Cisco DCNM OVA Installation Guide, Release 7.x

April 10, 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Text Part Number: OL-30761-01

CONTENTS

Preface v

Obtaining Documentation and Submitting a Service Request ii-viii

ii-viii

Overview 1-1

Information about Cisco Data Center Network Manager 1-1

Installing Cisco DCNM OVA Management Software 2-1

Information About the Cisco DCNM OVA 2-1

Cisco DCNM OVA and Cisco Dynamic Fabric Automation 2-1

Installing the Cisco DCNM OVA 2-2

Verifying Prerequisites 2-3

Downloading the OVA File 2-3

Deploying the OVA as an OVF Template 2-4

Deploying Virtual Machines 2-7

Configuring the Oracle Database for DCNM 2-8

Upgrading Cisco DCNM 7.0(1) to Version 7.0(2) 2-9

Migrating Cisco DCNM with a Local PostgreSQL Database and an External Oracle Database 2-9

Migrating Cisco DCNM in a High Availability Environment 2-10

Managing Applications After the DCNM OVA Deployment 3-1

Cisco DCNM OVA Applications 3-1

Application Details 3-2

Network Management 3-3

Network Services 3-3

Configuring Connectivity with DCNM 3-3

Cisco Prime Network Services Controller Adapter Manager Command-Line Interface 3-5

Config Profiles 3-5

Orchestration 3-6

Device Power On Auto Provisioning 3-7

Group Provisioning of Switches 3-7

Managing Applications 3-8

Verifying the Application Status after Deployment 3-8
Stopping, Starting, and Resetting Applications 3-9
XMPP User and Group Management 3-9
Importing SSL Certificates 3-11
Backing Up Cisco DCNM and Application Data 3-12
Backing Up Cisco DCNM 3-13
Backing Up Application Data 3-13
Using Scripted Backups for Backing Up Application Data 3-13
Restoring Applications 3-14

Managing Applications in a High-Availability Environment 4-1
Information About Application Level HA in the Cisco DCNM OVA 4-1
Automatic Failover 4-2
Manually Triggered Failovers 4-2
Prerequisites for Cisco DCNM OVA HA 4-2
Deploying Cisco DCNM OVAs 4-3
Creating an NFS/SCP Repository 4-3
Availability of Virtual IP Addresses 4-4
Installing an NTP Server 4-4
Application High Availability Details 4-4
Network Management 4-5
HA Implementation 4-5
RabbitMQ 4-7
HA Implementation 4-7
OpenLightweight Directory Access Protocol 4-8
Using the OVA-Packaged (Local) LDAP Server 4-8
Using the Remote LDAP Server 4-9
DCHP HA 4-9
DHCP POAP 4-9
DHCP Autoconfiguration 4-9
Changing DHCP Scope Configurations 4-10
Repositories 4-10
XMPP 4-10
Configuring DCNM OVA HA 4-10
Configuring the Active Peer 4-10
Configuring the Standby peer 4-12
Starting Applications in the Active Peer 4-14
Starting Applications in the Standby Peer 4-14
Starting DHCP in an HA Setup 4-14

Preface

This preface describes the audience, organization, and conventions of the *Cisco DCNM 7.0 OVA Installation Guide*. It also provides information on how to obtain related documentation.

This preface includes the following topics:

- Audience, page v
- Document Conventions, page v
- Document Conventions, page v
- Related Documentation, page vi
- Obtain Documentation and Submit a Service Request, page viii

Audience

This publication is for experienced network administrators who plan to install Cisco Data Center Network Manager (DCNM) Open Virtual Appliance (OVA) to configure, monitor, and maintain applications that provide a central point of management for Cisco Dynamic Fabric Automation (DFA). Cisco DFA works with only certain Cisco Nexus products. Consult your Cisco DFA documentation for specific information about products that work with Cisco DFA.

Document Conventions

This document uses the following conventions:

Note Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

In this document, the following shortened names are used:

- Cisco Data Center Network Manager is also referred to as Cisco DCNM.

- Cisco Data Center Network Manager Open Virtual Appliance is also referred to as Cisco DCNM OVA.
- Cisco Dynamic Fabric Automation is also referred to as Cisco DFA.

Related Documentation

This section contains information about the documentation available for Cisco DCNM OVA, Cisco DFA, and for the platforms that Cisco DCNM OVA and Cisco DFA manages.

This section includes the following topics:

- Cisco DCNM Documentation, page vi
- Cisco Nexus 1000V Series Switch Documentation, page vii
- Cisco Nexus 2000 Series Fabric Extender Documentation, page vii
- Cisco Nexus 3000 Series Switch Documentation, page vii
- Cisco Nexus 4000 Series Switch Documentation, page vii
- Cisco Nexus 5000 Series Switch Documentation, page viii
- Cisco Nexus 6000 Series Switch Documentation, page viii
- Cisco Nexus 7000 Series Switch Documentation, page viii
- Cisco Network Services Controller Documentation, page viii
- Cisco Dynamic Fabric Automation Documentation, page viii

Cisco DCNM Documentation

The Cisco DCNM documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

The documentation set for Cisco DCNM includes the following documents:

Release Notes

Cisco DCNM Release Notes, Release 7.x

Cisco DCNM 7.0 Fundamentals Guide

Cisco DCNM 7.0 Fundamentals Guide

Cisco DCNM for LAN Configuration Guides

FabricPath Configuration Guide, Cisco DCNM for LAN, Release 6.x

Interfaces Configuration Guide, Cisco DCNM for LAN, Release 6.x

Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 6.x

Security Configuration Guide, Cisco DCNM for LAN, Release 6.x

System Management Configuration Guide, Cisco DCNM for LAN, Release 6.x

Unicast Configuration Guide, Cisco DCNM for LAN, Release 6.x

Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 6.x
Virtual Device Context Quick Start, Cisco DCNM for LAN, Release 5.x
Web Services API Guide, Cisco DCNM for LAN, Release 5.x

Cisco DCNM for SAN Configuration Guides

System Management Configuration Guide, Cisco DCNM for SAN, Release 6.x
Interfaces Configuration Guide, Cisco DCNM for SAN, Release 6.x
Fabric Configuration Guide, Cisco DCNM for SAN, Release 6.x
Quality of Service Configuration Guide, Cisco DCNM for SAN, Release 6.x
Security Configuration Guide, Cisco DCNM for SAN, Release 6.x
IP Services Configuration Guide, Cisco DCNM for SAN, Release 6.x
Intelligent Storage Services Configuration Guide, Cisco DCNM for SAN, Release 6.x
High Availability and Redundancy Configuration Guide, Cisco DCNM for SAN, Release 6.x
Inter-VSAN Routing Configuration Guide, Cisco DCNM for SAN, Release 6.x
SMI-S and Web Services Programming Guide, Cisco DCNM for SAN, Release 6.x

Cisco Nexus 1000V Series Switch Documentation

The Cisco Nexus 1000V Series Switch documentation is available at the following URL:
http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Cisco Nexus 2000 Series Fabric Extender Documentation

The Cisco Nexus 2000 Series Fabric Extender documentation is available at the following URL:
http://www.cisco.com/en/US/products/ps10110/tsd_products_support_series_home.html

Cisco Nexus 3000 Series Switch Documentation

The Cisco Nexus 3000 Series switch documentation is available at the following URL:
http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

Cisco Nexus 4000 Series Switch Documentation

The Cisco Nexus 4000 Series Switch documentation is available at the following URL:
http://www.cisco.com/en/US/products/ps10596/tsd_products_support_series_home.html

Cisco Nexus 5000 Series Switch Documentation

The Cisco Nexus 5000 Series Switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

Cisco Nexus 6000 Series Switch Documentation

Cisco Nexus 6000 Series Switch Documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps12806/tsd_products_support_series_home.html

Cisco Nexus 7000 Series Switch Documentation

The Cisco Nexus 7000 Series Switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Cisco Network Services Controller Documentation

The Cisco Network Services Controller Documentation is available at the following URL:

http://www.cisco.com/en/US/partner/products/ps13213/tsd_products_support_series_home.html

Cisco Dynamic Fabric Automation Documentation

This Cisco Dynamic Fabric Automation documentation is available at the following URL:

http://cisco.com/en/US/solutions/ns340/ns517/ns224/ns945/dynamic_fabric_automation.html#~Products

Obtain Documentation and Submit a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

CHAPTER 1

Overview

This chapter contains the following section:

- Information about Cisco Data Center Network Manager, page 1-1

Information about Cisco Data Center Network Manager

Cisco Data Center Network Manager (DCNM) is a management system for the Cisco Unified Fabric. It enables you to provision, monitor, and troubleshoot the data center network infrastructure. It provides visibility and control of the unified data center so that you can optimize for the quality of service (QoS) required to meet service-level agreements.

Cisco DCNM provides a comprehensive feature set that meets the routing, switching, and storage administration needs of data centers. Cisco DCNM streamlines the provisioning for the unified fabric and monitors the SAN and LAN components. Cisco DCNM provides a high level of visibility and control through a single web-based management console for Cisco Nexus, Cisco MDS, and Cisco Unified Computing System (UCS) products.

Cisco DCNM also includes Cisco DCNM-SAN and Cisco DCNM-LAN client functionality.

All Cisco DCNM for SAN and Cisco DCNM for LAN product documentation is now published to the Data Center Network Manager listing page on Cisco.com:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_configure.html

CHAPTER 2

Installing Cisco DCNM OVA Management Software

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

- Information About the Cisco DCNM OVA section, page 2-1
- Cisco DCNM OVA and Cisco Dynamic Fabric Automation section, page 2-1
- Installing the Cisco DCNM OVA section, page 2-2
- Configuring the Oracle Database for DCNM section, page 2-8
- Upgrading Cisco DCNM 7.0(1) to Version 7.0(2) section, page 2-9

Information About the Cisco DCNM OVA

An Open Virtual Appliance (OVA) is a prebuilt software solution that comprises one or more virtual machines (VMs) that are packaged, maintained, updated, and managed as a single unit. The Cisco DCNM OVA has a preinstalled operating system (CentOS 6.3) and includes application functionality that is necessary for Dynamic Fabric Automation (DFA) functionality. DCNM as an OVA can be deployed on a VMWare Vsphere infrastructure.

Cisco DCNM OVA and Cisco Dynamic Fabric Automation

To bring up Cisco DFA, you can use the Cisco DCNM OVA to link the following two subnets:

- Management access (the outside subnet) to access and administer the DFA network
- Enhanced fabric management network (the inside network) which is connected to the devices through the mgmt0 interface of each device.

When installing Cisco DCNM OVA, you can choose to enable Cisco DFA functionality that simplifies fabric management.

Cisco DCNM provides a management system that offers the following benefits:

- Ease of deployment and use
- Standards-based control protocols and components
- Unlimited level of customization and integration with an operations support systems (OSS) network

Note For more information about Cisco Dynamic Fabric Automation, see to the *Cisco Dynamic Fabric Automation Solutions Guide.*

Cisco DCNM OVA includes the following application functionality:

- Network management
  - Cisco DCNM
- Network services
  - Network Service Controller (NSC) Adapter
- Orchestration
  - RabbitMQ AMQP Message Broker
  - Python integration script
  - OpenLDAP
- Device Power-on Auto Provisioning (POAP)
  - DHCP server
  - TFTP Repository for boot scripts
  - SCP repository for storing images and configurations
- Group provisioning of switches
  - XCP Extensible Messaging and Presence Protocol (XMPP) server (Cisco Jabber)

Note For detailed information about each of the applications that provide the Cisco DFA CPOM functions in Cisco DCNM, see Chapter 3, “Managing Applications After the DCNM OVA Deployment .”.

Installing the Cisco DCNM OVA

Three steps are required to install the OVA:

1. Verify Prerequisites. You must install various VMware components before you install the OVA.
2. Download the OVA file. You can access the required dcnm.ova file from www.cisco.com.
3. Deploy the OVA 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 OVA.

Note If you are using a high-availability (HA) environment for applications that are bundled within the DCNM OVA, you must download the OVA and deploy twice, once for Active and once for Host-Standby. For more information, see Chapter 4, “Managing Applications in a High-Availability Environment .”.

Verifying Prerequisites

Before you install the Cisco DCNM OVA, you will need to meet following software and database requirements:

- VMware vCenter Server 5.1.0 that is running on a Windows server (or alternatively, running as a virtual appliance)
- VMware ESXi 5.1.0 host imported into vCenter
- Two port groups on the ESXi host: one for the dcnm-mgmt-network and one for the enhanced-fabric-mgmt network.
- VMware vSphere client application installed on your desktop

Note The OVA cannot be deployed by connecting the vSphere client directly to the ESXi server.

- Determine the number of switches in your Cisco DFA fabric that will be managed by the Cisco DCNM OVA.
  - If you will be managing more than 50 switches or you expect the number of switches to grow over time, use an Oracle database.

    See "Configuring the Oracle Database for DCNM" section on page 2-8 for information on configuring the Oracle database.

Note Once you start using the PostgreSQL database that is built in to the Cisco DCNM OVA, you cannot migrate the data to an Oracle database.

Note For a complete list of prerequisites that are associated with Cisco DCNM, see the *Cisco DCNM Installation and Licensing Guide, Release 7.x.*

Note To accommodate for HA application functions, additional prerequisites are required. See the Prerequisites for Cisco DCNM OVA HA section, page 4-2.

Downloading the OVA File

The first step to installing the OVA 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/navigator.html

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 Prime 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 **7.0**.(x)

Step 5 Locate the DCNM OVA 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 OVA as an OVF Template

After you download the OVA 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 OVA 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 2-5

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

Step 6 Specify the name and location of the Cisco DCNM OVA.

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 DFA 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 OVA.

Note The OVA should not be deployed under a vApp.

Step 10 Choose the a destination storage for the virtual machine files and click **Next**.

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 2.8 GB 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 OVA. 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 OVA 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 OVA Properties**.**

a. The **Application Management** check box is selected by default to install applications related to DFA.

DFA includes implementations for the following protocols:

– XMPP

– LDAP

– DHCP

– AMQP

DFA includes implementations for the following repositories:

– TFTP

– SCP/SFTP

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 OVA.

Note The password must be at least eight characters long and must contain at least one alphabetic and one numeric character. It can contain the only the following special characters: .(dot), + (plus), _ (underscore), and - (hyphen).

If you do not comply with these password requirements, you can continue with the OVA 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:

- **Hostname** (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**

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 DNCM_OVA window appears and the OVA deployment starts and requires some time to complete.

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

After the OVA 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 section, page 3-8.

Step 5 Log in to the Cisco DCNM web UI:

a. Put the IP address in your browser.

The Cisco Prime 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 OVA 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 *DCNM 7.0 Fundamentals Guide* for configuration information.

Configuring the Oracle Database for DCNM

We recommend that you use an external Oracle database for Cisco DCNM for DFA for better performance, rather than the PostgreSQL database that is built in to the Cisco DCNM OVA.

Note Once you start using the PostgreSQL database that is built in to the Cisco DCNM OVA, you cannot migrate the data to an Oracle database.

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 as described in the *Cisco DCNM Installation and Licensing Guide, Release 7.x.*

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 OVA.

Step 4 Open the Secure Shell (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 OVA. This password is used to access AMQP/LDAP by default. You can change this password later in Cisco DCNM by using the following path: **Admin -> DFA Settings**.

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

```
The external DCNM DB will be configured so that all DFA applications can be accessed using
the root password of this server. You can later change them in the DCNM Web UI: Admin >
DFA Settings

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

done.
```

Step 6 Start the Cisco DCNM application in the OVA.

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

Upgrading Cisco DCNM 7.0(1) to Version 7.0(2)

This section includes instructions for upgrading your Cisco DCNM OVA installation from version 7.0(1) to 7.0(2). You can migrate both Cisco DCNM with a local PostgreSQL database and an external Oracle database and Cisco DCNM in a High Availability (HA) environment.

Migrating Cisco DCNM with a Local PostgreSQL Database and an External Oracle Database

Before you begin, make sure that Cisco DCNM 7.0(1) is up and running.

Step 1 Use the **appmgr backup all** command to backup all applications associated with the installation of Cisco DCNM 7.0(1).

Step 2 Back up Cisco DCNM 7.0(1) license files.

- **a.** Backup the license files saved in the following directory: /usr/local/cisco/dcm/licenses/.
- **b.** On Cisco Prime DCNM 7.0(2), ensure that the MAC address along with all network settings such as the IP address, default gateway, hostname, etc., are identical to the Cisco DCNM 7.0(1) installation.
- **c.** Copy the contents of the Cisco DCNM 7.0(1) files you backed up from the /usr/local/cisco/dcm/licenses/ directory into the Cisco DCNM 7.0(2) /usr/local/cisco/dcm/licenses/ directory.

Step 3 If you are using customized scripts like vCDclient.py, CPNR.py, move these files manually.

- **a.** Backup the following files and put these files in the same location by changing the name. (For example - /root/utils/vCDclient_backup.py).
  /root/utils/vCDclient.py
  root/utils/vCDclient-ini.conf
  root/utils/CPNRclient.py
  root/utils/CPNRclient-ini.conf

Note If you are using a customized poap_dcnm.py script in Cisco DCNM 7.0.(1), after migration the script will be saved as /var/lib/dcnm/poap_dcnm_backup.py in Cisco DCNM 7.0(2) and the new poap_dcnm.py will be there.

Step 4 Transfer the backup file to an external file system.

Step 5 Power off Cisco DCNM 7.0(1).

Step 6 Deploy the Cisco DCNM OVA file for version 7.0(2).

- **a.** Use the same network parameters (IP/subnet/gateway/DNS).
- **b.** Use the same administrative password.
- **c.** Use the same vCenter port groups for both network interfaces.
- **d.** Disable auto-power-on. (The **Power on OVA after deployment** check-box should not be selected).

Step 7 After Cisco DCNM 7.0(2) is deployed, right-click on **VM** -> **Edit Settings** -> **Hardware**.

- **a.** For both Network Adapters, update the MAC address to be the same as Cisco DCNM 7.0(1). This will cause the same MAC address to be used for the new Virtual Machine (VM); licenses on Cisco DCNM will not need to be regenerated in the event of an upgrade.

Step 8 Power on DCNM 7.0(2) VM.

Step 9 Copy the Cisco DCNM 7.0(1) backup file from the external repository to Cisco DCNM 7.0(2) and other files (for example, License etc.) to corresponding places.

Step 10 Use the **appmgr status all** command to make sure that all applications are up and running.

Step 11 Use the **appmgr stop all** command to shut down all applications on Cisco DCNM 7.0(2).

Step 12 Use the **appmgr upgrade <backup filename>** command to run the upgrade script on Cisco Prime DCNM 7.0(2).

- **a.** Select option **[1] Standalone DCNM with Local PostgreSQL database** or **[2] Standalone DCNM with External Oracle database** when prompted, based on your Cisco DCNM 7.0(1) setup:

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

Note If you choose option **[2] Standalone DCNM with External Oracle database**, make sure that the external database is up and running.

Migrating Cisco DCNM in a High Availability Environment

Before you begin, make sure that Cisco DCNM 7.0(1) Active and Standby peers are both up and running.

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

Step 1 Make sure that Cisco DCNM 7.0(2) Active and Standby peers are both deployed but not powered on.

Note Make sure that the MAC address and all network settings, such as the IP address, default gateway, hostname, etc., are identical to the Cisco DCNM 7.0(1) installation.

Step 2 Verify that the **appmgr backup all** command was run on both the Active and Standby peers and that separate tar archives were stored in an external file system (for example, as active.tar.gz and standby.tar.gz)

Step 3 Follow the same steps for the license files and other script files (vCDclient.py, CPNRclient.py etc) as instructed in "Migrating Cisco DCNM with a Local PostgreSQL Database and an External Oracle Database" section on page 2-9.

Step 4 Power off the Cisco DCNM 7.0(1) Active peer.

Step 5 Wait 4 to 5 minutes and then stop the DCNM application on the Cisco DCNM 7.0.(1) Standby peer.

This is to ensure that write operations to LDAP are prevented (which could lead to LDAP getting into an inconsistent state).

Step 6 Power-on the Cisco DCNM 7.0(2) Active peer.

Step 7 Stop all of the applications on the Cisco DCNM 7.0(2) Active peer.

Step 8 Use the **appmgr upgrade <active.tar.gz>** command to run the upgrade script.

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

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

b. Select option **[1] Active** when prompted.

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

Step 9 All applications are running on the Cisco DCNM 7.0(2) Active peer; power-off the Cisco Prime DCNM 7.0(1) Standby peer.

Step 10 Power on the Cisco DCNM 7.0(2) Standby peer.

Step 11 Stop all applications on the Cisco DCNM 7.0(2) Standby peer. (After waiting for all applications to start during OS boot up).

Step 12 Use the **appmgr upgrade <standby.tar.gz>** command to run the upgrade script.

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

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

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

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

Step 13 Invoke the following on the Active peer to establish SSH trust to the Standby peer:

```
sh /root/sshAutoLogin.sh <STANDBY_PEER_IP>
```

CHAPTER 3

Managing Applications After the DCNM OVA Deployment

This chapter describes how to verify and manage all of the applications that provide Cisco Dynamic Fabric Automation (DFA) central point of management functions after the DCNM open virtual appliance (OVA) is deployed. This chapter includes the following sections:

- Cisco DCNM OVA Applications, page 3-1
- Application Details, page 3-2
- Managing Applications, page 3-8
- Backing Up Cisco DCNM and Application Data, page 3-12
- Restoring Applications, page 3-14

Note For instructions on installing these applications with the Cisco DCNM OVA, see the "Installing the Cisco DCNM OVA" section on page 2-2.

Note For information about managing these applications in a high-availability (HA) environment, see "Managing Applications in a High-Availability Environment" section on page 4-1.

Cisco DCNM OVA Applications

A complete list of applications included in Cisco DCNM that provide Cisco DFA is in Table 3-1. Information about these applications and the corresponding login credentials are included.

Table 3-1 Cisco DCNM OVA Applications

Category	Application	Username	Password	Protocol Implemented
Network Management	Data Center Network Manager	admin	User choice[1]	Network Management
Network Services	Cisco Prime Network Services Controller Adapter	created by Cisco Prime Network Services Controller administrator	created by Cisco Prime Network Services Controller administrator	Network services (firewall and load balancing)
Orchestration	RabbitMQ	admin	User choice[1]	Advanced Messaging Queuing Protocol
Orchestration	OpenLDAP	cn=admin dc=cisco dc=com	User choice[1]	Lightweight Directory Access Protocol
Group Provisioning of Switches	Cisco Jabber Extensible Communications Platform (XCP)	admin@fully qualified domain name (FQDN)[2]	User choice[1]	Extensible Messaging and Presence Protocol
Device Power On Auto-Provisioning	Dhcpd	—	—	Dynamic Host Configuration Protocol
Device Power on Auto-Provisioning	Tftp servers[2] SSH/SFTP server	—	—	Trivial File Transfer Protocol

[1]User choice refers to the administration password entered by the user during OVA deployment.

2FQDN is the one that was entered during OVA deployment

[2]Place the files that you want to be accessed from outside through TFTP at /var/lib/dcnm/.

Application Details

This section describes the details of all the applications within the functions they provide in Cisco DCNM. The functions are as follows:

- Network Management
- Network Services
- Orchestration
- Power On Auto Provisioning (POAP)
- Group provisioning of switches

Network Management

The data center network management function is provided by the Cisco Prime Data Center Network Manager (DCNM) server. Cisco DCNM provides the setup, visualization, management, and monitoring of the data center infrastructure. Cisco DCNM can be accessed from your browser: http://[host/ip].

Note For more information about Cisco DCNM, see http://cisco.com/go/dcnm.

Network Services

In the Cisco DFA solution, traditional services, such as firewalls and load balancers, are deployed at regular leaf nodes within the spine-leaf topology, and at border leaf nodes, unlike more traditional data centers where these services are deployed at the aggregation layer.

Cisco Prime Network Services Controller (Prime NSC) provides the orchestration and automation of network services in Cisco DFA. The Prime NSC supports integration with virtual computer and storage managers such as vCenter and System Center Virtual Machine Manager (SCVMM) and provides end-to-end orchestration and automation for services in Cisco DFA.

Note For more information about the Prime NSC, see the Cisco Prime Network Services Controller documentation at the following URL:
http://www.cisco.com/en/US/partner/products/ps13213/tsd_products_support_series_home.html

A Prime NSC Adapter is bundled within the Cisco DCNM OVA. It performs the following functions:

- Enables DCNM to interoperate with one or more instances of the Prime NSC.
- Provides translation of DCNM language and objects into the Prime NSC language and objects.
- Ensures that the Prime NSC and DCNM are always synchronized.
- Maps the tenants and virtual data centers to the Prime NSC instances responsible for network services

Note The Prime NSC Adapter supports DCNM-to-Prime NSC integration for multiple Prime NSC instances. A single Prime NSC instance is not able to fulfill DFA scalability requirements for tenants and VMs. Consequently, multiple instances are required to achieve the scale that DFA requires.

You can create instances with the help of a Prime NSC Adapter Manager CLI feature. See the "Cisco Prime Network Services Controller Adapter Manager Command-Line Interface" section on page 3-5.

Configuring Connectivity with DCNM

This procedure describes how to configure connectivity between the Prime NSC and DCNM.

After you have successfully configured connectivity, the following aspects apply:

- When operating with DCNM, there is no option to create, modify, or delete a tenant or virtual data center from the Prime NSC

- The Prime NSC web UI does not allow any admin or tenant-admin to modify any of the tenant scoped L2 network- and subnetwork-related information. This restriction does not apply to management on HA L2 networks and subnetworks that are managed by the Prime NSC administrator.
- If you create, update, or delete a network service in Prime NSC, it will be reflected in both DCNM and the Prime NSC.

Before you begin to configure connectivity with DCNM, confirm the following:

- DCNM is running
- Enhanced fabric management network was enabled during DCNM deployment
- You have network access to DCNM
- You have appropriate privileges for configuring DCNM
- You have deployed the Prime NSC in Orchestrator mode.
- The Prime NSC administrator has created a user account, with administrator role, for use only by Prime NSC Adapter in DCNM

Step 1 Log in to the DCNM VM console as root.

Step 2 Navigate to the /opt/nscadapter/bin directory.

Step 3 Start the Prime NSC Adapter by entering the following command: **nsc-adapter-mgr start**.

Step 4 Use the **nsc-adapter-mgr nsc add** command to enter the following information to provide DCNM with access to Prime NSC:

- Prime NSC management IP address
- Username for Prime NSC access
- Password for Prime NSC access

The command format is **nsc-adapter-mgr nsc add** *ip-address user name password*.

Step 5 Log in to the Cisco DCNM web UI and do the following:

a. Choose **Admin > Dynamic Fabric Automation > Settings**.

b. Choose **Config > Dynamic Fabric Automation (DFA) > Auto-Configuration**.

c. Click **Add Organization** and enter the information for the organization. An organization in DCNM corresponds to a tenant in Prime NSC Adapter.

d. Add a network to the organization.

e. As needed, add partitions to the organization. A partition in DCNM corresponds to a virtual data center in Prime NSC.

Step 6 To confirm that connectivity is established between DCNM and Prime NSC, log in to Prime NSC and confirm that the organization is displayed in the Tenant Management tab.

See the "Cisco Prime Network Services Controller Adapter Manager Command-Line Interface" section on page 3-5 for a list of all of the CLI commands.

Cisco Prime Network Services Controller Adapter Manager Command-Line Interface

You can register a Cisco Prime Network Services Controller (Prime NSC) instance using the Prime NSC Adapter Manager command-line interface (CLI). A single Prime NSC instance is not able to fulfill Cisco DFA's scalability requirements for tenants and VMs; therefore, multiple instances are required to achieve the scale that Cisco DFA requires.

Even though the Prime NSC Adapter is part of the DCNM OVA, you must manually start the Prime NSC Adapter. Refer to the following table for CLI commands to start and stop the Prime NSC Adapter.

Table 3-2 Cisco Prime Network Services Controller Adapter commands

Command	Description
nsc-adapter-mgr [-h|--help]	Displays help
nsc-adapter-mgr adapter{**start** | **stop** | **status** | **connections**}	Starts/stops or displays the running status of the Prime NSC Adapter, or displays the status of the NSC Adapter connections
nsc-adapter-mgr dcnm update *ip-address username password*	Updates Cisco DCNM instances with provided IP address, user name, and password.
nsc-adapter-mgr nsc {[**add** *ip-address user name password* | **update** *ip-address username password* | **remove** *ip-address* [**force**] | **list-instances** [{**org** | **tenant**} *org/tenant* {**partition** | **vdc**} *partition/vdc*] | **list** {**org** | **tenants**} **instance** *ip-address*]}	Adds, updates, or removes an existing Prime NSC instance identified by the provided IP address with provided user name and password. When using list-instances, shows the status of all Prime NSC instances or displays the status of Prime NSC instances belonging to the provided Tenant or the provided VDC.

Note See the *Cisco Prime Network Services Controller User Guide* for more information about Cisco Prime Network Services Controller.

Config Profiles

When you are using autoconfiguration for DFA, the network is associated with a configuration profile (config profile). A config profile template instance is created on leaf nodes wherever a network appears. When using services in the Cisco Prime Network Services Controller (Prime NSC), you must select the correct config profile to orchestrate and automate the services in the DFA network.

Table 3-3 includes the sample guidelines for edge firewall with regards to selecting config profiles when you are using services.

Table 3-3 Service configuration profiles

Service Node	Network	Routing	Service Profile
Edge Firewall	Host Networks	N/A	defaultNetworkIpv4EfEdgeServiceProfile defaultNetworkIpv4TfEdgeServiceProfile
	Tenant Service Network	Static	serviceNetworkIpv4TfStaticRoutingProfile
		Dynamic	serviceNetworkIpv4TfDynamicRoutingProfile
	Tenant Ext Service Network	Static	externalNetworkIpv4TfStaticRoutingProfile
		Dynamic	externalNetworkIpv4TfDynamicRoutingProfile
Service Node as Router/Default Gateway	Host Networks	N/A	defaultNetworkL2Profile
Compute Firewall (L3 vPath)	Host Networks	N/A	defaultNetworkIpv4EfEdgeServiceProfile/ defaultNetworkIpv4TfEdgeServiceProfile
	Tenant Service Network	N/A	serviceNetworkIpv4TfL3VpathServiceNodeProfile
	Tenant Service Classifier Network	N/A	serviceNetworkIpvEfL3VpathServiceClassifierProfile
Compute Firewall (L2 VPath)	Host Networks	N/A	defaultNetworkIpvEfEdgeServiceProfile/ defaultNetworkIpvTfEdgeServiceProfile
	Tenant Service	N/A	serviceNetworkL2VpathProfile
Service Node as Router/Default Gateway	Host Networks	N/A	defaultNetworkL2Profile

Orchestration

Three components provide orchestration functions.

- RabbitMQ

  Rabbit MQ is the message broker that provides the Advanced Messaging Queuing Protocol (AMQP). The RabbitMQ message broker sends events from the vCloud Director/vShield Manager to the Python script for parsing. You can configure this protocol by using certain CLI commands from the Secure Shell (SSH) console of the OVA.

  Note For more information about RabbitMQ, go to http://www.rabbitmq.com/documentation.html

- Python Integration Script

The orchestration Python script receives and parses events from VMware's vCloud Director/vShield Manager through the RabbitMQ message broker. It communicates with vCloud Director/vShield Manager through web service APIs for detailed information and then calls Cisco DCNM REST APIs to populate data that is to be used by the fabric.

The Python integration scripts and the configuration files in the OVA are as follows:

/root/utils/vCDclient.py

/root/utils/vCDclient-ini.conf

You should edit the vCDclient-ini.conf file with your specific information and start the integration using Python2.7 as python2.7 vCDclient.py

Tip By invoking the script with the Python command, you will invoke the default Python 2.6 version, which might fail; the integration script requires certain modules that are available only in Python 2.7.

- OpenLightweight Directory Access Protocol (LDAP)

  The OVA installs LDAP that serves as an asset database to the switches.

Device Power On Auto Provisioning

Power On Auto Provisioning (POAP) occurs when a switch boots without any startup configuration. It is accomplished by two components that were installed with the OVA:

- DHCP Server

  The DHCP server parcels out IP addresses to switches in the fabric and points to the location of the POAP database, which provides the Python script and associates the devices with images and configurations.

  During the Cisco DCNM OVA installation, you define the IP Address for the inside fabric management address or OOB management network and the subnets associated with the Cisco DFA management.

  Note You should always configure DHCP through Cisco DCNM web UI by choosing: **UI > Config > POAP > DHCP Scopes**. Editing the /etc/dhcp/dhcp.conf file from an SSH terminal might lead to unexpected behavior.

- Repositories

  The TFTP server hosts boot scripts that are used for POAP.

  The SCP server downloads the database files, configuration files, and the software images.

Group Provisioning of Switches

You can accomplish group provisioning of switches by using the Extensible Messaging and Presence Protocol (XMPP) server. Through the XMPP server and Cisco Jabber, you have access to all devices in the fabric and can create chat groups of spines and leaves for group provisioning of switches.

The initial XMPP configuration can be done through the Cisco DCNM web UI by choosing: **Admin > DFA Settings**.

Note Before a switch can participate in XMPP, it must be added to the XMPP database by using the **appmgr** CLI command shown in Table 3-4. See the"XMPP User and Group Management" section on page 3-9 for information.

Managing Applications

You can manage the applications for Cisco DFA in the Cisco DCNM OVA through commands in an SSH terminal.

Enter the **appmgr** command from the SSH terminal by using the following credentials:

- Username: root
- Password: Administrative password provided during OVA deployment.

Note For your reference, context sensitive help is available for the **appmgr** command. Use the **appmgr ?** command to display help.

Use the **appmgr tech_support** command to produce a dump of the log files. You can then provide this information to the TAC team for troubleshooting and analysis of your setup.

Note This section does not describe commands for Network Services using Cisco Prime Network Services Controller. For network services commands, see the "Cisco Prime Network Services Controller Adapter Manager Command-Line Interface" section on page 3-5.

Verifying the Application Status after Deployment

After you deploy the OVA file, you can determine the status of the applications that were deployed in the OVA file. You can use the **appmgr status** command in an SSH session to perform this procedure.

Note Context-sensitive help is available for the **appmgr status** command. Use the **appmgr status ?** command to display help.

Step 1 Open up an SSH session:

a. Enter the **ssh root** ***DCNM network IP address*** command.

b. Enter the *administrative password* to login.

Step 2 Check the status of the applications by entering this command:

```
appmgr status all


DCNM Status

 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
 1891 root 20 02635m 815m  15m S  0.0 21.3   1:32.09 java
```

```
LDAP Status

 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
1470 ldap   20  0 692m 12m 4508 S 0.0 0.3  0:00.02 slapd

AMQP Status

 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
1504 root      20   0 52068  772  268 S  0.0  0.0   0:00.00 rabbitmq

TFTP Status

 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
1493 root   20  0 22088 1012  780 S 0.0 0.0  0:00.00 xinetd

XMPP Status

 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
1906 jabber  20  0 1389m 26m 6708 S 0.0 0.7  0:00.61 jabberd

DHCP Status

 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
1668 dhcpd 20   0 46356 3724 408 S  0.0  0.0   0:05.23 dhcp
```

Stopping, Starting, and Resetting Applications

Use the following CLI commands for stopping, starting, and resetting applications:

- To stop an application, use the **appmgr stop** ***application*** command.

```
# appmgr stop dhcp
Shutting down dhcpd:                                       [  OK  ]
```

- To start an application, use the **appmgr start** ***application*** command.

```
# appmgr start amqp
Starting vsftpd for amqp:                                  [  OK  ]
```

- To restart an application use the **appmgr restart** ***application*** command.

```
# appmgr restart tftp
Restarting TFTP...
Stopping xinetd:                                           [  OK  ]
Starting xinetd:                                           [  OK  ]
```

XMPP User and Group Management

XMPP in-band registration is disabled in the Cisco DCNM OVA from a security perspective.

Before a switch can participate in XMPP, it must be added to the XMPP database by using the **appmgr** CLI command shown in Table 3-4.

Note A switch that has gone through POAP does *not* need to be added to the XMPP database using the **appmgr** CLI commands.

When POAP definitions are created in DCNM Web UI for a given switch, an XMPP user for that switch is automatically created in the XMPP database with the switch hostname “XMPP user” and with an XMPP password specified in the POAP definitions.

When the Cisco DCNM OVA is deployed, an XMPP user named “admin” and a group named “dcnm-dfa” are created. This can be changed later in the DCNM Web UI by choosing **Admin > DFA Settings**.

Table 3-4 CLI Commands for XMPP user and group management

CLI Commands	Description
appmgr add_user xmpp -u ***username*** **-p** ***password***	-u is XMPP user ID without the domain name -p is XMPP user password (if user already exists, the password will be updated) For example, **appmgr add_user xmpp -u admin -p secret** creates a Jabber ID 'admin@xyz.com' with password 'secret', where xyz.com is the FQDN
appmgr add_group xmpp -u *username* **-p** *password* **-g** *group-name*	-u is XMPP user ID without the domain name -p is XMPP password -g XMPP group to be created, if it does not exist already For example, **appmgr add_group xmpp -u admin -g dcnm-dfa** creates an XMPP group ‘dcnm-dfa’ created by Jabber ID 'admin@xyz.com'
appmgr list_users xmpp	Lists the XMPP users
appmgr list_groups xmpp	Lists the XMPP groups

CLI Commands	Description
appmgr delete_user xmpp -u *user*	Deletes the XMPP user. You cannot delete a user if any group created by that user still exists in the XMPP database.
appmgr delete_group xmpp -u *username* **-p** *password* **-g** *group*	Deletes the XMPP group -u is the XMPP user ID without the domain name -p is the XMPP user password -g is the XMPP group to be deleted For example, **appmgr delete_group xmpp -u admin -p cisco123 -g dcnm-dfa** deletes the XMPP group 'dcnm-dfa' created by Jabber ID 'admin@xyz.com.' You cannot delete a group created by one user with the credentials of another user.

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.

Importing SSL Certificates

Perform the following task to import SSL certificates after you fetch the CSR certificates from the CA. CSR must include intermediate, root and server certificates.

Step 1 Stop DCNM servers.

Step 2 Update the server.xml with the key alias name.

```
vi server/dcnm/deploy/jboss-web.deployer/server.xml

added key-alias=<<key-alias-name>>

<Connector port="8443"

protocol="HTTP/1.1" SSLEnabled="true"
maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true"
server="Apache"
scheme="https" secure="true" clientAuth="false" sslProtocol = "TLS"
keystoreFile="${jboss.server.home.dir}/conf/fmserver.jks" keystorePass="fmserver_1_2_3"
allowTrace="false" key-alias="<<key-alias-name>>"/>
```

Step 3 Start the DCNM servers.

Note You must import the certificates in the order: intermediate, root and server certificates.

Step 4 If it is required to use the CA signed certificates for both Fabric server and the LAN server, the certificates must be imported in both the files

```
/fm/conf/fmserver.jks
```

and

```
../dcnm/conf/fmserver.jks)
```

Step 5 Use the following commands to import the certificates:

```
/usr/local/cisco/dcm/java/jre1.6/bin/keytool -importcert -alias inter -file inter.pem
-keystore ""/usr/local/cisco/dcm/jboss-4.2.2.GA/server/dcnm/conf/fmserver.jks" -storepass
fmserver_1_2_3

/usr/local/cisco/dcm/java/jre1.6/bin/keytool -importcert -alias root -file root.pem
-keystore ""/usr/local/cisco/dcm/jboss-4.2.2.GA/server/dcnm/conf/fmserver.jks " -storepass
fmserver_1_2_3

/usr/local/cisco/dcm/java/jre1.6/bin/keytool -importcert -alias mykey -file mykey.pem
-keystore ""/usr/local/cisco/dcm/jboss-4.2.2.GA/server/dcnm/conf/fmserver.jks " -storepass
fmserver_1_2_3

/usr/local/cisco/dcm/java/jre1.6/bin/keytool -importcert -alias inter -file inter.pem
-keystore "" /usr/local/cisco/dcm/jboss-4.2.2.GA/server/fm/conf/fmserver.jks" -storepass
fmserver_1_2_3

/usr/local/cisco/dcm/java/jre1.6/bin/keytool -importcert -alias root -file root.pem
-keystore "" /usr/local/cisco/dcm/jboss-4.2.2.GA/server/fm/conf/fmserver.jks " -storepass
fmserver_1_2_3

/usr/local/cisco/dcm/java/jre1.6/bin/keytool -importcert -alias mykey -file mykey.pem
-keystore ""/usr/local/cisco/dcm/jboss-4.2.2.GA/server/fm/conf/fmserver.jks " -storepass
fmserver_1_2_3
```

Step 6 To import the certificates to fmtrust.jks, perform the following:

```
/usr/local/cisco/dcm/java/jre1.6/bin/keytool -importcert -alias inter -file
/usr/local/cisco/dcm/jboss-4.2.2.GA/server/fm/conf/inter.pem -keystore
/usr/local/cisco/dcm/jboss-4.2.2.GA/server/fm/conf/fmtrust.jks -storepass fmserver_1_2_3

/usr/local/cisco/dcm/java/jre1.6/bin/keytool -importcert -alias root -file
/usr/local/cisco/dcm/jboss-4.2.2.GA/server/fm/conf/root.pem -keystore
/usr/local/cisco/dcm/jboss-4.2.2.GA/server/fm/conf/fmtrust.jks -storepass fmserver_1_2_3

/usr/local/cisco/dcm/java/jre1.6/bin/keytool -importcert -alias tomcat1 -file
/usr/local/cisco/dcm/jboss-4.2.2.GA/server/fm/conf/dcnm05.pem -keystore
/usr/local/cisco/dcm/jboss-4.2.2.GA/server/fm/conf/fmtrust.jks -storepass fmserver_1_2_3
```

Step 7

Backing Up Cisco DCNM and Application Data

You can use the **appgmr backup** command to back up Cisco DCNM and application data. See the following sections for details about backing up data. However, Cisco DCNM does not take a backup of the NX-OS image. You must take the backup of the NX-OS images separately.

Note For your reference, context sensitive help is available for the **appmgr backup** command. Use the **appmgr backup ?** command to display help.

Backing Up Cisco DCNM

You can back up Cisco DCNM with a single command.

- To back up Cisco DCNM, use the **appmgr backup dcnm** command.

Note Configuration archive directories are not part of this backup. The command backs up only the local PostgreSQL database used by Cisco DCNM.

Backing Up Application Data

Backing up all application data can be performed for a specific application or for all applications at once. Refer to the following table for CLI backup commands.

Table 3-5 CLI Commands for backing up application data

Command	Description
appmgr backup all	Backs up data for all applications.
appmgr backup dcnm	Backs up data for DCNM.
appmgr backup ldap	Backs up data for LDAP.
appmgr backup xmpp	Backs up data for both the XMPP/XCP configuration files and the local XMPP/XCP database.
appmgr backup amqp	Backs up data for AMQP.
appmgr backup repo	Backs up data for the repository contents (under /var/lib/dcnm). The **appmgr backup repo** command excludes the backup of image files (all files ending in the .bin extension under /var/lib/dcnm) to prevent the backup file from becoming too large.
appmgr back dhcp	Backs up data for the DHCP server.

Using Scripted Backups for Backing Up Application Data

If you use cron jobs for backup procedures, the database passwords can be assigned arguments so that there are no prompts. For example, you can use the **-p1** command for the Cisco DCNM database password. You can use the **-p2** command for the XMPP database password. Both passwords apply only to local databases.

```
appmgr backup dcnm -p1 dcnmdbpass
appmgr backup xmpp -p2 xmppdbpass
appmgr backup all -p1 dcnmdbpass -p2 xmppdbpass
```

Note Before upgrading or restoring backed-up data onto another OVA setup, the files under folder **/usr/local/cisco/dcm/fm/pm/db** needs to be backed-up since these files locally saved in the DCNM server instead of database.

Restoring Applications

Restoring an application clears all the existing data from that application. Before you restore an application, you should shut down the application.

Because all data will be cleared, you should perform a backup of the application that you are going to restore.

Use the following procedure to back up application data and restore the application on a new OVA.

Note A backup and restore procedure is supported only on either the same OVA or a new OVA deployed with an identical network configuration as the backed-up OVA.

Step 1 Stop all the DCNM services, by using the **appmgr stop all** command.

Step 2 Use the **appmgr backup** command on the existing OVA.

You must take the backup of the NX-OS images in the devices separately.

Step 3 Transfer the backup file to any repository.

Step 4 Power off the first OVA.

Step 5 Deploy another OVA with the same network configuration as the existing one, using the same IP/Netmask/Gateway/Hostname/DNS.

Step 6 Transfer the backup file to the second OVA.

The NX-OS images backup file must be restored to the **/var/lib/dcnm** folder.

Step 7 Run the **appmgr restore** with the new backup on the new OVA.

Note See Table 3-6 for a list of CLI commands to restore applications.

Table 3-6 CLI commands for restoring applications

Command	Description
appmgr restore all *file*	Restores all applications.
appmgr restore dcnm *file*	Restores DCNM.
appmgr restore ldap *file*	Restore LDAP.
appmgr restore amqp *file*	Restores AMQP.
appmgr restore repo *file*	Restores the repository contents
appmgr restore dhcp *file*	Restores the DHCP server.
appmgr restore xmpp *file*	Restores the XMPP server.

Note Before restoring backed-up data onto another OVA setup, the files under folder **/usr/local/cisco/dcm/fm/pm/db** needs to be restored back in the same location.

CHAPTER 4

Managing Applications in a High-Availability Environment

This chapter describes how to configure a high-availability (HA) environment in your Cisco DCNM OVA deployment for your Cisco Dynamic Fabric Automation (DFA) solution. It also includes details about the HA functionality for each of the applications bundled within the Cisco DCNM OVA.

This chapter includes the following sections:

- Information About Application Level HA in the Cisco DCNM OVA, page 4-1
- Prerequisites for Cisco DCNM OVA HA, page 4-2
- Application High Availability Details, page 4-4
- Configuring DCNM OVA HA, page 4-10

Note For instruction about installing these applications with the Cisco DCNM OVA, see the"Installing the Cisco DCNM OVA" section on page 2-2.

Information About Application Level HA in the Cisco DCNM OVA

To achieve HA for applications that are run on the Cisco DCNM OVA, you can run two virtual appliances. You can run one in Active mode and the other in Standby mode.

Note This document refers to these appliances as OVA-A and OVA-B, respectively.

In this scenario:

1. All applications run on both appliances.

   The application data is either constantly synchronized or applications share a common database as applicable.

2. Only one of the applications running on the two appliances serves the client requests. Initially this would be the applications running on OVA-A. The application continues to do so until one of the following happens:

   – The application on OVA-A crashes.

– The operating system on OVA-A crashes.
– OVA-A is powered off for some reason.

3. At this point, the application running on the other appliance (OVA-B) takes over.

   For DCNM REST API and AMQP, this transition is done by a load-balancing software that hides the interface address of the appliances using a Virtual IP (VIP) address.

   For LDAP, both nodes are configured as duplicates of each other. The LDAP clients (switches) are configured with primary and secondary LDAP IPs, so if the active LDAP fails they try contacting the LDAP running on the standby.

   For DHCP, when the first node fails, the second node starts serving the IP addresses.

4. The existing connections to OVA-A are dropped and the new connections are routed to OVA-B.

   This scenario demonstrates why one of the nodes (OVA-A) is initially referred to as the Active node and OVA-B is referred as the Standby node.

Automatic Failover

The application-level and virtual machine (VM)-level and switchover process is as follows.

- If any of the applications managed by the load-balancing software (DCNM/AMQP) goes down on OVA-A, the Active node that handles the client requests detects the failure and redirects subsequent requests to the Standby node (OVA-B). This process provides an application-level switchover.
- If the Active node (OVA-A) fails or is powered-off for some reason, the Standby node (OVA-B) detects the failure and enables the VIP address for Cisco DCNM/AMQP on OVA-B. It also sends a gratuitous ARP to the local switch to indicate the new MAC address that is associated with the IP address. For applications not using VIP, the DHCPD runninG on OVA-B detects the failure of DHCPD on OVA-A and activates itself; whereas LDAP running on OVA-B continues running as LDAP is deployed Active-Active. Consequently, a VM-level failover is accomplished for all four applications (DCNM/AMQP/DHCP/LDAP).

Manually Triggered Failovers

An application-level failover can also be triggered manually. For instance, you might want to run AMQP on OVA-B and the rest of the applications on OVA-A. In that case, you can log in to the SSH terminal of OVA-A and stop AMQP by using the **appmgr stop amqp** command.

This failover triggers the same process that is described in the "Automatic Failover" section on page 4-2; subsequent requests to the AMQP Virtual IP address are redirected to OVA-B

Prerequisites for Cisco DCNM OVA HA

This section contains the following topics that describe the prerequisites for obtaining a high-availability (HA) environment.

- Configuring the Oracle Database for DCNM
- Deploying Cisco DCNM OVAs
- Creating an NFS/SCP Repository

- Availability of Virtual IP Addresses
- Installing an NTP Server

Deploying Cisco DCNM OVAs

You must deploy two standalone OVAs. When you deploy both OVAs, 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 process ensures that both OVAs are duplicates of each other.

After the OVA is powered up, verify that all the applications are up and running by using the **appmgr status all** command.

After all of the applications are up and running, stop the applications by using the **appmgr stop all** command.

Note When the OVA is started up for the first time, please wait for all the applications to run before you shut down any of the applications or power off the virtual appliance.

Note For instructions on deploying the Cisco DCNM OVA, see Chapter 2, “Installing Cisco DCNM OVA Management Software”.

Creating an NFS/SCP Repository

The DCNM HA cluster needs a server that has both NFS/SCP capabilities. This server is typically a Linux server.

Note The server has to be in the enhanced fabric management network because the switches will use this server to download images and configurations.

Make sure that the exported directory is writable from both peers. The procedure to export a directory /var/lib/sharedarchive on a CentOS server is listed in the following paragraph. The steps will vary based on your environment.

Note You might need root privileges to execute these commands. If you are a nonroot user, please use them with ‘sudo’.

```
[root@repository ~]# mkdir -p /var/lib/sharedarchive
[root@repository ~]# chmod -R 777 /var/lib/sharedarchive
[root@repository ~]# vi /etc/exports
/var/lib/sharedarchive *(rw,sync)

 [root@repository ~]# cd /etc/init.d
[root@repository ~]# service nfs restart
```

The same folder /var/lib/sharedarchive can also be accessed through SCP with SCP credentials.

The **/var/lib/sharedarchive * (rw,sync)** command provides read-write permissions to all servers on /var/lib/sharedarchive. Refer to CentOS documentation for information on restricting write permissions to specific peers.

Availability of Virtual IP Addresses

Two free IPv4 addresses are needed to set up VIP addresses. The first IP address will be used in the management access network; it should be in the same subnet as the management access (eth0) interface of the OVAs. The second IP address should be in the same subnet as enhanced fabric management (eth1) interfaces (switch/POAP management network).

Installing an NTP Server

For most of the HA functionality to work, you must synchronize the time on both OVAs by using an NTP server. The installation would typically be in the management access network (eth0) interfaces.

Application High Availability Details

This section describes all of the Cisco DFA HA applications.

Cisco DCNM OVA has two interfaces: one that connects to the OVA management network and one that connects to the enhanced fabric management/DFA network. Virtual IP addresses are defined for both interfaces.

- From the OVA management network, the DCNM-REST API, DCNM interface, and AMQP are accessed through the VIP address
- From the enhanced fabric management network, LDAP and DHCP are accessed directly.

Only three Virtual IPs are defined:

- DCNM REST API (on dcnm management network)
- DCNM REST API (on enhanced fabric management network
- AMQP (on dcnm management network)

Note Although DCNM OVA in HA sets up a VIP, the VIP is intended to be used for the access of DCNM, REST API. For GUI access, we still recommend that you use the individual IP addresses of the DCNM HA peers and use the same to launch LAN/SAN Java clients, etc.

See the following table for a complete list of DFA applications and their corresponding HA mechanisms.

DFA Application	HA Mechanism	Use of Virtual IPs	Comments
Data Center Network Manager	DCNM Clustering/ Federation	Yes	Two VIPs defined on each network
RabbitMQ	RabbitMQ Mirrored Queues	Yes	One VIP defined on theOVA management network
LDAP	OpenLDAP Mirror-mode replication	No	—
XMPP	Not available in HA	—	Use XMPP on the Active peer for all configurations
DHCP	ISC DHCPD Failover	No	—
Repositories	—	—	External repositories have to be used

Network Management

The data center network management function is provided by the Cisco Prime Data Center Network Manager (DCNM) server. Cisco DCNM provides the setup, visualization, management, and monitoring of the data center infrastructure. Cisco DCNM can be accessed from your browser at http://[host/ip].

Note For more information about Cisco DCNM, see http://cisco.com/go/dcnm

HA Implementation

Cisco DCNMs that run on both OVAs are configured in clustering and federated modes for HA.

- Cisco DCNM clustering is an HA mechanism for LAN devices. Internally it uses JBoss clustering. The first OVA that is HA-enabled becomes the master and takes care of all updates to the database.
- Cisco DCNM federation is the HA mechanism for SAN devices. Groups of SAN devices can be managed by each node in the DCNM federated setup. All the devices can be managed using a single client interface.

You can enable automatic failover in the Cisco DCNM UI by choosing: **Admin > Federation**. If you enable an automatic failover and the Cisco DCNM that is running on OVA-A fails, the automatic failover moves only the fabrics and shallow-discovered LANs that are managed by OVA-A to OVA-B automatically.

DCNM Virtual IP Usage

An OVA HA setup has two VIP addresses (one for each network) for the Cisco DCNM at the default HTTP port. These VIPs can be used for accessing the DCNM RESTful services on the OVA management network and the enhanced fabric management network. For example, external systems such as Cisco UCS Director can point to the VIP in the OVA management network and the request gets directed to the active Cisco DCNM. Similarly, the switches in an enhanced fabric management network access the VIP address on the enhanced fabric management network during the POAP process.

You can still directly connect to Cisco DCNM real IP addresses and use them as you would in a DCNM in a cluster/federated set up.

Note We recommend that you use a VIP addresses only for accessing DCNM RESTful API. To access the Cisco DCNM Web UI/DCNM SAN/LAN thick client, connect to the server's real IP address.

Licenses

For Cisco DCNM, we recommend that you have licenses on the first instance and a spare matching license on the second instance.

Application Failovers

Enable an automatic failover option in the Cisco DCNM UI when an OVA HA pair is set up by choosing: **Admin > Federation**. 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).

The Cisco DCNM VIP address still resides on OVA-A. The Representational State Transfer Web Services (REST) calls initially hit the VIP addresses on OVA-A and get redirected to the Cisco DCNM that is running on OVA-B.

Application Failbacks

When the Cisco DCNM on OVA-A comes up, the VIP address automatically redirects the REST requests to DCNM-A.

Virtual-IP Failovers

The VIP address that is configured for Cisco DCNM REST API on OVA-A can fail due to two reasons:

- The load-balancing software running on OVA-A fails.
- OVA-A fails.

In both cases, the VIP address of Cisco DCNM automatically migrates to OVA-B. The only difference is which DCNM will be used after the failover.

  - If a load-balancing software failure occurs, the VIP address on OVA-B directs the requests to DCNM-A.
  - If an OVA-A failure occurs, the VIP address on OVA-B directs the requests to DCNM-B.

The automatic failover ensures that the ownership of all of the fabrics and shallow-discovered LANs managed by DCNM-A automatically change to DCNM-B.

Virtual-IP Failbacks

When OVA-A is brought up and Cisco DCNM is running, the VIP addresses keep running on the Standby node. The failback of Virtual IP addresses from OVA-B to OVA-A occurs only in the following sequence.

1. OVA-A comes up.
2. Cisco DCNM runs on OVA-A.
3. OVA-B goes down or the load-balancing software fails on OVA-B.

RabbitMQ

RabbitMQ is the message broker that provides the Advanced Messaging Queuing Protocol (AMQP).

Note For more information about RabbitMQ, go to http://www.rabbitmq.com/documentation.html

HA Implementation

Enabling the HA on the OVA creates a VIP address in the OVA management network. Orchestration systems such as vCloud Director, set their AMQP broker to the VIP address.

Enabling the HA on the OVA also configures the RabbitMQ broker that runs on each node to be a duplicate of the broker that is running on the other node. Both OVAs act as “disk nodes” of a RabbitMQ cluster, which means that all the persistent messages stored in durable queues are replicated. The RabbitMQ policy ensures that all the queues are automatically replicated to all the nodes.

Application Failovers

If RabbitMQ-A fails, the VIP address on OVA-A redirects the subsequent AMQP requests to RabbitMQ-B.

Application Failbacks

When RabbitMQ-A comes up, the VIP address automatically starts directing the AMQP requests to RabbitMQ-A.

Virtual-IP Failovers

The VIP address configured for the AMQP broker on OVA-A can fail due to two reasons:

- The load-balancing software running on OVA-A fails.
- OVA-A fails.

In both cases, the VIP address of the AMQP automatically migrates to OVA-B. The only difference is which AMQP broker will be used after the failover.

  - In a load-balancing software failure, the VIP address on OVA-B directs the requests to RabbitMQ-A.
  - In an OVA-A failure, the VIP address on OVA-B directs the requests to RabbitMQ-B.

"Virtual-IP" Failbacks

When OVA-A is brought up and AMQP-A is running, the VIP addresses keep running on the OVA-B (directing the requests to AMQP-A). The failback of the RabbitMQ VIP from OVA-B to OVA-A occurs only in the following sequence.

1. OVA-A comes up.
2. RabbitMQ runs on OVA-A.
3. OVA-B goes down or the load-balancing software fails on OVA-B.

OpenLightweight Directory Access Protocol

The OVA installs an LDAP server an asset database to the switches.

This section contains the following topics:

- "Using the OVA-Packaged (Local) LDAP Server" section on page 4-8
- "Using the Remote LDAP Server" section on page 4-9

Using the OVA-Packaged (Local) LDAP Server

LDAP HA is achieved through OpenLDAP mirror mode replication. Each LDAP server that is running on one OVA becomes a duplicate of the LDAP server that is running on the other OVA.

DCNM and LDAP Interaction

Both LDAP IP address show up in the Cisco DCNM Web UI (**Admin->DFA Settings**) in the following order: LDAP-A, LDAP-B.

Cisco DCNM always attempts to write on LDAP-A as follows.

- If the write operation succeeds, the data gets replicated to LDAP-B.
- If the write operation fails, then Cisco DCNM writes to LDAP-B.

  The data on LDAP-B eventually gets replicated to LDAP-A when it becomes available.

Switch and LDAP Interaction

When you configure the asset databases, every switch is configured with multiple LDAP servers, as shown in the following example.

The first active LDAP server that is configured in the switch becomes the Active LDAP server. The Active LDAP server is queried first for autoconfigurations.

For every read operation that the switch needs to perform, the Active LDAP server is contacted first, followed by the rest of the LDAP servers.

```
Leaf-0 # fabric database type network
Leaf-0 (config-fabric-db)# server protocol ldap host <LDAP-1-IP> vrf management
Leaf-0 (config-fabric-db)# db-table ou=networks,dc=cisco,dc=com key-type 1
Leaf-0 (config-fabric-db)# server protocol ldap host <LDAP-2-IP> vrf management
Leaf-0 (config-fabric-db)# db-table ou=networks,dc=cisco,dc=com key-type 1
```

Use the **show fabric database statistics** command to find the Active LDAP server, which is marked by an asterisk (*) in the output.

```
Leaf-0 # show fabric database statistics
```

```
DB-Type         Requests    Dispatched  Not dispatched  Re-dispatched
-------------------------------------------------------------------
network                1             1               0              0
cabling                0             0               0              0
profile                1             1               0              0
-------------------------------------------------------------------
TOTAL                  2             2               0              0

Per Database stats:
 T Prot Server/DB                        Reqs     OK  NoRes    Err  TmOut   Pend
-------------------------------------------------------------------------------
 n ldap 10.77.247.147                       5      2      1      2      0      0
*n ldap 10.77.247.148                       3      3      0      0      0      0
*p ldap 172.23.244.122                      1      1      0      0      0      0
Legend:
  T-Type (N-Network, C-Cabling, P-Profile)
  *-Active Server
```

In the previous example, during autoconfiguration, a leaf switch first queries 10.77.247.148, which is the active network database (indicated by "*n"). If that is not available, it automatically contacts the second LDAP server configured as an network database (10.77.247.147 in this example).

Using the Remote LDAP Server

This section describes the behavior when you use a remote LDAP server in an HA environment.

Cisco DCNM and LDAP Interaction

Cisco DCNM allows only two external LDAP servers that are assumed to be synchronized with each other.

Switch and LDAP interaction

The switch and LDAP interaction that use the remote LDAP server is the same interaction as when you are using the OVA-packaged LDAP. The Active LDAP server is contacted first; if it is not reachable, the switch then attempts to read from the next available LDAP server.

DCHP HA

DHCP on both OVAs listen on the interface of the enhanced fabric management network. The native Internet Systems Consortium (ISC) DHCPD failover mechanism is be used for HA. The lease information is automatically synchronized using native code.

DHCP POAP

The switches do a DHCP broadcast and get response from the Active DHCP server.

DHCP Autoconfiguration

When a tenant host or virtual machine (VM) comes up, it sends a broadcast that is relayed by the leaf node. In such a scenario, the VM profiles should be configured with both relay addresses of OVA-A and OVA-B.

```
interface vlan $vlanid
```

```
. . .
ip dhcp relay 1.2.3.4 vrf ..# eth1 IP of OVA-A
ip dhcp relay 1.2.3.5 vrf ..# eth1 IP of OVA-B
```

Changing DHCP Scope Configurations

Scope changes through the Cisco DCNM UI ensure proper synchronization of scopes among the peers. We do not recommend that you do a manual configuration of the DHCP scope configuration file.

Note You must update the IP range for the default scope before creating the new scope, otherwise DHCP will be unable to star. See the "Starting DHCP in an HA Setup" section on page 4-14 for information on updating the IP range for the DHCP scope through the Cisco DCNM UI.

Repositories

All repositories must be remote.

XMPP

Extensible Messaging and Presence Protocol (XMPP) HA is currently not available. The OVA HA configuration does not affect the XMPP servers that are running on either of the nodes in any way.

Configuring DCNM OVA HA

Because both of the OVAs in an HA environment are deployed identically, either one of them can be the Active peer. The other OVA would be the Standby peer. All of the configuration CLI commands in the following sections are executed from the secure shell (SSH) terminal.

Configuring the Active Peer

Step 1 Log in to the SSH terminal of the OVA that you want to become the Active peer and enter the **appmgr set ha active** command.

```
Active-peer# appmgr setup ha active
*****************************************************
You are about to enable High Availability in this DCNM virtual appliance.
Please make sure that you the following
1.      An Oracle Database with a user defined for DCNM
2.      A repository with NFS/SCP capabilities
3.      An NTP server for time synchronization
4.      A couple of free IP addresses to be used as Virtual IPs (one on each port group)
5.      A peer DCNM deployed with the same user profile (same username/password)
6.      Shut down all applications in this server using 'appmgr stop all'

*****************************************************
Do you want to continue? [y/n] [y]
```

Step 2 Make sure that each prerequisite is in place and press **y**; if not all of the pre-requisites are in place, press **n** to exit.

A prompt for the root password appears.

```
. . .
Enter the root password of this DCNM : <root-password-of-active-peer>
Enter it again for verification: <root-password-of-active-peer>
. . .
```

Step 3 Enter the administrative password created during OVA installation.

You will now be prompted for the management access interface (eth0 IP address) of the Standby peer.

Step 4 Enter the management IP address of the peer DCNM.

The active OVA generates a pair of authentication keys and transfers it to the peer's authorized keys.

a. Enter the root password of the Standby peer when prompted.

All of the other network information needed from the Standby peer is automatically picked up by the Active peer and displayed for confirmation.

b. Ensure that it is the correct peer and press **y** to continue.

```
. . .
Enter the mgmt IP of the peer DCNM (eth0 IP)  : <peer eth0 IP>
Generating ssh keys..
Enter the root password of the peer
root@10.77.247.148's password: <standby-peer root password>
Retrieving information...
Peer Details :
=============
Hostname:  abc.xyz.com
Eth0 IP :  1.2.3.4
Eth1 IP :  192.168.57.148
Do you want to continue? [y/n] [y]
```

Step 5 Enter the VIP addresses for both the management access (eth0) and enhanced fabric management networks (eth1).

Make sure that the VIP addresses are currently not used by any other interfaces in their respective networks.

```
Setting the Virtual IP addresses
============================
The Virtual IP in the eth0 network.
It serves as a single point of access for the following applications: DCNM REST API, AMQP
Enter the VIP  : <a free IP from eth0 subnet>

The Virtual IP in the eth1 network.
It serves as a single point of access for the following applications: DCNM REST API from
the switch network
Enter the VIP  : <a free IP from eth1 subnet>
```

Step 6 Enter the database URL to set the database. The script uses a JDBC thin driver, so you should enter the URL in the same format.

a. Enter the database password.

b. Enter the database password again for verification.

The script tries to do a sample query from the database to check the details entered. The Cisco DCNM schema and related data are loaded after you confirm that all the data are valid.

```
Setting the Database for DCNM
```

```
============================
Enter the DB URL {ex. jdbc:oracle:thin:@10.2.3.4:1521:XE}  :
jdbc:oracle:thin:@x.x.x.x:1521:XE
Enter the DB username  : <dbuser>
Enter the DB password :
Enter it again for verification:
```

Step 7 Enter repository settings:

a. Enter an SCP/NFS repository IP address for the enhanced fabric management network.

b. Enter the IP/exported-directory location.

The script does a test mount and unmounts it shortly after. It is permanently mounted after user confirmation. Similar checks are done for SCP repository users.

c. You will have to enter the SCP password three times (twice for the script and the third time when the script does a test write on the repository).

d. Enter an NTP server IP address. This step is very important for all the applications that run on a cluster.

```
Repository/NTP Details

note: A repository server in the DFA network that has both NFS and SSH/SCP capability.
======================
Enter the SCP/NFS repository IP  : <repository IP>
NFS Exported location {ex. /var/shared/dcnm/}  : /var/lib/dcnmuser
Performing a test mount to ensure that the server is reachable..
Performing a test-write to ensure the exported directory is writable
test-write successful. Proceeding..
Enter the SCP username for <repository IP>  : <repository user>
Enter the SCP password :
Enter it again for verification:
Performing a test-write to ensure the directory is writable through SCP..
root@<repository-ip>'s password:
test-write successful. Proceeding..
Enter an NTP server for time synchronization  : 10.56.14.161
```

Step 8 A summary of the details entered will be displayed. If you want to reenter the details, press **n**.

Once the HA setup is complete, you can check the role of the ha as follows:

```
OVA-A # appmgr show ha-role
Active
```

Configuring the Standby peer

Step 1 Log in to the SSH terminal of OVA-B and enter the **appmgr setup ha standby** command.

```
OVA-B # appmgr setup ha standby
******************************************************
You are about to enable High Availability in this DCNM virtual appliance.
Please make sure that you the following
1.      A peer DCNM virtual appliance deployed with the same user and configured as Active
peer
2.      Shut down all applications in this server using 'appmgr stop all'
******************************************************
Do you want to continue? [y/n] [y]
```

Step 2 Press **y** to continue.

The standby OVA generates a pair of authentication keys and transfers it to the peer's authorized keys.

a. Enter the root password of the Active peer when prompted.

All the other network information entered during active the OVA setup is automatically picked up by the Standby peer and displayed for confirmation.

b. Carefully check if it is the correct peer and press **y** to continue.

```
Retrieving information from details entered on Active...
Generating ssh keys..
Enter the root password of the peer
Warning: Permanently added '10.77.247.147' (RSA) to the list of known hosts.
Peer Details :
=============
Hostname        :  somehost.cisco.com
Eth0 IP :  10.77.247.147
Eth1 IP :  192.168.57.147

**************************************
Summary of details entered
**************************************

Virtual IP
=========================
Virtual IP in eth0 n/w  : 10.77.247.143
Virtual IP in eth1 n/w  : 192.168.57.143

Database for DCNM
=========================
Enter the DB URL        : jdbc:oracle:thin:@10.77.247.11:1521:XE
Enter the DB username   : dcnmuser

Archives/Repositories
=========================
SCP/NFS repository IP   : 10.77.247.11
NFS Exported location   : /var/lib/dcnmuser
SCP username            : root
NTP server              : 10.56.14.161

**************************************
Do you want to continue? [y/n] [y]
```

Once confirmed, OVA-B is configured to be a Standby peer, and the following message is displayed.

```
…
********************************************************************************
This node has been configured as standby
Please run 'appmgr start all' first on the active peer (10.77.247.147), and then on the
standby peer(10.77.247.148) to start using applications.
** note ** : dhcpd will not be up until the default poap scopes are updated with free IP
addresses from DCNM GUI
********************************************************************************
```

Note For information about updating default POAP scopes and starting DHCP using HA, please see, Starting DHCP in an HA Setup, page 4-14

Step 3 Check the HA role of the node by entering the **appmgr show ha-role** command.

```
OVA-A # appmgr show ha-role
Standby
```

Starting Applications in the Active Peer

Step 1 Log in to the SSH terminal of the Active peer (OVA-A) and start all applications by entering the **appmgr start all** command.

Step 2 Wait for all the applications to start. Once all applications (except dhcpd) are up and running, go to the next procedure.

Note To start DHCP using HA, see the "Starting DHCP in an HA Setup" section on page 4-14.

Starting Applications in the Standby Peer

Step 1 Login to the SSH terminal of the Standby peer and start all applications using the **appmgr start all** command. Wait for all the applications to start.

Step 2 Once all applications (except dhcpd) are up/running, proceed to the next step.

Note For starting DHCP using HA, please see, Starting DHCP in an HA Setup, page 4-14

Starting DHCP in an HA Setup

In an HA setup, DHCPD will be initially down. In this procedure, you will update the IP range address for the POAP DHCP scope. Use the following procedure to bring up DHCP.

Note You must update the IP range for the default scope before creating the new scope, otherwise DHCP will be unable to start.

Step 1 Log in to Cisco DCNM web UI.

Step 2 On the menu bar, choose **Config> POAP > DHCP Scope** and enter the free IP range address for the default DHCP scope named enhanced_fabric_mgmt_scope.

Step 3 Click **Apply**.

DHCP is automatically started on both the OVAs.

Step 4 Verify all applications are running by opening an SSH terminal session and using the **appmgr status all** command.