NSX Upgrade Guide

Modified on 07 MAY 2024

VMware NSX 4.1

vmware by Broadcom

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

https://docs.vmware.com/

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

Contents

Upgrading NSX

The *NSX Upgrade Guide* provides step-by-step information about upgrading the NSX 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 4.1. 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 https://www.vmware.com/topics/glossary.

Related Documentation

You can find the VMware NSX® Intelligence™ documentation at https://docs.vmware.com/en/VMware-NSX-Intelligence/index.html.

NSX Upgrade Checklist

1

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

Table 1-1. Upgrade NSX

Task	Instructions
Review the known upgrade problems and workaround documented in the NSX release notes.	See the *NSX Release Notes*.
Follow the system configuration requirements and prepare your infrastructure.	See the system requirements section of the *NSX Installation Guide*.
Evaluate the operational impact of the upgrade.	See Operational Impact of the NSX Upgrade.
Upgrade your supported hypervisor.	See Upgrading Your Host OS.
If you have an earlier version of NSX Intelligence installed, upgrade NSX Intelligence first.	See *Activating and Upgrading VMware NSX Intelligence* for version 3.2 or later at https://docs.vmware.com/en/VMware-NSX-Intelligence/index.html.
Complete the Pre-Upgrade Tasks.	See Pre-Upgrade Tasks.
Verify that the NSX environment is in a healthy state.	See Verify the Current State of NSX .
Download the latest NSX upgrade bundle.	See Download the NSX 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. Complete this task at least one week in advance of the maintenance window to allow time to address issues identified by the upgrade pre-checks.	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 Upgrading Management Plane.
Post-upgrade tasks.	See Verify the Upgrade.
Troubleshoot upgrade errors.	See Chapter 6 Troubleshooting Upgrade Failures.

Preparing to Upgrade NSX

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 one of the components and upgrade the other NSX components later, during another maintenance time frame.

Run the upgrade pre-checks at least one week in advance of the planned upgrade maintenance window. Running the pre-checks in advance allows you sufficient time to address and resolve issues identified by the pre-checks.

Upgrade Order

Starting NSX 4.0.1.1, you have the flexibility to change the order of upgrade for your edge clusters and hosts. You can alternate between groups of hosts and groups of edge nodes during upgrade.

For instance, if you have two edge clusters and two host clusters, you can first upgrade one of the edge clusters followed by a host cluster and then complete upgrade for the remaining clusters in any order you prefer.

You can either upgrade a cluster of hosts at a time or a cluster of edges. Host and edge nodes cannot be upgraded in parallel. The NSX Manager is upgraded only after all the edges and hosts have been upgraded.

Read the following topics next:

- Operational Impact of the NSX Upgrade
- Supported Upgrade Paths
- Pre-Upgrade Tasks
- Upgrading Your Host OS
- Verify the Current State of NSX
- Download the NSX Upgrade Bundle

Operational Impact of the NSX Upgrade

The duration for the NSX 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 components during an upgrade.

The upgrade process is as follows:

NSX Edge cluster > Hosts > Management plane.

Starting NSX 4.0.1.1, you have the flexibility to change the order of upgrade for your edge clusters and hosts. You can alternate between groups of hosts and groups of edge nodes during upgrade. The NSX Manager is upgraded only after all the edges and hosts have been upgraded.

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 older versions of the Management plane and the hosts. ■ New features introduced in the upgrade are not configurable until the Management plane is upgraded. ■ Run post checks to make sure that the upgraded NSX Edge cluster and NSX 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. For ESXi hosts that are part of a fully automated 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. ■ For ESXi host, for an in-place upgrade you do not need to power off the tenant VMs. ■ During an in-place upgrade: For VMs attached to an NSX logical switch or VMs connected to the distributed portgroup of a VDS prepared for NSX for vSphere, vmotion of VMs is not supported from and to the host on which an upgrade is in progress. Creating new VMs is also not supported on hosts on which an upgrade is in progress. ■ Configuration changes are allowed on NSX Manager. ■ You may experience brief disruption in traffic during in-place upgrade of the ESXi hosts. For critical applications that cannot handle packet loss, maintenance mode upgrade is recommended.	■ 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. ■ New features introduced in the upgrade are not configurable until the Management plane is upgraded. ■ Run post checks to make sure that the upgraded hosts and NSX do not have any problems.

Limitations on In-Place Upgrade

For ESXi hosts with version 7.0 and later, when upgrading from NSX 3.2 or later, in-place upgrade is not supported in the following scenarios:

- More than 1000 vNICs are configured on the ESXi host and the VM's vNICs connect to a single VDS. If the host has multiple VDS for NSX, this vNIC limit is per VDS.
- 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 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.
- IDS/IPS or distributed malware prevention is enabled for your NSX environment.

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 1000 vNICs are configured on the ESXi host and the VM's vNICs connect to a single VDS. If the host has multiple VDS for NSX, this vNIC limit is per VDS.
- ENS is configured on the host N-VDS switch.
- 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 Administration Guide* for information on uninstalling service insertion.
- A VProbe-based packet capture is in progress.
- IDS/IPS or distributed malware prevention is enabled for your NSX environment.

Management Plane Upgrade

During Upgrade	After Upgrade
When upgrading from NSX 3.2, or 3.2.0.1: ■ Do not make any configuration changes during the Management plane upgrade. ■ API service is momentarily unavailable. ■ User interface is unavailable for a short period.	■ Configuration changes are allowed. ■ New features introduced in the upgrade are configurable. ■ You need a valid license to use licensed features like T0, T1, Segments, and NSX intelligence. ■ From the Upgrade Coordinator, verify that the upgrade process has completed. Perform configuration tasks only after the upgrade process is complete.

Supported Upgrade Paths

The supported upgrade paths for the NSX product versions.

Adhere to the following upgrade paths for each NSX release version.

- NSX 3.2.x > NSX 4.1.x.
- NSX 4.0.x > NSX 4.1.x.

Note The following upgrade paths are not supported:

- Upgrade from NSX 3.2.2 to 4.0.1 or 4.0.1.1.
- Upgrade from NSX 3.2.3 to 4.1.0.0 or 4.1.0.1

The reason is that the General Availability (GA) of the targeted upgrade version happened before the GA of your current version of NSX. Some capabilities and important fixes might not be available in the targeted versions due to the chronological order in which the versions were released.

Table 2-1. Hypervisor Support

NSX 4.1, 4.0, 3.2: Supported vSphere Hypervisor (ESXi)

Table 2-2. Bare Metal Server Support

NSX 4.1	NSX 4.0	NSX 3.2
Ubuntu: 20.04, 18.04, 16.04	Ubuntu: 20.04, 18.04, 16.04	Ubuntu: 18.04, 16.04
RHEL: 8.4, 8.2, 7.9, 7.7, 7.6	RHEL: 8.4, 8.2, 7.9, 7.7, 7.6	RHEL: 8.3, 8.0, 7.9, 7.8, 7.7, 7.6
CentOS: 8.4, 8.2, 7.9, 7.7, 7.6	CentOS: 8.4, 8.2, 7.9, 7.7, 7.6	CentOS: 8.3, 8.0, 7.9, 7.8, 7.7, 7.6
SUSE Linux Enterprise Server (SLES): 12 sp5, 12 sp4, 12 sp3	SUSE Linux Enterprise Server (SLES): 12 sp5, 12 sp4, 12 sp3	SUSE Linux Enterprise Server (SLES): 12 sp4, 12 sp3
OEL: 7.9, 7.8, 7.7, 7.6	OEL: 7.9, 7.8, 7.7, 7.6	OEL: 7.9, 7.8, 7.7, 7.6
Windows Server: 2016, 2019	Windows Server: 2016, 2019	Windows Server: 2016, 2019

Pre-Upgrade Tasks

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

Procedure

1 NSX checks the upgrade readiness of your NSX Manager nodes as part of the upgrade pre-check. For more information on the readiness check, see the VMware knowledge base article at https://kb.vmware.com/s/article/87379.

2 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.

3 Ensure that you backup the NSX Manager before you start the upgrade process. See the *NSX Administration Guide*.

4 Ensure that your host OS is supported for NSX Manager. See *Supported Hosts for NSX Managers* in the *NSX Administration Guide*

5 Disable automatic backups before you start the upgrade process. See the *NSX Administration Guide* for more information on configuring backups.

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

7 Ensure that the appropriate communication ports are open from the Transport and Edge nodes to the NSX Manager nodes. For more information on ports, see https://ports.esp.vmware.com/home/NSX.

NSX Cloud Note NSX Cloud supports communication on port 80 between the Cloud Service Manager appliance installed on-premises with the NSX Public Cloud Gateway installed in your public cloud VPC/VNet.

8 You need a valid license to use licensed features like T0, T1, Segments, and NSX intelligence. Ensure that you have a valid license.

9 Delete all expired user accounts before you begin upgrade. Upgrade for NSX on vSphere fails if your exception list for vSphere lockdown mode includes expired user accounts. If your host is part of the vLCM-enabled cluster, several users such as lldp-vim-user, nsx-user, mux-user, and da-user, are created automatically and added to the exception users list on an ESXi host when NSX VIBS are installed. 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. For more details on these NSX user accounts on the ESXi host, refer to the KB article, https://kb.vmware.com/s/article/87795.

10 Ensure that you have the supported hardware version for your NSX Edge VMs. For more information, see https://kb.vmware.com/s/article/88934.

Upgrading Your Host OS

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

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

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 Upgrade Paths.
- Ensure that you have the supported version of VMware vCenter. See Product Interoperability Matrix.

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 Log in to VMware vCenter.

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

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

    d 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.

    e Export the image to ISO.

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

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

    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.
  - Perform the upgrade using a baseline group:

    a Log in to VMware vCenter.

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

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

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

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

   f 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.

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

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

- Starting NSX 3.1.1 and vSphere 7.0 update 1, for vSphere Lifecycle Manager-enabled clusters, you can upgrade your ESXi host along with NSX, using vSphere Lifecycle Manager.

   a Upload the ESXi host image to vSphere Lifecycle Manager depot.

   b Update the ESXi host version for the cluster image.

   c From the NSX Manager UI, select **Stage in vSphere Lifecycle Manager** when configuring the host upgrade. See Configure Hosts.

   d Follow the steps in Upgrade a vSphere Lifecycle Manager-enabled Cluster to complete the upgrade.

Verify the Current State of NSX

Before you begin the upgrade process, it is important to test the NSX 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 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 Upgrade Bundle

The upgrade bundle contains all the files to upgrade the NSX 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 Broadcom Support portal.

Procedure

1 Locate the NSX build on the Broadcom Support 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 upgrade bundle to the same system you are using to access the NSX Manager user interface.

Upgrading NSX

3

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

NSX Intelligence and NSX Application Platform Note For information about upgrading NSX Intelligence version 1.2.x and earlier to NSX Intelligence version 3.2 and later, see the *Activating and Upgrading VMware NSX Intelligence* documentation at https://docs.vmware.com/en/VMware-NSX-Intelligence/index.html.

For information about upgrading NSX Application Platform, see the *Deploying and Managing the VMware NSX Application Platform* documentation at https://docs.vmware.com/en/VMware-NSX/index.html.

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

Note Do not add or delete NSX Manager nodes during an upgrade.

You can use REST APIs to upgrade your NSX appliance. Identify the NSX version you are upgrading to. Refer to the API guide with your product version in developer.broadcom.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, the upgrade coordinator updates the NSX Edge cluster and hosts as per the order you select. The Management plane is upgraded at the end. 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 Upgrading Management Plane

The upgrade sequence upgrades the Management plane at the end.

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.

NSX Manager nodes are upgraded sequentially due to the rolling upgrade feature so that two nodes are up all the time. You can push new configurations while the NSX Manager upgrade is in progress.

Prerequisites

- Verify that the upgrade bundle is available. See Download the NSX Upgrade Bundle
- For upgrade from NSX 3.2, or 3.2.0.1, ensure that the NSX services are running and retrieve the IP address of the orchestrator node:

  ```
  get service install-upgrade
  ```

  See `Enabled on`. Use this IP address throughout the upgrade process.

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

  Note

  - When upgrading from NSX 3.2, or 3.2.0.1, ensure that you do not use any type of Virtual IP address or the FQDN to upgrade NSX and avoid any configuration changes from any of the nodes.
  - If in an NSX Federation environment, you are upgrading a Local Manager from the Global Manager and you have changed the orchestrator node of the Local Manager, this change takes some time to appear on the Global Manager UI.

Procedure

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

   - For upgrade from NSX 3.2, or 3.2.0.1, use the IP address of the orchestrator node.
   - For upgrade from NSX 3.2.1.x and later, log in as a local admin user to any one of the NSX manager nodes.

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

3 Click **Upgrade**.

4 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.

5 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 **Prepare for Upgrade** button appears.

6 Click **Prepare for Upgrade** to upgrade the upgrade coordinator.

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

The EULA appears.

7 Read and accept the EULA terms.

8 Accept the notification to upgrade the upgrade coordinator.

9 (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.

10 Click **Run Pre-Checks** to verify that all the NSX components are ready for upgrade.

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

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

When the upgrade coordinator displays a warning about a new pre-check upgrade bundle, download the latest bundle:

a Click **Pre-check Upgrade Bundle (.pub file)** to view the list of available bundles.

b Select the target version and click **Download** to initiate the download and installation of the bundle.

Note For an airgap environment, download the latest pre-check bundle from the Broadcom Support portal. Select **Upload Local File** or **Upload with Remote URL** to upload the new pre-check bundle on NSX.

c Continue to run the pre-checks with the latest bundle.

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

12 Acknowledge the issues as required and refresh your browser if needed.

13 Resolve issues detected from the pre-check.

   a In the **Edges** section, click the **Pre Check Status** issues to see the issue details.

   > **Important** If the allocated CPU cores or memory of the edge node is less than the standard edge node form factor, an alarm is generated to warn you. In this scenario, you must acknowledge this type of alarm to proceed with the edge upgrade which will result in the upgrade coordinator changing the edge CPU cores and memory to match the standard edge node form factor. After the upgrade, these type of alarms are cleared on the next edge transport node refresh action. For more details, see NSX Edge Node Upgrade Process by the Upgrade Coordinator.

   b In the **Hosts** section, click the **Pre Check Status** issues to see the issue details.

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

   c In the **NSX Manager** section, click the **Pre Check Status** issues to see the issue details.

   You can click **Download Pre-Check Results** to download a `CSV` file with details about pre-check errors for each component and their status.

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

   > **Note** If new NSX Manager nodes are added after the upgrade coordinator is upgraded, upload the upgrade bundle to the newly added nodes and upgrade the upgrade coordinator again.

Upgrade NSX Edge Cluster

After the upgrade coordinator has been upgraded, the upgrade coordinator updates the NSX Edge cluster and hosts as per the order you select. The Management plane is upgraded at the end. 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 twenty.

> **Note** Starting with VMware NSX® 4.0.1.1, NSX Edge virtual machine hardware will be upgraded to version vmx-20 during the edge upgrade for NSX edges that are managed by NSX 3.2 or higher and deployed on ESXi host version 8.0.

Prerequisites

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

  Any NSX Edge nodes that are not in an NSX Edge cluster are flagged during the upgrade coordinator pre-check and prevents the upgrade from proceeding.

- Familiarize yourself with the upgrade impact during and after the NSX Edge cluster upgrade. See Operational Impact of the NSX 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. **Note** The maximum limit of simultaneous upgrade of Edge upgrade unit groups is five.
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. **Note** The maximum limit of simultaneous upgrade of Edge upgrade unit groups is five.
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.

Note It is recommended to follow an order so that critical standby nodes are upgraded before active nodes. This order allows only one failover to occur during upgrade for critical nodes.

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**.

You can also do this with the following REST API. Reorder an upgrade unit within the upgrade unit group by placing it before/after the specified upgrade unit.

METHOD	POST
URI	`https://<nsx-mgr>/api/v1/upgrade/upgrade-unit-groups/<groupId>/upgrade-unit/<upgrade-unit-id>?action=reorder`
Payload	`{ "id": "<upgrad-uniti-id>", "is_before": "false" }`

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

Caution After reset, you cannot restore your previous configuration. Also, a reset causes the Edge upgrade unit group order to allow Edge nodes with standby logical routers to be upgraded first and followed by Edge nodes with active logical routers. This order reduces failovers.

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

5 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.

6 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.

7 (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.

NSX Edge Node Upgrade Process by the Upgrade Coordinator

The first component that the upgrade coordinator upgrades is the NSX Edge cluster nodes. Depending on how and when the NSX Edge nodes were deployed determines how they are upgraded.

Upgrade Process for Auto Deployed Edge Nodes

Note The upgrade process for auto deployed edge nodes applies when upgrading from NSX Data Center 3.2.x to NSX Data Center 4.0 and later.

This upgrade process does not work when upgrading from NSX Data Center 3.1.x to NSX Data Center 4.0 and later.

For auto deployed edge nodes managed by NSX Manager, the upgrade coordinator checks the edge node configuration settings and updates them if the settings do not match the standard values from the current NSX Data Center version.

When a NSX Data Center version introduces an improvement to the NSX Edge node configuration, that improvement only applies to NSX Edge nodes deployed after the upgrade. NSX Edge nodes deployed prior to the NSX Data Center upgrade are not automatically updated. You can use the upgrade coordinator to update auto deployed NSX Edge nodes to the latest configuration settings.

The upgrade workflow for auto deployed edge nodes is as follows:

1 The upgrade bundle file is uploaded and prepared by the upgrade coordinator.

2 The edge node is placed into maintenance mode.

3 The OS is downloaded to the edge node.

4 The OS is installed on the edge node.

5 The OS switch is performed on the edge node.

6 Using vSphere APIs, the edge node virtual machine is powered off.

   Note VMware vCenter should be running and reachable during this workflow.

7 Upgrade coordinator updates the edge node virtual machine configuration parameters and the allocation of CPU cores and memory.

   The following NSX Edge virtual machine configuration attributes are added or updated before powering on an edge virtual machine in the operating system:

   - `VMX` file properties:

```
    "ethernet0.ctxPerDev":"3",
    "ethernet1.ctxPerDev":"3",
    "ethernet2.ctxPerDev":"3",
    "ethernet3.ctxPerDev":"3",
    "ethernet4.ctxPerDev":"3",
    "ethernet0.udpRSS":"1",
    "ethernet1.udpRSS":"1",
    "ethernet2.udpRSS":"1",
    "ethernet3.udpRSS":"1",
    "ethernet4.udpRSS":"1",
    "ethernet0.pnicFeatures":"4",
    "ethernet1.pnicFeatures":"4",
    "ethernet2.pnicFeatures":"4",
    "ethernet3.pnicFeatures":"4",
    "ethernet4.pnicFeatures":"4",
    "featMask.vm.cpuid.PDPE1GB":"Val:1",
    "snapshot.maxSnapshots":"0"
```

- `OVF` file property:

  ```
  "memoryReservationLockedToMax":"true"
  ```

- CPU
- Memory

For the allocation of CPU cores, memory, and storage, the upgrade coordinator changes the edge node values to match the standard form factor values.

Note The edge node CPU core and memory values are only changed to match the form factor values if the existing edge node values are less than the form factor values. If the edge node values are greater than the form factor values, then no changes are made. Ensure that there are sufficient resources in the vSphere resource pool and cluster.

Table 3-1. Supported NSX Edge Form Factors for Upgrade

NSX Edge Form Factor	Memory	CPU Cores	Disk Space
Small Form Factor	4 GB	2	200 GB
Medium Form Factor	8 GB	4	200 GB
Large Form Factor	32 GB	8	200 GB
Extra Large Form	64 GB	16	200 GB

8 The edge node virtual machine is powered on.

9 Check for required reboot if there is a GRUB update, and if required, the OS is rebooted into the updated GRUB.

10 Upgrade coordinator verifies edge node version.

11 Users from the old OS are migrated to the edge node.

12 The edge node exits maintenance mode.

13 The upgrade process is completed and the edge node upgrade is marked as successful.

Upgrade Process for Manually Deployed Edge Nodes and Bare Metal Edge Nodes

For manually deployed edge nodes and bare metal edge nodes, the upgrade coordinator only updates the OS and does not change the edge parameters or CPU core and memory values.

The upgrade workflow for manually deployed edge nodes and bare metal edge nodes is as follows:

1 The upgrade bundle file is uploaded and prepared by the upgrade coordinator.
2 The edge node is placed into maintenance mode.
3 The OS is downloaded to the edge node.
4 The OS is installed on the edge node.
5 The OS switch is performed on the edge node.
6 The edge node reboots into the new OS.
7 Upgrade coordinator verifies edge node version.
8 The edge node exits maintenance mode.

Important Before upgrading manually deployed edge nodes, it is important to set the `VMX` file property `"featMask.vm.cpuid.PDPE1GB":"Val:1"` of the edge node virtual machine in order to prevent upgrade failure.

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, VMware vCenter managed ESXi 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 twenty host upgrade unit groups and five hosts per group.

Note Host upgrade unit group with hosts that belong to the same VMware vCenter 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.

Prerequisites

- If the ESXi hosts are part of a disabled DRS cluster or are standalone hosts, verify that they are placed in maintenance mode.

For ESXi hosts that are part of a fully automated 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.
- 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 ESXi hosts that are part of a fully automated 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.

   - 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 ESXi hosts that are part of a fully automated 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 VMware vCenter 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 VMware vCenter 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 VMware vCenter 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 VMware vCenter 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 API Guide*.

6 For vSphere Lifecycle Manager-enabled clusters, select one of the following options:

   - **NSX only Upgrade**: Use this option if you want to upgrade only NSX. The Upgrade Coordinator runs the entire upgrade process including the remediation of hosts.
   - **Stage in vSphere Lifecycle Manager**: Use this option if you want to upgrade NSX along with ESXi hosts and other solutions. You need to remediate the hosts using vSphere Lifecycle Manager. After remediation, you can monitor the upgrade from the Upgrade Coordinator.

7 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.
- If the ESXi hosts are part of a disabled DRS cluster or are standalone hosts, verify that they are placed in maintenance mode.

  For ESXi hosts that are part of a fully automated 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.

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.
- If the ESXi hosts are part of a disabled DRS cluster or are standalone hosts, verify that they are placed in maintenance mode.

  For ESXi hosts that are part of a fully automated 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 stateless ESXi host, log in VMware vCenter and update the ESXi image with the NSX kernel modules.

Procedure

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

  For vSphere Lifecycle Manager-enabled clusters, see Upgrade a vSphere Lifecycle Manager-enabled Cluster.

2 Click **Refresh** and 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 do not have any problems.

  Note If a host upgrade unit failed to upgrade and you removed the host from NSX, 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 packages is installed on the vSphere hosts and bare metal servers.

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

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 VMware vCenter 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 Upgrading Management Plane.

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

Upgrade a vSphere Lifecycle Manager-enabled Cluster

You can upgrade clusters that have vSphere Lifecycle Manager enabled.

Prerequisites

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

Procedure

1 For clusters set up as **Stage in vSphere Lifecycle Manager**, click **Stage** to copy the NSX vibs to vSphere Lifecycle Manager and to update the cluster with the new NSX image. Also stage the vibs for the solutions that you are upgrading along with NSX.

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

3 For clusters set up as **Stage in vSphere Lifecycle Manager**, log in the vCenter Server and remediate the hosts.

   For clusters set up as **NSX only Upgrade**, the Upgrade Coordinator performs the entire upgrade process including the remediation of hosts.

   Note While upgrading a DPU-backed ESXi host, the host reboots as part of host remediation.

   If the host fails to be placed in maintenance mode, you will need to manually power off all VMs and then retry the host upgrade.

4 Click **Refresh** and monitor the upgrade process from NSX Manager.

   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.

5 Click **Run Post Checks** to make sure that the upgraded hosts and NSX do not have any problems.

   Note If a host upgrade unit failed to upgrade and you removed the host from NSX, 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.

6 After the upgrade is successful, verify that the latest version of NSX packages is installed.

```
esxcli software vib list | grep nsx
```

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 Upgrading 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 Click **Stage** and proceed after staging is complete.

3 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-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>.
   ```

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

   All the manually upgraded hosts appear in the upgraded state.

5 After the upgrade is successful, verify that the latest version of NSX packages is installed on the vSphere hosts.

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

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

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

8 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.

9 (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.

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

11 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 Upgrading Management Plane.

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

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. See *Customer Experience Improvement Program* in the *NSX Administration Guide* for more information, including how to join or leave the program.

Upgrade Management Plane from NSX 3.2 or 3.2.0.1

The upgrade sequence upgrades 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.

If you are upgrading from NSX 3.2 or later versions, the upgrade process also includes taking a local backup of NSX Manager nodes that can be used to restore or rollback the system. Once all prechecks are complete, the system saves the configuration backup followed by local backup of all the nodes in the cluster. To check if the system saved the local backup, you can go to the root admin and check `/image/backup/<unified_app_version>/cluster-node-backups`. The rollback backup is also saved at `/config_bak`. If the local backup fails for any reason, the upgrade is stopped.

Prerequisites

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

Procedure

1 Backup the NSX Manager.

See the *NSX 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.

4 Monitor the upgrade progress from the NSX Manager CLI for the orchestrator node. The NSX Manager user interface might be inaccessible.

```
get upgrade progress-status
```

Note Do not reboot the appliance while the upgrade is in progress. It might take several minutes for all the nodes to be upgraded and for the cluster to reach a stable state.

You can log in to the NSX Manager user interface when `get upgrade progress-status` indicates that the upgrade is successful and the NSX Manager services have started.

5 In the CLI, log in to the NSX Manager to check the cluster status and 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.

  `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.

- `get cluster status`

  If the group status is not Stable, troubleshoot the problem.

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 NSX 3.2.1.x and later

The upgrade sequence upgrades the Management Plane at the end. If required, you can continue to make configuration changes while the Management Plane upgrade is in progress.

Prerequisites

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

NSX supports only an odd number of nodes in a cluster. A three-node cluster is the recommended configuration for fault tolerance. The upgrade process also includes taking a local backup of NSX Manager nodes that can be used to restore or rollback the system. Once all prechecks are complete, the system saves the configuration backup followed by local backup of all the nodes in the cluster. To check if the system saved the local backup, you can go to the root admin and check the following folder:

- `/image/backup/<unified_app_version>/cluster-node-backups` - if the upgrade is from NSX 4.0.x and earlier versions.

- `/config_bak/backup/<unified_app_version>/cluster-node-backups` - if the upgrade is from NSX 4.1.0 and later versions.

The rollback backup is also saved at `/config_bak`. If the local backup fails for any reason, the upgrade is stopped.

Procedure

1 Backup the NSX Manager.

   See the *NSX 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 NSX Manager node may be rebooting during the upgrade. You can continue to monitor the progress of the upgrade from the UI of any of the other NSX Manager nodes.

   If you are using a Virtual IP address, the UI remains accessible but you need to re-authenticate yourself after all the nodes have been upgraded.

4 In case of upgrade errors, NSX may prompt you to roll back the upgrade. The rollback is performed on all the NSX Manager nodes:

   a Run the following command from a root shell on all the NSX Manager nodes :

      `/etc/init.d/corfu-server stop`

   b Run the following command as an admin user on all the NSX Manager nodes:

      `node-rollback run-step step1_start_rollback`

   c Run the following command as an admin user on any one of the NSX Manager nodes:

      `node-rollback run-step step2_restore_data`

      If you encounter any errors, run the following commands:

      1 Execute `corfu_tool_runner` to delete the record from the registry table:

      ```
      /opt/vmware/bin/corfu_tool_runner.py  -t RegistryTable -n CorfuSystem --port
      9000 -o deleteRecord --keyToDelete='{"namespace": "CorfuSystem","tableName":
      "CompactionControlsTable"}'
      ```

      2 Run compaction verification:

      ```
      /opt/vmware/bin/corfu_compactor_upgrade_runner.py --runs 3 --lock false
      ```

      3 Stop `corfu-server` on all NSX Manager nodes.

      4 Start `corfu-server` on all NSX Manager nodes.

5. Resume with the restore command as an admin user on any one of the NSX Manager nodes:

   ```
   node-rollback run-step step2_restore_data
   ```

d. Run the following command as an admin user on all the NSX Manager nodes:

   ```
   node-rollback run-step step3_exit_rollback
   ```

The rollback applies only to the Management Plane upgrade. Your NSX Manager nodes return to the version prior to starting the Management Plane upgrade.

What to do next

- Check the cluster status and verify that the services have started from the NSX Manager user interface.
- 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

4

NSX Cloud components are upgraded using the following workflow.

Upgrading NSX Cloud components from 3.2.x to 4.1.x

If you are upgrading NSX Cloud components from NSX 3.2.x to 4.1.x, follow this checklist:

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 the NSX Tools first followed by the PCG upgrade.	See Upgrade NSX Tools and PCG .
❑ 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 NSX Tools and PCG

You must first upgrade NSX Tools and then PCG.

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 Installation Guide*.
- AWS: See: *Generate the IAM Profile and PCG Role* in the *NSX 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 version available to upgrade and navigate to **Product Downloads > NSX Cloud Upgrade Bundle for NSX <version>.**

2 Verify that the main 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 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.

- Download the upgrade bundle: Download the NSX Upgrade Bundle
- Upgrade the Upgrade Coordinator from NSX Manager: Upgrade the Upgrade Coordinator

What to do next

Upgrade NSX Tools and PCG

Upgrade NSX Tools and PCG

You must first upgrade NSX Tools and then 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 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.

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.

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

Note When upgrading from 3.0.x or 3.1.x to 3.2.0 and later, make sure you first upgrade NSX Tools and then PCG. You might notice inter-VPC traffic loss on the VMs where PCG is upgraded to 3.2.0 or later but the NSX Tools are still not upgraded to 3.2.0 or later.

6 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.

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

8 Click **Finish**.

Results

PCGs and NSX Tools are upgraded.

How long does the upgrade process take:

Note CSM and NSX 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 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 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 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.

See Upgrade Management Plane from NSX 3.2.1.x and later.

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 main 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 4.0.x or 3.0.x to later, follow the Chapter 5 Post-Upgrade Tasks steps as you have already upgraded NSX.

Post-Upgrade Tasks

5

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

Read the following topics next:

- Verify the Upgrade

Verify the Upgrade

After you upgrade NSX, 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 Administration Guide*.

Prerequisites

Perform a successful upgrade. See Chapter 3 Upgrading NSX.

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

6 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 Appliance	Memory	vCPU
NSX Edge Small VM	4 GB	2
NSX Edge Medium VM	8 GB	4
NSX Edge Large VM	32 GB	8

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 Administration Guide*.

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

Read the following topics next:

- Collect Support Bundles
- Upgrade Fails Due to a Timeout
- Upgrade Fails Due to Insufficient Space in Bootbank on ESXi Host
- Unable to Upgrade Host Placed in NSX Maintenance Mode
- Failure to Upload the Upgrade Bundle
- Backup and Restore During Upgrade
- Loss of Controller Connectivity after Host Upgrade
- In-place Upgrade Fails
- Upgrade Coordinator User Interface is Inaccesible
- NSX Manager User Interface is Inaccessible During Upgrade

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 **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.

NSX Application Platform Note For information about collecting support bundles for NSX Application Platform, see the *Deploying and Managing the VMware NSX Application Platform* documentation.

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 VMware vCenter 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 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

Unable to Upgrade Host Placed in NSX Maintenance Mode

Host unit fails during the upgrade process and the upgrade coordinator places this host in NSX maintenance mode. Unable to upgrade host placed in NSX maintenance mode on restarting upgrade.

Problem

Hosts that fail during upgrade are placed in NSX maintenance mode.

Solution

1 Manually troubleshoot and fix the problem on the host.

2 From the NSX Manager UI, select **System > Fabric > Hosts**.

3 Locate the host that you fixed and select it.

   The status of the host is maintenance mode.

4 Evacuate any VMs present on the host and restart the host.

5 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 Delete TAR files that contain PCAP files.

5 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.

Solution

If you have upgraded from NSX 3.2 or later versions, you can also restore the system from the local backup taken by the upgrade process just before upgrading the first NSX Manager. The local backup is available at `/<`*`storage_location`*`>/backup/<unified_app_version>/cluster-node-backups` on all manager nodes. Note that the *storage_location* is `/image` if the upgrade is from NSX 4.0.x and earlier versions. For upgrades from NSX 4.1.0 and later versions, the *storage_location* is `/config_bak`.

If you want to use the local backup for restore, copy the backup file from NSX Manager to an SFTP location and then perform the following steps to restore the system.

1 Log in to NSX Manager as a root user.

2 Change the directory to the storage location.

   `cd /image` - if upgrading from NSX 4.0.x and earlier versions.

   `cd /config_bak` - if upgrading from NSX 4.1.0 and later versions.

3 Run the following command to copy the backup file to an SFTP server.

```
scp -rp backup/<unified_app_version>/* user@<SFTP server IP address>:/
<backup_path>
```

4 Run the following command to view the generated passphrase.

```
cat .backup_keystore/.keyfile
```

5 Select the passphrase to copy and save it at a secure location.

While copying the file, you must maintain the same directory structure on the SFTP location as on NSX Manager.

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 ESXi 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 *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 VMware vCenter 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.

Upgrade Coordinator User Interface is Inaccesible

The Upgrade Coordinator user interface may not be accessible.

Problem

You cannot access the Upgrade Coordinator user interface or APIs.

Cause

Internal service dependencies may cause the Upgrade Coordinator user interface to become inacessible.

Solution

Run the following command to restart the Upgrade Coordinator service:

```
restart service install-upgrade
```

NSX Manager User Interface is Inaccessible During Upgrade

When upgrading from NSX 3.2, the NSX Manager User Interface may be inaccessible during the Management Plane upgrade.

Problem

The NSX upgrade has been running longer than expected and the NSX Manager user interface is not accessible.

Cause

When upgrading from NSX 3.2, the NSX Manager user interface is inaccessible during the Management Plane upgrade.

Solution

The inaccessability of the NSX Manager user interface does not necessarily indicate an upgrade failure. To verify the upgrade status, run the following command from the NSX Manager CLI:

```
get upgrade progress-status
```

If you see an upgrade failure, follow the troubleshooting steps that are displayed in the command output.

Upgrading your NSX Federation Deployment

7

Follow the workflow for upgrading NSX Federation appliances depending on the version you are upgrading from.

Starting with NSX 4.1.1 and later, Global Manager (GM) and Local Manager (LM) upgrades can occur in any order. The GM and LM continue to sync if they are at different versions between 4.0 and 4.1. If you are upgrading from releases prior to NSX 4.1.1, you must first manually upgrade the standby GM cluster from the GM UI, followed by the active GM cluster. Both active and standby Global Managers must have the same version.

Also starting with NSX 4.1.1, Global Managers support the same interoperability as Local Managers, for example, from 3.2.3 to 4.1.2. Refer to the Local Manager (LM) and Global Manager (GM) Upgrade table for LM and GM version compatibility. Prior to NSX 4.1.1 interoperability was N+1, and N-1. Starting with NSX 4.1.1 and later, you can upgrade from NSX 3.2 to 4.1.2 to support the following releases (N+2 and N-2).

For example:

- If you have 3.2 LMs and 3.2 GMs, all can be upgraded to NSX 4.0 and 4.1.2, but not NSX 4.1.0.
- If you have 3.2 LMs and 4.1.2 the standby GM, then the active GM, LMs cannot be upgraded to NSX 4.0. Upgrade them directly to NSX 4.1.2.

Note Upgrade from NSX 3.2.2 or 3.2.3 to 4.0.1 or 4.0.1.1 is not supported. The reason is that the General Availability (GA) of NSX 3.2.2 occurred after the GA of NSX versions 4.0.1 and 4.0.1.1. Some capabilities and important fixes in NSX 3.2.2 might not be available in versions 4.0.1 or 4.0.1.1 due to the chronological order in which these versions were released. Instead, you can upgrade from NSX 3.2.2 or 3.2.3 to 4.1.2.

The Local Manager (LM) and Global Manager (GM) Upgrade table shows the software and the valid versions that will continue to sync with both the earlier and the latest LM and GM versions.

Table 7-1. Local Manager (LM) and Global Manager (GM) Upgrade

From \ To	4.1.0	4.1.x
3.1	First upgrade to 3.2	First upgrade to 3.2
3.2	Not applicable. Use case not supported because an LM 3.2 cannot be managed by a GM 4.1.0. Note: After 3.2.2 may be upgraded to 4.1.1.	Supported*
4.0	Supported*	Supported*
4.1.0	Not applicable	Supported*
4.1.1	Not applicable	Supported*

For table asterisk (*), refer to the Interoperability Matrix for the supported minor release versions at https://interopmatrix.vmware.com/Upgrade?productId=912.

Upgrade VMware Cloud Foundation Deployments with NSX Federation

The VMware Cloud Foundation™ Deployments with Local Manager (LM) and Global Manager (GM) Upgrade table shows the software and the valid versions that are on the upgrade path for NSX Federation in a VMware Cloud Foundation (VCF) environment.

Note For prior releases of VMware Cloud Foundation, you must first upgrade to VCF 4.5.x.

Table 7-2. VMware Cloud Foundation Deployments with Local Manager (LM) and (GM) Upgrade

From/To	Steps
VCF 4.5 to 5.0 LM 3.2.1.2 to 4.1.0.2 GM 3.2.1.2 to 4.1.0.2	1 Manually upgrade the standby GM, then the active GM from 3.2.1.2 to 4.0.1.1. GM 4.0.1.1 is compatible with VCF 4.5 with LM 3.2.1.2. 2 Upgrade from VCF 4.5 to 5.0 with SDDC Manager, which upgrades from LM 3.2.1.2 to 4.1.0.2. 3 Manually upgrade the standby GM, then the active GM from 4.0.1.1 to 4.1.0.2.
VCF 4.5.1 to 5.0 LM 3.2.2.1 to 4.1.1 GM 3.2.2.1 to 4.1.1	1 Manually upgrade the standby GM, then the active GM from 3.2.2.1 to 4.1.1. GM 4.1.1 is compatible with VCF 4.5.1 with LM 3.2.2.1. 2 Upgrade from VCF 4.5.1 to 5.0 with SDDC Manager, which upgrades from LM 3.2.2.1 to 4.1.0.2. 3 Apply the VCF async patch tool to upgrade from LM 4.1.0.2 to 4.1.1. Refer to https://docs.vmware.com/en/VMware-Cloud-Foundation/services/ap-tool/GUID-49818DF1-94EA-4C85-8CB6-6EFFCE5F8060.html

Table 7-2. VMware Cloud Foundation Deployments with Local Manager (LM) and (GM) Upgrade (continued)

From/To	Steps
VCF 4.5.1 to 5.0 LM 3.2.2.1 to 4.1.2.1 GM 3.2.2.1 to 4.1.2.1	1 Manually upgrade the standby GM, then the active GM from 3.2.2.1 to 4.1.2.1. GM 4.1.2.1 is compatible with VCF 4.5.1 with LM 3.2.2.1. 2 Upgrade from VCF 4.5.1 to 5.0 with SDDC Manager, which upgrades from LM 3.2.2.1 to 4.1.0.2. 3 Apply the VCF async patch tool to upgrade from LM 4.1.0.2 to 4.1.2.1. Refer to https://docs.vmware.com/en/VMware-Cloud-Foundation/services/ap-tool/GUID-49818DF1-94EA-4C85-8CB6-6EFFCE5F8060.html
VCF 4.5.2 to 5.0 LM 3.2.3.1 to 4.1.x GM 3.2.3.1 to 4.1.x	No upgrade path.
VCF 4.5 to 5.1 LM 3.2.1.2 to 4.1.2.1 GM 3.2.1.2 to 4.1.2.1	1 Manually upgrade the standby GM, then the active GM from 3.2.1.2 to 4.0.1.1. GM 4.0.1.1 is compatible with VCF 4.5 with LM 3.2.1.2. 2 Upgrade from VCF 4.5 to 5.1 with SDDC Manager, which upgrades from LM 3.2.1.2 to 4.1.2.1. 3 Manually upgrade the standby GM, then the active GM from 4.0.1.1 to 4.1.2.1.
VCF 4.5.1 to 5.1 LM 3.2.2.1 to 4.1.2.1 GM 3.2.2.1 to 4.1.2.1	1 Manually upgrade the standby GM, then the active GM from 3.2.2.1 to 4.1.2.1. GM 4.1.2.1 is compatible with VCF 4.5.1 with LM 3.2.2.1. 2 Upgrade from VCF 4.5.1 to 5.1 with SDDC Manager, which upgrades from LM 3.2.2.1 to 4.1.2.1.
VCF 4.5.2 to 5.1 LM 3.2.3.1 to 4.1.2.1 GM 3.2.3.1 to 4.1.2.1	1 Manually upgrade the standby GM, then the active GM from 3.2.3.1 to 4.1.2.1. GM 4.1.2.1 is compatible with VCF 4.5.2 with LM 3.2.3.1. 2 Upgrade from VCF 4.5.2 to 5.1 with SDDC Manager, which upgrades from LM 3.2.3.1 to 4.1.2.1.