Upgrading Cisco DCNM

This chapter provides information about upgrading Cisco DCNM, and contains the following section:

- Upgrading to Cisco DCNM Release 11.5(2), on page 1
- Upgrading to Cisco DCNM Release 11.5(1), on page 2
- Retaining the CA Signed Certificate, on page 4
- Upgrading to Cisco SAN on Windows from Release 11.4(1) to 11.5(1) from Release 11.5(1) to 11.5(2) from Release 11.5(1) to 11.5(4), on page 5
- Upgrading to Cisco SAN on Linux from Release 11.4(1) to 11.5(1) from Release 11.5(1) to 11.5(2), on page 10
- Upgrade Cisco DCNM SAN 11.2(1) or 11.3(1) to 11.5(1) on Windows and Linux Deployments, on page 15
- Dropping Performance Manager Data , on page 20

Upgrading to Cisco DCNM Release 11.5(2)

The following table summarizes the type of upgrade that you must follow to upgrade to Release 11.5(2).

Current Release Number	Deployment Type	Upgrade type to upgrade to Release 11.5(2)
11.5(1)	SAN OVA/ISO **Note** This upgrade is supported only for specific beta equipment support only. For all other supported hardware, we recommend that you deploy Cisco DCNM Release 11.5(1).	Software Maintenance Upgrade (SMU) version 11.5(2)
	SAN Windows and Linux Installers **Note** This upgrade is supported only for specific beta equipment only. For all other supported hardware, we recommend that you deploy Cisco DCNM Release 11.5(1).	To Windows →Inline Upgrade To Linux → Inline Upgrade

Upgrading to Cisco DCNM Release 11.5(1)

Before Cisco DCNM Release 11.0(1), DCNM OVA, and ISO supported SAN functionality. From Cisco DCNM Release 11.3(1), you can install Cisco DCNM for SAN Deployment on both OVA and ISO virtual appliances.

The following table summarizes the type of upgrade that you must follow to upgrade to Release 11.5(1).

Table 1: Type of Upgrade for Cisco DCNM SAN deployments

Current Release Number	Upgrade type to upgrade to Release 11.5(1)
11.4(1)	To Windows—Inline Upgrade To Linux—Inline Upgrade To OVA\ISO—Inline Upgrade

Current Release Number	Upgrade type to upgrade to Release 11.5(1)
11.3(1)	To Windows—Inline Upgrade To Linux—Inline Upgrade To OVA\ISO—Inline Upgrade
11.2(1)	To Windows—Inline Upgrade To Linux—Inline Upgrade To OVA\ISO— **1.** Fresh 11.3(1) SAN Only Installation. **2.** Migrate Performance Manager Collections to 11.3(1) **Note** The old Performance Manager data will replace any existing Performance Manager data on 11.3(1). **3.** Inline upgrade to 11.5(1)
11.1(1)	To Windows— 11.1(1) → 11.4(1) → 11.5(1) To Linux— 11.1(1) → 11.4(1) → 11.5(1) To OVA\ISO— **1.** Fresh 11.3(1) SAN Only Installation. **2.** Migrate Performance Manager Collections to 11.3(1). **Note** The old Performance Manager data will replace any existing Performance Manager data on 11.3(1). **3.** Inline upgrade to 11.5(1)

Cisco DCNM Release 11.5(2) offers a Software Maintenance Update (SMU) that can be applied only on top of the DCNM Release 11.5(1) for the OVA/ISO/Appliance form factor. In addition, DCNM Release 11.5(2) also offers Cisco SAN Deployment on Windows and Linux.

Current Release Number	Deployment Type	Upgrade type to upgrade to Release 11.5(2)
11.5(1)	SAN OVA/ISO **Note** This upgrade is supported only for specific beta equipment support only. For all other supported hardware, we recommend that you deploy Cisco DCNM Release 11.5(1).	Software Maintenance Upgrade (SMU) version 11.5(2)
	SAN Windows and Linux Installers **Note** This upgrade is supported only for specific beta equipment only. For all other supported hardware, we recommend that you deploy Cisco DCNM Release 11.5(1).	To Windows →Inline Upgrade To Linux → Inline Upgrade

Retaining the CA Signed Certificate

Perform this procedure if you need to retain the CA signed SSL Certificate after upgrade.

When you configure a 3-node federation setup and apply external CA certificate, do the following:

1. Stop DCNM servers in Federation.
   - For Windows – Navigate to `C:\Program Files\Cisco Systems\dcm\dcnm\bin`. Double-click on the `StopLANSANServer.bat` to stop the services.
   - For Linux – Logon to `/root`. Execute **/root/Stop_DCNM_Servers** command to stop services.
2. Generate CA certificates for Primary Servers, and apply the same CA certificate in the three secondary servers.
3. Start the Primary server first, then the secondary, third server thereafter, on Federation.

Note that if you change the keystore password or alias, you need to update it in the **standalone-san.xml** document located at:

`<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\standalone-san.xml`

Update the password in the **keystore** tag and alias:

```
<keystore key-password>="<<storepass-pwd>> key-alias="updated-key-alias"
keystore-password="updated-password"
path="<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks">
```

Note *<<storepass-pwd>>* is the password string generated while installing DCNM Server. This string is located in the `<install dir>/dcm/fm/conf/serverstore.properties` directory. Fetch the **dcnm.fmserver.token** value for the **storepass-pwd**.

Procedure

Step 1 Backup the signed certificate from the location:

- For Windows: **<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks**
- For Linux: **<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks**

Step 2 Upgrade to Cisco DCNM Release 11.5(1).

Step 3 After upgrade, copy the certificate to the same location on the upgraded version of the Cisco DCNM.

Note You must load the certificates to the same location as mentioned in Step 1, on page 5.

Step 4 Restart the DCNM Services.

Upgrading to Cisco SAN on Windows from Release 11.4(1) to 11.5(1) from Release 11.5(1) to 11.5(2) from Release 11.5(1) to 11.5(4)

The following sections provide instructions to upgrade Cisco DCNM SAN on Windows to the latest version:

Note Cisco DCNM SAN Deployment using Windows and Linux installers supports specific beta equipment support. To enable this support with DCNM SAN deployment, upgrade to Cisco DCNM Release 11.5(2). For all other supported hardware, we recommend that you deploy Cisco DCNM Release 11.5(1).

You can upgrade to DCNM Release 11.5(2) from DCNM Release 11.5(1) only.

Upgrading Cisco DCNM Windows using GUI

Before you begin

- Ensure that Cisco DCNM 11.4(1)11.5(1) is up and running.
- Ensure that the Elasticsearch service is operational.
- Before you start to upgrade, close all instances of DCNM SAN client and Device Manager running on the server.
- For DCNM SAN deployment on Windows, disable all Antivirus software for the entire duration of DCNM upgrade. The antivirus software might block the DCNM upgrade process.

Procedure

Step 1 Stop the DCNM services.

- For Windows – Navigate to `C:\Program Files\Cisco Systems\dcm\dcnm\bin`. Double-click on the `StopLANSANServer.bat` to stop the services.
- For Linux – Logon to `/root`. Execute **/root/Stop_DCNM_Servers** command to stop services.

Note When DCNM services are stopped, Elasticsearch is also stopped. You must restart the Elasticsearch service.

- For Windows – Launch the task manager on the Windows server. Choose **Services** tab. Select the **Elasticsearch** application. Right click on the application and choose **Start**.
- For Linux – Execute **service elasticsearch start** command.

Step 2 Run the Cisco DCNM software for Release 11.5(1)11.5(2) executable file.

The following message appears:

```
Please close the DCNM Installation wizard gracefully using "Done" option
on last installation step and wait for the installation wizard to close automatically.
Do not restart the system or forcefully terminate the Installation wizard while it is still
 in progress."
```

Click **OK** to continue.

Step 3 Click **OK** to begin the upgrade.

Step 4 Click **Done** after the upgrade is complete.

The Cisco DCNM Release 11.5(1)11.5(2) services will start automatically.

Upgrading Cisco DCNM Windows Federation using GUI

Note Ensure that both primary and secondary database properties are same.

Before you begin

- Ensure that Cisco DCNM 11.4(1)11.5(1) is up and running.
- Ensure that the Elasticsearch service is operational.
- Before you start to upgrade, close all instances of DCNM SAN client and Device Manager running on the server.
- For DCNM SAN deployment on Windows, disable all Antivirus software for the entire duration of DCNM upgrade. The antivirus software might block the DCNM upgrade process.

Procedure

Step 1 Stop both the primary and secondary DCNM services.

Note Ensure that the Elasticsearch service is running.

Step 2 On the primary server, run the Cisco DCNM Release 11.5(1)11.5(2) executable file.

Upgrade notification window appears.

The following message appears:

```
Please close the DCNM Installation wizard gracefully using "Done" option
on last installation step and wait for the installation wizard to close automatically.
Do not restart the system or forcefully terminate the Installation wizard while it is still
 in progress."
```

Click **OK** to continue.

Step 3 Click **OK** to begin the upgrade.

Step 4 On the primary server, click **Done** after the upgrade is complete.

The Cisco DCNM Release 11.5(1)11.5(2) services will start automatically on the primary server.

Step 5 On the secondary server, run the Cisco DCNM Release 11.5(1)11.5(2) executable file.

Upgrade notification window appears.

The following message appears:

```
Please close the DCNM Installation wizard gracefully using "Done" option
on last installation step and wait for the installation wizard to close automatically.
Do not restart the system or forcefully terminate the Installation wizard while it is still
 in progress."
```

Click **OK** to continue.

Step 6 Click **OK** to begin the upgrade.

Step 7 On the secondary server, click **Done** after the upgrade is complete.

The Cisco DCNM Release 11.5(1)11.5(2) services will start automatically on the secondary server.

Upgrading Cisco DCNM Windows through Silent Installation

Note Cisco DCNM supports Silent installation and upgrade only on Local Authorization mode and not on Remote Authorization mode.

Before you begin

- Ensure that Cisco DCNM 11.4(1)11.5(1) is up and running.
- Ensure that the Elasticsearch service is operational.
- Before you start to upgrade, close all instances of DCNM SAN client and Device Manager running on the server.
- For DCNM SAN deployment on Windows, disable all Antivirus software for the entire duration of DCNM upgrade. The antivirus software might block the DCNM upgrade process.

Procedure

Step 1 Stop the DCNM services.

Step 2 Open the installer.properties file and update the following properties:

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE

ORA_DB_PATH=C:\\oraclexe\\app\\oracle\\product\\10.2.0\\server
#---------------Use Existing Oracle-------------
DCNM_DB_URL=jdbc\:oracle\:thin\:@<ip_address_of_oracle_machine>\:1521\:XE
DCNM_DB_NAME=XE
SELECTED_DATABASE=oracle
DCNM_DB_USERNAME=oracledbadmin1
DCNM_DB_USER_PASSWORD=oracledbadmin1
```

Step 3 Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:

dcnm-release.exe -i silent -f *<path_of_installer.properties>*

The Cisco DCNM Release 11.5(1)11.5(2) services will start after the upgrade is complete.

You can check the status of the upgrade in the Task Manager process.

Upgrading Cisco DCNM Windows Federation through Silent Installation

Note Cisco DCNM supports Silent installation and upgrade only on Local Authorization mode and not on Remote Authorization mode.

Note Ensure that both primary and secondary database properties are same.

Before you begin

- Ensure that Cisco DCNM 11.4(1)11.5(1) is up and running.
- Ensure that the Elasticsearch service is operational.
- Before you start to upgrade, close all instances of DCNM SAN client and Device Manager running on the server.
- For DCNM SAN deployment on Windows, disable all Antivirus software for the entire duration of DCNM upgrade. The antivirus software might block the DCNM upgrade process.

Procedure

Step 1 Stop both the primary and secondary DCNM services.

Step 2 On the primary server, open the installer.properties file and update the following properties:

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
```

Step 3 Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:

dcnm-release.exe -i silent -f *<path_of_installer.properties>*

You can check the status of the upgrade in the Task Manager process.

The Cisco DCNM Release 11.5(1)11.5(2) services will start automatically on the primary server.

Step 4 On the secondary server, open the installer.properties file and update the following properties:

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE

ORA_DB_PATH=C:\\oraclexe\\app\\oracle\\product\\10.2.0\\server
#---------------Use Existing Oracle-------------
DCNM_DB_URL=jdbc\:oracle\:thin\:@<ip_address_of_oracle_machine>\:1521\:XE
DCNM_DB_NAME=XE
SELECTED_DATABASE=oracle
DCNM_DB_USERNAME=oracledbadmin1
DCNM_DB_USER_PASSWORD=oracledbadmin1
```

Step 5 Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:

dcnm-release.exe -i silent -f <*path_of_installer.properties*>

You can check the status of the upgrade in the Task Manager process.

The Cisco DCNM Release 11.5(1)11.5(2) services will start automatically on the secondary server.

Upgrading Cisco DCNM Windows Federation when Elasticsearch Schema is modified

Before you begin

Ensure that the Elasticsearch must be running on 2 nodes in the Federation setup.

Procedure

Step 1 Stop the following DCNM services:

- For Windows – Navigate to `C:\Program Files\Cisco Systems\dcm\dcnm\bin`. Double-click on the `StopLANSANServer.bat` to stop the services.
- For Linux – Logon to `/root`. Execute **/root/Stop_DCNM_Servers** command to stop services.

Step 2 Upgrade Primary server first, and then the Secondary server in the Federation setup. For instructions, see Upgrading Cisco DCNM Windows Federation through Silent Installation, on page 9.

Step 3 Start the DCNM Services.

Upgrading to Cisco SAN on Linux from Release 11.4(1) to 11.5(1) from Release 11.5(1) to 11.5(2)

The following sections provide instructions to upgrade Cisco DCNM SAN on Linux to the latest version:

Note Cisco DCNM SAN Deployment using Windows and Linux installers supports specific beta equipment support. To enable this support with DCNM SAN deployment, upgrade to Cisco DCNM Release 11.5(2). For all other supported hardware, we recommend that you deploy Cisco DCNM Release 11.5(1).

You can upgrade to DCNM Release 11.5(2) from DCNM Release 11.5(1) only.

Upgrading Cisco DCNM Linux using GUI

Before you begin

- Ensure that Cisco DCNM 11.4(1)11.5(1) is up and running.
- Ensure that the Elasticsearch service is operational.
- Before you start to upgrade, close all instances of DCNM SAN client and Device Manager running on the server.

Procedure

Step 1 Stop the DCNM services.

Note Ensure that the Elasticsearch service is running.

Step 2 Run the Cisco DCNM software for Release 11.5(1)11.5(2) executable file.

Upgrade Notification window appears

Step 3 Click **OK** to begin the upgrade.

The following message appears:

```
Please close the DCNM Installation wizard gracefully using "Done" option
on last installation step and wait for the installation wizard to close automatically.
Do not restart the system or forcefully terminate the Installation wizard while it is still
 in progress."
```

Click **OK** to continue.

Step 4 Click **Done** after the upgrade is complete.

The Cisco DCNM Release 11.5(1)11.5(2) services will start automatically.

What to do next

After you upgrade from Cisco DCNM Release 11.2(1) on Linux Standalone server, ensure that you clear the browser cache and Java console cache before you launch the Web UI and download the SAN Client. The Java console remembers the previous version of the SAN client data. If you do not clear Java console cache, you will not be able to use the latest downloaded SAN Client.

Upgrading Cisco DCNM Linux Federation using GUI

Note Ensure that both primary and secondary database properties are same.

Before you begin

- Ensure that Cisco DCNM 11.4(1)11.5(1) is up and running.
- Ensure that the Elasticsearch service is operational.
- Before you start to upgrade, close all instances of DCNM SAN client and Device Manager running on the server.

Procedure

Step 1 Stop both the primary and secondary DCNM services.

Note Ensure that the Elasticsearch service is running.

Step 2 On the primary server, run the Cisco DCNM Release 11.5(1)11.5(2) executable file.

Upgrade notification window appears.

The following message appears:

```
Please close the DCNM Installation wizard gracefully using "Done" option
on last installation step and wait for the installation wizard to close automatically.
Do not restart the system or forcefully terminate the Installation wizard while it is still
 in progress."
```

Click **OK** to continue.

Step 3 Click **OK** to begin the upgrade.

Step 4 On the primary server, click **Done** after the upgrade is complete.

The Cisco DCNM Release 11.5(1)11.5(2) services will start automatically on the primary server.

Step 5 On the secondary server, run the Cisco DCNM Release 11.5(1)11.5(2) executable file.

Upgrade notification window appears.

The following message appears:

```
Please close the DCNM Installation wizard gracefully using "Done" option
on last installation step and wait for the installation wizard to close automatically.
Do not restart the system or forcefully terminate the Installation wizard while it is still
 in progress."
```

Click **OK** to continue.

Step 6 Click **OK** to begin the upgrade.

Step 7 On the secondary server, click **Done** after the upgrade is complete.

The Cisco DCNM Release 11.5(1)11.5(2) services will start automatically on the secondary server.

Upgrading Cisco DCNM Linux through Silent Installation

Note Cisco DCNM supports Silent installation and upgrade only on Local Authorization mode and not on Remote Authorization mode.

Note You must use the same database for Release 11.5(1)11.5(2) as in the existing DCNM set up.

Before you begin

- Ensure that Cisco DCNM 11.4(1)11.5(1) is up and running.
- Ensure that the Elasticsearch service is operational.
- Before you start to upgrade, close all instances of DCNM SAN client and Device Manager running on the server.

Procedure

Step 1 Stop the DCNM services.

Step 2 Open the `installer.properties` file and update the following properties:

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
```

Step 3 Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:

dcnm-release.bin -i silent -f *<path_of_installer.properties>*

The Cisco DCNM Release 11.5(1)11.5(2) services will start after the upgrade is complete.

You can check the status of the upgrade process by using the following command: **ps -ef | grep 'LAX'**. The prompt will return after the silent install is complete.

Upgrading Cisco DCNM Linux Federation through Silent Installation

Note Cisco DCNM supports Silent installation and upgrade only on Local Authorization mode and not on Remote Authorization mode.

Note Ensure that both primary and secondary database properties are same as in the previous Release set up.

Before you begin

- Ensure that Cisco DCNM 11.4(1)11.5(1) is up and running.
- Ensure that the Elasticsearch service is operational.
- Before you start to upgrade, close all instances of DCNM SAN client and Device Manager running on the server.

Procedure

Step 1 Stop both the primary and secondary DCNM services.

Step 2 On the primary server, open the `installer.properties` file and update the following properties:

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
```

Step 3 Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:

dcnm-release.bin -i silent -f <*path_of_installer.properties*>

You can check the status of the upgrade process by using the following command: **ps -ef | grep 'LAX'**. The prompt will return after the silent install is complete.

The Cisco DCNM Release 11.5(1)11.5(2) services will start automatically on the primary server.

Step 4 On the primary server, click **Done** after the upgrade is complete.

The Cisco DCNM Release 11.5(1)11.5(2) services will start automatically on the primary server.

Step 5 On the secondary server, open the installer.properties file and update the following properties:

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
```

Step 6 Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:

dcnm-release.bin -i silent -f <*path_of_installer.properties*>

You can check the status of the upgrade process by using the following command: **ps -ef | grep 'LAX'**. The prompt will return after the silent install is complete.

The Cisco DCNM Release 11.5(1)11.5(2) services will start automatically on the secondary server.

Upgrading Cisco DCNM Linux Federation when Elasticsearch Schema is modified

Before you begin

Ensure that the Elasticsearch must be running on 2 nodes in the Federation setup.

Procedure

Step 1 Stop the following DCNM services:

- For Windows – Navigate to `C:\Program Files\Cisco Systems\dcm\dcnm\bin`. Double-click on the `StopLANSANServer.bat` to stop the services.
- For Linux – Logon to `/root`. Execute **/root/Stop_DCNM_Servers** command to stop services.

Step 2 Upgrade Primary server first, and then the Secondary server in the Federation setup. For instructions, see Upgrading Cisco DCNM Linux Federation through Silent Installation, on page 13.

Step 3 Start the DCNM Services.

Upgrade Cisco DCNM SAN 11.2(1) or 11.3(1) to 11.5(1) on Windows and Linux Deployments

This sections includes the following topics:

Reindexing PMDB before upgrade to DCNM SAN Release 11.5(1)

If the Elasticsearch is not compatible for upgrade, you must reindex the performance manager data before upgrading to Release 11.5(1). To reindex the performance manager data, perform the following task:

If the existing Elasticsearch database is more than 250GB, Cisco DCNM Server requires more than 500GB HDD space to complete reindexing.

Procedure

Step 1 Stop the **FMServer** to prevent further population of old PM index.

Step 2 If alarms and DCNM database indices are created with Elasticsearch version 2.3, then reindex the alarms indices and delete the DCNM database indices.

- Reindex alarms using the **ReindexAlarmsCurl.bat** script for DCNM on Windows.

  Use **ReindexAlarmsCurl.sh** for DCNM on Linux and OVA/ISO.

- Delete **dcnmdb** index.
  - For Elasticsearch in Release 11.2(1)

    curl -XDELETE -k --tlsv1.2 https://localhost:9200/dcmdb
  - For Elasticsearch in Release 11.3(1)

    curl -XDELETE http://localhost:9200/dcmdb

Step 3 Delete the old PMDB index using **DeletePMDBIndexCurl.bat** script for DCNM on Windows.

Use **DeletePMDBIndexCurl.sh** for DCNM on Linux and OVA/ISO.

Note Reindexing task may still run in background if user gets http timeout code 504.

PmdbReindex.log file is generated for PMDB reindexing script.

Step 4 Verify if the Elasticsearch is not reindexing in the background, using the following commands:

This command output shows reindex tasks running in background.

- For Elasticsearch in Release 11.2(1)

  curl -XGET -k --tlsv1.2 "https://localhost:9200/_tasks?detailed=true&actions=*reindex&pretty=true"

- For Elasticsearch in Release 11.3(1)

  curl -XGET "http://localhost:9200/_tasks?detailed=true&actions=*reindex&pretty=true"

What to do next

After reindexing is complete, you can upgrade the DCNM to Release 11.5(1).

Upgrading Cisco DCNM Using GUI from Release 11.2(1) or 11.3(1) to 11.5(1)

As the Elasticsearch version supported in 11.2(1) and 11.3(1) is not compatible with the Elasticsearch supported with 11.5(1), you must reindex the Elasticsearch data before upgrading to Release 11.5(1).

The upgrade script will verify if the current version of Elasticsearch is compatible for upgrade. If it is not compatible, the upgrade process stops. When you run the upgrade script, the upgrade process terminates when it encounters the non-compatible performance data. You must reindex the data and continue with the upgrade.

If the existing Elasticsearch database is more than 250GB, Cisco DCNM Server requires more than 500GB HDD space to complete reindexing.

To upgrade Cisco DCNM Windows/Linux from 11.2(1) or 11.3(1) to Release 11.5(1), perform the following steps.

Before you begin

- Ensure that Cisco DCNM 11.2(1) or 11.3(1) is up and running.
- Ensure that the Elasticsearch service is operational.

  Elasticservice service must be operation on all nodes in a federation setup.
- Before you start to upgrade, close all instances of DCNM SAN client and Device Manager running on the server.
- For DCNM SAN deployment on Windows, disable all Antivirus software for the entire duration of DCNM upgrade. Antivirus software might block the DCNM upgrade process.

Additionally for Federation setup, perform upgrade in the following order:

1. Upgrade the Primary node.

Start the services. Reindex the primary node PM data.

2. Upgrade the Secondary node.

   Start the services.

3. Upgrade the Tertiary node.

   Start the services.

Procedure

Step 1 Stop the DCNM services.

Note Ensure that the Elasticsearch service is running.

For Federation setup, ensure that the Elasticsearch is running on all nodes for upgrade to continue.

Step 2 Run the Cisco DCNM software for Release 11.5(1) executable file.

The following message appears:

```
Please close the DCNM Installation wizard gracefully using "Done" option
on last installation step and wait for the installation wizard to close automatically.
Do not restart the system or forcefully terminate the Installation wizard while it is still
 in progress."
```

Click **OK** to continue.

Step 3 Click **OK** to begin the upgrade.

The installer verifies if the Elasticsearch is upgradable.

- If the Elasticsearch is not compatible for upgrade, the following error message is generated.

  ```
  Elasticsearch indices need manual reindexing
   Some Elastic Search indices are created with ES version 2.3.
   Please reindex these manually and proceed with upgrade.
   Reindexing package can be downloaded from CCO. DCNM Installer will now quit.
  ```

  Click **OK** to stop the upgrade process.

  You must reindex the PMDB data and begin to upgrade. For instructions to reindex PM data, see Reindexing PMDB before upgrade to DCNM SAN Release 11.5(1), on page 15.

- If the Elasticsearch upgrade is compatible, or if you've completed the reindexing the Elasticsearch, the process continues.

The Elasticsearch is also upgraded as a part of DCNM upgrade to Release 11.5(1). After the upgrade is complete, a message regarding the reindexing of the old PMDB data is generated.

```
PM DB manual reindexing
PMDB Elastic Search index needs to be reindexed manually using the
scripts under INSTALL_DIR/dcnm/dcnm/fm/reindexes/esmapping.
The old PMDB data will be available after reindexing.
```

Step 4 Click **Done** after the upgrade is complete.

The following message is generated:

```
Elasticsearch(ES) indices for historical Performance Monitoring (PM)
data need to be reindexed manually.
Check DCNM installation and upgrade guide for more details.
```

Step 5 Click **OK**.

The Cisco DCNM Release 11.5(1) services will start automatically.

Note Upgrade process will not reindex PMDB data. You must perform this task manually. If you need the PMDB data from the previous version on Release 11.5(1), you must reindex the data manually. For instructions to reindex PMDB data manually, see Reindexing PMDB post upgrade to DCNM SAN Release 11.5(1), on page 19.

Upgrading Cisco DCNM through Silent Installation from Release 11.2(1) or 11.3(1) to 11.5(1)

As the Elasticsearch version supported in 11.2(1) and 11.3(1) is not compatible with the Elasticsearch supported with 11.5(1), you must reindex the Elasticsearch data before upgrading to Release 11.5(1).

The upgrade script will verify if the current version of Elasticsearch is compatible for upgrade. If it is not compatible, the upgrade process stops. When you run the upgrade script, the upgrade process terminates when it encounters the non-compatible performance data. You must reindex the data and continue with the upgrade.

If the existing Elasticsearch database is more than 250GB, Cisco DCNM Server requires more than 500GB HDD space to complete reindexing.

To upgrade Cisco DCNM Windows/Linux from 11.2(1) or 11.3(1) to Release 11.5(1), perform the following steps.

Before you begin

- Ensure that Cisco DCNM 11.2(1) or 11.3(1) is up and running.
- Ensure that the Elasticsearch service is operational.
- Before you start to upgrade, close all instances of DCNM SAN client, both SAN Client and Device Manager running on the server.
- For DCNM SAN deployment on Windows, disable all Antivirus software for the entire duration of DCNM upgrade. Antivirus software might block the DCNM upgrade process.

Additionally for Federation setup, perform upgrade in the following order:

1. Upgrade the Primary node.

   Start the services. Reindex the primary node PM data.

2. Upgrade the Secondary node.

   Start the services.

3. Upgrade the Tertiary node.

   Start the services.

Procedure

Step 1 Stop the DCNM services.

Note Ensure that the Elasticsearch service is running.

For Federation setup, ensure that the Elasticsearch is running on all nodes for upgrade to continue.

Step 2 Open the installer.properties file and update the following properties:

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
```

Step 3 Go to the directory where you downloaded the Cisco DCNM software and run the appropriate installer by using the following command:

dcnm-release.exe -i silent -f *<path_of_installer.properties>*

If the Elasticsearch is not compatible for upgrade, the upgrade stops. An error message is generated in the **error.properties** file. You must reindex the PMDB data and begin to upgrade. For instructions about how to reindex see Reindexing PMDB before upgrade to DCNM SAN Release 11.5(1), on page 15.

If the Elasticsearch upgrade is compatible, or if you've completed the reindexing the Elasticsearch, the process continues.

What to do next

The Cisco DCNM Release 11.5(1) services will start after the upgrade is complete. You can check the status of the upgrade in the Task Manager process.

The message to reindex PMDB is generated in the **dcnm_installer.log** file.

Note Upgrade process will not reindex PMDB data. You must perform this task manually. If you need the PMDB data from the previous version on Release 11.5(1), you must reindex the data manually. For instructions to reindex PMDB data manually, see Reindexing PMDB post upgrade to DCNM SAN Release 11.5(1), on page 19.

The following message is included in the **dcnm_installer.log** file.

```
Elasticsearch(ES) indices for historical Performance Monitoring (PM)
data need to be reindexed manually.
Check DCNM installation and upgrade guide for more details.
```

Reindexing PMDB post upgrade to DCNM SAN Release 11.5(1)

If the Elasticsearch is not compatible for upgrade, you must reindex the performance manager data before upgrading to Release 11.5(1). To reindex the performance manager data, perform the following tasks:

If the existing Elasticsearch database is more than 250GB, Cisco DCNM Server requires more than 500GB HDD space to complete reindexing.

Before you begin

After you upgrade DCNM Release 11.2(1) or 11.3(1) to Release 11.5(1), you must delete the old PM database index.

If you choose to conserve the Performance Manager data when you upgrade to Release 11.5(1), we recommend that you contact Cisco TAC for further assistance.

Procedure

Step 1 Navigate to the **esmapping** directory, and locate the following scripts:

For DCNM on Windows:

- ReindexPMDBCurl.bat
- DeletePMDBIndexCurl.bat

Note Windows installation may need curl utility. Please install curl utility. A zip file is provided as **curl-win64.zip** in the **/esmapping** directory.

For DCNM on Linux:

- ReindexPMDBCurl.sh
- DeletePMDBIndexCurl.sh

If you choose to conserve the Performance Manager data when you upgrade to Release 11.5(1), we recommend that you contact Cisco TAC for further assistance.

Step 2 Run **ReindexPMDBCurl.bat** script for DCNM on Windows, or **ReindexPMDBCurl.sh** script for DCNM on Linux.

Ensure that you don't see any errors while running the script. Collect the output from the script to a file and verify is all the files are reindexed.

PmdbReindex.log file is generated for PMDB reindexing script.

Dropping Performance Manager Data

Note If you choose to conserve the Performance Manager data when you upgrade to Release 11.5(1), we recommend that you contact Cisco TAC for further assistance.

To drop the Performance Manager (PM) data, perform the following steps:

Before you begin

- Ensure that the DCNM appliance is operational. (for standalone upgrade)

- If you have a Federation setup, ensure that all the nodes in the DCNM Federation setup are operational. (for Federation setup)

Procedure

Step 1 Launch the SSH session and run the following command to view the PMDB indices.

Identify the PMDB indices in the performance manager database.

For example:

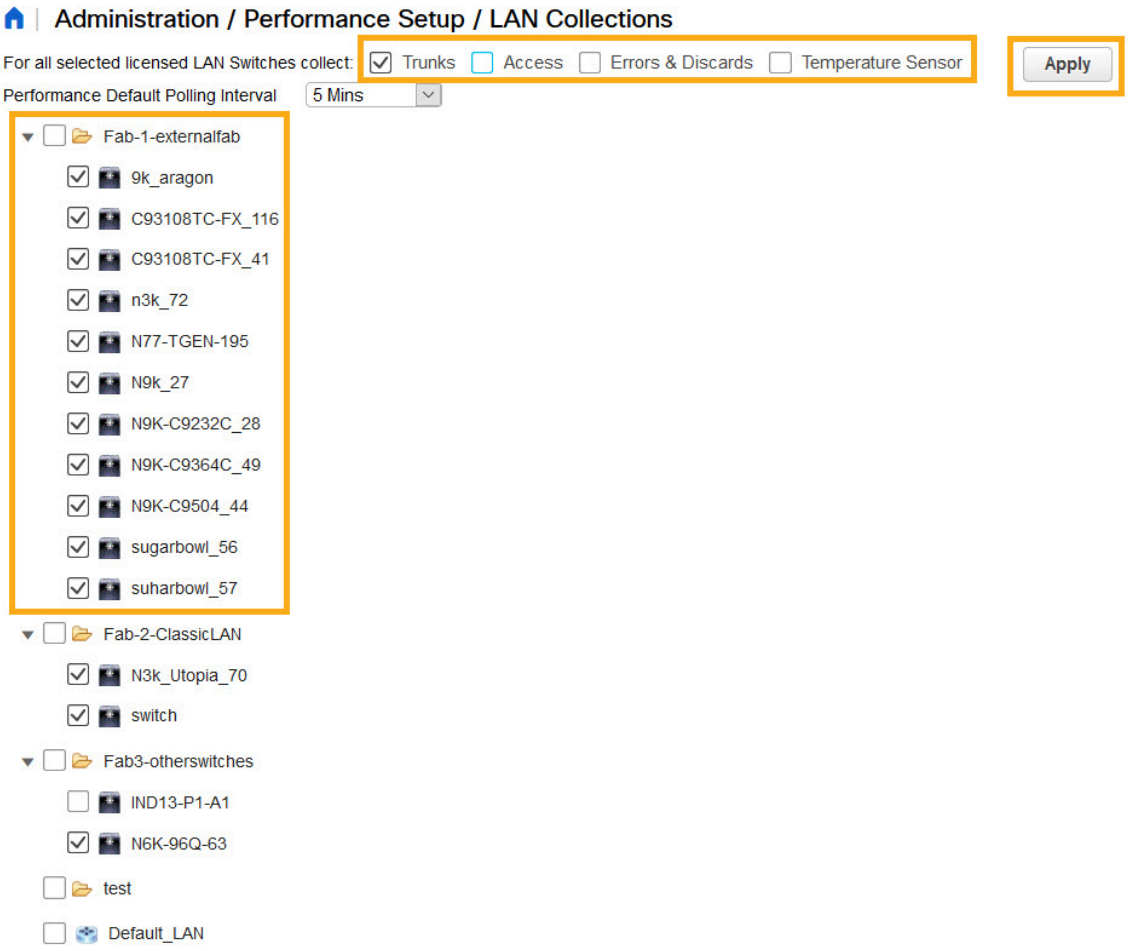
```
dcnm-root-11-4# curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb

  % Total    % Received % Xferd  Average Speed    Time    Time     Time  Current
                                 Dload   Upload   Total   Spent    Left  Speed
100  2448  100  2448    0     0   4523      0 --:--:-- --:--:-- --:--:--  4524
green open pmdb_cpumemdata                        rb-CJf-NR0my8M3mO-7QkA 5 1  7286   0
1.4mb 760.2kb
green open pmdb_ethintfratedata                   P18gMKdPTkCODv0TomYAdw 5 1  9283   0
2.4mb   1.2mb
```

You will see indices prefixed with "pmdb_"

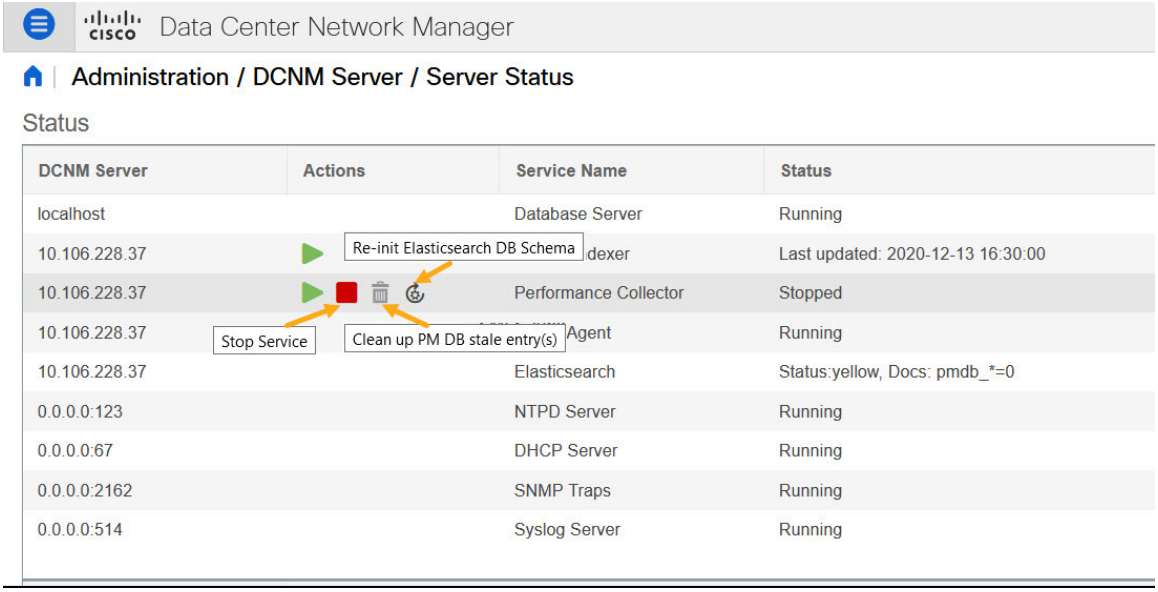
Step 2 On the Cisco DCNM Web UI, choose **Administration > Performance Setup > LAN Collections**.

Uncheck all the check boxes and click **Apply** to disable all switches and collections.



Step 3 Choose **Administration > DCNM Server > Server Status**.

Step 4 Against the **Performance Collector** service, click the stop icon in the Actions column to stop the data collection.



Step 5 Click the delete icon to clean the Performance Manager database.

This action deletes the stale entries in the performance manager database.

Step 6 Click on the reinitialize icon to reindex the Elasticsearch database schema.

This operation cleans the performance manager data in the Elasticsearch database and restarts the performance manager. It may take a few minutes to complete.

Step 7 Click **Continue**.

The status of the Performance Collector service shows **Stopped**.

Step 8 Ensure that you've deleted all the PMDB entries using the following command:

- For upgrading from Release 11.1(1)

  curl https://127.0.0.1:33500/_cat/indices?pretty | grep pmdb
- For upgrading from Release 11.2(1)

  curl https://127.0.0.1:33500/_cat/indices?pretty | grep pmdb
- For upgrading from Release 11.3(1)

  curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb
- For upgrading from Release 11.4(1)

  curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb

For example:

```
dcnm-root-11-4# curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb

  % Total    % Received % Xferd  Average  Speed   Time    Time     Time  Current
                                 Dload    Upload  Total   Spent    Left  Speed
100  2244  100  2244    0     0   3638      0 --:--:-- --:--:-- --:--:--  3636
```

Step 9 Proceed to upgrade the DCNM to Release 11.5(1).