Cisco Nexus Data Broker Configuration Guide, Release 3.10.x

First Published: 2021-01-08

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

Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

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.

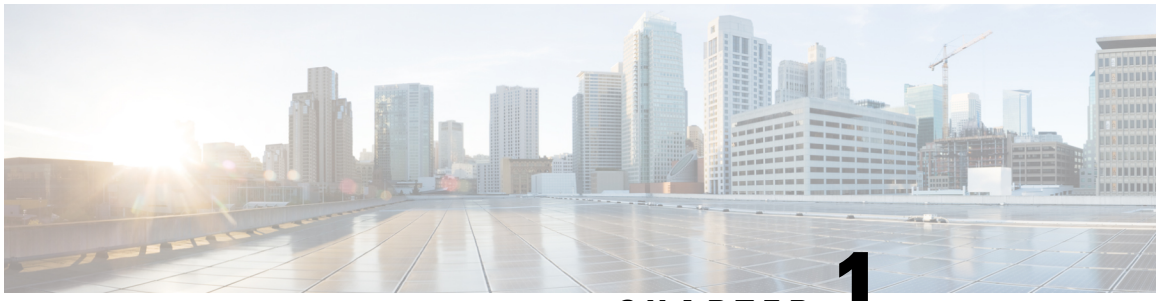
Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

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.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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)

Trademarks



CHAPTER 1

Overview

This chapter contains overview information of the Cisco Nexus Data Broker.

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 (NDB) 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. Using the Cisco NX-API agent to communicate to the switches, Cisco Nexus Data Broker provides advance features for traffic management.

Cisco NDB provides management support for multiple disjointed Cisco NDB networks. You can manage multiple Cisco NDB topologies that may be disjointed using the same application instance. For example, if you have 5 data centers and want to deploy an independent 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.

Basic Salient features of the the Cisco Nexus Data Broker:

- Scalable topology for TAP and SPAN port aggregation.
- Robust Representational State Transfer (REST) API and a web-based GUI for performing all functions.
- Ability to replicate and forward traffic to multiple monitoring tools.
- Rules for matching monitoring traffic based on Layer 1 through Layer 4 information.
- Time-stamping using PTP.
- Packet Truncation beyond a specified number of bytes to discard the payload.
- Custom filtering of packets using User Defined Fields.
- Ability to adapt to changes in TAP/SPAN aggregate network states.
- End-to-end visibility.
- High Availability.
- Load Balancing.
- Manage multiple disjointed networks.
- Integration with ACI devices/ APIC and NX-OS devices.
- Real-time statistics for easy troubleshooting.
- Application management via IPv6.
- 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.

Platform-wise support of the additional features of the Cisco Nexus Data Broker:

Table 1: Supported Features

Feature Name	Cisco Nexus 9200 C92304QC, C92160YC	Cisco Nexus 9300(First Gen) C93128TX, C9396TX	Cisco Nexus 9300(EX, FX, FX2) C93180LC-EX, C93180YC-EX, C93108TC-EX, C93108TC-FX, C93180YC-FX, C9336C-FX2, C93240YC-FX2, C93360YC-FX2
Port Channel Load Balancing	Y	Y	Y
MPLS Stripping	Y	Y	Y
MPLS Stripping- Label	N	Y	N

Feature Name	Cisco Nexus 9200 C92304QC, C92160YC	Cisco Nexus 9300(First Gen) C93128TX, C9396TX	Cisco Nexus 9300(EX, FX, FX2) C93180LC-EX, C93180YC-EX, C93108TC-EX, C93108TC-FX, C93180YC-FX, C9336C-FX2, C93240YC-FX2, C93360YC-FX2
MPLS Filtering	N	N	N
sFlow	Y	Y	Y
PTP/ Timestamping	Y	N	Y
Jumbo MTU	Y	Y	Y
NetFlow	N	N	Y
Q-in-Q Tagging (for TAP and SPAN input ports)	N	Y	Y
Span Destination	Y	Y	Y
Timestamping	Y	N	Y
Packet Truncation	N	N	Y
Timestamping Strip	Y	N	Y
Input Port - TAP/ SPAN	Y	Y	Y
Local Monitoring Tool	Y	Y	Y
Remote Monitoring Tool with ERSPAN support	Y	Y	Y
Remote Source	Y	N	Y
UDF	Y	Y	Y
UDF v6	N	Y	Y
UDE	N	N	N
Drop ICMPv6	Y	N	Y

Table 2: Supported Features (contd)

Feature Name	Cisco Nexus 9500(EX, FX) C9504, C9508, C9516	Cisco Nexus 9364C, 9332C	Cisco Nexus 9300-GX 93600CD-GX 9364C-GX 9316D-GX
Port Channel Load Balancing	Y	Y	Y
MPLS Stripping	N	N	Y
MPLS Stripping- Label	N	N	N
MPLS Filtering	N	N	N
sFlow	Y	Y	Y
PTP/ Timestamping	Y	Y	Y
Jumbo MTU	Y	Y	Y
NetFlow	Y	N	Y
Q-in-Q Tagging (for TAP and SPAN input ports)	Y	Y	Y
Span Destination	Y	Y	Y
Timestamping	Y	Y	Y
Packet Truncation	Y	Y	Y
Timestamping Strip	Y	Y	Y
Input Port - TAP/ SPAN	Y	Y	Y
Local Monitoring Tool	Y	Y	Y
Remote Monitoring Tool with ERSPAN support	Y	Y	Y
Remote Source	Y	N	Y
UDF	Y	Y	Y
UDF v6	Y	Y	Y
UDE	Y	N	N
Drop ICMPv6	Y	Y	Y

Note The Cisco Nexus Series switches indicated in the above tables are recommended. For the supported NX-OS versions on the Nexus switches, see the Interoperability Matrix table in the Cisco Nexus Data Broker Release Notes, Release 3.10.

The following Cisco Nexus Series switches are also supported:

- Cisco Nexus 3000 Series switches—3048, 3064
- Cisco Nexus 3100 Series switches—3172, 3164, 31108TC-V, 31108PC-V, 3132C-Z
- Cisco Nexus 3200 Series switches— 3232
- Cisco Nexus 3500 Series switches

Limitations of Cisco Nexus Series switches:

Table 3: Limitations

Cisco Nexus Series Switch	Limitations
9364C-GX, 93600CD-GX,9316D-GX	• Range for QinQ VLAN on input ports is from 2 to 509. • QinQ VLANs cannot be added after configuring MPLS label strip.

Prerequisites for Cisco Nexus Series Switches

Cisco Nexus Data Broker is supported on Cisco Nexus 3000, 3100, 3200, 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 NX-API mode on the Cisco Nexus Series switches, see the following pre-requisites.

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

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

Device Models	NX-API Mode
Cisco Nexus 3000 Series switches	Enter the following commands at the prompt: • **# hardware profile tcam region qos 0** • **# hardware profile tcam region racl 0** • **# hardware profile tcam region vacl 0** • **# hardware profile tcam region ifacl 1024 double-wide** • **# hardware access-list tcam region mac-ifacl 512** • **#feature nxapi** • **#feature lldp**
Cisco Nexus 3132Q, 3164Q switches	Enter the following commands at the prompt: • **# hardware profile tcam region qos 0** • **# hardware profile tcam region racl 0** • **# hardware profile tcam region vacl 0** • **# hardware profile tcam region ifacl 1024 double-wide** • **# hardware access-list tcam region mac-ifacl 512** • **#feature nxapi** • **#feature lldp**
Cisco Nexus 3172 Series switches	Use the **hardware profile mode tap-aggregation** [**l2drop**] CLI command to enable tap aggregation and to reserve entries in the interface table that are needed for VLAN tagging. The l2drop option drops non-IP traffic ingress on tap interfaces.

Device Models	NX-API Mode
Cisco Nexus 3200 Series switches	Enter the following commands at the prompt: • **# hardware access-list tcam region e-racl 0** • **# hardware access-list tcam region span 0** • **# hardware access-list tcam region redirect 0** • **# hardware access-list tcam region vpc-convergence 0** • **# hardware access-list tcam region racl-lite 256** • **# hardware access-list tcam region l3qos-intra-lite 0** • **# hardware access-list tcam region ifacl 256 double-wide** • **# hardware access-list tcam region mac-ifacl 512** • **# hardware access-list tcam region ipv6-ifacl 256** • **#feature nxapi** • **#feature lldp**
Cisco Nexus 9300 Series switches	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**

Device Models	NX-API Mode
Cisco Nexus 9200, 9300-EX, 9336C-FX2, 93240YC-FX2, and N9K-C93360YC-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 (9504, 9508 and 9516)	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**

Device Models	NX-API Mode
Cisco Nexus 9300-GX 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**

Supported Web Browsers

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

- Firefox 85.0 and later versions.
- Chrome 88.0 and later versions.
- Microsoft Edge 88.0 and later versions.

Note If incompatible browsers are used, you may encounter GUI display issues for Release 3.10.

Note Enable JavaScript on your browser.

System Requirements

The following table lists the system requirements as per the deployment size for Cisco NDB:

Table 4: System Requirements per Deployment Size

Description	Small	Medium	Large
CPUs (virtual or physical)	6-core	12-core	18-core
Memory	8 GB RAM	16 GB RAM	24 GB RAM

Description	Small	Medium	Large
Hard disk	Minimum of 40 GB of free space available on the partition on which the Cisco Nexus Data Broker software is installed.		
Operating System	A recent 64-bit Linux distribution that supports Java, preferably Ubuntu, Fedora, or Red Hat.		
Other	Java Virtual Machine 1.8.		

Guidelines and Limitations

Cisco NDB runs in a Java Virtual Machine (JVM). As a Java-based application, Cisco NDB 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.
- 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.
- The following special characters are not allowed in description field for Port Definitions, Port Groups, Connections, Redirections, Monitoring Devices, and Service Nodes: Apostrophe (‘), Less Than (<), Greater Than (>), Double Quotation (“), Back Slash (\), Vertical Bar (|), and Question Mark (?).
- 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.
- 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.

Filename Matrix

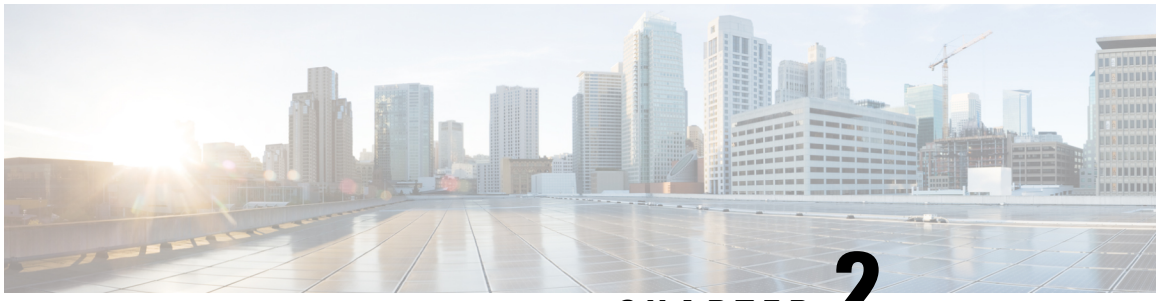
Filename Matrix for Cisco NDB:

Mode of Deployment	NXOS Image	Mode	File Name
Embedded	9.3(1) to 9.3(5)	NXAPI	`ndb1000-sw-app-emb-k9-`*`release-number`*`.zip`

Mode of Deployment	NXOS Image	Mode	File Name
Centralized	9.3(1) to 9.3(5)	NXAPI	`ndb1000-sw-app-k9-release-number.zip`

Interoperability Matrix

For the Interoperability Matrix, see the *Cisco Nexus Data Broker Release Notes, Release 3.10*.



CHAPTER 2

Managing TLS Certificate, KeyStore and TrustStore Files

This chapter has information and procedures for generating TLS Certificates and TrustStore files.

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:

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.

Step 1 Log in to the server.

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

Example:

```
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 Widgits Pty Ltd]:cisco
Organizational Unit Name (eg, section) []:insbu
Common Name (e.g. server FQDN or YOUR name) []:N9K-117.cisco.com
Email Address []:myname@cisco.com
```

Note If you have multiple switches, generate the certificate file and private key for each switch.

This command creates a certificate file (sw1-ca.pem) and a private key (sw1-ca.key).

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.

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 httpscrt 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-ndb-privatekey.pem
cp sw1-ca.pem sw1-ndb-cert.pem
```

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

Example:

```
docker@docker-virtual-machine:~/TLS$ cat sw1-ndb-privatekey.pem sw1-ndb-cert.pem > sw1-ndb.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-ndb.p12 -in sw1-ndb.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-ndb.p12 to a password protected Java KeyStore (tlsKeyStore) file using the **keytool** command. Use the jre/bin from the installed java directory.

Example:

```
docker@docker-virtual-machine:~/TLS$ ./(relativePath)/keytool -importkeystore -srckeystore sw1-ndb.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 enteries successfully imported, 0 enteries failed or cancelled.
```

Note By default an alias named "1" is stored in tlsKeyStore for the first switch. If the NDB controller is managing multiple switches, repeat this step for all the switches.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. Refer examples as shown below.

```
keytool -importkeystore -srckeystore sw2-ndb.p12 -srcstoretype pkcs12 -destkeystore
tlsKeyStore -deststoretype jks
keytool -importkeystore -srckeystore sw3-ndb.p12 -srcstoretype pkcs12 -destkeystore
tlsKeyStore -deststoretype jks
```

Step 12 List and verify content in the java tlsKeyStore using the **keytool** command.

Example:

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

What to do next

Proceed to the subsequent task, *Creating the TLS TrustStore File*.

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-ndb-cert.pem, sw2-ndb-cert.pem)

Step 1 Log in to the server.

Step 2 Convert the certificate file (For example, sw1-ndb-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. Use the jre/bin installed in the java directory.

Example:

```
docker@docker-virtual-machine:~/TLS$ ./(relativePath)/keytool -import -alias sw1 -file sw1-ndb-cert.pem
 -keystore tlsTrustStore -storetype jks
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)
```

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-ndb-cert.pem
-keystore tlsTrustStore
docker@docker-virtual-machine:~/TLS$ keytool -import -alias sw3 -file sw3-ndb-cert.pem
-keystore tlsTrustStore
// Here sw2 and sw3 are alias for switch 2 and switch 3 for identification purpose.
```

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:

Step 1 Log in to the NDB server.

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

Example:

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

Note When onboarding a device, ensure to provide the FQDN or IP address of the device, that was provided during the certificate generation for that device.

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

Example:

```
cp tlskeystore /root/ndb/configuration
cp tlsTrustStore /root/ndb/configuration
```

Step 4 Start the NDB application with TLS using the **runndb.sh** script.

Example:

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

Example:

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

```
./runndb.sh -osgiPasswordSync -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore
./configuration/tlsTrustStore
If ndb password is changed, OSGi webconsole password needs to be changed.
To set non-default OSGi webconsole password, enter ndb Admin Password [default]:
 (Type the non-default password which was set)
```

Note To disable TLS, run the **./runndb.sh -notls** command. To disable TLS and start NDB, run the **./runndb.sh -notls -start** command. Before disabling TLS, ensure to *stop* NDB. After TLS is disabled, the port number for the devices connected to the NDB server should be changed to 80.

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:

Step 1 Log in to the NDB server.

Step 2 Navigate to bin directory.

Example:

```
cd ndb/bin
```

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

Example:

```
./ndb config-keystore-passwords --user admin --password admin --url https://10.16.206.250:8443
--verbose --prompt --keystore-password cisco123 --truststore-password cisco123
Please enter your password: <enter the NDB GUI admin password>
```

In case NDB is configured with AAA (Tacacs/LDAP/Radius), and if the above command, **ndb config-keystore-passwords** fails, and you see a *401 unauthorized* error, then:

a. Go to `ndb` or `xnc` directory.

b. Stop the NDB server using `./runxnc.sh -stop`.

c. Enable the flag `enable.LocalUser.Authentication` by changing the value from *false* to *true* in the NDB **config.ini** file.

d. Start the ndb server using `./runxnc.sh -start`.

e. Run the **ndb config-keystore-passwords** command again.

Note In a HA environment, you need to run the above procedure for all the NDB servers in the cluster.

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
- Configuring TLS KeyStore and TrustStore Passwords on NDB

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.

Step 1 Log in to the server.

Step 2 Generate the private key (cert.key) and certificate signing request (cert.req) using openssl command.

Note If you have multiple switches, generate the certificate file and private key for each switch.

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:                          cisco123
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
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.

The cert.req file data needs to be submitted to 3rd party certification authority. Follow the relevant procedures and get the three (certificate) files.

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:

```
$cat N9K-117.cisco.com.cer test-root-ca-2048.cer test-ssl-ca.cer > server.cer
```

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 httpscrt 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:

Step 1 Create a TLS directory and navigate to it.

Example:

```
mkdir -p TLS
cd TLS
```

Step 2 Create three directories under *mypersonalca* and two prerequisite files.

Example:

```
mkdir -p mypersonalca/certs
mkdir -p mypersonalca/private
mkdir -p mypersonalca/crl
echo "01" > mypersonalca/serial
touch mypersonalca/index.txt
```

Generate the TLS private key and Certification Authority (CA) files for each switch connected to NDB using the command

Step 3 Generate the TLS private key and Certification Authority (CA) files for each switch connected to NDB using the **openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -out mypersonalca/certs/sw1-ca.pem -outform PEM -keyout mypersonalca/private/sw1-ca.key** command.

This step generates the TLS private key in PEM format with a key length of 2048 bits, and the CA file (mypersonalca/certs/sw1-ca.pem, mypersonalca/private/sw1-ca.key). If you have multiple switches then you need to create sw1-ca.pem and sw1-ca.key file for all the switches with the exact values that were provided when generating CSR for these switches.

Note Use the same inputs which were provided when generating cert.key in the *Obtaining Certificates from a Certification Authority* section. Any mismatch in the inputs will generate a new key.

Example:

```
docker@docker-virtual-machine:~/TLS$ openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -out
mypersonalca/certs/sw1-ca.pem -outform PEM -keyout mypersonalca/private/sw1-ca.key
Generating a 2048 bit RSA private key
...+++
.........................................+++
writing new private key to 'mypersonalca/private/sw1-ca.key'
-----
You are about to be asked to enter information that will be incorporated into your certificate
request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:SJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cisco
Organizational Unit Name (eg, section) []:insbu
Common Name (e.g. server FQDN or YOUR name) []:N9K-117.cisco.com
Email Address []:myname@cisco.com
```

Copy the cert.key and server.cer created in Obtaining Certificates from a Certification Authority section into the current directory (TLS). Select the certificate and key files for a single switch. These files were earlier generated for all the switches connecting to the controller. Using the server.cer and cert.key for the current switch, create the TLS KeyStore File.

Step 4 Copy the cert.key and server.cer created in the *Obtaining Certificates from a Certification Authority* section into the current directory (TLS). Select the certificate and key files for a single switch. These files were earlier generated for all the switches connecting to the controller. Using the server.cer and cert.key for the current switch, create the TLS KeyStore File.

If multiple switches are connected, repeat this step for each switch separately.

Step 5 Copy and convert the server.cer and cert.key files to .PEM format using the **copy** command.

Example:

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

Step 6 Concatenate the private key (sw1-ndb-privatekey.pem) and certificate file (sw1-ndb-cert.pem) into a single .PEM file using the **cat** command.

Example:

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

Step 7 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-ndb.pem file is converted to a password-protected sw1-ndb.p12 file.

Example:

```
docker@docker-virtual-machine:~/TLS$openssl pkcs12 -export -out sw1-ndb.p12 -in sw1-ndb.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 8 Convert the sw1-ndb.p12 to a password protected Java KeyStore (tlsKeyStore) file using the **keytool** command. This command converts the sw1-ndb.p12 file to a password-protected tlsKeyStore file.

Example:

```
docker@docker-virtual-machine:~/TLS$ keytool -importkeystore -srckeystore sw1-ndb.p12 -srcstoretype
 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. If the NDB controller is managing multiple switches, repeat this step for all the switches. 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. For example, see below.

```
keytool -importkeystore -srckeystore sw2-ndb.p12 -srcstoretype pkcs12 -destkeystore
tlsKeyStore -deststoretype jks
keytool -importkeystore -srckeystore sw3-ndb.p12 -srcstoretype pkcs12 -destkeystore
tlsKeyStore -deststoretype jks
```

Step 9 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 10 Convert the certificate file (sw1-ndb-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-ndb-cert.pem -keystore
tlsTrustStore -storetype jks
Enter keystore password: cisco123
Re-enter new password: cisco123
Owner: EMAILADDRESS=myname@cisco.com, CN=localhost, OU=insbu, O=cisco, L=SJ, ST=CA, C=US
Issuer: EMAILADDRESS=myname@cisco.com, CN=localhost, OU=insbu, O=cisco, L=SJ, ST=CA, C=US
Serial number: c557f668a0dd2ca5
Valid from: Thu Jun 15 05:43:48 IST 2017 until: Sun Jun 13 05:43:48 IST 2027
Certificate fingerprints:
MD5: C2:7B:9E:26:31:7A:74:25:55:DF:A7:91:C9:5D:20:A3
SHA1: 3C:DF:66:96:72:12:CE:81:DB:AB:58:30:60:E7:CC:04:4D:DF:6D:B2
SHA256:
DD:FB:3D:71:B4:B8:9E:CE:97:A3:E4:2D:D3:B6:90:CD:76:A8:5F:84:77:78:BE:49:6C:04:01:84:62:2C:2F:EB
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 0D B3 CF 81 66 4A 33 4E EF 86 7E 26 C3 50 9B 73 ....fJ3N...&.P.s
0010: 38 EF DF 40 8..@
]
]

#2: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:true
PathLen:2147483647
]
```

```
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 0D B3 CF 81 66 4A 33 4E EF 86 7E 26 C3 50 9B 73 ....fJ3N...&.P.s
0010: 38 EF DF 40 8..@
]
]

Trust this certificate? [no]: yes
Certificate was added to keystore
```

Note If 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-ndb-cert.pem -keystore tlsTrustStore
keytool -import -alias sw3 -file sw3-ndb-cert.pem -keystore tlsTrustStore
```

Step 11 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:

Step 1 Log in to the NDB server.

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

Example:

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

Note When onboarding a device, ensure to provide the FQDN or IP address of the device, that was provided during the certificate generation for that device.

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

Example:

```
cp tlskeystore /root/ndb/configuration
cp tlsTrustStore /root/ndb/configuration
```

Step 4 Start the NDB application with TLS using the **runndb.sh** script.

Example:

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

Example:

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

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

```
To set non-default OSGi webconsole password, enter ndb Admin Password [default]:
 (Type the non-default password which was set)
```

Note To disable TLS, run the **./runndb.sh -notls** command. To disable TLS and start NDB, run the **./runndb.sh -notls -start** command. Before disabling TLS, ensure to *stop* NDB. After TLS is disabled, the port number for the devices connected to the NDB server should be changed to 80.

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:

Step 1 Log in to the NDB server.

Step 2 Navigate to bin directory.

Example:

```
cd ndb/bin
```

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

Example:

```
./ndb config-keystore-passwords --user admin --password admin --url https://10.16.206.250:8443
--verbose --prompt --keystore-password cisco123 --truststore-password cisco123
Please enter your password: <enter the NDB GUI admin password>
```

In case NDB is configured with AAA (Tacacs/LDAP/Radius), and if the above command, **ndb config-keystore-passwords** fails, and you see a *401 unauthorized* error, then:

a. Go to `ndb` or `xnc` directory.

b. Stop the NDB server using `./runxnc.sh -stop`.

c. Enable the flag `enable.LocalUser.Authentication` by changing the value from *false* to *true* in the NDB **config.ini** file.

d. Start the ndb server using `./runxnc.sh -start`.

e. Run the **ndb config-keystore-passwords** command again.

Note In a HA environment, you need to run the above procedure for all the NDB servers in the cluster.

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 WebUI Browser and NDB Server

You can secure communication between a Web browser and NDB server running in centralized mode using self-signed certificates. This section describes how to generate a self-signed certificate to secure communication between a WebUI browser and NDB application. By default Cisco NDB is shipped with default certificate which is issued to Cisco NDB and issued by Cisco NDB with default validity. You can use the **generateWebUIcertificate.sh** script under configuration folder to create self-signed certificates. For Cisco NDB releases 3.5 and earlier, these certificates are valid for 6 months. Starting with Cisco NDB release 3.6, default validity of a certificate is 6 months but you can configure the validity of a certificate.

Note You can create self-signed TLS certificates for NDB in Centralized mode only.

- Generating TLS Self-Signed Certification Between WebUI Browser and NDB Server Running in Centralized Mode

Generating TLS Self-Signed Certification Between WebUI Browser and NDB Server Running in Centralized Environment

Complete the following steps to generate TLS self-signed certification between WebUI Browser and NDB Server running in Centralized mode:

Step 1 Log into the NDB server and change the current directory `\ndb\configuration`.

Example:

```
[root@RHEL-VM-NDB-ACI]# cd \ndb\configuration
```

Step 2 Generate the TLS self-signed certificate using the **generateWebUIcertificate.sh** script.

Example:

```
[root@RHEL-VM-NDB-ACI configuration]# ./generateWebUIcertificate.sh

**********************************
Entor Fully qualified domain name :
**********************************
NDB-browser 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 :
***************
cisco123
*****************
Enter storepass :
******************
cisco123
************************************
Enter the validity in number of days :
************************************
365  in NDB 3.5 this script will let you to specify the certificate validity.
*************************************************************************************************************************
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 6, 2019
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Issuer: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Serial number: b404be5
Valid from: Sun Jan 06 20:22:05 PST 2019 until: Mon Jan 06 20:22:05 PST 2020
Certificate fingerprints:
         MD5:  71:07:F6:4E:57:6A:08:3A:AD:06:32:B3:6C:5F:8F:52
         SHA1: 04:08:B9:D5:B7:EB:ED:E0:F9:22:49:14:FA:C6:09:39:22:32:43:A2
         SHA256:
34:D9:EB:34:0A:52:D1:4A:DD:F1:8B:14:D0:84:E4:1C:57:8B:2B:99:9B:E5:A1:4C:C7:8C:CD:AE:24:31:49:75

         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:
```

```
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 63 8A 92 8F 6F 0F 45 BD   EE 55 C5 A8 99 3B F6 F7  c...o.E..U...;..
0010: AC FA 4A 21                                        ..J!
]
]

*******************************
Displayed the generated keystore
*******************************
************************************************
Configured the keystore details on tomcat-server.xml
************************************************
*********************************************************************************************
The newly generated key will used on next NDB restart. Do you want to restart NDB
 now (y/n) ?
*********************************************************************************************
y
Doesn't seem any Controller daemon is currently running
Running controller in background with PID: 13573, to connect to it please SSH to
 this host on port 2400
NDB GUI can be accessed using below URL:
[https://10.16.206.160:8443]
[https://[fe80::250:56ff:fe90:b764]:8443]
[https://10.16.206.159:8443]
[https://192.168.1.123:8443]
[https://[fe80::250:56ff:fe90:9c79]:8443]

*************
NDB Restarted
*************
```

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

Step 3 Decode the generated certificate using the **keytool -list -v -keystore keystore_Name** command. Enter the store password when prompted.

Example:

```
[root@RHEL-VM-NDB-ACI configuration]# keytool -list -v -keystore keystore
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: cisco
Creation date: Jul 6, 2019
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Issuer: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
```

```
Serial number: b404be5
Valid from: Sun Jan 06 20:22:05 PST 2019 until: Mon Jan 06 20:22:05 PST 2020
Certificate fingerprints:
         MD5:  71:07:F6:4E:57:6A:08:3A:AD:06:32:B3:6C:5F:8F:52
         SHA1: 04:08:B9:D5:B7:EB:ED:E0:F9:22:49:14:FA:C6:09:39:22:32:43:A2
         SHA256:
34:D9:EB:34:0A:52:D1:4A:DD:F1:8B:14:D0:84:E4:1C:57:8B:2B:99:9B:E5:A1:4C:C7:8C:CD:AE:24:31:49:75
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 63 8A 92 8F 6F 0F 45 BD   EE 55 C5 A8 99 3B F6 F7  c...o.E..U...;..
0010: AC FA 4A 21                                        ..J!
]
]

*******************************************
*******************************************
```

Step 4 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. Convert JKS format certificate into PKCS12 format using the **keytool** command.

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

Example:

```
keytool -importkeystore -srckeystore keystore -srcstorepass cisco123 -srckeypass cisco123 -destkeystore
keystore.p12 -deststoretype PKCS12 -srcalias cisco -deststorepass cisco123 -destkeypass cisco123
```

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

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

Step 5 Add this certificate to Trusted Root certificate store on the browser. See help for respective Web browsers about how to add the certificate to the Trusted Root certificate store.

Generating TLS Self-Signed Certificate Between Web Browser and NDB Server Running in Embedded Mode Using Guest Shell Environment

To generate TLS self-signed certificate between Web browser and NDB server running in embedded mode using Guest Shell environment, complete the following steps.

Step 1 Connect to Guest Shell using **guestshell** command.

Example:

```
N9K-C93108TC-EX-108# guestshell
[admin@guestshell ~]$
[admin@guestshell ~]$
```

Step 2 Change the current directory to `\ndb\configuration`.

Example:

```
[admin@guestshell ~]$ cd \ndb\configuration
```

Step 3 Generate the TLS self-signed certificate using the `/home/admin/ndb/configuration/generateWebUIcertificate.sh` script.

Example:

```
[root@RHEL-VM-NDB-ACI configuration]# ./generateWebUIcertificate.sh

**********************************
Entor Fully qualified domain name :
**********************************
NDB-browser 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 :
***************
cisco123
*****************
Enter storepass :
*****************
cisco123
************************************
Enter the validity in number of days :
************************************
365  in NDB 3.5 this script will let you to specify the certificate validity.
************************************************************************************************************************
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 6, 2019
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Issuer: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Serial number: b404be5
Valid from: Sun Jan 06 20:22:05 PST 2019 until: Mon Jan 06 20:22:05 PST 2020
Certificate fingerprints:
         MD5:  71:07:F6:4E:57:6A:08:3A:AD:06:32:B3:6C:5F:8F:52
         SHA1: 04:08:B9:D5:B7:EB:ED:E0:F9:22:49:14:FA:C6:09:39:22:32:43:A2
         SHA256:
34:D9:EB:34:0A:52:D1:4A:DD:F1:8B:14:D0:84:E4:1C:57:8B:2B:99:9B:E5:A1:4C:C7:8C:CD:AE:24:31:49:75

         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 63 8A 92 8F 6F 0F 45 BD   EE 55 C5 A8 99 3B F6 F7  c...o.E..U...;..
0010: AC FA 4A 21                                        ..J!
]
]

*******************************
Displayed the generated keystore
*******************************
*************************************************
Configured the keystore details on jetty-ssl-context.xml
*************************************************
*************************************************************************************************
The newly generated key will used on next NDB restart. Do you want to restart NDB
 now (y/n) ?
*************************************************************************************************
n
*************
The newly generated key will be used on the next NDB restart.
*************
```

Note Manually reboot guestshell using the **guestshell reboot** command to ensure that the browser starts using this certificate when you access NDB java application from the browser.

Step 4 Decode the generated certificate using the **keytool -list -v -keystore keystore_Name** command. Enter the store password when prompted.

Example:

```
[root@RHEL-VM-NDB-ACI configuration]#  keytool -list -v -keystore keystore
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: cisco
Creation date: Jul 6, 2019
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Issuer: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Serial number: b404be5
Valid from: Sun Jan 06 20:22:05 PST 2019 until: Mon Jan 06 20:22:05 PST 2020
Certificate fingerprints:
         MD5:  71:07:F6:4E:57:6A:08:3A:AD:06:32:B3:6C:5F:8F:52
         SHA1: 04:08:B9:D5:B7:EB:ED:E0:F9:22:49:14:FA:C6:09:39:22:32:43:A2
         SHA256:
34:D9:EB:34:0A:52:D1:4A:DD:F1:8B:14:D0:84:E4:1C:57:8B:2B:99:9B:E5:A1:4C:C7:8C:CD:AE:24:31:49:75
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 63 8A 92 8F 6F 0F 45 BD   EE 55 C5 A8 99 3B F6 F7  c...o.E..U...;..
0010: AC FA 4A 21                                        ..J!
]
]

*******************************************
*******************************************
```

Step 5 The self-signed certificates are generated in JKS format which is not compatible with the browsers. 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. Convert JKS format certificate into PKCS12 format using the **keytool** command.

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

Example:

```
keytool -importkeystore -srckeystore keystore -srcstorepass cisco123 -srckeypass cisco123 -destkeystore
keystore.p12 -deststoretype PKCS12 -srcalias cisco -deststorepass cisco123 -destkeypass cisco123
```

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

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

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. Use the password that you created while creating the certificate when prompted while uploading the certificate to the Web browser.

Step 7 Restart the Guest Shell to restart the NDB.

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

You can secure communication between a Web browser and NDB server running in centralized mode. This section describes how to generate CA certificates, convert the certificates into JKS format, and upload the certificates into a Web browser. To generate a CA certificate, you need to generate a Certificate Signing Request (CSR) and send it to a Certificate issuing authority (CA). You can use an open source tool to generate a CSR.

- Generating TLS 3rd Party Certification Between WebUI Browser and NDB Server Running in Centralized Mode

Generating TLS 3rd Party Certification Between WebUI Browser and NDB Server Running in Centralized Mode

Complete these steps to generate TLS 3rd party certification between WebUI browser and NDB server running in centralized mode:

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

Example:

```
[root@NDB-server ~]# openssl req -newkey rsa:2048 -sha256 -keyout ndb-server.key -keyform PEM -out
 ndb-server.req -outform PEM
Generating a 2048 bit RSA private key
...+++
.....................................................+++
writing new private key to 'ndb-server.key'
Enter PEM pass phrase:  cisco123
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) []:ndb-server.cisco.com
Email Address []:chburra@cisco.com

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


[root@NDB-server ~]# ls
ndb-server.req   ndb-server.key
```

Note The ndb-server.req (CSR) file is submitted to the certificate issuing authority (CA).

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:

```
[root@NDB-server ~]# openssl req -noout -text -in ndb-server.req
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, ST=CA, L=SJ, O=cisco, OU=insbu,
CN=ndb-server.cisco.com/emailAddress=chburra@cisco.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b5:30:75:e8:c8:5f:05:3b:0e:4f:aa:00:d9:64:
                    8d:bf:b2:80:20:56:c3:be:b0:4c:e0:52:e5:be:d8:
                    d2:74:85:4e:8a:ba:d3:1e:30:76:bf:e5:de:7d:51:
                    11:79:8e:bc:96:38:7a:23:5a:26:31:50:50:fa:29:
                    44:ab:56:b6:0d:41:38:ba:d1:d5:b4:e3:ba:a3:6c:
                    4a:35:73:27:d9:fd:5c:4b:21:85:1a:f9:4d:b0:9e:
                    f3:ae:ce:49:98:ef:a2:f8:11:ab:bd:7e:64:ee:68:
                    68:19:6e:8f:3c:54:30:0f:28:01:13:b0:3d:34:b8:
                    f9:f5:cc:4a:84:d8:e5:d2:27:47:cc:83:76:92:ad:
                    92:62:f3:a3:35:be:14:ce:38:af:2a:c5:2e:fa:b8:
                    31:6b:71:cd:56:00:1f:0d:cc:b0:f8:fc:b0:52:91:
                    f8:9c:cf:45:13:c9:b5:86:fa:30:dd:88:78:01:15:
                    fb:5c:c9:6f:5b:b7:80:28:6c:86:54:c0:f2:5f:35:
                    70:82:49:5c:79:1c:f2:23:dd:50:d5:47:12:37:a3:
                    3f:f9:1d:90:8f:c0:e8:18:09:2e:66:8d:c3:72:17:
                    7f:7d:27:da:b1:cc:26:2d:8c:6b:ee:c5:e8:b5:78:
                    31:7c:bb:ba:6d:2c:e5:a3:29:7e:c1:4a:93:19:ed:
                    9a:e7
                Exponent: 65537 (0x10001)
        Attributes:
```

```
        unstructuredName         :cisco123
        challengePassword        :cisco123
Signature Algorithm: sha256WithRSAEncryption
    9c:9a:51:e0:1d:e4:0b:8f:c1:c6:f5:e0:d2:f6:30:0e:18:af:
    a7:b2:a4:4a:57:d7:07:44:cd:9c:fa:2d:0e:8b:c9:31:5b:16:
    6b:84:42:0b:ed:06:5c:ed:30:d8:9b:ee:5d:79:f4:8a:e3:52:
    3c:b3:4a:eb:6c:22:a2:f4:35:80:28:3a:67:62:7f:5f:dc:80:
    e0:74:f0:3c:39:26:39:3a:76:6a:6a:98:e9:68:f9:b7:58:bf:
    e7:44:2e:e7:73:0a:9c:62:28:b2:c6:09:41:81:b2:53:46:14:
    e6:e4:dc:ca:90:81:5a:5e:dc:1b:dc:36:2c:86:5f:37:29:4c:
    b0:ee:85:2b:34:f2:82:8a:d4:fc:a0:ce:10:e4:44:4e:d0:7a:
    37:6d:3e:f9:ff:a1:19:8c:db:06:bf:be:87:57:a1:cb:05:15:
    0b:9f:6c:8b:c2:ad:22:25:10:f0:4d:0f:4d:b7:be:71:87:f7:
    85:24:e7:2d:f9:59:86:1a:b7:88:57:16:93:31:1f:d7:e5:07:
    42:77:00:f9:ac:44:3b:6c:35:0f:80:5d:00:6f:ea:be:fe:e7:
    28:53:0c:6b:5f:0c:76:bf:8c:a7:60:57:63:05:06:ff:ac:3d:
    f1:63:54:d0:d0:13:44:b1:e9:53:6b:32:11:e2:83:26:04:f5:
    23:67:6b:de
```

Step 3 The private key, ndb-server.key, is secured with the passphrase. You need to unencrypt the certificate private key. Unencrypt the private key using the **openssl rsa** command.

Example:

```
[root@NDB-server ~]# cp ndb-server.key  ndb-server.keybkp
[root@NDB-server ~]# rm ndb-server.key
 [root@NDB-server ~]# openssl rsa -in ndb-server.keybkp -out ndb-server.key
Enter pass phrase for ndb-server.keybkp: cisco123
writing RSA key
```

Note The ndb-server.req file data needs to be submitted to 3rd party certification authority. Follow the relevant procedures and get the certificate files.

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: qvrca2.cer (root), hydsslg2.cer (intermediate), ndb-server.cisco.com-39891.cer (domain).

Certificates are mostly shared in .PEM file format.

Step 4 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 certificate root certificate intermediate certificate > ndb-server.cer*.

Example:

```
[root@NDB-server ~]# cat ndb-server.cisco.com-39891.cer qvrca.cer hydsslg2.cer > ndb-server.cer
```

Step 5 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-----
```

Step 6 Create the TLS NDB Server Keystore file using the ndb-server.cer and ndb-server.key files. Copy the files to switch using the copy command.

Example:

```
cp ndb-server.key ndb-server-ndb-privatekey.pem
      cp ndb-server.cer ndb-server-ndb-cert.pem
```

Step 7 Combine the private key and certificate file into a single .PEM file using the cat command.

Example:

```
cat ndb-server-ndb-privatekey.pem  ndb-server-ndb-cert.pem > ndb-server-ndb.pem
```

Step 8 CA provides certificates in PEM format and extension of the certificate is .pem. You need to convert the PEM format certificate to PKCS12 format. Convert the PEM file, ndb-server-ndb.pem, to .P12 file format using the **openssl pkcs12** command. Enter the export password when prompted. The password must contain at least 6 characters, for example, cisco123. The ndb-server-ndb.pem file is converted to a password-protected ndb-server-ndb.p12 file.

Example:

```
[root@NDB-server ~]# openssl pkcs12 -export -out ndb-server-ndb.p12 -in ndb-server-ndb.pem
Enter Export Password:□cisco123
Verifying - Enter Export Password:□cisco123
```

Step 9 Convert the ndb-server-ndb.p12 to a password protected Java KeyStore (ndb-server-keystore) file using the **keytool** command. This command converts the sw1-ndb.p12 file to a password-protected ndb-server-keystore file. Create a new password for the destination JKS store and enter the source keystore password when prompted.

Example:

```
[root@NDB-server ~]# .(relativePath)/keytool -importkeystore -srckeystore ndb-server-ndb.p12
-srcstoretype pkcs12 -destkeystore ndb-server-keystore -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
[root@NDB-server ~]#
```

Step 10 List and verify content in the java tlsKeyStore using the **keytool** command.

Example:

```
[root@NDB-server ~]#.(relativePath)/keytool -list -v -keystore ndb-server-keystore
```

Step 11 Copy the ndb-server-keystore file to the */ndb/configuration* folder.

Step 12 Configure `jetty-ssl-context.xml` (stored in */ndb/configuration/*etc) with key store password that was provided while generating the certificate. You can use VI editor and edit the following lines with KeyStorePath, KeyStorePassword, TrustStorePath, TrustStorePassword.

Example:

```
<Set name="KeyStorePath"><Property name="jetty.base" default="." />/<Property
name="jetty.sslContext.keyStorePath" deprecated="jetty.keystore"
default="configuration/ndb-server-keystore"/></Set>
<Set name="KeyStorePassword"><Property name="jetty.sslContext.keyStorePassword"
deprecated="jetty.keystore.password" default="cisco123"/></Set>
```

```
<Set name="KeyManagerPassword"><Property name="jetty.sslContext.keyManagerPassword"
deprecated="jetty.keymanager.password" default="cisco123"/></Set>
<Set name="TrustStorePath"><Property name="jetty.base" default="." />/<Property
name="jetty.sslContext.trustStorePath" deprecated="jetty.truststore"
default="configuration/ndb-server-keystore"/></Set>

<Set name="TrustStorePassword"><Property name="jetty.sslContext.trustStorePassword"
deprecated="jetty.truststore.password" default="cisco123"/></Set>
```

Step 13 Restart the NDB.

Step 14 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. Use the password that you created while creating the certificate when prompted while uploading the certificate to the Web browser.

Generating TLS 3rd Party Certificate Between Web Browser and NDB Server Running in Embedded Mode Using Guest Shell Environment

To generate TLS 3rd party certificate between Web browser and NDB server running in embedded mode using guest shell environment, complete the following steps.

Step 1 Enable bash-shell feature on the switch using the feature command.

Example:

```
N9396TX-116(config)# feature bash-shell
```

Step 2 Enter bash-shell mode on the switch using the run command.

Example:

```
N9396TX-116(config)# run bash
bash-4.2$
```

Step 3 Generate Certificate Signing Request (CSR) using the **openssl req** command. Enter the required information when prompted.

Example:

```
bash-4.2$ openssl req -newkey rsa:2048 -sha256 -keyout ndb-server.key -keyform PEM -out ndb-server.req
 -outform PEM
Generating a 2048 bit RSA private key
...+++
.............................................+++
writing new private key to 'ndb-server.key'
Enter PEM pass phrase:  cisco123
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) []:ndb-server.cisco.com
Email Address []:chburra@cisco.com

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



bash-4.2$ ls

ndb-server.req   ndb-server.key
```

Note The openssl command creates a privsate key, ndb-server.key, and a certificate signing request file, ndb-server.req. The ndb-server.req (CSR) file is submitted to the certificate issuing authority (CA).

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 4 To view the content or verify the CSR request, use the **openssl req** command.

Example:

```
bash-4.2$ openssl req -noout -text -in ndb-server.req
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, ST=CA, L=SJ, O=cisco, OU=insbu,
CN=ndb-server.cisco.com/emailAddress=chburra@cisco.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b5:30:75:e8:c8:5f:05:3b:0e:4f:aa:00:d9:64:
                    8d:bf:b2:80:20:56:c3:be:b0:4c:e0:52:e5:be:d8:
                    d2:74:85:4e:8a:ba:d3:1e:30:76:bf:e5:de:7d:51:
                    11:79:8e:bc:96:38:7a:23:5a:26:31:50:50:fa:29:
                    44:ab:56:b6:0d:41:38:ba:d1:d5:b4:e3:ba:a3:6c:
                    4a:35:73:27:d9:fd:5c:4b:21:85:1a:f9:4d:b0:9e:
                    f3:ae:ce:49:98:ef:a2:f8:11:ab:bd:7e:64:ee:68:
                    68:19:6e:8f:3c:54:30:0f:28:01:13:b0:3d:34:b8:
                    f9:f5:cc:4a:84:d8:e5:d2:27:47:cc:83:76:92:ad:
                    92:62:f3:a3:35:be:14:ce:38:af:2a:c5:2e:fa:b8:
                    31:6b:71:cd:56:00:1f:0d:cc:b0:f8:fc:b0:52:91:
                    f8:9c:cf:45:13:c9:b5:86:fa:30:dd:88:78:01:15:
                    fb:5c:c9:6f:5b:b7:80:28:6c:86:54:c0:f2:5f:35:
                    70:82:49:5c:79:1c:f2:23:dd:50:d5:47:12:37:a3:
                    3f:f9:1d:90:8f:c0:e8:18:09:2e:66:8d:c3:72:17:
                    7f:7d:27:da:b1:cc:26:2d:8c:6b:ee:c5:e8:b5:78:
                    31:7c:bb:ba:6d:2c:e5:a3:29:7e:c1:4a:93:19:ed:
                    9a:e7
                Exponent: 65537 (0x10001)
        Attributes:
            unstructuredName         :cisco123
            challengePassword        :cisco123
    Signature Algorithm: sha256WithRSAEncryption
        9c:9a:51:e0:1d:e4:0b:8f:c1:c6:f5:e0:d2:f6:30:0e:18:af:
        a7:b2:a4:4a:57:d7:07:44:cd:9c:fa:2d:0e:8b:c9:31:5b:16:
        6b:84:42:0b:ed:06:5c:ed:30:d8:9b:ee:5d:79:f4:8a:e3:52:
```

```
3c:b3:4a:eb:6c:22:a2:f4:35:80:28:3a:67:62:7f:5f:dc:80:
e0:74:f0:3c:39:26:39:3a:76:6a:6a:98:e9:68:f9:b7:58:bf:
e7:44:2e:e7:73:0a:9c:62:28:b2:c6:09:41:81:b2:53:46:14:
e6:e4:dc:ca:90:81:5a:5e:dc:1b:dc:36:2c:86:5f:37:29:4c:
b0:ee:85:2b:34:f2:82:8a:d4:fc:a0:ce:10:e4:44:4e:d0:7a:
37:6d:3e:f9:ff:a1:19:8c:db:06:bf:be:87:57:a1:cb:05:15:
0b:9f:6c:8b:c2:ad:22:25:10:f0:4d:0f:4d:b7:be:71:87:f7:
85:24:e7:2d:f9:59:86:1a:b7:88:57:16:93:31:1f:d7:e5:07:
42:77:00:f9:ac:44:3b:6c:35:0f:80:5d:00:6f:ea:be:fe:e7:
28:53:0c:6b:5f:0c:76:bf:8c:a7:60:57:63:05:06:ff:ac:3d:
f1:63:54:d0:d0:13:44:b1:e9:53:6b:32:11:e2:83:26:04:f5:
23:67:6b:de
```

Step 5 The private key, ndb-server.key, is secured with the passphrase. You need to unencrypt the certificate private key. Unencrypt the private key using the **openssl rsa** command.

Example:

```
bash-4.2$ cp ndb-server.key  ndb-server.keybkp
bash-4.2$ rm ndb-server.key
bash-4.2$ openssl rsa -in ndb-server.keybkp -out ndb-server.key
Enter pass phrase for ndb-server.keybkp: cisco123
writing RSA key
```

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: qvrca2.cer (root), hydsslg2.cer (intermediate), ndb-server.cisco.com-39891.cer (domain).

Certificates are mostly shared in .PEM file format.

Step 6 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 certificate root certificate intermediate certificate > ndb-server.cer*.

Example:

```
bash-4.2$ cat ndb-server.cisco.com-39891.cer qvrca.cer hydsslg2.cer > ndb-server.cer
```

Step 7 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-----
```

Step 8 Create the TLS NDB Server Keystore file using the ndb-server.cer and ndb-server.key files. Copy the files to switch using the **copy** command.

Example:

```
cp ndb-server.key ndb-server-ndb-privatekey.pem
      cp ndb-server.cer ndb-server-ndb-cert.pem
```

Step 9 Combine the private key and certificate file into a single .PEM file using the **cat** command.

Example:

```
cat ndb-server-ndb-privatekey.pem  ndb-server-ndb-cert.pem > ndb-server-ndb.pem
```

Step 10 CA provides certificates in PEM format and extension of the certificate is .pem. You need to convert the PEM format certificate to PKCS12 format. Convert the PEM file, ndb-server-ndb.pem, to .P12 file format using the **openssl pkcs12** command. Enter the export password when prompted. The password must contain at least 6 characters, for example, cisco123. The ndb-server-ndb.pem file is converted to a password-protected ndb-server-ndb.p12 file.

Example:

```
bash-4.2$ openssl pkcs12 -export -out ndb-server-ndb.p12 -in ndb-server-ndb.pem
Enter Export Password:cisco123
Verifying - Enter Export Password:cisco123
```

Step 11 Copy the certificate file to the NDB configuration folder.

Example:

```
bash-4.2$ sudo cp ndb-server-ndb.p12
/isan/vdc_1/virtual-instance/guestshell+/rootfs/usr/bin/ndb/configuration/
```

Step 12 Exit the bash shell mode using the **exit** command.

Example:

```
bash-4.2$ exit
exit
N9396TX-116#
```

Step 13 Connect to guest shell using guestshell command.

Example:

```
N9396TX-116# guestshell
[admin@guestshell ~]$
```

Step 14 Change current directory to `ndb/configuration`.

Example:

```
[admin@guestshell ~]$ cd ndb/configuration
```

Step 15 Convert the ndb-server-ndb.p12 to a password protected Java KeyStore (ndb-server-keystore) file using the **keytool** command. This command converts the ndb-server-ndb.p12 file to a password-protected ndb-server-keystore file. Create a new password for the destination JKS store and enter the source keystore password when prompted.

Example:

```
[admin@guestshell configuration]$ keytool -importkeystore -srckeystore ndb-server-ndb.p12
-srcstoretype pkcs12 -destkeystore ndb-server-keystore -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
```

Step 16 List and verify content in the java tlsKeyStore using the **keytool** command.

Example:

```
[admin@guestshell configuration]$ keytool -list -v -keystore ndb-server-keystore
```

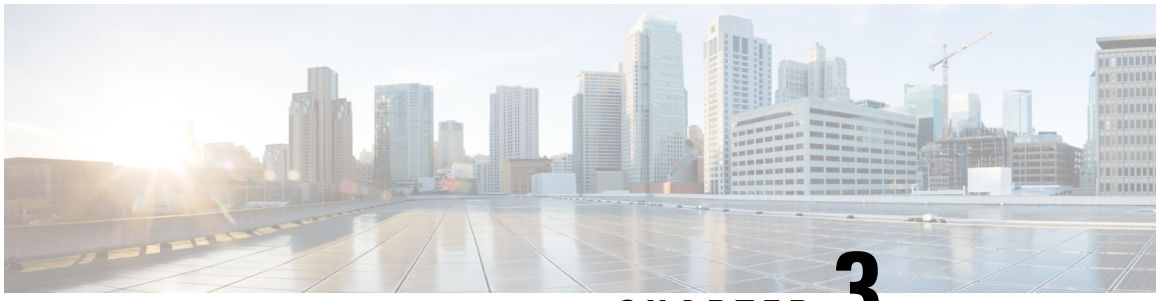
Step 17 Configure `jetty-ssl-context.xml` (stored in ndb/etc folder) with key store password that was provided while generating the certificate. You can use VI editor and edit the following lines with keystore and keystorepass.

Example:

```
<Set name="KeyStorePath"><Property name="jetty.base" default="." />/<Property
name="jetty.sslContext.keyStorePath" deprecated="jetty.keystore"
default="configuration/ndb-server-keystore"/></Set>
<Set name="KeyStorePassword"><Property name="jetty.sslContext.keyStorePassword"
deprecated="jetty.keystore.password" default="cisco123"/></Set>

<Set name="KeyManagerPassword"><Property name="jetty.sslContext.keyManagerPassword"
deprecated="jetty.keymanager.password" default="cisco123"/></Set>

<Set name="TrustStorePath"><Property name="jetty.base" default="." />/<Property
name="jetty.sslContext.trustStorePath" deprecated="jetty.truststore"
default="configuration/ndb-server-keystore"/></Set>

<Set name="TrustStorePassword"><Property name="jetty.sslContext.trustStorePassword"
deprecated="jetty.truststore.password" default="cisco123"/></Set>
```

Step 18 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. Use the password that you created while creating the certificate when prompted while uploading the certificate to the Web browser.

Step 19 Restart NDB.



CHAPTER 3

Configuring Cisco Nexus 9000 Series Switches

This chapter contains the following sections:

Guidelines and Limitations for Cisco Nexus 9000 Series Switches

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 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 9200 Series switches do not support Q-in-Q VLAN tagging for the Edge SPAN and Edge TAP port.
- 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.
- 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.
  - Enable NX-API feature in the switch using the **feature nxapi** command.
  - Configure **switchport mode trunk** on all the inter-switch ports and the port-channels.
- Cisco Nexus data broker periodically rediscovers the switch inventory, the topology interconnection, and the status. This information is updated in the GUI depending on the status. The rediscovery interval can be configured and the default value for the rediscovery interval is every 10 seconds.

Configuring TCAM Hardware Sizing on Cisco Nexus 9000 Series Switches

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

SUMMARY STEPS

1. Use the **hardware access-list tcam region <region> <tcam-size>** command to configure the following TCAM regions:

DETAILED STEPS

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

	Command or Action	Purpose
		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 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

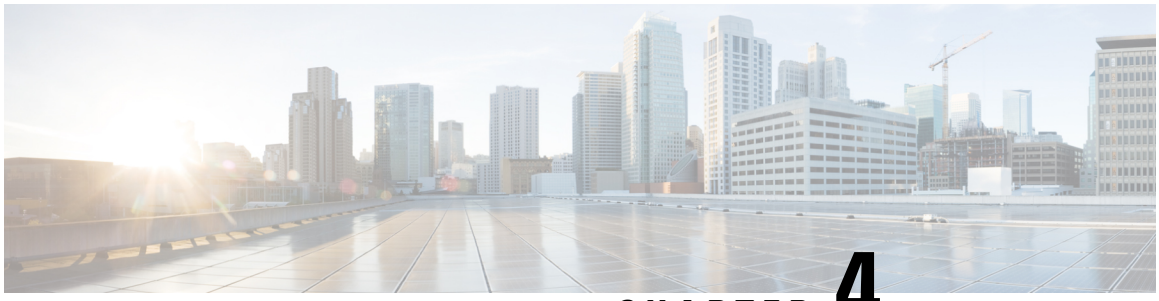
	Command or Action	Purpose
Step 1	Enable the management interface.	Enable the management interface on the switch.
Step 2	switch# **conf t**	Enter the configuration mode.
Step 3	switch (config) # **feature nxapi**	Enable the NX-API feature.
Step 4	switch (config) # **nxapi http port** *80*	Configure the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

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

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

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **config t**	Enables the configuration mode.
Step 2	switch(config)# interface {{**type** *slot*/*port*} | {*port-channel number*}}	Specifies an interface to configure.
Step 3	switch(config-if)# **switchport mode** {*access* | *trunk*}	Configures the switchport mode as access or trunk on the inter-switch ports and the port-channels.
Step 4	switch(config)# **exit**	Exits the configuration mode.



CHAPTER 4

Logging in and Managing the Cisco Nexus Data Broker

This chapter has details about logging in and managing the Cisco NDB and overview of the new GUI.

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 5: Cluster Operation Status

Cluster Indicator	Cluster Status	Recommendation
Green	Operational	
Yellow	Some of the cluster nodes are not available	Do not make any changes or add to the existing NDB configuration.

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

Before you begin

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

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

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

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

Step 4 Locate the following text:

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

Step 5 **Example:**

IPv4 example.

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

Example:

IPv6 example.

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

Step 6 Save the file and exit the editor.

What to do next

(Optional) Use this procedure to configure the delay time for a node and the number of retries.

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

2. Navigate to the configuration directory.
3. Use any text editor to open the `xncjgroups.xml`file.
4. Locate the following text:

   ```
   FD timeout="3000" max_tries="3"/
   ```

5. Modify the *Latency Time* value and *maximum_tries* value.
6. Save the file and exit the editor.
7. Repeat the above steps for all the instances of the cluster.

Password Protecting High Availability Clusters

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

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

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

Step 4 Locate the following text:

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

Step 5 Remove the comments from the AUTH line.

Example:

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

Step 6 (Optional) Change the password in the auth_value attribute.

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

Step 7 Save the file and exit the editor.

Logging in to Cisco Nexus Data Broker GUI

You can login to the Cisco Nexus Data Broher GUI using HTTPS. The default HTTPS web link for the Cisco NDB GUI is `https://Nexus_Data_Broker_IP:8443/monitor`.

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

Step 1 In your web browser, enter the Cisco NDB 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 **LOGIN**.

Changing Controller Access

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.

To change the controller access to HTTP, complete the following steps:

Before you begin

Cisco Nexus Data Broker is shipped with a certificate for the HTTPS connection between the Cisco Nexus Data Broker and a browser. You can change to a different certificate.

The script **generateWebUIcertificate.sh** is available in the **ndb/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.

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

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

Step 2 Restart the controller.

Cisco Nexus Data Broker GUI Overview

The Cisco Nexus Data Broker GUI contains the following tabs and each of these tabs are discussed in detail (as separate chapters) in the subsequent pages of this guide.

- Dashboard
- Topology
- Devices
- Connections

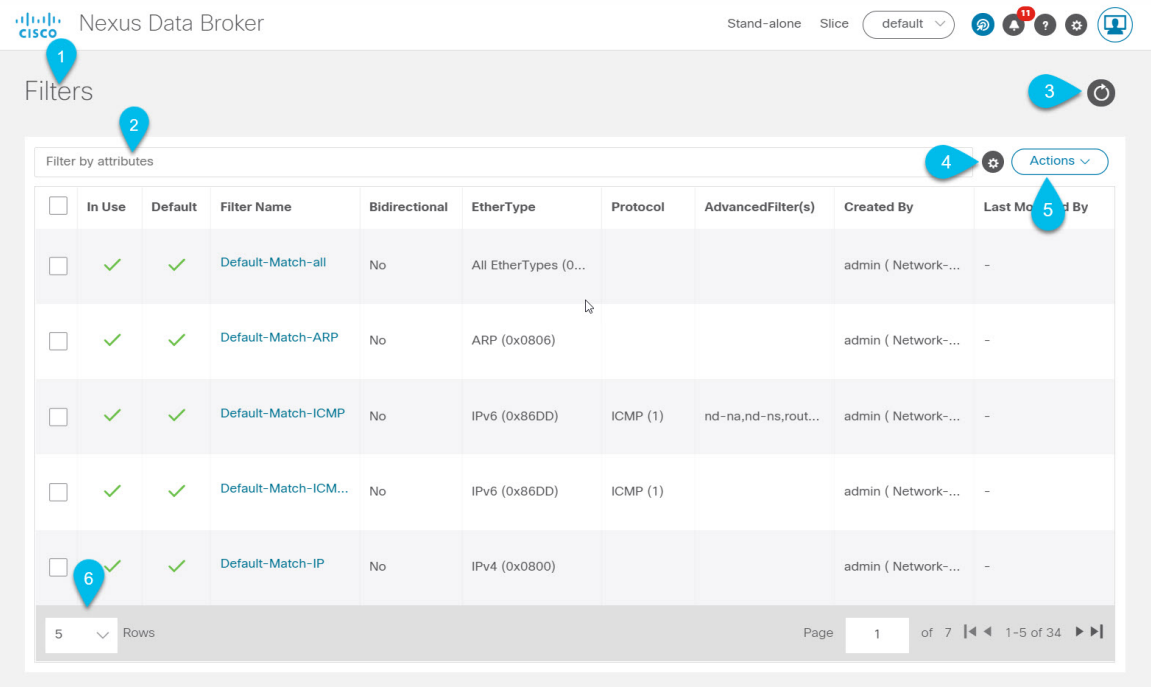
- Components
- Sessions
- Statistics
- Troubleshooting
- Administration

For details about the header icons, see Header.

Components of a screen of the Cisco Nexus Data Broker

When you click a tab/ sub-tab, the current information of the tab is displayed in a table.

A typical screen representing one of the tabs of the Release 3.10 Cisco NDB GUI is displayed here:



- 1—Name of the tab/sub-tab.
- 2—Use the *Filter by attributes* bar to filter the displayed table which has the details of the selected tab. Choose the attribute, operator and filter-value.

  You can also filter the displayed table based on the *filter* icon that appears when you hover over an element of the table.
- 3—Use the *Refresh* icon to refresh the displayed details and get the latest information about the tab/ sub-tab.
- 4—Use the *Column Customization* icon to select the columns you want to see in the displayed table.
- 5—Click the **Actions** button to see the available actions for the screen.

- 6—From the **Rows** drop-down list, select the number of rows to be displayed in the table.

Header

This section provides an overview of the Cisco Nexus Data Broker GUI Header (upper right corner) icons:

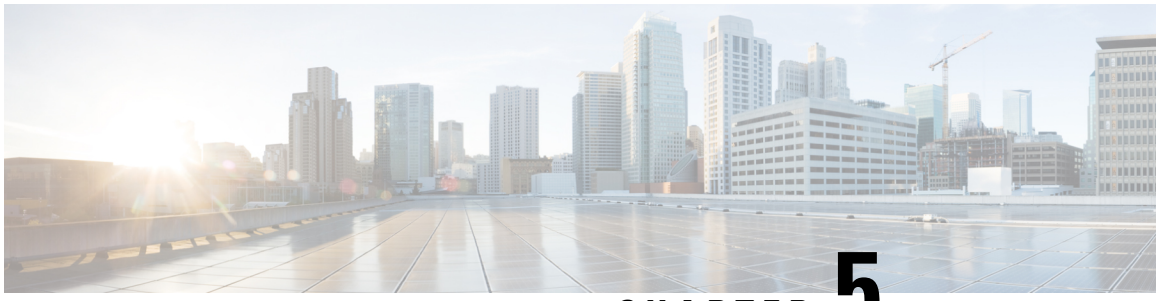
Table 6: Cisco Nexus Data Broker Header Icons

Icon	Description
Cluster	Displays the role of the current NDB controller instance-either Primary (P) or Member (M). The IP addresses of the primary and member(s) are displayed; the IP address of the primary cluster is denoted with an (*). If NDB controller is not in a cluster, `Stand-alone` is displayed.
Slice	Displays the slice name the user is currently logged in to. From the drop-down list, select another slice to change the network view.
Figure 1: Create 	Provides quick navigation to often-used configuration and administration procedures.
Figure 2: Alarm 	Displays the number of inconsistent NDB devices. Click the Alarm icon; you are directed to the Flow Management tab for details.
Figure 3: Help Menu-Bar 	Displays the following options: • **What's New**—Displays new features for the latest release. • **Help**—Displays online help content.

Icon	Description
Figure 4: System Tools Menu-Bar 	Provides the following options: • **Download Log**—Enables you to download log files to your local machine. • **Northbound API**—takes you to the **Swagger** UI for details about NDB REST APIs. • **Session Timeout**—Enables you to set the session timeout value. • **About Nexus Data Broker**—Displays NDB details such as, build and version.
Figure 5: User Profile Menu-Bar 	Provides the following options: • **Welcome** *User*—Displays the current user of the GUI. • **Change Password**—Enables you to change the password of the current user. • **Logout**—Enables you to logout of the GUI.

PART I

Configuring the Cisco Nexus Data Broker



CHAPTER 5

Dashboard

This chapter has details about the Cisco Nexus Data Broker dashboard. The dashboard integrates information from multiple components and devices into a unified display.

• Dashboard, on page 57

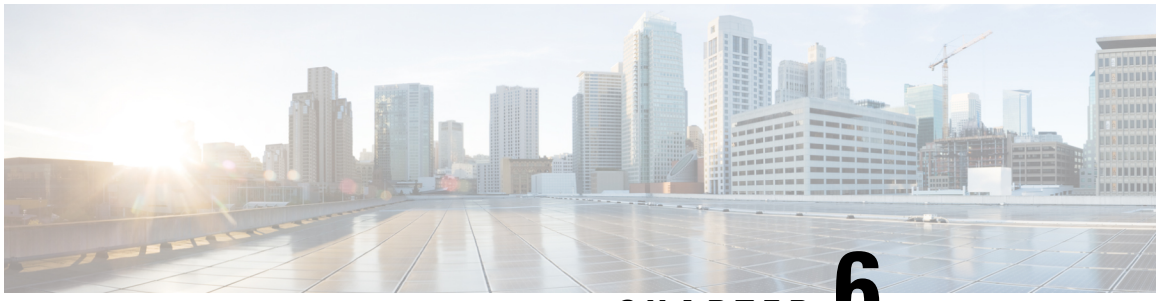
Dashboard

The intent of **Dashboard** is to enable network and storage administrators to focus on particular areas of concern around the health and performance of Cisco Nexus Data Broker. This information is provided as 24-hour snapshots.

From the left menu bar, choose **Dashboard**. The **Dashboard** window displays the following dashlets:

- **Status by Resources**—Status of the resources connected to the NDB controller are displayed in color-coded circles. The resources are:
  - NDB Devices
  - Input Ports
  - Filters
  - Monitoring Tools
  - Connections
- **Data Handled / Received since** *date* —Overall amount of data received and transmitted by the NDB controller since the *indicated date*.
- **Cluster Runtime**—Runtime of the current cluster.
- **Cluster Last Restart**—Date and time the cluster was last restarted.
- **Top Connections by Packet Count** (displayed in color coded bars)— Connections based on packet count (total packet count processed by the flows of the connection) and approximate bandwidth for a connection based on the packet count. The list is in descending order; the connection with the highest packet count is displayed at the top.
- **Top Input Ports by Received Packet Count** (displayed in color coded bars)— Input ports based on the number of packets received on the ports. The list is in descending order; the source port with the highest *received* packet count is displayed at the top.

- **Top Monitoring Tools by Transmitted Packet Count** (displayed in color coded bars)— Monitoring tools based on the transmitted packet count. The list is in descending order; the monitoring tool with the highest *transmitted* packet count is displayed at the top.
- **Top Filters by Filtered Packet Count** (displayed in color coded bars)— Filters based on the ACL-filtered packet count. The list is in descending order; the filter with the highest packet count is displayed at the top.
- **Top Device by TCAM Resource Utilization** (displayed in color coded bars)— Devices based on TCAM resource utilization. The list is in descending order; the device which has the highest utilization is displayed at the top.



CHAPTER 6

Topology

This chapter has details of the network topology with details of the devices and connections of the Cisco Nexus Data Broker.

Topology

The **Topology** tab provides an integrated view of the Cisco NDB network.

The topology diagram displays the elements of the network. Hover over an element to get details about it. Click an element, for more information about the element.

The displayed network elements are:

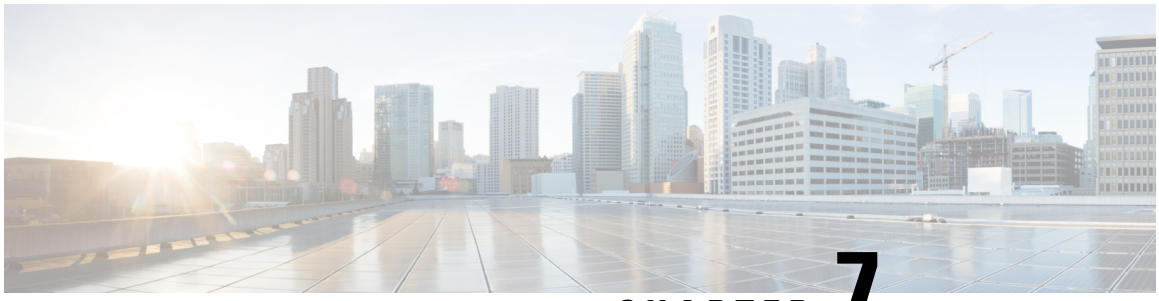
- Connected NDB devices
- Input ports
- Monitoring tools
- NX-OS Devices
- ACI Devices

Note

Click **Refresh**( ) to view the latest topology.

The following actions can be performed from the **Topology** tab:

- **Add NDB Device**— See Adding a Devicefor more details.
- **Add Span Device**— See *Adding a Span Device* for more details.
- **Add Monitoring Tool**—See Adding a Monitoring Tool for more details.



CHAPTER 7

Devices

This chapter has details about the devices of the Cisco Nexus Data Broker.

Devices

The **Devices** tab has the following sub tabs:

- **NDB Devices**—aggregation devices managed by the NDB controller. See NDB Devices for more details.
- **Span Devices**—NX-OS devices and ACI devices connected to the NDB controller. See Span Devices, on page 72 for more details.
- **Device Groups**—the groups to which the NDB devices are segregated into. See Device Groups for more details.

NDB Devices

The **NDB Devices** tab displays details of all the devices connected to the NDB controller.

A table is displayed with the following details:

Table 7: NDB Devices

Column Name	Description
Status (the first column of the table)	The current status of the device connected to the NDB; indicated by color. The options are: • Green—indicates that the device is operational and connected to the NDB controller. • Red—indicates failure and the device is not connected to the NDB controller. • Yellow—indicates that the device is connected but not ready yet. Reboot the device and wait for a few minutes for the status to turn green. Refresh and check. • Gray—indicates that the device is in maintenance mode.

Column Name	Description
IP Address	The IP address of the device. This field is a hyperlink. Click the IP address to view more details of the device. Click the **IP Address**. A new pane is displayed on the right which has more information about the device. Additional actions that can be performed from here are: • Editing a Device • Take Device Offline • Editing Global Configuration for a Device **Note** The *Take Device Offline* action is generally grayed out and is available only for devices in maintenance mode. You can also view the **Ports**, **Port Channels** and **Port Groups** of the device by clicking the corresponding tab. For more information about Port Channels and Groups, see Port Channels and Port Groups. Click the **Details** icon () to get additional details of the device. A new window displays the following details for the selected device: • General • Ports • Port Channel • Port Groups • Global Configuration • Monitor Sessions • Flow Statistics • Port Statistics • TCAM Resource Utilization Additional actions that can be performed from **Details** tab: • Trigger Global ACLs—this action identifies the non-configured interfaces of a device and attaches global ACLs to all these interfaces. It is mandatory for all interfaces of a device to be configured with global ACLs. • Adding a Port Channel

Column Name	Description
Device Name	The device name (switch name) as indicated by the administrator while configuring the device. Device name is displayed only if the device status is green. If the status of the device is red or yellow, the device name is not displayed.
Platform	The device platform.
Node ID	The node ID of the device.
Profile Name	The profile of the device as configured during device addition.
NX-OS	The software version currently running on the device.
Mode	The mode the switch is currently using. The options are: • NDB mode—indicates that the whole switch (all interfaces) is managed by the NDB controller. • Hybrid—indicates that only some interfaces in the device are managed by the NDB controller. **Note** By default, this column is hidden. When Hybrid mode is enabled on the device during device addition, this column is displayed.
Port	The port used by the NDB controller to communicate to the NDB device.
Status Description	The status of the connection between the NDB device and the NDB controller. The options are: • Connection succeeded—indicates that the connection between the device and NDB controller is successful. • Connection failed—indicates that the connection between the device and NDB controller has failed. A reason for failure is also displayed, such as authentication failed, connection refused (incorrect port). • Connection not ready—indicates that the device reload was not successful.

The following actions can be performed from the **NDB Devices** tab:

- **Add Device**—Use this to add a new device. See Adding a Device for details.
- **Rediscover Device**—Select the required device by checking the check box at the beginning of the row. Click **Actions** > **Rediscover Device(s)**. A pop-up appears. Click **Rediscover** to rediscover the selected devices. When you rediscover devices, the global ACLs are reattached.

Note Rediscovering a device leads to UDF, ports, global and connections reconfigurations and this results in traffic loss.

When there is a configuration error, use rediscover to reconfigure the device.

If you choose the rediscover action without selecting a check box, an error is displayed. You will be prompted to select a device.

- **Reconnect Device**— Select the required device by checking the check box at the beginning of the row. Click **Actions** > **Reconnect Device(s)**. A pop-up appears. Click **Reconnect** to reconnect the selected devices. The reconnect action is used to re-establish a failed connection between a device and NDB controller.

  If you choose the reconnect action without selecting a check box, an error is displayed. You will be prompted to select a device.

- **Update Profile**—Use this action to add or update the profile for a device. See Updating Device Profile for details about this task.

- **Delete Device**—Select the required device by checking the check box which is available at the beginning of the row. Click **Actions** > **Delete Device(s)**. A pop-up window displays two options:

  - **Delete**—Use this option to delete the device from the NDB controller while retaining the device configuration.

  - **Purge and Delete**—Use this option to delete the device and also remove device configuration from the NDB controller.

  If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a device.

Note If a device is not reachable and disconnects from the NDB controller, the NDB controller tries to locate and connect to the device after every 30 seconds.

Global deny ACLs are automatically added to all non-configured interfaces (Edge SPAN/TAP, Packet Truncation, Remote Source, and Local and Remote Monitor) on a device. By default, Global Deny ACL feature is enabled on all the devices. You can disable the Global Deny ACL feature by setting the configure.global.acls parameter to false in the **config.ini** file. Ensure that you restart NDB after making changes in the configuration file.

Adding a Device

Use this procedure to add a device to NDB controller.

Before you begin

Before adding a device to the NDB controller, do the following:

- Enable NXAPI on the device using the **feature nxapi** command.
- Use the Device Prerequisites option, if you are adding a device for the first time to the NDB controller.

Note Check the *Cisco Nexus Data Broker Release Notes, Release 3.10*, to see the supported Cisco Nexus Series switches and the supported NX-OS versions.

Step 1 Navigate to **Devices** > **NDB Devices**.

Step 2 From the **Actions** drop down menu, select **Add Device**.

Step 3 In the **Add Device** dialog box, enter the following details:

Table 8: Add Device

Field	Description
General	
IP Address/ Hostname	Enter the name or IP address of the device. To add multiple devices, add the hostnames or IP Addresses separated with a comma.
Username/ Profile	Select either **Username** or **Profile**. If you click **Username**, the following fields are displayed: • **Username**—Enter the switch username to login to the device. • **Password**—Enter the switch password. If you click **Profile**, the following fields are displayed: • **Profile**—From the **Select Profile** drop-down list, select a profile. **Note** You can associate multiple switches to a profile. The profile configuration is applied to all the member switches.
Connection Type	Select the Connection Type from the drop- down list. Currently, only NX-API is supported.
Port	Enter the device communication port. Use port 80 for NX-API over HTTP and 443 for HTTPS.

Field	Description
Device Prerequisites	Click the gray button to enable Device Prerequisites. The bar turns blue and the button moves to the right. The following check boxes appear: • **Interface Commands**—By default, this check box is checked. Device Prerequisites automatically executes a set of default interface commands. • **Reboot**—Check the check box to reboot the device before it gets added to NDB. • **TCAM**—Check the check box to set a TCAM value. Select **Default** or **Scale**. A memory of 1024 or 2048 is allocated, respectively. For more information about Device Prerequisites, see Device Prerequisites, on page 70.
Hybrid Mode	Slide the bar to the right to enable hybrid mode. In hybrid mode, only some interfaces of the device are managed by NDB. For this option to be displayed, the **config.ini** file should be enabled using **nx.hybrid.support=true**. Restart NDB to use this feature on all the the devices connected to NDB.

Step 4 Click **Add Device**.

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.

Editing a Device

Use this procedure to edit a device.

Before you begin

Create one or more devices.

Step 1 Navigate to **Devices** > **NDB Devices**.

Step 2 In the displayed table, click an **IP Address**.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Device**.

Step 4 In the **Edit Device** dialog box, the current device information is displayed. Modify these fields, as required:

Table 9: Edit Device

Field	Description
General	
IP Address/ Hostname	The current IP address of the device. This field cannot be edited.
Username/ Profile	Select either **Username** or **Profile**. If you click **Username**, the following fields are displayed: • **Username**— Username used to login to the device is displayed; you can edit this field. • **Password**—Enter the password for the username. If you click **Profile**, the following fields are displayed: • **Profile**—From the **Select Profile** drop-down list, select a profile. **Note** You can associate multiple switches to a profile. The profile configuration is applied to all the member switches.
Connection Type	Select the Connection Type from the drop down menu. Currently, only NXAPI is supported.
Port	Enter the device communication port. Use port 80 for NX-API over HTTP and 443 for HTTPS.
Device Prerequisites	Click the gray button to enable Device Prerequisites. The bar turns blue and the button moves to the right. The following check boxes appear: • **Interface Commands**—By default, this check box is checked. Device Prerequisites automatically executes a set of default interface commands. • **Reboot**—Check the check box to reboot the device before it gets added to NDB. • **TCAM**—Check the check box to set a TCAM value. Select **Default** or **Scale**. A memory of 1024 or 2048 is allocated, respectively. For more information about Device Prerequisites, see Device Prerequisites, on page 70.

Step 5 Click **Edit Device**.

Updating Device Profile

Use this procedure to assign (associate) a profile to a device or update the profile for a device.

Before you begin

Create one or more profiles.

Step 1 Navigate to **Devices** > **NDB Devices**.

Step 2 From the **Actions** drop-down menu, select **Assign/ Update Profile**.

Step 3 In the **Assign/ Update Profile** dialog box, enter the following details:

Table 10: Assign/ Update Profile

Field	Description
General	
Profile	Select a **Profile** from the drop down menu.
Connection Type	The default NXAPI connection type is displayed.

Step 4 Click **Assign/ Update Profile**.

Adding a Port Channel

Use this procedure to add a port channel.

See Port Channels and Port Groups for more information about port channels.

Step 1 Navigate to **Devices** > **NDB Devices**.

Step 2 Click an **IP Address** and select the Details icon.

Step 3 In the **Add Port Channel** dialog box, enter the following details:

Table 11: Add Port Channel

Field	Description
General	
ID	Enter a name for the port channel.
Description	Enter a description for the port channel.
Port	Click **Select Port**. Select the required check boxes and click **Select**.

Step 4 Click **Add Port Channel**.

Device Prerequisites

NDB pushes basic configuration to a newly added device. Ensure NX-API is enabled on the new device for NDB to push prerequisite configuration successfully. Manual configuration of the NX-API devices to make it ready for NDB is not required.

Device Prerequisites can be configured when you add or edit a device, or when you add or change profile to a device. See Adding a Device, on page 65 and/or Editing a Device, on page 67.

Following configurations are pushed into the new switch by NDB:

- While onboarding an NDB device, without STP pre-requisites (when independent links or port channels are connected to NDB devices), you need to manually configure the **switchport mode trunk** and **spanning-tree bpdufilter enable** commands.
- TCAM configurations based on the device platform
- MST mode is enabled on the Spanning Tree
- Basic VLAN configuration
- LLDP feature is enabled (only for the centralized mode of NDB)

Device is rebooted after all the configurations are successfully pushed by NDB. The device reboot is required because of the TCAM configurations. The reboot is supported from NX-OS is 9.2(3) and above.

Port Channels and Port Groups

Port Channels

A port channel is an aggregation of multiple physical interfaces that creates a logical interface. You can bundle up to 8 individual active links into a port channel to provide increased bandwidth and redundancy. If a member port within a port channel fails, the traffic previously carried over the failed link switches to the remaining member ports within the port channel. Port channeling also load balances traffic across these physical interfaces. The port channel stays operational as long as at least one physical interface within the port channel is operational.

You create a port channel by bundling compatible interfaces. You can configure and run either static port channels or ports channels running the Link Aggregation Control Protocol (LACP). Any configuration changes that you apply to the port channel are applied to each member interface of that port channel. For example, if you configure Spanning Tree Protocol (STP) parameters on the port channel, the Cisco NX-OS applies those parameters to each interface in the port channel.

You can use static port channels, with no associated protocol, for a simplified configuration. For more efficient use of the port channel, you can use the Link Aggregation Control Protocol (LACP), which is defined in IEEE 802.3ad. When you use LACP, the link passes protocol packets.

Port Groups

Ports of a device (or different devices) can be grouped together to form a port group. The port groups can be a combination of the edge-span and the edge-tap ports across different switches. Selecting individual ports of a port group is disabled when using a port group.

Precision Time Protocol

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

PTP is a time synchronization protocol for nodes distributed across a network. Its hardware timestamp feature provides excellent accuracy.

PTP is supported on the following platforms:

- Cisco Nexus 9200 switches
- Cisco Nexus 9300 switches—9300-FX, FX2, EX
- Cisco Nexus 9500 switches—9500-FX, EX
- Cisco Nexus 3548 switches

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

See Editing Global Configuration for a Device, on page 105 for configuring PTP.

Netflow

NetFlow identifies packet flows for ingress IP packets and provides statistics based on these packet flows. NetFlow does not require any change to either the packets themselves or to any networking device.

In order to provide enough free space to monitor flows, the ing-netflow TCAM region is carved to 512 by default on Cisco Nexus 9300-FX platform switches. If more space is required, use the **hardware access-list tcam region ing-netflow size** command to modify the size of this TCAM region, using a multiple of 512.

Netflow is supported on the following platforms:

- Cisco Nexus 9300 switches—9300-FX, FX2, EX
- Cisco Nexus 9500 switches—9500-FX, EX

See Editing Global Configuration for a Device, on page 105 for configuring Netflow.

For more information about Netflow, see *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.*

Sampled Flow

You can manage Sampled Flow (sFlow) on NDB that are based on NX-API. 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.

See Editing Global Configuration for a Device, on page 105 for configuring sFlow.

Symmetric and Non-Symmetric Load Balancing

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

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

Configuration Type	Hashing Configuration	Platforms	Options
Symmetric	SOURCE_DESTINATION	Nexus 9000 Series (all), N3K-C3164xx, N3K-C32xx	IP, IP-GRE, IP-L4PORT, IP-L4PORT-VLAN, IP-VLAN, L4PORT, MAC
		REST API	IP, IP-GRE, PORT, MAC, IP-ONLY,PORT-ONLY
Non-symmetric	SOURCE, DESTINATION	Nexus 9000 Series (all), N3K-C3164xx, N3K-C32xx	IP, IP-GRE, IP-L4PORT, IP-L4PORT-VLAN, IP-VLAN, L4PORT, MAC
		REST API	IP, IP-GRE, PORT, MAC

Span Devices

Switch port Analyzer (SPAN) is an efficient and high performance traffic monitoring system. It duplicates the network traffic and routes the packets to an the analyzer for monitoring. SPAN is used for troubleshooting connectivity issues and calculating network utilization, and performance monitoring.You can add, edit, remove, and rediscover a device to SPAN using NDB.

The **Span Devices** tab displays details of the devices connected to the SPAN.

Select **APIC/ ACI Devices** or **NX-OS Devices** to see the details.

- **NX-OS Devices**—devices that are running on NX-OS (standalone devices) and connected to the NDB controller.
- **ACI Devices/ APIC**—APIC and ACI devices connected to the NDB controller.

Note The NX-OS device can be a Cisco Nexus 9000 Series switch or Cisco Nexus 3000 Series switch in NX-OS mode. NX-API has to be enabled on the production (NX-OS) switches.

Table 12: ACI Devices/ APIC

Column	Description
Active IP	Active IP address of the APIC device.
Username	Username currently logged into the APIC device.
Primary IP Address	Primary IP address of the device.
Secondary IP Address	Secondary IP address of the device.
Tertiary IP Address	Tertiary IP address of the device.

Table 13: NX-OS Devices

Column	Description
Active IP	Active IP address of the NX-OS device.
Username	Username currently logged in to the NX-OS device.

The following actions can be performed from the **Span Devices** tab:

- **Add Span Device**—Use this to add a new span device. See Adding a Span Device for details.
- **Rediscover Span Device**—Select the required device by checking the check box at the beginning of the row. Click **Actions** > **Rediscover Span Device**. A pop-up window is displayed. Click **Rediscover** to rediscover the selected devices.

  Use the **Rediscover Span Device** option to re-establish the connection between the NDB controller and the Span device(s).

  If you choose the rediscover action without selecting a check box, an error is displayed. You will be prompted to select a device.
- **Delete Span Device**—Select the required device by checking the check box which is available at the beginning of the row. Click **Actions** > **Delete Span Device**.

  If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a device.

Adding a Span Device

Use this procedure to add a device to SPAN.

Step 1 Navigate to **Devices** > **Span Devices**.

Step 2 From the **Actions** drop down list, select **Add Span Device**.

Step 3 In the **Add Span Device** dialog box, enter the following details:

Table 14: Add Span Device

Field	Description
General	Select **ACI** or **NX-OS**. The options available for each are discussed in the rows, below.
Fields displayed for **ACI** :	
APIC IP Address/ Hostname	Enter the IP address for the APIC device.
APIC IP Address (Secondary)	Enter a secondary IP address for the APIC device.
APIC IP Address (Tertiary)	Enter a tertiary IP address for the APIC device.
Username	Enter a username to login to the device.
Password	Enter the password for the username.
Fields displayed for **NX-OS**:	
Address	IP address of the NX-OS device.
Port	The device communication port.
Username	Enter a username for the device.
Password	Enter the required password to authenticate the username.

Step 4 Click **Add Span Device**.

Editing a Span Device

Use this procedure to edit a Span device. Some of the parameters which were selected earlier (in the *Adding a Span Device* procedure) can not be changed.

Before you begin

Create one or more Span devices.

Step 1 Navigate to **Devices** > **Span Devices**.

Step 2 In the displayed table, click an **IP Address**.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Span Device**.

Step 4 In the **Edit Span Device** dialog box, the current span device information is displayed. Modify these fields, as required:

Table 15: Edit Span Device

Field	Description
General	This field cannot be edited. If you have added an ACI or NX-OS span device, that selection can not be changed. However, you can edit the parameters for ACI and NX-OS; they have been discussed in the subsequent rows.
Fields displayed for **ACI**:	
APIC IP Address/ Hostname	The primary IP address for the APIC/ ACI device. This field can not be edited.
APIC IP Address (Secondary)	Enter a secondary IP address for the APIC device.
APIC IP Address (Tertiary)	Enter a tertiary IP address for the APIC device.
Username	Enter a username to login to the device.
Password	Enter the password for the username.
Fields displayed for **NX-OS**:	
NX-OS	Select **NX-OS** to add an NX-OS device. The following options are displayed: • **Address** • **Port** • **Username** • **Password**
Address	IP address of the NX-OS device. This field cannot be edited.
Port	The device communication port.
Username	Username of the device.
Password	Enter password to authenticate the username.

Step 5 Click **Edit Span Device**.

Device Groups

The **Device Groups** tab displays details of the device groups. A table is displayed with the following details:

Table 16: Device Groups

Column Name	Description
Group	The device group name. This field is a hyperlink. Click the group name and a new pane is displayed on the right that has the list of devices included in the group. Additional actions that can be performed from here are: • Editing a Device Group
Devices	The number of devices in the device group.

The following actions can be performed from the **Device Groups** tab:

- **Add Device Group**—Use this to add a new device group. See Adding a Device Group.
- **Delete Device Group**—Select the required device group by checking the check box which is available at the beginning of the row. Click **Actions** > **Delete Device Group(s).** The selected device group(s) are deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a device group.

Adding a Device Group

Use this procedure to add a new device group.

Step 1 Navigate to **Devices** > **Device Groups**.

Step 2 From the **Actions** drop down menu, select **Add Device Group**.

Step 3 In the **Add Device Group** dialog box, enter the following details:

Table 17: Add Device Group

Field	Description
General	
Device Group Name	Enter a name for the device group.
Devices	Click **Select Device(s)**. The **Select Device** dialog box opens. Check the check box corresponding to the device(s) you want to add to the group. Click **Select**. **Note** Check if the device is already part of another group; if yes, the device is removed from the previous group and added to the new group.

Step 4 Click **Add Device Group**.

Editing a Device Group

Use this procedure to edit a device group.

Before you begin

Add one or more device groups.

Step 1 Navigate to **Devices** > **Device Groups**.

Step 2 Click a **Device Group** name.

A new pane is displayed on the right.

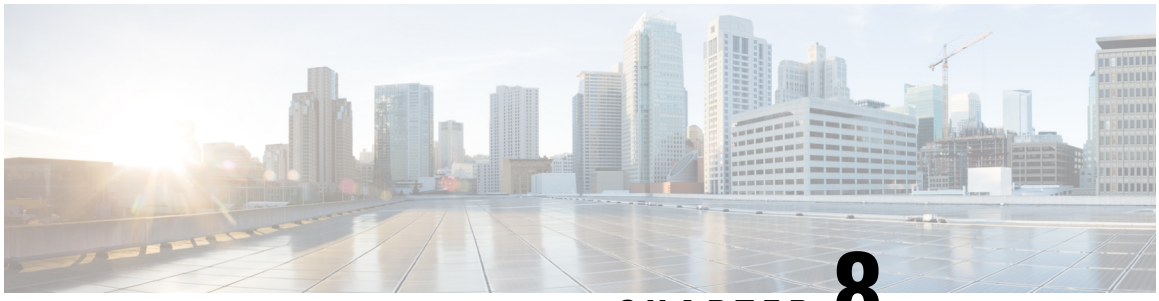
Step 3 Click **Action** > **Edit Device Group**.

Enter the following details, in the displayed window.

Table 18: Edit Device Group

Field	Description
General	
Device Group Name	Device group name. This field cannot be edited.
Devices	The devices which are currently part of the device group are displayed. You can delete devices from a group. To add more devices to the group, click **Select Device(s)**. The **Select Device** dialog box opens. Check the check box corresponding to the device(s) you want to add to the group. Click **Select**. **Note** Check if the device is already part of another group; if yes, the device is removed from the previous group and added to the new group.

Step 4 Click **Edit Device Group**.



CHAPTER 8

Connections

This chapter has details about the connections of the Cisco Nexus Data Broker.

Connections

The **Connections** tab has the following subtabs:

- **User Connections**—user-defined connections to manage traffic between an input port and monitoring tool port. See User Connections for more details.
- **Default Connections**—by default, ingress traffic on the input ports is denied, until a user-defined connection is defined. See Default Connections for more details.

User Connections

The **User Connections** tab displays details of all the user-defined connections between input port(s) (with or without filters) and monitoring tool port(s).

A table with the following details is displayed:

Table 19: User Connections

Column Name	Description
Connection Name	The name of the connection. This field is a hyperlink. Click the name of the connection. A new pane is displayed on the right which has more information about the connection. You can view the topology of the connection in either **Deployment View** or **Network View**. Additional actions that can be performed here: • **Edit Connection**—Select this action to edit a connection. See Editing or Cloning a Connection for details. • **Clone Connection**—Select this action to clone a connection. See Editing or Cloning a Connection for details. Cloning a connection is similar to editing a connection. Click the **Details** icon () to get additional details of the connection. A new window displays the following details for the selected connection: • General • Deployment View • Network View • Flow Statistics • Port Statistics
Type	Type of connection. The options are: • Normal— here, the connection applies filters on the input ports and redirects traffic to the monitoring tool. • Auto Priority— here, the connection redirects the traffic to the monitoring tool based on the set auto-priority number. For more details, see Auto Priority, on page 88.
Applied Filters	The number of **Allow** and **Drop** filters applied to the connection. Matching traffic is either dropped or allowed based on the selection. This field is a hyperlink. Click the displayed number and a new pane opens on the right. A list of all the filters applied to the connection is displayed.

Column Name	Description
Input Port/ Input Port Groups	The number of input ports and/or input port groups of the connection. This field is a hyperlink. Click the displayed number and a new pane opens on the right. A list of sources (production devices from which traffic reaches the NDB controller) and ports applicable to the connection is displayed.
Monitoring Tools/ Monitoring Tools Group	The number of monitoring tools and/or monitoring tool groups of the connection. This field is a hyperlink. Click the displayed number and a new pane opens on the right. A list of monitoring tools applicable to the connection is displayed.
Description	Description of the connection.
Created By	User who created the connection.
Last Modified By	User who last modified the connection.

A color coded circle and a lock are displayed at the beginning of each row. The factors impacting the status of a connection are— operational and administration state of the source ports, operational state and administration state of the monitoring tools and the sessions involved in the connection.

- A green circle indicates that the connection is successful.
- A red circle indicates that the connection has failed.
- A yellow circle indicates the connection is partially successful; one or more input port(s) and monitoring tools have errors.
- A gray circle indicates that the connection is not operational; check the state of all the input ports and monitoring tools.

The lock symbol indicates that the connection is locked and unauthorized modification of the connection parameters is not allowed. Only the user (or administrator) who has created the connection or the user who has locked the connection can make required changes. You can lock a connection while adding a connection.

The following actions can be performed from the **User Connections** tab:

- **Add Connection**—Select this action to add a new connection. See Adding a Connection for details about this task.
- **Delete Connection**—Select the required connection(s) by checking the check box which is at the beginning of the row. Click the **Actions** button and, select **Delete Connection**. The selected connection(s) are deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a connection.
- **Toggle Install**—Select the required connection(s) by checking the check box which is at the beginning of the row. Click the **Actions** button, select **Toggle Install** to install a connection. **Toggle Install** will install/ uninstall connection(s) on the NDB devices but the connection configuration will not be deleted from the NDB controller.

If you choose the toggle install action without selecting a check box, an error is displayed. You will be prompted to select a connection.

You can disable deny ACL on all the ISL interfaces by setting the **configure.global.acls** parameter to false in the **config.ini** file. Ensure that you restart NDB after making changes in the configuration file.

You can disable Global deny ACL or ISL deny ACL during the CLI upgrade or configuration upload by using the CLI upgrade command and setting the **configure.global.acls** parameter to false in the **config.ini** file. For example:

```
configure.global.acls=false
```

Adding a Connection

Use this procedure to add a connection. A connection establishes a link between the input ports (with filters) of a device to the monitoring tool ports of the device.

Before you begin

Complete these tasks:

- Define a filter for the connection
- Configure a monitoring tool (recommended)
- Configure an edge port (recommended)
- Use Dry Run (recommended)

Follow these restrictions and usage guidelines for creating a connection:

- Configure QinQ VLAN to add a new connection with auto priority across devices (with multiple hops).
- You can configure only one connection with auto priority for each input port/port group.

Step 1 Navigate to **Connections** > **User Connections**.

Step 2 From the **Actions** drop-down list, select **Add Connection**.

Step 3 In the **Add Connection** dialog box, enter the following details:

Table 20: Add Connection

Field	Description
Connection Name	Enter the connection name.
Description	Enter a description for the connection.

Field	Description
Priority	Enter the priority you want to set for the connection. By default, priority level is 100. Range is from 2 to 10000. Higher the number, greater the priority. For example, 200 indicates higher priority when compared to 100. Incoming traffic from the ports is matched based on priority. If two connections have the same inputs ports and same filters, traffic takes the connection with the higher priority. **Note** By default, Edit is enabled for the Cisco NDB administrator role.
Lock Connection	Click the gray button to lock the connection. The gray button turns blue and moves to the right indicating that locking is enabled. Locking a connection prevents unauthorized changes to a connection.
AutoPriority	Click the gray button to enable auto priority. The gray button turns blue and moves to the right indicating that AutoPriority is enabled. When **AutoPriority** is enabled, the **Priority** field is disabled. NDB automatically assigns a priority for a connection based on certain criteria (monitoring tools and filters). Auto priority provides flexibility to map filters to mulitple monitoring tools in a connection. For more details, see Auto Priority, on page 88.
Connection Topology	Here, you can define **Input Port(s), Filter(s) and Monitoring Tools(s)** for a connection.

Field	Description
Input Port	Select an input port for the connection. Click **Select Input Port(s)/ Group**. Select either **Input Port**or **Input Port Group**. If you select **Input Port**, a list of devices is displayed. **a.** To select a device, check the corresponding check box. Based on the selected device, the available ports of the device are displayed. **b.** To select a port, check the corresponding check box. Details of the selected port(s) are displayed on the right. The current status of the port is displayed by a color-coded circle. **Note** Click **Add Input Port** to add an input port for the selected device. For the detailed procedure, see Adding an Input Port. **c.** Click **Select** to include the selected source port(s) as part of the connection. If you select **Input Port Group**, a list of port groups is displayed. **a.** To select a port group, check the corresponding check box. Details of the selected port group(s) are displayed on the right. The current status of the port group is indicated by a color-coded circle. **Note** Click **Add Input Port Group** to add an input port group. For the detailed procedure, see Adding an Input Port Group. **b.** Click **Select** to include the selected source port group(s) as part of the connection.
Filter	Click **Select Filter(s)**. **a.** To select a filter, check the corresponding check box. Details of the selected filter(s) are displayed on the right. More than one filter can be selected. You can either choose to use the **Allow** or **Deny** behavior for a filter. Allow enables the traffic from the input ports to pass through; deny drops the traffic from the input ports. **Note** Click **Add Filter** to add a filter. For the detailed procedure, see Adding a Filter. **b.** Click **Select** to include the selected filter(s) as part of the connection. **Note** This field is disabled if **AutoPriority** is enabled.

Field	Description
Monitoring Tools	The **Select Monitoring Tool(s)/ Group** option is displayed if AutoPriority is not enabled. Click **Select Monitoring Tool(s)/ Group** . Select either **Monitoring Tool** or **Tool Group**. If you select **Monitoring Tool**, a list of monitoring tools is displayed. **a.** To select a monitoring tool, check the corresponding check box. The details of the monitoring tool are displayed on the right, with the current status of the monitoring tool. The status is indicated by color coded circles. **Note** Click **Add Monitoring Tool** to add a monitoring tool. For the detailed procedure, see Adding a Monitoring Tool. **b.** Click **Select** to include the monitoring tool(s) as part of the connection. If you select **Tool Group**, a list of monitoring tool groups is displayed. **a.** To select a tool group, check the corresponding check box. Details of the selected tool group(s) are displayed on the right. The current status of the tool group is indicated by a color coded circle. **Note** Click **Add Monitoring Tool Group** to add a monitoring tool group. For the detailed procedure, see Adding a Monitoring Tool Group. **b.** Click **Select** to include the selected tool group(s) as part of the connection. The **Select Monitoring Tool and Filter Pair** option is displayed if AutoPriority is enabled. **a.** Select one or more monitoring tool(s) and filter(s). **b.** Click **Select**.

Step 4 Click **Add Connection** to add the connection or **Install Connection** to add and deploy the connection on the NDB device.

Editing or Cloning a Connection

Use this procedure to edit or clone a connection.

Editing a connection means changing the parameters of an existing connection.

Cloning a connection means creating a new connection with identical parameters of an exisiting connection, and then, changing the required parameters. Ensure to change the name of the connection before saving it.

Before you begin

Create one or more connections.

Step 1 Navigate to **Connections** > **User Connections**.

Step 2 In the displayed table, click a **Connection Name**.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Connection**.

To clone a connection, select **Clone Connection**.

Step 4 In the **Edit Connection** or **Clone Connection** dialog box, the current connection information is displayed. Modify these fields, as required:

Table 21: Edit Connection/ Clone Connection

Field	Description
Connection Name	Connection name.
Description	Description of the connection.
Priority	The current priority of the connection.
Lock Connection	Click the gray button to lock the connection. The gray button turns blue and moves to the right indicating that locking is enabled. Locking a connection prevents unauthorized changes to a connection.
Auto Priority	If **Auto Priority** was not enabled while adding a connection, then this field is disabled.
Connection Topology	Here, you can define **Input Port(s), Filter(s) and Monitoring Tools(s)** for a connection.

Field	Description
Input Port	The current input port(s) included in the connection are displayed. Click the cross mark adjacent to an input port to delete the port from the connection. To edit the input ports, click **Select Input Port(s)/ Group**. Select either **Input Port**or **Input Port Group**. If you select **Input Port**, a list of devices is displayed. **a.** To select a device, check the corresponding check box. Based on the selected device, the available ports of the device are displayed. **b.** To select a port, check the corresponding check box. Details of the selected port(s) are displayed on the right. **c.** Click **Select** to include the selected source port(s) as part of the connection. If you select **Input Port Group**, a list of port groups is displayed. **a.** To select a port group, check the corresponding check box. Details of the selected port group(s) are displayed on the right. **b.** Click **Select** to include the selected source port group(s) as part of the connection.
Filter	The current filter(s) included in the connection are displayed. Click the cross mark adjacent to a filter to delete the filter from the connection. To edit filters, click **Select Filter(s)**. **a.** To select a filter, check the corresponding check box. Details of the selected filter(s) are displayed on the right. More than one filter can be selected. **b.** Click **Select** to include the selected filter(s) as part of the connection.

Field	Description
Monitoring Tools	The current monitoring tool(s) or tool group(s) included in the connection are displayed. Click the cross mark adjacent to a monitoring tool or tool group to delete it from the connection. To edit any of these, click **Select Monitoring Tool(s)/ Group** . Select either **Monitoring Tool** or **Tool Group**. If you select **Monitoring Tool**, a list of monitoring tools is displayed. **a.** To select a monitoring tool, check the corresponding check box. The details of the monitoring tool are displayed on the right, with the current status of the monitoring tool. The status is indicated by color coded circles. **b.** Click **Select** to include the monitoring tool(s) as part of the connection. If you select **Tool Group**, a list of monitoring tool groups is displayed. **a.** To select a tool group, check the corresponding check box. Details of the selected tool group(s) are displayed on the right. The current status of the tool group is indicated by a color coded circle. **b.** Click **Select** to include the selected tool group(s) as part of the connection.

Step 5 Click **Edit Connection** or **Clone Connection**.

Auto Priority

Auto priority provides flexibility to map filters to mulitple destination devices in a connection.The priority of a connection with Auto-Priority is set to the value configured in the `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.

Dry Run

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 paramter to a value greater than zero. If the mm.dryrun.timer paramter 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. Use the Dry Run feature before adding a new connection.

Default Connections

The **Default Connections** tab displays details of the default NDB connections. Default deny rules are system-configured on the input ports, monitoring tools and packet truncation ports. This means, by default, traffic received on the input ports is denied , until a user defined connection is configured.

By default, deny ACL is enabled on all the Inter Switch Links (ISL) interfaces causing all the traffic in the ISL interfaces to be dropped if there is no connection installed. The following connections are installed on the ISL interfaces:

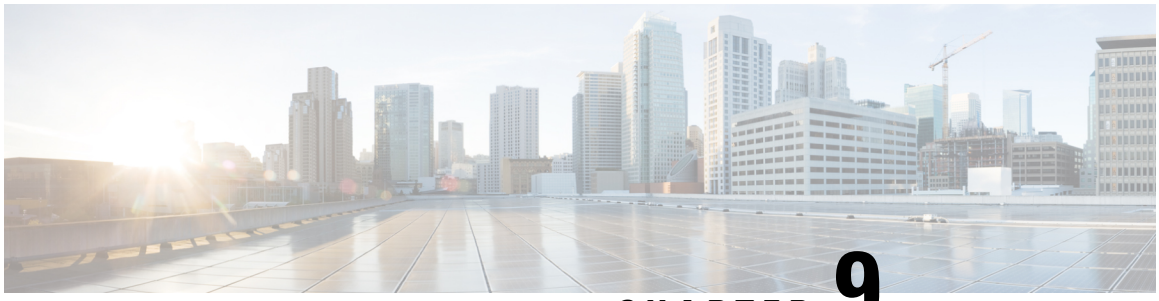
- Default-Deny-ISL-*device_name* connection with Default-Deny-All, Default-Deny-MPLS, and Default-Deny-ARP filters. This connection is supported on all the types of switches in NXAPI mode.
- Default-Deny-ISL-ICMP-*device_name* connection with Default-Deny-ICMP and Default-Deny-ICMP-All filters. This connection is supported on Nexus 9200, 9300EX, 9300FX, 9500EX, and 9500FX switches in NXAPI mode.
- You can manage this feature using the mm.addDefaultISLDenyRules attribute in config.ini file. By default, the mm.addDefaultISLDenyRules attribute is not be present in config.in file. To disable this feature, you need to add the mm.addDefaultISLDenyRules attribute to config.ini file ans set it to false and restart the device. For example:

```
mm.addDefaultISLDenyRules = false
```

A table is displayed with the following details:

Table 22: Default Connections

Column Name	Description
Connection Name	The default connection name. This field is a hyperlink. Click the name of the connection. A new pane is displayed on the right which has more information about the connection. The following actions can be performed here: • **Clone Connection**—Select this action to clone a connection. See Editing or Cloning a Connection for details. Cloning a connection is similar to editing a connection. **Note** Default connections cannot be edited.
Drop Filters	The number of drop filters for the connection. Drop filters on NDB drop the matching traffic.
Input / Monitoring Ports	The number of input or monitoring ports.
Description	Description of the connection.



CHAPTER 9

Components

This chapter has details about the components of the Cisco Nexus Data Broker.

Filters

The **Filters** tab displays details of all the filters available on the NDB controller. The tab provides information of the filtering criteria (used in a connection) for the incoming traffic.

The default filters include the following protocols for packet filtering:

- Default-match-all
- Default-match-IP
- Default-match-ARP
- Default-match-MPLS (unicast and multicast)
- Default-match-ICMP
- Default-match-ICMP-All

A table is displayed with the following details:

Table 23: Filters

Column Name	Description
In Use	A green tick mark indicates that the filter is in use, in a connection.

Column Name	Description
Filter	The filter name. Click **Filter**. A new pane is displayed on the right which has more information about the filter. The following additional actions can be performed from here: • Editing or Cloning a Filter **Note** Default filters cannot be edited.
Bidirectional	If a filter is bidirectional, a **Yes** is displayed; else a **No** is displayed. If a filter is marked bidirectional, incoming and outgoing traffic is filtered at the same port.
Ethertype	Layer 2 ethertype of the filter.
Protocol	Layer 3 protocol used by the filter.
Advanced Filter(s)	The advanced filters associated with the filter.
Created By	The user who created the filter.
Last Modified By	The user who last modified the filter.

The following actions can be performed from the **Filters** tab:

- **Add Filter**—Use this to add a new filter. See Adding a Filter for details about this task.
- **Delete Filter**—Select the filter(s) to be deleted by checking the check box which is available at the beginning of the row and then click **Actions** > **Delete Filter(s)**. The selected filter(s) is deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a filter.

Adding a Filter

Use this procedure to add a filter. The incoming traffic is matched based on the parameters defined in a filter.

Step 1 Navigate to **Components** > **Filters**.

Step 2 From the **Actions** drop down menu, select **Add Filter**.

Step 3 In the **Add Filter** dialog box, enter the following details:

Table 24: Add Filter

Field	Description
Filter Name	Enter a name for the filter.

Field	Description
Bidirectional	Check this box if you want the filter to capture bidirectional traffic information, that is, 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.

Layer 2	The options displayed for using Layer 2 filtering are:
	• Ethernet Type—Select the Ethernet Type from the drop-down list. The options are:
	  • IPv4
	  • IPv6
	  • LLDP
	  • MPLS
	  • ARP
	  • All Ethernet Types
	  • Predefined Ethernet Types— If you choose this option, all predefined Ethernet types contained in the `config.ini` file are associated with the rule, and you should not configure any other parameters.
	  • Enter Ethernet Type—If you choose this option, enter the ethernet type in hexadecimal format.
	• VLAN Identification Number—Enter 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.
	Maximum value is 4095.
	• VLAN Priority—Enter the VLAN priority for the traffic. VLAN Priority is matched for Layer 2 traffic only.
	• Source MAC Address—Enter the MAC address of the source device. MAC addresses are matched for Layer 2 traffic only.
	• Destination MAC Address—Enter the MAC address of the destination device. MAC addresses are matched for Layer 2 traffic only.
	• MPLS Label Value—Enter the MPLS value for Label 1, Label 2, Label 3, Label 4.
	The **MPLS Label Value** fields are displayed only if the **Ethernet Type** is set to MPLS. The MPLS label values are matched.

Field	Description
Layer 3 To enable options for Layer 3, choose **IPv4** or **IPv6** as **Ethertype** under the Layer 2 tab.	

Field	Description

	The options displayed for Layer 3 filtering are:
	• Source IP Address—Enter the Source IP address of the Layer 3 traffic. This can be one of the following:
	  • The host IP address in the standard IPv4 or IPv6 format
	  • An IPv4 or IPv6 address range
	  • Combination of an address range and standard IP addresses; example: 10.1.1.1, 10.1.1.2-10.1.1.5
	  • Comma-separated discontiguous IP addresses; example: 10.1.1.1, 10.1.1.2, 10.1.1.5
	Note 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.
	• Destination IP Address—Enter the Destination IP address of the Layer 3 traffic. This can be one of the following:
	  • The host IP address in the standard IPv4 or IPv6 format
	  • An IPv4 or IPv6 address range
	  • Combination of an address range and standard IP addresses; example: 10.1.1.1, 10.1.1.2-10.1.1.5
	  • Comma-separated discontiguous IP addresses; example: 10.1.1.1, 10.1.1.2, 10.1.1.5
	Note 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.
	• L4 Protocol—Select a Layer 4 protocol from the drop down list or enter a **Protocol Number**.
	• Advanced Filter—Click the button to enable advanced filtering and check the check-boxes to select the required options. For details about the options pertaining to Advanced Filters, see Advanced Filters.
	• Custom Filter—Click the button to enable custom filtering using User Defined Fields (UDF). Click **Select UDFs** and select a filter in the **Select Custom Filters** window. The

Field	Description
	UDFs created using Adding a User Defined Field are displayed here. The selected UDF(s) are displayed in a table. Enter the following details for the selected UDF: • Value—is the value to be matched in decimal notation (0-65535). E.g. if you want to match 0x0806 enter 2054 which is 0x0806 in decimal notation. • Mask—is the mask to be applied to the value for matching purposes. E.g. to exactly match 2054 (0x0806) enter 65535 (0xffff), to match 2048-2063 (0x0800-0x080f) use 65520 (0xfff0). **Note** When the monitoring tool port is on an ISL device, it is mandatory to select **Add Default UDF for inner vlan** checkbox. Ensure the input port has Q-in-Q configured.

Field	Description
Layer 4 To enable options for Layer 4, choose **IPv4** or **IPv6** as **Ethertype** under the Layer 2 tab and choose **TCP** or **UDP** as **L4 Protocol** under the Layer 3 tab.	The options displayed for Layer 4 filtering are: • Source Port—Select the source port from the drop down list. The options are: • FTP (Data) • FTP (Control) • SSH • Telnet • HTTP • HTTPS • Enter Source Port—Enter the source port. You can enter comma separated single port numbers or a range of source port numbers. **Note** If you enter a range of Layer 4 source ports, you cannot configure ranges of Layer 3 IP addresses or Layer 2 VLAN identifiers. • Destination Port—Select the destination port from the drop down list. The options are: • FTP (Data) • FTP (Control) • SSH • Telnet • HTTP • HTTPS • Enter Destination Port—Enter the source port. You can enter comma separated single port numbers or a range of source port numbers. **Note** If you enter a range of Layer 4 destination ports, you cannot configure ranges of Layer 2 VLAN identifiers or Layer 3 IP addresses.
Layer 7	Not supported.

Note For Custom Filtering: You can add upto four UDFs for a filter. UDF option is enabled for IPv4 and IPv6 ethertypes.

Step 4 Click **Add Filter** to add the filter.

Editing or Cloning a Filter

Use this procedure to edit or clone a filter.

Editing a filter means changing the parameters of an existing filter.

Cloning a filter means creating a new filter with the same parameters of an existing filter and making the required changes to the filter parameters. Ensure to change the name of the filter before saving it.

Note Default filters cannot be edited.

Before you begin

Add one or more filters.

Step 1 Navigate to **Components** > **Filters**.

Step 2 In the displayed table, click a **Filter**.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Clone Filter**.

Step 4 In the **Clone Filter** or **Edit Filter** dialog box, the current filter information is displayed. Modify these fields, as required:

Table 25: Edit/ Clone Filter

Field	Description
Filter Name	Name of the filter.
Bidirectional	Check this box if you want the filter to capture bidirectional traffic information, that is, 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.

Field	Description

Layer 2	The options displayed while using Layer 2 are:
	• Ethernet Type—Select the Ethernet Type from the drop-down list. The options are:
	  • IPv4
	  • IPv6
	  • LLDP
	  • MPLS
	  • ARP
	  • All Ethernet Types
	  • Predefined Ethernet Types— If you choose this option, all predefined Ethernet types contained in the `config.ini` file are associated with the rule, and you should not configure any other parameters.
	  • Enter Ethernet Type—If you choose this option, enter the ethernet type in hexadecimal format.
	• VLAN Identification Number—Enter 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.
	Maximum value is 4095.
	• VLAN Priority—Enter the VLAN priority for the traffic.
	VLAN Priority is matched for Layer 2 traffic only.
	• Source MAC Address—Enter the MAC address of the source device.
	MAC addresses are matched for Layer 2 traffic only.
	• Destination MAC Address—Enter the MAC address of the destination device.
	MAC addresses are matched for Layer 2 traffic only.
	• MPLS Label Value—Enter the MPLS value for Label 1, Label 2, Label 3, Label 4.
	The **MPLS Label Value** fields are displayed only if the **Ethernet Type** is set to MPLS. The MPLS label values are matched.

Field	Description
Layer 3 To enable options for Layer 3, choose **IPv4** or **IPv6** as **Ethertype** under the Layer 2 tab.	

Field	Description

	The options displayed while using Layer 3 are:
	• Source IP Address—Enter the Source IP address of the Layer 3 traffic. This can be one of the following:
	  • The host IP address in the standard IPv4 or IPv6 format
	  • An IPv4 or IPv6 address range
	  • Combination of an address range and standard IP addresses; example: 10.1.1.1, 10.1.1.2-10.1.1.5
	  • Comma-separated discontiguous IP addresses; example: 10.1.1.1, 10.1.1.2, 10.1.1.5
	Note 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.
	• Destination IP Address—Enter the Destination IP address of the Layer 3 traffic. This can be one of the following:
	  • The host IP address in the standard IPv4 or IPv6 format
	  • An IPv4 or IPv6 address range
	  • Combination of an address range and standard IP addresses; example: 10.1.1.1, 10.1.1.2-10.1.1.5
	  • Comma-separated discontiguous IP addresses; example: 10.1.1.1, 10.1.1.2, 10.1.1.5
	Note 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.
	• L4 Protocol—Select a Layer 4 protocol from the drop down list.
	• Advanced Filter—Click the button to enable advanced filtering and check the check-boxes to select the required options. For more details about Advanced Filters, see Advanced Filters.
	• Custom Filter—Click the button to enable custom filtering using User Defined Fields (UDF). Click **Select UDFs** and select a filter in the **Select Custom Filters** window.

Field	Description
Layer 4 To enable options for Layer 4, choose **IPv4** or **IPv6** as **Ethertype** under the Layer 2 tab and choose **TCP** or **UDP** as **L4 Protocol** under the Layer 3 tab.	The options displayed while using Layer 4 are: • Source Port—Select the source port from the drop down list. The options are: • FTP (Data) • FTP (Control) • SSH • Telnet • HTTP • HTTPS • Enter Source Port—Enter the source port. You can enter comma separated single port numbers or a range of source port numbers. **Note** If you enter a range of Layer 4 source ports, you cannot configure ranges of Layer 3 IP addresses or Layer 2 VLAN identifiers. • Destination Port—Select the destination port from the drop down list. The options are: • FTP (Data) • FTP (Control) • SSH • Telnet • HTTP • HTTPS • Enter Destination Port—Enter the source port. You can enter comma separated single port numbers or a range of source port numbers. **Note** If you enter a range of Layer 4 destination ports, you cannot configure ranges of Layer 2 VLAN identifiers or Layer 3 IP addresses.
Layer 7	Not supported.

Step 5 Click **Edit Filter** or **Clone Filter**.

Advanced Filters

Advanced filtering provides multiple options to filter (permit or deny) the traffic based on Ethernet type and attributes such as Acknowledgment, FIN, Fragments , PSH, RST, SYN, DSCP, Precedence, TTL, packet-length, and NVE. Advanced filtering is available for the following Ethernet types and options:

Table 26: Advanced Filtering Support

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

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

The Time to Live (TTL) attributes range 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.

Limitations for using Advanced Filtering

While configuring Advanced Filters, you cannot:

- Configure DSCP and precedence together.
- Configure fragments and ACK or SYN or FIN or PSH or RST together.
- Configure fragments and port numbers with UDP and IPv4 or IPv6 combination.
- Configure precedence and HTTP methods with IPv4 and TCP combination.

Global Configuration

The **Global Configuration** tab displays the devices connected to the NDB controller. New devices added to the NDB controller are displayed here by default.

Note Only *Connected* devices (connection status indicated in green) are displayed here. If a device is added to the NDB controller, but is *not connected* (connection status indicated in red), then, that device is not displayed here. To check the status of a device, see NDB Devices.

A table with the following details is displayed:

Table 27: Global Configuration

Column Name	Description
Device	The device name. This is a hyperlink, click the **Device** name to get the global configuration details of the device.
Loadbalancing	Displays the type of load balancing. The options are: • Symmetric • Non-symmetric
PTP	Displays if PTP is enabled or not. The options are: • Enabled • Disabled
Jumbo MTU	The Jumbo MTU size for the device. Jumbo MTU is the maximum MTU that can be configured for a device.
MPLS Strip	Displays if MPLS stripping is enabled or not on the device. The options are: • Enabled • Disabled
MPLS Filter	Displays if MPLS filtering on the device, is enabled or not. The options are: • Enabled • Disabled
Netflow	Displays if Netflow on the device, is enabled or not. The options are: • Enabled • Disabled

The following actions can be performed from the **Global Configuration** tab:

- **Edit Global Configuration**—For details of the procedure, see Editing Global Configuration for a Device, on page 105.

Editing Global Configuration for a Device

Use this procedure to edit global configuration for a device. You can make global changes to the parameters of a device. For example, the Jumbo MTU value set here, defines the MTU value for an input port of the device.

When a device is created, some basic configurations are created and some default values are set. Use this procedure to change or add one or more parameters for a device.

Before you begin

Create one or more devices. Check the status of the device.

Step 1 Navigate to **Components** > **Global Configuration**.

Step 2 Select a device by checking the check box at the beginning of the row.

Step 3 From the **Actions** drop down menu, select **Edit Global Configuration**.

Step 4 In the **Edit Global Configuration** dialog box, enter the following details:

Table 28: Edit Global Configuration

Field	Description
General	
Device	The device name is displayed based on your earlier selection.
Load Balancing Type Configuration	Select **Symmetric** or **Non-symmetric** from the drop-down list. For details about load balancing, see Symmetric and Non-Symmetric Load Balancing , on page 72.
Hashing Configuration	Select a hashing configuration from the drop-down list. The displayed drop-down list is dynamic and depends on the selected load balancing type.
Hashing Type	Select a hashing type from the drop-down list.
MPLS Configuration	
MPLS Strip Type Configuration	Click the gray button to enable MPLS strip type configuration. The button turns blue and moves to the right. All the MPLS packets from the input ports are stripped of the MPLS header. **Note** On Cisco Nexus 9300-GX Series switches, MPLS strip feature works only after switch reload.

Field	Description
Label Age	Set the time period after which the MPLS labels will age out. This field is available only for select devices. Supported platforms are the following Cisco Nexus Series switches - 93128TX, 3172, 3164, 3232, 3132C-Z.
Enable MPLS Filter Configuration	Click the gray button to enable MPLS filter configuration. The button turns blue and moves to the right. MPLS filter configuration enabled here, is applied to the input port of the device.
sFlow Configuration	
Enable sFlow	Click the gray button to enable Sampled Flow (sFlow). The button turns blue and moves to the right. For details about sFlow, see Sampled Flow , on page 71. Enter the following details: • **Agent IP Address**— Enter the agent ip address. • **Select VRF**—Select a VRF from the drop-down list. • **Collector IP Address** —Enter an IP address for the collector port. • **Collector UDP Port** —Enter the UDP port for the sFlow collector. • **Counter Poll Interval**—Enter a poll interval value for sFlow. • **Max Datagram Size**—Enter the maximum datagram size. • **Max Sampled Size**—Enter the maximum sampled size. • **Sampling Rate** —Enter the data sampling rate. • **Data Sources**—Click **Select Ports** and select the ports by checking the required check boxes and click **Add**. **Note** To verify sflow configuration on a device, use the **show sflow** command.
PTP Configuration	

Field	Description
Enable PTP	Click the gray button to enable PTP and receive updates from the master. The button turns blue and moves to the right. PTP enabled here is used for timestamping in the inputs ports and monitoring tools. For details about PTP, see Precision Time Protocol, on page 71. The following fields are displayed: • **Source IP Address**— Enter the source IP address for receiving PTP updates. • **Ports**—Click **Select Ports** and check the check boxes to select the required ports to which the PTP source IP is connected. **Note** You need to enable PTP for all the devices in the network to ensure PTP clock time synchronization.
Jumbo MTU Configuration	
MTU Value	Enter MTU value; range is 1502 to 9216. Jumbo MTU sets the maximum MTU value the device can accept. MTU size for traffic is typically 1500. To receive traffic with MTU more than 1500, enable this. The MTU value defined here is applied on the incoming traffic on the input ports of a device. Click **Reset to Default** to set the MTU value to the default value of 1500. **Note** MTU value must be an even number, in the specified range.
Netflow Configuration	
Enable Netflow	Click the gray button to enable netflow. The button turns blue and moves to the right. For details about Netflow, see Netflow, on page 71. To define the Netflow parameters, complete the following configurations (in the specified order): • Adding a Record for NetFlow, on page 108 • Adding an Exporter for NetFlow, on page 109 • Adding a Monitor for NetFlow, on page 110 To complete the NetFlow configuration, associate the NetFlow Monitor to an input port. See Adding an Input Port.

Step 5 Click **Edit Global Configuration** .

Adding a Record for NetFlow

Use this procedure to create a NetFlow record.

A flow record defines the keys that NetFlow uses to identify packets and other fields of interest that NetFlow gathers for the flow. The flow record determines the size of the data to be collected for a flow. The key fields are specified with the *match* keyword.

Step 1 Navigate to **Components** > **Global Configuration**.

Step 2 Select a device by checking the check box at the beginning of the row.

Step 3 From the **Actions** drop down menu, select **Edit Global Configuration**.

Step 4 In the **Edit Global Configuration** dialog box, click the gray button to **Enable Netflow**.

Step 5 Click **Add Record** and enter the following details:

Table 29: Add Record

Field	Description
Name	Name of the record.
Description	Description for the record.
Collect	Define the collection parameters. Check the corresponding check box to enable collection based on one or more of the following parameters: • Counter Bytes • Counter Packets • IP Version • Transport TCP Flags • System Uptime First • System Uptime Last
Match	Define the match parameters. The options available are **Layer 2** and **Layer 3/4**. Click either of them to select the match parameters. These parameters are discussed in the subsequent rows.

Field	Description
Layer 2	Check the check box to enable one or more matching Layer 2 parameters. • Mac Source Address • Mac Destination Address • Ethertype • VLAN
Layer 3/4	Check the check box to enable one or more matching Layer 3 and/or Layer 4 parameters. • IP Protocol • IP TOS • Transport Source Port • Transport Destination Port • IPv4 Source Address • IPv4 Destination Address • IPv6 Source Address • IPv6 Destination Address • IPv6 Flow Label • IPv6 Options

Step 6 Click **Add Record**.

Adding an Exporter for NetFlow

Use this procedure to create a NetFlow exporter. The flow exporter configuration defines the export parameters for a flow and specifies reachability information for the remote NetFlow Collector.

A flow exporter contains network layer and transport layer details for the NetFlow export packet.

Step 1 Navigate to **Components** > **Global Configuration**.

Step 2 Select a device by checking the check box at the beginning of the row.

Step 3 From the **Actions** drop down menu, select **Edit Global Configuration**.

Step 4 In the **Edit Global Configuration** dialog box, click the gray button to **Enable Netflow**.

Step 5 Click **Add Exporter** and enter the following details:

Table 30: Add Exporter

Field	Description
Name	Name of the exporter.
Description	Description of the exporter.
Destination	Export destination IP address. Check the corresponding check box to enable collection based on one or more of the following parameters:
Source	Source IP address. Interface on the device through which the flow cache reaches the destination.
UDP Port	UDP port where the NetFlow collector is listening for NetFlow packets. The range is from 1 to 65535.
DSCP	The differentiated services codepoint value. The range is from 0 to 63.
Version	The NetFlow export version. This field cannot be changed. **Note** Cisco NX-OS supports the Version 9 export format.
Option Exporter	Flow exporter statistics resend timer. The range is from 1 to 86400 seconds.
Template Data Timeout	Template data resend timer. The range is from 1 to 86400 seconds.

Step 6 Click **Add Exporter**.

Adding a Monitor for NetFlow

Use this procedure to create a NetFlow monitor.

You can create a flow monitor and associate it with a flow record and a flow exporter. All of the flows that belong to a monitor use the associated flow record to match on the different fields, and the data is exported to the specified flow exporter.

Before you begin

Complete the following configurations:

- Adding a record
- Adding an exporter

Step 1 Navigate to **Components** > **Global Configuration**.

Step 2 Select a device by checking the check box at the beginning of the row.

Step 3 From the **Actions** drop down menu, select **Edit Global Configuration**.

Step 4 In the **Edit Global Configuration** dialog box, click the gray button to **Enable Netflow**.

Step 5 Click **Add Monitor** and enter the following details:

Table 31: Add Monitor

Field	Description
Name	Name of the monitor.
Description	Description of the monitor.
Record	Click **Select Record**. In the **Select Record** window, choose a record by clicking the corresponding radio button. The details of the selected record are displayed on the right. Click **Select**.
Exporter	Click **Select Exporter**. In the **Select Exporter** window, choose an exporter by selecting the corresponding check box. The details of the selected exporter are displayed on the right. Click **Select**. **Note** You can select a maximum of two flow exporters for a monitor

Step 6 Click **Add Monitor**.

Symmetric and Non-Symmetric Load Balancing

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

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

Configuration Type	Hashing Configuration	Platforms	Options
Symmetric	SOURCE_DESTINATION	Nexus 9000 Series (all), N3K-C3164xx, N3K-C32xx	IP, IP-GRE, IP-L4PORT, IP-L4PORT-VLAN, IP-VLAN, L4PORT, MAC
		REST API	IP, IP-GRE, PORT, MAC, IP-ONLY,PORT-ONLY
Non-symmetric	SOURCE, DESTINATION	Nexus 9000 Series (all), N3K-C3164xx, N3K-C32xx	IP, IP-GRE, IP-L4PORT, IP-L4PORT-VLAN, IP-VLAN, L4PORT, MAC
		REST API	IP, IP-GRE, PORT, MAC

Sampled Flow

You can manage Sampled Flow (sFlow) on NDB that are based on NX-API. 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.

See Editing Global Configuration for a Device, on page 105 for configuring sFlow.

Precision Time Protocol

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

PTP is a time synchronization protocol for nodes distributed across a network. Its hardware timestamp feature provides excellent accuracy.

PTP is supported on the following platforms:

- Cisco Nexus 9200 switches
- Cisco Nexus 9300 switches—9300-FX, FX2, EX
- Cisco Nexus 9500 switches—9500-FX, EX
- Cisco Nexus 3548 switches

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

See Editing Global Configuration for a Device, on page 105 for configuring PTP.

Netflow

NetFlow identifies packet flows for ingress IP packets and provides statistics based on these packet flows. NetFlow does not require any change to either the packets themselves or to any networking device.

In order to provide enough free space to monitor flows, the ing-netflow TCAM region is carved to 512 by default on Cisco Nexus 9300-FX platform switches. If more space is required, use the **hardware access-list tcam region ing-netflow size** command to modify the size of this TCAM region, using a multiple of 512.

Netflow is supported on the following platforms:

- Cisco Nexus 9300 switches—9300-FX, FX2, EX

- Cisco Nexus 9500 switches—9500-FX, EX

See Editing Global Configuration for a Device, on page 105 for configuring Netflow.

For more information about Netflow, see *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide.*

Input Ports

The **Input Ports** tab displays details of the inputs ports on the NDB devices.

When an Edge-SPAN or an Edge-TAP or an Remote Source Edge-SPAN port is defined in the NX-API mode of configuration, the **spanning-tree bpdufilter enable** command 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.

Ensure to configure the **spanning-tree bpdufilter enable** command on all the inter-switch ports for Cisco Nexus series switches.

A table with the following details is displayed:

Table 32: Input Ports

Column Name	Description
Device	The device on which the input port is configured. This field is a hyperlink. Click the Device name to view more information about the device. For details and procedure, see Devices chapter.
Port	The port of the device that is configured as an input port. This field is a hyperlink. Click a **Port** to view more details of the port. Additional actions that can be performed from here are: • Editing an Input Port • Remove Configuration—the port is removed as an input port for the device.
In Use	A green tick mark indicates that the input port is in use.
Configuration	The configuration information of the input port (based on the parameters set during Adding an Input Port).

Column Name	Description
Type	Port type. The displayed options are: • Edge port-SPAN • Edge port-TAP • Remote Source Edge-SPAN • Packet Truncation
Span Destination	Details of the span destination. If the port is connected to ACI, then the DN value is displayed; if the port is connected to a production switch (NX-OS), then the device ID (of the production switch) with interface(s) are displayed.
Created By	The user who created the the input port.
Modified By	The user who last modified the input port.

The following actions can be performed from the **Input Ports** tab:

- **Add Input Port** —Use this to add a new input port. See Adding an Input Port for details about this task.
- **Delete Input Port** —Select the required input port by checking the check box which is available at the beginning of the row. Click **Actions** > **Delete Input Port(s)**. The selected port(s) is deleted.

Note *In Use* input ports cannot be deleted.

If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a device.

Adding an Input Port

Use this procedure to create an input port.

Input port of a device is the port through which traffic enters the packet broker network and is directed to the monitoring tool.

Before you begin

Add one or more devices.

Some of the input port parameters are defined at the device-level using the **Global Configuration** tab. To define these parameters (listed below), see Editing Global Configuration for a Device.

- PTP
- Netflow
- MPLS Filtering

- Jumbo MTU

Step 1 Navigate to **Components** > **Input Port Configuration**.

Step 2 From the **Actions** drop-down list, select **Add Input Port**.

Step 3 In the **Add Input Port** dialog-box, enter the following details:

Table 33: Add Input Port

Field	Description
General	
Device	To select a device on which the input port is being configured. Click **Select Device** . From the **Select Device** window, select a radio button and choose a device. Click **Select**.
Port(s)	To select a port to be configured as the input port. Click **Select Port**. From the **Select Port** window, select the required port(s). Click **Select**.
Port Type	Select from the drop-down list to define the input port type. The options are: • **Edge Port - SPAN** —creates an edge-port for incoming traffic from a configured session of the production switch . • **Edge Port- TAP**—creates an edge port for incoming traffic from a physical device on an ISL. • **Remote Source Edge - SPAN** —creates an edge-port for incoming traffic from a configured remote session of the production switch.
Port Description	Enter a description for the port.
VLAN ID (QinQ Supported)	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. **Note** After an interface is configured with Q-in-Q, do not configure VLAN filters for the Q-in-Q configured interface.
Block-Tx	Check the check-box to block the traffic that is being transmitted from the input ports. **Note** Only unicast and multicast traffic is blocked.

Field	Description
Drop ICMP v6 Neighbour Solicitation	Check the check-box to drop all ICMP traffic. By default, all the ICMP traffic is blocked for 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.
Enable Timestamp Tagging	Check the check-box to append the timestamp tag on packets using the Timestamp Tagging feature. For Nexus 9300-EX and 9200 series switches, this feature is applicable for Edge-SPAN and Edge-TAP ports. 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. **Note** If PTP is not enabled for the device using Global Configuration, then this option is grayed out.
Enable MPLS Filtering	Check the check-box to enable MPLS filtering. **Note** If MPLS filtering is not enabled for the device using Global Configuration, then this option is grayed out.
Apply Jumbo MTU	Check the check-box to enable the set Jumbo MTU value on this port. **Note** If Jumbo MTU is not configured for the device using Global Configuration, then this option is grayed out.
Netflow Monitor	Select an option from the drop-down list. The monitor names created at the Global Configuration level are listed here. **Note** If NetFlow is not enabled for the device using Global Configuration, then this option is grayed out.

The unique fields displayed for each **Port Type** are discussed below.

a) (Only for **Port Type**—Edge Port-SPAN) Enter the following details:

Field	Description
Destination Device Type	This is the source for the input ports (Span Destination). Select the required option from the drop down list. The options are: • ACI • NX-OS Device The options for each of the above are discussed in the subsequent rows.
Fields for **Destination Device Type : ACI** **Note** You must add an APIC/ ACI device before you configure SPAN destination.	
Span Destination Name	Enter a name for Span Destination.
Pod	Select a pod.
Node	Select a node.
Port	Select a port.
MTU	Set an MTU value for the span destination of APIC.
Fields for **Destination Device Type: NX-OS Device** **Note** You must add an NX-OS device before you configure SPAN destination.	
Span Destination Device	Click **Select Device** and select a device.
Span Destination Port	Click **Select Port** and select a port.

b) No unique fields are dispalyed, when you select **Port Type** as Edge-Port TAP.

c) (Only for **Port Type**—Remote Source Edge-SPAN) Enter the following details:

Note You can configure a maximum of four Remote Source Edge-SPAN ports, to receive traffic from a remote source.

Field	Description
Remote Input Termination Session	
ERSPAN ID	Enter an ERSPAN ID. Range is from 1 to 1023. The ERSPAN id entered here is matched with the source session id in the remote source.
Use Loopback Interface	Check the check-box to use a loopback interface.

Field	Description
Loopback	Click **Select Loopback** to select a loopback interface. If there are no configured loopback interfaces, click **Add Loopback**. See Configuring Loopback. Use a loopback interface to have more than one remote input port. Traffic from an L3 interface reaches the loopback interface and from there the session destination port. If the first remote source edge span input port was created with a loopback, then the following Remote Source Edge-SPAN ports must also be configured with the same loopback interface. If the first remote source edge span input port was created without a loopback, then the following Remote Source Edge-SPAN ports must also be configured without a loopback interface.
Session Destination	Click **Select Destination Port** and select a destination port (on the NDB device).
Remote Input Session	
Remote Input Port	Click **Remote Input Port** and select a remote input port (on the NDB device). **Note** Only one remote input port can be configured for the traffic reaching the Remote Source Edge-SPAN ports. If you have configured a loopback interface, then, the remote input ports can be different for each of the Remote Source Edge-SPAN ports.
IP Address	Enter an IP address. IP address entered here is the IP address of the remote source port to which the packets reach over L3 network. You need to enter this value only when configuring the first Remote Source Edge-SPAN port. For the next three ports that you configure, this field is grayed out as the same IP address is applied to all the four sessions with Remote Source Edge-SPAN ports.
Destination Device Type	Select the device type from the drop down list. For Remote Source Edge-SPAN ports, the supported destination type is ACI.
Span Destination ACI Fabric	Click **Select ACI Fabric** and select an ACI fabric.
Span Destination Name	Enter a name for the span destnation.
Tenant	Click **Select Tenant** to select a tenant.
Application Profile	Click **Select Application Profile** to select an application profile.
EPG	Click **Select EPG** to select an EPG.

Field	Description
Source IP Address	Enter the source IP address. This IP address is the base IP address of the IP subnet of the source packets.
Destination IP Address	This field is automatically populated. The IP address populated here is the same address that you entered as the IP address of the **Remote Input Port**. **Note** For APIC/ ACI devices, this is the destination port (remote input port), and hence called destination IP.
Flow ID	This field is automatically populated. Flow ID is the flow identifier of the SPAN packet. It is matched with the ERSPAN ID earlier specified for the Remote Source Edge-SPAN port.
TTL	Enter a TTL value. Default value is 64 hops.
DSCP	Select a DSCP value from the drop-down list.
MTU	Enter an MTU value for the span destination port. Range is from 64 to 9216.

Step 4 Click **Add Input Port**.

Editing an Input Port

Use this procedure to edit an input port.

Before you begin

Add one or more input ports.

Step 1 Navigate to **Components** > **Input Ports**.

Step 2 In the displayed table, click a **Port**.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Port**.

Table 34: Edit Input Port

Field	Description
General	

Field	Description
Device	The device name on which the input port is configured. This field cannot be edited.
Port(s)	The port configured as an input port. This field cannot be edited.
Port Type	Select from the drop-down list to define the input port type. The options are: • **Edge Port - SPAN** —creates an edge-port for incoming traffic from a configured session of the production switch . • **Edge Port- TAP**—Creates an edge port for incoming traffic from a physical device on an ISL. • **Remote Source Edge - SPAN** —creates an edge-port for incoming traffic from a configured remote session of the production switch.
Port Description	Enter a description for the port.
VLAN ID (QinQ Supported)	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. **Note** After an interface is configured with Q-in-Q, do not configure VLAN filters for the Q-in-Q configured interface.
Block-Tx	Check the check-box to block the traffic that is being transmitted from the input ports. **Note** Only unicast and multicast traffic is blocked.
Drop ICMP v6 Neighbour Solicitation	Check the check-box to drop all ICMP traffic. By default, all the ICMP traffic is blocked for 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.

Field	Description
Enable Timestamp Tagging	Check the check-box to append the timestamp tag on packets using the Timestamp Tagging feature. For Nexus 9300-EX and 9200 series switches, this feature is applicable for Edge-SPAN and Edge-TAP ports. 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. **Note** If PTP is not enabled for the device using Global Configuration, then this option is grayed out.
Enable MPLS Filtering	Check the check-box to enable MPLS filtering. **Note** If MPLS filtering is not enabled for the device using Global Configuration, then this option is grayed out.
Apply Jumbo MTU	Check the check-box to enable the set Jumbo MTU value on this port. **Note** If Jumbo MTU is not configured for the device using Global Configuration, then this option is grayed out.
Netflow Monitor	Select an option from the drop-down list. The monitor names created at the Global Configuration level are listed here. **Note** If NetFlow is not enabled for the device using Global Configuration, then this option is grayed out.
Destination Device Type Applicable only when the Port Type is, **Edge Port - SPAN**.	This is the source for the input ports (Span Destination). Select the required option from the drop-down list. The options are: • ACI • NX-OS The options for each of the above are discussed in the subsequent rows.
Destination Device Type: ACI **Note** You must add an APIC/ ACI device before you configure SPAN destination.	
Span Destination ACI Fabric	Click **Select ACI Fabric**. and select an ACI Fabric. Click **Select**.
Span Destination Name	Enter a name for Span Destination.
Pod	Select a pod.
Node	Select a node.

Field	Description
Port	Select a port.
MTU	Set an MTU value for the span destination of APIC.
Destination Device Type: NX-OS Device **Note** You must add an NX-OS device (production device) before you configure SPAN destination.	
Span Destination Device	Click **Select Device** and select a device in the Select Device window.
Span Destination Port	Click **Select Port** and select a port in the Select Port window.
Options available when **Port Type** is **Remote Source Edge - SPAN**. **Note** You can configure a maximum of four Remote Source Edge-SPAN ports, to receive traffic from a remote source. Enter the following **Remote Input Termination Session** details:	
ERSPAN ID	Enter an ERSPAN ID. Range is from 1 to 1023. The ERSPAN id entered here is matched with the source session id in the remote source.
Use Loopback Interface	Check the check-box to use a loopback interface.
Loopback	Click **Select Loopback** to select a loopback interface. If there are no configured loopback interfaces, click **Add Loopback**. See Configuring Loopback. Use a loopback interface to have more than one remote input port. Traffic from an L3 interface reaches the loopback interface and from there the session destination port. If the first remote source edge span input port was created with a loopback, then the following Remote Source Edge-SPAN ports must also be configured with the same loopback interface. If the first remote source edge span input port was created without a loopback, then the following Remote Source Edge-SPAN ports must also be configured without a loopback interface.
Session Destination	Click **Select Destination Port** and select a destination port (on the NDB device).
Enter the following **Remote Input Session** details:	
Remote Input Port	Click **Remote Input Port** and select a remote input port (on the NDB device). **Note** Only one remote input port can be configured for the traffic reaching the Remote Source Edge-SPAN ports. If you have configured a loopback interface, then, the remote input ports can be different for each of the Remote Source Edge-SPAN ports.

Field	Description
IP Address	Enter an IP address. IP address entered here is the IP address of the remote source port to which the packets reach over L3 network. You need to enter this value only when configuring the first Remote Source Edge-SPAN port. For the next three ports that you configure, this field is grayed out as the same IP address is applied to all the four sessions with Remote Source Edge-SPAN ports.
Destination Device Type	Select the device type from the drop-down list. For Remote Source Edge-SPAN ports, the supported destination type is ACI.
Span Destination ACI Fabric	Click **Select ACI Fabric** and select an ACI fabric.
Span Destination Name	Enter a name for the span destnation.
Tenant	Click **Select Tenant** to select a tenant.
Application Profile	Click **Select Application Profile** to select an application profile.
EPG	Click **Select EPG** to select an EPG.
Source IP Address	Enter the source IP address. This IP address is the base IP address of the IP subnet of the source packets.
Destination IP Address	This field is automatically populated. The IP address populated here is the same address that you entered as the IP address of the **Remote Input Port**. **Note** For APIC/ ACI devices, this is the destination port (remote input port), and hence called destination IP.
Flow ID	This field is automatically populated. Flow ID is the flow identifier of the SPAN packet. It is matched with the ERSPAN ID earlier specified for the Remote Source Edge-SPAN port.
TTL	Enter a TTL value. Default value is 64 hops.
DSCP	Select a DSCP value from the drop-down list.
MTU	Enter an MTU value for the span destination port. Range is from 64 to 9216.

Step 4 Click **Edit Input Port**.

Configuring Loopback

Use this procedure to configure a loopback for the Remote source edge span input port.

Step 1 Navigate to **Inputs Ports** > **Actions** > **Add Input Ports**.

Step 2 Select **Port Type** as Remote Source Edge Span Port and select the **Use Loopback Interface** check-box to select a loopback interface.

Step 3 Click **Configure Loopback** to create a new loopback interface.

In the **Configure Loopback** dialog-box, enter the following details:

Table 35: Configure Loopback

Field	Description
General	
Loopback Id	Enter a loopback ID.
IP Address	Enter the loopback IP address.

Step 4 Click **Configure Loopback**.

Monitoring Tools

The **Monitoring Tools** tab displays details of the monitoring tool ports of NDB devices. Traffic from the monitoring tool port of an NDB device is directed to the monitoring tool.

A table with the following details is displayed:

Table 36: Monitoring Tools

Column Name	Description
Status	Status is defined using two columns. First column indicates the traffic on the monitoring tool. • Green—indicates that the monitoring tool is currently carrying traffic. • Yellow—indicates that the monitoring tool is currently not carrying traffic. Second column indicates the status of the link between the monitoring tool port and monitoring tool. If the link between the monitoring tool port and the monitoring tool is up, then it is green in colour. • Green—indicates that the link is up and running. • Red—indicates that the link is down. • Yellow—indicates that the link is administratively down.
Monitoring Tool	The monitoring tool name. This field is a hyperlink. Click the **Monitoring Tool** name. A new pane is displayed on the right which has more details about the monitoring tool. The following additional actions can be performed from here: • Editing a Monitoring Tool, on page 129
Port	Monitoring tool port (with the device). Click the **Port** name to get more details of the port. The following additional actions can be performed from here: • Editing a Monitoring Tool, on page 129
Type	The type of monitoring tool. The option are: • Local Monitoring Tool—port that resides on the NDB device in the local network (L2 port). • Remote Monitoring Tool—port that resides outside the local network and reachable over L3 network.
In Use	If the monitoring tool port is in use, a *green tick mark* is displayed; else it is left blank.

Column Name	Description
Packet Truncation	If packet truncation is enabled on the monitoring tool port, a *green tick mark* is displayed; else it is left blank.
Block Rx	If incoming traffic from the monitoring tool to the monitoring tool port (on the NDB device) is blocked, then **Yes** is displayed.
Created By	The user who created the monitoring tool.
Last Modified By	The user who last modified the monitoring tool.

The following actions can be performed from the **Monitoring Tools** tab:

- **Add Monitoring Tool**—Use this to add a new monitoring device. See Adding a Monitoring Tool for details about this task.
- **Delete Monitoring Tool(s)**—Select the required device by checking the check box which is available at the beginning of the row. The selected device(s) are deleted. Click **Actions** > **Delete Monitoring Tool(s)**. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a device.

Note An *In use* monitoring tool cannot be deleted.

Adding a Monitoring Tool

Use this procedure to add a monitoring tool port. You can create a:

- Local Monitoring Tool—a port that resides on the NDB device in the local network (L2 port).
- Remote Monitoring Tool—a port that resides outside the local network and reachable over L3 network.

You can create a packet truncation port (used to block the ingress traffic) to be associated with the monitoring tool which is the egress port for a packet.

Before you begin

Restrictions:

- You cannot use more than one remote delivery port per switch per connection.
- Remote monitoring tool involving inter switched links is restricted to only one connection per ISL.
- If the monitoring tool is used with a packet truncation interface, then, 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 any NDB device. To change the port Layer 2 status to Up, you need to connect to another non-NDB device create a loopback using a third party loopback fiber optic.

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

Step 1 Navigate to **Components** > **Monitoring Tools**.

Step 2 From the **Actions** drop-down list, select **Add Monitoring Tool**.

Step 3 In the **Add Monitoring Tool** dialog box, enter the following details:

Table 37: Add Monitoring Tool

Field	Description
General	
Monitoring Tool Name	Enter a name for the monitoring tool name.
Device Name	Click **Select Device**. From the displayed list of devices, select a device using the radio button. The device details are displayed on the right. The monitoring tool port resides on this device. Click **Select Device**.
Port	Click **Select Port**. In the **Select Interface** window that opens, select a port by using the radio button. The displayed interfaces depends on the selected device. Click **Select**. The selected port is marked as the monitoring tool port. The traffic is redirected to the monitoring tool from here.
Port Description	Enter a description for the port.
Local Monitor Tool	Select the radio button to select a local monitor device. By selecting this option, a monitoring device is from the local network. The following options are displayed for local monitor device (discussed in detail in the rows below): • Block Rx • Block ICMPv6 Neighbour Solicitation • Enable Timestamp Tagging • Packet Truncation • Enable Timestamp Strip • Apply Jumbo MTU

Field	Description
Block Rx	Blocks traffic from the monitoring tool (to the monitoring tool port on the NDB device). This option is selected by default. You can turn this option off by unchecking the check box. **Note** Rx traffic is blocked using Unidirectional Ethernet for Cisco N9K-95xx switches with N9K-X97160YC-EX line card (NX-OS 9.3(3) or later).
Block ICMPv6 Neighbour Solicitation	Blocks ICMP traffic from the monitoring tool (to the monitoring tool port on the NDB device). This option is selected by default. You can turn this option off by unchecking the check box. Supported on Nexus 9300-EX and 9200 switches. For the rest of Nexus 9000 Series switches, user has to manually enable this feature to deny or block all the ICMP traffic.
Enable Timestamp Tagging	Check the check box to enable timestamp tagging. A timestamp tag is appended to all the outgoing packets of the monitoring tool port. You can configure this feature on a single device or multiple devices. To configure timestamp tagging, ensure that PTP is enabled on the device. You need to enable timestamp tagging on the monitoring device(s) and edge ports. If timestamp tagging is not configured on either side of the connection, Edge-SPAN/Edge-TAP and the monitor tools, then packets are not tagged with timestamp.
Packet Truncation	Check the check box to enable packet truncation and enter the MTU size. Packet truncation discards bytes from an incoming packet based on the MTU size. This is done in order to send only the the required traffic to the monitoring tool port. This is achieved by redirecting the traffic from the input port to the packet truncation port. The truncated packets from the packet tuncation port reach the monitoring tool. To set a packet truncation port, click **Select Packet Truncation Port**. See Adding a Packet Truncation Port, on page 132 for the detailed procedure.
Enable Timestamp Strip	Check the check box to enable timestamp strip. This removes the timestamp tag from the source packets.
Apply Jumbo MTU	Check the check box to enable jumbo MTU. Jumbo MTU sets a bigger packet size for the device. Enable **Jumbo MTU** in **Global Configuration** to apply the set Jumbo MTU size for a port of the device.

Field	Description
Remote Monitor Tool	Select the radio button to select a remote monitor device. By selecting this option, a monitoring device from a remote network is enabled. The following options are displayed for remote monitor device (discussed in detail in the rows below): • Block Rx • Interface IP • Destination IP • ERSPAN ID
Interface IP	IP address to be assigned to the monitoring tool port.
Destination IP	IP Address where ERSPAN terminates and should be reachable from the selected port.
ERSPAN ID	Enter ERSPAN id; range is 1 to 1023. You can use a device outside the network as a monitoring device using the Encapsulated Remote Switch Port Analyzer (ERSPAN) Source Session feature for Cisco Nexus 9300 FX and EX series switches.

Step 4 Click **Add Monitoring Tool**.

Editing a Monitoring Tool

Use this procedure to edit the parameters of a monitoring tool.

Before you begin

Add one or more monitoring tools.

Step 1 Navigate to **Components** > **Monitoring Tools**.

Step 2 In the displayed table, click a **Monitoring Tool** name.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Monitoring Tool**.

Step 4 In the **Edit Monitoring Tool** dialog box, the current information of the monitoring tool is displayed. Modify these fields, as required:

Table 38: Edit Monitoring Tool

Field	Description
General	
Monitoring Tool Name	Monitoring tool name is displayed; this cannot be edited.
Device Name	The device on which the monitoring tool port resides.
Port	The monitoring tool port.
Port Description	Enter a description for the port.
Local Monitor Tool	Select the radio button to select a local monitor device. By selecting this option, a monitoring device is from the local network. The following options are displayed for local monitor device (discussed in detail in the rows below): • Block Rx • Block ICMPv6 Neighbour Solicitation • Enable Timestamp Tagging • Packet Truncation • Enable Timestamp Strip • Apply Jumbo MTU
Block Rx	Blocks traffic from the monitoring tool (to the monitoring tool port on the NDB device). This option is selected by default. You can turn this option off by unchecking the check box. **Note** Rx traffic is blocked using Unidirectional Ethernet for Cisco N9K-95xx switches with N9K-X97160YC-EX line card (NX-OS 9.3(3) or later).
Block ICMPv6 Neighbour Solicitation	Blocks ICMP traffic from the monitoring tool (to the monitoring tool port on the NDB device). This option is selected by default. You can turn this option off by unchecking the check box. Supported on Nexus 9300-EX and 9200 switches. For the rest of Nexus 9000 Series switches, user has to manually enable this feature to deny or block all the ICMP traffic.

Field	Description
Enable Timestamp Tagging	Check the check box to enable timestamp tagging. A timestamp tag is appended to all the outgoing packets of the monitoring tool port. You can configure this feature on a single device or multiple devices. To configure timestamp tagging, ensure that PTP is enabled on the device. You need to enable timestamp tagging on the monitoring device(s) and edge ports. If timestamp tagging is not configured on either side of the connection, Edge-SPAN/Edge-TAP and the monitor tools, then packets are not tagged with timestamp.
Packet Truncation	Check the check box to enable packet truncation and enter the MTU size. If a packet truncation port was not configured during the addition of the monitoring tool, the **Select Packet Truncation Port** is disabled.
Enable Timestamp Strip	Check the check box to enable timestamp strip. This removes the timestamp tag from the source packets.
Apply Jumbo MTU	Check the check box to enable jumbo MTU. Jumbo MTU sets a bigger packet size for the device. Enable **Jumbo MTU** in **Global Configuration** to apply the set Jumbo MTU size for a port of the device.
Remote Monitor Tool	Select the radio button to select a remote monitor device. By selecting this option, a monitoring device from a remote network is enabled. The following options are displayed for remote monitor device (discussed in detail in the rows below): • Block Rx • Interface IP • Destination IP • ERSPAN ID
Interface IP	IP address to be assigned to the monitoring tool port.
Destination IP	IP Address where ERSPAN terminates and should be reachable from the selected port.
ERSPAN ID	Enter ERSPAN id; range is 1 to 1023. You can use a device outside the network as a monitoring device using the Encapsulated Remote Switch Port Analyzer (ERSPAN) Source Session feature for Cisco Nexus 9300 FX and EX series switches.

Step 5 Click **Save**.

Adding a Packet Truncation Port

Use this procedure to create a packet truncation port. A packet truncation port serves as an input port for the monitoring tool port. Hence, the created packet truncation port is listed as an input port, and unused packet truncation ports can be deleted from the Input Ports tab.

Before you begin

Packet truncation involves discarding bytes from a packet starting at a specified byte position. All the data after the specified byte position is discarded. Packet truncation is required when the main information of interest is in the header of a packet or in the initial part of the packet.

Note Packet truncation is supported for unicast traffic (not supported for multicast traffic).

Table 39: Support for Packet Truncation

EX Chassis	FX Chassis	Nexus 9364C, Nexus 9332C	Nexus 9336C-FX2	EOR switches with -EX or -FX LCs
MTU size range is 320 to 1518 bytes	MTU size range is 64 to 1518 bytes	MTU size range is 64 to 1518 bytes	MTU size range is 64 to 1518 bytes	Depends on LC

Step 1 Navigate to **Components** > **Monitoring Tools**.

Step 2 From the **Actions** drop-down list, select **Add Monitoring Tool**.

Step 3 Select a device and port and check the **Packet Truncation** check-box to enable packet truncation.

Step 4 Click **Select Packet Truncation Port**.

Step 5 In the **Select Packet Truncation Port** window that is displayed, click **Add Packet Truncation Port**.

Step 6 In the **Add Packet Truncation** dialog box, enter the following details:

Table 40: Add Packet Truncation

Field	Description
General	
Device	The device name is displayed.
Port	Click **Select Port**. In the **Select Port** window, select a port by selecting a radio button. Click **Submit**.
Port Type	Packet Truncation port is selected by default.

Field	Description
Port Description	Port description for the truncation port.
Drop ICMPv6 Neighbour Solicitation	Blocks ingress ICMP traffic for the packet truncation port. This option is selected by default. You can turn this option off by unchecking the check box.

Step 7 Click **Add** .

Port Groups

The **Port Groups** tab has the following subtabs:

- **Input Port Group**—input ports of a device (or across devices) are grouped together to form an input port group. See Input Port Group for more details.
- **Monitoring Tool Group**—monitoring tool ports of a device (or across devices) are grouped together to form a monitoring tool group. See Monitoring Tool Group for more details.

Input Port Group

Input ports of a device (or different devices) are grouped together to form a port group. Port groups can be a combination of the edge-span and the edge-tap ports across different devices. While creating a connection, instead of choosing input ports separately, you can select more than one input port simultaneously by grouping them.

A table with the following details is displayed:

Table 41: Input Port Group

Column Name	Description
Input Port Group Name	Input port group name. This field is a hyperlink. Click the **Input Port Group Name**. A new pane is displayed on the right which provides more information about the input port group. Additional tasks that can be performed from here are: • Editing an Input Port Group
Description	Description of the input port group.
Associated Connections	The connection(s) associated with the group.
Member(s)	The number of member input ports of the group.
Created By	User who created the group.

Column Name	Description
Last Modified By	User who last modified the group.

The following actions can be performed from the **Input Port Group** tab:

- **Add Input Port Group**—Use this to add a new input port group. SeeAdding an Input Port Group for details about this task.
- **Delete Input Port Group(s)**—Select the input port group(s) to be deleted by checking the check box which is available at the beginning of the row and then click **Actions** > **Delete Input Port Group**. The selected input port group(s) is deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select an input port group.

Adding an Input Port Group

Use this procedure to create an input port group.

While creating a connection, instead of choosing input ports separately, you can select more than one input port simultaneously by grouping them.

Before you begin

Create one or more devices.

Step 1 Navigate to **Components** > **Port Groups** > **Input Port Group**.

Step 2 From the **Actions** drop-down list, select **Add Input Port Group**.

Step 3 In the **Add Input Port Group** dialog box, enter the following details:

Table 42: Add Input Port Group

Field	Description
General	
Group Name	Enter a name for the input port group.
Description	Enter a description for the group.
Select Node	From the *All Nodes* box, select a device by clicking a radio button.
Choose Port(s)	Ports that are configured as inputs ports, are displayed. Click a port to select it. You can click **Add All** to select all the (input) ports of a device.
Selected Port(s)	The selected ports are populated here. These are the ports which will be part of the group. If you want to delete a port, click the cross-mark (x) displayed next to the port. You can click **Remove All** to delete all the selected ports.

Step 4 Click **Add Input Port Group**.

Editing an Input Port Group

Use this procedure to edit the parameters of an input port group.

Before you begin

Create one or more input port groups.

Step 1 Navigate to **Components** > **Port Groups** > **Input Port Group**.

Step 2 In the displayed table, click an **Input Port Group** name.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Input Port Group**.

Step 4 In the **Edit Input Port Group** dialog box, the current information of the group is displayed. Modify these fields, as required:

Table 43: Edit Input Port Group

Field	Description
General	
Group Name	Input port group name.
Description	Description of the group.
Select Node	From the *All Nodes* box, select a device by clicking a radio button.
Choose Port(s)	Ports configured as input ports, are displayed. Click a port to select it. You can click **Add All** to select all the ports of a device.
Selected Port(s)	The selected ports are populated here. These are the ports which will be part of the group. If you want to delete a port, click the cross-mark (x) displayed next to the port. You can click **Remove All** to delete all the selected ports.

Step 5 Click **Edit Input Port Group**.

Monitoring Tool Group

Monitoring tool ports grouped together across devices form a monitoring tool group.

A table with the following details is displayed:

Table 44: Monitoring Tool Group

Column Name	Description
Monitoring Tool Group Name	Monitoring tool group name. This field is a hyperlink. Click the **Monitoring Tool Group Name**. A new pane is displayed on the right which provides more information about the monitoring tool group. Additional tasks that can be performed from here are: • Editing a Monitoring Tool Group
Description	Description of the monitoring tool group.
Associated Connections	Connections using the monitoring tool group.
Member(s)	The number of member monitoring tool ports of the group.
Created By	User who created the group.
Last Modified By	User who last modified the group.

The following actions can be performed from the **Monitoring Tool Group** tab:

- **Add Monitoring Tool Group**—Use this to add a new monitoring tool group. See Adding a Monitoring Tool Group for details about this task.
- **Delete Monitoring Tool Group(s)**—Select the tool group(s) to be deleted by checking the check box which is available at the beginning of the row and then click **Actions** > **Delete Monitoring Tool Group(s)**. The selected tool group(s) is deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a tool group.

Adding a Monitoring Tool Group

Use this procedure to create a monitoring tool group.

Before you begin

Create one or more monitoring tools.

Step 1 Navigate to **Components** > **Port Groups** > **Monitoring Tool Group**.

Step 2 From the **Actions** drop-down list, select **Add Monitoring Tool Group**.

Step 3 In the **Add Monitoring Tool Group** dialog box, enter the following details:

Table 45: Add Monitoring Tool Group

Field	Description
General	

Field	Description
Group Name	Enter a name for the monitoring tool group.
Description	Enter a description for the group.
Select Node	From the *All Nodes* box, select a device by clicking a radio button.
Choose Port(s)	Ports that are configured as monitoring tool ports, are displayed. Click a port to select it. You can click **Add All** to select all the (monitoring) ports of a device.
Selected Port(s)	The selected ports are populated here. These are the ports which will be part of the group. If you want to delete a port, click the cross-mark (x) displayed next to the port. You can click **Remove All** to delete all the selected ports.

Step 4 Click **Add Monitoring Tool Group**.

Editing a Monitoring Tool Group

Use this procedure to edit the parameters of a monitoring tool group.

Before you begin

Create one or more monitoring tool groups.

Step 1 Navigate to **Components** > **Port Groups** > **Monitoring Tool Group**.

Step 2 In the displayed table, click a **Monitoring Tool Group** name.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Monitoring Tool Group**.

Step 4 In the **Edit Monitoring Tool Group** dialog box, the current information of the group is displayed. Modify these fields, as required:

Table 46: Edit Monitoring Tool Group

Field	Description
General	
Group Name	Name of the monitoring tool group.
Description	Description for the group.
Select Node	From the *All Nodes* box, select a device by clicking a radio button.

Field	Description
Choose Port(s)	Ports that are configured as monitoring tool ports, are displayed. Click a port to select it. You can click **Add All** to select all the (monitoring) ports of a device.
Selected Port(s)	The selected ports are populated here. These are the ports which will be part of the group. If you want to delete a port, click the cross-mark (x) displayed next to the port. You can click **Remove All** to delete all the selected ports.

Step 5 Click **Edit Monitoring Tool Group**.

Span Destination

The **Span Destination** tab displays details of the span ports connected to the input ports of NDB devices. Span destination is the traffic source (from ACI or NX-OS device) for the input ports. An L2 span destination (local) is created on an edge span port and an L3 span destination (remote) is created on a remote edge span port.

A table with the following details is displayed:

Table 47: Span Destination

Column Name	Description
Name	Name of the span destination port.
Destinations	Indicates if the span destination is on an ACI device or an NX-OS device.
Input Port	Input port of the NDB device which is connected to the span destination.
Input Port Type	Input port type. The options are: • Edge-SPAN port • Remote Source Edge-SPAN port
Span Device	Span device (traffic source). The options are: • AC—ACI device/ APIC • PS—NX-OS device (production switch)
Created By	The user who created the span destination.
Last Modified By	The user who last modified the span destination.

The following actions can be performed from the **Span Destinations** tab:

- **Delete Span Destination(s)**—Select the span destination to be deleted by checking the check box which is available at the beginning of the row and then click **Actions** > **Delete Span Destination(s)**. The selected span destination is deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a span destination.

Note For adding a Span Destination, see Adding an Input Port procedure. A span destination (on an ACI/ NX-OS device) is connected to the input port of an NDB device. You can add a SPAN destination only after either an ACI/ NX-OS device has been successfully added to the network.

For APIC SPAN destination, when you configure an input port as an Edge-SPAN port and the port is connected to the ACI side, you can select the pod, the node, and the port from the ACI side and set the port as SPAN destination. For NX-OS (production switch) SPAN destination, when you configure an input port as an Edge-SPAN port and the port is connected to an NX-OS device, select a node and port on the NX-OS device, and set the port as SPAN destination.

User Defined Field

The **User Defined Field (UDF)** tab displays details of UDFs on NDB devices.

A UDF enables you to filter packets based on an offset value. An offset value in a packet can be matched within 128 bytes.

By default, NDB controller generates two UDFs named *udfInnerVlan* and *udfInnerVlanv6*, used to match the inner VLAN in the ISL ports.

Table 48: UDF Support Matrix

UDF Ethertype	Platform
IPv4	Cisco Nexus 9200 and 9300 series switches
IPv6	Cisco Nexus 93xx EX/FX , 95xx EX/FX , 92xx series switches

Table 49: Qualifying Regions for UDF

Platform	UDF Qualifying TCAM Region
Cisco Nexus 9200, 9300-EX/9300-FX and 9500-EX/9500-FX series switches	ing-ifacl
Other platforms	ifacl

A table with the following details is displayed:

Table 50: User Defined Field

Column Name	Description
UDF	The UDF name. This field is a hyperlink. Click the UDF name and a new pane is displayed on the right with more details of the UDF. Additional tasks that can be performed from here are: • Editing or Cloning a User Defined Field .
Type	Displays **IPv4** or **IPv6**.
Keyword	Displays **Packet-Start** or **Header**.
In Use	A green tick-mark indicates that the UDF is currently in use.
Offset	The set offset value.
Length	Length (number of bytes) in a packet that are matched.
Devices	Number of devices a UDF is applied on.
Created By	User who created the UDF.
Last Modified By	User who last modified the UDF.

The following actions can be performed from the **User Defined Field** tab:

- **Add UDF**—Use this to add a new UDF. See Adding a User Defined Field for details about this task.
- **Delete UDF(s)**—Select a UDF by checking the check box which is available at the beginning of the row. Click **Actions** > **Delete UDF(s)**.

  If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a UDF.

Note Any change in a UDF definition requires device reboot.

Adding a User Defined Field

Use this procedure to add a user defined field.

Some protocols are not supported by default in some NX-OS devices. To support filtering of packets on these devices, use UDFs.

Note UDF can match a maximum of two offset bytes. To filter three consecutive bytes in a packet, we need to stack the UDFs. Create two UDFs, one after the other using the NDB GUI. The second UDF is called the stacking UDF.

Step 1 Navigate to **Components** > **User Defined Field**.

Step 2 From the **Actions** drop down list, select **Add UDF**.

Step 3 In the **Add UDF** dialog box, enter the following details:

Table 51: Add UDF

Field	Description
UDF Name	Name of the UDF.
Type	Select from the drop down list. The options are: • IPv4 • IPv6
Keyword	Select from the drop down list. The options are: • Header • Packet-Start If the **Header** option is selected, the Inner (Offset base from inner/outer header) and L3/L4 (Offset base from L3/L4 header) is enabled. If **Packet-Start** is selected, the offset base starts from the packet.
Header	Select from the drop down list. The options are: • Inner • Outer This field is enabled only when the selected keyword is **Header**. Enables you to select the base offset value from the inner or outer Header.
Layer	Select from the drop down list. The options are: • Layer 3 • Layer 4 This field is enabled only when the selected keyword is **Header** . Enables you to specify if the offset start value is from Layer 3 or Layer 4.

Field	Description
Offset	Set the byte **Offset** value; range is from 0 to 127. Filtering of packets is done based on the set offset value in UDF, packets are matched from the set offset value.
Length	Length (number of bytes) of a packet that are matched; range is from 1 to 2. The length depends on the offset value, if it is set to 1; then one byte starting with the set offset byte is matched.
Devices	Device on which the UDF is being created. Click **Select Devices**. In the **Select Device(s)** window, select a device and click **Select Device(s)**.

Step 4 Click **Add UDF**.

The created UDF is used as a *custom filter* while creating filters for a connection. See Adding a Filter for details.

Note 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.

Editing or Cloning a User Defined Field

Use this procedure to edit or clone a user defined field.

Editing a UDF means changing the parameters of an existing UDF.

Cloning a UDF means a new UDF is created with the same parameters as an existing UDF. You can change the parameters as required.

Before you begin

Create one or more user defined fields.

Step 1 Navigate to **Components** > **User Defined Field**.

Step 2 In the displayed table, click a **UDF**.

A new pane is displayed on the right.

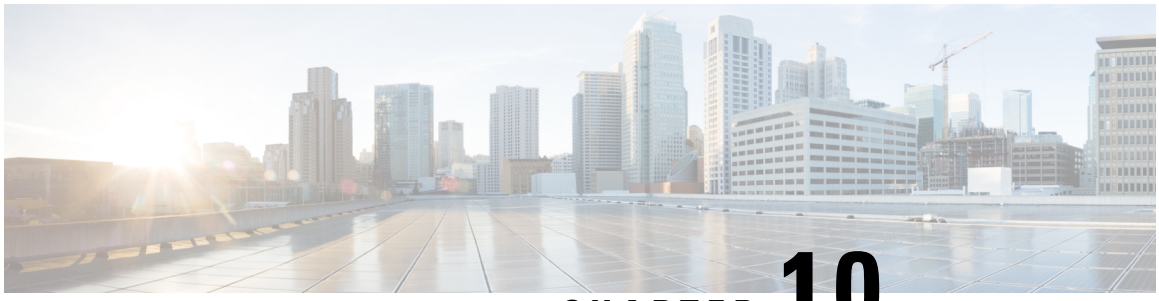
Step 3 Click **Actions** and select **Clone UDF** or **Edit UDF** .

Step 4 In the **Clone UDF** or **Edit UDF** dialog box, the current UDF information is displayed. Modify these fields, as required:

Table 52: Edit UDF

Field	Description
UDF Name	Name of the UDF. This field cannot be changed.
Type	The type selected during UDF creation. This field cannot be changed.
Keyword	Select from the drop down list. The options are: • Header • Packet-Start
Header	The Header selected during UDF creation. This field cannot be changed.
Layer	The Layer selected during UDF creation. This field cannot be changed.
Offset	Set the byte **Offset** value; range is from 0 to 127. Filtering of packets is done based on the set offset value in UDF, packets are matched from the set offset value.
Length	Length (number of bytes) of a packet that are matched; range is from 1 to 2. The length depends on the offset value, if it is set to 1; then one byte starting with the set offset byte is matched.
Devices	Device on which the UDF is currently applied on. You can delete the UDF from the current device or apply the UDF on more devices. Click **Select Devices**. In the **Select Device(s)** window, select a device and click **Select Device(s)**. **Note** You can not delete an *In-use* UDF from a device.

Step 5 Click **Edit UDF** or **Clone UDF** .



CHAPTER 10

Sessions

This chapter has details of the sessions created on the Cisco Nexus Data Broker.

Span Sessions

The **Span Sessions** tab displays details of the span sessions of the NDB controller.

A span session is the link between the span destination of span devices, and the input port of an NDB device. A span session is partially outside the NDB network, and defines the path of the packets from the span destination to the monitoring tool port.

A table is displayed with the following details:

Table 53: Span Sessions

Column Name	Description
Status	The status of a SPAN session depends on the operational status of the session in ACI / NX-OS device and the status of the connection attached to it. Click the displayed status icon to view the details of the session and connection. The factors impacting session status are—span destination, source (NX-OS/ ACI device), input port, monitoring tool port, ISL links(if any). The available statuses are: • Green—session is successful • Yellow—session is partially successful • Red—session has failed • Gray—session has not been installed

Column Name	Description
Span Session	Span session name. This field is a hyperlink. Click the **SPAN session** name and a new pane is displayed on the right. The following additional actions can be performed here: • Editing or Cloning a Span Session
IP Address	IP address of the span session source (span device).
Span Sources	The number of source ports for the span session. **Note** In case of VLAN, the source ports are EPGs on the ACI device.
Span Destination	The number of span destination(s) for the session. **Note** Only ACI devices can have multiple SPAN destinations If there are more than one span destination, then, internal sessions are created. These internal sessions are created based on the availability of source ports. Nexus devices support only one span destination per session.
Connection	Name(s) of connection(s) associated to the span session.
Created By	User who created the span session.
Last Modified By	User who last modified the span session.

The following actions can be performed from the **Span Sessions** tab:

- **Add Span Session**—Use this action to add a span session, see Adding a Span Session.
- **Synchronize Span Session / Destination**—Use this action to synchronize the information on the production switch or APIC with the NDB controller. In case the span session information is deleted /removed on the switch or APIC, this action synchronizes span destination configuration and span session configuration on the switch or controller with the configuration on the NDB controller.
- **Toggle Install** —Use this action to install/ uninstall a span session. You can install a span session on the switch / APIC uninstall a span session without removing it from the NDB controller. The SPAN session is uninstalled from the switch/ controller, but remains saved on the NDB controller for future use.
- **Delete Span Session(s)**—Select the span session to be deleted by checking the check box which is available at the beginning of the row and then click **Actions** > **Delete Span Session(s)**. The selected span session is deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a span session.

Adding a Span Session

Use this procedure to add a span session.

Note You can add a maximum of 4 active span sessions for a Nexus switch.

Before you begin

Add an ACI/ NX-OS device before setting up a span session.

Step 1 Navigate to **Sessions** > **Span Sessions**.

Step 2 From the **Actions** drop-down list, select **Add Span Session**.

Step 3 In the **Add Span Session** dialog box, enter the following details:

Table 54: Add Span Session

Field	Description
Span Session Name	Enter a name for the span session.
Span Sources	Select a Span Source. Select **ACI** or **NX-OS**. Each of these have a unique set of fields, which are discussed in the subsequent rows.
Span Source: ACI After selecting the ACI fabric, you can either select the **Leaf Ports** source type or **EPG/AAEP** source type.	
ACI Fabric	Click **Select ACI Fabric** and select an ACI fabric in the **Select ACI Fabric** window. Click **Select**.
Leaf Ports	Select **Leaf Ports** to add a leaf port to capture the traffic from multiple leaf ports. Click **Select Leaf Ports**. In the **Select Leaf Port(s)** window that is displayed, select a **Pod**. The devices in the selected pod are displayed. Select a **Device** and **Port(s)** of the device.

Field	Description
EPG/ AAEP	Select **EPG/ AAEP** to add an EPG/ AAEP source. Click **Select EPG/ AAEP**. In the **Select EPG/ AAEP** window that is displayed, select a **Tenant**, **Profile** , **EPG** and **EPG Members**. The displayed EPG members are- Dynamic, Static, AAEP. When you select, Dynamic or Static, the member details are displayed on the right. When you select **AAEP** as an EPG Member, in the **Select AAEP** column, select an AAEP. **Note** EPG interfaces work only when all the ports are within the same leaf switch. If an EPG is spread across multiple switches, select the corresponding SPAN destination on all the leaf switches.
Span Source: NX-OS You can either select the **Interface** source type or the **VLAN** source type.	
Interface	Click **Select NX-OS Interface** . and select a **Device** and **Port(s)**. The selected device and port(s) are used in the session.
VLAN	Click **Select NX-OS Device** and select a device. Enter a VLAN ID. The device matching the VLAN ID is used in the session.
Direction	Indicates traffic for the session source port of the ACI/ NX-OS device. Select from one of these options: • Incoming • Outgoing • Both
SPAN Destination	Click **Select SPAN Destination** and select span destination. If directly connected to the NDB device, select a local span destination, else select remote span destination. To install ACI SPAN session, NDB controller lists the SPAN destination(s) created in ACI. To install NX-OS SPAN session, NDB controller lists the SPAN destination(s) created for the NX-OS devices.

Field	Description
Apply Connection	Select a connection for the session. You can associate an existing connection to the span session or create a new connection for the span session. **Note** All span destinations which are part of a session should be a part of a connection too, to direct traffic to the monitoring tool. Click the button to enable addition of a connection to the span session. Click **Select Connection** and select a connection from the **Select Connection**window that is displayed.

Note For EPG:

- For EPG selection, if an EPG is selected, by default, the NDB controller listens for the changes in the statically or dynamically 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 `ndb/configuration` folder.
- When new EPG members are added in APIC, if there is no SPAN destination on the leaf switch that matches the newly added EPG member as part of the configured SPAN session, NDB ignores this event and the new EPG member are not shown in NDB.

Note For SPAN Destination:

Ensure that each leaf switch in the SPAN source has at least one corresponsing SPAN destination.

Step 4 Click **Add Span Session** to add the created span session, without installing it on the production device or controller. Click **Install Span Session** to save and install the created span session on the production device or controller.

Editing or Cloning a Span Session

Use this procedure to edit or clone a span session.

Editing a span session means changing some of the parameters of an exisiting span session.

Cloning a span session means creating a new span session with identical parameters of an exisiting span session, with required modifications. Ensure to change the name of the span session before saving it.

Before you begin

Add one or more span sessions.

Step 1 Navigate to **Sessions** > **Span Sessions**.

Step 2 In the displayed table, click a **Session**.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Span Session** or **Clone Span Session**.

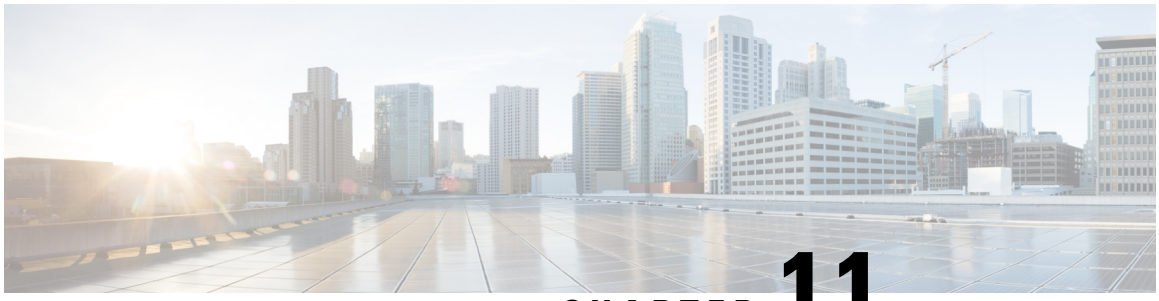
Edit the displayed parameters in the table.

Table 55: Edit / Clone Span Session

Field	Description
Span Session Name	Name of the span session. This field cannot be changed while editing a span session.
Span Sources	The selected span device type; can either be **ACI** or **NX-OS**. This field cannot be changed. Each of these have a unique set of fields, which are discussed in the subsequent rows.
Span Source: ACI After selecting the ACI fabric, you can either select the **Leaf Ports** source type or **EPG/AAEP** source type.	
ACI Fabric	Click the displayed **ACI Fabric** to change the ACI fabric
Leaf Ports	If **Leaf Ports** were selected while adding a span session, then, the selected leaf ports are displayed and you can make additions/ deletions. Click **Select Leaf Ports**. In the **Select Leaf Port(s)** window that is displayed, select a **Pod**. The devices in the selected pod are displayed. Select a **Device** and **Port(s)** of the device. **Note** If you had earlier selected the source type as **Leaf Ports**, delete all the leaf ports, before changing the source type to **EPG/ AAEP**.
EPG/ AAEP	If **EPG/AAEP** was earlier selected while adding a span session, then the EPG/AAEP details are displayed and you can make additions/ deletions. Click **Select EPG/ AAEP**. In the **Select EPG/ AAEP** window that is displayed, select a **Tenant**, **Profile** , **EPG** and **EPG Members**. The displayed EPG members are- Dynamic, Static, AAEP. When you select, Dynamic or Static, the member details are displayed on the right. When you select **AAEP** as an EPG Member, in the **Select AAEP** column, select an AAEP. **Note** If you had earlier selected the source type as **EPG/ AAEP**, you need to delete all the associated tenant and members before changing the source type to **Leaf Ports**.

Field	Description
Span Source: NX-OS You can either select the **Interface** source type or the **VLAN** source type.	
Interface	Click **Select NX-OS Interface** . and select a **Device** and **Port(s)**. The selected device and port(s) are used in the session.
VLAN	Click **Select NX-OS Device** and select a device. Enter a VLAN ID. The device matching the VLAN ID is used in the session.
Direction	Indicates traffic for the session source port of the ACI/ NX-OS device. Select from one of these options: • Incoming • Outgoing • Both
SPAN Destination	Click **Select SPAN Destination** and select span destination. If directly connected to the NDB device, select a local span destination, else select remote span destination. If you install ACI SPAN session, NDB controller lists the SPAN destination(s) created in ACI. If you install NX-OS SPAN session, NDB controller lists the SPAN destination(s) created for the NX-OS devices.
Apply Connection	Select a connection for the session. You can associate an existing connection to the span session or create a new connection for the span session. **Note** All span destinations which are part of a session should be a part of a connection too, to redirect traffic to the monitoring tool. Click the button to enable addition of a connection to the span session. Click **Select Connection** and select a connection from the **Select Connection**window that is displayed.

Step 4 Click **Edit Span Session** or **Clone Span Session**.



CHAPTER 11

Statistics

This chapter has details about the statistics of the connections and components of the Cisco Nexus Data Broker.

Connections

The **Connections** tab displays a list of connections configured on the NDB controller.

A table with the following details is displayed:

Column Name	Description
Connection	The connection name. This field is a hyperlink; click a **Connection** name to get more information about the connection. For related actions, see the Connections section.
Packet Count	The aggregate traffic volume shown in packets for the connection.

Filters

The **Filters** tab displays filters that are used in connections.

A table with the following details is displayed:

Column Name	Description
Filter	The filter name. This is hyperlink; click the **Filter** name for more details about the filter. For related actions, see the Filters section.
Packet Count	The aggregate traffic volume shown in packets for the filter.

Flows

The **Flows** tab displays device flows for NDB devices.

Click **Select Device** to select an NDB device for which the flow statistics will be fetched. If you want to fetch the flow statistics for another device, click **Change Device**.

A table with the following details is displayed:

Column Name	Description
In Port	The input port(s) from which the traffic is matched.
DL Src	The source MAC address to be matched for the incoming traffic.
DL Dst	The destination MAC address to be matched for the incoming traffic.
DL Type	The ethertype to be matched for the incoming traffic. For example, **IPv4** or **IPv6** is used for all IP traffic types.
DL VLAN	The VLAN ID to be matched for the incoming traffic.
VLAN PCP	The VLAN priority to be matched for the incoming traffic.
NW Src	The IPv4 or IPv6 source address for the incoming traffic.
NW Dst	The IPv4 or IPv6 destination address for the incoming traffic.
NW Proto	The network protocol to be matched for the incoming traffic. For example, "6" indicates the TCP protocol.
TP Src	The source port associated with the network protocol to be matched for the incoming traffic.
TP Dst	The destination port associated with the network protocol to be matched for the incoming traffic.

Column Name	Description
Packet Count	The aggregate traffic volume shown in packets that match the specified flow connection.

Input Ports

The **Input Ports** tab displays the packet count details for the input ports of the NDB devices.

A table with the following details is displayed:

Column Name	Description
Input Ports	The input port with the device name. Click the **Input Port** to get more details of the input port. For related actions, see the Input Ports section.
Packet Count	The aggregate traffic volume shown in packets for the input port.

TCAM Resource Utilization

The **TCAM Resource Utilization** tab displays TCAM resource utilization details for NDB devices.

A table with the following details is displayed:

Table 56: TCAM Resource Utilization

Column Name	Description
Device	The device name. This field is a hyperlink; click the **Device** name for more details of the device. For related actions, see the Devices section.
Utilization	The utilization pattern, indicated by colours. • Green—indicates that the TCAM utilization is optimum. • Orange—indicates that the TCAM utilization is within the range. • Red—indicates that the TCAM utilization is nearing the full limit.

Monitoring Tools

The **Monitoring Tools** tab displays the monitoring tool ports connected to the NDB controller.

A table with the following details is displayed:

Column Name	Description
Monitoring Tools	The monitoring tool name. This field is a hyperlink; click the monitoring tool name for more details. For related actions, see theMonitoring Toolssection.
TX Packets	The number of packets transmitted by the monitoring tool port.

Ports

The **Ports** tab displays the statistics for ports of an NDB device.

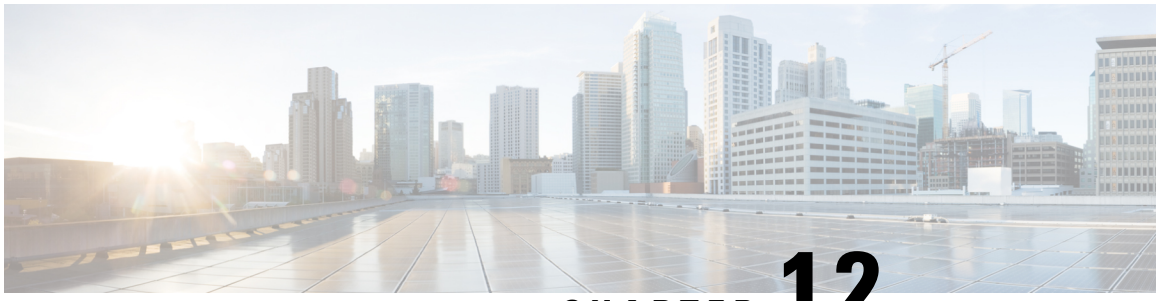
Click **Select Device** to fetch the port details of the selected device. Click **Change Device** to select another device.

A table with the following details is displayed:

Column Name	Description
Port	The interface of the device for which the statistcs are displayed. This is hyperlink; click the port for more details.
Rx Pkts	The number of received packets on the port.
Tx Pkts	The number of transmitted packets on the port.
Rx Bytes	The number of received bytes on the port.
Tx Bytes	The number of transmitted bytes on the port.
Rx Rate (kbps)	The rate of receiving packets.
Tx Rate (kbps)	The rate of transmitting packets.
Rx Drops	The rate at which packets are dropped at the port (Rx).
Tx Drops	The rate at which packets are dropped at the port (Tx).
Rx Errs	Errors at the port while receiving packets.
Tx Errs	Errors at the port while transmitting packets.

Column Name	Description
Rx Frame Errs	Frame errors at the port while receiving packets.
Rx OverRu	Overrun errors at the port while receiving packets.

Click **Actions** > **Clear Ports** to clear the statistics data of the selected device.



CHAPTER 12

Troubleshooting

This chapter has troubleshooting details of the Cisco Nexus Data Broker.

Audit Log

The **Audit Log** tab displays a record of activities or actions performed on NDB.

Note Read-only actions are not recorded.

A table is displayed with the following details:

Table 57: Audit Log

Column Name	Description
Date & Time	The date and time of activity.
Module Name	Module on which the event occurred. This is based on an internal mapping of modules, for example- logging in and logging out is part of the Security Module.
Slice	Slice pertaining to an action/ event. Some actions are not slice-relevant and they are left blank. Examples for slice-dependent actions- components, connections , sessions, statistics.

Column Name	Description
User	User responsible for the action/ event.
Action	Description of the action performed by the user.
Resource	Object on which the action was performed.
Description	The result of the performed action. The available options are: • Failure (with description) • Success
Origin	NDB controller on which the action was performed. **Note** For Standalone NDB, 127.0.0.1 is displayed.
Mode	Mode in which the action was performed. **Note** For Release 3.10, only Centralized mode is supported.

The following actions can be performed from the **Audit Log** tab:

- **Fetch Records**—Use this to set the number of audit logs that will be displayed.

  Click **Actions** > **Fetch Records** and enter a value for the **Record Count** field. Click **Fetch**. The **Audit Log** table is loaded accordingly.

Flow Management

The **Flow Management** tab enables you to view inconsistent connections and device flows and manage the inconsistent flows. You can view and download the details, which can be used for degugging.

The **Flow Management** tabs contains the following subtabs:

- **Consistency Check**—displays inconsistencies for NX-API based devices. The inconsistencies are automatically trigerred if there is an ACL/ ACE mismatch with the NDB database. See Consistency Check for more details.
- **Connection Flows**—displays details of the ACLs and ACEs generated for a connection. See Connections Flows for more details.
- **Device Flows**—displays details of the ACLs and ACEs generated for a device. See Device Flows for more details.

Consistency Check

The **Consistency Check** tab displays inconsistencies for NX-API based devices. The inconsistencies are automatically triggered if there is an ACL/ ACE mismatch with the NDB database.

The *Alarm* icon () in the header displays the number of devices that have inconsistencies.

A table is displayed with the following details:

Table 58: Consistency Check

Column Name	Description
Device	Device name. This field is an hyperlink. Click the **Device** name and a new pane is displayed on the right. For details about devices, see Devices.
Inconsistent Controller Flows	The inconsistent controller flows. This field is an hyperlink. Click the number indicated and a new pane is displayed on the right with a list of ACLs and their ACEs. The following actions can be performed from here: • **Fix Flows**—Select the required check-boxes and click **Fix Flows**. The selected flows (ACEs) are fixed and the number displayed in the **Inconsistent Controller Flows** column is updated accordingly. • **Export All**—Select this option to get a copy of the flows listed as ACLs and ACEs. A `.csv` file is downloaded to your local machine. This is useful for debugging.

Column Name	Description
Inconsistent Device Flows	The inconsistent or stale flows for a device; indicates the missing ACLs and ACEs in the device when compared to the controller flows. This field is an hyperlink. Click the number indicated and a new pane is displayed on the right with a list of ACLs and their ACEs. The following actions can be performed from here: • **Fix Flows**—Select the required check-boxes and click **Fix Flows**. The selected flows (ACEs) are fixed and the number displayed in the **Inconsistent Controller Flows** column is updated accordingly. • **Export All**—Select this option to get a copy of the flows listed as ACLs with their ACEs. A `.csv` file is downloaded to your local machine. This is useful for debugging.
Non NDB Flows	The number of ACLs present in the device. ACLs can be the default device ACLs or can be added manually. This field is an hyperlink. Click the number indicated and a new pane is displayed on the right with a list of ACLs and their ACEs. The following actions can be performed from here: • **Fix Flows**—Select the required check-boxes and click **Fix Flows**. The selected flows (ACEs) are fixed and the number displayed in the **Inconsistent Controller Flows** column is updated accordingly. • **Export All**—Select this option to get a copy of the flows listed as ACLs with their ACEs. A `.csv` file is downloaded to your local machine. This is useful for debugging.

Note ACLs which are NDB-generated are indicated with a *ndb_* prefix. Non-NDB flows are indicated by the respective component.

The following actions can be performed from the **Consistency Check** tab:

- **Check Controller Flows**—Select a device and click **Check Controller Flows**. A new pane is displayed on the right with the ACLs and ACEs.
- **Check Device Flows**—Select a device and click **Check Device Flows**. A new pane is displayed on the right with the ACLs and ACEs.

- **View non-NDB Flows**—Select a device and click **View non-NDB Flows**. A new pane is displayed on the right with the ACLs and ACEs.

Connections Flows

The **Connections Flows** tab provides details of the ACLs and ACEs generated for a connection.

A table is displayed with the following details:

Table 59: Connections Flows

Column Name	Description
Connection	Connection name. This field is a hyperlink. Click the **Connection** name and a new pane is displayed on the right with details of the connection. For information about the actions that can be performed here, see Connections chapter.
Flows	Number of flows (ACEs) for the connection (can be across devices). This field is hyperlink. Click the displayed number and a new pane is displayed on the right. The connection name is displayed, followed by the ACL and the ACEs that it contains. Actions that can be performed from here are: • **Export All**—Select this option to get a copy of the flows listed as ACLs with their ACEs. A `.csv` file is downloaded to your local machine.

The following actions can be performed from the **Connection Flows** tab:

- **Check Connection Flows**—Select a connection and click **Check Connection Flows**. A new pane is displayed on the right. The connection name is displayed, followed by the ACL and the ACEs that it contains. Actions that can be performed from here are:
  - **Export All**—Select this option to get a copy of the flows listed as ACLs with their ACEs. A `.csv` file is downloaded to your local machine.

Device Flows

The **Device Flows** tab provides details of the ACLs and ACEs generated for a device.

A table is displayed with the following details:

Table 60: Device Flows

Column Name	Description
Device	Device name. This field is a hyperlink. Click the **Device** name and a new pane is displayed on the right with details of the device. For information about the actions that can be performed here, see Devices chapter.
Flows	Number of flows (ACEs) for the device (can be across connections and all ports of the device). This field is a hyperlink. Click the displayed number and a new pane is displayed on the right. The connection name is displayed, followed by the ACL and the ACEs that it contains. Actions that can be performed from here are: • **Export All**—Select this option to get a copy of the flows listed as ACLs with their ACEs. A `.csv` file is downloaded to your local machine.

The following actions can be performed from the **Device Flows** tab:

- **Check Device Flows**—Select a device and click **Check Device Flows**. A new pane is displayed on the right. The device name is displayed, followed by the ACL and the ACEs that it contains. Actions that can be performed from here are:
  - **Export All**—Select this option to get a copy of the flows listed as ACLs with their ACEs. A `.csv` file is downloaded to your local machine.

JSON Export/ Import

The **JSON Export/ Import** tab enables you to export and import the device configuration in JSON file format. The configuration file includes information about the connected as well as disconnected devices with all the configuration information (except for port-channel).

The **JSON Export/ Import** tab contains the following subtabs:

- **Export**—enables you to export configurations from NDB (to your local machine). See Export for more details.
- **Import**—enables you to import configurations into NDB. See Import for more details.

Export

The **Export** tab enables you export configurations from NDB.

A table with the following details is displayed:

Table 61: Export

Column Name	Description
ID	Serial number of the device.
Name	Name of the device.
IP Address	IP address of the device.
Type	Type of the device. The options are: • NX—NDB connected to NX-API device • PS—NDB connected to production switch (NX-OS) • AC—NDB connected to ACI device
Status	The status of the device.

The following actions can be performed from the **JSON Export/ Import** > **Export**tab:

- **Export Configuration**—Click **Actions** > **Export Configuration** to export a JSON configuration to your local machine. Select the **Connections** check-box to include the connections of a device while exporting. Click **Export**.

Import

The **Import** tab enables you to import configurations into NDB.

A table with the following details is displayed:

Table 62: Import

Column Name	Description
ID	Serial number of the device.
Exported Device Name	Name of the device from which the configuration was exported.
IP Address	IP address of the device.
Type	Type of the device. The options are: • NX—NDB connected to NX-API device • PS—NDB connected to production switch (NX-OS) • AC—NDB connected to ACI device
Status	Status of the import action. The options are- success, failure, partial, in progress, abort.

Column Name	Description
Description	Description of the success/ failure status.

The following actions can be performed from the **JSON Export/ Import** > **Import**tab:

- **Import Configuration** —Click **Actions** > **Import Configuration** and select a JSON file from your local machine and click **Upload**. You can also *drag and drop* to upload a JSON file.
- **Apply Configuration**—Click **Actions** > **Apply Configuration**. The **Edit Device** screen is displayed. Enter the details of the device on which you intend to apply the configuration. Click **Apply and Check Compatibility**. The **Compatibility Matrix** screen is displayed. If both the devices are compatible, the status is indicated in green. Click **Apply**.

  The status of this action is indicated in the **Import** table.
- **Delete Import**—Click **Actions** > **Delete Import** to delete an imported configuration.

Purge Device

The **Purge Device** tab displays details of deleted NDB devices. Deleting a device only removes it from the NDB controller but the device configuration is retained, while purging a device deletes a device and also removes the device configuration from the NDB controller.

A table is displayed with the following details:

Table 63: Purge Device

Column Name	Description
Node ID	Node ID of the device connected to NDB controller.
Device	Device name.
IP Address	IP address of the device.

Use the *Filter by attributes* bar to filter the table based on displayed device group details. Choose the attribute, operator and filter-value.

The following actions can be performed from the **Purge Device** tab:

- **Purge Device(s)**—Select the required devices by checking the check box which is available at the beginning of the row; click **Purge Device(s)**.

  This is useful for removing the stale device configurations from the database.

RMA

The Return Material Authorization (**RMA**) tab displays a list of devices that have been deleted and awaiting replacement. This feature maps the configuration from the RMA device to the new device.

A table is displayed with the following details:

Table 64: RMA

Column Name	Description
Existing Node ID	The node ID of the (deleted) NDB device.
Node Name	Device name.
Serial Number	Serial number of the device.
IP Address	IP address of the device.

The following actions can be performed from the **RMA** tab:

- **Replace Node ID**— Select a Node ID by checking the check box. Click **Actions** > **Replace Node ID**. In the pop-up window that appears, enter the **Serial Number** and click **Replace** . The selected device is replaced with the device with the new serial number.

Note To get the serial number for a NX-API device, use **show module** command for non-modular chassis (look for Serial-Num in the output) or use **show hardware** command for modular chassis switches (look for serial number under Switch hardware ID information in the output.

Tech Support

The **Tech Support** tab displays details of the tech support jobs created on the NDB controller.

For more details about Tech Support About Tech Support, on page 169.

A table is displayed with the following details:

Table 65: Tech Support

Column Name	Description
Job ID	Job id created for a Tech Support job. This field is a hyperlink. Click the **Job ID** to view more details of the job. Click **Actions** > **Download** to download the details of the job to your local machine. The **Download and Delete** option downloads the details of the job to your local machine and then deletes it from the NDB controller.
Job Type	The Operation Type of the job. The options are: • Basic • Advanced

Column Name	Description
Status	Status of the tech support job. The available statuses are: • Success— job is successfully completed. • Partial— job is partially successful. For eg, if multiple devices were selected, then, may be the failure has occurred on one of the selected devices. • Failure— job is not successful. • In progress— job is currently in progress. • Created— job is ready for execution, but is in a queue. • Stop— job was created but was not allowed to complete.

The following actions can be performed from the **Tech Support** tab:

- **Trigger Job** — Use this to trigger a tech support job. See Trigger Tech Support, on page 168 for more details.
- **Re-trigger Job** —Select a check box next and click **Actions** > **Re-trigger Job** to re-trigger a job. *In Progress* and *Created* jobs cannot be re-triggered. The Tech Support log files are replaced with the latest set of files, after a retriggered job is successful.
- **Stop Job**—Select a check box and click **Actions** > **Stop Job** to stop an onging job. Only *In Progress* and *Created* jobs can be stopped.
- **Delete Job**—Select a check box and click **Actions** > **Delete Job** to delete a job. An *In Progress* job cannot be deleted.

Note Multiple eligible jobs can be removed/stopped/re-triggered at a time.

Trigger Tech Support

Use this procedure to trigger a tech support job.

Before you begin

Ensure that one or more devices are connected to NDB and the AUX mode is disabled.

Ensure to have a minimum available space of 64 MB in the device; else, the operation fails and a *No Enough Space* error is displayed.

Step 1 Navigate to **Troubleshooting** > **Tech Support**.

Step 2 Click **Actions** > **Trigger Job**.

Step 3 In the **Trigger Tech Support** dialog box, enter the following details:

Table 66: Trigger Tech Support

Field	Description
Trigger Settings	
Device	The device for which you need to collect data. Click **Select Device** to select a device.
Operation Type	Select **Basic** or **Advanced**. The `show commands` for each of these options is listed.

Step 4 Click **Add** to collect the outputs of the `show commands`.

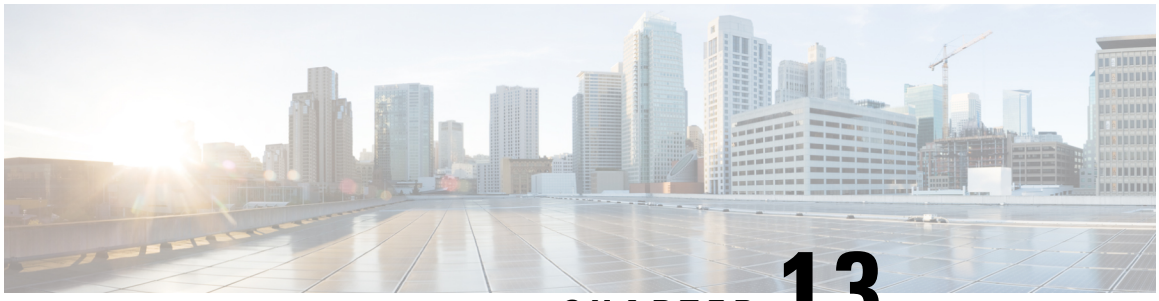
Note The following folders are by default downloaded besides the Tech Support folder – configuration folder, configuration start up folder and general logs. This enables the tech support team to get all the information together and results in faster analysis.

About Tech Support

The tech support for NX-API devices feature enables you to collect information from one or more switches in one attempt, instead of collecting data separately from each switch. This is useful during debugging as all the relevant logs are readily available and can be downloaded.

Tech support data collection from switches can be performed in two modes:

- Basic mode– contains a limited set of show commands.
- Advanced mode–contains a wider set of show commands:



CHAPTER 13

Administration

This chapter has details about the profiles and users of the Cisco Nexus Data Broker.

AAA

The **AAA** tab displays details of the AAA servers available on the NDB. For more details about AAA servers, see About AAA Servers, on page 174.

A table with the following details is displayed:

Column Name	Description
Server Address	The IP address of the AAA server.
Protocol	The protocol running on the server. The options are: • TACACS • RADIUS+ • LDAP

The following actions can be performed from the **AAA** tab:

- **Add Server**—Use this to add a new AAA server. See Adding an AAA Server, on page 172 for the detailed procedure.
- **Delete Server**—Select the server(s) to be deleted by checking the check box which is available at the beginning of the row and then click **Actions** > **Delete AAA Server**. The selected server(s) is deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a server.

Adding an AAA Server

Use this procedure to add an AAA server.

Step 1 Navigate to **Administration** > **AAA**.

Step 2 From the **Actions** drop down menu, select **Add AAA Server**.

Step 3 In the **Add AAA Server** dialog box, enter the following details:

Table 67: Add AAA Server

Field	Description
General	
Protocol	Choose a protocol for the AAA server. • Radius • LDAP • TACACS The fields relevant for each option are discussed below.
Protocol: Radius	
Server Address	Server IP address or domain name.
Secret	Secret configured on the AAA server.
Protocol: LDAP	
Server Address	Server IP address or domain name.
Port	Communication port for the AAA server.
User RDN	Enter the Relative Distinguished Name (RDN) , used to authenticate with the LDAP server. User hierarchy defined in the LDAP server. Example: While configuring LDAP in AAA, consider the following hierarchy (defined in LDAP), for user "cn=admin,ou=People,dc=ndb,dc=local", user RDN should be "ou=People,dc=ndb,dc=local". After NDB is configured with LDAP, then to login, only the *cn* value has to be provided for the username. In this case, username is "admin".

Field	Description
Role Attribute	Enter the role attribute which is the LDAP authorization attribute for users. Role Attribute can be any attribute in LDAP for the DN. For example, let *sn* be the defined role-attribute in the local LDAP server. So, for *admin user* in NDB, you can have "network-admin" as a value for the *sn* attribute. When NDB contacts the LDAP sever with the Role Attribute and User RDN and *admin user*, LDAP returns the *sn* value ("network-admin") as authentication.
Role Type Mapping	Click the button to enable Default setting. A list of **Role Mapping** values are displayed. If you have enabled **Default**, then, the following are the existing mapped values: • network-admin—*network-admin* • network-operator—*network-operator* • application-user—*application-user* • slice-user—*slice-user* Disable **Default**, to provide custom mapping of roles with values defined in LDAP. Select a role from the drop down list in the **Role Mapping** column, and enter a value defined in LDAP in the **Role Type Mapping** column. Click **Add Row** to add more Role Type Mapping rows.
Timeout	Enter the wait time by which the LDAP server should respond.
Protocol: TACACS+	
Server Address	TACACS+ server address.
Secret	Secret configured on the TACACS+ server.
Username	Username to login to the server.
Password	Password to login to the server.
Check Server	Click **Check Server** to check if the server is reachable and the authentication credentials are valid.

Note It is not recommended to change the admin password of the ndb controller when the user management of the ndb controller is performed through TACACS or AAA.

Step 4 Click **Add AAA Server** to add the server.

What to do next

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

Configuring User Authentication for RADIUS Server

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

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

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.

AAA server supports remote authentication and authorization. To authenticate each user, Cisco Nexus Data Broker uses both the login credentials and an attribute-value (AV) pair. An AV pair 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.

Backup/ Restore

The **Backup/ Restore** tab has two subtabs:

- **Scheduled Backups**—for details of the schedule of backup(s) on NDB, see Schedule of Backups, on page 174.
- **Backups** —for details of completed backups on NDB, see Backups, on page 176.

Schedule of Backups

The **Schedule of Backups** tab displays details of the scheduled backups for the NDB controller.

A table with the following details is displayed:

Table 68: Backup

Column Name	Description
Start Date	The start date for the backup.
Start Time	The start time for the backup.
End Date	The end date for the backup.

Column Name	Description
Pattern	The backup pattern. Options are: • Daily • Weekly • Monthly
Occurences	Number of occurrences based on the selected pattern.

The following actions can be performed from the **Backup** tab:

- **Schedule Backup**—Use this to schedule a backup. See Scheduling Backup, on page 175 .
- **Backup Locally**—Configuration is backed up on your local machine.
- **Restore Locally**—In the **Restore Locally** window that appears, choose a file from your local machine to restore the configuration.

  Select the **Restore** check-box if you want NDB to re-configure the configurations of the device, from the uploaded backup after NDB is restarted. The following configurations are reconfigured:

  - Global Configurations
  - Port Configurations
  - UDF
  - Connections

  The **Restore** check-box is applicable only for configuration downloaded from NDB 3.8 and above.

Scheduling Backup

Use this procedure to schedule a backup.

It is always recommended to take a backup before upgrading to the next NDB version.

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

Step 2 From the **Actions** drop-down list, select **Schedule Backup**.

Step 3 In the **Schedule Backup** dialog box, enter the following details:

Table 69: Schedule Backup

Field	Description
Schedule	
Start Date	Enter the start date for the backup.
Start Time	Enter the start time for the backup.

Field	Description
Repeat	Select one of the options: • **Daily**—the backup operation occurs daily. • **Weekly**—the backup operation occurs on the selected day of the week, every week. • **Monthly**—the backup operation starts on the selected date every month. **Note** Check the **Last Day** check-box for the backup to be perfomed till the end of the selected month.
End	Select one of the options to stop the backup process: • **No End Date**—continue taking back up. • **End Date** —continue taking backup till the specified end date. • **Occurences** —takes backup based on the number selected in the **Number of Occurrences** field.
Enable	The **Enable** check box is selected by default. Leave the check box checked, to enable the backup per the schedule.

Step 4 Click **Schedule**.

Backups

The **Backups** tab displays the backup information.

The information displayed here is based on the schedule generated using Scheduling Backup. A table with the following details is displayed:

Column Name	Description
Item	Time of backup.
Cluster Backup Status	Cluster backup status of the NDB controller. Options are: • Success • Failure
Description	Description of the backup.
Restore Triggers	Timestamp when the restore backup was triggered.

The following actions can be performed from the **Backups** tab:

- **Backup to NDB Server**—Backup is created at the specified time in the NDB server. After you select this option, the backup details appear in the **Backups** tab.
- **Restore Backup**—The selected backup is restored on the NDB controller. It is recommended to always choose the latest backup for restoration. If you choose an old backup, there could be connection failures based on recent topology changes.

Note Restart the NDB controller after restoring a backup.

- **Delete Backup**—Select the backup(s) to be deleted by checking the check box which is available at the beginning of the row and then click **Actions** > **Delete Backup(s)**.

Cluster

The **Cluster** tab displays details of the clusters available on the NDB. NDB supports high availability clustering in active/active mode with up to five controllers in a cluster.

A table with the following details is displayed:

Column Name	Description
Controller	The IP address of the controller.
Type	Displayed options are either **Primary** or **Member**.

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 inconsistencies in the data.

Note After a backup is uploaded, all the instances of the cluster should be shut down and the server on which the backup is uploaded should be started first.

Profile

The **Profiles** tab displays details of the profiles available on the NDB controller. A profile allows you to manage multiple devices associated to an NDB controller. You can attach multiple devices to a profile.

The profile configuration is applied to all the member switches.

A table with the following details is displayed:

Column Name	Description
Profile Name	Name of the profile.
User Name	User name that created the profile.

Use the *Filter by attributes* bar to filter the table based on displayed filter details. Choose the attribute, operator and filter-value.

The following actions can be performed from the **Profiles** tab:

- **Add Profile**—Use this to add a new profile. See *Add Profile* for details about this task.
- **Delete Profile**—Select the required profile(s) by checking the check box which is at the beginning of the row and then click **Delete Profile**. The selected profile(s) are deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a profile.

Note A profile which is in use cannot be deleted.

Adding a Profile

Use this procedure to add a new profile.

Step 1 Navigate to **Administration** > **Profile**.

Step 2 From the **Actions** drop down menu, select **Add Profile**.

Step 3 In the **Add Profile** dialog box, enter the following details:

Table 70: Add Profile

Field	Description
Profile Name	Enter a profile name.
Username	Enter a user name to login to the device.
Password	Enter a password for the username. 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 non-alphanumeric character.

Step 4 Click **Add Profile** to create the profile.

Editing a Profile

Use ths procedure to edit a profile.

Note When you edit a profile, devices that are using the profile will be reconnected.

Before you begin

Create one or more profiles.

Step 1 Navigate to **Administration** > **Profiles**.

Step 2 In the displayed table, click a **Profile Name**.

A new pane is displayed on the right.

Step 3 Click **Actions** and select **Edit Profile**.

Step 4 In the **Edit Profile** dialog box, the current profile information is displayed. Modify these fields, as required:

Table 71: Edit Profile

Field	Description
Profile Name	Profile name is displayed and can not be changed.
Username	Enter a username to login to the device.
Password	Enter a password for the username. 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 non-alphanumeric character.

Step 5 Click **Edit Profile** to edit the profile.

Slices

The **Slices** tab displays details of the slices available on the NDB.

Slicing enables you to partition a network into many logical networks. For more information, see About Slices, on page 182.

To view a different network partition, switch the slice using the **Slice** button in the header. As part of the initial NDB build, one slice is available and is called the **Default** slice. The following configurations can be performed only on the default slice of the NDB controller:

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

- Fixing inconsistent device and connection flows

A table with the following details is displayed:

Column Name	Description
Slice	Name of the slice. This field is a hyperlink. Click the **Slice** name and a new pane is displayed on the right. Additional actions that can be performed from here: • Editing a Slice
Configured Port(s)	Ports of a device (or different devices) that are currently part of the slice.
Available Port(s)	Ports of a device (or different devices) that are currently not part of the slice, but can be added to the slice.

You can perform the following actions from the **Slices** tab:

- **Add Slice**—For details about this action, see Adding a Slice.
- **Delete Slice**—Select the slices to be deleted and click **Actions** > **Delete Slice(s)**. If you choose the delete action, without selecting a check box, an error is displayed and you will be prompted to select a slice.

Adding a Slice

Use this procedure to add a slice.

Note A device can be a part of multiple slices; a port can be a part of only one slice at any given time.

Before you begin

Clear all port configurations and connections of a device which is already a part of the default slice, before adding the ports of a device to a new slice.

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

Step 2 From the **Actions** drop down menu, select **Add Slice**.

Step 3 In the **Add Slice** dialog box, enter the following details:

Table 72: Add Slice

Field	Description
General	

Field	Description
Slice Name	Enter a name for the slice.
Port	Click **Select Ports** and in the **Select Ports** window, select the device and required ports. **Note** Ensure to have all the ports of a device on the same slice.

Step 4 Click **Add Slice** to create the slice.

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

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

Editing a Slice

Use this procedure to edit a slice.

Before you begin

Delete the port configurations for a port before deleting the port from a slice.

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

Step 2 Click a **Slice** name. A new window opens on the right.

Step 3 Click **Action** > **Edit Slice**.

The **Edit Slice** window is displayed.

Step 4 Make required changes in the **Edit Slice** window. The following details are displayed:

Table 73: Edit Slice

Field	Description
General	
Slice Name	Name for the slice. This field cannot be changed.
Port	The ports that are part of the slice are listed. You can delete / add as required.

Step 5 Click **Edit Slice**.

About Slices

Slices enables you 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.

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.

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.

System Information

The **System Information** tab displays all the information about the NDB controller and the NDB controller host. The information is available under two headings:

- **NDB Information** —includes information such as Installation Type, Current Build Number, Previous Build number, etc.
- **System Information**—includes information such as Total Memory, Physical Memory, Used Memory, Free Memory of the NDB controller host.

User Management

The **User Management** tab has the following subtabs:

- **Users**—users of NDB controller. See Users for more details.
- **Roles**—roles that the users are assigned to. See Roles for more details.
- **Groups**—device groups that the ports are assigned to. See Groups for more details.

Users

The **Users** tab displays the details of the users of the NDB controller.

A table with the following details is displayed:

Column Name	Description
User	The login name of the user. This field is a hyperlink. Click **User** and a new pane is displayed on the right. The following additional actions can be performed from here: • Changing Password for a User • Changing Role for a User
Role	The role of the user that was assigned while creating the user.

The following actions can be performed from the **Users** tab:

- **Add User**—Use this to add a new user. See Adding a User for details about this task.
- **Delete User**—Select the user(s) to be deleted by checking the check box which is available at the beginning of the row and then click **Delete User**. The selected user(s) are deleted. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a user.

Adding a User

Use this procedure to add a new user.

Before you begin

Create role(s) that the new user can be assigned to.

Step 1 Navigate to **Administration** > **User Management** > **Users**.

Step 2 From the **Actions** drop down menu, select **Add User**.

Step 3 In the **Add User** dialog box, enter the following details:

Table 74: Add User

Field	Description
Username	Enter the user name.
Password	Enter a 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 non-alphanumeric character.
Verify Password	Verify the password by re-entering it.

Field	Description
Choose User Type	Select one of the options: • **Regular User**—can login to the NDB controller without a slice (default slice). • **Slice User**—has access only to a specific slice.
Select Slice This field is applicable only when the User Type is **Slice User**.	Select a slice from the drop-down list. The created user has access only to the selected slice.
Set Role This field is applicable only when the User Type is **Regular User**.	Click **Select Role**. In the **Select Role** dialog box that opens, check the check box for the role(s) you want to assign to the user. The role details are displayed on the right side. Click **Select** to assign the role. You can assign more than one role to a user. The available role options are: • Network Admin—Provides full administrative privileges to all applications. • Network Operator—Provides read-only privileges to all applications.

Step 4 Click **Add User** to add the user.

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

Changing Password for a User

Use this procedure to change the password for a user.

Before you begin

Create one or more users.

Step 1 Navigate to **Administration** > **User Management** > **Users**.

Step 2 Click a **User** name. A new window opens on the right.

Step 3 Click **Action** > **Change Password**.

The **Change Password** window is displayed.

Step 4 Make required changes in the **Change Password** window. The following details are displayed:

Table 75: Change Password

Field	Description
General	
User Name	Name of the user. This field cannot be changed.
Current Password	Enter the current password for the username. **Note** This field is displayed only for *admin* user.
Password	Enter the new password.
Verify Password	Enter the new password again.

Step 5 Click **Change Password**.

Changing Role for a User

Use this procedure to change the role of a user.

Before you begin

Create one or more users.

Step 1 Navigate to **Administration** > **User Management** > **Users**.

Step 2 Click a **User** name. A new window opens on the right.

Step 3 Click **Action** > **Change Role**.

The **Change Role** window is displayed.

Step 4 Make required changes in the **Change Role** window. The following details are displayed:

Table 76: Change Role

Field	Description
General	
User Name	Name of the user. This field cannot be changed.
Choose User Type	Select either **Regular User** or **Slice User**.
Select Slice	Select an option from the drop down list. This option is displayed only if your User Type selection was **Slice User**.

Field	Description
Select Role	Click **Select Role** and the **Select Role** window is displayed. Choose a role using the radio button and click **Select** . This option is displayed only if your User Type selection was **Regular User**.

Step 5 Click **Save**.

Roles

The **Roles** tab displays details of the roles available on the NDB controller. The default roles are:

- Network-Admin
- Network-Operator

A table is displayed with the following details:

Column Name	Description
Role	The name of the role. The displayed name is a hyperlink. Click the **Role** name, a new pane is displayed on the right. Additional actions that can be performed from here are: • Assigning a Group to a Role

Column Name	Description
Level	The level assigned to the role. The following levels are available: • App-Administrator— Has full access to all Cisco Nexus Data Broker resources but the App-Administrator cannot add NXAPI or production devices into NDB because Administration tab is not available in NDB for App-Administrator role . • App-User—Has access to create, edit, clone, or delete connections and redirections that are assigned to his resource group and resources that are created by another user with similar permissions. An App-User can only view Edge-SPAN, Tap, Monitoring device, and Production ports. An App-User can view resources that are created by another user with similar permissions in Toplogy page of NDB. But, you can not configure Edge-SPAN or Connections created by another App-User. • App-Operator—Has access for read-only operations.
Group	The group assigned to the role.

The following actions can be performed from the **Roles** tab:

- **Add Role**—Use this to add a new role. See Adding a Rolefor details about this task.
- **Delete Role**—Select the roles to be deleted by checking the check box which is available at the beginning of the row and then click **Delete Role** from the **Actions** menu. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a role.

Note Default roles cannot be deleted.

Adding a Role

Use this procedure to add a role and associate the role to a group.

Before you begin

Create one or more groups to associate a role.

Step 1 Navigate to **Administration** > **User Management** > **Roles**.

Step 2 From the **Actions** drop down menu, select **Add Role**.

Step 3 In the **Add Role** dialog box, enter the following details:

Table 77: Add Role

Field	Description
Role Name	Enter the role name.
Select Level	Select a level from the drop-down list.

Step 4 Click **Add** to add the role.

Assigning a Group to a Role

Use this procedure to assign a group to a role. This enables the role to access only the ports in the assigned group.

Before you begin

Add one or more groups.

Step 1 Navigate to **Administration** > **User Management** > **Roles**.

Step 2 Click a **Role** name in the displayed table.

A new pane is displayed on the right.

Step 3 Click **Action** > **Assign Group**.

Enter the following details:

Table 78: Assign Group

Field	Description
Role Name	Role name. This field cannot be edited.
Select Level	Level of the role. This field cannot be edited.
Set Group	Click **Select Group** and select a group in the **Select Group** window that is displayed.

Step 4 Click **Assign**.

Groups

The **Groups** tab displays details of the port groups. The default group is:

- allPorts

A group can be a group of ports of one device or across many devices.

A table with the following details is displayed:

Column Name	Description
Group	The name of the group. The displayed name is a hyperlink. Click the name to see more details of the group.
Ports	The number of ports assigned to the group.

The following actions can be performed from the **Groups** tab:

- **Add Group**—Use this to add a new group. See Adding a Group for details.
- **Delete Group**—Select the groups to be deleted by checking the check box which is available at the beginning of the row and then click **Delete Group** from the **Actions** menu. If you choose the delete action without selecting a check box, an error is displayed. You will be prompted to select a group.

Note Default group(s) cannot be deleted.

Adding a Group

Use this procedure to create a new group.

A group is created for defining access to port(s) for a user. A group is assigned to a role; a user is associated to a role.

Step 1 Navigate to **Administration** > **User Management** > **Groups**.

Step 2 From the **Actions** drop down menu, select **Add Group**.

Step 3 In the **Add Group** dialog box, enter the following details:

Table 79: Add Group

Field	Description
Group Name	Enter the group name.
Selected Port(s)	Click **Select Ports**. In the **Select Ports** dialog box that opens, check the check box to assign port(s) to the group. The port details are displayed on the right side. Click **Select** to assign the port.

Step 4 Click **Add Group** to add the group.