



CHAPTER 6

Managing Applications After DCNM Deployment

This chapter describes how to verify and manage all of the applications that provide DC3 (Programmable Fabric) central point of management functions after the DCNM is deployed. This chapter includes the following sections:

- [Cisco DCNM Applications, page 6-1](#)
- [Application Details, page 6-2](#)
- [Managing Applications, page 6-8](#)
- [Backing Up Cisco DCNM and Application Data, page 6-12](#)
- [Restoring Applications, page 6-14](#)
- [Updating the SFTP Server Address for IPv6, page 6-15](#)



Note

For information about managing these applications in a high-availability (HA) environment, see [“Managing Applications in a High-Availability Environment”](#) section on page 7-1.

Cisco DCNM Applications

A complete list of applications included in Cisco DCNM that provide Cisco Programmable Fabric is in [Table 6-1](#). Information about these applications and the corresponding login credentials are included.

Table 6-1 Cisco DCNM 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)

Category	Application	Username	Password	Protocol Implemented
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	DHCP	—	—	Dynamic Host Configuration Protocol
Device Power on Auto-Provisioning	TFTP servers ² SSH/SFTP server	—	—	Trivial File Transfer Protocol

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

²FQDN is the one that was entered during deployment

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



Note

Anonymous LDAP bind or access is disabled in Cisco DCNM Release 10.3(1). A read-only LDAP user has been introduced since DCNM 7.1(1), DCNM 7.0(2) and 7.0(1). We recommend you to upgrade to a later version for authenticated LDAP access.

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 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://\[host/ip\]](http://[host/ip]).

**Note**

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

Network Services

In the Cisco Programmable Fabric 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 (NSC) provides the orchestration and automation of network services in Cisco Programmable Fabric. 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 Programmable Fabric.

**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. 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 Programmable Fabric scalability requirements for tenants and VMs. Consequently, multiple instances are required to achieve the scale that Programmable Fabric requires.

Config Profiles

When you are using autoconfiguration for Programmable Fabric, 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 (NSC), you must select the correct config profile to orchestrate and automate the services in the Programmable Fabric network.

Table 6-2 includes the sample guidelines for edge firewall with regards to selecting config profiles when you are using services.

Table 6-2 Service configuration profiles

Service Node	Network	Routing	Service Profile
Edge Firewall	Host Networks	N/A	defaultNetworkIpv4EfESProfile defaultNetworkIpv4TfESProfile
		Static	serviceNetworkIpv4TfStaticRoutingESProfile
	Tenant Service Network	Dynamic	serviceNetworkIpv4DynamicRoutingESProfile
		Static	externalNetworkIpv4TfStaticRoutingESProfile
Tenant-Ext Service Network	Dynamic	externalNetworkIpv4DynamicRoutingESProfile	
	Compute Firewall (L3 vPath)	Host Networks	defaultNetworkIpv4EfProfile defaultNetworkIpv4TfProfile
Tenant Service Network		N/A	serviceNetworkIpv4TfL3VpathServiceNodeProfile
Tenant Service Classifier Network		N/A	serviceNetworkIpv4EfL3VpathServiceClassifierProfile
Compute Firewall (L2 vPath)	Host Networks	N/A	defaultNetworkIpv4EfProfile defaultNetworkIpv4TfProfile
	Tenant Service Network	N/A	serviceNetworkL2VpathProfile
Service Node as Router/Default Gateway	Host Networks	N/A	defaultNetworkL2Profile
Load Balancer	Host Networks	N/A	defaultNetworkIpv4TfStaticRoutingLBProfile/ defaultNetworkIpv4TfDynamicRoutingLBProfile/ defaultNetworkIpv4EfDynamicRoutingLBProfile/ defaultNetworkIpv4EfStaticRoutingLBProfile
		Static	serviceNetworkIpv4TfStaticRoutingLBProfile
	Tenant Service Network	Dynamic	serviceNetworkIpv4DynamicRoutingLBProfile
Load Balancer + Edge Firewall	Host Networks	N/A	defaultNetworkIpv4EfChainLBESProfile/ defaultNetworkIpv4TfChainLBESProfile
	Load Balancer Service Network	Dynamic	serviceNetworkIpv4ESChainLBESProfile
	Edge Firewall Service Network	Dynamic	serviceNetworkIpv4LBChainLBESProfile

Universal config profile selection for Load Balancer and Edge Services

From Cisco DCNM Release 7.1.1, the universal configuration profiles are to decouple network profiles from VRF profiles, and therefore, allowing you to choose the network/VRF profile combination which best suits your requirement.

The table below shows how to use those universal profiles for a few cases with load balancers and (tenant) edge routers, depending on how such services are deployed.

Table 6-3

Load balancer	Edge Router	Internal vrf profile	External vrf profile	Internal Host network profile	Internal LB service network profile	Internal ES service network profile	External service network profile
No	No	vrf-common-universal	N/A	defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles	N/A	N/A	N/A
Yes, static routing	No	vrf-common-universal-static	N/A	defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles	serviceNetworkUniversalTfStaticRoutingProfile	N/A	N/A
Yes, dynamic routing	No	vrf-common-universal-dynamic-LB-ES	N/A	defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles	serviceNetworkUniversalDynamicRoutingLBPProfile	N/A	N/A
No	Yes, static routing	vrf-common-universal	vrf-common-universal-external-static	defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles	N/A	serviceNetworkUniversalTfStaticRoutingProfile	externalStaticRoutingESProfile
No	Yes, dynamic routing	vrf-common-universal-dynamic-LB-ES	vrf-common-universal-external-dynamic-ES	defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles	N/A	serviceNetworkUniversalDynamicRoutingESProfile	externalDynamicRoutingESProfile

Table 6-3

Load balancer	Edge Router	Internal vrf profile	External vrf profile	Internal Host network profile	Internal LB service network profile	Internal ES service network profile	External service network profile
Yes, static routing	Yes, static routing	vrf-common-universal-static	vrf-common-universal-external-static	defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles	serviceNetworkUniversalTfStaticRoutingProfile	serviceNetworkUniversalTfStaticRoutingProfile	externalUniversalTfStaticRoutingProfile
Yes, static routing	Yes, dynamic routing	vrf-common-universal-static	vrf-common-universal-external-dynamic-ES	defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles	serviceNetworkUniversalTfStaticRoutingProfile	serviceNetworkUniversalESChainStaticLBESProfile	externalUniversalTfStaticRoutingProfile
Yes, dynamic routing	Yes, static routing	vrf-common-universal-dynamic-LB-ES	vrf-common-universal-external-static	defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles	serviceNetworkUniversalDynamicRoutingLBPProfile	serviceNetworkUniversalTfStaticRoutingProfile	externalUniversalTfStaticRoutingProfile
Yes, dynamic routing	Yes, dynamic routing	vrf-common-universal-dynamic-LB-ES	vrf-common-universal-external-dynamic-ES	defaultUniversalTfProfile, defaultUniversalEfProfile, other profiles	serviceNetworkUniversalDynamicRoutingLBPProfile	serviceNetworkUniversalESChainLBESProfile	externalUniversalTfStaticRoutingProfile

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 firmware.

**Note**

You need to stop and restart AMQP on both DCNM's server in HA within 30 seconds, otherwise AMQP may not start.

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 DCNM Open Virtual Appliance are as follows:

```
/root/utls/vCDclient.py
```

```
/root/utls/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 DCNM Open Virtual Appliance installs LDAP that serves as an asset database to the switches.

**Note**

From Cisco DCNM Release 7.1.x, during installation of Virtual Appliances, Secure LDAP is enabled by default on Port 636.

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:

- 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 installation, you define the IP Address for the inside fabric management address or OOB management network and the subnets associated with the Cisco Programmable Fabric management.

**Note**

You should always configure DHCP through Cisco DCNM web UI by choosing: **UI > Configure > 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: **Configure > LAN Fabric Settings > General**.



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 6-4](#). See the “[XMPP User and Group Management](#)” section on page 6-10 for information.

Managing Applications

You can manage the applications for Cisco Programmable Fabric in the Cisco DCNM 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 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.

This section includes the following:

- [Verifying the Application Status after Deployment, page 6-9](#)
- [Stopping, Starting, and Resetting Applications, page 6-9](#)
- [XMPP User and Group Management, page 6-10](#)
- [Change from Local Database to an External Database, page 6-11](#)
- [Change password for Linux root user, page 6-12](#)

Verifying the Application Status after Deployment

After you deploy the OVA/ISO file, you can determine the status of the applications that were deployed in the 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.

DETAILED STEPS

- Step 1** Open up an SSH session:
- Enter the **ssh root DCNM network IP address** command.
 - 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	0	2635m	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

DHCP Status

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
===	=====	===	==	=====	===	===	=	=====	=====	=====	=====
1668	dhcpcd	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 ]
```

**Note**

From Cisco DCNM Release 7.1.x, when you stop an application by using the **appmgr stop <<app_name>>** command, the application will not start during successive reboots.

For example, if DHCP is stopped by using the **appmgr stop dhcp** command, and the OS is rebooted, the DHCP application will still be down after the OS is up and running.

To start again, use the command **appmgr start dhcp**. The DHCP application will be started after reboots also. This is to ensure that when an environment uses an application that is not packaged as part of the virtual appliance (like CPNR instead of DHCP), the application locally packaged with the virtual appliance will not interfere with its function after any OS reboots.

**Note**

When a DCNM appliance (ISO/OVA) is deployed, the Cisco SMIS component will not get started by default. However, this component can be managed using the appmgr CLI: **appmgr start/stop dcnm-smis** **appmgr start/stop dcnm** will start/stop only the DCNM web component.

XMPP User and Group Management

XMPP in-band registration is disabled in the Cisco DCNM 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 6-4](#).

**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 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 **Configure > LAN Fabric Settings > General**.

Table 6-4 CLI Commands for XMPP user and group management

CLI Commands	Description
appmgr add_user xmpp -u username -p password	<p>-u is XMPP user ID without the domain name</p> <p>-p is XMPP user password (if user already exists, the password will be updated)</p> <p>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</p>
appmgr add_group xmpp -u username -p password -g group-name	<p>-u is XMPP user ID without the domain name</p> <p>-p is XMPP password</p> <p>-g XMPP group to be created, if it does not exist already</p> <p>For example, appmgr add_group xmpp -u admin -g dcnm-dfa creates an XMPP group 'dcnm-dfa' created by Jabber ID 'admin@xyz.com'</p>
appmgr list_users xmpp	Lists the XMPP users
appmgr list_groups xmpp	Lists the XMPP groups
appmgr delete_user xmpp -u user	<p>Deletes the XMPP user.</p> <p>You cannot delete a user if any group created by that user still exists in the XMPP database.</p>
appmgr delete_group xmpp -u username -p password -g group	<p>Deletes the XMPP group</p> <p>-u is the XMPP user ID without the domain name</p> <p>-p is the XMPP user password</p> <p>-g is the XMPP group to be deleted</p> <p>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.'</p> <p>You cannot delete a group created by one user with the credentials of another user.</p>

Change from Local Database to an External Database

Cisco recommends that you use an external Oracle database if you have large number of devices to be managed by your Cisco DCNM. Perform the following procedures to change from local database to an external database, when required.

Reconfigure DCNM to use an external Oracle database



Note Reconfiguring Cisco DCNM to use an external Oracle database is supported only for OVA/ISO deployments.

Perform the following steps to reconfigure the DCNM to use an external Oracle database.

-
- Step 1** Stop DCNM server.
- Step 2** To configure the DCNM to use an external Oracle database, use **appmgr update dcnm -u <oracle_jdbc_url> -n <oracle_db_user> -p <oracle_db_password>** command.
- where,
- u <oracle_jdbc_url> : Oracle JDBC URL, example, jdbc:oracle:thin:@1.2.3.4:1521:XE
 - n <oracle_db_user> : Database Username
 - p <oracle_db_password>: Database User Password
- Step 3** Start DCNM server.
-

Change password for Linux root user

Use the following CLI command to change the password of the Linux root user.

```
appmgr change_pwd ssh root
```

At the prompt, enter the new password:

```
Enter the new ssh password for root user : <new password>
```

```
Enter it again for verification: <new password>
```



Note

Do not use the following characters in your password: "&,\$%' and <SPACE>.

Backing Up Cisco DCNM and Application Data

You can use the **appmgr backup** command to back up Cisco DCNM and application data. See the following sections for details about backing up data.



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 6-5 CLI Commands for backing up application data

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

Collecting Log Files

Log files are needed to troubleshoot the Cisco DCNM installation.

Cisco DCNM-SAN is installed under `<DCNM_HOME>`. The following are the default installation directories:

- Microsoft Windows—`C:\Program Files\Cisco Systems`



Note In Microsoft Windows, when a Cisco DCNM 32-bit installer is used for installation in a 64-bit environment, the default installation directory is `C:\Program Files <x86>\Cisco Systems`.

- Linux—`/usr/local/cisco`
- OVA/ISO—`appmgr tech_support` command

Once the Cisco DCNM installation is complete, you can find the installer logs under:

- Microsoft Windows—*USER_HOME\dcnm_installer.log*
- Linux—*/root/dcnm_installer.log*
- OVA/ISO— **appmgr tech_support** command

**Note**

When you have several Cisco DCNM installations on the same machine, the installer preserves the logs with a timestamp. When the installation is done in the debug mode, the *dcnm_installer.log* file is not available.

The PostgreSQL install logs are available under:

- Microsoft Windows—*USER_TEMP_DIR\install-postgresql.log*
- Linux: */tmp/install-postgresql.log*
- OVA/ISO— **appmgr tech_support** command

The Cisco DCNM-SAN server logs are available under:

- Microsoft Windows—*DCNM_HOME>\dcm\jboss\server\fm\logs*
- Linux—*DCNM_HOME/dcm/jboss/server/fm/logs*
- OVA/ISO— **appmgr tech_support** command

**Note**

For Cisco DCNM Virtual Appliance, 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.

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 DCNM Open Virtual Appliance.

**Note**

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

DETAILED STEPS

- Step 1** Use the **appmgr backup** command on the existing Open Virtual Appliance.

- Step 2** Transfer the backup file to any repository.
- Step 3** Power off the first Open Virtual Appliance.
- Step 4** Deploy another Open Virtual Appliance with the same network configuration as the existing one, using the same IP/Netmask/Gateway/Hostname/DNS.
- Step 5** Transfer the backup file to the second Open Virtual Appliance.
- Step 6** Run the **appmgr restore** with the new backup on the new Open Virtual Appliance.



Note See [Table 6-6](#) for a list of CLI commands to restore applications.

Table 6-6 CLI commands for restoring applications

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

Updating the SFTP Server Address for IPv6

After deploying the DCNM OVA/ISO successfully with EFM IPv4 and IPv6, by default the SFTP address is pointed to IPv4 only. You need to change the IPv6 address manually in the following two places:

- In the DCNM Web Client, choose **Administration > Server Properties** and then update the below fields to IPv6 and click the **Apply Changes** button.

```
#
# GENERAL>xFTP CREDENTIAL
#
# xFTP server's ip address for copying switch files:
server.FileServerAddress
```

- Log in to the DCNM through ssh and update the SFTP address with IPv6 manually in the server.properties file (/usr/local/cisco/dcm/fm/conf/server.properties).

```
# xFTP server's ip address for copying switch files:
server.FileServerAddress=2001:420:5446:2006::224:19
```

