Activating and Upgrading VMware NSX Intelligence

Modified 12 JUL 2024

VMware NSX Intelligence 4.0

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

Activating and Upgrading VMware NSX Intelligence

The *Activating and Upgrading VMware NSX Intelligence* document describes how to activate (install) or upgrade the VMware NSX® Intelligence™ feature.

Intended Audience

This information is intended for enterprise system administrators who must activate, upgrade, or use the NSX Intelligence feature. This information is provided for experienced enterprise system administrators who are familiar with virtual machine technology and network virtualization concepts.

Related Documentation

- VMware NSX® Documentation set for version 3.2 or later.

  You use the NSX Manager user interface to activate and access the VMware NSX® Intelligence™ feature.

- *Deploying and Managing the VMware NSX Application Platform* document included in the VMware NSX Documentation set for NSX version 3.2 or later.

  You must first deploy the VMware NSX® Application Platform before you can activate the NSX Intelligence feature.

- *Using and Managing VMware NSX Intelligence* document for version 3.2 or later for information on how to use and manage the NSX Intelligence feature. Information on how to use the NSX Suspicious Traffic feature is also included.

  This document is delivered with the NSX Intelligence Documentation set.

- For information about activating and administering the VMware NSX® Network Detection and Response™ feature, see the NSX Network Detection and Response topics in the Security section of the *NSX Administration Guide* version 3.2 or later.

  The *NSX Administration Guide* document is delivered with the VMware NSX Documentation set .

Overview of NSX Intelligence

1

VMware NSX® Intelligence™ provides a graphical user interface to visualize the security posture and network traffic flows that have occurred in your on-premises NSX environment.

What is NSX Intelligence

NSX Intelligence is a modern application that is hosted on the VMware NSX® Application Platform, which is a platform based on a microservices architecture.

NSX Intelligence 3.2 or later is available for ESXi-based hosts, physical server hosts, and ESX clusters that are enabled by the VMware vSphere® Lifecycle Manager.

NSX Intelligence 3.2 or later provides the following functionalities.

- A graphical visualization of the NSX components, such as groups, VMs, physical servers, IPs, and network traffic flows, in your NSX 3.2 or later environment. The data used is based on the network traffic flows aggregated during the specified time period.
- Recommendations for security policies, policy security groups, and services for applications. The recommendations assist you with the implementation of micro-segmentation at the application level. When you implement these recommendations, you can enforce a more dynamic security policy by correlating traffic patterns of communication that is occurring between the VMs, physical servers, and IPs in your NSX environment.
- Detection of suspicious or anomalous network behaviors in your data center network using the NSX Suspicious Traffic feature. To filter out those activities that are interesting from a security perspective, the NSX Suspicious Traffic feature applies threat-centric detectors to the traffic flow data that NSX Intelligence collects. The detection events generated by these detectors might be associated to specific techniques or tactics in the MITRE ATT&CK® Framework. If you have activated the VMware NSX® Network Detection and Response™ feature, the detection events are sent to the VMware NSX® Advanced Threat Prevention cloud service for further analysis. If the cloud service determined that the detection events are related, those events are correlated into a campaign that is organized into a timeline on the NSX Network Detection and Response UI. Each campaign can then be further investigated by your network security team using the NSX Network Detection and Response UI.

Prepare to Use NSX Intelligence

Use the information in Chapter 2 NSX Intelligence Activation and Usage Workflow to guide you on the steps you need to perform to get started with upgrading, activating, and using NSX Intelligence 3.2 or later.

Start Using NSX Intelligence

After you successfully activate and configure NSX Intelligence 3.2 or later, you can use its features in the following sections of the NSX Manager user interface.

- For traffic flow visualization, go to **Plan & Troubleshoot > Discover & Take Action** section of the NSX Manager UI.
- For micro-segmentation rule recommendations, navigate to **Plan & Troubleshoot > Recommendations** UI page.
- To manage suspicious or anomalous network traffic, use the **Security > Suspicious Traffic** page.

For more details, see the *Using and Managing VMware NSX Intelligence* document for version 3.2 or later available in the VMware NSX Intelligence Documentation set.

NSX Intelligence Activation and Usage Workflow

2

To track your progress in activating and configuring NSX Intelligence, and to quickly guide you on getting started in using its features, use the following checklist.

Perform these procedures in the order they are listed.

1. Install NSX 3.2 or later.

   See the installation workflow details in the *NSX Installation Guide* for version 3.2 or later that is delivered with the VMware NSX Documentation set.

2. Ensure you have met all the NSX Intelligence system requirements and reviewed all the resource limits listed in Chapter 3 Preparing to Activate NSX Intelligence.

3. (Optional) If you are upgrading from NSX Intelligence 1.2.x or earlier, see Chapter 6 Upgrading NSX Intelligence for details.

4. If you are activating NSX Intelligence for the first time, use the NSX Manager 3.2 or later user interface to deploy the NSX Application Platform with the Advanced form factor (for production environment) or Evaluation form factor (for non-production environment).

   NSX Intelligence is an application hosted on NSX Application Platform. For details, see the *Deploying and Managing the VMware NSX Application Platform* for version 3.2 or later that is delivered with the VMware NSX Documentation set.

5. Activate NSX Intelligence on the NSX Application Platform. See Chapter 4 Activate NSX Intelligence for more information.

6. (Optional) Configure NSX Intelligence settings to define for which standalone hosts or clusters of hosts NSX Intelligence needs to collect network traffic data.

   By default, after NSX Intelligence is activated, it starts collecting network traffic data on all standalone hosts and cluster of hosts in your NSX environment. You can optionally configure NSX Intelligence to deactivate traffic data collection for one or more standalone hosts or clusters of hosts. See Chapter 5 Configure NSX Intelligence Settings.

7. To start viewing the graphical visualization of your NSX workloads, click **Go to NSX Intelligence** on the NSX Intelligence feature card on the **Systems** > **NSX Application Platform** UI page.

   Alternatively, navigate to **Plan & Troubleshoot** > **Discover & Take Action** and refresh the web browser you are using for the NSX Manager session.

8 Begin using the NSX Intelligence features, including the NSX recommendations for micro-segmentation feature and the NSX Suspicious Traffic feature.

For information about getting started using NSX Intelligence, see the *Using and Managing VMware NSX Intelligence* document for version 3.2 or later.

Preparing to Activate NSX Intelligence

3

You must prepare the deployment environment so that it meets the minimum license and system requirements required for activating NSX Intelligence.

As previously mentioned, beginning with version 3.2, NSX Intelligence has transitioned from being a VM-based appliance to a modern application that is hosted on VMware NSX® Application Platform.

Read the following topics next:

- Requirements for Activating NSX Intelligence
- NSX Intelligence Limits and Web Client Requirements

Requirements for Activating NSX Intelligence

To perform the NSX Intelligence activation and use its features, your system environment must meet the license, system, and software requirements. You also must use the required NSX built-in user role.

License Requirements

- To activate, configure, and use NSX Intelligence, you need one of the following base licenses, with add-on licenses where applicable.

Base SKU License	Add-on SKU License
NSX Data Center Evaluation	None required
NSX-T Evaluation	None required
NSX-T Enterprise Plus	None required
NSX Data Center Enterprise Plus	None required
One of the following: ■ NSX Data Center Advanced ■ NSX Firewall ■ NSX-T Advanced	NSX Advanced Threat Prevention
NSX Distributed Firewall	None required
NSX Distributed Firewal with Threat Prevention	None required

Base SKU License	Add-on SKU License
NSX Distributed Firewall with Advanced Threat Prevention	None required
One of the following: ■ NSX Data Center Advanced ■ NSX-T Advanced	NSX Threat Prevention Add On for Distributed Firewall
One of the following: ■ NSX Data Center Advanced ■ NSX-T Advanced ■ NSX Distributed Firewall with Threat Prevention	NSX Advanced Threat Prevention Add On for NSX Distributed Firewall
NSX Advanced with Threat Prevention	None required
NSX Advanced with Advanced Threat Prevention	None required
NSX Enterprise Plus with Threat Prevention	None required
NSX Enterprise Plus with Advanced Threat Prevention	None required

- To use the NSX Suspicious Traffic and NSX Network Detection and Response features, one of the following licenses is required during your NSX Manager session.
  - NSX Distributed Firewall with Advanced Threat Prevention
  - NSX Advanced with Advanced Threat Prevention
  - NSX Enterprise Plus with Advanced Threat Prevention
- See VMware Knowledge Base article 89137 for information on licensing editions required for specific NSX Intelligence features.

System Requirements

Because the VMware NSX® Application Platform hosts the NSX Intelligence feature beginning with version 3.2, you must meet the minimum NSX Application Platform system requirements needed to activate the NSX Intelligence feature. For more information, see the "NSX Application Platform System Requirements" topic in the *Deploying and Managing the VMware NSX Application Platform* documentation for version 3.2 or later. The document is delivered in the VMware NSX Documentation set.

For the NSX Application Platform form factors required for activating the NSX Intelligence feature, see the information in the following "Software Requirements" section.

Software Requirements

- NSX 3.2 or later must be installed. See the *NSX Installation Guide* documentation that is included with the VMware NSX Documentation set. Select the folder for the specific NSX version that you plan to install and locate the *NSX Installation Guide*.
- NSX Application Platform must be deployed using the NSX Manager 3.2 or later user interface.

To be able to activate NSX Intelligence, you must select one of the following form factors during the NSX Application Platform deployment preparation.

- **Advanced** form factor when deploying the NSX Application Platform for a production environment.
- **Evaluation** form factor for a non-production environment for use in evaluations and demonstrations only.

For more details, see the "NSX Application Platform System Requirements" topic in the Getting Started with the NSX Application Platform section of the *Deploying and Managing the VMware NSX Application Platform* documentation that is included in the VMware NSX Documentation set. Select the folder for the specific NSX version that you have installed or plan to install and locate the *Deploying and Managing the VMware NSX Application Platform* document.

User Role Requirement

To activate, back up, restore, and upgrade NSX Intelligence, you must use an account with the built-in NSX-T Enterprise Admin role when using the NSX Manager user interface to perform the administrative tasks.

NSX Intelligence Limits and Web Client Requirements

Before you use the NSX Intelligence features, review the resource limitations and ensure that your client environment meets the minimum requirements for the client system where the NSX Intelligence user interface (UI) features are displayed.

NSX Intelligence Resource Limits

The following table lists the two NSX Application Platform form factors that support NSX Intelligence and the estimated maximum number of hosts, workloads, and traffic flows supported for each form factor. The NSX Intelligence hosted on an Evaluation form factor is suitable for non-production environment only. The NSX Intelligence hosted on an Advanced form factor is suitable for a production environment. For NSX Application Platform system requirements details, see the *Deploying and Managing the VMware NSX Application Platform* documentation delivered with the VMware NSX Documentation set.

Note NSX Intelligence is supported only on NSX Manager 3.2 or later. Only one activated NSX Intelligence feature is supported per NSX Manager Unified Appliance cluster.

NSX Application Platform Form Factor	Max. # of Hosts	Max. # of VM or Physical Server Workloads	Max. # of Flows
Evaluation (for non-production use only)	50 hosts	2,000 VMs Up to 500 can be physical servers and the remainder VMs.	250,000 flows per 5-minute interval
Advanced	250 hosts	5,000 VMs Up to 1,000 can be physical servers and the remainder VMs.	■ 500,000 per 5-minute interval when using 3 worker nodes (See Important Note after this table.) ■ 1,000,000 flows per 5-minute interval when using 8 worker nodes

Important The NSX Application Platform generates alarms when a scale-out operation is required due to resource usage exceeding the current capacity for the number of worker nodes that have been deployed. To resolve these alarms, scale out the NSX Application Platform by incrementally adding more worker nodes to your guest cluster.

NSX Intelligence Web Client Memory, CPU, and Browser Requirements

For an optimal performance, your client system must have a minimum of two 1.4 GHz CPU cores and at least 16 GB of RAM.

The following table lists the web browser versions supported for NSX Intelligence. The minimum supported browser resolution is 1280 x 800 pixels.

Browser	Windows 10	MacOS 10.14, 10.15	Ubuntu 18.4
Google Chrome 80 or later	Yes	Yes	Yes
Mozilla Firefox 72 or later	Yes	Yes	Yes
Microsoft Edge 80 or later	Yes	Yes	Yes

Activate NSX Intelligence

4

Beginning with version 3.2, NSX Intelligence has transitioned from a VM-based appliance to a modern application that runs on VMware NSX® Application Platform, which is based on a micro-services architecture. You use the NSX Manager user interface (UI) to install and configure the NSX Intelligence appliance.

Prerequisites

- Ensure that your environment meets the minimum license and system requirements for activating NSX Intelligence. One of the key requirements is a successfully deployed NSX Application Platform. See Chapter 3 Preparing to Activate NSX Intelligence for details.
- The deployed NSX Application Platform must be in a `STABLE` state.
- You must have NSX Enterprise Administrator user privileges.
- A valid NSX Data Center Enterprise Plus edition license must be in effect for your NSX Manager session.
- The number of transport nodes must not exceed 250.

Procedure

1. From your browser, log in with Enterprise Administrator privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. In the NSX Manager UI, select **System** and in the Configuration section, select **NSX Application Platform**.
3. Navigate to the Features section, locate the **NSX Intelligence** feature card, and click **Activate** or anywhere in the card.
4. In the **NSX Intelligence** activation dialog box, click **Run Prechecks**.

   The system proceeds to check that the NSX Application Platform is deployed with the Advanced form factor, which is required to activate NSX Intelligence. It also verifies that you have at least a valid NSX Data Center Enterprise Plus edition license and that the number of transport nodes does not exceed the limit of 250.
5. Click **Activate**.

   The activation progress is shown on the NSX Intelligence feature card under the **System > NSX Application Platform** tab. The activation can take around 15 minutes to finish.

If there is any error reported, use the information provided in the error messages to resolve the reported problem. See Chapter 8 Troubleshooting NSX Intelligence Feature Activation for possible hints in resolving problems you might have encountered.

After the problem is resolved, you must delete the NSX Intelligence application first and try to reactivate it from the **System > NSX Application Platform** tab. See Chapter 7 Delete NSX Intelligence for information.

6 After NSX Intelligence is successfully activated, the feature card displays an `UP` status. Click **Go to NSX Intelligence**.

The NSX Manager UI refreshes with the NSX Intelligence features enabled in the **Plan & Troubleshoot > Discover & Plan** section of the UI.

If the activation is taking longer than 30 minutes or if you see any error messages, consult the Chapter 8 Troubleshooting NSX Intelligence Feature Activation topics.

7 (Optional) Configure NSX Intelligence settings to define for which standalone hosts or cluster of hosts NSX Intelligence needs to collect network traffic data

By default, after NSX Intelligence is activated, it starts collecting network traffic data on all standalone hosts and cluster of hosts in your NSX environment. You can optionally set NSX Intelligence to deactivate traffic data collection for specific hosts or cluster of hosts. See Chapter 5 Configure NSX Intelligence Settings.

What to do next

Begin using the NSX Intelligence features using the **Plan & Troubleshoot > Discover & Plan** section of the NSX Manager UI. For information on getting started with using NSX Intelligence, see the *Using and Managing VMware NSX Intelligence* documentation.

Configure NSX Intelligence Settings

5

After you activate NSX Intelligence, by default, NSX Intelligence collects network traffic data on all standalone hosts and cluster of hosts. If necessary, you can optionally stop data collection from a standalone host or cluster of hosts.

The **Standalone Host** section in the **Data Collection** tab in the **System Settings > NSX Intelligence** UI lists only the hosts that do not belong to a cluster and hosts that are not managed by a compute manager. The **Cluster** section lists all the clusters in your NSX environment.

You cannot deactivate or activate data collection for a single host that belongs to a cluster. You can only deactivate or activate data collection on the entire cluster to which that host belongs. When data collection is deactivated for a cluster, **NSX Intelligence** stops collecting data on all the hosts that belong to that cluster. Similarly, if data collection mode is activated on a cluster, **NSX Intelligence** starts collecting data on all the hosts that belong to that cluster.

If the data collection mode is deactivated for a standalone host and that host is added to a cluster whose data collection is activated, **NSX Intelligence** starts collecting data on that host after it joins that cluster. If a host moves from a cluster (with an activated data collection setting) to a standalone host, the data collection setting is retained in the now standalone host. If a standalone host has its data collection mode activated and it is added to a cluster whose data collection is deactivated, **NSX Intelligence** stops data collection on that host after it joins that cluster.

Prerequisites

- NSX Intelligence must be activated on NSX Application Platform. See Chapter 4 Activate NSX Intelligence.
- You must have NSX Enterprise Administrator user privileges.
- At least a valid NSX Data Center Enterprise Plus edition license is in effect for your NSX Manager session.

Procedure

1 From your browser, log in with Enterprise Administrator privileges to an NSX Manager at https://<nsx-manager-ip-address>.

2 In the NSX Manager UI, select **System** and in the Settings section, select **NSX Intelligence**.

3 To manage traffic data collection for one or more hosts, perform one of the following steps.

   a To stop traffic data collection, select the host or hosts in the **Standalone Host** section, click **Deactivate**, and click **Confirm** when prompted if you are sure.

   b To start traffic data collection, select the host or hosts, click **Activate**, and click **Confirm** when prompted if you are sure.

   The system updates the **Collection Status** value for each affected host to `Deactivated` or `Activated`, depending on the data collection mode you had set.

4 To manage traffic data collection for one or more clusters of hosts, perform one of the following steps.

   a To stop data collection for one or more clusters, select the cluster or clusters in the **Cluster** section, click **Deactivate**, and click **Confirm** when prompted if you are sure.

   b To start traffic data collection, select the cluster or clusters, click **Activate**, and click **Confirm** when prompted if you are sure.

   The system updates the **Collection Status** value for each affected cluster to `Deactivated` or `Activated`, depending on the data collection mode you had set.

Upgrading NSX Intelligence

6

Upgrading from earlier versions of VMware NSX® Intelligence™ to NSX Intelligence 3.2 or later depends on the NSX Intelligence version that you currently have installed.

Beginning with version 3.2, NSX Intelligence has transitioned from being a VM-based appliance to a modern application that is hosted on VMware NSX® Application Platform, a platform based on a microservices architecture. As a result, the NSX Intelligence upgrade path you must use depends on the current NSX Intelligence version you have installed.

The only direct upgrade path supported to NSX Intelligence 3.2.0 is from NSX Intelligence 1.2.x. Installations using NSX Intelligence 1.1 or 1.0 must first upgrade to version 1.2.x in order to upgrade to NSX Intelligence 3.2.0.

The system supports an in-place upgrade mode only. All the NSX Intelligence services and user interface are not available during the upgrade. You have the option to retain all the data from the NSX Intelligence 1.1.x or earlier appliance node.

Network traffic data migration support is available when upgrading from NSX Intelligence version 1.2 to version 3.2.

To upgrade to NSX Intelligence 3.2 or later, locate in the following table the NSX Intelligence upgrade path that fits your current installation and use the corresponding instructions.

Upgrade Path	Instructions
From NSX Intelligence 1.0.x to version 3.2 or later	1 Use NSX Intelligence 1.0 command-line interface (CLI) to upgrade your NSX Intelligence 1.0.x appliance to NSX Intelligence 1.2.x. See Upgrade the NSX Intelligence 1.0 Using the CLI. 2 Use the instructions for upgrading from NSX Intelligence 1.2.x to NSX Intelligence 3.2. See Upgrade NSX Intelligence 1.2 Using the UI.
From NSX Intelligence 1.1.x to version 3.2.0	1 Use the NSX Manager user interface (UI) to upgrade your NSX Intelligence 1.1.x to NSX Intelligence 1.2.x. See Upgrade the NSX Intelligence 1.1 Using the UI. 2 Use the instructions for upgrading from NSX Intelligence 1.2.x to NSX Intelligence 3.2.0. See Upgrade NSX Intelligence 1.2 Using the UI.

Upgrade Path	Instructions
From NSX Intelligence 1.2.x to version 3.2.0	Use the NSX Manager UI to upgrade to NSX Intelligence 3.2.0. Upgrade NSX Intelligence 1.2 Using the UI.
From NSX Intelligence 3.2.0 to version 3.2.1 or later	1 You must first upgrade the NSX Application Platform 3.2.0 to version 3.2.1 or later using the NSX Manager UI. 2 After upgrading the NSX Application Platform 3.2.0 successfully, use the same UI to update NSX Intelligence 3.2.0 to version 3.2.1 or later. For details about upgrading the NSX Application Platform and the associated NSX features, such as NSX Intelligence, see the "Upgrade NSX Application Platform" topic in the *Deploying and Managing the VMware NSX Application Platform* documentation delivered with NSX 3.2 or later in the VMware NSX Documentation set.

Read the following topics next:

- Preparing to Upgrade NSX Intelligence
- Verify the Current State of NSX Intelligence
- Download the NSX Intelligence Upgrade Bundle
- Upgrade the NSX Intelligence 1.0 Using the CLI
- Upgrading NSX Intelligence Using the UI

Preparing to Upgrade NSX Intelligence

Before you upgrade your NSX Intelligence appliance, make some preparations first.

Use the following list before proceeding with the upgrade.

1 Check for any known upgrade problems and workarounds that are documented in the *VMware NSX Intelligence Release Notes*.

2 Ensure that the NSX Manager Unified Appliance cluster has a valid NSX Enterprise Plus license that allows the upgrade of the NSX Intelligence appliance. Specifically, check that the license has not expired.

   If you do not have the appropriate Enterprise Plus license, you might encounter an error while attempting to upgrade your current NSX Intelligence appliance version. For example, if you are attempting to upgrade an NSX Intelligence 1.1.0 or 1.1.1 appliance that was installed using NSX 3.0 or later, and NSX has a default vShieldEndpoint license only, you encounter the following error.

   ```
   Stop NSX Intelligence data collection error: Your current license is
   insufficient for using the upgrade feature. Verify your current license
   before trying to upgrade your NSX Intelligence appliance again.
   ```

3 Verify that the current NSX Intelligence appliance is in a healthy state.

   See Verify the Current State of NSX Intelligence.

4 Download the latest NSX Intelligence upgrade bundle.

   See Download the NSX Intelligence Upgrade Bundle.

Verify the Current State of NSX Intelligence

Before you begin the upgrade process, it is important to test the working state of NSX Intelligence to help determine whether any post-upgrade problems you might encounter are related to the upgrade.

Procedure

1 From your browser, log in with Enterprise Administrator privileges to an NSX Manager at https://<nsx-manager-ip-address>.

2 Click **Plan & Troubleshoot > Discover & Take Action** and verify that security postures are being displayed without errors.

3 Click **Plan & Troubleshoot > Recommendations** and verify that any existing recommendations are listed without errors and new recommendations can be generated without errors.

4 If you are upgrading from NSX Intelligence 1.1.x or 1.2.x, verify that there are no active alarms and that the NSX Intelligence appliance is in a healthy state.

   a Click **System > Configuration > Appliances**.

   b Locate the NSX Intelligence feature card.

   c Ensure that there are no active alarms displayed on the card and that the node is shown to be in a healthy state.

5 If you are upgrading from NSX Intelligence 3.2 or later, verify that there are no active alarms and that NSX Intelligence is in a healthy state.

   a Click **System > NSX Application Platform**.

   b Locate the NSX Intelligence feature card.

   c Ensure that Status displays `UP`.

Results

If any alarms or errors are reported while performing the previous steps, address those alarms and errors before proceeding with the upgrade process.

Download the NSX Intelligence Upgrade Bundle

Before you begin the upgrade process, download the correct NSX Intelligence upgrade bundle version and file type to use. The upgrade bundle contains all the files to upgrade your currently installed NSX Intelligence. This upgrade bundle is required when you are upgrading from NSX Intelligence 1.2 to NSX Intelligence 3.2 or later.

Procedure

1 On the VMware NSX Intelligence Product Download webpage, select the target NSX Intelligence version to which you want to upgrade.

2 In the Product Downloads tab, locate the available NSX Intelligence upgrade bundle for the selected target version.

3 Use the following table to determine which upgrade bundle you must download.

Version Upgrade Path	NSX Version	Upgrade Bundle File Type	Filename Format	Example
From NSX Intelligence version 1.0.x to version 1.2.x	2.5.x	`NUB`	`VMware-NSX-Intelligence-appliance-`	`VMware-NSX-Intelligence-appliance-1.2.0.0.0.16730870.nub`
From NSX Intelligence version 1.1.x to 1.2.x version	2.5.x	`NUB`	`VMware-NSX-Intelligence-appliance-`	`VMware-NSX-Intelligence-appliance-1.2.0.0.0.16730870.nub`
From NSX Intelligence version 1.1.x to version 1.2.x	3.0.x or later	`MUB`	`VMware-NSX-Intelligence-upgrade-bundle-`	`VMware-NSX-Intelligence-upgrade-bundle-1.2.0.0.0.16730870.mub`
From NSX Intelligence version 1.2.x to version 3.2 or later	3.1.x or later	`MUB`	`VMware-NSX-Intelligence-upgrade-bundle-`	`VMware-NSX-Intelligence-upgrade-bundle-3.2.0.0.0.18757071.mub`

4 Click **Download Now** and store the selected NSX Intelligence upgrade bundle to a local system or to a remote web server that is accessible from your current NSX Intelligence appliance.

What to do next

Install the upgrade bundle to your current NSX Intelligence installation.

- If you are upgrading from NSX Intelligence version 1.0.x, see Upgrade the NSX Intelligence 1.0 Using the CLI.
- If you are upgrading from NSX Intelligence version 1.1 or later, see Upgrading NSX Intelligence Using the UI.

Upgrade the NSX Intelligence 1.0 Using the CLI

You must use the NSX Intelligence CLI when upgrading your NSX Intelligence 1.0 installation to NSX Intelligence version 1.1 or later.

Beginning with NSX Intelligence version 1.1, you upgrade the NSX Intelligence version 1.1 or later appliance using the NSX Manager UI only. Although you can upgrade from version 1.1 of the appliance using the CLI, that CLI upgrade process does not include important pre-upgrade checks. See Upgrade the NSX Intelligence 1.1 Using the UI.

To upgrade from NSX Intelligence 1.0.x to NSX Intelligence 3.2 or later, you must first upgrade your current installation to NSX Intelligence 1.2.x using the NSX Intelligence 1.0.x CLI. You must then use the NSX Manager 3.1.x UI to upgrade to NSX Intelligence 3.2 or later.

Caution When using the CLI method to upgrade the NSX Intelligence appliance, do not forcefully end the SSH session or press Ctrl+C. Doing so ends the upgrade process and might leave the NSX Intelligence appliance in an unhealthy state.

Prerequisites

- Download the NSX Intelligence upgrade bundle (`.nub`) file. See Download the NSX Intelligence Upgrade Bundle.
- Verify that there is free space in the `/tmp` partition in the NSX Intelligence host. The free space must be at least the size of the `.nub` upgrade bundle file that you downloaded.
- Also verify that there is at least twice the size of the `.nub` upgrade bundle file or 4 GB of free space in the `/image` partition in the NSX Intelligence host.

Procedure

1 Log in to your NSX Intelligence appliance using the CLI admin credentials that you had set up during the previous NSX Intelligence appliance deployment.

```
$ssh admin@<NSX Intelligence IP Address>
```

2 From the NSX Intelligence command line, use the following command to copy the NSX Intelligence`.nub` upgrade file from where you downloaded it.

```
copy url <url_to_NSX_intelligence_upgrade_nub>
```

Following is an example, using a NSX Intelligence version 1.2 `.nub` file.

```
copy url http://localserver/VMware-NSX-Intelligence-appliance-1.2.0.0.0.16730870.nub
```

3 Verify the upgrade bundle using the following command.

Tip Press Tab after entering `upgrade-bundle` and the *<upgrade_bundle_name>* is auto-filled.

```
verify upgrade-bundle upgrade_bundle_name
```

Following is a sample output for updating the `verify upgrade-bundle command`.

```
Checking upgrade bundle /var/vmware/nsx/file-store/VMware-NSX-Intelligence-
appliance-1.2.0.0.0.16730870.nub contents
Verifying bundle VMware-NSX-Intelligence-appliance-1.2.0.0.0.16730870.bundle with
signature VMware-NSX-Intelligence-appliance-1.2.0.0.0.16730870.bundle.sig
Moving bundle to /image/VMware-NSX-Intelligence-appliance-1.2.0.0.0.16730870.bundle
Extracting bundle payload
```

```
Successfully verified upgrade bundle
Bundle manifest:
       appliance_type: 'nsx-intelligence-appliance'
       version: '1.2.0.0.0.16730870'
       os_image_path: 'files/nsx-root.squashfs'
       os_image_md5_path: 'files/nsx-root.squashfs.md5'
Current upgrade info:
{
  "info": "",
  "body": {
    "meta": {
      "from_version": "1.0.1.0.0.14576942",
      "old_data_dev": "/dev/mapper/nsx-data",
      "new_data_dev": "/dev/mapper/nsx-data__bak",
      "new_os_dev": "/dev/sda3",
      "to_version": "1.2.0.0.0.16730870",
      "new_config_dev": "/dev/mapper/nsx-config__bak",
      "old_os_dev": "/dev/sda2",
      "bundle_path": "/image/VMware-NSX-Intelligence-appliance-1.2.0.0.0.16730870",
      "old_config_dev": "/dev/mapper/nsx-config"
    },
    "history": []
  },
  "state": 1,
  "state_text": "CMD_SUCCESS"
}
```

4 Upgrade the NSX Intelligence 1.0.x appliance using the NSX Intelligence Playbook.

Tip Press Tab after entering `upgrade-bundle` and the *<upgrade_bundle_name>* is auto-filled. Press Tab after entering `playbook` and the *<nsx_intelligence_playbook_name>* is auto-populated.

```
start upgrade-bundle <upgrade_bundle_name> playbook <nsx_intelligence_playbook_name>
```

Note If the `/data` partition is large, the step to copy data from that partition might take some time to finish if the partition is large.

The system reboots as part of the upgrade process, as shown in the following example.

```

mynsxintel> start upgrade-bundle VMware-NSX-Intelligence-appliance-1.2.0.0.0.16730870
playbook VMware-NSX-Intelligence-appliance-1.2.0.0.0.16730870-playbook
*****************************************************************************
Node Upgrade is in progress. Please do not make any changes, until
the upgrade operation is complete.
*****************************************************************************

2020-09-13 13:50:26,455 - Validating playbook /var/vmware/nsx/file-store/VMware-NSX-
Intelligence-appliance-1.2.0.0.0.16730870-playbook.yml
2020-09-13 13:50:26,583 - Running "shutdown_pace_svc" (step 1 of 7)
2020-09-13 13:50:51,734 - Running "install_os" (step 2 of 7)
```

```
2020-09-13 13:51:55,482 - Running "retain_pace_config" (step 3 of 7)
2020-09-13 13:52:00,529 - Running "switch_os" (step 4 of 7)
2020-09-13 13:52:17,786 -

System will now reboot (step 5 of 7)
{
  "info": "",
  "body": null,
  "state": 1,
  "state_text": "CMD_SUCCESS"
}
mynsxintel>
Broadcast message from root@mynsxintel (Fri 2020-09-13 13:52:22 UTC):

The system is going down for reboot at Fri 2020-09-13 13:53:22 UTC!
```

5 (Optional) If you are upgrading from NSX Intelligence 1.0.1 or later, you can verify the upgrade's progress using the following command.

```
get upgrade progress-status
```

6 (Optional) After the reboot process is finished, log in to the NSX Intelligence appliance console as `admin` and run the following command to verify the appliance upgrade status.

```
get upgrade progress-status | json
```

7 (Optional) From the NSX Intelligence appliance console, verify that the NSX Intelligence appliance version is correct and matches the version of the upgrade bundle you downloaded from the VMware download portal.

```
get version
```

Following is a sample output based on the examples used in earlier steps.

```

mynsxintel> get version
VMware NSX Intelligence, Version 1.2.0.0.0.16730870
```

Upgrading NSX Intelligence Using the UI

Beginning with NSX Intelligence version 1.1, you upgrade the NSX Intelligence version 1.1 or later appliance using the NSX Manager UI only. Although you can upgrade the appliance using the CLI, that CLI upgrade process does not include important pre-upgrade checks. The upgrade bundle must be of the `MUB` filetype.

Use one of the following topics depending on the current version of your NSX Intelligence installation.

Upgrade the NSX Intelligence 1.1 Using the UI

Use the NSX Manager user interface (UI) to upgrade your current NSX Intelligence 1.1.x to NSX Intelligence 1.2.x version.

To upgrade from NSX Intelligence 1.1.x to NSX Intelligence 4.0.x, you must first upgrade to NSX Intelligence 1.2.x using the NSX Manager UI. You can then migrate from NSX Intelligence 1.2.x to NSX Intelligence 3.2.x and upgrade to NSX Intelligence 4.0.x using the NSX Manager UI.

Note NSX Intelligence 1.2.x cannot be upgraded directly to NSX Application Platform 4.x.

Caution Do not power off NSX Intelligence manually during the upgrade process. It is rebooted as part of the upgrade process.

Prerequisites

- Download the NSX Intelligence bundle (`.mub`) file. See Download the NSX Intelligence Upgrade Bundle.
- Ensure that the `/image` partition in the NSX Manager host has enough space for the `MUB` file to be uploaded to the NSX Manager host.
- The `/image` and `/tmp` partitions of the NSX Intelligence node must have enough space to upload and verify the NSX Intelligence upgrade bundle.

Procedure

1. From your browser, log in with enterprise administrator privileges to an NSX Manager at `https://<nsx-manager-ip-address>`.
2. In NSX Manager, select **System > Upgrade**.
3. Locate the NSX Intelligence Appliances card and click **Upgrade NSX Intelligence**.
4. In the Upgrade Bundle pane, use the following information to decide which method to use to upload the upgrade bundle.
   - Select **Upload MUB File** if you downloaded the `MUB` update bundle to a local datastore.
   - Select **Upload From Remote Location** if you downloaded the `MUB` update bundle to a remote web server.
5. Enter the filename of the upgrade bundle using the following information.

   Important The `MUB` filename entered must match exactly as the upgrade bundle file that you downloaded from the Broadcom support portal.

   a. If you selected the **Upload MUB File** method, click **Select File**, navigate to the downloaded `MUB` file location, and select the file.

   b. If you selected **Upload From Remote Location** method, enter the full URL of the `MUB` file you downloaded on your remote web server.

6 Click **Upload File**.

The upload might take some time. The progress of the upload and verification of the upgrade bundle is displayed. If you decide not to continue with the upload, click **Cancel**. A message is displayed to confirm the bundle upload cancellation. You must reupload the bundle again to proceed with the upgrade process.

7 After the upgrade bundle is uploaded successfully, click **Start Upgrade**.

The Upgrade Coordinator is upgraded with the NSX Intelligence upgrade information. The Upgrade Coordinator runs in NSX Manager. It is a self-contained web application that orchestrates the upgrade process of NSX Intelligence and other NSX objects. The Upgrade Coordinator guides you through the proper upgrade sequence. You can track the upgrade process from the user interface.

8 After the Upgrade Coordinator is updated successfully, the **Summary** tab shows the current NSX Intelligence version and the target version to be used for the upgrade.

Note When performing a maintenance release upgrade, if you upgrade the NSX Intelligence Upgrade Coordinator with the maintenance bundle, but you proceed to upgrade NSX Manager first, you must repeat the preceding steps 1–8 when the NSX Manager upgrade is finished.

9 Click **Run Pre-Checks**.

The health of NSX Intelligence is verified. Also, the upgrade pre-check process verifies if there is any NSX upgrade in progress and handles it accordingly. When the pre-checks are finished without errors, the green `Ready` text and checkmark icon appears on the NSX Intelligence upgrade card. If errors were encountered during the pre-checks, the error messages are displayed.

10 Click **Next**.

11 On the **NSX Intelligence Appliance Upgrade** tab, verify that the target version, upgrade unit, and IP address shown are correct.

12 Click **Start Upgrade**.

The **Status** column in the table changes from `Not Started` to `In Progress` and the upgrade's progress is displayed next to **Details**.

Note If the `/data` partition is large, the step to copy data from that partition might take some time to finish if the partition is large.

If an error is encountered, the value in the **Status** column is changed to `Failed`. You can look at the error information provided in **Details** or click **Recent Logs** to view the upgrade process log output. Determine the necessary action you must do to resolve the error encountered.

13 (Optional) If the upgrade attempt failed and you have determined that it is safe to try the upgrade again, click **Retry Upgrade**.

The upgrade steps that finished successfully in the previous attempt are not redone. The upgrade process step where the failure happened is attempted again. When all the upgrade steps are finished successfully, the `Upgrade Successful` banner message is displayed and the **Status** value in the table is changed to `Upgraded`.

14 Click **Finish**.

The NSX Intelligence Appliances card displays the information about the new NSX Intelligence version and the summary of the upgrade that finished.

What to do next

Navigate to **Plan & Troubleshoot > Discover & Take Action** and verify that the data flow visualization is intact and new traffic flow data is getting collected as expected.

Upgrade NSX Intelligence 1.2 Using the UI

Use the NSX Manager user interface (UI) to upgrade your current NSX Intelligence 1.2.x installation to NSX Intelligence 3.2 or later.

NSX Intelligence has transitioned from using a VM-based appliance to being hosted on the NSX Application Platform, a Kubernetes cluster-based platform. Before you upgrade to NSX Intelligence 3.2, you must decide whether to migrate the NSX Intelligence traffic flow data that has been collected to date. Migrating the flow data requires preparation of the NSX Intelligence upgrade bundle that is used during the upgrade to NSX Intelligence 3.2. If you choose not to migrate the traffic data, all the traffic data analytics are lost permanently.

Caution Do not power off the NSX Intelligence appliance manually during the upgrade process.

Prerequisites

- Download the NSX Intelligence appliance bundle (`.mub`) file. See Download the NSX Intelligence Upgrade Bundle.
- Ensure that the `/image` partition in the NSX Manager host has enough space for the `MUB` file to be uploaded to the NSX Manager host.
- The `/image` and `/tmp` partitions of the NSX Intelligence appliance node must have enough space to upload and verify the NSX Intelligence upgrade bundle.

Procedure

1 From your browser, log in with enterprise administrator privileges to the orchestrator NSX Manager node at `https://<nsx-manager-ip-address>`.

2 In NSX Manager, select **System > Upgrade**.

3 Locate the NSX Intelligence Appliances card and click **Upgrade NSX Intelligence**.

4 In the **Upgrade Bundle** page, use the following information to decide which method to use to upload the upgrade bundle.

   - Select **Upload MUB File** if you downloaded the `MUB` update bundle to a local datastore.
   - Select **Upload From Remote Location** if you downloaded the `MUB` update bundle to a remote web server.

5 Enter the filename of the upgrade bundle using the following information.

   Important The `MUB` filename entered must match exactly as the upgrade bundle file that you downloaded from the VMware Products Download portal.

   a If you selected the **Upload MUB File** method, click **Select**, navigate to the downloaded `MUB` file location, and select the file.

   b If you selected **Upload From Remote Location** method, enter the full URL of the `MUB` file you downloaded on your remote web server.

6 Click **Upload**.

   The upload might take some time. The progress of the upload and verification of the upgrade bundle is displayed. If you decide to not continue with the upload, click **Cancel**. A message is displayed to confirm the bundle upload cancellation. You must reupload the bundle again to proceed with the upgrade process.

7 After the `.MUB` file is uploaded successfully, click **Start Upgrade**.

   The Upgrade Coordinator is upgraded with the NSX Intelligence upgrade information. The Upgrade Coordinator runs in NSX Manager. It is a self-contained web application that orchestrates the upgrade process of NSX Intelligence. The Upgrade Coordinator guides you through the proper upgrade sequence. You can track the upgrade process from the user interface.

8 In the **Prepare for Upgrade** tab, decide if you want to retain the analytical data collected by NSX Intelligence 1.2 and migrate it to the target NSX Intelligence 3.2 installation.

Retain Data?	Instructions
Yes	1 Click **Yes** to retain the analytical data collected by NSX Intelligence. 2 Read the Note about the data migration and click **Confirm**. 3 Click **Run Prechecks**. If errors are encountered during the prechecks, click the **Issues found** link, review the details about the reported issues, and resolve the issues before continuing. 4 After the precheck status returns `Success` or the **Next** button is enabled, click **Next**. 5 Click **Prepare for Migration**. The system proceeds to upload the upgrade bundle, stops the data collection, shuts down all of the services, and prepares the data for migration from your NSX Intelligence 1.2 appliance. Details about the progress is shown on the UI. You can also click **Recent Logs** to see the progress. 6 After the appliance is marked as ready for migration, click **Finish**. In the **System > Upgrade** page, the **NSX Intelligence Appliances** card displays the Upgrade Summary 7 On the **NSX Intelligence Appliances** card, click **Show Upgrade History** to verify that the target version is correct.
No	**Caution** All analytical data previously collected by NSX Intelligence will be lost when you choose not to migrate the data. 1 Click **No** and click **Go to Appliances**. You can proceed to delete the NSX Intelligence appliance. 2 Locate the NSX Intelligence card, click **Actions**, and select **Delete** from the drop-down menu. See Chapter 7 Delete NSX Intelligence for details.

9 Upgrade your NSX 3.1.x installation to NSX 3.2 or later.

For details, see the *NSX Installation Guide* for version 3.2 or later in the VMware NSX Documentation set.

10 Deploy NSX Application Platform.

See the *Deploying and Managing the VMware NSX Application Platform* document that is included with the NSX Data Center version 3.2 or later in the VMware NSX Documentation set.

11 Prepare NSX Intelligence 3.2 or later for activation.

a In the **System > NSX Application** page, locate the NSX Intelligence card and click **Get Started**.

b Review the information shown in the NSX Intelligence dialog box.

   c   Click **Yes** to confirm that you want to migrate the traffic flow data from earlier NSX Intelligence version and click **Migrate**.

       This step can take some time depending on the size of the data being migrated.

   d   If you decide not to migrate the data, click **No**.

12 When the NSX Intelligence feature card displays the **Activate** button, click **Activate**.

   See Chapter 2 NSX Intelligence Activation and Usage Workflow for details on the activation process.

What to do next

Navigate to **Plan & Troubleshoot > Discover & Take Action** and verify that the data flow visualization is intact and new traffic flow data is getting collected as expected.

Delete NSX Intelligence

7

If for some reason you must delete NSX Intelligence 3.2 or later, use the steps described in this section.

Caution When you delete NSX Intelligence 3.2, the system deletes all the data analytics that have been gathered, along with NSX Intelligence. The action is permanent and results in loss of previously collected data.

Prerequisites

- NSX Application Platform must be in a good state and no active alarms exist.
- You must have NSX Enterprise Administrator user privileges.

Procedure

1. From your browser, log in with Enterprise Administrator privileges to an NSX Manager at https://<nsx-manager-ip-address>.
2. In the NSX Manager UI, select **System > NSX Application Platform**.
3. Navigate to the Features section and in the NSX Intelligence feature card, click Actions and select **Delete**.
4. In the **Delete NSX Intelligence** dialog box, click **Delete**.

   This step might take some time complete. The status of the deletion process is provided on the NSX Intelligence feature card.

Results

After a successful deletion, the NSX Intelligence feature card returns to a ready-to-activate state.

Troubleshooting NSX Intelligence Feature Activation

8

This section provides information on how to resolve problems you might encounter when activating the NSX Intelligence feature on NSX Application Platform.

Read the following topics next:

- NSX Intelligence Activation Failed
- NSX Intelligence Deletion Failed

NSX Intelligence Activation Failed

The NSX Intelligence activation failed.

Problem

The NSX Intelligence activation failed to complete successfully. You might have seen one of the following error messages.

- `Cluster status needs to be STABLE before feature deployment.`

  This error message might appear after you clicked **Activate**.

- `The feature activation took too long. Either the Kubernetes pods failed to come up or the registration with NSX Manager failed. Please contact your Infrastructure Administrator for assistance.`

Cause

The NSX Intelligence activation failure might be due to one of the following reasons.

- The Kubernetes pods used by the NSX Application Platform is in a degraded or unstable status. Because NSX Intelligence is to be hosted on the platform, the activation cannot proceed if the platform is unstable.
- The Kubernetes pods failed to come up or an attempt to register NSX Intelligence with the NSX Manager failed.

Solution

To try to resolve the issue, perform one of the following suggested solutions that corresponds to the cause listed in the previous section.

- If you received the `Cluster status needs to be STABLE before feature deployment` error message, resolve the issue that caused the Kubernetes cluster on which the NSX Application Platform deployed to be in an unstable state. For information, see the "Troubleshooting Issues with the NSX Application Platform" section of the *Deploying and Managing the VMware NSX Application Platform* document that is delivered with the VMware NSX Documentation set for versions 3.2 and later.
- If you received the `The feature activation took too long` error message, use the following information to narrow down the root cause of the failure.

  a Examine the logs for the `cluster-api` pod.

  1 Log in to the NSX Manager appliance with root account.

  2 Run the following command at the system prompt.

  ```
  napp-k logs cluster-api-xxxx -c cluster-api
  ```

  The exact `cluster-api` pod name can be derived from the `napp-k get pods` command. An autogenerated suffix is appended to the `cluster-api` pod name, denoted as *-xxxx* in the above command

  The Helm repository must be reachable from within the `cluster-api` pod. If there is a connectivity issue between the `cluster-api` pod and Helm repository, the `cluster-api` pod might not be able to fetch the Helm chart and render it to create Kubernetes resources for NSX Intelligence. Connectivity depends on the network policies and other firewall rules that your Kubernetes infrastructure administrator put in place. Work with your infrastructure administrator to investigate this issue further and resolve it.

  b Verify if all the desired pods are able to start up. The pod startup depends on the Docker registry being reachable. In the event that the Docker registry is unreachable or the download action fails due to authentication or authorization reasons, the Kubernetes worker node might not be able to download the Docker container image required to run the workloads. Check the connectivity as described in step 1. Docker registries with authentication are not currently supported.

  c Check that all pods reach a `Running` state and all the jobs have completed successfully. Once the Docker container image is downloaded, the pods must be able to start up and run. For pods that are not in `Running` state, check the events using the following `describe` command.

  ```
  napp-k describe pod <pod-name>
  ```

For jobs that are not successfully completed, check the logs using the following command.

```
napp-k logs <pod-name>
```

NSX Intelligence Deletion Failed

The NSX Intelligence feature deletion failed to complete.

Problem

An attempt to delete the NSX Intelligence feature did not complete successfully.

Cause

If while the NSX Intelligence feature is being deleted, the NSX Application Platform gets into an unstable state or connectivity issue occurred between NSX Manager and NSX Application Platform, the deletion can fail.

Solution

Try the **Delete** action again after resolving the issue that caused the NSX Application Platform to be in an unstable state or to have connectivity issues. For more information, see the troubleshooting topics in the *Deploying and Managing the VMware NSX Application Platform* document for version 3.2 or later that is delivered with the VMware NSX Documentation set.

Troubleshooting NSX Intelligence Upgrade

9

This section provides information to help you resolve problems you might encounter when upgrading the NSX Intelligence feature.

Read the following topics next:

- NSX Intelligence Traffic Flow Data Migration Failed

NSX Intelligence Traffic Flow Data Migration Failed

The NSX Intelligence traffic flow data migration did not complete successfully.

Problem

The system encountered an error while attempting to migrate the traffic flow data from the previous NSX Intelligence 1.2.x installation. The `Migration Failed` error message, along with a reason for the failure, appears on the NSX Intelligence feature card.

Cause

There can be any one of the following reasons why the migration failed.

1. The NSX Intelligence 1.2.x appliance is down during the time the migration was attempted.
2. The appropriate ports are not open on the NSX Intelligence 1.2.x appliance.
3. Network latency might have caused the migration to time out.

Solution

Fix the issue displayed with the `Migration Failed` error message and retry the traffic flow data migration again.