NSX-Upgrade-Handbuch zu vShield Endpoint

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

NSX-Upgrade-Handbuch zu vShield Endpoint

1

Das Handbuch *NSX-Upgrade-Handbuch zu vShield Endpoint* beschreibt, wie für das VMware® NSX™-System ein Upgrade mithilfe des vSphere Web Client durchgeführt werden kann. Zu den bereitgestellten Informationen gehören schrittweise Anleitungen für das Upgrade sowie empfohlene Vorgehensweisen.

Zielgruppe

Dieses Handbuch ist für Benutzer gedacht, die vCloud Networking and Security ausschließlich wegen der Endpoint-Funktionalität verwenden und ein Upgrade auf NSX für die Bereitstellung und Verwaltung von vShield Endpoint nur für die Antivirenfunktion durchführen 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.

Wenn Sie andere Funktionen von NSX, einschließliche logische Switches, logische Router, Distributed Firewall oder NSX Edge, verwenden möchten, fidnen Sie Erläuterungen unter *Upgrade-Handbuch für NSX*

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.

Dieses Kapitel behandelt die folgenden Themen:

- Lesen der unterstützenden Dokumente
- Systemanforderungen von NSX für vShield Endpoint
- Für NSX erforderliche Ports und Protokolle

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.

Systemanforderungen von NSX für vShield Endpoint

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

Hardware

Tabelle 1-1. Hardwareanforderungen

Appliance	Arbeitsspeicher	vCPU	Festplattenspeicher
NSX Manager	16 GB (24 GB mit bestimmten NSX-Bereitstellungsgrößen*)	4 (8 mit bestimmten NSX-Bereitstellungsgrößen*)	60 GB
Guest Introspection	1 GB	2	4 GB

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

Dies sind die empfohlenen Versionen der VMware-Produkte.

- VMware vCenter Server 5.5U3
- VMware vCenter Server 6.0U2

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 1-2. 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	
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	

Tabelle 1-2. Für NSX erforderliche Ports und Protokolle (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Zweck	Sensibel	TLS	Authentifizierung
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	
Primärer NSX Manager	Globaler NSX Controller-Cluster	443	TCP	NSX Controller-REST-API	Nein	Ja	Benutzer/Kennwort

Tabelle 1-2. Für NSX erforderliche Ports und Protokolle (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Zweck	Sensibel	TLS	Authentifizierung
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

2

Dieses Kapitel behandelt die folgenden Themen:

- Vorbereiten des Upgrades von vCloud Networking and Security auf NSX für vShield Endpoint
- Upgrade von vCloud Networking and Security 5.5.x auf NSX 6.2.x für vShield Endpoint

Vorbereiten des Upgrades von vCloud Networking and Security auf NSX für vShield Endpoint

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. Weitere Informationen dazu finden Sie unter Für NSX erforderliche Ports und Protokolle.
3. Stellen Sie sicher, dass vCenter die Systemanforderungen für NSX 6.2.x erfüllt. Siehe Systemanforderungen von NSX für vShield Endpoint
4. Stellen Sie sicher, dass Sie den Uplink-Portnamen für vSphere Distributed Switches abrufen können. Weitere Informationen dazu finden Sie unter https://kb.vmware.com/kb/2129200.

5 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“. 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.

6 Wenn Sie über Data Security in Ihrer Umgebung verfügen, deinstallieren Sie es, bevor Sie ein Upgrade auf vShield Manager durchführen. Weitere Informationen dazu finden Sie unter Deinstallieren von vShield Data Security.

7 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.

8 Stellen Sie sicher, dass Sie über eine aktuelle Sicherung von vShield Manager, vCenter und anderen vCloud Networking and Security-Komponenten verfügen. Weitere Informationen dazu finden Sie unter Sichern und Wiederherstellen von vCloud Networking and Security.

9 Erstellen Sie ein Tech-Support-Paket.

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

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

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

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

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

Operative Auswirkungen von Upgrades für vShield Endpoint

Der Upgrade-Vorgang für vCloud Networking and Security kann einige Zeit in Anspruch nehmen. Bei einem Upgrade ist die Kenntnis des Betriebszustands der vCloud Networking and Security-Komponenten erforderlich.

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

- vShield Manager
- 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.

Nach dem Vorgang gilt Folgendes:

- Alle vShield- und NSX-Konfigurationsänderungen sind zulässig.

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 vShield Endpoint

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. Notieren Sie sich die aktuellen Versionen von vShield Manager, vCenter Server und ESXi.
5. Inspizieren Sie die vShield -Umgebung visuell, um sicherzustellen, dass alle Statusanzeigen grün, normal oder bereitgestellt lauten.
6. Stellen Sie sicher, dass syslog konfiguriert ist.
7. Stellen Sie sicher, dass die Partnerlösung funktioniert.

   Beispielsweise können Sie die Standardtestdatei von EICAR zum Testen der Antivirenfunktion verwenden: http://www.eicar.org/86-0-Intended-use.html.
8. (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.

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

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.

Das Upgrade der vCloud Networking and Security-Komponenten muss in der folgenden Reihenfolge ausgeführt werden:

1 vShield Manager auf NSX Manager

2 vShield Endpoint auf NSX Guest Introspection

Upgrade von vShield Manager auf NSX Manager für vShield Endpoint

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

- Stellen Sie sicher, dass alle in Vorbereiten des Upgrades von vCloud Networking and Security auf NSX für vShield Endpoint beschriebenen Aufgaben zur Upgrade-Vorbereitung abgeschlossen sind.
- Stellen Sie sicher, dass vShield Manager über genügend Festplattenspeicher für das Upgrade auf NSX Manager verfügt. Siehe Systemanforderungen von NSX für vShield Endpoint.
- 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 Systemanforderungen von NSX für vShield Endpoint.

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.

Weiter

Erstellen Sie eine Sicherung des NSX Manager. Die vorherige NSX Manager-Sicherung gilt nur für die vorherige Version. Siehe Sichern von NSX Manager-Daten für vShield Endpoint.

Sichern von NSX Manager-Daten für vShield Endpoint

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.

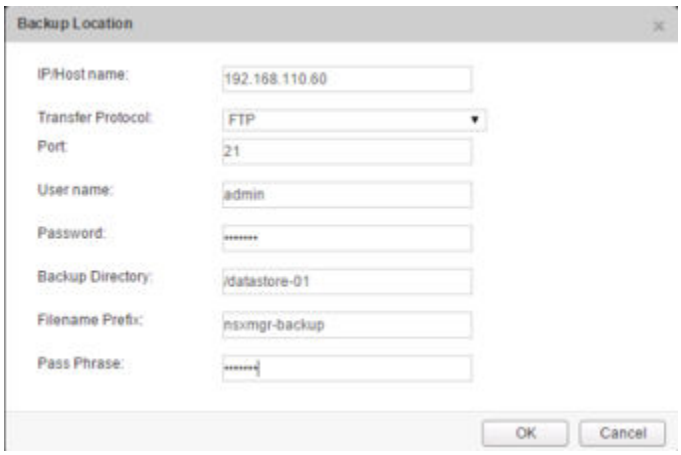
   Dieser Text wird jedem Sicherungsdateinamen vorangestellt, um eine leichte Identifizierung auf dem Sicherungssystem zu ermöglichen. Wenn Sie beispielsweise **ppdb** als Präfix verwenden, lautet der Sicherungsname `ppdbHH_MM_SS_DayDDMonYYYY`.

g Geben Sie zum Sichern der Sicherungsdatei einen Kennwortsatz ein.

Sie benötigen diese Passphrase, um die Sicherung wiederherzustellen.

h Klicken Sie auf **OK**.

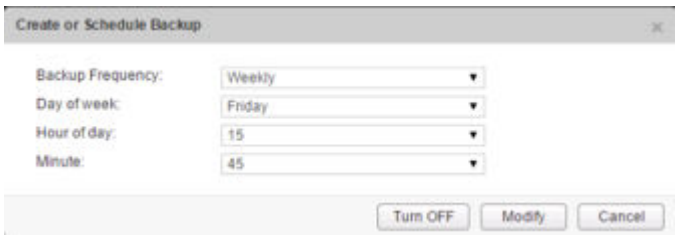
Beispiel:



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.

Weiter

Upgrade von vShield Endpoint. Weitere Informationen dazu finden Sie unter Upgrade auf Guest Introspection in NSX für vShield Endpoint.

Upgrade auf Guest Introspection in NSX für vShield Endpoint

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

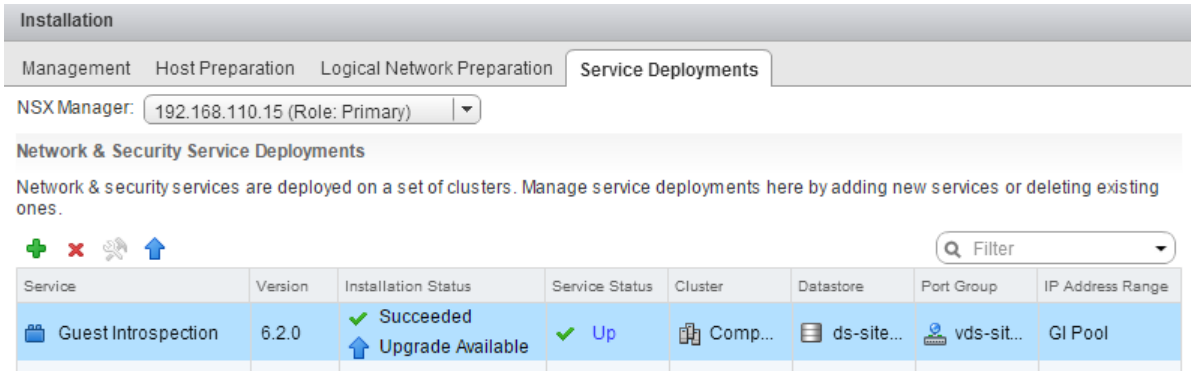
Hinweis Für die Guest Introspection-Dienst-VMs kann ein Upgrade über vSphere Web Client durchgeführt werden. Sie müssen die Dienst-VM für deren Upgrade nach dem Upgrade von NSX Manager nicht löschen. Wenn Sie die Dienst-VM löschen, wird für den Dienststatus `Fehlgeschlagen` angezeigt, da die Agenten-VM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

Vergewissern Sie sich, dass NSX Manager auf die Version 6.2.x aktualisiert wurde.

Vorgehensweise

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

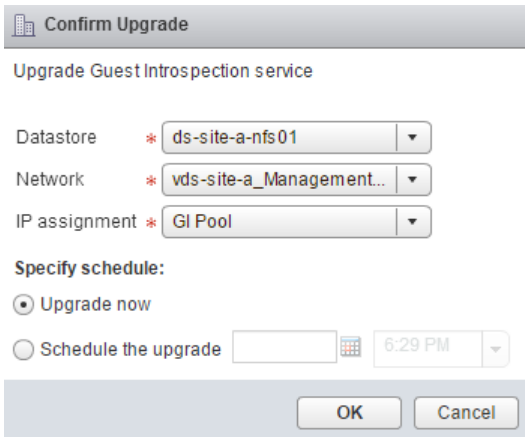


   Die Spalte **Installationsstatus (Installation Status)** enthält den Wert **Upgrade verfügbar (Upgrade available)**.

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“.

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
```

Verwenden von Partnerdiensten in NSX für vShield Endpoint

3

Guest Introspection ermöglicht die Nutzung von Partnerdiensten in Ihrer NSX-Bereitstellung.

Dieses Kapitel behandelt die folgenden Themen:

Upgrade eines Partnerdienstes in NSX für vShield Endpoint

Nachdem Sie ein Upgrade von vCloud Networking and Security auf NSX durchgeführt haben, kann es erforderlich oder wünschenswert sein, den Partnerdienst zu aktualisieren.

Voraussetzungen

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

Vorgehensweise

1. Aktualisieren Sie die Partnerverwaltungslösung.
2. Registrieren Sie den Partnerdienst im NSX Manager auf der Anbieterkonsole.

   Halten Sie sich an die Anweisungen in der Partnerdienstdokumentation.
3. Schalten Sie die VMs des alten Partnerdiensts aus und löschen Sie sie.

Weiter

Bereitstellen von Partnerdiensten

Bereitstellen von Partnerdiensten

Enthält die Partnerlösung eine virtuelle Appliance auf einem Host, können Sie den Dienst installieren, nachdem die Lösung in NSX Manager registriert worden ist.

Voraussetzungen

Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Die Partnerlösung wurde in NSX Manager registriert.
- NSX Manager kann auf die Verwaltungskonsole der Partnerlösung zugreifen.

Vorgehensweise

1. Klicken Sie auf **Networking & Security** und anschließend auf **Installation**.
2. Klicken Sie auf die Registerkarte **Dienstbereitstellungen (Service Deployments)** und auf das Symbol **Neue Dienstbereitstellung (New Service Deployment)** ( ).
3. Wählen Sie im Dialogfeld „Netzwerk- und Sicherheitsdienste bereitstellen“ die entsprechende(n) Lösung(en) aus.
4. Wählen Sie (unten im Dialogfeld) unter **Zeitplan angeben (Specify schedule)** die Option **Jetzt bereitstellen (Deploy now)**, um die Lösung sofort bereitzustellen, oder wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
5. Klicken Sie auf **Weiter (Next)**.
6. Wählen Sie das Datencenter und den bzw. die Cluster aus, in denen Sie die Lösung bereitstellen möchten, und klicken Sie auf **Weiter (Next)**.
7. Wählen Sie den Datenspeicher aus, auf dem Sie den VM-Speicher für den Dienst hinzufügen möchten, oder wählen Sie **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 für das Netzwerk die Einstellung **Angegeben auf dem Host (Specified on host)** gewählt wurde, muss das zu verwendende Netzwerk für jeden Host im Cluster in der Eigenschaft **Agent-VM-Einstellungen > Netzwerk (Agent VM Settings > Network)** angegeben werden. Weitere Informationen hierzu finden Sie in der *vSphere-API/SDK-Dokumentation*.

Sie müssen die Agent-VM-Netzwerkeigenschaft auf einem Host festlegen, bevor Sie ihn zu einem Cluster hinzufügen. Navigieren Sie zu **Verwalten (Manage) > Einstellungen (Settings) > Agent-VM-Einstellungen (Agent VM Settings) > Netzwerk (Network)** und klicken Sie auf **Bearbeiten (Edit)**, um das Agent-VM-Netzwerk einzustellen.

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 Dienst-VM eine IP-Adresse über Dynamic Host Configuration Protocol (DHCP) zu.
Einen IP-Pool	Weisen Sie der Dienst-VM eine IP-Adresse aus dem ausgewählten IP-Pool zu.

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

11 Überwachen Sie die Bereitstellung, bis „Erfolgreich“ für **Installationsstatus (Installation Status)** anzeigt wird. Wenn als Status „Fehlgeschlagen“ angezeigt wird, klicken Sie auf das Symbol neben „Fehlgeschlagen“ und führen Sie die nötigen Schritte aus, um den Fehler zu beheben.

Weiter

Sie können den Partnerdienst jetzt über die NSX-Benutzeroberfläche oder die NSX API belegen.

Verwenden von Service Composer in NSX für vShield Endpoint

Mit Service Composer können Sie Netzwerk- und Sicherheitsdienste für Anwendungen in einer virtuellen Infrastruktur bereitstellen und zuweisen.

Sie können Service Composer zum Erstellen von Sicherheitsgruppen (Security Groups) und Sicherheitsrichtlinien verwenden. Sicherheitsgruppen können Definitionen von statischen und dynamischen Gruppenmitgliedschaften enthalten. Die Sicherheitsrichtlinien weisen den Sicherheitsgruppen Dienste zu.

Weitere Informationen und Anweisungen finden Sie in der Dokumentation des Service Composer im *Administratorhandbuch für NSX*.