Cisco Nexus Dashboard User Guide,
Release 2.0.1
Table of Contents

New and Changed Information ................................................................. 3
  Latest Version of This Document ...................................................... 3
Cisco Nexus Dashboard Overview ......................................................... 4
  Hardware vs Software Stack ............................................................... 4
  Available Form Factors ........................................................................ 4
  Supported Applications ......................................................................... 4
  Cluster Sizing Guidelines ..................................................................... 4
Network Connectivity ................................................................................ 5
  Internal Networks .................................................................................. 6
  Communication Ports ............................................................................ 6
Fabric Connectivity .................................................................................. 7
  Connecting via External Layer 3 Network ........................................... 7
  Connecting the Nodes Directly to Leaf Switches ................................... 9
GUI Overview .......................................................................................... 13
  Dashboard ............................................................................................ 13
  System Overview ................................................................................ 14
  Service Catalog .................................................................................... 15
  System Resource .................................................................................. 15
  Operations ............................................................................................ 16
  Infrastructure ........................................................................................ 16
  Administrative ...................................................................................... 16
Site Management ..................................................................................... 17
  Adding Sites .......................................................................................... 17
  Deleting Sites ......................................................................................... 19
Application Management (Service Catalog) ............................................ 20
  Installing Applications Using App Store ............................................ 20
  Installing Applications Manually ....................................................... 21
  Enabling Applications ........................................................................... 22
  Updating Applications .......................................................................... 24
  Disabling Applications .......................................................................... 24
  Restarting Applications ......................................................................... 24
  Uninstalling Applications ..................................................................... 24
Operations ................................................................................................. 25
  Firmware Management (Cluster Upgrades) ......................................... 25
    Adding Images ..................................................................................... 25
    Upgrading the Cluster ........................................................................ 26
    Deleting Images .................................................................................. 28
Tech Support ............................................................................................... 28
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017-2020 Cisco Systems, Inc. All rights reserved.
New and Changed Information

The following table provides an overview of the significant changes to the organization and features in this guide from the release the guide was first published to the current release. The table does not provide an exhaustive list of all changes made to the guide.

Table 1. Latest Updates

<table>
<thead>
<tr>
<th>Release</th>
<th>Change</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0.1</td>
<td>First release of this document.</td>
<td>—</td>
</tr>
</tbody>
</table>

Latest Version of This Document

This document is available from your Nexus Dashboard GUI as well as online at www.cisco.com. For the latest version of this document, visit https://www.cisco.com/c/dam/en/us/td/docs/dcn/nd/2x/user-guide/cisco-nexus-dashboard-user-guide-2x.pdf.
Cisco Nexus Dashboard Overview

Cisco Nexus Dashboard is a central management console for multiple data center sites and a common platform for hosting Cisco data center operation applications, such as Nexus Insights and Nexus Assurance Engine, which are universally available for all the data center sites and provide real time analytics, visibility, and assurance for network policies and operations. Cisco Multi-Site Orchestrator can also run on Nexus Dashboard as a hosted app. Nexus Dashboard provides a common platform and modern technology stack for these micro-services-based applications, simplifying the life cycle management of the different modern applications and reducing the operational overhead to run and maintain these applications. It also provides a central integration point for external 3rd party applications with the locally hosted applications.

Each Nexus Dashboard cluster consists of 3 master nodes. In addition, you can add up to 4 additional worker nodes to enable horizontal scaling and up to 2 standby nodes for easy cluster recovery in case of a master node failure.

Hardware vs Software Stack

Nexus Dashboard is offered as a cluster of specialized Cisco UCS servers (Nexus Dashboard platform) with the software framework (Nexus Dashboard) pre-installed on it. With addition of other form factors in future releases, the Cisco Nexus Dashboard stack can be decoupled from the hardware and deployed as virtual form factors. For the purposes of this document, we will use "Nexus Dashboard platform" specifically to refer to the hardware and "Nexus Dashboard" to refer to the software stack and the GUI console.

This guide describes how to use the Nexus Dashboard; for hardware installation, see Nexus Dashboard Hardware Installation Guide and for deployment planning and Nexus Dashboard software installation, see the Nexus Dashboard Deployment Guide.

Available Form Factors

Cisco Nexus Dashboard, Release 2.0.1 can be deployed as a physical appliance only. This refers to software stack already deployed on the Nexus Dashboard platform hardware that you purchase.

Supported Applications

For the full list of supported applications and the associated compatibility information, see the Data Center Networking Applications Compatibility Matrix.

Cluster Sizing Guidelines

Nexus Dashboard supports co-hosting of applications. Depending on the type and number of applications you choose to run, you may be required to deploy additional worker nodes in your cluster. For cluster sizing information and recommended number of nodes based on specific use cases, see the Nexus Dashboard Capacity Planning tool.
Adding worker nodes to your cluster is described in Managing Worker Nodes.

Network Connectivity

Cisco Nexus Dashboard is deployed as a cluster, connecting each service node to two networks. When first configuring Nexus Dashboard, you will need to provide two IP addresses for the two Nexus Dashboard interfaces—one connected to the Data Network and the other to the Management Network.

This section describes the purpose and functionality of the networks as they are used by the Nexus Dashboard services. Individual applications installed in the Nexus Dashboard may utilize the two networks for additional purposes, so we recommend consulting the specific application’s documentation in addition to this document for your deployment planning.

**Data network** is used for:

- Nexus Dashboard node clustering
- Application to application communication
- Nexus Dashboard nodes to Cisco APIC nodes communication

  For example, the network traffic for Day-2 Operations applications such as NAE.

**Management Network** is used for:

- Accessing the Nexus Dashboard GUI
- Accessing the Nexus Dashboard CLI via SSH
- DNS and NTP communication
- Nexus Dashboard firmware upload
- Cisco DC App Center (AppStore)

  If you want to use the Nexus Dashboard App Store to install applications as described in Application Management (Service Catalog), the [https://dcappcenter.cisco.com](https://dcappcenter.cisco.com) page must be reachable via the Management Network.

- Intersight device connector

The two interfaces can be in the same or different subnets. In addition, each network’s interfaces across different nodes in the cluster can also be in different subnets.

Except for Nexus Insights application where the two interfaces must be in separate subnets.

The data network must have IP reachability to the fabrics’ in-band IPs for Day-2 Operations apps. For Multi-Site Orchestrator deployments, this network can have in-band and/or out-of-band IP reachability depending on your deployment scenario. The data network uses MTU of 1500 by default, but supports higher MTU as well.
Connectivity between the nodes is required on both networks with the following additional round trip time (RTT) requirements:

You must always use the lowest RTT requirement when deploying the Nexus Dashboard cluster and applications. For example, if you plan to co-host MSO and NI apps, site connectivity RTT must not exceed 50ms.

<table>
<thead>
<tr>
<th>Application</th>
<th>Connectivity</th>
<th>Maximum RTT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nexus Dashboard cluster</td>
<td>Between nodes</td>
<td>150 ms</td>
</tr>
<tr>
<td>Multi-Site Orchestrator (MSO)</td>
<td>Between nodes</td>
<td>150 ms</td>
</tr>
<tr>
<td></td>
<td>To sites</td>
<td>500 ms</td>
</tr>
<tr>
<td>Nexus Insights (NI)</td>
<td>Between nodes</td>
<td>50 ms</td>
</tr>
<tr>
<td></td>
<td>To sites</td>
<td>50 ms</td>
</tr>
<tr>
<td>Network Assurance Engine (NAE)</td>
<td>Between nodes</td>
<td>50 ms</td>
</tr>
<tr>
<td></td>
<td>To sites</td>
<td>50 ms</td>
</tr>
</tbody>
</table>

**Internal Networks**

Two additional internal networks are required for communication between the containers used by the Nexus Dashboard:

- **Application overlay** is used for applications internally within Nexus Dashboard
  
  Application overlay must be a /16 network.

- **Service overlay** is used internally by the Nexus Dashboard.
  
  Service overlay must be a /16 network.

Note that communications between containers deployed in different Nexus Dashboard nodes is VXLAN-encapsulated and uses the data interfaces IP addresses as source and destination. This means that the Application Overlay and Service overlay addresses are never exposed outside the data network and any traffic on these subnets is routed internally and does not leave the cluster nodes. For example, if you had another service (such as DNS) on the same subnet as one of the Overlay networks, you would not be able to access it from your Nexus Dashboard as the traffic on that subnet would never be routed outside the cluster. As such, when configuring these networks, ensure that they are unique and do not overlap with any existing networks or services you may need to access from the Nexus Dashboard cluster nodes.

**Communication Ports**

The following ports are required by the Nexus Dashboard cluster and its applications:

- For traffic to and from the Nexus Dashboard cluster over management network:
  
  Port 53 for DNS
○ Port 443 for HTTPS
○ Ports 22 and 1022 for SSH

• For traffic between the Nexus Dashboard nodes over data network:
  ○ Ports 3379, 3380, 9969, 9979, 15223 for KMS
  ○ Port 19999 for confd
  ○ Ports 30000-30100 for Nexus Dashboard cluster services
  ○ Ports 30500-30600 for Kubernetes

• For traffic between the Nexus Dashboard cluster and Cisco ACI fabrics:
  ○ Port 443 for site manager services
  ○ Ports 2022 and 884 for Network Insights Assurance
  ○ Ports 5640-5656 for Network Insights Resources

Fabric Connectivity

You can connect the Nexus Dashboard cluster to your fabrics in two ways:

• The Nexus Dashboard cluster connected to the fabric via a Layer 3 network.
• The Nexus Dashboard nodes connected to the leaf switches as typical hosts.

Connecting via External Layer 3 Network

Connectivity depends on the type of applications deployed in the Nexus Dashboard:

• If you are deploying Day-2 Operations applications, you will use the data interface IP to communicate to the in-band network of each fabric.
• In addition, if you are deploying Multi-Site Orchestrator, you must also establish connectivity to the out-of-band (OOB) interface of each site’s APIC or DCNM cluster.

If you plan to connect the cluster across an external Layer 3 network, keep the following in mind:

• For ACI fabrics, you must configure an L3Out and the external EPG for Cisco Nexus Dashboard data network connectivity in the management tenant.

  Configuring external connectivity in an ACI fabric is described in Cisco APIC Layer 3 Networking Configuration Guide.

• If you specify a VLAN ID for your data interface during setup of the cluster, the host port must be configured as trunk allowing that VLAN.

  However, in most common deployments, you can leave the VLAN ID empty and configure the host port in access mode.

The following two figures show two distinct network connectivity scenarios when connecting the Nexus Dashboard cluster to the fabrics via an external Layer 3 network. The primary purpose of
each depends on the type of application you may be running in your Nexus Dashboard.

Note that the "L3 Network" and the "Management Network" can be the same network infrastructure, for example in case the Nexus Dashboard nodes have the management and data network interfaces in the same subnet.

Figure 1. Connecting via External Layer 3 Network, Day-2 Operations Applications
Connecting the Nodes Directly to Leaf Switches

Like in the previous example, connectivity depends on the type of applications deployed in the Nexus Dashboard:

- If you are deploying Day-2 Operations applications, you will use the data interface IP to communicate to the in-band network of each fabric.

For ACI fabrics, the data interface IP subnet connects to an EPG/BD in the fabric and must have a contract established to the local in-band EPG in the management tenant. We recommend deploying
the Nexus Dashboard in the management tenant and in-band VRF. Connectivity to other fabrics is established via an L3Out.

- In addition, if you are deploying Multi-Site Orchestrator, you must also establish connectivity to the out-of-band (OOB) interface of each site’s Cisco APIC cluster.

If you plan to connect the cluster directly to the leaf switches, keep the following in mind:

- For ACI fabrics, we recommend configuring the bridge domain (BD), subnet, and endpoint group (EPG) for Cisco Nexus Dashboard connectivity in management tenant.

  Because the Nexus Dashboard requires connectivity to the in-band EPG in the in-band VRF, creating the EPG in the management tenant means no route leaking is required.

- For ACI fabrics, you must create a contract between the fabric’s in-band management EPG and Cisco Nexus Dashboard EPG.

- If you specify a VLAN ID for your data network during setup of the cluster, the Nexus Dashboard interface and the port on the connected network device must be configured as trunk.

  However, in most cases we recommend not assigning a VLAN to the data network, in which case you must configure the ports in access mode.

- For ACI fabrics, if several fabrics are monitored with apps on the Services Engine cluster, L3Out with default route or specific route to other ACI fabric in-band EPG must be provisioned and a contract must be established between the cluster EPG and the L3Out’s external EPG.

The following two figures show two distinct network connectivity scenarios when connecting the Nexus Dashboard cluster directly to the fabrics’ leaf switches. The primary purpose of each depends on the type of application you may be running in your Nexus Dashboard.

Note that the "L3 Network" and the "Management Network" can be the same network infrastructure, for example in case the Nexus Dashboard nodes have the management and data network interfaces in the same subnet.
Figure 3. Connecting via an EPG/BD, Day-2 Operations Applications
Figure 4. Connecting via an EPG/BD, Multi-Site Orchestrator
GUI Overview

After you have deployed the Cisco Nexus Dashboard cluster, you can perform all remaining actions using its GUI. To access Cisco Nexus Dashboard GUI, simply browse to any one of the nodes’ management IP addresses:

https://<node-mgmt-ip>

Depending on the permissions of the user logged in to the Nexus Dashboard GUI, the UI will display only the objects and settings the user is allowed to access. The following sections describe all GUI elements as visible by an admin user. For more information on user configuration and permissions, see Users.

Dashboard

The Dashboard provides a wholistic view of the Cisco Nexus Dashboard. You can use this view to monitor system health, sites, and apps connectivity status.

The Dashboard view contains the following information:

1. You can toggle the Site Map view to change between the geographical view and the detailed list of available sites.
2. The Filter by attributes field allows you to filter the list based on one or more attribute-value pairs.
3. You can click the site **Name** to open a **Details** pane that contains additional information such as IP addresses of the site’s controllers, its inventory, etc.

4. You can click the **Open** link to open the GUI for the site’s controller, such as APIC, Cloud APIC, or DCNM.

5. Similarly, clicking an application in the **Your Services** area will open that application’s GUI.

**System Overview**

The **System Overview** provides information about the Nexus Dashboard application resources usage.

![Nexus Dashboard System Overview](image)

**Figure 6. System Overview**

- The **Overview** tile displays System Status, Cluster Health, and Cisco Intersight Status.

- The **Sites, Apps, and Infra Services** tile displays the **Sites** by connectivity, as well as **Apps** and **Infra Services** by status.

  The status is displayed in number of apps or services that are **healthy**, have **minor** faults, or have **critical** faults.

- The **Inventory** tile provides details of the **nodes**, **pods**, **deployments**, **stateful sets**, **daemon sets**. The following additional information is also shown:
  - **Service Node Storage**
Utilization

Memory

Note that you can click different areas in the System Overview tab to open the corresponding GUI screens where you can see additional details or make configuration changes.

Service Catalog

The Service Catalog category in the left navigation pane provides a single pane of glass access to managing applications in your Nexus Dashboard. Here you can explore, download, and install the applications available on the DC App Center.

Any applications that are already deployed are listed here along with the following information:

- **Name** — the name of the application
- **Description** — description of the application
- **Versions** — number of application versions available
- **Pods** — number of pods used by the application
- **Containers** — number of containers in use by the application

For additional information on managing applications, see [Service Catalog (Application Management)].

System Resource

The System Resources category in the left navigation pane displays the application resources provided by the Nexus Dashboard cluster.

The category contains the following subcategories:

- **Nodes** — displays the details of the service nodes configured and running on the selected app. Up to seven nodes are admitted in a cluster; three master nodes and four worker nodes.
  
  Only worker nodes can be registered using the GUI. Master nodes are brought up using the command line as specified in Deploying the Cisco Nexus Dashboard section

- **Pods** — displays the configured pods running on the selected app.
- **Containers** — displays all the configured containers, container status, IP address, and the configured service node.
- **Deployments** — displays all the deployments, status, IP address, and the configured service node.
- **StatefulSets** — displays all the configured statefulsets, status, IP address, and the configured service node.
- **Services** — displays all the configured services, status, namespaces, IP addresses.
- **Namespaces** — displays the service name, cluster IP, configured ports and the selectors for the
Operations

The Operations category in the left navigation pane displays the actions that can be performed on Cisco Nexus Dashboard.

The category contains the following subcategories:

• Firmware Management — Firmware Management is used to perform cluster (firmware) upgrade or downgrade.
• Tech Support — An administrator can perform technical support collections.
• Audit Logs — Audit Logs are user triggered configuration changes.
• Backup and Restore — Backup and Restore displays the backed up and restored configuration.

Infrastructure

The Infrastructure category in the left navigation pane allows you to management the Nexus Dashboard cluster, Cisco Intersight connector, and application Infra services.

• Cluster Configuration — provides cluster details such as name, app subnet, and service subnet. It also provides details of the NTP and DNS servers.
• Resource Utilization — provides real-time information about the resource utilization of your Nexus Dashboard cluster.
• Intersight — provides access to Cisco Intersight device connector configuration.

The Cisco NIA app depends on the Intersight Device Connector for app to be configured and available on the service node.

• App Infra Services — provides information about the infra services running on your Nexus Dashboard and allows you to restart individual microservices if needed.

Administrative

The Administrative category in the left navigation pane allows you to manage authentication and users.

• Authentication — allows you to configure remote authentication domains as described in Authentication.
• Security — allows you to view and edit the security configurations, such keys and certificates.
• Users — allows you to create and update local Nexus Dashboard users as described in Users or view the users configured on any remote authentication servers you added to the Nexus Dashboard.
Site Management

With Cisco Nexus Dashboard, you can on-board multiple Cisco ACI and Cisco DCNM fabrics as individual sites to the same cluster. Once the fabrics are on-boarded, they can be used by the applications running on the same Cisco Nexus Dashboard cluster.

To add a site, you need its controller's management IP address and credentials. The Cisco Nexus Dashboard nodes must have IP reachability to the site’s controller's management IP. The login credentials are not stored in the Cisco Nexus Dashboard cluster, and are only used to copy the SSL keys to the sites’ controllers. Sites added to the Cisco Nexus Dashboard cluster are not enabled in the apps by default, so you will need to explicitly enable directly from each app’s own GUI.

After you on-board one or more sites to your Nexus Dashboard, you can view them in the Nexus Dashboard GUI by selecting Sites from the left navigation sidebar. You can also use the Sites page to launch directly into any of the site’s GUIs by clicking the Open link next to the site’s name.

If you are using remote authentication to login to your Nexus Dashboard and you have the same login domain and user configured in the site you are launching, you will be able to login to the site's GUI automatically without having to re-authenticate yourself.

Adding Sites

Before you begin

- Fabric connectivity must be already configured.
- While Cisco Nexus Dashboard supports on-boarding Cisco ACI, Cloud ACI, and DCNM fabrics, applications shipping with this release of Nexus Dashboard support on-premises Cisco ACI fabrics only. For additional information about application and fabric compatibility, see the Cisco Data Center Networking Applications Compatibility Matrix.
- If adding a Cisco DCNM site, the site must be running Release 11.5(1) or later.
- If adding a Cisco APIC or Cloud APIC site, the site must be running Release 4.2(4) or later.
- If adding a Cisco APIC site, EPG/L3Out for Cisco Nexus Dashboard data network IP connectivity must be pre-configured.

Refer to Fabric Connectivity for more information.

- If adding a Cisco APIC site and planning to deploy Cisco NIR application:
- IP connectivity from Cisco Nexus Dashboard to Cisco APIC Inband IP over data network must be configured.
- IP connectivity from Cisco Nexus Dashboard to the leaf nodes and spine nodes Inband IPs must be configured.

To add a site:

1. Log in to your Nexus Dashboard GUI.
2. Add a site.

   a. From the left sidebar, select **Sites**.
   b. In top right of the main pane, click the **Actions** menu and select **Add Site**.

   The **Add Site** screen opens.

3. Select the type of site you want to add.

   - **ACI** — for on-premises sites managed by Cisco APIC
   - **DCNM** — for sites managed by Cisco DCNM

4. Provide the site’s information.

   a. If adding an **ACI** site, provide the following:
      - **Site Name** — used throughout the Nexus Dashboard GUI when referring to this site.
      - **Host Name/IP Address** — used to communicate with the site controller.
      - **User Name** and **Password** — used to manage the site.
      - (Optional) **Login Domain** — if you leave this field empty, the site’s local login is used.
      - (Optional) **In-Band EPG** — required when connecting to an ACI fabric via an EPG and bridge domain. For more information on fabric connectivity, see **Fabric Connectivity**.

   You must provide the In-Band EPG if you plan to use this site with the Nexus Insights
b. If adding a DCNM site, provide the following:
   - **Host Name/IP Address** — used to communicate with the site controller.
   - **User Name** and **Password** — used to manage the site.
   - **Sites on DCNM** — click **Add Sites** to select the DCNM fabrics managed by the controller you provided.

5. Click **Add** to finish adding the site.

6. (Optional) Click on the **Geographical Location** map to specify where the site is located.

7. (Optional) Repeat these steps for any additional sites.

## Deleting Sites

*Before you begin*

- Ensure that the site is not used by any applications installed in your Nexus Dashboard.

Deleting a site will cause an interruption to all applications using this site.

- When a Cisco ACI fabric is added as a site to Cisco Nexus Dashboard, some policies may be created in the Cisco APIC. If the Cisco Nexus Dashboard is clean rebooted without deleting the on-boarded site, the policies created on Cisco APIC will not be deleted. To clean up these policies on Cisco APIC, the site should be re-added and deleted.

To remove one or more sites:

1. Log in to your Nexus Dashboard GUI.
2. From the left sidebar, select **Sites**.
3. Select one or more sites that you want to remove.
4. In top right of the main pane, click the **Actions** menu and select **Delete Site**.
5. In the **Confirm Delete** window, provide the login information for the site.

   The **Force Delete** option will remove the site even if it is still being used by one or more applications or if the site is not reachable.

6. Click **OK** to remove the site.
Application Management (Service Catalog)

With Cisco Nexus Dashboard, you can manage all of your applications including their entire lifecycle from the Service Catalog GUI page. This page also allows you to explore the Cisco DC App Center and discover all the applications that are available for the Nexus Dashboard.

![Service Catalog GUI page](image)

*Figure 7. Available Applications*

Installing Applications Using App Store

The App Store screen allows you to deploy applications directly from the Cisco DC App Center.

*Before you begin*

- You must have administrative privileges to install applications.
- The Cisco DC App Center must be reachable from the Nexus Dashboard via the Management Network directly or using a proxy configuration.

  Setting up a proxy is described in [Cluster Configuration](#).

- Keep in mind that only the latest versions of applications are available for installation using the App Store.

  If you want to install a version of an application prior to the latest available in the App Store, you can follow the manual installation procedures as described in [Installing Applications Manually](#).

To install an application from the App Store:

1. Log in to your Nexus Dashboard GUI.
2. Install an application from the App Store.
Figure 8. Cisco DC App Center

a. From the left sidebar, select **Service Catalog**.

b. In the main pane, select the **App Store** tab.

c. In the tile of the application you want to install, click **Install**.

Nexus Dashboard will download the application directly from the DC App Center and install it. After the process completes, the application will be available in your **Service Catalog**.

3. Enable the application.

   By default, after the application is installed, it remains in the **disabled** state. Follow the steps described in **Enabling Applications** to enable it.

   This may take up to 20 minutes depending on the application.

### Installing Applications Manually

Alternatively, you may choose to manually download the applications from the DC App Center and then upload them to the Nexus Dashboard to install.

**Before you begin**

- You must have administrative privileges to install applications.

To manually download an application:

1. Browse to the **Cisco DC App Center**.

2. In the **Search for apps...** field, enter the name of the application you want to download and press Enter.

   For example, **network insights**

3. On the search results page, click the application.
4. On the application page, click **Download**.

5. In the **License Agreement** window, click **Agree and download**.

   This will download the application’s `.aci` file to your system.

To install an application:

1. Log in to your Nexus Dashboard GUI.

2. Upload the application.
   
   a. From the left sidebar, select **Service Catalog**.
   
   b. In top right of the main pane, click the **Actions** menu and select **Upload App**.
   
   c. Choose the app file you downloaded.

   You can choose to upload the application from an **http** service or from your local machine.

   Select **Remote** and provide the URL to the `.aci` file or select **Local**, then click **Choose File**
   and select the application file you downloaded to your local system.

   Finally click **Upload** to upload the app.

3. Wait for the upload and initialization process to finish.

4. Enable the app.

   By default, after the application is installed, it remains in the **disabled** state. Follow the steps
described in [Enabling Applications] to enable it.

   This may take up to 20 minutes depending on the application.

**Enabling Applications**

By default, after the application is installed, it remains in the **disabled** state. This section describes
how to enable an application.

**Before you begin**

- You must have already installed the application as described in [Installing Applications].

To enable an application:

1. Log in to your Nexus Dashboard GUI.

2. From the left sidebar, select **Service Catalog**.

3. In the application’s tile, click **Enable**.

   **Enable <application-name>** window opens.

4. From the **Deployment Profile** dropdown, select the application profile you want to use.

   When you enable an application, you will be prompted to select a **Deployment Profile** as
shown in the following figure, which will define the resources that the Nexus Dashboard will allocate to the application.

![Deployment Profile](image)

**Figure 9. Deployment Profile**

The profiles are defined by the application developer and contain a set of tested and verified resource requirements based on specific use cases. Consult your application’s documentation for more information on the available deployment profiles.

The deployment profile can be changed in one of the following three ways:

- When you first enable the application as described here.
- When you **Restart** the application.
  
  You can restart an application from the (...) menu on the application tile.
- When you upgrade the application.
  
  You will be automatically prompted to select the deployment profile again.

5. Click **Enable** to enable the application.
Updating Applications

The process for updating applications is similar to first deploying it, as described in Installing Applications Using App Store or Installing Applications Manually.

When you upload a new version of an existing application, you will be able to select one of the available versions from the (...) menu on the application tile in the Service Catalog screen.

To update an existing application:

1. Deploy the new version as described in Installing Applications Using App Store or Installing Applications Manually.
2. Navigate to the Service Catalog screen in the Nexus Dashboard GUI.
3. Click the (...) menu on the application’s tile.
5. In the available versions window that opens, click Activate next to the new version.

Disabling Applications

1. Log in to your Nexus Dashboard GUI.
2. From the left sidebar, select Service Catalog.
   All applications installed in your Nexus Dashboard are displayed here.
3. Click … on the application’s tile and select Disable to disable the application.

Restarting Applications

1. Log in to your Nexus Dashboard GUI.
2. From the left sidebar, select Service Catalog.
   All applications installed in your Nexus Dashboard are displayed here.
3. Click … on the application’s tile and select Restart to restart the application.

Uninstalling Applications

Before you begin
You must disable the application before you can delete it.

1. Log in to your Nexus Dashboard GUI.
2. From the left sidebar, select Service Catalog.
   All applications installed in your Nexus Dashboard are displayed here.
3. Click … on the application’s tile and select Delete to remove the application.
Operations

Firmware Management (Cluster Upgrades)

This section describes how to manage different firmware versions and perform cluster upgrades.

The upgrade process involves uploading a new image and then deploying it. As such, the same workflow can be used for cluster firmware downgrades as well.

Downgrading to releases prior to Release 2.0.1 is not supported. If you want to downgrade from Nexus Dashboard to Application Services Engine, you will need to deploy a new cluster as described in Cisco Application Services Engine Deployment Guide.

Adding Images

Before you can upgrade your Nexus Dashboard cluster, you need to make the upgrade image available by adding it using the GUI.

1. Log in to your Nexus Dashboard GUI.
2. Add an image.
   a. From the left sidebar, select Operations > Firmware Management.
   b. In the main pane, select the Images tab.
      The page will list any previously added images.
   c. In top right of the main pane, click the Actions menu and select Add Image.
3. In the Add Firmware Image window that opens, choose whether your image is stored on a remote server or local system.
   a. If specifying a remote image, provide the full URL to the image.
   b. If uploading a local image, click Choose File and select the image file from your local system.
4. Click **Upload** to upload the image.

**Upgrading the Cluster**

*Before You begin*

- Ensure that the master nodes and the cluster are healthy.
- You must have the target image already uploaded to the Nexus Dashboard as described in *Adding Images*.
- You must not make any configuration changes to the cluster, such as adding worker or standby nodes, while the upgrade is in progress.

1. Log in to your Nexus Dashboard GUI.
2. Initiate an update.
   
   a. From the left sidebar, select **Operations > Firmware Management**.
   b. In the main pane, select the **Updates** tab.
   c. Click **Setup Update**.

   If you have previously upgraded the cluster, the last upgrade's details will be displayed in this page instead of the **Setup Update** button. In this case, click the **Modify Details** button at the top right of the screen.

3. In the **Setup/Version Selection** screen, select the target version and click **Next** to proceed.

   If you uploaded multiple images to your Nexus Dashboard, they will be listed here.

4. In the **Setup/Confirmation** screen, review the details of the update and click **Begin Install** to proceed.

   The screen will proceed to the **Install** tab and you will be able to see the progress of each node.
The process can take up to 20 minutes and you can navigate away from this screen in the meantime.

5. Wait for the image installation to complete.

You can check the installation status by navigating back to **Operations > Firmware Management** screen and clicking **View Details** link in the **Last Status** tile.

6. Click **Activate**.

If you navigated away from the installation screen, navigate back to **Operations > Firmware Management** screen and click **View Details** link in the **Last Status** tile.

It may take up to 20 additional minute for all the cluster services to start and the GUI may become unavailable during this process. The page will automatically reload when the process is completed. You can track the activation process in the **Activate** screen as shown below.
Deleting Images

Nexus Dashboard will retain any firmware images that you upload to it. If at any time you want to remove any of the images (for example, from older upgrades), you can use the following steps:

1. Log in to your Nexus Dashboard GUI.
2. From the left sidebar, select Operations > Firmware Management.
3. In the main pane, select the Images tab.
4. Select one or more images.
5. In top right of the main pane, click the Actions menu and select Delete Image.
6. In the Confirm Delete prompt, click OK to confirm.

Tech Support

Tech support enables you to collect logs and activities in the system for further troubleshooting by Cisco TAC. Cisco Nexus Dashboard provides best-effort tech support collection and gives ability to download tech support for individual nodes, the whole cluster, or applications. Tech support files are hosted on the Cisco Nexus Dashboard and can be downloaded at any time.

To collect Tech Support information:

1. Log in to your Nexus Dashboard GUI.
2. Collect Tech Support.
a. From the left sidebar, select **Operations > Tech Support**.

b. In top right of the main pane, click the **Actions** menu and select **Collect Tech Support**.

3. In the **Collect Tech Support** window that opens, provide the description and click **Collect**.

After you begin Tech Support collection, you can see the progress in the same screen.

If for any reason the tech support collection process fails, you can also obtain the same information by logging into each node as the `rescue-user` and running the `acs techsupport collect` command.

4. Download the Tech Support archive.

After the collection is finished, you can download the archive by clicking **Download** next it:

If you want to delete an existing Tech Support package, simply select it in the **Tech Support** screen and choose **Delete Tech Support** from the **Actions** menu.

**Audit Logs**

Nexus Dashboard audit logging is automatically enabled when you first deploy the cluster and captures the operational changes made by the users in the environment.

You can view the audit logs directly in the GUI by selecting **Operations > Audit Logs** from the main
navigation menu.

Note that the logs are not sorted by default; you can sort the list by clicking on any of the column headings.

You can choose to filter the list using the **Filter by attributes** field and providing a specific attribute and value pair.

![Audit Logs](image)

**Figure 10. Audit Logs**

Additionally, to view detailed information about a specific entry, simply click the entry in the list to open the **Details** tab.

# Back up and Restore

This section describes how to back up or restore Nexus Dashboard cluster configuration.

## Creating Configuration Backups

1. Log in to your Nexus Dashboard GUI.
2. Start a back up.

   a. From the left sidebar, select **Operations > Backup & Restore**.
b. In the main pane, select the **Backup Jobs** tab.

c. In top right of the main pane, click the **Actions** menu and select **Backup Configuration**.

3. In the **Backup Configuration** window that opens, provide the **Encryption Key** and the **File Name**.

   The encryption key is used to encrypt the archive and must be at least 8 characters long.

4. Click **Download** to start the backup.

   Cisco Nexus Dashboard does not store configuration backups or encryption keys, so you must download and maintain them outside the Nexus Dashboard cluster.

**Restoring Configuration**

1. Log in to your Nexus Dashboard GUI.

2. Begin restoring a configuration.

   a. From the left sidebar, select **Operations > Backup & Restore**.

   b. In the main pane, select the **Restore Jobs** tab.

   c. In top right of the main pane, click the **Actions** menu and select **Restore Configuration**.

3. Provide the details.
a. Choose **Type**.

You can choose to either **Replace** the existing configuration with the back up or **Merge** them.

b. Provide the **Encryption Key**.

This must be the same encryption key that you used when creating the backup.

c. Click **Choose File** and select the backup file.

Cisco Nexus Dashboard does not store configuration backups, so you must upload the backup file before restoring it.

The file must be in `.tgz` or `tar.gz` format.

4. Click **Import** to start the restore procedure.
Deleting Configuration Backups

1. Log in to your Nexus Dashboard GUI.
2. Delete one or more existing backup files.

   a. From the left sidebar, select **Operations > Backup & Restore**.
   b. In the main pane, select the **Backup Jobs** tab.
   c. Select one or more entries in the list.
   d. In top right of the main pane, click the **Actions** menu and select **Delete Backup Job**.
Infrastructure Management

Cluster Configuration

The cluster configuration GUI screen allows you to configure a number of options specific to the Nexus Dashboard cluster and its nodes.

Only IPv4 addresses are supported for any of the following cluster configuration IP settings.

1. To configure NTP settings, click the Edit icon in the NTP tile.

   By default, the NTP server that you configured when deploying the Nexus Dashboard cluster is listed here.

   You can provide additional NTP servers by clicking +Add NTP Server. Or you can remove existing NTP server by clicking the Delete icon next to it. Keep in mind that at least one NTP server must be configured in your cluster.

2. To add one or more Management Network or Data Network routes, click the Edit icon in the Routes tile.

   In the routes screen that opens:
   
   ◦ To add a management network route, click Add Management Network Routes and provide the new route.
   
   ◦ To add a data network route, click Add Data Network Routes and provide the new route.

3. To configure DNS settings, click the Edit icon in the DNS tile.
By default, the DNS server and search domain that you configured when deploying the Nexus Dashboard cluster are listed here.

You can provide additional DNS servers and search domains by clicking **Add a Provider** or **Add a Search Domain** respectively.

Or you can remove existing DNS server by clicking the **Delete** icon next to it. Keep in mind that at least one NTP server must be configured in your cluster.

4. To configure a proxy for the Nexus Dashboard, click the **Edit** icon in the **Proxy Configuration** tile.

In certain deployment scenarios, such as with a combination of on-premises and cloud sites and the Nexus Dashboard cluster deployed inside a corporate network, you may have to access the internet and the cloud sites through a proxy.

To add a proxy server:

a. Click **Add Server** in the proxy configuration window. Then specify the server's IP address, port, and protocol.

b. If the server requires login credentials, enable the **Username and Password** knob and provide the **Username** and **Password**.

c. If you want to add one or more hosts with a direct connection to the Nexus Dashboard, click **Add Ignore Host** and provide the list of IP address with which the cluster will communicate directly bypassing the proxy.

### Deploying Additional Nodes

Initial cluster deployment is described in *Nexus Nexus Dashboard Deployment Guide*. The following sections describe how to set up additional cluster nodes, such as **worker** nodes used for horizontal scaling of the cluster and **standby** node used for easy failover and cluster recovery.

After you deploy an additional node, you can register and add it to the cluster based on its role:

- For more information about **worker** nodes, see [Managing Worker Nodes](#).
- For more information about **standby** nodes, see [Managing Standby Nodes](#).

### Prerequisites and Guidelines

Before deploying additional nodes, you must:

- Have reviewed and completed the general prerequisites described in the *Cisco Nexus Dashboard Overview*, especially the network and fabric connectivity sections.
- Ensure you are using the correct hardware.

The physical appliance form factor is supported on the original Nexus Dashboard hardware only. The following table lists the PID and specifications of the physical appliance server:
Table 2. Supported Hardware

<table>
<thead>
<tr>
<th>PID</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>SE-NODE-G2</td>
<td>• UCS C220 M5 Chassis</td>
</tr>
<tr>
<td></td>
<td>• 2x 10 core 2.2G Intel Xeon Silver CPU</td>
</tr>
<tr>
<td></td>
<td>• 4x 25G Virtual Interface Card 1455</td>
</tr>
<tr>
<td></td>
<td>• 4x 2.4TB HDDs</td>
</tr>
<tr>
<td></td>
<td>• SSD, NVMe and M2 SATA</td>
</tr>
<tr>
<td></td>
<td>• 256 GB of RAM</td>
</tr>
<tr>
<td></td>
<td>• 1050W power supply</td>
</tr>
</tbody>
</table>

The above hardware supports Nexus Dashboard software only. If any other operating system is installed, the node can no longer be used as a Nexus Dashboard node.

• Have the physical server racked and connected as described in *Nexus Dashboard Hardware Installation Guide*.

• Ensure the hardware is running Nexus Dashboard, Release 2.0.1 or later.

If the new node is running an earlier release, you must install the Release 2.0.1 image on it, as described in *Re-Imaging Nodes*.

### Re-Imaging Nodes

When you first receive the Nexus Dashboard physical hardware, it comes preloaded with the software image. If you simply want to configure the existing software, skip this section and proceed to *Managing Worker Nodes* or *Managing Standby Nodes*.

Alternatively, you can choose to redeploy the software stack on the Nexus Dashboard hardware as described here. For example, if your existing hardware came with an earlier release image and you want to deploy the Release 2.0.1 instead.

**Before You Begin**

• Ensure that you meet the requirements and guidelines described in *Prerequisites and Guidelines* section above.

• You must be able to connect to the server’s CIMC using the Serial over LAN (SoL) port, so ensure that you have the server’s CIMC IP address and an SSH client.


• Ensure that you are running a supported version of Cisco Integrated Management Controller (CIMC).
To re-install the Nexus Dashboard software:

1. Download the Cisco Nexus Dashboard image.
   a. Browse to the Nexus Dashboard page and download the image.
      
   b. Click the Downloads tab.
   c. Choose the Nexus Dashboard version you want to download.
   e. Host the image in a web server in your environment

      You will need to provide an http URL when mounting the image.

2. Deploy the ISO to the server.


   a. SSH into the server's CIMC.
   b. Connect to the virtual media.

      C220-WZP21510DHS# scope vmedia
      C220-WZP21510DHS /vmedia #

   c. Map the Nexus Dashboard image you downloaded to the CIMC-Mapped vDVD.

      C220-WZP21510DHS /vmedia # map-www image http://<ip-address>/<path> <image>

      For example:

      C220-WZP21510DHS /vmedia # map-www image http://172.31.131.47/images nd-dk9.2.0.1.iso

   d. Verify that the image is mounted.
C220-WZP21510DHS /vmedia # show mappings

<table>
<thead>
<tr>
<th>Volume</th>
<th>Map-Status</th>
<th>Drive-Type</th>
<th>Remote-Share</th>
<th>Remote-File</th>
<th>Mount-Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>image</td>
<td>OK</td>
<td>CD</td>
<td>[&lt;ip&gt;/&lt;path&gt;]</td>
<td>nd-dk9.2.0.1.iso</td>
<td>www</td>
</tr>
</tbody>
</table>

e. Reboot the server and connect to its console.

```
C220-WZP23150D4C /vmedia # exit
C220-WZP23150D4C# scope chassis
C220-WZP23150D4C /chassis # power cycle
C220-WZP23150D4C /chassis # exit
C220-WZP23150D4C# connect host
CISCO Serial Over LAN:
Press Ctrl+x to Exit the session
```

f. Select the boot device.

Watch the boot process until you see the following message:

```
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8> Cisco IMC Configuration, <F12> Network Boot
```

Then press F6 and select the virtual media device where you mounted the image (Cisco CIMC-Mapped vDVD1):

```
/------------------------------------\
<table>
<thead>
<tr>
<th>Please select boot device:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Bus 05 Dev 00)PCI RAID Adapter</td>
</tr>
<tr>
<td>UNIGEN PHF16H0CM1-DTE PMAP</td>
</tr>
<tr>
<td>Cisco vKVM-Mapped vHDD1.22</td>
</tr>
<tr>
<td>Cisco CIMC-Mapped vHDD1.22</td>
</tr>
<tr>
<td>Cisco vKVM-Mapped vDVD1.22</td>
</tr>
<tr>
<td>Cisco CIMC-Mapped vDVD1.22</td>
</tr>
<tr>
<td>Cisco vKVM-Mapped vFDD1.22</td>
</tr>
<tr>
<td>UEFI: Built-in EFI Shell</td>
</tr>
<tr>
<td>IBA GE Slot 0100 v1585</td>
</tr>
<tr>
<td>IBA GE Slot 0101 v1585</td>
</tr>
<tr>
<td>Enter Setup</td>
</tr>
<tr>
<td>--------------------------</td>
</tr>
<tr>
<td>^ and v to move selection</td>
</tr>
<tr>
<td>ENTER to select boot device</td>
</tr>
<tr>
<td>ESC to boot using defaults</td>
</tr>
</tbody>
</table>
\------------------------------------/
```

g. Configure the networking.
When the server first boots, you will see the following output:
 awk -F '/|:' '{print $4}'
urlip=172.31.131.47
[' -z 172.31.131.47 ']
break
[' -n http://172.31.131.47/nd-dk9.2.0.1.iso ']
set +e
[' 0 -eq 0 ']
echo 'Configuring network interface'
Configuring network interface
echo 'type static, dhcp, bash for a shell to configure networking, or url to re-enter the url: '
type static, dhcp, bash for a shell to configure networking, or url to re-enter the url:
read -p '? ' ntype
? static
read -p 'address: ' addr
address: 172.23.53.59/21
read -p 'gateway: ' gw
gateway: 172.23.48.1
ip addr add 172.23.53.59/23 dev eno1
ip link set eno1 up
ip route add default via 172.23.48.1
RTNETLINK answers: Network is unreachable
seq 1 2
for count in $(seq 1 2)
ping -c 1 172.31.131.47

For IP address, enter dhcp if there is a DHCP server in your environment or static.
② For the interface, enter the first management port (en01).
③ If you chose static, provide the IP address for the connection.
④ If you chose static, provide the gateway for the connection.

3. After the server boots from the provided image, select the only available installation option.
   It may take up to 20 minutes for the installation process to complete.

   After the image is deployed, you can add the node to your cluster as described in Managing Worker Nodes or Managing Standby Nodes.

Managing Worker Nodes

You can add up to 4 worker nodes to an existing 3-node cluster for horizontal scaling to enable application co-hosting.

For additional information about application co-hosting and cluster sizing, see the [Overview] section of this document.

Adding Worker Nodes

This section describes how to add a worker node to your cluster to enable horizontal scaling

Before you begin

• Ensure that the existing master nodes and the cluster are healthy.
• You must have the node prepared as described in Deploying Additional Nodes.
• Ensure that the node you are adding is powered on.
• Ensure that you have the new node’s CIMC IP address and login information.

   You will need to use the CIMC information to add the new node using the Nexus Dashboard GUI.

To add a worker node:

1. Log in to the Cisco Nexus Dashboard GUI.
2. From the left sidebar, select System Resources > Nodes.
3. In the main pane, select Actions > Add.
   
   The Add New Node screen opens.
4. In the Add New Node screen, provide the node information.
   a. Provide the node’s CIMC IP address and login information, then click Verify.
      
      The server’s serial number will be populated.
   b. Provide the Data Network IP address and gateway.
   c. Provide the Management Network IP address and gateway.
d. From the **Role** dropdown, select **Worker**.

5. Click **Save** to add the node.

The configuration will be pushed to the node and the node will be added to the list in the GUI.

Note that the node’s status will remain unregistered and you will need to register the new node to finish adding it to the cluster, as described in the next step.

6. In the **Status** column of the new node, click **Register**.

The node’s information will be populated based on what you provided in the previous step.

7. Click **Save** to finish registering the node.

The node’s status will change from **unregistered** to **discovering** to **active** as it goes through the discovery and registration process.

8. If you are running Nexus Insights or Network Assurance Engine application, disable and re-enable the application.

After you add the new worker node, you must disable and re-enable the application for its services to be properly distributed to the new node.

### Deleting a Worker node

**Before you begin**

- Ensure that the master nodes and the cluster are healthy.

To delete an existing worker node:

1. Log in to the Cisco Nexus Dashboard GUI.
2. From the left sidebar, select **System Resources > Nodes**.
3. Select the checkbox next to the worker node you want to delete.
4. From the **Actions** menu, choose **Delete** to delete the node.

### Managing Standby Nodes

You can add up to two standby nodes, which you can use to quickly restore the cluster functionality in case one or more master nodes fail by replacing the failed master node with the standby node.

Standby nodes are similar to worker nodes in deployment, initial configuration, and upgrades. However, unlike worker nodes, the cluster will not use the standby nodes for any workloads.

The following two cases are supported:

- **Single master node failure**

  You can use the UI to convert the standby node into a new master node.
Two master nodes failure

You will need to perform manual failover of one of the nodes to restore cluster functionality. Then fail over the second node using standard procedure.

**Adding Standby Nodes**

This section describes how to add a standby node to your cluster for easy cluster recover in case of a master node failure.

**Before you begin**

- Ensure that the existing master nodes and the cluster are healthy.
- You must have the node prepared as described in Deploying Additional Nodes.
- Ensure that the node you are adding is powered on.
- Ensure that you have the new node’s CIMC IP address and login information.

You will need to use the CIMC information to add the new node using the Nexus Dashboard GUI.

To add a standby node:

1. Log in to the Cisco Nexus Dashboard GUI.
2. From the left sidebar, select **System Resources > Nodes**.
3. In the main pane, select **Actions > Add**.

   The **Add New Node** screen opens.

4. In the **Add New Node** screen, provide the node information.
   a. Provide the node's CIMC IP address and login information, then click **Verify**.

   The server’s serial number will be populated.

   b. Provide the **Data Network** IP address and gateway.

   c. Provide the **Management Network** IP address and gateway.

   d. From the **Role** dropdown, select **Standby**.

5. Click **Save** to add the node.

   The configuration will be pushed to the node and the node will be added to the list in the GUI. Note that the node's status will remain unregistered and you will need to register the new node to finish adding it to the cluster, as described in the next step.

6. In the **Status** column of the new node, click **Register**.

   The node's information will be populated based on what you provided in the previous step.

7. Click **Save** to finish registering the node.
The node’s status will change from unregistered to discovering to active as it goes through the discovery and registration process.

**Replacing Single Master Node with Standby Node**

This section describes failover using a pre-configured standby node. If your cluster does not have a standby node, follow the steps described in [Replacing Single Master Node without Standby Node](#) instead.

**Before you begin**

- Ensure that at least 2 master nodes are healthy.

  If two of the master nodes are unavailable, you will need to manually restore the cluster as described in [Replacing Two Master Nodes without Standby Node](#).

- You must have set up and configured the standby nodes as described in [Adding Standby Nodes](#).

- Ensure that the master node you want to replace is powered off.

To failover a single master node:

1. Log in to the Cisco Nexus Dashboard GUI.
2. From the left sidebar, select **System Resources > Nodes**.
3. Select the checkbox next to the Inactive master node that you want to replace.
4. From the **Actions** menu, choose **Failover**.
5. In the **Fail Over** window that opens, select a standby node from the dropdown.
6. Click **Save** to complete the failover.

   The failed master node will be removed from the list and replaced by the standby node you selected. The status will remain Inactive while the services are being restored to the new master node.

   It can take up to 10 minutes for all services to be restored, at which point the new master node’s status will change to **Active**.

**Replacing Two Master Nodes with Standby Nodes**

This section describes failover using a pre-configured standby node. If your cluster does not have a standby node, follow the steps described in [Replacing Two Master Nodes without Standby Node](#) instead.

If only one of your master nodes failed, you can use the GUI to replace it with a standby node as described in [Replacing Single Master Node with Standby Node](#).

However, when two master nodes are unavailable, the entire cluster is put into read-only mode. In this case, most operations including the UI are disabled and no changes can be made to the cluster. This section describes how to fail over one of the failed master nodes to a standby node to recover the cluster and restore normal operations, at which point you can recover the second master node.
using the normal procedure.

**Before you begin**

- Ensure that the master nodes you want to replace are powered off.
- You must have set up and configured the **standby** nodes as described in *Adding Standby Nodes*.

To fail over two master nodes:

1. Log in to the remaining master node via CLI as **rescue-user**.
2. Execute the failover command.

   In the following command, replace `<node1-data-ip>` and `<node2-data-ip>` with the data network IP addresses of the failed nodes:

   ```
   # acs failover --failedIP <node1-data-ip> --failedIP <node2-data-ip>
   ```

   Even though only the first node is failed over, the second failed node you provide is required internally to recover the cluster.

   By default, the healthy master node will automatically pick an available standby node and fail over the first failed node you provide (`<node1-data-ip>`) to it.

   If you would like to provide a specific standby node, you can add `<standby-node-data-ip>` to the above command:

   ```
   # acs failover --failedIP <node1-data-ip> --failedIP <node2-data-ip> \
   --standbyIP <standby-node1-data-ip>
   ```

3. Confirm that you want to proceed.

   ```
   Warning: Failover can be a disruptive operation and should only be performed as last resort option to recover cluster from disasters using standby where two master nodes have lost their state due to hardware faults.
   Proceed? (y/n): y
   ```

   The master node will copy the configuration state to the standby node and both nodes will restart. It may take up to 30 minutes for the nodes to come up and the cluster to be restored. You can check the progress by navigating to the master node's UI.

4. After the cluster is back up, fail over the second failed master node.

   At this point, you can use the standard procedure described in *Replacing Single Master Node with Standby Node*. 

---

45
Deleting Standby Nodes

Before you begin

- Ensure that the master nodes and the cluster are healthy.

To delete an existing standby node:

1. Log in to the Cisco Nexus Dashboard GUI.
2. From the left sidebar, select **System Resources > Nodes**.
3. Select the checkbox next to the standby node you want to delete.
4. From the **Actions** menu, choose **Delete** to delete the node.
Administrative Authentication

You can choose how the users logging into the Nexus Dashboard GUI are authenticated. This release supports local authentication as well as LDAP, RADIUS, and TACACS remote authentication servers.

If configuring external authentication servers:

- You must configure each user on the remote authentication servers.
- All LDAP configurations are case sensitive.

For example, if you have `OU=Cisco Users` on the LDAP server and `OU=cisco users` on the Nexus Dashboard, the authentication will not work.

- For LDAP configurations, we recommend using `CiscoAVPair` as the attribute string. If, for any reason, you are unable to use an Object ID `1.3.6.1.4.1.9.22.1`, an additional Object IDs `1.3.6.1.4.1.9.2742.1-5` can also be used in the LDAP server.

Alternatively, instead of configuring the Cisco AVPair values for each user, you can create LDAP group maps in the Nexus Dashboard.

- Single sign-on (SSO) between the Nexus Dashboard, sites, and applications is available for remote users only.

Configuring Remote Authentication Server

When configuring the remote authentication server for the Nexus Dashboard users, you must add a custom attribute-value (AV) pair, specifying the username and the roles assigned to them.

The user roles and their permissions are the same as for the local users you would configure directly in the Nexus Dashboard GUI as described in Users.

The following table lists the Nexus Dashboard user roles and the AV pair you would use to define the roles on a remote authentication server, such as LDAP.

<table>
<thead>
<tr>
<th>User Role</th>
<th>AV Pair Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>admin</td>
</tr>
<tr>
<td>User Manager</td>
<td>aaa</td>
</tr>
<tr>
<td>Dashboard User</td>
<td>app-user</td>
</tr>
<tr>
<td>Site Administrator (Dashboard role)</td>
<td>site-admin</td>
</tr>
<tr>
<td>Site Manager (App role)</td>
<td>config-manager</td>
</tr>
<tr>
<td>Policy Manager (App role)</td>
<td>site-policy</td>
</tr>
<tr>
<td>Tenant Manager (App role)</td>
<td>tenant-policy</td>
</tr>
</tbody>
</table>

The AV pair string format differs when configuring a read-write role, read-only role, or a
A typical string includes the domain, followed by the read-write roles separated from the read-only roles using the slash (/) character; individual roles are separated by the pipe (|) character:

```
shell:domains=<domain>/<writeRole1>|<writeRole2>/<readRole1>|<readRole2>
```

In this release, only the all domain is supported and is required for consistency with the APIC AV pair format in order to support the single sign-on (SSO) feature.

For example, the following string illustrates how to assign the Tenant Manager and Policy Manager roles to a user, while still allowing them to see objects visible to the User Manager users:

```
shell:domains=all/tenant-policy|site-policy/aaa
```

Note that if you want to configure only the read-only or only read-write permissions for a user, you must still include the slash (/) character. The following examples show how to set just the read-write or read-only access to the objects available to Site Administrator role:

- Read-only: `shell:domains=all//site-admin`
- Read-write: `shell:domains=all/site-admin/`

### Adding LDAP as Remote Authentication Provider

**Before you begin**

- You must have at least one user already configured on the LDAP server as described in Configuring Remote Authentication Server.

You will need to use an existing user for end-to-end verification of LDAP configuration settings.

To add an LDAP remote authentication provider:

1. Log in to your Nexus Dashboard GUI.
2. Add an authentication domain.
a. From the left sidebar, select **Administrative > Authentication**.

b. In top right of the main pane, click the **Actions** menu and select **Create Login Domain**.

3. In the **Create Login Domain** screen that opens, provide domain details.
   a. Provide the **Name** for the domain.
   b. (Optional) Provide its **Description**.
   c. From the **Realm** dropdown, select **Ldap**.
   d. Then click +**Add Provider** to add a remote authentication server.

   The **Add Provider** window opens.

4. Provide the remote authentication server details.
   a. Provide the **Hostname** or **IP Address** of the server.
   b. (Optional) Provide the **Description** of the server.
   c. Provide the **Port** number.

   The default port is **389** for LDAP.

d. Provide the **Base DN** and **Bind DN**.

   The Base DN and Bind DN depend on how your LDAP server is configured. You can get the Base DN and Bind DN values from the distinguished name of the user created on the LDAP server.

   Base DN is the point from which the server will search for users. For example, **DC=nd,DC=local**.

   Bind DN is the credentials used to authenticate against the server. For example, **CN=admin, CN=Users,DC=nd,DC=local**.

e. Provide and confirm the **Key**.

   This is the password for your Bind DN user. Anonymous bind is not supported, so you must provide a valid value in these fields.

f. Specify the **Timeout** and number of **Retries** for connecting to the authentication server.

g. Provide the **LDAP Attribute** field for determining group membership and roles.

   The following two options are supported:

   - **ciscoAVPair** (default) — used for LDAP servers configured with Cisco AVPair attributes for user roles.
   - **memberOf** — used for LDAP servers configured with LDAP group maps. Adding a group map is described in a following step.

h. (Optional) Enable **SSL** for LDAP communication.

   If you enable SSL, you must also provide the **SSL Certificate** and the **SSL Certificate**
**Validation** type:

- **Permissive**: Accept a certificate signed by any certificate authority (CA) and use it for encryption.
- **Strict**: Verify the entire certificate chain before using it.

i. (Optional) Enable **Server Monitoring**.

If you choose to enable monitoring, you must also provide the **Username** and **Password** for it.

j. In the **Validation** fields, provide a **Username** and **Password** of a user already configured on the LDAP server you are adding.

Nexus Dashboard will use this user to verify the end-to-end authentication to ensure that the settings you provided are valid.

k. Click **Save** to complete provider configuration.

l. Repeat this step for any additional LDAP authentication servers you want to use with this domain.

5. (Optional) Enable and configure **LDAP Group Map Rules**.

If you want to authenticate your LDAP users using Cisco AV pair strings, skip this step.

a. In the **LDAP Auth Choice**, select **LDAP Group Map Rules**.

b. Click **Add LDAP Group Map Rule**.

The **Add LDAP Group Map Rule** window opens.

c. Provide the **Group DN** for the group.

d. Select one or more **Roles** for the group.

e. Click **Save** to save the group configuration.

f. Repeat this step for any additional LDAP groups.

6. Click **Create** to finish adding the domain.

### Adding Radius or TACACS as Remote Authentication Provider

**Before you begin**

- You must have at least one user already configured on the remote authentication server as described in **Configuring Remote Authentication Server**.

You will need to use an existing user for end-to-end verification of the provider configuration settings.

To add a Radius or TACACS remote authentication provider:

1. Log in to your Nexus Dashboard GUI.
2. Add an authentication domain.

a. From the left sidebar, select **Administrative > Authentication**.
b. In top right of the main pane, click the **Actions** menu and select **Create Login Domain**.

3. In the **Create Login Domain** screen that opens, provide domain details.
   a. Provide the **Name** for the domain.
   b. (Optional) Provide its **Description**.
   c. From the **Realm** dropdown, select **Radius** or **Tacacs**.
   d. Then click **+Add Provider** to add a remote authentication server.

   The **Add Provider** window opens.

4. Provide the remote authentication server details.
   a. Provide the **Hostname** or **IP Address** of the server.
   b. (Optional) Provide the **Description** of the server.
   c. Choose **Authorization Protocol** used by the server.

   You can choose **PAP**, **CHAP**, or **MS-CHAP**.
   d. Provide the **Port** number.

   The default port is **1812** for RADIUS and **49** for TACACS.
   e. Provide and confirm the **Key**.

   This is the password used for connecting to the provider server.
   f. (Optional) Choose whether you want to enable **Server Monitoring**.

   If you choose to enable monitoring, you must also provide the **Username** and **Password** for it.
   g. In the **Validation** fields, provide a **Username** and **Password** of a user already configured on the remote server you are adding.

   Nexus Dashboard will use this user to verify the end-to-end authentication to ensure that
the settings you provided are valid.

h. Click **Save** to complete provider configuration.
i. Repeat this step for any additional remote authentication servers.

5. Click **Create** to finish adding the domain.

### Editing Remote Authentication Domains

If you want to make changes to a domain you have created:

1. Log in to your Nexus Dashboard GUI.
2. From the left sidebar, select **Administrative > Authentication**.
3. Double-click the domain you want to edit in the list.

   The domain’s details screen opens.

4. In the top right of the screen, click the **Edit** icon.

   You cannot change the name and the type of the authentication domain, but you can make changes to the description and provider configuration.

   If you make any changes to the login domain, including simply updating the description, you must re-enter the **key** for all existing providers.

### Choosing Default Authentication Domain

1. Log in to your Nexus Dashboard GUI.
2. Choose the default login domain.

   a. From the left sidebar, select **Administrative > Authentication**.
   b. In top right of the **Default Authentication** tile, click the **Edit** icon.

   The **Default Authentication** window opens.

3. In the **Default Authentication** that opens, choose the **Login Domain** from the dropdown.
Deleting Remote Authentication Domains

1. Log in to your Nexus Dashboard GUI.
2. From the left sidebar, select **Administrative > Authentication**.
3. Select one or more domains from the list.
4. In top right of the main pane, click the **Actions** menu and select **Delete Login Domain**.
5. In the **Confirm Delete** prompt, click **OK** to confirm.

**Users**

The **Users** GUI page allows you to view and manage all users that have access to the Nexus Dashboard.

The **Local** tab displays all local users while the **Remote** tab displays users that are configured on the remote authentication servers you have added as described in the **Authentication** section.

**Roles and Permissions**

Cisco Nexus Dashboard allows access according to a user’s roles defined by role-based access control (RBAC). Roles are used in both local and external authentication and apply to either the Nexus Dashboard or the applications running in it. The following user roles are available in Nexus Dashboard:

- **Administrator** — allows access to all objects and configurations.
- **User Manager** — allows access to users and authentication configurations.
- **Dashboard User** — allows access only to the Dashboard view and launching applications; does not allow any changes to the Nexus Dashboard configurations.
- **Site Administrator** — allows access to configurations related to the sites on-boarding and configuration.
- **Site Manager** — allows application user to manage the sites used by that application.
- **Policy Manager** — allows application user to view policy objects.
- **Tenant Manager** — allows application user to view tenants.

Each role above is associated with a set of permissions, which in turn are used to show relevant and hide irrelevant elements from the user’s view in the GUI. For example, the following figure shows GUI screen as seen by a user with **User Manager** and **Site Administrator** permissions only with other categories unavailable:
Figure 12. Role-Based GUI Access

Depending on the permissions you set for the user, the UI will display only the objects and settings the user is allowed to access.

The same roles can be configured on a remote authentication server and the server can be used to authenticate the Nexus Dashboard users. Additional details about remote authentication are available in the Authentication section.

Adding Local Users

1. Log in to your Nexus Dashboard GUI.
2. Create a new local user.
   a. From the left sidebar, select Administrative > Users.
   b. In top right of the main pane, click the Actions menu and select Create Local User.
3. In the Create Local User screen that opens, provide user details.
   a. Provide the User ID that will be used for loggin in.
   b. Provide and confirm the initial Password.
   c. Provide the First Name, Last Name, and Email Address for the user.
   d. Choose the user's Roles and Privileges.

   You can select one or more roles for each user. The available roles and their permissions are described in Roles and Permissions.

   For all of the user roles you select, you can choose to enable read-only or read-write access. In case of read-only access, the user will be able to view the objects and settings allowed by their user Role but unable to make any changes to them.

   e. Click Create to save the user.

Editing Local Users

1. Log in to your Nexus Dashboard GUI.
2. Open user details screen.
a. From the left sidebar, select **Administrative** > **Users**.

b. In the main pane, click on the user's name.

c. In the details pane that opens, click the **Details** icon.

3. In the `<user-name>` details screen that opens, click the **Edit** icon.

4. In the **Edit User** screen that opens, update the settings as necessary.
Cisco Intersight

Cisco Intersight is a Software-as-a-Service (SaaS) infrastructure management platform that is augmented by other intelligent systems. It provides global management of the Cisco Unified Computing System (Cisco UCS) and Cisco HyperFlex hyperconverged infrastructure, Cisco APIC, and other platforms including Cisco Nexus Dashboard.

Data center apps, such as Cisco Nexus Insights, connect to the Cisco Intersight portal through a Device Connector that is embedded in the management controller of each system, in this case your Nexus Dashboard platform. Device Connector provides a secure way for the connected devices to send information and receive control instructions from the Cisco Intersight portal, using a secure internet connection.

When an Intersight-enabled device or application starts, the Device Connector starts at boot by default and attempts to connect to the cloud service. If the Auto Update option is enabled, the Device Connector is automatically updated to the latest version through a refresh by the Intersight service when you connect to Cisco Intersight. For more information on the Auto Update option, see Configuring Device Connector Settings.

For additional information on Cisco Intersight, see https://www.intersight.com/help/getting_started.

If you upgraded from Application Services Engine and your Intersight device connector is claimed with a proxy configured, you will need to re-configure the proxy in the Cluster Configuration screen. For more information, see Cluster Configuration.

Configuring Device Connector Settings

This section describes how to configure the basic Device Connector settings.

1. Log in to your Nexus Dashboard GUI.
2. From the left sidebar, select Infrastructure > Intersight.
3. In the top right of the main pane, click Settings.
4. Click the General tab to configure basic options.
   a. Use the Device Connector knob to enable or disable the Device Connector.
      
      This enables you to claim the device and leverage the capabilities of Intersight. If it is disabled, no communication is allowed to Cisco Intersight.

   b. In the Access Mode area, choose whether to allow Intersight the capability to make changes to this device.
      
      ▪ Allow Control (default)—enables you to perform full read or write operations from the cloud based on the features available in Cisco Intersight.
      ▪ Read-only—ensures that no changes are made to this device from Cisco Intersight.

      For example, actions such as upgrading firmware or a profile deployment will not be...
allowed in read-only mode. However, the actions depend on the features available for a particular system.

c. Use the **Auto Update** knob to enable automatic Device Connector updates.

We recommend that you enable automatic updates so that the system automatically updates the Device Connector software. When enabled, the Device Connector will automatically upgrade its image whenever there is any upgrade push from Intersight.

If you disable the automatic updates, you will be asked to manually update the software when new releases become available. Note that if the Device Connector is out-of-date, it may be unable to connect to Cisco Intersight.

5. Click **Save** to save the changes.

6. Click the **Certificate Manager** tab if you want to import additional certificates.

By default, the device connector trusts only the built-in certificate. If the device connector establishes a TLS connection and a server sends a certificate that does not match the built-in certificate, the device connector terminates TLS connections because it cannot determine if the server is a trusted device.

You can choose to upload additional certificates by clicking the **Import** button in this screen. The imported certificates must be in the `.pem` (base64 encoded) format. After a certificate is successfully imported, it is listed in the list of **Trusted Certificates** and if the certificate is correct, it is shown in the **In-Use** column.

You can click the **View** icon at the end of the certificate’s row to view its details such as name, issue and expiration dates.

---

**Claiming the Device**

This section describes how to claim the Nexus Dashboard platform as a device for Cisco Intersight.

*Before you begin*

You must have configured the Intersight Device Connector as described in [Configuring Device Connector Settings](#).

To claim the device:

1. Log in to your Nexus Dashboard GUI.
2. From the left sidebar, select **Infrastructure > Intersight**.
3. Check whether the Device Connector is already configured.
   - If you see a green dotted line connecting **Internet to Intersight** in the **Device Connector** page and the text **Claimed**, then your Intersight Device Connector is already configured and connected to the Intersight cloud service, and the device is claimed. In this case, you can skip the rest of this section.
   - If you see a red dotted line connecting to **Internet** in the **Device Connector** page, you must
configure a proxy for your Nexus Dashboard cluster to be able to access the Internet, as described in Cluster Configuration before continuing with the rest of this section.

- If you see a yellow dotted line and a caution icon connecting Internet to Intersight in the Device Connector page and the text Not Claimed, then your Intersight Device Connector is not yet configured and connected to the Intersight service, and the device is not yet claimed. Follow these procedures to configure the Intersight Device Connector and connect to the Intersight cloud service, and claim the device. In this case, proceed with the rest of the steps to configure the device.

4. If necessary, update the device connector software.

If there is a new Device Connector software version available and you do not have the Auto Update option enabled, you will see a message at the top of the screen informing you that Device Connector has important updates available. Enabling the auto-update feature is described in Configuring Device Connector Settings.

To manually update the Device Connector, click the Update Now link.

5. Note down the Device ID and Claim Code listed on the Nexus Dashboard’s Intersight page.


7. In the Cisco Intersight cloud site, click Devices tab and then click Claim a New Device.

The Claim a New Device page appears.

8. Provide the Device ID and Claim Code you copied from the Nexus Dashboard’s Intersight page.
9. Click **Claim**.

The message "Your device has been successfully claimed" is displayed in the **Claim a New Device** page. Also, in the main page, you should see your Cisco Nexus Dashboard platform, with **Connected** shown in the **Status** column.

10. Navigate back to the Nexus Dashboard’s **Intersight** page and verify that the system was claimed successfully.

You should see green dotted lines connecting **Internet** to **Intersight** in the **Device Connector** page, and the text **Claimed**.

![Intersight Device Connector](image)

You may need to click **Refresh** in top right of the page to update the latest status.

**Unclaiming the Device**

To unclaim the Nexus Dashboard as a device from Intersight:

1. Log in to your Nexus Dashboard GUI.
2. From the left sidebar, select **Infrastructure > Intersight**.
3. In the main pane, click **Unclaim**.
Troubleshooting

Useful Commands

You can log in to any of the cluster nodes as rescue-user for a limited access to system data. You can use the following commands to perform various operations in Cisco Nexus Dashboard.

Cluster Troubleshooting:
- `acs health` — displays cluster health information and any existing issues.
- `acs cluster config` — displays cluster configuration.
- `acs cluster masters` — displays master nodes configuration.
- `acs cluster workers` — displays worker nodes configuration.
- `acs cluster standbys` — displays standby nodes configuration.
- `acs techsupport collect` — collects Tech Support information.
- `acs version` — returns the Nexus Dashboard version.

Resetting Devices:
- `acs reboot` — reboots the node.
- `acs reboot clean` — removes all data for Nexus Dashboard and applications, but preserves the Nexus Dashboard bootstrap configuration and pod images.

When you first bring up your Nexus Dashboard cluster, initial deployment process installs all required pod images. Retaining pod images will speed up cluster bring up after reboot.

- `acs reboot clean-wipe` — removes all data for Nexus Dashboard and applications including application images, but preserves the Nexus Dashboard bootstrap configuration.

When the cluster boots up again, pod images will be re-installed.

- `acs reboot factory-reset` — removes all data for Nexus Dashboard and applications including cluster bootstrap configuration, but preserves application images.

When you first bring up your Nexus Dashboard cluster, initial deployment process installs all required pod images. Retaining pod images will speed up cluster bring up.

- `acs reboot factory-wipe` — removes all data for Nexus Dashboard and applications, including application images and cluster bootstrap configuration.

When the cluster boots up again, the pod images will be re-installed.

System and Connectivity Troubleshooting:
- The `/logs` directory is mounted into the rescue-user container and can be inspected with standard tools.
- The `ping` command is supported with most options.
• The `ip` command supports a read-only subset of commands, including `ip addr show` and `ip route show`.

• The `esctl` command can be used to debug elastic search.

• The `kubectl` command can be used to support read-only kubectl commands.

**Application Information:**

• The `acs apps instances` commands displays all applications running on the cluster.

• The `acs apps actions` command displays the history operations done on the applications, such as installations, upgrades, or deletions.

## Manual Upgrades

Typically, you would use the procedure described in Firmware Management (Cluster Upgrades) section to upgrade your cluster.

If for any reason you want to perform a manual upgrade of each node, you can use the following steps instead:

1. Log in to one of the nodes as `rescue-user`.
2. Copy the upgrade ISO image file into the `/tmp` directory on the node.
3. Start the upgrade.

```
# acs installer update -f /tmp/nd-dk9.2.0.1a.iso
Warning: This command will initiate node update to new version.
Proceed? (y/n): y
Update in Progress ... Do not press Ctrl+C
```

4. Wait for the upgrade to complete.

```
Update succeeded, reboot your host
```

5. Reboot the node.

```
# acs reboot
This command will restart this device, Proceed? (y/n): y
```

6. Verify the node is healthy.

```
# acs health
All components are healthy
```

7. After the first node is successfully upgraded, repeat the steps on the other two nodes in turn.
You must update one node at a time; no more than a single node should be unavailable at any time.

8. Once all nodes are up with new version and healthy, run post-upgrade tasks.

You can run the following command on all nodes in parallel.

```
# acs installer post-update
Warning: This command will run the post-update scripts. Proceed? (y/n): y
Update in Progress ... Do not press Ctrl^C
Post-update succeeded
```

**AppStore Errors**

When attempting to access the Service Catalog > AppStore tab in the Nexus Dashboard GUI, you may encounter the following error:

```
{
    "error": "There was a problem proxying the request"
}
```

*Cause*

When a master node where the AppStore service is running fails, it may take up to 5 minutes for the AppStore services to relocate to another master node.

*Resolution*

Simply wait for the services to recover and refresh the page.

**Factory Reset**

You can reset the whole cluster by running the following command on each node:

```
# acs reboot factory-reset
```

Doing this will lose all cluster configuration and applications and you will need to rebuild the cluster.

**Replacing Nodes without Standby Node (RMA)**

This section describes how to recover from one or two master node failures in a cluster without standby nodes. The RMA procedure is for hardware issues that require it to be physically replaced; if the node is simply in a bad software state, you can use the `acs reboot clean` commands instead.
Replacing Single Master Node without Standby Node

If your cluster has a standby node configured, we recommend using the steps described in Replacing Single Master Node with Standby Node instead.

Before you begin

- Ensure that at least 2 master nodes are healthy.
- If two of the master nodes are unavailable, you will need to manually restore the cluster as described in Replacing Two Master Nodes with Standby Nodes
- Ensure that the master node you want to replace is powered off.
- You must have the new node prepared as described in Deploying Additional Nodes.
- Ensure that you have the same CIMC IP address and login information on the new node as you configured for the failed node.

The remaining master node will use the CIMC information to restore configuration to the new node.

- Ensure that the new node is powered on and note down its serial number.

To replace a single failed master node:

1. Log in to your Nexus Dashboard GUI using the management IP of one of the other master nodes.
2. From the left sidebar, select System Resources > Nodes.
3. In the nodes list, find the Serial number of the node you want to replace and ensure that the node’s Status shows Inactive.
4. In the Nexus Dashboard’s Nodes screen, select the inactive node by clicking the checkbox next to it.
5. From the Actions menu, select Replace.
6. In the New Serial Number field, provide the serial number of the new node and click Replace.

After the process is completed, you will see the serial number of the old node updated to the new node’s serial number and the status will change to Active once the new master has successfully joined the cluster.

Replacing Two Master Nodes without Standby Nodes

If your cluster has a standby node configured, we recommend using the steps described in Replacing Two Master Nodes with Standby Node instead.

Because the cluster requires at least two master nodes to be available, you cannot simply add another master. Instead, you must restore the cluster configuration from the remaining healthy node to the two new nodes.

Before you begin

- Ensure that the master nodes you want to replace are powered off and note down their serial
numbers and network configuration.

You will need to provide the failed nodes’ serial numbers, data network, and management network information during the recovery process.

- You must have the new nodes prepared as described in Deploying Additional Nodes.
- Ensure that the new nodes are running the same Nexus Dashboard software version as the remaining healthy node.
- Ensure that you have the same CIMC IP addresses and login information on the new nodes as you configured for the failed nodes.

The remaining master node will use the CIMC information to restore configuration to the new node.

- Ensure that the new nodes are powered on and note down their serial numbers.

You will need to provide the new nodes’ serial numbers during the recovery process.

To replace two failed master nodes:

1. Power on the two new master nodes and note down the serial numbers of the new nodes.

2. Log in to your remaining healthy master node as rescue-user and run the recovery command.

   In the following command, provide the serial numbers of the two failed nodes and two new nodes as well as the same network configuration parameters as you used for the two failed nodes:

   ```
The backslash (\) character indicates continuation of the same command, do not enter this character as you enter the entire command.

   acs rma --oldSerial WZP22140ZLP --newSerial WZP23390GLM \
   --cimcIP 10.10.1.10 --cimcUser admin --cimcPassword <password> \
   --mgmtSubnet 10.10.1.1/24 --mgmtGateway 10.10.1.1 \
   --dataSubnet 100.11.11.1/24 --dataGateway 100.11.11.1 --dataVlan 201 \
   --oldSerial WZP22470ZLR --newSerial WZP23380ZXV \
   --cimcIP 10.10.1.12 --cimcUser admin --cimcPassword <password> \
   --mgmtSubnet 10.10.1.13/24 --mgmtGateway 10.10.1.1 \
   --dataSubnet 100.12.12.12/24 --dataGateway 100.12.12.1 --dataVlan 202
   ```

3. Wait for the nodes to come up and the cluster to recover.

   Depending on the number of applications installed in the cluster, it may take 20-60 minutes for the cluster to recover.

4. Verify that the cluster is healthy.
   a. Log in to your Nexus Dashboard GUI using the management IP of one of the master nodes.
   b. From the left sidebar, select System Resources > Nodes.
c. Verify that all nodes are listed as Active

**Replacing Worker Nodes**

When replacing a failed work node, you simply delete the Inactive node from the GUI and then deploy a brand new worker node as you typically would.

*Before You begin*

- Ensure that the worker node you want to replace is powered off.

To replace a failed worker node:

1. Log in to your Nexus Dashboard GUI.
2. From the left sidebar, select **System Resources > Nodes**.
3. In the nodes list, find the **Serial** number of the node you want to replace and ensure that the node's **Status** shows **Inactive**.
4. Select the inactive node by clicking the checkbox next to it.
5. From the **Actions** menu, select **Delete**.
   
   This will remove the node from the list.

6. Power on the new node and add it as a new **worker** node to the cluster as described in **Managing Worker Nodes**.

   Use the same configuration parameters as you used to set up the old node.