Installing the Cisco DCNM

This chapter contains the following sections:

Installing Cisco DCNM on Windows

Perform the following tasks to install Cisco DCNM on Windows.

Uninstalling the Cisco DCNM on Windows

Perform this procedure to uninstall Cisco DCNM on Windows.

Note We recommend that you follow these steps in the same order.

Before you begin

You must remove the Cisco DCNM instance completely before you use the same server to install a different version of DCNM.

Procedure

Step 1 Stop Cisco DCNM Services.

Step 2 Uninstall the Postgres database.

Step 3 Uninstall the Cisco DCNM.

Step 4 Navigate to `C:\Users\Administrator` location, and delete **.cisco_mds9000** folder.

Step 5 Navigate to `C:\Program Files\Zero G Registry` location, and delete the **Zero G Registry** folder.

Step 6 Navigate to `C:\Users\Administrator` location, and delete **InstallAnywhere** folder.

Step 7 Ensure that all the ports required for Cisco DCNM installation are free and available.

Step 8 Delete the Cisco DCNM directory.

Step 9 Restart the Windows VM.

Downloading the Cisco DCNM Windows Installer and Properties File

The first step to installing the DCNM on Windows is to download the dcnm.exe file.

Note If you plan to use Federation application functions, you must deploy the dcnm.exe file twice.

Procedure

Step 1 Go to the following site: http://software.cisco.com/download/ .

Step 2 In the Select a Product search box, enter Cisco Data Center Network Manager.

Click on Search icon.

Step 3 Click on **Data Center Network Manager** from the search results.

A list of the latest release software for Cisco DCNM available for download is displayed.

Step 4 In the Latest Releases list, choose .

Step 5 Locate the DCNM Windows Installer and click the **Download** icon.

The installer file is of the format .

Step 6 Locate the DCNM Silent Installer Property Files and click the **Download** icon.

This file will be used during Silent Installation.

Step 7 Save both the files to your directory that will be easy to find when you begin the installation.

Installing Cisco DCNM on Windows Using the GUI

Perform the following steps to install DCNM Windows using the GUI:

Procedure

Step 1 Locate the `dcnm.exe` file that you have downloaded.

Double click on the `dcnm.exe` file.

InstallAnywhere progress bar appears showing the progress.

Step 2 On the Introduction screen, read the instructions.

Choose a vendor from the OEM Vendor drop-down list.

- Cisco Systems, Inc—to install Cisco Data Center Network Manager.
- IBM—to install the IBM Data Center Network Manager.

Click **Next**.

Step 3 Check **Add server to existing federation** checkbox if DCNM is installed as a secondary appliance in a Federation setup.

Step 4 Check **Secure Ciphers** checkbox to allow only switches with strong ciphers to be discovered by DCNM.

Step 5 To install DCNM-SAN and SMI-S for the first time, choose the location for installation. In the Install Location field, click **Choose**, and provide the appropriate folder path. Click **Restore Default Folder** if DCNM is installed as a part of the Federation setup.

Click **Next**.

Step 6 Choose the appropriate RDBMS for the DCNM server.

Select the database that is based on your requirement.

- Install PostgreSQL—Installs the PostgreSQL database that is bundled along with the dcnm.exe.
- Existing PostgreSQL 9.4
- Existing Oracle 10g/11g/12c
- Existing Oracle 10g/11g/12c RAC

  In the Service Name field, enter the service name of the Oracle RAC server. Enter a maximum of three host IP addresses. Click OK. The DB URL is generated.

If the Cisco DCNM installer detected an existing RDBMS installation, the DB URL field shows the hostname.

Cisco DCNM installation with existing PostgresSQL requires an existing schema with the same name as the DCNM username, which is owned by the same username. When there are no schemas existing with the DCNM username, or if you do not have the ownership of the schema with the same dcnmuser name, the tables are created in the default schema, which is known as “public”.

Note You cannot upgrade the DCNM Server with tables created in the default public schema.

Note In Oracle, when a new user is created, a schema name with the same name as the username is created automatically.

In the DCNM DB User field, enter the username that the Cisco DCNM uses to access the database. In the DCNM DB Password field, enter the password for the database user account that you specified. If you select **Add Server to an existing federation**, modify the database URL by selecting the corresponding RDBMS option. Because all the servers in federation refer to the same database, you must provide the dcnmuser name and password of the primary server.

Click **Next**. Review the limitations with Oracle Database and click **OK**.

Click **Next**.

Step 7 In the Port Configuration Options screen, choose the interface and web ports for Cisco DCNM.

- From the Server IP Address list, choose the IP address that you want to use for the Cisco DCNM server. The list shows only the IP addresses currently that are assigned to network interfaces on the server system.

- If you want to change the port that the Cisco DCNM-SAN web server listens to, enter the new port number in the SAN Web Server Port field. By default, the Cisco DCNM-SAN web server listens to TCP port 443.

  Note During Cisco DCNM installation, use port numbers that are not commonly used. For example, 87 and 23 are reserved or restricted web ports.

Click **Next**.

Step 8 In the Choose archive Folder for DCNM screen, provide a folder path to store device configuration files, user preferences and so on.

Perform one of the following:

- Click **Choose** to select a path to store the DCNM LAN archive directory.

  Note If you must choose a remote system, provide the UNC path. For example: `//Server/Share/directorypath`.

- Click **Restore Default Folder** to retain the default folder.

  Note Ensure that this folder is accessible by all nodes in the Federation setup.

Click **Next**.

Step 9 In the Local User Credentials screen, provide a valid username and password to access both DCNM SAN and DCNM LAN appliances.

- In the Admin Username field, enter a name for a Cisco DCNM server user. The installer creates the Cisco DCNM server user and assigns the Administrator role to it.
- In the Password field, enter a password for the user, and in the Confirm Password field, reenter the password.

  Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application may not function properly:

  - It must be at least 8 characters long and contain at least one alphabet and one numeral.
  - It can contain a combination of alphabets, numerals, and special characters.
  - Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

Click **Next**.

Step 10 In the Authentication Settings screen, choose the authentication method that the Cisco DCNM server should use to authenticate users who log on to the Cisco DCNM client. You can choose one of the following:

- **Local**—Cisco DCNM client users are authenticated by the Cisco DCNM server user accounts only.
- **RADIUS**—Cisco DCNM client users are authenticated by a RADIUS server.
- **TACACS+**—Cisco DCNM client users are authenticated by a TACACS+ server.

You can configure LDAP authentication after installing DCNM.

Note After TACACS/RADIUS/LDAP is enabled, Local user "admin" cannot be accessible. This is default behavior.

Only if the TACACS/RADIUS/LDAP server is not reachable or down, the Local user will be validated and will be able to login.

If LDAP/RADIUS/TACACS server is reachable and authentication fails on TACACS/LDAP/RADIUS then no fall back to local.

Step 11 If you chose RADIUS or TACACS+, do the following:

a) In the primary server address field, enter the IPv4 address of the server in dotted-decimal format.
b) In the primary server key field, enter the shared secret of the server.
c) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
d) In the secondary server address field, enter the IPv4 address of the server in dotted-decimal format.
e) In the secondary server key field, enter the shared secret of the server.
f) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
g) In the tertiary server address field, enter the address of the server in the dotted-decimal format.
h) In the tertiary server key field, enter the shared secret of the server.
i) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.

Click **Next**.

Step 12 In the Choose Shortcut Folder screen, specify path where you want to create the DCNM icons.

If you want the installer to create the shortcuts for all users who can log into the server system, check the **Create icons for All Users** check box.

Click **Next**.

Step 13 In the Pre-Installation Summary screen, review the installation configuration.

Click **Previous** to go to the previous tabs and modify the configuration.

Click **Next**.

Step 14 On the confirmation window, click **Yes** to begin the DCNM installation.

The progress bar description shows the process during the installation.

Step 15 On the Install Complete screen, the installed components are listed. Click **Done** to start the DCNM server.

Wait until the DCNM is deployed on the system.

The prompt will return after the silent install is complete.

Step 16 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM on Windows for LAN and SAN Management.

Installing Cisco DCNM Windows in a Server Federation Environment using GUI

To install DCNM in a server federation environment:

Before you begin

Ensure that you have installed DCNM on the Primary server. Follow the instructions provided in Installing Cisco DCNM on Windows Using the GUI, on page 2 section.

Procedure

Step 1 While installing DCNM on the Secondary server, check **Add server to existing federation** checkbox.

This makes the DCNM installed as a secondary appliance in a Federation setup. The Pre-installation Summary screen displays the Federation status and nodes in the Federation Settings area.

Step 2 Check Secure Ciphers checkbox to allow only switches with strong ciphers to be discovered by DCNM, only if the Secure Ciphers was enabled on the Primary.

Cisco DCNM uses both strong and weak ciphers when connecting to switches. If user you wants to use only strong ciphers for network, select the checkbox. Ensure that the switches in your network support strong ciphers before you select checkbox, as DCNM will not be able to connect to switches which do not support strong ciphers.

Step 3 Modify the database URL by selecting the corresponding RDBMS option.

Note All the servers in federation refer to the same database, and therefore you must provide the DCNM user name and password of the primary server. Also, you must provide the database user name and password of the primary server.

The user name and password of the database are same for all the server installation forming the federation. Similarly, the user name and password of DCNM are same for all the server installation forming the federation.

Installing Cisco DCNM Windows through Silent Installation

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

Perform the following steps to install DCNM Windows through silent installation.

Procedure

Step 1 Unzip, extract and open the `installer.properties` file and update the following properties.

```
#-----------------BASIC Properties---------------------
DCNM_IP_ADDRESS=<ip_address_of_host_machine>
USER_INSTALL_DIR=C:\\Program Files\\Cisco Systems
INSTALLATION_TYPE=NEW_INSTALL
#INSTALLATION_TYPE=UPGRADE
SAN_FEDERATION=FALSE
#SAN_FEDERATION=TRUE
```

Step 2 Configure the database parameters.

If you are using PostgreSQL database, edit this block:

```
#------------------DATABASE Properties--------------------
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#----------------------------------------------------
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE

PG_DB_PATH=C:\\Program Files\\Cisco Systems\\dcm\\db

#----------New Postgres---------------------------------
DCNM_DB_URL=jdbc\:postgresql\://localhost\:5432/dcmdb
DCNM_DB_NAME=dcmdb
SELECTED_DATABASE=postgresql
DCNM_DB_USERNAME=dcnmuser
DCNM_DB_USER_PASSWORD=dcnmuser
```

If you are using the Oracle database, edit this block:

```
#------------------DATABASE Properties--------------------
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#----------------------------------------------------
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE

ORA_DB_PATH=C:\\oraclexe\\app\\oracle\\product\\10.2.0\\server
```

Step 3 Configure the user credentials for DCNM.

```
#-----------------User Configuration-----------------
#DCNM User Configuration Properties
#If you want to use special characters in DCNM_ADMIN
#credentials,Please use escape character(\) before
#the symbol [For eg. Password  "an$6x12" must be specified as "an\$6x12" ].
#----------------------------------------------------

DECRYPT_PASSWORDS=FALSE
DCNM_ADMIN_USER=admin
DCNM_ADMIN_USER_PASSWORD=admin123

#-----------------User Configuration-----------------
```

Step 4 Enable the Secure Ciphers.

```
#----------------Secure Ciphers-------------------------------------
#DCNM uses both strong and weak ciphers when connecting to switches
#If user wants to use only strong ciphers for connection, please set
#property to TRUE. Make sure your switches support strong ciphers before
#setting the property as DCNM will not be able to connect to switches which
#support only weak ciphers.

#-----------------------------------------------------------------------
SECURE_CIPHER=FALSE
#SECURE_CIPHER=TRUE
#-----------------------------------------------------------------------
```

Step 5 Configure IBM Raven to install IBM Data Center Network Manager.

```
#------------------------------IBM Raven Support----------------------
#Set true if Vendor is IBM, by default false
#---------------------------------------------------------------------
```

```
IBM_INSTALL=FALSE /*Does not install IBM Data Center Network Manager*/
#-----------------------------------------------------------------
```

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

dcnm-release.exe -i silent -f *path_of_installer.properties_file*

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

Step 7 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM for SAN Management.

Installing Cisco DCNM on Linux

Perform the following tasks to install Cisco DCNM on Linux.

Uninstalling the Cisco DCNM on Linux

Perform this procedure to uninstall Cisco DCNM on Linux.

Note We recommend that you follow these steps in the same order.

Before you begin

You must remove the Cisco DCNM instance completely before you use the same server to install a different version of DCNM.

Procedure

Step 1 Stop DCNM services on the DCNM server using the **/root/Stop_DCNM_Servers** command.

Step 2 Uninstall the Postgres database using the <<*dcnm_directory_location*>**/db/uninstall-postgresql** command.

Step 3 Uninstall the Cisco DCNM Server using the **/root/Uninstall_DCNM** command.

Step 4 Delete the hidden `.cisco_mds9000` file, using the **rm -rf .cisco_mds9000** command.

Step 5 Delete the Zero G Registry using the **rm -rf /var/.com.zerog.registry.xml** command.

Step 6 Delete the hidden `InstallAnywhere` folder using the **rm -rf .InstallAnywhere** command.

Step 7 Ensure that all the ports required for Cisco DCNM installation are free and available.

Step 8 Delete the DCNM directory using the **rm -rf /usr/local/cisco/***. Delete the DCNM directory if you've saved in any other directory.

Step 9 Restart the RHEL system.

Uninstalling the Cisco DCNM on Linux

The following sample shows the list of commands that you must run, to uninstall te Cisco DCNM on Linux.

```
[dcnm-linux]# /root/Stop_DCNM_Servers
[dcnm-linux]# /<<dcnm_installed dir>>/db/uninstall-postgresql
[dcnm-linux]# /root/Uninstall_DCNM
[dcnm-linux]# rm -rf .cisco_mds9000
[dcnm-linux]# rm -rf /var/.com.zerog.registry.xml
[dcnm-linux]# rm -rf .InstallAnywhere
[dcnm-linux]# rm -rf /usr/local/cisco/*
[dcnm-linux]# restart
[dcnm-linux]#
```

Downloading the Cisco DCNM Linux Installer and Properties File

The first step to installing the DCNM on Linux is to download the dcnm.bin file.

Note If you plan to use Federation application functions, you must deploy the dcnm.bin file twice.

Procedure

Step 1 Go to the following site: http://software.cisco.com/download/ .

Step 2 In the Select a Product search box, enter Cisco Data Center Network Manager.

Click on Search icon.

Step 3 Click on **Data Center Network Manager** from the search results.

A list of the latest release software for Cisco DCNM available for download is displayed.

Step 4 In the Latest Releases list, choose Release 11.1(1).

Step 5 Locate the DCNM Linux Installer and click the **Download** icon.

The installer file is of the format `dcnm-installer-x64.11.1.1.bin`.

Step 6 Locate the DCNM Silent Installer Property Files and click the **Download** icon.

This file will be used during Silent Installation.

Step 7 Save both the files to your directory that will be easy to find when you begin the installation.

Installing Cisco DCNM on Linux Using the GUI

Perform the following steps to install DCNM Linux using the GUI:

Procedure

Step 1 Locate the `dcnm-installer-x64.<release-name>.bin` file that you have downloaded.

Run the `dcnm.bin` installer file.

InstallAnywhere progress bar appears showing the progress.

Step 2 On the Introduction screen, read the instructions.

Choose a vendor from OEM Vendor drop-down list.

- Cisco Systems, Inc—to install Cisco Data Center Network Manager
- IBM—to install IBM Data Center Network Manager

Click **Next**.

Step 3 Check **Add server to existing federation** checkbox if DCNM is installed as a secondary appliance in a Federation setup.

Step 4 Check **Secure Ciphers** checkbox to allow only switches with strong ciphers to be discovered by DCNM.

Step 5 To install DCNM-SAN and SMI-S for the first time, choose the location for installation. In the Install Location field, click **Choose**, and provide the appropriate folder path. Click **Restore Default Folder** if DCNM is installed as a part of the Federation setup.

Click **Next**.

Step 6 Choose the appropriate RDBMS for the DCNM server.

Select the database that is based on your requirement.

- Install PostgreSQL—Installs the PostgreSQL database that is bundled along with the `dcnm.bin`.
- Existing PostgreSQL 9.4—Existing PostgreSQL database that is already set up, with a clean schema.
- Existing Oracle 10g/11g/12c—Existing Oracle database that is already set up, with a clean schema.
- Existing Oracle 10g/11g/12c RAC—Existing Oracle database that is already set up, with a clean schema.

In the Service Name field, enter the service name of the Oracle RAC server. Enter a maximum of three host IP addresses. Click **OK**. The DB URL is generated.

If the Cisco DCNM installer detected an existing RDBMS installation, the DB URL field shows the hostname.

Note Cisco DCNM installation with existing PostgresSQL requires an existing schema with the same name as the DCNM username, which is owned by the same username. When there is no schema existing with the DCNM username, or if you do not have the ownership of the schema with the same dcnmuser name, the tables are created in the default schema, known as “public”.

If the tables are created in the default schema, you may encounter authentication issues after upgrading Cisco DCNM. You will have to create a schema with the sane name as the DCNM username owned by the same username. For instructions, see User and Schemas.

Note In Oracle, when a new user is created, a schema name with the same name as the username is created automatically.

In the **DCNM DB User** field, enter the username that Cisco DCNM user uses to access the database. In the **DCNM DB Password** field, enter the password for the database user account that you specified. If you select

Add Server to an existing federation, modify the database URL by selecting the corresponding RDBMS option. Because all the servers in Federation refer to the same database, you must provide the dcnmuser name and password of the primary server.

Click **Next**. Review the limitations with Oracle Database and click **OK**.

Click **Next**.

Step 7 In the Port Configuration Options screen, choose the interface and web ports for Cisco DCNM.

- From the Server IP Address list, choose the IP address that you want to use for the Cisco DCNM server. The list shows only the IP addresses currently that are assigned to network interfaces on the server system.
- If you want to change the port that the Cisco DCNM-SAN web server listens to, enter the new port number in the SAN Web Server Port field. By default, the Cisco DCNM-SAN web server listens to TCP port 443.

  Note During Cisco DCNM installation, use port numbers that are free. For example, 87 and 23 are reserved or restricted web ports.

Click **Next**.

Step 8 In the Choose archive Folder for DCNM screen, provide a folder path to store device configuration files, user preferences and so on.

Perform one of the following:

- Click **Choose** to select a path to store the DCNM archive directory.

  Note If you must choose a remote system, provide the UNC path. For example: `//Server/Share/directorypath`.
- Click **Restore Default Folder** to retain the default folder.

Click **Next**.

Step 9 In the Local User Credentials screen, provide a valid username and password to access DCNM SAN appliances.

- In the Admin Username field, enter a name for a Cisco DCNM server user. The installer creates the Cisco DCNM server user and assigns the Administrator role to it.
- In the Password field, enter a password for the user, and in the Confirm Password field, reenter the password.

  Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application may not function properly:

  - It must be at least eight characters long and contain at least one alphabet and one numeral.
  - It can contain a combination of alphabets, numerals, and special characters.
  - Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

Click **Next**.

Step 10 In the Authentication Settings screen, choose the authentication method that the Cisco DCNM server must use to authenticate users who log on to the Cisco DCNM client. You can choose one of the following:

- **Local**—Cisco DCNM client users are authenticated by the Cisco DCNM server user accounts only.
- **RADIUS**—Cisco DCNM client users are authenticated by a RADIUS server.
- **TACACS+**—Cisco DCNM client users are authenticated by a TACACS+ server.

Step 11 If you chose RADIUS or TACACS+, do the following:

a) In the primary server address field, enter the IPv4 address of the server in dotted-decimal format.
b) In the primary server key field, enter the shared secret of the server.
c) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
d) In the secondary server address field, enter the IPv4 address of the server in dotted-decimal format.
e) In the secondary server key field, enter the shared secret of the server.
f) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
g) In the tertiary server address field, enter the address of the server in the dotted-decimal format.
h) In the tertiary server key field, enter the shared secret of the server.
i) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.

Click **Next**.

The Choose Link Folder is skipped and by default the location is `/root` directory.

Step 12 In the Pre-Installation Summary screen, review the installation configuration.

Click **Previous** to go to the previous tabs and modify the configuration.

Click **Next**.

Step 13 On the confirmation window, click **Yes** to begin the DCNM installation.

The progress bar description shows the process during the installation.

Step 14 On the Install Complete screen, the installed components are listed. Click **Done** to start the DCNM server.

Wait until the DCNM is deployed on the system.

Step 15 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM for SAN Management.

Installing Cisco DCNM Linux in a Server Federation Environment Using GUI

To install DCNM in a server federation environment:

Before you begin

Ensure that you have installed DCNM on the Primary server. Follow the instructions in Installing Cisco DCNM on Linux Using the GUI, on page 9 section.

Procedure

Step 1 While installing DCNM on the Secondary server, check **Add server to existing federation** checkbox.

This makes the DCNM installed as a secondary appliance in a Federation setup. The Pre-installation Summary screen displays the Federation status and nodes in the Federation Settings area.

Step 2 Check Secure Ciphers checkbox to allow only switches with strong ciphers to be discovered by DCNM, only if the Secure Ciphers were enabled on the Primary.

Cisco DCNM uses both strong and weak ciphers when connecting to switches. If you use only strong ciphers for the network, select the checkbox. Ensure that the switches in your network support strong ciphers before you select checkbox, as DCNM will not be able to connect to switches which do not support strong ciphers.

Step 3 Modify the database URL by selecting the corresponding RDBMS option.

Note All the servers in federation refer to the same database, and therefore you must provide the DCNM username and password of the primary server. Also, you must provide the database username and password of the primary server.

The username and password of the database are same for all the server installation forming the federation. Similarly, the username and password of DCNM are same for all the server installation forming the federation.

Installing Cisco DCNM Linux Through Silent Installation

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

Perform the following steps to install DCNM Linux through silent installation.

Procedure

Step 1 Unzip, extract, and open the `installer.properties` file and update the following properties.

```
#-----------------BASIC Properties---------------------
DCNM_IP_ADDRESS=<ip_address_of_host_machine>
USER_INSTALL_DIR=/usr/local/cisco/dcm
INSTALLATION_TYPE=NEW_INSTALL
#INSTALLATION_TYPE=UPGRADE
SAN_FEDERATION=FALSE
#SAN_FEDERATION=TRUE
```

Step 2 Configure the database parameters.

If you are using PostgreSQL database, edit this block:

```
#--------------New Postgress---------------------------
PG_DB_PATH=/usr/local/cisco/dcm/db

#PG_DB_PATH=/opt/dctest/cisco/dcm/db /*non-default installation directory*/
#BACKUP_FILE=/opt/dctest/cisco/dcm/dcnm/bin/<backup-filename> /*non-default backup file
directory*/

DCNM_DB_URL=jdbc\:postgresql\://localhost\:5432/dcmdb
DCNM_DB_NAME=dcmdb
SELECTED_DATABASE=postgresql
DCNM_DB_USERNAME=dcnmuser
DCNM_DB_USER_PASSWORD=dcnmuser
#CLEAN_DATABASE=TRUE
```

If you are using the Oracle database, edit this block:

```
#------------------DATABASE Properties--------------------
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#-----------------------------------------------------
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE
ORA_DB_PATH=C:\\oraclexe\\app\\oracle\\product\\10.2.0\\server
```

Step 3 Configure the Data Path for DCNM.

```
#---------------------DATA PATH----------------
#Data path is the folder location where DCNM LAN related
#information like Config archives, templates etc. are stored.
# In DCNM LAN Cluster mode this folder has to be a shared folder.
#For linux and windows it will be different as the folder structure vaires
#-----------------------------------------------------

DATA_PATH=/usr/local/cisco/dcm/dcnm
#---------------------DATA PATH----------------
```

Step 4 Configure the user credentials for DCNM.

```
#-----------------User Configuration-----------------
#DCNM User Configuration Properties
#If you want to use special characters in DCNM_ADMIN
#credentials,Please use escape character(\) before
#the symbol [For eg. Password  "an$6x12" must be specified as "an\$6x12" ].
#-----------------------------------------------------

DECRYPT_PASSWORDS=FALSE
DCNM_ADMIN_USER=admin
DCNM_ADMIN_USER_PASSWORD=admin123

#-----------------User Configuration-----------------
```

Step 5 Enable the Secure Ciphers.

```
#----------------Secure Ciphers-------------------------------------
#DCNM uses both strong and weak ciphers when connecting to switches
#If user wants to use only strong ciphers for connection, please set
#property to TRUE. Make sure your switches support strong ciphers before
#setting the property as DCNM will not be able to connect to switches which
#support only weak ciphers.

#------------------------------------------------------------------------
SECURE_CIPHER=FALSE
#SECURE_CIPHER=TRUE
#------------------------------------------------------------------------
```

Step 6 Configure IBM Raven to install IBM Data Center Network Manager.

```
#------------------------------IBM Raven Support----------------------
#Set true if Vendor is IBM, by default false
#----------------------------------------------------------------------

IBM_INSTALL=FALSE /*Does not install IBM Data Center Network Manager*/
#----------------------------------------------------------------------
```

Step 7 Navigate to the directory where you downloaded the Cisco DCNM Linux software and run the appropriate installer by using the following command:

dcnm-release.bin -i silent -f *path_of_installer.properties_file*

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

Step 8 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM on Linux for SAN Management.

Installing DCNM on Open Virtual Appliance

This chapter contains the following sections:

Downloading the Open Virtual Appliance File

The first step to install the Open Virtual Appliance is to download the `dcnm.ova` file. Point to that `dcnm.ova` file on your computer when deploying the OVF template.

Note If you plan to use HA application functions, you must deploy the `dcnm.ova` file twice.

Procedure

Step 1 Go to the following site: http://software.cisco.com/download/ .

Step 2 In the Select a Product search box, enter **Cisco Data Center Network Manager**.

Click **Search** icon.

Step 3 Click **Data Center Network Manager** from the search results.

A list of the latest release software for Cisco DCNM available for download is displayed.

Step 4 In the Latest Releases list, choose Release 11.3(1).

Step 5 Locate the DCNM Open Virtual Appliance Installer and click the **Download** icon.

Step 6 Save the `dcnm.ova` file to your directory that is easy to find when you start to deploy the OVF template.

Deploying the Open Virtual Appliance as an OVF Template

After you download the Open Virtual Appliance file, you must deploy the OVF template from the vSphere Client application or the vCenter Server.

Note Deploy two OVAs for the HA setup.

Procedure

Step 1 Open the vCenter Server application and connect to the vCenter Server with your vCenter user credentials.

Note ESXi host must be added to the vCenter Server application.

Depending on the version of the VMware vsphere web HTML5 interface may not work properly when deploying Huge or Compute OVA, as it does not allow users to specify extra disk size. Therefore, we recommend that you use Flex interface for deploying VMs.

If you're deploying OVF template using the ESXi 6.7, the installation fails if you use Internet Explorer browser with HTML5. Ensure that you one of the following options to successfully deploy OVF template with ESXi and 6.7:

- Mozilla Firefox browser, with HTML 5 support

  Use flex interface if HTML 5 is not supported

- Mozilla Firefox browser, with flex\flash support

- Google Chrome browser, with HTML 5 support

  Use flex interface if HTML 5 is not supported

Step 2 Navigate to **Home > Inventory > Hosts and Clusters** and choose the host on which the OVF template is deployed.

Step 3 On the correct Host, right-click and select **Deploy OVF Template**.

You can also choose **Actions > Deploy OVF Template.**

Deploy OVF Template Wizard opens.

Step 4 On the Select template screen, navigate to the location where you have downloaded the OVA image.

You can choose the OVA file by one of the following methods:

- Select the **URL** radio button. Enter the path of the location of the image file.

- Select **Local File** radio button. Click **Browse**. Navigate to the directory where the image is stored. Click **OK**.

Click **Next**.

Step 5 Verify the OVA template details and click **Next**.

Step 6 On the End User License Agreement screen, read the license agreement.

Click **Accept** and click **Next**.

Step 7 On the Select name and location screen, enter the following information:

- In the Name field, enter an appropriate name for the OVF.

  Note Ensure that the VM name is unique within the Inventory.

- In the Browse tab, select **Datacenter** as the deployment location under the appropriate ESXi host.

Click **Next**.

Step 8 On the Select configuration screen, select the configuration from the drop-down list.

- Choose **Small** (Lab or POC) to configure the virtual machine with 8 vCPUs, 24GB RAM.

  Choose Small for proof-of-concept and other small-scale environments with fewer than 50 switches that are not expected to grow with time.

- Choose **Large** (Production) to configure the virtual machine with 16 vCPUs, 32GB RAM.

  We recommend that you use a Large deployment configuration when you are managing more than 50 devices to leverage better RAM, heap memory, and CPUs. For setups that could grow, choose Large.

- Choose **Compute** to configure the virtual machine with 16 vCPUs, 64GB RAM.

  You must have DCNM deployed in Compute mode to use applications in your deployment.

- Choose **Huge** to configure the virtual machine with 32 vCPUs, 128GB RAM.

  We recommend that you choose this configuration if you are deploying the SAN Insights features.

Click **Next**.

Step 9 On the Select a resource screen, select the host on which you want to deploy the OVA template.

Click **Next**.

Step 10 On the Select storage screen, based on the Datastore and Available space choose the disk format and the destination storage for the virtual machine file.

a) Select the virtual disk format from the drop-down list.

   The available disk formats are:

   Note Choose one of the thick provision types if you have enough storage capacity as required by the virtual appliance and want to set a specific allocation of space for the virtual disks.

   - **Thick Provision Lazy Zeroed**: The space that is required for the virtual disk is allocated when the virtual disk is created. The data that remains on the physical device is not erased when the virtual disk is created but is zeroed out on demand later on first write from the virtual disk.

   - **Thin Provision**: The disk space available is less than 100 GB. The initial disk consumption is 3GB and increases as the size of the database increases with the number of devices being managed.

   - **Thick Provision Eager Zeroed**: The space that is required for the virtual disk is allocated when the virtual disk is created. Unlike the Lazy Zeroed option, the data that remains on the physical device is erased when the virtual disk is created.

     Note With 500G, the DCNM installation will appear to be stuck with option Thick Provision Eager Zeroed. However, it takes longer time to complete.

b) Select the VM storage policy from the drop-down list.

   By default, no policy is selected.

c) Check the **Show datastores from Storage DRS clusters** to view the clusters datastores.

d) Select the destination storage for the virtual machine, available in the datastore.

Click **Next**.

Step 11 On the Select Networks screen, map the networks that are used in the OVF template to networks in your inventory.

- **dcnm-mgmt network**

  This network provides connectivity (SSH, SCP, HTTP, HTTPS) to the Cisco DCNM Open Virtual Appliance. Associate this network with the portgroup that corresponds to the subnet that is associated with the DCNM Management network.

- **enhanced-fabric-mgmt**

  This network provides enhanced fabric management of Nexus switches. You must associate this network with the port group that corresponds to management network of leaf and spine switches.

- **enhanced-fabric-inband**

  This network provides in-band connection to the fabric. You must associate this network with port group that corresponds to a fabric in-band connection.

  Note If you do not configure enhanced-fabric-inband network, Endpoint Locator and Telemetry features are not operational.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation.

From the Destination Network drop-down list, choose to associate the network mapping with the port group that corresponds to the subnet that is associated with the corresponding network.

If you are deploying more than one DCNM Open Virtual Appliance for HA functionality, you must meet the following criteria:

- Both OVAs must have their management access (eth0), enhanced fabric management (eth1) and inband management (eth2) interfaces in the same subnet.
- Each OVA must have their eth0-eth1 and eth2 interfaces in different subnets.
- Both OVAs must be deployed with the same administrative password. This is to ensure that both OVAs are duplicates of each other for application access. Do not use the following characters in your password:

Click **Next**.

Step 12 On the Customize template screen, enter the Management Properties information.

Enter the **IP Address** (for the outside management address for DCNM), **Subnet Mask**, and **Default Gateway**.

Note During Native HA installation and upgrade, ensure that you provide appropriate Management Properties for both Active and Standby appliances.

Ensure that add valid values for the **Management Network** properties. Properties with invalid values will not be assigned. The VM will not power on until you enter valid values.

From Release 11.3(1), for Huge and Compute configurations, you can add extra disk space on the VM. You can add from 32GB up to 1.5TB of disk space. In the **Extra Disk Size** field, enter the extra disk size that will be created on the VM.

Click **Next**.

Step 13 On the Ready to Complete screen, review the deployment settings.

Click **Back** to go to the previous screens and modify the configuration.

Click **Finish** to deploy the OVF template.

You can see the deployment status in the Recent Tasks area on the vSphere Client.

Step 14 After the installation is complete, right click on the installed VM and select **Power > Power On**.

Note Before you power on the VM, ensure that you have reserved appropriate resources for the VM, such as CPU and memory, based on the chosen deployment configuration.

You can see the status in the Recent Tasks area.

Step 15 Navigate to the Summary tab and click **Settings** icon and select **Launch Web Console**.

A message indicating that the DCNM appliance is configuring appears on the screen.

```
***************************************************************
Please point your web browser to
https://<IP-address>:<port-number>
to complete the application
***************************************************************
```

Copy and paste the URL to the browser to complete the installation, using the Web Installer.

What to do next

The DCNM installer creates a _deviceImage-0.iso in the DCNM VM folder and mounts the ISO permanently to the VM. If this ISO is removed or the CD/DVD is disconnected, the VM will not boot. The VM will enter Emergency Mode and prompt you with the message:Give root password for maintenance. If the VM is down, CD/DVD drive can be disconnected. However, after you power it up again, the VM will enter Emergency Mode and provide a prompt.

You can choose to install DCNM in Standalone mode or Native HA mode. For more information, see Installing the Cisco DCNM OVA in Standalone Mode, on page 19 or Installing the Cisco DCNM OVA in Native HA mode, on page 22.

Installing the Cisco DCNM OVA in Standalone Mode

Paste the URL displayed on the Console tab and hit Enter key. A welcome message appears.

To complete the installation of Cisco DCNM from the web installer, perform the following procedure.

Procedure

Step 1 On the Welcome to Cisco DCNM screen, click **Get Started**.

Step 2 On the Cisco DCNM Installer screen, select **Fresh Installation – Standalone** radio button.

Click **Continue**.

Step 3 On the Administration tab, enter the password that is used to connect to all the applications in the Cisco DCNM Open Virtual Appliance.

Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application may not function properly.

- It must be at least eight characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.

- Do not use any of these special characters in the DCNM password for all platforms:

  <SPACE> " & $ % ' ^ = < > ; : ` \ | / , .*

Select the **Show passwords in clear text** checkbox to view the password you have typed.

Click **Next**.

Step 4 In the Install Mode tab, from the drop-down list, choose **SAN Only** installation mode for the OVA DCNM Appliance.

Check the **Enable Clustered Mode** checkbox, if you want to deploy Cisco DCNM in Cluster mode.

The Compute nodes will be displayed on the Cisco DCNM **Web UI > Applications > Compute**. You can add the compute nodes to a Cluster, later.

Note If **Enable Clustered Mode** is selected, applications such as, Config Compliance, EPL, and NIA, and NIR won't work until you install the compute nodes.

Click **Next**.

Step 5 On the System Settings, configure the settings for the DCNM Appliance.

- In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
- In the DNS Server Address field, enter the DNS IP address.

  Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.
- In the NTP Server field, enter the IP address of the NTP server.

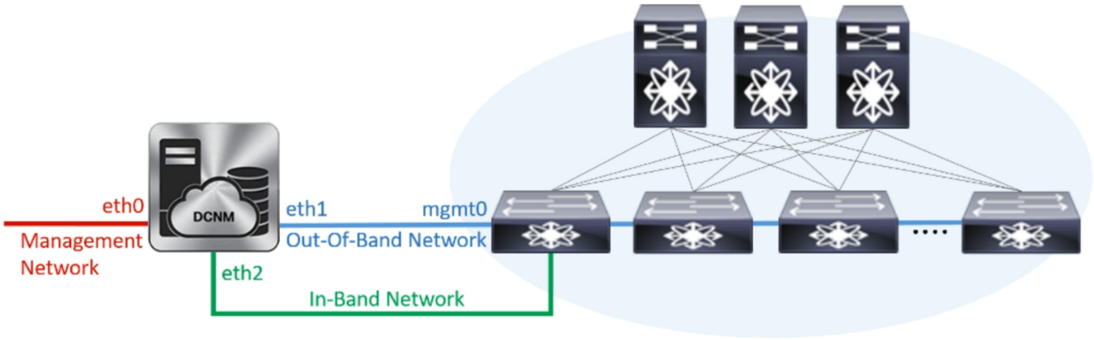
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

From Release 11.3(1), you can configure more than one DNS server and NTP server.

Click **Next**.

Step 6 On the Network Settings tab, configure the network parameters.

Figure 1: Cisco DCNM Management Network Interfaces



a) In the Management Network area, verify if the auto-populated IP Address and Default Gateway address are correct. Modify, if necessary.

Note Beginning with Cisco DCNM Release 11.2(1), you can also use an IPv6 address for the Management Network.

(Optionally) Enter a valid IPv6 address along with the prefix to configure the Management address and the Management Network Default IPv6 Gateway.

b) In the Out-of-Band Network area, enter the IP address, gateway IP Address. If DCNM is on the IPv6 network, configure the network with an IPv6 Address.

Out-of-band management provides a connection to the device management ports (Typically mgmt0).

Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

c) In the In-Band Network area, enter the IP Address and gateway IP Address for the in-band network.

The In-Band Network provides reachability to the devices via the front-panel ports.

Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation.

Click **Next**.

Step 7 On the **Applications** tab, in the IPv4 Subnet field, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

The Cluster Mode configuration area appears only if you have selected the Enable Clustered Mode checkbox in Step Step 4, on page 20.

Note In Clustered mode, the Cisco DCNM Applications run on separate DCNM Compute Nodes.

a. In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the out-of-band IPv4 network to be used in the Clustered Mode.

The address must be a smaller prefix of available IP addresses from the eth1 subnet. For example: Use 10.1.1.240/28 if the eth1 subnet was configured as 10.1.1.0/24 during installation.

This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

b. In the **Out-of-Band IPv6 Network Address Pool**, enter the address pool from the out-of-band IPv6 network to be used in the Clustered Mode. The address pool must be an IPv6 subnet.

c. In the In-Band IPv4 Network Address Pool, enter the address pool from the out-of-band IPv4 network to be used in the Clustered Mode.

The address must be a smaller prefix of available IP addresses eth2 subnet. For example: Use 11.1.1.240/28 if the eth2 subnet was configured as 11.1.1.0/24 during installation.

This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

d. In the In-Band IPv6 Network Address Pool, enter the address pool from the in-band IPv6 network to be used in the Clustered Mode. The address pool must be an IPv6 subnet.

Click **Next**.

Step 8 On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
***************************************************************
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at
https://<<IP Address>>:2443
You will be redirected there in 60 seconds.
Thank you
***************************************************************
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

Note If you try to access the DCNM Web UI using the Management IP address while the installation is still in progress, an error message appears on the console.

```
***************************************
*Preparing Appliance*

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

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Click the **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

If you have configured inband management (eth2) IP addresses for device management, login to standalone server and configure the inband network reachability from eth2 of the server to the switches by using the following commands:

```
dcnm# appmgr setup inband-route --subnet switches-fabric-links-IP-subnet/mask
dcnm# appmgr setup inband-route --subnet switch-loopback-IP-subnet>/mask
```

For example: If you have four switches with all fabric links connected through 10.0.0.x/30 subnet, and if all switches are configured with the loopback interface for inband reachability in subnet 40.1.1.0/24, use the following commands:

```
dcnm# appmgr setup inband-route --subnet 10.0.0.0/24
dcnm# appmgr setup inband-route --subnet 40.1.1.0/24
```

Installing the Cisco DCNM OVA in Native HA mode

The native HA is supported on DCNM appliances with ISO or OVA installation only.

By default, an embedded PostgreSQL database engine with the Cisco DCNM. The native HA feature allows two Cisco DCNM appliances to run as active and standby applications, with their embedded databases synchronized in real time. Therefore, when the active DCNM is not functioning, the standby DCNM takes over with the same database data and resume the operation.

Perform the following task to set up Native HA for DCNM.

Procedure

Step 1 Deploy two DCNM Virtual Appliances (either OVA or ISO).

For example, let us indicate them as **dcnm1** and **dcnm2**.

Step 2 Configure **dcnm1** as the Primary node. Paste the URL displayed on the Console tab of **dcnm1** and press **Enter** key.

A welcome message appears.

a) On the Welcome to Cisco DCNM screen, click **Get Started**.

b) On the Cisco DCNM Installer screen, select **Fresh Installation - HA Primary** radio button, to install **dcnm1** as Primary node.

Click **Continue**.

c) On the Administration tab, enter the password that is used to connect to all the applications in the Cisco DCNM Open Virtual Appliance.

Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application may not function properly.

- It must be at least eight characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password for Linux, Windows, OVA, and ISO platforms:

  <SPACE> " & $ % ' ^ = < > ; : ` \ | / , .*

Select the **Show passwords in clear text** checkbox to view the password you have typed.

Click **Next**.

d) In the Install Mode tab, from the drop-down list, choose installation mode for the DCNM Appliance.

Check the **Enable Clustered Mode** checkbox, if you want to deploy Cisco DCNM in Cluster mode.

The Compute nodes will be displayed on the Cisco DCNM **Web UI > Applications > Compute**. You can add the compute nodes to a Cluster, later.

Note If **Enable Clustered Mode** is selected, applications such as, Config Compliance, EPL, and NIA, and NIR won't work until you install the compute nodes.

Click **Next**.

e) On the System Settings, configure the settings for the DCNM Appliance.

- In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
- In the DNS Server Address field, enter the DNS IP address.

Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.

- In the NTP Server field, enter the IP address of the NTP server.

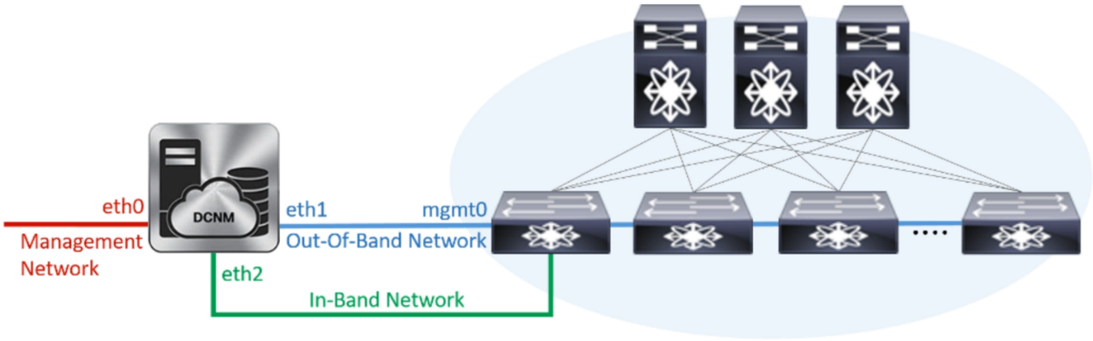
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

From Release 11.3(1), you can configure more than one DNS server and NTP server.

Click **Next**.

f) On the Network Settings tab, configure the network parameters.

Figure 2: Cisco DCNM Management Network Interfaces



- In the Management Network area, verify is the auto-populated IP Address and Default gateway address are correct. Modify, if necessary.

  Note Beginning with Cisco DCNM Release 11.2(1), you can also use an IPv6 address for the Management Network.

  (Optionally) Enter a valid IPv6 address along with the prefix to configure the Management address and the Management Network Default IPv6 Gateway.

- In the Out-of-Band Network area, enter the IP address, gateway IP Address. If DCNM is on the IPv6 network, configure the network with an IPv6 Address.

  Out-of-band management provides a connection to the device management ports (Typically mgmt0).

  Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

- In the In-Band Network area, enter the VIP Address and gateway IP Address for the in-band network. The In-Band Network provides reachability to the devices via the front-panel ports.

  Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

- In the Internal Application Services Network area, enter the IP subnet to access the applications that run internally to DCNM.

  All the applications use the IP Address from this subnet.

  Note Ensure that you configure the same IP subnet on both the Primary HA and the Secondary HA node.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation.

Click **Next**.

g) On the HA Settings tab, a confirmation message appears.

```
You are installing the primary DCNM HA node.
Please note that HA setup information will need to
be provided when the secondary DCNM HA node is
installed.
```

Click **Next**.

h) On the **Applications** tab, in the IPv4 Subnet field, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

The Cluster Mode configuration area appears only if you have selected the Enable Clustered Mode checkbox in Step 2.d, on page 23.

Note In Clustered mode, the Cisco DCNM Applications run on separate DCNM Compute Nodes.

1. In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the out-of-band IPv4 network to be used in the Clustered Mode.

   The address must be a smaller prefix of available IP addresses from the eth1 subnet. For example: Use 10.1.1.240/28 if the eth1 subnet was configured as 10.1.1.0/24 during installation.

   This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

2. In the **Out-of-Band IPv6 Network Address Pool**, enter the address pool from the out-of-band IPv6 network to be used in the Clustered Mode. The address pool must be an IPv6 subnet.

3. In the In-Band IPv4 Network Address Pool, enter the address pool from the out-of-band IPv4 network to be used in the Clustered Mode.

   The address must be a smaller prefix of available IP addresses eth2 subnet. For example: Use 11.1.1.240/28 if the eth2 subnet was configured as 11.1.1.0/24 during installation.

   This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

4. In the In-Band IPv6 Network Address Pool, enter the address pool from the in-band IPv6 network to be used in the Clustered Mode. The address pool must be an IPv6 subnet.

Click **Next**.

i) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A warning message appears stating that the setup is not complete until you install the Secondary node.

```
WARNING: DCNM HA SETUP IS NOT COMPLETE!
Your Cisco Data Center Network Manager software has been installed on
this HA primary node.
However, the system will be ready to be used only after installation
of the secondary node has been completed.
Thank you.
```

Step 3 Configure **dcnm2** as the Secondary node. Paste the URL displayed on the Console tab of **dcnm2** and hit Enter.

A welcome message appears.

a) On the Welcome to Cisco DCNM screen, click **Get Started**.

b) On the Cisco DCNM Installer screen, select **Fresh Installation - HA Secondary** radio button, to install **dcnm2** as Secondary node.

Click **Continue**.

c) On the Administration tab, enter the password that is used to connect to all the applications in the Cisco DCNM Open Virtual Appliance.

Note The password for the secondary node must be the same as the Administrative password for primary, as entered in Step 2.c, on page 23.

Click **Next**.

d) In the Install Mode tab, from the drop-down list, choose the same installation mode that you selected for the Primary node.

Note The HA installation fails if you do not choose the same installation mode as Primary node.

Click **Next**.

e) On the System Settings, configure the settings for the DCNM Appliance.

- In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
- In the DNS Server Address field, enter the DNS IP address.

  Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.
- In the NTP Server field, enter the IP address of the NTP server.

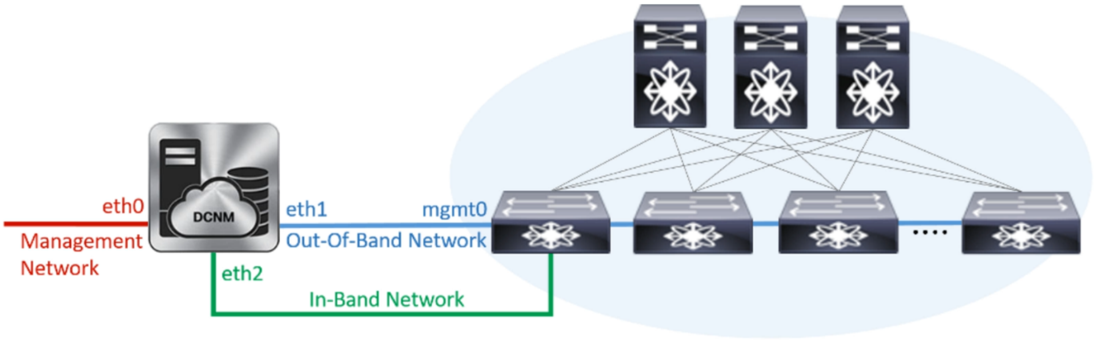
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

From Release 11.3(1), you can configure more than one DNS server and NTP server.

Click **Next**.

f) On the Network Settings tab, configure the network parameters.

Figure 3: Cisco DCNM Management Network Interfaces



- In the Management Network area, verify is the auto-populated IP Address and Default gateway address are correct. Modify, if necessary.

  Note Ensure that the IP Address belongs to the same Management Network as configured on the Primary node for HA setup to complete successfully.

  Note Beginning with Cisco DCNM Release 11.2(1), you can also use an IPv6 address for the Management Network.

  (Optionally) Enter a valid IPv6 address along with the prefix to configure the Management address and the Management Network Default IPv6 Gateway.

- In the Out-of-Band Network area, enter the IP address, gateway IP Address. If DCNM is on the IPv6 network, configure the network with an IPv6 Address.

  Out-of-band management provides a connection to the device management ports (Typically mgmt0).

  Note Ensure that the IP Address, IP address gateway, and the IPv6 address belong to the same Out-of-Band Network as configured on the Primary node for HA setup to complete successfully.

  Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

  You can also configure an IPv6 address for out-of-band management network.

- In the In-Band Network area, enter the IP Address and gateway IP Address for the in-band network. The In-Band Network provides reachability to the devices via the front-panel ports.

  Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

  However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation.

- In the Internal Application Services Network area, enter the IP subnet to access the applications that run internally to DCNM.

  All the applications use the IP Address from this subnet.

Note Ensure that you configure the same IP subnet on both the Primary HA and the Secondary HA node.

Click **Next**.

g) On the **Applications** tab, in the IPv4 Subnet field, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

Note Ensure that you configure the same IP subnet on both the Primary HA and the Secondary HA node.

Click **Next**.

h) On the HA Settings tab, configure the system settings..

- In the Management IP Address of primary DCNM node field, enter the appropriate IP Address to access the DCNM UI.
- In the VIP Fully qualified Host Name field, enter hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
- Enter the Management Network VIP address, VIPv6 address, and OOB Network VIP address appropriately.

  Note If you have configured the Management network using IPv6 address, ensure that you configure the Management Network VIPv6 Address.
- Enter OOB Network VIPv6 Address to configure IPv6 address for VIP.
- In the In-Band Network area, enter the VIP Address for the in-band network.

  This is the VIP address for the In-Band network. This field is mandatory if you have provided an IP address for In-Band network in the Network Settings tab.
- Enter the HA ping IP address if necessary.

  HA_PING_ADDRESS, must be different from the DCNM Active and Standby addresses.

  You must configure the HA ping IP Address to avoid the Split Brain scenario. This address must belong to Enhanced Fabric management network.

Click **Next**.

i) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM OVA Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
***************************************************************
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at
https://<<IP Address>>:2443
You will be redirected there in 60 seconds.
```

```
Thank you
******************************************************************
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Click the **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

If you have configured inband management (eth2) IP addresses for device management, login to standalone server and configure the inband network reachability from eth2 of the server to the switches by using the following commands:

```
dcnm# appmgr setup inband-route --subnet switches-fabric-links-IP-subnet/mask
dcnm# appmgr setup inband-route --subnet switch-loopback-IP-subnet>/mask
```

For example: If you have four switches with all fabric links connected through 10.0.0.x/30 subnet, and if all switches are configured with the loopback interface for inband reachability in subnet 40.1.1.0/24, use the following commands:

```
dcnm# appmgr setup inband-route --subnet 10.0.0.0/24
dcnm# appmgr setup inband-route --subnet 40.1.1.0/24
```

Installing DCNM on ISO Virtual Appliance

This chapter contains the following sections:

Downloading the ISO Virtual Appliance File

The first step to installing the ISO Virtual Appliance is to download the `dcnm.iso` file. You must point to that dcnm.iso file on your computer when preparing the server for installing DCNM.

Note If you plan to use HA application functions, you must deploy the `dcnm.iso` file twice.

Procedure

Step 1 Go to the following site: http://software.cisco.com/download/ .

Step 2 In the Select a Product search box, enter Cisco Data Center Network Manager.

Click on Search icon.

Step 3 Click on **Data Center Network Manager** from the search results.

A list of the latest release software for Cisco DCNM available for download is displayed.

Step 4 In the Latest Releases list, choose Release 11.3(1).

Step 5 Locate the DCNM ISO Virtual Appliance Installer and click the **Download** icon.

Step 6 Locate the DCNM VM templates at DCNM Virtual Appliance definition files for VMWare (.ovf) and KVM (domain XMLs) environment and click **Download**.

Step 7 Save the `dcnm.iso` file to your directory that will be easy to find when you being the installation.

What to do next

You can choose to install DCNM On KVM or Baremetal servers. Refer to Installing the DCNM ISO Virtual Appliance on KVM, on page 37 or Installing the DCNM ISO Virtual Appliance on UCS (Bare Metal), on page 30 for more information.

Installing the DCNM ISO Virtual Appliance on UCS (Bare Metal)

From Release 11.3(1), you can install Cisco DCNM ISO using an additional mode where the physical interfaces are bound together for a port channel or ethernet channel configured as a trunk with the management traffic, out-of-band traffic, and in-band traffic separated in different VLANs.

Ensure that the switch is configured correctly for bundled interface mode. The following shows a sample switch configuration for bundled interface mode:

```
vlan 100
vlan 101
vlan 102
interface port-channel1
  switchport
  switchport mode trunk

interface Ethernet101/1/1
  switchport mode trunk
  channel-group 1
  no shutdown

interface Ethernet101/1/2
  switchport mode trunk
  channel-group 1
  no shutdown

interface Ethernet101/1/3
  switchport mode trunk
  channel-group 1
  no shutdown

interface Ethernet101/1/4
  switchport mode trunk
  channel-group 1
  no shutdown
```

Perform the following tasks to install the DCNM ISO virtual appliance on UCS.

Procedure

Step 1 Launch Cisco Integrated Management Controller (CIMC).

Step 2 Click the **Launch KVM** button.

You can either launch Java-based KVM or HTML-based KVM.

Step 3 Click the URL displayed on the window to continue loading the KVM client application.

Step 4 On the Menu bar, click **Virtual Media > Activate Virtual Devices**.

Step 5 Click **Virtual Media** and choose one of the following mediums to browse and upload DCNM ISO images from the following:

- Map CD/DVD
- Map Removable Disk
- Map Floppy Disk

Navigate to the location where the ISO image is located and load the ISO image.

Step 6 Select **Power > Reset System (warm boot)** and Ok to continue and restart the UCS box.

Step 7 Press **F6** interrupt the reboot process when the server starts to select a boot device. The boot selection menu appears.

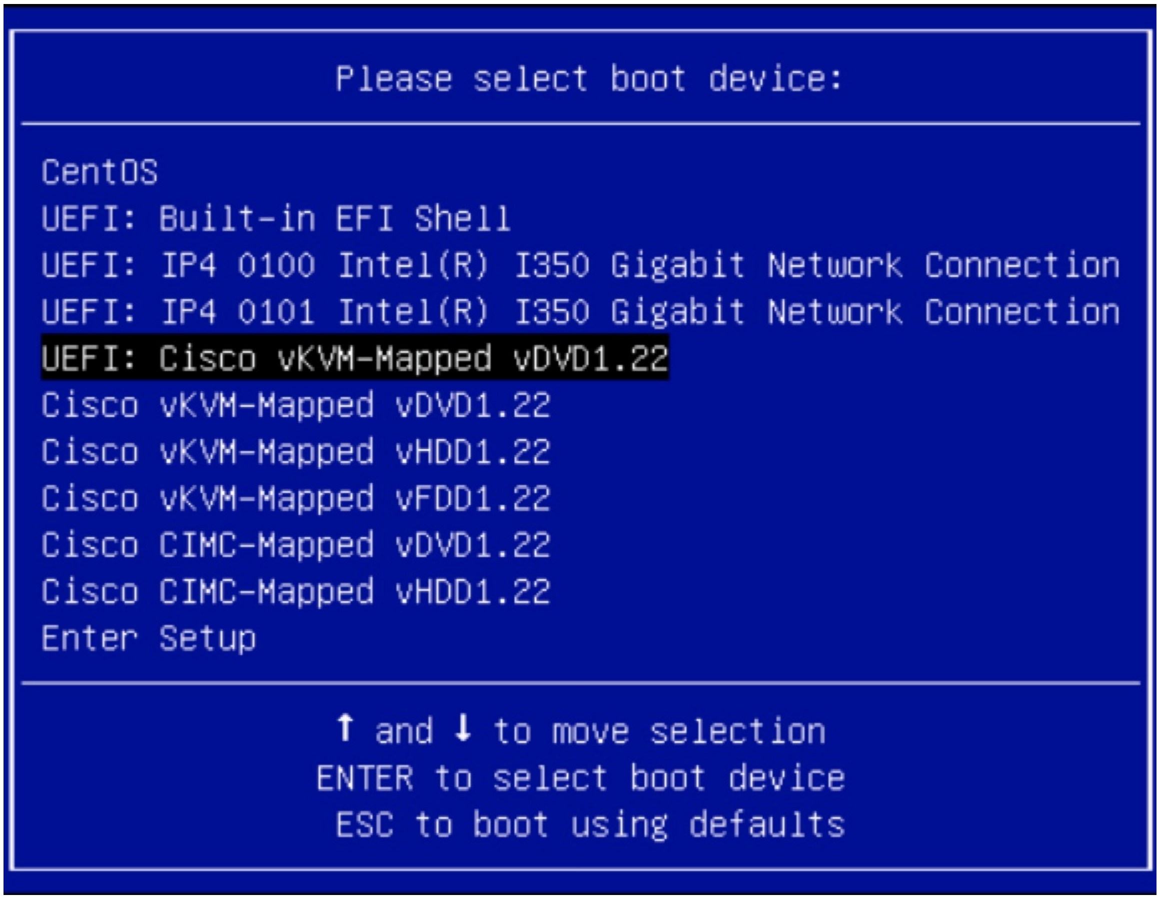
For more information about using the UCS KVM Console window, see the Cisco UCS Server Configuration Utility, Release 3.1 User Guide at the following URL:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/ucsscu/user/guide/31/UCS_SCU/booting.html#wp1078073

Step 8 Use the arrow keys to select Cisco Virtual CD/DVD and press **Enter**. The server boots with the DCNM ISO image from the mapped location.

Note The following image highlights UEFI installation. However, you can also choose **Cisco vKVM-Mapped vDVD1.22** for BIOS installation. ISO can be booted in both modes, BIOS, and UEFI.

UEFI is mandatory for a system with minimum of 2TB disks.

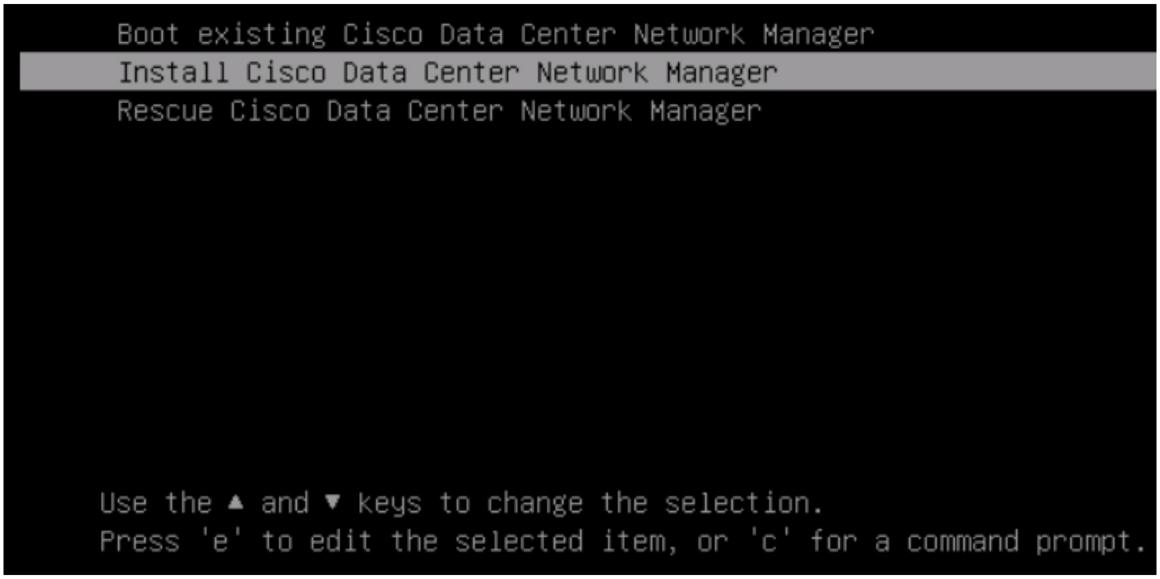


```
Please select boot device:

CentOS
UEFI: Built-in EFI Shell
UEFI: IP4 0100 Intel(R) I350 Gigabit Network Connection
UEFI: IP4 0101 Intel(R) I350 Gigabit Network Connection
UEFI: Cisco vKVM-Mapped vDVD1.22
Cisco vKVM-Mapped vDVD1.22
Cisco vKVM-Mapped vHDD1.22
Cisco vKVM-Mapped vFDD1.22
Cisco CIMC-Mapped vDVD1.22
Cisco CIMC-Mapped vHDD1.22
Enter Setup

↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults
```

For Cisco UCS with the disk size of 2TB or higher and with 4K sector size drivers, the UEFI boot option is required. For more information, see UEFI Boot Mode.

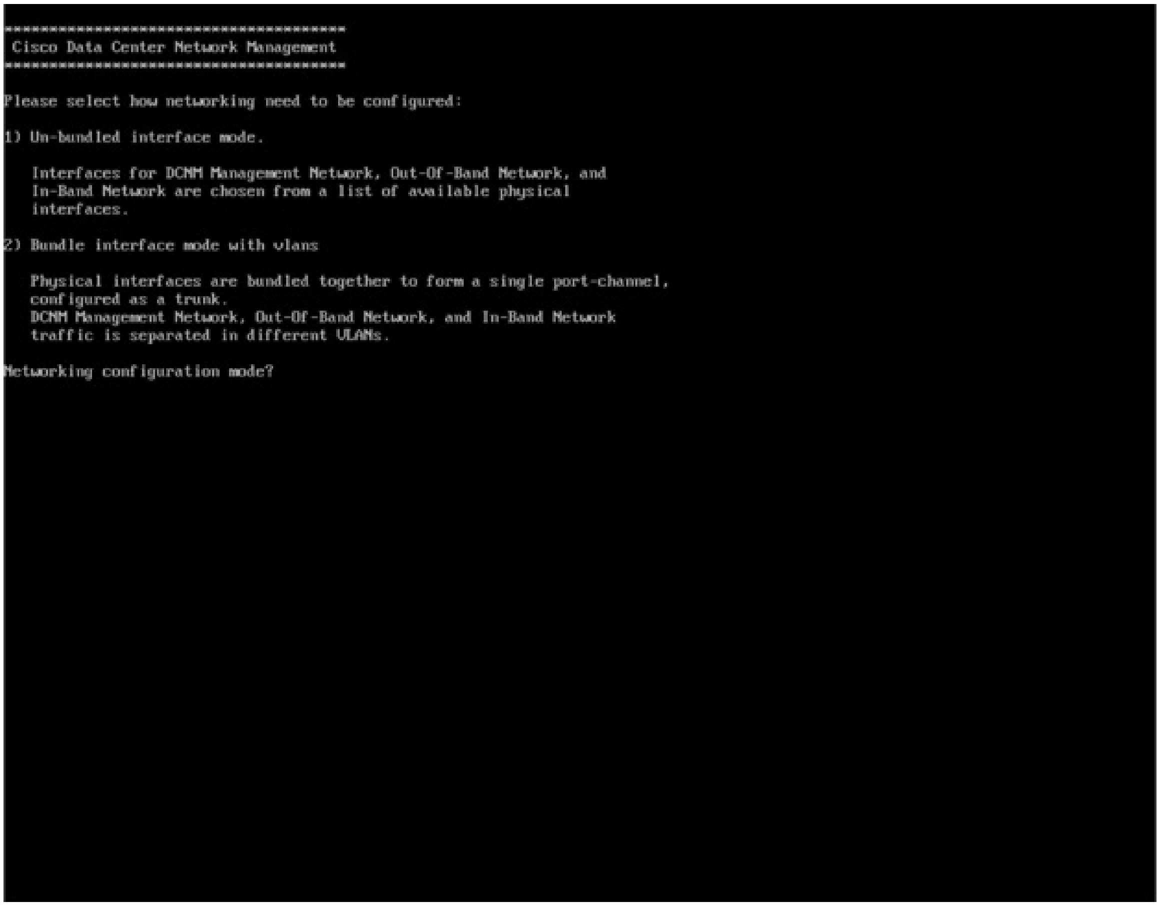
Step 9 Select **Install Cisco Data Center Network Manager** using the up or down arrow keys. Press **Enter**.

The option shown in the following image appears when the ISO image is booted with UEFI.



```
      Boot existing Cisco Data Center Network Manager
      Install Cisco Data Center Network Manager
      Rescue Cisco Data Center Network Manager






     Use the ▲ and ▼ keys to change the selection.
     Press 'e' to edit the selected item, or 'c' for a command prompt.
```

Step 10 On the Cisco Management Network Management screen, select the mode to configure the network.



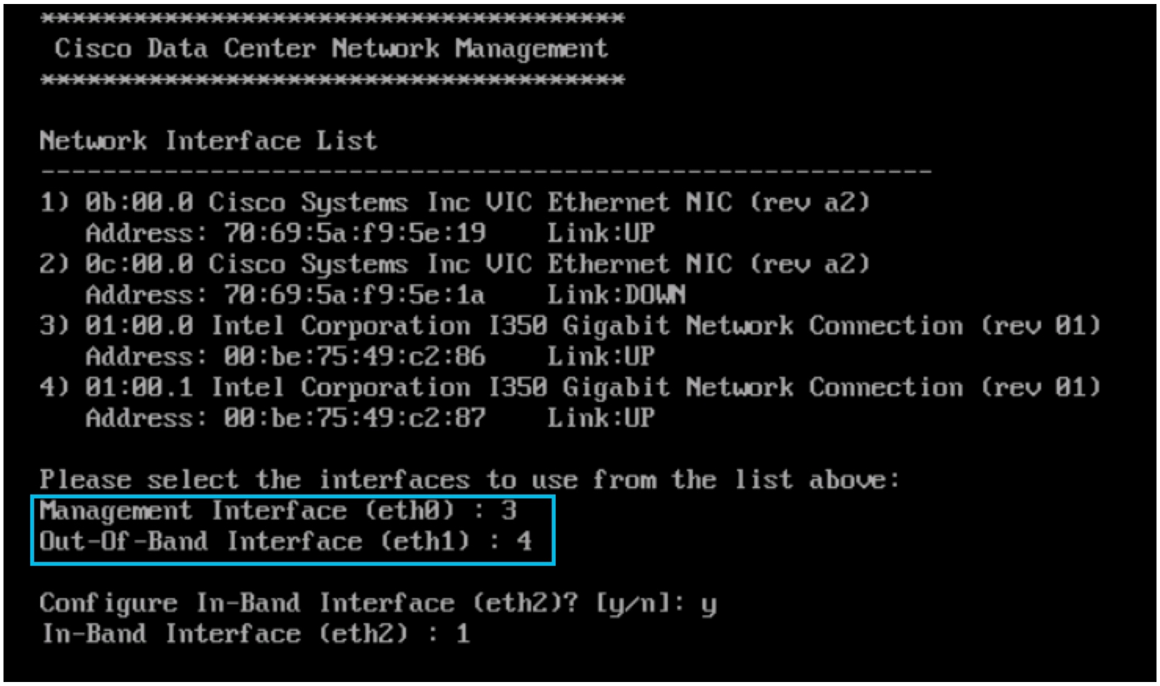
```
**************************************
 Cisco Data Center Network Management
**************************************

Please select how networking need to be configured:

1) Un-bundled interface mode.

   Interfaces for DCNM Management Network, Out-Of-Band Network, and
   In-Band Network are chosen from a list of available physical
   interfaces.

2) Bundle interface mode with vlans

   Physical interfaces are bundled together to form a single port-channel,
   configured as a trunk.
   DCNM Management Network, Out-Of-Band Network, and In-Band Network
   traffic is separated in different VLANs.

Networking configuration mode?
```

Enter 1 to configure the Cisco DCNM network interfaces from the available physical interfaces.

Enter 2 to configure the Cisco DCNM network interfaces from the available physical interfaces that are bundled together to form a single port-channel, configured as a trunk.

Step 11 If you entered 1, to install Cisco DCNM ISO in un-bundled interface mode, select the interface for the networks. The list of available interfaces is displayed on the screen.

Choose the Management Interface (eth0) and Out-of-Band interface (eth1) from the Network Interface List. You can also configure the in-band interface (eth2) if necessary.



```
 ****************************************
  Cisco Data Center Network Management
 ****************************************

 Network Interface List
 ------------------------------------------------------------
 1) 0b:00.0 Cisco Systems Inc VIC Ethernet NIC (rev a2)
    Address: 70:69:5a:f9:5e:19    Link:UP
 2) 0c:00.0 Cisco Systems Inc VIC Ethernet NIC (rev a2)
    Address: 70:69:5a:f9:5e:1a    Link:DOWN
 3) 01:00.0 Intel Corporation I350 Gigabit Network Connection (rev 01)
    Address: 00:be:75:49:c2:86    Link:UP
 4) 01:00.1 Intel Corporation I350 Gigabit Network Connection (rev 01)
    Address: 00:be:75:49:c2:87    Link:UP

 Please select the interfaces to use from the list above:
 Management Interface (eth0) : 3
 Out-Of-Band Interface (eth1) : 4

 Configure In-Band Interface (eth2)? [y/n]: y
 In-Band Interface (eth2) : 1
```

Note If you do not configure In-Band interface, Endpoint Locator and Telemetry features are not operational.

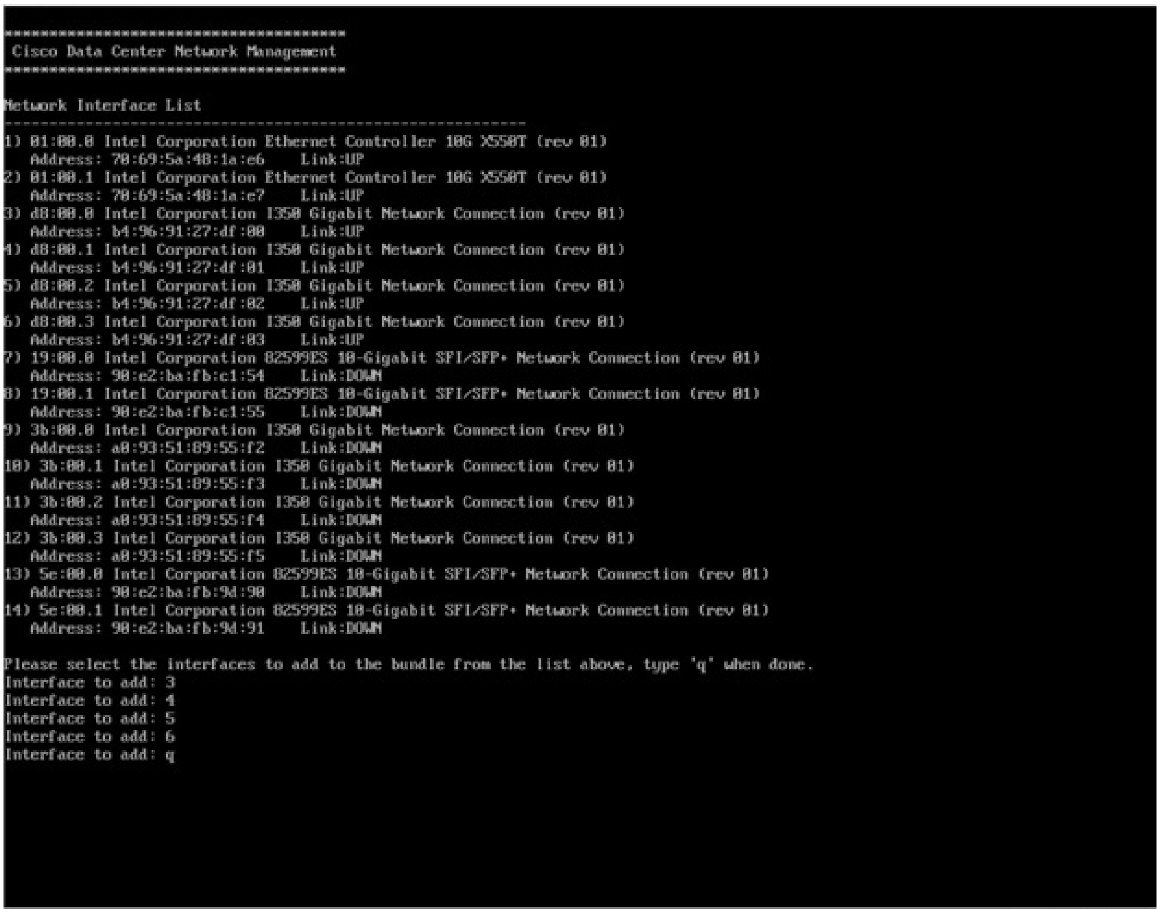
However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation.

Step 12 If you entered 2, to install Cisco DCNM ISO in bundled interface mode, perform the following tasks:

a) Select interface from the list to form a bundle.

Note A minimum of one physical interface must be a part of the bundle.

Enter **q** after you enter all the interface that must be added to the bundle.

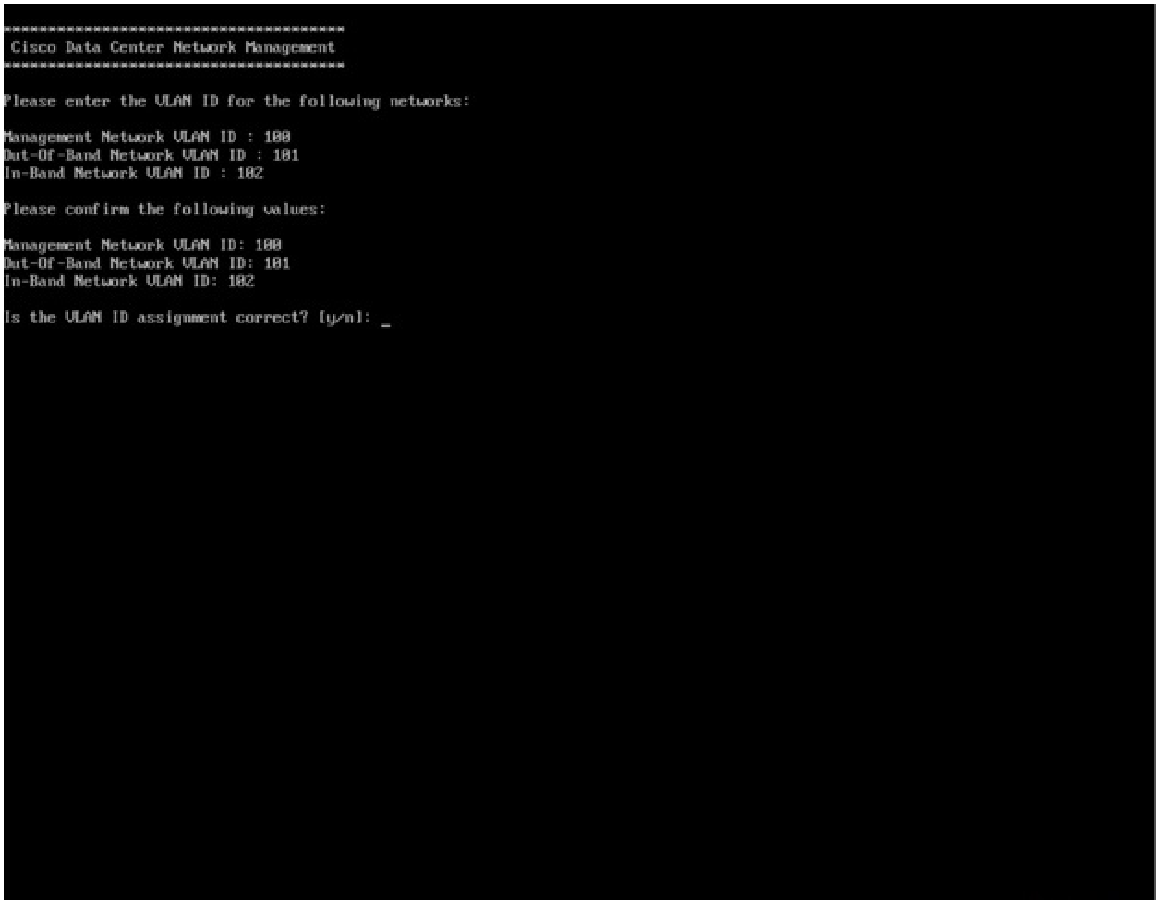


```
*************************************
 Cisco Data Center Network Management
*************************************

Network Interface List
----------------------------------------------------------
1) 01:00.0 Intel Corporation Ethernet Controller 10G X550T (rev 01)
   Address: 70:69:5a:48:1a:e6    Link:UP
2) 01:00.1 Intel Corporation Ethernet Controller 10G X550T (rev 01)
   Address: 70:69:5a:48:1a:e7    Link:UP
3) d8:00.0 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: b4:96:91:27:df:00    Link:UP
4) d8:00.1 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: b4:96:91:27:df:01    Link:UP
5) d8:00.2 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: b4:96:91:27:df:02    Link:UP
6) d8:00.3 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: b4:96:91:27:df:03    Link:UP
7) 19:00.0 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
   Address: 90:e2:ba:fb:c1:54    Link:DOWN
8) 19:00.1 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
   Address: 90:e2:ba:fb:c1:55    Link:DOWN
9) 3b:00.0 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: a0:93:51:89:55:f2    Link:DOWN
10) 3b:00.1 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: a0:93:51:89:55:f3    Link:DOWN
11) 3b:00.2 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: a0:93:51:89:55:f4    Link:DOWN
12) 3b:00.3 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: a0:93:51:89:55:f5    Link:DOWN
13) 5e:00.0 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
   Address: 90:e2:ba:fb:9d:90    Link:DOWN
14) 5e:00.1 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
   Address: 90:e2:ba:fb:9d:91    Link:DOWN

Please select the interfaces to add to the bundle from the list above, type 'q' when done.
Interface to add: 3
Interface to add: 4
Interface to add: 5
Interface to add: 6
Interface to add: q
```

b) Enter the VLAN IDs to be used for Management Network, Out-Of-Band Network and In-band Network Select interface from the list to form a bundle.

Verify and confirm if the correct VLAN IDs are assigned.

Note The VLAN IDs for Management Network and Out-Of-Band Network can be the same when Management Network and Out-Of-Band Network use the same subnet (that is, when eth0/eth1 are in the same subnet)



```
****************************************
 Cisco Data Center Network Management
****************************************

Please enter the VLAN ID for the following networks:

Management Network VLAN ID : 100
Out-Of-Band Network VLAN ID : 101
In-Band Network VLAN ID : 102

Please confirm the following values:

Management Network VLAN ID: 100
Out-Of-Band Network VLAN ID: 101
In-Band Network VLAN ID: 102

Is the VLAN ID assignment correct? [y/n]: _
```

Step 13 Review the selected interfaces. Press **y** to confirm and continue with the installation.

Step 14 Configure the Management Network for Cisco DCNM. Enter the IP address, Subnet Mask, and Gateway. Press **y** to continue with the installation.

After the installation is complete, the system reboots and a message indicating that the DCNM appliance is configuring appears on the screen.

```
***************************************************************
Please point your web browser to
http://<IP-address>:<port-number>
to complete the application
***************************************************************
```

Copy and paste the URL to the browser to complete the installation using the Web Installer.

What to do next

You can choose to install DCNM in Standalone mode or Native HA mode. Refer to Installing Cisco DCNM ISO in Standalone Mode, on page 38 or Installing the Cisco DCNM ISO in Native HA mode, on page 42 for more information.

Installing the DCNM ISO Virtual Appliance on KVM

Perform the following tasks to install the ISO virtual appliance on KVM.

Procedure

Step 1 Unzip and extract **dcnm-va-ovf-kvm-files.11.3.1.zip** and locate the **dcnm-kvm-vm.xml** file.

Step 2 Upload this file on the RHEL server that is running KVM to the same location as the ISO.

Step 3 Connect to the RHEL server running KVM via SCP File transfer terminal.

Step 4 Upload the **dcnm-va.11.3.1.iso** and **dcnm-kvm-vm.xml** to the RHEL server.

Step 5 Close the file transfer session.

Step 6 Connect to the RHEL server running KVM via SSH terminal.

Step 7 Navigate to the location where both the ISO and domain XMLs is downloaded.

Step 8 Create the VM (or Domains, as they are known in the KVM terminology) using the **virsh** command.

need info on dcnm-kvm-vm-huge.xml

```
sudo virsh define [{dcnm-kvm-vm-huge.xml|dcnm-kvm-vm-compute.xml|
dcnm-kvm-vm-large.xml|dcnm-kvm-vm-small.xml}]
```

Step 9 Enable a VNC server and open the required firewall ports.

Step 10 Close the SSH session.

Step 11 Connect to the RHEL server running KVM via a VNC terminal.

Step 12 Navigate to **Applications > System Tools > Virtual Machine Manager (VMM)**.

A VM is created in the Virtual Machine Manager.

Step 13 From Virtual Machine Manager, edit the VM by selecting the VM in the listing. Click **Edit > Virtual Machine Details > Show virtual hardware details**.

Step 14 In the Virtual Hardware Details, navigate to **Add Hardware > Storage**.

Step 15 Create a hard disk with Device type withe the following specifications:

- device type: IDE disk
- cache-mode: default
- storage format: raw

We recommend that you use storage size of 500GB.

Step 16 Select IDE CDROM on the edit window of the Virtual Machine and click **Connect**.

Step 17 Navigate to dcnm-va.iso and click **OK**.

Step 18 Select both the NICs and assign appropriate networks that are created.

Step 19 Power on the Virtual Machine.

Note Before you power on the VM, ensure that you have reserved appropriate resources for the VM, such as CPU and memory, based on the chosen deployment configuration.

The operating system is installed.

Step 20 On the Cisco Management Network Management screen, select the interface for the networks. The list of available interfaces is displayed on the screen.

Choose the Management Interface (eth0) and Out-of-Band interface (eth1) from the Network Interface List. You can also configure in-band interface (eth2) if necessary.

Note If you do not configure in-band interface (eth2), Endpoint Locator and Telemetry features are not operational.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation.

Step 21 Press **y** to confirm and continue with the installation.

Step 22 Configure the Management Network. Enter the IP address, Subnet Mask, and Gateway. Press **y** to continue with the installation.

After the installation is complete, the system reboots and a message indicating that the DCNM appliance is configuring appears on the screen.

```
***************************************************************
Please point your web browser to
http://<IP-address>:<port-number>
to complete the application
***************************************************************
```

Copy and paste the URL to the browser to complete the installation using the Web Installer.

What to do next

You can choose to install DCNM in Standalone mode or Native HA mode. Refer to Installing Cisco DCNM ISO in Standalone Mode, on page 38 or Installing the Cisco DCNM ISO in Native HA mode, on page 42 for more information.

Installing Cisco DCNM ISO in Standalone Mode

Paste the URL displayed on the Console tab and hit Enter key. A welcome message appears.

To complete the installation of Cisco DCNM from the web installer, perform the following procedure.

Procedure

Step 1 On the Welcome to Cisco DCNM screen, click **Get Started**.

Step 2 On the Cisco DCNM Installer screen, select **Fresh Installation – Standalone** radio button.

Click **Continue**.

Step 3 On the Administration tab, enter the password that is used to connect to all the applications in the Cisco DCNM Open Virtual Appliance.

Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application may not function properly.

- It must be at least eight characters long and contain at least one alphabet and one numeral.

- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password for all platforms:

  <SPACE> " & $ % ' ^ = < > ; : ` \ | / , .*

Select the **Show passwords in clear text** checkbox to view the password you have typed.

Click **Next**.

Step 4 In the Install Mode tab, from the drop-down list, choose **SAN Only** installation mode for the OVA DCNM Appliance.

Check the **Enable Clustered Mode** checkbox, if you want to deploy Cisco DCNM in Cluster mode.

The Compute nodes will be displayed on the Cisco DCNM **Web UI > Applications > Compute**. You can add the compute nodes to a Cluster, later.

Note If **Enable Clustered Mode** is selected, applications such as, Config Compliance, EPL, and NIA, and NIR won't work until you install the compute nodes.

Click **Next**.

Step 5 On the System Settings, configure the settings for the DCNM Appliance.

- In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
- In the DNS Server Address field, enter the DNS IP address.

  Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.
- In the NTP Server field, enter the IP address of the NTP server.

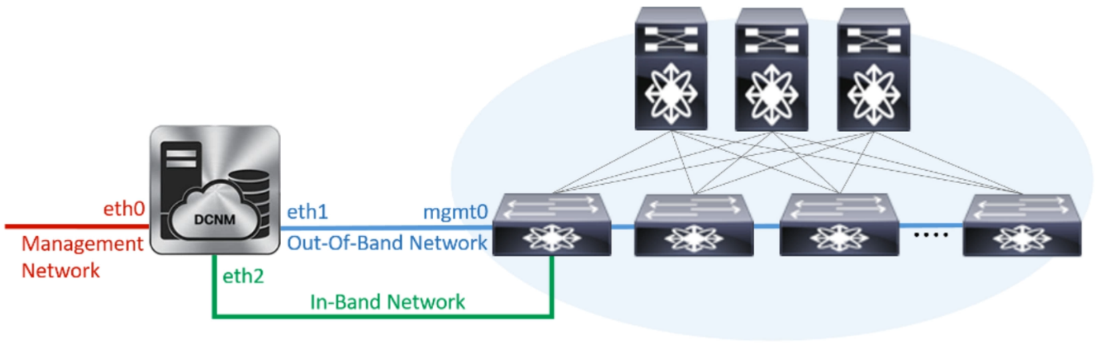
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

From Release 11.3(1), you can configure more than one DNS server and NTP server.

Click **Next**.

Step 6 On the Network Settings tab, configure the network parameters.

Figure 4: Cisco DCNM Management Network Interfaces



a) In the Management Network area, verify if the auto-populated IP Address and Default Gateway address are correct. Modify, if necessary.

Note Beginning with Cisco DCNM Release 11.2(1), you can also use an IPv6 address for the Management Network.

(Optionally) Enter a valid IPv6 address along with the prefix to configure the Management address and the Management Network Default IPv6 Gateway.

b) In the Out-of-Band Network area, enter the IP address, gateway IP Address. If DCNM is on the IPv6 network, configure the network with an IPv6 Address.

Out-of-band management provides a connection to the device management ports (Typically mgmt0).

Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

c) In the In-Band Network area, enter the IP Address and gateway IP Address for the in-band network.

The In-Band Network provides reachability to the devices via the front-panel ports.

Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation.

Click **Next**.

Step 7 On the **Applications** tab, in the IPv4 Subnet field, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

The Cluster Mode configuration area appears only if you have selected the Enable Clustered Mode checkbox in Step Step 4, on page 39.

Note In Clustered mode, the Cisco DCNM Applications run on separate DCNM Compute Nodes.

a. In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the out-of-band IPv4 network to be used in the Clustered Mode.

   The address must be a smaller prefix of available IP addresses from the eth1 subnet. For example: Use 10.1.1.240/28 if the eth1 subnet was configured as 10.1.1.0/24 during installation.

   This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

b. In the **Out-of-Band IPv6 Network Address Pool**, enter the address pool from the out-of-band IPv6 network to be used in the Clustered Mode. The address pool must be an IPv6 subnet.

c. In the In-Band IPv4 Network Address Pool, enter the address pool from the out-of-band IPv4 network to be used in the Clustered Mode.

   The address must be a smaller prefix of available IP addresses eth2 subnet. For example: Use 11.1.1.240/28 if the eth2 subnet was configured as 11.1.1.0/24 during installation.

   This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

d. In the In-Band IPv6 Network Address Pool, enter the address pool from the in-band IPv6 network to be used in the Clustered Mode. The address pool must be an IPv6 subnet.

Click **Next**.

Step 8 On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
***************************************************************
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at
https://<<IP Address>>:2443
You will be redirected there in 60 seconds.
Thank you
***************************************************************
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

Note If you try to access the DCNM Web UI using the Management IP address while the installation is still in progress, an error message appears on the console.

```
***************************************
*Preparing Appliance*

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

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Click the **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

If you have configured inband management (eth2) IP addresses for device management, login to standalone server and configure the inband network reachability from eth2 of the server to the switches by using the following commands:

```
dcnm# appmgr setup inband-route --subnet switches-fabric-links-IP-subnet/mask
dcnm# appmgr setup inband-route --subnet switch-loopback-IP-subnet>/mask
```

For example: If you have four switches with all fabric links connected through 10.0.0.x/30 subnet, and if all switches are configured with the loopback interface for inband reachability in subnet 40.1.1.0/24, use the following commands:

```
dcnm# appmgr setup inband-route --subnet 10.0.0.0/24
dcnm# appmgr setup inband-route --subnet 40.1.1.0/24
```

Installing the Cisco DCNM ISO in Native HA mode

The native HA is supported on DCNM appliances with ISO or OVA installation only.

By default, an embedded PostgreSQL database engine with the Cisco DCNM. The native HA feature allows two Cisco DCNM appliances to run as active and standby applications, with their embedded databases synchronized in real time. Therefore, when the active DCNM is not functioning, the standby DCNM takes over with the same database data and resume the operation.

Perform the following task to set up Native HA for DCNM.

Procedure

Step 1 Deploy two DCNM Virtual Appliances (either OVA or ISO).

For example, let us indicate them as **dcnm1** and **dcnm2**.

Step 2 Configure **dcnm1** as the Primary node. Paste the URL displayed on the Console tab of **dcnm1** and press **Enter** key.

A welcome message appears.

a) On the Welcome to Cisco DCNM screen, click **Get Started**.

b) On the Cisco DCNM Installer screen, select **Fresh Installation - HA Primary** radio button, to install **dcnm1** as Primary node.

Click **Continue**.

c) On the Administration tab, enter the password that is used to connect to all the applications in the Cisco DCNM Open Virtual Appliance.

Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application may not function properly.

- It must be at least eight characters long and contain at least one alphabet and one numeral.

- It can contain a combination of alphabets, numerals, and special characters.

- Do not use any of these special characters in the DCNM password for Linux, Windows, OVA, and ISO platforms:

  <SPACE> " & $ % ' ^ = < > ; : ` \ | / , .*

Select the **Show passwords in clear text** checkbox to view the password you have typed.

Click **Next**.

d) In the Install Mode tab, from the drop-down list, choose installation mode for the DCNM Appliance.

Check the **Enable Clustered Mode** checkbox, if you want to deploy Cisco DCNM in Cluster mode.

The Compute nodes will be displayed on the Cisco DCNM **Web UI > Applications > Compute**. You can add the compute nodes to a Cluster, later.

Note If **Enable Clustered Mode** is selected, applications such as, Config Compliance, EPL, and NIA, and NIR won’t work until you install the compute nodes.

Click **Next**.

e) On the System Settings, configure the settings for the DCNM Appliance.

- In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
- In the DNS Server Address field, enter the DNS IP address.

  Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.
- In the NTP Server field, enter the IP address of the NTP server.

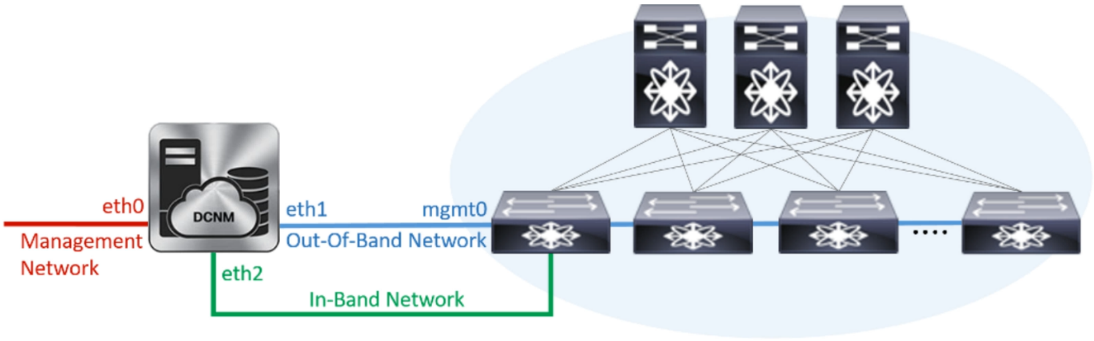
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

From Release 11.3(1), you can configure more than one DNS server and NTP server.

Click **Next**.

f) On the Network Settings tab, configure the network parameters.

Figure 5: Cisco DCNM Management Network Interfaces



- In the Management Network area, verify is the auto-populated IP Address and Default gateway address are correct. Modify, if necessary.

Note Beginning with Cisco DCNM Release 11.2(1), you can also use an IPv6 address for the Management Network.

(Optionally) Enter a valid IPv6 address along with the prefix to configure the Management address and the Management Network Default IPv6 Gateway.

- In the Out-of-Band Network area, enter the IP address, gateway IP Address. If DCNM is on the IPv6 network, configure the network with an IPv6 Address.

  Out-of-band management provides a connection to the device management ports (Typically mgmt0).

  Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

- In the In-Band Network area, enter the VIP Address and gateway IP Address for the in-band network. The In-Band Network provides reachability to the devices via the front-panel ports.

  Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

- In the Internal Application Services Network area, enter the IP subnet to access the applications that run internally to DCNM.

  All the applications use the IP Address from this subnet.

  Note Ensure that you configure the same IP subnet on both the Primary HA and the Secondary HA node.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation.

Click **Next**.

g) On the HA Settings tab, a confirmation message appears.

```
You are installing the primary DCNM HA node.
Please note that HA setup information will need to
be provided when the secondary DCNM HA node is
installed.
```

Click **Next**.

h) On the **Applications** tab, in the IPv4 Subnet field, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

The Cluster Mode configuration area appears only if you have selected the Enable Clustered Mode checkbox in Step 2.d, on page 43.

Note In Clustered mode, the Cisco DCNM Applications run on separate DCNM Compute Nodes.

1. In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the out-of-band IPv4 network to be used in the Clustered Mode.

   The address must be a smaller prefix of available IP addresses from the eth1 subnet. For example: Use 10.1.1.240/28 if the eth1 subnet was configured as 10.1.1.0/24 during installation.

   This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

2. In the **Out-of-Band IPv6 Network Address Pool**, enter the address pool from the out-of-band IPv6 network to be used in the Clustered Mode. The address pool must be an IPv6 subnet.

3. In the In-Band IPv4 Network Address Pool, enter the address pool from the out-of-band IPv4 network to be used in the Clustered Mode.

   The address must be a smaller prefix of available IP addresses eth2 subnet. For example: Use 11.1.1.240/28 if the eth2 subnet was configured as 11.1.1.0/24 during installation.

   This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

4. In the In-Band IPv6 Network Address Pool, enter the address pool from the in-band IPv6 network to be used in the Clustered Mode. The address pool must be an IPv6 subnet.

Click **Next**.

i) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A warning message appears stating that the setup is not complete until you install the Secondary node.

```
WARNING: DCNM HA SETUP IS NOT COMPLETE!
Your Cisco Data Center Network Manager software has been installed on
this HA primary node.
However, the system will be ready to be used only after installation
of the secondary node has been completed.
Thank you.
```

Step 3 Configure **dcnm2** as the Secondary node. Paste the URL displayed on the Console tab of **dcnm2** and hit Enter.

A welcome message appears.

a) On the Welcome to Cisco DCNM screen, click **Get Started**.

b) On the Cisco DCNM Installer screen, select **Fresh Installation - HA Secondary** radio button, to install **dcnm2** as Secondary node.

Click **Continue**.

c) On the Administration tab, enter the password that is used to connect to all the applications in the Cisco DCNM Open Virtual Appliance.

Note The password for the secondary node must be the same as the Administrative password for primary, as entered in Step 2.c, on page 42.

Click **Next**.

d) In the Install Mode tab, from the drop-down list, choose the same installation mode that you selected for the Primary node.

Note The HA installation fails if you do not choose the same installation mode as Primary node.

Click **Next**.

e) On the System Settings, configure the settings for the DCNM Appliance.

- In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
- In the DNS Server Address field, enter the DNS IP address.

  Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.
- In the NTP Server field, enter the IP address of the NTP server.

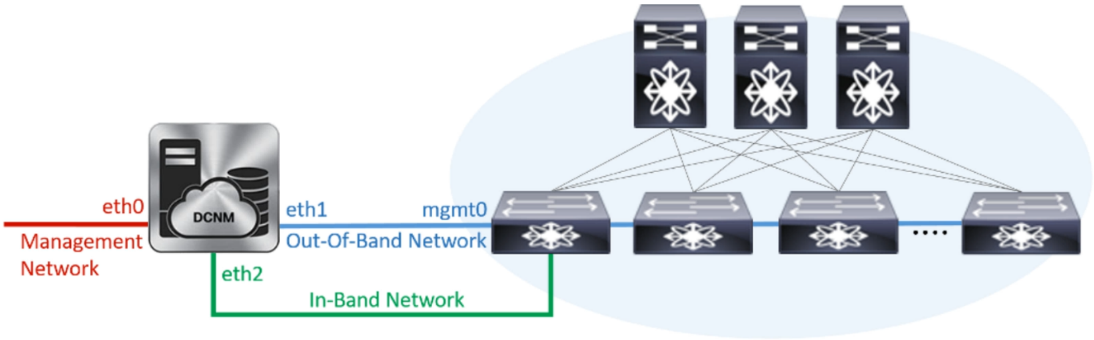
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

From Release 11.3(1), you can configure more than one DNS server and NTP server.

Click **Next**.

f) On the Network Settings tab, configure the network parameters.

Figure 6: Cisco DCNM Management Network Interfaces



- In the Management Network area, verify is the auto-populated IP Address and Default gateway address are correct. Modify, if necessary.

  Note Ensure that the IP Address belongs to the same Management Network as configured on the Primary node for HA setup to complete successfully.

  Note Beginning with Cisco DCNM Release 11.2(1), you can also use an IPv6 address for the Management Network.

(Optionally) Enter a valid IPv6 address along with the prefix to configure the Management address and the Management Network Default IPv6 Gateway.

- In the Out-of-Band Network area, enter the IP address, gateway IP Address. If DCNM is on the IPv6 network, configure the network with an IPv6 Address.

  Out-of-band management provides a connection to the device management ports (Typically mgmt0).

  Note Ensure that the IP Address, IP address gateway, and the IPv6 address belong to the same Out-of-Band Network as configured on the Primary node for HA setup to complete successfully.

  Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

  You can also configure an IPv6 address for out-of-band management network.

- In the In-Band Network area, enter the IP Address and gateway IP Address for the in-band network. The In-Band Network provides reachability to the devices via the front-panel ports.

  Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

  However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation.

- In the Internal Application Services Network area, enter the IP subnet to access the applications that run internally to DCNM.

  All the applications use the IP Address from this subnet.

  Note Ensure that you configure the same IP subnet on both the Primary HA and the Secondary HA node.

Click **Next**.

g) On the **Applications** tab, in the IPv4 Subnet field, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

Note Ensure that you configure the same IP subnet on both the Primary HA and the Secondary HA node.

Click **Next**.

h) On the HA Settings tab, configure the system settings..

- In the Management IP Address of primary DCNM node field, enter the appropriate IP Address to access the DCNM UI.
- In the VIP Fully qualified Host Name field, enter hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
- Enter the Management Network VIP address, VIPv6 address, and OOB Network VIP address appropriately.

Note If you have configured the Management network using IPv6 address, ensure that you configure the Management Network VIPv6 Address.

- Enter OOB Network VIPv6 Address to configure IPv6 address for VIP.
- In the In-Band Network area, enter the VIP Address for the in-band network.

  This is the VIP address for the In-Band network. This field is mandatory if you have provided an IP address for In-Band network in the Network Settings tab.
- Enter the HA ping IP address if necessary.

  HA_PING_ADDRESS, must be different from the DCNM Active and Standby addresses.

  You must configure the HA ping IP Address to avoid the Split Brain scenario. This address must belong to Enhanced Fabric management network.

Click **Next**.

i) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM OVA Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
***************************************************************
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at
https://<<IP Address>>:2443
You will be redirected there in 60 seconds.
Thank you
***************************************************************
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Click the **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

If you have configured inband management (eth2) IP addresses for device management, login to standalone server and configure the inband network reachability from eth2 of the server to the switches by using the following commands:

```
dcnm# appmgr setup inband-route --subnet switches-fabric-links-IP-subnet/mask
dcnm# appmgr setup inband-route --subnet switch-loopback-IP-subnet>/mask
```

For example: If you have four switches with all fabric links connected through 10.0.0.x/30 subnet, and if all switches are configured with the loopback interface for inband reachability in subnet 40.1.1.0/24, use the following commands:

```
dcnm# appmgr setup inband-route --subnet 10.0.0.0/24
dcnm# appmgr setup inband-route --subnet 40.1.1.0/24
```

Launching SAN Client and Device Manager

This following sections explain the various methods to launch Cisco DCNM SAN Client and Device Manager.

Launching SAN Client and Device Manager from Web UI

To launch Cisco DCNM SAN Client and Device Manager from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Log in to Cisco DCNM Web UI after installing Cisco DCNM SAN deployment.

Step 2 Click on the gear icon, and click **DCNM SAN & DM**.

Save the `dcnm-client.zip` to your directory.

Step 3 Extract the contents of `dcnm-client.zip` to `dcnm-clientzip/bin` directory.

Step 4 To launch the SAN Client and Device Manager:

- **For Windows deployment:**

  Double-click on the **FMClient.bat** file to launch the Cisco DCNM SAN Client.

  Double-click on the **DeviceManager.bat** to launch the Cisco DCNM Device Manager.

- **For Linux deployment:**

  Run **./FMClient.sh** Script to launch SAN Client.

  Run **./Devicemanager.sh** script to launch Device Manager.

Launching SAN Client and Device Manager from DCNM Server

By default, the SAN Client and Device Manager are installed along with the Cisco DCNM Server, when you install DCNM. To launch Cisco DCNM SAN Client and Device Manager from the Cisco DCNM Server, perform the following steps:

Procedure

Step 1 Log in to the DCNM server.

Step 2 Navigate to `Cisco Systems\dcm\fm\bin\` directory.

Step 3 To launch the SAN Client and Device Manager:

- **For Windows deployment:**

Double-click on the **FabricManager.bat** file to launch the Cisco DCNM SAN Client.

Double-click on the **DeviceManager.bat** file to launch the Cisco DCNM Device Manager.

- **For Linux deployment:**

  Run the **./ FabricManager.sh** script to launch the Cisco DCNM SAN Client.

  Run the **./DeviceManager.sh** script to launch the Cisco DCNM Device Manager.

Launching DCNM SAN Client from DCNM SAN for Windows deployment with SSL enabled

When you install Cisco DCNM for Windows with custom SSL configured on the DCNM server, you can’t launch the SAN Client. Modify the certificates to launch the SAN Client successfully.

To modify the certificates and launch the DCNM SAN Client from Windows Deployment, perform the following steps:

Procedure

Step 1 Extract public key using the **keytool.exe -exportcert -file dcnmweb.crt -alias sme C:\[DCNM Install directory]\cisco\dcm\wildfly-14.0.1.Final\Standalone\configuration\fmserver.jks** command.

```
// extract public key from the new fmserver.jks and save it to dcnmweb.crt,  alias “sme”,
 password “fmserver_1_2_3”
c:\[DCNM install dirrectory]\dcm\java\jdk11\bin>keytool.exe -exportcert -file dcnmweb.crt
-alias sme C:\[DCNM Install
directory]\cisco\dcm\wildfly-14.0.1.Final\Standalone\configuration\fmserver.jks
Enter keystore password:
Certificate stored in file <dcnmweb.crt>
c:\[DCNM install dirrectory]\dcm\java\jdk11\bin>dir
chain-cert.pem  dcnmweb.crt  jjs         keytool  rmiregistry
dcnm.csr        java         jrunscript  rmid
```

Step 2 Generate key store using the **keytool.exe -importcert -trustcacerts -file dcnmweb.crt -keystore fmtrust.jks -storetype jks** command.

```
// generate key store without password,  during the command,  just use random password
dcnm123
c:\[DCNM install dirrectory]\dcm\java\jdk11\bin>keytool.exe -importcert -trustcacerts -file
 dcnmweb.crt -keystore fmtrust.jks -storetype jks
Enter keystore password:
Re-enter new password:
Owner: CN=Lin, OU=cisco, O=cisco, L=sj, ST=ca, C=US
Issuer: CN=rhel144, OU=DCBu, O=Cisco, L=BGL, ST=KA, C=IN
Serial number: 1086
Valid from: Wed Nov 13 12:17:23 PST 2019 until: Thu Nov 12 12:17:23 PST 2020
Certificate fingerprints:
         SHA1: F8:19:CB:79:FC:93:08:54:74:9A:BC:F3:8F:CB:9C:A7:22:56:3D:0F
         SHA256:
8F:06:1F:72:15:FD:12:B5:E9:43:E4:61:0E:00:E0:1C:96:CE:9C:90:82:3C:5C:EA:A1:49:A8:A9:66:9B:86:31
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
```

```
Extensions:

#1: ObjectId: 2.16.840.1.113730.1.13 Criticality=false
0000: 16 1D 4F 70 65 6E 53 53   4C 20 47 65 6E 65 72 61  ..OpenSSL Genera
0010: 74 65 64 20 43 65 72 74   69 66 69 63 61 74 65     ted Certificate

#2: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: C9 1E 9B 17 EF AE E4 AF   7A E3 88 BC 2D C9 B9 E9  ........z...-...
0010: FC EC 40 82                                        ..@.
]
]#3: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:false
  PathLen: undefined
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 9A 9E B4 98 95 8C 9F FB   0B 57 A5 6D 78 EB 8D C1  .........W.mx...
0010: BB 80 00 DE                                        ....
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
c:\[DCNM install dirrectory]\dcm\java\jdk11\bin>dir
chain-cert.pem  dcnmweb.crt  java  jrunscript  rmid
dcnm.csr        fmtrust.jks  jjs   keytool     rmiregistry
```

Step 3 Copy the newly created **fmtrust.jks** to `\fm\lib\fm` directory.

```
c:\[DCNM install dirrectory]\dcm\java\jdk11\bin>cp fmtrust.jks ..\..\..\fm\lib\fm
cp: overwrite â..\..\..\fm\lib\fm\fmtrust.jks? y
```

Step 4 Locate the **dcnm-client.zip**, downloaded from Web UI or DCNM server.

Step 5 Unzip and replace the **vin\fmtrust.jks** with the newly created **fmtrust.jks** file.

Step 6 Run the **FabricManager.bat** batch file to launch the Cisco DCNM SAN Client.

Launching DCNM SAN Client from DCNM SAN for Linux deployment with SSL enabled

When you install Cisco DCNM for Linux with custom SSL configured on the DCNM server, you cant launch the SAN Client. You must modify the certificates to launch the SAN Client successfully.

To modify the certificates and launch the DCNM SAN Client from Linux Deployment, perform the following steps:

Procedure

Step 1 Extract public key using the **./keytool -exportcert -file dcnmweb.crt -alias sme -keystore /usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks** command.

```
// extract public key from the new fmserver.jks and save it to dcnmweb.crt,  alias “sme”,
 password “fmserver_1_2_3”
[root@dcnm-lnx1 bin]# ./keytool -exportcert -file dcnmweb.crt -alias sme -keystore
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks
Enter keystore password:
Certificate stored in file <dcnmweb.crt>
[root@dcnm-M5-2-lnx1 bin]# ls
chain-cert.pem  dcnmweb.crt  jjs         keytool  rmiregistry
dcnm.csr        java         jrunscript  rmid
```

Step 2 Generate key store using the **./keytool -importcert -trustcacerts -file dcnmweb.crt -keystore fmtrust.jks -storetype jks** command.

```
// generate key store without password,  during the command,  just use random password
dcnm123
[root@dcnm-lnx1 bin]# ./keytool -importcert -trustcacerts -file dcnmweb.crt -keystore
fmtrust.jks -storetype jks
Enter keystore password:
Re-enter new password:
Owner: CN=Lin, OU=cisco, O=cisco, L=sj, ST=ca, C=US
Issuer: CN=rhel144, OU=DCBu, O=Cisco, L=BGL, ST=KA, C=IN
Serial number: 1086
Valid from: Wed Nov 13 12:17:23 PST 2019 until: Thu Nov 12 12:17:23 PST 2020
Certificate fingerprints:
         SHA1: F8:19:CB:79:FC:93:08:54:74:9A:BC:F3:8F:CB:9C:A7:22:56:3D:0F
         SHA256:
8F:06:1F:72:15:FD:12:B5:E9:43:E4:61:0E:00:E0:1C:96:CE:9C:90:82:3C:5C:EA:A1:49:A8:A9:66:9B:86:31
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.16.840.1.113730.1.13 Criticality=false
0000: 16 1D 4F 70 65 6E 53 53   4C 20 47 65 6E 65 72 61  ..OpenSSL Genera
0010: 74 65 64 20 43 65 72 74   69 66 69 63 61 74 65     ted Certificate


#2: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: C9 1E 9B 17 EF AE E4 AF   7A E3 88 BC 2D C9 B9 E9  ........z...-...
0010: FC EC 40 82                                        ..@.
]
]

#3: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:false
  PathLen: undefined
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 9A 9E B4 98 95 8C 9F FB   0B 57 A5 6D 78 EB 8D C1  .........W.mx...
0010: BB 80 00 DE                                        ....
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
[root@dcnm-M5-2-lnx1 bin]# ls
chain-cert.pem  dcnmweb.crt  java  jrunscript  rmid
```

```
dcnm.csr        fmtrust.jks  jjs   keytool     rmiregistry
[root@dcnm-M5-2-lnx1 bin]# pwd
/usr/local/cisco/dcm/java/jdk11/bin
```

Step 3 Copy the newly created **fmtrust.jks** to `/fm/lib/fm` directory.

```
[root@dcnm-M5-2-lnx1 bin]# cp fmtrust.jks ../../../fm/lib/fm
cp: overwrite â../../../fm/lib/fm/fmtrust.jks? y
```

Step 4 Locate the **dcnm-client.zip**, downloaded from Web UI or DCNM server.

```
[root@dcnm-M5-2-lnx1 dcm]# cd fm/download/
[root@dcnm-M5-2-lnx1 download]# pwd
/usr/local/cisco/dcm/fm/download
[root@dcnm-M5-2-lnx1 download]# ls
dcnm-clientzip.zip
// for remote access, in fm/download/dcnm-clientzip.zip,  replace bin/fmtrust.jks with this
 new fmtrust.jks
```

Step 5 Replace the **fmtrust.jks** in the `/bin` directory with the newly created **fmtrust.jks** file.

Step 6 Run the **./ FabricManager.sh** script to launch the Cisco DCNM SAN Client.