten. Melden Sie sich bei den drei Controller-Knoten an und führen Sie den Befehl **show controller-cluster status** aus.

```
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. Siehe Operative Auswirkungen von NSX-Upgrades.

Vorgehensweise

- Navigieren Sie im vSphere Web Client zu **Startseite > Networking & Security > Installation**, wählen Sie die Registerkarte **Verwaltung** aus und klicken Sie auf **Upgrade verfügbar** in der Spalte **Status des Controller-Clusters**.



  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** im NSX Manager-Abschnitt zeigt den Upgrade-Status des Clusters an. Wenn das Upgrade beginnt, lautet der Status **Upgrade-Datei wird heruntergeladen**. Wenn die Upgrade-Datei auf alle Controller im Cluster heruntergeladen wurde, ändert sich der Status in **Vorgang läuft**. Wenn alle Controller im Cluster aktualisiert wurden, lautet der angezeigte Status **Vollständig** und diese Spalte wird nicht mehr angezeigt.
  - Die Spalte **Status** im Bereich der NSX Controller-Knoten zeigt den Status jedes Controllers an. Anfangs lautet der Status **Normal**. Wenn die Controller-Dienste heruntergefahren werden und der Controller neu gestartet wird, ändert sich der Status in **Getrennt**. Nach dem Abschluss des Upgrades für diesen Controller lautet der Status wieder **Normal**.
  - Die Spalte **Upgrade-Status** im Bereich der NSX Controller-Knoten zeigt den Upgrade-Status für jeden Controller an. Der Status lautet anfangs **Upgrade-Datei wird heruntergeladen**, dann **Upgrade läuft** und danach **Neustarten**. Nach Abschluss des Controller-Upgrades lautet der Status **Aktualisiert**.

Wenn das Upgrade abgeschlossen ist, wird in der Spalte **Softwareversion** im Bereich der NSX Controller-Knoten für jeden Controller **6.2.***buildNumber* angezeigt. Führen Sie den Befehl **show controller-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** der Status **Fehlgeschlagen** angezeigt. Klicken Sie im NSX Manager-Abschnitt erneut auf **Upgrade verfügbar**, 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.

Weiter

Führen Sie ein Upgrade der Host-Cluster durch.

Aktualisieren von Hostclustern

Nach dem Upgrade von NSX Manager und der NSX Controller auf Version 6.2.x können Sie die entsprechenden Cluster in Ihrer Umgebung aktualisieren. Bei diesem Vorgang erhält jeder Host im Cluster ein Software-Update und wird dann neu gestartet.

Bei einem Upgrade der Hostcluster werden die NSX-VIBs esx-vsip und esx-vxlan aktualisiert.

- Wenn Sie das Upgrade von einer NSX-Version vor NSX 6.2 ausführen, weisen die vorbereiteten Hosts einen zusätzlichen VIB auf, „esx-dvfilter-switch-security“. In NSX 6.2 und neueren Versionen ist „esx-dvfilter-switch-security“ im „esx-vxlan“-VIB enthalten.
- Wenn Sie ein Upgrade von NSX 6.2.x ausführen, wobei die Version NSX 6.2.4 oder höher lautet, weisen die vorbereiteten Hosts den zusätzlichen „esx-vdpi“-VIB auf.

Voraussetzungen

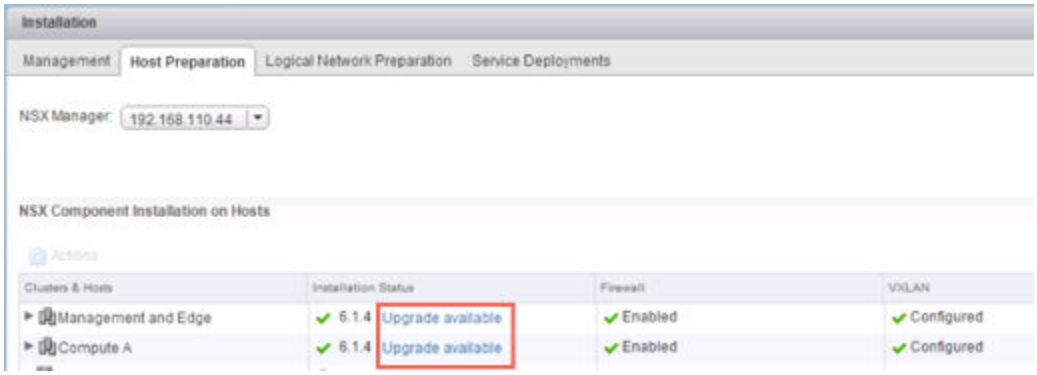
- Stellen Sie sicher, dass die vollqualifizierten Domänennamen (FQDNs) all Ihrer Hosts aufgelöst werden können.

- Melden Sie sich bei einem der Hosts im Cluster an und führen Sie den Befehl `esxcli software vib list` aus. Beachten Sie die aktuelle Version folgender VIBs:
  - esx-vsip
  - esx-vxlan
- Führen Sie ein Upgrade von NSX Manager und des NSX Controller-Clusters durch.
- 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.
- 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 **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.

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 | grep esx` aus. Stellen Sie sicher, dass die folgenden VIBs auf die erwartete Version aktualisiert wurden.

- esx-vsip
- esx-vxlan

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

Ändern des VXLAN-Ports

Ändern des VXLAN-Ports

Sie können den für den VXLAN-Datenverkehr verwendeten Port ändern.

In NSX 6.2.3 und höher lautet der von IANA zugewiesene Standard-VXLAN-Port 4789. Vor NSX 6.2.3 lautete die Standard-VXLAN-UDP-Portnummer 8472.

Alle neuen NSX-Installationen verwenden jetzt den UDP-Port 4789 für VXLAN.

Wenn Sie von NSX 6.2.2 oder früher ein Upgrade auf NSX 6.2.3 oder höher durchführen und für Ihre Installation vor dem Upgrade die alte Standardnummer (8472) oder eine benutzerdefinierte Portnummer verwendet wurde (z. B. 8888), wird dieser Port so lange nach dem Upgrade weiter benutzt, bis Sie diesen ändern.

Wenn die Installation, für die ein Upgrade durchgeführt wurde, Hardware-VTEP-Gateways („ToR-Gateways“) verwendet oder verwenden soll, müssen Sie zum VXLAN-Port 4789 wechseln.

Cross-vCenter NSX erfordert nicht die Verwendung von 4789 für den VXLAN-Port. Allerdings muss für alle Hosts in einer Cross-vCenter NSX-Umgebung die Verwendung desselben VXLAN-Ports konfiguriert werden. Dadurch wird bei einem Wechsel zu Port 4789 sichergestellt, dass neue der Cross-vCenter NSX-Umgebung hinzugefügte NSX-Installationen denselben Port wie vorhandene NSX-Bereitstellungen verwenden.

Die Änderung des VXLAN-Ports erfolgt in drei Stufen und führt nicht zur Unterbrechung des VXLAN-Datenverkehrs.

1. NSX Manager konfiguriert alle Hosts, die auf VXLAN-Datenverkehr sowohl auf den alten wie auf den neuen Ports überwacht werden sollen. Hosts senden weiterhin VXLAN-Datenverkehr auf den alten Port.
2. NSX Manager konfiguriert alle Hosts für das Senden des Datenverkehrs auf den neuen Port.
3. NSX Manager konfiguriert alle Hosts für das Beenden der Überwachung auf dem alten Port. Der gesamte Datenverkehr wird auf dem neuen Port gesendet und empfangen.

In einer Cross-vCenter NSX-Umgebung müssen Sie die Änderung des Ports auf dem primären NSX Manager initiieren. In jeder Phase werden die Konfigurationsänderungen auf allen Hosts in der Cross-vCenter NSX-Umgebung durchgeführt, bevor mit der nächsten Phase fortgesetzt wird.

Voraussetzungen

- Stellen Sie sicher, dass der Port, den Sie für VXLAN verwenden möchten, nicht durch eine Firewall blockiert ist.
- Stellen Sie sicher, dass die Hostvorbereitung nicht zur gleichen Zeit ausgeführt wird wie die Änderung des VXLAN-Ports.

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 **Vorbereitung des logischen Netzwerks (Logical Network Preparation)** und dann auf **VXLAN-Transport (VXLAN Transport)**.
4. Klicken Sie im VXLAN-Portbereich auf die Schaltfläche **Ändern (Change)**. Geben Sie den Port ein, zu dem Sie wechseln möchten. 4789 ist der Port, der von IANA für VXLAN zugewiesen wurde.

   Es dauert einen Moment, bis die Portänderung an alle Hosts übermittelt wird.
5. (Optional) Sie können den Fortschritt der Portänderung mit der API-Anforderung `GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus` überprüfen.

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
    <prevPort>8472</prevPort>
    <targetPort>4789</targetPort>
    <taskPhase>PHASE_TWO</taskPhase>
    <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

...

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
    <prevPort>8472</prevPort>
    <targetPort>4789</targetPort>
    <taskPhase>FINISHED</taskPhase>
    <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

Weiter

Upgrade von NSX Edge

Upgrade von NSX Edge

NSX Edges können unabhängig vom NSX Controller-Cluster oder von Host-Cluster-Upgrades aktualisiert werden. Sie können auch dann ein Upgrade für ein NSX Edge durchführen, wenn Sie den NSX Controller-Cluster oder die Host-Cluster noch nicht aktualisiert haben.

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.

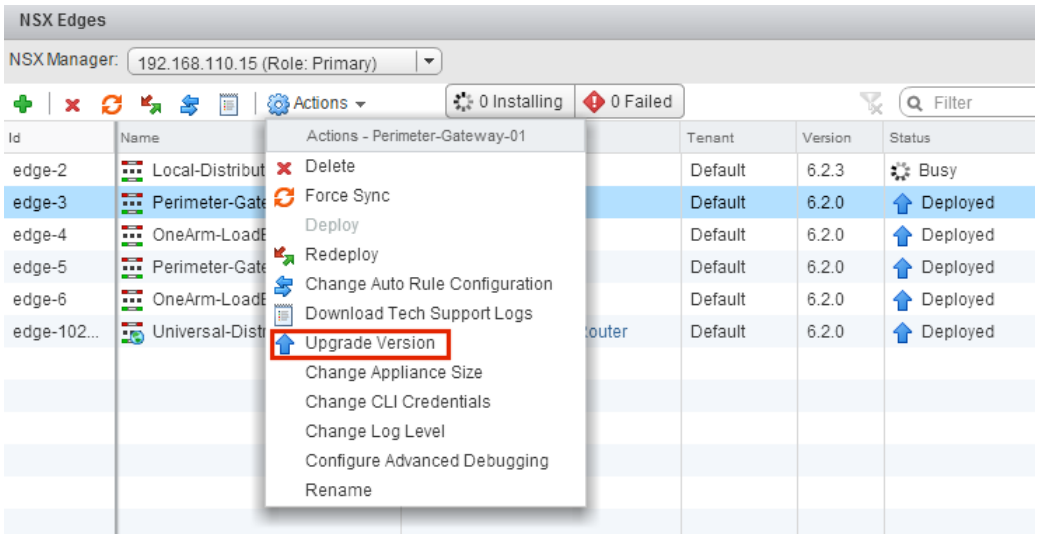
Voraussetzungen

- Vergewissern Sie sich, dass NSX Manager auf die Version 6.2.x aktualisiert wurde.
- 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.
  - Ab der Version NSX 6.2.3 werden, wenn für eine NSX Edge-Instanz mit Hochverfügbarkeit (HA, High Availability) ein Upgrade durchgeführt wird, 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.
  - Vor der Version NSX 6.2.3 wird, wenn für eine NSX Edge-Instanz mit Hochverfügbarkeit ein Upgrade durchgeführt wird, jeweils nur eine Ersetzungs-Appliance bereitgestellt, während die alten Appliances ersetzt werden. Es befinden sich dann während des Upgrades einer bestimmten NSX Edge drei NSX Edge-Appliances der geeigneten Größe im eingeschalteten Status. Nach dem Upgrade der NSX Edge-Instanz wird in der Regel die NSX Edge-Appliance mit dem HA-Index 0 aktiv.
- Machen Sie sich während der Durchführung des Upgrades mit den operativen Auswirkungen des NSX Edge-Upgrades vertraut. Weitere Informationen dazu finden Sie unter Operative Auswirkungen von NSX-Upgrades.

- Das Durchführen eines Upgrades für einen NSX Edge mit Version 5.5 oder 6.0 mit aktiviertem L2 VPN wird nicht unterstützt. Sie müssen die L2 VPN-Konfiguration löschen, bevor Sie ein Upgrade durchführen. Nach dem Upgrade können Sie L2 VPN neu konfigurieren. Weitere Informationen finden Sie im Dokument *Installationshandbuch für NSX* unter „Überblick über L2 VPN“.
- Wenn Sie ein Upgrade von NSX 6.2.x auf NSX 6.2.3 durchführen und ein Load Balancer konfiguriert wurde, finden Sie im folgenden Knowledgebase-Artikel Informationen zur Vermeidung von Upgrade-Problemen: https://kb.vmware.com/kb/2145887

Vorgehensweise

1. Melden Sie sich beim vSphere Web Client an.
2. Klicken Sie auf **Networking & Security** und anschließend auf **NSX Edges**.
3. Wählen Sie für jede NSX Edge-Instanz die Option **Upgrade der Version durchführen (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

Konfigurieren Sie bei Bedarf alle L2 VPN-Konfigurationen neu. Weitere Informationen finden Sie im *Installationshandbuch für NSX* unter „Überblick über L2 VPN“.

Upgrade von Guest Introspection

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

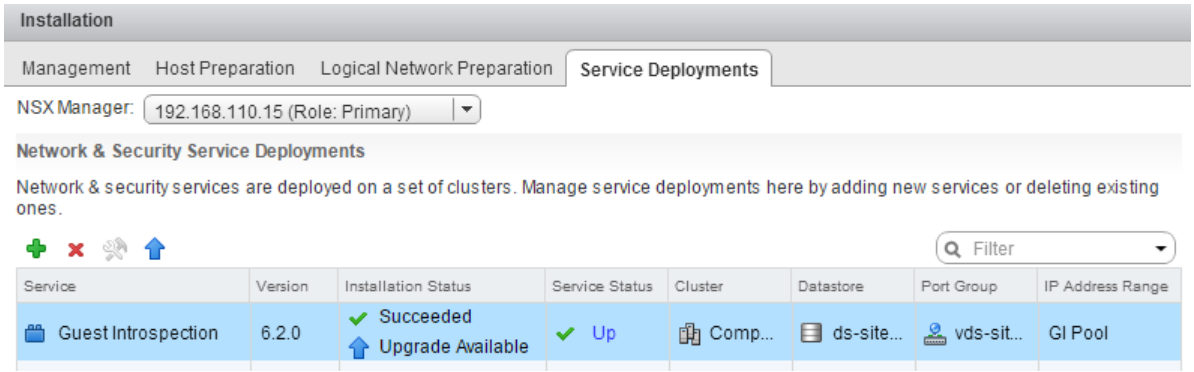
Hinweis Für die Guest Introspection-Dienst-VMs kann ein Upgrade über vSphere Web Client durchgeführt werden. Sie müssen die Dienst-VM für deren Upgrade nach dem Upgrade von NSX Manager nicht löschen. Wenn Sie die Dienst-VM löschen, wird für den Dienststatus `Fehlgeschlagen` angezeigt, da die Agenten-VM 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

Voraussetzung dafür ist das Upgrade von NSX Manager, Controllern, vorbereiteten Host-Clustern und NSX Edges auf Version 6.2.x.

Vorgehensweise

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

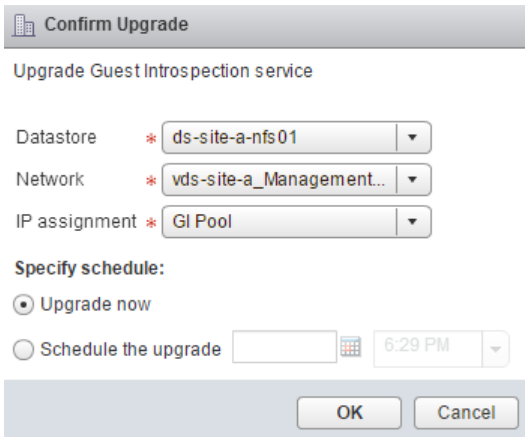


Die Spalte **Installationsstatus (Installation Status)** enthält den Wert **Upgrade verfügbar (Upgrade available)**.

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, wie virtuelle Sicherheits-Appliances von VMware-Partnern 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.

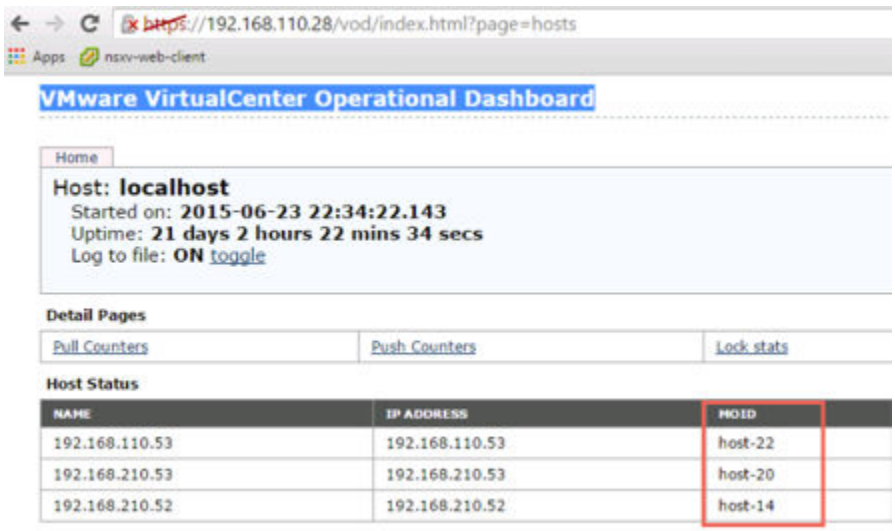
NSX Data Security

Sie sollten NSX Data Security vor dem Upgrade von NSX deinstallieren und nach Abschluss des NSX-Upgrades neu installieren. Wenn Sie NSX bereits aktualisiert haben, ohne NSX Data Security vorher zu deinstallieren, müssen Sie Data Security mithilfe eines REST-API-Aufrufs deinstallieren.

Geben Sie den folgenden API-Aufruf aus:

```
DELETE https://<nsx-manager-ip>/api/1.0/vshield/<host-id>/vsds
```

Die Host-ID ist die MOID des ESXi-Hosts. Um die MOID abzurufen, öffnen Sie das VMware VirtualCenter Operational Dashboard: https://<vcenter-ip>/vod/index.html?page=hosts.



Für den ESXi-Host mit der MOID „host-22“ auf vCenter Server 192.168.110.28 würde der API-Aufruf folgendes Format aufweisen:

```
DELETE https://192.168.110.28/api/1.0/vshield/host-22/vsds
```

Stellen Sie sicher, dass Sie den API-Aufruf auf allen Ihren ESXi-Hosts ausführen.

Nach der Deinstallation von Data Security können Sie die neue Version installieren. Weitere Informationen dazu finden Sie unter Installieren von NSX Data Security.

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 6.2.x der SSL VPN-Clients. Diese „Installieren des SSL-Clients auf der Remote-Site“ im *Administratorhandbuch für NSX*.

NSX L2 VPN

Das Durchführen eines Upgrades für NSX Edge wird nicht unterstützt, wenn Sie L2 VPN auf einem NSX Edge mit Version 5.5.x oder 6.0.x installiert haben. Alle L2 VPN-Konfigurationen müssen vor dem Upgrade von NSX Edge gelöscht werden.

Installieren von NSX Data Security

Hinweis Ab der Version NSX 6.2.3 wird die NSX Data Security-Funktion eingestellt. In NSX 6.2.3 können Sie diese Funktion noch auf eigene Verantwortung weiter benutzen. In künftigen NSX-Versionen ist diese Funktion jedoch nicht mehr enthalten.

Voraussetzungen

NSX Guest Introspection muss auf dem Cluster installiert sein, auf dem Sie Data Security installieren.

Wenn Sie der VM des Data Security-Diensts eine IP-Adresse aus einem IP-Pool zuweisen möchten, erstellen Sie den IP-Pool, bevor Sie Data Security installieren. Siehe „Gruppieren von Objekten“ im *Administratorhandbuch für NSX*.

Vorgehensweise

1. Klicken Sie auf der Registerkarte **Installation** auf **Dienstbereitstellungen (Service Deployments)**.
2. Klicken Sie auf das Symbol **Neue Dienstbereitstellung (New Service Deployment)** ( ).
3. Wählen Sie im Dialogfeld „Netzwerk- und Sicherheitsdienste bereitstellen“ **Data Security** und klicken Sie auf **Weiter (Next)**.
4. Wählen Sie in **Zeitplan angeben (Specify schedule)** (unten im Dialogfeld) **Jetzt bereitstellen (Deploy now)**, um Data Security bereitzustellen, sobald es installiert ist, oder wählen Sie ein Datum und eine Uhrzeit für die Bereitstellung aus.
5. Klicken Sie auf **Weiter (Next)**.
6. Wählen Sie das Datencenter und die Cluster dort aus, wo Sie Data Security installieren wollen, und klicken Sie auf **Weiter (Next)**.
7. Wählen Sie auf der Seite „Speicher- und Verwaltungsnetzwerk auswählen“ den Datenspeicher aus, auf dem Sie den VM-Speicher für den Dienst hinzufügen möchten, oder wählen Sie die Option **Angegeben auf dem Host (Specified on host)** aus.

   Der ausgewählte Datenspeicher muss auf allen Hosts im ausgewählten Cluster verfügbar sein.

   Wenn Sie **Angegeben auf dem Host (Specified on host)** ausgewählt haben, muss der Datenspeicher für den ESX-Host in den **Agent-VM-Einstellungen (AgentVM Settings)** des Hosts angegeben werden, bevor dieser zum Cluster hinzugefügt wird. Weitere Informationen hierzu finden Sie in der *vSphere-API/SDK-Dokumentation*.

8 Wählen Sie die verteilte virtuelle Portgruppe aus, in der die Verwaltungsschnittstelle gehostet werden soll. Diese Portgruppe muss in der Lage sein, die Portgruppe des NSX Managers zu erreichen.

   Wenn der Datenspeicher auf **Angegeben auf dem Host (Specified on host)** festgelegt ist, muss das zu verwendende Netzwerk in der Eigenschaft **agentVmNetwork** jedes Hosts im Cluster angegeben werden. Weitere Informationen hierzu finden Sie in der *vSphere-API/SDK-Dokumentation*.

   Die Eigenschaft **agentVmNetwork** muss für alle Hosts, die Sie zum Cluster hinzufügen möchten, vorher festgelegt werden.

   Die ausgewählte Portgruppe muss auf allen Hosts im ausgewählten Cluster verfügbar sein.

9 Wählen Sie unter „IP-Zuweisungen“ eine der folgenden Optionen aus:

Option	Zweck
DHCP	Weisen Sie der VM des Data Security-Diensts eine IP-Adresse über Dynamic Host Configuration Protocol (DHCP) zu.
Einen IP-Pool	Weisen Sie der VM des Data Security-Diensts eine IP-Adresse aus dem ausgewählten IP-Pool zu.

   Beachten Sie, dass statische IP-Adressen nicht unterstützt werden.

10 Klicken Sie auf der Seite „Bereit zum Abschließen“ auf **Weiter (Next)** und anschließend auf **Beenden (Finish)**.

11 Überwachen Sie die Bereitstellung, bis **Erfolg (Succeeded)** für die Spalte **Installationsstatus (Installation Status)** angezeigt wird.

12 Wenn **Fehlgeschlagen (Failed)** für die Spalte **Installationsstatus (Installation Status)** angezeigt wird, klicken Sie auf das Symbol neben „Fehlgeschlagen“. Es werden alle Bereitstellungsfehler angezeigt. Klicken Sie auf **Auflösen (Resolve)**, um die Fehler zu beheben. In einigen Fällen werden beim Auflösen der Fehler zusätzliche Fehlermeldungen angezeigt. Führen Sie die nötige(n) Aktion(en) aus und klicken Sie wieder auf **Auflösen (Resolve)**.

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 6.2.x mit Cross-vCenter NSX

Um in einer Cross-vCenter-Umgebung ein Upgrade auf NSX 6.2.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.

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.

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.

Voraussetzungen

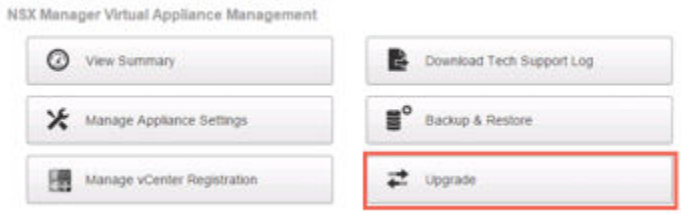
- Überprüfen Sie die NSX Manager-Nutzung des Dateisystems und führen Sie eine Bereinigung durch, wenn die Nutzung bei 100 Prozent liegt.
  a Melden Sie sich bei NSX Manager an und führen Sie `show filesystems` aus, um die /dev/sda2-Nutzung des Dateisystems anzuzeigen.
  b Wenn die Nutzung bei 100 Prozent 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.
- Vergrößern Sie den reservierten Arbeitsspeicher der virtuellen NSX Manager-Appliance vor dem Upgrade für NSX 6.2.x auf mindestens 16 GB.

  Siehe Systemvoraussetzungen für NSX.
- Wenn sich Data Security in Ihrer Umgebung befindet, deinstallieren Sie es, bevor Sie NSX Manager aktualisieren. Siehe Deinstallieren von NSX Data Security.
- Sichern Sie Ihre aktuelle Konfiguration und laden Sie die Protokolle des technischen Supports herunter, bevor Sie mit dem Upgrade beginnen. Siehe Sichern und Wiederherstellen von NSX.
- Laden Sie das NSX-Upgrade-Paket herunter und überprüfen Sie die MD5-Prüfsumme. Siehe 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. Siehe Operative Auswirkungen von NSX-Upgrades.

Vorgehensweise

1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.

2 Auf der Homepage von NSX Manager klicken Sie auf **Upgrade**.



3 Klicken Sie auf **Upgrade durchführen**, anschließend auf **Datei auswählen** und rufen Sie die Datei `VMware-NSX-Manager-upgrade-bundle-`*releaseNumber-NSXbuildNumber*`.tar.gz` auf. Klicken Sie auf **Fortsetzen**, 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**, 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 virtuelle NSX Manager-Appliance an und bestätigen Sie, dass der Upgrade-Zustand **Vollständig** lautet und die Version und Build-Nummer oben rechts mit denen des Upgrade-Pakets übereinstimmen, das Sie gerade installiert haben.

Wenn Sie während des Upgrades beim vSphere Web Client angemeldet sind, werden auf der Seite **Networking & 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. Siehe 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.

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 /dev/sda2-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.

- Vergrößern Sie den reservierten Arbeitsspeicher der virtuellen NSX Manager-Appliance vor dem Upgrade für NSX 6.2.x auf mindestens 16 GB.

  Siehe Systemvoraussetzungen für NSX.

- Wenn sich Data Security in Ihrer Umgebung befindet, deinstallieren Sie es, bevor Sie NSX Manager aktualisieren. Siehe Deinstallieren von NSX Data Security.
- Sichern Sie Ihre aktuelle Konfiguration und laden Sie die Protokolle des technischen Supports herunter, bevor Sie mit dem Upgrade beginnen. Siehe Sichern und Wiederherstellen von NSX.
- Laden Sie das NSX-Upgrade-Paket herunter und überprüfen Sie die MD5-Prüfsumme. Siehe 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. Siehe Operative Auswirkungen von NSX-Upgrades.

Vorgehensweise

1 Klicken Sie auf **Upgrade durchführen**, anschließend auf **Datei auswählen** und rufen Sie die Datei `VMware-NSX-Manager-upgrade-bundle-`*releaseNumber-NSXbuildNumber*`.tar.gz` auf. Klicken Sie auf **Fortsetzen**, um das Hochladen zu starten.

   Der Upload-Status wird im Browserfenster angezeigt.

2 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**, 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.

3 Melden Sie sich erneut bei der virtuelle NSX Manager-Appliance an und bestätigen Sie, dass der Upgrade-Zustand **Vollständig** lautet und die Version und Build-Nummer oben rechts mit denen des Upgrade-Pakets übereinstimmen, das Sie gerade installiert haben.

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. Siehe 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** 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.

Voraussetzungen

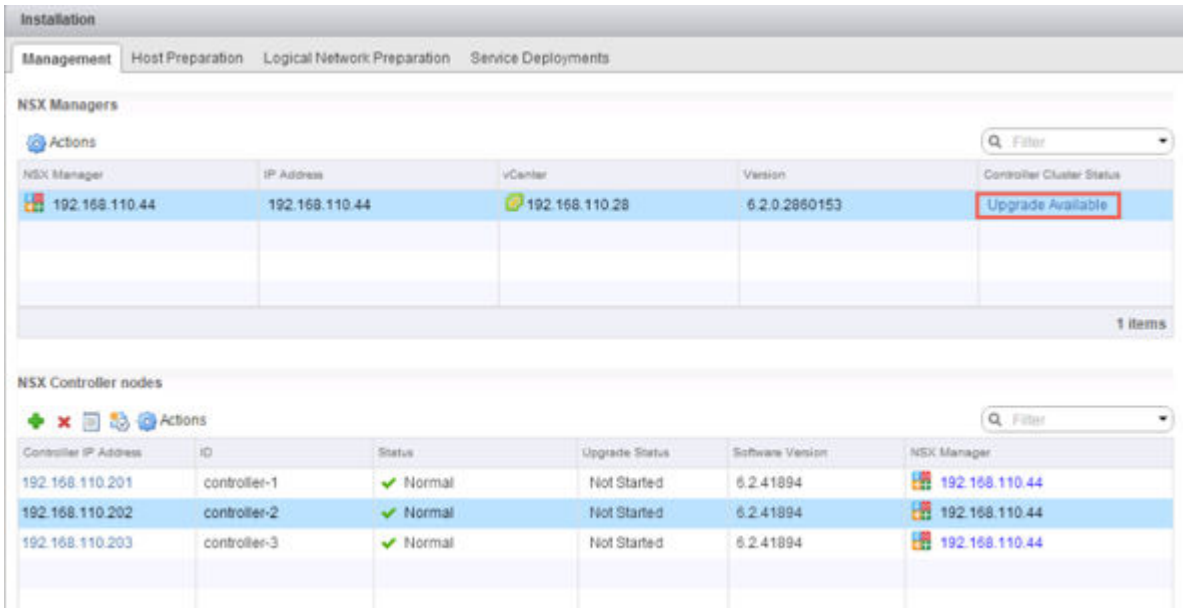
- Stellen Sie sicher, dass sich alle Controller im normalen Zustand befinden. Ein Upgrade ist nicht möglich, wenn sich ein oder mehrere Controller im Zustand „Getrennt“ befinden. Um einen getrennten Controller neu zu verbinden, versuchen Sie, die virtuelle Controller-Appliance zurückzusetzen. Klicken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

Vorgehensweise

- Navigieren Sie im vSphere Web Client zu **Startseite > Networking & Security > Installation**, wählen Sie die Registerkarte **Verwaltung** aus und klicken Sie auf **Upgrade verfügbar** in der Spalte **Status des Controller-Clusters**.



  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** im NSX Manager-Abschnitt zeigt den Upgrade-Status des Clusters an. Wenn das Upgrade beginnt, lautet der Status **Upgrade-Datei wird heruntergeladen**. Wenn die Upgrade-Datei auf alle Controller im Cluster heruntergeladen wurde, ändert sich der Status in **Vorgang läuft**. Wenn alle Controller im Cluster aktualisiert wurden, lautet der angezeigte Status **Vollständig** und diese Spalte wird nicht mehr angezeigt.
  - Die Spalte **Status** im Bereich der NSX Controller-Knoten zeigt den Status jedes Controllers an. Anfangs lautet der Status **Normal**. Wenn die Controller-Dienste heruntergefahren werden und der Controller neu gestartet wird, ändert sich der Status in **Getrennt**. Nach dem Abschluss des Upgrades für diesen Controller lautet der Status wieder **Normal**.
  - Die Spalte **Upgrade-Status** im Bereich der NSX Controller-Knoten zeigt den Upgrade-Status für jeden Controller an. Der Status lautet anfangs **Upgrade-Datei wird heruntergeladen**, dann **Upgrade läuft** und danach **Neustarten**. Nach Abschluss des Controller-Upgrades lautet der Status **Aktualisiert**.

Wenn das Upgrade abgeschlossen ist, wird in der Spalte **Softwareversion** im Bereich der NSX Controller-Knoten für jeden Controller **6.2.***buildNumber* angezeigt. Führen Sie den Befehl **show controller-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** der Status **Fehlgeschlagen** angezeigt. Klicken Sie im NSX Manager-Abschnitt erneut auf **Upgrade verfügbar**, 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.

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 auf NSX 6.2.x müssen Sie alle Host-Cluster in der Cross-vCenter NSX-Umgebung aktualisieren. Bei diesem Vorgang erhält jeder Host im Cluster ein Software-Update und wird dann neu gestartet.

Bei einem Upgrade der Hostcluster werden die NSX-VIBs esx-vsip und esx-vxlan aktualisiert.

- Wenn Sie das Upgrade von einer NSX-Version vor NSX 6.2 ausführen, weisen die vorbereiteten Hosts einen zusätzlichen VIB auf, „esx-dvfilter-switch-security“. In NSX 6.2 und neueren Versionen ist „esx-dvfilter-switch-security“ im „esx-vxlan“-VIB enthalten.
- Wenn Sie ein Upgrade von NSX 6.2.x ausführen, wobei die Version NSX 6.2.4 oder höher lautet, weisen die vorbereiteten Hosts den zusätzlichen „esx-vdpi“-VIB auf.

Voraussetzungen

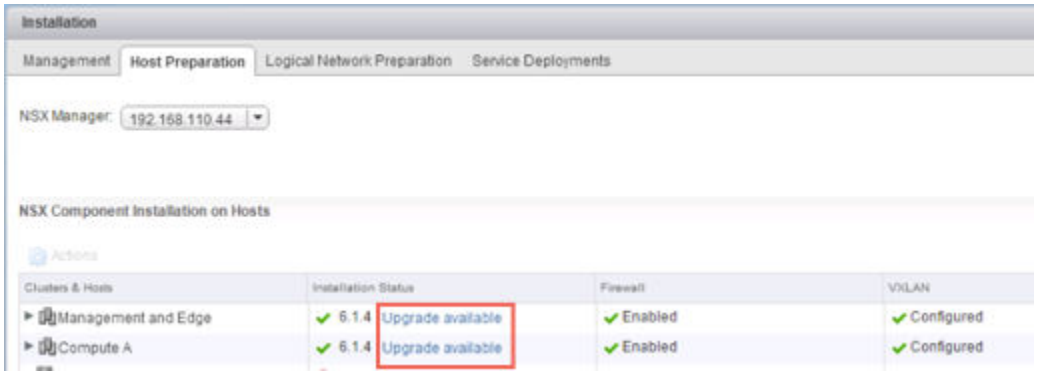
- Stellen Sie sicher, dass die vollqualifizierten Domänennamen (FQDNs) all Ihrer Hosts aufgelöst werden können.

- Melden Sie sich bei einem der Hosts im Cluster an und führen Sie den Befehl `esxcli software vib list` aus. Beachten Sie die aktuelle Version folgender VIBs:
  - esx-vsip
  - esx-vxlan
- Führen Sie ein Upgrade von NSX Manager und des NSX Controller-Clusters durch.
- 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.
- 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 **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.

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 | grep esx` aus. Stellen Sie sicher, dass die folgenden VIBs auf die erwartete Version aktualisiert wurden.

- esx-vsip
- esx-vxlan

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*.

Ändern des VXLAN-Ports in Cross-vCenter NSX

Sie können den für den VXLAN-Datenverkehr verwendeten Port ändern.

In NSX 6.2.3 und höher lautet der von IANA zugewiesene Standard-VXLAN-Port 4789. Vor NSX 6.2.3 lautete die Standard-VXLAN-UDP-Portnummer 8472.

Alle neuen NSX-Installationen verwenden jetzt den UDP-Port 4789 für VXLAN.

Wenn Sie von NSX 6.2.2 oder früher ein Upgrade auf NSX 6.2.3 oder höher durchführen und für Ihre Installation vor dem Upgrade die alte Standardnummer (8472) oder eine benutzerdefinierte Portnummer verwendet wurde (z. B. 8888), wird dieser Port so lange nach dem Upgrade weiter benutzt, bis Sie diesen ändern.

Wenn die Installation, für die ein Upgrade durchgeführt wurde, Hardware-VTEP-Gateways („ToR-Gateways“) verwendet oder verwenden soll, müssen Sie zum VXLAN-Port 4789 wechseln.

Cross-vCenter NSX erfordert nicht die Verwendung von 4789 für den VXLAN-Port. Allerdings muss für alle Hosts in einer Cross-vCenter NSX-Umgebung die Verwendung desselben VXLAN-Ports konfiguriert werden. Dadurch wird bei einem Wechsel zu Port 4789 sichergestellt, dass neue der Cross-vCenter NSX-Umgebung hinzugefügte NSX-Installationen denselben Port wie vorhandene NSX-Bereitstellungen verwenden.

Die Änderung des VXLAN-Ports erfolgt in drei Stufen und führt nicht zur Unterbrechung des VXLAN-Datenverkehrs.

1 NSX Manager konfiguriert alle Hosts, die auf VXLAN-Datenverkehr sowohl auf den alten wie auf den neuen Ports überwacht werden sollen. Hosts senden weiterhin VXLAN-Datenverkehr auf den alten Port.

2 NSX Manager konfiguriert alle Hosts für das Senden des Datenverkehrs auf den neuen Port.

3 NSX Manager konfiguriert alle Hosts für das Beenden der Überwachung auf dem alten Port. Der gesamte Datenverkehr wird auf dem neuen Port gesendet und empfangen.

In einer Cross-vCenter NSX-Umgebung müssen Sie die Änderung des Ports auf dem primären NSX Manager initiieren. In jeder Phase werden die Konfigurationsänderungen auf allen Hosts in der Cross-vCenter NSX-Umgebung durchgeführt, bevor mit der nächsten Phase fortgesetzt wird.

Voraussetzungen

- Stellen Sie sicher, dass der Port, den Sie für VXLAN verwenden möchten, nicht durch eine Firewall blockiert ist.

- Stellen Sie sicher, dass die Hostvorbereitung nicht zur gleichen Zeit ausgeführt wird wie die Änderung des VXLAN-Ports.

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 **Vorbereitung des logischen Netzwerks (Logical Network Preparation)** und dann auf **VXLAN-Transport (VXLAN Transport)**.
4. Klicken Sie im VXLAN-Portbereich auf die Schaltfläche **Ändern (Change)**. Geben Sie den Port ein, zu dem Sie wechseln möchten. 4789 ist der Port, der von IANA für VXLAN zugewiesen wurde.

   Es dauert einen Moment, bis die Portänderung an alle Hosts übermittelt wird.
5. (Optional) Sie können den Fortschritt der Portänderung mit der API-Anforderung `GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus` überprüfen.

   ```
   GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
   ```

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <vxlanPortUpdatingStatus>
       <prevPort>8472</prevPort>
       <targetPort>4789</targetPort>
       <taskPhase>PHASE_TWO</taskPhase>
       <taskStatus>PAUSED</taskStatus>
   </vxlanPortUpdatingStatus>
   ```

   ...

   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <vxlanPortUpdatingStatus>
       <prevPort>8472</prevPort>
       <targetPort>4789</targetPort>
       <taskPhase>FINISHED</taskPhase>
       <taskStatus>SUCCEED</taskStatus>
   </vxlanPortUpdatingStatus>
   ```

Weiter

Upgrade von NSX Edge in Cross-vCenter NSX

Upgrade von NSX Edge in Cross-vCenter NSX

NSX Edges können unabhängig vom NSX Controller-Cluster oder von Host-Cluster-Upgrades aktualisiert werden. Sie können ein NSX Edge auch dann aktualisieren, wenn Sie den NSX Controller-Cluster oder die Host-Cluster noch nicht aktualisiert haben. Führen Sie ein Upgrade für die NSX Edges in allen NSX-Installationen der Cross-vCenter NSX-Umgebung durch.

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.

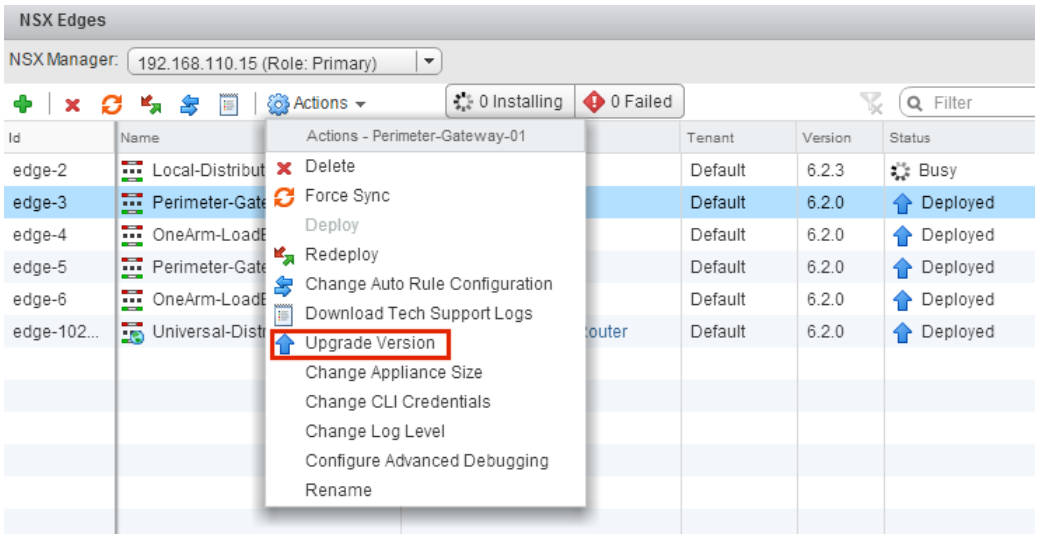
Voraussetzungen

- Vergewissern Sie sich, dass NSX Manager auf die Version 6.2.x aktualisiert wurde.
- 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.
  - Ab der Version NSX 6.2.3 werden, wenn für eine NSX Edge-Instanz mit Hochverfügbarkeit (HA, High Availability) ein Upgrade durchgeführt wird, 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.
  - Vor der Version NSX 6.2.3 wird, wenn für eine NSX Edge-Instanz mit Hochverfügbarkeit ein Upgrade durchgeführt wird, jeweils nur eine Ersetzungs-Appliance bereitgestellt, während die alten Appliances ersetzt werden. Es befinden sich dann während des Upgrades einer bestimmten NSX Edge drei NSX Edge-Appliances der geeigneten Größe im eingeschalteten Status. Nach dem Upgrade der NSX Edge-Instanz wird in der Regel die NSX Edge-Appliance mit dem HA-Index 0 aktiv.
- Machen Sie sich während der Durchführung des Upgrades mit den operativen Auswirkungen des NSX Edge-Upgrades vertraut. Weitere Informationen dazu finden Sie unter Operative Auswirkungen von NSX-Upgrades.

- Das Durchführen eines Upgrades für einen NSX Edge mit Version 5.5 oder 6.0 mit aktiviertem L2 VPN wird nicht unterstützt. Sie müssen die L2 VPN-Konfiguration löschen, bevor Sie ein Upgrade durchführen. Nach dem Upgrade können Sie L2 VPN neu konfigurieren. Weitere Informationen finden Sie im Dokument *Installationshandbuch für NSX* unter „Überblick über L2 VPN“.
- Wenn Sie ein Upgrade von NSX 6.2.x auf NSX 6.2.3 durchführen und ein Load Balancer konfiguriert wurde, finden Sie im folgenden Knowledgebase-Artikel Informationen zur Vermeidung von Upgrade-Problemen: https://kb.vmware.com/kb/2145887

Vorgehensweise

1. Melden Sie sich beim vSphere Web Client an.
2. Klicken Sie auf **Networking & Security** und anschließend auf **NSX Edges**.
3. Wählen Sie für jede NSX Edge-Instanz die Option **Upgrade der Version durchführen (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

Konfigurieren Sie bei Bedarf alle L2 VPN-Konfigurationen neu. Weitere Informationen finden Sie im *Installationshandbuch für NSX* unter „Überblick über L2 VPN“.

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.

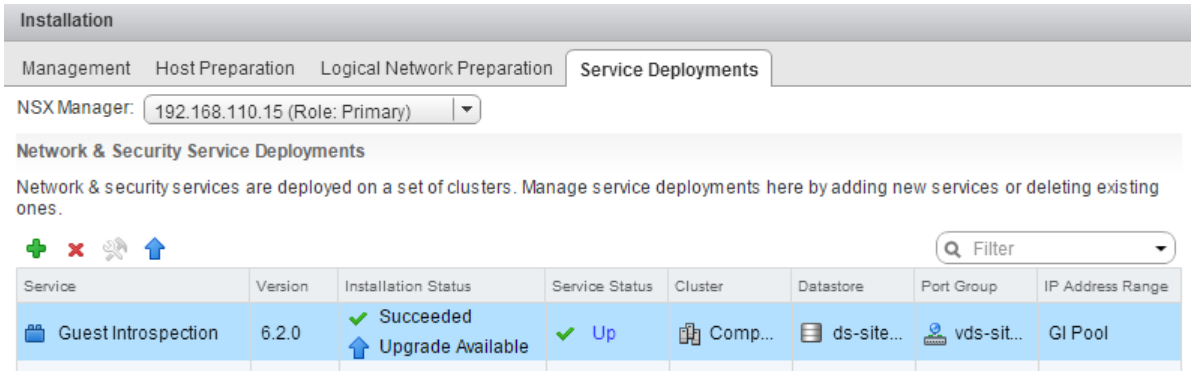
Hinweis Für die Guest Introspection-Dienst-VMs kann ein Upgrade über vSphere Web Client durchgeführt werden. Sie müssen die Dienst-VM für deren Upgrade nach dem Upgrade von NSX Manager nicht löschen. Wenn Sie die Dienst-VM löschen, wird für den Dienststatus `Fehlgeschlagen` angezeigt, da die Agenten-VM 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

Voraussetzung dafür ist das Upgrade von NSX Manager, Controllern, vorbereiteten Host-Clustern und NSX Edges auf Version 6.2.x.

Vorgehensweise

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

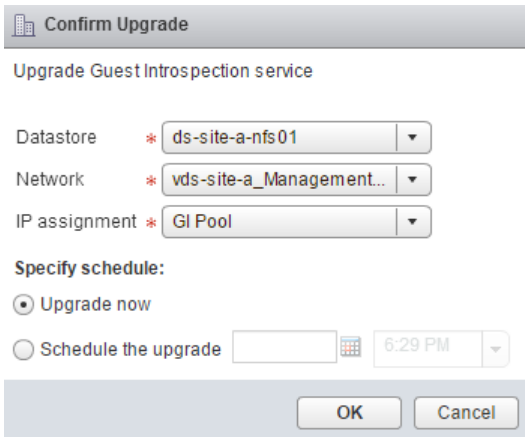


Die Spalte **Installationsstatus (Installation Status)** enthält den Wert **Upgrade verfügbar (Upgrade available)**.

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, wie virtuelle Sicherheits-Appliances von VMware-Partnern 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.

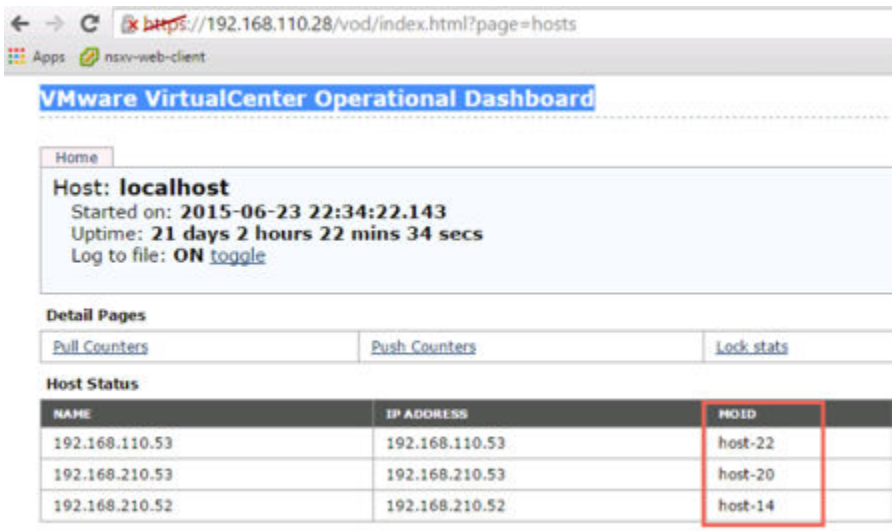
NSX Data Security

Sie sollten NSX Data Security vor dem Upgrade von NSX deinstallieren und nach Abschluss des NSX-Upgrades neu installieren. Wenn Sie NSX bereits aktualisiert haben, ohne NSX Data Security vorher zu deinstallieren, müssen Sie Data Security mithilfe eines REST-API-Aufrufs deinstallieren.

Geben Sie den folgenden API-Aufruf aus:

```
DELETE https://<nsx-manager-ip>/api/1.0/vshield/<host-id>/vsds
```

Die Host-ID ist die MOID des ESXi-Hosts. Um die MOID abzurufen, öffnen Sie das VMware VirtualCenter Operational Dashboard: https://<vcenter-ip>/vod/index.html?page=hosts.



Für den ESXi-Host mit der MOID „host-22“ auf vCenter Server 192.168.110.28 würde der API-Aufruf folgendes Format aufweisen:

```
DELETE https://192.168.110.28/api/1.0/vshield/host-22/vsds
```

Stellen Sie sicher, dass Sie den API-Aufruf auf allen Ihren ESXi-Hosts ausführen.

Nach der Deinstallation von Data Security können Sie die neue Version installieren. Weitere Informationen dazu finden Sie unter Installieren von NSX Data Security.

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 6.2.x der SSL VPN-Clients. Diese „Installieren des SSL-Clients auf der Remote-Site“ im *Administratorhandbuch für NSX*.

NSX L2 VPN

Das Durchführen eines Upgrades für NSX Edge wird nicht unterstützt, wenn Sie L2 VPN auf einem NSX Edge mit Version 5.5.x oder 6.0.x installiert haben. Alle L2 VPN-Konfigurationen müssen vor dem Upgrade von 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 3

Wenn Sie für vSphere in einer NSX-Umgebung ein Upgrade durchführen, müssen Sie sicherstellen, dass die Versionen von NSX und vSphere kompatibel sind.

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.

Dieses Kapitel behandelt die folgenden Themen:

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

Upgrade von ESXi 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.

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-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

- 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 | grep esx-v` ausgeben. Im ersten Teil der VIB-Version wird die ESXi-Version für den VIB angezeigt. Beispiel: vor dem Upgrade von ESXi 5.5 auf ESXi 6.0.

```
[root@host-1:~] esxcli software vib list | grep esx-v
esx-vsip    5.5.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-01-23
esx-vxlan   5.5.0-0.0.XXXXXXX    VMware  VMwareCertified   2017-01-23
```

Nach dem Upgrade auf ESXi 6.0:

```
[root@host-1:~] esxcli software vib list | grep esx-v
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
```

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.