THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018–2019 Cisco Systems, Inc. All rights reserved.
CHAPTER 1

Cisco Nexus Data Broker Overview

This chapter contains the following sections:

- About Cisco Nexus Data Broker, on page 1
- Supported Web Browsers, on page 6
- System Requirements, on page 6
- Guidelines and Limitations, on page 7
- Cisco Nexus Data Broker Software Release Filename Matrix, on page 8
- Nexus Data Broker Hardware and Software Interoperability Matrix, on page 9
- Prerequisites for Cisco Nexus Series Switches, on page 11

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.
Starting with Cisco NDB release 3.6, when a new switch is discovered on NDB, the following connections are installed on the ISL interfaces:

- Default-Deny-ISL connection with Default-Deny-All, Default-Deny-MPLS, and Default-Deny-ARP filters. This connection is supported on all the types of switches in NXAPI mode.
- Default-Deny-ISL-ICMP connection with Default-Deny-ICMP and Default-Deny-ICMP-All filters. This connection is supported on 9200, 9300EX, 9300FX, 9500EX, and 9500FX switches in NXAPI mode.

All the ACLs related to the default filters are installed on the ISL interfaces of the new switch. By default, this feature is enabled for all the new ISL interfaces.

**Note** You can configure a maximum of 30 unique Port ACLs (PACLs) for the Cisco Nexus 9300 FX Platform.

**Note** Each PACL takes one label. If the same PACL is configured on multiple interfaces, the same label is shared. If each PACL has unique entries, the PACL labels are not shared, and the label limit is 30.

**Note** You can manage this feature using the `mm.addDefaultISLDenyRules` attribute in `config.ini` file. By default, the `mm.addDefaultISLDenyRules` attribute is not present in `config.ini` file. To disable this feature, you need to add the `mm.addDefaultISLDenyRules` attribute to `config.ini` file and set it to false and restart the device. For example:

```
mm.addDefaultISLDenyRules = false
```

**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 NDB release 3.6, Global ACLs are automatically added to all the interfaces on a device. By default, Global ACLs are enabled for a device. To manage Global ACLs, you need to add the `configure.global.acls` parameter in the `config.ini` file. Set the `configure.global.acls` parameter to `false` and restart the device to disable Global ACLs on the device.

**Note** Starting with Cisco NDB release 3.6, constistency check option is now available for NX-API based devices along with the OpenFlow based devices.
Starting with Cisco NDB Release 3.4, you can configure the timeout interval for NDB GUI. By default, a user is logged out if the session is inactive for more than 10 minutes. You can configure the inactive timeout interval by modifying the timeout interval attribute in the `xnc/configuration/web.xml` file. You need to restart the NDB to apply the new interval.

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.

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.

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.

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.
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

---

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:

• 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 `generateWebUIcertificatetee.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 45.x and later versions
• Chrome 45.x and later versions
• Internet Explorer 11 or 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 3.6.1.
### 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:

- **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:**

```bash
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
```


- **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.**
- **Starting with Cisco NDB Release 3.7, you can use all the special characters for description field for Port Definitions, Port Groups, Connections, Redirections, Monitoring Devices, and Service Nodes except for the following special characters: Apostrophe (‘), Less Than (<), Greater Than (>), Double Quotation (“), Back Slash (\), Vertical Bar (|), and Question Mark (?).**

---

**Table 1: System Requirements per Deployment Size**

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

<table>
<thead>
<tr>
<th>Mode of Deployment</th>
<th>NXOS Image</th>
<th>Mode</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(3) to 7.0(3)I7(6), 9.2(1) to 9.2(3).</td>
<td>NXAPI</td>
<td>ndb1000-sw-app-emb-i6-plus-k9-3.6.1.zip</td>
</tr>
<tr>
<td>Embedded</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(6), 9.2(1) to 9.2(3).</td>
<td>OpenFlow</td>
<td>ndb1000-sw-app-emb-i6-plus-k9-3.6.1.zip</td>
</tr>
<tr>
<td>Embedded</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(3) to 7.0(3)I7(6), 9.2(1) to 9.2(3).</td>
<td>NXAPI</td>
<td>ndb1000-sw-app-emb-nxapi-3.6.1-k9.zip</td>
</tr>
</tbody>
</table>
### Nexus Data Broker Hardware and Software Interoperability Matrix

The following table lists the hardware and software interoperability matrix for Cisco NDB Release 3.6.1.

<table>
<thead>
<tr>
<th>Mode of Deployment</th>
<th>NXOS Image</th>
<th>Mode</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(6), 9.2(1) to 9.2(3)</td>
<td>Openflow</td>
<td>ndb1000-sw-emb-cfa_mmemb-2.1.4-r2-nxos-SPA-k9.zip</td>
</tr>
<tr>
<td>Embedded</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(6), 9.2(1) to 9.2(3)</td>
<td>Openflow</td>
<td>ndb1000-sw-emb-cfa_mmemb-1.1.4-r3-n3000-SPA-k9.zip</td>
</tr>
<tr>
<td>Centralized</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(3) to 7.0(3)I7(6), 9.2(1) to 9.2(3)</td>
<td>NXAPI</td>
<td>ndb1000-sw-app-k9-3.6.1.zip</td>
</tr>
<tr>
<td>Centralized</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(6), 9.2(1) to 9.2(3)</td>
<td>OpenFlow</td>
<td>ndb1000-sw-app-k9-3.6.1.zip</td>
</tr>
<tr>
<td>Nexus Switch Model(s)</td>
<td>Implementation Type</td>
<td>Supported NX-OS Versions</td>
<td>Open Flow Agent</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------</td>
<td>--------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Nexus 3048 / 3064 / 3172</td>
<td>OpenFlow</td>
<td>6.0(2)U6</td>
<td>1.1.5</td>
</tr>
<tr>
<td>Nexus 3048 / 3064 / 3172</td>
<td>OpenFlow</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(6), 9.2(1) to 9.2(3)</td>
<td>2.1.4</td>
</tr>
<tr>
<td>Nexus 3048 / 3064</td>
<td>NXAPI</td>
<td>6.0(2)U6(x), and 7.0(3)I4(1) to 7.0(3)I4(8b)</td>
<td>NA</td>
</tr>
<tr>
<td>Nexus 3172</td>
<td>NXAPI</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(3) to 7.0(3)I7(6), 9.2(1) to 9.2(3)</td>
<td>NA</td>
</tr>
<tr>
<td>Nexus 3164</td>
<td>OpenFlow</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Nexus 3164</td>
<td>NXAPI</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(3) to 7.0(3)I7(6), 9.2(1) to 9.2(3)</td>
<td>NA</td>
</tr>
<tr>
<td>Nexus 3232</td>
<td>OpenFlow</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(6), 9.2(1) to 9.2(3)</td>
<td>2.1.4</td>
</tr>
<tr>
<td>Nexus 3232</td>
<td>NXAPI</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(3) to 7.0(3)I7(6), 9.2(1) to 9.2(3)</td>
<td>NA</td>
</tr>
<tr>
<td>Nexus 3548</td>
<td>OpenFlow</td>
<td>6.0(2)A6(x) and 6.0(2)A8(x) I7(5) and I7(5a) (OF agent is not required)</td>
<td>1.1.5</td>
</tr>
<tr>
<td>Nexus 3548</td>
<td>NXAPI</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Nexus 92160/92304</td>
<td>OpenFlow</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Nexus 92160/92304</td>
<td>NXAPI</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(3) to 7.0(3)I7(6), 9.2(1) to 9.2(3)</td>
<td>NA</td>
</tr>
<tr>
<td>Nexus 9372 / 9396 / 93128</td>
<td>OpenFlow</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(2) to 7.0(3)I7(6), 9.2(1) to 9.2(3)</td>
<td>2.1.4</td>
</tr>
<tr>
<td>Nexus 9372 / 9396 / 93128</td>
<td>NXAPI</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(3) to 7.0(3)I7(6), 9.2(1) to 9.2(3)</td>
<td>NA</td>
</tr>
<tr>
<td>Nexus 93180LC-EX</td>
<td>OpenFlow</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Nexus 93180LC-EX</td>
<td>NXAPI</td>
<td>7.0(3)I4(1) to 7.0(3)I4(8), 7.0(3)I6(1), 7.0(3)I7(3) to 7.0(3)I7(6), 9.2(1) to 9.2(3)</td>
<td>NA</td>
</tr>
<tr>
<td>Nexus 93180TC-EX / 93180YC-EX</td>
<td>OpenFlow</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Nexus 93180TC-EX / 93180YC-EX</td>
<td>NXAPI</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(3) to 7.0(3)I7(6), 9.2(1) to 9.2(3)</td>
<td>NA</td>
</tr>
<tr>
<td>Nexus 93108TC-FX / 93108YC-FX</td>
<td>OpenFlow</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Nexus Switch Model(s)</td>
<td>Implementation Type</td>
<td>Supported NX-OS Versions</td>
<td>Open Flow Agent</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------</td>
<td>---------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Nexus 93108TC-FX/93108YC-FX</td>
<td>NXAPI</td>
<td>7.0(3)I4(1) to 7.0(3)I4(8), 7.0(3)I6(1), 7.0(3)I7(3) to 7.0(3)I7(6), 9.2(1) to 9.2(3).</td>
<td>NA</td>
</tr>
<tr>
<td>Nexus 9504 / 9508 / 9516</td>
<td>OpenFlow</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>Nexus 9504 / 9508 / 9516</td>
<td>NXAPI</td>
<td>7.0(3)I4(1) to 7.0(3)I4(9), 7.0(3)I6(1), 7.0(3)I7(3) to 7.0(3)I7(6), 9.2(1) to 9.2(3).</td>
<td>NA</td>
</tr>
<tr>
<td>Nexus 31108TC-V / 31108PC-V</td>
<td>NXAPI</td>
<td>7.0(3)I7(5), 7.0(3)I7(5a), 9.2(1), and 9.2(2).</td>
<td>NA</td>
</tr>
<tr>
<td>Nexus 31108TC-V / 31108PC-V</td>
<td>OpenFlow</td>
<td>7.0(3)I7(5), 7.0(3)I7(5a), 9.2(1), and 9.2(2).</td>
<td>NA</td>
</tr>
<tr>
<td>Nexus 9336C-FX2 / 93240YC-FX2</td>
<td>NXAPI</td>
<td>7.0(3)I7(5), 7.0(3)I7(5a), 9.2(1), and 9.2(2).</td>
<td>NA</td>
</tr>
</tbody>
</table>

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 the first NDB deployment with NXOS version 9.2(1), ensure that the `feature nxapi` and `nxapi http port 80` commands are configured on the NDB switch. If you upgrading NDB switch from NXOS version I7(x) to 9.2(1), the `feature nxapi` and `nxapi http port 80` configurations are not required.

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`. 
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.

<table>
<thead>
<tr>
<th>Device Models</th>
<th>OpenFlow Mode</th>
<th>NX-API Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 3000 Series switches</td>
<td>Enter the <code># hardware profile openflow</code> command at the prompt.</td>
<td>Enter the following commands at the prompt:</td>
</tr>
<tr>
<td>Cisco Nexus 3164Q switches</td>
<td>The OpenFlow mode is not supported on the Nexus 3164Q switches.</td>
<td>• <code># hardware profile tcam region qos 0</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code># hardware profile tcam region racl 0</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code># hardware profile tcam region vacl 0</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code># hardware profile tcam region ifacl 1024 double-wide</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code># hardware access-list tcam region mac-ifacl 512</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>#feature nxapi</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>#feature lldp</code></td>
</tr>
<tr>
<td>Cisco Nexus 3172 Series switches</td>
<td>Enter the <code># hardware profile openflow</code> command at the prompt.</td>
<td>Use the <code>hardware profile mode tap-aggregation [l2drop]</code> 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.</td>
</tr>
</tbody>
</table>
### Device Models

<table>
<thead>
<tr>
<th>Device Models</th>
<th>OpenFlow Mode</th>
<th>NX-API Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 3200 Series switches</td>
<td>Enter the <strong>hardware access-list team region openflow 256</strong> command at the prompt.</td>
<td>Enter the following commands at the prompt:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• # hardware access-list team region e-racl 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• # hardware access-list team region span 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• # hardware access-list team region redirect 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• # hardware access-list team region vpc-convergence 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• # hardware access-list team region racl-lite 256</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• # hardware access-list team region l3qos-intra-lite 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• # hardware access-list team region ifacl 256 double-wide</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• # hardware access-list team region mac-ifacl 512</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• # hardware access-list team region ipv6-ifacl 256</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• #feature nxapi</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• #feature lldp</td>
</tr>
<tr>
<td>Cisco Nexus 3500 series switches</td>
<td>Enter either of the following commands at the prompt to configure OpenFlow TCAM:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• # hardware profile forwarding-mode openflow-hybrid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• #hardware profile forwarding-mode openflow-only</td>
<td></td>
</tr>
<tr>
<td>Device Models</td>
<td>OpenFlow Mode</td>
<td>NX-API Mode</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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 IPv4 and IPv6, 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  
  • #feature nxapi  
  • #feature lldp |
<table>
<thead>
<tr>
<th>Device Models</th>
<th>OpenFlow Mode</th>
<th>NX-API Mode</th>
</tr>
</thead>
</table>
| Cisco Nexus 9200, 9300-EX, 9336C-FX2, and 93240YC-FX2 switches | The OpenFlow mode is not supported on the 9200, 9300-EX, 9336C-FX2, and 93240YC-FX2 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`  
  - `#feature nxapi`  
  - `#feature lldp` |
| 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`  
  - `#feature nxapi`  
  - `#hardware acl tap-agg`  
  - `#feature lldp` |
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, on page 17

Installing Cisco Nexus Data Broker in Centralized Mode

Installing the Cisco Nexus Data Broker Software in Centralized Mode

To install the Cisco Nexus Data Broker software in Centralized mode, complete the following steps:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In a web browser, navigate to <a href="http://www.cisco.com">www.cisco.com</a>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Under Support, click All Downloads.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the center pane, click Cloud and Systems Management.</td>
</tr>
<tr>
<td>Step 4</td>
<td>If prompted, enter your Cisco.com username and password to log in.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the right pane, click Network Controllers and Applications, and then click Cisco Nexus Data Broker. The file information for Release 3.6.1 is displayed: Cisco Nexus Data Broker Software Application: ndb1000-sw-app-k9-3.6.1.zip</td>
</tr>
<tr>
<td>Step 6</td>
<td>Download the Cisco Nexus Data Broker application bundle.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Create a directory in your Linux machine where you plan to install Cisco Nexus Data Broker. For example, in your Home directory, create CiscoNDB.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Copy the Cisco Nexus Data Broker zip file into the directory that you created.</td>
</tr>
<tr>
<td>Step 9</td>
<td>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:</td>
</tr>
</tbody>
</table>
  • runxnc.sh file—The file that you use to launch Cisco Nexus Data Broker. |
• `version.properties` file—The Cisco Nexus Data Broker build version.

• `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 3.6.1. 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 and only then you can upgrade to Cisco Nexus Data Broker Release 3.6.1. 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 3.6.1, you cannot use the downgrade option to rollback to a previous release. You have to use the configuration archive that is created during the upgrade process to rollback the software.

**Note** When you upgrade the software to Cisco Nexus Data Broker Release 3.2 or later release, the hostname should not be changed during the upgrade process. If the hostname is changed during the upgrade process, the upgrade might fail. If you are upgrading from release 2.x, 3.0 and 3.1, the domain name configuration in the switch should be removed before upgrading the software.

When you run the `upgrade` command, the installation and the configuration are upgraded. However, any changes you made to the shell scripts or configuration files, for example, `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.

- Backup up the NDB configuration. For more information, see Backing Up or Restoring the Configuration Using NDB GUI section.

- 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 file.

- All the HA cluster members send keepalive message every 3 seconds. If a peer does not respond to keepalive message, peers attempt three retries to determine whether the peer is alive or dead. If a peer does not respond even after three retries, split-brain situation occurs where multiple HA members act as coordinators.

---

**Important**

You should manually backup your config.ini file 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, 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 3.6.1 application bundle: Cisco Nexus Data Broker Software Application—ndb1000-sw-app-k9-3.6.1.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_Upsgrade.

**Step 7**  Unzip the Cisco Nexus Data Broker Release 3.6.1 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 3.6.1 upgrade software.
Starting the Application

Procedure

Step 1 (Optional) Change the default password supplied with Cisco Nexus Data Broker by entering the
\( \text{reset-admin-password} \ [--wait-seconds \ \{\text{wait\_time}\} \ --password \ \{\text{password}\}] \) command.

The \( \{\text{password}\} \) variable resets the administrator password to the value that you specify by restarting the user
manager. The \( \{\text{wait\_time}\} \) is the number of seconds to wait while the user manager restarts. The minimum
\( \{\text{wait\_time}\} \) value is 5 seconds and the maximum is 60 seconds.
Note

- If double ENTER is used instead of entering a value for the password, the password is set to the default values, for example, admin/admin.
- The password must be from 8 to 256 characters, contain both uppercase and lowercase characters, and have at least one number and one nonalphanumeric 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.

Step 2

Navigate to the xnc directory and start Cisco Nexus Data Broker by entering the /runxnc.sh command.

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no option</td>
<td>Starts Cisco Nexus Data Broker with the default option.</td>
</tr>
<tr>
<td>-jmxport port_number</td>
<td>Enables JMX remote access on the specified JVM port.</td>
</tr>
<tr>
<td>-debugport port_number</td>
<td>Enables debugging on the specified JVM port.</td>
</tr>
<tr>
<td>-start</td>
<td>Starts Cisco Nexus Data Broker.</td>
</tr>
<tr>
<td>-start port_number</td>
<td>Starts Cisco Nexus Data Broker on the given port.</td>
</tr>
<tr>
<td>-stop</td>
<td>Stops Cisco Nexus Data Broker.</td>
</tr>
<tr>
<td>-restart</td>
<td>Restarts Cisco Nexus Data Broker.</td>
</tr>
<tr>
<td>-status</td>
<td>Displays the status of Cisco Nexus Data Broker with process ID.</td>
</tr>
<tr>
<td>-console</td>
<td>Starts Cisco Nexus Data Broker with the login console.</td>
</tr>
<tr>
<td>-help</td>
<td>Displays the options for the /runxnc.sh command.</td>
</tr>
<tr>
<td>-tls</td>
<td>Enables TLS secure connections between Cisco Nexus Data Broker and OpenFlow switches.</td>
</tr>
<tr>
<td></td>
<td>To enable TLS, start the controller by entering the /runxnc.sh -tls</td>
</tr>
<tr>
<td></td>
<td>-tlskeystore keystore_file_location -tlstruststore truststore_file_location command.</td>
</tr>
<tr>
<td>-osgiPasswordSync</td>
<td>To set the OSGi web console password same as the XNC password if the XNC password is changed.</td>
</tr>
<tr>
<td></td>
<td>Note  This step is optional. If the application is started without this option, the OSGi console can be accessed through the default credentials.</td>
</tr>
</tbody>
</table>
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**

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

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

3. **Step 3**
   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!`

   **Note**
   Nexus Data Broker can be accessed via Web browser at:

   `https://Nexus_data_broker_ip:8443`

**What to do next**

Connect the switches to the controller. For more information, see the configuration guide for your switches.
Managing TLS Certificate, KeyStore, and TrustStore Files

This chapter contains the following sections:

• Generating TLS Self-Signed Certification Between NDB Server and NDB Switch for NXAPI, on page 23
• Generating TLS 3rd Party Certification Between NDB Server and NDB Switch for NXAPI, on page 28
• Generating TLS Self-Signed Certification Between NDB Server and NDB Switch for OpenFlow, on page 34
• Generating TLS Self-Signed Certification Between WebUI Browser and NDB Server, on page 43
• Generating TLS 3rd Party Certification Between WebUI Browser and NDB Server, on page 46

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

This section describes how to generate TLS self-signed certification between NDB server and NDB Switch. You need to generate certificates and keys for each switch to enable TLS. TLS communication between NDB switch and NDB server uses port 443 only.

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

• Generating Self-Signed Certificate and Key, on page 24
• Creating the TLS TrustStore File, on page 26
• Starting NDB with TLS, on page 27
• Configuring TLS KeyStore and TrustStore Passwords on NDB, on page 28

Note

You cannot configure a controller to communicate using port 80 after configuring TLS.
Generating Self-Signed Certificate and Key

This section describes how to generate self-signed certificate and key.

**Before you begin**

Ensure that you have domain name configured on the switch using `ip domain-name` command for each NDB switch that acts as the Fully Qualified Domain Name (FQDN) for the switch. For example:

```
conf t
ip domain-name cisco.com
hostname N9k-117
end
```

The FQDN for the switch is configured to N9k-117.cisco.com.

**Procedure**

**Step 1**  
Log in to the server.

**Step 2**  
Generate the private key and self-signed certificate using the `openssl req` command.

**Example:**

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

Generating a 2048 bit RSA private key

...+++

.................................++++

writing new private key to '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 Widgeit 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  
If you have multiple switches, generate the certificate file and private key for each switch.

**Step 3**  
Log in to the NDB switch.

**Step 4**  
Copy the certificate file, sw1-ca.pem, and keyfile, sw1-ca.key, to the switch using the `copy` command.

This command creates a certificate file (sw1-ca.pem) and a private key (sw1-ca.key).
Example:
N9K-117# copy scp://docker@10.16.206.250/home/docker/Mallik/TLS_CA_june_23/sw1-ca.pem
bootflash:
Enter vrf (If no input, current vrf 'default' is considered): management
docker@10.16.206.250's password:
server.cer

100% 4676  4.6KB/s  00:00
Copy complete, now saving to disk (please wait)...

N9K-117# copy scp://docker@10.16.206.250/home/docker/Mallik/TLS_CA_june_23/sw1-ca.key
bootflash:
Enter vrf (If no input, current vrf 'default' is considered): management
docker@10.16.206.250's password:
cert.key

100%
Copy complete, now saving to disk (please wait)...

Note  If you have multiple switches, repeat this step for all the switches.

Step 5  Configure the certificate file, sw1-ca.pem, and keyfile, sw1-ca.key in the switch using the nxapi command.

Example:
N9K-117 (config)# nxapi certificate httpskey keyfile bootflash:sw1-ca.key
Upload done. Please enable. Note cert and key must match.
N9K-117 (config)#
N9K-117 (config)# nxapi certificate httpscert certfile bootflash:sw1-ca.pem
Upload done. Please enable. Note cert and key must match.
N9K-117 (config)#

Note  If you have multiple switches, configure the corresponding certificate and private key to each switch.

Step 6  Enable self-signed certificates on the switch using the nxapi certificate command.

Example:
N9K-117 (config)# nxapi certificate enable
N9K-117 (config)#

Note  Ensure that there is no error while enabling self-signed certificates on the switch.

Step 7  Log in to the server.

Step 8  Copy and convert the sw1-ca.key and sw1-ca.pem files to .PEM format using the copy command.

Example:
cp sw1-ca.key sw1-xnc-privatekey.pem
cp sw1-ca.pem sw1-xnc-cert.pem

Step 9  Concatenate the private key and the certificate file using cat command.

Example:
docker@docker-virtual-machine:~/TLS$ cat sw1-xnc-privatekey.pem sw1-xnc-cert.pem > sw1-xnc.pem
Step 10 Convert the .pem file to .p12 file format using the **openssl** command. Enter the export password when prompted to create a password protected .p12 certificate file.

**Example:**
```
docker@docker-virtual-machine:~/TLS$ openssl pkcs12 -export -out sw1-xnc.p12 -in sw1-xnc.pem
Enter Export Password: cisco123
Verifying - Enter Export Password: cisco123
```
Enter a password at the prompt. Use the same password that you entered in the previous Step (cisco123)

Step 11 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: cisco123
Re-enter new password: cisco123
```
Enter source keystore password: cisco123
```
Entry for alias 1 successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled.
```

**Note** By default an alias named “1” is stored in tlsKeyStore for the first switch. When you add the second switch, the utility allows you to rename the first switch alias and also provides a provision to rename alias for the second switch.

Step 12 Transfer the keystore entries .p12 keystore to .jks keystore using the **keytool -importkeystore** command.

**Example:**
```
docker@docker-virtual-machine:~/TLS$ keytool -importkeystore
```

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

Step 13 List and verify content in the java tlsKeyStore using the **keytool** command.

**Example:**
```
docker@docker-virtual-machine:~/TLS$ keytool -list -v -keystore tlsKeyStore | more
```

---

### Creating the TLS TrustStore File

TrustStore is created from the self-signed certificates that are generated for one or more switches. It holds certificates for one or more switches in the controller. This section describes how to create a Truststore using the self-signed certificate created in **Generating Self-Signed Certificate and Key** section. If you have multiple switches in the controller, each switch will have separate certificate file (For example, sw1-xnc-cert.pem, sw2-xnc-cert.pem)

**Procedure**

---

**Step 1** Log in to the server.
Step 2 Convert the certificate file (For example, sw1-xnc-cert.pem) to a Java TrustStore (tlsTrustStore) file using the `keytool` command. Enter a password when prompted to create a password protected Java TrustStore (tlsTrustStore) file. The password should be at least six characters.

**Example:**

```
docker@docker-virtual-machine:~/TLS$ keytool -import -alias sw1 -file sw1-xnc-cert.pem -keystore tlsTrustStore
Enter Export Password: cisco123
Verifying – Enter Export Password: cisco123
```

Note If a NDB controller manages multiple switches, repeat this step for all the switches to add all switch keys into the same TrustStore. For example:

```
docker@docker-virtual-machine:~/TLS$ keytool -import -alias sw2 -file sw2-xnc-cert.pem -keystore tlsTrustStore
docker@docker-virtual-machine:~/TLS$ keytool -import -alias sw3 -file sw3-xnc-cert.pem -keystore tlsTrustStore
```

Step 3 List and verify keys for multiple switches in the same tlsTrustStore using the `keytool` command.

**Example:**

```
docker@docker-virtual-machine:~/TLS$ keytool -list -v -keystore tlsTrustStore | more
```

---

**Starting NDB with TLS**

To start NDB with TLS, complete these steps:

**Procedure**

**Step 1** Log in to the NDB server.

**Step 2** Stop the NDB application, if running, using the `runxnc.sh` command.

**Example:**

```
./runxnc.sh -stop
Controller with PID: 17426 -- Stopped!
```

**Step 3** Copy the tlsKeystore and tlsTruststore files that you created to configuration folder of NDB (xnc/configuration).

**Example:**

```
cp tlskeystore /root/xnc/configuration
```

**Step 4** Start the NDB application with TLS using the `runxnc.sh`.

**Example:**

```
./runxnc.sh -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore ./configuration/tlsTrustStore
```
Configuring TLS KeyStore and TrustStore Passwords on NDB

You need to configure TLS KeyStore and TrustStore passwords to enable NDB to read password protected TLS KeyStore and TrustStore files. To configure TLS KeyStore and TrustStore passwords on NDB, complete these steps:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the NDB server.</td>
</tr>
</tbody>
</table>
| Step 2 | Navigate to bin directory.  
   **Example:**  
   `cd xnc/bin` |
| Step 3 | Configure the TLS KeyStore and TrustStore passwords using the `xnc config-keystore-passwords` command.  
   **Example:**  

After the TLS is enabled on NDB, all the connections between NDB server and NDB switch are established using port 443. Ensure that you change device connections in NDB to use port 443.

Up on successfully completing these steps, you can add nexus switch in the controller using port 443. Use FQDN of the switch to add the device to the NDB controller.

You can verify the Certificate information using the WebUI Sandbox of the switch.

Generating TLS 3rd Party Certification Between NDB Server and NDB Switch for NXAPI

This section describes how to generate TLS 3rd party certification between NDB server and NDB Switch. You need to request for a separate certificate and key for each switch in you network. TLS communication between NDB switch and NDB server uses port 443 only.

Complete the following steps to generate TLS 3rd party certification between NDB Server and NDB Switch for NXAPI:

- Obtaining Certificates from a Certification Authority
- Creating TLS Keystore and Truststore Files for NDB Controller
- Starting NDB with TLS, on page 27
- Configuring TLS KeyStore and TrustStore Passwords on NDB, on page 28
Note: Complete all the steps under both the sections to ensure successful communication between the controller and the switch over TLS.

Obtaining Certificates from a Certification Authority

You can obtain certificate from a Certification Authority (CA) in two ways. You can either directly approach a CA for both the private key and certificate. The CA will generate a private key on your behalf along with the certificate that contains the public key with issuing CA’s signature.

In the other approach, you can generate a private key using tools such as openssl and generate a Certificate Signing Request (CSR) to a certificate issuing authority. The CA generates the certificates with public key using the user identity information from CSR.

Before you begin

Ensure that you have domain name configured in the switch using `ip domain-name` command for each NDB switch that acts as the Fully Qualified Domain Name (FQDN) for the switch. For example:

```
conf t
ip domain-name cisco.com
hostname N9k-117
end
```

The FQDN for the switch is configured to N9K-117.cisco.com.

Procedure

**Step 1**

Log in to the server.

**Step 2**

Generate the private key (cert.key) and certificate signing request (cert.req) using openssl 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

```
.................+++                       +++
writing new private key to 'cert.key'
```

Enter PEM pass phrase:

```
Verifying - Enter PEM pass phrase:  cisco123
-----
```

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
```

Cisco Nexus Data Broker Configuration Guide, Release 3.6.1
Email Address [:] myname@cisco.com

Please enter the following 'extra' attributes to be sent with your certificate request:
A challenge password [:] cisco123
An optional company name [:] cisco123

docker@docker-virtual-machine: # ls
cert.key  cert.req

Step 3 Verify the CSR using the openssl command.

Example:
docker@docker-virtual-machine:~/Mallik/TLS_CA$ openssl req -noout -text -in cert.req

Step 4 The private key is generated with a security passphrase. You may need to unencrypt the private key. To remove the passphrase from the private key, use the openssl command.

Example:
docker@docker-virtual-machine:~/Mk/TLS_CA$ ls
cert.key  cert.req
docker@docker-virtual-machine:~/Mk/TLS_CA$ cp cert.key cert.keybkp
docker@docker-virtual-machine:~/Mk/TLS_CA$ rm cert.key

docker@docker-virtual-machine:~/Mk/TLS_CA$ openssl rsa -in cert.keybkp -out cert.key

Enter pass phrase for cert.keybkp: cisco123

Note Repeat this step to remove passphrase from private keys for all the switches.

Note Depending on the tier of the CA you choose, you can get up to three certificates (certificate chain) for each CSR. This means you get three certificates (root, intermediate and domain) from CA for each NDB switch. You need to check with CA to identify each type of certificate. Certificate naming convention might be different for different certifying authorities. For example: test-root-ca-2048.cer (root), test-ssl-ca.cer (intermediate), N9K-117.cisco.com.cer (domain).

Certificates are mostly shared in .PEM file format.

Step 5 Create a single certificate file from the three certificate files using the cat command. The concatenation should be done in the following order, domain certificate, root certificate, and intermediate certificate. Syntax for cat command: Cat domain certificateroot certificateintermediate certificate > server.cer.

Example:

Step 6 Edit the newly created server.cer file to separate the concatenated END and BEGIN lines. Do not delete anything in the file.

Example:

-----END CERTIFICATE-------------BEGIN CERTIFICATE-----

///// Modify the above line like this by adding a line feed between the two.

-----END CERTIFICATE------

----BEGIN CERTIFICATE------

Note Repeat this step all the switches.
Step 7 Log into the NDB switch.

Step 8 Copy the private key (cert.key) and the certificate from CA (server.cer) to the switch using the copy command.

Example:

```
N9K-117# copy scp://docker@10.16.206.250/home/docker/Mallik/TLS_CA_june_23/server.cer
bootflash:
Enter vrf (If no input, current vrf 'default' is considered): management
docker@10.16.206.250's password:
server.cer
100% 4676 4.6KB/s 00:00
Copy complete, now saving to disk (please wait)...
```

```
N9K-117# copy scp://docker@10.16.206.250/home/docker/Mallik/TLS_CA_june_23/cert.key bootflash:
Enter vrf (If no input, current vrf 'default' is considered): management
docker@10.16.206.250's password:
cert.key
100%
Copy complete, now saving to disk (please wait)...
```

Note Repeat this step for all the switches.

Step 9 Configure the certificate file, sw1-ca.pem, and keyfile, sw1-ca.key in the switch using the `nxapi` command.

Example:

```
N9K-117 (config)# nxapi certificate httpskey keyfile bootflash:cert.key
Upload done. Please enable. Note cert and key must match.
N9K-117 (config)#
N9K-117 (config)# nxapi certificate httpsct certfile bootflash:server.cer
Upload done. Please enable. Note cert and key must match.
N9K-117 (config)#
```

Note If you have multiple switches, configure the corresponding certificate and private key to each switch.

Step 10 Enable self-signed certificates on the switch using the `nxapi certificate` command.

Example:

```
N9K-117 (config)# nxapi certificate enable
N9K-117 (config)#
```

Note Ensure that there is no error while enabling self-signed certificates on the switch.

---

**Creating TLS Keystore and Truststore Files for NDB Controller**

NDB uses certificates and keys to secure communication between switches. It stores the keys and certificates in keystores. These files are stored as tlsTruststore and tlsKeystore files in NDB. Complete the following steps to generate the Java tlsKeyStore and tlsTrustStore files for NDB Controller:

**Procedure**

**Step 1** Copy and convert the server.cer and cert.key files to .PEM format using the `copy` command.

Example:
Step 2 Concatenate the private key (sw1-xnc-privatekey.pem) and certificate file (sw1-xnc-cert.pem) into a single .PEM file using the `cat` command.

**Example:**
```
cat sw1-xnc-privatekey.pem sw1-xnc-cert.pem > sw1-xnc.pem
```

Step 3 Convert the .PEM file to .P12 format using the `openssl` command. Enter the export password when prompted. The password must contain at least 6 characters, for example, cisco123. The sw1-xnc.pem file is converted to a password-protected sw1-xnc.p12 file.

**Example:**
```
docker@docker-virtual-machine:~/TLS$ openssl pkcs12 -export -out sw1-xnc.p12 -in sw1-xnc.pem
Enter Export Password: cisco123
Verifying -  Enter Export Password: cisco123
```

Step 4 Convert the sw1-xnc.p12 to a password protected Java KeyStore (tlsKeyStore) file using the `keytool` command. This command converts the sw1-xnc.p12 file to a password-protected tlsKeyStore file.

**Example:**
```
docker@docker-virtual-machine:~/TLS$ keytool -importkeystore -srckeystore sw1-xnc.p12 -srcestoretype pkcs12 -destkeystore tlsKeyStore -deststoretype jks
Enter Destination Keystore password:cisco123
```

**Note** By default an alias named “1” is stored in tlsKeyStore for the first switch. When you add the second switch, the utility allows you to rename the first switch alias and also provides a provision to rename alias for the new switch.

Step 5 Transfer the keystore entries from keystore to another using the keytool command.

**Example:**
```
docker@docker-virtual-machine:~/TLS$ keytool -importkeystore
```

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

Step 6 List and verify content in the java tlsKeyStore using the keytool command.

**Example:**
```
docker@docker-virtual-machine:~/TLS$ keytool -list -v -keystore tlsKeyStore | more
```

Step 7 Convert the certificate file (sw1-xnc-cert.pem) to a Java TrustStore (tlsTrustStore) file using the `keytool` command. Enter a password when prompted to create a password protected Java TrustStore (tlsTrustStore) file. The password should be at least six characters.

**Example:**
```
docker@docker-virtual-machine:~/TLS$ keytool -import -alias sw1 -file sw1-xnc-cert.pem -keystore tlsTrustStore
```

Owner: EMAILADDRESS=mynname@cisco.com, CN=localhost, OU=insbu, O=cisco, L=SJ, ST=CA, C=US
Issuer: EMAILADDRESS=mynname@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:
Starting NDB with TLS

To start NDB with TLS, complete these steps:

Procedure

Step 1 Log in to the NDB server.
Step 2 Stop the NDB application, if running, using the runxnc.sh command

Example:
docker@docker-virtual-machine:~/TLS$ keytool -list -v -keystore tlsTrustStore | more

Starting NDB with TLS

If a NDB controller manages multiple switches, repeat this step for all the switches to add all switch keys into the same TrustStore. For example:

keytool -import -alias sw2 -file sw2-xnc-cert.pem -keystore tlsTrustStore
keytool -import -alias sw3 -file sw3-xnc-cert.pem -keystore tlsTrustStore

Step 8 List and verify keys for multiple switches in the same tlsTrustStore using the keytool command.

Example:
docker@docker-virtual-machine:~/TLS$ keytool -list -v -keystore tlsTrustStore | more

Note

If a NDB controller manages multiple switches, repeat this step for all the switches to add all switch keys into the same TrustStore. For example:

Keytool -import -alias sw2 -file sw2-xnc-cert.pem -keystore tlsTrustStore
Keytool -import -alias sw3 -file sw3-xnc-cert.pem -keystore tlsTrustStore

Step 8 List and verify keys for multiple switches in the same tlsTrustStore using the keytool command.

Example:
docker@docker-virtual-machine:~/TLS$ keytool -list -v -keystore tlsTrustStore | more

Starting NDB with TLS

To start NDB with TLS, complete these steps:

Procedure

Step 1 Log in to the NDB server.
Step 2 Stop the NDB application, if running, using the runxnc.sh command

Example:
Step 3 Copy the tlsKeystore and tlsTruststore files that you created to configuration folder of NDB (xnc/configuration).

**Example:**

```
cp tlskeystore /root/xnc/configuration
```

Step 4 Start the NDB application with TLS using the `runxnc.sh`.

**Example:**

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

---

**Configuring TLS KeyStore and TrustStore Passwords on NDB**

You need to configure TLS KeyStore and TrustStore passwords to enable NDB to read password protected TLS KeyStore and TrustStore files. To configure TLS KeyStore and TrustStore passwords on NDB, complete these steps:

**Procedure**

**Step 1** Log in to the NDB server.

**Step 2** Navigate to bin directory.

**Example:**

```
cd xnc/bin
```

**Step 3** Configure the TLS KeyStore and TrustStore passwords using the `xnc config-keystore-passwords` command.

**Example:**

```
```

After the TLS is enabled on NDB, all the connections between NDB server and NDB switch are established using port 443. Ensure that you change device connections in NDB to use port 443.

Up on successfully completing these steps, you can add nexus switch in the controller using port 443. Use FQDN of the switch to add the device to the NDB controller.

You can verify the Certificate information using the WebUI Sandbox of the switch.

---

**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
  dir = ./mypersonalca
  # 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
Managing TLS Certificate, KeyStore, and TrustStore Files

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

```plaintext
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 PEM
generating 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:
```bash
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:
```bash
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
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

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
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
Certificate fingerprints:
SHA256:
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
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:
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
```

The certificate trust and key store files are located in XNC/bin directory.

### Managing TLS Certificate, KeyStore, and TrustStore Files

Starting the NDB Application with TLS Enabled

```
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
```


```
---- REQUEST HEADERS ----
GET https://10.16.206.189:8443/controller/osgi/system/console/vmstat HTTP/1.1

```

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.processRecord(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.HttpsURLConnectionImpl.connect(HttpsURLConnectionImpl.java:185)
at java.net.URLStreamHandler.openConnection(URLStreamHandler.java:93)
at java.net.URLStreamHandler.parseURL(URLStreamHandler.java:338)
at com.cisco.ccdn.cli.online.HttpClient$HttpResponse.<init>(HttpClient.java:191)
at com.cisco.ccdn.cli.online.HttpClient.sendRequest(HttpClient.java:108)
at com.cisco.ccdn.cli.online.HttpClient.get(HttpClient.java:92)
at com.cisco.ccdn.cli.online.OnlineCommand.isRunning(OnlineCommand.java:88)
at com.cisco.ccdn.cli.online.ConfigKeyStorePasswordCommand.processCommand(ConfigKeyStorePasswordCommand.java:46)
at com.cisco.ccdn.cli.Cli.processCommand(Cli.java:70)
at com.cisco.ccdn.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.
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.

**Note**

You can create self-signed TLS certificates for NDB in Centralized mode only. NDB in Embedded mode does not support self-signed TLS certificates.

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 :
password
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:
SHA256:
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 .... ] ]
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

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 -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
................+++ writing new 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:
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 file (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, on page 49
- Logging in to the Cisco Nexus Data Broker GUI, on page 53
- Changing the Controller Access to HTTP, on page 53
- Cisco Nexus Data Broker GUI Overview, on page 54
- Saving Configuration Changes, on page 56

Configuring Cisco Nexus Data Broker

Configuring High Availability Clusters

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

Note

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

Note

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

| Table 2: Cluster Operation Status |

<table>
<thead>
<tr>
<th>Cluster Indicator</th>
<th>Cluster Status</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Operational</td>
<td></td>
</tr>
</tbody>
</table>
### Cluster Indicators

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

### 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 51.

### Procedure

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

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

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

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

**Step 5**
Locate the following text:

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

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

**Example:**

IPv4 example.

```plaintext
# 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.

```plaintext
# 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
```
Password Protecting the High Availability Clusters

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

**Procedure**

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

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

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

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

**Step 5** Locate the following text:

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

**Step 6** Remove the comments from the AUTH line.

**Example:**

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

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

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

**Step 8** Save the file and exit the editor.

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

**Step 10** Restart Cisco Nexus Data Broker.

Editing 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 rediscover switches 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**

**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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Predefined Value in Seconds</th>
<th>Minimum Value in Seconds</th>
<th>Recommended Value in Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>of.messageResponseTimer</td>
<td>60</td>
<td>2</td>
<td>60</td>
</tr>
<tr>
<td>of.switchLivenessTimeout</td>
<td>120.5</td>
<td>60.5</td>
<td>120.5</td>
</tr>
<tr>
<td>of.flowStatsPollInterval</td>
<td>240</td>
<td>10</td>
<td>240</td>
</tr>
<tr>
<td>of.portStatsPollInterval</td>
<td>240</td>
<td>5</td>
<td>240</td>
</tr>
<tr>
<td>of.descStatsPollInterval</td>
<td>240</td>
<td>60</td>
<td>240</td>
</tr>
<tr>
<td>of.barrierMessagePriorCount</td>
<td>50</td>
<td>100</td>
<td>50</td>
</tr>
<tr>
<td>of.discoveryInterval</td>
<td>300</td>
<td>30</td>
<td>300</td>
</tr>
<tr>
<td>of.discoveryTimeoutMultiple</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

**NX-API related system parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Predefined Value in Seconds</th>
<th>Minimum Value in Seconds</th>
<th>Recommended Value in Seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>nx.connectionDelayTimer</td>
<td>300</td>
<td>—</td>
<td>300</td>
</tr>
<tr>
<td>nx.flowStatsPollInterval</td>
<td>120</td>
<td>—</td>
<td>120</td>
</tr>
<tr>
<td>nx.tableStatsPollInterval</td>
<td>120</td>
<td>—</td>
<td>120</td>
</tr>
<tr>
<td>nx.portStatsPollInterval</td>
<td>120</td>
<td>—</td>
<td>120</td>
</tr>
<tr>
<td>nx.descStatsPollInterval</td>
<td>120</td>
<td>—</td>
<td>120</td>
</tr>
<tr>
<td>nx.lldpPollingTimer</td>
<td>10</td>
<td>—</td>
<td>10</td>
</tr>
<tr>
<td>nx.portPollingTimer</td>
<td>20</td>
<td>—</td>
<td>20</td>
</tr>
</tbody>
</table>

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

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

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

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Open the config.ini file for editing.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Locate the line <code># Enforce restriction on edge/tap ports user can capture (default false).</code></td>
</tr>
<tr>
<td>Step 3</td>
<td>Remove the comment character from the following line: <code>monitor.strictAuthorization=true</code></td>
</tr>
<tr>
<td>Step 4</td>
<td>Save your work and close the file.</td>
</tr>
<tr>
<td>Step 5</td>
<td>If Cisco Nexus Data Broker is running, restart the application to enable the change.</td>
</tr>
</tbody>
</table>

---

**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

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" />
</Service>
```

**Example:**
Remove the comment character as displayed in the following example:
```
<Service name="Catalina">
  <Connector port="8080" protocol="HTTP/1.1"
  connectionTimeout="20000"
  redirectPort="8443" server="Cisco XNC" enableLookups="false" />
  <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
  scheme="https" secure="true"
  clientAuth="false" sslProtocol="TLS"
  keystoreFile="configuration/keystore"
  keystorePass="ciscoxnc" server="Cisco XNC"
  connectionTimeout="60000" enableLookups="false" />
</Service>
```

Step 2
Restart the controller.

Cisco Nexus Data Broker GUI Overview

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

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

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

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

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

**Topology Tools**

The left side of the topology pane contains a zoom slider that allows you to 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.
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
- IP Address of 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.

Starting with Cisco NDB release 3.6, Global deny ACLs are automatically added to all non-configured (Edge SPAN/TAP & Monitor) interfaces on a device. The Global deny ACL feature is equivalent to Block Rx feature. By default, Global Deny ACL feature is enabled for a device. To disable the Global Deny ACL feature, you need to add the configure.global.acls parameter and set it to false in the config.ini file. After setting the
configure.global.acls parameter, you need to restart the system to disable Global Deny ACLs on the newly added devices.

---

**Note**

To disable Global Deny ACL during CLI upgrade, run the CLI upgrade command and then configure the configure.global.acls parameter to `false` in the `config.ini` file before restarting the NDB. For example:

```
./xnc upgrade --perform --target-home {xnc_directory_to_be_upgraded} [--verbose] [--backupfile {xnc_backup_location_and_zip_filename}]
// In the config.ini file//
configure.global.acls=false
```

To disable Global Deny ACL features during configuration upload, set the configure.global.acls parameter to `false` in the `config.ini` file before restarting the NDB.

---

Starting with Cisco NDB release 3.6, when a new switch is discovered on NDB, the following connections are installed on the ISL interfaces:

- Default-Deny-ISL connection with Default-Deny-All, Default-Deny-MPLS, and Default-Deny-ARP filters. This connection is supported on all the types of switches in NXAPI mode.

- Default-Deny-ISL-ICMP connection with Default-Deny-ICMP and Default-Deny-ICMP-All filters. This connection is supported on 9200, 9300EX, 9300FX, 9500EX, and 9500FX switches in NXAPI mode.

All the ACLs related to the default filters are installed on the ISL interfaces of the new switch. By default, this feature is enabled for all the new ISL interfaces.

---

**Note**

You can manage this feature using the `mm.addDefaultISLDenyRules` parameter in `config.ini` file. By default, the `mm.addDefaultISLDenyRules` parameter is not be present in `config.ini` file. To disable this feature, you need to add the `mm.addDefaultISLDenyRules` parameter to `config.ini` file and set it to `false` and restart the device. For example:

```
mm.addDefaultISLDenyRules = false
```

---

**Note**

To disable Default-Deny-ISL Default-Deny-ISL-ICMP features during CLI upgrade, run the CLI upgrade command and then configure the `mm.addDefaultISLDenyRules` parameter to `false` in the `config.ini` file before restarting the NDB. For example:

```
./xnc upgrade --perform --target-home {xnc_directory_to_be_upgraded} [--verbose] [--backupfile {xnc_backup_location_and_zip_filename}]
// In the config.ini file//
mm.addDefaultISLDenyRules=false
```

To disable Default-Deny-ISL Default-Deny-ISL-ICMP features during configuration upload, set the `mm.addDefaultISLDenyRules` parameter to `false` in the `config.ini` file before restarting the NDB.
Configuring Cisco Nexus 9000 Series Switches

This chapter contains the following sections:

- Guidelines and Limitations, on page 61
- Configuring TCAM Hardware Sizing on Cisco Nexus 9000 Series Switches, on page 62
- Enabling Cisco NX-API on Cisco Nexus 9000 Series Switches Using CLI, on page 63
- Enabling Switch Port Mode as Trunk on the Inter-switch Ports and Port Channels, on page 64

Guidelines and Limitations

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

- Beginning with Cisco NX-OS Release 7.0(3)I7(2), you can enable TAP aggregation for Cisco Nexus 9500 platform switches with N9K-X9700-EX and N9K-X9700-FX line card.

- To enable TAP AGG feature on N9K-X9700-EX and N9K-X9700-FX line card, you need to configure hardware acl tap-agg globally on the Cisco Nexus 9500 switches.

- 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 rediscoverstheswitch 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.

Cisco Nexus Data Broker in OpenFlow mode supports Ethernet MAC source and destination addresses as match capabilities only when the OpenFlow TCAM region is configured as double wide (for example, `hardware access-list tcam region openflow 512 double-wide`). Only ether type match is supported in non double wide mode.

## 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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 |
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 plugin 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enable the management interface. Enable the management interface on the switch.</td>
</tr>
<tr>
<td>switch# conf t</td>
<td>Enter the configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enable the NX-API feature.</td>
</tr>
<tr>
<td>switch (config) # feature nxapi</td>
<td>Configure the NX-API feature.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Configure the HTTP port.</td>
</tr>
<tr>
<td>switch (config) # nxapi http port 80</td>
<td>Configure the HTTP port.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configure the HTTPS port.</td>
</tr>
<tr>
<td>switch (config) # nxapi https port 443</td>
<td>Configure the HTTPS port.</td>
</tr>
<tr>
<td></td>
<td>For the step-by-step configuration information for enabling the NX-API feature on Cisco Nexus 9000 Series switches.</td>
</tr>
</tbody>
</table>

Note: Cisco NDB in OpenFlow mode supports Ethernet MAC source and destination addresses as match capabilities only when the OpenFlow TCAM region is configured as double wide (for example, **hardware access-list tcam region openflow 512 double-wide**). If the OpenFlow TCAM region is configured as non double wide, only ether type match is supported as match capabilities.
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> switch(config)# config t</td>
<td>Enables the configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> switch(config)# interface {type slot/port</td>
<td>port-channel number}</td>
</tr>
<tr>
<td><strong>Step 3</strong> switch(config-if)# switchport mode {access</td>
<td>trunk}</td>
</tr>
<tr>
<td><strong>Step 4</strong> switch(config)# exit</td>
<td>Exits the configuration mode.</td>
</tr>
</tbody>
</table>
CHAPTER 7

Configuring the Nexus Data Broker

This chapter contains the following sections:

- Viewing Topology, on page 65
- Configuring Port Definition, on page 65
- Configuring Port Groups, on page 71
- Editing In Use Monitoring Device, on page 72
- Adding a Service Node, on page 73
- User Defined Field, on page 74
- Adding Filters, on page 76
- Adding Connections, on page 84
- Connection with AutoPriority, on page 88
- Adding Redirections, on page 90
- Viewing Statistics, on page 94
- Viewing Connection Port Statistics, on page 96
- Deleting Flow and Port Statistics, on page 96
- Purging Device Configuration, on page 97
- Adding SPAN Sessions, on page 97
- Exporting and Importing NDB Configuration, on page 99
- Managing Sampled Flow Configuration, on page 100
- Configuring Symmetric/Non-Symmetric Load Balancing and MPLS Tag Stripping, on page 101
- Configuring PTP Using NDB, on page 102
- Configuring Packet Truncation, on page 103

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:
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** Starting with Cisco NDB Release 3.6, you can configure Maximum Transmission Unit (MTU) for all the Cisco Nexus 9xxx devices in NX-API mode using NDB GUI. MTU can be configured at the system level (node level or global level) and the Interface Level (supported only on SPAN and TAP ports). The default value for MTU is 1500 and you can configure MTU between 1500 and 9216. Jumbo MTU is the maximum MTU that can be configured for a node. When you configure Jumbo MTU at the system level, the same MTU value is applied to all the node ISLs.

**Note** Starting with Cisco NDB Release 3.4, a description can have a leading numerical for Edge-SPAN, Edge-TAP, Monitoring devices, Production ports, Filter names, Connections, and Redirections (NX-API, OpenFlow and NX-AUX mode).

**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.
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 bpdudfilter 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 bpdudfilter enable
```

**Note**
Production port has been 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 bpdudfilter 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 for both Edge-SPAN and Edge-TAP where you can block the traffic that is being transmitted out of Edge-SPAN AND Edge-TAP interface.

**Step 9**
A check box is added for **Drop ICMPv6 Neighbour Solicitation** and by default all the ICMP traffic is blocked for all the Edge-SPAN and Edge-TAP port types for Nexus 9300-EX and 9200 Series switches. For the rest of Nexus 9000 Series switches, user has to manually enable this feature to deny or block all the ICMP traffic. This feature is currently available on NX-API based switches for NX-OS versions I5 and later.

**Step 10**
A check box is added for **Enable Timestamp Tagging** to append timestamp tag on the packets using the Timestamp Tagging feature. You can configure this feature on a single device or multiple devices.

For Nexus 9300-EX and 9200 series switches, this feature is applicable for Edge-SPAN and Edge-TAP ports and on the Monitoring devices. To configure Timestamp Tagging feature, ensure that PTP feature is enabled.
on the device. You need to enable Timestamp tagging on monitoring device and edge ports. If Timestamp Tagging feature is not configured on either side of the connection, Edge-SPAN/Edge-TAP and Monitor Devices, the packets are not tagged with timestamp. For Nexus 3500 Series switches, the Timestamp Tagging feature is applicable only for the Monitoring devices.

**Step 11**

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:

<table>
<thead>
<tr>
<th>Section</th>
<th>Field</th>
<th>Editable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Configuration</td>
<td>Port Description</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Block Tx</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Port Type</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>VLAN Packet Truncation</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Drop ICMPv6 Neighbour Solicitation</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Enable Timestamp Tagging</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**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. 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.

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.

Starting with NDB 3.4 release, you can now configure selected fields under Port Group. This feature is supported on the switches running in NX-API, OpenFlow, or NX-AUX mode.
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select the switch for which you want to configure the port details on the Port Group pane.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Edit on the listed table row.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Section</th>
<th>Field</th>
<th>Editable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Group</td>
<td>Port Description</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Port</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Port Name</td>
<td>Yes (If the port is not part of an active connection)</td>
</tr>
<tr>
<td></td>
<td>Port Group</td>
<td>Yes (If the port group is not part of an active connection)</td>
</tr>
</tbody>
</table>

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:
## Adding a Service Node

Starting with Cisco NDB Release 3.7, **Created By** and **Modified By** information is displayed for Service Nodes in the NDB UI.

Complete the following steps to add a service node:

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Navigate to the <strong>Service Nodes</strong> tab under <strong>Configuration</strong> and click <strong>+ Service Node</strong>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In the <strong>Add Service Node</strong> window, enter the name of the service node.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select the ingress port for the service node from the <strong>Service Node Ingress Port</strong> drop-down list.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Select the egress port for the service node from the <strong>Service Node Egress Port</strong> drop-down list.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Enable health check on a service node by selecting the <strong>Service Node Health Check</strong> option. Beginning with Cisco Nexus Data Broker, Release 3.2, you can configure the wait interval in the <strong>config.ini</strong> file before the health check is up. The <strong>ServiceNodeHealthCheckWaitInterval</strong> is the variable in the <strong>config.ini</strong> 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 <strong>config.ini</strong> 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.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Select a service node icon from the available options.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

### Table: Monitor Devices Section

<table>
<thead>
<tr>
<th>Section</th>
<th>Field</th>
<th>Editable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Devices</td>
<td>Monitor Devices Name</td>
<td>Yes (If the monitoring device is not in use)</td>
</tr>
<tr>
<td></td>
<td>Port Description</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Block Rx</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Icons</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Enable Timestamp Tagging</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Enable Timestamp Strip</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Adding a Service Node

| **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. |
| **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:

<table>
<thead>
<tr>
<th>Section</th>
<th>Field</th>
<th>Editable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Node</td>
<td>Description</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Icon</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Service Node Health Check</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Service Node Name</td>
<td>Yes (If the service node is not in use)</td>
</tr>
<tr>
<td></td>
<td>Service Node Ingress Port</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Service Node Egress Port</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Ingress port Description</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Egress port Description</td>
<td>Yes</td>
</tr>
</tbody>
</table>

User Defined Field

You can define a User Defined Field (UDF) and use it while creating a filter for traffic management.

**Note**

Starting with Cisco NDB Release 3.6, you can add multiple UDFs while defining a filter. You can add up to four UDFs for each filter.

**Table 3: UDF Support Matrix**

<table>
<thead>
<tr>
<th>UDF Ethertype</th>
<th>NDB Version</th>
<th>NXOS Version</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>3.3</td>
<td>7.0(3)I5(2)</td>
<td>9200 &amp; 9300</td>
</tr>
<tr>
<td>IPv6</td>
<td>3.6</td>
<td>7.0(3)I6(1)</td>
<td>93xx EX/FX , 95xx EX/FX , 92xx</td>
</tr>
</tbody>
</table>

**Note**

Please refer the NXOS documentation for number of UDF support per platform.

To use UDF to manage traffic, you need to:

- Define a UDF, see [Defining a UDF](#).
Defining a UDF

Complete the following steps to define a UDF:

**Procedure**

**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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the user defined field.</td>
</tr>
<tr>
<td>Keyword</td>
<td>If <em>Header</em> option is selected, the Inner (Offset base from inner/outer header) and L3/L4 (Offset base from L3/L4 header) is enabled.</td>
</tr>
<tr>
<td>Offset field</td>
<td>Number of characters to offset while using matching criteria.</td>
</tr>
<tr>
<td>Devices</td>
<td>Cisco Nexus 9000 Series switch name.</td>
</tr>
<tr>
<td>Type</td>
<td>Specify UDFv4 or UDFv6 support.</td>
</tr>
</tbody>
</table>

**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* and *udfInnerVlanv6*, used to match the inner VLAN in the ISL ports.

---

**Table 4: Qualifying Region for UDF for Different Platforms**

<table>
<thead>
<tr>
<th>Platform</th>
<th>UDF Qualifying TCAM region</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 9200, 9300-EX/9300-FX and 9500-EX/9500-FX</td>
<td>ing-ifacl</td>
</tr>
<tr>
<td>Other platforms</td>
<td>ifacl</td>
</tr>
</tbody>
</table>

- Create a filter using the UDF, see *Adding Filters*.
- Apply the filter (configured with UDF) to a connection to manage traffic, see *Adding Connections*.
The icon for UDF is yellow in color immediately after it is created. After you reboot the device, if the UDF is successfully installed, the UDF icon color changes to green, else it changes to red color.

---

### 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`.

**Note**

Beginning with NDB 3.4 release, you can now edit Filter Name using the NDB GUI. This feature is supported on the switches running in NX-API, OpenFlow, or NX-AUX mode.

**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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the filter. The name cannot be changed once you have saved it.</td>
</tr>
</tbody>
</table>
### Step 3
In the **Layer 2** section of the **Add Filter** window, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bidirectional check box</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Ethernet Type field</strong></td>
<td>Required. The Ethernet type of the Layer 2 traffic. The default value displayed is IPv4, or you can choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• IPv6</td>
</tr>
<tr>
<td></td>
<td>• ARP</td>
</tr>
<tr>
<td></td>
<td>• LLDP</td>
</tr>
<tr>
<td></td>
<td>• Predefined EtherTypes</td>
</tr>
<tr>
<td></td>
<td>• All EtherTypes</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td><strong>VLAN Identification Number field</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>VLAN Priority field</strong></td>
<td>The VLAN priority for the Layer 2 traffic.</td>
</tr>
<tr>
<td><strong>Source MAC Address field</strong></td>
<td>The source MAC address of the Layer 2 traffic.</td>
</tr>
<tr>
<td><strong>Destination MAC Address field</strong></td>
<td>The destination MAC address of the Layer 2 traffic.</td>
</tr>
</tbody>
</table>

### Step 4
In the **Layer 3** section of the **Add Filter** window, update the following fields:
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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, 4.4.4.1,4.4.4.2-4.4.4.4.4.4.5.  |
| **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.  
<p>| <strong>Note</strong>         | When using IPv6 address in the filter, the <strong>Ethernet Type</strong> should be set to IPv6. |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination IP Address field</td>
<td>The destination IP address of the Layer 3 traffic. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• The host IP address, for example, 10.10.10.11</td>
</tr>
<tr>
<td></td>
<td>• An IPv4 address range, for example, 10.10.10.11-10.10.10.18</td>
</tr>
<tr>
<td></td>
<td>• An IPv4 subnet, for example, 10.1.1.0/24</td>
</tr>
<tr>
<td></td>
<td>• The host IP address in IPv6 format, for example, 2001::4</td>
</tr>
<tr>
<td></td>
<td>• The subnet, for example, 10.0.0.0/25</td>
</tr>
<tr>
<td>Note</td>
<td>• 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 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 team region ipv6-ifacl 512.</td>
</tr>
<tr>
<td></td>
<td>• If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 4 source or destination ports.</td>
</tr>
<tr>
<td></td>
<td>• If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 2 VLAN identifiers.</td>
</tr>
<tr>
<td>Protocol drop-down list</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• ICMP</td>
</tr>
<tr>
<td></td>
<td>• TCP</td>
</tr>
<tr>
<td></td>
<td>• UDP</td>
</tr>
<tr>
<td></td>
<td>• Enter Protocol</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UDF drop-down list</td>
<td>User Defined Field.</td>
</tr>
<tr>
<td></td>
<td>• UDF: UDF name.</td>
</tr>
<tr>
<td></td>
<td>• UDF value: Value to be matched.</td>
</tr>
<tr>
<td></td>
<td>• UDF Mask: Mask value in packet to match.</td>
</tr>
<tr>
<td>Note</td>
<td>Starting with Cisco NDB Release 3.6, you can add up to four UDFs to a filter.</td>
</tr>
<tr>
<td>Note</td>
<td>If Add default udf for inner vlan option is selected, you can add only one UDF (UDF that matches outer vlan offset). The udfInnerVlan is applied to the ISL links along with QinQ vlan specified on the SPAN port.</td>
</tr>
<tr>
<td>Note</td>
<td>UDF option is enabled for IPv4 and IPv6 ethertypes.</td>
</tr>
<tr>
<td>ToS Bits field</td>
<td>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.</td>
</tr>
<tr>
<td>Advanced Filter field</td>
<td>Advanced filter, combination of Ethernet type and attributes to manage traffic.</td>
</tr>
</tbody>
</table>

**Step 5** In the **Layer 4** section of the **Add Filter** dialog box, complete the following fields:
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.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination Port</strong> drop-down list</td>
<td>Choose the destination port of the Layer 4 traffic. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• FTP (Data)</td>
</tr>
<tr>
<td></td>
<td>• FTP (Control)</td>
</tr>
<tr>
<td></td>
<td>• SSH</td>
</tr>
<tr>
<td></td>
<td>• TELNET</td>
</tr>
<tr>
<td></td>
<td>• HTTP</td>
</tr>
<tr>
<td></td>
<td>• HTTPS</td>
</tr>
<tr>
<td></td>
<td>• Enter Destination Port</td>
</tr>
</tbody>
</table>

**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:
**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, SY, DSCP, Precedence, TTL, packet-length, and NVE. Advanced filtering is available for the following Ethernet types and options:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Method field</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>• Connect</td>
</tr>
<tr>
<td></td>
<td>• Delete</td>
</tr>
<tr>
<td></td>
<td>• Get</td>
</tr>
<tr>
<td></td>
<td>• Head</td>
</tr>
<tr>
<td></td>
<td>• Post</td>
</tr>
<tr>
<td></td>
<td>• Put</td>
</tr>
<tr>
<td></td>
<td>• Trace</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TCP Option Length field</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.
### Table 5: Advanced Filtering Support

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Supported Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>DSCP, Fragment, Precedence, and TTL</td>
</tr>
<tr>
<td>IPv4 with TCP</td>
<td>Acknowledgment, DSCP, Fragment, FIN, Precedence, PSH, RST, SYN, and TTL</td>
</tr>
<tr>
<td>IPv4 with UDP</td>
<td>DSCP, Fragment, Precedence, and TTL</td>
</tr>
<tr>
<td>IPv6</td>
<td>DSCP and Fragment</td>
</tr>
<tr>
<td>IPv6 with TCP</td>
<td>Acknowledgment, DSCP, Fragment, FIN, PSH, RST, SYN</td>
</tr>
<tr>
<td>IPv6 with UDP</td>
<td>DSCP and Fragment</td>
</tr>
</tbody>
</table>

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

Complete the following steps to add a new connection.

**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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Name</td>
<td>The name of the connection.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description when creating a new connection.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority that you want to set for the connection.</td>
</tr>
<tr>
<td></td>
<td>Connection by default has priority of 100. It can be changed in the range of &lt;1-10000&gt;.</td>
</tr>
<tr>
<td>Lock Connection</td>
<td>Select this option to lock the connection you are creating to prevent any unauthorized modification.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow Filters</strong> drop-down list</td>
<td>Choose a filter to use to allow matching traffic.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You cannot choose the same filter for <strong>Allow Filters</strong> that you choose for <strong>Drop Filters</strong>.</td>
</tr>
<tr>
<td><strong>Set VLAN</strong> field</td>
<td>The VLAN ID that you want to set for the connection.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This functionality is available only in Openflow mode.</td>
</tr>
<tr>
<td><strong>Select Destination Port Group(s)</strong> field</td>
<td>Select <strong>Port Group</strong> option and then select the destination port group from the drop-down list for the new connection.</td>
</tr>
<tr>
<td><strong>Strip VLAN at delivery port</strong> check box</td>
<td>Check this box to strip the VLAN tag from the packet before it reaches the delivery port.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Destination Devices</strong> list</td>
<td>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.</td>
</tr>
</tbody>
</table>
Step 4  In the **Drop Matching Traffic** area, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Drop Filters</strong></td>
<td>Choose the default filter <strong>Default-Match-all</strong> or use other filters to drop the matching traffic.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You cannot choose the same filter for <strong>Drop Filters</strong> that you choose for <strong>Allow Filters</strong>.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select Source Node</strong> drop-down list</td>
<td>Choose the source node that you want to assign.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select Source Port</strong> drop-down list</td>
<td>Choose the port on the source node that you want to assign.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Only edge ports can be used as source ports.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the <strong>Source Ports (Optional)</strong> area, select <strong>Port Group</strong> instead of <strong>Source Ports</strong></td>
<td>Select a port group from <strong>Select Port Group</strong> drop-down list. If you do not have any port groups configured, click + <strong>Port Group</strong> to add a port group.</td>
</tr>
</tbody>
</table>
Similar to the number of Edge-TAP or Edge-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.

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 **Dry Run** to estimate the amount of traffic that will be generated on the new connection.
- Click **Close** to exit the connection without saving it.

Starting with Cisco NDB Release 3.6, you can estimate the amount of traffic generated for a new connection using the Dry Run feature. This feature samples the traffic for 30 seconds for the new connection and estimates the approximate traffic generated for the connection. You can use the Dry Run feature before adding a new connection.

You can manage the Dry Run feature using the `mm.dryrun.timer` parameter in the `config.ini` file. To enable the Dry Run feature, set the `mm.dryrun.timer` parameter to a value greater than zero. If the `mm.dryrun.timer` parameter is set to zero, the Dry Run feature is disabled.

The Dry Run feature shows the topology for the new connection with information about the estimated traffic. The feature samples the traffic for few (`mm.dryrun.timer value in config.ini file`) seconds for the new connection and estimates the approximate traffic generated for the connection. You can use the Dry Run feature before adding a new connection.

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

- Name
- Allow Filters
- Drop Filters
- Source Ports/Port Groups
- Devices
- Priority
- Last Modified By
- Description
- Status
- Action
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 iSearch Connections tab in the Connections screen to search for the connections using the keywords, Success, Installing, Creating, Partial, and Failed.

If a remote monitoring tool is selected, same sources or remote monitoring tool cannot be shared across connections. This condition applies to ISL links also.

Connection with AutoPriority

Starting with Cisco NDB Release 3.4, you can configure filters with overlapping IP address. The traffic from the interfaces with overlapping IP addresses is forwarded to all the monitors configured for the IP address. This feature is supported for the switches running NX-API, OpenFlow, and AUX mode.

You can also configure rules with common IP addresses. You can configure IP address and port overlapping in the same filter.

Beginning with Cisco Nexus Data Broker, Release 3.3, you can now add a new connection with AutoPriority. This functionality provides flexibility to map filters to multiple destination devices 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:

- 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.

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

**Step 1**  Log into the NDB application.

**Step 2**  Navigate to Configuration -> Connection, and click **New Connection with AutoPriority** to add a new connection. The **New Connection with AutoPriority** window is displayed.

**Step 3**  In the **New Connection with AutoPriority** window, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection Name field</strong></td>
<td>The name of the connection.</td>
</tr>
<tr>
<td><strong>Description</strong> field</td>
<td>Short description of the connection.</td>
</tr>
<tr>
<td><strong>Devices/Port Groups</strong></td>
<td>The name of the destination device or the destination port group.</td>
</tr>
<tr>
<td><strong>Devices/Port Groups</strong></td>
<td>Select Devices and then 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. Select Port Group and then select destination port group.</td>
</tr>
<tr>
<td><strong>Allow Filters</strong> list</td>
<td>Filter to apply to the destination device.</td>
</tr>
<tr>
<td><strong>Set VLAN field</strong></td>
<td>VLAN ID range to override the incoming tagged VLAN traffic.</td>
</tr>
<tr>
<td><strong>(Optional) Source Ports</strong></td>
<td>Select Source Ports or Port Group button to create or modify a connection.</td>
</tr>
<tr>
<td><strong>Select Source Node</strong></td>
<td>Source Node Id.</td>
</tr>
<tr>
<td><strong>Select Source port</strong></td>
<td>Source Node port number.</td>
</tr>
<tr>
<td><strong>Select Port Group</strong></td>
<td>If Port Group Button is enabled, select a Port Group from the drop down for creating or modifying a connection.</td>
</tr>
</tbody>
</table>

Cisco Nexus Data Broker Configuration Guide, Release 3.6.1
Adding Redirections

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirection Name</td>
<td>The name of the redirection.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The name of the redirection cannot be changed once you have saved it.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description when creating a new redirection.</td>
</tr>
</tbody>
</table>
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.

Step 3

In the Matching Traffic area, modify the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filters drop-down list</td>
<td>Choose a filter to use to allow matching traffic.</td>
</tr>
<tr>
<td>Note</td>
<td>You cannot choose the same redirection for the filter.</td>
</tr>
</tbody>
</table>

Step 4

In the Redirection Switch area, modify the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Redirection Switch drop-down list</td>
<td>Select the redirection switch that you want to assign.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Service Node drop-down list</td>
<td>Select the redirection service node that you want to assign and click Add Service Node.</td>
</tr>
</tbody>
</table>
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.

**Note**

**Step 6**

Select the **Reverse Service Node 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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. |
| **Select Production Egress Port** drop-down list | Select the production egress port that you want to assign. |

**Step 8**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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. |
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 options 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)

### Table: Field and Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Monitor Traffic</td>
<td>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 options 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).</td>
</tr>
</tbody>
</table>

### 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.
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)
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.

   - 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.

   

   **Note**

   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 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.

---

### 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**

**Step 1** Navigate to **Administration -> System -> Backup/Restore -> Node**, and click **Export** tab.

**Step 2** Click **Refresh** to list the latest list of NDB devices.
**Importing NDB Configuration**

Complete the following steps to import a configuration into NDB:

**Procedure**

1. Navigate to **Administration -> System -> Backup/Restore -> Node**, and click **Import** tab.
2. Click **Select Configuration**, the **File Upload** dialog box appears.
3. Select a JSON file and click **Open**. The selected configuration appears in the **Import** section.
4. Click **Edit** to enter device password (applicable only for NXAPI and NX-AUX mode).
5. (Optional) Select **Include Connections** check box to include connection information such as filters and connections.
6. (Optional) Select **Include Redirections** check box to include connection information such as filters, service nodes, and redirections.
7. Click **Apply** to apply the configuration to NDB. The **Compatibility Matrix** page appears.
8. Select **Accept and continue** to import the configuration.

**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**

1. Log into the NDB GUI.
2. Navigate to **CONFIGURATION -> Port Definition** tab.
3. Click **Configure Node** to open the **Node Configuration** pane. The **Node Configuration** window is displayed.
4. Click **Configure sFlow** to open the **Configure sFlow** pane.
5. Select **Enable sFlow** from the **Enable/Disable sFlow** drop-down list to open the **Configure sFlow** pane.
Step 6

In the **Configure sFlow** pane, enter the following details and click Submit.

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

**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:

```bash
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/Non-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 Load Balancing Type Configuration drop-down list, select the type and corresponding 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 6: Symmetric / Non-Symmetric Load Balancing Port Channel Support

<table>
<thead>
<tr>
<th>Configuration type</th>
<th>Hashing Configuration</th>
<th>Platforms</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Rest</td>
<td>Rest</td>
<td>IP, IP-GRE, PORT, MAC, IP-ONLY, PORT-ONLY</td>
</tr>
<tr>
<td></td>
<td>Rest</td>
<td>Rest</td>
<td>IP, IP-GRE, PORT, MAC</td>
</tr>
</tbody>
</table>

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.

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

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

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.

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring Device Name</td>
<td>Name of the monitoring device.</td>
</tr>
<tr>
<td>Select Switch Name</td>
<td>Name of the switch to add the monitoring device to.</td>
</tr>
<tr>
<td>Select Port</td>
<td>Packet truncation port you configured.</td>
</tr>
<tr>
<td>Port Description</td>
<td>Description of the port.</td>
</tr>
</tbody>
</table>

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, on page 107
- Viewing the SPAN Destination Tab, on page 108
- Adding SPAN Destination, on page 108
- Creating Copy Devices Using Copy Sessions (BETA), on page 109
- Adding SPAN Sessions, on page 111

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Click + SPAN Session to add a SPAN session. The Add SPAN Session window is displayed.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In the Add SPAN Session window, add a session name in the SPAN Session Name field.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) Select a connection in the Select Connections field.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>In the Action pane, select a priority for the SPAN session.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Select a destination device to which the traffic is sent.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>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:</td>
</tr>
<tr>
<td>a) In the Add Leaf Ports window, select a pod using the drop-down list in the POD field.</td>
<td></td>
</tr>
<tr>
<td>b) Select a node using the drop-down list in the Node field.</td>
<td></td>
</tr>
<tr>
<td>c) Select a port using the drop-down list in the Port field.</td>
<td></td>
</tr>
<tr>
<td>d) Click Add Leaf Ports.</td>
<td></td>
</tr>
<tr>
<td>e) In the SPAN SOURCES pane, select a direction from the Incoming, Outgoing, or Both options.</td>
<td></td>
</tr>
</tbody>
</table>

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.
Viewing and Adding Flows

This chapter contains the following sections:

- Viewing Flows, on page 115
- Adding a Flow, on page 115

Viewing Flows

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:
<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
</table>
| **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 once 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 |
<p>| <strong>VLAN Identification Number field</strong> | The VLAN ID for the Layer 2 traffic. |
| <strong>VLAN Priority field</strong> | The VLAN priority for the Layer 2 traffic. |
| <strong>Source MAC Address field</strong> | The source MAC address for the Layer 2 traffic. |
| <strong>Destination MAC Address field</strong> | The destination MAC address for the Layer 2 traffic. |
| <strong>Layer 4</strong> | |
| <strong>Source Port field</strong> | The source port of the Layer 4 traffic. |
| <strong>Destination Port field</strong> | The destination port of the Layer 4 traffic. |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol field</td>
<td>The Internet protocol number of the Layer 4 traffic. Enter the IP protocol</td>
</tr>
<tr>
<td>Actions drop-down list</td>
<td>Select an action from the drop-down list.</td>
</tr>
</tbody>
</table>

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.
Consistency Check

Consistency check shows the number of controller or node inconsistencies for each device and provides option to resolve the inconsistency issues. The consistency check feature shows two types of inconsistencies:

- Controller flows inconsistency: Flows are present in Cisco NDB, but missing from the device.
- Node flows inconsistency: Flows are present in the switch, but missing from Cisco NDB.

Starting with Cisco NDB Release 3.6, consistency check option is now available for NX-API based devices along with the OpenFlow based devices.

Viewing Consistency Check

To check for inconsistency for an OpenFlow or NX-API based device, complete the following steps:

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

**Procedure**

- **Step 1** Navigate to **ADMINISTRATION > Consistency Check**.
- **Step 2** Click **FLOW CHECK NX-API/OpenFlow** tab to view the summary of inconsistencies for the NX-API/OpenFlow based devices. On the **Consistency Check** tab, the following details are displayed:
  - Node Name
  - Inconsistent Controller Flow
• Inconsistent Node Flow
• Non NDB Flows

Note To fix an inconsistent flow, select the devices from the list and click **Fix Inconsistent Flow**.

**Step 3** To view detailed inconsistency information:
- Click **Inconsistent Controller Flows** to view the controller inconsistencies.
- Click **Inconsistent Node Flows** to view the node inconsistencies.
- Click **Non NDB Flows** (available only for NX-API) to view the ACLs present in the device by default or added manually.

**Step 4** To resolve the inconsistency issues:
- Click **Fix Inconsistent Flows** on the **Controller Inconsistent** page, to add the missing controller flows to the device.
- Click **Fix Inconsistent Flows** on the **Node Inconsistent** page, to remove the stale flows from the device.
Managing Users

This chapter contains the following sections:

• Adding a User, on page 121
• Adding a Role, on page 122
• Adding a Group, on page 123

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username field</td>
<td>The name that you want to assign to the user.</td>
</tr>
<tr>
<td>Password field</td>
<td>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.</td>
</tr>
<tr>
<td>Verify Password field</td>
<td>Verify the password by re-entering it.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The name of the role.</td>
</tr>
<tr>
<td>Level drop-down list</td>
<td>Choose the level that you want to assign to the role. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• App-Administrator—Has full access to all Cisco Nexus Data Broker resources.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Assign Group(s)</td>
<td>Assign groups to the selected role.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource Group Name</strong></td>
<td>The name of the resource group.</td>
</tr>
<tr>
<td><strong>Select Switch Node</strong></td>
<td>Select a switch node from the drop-down list.</td>
</tr>
<tr>
<td><strong>+ Assign Switch and Ports</strong></td>
<td>Click + to add a new switch to the group.</td>
</tr>
<tr>
<td><strong>Select Ports</strong></td>
<td>Select the ports associated with the switch.</td>
</tr>
<tr>
<td><strong>Assign Group to Roles</strong></td>
<td>Assign a role to the group.</td>
</tr>
</tbody>
</table>

**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, on page 125
- Configuring Cisco Nexus Data Broker in Centralized Mode Using The GUI, on page 129

Configuring Cisco Nexus Data Broker For Centralized Mode Using The CLI

Complete the following steps to configure

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create two connections.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Run Cisco Nexus Data Broker in Linux server.</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Verify that the ofa package is there.</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Install ofa.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure OpenFlow switch.</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

Run Cisco Nexus Data Broker in Linux server.

```
[root@rhe164-ndb-nxapi NDB3.0.0]#
[root@rhe164-ndb-nxapi NDB3.0.0]# ls
ndb1000-sw-app-k9-3.0.0.zip xnc
[root@rhe164-ndb-nxapi NDB3.0.0]#
[root@rhe164-ndb-nxapi NDB3.0.0]# cd xnc/
[root@rhe164-ndb-nxapi xnc]# ls
bin configuration etc lib logs plugins runxnc.cmd runxnc.sh version.properties work
```
Configure NDB to run as a service in the Linux server.

1. Download the script file named, ndb, based on the operating system (Ubuntu, CentOS, or Redhat). The service script is available at: https://github.com/datacenter/nexus9000/tree/master/nexusdatabroker/serviceScripts.

2. Update the Java Home location in the script file for NDB version is 3.2 and earlier. For the NDB version 3.3 and later, comment the line that configures Java Home.

   ```bash
   export JAVA_HOME=/usr/lib/jvm/java-8-openjdk-amd64/jre
   ```

3. Change the permissions for the script file to 755. Use the `chmod 755 ndb` command. For example:

   ```bash
   ndb-inst# chmod 755 ndb
   ```

4. Update the NDB location in the downloaded script file.

   ```bash
   NDB_PATH = /home/user/xnc
   ```

5. Copy the script file to the `/etc/init.d/` folder in the Linux server.

6. Start, stop, and restart the NDB using the following commands

   ```bash
   ndb-inst # ndb stop
   ndb-inst # ndb start
   ndb-inst # ndb restart
   ```

Verify that the ofa package is installed.

```bash
switch-1 - Switch

switch-1# dir
```

```bash
4096  Jun  01 23:55:07 2016 .patch/
1024  Aug 13  0:01:15 2014 20140813_001215_poap_3799_init.log
  16  Aug 13  0:30:15 2014 cert.err
  9255 Jun  01 23:38:11 2016 clean_config
2885664  May 12 22:11:57 2016 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
180244286 Jun 01 23:42:07 2016 n3500-uk9.6.0.2.A6.0.15.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 sertcert.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_bk_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://
Install ofa.

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Package Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ofa</td>
<td>Installed</td>
<td>ofa_mmemb-1.1.5-r3-n3000-SPA-k9.ova</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Package Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ofa</td>
<td>Activated</td>
<td>ofa_mmemb-1.1.5-r3-n3000-SPA-k9.ova</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>VLAN</th>
<th>Type</th>
<th>Mode</th>
<th>Status</th>
<th>Reason</th>
<th>Speed</th>
<th>Port Ch #</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/1</td>
<td>1</td>
<td>eth</td>
<td>access up</td>
<td>none</td>
<td>10G(D)</td>
<td>10G(D)</td>
<td></td>
</tr>
<tr>
<td>Eth1/2</td>
<td>1</td>
<td>eth</td>
<td>access down</td>
<td>SFP not inserted</td>
<td>10G(D)</td>
<td>10G(D)</td>
<td></td>
</tr>
<tr>
<td>Eth1/3</td>
<td>1</td>
<td>eth</td>
<td>access up</td>
<td>none</td>
<td>10G(D)</td>
<td>10G(D)</td>
<td></td>
</tr>
<tr>
<td>Eth1/4</td>
<td>1</td>
<td>eth</td>
<td>access up</td>
<td>none</td>
<td>10G(D)</td>
<td>10G(D)</td>
<td></td>
</tr>
<tr>
<td>Eth1/5</td>
<td>1</td>
<td>eth</td>
<td>access down</td>
<td>SFP not inserted</td>
<td>10G(D)</td>
<td>10G(D)</td>
<td></td>
</tr>
<tr>
<td>Eth1/6</td>
<td>1</td>
<td>eth</td>
<td>access down</td>
<td>SFP not inserted</td>
<td>10G(D)</td>
<td>10G(D)</td>
<td></td>
</tr>
<tr>
<td>Eth1/7</td>
<td>1</td>
<td>eth</td>
<td>access down</td>
<td>SFP not inserted</td>
<td>10G(D)</td>
<td>10G(D)</td>
<td></td>
</tr>
<tr>
<td>Eth1/8</td>
<td>1</td>
<td>eth</td>
<td>access down</td>
<td>SFP not inserted</td>
<td>10G(D)</td>
<td>10G(D)</td>
<td></td>
</tr>
<tr>
<td>Eth1/9</td>
<td>1</td>
<td>eth</td>
<td>access down</td>
<td>SFP not inserted</td>
<td>10G(D)</td>
<td>10G(D)</td>
<td></td>
</tr>
<tr>
<td>Eth1/10</td>
<td>1</td>
<td>eth</td>
<td>access down</td>
<td>SFP not inserted</td>
<td>10G(D)</td>
<td>10G(D)</td>
<td></td>
</tr>
<tr>
<td>Eth1/11</td>
<td>1</td>
<td>eth</td>
<td>access down</td>
<td>SFP not inserted</td>
<td>10G(D)</td>
<td>10G(D)</td>
<td></td>
</tr>
<tr>
<td>Eth1/12</td>
<td>1</td>
<td>eth</td>
<td>access down</td>
<td>SFP not inserted</td>
<td>10G(D)</td>
<td>10G(D)</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>VRF</td>
<td>Status</td>
<td>IP Address</td>
<td>Speed</td>
<td>MTU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
<td>--------</td>
<td>------------</td>
<td>-------</td>
<td>-----</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mgmt0</td>
<td>up</td>
<td></td>
<td>10.1.6.206.129</td>
<td>1000</td>
<td>1500</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
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-2
```

```
switch-2(config-ofa-switch)# show virtual-service list
```

Virtual Service List:

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Package Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ofa</td>
<td>Activated</td>
<td>ofa_mmemb-1.1.5-r3-n3000-SPA-k9.ova</td>
</tr>
</tbody>
</table>

```
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`.
**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
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
Managing System

This chapter contains the following sections:

- About Slices, on page 137
- Adding a Slice, on page 138
- Adding a Flow Specification, on page 138
- About AAA Servers, on page 139
- Adding a AAA Server, on page 139
- Configuring User Authentication for LDAP Server, on page 140
- Viewing Cluster Information, on page 142
- Viewing the OSGi Console, on page 142
- Viewing the Northbound API Content, on page 142
- Downloading the System Log Files, on page 143
- Backing Up or Restoring the Configuration Using NDB GUI, on page 143
- Recovering the Administrative Password, on page 146
- Uninstalling the Application Software, on page 147

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.
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name that you want to assign to the slice.</td>
</tr>
<tr>
<td>Select Devices</td>
<td>Select the devices that you want to associate with the slice.</td>
</tr>
</tbody>
</table>

**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:
### 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

Starting with Cisco NSB Release 3.4, you can configure a AAA server using a Domain Name or an IP address.

**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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol field</td>
<td>Choose the protocol for the AAA server. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Radius+</td>
</tr>
<tr>
<td></td>
<td>• TACACS+</td>
</tr>
<tr>
<td></td>
<td>• LDAP</td>
</tr>
<tr>
<td>Note</td>
<td>For detailed information about how to configure LDAP for AAA server, see Configuring User Authentication for LDAP.</td>
</tr>
<tr>
<td>Server Address field</td>
<td>Server IP address or Domain Name.</td>
</tr>
<tr>
<td>Secret field</td>
<td>The shared secret configured on the AAA server.</td>
</tr>
<tr>
<td>User Name field</td>
<td>User name for authentication.</td>
</tr>
<tr>
<td>Password field</td>
<td>Password for authenticating the user.</td>
</tr>
</tbody>
</table>

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

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

Step 4  Click Save.

What to do next

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

Configuring User Authentication for 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol field</td>
<td>The protocol to use for AAA server, choose LDAP.</td>
</tr>
<tr>
<td>Server Address field</td>
<td>IP address of the LDAP server.</td>
</tr>
<tr>
<td>Port field</td>
<td>Port number of the LDAP server.</td>
</tr>
<tr>
<td>User RDN field</td>
<td>Relative Domain Name (RDN) where a user can be found in the LDAP tree.</td>
</tr>
<tr>
<td>Role Attribute field</td>
<td>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.</td>
</tr>
</tbody>
</table>

*Example:*  
```
  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 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.

---

**Backing Up or Restoring the Configuration Using NDB GUI**

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

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

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

Cisco NDB provides two restore options:
• Restore from Server—Configuration is restored from a server.
• Restore Locally—Configuration is restored from a local directory.

Back Up or Restoring the Configuration Using the CLI

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

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

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

Step 4  Restore the configuration by entering the ./xnc config --restore --backupfile \{zip_filename\} command.

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

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

Scheduling Configuration Backup to NDB Server

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

Note

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

Procedure

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

Step 2  From the Backup drop-down list, select Schedule backup to NDB Server to open the Schedule page.
Step 3
In the Schedule page, enter the following details:

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

Restoring Configuration Locally

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

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

Procedure

Step 1 Navigate to the System tab under Administration and click Restore Locally to upload the configuration.

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

Step 3 Click on the archive file.

The system configuration is uploaded and the browser displays a message informing you that you need to restart the server.

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

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

**Procedure**

**Step 1** Navigate to **Administration** -&gt; **System** -&gt; **Backup/Restore** tab.

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

Restoring Configuration from a Server

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

**Procedure**

**Step 1** Navigate to **Administration** -&gt; **System** -&gt; **Backup/Restore** tab.

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

Recovering the Administrative Password

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

**Note**

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

**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.
INDEX

3rd Party Certification 46

G

Generating Self-Signed Certification 34, 43, 46
Generating TLS 34, 43, 46