CHAPTER 4

Upgrading Cisco Prime DCNM

This section includes instructions for upgrading your Cisco Prime DCNM Open Virtual Appliance installation in the following scenarios:

Cisco Prime DCNM Installer version	Release from which you can upgrade
DCNM 7.2(1) ISO/OVA	• Cisco Prime DCNM, Release 7.1(1) • Cisco Prime DCNM, Release 7.1(2)
DCNM 7.2(1) EXE/BIN	• Cisco Prime DCNM, Release 6.3(2) • Cisco Prime DCNM, Release 7.1(1) • Cisco Prime DCNM, Release 7.1(2)
DCNM 7.2(2) ISO/OVA and DCNM 7.2(2) EXE/BIN	• Cisco Prime DCNM, Release 7.1(1) • Cisco Prime DCNM, Release 7.1(2) • Cisco Prime DCNM, Release 7.2(1)
DCNM 7.2(2a) ISO/OVA and DCNM 7.2(2a) EXE/BIN	• Cisco Prime DCNM, Release 7.1(1) • Cisco Prime DCNM, Release 7.1(2) • Cisco Prime DCNM, Release 7.2(1) • Cisco Prime DCNM, Release 7.2(2)
DCNM 7.2(3) ISO/OVA and DCNM 7.2(3) EXE/BIN	• Cisco Prime DCNM, Release 7.1(1) • Cisco Prime DCNM, Release 7.1(2) • Cisco Prime DCNM, Release 7.2(1) • Cisco Prime DCNM, Release 7.2(2) • Cisco Prime DCNM, Release 7.2(2a)

You can migrate Cisco Prime DCNM with a local PostgreSQL database and an external Oracle database and Cisco Prime DCNM in a High Availability (HA) environment.

Note In Cisco DCNM for SAN Release 6.x, the HA setup for XMPP uses external oracle database. You must provide username and password for external oracle database. Create a new username and password for the XMPP application to use in the same remote Database instance, used by the Cisco Prime DCNM. Do not use the following characters in your password: “&$%’ and <SPACE>.

Note Before upgrading Cisco Prime DCNM, ensure that auto move is disabled. Otherwise, if one server within the federation is down, the devices discovered by the server will be moved to the other DCNM server which comes up first after upgrade. To prevent the auto move for DCNM upgrade, you need to disable the auto move on all DCNMs within the federation, and then upgrade the DCNM server one by one. Only after all the DCNMs upgrade successfully and run normally, then enable the auto move again.
To enable / disable auto move, please go to **Admin > Federation** from DCNM web page, click on the checkbox at top left for **Enable Automatic Failover**.

This chapter contains the following:

Retaining the CA Signed Certificate

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

DETAILED STEPS

Step 1 Backup the signed certificate from the location

<DCNM_install_root>\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks

Step 2 Upgrade to Cisco DCNM for SAN Release 6.x based on the requirement.

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

Note You must load the certificates to the same location as mentioned in Step 1.

Step 4 Open the following files:

- <Install root>/dcm/JBoss- 7.2.0.Final/standalone/configuration/standalone-san.xml
- <Install root>/dcm/JBoss- 7.2.0.Final/standalone/configuration/ standalone-lan.xml

Step 5 Search for **key-alias**="sme" and replace with key-alias="<key-alias used to create CA signed SSL Certificate>"

Step 6 Restart the DCNM Services.

Upgrading Cisco Prime DCNM Windows and Linux through GUI Installation

Before you begin, make sure that Cisco Prime DCNM 6.x is up and running.

DETAILED STEPS

Step 1 Stop the DCNM services.

Step 2 Run the Cisco DCNM for SAN Release 6.x executable file.

Upgrade Notification window appears

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

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

The Cisco DCNM for SAN Release 6.x services will start automatically.

Upgrading Cisco Prime DCNM Windows and Linux through Silent Installation

Before you begin, make sure that Cisco Prime DCNM Release 7.1.x is up and running.

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

DETAILED STEPS

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 Prime DCNM software and run the appropriate installer by using the following command:

- For Windows installer—*dcnm-release.exe -i silent -f <path_of_installer.properties>*
- For Linux installer—*dcnm-release.bin -i silent -f <path_of_installer.properties>*

The Cisco DCNM for SAN Release 6.x services will start after the upgrade is complete.

Note For Windows upgrade, you can check the status of the upgrade in the Task Manager process.

For Linux upgrade, 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 the Cisco Prime DCNM Windows and Linux Federation through GUI Installation

Before you begin, make sure that the Cisco Prime DCNM 7.1(x) is up and running.

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

Step 1 Stop both the primary and secondary DCNM services.

Step 2 On the primary server, run the Cisco Prime DCNM Release 7.2(x) executable file.

Upgrade notification window appears.

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

Step 4 On the secondary server, perform run the Cisco Prime DCNM Release 7.2(x) executable file.

Upgrade notification window appears.

Step 5 Click **OK** to begin the upgrade.

Step 6 On the primary server, click **Done** after the upgrade is complete.

The Cisco Prime DCNM Release 7.2(x) services will start automatically on the primary server.

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

The Cisco Prime DCNM Release 7.2(x) services will start automatically on the secondary server.

Upgrading Cisco Prime DCNM Windows and Linux Federation through Silent Installation

Before you begin, make sure that the Cisco Prime DCNM 7.1(x) is up and running.

Note Cisco Prime 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.

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 Prime DCNM software and run the appropriate installer by using the following command:

- For Windows installer—*dcnm-release.exe -i silent -f <path_of_installer.properties>*
- For Linux installer—*dcnm-release.bin -i silent -f <path_of_installer.properties>*

Note For Windows upgrade, you can check the status of the upgrade in the Task Manager process.

For Linux upgrade, 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.

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

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

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

- For Windows installer—*dcnm-release.exe -i silent -f <path_of_installer.properties>*
- For Linux installer—*dcnm-release.bin -i silent -f <path_of_installer.properties>*

Step 6 On the primary server, click **Done** after the upgrade is complete.

The Cisco Prime DCNM Release 7.2(x) services will start automatically on the primary server.

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

The Cisco Prime DCNM Release 7.2(x) services will start automatically on the secondary server.

Upgrading Cisco Prime DCNM Appliance with a Local PostgreSQL Database

Before you begin, make sure that Cisco Prime DCNM 7.1(2) is up and running.

DETAILED STEPS

Step 1 Use the appmgr backup all command to backup all applications associated with the installation of Cisco Prime DCNM 7.1(2).

A prompt appears to provide the DCNM DB password and XMPP DB password. By default, this password is the administrative password provided during the Open Virtual Appliance installation.

Step 2 On Cisco Prime DCNM 7.2(1), ensure that the MAC addresses along with all network settings such as the IP address, default gateway, hostname, etc., are identical to the Cisco Prime DCNM 7.1(2) installation.

Step 3 Transfer the backup file to an external file system.

Step 4 Power off Cisco Prime DCNM 7.1(2).

Step 5 Deploy the Cisco Prime DCNM Open Virtual Appliance file for version 7.2(1).

- Use the same network parameters (IP address/subnet/gateway/DNS).
- Use the same administrative password.
- Use the same vCenter port groups for both network interfaces.
- Disable auto-power-on. (The Power on Open Virtual Appliance after deployment check-box should not be selected).

Step 6 After Cisco Prime DCNM 7.2(1) is deployed, right-click on **VM > Edit Settings > Hardware**.

For both Network Adapters, update the MAC address to be the same as Cisco Prime DCNM 7.1(2). This ensures that the same MAC address is used for the new Virtual Machine (VM); licenses on Cisco Prime DCNM will not need to be regenerated in the event of an upgrade.

Step 7 Power on DCNM 7.2(1) VM.

Step 8 Copy the Cisco Prime DCNM 7.1(2) backup file from the external repository to Cisco Prime DCNM 7.2(1).

Step 9 Use the appmgr status all command to make sure that all applications are up and running.

Step 10 Use the appmgr stop all command to shut down all applications on Cisco Prime DCNM 7.2(1).

Step 11 Use the appmgr upgrade <backup filename> command to run the upgrade script on Cisco Prime DCNM 7.2(1).

The application displays the following message:

```
Please Shut Down All Applications Before Continuing.
Press 'y' to continue [y/n] [n]
```

Step 12 Press **Y** to continue.

Press [1] or [2] or [3] when prompted, based on your Cisco Prime DCNM 7.1(2) setup:

Choose [1] Standalone DCNM with Local PostgreSQL database

[2] Standalone DCNM with External Oracle database

[3] High Availability

If you choose option [1] Standalone DCNM with Local PostgreSQL database, It will get upgraded successfully.

If you choose option [2] Standalone DCNM with External Oracle database, ensure that the external database is up and running. For more information, see Upgrading Cisco Prime DCNM Virtual Appliance with External Oracle Database, page 4-7.

Upgrading Cisco Prime DCNM Virtual Appliance with External Oracle Database

When you select Option [2] in Step 12 of the procedure Upgrading Cisco Prime DCNM Appliance with a Local PostgreSQL Database, page 4-5, the following query appears:

Prior to upgrade, we strongly advise that you make a backup of your remote Oracle instance. Do you want to proceed with upgrade?

Press 'y' to continue [y/n] [n]

Step 1 Press **Y** to continue.

Step 2 Enter the DB URL.

`Example: jdbc:oracle:thin:@10.2.3.4:1521:XE`

Step 3 Enter the DB username

Step 4 Enter the DB password.

Enter it again for verification:

Step 5 Choose the XMPP DB type as per backup:

```
[1] Local Postgre | [2] External Oracle     [1]
```

If you choose option [1], go to Step 6.

If you choose option [2], perform the following steps:

a. Enter the XMPP DB URL.

b. Enter the XMPP database username.

c. Enter the XMPP database password.

Step 6 Enter the administrative password provided during Virtual Appliance installation, when prompted for the root password.

The external DCNM database will be configured to access all the Fabric applications using the root password of this server.

Note You can change the password using the Cisco Prime DCNM Web Client, from **Admin > Fabric Settings.**

```
Root password:
Enter it again for verification:
```

Upgrading Cisco Prime DCNM appliances in High Availability Environment

Before you begin, make sure that both the Cisco DCNM 7.1(x) Active and Standby peers are up and running.

Note Note For more information on Active and Standby peers in a High Availability environment, see "Managing Applications in a High-Availability Environment".

DETAILED STEPS

Step 1 Verify if the **appmgr backup all** command was executed on both the Active and Standby peers. Check if separate tar archives are stored in an external file system.

```
Example: active.tar.gz and standby.tar.gz
```

Note If it is the non-DFA environment, please verify if the **appmgr backup dcnm** command was executed on both the Active and Standby peers.

Step 2 Power off the Cisco Prime DCNM 7.1(x) Active peer.

Step 3 Wait for 4 to 5 minutes, before you stop all the DCNM applications by using **appmgr stop all** command on the Cisco Prime DCNM 7.1.(x) Standby peer.

This is to ensure that the write operations to LDAP are completed, and avoid LDAP from entering an inconsistent state.

Step 4 Power-on the Cisco Prime DCNM 7.2(x) Active peer.

Step 5 Use the **appmgr status all** command to ensure that all the applications are up and running on the Cisco Prime DCNM 7.1(2) Active peer.

Step 6 Stop all DCNM applications on the Cisco Prime DCNM 7.2.(x) Active peer, by using **appmgr stop all** command.

Step 7 Use the **appmgr upgrade <active.tar.gz>** command to run the upgrade script.

```
a. PLEASE SHUT DOWN ALL APPLICATIONS BEFORE CONTINUING.
        Press 'y' to continue [y/n] [n]
y
b.  Choose option [3] High Availability when prompted.
Choose option [1] Standalone DCNM with Local PostgreSQL database
[2] Standalone DCNM with External Oracle database
[3] High Availability

c. Prior to upgrade, we strongly advise that you make a backup of your remote Oracle
instance. Do you want to proceed with upgrade?
        Press 'y' to continue [y/n] [n]
y

d.  Select option [1] Active when prompted.
Choose [1] Active [2] Standby

f.  Enter the standby eth0 IP address.
g.  Enter the Management IP Address of the peer DCNM (eth0 IP).
h.  Enter the root password of the peer.
i.  Enter the Database username for XMPP tables.
j.  Enter the Database password for XMPP tables.
k.  Enter the Database password for XMPP tables again for verification.
l.  Enter the common FQDN for VIP on both DCNM management and EFM networks:
After the upgrade is completed successfully, you will see the following message:
**** Check /root/upgrade.log for details...****
Ensure that all applications are running on the Cisco Prime DCNM 7.1(2) Active peer.
```

Step 8 Power off the Cisco Prime DCNM 7.1(x) Standby peer.

Step 9 Power on the Cisco Prime DCNM 7.2(x) Standby peer. Use the **appmgr status all** command to make sure that all applications are up and running.

Step 10 Stop all applications on the Cisco Prime DCNM 7.2(x) Standby peer.

Step 11 Use the **appmgr upgrade <standby.tar.gz>** command to run the upgrade script on the Cisco Prime DCNM 7.1(x) Standby peer.

a. Choose option **[3] High Availability** when prompted.

```
Choose option [1] Standalone DCNM with Local PostgreSQL database
              [2] Standalone DCNM with External Oracle database
              [3] High Availability
```

b. Select option **[2] Standby** when prompted.

```
Choose [1] Active [2] Standby
```

To migrate the standby peer, perform the following:

a. Enter the **active eth0 IP** address.

Step 12 Invoke the following on the Active peer to establish SSH trust to the Standby peer:

sh /root/sshAutoLogin.sh <STANDBY_PEER_IP>

Upgrading Cisco Prime DCNM appliances (non-unified fabric installation) in HA Environment

Before you begin, make sure that virtual appliance should be installed in Non Unified Fabric mode.

Note For instruction about installing these applications with the Cisco DCNM Open Virtual Appliance, see DCNM Non-Unified Fabric Installation, page 3-18.
For more information on NON DFA High Availability environment, see Managing Applications in a High-Availability Environment, page 6-1.

DETAILED STEPS

Step 1 Make sure that both Cisco Prime DCNM 7.1(x) servers are deployed, powered on and made it as a First and Federated node by using the below commands.

appmgr setup ha -type first-node and appmgr setup ha -type federated-node

Step 2 Verify if the **appmgr backup dcnm** command was executed on both the First Node and Federated Node using the below command. Check if separate tar archives are stored in an external file system.

Example: **first_node.tar.gz and federated_node.tar.gz**

Step 3 Bring up the DCNM 7.2(3) Active and Standby peer. Do not power on the DCNM yet.

a. Power-off the Cisco Prime DCNM 7.2(1) Active peer. Wait for five minutes.

b. Stop the Cisco Prime DCNM 7.2(1) Standby peer, using the command:

appmgr stop dcnm

c. Power-on Cisco Prime DCNM 7.2(3) Active peer. Check the status by using the command:

appmgr status dcnm

d. Stop the Cisco Prime DCNM 7.2(3) Active peer, by using the command.

appmgr stop dcnm

e. Copy the files saved during the backup of 7.2(1) Active peer to the root directory.

f. Copy the RRD files also to the Cisco Prime DCNM 7.2(3) Active peer.

Use **$INSTALLDIR/dcm/fm/pm** folder and **PM.sh** script for syncing PM data

g. Upgrade the DCNM using the command:

appmgr upgrade <*active.tar.gz*>

h. Start Cisco Prime DCNM Active peer, by using the command:

appmgr start dcnm

i. Check if Cisco Prime DCNM 7.2(3) Active peer is up and running.

j. Power-off the Cisco Prime DCNM 7.2(1) Standby peer. Wait for five minutes.

k. Power-on Cisco Prime DCNM 7.2(3) standby peer.

l. Stop the Cisco Prime DCNM 7.2(3) Standby peer, using the command:

appmgr stop dcnm

m. Copy the files saved during the backup of 7.2(1) Standby peer to the root directory.

n. Copy the RRD files also to the Cisco Prime DCNM 7.2(3) Standby peer.

Use **$INSTALLDIR/dcm/fm/pm** folder and **PM.sh** script for syncing PM data

o. Upgrade the DCNM using the command:

appmgr upgrade <standby.tar.gz>

p. Start Cisco Prime DCNM Active peer, by using the command:

appmgr start dcnm

q. Check if Cisco Prime DCNM 7.2(3) Standby peer is up and running.

r. Invoke the following on the Active peer to establish SSH trust to the Standby peer:

/'sh/root/sshAutoLogin.sh STANDBY_PEER'

Step 4 Power off the Cisco Prime DCNM 7.1(x) First and Federated Node virtual appliance.

Step 5 Power-on the Cisco Prime DCNM 7.2(3) First and Federated Node virtual appliance which should be deployed in the same eth0 IP of 7.1(x).

Step 6 Use the appmgr status all command to ensure that DCNM applications are up and running on the Cisco Prime DCNM 7.2(3) First and Federated Nodes.

Step 7 Stop the applications on the Cisco Prime DCNM 7.2(3) First node, by using **appmgr stop dcnm** command.

Step 8 Use the command **appmgr upgrade <first_node.tar.gz>** on the Cisco Prime DCNM 7.2(3) First node to run the upgrade script. After issuing **appmgr upgrade <first_node.tar.gz>** on First Node, user will be prompted for various inputs. Provide the inputs as per the sample given below.

PLEASE SHUT DOWN ALL APPLICATIONS BEFORE CONTINUING. .

Press 'y' to continue [y/n] [n]

y

Select an option for upgrading this appliance [ ] :

[1] Standalone DCNM with Local PostgreSQL database

[2] Standalone DCNM with External Oracle database

[3] High Availability

Choice [1|2|3]

3

Prior to upgrade, we strongly advise that you make a backup of your remote Oracle instance.
Do you want to proceed with upgrade?

Press 'y' to continue [y/n] [n]

y

Please enter the type of server:

[1] First Node | [2] Federated Node [1]

1

****

You are about to be federated for DCNM alone in this DCNM appliance.

Please make sure that you have the following

1. An Oracle Database with a user defined for DCNM.

2. A repository with NFS capabilities.

3. An NTP server for time synchronization.

****

a) Do you want to continue? [y/n] [y]

b) Enter the DB URL {ex. jdbc:oracle:thin:@ipaddr:1521:<SID or Servicename>} :

c) Enter the DB username for DCNM tables: <dcnm-dbuser>

d) Enter the DB password for DCNM tables :

e) Enter it again for verification:

f) Enter the SCP/NFS repository IP : <repository IP>

g) NFS Exported location {ex. /var/shared/dcnm/} :

h) Enter an NTP server for time synchronization "NTP_SERVER":

**********************Successfully Completed. Run 'appmgr start dcnm'****************

i) Verify whether HA Federation enabled after upgrade by using command "appmgr show ha-role".

j) Start DCNM using "appmgr start dcnm".

Step 9 Stop DCNM applications on the Cisco Prime DCNM 7.2(3) Federated Node by using **appmgr stop dcnm** command.

Step 10 Use the **appmgr upgrade <federated_node.tar.gz>** command to run the upgrade script on the Cisco Prime DCNM 7.2(3) Federated Node. After issuing **appmgr upgrade <first_node.tar.gz>** on First Node, user will be prompted for various inputs. Provide the inputs as per the sample given below.

PLEASE SHUT DOWN ALL APPLICATIONS BEFORE CONTINUING..

Press 'y' to continue [y/n] [n]

Y

Select an option for upgrading this appliance [] :

[1] Standalone DCNM with Local PostgreSQL database

[2] Standalone DCNM with External Oracle database

[3] High Availability

Choice [1|2|3]

3

Prior to upgrade, we strongly advise that you make a backup of your remote Oracle instance. Do you want to proceed with upgrade?

Press 'y' to continue [y/n] [n]

Y

Please enter the type of server :

[1] First Node | [2] Federated Node [1]

2

****

You are about to enable High Availability for DCNM alone in this DCNM appliance.

Please make sure that you have the following

1. An Existing Federated server.

****

a)Do you want to continue? [y/n] [y]

b)Enter the existing Federated server IP (eth0 IP) : <PEER_ETH0_IP>

c)Enter the root password of the peer

d)Root password : <root_password_of_this_node>

********** **Successfully Completed.**********

e)Verify whether HA Federation enabled after upgrade using command "appmgr show ha-role".

Database Utility Scripts

Local PostgreSQL Database Utility Scripts for Backup and Restore

Utility scripts for Local PostgreSQL database that is installed in RHEL machine are:

1. backup-pgsql-dcnm-db.sh
2. restore-pgsql-dcnm-db.sh

Utility scripts for Local PG database that is installed in Windows machine are:

1. backup-pgsql-dcnm-db.bat
2. restore-pgsql-dcnm-db.bat

Remote Oracle Database Utility Scripts for Backup and Restore

Irrespective of the platform, Cisco Prime DCNM is installed (Windows or Linux), the following scripts to backup and restore the remote Oracle database.

Utility scripts for Oracle database that is installed on Linux platform are;

1. backup-remote-oracledb.sh
2. restore-remote-oracledb.sh

Utility scripts for Oracle database that is installed on Windows platform are:

1. backup-remote-oracledb.bat
2. restore-remote-oracledb.bat

Cisco Prime DCNM host is configured to run with a remote Oracle database. As part of housekeeping, you can copy DCNM utility scripts to a remote Oracle database and restore the DCNM database schema.

To run the utility scripts, you need the database administrator credentials. These scripts will prompt you for:

1. DCNM database password (the user name is already present)
2. Username/password of the admin user.

While entering the DBA user credentials, ensure that you do not to enter “sys” as sysdba" because in some versions of Oracle, the presence of space might cause the backup/restore to fail. Instead, user should provide valid user credentials that does not have a space in the user name, for example, system or sysdba. The admin credentials are not saved/cached and hence they do not leak sensitive credential information.

Note User scripts under ***dcnm/bin*** can be run only by administrator user.