Installing the Cisco DCNM

This chapter contains the following sections:

If you are installing Cisco DCNM on SE, install the DCNM ISO Virtual Appliance (.iso) installer.

- Installing Cisco DCNM on Windows, on page 1
- Installing Cisco DCNM on Linux, on page 8
- Launching SAN Client and Device Manager, on page 16

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. Ensure that you delete the `pgevent.dll` (located at `dcm db path \db\lib\pgevent.dll`) before beginning to upgrade.

Procedure

Step 1 Stop Cisco DCNM Services.

Close all instances of DCNM SAN client and Device Manager running on the server.

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.

Before you begin

To support specific beta equipment support, download DCNM Release 11.5(2) installer and properties file. For all other supported hardware, we recommend that you deploy Cisco DCNM Release 11.5(1).

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 11.5(1)Release 11.5(2).

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

The installer file is of the format `dcnm-installer-x64.11.5.1.exedcnm-installer-x64.11.5.2.exe`.

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 to show 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.

The following message appears:

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

Click **OK** to continue.

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 don’t 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 can’t 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 don’t 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" can’t be accessible. This is default behavior.

Only if the TACACS/RADIUS/LDAP server isn’t reachable or down, the Local user will be validated and is able to log in.

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.

Note Do not close the installer, nor kill the wizard. Ensure that you click **Done**.

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.

The following message appears:

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

Click **OK** to continue.

Step 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.

Close all instances of DCNM SAN client and Device Manager running on the server.

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.

Note If you're uninstalling RHEL 8.x, use **./Uninstall_DCNM -i silent** command. However, RHEL 8.x doesn’t support uninstalling via the Web UI.

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    /* for uninstalling RHEL 7.x */
[dcnm-linux]# ./Uninstall_DCNM -i silent /* for uninstalling RHEL 8.x */
[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.

Before you begin

To support specific beta equipment support, download DCNM Release 11.5(2) installer and properties file. For all other supported hardware, we recommend that you deploy Cisco DCNM Release 11.5(1).

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 11.5(1)Release 11.5(2).

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

The installer file is of the format `dcnm-installer-x64.11.5.2.bindcnm-installer-x64.11.5.1.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:

Before you begin

Ensure that the DISPLAY variable is set to 1.

- Check if DISPLAY variable is set to 1 by using the following command:

  echo $DISPLAY
- Set DISPLAY variable to 1 by using the following command:

  export DISPLAY=:1

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

The following message appears:

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

Click **OK** to continue.

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.

Note The location for installation must be within the partition where the required disk space is provisioned. Ensure that there is sufficient disk space for deployment.

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 10 section.
- Ensure that the DISPLAY variable is set to 1.
    - Check if DISPLAY variable is set to 1 by using the following command:

      echo $DISPLAY
    - Set DISPLAY variable to 1 by using the following command:

      export DISPLAY=:1

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.

The following message appears:

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

Click **OK** to continue.

Step 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.

Before you begin

Ensure that you have execution permissions to the /tmp directory before you begin to install Cisco DCNM on Linux.

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.

Launching SAN Client and Device Manager

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

Note For OVA/ISO deployments, you must update the certificates after upgrading to Cisco DCNM Release 11.5(1), before launching the SAN Client or Device Manager. Use the **appmgr afw update-cert-dcnm-client** command to update the certificates.

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:

- **If you are launching DCNM on Windows environment:**

  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.

- **If you are launching DCNM on Linux environment:**

  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 Custom SSL Certificate

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 following command. command.

keytool.exe -exportcert -file dcnmweb.crt -alias sme -keystore   C:\[DCNM Install directory]\cisco\dcm\wildfly-14.0.1.Final\Standalone\configuration\fmserver.jks

Step 2 Generate key store using the following command.

keytool.exe -importcert -trustcacerts -file dcnmweb.crt -keystore fmtrust.jks -storetype jks

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

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

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

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

Example

The following sample example shows the command to modify the certificates and launch the DCNM SAN Client from Windows Deployment.

```
// extract public key from the new fmserver.jks and save it to dcnmweb.crt,
alias “sme”,  password “<<storepass-kwd>>”
c:\[DCNM install directory]\dcm\java\jdk11\bin>
keytool.exe -exportcert -file dcnmweb.crt -alias sme -keystore 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 directory]\dcm\java\jdk11\bin> dir
chain-cert.pem  dcnmweb.crt  jjs         keytool  rmiregistry
dcnm.csr        java         jrunscript  rmid


// generate key store without password,  during the command,
just use random password  dcnm123
c:\[DCNM install directory]\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 directory]\dcm\java\jdk11\bin>dir
chain-cert.pem  dcnmweb.crt  java  jrunscript  rmid
dcnm.csr        fmtrust.jks  jjs   keytool     rmiregistry


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


c:\[DCNM install directory]\dcm\java\jdk11\bin> FabricManager.bat
```

Launching DCNM SAN Client from DCNM SAN for Linux deployment with Custom SSL Certificate

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 following command.

./keytool -exportcert -file dcnmweb.crt -alias sme -keystore /usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks

Step 2 Generate key store using the following command.

./keytool -importcert -trustcacerts -file dcnmweb.crt -keystore fmtrust.jks -storetype jks

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

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

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.

Example

The following sample example shows the command to modify the certificates and launch the DCNM SAN Client from Linux Deployment.

```
// extract public key from the new fmserver.jks and save it to dcnmweb.crt,
alias “sme”,  password “<<storepass-pwd>>”
[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


// generate key store without password,  during the command.
[root@dcnm-lnx1 bin]# ./keytool -importcert -trustcacerts -file dcnmweb.crt
-keystore fmtrust.jks -storetype jks
Enter keystore password:       //Navigate to
/usr/local/cisco/dcm/fm/conf/serverstore.properties.
//Fetch the keystore password from dcnmtrustedclient.token field.
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

[root@dcnm-M5-2-lnx1 bin]#

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


[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


[root@dcnm-M5-2-lnx1 bin]# ./ FabricManager.sh
```

Launching Cisco DCNM SAN Client in Linux Federation Setup with Self-signed DCNM Certificates

Before 11.4.1, the static password **fmserver_1_2_3** was used by DCNM for **fmtrust.jks** deployment. Therefore, you can download SAN client from Node1 or VNC to Node1 and launch the SAN Client. You can then logon to any server in the Federation setup (Node1/Node2/Node3).

Beginning from 11.4.1, DCNM uses a unique **dcnm.fmserver.token** password. Therefore, the **fmtrust.jks** file is different in each server in the Federation setup, by default. If you download SAN client from Node1 or VNC to Node1 and try to launch SAN client with Node2 or Node3, it fails.

If you are using a default DCNM self-signed certificate in Federation setup, you must download the SAN client from the respective server, and launch the SAN Client. You must open the fabric managed by the same server.

For Example:

- Downloaded SAN Client from Node1 or VNC to Node1, Launch SAN Client and Login to Node1
- Downloaded SAN Client from Node2 or VNC to Node2, Launch SAN Client and Login to Node2
- Downloaded SAN Client from Node3 or VNC to Node3, Launch SAN Client and Login to Node3

Note This is applicable on all DCNM Federation fresh installation, with default DCNM self-signed certificate. It is also applicable on DCNM Federation upgrade with default DCNM self-signed certificate.

Launching DCNM SAN Client from DCNM SAN for OVA/ISO deployment with Custom SSL Certificate

When you install Cisco DCNM SAN OVA/ISO with custom SSL configured on the DCNM server, you can't launch the SAN Client. Install the CA signed certificate, and then, download and launch the DCNM SAN Client from the Web UI.

Refer to Installing a CA Signed Certificate for instructions on how to install the CA signed certificate on the Cisco DCNM SAN OVA/ISO server.

For OVA/ISO deployments, you must update the certificates after upgrading to Cisco DCNM Release 11.5(1), before launching the SAN Client or Device Manager. Use the **appmgr afw update-cert-dcnm-client** command to update the certificates.

Launch the Web UI. Download the DCNM SAN Client. Launch the DCNM SAN Client and Device Manager.

Launching DCNM SAN Client from Cisco SAN OVA/ISO Server

To launch DCNM SAN client on the Cisco DCNM SAN OVA/ISO server, perform the following steps:

Note Do not install any GUI package / X11 or VNC on DCNM SAN OVA/ISO server.

Before you begin

For OVA/ISO deployments, you must update the certificates after upgrading to Cisco DCNM Release 11.5(1), before launching the SAN Client or Device Manager. Use the **appmgr afw update-cert-dcnm-client** command to update the certificates.

Procedure

Step 1 VNC to any DCNM server where VNC is installed, for example, `vnc-lnx:2`.

Step 2 Open two terminals in `vnc-lnx`.

Step 3 In one terminal execute the command **xhost +**.

Step 4 In the second terminal, SSH to DCNM OVA server.

Step 5 Export **DISPLAY=vnc-lnx:2.0**.

Step 6 Launch the SAN client from the terminal in Step Step 4, on page 23.

Launching Fabric Manager and Device Manager using VNC

From Release 11.5(1), Cisco DCNM provisions an environment to use Device Manager and Fabric Manager on a local VNC server. This environment is set up during installation of Cisco DCNM SAN for OVA/ISO deployments.

For OVA/ISO deployments, you must update the certificates after upgrading to Cisco DCNM Release 11.5(1), before launching the SAN Client or Device Manager. Use the **appmgr afw update-cert-dcnm-client** command to update the certificates.

Connect the DCNM IP address with the VNC client software. After the connection is established, VNC client displays the virtual desktop.

On the Menu bar, select **Applications**. Locate **Cisco Systems, Inc.**. The relevant applications are displayed. You can select and run Device Manager and Fabric Manager applications.

Note The VNC client-server session is not encrypted.