

NSX Upgrade Guide for vShield Endpoint

Update 5

Modified on 20 NOV 2017

VMware NSX Data Center for vSphere 6.2



vmware®

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Copyright © 2010–2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1 NSX Upgrade Guide for vShield Endpoint 4**
 - [Read the Supporting Documents 5](#)
 - [System Requirements for NSX for vShield Endpoint 5](#)
 - [Ports and Protocols Required by NSX 6](#)

- 2 vCloud Networking and Security to NSX Upgrade 10**
 - [Preparing for the vCloud Networking and Security to NSX for vShield Endpoint Upgrade 10](#)
 - [Upgrade from vCloud Networking and Security 5.5.x to NSX 6.2.x for vShield Endpoint 18](#)

- 3 Using Partner Services in NSX for vShield Endpoint 26**
 - [Upgrade a Partner Service in NSX for vShield Endpoint 26](#)
 - [Deploy a Partner Service 26](#)
 - [Using Service Composer in NSX for vShield Endpoint 28](#)

NSX Upgrade Guide for vShield Endpoint

1

This manual, the *NSX Upgrade Guide for vShield Endpoint*, describes how to upgrade the VMware[®] NSX[™] system using the vSphere Web Client. The information includes step-by-step upgrade instructions and suggested best practices.

Intended Audience

This manual is intended for anyone who uses vCloud Networking and Security solely for the Endpoint functionality, and is upgrading to NSX for deploying and managing vShield Endpoint for anti-virus offload capability only. The information in this manual is written for experienced system administrators who are familiar with virtual machine technology and virtual datacenter operations. This manual assumes familiarity with VMware vSphere 5.5 or 6.0, including VMware ESXi, vCenter Server, and the vSphere Web Client.

If you need to use any other features of NSX, including logical switches, logical routers, Distributed Firewall, or NSX Edge, please see the *NSX Upgrade Guide*

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to <http://www.vmware.com/support/pubs>.

This chapter includes the following topics:

- [Read the Supporting Documents](#)
- [System Requirements for NSX for vShield Endpoint](#)
- [Ports and Protocols Required by NSX](#)

Read the Supporting Documents

In addition to this upgrade guide, VMware publishes various other documents that support the upgrade process.

Release Notes

Before beginning the upgrade, check the release notes. Known upgrade issues and workarounds are documented in the NSX release notes. Reading the upgrade issues before you begin the upgrade process can save you time and effort. See <https://docs.vmware.com/en/VMware-NSX-for-vSphere/index.html>.

Product Interoperability Matrix

Verify interoperability with other VMware products, such as vCenter. See the VMware Product Interoperability Matrix at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php on the **Interoperability** tab.

Verify support for the upgrade path from your current version of NSX to the version that you are upgrading to. On the **Upgrade Path** tab, select **VMware NSX** from the product menu.

Compatibility Guide

Verify the compatibility of partner solutions with NSX at the VMware Compatibility Guide, at <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>.

System Requirements for NSX for vShield Endpoint

Before you install or upgrade NSX, consider your network configuration and resources. You can install one NSX Manager per vCenter Server, one instance of Guest Introspection per ESXi™ host, and multiple NSX Edge instances per datacenter.

Hardware

Table 1-1. Hardware Requirements

Appliance	Memory	vCPU	Disk Space
NSX Manager	16 GB (24 GB with certain NSX deployment sizes*)	4 (8 with certain NSX deployment sizes*)	60 GB
Guest Introspection	1 GB	2	4 GB

As a general guideline, you should increase NSX Manager resources to 8 vCPU and 24 GB of RAM if your NSX managed environment contains more than 256 hypervisors or more than 2000 VMs.

For specific sizing details contact VMware support.

For information about increasing the memory and vCPU allocation for your virtual appliances, see *Allocate Memory Resources*, and *Change the Number of Virtual CPUs in vSphere Virtual Machine Administration*.

Software

These are the recommended versions of VMware products.

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

Client and User Access

- If you added ESXi hosts by name to the vSphere inventory, ensure that forward and reverse name resolution is working. Otherwise, NSX Manager cannot resolve the IP addresses.
- Permissions to add and power on virtual machines
- Access to the datastore where you store virtual machine files, and the account permissions to copy files to that datastore
- Cookies enabled on your Web browser, to access the NSX Manager user interface
- From NSX Manager, ensure port 443 is accessible from the ESXi host, the vCenter Server, and the NSX appliances to be deployed. This port is required to download the OVF file on the ESXi host for deployment.
- A Web browser that is supported for the version of vSphere Web Client you are using. See *Using the vSphere Web Client* in the *vCenter Server and Host Management* documentation for details.

Ports and Protocols Required by NSX

The following ports must be open for NSX to operate properly.

Table 1-2. Ports and Protocols required by NSX

Source	Target	Port	Protocol	Purpose	Sensitive	TLS	Authentication
Client PC	NSX Manager	443	TCP	NSX Manager Administrative Interface	No	Yes	PAM Authentication
Client PC	NSX Manager	80	TCP	NSX Manager VIB Access	No	No	PAM Authentication
ESXi Host	vCenter Server	443	TCP	ESXi Host Preparation	No	No	
vCenter Server	ESXi Host	443	TCP	ESXi Host Preparation	No	No	
ESXi Host	NSX Manager	5671	TCP	RabbitMQ	No	Yes	RabbitMQ User/Password

Table 1-2. Ports and Protocols required by NSX (Continued)

Source	Target	Port	Protocol	Purpose	Sensitive	TLS	Authentication
ESXi Host	NSX Controller	1234	TCP	User World Agent Connection	No	Yes	
NSX Controller	NSX Controller	2878, 2888, 3888	TCP	Controller Cluster - State Sync	No	Yes	IPsec
NSX Controller	NSX Controller	7777	TCP	Inter-Controller RPC Port	No	Yes	IPsec
NSX Controller	NSX Controller	30865	TCP	Controller Cluster - State Sync	No	Yes	IPsec
NSX Manager	NSX Controller	443	TCP	Controller to Manager Communication	No	Yes	User/Password
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	No	Yes	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	No	Yes	
NSX Manager	ESXi Host	443	TCP	Management and provisioning connection	No	Yes	
NSX Manager	ESXi Host	902	TCP	Management and provisioning connection	No	Yes	
NSX Manager	DNS Server	53	TCP	DNS client connection	No	No	
NSX Manager	DNS Server	53	UDP	DNS client connection	No	No	
NSX Manager	Syslog Server	514	TCP	Syslog connection	No	No	
NSX Manager	Syslog Server	514	UDP	Syslog connection	No	No	
NSX Manager	NTP Time Server	123	TCP	NTP client connection	No	Yes	
NSX Manager	NTP Time Server	123	UDP	NTP client connection	No	Yes	
vCenter Server	NSX Manager	80	TCP	Host Preparation	No	Yes	
REST Client	NSX Manager	443	TCP	NSX Manager REST API	No	Yes	User/Password

Table 1-2. Ports and Protocols required by NSX (Continued)

Source	Target	Port	Protocol	Purpose	Sensitive	TLS	Authentication
VXLAN Tunnel End Point (VTEP)	VXLAN Tunnel End Point (VTEP)	8472 (default before NSX 6.2.3) or 4789 (default in new installs of NSX 6.2.3 and later)	UDP	Transport network encapsulation between VTEPs	No	Yes	
ESXi Host	ESXi Host	6999	UDP	ARP on VLAN LIFs	No	Yes	
ESXi Host	NSX Manager	8301, 8302	UDP	DVS Sync	No	Yes	
NSX Manager	ESXi Host	8301, 8302	UDP	DVS Sync	No	Yes	
Guest Introspection VM	NSX Manager	5671	TCP	RabbitMQ	No	Yes	RabbitMQ User/Password
Primary NSX Manager	Secondary NSX Manager	443	TCP	Cross-vCenter NSX Universal Sync Service	No	Yes	
Primary NSX Manager	vCenter Server	443	TCP	vSphere API	No	Yes	
Secondary NSX Manager	vCenter Server	443	TCP	vSphere API	No	Yes	
Primary NSX Manager	NSX Universal Controller Cluster	443	TCP	NSX Controller REST API	No	Yes	User/Password
Secondary NSX Manager	NSX Universal Controller Cluster	443	TCP	NSX Controller REST API	No	Yes	User/Password
ESXi Host	NSX Universal Controller Cluster	1234	TCP	NSX Control Plane Protocol	No	Yes	
ESXi Host	Primary NSX Manager	5671	TCP	RabbitMQ	No	Yes	RabbitMQ User/Password
ESXi Host	Secondary NSX Manager	5671	TCP	RabbitMQ	No	Yes	RabbitMQ User/Password

Ports for Cross-vCenter NSX and Enhanced Linked Mode

If you have a cross-vCenter NSX environment and your vCenter Server systems are in Enhanced Linked Mode, in order to manage any NSX Manager from any vCenter Server system each NSX Manager appliance must have the required connectivity to each vCenter Server system in the environment.

vCloud Networking and Security to NSX Upgrade

2

This chapter includes the following topics:

- [Preparing for the vCloud Networking and Security to NSX for vShield Endpoint Upgrade](#)
- [Upgrade from vCloud Networking and Security 5.5.x to NSX 6.2.x for vShield Endpoint](#)

Preparing for the vCloud Networking and Security to NSX for vShield Endpoint Upgrade

To help ensure a successful upgrade to NSX, be sure to check the release notes for upgrade issues, make sure that you are using the correct upgrade sequence, and make sure that the infrastructure is properly prepared for the upgrade. The following guidelines can be used as a pre-upgrade checklist.

Caution Downgrades are not supported:

- Always capture a backup of NSX Manager before proceeding with an upgrade.
 - Once NSX Manager has been upgraded successfully, NSX cannot be downgraded.
-

VMware recommends doing upgrade work in a maintenance window as defined by your company.

The following guidelines can be used as a pre-upgrade checklist.

- 1 Verify that vCloud Networking and Security is version 5.5. If not, see the *vShield Installation and Upgrade Guide* version 5.5 for upgrade instructions.
- 2 Verify that all required ports are open. See [Ports and Protocols Required by NSX](#).
- 3 Verify that vCenter meets the system requirements for NSX 6.2.x. See [System Requirements for NSX for vShield Endpoint](#)
- 4 Verify that you can retrieve uplink port name information for vSphere Distributed Switches. See <https://kb.vmware.com/kb/2129200>.
- 5 If any vShield Endpoint partner services are deployed, verify compatibility before upgrading:
 - In most circumstances, vCloud Networking and Security can be upgraded to NSX without impacting partner solutions. However, if your partner solution is not compatible with the version of NSX to which you are upgrading, you will need to upgrade the partner solution to a compatible version before upgrading to NSX.

- consult the VMware Compatibility Guide for Networking and Security. See <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>.
 - consult the partner documentation for compatibility and upgrade details.
- 6 If you have Data Security in your environment, uninstall it before upgrading vShield Manager. See [Uninstall vShield Data Security](#).
 - 7 If you are using Cisco Nexus 1000V as an external switch provider, you must migrate those networks to vSphere Distributed Switch before upgrading to NSX. Once NSX is installed, you can migrate the vSphere Distributed Switches to logical switches.
 - 8 Verify that you have a current backup of the vShield Manager, vCenter and other vCloud Networking and Security components. See [vCloud Networking and Security Backup and Restore](#).
 - 9 Create a Tech Support Bundle.
 - 10 Ensure that forward and reverse domain name resolution is working, using the nslookup command.
 - 11 If VUM is in use in the environment, ensure that the bypassVumEnabled flag is set to true in vCenter. This setting configures the EAM to install the VIBs directly to the ESXi hosts even when the VUM is installed and/or not available. See <http://kb.vmware.com/kb/2053782>.
 - 12 Download and stage the upgrade bundle, validate with md5sum. See [Download the vShield Manager to NSX Upgrade Bundle and Check the MD5](#).
 - 13 As a best practice, quiesce all operations in the environment until all sections of the upgrade are complete.
 - 14 Do not power down or delete any vCloud Networking and Security components or appliances before instructed to do so.

Operational Impacts of Upgrades for vShield Endpoint

The vCloud Networking and Security upgrade process can take some time. It is important to understand the operational state of vCloud Networking and Security components during an upgrade.

To upgrade vCloud Networking and Security to NSX 6.2, you must upgrade the NSX components in the following order:

- vShield Manager
- vShield Endpoint

VMware recommends that you run the upgrade in a single outage window to minimize downtime and reduce confusion among vCloud Networking and Security users who cannot access certain vCloud Networking and Security management functions during the upgrade. However, if your site requirements prevent you from completing the upgrade in a single outage window, the information below can help your vCloud Networking and Security users understand what features are available during the upgrade.

vCenter Upgrade

If you are using vCenter embedded SSO and you are upgrading vCenter 5.5 to vCenter 6.0, vCenter might lose connectivity with vShield Manager. This happens if vCenter 5.5 was registered with vShield using the root user name. Starting in NSX 6.2, vCenter registration with root is deprecated. As a workaround, re-register vCenter with vShield using the administrator@vsphere.local user name instead of root.

If you are using external SSO, no change is necessary. You can retain the same user name, for example admin@mybusiness.mydomain, and vCenter connectivity will not be lost.

vShield Manager Upgrade

During:

- vShield Manager configuration is blocked. The vShield API service is unavailable. No changes to the vShield configuration can be made. Existing VM communication continues to function.

After:

- All vShield and NSX configuration changes are allowed.

vShield Endpoint Migrated to Guest Introspection

In NSX 6.x, vShield Endpoint is renamed Guest Introspection. After you have upgraded NSX Manager, if you navigate to **Networking & Security > Installation > Service Deployments** the Guest Introspection service will display an **Upgrade** link. When you upgrade from vCloud Networking and Security to NSX, the Guest Introspection virtual appliance and the host agent for Guest Introspection are deployed on each host in the cluster where Guest Introspection is enabled.

During:

- There is a loss of protection for VMs in the NSX cluster when there is a change to the VMs, such as VM additions, vMotions, or deletions.

After:

- VMs are protected during VM additions, vMotions, and deletions.

Verify the Working State of vShield Endpoint

Before beginning the upgrade, it is important to test the vCloud Networking and Security working state. Otherwise, you will not be able to determine if any post-upgrade issues were caused by the upgrade process or if they preexisted the upgrade process.

Do not assume everything is working before you start to upgrade the vCloud Networking and Security infrastructure. Make sure to check it first.

You can use the following procedure as a pre-upgrade checklist.

Procedure

- 1 Identify administrative user IDs and passwords.

- 2 Verify that forward and reverse name resolution is working for all components.
- 3 Verify you can log in to all vSphere and vShield components.
- 4 Note the current versions of vShield Manager, vCenter Server, and ESXi.
- 5 Visually inspect the vShield environment to make sure all status indicators are green, normal, or deployed.
- 6 Verify that syslog is configured.
- 7 Verify that the partner solution is functioning.

For example, you can use the EICAR Standard Anti-Virus Test File for testing anti-virus functionality: <http://www.eicar.org/86-0-Intended-use.html>.

- 8 (Optional) If you have a test environment, test the upgrade and post-upgrade functionality before upgrading a production environment.

Migrate the Local Admin User to the CLI Admin User

Prior to NSX 6.x series, the user admin was a local database user. Starting in NSX 6.0, the user admin became a CLI user. For backward compatibility, there are steps you can take to migrate the admin user.

For vCloud Networking and Security 5.x series, the admin user in the CLI and the admin user in the UI (VSM) were two different users. The CLI user admin's password was managed by the OS, and the VSM user's password was managed by the local database of users. When you changed the password for the CLI admin user, the change did not affect the VSM admin user's password. Likewise, when you changed the VSM admin user's password, the change did not affect the CLI admin password.

For NSX 6.x series, the VSM user database is deprecated. The CLI user can log in to the NSX Manager directly.

In an upgrade scenario, for backward compatibility, the admin user is present in both the CLI and Web UI databases. In this case, if the password of the CLI user is changed, the change does not get reflected in the UI or in REST API calls. Prior to NSX 6.x series, the CLI user could not log in to the UI or to the REST API.

In fresh (green field) deployments of NSX 6.x series, the CLI user and the NSX Manager (UI or REST) are the same, and the credentials are the same.

If you want your upgraded NSX deployment to behave like a fresh deployment of NSX 6.x, you have two options.

- Option 1---Change the password for the admin database user.

You can use the following REST API to change the password. This option requires you to know the old password.

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>
```

For example, using 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</userId><password>123</password><fullname>admin</fullname><email>admin@com
pany.com</email><accessControlEntry><role>security_admin</role><resource><resourceId>datacenter-312
</resourceId></resource></accessControlEntry></userInfo>'
```

The API can be used to update a local user account including the password. If a password is not provided, the existing password is retained. The userId variable in the URI should be the same as the one specified in XML.

- Option 2---Instead of keeping the Web UI admin user, you can remove it and add a role to the CLI admin user. After this change, you can log in to NSX Manager using the CLI user credentials, and a password change for the CLI admin user is reflected on the NSX Manager admin user.

Because the Web UI admin user is the super_user, you need to add another user with super_user privileges before you can delete the Web UI admin user.

- Add a new user tempadmin with the super_user role.

For example, using 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>tempadmin</userId><password>123</password><fullname>tempadmin</fullname><ema
il>tempadmin@company.com</email><accessControlEntry><role>super_user</role><resource><resourceI
d>datacenter-312</resourceId></resource></accessControlEntry></userInfo>'
```

- Use tempadmin to delete the Web UI user admin.

For example, using curl:

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

- Add the super_user role to the CLI user admin.

For example, using 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
'<accessControlEntry><role>super_user</role></accessControlEntry>'
```

Uninstall vShield Data Security

If you have Data Security in your environment, uninstall it before upgrading to NSX.

As of NSX 6.2.3, the NSX Data Security feature has been deprecated. In NSX 6.2.3, you can continue to use this feature at your discretion, but be aware that this feature will be removed from NSX in a future release.

Procedure

- 1 From the vShield Manager 5.5 inventory panel, expand the **Datcenters** folder and navigate to a host where vShield Data Security is installed.
- 2 On each host where vShield Data Security is installed, complete these steps to uninstall it.
 - a Click the host, and in the **Summary** tab, in the vShield Host Preparation pane, click the **Uninstall** link for vShield Data Security.
 - b In the Select Services to Uninstall pane verify that vShield Data Security is selected, and click the **Uninstall** button.

vShield Data Security is uninstalled and the vShield Host Preparation pane shows the status as Not Installed.

vCloud Networking and Security Backup and Restore

Proper backup of all vCloud Networking and Security components is crucial to restore the system to its working state in the event of a failure.

The vShield Manager backup contains all of the vShield configuration, including virtual wires and routing entities, security, vApp rules, and everything else that you configure within the vShield Manager UI or API. The vCenter database and related elements like the virtual switches need to be backed up separately.

At a minimum, we recommend taking regular backups of vShield Manager and vCenter. Your backup frequency and schedule might vary based on your business needs and operational procedures. We recommend taking vCloud Networking and Security backups frequently during times of frequent configuration changes.

vShield Manager backups can be taken on demand or on an hourly, daily, or weekly basis.

We recommend taking backups in the following scenarios:

- Before a vCloud Networking and Security or vCenter upgrade.
- After a vCloud Networking and Security or vCenter upgrade.
- After Day Zero deployment and initial configuration of vCloud Networking and Security components, such as after the creation of virtual switches, edges, security, and firewall policies.
- After infrastructure or topology changes.
- After any major Day 2 change.

To provide an entire system state at a given time to roll back to, we recommend synchronizing vCloud Networking and Security component backups with your backup schedule for other interacting components, such as vCenter, cloud management systems, operational tools, and so on.

Back Up Your vShield Manager Data on Demand

You can back up vShield Manager data at any time by performing an on-demand backup.

Procedure

- 1 Click **Settings & Reports** from the vShield Manager inventory panel.
- 2 Click the **Configuration** tab.
- 3 Click **Backups**.
- 4 (Optional) Select the **Exclude System Events** check box if you do not want to back up system event tables.
- 5 (Optional) Select the **Exclude Audit Logs** check box if you do not want to back up audit log tables.
- 6 Type the **Host IP Address** of the system where the backup will be saved.
- 7 Type the **Host Name** of the backup system.
- 8 Type the **User Name** required to log in to the backup system.
- 9 Type the **Password** associated with the user name for the backup system.
- 10 In the **Backup Directory** field, type the absolute path where backups are to be stored.
- 11 Type a text string in **Filename Prefix**.

This text is prepended to the backup filename for easy recognition on the backup system. For example, if you type **ppdb**, the resulting backup is named as **ppdbHH_MM_SS_DayDDMonYYYY**.

12 Enter a **Pass Phrase** to secure the backup file.

In vCloud Networking and Security, a pass phrase was optional. In NSX, it is required.

13 From the **Transfer Protocol** drop-down menu, select either **SFTP** or **FTP**.

14 Click **Backup**.

Once complete, the backup appears in a table below this forms.

15 Click **Save Settings** to save the configuration.

Note that if all of your backups are saved in a single directory, you might experience issues viewing backups. A best practice is to occasionally move backup files to an archive folder.

Back Up vSphere Distributed Switches

You can export vSphere distributed switch and distributed port group configurations to a file.

The file preserves valid network configurations, enabling distribution of these configurations to other deployments.

This functionality is available only with the vSphere Web Client 5.1 or later. VDS settings and port-group settings are imported as part of the import.

As a best practice, export the VDS configuration before preparing the cluster for VXLAN. For detailed instructions, see <http://kb.vmware.com/kb/2034602>.

Back Up vCenter

To secure your NSX deployment, it is important to back up the vCenter database and take snapshots of the VMs.

Refer to the vCenter documentation for your vCenter version for vCenter backup and restore procedures and best practices.

For VM snapshots, see <http://kb.vmware.com/kb/1015180>.

Useful links for 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>

Useful links for 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>

Download the vShield Manager to NSX Upgrade Bundle and Check the MD5

The vShield Manager to NSX upgrade bundle contains all the files needed to upgrade the NSX infrastructure. Before upgrading vShield Manager you will first need to download the upgrade bundle for the version you wish to upgrade to.

Prerequisites

An MD5 checksum tool.

Procedure

- 1 Download the vShield Manager to NSX upgrade bundle to a location vShield Manager can browse to. The name of the upgrade bundle file has a format similar to `VMware-vShield-Manager-upgrade-bundle-to-NSX-releaseNumber-NSXbuildNumber.tar.gz`.

- 2 Verify the upgrade filename ends with `tar.gz`.

Some browsers might alter the file extension. For example if the download filename is:

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

Change it to:

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

Otherwise, after uploading the upgrade bundle, the following error message appears: "Invalid upgrade bundle file `VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx.gz`, upgrade file name has extension `tar.gz`."

- 3 Use an MD5 checksum tool to compare the upgrade bundle's official MD5 sum shown on the VMware Web site with the MD5 sum calculated by the checksum tool.
 - a In the MD5 checksum tool, browse to the upgrade bundle.
 - b Use the tool to calculate the checksum of the bundle.
 - c Paste in the checksum listed on the VMware Web site.
 - d Use the tool to compare the two checksums.

If the two checksums do not match, repeat the upgrade bundle download.

Upgrade from vCloud Networking and Security 5.5.x to NSX 6.2.x for vShield Endpoint

To upgrade to NSX 6.2.x, you must upgrade the vCloud Networking and Security components in the order in which they are documented in this guide.

vCloud Networking and Security components must be upgraded in the following order:

- 1 vShield Manager to NSX Manager

2 vShield Endpoint to NSX Guest Introspection

Upgrade vShield Manager to NSX Manager for vShield Endpoint

The first step in the NSX infrastructure upgrade process is the NSX Manager appliance upgrade.

Caution Do not uninstall a deployed instance of vShield Manager appliance.

Prerequisites

- Verify you have completed all the upgrade preparation tasks described in [Preparing for the vCloud Networking and Security to NSX for vShield Endpoint Upgrade](#).
- Verify that vShield Manager has sufficient disk space for the upgrade to NSX Manager. See [System Requirements for NSX for vShield Endpoint](#).
- Increase the vShield Manager virtual appliance's reserved memory to at least 16 GB and allocate 4 vCPU before upgrading to NSX 6.2.x.

See [System Requirements for NSX for vShield Endpoint](#).

Procedure

- 1 Download the NSX upgrade bundle to a location to which vShield Manager can browse. The name of the upgrade bundle file is similar to `VMware-vShield-Manager-upgrade-bundle-to-NSX-release-buildNumber.tar.gz`.
- 2 From the vShield Manager 5.5 inventory panel, click **Settings & Reports**.
- 3 Click the **Updates** tab and then click **Upload Upgrade Bundle**.
- 4 Click **Choose File**, select the `VMware-vShield-Manager-upgrade-bundle-to-NSX-release-buildNumber.tar.gz` file, and click **Open**.
- 5 Click **Upload File**.

Uploading the file takes a few minutes.

- 6 Click **Install** to begin the upgrade process.
- 7 Click **Confirm Install**. The upgrade process reboots vShield Manager, so you might lose connectivity to the vShield Manager user interface. None of the other vShield components are rebooted.
- 8 After the reboot, log in to the NSX Manager virtual appliance by opening a Web browser window and typing the IP address, for example, `https://10.10.10.10`. The upgraded NSX Manager has the same IP address as the vShield Manager.

The Summary tab displays the version of NSX Manager that you just installed.

- 9 Navigate to **Home > Manage vCenter Registration** and verify that the vCenter Server status is Connected.
- 10 Close any existing browser sessions accessing the vSphere Web Client. Wait a few minutes and clear the browser cache before logging back in to the vSphere Web Client.

- 11 If SSH was enabled on vShield Manager, you must enable it on NSX Manager after the upgrade. Log in to the NSX Manager virtual appliance and click **View Summary**. In System-level components, click **Start** for SSH service.

Important After upgrading from vCloud Networking and Security 5.x to NSX 6.x, you must use your CLI administrative login credentials to log in to the NSX Manager. Previously, in vCloud Networking and Security, two passwords were required, one for the CLI and another for the UI. Starting in NSX 6.x, only one password is required. For example:

Passwords in vCloud Networking and Security

- mypassword#123 for the CLI
- mypassword#456 for the UI

Passwords after upgrade to NSX

- mypassword#123 for the CLI
 - mypassword#123 for the UI
-

After upgrading NSX Manager, you must log out and log back in to the vSphere Web Client.

If the NSX plug-in does not display correctly in the vSphere Web Client, clear your browser's cache and history. If this step is not done, you might see an error similar to "An internal error has occurred - Error #1009" when making NSX configuration changes in the vSphere Web Client.

If the Networking and Security tab does not appear in the vSphere Web Client, reset the vSphere web client server:

- In vCenter 5.5, open `https://<vcenter-ip>:5480` and restart the Web Client server.
- In the vCenter Server Appliance 6.0, log into the vCenter Server shell as root and run the following commands:

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

- In vCenter Server 6.0 on Windows, you can do this by running the following commands.

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

It is recommended to use different Web Clients to manage vCenter Servers running different versions of NSX Managers to avoid unexpected errors when different versions of NSX plug-ins are running.

What to do next

Create a backup of the NSX Manager. The previous NSX Manager backup is valid only for the previous release. See [Back Up NSX Manager Data for vShield Endpoint](#).

Back Up NSX Manager Data for vShield Endpoint

You can back up NSX Manager data by performing an on-demand backup or a scheduled backup.

NSX Manager backup and restore can be configured from the NSX Manager virtual appliance web interface or through the NSX Manager API. Backups can be scheduled on an hourly, daily or weekly basis.

The backup file is saved to a remote FTP or SFTP location that NSX Manager can access. NSX Manager data includes configuration, events, and audit log tables. Configuration tables are included in every backup.

Restore is only supported on the same NSX Manager version as the backup version. For this reason, it is important to create a new backup file before and after performing an NSX upgrade, one backup for the old version and another backup for the new version.

Procedure

- 1 Log in to the NSX Manager Virtual Appliance.
- 2 Under Appliance Management, click **Backups & Restore**.
- 3 To specify the backup location, click **Change** next to FTP Server Settings.
 - a Type the IP address or host name of the backup system.
 - b From the **Transfer Protocol** drop-down menu, select either **SFTP** or **FTP**, based on what the destination supports.
 - c Edit the default port if required.
 - d Type the user name and password required to login to the backup system.

- e In the **Backup Directory** field, type the absolute path where backups will be stored.

To determine the absolute path, you can log in to the FTP server, navigate to the directory that you want to use, and run the present working directory command (pwd). For example:

```
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 Type a text string in **Filename Prefix**.

This text is prepended to each backup filename for easy recognition on the backup system. For example, if you type **ppdb**, the resulting backup is named as ppdbHH_MM_SS_DayDDMonYYYY.

- g Type the pass phrase to secure the backup.

You will need this pass phrase to restore the backup.

- h Click **OK**.

For example:

The screenshot shows a 'Backup Location' dialog box with the following fields and values:

- IP/Host name: 192.168.110.60
- Transfer Protocol: FTP
- Port: 21
- User name: admin
- Password: (masked with asterisks)
- Backup Directory: /datastore-01
- Filename Prefix: nsxmgr-backup
- Pass Phrase: (masked with asterisks)

At the bottom right, there are 'OK' and 'Cancel' buttons.

- 4 For an on-demand backup, click **Backup**.

A new file is added under **Backup History**.

- 5 For scheduled backups, click **Change** next to Scheduling.

The screenshot shows a dialog box titled "Create or Schedule Backup". It contains four dropdown menus for scheduling a backup: "Backup Frequency" (set to Weekly), "Day of week" (set to Friday), "Hour of day" (set to 15), and "Minute" (set to 45). At the bottom of the dialog are three buttons: "Turn OFF", "Modify", and "Cancel".

- a From the **Backup Frequency** drop-down menu, select **Hourly**, **Daily**, or **Weekly**. The Day of Week, Hour of Day, and Minute drop-down menus are disabled based on the selected frequency. For example, if you select Daily, the Day of Week drop-down menu is disabled as this field is not applicable to a daily frequency.
 - b For a weekly backup, select the day of the week the data should be backed up.
 - c For a weekly or daily backup, select the hour at which the backup should begin.
 - d Select the minute to begin and click **Schedule**.
- 6 To exclude logs and flow data from being backed up, click **Change** next to Exclude.
- a Select the items you want to exclude from the backup.
 - b Click **OK**.
- 7 Save your FTP server IP/hostname, credentials, directory details, and pass phrase. This information is needed to restore the backup.

What to do next

Upgrade vShield Endpoint. See [Upgrade to Guest Introspection in NSX for vShield Endpoint](#).

Upgrade to Guest Introspection in NSX for vShield Endpoint

It is important to upgrade Guest Introspection to match the NSX Manager version.

Note The Guest Introspection service VMs can be upgraded from the vSphere Web Client. You do not need to delete the service VM after the upgrade of the NSX Manager to upgrade it. If you do delete the service VM, the Service Status will be shown as **Failed** because the Agent VM is missing. Click on **Resolve** to deploy a new service VM, then click **Upgrade Available** to deploy the latest Guest Introspection service VM.

Prerequisites

Verify NSX Manager has been upgraded to 6.2.x.

Procedure

- 1 In the **Installation** tab, click **Service Deployments**.

Installation

Management Host Preparation Logical Network Preparation **Service Deployments**

NSX Manager: 192.168.110.15 (Role: Primary)

Network & Security Service Deployments

Network & security services are deployed on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.

Service	Version	Installation Status	Service Status	Cluster	Datastore	Port Group	IP Address Range
Guest Introspection	6.2.0	Succeeded Upgrade Available	Up	Comp...	ds-site...	vds-sit...	GI Pool

The **Installation Status** column says **Upgrade Available**.

- 2 Select the Guest Introspection deployment that you want to upgrade.

The **Upgrade** () icon in the toolbar above the services table is enabled.

- 3 Click the **Upgrade** () icon and follow the UI prompts.

Confirm Upgrade

Upgrade Guest Introspection service

Datastore *

Network *

IP assignment *

Specify schedule:

☒ Upgrade now

☐ Schedule the upgrade

OK Cancel

After Guest Introspection is upgraded, the installation status is Succeeded and service status is Up. Guest Introspection service virtual machines are visible in the vCenter Server inventory.

What to do next

After Guest Introspection is upgraded for a particular cluster, you can upgrade any partner solutions. If partner solutions are enabled, refer to the upgrade documentation provided by the partner. Even if the partner solution is not upgraded, protection is maintained.

If you upgrade a partner solution to a version which is NSX certified, you must use Service Composer to create policies based on the partner solutions to maintain protection. See Using Service Composer in the *NSX Administration Guide*.

Post-Upgrade Checklist

After the upgrade is complete, follow these steps.

Procedure

- 1 Create a current backup of the NSX Manager after the upgrade.
- 2 Check that VIBs have been installed on the hosts.

NSX installs these VIBs:

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

If Guest Introspection has been installed, also check that this VIB is present on the hosts:

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

- 3 Resynchronize the host message bus. VMware advises that all customers perform resync after an upgrade.

You can use the following API call to perform the resynchronization on each host.

```
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
```

Using Partner Services in NSX for vShield Endpoint

3

Guest Introspection allows you to use partner services in your NSX deployment.

This chapter includes the following topics:

- [Upgrade a Partner Service in NSX for vShield Endpoint](#)
- [Deploy a Partner Service](#)
- [Using Service Composer in NSX for vShield Endpoint](#)

Upgrade a Partner Service in NSX for vShield Endpoint

After upgrading from vCloud Networking and Security to NSX, you may need to or want to upgrade the partner service.

Prerequisites

Consult the partner service documentation for compatibility and upgrade details.

Procedure

- 1 Upgrade the partner management solution.
- 2 Register the partner service with NSX Manager on the vendor's console.
Refer to the partner service documentation for instructions.
- 3 Power off and delete old partner service VMs.

What to do next

[Deploy a Partner Service](#)

Deploy a Partner Service

If the partner solution includes a host-resident virtual appliance, you can deploy the service after the solution is registered with NSX Manager.


Prerequisites

Ensure that:

- The partner solution is registered with NSX Manager.

- NSX Manager can access the partner solution's management console.

Procedure

- 1 Click **Networking & Security** and then click **Installation**.
- 2 Click the **Service Deployments** tab and click the **New Service Deployment** () icon.
- 3 In the Deploy Network and Security Services dialog box, select the appropriate solution(s).
- 4 In **Specify schedule** (at the bottom of the dialog box), select **Deploy now** to deploy the solution immediately or select a deployment date and time.
- 5 Click **Next**.
- 6 Select the datacenter and cluster(s) where you want to deploy the solution and click **Next**.
- 7 Select the datastore on which to add the solution service virtual machines storage or select **Specified on host**.

The selected datastore must be available on all hosts in the selected cluster.

If you selected **Specified on host**, the datastore for the ESX host must be specified in the **Agent VM Settings** of the host before it is added to the cluster. See *vSphere API/SDK Documentation*.

- 8 Select the distributed virtual port group to host the management interface. This port group must be able to reach the NSX Manager's port group.

If the network is set to **Specified on host**, the network to be used must be specified in the **Agent VM Settings > Network** property of each host in the cluster. See *vSphere API/SDK Documentation*.

You must set the agent VM network property on a host before you add it to a cluster. Navigate to **Manage > Settings > Agent VM Settings > Network** and click **Edit** to set the agent VM network.

The selected port group must be available on all hosts in the selected cluster.

- 9 In IP assignment, select one of the following:

Select	To
DHCP	Assign an IP address to the service virtual machine through Dynamic Host Configuration Protocol (DHCP).
An IP pool	Assign an IP address to the service virtual machine from the selected IP pool.

- 10 Click **Next** and then click **Finish** on the Ready to complete page.
- 11 Monitor the deployment until the **Installation Status** displays Successful. If the status displays Failed, click the icon next to Failed and take action to resolve the error.

What to do next

You can now consume the partner service through NSX UI or NSX API.

Using Service Composer in NSX for vShield Endpoint

Service Composer helps you provision and assign network and security services to applications in a virtual infrastructure.

You use Service Composer to create security groups and security policies. Security groups can contain static and dynamic group membership definitions. Security policies apply services to security groups.

See the Service Composer documentation in the *NSX Administration Guide* for information and instructions.