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 [1]	Network Management

[1] 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

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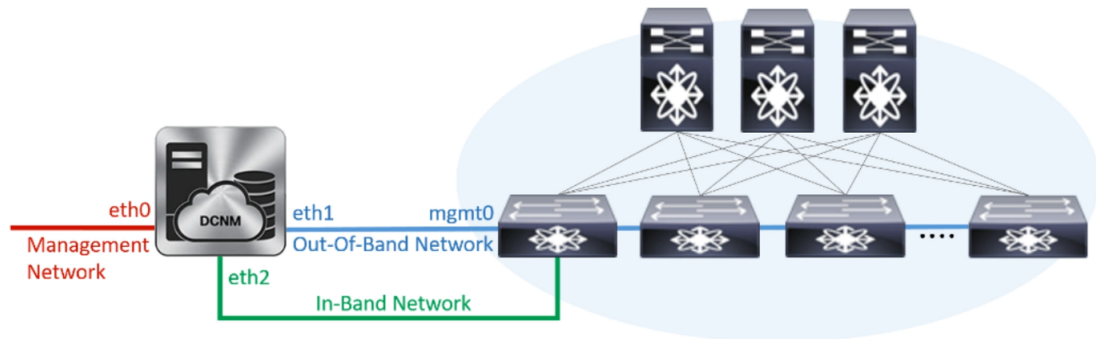
During Cisco DCNM installation for your deployment type, you can configure these interfaces. However, from Cisco DCNM Release 11.2(1), you can edit and modify the network settings post installation.

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

Modifying Network Interfaces (eth0 and eth1) Post DCNM Installation

Along with the eth0 and eth1 IP address (IPv4 and\or IPv6), you can also modify the DNS and the NTP server configuration using the **appmgr update network-properties** command.

For step-by-step instructions on how to modify the network parameters using the **appmgr update network-properties** commands, see the following sections.

- Modifying Network Properties on DCNM in Standalone Mode, on page 2

  Sample Command Output for Modifying Network Parameters in the Cisco DCNM Standalone Setup, on page 3

- Modifying Network Properties on DCNM in Native HA Mode, on page 4

  Sample Command Output for Modifying Network Parameters in the Cisco DCNM Native HA Setup, on page 5

Modifying Network Properties on DCNM in Standalone Mode

The following sample shows the output for the **appmgr update network-properties** command for a Cisco DCNM Standalone Appliance.

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

1. Initiate a session on the console, using the following command:

   appmgr update network-properties session start

2. Update the Network Properties using the following command:

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

   Enter the new IPv4 address for the Management (eth0) interface, along with the subnet mask and gateway IP addresses.

3. View and verify the changes by using the following command:

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

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
*******************************************************************
 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

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

The following sample shows output to modify the network parameters using the **appmgr update network-properties** command for a Cisco DCNM Native HA Appliance.

Note
- Execute the following commands on the DCNM Active and Standby node console to avoid premature session timeout.

- Ensure that you execute the commands in the same order as mentioned in the following steps.

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.

2. Stop the DCNM Applications on the Active node by using the following command:

   appmgr stop all

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

4. On the Active node, modify the network interface parameters by using the following commands:

   1. Configure the IP address for eth0 and eth1 address by using the following command:

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

      Enter the new IPv4 or IPv6 address for the eth1 interface, along with the subnet mask and gateway IP addresses.

   2. Configure the VIP IP address by using the following command:

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

      Enter the vip0 address for eth0 interface. Enter the vip1 address for eth1 interface.

   3. Configure the peer IP address by using the following command:

      appmgr update network-properties set ipv4 {peer0|peer1}<*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.

4. 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*}

   View the changes that you have configured by using the following command:

5. On the Standby node, modify the network interface parameters using the commands described in Step 4.

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.

7. After you validate the changes, apply the configuration on the Standby node by using the following command:

   appmgr update network-properties session apply

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.

9. Start all the applications on the Standby node by using the following command:

   appmgr start all

10. Establish peer trust key on the Active node by using the following command:

    appmgr update ssh-peer-trust

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@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@dcnm1]#

[root@dcnm1]# appmgr update network-properties session start
[root@dcnm2]# appmgr update network-properties session start

[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 100.0.0.244 255.0.0.0
******************************************************************
 WARNING: fabric/poap configuration may need to be changed
 manually after changes are applied.
******************************************************************
[root@dcnm1]# appmgr update network-properties set ipv4 vip0 172.28.10.238 255.255.255.0
[root@dcnm1]# appmgr update network-properties set ipv4 vip1 100.0.0.238 255.0.0.0
[root@dcnm1]# appmgr update network-properties set ipv4 peer0 172.28.10.245
[root@dcnm1]# appmgr update network-properties set ipv4 peer1 100.0.0.245
[root@dcnm1]# appmgr update network-properties session show changes

[root@dcnm2]# appmgr update network-properties set ipv4 eth0 172.28.10.245 255.255.255.0
172.28.10.1
[root@dcnm2]# appmgr update network-properties set ipv4 eth1 100.0.0.245 255.0.0.0
******************************************************************
 WARNING: fabric/poap configuration may need to be changed
 manually after changes are applied.
******************************************************************
[root@dcnm2]# appmgr update network-properties set ipv4 vip0 172.28.10.238 255.255.255.0
[root@dcnm2]# appmgr update network-properties set ipv4 vip1 100.0.0.238 255.0.0.0
[root@dcnm2]# appmgr update network-properties set ipv4 peer0 172.28.10.244
[root@dcnm2]# appmgr update network-properties set ipv4 peer1 100.0.0.244
[root@dcnm2]# appmgr update network-properties session show changes

[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          ->  100.0.0.244/255.0.0.0
eth0 VIP        172.28.10.248/24             ->  172.28.10.238/24
eth1 VIP        1.0.0.248/8                  ->  100.0.0.238/8
Peer eth0 IP    172.28.10.247                ->  172.28.10.245
Peer eth1 IP    1.0.0.245                    ->  100.0.0.245

[root@dcnm1]# appmgr update network-properties session show config
======= Current configuration ======
```

```
NTP Server      1.ntp.esl.cisco.com
eth0 IPv4 addr  172.28.10.246/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 DNS        171.70.168.183
eth0 IPv6 addr  2001:420:284:2004:4:112:210:20/112
eth0 IPv6 GW    2001:420:284:2004:4:112:210:1
eth1 IPv4 addr  1.0.0.246/255.0.0.0
eth1 IPv4 GW
eth1 DNS        1.0.0.246
eth1 IPv6 addr
eth2 IPv4 addr  /
eth2 IPv4 GW
Peer eth0 IP    172.28.10.247
Peer eth1 IP    1.0.0.247
Peer eth2 IP
eth0 VIP        172.28.10.248/24
eth1 VIP        1.0.0.248/8
eth2 VIP        /
eth0 VIPv6      /
eth1 VIPv6      /

====== Session configuration ======
NTP Server      1.ntp.esl.cisco.com
eth0 IPv4 addr  172.28.10.244/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 DNS        171.70.168.183
eth0 IPv6 addr  2001:420:284:2004:4:112:210:20/112
eth0 IPv6 GW    2001:420:284:2004:4:112:210:1
eth1 IPv4 addr  100.0.0.244/255.0.0.0
eth1 IPv4 GW
eth1 DNS        1.0.0.246
eth1 IPv6 addr
eth2 IPv4 addr  /
eth2 IPv4 GW
Peer eth0 IP    172.28.10.245
Peer eth1 IP    100.0.0.245
Peer eth2 IP
eth0 VIP        172.28.10.238/24
eth1 VIP        100.0.0.238/8
eth2 VIP        /
eth0 VIPv6      /
eth1 VIPv6      /
[root@dcnm1]#

[root@dcnm2]# appmgr update network-properties session show config
======= Current configuration ======
NTP Server      1.ntp.esl.cisco.com
eth0 IPv4 addr  172.28.10.247/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 DNS        171.70.168.183
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr  1.0.0.247/255.0.0.0
eth1 IPv4 GW
eth1 DNS        1.0.0.247
eth1 IPv6 addr
eth2 IPv4 addr  /
eth2 IPv4 GW
Peer eth0 IP    172.28.10.246
Peer eth1 IP    1.0.0.246
Peer eth2 IP
eth0 VIP        172.28.10.248/24
eth1 VIP        1.0.0.248/8
eth2 VIP        /
```

```
eth0 VIPv6       /
eth1 VIPv6       /

====== Session configuration ======
NTP Server      1.ntp.esl.cisco.com
eth0 IPv4 addr  172.28.10.245/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 DNS        171.70.168.183
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr  100.0.0.245/255.0.0.0
eth1 IPv4 GW
eth1 DNS        1.0.0.247
eth1 IPv6 addr
eth2 IPv4 addr  /
eth2 IPv4 GW
Peer eth0 IP    172.28.10.244
Peer eth1 IP    100.0.0.244
Peer eth2 IP
eth0 VIP        172.28.10.238/24
eth1 VIP        100.0.0.238/8
eth2 VIP        /
eth0 VIPv6      /
eth1 VIPv6      /
[root@dcnm2]#

[root@dcnm1]# 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.
**********************************************************************
**********************************************************************
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 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
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]#

[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]#
```

Wait until dcnm1 becomes 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'
'dcnm-247.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'
'dcnm-246.cisco.com'"
and check to make sure that only the key(s) you wanted were added.
[root@dcnm2]#
```

Configuring Enhanced-Fabric-Inband Interface (eth2) Post DCNM Installation

During the DCNM installation, you can configure the In-Band Management interface. You must associate this network with the port group that corresponds to a fabric in-band connection. The In-Band Network provides reachability to the devices via the front-panel ports.

Note   If you need to modify the already configured in-band network (eth2 interface), execute the **ifconfig eth2 0.0.0.0** command and run the **appmgr setup inband** command again.

Note   You cannot use Endpoint Locator and Telemetry features if the eth2 interface is not configured.

To configure the eth2 interface for the in-band management network, use the **appmgr setup inband** command.

The following example shows a sample output for the **appmgr setup inband** command for a Cisco DCNM Standalone Appliance.

```
[root@dcnm]# appmgr setup inband
Configuring Interface for InBand Connectivity...
Please enter the information as prompted:
InBand Physical IP [e.g. 2.2.2.69]: 2.0.0.250
```

```
InBand Network Mask [e.g. 255.255.255.0]: 255.0.0.0
InBand Gateway [e.g. 2.2.2.1]: 2.0.0.1
Validating Inputs ...

You have entered these values..
PIP=2.0.0.250
NETMASK=255.0.0.0
GATEWAY=2.0.0.1

Press 'y' to continue configuration, 'n' to discontinue [y] y
{"ResponseType":0,"Response":"Refreshed"}
{"ResponseType":0,"Response":{"AfwServerEnabled":true,"AfwServerReady":true,"InbandSubnet":"2.0.0.0/8",
"InbandGateway":"2.0.0.1","OutbandSubnet":"0.0.0.0/8","OutbandGateway":"0.0.0.0","UnclusteredMode":true}}

Done.
[root@dcnm]#
```

The following example shows a sample output for the **appmgr setup inband** command for a Cisco DCNM Native HA Appliance.

On Cisco DCNM Primary appliance:

```
[root@dcnm-primary]# appmgr setup inband
Configuring Interface for InBand Connectivity...
Please enter the information as prompted:
InBand Physical IP [e.g. 2.2.2.69]: 2.0.0.244
InBand Network Mask [e.g. 255.255.255.0]: 255.0.0.0
InBand Gateway [e.g. 2.2.2.1]: 2.0.0.1
InBand Virtual IP for HA setup [e.g. 2.2.2.60]: 2.0.0.243
InBand Virtual Network Mask [mandatory for HA setup] [e.g. 255.255.255.0]: 255.0.0.0
Peer Inband IP [mandatory for HA setup] [e.g. 2.2.2.59]: 2.0.0.244
Validating Inputs ...

You have entered these values..
PIP=2.0.0.244
NETMASK=255.0.0.0
GATEWAY=2.0.0.1
VIP=2.0.0.243
VIP_NETMASK=255.0.0.0
PEER_ETH2=2.0.0.244

Press 'y' to continue configuration, 'n' to discontinue [y] y

Done.
[root@dcnm-primary]#
```

On Cisco DCNM Secondary appliance:

```
[root@dcnm-secondary]# appmgr setup inband
Configuring Interface for InBand Connectivity...
Please enter the information as prompted:
InBand Physical IP [e.g. 2.2.2.69]: 2.0.0.245
InBand Network Mask [e.g. 255.255.255.0]: 255.0.0.0
InBand Gateway [e.g. 2.2.2.1]: 2.0.0.1
InBand Virtual IP for HA setup [e.g. 2.2.2.60]: 2.0.0.243
InBand Virtual Network Mask [mandatory for HA setup] [e.g. 255.255.255.0]: 255.0.0.0
Peer Inband IP [mandatory for HA setup] [e.g. 2.2.2.59]: 2.0.0.244
Validating Inputs ...

You have entered these values..
PIP=2.0.0.245
NETMASK=255.0.0.0
GATEWAY=2.0.0.1
```

```
VIP=2.0.0.243
VIP_NETMASK=255.0.0.0
PEER_ETH2=2.0.0.244

Press 'y' to continue configuration, 'n' to discontinue [y] y
HA Role is Active {"ResponseType":0,"Response":"Refreshed"}
Done.

[root@dcnm-secondary]#
```

Changing the DCNM 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}**[*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.

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:

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: **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.

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:

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

b) Enter the administrative password to login.

Step 2   Check the status by using the following command:

appmgr status all

Example:

The following sample if taken from Cisco DCNM for Media Controller Deployment.

```
dcnm# appmgr status all

DCNM v11 will only use HTTPS. Insecure access via HTTP is disabled.
Please use the url https://<DCNM-IP-ADDRESS> or https://<HOSTNAME> to launch the DCNM UI.

DCNM Status

  PID  USER       PR  NI   VIRT    RES    SHR  S  %CPU %MEM   TIME+   COMMAND
  ===  ====       ==  ==  ======= ======  ===== =  ==== ====   ======= =======
27724 root        20   0   12.2g   3.9g  49328 S   0.0 16.6  60:24.10 java

Elasticsearch Status

  PID  USER       PR  NI   VIRT    RES    SHR  S  %CPU %MEM   TIME+   COMMAND
  ===  ====       ==  ==  ======= ======  ===== =  ==== ====   ======= =======
 2861 elastic+    20   0 6858536 346396  16484 S   6.2  1.4  11:03.40 java

Telemetry Manager Status

  PID  USER       PR  NI   VIRT    RES    SHR  S  %CPU %MEM   TIME+   COMMAND
  ===  ====       ==  ==  ======= ======  ===== =  ==== ====   ======= =======
 2964 root        20   0  796984   5060   3416 S   0.0  0.0   1:06.11 telemetry-mgr.b

PMN Telemetry Status

  PID  USER       PR  NI   VIRT    RES    SHR  S  %CPU %MEM   TIME+   COMMAND
  ===  ====       ==  ==  ======= ======  ===== =  ==== ====   ======= =======
 3779 root        20   0   10.6g 233640  16236 S   0.0  1.0   0:06.82 java

TFTP Status

  PID  USER       PR  NI   VIRT    RES    SHR  S  %CPU %MEM   TIME+   COMMAND
  ===  ====       ==  ==  ======= ======  ===== =  ==== ====   ======= =======
30377 root        20   0   27164   1072    820 S   0.0  0.0   0:00.00 xinetd

DHCP Status

  PID  USER       PR  NI   VIRT    RES    SHR  S  %CPU %MEM   TIME+   COMMAND
  ===  ====       ==  ==  ======= ======  ===== =  ==== ====   ======= =======
30416 dhcpd       20   0  105616   5656   3448 S   0.0  0.0   0:25.32 dhcpd
```

```
AMQP Status

 PID USER      PR  NI  VIRT    RES     SHR  S  %CPU %MEM    TIME+  COMMAND
 === ====      ==  == ======= ======  ===== =  ==== ====   ======= =======
32157 rabbitmq  20   0 5996960  78564   4272 S   0.0  0.3   9:30.39 beam.smp
```

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.