# NSX Upgrade Guide

Update 5
Modified on 20 NOV 2017
VMware NSX for vSphere 6.2

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

# Contents

# NSX Upgrade Guide

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

## Intended Audience

This manual is intended for anyone who wants to install 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 5.5 or 6.0, 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 VMware Product Interoperability Matrix at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php on the **Interoperability** tab. |

| | |
|---|---|
| | Verify support for the upgrade path from your current version of NSX to the version that you are upgrading to. On the **Upgrade Path** tab, select **VMware NSX** from the product menu. |
| **Compatibility Guide** | Verify the compatibility of partner solutions with NSX at the VMware Compatibility Guide, at http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security. |

# System Requirements for NSX

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 and Data Security per ESXi™ host, and multiple NSX Edge instances per datacenter.

## Hardware

**Table 1. Hardware Requirements**

| Appliance | Memory | vCPU | Disk Space |
|---|---|---|---|
| NSX Manager | 16 GB (24 GB with certain NSX deployment sizes*) | 4 (8 with certain NSX deployment sizes*) | 60 GB |
| NSX Controller | 4 GB | 4 | 20 GB |
| NSX Edge | ■ Compact: 512 MB<br>■ Large: 1 GB<br>■ Quad Large: 1 GB<br>■ X-Large: 8 GB | ■ Compact: 1<br>■ Large: 2<br>■ Quad Large: 4<br>■ X-Large: 6 | ■ Compact: 1 disk 500MB<br>■ Large: 1 disk 500MB + 1 disk 512MB<br>■ Quad-Large: 1 disk 500MB + 1 disk 512MB<br>■ X-Large: 1 disk 500MB + 1 disk 2GB |
| Guest Introspection | 1 GB | 2 | 4 GB |
| NSX Data Security | 512 MB | 1 | 6 GB per ESXi host |

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

For specific sizing details contact VMware support.

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

## Software

For the latest interoperability information, see the Product Interoperability Matrixes at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

For recommended versions of NSX, vCenter Server, and ESXi, see the release notes at https://docs.vmware.com/en/VMware-NSX-for-vSphere/index.html.

Note that 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 | ■ ESXi 6.0 or later<br>■ Host clusters prepared with NSX 6.2 or later VIBs |

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 check 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

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

# Ports and Protocols Required by NSX

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

### Table 2. Ports and Protocols required by NSX

| Source | Target | Port | Protocol | Purpose | Sensitive | TLS | Authentication |
|---|---|---|---|---|---|---|---|
| Client PC | NSX Manager | 443 | TCP | NSX Manager Administrative Interface | No | Yes | PAM Authentication |
| Client PC | NSX Manager | 80 | TCP | NSX Manager VIB Access | No | No | PAM Authentication |
| ESXi Host | vCenter Server | 443 | TCP | ESXi Host Preparation | No | No | |
| vCenter Server | ESXi Host | 443 | TCP | ESXi Host Preparation | No | No | |
| ESXi Host | NSX Manager | 5671 | TCP | RabbitMQ | No | Yes | RabbitMQ User/Password |
| ESXi Host | NSX Controller | 1234 | TCP | User World Agent Connection | No | Yes | |
| NSX Controller | NSX Controller | 2878, 2888, 3888 | TCP | Controller Cluster - State Sync | No | Yes | IPsec |
| NSX Controller | NSX Controller | 7777 | TCP | Inter-Controller RPC Port | No | Yes | IPsec |
| NSX Controller | NSX Controller | 30865 | TCP | Controller Cluster - State Sync | No | Yes | IPsec |
| NSX Manager | NSX Controller | 443 | TCP | Controller to Manager Communication | No | Yes | User/Password |
| NSX Manager | vCenter Server | 443 | TCP | vSphere Web Access | No | Yes | |
| NSX Manager | vCenter Server | 902 | TCP | vSphere Web Access | No | Yes | |
| NSX Manager | ESXi Host | 443 | TCP | Management and provisioning connection | No | Yes | |
| NSX Manager | ESXi Host | 902 | TCP | Management and provisioning connection | No | Yes | |
| NSX Manager | DNS Server | 53 | TCP | DNS client connection | No | No | |
| NSX Manager | DNS Server | 53 | UDP | DNS client connection | No | No | |
| NSX Manager | Syslog Server | 514 | TCP | Syslog connection | No | No | |
| NSX Manager | Syslog Server | 514 | UDP | Syslog connection | No | No | |
| NSX Manager | NTP Time Server | 123 | TCP | NTP client connection | No | Yes | |

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

| Source | Target | Port | Protocol | Purpose | Sensitive | TLS | Authentication |
|---|---|---|---|---|---|---|---|
| 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 |
| 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 | |

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

| Source | Target | Port | Protocol | Purpose | Sensitive | TLS | Authentication |
|---|---|---|---|---|---|---|---|
| ESXi Host | Primary NSX Manager | 5671 | TCP | RabbitMQ | No | Yes | RabbitMQ User/Password |
| ESXi Host | Secondary NSX Manager | 5671 | TCP | RabbitMQ | No | Yes | RabbitMQ User/Password |

## Ports for Cross-vCenter NSX and Enhanced Linked Mode

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

# vCloud Networking and Security to NSX Upgrade

1

This section includes the following topics:



## Preparing for the vCloud Networking and Security to NSX Upgrade

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

**Caution** Downgrades are not supported:

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

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

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

1. Verify that vCloud Networking and Security is version 5.5. If not, see the *vShield Installation and Upgrade Guide* version 5.5 for upgrade instructions.
2. Verify that all required ports are open. See Ports and Protocols Required by NSX.
3. Verify that you can retrieve uplink port name information for vSphere Distributed Switches. See https://kb.vmware.com/kb/2129200.
4. If any vShield Endpoint partner services are deployed, verify compatibility before upgrading:
   - In most circumstances, vCloud Networking and Security can be upgraded to NSX without impacting partner solutions. However, if your partner solution is not compatible with the version of NSX to which you are upgrading, you will need to upgrade the partner solution to a compatible version before upgrading to NSX.
   - consult the VMware Compatibility Guide for Networking and Security. See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security.

- consult the partner documentation for compatibility and upgrade details.

5 If you have Data Security in your environment, uninstall it before upgrading vShield Manager. See Uninstall vShield Data Security.

6 If you are using Cisco Nexus 1000V as an external switch provider, you must migrate those networks to vSphere Distributed Switch before upgrading to NSX. Once NSX is installed, you can migrate the vSphere Distributed Switches to logical switches.

7 Verify that you have a current backup of the vShield Manager, vCenter and other vCloud Networking and Security components. See vCloud Networking and Security Backup and Restore.

8 Create a Tech Support Bundle.

9 Ensure that forward and reverse domain name resolution is working, using the nslookup command.

10 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.

11 Download and stage the upgrade bundle, validate with md5sum. See Download the vShield Manager to NSX Upgrade Bundle and Check the MD5.

12 As a best practice, quiesce all operations in the environment until all sections of the upgrade are complete.

13 Do not power down or delete any vCloud Networking and Security components or appliances before instructed to do so.

## Evaluate License Needs Before Upgrading vCloud Networking and Security to NSX

When you upgrade from vCloud Networking and Security to NSX, your existing license is converted to a NSX for vShield Endpoint license.

Starting in NSX 6.2.3, the default license upon install will be NSX for vShield Endpoint. This license enables use of NSX for deploying and managing vShield Endpoint for anti-virus offload capability only, and has hard enforcement to restrict usage of VXLAN, firewall, and Edge services, by blocking host preparation and creation of NSX Edges.

If you have already have vCloud Networking and Security features deployed, including prepared hosts, virtual wires, vShield App, or vShield Edge, they will continue to function, but you cannot upgrade them to NSX, and you cannot make any changes to them.

If you need other NSX features, including logical switches, logical routers, Distributed Firewall, or NSX Edge, you must either purchase an NSX license to use these features, or request an evaluation license for short-term evaluation of the features.

See the NSX License FAQ https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf

# Operational Impacts of vCloud Networking and Security Upgrades

The vCloud Networking and Security upgrade process can take some time, especially when upgrading ESXi hosts, because hosts must be rebooted. It is important to understand the operational state of vCloud Networking and Security components during an upgrade, such as when some but not all hosts have been upgraded, or when NSX Edges have not yet been upgraded.

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

- vShield Manager
- Host clusters and virtual wires
- vShield App
- vShield Edge
- vShield Endpoint

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

## vCenter Upgrade

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

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

## vShield Manager Upgrade

During:

- vShield Manager configuration is blocked. The vShield API service is unavailable. No changes to the vShield configuration can be made. Existing VM communication continues to function. New VM provisioning continues to work in vSphere, but the new VMs cannot be connected to vShield virtual wires during the vShield Manager upgrade.

After:

- All vShield configuration changes are allowed.

## Host Cluster Upgrade and Virtual Wires

As part of the host cluster upgrade, new VIBs are installed on the hosts.

In NSX, virtual wires are renamed logical switches.

During:

- Configuration changes are not blocked on NSX Manager.
- Upgrade is performed on a per-cluster basis. If DRS is enabled on the cluster, DRS manages the upgrade order of the hosts.

When some NSX hosts in a cluster are upgraded and others are not:

- NSX Manager configuration changes are not blocked. Additions and changes to logical networks are allowed. Provisioning new VMs continues to work on hosts that are not currently undergoing upgrade. Hosts currently undergoing upgrade are placed in maintenance mode, so VMs must be powered off or evacuated to other hosts. This can be done with DRS or manually.

## vShield App Migrated to NSX Distributed Firewall

As part of the host cluster upgrade, the vShield App configuration is migrated to Distributed Firewall.

During:

- While the migration is in progress, existing filters continue to work.
- Do not add or change filters while the migration is in progress.

After:

- Inspect each migrated section and rule to ensure it works as intended.
- After the migration, remove vShield App via the Service Deployment page in NSX.

## vShield Edge Upgrade

vShield Edges can be upgraded without any dependency on host upgrades. You can upgrade a vShield Edge even if you have not yet upgraded the hosts.

**Caution** If you are using a vCloud Director version earlier than 8.10, do not upgrade NSX Edge.. See Determine Whether to Upgrade vShield Edge in a vCloud Director Environment.

During:

- On the vShield Edge device currently being upgraded, configuration changes are blocked.
- Packet forwarding is temporarily interrupted.
- Additions and changes to logical switches are allowed.
- Provisioning new VMs continues to work.

After:

- Configuration changes are not blocked. Any new features introduced in the upgrade to NSX will not be configurable until NSX Controllers are installed and all host clusters have been upgraded to NSX version 6.2.x.
- L2 VPN must be reconfigured after upgrade.
- SSL VPN clients must be reinstalled after upgrade.

### vShield Endpoint Migrated to Guest Introspection

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

During:

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

After:

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

## Verify the vCloud Networking and Security Working State

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

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

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

#### Procedure

1. Identify administrative user IDs and passwords.
2. Verify that forward and reverse name resolution is working for all components.
3. Verify you can log in to all vSphere and vShield components.
4. Note the current versions of vShield Manager, vCenter Server, ESXi and vShield Edges.
5. 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 virtual wire 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.

6 Validate North-South connectivity by pinging out from a VM.

7 Record BGP and OSPF states on the NSX Edge devices.

8 Visually inspect the vShield environment to make sure all status indicators are green, normal, or deployed.

9 Verify that syslog is configured.

10 If possible, in the pre-upgrade environment, create some new components and test their functionality.

11 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 vShield Manager, run the `show tech-support save session` command, and search for "5671" to ensure that all hosts are connected to vShield Manager.

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

## Migrate the Local Admin User to the CLI Admin User

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

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

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

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

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

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

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

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

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

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

  For example, using curl:

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

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

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

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

  - Add a new user tempadmin with the super_user role.

    For example, using curl:

    ```
    curl –k –H 'authorization: Basic YWRtaW46ZGVmYXVsdA==' –H 'Content-Type: application/xml' –X
    PUT https://<vsm-ip>/api/2.0/services/usermgmt/user/local/admin –d
    '<userInfo><userId>tempadmin</userId><password>123</password><fullname>tempadmin</fullname><ema
    il>tempadmin@company.com</email><accessControlEntry><role>super_user</role><resource><resourceI
    d>datacenter-312</resourceId></resource></accessControlEntry></userInfo>'
    ```

- Use tempadmin to delete the Web UI user admin.

  For example, using curl:

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

- Add the super_user role to the CLI user admin.

  For example, using curl:

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

## Uninstall vShield Data Security

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

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

### Procedure

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

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

## vCloud Networking and Security Backup and Restore

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

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

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

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

We recommend taking backups in the following scenarios:

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

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

## Back Up Your vShield Manager Data on Demand

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

### Procedure

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

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

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

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

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

14 Click **Backup**.

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

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

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

## Back Up vSphere Distributed Switches

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

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

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

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

## Back Up vCenter

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

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

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

Useful links for vCenter 5.5:

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

Useful links for vCenter 6.0:

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

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

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

### Prerequisites

An MD5 checksum tool.

### Procedure

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

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

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

   Change it to:

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

   Otherwise, after uploading the upgrade bundle, the following error message appears: "Invalid upgrade bundle file VMware-vShield-Manager-upgrade-bundle-to-NSX-6.x.x-xxxxx,gz, upgrade file name has extension tar.gz."
3. Use an MD5 checksum tool to compare the upgrade bundle's official MD5 sum shown on the VMware Web site with the MD5 sum calculated by the checksum tool.
   a. In the MD5 checksum tool, browse to the upgrade bundle.
   b. Use the tool to calculate the checksum of the bundle.
   c. Paste in the checksum listed on the VMware Web site.
   d. Use the tool to compare the two checksums.

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

## Additional Upgrade Preparation Steps for vCloud Director Environments

vCloud Director Network Isolation (VCDNI) is supported with NSX, but is a deprecated technology.

Before VXLAN gained mass adoption, vCloud Director relied on vCloud network isolation technology to provide a logical network overlay. This MAC-in-MAC proprietary encapsulation technology is still supported, however, support for this technology is now deprecated. Unlike VXLAN logical networks, VCDNI logical networks are created directly by vCloud Director, which communicates with ESXi hosts through the vCloud Agent running in the VMkernel. Therefore, a vCloud Networking and Security upgrade has no impact on VCDNI networks and there is no limitation of using them together with NSX.

You are, however, encouraged to use VXLAN technology because VCDNI is a deprecated technology and is supported only for legacy deployments.

# Upgrade from vCloud Networking and Security 5.5.x to NSX 6.2.x

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

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

1 Upgrade vShield Manager to NSX Manager

2 Deploy NSX Controller cluster - optional, required for logical (distributed) routers and changing control plane mode to hybrid or unicast

3 Update host clusters

4 Update Transport Zone - optional, if NSX Controller cluster is deployed, can change control plane mode to hybrid or unicast

5 Upgrade vShield App to NSX Distributed Firewall

6 Upgrade vShield Edge to NSX Edge

7 Upgrade vShield Endpoint to NSX Guest Introspection

The upgrade process is managed by the vShield 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.

**Important** If you have virtual wires in your environment, once you have upgraded to NSX Manager you must update your host clusters.

## Upgrade vShield Manager to NSX Manager

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

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

### Prerequisites

- Verify you have completed all the upgrade preparation tasks described in Preparing for the vCloud Networking and Security to NSX Upgrade, including checking system requirements and performing backups.
- Verify that vShield Manager has sufficient disk space for the upgrade to NSX Manager. See System Requirements for NSX.
- Increase the vShield Manager virtual appliance's reserved memory to at least 16 GB and allocate 4 vCPU before upgrading to NSX 6.2.x.

  See System Requirements for NSX.
- Verify that vShield Edge instances prior to version 5.5, if any, have been upgraded to version vShield 5.5.

  Pre-5.5 vShield Edge instances cannot be managed or deleted after vShield Manager has been upgraded to NSX Manager.

### Procedure

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

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

   The Summary tab displays the version of NSX Manager that you just installed.
9. Navigate to **Home > Manage vCenter Registration** and verify that the vCenter Server status is `Connected`.
10. Close any existing browser sessions accessing the vSphere Web Client. Wait a few minutes and clear the browser cache before logging back in to the vSphere Web Client.

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

---

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

Passwords in vCloud Networking and Security

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

Passwords after upgrade to NSX

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

---

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

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

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

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

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

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

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

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

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

Install and Assign an NSX License.

## Install and Assign an NSX License

You can install and assign an NSX for vSphere license after the NSX Manager upgrade is complete by using the vSphere Web Client.

Starting in NSX 6.2.3, the default license upon install will be NSX for vShield Endpoint. This license enables use of NSX for deploying and managing vShield Endpoint for anti-virus offload capability only, and has hard enforcement to restrict usage of VXLAN, firewall, and Edge services, by blocking host preparation and creation of NSX Edges.

If you need other NSX features, including logical switches, logical routers, Distributed Firewall, or NSX Edge, you must either purchase an NSX license to use these features, or request an evaluation license for short-term evaluation of the features.

See the NSX License FAQ https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf

For more information about NSX licensing, see http://www.vmware.com/files/pdf/vmware-product-guide.pdf.

### Procedure

- In vSphere 5.5, complete the following steps to add a license for NSX.
  a. Log in to the vSphere Web Client.
  b. Click **Administration** and then click **Licenses**.
  c. Click the **Solutions** tab.
  d. Select NSX for vSphere in the Solutions list. Click **Assign a license key**.
  e. Select **Assign a new license key** from the drop-down menu.
  f. Type the license key and an optional label for the new key.
  g. Click **Decode**.

     Decode the license key to verify that it is in the correct format, and that it has enough capacity to license the assets.
  h. Click **OK**.
- In vSphere 6.0, complete the following steps to add a license for NSX.
  a. Log in to the vSphere Web Client.
  b. Click **Administration** and then click **Licenses**.
  c. Click the **Assets**tab, then the **Solutions** tab.
  d. Select NSX for vSphere in the Solutions list. From the **All Actions** drop-down menu, select **Assign license...**.

e Click the **Add ( )** icon. Enter a license key and click **Next**. Add a name for the license, and click **Next**. Click **Finish** to add the license.

f Select the new license.

g (Optional) Click the **View Features** icon to view what features are enabled with this license. View the **Capacity** column to view the capacity of the license.

h Click **OK** to assign the new license to NSX.

### What to do next

Deploy NSX Controller Cluster.

If you are not deploying controllers, Update Host Clusters.

## Deploy NSX Controller Cluster

NSX Controller is an advanced distributed state management system that provides control plane functions for NSX logical switching and routing functions. It serves as the central control point for all logical switches within a network and maintains information about all hosts, logical switches (VXLANs), and distributed logical routers. Controllers are required if you are planning to deploy 1) distributed logical routers or 2) VXLAN in unicast or hybrid mode.

No matter the size of the NSX deployment, VMware requires that each NSX Controller cluster contain three controller nodes. Having a different number of controller nodes is not supported.

The cluster requires that each controller's disk storage system has a peak write latency of less than 300ms, and a mean write latency of less than 100ms. If the storage system does not meet these requirements, the cluster can become unstable and cause system downtime.

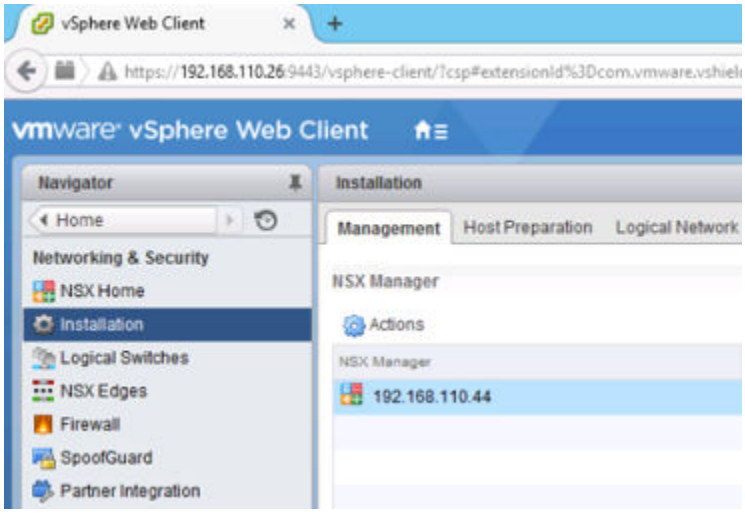
### Prerequisites

- Before deploying NSX Controllers, you must deploy an NSX Manager appliance and register vCenter with NSX Manager.
- Determine the IP pool settings for your controller cluster, including the gateway and IP address range. DNS settings are optional. The NSX Controller IP network must have connectivity to the NSX Manager and to the management interfaces on the ESXi hosts.

### Procedure

1 In vCenter, navigate to **Home > Networking & Security > Installation** and select the **Management** tab.

For example:

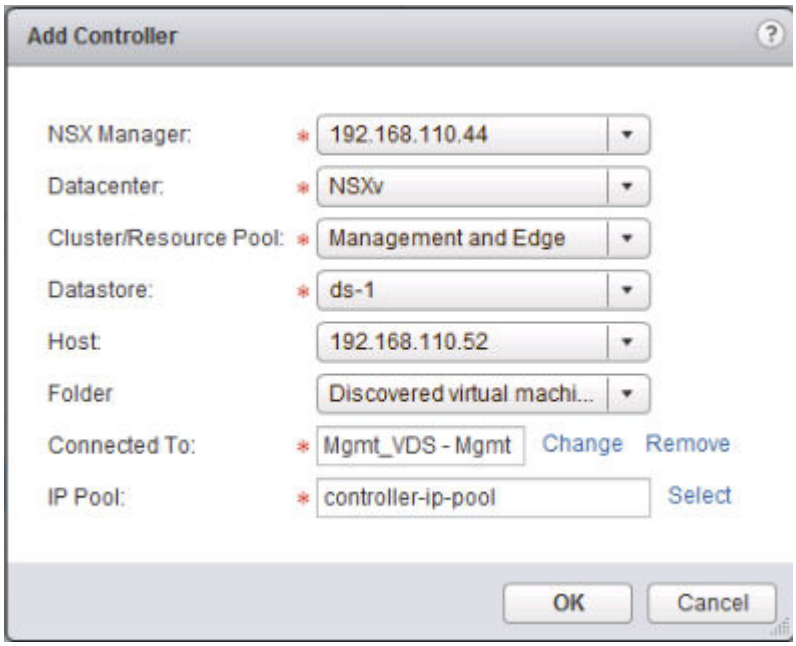



2 In the NSX Controller nodes section, click the **Add Node** ( ) icon.

3 Enter the NSX Controller settings appropriate to your environment.

NSX Controllers should be deployed to a vSphere Standard Switch or vSphere Distributed Switch port group which is not VXLAN based and has connectivity to the NSX Manager, other controllers, and to hosts via IPv4.

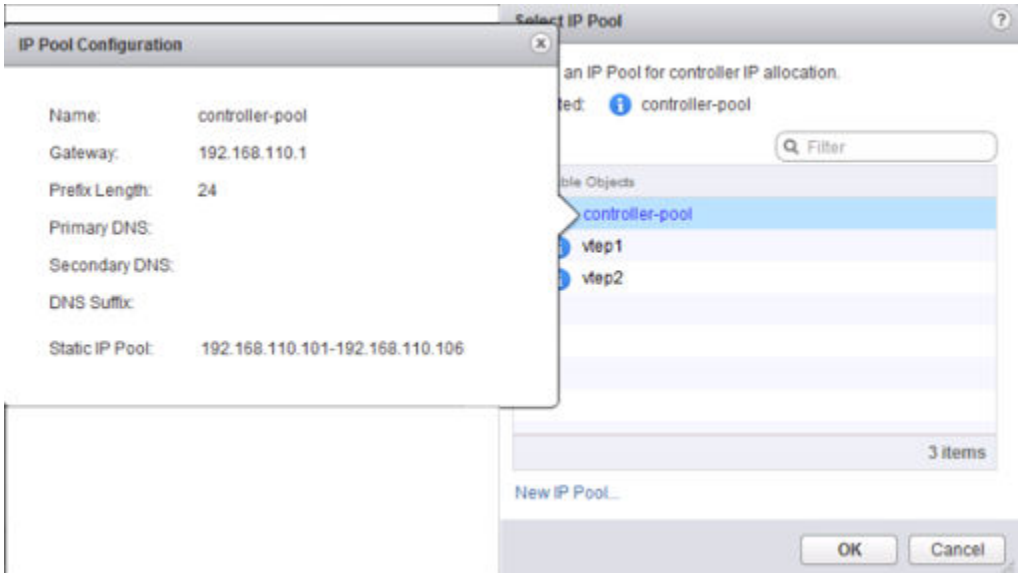
For example:



4 If you have not already configured an IP pool for your controller cluster, configure one now by clicking **New IP Pool**.

Individual controllers can be in separate IP subnets, if necessary.

For example:




5 Type and re-type a password for the controller.

**Note** Password must not contain the username as a substring. Any character must not consecutively repeat 3 or more times.

The password must be at least 12 characters and must follow 3 of the following 4 rules:

- At least one upper case letter
- At least one lower case letter
- At least one number
- At least one special character

6 After the first controller is completely deployed, deploy two additional controllers.

Having three controllers is mandatory. We recommend configuring a DRS anti-affinity rule to prevent the controllers from residing on the same host.

### What to do next

Update Host Clusters

# Update Host Clusters

You must prepare your environment for network virtualization by installing network infrastructure components on a per-cluster level for each vCenter server. This deploys the required software on all hosts in the cluster and renames virtual wires to NSX logical switches. During this process, each host in the cluster receives a software update and is then rebooted.

If you have virtual wires in your environment, once you have upgraded to NSX Manager you must update your host clusters.

It is recommended that you update host clusters in a datacenter maintenance window.

If DRS is enabled, monitor the progress of host evacuation, hosts entering maintenance mode, and host reboot. If DRS is disabled or in manual mode, host evacuations and reboots must be done manually. During host preparation, warnings may occur and can be seen by clicking the warning icon, click **Resolve** where required.

While the upgrade is in progress, do not deploy, upgrade, or uninstall any service or component.

**Note** VTEPs that were created in vCloud Networking and Security use DHCP or manually assigned IP addresses, not IP pools.

### Prerequisites

- Verify that vShield Manager has been upgraded to NSX Manager.
- Verify that the VXLAN Column in Host Preparation tab displays **Enabled**.
- Verify that 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.
  - Verify that DRS is enabled on the host clusters.
  - Verify that vMotion functions correctly.
  - Verify the host connection state with vCenter.
  - Verify 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.

### Procedure

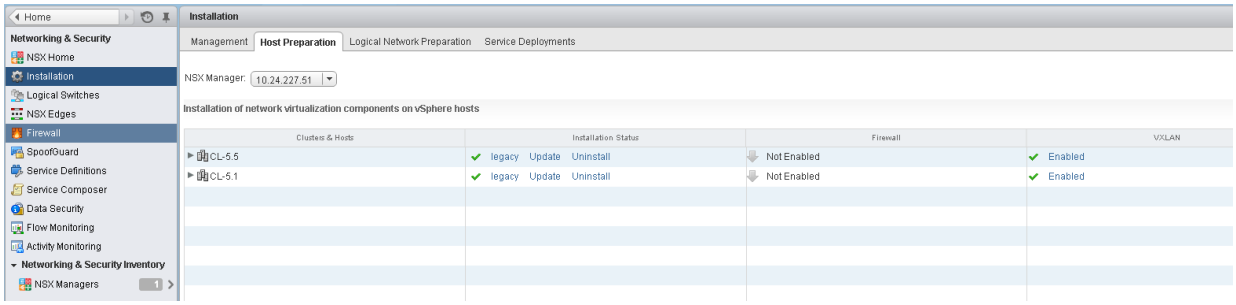
1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **Installation**.

3 Click the **Host Preparation** tab.

All clusters in your infrastructure are displayed.

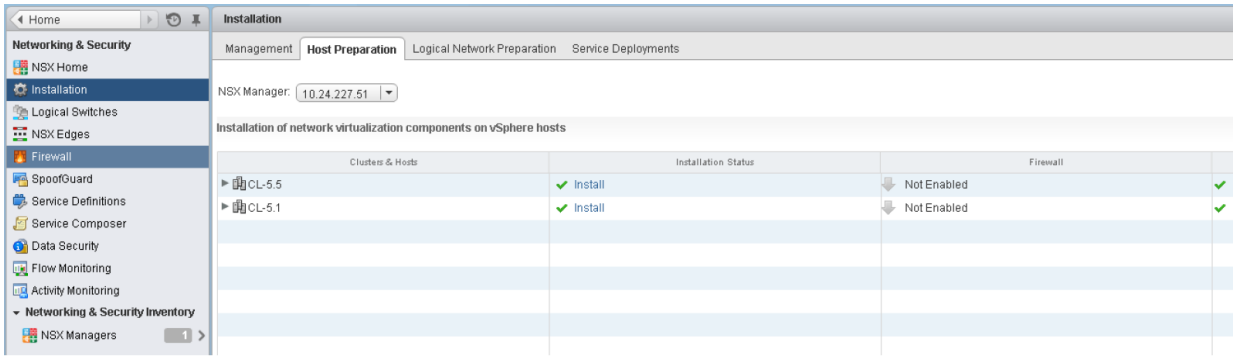
If you had Virtual Wires in your 5.5 environment, the **Installation Status** column displays **legacy**, **Update**, and **Uninstall**.

**Figure 1-1. Installation Status displays Update when you have Virtual Wires in your 5.5 environment**




If you did not have Virtual Wires in your 5.5 environment, the **Installation Status** column displays **Install**.

**Figure 1-2. Installation Status displays Install when you do not have Virtual Wires in your 5.5 environment**




4 For each cluster, click **Update** or **Install** in the Installation Status column.

Each host in the cluster receives the new logical switch software.

The host upgrade initiates a host scan. The old VIBs are removed (though they are not completely deleted until after the reboot). New VIBs are installed on the altboot partition. To view the new VIBs on a host that has not yet rebooted, you can run the `esxcli software vib list --rebooting-image | grep esx` command.

5 Monitor the installation until the **Installation Status** column displays a green check mark.

If the cluster has DRS enabled, DRS attempts to reboot the hosts in a controlled fashion that allows the VMs to continue running. vMotion moves the running VMs to other hosts in the cluster and places the host into maintenance mode.

If hosts 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**. Click ⚠ to display the errors.

After manually evacuating the hosts, select the cluster and click the **Resolve** action. The **Resolve** action attempts to complete the upgrade and reboot all hosts in the cluster. If the host reboot fails for any reason, the **Resolve** action halts. 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.

All virtual wires from your 5.5 infrastructure are renamed to NSX logical switches, and the VXLAN column for the cluster says **Enabled**.

Ensure that the VXLAN Column in the Host Preparation tab displays **Enabled**.

When the cluster is updated, the **Installation Status** column displays the software version that you have updated to.

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

- esx-vsip
- esx-vxlan

**Note** In NSX 6.2, the esx-dvfilter-switch-security VIB is included within the esx-vxlan VIB.

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.

### What to do next

Change VXLAN Port

## Change VXLAN Port

You can change the port used for VXLAN traffic.

In NSX 6.2.3 and later, the default VXLAN port is 4789, the standard port assigned by IANA. Before NSX 6.2.3, the default VXLAN UDP port number was 8472.

Any new NSX installations will use UDP port 4789 for VXLAN.

If you upgrade from NSX 6.2.2 or earlier to NSX 6.2.3 or later, and your installation used the old default (8472), or a custom port number (for example, 8888) before the upgrade, that port will continue to be used after the upgrade unless you take steps to change it.

If your upgraded installation uses or will use hardware VTEP gateways (ToR gateways), you must switch to VXLAN port 4789.

Cross-vCenter NSX does not require that you use 4789 for the VXLAN port, however, all hosts in a cross-vCenter NSX environment must be configured to use the same VXLAN port. If you switch to port 4789, this will ensure that any new NSX installations added to the cross-vCenter NSX environment are using the same port as the existing NSX deployments.

Changing the VXLAN port is done in a three phase process, and will not interrupt VXLAN traffic.

1 NSX Manager configures all hosts to listen for VXLAN traffic on both the old and new ports. Hosts continue to send VXLAN traffic on the old port.

2 NSX Manager configures all hosts to send traffic on the new port.

3 NSX Manager configures all hosts to stop listening on the old port, all traffic is sent and received on the new port.

In a cross-vCenter NSX environment you must initiate the port change on the primary NSX Manager. For each stage, the configuration changes are made on all hosts in the cross-vCenter NSX environment before proceeding to the next stage.

#### Prerequisites

- Verify that the port you want to use for VXLAN is not blocked by a firewall.
- Verify that host preparation is not running at the same time as the VXLAN port change.

#### Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Installation**.

3 Click the **Logical Network Preparation** tab, then click **VXLAN Transport**.

4 Click the **Change** button in the VXLAN Port panel. Enter the port you want to switch to. 4789 is the port assigned by IANA for VXLAN.

It will take a short time for the port change to propagate to all hosts.

5 (Optional) Check the progress of the port change with the `GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus` API request.

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

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

...

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

### What to do next

Update Transport Zones and Logical Switches.

## Update Transport Zones and Logical Switches

If you deploy an NSX Controller cluster, you do not have to rely on multicast for logical networks. You can update the control plane mode on your transport zones and logical switches to unicast or hybrid.

The change of control plane mode and migration of existing logical switches has no impact on the networking data plane traffic.

### Procedure

1. In the vSphere Web Client, navigate to **Home > Networking & Security > Installation > Logical Network Preparation > Transport Zones**.
2. Select your transport zone, and click **Actions > Edit Settings**. Select the desired replication mode.
   - **Multicast**: Multicast IP addresses in the physical network are used for the control plane. This mode is recommended only when you are upgrading from older VXLAN deployments. Requires PIM/IGMP in the physical network.
   - **Unicast**: The control plane is handled by an NSX controller. All unicast traffic leverages optimized headend replication. No multicast IP addresses or special network configuration is required.
   - **Hybrid**: Offloads local traffic replication to the physical network (L2 multicast). This requires IGMP snooping on the first-hop switch and access to an IGMP querier in each VTEP subnet, but does not require PIM. The first-hop switch handles traffic replication for the subnet.
3. Select the check box for **Migrate existing Logical Switches to the new control plane mode** and click **OK**.

### What to do next

Upgrade vShield App to Distributed Firewall.

# Upgrade vShield App to Distributed Firewall

You can upgrade to Distributed Firewall only from vShield App version 5.5. If you have a prior version of vShield App in your infrastructure, you must upgrade to version 5.5 before upgrading to version 6.2.x. For information on upgrading to version 5.5, see *vShield Installation and Upgrade Guide* version 5.5.

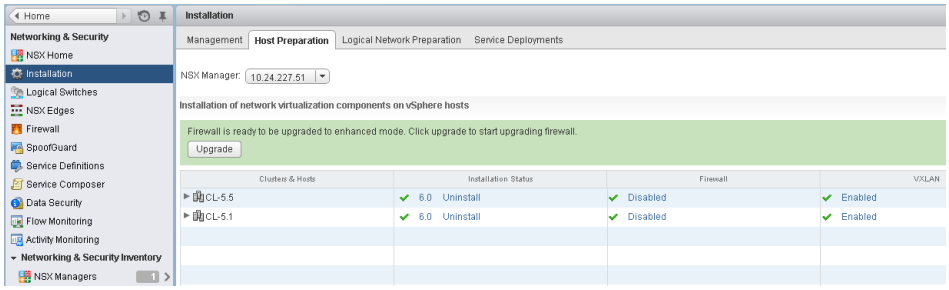
The duration of the following procedure depends on the number of rules in your environment. When you migrate from vShield App to NSX distributed firewall (enhanced mode), the rules are migrated and pushed. This causes a traffic disruption. This work should be completed during a maintenance window.

### Prerequisites

- vShield Manager has been upgraded to NSX Manager.
- Virtual wires have been upgraded to NSX Logical Switches. For non-VXLAN users, network virtualization components have been installed.
- If you want to migrate vShield App 5.5 rules to Distributed Firewall, do not delete the vShield App appliances before upgrading to Distributed Firewall.

### Procedure

1 After you prepare all clusters in your environment for network virtualization components, a message indicates that Firewall is ready to be upgraded.




2 Click **Upgrade**.

vShield App 5.5 rules are migrated to NSX in the following way:

a A new section is created in the central firewall table for each namespace (datacenter and virtual wire) configured in vShield App version 5.5. Each section includes the corresponding firewall rules.

b All rules in each section have the same value in the **AppliedTo** field - datacenter ID for datacenter namespace, virtual wire ID for virtual wire namespace, and port group ID for port group based namespace.

c Containers created at different namespace levels are moved to the global level.

d Section order is as below to ensure that firewall behavior after the upgrade remains the same:

*Section_Namespace_Portgroup-1*

.....

*Section_Namespace_Portgroup-N*

*Section_Namespace_VirtualWire-1*

.....

*Section_Namespace_VirtualWire-N*

*Section_Namespace_Datacenter_1*

.....

*Section_Namespace_Datacenter_N*

*Default_Section_DefaultRule*

After the upgrade is complete, the Firewall column displays **Enabled**.

3. Click on **Home > Hosts and Clusters** and navigate to the hosts that have vShield App service virtual machines running. Shut down the legacy vShield App service virtual machines.
4. Navigate to **Networking & Security > Firewall** and nspect each upgraded section and rule and test that it works as intended.
5. Navigate to the **Installation > Service Deployments** tab and ensure that all alarms are resolved and that the legacy vShield App service status displays **Succeeded**.
6. If the rules are working correctly, from the **Service Deployments** tab, select vShield App and click **Delete Service Deployment (✖)** to delete the legacy vShield App service virtual machines.

### What to do next

Upgrade vShield Edge to NSX Edge

## Upgrade vShield Edge to NSX Edge

You can upgrade only from version vShield 5.5 to NSX Edge 6.2.x. If you have a prior version of vShield Edge in your infrastructure, you must upgrade to version 5.5 before upgrading to version 6.2.x. For information on upgrading to version 5.5, see *vShield Installation and Upgrade Guide* version 5.5.

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 minimizing the impact by configuring the Edge to work in ECMP mode.

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

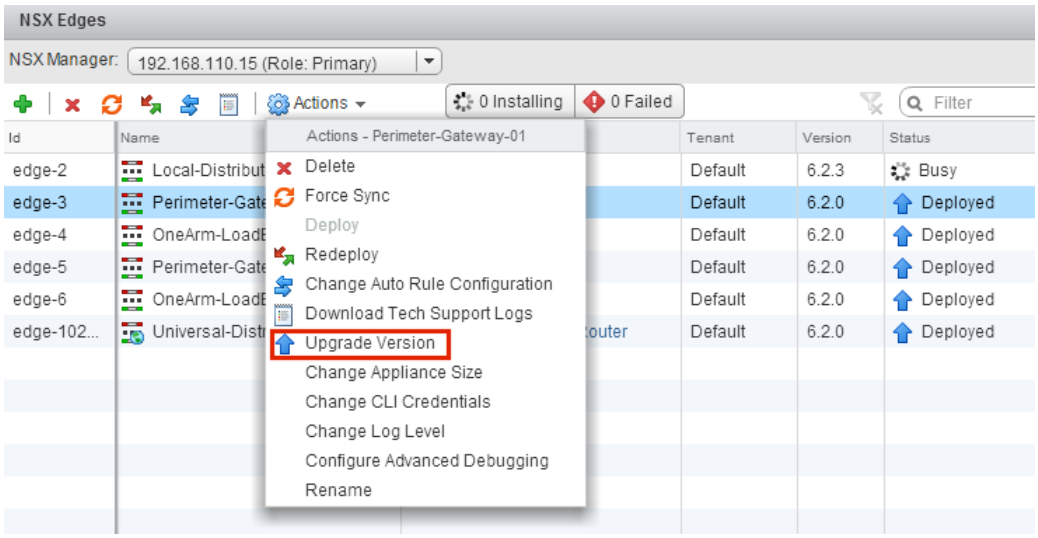
### Prerequisites

- Verify vShield Manager has been upgraded to NSX Manager.

- Understand the operational impact of the NSX Edge upgrade while the upgrade is in progress. See Operational Impacts of vCloud Networking and Security Upgrades.
- 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 will be two NSX Edge appliances of the appropriate size in the poweredOn state during upgrade.
  - Starting in NSX 6.2.3, when upgrading an NSX Edge instance with high availability, both replacement appliances are deployed before replacing the old appliances. This means there will be 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.
  - Prior to NSX 6.2.3, when upgrading an NSX Edge instance with high availability, only one replacement appliance is deployed at time while replacing the old appliances. This means there will be three NSX Edge appliances of the appropriate size in the poweredOn state during the upgrade of a given NSX Edge. Once the NSX Edge instance is upgraded, usually the NSX Edge appliance with HA index 0 becomes active.
- Upgrading an NSX Edge with version 5.5 or 6.0 with L2 VPN enabled is not supported. 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. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. 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.

NSX Edge firewall rules do not support sourcePort, so vShield Edge version 5.5 rules containing sourcePort are modified during the upgrade as follows.

- If there are no applications used in the rule, a service is created with protocol=any, port=any and sourcePort=asDefinedInTheRule.
- If there are applications or applicationGroups used in the rule, these grouping objects are duplicated by adding the sourcePort to them. Because of this, the groupingObjectIds used in the firewall rule change after the upgrade.

User firewall rules in NSX Edge 6.x do not generate internal IPSets and applicationSets based on input from REST APIs. Instead they will be retained in the raw format. During upgrade, the internally generated IPSet and applicationSets are used to create rules with raw data. The internal groupingObjects will no longer appear in the user firewallRules

### What to do next

If needed, reconfigure any L2 VPN configurations. See L2 VPN Overview in the *NSX Installation Guide*.

Upgrade Guest Introspection

## Upgrade vShield Endpoint to NSX Guest Introspection

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

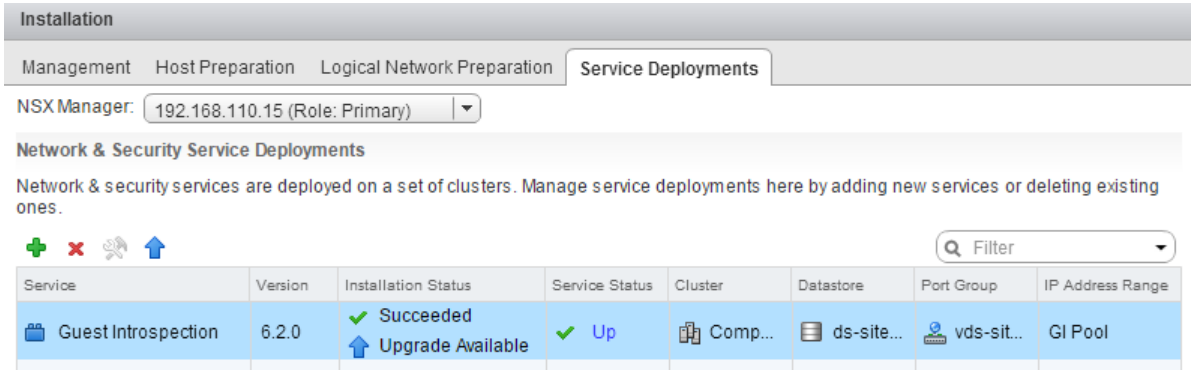
**Note** The Guest Introspection service VMs can be upgraded from the vSphere Web Client. You do not need to delete the service VM after the upgrade of the NSX Manager to upgrade it. If you do delete the service VM, the Service Status will be shown as `Failed` because the Agent VM is missing. Click on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

### Prerequisites

NSX Manager, controllers, prepared host clusters, and NSX Edges must have been upgraded to 6.2.x.

### Procedure

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

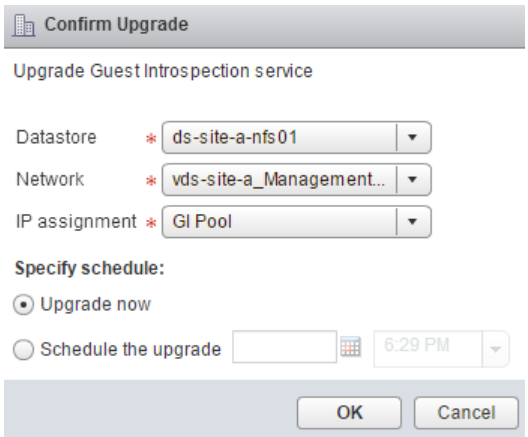



The **Installation Status** column says **Upgrade Available**.

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.

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

# NSX Services That Do Not Support Direct Upgrade

Some NSX services, such as VMware Partner Security Virtual Appliances, 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.

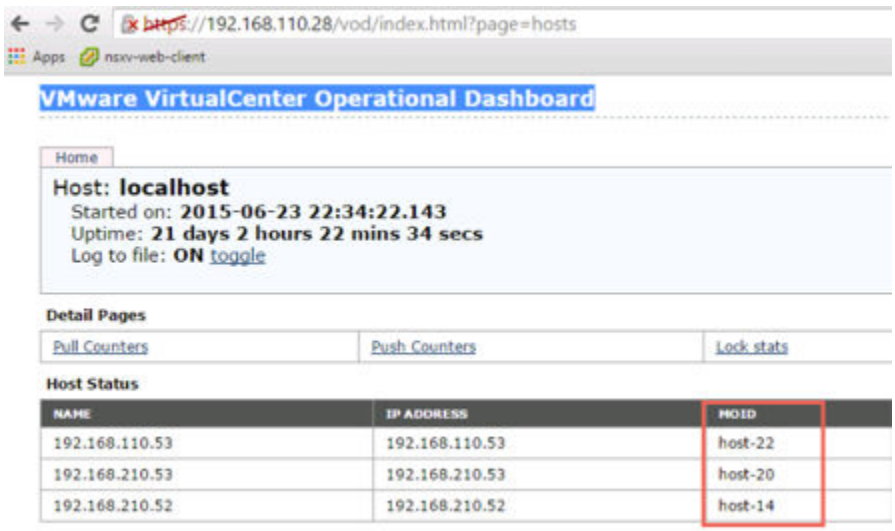
## NSX Data Security

You should uninstall NSX data security before upgrading NSX and then reinstall it after the NSX upgrade is complete. If you have already upgraded NSX without first uninstalling NSX data security, you must uninstall data security using a REST API call.

Issue the following API call:

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

The host-id is the MOID of the ESXi host. To retrieve the MOID, open the VMware VirtualCenter Operational Dashboard: https://<vcenter-ip>/vod/index.html?page=hosts.




For the ESXi host with the MOID "host-22" on vCenter Server 192.168.110.28, the API call would be formatted as follows:

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

Make sure to issue the API call on all of your ESXi hosts.

After data security is uninstalled, you can install the new version. See Install NSX Data Security.

## 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 6.2.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 versions 5.5.x or 6.0.x. Any L2 VPN configuration must be deleted before you can upgrade the NSX Edge.

## Install NSX Data Security

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

### Prerequisites

NSX Guest Introspection must be installed on the cluster where you are installing Data Security.

If you want to assign an IP address to the Data Security service virtual machine from an IP pool, create the IP pool before installing Data Security. See Grouping Objects in the *NSX Administration Guide*.

### Procedure

1. In the **Installation** tab, click **Service Deployments**.
2. Click the **New Service Deployment** ( ) icon.
3. In the Deploy Network and Security Services dialog box, select **Data Security** and click **Next**.
4. In **Specify schedule** (at the bottom of the dialog box), select **Deploy now** to deploy Data Security as soon as it is installed or select a deployment date and time.
5. Click **Next**.
6. Select the datacenter and cluster(s) where you want to install Data Security and click **Next**.
7. On the Select storage and Management Network page, select the datastore on which to add the service virtual machines storage or select **Specified on host**.

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

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

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

   If the datastore is set to **Specified on host**, the network to be used must be specified in the **agentVmNetwork** property of each host in the cluster. See *vSphere API/SDK Documentation*.

   When you add a host(s) to the cluster, the **agentVmNetwork** property for the host must be set before it is added to the cluster.

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

9 In IP assignment, select one of the following:

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

   Note that static IP address are not supported.

10 Click **Next** and then click **Finish** on the Ready to complete page.

11 Monitor the deployment until the **Installation Status** column displays **Succeeded**.

12 If the **Installation Status** column displays **Failed**, click the icon next to Failed. All deployment errors are displayed. Click **Resolve** to fix the errors. In some cases, resolving the errors displays additional errors. Take the required action and click **Resolve** again.

## 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 from vCloud Networking and Security 5.5.x to NSX in a vCloud Director Environment

The version of vCloud Director will determine the version of NSX you can upgrade to. VMware recommends upgrading to the latest supported NSX version that is compatible with the other solutions and tools in your environment.

See the VMware Product Interoperability Matrix at https://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

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

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

1 Upgrade vShield Manager to NSX Manager

2 Deploy NSX Controller cluster - optional, required for logical (distributed) routers and changing control plane mode to hybrid or unicast

3 Update host clusters

4 Update Transport Zone - optional, if NSX Controller cluster is deployed, can change control plane mode to hybrid or unicast

5 NSX Edge - upgrade to NSX Edge only if you are using vCloud Director 8.10 or later.

---

**Important** If you have virtual wires in your environment, once you have upgraded to NSX Manager you must update your host clusters.

---

Optional vCloud Networking and Security components not integrated with vCloud Director:

1 vShield App - see Upgrade vShield App to Distributed Firewall

2 vShield Endpoint - see Upgrade vShield Endpoint to NSX Guest Introspection.

3 vShield Data Security - does not support upgrade. See uninstall instructions: NSX Services That Do Not Support Direct Upgrade and installation instructions: Install NSX Data Security.

# Upgrade vShield Manager to NSX Manager in a vCloud Director Environment

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

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

### Prerequisites

- Verify you have completed all the upgrade preparation tasks described in Preparing for the vCloud Networking and Security to NSX Upgrade, including checking system requirements and performing backups.
- Verify that vShield Manager has sufficient disk space for the upgrade to NSX Manager. See System Requirements for NSX.
- Increase the vShield Manager virtual appliance's reserved memory to at least 16 GB and allocate 4 vCPU before upgrading to NSX 6.2.x.

  See System Requirements for NSX.
- Verify that vShield Edge instances prior to version 5.5, if any, have been upgraded to version vShield 5.5.

  Pre-5.5 vShield Edge instances cannot be managed or deleted after vShield Manager has been upgraded to NSX Manager.

### Procedure

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

   Uploading the file takes a few minutes.
6. Click **Install** to begin the upgrade process.
7. Click **Confirm Install**. The upgrade process reboots vShield Manager, so you might lose connectivity to the vShield Manager user interface. None of the other vShield components are rebooted.

8 After the reboot, log in to the NSX Manager virtual appliance by opening a Web browser window and typing the IP address, for example, https://10.10.10.10. The upgraded NSX Manager has the same IP address as the vShield Manager.

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

9 Navigate to **Home > Manage vCenter Registration** and verify that the vCenter Server status is `Connected`.

10 Close any existing browser sessions accessing the vSphere Web Client. Wait a few minutes and clear the browser cache before logging back in to the vSphere Web Client.

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

---

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

Passwords in vCloud Networking and Security

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

Passwords after upgrade to NSX

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

---

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

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

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

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

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

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

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

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

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

Install and Assign an NSX License in a vCloud Director Environment

## Install and Assign an NSX License in a vCloud Director Environment

You can install and assign an NSX for vSphere license after NSX Manager upgrade is complete by using the vSphere Web Client.

Starting in NSX 6.2.3, the default license upon install will be NSX for vShield Endpoint. This license enables use of NSX for deploying and managing vShield Endpoint for anti-virus offload capability only, and has hard enforcement to restrict usage of VXLAN, firewall, and Edge services, by blocking host preparation and creation of NSX Edges.

To use NSX with vCloud Director, you must purchase an NSX license to cover additional required NSX features, including NSX Edge.

See the NSX License FAQ https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf

For more information about NSX licensing, see http://www.vmware.com/files/pdf/vmware-product-guide.pdf.

### Procedure

- In vSphere 5.5, complete the following steps to add a license for NSX.
  a. Log in to the vSphere Web Client.
  b. Click **Administration** and then click **Licenses**.
  c. Click the **Solutions** tab.
  d. Select NSX for vSphere in the Solutions list. Click **Assign a license key**.
  e. Select **Assign a new license key** from the drop-down menu.
  f. Type the license key and an optional label for the new key.

g Click **Decode**.

Decode the license key to verify that it is in the correct format, and that it has enough capacity to license the assets.

h Click **OK**.

- In vSphere 6.0, complete the following steps to add a license for NSX.

a Log in to the vSphere Web Client.

b Click **Administration** and then click **Licenses**.

c Click the **Assets**tab, then the **Solutions** tab.

d Select NSX for vSphere in the Solutions list. From the **All Actions** drop-down menu, select **Assign license...**.

e Click the **Add (** **)** icon. Enter a license key and click **Next**. Add a name for the license, and click **Next**. Click **Finish** to add the license.

f Select the new license.

g (Optional) Click the **View Features** icon to view what features are enabled with this license. View the **Capacity** column to view the capacity of the license.

h Click **OK** to assign the new license to NSX.

### What to do next

Deploy NSX Controller Cluster for NSX in a vCloud Director Environment (optional, allows you to choose a control plane mode other than multicast).

If you are not deploying controllers, Update Host Clusters from vCNS to NSX in a vCloud Director Environment

## Deploy NSX Controller Cluster for NSX in a vCloud Director Environment

NSX Controller is an advanced distributed state management system that provides control plane functions for NSX logical switching and routing functions. It serves as the central control point for all logical switches within a network and maintains information about all hosts, logical switches (VXLANs), and distributed logical routers. Controllers are required if you are planning to deploy 1) distributed logical routers or 2) VXLAN in unicast or hybrid mode.

No matter the size of the NSX deployment, VMware requires that each NSX Controller cluster contain three controller nodes. Having a different number of controller nodes is not supported.

### Prerequisites

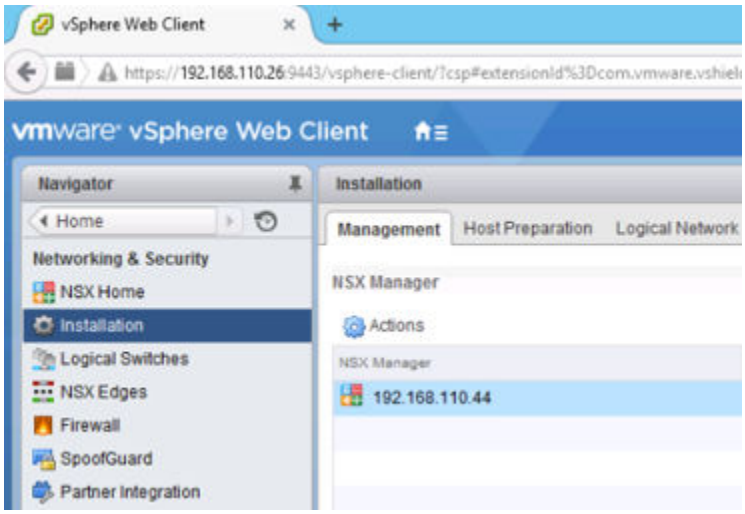
- Before deploying NSX Controllers, you must deploy an NSX Manager appliance and register vCenter with NSX Manager.

- Determine the IP pool settings for your controller cluster, including the gateway and IP address range. DNS settings are optional. The NSX Controller IP network must have connectivity to the NSX Manager and to the management interfaces on the ESXi hosts.

**Procedure**

1 In vCenter, navigate to **Home > Networking & Security > Installation** and select the **Management** tab.

For example:

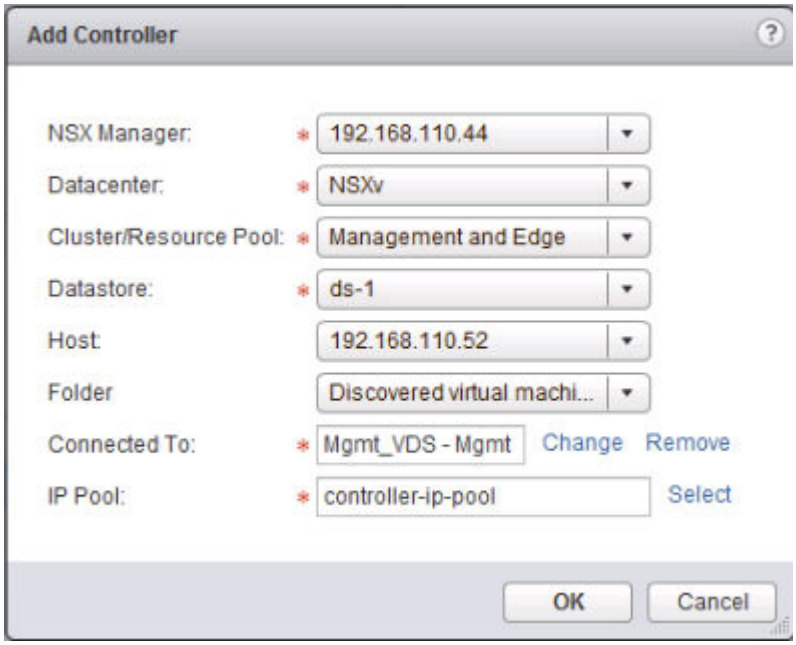



2 In the NSX Controller nodes section, click the **Add Node** ( ) icon.

3 Enter the NSX Controller settings appropriate to your environment.

NSX Controllers should be deployed to a vSphere Standard Switch or vSphere Distributed Switch port group which is not VXLAN based and has connectivity to the NSX Manager, other controllers, and to hosts via IPv4.

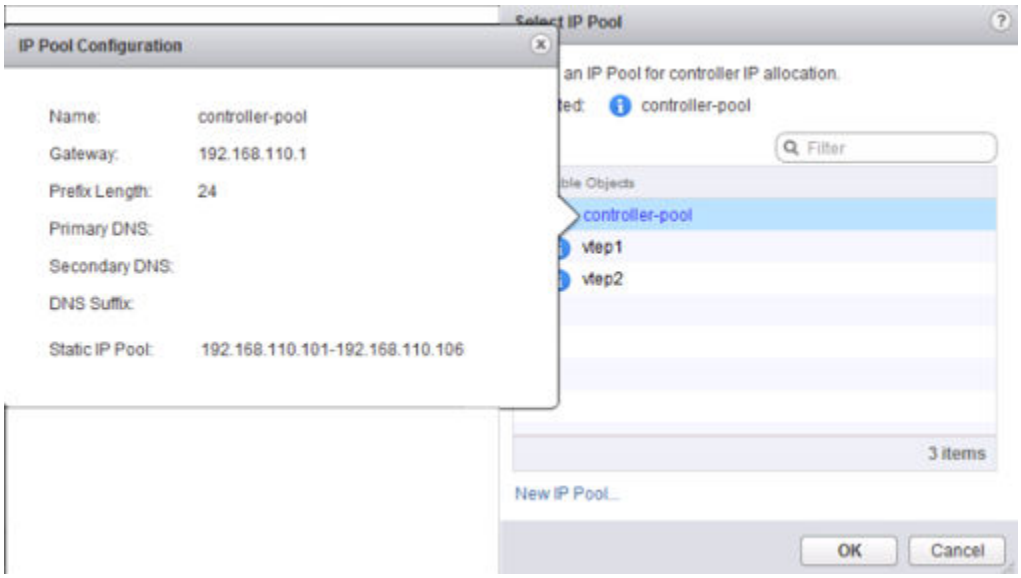
For example:




4 If you have not already configured an IP pool for your controller cluster, configure one now by clicking **New IP Pool**.

Individual controllers can be in separate IP subnets, if necessary.

For example:



5 Type and re-type a password for the controller.

**Note** Password must not contain the username as a substring. Any character must not consecutively repeat 3 or more times.

The password must be at least 12 characters and must follow 3 of the following 4 rules:

- At least one upper case letter
- At least one lower case letter
- At least one number
- At least one special character

6 After the first controller is completely deployed, deploy two additional controllers.

Having three controllers is mandatory. We recommend configuring a DRS anti-affinity rule to prevent the controllers from residing on the same host.

When successfully deployed, the controllers have a **Normal** status and display a green check mark.

SSH to each controller and make sure they can ping the host management interface IP addresses. If the ping fails, make sure all controllers have the correct default gateway. To view a controller routing table, run the **show network routes** command. To change a controller's default gateway run the **clear network routes** command followed by the **add network default-route <IP-address>** command.

Run the following commands to verify the control cluster is behaving as expected.

- `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.

- `show control-cluster roles`

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

  One controller node will be the master for each role. In this example, a single node is the master for all roles.

  If a master NSX Controller instance for a role fails, the cluster elects a new master for that role from the available NSX Controller instances.

  NSX Controller instances are on the control plane, so an NSX Controller failure does not affect data plane traffic.

- `show control-cluster connections`

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

  This command shows the intra-cluster communication status.

  The controller cluster majority leader listens on port 2878 (as shown by the “Y” in the “listening” column). The other controller nodes will have a dash (-) in the “listening” column for Port 2878.

  All other ports should be listening on all three controller nodes.

  The open conns column shows the number of open connections that the controller node has with other controller nodes. In a 3-node controller cluster, the controller node should have no more than two open connections.

### What to do next

**Caution** While a controller status is **Deploying**, do not add or modify logical switches or distributed routing in your environment. Also, do not continue to the host preparation procedure. After a new controller is added to the controller cluster, all controllers are inactive for a short while (no more than 5 minutes). During this downtime, any operation related to controllers---for example, host preparation---might have unexpected results. Even though host preparation might seem to complete successfully, the SSL certification might not establish correctly, thus causing issues in the VXLAN network.

If you need to delete a deployed controller, see Recover from an NSX Controller Failure in the *NSX Administration Guide*.

On the hosts where the NSX Controller nodes are first deployed, NSX enables automatic VM startup/shutdown. If the controller node VMs are later migrated to other hosts, the new hosts might not have automatic VM startup/shutdown enabled. For this reason, VMware recommends that you check all hosts in the cluster to make sure that automatic VM startup/shutdown is enabled. See http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-5FE08AC7-4486-438E-AF88-80D6C7928810.html.

## Update Host Clusters from vCNS to NSX in a vCloud Director Environment

You must prepare your environment for network virtualization by installing network infrastructure components on a per-cluster level for each vCenter server. This deploys the required software on all hosts in the cluster and renames virtual wires to NSX logical switches. During this process, each host in the cluster receives a software update and is then rebooted.

If you have virtual wires in your environment, once you have upgraded to NSX Manager you must update your host clusters.

It is recommended that you update host clusters in a datacenter maintenance window.

While the upgrade is in progress, do not deploy, upgrade, or uninstall any service or component.

When you install or upgrade NSX, it will automatically try to put each host into maintenance mode and reboot it. This is not recommended in vCloud Director environments.

Instead, you should upgrade the VIBs on each cluster, but do not click **Resolve**. You must disable the host in vCloud Director before entering maintenance mode and rebooting.

**Note** VTEPs that were created in vCloud Networking and Security use DHCP or manually assigned IP addresses, not IP pools.

### Procedure

1 Upgrade VIBs on Hosts in a vCloud Director Environment

  In a vCloud Director environment, you must you must set DRS to Manual before upgrading VIBs on clusters, otherwise NSX will attempt to put the hosts in maintenance mode.

2 Reboot Hosts Manually after VIB Installation in a vCloud Director Environment

Hosts must be rebooted for the installed NSX VIBs to take effect. You must disable hosts in vCloud Director before rebooting them. This prevents vCloud Director from attempting to use the hosts during the reboot.

## Upgrade VIBs on Hosts in a vCloud Director Environment

In a vCloud Director environment, you must you must set DRS to Manual before upgrading VIBs on clusters, otherwise NSX will attempt to put the hosts in maintenance mode.

### Prerequisites

- Verify that vShield Manager has been upgraded to NSX Manager.
- Verify that the VXLAN Column in Host Preparation tab displays **Enabled**.
- Verify that the fully qualified domain names (FQDNs) of all of your hosts can be resolved.
- Before beginning the upgrade, make sure that DRS can work in your environment.
  - Verify that DRS is enabled on the host clusters.
  - Verify that vMotion functions correctly.
  - Verify the host connection state with vCenter.
  - Verify 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.
- 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.
  - Verify that DRS is enabled on the host clusters.
  - Verify that vMotion functions correctly.
  - Verify the host connection state with vCenter.
  - Verify 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.

### Procedure

1 In the vSphere Web Client, navigate to **Home > Hosts and Clusters**.

2 Set DRS to manual on the host clusters. Repeat these steps for all clusters that have vCloud Networking and Security installed.

**Caution** Do not disable DRS. Disabling DRS will delete your resource pools and corrupt your vCloud Director installation.

a Select a cluster, and then navigate to **Manage > Settings > vSphere DRS**.

b Take note of the current **DRS Automation** setting, as you will revert this change later.

c Click **Edit**. In the **DRS Automation** section, select **Manual** and click **OK**.

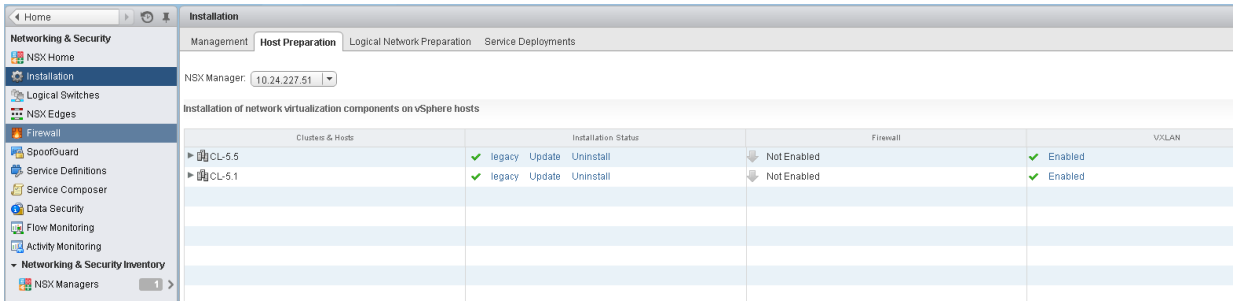
3 Navigate to **Home > Networking & Security > Installation**.

4 Click the **Host Preparation** tab.

All clusters in your infrastructure are displayed.

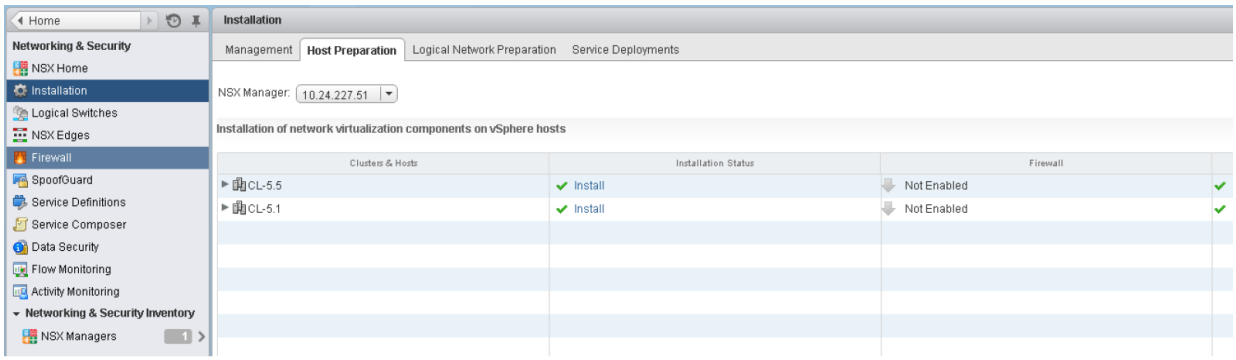
If you had Virtual Wires in your 5.5 environment, the **Installation Status** column displays **legacy**, **Update**, and **Uninstall**.

**Figure 1-3. Installation Status displays Update when you have Virtual Wires in your 5.5 environment**




If you did not have Virtual Wires in your 5.5 environment, the **Installation Status** column displays **Install**.

**Figure 1-4. Installation Status displays Install when you do not have Virtual Wires in your 5.5 environment**



5 For each cluster, click **Update** or **Install** in the Installation Status column.

   Each host in the cluster receives the new logical switch software.

   The host upgrade initiates a host scan. The old VIBs are removed (though they are not completely deleted until after the reboot). New VIBs are installed on the altboot partition. To view the new VIBs on a host that has not yet rebooted, you can run the `esxcli software vib list --rebooting-image | grep esx` command.

6 Monitor the installation until the **Installation Status** column displays **Not Ready**.

   Do not click **Resolve**.

7 Navigate to **Home > Hosts and Clusters**.

8 Revert the DRS changes on the host clusters. Repeat these steps for all clusters that have NSX installed.

   a Select a cluster, and then navigate to **Manage > Settings**

   b Select **vSphere DRS** and click **Edit**. In the **DRS Automation** section, select your original DRS setting and click **OK**.

#### What to do next

Reboot Hosts Manually after VIB Installation in a vCloud Director Environment.

## Reboot Hosts Manually after VIB Installation in a vCloud Director Environment

Hosts must be rebooted for the installed NSX VIBs to take effect. You must disable hosts in vCloud Director before rebooting them. This prevents vCloud Director from attempting to use the hosts during the reboot.

#### Prerequisites

- Verify that all hosts have a status of **Not Ready**.
- Verify that each vSphere cluster has enough capacity to temporarily run without one host.
- Verify that DRS is enabled and not set to Manual.

#### Procedure

1 In vCloud Director, disable the host.

   a Navigate to **Manage & Monitor > Hosts.**.

   b Right click on a host, and select **Disable Host**.

2 In the vSphere Web Client, navigate to **Home > Hosts and Clusters**.

3 Right click on the host you have disabled in vCloud Director and select **Enter Maintenance Mode**. In the Confirm Maintenance Mode dialog box, Select **Move powered-off and suspended virtual machines to other hosts in the cluster** and click **OK**.

4 If all virtual machines are not moved to other hosts, manually move them.

5 Once the host is in maintenance mode, right click the host and select **Reboot**. Enter a reason for the reboot, and click **OK**.

6 Once the host is back up, right click the host and select **Exit Maintenance Mode**.

7 In vCloud Director, enable the host.

   a Navigate to **Manage & Monitor > Hosts.**.

   b Right click on the host, and select **Enable Host**.

8 Once the host is enabled in vCloud Director, repeat these steps with the next host.

All virtual wires from your 5.5 infrastructure are renamed to NSX logical switches, and the VXLAN column for the cluster says **Enabled**.

**Enabled**

When the cluster is updated, the **Installation Status** column displays the software version that you have updated to.

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

- esx-vsip
- esx-vxlan

**Note** In NSX 6.2, the esx-dvfilter-switch-security VIB is included within the esx-vxlan VIB.

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.

### What to do next

If you have deployed an NSX Controller cluster, you can optionally change the control plane mode: Update Transport Zones and Logical Switches in a vCloud Director Environment.

Otherwise, Determine Whether to Upgrade vShield Edge in a vCloud Director Environment

## Update Transport Zones and Logical Switches in a vCloud Director Environment

If you deploy an NSX Controller cluster, you do not have to rely on multicast for logical networks. You can update the control plane mode on your transport zones and logical switches to unicast or hybrid.

The change of control plane mode and migration of existing logical switches has no impact on the networking data plane traffic.

### Procedure

1. In the vSphere Web Client, navigate to **Home > Networking & Security > Installation > Logical Network Preparation > Transport Zones**.
2. Select your transport zone, and click **Actions > Edit Settings**. Select the desired replication mode.
   - **Multicast**: Multicast IP addresses in the physical network are used for the control plane. This mode is recommended only when you are upgrading from older VXLAN deployments. Requires PIM/IGMP in the physical network.
   - **Unicast**: The control plane is handled by an NSX controller. All unicast traffic leverages optimized headend replication. No multicast IP addresses or special network configuration is required.
   - **Hybrid**: Offloads local traffic replication to the physical network (L2 multicast). This requires IGMP snooping on the first-hop switch and access to an IGMP querier in each VTEP subnet, but does not require PIM. The first-hop switch handles traffic replication for the subnet.
3. Select the check box for **Migrate existing Logical Switches to the new control plane mode** and click **OK**.

### What to do next

Determine Whether to Upgrade vShield Edge in a vCloud Director Environment

# Determine Whether to Upgrade vShield Edge in a vCloud Director Environment

The version of vCloud Director determines whether or not you should upgrade vShield Edge.

If you are using vCloud Director earlier than 8.10, you must not upgrade vShield Edge.

Additionally, if you are using vCloud Director 5.x, you must make a configuration change in the vCloud Directordatabase to prevent vCloud Director from upgrading the Edges on redeploy. See Prevent Legacy vShield Edge Redeployment in a vCloud Director Environment.

Starting in vCloud Director 8.10, NSX Edge 6.x is supported, and you can upgrade vShield Edge to NSX Edge 6.x. See Upgrade vShield Edge to NSX Edge in a vCloud Director Environment

## Prevent Legacy vShield Edge Redeployment in a vCloud Director Environment

If you are using vCloud Director 5.x, once you've upgraded to NSX, you must made a database change to prevent legacy vShield Edge appliances being deployed as NSX Edge appliances.

It is important not to upgrade legacy edge services gateways to VMware NSX 6.x because this will break vCloud Director compatibility. vCloud Director 5.x will upgrade an Edge on vCloud Director when an Edge is redeployed. To prevent this behavior, the following vCloud Director database change is necessary prior to vCloud Network and Security migration.

For more information, see the following VMware Knowledge Base articles: http://kb.vmware.com/kb/2096351 and http://kb.vmware.com/kb/2108913.

### Procedure

1 Log in to the vCloud Director SQL Server database.

2 Add this line to the config table.

```
INSERT INTO config (cat, name, value, sortorder) VALUES
('vcloud','networking.edge_version_for_vsm6.2', '5.5', 0);
```

**Note** Use `networking.edge_version_for_vsm6.1` if NSX 6.1 is used or `networking.edge_version_for_vsm6.0` if NSX 6.0 is used.

## Upgrade vShield Edge to NSX Edge in a vCloud Director Environment

vCloud Director 8.10 supports NSX Edge 6.x, which allows you to upgrade vShield Edge to NSX Edge. If you are using an earlier version of vCloud Director, NSX Edge 6.x is not supported, and you should not upgrade NSX Edge.

You can upgrade vShield Edge to NSX Edge in two ways, using NSX, or using vCloud Director.

To upgrade Edge using vCloud Director, see Upgrade vCenter Server Systems, Hosts, and NSX Edges in the *vCloud DirectorInstallation and Upgrade Guide*.

**Attention** If you are using vCloud Director earlier than 8.10, do not upgrade NSX Edge.

### Prerequisites

- Verify vShield Manager has been upgraded to NSX Manager.
- Understand the operational impact of the NSX Edge upgrade while the upgrade is in progress. See Operational Impacts of vCloud Networking and Security Upgrades.
- 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 will be two NSX Edge appliances of the appropriate size in the poweredOn state during upgrade.
  - Starting in NSX 6.2.3, when upgrading an NSX Edge instance with high availability, both replacement appliances are deployed before replacing the old appliances. This means there will be 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.

- Prior to NSX 6.2.3, when upgrading an NSX Edge instance with high availability, only one replacement appliance is deployed at time while replacing the old appliances. This means there will be three NSX Edge appliances of the appropriate size in the poweredOn state during the upgrade of a given NSX Edge. Once the NSX Edge instance is upgraded, usually the NSX Edge appliance with HA index 0 becomes active.

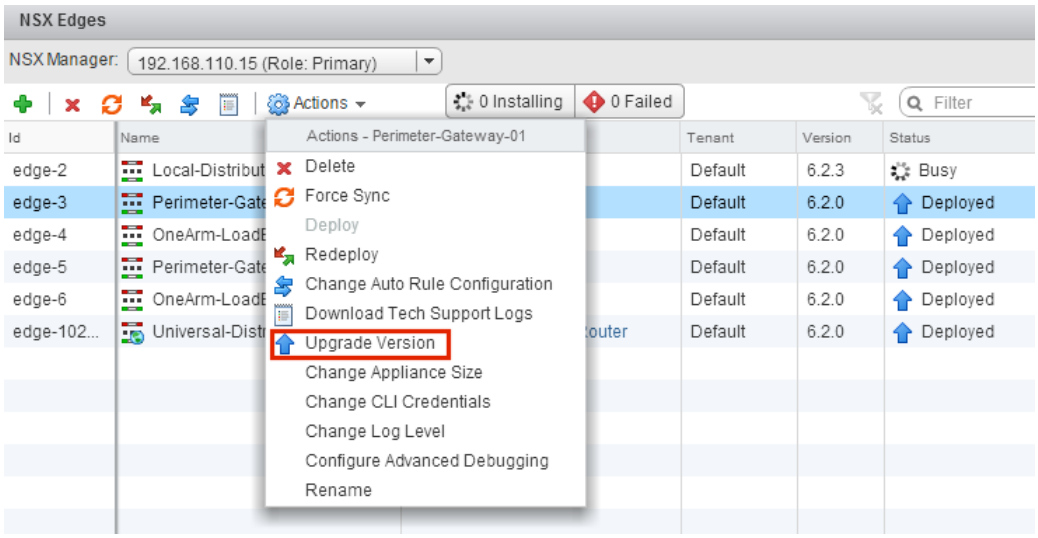
- Upgrading an NSX Edge with version 5.5 or 6.0 with L2 VPN enabled is not supported. You must delete the L2 VPN configuration before you upgrade. Once you have upgraded, you can reconfigure L2 VPN. See "L2 VPN Overview" in the *NSX Installation Guide*.

**Procedure**

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **NSX Edges**.

3 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.

NSX Edge firewall rules do not support sourcePort, so vShield Edge version 5.5 rules containing sourcePort are modified during the upgrade as follows.

- If there are no applications used in the rule, a service is created with protocol=any, port=any and sourcePort=asDefinedInTheRule.
- If there are applications or applicationGroups used in the rule, these grouping objects are duplicated by adding the sourcePort to them. Because of this, the groupingObjectIds used in the firewall rule change after the upgrade.

User firewall rules in NSX Edge 6.x do not generate internal IPSets and applicationSets based on input from REST APIs. Instead they will be retained in the raw format. During upgrade, the internally generated IPSet and applicationSets are used to create rules with raw data. The internal groupingObjects will no longer appear in the user firewallRules

### What to do next

If needed, reconfigure any L2 VPN configurations. See L2 VPN Overview in the *NSX Installation Guide*.

## Post-Upgrade Checklist

After the upgrade is complete, follow these steps.

### Procedure

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

   NSX installs these VIBs:

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

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

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

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

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

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

   Headers:

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

# NSX Upgrade

2

This section includes the following topics:



## 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 Manager. See Uninstall NSX Data Security.

4 Plan to upgrade all NSX Managers that are connected to vCenter Server systems that use the same SSO server (including vCenter Server systems in Enhanced Linked Mode). If you cannot, see https://kb.vmware.com/kb/2127061 for a workaround.

5 Verify that you have a current backup of the NSX Manager, vCenter and other NSX components. See NSX Backup and Restore.

6 Create a Tech Support Bundle.

7 Ensure that forward and reverse domain name resolution is working, using the nslookup command.

8 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.

9 Download and stage the upgrade bundle, validate with md5sum. See Download the NSX Upgrade Bundle and Check the MD5.

10 As a best practice, quiesce all operations in the environment until all sections of the upgrade are complete.

11 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 an earlier version of NSX to NSX 6.2.3, your existing license is converted to a NSX Enterprise license, and you will be entitled to the same functionality in the Enterprise offering.

See the NSX License FAQ https://www.vmware.com/files/pdf/products/nsx/vmware-nsx-editions-faq.pdf

## Operational Impacts of NSX Upgrades

The NSX upgrade process can take some time, especially when upgrading ESXi hosts, because hosts must be rebooted. 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.
- If you are upgrading from NSX 6.1.x to NSX 6.2.x or later, you must upgrade the NSX Manager and the NSX Controller cluster 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 theNSX 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, those are unavailable for configuration (greyed out) in the user interface 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.
- If you are upgrading from NSX 6.1.x to NSX 6.2.x or later, you must upgrade the NSX Manager and the NSX Controller cluster in the same maintenance window.

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.
- 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. Any new features introduced for Edge Services Gateway in the NSX upgrade will not be configurable until all NSX Controllers and all host clusters have been upgraded.

## 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.

# 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

Uninstall NSX data security either because you are no longer using it or because you are upgrading NSX Manager. NSX data security does not support a direct upgrade. Before upgrading NSX Manager, it is important to first uninstall NSX data security and then reinstall it after the upgrade.

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

### Procedure

1 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 NSX Manager Data

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

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

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

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

### Procedure

1 Log in to the NSX Manager Virtual Appliance.

2 Under Appliance Management, click **Backups & Restore**.

3 To specify the backup location, click **Change** next to FTP Server Settings.

   a Type the IP address or host name of the backup system.

   b From the **Transfer Protocol** drop-down menu, select either **SFTP** or **FTP**, based on what the destination supports.

   c Edit the default port if required.

   d Type the user name and password required to login to the backup system.

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

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

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

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

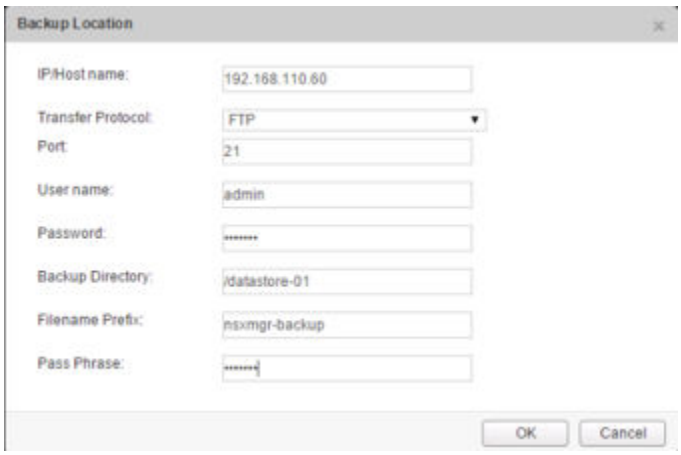
   This text is prepended to each backup filename for easy recognition on the backup system. For example, if you type **ppdb**, the resulting backup is named as `ppdbHH_MM_SS_DayDDMonYYYY`.

g Type the pass phrase to secure the backup.

You will need this pass phrase to restore the backup.

h Click **OK**.

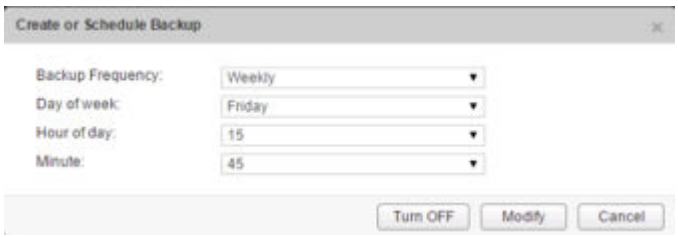
For example:




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 officially 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 screen shots of the current settings for the old NSX Manager appliance or note them so that they can be used to specify IP information and backup location information for the newly deployed NSX Manager appliance.

#### Procedure

1. Take screen shots or note all settings on the existing NSX Manager appliance.
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 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.
6. In the Backups History section, select the check box for the backup to restore and click **Restore**.

## Back Up NSX Edges

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

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

Taking individual NSX Edge backups is not supported.

## Back Up vSphere Distributed Switches

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

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

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

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

### Back Up vCenter

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

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

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

Useful links for vCenter 5.5:

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

Useful links for vCenter 6.0:

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

## Download the 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 from NSX 6.1.x or 6.2.x to NSX 6.2.x

To upgrade to NSX 6.2.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

5 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 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.

### Prerequisites

- Validate the NSX Manager file system usage, and perform a cleanup if file system usage is at 100 percent.

  a Login to NSX Manager and run `show filesystems` to show the /dev/sda2 filesystem usage.

  b If the usage is 100 percent, run the `purge log manager` and `purge log system` commands.

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

- Increase the NSX Manager virtual appliance's reserved memory to at least 16 GB before upgrading for NSX 6.2.x.

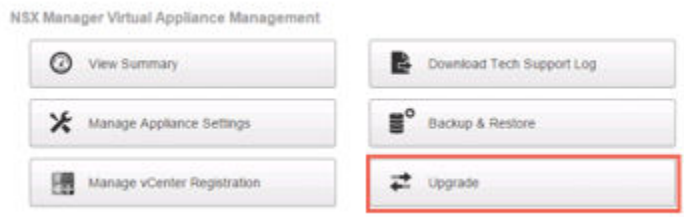
  See System Requirements for NSX.

- If you have Data Security in your environment, uninstall it before upgrading NSX Manager. See Uninstall NSX Data Security.
- 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.

**Procedure**

1 Log in to the NSX Manager virtual appliance.

2 On the NSX Manager 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 In the Upgrade dialog box, specify 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.

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

5 Log in to the NSX Manager virtual appliance again and 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 upgrade 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.

### 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**.

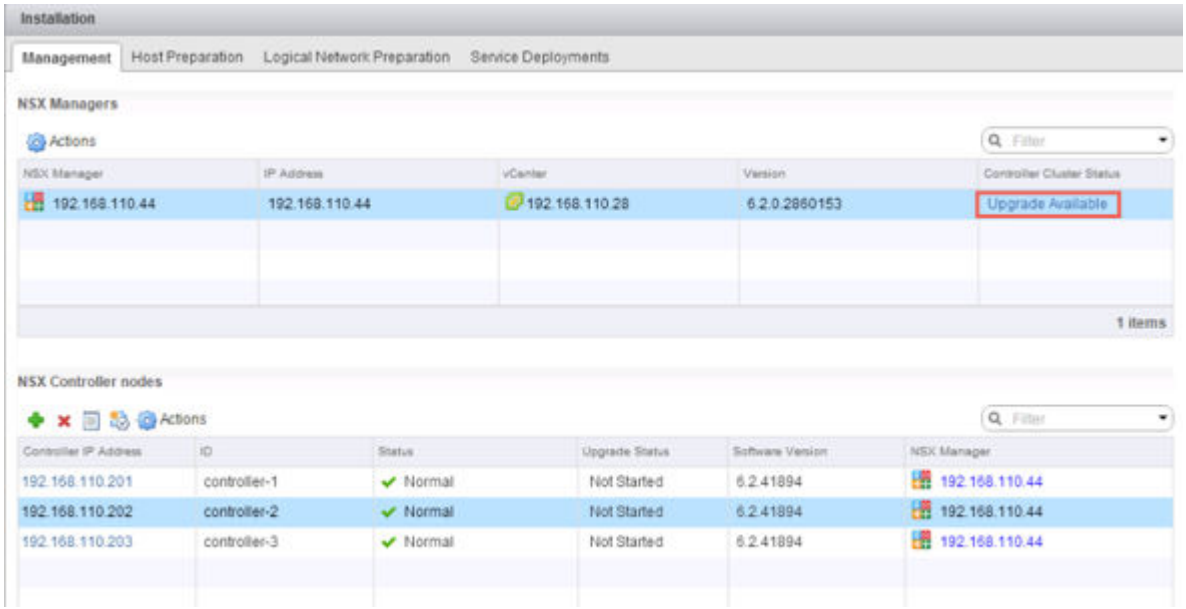
- A valid NSX Controller cluster contains three controller nodes. Log in to the three controller nodes and run the **show controller-cluster status** command.

```
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.

### Procedure

- In the vSphere Web Client, 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 **Normal** to begin with. 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 **Normal** again.
  - 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**.

When the upgrade is complete, the **Software Version** column in the NSX Controller nodes section displays **6.2.***buildNumber* for each controller. Rerun the **show controller-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.

#### What to do next

Upgrade the host clusters.

## Upgrade Host Clusters

After upgrading NSX Manager and NSX Controllers to version 6.2.x, you can update the appropriate clusters in your environment. During this process, each host in the cluster receives a software update and is then rebooted.

Upgrading the host clusters upgrades the NSX VIBs, esx-vsip and esx-vxlan.

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

#### Prerequisites

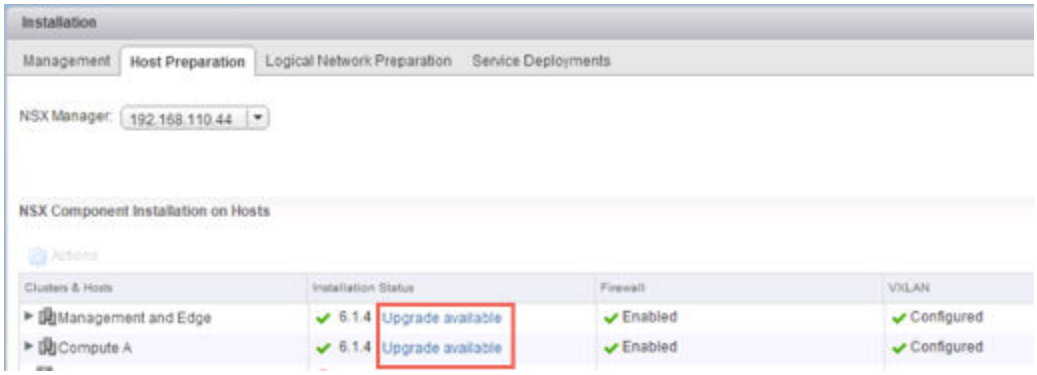
- Make sure the fully qualified domain names (FQDNs) of all of your hosts can be resolved.
- Log into one of the hosts in the cluster and run the `esxcli software vib list` command. Note the current version of the following VIBs:
  - esx-vsip
  - esx-vxlan
- Upgrade NSX Manager and the NSX Controller cluster.
- 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.

- 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 **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.

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

- esx-vsip
- esx-vxlan

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

Change VXLAN Port

## Change VXLAN Port

You can change the port used for VXLAN traffic.

In NSX 6.2.3 and later, the default VXLAN port is 4789, the standard port assigned by IANA. Before NSX 6.2.3, the default VXLAN UDP port number was 8472.

Any new NSX installations will use UDP port 4789 for VXLAN.

If you upgrade from NSX 6.2.2 or earlier to NSX 6.2.3 or later, and your installation used the old default (8472), or a custom port number (for example, 8888) before the upgrade, that port will continue to be used after the upgrade unless you take steps to change it.

If your upgraded installation uses or will use hardware VTEP gateways (ToR gateways), you must switch to VXLAN port 4789.

Cross-vCenter NSX does not require that you use 4789 for the VXLAN port, however, all hosts in a cross-vCenter NSX environment must be configured to use the same VXLAN port. If you switch to port 4789, this will ensure that any new NSX installations added to the cross-vCenter NSX environment are using the same port as the existing NSX deployments.

Changing the VXLAN port is done in a three phase process, and will not interrupt VXLAN traffic.

1 NSX Manager configures all hosts to listen for VXLAN traffic on both the old and new ports. Hosts continue to send VXLAN traffic on the old port.

2 NSX Manager configures all hosts to send traffic on the new port.

3 NSX Manager configures all hosts to stop listening on the old port, all traffic is sent and received on the new port.

In a cross-vCenter NSX environment you must initiate the port change on the primary NSX Manager. For each stage, the configuration changes are made on all hosts in the cross-vCenter NSX environment before proceeding to the next stage.

### Prerequisites

- Verify that the port you want to use for VXLAN is not blocked by a firewall.
- Verify that host preparation is not running at the same time as the VXLAN port change.

### Procedure

1 Log in to the vSphere Web Client.

2 Click **Networking & Security** and then click **Installation**.

3 Click the **Logical Network Preparation** tab, then click **VXLAN Transport**.

4 Click the **Change** button in the VXLAN Port panel. Enter the port you want to switch to. 4789 is the port assigned by IANA for VXLAN.

It will take a short time for the port change to propagate to all hosts.

5 (Optional) Check the progress of the port change with the `GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus` API request.

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

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

...

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

### What to do next

Upgrade NSX Edge

## Upgrade NSX Edge

NSX Edges can be upgraded without any dependency on the NSX Controller cluster or host cluster upgrades. You can upgrade an NSX Edge even if you have not yet upgraded the NSX Controller cluster or host clusters.

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 minimizing the impact by configuring the Edge to work in ECMP mode.

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

### Prerequisites

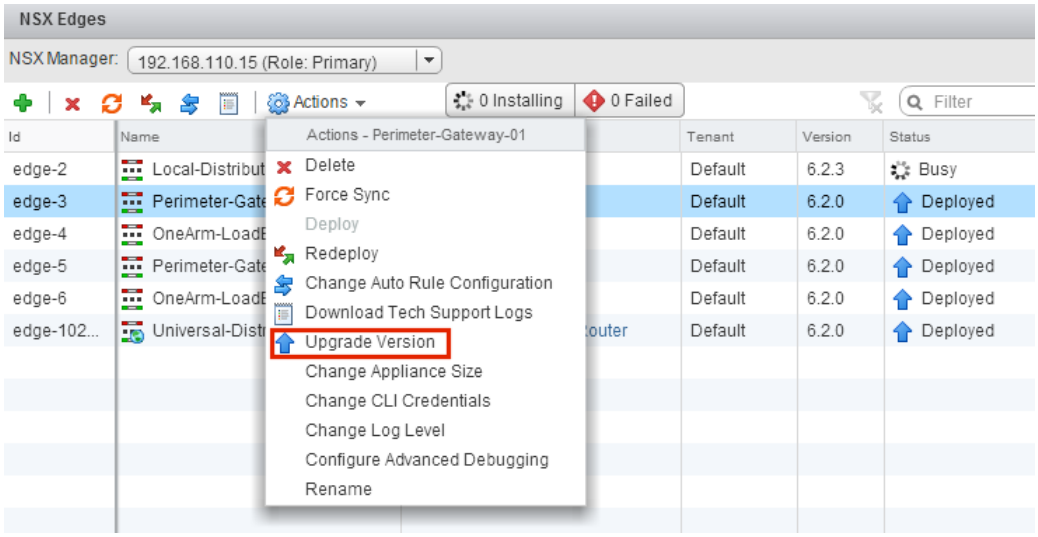
- Verify that NSX Manager has been upgraded to 6.2.x.
- Verify that there is a local segment ID pool, even if you have no plans to create NSX logical switches.
- Verify the hosts have enough resources to deploy additional NSX Edge Services Gateway appliances during the upgrade, particularly if you are 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 will be two NSX Edge appliances of the appropriate size in the poweredOn state during upgrade.
    - Starting in NSX 6.2.3, when upgrading an NSX Edge instance with high availability, both replacement appliances are deployed before replacing the old appliances. This means there will be 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.

- Prior to NSX 6.2.3, when upgrading an NSX Edge instance with high availability, only one replacement appliance is deployed at time while replacing the old appliances. This means there will be three NSX Edge appliances of the appropriate size in the poweredOn state during the upgrade of a given NSX Edge. Once the NSX Edge instance is upgraded, usually the NSX Edge appliance with HA index 0 becomes active.

- Understand the operational impact of the NSX Edge upgrade while the upgrade is in progress. See Operational Impacts of NSX Upgrades.
- Upgrading an NSX Edge with version 5.5 or 6.0 with L2 VPN enabled is not supported. 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*.
- If you are upgrading from NSX 6.2.x to NSX 6.2.3 and load balancer is configured, see this Knowledge Base article to avoid problems with the upgrade: https://kb.vmware.com/kb/2145887

### Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. 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

If needed, reconfigure any L2 VPN configurations. See L2 VPN Overview in the *NSX Installation Guide*.

# Upgrade Guest Introspection

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

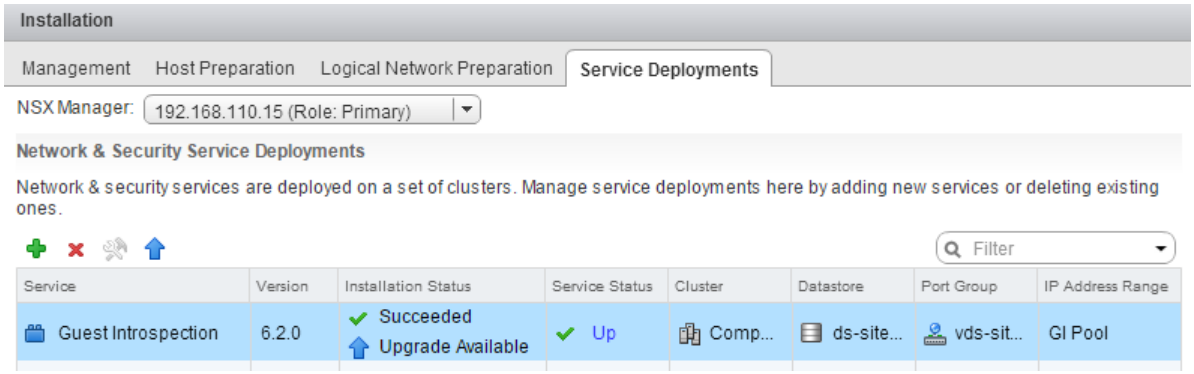
**Note** The Guest Introspection service VMs can be upgraded from the vSphere Web Client. You do not need to delete the service VM after the upgrade of the NSX Manager to upgrade it. If you do delete the service VM, the Service Status will be shown as `Failed` because the Agent VM is missing. Click on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

### Prerequisites

NSX Manager, controllers, prepared host clusters, and NSX Edges must have been upgraded to 6.2.x.

### Procedure

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

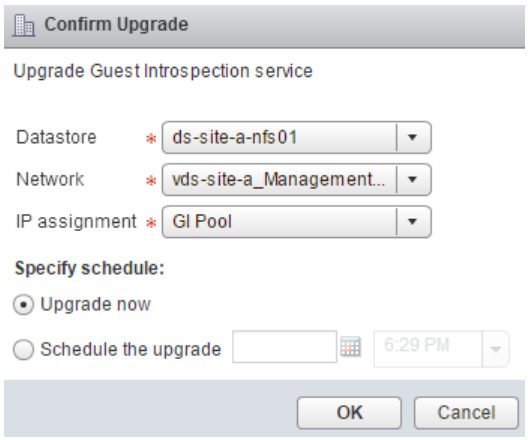



The **Installation Status** column says **Upgrade Available**.

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.

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, such as VMware Partner Security Virtual Appliances, 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.

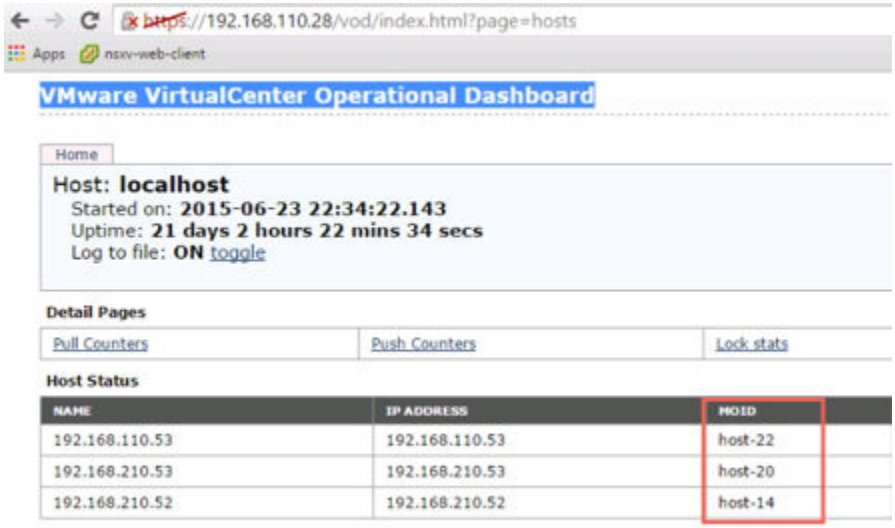
### NSX Data Security

You should uninstall NSX data security before upgrading NSX and then reinstall it after the NSX upgrade is complete. If you have already upgraded NSX without first uninstalling NSX data security, you must uninstall data security using a REST API call.

Issue the following API call:

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

The host-id is the MOID of the ESXi host. To retrieve the MOID, open the VMware VirtualCenter Operational Dashboard: https://<vcenter-ip>/vod/index.html?page=hosts.




For the ESXi host with the MOID "host-22" on vCenter Server 192.168.110.28, the API call would be formatted as follows:

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

Make sure to issue the API call on all of your ESXi hosts.

After data security is uninstalled, you can install the new version. See Install NSX Data Security.

## 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 6.2.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 versions 5.5.x or 6.0.x. Any L2 VPN configuration must be deleted before you can upgrade the NSX Edge.

## Install NSX Data Security

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

### Prerequisites

NSX Guest Introspection must be installed on the cluster where you are installing Data Security.

If you want to assign an IP address to the Data Security service virtual machine from an IP pool, create the IP pool before installing Data Security. See Grouping Objects in the *NSX Administration Guide*.

### Procedure

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

2 Click the **New Service Deployment** ( ) icon.

3 In the Deploy Network and Security Services dialog box, select **Data Security** and click **Next**.

4 In **Specify schedule** (at the bottom of the dialog box), select **Deploy now** to deploy Data Security as soon as it is installed or select a deployment date and time.

5 Click **Next**.

6 Select the datacenter and cluster(s) where you want to install Data Security and click **Next**.

7 On the Select storage and Management Network page, select the datastore on which to add the service virtual machines storage or select **Specified on host**.

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

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

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

If the datastore is set to **Specified on host**, the network to be used must be specified in the **agentVmNetwork** property of each host in the cluster. See *vSphere API/SDK Documentation*.

When you add a host(s) to the cluster, the **agentVmNetwork** property for the host must be set before it is added to the cluster.

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

9 In IP assignment, select one of the following:

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

Note that static IP address are not supported.

10 Click **Next** and then click **Finish** on the Ready to complete page.

11 Monitor the deployment until the **Installation Status** column displays **Succeeded**.

12 If the **Installation Status** column displays **Failed**, click the icon next to Failed. All deployment errors are displayed. Click **Resolve** to fix the errors. In some cases, resolving the errors displays additional errors. Take the required action and click **Resolve** again.

## 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 6.2.x with Cross-vCenter NSX

To upgrade to NSX 6.2.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.

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.

**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.

### Prerequisites

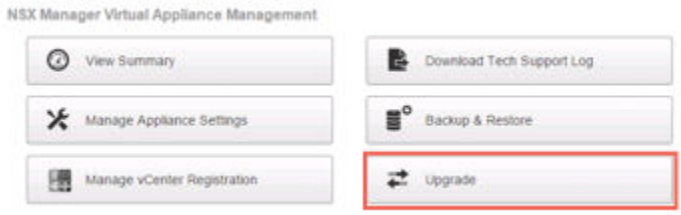
- Validate the NSX Manager file system usage, and perform a cleanup if file system usage is at 100 percent.
  a Login to NSX Manager and run `show filesystems` to show the /dev/sda2 filesystem usage.
  b If the usage is 100 percent, run the `purge log manager` and `purge log system` commands.
  c Reboot the NSX Manager appliance for the log cleanup to take effect.
- Increase the NSX Manager virtual appliance's reserved memory to at least 16 GB before upgrading for NSX 6.2.x.

  See System Requirements for NSX.
- If you have Data Security in your environment, uninstall it before upgrading NSX Manager. See Uninstall NSX Data Security.
- 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.

### Procedure

1 Log in to the NSX Manager virtual appliance.

2 On the NSX Manager 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 In the Upgrade dialog box, specify 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.

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

5 Log in to the NSX Manager virtual appliance again and 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 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.

### 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. Login to NSX Manager and run `show filesystems` to show the /dev/sda2 filesystem usage.
  b. If the usage is 100 percent, run the `purge log manager` and `purge log system` commands.
  c. Reboot the NSX Manager appliance for the log cleanup to take effect.
- Increase the NSX Manager virtual appliance's reserved memory to at least 16 GB before upgrading for NSX 6.2.x.

  See System Requirements for NSX.
- If you have Data Security in your environment, uninstall it before upgrading NSX Manager. See Uninstall NSX Data Security.
- 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.

**Procedure**

1. 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.

2. In the Upgrade dialog box, specify 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.

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

3. Log in to the NSX Manager virtual appliance again and 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 upgrade 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.

### 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 controller-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
```

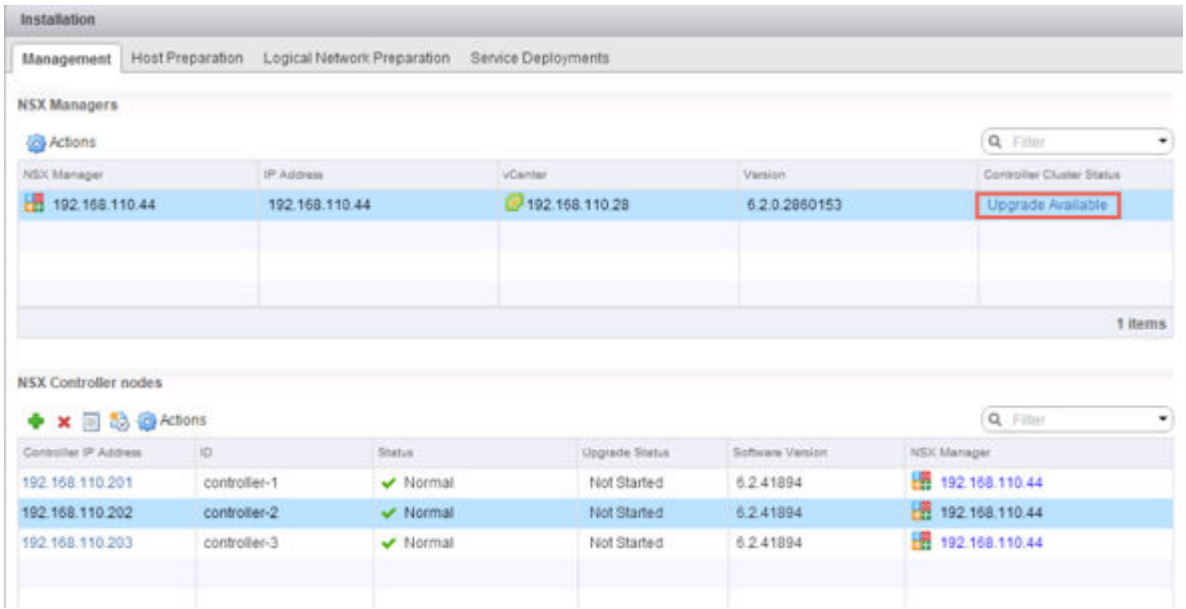
  - For Join status, verify the controller node is reporting Join Complete.
  - For Majority status, verify the controller is connected to the cluster majority.
  - For Cluster ID, all the controller nodes in a cluster should have the same cluster ID.

- 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.

**Procedure**

- In the vSphere Web Client, 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 **Normal** to begin with. 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 **Normal** again.
- 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**.

When the upgrade is complete, the **Software Version** column in the NSX Controller nodes section displays **6.2.***buildNumber* for each controller. Rerun the **show controller-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.

### 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 to NSX 6.2.x, you should update all host clusters in the cross-vCenter NSX environment. During this process, each host in the cluster receives a software update and is then rebooted.

Upgrading the host clusters upgrades the NSX VIBs, esx-vsip and esx-vxlan.

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

### Prerequisites

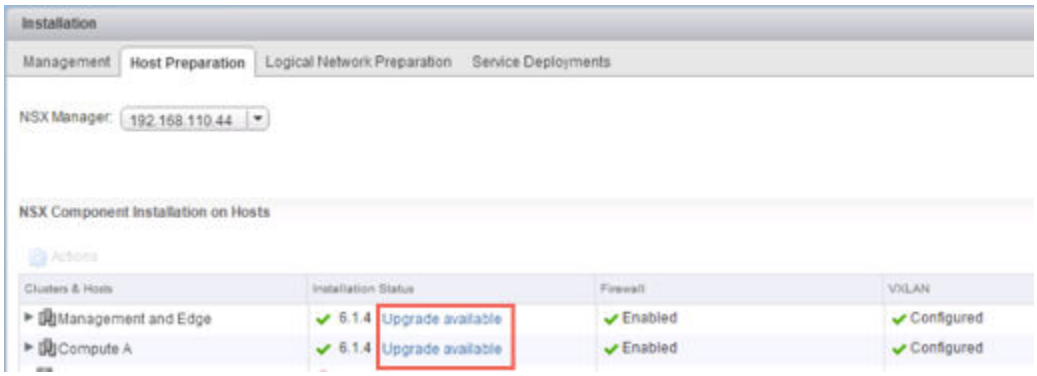
- Make sure the fully qualified domain names (FQDNs) of all of your hosts can be resolved.

- Log into one of the hosts in the cluster and run the `esxcli software vib list` command. Note the current version of the following VIBs:
  - esx-vsip
  - esx-vxlan
- Upgrade NSX Manager and the NSX Controller cluster.
- 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.
- 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 **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.

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

- esx-vsip
- esx-vxlan

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.

# Change VXLAN Port in Cross-vCenter NSX

You can change the port used for VXLAN traffic.

In NSX 6.2.3 and later, the default VXLAN port is 4789, the standard port assigned by IANA. Before NSX 6.2.3, the default VXLAN UDP port number was 8472.

Any new NSX installations will use UDP port 4789 for VXLAN.

If you upgrade from NSX 6.2.2 or earlier to NSX 6.2.3 or later, and your installation used the old default (8472), or a custom port number (for example, 8888) before the upgrade, that port will continue to be used after the upgrade unless you take steps to change it.

If your upgraded installation uses or will use hardware VTEP gateways (ToR gateways), you must switch to VXLAN port 4789.

Cross-vCenter NSX does not require that you use 4789 for the VXLAN port, however, all hosts in a cross-vCenter NSX environment must be configured to use the same VXLAN port. If you switch to port 4789, this will ensure that any new NSX installations added to the cross-vCenter NSX environment are using the same port as the existing NSX deployments.

Changing the VXLAN port is done in a three phase process, and will not interrupt VXLAN traffic.

1 NSX Manager configures all hosts to listen for VXLAN traffic on both the old and new ports. Hosts continue to send VXLAN traffic on the old port.

2 NSX Manager configures all hosts to send traffic on the new port.

3 NSX Manager configures all hosts to stop listening on the old port, all traffic is sent and received on the new port.

In a cross-vCenter NSX environment you must initiate the port change on the primary NSX Manager. For each stage, the configuration changes are made on all hosts in the cross-vCenter NSX environment before proceeding to the next stage.

### Prerequisites

- Verify that the port you want to use for VXLAN is not blocked by a firewall.
- Verify that host preparation is not running at the same time as the VXLAN port change.

### Procedure

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **Installation**.
3. Click the **Logical Network Preparation** tab, then click **VXLAN Transport**.
4. Click the **Change** button in the VXLAN Port panel. Enter the port you want to switch to. 4789 is the port assigned by IANA for VXLAN.

   It will take a short time for the port change to propagate to all hosts.

5 (Optional) Check the progress of the port change with the `GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus` API request.

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

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

...

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

### What to do next

Upgrade NSX Edge in Cross-vCenter NSX

## Upgrade NSX Edge in Cross-vCenter NSX

NSX Edges can be upgraded without any dependency on the NSX Controller cluster or host cluster upgrades. You can upgrade an NSX Edge even if you have not yet upgraded the NSX Controller cluster or host clusters. Upgrade NSX Edges in all NSX installations in the cross-vCenter NSX environment.

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 minimizing the impact by configuring the Edge to work in ECMP mode.

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

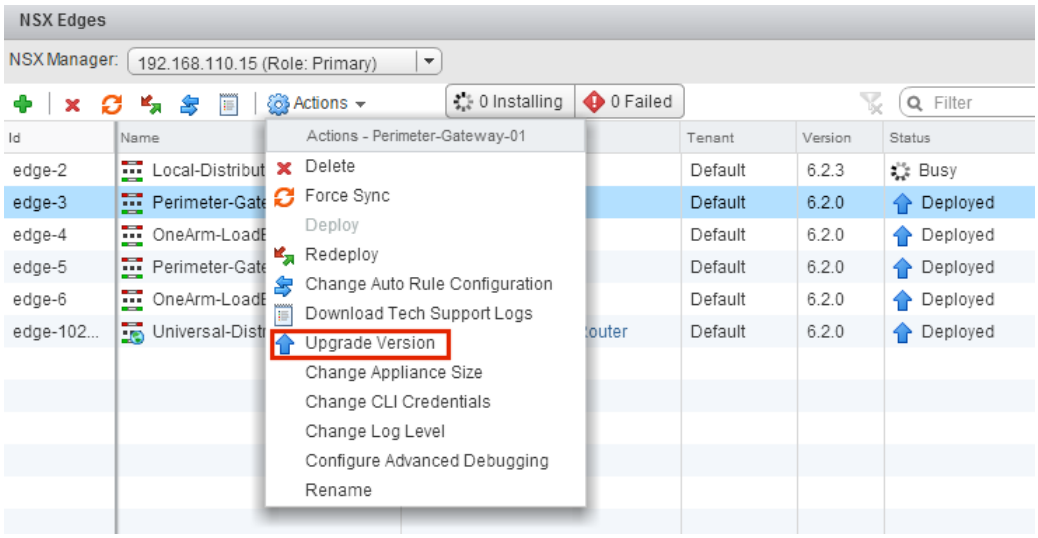
### Prerequisites

- Verify that NSX Manager has been upgraded to 6.2.x.
- 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 will be two NSX Edge appliances of the appropriate size in the poweredOn state during upgrade.
  - Starting in NSX 6.2.3, when upgrading an NSX Edge instance with high availability, both replacement appliances are deployed before replacing the old appliances. This means there will be 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.
  - Prior to NSX 6.2.3, when upgrading an NSX Edge instance with high availability, only one replacement appliance is deployed at time while replacing the old appliances. This means there will be three NSX Edge appliances of the appropriate size in the poweredOn state during the upgrade of a given NSX Edge. Once the NSX Edge instance is upgraded, usually the NSX Edge appliance with HA index 0 becomes active.
- Understand the operational impact of the NSX Edge upgrade while the upgrade is in progress. See Operational Impacts of NSX Upgrades.
- Upgrading an NSX Edge with version 5.5 or 6.0 with L2 VPN enabled is not supported. 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*.
- If you are upgrading from NSX 6.2.x to NSX 6.2.3 and load balancer is configured, see this Knowledge Base article to avoid problems with the upgrade: https://kb.vmware.com/kb/2145887

**Procedure**

1. Log in to the vSphere Web Client.
2. Click **Networking & Security** and then click **NSX Edges**.
3. 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

If needed, reconfigure any L2 VPN configurations. See L2 VPN Overview in the *NSX Installation Guide*.

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.

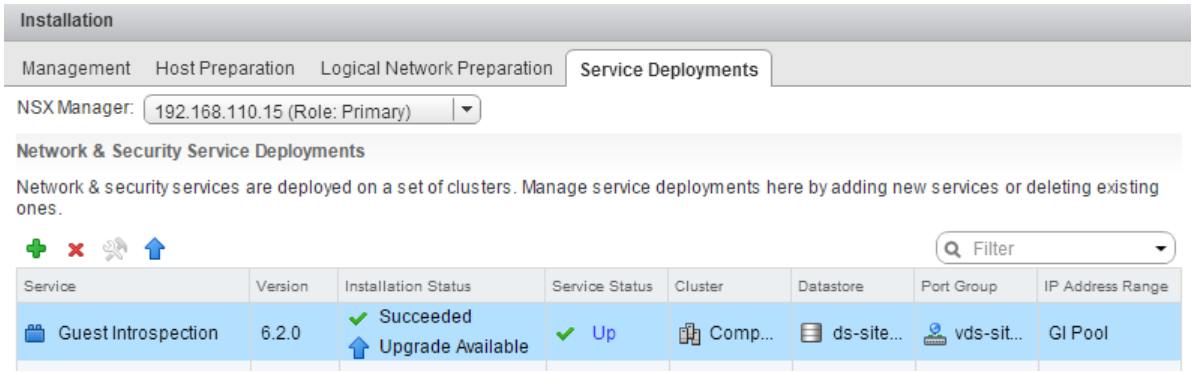
**Note** The Guest Introspection service VMs can be upgraded from the vSphere Web Client. You do not need to delete the service VM after the upgrade of the NSX Manager to upgrade it. If you do delete the service VM, the Service Status will be shown as `Failed` because the Agent VM is missing. Click on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

### Prerequisites

NSX Manager, controllers, prepared host clusters, and NSX Edges must have been upgraded to 6.2.x.

### Procedure

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

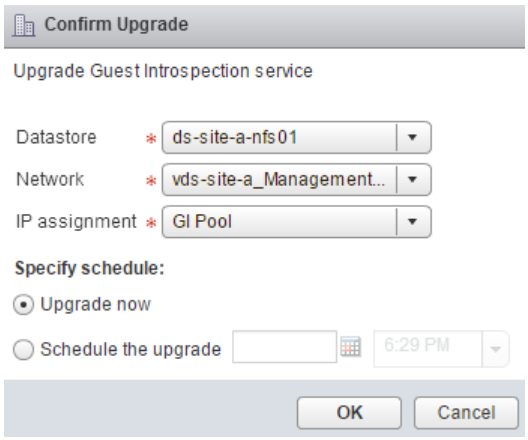



The **Installation Status** column says **Upgrade Available**.

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, such as VMware Partner Security Virtual Appliances, 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.

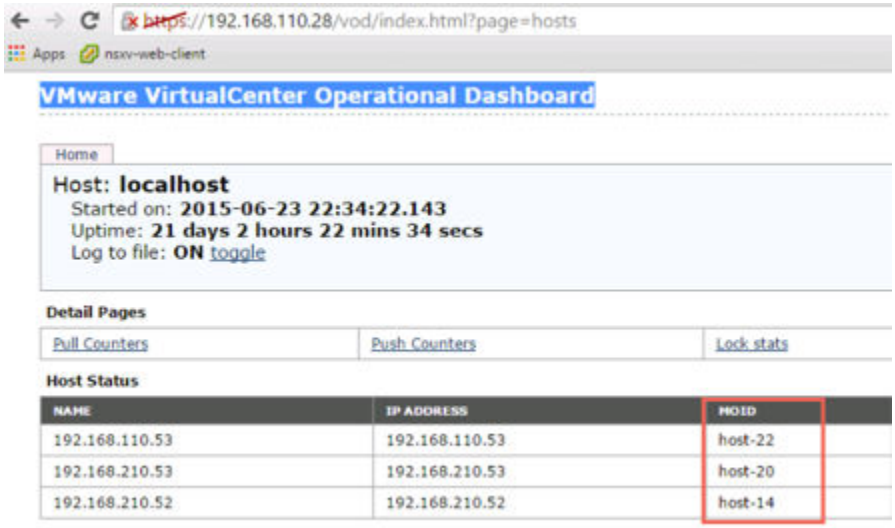
### NSX Data Security

You should uninstall NSX data security before upgrading NSX and then reinstall it after the NSX upgrade is complete. If you have already upgraded NSX without first uninstalling NSX data security, you must uninstall data security using a REST API call.

Issue the following API call:

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

The host-id is the MOID of the ESXi host. To retrieve the MOID, open the VMware VirtualCenter Operational Dashboard: https://<vcenter-ip>/vod/index.html?page=hosts.




For the ESXi host with the MOID "host-22" on vCenter Server 192.168.110.28, the API call would be formatted as follows:

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

Make sure to issue the API call on all of your ESXi hosts.

After data security is uninstalled, you can install the new version. See Install NSX Data Security.

### 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 6.2.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 versions 5.5.x or 6.0.x. 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

3

When you upgrade vSphere in an NSX environment, you must ensure the versions of NSX and vSphere are compatible.

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.

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.

This section includes the following topics:



## Upgrade ESXi 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.

**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.
- 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 | grep esx-v` command. The first part of the VIB version displays the version of ESXi for the VIB. For example, before upgrade from ESXi 5.5 to ESXi 6.0.

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

After upgrade to ESXi 6.0:

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

# 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.