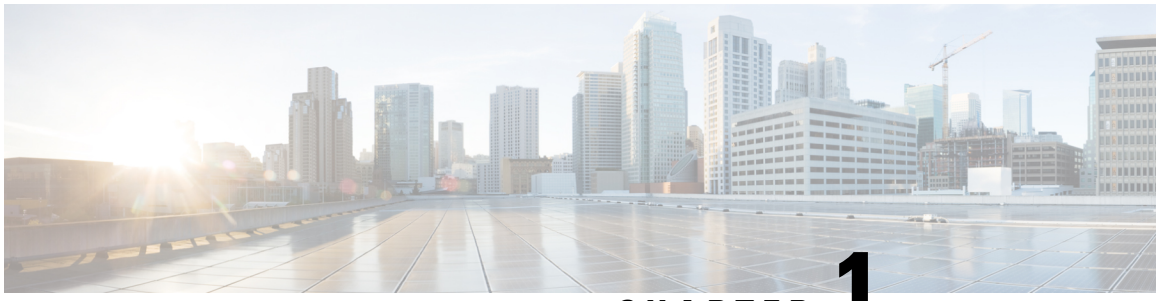
Cisco Nexus Data Broker Configuration Guide, Release 3.3

First Published: 2017-06-20

Last Modified: 2018-08-20

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Cisco Nexus Data Broker Overview

This chapter contains the following sections:

About Cisco Nexus Data Broker

Visibility into application traffic has traditionally been important for infrastructure operations to maintain security, troubleshooting, and compliance and perform resource planning. With the technological advances and growth in cloud-based applications, it has become imperative to gain increased visibility into the network traffic. Traditional approaches to gain visibility into network traffic are expensive and rigid, making it difficult for managers of large-scale deployments.

Cisco Nexus Data Broker with Cisco Nexus Switches provides a software-defined, programmable solution to aggregate copies of network traffic using Switched Port Analyzer (SPAN) or network Test Access Point (TAP) for monitoring and visibility. As opposed to traditional network taps and monitoring solutions, this packet-brokering approach offers a simple, scalable and cost-effective solution that is well-suited for customers who need to monitor higher-volume and business-critical traffic for efficient use of security, compliance, and application performance monitoring tools.

With the flexibility to use a variety of Cisco Nexus Switches and the ability to interconnect them to form a scalable topology provides the ability to aggregate traffic from multiple input TAP or SPAN ports, and replicate and forward traffic to multiple monitoring tools which may be connected across different switches. Combining the use of Cisco plugin for OpenFlow and the Cisco NX-API agent to communicate to the switches, Cisco Nexus Data Broker provides advance features for traffic management.

Cisco Nexus Data Broker provides management support for multiple disjointed Cisco Nexus Data Broker networks. You can manage multiple Cisco Nexus Data Broker topologies that may be disjointed using the same application instance. For example, if you have 5 data centers and want to deploy an independent Cisco Nexus Data Broker solution for each data center, you can manage all 5 independent deployments using a single application instance by creating a logical partition (network slice) for each monitoring network.

Note A Cisco Nexus Data Broker instance can support either the OpenFlow or NX-API device configuration mode, it does not support both device types.

Note Starting with Cisco Nexus Data Broker Release 3.1, the user strings for Cisco Nexus Data Broker can contain alphanumeric characters including the following special characters: period (.), underscore (_), or hyphen (-) . These are the only special characters that are allowed in the user strings.

Note Starting with Cisco Nexus Data Broker, Release 3.3:

- Advanced filtering based on TCP AND UDP flags is supported to filter the traffic.
- IPv6, QinQ, and UDF are supported for NX-OS I6 release platform.
- You can define a User Defined Filter (UDF) and use it while creating a filter for traffic management.
- Edit Priority field for the connections is configurable. By default, edit is enabled for the Cisco NDB administrator role.

Note Starting with Cisco NDB release 3.2.2, IPv6 addressing is supported in centralized mode. You can configure NDB to use either IPv6 addressing or both IPv4 and IPv6 addressing. Set `ipv6.strict` attribute in config.ini file to *true* to make NDB accessible only through IPv6 address. If you set the `ipv6.strict` attribute to *false*, you can access NDB through IPv4 or IPv6 address.

Note The hostname string for Cisco Nexus Data Broker can contain between 1 and 256 alphanumeric characters including the following special characters: period (.), underscore (_), or hyphen (-) . These are the only special characters that are allowed in the user strings.

Cisco Nexus Data Broker provides the following:

- Support for the OpenFlow mode or the NX-API mode of operation.

Note The OpenFlow mode and the NX-API mode are supported on both Cisco Nexus 3000 Series and Cisco Nexus 9000 Series switches. Cisco Nexus 9500, 9200, and 9300-EX switches support only NX-API mode of deployment. Cisco Nexus 3500 supports only Openflow mode of deployment. You can enable only one mode, either OpenFlow or NX-API mode, at a time.

You can enable only one mode, either OpenFlow or NX-API mode, at a time.

When using OpenFlow mode, NX-API is available for auxiliary configurations only, for example, Enabling Q-in-Q on the SPAN and TAP ports.

Cisco Nexus 9300-EX Series switches support only Cisco NX-OS Release 7.0(3)I5(1) and later releases.

The configuration that is supported in the AUX mode is:

- Pull and push of interface description
- Q-in-Q configuration
- Redirection
- Port Channel load balancing
- MPLS Stripping

Note Starting with Cisco Nexus 3000 Release 7.x, the NX-API configuration is supported on the following Cisco Nexus Series switches:

- Cisco Nexus 3172 switches
- Cisco Nexus 3132 switches
- Cisco Nexus 3164 switches
- Cisco Nexus 31128 switches
- Cisco Nexus 3232 switches
- Cisco Nexus 3264 switches
- Cisco Nexus 3100-V switches

- The features that are supported with the Cisco Nexus 9500 Series switches are:
  - The NX-API feature is supported. (OpenFlow is not supported.)
  - The MPLS strip feature is supported.
  - The label age CLI feature is not supported.
- Support for Layer-7 filtering for the HTTP traffic using the HTTP methods.
- Support for VLAN and MPLS tag stripping.

- A scalable topology for TAP and SPAN port aggregation.
- Support for Q-in-Q to tag input source TAP and SPAN ports.
- Symmetric load balancing.
- Rules for matching monitoring traffic based on Layer 1 through Layer 4 information.
- The ability to replicate and forward traffic to multiple monitoring tools.
- Time stamping using Precision Time Protocol (PTP).
- Packet truncation beyond a specified number of bytes to discard payload.
- Reaction to changes in the TAP/SPAN aggregation network states.
- Security features, such as role-based access control (RBAC), and integration with an external Active Directory using RADIUS, TACACS, or LDAP for authentication, authorization, and accounting (AAA) functions.
- End-to-end path visibility, including both port and flow level statistics for troubleshooting.
- Robust Representational State Transfer (REST) API and a web-based GUI for performing all functions
- Support for Cisco plugin for Open Flow, version 1.0
- Cisco Nexus Data Broker adds NX-API plugin to support Cisco Nexus 9000 Series switches as TAP/SPAN aggregation. The NX-API supports JSON-RPC, XML, and JSON. Cisco Nexus Data Broker interacts with Cisco Nexus 9000 Series using the NX-API in JSON message formats.
- Beginning with Cisco Nexus Data Broker, Release 3.1, Cisco Nexus Data Broker is certified with Cisco Nexus 9200 Series and Cisco Nexus 9300-EX Series switches.

  The following features are supported on the Cisco Nexus 9300-EX Series switches:

  - Symmetric Load Balancing
  - Q-in-Q
  - Switch Port Configuration
  - MPLS Stripping
  - BlockTx

  The following features are not supported on the Cisco Nexus 9300-EX Series switches:

  - Timestamp Tagging
  - Truncate

- Beginning with Cisco Nexus Data Broker, Release 3.1, Cisco Nexus Data Broker is shipped with a certificate for the HTTPS connection between the Cisco Nexus Data Broker and a browser. Now with this feature, you can change to a different certificate than the shipped certificate.

  The script **generateWebUIcertificate.sh** is available in the **xnc/configuration** folder. If you execute this script, it moves the shipped certificate to **old_keystore** and the new certificate is generated in **keystore**. On the next Cisco Nexus Data Broker restart, this new certificate is used.

With Cisco Nexus Data Broker, you can:

- Classify Switched Port Analyzer (SPAN) and Test Access Point (TAP) ports.
- Integrate with Cisco ACI through Cisco APIC to configure SPAN destinations and SPAN sessions.
- Add monitoring devices to capture traffic.
- Filter which traffic should be monitored.
- Redirect packets from a single or multiple SPAN or TAP ports to multiple monitoring devices through delivery ports.
- Restrict which users can view and modify the monitoring system.
- If Cisco Nexus 9000 Series switch is using 7.0(3)I4(1) or later version in NX-API mode and if a flow is installed using a VLAN filer, then the device goes through an IP access list and it does not match on the Layer 2 packet.
- Configure these additional features, depending upon the type of switch:
  - Enable MPLS Tag stripping.
  - Set VLAN ID on Cisco Nexus 3000 Series switches.
  - Symmetric load balancing on Cisco Nexus 3100 Series switches and Cisco Nexus 9000 Series switches.
  - Q-in-Q on Cisco Nexus 3000 Series switches, 3100 Series switches, and Cisco Nexus 9000 Series switches.
  - Timestamp tagging and packet truncation on Cisco Nexus 3500 Series switches.
  - You can now configure the **watchdog_timer** configuration parameter in the **config.ini** file. If the value of the parameter is set to 0, the watchdog timer functionality is not available. The value of 30 seconds is a minimum value of the parameter and if the value of the parameter is set to a value more the 30 seconds, the watchdog timer monitors the JAVA process for the configured time interval.

Supported Web Browsers

The following web browsers are supported for Cisco Nexus Data Broker:

- Firefox 18.x and later versions
- Chrome 24.x and later versions

Note JavaScript 1.5 or a later version must be enabled in your browser.

System Requirements

The following table lists the system requirements as per the deployment size for Cisco Nexus Data Broker 3.6.

Table 1: System Requirements per Deployment Size

Description	Small	Medium	Large
CPUs (virtual or physical)	6-core	12-core	18-core
Memory	8 GB RAM	16 GB RAM	24 GB RAM
Hard disk	Minimum of 40 GB of free space available on the partition on which the Cisco Nexus Data Broker software is installed.		
Operating System	A recent 64-bit Linux distribution that supports Java, preferably Ubuntu, Fedora, or Red Hat.		
Other	Java Virtual Machine 1.8 or later.		

Guidelines and Limitations

Cisco Nexus Data Broker runs in a Java Virtual Machine (JVM). As a Java-based application, Cisco Nexus Data Broker can run on any x86 server. For best results, we recommend the following:

- One 8-core CPU at 2 GHz or higher.
- A minimum of 16 GB of memory.
- A minimum of 40 GB of free hard disk space must be available on the partition where you will be installing the Cisco Nexus Data Broker application.
- A 64-bit Linux distribution with Java, such as the following:
  - Ubuntu Linux
  - Red Hat Enterprise (RHEL) Linux
  - Fedora Linux
- Java Virtual Machine 1.8.0_45 and higher.
- Python 2.7.3 and a higher version is required for the backup and restore script. This is also required to do the TLS configuration if Cisco Nexus Data Broker needs to use TLS for the device communication.
- A $JAVA_HOME environment variable in your profile that is set to the path of the JVM.
- JConsole and VisualVM that are both part of JDK are the recommended (but not required) additions for troubleshooting.
- During OpenFlow configuration for Cisco NXOS Release 7.0(3)I5(1) software image, virtual service ofa should not be installed and the following configuration should be used:

```
switch#
conf t
feature openflow
openflow
 switch 1 pipeline 201
 controller ipv4 10.16.206.162 port 6653 vrf management security none
 of-port interface ethernet1/1-30
```

See the following link for further details on NXOS configuration for OpenFlow:http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus/openflow/b_openflow_agent_nxos_1_3/Cisco_Plug_in_for_OpenFlow.html#reference_B6284F508CC6461B8EF30DCF870C809F

- You should not configure the same name for more than one switch in the topology to avoid unpredictable behavior in the link discovery by Cisco Nexus Data Broker.
- When the domain name is enabled in the switch, it does not reflect the change in the LLDP neighbors and the links get removed for that particular switch. The workaround for this issue is to disable the LLDP feature and then to enable it again by using **no feature lldp** and **feature lldp** CLI commands respectively.

Global Updates with Cisco Nexus Data Broker, Release 3.3

See the following global updates that are available with Cisco Nexus Data Broker, Release 3.3:

- The ports in the Graphical User Interface (GUI) are listed in a sorted order.
- A new field, **Row Count** is added in the GUI to display the rows in the multiples of 10, 25, 50, and 100.

Cisco Nexus Data Broker Software Release Filename Matrix

See the Cisco Nexus Data Broker software release filename matrix for more information on the software images:

Mode of Deployment	NXOS Image	Mode	File Name
Embedded	7.0(3)I6(1)	NXAPI	`ndb1000-sw-app-emb-i6-nxapi-k9-3.3.zip`
Embedded	7.0(3)I4 ,7.0(3)I3	NXAPI	`ndb1000-sw-app-emb-nxapi-3.3-k9.zip`
Embedded	7.0(3)I4, 7.0(3)I3	Openflow	`ndb1000-sw-app-emb-3.3-ofa_mmemb-2.1.4-r2-nxos-SPA-k9.zip`
Embedded	6.0(2)U6(3), 6.0(2)A8(1)	Openflow	`ndb1000-sw-app-emb-3.3-ofa_mmemb-1.1.5-r3-n3000-SPA-k9.zip`
Centralized	Upto 7.0(3)I6(1)	NXAPI, Openflow	`ndb1000-sw-app-k9-3.3.zip`

Nexus Data Broker Hardware and Software Interoperability Matrix

The following table lists the hardware and software ineteroperability matrix for NDB Release 3.6.

Nexus Switch Model(s)	Implementation Type	Supported NX-OS Versions	Open Flow Agent
30xx/31xx	OpenFlow	6.0(2)U6(x)	1.1.5
30xx/31xx	OpenFlow	7.0(3)I4(1) to 7.0(3)I4(7) and 7.0(3)I6(x), 7.0(3)I7(2), 7.0(3)I7(3), and 7.0(3)I7(4).	2.1.4
30xx	NXAPI	6.0(2)U6(x), and 7.0(3)I4(1) to 7.0(3)I4(7)	Not Supported
31xx	NXAPI	7.0(3)I4(1) to 7.0(3)I4(7) and 7.0(3)I6(x), 7.0(3)I7(1), 7.0(3)I7(3), and 7.0(3)I7(4)	NA
3164	OpenFlow	Not Supported	Not Supported
3164	NXAPI	7.0(3)I4(1) to 7.0(3)I4(7) and 7.0(3)I6(x), 7.0(3)I7(1), 7.0(3)I7(3), and 7.0(3)I7(4)	NA
32xx	OpenFlow	7.0(3)I4(1) to 7.0(3)I4(7) and 7.0(3)I6(x), 7.0(3)I7(2), 7.0(3)I7(3), and 7.0(3)I7(4)	2.1.4
32xx	NXAPI	7.0(3)I4(1) to 7.0(3)I4(7) and 7.0(3)I6(x), 7.0(3)I7(1), 7.0(3)I7(3), and 7.0(3)I7(4)	NA
35xx	OpenFlow	6.0(2)A6(x) or 6.0(2)A8(x)	1.1.5
35xx	NXAPI	Not Supported	Not Supported
92xx	OpenFlow	Not Supported	Not Supported
92xx	NXAPI	7.0(3)I4(2) to 7.0(3)I4(7) and 7.0(3)I6(x), 7.0(3)I7(1), 7.0(3)I7(3), and 7.0(3)I7(4)	NA
93xx	OpenFlow	7.0(3)I4(1) to 7.0(3)I4(7) and 7.0(3)I6(x), 7.0(3)I7(2), 7.0(3)I7(3), and 7.0(3)I7(4)	2.14
93xx	NXAPI	7.0(3)I4(1) to 7.0(3)I4(7) and 7.0(3)I6(x), 7.0(3)I7(1), 7.0(3)I7(3), and 7.0(3)I7(4)	NA
93xxx-EX	OpenFlow	Not Supported	Not Supported
93xxx-EX	NXAPI	7.0(3)I4(2) to 7.0(3)I4(7) and 7.0(3)I6(x), 7.0(3)I7(1), 7.0(3)I7(3), and 7.0(3)I7(4)	NA
93xxx-FX	OpenFlow	Not Supported	Not Supported
93xxx-FX	NXAPI	7.0(3)I4(2) to 7.0(3)I4(7) and 7.0(3)I6(x), 7.0(3)I7(1), 7.0(3)I7(3), and 7.0(3)I7(4)	NA
95xx	OpenFlow	Not Supported	Not Supported
95xx	NXAPI	7.0(3)I4(1) to 7.0(3)I4(7) and 7.0(3)I6(x), 7.0(3)I7(1), 7.0(3)I7(3), and 7.0(3)I7(4)	NA

Prerequisites for Cisco Nexus Series Switches

Cisco Nexus Data Broker is supported on Cisco Nexus 3000, 3100, 3200, 3500, and 9000 series switches. Before you deploy the software, you must do the following:

- Ensure that you have administrative rights to log in to the switch.
- Verify that the management interface of the switch (mgmt0) has an IP address configured using the **show running-config interface mgmt0** command.
- Ensure that the switch is in Multiple Spanning Tree (MST) mode. You can use **spanning-tree mode mst** command to enable MST mode on a switch.
- Add the VLAN range in the database that is to be used in Cisco Nexus Data Broker for tap aggregation and inline monitoring redirection to support VLAN filtering. For example, the VLAN range is <1-3967>.
- Ensure that the spanning tree protocol is disabled for all the VLANs. You can use the **no spanning-tree vlan 1-3967** to disable spanning tree on all the VLANs.

For running the OpenFlow and NX-API mode on the Cisco Nexus Series switches, see the following pre-requisites.

Note The hardware command that is a pre-requisite for the IPv6 feature is **hardware access-list tcam region ipv6-ifacl 512 double-wide**.

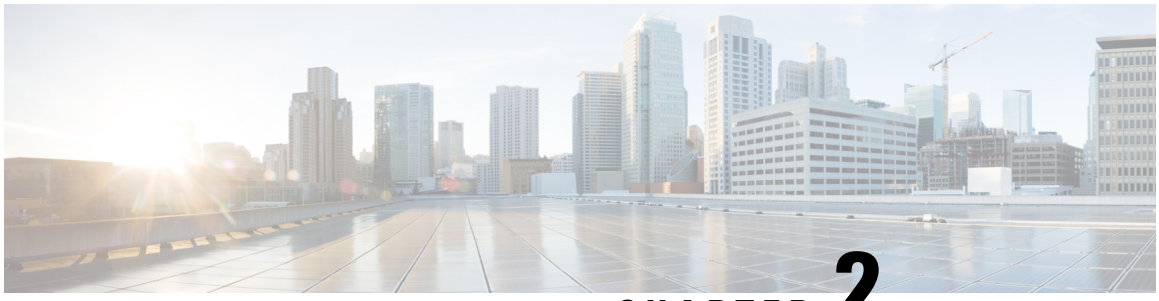
Note The TCAM configurations are based on the type of filters required. You may configure multiple TCAM entries from a specific region based on the network requirement. For example, *ing-ifacl* is the TCAM region to cater MAC, IPv4, IPv6 filters in case of N93180YC-E. You may configure multiple TCAM from this region to fit more filtering ACL TCAM entries.

Device Models	OpenFlow Mode	NX-API Mode
Cisco Nexus 3000 Series switches	Enter the # **hardware profile openflow** command at the prompt.	With Cisco Nexus 3000 Series switches, only Openflow mode is supported.

Device Models	OpenFlow Mode	NX-API Mode
Cisco Nexus 3164Q switches	The OpenFlow mode is not supported on the Nexus 3164Q switches.	Enter the following commands at the prompt: • **# hardware profile tcam region qos 0** • **# hardware profile tcam region racl 0** • **# hardware profile tcam region vacl 0** • **# hardware profile tcam region ifacl 1024 double-wide** • **# hardware access-list tcam region mac-ifacl 512**
Cisco Nexus 3172 Series switches	Enter the **# hardware profile openflow** command at the prompt.	Use the **hardware profile mode tap-aggregation** [**l2drop**] CLI command to enable tap aggregation and to reserve entries in the interface table that are needed for VLAN tagging. The l2drop option drops non-IP traffic ingress on tap interfaces.
Cisco Nexus 3200 Series switches	Enter the **hardware access-list tcam region openflow 256** command at the prompt.	Enter the following commands at the prompt: • **# hardware access-list tcam region e-racl 0** • **# hardware access-list tcam region span 0** • **# hardware access-list tcam region redirect 0** • **# hardware access-list tcam region vpc-convergence 0** • **# hardware access-list tcam region racl-lite 256** • **# hardware access-list tcam region l3qos-intra-lite 0** • **# hardware access-list tcam region ifacl 256 double-wide** • **# hardware access-list tcam region mac-ifacl 512**

Device Models	OpenFlow Mode	NX-API Mode
Cisco Nexus 3500 series switches	Enter the following commands at the prompt: • **# hardware profile forwarding-mode openflow-hybrid** command at the prompt to configure OpenFlow tcam. • **#hardware profile forwarding-mode openflow-only**	
Cisco Nexus 9300 Series switches	Enter the **hardware access-list tcam region openflow 512 double-wide** command at the prompt to configure the MAC filters. For other scenarios, enter the **hardware access-list tcam region openflow 512** command. **Note** IPv6 and IPv4 dual stack is not supported in I6 and I7.	Enter the following commands at the prompt: • **# hardware access-list tcam region qos 0** • **# hardware access-list tcam region vacl 0** • **# hardware access-list tcam region racl 0** • **# hardware access-list tcam region redirect 0** • **# hardware access-list tcam region vpc-convergence 0** • **#hardware access-list tcam region ifacl 1024 double-wide** • **# hardware access-list tcam region mac-ifacl 512** • **# hardware access-list tcam region ipv6-ifacl 512**

Device Models	OpenFlow Mode	NX-API Mode
Cisco Nexus 9200, 9300-EX and 9300-FX switches	The OpenFlow mode is not supported on the 9200, 9300-EX, and 9300_FX switches.	Enter the following commands at the prompt: • **#hardware access-list tcam region ing-l2-span-filter 0** (For Cisco Nexus 93108 series switch only) • **#hardware access-list tcam region ing-l3-span-filter 0** (For Cisco Nexus 93108 series switch only) • **# hardware access-list tcam region ing-racl 0** • **hardware access-list tcam region ing-l3-vlan-qos 0** • **# hardware access-list tcam region egr-racl 0** • **# hardware access-list tcam region ing-ifacl 1024**
Cisco Nexus 9500-EX and 9500-FX Series switches	The OpenFlow mode is not supported on the Cisco Nexus 9500-EX and 9500-FX Series switches.	Enter the following commands at the prompt: • **# hardware access-list tcam region ing-racl 0** • **# hardware access-list tcam region ing-l3-vlan-qos 0** • **# hardware access-list tcam region egr-racl 0** • **# hardware access-list tcam region ing-ifacl 1024**



CHAPTER 2

Installing or Upgrading the Cisco Nexus Data Broker Software in Centralized Mode

This chapter contains the following sections:

Installing Cisco Nexus Data Broker in Centralized Mode

Installing or Upgrading the Cisco Nexus Data Broker Software in Centralized Mode

Important Direct upgrade path to Cisco Nexus Data Broker Release 3.3 is available from Cisco Nexus Data Broker release 3.0 or above. If you are running a previous release, upgrade to Release 3.0 first before upgrading to Release 3.3.

- To complete a new installation of Cisco Nexus Data Broker, see the *Installing the Cisco Nexus Data Broker Software* section.

Installing the Cisco Nexus Data Broker Software in Centralized Mode

Procedure

Step 1 In a web browser, navigate to **www.cisco.com**.

Step 2 Under **Support**, click **All Downloads**.

Step 3 In the center pane, click **Cloud and Systems Management**.

Step 4 If prompted, enter your Cisco.com **username** and **password** to log in.

Step 5 In the right pane, click **Network Controllers and Applications**, and then click **Cisco Nexus Data Broker.**

The file information for Release 3.3 is displayed: Cisco Nexus Data Broker Software Application: ndb1000-sw-app-k9-3.3.zip

Step 6 Download the Cisco Nexus Data Broker application bundle.

Step 7 Create a directory in your Linux machine where you plan to install Cisco Nexus Data Broker.

For example, in your Home directory, create `CiscoNDB`.

Step 8 Copy the Cisco Nexus Data Broker zip file into the directory that you created.

Step 9 Unzip the Cisco Nexus Data Broker zip file.

The Cisco Nexus Data Broker software is installed in a directory called `xnc`. The directory contains the following:

- `runxnc.sh` file—The file that you use to launch Cisco Nexus Data Broker.
- `version.properties` file—The Cisco Nexus Data Broker build version.
- `captures` directory—The directory that contains output dump files from analytics run in Cisco Nexus Data Broker.

  Note The `captures` directory is created after you execute the Cisco Nexus Data Broker analytics tool.

- `configuration` directory—The directory that contains the Cisco Nexus Data Broker initialization files.

  This directory also contains the `startup` subdirectory where configurations are saved.

- `bin` directory—The directory that contains the following script:
  - `xnc` file—This script contains the Cisco Nexus Data Broker common CLI.
- `etc` directory—The directory that contains profile information.
- `lib` directory—The directory that contains the Cisco Nexus Data Broker Java libraries.
- `logs` directory—The directory that contains the Cisco Nexus Data Broker logs.

  Note The `logs` directory is created after the Cisco Nexus Data Broker application is started.

- `plugins` directory—The directory that contains the OSGi plugins.
- `work` directory—The webserver working directory.

  Note The `work` directory is created after the Cisco Nexus Data Broker application is started.

Upgrading the Application Software in Centralized Mode

Use the **upgrade** command to upgrade to Cisco Nexus Data Broker Release 3.3. When you are upgrading from Release 2.2.0 and/or Release 2.2.1, you first need to upgrade to Release 3.0.0 or Release 3.1.0 or Release 3.2.0, or Release 3.2.1 and only then you can upgrade to Cisco Nexus Data Broker Release 3.3. This upgrade is an in-place upgrade, which means that the product bits are replaced. A backup archive is created to restore your original installation, if necessary.

Note Once you upgrade to Cisco Nexus Data Broker Release 3.3, you cannot use the downgrade option to rollback to 3.2.1, 3.2.0 or 3.1.0 or 3.0.0. You have to use the configuration archive that is created during the upgrade process to rollback the software.

Note When you upgrade the software, the hostname should not be changed during the upgrade process. While upgrading to Cisco Nexus Data Broker Release 3.3, user should not allowed to change the hostname. If the hostname is changed during the upgrade, the upgrade process is not done successfully.

When you execute the **upgrade** command, the installation and the configuration are upgraded. However, any changes you made to the shell scripts or configuration files, for example, `runxnc.sh` and `config.ini`, are overwritten. After you complete the upgrade process, you must manually reapply your changes to those files.

Before you begin

- Stop all controller instances that use the Cisco Nexus Data Broker installation. This will avoid conflicts with the file system, which is updated during the upgrade.
- If you are using high availability clustering, stop all application instances in the cluster to ensure that there are no inconsistencies.
- Back up your `config.ini` and `runxnc.sh` files.

Important You should manually backup your `config.ini` and `runxnc.sh` files before upgrading, because the backup process does not back them up for you. If you do not backup your files before upgrading, any changes you made will be lost.

Note When you run `runxnc.sh` script after upgrading from Cisco Nexus Data Broker, make sure that you upgrade your current Java version and you have set JAVA_HOME to point to the correct JAVA version. If the current Java version used is lower than 1.8.0_45, the Java process does not start and it does not get the Web access.

Note When you run `runxnc.sh` script, there is a thread in the script that monitors the log and the Cisco Nexus Data Broker JAVA process to monitor the health of the Cisco Nexus Data Broker. The default value for this option is 30 Seconds.

Procedure

Step 1 In a web browser, navigate to Cisco.com.

Step 2 Under **Support**, click **All Downloads**.

Step 3 In the center pane, click **Cloud and Systems Management**.

Step 4 In the right pane, click **Network Controllers and Applications**, and then click **Cisco Nexus Data Broker.**

Step 5 Download the Cisco Nexus Data Broker Release 3.3 application bundle: Cisco Nexus Data Broker Software Application—ndb1000-sw-app-k9-3.3.zip

Step 6 Create a temporary directory in your Linux machine where you plan to upgrade to Cisco Nexus Data Broker.

For example, in your `Home` directory, create `CiscoNDB_Upgrade`.

Step 7 Unzip the Cisco Nexus Data Broker Release 3.3 zip file into the temporary directory that you created.

Step 8 Navigate to the `xnc` directory that was created when you installed the Cisco Nexus Data Broker release earlier.

Step 9 Backup your Cisco Nexus Data Broker release installation using your standard backup procedures.

Step 10 Stop running all Cisco Nexus Data Broker release processes.

Step 11 Navigate to the `xnc/bin` directory in the temporary directory that you created for the Cisco Nexus Data Broker Release 3.3 upgrade software.

Step 12 Upgrade the application by entering the **./xnc upgrade --perform --target-home** {*xnc_directory_to_be_upgraded*} **[--verbose] [--backupfile** {*xnc_backup_location_and_zip_filename*}**]** command.

You can use one of the following options:

Option	Description
--perform --target-home {*xnc_directory_to_be_upgraded*}	Upgrades the Cisco XNC Monitor Manager installation to Cisco Nexus Data Broker.
--perform --target-home {*xnc_directory_to_be_upgraded*} **--backupfile** {*xnc_backup_location_and_zip_filename*}	Upgrades the Cisco XNC Monitor Manager installation to Cisco Nexus Data Broker and creates a backup .zip file in the directory path that you set. **Note** You must provide the name of the backup file and the .zip extension.
--rollback --target-home {*xnc_directory_to_be_upgraded*}	Rolls back to the previous Cisco XNC Monitor Manager installation.
--rollback --target-home {*xnc_directory_to_be_upgraded*} **--backupfile** {*xnc_backup_location_and_zip_filename*}	Rolls back to the previous Cisco XNC Monitor Manager installation using the backup file in the absolute path that you set.
--verbose	Displays detailed information to the console. This option can be used with any other option and is disabled by default.
--validate --target-home {*xnc_directory_to_be_upgraded*}	Validates the installation.
./xnc help upgrade	Displays the options for the **upgrade** command.

Step 13 Navigate to the `xnc` directory where you originally installed Cisco XNC Monitor Manager.

Step 14 Start the application processes that you previously stopped.

Note Press Ctrl–F5, or press the Cmd, Shift, and R keys simultaneously when you access Cisco Nexus Data Broker through a web UI following an upgrade.

Step 15 If you have any upgrade-related issues, perform the following tasks:

a) Stop all application processes.
b) Navigate to the temporary directory that you created in Step 6.
c) Enter the **./xnc upgrade --rollback --target-home** {*xnc_directory_to_be_downgraded*} **--backupfile** {*xnc_backup_location_and_zip_filename*} **[--verbose]** command.
d) Restart the application processes.

Note Press Ctrl–F5, or press the Cmd, Shift, and R keys simultaneously when you access Cisco XNC Monitor Manager through a web UI following a rollback.

Starting the Application

Procedure

Note When you are running xnc for the first time, the URL that you need to connect to and the port that it is listening on are displayed on the screen. For example, when you run the ./runxnc.sh script, the following message is displayed on the screen: Web GUI can be accessed using below URL: *[https://<IP_address>: 8443]*.

You can use one of the following options:

Option	Description
no option	
-jmx	
-jmxport *port_number*	Enables JMX remote access on the specified JVM port.
-debug	
-debugsuspend	
-debugport *port_number*	Enables debugging on the specified JVM port.
-start	
-start *port_number*	
-stop	
-status	
-console	
-help	Displays the options for the **./runxnc.sh** command.

Option	Description
-tls	To enable TLS, start the controller by entering the **./runxnc.sh -tls -tlskeystore** *keystore_file_location* **-tlstruststore** *truststore_file_location* command.
-osgiPasswordSync	To set the OSGi web console password same as the XNC password if the XNC password is changed. **Note** This step is optional. If the application is started without this option, the OSGi console can be accessed through the default credentials.

Note Use runxnc.sh script to start Cisco Nexus Data Broker. You have to set a path variable named JAVA_HOME. It sets the path variables that are used for startup and launches the OSGi framework with the specified options. If a user attempts to start the Cisco Nexus Data Broker application with Java version lower than 1.7, an error message is displayed and the application aborts. To resolve the issue, upgrade your current Java version and restart Cisco Nexus Data Broker. If the current Java Version used is lower than 1.8.0_45, a warning message is issued before the start that Upgrade to 1.8.0_45 or above is recommended.

Verifying That The Application is Running

Procedure

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

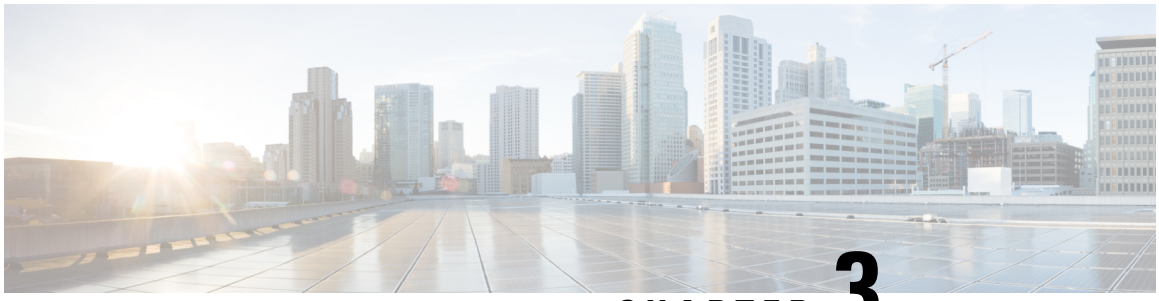
Step 2 Verify that the application is running by entering the **./runxnc.sh -status** command.

The controller outputs the following, which indicates that the controller is running the Java process with PID 21680:

```
Controller with PID:21680 -- Running!
```

What to do next

Connect the switches to the controller. For more information, see the configuration guide for your switches.



CHAPTER 3

Managing TLS Certificate, KeyStore, and TrustStore Files

This chapter contains the following sections:

About the TLS Certificate, KeyStore, and TrustStore Files

Note When Cisco Nexus Data Broker is started in a normal way, the connection to the device is HTTP. When Cisco Nexus Data Broker is started using the TLS protocol, the connection to the device is in HTTPS.

Note To configure High Availability clusters in TLS mode, you need to run Cisco Nexus Data Broker in TLS mode for each instance of Cisco Nexus Data Broker.

Cisco Nexus Series switches connecting to Cisco Nexus Data Broker over OpenFlow require additional credentials, including Private Key, Certificate, and Certificate Authority (CA).

- The TLS TrustStore file contains the Certification Authority (CA) certificates used to sign the certificates on the connecting switches.

Preparing to Generate the TLS Credentials

OpenFlow switches require cryptographic configuration to enable TLS.

The NX-API protocol plugin now supports TLS for secure communication to the devices. You can connect to the NX-API protocol plugin on the secure port 443. All configuration, discovery, and statistics collection is done using secure communication. Cisco Nexus Data Broker should be configured with the required certificates and it should be started in the secure mode. When Cisco Nexus Data Broker is started in TLS mode, all devices support the TLS connection. The normal unencrypted connection to the switches is not accepted.

Caution Self-signed certificates are appropriate only for test environment. For security and granular controls over individual certificate use and revocation, you should use certificates generated by your organization's Certificate Authority. The self-signed certificate do not provide any security in production environment and NXAPI web interface will display as `Not Secure`.

Before you begin

Ensure that OpenSSL is installed on the Linux host where these steps will be performed.

Procedure

Step 1 Create a TLS directory using **mkdir -p TLS** command and then navigate to it using **cd TLS** command:

mkdir -p TLS

cd TLS

Step 2 Set up the directories for your CA system to function within. Create three directories under `mypersonalca` using **mkdir -p mypersonalca/<directory name>** command. To initialize the `serial` file and the `index.txt` file, enter **echo "01" > mypersonalca/serial** command and **touch mypersonalca/index.txt** command respectively.

mkdir -p mypersonalca/certs

mkdir -p mypersonalca/private

mkdir -p mypersonalca/crl

echo "01" > mypersonalca/serial

touch mypersonalca/index.txt

The `serial` file and the `index.txt` file are used by the CA to maintain its database of the certificate files.

Step 3 Create the CA configuration file (ca.conf). Before saving the ca.cnf file, some changes need to be made that are specific to the devices. One critical change is to change the [alt_names] section in the ca.conf file to be relevant to the device IP address, because these IP addresses should be specified in the configuration file. If you need more or fewer IP/DNS names, you can add or remove the lines.

Note This step is applicable to NX-API only.

The following is an example of the content of the ca.conf file:

```
[ ca ]
default_ca              = CA_default


[ CA_default ]
dir                     = .
serial                  = $dir/serial
database                = $dir/index.txt
new_certs_dir           = $dir/newcerts
certs                   = $dir/certs
certificate             = $certs/cacert.pem
private_key             = $dir/private/cakey.pem
default_days            = 365
default_md              = sha1
preserve                = no
email_in_dn             = no
nameopt                 = default_ca
certopt                 = default_ca
policy                  = policy_match
copy_extensions         = copy


[ policy_match ]
countryName             = match
stateOrProvinceName     = match
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional



[ req ]
default_bits            = 2048                  # Size of keys
default_keyfile         = example.key           # name of generated keys
default_md              = sha1                  # message digest algorithm
string_mask             = nombstr               # permitted characters
distinguished_name      = req_distinguished_name
req_extensions          = v3_req
x509_extensions         = v3_req


[ req_distinguished_name ]
# Variable name           Prompt string
#----------------------   ----------------------------------
0.organizationName      = Organization Name (company)
organizationalUnitName  = Organizational Unit Name (department, division)
emailAddress            = Email Address
emailAddress_max        = 40
localityName            = Locality Name (city, district)
stateOrProvinceName     = State or Province Name (full name)
countryName             = Country Name (2 letter code)
countryName_min         = 2
countryName_max         = 2
commonName              = Common Name (hostname, IP, or your name)
commonName_max          = 64


# Default values for the above, for consistency and less typing.
# Variable name                  Value
#------------------------------   ------------------------------
commonName_default             = www.cisco.com
```

```
0.organizationName_default      = Cisco
localityName_default            = San Jose
stateOrProvinceName_default     = CA
countryName_default             = US
emailAddress_default            = webmaster@cisco.com


[ v3_ca ]
basicConstraints        = CA:TRUE
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always,issuer:always



[ v3_req ]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment


# Some CAs do not yet support subjectAltName in CSRs.
# Instead the additional names are form entries on web
# pages where one requests the certificate...
subjectAltName          = @alt_names


[alt_names]
IP.1   = 1.1.1.1
IP.2   = 2.2.2.2
IP.3   = 3.3.3.3
IP.4   = 4.4.4.4


[ server ]
# Make a cert with nsCertType set to "server"
basicConstraints=CA:FALSE
nsCertType                      = server
nsComment                       = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always


[ client ]
# Make a cert with nsCertType set to "client"
basicConstraints=CA:FALSE
nsCertType                      = client
nsComment                       = "OpenSSL Generated Client Certificate"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always
```

Step 4 Once the directory structure is created and the configuration file (ca.cnf) is saved on your disk, create the TLS certificate file.

Generate the TLS private key and Certification Authority (CA) files by entering the **openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -out mypersonalca/certs/ca.pem -outform PEM -keyout mypersonalca/private/ca.key** command. This step generates the TLS private key in PEM format with a key length of 2048 bits and the CA file.

Generate the certificates (**server.key** and **server.crt**) file by entering:

```
openssl req -new -x509 -days 365 -nodes -out server.crt -keyout server.key -config ca.conf
```

Step 5 Copy **server.key** and **server.crt** into respective devices and install by using the following commands:

configure terminal to enter the configure terminal mode.

DEVICE# copy scp://<Username>@<Server_IP/home/TLS/server.crt bootflash: vrf management where bootflash:/// is the file location of **server.key**.

DEVICE# copy scp://<Username>@<Server_IP/home/TLS/server.key bootflash: vrf management where bootflash:/// is the file location of **server.crt**.

nxapi certificate httpskey keyfile bootflash:///server.key where bootflash:/// is the file location of **server.key**.

nxapi certificate httpscrt certfile bootflash:///server.crt where bootflash:/// is the file location of **server.crt**.

nxapi certificate enable

Step 6 Create the TLS KeyStore file.

Note The TLS KeyStore file should be placed in the configuration directory of Cisco Nexus Data Broker.

Copy **server.key** to **xnc-privatekey.pem**. This command copies the **server.key** file that was generated in the previous step. For example, use the command **cp server.key xnc-privatekey.pem**.

Copy **server.crt** to **xnc-cert.pem**. This command makes a copy of the *server.crt* file that was generated in previous step. For example, use the command **cp server.crt xnc-cert.pem**.

Create the **xnc.pem** file, that contains the private key and certificate, by entering the **cat xnc-privatekey.pem xnc-cert.pem > xnc.pem** command.

Convert the PEM file **xnc.pem** file to the file **xnc.p12** file by entering the **openssl pkcs12 -export -out xnc.p12 -in xnc.pem** command. Enter a password at the prompt. This is the Export password. The password must contain at least 6 characters, for example, cisco123. You must use the same password in all the steps. The xnc.pem file is converted to a password-protected .p12 file.

Convert the xnc.p12 to a Java KeyStore (tlsKeyStore) file by entering the **keytool -importkeystore -srckeystore xnc.p12 -srcstoretype pkcs12 -destkeystore tlsKeyStore -deststoretype jks** command. This command converts the xnc.p12 file to a password-protected tlsKeyStore file. Enter a password at the prompt. Use the same password that you entered in previous step.

Step 7 Create the TLS TrustStore file.

The TLS TrustStore file should be placed in the application configuration directory.

Copy the **mypersonalca/certs/ca.pem** file to **sw-cacert.pem**.

Convert the **sw-cacert.pem** file to a Java TrustStore (tlsTrustStore) file by entering the **keytool -import -alias swca1 -file sw-cacert.pem -keystore tlsTrustStore** command.

Enter a password at the prompt. The **sw-cacert.pem** file is converted into a password-protected Java TrustStore (tlsTrustStore) file. The password must be at least six characters long, for example, *cisco123*

Step 8 Start application with TLS.

Complete these steps to start NDB application with TLS:

1. Copy the tlsKeystore and tlsTruststore files to the `configuration` folder under NDB.
2. Start Cisco Nexus Data Broker by entering the **./runxnc.sh -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore ./configuration/tlsTrustStore** command.
3. Cisco Nexus Data Broker starts with TLS enabled.

Step 9 Provide the TLS KeyStore and TrustStore Passwords.

The TLS KeyStore and TrustStore passwords are synced to Cisco Nexus Data Broker so that it can read the password-protected TLS KeyStore and TrustStore files. Complete these steps to configure TLS KeyStore and TrustStore Passwords:

1. Log in to Cisco NDB command interface.
2. Navigate to the `xnc/bin` directory.
3. Enter the TLS KeyStore and TLS TrustStore passwords using the **./xnc config-keystore-passwords [--user {user} --password {password} --url {url} --verbose --prompt --keystore-password {keystore_password} --truststore-password {truststore_password}]** command.
   - user—The user name
   - password—The password for the user.
   - url—The web URL of the application.
   - keystore_password—The TLS KeyStore password.
   - truststore_password—The TLS TrustStore password.

```
./xnc config-keystore-passwords --user admin --password admin --url
https://Nexus_Data_Broker_IP:8443 --verbose --prompt --keystore-password cis123
--truststore-password cis123
```

Step 10 Add the switch into the controller using port number 443.

Note Switch cannot be added into the controller with port 80 after enabling TLS.

Step 11 Verify that the TLS communication is enabled on the switch using the **show nxapi** command.

```
N9K# sh nxapi
nxapi enabled
HTTP Listen on port 80
HTTPS Listen on port 443
N9K#
```

You can also verify the TLS communication status by logging in to Nexus Device Sandbox UI using HTTPS and verify the certificates details and dates.

Generating TLS Self-Signed Certification Between NDB Server and NDB Switch for NXAPI

Complete the following steps to generate TLS self-signed certification between NDB Server and NDB Switch for NXAPI:

Procedure

Step 1 Create a TLS directory using the **mkdir directory_name** and navigate to the new directory.

Example:

```
[ndb]# mkdir -p TLS
[ndb]# cd TLS
```

Step 2 Create 3 directories under mypersonalca folder for CA system.

Example:

```
[ndb]# mkdir -p mypersonalca/certs
[ndb]# mkdir -p mypersonalca/private
[ndb]# mkdir -p mypersonalca/crl
```

Step 3 Initialize the serial file using the **echo** command. The serial file and the index.txt file are used by the CA to maintain its database of the certificate files.

Example:

```
[ndb]# echo "01" > mypersonalca/serial
```

Step 4 Initialize the index file using the **touch** command.

Example:

```
[ndb]# touch mypersonalca/index.txt
```

Step 5 Create a CA configuration file and configure the alt_names section with relevant IP Addresses.

Example:

```
[ ca ]
default_ca = CA_default
[ CA_default ]
dir = .
serial = $dir/serial
database = $dir/index.txt
new_certs_dir = $dir/newcerts
certs = $dir/certs
certificate = $certs/cacert.pem
private_key = $dir/private/cakey.pem
default_days = 365
default_md = sha1
preserve = no
email_in_dn = no
nameopt = default_ca
certopt = default_ca
policy = policy_match
copy_extensions = copy
[ policy_match ]
countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
[req ]
default_bits = 2048 # Size of keys
default_keyfile = example.key # name of generated keys
default_md = sha1 # message digest algorithm
string_mask = nombstr # permitted characters
distinguished_name = req_distinguished_name
```

```
req_extensions = v3_req
x509_extensions = v3_req
[ req_distinguished_name ]
# Variable name Prompt string
#---------------------- ----------------------------------
0.organizationName = Organization Name (company)
organizationalUnitName = Organizational Unit Name (department, division)
emailAddress = Email Address
emailAddress_max = 40
localityName = Locality Name (city, district)
stateOrProvinceName = State or Province Name (full name)
countryName = Country Name (2 letter code)
countryName_min = 2
countryName_max = 2
commonName = Common Name (hostname, IP, or your name)
commonName_max = 64
# Default values for the above, for consistency and less typing.
# Variable name Value
#------------------------------ ------------------------------
commonName_default = www.cisco.com
0.organizationName_default = Cisco
localityName_default = San Jose
stateOrProvinceName_default = CA
countryName_default = US
emailAddress_default = webmaster@cisco.com
[ v3_ca ]
basicConstraints = CA:TRUE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
[ v3_req ]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
# Some CAs do not yet support subjectAltName in CSRs.
# Instead the additional names are form entries on web
# pages where one requests the certificate...
subjectAltName = @alt_names
[alt_names]
IP.1 = 1.1.1.1
IP.2 = 2.2.2.2
IP.3 = 3.3.3.3
IP.4 = 10.16.206.104
[ server ]
# Make a cert with nsCertType set to "server"
basicConstraints=CA:FALSE
nsCertType = server
nsComment = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always
[ client ]
# Make a cert with nsCertType set to "client"
basicConstraints=CA:FALSE
nsCertType = client
nsComment = "OpenSSL Generated Client Certificate"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always
```

Step 6 Generate the TLS private key and Certification Authority (CA) files using the **openssl req** command. The TLS private key is created in PEM format with a key length of 2048 bits and the CA file.

Example:

```
openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -out mypersonalca/certs/ca.pem -outform
 PEM -keyout mypersonalca/private/ca.key
```

```
Generating a 2048 bit RSA private key
.....................................................................................................................+++
.....................................+++
writing new private key to 'mypersonalca/private/ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:CA
Locality Name (eg, city) [Newbury]:SJ
Organization Name (eg, company) [My Company Ltd]:cisco
Organizational Unit Name (eg, section) []:insbu
Common Name (eg, your name or your server's hostname) []:N9K-104.cisco.com
Email Address []:xyz@abc.com
```

Step 7 Generate the certificate files, server.key and server.crt, using the **openssl req** command.

Example:

```
openssl req -new -x509 -days 365 -nodes -out server.crt -keyout server.key -config ca.conf
Generating a 2048 bit RSA private key
.....+++
.....................................+++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Organization Name (company) [Cisco]:cisco
Organizational Unit Name (department, division) []:insbu
Email Address [webmaster@cisco.com]:kemanoha@cisco.com
Locality Name (city, district) [San Jose]:SJ
State or Province Name (full name) [CA]:CA
Country Name (2 letter code) [US]:US
Common Name (hostname, IP, or your name) [www.cisco.com]:N9K-104.cisco.com
```

Step 8 Copy server.key and server.crt to the respective devices and install the certificate files using the **nxapi certificate httpskey keyfile** command.

Example:

```
configure terminal to enter the configure terminal mode.
DEVICE# copy scp://<Username>@<Server_IP/home/TLS/server.crt bootflash: vrf management where
```

```
 bootflash:/// is the file location of server.key.
DEVICE# copy scp://<Username>@<Server_IP/home/TLS/server.key bootflash: vrf management where
 bootflash:/// is the file location of server.crt.
nxapi certificate httpskey keyfile bootflash:///server.key where bootflash:/// is the file
 location of server.key.
nxapi certificate httpscrt certfile bootflash:///server.crt where bootflash:/// is the file
 location of server.crt.
nxapi certificate enable
```

Step 9 Create the TLS KeyStore file. Copy the TLS Keystore in the configuration directory of Cisco Nexus Data Broker.

Example:

Example:

```
# cp server.key xnc-privatekey.pem
//Copies server.key to xnc-privatekey.pem
# cp server.crt xnc-cert.pem
//Copies server.crt to xnc-cert.pem
# cat xnc-privatekey.pem xnc-cert.pem > xnc.pem
//Creates the xnc.pem file, that contains the private key and certificate
# openssl pkcs12 -export -out xnc.p12 -in xnc.pem
//Converts the PEM file xnc.pem file to the file xnc.p12 file. Enter the export
//passowrd at the prompt. Use the same password in all the steps. The xnc.pem file
//is converted to a password-protected .p12 file.
# keytool -importkeystore -srckeystore xnc.p12 -srcstoretype pkcs12 -destkeystore tlsKeyStore
 -deststoretype jks
//Converts the xnc.p12 to a password protected Java KeyStore (tlsKeyStore) file
# cp server.crt xnc-cert.pem
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
Entry for alias 1 successfully imported.
Import command completed: 1 entries successfully imported, 0 entries
failed or cancelled
```

Step 10 Create the TLS TrustStore file. Copy the TLS Keystore in the application configuration directory of Cisco Nexus Data Broker.

Example:

```
# cp mypersonalca/certs/ca.pem sw-cacert.pem
//Copies the mypersonalca/certs/ca.pem file to sw-cacert.pem
# keytool -import -alias swca1 -file sw-cacert.pem -keystore tlsTrustStore
//Converts the sw-cacert.pem file to a password protected Java TrustStore (tlsTrustStore)
file
Enter keystore password:
Re-enter new password:
Owner: EMAILADDRESS=kemanoha@cisco.com, CN=N9K-104.cisco.com, OU=insbu,
O=cisco, L=SJ, ST=CA, C=US
Issuer: EMAILADDRESS=kemanoha@cisco.com, CN=N9K-104.cisco.com, OU=insbu,
 O=cisco, L=SJ, ST=CA, C=US
Serial number: 9f383a65a18c77e8
Valid from: Sun May 13 18:25:12 PDT 2018 until: Wed May 10 18:25:12 PDT
2028
Certificate fingerprints:
MD5: BE:72:CD:62:3F:1F:DB:A3:E4:8F:E5:BE:7F:3A:3A:D3
SHA1: DA:A1:32:89:3C:C7:0E:A5:08:B3:D9:6C:BC:71:7B:C0:64:3B:CB:16
SHA256:
```

```
6D:DE:03:D1:A7:1C:16:CE:B2:72:46:90:6D:9B:7D:46:86:DC:5F:72:71:1B:3F:33:0B:99:9F:51:AD:B0:EC:DB
Signature algorithm name: SHA1withRSA
Version: 3
Extensions:
#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: FE 5A C8 68 CE 8D D7 98 27 E8 54 88 87 89 63 F4 .Z.h....'.T...c.
0010: 1B 28 77 14 .(w.
]
[EMAILADDRESS=kemanoha@cisco.com, CN=N9K-104.cisco.com, OU=insbu, O=cisco,
 L=SJ, ST=CA, C=US]
SerialNumber: [ 9f383a65 a18c77e8]
]
#2: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:true
PathLen:2147483647
]
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: FE 5A C8 68 CE 8D D7 98 27 E8 54 88 87 89 63 F4 .Z.h....'.T...c.
0010: 1B 28 77 14 .(w.
]
]
Trust this certificate [no]: yes
Certificate was added to keystore
```

Step 11 Restart NDB application with TLS

Example:

```
# cp mypersonalca/certs/ca.pem sw-cacert.pem
//Copies the tlsKeystore and tlsTruststore files to the configuration folder under NDB.
# ./runxnc.sh -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore
./configuration/tlsTrustStore
//Starts the NSB application
```

Step 12 Enter the TLS KeyStore and TrustStore passwords.

Step 13 Configure TLS KeyStore and TrustStore Passwords

a) Log in to Cisco NDB command interface.
b) Navigate to the xnc/bin directory.
c) Configure the TLS KeyStore and TLS TrustStore passwords using the **../xnc config-keystore-passwords [--user {user} --password {password} --url {url} --verbose --prompt --keystore-password {keystore_password} --truststore-password {truststore_password}]** command.

Example:

```
. /xnc config-keystore-passwords --user admin --password admin --url
https://Nexus_Data_Broker_IP:8443 --verbose --prompt --keystore-password pwd123
--truststore-password pwd123
```

Step 14 Add the switch into the controller using port number 443.

Note You cannot add a switch into the controller with port 80 after enabling TLS.

Step 15 Verify that the TLS communication is enabled on the switch using the **show nxapi** command.

Example:

```
N9K# sh nxapi
nxapi enabled
HTTP Listen on port 80
HTTPS Listen on port 443
N9K#
```

Note You can also verify the TLS communication status by logging in to Nexus Device Sandbox UI using HTTPS and verify the certificates details and dates.

Generating TLS Self-Signed Certification Between NDB Server and NDB Switch for OpenFlow

Complete the following steps to generate TLS self-signed certification between NDB Server and NDB Switch for OpenFlow:

Procedure

Step 1 Create a TLS directory using the **mkdir directory_name** and navigate to the new directory.

Example:

```
[]# mkdir -p TLS
[]# cd TLS
```

Step 2 Create 3 directories under mypersonalca folder for CA system.

Example:

```
[]# mkdir -p mypersonalca/certs
[]# mkdir -p mypersonalca/private
[]# mkdir -p mypersonalca/crl
```

Step 3 Initialize the serial file using the **echo** command. The serial file and the index.txt file are used by the CA to maintain its database of the certificate files.

Example:

```
[]# echo "01" > mypersonalca/serial
```

Step 4 Initialize the index file using the **touch** command.

Example:

```
[]# touch mypersonalca/index.txt
```

Step 5 Create a CA configuration file and configure the alt_names section with relevant IP Addresses.

Example:

```
[ ca ]
default_ca = mypersonalca
[ mypersonalca ]
#
# WARNING: if you change that, change the default_keyfile in the [req] section below too
# Where everything is kept
dir = ./mypersonalca
# Where the issued certs are kept
certs = $dir/certs
# Where the issued crl are kept
crl_dir = $dir/crl
# database index file
database = $dir/index.txt
# default place for new certs
new_certs_dir = $dir/certs
#
# The CA certificate
certificate = $dir/certs/ca.pem
# The current serial number
serial = $dir/serial
# The current CRL
crl = $dir/crl/crl.pem
# WARNING: if you change that, change the default_keyfile in the [req] section below too
# The private key
private_key = $dir/private/ca.key
# private random number file
RANDFILE = $dir/private/.rand
# The extentions to add to the cert
x509_extensions = usr_cert
# how long to certify for
default_days = 365
# how long before next CRL
default_crl_days= 30
# which md to use; people in comments indicated to use sha1 here
default_md = sha1
# keep passed DN ordering
preserve = no
# Section names
policy = mypolicy
x509_extensions = certificate_extensions
[ mypolicy ]
# Use the supplied information
commonName = supplied
stateOrProvinceName = optional
countryName = optional
emailAddress = optional
organizationName = optional
organizationalUnitName = optional
[ certificate_extensions ]
# The signed certificate cannot be used as CA
basicConstraints = CA:false
[ req ]
# same as private_key
default_keyfile = ./mypersonalca/private/ca.key
# Which hash to use
default_md = sha1
# No prompts
prompt = no
# This is for CA
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer
```

```
string_mask = utf8only
basicConstraints = CA:true
distinguished_name = root_ca_distinguished_name
x509_extensions = root_ca_extensions
[ root_ca_distinguished_name ]
commonName = Controller
stateOrProvinceName = Mass
countryName = US
emailAddress = root_ca_userid@cisco.com
organizationName = Cisco
[ root_ca_extensions ]
basicConstraints = CA:true
```

Step 6 Generate the TLS private key, certificate, and Certification Authority (CA) files using the **openssl req** command. The TLS private key is created in PEM format with a key length of 2048 bits and the CA file.

Example:

```
openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -out mypersonalca/certs/ca.pem -outform
 PEM -keyout mypersonalca/private/ca.key
Generating a 2048 bit RSA private key
.............+++
...............................+++
writing new private key to 'mypersonalca/private/ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Mass
Locality Name (eg, city) []:San
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:NDB
Common Name (e.g. server FQDN or YOUR name) []:Controller
Email Address []:masavanu@cisco.com
```

Note This step generates the TLS private key in PEM format with a key length of 2048 bits, and the CA file.

Step 7 Generate the certificate key and certificate request files, using the **openssl req** command.

Example:

```
openssl req -newkey rsa:2048 -keyout cert.key -keyform PEM -out cert.req -outform
PEMGenerating a 2048 bit RSA private key
Generating a 2048 bit RSA private key
.........................................+++
........+++
writing new private key to 'cert.key'
Enter PEM pass phrase:(Enter pwd123 here)
Verifying - Enter PEM pass phrase:(Enter pwd123 here)
```

```
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Mass
Locality Name (eg, city) []:San
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:NDB
Common Name (e.g. server FQDN or YOUR name) []:Controller
Email Address []:masavanu@cisco.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:pwd123
An optional company name []:
```

Note This step generates the controller key (cert.key) and certificate request (cert.req) files in PEM format.

Step 8 Generate the certificate file, using the **openssl ca** command.

Example:

```
openssl ca -batch -notext -in cert.req -out cert.pem -config ca.cnf
Using configuration from ca.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'US'
stateOrProvinceName :ASN.1 12:'Mass'
localityName :ASN.1 12:'San'
organizationName :ASN.1 12:'Cisco'
organizationalUnitName:ASN.1 12:'NDB'
commonName :ASN.1 12:'Controller'
emailAddress :IA5STRING:'masavanu@cisco.com'
Certificate is to be certified until May 17 02:59:40 2017 GMT (365 days)
Write out database with 1 new entries
Data Base Updated
```

Note This step generates the certificate (cert.pem) file in PEM format using the certificate request (cert.req) and the certificate configuration (ca.cnf) files.

Step 9 Configure the Cryptographic Keys on the Switch.

Example:

```
switch(config)# ip domain-name domain-name
//Configures the domain name for the switch
switch(config)# crypto key generate rsa label myKey2 exportable modulus 2048
//Generates the cryptographic key.
switch(config)# crypto ca trustpoint myCA
//Enters the trustpoint configuration mode and installs the trustpoint file on the switch
```

```
switch(config-trustpoint)# rsakeypair myKey2
//Installs the key files on the switch
switch(config-trustpoint)# exit
//Exits trustpoint configuration mode
switch# show crypto ca trustpoints
//(Optional) Verifies creation of the trustpoint files.
switch# show crypto key mypubkey rsa
//(Optional) Verifies creation of the key files.
cat mypersonalca/certs/ca.pem
//Displays the certificate file on the machine hosting the generated TLS certificates
switch(config)# crypto ca authenticate myCA
-----BEGIN CERTIFICATE----------
-----END CERTIFICATE-----
END OF INPUT:
Fingerprint(s): SHA1
Fingerprint=56:0F:56:85:6A:07:A1:44:6C:F4:4C:45:CF:CC:BA:47:22:17:1D:93
Do you accept this certificate [yes/no]:yes

switch(config)# crypto ca enroll myCA
//Generates the certificate request on the switch

Create the certificate request ..
Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:pwd123
The subject name in the certificate will be the name of the switch.
Include the switch serial number in the subject name [yes/no]:no
Include an IP address in the subject name [yes/no]:no
Include the Alternate Subject Name  [yes/no]:no
The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
.....
-----END CERTIFICATE REQUEST-----
openssl ca -in n3k-cert.req -out newcert.pem -config ./ca.cnf
//Copies the certificate request from the switch to the file n3k-cert.req on your Linux
machine, and then uses it to generate the switch certificate.
Using configuration from ./ca.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName :PRINTABLE:'ndb-3172-4.cisco.com'
Certificate is to be certified until May 17 04:27:57 2017 GMT (365 days)
Sign the certificate [y/n]:y
out of 1 certificate requests certified, commit [y/n]y
Write out database with 1 new entries
Data Base Updated

cat newcert.pem
//Copies the certificate (newcert.pem) to the switch

switch(config)# crypto ca import myCA certificate
switch(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
```

```
switch# show crypto ca certificates
//Displays the certificates on the switch
```

Step 10 Enable the TLS OpenFlow Switches

Example:

```
switch(config)# openflow
//Enters OpenFlow agent configuration mode on the switch.
switch(config-ofa)# switch 1
//Enters OpenFlow agent configuration mode for switch 1.
switch(config-ofa)# tls trust-point local myCA remote myCA
//Enables TLS certificate authority on the switch.
switch(config-ofa-switch)# pipeline{201/203}
//Configures the pipeline
switch(config-ofa-switch)#controller ipv4 {A.B.C.D} port 6653 vrf management security tls
//Enables TLS for OpenFlow switches
```

Step 11 Create the TLS KeyStore File

Example:

```
cp cert.key xnc-privatekey.pem
//Copy cert.key to xnc-privatekey.pem
cp cert.pem xnc-cert.pem
//Copy cert.pem to xnc-cert.pem under TLS folder
cat xnc-privatekey.pem xnc-cert.pem > xnc.pem
Creates the xnc.pem file, which contains the private key and certificate.

openssl pkcs12 -export -out xnc.p12 -in xnc.pem
//Convert the PEM file xnc.pem file to the file xnc.p12
Enter a password at the prompt
The xnc.pem file is converted to a password-protected .p12 file.
openssl pkcs12 -export -out xnc.p12 -in xnc.pem
Enter pass phrase for xnc.pem:(enter pass phrase as pwd123)
Enter Export Password:(Enter Export password as pwd123)
Verifying - Enter Export Password:(Enter as pwd123)
```

Step 12 Convert the xnc.p12 file to password protected TLS KeyStore

Example:

```
keytool -importkeystore -srckeystore xnc.p12 -srcstoretype pkcs12 -destkeystore tlsKeyStore
 -deststoretype jks
Enter destination keystore password: (Enter pwd123)
Re-enter new password: (Enter pwd123)
Enter source keystore password: (Enter pwd123)
Entry for alias 1 successfully imported.
Import command completed: 1 entries successfully imported, 0 entries
failed or cancelled
```

Step 13 Enter the TLS KeyStore password.

Step 14 Create the TLS TrustStore File.

Example:

```
cp mypersonalca/certs/ca.pem sw-cacert.pem
//Copies the mypersonalca/certs/ca.pem file to sw-cacert.pem
keytool -import -alias swca1 -file sw-cacert.pem -keystore tlsTrustStore
Enter keystore password: (Enter pwd123)
Re-enter new password: (Enter pwd123)
Owner: EMAILADDRESS=masavanu@cisco.com, CN=Controller, OU=NDB, O=Cisco,
```

```
L=San, ST=Mass, C=US
Issuer: EMAILADDRESS=masavanu@cisco.com, CN=Controller, OU=NDB, O=Cisco,
 L=San, ST=Mass, C=US
Serial number: d764c5b1e5e6b531
Valid from: Mon May 16 22:49:13 EDT 2016 until: Thu May 14 22:49:13 EDT
2026
Certificate fingerprints:
MD5: BD:C8:21:13:D0:7F:ED:A4:B4:FA:97:9A:D0:EA:12:78
SHA1: 56:0F:56:85:6A:07:A1:44:6C:F4:4C:45:CF:CC:BA:47:22:17:1D:93
SHA256:
09:32:74:12:BF:56:04:07:42:8C:D8:1B:78:AD:7A:40:0D:51:AA:56:91:B1:1A:18:90:6A:A5:A0:44:04:6A:EC
Signature algorithm name: SHA256withRSA
Version: 3
Extensions:
#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 78 C5 2B 09 7F AF EC 86 FE 50 EA 6C 8A 56 B3 BE x.+......P.l.V..
0010: BE F2 97 98 ....
]
]
#2: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:true
PathLen:2147483647
]
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 78 C5 2B 09 7F AF EC 86 FE 50 EA 6C 8A 56 B3 BE x.+......P.l.V..
0010: BE F2 97 98 ....
]
]
Trust this certificate [no]: yes
Certificate was added to keystore
```

Note The sw-cacert.pem file is converted into a password-protected Java TrustStore (tlsTrustStore) file.

Starting the NDB Application with TLS Enabled

Complete the following steps to start NDB application with TLS enabled.

Before you begin

Copy TLS Truststore and TLS Keystore files created under TLS folder to the configuration directory of Cisco Nexus Data Broker.

Procedure

Step 1 Start the NDB application using the **runxnc.sh** script.

Example:

```
./runxnc.sh -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore
./configuration/tlsTrustStore
```

Example:

To start NDB with default username (admin) and a non-default password (for example, pwd123):

```
./runxnc.sh -osgiPasswordSync -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore
 ./configuration/tlsTrustStore
If XNC password is changed, OSGi webconsole password needs to be changed,

to set non-default OSGi webconsole password Enter XNC Admin Password
[default] :( Type the non-default password which was set.
```

Example:

To start NDB with default username (admin) and password (admin):

```
./runxnc.sh -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore
./configuration/tlsTrustStore
```

Step 2 Configure the TLS KeyStore and TrustStore passwords in Cisco NDB. You need to configure TLS KeyStore and TrustStore Passwords to enable NDB to read the password-protected TLS KeyStore and TrustStore files.

Example:

```
xnc/bin directory# ./xnc config-keystore-passwords --user admin --password admin --url
https://NDB_URL:8443
--verbose --prompt --keystore-password pwd123 --truststore-password pwd123
```

If the TLS KeyStore and TrustStore passwords configuration fails with `Failed to connect to the controller`, you need to change the protocol to HTTP.

```
./xnc config-keystore-passwords --user admin --password admin --url https://localhost:8443
 --verbose --prompt --keystore-password pwd123 --truststore-password pwd123
[Info] Sending request: https://10.16.206.189:8443/controller/osgi/system/console/vmstat
---- REQUEST HEADERS ----
GET https://10.16.206.189:8443/controller/osgi/system/console/vmstat HTTP/1.1
-------------------------
[Error] Failed to connect to the controller at "https://10.16.206.189:8443". Controller may
 not be running.
javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException:
No subject alternative names present
at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1949)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:302)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:296)
at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1509)
at sun.security.ssl.ClientHandshaker.processMessage(ClientHandshaker.java:216)
at sun.security.ssl.Handshaker.processLoop(Handshaker.java:979)
at sun.security.ssl.Handshaker.process_record(Handshaker.java:914)
at sun.security.ssl.SSLSocketImpl.readRecord(SSLSocketImpl.java:1062)
at sun.security.ssl.SSLSocketImpl.performInitialHandshake(SSLSocketImpl.java:1375)
at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1403)
at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1387)
at sun.net.www.protocol.https.HttpsClient.afterConnect(HttpsClient.java:559)
at
```

```
sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.java:185)

at sun.net.www.protocol.http.HttpURLConnection.getInputStream0(HttpURLConnection.java:1513)

at sun.net.www.protocol.http.HttpURLConnection.getInputStream(HttpURLConnection.java:1441)

at java.net.HttpURLConnection.getResponseCode(HttpURLConnection.java:480)
at
sun.net.www.protocol.https.HttpsURLConnectionImpl.getResponseCode(HttpsURLConnectionImpl.java:338)

at com.cisco.csdn.cli.online.HttpClient$HttpResponse.<init>(HttpClient.java:191)
at com.cisco.csdn.cli.online.HttpClient.sendRequest(HttpClient.java:108)
at com.cisco.csdn.cli.online.HttpClient.get(HttpClient.java:92)
at com.cisco.csdn.cli.online.OnlineCommand.isRunning(OnlineCommand.java:88)
at
com.cisco.csdn.cli.online.ConfigKeyStorePasswordCommand.processCommand(ConfigKeyStorePasswordCommand.java:46)

at com.cisco.csdn.cli.Cli.processCommand(Cli.java:70)
at com.cisco.csdn.cli.Main.main(Main.java:33)
Caused by: java.security.cert.CertificateException: No subject alternative names present
at sun.security.util.HostnameChecker.matchIP(HostnameChecker.java:144)
at sun.security.util.HostnameChecker.match(HostnameChecker.java:93)
at sun.security.ssl.X509TrustManagerImpl.checkIdentity(X509TrustManagerImpl.java:455)
at sun.security.ssl.X509TrustManagerImpl.checkIdentity(X509TrustManagerImpl.java:436)
at sun.security.ssl.X509TrustManagerImpl.checkTrusted(X509TrustManagerImpl.java:200)
at sun.security.ssl.X509TrustManagerImpl.checkServerTrusted(X509TrustManagerImpl.java:124)

at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1491)
... 20 more

//Change the protocol to HTTP.
./xnc config-keystore-passwords --user admin --password admin --url http://localhost:8080
--verbose --prompt --keystore-password pwd123 --truststore-password pwd123
```

Generating the Java tlsKeyStore and tlsTrustStore for NDB Controller

Complete the following steps to generate the Java tlsKeyStore and tlsTrustStore files for NDB Controller:

Procedure

Step 1 Create a TLS directory using the **mkdir directory_name** and navigate to the new directory.

Example:

```
[]# mkdir -p TLS
[]# cd TLS
```

Step 2 Create 3 directories under mypersonalca folder for CA system.

Example:

```
[]# mkdir -p mypersonalca/certs
```

```
[]# mkdir -p mypersonalca/private
[]# mkdir -p mypersonalca/crl
```

Step 3 Initialize the serial file using the **echo** command. The serial file and the index.txt file are used by the CA to maintain its database of the certificate files.

Example:

```
[]# echo "01" > mypersonalca/serial
```

Step 4 Initialize the index file using the **touch** command.

Example:

```
[]# touch mypersonalca/index.txt
```

Step 5 Generate the TLS private key and Certification Authority (CA) files for each switch connected to NDB using the **openssl req** command. The TLS private key is created in PEM format with a key length of 2048 bits and the CA file.

Example:

```
docker@docker-virtual-machine:~/TLS$ openssl req -x509 -nodes -days 3650 -newkey rsa:2048
-out mypersonalca/certs/sw1-ca.pem -outform PEM -keyout mypersonalca/private/sw1-ca.key

Generating a 2048 bit RSA private key
...+++
.........................................+++
writing new private key to 'mypersonalca/private/sw1-ca.key'
-----
You are about to be asked to enter information that will be incorporated
 into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value, If you enter '.', the field
 will be left blank.
----- Country Name (2 letter code) [AU]:US State or Province Name (full
name) [Some-State]:CA Locality Name (eg, city) []:SJ Organization Name
(eg, company) [Internet Widgits Pty Ltd]:cisco
Organizational Unit Name (eg, section) []:insbu Common Name (e.g. server
 FQDN or YOUR name) []:N9K-117.cisco.com Email Address []:myname@cisco.com
```

Note Save the `sw1-ca.pem` file in `mypersonalca/certs` directory and `sw1-ca.key` file in the `mypersonalca/private` directory.

Step 6 Copy the `cert.key` and `server.cer` to each switch.

Example:

```
cp cert.key sw1-xnc-privatekey.pem
cp server.cer sw1-xnc-cert.pem
```

Step 7 Create the sw1-xnc.pem file, which contains the private key and certificate using the **cat** command.

Example:

```
cat sw1-xnc-privatekey.pem sw1-xnc-cert.pem > sw1-xnc.pem
```

Step 8 Convert the PEM file to PKSC12 file format, using the openssl command. For example, sw1-xnc.pem file to sw1-xnc.p12 file.

Example:

```
docker@docker-virtual-machine:~/TLS$ openssl pkcs12 -export - out sw1-xnc.p12 -in sw1-xnc.pem
Enter Export Password:pwd123
Verifying - Enter Export Password:pwd123
Enter a password at the prompt. Use the same password that you entered in previous
Step(pwd123)
```

Step 9 Convert the sw1-xnc.p12 to a password protected Java KeyStore (tlsKeyStore) file using the **keytool** command.

Example:

```
docker@docker-virtual-machine:~/TLS$ keytool -importkeystore -srckeystore sw1-xnc.p12
-srcstoretype pkcs12 -destkeystore tlsKeyStore -deststoretype jks
Enter destination keystore password:pwd123
Re-enter new password: pwd123
Enter source keystore password: pwd123
Entry for alias 1 successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled
```

Note By default, an allias named "1" is stored in tlsKeyStore for the first switch. When the second switch is added, the utility lets you to rename the first switch alias and also provides a provision to give alias name for the new switck.

Note If the NDB controller is managing multiple switches, repeat the above step for all the switches.

Step 10 List and verift the contents in the Java tlsKeyStore file after all the certificates are added to the keystore using the **keytool** command.

Example:

```
keytool -list -v -keystore tlsKeyStore | more
```

Step 11 Create the TLS TrustStore File.

Example:

```
docker@docker-virtual-machine:~/TLS$ keytool -import -alias sw1 -file
mypersonalca/certs/sw1-ca.pem -keystore tlsTrustStore
Enter keystore password: pwd123
Re-enter new password: pwd123
Owner: EMAILADDRESS=myname@cisco.com, CN=localhost, OU=insbu, O=cisco, L=SJ, ST=CA, C=US
Issuer: EMAILADDRESS=myname@cisco.com, CN=localhost, OU=insbu, O=cisco, L=SJ, ST=CA, C=US
Serial number: c557f668a0dd2ca5
Valid from: Thu Jun 15 05:43:48 IST 2017 until: Sun Jun 13
05:43:48 IST 2027
Certificate fingerprints:
MD5: C2:7B:9E:26:31:7A:74:25:55:DF:A7:91:C9:5D:20:A3
SHA1:
3C:DF:66:96:72:12:CE:81:DB:AB:58:30:60:E7:CC:04:4D:DF:6D:B2
SHA256: DD:FB:3D:71:B4:B8:9E:CE:97:A3:E4:2D:D3:B6:90:CD:76:A8:5F:84:77
:78:BE:49:6C:04:01:84:62:2C:2F:EB
Signature algorithm name: SHA256withRSA Version: 3
Extensions:
#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [ KeyIdentifier [
0000: 0D B3 CF 81 66 4A 33 4E EF 86 7E 26 C3 50 9B 73
....fJ3N...&.P.s
0010: 38 EF DF 40 8..@
```

```
]
]
#2: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[ CA:true PathLen:2147483647
]
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [ KeyIdentifier [
0000: 0D B3 CF 81 66 4A 33 4E EF 86 7E 26 C3 50 9B 73
....fJ3N...&.P.s
0010: 38 EF DF 40 8..@
]
]
Trust this certificate [no]: yes
Certificate was added to keystore
```

Note If NDB controller manages multiple switches, add all switch keys into the same TrustStore. Use **keytool -list -v -keystore tlsTrustStore | more** command to see the keys for multiple switches in the same tlsTrustStore.

Step 12 Start the NDB application with TLS.

Example:

```
./runxnc.sh –stop
cp tlsKeystore xnc/configuration
cp tlsTruststore xnc/configuration
./runxnc.sh -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore
./configuration/tlsTrustStore
```

Step 13 Configure the TLS KeyStore and TrustStore passwords in Cisco NDB. You need to configure TLS KeyStore and TrustStore Passwords to enable NDB to read the password-protected TLS KeyStore and TrustStore files.

Example:

```
xnc/bin directory# ./xnc config-keystore-passwords --user admin --password admin --url
https://NDB_URL:8443
--verbose --prompt --keystore-password pwd123 --truststore-password pwd123
```

Table 2: Troubleshooting TLS Implementation

Error Log	Cause	Solution
2017-06-23 18:41:52.787 IST [http-bio-8443-exec-7] DEBUG com.cisco.nbp.tool_plugin.api.service.internal.RestService - REST method: POST url: https://10.16.206.117:443/ins caught exception: Certificate for <10.16.206.117> doesn't match common name of the certificate subject: N9k-117.cisco.com 2017-06-23 18:41:52.787 IST [http-bio-8443-exec-7] ERROR com.cisco.nbp.tool_plugin.api.service.internal.ErrorHandler - Failed to connect to 10.16.206.117, Error: javax.net.ssl.SSLException: Certificate for <10.16.206.117> doesn't match common name of the certificate subject: N9k-117.cisco.com	Occurs when the common name used in the certificate does not match names the switch.	1. Add switch FQDN in /etc/hosts on the serever where NDB is running to resolve the DNS (if you have configured a DNS, this solution may not help.) 2. Add the switch using FQDN in NDB device connection – for example, use N9K-117.cisco.com instead of IP address. 3. Ensure that IP domain and hostname are correctly configured in the switch. 4. Switch FQDN is resolved through DNS

Generating TLS Self-Signed Certification Between WebUI Browser and NDB Server

By default Cisco NDB is shipped with default certificate which is issued to Cisco XNC and issued by Cisco XNC with default validity. You can use the **generateWebUIcertificate.sh** script under configuration folder to create self-signed certificates that are valid for 6 months. You can also configure the validity of certificate. Complete the following steps to generate TLS self-signed certification between WebUI Browser and NDB Server:

Procedure

Step 1 Generate the TLS self-signed certificate using the **generateWebUIcertificate.sh** script.

Example:

```
cisco@cisco:~/user/NDB3.5_centra_cco/xnc/configuration$ ./generateWebUIcertificate.sh
 **********************************
Enter Fully qualified domain name:
**********************************
10.16.206.117 (This can be FQDN of the NDB java application as well).
**************************
Enter Organizational unit :
```

```
**************************
INSBU
********************
Enter Organization :
********************
cisco
****************
Enter Location :
****************
SJ
*************
Enter State :
*************
CA
***************
Enter Country :
***************
USA
***************
Enter keypass :
***************
pwd123
*****************
Enter storepass :
******************
pwd123
************************************
Enter the validity in number of days :
************************************
365
*****************************************************************************************************************************

Below process will rename the existing key file to <old_keystore>, will generate a new key
 file. Do you want to continue (y/n)?
*****************************************************************************************************************************

y
*******************************
Self-Signed Certificate Created
*******************************
Alias name: cisco
Creation date: Jan 3, 2018
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=10.16.206.117, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Issuer: CN=10.16.206.117, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Serial number: 2e61c095
Valid from: Wed Jan 03 07:05:39 EST 2018 until: Thu Jan 03 07:05:39 EST 2019
Certificate fingerprints:
MD5: 9F:9C:A2:2C:48:89:05:B9:54:DA:5E:84:57:E2:84:0B
SHA1: 6D:A2:C4:11:0C:65:E5:C2:2A:33:BA:39:9E:52:2A:EF:76:33:C1:E6
SHA256:
11:A6:B6:88:BA:91:81:41:7C:73:D3:5B:ED:AE:FD:96:B5:B7:F4:C6:16:67:CF:96:77:FD:67:74:BF:2B:1A:6B

Signature algorithm name: SHA256withRSA
Version: 3
Extensions:
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier
[ KeyIdentifier [ 0000: 95 88 E6 C9 07 A7 1C 7C 9B 0F AC F6 76 16 5C 9D ............v.\.
0010: E5 AB 17 FF .... ] ]
*******************************
Displayed the generated keystore
```

```
*******************************
************************************************
Configured the keystore details on tomcat-server.xml
************************************************
*****************************************************************************************

The newly generated key will used on next NDB restart. Do you want to restart NDB now (y/n)
 ?
*****************************************************************************************

y
Controller with PID: 11757 -- Stopped!
Another instance of controller running, check with ./runxnc.sh -status
*************
NDB Restarted
*************
cisco@cisco:~/user/NDB3.5_centra_cco/xnc/configuration$ ps -ef | grep java
cisco 19320 1 99 07:06 pts/6 00:00:08 jre1.8.0_131/bin/java -server
-XX:+HeapDumpOnOutOfMemoryError -Xmx1024m -XX:MaxMetaspaceSize=256m
-Djava.io.tmpdir=/home/cisco/Mallik/NDB3.5_centra_cco/xnc/work/tmp
-Dosgi.install.area=/home/cisco/Mallik/NDB3.5_centra_cco/xnc
-Dosgi.configuration.area=/home/cisco/Mallik/NDB3.5_centra_cco/xnc/configuration
-Dosgi.frameworkClassPath=file:/home/cisco/Mallik/NDB3.5_centra_cco/xnc/lib/org.eclipse.osgi-3.8.1.v20120830-144521.jar,
file:/home/cisco/Mallik/NDB3.5_centra_cco/xnc/lib/org.eclipse.virgo.kernel.equinox.extensions-3.6.0.RELEASE.jar,
file:/home/cisco/Mallik/NDB3.5_centra_cco/xnc/lib/org.eclipse.equinox.launcher-1.3.0.v20120522-1813.jar

-Dosgi.framework=file:/home/cisco/Mallik/NDB3.5_centra_cco/xnc/lib/org.eclipse.osgi-3.8.1.v20120830-144521.jar

-Dosgi.console.ssh=2400 -Djava.awt.headless=true -Dinteractive=0
-classpath
/home/cisco/Mallik/NDB3.5_centra_cco/xnc/lib/org.eclipse.osgi-3.8.1.v20120830-144521.
jar:/home/cisco/Mallik/NDB3.5_centra_cco/xnc/lib/org.eclipse.virgo.kernel.equinox.extensions-3.6.0.RELEASE.
jar:/home/cisco/Mallik/NDB3.5_centra_cco/xnc/lib/org.eclipse.equinox.launcher-1.3.0.v20120522-1813.
jar org.eclipse.equinox.launcher.Main -consoleLog cisco 23419 18805 0 07:06 pts/6 00:00:00
 grep --color=auto java
cisco@cisco:~/Mallik/NDB3.5_centra_cco/xnc/configuration$
```

Note Use **keytool -list -v -keystore keystore_Name** command to decode the certificate.

Note The **generateWebUIcertificate.sh** script reloads the NDB application to ensure that the browser starts using this certificate when we access NDB java application from the browser.

Step 2 Add this certificate to Trusted Root certificate store on the browser. See help for respective Web browsers about how to add the certificate to the Trusted Root certificate store.

Converting JKS Format Key to PKCS12 Format

The self-signed certificates are generated in JKS format which is not compatible with the browsers. Hence, you need to convert these certificates into PKCS12 format before importing the certificate in the browser. Complete the following steps to convert JKS format certificate to PKCS12 format.

Note Ensure that you keep a copy of the original certificates before proceeding with the conversion.

Procedure

Step 1 Convert JKS format certificate into PKCS12 format using the **keytool** command.

Example:

```
 keytool -importkeystore -srckeystore keystore -srcstorepass pwd123 -srckeypass pwd123
-destkeystore keystore.p12 -deststoretype PKCS12 -srcalias cisco -deststorepass pwd123
-destkeypass pwd123
```

Note The inputs in the **keytool** command should match the inputs provided during UI certificate generation.

Note The resulting certificate (keystore.p12) created is in PKSC12 format.

Step 2 Upload the certificate into Trusted Root certificate store of Web browser. See help for respective Web browsers about how to add the certificate to the Trusted Root certificate store.

Generating TLS 3rd Party Certification Between WebUI Browser and NDB Server

Complete the following steps to generate TLS 3rd party certification between NDB Server and WebUI browser :

Procedure

Step 1 Generate Certificate Signing Request (CSR) using the **openssl req** command.

Example:

```
docker@docker-virtual-machine:~/Mallik/TLS_CA$  openssl req -newkey rsa:2048 -sha256 -keyout
 cert.key -keyform PEM -out cert.req -outform PEM
Generating a 2048 bit RSA private key
 ..............+++
.....................+++
writingnew private key to 'cert.key'
Enter PEM pass phrase: pwd123
Verifying - Enter PEM pass phrase: pwd123
-----
You are about to be asked to enter information that will be incorporated
 into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value, If you enter '.', the field
 will be left blank.
 -----
Country Name (2 letter code) [GB]:US
```

```
State or Province Name (full name) [Berkshire]:CA
Locality Name (eg, city) [Newbury]:SJ
Organization Name (eg, company) [My Company Ltd]:cisco
Organizational Unit Name (eg, section) []:insbu
Common Name (eg, your name or your server's hostname) []:N9K-117.cisco.com
 à this will be NDB application url)
Email Address []:myname@cisco.com
Please enter the following 'extra' attributes to be sent with your
certificate request
A challenge password []: pwd123
An optional company name []:pwd123
docker@docker-virtual-machine: # ls cert.key cert.req
```

Note You need to use the same information when exporting the CA provided certificate into browser. The CSR file, cert.req, is submitted to CA.

Step 2 To verify or view the CSR request, use the **openssl req** command.

Example:

```
[??]# openssl req -noout -text -in cert.req
```

Converting CA Provided Certificate into JKS Format

CA provides certificates in PEM format and extension of the certificate is .pem. You need to convert the PEM format certificate to PKCS12 format. Complete the following steps to convert PEM format certificate to PKCS12 format.

Note Ensure that you keep a copy of the original certificates before proceeding with the conversion.

Procedure

Step 1 Convert PEM format certificate into PKCS12 format using the **openssl pkcs12** command.

Example:

```
openssl pkcs12 -export -out sw1-xnc.p12 -in sw1-xnc.pem
```

Note Use the export password.

Note You need to use the same information when exporting the CA provided certificate into browser. The CSR file, cert.req, is submitted to CA.

Step 2 Convert the sw1-xnc.p12 to a password-protected tlsKeyStore file, use the **keytool** command.

Example:

```
[??]# keytool -importkeystore -srckeystore sw1-xnc.p12 -srcstoretype pkcs12 -destkeystore
tlsKeyStore -deststoretype jks
```

Note Use the **keytool -list -v -keystore tlsKeyStore** command to decode the keystore.

Step 3 Copy the converted certificate into NDB xnc/configuration directory and refer to this file in tomcat-server.xml file.

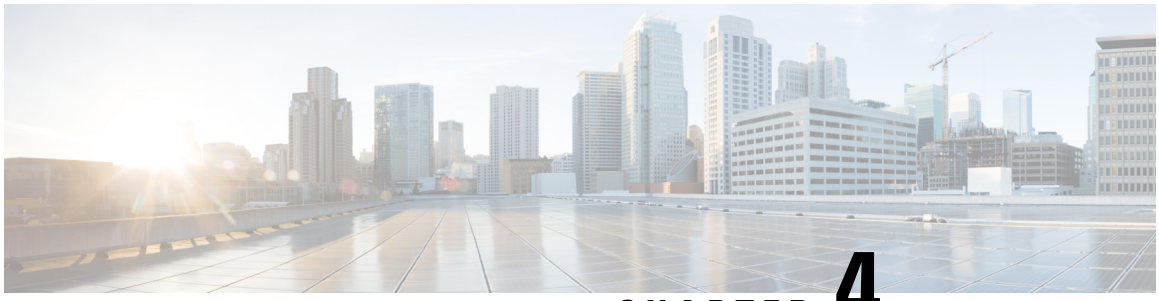
Step 4 Configure the tomcat server configuration flle (tomcat-server.xml) to the converted certificate.

Example:

```
keystoreFile="configuration/keystore"
keystorePass="ciscoxnc"
```

Step 5 Start the NDB application.

Step 6 Upload the CA certificate into Trusted Root certificate store of Web browser. See help for respective Web browsers about how to add the certificate to the Trusted Root certificate store.



CHAPTER 4

Logging in and Managing Cisco Nexus Data Broker

This chapter contains the following sections:

Configuring Cisco Nexus Data Broker

Configuring High Availability Clusters

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 50.

Procedure

Step 1 Open a command window on one of the instances in the cluster.

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

Step 3 Use any text editor to open the `config.ini` file.

Step 4 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 5 **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 6 Save the file and exit the editor.

Password Protecting the High Availability Clusters

Procedure

Step 1 Open a command window on one of the instances in the cluster.

Step 2 Navigate to the `xnc/configuration` directory.

Step 3 Use any text editor to open the `xncjgroups.xml` file.

Step 4 Locate the following text:

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

Step 5 Remove the comments from the AUTH line.

Example:

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

Step 6 (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, if you make the same change on all machines in the cluster.

Step 7 Save the file and exit the editor.

Editing the Configuration Files for Cisco Nexus Switches

Cisco Nexus Data Broker has the ability to periodically rediscover 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.

Procedure

	Command or Action	Purpose
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
of.switchLivenessTimeout	120.5	60.5	120.5
of.flowStatsPollInterval	240	10	240
of.portStatsPollInterval	240	5	240
of.descStatsPollInterval	240	60	240
of.barrierMessagePrioCount	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

	Command or Action	Purpose
		Note Predefined values are the values that Cisco includes in the `config.ini` file that is shipped with Cisco Nexus Data Broker. A 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 User Roles for Edge Ports

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

Procedure

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.

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.

Procedure

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:

Procedure

	Command or Action	Purpose

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" />`	

	Command or Action	Purpose
	<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.

Note You should always click **Save** after making any configuration changes.

- 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.

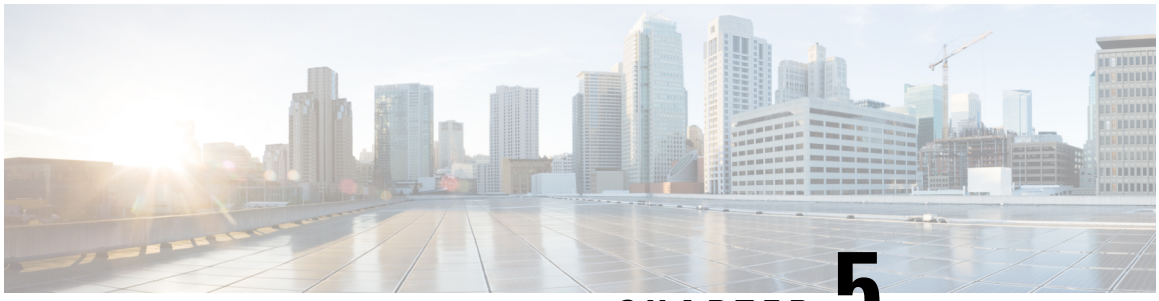
To view information about a filter, hover over the **Name** of the filter in the **Filters** tab.

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.

Procedure

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



CHAPTER 5

Viewing and Adding Devices

This chapter contains the following sections:

Viewing and Adding Devices

On the **Devices** screen, the following tabs are displayed:

- Nodes Learned
- Device Connections
- Device Groups
- SPAN Management
- Subnet Gateway Configuration

On the **Nodes Learned** tab, the following details are displayed for each node:

- The name of the node
- The ID of the node
- The hardware on the node
- The number of ports on the node

When you click the node name under the tab **Node Name**, the **Update Node Information** window is displayed. Update the following fields in the window:

- **Node ID**: Enter the node ID.
- **Node Name**: The name of the node.
- **Tier**: Select the tier of the node from the following options in the drop-down list: Unknown, Access, Distribution, and Core.
- **Operation Mode**: Choose how the traffic is handled based on the flows. This can be one of the following:

  Allow reactive forwarding—No default flows are programmed. How traffic that does not match a flow is treated depends upon the switch implementation.

Proactive forwarding only—The following default flows are programmed on the switch:

- Punt Link Layer Discovery Protocol (LLDP) packets.
- Drop all other traffic.

On the **Device Connections** tab, click **Add Device** to add a device, click **Remove Devices** to remove a device, or click **Rediscover Devices** to rediscover a device. When you click **Rediscover Devices** tab, the **Rediscover Device** window is displayed. Click **Rediscover Device** so that the device gets deleted and rediscovered again.

In each device window, click **View**, **Edit**, or **Delete** to add a device, edit an existing device, or delete a device. The following details are displayed for each device in each device window:

- The name of the device and its IP address
- The username on the device
- The type of the mode, for example, NX-API
- The uptime on the device, for example, date and time
- The hardware on the node

On the **Device Groups** tab, click **+ Group** to add a group of devices. In each group window, click **View**, **Edit**, or **Delete** to add a group of devices, edit an existing group of devices, or delete a group of devices respectively. The following details are displayed in each group window:

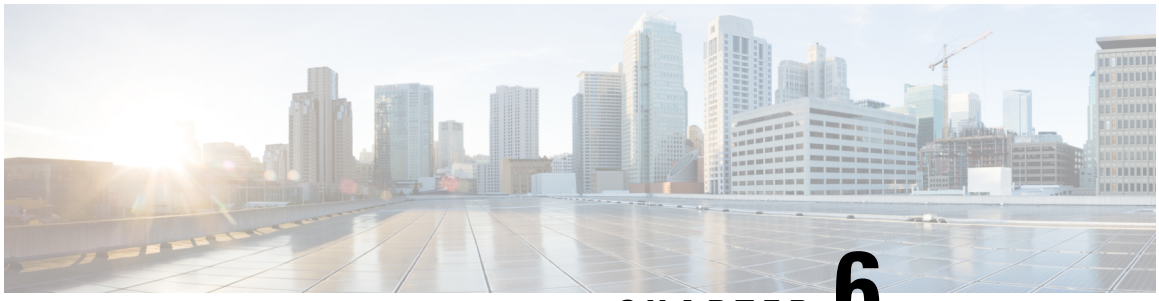
- The name of the node group, for example, Node Group Name One
- The names of the nodes in the group, for example, nx-tap-agg-sw1 and nx-tap-agg-sw2

On the **SPAN Management** tab, click **+ Add Device** to add an APIC device or the production switch to the network. Click **Remove Devices** to delete the devices or click **Rediscover Devices** to rediscover the devices. The production switch should be a Cisco Nexus 9000 Series switch or Cisco Nexus 3000 Series switch in NXOS mode. The feature NXAPI has to be enabled on these production switches.

The following columns are displayed on the **SPAN Management** tab to display the information about the devices:

- IP Address
- Username
- Type: The APIC device is listed as AC and the production switch will belated here is listed as PS.
- Active IP
- Secondary IP Address
- Tertiary IP Address
- Action

You must add an APIC controller before you can set up SPAN session and SPAN destination.



CHAPTER 6

Configuring Cisco Nexus 9000 Series Switches

This chapter contains the following sections:

Guidelines and Limitations

See the following guidelines and limitations for configuring Cisco Nexus 9000 Series switches through Cisco Nexus Data Broker.

- Cisco Nexus Data Broker supports NX-API protocol for Cisco Nexus 9000 series family of devices starting with Release 7.x.
- The NX-API device Edit option is not supported in the current release.
- The devices that are going to provisioned by Cisco Nexus Data Broker are assumed to have LLDP enabled and the LLDP feature should not be disabled during the device association with Cisco Nexus Data Broker. If the LLDP feature is disabled, there might be an inconsistency in Cisco Nexus Data Broker that cannot be fixed without device deletion and re-addition.
- Cisco Nexus Data Broker assumes that the device interfaces configured by the port definitions are L2 switch ports and these interfaces have device configurations as switchport trunk by default.
- Cisco Nexus 9000 series devices do not support VLAN ID for the Edge Port, SPAN and Edge port, and the TAP interfaces.
- If the devices that are added in the Cisco Nexus Data Broker are to be removed, the devices associated the port definitions and the connections should be removed first.
- For Cisco Nexus 9000 Series switches, upgrade the Cisco NX-OS software to Cisco NX-OS Release 7.x or above.
- You can now add a Cisco Nexus 9000 Series switch to the Cisco Nexus Data Broker that can be discovered through NX-API protocol. Once the connection is successful, all the line card information for chassis model 9500 is discovered.
- Cisco Nexus Data Broker uses the TAP aggregation feature and the NX-API support for JSON-RPC.

- Prior to deploying the Cisco Nexus 9000 Series switches for Tap/SPAN aggregation through Cisco Nexus Data Broker with NX-API mode, the following configurations should be completed:
  - Configure the ACL TCAM region size for IPV4 port ACLs or MAC port ACLs using the **hardware access-list tcam region {ifacl | mac-ifacl} 1024 double-wide** command on the switch.
  - Enable NX-API with **feature manager** CLI command on the switch.
  - Configure **switchport mode trunk** on all the inter-switch ports and the port-channels.
- Prior to deploying the Cisco Nexus 9000 Series switches for Tap/SPAN aggregation through Cisco Nexus Data Broker with OpenFlow mode, enter the command **hardware access-list tcam region openflow 512** at the prompt.
- Cisco Nexus data broker periodically rediscovers the switch inventory, the topology interconnection, and the status. This information is updated in the GUI depending on the status. The rediscovery interval can be configured and the default value for the rediscovery interval is every 10 seconds.

Configuring TCAM Hardware Sizing on Cisco Nexus 9000 Series Switches

The TCAM configuration is based on the filtering requirement. You may need to configure multiple TCAM entries based on your filtering requirement. Complete these steps to configure a TCAM:

Procedure

	Command or Action	Purpose
Step 1	Use the **hardware access-list tcam region <region> <tcam-size>** command to configure the following TCAM regions:	• IPV4 PACL [ifacl] size = 1024 • IPV6 PACL [ipv6-ifacl] size = 0 • MAC PACL [mac-ifacl] size = 512 • Egress IPV4 RACL [e-racl] size = 256 • Egress IPV6 RACL [e-ipv6-racl] size = 0 • Ingress System size = 256 • Egress System size = 256 • SPAN [span] size = 256 • Ingress COPP [copp] size = 256 See the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide* for the step-by-step TCAM hardware sizing configuration on Cisco Nexus 9000 Series Switches.

Enabling Cisco NX-API on Cisco Nexus 9000 Series Switches Using CLI

You can now manage multiple Cisco Nexus 9000 Series switches that are connected in a topology. Cisco Nexus Data Broker pugin can discover the switch interconnections using LLDP and update the topology services within Cisco Nexus Data Broker. The switch interconnections can be a physical link or a port-channel interface. The topology displays only the interconnections between Cisco Nexus 9000 Series switches that are added to the Cisco Nexus Data Broker device list. The topology interconnection is displayed in the GUI.

Complete the following steps for enabling Cisco NX-API on Cisco Nexus 9000 Series switches:

Procedure

	Command or Action	Purpose
Step 1	Enable the management interface.	Enable the management interface on the switch.
Step 2	switch# **conf t**	Enter the configuration mode.
Step 3	switch (config) # **feature nxapi**	Enable the NX-API feature.
Step 4	switch (config) # **nxapi http port** *80*	Configure the HTTP port.
Step 5	switch (config) # **nxapi https port** *443*	Configure the HTTPS port. For the step-by-step configuration information for enabling the NX-API feature on Cisco Nexus 9000 Series switches, see the *Cisco Nexus 9000 Series NX-OS Programmability Guide*.

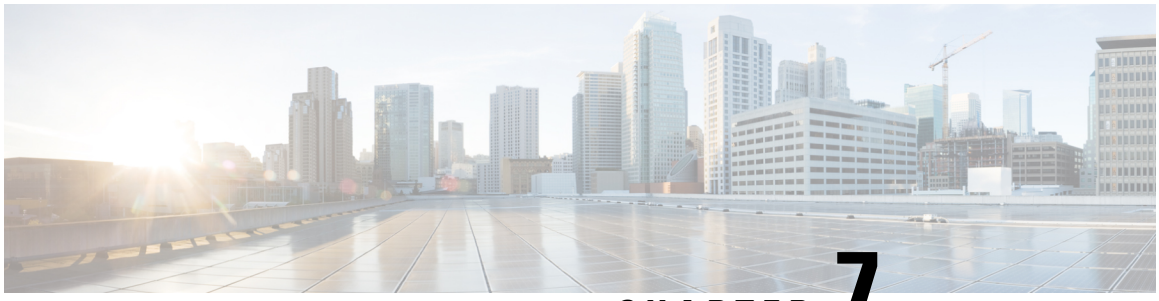
Enabling Switch Port Mode as Trunk on the Inter-switch Ports and Port Channels

Complete the following steps to enable the switch port mode on the inter-switch ports and port-channels:

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **config t**	Enables the configuration mode.
Step 2	switch(config)# interface {{**type** *slot*/*port*} | {*port-channel number*}}	Specifies an interface to configure.
Step 3	switch(config-if)# **switchport mode** {*access* | *trunk*}	Configures the switchport mode as access or trunk on the inter-switch ports and the port-channels.

	Command or Action	Purpose
Step 4	switch(config)# **exit**	Exits the configuration mode.



CHAPTER 7

Configuring the Nexus Data Broker

This chapter contains the following sections:

Viewing Topology

Click the **Topology** tab in the left frame to view the topology in the network.

Configuring Port Definition

When you click **Port Definition** tab in the GUI, the **Port Definition** screen is displayed. Select the switch from the drop-down list to configure the ports.

On the **Port Definition** screen, the following two tabs are displayed:

- Port Configuration
- SPAN Destination

Click the **Port Configuration** tab, the following tabs are displayed:

- Configure Multiple Ports
- Remove port Configuration
- Add Service Node
- Add Monitoring Device

When you click **Configure Multiple Ports** tab, the **Configure Multiple Ports** window is displayed. The following details are displayed on the screen: Number, Status, Port Name, Type, In Use, Port ID, and Action.

Note Beginning with Cisco Nexus Data Broker, Release 3.1, the interface description is updated from the Cisco Nexus Data Broker GUI to the switch and the interface description is also available from the switch into the Cisco Nexus Data Broker GUI. When using in Openflow mode, the NX-API auxiliary connection is required for this functionality to work.

Note On the Port Configuration tab, the port name and the interface are displayed as hyperlinks. When you click the port name, you can view the running configuration for that interface on the tab.

If you want to remove any ports, select the port and click **Remove port Configuration** tab.

Click **Add Service Node** to add a service node.

Click **Add Monitoring Device** to add a monitoring device.

On the **Port Configuration** screen, the following port details are displayed for the selected node:

- Serial Number
- Status
- Port name
- Type
- In Use
- Port ID
- Action—When you click **Configure**, the **Configure Ports** window is displayed.

On the **SPAN Destination** tab, the following details are displayed:

- SPAN Destination Name
- SPAN Destinations

- Node Connector
- Monitor Port Type
- Description

Configuring Ports

Procedure

Step 1 Select the switch for which you want to configure the port details on the **Port Configuration** screen.

Step 2 Click **Configure** under **Action**.

The **Configure Ports** window is displayed.

Step 3 In the **Configure Ports** window, configure the port type from the **Select a port type** drop-down list by selecting one of the following options:

- **Add Monitoring Device**
- **Edge Port-SPAN**
- **Edge Port-TAP**
- **Production Port**

Monitoring Device—Creates a monitoring device for capturing traffic and configures the corresponding delivery port.

Edge Port-SPAN—Creates an edge port for incoming traffic connected to an upstream switch that is configured as a SPAN destination.

Edge Port-TAP—Creates an edge port for incoming traffic connected to a physical TAP port.

Production Port—Creates a production port for the ingress and egress traffic.

Note To receive the traffic from the production network, the production ingress port is configured. After entering the service nodes (multiple security tools), the traffic exits the data center through the production egress port.

Note Starting with Cisco Nexus Data Broker, Release 3.2, when Edge-SPAN, Edge-TAP, monitoring device, or production port is defined in NX-API mode of configuration, the CLI command, **spanning-tree bpdufilter enable** is automatically configured in the interface mode on the ports to filter the BPDU packets. This configuration is applicable for all Cisco Nexus 3000 and 9000 Series switches. The sample configuration is displayed in the example:

```
switch#
show run interface eth1/1
interface ethernet1/1
switchport mode trunk
mode tap-aggregation
spanning-tree bpdufilter enable
```

Note Production port has be enabled for Q-in-Q in Cisco Nexus Data Broker and a unique VLAN should be assigned for each production port. This VLAN should not overlap with any production VLAN numbers.

Note The **spanning-tree bpdufilter enable** CLI command should be configured by the user on all the inter-switch ports for all Cisco Nexus series switches and Cisco Nexus Data Broker does not configure this command.

Note Once an interface is configured with Q-in-Q, do not configure multiple VLAN filters for the Q-in-Q configured interface.

When you select the port type, the title of the window changes to **Manage Configure Ports**.

Step 4 (Optional) In the **Port Description** field, enter the port description.

Beginning with Cisco Nexus Data Broker, Release 3.1, the interface description is updated from the Cisco Nexus Data Broker GUI to the switch and the interface description is also available from the switch into the Cisco Nexus Data Broker GUI. When using in Openflow mode, the NX-API auxiliary connection is required for this functionality to work.

Step 5 Required: Enter VLAN ID for the port.

The port is configured as dot1q to preserve any production VLAN information. The VLAN ID is used to identify the port that the traffic is coming from.

Step 6 (Optional) If APIC is available, you can select the ACI side port and designate it as the SPAN destination port.

Step 7 In the **Enable Packet Truncation** field, enter the packet length.

Step 8 A check box is added for **Block Tx** and it is applicable only for Edge-SPAN where you can block the traffic that is being transmitted out of Edge-SPAN interface.

Step 9 Click **Submit** to save the settings or click **Clear** to clear the details.

Once you configure a port, you can click **Edit** under **Action** on the **Port Configuration** screen to edit the port details. You can click **Remove** under **Action** on the **Port Configuration** screen to clear the port details.

Editing In Use Ports

Starting with NDB Release 3.4, you can edit the select fields under Port configuration(Edge-Span, Edge-Tap or Production) while in use. Ports can be edited in all the modes of connection. The following table lists the fields that you can edit for port in use.:

Section	Field	Editable
Port Configuration	Port Description	Yes
	Block Tx	Yes
	Port Type	No
	VLAN Packet Truncation	No
	Drop ICMPv6 Neighbour Solicitation	Yes
	Enable Timestamp Taggin	Yes

Enabling or Disabling Ports

Starting with Cisco NDB Release 3.4, you can now enable or disable an interface using the NDB GUI. This feature is currently available for NX-API and NX-AUX based switches. A switch based on OpenFlow mode does not support this feature.

Procedure

Step 1 Select the switch for which you want to configure the port details on the **Port Configuration** screen.

Step 2 Click **Enable/Disable** to enable or disable the selected port.

Note You can enable or disable only one interface at a time.

Adding SPAN Destination

When you configure a port as an edge SPAN port and the port is connected to the API side, you can select the pod, node, and port from the ACI side and set the port as SPAN destination.

Note You can add SPAN destination only after APIC has been successfully added to the network.

Procedure

Step 1 Select the switch for which you want to configure the port details on the **Port Configuration** screen.

Step 2 Click **Configure** under **Action**.

The **Configure Ports** window is displayed.

Step 3 In the **Configure Ports** window, configure the port type from the **Select a port type** drop-down list by selecting one of the following options:

- **Add Monitoring Device**
- **Edge Port-SPAN**
- **Edge Port-TAP**
- **Production Port**

Monitoring Device—Creates a monitoring device for capturing traffic and configures the corresponding delivery port.

Edge Port-SPAN—Creates an edge port for incoming traffic connected to an upstream switch that is configured as a SPAN destination.

Edge Port-TAP—Creates an edge port for incoming traffic connected to a physical TAP port.

Production Port—Creates a production port for the ingress and egress traffic.

When you select the port type, the title of the window changes to **Manage Configure Ports**.

Step 4 In the SPAN DESTINATION pane, select the pod from the **Pod** drop-down list.

Step 5 Select the ACI leaf from the **Leaf** drop-down list.

Step 6 Select the port from the ACI side from the **Port** drop-down list and set the interface as SPAN destination.

Step 7 Click **Submit** to save the settings.

The port is now configured as SPAN destination part and it is displayed on the Port Definition screen.

Configuring Multiple Ports

You can configure multiple ports for a node.

Procedure

Step 1 Click **Configure Multiple Ports** on the **Port Configuration** screen. The **Configure Multiple Ports** window is displayed.

Step 2 Use **CTRL/SHIFT** to select multiple ports in the **Select Ports** field.

Step 3 Select port type from the drop-down list in the **Select Port Type** field.

Step 4 Click **Submit** to save the settings.

Configuring Port Groups

You can create a port group and add the ports to the connection.

Note Starting with Cisco Nexus Data Broker, Release 3.2, you can create port groups for different source ports. The port groups can be a combination of the edge-span and the edge-tap ports across different switches. You can select ports, define port groups, provide a name to the port group, select the port group in a connection screen (only one port group per connection), and use the ports defined in the port group as source ports for creating a connection. Selecting individual ports is disabled when using a port group.

You cannot edit the port group even if it is part of a connection. The connection is automatically updated with the new port group. Deleting a port group is not allowed when the port group is in use.

Complete the following steps to configure port groups:

Before you begin

Procedure

Step 1 Select the switch for which you want to configure the port details on the Port Configuration screen.

Step 2 Click **Port Groups** tab in the left frame.

Step 3 Click **+ Add Group** to create a port group.

Step 4 In the **Create Port Group** window, enter the group name in the **Group Name** field.

Step 5 In the **Select Node** field, select a node, for example, N9K-116.

Step 6 In the **Select Port** field, select a port, for example, Ethernet1/1 (Ethernet1/1).

You can add only edge-span and edge-tap ports and you cannot add production ports to the port groups.

Step 7 Click **+ Add To Group** to add the port to the group.

You can add multiple ports to the group.

Step 8 Click **Apply**.

The port group is displayed on the **Port Groups** screen with the following information for the group, for example, **Name**, **Connection Name**, **Ports** and **Action**.

Editing In Use Port Groups

Starting with NDB 3.4 release, you can edit the port groups that are currently in use in a connection. This feature is supported on the switches running in NX-API, OpenFlow, or NX-AUX mode.

Procedure

Step 1 Select the switch for which you want to configure the port details on the **Port Group** pane.

Step 2 Click **Edit** on the listed table row.

Editable Attributes for In Use Port Groups

The following table lists the fields that you can edit for a Port Group that is currently in use:

Section	Field	Editable
Port Group	Port Description	Yes
	Port	Yes
	Port Name	Yes (If the port is not part of an active connection)
	Port Group	Yes (If the port group is not part of an active connection)

Adding a Monitoring Device

To add a new monitoring device, complete these steps:

Procedure

Step 1 Navigate to the **Monitoring Device** tab under **Configuration**.

Step 2 Click **Add Monitoring Device**.

Step 3 In the **Monitoring Device** window, complete the following fields:

Name	Description
Monitoring Device Name	Add the service node name. **Note** The valid characters for the monitoring devices are the alphanumeric characters and the special characters: period ("."), underscore ("_"), and hyphen ("-").
Select Switch Node	Select the switch node.
Select Port	Select the port.
Icons	Select a Monitoring Device Icon.
Block Rx	Block any traffic from being received from the monitoring tools. This option is selected by default. You can turn this option off by unchecking the box.
Enable Timestamp Tagging	Time stamp tagging is supported on Cisco Nexus 3500, 9200 and 93XXX-EX Series switches. Cisco Nexus 3500 Series switches require NX-OS Release 6.0(2)A8(1) or later version.

Step 4 Click **Submit** to create the monitoring device.

Editing In Use Monitoring Device

Starting with Cisco NDB, Release 3.4, you can edit a monitoring device configuration using the NDB GUI. Support to edit description of a Monitoring device is available for NX-API, OpenFlow, and NX-AUX based switches. For the OpenFlow devices, the updated descriptions are synchronized to NDB User Interface (UI) only. For NX-API and NX-AUX devices, the updates are synchronized to NDB UI and the switch interface.

The following table lists the fields that you can configure for Monitoring Devices:

Section	Field	Editable
Monitor Devices	Monitor Devices Name	Yes (If the monitoring device is not in use)
	Port Description	Yes
	Block Rx	Yes
	Icons	Yes
	Enable Timestamp Tagging	Yes

Adding a Service Node

Procedure

Step 1 Navigate to the **Service Nodes** tab under **Configuration** and click **+ Service Node**.

Step 2 In the **Add Service Node** window, enter the name of the service node.

Step 3 Select the ingress port for the service node from the **Service Node Ingress Port** drop-down list.

Step 4 Select the egress port for the service node from the **Service Node Egress Port** drop-down list.

Step 5 Enable health check on a service node by selecting the **Service Node Health Check** option.

Beginning with Cisco Nexus Data Broker, Release 3.2, you can configure the wait interval in the **config.ini** file before the health check is up. The **ServiceNodeHealthCheckWaitInterval** is the variable in the **config.ini** file to set the wait interval. If you do not specify a value or if the value is 0 for the wait interval in the **config.ini** file, the default value of 5 Seconds is used. The wait interval is not applicable if the port is in shutdown state.

This option works only in the OpenFlow mode. The controller or the NDB injects a packet in the service node ingress port and the packet is received at the egress port. The packets are checked at the interval of every 5 seconds. If five packets are not received in 5 seconds, the health of the service node is considered as down.

For the service node, a new field is displayed in the details: Service Node Status. This field displays the status of the service node.

Step 6 Select a service node icon from the available options.

Step 7 Click **Save**.

Editable Fields for an Active Service Node

Starting with Cisco NDB, Release 3.4, you can now edit and configure Service Node fields using the NDB GUI. For the OpenFlow devices, the updated descriptions are synchronized to NDB User Interface (UI) only. For NX-API and NX-AUX devices, the updates are synchronized to NDB UI and the switch interface.

The following table lists the fields that you can configure for an active Service Node:

Section	Field	Editable
Service Node	Description	Yes
	Icon	Yes
	Service Node Health Check	Yes
	Service Node Name	Yes (If the service node is not in use)
	Service Node Ingress Port	No
	Service Node Egress Port	No
	Ingress port Description	Yes
	Egress port Description	Yes

User Defined Filter

Beginning with Cisco Nexus Data Broker, Release 3.3, you can define a User Defined Filter (UDF) and use it while creating a filter for traffic management.

Note UDF is supported on Cisco Nexus 9000 Series switches in NXAPI mode with NXOS version higher than Release 7.0(3)I5(2).

Note You can configure a maximum of four UDF for a Cisco Nexus 9000 Series switch. For 9200 and 9300-EX series switches, you can configure a maximum of two UDFs.

To use UDF to manage traffic, you need to:

- Define a UDF, see Defining a UDF.
- Create a filter using the UDF, see Adding Filters.
- Apply the filter (configured with UDF) to a connection to manage traffic, see Adding Connections.

Defining a UDF

Complete the following steps to define a UDF:

Procedure

	Command or Action	Purpose
Step 1	Log into NDB application.	
Step 2	Navigate to **Configuration** tab, click **UDF Definition** to define a user defined filter. The **UDF Definition** window is displayed.	
Step 3	In the **UDF Definition** window, complete the following fields:	**Name** field: The name of the user defined filter. **Keyword**: Header or packet-start **Offset** field: Number of characters to offset while using matching criteria. **Devices**: Cisco Nexus 9000 Series switch name.
Step 4	Click **Add UDF**. The newly added UDF appears in the **UDF Definition** window.	**Note** Any change in a UDF definition requires device reboot. **Note** By default, NDB generates a UDF named *udfInnerVlan*, used to match the inner VLAN in the ISL ports.

Adding Filters

Beginning with Cisco Nexus Data Broker, Release 3.3, the Default-Match-All filter includes the following protocols packet filtering:

- IPv4
- IPv6
- ARP
- MPLS Unicast
- MPLS Multicast
- MAC

Before you begin

Note The hardware command that is a pre-requisite for the IPv6 feature is **hardware access-list tcam region ipv6-ifacl 512 double-wide**.

Procedure

Step 1 On the **Filters** tab, click **Add Filter** to add a filter. The **Add Filter** window is displayed.

Step 2 In the **Filter Description** section of the **Add Filter** window, complete the following fields:

Name	Description
Name field	The name of the filter. **Note** The name cannot be changed once you have saved it.
Bidirectional check box	Check this box if you want the filter to capture traffic information from a source IP, source port, or source MAC address to a destination IP, destination port, or destination MAC address, and from a destination IP, destination port, or destination MAC to a source IP, source port, or source MAC address.

Step 3 In the **Layer 2** section of the **Add Filter** window, complete the following fields:

Ethernet Type field	Required. The Ethernet type of the Layer 2 traffic. The default value displayed is IPv4, or you can choose one of the following: • IPv6 • ARP • LLDP • Predefined EtherTypes • All EtherTypes • Enter Ethernet Type—If you choose Enter Ethernet Type as the type, enter the Ethernet type in hexadecimal format. If you choose Predefined EtherTypes, all predefined Ethernet types contained in the config.in file are associated with the rule, and you should not configure any other parameters. **Note** You can now configure more than 1 user-defined Ethernet type per filter. You can apply an arbitrary number of Ethernet types that are separated by "," so that a single filter can be setup for the different traffic types.
VLAN Identification Number field	The VLAN ID for the Layer 2 traffic. You can enter a single VLAN ID, a range of VLAN ID values, or comma-separated VLAN ID values and VLAN ID ranges, for example, 1-4,6,8,9-12. **Note** For NX-API, a VLAN ID with Layer 3 address is not supported. If a VLAN ID with Layer 3 address is configured, it results in the inconsistent flows. You have to troubleshoot and fix the flows.
VLAN Priority field	The VLAN priority for the Layer 2 traffic.
Source MAC Address field	The source MAC address of the Layer 2 traffic.
Destination MAC Address field	The destination MAC address of the Layer 2 traffic.

Step 4 In the **Layer 3** section of the **Add Filter** window, update the following fields:

Name	Description
Source IP Address field	The source IP address of the Layer 3 traffic. This can be one of the following: • The host IP address, for example, 10.10.10.10 • Discontiguous source IP address, for example, 10.10.10.10, 10.10.10.11, 10.10.10.12 • An IPv4 address range, for example, 10.10.10.10-10.10.10.15 • An IPv4 subnet, for example, 10.1.1.0/24 • The host IP address in IPv6 format, for example, 2001::0 • Combination of range and simple IP addresses, for example, 4.4.4.1,4.4.4.2-4.4.4.4,4.4.4.5. **Note** • When a switch is used in NX-API mode, you can now select an IPv6 filter and setup a connection. You can enter a single IPv6 address, comma separated multiple IPv6 addresses, an IPv6 address range, and/or IPv6 subnet in the **Source IP Address** field. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 4 source or destination ports. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 2 VLAN identifiers. **Note** When using IPv6 address in the filter, the **Ethernet Type** should be set to IPv6.

Name	Description
Destination IP Address field	The destination IP address of the Layer 3 traffic. This can be one of the following: • The host IP address, for example, 10.10.10.11 • An IPv4 address range, for example, 10.10.10.11-10.10.10.18 • An IPv4 subnet, for example, 10.1.1.0/24 • The host IP address in IPv6 format, for example, 2001::4 • The subnet, for example, 10.0.0.0/25 **Note** • When a switch is used in NX-API mode, you can now select a IPv6 filter and setup a connection. You can enter a single IPv6 address only in the **Destination IP Address** field. The comma separated multiple IPv6 addresses, an IPv6 address range, and/or IPv6 subnets are not supported. The hardware command that is a pre-requisite is for using the IPv6 feature is **hardware access-list tcam region ipv6-ifacl 512**. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 4 source or destination ports. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 2 VLAN identifiers.
Protocol drop-down list	Choose the Internet protocol of the Layer 3 traffic. This can be one of the following: If you choose Enter Protocol as the type, enter the protocol number in decimal format. • ICMP • TCP • UDP • Enter Protocol

Name	Description
UDF drop-down list	User Defined Filter. • UDF value: Value to be matched. • UDF Mask: Mask value in packet to match. **Note** UDF option is enabled only for IPv4.
ToS Bits field	The Type of Service (ToS) bits in the IP header of the Layer 3 traffic. Only the Differentiated Services Code Point (DSCP) values are used.
Advanced Filter field	Advanced filter, combination of Ethernet type and attributes to manage traffic.

Step 5 In the **Layer 4** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
Source Port drop-down list	Choose the source port of the Layer 4 traffic. This can be one of the following: • FTP (Data) • FTP (Control) • SSH • TELNET • HTTP • HTTPS • Enter Source Port **Note** Beginning with Cisco Nexus Data Broker Release 3.2 , you can enter comma separated single port numbers and a range of the source port numbers in the **Enter Source Port** field. **Note** • If you configure a range of Layer 4 source ports, you cannot configure ranges of Layer 3 IP source or destination addresses. • If you configure a range of Layer 4 source ports, you cannot configure ranges of Layer 2 VLAN identifiers

Name	Description
Destination Port drop-down list	Choose the destination port of the Layer 4 traffic. This can be one of the following: • FTP (Data) • FTP (Control) • SSH • TELNET • HTTP • HTTPS • Enter Destination Port **Note** Beginning with Cisco Nexus Data Broker Release 3.2 , you can enter comma separated single port numbers and a range of the source port numbers in the **Enter Destination Port** field. **Note** • If you configure a range of Layer 4 destination ports, you cannot configure ranges of Layer 3 IP source or destination addresses. • If you configure a range of Layer 4 destination ports, you cannot configure ranges of Layer 2 VLAN identifiers

Step 6 In the **Layer 7** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
HTTP Method field	You can configure matching on the HTTP methods and redirect the traffic based on that method. Select one or more methods to match within a single filter. This option is available only when the destination port is HTTP or HTTPS. • Connect • Delete • Get • Head • Post • Put • Trace **Note** Layer 7 match is supported only with the NX-API mode only and it is not supported in OpenFlow. **Note** The TCP option length is enabled when you select any one of the methods from Layer 7 traffic.
TCP Option Length field	You can extend the filter configuration to specify the TCP option length in the text box. The default value on the text box is 0. All methods within the filter have the same option length. Enter the TCP option length in a decimal format. **Note** The value on the text box should be in the multiples of 4 and it can range from 0-40.

Step 7 Click **Add Filter**.

Advanced Filter support

Starting with Cisco Nexus Data Broker, Release 3.3, advanced filtering option is available to manage the traffic. Advanced filtering provides multiple options to filter (permit or deny) the traffic based on Ethernet type and attributes such as Acknowledgment, FIN, Fragments , PSH, RST, SYN, DSCP, Precedence, TTL, packet-length, and NVE. Advanced filtering is available for the following Ethernet types and options:

Table 3: Advanced Filtering Support

Data Type	Supported Options
IPv4	DSCP, Fragment, Precendence, and TTL
IPv4 with TCP	Acknowledgment, DSCP, Fragment, FIN, Precedence, PSH, RST, SYN, and TTL
IPv4 with UDP	DSCP, Fragment, Precendence, and TTL
IPv6	DSCP and Fragment
IPv6 with TCP	Acknowledgment, DSCP, Fragment, FIN, PSH, RST, and SYN
IPv6 with UDP	DSCP and Fragment

Important Advanced Filtering is available only for NX-API on Cisco Nexus 9000 platform.

Important The value of Time to Live (TTL) attribute ranges from 0 to 255.

- For Nexus 9200 devices, the maximum value of TTL that can be set is 3.
- For rest of the Nexus 9000 series devices, the maximum TTL value can be 3 for NX-OS version 7.0(3)I6(1) and above. For NXOS versions 7.0(3)I4(1) and below, you can configure any value within the range.

While configuring advanced filtering support, you cannot:

- Configure DSCP and Precedence together in advance filtering.
- Configure fragments and ACK or SYN or FIN or PSH or RST together in advance filtering.
- Configure fragments and port numbers with UDP and IPv4 or IPv6 Combination
- Configure Precedence and HTTP Methods with IPv4 and TCP Combination.

Adding Connections

Before you begin

- Add a filter to be assigned to the connection.
- Configure a monitoring device (optional).
- Configure an edge port or multiple edge ports (optional).

Procedure

Step 1 On the **Connections** tab, click **+ Connection**. The **Add Connections** window is displayed.

Step 2 In the **Add Connections** window, you can add the **Connection Name** and the **Priority** of the connection in the **Connection Details** area:

Field	Description
Connection Name	The name of the connection.
Description	Enter the description when creating a new connection.
Priority	The priority that you want to set for the connection. Connection by default has priority of 100. It can be changed in the range of <1-10000>.

Step 3 In the **Allow Matching Traffic** area, modify the following fields:

Field	Description
Allow Filters drop-down list	Choose a filter to use to allow matching traffic. **Note** You cannot choose the same filter for Allow Filters that you choose for Drop Filters.
Set VLAN field	The VLAN ID that you want to set for the connection. **Note** This functionality is available only in Openflow mode.
Strip VLAN at delivery port check box	Check this box to strip the VLAN tag from the packet before it reaches the delivery port. **Note** The Strip VLAN at delivery port action is only valid for connections with a single edge port and one or more delivery devices for a single, separate node. This functionality is available only in Openflow mode.
Destination Devices list	The monitoring devices that you want to associate with the filter. You can choose one or more devices by checking the boxes next to their names.
Drop Filters drop-down list	

Step 4 In the **Drop Matching Traffic** area, complete the following fields:

Field	Description
Drop Filters	Choose the default filter **Default-Match-all** or use other filters to drop the matching traffic. **Note** You cannot choose the same filter for Drop Filters that you choose for Allow Filters.

Step 5 In the **Source Ports (Optional)** area, complete the following fields:

Field	Description
Select Source Node drop-down list	Choose the source node that you want to assign. **Note** If you do not choose a source node, the any-to-multipoint loop-free forwarding path option is used, and traffic from all nondelivery ports is evaluated against the filter. **Note** When setting up a new redirection, you can see the number of flows that are part of each input port. When you click the port number, the flow details are displayed.
Select Source Port drop-down list	Choose the port on the source node that you want to assign. **Note** Only edge ports can be used as source ports. **Note** If you do not select a source port while adding a new connection, the following warning message is displayed: No source port is selected. Connection will be setup from all configured Edge-SPAN and Edge-TAP ports. Click OK to continue with the connection installation/creation. It ensures that you do not install any to multi point connection and disrupt any existing traffic. Click Cancel to take you to the connection setup page.
In the **Source Ports (Optional)** area, select **Port Group** instead of **Source Ports**.	Select port group.
Select a port group from **Select Port Group** drop-down list. If you do not have any port groups configured, click **+ Port Group** to add a port group.	Select a port group.

Note Similar to the number of Edge-Tap or SPAN ports are displayed on top of each switch in the topology, the number of forwarding rules that a particular monitoring tool is part of are displayed when you hover the mouse over a switch. A popup table displays the rule (connection) names within which the monitoring tool is being used.

Note In Cisco Nexus Data Broker, Release 3.2.0, you can also select a port group in which case the individual ports cannot be selected.

Step 6 Do one of the following:

- Click **Save Connection** to save the connection, but not to install it until later.
- Click **Install Connection** to save the connection and install it at the same time.
- Click **Close** to exit the connection without saving it.

The following fields are displayed on the **Connection Setup** screen:

- Name
- Allow Filters
- Drop Filters
- Source Ports
- Devices
- Priority
- Last Modified By
- Description

The following fields are displayed In the Connections tab: **Status**, **Name**, **Allow Filters**, **Drop Filters**, **Source Ports**/**Port Group**, **Devices**, **Priority**, **Last modified by**, **Description**, and **Action**.

Note Beginning with Cisco Nexus Data Broker, Release 3.2, if you have added two or more interfaces (source ports) using the Connections tab, two interfaces (source ports) are displayed by default. If you have more than two interfaces (source ports) in the **Connections** tab, you can expand or collapse the source ports by using **more...** or **less...** options that are provided in the GUI.

Click **i Search Connections** tab in the Connections screen to search for the connections using the keywords, **Success**, **Installing**, **Creating**, **Partial**, and **Failed**.

Connection with AutoPriority

Beginning with Cisco Nexus Data Broker, Release 3.3, you can now add a new connection with AutoPriority. This functionality provides the flexibility to group multiple destination devices and filters in a connection. The priority of a connection with Auto-Priority is set to the value configured in **config.ini** file. You can configure the *connection.autopriority.priorityValue* attribute in the **config.ini** file with a priority value to be

used for all the new connections with auto-priority. The connection information lists the allowed filters along with the destination devices.

Restrictions and Usage Guidelines

Follow these restrictions and usage guidelines for creating a connection with auto-priority:

- ACL Overlapping is not supported for the filters of the same protocol type (different IP address and Ports) assigned to different destination devices, because only the filters are prioritized.
- To add a new connection with AutoPriority across devices (with multiple hops), the QinQ VLAN configuration is required.
- You can configure only one connection with Auto-Priority mode for each source port/port group.
- Connection with AutoPriority is a BETA release.

Adding a New Connection With Auto-Priority

To add a new connection with Auto-Priority, complete these steps:

Before you begin

Ensure that you have configured the monitoring device, destination device, and filters before adding a new connection.

Procedure

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td>Step 1</td><td>Log into the NDB application.</td><td></td></tr>
<tr><td>Step 2</td><td>Navigate to Configuration -> Connection, and click New Connection with AutoPriority (Beta) to add a new connection. The New Connection with AutoPriority (Beta) window is displayed.</td><td></td></tr>
<tr><td>Step 3</td><td>In the New Connection with AutoPriority (Beta) window, complete the following fields:</td><td>
<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Connection Name field</td><td>The name of the connection.</td></tr>
<tr><td>Description field</td><td>Short description of the connection.</td></tr>
</table>
</td></tr>
</table>

	Command or Action	Purpose

Name	Description
Destination Device drop-down list	The name of the destination device. Select a destination device from the Destination Device drop-down list and select corresponding filter from the Allow Filter drop-down list. You can add multiple destination devices with filters for a connection with AutoPriority mode.
Allow Filters list	Filter to apply to the destination device.
Drop Filter drop-down list	The name of the drop filter to apply to the connection.
Set VLAN field	VLAN ID range to override the incoming tagged VLAN traffic.
(Optional) **Source Ports** Section	Source port or port range for managing the traffic
Select Source Node drop-down list	Source Node Id.
Select Source port drop-down list	Source Node port number.

Adding Redirections

Note The redirection setup feature is supported on Cisco Nexus 3000 Series and Cisco Nexus 9300 switches with Release 7.x.

Cisco Nexus Data Broker lets you configure redirection policies that match specific traffic, redirecting it through multiple security tools before it enters or exits your data center using redirection.

Before you begin

- Add a filter to be assigned to the redirection.
- Configure a monitoring device (optional).
- Configure an edge port or multiple edge ports (optional).
- The production ingress port, the production egress port, and the service node should be on the same redirection switch.

Procedure

Step 1 On the **Redirections** tab, click **+ Redirection**. The **Add Redirection** window is displayed.

Step 2 In the **Add Redirection** window, you can add the **Redirection Name** and the **Priority** of the redirection in the **Redirection Details** area:

Field	Description
Redirection Name	The name of the redirection. **Note** The name of the redirection cannot be changed once you have saved it.
Description	Enter the description when creating a new redirection.
Set Auto Priority checkbox	Check this option to enable the auto-priority for redirection, The priority of the redirection is set based on the existing redirections that are installed on the selected ingress ports. If auto-priority is enabled, redirection has a default priority of 10000. Next redirection with auto-priority enabled will have the priority value as the last priority minus 1. Without the auto-priority feature, the default value is 100. It can be changed in the range of <2-10000>. Priority value 1 is reserved for the backup bypass flows. **Note** The priority of the redirection should not be configured as 1. Also, if the last priority is configured as 2, you cannot clone the redirection with auto-priority enabled. You have to manually clone the redirection.
Priority	The priority that you want to set for the redirection. The valid range of the values is 0–10000. The default is 100.
Automatic Fail-safe checkbox	Check this option to enable the fail-safe feature of redirection. When you enable this feature, the direct flow from the production ingress port and the egress port is created that matches all ethertype traffic of low priority.

Step 3 In the **Matching Traffic** area, modify the following fields:

Field	Description
Filters drop-down list	Choose a filter to use to allow matching traffic. **Note** You cannot choose the same redirection for the filter.

Step 4 In the **Redirection Switch** area, modify the following fields:

Field	Description
Select Redirection Switch drop-down list	Select the redirection switch that you want to assign.

Note You can have only one ingress port and one egress port per one redirection switch.

Step 5 In the **Service Nodes (OPTIONAL)** area, complete the following fields:

Field	Description
Select Service Node drop-down list	Select the redirection service node that you want to assign and click **Add Service Node**.

Note If you want to add multiple service nodes, you should add them in an order in which you want the packets to travel.

Starting with Cisco Nexus Data Broker, Release 3.2.0, the order of the service nodes is maintained. For example, if you have added the service nodes s1, s2, and s3 to redirection in an order. The service nodes become operationally down and therefore, they get removed from the redirection. Once the nodes become operationally up, they are added to the redirection in the same order.

Step 6 Select the **Reverse ServiceNode Direction** option to enable reverse direction on the service node.

When you enable this option and click **Submit**, the ingress and egress ports of the service node are swapped and reverse redirection is enabled on the service node. The option is also displayed as enabled in the **Redirections** tab.

Step 7 In the **Production Ports** area, complete the following fields:

Field	Description
Select Production Ingress Port drop-down list	Select the production ingress port that you want to assign. **Note** You can select only one ingress port. Multiple ingress ports are not allowed. You cannot use the same ports as the ingress and the egress ports. **Note** When setting up a new redirection, you can see the number of flows that are part of each input port. When you click the port number, the flow details are displayed.

Field	Description
Select Production Egress Port drop-down list	Select the production egress port that you want to assign.

Step 8 In the **Delievery Devices to copy traffic (OPTIONAL)** area, complete the following fields:

Field	Description
Select Device drop-down list	Select a device, for example, a switch from the drop-down list, that you want to assign and click **Add Device**. **Note** You can select multiple delivery devices for the redirection.
Select Monitor Traffic drop-down list	When creating inline redirection with copy, the monitoring port receives one flow from the production ingress port and another from the egress port of service node. Starting with Cisco Nexus Data broker Release 3.2, a filtering mechanism is added in the GUI to filter out the traffic. Use the drop down list to select the traffic to copy device in redirection. The following optios are displayed in the drop-down list: • Production Ingress-- Flow from the production ingress port • Production Egress-- Flow from the egress port of the service node • Both-- Flow from both the ports (the ingress and the egress ports)

Step 9 Do one of the following:

- Click **Save Redirection** to save the redirection, but not to install it until later.
- Click **Install Redirection** to save the redirection and install it at the same time.
- Click **Close** to exit the redirection without saving it.

Step 10 When you click **Install Redirection** to save the redirection and install it at the same time, the redirection path on the redirection switch is displayed on the production ingress ports, service nodes, and the production egress ports.

Step 11 Click **Flow Statistics** to view the flow statistics for the redirection switch.

The following fields provide information on the flow statistics:

- In Port field—The Input port(s) from which the traffic is matched. An asterisk ("*") indicates any input port.

- DL Drc field—The source MAC address to be matched for the incoming traffic. An asterisk ("*") indicates any source MAC address.
- DL Dst field—The destination MAC address to be matched for the incoming traffic. An asterisk ("*") indicates any destination MAC address.
- DL Type field—The Ethertype to be matched for the incoming traffic. For example, "IPv4" or "IPv6" is used for all IP traffic types.
- DL VLAN field—The VLAN ID to be matched for the incoming traffic. An asterisk ("*") indicates any VLAN ID.
- VLAN PCP field—The VLAN priority to be matched for the incoming traffic. An asterisk ("*") is almost always displayed in this field.
- NW Src field—The IPv4 or IPv6 source address for the incoming traffic. An asterisk ("*") indicates any source address based on IPv4 or IPv6 Ethertypes.
- NW Dst field—The IPv4 or IPv6 destination address for the incoming traffic. An asterisk ("*") indicates any destination address based on IPv4 or IPv6 Ethertypes.
- NW Proto field—The network protocol to be matched for the incoming traffic. For example, "6" indicates the TCP protocol.
- TP Src field—The source port associated with the network protocol to be matched for the incoming traffic. An asterisk ("*") indicates any port value.
- TP Dst field—The destination port associated with the network protocol to be matched for the incoming traffic. An asterisk ("*") indicates any port value.
- Actions field—The output action to be performed for the traffic matching the criteria specified, for example, "OUTPUT = OF|2".
- Byte Count field—The aggregate traffic volume shown in bytes that match the specified flow connection.
- Packet Count field—The aggregate traffic volume shown in packets that match the specified flow connection.
- Duration Seconds field—The amount of time, in milliseconds, that the specific flow connection has been installed in the switch.
- Idle Timeout field—The amount of time, in milliseconds, that the flow can be idle before it is removed from the flow table.
- Priority field—The priority assigned to the flow. The flows with higher priority numbers take precedence.

Step 12 Click **Close** to close the flow statistics display window.

Viewing Statistics

View the flow and port statistics for the switches on the Statistics tab.

Note When you select a switch on the statistics page, the **Auto Refresh** tab for the switch is ON by default. Click **Auto Refresh: Off** to disable auto refresh on the Statistics tab. The screen is refreshed every 30 seconds and the updated statistics for the switch are displayed on the screen.

Procedure

Step 1 Navigate to the **Statistics** tab under **Configuration** and click a node from the drop-down list to check and view the flow and port statistics of that node.

You can also navigate to the statistics of another switch by selecting the switch in the drop down box.

You can view the flow statistics, for example:

- Flow Name
- In Port
- DL Source
- DL Destination
- DL Type
- DL VLAN
- VLAN PCP
- NW Source
- NW Destination
- NW Proto
- TP Source
- TP Destination
- AP HttpMd
- AP TcpOptLn
- Actions
- Byte Count
- Packet Count
- Duration Seconds
- Idle Timeout
- Priority

Step 2 Click the **Ports** tab to check the ports statistics.

You can view the ports statistics as displayed in the following fields.

Note If you are programming the switches with OpenFlow, when you navigate to the **Statistics** tab, select a switch, and select **Ports** tab, the statistics gathered from the switches for the **Rx Frame Errs** and **Collisions** are not supported. The value of -1 is displayed rather than N/A because the variable needs to be an integer.

- Port Name
- Rx Packets
- Tx Packets
- Rx Bytes
- Tx Bytes
- Rx Rate (kbps)
- Tx rate (kbps)
- Rx Drops
- Tx Drops
- Rx Errors
- Tx Errors
- Rx Frame Errors
- Rx Overrun Errors
- Rx CRC Errors
- Collisions

Viewing Connection Port Statistics

Starting with Cisco NDB Release 3.4, port statistics are shown along with the connection path information in the NDB GUI. This feature is supported for Nexus 9K and Nexus 3K Series switches based on NX-API, OpenFlow, and NX-AUX mode.

To view the port statistics for a connection, complete the following steps:

Procedure

Step 1 Navigate to **CONFIGURATION** -> **Connections** .

Step 2 On the **Connection** page, click a connection name for which you want to view the port statistics.

Step 3 Click **Port Statistics** to open the **Flow Statistics** page.

Step 4 Click **Port** tab to view the port statistics for the selected connection.

Deleting Flow and Port Statistics

Starting with Cisco NDB release 3.4, you can now clear port and flow statistics using the NDB GUI. You can either clear all the port related statistics for a switch or clear statistics for a specific port on the switch. For This feature is currently available only for NXAPI based Nexus 9K and Nexus 3K switches.

To clear flow statistics, complete the following steps:

Procedure

Step 1 Navigate to the **CONFIGURATION → Statistics** and click the **Flows** tab to clear flow statistic. Click **Delete ALL** to clear all the flow statistics such as byte count and packet count for the switch.

Step 2 Click the **Ports** tab to clear port statistics.

a) Select a port and click **Delete** to delete statistics for the selected port.

b) Click **Delete All** to clear statistics for all the ports (interfaces) on the switch.

Purging Device Configuration

Starting with Cisco NDB release 3.6, you can now remove and purge all the configuration information (such as connection and redirection) associated with a device that has been removed from the NDB.

To remove device configuration, complete the following steps:

Procedure

Step 1 Navigate to the **ADMINISTRATION** > **Devices** > **Purge Devices**.

Step 2 Select the devices for which you want to remove all the configuration information and click **Remove devices** . All the configurations associated with the removed device will be deleted from NDB database.

Adding SPAN Sessions

On the SPAN Sessions tab, the following fields are displayed:

- SPAN Session
- Filter
- Devices
- SPAN Source
- SPAN Destination

You can add a SPAN session in ACI.

Procedure

Step 1 Click **+ SPAN Session** to add a SPAN session. The **Add SPAN Session** window is displayed.

Step 2 In the **Add SPAN Session** window, add a session name in the **SPAN Session Name** field.

Step 3 (Optional) Select a connection in the **Select Connections** field.

Step 4 In the **Action** pane, select a priority for the SPAN session.

Step 5 Select a rule using the drop-down list in the **Rule Filter** field. You can select the default filter rule, **Default-Match-IP** or select another filter from the drop-down list.

The available filter rules are **Default-Match-IP**, **Match-HTTP**, **Match-vlan**, and **Default-Match-all**.

Step 6 Select a destination device to which the traffic is sent.

Step 7 In the **SPAN SOURCES** pane, select the device type as ACI or NXOS in the **Select Device Type** field. When you select ACI device and click +Add SPAN Source, the **Add Leaf Ports** or **+Add EPG** tabs are displayed.

a) In the **Add Leaf Ports** window, select a pod using the drop-down list in the **POD** field.
b) Select a node using the drop-down list in the **Node** field.
c) Select a port using the drop-down list in the **Port** field.
d) Click **Add Leaf Ports**.
e) In the **SPAN SOURCES** pane, select a direction from the **Incoming**, **Outgoing**, or **Both** options.

The selected Span source is displayed in the **Span Source** field.

f) If you select **+Add EPG** to add EPG source, select a tenant using the drop-down list in the **Tenant** field in the **Add EPG** window.

Note
- All EPG interfaces work only when all the ports are within the same leaf switch.
- If same EPG is across multiple switches, you have to select the leaf switch and the associated ports. One SPAN session needs to be setup for each leaf switch.

g) Select a profile using the drop-down list in the **Profile** field.
h) Select EPG associated with the tenant using the drop-down list in the **EPG** field.

The selected **SPAN Source** is displayed.

i) Select **Include All EPG Interfaces** option.

When you enable this option, the statically configured interfaces are added to the EPG.

Note This option can be used only when all EPG sources are within the same leaf switch.

If the EPG is selected, by default, Cisco Nexus Data Broker listens for the changes in the statically configured interfaces of the selected EPG. If there is any change, it is applied to the SPAN session. The web socket connection is not secured with the certificates. To disable the event listening, add **enableWebSocketHandle=false** in the **config.ini** file under **xnc/configuration** folder.

j) Click **Add EPG**.

Step 8 In the **SPAN SOURCES** pane, when you select the device type as NXOS in the **Select Device Type** field and click **+Add SPAN Source**, the **Add Interface** or **Add VLAN** tabs are displayed.

This field allows to add NXOS SPAN session via NXAPI. It allows to add 2 types of SPAN sources. If you need to add interface as source, click **+ ADD SPAN Source** and click **Interface**. If you need to allow traffic of a particular VLAN, click **VLAN**.

Note You cannot add interfaces and VLAN as SPAN source for the same NXOS SPAN session.

You cannot have ACI and NXOS SPAN sources in the same SPAN session.

Step 9 When you click **+Add Interface**, the **Add Production Switch Interface** window is displayed.

You can select a node, select an interface, and click **Submit**.

Step 10 When you click **+Add VLAN**, the **Add Production Switch VLAN** window is displayed.

You can select a node, enter a VLAN, and click **Submit**.

Step 11 In the **SPAN Destination** field, you can select the SPAN destination.

This field displays SPAN destination for ACI in the ACI SPAN session or SPAN destination for NXOS in the NXOS SPAN session.

Note The SPAN destination should be the same leaf where the SPAN sources are being selected.

SPAN destination and SPAN source interface of ACI should be in the same node. If both are in different nodes, the SPAN session cannot be created.

Step 12 Click **Add SPAN Session**.

A message box is displayed asking you to confirm, **Are you sure you want to add SPAN session?**, if you want to add the SPAN session.

Step 13 Click **OK**.

As a result, a SPAN session is set up in ACI. It also sets up a connection automatically on the Cisco Nexus Data Broker with the same SPAN session name and this connection redirects the traffic from that source port to the monitoring device.

Note Each leaf can have a maximum of 4 SPAN sessions.

You can set up additional SPAN sessions. You can append a new SPAN session to the existing connection. In that case, you can select the new SPAN session in the Add SPAN Session window, use the same connection that is previous ly created, select new SPAN sources from different leaf ports, select the SPAN destination, and add the SPAN session.

It creates a new session in ACI, but it appends an existing connection to include the new traffic on the Cisco Nexus Data Broker side.

You can edit or clone the existing SPAN sessions. If you want to remove a SPAN session, click the session and click **Remove SPAN Session(s)** A message box is displayed asking you to confirm, **Remove the following sessions?**, if you want to remove the displayed SPAN session. Click **Remove SPAN Sessions** to confirm. If the SPAN session is using an existing connection, the connection is updated automatically with the changes. If it is the last connection associated with the SPAN session, the connection is deleted.

Exporting and Importing NDB Configuration

Starting with Cisco Nexus Data Broker,Release 3.4, you can now export and import the device configuration in JSON file format.The configuration file includes information about connected as well as disconnected devices with configuration information such as filters, ports, connections, and redirections.

Exporting NDB Configuration

Complete the following steps to export a configuration from NDB:

Procedure

	Command or Action	Purpose
Step 1	Log into the NDB application.	
Step 2	Navigate to **Administration** -> **System** -> **Configuration**, and click **Export** tab.	
Step 3	Select a device for exporting the configuration from the **Configuration** Pane.	
Step 4	(Optional) Select **Include Connections** check box to include connection information such as filters, connections, service nodes, and redirections.	
Step 5	Click **Generate new Configuration**.	
Step 6	Click **Save** to save the configuration.	

Importing NDB Configuration

Complete the following steps to import a configuration into NDB:

Procedure

	Command or Action	Purpose
Step 1	Log into the NDB application.	
Step 2	Navigate to **Administration** -> **System** -> **Configuration**, and click **Import** tab.	
Step 3	Click **Choose Configuration**, the **File Upload** dialog box appears.	
Step 4	Select a configuration and click **Open**. The selected configuration appears in the **Configuration** Pane.	
Step 5	Select a configuration from the **Configuration** Pane.	

	Command or Action	Purpose
Step 6	(Optional) Select **Include Connections** check box to include connection information such as filters, connections, service nodes, and redirections.	
Step 7	Click **Apply** to apply the configuration to NDB.	

Managing Sampled Flow Configuration

Starting with Cisco NDB Release 3.4, you can now manage the Sampled Flow (sFlow) on NDB switches that are based on NX-API. This feature is currently not available for OpenFlow and NX-AUX based switches. sFlow allows you to monitor real-time traffic in data networks that contain switches and routers. It uses the sampling mechanism in the sFlow agent software on switches and routers to monitor traffic and to forward the sample data to the central data collector.

To enable sFlow on a port, complete the following steps:

Procedure

Step 1 Log into the NDB GUI.

Step 2 Navigate to **CONFIGURATION** -> **Port Definition** tab.

Step 3 Click **Configure Node** to open the **Node Configuration** pane. The **Node Configuration** window is displayed.

Step 4 Click **Configure sFlow** to open the **Configure sFlow** pane.

Step 5 Select **Enable sFlow** from the **Enable/Disable sFlow** drop-down list to open the **Confiigure sFlow** pane.

Step 6 In the **Confiigure sFlow** pane, enter the following details and click Submit.

Field	Description
Agent IP address	sFlow agent IP address.
Select a VRF	VRF to use to reach the SFlow collector IP address.
Collector IP address	SFlow collector address.
Collector UDP	SFlow collector UDP.
Counter Poll Interval	SFlow counter poll interval.
Max Datagram Size	Maximum sampling data size.
Sampling rate	Data sampling rate.
Select Data Source(s)	SFlow datasource interface (Edge-ports)

Note Use **Add to Group** option to add the configured port to a Group of ports.

Note In Sflow pane, the **Select Data Source** field displays only those ports that are configured either as a Edge-SPAN or as a Edge-TAP .

To verify SFLow configuration on a switch, use the show sflow command:

```
RU-29-2003(config)# show sflow
sflow sampling-rate : 4096
sflow max-sampled-size : 128
sflow counter-poll-interval : 20
sflow max-datagram-size : 1400
sflow collector-ip : 0.0.0.0 , vrf : default
sflow collector-port : 6343
sflow agent-ip : 10.16.206.122
sflow data-source interface Ethernet1/1
```

Configuring Symmetric Load Balancing and MPLS Tag Stripping

From the Cisco Nexus Data Broker GUI and the REST API interfaces, you can now configure symmetric load balancing and enable MPLS tag stripping on the Cisco Nexus 3000 Series and Cisco Nexus 9000 Series switches using NX-API as the configuration mode.

Before you begin

Add device to Cisco Nexus Data Broker using NX-API.

Procedure

Step 1 In the topology diagram, click the node for which you wish to configure MPLS tag stripping.

Step 2 In the **Port Configuration** window, click **Configure Node**. The **Node Configuration** window is displayed.

Step 3 In the **Symmetric Load Balancing on Port Channel** drop-down list, select the **Hashing Option**.

Step 4 In the **MPLS Strip Configuration** drop-down list, choose one of the following:

- Enable MPLS Strip.
- Disable MPLS Strip.

Step 5 When you select **Enable MPLS Strip** option, the **Label Age** field is displayed. In the field, enter a value for the MPLS strip label age. The range for MPLS strip label age configuration is 61-31622400.

Step 6 Click **Submit**.

Symmetric/Non-Symmetric Load Balancing Options

The following table lists the symmetric and non-symmetric load balancing options:

Table 4: Symmetric / Non-Symmetric Load Balancing Port Channel Support

Configuration type	Hashing Configuration	Platforms	Options
Symmetric	SOURCE_DESTINATION	N9K*, N3K-C3164XXX, N3K-C32XXX	IP, IP-GRE, IP-L4PORT, IP-L4PORT-VLAN, IP-VLAN, L4PORT, MAC
		Rest	IP, IP-GRE, PORT, MAC, IP-ONLY, PORT-ONLY
Non-symmetric	SOURCE DESTINATION	N9K*, N3K-C3164XXX, N3K-C32XXX	IP, IP-GRE, IP-L4PORT, IP-L4PORT-VLAN, IP-VLAN, L4PORT, MAC
		Rest	IP, IP-GRE, PORT, MAC

Configuring PTP Using NDB

Starting with Cisco NDB Release 3.4, you can configure PTP Timestamping feature using the NDB GUI. PTP is a time synchronization protocol for nodes distributed across a network. Its hardware timestamp feature provides greater accuracy than other time synchronization protocols such as Network Time Protocol (NTP).

A PTP system can consist of a combination of PTP and non-PTP devices. PTP devices include ordinary clocks, boundary clocks, and transparent clocks. Non-PTP devices include ordinary network switches, routers, and other infrastructure devices.

PTP is a distributed protocol that specifies how real-time PTP clocks in the system synchronize with each other. These clocks are organized into a master-member synchronization hierarchy with the grandmaster clock, the clock at the top of the hierarchy, determining the reference time for the entire system. Synchronization is achieved by exchanging PTP timing messages, with the members using the timing information to adjust their clocks to the time of their master in the hierarchy. PTP operates within a logical scope called a PTP domain.

Note For Cisco NDB 3.4 release and later, PTP Time-stamping feature is supported on the Cisco Nexus 93XXX-EX and 92XX Series switches.

Note You need to enable PTP for all the devices in the network to ensure PTP clock time synchronization.

Note After PTP is configured. the default PTP configuration is synchronized with all the ISL ports of the corresponding device.

To configure PTP using NDB GUI, complete these steps:

Procedure

Step 1 Log into Cisco NDB GUI.
Step 2 Navigate to **CONFIGURATION** -> **Port Definition** tab.
Step 3 Click **Configure Node** to open the **Node Configuration** pane.
Step 4 Click **Configure PTP** to open the **Configure PTP** pane.
Step 5 Select **Enable PTP** from the **Enable/Disable PTP** drop-down list.
Step 6 Enter the PTP source IP address in the **Source IP Address** text field.
Step 7 Select the interfaces on which you want to enable PTP from the **Select Port(s)** list.
Step 8 Click **Submit** to enable PTP on the selected interfaces.

Configuring Packet Truncation

Starting with Cisco NDB Release 3.5, you can configure packet truncation on egress ports for Cisco Nexus 9300 FX and EX series switches. Packet truncation involves discarding bytes from a packet starting at a specified byte position. All the data after the specified byte position is discarded. Packet truncation is required when the main information of interest is in the header of a packet or in the initial part of the packet.

Note You can configure a maximum of four monitoring devices with packet truncation on a switch.

To configure packet truncation on a device, you need to:

1. Configuring a Packet Truncation Interface
2. Defining a Monitoring Device with Packet Truncation Interface
3. Adding Connections

Configuring a Packet Truncation Interface

To configure a packet truncation interface, complete these steps:

Procedure

Step 1 Log into NDB.
Step 2 Navigate to the **CONFIGURATION** > **Port Definition** and select the switch for which you plan to configure packet truncation.
Step 3 Click **PORT CONFIGURATION** tab.
Step 4 Click **Configure** for the interface selected for configuration.
Step 5 In the **Configure Ports** pane, click **Select a port type** and then click **Packet Truncation Port**.
Step 6 (Optional) Enter description for the port in the **Port Description** text field.

Step 7 Click **Submit** to create a packet truncation port.

By default a packet truncation port is blocked for ingress traffic.

Note Ensure that the status of the packet truncation port is Administratively Up (green icon) and that the other end of the link is not connected to the same NDB switch.

What to do next

After the packet truncation port is created, you need to create a monitoring device with the packet truncation port. For more information, see Defining a Monitoring Device with Packet Truncation Interface section.

Defining a Monitoring Device with Packet Truncation Interface

Complete the following steps to define a monitoring device with a packet truncation interface:

Procedure

Step 1 Navigate to the **CONFIGURATION** > **Port Definition** and select the switch for which you plan to configure packet truncation.

Step 2 Click **PORT CONFIGURATION** tab.

Step 3 Click **Configure** for the interface selected for configuration.

Step 4 In the **Configure Ports** pane, click **Add Monitoring Device**.

Step 5 In the **Monitoring Device** window, complete the following fields:

Name	Description
Monitoring Device Name	Name of the monitoring device.
Select Switch Name	Name of the switch to add the monitoring device to.
Select Port	Packet truncation port you configured.
Port Description	Description of the port.

Step 6 Select **Packet Truncation**.

Step 7 Enter maximum packet size in the **MTU Size** text field. The MTU size can be between 320 and 1518 bytes.

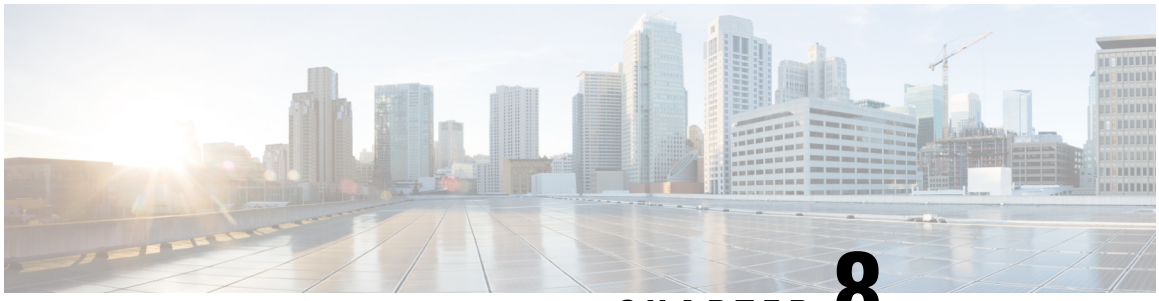
Step 8 From the **Select Packet Truncation Port** drop-down list, select the packet truncation port you created on the same switch.

Step 9 (Optional) Select device icon for the monitoring device.

Step 10 Click **Submit** to create the monitoring device.

What to do next

Create a new connection using the monitoring device to implement the packet truncation feature. For more information, see Adding Connections.



CHAPTER 8

Integrating Cisco Nexus Data Broker With Cisco ACI

This chapter contains the following sections:

Viewing the SPAN Management Tab

The **SPAN Management** tab is displayed on the **Devices** screen under the **Administration** tab in the GUI.

On the **SPAN Management** tab, click + **Add Device**. The **Connect to Device** window is displayed. Complete the following steps to connect to the device:

Before you begin

For APIC and production switches, the centralized deployment of Cisco Nexus Data Broker is mandatory.

Procedure

Step 1 Choose **ACI** device to add an APIC device.

Step 2 In the **APIC IP Addresses** panel, add the **APIC IP Address** (**Primary**), **APIC IP address** (**Secondary**), and **APIC IP address** (**Tertiary**).

Step 3 In the **User Details** panel, add **Username** and **Password**.

Step 4 After an ACI device has been added, the ACI radio button is disabled. Then you can add a NXOS production switch. Click **NXOS** in the first step to add a NXOS production switch.

The NX-API feature has to be enabled for the NXOS production switch to be added. To add a NXOS production switch in the **SPAN Management** tab, one NX-API device should already exist. This is a pre-requisite.

Step 5 Click **Connect**.

The NXOS production switch is displayed with the **Type** as **PS** in the **SPAN Management** tab. The **APIC IP Address** (**Primary**), **APIC IP address** (**Secondary**), and **APIC IP address** (**Tertiary**) do not apply to the NXOS production switch. Therefore, those fields are blank. You can also edit the credentials of the NXOS production switch. Once the production switch is added, it is displayed in the Configuration tab in green. In the Port Configuration window, you can configure SPAN Destination in the production Nexus switches that are NX-API enabled.

Viewing the SPAN Destination Tab

When you click **Port Definition** tab in the GUI, the **Port Definition** screen is displayed. Select the switch from the drop-down list to configure the ports.

On the **Port Definition** screen, the following two tabs are displayed:

- Port Configuration
- SPAN Destination

On the **SPAN Destination** tab, the following details are displayed:

- SPAN Destination Name
- SPAN Destinations
- Node Connector
- Monitor Port Type
- Description

Adding SPAN Destination

When you configure a port as an edge SPAN port and the port is connected to the API side, you can select the pod, node, and port from the ACI side and set the port as SPAN destination. SPAN destination can now be configured on the Cisco Nexus 9000 or Cisco Nexus 3000 Series production switches.

Note For APIC SPAN destination, when you configure a port as an Edge SPAN port and the port is connected to the API side, you can select the pod, the node, and the port from the ACI side and set the port as SPAN destination. For production switch SPAN destination, when you configure a port as an Edge SPAN port and the port is connected to the production switch side, you can select the node and the port from the production switch side and set the port as SPAN destination.

You can add SPAN destination only after either an APIC or the production switch has been successfully added to the network.

Procedure

Step 1 Select the switch for which you want to configure the port details on the **Port Configuration** screen.

Step 2 Click **Configure** under **Action**.

The **Configure Ports** window is displayed.

Step 3 In the **Configure Ports** window, configure the port type from the **Select a port type** drop-down list by selecting one of the following options:

- **Add Monitoring Device**
- **Edge Port-SPAN**
- **Edge Port-TAP**
- **Production Port**

Monitoring Device—Creates a monitoring device for capturing traffic and configures the corresponding delivery port.

Edge Port-SPAN—Creates an edge port for incoming traffic connected to an upstream switch that is configured as a SPAN destination.

Edge Port-TAP—Creates an edge port for incoming traffic connected to a physical TAP port.

Production Port—Creates a production port for the ingress and egress traffic.

When you select the port type, the title of the window changes to **Manage Configure Ports**.

Step 4 In **Manage Configure Ports** window, the details of the selected node are displayed.

Step 5 In the **Destination** panel, if the APIC device is added, it is listed in the drop-down list. Select the **Node Type** as **APIC** from the drop-down list.

The **SPAN Destination** and **Copy Device** tabs are displayed.

Step 6 When you click the **SPAN Destination** tab, the **Select SPAN Destination** window is displayed. It contains the following fields: **Select Pod**, **Select Node**, **Select Port**, and **SPAN Destination**.

Step 7 Select the values for the fields and click **Apply**.

The port is now configured as SPAN destination part and it is displayed on the Port Definition screen.

Creating Copy Devices Using Copy Sessions (BETA)

When you configure a port as an edge-SPAN port, you can create copy devices using Copy Sessions (BETA) functionality.

Note You can add SPAN destination and copy devices only after an APIC device has been successfully added to the network.

Procedure

Step 1 Select the switch for which you want to configure the port details using the **Port Configuration** screen.

Step 2 Click **Configure** under **Action**.

The **Configure Ports** window is displayed.

Step 3 In the **Configure Ports** window, configure the port type from the **Select a port type** drop-down list by selecting one of the following options:

- **Add Monitoring Device**
- **Edge Port-SPAN**
- **Edge Port-TAP**
- **Production Port**

Monitoring Device—Creates a monitoring device for capturing traffic and configures the corresponding delivery port.

Edge Port-SPAN—Creates an edge port for incoming traffic connected to an upstream switch that is configured as a SPAN destination.

Edge Port-TAP—Creates an edge port for incoming traffic connected to a physical TAP port.

Production Port—Creates a production port for the ingress and egress traffic.

When you select the port type, the title of the window changes to **Manage Configure Ports**.

Step 4 In **Manage Configure Ports** window, the details of the selected node are displayed.

Step 5 In the **Destination** panel, if the APIC device is added, it is listed in the drop-down list. Select the **Node Type** as **APIC** from the drop-down list.

The **SPAN Destination** and **Copy Device** tabs are displayed. See *Adding SPAN Destination* section for adding SPAN destination.

Step 6 When you click the **Copy Device** tab in the same window, the **Create Copy Device (BETA)** window is displayed.

Step 7 In the General panel, enter the name of the device in the **Name** field. The values for the fields, **Device Type** and **Physical Domain** are hard-coded.

Step 8 In the Device Interface panel, enter the details in the following fields: **Name**, **Pod**, **Node**, and **Port**. The value for the field, **Path Type** is hard-coded.

Step 9 In the Cluster panel, enter the details in the following fields, **Name** and **VLAN Encap**. The value for the field, **Interface** is hard-coded.

Step 10 Click **Submit** to save the settings.

The name and the path of the copy device is displayed in the destination panel.

Step 11 When you click **Submit** in **Manage Configure Ports** window, the device is displayed in the **Destination** column in the **Port Configuration** screen. When you hover over the device name in the GUI, the name of the **Copy Device** is displayed.

Step 12 Once the **Copy Device** is added, it is displayed in the **APIC Copy Session (BETA)** screen under the **Copy Device** tab.

The following fields are displayed under the **Copy Device** tab: **Cluster Name**, **Managed**, **Device Type**, and **Service Type**.

Step 13 In the **APIC Copy Session (BETA)** screen, the **Service Graph** tab is displayed. When you click **+Add Service Graph**, the **Add Service Graph (BETA)** window is displayed.

Step 14 Add name for the service graph in the **Name** field.

Step 15 Select the copy device for the service graph in the **Copy Device** field.

The copy devices that are created by Cisco Nexus Data Broker are listed in the **Copy Device** field.

Step 16 Click **Submit** to save the settings.

Once the service graph is added, it is displayed in the **APIC Copy Session (BETA)** screen under the **Service Graph** tab. The fields that are displayed on the tab are **Name**, **Copy Device**, **Function Nodes**, and **Action**. The parameters that can be edited for the service graph are **Name** and **Copy Device** only. You can click **Remove** under **Action** column in the **APIC Copy Session (BETA)** screen to remove the service graph.

Note By default, the copy device and the service graph get created under the common tenant.

Adding SPAN Sessions

On the SPAN Sessions tab, the following fields are displayed:

- SPAN Session
- Filter
- Devices
- SPAN Source
- SPAN Destination

You can add a SPAN session in ACI.

Procedure

Step 1 Click **+ SPAN Session** to add a SPAN session. The **Add SPAN Session** window is displayed.

Step 2 In the **Add SPAN Session** window, add a session name in the **SPAN Session Name** field.

Step 3 (Optional) Select a connection in the **Select Connections** field.

Step 4 In the **Action** pane, select a priority for the SPAN session.

Step 5 Select a rule using the drop-down list in the **Rule Filter** field. You can select the default filter rule, **Default-Match-IP** or select another filter from the drop-down list.

The available filter rules are **Default-Match-IP**, **Match-HTTP**, **Match-vlan**, and **Default-Match-all**.

Step 6 Select a destination device to which the traffic is sent.

Step 7 In the **SPAN SOURCES** pane, click **+ Add SPAN Source**. In the pane, click **+ Add Leaf Ports** to add a leaf port to capture the traffic from multiple leaf ports. OR optionally, you can click **+Add EPG** to add an EPG source. Enter the values in the following fields:

a) In the **Add Leaf Ports** window, select a pod using the drop-down list in the **POD** field.
b) Select a node using the drop-down list in the **Node** field.
c) Select a port using the drop-down list in the **Port** field.
d) Click **Add Leaf Ports**.
e) In the **SPAN SOURCES** pane, select a direction from the **Incoming**, **Outgoing**, or **Both** options.

The selected Span source is displayed in the **Span Source** field.

f) If you select **+Add EPG** to add EPG source, select a tenant using the drop-down list in the **Tenant** field in the **Add EPG** window.

Note
- All EPG interfaces work only when all the ports are within the same leaf switch.
- If same EPG is across multiple switches, you have to select the leaf switch and the associated ports. One SPAN session needs to be setup for each leaf switch.

g) Select a profile using the drop-down list in the **Profile** field.

h) Select EPG associated with the tenant using the drop-down list in the **EPG** field.

The selected **SPAN Source** is displayed.

i) Select **Include All EPG Interfaces** option.

When you enable this option, the statically configured interfaces are added to the EPG.

Note This option can be used only when all EPG sources are within the same leaf switch.

If the EPG is selected, by default, Cisco Nexus Data Broker listens for the changes in the statically configured interfaces of the selected EPG. If there is any change, it is applied to the SPAN session. The web socket connection is not secured with the certificates. To disable the event listening, add **enableWebSocketHandle=false** in the **config.ini** file under **xnc/configuration** folder.

j) Click **Add EPG**.

Step 8 In the **SPAN Destination** field, select SPAN destination.

If you install ACI SPAN session, it lists the SPAN destination that is created in ACI.

If you install NXOS SPAN session, it lists the SPAN destination that is created in NXOS.

Note The SPAN destination should be the same leaf where the SPAN sources are being selected.

Step 9 Click **Add SPAN Session**.

A message box is displayed asking you to confirm, **Are you sure you want to add SPAN session?**, if you want to add the SPAN session.

Step 10 Click **OK**.

As a result, a SPAN session is set up in ACI. It also sets up a connection automatically on the Cisco Nexus Data Broker with the same SPAN session name and this connection redirects the traffic from that source port to the monitoring device.

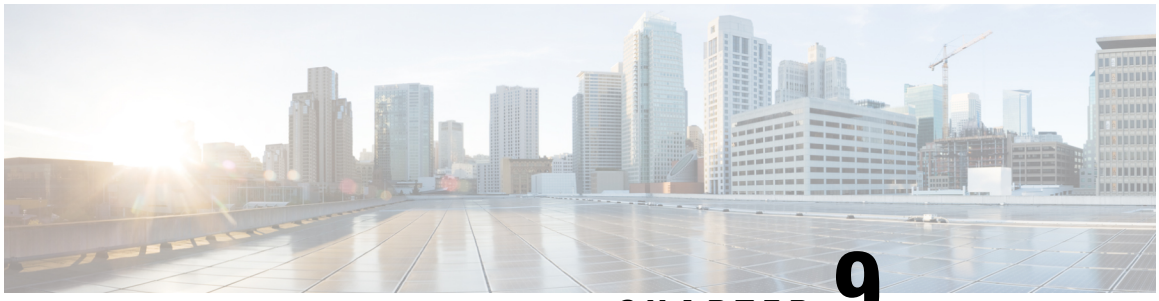
Note Each leaf can have a maximum of 4 SPAN sessions.

You can set up additional SPAN sessions. You can append a new SPAN session to the existing connection. In that case, you can select the new SPAN session in the Add SPAN Session window, use the same connection that is previously created, select new SPAN sources from different leaf ports, select the SPAN destination, and add the SPAN session.

It creates a new session in ACI, but it appends an existing connection to include the new traffic on the Cisco Nexus Data Broker side.

You can edit or clone the existing SPAN sessions. If you want to remove a SPAN session, click the session and click **Remove SPAN Session(s)** A message box is displayed asking you to confirm, **Remove the following sessions?**, if you want to remove the displayed SPAN session. Click **Remove SPAN Sessions** to confirm. If

the SPAN session is using an existing connection, the connection is updated automatically with the changes. If it is the last connection associated with the SPAN session, the connection is deleted.



CHAPTER 9

Viewing and Adding Flows

This chapter contains the following sections:

Viewing Flows

Note This functionality is applicable only for OpenFlow mode of deployment.

On the **Flows** tab, the following fields are displayed:

- Serial Number
- Status
- Flow Name
- Node

What to do next

Click + **Flow** to add a flow.

Adding a Flow

Procedure

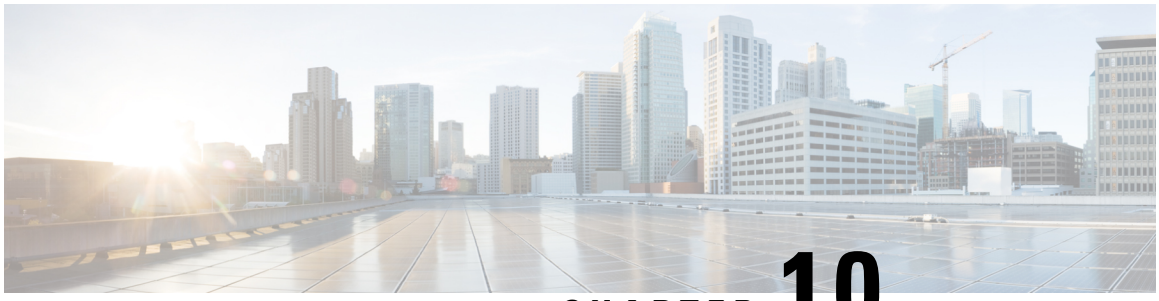
Step 1 Navigate to the **Flows** tab under **Administration**, click + **Flow** to add a flow.

Step 2 On the **Add Flow Description** window, update the following fields:

Name	Description
Name field	The name that you want to assign to the flow. **Note** You cannot change the name of the flow entry after it is saved.
Select a Node drop-down list	Select a node name for the device. **Note** The node you choose cannot be changed one you save the flow entry.
Input Port drop-down list	Choose the port on the node where traffic enters the flow.
Priority field	The priority that you want to apply to the flow. The default priority is 500. Flows with a higher priority are given precedence over flows with a lower priority. **Note** The priority is considered only when all of the Layer 2, Layer 3, and Layer 4 match fields are equal.
Hard Timeout field	The amount of time in milliseconds for the flow to be installed before it is removed from the flow table.
Idle Timeout field	The amount of time in milliseconds that the flow can be idle before it is removed from the flow table.
Layer 2	
Ethernet Type field	The Ethernet type for the Layer 2 traffic. The Ethernet type for IPv4, in hexadecimal format, is displayed by default. Either accept the default value, or enter one of the following, in hexadecimal format: • IPv6 • ARP • LLDP
VLAN Identification Number field	The VLAN ID for the Layer 2 traffic.
VLAN Priority field	The VLAN priority for the Layer 2 traffic.
Source MAC Address field	The source MAC address for the Layer 2 traffic.
Destination MAC Address field	The destination MAC address for the Layer 2 traffic.
Layer 4	
Source Port field	The source port of the Layer 4 traffic.
Destination Port field	The destination port of the Layer 4 traffic.

Name	Description
Protocol field	The Internet protocol number of the Layer 4 traffic. Enter the IP protocol number in decimal, hexadecimal, or octal format.
Actions drop-down list	Select an action from the drop-down list.

Step 3 Click **Install Flow** to install the flow into the device OR click **Save Flow** to save the flow to the **Flow Entries** table, but the system does not install the flow in the flow table of the device.



CHAPTER 10

Viewing Consistency Check

This chapter contains the following sections:

Viewing Consistency Check

On the **Consistency Check** tab, the following details are displayed:

- Node ID
- Inconsistent Controller Flow
- Inconsistent Node Flow
- Statistics: Click **Flows & Ports** for the node statistics.

Procedure

Step 1 Select the node name from the list of available nodes in the **Node Name** field.

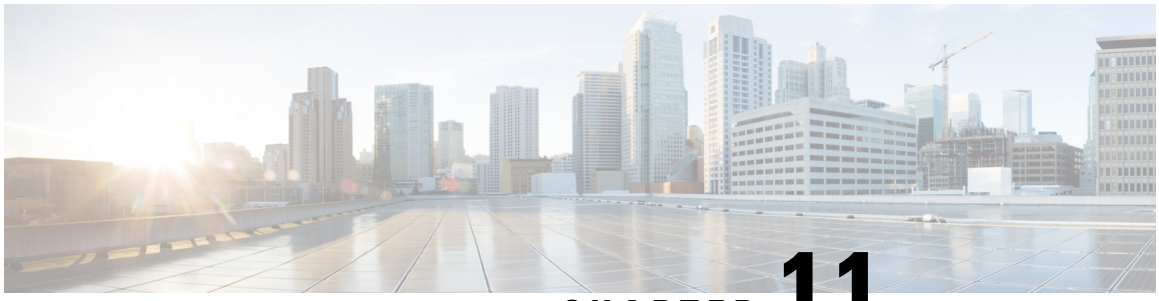
The ID for the selected node is displayed in the **Node ID** field.

Step 2 Click the value in the **Inconsistent Controller Flow** field to view the inconsistent controller flows that display the following fields, **Switch**, **Priority**, **Hard Timeout**, **Idle Timeout**.

Step 3 Click the value in the **Inconsistent Node Flow** field to view the inconsistent node flows.

Step 4 Click **Statistics** to view the flow and port statistics.

Viewing Consistency Check



CHAPTER 11

Managing Users

This chapter contains the following sections:

Adding a User

After creating a user, you can change the password, but you cannot change the roles assigned to the user.

Procedure

Step 1 Navigate to the **User Management** tab under **Administration** and click **+ User** to add a user.

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

Name	Description
Username field	The name that you want to assign to the user.
Password field	The password for the user. Passwords must be between 8 and 256 characters long, contain uppercase and lowercase characters, have at least one numeric character, and have at least one nonalphanumeric character.
Verify Password field	Verify the password by re-entering it.

Name	Description
Choose Role(s) drop-down list	Choose the role that you want to assign to the user. You can assign more than one role. It can be one of the following: • **Application User**—Provides privileges that are defined in the specified application. • **Security**—Provides privileges that are defined in the security application. • **Network Administrator**—Provides full administrative privileges to all applications. • **Network Operator**—Provides read-only privileges to all applications. • **Slice User**—Provides access to a specified slice.
Enter a Role Name field	If you choose **Application User**, enter the name that you want to assign to the role.

Step 3 Click **Save** in the **User Management** window or click **Cancel** to cancel the action.

Adding a Role

Procedure

Step 1 Navigate to the **User Management** tab under **Administration** and click **+ Role**.

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

Field	Description
Name field	The name of the role.
Level drop-down list	Choose the level that you want to assign to the role. This can be one of the following: • App-Administrator—Has full access to all Cisco Nexus Data Broker resources. • App-User—Has full access to resources that are assigned to his resource group and resources that are created by another user who has similar permissions.
Assign Group(s)	Assign groups to the selected role.

Step 3 Click **save**.

Adding a Group

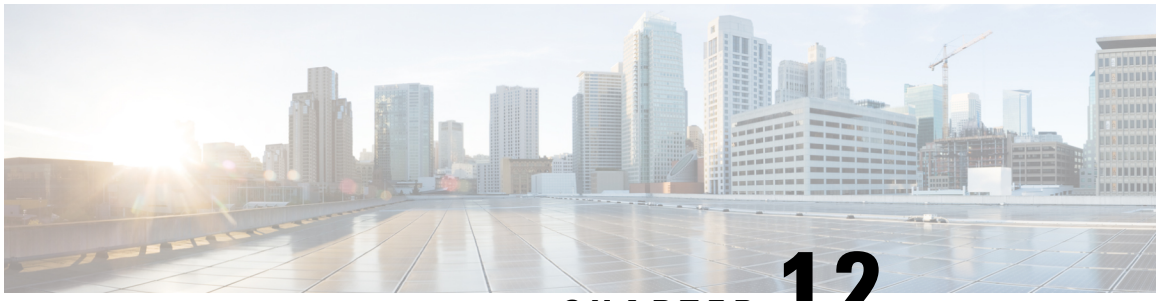
Procedure

Step 1 Navigate to the **User Management** tab under **Administration** and click **+ Groups**.

Step 2 In the **Add Group** window, complete the following field:

Field	Description
Resource Group Name	The name of the resource group.
Select Switch Node	Select a switch node from the drop-down list.
+ Assign Switch and Ports	Click + to add a new switch to the group.
Select Ports	Select the ports associated with the switch.
Assign Group to Roles	Assign a role to the group.

Step 3 Click **Save**.



CHAPTER 12

Configuring the Setup for a Use Case in the Centralized Mode

This chapter contains the following sections:

Configuring Cisco Nexus Data Broker For Centralized Mode Using The CLI

Complete the following steps to configure

Procedure

	Command or Action	Purpose
Step 1	Create two connections.	
Step 2	Run Cisco Nexus Data Broker in Linux server.	
Step 3	Verify that the ofa package is there.	
Step 4	Install ofa.	
Step 5	Configure OpenFlow switch.	

Example

Run Cisco Nexus Data Broker in Linux server.

```
[root@rhel64-ndb-nxapi NDB3.0.0]#
[root@rhel64-ndb-nxapi NDB3.0.0]# ls
ndb1000-sw-app-k9-3.0.0.zip  xnc
[root@rhel64-ndb-nxapi NDB3.0.0]#
 [root@rhel64-ndb-nxapi NDB3.0.0]# cd xnc/
[root@rhel64-ndb-nxapi xnc]# ls
bin  configuration  etc  lib  logs  plugins  runxnc.cmd  runxnc.sh  version.properties
work
```

```
[root@rhel64-ndb-nxapi xnc]# ./runxnc.sh -start
Running controller in background with PID: 11987, to connect to it please SSH to this host
 on port 2400
[root@rhel64-ndb-nxapi xnc]#
```

Verify that the ofa package is installed.

```
switch-1 - Switch
=============

switch-1#
switch-1# dir
       4096    Jun 01 23:55:07 2016  .patch/
       1044    Aug 13 00:15:17 2014  20140813_001215_poap_3799_init.log
         16    Aug 13 00:30:15 2014  cert.err
       9255    Jun 01 23:38:11 2016  clean_config
    2885642    May 12 22:11:57 2014  lltormtc-dplug-mzg.6.0.2.A3.0.23.bin
    4194304    Sep 08 19:24:42 2014  messages
       3752    Mar 18 00:48:03 2014  mts.log
   36825088    Apr 19 18:47:44 2016  n3500-uk9-kickstart.6.0.2.A6.5a.bin
   37472256    Jun 01 23:43:34 2016  n3500-uk9-kickstart.6.0.2.A8.0.15.bin
  180349300    Apr 19 18:49:37 2016  n3500-uk9.6.0.2.A6.5a.bin
  190244286    Jun 01 23:42:07 2016  n3500-uk9.6.0.2.A8.0.15.bin
   54343680    Apr 24 05:27:43 2016  ofa_mmemb-1.1.5-r3-n3000-SPA-k9.ova
       4096    Mar 18 06:08:07 2014  onep/
       3314    Apr 25 18:14:18 2014  sercert.p12
       1024    Apr 19 18:58:37 2016  sprom_cstruct_2_0_0
       1024    Apr 19 18:59:22 2016  sprom_cstruct_3_0_0
       4096    Jan 01 03:25:17 2011  vdc_2/
       4096    Jan 01 03:25:17 2011  vdc_3/
       4096    Jan 01 03:25:17 2011  vdc_4/
       4096    Jun 01 23:31:49 2016  virt_strg_pool_bf_vdc_1/
       4096    Jun 01 23:31:49 2016  virtual-instance/
       4096    Aug 09 02:20:14 2014  virtual-instance-stby-sync/
  243671040    May 09 20:55:18 2016  xnclite_ofa_jdk1877.ova
  243732480    May 10 21:51:52 2016  xnclite_ofa_jdk1892.ova

Usage for bootflash://
 1124974592 bytes used
 770195456 bytes free
 1895170048 bytes total
switch-1#
```

Install ofa.

```
switch-1#
switch-1# virtual-service install name ofa package ofa_mmemb-1.1.5-r3-n3000-SPA-k9.ova
Note: Installing package 'bootflash:/ofa_mmemb-1.1.5-r3-n3000-SPA-k9.ova' for virtual service
 'ofa'. Once the install has finished, the VM may be activated. Use 'show virtual-service
list' for progress.

switch-1# sh virtual-service list

Virtual Service List:

Name                     Status              Package Name
--------------------------------------------------------------------------------
ofa                      Installed           ofa_mmemb-1.1.5-r3-n3000-SPA-k9.ova

switch-1# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch-1(config)# virtual-service ofa
switch-1(config-virt-serv)# activate
Note: Activating virtual-service 'ofa', this might take a few minutes. Use 'show
```

```
virtual-service list' for progress.
switch-1(config-virt-serv)# show virtual-service list

Virtual Service List:

Name                      Status              Package Name
--------------------------------------------------------------------------
ofa                       Activated           ofa_mmemb-1.1.5-r3-n3000-SPA-k9.ova

switch-1(config-virt-serv)#
```

Configure OpenFlow switch.

```
switch-1(config-virt-serv)# openflow
switch-1(config-ofa)# switch 1
switch-1(config-ofa-switch)# pipeline 203
switch-1(config-ofa-switch)# controller ipv4 10.16.206.161 port 6653 vrf management security
 none
switch-1(config-ofa-switch)# sh int br

--------------------------------------------------------------------------------
Ethernet      VLAN    Type Mode   Status  Reason                   Speed     Port
Interface                                                                    Ch #
--------------------------------------------------------------------------------
Eth1/1        1       eth  access up      none                       10G(D) --
Eth1/2        1       eth  access down    SFP not inserted           10G(D) --
Eth1/3        1       eth  access up      none                       10G(D) --
Eth1/4        1       eth  access up      none                       10G(D) --
Eth1/5        1       eth  access down    SFP not inserted           10G(D) --
Eth1/6        1       eth  access down    SFP not inserted           10G(D) --
Eth1/7        1       eth  access down    SFP not inserted           10G(D) --
Eth1/8        1       eth  access down    SFP not inserted           10G(D) --
Eth1/9        1       eth  access down    SFP not inserted           10G(D) --
Eth1/10       1       eth  access down    SFP not inserted           10G(D) --
Eth1/11       1       eth  access down    SFP not inserted           10G(D) --
Eth1/12       1       eth  access down    SFP not inserted           10G(D) --
Eth1/13       1       eth  access down    SFP not inserted           10G(D) --
Eth1/14       1       eth  access down    SFP not inserted           10G(D) --
Eth1/15       1       eth  access down    SFP not inserted           10G(D) --
Eth1/16       1       eth  access down    SFP not inserted           10G(D) --
Eth1/17       1       eth  access down    SFP not inserted           10G(D) --
Eth1/18       1       eth  access down    SFP not inserted           10G(D) --
Eth1/19       1       eth  access down    SFP not inserted           10G(D) --
Eth1/20       1       eth  access down    SFP not inserted           10G(D) --
Eth1/21       1       eth  access down    SFP not inserted           10G(D) --
Eth1/22       1       eth  access down    SFP not inserted           10G(D) --
Eth1/23       1       eth  access down    SFP not inserted           10G(D) --
Eth1/24       1       eth  access down    SFP not inserted           10G(D) --
Eth1/25       1       eth  access down    SFP not inserted           10G(D) --
Eth1/26       1       eth  access down    SFP not inserted           10G(D) --
Eth1/27       1       eth  access down    SFP not inserted           10G(D) --
Eth1/28       1       eth  access down    SFP not inserted           10G(D) --
Eth1/29       1       eth  access down    SFP not inserted           10G(D) --
Eth1/30       1       eth  access down    SFP not inserted           10G(D) --
Eth1/31       1       eth  access down    SFP not inserted           10G(D) --
Eth1/32       1       eth  access down    SFP not inserted           10G(D) --
Eth1/33       1       eth  access down    SFP not inserted           10G(D) --
Eth1/34       1       eth  access down    SFP not inserted           10G(D) --
Eth1/35       1       eth  access down    SFP not inserted           10G(D) --
Eth1/36       1       eth  access down    SFP not inserted           10G(D) --
Eth1/37       1       eth  access down    SFP not inserted           10G(D) --
Eth1/38       1       eth  access down    SFP not inserted           10G(D) --
Eth1/39       1       eth  access down    SFP not inserted           10G(D) --
```

```
Eth1/40       1       eth  access down    SFP not inserted           10G(D) --
Eth1/41       1       eth  access down    SFP not inserted           10G(D) --
Eth1/42       1       eth  access down    SFP not inserted           10G(D) --
Eth1/43       1       eth  access down    SFP not inserted           10G(D) --
Eth1/44       1       eth  access down    SFP not inserted           10G(D) --
Eth1/45       1       eth  access down    SFP not inserted           10G(D) --
Eth1/46       1       eth  access down    SFP not inserted           10G(D) --
Eth1/47       1       eth  access up      none                       10G(D) --
Eth1/48       1       eth  access down    SFP not inserted           10G(D) --

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     10.16.206.129                           1000     1500
switch-1(config-ofa-switch)#
switch-1(config-ofa-switch)#
switch-1(config-ofa-switch)#
switch-1(config-ofa-switch)# of-port interface ethernet1/1-4
switch-1(config-ofa-switch)# of-port interface ethernet1/47
switch-1(config-ofa-switch)#

Switch-2
======

switch-2(config-ofa-switch)# show virtual-service list

Virtual Service List:

Name                    Status             Package Name
------------------------------------------------------------------------
ofa                     Activated          ofa_mmemb-1.1.5-r3-n3000-SPA-k9.ova

switch-2(config-ofa-switch)#
```

What to do next

For centralized mode, complete the steps for configuring Cisco Nexus Data Broker using the GUI as outlined in the next section.

Configuring Cisco Nexus Data Broker in Centralized Mode Using The GUI

After configuring the Cisco Nexus Data Broker using the CLI, complete the following steps:

Procedure

Step 1 Open a new browser window and type *https://<NDB-IP>:8443*.

a)

Step 2 Configure the TAP and SPAN ports using the GUI.

Step 3 Select switch 2 and configure the delivery ports.

Step 4 Add switch 1 and switch 2 in NX-API as in auxiliary mode by enabling the **Set Auxiliary Node** option in the **Add Device** window.

Step 5 Click **Nodes Learned** to configure the mode.

Step 6 For switch 1, click on the OpenFlow device ID and change the **Operation Mode** in the **Update Node Information** window to **Proactive forwarding only** option.

Step 7 For switch 2, click on the OpenFlow device ID and change the **Operation Mode** in the **Update Node Information** window to **Proactive forwarding only** option.

Step 8 In the **Port Definition** window, click **Edit** for delivery port 1/1.

Step 9 Check the **Enable Timestamp Tagging** option in the **Configure Ports** window and click **Submit**.

Step 10 In the **Port Definition** window, click **Edit** for delivery port 1/2.

Step 11 Check the **Enable Timestamp Tagging** option in the **Configure Ports** window and click **Submit**.

After you configure the timestamp, the **TS-Tag** field is displayed next to the port under the **Port Configuration** tab. You can view the monitoring devices in the **Monitoring Devices** tab.

Step 12 Add different traffic filters under the **Filters** tab.

Step 13 Click **Topology** to understand how the devices are learned.

Step 14 Click **Connections** to create a connection.

Step 15 Click **Add Connection** and add filters and the monitoring devices for connection 1.

Step 16 Add connection 2 in a similar way.

After the connections are created, view the connections in the **Connections** tab.

Step 17 View the final topology.

Example of the configuration on switch 1 and switch 2:

```
Switch 1 Configuration: switch-1

hardware profile tcam region racl 512
hardware profile tcam region ifacl 1024 double-wide
hardware profile forwarding-mode openflow-only
hardware internal mtc-usd ttag-eth-type 0x88b5
snmp-server user admin network-admin auth md5 0x188749ba5e1c6af881227235b1b14d04 priv
0x188749ba5e1c6af881227235b1b14d04 localizedkey

vlan 1
vrf context management
  ip route 0.0.0.0/0 10.16.206.1

interface Ethernet1/1
  no lldp transmit
  spanning-tree bpdufilter enable
  mode openflow
  no shutdown

interface Ethernet1/2
  no lldp transmit
  spanning-tree bpdufilter enable
  mode openflow
  no shutdown

interface Ethernet1/3
```

```
  no lldp transmit
  switchport mode trunk
  spanning-tree bpdufilter enable
  mode openflow
  no shutdown

interface Ethernet1/4
  no lldp transmit
  switchport mode trunk
  spanning-tree bpdufilter enable
  mode openflow
  no shutdown

interface Ethernet1/5
  no shutdown

interface Ethernet1/6
  no shutdown

interface Ethernet1/7
  no shutdown

interface Ethernet1/8
  no shutdown

interface Ethernet1/9
  no shutdown

interface Ethernet1/10
  no shutdown

interface Ethernet1/11
  no shutdown

interface Ethernet1/12
  no shutdown

interface Ethernet1/13
  no shutdown

interface Ethernet1/14
  no shutdown

interface Ethernet1/15
  no shutdown

interface Ethernet1/16
  no shutdown

interface Ethernet1/17
  no shutdown

interface Ethernet1/18
  no shutdown

interface Ethernet1/19
  no shutdown

interface Ethernet1/20
  no shutdown

interface Ethernet1/21
  no shutdown
```

```
interface Ethernet1/22
  no shutdown

interface Ethernet1/23
  no shutdown

interface Ethernet1/24
  no shutdown

interface Ethernet1/25
  no shutdown

interface Ethernet1/26
  no shutdown

interface Ethernet1/27
  no shutdown

interface Ethernet1/28
  no shutdown

interface Ethernet1/29
  no shutdown

interface Ethernet1/30
  no shutdown

interface Ethernet1/31
  no shutdown

interface Ethernet1/32
  no shutdown

interface Ethernet1/33
  no shutdown

interface Ethernet1/34
  no shutdown

interface Ethernet1/35
  no shutdown

interface Ethernet1/36
  no shutdown

interface Ethernet1/37
  no shutdown

interface Ethernet1/38
  no shutdown

interface Ethernet1/39
  no shutdown

interface Ethernet1/40
  no shutdown

interface Ethernet1/41
  no shutdown

interface Ethernet1/42
  no shutdown

interface Ethernet1/43
```

```
  no shutdown

interface Ethernet1/44
  no shutdown

interface Ethernet1/45
  no shutdown

interface Ethernet1/46
  no shutdown

interface Ethernet1/47
  no lldp transmit
  spanning-tree bpdufilter enable
  mode openflow
  no shutdown

interface Ethernet1/48
  no shutdown

interface mgmt0
  vrf member management
  ip address 10.16.206.129/24
line console
line vty
boot kickstart bootflash:/n3500-uk9-kickstart.6.0.2.A8.0.15.bin
boot system bootflash:/n3500-uk9.6.0.2.A8.0.15.bin
openflow
  switch 1
    pipeline 203
    controller ipv4 10.16.206.161 port 6653 vrf management security none
    of-port interface ethernet1/1-4
    of-port interface ethernet1/47
virtual-service ofa
  activate
====================================

Switch 2 Configuration  : switch-2


hardware profile tcam region racl 512
hardware profile tcam region ifacl 1024 double-wide
hardware profile forwarding-mode openflow-only
hardware internal mtc-usd ttag-eth-type 0x88b5
snmp-server user admin network-admin auth md5 0xb7289bc7f348c5044b495f93bac10137 priv
0xb7289bc7f348c5044b495f93bac10137 localizedkey

vlan 1
vrf context management
  ip route 0.0.0.0/0 10.16.206.1

interface Ethernet1/1
  no lldp transmit
  ttag
  switchport mode trunk
  spanning-tree bpdufilter enable
  mode openflow
  no shutdown

interface Ethernet1/2
  no lldp transmit
  ttag
  switchport mode trunk
  spanning-tree bpdufilter enable
```

```
  mode openflow
  no shutdown

interface Ethernet1/3
  no shutdown

interface Ethernet1/4
  no shutdown

interface Ethernet1/5
  no shutdown

interface Ethernet1/6
  no shutdown

interface Ethernet1/7
  no shutdown

interface Ethernet1/8
  no shutdown

interface Ethernet1/9
  no shutdown

interface Ethernet1/10
  no shutdown

interface Ethernet1/11
  no shutdown

interface Ethernet1/12
  no shutdown

interface Ethernet1/13
  no shutdown

interface Ethernet1/14
  no shutdown

interface Ethernet1/15
  no shutdown

interface Ethernet1/16
  no shutdown

interface Ethernet1/17
  no shutdown

interface Ethernet1/18
  no shutdown

interface Ethernet1/19
  no shutdown

interface Ethernet1/20
  no shutdown

interface Ethernet1/21
  no shutdown

interface Ethernet1/22
  no shutdown

interface Ethernet1/23
```

```
  no shutdown

interface Ethernet1/24
  no shutdown

interface Ethernet1/25
  no shutdown

interface Ethernet1/26
  no shutdown

interface Ethernet1/27
  no shutdown

interface Ethernet1/28
  no shutdown

interface Ethernet1/29
  no shutdown

interface Ethernet1/30
  no shutdown

interface Ethernet1/31
  no shutdown

interface Ethernet1/32
  no shutdown

interface Ethernet1/33
  no shutdown

interface Ethernet1/34
  no shutdown

interface Ethernet1/35
  no shutdown

interface Ethernet1/36
  no shutdown

interface Ethernet1/37
  no shutdown

interface Ethernet1/38
  no shutdown

interface Ethernet1/39
  no shutdown

interface Ethernet1/40
  no shutdown

interface Ethernet1/41
  no shutdown

interface Ethernet1/42
  no shutdown

interface Ethernet1/43
  no shutdown

interface Ethernet1/44
  no shutdown
```

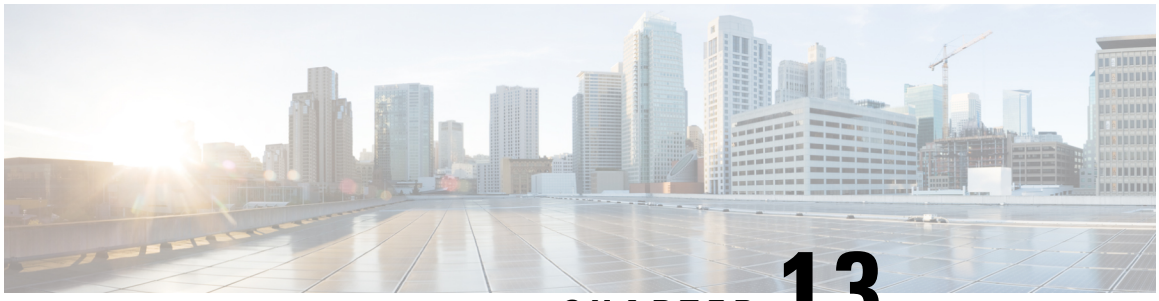
```
interface Ethernet1/45
  no shutdown

interface Ethernet1/46
  no shutdown

interface Ethernet1/47
  no lldp transmit
  spanning-tree bpdufilter enable
  mode openflow
  no shutdown

interface Ethernet1/48
  no shutdown

interface mgmt0
  vrf member management
  ip address 10.16.206.130/24
line console
line vty
boot kickstart bootflash:/n3500-uk9-kickstart.6.0.2.A8.0.15.bin
boot system bootflash:/n3500-uk9.6.0.2.A8.0.15.bin
openflow
  switch 1
    pipeline 203
    controller ipv4 10.16.206.154 port 6653 vrf management security none
    controller ipv4 10.16.206.161 port 6653 vrf management security none
    of-port interface ethernet1/1-2
    of-port interface ethernet1/47
virtual-service ofa
  activate
```



CHAPTER 13

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

Procedure

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.

Procedure

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.

Procedure

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.

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:

Procedure

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

Procedure

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.

Configuring User Authentication for RADIUS Server

User authorization on a RADIUS server must conform to the Cisco Attribute-Value (av-pair) format.

Procedure

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.

Configuring User Authentication for LDAP Server

Starting with Cisco Nexus Data Broker, Release 3.3, you can configure Lightweight Directory Access Protocol (LDAP) for remote authentication, authorization, and accounting (AAA) functions. LDAP provides centralized validation of users attempting to gain access to a Cisco NDB device. LDAP services are maintained in a database on an LDAP server (daemon). You need to configure LDAP server before you configure LDAP features on Cisco NDB for AAA functionality.

LDAP provides for separate authentication and authorization facilities. LDAP allows for a single access control server (the LDAP daemon) to provide each service authentication and authorization independently.

Complete the following steps to configure user authentication using LDAP server:

Procedure

Step 1 Log into NDB application.

Step 2 Navigate to the **Administration**-> **System** -> **AAA** and click **Add Server** to open Add AAA Server dialog box.

Step 3 In the **Add AAA Server** dialog box, complete the following fields:

Name	Description
Protocol field	The protocol to use for AAA server, choose LDAP.
Server Address field	IP address of the LDAP server.
Port field	Port number of the LDAP server.
User RDN field	Relative Domain Name (RDN) where a user can be found in the LDAP tree.

Role Attribute field	The LDAP server user field which identifies the user role. For example, a custom field, ciscoAVPair, can be defined in LDAP schema and used for the user object to store the authorization flag.
	`cn = user1`
	`...`
	`...`
	`ciscoAVPair = network-admin`

Role Type Mapping field	The mapping between the NDB authorization flags and LDAP server. Supported NDB flags are: *network-admin*, *network-operator*, *application-user*, and *slice-user*.

Step 4 Click **Add Server**.

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

Viewing Cluster Information

Procedure

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.

Procedure

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.

Procedure

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.

Procedure

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.

Procedure

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.

Direct upload path to Cisco Nexus Data Broker, Release 3.2 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.

Before you begin

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

Procedure

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.

Scheduling Configuration Backup

Beginning with Cisco Nexus Data Broker, Release 3.2, you can schedule automatic configuration backup with a start date and an end date. The backup is saved at a server location that is set with the variable **scheduler.backup.path=/home** in **config.ini** file with default value as **/home**. When any configuration is performed in Cisco Nexus Data Broker, it can be 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.

Procedure

Step 1 Navigate to **Administration** -> **System** -> **Configuration** and click **Schedule**.

Step 2 Click **Start Date** and **End Date**.

Step 3 (Optional) Or you can select **No End Date**.

Step 4 Choose the start time of the backup using the **Start Time** field in the AM/PM format.

Step 5 Choose the pattern as **Daily**, **Weekly**, or **Monthly**.

Step 6 Choose the days of the week for the scheduled backup.

Step 7 Click **Enable**.

Step 8 Click **Apply**.

After you click **Enable** and click **Apply**, your scheduled backup starts. If you do not click **Enable** but only click **Apply**, the values are saved. The scheduled backup is triggered only after clicking **Enable** and then clicking **Apply**. The scheduled backup is saved and it is displayed under the **Recovery** tab as per the scheduled backup time.

The information for the scheduled backup is displayed using the following columns: **Item** (scheduled backup date and time), **Backup Status**, **Description**, **Restore Triggers**, and **Action**. If you click **Restore** under **Action**, the configuration that is present at the scheduled backup time is restored.

You can search for a particular backup that is taken on a particular start date by adding a date in the **Filter by** field.

Backing Up or Restoring the Configuration

Procedure

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.

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.

Procedure

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.

Procedure

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.