# NSX-T Data Center Upgrade Guide

**vm**ware®

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

https://docs.vmware.com/

# Contents

# Upgrading NSX-T Data Center

The *NSX-T Data Center Upgrade Guide* provides step-by-step information about upgrading the NSX-T Data Center components, which include the data plane, control plane, and management plane with minimum system downtime.

## Intended Audience

This information is intended for anyone who wants to upgrade to NSX-T Data Center 3.0. The information is written for experienced system administrators who are familiar with virtual machine technology, virtual networking, and security concepts and operations.

## 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.

## Related Documentation

You can find the VMware NSX® Intelligence™ documentation at https://docs.vmware.com/en/VMware-NSX-Intelligence/index.html. The NSX Intelligence 1.0 content was initially included and released with the NSX-T Data Center 2.5 documentation set.

# NSX-T Data Center Upgrade Checklist

1

Use the checklist to track your work on the upgrade process.

Table 1-1. Upgrade NSX-T Data Center

| Task | Instructions |
| --- | --- |
| Review the known upgrade problems and workaround documented in the NSX-T Data Center release notes. | See the *NSX-T Data Center Release Notes*. |
| Follow the system configuration requirements and prepare your infrastructure. | See the system requirements section of the *NSX-T Data Center Installation Guide*. |
| Evaluate the operational impact of the upgrade. | See Operational Impact of the NSX-T Data Center Upgrade. |
| Upgrade your supported hypervisor. | See Upgrading Your Host OS. |
| If you have an earlier version of NSX Intelligence installed, upgrade the NSX Intelligence appliance first. | See the *Installing and Upgrading VMware NSX Intelligence* documentation at https://docs.vmware.com/en/VMware-NSX-Intelligence/index.html for more information. |
| Complete the Pre-Upgrade Tasks. | See Pre-Upgrade Tasks. |
| Verify that the NSX-T Data Center environment is in a healthy state. | See Verify the Current State of NSX-T Data Center . |
| Download the latest NSX-T Data Center upgrade bundle. | See Download the NSX-T Data Center Upgrade Bundle. |
| If you are using NSX Cloud for your public cloud workload VMs, upgrade NSX Cloud components. | See Chapter 4 Upgrading NSX Cloud Components . |
| Upgrade your upgrade coordinator. | See Upgrade the Upgrade Coordinator. |
| Upgrade the NSX Edge cluster. | See Upgrade NSX Edge Cluster. |
| Upgrade the hosts. | See Configuring and Upgrading Hosts . |
| Upgrade the Management plane. | See Upgrade Management Plane. |
| Post-upgrade tasks. | See Verify the Upgrade. |
| Troubleshoot upgrade errors. | See Chapter 6 Troubleshooting Upgrade Failures. |

# Preparing to Upgrade NSX-T Data Center

<span style="font-size:3em; color:gray; float:right;">2</span>

You must prepare your infrastructure and follow the task sequence provided in the checklist for the upgrade process to be successful.

You can perform the upgrade process in a maintenance time frame defined by your company. You can, for example, upgrade only one of the components and upgrade the other NSX-T Data Center components later, during another maintenance time frame. Ensure that you follow the upgrade order while upgrading the components: NSX Edge cluster > Hosts > Management plane.

This chapter includes the following topics:

- Operational Impact of the NSX-T Data Center Upgrade
- Supported Hypervisor Upgrade Path
- Pre-Upgrade Tasks
- Upgrading Your Host OS
- Verify the Current State of NSX-T Data Center
- Download the NSX-T Data Center Upgrade Bundle

## Operational Impact of the NSX-T Data Center Upgrade

The duration for the NSX-T Data Center upgrade process depends on the number of components you have to upgrade in your infrastructure. It is important to understand the operational state of NSX-T Data Center components during an upgrade.

The upgrade process is as follows:

NSX Edge cluster > Hosts > Management plane.

## NSX Edge Cluster Upgrade

| During Upgrade | After Upgrade |
| --- | --- |
| ■ During the NSX Edge upgrade, you might experience the following traffic interruption:<br><br>   ■ North-south datapath is affected if the NSX Edge is part of the datapath.<br><br>   ■ East-west traffic between tier-1 routers using NSX Edge firewall, NAT, or load balancing.<br><br>   ■ Temporary Layer 2 and Layer 3 interruption.<br><br>■ Configuration changes are not blocked on NSX Manager but might be delayed. | ■ Configuration changes are allowed.<br><br>■ Upgraded NSX Edge cluster is compatible with the older versions of the Management plane and the hosts.<br><br>■ New features introduced in the upgrade are not configurable until the Management plane is upgraded.<br><br>■ Run post checks to make sure that the upgraded NSX Edge cluster and NSX-T Data Center do not have any problems. |

## Hosts Upgrade

| During Upgrade | After Upgrade |
| --- | --- |
| ■ For standalone ESXi hosts or ESXi hosts that are part of a disabled DRS cluster, place hosts in maintenance mode.<br><br>For ESXi hosts that are part of a fully enabled DRS cluster, if the host is not in maintenance mode, the upgrade coordinator requests the host to be put in maintenance mode. The vSphere DRS tool migrates the VMs to another host in the same cluster during the upgrade and places the host in maintenance mode.<br><br>**Note** Before you place your ESXi host in maintenance mode, power off any NSX Edge VMs that may be residing on the host and ensure that the NSX Edge VMs continue to reside on the same host.<br><br>■ For ESXi host, for an in-place upgrade you do not need to power off the tenant VMs.<br><br>■ For a KVM host, for an in-place upgrade you do not need to power off the VMs. For a maintenance mode upgrade, power off the VMs.<br><br>■ Configuration changes are allowed on NSX Manager. | ■ Power on or return the tenant VMs of standalone ESXi hosts or ESXi hosts that are part of a disabled DRS cluster that were powered off before the upgrade.<br><br>■ New features introduced in the upgrade are not configurable until the Management plane is upgraded.<br><br>■ Run post checks to make sure that the upgraded hosts and NSX-T Data Center do not have any problems. |

## Limitations on In-Place Upgrade

For ESXi hosts with version 7.0 and later, when upgrading from NSX-T 3.0 or later, in-place upgrade is not supported in the following scenarios:

■ More than 400 vNICs are configured on the host N-VDS or the VDS switch.

■ CPU use for the `hostd`, `nsxa`, or the `config-agent` service is high.

■ Layer 7 firewall rules or Identity Firewall rules are enabled.

■ Service Insertion has been configured to redirect north-south traffic or east-west traffic. See *Security* in the *NSX-T Data Center Administration Guide* for information on uninstalling service insertion.

■ A VProbe-based packet capture is in progress.

- The `nsx-cfgagent` service is not running on the host.

For ESXi hosts with versions earlier than 7.0, in-place upgrade of a host is not supported in the following scenarios:

- More than one N-VDS switch is configured on the host.

- More than 100 vNICs are configured on the host N-VDS switch.

- ENS is configured on the host N-VDS switch.

- CPU use for the `hostd`, `nsxa`, or the `config-agent` service is high.

- vSAN(with LACP) is configured on the host N-VDS switch.

- Layer 7 firewall rules or Identity Firewall rules are enabled.

- VMkernel interface is configured on the overlay network.

- Service Insertion has been configured to redirect north-south traffic or east-west traffic. See *Security* in the *NSX-T Data Center Administration Guide* for information on uninstalling service insertion.

- A VProbe-based packet capture is in progress.

## Management Plane Upgrade

| During Upgrade | After Upgrade |
|---|---|
| <ul><li>Configuration changes are not blocked on the Management plane. Do not make any changes during the Management plane upgrade.</li><li>API service is momentarily unavailable.</li><li>User interface is unavailable for a short period.</li></ul> | <ul><li>Configuration changes are allowed.</li><li>New features introduced in the upgrade are configurable.</li><li>For NSX-T Data Center 3.0, you need a valid license to use licensed features like T0, T1, Segments, and NSX intelligence.</li><li>From the Upgrade Coordinator, verify that the upgrade process has completed. Perform configuration tasks only after the upgrade process is complete.</li></ul> |

# Supported Hypervisor Upgrade Path

The supported hypervisor upgrade paths for the NSX-T Data Center product versions.

Table 2-1. Supported Hypervisor

| NSX-T Data Center 3.0 | NSX-T Data Center 2.5 | NSX-T Data Center 2.4 |
|---|---|---|
| Supported vSphere Hypervisor (ESXi) | Supported vSphere Hypervisor (ESXi) | Supported vSphere Hypervisor (ESXi) |
| Ubuntu 18.04 and Ubuntu 16.04.2 LTS with Kernel version 4.4.0.x | Ubuntu 18.04.2 and Ubuntu 16.04.2 LTS with Kernel version 4.4.0.x | Ubuntu 18.04 and Ubuntu 16.04.2 LTS with Kernel version 4.4.0.x |
| RHEL 7.6, RHEL 7.7 | RHEL 7.6, RHEL 7.5, and RHEL 7.4 | RHEL 7.5 and RHEL 7.4 |
| CentOS 7.6, CentOS 7.7 | CentOS 7.5 and CentOS 7.4 | CentOS 7.5 and CentOS 7.4 |
| SUSE Linux Enterprise Server (SLES) 12 sp3, sp4 | SUSE Linux Enterprise Server (SLES) 12 sp3, sp4 | SUSE Linux Enterprise Server (SLES) 12 sp3 |

Adhere to the following upgrade paths for each NSX-T Data Center release version.

▪ NSX-T Data Center 2.4.x > NSX-T Data Center 3.0.

▪ NSX-T Data Center 2.5.x > NSX-T Data Center 3.0.

# Pre-Upgrade Tasks

Before you upgrade NSX-T Data Center, perform the pre-upgrade tasks to ensure that the upgrade is successful.

**Procedure**

**1** If you are upgrading from a version earlier than NSX-T Data Center 3.0, provision a secondary disk of exactly 100 GB capacity on all NSX Manager appliances.

▪ For an ESXi host, login to vCenter Server, navigate to the NSX Manager VM and add a disk of exactly 100GB capacity.

▪ For a KVM host:

1 Create a disk of 100 GB capacity:

```
qemu-img create -f qcow2 nsx-unified-appliance-secondary.qcow2 100G
```

2 Create an xml file ( */<download folder>/<nsx_manger_vm_name_storage_file.xml>*) for the additional storage:

```
<disk type='file' device='disk'>
 <driver name='qemu' type='qcow2' cache='none'/>
 <source file='/<diskPath>/nsx-unified-appliance-secondary.qcow2'/>
 <target dev='vdb' bus='virtio' />
</disk>
```

3 Make the VM persistent using the following commands:

```
virsh dumpxml <NSX Manager VM> > /<download folder>/<nsx_manager_vm_name.xml>
virsh define /<download folder>/<nsx_manager_vm_name.xml>
virsh list -all
```

4 Attach the secondary disk to the NSX Manager appliance:

```
virsh attach-device --config  <NSX Manager VM> /<download folder>/
<nsx_manger_vm_name_storage_file.xml>
```

5 Shutdown and start the NSX Manager appliance:

```
virsh shutdown <NSX Manager VM>
virsh start <NSX Manager VM>
```

6    Repeat the process for the other NSX Manager appliances in the cluster.

**Note**   Reboot the appliance if the secondary disk is not detected by the Upgrade Coordinator. Run the pre-check to ensure that the secondary disk is detected and proceed with other NSX Manager appliances.

2    If you are upgrading from a version earlier than NSX-T Data Center 3.0, disable inter-SR (service router) routing before you begin the upgrade. For more information on upgrade scenarios and workaround options, see the VMware knowledge base article at https://kb.vmware.com/s/article/85288.

3    Ensure that your transport node profiles have the appropriate transport zones added to them. NSX Manager may not display the list of transport node profiles if any of the transport node profiles do not have transport zones added to them.

4    Ensure that you backup the NSX Manager before you start the upgrade process. See the *NSX-T Data Center Administration Guide*.

5    Ensure that your host OS is supported for NSX Manager. See *Supported Hosts for NSX Managers* in the *NSX-T Data Center Administration Guide*

6    Disable automatic backups before you start the upgrade process. See the *NSX-T Data Center Administration Guide* for more information on configuring backups.

7    Terminate any active SSH sessions or local shell scripts that may be running on the NSX Manager, before you begin the upgrade process.

8    Ensure that the appropriate communication ports are open from the Transport and Edge nodes to the NSX Managers:

   ▪    TCP ports 1234 to NSX Manager

   ▪    TCP port 1235 to NSX Controller

   ▪    TCP port 9040 between the NSX Manager nodes

   ▪    Keep port 5671 open during the upgrade process.

   **NSX Cloud Note**   Starting with NSX-T Data Center 2.5.1, NSX Cloud supports communication on port 80 between the Cloud Service Manager appliance installed on-prem with the NSX Public Cloud Gateway installed in your public cloud VPC/VNet. NSX-T Data Center versions 2.5.0 and earlier require port 7442 for this communication. During the upgrade from versions 2.5.0 and earlier to 2.5.1, keep port 7442 open. See Enable Access to Ports and Protocols in the *NSX-T Data Center Installation Guide* for more information.

9    Before you place your ESXi host in maintenance mode, power off any NSX Edge VMs that may be residing on the host and ensure that the NSX Edge VMs continue to reside on the same host.

10   For NSX-T Data Center 3.0, you need a valid license to use licensed features like T0, T1, Segments, and NSX intelligence. Ensure that you have a valid license.

**11** Ensure that you perform an automated pre-check to verify whether the NSX-T Data Center components are ready for upgrade. The pre-check process scans for component activity, version compatibility, component status of the hosts, NSX Edge, and management plane. Resolve any warning notifications to avoid problems during the upgrade.

**12** Delete all expired user accounts before you begin upgrade. Upgrade for NSX-T Data Center on vSphere fails if your exception list for vSphere lockdown mode includes expired user accounts. For more information on accounts with access privileges in lockdown mode, see *Specifying Accounts with Access Privileges in Lockdown Mode* in the *vSphere Security* Guide.

# Upgrading Your Host OS

To avoid problems during the host upgrade, your host OS must be supported in NSX-T Data Center.

If the version of your host OS is unsupported, you can manually upgrade the host OS to the supported version. See Supported Hypervisor Upgrade Path.

For RHEL, CentOS, Ubuntu, and SLES host upgrade instructions, refer to the host web site.

## Upgrade ESXi Host

If your ESXi host is unsupported, manually upgrade your ESXi host to the supported version.

### Prerequisites

Verify that the ESXi host is supported. See Supported Hypervisor Upgrade Path.

### Procedure

◆ Upgrade the ESXi host using one of the following options.

- Perform the upgrade from the ESXi CLI:

  a Place your ESXi host in maintenance mode.

  b Run the following command from the ESXi CLI:

  ```
  esxcli software profile update --depot <path-to-depot-file> ESXi-X.X.X-XXXXXX-
  standard --allow-downgrades --no-sig-check
  ```

  c Download the NSX kernel module for VMware ESXi x.x.

  d Install the NSX kernel module.

  ```
  esxcli software vib install -d <path_to_kernel_module_file> --no-sig-check
  ```

  e Reboot the ESXi host.

  f Move your ESXi host out of maintenance mode.

- Upgrade ESXi in an offline environment using vSphere Update Manager:

  a Upgrade to a supported version of vCenter Server.

b    Log in to the upgraded vCenter Server.

c    Download and add the supported ESXi software depot to the image builder inventory.

d    Download and add the NSX kernel module for VMware ESXi x.x to the image builder inventory.

e    Create a customized software depot, create a new image profile, and select the packages from the software depots that you added to the image builder inventory.

f    Export the image to ISO.

g    Upload the installation ISO image to the vSphere Update Manager repository.

h    Create a baseline based on the uploaded ISO image in vSphere Update Manager, and attach it to a cluster.

i    Start the remediate process and wait for the upgrade process to complete.

j    Run the remediate process again if you see any upgrade failures.

- Perform the upgrade using a baseline group:

a    Upgrade to the supported version of vCenter Server.

b    Log in to the upgraded vCenter Server.

c    In the lifecycle manager, upload the ESXi x.x installation ISO and import the NSX kernel modules for VMware ESXi x.x .

d    Create an upgrade baseline using the imported ESXi x.x installation ISO

e    Create an extension baseline using the uploaded NSX kernel modules.

f    Create a baseline group using the baselines you created in the preceding steps.

g    Attach the baseline group to a cluster. Ensure the vmknics on the hosts have been configured. If the vmknics are configured to use DHCP, make sure the DHCP server is running.

h    Start the remediate process and wait for the upgrade process to complete.

i    Run the remediate process again if you see any upgrade failures.

## Upgrade Ubuntu Host

If your Ubuntu host is unsupported, manually upgrade your Ubuntu host to the supported version.

**Prerequisites**

Verify that the Ubuntu host is supported. See Supported Hypervisor Upgrade Path.

Ubuntu requires the following dependencies for the LCP package and host components to work properly.

```
libunwind8, libgflags2v5, libgoogle-perftools4, traceroute, python-mako, python-simplejson,
python-unittest2, python-yaml, python-netaddr, libprotobuf9v5, libboost-chrono1.58.0,
libgoogle-glog0v5, dkms, libboost-date-time1.58.0, libleveldb1v5, libsnappy1v5, python-
gevent, python-protobuf, ieee-data, libyaml-0-2, python-linecache2, python-traceback2,
libtcmalloc-minimal4, python-greenlet, python-markupsafe, libboost-program-options1.58.0,
libelf-dev
```

### Procedure

1   Follow the instructions available on the Ubuntu web site to upgrade your host. Reboot the Ubuntu KVM host after the upgrade process has completed.

2   If you have an existing Ubuntu KVM host as a transport node, back up the `/etc/network/interfaces` file.

3   Download the NSX kernel module for Ubuntu x.x.

4   Install the NSX kernel module.

```
tar -xvf <path_to_kernel_module_file>
cd <folder_extracted_from_previous_step>
sudo dpkg -i *.deb
dpkg -i | grep nsx
```

## Upgrade CentOS Host

If your CentOS host is unsupported, manually upgrade your CentOS host to the supported version.

### Prerequisites

Verify that the CentOS host is supported. See Supported Hypervisor Upgrade Path.

CentOS requires the following dependencies for the LCP package and host components to work properly.

```
PyYAML, c-ares, libev, libunwind, libyaml, python-beaker, python-gevent, python-greenlet,
python-mako, python-markupsafe, python-netaddr, python-paste, python-tempita
```

### Procedure

1   Follow the instructions available on the CentOS web site to upgrade your host. Reboot the CentOS host after the upgrade process has completed.

2   Download the NSX kernel module for CentOS xx.x.

**3** Install the NSX kernel module.

```
tar - xvf <path_to_kernel_module_file>
cd <folder_extracted_from_previous_step>
sudo yum install *.rpm
rpm -qa | grep nsx
```

## Upgrade RHEL Host

If your RHEL host is unsupported, manually upgrade your RHEL host to the supported version.

**Prerequisites**

Verify that the RHEL host is supported. See Supported Hypervisor Upgrade Path.

RHEL requires the following dependencies for the LCP package and host components to work properly.

```
PyYAML, c-ares, libev, libunwind, libyaml, python-beaker, python-gevent, python-greenlet,
python-mako, python-markupsafe, python-netaddr, python-paste, python-tempita
```

**Procedure**

**1** Follow the instructions available on the RHEL web site to upgrade your host. Reboot the RHEL host host after the upgrade process has completed.

**2** Restart the NSX agent.

```
/etc/init.d/nsx-opsagent restart
```

**3** Download the NSX kernel module for RHEL x.x.

**4** Install the NSX kernel module.

```
tar - xvf <path_to_kernel_module_file>
cd <folder_extracted_from_previous_step>
sudo yum install *.rpm
rpm -qa | grep nsx
```

## Upgrade SLES Host

If your SUSE Linux Enterprise Server (SLES) host is unsupported, manually upgrade your SLES host to the supported version.

**Prerequisites**

Verify that the SLES host is supported. See Supported Hypervisor Upgrade Path.

SLES requires the following dependencies for the LCP package and host components to work properly.

```
python-simplejson, python-netaddr, python-PyYAML, lsb-release, libcap-progs
```

**Procedure**

1   Follow the instructions available on the SLES web site to upgrade your host. Reboot the SLES host after the upgrade process has completed.

2   Download the NSX kernel module for SLES x.x.

3   Install the NSX kernel module.

```
tar - xvf <path_to_kernel_module_file>
cd <folder_extracted_from_previous_step>
sudo rpm -ivh *.rpm
rpm -qa | grep nsx
```

4   (Optional) Restart the NSX agent.

```
/etc/init.d/nsx-opsagent restart
```

# Verify the Current State of NSX-T Data Center

Before you begin the upgrade process, it is important to test the NSX-T Data Center working state. Otherwise, you cannot determine if the upgrade caused post-upgrade problems or if the problem existed before the upgrade.

**Note**   Do not assume that everything is working before you start to upgrade the NSX-T Data Center infrastructure.

**Procedure**

1   Identify and record the administrative user IDs and passwords.

2   Verify that you can log in to the NSX Manager web user interface.

3   Check the **Dashboard**, system overview, host transport nodes, edge transport nodes, NSX Edge cluster, transport nodes, HA status of the edge, and all logical entities to make sure that all the status indicators are green, deployed, and do not show any warnings.

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

5   Validate that there is an East-West connectivity between any two VMs in your environment.

6   Record BGP states on the NSX Edge devices.

- ```
  get logical-routers
  ```

- ```
  vrf <vrf>
  ```

- ```
  get bgp
  ```

- ```
  get bgp neighbor
  ```

# Download the NSX-T Data Center Upgrade Bundle

The upgrade bundle contains all the files to upgrade the NSX-T Data Center infrastructure. Before you begin the upgrade process, you must download the correct upgrade bundle version.

You can also navigate to the upgrade bundle and save the URL. When you upgrade the upgrade coordinator, paste the URL so that the upgrade bundle is uploaded from the VMware download portal.

**Procedure**

**1** Locate the NSX-T Data Center build on the VMware download portal.

**2** Navigate to the upgrade bundle file and click **Read More**.

**3** Verify that the upgrade bundle filename extension ends with `.mub`.

The upgrade bundle filename has a format similar to `VMware-NSX-upgrade-bundle-`*`ReleaseNumberNSXBuildNumber`*`.mub`.

**4** Download the NSX-T Data Center upgrade bundle to the same system you are using to access the NSX Manager user interface.

# Upgrading NSX-T Data Center

# 3

After you finish the prerequisites for upgrading, your next step is to update the upgrade coordinator to initiate the upgrade process.

After the upgrade, based on your input, the upgrade coordinator updates the hosts, NSX Edge cluster, and Management plane.

You can use REST APIs to upgrade your NSX-T Data Center appliance. Identify the NSX-T Data Center version you are upgrading to. Refer to the API guide with your product version in code.vmware.com to find the latest upgrade-related APIs.

**Procedure**

**1**  Upgrade the Upgrade Coordinator

The upgrade coordinator runs in the NSX Manager. It is a self-contained web application that orchestrates the upgrade process of hosts, NSX Edge cluster, and Management plane.

**2**  Upgrade NSX Edge Cluster

After the upgrade coordinator has been upgraded, based on your input, the upgrade coordinator updates the NSX Edge cluster, hosts, and the Management plane. Edge upgrade unit groups consist of NSX Edge nodes that are part of the same NSX Edge cluster. You can reorder Edge upgrade unit groups and enable or disable an Edge upgrade unit group from the upgrade sequence.

**3**  Configuring and Upgrading Hosts

You can upgrade your hosts using the upgrade coordinator.

**4**  Upgrade Management Plane

The upgrade coordinator orchestrates the upgrade of the Management Plane at the end. When the Management Plane upgrade is in progress, avoid any configuration changes from any of the nodes.

## Upgrade the Upgrade Coordinator

The upgrade coordinator runs in the NSX Manager. It is a self-contained web application that orchestrates the upgrade process of hosts, NSX Edge cluster, and Management plane.

The upgrade coordinator guides you through the proper upgrade sequence. You can track the upgrade process and if necessary you can pause and resume the upgrade process from the user interface.

The upgrade coordinator allows you to upgrade groups in a serial or parallel order. It also provides the option of upgrading the upgrade units within that group in a serial or parallel order.

**Prerequisites**

Verify that the upgrade bundle is available. See Download the NSX-T Data Center Upgrade Bundle.

**Procedure**

1   In the NSX Manager CLI, verify that the NSX-T Data Center services are running.

    ```
    get service install-upgrade
    ```

    If the services are not running, troubleshoot the problem. See the *NSX-T Data Center Troubleshooting Guide.*

    ■   `get service install-upgrade` lists the IP address of the orchestrator node. See `Enabled on`. Use this IP address throughout the upgrade process.

        **Note**   Ensure that you do not use any type of Virtual IP address to upgrade NSX-T Data Center.

    ■   To change the orchestrator node, log in to the node that you want to set as an orchestrator node and run `set repository-ip`

    ■   When the Management Plane upgrade is in progress, avoid any configuration changes from any of the nodes.

2   From your browser, log in as a local admin user to an NSX Manager at https://*nsx-manager-ip-address/login.jsp?local=true.*

3   Select **System > Upgrade** from the navigation panel.

4   Click **Proceed to Upgrade**.

5   Navigate to the upgrade bundle `.mub` file by navigating to the downloaded upgrade bundle or pasting the download URL link.

    ■   Click **Browse** to navigate to the location you downloaded the upgrade bundle `.mub` file.

    ■   Paste the VMware download portal URL where the upgrade bundle `.mub` file is located.

6   Click **Upload**.

    Upgrading the upgrade coordinator might take 10–20 minutes, depending on your network speed. If the network times out, reload the upgrade bundle.

    When the upload process finishes, the **Begin Upgrade** button appears.

7   Click **Begin Upgrade** to upgrade the upgrade coordinator.

> **Note**   Do not initiate multiple simultaneous upgrade processes for the upgrade coordinator.

The EULA appears.

8   Read and accept the EULA terms.

9   Accept the notification to upgrade the upgrade coordinator.

10  (Optional) If a patch release becomes available after the upgrade coordinator is updated, upload or add the URL of the latest upgrade bundle and upgrade the upgrade coordinator.

11  Click **Run Pre Checks** to verify that all the NSX-T Data Center components are ready for upgrade.

This action checks for component connectivity, version compatibility, and component status among other environment readiness checks, for your current upgrade plan.

> **Note**   You must run the pre-checks when you change or reset your upgrade plan, or upload a new upgrade bundle.

12  (Optional) View the list of pre-checks that are performed with the API call `GET https://<nsx-manager>/api/v1/upgrade/upgrade-checks-info`.

13  Resolve any warning notifications to avoid problems during the upgrade.

    a   Click the Hosts notification next to **Pre Check Status** to see the warning details.

       You might have to place some of the hosts in maintenance mode.

    b   Click the Edges notification next to **Pre Check Status** to see the warning details.

       You might have to resolve connectivity problems.

    c   Click the Management Nodes notification next to **Pre Check Status** to see the warning details.

You can click **Export Pre Checks CSV** and download details about any pre-check errors for all the components and their status in a CSV file.

14  (Optional) Click **Show Upgrade History** and view information about previous NSX Manager upgrades.

## Upgrade NSX Edge Cluster

After the upgrade coordinator has been upgraded, based on your input, the upgrade coordinator updates the NSX Edge cluster, hosts, and the Management plane. Edge upgrade unit groups consist of NSX Edge nodes that are part of the same NSX Edge cluster. You can reorder Edge

upgrade unit groups and enable or disable an Edge upgrade unit group from the upgrade sequence.

**Note** You cannot move an NSX Edge node from one Edge upgrade unit group to another because the Edge upgrade unit group membership adheres to the NSX Edge cluster membership before the upgrade.

The NSX Edge nodes are upgraded in serial mode so that when the upgrading node is down, the other nodes in the NSX Edge cluster remain active to continuously forward traffic.

The maximum limit of simultaneous upgrade of Edge upgrade unit groups is five.

Prerequisites

- Verify that the NSX Edge nodes are in an NSX Edge cluster.

- Familiarize yourself with the upgrade impact during and after the NSX Edge cluster upgrade. See Operational Impact of the NSX-T Data Center Upgrade.

Procedure

1 Enter the NSX Edge cluster upgrade plan details.

| Option | Description |
| --- | --- |
| **Serial** | Upgrade all the Edge upgrade unit groups consecutively. |
| | This menu item is selected by default. This selection is applied to the overall upgrade sequence. |
| **Parallel** | Upgrade all the Edge upgrade unit groups simultaneously. |
| | For example, if the overall upgrade is set to the parallel order, the Edge upgrade unit groups are upgraded together and the NSX Edge nodes are upgraded one at a time. |
| **When an upgrade unit fails to upgrade** | Selected by default so that you can fix an error on the Edge node and continue the upgrade. |
| | You cannot deselect this setting. |
| **After each group completes** | Select to pause the upgrade process after each Edge upgrade unit group finishes upgrading. |

2 (Optional) Reorder the upgrade sequence of an Edge upgrade unit group.

For example, if you configure the overall group upgrade as serial, you can reorder the Edge upgrade unit groups serving internal networks or Edge upgrade unit groups interfacing with external networks to be upgraded first.

You cannot reorder the NSX Edge nodes within an Edge upgrade unit group.

a Select the Edge upgrade unit group and click the **Actions** tab.

b Select **Reorder** from the drop-down menu.

c Select **Before** or **After** from the drop-down menu.

d Click **Save**.

**3**   (Optional) Disable an Edge upgrade unit group from the upgrade sequence.

You can disable some Edge upgrade unit groups and upgrade them later.

a   Select the Edge upgrade unit group and click the **Actions** tab.

b   Select **Change State > Disabled** to disable the Edge upgrade unit group.

c   Click **Save**.

**4**   (Optional) Click **Reset** to revert to the default state.

---

**Caution**   After reset, you cannot restore your previous configuration.

---

**5**   Click **Start** to upgrade the NSX Edge cluster.

**6**   Monitor the upgrade process.

You can view the overall upgrade status and progress details of each Edge upgrade unit group. The upgrade duration depends on the number of Edge upgrade unit groups you have in your environment.

You can pause the upgrade to configure the Edge upgrade unit group that is not upgraded and restart the upgrade.

**7**   Click **Run Post Checks** to verify whether the Edge upgrade unit groups were successfully upgraded.

If some Edge upgrade unit groups failed to upgrade, resolve the errors.

**8**   (Optional) In the NSX Manager, select **System > Overview** and verify that the product version is updated on each NSX Edge node.

**What to do next**

If the process is successful, you can proceed with the upgrade. See Configuring and Upgrading Hosts.

If there are upgrade errors, you must resolve the errors. See Chapter 6 Troubleshooting Upgrade Failures.

## Configuring and Upgrading Hosts

You can upgrade your hosts using the upgrade coordinator.

## Configure Hosts

You can customize the upgrade sequence of the hosts, disable certain hosts from the upgrade, or pause the upgrade at various stages of the upgrade process.

All the existing standalone ESXi hosts, vCenter Server managed ESXi hosts, KVM hosts, and bare metal server are grouped in separate host upgrade unit groups by default.

Before you upgrade the hosts, you can select to update the hosts in parallel or serial mode. The maximum limit for a simultaneous upgrade is five host upgrade unit groups and five hosts per group.

**Note**  Host upgrade unit group with hosts that belong to the same vCenter Server cluster can be upgraded serially.

You can customize the host upgrade sequence before the upgrade. You can edit a host upgrade unit group to move a host to a different host upgrade unit group that upgrades immediately and another host to a host upgrade unit group that upgrades later. If you have a frequently used host, you can reorder the host upgrade sequence within a host upgrade unit group so it is upgraded first and move the least used host to upgrade last.

**Note**  You can upgrade your bare metal server using the same steps as provided for upgrading a KVM host.

Prerequisites

- Verify that ESXi hosts that are part of a disabled DRS cluster or standalone ESXi hosts are placed in maintenance mode.

  For ESXi hosts that are part of a fully enabled DRS cluster, if the host is not in maintenance mode, the upgrade coordinator requests the host to be put in maintenance mode. vSphere DRS migrates the VMs to another host in the same cluster during the upgrade and places the host in maintenance mode.

- For ESXi host, for an in-place upgrade you do not need to power off the tenant VMs.

- For a KVM host, for an in-place upgrade you do not need to power off the VMs. For a maintenance mode upgrade, power off the VMs.

- Verify that the transport zone or transport node N-VDS name does not contain spaces.

  If there are spaces, create a transport zone with no spaces in the N-VDS name. You must reconfigure all the components that are associated with the old transport zone to use the new transport zone and delete the old transport zone.

- Verify that your vSAN environment is in good health before you use the in-place upgrade mode.

See the *Place a Host in Maintenance Mode* section of the *vSphere Resource Management* guide.

Procedure

**1** Enter the host upgrade plan details.

You can configure the overall group upgrade order to set the host upgrade unit groups to be upgraded first.

| Option | Description |
| --- | --- |
| **Serial** | Upgrade all the host upgrade unit groups consecutively. |
| | This menu item is selected by default and applied to the overall upgrade sequence. This selection is useful to maintain the step-by-step upgrade of the host components. |
| | For example, if the overall upgrade is set to serial and the host upgrade unit group upgrade is set to parallel, the host upgrade unit group is upgraded one after the other. The hosts within the group are updated in parallel. |
| **Parallel** | Upgrade all the host upgrade unit groups simultaneously. |
| | You can upgrade up to five hosts simultaneously. |
| **When an upgrade unit fails to upgrade** | Select to pause the upgrade process if any host upgrade fails. |
| | This selection allows you to fix the error on the host upgrade unit group and resume the upgrade. |
| **After each group completes** | Select to pause the upgrade process after each host upgrade unit group finishes upgrading. |

**2** (Optional) Change the host upgrade unit group upgrade order.

If you configure the overall group upgrade in the serial order, the upgrade waits for a host upgrade unit group upgrade to finish before proceeding to upgrade the second host upgrade unit group. You can reorder the host upgrade unit group upgrade sequence to set a host upgrade unit group to upgrade first.

a Select the host upgrade unit group and click the **Actions** tab.

b Select **Reorder** from the drop-down menu.

c Select **Before** or **After** from the drop-down menu.

**3** (Optional) Remove a host upgrade unit group from the upgrade sequence.

a Select the host upgrade unit group and click the **Actions** tab.

b Select **Change State** from the drop-down menu.

c Select **Disabled** to remove the host upgrade unit group.

**4** (Optional) Change the individual host upgrade unit group upgrade sequence.

By default, the upgrade sequence is set to the parallel order.

a Select the host upgrade unit group and click the **Actions** tab.

b Select **Change Upgrade Order** from the drop-down menu.

c Select **Serial** to change the upgrade sequence.

**5**  (Optional) Change the host upgrade unit group upgrade mode.

- Select **Maintenance** mode.

    For standalone ESXi hosts and ESXi hosts that are part of a disabled DRS cluster, place the hosts into maintenance mode.

    For KVM hosts, power off the VMs.

    For ESXi hosts that are part of a fully enabled DRS cluster, if the host is not in maintenance mode, the upgrade coordinator requests the host to be put in maintenance mode. vSphere DRS migrates the hosts to another host in the same cluster during the upgrade and places the host in maintenance mode.

- Select **In-place** mode to avoid powering off and placing a host into maintenance mode before the upgrade.

    For standalone ESXi hosts and ESXi hosts that are part of a disabled DRS cluster, you do not need to place the hosts into maintenance mode.

    For KVM hosts, you do not need to power off the VMs.

    For ESXi hosts that are part of a fully enabled DRS cluster, you do not need to place the host into maintenance mode.

    **Note**  During upgrade the host might experience a packet drop in the workload traffic.

- Use an API call `PUT https://<nsx-manager>/api/v1/upgrade/upgrade-unit-groups/<group-id>` and enable the upgrade coordinator to restart the ESXi host.

    The `rebootless_upgrade:true` parameter states that after the ESXi host upgrade, the host is not rebooted.

    By default, the upgrade coordinator does not restart the ESXi host. This mode is used for troubleshooting purposes.

- Use an API call `PUT https://<nsx-manager>/api/v1/upgrade/upgrade-unit-groups/<group-id>` and upgrade vCenter Server managed ESXi hosts that are part of a DRS cluster with vSAN configured.

    The `ensure_object_accessibility` parameter requires vSAN to assume control of data accessibility while a vCenter Server managed ESXi host that is part of a DRS cluster is placed in maintenance mode for the upgrade.

    The `evacuate_all_data` parameter requires vSAN to take all the data from a vCenter Server managed ESXi host that is part of a DRS cluster to another managed ESXi host that is part of a DRS cluster while placed in maintenance mode for the upgrade.

    The `no_action` parameter requires vSAN to take no action while the vCenter Server managed ESXi host that is part of a DRS cluster is placed in maintenance mode for the upgrade.

> For more information about the parameters, see the *Update the upgrade unit group* section of the *NSX-T Data Center REST API guide*.

6   Click **Reset** to discard your custom upgrade plan and revert to the default state.

> **Caution**   You cannot restore your previous upgrade configuration.

If you register a new host transport node during the upgrade, you must click **Reset** to view the status of the recently added host and to continue the upgrade process.

**What to do next**

Determine whether to add, edit, or delete host upgrade unit groups or to upgrade host upgrade unit groups. See Manage Host Upgrade Unit Groups or Upgrade Hosts.

## Manage Host Upgrade Unit Groups

You can edit and delete an existing host upgrade unit group before you start the upgrade or after you pause the upgrade.

Hosts in a ESXi cluster appear in one host upgrade unit group in the upgrade coordinator. You can move these hosts from one host upgrade unit group to another host upgrade unit group.

> **Note**   If any of the hosts are part of a vSAN enabled cluster, retain the default upgrade unit groups without recreating any groups.

**Prerequisites**

- Verify that you have configured the overall hosts upgrade. See Configure Hosts.
- Verify that ESXi hosts that are part of a disabled DRS cluster or standalone ESXi hosts are placed in maintenance mode.

  For ESXi hosts that are part of a fully enabled DRS cluster, if the host is not in maintenance mode, the upgrade coordinator requests the host to be put in maintenance mode. vSphere DRS migrates the VMs to another host in the same cluster during the upgrade and places the host in maintenance mode.

- For ESXi host, for an in-place upgrade you do not need to power off the tenant VMs.
- For a KVM host, for an in-place upgrade you do not need to power off the VMs. For a maintenance mode upgrade, power off the VMs.

**Procedure**

1   Create a host upgrade unit group.

  a   Click **Add** to include existing hosts into a host upgrade unit group.

  b   Toggle the **State** button to enable or disable the host upgrade unit group from the upgrade.

    c    Select an existing host and click the arrow icon to move that host to the newly created host upgrade unit group.

        If you select an existing host that was part of a host upgrade unit group, the host is moved to the new host upgrade unit group.

    d    Select whether to upgrade the host upgrade unit group in parallel or serial mode.

    e    Select the upgrade mode.

        See step 5 of Configure Hosts.

    f    (Optional) Select **Reorder** from the drop-down menu to reposition the host upgrade unit groups.

    g    (Optional) Select **Before** or **After** from the drop-down menu.

**2**    Move an existing host to another host upgrade unit group.

    If an enabled DRS ESXi cluster is part of the upgrade, then a host upgrade unit group is created for the hosts managed by this cluster.

    a    Select a host upgrade unit group.

    b    Select a host.

    c    Click the **Actions** tab.

    d    Select **Change Group** from the drop-down menu to move the host to another host upgrade unit group.

    e    Select the host upgrade unit group name from the drop-down menu to move the host to.

    f    (Optional) Select **Reorder** from the drop-down menu to reposition the host within the host upgrade unit group.

    g    (Optional) Select **Before** or **After** from the drop-down menu.

**3**    Delete a host upgrade unit group.

    You cannot delete a host upgrade unit group that has hosts. You must first move the hosts to another group.

    a    Select the host upgrade unit group.

    b    Select a host.

    c    Click the **Actions** tab.

    d    Select **Change Group** from the drop-down menu to move the host to another host upgrade unit group.

    e    Select the host upgrade unit group name from the drop-down menu to move the host to.

    f    Select the host upgrade unit group you want to remove and click **Delete**.

    g    Accept the notification.

**What to do next**

Upgrade the newly configured hosts. See Upgrade Hosts.

# Upgrade Hosts

Upgrade the hosts in your environment using the upgrade coordinator.

**Prerequisites**

- Verify that you have configured the overall hosts upgrade plan. See Configure Hosts.

- Verify that ESXi hosts that are part of a disabled DRS cluster or standalone ESXi hosts are placed in maintenance mode.

  For ESXi hosts that are part of a fully enabled DRS cluster, if the host is not in maintenance mode, the upgrade coordinator requests the host to be put in maintenance mode. vSphere DRS migrates the VMs to another host in the same cluster during the upgrade and places the host in maintenance mode.

- For ESXi host, for an in-place upgrade you do not need to power off the tenant VMs.

- For a KVM host, for an in-place upgrade you do not need to power off the VMs. For a maintenance mode upgrade, power off the VMs.

- For hosts running ESXi 6.5U2/U3 or ESXi 6.7U1/U2, during maintenance mode upgrade to NSX-T Data Center 2.5.1, the host is rebooted if stale DV filters are found to be present on the host. Upgrade to ESXi 6.7 U3 or ESXi 6.5 P04 prior to upgrading to NSX-T Data Center 2.5.1 if you want to avoid rebooting the host during the NSX-T Data Center upgrade.

- For a stateless ESXi host, log in vCenter Server and update the ESXi image with the NSX-T Data Center kernel modules.

**Procedure**

1  Click **Start** to upgrade the hosts.

2  Monitor the upgrade process.

   You can view the overall upgrade status and specific progress of each host upgrade unit group. The upgrade duration depends on the number of host upgrade unit groups you have in your environment.

   Wait until the in progress upgrade units are successfully upgraded. You can then pause the upgrade to configure the host upgrade unit group that is not upgraded and resume the upgrade.

3    Click **Run Post Checks** to make sure that the upgraded hosts and NSX-T Data Center do not have any problems.

> **Note**  If a host upgrade unit failed to upgrade and you removed the host from NSX-T Data Center, refresh the upgrade coordinator to view all the successfully upgraded host upgrade units.
>
> If a host fails during the upgrade, reboot the host and try the upgrade again.

4    After the upgrade is successful, verify that the latest version of NSX-T Data Center packages is installed on the vSphere, KVM hosts, and bare metal server.

- For vSphere hosts, enter `esxcli software vib list | grep nsx`

- For Ubuntu hosts, enter `dpkg –l | grep nsx`

- For SUSE Linux Enterprise Server, Red Hat, or CentOS hosts, enter `rpm –qa | egrep 'nsx|openvswitch|nicira'`

5    Power on the tenant VMs of standalone ESXi hosts that were powered off before the upgrade.

6    Migrate the tenant VMs on hosts managed by vCenter Server that are part of the enabled DRS cluster to the appropriate host.

7    Power on or return the tenant VMs of ESXi hosts that are part of a disabled DRS cluster that were powered off before the upgrade.

**What to do next**

You can proceed with the upgrade only after the upgrade process finishes successfully. If some of the hosts are disabled, you must enable and upgrade them before you proceed. See Upgrade Management Plane.

If there are upgrade errors, you must resolve the errors. See Chapter 6 Troubleshooting Upgrade Failures.

## Upgrade Hosts Manually

You can manually upgrade hosts in a host upgrade unit group.

**Prerequisites**

Verify that the upgrade coordinator is updated. See Upgrade the Upgrade Coordinator.

**Procedure**

1    In the upgrade coordinator, navigate to the Host Upgrade tab.

2    Select an enabled host upgrade unit group.

3    Select **Actions > Change State > Disabled**.

If you have other enabled host upgrade unit groups, set them to **Disabled**.

**4** Click **Start** to perform the pre-upgrade process.

**5** Wait for the host upgrade to pause.

**6** Upgrade your ESXi host manually.

> **Note** If a host fails during the upgrade, reboot the host and try the upgrade again.

   a Put the ESXi host in Maintenance mode.

   b Navigate to the ESXi offline bundle location from the NSX Manager.

   http://<nsx-manager-ip-address>:8080/repository/<target-nsx-t-version>/metadata/
   manifest.

   c Download the ESXi offline bundle to `/tmp` on ESXi.

   d Upgrade the ESXi host.

   ```
   esxcli software vib install -d /tmp/<offline-bundle-name>.
   ```

**7** Upgrade your KVM host manually.

> **Note** If a host fails during the upgrade, reboot the host and try the upgrade again.

   a Download the upgrade script.

   http://<nsx-manager-ip-address>:8080/repository/<target-nsx-t-version>/
   HostComponents/<os-type>/upgrade.sh

   Where the os_type is rhel76_x86_64, rhel77_x86_64, xenial_amd64, linux64-bionic,
   linux64-sles12sp3, or linux64-sles12sp4.

   b Upgrade the KVM host.

   ```
   upgrade.sh <host-upgrade-bundle-url>
   ```

   Where the host upgrade bundle URL is, http://<nsx-manager-ip-address>:8080/xyz
   where xyz, is one of the paths from the http://<nsx-manager-ip-address>:8080/
   repository/<target-nsx-version>/metadata/manifest file.

   For example, http://<nsx-manager-ip-address>:8080/repository/3.0.0.0.0.99999999/
   HostComponents/rhel76_x86_64/nsx-lcp-2.3.0.0.0.9999999-rhel76_x86_64.tar.gz.

**8** In the upgrade coordinator, navigate to the **Hosts** tab and refresh the page.

   All the manually upgraded hosts appear in the upgraded state.

**9** After the upgrade is successful, verify that the latest version of NSX-T Data Center packages
   is installed on the vSphere and KVM hosts.

   ■ For vSphere hosts, enter `esxcli software vib list | grep nsx`.

   ■ For Ubuntu hosts, enter `dpkg -l | grep nsx`.

   ■ For SUSE Linux Enterprise Server, Red Hat, or CentOS hosts, enter `rpm -qa | egrep
   'nsx|openvswitch|nicira'`.

10 Power on the tenant VMs of standalone ESXi hosts that were powered off before the upgrade.

11 Migrate the tenant VMs of managed ESXi hosts that are part of the DRS disabled cluster to the appropriate host.

12 Power on or return the tenant VMs of ESXi hosts that are part of a DRS disabled cluster that were powered off before the upgrade.

13 (Optional) In the NSX Manager appliance, select **System > Appliances** and verify that all the status indicators for host and transport node deployment appear as installed and connection status is up and green.

14 In the upgrade coordinator, navigate to the **Hosts** tab and select a disabled host upgrade unit group.

15 Select **Actions > Change State > Enabled**.

If you have other disabled host upgrade unit groups, set them to **Enabled**.

**What to do next**

You can proceed with the upgrade only after the upgrade process finishes successfully. See Upgrade Management Plane.

If there are upgrade errors, you must resolve the errors. See Chapter 6 Troubleshooting Upgrade Failures.

## Upgrade Management Plane

The upgrade coordinator orchestrates the upgrade of the Management Plane at the end. When the Management Plane upgrade is in progress, avoid any configuration changes from any of the nodes.

**Note** After you initiate the upgrade, the NSX Manager user interface is briefly inaccessible. Then the NSX Manager user interface, API, and CLI are not accessible until the upgrade finishes and the Management plane is restarted.

**Prerequisites**

Verify that the NSX Edge cluster is upgraded successfully. See Upgrade NSX Edge Cluster.

If you are upgrading from a version earlier than NSX-T Data Center 3.0, provision a secondary disk of exactly 100 GB capacity on all NSX Manager appliances. Reboot the appliance if the secondary disk is not detected by the Upgrade Coordinator.

**Procedure**

1 Backup the NSX Manager.

See the *NSX-T Data Center Administration Guide*.

2 Click **Start** to upgrade the Management plane.

**3** Accept the upgrade notification.

You can safely ignore any upgrade related errors such as, HTTP service disruption that appears at this time. These errors appear because the Management plane is rebooting during the upgrading.

Wait until all the nodes are upgraded. It may take several minutes for the cluster to reach a stable state.

**4** In the CLI, log in to the NSX Manager to verify that the services have started and to check the cluster status.

- `get service`

  When the services start, the Service state appears as running. Some of the services include, SSH, install-upgrade, and manager.

  `get service` lists the IP address of the orchestrator node. See `Enabled on`. Use this IP address throughout the upgrade process.

  ---
  **Note** Ensure that you do not use any type of Virtual IP address to upgrade NSX-T Data Center.

  ---

  If the services are not running, troubleshoot the problem. See the *NSX-T Data Center Troubleshooting Guide*.

- `get cluster status`

  If the group status is not Stable, troubleshoot the problem. See the *NSX-T Data Center Troubleshooting Guide*.

**What to do next**

Perform post-upgrade tasks or troubleshoot errors depending on the upgrade status. See Chapter 5 Post-Upgrade Tasks or Chapter 6 Troubleshooting Upgrade Failures.

# Upgrading NSX Cloud Components

<div style="text-align: right">**4**</div>

NSX Cloud components are upgraded using the following workflow.

## Upgrading NSX Cloud components from 3.0.0 to later

If you are upgrading NSX Cloud components from NSX-T Data Center 3.0.0 to later, follow this checklist:

Table 4-1. Checklist to upgrade NSX Cloud components from 3.0.0 to later

| Task | Instructions |
|------|-------------|
| ❏ Run the day-0 NSX Cloud scripts to update permissions for the PCG role in your public cloud. | See Regenerate the Public Cloud Permissions |
| ❏ Upgrade the **Upgrade Coordinator** from CSM. | See Upgrade the Upgrade Coordinator from CSM. |
| ❏ Upgrade the **Upgrade Coordinator** from NSX Manager. | See: Upgrade the Upgrade Coordinator from NSX Manager . |
| ❏ Upgrade PCG and NSX Tools. | See Upgrade PCG and NSX Tools. |
| ❏ Upgrade NSX Manager. | See Upgrade NSX Manager. |
| ❏ Upgrade CSM. | See Upgrade CSM |

## Upgrading NSX Cloud components from 2.5.x to later

If you are upgrading NSX Cloud components from NSX-T Data Center 2.5.x to later, follow this checklist:

Table 4-2. Checklist to upgrade NSX Cloud components from 2.5.x to later

| Task | Instructions |
|------|-------------|
| ❏ Run the day-0 NSX Cloud scripts to update permissions for the PCG role in your public cloud. | See Regenerate the Public Cloud Permissions |
| ❏ Upgrade the **Upgrade Coordinator** from CSM. | See Upgrade the Upgrade Coordinator from CSM. |
| ❏ Upgrade the **Upgrade Coordinator** from NSX Manager. | See: Upgrade the Upgrade Coordinator from NSX Manager . |

Table 4-2. Checklist to upgrade NSX Cloud components from 2.5.x to later (continued)

| Task | Instructions |
| --- | --- |
| ☐ Upgrade PCG and NSX Tools. | See Upgrade PCG and NSX Tools. |
| ☐ Upgrade CSM. | See Upgrade CSM |
| ☐ Upgrade NSX Manager. | See Upgrade NSX Manager. |

Procedure

**1**　Regenerate the Public Cloud Permissions

Before upgrading NSX Cloud components, regenerate the necessary permissions for your public cloud account required by NSX Cloud.

**2**　Upgrade the Upgrade Coordinator from CSM

Follow these instructions to first download the upgrade bundle in CSM and then upgrade the Upgrade Coordinator from CSM

**3**　Upgrade the **Upgrade Coordinator** from NSX Manager

Follow these instructions to download the upgrade bundle in NSX Manager and upgrade the **Upgrade Coordinator** from NSX Manager.

**4**　Upgrade PCG and NSX Tools

Upgrade PCG first and then NSX Tools.

**5**　Upgrade NSX Manager

Follow these instructions to upgrade NSX Manager.

**6**　Upgrade CSM

In the current release, CSM can only be upgraded using NSX CLI.

## Regenerate the Public Cloud Permissions

Before upgrading NSX Cloud components, regenerate the necessary permissions for your public cloud account required by NSX Cloud.

- Microsoft Azure: See: *Generate the Service Principal and Roles* in the *NSX-T Data Center Installation Guide*.

- AWS: See: *Generate the IAM Profile and PCG Role* in the *NSX-T Data Center Installation Guide*.

## Upgrade the Upgrade Coordinator from CSM

Follow these instructions to first download the upgrade bundle in CSM and then upgrade the Upgrade Coordinator from CSM

# Download the NSX Cloud Upgrade Bundle

Begin the upgrade process by downloading the NSX Cloud upgrade bundle.

The NSX Cloud upgrade bundle contains all the files to upgrade the NSX Cloud infrastructure. Before you begin the upgrade process, you must download the correct upgrade bundle version.

**Procedure**

1 In the VMware download portal, locate the NSX-T Data Center version available to upgrade and navigate to **Product Downloads > NSX Cloud Upgrade Bundle for NSX-T <version>.**

2 Verify that the master upgrade bundle (`.mub`) filename has a format similar to `VMware-CC-upgrade-bundle-`*ReleaseNumberNSXBuildNumber*`.mub`.

   **Note**  This is a separate file and must be downloaded in addition to the NSX-T Data Center upgrade bundle.

3 Click **Download Now** to download the NSX Cloud upgrade bundle.

   **Note**  The upgrade bundle is uploaded into CSM. Download it either on the same system from where you access the CSM UI, or note the location of the system where you download it, to provide a remote URL of this system into CSM for uploading.

**What to do next**

Upgrade the Upgrade Coordinator in CSM.

# Upgrade the Upgrade Coordinator in CSM

Upload the upgrade bundle and upgrade the Upgrade Coordinator appliance in CSM

**Procedure**

1 Log in to CSM with the Enterprise Administrator role.

2 Click **Utilities > Upgrade**

3 Click **Upload Upgrade Bundle**. Pick a location for the upgrade bundle. You can provide a remote location using a URL.

4 After the upgrade bundle finishes uploading in CSM, click **Prepare for Upgrade** to start the process of upgrading the Upgrade Coordinator.

   **Note:** The upgrade bundle must be a valid file in the `.mub` format. Do not use `.nub` or other files. See Upgrade the Upgrade Coordinator for details.

   When the Upgrade Coordinator upgrade process finishes, the **Begin Upgrade** button becomes active.

**What to do next**

Upgrade the Upgrade Coordinator from NSX Manager .

# Upgrade the **Upgrade Coordinator** from NSX Manager

Follow these instructions to download the upgrade bundle in NSX Manager and upgrade the **Upgrade Coordinator** from NSX Manager.

**Note**  If you are upgrading from 2.5.0, this step is not required during the NSX Cloud upgrade. Proceed with the next step.

- Download the upgrade bundle: Download the NSX-T Data Center Upgrade Bundle

- Upgrade the Upgrade Coordinator from NSX Manager: Upgrade the Upgrade Coordinator

## What to do next

Upgrade PCG and NSX Tools

# Upgrade PCG and NSX Tools

Upgrade PCG first and then NSX Tools.

**Prerequisites**

- Outbound port 8080 must be open on workload VMs that need to be upgraded.

- The PCGs must be powered on when the upgrade of NSX Tools installed on workload VMs or of PCGs is in progress.

**Procedure**

1 Log in to CSM with the Enterprise Administrator role.

2 Click **Utilities > Upgrade > Begin Upgrade**. The **Upgrade CSM** wizard starts.

   **Note:** Although the name of the wizard is **Upgrade CSM**, you can only upgrade NSX Tools and PCG from this wizard.

3 In the **Upgrade CSM > Overview** screen, you can see an overview of the default upgrade plan. Based on the upgrade bundle you have uploaded, you can see which versions of NSX Tools and PCG are compatible for an upgrade via the upgrade bundle uploaded.

4 Click **Next**. The **CSM > Select NSX Tools** screen appears.

5 Click **Skip NSX Tools Upgrade**. See Skip Upgrading NSX Tools for details.

6 Click **Next** to proceed with upgrading the PCG. With an HA pair of PCGs, there are two failovers during the upgrade process and when the upgrade finishes, the preferred PCG is reinstated as the active gateway.

7 Click **Finish** to upgrade PCG.

**8**    Return to the CSM Upgrade Coordinator and click **Begin Upgrade**. Then click **Next** on the **Upgrade Plan** screen to proceed with upgrading NSX Tools.

A list of all compatible NSX Tools that can be upgraded to the target version in all your VPCs or VNets, are displayed. You can filter NSX Tools based on which private cloud network they are in or which OS they are deployed on. All NSX-managed VMs are eligible for upgrade and listed for you to select. Fix any errors on NSX-managed VMs which are quarantined before selecting them for upgrade to prevent the upgrade of NSX Tools on such VMs from failing.

a    Select the NSX Tools you want to upgrade and move them to the **Selected** window.

b    Click **Next**. CSM downloads the upgrade bits to the PCG on which the NSX Tools reside. The PCG copies these upgrade bits to the VMs which have been selected for upgrade.

If you have an HA pair of PCG, CSM downloads the upgrade bits to each PCG and starts upgrading the selected NSX Tools. NSX Tools in the same VPC/VNet are upgraded in parallel. Ten NSX Tools under a VPC/VNet are upgraded simultaneously.

If you have more than ten NSX Tools, they are queued for upgrading. PCG maintains a flag on VMs that are unreachable and attempts to upgrade them when they can be reached. For example, a powered off workload VM is upgraded when powered on again and able to communicate with PCG. Similarly for a workload VM on which port 8080 is blocked at first but when port 8080 is opened and PCG can access it, the upgrade for that workload VM proceeds. If some NSX Tools are not able to be upgraded, you can skip upgrading them in order to proceed. See Skip Upgrading NSX Tools for details on this option.

If you run into problems while upgrading NSX Tools, refer to these troubleshooting instructions: Troubleshooting NSX Tools Upgrade on Windows Workload VMs and Troubleshooting NSX Tools Upgrade on Linux Workload VMs

**Results**

PCGs and NSX Tools are upgraded.

**Note**   If you are upgrading from NSX-T Data Center 2.x to NSX-T Data Center 3.x and you have service insertion set up in version 2.x, you must create a lowest priority default catch-all rule with the action set to **Do Not Redirect**. Follow instructions described in "Set Up Redirection Rules" in the *NSX-T Data Center Administration Guide*.

**How long does the upgrade process take**

**Note**   CSM and NSX-T Data Center components are upgraded separately, and that time is not included here. This is an estimation to help you plan your upgrade cycles.

■   **One or an HA pair of PCGs**: PCGs in different VPCs or VNets are upgraded in parallel, but PCGs in HA pair upgrade serially. It takes about 20 minutes for one PCG to upgrade.

■   **One VPC or VNet**: For a VPC or VNet with up to 10 VMs and an HA pair of PCGs, it can take up to 45 minutes to upgrade. This time may vary depending on the OS on the VMs and their size.

- **NSX Tools installed on a workload VM**: It takes from 3 to 5 minutes for each NSX Tools installation on a VM to upgrade, not accounting for the time it takes to upload the upgrade bundle from CSM to the public cloud. 10 VMs with NSX Tools installed are upgraded simultaneously. For multiple compute VPCs/VNets per Transit VPC/VNet, all VMs with NSX Tools installed on one Compute VPC/VNet are first upgraded before proceeding to the next. The time to upgrade NSX Tools also varies for different operating systems and the VM size.

**What to do next**

Follow the next step in the checklist that applies to the version you are upgrading from: Chapter 4 Upgrading NSX Cloud Components .

## Skip Upgrading NSX Tools

You can skip upgrading NSX Tools for reasons listed here.

Except under the following scenarios, do not skip the upgrade of NSX Tools because VMs with NSX Tools in a different version compared to PCG will lose connectivity with the PCG.

Scenarios for skipping NSX Tools upgrade:

- You are upgrading to 3.0.x or 3.1.x from an earlier version. In this case skip upgrading NSX Tools, upgrade PCG, and return to upgrading NSX Tools.

  You are able to upgrade NSX Tools after the upgrade of PCG in this case because the system maintains connectivity for the duration of this upgrade.

- You want to upgrade only selected private clouds within your public cloud.

- You do not want any downtime on certain critical managed workload VMs.

- You do not want powered off VMs to block the upgrade process.

- You might want to apply a bug-fix patch only to the PCG without affecting NSX Tools.

## Troubleshooting NSX Tools Upgrade on Windows Workload VMs

Upgrading NSX Tools on Windows workload VMs might fail at first. Try the following troubleshooting options.

### Manually uninstall and reinstall NSX Tools

If NSX Tools are not getting upgraded, you might have to manually uninstall them, recover the system, and then install the new version. Follow these steps:

1   Uninstall NSX Tools by running the command:

```
> powershell -file nsx_install.ps1 -operation uninstall
```

2   Recover the system and restore it to a stable state by running the following commands:

a   Check whether any NSX or OVS services are still running:

```
> powershell Get-ScheduledTask -Taskname nsx_watchdog
> powershell Unregister-ScheduledTask -TaskName nsx_watchdog
> tasklist | findstr nsx
> tasklist | findstr ovs
```

b   If NSX/OVS services are running, stop the services in the following order:

```
> sc.exe stop nsx-agent
> sc.exe delete nsx-agent

> sc.exe stop nsx-exporter
> sc.exe delete nsx-exporter

> sc.exe stop nsx-vm-command-relay-agent
> sc.exe delete nsx-vm-command-relay-agent

> sc.exe stop ovs-vswitchd
> sc.exe delete ovs-vswitchd

> sc.exe stop ovsdb-server
> sc.exe delete ovs-vswitchd
```

c   Check whether the OVSIM kernel driver is installed. If installed, manually uninstall the driver.

```
>netcfg -q ovsim
>netcfg /u ovsim
```

d   Reset TCP/IP stack to restore the TCP/IP stack to default state.

```
> netsh winsock reset
> netsh int ip reset
```

e   Remove all NSX components files.

```
> Remove-Item "C:\ProgramData\VMware\NSX\Data" -Force
> Remove-Item "C:\Program Files\VMware\NSX" -Force
```

f   Reboot the system. After reboot, clean up the driver (INF) files. Retrieve the INF file name using `nsx_conf.json`.

---

**Note**  If the file `nsx_conf.json` is not present, skip this step.

---

```
> C:\Windows\system32>more C:\ProgramData\VMware\NSX\Data\nsx_conf.json

{
     "NSX": {
      "version": null,
      "OVS": {
      "version": "2.12.1.32033",
       "driver_inf": "oem9.inf"
       }
       }
}

> pnputil -d oem9.inf
```

3   Install NSX Tools by following instructions at "Install NSX Tools" in the *NSX-T Data Center Administration Guide*.

4   In your public cloud, remove the `nsx.network=default` tag from the VM, wait for at least two minutes and add the tag back. This ensures the workload VM gets connected with the PCG.

## Troubleshooting NSX Tools Upgrade on Linux Workload VMs

Upgrading NSX Tools on Linux workload VMs might fail at first.

From the Linux workload VMs where upgrade failed, uninstall NSX Tools and reinstall the new version of NSX Tools.

1   To uninstall NSX Tools:

a   Remote log in to the VM using SSH.

b   Run the installation script with the uninstall option: `sudo ./install_nsx_vm_agent.sh --uninstall`

2   To reinstall NSX Tools, see instructions in "Install NSX Tools on Linux VMs" in the *NSX-T Data Center Administration Guide*.

3   In your public cloud, remove the `nsx.network=default` tag from the VM, wait for at least two minutes and add the tag back. This ensures the workload VM gets connected with the PCG.

# Upgrade NSX Manager

Follow these instructions to upgrade NSX Manager.

**Note** If you are upgrading from 2.5.0, upgrade NSX Manager after upgrading CSM.

See Upgrade Management Plane.

## What to do next

Upgrade CSM.

# Upgrade CSM

In the current release, CSM can only be upgraded using NSX CLI.

### Prerequisites

- See Chapter 4 Upgrading NSX Cloud Components to find the correct order to follow for upgrading CSM.

- You must have extracted the file `VMware-NSX-unified-appliance-<version>.nub` from the NSX Cloud master upgrade bundle (MUB) and hosted on an FTP server accessible from CSM.

### Procedure

**1** Log in to NSX CLI with CSM admin credentials:

```
$ssh <csm-admin>@<NSX-CSM-IP>
```

and run the following NSX CLI command:

```
nsxcsm> copy url scp://<username>@<ftp-server-ip>/<path-to-file>/VMware-NSX-unified-
appliance-<version>.nub
```

**2** Extract and verify the file `VMware-NSX-unified-appliance-<version>.nub`:

```
nsxcsm> verify upgrade-bundle VMware-NSX-unified-appliance-<version>
```

Example output:

```
Checking upgrade bundle /var/vmware/nsx/file-store/VMware-NSX-unified-appliance-
<version>.nub contents
Verifying bundle VMware-NSX-unified-appliance-<version>.bundle with signature VMware-NSX-
unified-appliance-<version>.bundle.sig
Moving bundle to /image/VMware-NSX-unified-appliance-<version>.bundle
Extracting bundle payload
Successfully verified upgrade bundle
```

```
Bundle manifest:
    appliance_type: 'nsx-unified-appliance'
    version: '<upgrade version>'
    os_image_path: 'files/nsx-root.fsa'
    os_image_md5_path: 'files/nsx-root.fsa.md5'
Current upgrade info:
{
  "info": "",
  "body": {
    "meta": {
      "from_version": "<current version>",
      "old_config_dev": "/dev/mapper/nsx-config",
      "to_version": "<post-upgrade version>",
      "new_config_dev": "/dev/mapper/nsx-config__bak",
      "old_os_dev": "/dev/xvda2",
      "bundle_path": "/image/VMware-NSX-unified-appliance-<version>",
      "new_os_dev": "/dev/xvda3"
    },
    "history": []
  },
  "state": 1,
  "state_text": "CMD_SUCCESS"
}
```

**3**   Start the upgrade:

```
nsxcsm> start upgrade-bundle VMware-NSX-unified-appliance-<version> playbook VMware-NSX-
cloud-service-manager-<version>-playbook
```

Example output:

```
Validating playbook /var/vmware/nsx/file-store/VMware-NSX-cloud-service-manager-<version>-
playbook.yml
Running "shutdown_csm_svc" (step 1 of 6)
Running "install_os" (step 2 of 6)
Running "migrate_csm_config" (step 3 of 6)

System will now reboot (step 4 of 6)
After the system reboots, use "resume" to start the next step, "start_csm_svc".
{
  "info": "",
  "body": null,
  "state": 1,
  "state_text": "CMD_SUCCESS"
}
Autoimport-nsx-cloud-service-manager-thin>
Broadcast message from root@Autoimport-nsx-cloud-service-manager-thin (Fri 2017-08-25
21:11:36 UTC):

The system is going down for reboot at Fri 2017-08-25 21:12:36 UTC!
```

**4**   Wait for the upgrade to complete. CSM reboots during upgrade, and the upgrade is finalized when the CSM UI restarts after rebooting.

**5** Verify the version of CSM to confirm that it has upgraded:

```
nsxcsm> get version
```

**Results**

The CSM appliance is upgraded and the PCGs are automatically resized to 191 GB.

**What to do next**

- If you are upgrading from version 2.4.x to 2.5.0 or later, or from 3.0.x to later, follow the steps here for Chapter 5 Post-Upgrade Tasks because you have already upgraded NSX-T Data Center.

- If you are upgrading from version 2.5.0 to later, proceed to Chapter 3 Upgrading NSX-T Data Center.

# Post-Upgrade Tasks

# 5

After you upgrade NSX-T Data Center, perform post-upgrade verification tasks to check whether the upgrade was successful.

This chapter includes the following topics:

- Verify the Upgrade

- Enhance NSX Edge Performance after ESXi Host Upgrade

- Update NSX Intelligence Appliance

## Verify the Upgrade

After you upgrade NSX-T Data Center, you can verify whether the versions of the upgraded components have been updated. For more information on the NSX Manager, see "Overview of the NSX Manager" in the *NSX-T Data Center Administration Guide*.

**Prerequisites**

Perform a successful upgrade. See Chapter 3 Upgrading NSX-T Data Center.

**Procedure**

1  From your browser, log in as a local admin user to an NSX Manager at https://*nsx-manager-ip-address/login.jsp?local=true*.

2  Select **System > Upgrade**.

**3** Verify that the overall upgrade version, component version, and initial and target product version are accurate.

    a   (Optional) Verify that the Dashboard, fabric hosts, NSX Edge cluster, transport nodes, and all logical entities status indicators are green, normal, deployed, and do not show any warnings.

    b   (Optional) Verify the status of several components.

- Fabric nodes installation

- Transport node Local Control Plane (LCP) and Management plane agent connectivity

- Routers connectivity

- NAT rules

- DFW rules

- DHCP lease

- BGP details

- Flows in the IPFIX collector

- TOR connectivity to enable the network traffic

The status of the upgrade appears as Successful.

**4** Modify the default admin password expiration.

If the password expires, you will be unable to log in and manage components. Additionally, any task or API call that requires the administrative password to execute will fail. By default, passwords expire after 90 days. If your password expires, see Knowledge Base article 70691 NSX-T admin password expired.

    a   Reset the expiration period.

You can set the expiration period for between 1 and 9999 days.

```
nsxcli set user admin password-expiration <1 - 9999>
```

    b   (Optional) You can disable password expiry so the password never expires.

```
nsxcli clear user audit password-expiration
```

**5** If you have an existing Ubuntu KVM host as a transport node, back up the `/etc/network/interfaces` file.

**6** If you have VIDM enabled, access your the local account at https://*nsx-manager-ip-address*/login.jsp?local=true.

**7** Verify CPU and Memory values for NSX Edge VMs.

After upgrading, log in to the vSphere Client to verify if your existing NSX Edge VMs are configured with the following CPU and Memory values. If they are not, edit the VM settings to match these values.

| NSX-T Data Center Appliance | Memory | vCPU |
|---|---|---|
| NSX Edge Small VM | 4 GB | 2 |
| NSX Edge Medium VM | 8 GB | 4 |
| NSX Edge Large VM | 32 GB | 8 |

# Enhance NSX Edge Performance after ESXi Host Upgrade

vSphere ESXi 6.7 supports Receive Side Scaling (RSS) for UDP which provides significant improvement in throughput. Use this feature for workloads that are sensitive to network latency and bandwidth. Update your NSX Edge settings for performance enhancement.

Procedure

1   (Optional) If all your ESXi hosts are upgraded to vSphere 6.7 Update 3, upgrade the hardware version for the NSX Edge virtual machine and skip the remaining steps.

   For more information on upgrading VM hardware, see the VMware knowledge base article at https://kb.vmware.com/s/article/1010675

   **Note**   Do not update the hardware version for NSX Edge VMs if any of your ESXi hosts are not upgraded to vSphere 6.7 Update 3 or later.

2   Log in to the vSphere Web Client as an administrator, and connect to the ESXi host where your NSX Edge virtual machine (VM) resides.

3   Power off the NSX Edge VM.

4   Download the `<virtual_machine_file>.vmx` file from the datastore on the ESXi host.

   Create a backup of the `.vmx` file that you can restore to, if necessary.

5   Edit the `<virtual_machine_file>.vmx` file to add the new property, `udpRSS=1`, and save your changes.

   For more information on editing files, see the VMware knowledge base article at https://kb.vmware.com/s/article/1714 and https://kb.vmware.com/s/article/1020302.

6   Save a backup of the edited `.vmx` file.

   If the edited version of your file is overwritten due configuration changes, copy the relevant sections from the backup into the current file. Do not replace the entire `.vmx` file with an older backup.

7   Upload the edited `<virtual_machine_file>.vmx` file to the datastore.

8   Power on the NSX Edge VM.

# Update NSX Intelligence Appliance

Update the NSX Intelligence appliance with information about the NSX Manager appliance that you have upgraded.

This task is applicable only if you have an NSX Intelligence appliance deployed and connected to an NSX Manager appliance that you have updated. To ensure that the correct NSX Manager connectivity information is used when using NSX Intelligence, you must update the NSX Manager appliance's IP address, Certificate, and Certificate Thumbprint information stored in the NSX Intelligence appliance.

**Procedure**

◆ Use the steps described in the VMware Knowledge Base article https://kb.vmware.com/s/article/78505.

# Troubleshooting Upgrade Failures 6

You can review the support bundle log messages to identify the upgrade problem.

You can also perform any of the following debugging tasks.

- Log in to the NSX Manager CLI as root user and navigate to the upgrade coordinator log files `/var/log/upgrade-coordinator/upgrade-coordinator.log`.

- Navigate to the system log files `/var/log/syslog` or API log files `/var/log/proton/nsxapi.log`.

- Configure a remote logging server and send log messages for troubleshooting. See *NSX-T Data Center Administration Guide*.

**Note** If you are unable to troubleshoot the failure and want to revert to the previous working version of NSX-T Data Center, contact VMware support.

This chapter includes the following topics:

- Collect Support Bundles
- Upgrade Fails Due to a Timeout
- Upgrade Fails Due to Insufficient Space in Bootbank on ESXi Host
- Failed Upgrade Host Placed in Maintenance Mode
- Failure to Upload the Upgrade Bundle
- Backup and Restore During Upgrade
- Loss of Controller Connectivity after Host Upgrade
- In-place Upgrade Fails
- Purple diagnostic screen when Upgrading from NSX-T Data Center 2.5.2

## Collect Support Bundles

You can collect support bundles on registered cluster and fabric nodes and download the bundles to your machine or upload them to a file server.

If you choose to download the bundles to your machine, you get a single archive file consisting of a manifest file and support bundles for each node. If you choose to upload the bundles to a file server, the manifest file and the individual bundles are uploaded to the file server separately.

**NSX Cloud Note**   If you want to collect the support bundle for CSM, log in to CSM, go to **System > Utilities > Support Bundle** and click on **Download**. The support bundle for PCG is available from NSX Manager using the following instructions. The support bundle for PCG also contains logs for all the workload VMs.

Procedure

1   From your browser, log in as a local admin user to an NSX Manager at https://*nsx-manager-ip-address/login.jsp?local=true*.

2   Select **System > Support Bundle**

3   Select the target nodes.

    The available types of nodes are **Management Nodes**, **Edges**, **Hosts**, and **Public Cloud Gateways**.

4   (Optional) Specify log age in days to exclude logs that are older than the specified number of days.

5   (Optional) Toggle the switch that indicates whether to include or exclude core files and audit logs.

    **Note**   Core files and audit logs might contain sensitive information such as passwords or encryption keys.

6   (Optional) Select the check box to upload the bundles to a remote file server.

7   Click **Start Bundle Collection** to start collecting support bundles.

    Depending on how many log files exist, each node might take several minutes.

8   Monitor the status of the collection process.

    The status tab shows the progress of collecting support bundles.

9   Click **Download** to download the bundle if the option to send the bundle to a file remote server was not set.

    The bundle collection may fail for a manager node if there is not enough disk space. If you encounter an error, check whether older support bundles are present on the failed node. Log in to the NSX Manager UI of the failed manager node using its IP address and initiate the bundle collection from that node. When prompted by the NSX Manager, either download the older bundle or delete it.

# Upgrade Fails Due to a Timeout

An event during the upgrade process fails and the message from the Upgrade Coordinator indicates a timeout error.

### Problem

During the upgrade process, the following events might fail because they do not complete within a specific time. The Upgrade Coordinator reports a timeout error for the event and the upgrade fails.

| Event | Timeout Value |
| --- | --- |
| Putting a host into maintenance mode | 4 hours |
| Waiting for a host to reboot | 32 minutes |
| Waiting for the NSX service to be running on a host | 13 minutes |

### Solution

◆ For the maintenance mode issue, log in to vCenter Server and verify the status of tasks related to the host. Resolve any problems.

◆ For the host reboot issue, check the host to see why it failed to reboot.

◆ For the NSX service issue, log in to the NSX Manager UI, select **System > Appliances** and see if the host has an installation error. If so, you can resolve it from the NSX Manager UI. If the error cannot be resolved, you can refer to the upgrade logs to determine the cause of the failure.

# Upgrade Fails Due to Insufficient Space in Bootbank on ESXi Host

NSX-T Data Center upgrade might fail if there is insufficient space in the bootbank or in the alt-bootbank on an ESXi host.

### Problem

Unused VIBs on the ESXi host might be relatively large in size and therefore use up significant disk space. The unused VIBs can result in insufficient space in the bootbank or in the alt-bootbank during upgrade.

### Solution

Uninstall the VIBs that are no longer required and free up additional disk space.

For more information on locating and deleting VIBs, see the VMware knowledge base article at https://kb.vmware.com/s/article/74864

# Failed Upgrade Host Placed in Maintenance Mode

Host unit fails during the upgrade process and the upgrade coordinator places this host in maintenance mode.

**Problem**

Failed host during upgrade is placed in the maintenance mode.

**Solution**

1   Manually troubleshoot and fix the problem on the host.

2   From the NSX Manager UI, select **System > Fabric > Nodes > Host Transport Nodes**.

3   Locate the host that you fixed and select it.

    The status of the host is maintenance mode.

4   Select **Actions > Exit Maintenance Mode**.

# Failure to Upload the Upgrade Bundle

The upgrade bundle fails to upload because of insufficient disk space.

**Solution**

1   In the NSX Manager CLI, delete the unused files located at `/image/vmware/nsx/file-store/*` and `/image/core/*`.

    ---

    **Note**  Ensure that you do not delete the `/image/upgrade-coordinator-tomcat` folder or other folders located at `/image`.

    ---

2   From your browser, log in as a local admin user to an NSX Manager at https://*nsx-manager-ip-address/login.jsp?local=true*.

3   Select **System > Support Bundle** and delete any unused support bundles.

4   Reupload the upgrade bundle and continue with the upgrade process.

# Backup and Restore During Upgrade

The Management Plane stops responding during the upgrade process and you need to restore a backup that was taken while the upgrade was in progress.

**Problem**

The Upgrade Coordinator has been upgraded and the Management Plane stops responding. You have a backup that was created while the upgrade was in progress.

Solution

**1** Deploy your Management Plane node with the same IP address that the backup was created from.

**2** Upload the upgrade bundle that you used at the beginning of the upgrade process.

**3** Upgrade the Upgrade Coordinator.

**4** Restore the backup taking during the upgrade process.

**5** Upload a new upgrade bundle if necessary.

**6** Continue with the upgrade process.

# Loss of Controller Connectivity after Host Upgrade

Controller connectivity is lost after you upgrade your hosts.

Problem

After upgrading your host, when running post checks, your **Node Status** shows loss of connectivity to the controller.

Solution

**1** Open an SSH session to the EXSi host experiencing the issue and confirm that none of the three NSX controllers are in a connected state. Run the `nsxcli -c get controllers` command.

Example response:

```
Controller IP    Port  SSL     Status       Is Physical Master   Session State
Controller FQDN
192.168.60.5    1235  enabled  disconnected  true                 down
nsxmgr.corp.com
```

In a working configuration, two controllers display the not used status and one controller has the connected status. If the NSX controller shows connected, refresh the UI and confirm that the status is green. If the controller shows not connected, continue to the next step.

**2** Open an SSH session to one of the NSX Manager nodes as admin and run the `get certificate api thumbprint` command.

The command output is a string of alphanumeric numbers that is unique to this NSX Manager.

**3** On the ESXi host, push the host certificate to the Management Plane:

```
ESXi1> nsxcli -c push host-certificate <NSX Manager IP or FQDN> username admin thumbprint
<thumbprint obtained in step #1>
```

When prompted, enter the admin user password for the NSX Manager. See the NSX-T Data Center *Command-Line Interface Reference* for more information.

**4**   Confirm the controller status is connected.

```
ESXi1> nsxcli -c get controllers
```

Confirm the controller connection state is green on the UI for this Transport Node.

If this issue continues, restart the following NSX services on the ESXi host:

```
ESXi1> /etc/init.d/nsx-opsagent restart
```

```
ESXi1> /etc/init.d/nsx-proxy restart
```

# In-place Upgrade Fails

If an in-place upgrade fails for an ESXi 7.0 host, except when you see a PSOD, vMotion the VMs out of the host and then reboot the host.

### Solution

**1**   Log in to vCenter Server and place the host in maintenance mode.

**2**   For an ESXi 7.0 host, use the following command to clear the upgrade status flag on the host:

```
nsxcli -c set host-switch upgrade-status false
```

**3**   vMotion the VM's out of the host.

**4**   Reboot the host and resume the upgrade process.

# Purple diagnostic screen when Upgrading from NSX-T Data Center 2.5.2

You may see the purple diagnostic screen(PSoD) when upgrading from NSX-T Data Center 2.5.2.

### Problem

When you run in-place upgrade from NSX-T Data Center 2.5.2, the purple diagnostic screen is displayed.

### Cause

In-place upgrade from NSX-T Data Center 2.5.2 fails if any of the following features are enabled on the NSX-T Data Center host switch of the ESXi host:

- LACP-based teaming is enabled for uplinks.

- MAC learning is enabled on one or more logical ports.

- NetQueue is enabled on one or more pNICs.

### Solution

- Use the maintenance mode when upgrading from NSX-T Data Center 2.5.2.

■ Disable MAC learning on all the logical ports and logical switches of the host switch.

■ Disable NetQueue on all the pNICs of the host switch prior to upgrade. You can then enable NetQueue after upgrade. For more information on disabling NetQueue, see *VMware vSphere Documentation*.

# Upgrading your NSX Federation Deployment 7

Upgrade the Global Manager before upgrading the Local Managers.

Upgrade the Global Manager first. Each Local Manager that is upgraded to the same version as the Global Manager resumes synchronization with the Global Manager. Local Manager appliances not upgraded to the same version as that of the Global Manager, remain disconnected from the Global Manager until they are upgraded.

The Global Manager and Local Manager must be at the same version. If the versions do not match, the Global Manager does not synchronize with the Local Manager. The versions of the Local Manager appliances must also be the same or the communication between Local Manager appliances stops. For example,

| Global Manager version | Local Manager at location 1 (LM1) version | Local Manager at location 2 (LM2) version | Can NSX Federation appliances communicate? |
|---|---|---|---|
| 3.0.0 | 3.0.0 | 3.0.0 | Yes |
| 3.0.0 | 3.0.1 | 3.0.0 | No |
| 3.0.1 | 3.0.0 | 3.0.1 | Supported for Global Manager and LM2. |
| 3.0.1 | 3.0.1 | 3.0.1 | Yes |
| 3.0.1 | 3.0.1 | 3.0.2 | Supported for Global Manager and LM1. |
| 3.0.2 | 3.0.1 | 3.0.2 | Supported for Global Manager and LM2. |
| 3.0.2 | 3.0.2 | 3.0.2 | Yes |

Table 7-1. Upgrading your NSX Federation Deployment

| Task | Instructions |
|---|---|
| Review the upgrade checklist before you begin. | Chapter 1 NSX-T Data Center Upgrade Checklist |
| Upgrade the Global Manager appliance. | 1  Upgrade the Upgrade Coordinator. <br> 2  Upgrade Management Plane. |
| Upgrade each Local Manager. | Chapter 3 Upgrading NSX-T Data Center. |