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:

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.