Installation of DCNM

Before upgrading or uninstalling Cisco DCNM or Device Manager, make sure that any instances of these applications have been shut down.

This chapter contains the following sections:

- "Installation options" section on page 3-1
- "DCNM Programmable Fabric Installation" section on page 3-2
- "DCNM installation without Enhanced Fabric Management capabilities" section on page 3-19
- "DCNM Native HA Installation" section on page 3-29
- "Running Cisco DCNM Behind a Firewall" section on page 3-32

Installation options

Fresh Installation

- For Windows and Linux installers, the installer installs Cisco DCNM-SAN and Cisco SMI-S agent on your system.
- For Virtual Appliances (OVA/ISO), the installer installs the Operating system and Cisco DCNM components.

Note When the ISO/OVA appliance is deployed in DFA mode, the Cisco SMI-S component will not start by default. However, the component can be managed using the following commands:

appmgr start or **stop dcnm-smis**

The **appmgr start** or the **stop dcnm** command will start or stop the Web component.

While for non-DFA deployments (ISO/OVA/.exe/.bin), all services will be started by default.

For more information about the application management, see Managing Applications, page 6-8.

- From Release 10.0(1), Cisco DCNM will ask you to choose from the following options during installation. Based on the option you select, the application will be installed
  - DCNM Web Client

– DCNM SAN Client

Upgrade

- For Windows and Linux installers, the default is to upgrade to the latest version of Cisco DCNM.
- For Virtual Appliances (OVA/ISO), you must execute the **appmgr** command to upgrade. For more information, see "Upgrading Cisco DCNM".

Note The password can contain a combination of alphabets, numeric, and special characters. The only chars that are not allowed in the DCNM password for Linux/Windows/OVA/ISO platforms are: <SPACE>&$% single and double quotes. And the rest are all allowed: ! @ # ^ * - + = : ; ?,. / ~ ` \ | < > ().

This chapter describes how to install Cisco Data Center Network Manager (DCNM) and includes the following sections:

- DCNM Programmable Fabric Installation, page 3-2
- DCNM installation without Enhanced Fabric Management capabilities, page 3-19
- Running Cisco DCNM Behind a Firewall, page 3-32

DCNM Programmable Fabric Installation

This section contains the following:

- DCNM Open Virtual Appliance Installation in Programmable Fabric mode, page 3-2
- DCNM ISO Virtual Appliance Installation, page 3-9
- Configuring Media Controller for IP Fabric, page 3-26
- DCNM OVA in High Availability/Federation, page 3-26

Note Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. For more information, see Setting the Timezone for Cisco DCNM Virtual Appliances, page 3-18.

DCNM Open Virtual Appliance Installation in Programmable Fabric mode

For information about the Prerequisites before you begin the installation, see Prerequisites for DCNM Open Virtual Appliance section.

Three steps are required to install the DCNM Open Virtual Appliance:

1. Verify Prerequisites. You must install various VMware components before you install the Open Virtual Appliance. See Verifying Prerequisites, page 3-3.
2. Download the Open Virtual Appliance file. You can access the required dcnm.ova file from www.cisco.com. See Downloading the Open Virtual Appliance File, page 3-3.

3. Deploy the Open Virtual Appliance as an OVF template. A step-by-step template in the vSphere Client guides you through this process. After you have completed the step-by-step template, you can review all of the information that you provided, make any corrections, and then deploy the Open Virtual Appliance. See Deploying the Open Virtual Appliance as an OVF Template, page 3-3.

Note If you are using a high-availability (HA) environment for applications that are bundled within the DCNM ISO Virtual Appliance, you must download the ISO and deploy twice, once for Active and once for Host-Standby. For more information, see Chapter 7, "Managing Applications in a High-Availability Environment".

Verifying Prerequisites

For more information, see Prerequisites for DCNM Open Virtual Appliance section.

Downloading the Open Virtual Appliance File

The first step to installing the Open Virtual Appliance is to download the dcnm.ova file. You will 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.

DETAILED STEPS

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

Step 2 In the **Product/Technology Support** section, choose **Download Software**.

Step 3 In the **Select a Product** section, navigate to the DCNM software by choosing **Products > Switches > Data Center Switches > Data Center Network Management > Cisco Data Center Network Manager**.

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

Step 4 In the **Latest Releases** list, choose **10.1(x)**.

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

Step 6 Save the dcnm.ova file to your computer in a place that will be 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 will deploy the OVF template from the vSphere Client application.

DETAILED STEPS

Step 1 Log in to your vSphere Client:

a. Open the VMware vSphere client application on your desktop.

b. Connect to the vCenter Server with your vCenter user credentials.

Note You cannot deploy the Open Virtual Appliance by connecting the vSphere Client directly to the ESXi server.

Step 2 Use the vSphere Client to access the OVF template:

a. Choose **Home > Inventory > Hosts and Clusters**.

b. Choose the host on which the OVF template will be deployed.

c. Choose **File > Deploy OVF Template** to open the Deploy OVF Template window.

Step 3 Choose the Source location:

a. Click the **Browse** button.

b. Locate the dcnm.ova file that you downloaded to your computer and click **Next**.

Step 4 Review the OVF Template Details and click **Next**.

Some of the details about the Cisco DCNM virtual appliance include:

- Version number
- Download size
- Size on disk:
  - Thin provision for the amount of disk space consumed by the virtual appliance immediately after deployment. It is the minimum amount of disk space needed to deploy the virtual appliance.
  - Thick provision for the maximum amount of disk space the virtual appliance can consume.

Note For more information on thick and thin provision, see "Step 11 - Choose the disk format." task on page 3-5

Step 5 Read and accept the End User License Agreement and click **Next**.

Step 6 Specify the name and location of the Cisco DCNM Open Virtual Appliance.

a. In the **Name** box, enter a name for the virtual appliance. This name is not the hostname, but the name of the virtual appliance hardware and is specific to the vSphere infrastructure.
The name can contain up to 80 alphanumeric characters and must be unique within the Inventory folder.

b. In the **Inventory Location** tree, choose the folder location for the virtual appliance.

c. Click **Next.**

Step 7 Choose the deployment configuration:

- **Choose Small** to configure the virtual machine with two vCPUs and 8G RAM.
- **Choose Large** to configure the virtual machine with four vCPUs and 12G RAM.

Note We recommend that you use a Large deployment configuration when you are managing more than 50 devices (and up to the upper limit of the Cisco Programmable Fabric) to leverage better RAM, heap memory, and CPUs.

For setups that could grow, you should choose Large.

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

Step 8 Click **Next**.

Step 9 Specify the host and click **Next**.

Note A host will not be available if you already selected a host in the vSphere Client before you deploy the Open Virtual Appliance.

Note The DCNM Open Virtual Appliance should not be deployed under vApp.

Step 10 Choose a destination storage for the virtual machine files.

Step 11 Choose the disk format.

- 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 at a later time on first write from the virtual disk.
  - **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.
- Choose **Thin Provision** if you have less than 100 GB of disk space available. The initial disk consumption will be 3GB and will increase as the size of the database increases with the number of devices being managed.

Step 12 Click **Next.**

Step 13 Choose your network mapping.

a. The dcnm-mgmt network provides connectivity (ssh, scp, http, https) to the Cisco DCNM Open Virtual Appliance. In the **Destination Network** column, associate the network mapping with the port group that corresponds to the subnet that is associated with the Cisco DCNM management network.

b. Map the enhanced-fabric-mgmt network to the port group that connects to the management network of switches.

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

- Both OVAs should have their management access (eth0) and enhanced fabric management (eth1) interfaces in the same subnet.
- Both OVAs should be deployed with the same administrative password. This is to ensure that both OVAs are duplicates of each other for application access.

Step 14 Click **Next**.

Step 15 Choose the Cisco DCNM Open Virtual Appliance Properties**.**

a. The **Application Management** check box is selected by default to install the SAN management functionalities.

b. In the **Management Properties** section, enter a password in the **Enter Password** and **Confirm Password** boxes to establish the password that will be used to connect all applications in the DCNM Open Virtual Appliance.

Note The password can contain a combination of alphabets, numeric, and special characters. The only chars that are not allowed in the DCNM password for Linux/Windows/OVA/ISO platforms are: <SPACE>&$% single and double quotes. And the rest are all allowed: ! @ # ^ * - + = : ; ?,. / ~ ` \ | < > ().

If you do not comply with these password requirements, you can continue with the DCNM Open Virtual Appliance deployment; however, you subsequently may not be able to log in to other applications like DCNM.

c. In the **DCNM Network** section, complete each of the required fields:

- **Hostnam**e (should be a fully qualified domain name, otherwise you may encounter issues when using the XMPP application after deployment)
- **IP Address** (for the outside management address for DCNM)
- **Subnet Mask**
- **Default Gateway**
- **DNS IP**

d. In the **Enhanced Fabric Management** section, complete each of the required fields:

- **IP Address** (for the inside fabric management address or OOB Management Network)
- **Subnet mask**
- **DNS IP**

Note If the parameters in this section are not provided, features such as POAP and auto-configuration will not be functional.

Step 16 Click **Next**

Step 17 Review each of the deployment settings that you have established. Press the **Back** button to go to any settings if you want to change them.

After you have reviewed each of the deployment settings in the OVF template, perform the following procedure to deploy the virtual machine.

Deploying Virtual Machines

Step 1 Check the **Power on after deployment** check box.

Step 2 Click the **Finish** button.

A Deploying DCNM_OVA window appears and the Open Virtual Appliance deployment starts and requires some time to complete.

Note The time for the DCNM Open Virtual Appliance deployment could take 5 to 6 minutes (or more) depending on the network latency.

After the Open Virtual Appliance is deployed, a Deployment Completed Successfully message appears.

Step 3 On the **Summary** tab in the vSphere Client, review the information about the VM and make note of the IP address.

Step 4 Check the console of the VM in the vSphere Client for the login prompt. Once the login prompt appears, log in with root credentials and use the **appmgr status all** command to check the status of the applications. After all applications are up and running, go to the next step.

Note For more information about verifying application status see the Verifying the Application Status after Deployment, page 6-9.

Step 5 Log in to the Cisco DCNM web UI:

a. Put the IP address in your browser.

The Cisco Data Center Network Manager window is displayed.

b. In the **User Name** field, enter **admin**.

c. In the **Password** field, enter the administrative password given to you during the DCNM Open Virtual Appliance deployment.

Note If you are deploying multiple OVAs for HA functions, you should deploy both the OVAs with the same administrative password. This action ensures that both OVAs are duplicates of each other for application access.

You are ready to begin POAP configuration and Device Discovery.

Note See the *Cisco DCNM Fundamentals Guide* for configuration information.

Configuring the Oracle Database for DCNM Virtual Appliances

Cisco DCNM, Release 10.1(x) contains a built-in PostgreSQL database that supports full-scale deployments with High-Availability. However, you can optionally use the Oracle Database for backend storage.

DETAILED STEPS

Step 1 Prepare the Oracle database.

For more information, see Preparing the Oracle Database, page 2-21.

Note If you are configuring the Oracle database for an HA environment, only Step 1 is required. If you are configuring the Oracle database for a standalone DCNM, continue with the following steps in the procedure.

Step 2 Get the JDBC database URL, database username, and database password.

Step 3 Stop the Cisco DCNM application in the Open Virtual Appliance by entering the following command:

appmgr stop dcnm

Step 4 Open the SSH terminal and enter the following CLI command:

appmgr update dcnm -u *<DB_URL>* -n *<DB_USER>* -p *<DB_PASSWORD>*

Step 5 Enter the root password of the Cisco DCNM Open Virtual Appliance.

This password is used to access AMQP/LDAP by default. You can change this password later in Cisco DCNM Web Client by using the following path: **Configure > LAN Fabric Settings > General**.

```
[root@DCNM ~]# appmgr update dcnm -u jdbc:oracle:thin:@10.77.247.11:1521:XE -n extuser -p
extuserpwd
```

The external DCNM database will be configured to access all the Programmable Fabric applications using the root password of this server. You can change the password from the Cisco DCNM Web Client on **Configure > LAN Fabric Settings > General** page.

```
Root password :
Enter it again for verification:
Please wait...this could take a few minutes

Done.
```

Note The password can contain a combination of alphabets, numeric, and special characters. The only chars that are not allowed in the DCNM password for Linux/Windows/OVA/ISO platforms are: <SPACE>&$% single and double quotes. And the rest are all allowed: ! @ # ^ * - + = : ; ?,. / ~ ` \ | < > ().

Step 6 Start the Cisco DCNM application in the Open Virtual Appliance by entering the following command:

appmgr start dcnm

Step 7 Update the Fabric setting in Cisco DCNM, if necessary.

Configuring the Oracle Database for XMPP

Perform the following steps to configure Oracle Database for XMPP:

Note If you configure a remote Oracle database for both DCNM and XMPP in an appliance (OVA/ISO), create two separate database users—one for the DCNM and the other for XMPP.

Step 1 Prepare the Oracle database.

For more information, see Preparing the Oracle Database, page 2-21.

Step 2 Get the JDBC database URL, database username and database password.

Step 3 Stop the Cisco XMPP application in the DCNM Open Virtual Appliance.

Step 4 Open the SSH terminal and enter the following command:

appmgr update xmpp -u <oracle_jdbc_url> -n <oracle_db_user> -p <oracle_db_password>

where:

-u <oracle_jdbc_url> : Oracle JDBC URL

-n <oracle_db_user> : Database Username

-p <oracle_db_password>: Database User Password

```
For example,
appmgr update xmpp  -u  jdbc:oracle:thin:@1.2.3.4:1521:XE  -n  admin  -p  secret
```

Step 5 Start the Cisco XMPP application in the DCNM Open Virtual Appliance.

Note Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. For more information, see Setting the Timezone for Cisco DCNM Virtual Appliances, page 3-18.

DCNM ISO Virtual Appliance Installation

The DCNM ISO Virtual Appliance can be deployed in ESXi and KVM Hypervisors.

You can change from the local database to an external Oracle database, if required. For instructions, see Change from Local Database to an External Database, page 6-11.

During the installation of the Cisco DCNM ISO Virtual Appliance, an error message appears on the graphical console, based on based on the hardware of the setup.

If an unsupported Hardware Detected, perform one of the following:

- Ignore the error message and click OK to continue with the installation
- Try installing the DCNM ISO Virtual Appliance on a different hardware platform. Refer to the the CentOS hardware compatibility matrix located at www.centos.org/hardware

Note It is strongly recommended to install the Cisco DCNM ISO Virtual Appliance on a supported hardware platform.

Downloading DCNM ISO Virtual Appliance Installer

Note This procedure is common to both DCNM ISO Virtual Appliance Installation on VMWare ESXi and KVM deployments.

Step 1 Navigate to http://software.cisco.com/download/navigator.html.

Step 2 In the **Product/Technology Support** section, select **Download Software**.

Step 3 In the **Select a Product** section, navigate to the DCNM software. Select **Products > Switches > Data Center Switches > Data Center Network Management > Data Center Network Manager**.

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

Step 4 In the Latest Releases list, choose 10.1(x)

Step 5 Locate the DCNM ISO **dcnm-va.iso** at **DCNM Virtual Appliance for VMWare, KVM** and click **Download**.

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

Proceed to one of the following:

Note You can change from the local database to an external Oracle database, if required. For instructions, see Change from Local Database to an External Database, page 6-11.

- Installing the DCNM ISO Virtual Appliance on VMWare ESXi, page 3-10
- Installing the DCNM ISO Virtual Appliance on KVM, page 3-14
- Installing the DCNM ISO Virtual Appliance on N1110, page 3-16

Installing the DCNM ISO Virtual Appliance on VMWare ESXi

Perform the following tasks to install the ISO virtual appliance on VMWare ESXi.

Step 1 Unzip and extract the **dcnm-va-ovf-kvm-files.<10.1.1>.zip** and locate **dcnm-esxi-vm.ovf** file.

Step 2 Launch **VMWare vSphere client** application and connect the **vCenter Server** using the vCenter/ESXi user credentials.

Step 3 Use the vSphere Client to deploy the OVF template.

Step 4 Navigate to **Home > Inventory > Hosts and Clusters**.

Select the host on which the OVF template must be deployed.

Step 5 Navigate to **File > Deploy OVF Template** to open the Deploy OVF template window.

Choose the Source location, and click **Browse**.

Step 6 Locate the **dcnm-esxi-vm.ovf** file and click **Next**.

Step 7 Review the OVF template details and click **Next**.

Step 8 Read and accept the End User License Agreement and click **Next**.

Step 9 Specify the name and location of the Cisco DCNM appliance.

In the Name box, enter a name for the ISO Virtual Appliance. This is the name of the virtual appliance hardware and is specific to the vSphere infrastructure.The name can contain up to 80 alphanumeric characters and must be unique within the Inventory folder.

Step 10 In the **Inventory Location** tree, choose the folder location for the virtual appliance and click **Next**.

Step 11 Choose the deployment configuration:

- Small—to configure the virtual machine with two vCPUs and 8G RAM.
- Large—to configure the virtual machine with four vCPUs and 12G RAM.

Note Cisco recommends that you use a Large deployment configuration when you are managing more than 50 devices (and up to the upper limit of the Cisco Fabric) to leverage better RAM, heap memory, and CPUs. For setups that could grow, you should choose Large. Choose Small for proof-of-concept and other small-scale environments with fewer than 50 switches that are not expected to grow with time. You can change from the local database to an external Oracle database, if required. For instructions, see Change from Local Database to an External Database, page 6-11.

Click **Next**.

Step 12 Specify the **Host** and click **Next**.

Note A host will not be available if you already selected a host in the vSphere Client before you deploy the Cisco DCNM Appliance.

Step 13 Choose a destination storage for the virtual machine files.

Step 14 Choose the disk format.

- Select any 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 required for the virtual disk is allocated when the virtual disk is created. The data on the physical device will not be erased when the virtual disk is created. However, it is erased when the new data is saved from the virtual disk.
  - Thick Provision Eager Zeroed

    The space required for the virtual disk is allocated when the virtual disk is created. The data on the physical device is erased when the virtual disk is created.
- Choose Thin Provision if you have less than 100 GB of disk space available. The initial disk consumption will be around 3 GB and will increase as the size of the database increases with the number of devices being managed.

Step 15 Choose your network mapping for the networks created in the prerequisites.

The **dcnm-mgmt** network provides connectivity (SSH, SCP, HTTP, HTTPS) to the Cisco DCNM Open Virtual Appliance. In the **Destination Network** column, associate the network mapping with the port group that corresponds to the subnet associated with the Cisco DCNM management network.

a. Map the enhanced-fabric-mgmt network to the port group that connects to the management network of switches.

b. If you are deploying more than one OVA for HA functionality, the following criteria must be met:

   – Both Appliances should have their management access (eth0) and enhanced fabric management (eth1) interfaces in the same subnet.

   – Both Appliances should be deployed with the same administrative password. This is to ensure that both Open Virtual Appliances are duplicates of each other for application access.

Step 16 Click **Next**.

Note Do not select **Power on after deployment**.

Step 17 Click **Finish**.

The **Deploying DCNM Virtual Machine Template** appears and the virtual hardware is created.

After the VM is deployed, a **Deployment Completed Successfully** message appears.

Step 18 Right click on the VM and select **Edit Settings**.

Step 19 Navigate Hardware and click **Add**.

Step 20 Select a **Hard Disk** and click **Next**.

Step 21 With the default option set to **Create a new virtual disk**, click **Next**.

Step 22 In the Disk Size field, enter **100GB**.

Step 23 Select thick or thin provisioning based on the requirement.

Step 24 Click **Next**.

Step 25 Select the location as **Store** with the virtual machine.

Step 26 Retain the default values for Virtual Device Node. Click **Next**.

Note Ensure that you do not select **Mode**.

Step 27 Click **Finish**.

Step 28 You can link the DCNM ISO to the VM by one of the following methods:

- connecting to the ISO Virtual Appliance image on local disk, if the ISO is on the same system as the vSphere client. This must be performed only after the VM is powered on.
- connecting to the host device, if the ISO Virtual Appliance is located on the ESXi host.
- connecting to ISO Virtual Appliance image on datastore, if the ISO is located on the datastore.

Navigate to **Hardware**.

Step 29 Click the **CD/DVD** drive. Select the Datastore ISO File and locate the ISO file.

Step 30 Click **OK**.

Step 31 Power on the Virtual Machine. The operating system is installed.

Step 32 Logon to the VM console in vSphere client using the default credentials

username: root

password: cisco123

Step 33 Run the appmgr CLI to setup the network properties.

The status of all the applications is displayed after the installation is complete.

Example: appmgr CLI to setup network properties

```
[root@dcnm ~]# appmgr setup standalone
Hostname (Fully Qualified Domain Name): dcnm.cisco.com

*** Configuring DCNM Management network ***
IP address  : 10.197.67.57
Subnet Mask  : 255.255.255.192
Gateway   : 10.197.67.1
DNS server  : 72.163.128.140

*** Configuring EFM Management network ***
Do you want to install SAN management features along with LAN? Yes/No [Yes] :
IP address  : 192.168.57.57
Subnet Mask  : 255.255.255.0
DNS server  : 72.163.128.140

*** Administrative settings ***

Management password :
Enter it again for verification:


You have entered these values..

HOSTNAME=dcnm.cisco.com
ETH0_IP=10.197.67.57
ETH0_NM=255.255.255.192
ETH0_GW=10.197.67.1
ETH0_DNS=72.163.128.140
ETH1_IP=192.168.57.57
ETH1_NM=255.255.255.0
ETH1_DNS=0.0.0.0

INSTALL_OPTION=BOTH(LAN+SAN)
Press 'y' to continue installation, 'n' to re-enter values, 'q' to quit [y] y


Installing applications..
done.

appmgr status all


DCNM v10 will only use HTTPS. Insecure access via HTTP is now disabled.
Please use the url https://DCNM-IP-ADDRESS or https://HOSTNAME to launch the DCNM UI.

DCNM Status

 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
1562 root  20  0 3940m 763m 27m S 0.0 9.7 18:28.59 java

LDAP Status
```

```
PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
1208 ldap  20 0 210m 5312 2100 S 0.0 0.1 0:00.02 slapd

TFTP Status

PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
1236 root  20 0 22188 1020 764 S 0.0 0.0 0:00.00 xinetd

DHCP Status

PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
1249 dhcpd  20 0 46336 1212 196 S 0.0 0.0 0:00.00 dhcpd

XMPP Status

PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
1791 root  20 0 1389m 16m 6640 S 0.0 0.2 0:14.15 jabberd

AMQP Status

PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
1326 rabbitmq  20   0 1103m  71m 2704 S  0.0  0.9   8:14.46 beam.smp
```

Installing the DCNM ISO Virtual Appliance on KVM

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

Step 1 Unzip and extract **dcnm-va-ovf-kvm-files.<10.1.1>.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.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.

```
sudo virsh define dcnm-kvm-vm.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

Note Cisco recommends that you use storage size of 100GB for Programmable Fabric deployments.

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 created. Refer to Prerequisites for DCNM ISO Virtual Appliance, page 2-2.

Step 19 Power on the Virtual Machine.

The operating system is installed.

The VM is powered off automatically after the OS installation.

Step 20 Navigate to **Edit > Virtual Machine Details > Show virtual hardware details** and edit the Virtual Machine.

Step 21 Click **IDE CDROM** in the Hardware section and disconnect the ISO from the VM.

This is to ensure that the next time the VM boots, it boots from the hard disk instead of CD/DVD.

Step 22 Click **OK**.

Step 23 Power on the Virtual Machine.

Step 24 Logon to the VM console in Virtual Machine Manager using the default credentials

username : root

password : cisco123

Step 25 Run the **appmgr** command to setup the network properties. For more information, see the example below.

The status of all the applications is displayed after the installation is complete.

Example: appmgr CLI to setup network properties

```
[root@dcnm ~]# appmgr setup standalone
Hostname (Fully Qualified Domain Name): dcnm.cisco.com
*** Configuring DCNM Management network ***
IP address : 10.197.67.57
Subnet Mask : 255.255.255.192
Gateway : 10.197.67.1
DNS server : 72.163.128.140
*** Configuring EFM Management network ***
Do you want to install SAN management features along with LAN? Yes/No [Yes] :
IP address : 192.168.57.57
Subnet Mask : 255.255.255.0
DNS server : 72.163.128.140
*** Administrative settings ***
Management password :
Enter it again for verification:
```

```
You have entered these values..
HOSTNAME=dcnm.cisco.com
ETH0_IP=10.197.67.57
ETH0_NM=255.255.255.192
ETH0_GW=10.197.67.1
ETH0_DNS=72.163.128.140
ETH1_IP=192.168.57.57
ETH1_NM=255.255.255.0
ETH1_DNS=0.0.0.0
Press 'y' to continue installation, 'n' to re-enter values, 'q' to quit [y] y
Installing applications..
done.

appmgr status all

DCNM v10 will only use HTTPS. Insecure access via HTTP is now disabled.
Please use the url https://DCNM-IP-ADDRESS or https://HOSTNAME to launch the DCNM UI.

DCNM Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== ===== === == ==== === === = ==== ===== ====== =======
1562 root 20 0 3940m 763m 27m S 0.0 9.7 18:28.59 java

LDAP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== ===== === == ==== === === = ==== ===== ====== =======
1208 ldap 20 0 210m 5312 2100 S 0.0 0.1 0:00.02 slapd

TFTP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== ===== === == ==== === === = ==== ===== ====== =======
1236 root 20 0 22188 1020 764 S 0.0 0.0 0:00.00 xinetd

DHCP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== ===== === == ==== === === = ==== ===== ====== =======
1249 dhcpd 20 0 46336 1212 196 S 0.0 0.0 0:00.00 dhcpd

XMPP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== ===== === == ==== === === = ==== ===== ====== =======
1791 root 20 0 1389m 16m 6640 S 0.0 0.2 0:14.15 jabberd

AMQP Status
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
=== ===== === == ==== === === = ==== ===== ====== =======
1326 rabbitmq 20 0 1103m 71m 2704 S 0.0 0.9 8:14.46 beam.smp
```

Installing the DCNM ISO Virtual Appliance on N1110

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

Step 1 Launch the CSP 2100 UI and navigate to **Configuration > Repository > Select > Upload**.

Step 2 Select **dcnm-csp2100.iso**. Click **Upload**.

Step 3 On the Configuration tab, click **Services > Create**.

The Service Creation page appears.

Step 4 In the service creation panel, enter the following parameters.

a. Enter the **Service Name**.

b. Select the **Target Host Name**.

c. Select the **HA Host Name.**

The default value is none.

d. Select the image that you have uploaded in Step 1.

After you select the image, 2 vNIC's and Resource Config tab is populated with resource (4core, 80GB, 8192MB RAM) information.

e. In the vNIC tab, navigate to **vNIC1 > Network Name > Internal/External Network**.

On the Select Network Interface panel, select the physical network interface.

f. Navigate to **vNIC2 > Network Name > Internal/External Network**.

On the Select Network Interface panel, select the physical network interface.

g. The Resource Config tab displays the minimum resources to deploy the Cisco DCNM Application. You can modify the resources to have higher resource values, based on your requirement.

h. (Optional) On the **Storage Config** tab, add the storage details.

i. (Optional) On the VNC Password tab, enter **VNC password** to access the virtual machine VNC Console.

j. (Optional) Enter the **Crypto Bandwidth** and **Serial Port** details.

k. Click **Save**.

Step 5 Select the image which is uploaded to enter additional information.

Upon selection of the image in Step 4d., **Additional Image Info Required** window appears.

a. In the HA Role for the appliance, enter **Primary** or **Secondary**.

b. Enter fully qualified **hostname**.

For example: **dcnm.cisco.com**.

c. Enter **Management IP address**, **Subnet Mask**, **Gateway** and **DNS** for DCNM Management.

d. Enter **Default Gateway IP address**, **Subnet Mask** and **DNS** for Spine Management.

e. From the **Enable DFA for DCNM** drop-down, choose "**Y**" or "**N**"

f. Enter **Administrative Password**.'

g. Click **Save**.

Step 6 Click **Deploy** to deploy the virtual machine with the above configured values.

Step 7 Navigate to **Configuration > Services** to check the status of deployment.

The values of Power/State will show **on/deployed**.

Step 8 Click on the **Console** icon to launch the VM console.

Virtual machine VNC console appears.

Please input the VNC password entered earlier in step 3 and click connect. If no password is entered, just click on connect to access the Console.

Step 9 Enter the **VNC password**, provided in Step i, and click **Connect**.

If no password was entered earlier, click **Connect** to access the Console.

Step 10 After the OS boots, launch the CLI using the credentials:

```
username: root
password: cisco123
```

Step 11 Install Cisco DCNM by using one of the following commands:

- **appmgr setup standalone**

  Enter the following parameters:

```
Hostname (Fully Qualified Domain Name): dcnm.cisco.com
    *** Configuring DCNM Management network ***
    IP address: 10.197.67.57
    Subnet Mask: 255.255.255.192
    Gateway: 10.197.67.1
    DNS server: 72.163.128.140
    *** Configuring EFM Management network ***
    IP address: 192.168.57.57
    Subnet Mask: 255.255.255.0
    DNS server: 72.163.128.140
    *** Administrative settings ***
    Do you want to install DFA applications True/False [True]: True
    Management password:
    Enter it again for verification:
```

- **appmgr setup standalone -i silent -f *<filename>***

  This command reads the parameters from the file located at `/root/packaged-files/properties/fabric-installer.properties`

  The installation will proceed with the parameters provided in the file.

- **appmgr setup standalone -i silent -f <filename>**

  This command allows you to specify the filename which contains the user-defined parameters. The installation will proceed with the parameters provided in the file.

Step 12 Enter **Y** to proceed with the installation.

Enter **N** to modify the parameters.

Step 13 After the successful installation verify if Cisco DCNM is operational, by using the **appmgr status all** command.

Note Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. For more information, see Setting the Timezone for Cisco DCNM Virtual Appliances, page 3-18.

Setting the Timezone for Cisco DCNM Virtual Appliances

After installing Cisco DCNM Virtual Appliances, before performing any operations, ensure that you set the timezone on the DCNM Appliance. This will ensure that the system-generated reports and other statistics show the correct date as per your timezone.

Perform the following procedure to set the timezone.

Step 1 On the Cisco DCNM Virtual appliance, save the current timezone by using the following command:

mv /etc/localtime /etc/localtime.bak

Step 2 Update the current timezone to your desired timezone, using the following command:

ln -s /usr/share/zoneinfo/<<country_name>>/<<state_name>> /etc/localtime

Step 3 Check and confirm if the timezone if updated using the following command: --- date is the command they need to run.

date

Step 4 Restart the Cisco DCNM, using the **appmgr restart dcnm** command.

Note If you have installed Cisco DCNM Native HA appliance, restart using the appmgr restart ha-apps command.

DCNM installation without Enhanced Fabric Management capabilities

This section details the tasks for DCNM installation without Enhanced Fabric Management capabilities based on the installers. This section contains the following:

- Windows Installation, page 3-19
- Linux RHEL Server Installation, page 3-20
- DCNM Open Virtual Appliance (OVA) Installation, page 3-25
- ISO Virtual Appliance Installation on KVM, page 3-25
- DCNM OVA in High Availability/Federation, page 3-26

Windows Installation

You can install DCNM on the either Windows XP, Windows 2008, Windows 7 and Windows 2012.

- For instructions on how to install DCNM for Windows 2012, see Installing Cisco DCNM on Windows 2012.
- For other versions of Windows, see Installing Cisco DCNM on Windows and Linux using the GUI.

Prerequisites

For information about the prerequisites before you begin the installation, see the following sections:

- General Prerequisites for Installing the Cisco DCNM on Windows and Linux, page 2-3
- Prerequisites for Windows Installer, page 2-16.

Installing Cisco DCNM on Windows 2012

Perform the following steps to install DCNM:

DETAILED STEPS

Step 1 Right click on the installer and select **Troubleshoot compatibility**. to troubleshoot issues if your system is not compatible with the installer.

Step 2 Select **Try recommended settings**. Click **Next** to test run the program using recommended compatibility settings.

Step 3 After settings are applied, click **Next**.

Cancel the installation process at that point

Step 4 Select **Save the settings for this program** and close the troubleshooter.

Step 5 Invoke the installer.exe and install the DCNM.

Linux RHEL Server Installation

Perform the following steps to install DCNM:

Prerequisites

For information about the prerequisites before you begin the installation, see the following sections:

- General Prerequisites for Installing the Cisco DCNM on Windows and Linux, page 2-3
- Prerequisites for Linux RHEL Server, page 2-17.

Installing Cisco DCNM on Windows and Linux using the GUI

Note Before upgrading or uninstalling the Cisco DCNM or Device Manager, ensure that all the instances are shut down.

If the PostgreSQL database is not present on your computer, the installer installs PostgreSQL9.4. You can change the default credentials after the installation is complete.

Note When installing or upgrading Cisco DCNM SAN federation with same or different subnets, Cisco DCNM-SAN services do not start at the end of the DCNM installation. You must start the Cisco DCNM services manually using the shortcuts available under ../dcnm/fm/bin or when asked by installer in the end of the installation.

Cisco DCNM has only 64-bit executable. 32-bit executable is not supported for Cisco DCNM.

Note Before you execute the installer, ensure that you create a database user with a user role and assigned schema. If you are using the Oracle database, a mapped schema is already created. If you are using a PostgreSQL database, ensure that you create a new schema with the exact string as the new username and that the new user is the schema owner.

DETAILED STEPS

Step 1 Go to the directory where you downloaded the Cisco DCNM software and run the dcnm-*release.exe* file.

After the installer prepares the installation, the Introduction step appears in the Cisco DCNM installer window.

Step 2 Click **Next** when the Introduction step appears in the Cisco DCNM installer window after the installer prepares the installation.

Step 3 Click **Next** when the Please Read Before Continuing information appears in the Cisco DCNM installer window.

Step 4 Enter the following when the Choose Install Folder step appears in the Cisco DCNM installer window:

a. (Optional) If you want to add the server to the existing federation, check the **Add Server to an existing server federation** checkbox.

b. (Optional) If you want to change the default installation folder, enter or choose the desired installation folder.

c. Click **Next**.

As part of the Cisco DCNM installation, one of the following options are displayed according to your system requirements.

- New installation—The installer installs Cisco DCNM-SAN, and SMI-S for the first time.

Note Cisco DCNM-SAN federation can be deployed across nodes and databases in the different subnets.

- Upgrade Cisco DCNM-SAN—The installer discovered a previous version of Cisco DCNM-SAN. The installer upgrades to the latest version of DCNM-SAN, and installs the SMI-S agent.
- Upgrade Cisco DCNM-SAN—The installer discovered a previous version of Cisco DCNM-SAN. The installer upgrades to the latest version of Cisco DCNM-SAN and SMI-S agent.

The Database Options step appears in the Cisco DCNM installer window. You can use an existing PostgreSQL installation or an existing Oracle installation. If PostgreSQL is not installed on the server system, you can use the Cisco DCNM installer to add a PostgreSQL installation.

Step 5 If you want to install PostgreSQL, do the following:

Note When you install PostgreSQL with Cisco DCNM, the database admin username and password is the same as the database username and password appended with 123. For example, if your database username is dcnmuser, the admin username is dcnmuser123. Similarly, if the database password is dcnmtest, the admin password is dcnmtest123.

Note

- On Linux—If you want install PostgreSQL, ensure you have a non-root privileged user called postgres in the server. If you have not created a non-root privileged user, the installer will prompt you to create one and if you skip entering the details, the installer will automatically create a user called postgres with non-root privileges.
- On Linux—To allow remote access to the database, modify the pg_hba.conf file and restart the postgres service using the command <*dbroot*>/bin/pg_ctl.

a. Next to RDBMS, click **Install PostgreSQL**.

If your server system runs RHEL, the System User dialog box appears.

b. (RHEL only) In the System User dialog box, enter the username for the user account that should be used to run the PostgreSQL software. This user account should not have administrator or root privileges.

c. In the DCNM DB User field, enter the username that Cisco DCNM-SAN should use to access the database. The default username is dcnmuser. The installer creates the user account that you specify.

d. In the DCNM DB Password field, enter the password for the database user account that you specified.

e. In the Confirm DCNM DB Password field, reenter the password for the database user account that you specified.

f. (Optional) If you want to change the default PostgreSQL database installation folder, in the Install Location field, enter or choose the desired installation folder.

Step 6 If you want to use an existing relational database management system (RDBMS) installation, do the following:

a. Next to RDBMS, click one of the following:

- **Use existing PostgreSQL 8.1/8.2/8.3/9.4**
- **Use existing Oracle 10g/11g**
- **Use Oracle RAC**

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, owned by the same username. When there are 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”.

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

b. If the DB URL field does not have the correct URL to the database, enter the correct URL.

Note The database is not automatically created. You must manually create the database. A valid database URL is required to create a database schema and connect to it.

c. In the DCNM DB User field, enter the username that Cisco DCNM should use to access the database.

d. In the DCNM DB Password field, enter the password for the database user account that you specified.

e. If user selects “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.

Step 7 Click **Next**.

The Configuration Options step appears in the Cisco DCNM installer window.

Step 8 If you want to use an existing Oracle 10g/11g RAC, do the following:

a. Next to RDBMS, click the following:
   - Use the existing Oracle 10g/11g RAC

The Oracle RAC configuration dialog box appears.

b. In the Service Name field, enter the service name of the Oracle RAC server.

c. Enter a maximum of three host IP addresses. Click **OK**. The DB URL is generated.

Step 9 In the Configuration Options dialog box, do the following:

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

a. 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.

b. 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.

Step 10 Click **Next**.

The Local User Credentials step appears in the Cisco DCNM installer window.

Step 11 In the Local 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.

Step 12 In the Password field, enter a password for the user, and in the Confirm Password field, reenter the password.

Note The password can contain a combination of alphabets, numeric, and special characters. The only chars that are not allowed in the DCNM password for windows/linux platforms are:
<SPACE> &$% single and double quotes
And the rest are all allowed:
! @ # ^ * - + = : ; ?,. / ~ ` \ | < > ()

Step 13 If you want to create a SAN admin user, do the following:

a. Check the **Create SAN Admin User** check box.

a. In the Local Admin Username field, enter a name for a Cisco DCNM-SAN server user. The installer creates the Cisco DCNM-SAN server user and assigns the Administrator role to it.

b. In the Password field, enter a password for the user, and in the Confirm Password field, reenter the password.

Step 14 Click **Next**.

The Authentication Settings step appears in the Cisco DCNM installer window.

Choose the authentication method that the Cisco DCNM server should use to authenticate users who log into 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 15 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 tertirary servery 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**.

Step 16 Click **Next**.

If you are using Microsoft Windows, the installer asks you to specify a shortcut to the application. If you are using RHEL, the installer asks you to specify a link folder.

Step 17 Choose the shortcut or link options that you want.

Step 18 (Optional) 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.

Step 19 Click **Next**.

The Pre-Installation Summary step appears in the Cisco DCNM installer window.

Step 20 Carefully review the summary of your choices. If you need to change anything, click **Previous** until the Cisco DCNM installer window displays the step that you need to change, and then return to the applicable preceding step.

Step 21 Click **Next** when you are ready to install the Cisco DCNM server software.

The installer installs the Cisco DCNM server software.

The Installing Cisco DCNM installer window appears.

Step 22 Choose whether you want to start the Cisco DCNM server now. If you start the Cisco DCNM server now, a splash screen appears while the server starts.

The Install Complete step appears in the Cisco DCNM installer window. The Cisco DCNM instance ID number is displayed.

Step 23 (Optional) If you plan to order licenses for Cisco DCNM, record the Cisco DCNM instance ID number. The licensing process requires that you enter that number.

Note You can begin using Cisco DCNM without a license but some features are not available unless you purchase and install a license and apply the license to managed devices that you want to use licensed features with.

Step 24 Click **Done**.

Copying Certificates

When you add a new Cisco DCNM instance to an existing federation or cluster, ensure you copy fmtrust.jks and fmserver.jks certificate files manually from any one of the nodes present in the Cisco DCNM federation or cluster.

You should get the certifcate files under the following folders:

- **On Microsoft Windows**—<*DCNM install folder*>\dcm\jboss-4.2.2.GA\server\fm\conf
- **On Linux**—<*DCNM install folder*>/dcm/jboss-4.2.2.GA/server/fm/conf

In the new node, you should copy the certifcate files under the following folders:

- **On Microsoft Windows**—<*DCNM install folder*>\dcm\jboss-4.2.2.GA\server\fm\conf
- **On Linux**—<*DCNM install folder*>/dcm/jboss-4.2.2.GA/server/fm/conf

Note Ensure you restart the Cisco DCNM servers after copying the certificate files.

Collecting PM Data

To setup a shared rrd path to collect PM data, perform these steps:

Step 1 Locate the server.properties file under C:\Program Files\Cisco Systems\dcm\fm\conf.

Step 2 Add the pm.rrdpath property file information to the server.properties file. For example, add the server location that needs to be accessible from the DCNM server.

Step 3 Save the server.properties file.

Step 4 Restart the Cisco DCNM-SAN server.

Once PM server is ready, the new shared location will be used by the PM server to save .rrd files. PM will create a new directory called db under pm. Ensure you do not open or change these .rrd files as PM server is actively writing into the .rrd files.

DCNM Open Virtual Appliance (OVA) Installation

For instruction on how to install DCNM Open Virtual Appliance in non-Programmable Fabric mode, see DCNM Open Virtual Appliance Installation in Programmable Fabric mode, page 3-2.

Note During installation, when you enter the OVF properties in vSphere client, do not enter any values for the parameters under the section "**Enhanced Fabric Management Network**.

ISO Virtual Appliance Installation on KVM

For instruction on how to install DCNM ISO Virtual Appliance in non-Programmable Fabric mode, see DCNM ISO Virtual Appliance Installation, page 3-9.

Note During the installation, when you configure the appliance using the appmgr setup standalone command, ensure that to provide the default values for EFM Management network as like below

```
*** Configuring EFM Management network ***
IP address : 0.0.0.0
Subnet Mask : 0.0.0.0
DNS server : 1.1.1.1
```

Configuring Media Controller for IP Fabric

Beginning from Release 10.1(2), Cisco DCNM OVA or ISO installation allows you to monitor and control IP Fabric for Cisco Nexus 9000 Series Switched through Cisco DCNM Web Client. This feature is available if you have enabled the Media Controller feature explicitly, after the Cisco DCNM OVA/ISO installation is complete.

Note This feature can be enabled only on the DCNM Open Virtual Appliance or DCNM ISO Virtual Appliance Installation.

To enable the Media Controller feature on the Cisco DCNM Web Client, perform the following.

Step 1 Log in to the SSH terminal of the Cisco DCNM OVA/ISO.

Step 2 Stop all the applications by using the following command:

appmgr stop dcnm

Step 3 Enable the Media Controller on the Cisco DCNM Web Client, by using the following command:

appmgr set-mode media-controller

Logon to Cisco DCNM **Web Client > Media Controller** to perform various operations on the IP Fabric, for Cisco Nexus 9000 Series Switches.

Note To bring up the devices from the basic configuration using POAP, you must define the templates and publish the POAP definition through Cisco DCNM **Web Client > Configure > Deploy > POAP**.

DCNM OVA in High Availability/Federation

To achieve non-Programmable Fabric Federation (HA for Non-Enhanced Fabric mode) that are run on the Cisco DCNM Open Virtual Appliance. Deploying a federation includes one primary server and one and more secondary servers. This procedure provides the general steps that you must take to deploy a federated Cisco DCNM environment.

Note XMPP takes the first server from the Oracle RAC URL. If the first server is down, then swap the server IP address.

This section includes:

- Configuring First Node, page 3-27
- Configuring Federated Nodes, page 3-28
- Application or Server Failover, page 3-28

Prerequisites

This section contains the following topics that describe the prerequisites for obtaining a Non DFA Federation environment. OVA/ISO should be deployed in a Non-Enhanced Fabric mode.

For more information, see Prerequisites for Cisco DCNM Open Virtual Appliance HA, page 7-2.

Configuring First Node

Perform the following procedure to configure the Cisco DCNM non-Unified appliance as first node.

Step 1 Stop all the applications by using the following command:

appmgr stop dcnm

Step 2 Log in to the SSH terminal of the Open Virtual Appliance that you want designate as the first node, by using the following command:

appmgr setup ha-type first-node

The following prompt appears.

****

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

Please make sure that you have the following

1. An Oracle Database with a user defined for DCNM.
2. A repository with NFS capabilities.
3. An NTP server for time synchronization.

****

Step 3 Choose **Y** to continue.

A prompt for the Database for DCNM appears.

Step 4 Configure the database.

a. Enter the database URL to configure the database.

The script uses a JDBC thin driver. Therefore, enter the URL in the same format.

b. Enter the database password.

c. Enter the database password again for verification.

The script runs a sample query from the database to validate the details entered. The Cisco DCNM schema and related data are loaded after the data is validated.

d. Enter the database username for DCNM tables.

e. Enter the database password for DCNM tables.

f. Enter the database password again for verification.

Step 5 Configure the Repository and NFS.

Note A repository server in the non-Unified network must have NFS capability.

a. Enter the SCP/NFS repository IP address.

b. Enter the location for the NFS Exported file.

The system performs a test mount to ensure that the server is reachable. The system also performs a test-write to ensure the exported directory is writable

Step 6 Enter an NTP server for time synchronization.

A summary of the details entered will be displayed.

Step 7 Choose **Y** to continue.

Choose **N** to edit or update the details.

Step 8 After the high availability configuration is complete, check the role by using the following command.

appmgr show ha-role

This node is part of HA Federation.

Configuring Federated Nodes

Perform the following procedure to configure the Cisco DCNM non-Unified appliance as a federated node.

Step 1 Log in to the SSH terminal of OVA-B.

Step 2 Configure the federated node by using the following command:

appmgr setup ha-type federated-node

Step 3 Choose Y to continue.

Step 4 Enter the existing Federated server IP (eth0 IP) address.

Step 5 Enter the root password of the peer.

After confirmation, the OVA-B is configured as a federated node, and the following message is displayed.

appmgr start dcnm in first-node and then federated-node

Application or Server Failover

Automatic failover option enabled in the Cisco DCNM UI. This process ensures that if the DCNM that is running on OVA-A fails, all the fabrics and shallow-discovered LANs managed by DCNM-A are managed by DCNM-B automatically after a given time interval (usually about 5 minutes after the failure of DCNM on OVA-A).

DCNM Native HA Installation

The native HA is only supported on DCNM appliances with ISO or OVA installation. Unlike HA mechanisms, it doesn't require any external dependencies like an Oracle database or a shared NFS filesystem.

By default, Cisco DCNM is bundled with an embedded PostgreSQL database engine. 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 will take over with the same database data and resume the operation.

Perform the following task to setup Native HA for DCNM.

Step 1 Deploy two DCNM virtual appliances (OVA/ISO).

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

If both eth0 and eth1 interfaces are in the same subnet, edit the /etc/sysctl.conf file for DCNM ISO Virtual appliance Native HA installation on both active and standby nodes for both the appliances, as follows:

- Change the value of net.ipv4.conf.default.rp_filter from **1** to **2**.
- Add **net.ipv4.conf.all.rp_filter = 2** to the sysctl.conf file.

Save and close the file. On the SSH terminal, execute the **sysctl --system** command.

Step 2 Wait for all the applications to be operational.

Use the **appmgr status all** command to check the status of the applications.

```
dcnm1# appmgr status all
dcnm2# appmgr status all
```

Step 3 Use the **appmgr stop all command** to shut down all applications on both the Cisco DCNM applications.

Use the **appmgr stop all** command to check the status of the applications.

```
dcnm1# appmgr stop all
dcnm2# appmgr stop all
```

Step 4 On the active node, edit the **ha-setup.properties** file, by using the following command:

```
dcnm1# vi /root/packaged-files/properties/ha-setup.properties
```

Step 5 Edit the active node parameters and enter appropriate values.

Note Please refer to Example for DCNM Native HA Installation, page 3-30 section for more information.

Step 6 Install NativeHA on the active node with the following command:

```
dcnm1# appmgr setup native-ha active
```

Step 7 On the standby node, check if the below property values are updated in the ha-setup.properties file, by using the following command:

```
dcnm2# vi /root/packaged-files/properties/ha-setup.properties
```

Step 8 Verify if the secondary node parameters are updated.

Note To setup Cisco DCNM Native HA successfully, it is important to use valid FQDN as hostname for both hosts while installing DCNM OVA/ISO. After installation, you must be able to ping the FQDN for both hosts. If the ping is not successful, the Native HA setup may fail.

Step 9 If it is auto-populated and validated, install Native HA on the stand-by node, using the following command:

```
dcnm2# appmgr setup native-ha standby
```

On the active node, all the applications, excluding DHCP will be started. On the standy node only LDAP and AMQP will be enabled.

Launch the DCNM on the active node and enter the **POAP IP Range** on the Cisco DCNM **Web Client > Configure > POAP > DHCP Scope**. DHCP will be started automatically on both the active and standby nodes.

DCNM, XMPP and TFTP are automatically started on the standby node immediately after the active node stops working.

Example for DCNM Native HA Installation

The example in this section considers the following parameters and shows how to install DCNM Native HA.

Parameter	Active	Standby	Virtual IP (VIP)
Eth0 IP	1.1.1.1/24	1.1.1.2/24	1.1.1.3/24
Eth1 IP	2.2.0.1/16	2.2.0.2/16	2.2.0.3/16
Hostname (FQDN)	dcnm1.cisco.com	dcnm2.cisco.com	dcnm3.cisco.com

On the active node, edit the property file by using the following command:

dcnm1# vi /root/packaged-files/properties/ha-setup.properties

```
# NODE_ID refers the role of this node in HA.
# Example:  NODE_ID=1 (For Active)
# Example:  NODE_ID=2 (For standby, though typically, standby gets updated during active
setup)
NODE_ID=1

# IPv4 address of the peer
# Example : PEER_ETH0_IP=1.1.1.2
PEER_ETH0_IP=1.1.1.2

# IPv4 address of the Virtual IP address on the DCNM management network (eth0 network)
# Example : VIP_ADDRESS=1.1.1.3
VIP_ADDRESS=1.1.1.3

# Network prefix of Virtual IP address on DCNM management network, example : for a
255.255.255.0 network mask, enter the prefix as 24
# Example : VIP_PREFIX=24
VIP_PREFIX=24

# IPv4 address of the Virtual IP address on the Enhanced Fabric management network (eth0
network)
# Example : VIP1_ADDRESS=2.2.2.3
VIP1_ADDRESS=2.2.0.3

# Network prefix of Virtual IP address on Enhanced Fabric management network, example :
for a 255.255.255.0 network, enter the prefix as 24
# Example : VIP1_PREFIX=24
VIP1_PREFIX=16

# Fully Qualified Domain name for the Virtual IP
# Example : VIP_FQDN=dcnm.xy.com
VIP_FQDN=dcnm3.cisco.com
```

On the standby node, check if the property values are updated in /root/packaged-files/properties/ha-setup.properties

dcnm2# vi /root/packaged-files/properties/ha-setup.properties

```
# NODE_ID refers the role of this node in HA.
# Example:  NODE_ID=1 (For Active)
# Example:  NODE_ID=2 (For standby, though typically, standby gets updated during active
setup)
NODE_ID=2

# IPv4 address of the peer
# Example : PEER_ETH0_IP=1.1.1.2
PEER_ETH0_IP=1.1.1.1

# IPv4 address of the Virtual IP address on the DCNM management network (eth0 network)
# Example : VIP_ADDRESS=1.1.1.3
VIP_ADDRESS=1.1.1.3

# Network prefix of Virtual IP address on DCNM management network, example : for a
255.255.255.0 network mask, enter the prefix as 24
# Example : VIP_PREFIX=24
VIP_PREFIX=24

# IPv4 address of the Virtual IP address on the Enhanced Fabric management network (eth0
network)
# Example : VIP1_ADDRESS=2.2.2.3
VIP1_ADDRESS=2.2.0.3

# Network prefix of Virtual IP address on Enhanced Fabric management network, example :
for a 255.255.255.0 network, enter the prefix as 24
# Example : VIP1_PREFIX=24
VIP1_PREFIX=16

# Fully Qualified Domain name for the Virtual IP
# Example : VIP_FQDN=dcnm.xy.com
VIP_FQDN=dcnm3.cisco.com
```

Note The Virtual IP (VIP) is seen on the active node. You can verify VIP by using the **ip address show** command.

Running Cisco DCNM Behind a Firewall

For Windows PCs running Cisco DCNM-SAN, Device Manager, behind a firewall, certain ports need to be available.

By default, Cisco DCNM-SAN Client and Device Manager use the first available UDP port for sending and receiving SNMP responses. The UDP SNMP trap local ports are 1162 for Cisco DCNM-SAN, and 1163 or 1164 for Device Manager. Cisco DCNM-SAN Server also opens TCP RMI port 4447.

In DCNM Release 5.0(1) or later releases, you can select the UDP port that Fabric Manager Client or Device Manager uses for SNMP responses by uncommenting the following statement:

- On a Windows desktop, uncomment the following in the FabricManager.bat or DeviceManager.bat file in the C:\Program Files\Cisco Systems\MDS9000\bin directory:

  ```
  rem JVMARGS=%JVMARGS% -Dsnmp.localport=9001
  ```

- On a UNIX desktop, uncomment the following in the FabricManager.sh or DeviceManager.sh file in the $HOME/.cisco_mds9000/bin directory:

```
# JVMARGS=$JVMARGS -Dsnmp.localport=9001
```

From Cisco DCNM Release 6.3(1), DCNM San Client initiates communication with DCNM San Server on the following ports:

- 4447 for Java Remoting,
- 5457 and 5455 for Java Messaging Service.

DCNM proxy services use a configurable TCP port (9198 by default) for SNMP communications between the DCNM San Client or Device Manager and DCNM Server.

The DCNM San Server component requires two predictable TCP ports to be opened on the firewall for an incoming connection:

- 4447 for Server
- 9100 for Server Data

Note The Fabric Manager Client can connect to the server only if these two ports are open. Other TCP ports connected to DCNM San Client are initiated by the server, which is behind the firewall.

The following table lists all ports used by Cisco DCNM applications:

Communication Type	Port(s) Used
Used by All Applications	
SSH	Port 22 (TCP)
Telnet	Port 23 (TCP)
HTTP	Port 80 (TCP)
SLAPd	Port 636 (TCP)
LDAP	Port 389 (TCP)
XMPP/Jabber	Port 7400
TFTP	Port 69 (UDP)
RabbitMQ	Port 4369 (TCP)
Open AMQP	Port 5672 (TCP)
SNMP	Port 161 (UDP/TCP) **Note** DCNM configured via server.properties to use TCP will use TCP port 161 instead of UDP port 161.
Syslog	Port 514 (UDP)
Used by Cisco DCNM-SAN Server and Performance Manager	
SNMP_TRAP	Port 2162 (UDP)
SNMP	Picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. Can be changed in server.properties.
Java Remoting	4447
Java Messaging	5457, 5455
Used by Cisco DCNM-SAN Client	

Communication Type	Port(s) Used
SNMP	Picks a random free local port (UDP) if SNMP proxy is enabled. Can be changed with the client -Dsnmp.localport option.
Used by Device Manager	
SNMP_TRAP	Picks a free local port between 1163 and 1170 (UDP).
SNMP	Picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. Can be changed in **server.properties**.

The following table lists all the ports and descriptions:

Port(s) Used/Type	Service Descriptor	Service Name	Attribute Name	Description
80 or 443	Standalone/configuration/standalone-san.xml	JBoss http (or https) port	http (or https) service for webclient, SOAP and REST API	http (or https) service for webclient, SOAP and REST API
4447	Standalone/configuration/standalone-san.xml	jboss:service=Remoting	Remoting Service Port	This port is for JNDI-based naming services. The client look up this port for JNDI-binding objects and resources.
5455 5457	Standalone/configuration/standalone-san.xml	Messaging Service	Unified Invocation Layer for JMS	This port is used for JMS services.