Logging in and Managing Cisco Nexus Data Broker

This chapter contains the following sections:

- Configuring Cisco Nexus Data Broker, on page 1
- Logging in to the Cisco Nexus Data Broker GUI, on page 5
- Changing the Controller Access to HTTP, on page 6
- Cisco Nexus Data Broker GUI Overview, on page 6
- Saving Configuration Changes , on page 8

Configuring Cisco Nexus Data Broker

Configuring High Availability Clusters

Cisco Nexus Data Broker supports high availability clustering in active/active mode with up to five controllers. To use high availability clustering with Cisco Nexus Data Broker, you must edit the `config.ini` file for each instance of Cisco Nexus Data Broker.

Note IPv6 is supported in centralized NDB mode only, it is not supported in Embedded mode.

Note Cisco NDB supports only 2 node configuration or odd number node configuration. If you configure even number of nodes, the last node is not included in the cluster formation, ensuring odd number of nodes in a setup.

Table 1: Cluster Operation Status

Cluster Indicator	Cluster Status	Recommendation
Green	Operational	

Cluster Indicator	Cluster Status	Recommendation
Yellow	Some of the cluster nodes are not available	Do not make any changes or add to the existing NDB configuration.
Red	The node is isolated from the cluster.	Do not make any changes or add to the existing NDB configuration. Note: For two node cluster, you need to override in any one of the cluster node only, to ensure regular operation.

Before you begin

- All IP addresses must be reachable and capable of communicating with each other.
- All switches in the cluster must connect to all of the controllers.
- All controllers must have the same HA clustering configuration information in the `config.ini` files.
- All controllers must have the same information in the `xnc/configuration/startup` directory.
- If using cluster passwords, all controllers must have the same password configured in the `xncjgroups.xml` file. See Password Protecting the High Availability Clusters, on page 3.

Step 1 Ensure that Cisco Nexus Data Broker is not running on any of the instances in the cluster.

Step 2 Open a command window on one of the instances in the cluster.

Step 3 Navigate to the `xnc/configuration` directory that was created when you installed the software.

Step 4 Use any text editor to open the `config.ini` file.

Step 5 Locate the following text:

```
# HA Clustering configuration (semi-colon-separated IP addresses of all controllers that are part of
 the cluster.)
# supernodes=<ip1>;<ip2>;<ip3>;<ipn>
```

Step 6 Remove the comments on the # supernodes line, and replace <ip1>;<ip2>;<ip3>;<ipn> with the IP addresses for each instance of Cisco Nexus Data Broker in the cluster. You can enter from two to five IP addresses.

Example:

IPv4 example.

```
# HA Clustering configuration (semi-colon-separated IP addresses of all controllers that are part of
 the cluster.)
supernodes=10.1.1.1;10.2.1.1;10.3.1.1;10.4.1.1;10.5.1.1
```

Example:

IPv6 example.

```
# HA Clustering configuration (semi-colon-separated IP addresses of all controllers that are part of
 the cluster.)
supernodes=2001:22:11::1;2001:33::44::1;2001:55:66::1
```

Step 7 Save the file and exit the editor.

Step 8 Repeat Step 3 through Step 7 for each instance of Cisco Nexus Data Broker in the cluster.

Step 9 Restart Cisco Nexus Data Broker.

Password Protecting the High Availability Clusters

You can enable password protection on your HA clusters with the `xncjgroups.xml` file. This file must be exactly the same for each instance of Cisco Nexus Data Broker.

Step 1 Ensure that Cisco Nexus Data Broker is not running on any of the instances in the cluster.

Step 2 Open a command window on one of the instances in the cluster.

Step 3 Navigate to the `xnc/configuration` directory.

Step 4 Use any text editor to open the `xncjgroups.xml` file.

Step 5 Locate the following text:

```
<!-- <AUTH auth_class="org.jgroups.auth.MD5Token" auth_value="ciscoXNC" token_hash="MD5"></AUTH>
-->
```

Step 6 Remove the comments from the AUTH line.

Example:

```
<AUTH auth_class="org.jgroups.auth.MD5Token" auth_value="ciscoXNC" token_hash="MD5"></AUTH>
```

Step 7 (Optional) Change the password in the auth_value attribute.

By default, the cluster is protected with the password "ciscoXNC". You can change this password to whatever value you want, you need make the similar changes on all machines in the cluster.

Step 8 Save the file and exit the editor.

Step 9 Repeat Step 4 through Step 8 for each instance of Cisco Nexus Data Broker in the cluster.

Step 10 Restart Cisco Nexus Data Broker.

Editing Cisco Nexus Switch Configuration

Cisco Nexus Data Broker periodically verifies the Cisco Nexus Switch inventory and the topology so that the topology and inventory is in sync. Cisco Nexus data broker periodically rediscovers the switch inventory and the topology interconnection and status. This information is updated in the GUI depending on the status. You can configure the rediscovery interval and the default value is 60 seconds.

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

Step 2 Use any text editor to open the `config.ini` file.

Step 3 Update the following parameters:

Name	Predefined Value in Seconds	Minimum Value in Seconds	Recommended Value in Seconds
of.messageResponseTimer	60	2	60

Name	Predefined Value in Seconds	Minimum Value in Seconds	Recommended Value in Seconds
of.switchLivenessTimeout	120.5	60.5	120.5
of.flowStatsPollInterval	240	10	240
of.portStatsPollInterval	240	5	240
of.descStatsPollInterval	240	60	240
of.barrierMessagePriorCount	50	100	50
of.discoveryInterval	300	30	300
of.discoveryTimeoutMultiple	2	2	2
NX-API related system parameters			
nx.connectionDelayTimer	300	—	300
nx.flowStatsPollInterval	120	—	120
nx.tableStatsPollInterval	120	—	120
nx.portStatsPollInterval	120	—	120
nx.descStatsPollInterval	120	—	120
nx.lldpPollingTimer	10	—	10
nx.portPollingTimer	20	—	20

Note Predefined values are the values that Cisco includes in the `config.ini` file that is shipped with Cisco Nexus Data Broker. An em dash ("—") in this column of the table means that unless you explicitly update the value, the minimum value will be used.

Step 4 Save the file and exit the editor.

Step 5 Restart Cisco Nexus Data Broker.

Configuring Inactivity Timeout

By default, a user is logged out if the session is inactive for more than 10 minutes. You need to re-log in to the NDB to apply the new interval.

Step 1 Log into NDB UI.

Step 2 Navigate to **Administration** > **System** > **Session Timeout**.

Step 3 Enter inactivity timeout value in the **Session Timeout** text field and click **Submit**.

Step 4 Log out and log into NDB to apply the changes.

Configuring User Roles for Edge Ports

To manage which edge ports a Cisco XNC application user can use for creating rules for edge ports, you must modify the App-User role settings in the `config.ini` file to enable role-based access control (RBAC) for application users. After you make your changes and restart Cisco XNC, note these restrictions:

To manage which edge ports a Cisco Nexus Data Broker application user can use for creating rules for edge ports, you must modify the App-User role settings in the `config.ini` file to enable role-based access control (RBAC) for application users. After you make your changes and restart Cisco Nexus Data Broker, note these restrictions:

- Cisco XNC App-User role users will be able to create rules only for source ports which are part of the resource group or groups assigned to that role .
- Only Cisco XNC App-Admin role users will be able create rules with no source.
- Cisco Nexus Data Broker App-User role users will be able to create rules only for source ports which are part of the resource group or groups assigned to that role .
- Only Cisco Nexus Data Broker App-Admin role users will be able create rules with no source.

To enable RBAC for the App-User role, follow these steps:

Step 1 Open the `config.ini` file for editing.

Step 2 Locate the line `# Enforce restriction on edge/tap ports user can capture (default false).`

Step 3 Remove the comment character from the following line:

```
monitor.strictAuthorization=true
```

Step 4 Save your work and close the file.

Step 5 If Cisco XNC is running, restart the application to enable the change.

Step 6 If Cisco Nexus Data Broker is running, restart the application to enable the change.

Logging in to the Cisco Nexus Data Broker GUI

You can log into the Cisco Nexus Data Broker using HTTPS. The default HTTPS web link for the Cisco Nexus Data Broker GUI is `https://Nexus_Data_Broker_IP:8443/monitor`.

Note You must manually specify the https:// protocol in your web browser. The controller must also be configured for HTTPS.

Step 1 In your web browser, enter the Cisco Nexus Data Broker web link.

Step 2 On the launch page, do the following:

a) Enter your username and password.

The default username and password is admin/admin.

b) Click **Log In**.

Changing the Controller Access to HTTP

Starting with Cisco Nexus Data Broker Release 2.1, an unencrypted (HTTP) access to the GUI and the API to the controller access is disabled by default. You cannot access the controller with the URL http://<host>:8080.

If you want to change the controller access to HTTP, complete the following steps:

Step 1 Remove the comment character from the connector for port 8080 in the tomcat-server.xml file in the configuration directory as displayed in the following example:

Example:

```
 <Service name="Catalina">
  <!--
    <Connector port="8080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" server="Cisco XNC" enableLookups="false" />
  -->
    <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
               scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS"
               keystoreFile="configuration/keystore"
               keystorePass="ciscoxnc" server="Cisco XNC"
               connectionTimeout="60000" enableLookups="false" />
```

Example:

Remove the comment character as displayed in the following example:

```
<Service name="Catalina">
    <Connector port="8080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" server="Cisco XNC" enableLookups="false" />

    <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
               scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS"
               keystoreFile="configuration/keystore"
               keystorePass="ciscoxnc" server="Cisco XNC"
               connectionTimeout="60000" enableLookups="false" />
```

Step 2 Restart the controller.

Cisco Nexus Data Broker GUI Overview

The Cisco Nexus Data Broker Release GUI contains the following tabs:

- Cisco Nexus Data Broker, Release Version
- **Configuration** tab at the top of the screen
- **Administration** tab at the top of the screen
- **Default** tab displaying the switches in use
- **Save** button—Enables you to save any additions or changes you make in Cisco Nexus Data Broker.
- The **Online help** button—Provides access to the online help for the current page.
- Bookmarks
- Administrator Details

The **Configuration** tab contains the following items:

- Topology
- Port Definitions
- Port Groups
- Monitoring Devices
- Service Nodes
- Filters
- Connections
- Redirections
- Statistics
- SPAN Sessions

The **Administration** tab contains the following items:

- Device Management
- Devices
- Flows
- Troubleshoot
- Consistency Check
- System Management
- User Management
- System

Topology Tools

The left side of the topology pane contains a zoom slider that allows you increase or decrease the size of the topology diagram. You can also increase or decrease the size of the topology diagram by scrolling up or down, respectively, with your mouse wheel.

You can move the entire topology diagram, a single topology element, or a node group. To move the diagram, an element, or a node group, click it and drag it.

To view information about a node or an edge port, hover over the node or edge port icon with your mouse. The information displayed depends on the device you choose.

To view information about a path, hover over the path in the topology diagram.

To view information about a filter, hover over the **Name** of the filter in the **Filters** tab.

What's New Utility Tool

Starting with Cisco NDB Release 3.7, a new utility tools is added to the NDB user interface. This utility appears when you log into NDB and lists all the new features introduced for the release. You can also open this utility using the What's New icon on the NDB GUI.

Saving Configuration Changes

In Cisco Nexus Data Broker, Release 3.2.0 the auto-save configuration option is added. You can save the configuration changes, but it is not required. For example, if you configure Edge-SPAN, monitor the device, or configure any other functionality in Cisco Nexus Data Broker, it is saved automatically.

On the menu bar, click **Save**.