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, on page 1
- Convert Standalone Setup to Native-HA Setup, on page 25
- Utility Services Details, on page 29
- Managing Applications and Utility Services , on page 30
- Updating the SFTP Server Address for IPv6, on page 32

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.

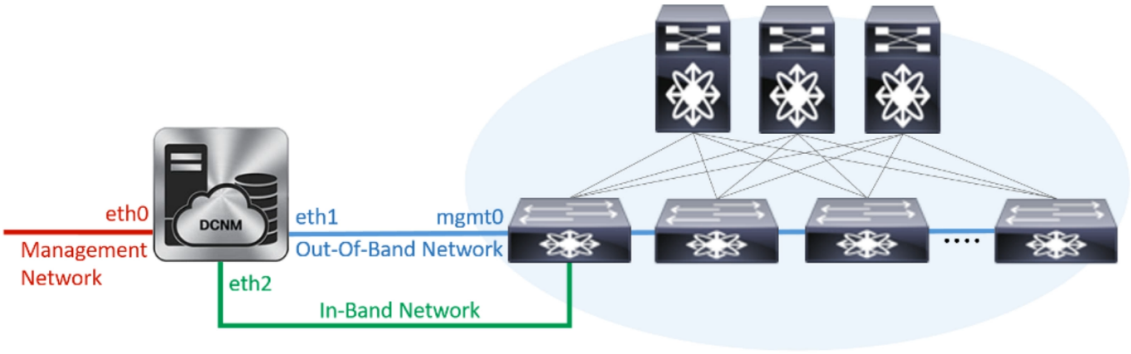
- enhanced-fabric-mgmt (eth1) interface

  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.

Note We recommend that you use **appmgr** commands to update network properties. Do not restart network interfaces manually.

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 6

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:

   a. 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.

b. 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.

c. 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.

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*}

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]#
```

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.

Note Native HA nodes must be considered as a single entity. When you change the Active node eth1 IP address, you must also change the Standby node eth1 IP address.

When you change the eth0 IP address in any node, you must change the eth2 IP address for that node.

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:

a) 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.

b) 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.

c) 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 procedure in Step Step 4, on page 14.

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 ~]# appmgr 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 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 ~]#


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 on Standalone Setup

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.

Example

```
dcnm# appmgr stop all

dcnm# appmgr change_pwd ssh root <<new-password>>
dcnm# appmgr change_pwd ssh poap <<new-password>>
dcnm# appmgr change_pwd ssh sysadmin <<new-password>>

dcnm# appmgr start all
```

Changing the DCNM Server Password on Native HA Setup

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 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 password for the management interface by using the **appmgr change_pwd ssh {root|poap|sysadmin}**[*password*] command. on both Active and Standby nodes.

Note You provide the same password for both the nodes at the prompt.

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

Ensure that all the applications have started 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 started 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 ssh root <<new-password>>
dcnm1# appmgr change_pwd ssh poap <<new-password>>
dcnm1# appmgr change_pwd ssh sysadmin <<new-password>>

dcnm2# appmgr change_pwd ssh root <<new-password>>
dcnm2# appmgr change_pwd ssh poap <<new-password>>
dcnm2# appmgr change_pwd ssh sysadmin <<new-password>>

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

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 started 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 started 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
```

Convert Standalone Setup to Native-HA Setup

To convert an existing Cisco DCNM Standalone setup to a Native HA setup, perform the following steps:

Before you begin

Ensure that the Standalone setup is active and operational, by using the **appmgr show version** command.

```
dcnm# appmgr show version

Cisco Data Center Network Manager
Version: 11.4(1)
Install mode: LAN Fabric
Standalone node. HA not enabled.
dcnm#
```

Procedure

Step 1 On the Standalone setup, launch SSH and enable **root** user access by using the **appmgr root-access permit** command:

```
dcnm# appmgr root-access permit
```

Step 2 Deploy a new DCNM as secondary node. Choose **Fresh installation - HA Secondary**

For example, let us indicate the existing setup as **dcnm1** and the new DCNM as secondary node as **dcnm2**.

Caution If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

Step 3 Configure **dcnm2** as the Secondary node. Paste the URL displayed on the Console tab of **dcnm2** and hit Enter.

A welcome message appears.

a) On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

b) On the Cisco DCNM Installer screen, select **Fresh Installation - HA Secondary** radio button, to install **dcnm2** as Secondary node.

Click **Continue**.

c) On the **Install Mode** tab, from the drop-down list, choose the same installation mode that you selected for the Primary node.

Note The HA installation fails if you do not choose the same installation mode as Primary node.

Check the **Enable Clustered Mode** check box, if you have configured the Cisco DCNM Primary in Clustered mode.

Click **Next**.

d) On the **Administration** tab, enter information about passwords.

Note All the passwords must be same as the passwords that you provided while configuring the Primary node.

e) On the **System Settings**, configure the settings for the DCNM Appliance.

- In the **Fully Qualified Hostname** field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Hostnames with only digits is not supported.
- In the **DNS Server Address List** field, enter the DNS IP address.

  Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.

  From Release 11.3(1), you can configure more than one DNS server.

  Note If you're using Network Insights applications, ensure that the DNS server is valid and reachable.
- In the **NTP Server Address List** field, enter the IP address of the NTP server.

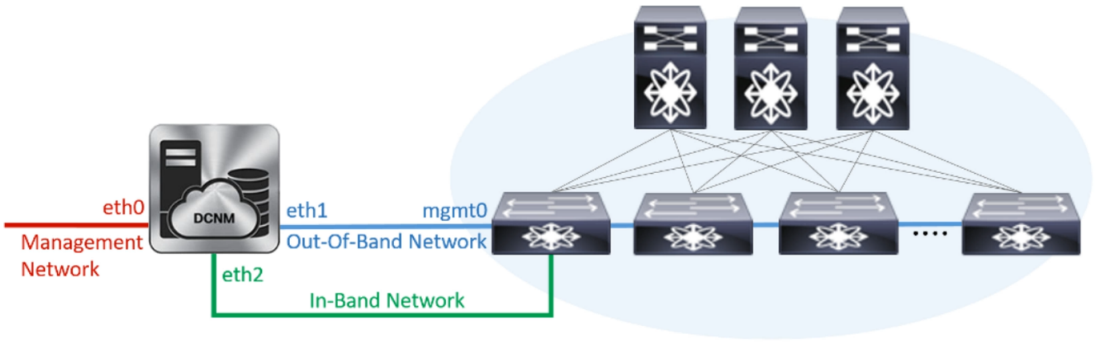
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

  From Release 11.3(1), you can configure more than one NTP server.
- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

f) On the **Network Settings** tab, configure the network parameters used to reach the DCNM Web UI.

Figure 1: Cisco DCNM Management Network Interfaces



1. In the **Management Network** area, verify if the auto-populated addresses for **Management IPv4 Address** and **Management Network Default IPv4 Gateway** are correct. Modify, if necessary.

   Note Ensure that the IP address belongs to the same Management Network configured on the Primary node.

   (Optionally) Enter a valid IPv6 address along with the prefix to configure the **Management IPv6 Address** and the **Management Network Default IPv6 Gateway**.

2. In the **Out-of-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address**.

   If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

Note Ensure that the IP addresses belong to the same Out-of-Band network configured on the Primary node.

Out-of-band management provides a connection to the device management ports (Typically mgmt0).

Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

3. In the **In-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address** for the in-band network.

   If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

   Note Ensure that the IP addresses belong to the same In-Band network configured on the Primary node.

   The In-Band Network provides reachability to the devices via the front-panel ports.

   Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

Click **Next**.

g) On the **Applications** tab, configure the Internal Applications Services Network, and Cluster mode settings.

1. In the **Internal Application Services Network** area, in the **IPv4 Subnet field**, enter the IP subnet to access the applications that run internally to DCNM.
2. In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.
   - In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the Out-of-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.
   - In the **In-Band IPv4 Network Address Pool**, enter the address pool from the In-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

Ensure that the IP addresses belong to the same pool as configured on the Primary node.

h) On the **HA Settings** tab, configure the system settings for the Secondary node.

- In the **Management IPv4 Address of Primary DCNM node** field, enter the appropriate IP Address to access the DCNM UI.
- In the **VIP Fully qualified Host Name** field, enter hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Host names with only digits is not supported.
- In the **Management Network VIP address** field, enter the IP address used as VIP in the management network.

Optionally, you can also enter an IPv6 VIP address in the **Management Network VIPv6 address** field.

Note If you have configured the Management network using IPv6 address, ensure that you configure the Management Network VIPv6 Address.

- In the **Out-of-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

  Optionally, you can also enter an IPv6 VIP address in the **Out-of-Band Network VIPv6 Address** field.

- In the **In-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

  Optionally, you can also enter an IPv6 VIP address in the **In-Band Network VIPv6 Address** field.

  Note This field is mandatory if you have provided an IP address for In-Band network in the **Network Settings** tab.

- In the **HA Ping Feature IPv4 Address** field, enter the HA ping IP address and enable this feature, if necessary.

  Note The configured IPv4 address must respond to the ICMP echo pings.

  HA_PING_ADDRESS, must be different from the DCNM Active and Standby addresses.

  You must configure the HA ping IPv4 Address to avoid the Split Brain scenario. This IP address must belong to Enhanced Fabric management network.

Click **Next**.

i) On the **Summary** tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM OVA Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
************************************************************
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at
https://<<IP Address>>
You will be redirected there in 60 seconds.
Thank you
************************************************************
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

What to do next

Verify the HA role by using the appmgr show ha-role command.

On the Active node (old standalone node):

```
dcnm1# appmgr show ha-role
Native HA enabled.
Deployed role: Active
Current role: Active
```

On the Standby node (newly deployed node):

```
dcnm2# appmgr show ha-role
Native HA enabled.
Deployed role: Standby
Current role: Standby
```

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.

After upgrade, enable RabbitMQ management service stop the service and start the services using the following commands:

```
dcnm# appmgr stop amqp
dcnm# appmgr start amqp
```

If AMQP is not running. the memory space must be exhausted that is indicated in the file `/var/log/rabbitmq/erl_crash.dump`.

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:

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:

```
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

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
```