NSX-T Data Center Upgrade Guide

Modified on 02 FEB 2021
VMware NSX-T Data Center 2.4

vmware®

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

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.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 NSX-T Data Center 2.3 to NSX-T Data Center 2.4. 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.

NSX-T Data Center Upgrade Checklist

1

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

Warning You must follow the prescribed order and upgrade the hosts, NSX Edge cluster, NSX Controller cluster, and Management plane.

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.
☐ 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 Upgrading NSX Cloud Components from NSX-T Data Center 2.4 to 2.4.x
☐ Upgrade your upgrade coordinator.	See Upgrade the Upgrade Coordinator.
☐ Upgrade the hosts.	See Configuring and Upgrading Hosts .
☐ Upgrade the NSX Edge cluster.	See Upgrade NSX Edge Cluster.
☐ Upgrade the NSX Controller cluster.	See Upgrade NSX Controller Cluster.
☐ Upgrade the Management plane.	See Upgrade Management Plane from 2.3.x to NSX-T Data Center 2.4.x.
☐ Post-upgrade tasks.	See Verify the Upgrade.
☐ Troubleshoot upgrade errors.	See Chapter 6 Troubleshooting Upgrade Failures.

Preparing to Upgrade NSX-T Data Center

2

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 the host and upgrade the other NSX-T Data Center components later.

This chapter includes the following topics:

- Operational Impact of the NSX-T Data Center Upgrade
- Supported Hypervisor Upgrade Path
- Upgrading Your Host
- 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, such as when some hosts have been upgraded, or when NSX Edge nodes have not been upgraded.

The upgrade process is as follows:

Hosts > NSX Edge cluster > Management plane.

Check NSX-T Data Center Components

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

Before you upgrade, you must verify that your existing NSX-T Data Center 2.3 NSX Manager meets the vCPU and RAM limits in the vSphere Client and make necessary changes.

NSX-T Data Center 2.3 Appliance	Memory	vCPU	NSX-T Data Center 2.4 Appliance	Memory	vCPU
N/A	N/A	N/A	NSX Manager Extra Small VM	8 GB	2
NSX Manager Small VM	8 GB	2	NSX Manager Small VM	16 GB	4
NSX Manager Medium VM	16 GB	4	NSX Manager Medium VM	24 GB	6
NSX Manager Large VM	35 GB	8	NSX Manager Large VM	48 GB	12

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. 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 hosts 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. ■ 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. ■ Upgraded hosts are compatible with non-upgraded hosts, NSX Edge cluster and Management plane. ■ New features introduced in the upgrade are not configurable until the NSX Edge cluster and Management plane are upgraded. ■ 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 NSX-T Data Center, 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 50 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) or iSCSI storage is configured on the host N-VDS switch.

■ VMkernel interface is configured on the overlay network.

NSX Edge Cluster Upgrade

During Upgrade	After Upgrade

■ During the NSX Edge upgrade, you might experience the following traffic interruption:
   ■ North-south datapath is affected if the NSX Edge is part of the datapath.
   ■ East-west traffic between tier-1 routers using NSX Edge firewall, NAT, or load balancing.
   ■ Temporary Layer 2 and Layer 3 interruption.
 ■ Configuration changes are not blocked on NSX Manager but might be delayed.
	■ Configuration changes are allowed.
	 ■ Upgraded NSX Edge cluster is compatible with the upgraded hosts and older versions of the Management plane.
	 ■ New features introduced in the upgrade are not configurable until the Management plane is upgraded.

NSX Controller Cluster Upgrade

Note In the NSX-T Data Center 2.4 release, the NSX Controller is merged with the NSX Manager during upgrade.

Management Plane Upgrade

Note Before you configure your NSX-T Data Center 2.3 NSX Manager for upgrade, you must backup the NSX Manager. See the *NSX-T Data Center Administration Guide*.

During Upgrade	After Upgrade
■ Configuration changes are not blocked on the Management plane. Do not to make any changes during the Management plane upgrade. ■ API service is available. ■ User interface is unavailable for a short period.	■ Configuration changes are allowed. ■ New features introduced in the upgrade are configurable.

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 2.4	NSX-T Data Center 2.3	NSX-T Data Center 2.2	NSX-T Data Center 2.1
Supported vSphere Hypervisor (ESXi)	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 16.04.2 LTS with Kernel version 4.4.0.x	Ubuntu 16.04.2 LTS with Kernel version 4.4.0.x	Ubuntu 16.04.2 LTS with Kernel version 4.4.0.x
RHEL 7.5 and RHEL 7.4	RHEL 7.5 and RHEL 7.4	RHEL 7.4	RHEL 7.4 and RHEL 7.3
CentOS 7.5 and CentOS 7.4	CentOS 7.4		
SLES 12 sp3			

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

- NSX-T Data Center 2.3 > NSX-T Data Center 2.4.

- NSX-T Data Center 2.2 > NSX-T Data Center 2.3 > NSX-T Data Center 2.4.

- NSX-T Data Center 2.1 > NSX-T Data Center 2.3 > NSX-T Data Center 2.4.

Upgrading Your Host

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

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

For RHEL, CentOS, and Ubuntu 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

1 Place your ESXi host in maintenance mode.

2 Upgrade the ESXi host.

- Upgrade ESXi 6.5xx to ESXi 6.5 P03.

```
esxcli software profile update --depot <build_path> ESXi-6.5.0-XXXXXX-standard --allow-
downgrades --no-sig-check
```

- Upgrade ESXi 6.7xx to ESXi 6.7 EP 06.

```
esxcli software profile update --depot <build_path> --profile ESXi-6.7.0-XXXXXX-standard --
allow-downgrades --no-sig-check
```

- Upgrade ESXi 6.5xx to ESXi 6.7 EP 06.

```
esxcli software profile update --depot <build_path> --profile ESXi-6.7.0-XXXXXX-standard --
allow-downgrades --no-sig-check
```

Install the NSX-T Data Center 2.3 LCP bundle for ESXi 6.7.

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

4 Install the NSX kernel module.

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

5   Reboot the ESXi host.

    `reboot`

6   Move your ESXi host out of maintenance mode.

7   (Optional) Upgrade ESXi in an offline environment using esxcli.

    a   Download the depot file and copy the file to the server.

    b   Upgrade the ESXi host.

    `esxcli software profile update -d <path-to-depot-file> -p <build> -standard`
    `--allow-downgrades --no-sig-check`

8   (Optional) Upgrade ESXi in an offline environment using VUM.

    a   Import an installation ISO image into VUM repository.

    b   Create a baseline based on the imported image.

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
```

Procedure

1   Follow the instructions available on the Ubuntu web site to upgrade your host.

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.

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.

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
```

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, fabric hosts, NSX Edge cluster, transport nodes, 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`

- `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 Cloud Components

<div style="text-align: right; font-size: 3em;">3</div>

NSX Cloud components need to be reinstalled if you are upgrading from versions 2.3 or earlier to versions 2.4 or later. If upgrading from versions 2.4 onwards, follow the upgrade workflow.

This chapter includes the following topics:

- Upgrading NSX Cloud from NSX-T Data Center 2.3 or earlier
- Upgrading NSX Cloud Components from NSX-T Data Center 2.4 to 2.4.x

Upgrading NSX Cloud from NSX-T Data Center 2.3 or earlier

If upgrading from NSX-T Data Center 2.3 or earlier to NSX-T Data Center 2.4 or later, you must uninstall NSX Cloud components and reinstall them.

Note If you are upgrading from NSX-T Data Center 2.4 onwards, follow instructions here: Upgrading NSX Cloud Components from NSX-T Data Center 2.4 to 2.4.x .

Uninstall and reinstall NSX Cloud components as described in the following checklist.

Table 3-1. Checklist to upgrade NSX Cloud components from NSX-T Data Center 2.3 or earlier to NSX-T Data Center 2.4 or later

Task	Instructions
❑ From your public cloud, uninstall the previous version's NSX Agent from all the workload VMs that have it running.	Follow instructions at NSX Agent Install Script Options and Uninstallation in the *NSX-T Data Center Administration Guide*.
❑ From your public cloud, remove the tag "nsx.network=default" from all the workload VMs that have the tag applied to them.	Find instructions on removing tags in your public cloud's documentation.
❑ From the previous version's deployment of CSM, undeploy all PCGs from all VPCs or VNets.	Follow instructions at Undeploy PCG in the *NSX-T Data Center Installation Guide*.
❑ Uninstall CSM	Shut down the CSM appliance and delete it from the disk.
❑ Upgrade NSX-T Data Center to 2.4.x.	Follow instructions here: Chapter 4 Upgrading NSX-T Data Center.
❑ Install CSM.	Follow instructions at Install CSM in the *NSX-T Data Center Installation Guide*.

Table 3-1. Checklist to upgrade NSX Cloud components from NSX-T Data Center 2.3 or earlier to NSX-T Data Center 2.4 or later (continued)

Task	Instructions
☐ Add one or more of your public cloud accounts in CSM.	Follow instructions at Add Your Public Account in the *NSX-T Data Center Installation Guide*.
☐ Deploy PCG in your Transit VPCs or VNets and link to your Compute VPCs or VNets.	Follow instructions at Deploy or Link PCGs in the *NSX-T Data Center Installation Guide*.
☐ Onboard workload VMs by tagging in your public cloud and installing the NSX Tools on them.	Follow instructions at Onboard Workload VMs in the *NSX-T Data Center Administration Guide*.

Upgrading NSX Cloud Components from NSX-T Data Center 2.4 to 2.4.x

NSX Cloud components are upgraded using the CSM Upgrade Coordinator.

The NSX Cloud Upgrade Workflow

First upgrade NSX Cloud components as follows. After that, upgrade NSX-T Data Center.

Note   Upgrading NSX Cloud components from NSX-T Data Center 2.3 or earlier to NSX-T Data Center 2.4 or later is not supported. If you are upgrading from NSX-T Data Center 2.3 or earlier, you must uninstall NSX Cloud components and reinstall them. See instructions in the topic: Upgrading NSX Cloud from NSX-T Data Center 2.3 or earlier

Procedure

1   Download the NSX Cloud Upgrade Bundle

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

2   Upgrade NSX Agents and PCG

Upload the upgrade bundle to proceed with upgrading NSX agents and PCG.

3   Upgrade CSM

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

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.

Upgrade NSX Agents and PCG

Upload the upgrade bundle to proceed with upgrading NSX agents and PCG.

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 agents 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**

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.

5   Click **Begin Upgrade**. The **Upgrade CSM** wizard starts.

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

6   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 agent and PCG are compatible for an upgrade via the upgrade bundle uploaded.

7   Click **Next**. The **CSM > Select NSX Agents** screen appears. A list of all compatible NSX agents that can be upgraded to the target version in all your VNets, are displayed. You can filter the agents based on which private cloud network they are in or which OS they are deployed on.

> **Note**   If there are any quarantined VMs, they are not included in the upgrade plan and you cannot upgrade them. Quarantined VMs do not have any connectivity with PCG and therefore not upgrading them does not affect the upgrade process.

8   Select the NSX Agents you want to upgrade and move them to the **Selected** window. Click **Next**. CSM downloads the upgrade bits to the PCG on which the NSX agents reside. If you have an HA pair of PCG, CSM downloads the upgrade bits to each PCG and starts upgrading the selected NSX agents.

Note: Agents in the same VPC/VNet are upgraded in parallel. 10 agents under a VPC/VNet are upgraded simultaneously. If you have more than 10 agents, 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.

Until all the agents are upgraded, you cannot upgrade PCG. If some agents are not able to be upgraded, you can skip upgrading them in order to proceed with upgrading PCG. See (Not recommended) Skip Upgrading NSX Agent(s) for details on this option.

9   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.

10   Click **Finish**.

Results

NSX Agents and PCGs are upgraded.

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.

- **NSX Agent installed on a workload VM**: It takes from 3 to 5 minutes for 1 NSX agent to upgrade, not accounting for the time it takes to upload the upgrade bundle from CSM to the public cloud. 10 agents are upgraded simultaneously. For multiple compute VPCs/VNets per Transit VPC/VNet, all agents installed on one Compute VPC/VNet are first upgraded before proceeding to the next. The time to upgrade agents also varies for different operating systems and the VM size.

- **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.

(Not recommended) Skip Upgrading NSX Agent(s)

You have the option to skip upgrading NSX agents, but this is not recommended.

You must upgrade NSX agents before upgrading PCG, but you have the option to skip upgrading NSX agents as a feature to continue with the workflow under certain conditions. We do not recommend skipping the upgrade of NSX agents because VMs with NSX agents in a different version compared to PCG will lose connectivity with the PCG.

Why you may consider skipping agent 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 may want to apply a bug-fix patch only to the PCG without affecting the agents.

If you do skip upgrading NSX agents, you cannot upgrade them later using the UI or APIs. This can potentially break connectivity between such NSX agents and the upgraded PCG. The only workaround for restoring connectivity in that case is to uninstall the old NSX agents and reinstall the latest NSX agents on those VMs.

Note If there are any quarantined VMs, they are not included in the upgrade plan and you cannot upgrade them. Quarantined VMs do not have any connectivity with PCG and therefore not upgrading them does not affect the upgrade process.

Upgrade CSM

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

Prerequisites

- You must have already completed upgrading NSX agents and PCGs.

- Make sure you have root privileges on CSM that are required for this task.

Procedure

1 Log in to CSM as `root` and copy the `VMware-NSX-unified-appliance-<version>.nub` file into this location: `/var/vmware/nsx/file-store/`.

```
$ssh root@<NSX CSM IP Address>
root@nsxcsm:~# cp /repository/<version>/CloudServiceManager/nub/VMware-NSX-unified-appliance-
<version>.nub /var/vmware/nsx/file-store/
```

Note When you upload the NSX Cloud master upgrade bundle (`.mub`) file into CSM as described in Upgrade NSX Agents and PCG, the file `VMware-NSX-unified-appliance-<version>.nub` is extracted into this location: `/repository/<version>/CloudServiceManager/nub/`.

You need to copy this file into the location: `/var/vmware/nsx/file-store/` to proceed with upgrading CSM.

2 Log in to the NSX CLI.

```
root@nsxcsm:~# nsxcli
```

3 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"
}
```

4 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!
```

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

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

```
nsxcsm> get version
```

7 If using a Microsoft Azure account in CSM, you must generate the MSI role names that are new in this release:

- Follow the steps in the topic **Enable CSM to access your Microsoft Azure inventory** in the *NSX-T Data Center Administration Guide* . You must do this when upgrading in order to generate MSI roles for CSM and PCG, and the NSX Cloud Service Principal.

- Log in to CSM and go to **Clouds > Accounts > Azure > Actions > Edit Account** and add the **Gateway Role Name**. The default name is `nsx-pcg-role`.

What to do next

Follow the steps here for Chapter 4 Upgrading NSX-T Data Center.

Upgrading NSX-T Data Center

4

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, NSX Controller 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, NSX Controller cluster, and Management plane.

2 Configuring and Upgrading Hosts

You can upgrade your hosts using the upgrade coordinator.

3 Upgrade NSX Edge Cluster

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.

4 Upgrade NSX Controller Cluster

In the NSX-T Data Center 2.4 release, the NSX Controller is merged with the NSX Manager during upgrade.

5 Upgrading Management Plane

The upgrade sequence upgrades the Management plane at the end.

6 Upgrade Policy Manager

In the NSX-T Data Center 2.4 release, the NSX Policy Manager is merged with the NSX Manager. To use the policies that you defined in NSX Policy Manager 2.3, migrate your policies to NSX-T Data Center 2.4.

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, NSX Controller 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
```

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

For NSX-T Data Center 2.4 > NSX-T Data Center 2.4.x upgrade:

- `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.

- 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 with admin privileges to an NSX Manager at https://*nsx-manager-ip-address*.

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

The existing NSX-T Data Center release version and components are listed.

  a Identify a component such as, Host or Edge.

  b Click the number listed under the Count column.

  A list of all the configured hosts or NSX Edge nodes appear in the dialog box.

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   Scroll to the bottom of the EULA 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 pre-check details for every component with the API call `GET https://<nsx-manager>/api/v1/upgrade/upgrade-checks-info`.

13 Resolve the red warning notification to avoid problems during the upgrade.

a   Click the Hosts notification to see the warning details.

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

b   Click the Edges notification to see the warning details.

You might have to resolve connectivity problems.

c   Click the Management Nodes notification to see the warning details.

You might have to increase the NSX Manager CPU and RAM limits in the vSphere Client.

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.

Results

The hosts are ready to be upgraded and the planned upgrade sequence appears. See Configure Hosts.

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 hosts 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.
	By default, the upgrade pauses when all the hosts are upgraded. After you review the upgrade result, you can proceed to upgrade the next host upgrade unit group or the NSX Edge cluster.

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.

- For upgrade from an NSX-T Data Center 2.4 version to an NSX-T Data Center 2.4.x version, 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 any ESXi host after uploading the latest upgrade bundle, you must click **Reset** so that you can upgrade the recently added ESXi host.

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 hosts 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 hosts 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 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 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 upgraded 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 NSX Edge Cluster.

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 rhel74_x86_64 or xenial_amd64.

    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/2.3.0.0.0.9999999/
        HostComponents/rhel74_x86_64/nsx-lcp-2.3.0.0.0.9999999-rhel74_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 Ubuntu hosts.

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

    ▪   For Ubuntu hosts, enter `dpkg —l | grep nsx`.

■ For 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 upgraded 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 > Overview** 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 NSX Edge Cluster.

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

Upgrade NSX Edge Cluster

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.

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

Prerequisites

■ Verify that the hosts are upgraded successfully. See Upgrade Hosts.

- 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 NSX Edge Cluster 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. By default, the upgrade pauses when the NSX Edge cluster is updated. After you review the upgrade result, you can proceed to upgrade the next Edge upgrade unit group.

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 Upgrade NSX Controller Cluster.

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

Upgrade NSX Controller Cluster

In the NSX-T Data Center 2.4 release, the NSX Controller is merged with the NSX Manager during upgrade.

> **Important**   During the management plane upgrade, the NSX Controller cluster data and services are migrated to the NSX Manager.

What to do next

Proceed with the upgrade. See Upgrade Management Plane from 2.3.x to NSX-T Data Center 2.4.x.

Upgrading Management Plane

The upgrade sequence upgrades the Management plane at the end.

After you upgrade the Management plane, you can join the Customer Experience Improvement Program (CEIP) for NSX-T Data Center. See Customer Experience Improvement Program in the NSX-T Data Center Administration Guide for more information, including how to join or leave the program.

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

Upgrade Management Plane from 2.3.x to NSX-T Data Center 2.4.x

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 accessible. 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.

Procedure

1   Backup the NSX Manager.

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

2   When upgrading to NSX-T Data Center 2.4, in the vSphere Client, verify that your NSX-T Data Center 2.3 NSX Manager meets the vCPU and RAM limits and make necessary changes.

NSX-T Data Center 2.3 Appliance	Memory	vCPU	NSX-T Data Center 2.4 Appliance	Memory	vCPU
N/A	N/A	N/A	NSX Manager Extra Small VM	8 GB	2
NSX Manager Small VM	8 GB	2	NSX Manager Small VM	16 GB	4
NSX Manager Medium VM	16 GB	4	NSX Manager Medium VM	24 GB	6
NSX Manager Large VM	35 GB	8	NSX Manager Large VM	48 GB	12

3   Select a Management plane upgrade plan.

- You can allow a transport node connection to a single NSX Controller node after upgrade.

- You can block the transport node connection to the NSX Controller until a three-node NSX Manager cluster is created.

    The transport node status is degraded because the connection between the transport node and the NSX Controller is blocked.

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

5 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 the reboot finishes and the services are reestablished.

6 In the CLI, log in to the NSX Manager to verify that the services have started.

```
get service
```

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

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

7 In the web browser, click **Reload** to refresh the browser.

8 From your browser, log in with admin privileges to an NSX Manager at https://*nsx-manager-ip-address*.

9 (Optional) Depending on the upgrade plan, allow the host connection to the single NSX Controller node.

10 (Optional) Click the Help icon in the top right corner.

11 (Optional) Select **About** to verify that the product version is updated.

12 For NSX-T Data Center 2.3.x > NSX-T Data Center 2.4.x upgrade, complete the following tasks.

    a Select **System > Overview** and deploy two NSX Manager nodes to form a cluster.

       The newly deployed nodes continue to use pre-upgrade passwords. It is recommended that you change your passwords to match the password complexity recommendations for NSX-T Data Center 2.4.

       See instructions on how to deploy NSX Manager and create a cluster in the *NSX-T Data Center Installation Guide*.

    b Select **System > Overview** and verify that the repository synchronization for the cluster is complete.

    c Log in with admin privileges to the newly deployed NSX Manager node.

d   Verify that the cluster status is UP and Stable.

```
get cluster status
```

e   For a VMware Integrated OpenStack deployment, add the node IP addresses to the `nsx.ini` file.

```
/etc/neutron/plugins/vmware/nsx.ini
```

Restart the Neutron service.

```
sudo systemctl restart devstack@q-svc.service
```

13 For NSX-T Data Center 2.2.x > NSX-T Data Center 2.3.x > NSX-T Data Center 2.4.x upgrade, complete the following tasks.

a   Select **System > Overview** and deploy three NSX Manager nodes to form a cluster.

The newly deployed nodes continue to use pre-upgrade passwords. It is recommended that you change your passwords to match the password complexity recommendations for NSX-T Data Center 2.4.

See instructions on how to deploy NSX Manager and create a cluster in the *NSX-T Data Center Installation Guide*.

b   Select **System > Overview** and verify that the repository synchronization for the cluster is complete.

c   Log in with admin privileges to the newly deployed NSX Manager node.

d   Verify that the cluster status is UP and Stable.

```
get cluster status
```

e   Detach the upgraded NSX Manager node from the cluster using the command, `detach node <upgraded-node-uuid>`.

f   Set the newly deployed NSX Manager node as the upgrade-coordinator orchestrator using the command, `set repository-ip`.

Important   You must implement this step so that the newly deployed node functions properly.

---

g   Power off and delete the detached NSX Manager node.

Note   The detached node is no longer part of NSX-T Data Center.

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.

Upgrade Management Plane from 2.4 to NSX-T Data Center 2.4.x

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 accessible. 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.

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.

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*.

Upgrade Policy Manager

In the NSX-T Data Center 2.4 release, the NSX Policy Manager is merged with the NSX Manager. To use the policies that you defined in NSX Policy Manager 2.3, migrate your policies to NSX-T Data Center 2.4.

Prerequisites

Verify that the NSX Management Plane is upgraded successfully. See Upgrade Management Plane from 2.3.x to NSX-T Data Center 2.4.x.

Note This procedure applies only to upgrade from NSX Policy Manager 2.3.

Procedure

1 Upgrade the NSX Policy Manager appliance.

   a   Locate the nub for upgrade.

```
http://<NSX_Manager_IP>:8080/repository/
<Target_Upgrade_BUILD_Number_of_NSX_T>/Manager/nub/VMware-NSX-unified-
appliance-<TO_BUILD_Number_of_NSX_Unified_Appliance>.nub
```

   To find `TO_BUILD_Number_of_NSX_Unified_Appliance`, run `get version` from the command line for the NSX manager.

   b   Copy the nub to the NSX Policy Manager appliance.

```
copy url <url_to_upgrade_nub>
```

   c   Verify the upgrade bundle.

```
verify upgrade-bundle <BUNDLE_NAME>
```

   d   Start the upgrade using the Policy Playbook.

   start upgrade-bundle <BUNDLE_NAME> playbook <POLICY_PLAYBOOK_NAME>

   Verify the appliance upgrade status in the `/var/log/resume-upgrade.log` file, after reboot.

2 Create a backup copy of the upgraded NSX Policy Manager.

   a   Use an API call to configure the backup process.

```
PUT https://<policy-mgr>/policy/api/v1/cluster/backups/config
```

   See the *Configure backup* section of the *NSX-T Data Center API Guide*.

   a   Use an API call to initiate the backup process.

```
POST https://<policy-mgr>/policy/api/v1/cluster?action=backup_to_remote
```

   See the *Request one-time backup* section of the *NSX-T Data Center API Guide*.

In the NSX-T Data Center 2.4 release, the NSX Policy Manager is merged with the NSX Manager.

3   Restore your policy data to the upgraded NSX Manager.

See the *Restore a Backup* section of the *NSX-T Data Center Administration Guide*.

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
- Delete NSX Controllers

Verify the Upgrade

After you upgrade NSX-T Data Center, you can verify whether the versions of the upgraded components have been updated.

If you are upgrading from NSX-T Data Center 2.3 or earlier, your networking configuration is found under the **Advanced Networking & Security** and **System** tabs. You should continue to manage your environment using these tabs. See "Overview of the NSX Manager" in the *NSX-T Data Center Administration Guide* for more information.

Prerequisites

Perform a successful upgrade. See Chapter 4 Upgrading NSX-T Data Center.

Procedure

1 From your browser, log in with admin privileges to an NSX Manager at https://*nsx-manager-ip-address*.

2 Select **System > Upgrade**.

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

   The status of the upgrade appears as Successful.

4 (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.

5 (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

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

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

8 If you did not use NSX Policy Manager 2.3 to create your DFW rules, move your rules to the upgraded NSX Manager.

   a Navigate to the **Security** tab and recreate your rules.

     Your pre-upgrade configuration is available under

     Advanced Networking & Security > Security > Distributed Firewall

     .

   b Navigate to **Advanced Networking & Security > Security > Distributed Firewall** and delete your pre-upgrade rules.

   c Delete the `infra_EC_to_FL_Connectivity_Strategy` constraint to reset connectivity strategy.

     The connectivity strategy is set to NONE after the upgrade. To reset connectivity strategy, use an API call to delete the `infra_EC_to_FL_Connectivity_Strategy` constraint.

     `DELETE https://<policy-mgr>/policy/api/v1/infra/constraints/<constraint-id>`

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

Delete NSX Controllers

After successfully upgrading to NSX-T Data Center 2.4, you can delete the NSX-T Data Center 2.3 NSX Controllers.

Note Delete only the NSX-T Data Center 2.3 NSX Controllers.

Prerequisites

Make sure that the upgrade is successful. See Chapter 4 Upgrading NSX-T Data Center.

Procedure

1 For vSphere Client, complete the following tasks.

    a Locate and power off the NSX Controllers.

    b Right-click and select **Delete from Disk**.

2 For KVM, complete the following tasks.

    a Run the `virsh list` command.

    b Power off the NSX Controllers.

```
virsh shutdown <nsx-controller-name>
```

    c Delete the NSX Controllers.

```
virsh destroy <nsx-controller-name>
```

Troubleshooting Upgrade Failures

<div style="text-align: right">6</div>

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
- Failed Upgrade Host Placed in Maintenance Mode

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 with admin privileges to an NSX Manager at https://<nsx-manager-ip-address>.

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 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 server was not set.

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 > Overview** 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.

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**.