

# NSX Upgrade Guide

Update 10

Modified on 29 MAR 2018

VMware NSX for vSphere 6.3



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](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2010 – 2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

<b>NSX Upgrade Guide</b>	<b>4</b>
Read the Supporting Documents	4
System Requirements for NSX	5
Ports and Protocols Required by NSX	7
<b>1 Upgrading NSX</b>	<b>10</b>
Preparing for the NSX Upgrade	10
Upgrade to NSX 6.3.x	26
Upgrade to NSX 6.3.x with Cross-vCenter NSX	39
<b>2 Upgrading vSphere in an NSX Environment</b>	<b>57</b>
Upgrade to ESXi 6.0 in an NSX Environment	58
Upgrade to ESXi 6.5 in an NSX Environment	60
Redeploy Guest Introspection after ESXi Upgrade	63

# NSX Upgrade Guide

The *NSX Upgrade Guide*, describes how to upgrade the VMware NSX<sup>®</sup> for vSphere<sup>®</sup> system using the NSX Manager user interface and 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 wants to upgrade or use NSX in a VMware vCenter environment. 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, including VMware ESXi, vCenter Server, and the vSphere Web Client.

## 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>.

## 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 **Interoperability** tab of the VMware Product Interoperability Matrix at [http://partnerweb.vmware.com/comp\\_guide2/sim/interop\\_matrix.php#interop&93=](http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#interop&93=).

## Upgrade Path Matrix

Verify support for the upgrade path from your current version of NSX to the version that you are upgrading to. See the **Upgrade Path** tab of the VMware Product Interoperability Matrix at [http://partnerweb.vmware.com/comp\\_guide2/sim/interop\\_matrix.php#upgrade&solution=93](http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php#upgrade&solution=93).

## 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

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

This table lists the hardware requirements for NSX appliances.

**Table 1. Hardware Requirements for Appliances**

Appliance	Memory	vCPU	Disk Space
NSX Manager	16 GB (24 GB for larger NSX deployments)	4 (8 for larger NSX deployments)	60 GB
NSX Controller	4 GB	4	28 GB
NSX Edge	<ul style="list-style-type: none"> <li>■ Compact: 512 MB</li> <li>■ Large: 1 GB</li> <li>■ Quad Large: 2 GB</li> <li>■ X-Large: 8 GB</li> </ul>	<ul style="list-style-type: none"> <li>■ Compact: 1</li> <li>■ Large: 2</li> <li>■ Quad Large: 4</li> <li>■ X-Large: 6</li> </ul>	<ul style="list-style-type: none"> <li>■ Compact, Large, Quad Large: 1 disk 584MB + 1 disk 512MB</li> <li>■ XLarge: 1 disk 584MB + 1 disk 2GB + 1 disk 256MB</li> </ul>
Guest Introspection	2 GB	2	5 GB (Provisioned space is 6.26 GB)

As a general guideline, 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*.

The provisioned space for a Guest Introspection appliance shows as 6.26 GB for Guest Introspection. This is because vSphere ESX Agent Manager creates a snapshot of the service VM to create fast clones, when multiple hosts in a cluster shares a storage. For more information on how to disable this option via ESX Agent Manager, refer to *ESX Agent Manager* documentation.

## Network Latency

You should ensure that the network latency between components is at or below the maximum latency described.

**Table 2. Maximum network latency between components**

Components	Maximum latency
NSX Manager and NSX Controllers	150 ms RTT
NSX Manager and ESXi hosts	150 ms RTT
NSX Manager and vCenter Server system	150 ms RTT
NSX Manager and NSX Manager in a cross-vCenter NSX environment	150 ms RTT

## Software

For the latest interoperability information, see the Product Interoperability Matrixes at [http://partnerweb.vmware.com/comp\\_guide/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php).

For recommended versions of NSX, vCenter Server, and ESXi, see the release notes for the version of NSX to which you are upgrading. Release notes are available at the NSX for vSphere documentation site: <https://docs.vmware.com/en/VMware-NSX-for-vSphere/index.html>.

For an NSX Manager to participate in a cross-vCenter NSX deployment the following conditions are required:

Component	Version
NSX Manager	6.2 or later
NSX Controller	6.2 or later
vCenter Server	6.0 or later
ESXi	<ul style="list-style-type: none"> <li>■ ESXi 6.0 or later</li> <li>■ Host clusters prepared with NSX 6.2 or later VIBs</li> </ul>

To manage all NSX Managers in a cross-vCenter NSX deployment from a single vSphere Web Client, you must connect your vCenter Servers in Enhanced Linked Mode. See *Using Enhanced Linked Mode in vCenter Server and Host Management*.

To verify the compatibility of partner solutions with NSX, see the VMware Compatibility Guide for Networking and Security at <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>.

## Client and User Access

The following items are required to manage your NSX environment:

- Forward and reverse name resolution. This is required if you have added ESXi hosts by name to the vSphere inventory, 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 must be enabled on your Web browser to access the NSX Manager user interface.
- Port 443 must be open between the NSX Manager and 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.

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

**Table 3. Ports and Protocols Required by NSX for vSphere**

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	443	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
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

**Table 3. Ports and Protocols Required by NSX for vSphere (Continued)**

Source	Target	Port	Protocol	Purpose	Sensitive	TLS	Authentication
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 3. Ports and Protocols Required by NSX for vSphere (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

# Upgrading NSX

This chapter includes the following topics:

- [Preparing for the NSX Upgrade](#)
- [Upgrade to NSX 6.3.x](#)
- [Upgrade to NSX 6.3.x with Cross-vCenter NSX](#)

## Preparing for the NSX Upgrade

To help ensure a successful NSX upgrade, 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.

---

**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 vCenter meets the system requirements for NSX. See [System Requirements for NSX](#).
- 2 If any Guest Introspection or Network Extensibility partner services are deployed, verify compatibility before upgrading:
  - In most circumstances, NSX can be upgraded 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 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.
- 3 If you have Data Security in your environment, uninstall it before upgrading NSX. Data Security is not supported in NSX 6.3.x. See [Uninstall NSX Data Security](#).

- 4 If you have a hardware gateway (hardware VTEP) installed in your environment, upgrade to NSX 6.3.0 and 6.3.1 is blocked. You must contact VMware support to proceed with the upgrade. See <https://kb.vmware.com/kb/2148511> for more information. Upgrade to NSX 6.3.2 is allowed.
- 5 If you have any NSX 5.5 or earlier NSX Edge appliances, you must upgrade them to NSX 6.x before upgrading to NSX 6.3.x.
- 6 If you are upgrading to NSX 6.3.3 the NSX Controller cluster must contain three controller nodes. If it has fewer than three you must add additional nodes before starting the upgrade. See "Deploy NSX Controller Cluster" in the *NSX Installation Guide* for steps to add controller nodes.
- 7 Determine which NSX Managers must be upgraded in the same maintenance window.
  - If you have a cross-vCenter NSX environment, you must upgrade the primary and all secondary NSX Managers to the same NSX version in a single maintenance window.
  - If you have multiple NSX Managers connected to vCenter Server systems that use the same SSO server, not all combinations of NSX Manager version are supported. You must plan the upgrade of your NSX Managers so that you have a supported configuration at the end of the maintenance window
    - All NSX Managers using the same version of NSX is supported.
    - NSX Managers using different version of NSX is supported if at least one NSX Manager has NSX 6.4.0 or later installed, and all other NSX Managers have NSX 6.3.3 or later installed.
- 8 Verify that you have a current backup of the NSX Manager, vCenter and other NSX components. See [NSX 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 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 NSX components or appliances before instructed to do so.

## Evaluate License Needs when Upgrading NSX

NSX introduced a new licensing model in May 2016.

If you have an active support contract, when you upgrade from NSX 6.2.2 or earlier to NSX 6.2.3 or later, your existing license is converted to a NSX Enterprise license, and you will be entitled to the same functionality in the Enterprise offering.

For information about the NSX licencing editions and associated features, see <https://kb.vmware.com/kb/2145269>.

## Operational Impacts of NSX Upgrades

The NSX upgrade process can take some time. It is important to understand the operational state of NSX components during an upgrade, such as when some but not all hosts have been upgraded, or when NSX Edges have not yet been upgraded.

VMware recommends that you upgrade all NSX components in a single outage window to minimize downtime and reduce confusion among NSX users who cannot access certain NSX 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 NSX users understand what features are available during the upgrade.

An NSX deployment upgrade proceeds as follows:

NSX Manager → NSX Controller Cluster → NSX Host Clusters → Distributed Logical Routers → Guest Introspection

Edge Services Gateways can be upgraded at any time after the NSX Manager upgrade.

---

**Important** Before you start the upgrade, read [Preparing for the NSX Upgrade](#) and the *NSX for vSphere Release Notes* for detailed information about upgrade prerequisites and upgrade known issues.

---

### NSX Manager Upgrade

Planning the NSX Manager upgrade:

- In a cross-vCenter NSX environment, you must upgrade the primary NSX Manager first, and then upgrade secondary NSX Managers.
- In a cross-vCenter NSX environment you must upgrade all NSX Managers in the same maintenance window.

Impact during the NSX Manager upgrade:

- NSX Manager configuration using the vSphere Web Client and API is blocked.
- Existing VM communication continues to function.
- New VM provisioning continues to work in vSphere, but the new VMs cannot be connected to NSX or disconnected from logical switches during the NSX Manager upgrade.
- During the NSX Manager upgrade in a cross-vCenter NSX environment, do not make any changes to universal objects until the primary and all secondary NSX Managers are upgraded. This includes create, update, or delete of universal objects, and operations involving universal objects (for example, apply a universal security tag to a VM).

After the NSX Manager upgrade:

- All NSX configuration changes are allowed.
- At this stage, if any new NSX Controller appliances are deployed, they will be deployed with the version matching the existing NSX Controller cluster until the NSX Controller cluster is upgraded.

- Changes to the existing NSX configuration are allowed. New logical switches, logical routers, and edge service gateways can be deployed.
- For distributed firewall, if new features are introduced after the upgrade, you cannot use them until all hosts are upgraded.
- Depending on the NSX release, once the NSX Manager has been upgraded, the Communication Channel Health status will display as Unknown for the control plane. You must complete the controller and host upgrades to see a status of Up.

## NSX Controller Cluster Upgrade

Planning the NSX Controller upgrade:

- You can upgrade the NSX Controller cluster after NSX Manager is upgraded.
- In a cross-vCenter NSX environment, you must upgrade all NSX Managers before upgrading the NSX Controller cluster.
- VMware highly recommends upgrading the NSX Controller cluster in the same maintenance window as the NSX Manager upgrade.

Impact during the NSX Controller upgrade:

- Logical network creation and modifications are blocked during the upgrade process. Do not make logical network configuration changes while the NSX Controller cluster upgrade is in progress.
- Do not provision new VMs during this process. Also, do not move VMs or allow DRS to move VMs during the upgrade.
- During the upgrade, when there is a temporary non-majority state, existing virtual machines do not lose networking.
- Do not allow dynamic routes to change during the upgrade.

After the NSX Controller upgrade:

- Configuration changes are allowed.

## NSX Host Upgrade

Planning the NSX host cluster upgrade:

- You can upgrade host clusters after NSX Managers and the NSX Controller cluster are upgraded.
- You can upgrade your host clusters in a separate maintenance window from the NSX Manager and NSX Controller cluster upgrades.
- You do not need to upgrade all host clusters in the same maintenance window. However, if Distributed Firewall is enabled, there is a limitation on migrating VMs between clusters with different NSX versions:
  - Migrating VMs from clusters with a later version of NSX to clusters with an earlier version of NSX might cause the VMs to lose network connectivity.
  - Migrating VMs from clusters with an earlier version of NSX to clusters with a later version of NSX is supported.

- New features of the NSX version installed on NSX Manager appear in the vSphere Web Client and the API, but might not function until the VIBs are upgraded.
- To take advantage of all the new features of an NSX release, upgrade the host clusters so that the host VIBs match the NSX Manager version.

Impact during the NSX host cluster upgrade:

- Configuration changes are not blocked on NSX Manager.
- Controller-to-host communication is backward compatible, meaning that upgraded controllers can communicate with non-upgraded hosts.
- Upgrade is performed on a per-cluster basis. If DRS is enabled on the cluster, DRS manages the upgrade order of the hosts.
- Hosts currently undergoing upgrade must be placed in maintenance mode, so VMs must be powered off or evacuated to other hosts. This can be done with DRS or manually.
- Additions and changes to logical network are allowed.
- Provisioning of new VMs continues to work on hosts that are not currently in maintenance mode.

## NSX Edge Upgrade

Planning the NSX Edge upgrade:

- You can upgrade NSX Edges in separate maintenance windows from other NSX components.
- You can upgrade Logical Routers after NSX Managers, NSX Controller cluster, and host clusters are upgraded.
- You can upgrade an Edge Services Gateway even if you have not yet upgraded the NSX Controller cluster or host clusters.
- You do not need to upgrade all NSX Edges in the same maintenance window.
- If an upgrade is available for NSX Edge but you have not upgraded, changing size, resources, datastore, enabling advanced debugging, and enabling HA on the appliance will be blocked until the NSX Edge is upgraded.

Impact during the NSX Edge upgrade:

- On the NSX Edge device currently being upgraded, configuration changes are blocked. Additions and changes to logical switches are allowed. Provisioning new VMs continues to work.
- Packet forwarding is temporarily interrupted.
- In NSX Edge 6.0 and later, OSPF adjacencies are withdrawn during upgrade if graceful restart is not enabled.

After the NSX Edge upgrade:

- Configuration changes are not blocked.

## Guest Introspection Upgrade

Planning the Guest Introspection upgrade:

- You can upgrade Guest Introspection after NSX Managers, NSX Controller cluster, and host clusters are upgraded.
- See the partner documentation for partner solution upgrade information.

Impact during the Guest Introspection upgrade:

- 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 the Guest Introspection upgrade:

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

## Understand FIPS Mode and NSX Upgrade

Starting in NSX 6.3.0, you can enable FIPS mode, which turns on the cipher suites that comply with FIPS.

**Caution** When you upgrade from a version of NSX earlier than NSX 6.3.0 to NSX 6.3.0 or later, you must not enable FIPS mode before the upgrade is completed. Enabling FIPS mode before the upgrade is complete will interrupt communication between upgraded and not-upgraded components.

## NSX Upgrade and FIPS Status

**Table 1-1. FIPS mode status in NSX components after upgrade to NSX 6.3.x.**

NSX Component	FIPS Mode Status
NSX Manager	After upgrade to 6.3.x, FIPS mode on NSX Manager appliances is available and turned off. Do not enable FIPS until upgrade of all NSX components is complete, and FIPS has been enabled on all NSX Edge appliances.
NSX Controller cluster	After upgrade to 6.3.x, the NSX Controller cluster is FIPS compliant. This is not configurable.
NSX host cluster	After upgrade to 6.3.x, NSX host clusters are FIPS compliant. This is not configurable.
NSX Edge	After upgrade to 6.3.x, FIPS mode on NSX Edge appliances is available and turned off. Do not enable FIPS until upgrade of all NSX components is complete.
Guest Introspection service VM	After upgrade to 6.3.x, the Guest Introspection service VM is FIPS compliant. This is not configurable.

## Enable FIPS

If you are upgrading to NSX 6.3.x and want to enable FIPS, you must complete the following steps:

- 1 Verify any partner solutions are FIPS mode certified. See the VMware Compatibility Guide at <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>. Check the partner documentation for information.
- 2 Upgrade NSX Manager to NSX 6.3.0 or later.

- 3 Upgrade the NSX Controller cluster to NSX 6.3.0 or later.
- 4 Upgrade all host clusters running NSX workloads to NSX 6.3.0 or later.
- 5 Upgrade all NSX Edge appliances to NSX 6.3.0 or later.
- 6 If installed, upgrade Guest Introspection on all host clusters to NSX 6.3.0 or later.
- 7 Enable FIPS mode on NSX Edge appliances. See *Change FIPS Mode on NSX Edge* in the *NSX Administration Guide*.
- 8 Enable FIPS mode on the NSX Manager appliances. See *Change FIPS Mode and TLS Settings on NSX Manager* in the *NSX Administration Guide*.

## Verify the NSX Working State

Before beginning the upgrade, it is important to test the NSX 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 NSX infrastructure. Make sure to check it first.

### Procedure

- 1 Note the current versions of NSX Manager, vCenter Server, ESXi and NSX Edges.
- 2 Identify administrative user IDs and passwords.
- 3 Verify you can log into the following components:
  - vCenter Server
  - NSX Manager Web UI
  - Edge services gateway appliances
  - Distributed logical router appliances
  - NSX Controller appliances
- 4 Verify that VXLAN segments are functional.

Make sure to set the packet size correctly and include the don't fragment bit.

- Ping between two VMs that are on same logical switch but on two different hosts.
  - From a Windows VM: ping -l 1472 -f <dest VM>
  - From a Linux VM: ping -s 1472 -M do <dest VM>
- Ping between two hosts' VTEP interfaces.
  - ping ++netstack=vxlan -d -s 1572 <dest VTEP IP>

---

**Note** To get a host's VTEP IP, look up the vmknicPG IP address on the host's **Manage > Networking > Virtual Switches** page.

---



- 5 Validate North-South connectivity by pinging out from a VM.
- 6 Visually inspect the NSX environment to make sure all status indicators are green/normal/deployed.
  - Check **Installation > Management**.
  - Check **Installation > Host Preparation**.
  - Check **Installation > Logical Network Preparation > VXLAN Transport**.
  - Check **Logical Switches**.
  - Check **NSX Edges**.
- 7 Record BGP and OSPF states on the NSX Edge devices
  - `show ip ospf neighbor`
  - `show ip bgp neighbor`
  - `show ip route`
- 8 Verify that syslog is configured.  
See [Specify a Syslog Server](#).
- 9 If possible, in the pre-upgrade environment, create some new components and test their functionality.
  - Create a new logical switch.
  - Create a new edge services gateway and a new distributed logical router.
  - Connect a VM to the new logical switch and test the functionality.
- 10 Validate netcpad and vsfwd user-world agent (UWA) connections.
  - On an ESXi host, run `esxcli network vswitch dvs vmware vxlan network list --vds-name=<VDS_name>` and check the controller connection state.
  - On NSX Manager, run the `show tech-support save session` command, and search for "5671" to ensure that all hosts are connected to NSX Manager.
- 11 (Optional) If you have a test environment, test the upgrade and post-upgrade functionality before upgrading a production environment.

## Uninstall NSX Data Security

NSX Data Security was deprecated in NSX 6.2.3, and has been removed from NSX 6.3.0. You must uninstall NSX Data Security before upgrading to NSX 6.3.x.

### Procedure

- 1 In the **Installation** tab, click **Service Deployments**.
- 2 Select the NSX Data Security service and click the **Delete Service Deployment** (✖) icon.
- 3 In the Confirm Delete dialog box, click **Delete now** or select a date and time for the delete to take effect.

4 Click **OK**.

## NSX Backup and Restore

Proper backup of all NSX components is crucial to restore the system to its working state in the event of a failure.

The NSX Manager backup contains all of the NSX configuration, including controllers, logical switching and routing entities, security, firewall rules, and everything else that you configure within the NSX 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 NSX Manager and vCenter. Your backup frequency and schedule might vary based on your business needs and operational procedures. We recommend taking NSX backups frequently during times of frequent configuration changes.

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

We recommend taking backups in the following scenarios:

- Before an NSX or vCenter upgrade.
- After an NSX or vCenter upgrade.
- After Day Zero deployment and initial configuration of NSX components, such as after the creation of NSX Controllers, logical switches, logical routers, edge services gateways, 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 NSX component backups (such as NSX Manager) with your backup schedule for other interacting components, such as vCenter, cloud management systems, operational tools, and so on.

### Back Up and Restore NSX Manager

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.

### Back Up NSX Manager Data

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

**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*.

---

**Note** Files in the Backup Directory must be limited to 100. If number of files in the directory exceeds the limit, you will receive a warning message.

---

- g Type the pass phrase to secure the backup.  
You will need this pass phrase to restore the backup.
- h Click **OK**.

For example:

- 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.

- 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.

## Restore an NSX Manager Backup

Restoring NSX Manager causes a backup file to be loaded on an NSX Manager appliance. The backup file must be saved to a remote FTP or SFTP location that NSX Manager can access. NSX Manager data includes configuration, events, and audit log tables.

---

**Important** Back up your current data before restoring a backup file.

---

### Prerequisites

Before restoring NSX Manager data, we recommend reinstalling the NSX Manager appliance. Running the restore operation on an existing NSX Manager appliance might work, too, but is not supported. The assumption is that the existing NSX Manager has failed, and therefore a new NSX Manager appliance is deployed.

The best practice is to take note of the current settings for the old NSX Manager appliance so that they can be used to specify IP information and backup location information for the newly deployed NSX Manager appliance.

### Procedure

- 1 Take note of all settings on the existing NSX Manager appliance. Also, note down FTP server settings.
- 2 Deploy a new NSX Manager appliance.  
The version must be the same as the backed up NSX Manager appliance.
- 3 Log in to the new NSX Manager appliance.
- 4 Under Appliance Management, click **Backups & Restore**.
- 5 In FTP Server Settings, click **Change** and add the FTP server settings.

The **Host IP Address**, **User Name**, **Password**, **Backup Directory**, **Filename Prefix**, and **Pass Phrase** fields in the Backup Location screen must identify the location of the backup to be restored.

The **Backup History** section displays the backup folder.

---

**Note** If the backup folder does not appear in the **Backup History** section, verify the FTP server settings. Check if you can connect to FTP server and view the backup folder.

---

- 6 In the **Backup History** section, select the required backup folder to restore, and click **Restore**.  
Restoring the NSX Manager data begins.

NSX configuration is restored to the NSX Manager.

---


**Caution** After restoring an NSX Manager backup, you might need to take additional action to ensure correct operation of NSX Edge appliances and logical switches. See [Restore NSX Edges](#) and [Resolve Out of Sync Errors on Logical Switches](#).

---

## **Restore NSX Edges**

All NSX Edge configurations (logical routers and edge services gateways) are backed up as part of NSX Manager data backup.

Taking individual NSX Edge backups is not supported.

If you have an intact NSX Manager configuration, you can recreate an inaccessible or failed Edge appliance VM by redeploying the NSX Edge (click **Redeploy NSX Edge** (  ) in the vSphere Web Client). See "Redeploy NSX Edge" in the *NSX Administration Guide*.

---

**Caution** After restoring an NSX Manager backup, you might need to take additional action to ensure correct operation of NSX Edge appliances.

- Edge appliances created after last backup are not removed during restore. You must delete the VM manually.
- Edge appliances deleted after the last backup are not restored unless redeployed.
- If both the configured and current locations of an NSX Edge appliance saved in the backup no longer exist when the backup is restored, operations such as redeploy, migrate, enable or disable HA will fail. You must edit the appliance configuration and provide valid location information. Use `PUT /api/4.0/edges/{edgeId}/appliances` to edit the appliance location configuration (*resourcePoolId*, *datastoreId*, *hostId* and *vmFolderId* as necessary). See "Working With NSX Edge Appliance Configuration" in the *NSX API Guide*.

If any of the following changes have occurred since the last NSX Manager backup, the restored NSX Manager configuration and the configuration present on the NSX Edge appliance will differ. You must **Force Sync** the NSX Edge to revert these changes on the appliance and ensure correct operation of the NSX Edge. See "Force Sync NSX Edge with NSX Manager" in the *NSX Administration Guide*.

- Changes made via Distributed Firewall for preRules for NSX Edge firewall.
- Changes in grouping objects membership.

If any of the following changes have occurred since the last NSX Manager backup, the restored NSX Manager configuration and the configuration present on the NSX Edge appliance will differ. You must **Redeploy** the NSX Edge to revert these changes on the appliance and ensure correct operation of the NSX Edge. See "Redeploy NSX Edge" in the *NSX Administration Guide*.

- Changes in Edge appliance settings:
  - HA enabled or disabled
  - appliance moved from deployed to undeployed state
  - appliance moved from undeployed to deployed state
  - resource reservation settings have been changed
- Changes in Edge appliance vNic settings:
  - add, remove, or disconnect vNic
  - port groups
  - trunk ports
  - fence parameters
  - shaping policy

## Resolve Out of Sync Errors on Logical Switches

If logical switch changes have occurred between taking the NSX Manager backup and restoring the backup, logical switches might report being out of sync.

### Procedure

- 1 Log in to the vSphere Web Client.
- 2 Navigate to **Networking & Security > Logical Switches**.
- 3 If present, click the **Out of sync** link in the Status column to display error details.
- 4 Click **Resolve** to recreate missing backing port groups for the logical switch.

## 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.

vSphere Distributed Switch settings and port-group settings are imported as part of the import.

As a best practice, export the vSphere Distributed Switch 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>

## Managing NSX Manager Backups Created During Upgrade

When you upgrade NSX Manager to NSX 6.3.6, a backup is taken and saved locally as part of the upgrade process. You must contact VMware customer support to restore this backup. This automatic backup is intended as a failsafe in case the regular backup fails.



After NSX Manager is successfully upgraded, new commands are available in privileged (**enable**) mode to allow you to manage the backup files. You can use these commands to list, copy, or delete the backup files.

If you don't delete them, the backup files remain in place until the next upgrade. When the next upgrade is started, the backup files are deleted, and a new backup is taken.

## show backup

List the backup files.

```
nsxmgr-01a.corp.local# show backup
total 3040
-rw-r--r-- 1 root root 3102752 Mar 23 01:12 backup_file
-rw-r--r-- 1 root root      230 Mar 23 01:12 backup_metadata
```

## export backup

Copy the backup files to another location.

```
nsxmgr-01a.corp.local# export backup scp root@backup-server:/backups
Exporting...
Password:
backup_file                100% 3030KB  19.8MB/s   00:00
backup_metadata            100% 230      27.3KB/s   00:00
nsxmgr-01a.corp.local#
```

## delete backup

Delete the backup files. Only delete the backup if you are sure that you no longer need it.

```
nsxmgr-01a.corp.local# delete backup
Do you want to delete the backup files (y|N)y
nsxmgr-01a.corp.local#
```

## Download the NSX Upgrade Bundle and Check the MD5

The NSX Upgrade Bundle contains all the files needed to upgrade the NSX infrastructure. Before upgrading NSX 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 NSX upgrade bundle to a location NSX Manager can browse to. The name of the upgrade bundle file has a format similar to `VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz`.

- 2 Verify the NSX Manager upgrade filename ends with tar.gz.

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

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

Change it to:

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

Otherwise, after uploading the upgrade bundle, the following error message appears: "Invalid upgrade bundle file VMware-NSX-Manager-upgrade-bundle-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 to NSX 6.3.x

To upgrade to NSX 6.3.x, you must upgrade the NSX components in the order in which they are documented in this guide.

NSX components must be upgraded in the following order:

- 1 NSX Manager appliance
- 2 NSX Controller cluster
- 3 Host clusters
- 4 NSX Edge (see Note)
- 5 Guest Introspection

---

**Note** Edge Services Gateways can be upgraded at any time after the NSX Manager upgrade. However, logical routers cannot be upgraded until the NSX Controller cluster and host clusters have been upgraded. See [Operational Impacts of NSX Upgrades](#) for more information about upgrade dependencies.

---

The upgrade process is managed by the NSX Manager. If the upgrade of a component fails or is interrupted and you need to repeat or restart the upgrade, the process begins from the point at which it stopped; it does not start over from the beginning.

The upgrade status is updated for each node and at the cluster level.

## Upgrade NSX Manager

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

During the upgrade, you can choose to join the Customer Experience Improvement Program (CEIP) for NSX. See Customer Experience Improvement Program in the *NSX Administration Guide* for more information about the program, including how to join or leave the program.

If you are upgrading from NSX 6.3.0 or later, uploading the upgrade bundle and starting the upgrade can happen independently. To start an upgrade from a previously uploaded upgrade bundle, navigate to **Home > Upgrade** and click **Begin Upgrade**.

When you upgrade NSX Manager to NSX 6.3.6, a backup is automatically taken and saved locally as part of the upgrade process. See [Managing NSX Manager Backups Created During Upgrade](#) for information about managing these backup files.

- If the automatic backup taken during the upgrade fails, the upgrade will not continue. Contact VMware customer support for assistance.
- The automatic backup is intended as a failsafe in case your regular backup fails.
  - Always take a regular NSX Manager backup before upgrading. See [Back Up NSX Manager Data](#) for more information. You can restore this backup without assistance from VMware customer support.
  - If you need to restore the automatic backup, you must contact VMware customer support.

### Prerequisites

- Validate the NSX Manager file system usage, and perform a cleanup if file system usage is at 100 percent.
  - a Log in to NSX Manager and run `show filesystems` to show the filesystem usage.
  - b If the usage is 100 percent, enter privileged (enable) mode, and run the `purge log manager` and `purge log system` commands.
  - c Reboot the NSX Manager appliance for the log cleanup to take effect.
- Verify the NSX Manager virtual appliance reserved memory meets the system requirements before upgrading.
 

See [System Requirements for NSX](#).
- If you have Data Security in your environment, uninstall it before upgrading NSX Manager. See [Uninstall NSX Data Security](#). Data Security has been removed from NSX 6.3.x.
- Back up your current configuration and download technical support logs before upgrading. See [NSX Backup and Restore](#).
- Download the upgrade bundle and check the MD5. See [Download the NSX Upgrade Bundle and Check the MD5](#).
- Make sure that you understand the operational impact of the NSX Manager upgrade while the upgrade is in progress. See [Operational Impacts of NSX Upgrades](#).

- You must upgrade all NSX Managers in a cross-vCenter NSX environment in the same maintenance window.
- Determine which NSX Managers must be upgraded in the same maintenance window.
  - If you have a cross-vCenter NSX environment, you must upgrade the primary and all secondary NSX Managers to the same NSX version in a single maintenance window.
  - If you have multiple NSX Managers connected to vCenter Server systems that use the same SSO server, not all combinations of NSX Manager version are supported. You must plan the upgrade of your NSX Managers so that you have a supported configuration at the end of the maintenance window
    - All NSX Managers using the same version of NSX is supported.
    - NSX Managers using different version of NSX is supported if at least one NSX Manager has NSX 6.4.0 or later installed, and all other NSX Managers have NSX 6.3.3 or later installed.

### Procedure

- 1 Log in to the NSX Manager virtual appliance.
- 2 From the home page, click **Upgrade**.
- 3 Click **Upgrade**, then click **Choose File** and browse to the `VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz` file. Click **Continue** to start the upload.

The upload status displays in the browser window.

- 4 If you want to start the upgrade later, click **Close** in the Upgrade dialog box.
 

When you are ready to start the upgrade, navigate to **Home > Upgrade** and click **Begin Upgrade**.
- 5 In the Upgrade dialog box, select whether you want to enable SSH, and whether you want to participate in VMware's Customer Experience Improvement Program ("CEIP"). Click **Upgrade** to start the upgrade.

The upgrade status displays in the browser window.

---

**Note** The Upgrade dialog box displays a message indicating that the automatic backup has been taken.

---

Wait until the upgrade procedure finishes and the NSX Manager login page appears.

- 6 Log in to the NSX Manager virtual appliance again, and from the home page click **Upgrade**. Confirm that the upgrade state is **Complete**, and the version and build number on the top right matches the upgrade bundle you just installed.

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.

After the NSX Manager is upgraded, create a new NSX Manager backup file. See [NSX Backup and Restore](#) . The previous NSX Manager backup is only valid for the previous release.

### What to do next

Upgrade the NSX Controller cluster.

## Upgrade the NSX Controller Cluster

The controllers in your environment are upgraded at the cluster level. If an upgrade is available for a controller node, an upgrade link appears in the NSX Manager.

It is recommended that you upgrade the controllers during a maintenance window.

The NSX Controller upgrade causes an upgrade file to be downloaded to each controller node. The controllers are upgraded one at a time. While an upgrade is in progress, the **Upgrade Available** link is not clickable, and API calls to upgrade the controller cluster are blocked until the upgrade is complete.

If you deploy new controllers before the existing controllers are upgraded, they are deployed as the old version. Controller nodes must be the same version to join a cluster.

---

**Important** In NSX 6.3.3 the underlying operating system of the NSX Controller changes. This means that when you upgrade from NSX 6.3.2 or earlier to NSX 6.3.3 or later, instead of an in-place software upgrade, the existing controllers are deleted one at a time, and new Photon OS based controllers are deployed using the same IP addresses.

When the controllers are deleted, this also deletes any associated DRS anti-affinity rules. You must create new anti-affinity rules in vCenter to prevent the new controller VMs from residing on the same host.

---

## Prerequisites

- Ensure that all of the controllers are in the normal state. Upgrading is not possible when one or more of the controllers are in the disconnected state. To reconnect a disconnected controller, try resetting the controller virtual appliance. In the **Hosts and Clusters** view, right-click the controller and select **Power > Reset**.
- A valid NSX Controller cluster contains three controller nodes. Log in to the three controller nodes and run the **show control-cluster status** command.

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

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

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

- For Join status, verify the controller node is reporting Join Complete.
  - For Majority status, verify the controller is connected to the cluster majority.
  - For Cluster ID, all the controller nodes in a cluster should have the same cluster ID.
  - For Configured status and Active status, verify that the all the controller roles are enabled and activated.
- Make sure that you understand the operational impact of the NSX Controller upgrade while the upgrade is in progress. See [Operational Impacts of NSX Upgrades](#).
  - If you are upgrading to NSX 6.3.3 the NSX Controller cluster must contain three controller nodes. If it has fewer than three you must add additional nodes before starting the upgrade. See "Deploy NSX Controller Cluster" in the *NSX Installation Guide* for steps to add controller nodes.

## Procedure

- ◆ Navigate to **Home > Networking & Security > Installation**, select the **Management** tab, and click **Upgrade Available** in the **Controller Cluster Status** column.

The controllers in your environment are upgraded and rebooted one at a time. After you initiate the upgrade, the system downloads the upgrade file, upgrades each controller, reboots each controller, and updates the upgrade status of each controller. The following fields display controller status:

- The **Controller Cluster Status** column in the NSX Manager section displays the upgrade status of the cluster. When the upgrade begins, the status says **Downloading upgrade file**. When the upgrade file has been downloaded on all controllers in the cluster, the status changes to **In progress**. After all the controllers in the cluster have been upgraded, the status displayed is **Complete**, and then this column is no longer displayed.
- The **Status** column in the NSX Controller nodes section displays the status of each controller, which is **Connected** or **Normal** before the upgrade, depending on the original NSX version. When the controller services are shut down and the controller is rebooted, the status changes to **Disconnected**. After the upgrade for that controller is complete, the status is **Connected**.
- The **Upgrade Status** column in the NSX Controller nodes section displays the upgrade status for each controller. The status displays **Downloading upgrade file** to begin with, then displays **Upgrade in progress**, and then **Rebooting**. After the controller is upgraded, the status displays **Upgraded**.

---

**Note** When you upgrade from NSX 6.3.2 or earlier to NSX 6.3.3 or later, the **Downloading upgrade file** status is replaced with **Queued For Upgrade**.

---

When the upgrade is complete, the **Software Version** column in the NSX Controller nodes section displays **6.3.buildNumber** for each controller. Rerun the **show control-cluster status** command to make sure the controllers are able to create a majority. If the NSX Controller cluster majority is not re-formed review controller and NSX Manager logs.

The average upgrade time for each upgrade is 6-8 minutes. If the upgrade does not complete within the timeout period (30 minutes), the **Upgrade Status** column displays **Failed**. Click **Upgrade Available** in the NSX Manager section again to resume the upgrade process from the point where it stopped.

If network issues are preventing a successful upgrade within the 30-minute timeout period, you may need to configure a longer timeout period. Work with VMware Support to diagnose and resolve any underlying issues and, if needed, configure a longer timeout period.

If the controller upgrade fails, check connectivity between the controllers and the NSX Manager.

There is a scenario in which the first controller upgrades successfully, and the second controller does not. Assuming you have three controllers in a cluster, the first controller is successfully upgraded to the new version, and the second controller is being upgraded. If the upgrade of the second controller fails, the second controller might be left in a disconnected state. At the same time, the first and third controllers now have two different versions (one upgraded, one not) and are therefore unable to form a majority. At

this point, the upgrade cannot be relaunched. To work around this scenario, create another controller. The newly created controller will be of the older version (matching controller three) and will therefore form a majority with controller three. At this point, you can relaunch the upgrade procedure. See [Redeploy an NSX Controller](#) in the *NSX Troubleshooting Guide* for instructions on creating another controller.

### What to do next

Upgrade the host clusters.

## Upgrade Host Clusters

After upgrading NSX Manager and NSX Controllers, you can update the appropriate clusters in your environment.

Upgrading the host clusters upgrades the NSX VIBs.

If you are upgrading from NSX 6.2.x or earlier, or if you are upgrading from NSX 6.3.0 or later with ESXi 5.5, hosts must be rebooted to complete the upgrade.

- If the cluster has DRS enabled, when you click **Resolve all** DRS attempts to reboot the hosts in a controlled fashion that allows the VMs to continue running. VMs are moved to other hosts in the cluster and the hosts enter maintenance mode and are rebooted.
- If the cluster does not have DRS enabled, you must power off or vMotion the VMs manually before beginning the upgrade. When you click **Resolve all** the hosts enter maintenance mode and are rebooted.

If you are upgrading from NSX 6.3.0 or later with ESXi 6.0 or later, the hosts must enter maintenance mode to complete the upgrade. Rebooting is not required.

- If the cluster has DRS enabled, when you click **Resolve all** DRS attempts to put the hosts into maintenance mode in a controlled fashion that allows the VMs to continue running. VMs are moved to other hosts in the cluster and the hosts enter maintenance mode.
- If the cluster does not have DRS enabled, you must power off or vMotion the VMs manually before beginning the upgrade. You must manually put the hosts into maintenance mode to complete the upgrade.

In NSX 6.3.5 and later you can view the EAM status on the **Host Preparation** tab.

### Prerequisites

- Upgrade NSX Manager and the NSX Controller cluster.
- Log out of and log back in to the vSphere Web client after upgrading NSX Manager and before upgrading the host clusters.
- Make sure that you understand the operational impact of a host cluster upgrade while the upgrade is in progress. See [Operational Impacts of NSX Upgrades](#).
- Make sure the fully qualified domain names (FQDNs) of all of your hosts can be resolved.
- If DRS is disabled, power off or vMotion the VMs manually before beginning the upgrade.



- If DRS is enabled, the running VMs are moved automatically during the host cluster upgrade. Before beginning the upgrade, make sure that DRS can work in your environment.
  - Make sure that DRS is enabled on the host clusters.
  - Make sure that vMotion functions correctly.
  - Check the host connection state with vCenter.
  - Check that you have a minimum three ESXi hosts in each host cluster. During an NSX upgrade, a host cluster with only one or two hosts is more likely to have issues with DRS admission control. For a successful NSX upgrade, VMware recommends that each host cluster have at least three hosts. If a cluster contains fewer than three hosts, the recommendation is to manually evacuate the hosts.
  - In a small cluster with only two or three hosts, if you have created anti-affinity rules stating that certain VMs must reside on separate hosts, these rules might prevent DRS from moving the VMs during the upgrade. Either add additional hosts to the cluster or disable the anti-affinity rules during the upgrade and reenable them after the upgrade is complete. To disable an anti-affinity rule, navigate to **Hosts and Clusters > Cluster > Manage > Settings > VM/Host Rules**. Edit the rule and deselect **Enable rule**.
- Log into one of the hosts in the cluster and run the `esxcli software vib list` command.

The VIBs present will depend on the ESXi and NSX versions, and therefore might change as part of the upgrade. Note the current version of the installed VIBs:

ESXi version	NSX version	VIBs installed
5.5	6.1.x, 6.2.x or 6.3.x	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 or later	6.3.2 or earlier	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 or later	6.3.3 or later	<ul style="list-style-type: none"> <li>■ esx-nsxv</li> </ul>

**Note** Some versions of NSX have additional VIBs which will be removed during the upgrade.


- If you are upgrading from a version of NSX earlier than NSX 6.2, prepared hosts have an additional VIB, `esx-dvfilter-switch-security`.
- If you are upgrading from NSX 6.2.x where the version is NSX 6.2.4 or later, prepared hosts have an additional VIB, `esx-vdpi`.



## Procedure

- 1 In the vSphere Web Client, navigate to **Home > Networking & Security > Installation**, select the **Host Preparation** tab.

- 2 For each cluster that you want to upgrade, click **Upgrade available**.

**NSX Component Installation on Hosts**

 **Actions**

Clusters & Hosts	Installation Status	Firewall	VXLAN
▶  Compute Cluster A	✓ 6.2.0 <b>Upgrade available</b>	✓ Enabled	✓ Configured
▶  Management & Edge Cluster	✓ 6.2.0 Upgrade available	✓ Enabled	✓ Configured

The Installation Status displays *Installing*.

- 3 The cluster Installation Status displays *Not Ready*. Click **Not Ready** to display more information. Click **Resolve all** to attempt to complete the VIB installation.

The hosts are put in maintenance mode, and rebooted if required, to complete the upgrade.

The Installation Status column displays *Installing*. Once the upgrade is complete the Installation Status column displays a green check mark and the upgraded NSX version.

- 4 If the **Resolve** action fails when DRS is enabled, the hosts might require manual intervention to enter maintenance mode (for example, due to HA requirements or DRS rules), the upgrade process stops and the cluster Installation Status displays *Not Ready* again. Click **Not Ready** to display more information. Check the hosts in the **Hosts and Clusters** view, make sure the hosts are powered on, connected, and contain no running VMs. Then retry the **Resolve** action.

The Installation Status column displays *Installing*. Once the upgrade is complete the Installation Status column displays a green check mark and the upgraded NSX version.

- 5 If the **Resolve** action fails when DRS is disabled and you are upgrading from NSX 6.3.0 or later with ESXi 6.0 or later, you must manually put the hosts into maintenance mode to complete the upgrade.
- Place the evacuated hosts in maintenance mode.
  - Navigate to **Networking & Security > Installation > Host Preparation**.

The upgrade automatically starts when the hosts enter maintenance mode. The Installation Status column displays *Installing*. If you do not see the *Installing* status, refresh the page.

Once the upgrade is complete the Installation Status column displays a green check mark and the upgraded NSX version.

- Remove the hosts from maintenance mode.

To confirm the host update, log into one of the hosts in the cluster and run the `esxcli software vib list` command. Make sure that the appropriate VIBs have been updated to the expected version.

If a host fails to upgrade, perform the following troubleshooting steps:

- Check the ESX Agent Manager on vCenter, and look for alerts and errors.
- Log in to the host, check the `/var/log/esxupdate.log` log file, and look for recent alerts and errors.

- Ensure that DNS and NTP are configured on the host.

See "Host Preparation" in the *NSX Troubleshooting Guide* for more troubleshooting steps.

### What to do next

#### [Upgrade NSX Edge](#)

## Upgrade NSX Edge

During the upgrade process, a new Edge virtual appliance is deployed alongside the existing one.

When the new Edge is ready, the old Edge's vNICs are disconnected and the new Edge's vNICs are connected. The new Edge then sends gratuitous ARP (GARP) packets to update the ARP cache of connected switches. When HA is deployed, the upgrade process is performed two times.

This process can temporarily affect packet forwarding. You can minimize the impact by configuring the Edge to work in ECMP mode.

OSPF adjacencies are withdrawn during upgrade if graceful restart is not enabled.

### Prerequisites

- Verify that NSX Manager has been upgraded.
- Verify that the NSX Controller cluster and host preparation have been upgraded before upgrading logical routers.
- Verify that there is a local segment ID pool, even if you have no plans to create NSX logical switches.
- Verify the hosts have enough resources to deploy additional NSX Edge Services Gateway appliances during the upgrade, particularly if you are upgrading multiple NSX Edge appliances in parallel. See the [System Requirements for NSX](#) for the resources required for each NSX Edge size.
  - For a single NSX Edge instance, there are two NSX Edge appliances of the appropriate size in the poweredOn state during upgrade.
  - For an NSX Edge instance with high availability, both replacement appliances are deployed before replacing the old appliances. This means there are four NSX Edge appliances of the appropriate size in the poweredOn state during upgrade of a given NSX Edge. Once the NSX Edge instance is upgraded, either of the HA appliances could become active.
- Verify that the host clusters listed in the configured location and live location for the NSX Edge appliance are prepared for NSX and that their messaging infrastructure status is GREEN. If the configured location is not available, for example, because the cluster has been removed since the NSX Edge appliance was created, then verify the live location only.
  - Find the ID of the original configured location (*configuredResourcePool > id*) and the current live location (*resourcePoolId*) with the GET `https://NSX-Manager-IP-Address/api/4.0/edges/{edgeId}/appliances` API request.

- Find the host preparation status and the messaging infrastructure status for those clusters with the GET `https://NSX-Manager-IP-Address/api/2.0/nwfabric/status?resource={resourceId}` API request, where *resourceId* is the ID of the configured and live location of the NSX Edge appliances found previously.
- Look for the status corresponding to the *featureId* of `com.vmware.vshield.vsm.nwfabric.hostPrep` in the response body. The status must be GREEN.

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

- Look for the status corresponding to the *featureId* of `com.vmware.vshield.vsm.messagingInfra` in the response body. The status must be GREEN.

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

- Understand the operational impact of the NSX Edge upgrade while the upgrade is in progress. See *Operational Impacts of NSX Upgrades* in the *NSX Upgrade Guide*.
- If you are upgrading from NSX 6.0.x and you have L2 VPN enabled on an NSX Edge you must delete the L2 VPN configuration before you upgrade. Once you have upgraded, you can reconfigure L2 VPN. See "L2 VPN Overview" in the *NSX Installation Guide*.

## Procedure

- 1 In the vSphere Web Client, select **Networking & Security > NSX Edges**.
- 2 For each NSX Edge instance, select **Upgrade Version** from the **Actions** (⚙️) menu.

If the upgrade fails with the error message "Failed to deploy edge appliance," make sure that the host on which the NSX edge appliance is deployed is connected and not in maintenance mode.

After the NSX Edge is upgraded successfully, the **Status** is Deployed, and the **Version** column displays the new NSX version.

If an Edge fails to upgrade and does not rollback to the old version, click the **Redeploy NSX Edge** icon and then retry the upgrade.

### What to do next

After you upgrade your 6.2.4 or earlier NSX Edges to 6.2.5 or later, you must turn off vSphere Virtual Machine Startup for each NSX Edge in a cluster where vSphere HA is enabled and Edges are deployed. To do this, open the vSphere web client and find the ESXi host where NSX Edge virtual machine resides. Click **Manage > Settings** and under Virtual Machines, select VM Startup/Shutdown, click **Edit**, and make sure that the virtual machine is in Manual mode (that is, make sure it is not added to the Automatic Startup/Shutdown list).

## Upgrade Guest Introspection

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

Upgrade NSX Manager, controllers, prepared host clusters, and NSX Edges.

### Procedure

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

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 \* ds-site-a-nfs01

Network \* vds-site-a\_Management...

IP assignment \* GI Pool

**Specify schedule:**

Upgrade now

Schedule the upgrade   6:29 PM

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.

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.

## NSX Services That Do Not Support Direct Upgrade

Some NSX services do not support a direct upgrade. In these cases, you must uninstall and reinstall the services.

### VMware Partner Security Virtual Appliances

Check the partner documentation to verify if the partner security virtual appliance can be upgraded.

### NSX SSL VPN

Starting in NSX 6.2, the SSL VPN gateway only accepts the TLS protocol. However, after upgrading to NSX 6.2 or later, any new clients that you create automatically use the TLS protocol during connection establishment. Additionally, starting in NSX 6.2.3 TLS 1.0 is deprecated.

Because of the protocol change, when an NSX 6.0.x client tries to connect to an NSX 6.2 or later gateway, the connection establishment fails at the SSL handshake step.

After the upgrade from NSX 6.0.x, uninstall your old SSL VPN clients and install the NSX 6.3.x version of the SSL VPN clients. See "Install SSL Client on Remote Site" in the *NSX Administration Guide*.

### NSX L2 VPN

NSX Edge upgrade is not supported if you have L2 VPN installed on an NSX Edge with NSX 6.0.x installed. Any L2 VPN configuration must be deleted before you can upgrade the NSX Edge.

## 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
```

## Upgrade to NSX 6.3.x with Cross-vCenter NSX

To upgrade to NSX 6.3.x in a cross-vCenter environment, you must upgrade the NSX components in the order in which they are documented in this guide.

NSX components must be upgraded in the following order:

- 1 Primary NSX Manager appliance
- 2 All secondary NSX Manager appliances
- 3 NSX Controller cluster
- 4 Host clusters
- 5 NSX Edge

## 6 Guest Introspection

The upgrade process is managed by the NSX Manager. If the upgrade of a component fails or is interrupted and you need to repeat or restart the upgrade, the process begins from the point at which it stopped; it does not start over from the beginning.

The upgrade status is updated for each node and at the cluster level.

## Upgrade the Primary NSX Manager in Cross-vCenter NSX

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

---

**Caution** Running with NSX Manager appliances of different versions in a cross-vCenter NSX environment is not supported. Once you upgrade the primary NSX Manager appliance, you must upgrade the secondary NSX Manager appliances.

---

During the NSX Manager upgrade in a cross-vCenter NSX environment, do not make any changes to universal objects until the primary and all secondary NSX Managers are upgraded. This includes create, update, or delete of universal objects, and operations involving universal objects (for example, apply a universal security tag to a VM).

During the upgrade, you can choose to join the Customer Experience Improvement Program (CEIP) for NSX. See *Customer Experience Improvement Program* in the *NSX Administration Guide* for more information about the program, including how to join or leave the program.

If you are upgrading from NSX 6.3.0 or later, uploading the upgrade bundle and starting the upgrade can happen independently. To start an upgrade from a previously uploaded upgrade bundle, navigate to **Home > Upgrade** and click **Begin Upgrade**.

When you upgrade NSX Manager to NSX 6.3.6, a backup is automatically taken and saved locally as part of the upgrade process. See [Managing NSX Manager Backups Created During Upgrade](#) for information about managing these backup files.

- If the automatic backup taken during the upgrade fails, the upgrade will not continue. Contact VMware customer support for assistance.
- The automatic backup is intended as a failsafe in case your regular backup fails.
  - Always take a regular NSX Manager backup before upgrading. See [Back Up NSX Manager Data](#) for more information. You can restore this backup without assistance from VMware customer support.
  - If you need to restore the automatic backup, you must contact VMware customer support.

### Prerequisites

- Validate the NSX Manager file system usage, and perform a cleanup if file system usage is at 100 percent.
  - a Log in to NSX Manager and run `show filesystems` to show the filesystem usage.
  - b If the usage is 100 percent, enter privileged (enable) mode, and run the `purge log manager` and `purge log system` commands.



c Reboot the NSX Manager appliance for the log cleanup to take effect.

- Verify the NSX Manager virtual appliance reserved memory meets the system requirements before upgrading.

See [System Requirements for NSX](#).

- If you have Data Security in your environment, uninstall it before upgrading NSX Manager. See [Uninstall NSX Data Security](#). Data Security has been removed from NSX 6.3.x.
- Back up your current configuration and download technical support logs before upgrading. See [NSX Backup and Restore](#).
- Download the upgrade bundle and check the MD5. See [Download the NSX Upgrade Bundle and Check the MD5](#).
- Make sure that you understand the operational impact of the NSX Manager upgrade while the upgrade is in progress. See [Operational Impacts of NSX Upgrades](#).
- You must upgrade all NSX Managers in a cross-vCenter NSX environment in the same maintenance window.
- Determine which NSX Managers must be upgraded in the same maintenance window.
  - If you have a cross-vCenter NSX environment, you must upgrade the primary and all secondary NSX Managers to the same NSX version in a single maintenance window.
  - If you have multiple NSX Managers connected to vCenter Server systems that use the same SSO server, not all combinations of NSX Manager version are supported. You must plan the upgrade of your NSX Managers so that you have a supported configuration at the end of the maintenance window
    - All NSX Managers using the same version of NSX is supported.
    - NSX Managers using different version of NSX is supported if at least one NSX Manager has NSX 6.4.0 or later installed, and all other NSX Managers have NSX 6.3.3 or later installed.

## Procedure

- 1 Log in to the NSX Manager virtual appliance.
- 2 From the home page, click **Upgrade**.
- 3 Click **Upgrade**, then click **Choose File** and browse to the `VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz` file. Click **Continue** to start the upload.

The upload status displays in the browser window.

- 4 If you want to start the upgrade later, click **Close** in the Upgrade dialog box.

When you are ready to start the upgrade, navigate to **Home > Upgrade** and click **Begin Upgrade**.

- 5 In the Upgrade dialog box, select whether you want to enable SSH, and whether you want to participate in VMware's Customer Experience Improvement Program ("CEIP"). Click **Upgrade** to start the upgrade.

The upgrade status displays in the browser window.

---

**Note** The Upgrade dialog box displays a message indicating that the automatic backup has been taken.

---

Wait until the upgrade procedure finishes and the NSX Manager login page appears.

- 6 Log in to the NSX Manager virtual appliance again, and from the home page click **Upgrade**. Confirm that the upgrade state is **Complete**, and the version and build number on the top right matches the upgrade bundle you just installed.

If you are logged in to the vSphere Web Client during the upgrade, you will see synchronization issue warnings on the **Networking and Security > Installation > Management** page. This is because you have NSX Manager appliances with different versions of NSX. You must upgrade the secondary NSX Manager appliances before proceeding with any other part of the upgrade.

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.

After the NSX Manager is upgraded, create a new NSX Manager backup file. See [NSX Backup and Restore](#) . The previous NSX Manager backup is only valid for the previous release.

**What to do next**

Upgrade all secondary NSX Manager appliances.

## Upgrade all Secondary NSX Manager Appliances in Cross-vCenter NSX

You must upgrade all secondary NSX Manager appliances before upgrading any other NSX components.

Complete the following steps to upgrade a secondary NSX Manager appliance. Repeat these steps for all secondary NSX Manager appliances in the cross-vCenter NSX environment.

During the NSX Manager upgrade in a cross-vCenter NSX environment, do not make any changes to universal objects until the primary and all secondary NSX Managers are upgraded. This includes create, update, or delete of universal objects, and operations involving universal objects (for example, apply a universal security tag to a VM).

During the upgrade, you can choose to join the Customer Experience Improvement Program (CEIP) for NSX. See Customer Experience Improvement Program in the *NSX Administration Guide* for more information about the program, including how to join or leave the program.

If you are upgrading from NSX 6.3.0 or later, uploading the upgrade bundle and starting the upgrade can happen independently. To start an upgrade from a previously uploaded upgrade bundle, navigate to **Home > Upgrade** and click **Begin Upgrade**.

When you upgrade NSX Manager to NSX 6.3.6, a backup is automatically taken and saved locally as part of the upgrade process. See [Managing NSX Manager Backups Created During Upgrade](#) for information about managing these backup files.

- If the automatic backup taken during the upgrade fails, the upgrade will not continue. Contact VMware customer support for assistance.
- The automatic backup is intended as a failsafe in case your regular backup fails.
  - Always take a regular NSX Manager backup before upgrading. See [Back Up NSX Manager Data](#) for more information. You can restore this backup without assistance from VMware customer support.
  - If you need to restore the automatic backup, you must contact VMware customer support.

**Prerequisites**

- Verify that the primary NSX Manager is upgraded.
- Validate the NSX Manager file system usage, and perform a cleanup if file system usage is at 100 percent.
  - a Log in to NSX Manager and run `show filesystems` to show the filesystem usage.
  - b If the usage is 100 percent, enter privileged (enable) mode, and run the `purge log manager` and `purge log system` commands.
  - c Reboot the NSX Manager appliance for the log cleanup to take effect.

- Verify the NSX Manager virtual appliance reserved memory meets the system requirements before upgrading.  
See [System Requirements for NSX](#).
- If you have Data Security in your environment, uninstall it before upgrading NSX Manager. See [Uninstall NSX Data Security](#). Data Security has been removed from NSX 6.3.x.
- Back up your current configuration and download technical support logs before upgrading. See [NSX Backup and Restore](#).
- Download the upgrade bundle and check the MD5. See [Download the NSX Upgrade Bundle and Check the MD5](#).
- Make sure that you understand the operational impact of the NSX Manager upgrade while the upgrade is in progress. See [Operational Impacts of NSX Upgrades](#).
- You must upgrade all NSX Managers in a cross-vCenter NSX environment in the same maintenance window.
- Determine which NSX Managers must be upgraded in the same maintenance window.
  - If you have a cross-vCenter NSX environment, you must upgrade the primary and all secondary NSX Managers to the same NSX version in a single maintenance window.
  - If you have multiple NSX Managers connected to vCenter Server systems that use the same SSO server, not all combinations of NSX Manager version are supported. You must plan the upgrade of your NSX Managers so that you have a supported configuration at the end of the maintenance window
    - All NSX Managers using the same version of NSX is supported.
    - NSX Managers using different version of NSX is supported if at least one NSX Manager has NSX 6.4.0 or later installed, and all other NSX Managers have NSX 6.3.3 or later installed.

### Procedure

- 1 Log in to the NSX Manager virtual appliance.
- 2 From the home page, click **Upgrade**.
- 3 Click **Upgrade**, then click **Choose File** and browse to the `VMware-NSX-Manager-upgrade-bundle-releaseNumber-NSXbuildNumber.tar.gz` file. Click **Continue** to start the upload.

The upload status displays in the browser window.

- 4 If you want to start the upgrade later, click **Close** in the Upgrade dialog box.

When you are ready to start the upgrade, navigate to **Home > Upgrade** and click **Begin Upgrade**.

- 5 In the Upgrade dialog box, select whether you want to enable SSH, and whether you want to participate in VMware's Customer Experience Improvement Program ("CEIP"). Click **Upgrade** to start the upgrade.

The upgrade status displays in the browser window.

---

**Note** The Upgrade dialog box displays a message indicating that the automatic backup has been taken.

---

Wait until the upgrade procedure finishes and the NSX Manager login page appears.

- 6 Log in to the NSX Manager virtual appliance again, and from the home page click **Upgrade**. Confirm that the upgrade state is **Complete**, and the version and build number on the top right matches the upgrade bundle you just installed.

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.

After the NSX Manager is upgraded, create a new NSX Manager backup file. See [NSX Backup and Restore](#) . The previous NSX Manager backup is only valid for the previous release.

### What to do next

[Upgrade NSX Controller Cluster in Cross-vCenter NSX](#)

## Upgrade NSX Controller Cluster in Cross-vCenter NSX

The controllers in your environment are upgraded at the cluster level. If an upgrade is available for the NSX Controller cluster, an upgrade link appears next to the primary NSX Manager in the **Networking & Security > Installation > Management** panel.

It is recommended that you upgrade the controllers during a maintenance window.

The NSX Controller upgrade causes an upgrade file to be downloaded to each controller node. The controllers are upgraded one at a time. While an upgrade is in progress, the **Upgrade Available** link is not clickable, and API calls to upgrade the controller cluster are blocked until the upgrade is complete.

If you deploy new controllers before the existing controllers are upgraded, they are deployed as the old version. Controller nodes must be the same version to join a cluster.

---

**Important** In NSX 6.3.3 the underlying operating system of the NSX Controller changes. This means that when you upgrade from NSX 6.3.2 or earlier to NSX 6.3.3 or later, instead of an in-place software upgrade, the existing controllers are deleted one at a time, and new Photon OS based controllers are deployed using the same IP addresses.

When the controllers are deleted, this also deletes any associated DRS anti-affinity rules. You must create new anti-affinity rules in vCenter to prevent the new controller VMs from residing on the same host.

---

### Prerequisites

- Ensure that all of the controllers are in the normal state. Upgrading is not possible when one or more of the controllers are in the disconnected state. To reconnect a disconnected controller, try resetting the controller virtual appliance. In the **Hosts and Clusters** view, right-click the controller and select **Power > Reset**.
- A valid NSX Controller cluster contains three controller nodes. Log in to the three controller nodes and run the **show control-cluster status** command.

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

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

persistence_server	enabled	activated
switch_manager	enabled	activated
logical_manager	enabled	activated
directory_server	enabled	activated

- For Join status, verify the controller node is reporting Join Complete.
- For Majority status, verify the controller is connected to the cluster majority.
- For Cluster ID, all the controller nodes in a cluster should have the same cluster ID.
- For Configured status and Active status, verify that the all the controller roles are enabled and activated.
- Make sure that you understand the operational impact of the NSX Controller upgrade while the upgrade is in progress. See [Operational Impacts of NSX Upgrades](#).
- If you are upgrading to NSX 6.3.3 the NSX Controller cluster must contain three controller nodes. If it has fewer than three you must add additional nodes before starting the upgrade. See "Deploy NSX Controller Cluster" in the *NSX Installation Guide* for steps to add controller nodes.

#### Procedure

- ◆ Navigate to **Home > Networking & Security > Installation**, select the **Management** tab, and click **Upgrade Available** in the **Controller Cluster Status** column.

The controllers in your environment are upgraded and rebooted one at a time. After you initiate the upgrade, the system downloads the upgrade file, upgrades each controller, reboots each controller, and updates the upgrade status of each controller. The following fields display controller status:

- The **Controller Cluster Status** column in the NSX Manager section displays the upgrade status of the cluster. When the upgrade begins, the status says **Downloading upgrade file**. When the upgrade file has been downloaded on all controllers in the cluster, the status changes to **In progress**. After all the controllers in the cluster have been upgraded, the status displayed is **Complete**, and then this column is no longer displayed.
- The **Status** column in the NSX Controller nodes section displays the status of each controller, which is **Connected** or **Normal** before the upgrade, depending on the original NSX version. When the controller services are shut down and the controller is rebooted, the status changes to **Disconnected**. After the upgrade for that controller is complete, the status is **Connected**.
- The **Upgrade Status** column in the NSX Controller nodes section displays the upgrade status for each controller. The status displays **Downloading upgrade file** to begin with, then displays **Upgrade in progress**, and then **Rebooting**. After the controller is upgraded, the status displays **Upgraded**.

---

**Note** When you upgrade from NSX 6.3.2 or earlier to NSX 6.3.3 or later, the **Downloading upgrade file** status is replaced with **Queued For Upgrade**.

---

When the upgrade is complete, the **Software Version** column in the NSX Controller nodes section displays **6.3.buildNumber** for each controller. Rerun the **show control-cluster status** command to make sure the controllers are able to create a majority. If the NSX Controller cluster majority is not re-formed review controller and NSX Manager logs.

After upgrading controllers, one or more controller nodes may be assigned a new controller ID. This behavior is expected and depends on when the secondary NSX Manager polls the nodes.

The average upgrade time for each upgrade is 6-8 minutes. If the upgrade does not complete within the timeout period (30 minutes), the **Upgrade Status** column displays **Failed**. Click **Upgrade Available** in the NSX Manager section again to resume the upgrade process from the point where it stopped.

If network issues are preventing a successful upgrade within the 30-minute timeout period, you may need to configure a longer timeout period. Work with VMware Support to diagnose and resolve any underlying issues and, if needed, configure a longer timeout period.

If the controller upgrade fails, check connectivity between the controllers and the NSX Manager.

There is a scenario in which the first controller upgrades successfully, and the second controller does not. Assuming you have three controllers in a cluster, the first controller is successfully upgraded to the new version, and the second controller is being upgraded. If the upgrade of the second controller fails, the second controller might be left in a disconnected state. At the same time, the first and third controllers now have two different versions (one upgraded, one not) and are therefore unable to form a majority. At this point, the upgrade cannot be relaunched. To work around this scenario, create another controller. The newly created controller will be of the older version (matching controller three) and will therefore form a majority with controller three. At this point, you can relaunch the upgrade procedure. See *Redeploy an NSX Controller* in the *NSX Troubleshooting Guide* for instructions on creating another controller.

#### What to do next

[Upgrade Host Clusters in Cross-vCenter NSX.](#)

## Upgrade Host Clusters in Cross-vCenter NSX

After upgrading all NSX Manager appliances and the NSX Controller cluster, you should update all host clusters in the cross-vCenter NSX environment.

Upgrading the host clusters upgrades the NSX VIBs.

If you are upgrading from NSX 6.2.x or earlier, or if you are upgrading from NSX 6.3.0 or later with ESXi 5.5, hosts must be rebooted to complete the upgrade.

- If the cluster has DRS enabled, when you click **Resolve all** DRS attempts to reboot the hosts in a controlled fashion that allows the VMs to continue running. VMs are moved to other hosts in the cluster and the hosts enter maintenance mode and are rebooted.
- If the cluster does not have DRS enabled, you must power off or vMotion the VMs manually before beginning the upgrade. When you click **Resolve all** the hosts enter maintenance mode and are rebooted.



If you are upgrading from NSX 6.3.0 or later with ESXi 6.0 or later, the hosts must enter maintenance mode to complete the upgrade. Rebooting is not required.

- If the cluster has DRS enabled, when you click **Resolve all** DRS attempts to put the hosts into maintenance mode in a controlled fashion that allows the VMs to continue running. VMs are moved to other hosts in the cluster and the hosts enter maintenance mode.
- If the cluster does not have DRS enabled, you must power off or vMotion the VMs manually before beginning the upgrade. You must manually put the hosts into maintenance mode to complete the upgrade.

In NSX 6.3.5 and later you can view the EAM status on the **Host Preparation** tab.

### Prerequisites

- Upgrade NSX Manager and the NSX Controller cluster.
- Log out of and log back in to the vSphere Web client after upgrading NSX Manager and before upgrading the host clusters.
- Make sure that you understand the operational impact of a host cluster upgrade while the upgrade is in progress. See [Operational Impacts of NSX Upgrades](#).
- Make sure the fully qualified domain names (FQDNs) of all of your hosts can be resolved.
- If DRS is disabled, power off or vMotion the VMs manually before beginning the upgrade.
- If DRS is enabled, the running VMs are moved automatically during the host cluster upgrade. Before beginning the upgrade, make sure that DRS can work in your environment.
  - Make sure that DRS is enabled on the host clusters.
  - Make sure that vMotion functions correctly.
  - Check the host connection state with vCenter.
  - Check that you have a minimum three ESXi hosts in each host cluster. During an NSX upgrade, a host cluster with only one or two hosts is more likely to have issues with DRS admission control. For a successful NSX upgrade, VMware recommends that each host cluster have at least three hosts. If a cluster contains fewer than three hosts, the recommendation is to manually evacuate the hosts.
  - In a small cluster with only two or three hosts, if you have created anti-affinity rules stating that certain VMs must reside on separate hosts, these rules might prevent DRS from moving the VMs during the upgrade. Either add additional hosts to the cluster or disable the anti-affinity rules during the upgrade and reenable them after the upgrade is complete. To disable an anti-affinity rule, navigate to **Hosts and Clusters > Cluster > Manage > Settings > VM/Host Rules**. Edit the rule and deselect **Enable rule**.
- Log into one of the hosts in the cluster and run the `esxcli software vib list` command.

The VIBs present will depend on the ESXi and NSX versions, and therefore might change as part of the upgrade. Note the current version of the installed VIBs:

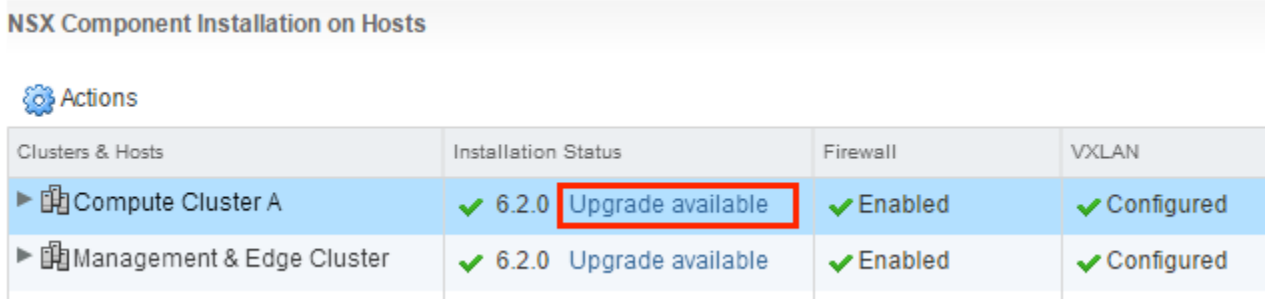
ESXi version	NSX version	VIBs installed
5.5	6.1.x, 6.2.x or 6.3.x	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 or later	6.3.2 or earlier	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 or later	6.3.3 or later	<ul style="list-style-type: none"> <li>■ esx-nsxv</li> </ul>

**Note** Some versions of NSX have additional VIBs which will be removed during the upgrade.

- If you are upgrading from a version of NSX earlier than NSX 6.2, prepared hosts have an additional VIB, esx-dvfilter-switch-security.
- If you are upgrading from NSX 6.2.x where the version is NSX 6.2.4 or later, prepared hosts have an additional VIB, esx-vdpi.

**Procedure**

- 1 In the vSphere Web Client, navigate to **Home > Networking & Security > Installation**, select the **Host Preparation** tab.
- 2 For each cluster that you want to upgrade, click **Upgrade available**.



The Installation Status displays *Installing*.

- 3 The cluster Installation Status displays *Not Ready*. Click **Not Ready** to display more information. Click **Resolve all** to attempt to complete the VIB installation.

The hosts are put in maintenance mode, and rebooted if required, to complete the upgrade.

The Installation Status column displays *Installing*. Once the upgrade is complete the Installation Status column displays a green check mark and the upgraded NSX version.

- 4 If the **Resolve** action fails when DRS is enabled, the hosts might require manual intervention to enter maintenance mode (for example, due to HA requirements or DRS rules), the upgrade process stops and the cluster Installation Status displays *Not Ready* again. Click **Not Ready** to display more information. Check the hosts in the **Hosts and Clusters** view, make sure the hosts are powered on, connected, and contain no running VMs. Then retry the **Resolve** action.

The Installation Status column displays *Installing*. Once the upgrade is complete the Installation Status column displays a green check mark and the upgraded NSX version.

- 5 If the **Resolve** action fails when DRS is disabled and you are upgrading from NSX 6.3.0 or later with ESXi 6.0 or later, you must manually put the hosts into maintenance mode to complete the upgrade.
  - a Place the evacuated hosts in maintenance mode.
  - b Navigate to **Networking & Security > Installation > Host Preparation**.  
  
The upgrade automatically starts when the hosts enter maintenance mode. The Installation Status column displays *Installing*. If you do not see the *Installing* status, refresh the page.  
  
Once the upgrade is complete the Installation Status column displays a green check mark and the upgraded NSX version.
  - c Remove the hosts from maintenance mode.

To confirm the host update, log into one of the hosts in the cluster and run the `esxcli software vib list` command. Make sure that the appropriate VIBs have been updated to the expected version.

If a host fails to upgrade, perform the following troubleshooting steps:

- Check the ESX Agent Manager on vCenter, and look for alerts and errors.
- Log in to the host, check the `/var/log/esxupdate.log` file, and look for recent alerts and errors.
- Ensure that DNS and NTP are configured on the host.

See "Host Preparation" in the *NSX Troubleshooting Guide* for more troubleshooting steps.

#### What to do next

[Upgrade NSX Edge in Cross-vCenter NSX](#)

## Upgrade NSX Edge in Cross-vCenter NSX

During the upgrade process, a new Edge virtual appliance is deployed alongside the existing one.

When the new Edge is ready, the old Edge's vNICs are disconnected and the new Edge's vNICs are connected. The new Edge then sends gratuitous ARP (GARP) packets to update the ARP cache of connected switches. When HA is deployed, the upgrade process is performed two times.

This process can temporarily affect packet forwarding. You can minimize the impact by configuring the Edge to work in ECMP mode.

OSPF adjacencies are withdrawn during upgrade if graceful restart is not enabled.

Upgrade NSX Edges in all NSX installations in the cross-vCenter NSX environment.

#### Prerequisites

- Verify that NSX Manager has been upgraded.
- Verify that the NSX Controller cluster and host preparation have been upgraded before upgrading logical routers.
- Verify that there is a local segment ID pool, even if you have no plans to create NSX logical switches.

- Verify the hosts have enough resources to deploy additional NSX Edge Services Gateway appliances during the upgrade, particularly if you are upgrading multiple NSX Edge appliances in parallel. See the [System Requirements for NSX](#) for the resources required for each NSX Edge size.
  - For a single NSX Edge instance, there are two NSX Edge appliances of the appropriate size in the poweredOn state during upgrade.
  - For an NSX Edge instance with high availability, both replacement appliances are deployed before replacing the old appliances. This means there are four NSX Edge appliances of the appropriate size in the poweredOn state during upgrade of a given NSX Edge. Once the NSX Edge instance is upgraded, either of the HA appliances could become active.
- Verify that the host clusters listed in the configured location and live location for the NSX Edge appliance are prepared for NSX and that their messaging infrastructure status is GREEN. If the configured location is not available, for example, because the cluster has been removed since the NSX Edge appliance was created, then verify the live location only.
  - Find the ID of the original configured location (*configuredResourcePool > id*) and the current live location (*resourcePoolId*) with the GET `https://NSX-Manager-IP-Address/api/4.0/edges/{edgeId}/appliances` API request.
  - Find the host preparation status and the messaging infrastructure status for those clusters with the GET `https://NSX-Manager-IP-Address/api/2.0/nwfabric/status?resource={resourceId}` API request, where *resourceId* is the ID of the configured and live location of the NSX Edge appliances found previously.
    - Look for the status corresponding to the *featureId* of `com.vmware.vshield.vsm.nwfabric.hostPrep` in the response body. The status must be GREEN.

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

- Look for the status corresponding to the *featureId* of `com.vmware.vshield.vsm.messagingInfra` in the response body. The status must be GREEN.

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

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

- Understand the operational impact of the NSX Edge upgrade while the upgrade is in progress. See Operational Impacts of NSX Upgrades in the *NSX Upgrade Guide*.
- If you are upgrading from NSX 6.0.x and you have L2 VPN enabled on an NSX Edge you must delete the L2 VPN configuration before you upgrade. Once you have upgraded, you can reconfigure L2 VPN. See "L2 VPN Overview" in the *NSX Installation Guide*.

### Procedure

- 1 In the vSphere Web Client, select **Networking & Security > NSX Edges**.
- 2 For each NSX Edge instance, select **Upgrade Version** from the **Actions** (⚙️) menu.

If the upgrade fails with the error message "Failed to deploy edge appliance," make sure that the host on which the NSX edge appliance is deployed is connected and not in maintenance mode.

After the NSX Edge is upgraded successfully, the **Status** is Deployed, and the **Version** column displays the new NSX version.

If an Edge fails to upgrade and does not rollback to the old version, click the **Redeploy NSX Edge** icon and then retry the upgrade.

### What to do next

After you upgrade your 6.2.4 or earlier NSX Edges to 6.2.5 or later, you must turn off vSphere Virtual Machine Startup for each NSX Edge in a cluster where vSphere HA is enabled and Edges are deployed. To do this, open the vSphere web client and find the ESXi host where NSX Edge virtual machine resides. Click **Manage > Settings** and under Virtual Machines, select VM Startup/Shutdown, click **Edit**, and make sure that the virtual machine is in Manual mode (that is, make sure it is not added to the Automatic Startup/Shutdown list).

[Upgrade Guest Introspection in Cross-vCenter NSX](#)

## Upgrade Guest Introspection in Cross-vCenter NSX

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.

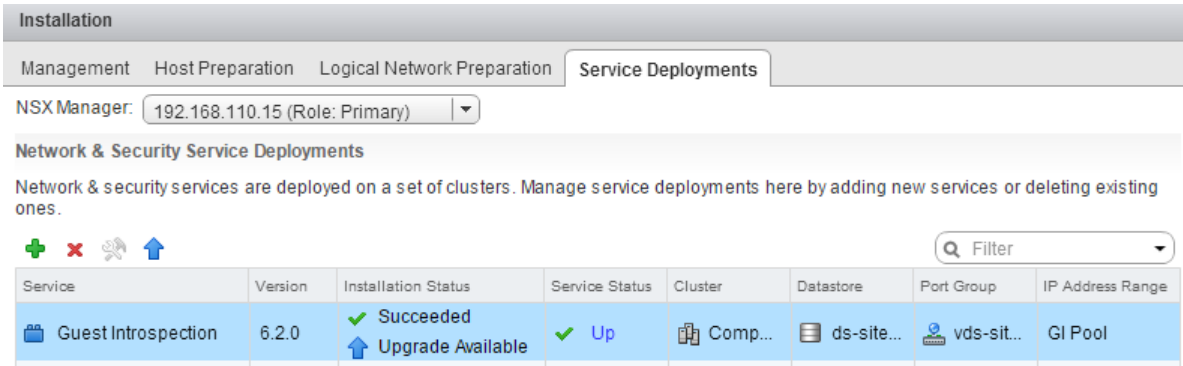
---

### Prerequisites

Upgrade NSX Manager, controllers, prepared host clusters, and NSX Edges.

## Procedure

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



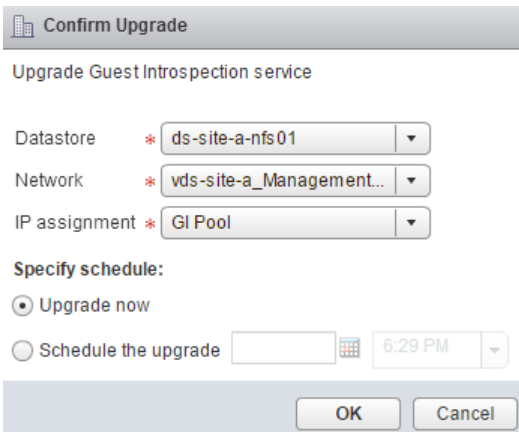
Service	Version	Installation Status	Service Status	Cluster	Datastore	Port Group	IP Address Range
Guest Introspection	6.2.0	Succeeded Upgrade Available	Up	Comp...	ds-site...	vds-sit...	GI Pool

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.



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.

## NSX Services That Do Not Support Direct Upgrade

Some NSX services do not support a direct upgrade. In these cases, you must uninstall and reinstall the services.

## VMware Partner Security Virtual Appliances

Check the partner documentation to verify if the partner security virtual appliance can be upgraded.

### NSX SSL VPN

Starting in NSX 6.2, the SSL VPN gateway only accepts the TLS protocol. However, after upgrading to NSX 6.2 or later, any new clients that you create automatically use the TLS protocol during connection establishment. Additionally, starting in NSX 6.2.3 TLS 1.0 is deprecated.

Because of the protocol change, when an NSX 6.0.x client tries to connect to an NSX 6.2 or later gateway, the connection establishment fails at the SSL handshake step.

After the upgrade from NSX 6.0.x, uninstall your old SSL VPN clients and install the NSX 6.3.x version of the SSL VPN clients. See "Install SSL Client on Remote Site" in the *NSX Administration Guide*.

### NSX L2 VPN

NSX Edge upgrade is not supported if you have L2 VPN installed on an NSX Edge with NSX 6.0.x installed. Any L2 VPN configuration must be deleted before you can upgrade the NSX Edge.

## 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
```



# Upgrading vSphere in an NSX Environment

# 2

If you need to upgrade both NSX and vSphere, VMware recommends completing the NSX upgrade first, and then completing the vSphere upgrade.

Check the VMware Product Interoperability Matrix to verify which versions of vSphere and ESXi are compatible with your NSX installation. See

[http://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php](http://www.vmware.com/resources/compatibility/sim/interop_matrix.php).

See the appropriate version of the vSphere documentation for detailed instructions on upgrading vSphere, including the *vSphere Upgrade Guide* and the *Installing and Administering VMware vSphere Update Manager Guide*.

When you upgrade ESXi on a host, you must also install new NSX VIBs on the host to be compatible with the new ESXi version. NSX workloads cannot run on the upgraded host until the NSX VIBs are updated.

The procedure to upgrade ESXi when NSX 6.3.x is installed will vary depending on the version of ESXi you are upgrading to and from.

**Table 2-1. ESXi Upgrade Procedure When NSX 6.3.x is Installed**

Host Upgrade Type	Host Maintenance Mode Requirements	Host Reboot Requirements
ESXi 5.5 to ESXi 6.0. See <a href="#">Upgrade to ESXi 6.0 in an NSX Environment</a> .	Host must stay in maintenance mode until ESXi upgrade and subsequent NSX VIB upgrade is complete.	Reboot is required during ESXi upgrade. Reboot is required during subsequent NSX VIB upgrade.
ESXi 5.5 to ESXi 6.5. See <a href="#">Upgrade to ESXi 6.5 in an NSX Environment</a> .	Host can exit maintenance mode after ESXi upgrade. vMotion of VMs to VXLAN prepared vSphere Distributed Switches on the upgraded host is blocked until the subsequent NSX VIB upgrade is completed.	Reboot is required during ESXi upgrade. Reboot is required during subsequent NSX VIB upgrade.
ESXi 6.0 to ESXi 6.5 See <a href="#">Upgrade to ESXi 6.5 in an NSX Environment</a> .	Host can exit maintenance mode after ESXi upgrade. vMotion of VMs to VXLAN prepared vSphere Distributed Switches on the upgraded host is blocked until the subsequent NSX VIB upgrade is completed.	Reboot is required during ESXi upgrade. Reboot is not required during subsequent NSX VIB upgrade.

This chapter includes the following topics:

- [Upgrade to ESXi 6.0 in an NSX Environment](#)
- [Upgrade to ESXi 6.5 in an NSX Environment](#)

- [Redeploy Guest Introspection after ESXi Upgrade](#)

## Upgrade to ESXi 6.0 in an NSX Environment

NSX VIBs are specific to the version of ESXi that is installed on the host. If you upgrade ESXi, you must install new NSX VIBs appropriate for the new ESXi version.

The NSX VIBs installed depend on the ESXi and NSX versions. If you have NSX 6.3.3 or later installed, and you upgrade from ESXi 5.5 to 6.0, the `esx-vsip` and `esx-vxlan` VIBs are removed and replaced with the `esx-nsxv` VIB.

ESXi version	NSX version	VIBs installed
5.5	Any 6.3.x	<ul style="list-style-type: none"> <li>▪ <code>esx-vsip</code></li> <li>▪ <code>esx-vxlan</code></li> </ul>
6.0 or later	6.3.2 or earlier	<ul style="list-style-type: none"> <li>▪ <code>esx-vsip</code></li> <li>▪ <code>esx-vxlan</code></li> </ul>
6.0 or later	6.3.3 or later	<ul style="list-style-type: none"> <li>▪ <code>esx-nsxv</code></li> </ul>

**Important** You must ensure the host stays in maintenance mode throughout the upgrade process to avoid DRS or vMotion moving VMs to the host before the upgrade is complete.

### Prerequisites

- Check the VMware Product Interoperability Matrix to verify which versions of vSphere and ESXi are compatible with your NSX installation. See [http://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php](http://www.vmware.com/resources/compatibility/sim/interop_matrix.php).
- Read the appropriate version of the vSphere documentation for detailed instructions on upgrading vSphere, including the *vSphere Upgrade Guide* and the *Installing and Administering VMware vSphere Update Manager Guide*.
- Verify Platform Services Controller and vCenter Server systems are upgraded to the new vSphere version.
- Make sure the fully qualified domain names (FQDNs) of all of your hosts can be resolved.
- If DRS is disabled, power off or vMotion the VMs manually before beginning the upgrade.
- If DRS is enabled, the running VMs are moved automatically during the host cluster upgrade. Before beginning the upgrade, make sure that DRS can work in your environment.
  - Make sure that DRS is enabled on the host clusters.
  - Make sure that vMotion functions correctly.
  - Check the host connection state with vCenter.

- Check that you have a minimum three ESXi hosts in each host cluster. During an NSX upgrade, a host cluster with only one or two hosts is more likely to have issues with DRS admission control. For a successful NSX upgrade, VMware recommends that each host cluster have at least three hosts. If a cluster contains fewer than three hosts, the recommendation is to manually evacuate the hosts.
- In a small cluster with only two or three hosts, if you have created anti-affinity rules stating that certain VMs must reside on separate hosts, these rules might prevent DRS from moving the VMs during the upgrade. Either add additional hosts to the cluster or disable the anti-affinity rules during the upgrade and reenable them after the upgrade is complete. To disable an anti-affinity rule, navigate to **Hosts and Clusters > Cluster > Manage > Settings > VM/Host Rules**. Edit the rule and deselect **Enable rule**.

### Procedure

- ◆ For each host that must be upgraded, complete the following steps.
  - a Put the host into maintenance mode.
 

If the cluster has DRS enabled, DRS will attempt to move VMs to other hosts. If DRS fails for any reason, you may need to move the VMs manually and then put the host into maintenance mode.
  - b Upgrade ESXi on the host.
 

Reboot the host after the ESXi upgrade is complete.
  - c If the host has status Not connected after the reboot, connect the host. Right click the host and select **Connection > Connect**.
  - d Navigate to **Networking & Security > Installation > Host Preparation**.
  - e Select the host on which you upgraded ESXi. The Installation Status displays **Not Ready**.
  - f Click **Actions > Resolve** complete the NSX VIB update.
 

NSX VIBs are updated on the host, and the host is rebooted.
  - g Once the host has completed the reboot, exit from maintenance mode.

You can verify that the VIBs are updated by connecting to the host command line and issuing the `esxcli software vib list` command. The first part of the VIB version displays the version of ESXi for the VIB.

For example, after upgrade to ESXi 6.0 with NSX 6.3.2 or earlier:

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

After upgrade to ESXi 6.0 with NSX 6.3.3 or later:

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

## Upgrade to ESXi 6.5 in an NSX Environment

NSX VIBs are specific to the version of ESXi that is installed on the host. If you upgrade ESXi, you must install new NSX VIBs appropriate for the new ESXi version.

When you upgrade to ESXi 6.5 with NSX 6.3.x installed, vMotion of VMs to VXLAN prepared vSphere Distributed Switches on the upgraded host is blocked until the new NSX VIBs have been installed.

VMware recommends using vSphere Upgrade Manager to upgrade hosts to ESXi 6.5 in an NSX 6.3.x environment.

Whatever method you use to upgrade ESXi, you should follow this workflow. On one host at a time, do the following:

### 1 Upgrade ESXi

Once the ESXi upgrade completes, the host exits maintenance mode, however, you cannot move VMs connected to logical switches to the host until the next step has completed.

### 2 Upgrade NSX VIBs

Once the VIBs are upgraded and the host has been removed from maintenance mode, you can move VMs connected to logical switches to the host.

---

**Important** You must upgrade one host at a time. Do not select a cluster or datacenter to remediate when you to upgrade ESXi.

---

The NSX VIBs installed depend on the ESXi and NSX versions. If you have NSX 6.3.3 or later installed, and you upgrade from ESXi 5.5 to 6.5, the esx-vsip and esx-vxlan VIBs are removed and replaced with the esx-nsxv VIB.

ESXi version	NSX version	VIBs installed
5.5	Any 6.3.x	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 or later	6.3.2 or earlier	<ul style="list-style-type: none"> <li>■ esx-vsip</li> <li>■ esx-vxlan</li> </ul>
6.0 or later	6.3.3 or later	<ul style="list-style-type: none"> <li>■ esx-nsxv</li> </ul>

### Prerequisites

- Verify NSX 6.3.x is installed.
- Check the VMware Product Interoperability Matrix to verify which versions of vSphere and ESXi are compatible with your NSX installation. See [http://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php](http://www.vmware.com/resources/compatibility/sim/interop_matrix.php).

---

**Important** NSX 6.3.x is not interoperable with the initial release of ESXi 6.5. You must upgrade to ESXi 6.5.0a or later to be compatible with NSX 6.3.0. Check the interoperability matrix for the latest interoperability information.

---

- Read the appropriate version of the vSphere documentation for detailed instructions on upgrading vSphere, including the *vSphere Upgrade Guide* and the *Installing and Administering VMware vSphere Update Manager Guide*.
- Verify Platform Services Controller and vCenter Server systems are upgraded to the new vSphere version.
- Verify vSphere Update Manager is installed and configured.
- Make sure the fully qualified domain names (FQDNs) of all of your hosts can be resolved.
- If DRS is disabled, power off or vMotion the VMs manually before beginning the upgrade.
- If DRS is enabled, the running VMs are moved automatically during the host cluster upgrade. Before beginning the upgrade, make sure that DRS can work in your environment.
  - Make sure that DRS is enabled on the host clusters.
  - Make sure that vMotion functions correctly.
  - Check the host connection state with vCenter.
  - Check that you have a minimum three ESXi hosts in each host cluster. During an NSX upgrade, a host cluster with only one or two hosts is more likely to have issues with DRS admission control. For a successful NSX upgrade, VMware recommends that each host cluster have at least three hosts. If a cluster contains fewer than three hosts, the recommendation is to manually evacuate the hosts.

- In a small cluster with only two or three hosts, if you have created anti-affinity rules stating that certain VMs must reside on separate hosts, these rules might prevent DRS from moving the VMs during the upgrade. Either add additional hosts to the cluster or disable the anti-affinity rules during the upgrade and reenable them after the upgrade is complete. To disable an anti-affinity rule, navigate to **Hosts and Clusters > Cluster > Manage > Settings > VM/Host Rules**. Edit the rule and deselect **Enable rule**.

### Procedure

- 1 In the vSphere Web Client, navigate to **Update Manager > Update Manager Object > Manage**.
- 2 Follow the instructions in *Import Host Upgrade Images and Create Host Upgrade Baselines* to import a host upgrade image and create a host upgrade baseline.
  - a Click the **ESXi Images** tab, click **Import ESXi Image** and browse to the image you want to upload.
  - b Click the **Host Baselines** tab and click **New Baseline**. Use the New Baseline wizard to create a new Baseline, selecting **Host Upgrade** as the Baseline type.
- 3 Upgrade one host at a time. Repeat these steps for each host.
  - a Navigate to **Hosts and Clusters** and select a host to upgrade. Do not select a cluster or datacenter.
  - b Right click the host and select **Update Manager > Attach Baseline....** Use the Attach Baseline or Baseline Group wizard to select a baseline. See *Attach Baselines and Baseline Groups to Objects* in the vSphere documentation for full instructions.
  - c Right click the host and select **Update Manager > Remediate....** Use the Remediate wizard to select a baseline. See *Remediate Hosts Against an Upgrade Baseline* in the vSphere documentation for full instructions.
  - d If the host has status Not connected after the reboot, connect the host. Right click the host and select **Connection > Connect**.
  - e To verify the upgrade is complete, right click the host and select **Update Manager > Scan for Updates....** Select the **Upgrades** check box to scan for upgrade compliance. If the Compliance Status is Compliant, the upgrade is complete.  
  
See *Manually Initiate a Scan of ESXi Hosts* in the vSphere documentation for full instructions.
  - f Navigate to **Networking & Security > Installation > Host Preparation**.

- g Locate the host on which you upgraded ESXi. The Installation Status displays **Not Ready**. Click **Not Ready** to see more information.

- h Select the host and click **Actions > Resolve** to trigger NSX VIB installation.

If you are upgrading from ESXi 5.5, and the cluster has DRS enabled, DRS will attempt to reboot the host in a controlled fashion that allows the VMs to continue running. If DRS fails for any reason, the **Resolve** action halts. In this case, you may need to move the VMs manually and then retry the **Resolve** action or put the host into maintenance mode and reboot manually.

If you are upgrading from ESXi 6.0, and the cluster has DRS enabled, DRS will attempt to put the host into maintenance mode in a controlled fashion that allows the VMs to continue running. If DRS fails for any reason, the **Resolve** action halts. In this case, you may need to move the VMs manually and then retry the **Resolve** action or put the host into maintenance mode manually.

---

**Important** If you are upgrading from ESXi 6.0, and you manually put a host into maintenance mode to install the host VIBs, you must verify that the host VIB install has completed before you take the host out of maintenance mode. The **Host Preparation** will display Installation Status Installing even though the install is complete.

- 1 Check the Recent Tasks pane in the vSphere Web Client and verify all Install tasks have completed.
- 2 Connect to the host command line and run the `esxcli software vib list` command. The first part of the VIB version displays the version of ESXi for the VIB.

For example, after upgrade to ESXi 6.5 with NSX 6.3.2 or earlier:

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

After upgrade to ESXi 6.5 with NSX 6.3.3 or later:

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

## Redeploy Guest Introspection after ESXi Upgrade

If you upgrade ESXi on a cluster where Guest Introspection is deployed, you should check the Service Deployments tab to see if Guest Introspection needs to be redeployed.

---

**Important** You must complete the ESXi upgrade and associated NSX VIB upgrade before you redeploy Guest Introspection.

---

### Prerequisites

- Complete ESXi upgrade.
- Complete NSX VIBs (Host Preparation) upgrade after the ESXi upgrade.

### Procedure

- 1 Log in to the vSphere Web Client.
- 2 Click **Networking & Security** and then click **Installation**.
- 3 Click the **Service Deployments** tab.
- 4 If the Installation Status column shows Succeeded, redeploy is not required.
- 5 If the Installation Status column shows Not Ready, click the **Not Ready** link. Click **Resolve all** to redeploy Guest Introspection.