Managing System

This chapter contains the following sections:

About Slices

The slices screen provides a way for you, as a network administrator, to partition networks into many logical networks. This feature allows you to create multiple disjoint networks and assign different roles and access levels to each one. Each logical network can be assigned to departments, groups of individuals, or applications. Multiple disjoint networks can be managed using the Cisco Nexus Data Broker application.

The slices are created based on the following criteria:

- Network devices—The devices that can be used in the slice.

  Network devices can be shared between slices.

- Network device interfaces—The device interfaces that can be used in the slice.

  Network device interfaces can be shared between slices.

- Flow Specification—A combination of source and destination IP, protocol, and source and destination transport ports used to identify the traffic that belongs to the slice.

Flow specifications can be assigned to different slices if the associated network devices and interfaces are disjointed.

Note You can also use VLAN IDs to segregate the slice traffic.

Slices must be created by a Cisco Nexus Data Broker user with the Network Administrator role. After creation, the slices can be managed by a user with the Slice Administrator role.

As part of the initial NDB build, one slice is available and is called the Default slice. The following configurations can be performed only on the default slice of the NDB controller:

- Adding a new device
- Editing global configurations for devices
- Changing profiles for users
- Changing the parameters for users and associated roles
- Fixing inconsistent device and connection flows

Adding a Slice

Step 1 Log in to the Cisco Nexus Data Broker GUI using your administrator credentials.

Step 2 Navigate to **Administration** > **System** > **Slices**.

Step 3 To add a slice, click the **Add Slice** button.

The **Add Slice** slide-in pane is displayed.

Step 4 Enter the required details for the slice that you want to create in the **Add Slice** pane.

Step 5 Click **Add Slice**.

You can view the new slice in the **Slices** tab.

Note After a new slice is added, the default slice is in *read-only* mode. If an active port configuration and/or connection is present on the default slice, then, it is rendered unavailable.

The devices added to a slice are displayed in the slice. For example, if device D1 is added to slice S1, and if the device goes into maintenance mode (or failed state or not ready state), the device is no longer displayed on S1, but is displayed on the default slice.

Adding Nodes and Ports to a Slice

Note While a switch can be a part of multiple slices, a port can be a part of only one slice at any given time.

Before you begin

- Ensure that the ports are not configured before you add them to a slice.

Step 1 Navigate to **Administration** > **System** > **Slices**.

Step 2 From the list of slices in the **Slices** tab, click to choose the slice for which you want to add the nodes and ports.

The **Slice Details** slide-in pane is displayed with the slice name that you chose.

Step 3 To add a node to a slice, choose a node from the **Select Node** drop-down list and then select the list of ports from the **Add Ports To Slice** menu.

Step 4 Click **Add Port(s)**.

Ensure to have all the ports of a device on the same slice.

Removing a Node from the Slice

Before you begin

- Ensure that you remove the connections, UDFs, filters, and port configurations,in a slice before you remove it.

Step 1 Log in to the Cisco Nexus Data Broker GUI using your administrator credentials.

Step 2 Navigate to **Administration** > **System** > **Slices**.

The list of slices is displayed.

Step 3 From the list of slices, choose the slice that you want to remove.

The **Slice Details** slide-in pane is displayed with the details of the slice.

Step 4 Make a note of the ports and nodes added to the slice.

Step 5 You must remove the connections, port configurations and ports in a slice before you remove it.

To remove the connections:

a) Navigate to **Configurations** > **Connections** .

b) Select the required connection and click **Remove Connections** .

To remove the port configurations:

a) Navigate to **Configurations** > **Port Definition** > **Port Configurations** .
b) Select the required port and click **Remove Port Configuration** .

The port configurations and connections have been removed from the slice.

Step 6 Navigate to **Administration** > **System** > **Slices**.

Step 7 Select the **default** slice from the drop-down list on top of the window.

Step 8 Choose the slice from which a node is to be removed.

The **Slice Details** slide-in pane is displayed with the appropriate slice details.

Step 9 Select all the ports associated with the nodes to be removed from the slice and click **Remove Ports**.

The ports are removed from the slice.

Removing a Slice

Before you begin

- Ensure that you remove the connections, UDFs, filters, and port configurations,in a slice before you remove it.

Step 1 Log in to the Cisco Nexus Data Broker GUI using your administrator credentials.

Step 2 Navigate to **Administration** > **System** > **Slices**.

The list of slices is displayed.

Step 3 From the list of slices, choose the slice that you want to remove.

The **Slice Details** slide-in pane is displayed with the details of the slice.

Step 4 Make a note of the ports and nodes added to the slice.

Step 5 You must remove the connections, port configurations and ports in a slice before you remove it.

To remove the connections:

a) Navigate to **Configurations** > **Connections** .
b) Select the required connection and click **Remove Connections** .

To remove the port configurations:

a) Navigate to **Configurations** > **Port Definition** > **Port Configurations** .
b) Select the required port and click **Remove Port Configuration** .

The port configurations and connections have been removed from the slice.

Step 6 Navigate to **Administration** > **System** > **Slices**.

Step 7 Select the **default** slice from the drop-down list on top of the window.

Step 8 From the list of slices, choose the slice(s) that you want to remove and click **Remove Slice** button.

The **Remove Slice** slide-in pane is displayed.

Step 9 Click **Remove Slice** in the pane.

Adding a Flow Specification

Before you begin

Create a slice before you add a flow specification.

Note Be default, a flow specification is bidirectional.

Step 1 Navigate to the **System** tab under **Administration** and click **+ Flow Spec** to add a flow specification for the selected slice.

Step 2 In the **Add Flow Spec** dialog box, complete the following fields:

Name	Description
Name field	The name that you want to use for the flow specification.
VLAN field	The VLAN ID or the range of VLAN IDs that you want to use for the flow specification.
Source IP field	The source IP address that you want to use for the flow specification.
Destination IP field	The destination IP address that you want to use for the flow specification.
Protocol field	The IP protocol number in decimal format that you want to use for the flow specification.
Source Port field	The source port that you want to use for the flow specification.
Destination Port field	The destination port that you want to use for the flow specification.

Step 3 Click **Save**.

OR you can click **Cancel** to cancel the action.

About AAA Servers

AAA enables the security appliance to determine who the user is (authentication), what the user can do (authorization), and what the user did (accounting). Cisco Nexus Data Broker uses Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) to communicate with an AAA server.

Remote authentication and authorization is supported using the AAA server. To authenticate each user, Cisco Nexus Data Broker uses both the login credentials and an attribute-value (AV) pair that assigns the authorized role for the user as part of the user administration. After successful authentication, the Cisco AV pair is returned to Cisco Nexus Data Broker for resource access authorization.

Adding a AAA Server

Note You can verify the status of AAA TACACS server before adding it using the **Check Server** option on the **Add AAA Server** dialog box. The **Check Server** option verifies whether the AAA server that you are configuring is reachable or not and whether the credentials are valid or not.

Note When the configured AAA server(s) are not reachable, the user request is authenticated locally. If the AAA server is reachable and the user authentication fails, the user request is not authenticated locally.

Step 1 Navigate to the **AAA** tab under **System** and click **Add Server**.

The **Add AAA Server** window is displayed.

Step 2 In the **Add AAA Server** window, complete the following fields:

Name	Description
Protocol field	Choose the protocol for the AAA server. This can be one of the following: • **Radius+** • **TACACS+** • **LDAP** **Note** For detailed information about how to configure LDAP for AAA server, see Configuring User Authentication for LDAP.
Server Address field	Server IP address or Domain Name.
Secret field	The shared secret configured on the AAA server.

Name	Description
User Name field	User name for authentication..
Password field	Password for authenticating the user.

Step 3 (Optional) Click **Check Server** to verify whether the server is reachable and authentication credentials are valid or not.

Note The **Check Server** option is available only for TACACS AAA server.

Step 4 Click **Save**.

What to do next

If you chose RADIUS as the protocol for the AAA server, you need to configure user authentication for RADIUS.

Configuring User Authentication for RADIUS Server

User authorization on a RADIUS server must conform to the Cisco Attribute-Value (av-pair) format. In the RADIUS server, configure the Cisco av-pair attribute for a user as follows:

```
shell:roles="Network-Admin Slice-Admin"
```

Viewing Cluster Information

Navigate to the **Cluster** tab under **System** to view information about the clusters.

The cluster management dialog boxes are read-only. The dialog box lists the IP addresses of all of the Cisco Nexus Data Broker instances in the cluster.

Note For the backup and upload features to work properly, all the servers in the cluster should be stopped and then they should be restarted. You should not configure any functionality during this time. Once the upload configuration is done, you should not configure anything from any other nodes in the cluster as it might to lead to few inconsistencies in the data.

Viewing the OSGi Console

You can view all of Cisco Nexus Data Broker bundles that comprise the application by viewing the OSGi Web Console.

Note This procedure does not provide a step-by-step guide to everything you can do in the OSGi Web Console for **Cisco XNC Bundles** list. It guides you in opening the OSGi Web Console and viewing bundle information.

Step 1 Navigate to the **System** tab under **Administration**.
A new browser tab opens.

Step 2 Click **OSGI**.

Step 3 Enter your username and password, and then press **Enter**.

The **Cisco – XNC Bundles** list is displayed. In this page you can view all of the active packages, filter on the package name to specify bundle names, and complete other tasks.

Step 4 When you are finished viewing the list, close the **Cisco – XNC Bundles** browser tab.

Viewing the Northbound API Content

You can view all of Cisco Nexus Data Broker northbound API content for the application by opening a browser tab using the **Northbound API** tool (book icon) in the menu bar.

Step 1 From the menu bar, click the **Northbound API** button.

A new browser tab (Swagger UI) is opened and the complete list of northbound API content used in Cisco Nexus Data Broker is displayed.

From this tab, you can do the following:

- Show or hide the operations for an API.
- List the operations for an API.
- Expand the operations for an API.

Step 2 When you are finished viewing northbound API content, close the browser tab.

Downloading the System Log Files

You can download log files for Cisco Nexus Data Broker to use for analysis. Log files are saved as a .zip archive.

Note Starting with Cisco Nexus Data Broker Release 3.7, naming convention for the System log files has changed. The System log file name now reflects the time stamp when the file is generated. For example, `NDBLogs-21Aug2018_11_15_08.zip`.

Note Starting with Cisco Nexus Data Broker Release 3.7, the System log file now provides additional details such as the device connection information, number of redirections, and details about all the devices managed by NDB.

Step 1 Navigate to the **System** tab under **Administration**.

Step 2 Click **Download Logs**.

A dialog box opens in the browser prompting you to either open or save the .zip file.

Step 3 Do one of the following:

- Save the archive to a location of your choosing, for example, `home/ndbconfig`.
- Open the archive to view the contents, and then save it.

Backing Up or Restoring the Configuration Using NDB GUI

Starting with Cisco NDB, Release 3.4, you can create and restore a NDB configuration backup instantly during the pre-deployment phase. Support for instant backup is currently available in NX-OS, OpenFlow, and AUX switches.

Using this feature, a backup point is created with current NDB configuration that can be restored to the system. Cisco NDB provides three backup options:

- Schedule backup to NDB Server—Backup is created at the specified time in the NDB server in the backup directory of xnc.
- Backup now to NDB server—Backup is created in the NDB server in the backup directory of xnc.
- Backup now locally—Backup is created and available for download using Web browser.

Cisco NDB provides two restore options:

- Restore from Server—Configuration is restored from a server.
- Restore Locally—Configuration is restored from a local directory.

Backing Up or Restoring the Configuration Using the CLI

Step 1 Navigate to the `xnc/bin` directory that was created when you installed the software.

Step 2 Back up the configuration by entering the **./xnc config --backup** command.

The **--backup** option creates a backup archive (in .zip format) of the startup configuration in the current `xnc` distribution. The backup archive is stored in `{xncHome}/backup/`. A new archive is created each time that the backup command is entered using a filename with the current timestamp.

Step 3 Restore the configuration by entering the **./xnc config --restore --backupfile** {*zip_filename*} command.

The **--restore** option restores the startup configuration of the current `xnc` distribution from an existing backup archive. The restore action requires the absolute path of the backup archive.

Scheduling Configuration Backup to NDB Server

Beginning with Cisco Nexus Data Broker, Release 3.2, you can schedule automatic configuration backup to a server with a start date and an end date. Backup is created at the specified time in the NDB server in the backup directory of XNC. When any configuration is performed in Cisco Nexus Data Broker, it is saved automatically.

Note Beginning with Cisco Nexus Data Broker, Release 3.2, you do not need to use the **Save** option to save the Cisco Nexus Data Broker configurations. Even after you restart the server, the configuration is autosaved.

Step 1 Navigate to **Administration** -> **System** -> **Backup/Restore** tab.

Step 2 From the **Backup** drop-down list, select **Schedule backup to NDB Server** to open the **Schedule** page.

Step 3 In the **Schedule** page, enter the following details:

Field	Description
Start Date	Date to start the configuration backup.
Start Time	Time to start the configuration backup.
Choose Pattern	Select the pattern of the backup. Valid options are: • Daily • Weekly • Monthly
Choose	Select when to stop the backup process. Valid options are: • No End Date: Continue taking backup as per the specified frequency. • End Date: Continue taking backup till the specified date. • Occurences: Indicates the number of times to take the backup.
Enable	Enables the scheduled backup.

Restoring Configuration Locally

You can upload the saved system configuration files for Cisco Nexus Data Broker to restore the Cisco Nexus Data Broker application in the case of a failure or other event. After restoring you configuration, you will need to restart Cisco Nexus Data Broker.

Direct upload path to Cisco Nexus Data Broker is available from Cisco Nexus Data Broker, Release 3.0 or above. If you are running a previous release, upload it to Release 3.0 first before uploading to Release 3.2.

Step 1 Navigate to **Administration** > **System** > **Backup/ Restore**.

Step 2 Click the **Restore Locally** button.

The **Upload Configuration** pane is dislayed.

Step 3 Browse in your local machine and navigate to the file.

Step 4 Check the Restore checkbox.

When you check the Restore check box, the configuration is restored in the NDB switch too. This is applicable for release 3.8 and after.

The backup earlier performed by clicking the **Backup** button is used for restore.

Step 5 Click **Upload Configuration**.

Step 6 Restart the server, and then log back in to the Cisco Nexus Data Broker GUI.

Backing Up Configuration Locally

Configuration backup is created in the local machine in the specified directory. You can backup the system configuration locally in case you need to restore the system after an upgrade or other change. System configuration files are saved in a zipped archive.

Step 1 Navigate to **Administration** -> **System** -> **Backup/Restore** tab.

Step 2 From the **Backup** drop-down list, select **backup now locally**.
The configuration backup is created and dowloaded to the local directory.

Restoring Configuration from a Server

You can restore NDB configuration from a server using the NDB GUI. Complete the following steps to restore a confguration from a server:

SUMMARY STEPS

1. Navigate to **Administration** -> **System** -> **Backup/Restore** tab.
2. Select a backup from the list and click **Restore** to restore the selected configuration.

DETAILED STEPS

Step 1 Navigate to **Administration** -> **System** -> **Backup/Restore** tab.

Step 2 Select a backup from the list and click **Restore** to restore the selected configuration.

Recovering the Administrative Password

The Cisco Nexus Data Broker network administrator user can return the administrative password to the factory default.

Note The software may or may not be running when this command is used. If the software is not running, the password reset takes effect the next time that it is run.

Step 1 Open a command window where you installed Cisco Nexus Data Broker.

Step 2 Navigate to the `xnc/bin` directory that was created when you installed the software.

Step 3 Reset the administrative password by entering the **./xnc reset-admin-password** [**--wait-seconds** {*wait_time*} **--password** {*password*}] command.

Resets the admin password to the default or specified password by restarting the user manager.

- The **wait-seconds** is the length of time, in seconds, to wait for the user manager to restart. The minimum is 5 seconds and the maximum is 60 seconds.
- The **password** is the administrative password.

Note

- The password must be from 8 to 256 characters, contain both uppercase and lowercase characters, and have at least one number and one non-alphanumeric character.
- If you leave the password blank, it is reset to the factory default of "admin".
- Each time that you reset the administrative password, make sure that the new password meets these requirements or you will not be able to log in to Cisco Nexus Data Broker.

Uninstalling the Application Software

Before you begin

Ensure that your Cisco Nexus Data Broker application is stopped before proceeding.

Step 1 Navigate to the directory where you created the Cisco Nexus Data Broker installation.

For example, if you installed the software in `Home/CiscoNDB`, navigate to the `Home` directory.

Step 2 Delete the `CiscoNDB` directory.