



Deploying Cisco Nexus Data Broker

This chapter contains the following sections:

- [Installing Cisco Nexus Data Broker, page 1](#)

Installing Cisco Nexus Data Broker

Installing or Upgrading the Cisco Nexus Data Broker Software



Important

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

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

Installing the Cisco Nexus Data Broker Software

- Step 1** In a web browser, navigate to **www.cisco.com**.
- Step 2** Under **Support**, click **All Downloads**.
- Step 3** In the center pane, click **Cloud and Systems Management**.
- Step 4** If prompted, enter your Cisco.com **username** and **password** to log in.
- Step 5** In the right pane, click **Network Controllers and Applications**, and then click **Cisco Nexus Data Broker**. The file information for Release 3.2.0 is displayed: Cisco Nexus Data Broker Software Application: ndb1000-sw-app-k9-3.2.0.zip
- Step 6** Download the Cisco Nexus Data Broker application bundle.
- Step 7** Create a directory in your Linux machine where you plan to install Cisco Nexus Data Broker.

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

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

Step 9 Unzip the Cisco Nexus Data Broker zip file.

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

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

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

- `configuration` directory—The directory that contains the Cisco Nexus Data Broker initialization files. This directory also contains the `startup` subdirectory where configurations are saved.

- `bin` directory—The directory that contains the following script:

- `xnc` file—This script contains the Cisco Nexus Data Broker common CLI.

- `etc` directory—The directory that contains profile information.
- `lib` directory—The directory that contains the Cisco Nexus Data Broker Java libraries.
- `logs` directory—The directory that contains the Cisco Nexus Data Broker logs.

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

- `plugins` directory—The directory that contains the OSGi plugins.

- `work` directory—The webserver working directory.

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

Upgrading the Application Software

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



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

**Note**

When you upgrade the software, the hostname should not be changed during the upgrade process. While upgrading to Cisco Nexus Data Broker Release 3.2.0, user should not allowed to change the hostname. If the hostname is changed during the upgrade, the upgrade process is not done successfully.

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

Before You Begin

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

**Important**

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

**Note**

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

**Note**

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

- Step 1** In a web browser, navigate to [Cisco.com](https://www.cisco.com).
- Step 2** Under **Support**, click **All Downloads**.
- Step 3** In the center pane, click **Cloud and Systems Management**.
- Step 4** In the right pane, click **Network Controllers and Applications**, and then click **Cisco Nexus Data Broker**.
- Step 5** Download the Cisco Nexus Data Broker Release 3.2.0 application bundle: Cisco Nexus Data Broker Software Application—`ndb1000-sw-app-k9-3.2.0.zip`
- Step 6** Create a temporary directory in your Linux machine where you plan to upgrade to Cisco Nexus Data Broker. For example, in your `Home` directory, create `CiscoNDB_Upgrade`.

- Step 7** Extract the Cisco Nexus Data Broker Release 3.2.0 zip file into the temporary directory that you created.
- Step 8** Navigate to the `xnc` directory that was created when you installed the Cisco Nexus Data Broker release earlier.
- Step 9** Backup your Cisco Nexus Data Broker release installation using your standard backup procedures.
- Step 10** Stop running all Cisco Nexus Data Broker release processes.
- Step 11** Navigate to the `xnc/bin` directory in the temporary directory that you created for the Cisco Nexus Data Broker Release 3.2.0 upgrade software.
- Step 12** Upgrade the application by entering the `./xnc upgrade --perform --target-home {xnc_directory_to_be_upgraded} [--verbose] [--backupfile {xnc_backup_location_and_zip_filename}]` command.
You can use one of the following options:

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

- Step 13** Navigate to the `xnc` directory where you originally installed Cisco XNC Monitor Manager.
- Step 14** Start the application processes that you previously stopped.
Note Press Ctrl-F5, or press the Cmd, Shift, and R keys simultaneously when you access Cisco Nexus Data Broker through a web UI following an upgrade.
- Step 15** If you have any upgrade-related issues, perform the following tasks:
- Stop all application processes.
 - Navigate to the temporary directory that you created in Step 6.
 - Enter the `./xnc upgrade --rollback --target-home {xnc_directory_to_be_downgraded} --backupfile {xnc_backup_location_and_zip_filename} [--verbose]` command.
 - Restart the application processes.

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

Starting the Application

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

The *{password}* variable resets the administrator password to the value that you specify by restarting the user manager. The *{wait_time}* is the number of seconds to wait while the user manager restarts. The minimum *{wait_time}* value is 5 seconds and the maximum is 60 seconds.

- Note**
- If double ENTER is used instead of entering a value for the password, the password is set to the default vales, for example, **admin/admin**.
 - The password must be from 8 to 256 characters, contain both uppercase and lowercase characters, and have at least one number and one nonalphanumeric character.
 - If you leave the password blank, it is reset to the factory default of "admin".
 - Each time that you reset the administrative password, make sure that the new password meets these requirements or you will not be able to log in to Cisco Nexus Data Broker.

Step 2 Navigate to the `xnc` directory and start Cisco Nexus Data Broker by entering the **./runxnc.sh** command.

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

You can use one of the following options:

Option	Description
no option	Starts Cisco Nexus Data Broker with the -start option.
-jmx	Enables Java Management Extensions (JMX) remote access on the Cisco Nexus Data Broker JVM, which can be used to troubleshoot performance issues.
-jmxport <i>port_number</i>	Enables JMX remote access on the specified JVM port.
-debug	Enables debugging on the Cisco Nexus Data Broker JVM.
-debugsuspend	Suspends the Cisco Nexus Data Broker startup until a debugger is connected.
-debugport <i>port_number</i>	Enables debugging on the specified JVM port.
-start	Starts Cisco Nexus Data Broker and provides Secure Shell (SSH) access on port 2400. Note The SSH server can be accessed by any Cisco Nexus Data Broker user with the network-administrator role.

Option	Description
<code>-start port_number</code>	Starts Cisco Nexus Data Broker and provides SSH access to the controller on the specified port number. Note The SSH server can be accessed by any Cisco Nexus Data Broker user with the network-administrator role. The valid range of values for <code>port_num</code> is 1024 through 65535.
<code>-stop</code>	Stops Cisco Nexus Data Broker.
<code>-status</code>	Displays the status of Cisco Nexus Data Broker.
<code>-console</code>	Starts Cisco Nexus Data Broker with the OSGi console.
<code>-help</code>	Displays the options for the <code>./runxnc.sh</code> command.
<code>-tls</code>	Enables TLS secure connections between Cisco Nexus Data Broker and OpenFlow switches. To enable TLS, start the controller by entering the <code>./runxnc.sh -tls -tlskeystore keystore_file_location -tlstruststore truststore_file_location</code> command.
<code>-osgiPasswordSync</code>	To set the OSGi web console password same as the XNC password if the XNC password is changed. Note This step is optional. If the application is started without this option, the OSGi console can be accessed through the default credentials.

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

Verifying That The Application is Running

- Step 1** Open a command window where you installed Cisco Nexus Data Broker.
- Step 2** Navigate to the `xnc` directory that was created when you installed the software.
- Step 3** Verify that the application is running by entering the `./runxnc.sh -status` command. The controller outputs the following, which indicates that the controller is running the Java process with PID 21680:
- ```
Controller with PID:21680 -- Running!
```

**Note** Nexus Data Broker can be accessed via Web browser at:  
`https://Nexus_data_broker_ip:8443`

---

### **What to Do Next**

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

