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.

Slices can overlap if each slice has at least one unique attribute. For example, a slice can share the same physical switches and ports, but be differentiated by the type of traffic it receives.

Adding a Slice

Step 1 Navigate to the **System** tab under **Administration** and click **+ Slice**.
The **Add Slice** window is displayed.

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

Name	Description
Name	The name that you want to assign to the slice.
Select Devices	Select the devices that you want to associate with the slice.

Step 3 Click **Save**.

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 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
Server Address field	The IP address of the AAA server.
Secret field	The shared secret configured on the AAA server.
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.

Step 3 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"
```

Note This is applicable for both RADIUS, TACACS, and LDAP servers.

Installing the TACACS+ Server

Execute the following steps to setup the TACACS+ server in Linux platform. To make the authentication to work, you need to create the user in the Linux machine and install TACAS+ server with PAM support.

Complete the following steps to install the TACACS+ server:

Step 1 **sudo su**

Step 2 **apt-get update && apt-get install -y gcc make flex bison libwrap0-dev**

Step 3 **apt-get install libpam-dev**

Step 4 **wget ftp://ftp.shrubbery.net/pub/tac_plus/tacacs+-F4.0.4.26.tar.gz && tar zxvf tacacs+-F4.0.4.26.tar.gz**

Step 5 **cd tacacs+-F4.0.4.26**

Step 6 **./configure --prefix=/usr --enable-acls --enable-uenable --enable-maxsess --enable-finger --enable-debug && make install**

Configuring the TACACS+ Server Required for Cisco Nexus Data Broker

The TACACS+ server supports two types of roles in Cisco NDB: **Network-Admin** and **Network-Operator**. Complete the following steps to configure the TACACS+ server:

Before You Begin

Step 1 Insert the line, **vi /etc/ld.so.conf** in the **ld.so.conf** file.

Step 2 **/usr/lib**

Step 3 **ldconfig**

Step 4 **mkdir /etc/tacacs**

Step 5 **cd /etc/tacacs**

Step 6 **touch tac_plus.conf**
A sample **tac_plus.conf** file is displayed in the example. You can ignore the lines while adding it to a file. Create user in Linux machine and the password should be the same as configured in**tac_plus.conf** file.

```
--------------START----------------------------
accounting syslog;
accounting file = /var/log/tac_plus.acct
key = "cisco123"
group = admin {
default service = permit
service = exec {
  priv-lvl = 15
  shell:roles="Network-Admin"
}
}
user =  ndb {
login = ndb
member = admin
}
default authentication = file /etc/passwd
-----------------END---------------------------
```

Step 7 **chmod 755 tac_plus.conf**

Step 8 **mkdir /var/log/tac_plus**

Step 9 **touch /var/log/tac_plus/tac_plus.acct**

Step 10 **adduser ndb**

Step 11 **tac_plus -C /etc/tacacs/tac_plus.conf**
To start the TACACS+ server, use this command.

Step 12 **kill -9 (Process id)**
To stop the TACACS+ service, use this command.

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.

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.

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.

Downloading the System Configuration Files

You can download the system configuration files for Cisco Nexus Data Broker to save them 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 the **System** tab under **Administration**.

Step 2 Click **Download Configuration**.
A dialog box opens in the browser prompting you to either open or save the 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.

Uploading the System Configuration Files

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.

Before You Begin

You must download the system configuration files and save them in a zipped archive.

Step 1 Navigate to the **System** tab under **Administration** and click **Upload Configuration**.

Step 2 Navigate to the location of the file `configuration_startup.zip`.

Step 3 Click on the archive file.
The system configuration is uploaded and the browser displays a message informing you that you need to restart the server.

Step 4 Restart the server, and then log back in to the Cisco Nexus Data Broker GUI.

Backing Up or Restoring the Configuration

The backup and restore commands allow you to back up your Cisco Nexus Data Broker configurations and restore them.

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 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 4 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.

Step 5 If you are restoring a configuration, stop and restart Cisco Nexus Data Broker for the restored configuration to take effect.

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.