



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、 ¹ を選択します。	ネットワーク管理

¹ [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 \(1 ページ\)](#)
- [ユーティリティ サービスの詳細, on page 14](#)
- [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 16](#)
- [IPv6 の SFTP サーバアドレスの更新, on page 18](#)

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。

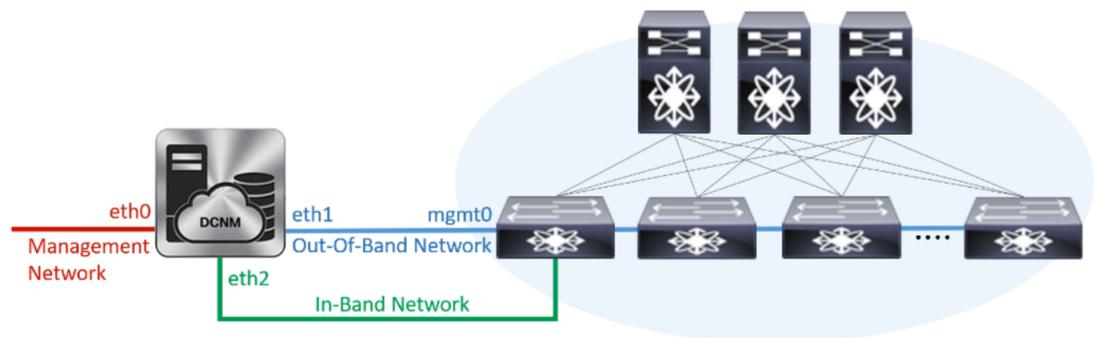
- enhanced-fabric-mgmt (eth1) インターフェイス

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。

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 上でのネットワーク 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。

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** スタンバイ ノードで DCNM アプリケーションを停止するには、次のコマンドを使用します。
- 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のを待ちます。
- 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** 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するには、次のコマンドを使用します。
- appmgr update network-properties session start**
- ステップ 4** アクティブ ノードで、ネットワーク インターフェイス パラメータを変更するには、次のコマンドを使用します。

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

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

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

- b) VIP IP アドレスを設定するには、次のコマンドを使用します。

```
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 ノードの 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 ノードの 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 ノードの 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、[#unique_77 unique_77_Connect_42_substeps_active, on page 5](#) で説明されているコマンドを使用して、ネットワーク パラメータを変更します。

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

```
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実行されるまで待ちます。

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 ノードでピア信頼キーを確立します。

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ためのサンプル 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 たとえば、アクティブおよびスタンバイ アプライアンスをそれぞれ **dcnm1** と **dcnm2** として示すことにします。

```
[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

[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      /

```

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

```

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'
'dcnml.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
```

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。

ネットワーク管理

データセンター ネットワーク管理機能は、Cisco Data Center Network Manager (DCNM) サーバで提供されます。Cisco DCNM はデータセンター インフラストラクチャのセットアップ、仮想化、管理、およびモニタリングを提供します。Cisco DCNM には、ブラウザからアクセスできます。http://<<hostname/IP address>>。



Note Cisco DCNM の詳細については、<http://cisco.com/go/dcnm> を参照してください。

オーケストレーション

RabbitMQ

RabbitMQ は、Advanced Messaging Queuing Protocol (AMQP) を提供するメッセージブロッカーです。RabbitMQ メッセージブロッカーは、vCloud Director/vShield Manager から解析用の Python スクリプトにイベントを送信します。ファームウェアの Secure Shell (SSH) コンソールから、特定の CLI コマンドを使用して、このプロトコルを設定できます。



Note 30 秒以内に DCNM のサーバ両方で AMQP を停止および再起動する必要があります。そうしない場合、AMQP が開始しない場合があります。RabbitMQ の詳細については、<https://www.rabbitmq.com/documentation.html> を参照してください。

アップグレード後、RabbitMQ 管理サービスを有効にして、次のコマンドを使用して罫線を停止および開始します。

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

AMQP が実行されない場合、メモリ スペースはファイル /var/log/rabbitmq/erl_crash.dump に示されているように使いきっています。

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を定義します。

- 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:

```
DCNM Status
PID  USER      PR  NI VIRT RES  SHR  S  %CPU %MEM  TIME+  COMMAND
===  =====  ===  == =====  ===  ==  ==  =====  =====  =====  =====
1891 root    20  0 2635m 815m 15m S  0.0 21.3   1:32.09  java

LDAP Status
PID  USER      PR  NI VIRT RES  SHR  S  %CPU %MEM  TIME+  COMMAND
===  =====  ===  == =====  ===  ==  ==  =====  =====  =====  =====
1470 ldap    20  0 692m 12m 4508 S  0.0 0.3    0:00.02  slapd

AMQP Status
PID  USER      PR  NI VIRT RES  SHR  S  %CPU %MEM  TIME+  COMMAND
===  =====  ===  == =====  ===  ==  ==  =====  =====  =====  =====
1504 root     20  0 52068 772 268 S  0.0 0.0    0:00.00  rabbitmq

TFTP Status
PID  USER      PR  NI VIRT RES  SHR  S  %CPU %MEM  TIME+  COMMAND
===  =====  ===  == =====  ===  ==  ==  =====  =====  =====  =====
1493 root     20  0 22088 1012 780 S  0.0 0.0    0:00.00  xinetd

DHCP Status
PID  USER      PR  NI VIRT RES  SHR  S  %CPU %MEM  TIME+  COMMAND
===  =====  ===  == =====  ===  ==  ==  =====  =====  =====  =====
1668 dhcpd 20  0 46356 3724 408 S  0.0 0.0    0:05.23  dhcp
```

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。

IPv6 の SFTP サーバアドレスの更新

DCNM OVA/ISO を EFM IPv4 および IPv6 で正常に展開した後、デフォルトでは SFTP アドレスは IPv4 のみを指します。次の 2 つの場所で IPv6 アドレスを手動で変更する必要があります。

- DCNM Web クライアントで、**Administration > Server Properties** を選択してから、次のフィールドを IPv6 に更新し、**Apply Changes** ボタンをクリックします。

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

- ssh を使用して DCNM にログインし、`server.properties` ファイル (`/usr/local/cisco/dcm/fm/conf/server.properties`) で SFTP アドレスを IPv6 で手動で更新します。

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