



# Managing Utility Services After DCNM Deployment

This chapter describes how to verify and manage all of the utility services that provide DC3 (Programmable Fabric) central point of management functions after the DCNM is deployed.

*Table 1: Cisco DCNM Utility Services*

Category	Application	Username	Password	Protocol Implemented
Network Management	Data Center Network Manager	admin	User choice <sup>1</sup>	Network Management

<sup>1</sup> User choice refers to the administration password entered by the user during the deployment.

This chapter contains the following sections:

- [Editing Network Properties Post DCNM Installation, on page 1](#)
- [Utility Services Details, on page 13](#)
- [Managing Applications and Utility Services , on page 14](#)
- [Updating the SFTP Server Address for IPv6, on page 16](#)

## Editing Network Properties Post DCNM Installation

The Cisco DCNM OVA or the ISO installation consists of 3 network interfaces:

- dcnm-mgmt network (eth0) interface

This network provides connectivity (SSH, SCP, HTTP, HTTPS) to the Cisco DCNM Open Virtual Appliance. Associate this network with the port group that corresponds to the subnet that is associated with the DCNM Management network.

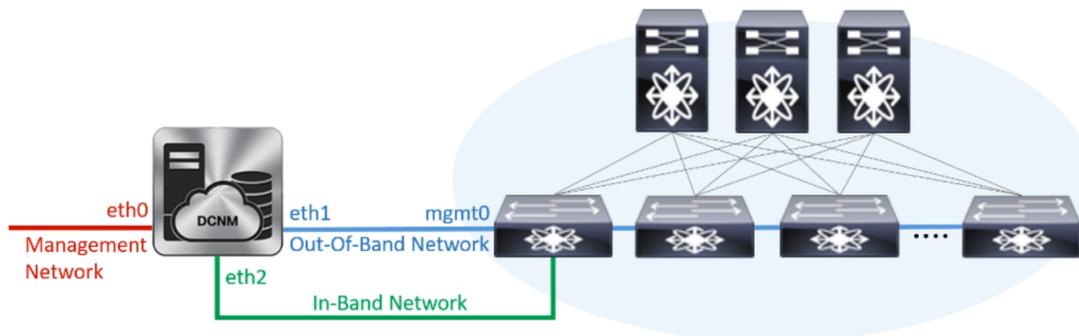
- enhanced-fabric-mgmt (eth1) interface

This network provides enhanced fabric management of Nexus switches. Associate this network with the port group that corresponds to management network of leaf and spine switches.

- enhanced-fabric-inband (eth2) interface

This network provides in-band connection to fabric. Associate this network with the port group that corresponds to a fabric in-band connection.

The following figure shows the network diagram for the Cisco DCNM Management interfaces.



During Cisco DCNM installation for your deployment type, you can configure these interfaces. However, from Cisco DCNM Release 11.2(1), you can edit and modify the network settings post installation.

You can modify the parameters as explained in the following sections:

## Modifying Network Properties on DCNM in Standalone Mode



**Note** Execute the following commands on the DCNM Appliance console to avoid a premature session timeout.

To change the Network Properties on Cisco DCNM Standalone setup, perform the following steps:

### Procedure

- 
- Step 1** Initiate a session on the console, using the following command:
- ```
appmgr update network-properties session start
```
- Step 2** Update the Network Properties using the following command:

```
appmgr update network-properties set ipv4 {eth0|eth1|eth2} <ipv4-address> <network-mask> <gateway>
```

**Step 3** View and verify the changes by using the following command:

```
appmgr update network-properties session show {config | changes | diffs}
```

**Step 4** After you validate the changes, apply the configuration using the following command:

```
appmgr update network-properties session apply
```

Wait for a few minutes before you can logon to the Cisco DCNM Web UI using the eth0 Management Network IP address.

---

### Sample Command Output for Modifying Network Parameters in the Cisco DCNM Standalone Setup

The following sample example shows how to modify the network parameters post installation for a Cisco DCNM Standalone setup.

```

dcnm# appmgr update network-properties session start

dcnm# appmgr update network-properties set ipv4 eth0 172.28.10.244 255.255.255.0 172.28.10.1
dcnm# appmgr update network-properties set ipv4 eth1 100.0.0.244 255.0.0.0
dcnm# appmgr update network-properties set ipv4 eth2 2.0.0.251 255.0.0.0 2.0.0.1
*****
WARNING: fabric/poap configuration may need to be changed
manually after changes are applied.
*****

dcnm# appmgr update network-properties session show changes
eth0 IPv4 addr 172.28.10.246/255.255.255.0 -> 172.28.10.244/255.255.255.0
eth1 IPv4 addr 1.0.0.246/255.0.0.0 -> 100.0.0.244/255.0.0.0
eth2 IPv4 addr 10.0.0.246/255.0.0.0 -> 2.0.0.251/255.0.0.0 2.0.0.1

dcnm# appmgr update network-properties session apply
*****
WARNING

Applications of both nodes of the DCNM HA system need to be stopped
for the changes to be applied properly.

PLEASE STOP ALL APPLICATIONS MANUALLY
*****

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
server signaled
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
'tentative' state
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
'tentative' state
*****
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
*****

dcnm# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO: Resource is stopped
Done.

Warning: PID file not written; -detached was passed.

```

```
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
dcnm#
```

## Modifying Network Properties on DCNM in Native HA Mode



**Note** Execute the following commands on the DCNM Appliance console to avoid a premature session timeout. Ensure that you execute the commands in the same order as mentioned in the following steps.

To change the Network Properties on Cisco DCNM Native HA setup, perform the following steps:

### Procedure

- Step 1** Stop the DCNM Applications on the Standby node by using the following command:
- ```
appmgr stop all
```
- Wait until all the applications stop on the Standby node before you go proceed.
- Step 2** Stop the DCNM Applications on the Active node by using the following command:
- ```
appmgr stop all
```
- Step 3** Initiate a session on the Cisco DCNM console of both the Active and Standby nodes by using the following command:
- ```
appmgr update network-properties session start
```
- Step 4** On the Active node, modify the network interface parameters by using the following commands:
- Configure the IP address for eth0, eth1, and eth2 address by using the following command:
 

```
appmgr update network-properties set ipv4 {eth0|eth1|eth2}<ipv4-address> <network-mask>  
<gateway>
```

Enter the new IPv4 or IPv6 address for the interface, along with the subnet mask and gateway IP addresses.
  - Configure the VIP IP address by using the following command:
 

```
appmgr update network-properties set ipv4 {vip0|vip1|vip2}<ipv4-address> <network-mask>
```

Enter the vip0 address for eth0 interface. Enter the vip1 address for eth1 interface. Enter the vip2 address for eth2 interface.
  - Configure the peer IP address by using the following command:
 

```
appmgr update network-properties set ipv4 {peer0|peer1|peer2}<ipv4-address>
```

Enter the eth0 address of the Standby node as peer0 address for Active node. Enter the eth1 address of the Standby node as peer1 address for Active node. Enter the eth2 address of the Standby node as peer2 address for Active node.

- d) View and validate the changes that you have made to the network parameters by using the following command:

```
appmgr update network-properties session show {config | changes | diffs}
```

- Step 5** On the Standby node, modify the network interface parameters using the commands described in [#unique\\_65 unique\\_65\\_Connect\\_42\\_substeps\\_active, on page 4](#).
- Step 6** After you validate the changes, apply the configuration on the Active node by using the following command:  
**appmgr update network-properties session apply**  
 Wait until the prompt returns, to confirm that the network parameters are updated.
- Step 7** After you validate the changes, apply the configuration on the Standby node by using the following command:  
**appmgr update network-properties session apply**
- Step 8** Start all the applications on the Active node by using the following command:  
**appmgr start all**  
**Note** Wait until all the applications are running successfully on the Active node, before proceeding to the next step.
- Step 9** Start all the applications on the Standby node by using the following command:  
**appmgr start all**
- Step 10** Establish peer trust key on the Active node by using the following command:  
**appmgr update ssh-peer-trust**
- Step 11** Establish peer trust key on the Standby node by using the following command:  
**appmgr update ssh-peer-trust**

### Sample Command Output for Modifying Network Parameters in the Cisco DCNM Native HA Setup

The following sample example shows how to modify the network parameters post installation for a Cisco DCNM Native HA setup.



**Note** For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.

```
[root@dcnm2 ~]# appmgr stop all
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.
Stopping and halting node rabbit@dcnm-dcnm2 ...
Note: Forwarding request to 'systemctl enable rabbitmq-server.service'.
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
```

```

Stopped Application Framework...
[root@dcnm2 ~]#

[root@dcnm1 ~]# appmgr stop all
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.
Stopping and halting node rabbit@dcnm1 ...
Note: Forwarding request to 'systemctl enable rabbitmq-server.service'.
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
[root@dcnm-1 ~]#

[root@dcnm1 ~]# appmgr update network-properties session start
[root@dcnm1 ~]#

[root@dcnm2 ~]# appmgr update network-properties session start
[root@dcnm2 ~]#

[root@dcnm1 ~]# appmgr update network-properties set ipv4 eth0 172.28.10.244 255.255.255.0
172.28.10.1
[root@dcnm1 ~]# appmgr update network-properties set ipv4 eth1 1.0.0.244 255.0.0.0 1.0.0.1
*****
WARNING: fabric/poap configuration may need to be changed
manually after changes are applied.
*****
[root@dcnm1 ~]# appmgr update network-properties set ipv4 eth2 2.0.0.244 255.0.0.0 2.0.0.1
[root@dcnm1 ~]# appmgr update network-properties set ipv4 peer0 172.29.10.238
[root@dcnm1 ~]# appmgr update network-properties set ipv4 peer1 1.0.0.238
[root@dcnm1 ~]# appmgr update network-properties set ipv4 peer2 2.0.0.238
[root@dcnm1 ~]# appmgr update network-properties set ipv4 vip0 172.28.10.239 255.255.255.0
[root@dcnm1 ~]# appmgr update network-properties set ipv4 vip1 1.0.0.239 255.0.0.0
[root@dcnm1 ~]# appmgr update network-properties set ipv4 vip2 2.0.0.239 255.0.0.0
[root@dcnm1 ~]# appmgr update network-properties set hostname local dcnm3.cisco.com
[root@dcnm1 ~]# appmgr update network-properties set hostname peer dcnm4.cisco.com
[root@dcnm1 ~]# appmgr update network-properties set hostname vip dcnm5.cisco.com
[root@dcnm1 ~]#

[root@dcnm2 ~]# appmgr update network-properties set ipv4 eth0 172.28.10.238 255.255.255.0
172.28.10.1
[root@dcnm2 ~]# appmgr update network-properties set ipv4 eth1 1.0.0.238 255.0.0.0 1.0.0.1
*****
WARNING: fabric/poap configuration may need to be changed
manually after changes are applied.
*****
[root@dcnm2 ~]# appmgr update network-properties set ipv4 eth2 2.0.0.238 255.0.0.0 2.0.0.1
[root@dcnm2 ~]# appmgr update network-properties set ipv4 peer0 172.29.10.244
[root@dcnm2 ~]# appmgr update network-properties set ipv4 peer1 1.0.0.244
[root@dcnm2 ~]# appmgr update network-properties set ipv4 peer2 2.0.0.244
[root@dcnm2 ~]# appmgr update network-properties set ipv4 vip0 172.28.10.239 255.255.255.0
[root@dcnm2 ~]# appmgr update network-properties set ipv4 vip1 1.0.0.239 255.0.0.0
[root@dcnm2 ~]# appmgr update network-properties set ipv4 vip2 2.0.0.239 255.0.0.0
[root@dcnm2 ~]# appmgr update network-properties set hostname local dcnm3.cisco.com
[root@dcnm2 ~]# appmgr update network-properties set hostname peer dcnm4.cisco.com
[root@dcnm2 ~]# appmgr update network-properties set hostname vip dcnm5.cisco.com
[root@dcnm2 ~]#

[root@dcnm2 ~]#
[root@dcnm1 ~]# appmgr update network-properties session show changes

```

```

eth0 IPv4 addr      172.28.10.246/255.255.255.0  ->  172.28.10.244/255.255.255.0
eth1 IPv4 addr      1.0.0.246/255.0.0.0          ->  1.0.0.244/255.0.0.0
eth1 IPv4 GW        ->  1.0.0.1
eth2 IPv4 addr      /                               ->  2.0.0.244/255.0.0.0
eth2 IPv4 GW        ->  2.0.0.1
Hostname            dcnm1.cisco.com              ->  dcnm3.cisco.com
eth0 VIP            172.28.10.248/24            ->  172.28.10.239/24
eth1 VIP            1.0.0.248/8                ->  1.0.0.239/8
eth2 VIP            /                               ->  2.0.0.239/8
Peer eth0 IP        172.28.10.247            ->  172.29.10.238
Peer eth1 IP        1.0.0.247                ->  1.0.0.238
Peer eth2 IP        ->  2.0.0.238
Peer hostname       dcnm2.cisco.com          ->  dcnm4.cisco.com
VIP hostname        dcnm6.cisco.com          ->  dcnm5.cisco.com

```

```
[root@dcnm1 ~]# apmgr update network-properties session show config
```

```
===== Current configuration =====
```

```

Hostname dcnm1.cisco.com
NTP Server      1.ntp.esl.cisco.com
DNS Server      171.70.168.183,1.0.0.246
eth0 IPv4 addr  172.28.10.246/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr  1.0.0.246/255.0.0.0
eth1 IPv4 GW
eth1 IPv6 addr
eth1 IPv6 GW
eth2 IPv4 addr  /
eth2 IPv4 GW
eth2 IPv6 addr
eth2 IPv6 GW
Peer hostname   dcnm2.cisco.com
Peer eth0 IP    172.28.10.247
Peer eth1 IP    1.0.0.247
Peer eth2 IP
Peer eth0 IPv6
Peer eth1 IPv6
eth0 VIP        172.28.10.248/24
eth1 VIP        1.0.0.248/8
eth2 VIP        /
eth0 VIPv6      /
eth1 VIPv6      /
VIP hostname    dcnm6.cisco.com

```

```
===== Session configuration =====
```

```

Hostname dcnm3.cisco.com
NTP Server      1.ntp.esl.cisco.com
DNS Server      171.70.168.183,1.0.0.246
eth0 IPv4 addr  172.28.10.244/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr  1.0.0.244/255.0.0.0
eth1 IPv4 GW    1.0.0.1
eth1 IPv6 addr
eth1 IPv6 GW
eth2 IPv4 addr  2.0.0.244/255.0.0.0
eth2 IPv4 GW    2.0.0.1
eth2 IPv6 addr
eth2 IPv6 GW
Peer hostname   dcnm4.cisco.com
Peer eth0 IP    172.29.10.238
Peer eth1 IP    1.0.0.238

```

```

Peer eth2 IP      2.0.0.238
Peer eth0 IPv6
Peer eth1 IPv6
eth0 VIP         172.28.10.239/24
eth1 VIP         1.0.0.239/8
eth2 VIP         2.0.0.239/8
eth0 VIPv6 /
eth1 VIPv6 /
VIP hostname dcnm5.cisco.com
[root@dcnm1 ~]#

[root@dcnm2 ~]# appmgr update network-properties session show changes
eth0 IPv4 addr   172.28.10.247/255.255.255.0   -> 172.28.10.238/255.255.255.0
eth1 IPv4 addr   1.0.0.247/255.0.0.0                       -> 1.0.0.238/255.0.0.0
eth1 IPv4 GW     /                               -> 1.0.0.1
eth2 IPv4 addr   /                               -> 2.0.0.238/255.0.0.0
eth2 IPv4 GW     /                               -> 2.0.0.1
Hostname         dcnm2.cisco.com              -> dcnm4.cisco.com
eth0 VIP         172.28.10.248/24              -> 172.28.10.239/24
eth1 VIP         1.0.0.248/8                  -> 1.0.0.239/8
eth2 VIP         /                            -> 2.0.0.239/8
Peer eth0 IP     172.28.10.246                 -> 172.29.10.244
Peer eth1 IP     1.0.0.246                    -> 1.0.0.244
Peer eth2 IP     /                            -> 2.0.0.244
Peer hostname    dcnm1.cisco.com              -> dcnm3.cisco.com
VIP hostname     dcnm6.cisco.com              -> dcnm5.cisco.com
[root@dcnm2 ~]# appmgr update network-properties session show configuration
===== Current configuration =====
Hostname dcnm2.cisco.com
NTP Server      1.ntp.esl.cisco.com
DNS Server      171.70.168.183,1.0.0.247
eth0 IPv4 addr  172.28.10.247/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr  1.0.0.247/255.0.0.0
eth1 IPv4 GW
eth1 IPv6 addr
eth1 IPv6 GW
eth2 IPv4 addr  /
eth2 IPv4 GW
eth2 IPv6 addr
eth2 IPv6 GW
Peer hostname   dcnm1.cisco.com
Peer eth0 IP    172.28.10.246
Peer eth1 IP    1.0.0.246
Peer eth2 IP
Peer eth0 IPv6
Peer eth1 IPv6
eth0 VIP        172.28.10.248/24
eth1 VIP        1.0.0.248/8
eth2 VIP        /
eth0 VIPv6     /
eth1 VIPv6     /
VIP hostname    dcnm6.cisco.com

===== Session configuration =====
Hostname dcnm4.cisco.com
NTP Server      1.ntp.esl.cisco.com
DNS Server      171.70.168.183,1.0.0.247
eth0 IPv4 addr  172.28.10.238/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 IPv6 addr
eth0 IPv6 GW

```

```

eth1 IPv4 addr    1.0.0.238/255.0.0.0
eth1 IPv4 GW     1.0.0.1
eth1 IPv6 addr
eth1 IPv6 GW
eth2 IPv4 addr    2.0.0.238/255.0.0.0
eth2 IPv4 GW     2.0.0.1
eth2 IPv6 addr
eth2 IPv6 GW
Peer hostname dcnm3.cisco.com
Peer eth0 IP     172.29.10.244
Peer eth1 IP     1.0.0.244
Peer eth2 IP     2.0.0.244
Peer eth0 IPv6
Peer eth1 IPv6
eth0 VIP         172.28.10.239/24
eth1 VIP         1.0.0.239/8
eth2 VIP         2.0.0.239/8
eth0 VIPv6      /
eth1 VIPv6      /
VIP hostname dcnm5.cisco.com
[root@dcnm2 ~]#

```

```

[root@dcnm1 ~]# appmgr update network-properties session apply
*****

```

WARNING

Applications of both nodes of the DCMN HA system need to be stopped for the changes to be applied properly.

PLEASE STOP ALL APPLICATIONS MANUALLY

```
*****
```

Have applications been stopped? [y/n]: **y**

Applying changes

DELETE 1

Node left the swarm.

Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties

log4j:WARN No appenders could be found for logger (fms.db).

log4j:WARN Please initialize the log4j system properly.

log4j:WARN See <http://logging.apache.org/log4j/1.2/faq.html#noconfig> for more info.

UPDATE 1

UPDATE 1

DELETE 1

server signaled

INFO : [ipv6\_wait\_tentative] Waiting for interface eth0 IPv6 address(es) to leave the 'tentative' state

INFO : [ipv6\_wait\_tentative] Waiting for interface eth0 IPv6 address(es) to leave the 'tentative' state

```
*****
```

Please run 'appmgr start afw; appmgr start all' to restart your nodes.

```
*****
```

```
*****
```

Please run 'appmgr update ssh-peer-trust' on the peer node.

```
*****
```

```
[root@dcnm1 ~]#
```

```

[root@dcnm2 ~]# appmgr update network-properties session apply
*****

```

WARNING

Applications of both nodes of the DCMN HA system need to be stopped for the changes to be applied properly.

PLEASE STOP ALL APPLICATIONS MANUALLY

```
*****
```

Have applications been stopped? [y/n]: **y**

```

Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
afwnetplugin:0.1
server signaled
*****
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
*****
*****
Please run 'appmgr update ssh-peer-trust' on the peer node.
*****
[root@dcnm2 ~]#

```

## Step 7

```

[root@dcnm1 ~]# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO: Resource is stopped
Done.
Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
[root@dcnm1 ~]#

```

Waiting for dcnm1 to become active again.

```

[root@dcnm2 ~]# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO: Resource is stopped
Done.
Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
[root@dcnm2 ~]#

```

```

[root@dcnm1 ~]# appmgr update ssh-peer-trust
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

```

Now try logging into the machine, with: "ssh -o 'StrictHostKeyChecking=no' '172.28.10.245'" and check to make sure that only the key(s) you wanted were added.

```

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh -o 'StrictHostKeyChecking=no' '100.0.0.245'"
and check to make sure that only the key(s) you wanted were added.

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh -o 'StrictHostKeyChecking=no'
'dcnm2.cisco.com'"
and check to make sure that only the key(s) you wanted were added.

[root@dcnm1 ~]#

[root@dcnm2 ~]# appmgr update ssh-peer-trust
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh -o 'StrictHostKeyChecking=no' '172.28.10.244'"
and check to make sure that only the key(s) you wanted were added.

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh -o 'StrictHostKeyChecking=no' '100.0.0.244'"
and check to make sure that only the key(s) you wanted were added.

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh -o 'StrictHostKeyChecking=no'
'dcnm1.cisco.com'"
and check to make sure that only the key(s) you wanted were added.

[root@dcnm2 ~]#

```

## Changing the DCNM Server Password Post DCNM Installation

The password to access Cisco DCNM Web UI is configured while installing the Cisco DCNM for your deployment type. However, you can modify this password post installation also, if required.

To change the password post installation, perform the following steps:

### Procedure

- 
- Step 1** Stop the applications using the **appmgr stop all** command.  
Wait until all the applications stop running.
  - Step 2** Change the password for the management interface by using the **appmgr change\_pwd ssh {root|poap|sysadmin}[password]** command.

Ensure that the new password adheres to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:

- It must be at least 8 characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password: <SPACE> " & \$ % ' ^ = < > ; : ` \ | / , . \*

**Step 3** Start the application using the **appmgr start all** command.

---

## Changing the DCNM Database Password on Standalone Setup

To change the Postgres database password on Cisco DCNM Standalone setup, perform the following steps:

### Procedure

---

- Step 1** Stop all the applications using the **appmgr stop all** command.  
Ensure that all the applications have stopped using the **appmgr status all** command.
- Step 2** Change the Postgres password by using the **appmgr change\_pwd db** command.  
Provide the new password at the prompt.
- Step 3** Start the application using the **appmgr start all** command.  
Ensure that all the applications have started using the **appmgr status all** command.
- 

### Example

```
dcnm# appmgr stop all
dcnm# appmgr change_pwd db <<new-password>>
dcnm# appmgr start all
```

## Changing the DCNM Database Password on Native HA Setup

To change the Postgres database password on Cisco DCNM Native HA setup, perform the following steps:

### Procedure

---

- Step 1** Stop all the applications on the Standby appliance using the **appmgr stop all** command.  
Ensure that all the applications have stopped using the **appmgr status all** command.
- Step 2** Stop all the applications on the Active appliance using the **appmgr stop all** command.

Ensure that all the applications have stopped using the **appmgr status all** command.

**Step 3** Change the Postgres password by using the **appmgr change\_pwd db** command on both Active and Standby nodes.

Ensure that you provide the same password at the prompt.

**Step 4** Start the applications on the Active appliance, using the **appmgr start all** command.

Ensure that all the applications have stopped using the **appmgr status all** command.

**Step 5** Start the applications on the Standby appliance, using the **appmgr start all** command.

Ensure that all the applications have stopped using the **appmgr status all** command.

---

### Example

Let us consider Active and standby as **dcnm1** and **dcnm2**, respectively.

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

dcnm1# appmgr change_pwd db <<new-password>>
dcnm2# appmgr change_pwd db <<new-password>>

dcnm1# appmgr start all
dcnm2# appmgr start all
```

## Utility Services Details

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

### 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://<<hostname/IP address>>`.



---

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

---

### Orchestration

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 <https://www.rabbitmq.com/documentation.html>.

---

## 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.

- 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.

## Managing Applications and Utility Services

You can manage the applications and utility services 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 and Utility Services Status after Deployment

After you deploy the OVA/ISO file, you can determine the status of various applications and utility services 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.

### Procedure

- 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 by using the following command:  
**appmgr status all**

#### Example:

```
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 dhcpd 20 0 46356 3724 408 S 0.0 0.0 0:05.23 dhcp
```

## Stopping, Starting, and Resetting Utility Services

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

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

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

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

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

- To restart an application use the **appmgr restart** 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 or stop only the DCNM web component.

---

## 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
```