



# DCNM 展開後にユーティリティ サービスを管理する

この章では、DCNM 展開後、管理機能の DC3 (プログラミング可能なファブリック) の主要目的を提供するユーティリティ サービスをすべて確認し、管理する方法を説明します。

表 1: Cisco DCNM ユーティリティ サービス

カテゴリ	アプリケーション	[ユーザ名 (Username) ]	パスワード	プロトコルの実装
ネットワーク管理	Data Center Network Manager	admin	ユーザーは、 <sup>1</sup> を選択します。	ネットワーク管理

<sup>1</sup> [展開中にユーザーによって入力された管理パスワードを参照するようにユーザーが選択する (User choice refers to the administration password entered by the user during the deployment)]

この章は、次の項で構成されています。

- [DCNM インストール後のネットワーク プロパティ \(1 ページ\)](#)
- [スタンドアロンセットアップからネイティブ HA セットアップへの変換 \(15 ページ\)](#)
- [ユーティリティ サービスの詳細, on page 20](#)
- [アプリケーションとユーティリティ サービスの管理 , on page 20](#)

## DCNM インストール後のネットワーク プロパティ

Cisco DCNM OVA または ISO iインストールは、3つのネットワーク インターフェイスで構成されています。

- dcnm-mgmt network (eth0) インターフェイス

このネットワークは、Cisco DCNM オープン仮想アプライアンスに接続 (SSH、SCP、HTTP、HTTPS) を提供します。DCNM 管理ネットワークに関連付けられているサブネットに対応するポート グループに、このネットワークを関連付けます。

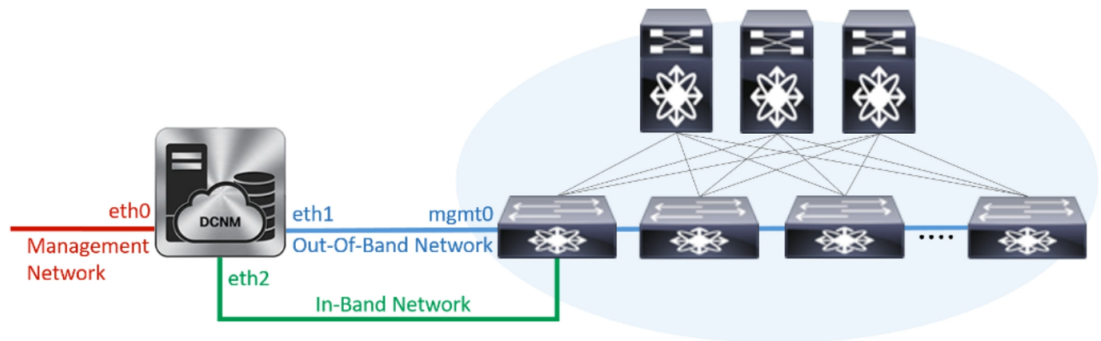
- enhanced-fabric-mgmt (eth1) インターフェイス

このネットワークは、Nexus スイッチのファブリック管理を強化します。リーフおよびスパインスイッチの管理ネットワークに対応するポートグループに、このネットワークを関連付けます。

- enhanced-fabric-inband (eth2) インターフェイス

このネットワークは、ファブリックへのインバンド接続を提供します。このネットワークを、ファブリック インバンド接続に対応するポートグループに関連付けます。

次の図は、Cisco DCNM 管理インターフェイスのネットワーク図を示しています。



展開タイプの Cisco DCNM のインストール中に、これらのインターフェイスを設定できます。ただし、Cisco DCNM リリース 11.2(1)以降では、インストール後のネットワーク設定を編集および変更できます。



(注) ネットワーク プロパティを更新するために、**appmgr** コマンドを使用するようにお勧めします。ネットワーク インターフェイスを手動で再起動しないでください。

次の項で説明するように、パラメータを変更できます。

## スタンドアロン モードの DCNM 上でネットワーク プロパティの変更



**Note** DCNM アプライアンス コンソールで次のコマンドを実行し、早期のセッション タイムアウトを防止します。

Cisco DCNM スタンドアロンセットアップでネットワーク プロパティを変更するには、次の手順を実行します。

### Procedure

**ステップ 1** 次のコマンドを使用して、コンソールのセッションを開始します。

**appmgr update network-properties session start**

**ステップ 2** 次のコマンドを使用して、ネットワーク プロパティを更新します。

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

**ステップ 3** 次のコマンドを使用して、変更を表示し確認します。

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

**ステップ 4** 変更を確認した後、次のコマンドを使用して設定を適用します。

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

eth0 管理ネットワーク IP アドレスを使用して Cisco DCNM Web UI にログオンする前に、数分待機します。

---

### Cisco DCNM スタンドアロンセットアップでネットワーク パラメータを変更する場合のサンプルコマンド出力

次のサンプル例では、Cisco DCNM スタンドアロンセットアップ用に、インストール後ネットワーク パラメータを変更する方法を示します。

```
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#

```

## ネイティブ HA モードの DCNM 上でネットワーク プロパティの変更



**Note** DCNM アプライアンス コンソールで次のコマンドを実行し、早期のセッション タイムアウトを防止します。

次の手順で示されているように、同じ順番でコマンドを実行します。



**Note** ネイティブ HA ノードは、単一のエンティティと見なす必要があります。アクティブノードの eth1 IP アドレスを変更する場合は、スタンバイ ノードの eth1 IP アドレスも変更する必要があります。

任意のノードの eth0 IP アドレスを変更する場合は、そのノードの eth2 IP アドレスを変更する必要があります。

Cisco DCNM ネイティブ HA セットアップでネットワーク プロパティを変更するには、次の手順を実行します。

### Procedure

**ステップ 1** 次のコマンドを使用して、スタンバイ ノードで DCNM アプリケーションを停止します。

**appmgr stop all**

続行する前に、スタンバイ ノードですべてのアプリケーションが停止するまで待ちます。

**ステップ 2** 次のコマンドを使用して、アクティブ ノードで DCNM アプリケーションを停止します。

**appmgr stop all**

**ステップ 3** 次のコマンドを使用して、アクティブおよびスタンバイ ノードの両方の Cisco DCNM コンソールでセッションを開始します。

**appmgr update network-properties session start**

**ステップ 4** アクティブ ノードで、次のコマンドを使用してネットワーク インターフェイス パラメータを変更します。

a) 次のコマンドを使用して、eth0、eth1、および eth2 アドレスの IP アドレスを設定します。

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

サブネット マスクおよびゲートウェイ IP アドレスとともに、インターフェイスの新しい IPv4 または IPv6 アドレスを入力します。

b) 次のコマンドを使用して、VIP IP アドレスを設定します。

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

eth0 インターフェイスの vip0 アドレスを入力します。eth1 インターフェイスの vip1 アドレスを入力します。eth2 インターフェイスの vip2 アドレスを入力します。

c) 次のコマンドを使用して、ピア IP アドレスを設定します。

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

アクティブ ノードに peer0 アドレスとして、スタンバイ ノードの eth0 アドレスを入力します。アクティブ ノードに peer1 アドレスとして、スタンバイ ノードに eth1 アドレスを入力します。アクティブ ノードに peer2 アドレスとしてスタンバイ ノードの eth2 アドレスを入力します。

d) 次のコマンドを使用して、ネットワーク パラメータに行った変更を表示および確認します。

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

**ステップ 5** スタンバイ ノードで、ステップ [ステップ 4, on page 5](#) で説明したコマンドを使用して、ネットワーク インターフェイスのパラメータを変更します。

**ステップ 6** 変更を確認した後、アクティブ ノードで次のコマンドを使用して設定を適用します。

**appmgr update network-properties session apply**

ネットワーク パラメータが更新されていることを確認するため、プロンプトが返されるまで待ちます。

**ステップ 7** 変更を確認した後、次のコマンドを使用してスタンバイ ノードで設定を適用します。

**appmgr update network-properties session apply**

**ステップ 8** 次のコマンドを使用して、アクティブ ノードですべてのアプリケーションを開始します。

**appmgr start all**

**Note** 次の手順に進む前に、アクティブ ノードですべてのアプリケーションが正常に稼働するまで待ちます。

**ステップ 9** 次のコマンドを使用して、スタンバイ ノードですべてのアプリケーションを開始します。

**appmgr start all**

**ステップ 10** 次のコマンドを使用して、アクティブ ノードでピア信頼キーを確立します。

**appmgr update ssh-peer-trust**

**ステップ 11** 次のコマンドを使用して、スタンバイ ノードでピアトラスト キーを確立します。

**appmgr update ssh-peer-trust**

### Cisco DCNM ネイティブ HA セットアップでネットワーク パラメータを変更する場合のサンプル コマンド出力

次のサンプル例では、Cisco DCNM ネイティブ HA セットアップ用に、インストール後ネットワーク パラメータを変更する方法を示します。



**Note** 例えば、アクティブおよびスタンバイ アプライアンスを **dcnm1** および **dcnm2** に個別に示します。

```
[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

```

## ネイティブ HA モードの DCNM 上でネットワーク プロパティの変更

```
[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

```

## ネイティブ HA モードの DCNM 上でネットワーク プロパティの変更

```

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'
```

## DCNM インストール後に DCNM サーバパスワードを変更する

```
'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 ~]#
```

## DCNM インストール後に DCNM サーバパスワードを変更する

The password to access Cisco DCNM Web UI にアクセスするためのパスワードは、展開タイプの Cisco DCNM をインストールする間に設定されます。ただし、必要に応じてインストール後にこのパスワードを変更できます。

インストール後にパスワードを変更するには、次の手順を実行します。

### Procedure

**ステップ 1 appmgr stop all** コマンドを使用して、アプリケーションを停止します。

すべてのアプリケーションが稼働を停止するまで待ちます。

**ステップ 2 appmgr change\_pwd ssh {root|poap|sysadmin}[password]** コマンドを使用して、管理インターフェイスのパスワードを変更します。

新しいパスワードが次のパスワード要件に準拠していることを確認します。要件に従わない場合、DCNM アプリケーションは適切に機能しない場合があります。

- 最小でも 8 文字を含み、1 個のアルファベットと 1 個の数字を含む必要があります。
- アルファベット、数字、特殊文字 (-\_#@&\$ など) の組み合わせを含むことができます。

- DCNM パスワードにこれらの特殊文字を使用しないでください。 <SPACE> " & \$ % ' ^ = < > ; : ` \ | / , . \*`

ステップ 3 **appmgr start all** コマンドを使用して、アプリケーションを起動します。

---

## スタンドアロンセットアップで DCNM データベース パスワードを変更する

Cisco DCNM スタンドアロンセットアップで Postgres データベースのパスワードを変更するには、次の手順を実行します。

### Procedure

ステップ 1 **appmgr stop all** コマンドを使用して、すべてのアプリケーションを停止します。

**appmgr status all** コマンドを使用してすべてのアプリケーションが停止していることを確認します。

ステップ 2 **appmgr change\_pwd db** コマンドを使用して Postgres パスワードを変更します。

プロンプトで新しいパスワードを入力します。

ステップ 3 **appmgr start all** コマンドを使用して、アプリケーションを起動します。

**appmgr status all** コマンドを使用して、すべてのアプリケーションが起動していることを確認します。

---

### Example

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

## ネイティブ HA セットアップで DCNM データベース パスワードを変更する

Cisco DCNM ネイティブ HA セットアップで Postgres データベースのパスワードを変更するには、次の手順を実行します。

## Procedure

---

- ステップ 1** `appmgr stop all` コマンドを使用して、スタンバイ アプライアンスですべてのアプリケーションを停止します。
- `appmgr status all` コマンドを使用して、すべてのアプリケーションが停止していることを確認します。
- ステップ 2** `appmgr stop all` コマンドを使用して、アクティブ アプライアンスですべてのアプリケーションを停止します。
- `appmgr status all` コマンドを使用して、すべてのアプリケーションが停止していることを確認します。
- ステップ 3** アクティブおよびスタンバイ ノードで `appmgr change_pwd db` コマンドを使用して、Postgres パスワードを変更します。
- プロンプトで同じパスワードを提供するようにします。
- ステップ 4** `appmgr start all` コマンドを使用して、アクティブ アプライアンスでアプリケーションを停止します。
- `appmgr status all` コマンドを使用して、すべてのアプリケーションが停止していることを確認します。
- ステップ 5** `appmgr start all` コマンドを使用して、スタンバイ アプライアンスでアプリケーションを開始します。
- `appmgr status all` コマンドを使用して、すべてのアプリケーションが停止していることを確認します。
- 

## Example

アクティブおよびスタンバイを `dcnm1` および `dcnm2` として個別に考慮します。

```
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
```

# スタンドアロンセットアップからネイティブ HA セットアップへの変換

既存の Cisco DCNM スタンドアロンセットアップをネイティブ HA セットアップに変換するには、次の手順を実行します。

## 始める前に

**appmgr show version** コマンドを使用して、スタンドアロンセットアップがアクティブで動作していることを確認します。

```
dcnm# appmgr show version

Cisco Data Center Network Manager
Version: 11.5(1)
Install mode: LAN Fabric
Standalone node. HA not enabled.
dcnm#
```

## 手順

**ステップ 1** スタンドアロンセットアップで、**appmgr root-access permit** のコマンドを使用して SSH を起動し、**root** ユーザー アクセスを有効にします。

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

**ステップ 2** 新しい DCNM をセカンダリ ノードとして展開します。[新規インストール - HA セカンダリ] を選択します

たとえば、既存のセットアップを **dcnm1** として、新しい DCNM をセカンダリノードとして **dcnm2** として指定します。

**注意** システム設定が最小リソース要件を満たしていない場合は、Web インストーラに **SYSTEM RESOURCE ERROR** と表示され、インストールが中止されます。システム要件を変更し、Web インストーラを起動してインストールを完了します。

**ステップ 3** セカンダリ ノードとして **dcnm2** を設定します。 **dcnm2** の [コンソール (Console)] タブに表示されている URL を貼り付け、[Enter] キーを押します。

初期メッセージが表示されます。

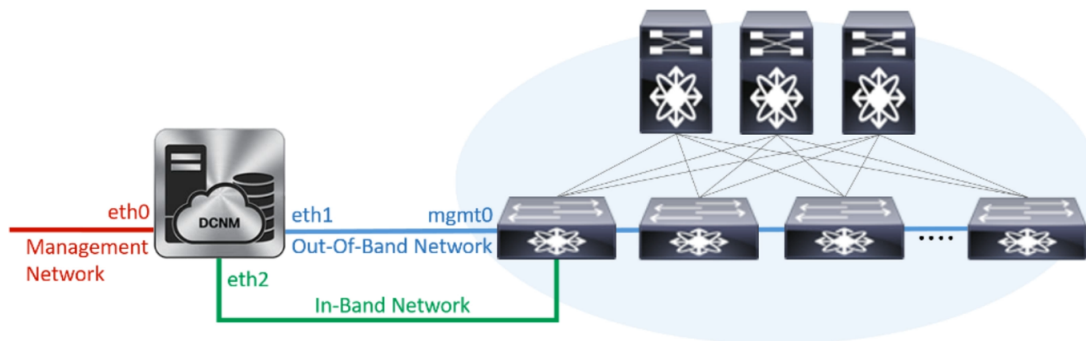
a) [Cisco DCNM へようこそ (Welcome to Cisco DCNM)] 画面から、[開始 (Get Started)] をクリックします。

**注意** システム設定が最小リソース要件を満たしていない場合は、Web インストーラに **SYSTEM RESOURCE ERROR** と表示され、インストールが中止されます。システム要件を変更し、Web インストーラを起動してインストールを完了します。

- b) [Cisco DCNM インストーラ (Cisco DCNM Installer)] 画面で、**[新規インストール - HA セカンドリ (Fresh Installation - HA Secondary)]** オプション ボタンを選択して、**dcnm2** をセカンドリ ノードとしてインストールします。
- [Continue] をクリックします。
- c) **[インストール モード (Install Mode)]** タブで、ドロップダウン リストからプライマリ ノードに選択したものと同一インストール モードを選択します。
- (注) プライマリ ノードと同じインストール モードを選択しない場合、HA のインストールは失敗します。
- [Next] をクリックします。
- d) **[管理 (Administration)]** タブで、パスワードに関する情報を入力します。
- (注) すべてのパスワードは、プライマリ ノードの設定時に指定したパスワードと同じである必要があります。
- e) **[システム設定 (System Settings)]** で、DCNM アプライアンスの設定を行います。
- **[完全修飾ホスト名 (Fully Qualified Hostname)]** フィールドで、RFC1123 セクション 2.1 の通りに、完全修飾ドメイン名 (FQDN) のホスト名を入力します。数字のみのホスト名はサポートされていません。
  - **[DNS サーバ アドレス (DNS Server Address)]** フィールドで、DNS IP アドレスを入力します。  
リリース 11.2(1) から、IPv6 アドレスを使用した DNS サーバも設定できます。  
リリース 11.3(1) から、1 個以上の DNS サーバと NTP サーバを設定できます。
  - **[NTP サーバ アドレス リスト (NTP Server Address List)]** フィールドでは、NTP サーバの IP アドレスを入力します。  
値は IP または IPv6 アドレスか RFC 1123 に準拠した名前である必要があります。  
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。
  - **タイムゾーン** ドロップダウン リストから、DCNM を展開しているタイムゾーンを選択します。
- [Next] をクリックします。
- f) **[ネットワーク設定 (Network Settings)]** タブで、DCNM Web UI に到達するために使用されるネットワーク パラメータを構成します。



図 1: Cisco DCNM 管理ネットワーク インターフェイス



1. [管理ネットワーク (Management Network)] 領域で、[管理 IPv4 アドレス (Management IPv4 Address)] と [管理ネットワーク デフォルト IPv4 ゲートウェイ (Management Network Default IPv4 Gateway)] の自動入力 IP アドレスが正しいことを確認します。必要に応じて変更します。

(注) HA セットアップが正常に完了するために、IP アドレスがプライマリ ノードで設定されているのと同じ管理ネットワークに属していることを確認します。

(オプション) プレフィックスとともに有効な IPv6 アドレスを入力し、管理 IPv6 アドレスと管理ネットワーク デフォルト IPv6 ゲートウェイを構成します。

2. [アウトオブバンド ネットワーク (Out-of-Band Network)] 領域で、IPv4 アドレス と ゲートウェイ IPv4 アドレス を入力します。

DCNMがIPv6ネットワーク上にある場合は、IPv6アドレスとゲートウェイIPv6アドレスに関連するIPv6アドレスを入力して、ネットワークを設定します。

(注) IPアドレスがプライマリノードで設定された同じアウトオブバンドネットワークに属していることを確認します。

アウトオブバンド管理では、デバイス管理ポート (通常 mgmt0) への接続を提供します。

(注) アウトオブバンド管理が設定されていない場合、クラスタ モードで Cisco DCNM を設定できません。

3. [インバンド ネットワーク (In-Band Network)] 領域で、インバンド ネットワークの IPv4 アドレスおよびゲートウェイ IPv4 アドレスを入力します。

DCNM が IPv6 ネットワーク上にある場合は、IPv6 アドレス と ゲートウェイ IPv6 アドレス の関連する IPv6 アドレスを入力することで、ネットワークを構成します。

(注) IPアドレスがプライマリノードで設定された同じインバンドネットワークに属していることを確認します。

インバンドネットワークにより、前面パネルのポートを介してデバイスへ到達可能になります。

(注) インバンドネットワークを設定しない場合、エンドポイントロケータおよびテレメトリ機能は操作できません。

[Next] をクリックします。

g) [アプリケーション (Applications)] タブで、[内部アプリケーション サービス ネットワーク] を構成します。

1. [内部アプリケーション サービス ネットワーク (Internal Application Services Network)] 領域で、DCNM に対して内部で実行するアプリケーションへアクセスするための IPv4 IP サブネット フィールドに IP サブネットを入力します。

h) [HA 設定 (HA Settings)] タブで、セカンダリ ノードのシステム設定を行います。

- [プライマリ DCNM ノードの管理 IP アドレス (Management IP Address of primary DCNM node)] フィールドに、DCNM UI にアクセスするための適切な IP アドレスを入力します。
- [VIP 完全修飾ホスト名 (VIP Fully Qualified Host Name)] フィールドで、RFC1123 セクション 2.1 の通りに、完全修飾ドメイン名 (FQDN) のホスト名を入力します。数字のみのホスト名はサポートされていません。
- [管理ネットワーク VIP アドレス (Management Network VIP Address)] フィールドに、管理ネットワークの VIP として使用された IP アドレスを入力します。  
オプションで、[管理ネットワークの IPv6 アドレス (Management Network IPv6 Address)] フィールドに IPv6 VIP アドレスを入力することもできます。  
(注) IPv6 アドレスを使用して管理ネットワークを設定している場合は、管理ネットワークの IPv6 アドレスを設定していることを確認します。
- [アウトオブバンドネットワーク VIP アドレス (Out-of-Band Network VIP Address)] フィールドにアウトオブバンドネットワークの VIP として使用される IP アドレスを入力します。  
オプションで、[アウトオブバンドネットワークの IPv6 アドレス (Out-of-Band Network IPv6 Address)] フィールドに IPv6 VIP アドレスを入力することもできます。
- [インバンドネットワーク VIP アドレス (In-Band Network VIP Address)] フィールドにアウトオブバンドネットワークの VIP として使用される IP アドレスを入力します。  
オプションで、[インバンドネットワークの IPv6 アドレス (In-Band Network IPv6 Address)] フィールドに IPv6 VIP アドレスを入力することもできます。  
(注) [ネットワーク設定 (Network Settings)] タブでインバンドネットワークの IP アドレスを指定した場合、このフィールドは必須です。
- [HA Ping 機能 IPv4 アドレス (HA Ping Feature IPv4 Address)] フィールドに、必要に応じて、HA ping IP アドレスを入力し、この機能を有効にします。

(注) 構成済みの IPv4 アドレスは、ICMP echo ping に応答する必要があります。

HA\_PING\_ADDRESS は、DCNM アクティブおよびスタンバイ アドレスとは異なっている必要があります。

HA ping IPv4 アドレスを Split Brain シナリオを避けるように構成する必要があります。この IP アドレスは、Enhanced Fabric 管理ネットワークに属する必要があります。

[次へ (Next)] をクリックします。

- i) [サマリー (Summary)] タブで、構成の詳細を見直します。

前のタブに移動して設定を変更するには、[前 (previous)] をクリックします。[インストールの開始 (Start Installation)] をクリックし、選択した展開モードの Cisco DCNM OVA インストールを完了します。

進行状況バーが表示され、完了したパーセンテージ、動作の説明、およびインストール中の経過時間が表示されます。経過表示バーに 100% と表示されたら、[続行 (Continue)] をクリックします。

DCNM Web UI にアクセスするための URL とともに成功メッセージが表示されます。

```
*****
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
*****
```

(注) Cisco DCNM がファイアウォールの背後で実行されている場合、ポート 2443 を開き、Cisco DCNM Web UI を起動します。

## 次のタスク

appmgr show ha-role コマンドを使用して、HA ロールを確認します。

アクティブノード (古いスタンダオンノード) :

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

スタンバイノード (新しく展開されたノード) :

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

## ユーティリティ サービスの詳細

ここでは、Cisco DCNM で提供される機能内のすべてのユーティリティ サービスの詳細について説明します。機能は次のとおりです。

### 電源オン自動プロビジョニング

Power On Auto Provisioning (POAP) は、スタートアップ設定を使用せずにスイッチを起動すると発生します。これは、インストールされた 2 つのコンポーネントによって発生します。

- DHCP サーバ

DHCP サーバは、ファブリック内のスイッチに IP アドレスをパーセルし、POAP データベースの場所を指します。これにより、Python スクリプトが提供され、デバイスがイメージと設定に関連付けられます。

Cisco DCNM のインストール時に、内部ファブリック管理アドレスまたは OOB 管理ネットワークの IP アドレスと、Cisco プログラマブルファブリック管理に関連付けられたサブネットワークを定義します。



**Note** [設定 (Configure)] > [POAP] > [DHCP 範囲 (DHCP Scopes)] を選択し、Cisco DCNM Web UI を使用して DHCP を常に設定する必要があります。SSH 端末から `/etc/dhcp/dhcp.conf` ファイルを編集すると、予期しない動作が発生する可能性があります。

- リポジトリ

TFTP サーバは、POAP に使用される起動スクリプトをホストします。

SCP サーバは、データベース ファイル、設定ファイル、およびソフトウェア イメージをダウンロードします。

## アプリケーションとユーティリティ サービスの管理

SSH 端末のコマンドを通して、Cisco DCNM で Cisco プログラマブルファブリックのアプリケーションとユーティリティ サービスを管理できます。

次のクレデンシャルを使用して、SSH 端末から **appmgr** コマンドを入力します。

- ユーザ名 : root
- パスワード : 展開中に提供された管理パスワード



**Note** 参考に、コンテキスト サービス ヘルプが **appmgr** コマンドに利用可能です。 **appmgr** コマンドを使用してヘルプを表示します。

**appmgr tech\_support** コマンドを使用して、ログ ファイルのダンプを生成します。セットアップのトラブルシューティングと分析のため、この情報を TAC チームに提供できます。



**Note** このセクションは、Cisco Prime Network Services Controller を使用したネットワーク サービスのコマンドは説明しません。

このセクションの内容は次のとおりです。

## 展開後にアプリケーションおよびユーティリティ サービス ステータスを確認する

OVA/ISO ファイルを展開後、ファイルに展開したさまざまなアプリケーションおよびユーティリティ サービスのステータスを決定できます。SSH セッションの **appmgr status** コマンドを使用して、この手順を実行します。



**Note** コンテキストの機密ヘルプは **appmgr status** コマンドで使用できます。 **appmgr status ?** コマンドを使用してヘルプを表示します。

### Procedure

**ステップ 1** SSH セッションを開きます。

- a) **ssh root DCNM network IP address** コマンドを入力します。
- b) 管理パスワードを入力してログインします。

**ステップ 2** 次のコマンドを使用して、ステータスをチェックします。

**appmgr status all**

#### Example:

メディア コントローラ展開用 Cisco DCNM を取得した場合の例は次のようになります。

```
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
```

## ユーティリティ サービスの停止、開始、リセット

```

===  ===  == == ===== ===== ===== =  ===  ===  =====  =====
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

```

## ユーティリティ サービスの停止、開始、リセット

ユーティリティ サービスの停止、開始、リセットには、次の CLI コマンドを使用します。

- アプリケーションを停止するには、**appmgr stop** コマンドを使用します。

```

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

```

- アプリケーションを開始するには、**appmgr start** コマンドを使用します。

```

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

```

- アプリケーションを再起動するには、**appmgr restart** コマンドを使用します。

```

# appmgr restart tftp
Restarting TFTP...
Stopping xinetd:         [ OK ]
Starting xinetd:         [ OK ]

```



---

**Note** Cisco DCNM リリース 7.1.x から、**appmgr stop *app\_name*** コマンドを使用してアプリケーションを停止する場合、正常な再起動でアプリケーションが開始しません。

---

たとえば、DHCP が **appmgr stop dhcp** コマンドを使用して停止し、OS が再起動する場合、OS がアップ状態になり実行した後でも、DHCP アプリケーションはダウンしたままです。

再度開始するには、**appmgr start dhcp** コマンドを使用します。再起動後も DHCP アプリケーションが開始されます。これは、環境で仮想アプライアンス (DHCP の代わりに CPNR など) の一部としてパッケージ化されていないアプリケーションを使用している場合、ローカルで仮想アプライアンスとともにパッケージ化されているアプリケーションは OS 再起動後に機能を妨げることはありません。



---

**Note** DCNM アプライアンス (ISO/OVA) が展開されると、Cisco SMIS コンポーネントはデフォルトでは開始しません。しかし、このコンポーネントは、**appmgr CLI** を使用して管理できます。  
**appmgr start/stop dcnm-smis**

**appmgr start/stop dcnm** DCNM Web コンポーネントのみを開始または停止します。

---

ユーティリティ サービスの停止、開始、リセット