



## **Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment, Release 11.5(4)**

**First Published:** 2022-03-04

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

#### 概要 1

はじめに 1

Installation Options 2

展開オプション 2

root および sysadmin のユーザー権限 3

---

### CHAPTER 2

#### 注意事項と制約事項 5

注意事項と制約事項 5

---

### CHAPTER 3

#### 前提条件 9

DCNM オープン仮想アプライアンスの前提条件 9

DCNM ISO 仮想アプライアンスの前提条件 10

Cisco DCNM 仮想アプライアンス HA の前提条件 10

HA モードで Cisco DCNM 仮想アプライアンスを展開する 11

仮想 IP アドレスの可用性 11

NTP サーバのインストール 11

---

### CHAPTER 4

#### Installing the Cisco DCNM 13

オープン仮想アプライアンスで DCNM をインストールする 13

オープン仮想アプライアンス ファイルのダウンロード 14

OVF テンプレートとしてのオープン仮想アプライアンスの展開 14

スタンドアロンモードでの Cisco DCNM OVA のインストール 19

ネイティブ HA モードでの Cisco DCNM OVA のインストール 24

ISO 仮想アプライアンスで DCNM をインストールする 34

ISO 仮想アプライアンス ファイルのダウンロード	34
UCS (ベア ブレード) 上での DCNM ISO 仮想アプライアンスのインストール	35
KVM 上での DCNM ISO 仮想アプライアンスのインストール	42
Windows Hyper-V 上での DCNM ISO 仮想アプライアンスのインストール	44
仮想スイッチの作成	44
仮想マシンの作成	46
DCNM ISO 仮想アプライアンスのインストール	50
スタンドアロン モードでの Cisco DCNM ISO のインストール	54
ネイティブ HA モードで Cisco DCNM ISO をインストールする	59
Cisco APIC SE への Cisco DCNM SE ISO のインストール	69
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	71
Cisco DCNM コンピューティング ノードのインストール	76

**CHAPTER 5****Upgrading Cisco DCNM 81**

インラインアップグレードを使用して ISO または OVA をアップグレードする	81
スタンドアロン モードでの DCNM 仮想アプライアンスのインラインアップグレード	82
ネイティブ HA モードでの DCNM 仮想アプライアンスのインラインアップグレード	84
DCNM コンピューティング ノードのインラインアップグレード	89

**CHAPTER 6****Cisco DCNM Classic LAN 展開のアップグレード 91**

概要	91
ファブリックの移行	92
アップグレード後の LAN ファブリックでサポートされるスイッチ ロール	94
LAN ファブリックの従来の LAN テンプレート	95
クラシック LAN 展開から LAN ファブリック展開へのアップグレード	98
LAN クラシック ファブリック テンプレートの機能	102

**CHAPTER 7****展開のベスト プラクティス 105**

Cisco DCNM およびコンピューティング展開のベスト プラクティス	105
ベスト プラクティスを使用するためのガイドライン	106
Cisco DCNM で冗長性の展開	106

Cisco DCNM での IP アドレスの設定 108

シナリオ 1: 3 つのイーサネット インターフェイスはすべて異なるサブネットにあります 108

シナリオ 2: 異なるサブネットの eth2 インターフェイス 110

Cisco DCNM およびコンピューティング ノードの物理接続 112

---

## CHAPTER 8

ディザスタ リカバリ (バックアップおよび復元) 117

スタンドアロン DCNM セットアップでの Cisco DCNM およびアプリケーションデータのバックアップおよび復元 117

ネイティブ HA セットアップでの Cisco DCNM およびアプリケーションデータのバックアップおよび復元 119

Cisco DCNM シングル HA ノードのリカバリ 120

管理者アカウントの回復 123

SRM を使用した HA の災害回避 124

---

## CHAPTER 9

証明書 129

の証明書管理 129

証明書管理のベスト プラクティス 130

インストールされた証明書の表示 130

CA 署名付き証明書のインストール 132

Cisco DCNM スタンドアロン セットアップで CA 署名済み証明書をインストールする 132

DCNM ネイティブ HA セットアップで CA 署名済み証明書をインストールする 134

アクティブ ノードからスタンバイ ノードへ証明書をエクスポートする 136

アップグレード後に証明書を復元する 137

アップグレード後に Cisco DCNM スタンドアロン セットアップで証明書を復元する 138

アップグレード後に Cisco DCNM ネイティブ HA セットアップで証明書を復元する 139

以前にインストールされた CA 署名付き証明書の回復と復元 140

インストールした証明書の確認 141

---

## CHAPTER 10

ファイアウォール背後での Cisco DCNM の実行 145

ファイアウォール背後での Cisco DCNM の実行 145

カスタム ファイアウォールの設定 148

---

**CHAPTER 11**

**Cisco DCNM サーバのセキュアなクライアント通信 151**

Cisco DCNM サーバのセキュアなクライアント通信 151

仮想アプライアンスの HA 環境で Cisco DCNM 上の SSL/HTTPS を有効にする 151

---

**CHAPTER 12**

**ハイ アベイラビリティ環境でのアプリケーションの管理 153**

Information About Application Level HA in the Cisco DCNM オープン仮想アプライアンスのアプリケーション レベル HA に関する情報 153

自動フェールオーバー 154

手動でトリガされたフェールオーバー 155

ネイティブ HA フェールオーバーおよびトラブルシューティング 155

アプリケーションハイ アベイラビリティ 157

データセンターのネットワーク管理 158

RabbitMQ 160

リポジトリ 161

---

**CHAPTER 13**

**DCNM 展開後にユーティリティ サービスを管理する 163**

DCNM インストール後のネットワーク プロパティ 163

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 164

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 166

DCNM インストール後に DCNM サーバパスワードを変更する 174

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 175

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 175

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 177

ユーティリティ サービスの詳細 182

ネットワーク管理 182

オーケストレーション 182

電源オン自動プロビジョニング 183

アプリケーションとユーティリティ サービスの管理 183

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 184

ユーティリティ サービスの停止、開始、リセット 185

IPv6 の SFTP サーバアドレスの更新 186

---

CHAPTER 14

DCNM 検証を行う Tetration エージェント 187

DCNM 検証を行う Tetration エージェント 187

---

CHAPTER 15

TACACS+ サーバ経由で認証をセットアップ 191

TACACS+ Server 経由のリモート認証 191





# 第 1 章

## 概要

Cisco Data Center Network Manager (DCNM) は、Cisco NXOS ベースのストレージ ファブリックの管理システムです。データセンター ネットワーク インフラストラクチャのプロビジョニング、モニタリング、およびトラブルシューティングに加えて、Cisco DCNM はデータセンターのルーティング、スイッチング、およびストレージ管理のニーズを満たす包括的な機能セットを提供します。これにより、プログラマブル ファブリックのプロビジョニングが合理化され、SAN コンポーネントがモニタされます。

Cisco DCNM は、Cisco Nexus シリーズ スイッチ、Cisco MDS および Cisco Unified Computing System (UCS) に単一の Web ベース管理コンソールを通して、高度なレベルの可視性とコントロールを提供します。Cisco DCNM には、Cisco DCNM SAN クライアントとデバイス マネージャの機能も含まれています。

ここでは、次の項目について説明します。

- [はじめに, on page 1](#)
- [Installation Options, on page 2](#)
- [展開オプション, on page 2](#)
- [root および sysadmin のユーザー権限, on page 3](#)

## はじめに

Cisco DCNM は、スイッチ設定コマンドにコマンドライン インターフェイス (CLI) に代理を提供します。

Cisco DCNM には、これらの管理アプリケーションが含まれます。

### Cisco DCNM Web UI

Cisco DCNM Web UI では、Web ブラウザを使用してリモートの場所から Cisco MDS and Nexus イベント、パフォーマンス、インベントリのレポートをモニタし取得するように操作できます。ライセンスと検索は Cisco DCNM Web UI の一部です。

### Performance Manager

Performance Manager は SNMP を使用してデータを取り込み、詳細なトラフィック分析を行います。このデータは、Cisco DCNM Web UI で表示可能なさまざまなグラフや表にコンパイルされません。

## Installation Options

Cisco DCNM ソフトウェア イメージは、Cisco DCNM インストーラ、署名証明書、および署名検証スクリプトを使用してパッケージ化されます。目的の Cisco DCNM インストーラ イメージの ZIP ファイルをディレクトリに解凍します。README ファイルの手順に従って、イメージの署名を確認します。このパッケージからのインストーラにより、Cisco DCNM ソフトウェアがインストールされます。

### DCNM オープン仮想アプライアンス (OVA) インストーラ

このインストーラは、オープン仮想アプライアンス ファイル (.ova) として使用できます。インストーラには、事前にインストールされた OS、DCNM、およびプログラミング可能なファブリックに必要なその他のアプリケーションが含まれています。

### DCNM ISO 仮想アプライアンス (ISO) インストーラ

このインストーラは ISO イメージファイル (.iso) として使用できます。インストーラは、動的ファブリック自動化に必要な OS、DCNM、およびその他のアプリケーションのバンドルです。

## 展開オプション

Cisco DCNM インストーラは、次のいずれかのモードで展開できます。

### サポートされる遅延

Cisco DCNM LAN ファブリック 展開でサポートされる遅延は、次のとおりです。

- ネイティブ HA プライマリ アプライアンスとセカンダリ アプライアンス間の遅延は 50 ミリ秒です。
- DCNM ネイティブ HA プライマリ アプライアンスからスイッチまでの遅延は 50 ミリ秒です。
- DCNM コンピューティング間の遅延は 100 ミリ秒です。

### スタンドアロンサーバ

すべてのタイプのインストーラは、PostgreSQL データベースとともにパッケージ化されます。各インストーラのデフォルトのインストール手順によって、このモードの展開が行われます。



**Note** Cisco DCNM はネイティブ HA モードで展開することを推奨します。

### 仮想アプライアンスのハイ アベイラビリティ

DCNM 仮想アプライアンス (OVA と ISO の両方) をハイ アベイラビリティ モードで展開して、アプリケーションまたは OS で障害が発生した場合に復元力を持たせることができます。

### DCNM コンピューティング

コンピューティング ノードは、大規模なファブリックにサービスを提供するためにリソースを大量に消費するサービスを実行するスケールアウト アプリケーション ホスティング ノードです。コンピューティング ノードを追加すると、コンテナであるすべてのサービスがこれらのノードのみ実行されます。これには、Config Compliance、Endpoint Locator、および Virtual Machine Manager が含まれます。

### クラスタ モードの DCNM

クラスタモードでは、より多くのコンピューティング ノードを備えた Cisco DCNM サーバは、より多くのアプリケーションを展開するときにリソースを拡張するアーキテクチャを提供します。DCNM サーバは、コンテナ化されたアプリケーションを実行しません。非クラスタ化モードで動作するすべてのアプリケーションは、クラスタ化モードでも動作します。

### クラスタ化されていないモードの DCNM

非クラスタモードでは、Cisco DCNM は内部サービスの一部をコンテナとして実行します。Cisco DCNM は、一部のコンテナアプリケーションの実行にスタンバイ ノードのリソースを利用します。Cisco DCNM のアクティブノードとスタンバイ ノードは連携して動作し、DCNM とそのアプリケーションの全体的な機能と展開にリソースを拡張します。ただし、一部の高度なアプリケーションを実行したり、システムを拡張して Cisco AppCenter を介して配信されるアプリケーションをさらに導入したりするには、リソースが限られています。

## root および sysadmin のユーザー権限

次の表に、DCNM 11.5(1) と以前のリリースとのユーザー権限の違いをまとめます。



**Note** これは、DCNM OVA/ISO 展開にのみ適用されます。

説明	DCNM 11.5(1) リリースの機能	DCNM 11.4(1) および 11.3(1) リリースの機能	備考
su コマンド	ローカル <b>root</b> パスワードが必要です。 <b>sysadmin</b> ユーザーは <b>sudo su</b> コマンドを実行できません	システム管理者パスワードが必要 <b>su</b> は次のエイリアスです <b>sudo su</b>	リモート認証が設定されている場合でも、 <b>su</b> コマンドにはローカルパスワードが必要です。
appmgr change_pwd ssh root コマンド	このコマンドを実行できるのは <b>root</b> ユーザーだけです。	<b>sysadmin</b> もこのコマンドを実行できます。	-
appmgr root-access {permit deny ...} コマンド	<b>root</b> ユーザーのみがこのコマンドを実行できます	<b>sysadmin</b> ユーザーはこのコマンドを実行することもできます	-
appmgr remote-auth コマンド	<b>root</b> ユーザーのみがこのコマンドを実行できます	使用不可	-
その他の appmgr コマンド	<b>root</b> または <b>sysadmin</b> ユーザーはこれらのコマンドを実行できます	<b>root</b> または <b>sysadmin</b> ユーザーはこれらのコマンドを実行できます	-



## 第 2 章

# 注意事項と制約事項

- [注意事項と制約事項, on page 5](#)

## 注意事項と制約事項

Cisco DCNM のインストールとアップグレードのためのガイドラインと制限は以下のとおりです。

### 一般的なガイドラインと制限事項

- 次のパスワード要件に従います。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) の組み合わせを含めることができます。
  - パスワードは、`%^=&,*\'' <SPACE>` を除くすべての特殊文字を使用できます。
  - アップグレードした後で、新しい `sysadmin` パスワードを使用して、DCNM サーバにログインできます。しかし、Web UI にログインするには、古い DCNM パスワードを使用する必要があります。
  - 入力されている新しい管理パスワードは、次のシナリオで使用されています。
    - —コンソールを経由して DCNM アプライアンスにアクセスします。
    - —SSH を経由してアプライアンスにアクセスします。
    - —アプライアンスで実行されているアプリケーション (例: Postgres DBMS)
- DCNM をインストールするときに、起動プロセスを中断しないでください (Ctrl+ALT+DELETE キーを押すなど)。中断する場合は、インストールプロセスを再起動する必要があります。
- インストールまたはアップグレード後、そして Cisco DCNM アプライアンスでその他の操作を実行する前に、タイムゾーンを設定します。タイムゾーンの設定には NTP サーバを使用します。

- ネイティブ HA セットアップで実行中の Postgres データベースのステータスを確認するには、次のコマンドを使用します。

```
dcnm# su - postgres -c
dcnm# pg_ctl -D /usr/local/cisco/dcm/db/data status
```

**systemctl** コマンドは使用しないでください。

- ハッシュ (#) 記号でパスワードを開始しないでください。Cisco DCNM は、# 記号で始まるパスワードを暗号化されたテキストと見なします。

## 新規インストール

- 仮想アプライアンス (OVA/ISO) の場合、インストーラはオペレーティング システムと Cisco DCNM コンポーネントをインストールします。
- DCNM OVA は、vSphere クライアントを ESXi サーバに直接接続することで展開できます。

## アップグレード

- SSH セッションからインラインアップグレードを実行しないでください。セッションがタイムアウトし、アップグレードが不完全になることがあります。
- アップグレードする前に、以前のリリースのテレメトリを無効にします。
- コンピューティング ノードを展開する前に、テレメトリを無効にします。コンピューティング ノードを展開後、テレメトリを有効にできます。  
ネイティブ HA モードの DCNM の場合、テレメトリは 3 個のコンピューティング ノードのみでサポートされます。
- Network Insights アプリケーションを実行する必要がある場合、3 個のコンピューティング ノードをインストールする必要があります。
- インターフェイス設定を変更する前に、テレメトリを無効にします。設定を変更後、テレメトリを有効にできます。
- バックアップと復元プロセスの間、コンピューティング ノードはバックアップにも含まれません。新しいコンピューティングを展開後、コンピューティング ノードでバックアップを復元できます。  
バックアップがなかった場合、3 コンピューティング ノードを接続解除し、すべてのコンピューティング ノードでデータを消去します。Cisco DCNM Web Client UI で、[アプリケーション (Application)] > [コンピューティング (Compute)] に移動します。[+] アイコンを選択して、コンピューティング ノードに参加します。
- コンピューティング ノードでデータを消去するには、SSH セッションを通してコンピューティング ノードにログオンして、**rm -rf /var/afw/vols/data** コマンドを使用してデータを消去します。



---

**Note** すべてのコンピューティング ノードで上のコマンドを個別に実行し、データを消去する必要があります。

---

- アップグレード後に NIR アプリケーションを起動する前に、DCNM Web UI で **[アプリケーション (Application)] > [設定 (Preferences)]** を選択します。必要に応じてネットワーク設定を変更します。アップグレード後にファブリックのテレメトリを有効にする前にネットワーク設定を変更しないと、設定は完了しません。この問題を解決するには、NIR アプリを停止し、ネットワーク設定を変更してからアプリを再起動する必要があります。





## 第 3 章

### 前提条件

この章では、*Cisco Data Center Network Manager* の展開に関するリリース固有の前提条件について説明します。

- [DCNM オープン仮想アプライアンスの前提条件, on page 9](#)
- [DCNM ISO 仮想アプライアンスの前提条件, on page 10](#)
- [Cisco DCNM 仮想アプライアンス HA の前提条件, on page 10](#)

### DCNM オープン仮想アプライアンスの前提条件

Cisco DCNM オープン仮想アプライアンスをインストールする前に、次のソフトウェアとデータベース要件を満たす必要があります。

- Windows サーバで実行されている VMware vCenter サーバ (または代わりに仮想アプライアンスとして実行されている)。
- vCenter にインポートされた ESXi ホストを VMware します。
- ESXi ホスト上の 3 つのポート グループ: DCNM 管理ネットワーク、拡張されたファブリック管理ネットワーク、EPL およびテレメトリ機能用インバンドインターフェイス。
- Cisco DCNM オープン仮想アプライアンスにより管理される Cisco プログラマブルファブリックでスイッチの数を決定します。
- VMware vCenter Web クライアントが DCNM OVA インストールのため起動されているホストで、ウイルス対策ソフトウェア (McAfee など) が実行されていないことを確認します。ウイルス対策ソフトウェアが実行中の場合、DCNM インストールに失敗する可能性があります。
- DCNM オープン仮想アプライアンスは、ESXi ホストで展開されているものとも互換性があります。ESXi ホストでの展開の場合、VMware vSphere クライアントアプリケーションは必須です。



**Note** CPU およびメモリ要件の詳細については、[memory requirements](#), Cisco DCNM リリース ノート、リリース *11.0(1)* の「」のセクションを参照してください。

## DCNM ISO 仮想アプライアンスの前提条件

既存のアクティブ/スタンバイ ネイティブ HA DCNM アプライアンスに、追加のアクティブまたはスタンバイ ノードを追加しないようにしてください。インストールは失敗します。

Cisco DCNM ISO 仮想アプライアンスをインストールする前に、ホストまたはハイパーバイザを設定する必要があります。要件に基づいて、CPUとメモリの要件に基づいて、セットアップホストマシンまたはハイパーバイザを設定します。



**Note** CPUとメモリ要件の詳細については、「Cisco DCNM リリース ノート」の「サーバリソースの要件」セクションを参照してください。

次のいずれかのホストを設定して、DCNM ISO 仮想アプライアンスをインストールすることができます。

### VMware ESXi

ホストマシンはESXiを使用してインストールされ、2つのポートグループが作成されます。1つはEFMネットワーク用、もう1つはDCNM管理ネットワーク用です。拡張ファブリックインバンドネットワークはオプションです。

### カーネルベース仮想マシン (KVM)

ホストマシンは、Red Hat Enterprise Linux (RHEL) 5.x、6.xまたは7.xとともにインストールされ、KVMライブラリとグラフィカルユーザーインターフェイス(GUI)にアクセスします。GUIでは、仮想マシン マネージャにアクセスして、Cisco DCNM 仮想アプライアンスを展開して管理することができます。2つのネットワークが作成されます (EFM ネットワークと DCNM 管理ネットワーク)。通常、DCNM管理ネットワークは、他のサブネットからアクセスするためにブリッジされません。さまざまなタイプのネットワークを作成する方法については、KVMのマニュアルを参照してください。



**Note** CentOS や Ubuntu などの他のプラットフォームの KVM は、互換性マトリクスが増加するためサポートされません。

## Cisco DCNM 仮想アプライアンス HA の前提条件

ここでは、ハイアベイラビリティ (HA) 環境を得るための前提条件について説明します。

## HA モードで Cisco DCNM 仮想アプライアンスを展開する

2つのスタンドアロン仮想アプライアンス (OVA と ISO) を展開する必要があります。両方の仮想アプライアンスを展開する場合は、次の条件を満たす必要があります。

- アクティブ OVA の eth0 は、スタンバイ仮想アプライアンスの eth0 と同じサブネットに存在する必要があります。アクティブ仮想アプライアンスの eth1 は、スタンバイ OVA の eth1 と同じサブネットに存在する必要があります。アクティブ仮想アプライアンスの eth2 は、スタンバイアプライアンスの eth2 と同じサブネットに存在する必要があります。
- 両方の仮想アプライアンスは、同じ管理パスワードを使用して展開する必要があります。このプロセスにより、両方の仮想アプライアンスが互いに重複していることが保証されます。
- 既存のアクティブ/スタンバイ ネイティブ HA DCNM アプライアンスに追加のアクティブまたはスタンバイノードを追加しようとすると、インストールが失敗します。

## 仮想 IP アドレスの可用性

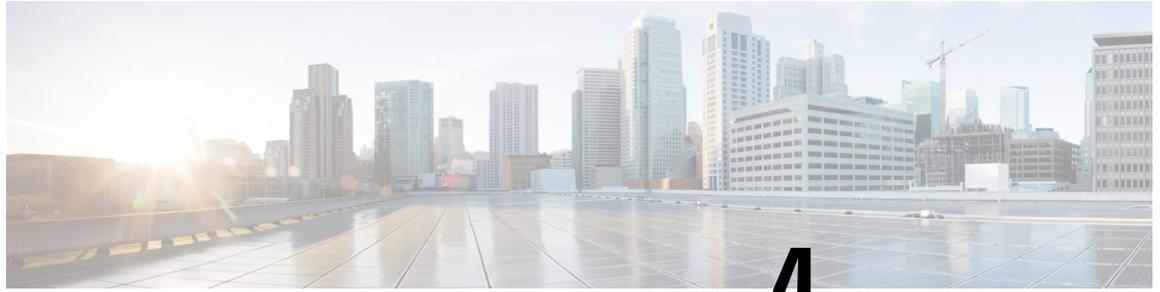
サーバ eth0 および eth1 インターフェイスを設定するには、2つの空き IP アドレスが必要です。ただし、eth2 IP アドレスはオプションです。最初の IP アドレスは、管理アクセス ネットワークで使用されます。これは、OVA の管理アクセス (eth0) インターフェイスと同じサブネット内にある必要があります。2番目の IP アドレスは、enhanced fabric management (eth1) インターフェイス (スイッチ/POAP 管理ネットワーク) と同じサブネット内にある必要があります。

DCNM サーバのインバンド 管理 (eth2) の設定を選択した場合は、別の IP アドレスを予約する必要があります。ネイティブ HA セットアップでは、プライマリ サーバとセカンダリ サーバの eth2 インターフェイスが同じサブネット内にある必要があります。

## NTP サーバのインストール

大部分の HA 機能を動作させるには、NTP サーバを使用して両方の OVA の時刻を同期する必要があります。通常、インストールは管理アクセス ネットワーク (eth0) インターフェイスにあります。





## 第 4 章

# Cisco DCNM のインストール

### サポートされる遅延

Cisco DCNM LAN ファブリック 展開でサポートされる遅延は、次のとおりです。

- ネイティブ HA プライマリ アプライアンスとセカンダリ アプライアンス間の遅延は 50 ミリ秒です。
- DCNM ネイティブ HA プライマリ アプライアンスからスイッチまでの遅延は 50 ミリ秒です。
- DCNM コンピューティング間の遅延は 100 ミリ秒です。

この章は、次の項で構成されています。



(注) リリース11.4(1)以降、コンピューティングとともに、Cisco DCNM をスタンドアロンおよびネイティブ HA モードで Cisco Applications Services Engine にインストールできます。詳細については、『[Cisco Application Services Engine Installation Guide For Cisco DCNM](#)』を参照してください。

- [オープン仮想アプライアンスで DCNM をインストールする \(13 ページ\)](#)
- [ISO 仮想アプライアンスで DCNM をインストールする \(34 ページ\)](#)
- [Cisco APIC SE への Cisco DCNM SE ISO のインストール \(69 ページ\)](#)
- [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 \(71 ページ\)](#)
- [Cisco DCNM コンピューティング ノードのインストール, on page 76](#)

## オープン仮想アプライアンスで DCNM をインストールする

この章は、次の項で構成されています。

## オープン仮想アプライアンス ファイルのダウンロード

オープン仮想アプライアンスをインストールする最初の手順は、`dcnm.ova` ファイルをダウンロードすることです。OVF テンプレートを展開するとき、コンピュータの `dcnm.ova` ファイルを指します。



---

**Note** HA アプリケーション機能を使用する予定の場合は、`dcnm.ova` ファイルを 2 回展開する必要があります。

---

### Procedure

---

- Step 1** 次のサイトに移動します。 <http://software.cisco.com/download/>。  
ダウンロード可能な Cisco DCNM の最新リリース ソフトウェアのリストが表示されます。
  - Step 2** 最新リリースのリストで、 を選択します。
  - Step 3** DCNM オープン仮想アプライアンス インストーラを検索し、[ダウンロード (Download)] アイコンをクリックします。
  - Step 4** `dcnm.ova` ファイルをディレクトリに保存し、OVF テンプレートの展開を開始するときに見つけやすくなります。
- 

## OVF テンプレートとしてのオープン仮想アプライアンスの展開

OVA 仮想アプライアンス ファイルをダウンロードしたら、vSphere Client アプリケーションからまたは vCenter サーバから OVF テンプレートを展開します。



---

**Note** HA セットアップ用に 2 つの OVA を展開します。

---

### Procedure

---

- Step 1** vCenter サーバアプリケーションを開き、vCenter ユーザークレデンシャルを使用して vCenter サーバに接続します。

**Note** ESXi ホストを vCenter サーバアプリケーションに追加する必要があります。

VMware vsphere のバージョンによっては、大規模またはコンピューティング OVA を展開する場合に、ユーザーが追加のディスクサイズを指定できないため、Web HTML5 インターフェイスが適切に動作しない場合があります。したがって、VM を展開するには Flex インターフェイスを使用することをお勧めします。

ESXi 6.7 を使用して OVF テンプレートを展開している場合、HTML5 で Internet Explorer ブラウザを使用すると、インストールが失敗します。ESXi および 6.7 を使用して OVF テンプレートを正常に展開するには、次のいずれかのオプションを確認します。

- Mozilla Firefox ブラウザ、HTML 5 サポートあり  
HTML 5 がサポートされていない場合の flex インターフェイスの使用
- Mozilla Firefox ブラウザ、flex\flash サポートあり
- Google Chrome ブラウザ、HTML 5 サポートあり  
HTML 5 がサポートされていない場合の flex インターフェイスの使用

**Step 2** [ホーム (Home)] > [インベントリ (Inventory)] > [ホストおよびクラスター (Hosts and Clusters)] に移動し、OVF テンプレートが展開されているホストを選択します。

**Step 3** [ホスト (Host)] を右クリックして [OVF テンプレートの展開 (Deploy OVF Template)] を選択します。

[アクション (Actions)] > [OVF テンプレートの展開 (Deploy OVF Template)] を選択することもできます。

[OVF テンプレートの展開 (Deploy OVF Template)] ウィザードが表示されます。

**Step 4** [テンプレートの選択 (Select template)] 画面で、OVA イメージをダウンロードした場所に移動します。

次のいずれかの方法で OVA ファイルを選択できます。

- [URL] オプション ボタンを選択します。イメージファイルの場所へのパスを入力します。
- [ローカル ファイル (Local File)] オプション ボタンを選択します。[参照 (Browse)] をクリックします。イメージが保存されているディレクトリに移動します。[OK] をクリックします。

[次へ (Next)] をクリックします。

**Step 5** OVF テンプレートの詳細を確認して、[次へ (Next)] をクリックします。

**Step 6** [エンドユーザー ライセンス契約 (End User License Agreement)] 画面で、ライセンス契約書をお読みください。

[承認 (Accept)] をクリックし、[次へ (Next)] をクリックします。

**Step 7** [名前と場所 (Name and Location)] 画面で、次の情報を入力します。

- [名前 (Name)] フィールドに、OVF の適切な名前を入力します。  
**Note** VM 名がインベントリ内で固有であることを確認します。
- [参照 (Browse)] タブで、適切な ESXi ホストの下の展開場所として [データセンター (Datacenter)] を選択します。

[次へ (Next)] をクリックします。

**Step 8** [設定の選択 (Select Configuration)] ドロップダウン リストから設定を選択します。

- **[小規模 (Small)]** (ラボまたは POC) を選択して、8 個の vCPU、24 GB RAM を搭載した仮想マシンを設定します。

コンセプト実証には [小規模 (Small)]、時間の増加が予想されないスイッチ 50 個未満のその他の小規模環境の場合は [小規模 (small-scale)] を選択します。

- 16 個の vCPU、32GB RAM を搭載した仮想マシンを設定するには、**[大規模 (Large)]** (生産) を選択します。

より優れた RAM、ヒープメモリ、および CPU を利用するために、50 個を超えるデバイスを管理する場合は、大規模な展開構成を使用することを推奨します。設定が増える可能性がある場合は、[大規模 (Large)] を選択します。

- **[コンピューティング (Compute)]** を選択して、16 個の vCPU、64GB RAM を搭載した仮想マシンを設定するには、

展開でアプリケーションを使用するには、コンピューティング モードで DCNM を展開する必要があります。

- **[特大 (Huge)]** を選択して、32 vCPU、128GB RAM を搭載した仮想マシンを設定します。

この設定は、SAN 管理用に DCNM を導入し、SAN Insights 機能を使用する場合に推奨されません。

- **[ComputeHuge]** を選択して、32 vCPU、128GB RAM を搭載した仮想マシンを設定します。

この設定は、Cisco Network Insights アプリケーションを使用する場合に推奨されます。

[Next] をクリックします。

**Step 9** [リソースの選択 (Select a resource)] 画面で、OVA テンプレートを展開するホストを選択します。

[Next] をクリックします。

**Step 10** [ストレージの選択 (Select storage)] 画面で、データストアと使用可能なスペースに基づいて、仮想マシン ファイルのディスク形式と宛先ストレージを選択します。

- a) ドロップダウン リストから仮想ディスク形式を選択します。

使用可能なディスクの形式は次のとおりです。

**Note** 仮想アプライアンスに必要なストレージとして十分な容量があり、仮想ディスクに対して領域の特定の割り当てを設定したい場合は、次のシック プロビジョン タイプのいずれかを選択します。

- **Thick Provision Lazy Zeroed:** 仮想ディスクが作成されるときに、仮想ディスク ファイルに対して指定された領域全体が割り当てられます。仮想ディスクが作成されたが、仮想ディスクから最初に書き込む際に後でオンデマンドでゼロ設定されると、物理デバイスに残っているデータは消去されません。
- **Thin Provision:** 使用可能なディスク容量は 100 GB 未満です。最初のディスク使用量は 3GB で、データベースのサイズは管理対象デバイス数が増加するにつれて増加します。

- **Thick Provision Eager Zeroed:** 仮想ディスクに必要なスペースは、仮想ディスクを作成する際に割り当てられます。Lazy Zeroed オプションと異なり、仮想ディスクの作成時に、物理デバイスに残っているデータは消去されます。

**Note** 500G を使用すると、DCNM インストールはオプション Thick Provision Eager Zeroed を使用してスタックされているように見えます。ただし、完了するには時間がかかります。

- b) ドロップダウン リストから VM ストレージ ポリシーを選択します。

デフォルトでは、ポリシーは選択されていません。

- c) クラスタデータストアを表示するには、[ストレージ DRS クラスタからデータストアを表示する (Show datastores from Storage DRS clusters)] をオンにします。
- d) データストアで利用可能な仮想マシンの宛先ストレージを選択します。

[次へ (Next)] をクリックします。

## Step 11

[ネットワークの選択 (Select Networks)] ページで、OVF テンプレートで使用されているネットワークをインベントリのネットワークにマッピングします。

### • dcnm-mgmt network

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

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る必要があります。

### • enhanced-fabric-inband

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行います。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る必要があります。

**Note** enhanced-fabric-inband 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。

ただし、**appmgr update network-properties** コマンドを使用して、必要に応じてインストール後にネットワーク プロパティを編集できます。詳細については、「[DCNM インストール後のネットワーク プロパティ, on page 163](#)」を参照してください。

[宛先ネットワーク (Destination Network)] ドロップダウン リストから、対応するネットワークに関連付けられているサブネットに対応しているポートグループに、ネットワークマッピングを関連付けることを選択します。

HA 機能用に複数の DCNM オープン仮想アプライアンスを展開する場合は、次の条件を満たす必要があります。

- 両方の OVA には、同じサブネット内に管理アクセス (eth0)、拡張ファブリック管理 (eth1)、およびインバンド管理 (eth2) インターフェイスが必要です。
- 各 OVA には、異なるサブネットに eth0 と eth2 のインターフェイスが必要です。
- 両方の OVA は、同じ管理パスワードを使用して展開する必要があります。これは、両方の OVA がアプリケーションアクセスのため互いに重複していることを確認するためです。  
パスワードは、%\$^=;.\*\'' <SPACE> を除くすべての特殊文字を使用できます。

[Next] をクリックします。

**Step 12** [テンプレートのカスタマイズ (Customize template)] 画面で、管理プロパティの情報を入力します。

[IP アドレス (IP Address): (DCNM の外部管理アドレス用)、[サブネット マスク (Subnet Mask)], および [デフォルト ゲートウェイ (Default Gateway)] を入力します。

**Note** ネイティブ HA のインストールとアップグレード時に、アクティブ アプライアンスとスタンバイアプライアンスの両方に適切な管理プロパティが提供されていることを確認します。

[管理ネットワーク (Management Network)] プロパティに有効な値が追加されていることを確認します。無効な値を持つプロパティは割り当てられません。有効な値を入力するまで、VM の電源はオンになりません。

リリース 11.3(1) 以降では、大規模なコンピューティング構成の場合、VM に追加のディスク領域を追加できます。32GB から最大 1.5TB のディスク領域を追加できます。[追加ディスク サイズ (Extra Disk Size)] フィールドに、VM に作成される追加のディスク サイズを入力します。

[次へ (Next)] をクリックします。

**Step 13** [完了の準備 (Ready to Complete)] 画面で、展開設定を確認します。

[戻る (Back)] をクリックして前の画面に移動し、設定を変更します。

[終了 (Finish)] をクリックし、OVF テンプレートを展開します。

vSphere クライアントの [最近のタスク (Recent Tasks)] 領域に展開ステータスが表示されます。

**Note** この展開がアップグレードプロセスの一部である場合は、VM の電源をオンにしないでください。MAC アドレスを編集して提供し、VM の電源をオンにします。

**Step 14** インストールが完了したら、インストールされている VM を右クリックし、[電源 (Power)] > [電源オン (Power On)] を選択します。

**Note** VM の電源をオンにする前に、選択した展開設定に基づき、CPU やメモリなど VM に予約されている適切なリソースがあることを確認します。

[最近のタスク (最近のタスク)] 領域にステータスが表示されます。

**Step 15** [概要 (Summary)] タブに移動し、[設定 (Settings)] アイコンをクリックして、[Web コンソールの起動 (Launch Web Console)] を選択します。

DCNM アプライアンスが設定されていることを示すメッセージが画面に表示されます。

```
*****
Please point your web browser to https://<IP-address>:<port-number>
to complete the application
*****
```

ブラウザに URL をコピーして貼り付け、Web インストーラを使用してインストールを完了します。

---

### What to do next

スタンドアロンモードまたはネイティブ HA モードで DCNM をインストールするように選択できます。詳細については、または [ネイティブ HA モードでの Cisco DCNM OVA のインストール](#), on [page 24](#) を参照してください。

## スタンドアロンモードでの Cisco DCNM OVA のインストール

[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。

Web インストーラから Cisco DCNM のインストールを完了するには、次の手順を実行します。

### Procedure

---

**Step 1** [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。

**Caution** 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。

**Step 2** [Cisco DCNM インストーラ (Cisco DCNM Installer)] 画面で、[新規インストール - スタンドアロン (Fresh Installation - Standalone)] オプション ボタンを選択します。

[Next] をクリックします。

**Step 3** [インストール モード (Install Mode)] タブで、DCNM 導入タイプを選択します。

[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 OVA DCNM アプライアンスの [LAN ファブリック (LAN Fabric)] インストール モードを選択します。

クラスタモードで Cisco DCNM を展開する場合は、[クラスタ モードを有効にする (Enable Clustered Mode)] チェックボックスをオンにします。コンピューティング ノードが Cisco DCNM [Web UI] > [アプリケーション (Applications)] > [コンピューティング (Compute)] に表示されます。アプリケーションはコンピューティングノードで実行されます。後でコンピューティングノードをクラスタに追加できます。You can add the compute nodes to a Cluster, later.

コンピューティング クラスタが必要な場合は、仮想アプライアンスの設定時に 3NIC があることを確認します。後で NIC をインストールすることはサポートされていません。3つのNICがない場合は、[クラスタモードの有効化 (Enable Clustered Mode)] は使用できません。

**Note** [クラスタモードを有効にする (Enable Clustered Mode)] がオンになっている場合、設定、コンプライアンス、EPL、NIA などのアプリケーションはコンピューティング ノードがインストールされるまで動作しません。

[Next] をクリックします。

**Step 4** [管理 (Administration)] タブで、パスワードに関する情報を入力します。

- [管理者のパスワード] フィールドで、Cisco DCNM のアプリケーションに接続するために使用されるパスワードを入力してください。

パスワードは、 `'%$^=;.*\'' <SPACE>` を除くすべての特殊文字を使用できます。

[管理者パスワードの確認] フィールドにパスワードをもう一度入力します。

- [データベースパスワード (Database Password)] フィールドに、PostgreSQL データベースのパスワードを入力します。

すべての特殊文字は  `'%$^=;.*\'' <SPACE>` を除き、パスワードに使用できます。

[管理者パスワードの確認] フィールドにパスワードをもう一度入力します。

**Note** [データベースパスワード (Database Password)] フィールドを空白のままにすると、管理者パスワードが PostgreSQL のパスワードと見なされます。

- [Superuser Password (root)] フィールドに、スーパーユーザーが root 権限にアクセスするためのパスワードを入力します。

[スーパーユーザーパスワード (Superuser Password)] フィールドにもう一度パスワードを入力します。

**Note** スーパーユーザーパスワードが空白のままの場合は、管理者パスワードをスーパーユーザーパスワードと見なします。ただし、セキュリティ上の理由から、強力なパスワードを設定することを推奨します。

入力したパスワードを表示するには、[入力したパスワードを表示する (Show passwords in clear text)] チェックボックスをオンにします。

[次へ (Next)] をクリックします。

**Step 5** [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。IPv6 アドレスを使用して DNS サーバを設定することもできます。

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。

**Note** Network Insights アプリケーションを使用している場合は、DNS サーバが有効で到達可能であることを確認します。

- **[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。

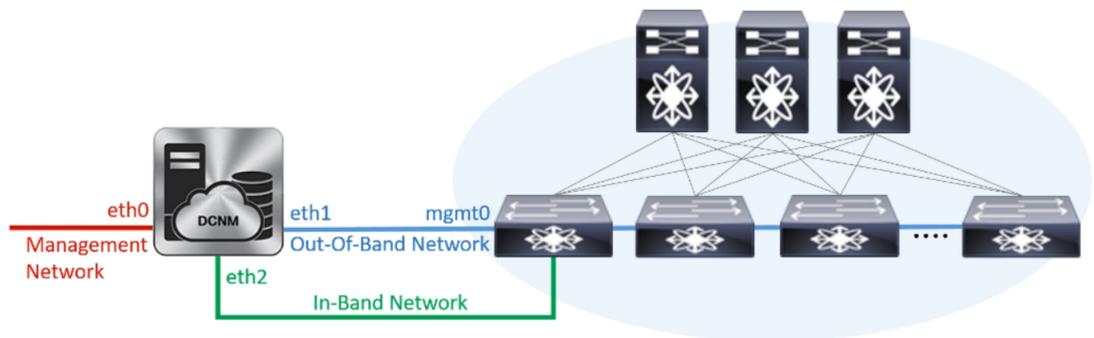
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **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。

**Step 6** **[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。

**Figure 1: Cisco DCNM 管理ネットワーク インターフェイス**



- a) **[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。

**Note** Cisco DCNM リリース 11.2(1) から、管理ネットワークの IPv6 アドレスも使用できます。

(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。

- b) **[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。

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。

**Note** 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。

- c) (Optional) [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。

ステップ [Step 3, on page 19](#) でクラスタの有効化モードを選択した場合、このフィールドは必須です。

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。

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。

**Note** 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。

コンピューティングクラスタが必要な場合は、仮想アプライアンスの設定時に 3NIC があることを確認します。後で NIC をインストールすることはサポートされていません。3 NICs がなく、[クラスタ モードを有効にする (Enable Clustered Mode)] が使用できない場合、eth2 インターフェイスを構成できません。

ただし、`appmgr update network-properties` コマンドを使用して、必要に応じてインストール後にネットワーク プロパティを編集できます。詳細については、「[DCNM インストール後のネットワーク プロパティ, on page 163](#)」を参照してください。

[Next] をクリックします。

- Step 7** [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]、および [クラスタ モード設定] を構成します。

**Note** デバイス コネクタは、デフォルトで有効になります。

デバイス コネクタは、クラウドベース管理プラットフォームである Cisco Intersight の機能を実現する組み込み管理コントローラです。

- a) (Optional) [プロキシ サーバー (Proxy Server)] フィールドで、プロキシ サーバーの IP アドレスを入力します。

プロキシ サーバーは RFC1123 準拠名でなければなりません。

**Note** デフォルトで、ポート 80 がプロキシ サーバに使用されます。<proxy-server-ip>:<port> を使用して、プロキシ サーバに異なるポートを使用します。

プロキシ サーバが認証を必要とする場合、関連するユーザー名とパスワードを [プロキシ サーバ ユーザー名 (Proxy Server Username)] と [プロキシ サーバ パスワード (Proxy Server Password)] フィールドに入力します。

- b) [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。

すべてのアプリケーションがこのサブネットからの IP アドレスを使用します。

- c) [クラスタ モード設定 (**Clustered mode configuration**)] 領域で、ネットワーク設定を構成して、クラスタ モードで DCNM インスタンスを展開します。クラスタ モードで、アプリケーションは個別のコンピューティング ノードで実行されます。

手順 [Step 3, on page 19](#) で [クラスタ モードを有効にする (**Enable Clustered Mode**)] チェックボックスをオンにしている場合、[クラスタ モード設定 (**Cluster Mode configuration**)] 領域が表示されます。

**Note** [クラスタ モード (**Clustered mode**)] では、Cisco DCNM アプリケーションは別の DCNM コンピューティング ノード実行します。

- [アウトオブバンド IPv4 ネットワーク アドレス プール (**Out-of-Band IPv4 Network Address Pool**)] で、クラスタ モードで使用するアウトオブバンド IPv4 ネットワークからアドレスプールを入力します。

オプションで、[アウトオブバンド IPv6 ネットワーク アドレス プール (**Out-of-Band IPv6 Network Address Pool**)] フィールドに IPv6 アドレス プールを入力することもできます。

- [インバンド IPv4 ネットワーク アドレス プール (**In-Band IPv4 Network Address Pool**)] で、クラスタ モードで使用するインバンド IPv4 ネットワークからアドレスプールを入力します。

オプションで、[インバンド IPv6 ネットワーク アドレス プール (**In-Band IPv6 Network Address Pool**)] フィールドに IPv6 アドレス プールを入力することもできます。

アドレスは eth1 サブネットから利用可能で小さい IP アドレスのプレフィックスである必要があります。例: eth1 サブネットがインストール中に 10.1.1.0/24 に設定された場合、10.1.1.240/28 を使用します。このサブネットは、最小で /28 (16 アドレス) および最大で /24 (256 アドレス) である必要があります。また、east-west プール以上にしないでください。このサブネットは、スイッチとの通信のためコンテナに割り当てられます。

[次へ (**Next**)] をクリックします。

**Step 8** [概要 (**Summary**)] タブで、設定の詳細を確認します。

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 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
*****

```

**Note** 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。

**Note** インストールが進行中に管理 IP アドレスを使用して DCNM Web UI にアクセスする場合、エラーメッセージがコンソールに表示されます。

```

*****
*Preparing Appliance*
*****

```

## What to do next

適切なクレデンシャルを使用して DCNM Web UI にログオンします。

[設定 (Settings)] アイコンをクリックし、[DCNM の詳細 (About DCNM)] を選択します。展開したインストールタイプを表示して確認できます。

デバイス管理にインバンド管理 (eth2) IP アドレスを設定している場合、スタンドアロンサーバにログインし、次のコマンドを使用して、サーバの eth2 からスイッチにインバンドネットワーク到達可能性を設定します。

```
dcnm# appmgr update network-properties add route ipv4 eth2 <ipv4-network-ip-address/prefix>
```

例: 10.0.0.x/30 サブネットを介して接続しているすべてのファブリック リンクを備えた 4 つのスイッチがある場合、およびサブネット 40.1.1.0/24 のインバンド到達可能性に対してすべてのスイッチがループバック インターフェイスで設定されている場合、次のコマンドを使用します。

```

dcnm# appmgr update network-properties session start
dcnm# appmgr update network-properties add route ipv4 eth2 10.0.0.0/24
dcnm# appmgr update network-properties add route ipv4 eth2 40.1.1.0/24
dcnm# appmgr update network-properties session apply

```

## ネイティブ HA モードでの Cisco DCNM OVA のインストール

ネイティブ HA は ISO または OVA インストールのみを使用した DCNM アプライアンスでサポートされています。

デフォルトでは、Cisco DCNM を使用した組み込み型 PostgreSQL データベース エンジンです。ネイティブ HA 機能は、Cisco DCNM アプライアンスによって、リアルタイムで同期されている組み込みデータベースを使用したアクティブおよびスタンバイ アプリケーションとして実行可能です。したがって、アクティブ DCNM が機能していない場合、スタンバイ DCNM は同じデータベースデータを引き継ぎ、操作を再開します。

DCNM のネイティブ HA をセットアップするには、次の作業を実行します。

## Procedure

- Step 1** 2つの DCNM 仮想アプライアンス (OVA または ISO のいずれか) を展開します。
- 例えば、**dcnm1** および **dcnm2** として示します。
- Step 2** **dcnm1** をプライマリ ノードとして設定します。 **dcnm1** 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。
- Caution** 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 **SYSTEMRESOURCEERROR** 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)] タブで、[新規インストール - HA プライマリ (Fresh Installation - HA Primary)] オプション ボタンを選択して、**dcnm1** をプライマリ ノードとしてインストールします。
- [Next] をクリックします。
- c) [インストール モード (Install Mode)] タブで、DCNM 導入タイプを選択します。
- [インストール モード (Installation mode)] ドロップダウン リストから DCNM アプライアンスの [LAN ファブリック (LAN Fabric)] インストール モードを選択します。
- クラスタ モードで Cisco DCNM を展開する場合は、[クラスタ モードを有効にする (Enable Clustered Mode)] チェックボックスをオンにします。コンピューティング ノードが Cisco DCNM [Web UI] > [アプリケーション (Applications)] > [コンピューティング (Compute)] に表示されます。アプリケーションはコンピューティング ノードで実行されます。後でコンピューティング ノードをクラスタに追加できます。You can add the compute nodes to a Cluster, later.
- コンピューティング クラスタが必要な場合は、仮想アプライアンスの設定時に 3NIC があることを確認します。後で NIC をインストールすることはサポートされていません。3つのNICがない場合は、[クラスタモードの有効化 (Enable Clustered Mode)] は使用できません。
- Note** [クラスタ モードを有効にする (Enable Clustered Mode)] がオンになっている場合、設定、コンプライアンス、EPL、NIA などのアプリケーションはコンピューティング ノードがインストールされるまで動作しません。
- [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。
- [管理者のパスワード] フィールドで、Cisco DCNM のアプリケーションに接続するために使用されるパスワードを入力してください。
- パスワードは、 `'%$^=;,*\' " <SPACE>` を除くすべての特殊文字を使用できます。

[管理者パスワードの確認] フィールドにパスワードをもう一度入力します。

- [データベース パスワード (Database Password)] フィールドに、PostgreSQL データベースのパスワードを入力します。

すべての特殊文字は %\$^=;\*'" <SPACE> を除き、パスワードに使用できます。

[管理者パスワードの確認] フィールドにパスワードをもう一度入力します。

**Note** [データベース パスワード (Database Password)] フィールドを空白のままにすると、管理者パスワードが PostgreSQL のパスワードと見なされます。

- [Superuser Password (root)] フィールドに、スーパーユーザーが root 権限にアクセスするためのパスワードを入力します。

[スーパーユーザー パスワード (Superuser Password)] フィールドにもう一度パスワードを入力します。

**Note** スーパーユーザー パスワードが空白のままの場合は、管理者パスワードをスーパーユーザー パスワードと見なします。ただし、セキュリティ上の理由から、強力なパスワードを設定することを推奨します。

入力したパスワードを表示するには、[入力したパスワードを表示する (Show passwords in clear text)] チェックボックスをオンにします。

[次へ (Next)] をクリックします。

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。

**Note** Network Insights アプリケーションを使用している場合は、DNS サーバが有効で到達可能であることを確認します。

- [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。

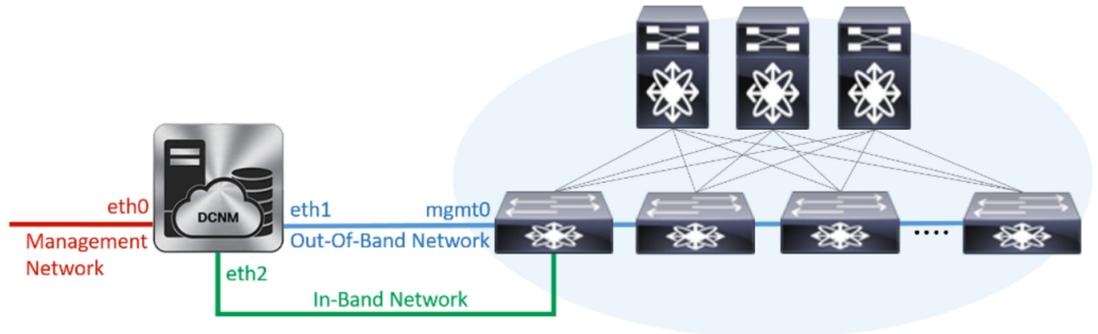
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- 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。

Figure 2: 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。

**Note** Cisco DCNM リリース 11.2(1) から、管理ネットワークの IPv6 アドレスも使用できます。

(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。

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。

**Note** 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。

[クラスタを有効にする (Enable Cluster)] モードを選択した場合、このフィールドは必須です。

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。

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。

**Note** 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。

コンピューティングクラスタが必要な場合は、仮想アプライアンスの設定時に 3NIC があることを確認します。後で NIC をインストールすることはサポートされていません。3 NICs がなく、[クラスタ モードを有効にする (Enable Clustered Mode)] が使用できない場合、eth2 インターフェイスを構成できません。

ただし、`appmgr update network-properties` コマンドを使用して、必要に応じてインストール後にネットワーク プロパティを編集できます。詳細については、「[DCNM インストール後のネットワーク プロパティ, on page 163](#)」を参照してください。

[Next] をクリックします。

- g) [アプリケーション (Applications)] タブで、[デバイス コネクタ] と [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。

**Note** デバイス コネクタは、デフォルトで有効になります。

デバイス コネクタは、クラウドベース管理プラットフォームである Cisco Intersight の機能を実現する組み込み管理コントローラです。

1. [プロキシ サーバー (Proxy Server)] フィールドで、プロキシ サーバーの IP アドレスを入力します。

プロキシ サーバーは RFC1123 準拠名でなければなりません。

**Note** デフォルトで、ポート 80 がプロキシ サーバに使用されます。  
`<proxy-server-ip>:<port>` を使用して、プロキシ サーバに異なるポートを使用します。

プロキシ サーバが認証を必要とする場合、関連するユーザー名とパスワードを [プロキシ サーバー ユーザー名 (Proxy Server Username)] と [プロキシ サーバー パスワード (Proxy Server Password)] フィールドに入力します。

2. [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。

すべてのアプリケーションがこのサブネットからの IP アドレスを使用します。デフォルトで、

手順 2.c, on page 25 で [クラスタ モードを有効にする (Enable Clustered Mode)] チェックボックスをオンにしている場合、[クラスタ モード設定 (Cluster Mode configuration)] 領域が表示されます。

**Note** [クラスタ モード (Clustered mode)] では、Cisco DCNM アプリケーションは別の DCNM コンピューティング ノード実行します。

3. [クラスタ モード設定 (Clustered mode configuration)] 領域で、ネットワーク設定を構成して、クラスタ モードで DCNM インスタンスを展開します。クラスタ モードで、アプリケーションは個別のコンピューティング ノードで実行されます。

- [アウトオブバンド IPv4 ネットワーク アドレス プール (Out-of-Band IPv4 Network Address Pool)] で、クラスタ モードで使用するアウトオブバンド IPv4 ネットワークからアドレス プールを入力します。

オプションで、[アウトオブバンド IPv6 ネットワーク アドレス プール (Out-of-Band IPv6 Network Address Pool)] フィールドに IPv6 アドレス プールを入力することもできます。

- [インバンド IPv4 ネットワーク アドレス プール (In-Band IPv4 Network Address Pool)] で、クラスタ モードで使用するインバンド IPv4 ネットワークからアドレス プールを入力します。

オプションで、[インバンド IPv6 ネットワーク アドレス プール (In-Band IPv6 Network Address Pool)] フィールドに IPv6 アドレス プールを入力することもできます。

アドレスは eth1 サブネットから利用可能で小さい IP アドレスのプレフィックスである必要があります。例: eth1 サブネットがインストール中に 10.1.1.0/24 に設定された場合、10.1.1.240/28 を使用します。このサブネットは、最小で /28 (16 アドレス) および最大で /24 (256 アドレス) である必要があります。また、east-west プール以上にしないでください。このサブネットは、スイッチとの通信のためコンテナに割り当てられます。

- h) [HA 設定 (HA Settings)] タブで、確認メッセージが表示します。

```
You are installing the primary DCNM HA node.  
Please note that HA setup information will need to  
be provided when the secondary DCNM HA node is  
installed.
```

[次へ (Next)] をクリックします。

- i) [概要 (Summary)] タブで、設定の詳細を確認します。

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 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。

セカンダリ ノードをインストールするまで、セットアップが完了していないことを示す警告メッセージが表示されます。

```
WARNING: DCNM HA SETUP IS NOT COMPLETE!  
Your Cisco Data Center Network Manager software has been installed on  
this HA primary node.  
However, the system will be ready to be used only after installation  
of the secondary node has been completed.  
Thank you.
```

**Step 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。

**Caution** 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 **SYSTEMRESOURCEERROR** 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 セカンダリ (Fresh Installation - HA Secondary)] オプション ボタンを選択して、 **dcnm2** をセカンダリ 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。

**Note** 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。

クラスタ モードで Cisco DCNM プライマリを構成している場合は、[クラスタ モードを有効にする (Enable Clustered Mode)] チェックボックスをオンにします。

[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。

**Note** 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。

**Note** Network Insights アプリケーションを使用している場合は、DNS サーバが有効で到達可能であることを確認します。

- [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。

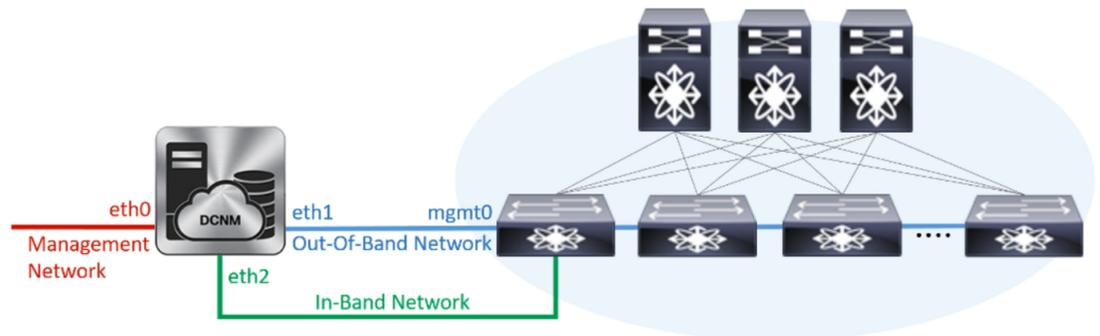
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **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。

Figure 3: 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。

**Note** 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。

**Note** 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。

**Note** 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。

**Note** 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。

**Note** 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]**、および **[クラスタ モード設定]** 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。

2. **[クラスタ モード設定 (Clustered mode configuration)]** 領域で、ネットワーク設定を構成して、クラスタ モードで DCNM インスタンスを展開します。クラスタ モードで、アプリケーションは個別のコンピューティング ノードで実行されます。

- **[アウトオブバンド IPv4 ネットワーク アドレス プール (Out-of-Band IPv4 Network Address Pool)]** で、クラスタ モードで使用するアウトオブバンド IPv4 ネットワークからアドレス プールを入力します。

オプションで、**[アウトオブバンド IPv6 ネットワーク アドレス プール (Out-of-Band IPv6 Network Address Pool)]** フィールドに IPv6 アドレス プールを入力することもできます。

- **[インバンド IPv4 ネットワーク アドレス プール (In-Band IPv4 Network Address Pool)]** で、クラスタ モードで使用するインバンド IPv4 ネットワークからアドレス プールを入力します。

オプションで、**[インバンド IPv6 ネットワーク アドレス プール (In-Band IPv6 Network Address Pool)]** フィールドに IPv6 アドレス プールを入力することもできます。

IP アドレスがプライマリ ノードで構成されたものと同じプールに属していることを確認します。

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VIPv6アドレス (Management Network VIPv6 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。

**Note** 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 VIPv6 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VIPv6アドレス (Out-of-Band Network VIPv6 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VIPv6アドレス (In-Band Network VIPv6 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。

**Note** **[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。

**Note** 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
*****
```

**Note** 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。

### What to do next

適切なクレデンシャルを使用して DCNM Web UI にログオンします。

[設定 (Settings)] アイコンをクリックし、[DCNM の詳細 (About DCNM)] を選択します。展開したインストールタイプを表示して確認できます。

デバイス管理にインバンド管理 (eth2) IP アドレスを設定している場合、スタンドアロンサーバにログインし、次のコマンドを使用して、サーバの eth2 からスイッチにインバンドネットワーク到達可能性を設定します。

```
dcnm# appmgr update network-properties add route ipv4 eth2 <ipv4-network-ip-address/prefix>
```

例: 10.0.0.x/30 サブネットを介して接続しているすべてのファブリック リンクを備えた 4 つのスイッチがある場合、およびサブネット 40.1.1.0/24 のインバンド到達可能性に対してすべてのスイッチがループバック インターフェイスで設定されている場合、次のコマンドを使用します。

```
dcnm# appmgr update network-properties session start
dcnm# appmgr update network-properties add route ipv4 eth2 10.0.0.0/24
dcnm# appmgr update network-properties add route ipv4 eth2 40.1.1.0/24
dcnm# appmgr update network-properties session apply
```

## ISO 仮想アプライアンスで DCNM をインストールする

この章は、次の項で構成されています。



(注) このセクションのスクリーンショットは、ISO の起動方法に基づく設定で異なる可能性があります。青い (BIOS) 画面または黒い (UEFI) 画面が表示されます。

## ISO 仮想アプライアンス ファイルのダウンロード

ISO 仮想アプライアンスをインストールする最初の手順は、dcnm .iso ファイルをダウンロードすることです。DCNM をインストールするためのサーバを準備する際には、コンピュータ上の dcnm.iso ファイルを参照する必要があります。



**Note** HA アプリケーション機能を使用する予定の場合は、dcnm.iso ファイルを 2 回展開する必要があります。

## Procedure

- 
- Step 1** 次のサイトに移動します。 <http://software.cisco.com/download/>。
- Step 2** [製品の選択 (Select a Product)] 検索ボックスに「Cisco Data Center Network Manager」と入力します。  
[検索 (Search)] アイコンをクリックします。
- Step 3** 検索結果から **[Data Center Network Manager]** をクリックします。  
ダウンロード可能な Cisco DCNM の最新リリース ソフトウェアのリストが表示されます。
- Step 4** 最新リリースのリストで、 を選択します。
- Step 5** DCNM ISO 仮想アプライアンス インストーラを検索し、**[ダウンロード (Download)]** アイコンをクリックします。
- Step 6** VMWare (ovf) および KVM (domain Xml) 環境の DCNM 仮想アプライアンスの定義ファイルで DCNM VM テンプレートを検索し、**[ダウンロード (Download)]** をクリックします。
- Step 7** インストール時に簡単に見つけることができるように、`dcnm.iso` ファイルをディレクトリに保存します。
- 

## What to do next

KVM またはベアメタルサーバに DCNM をインストールすることを選択できます。詳細については [KVM 上での DCNM ISO 仮想アプライアンスのインストール, on page 42](#) または [UCS \(ベアブレード\) 上での DCNM ISO 仮想アプライアンスのインストール, on page 35](#) を参照してください。

# UCS(ベアブレード)上でのDCNMISO仮想アプライアンスのインストール

リリース 11.3(1) 以降では、物理インターフェイスが異なる VLAN で分離された管理トラフィック、アウトオブバンドトラフィック、およびインバンドトラフィックを持つトランクとして設定されたポートチャンネルまたはイーサネットチャンネルに対して結合されている追加モードを使用して、Cisco DCNM ISO をインストールできます。

バンドルインターフェイスモードに対してスイッチが正しく設定されていることを確認します。次に、バンドルされたインターフェイス モードのスイッチ設定例を示します。

```
vlan 100
vlan 101
vlan 102
interface port-channel1
  switchport
  switchport mode trunk

interface Ethernet101/1/1
  switchport mode trunk
  channel-group 1
  no shutdown

interface Ethernet101/1/2
```

```

switchport mode trunk
channel-group 1
no shutdown

interface Ethernet101/1/3
switchport mode trunk
channel-group 1
no shutdown

interface Ethernet101/1/4
switchport mode trunk
channel-group 1
no shutdown

```

UCS に DCNM ISO 仮想アプライアンスをインストールするには、次のタスクを実行します。

### Procedure

- 
- Step 1** Cisco Integrated Management Controller (CIMC) を起動します。
- Step 2** **[KVM の起動 (Launch KVM)]** ボタンをクリックします。
- Java ベース KVM または HTML ベース KVM のいずれかを起動できます。
- Step 3** ウィンドウに表示されている URL をクリックして、KVM クライアントアプリケーションのロードを続行します。
- Step 4** メニューバーで **[仮想メディア (Virtual Media)]** > **[仮想デバイスのアクティブ化 (Activate Virtual Devices)]** の順をクリックします。
- Step 5** **[仮想メディア (Virtual Media)]** をクリックし、次のいずれかのメディアを選択し、次から DCNM ISO イメージを参照およびアップロードします。
- CD/DVD のマップ
  - リムーバブルディスクのマップ
  - フロッピーディスクのマップ
- ISO イメージが配置されている場所へ移動し、ISO イメージをロードします。
- Step 6** **[電源 (Power)]** > **[システムのリセット (ウォームブート) (Reset System (warm boot))]** を選択し、**[OK]** を選択して続行して、UCS ボックスを再起動します。
- Step 7** サーバが起動デバイスの選択を開始したら、**F6** を押して再起動プロセスを中断します。ブート選択メニューが表示されます。
- [UCS KVM コンソール (UCS KVM Console)]** ウィンドウの使用方法の詳細については、次の URL にある『リリース 3.1 ユーザーガイド Cisco UCS サーバ設定ユーティリティ』を参照してください。
- [https://www.cisco.com/c/en/us/td/docs/unified\\_computing/ucs/sw/ucsscu/user/guide/31/UCS\\_SCU/booting.html#wp1078073](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/ucsscu/user/guide/31/UCS_SCU/booting.html#wp1078073)
- Step 8** 矢印キーを使用して、Cisco 仮想 CD/DVD を選択し、**[Enter]** を押します。サーバは、マッピングされた場所から DCNM ISO イメージを使用して起動します。

**Note** 次の図は、UEFI のインストールを強調しています。ただし、BIOS インストールに **Cisco vKVM-Mapped vDVD1.22** を選択することもできます。ISO は、両方のモード、BIOS、および UEFI で起動できます。

UEFI は、2 TB 以上のディスクを搭載したシステムでは必須です。

```
Please select boot device:

CentOS
UEFI: Built-in EFI Shell
UEFI: IP4 0100 Intel(R) I350 Gigabit Network Connection
UEFI: IP4 0101 Intel(R) I350 Gigabit Network Connection
UEFI: Cisco vKVM-Mapped vDVD1.22
Cisco vKVM-Mapped vDVD1.22
Cisco vKVM-Mapped vHDD1.22
Cisco vKVM-Mapped vFDD1.22
Cisco CIMC-Mapped vDVD1.22
Cisco CIMC-Mapped vHDD1.22
Enter Setup

↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults
```

ディスク サイズが 2 TB 以上で、4K セクター サイズ ドライバを使用している Cisco UCS の場合は、UEFI 起動オプションが必要です。詳細については、「[UEFI 起動モード](#)」を参照してください。

**Step 9** 上下矢印キーを使用して、**[Cisco Data Center Network Manager のインストール (Install Cisco Data Center Network Manager)]** を選択します。Enter を押します。

次の図に示すオプションは、ISO イメージが UEFI で起動された場合に表示されます。

```
Boot existing Cisco Data Center Network Manager
Install Cisco Data Center Network Manager
Rescue Cisco Data Center Network Manager

Use the ▲ and ▼ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
```

**Step 10** [Cisco 管理ネットワーク管理 (Cisco Management Network Management)] 画面で、ネットワークを設定するモードを選択します。

```
*****
Cisco Data Center Network Management
*****

Please select how networking need to be configured:

1) Un-bundled interface mode.

   Interfaces for DCNM Management Network, Out-Of-Band Network, and
   In-Band Network are chosen from a list of available physical
   interfaces.

2) Bundle interface mode with vlans

   Physical interfaces are bundled together to form a single port-channel,
   configured as a trunk.
   DCNM Management Network, Out-Of-Band Network, and In-Band Network
   traffic is separated in different VLANs.

Networking configuration mode?
```

使用可能な物理インターフェイスから Cisco DCNM ネットワーク インターフェイスを設定するには、1 を入力します。

2 を入力して、バンドルされている使用可能な物理インターフェイスから Cisco DCNM ネットワーク インターフェイスを設定し、トランクとして設定された単一のポートチャネルを形成します。

### Step 11

1 を入力した場合は、バンドルされていないインターフェイス モードで Cisco DCNM ISO をインストールするため、ネットワークのインターフェイスを選択します。利用可能なインターフェイスのリストが画面に表示されます。

[ネットワーク インターフェイス リスト (Network Interface List)] から [管理インターフェイス (eth0) (Management Interface (eth0))] および [アウトオブバンドインターフェイス (eth1) (Out-of-Band interface (eth1))] を選択します。また、必要に応じてインバンドインターフェイス (eth2) を設定することもできます。

```

*****
Cisco Data Center Network Management
*****

Network Interface List
-----
1) 0b:00.0 Cisco Systems Inc VIC Ethernet NIC (rev a2)
   Address: 70:69:5a:f9:5e:19   Link:UP
2) 0c:00.0 Cisco Systems Inc VIC Ethernet NIC (rev a2)
   Address: 70:69:5a:f9:5e:1a   Link:DOWN
3) 01:00.0 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: 00:be:75:49:c2:86   Link:UP
4) 01:00.1 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: 00:be:75:49:c2:87   Link:UP

Please select the interfaces to use from the list above:
Management Interface (eth0) : 3
Out-Of-Band Interface (eth1) : 4

Configure In-Band Interface (eth2)? [y/n]: y
In-Band Interface (eth2) : 1

```

**Note** インバンドインターフェイスを設定しない場合、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。

ただし、**appmgr update network-properties** コマンドを使用して、必要に応じてインストール後にネットワーク プロパティを編集できます。詳細については、「[DCNM インストール後のネットワーク プロパティ, on page 163](#)」を参照してください。

### Step 12

2 を入力した場合は、バンドル インターフェイス モードで Cisco DCNM ISO をインストールするには、次のタスクを実行します。

a) バンドルを形成するには、リストからインターフェイスを選択します。

**Note** 少なくとも 1 個の物理インターフェイスがバンドルの一部である必要があります。

バンドルに追加する必要があるすべてのインターフェイスを入力した後に **q** を入力します。

```

*****
Cisco Data Center Network Management
*****

Network Interface List
-----
1) 01:00:0 Intel Corporation Ethernet Controller 10G X550T (rev 01)
   Address: 78:69:5a:48:1a:e6   Link:UP
2) 01:00:1 Intel Corporation Ethernet Controller 10G X550T (rev 01)
   Address: 78:69:5a:48:1a:e7   Link:UP
3) d8:00:0 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: b4:96:91:27:df:00   Link:UP
4) d8:00:1 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: b4:96:91:27:df:01   Link:UP
5) d8:00:2 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: b4:96:91:27:df:02   Link:UP
6) d8:00:3 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: b4:96:91:27:df:03   Link:UP
7) 19:00:0 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
   Address: 98:e2:ba:fb:c1:54   Link:DOWN
8) 19:00:1 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
   Address: 98:e2:ba:fb:c1:55   Link:DOWN
9) 3b:00:0 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: a8:93:51:09:55:f2   Link:DOWN
10) 3b:00:1 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: a8:93:51:09:55:f3   Link:DOWN
11) 3b:00:2 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: a8:93:51:09:55:f4   Link:DOWN
12) 3b:00:3 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: a8:93:51:09:55:f5   Link:DOWN
13) 5e:00:0 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
   Address: 98:e2:ba:fb:9d:90   Link:DOWN
14) 5e:00:1 Intel Corporation 82599ES 10-Gigabit SFI/SFP+ Network Connection (rev 01)
   Address: 98:e2:ba:fb:9d:91   Link:DOWN

Please select the interfaces to add to the bundle from the list above, type 'q' when done.
Interface to add: 3
Interface to add: 4
Interface to add: 5
Interface to add: 6
Interface to add: q

```

- b) 管理ネットワーク、アウトオブバンドネットワーク、およびインバンドネットワークのインターフェイスをリストから選択するために使用する VLAN ID を入力し、バンドルを形成します。

正しい VLAN ID が割り当てられているかどうかを確認します。

**Note** 管理ネットワークとアウトオブバンドネットワークの VLAN ID は、管理ネットワークとアウトオブバンドネットワークが同じサブネットを使用している場合(つまり、eth0/eth1 が同じサブネットにある場合)、同じにすることができます。

```

*****
Cisco Data Center Network Management
*****
Please enter the VLAN ID for the following networks:
Management Network VLAN ID : 188
Out-Of-Band Network VLAN ID : 181
In-Band Network VLAN ID : 182
Please confirm the following values:
Management Network VLAN ID: 188
Out-Of-Band Network VLAN ID: 181
In-Band Network VLAN ID: 182
Is the VLAN ID assignment correct? (y/n): _

```

- Step 13** 選択したインターフェイスを確認します。[y] を押して、インストールを確認して続行します。
- Step 14** Cisco DCNM の管理ネットワークを設定します。[IP アドレス (IP address)]、[サブネット (Subnet)]、[マスク (Mask)]、[ゲートウェイ (Gateway)] と入力します。[y] を押して、インストールを続行します。

インストールが完了した後、システムが再起動し、DCNM アプライアンスが設定されていることを示すメッセージが画面に表示されます。

```

*****
Please point your web browser to
http://<IP-address>:<port-number>
to complete the application
*****

```

ブラウザに URL をコピーして貼り付け、Web インストーラを使用してインストールを完了します。

**What to do next**

スタンドアロンモードまたはネイティブ HA モードで DCNM をインストールするように選択できます。詳細については、または [ネイティブ HA モードで Cisco DCNM ISO をインストールする](#), [on page 59](#) を参照してください。

**KVM 上での DCNM ISO 仮想アプライアンスのインストール**

次のタスクを実行して、KVM に ISO 仮想アプライアンスをインストールします。

**Procedure**

- 
- Step 1** を解凍し抽出し、**dcnm-kvm-vm.xml** ファイルを検索します。
  - Step 2** KVM を実行している RHEL サーバのこのファイルを ISO として同じ場所にアップロードします。
  - Step 3** SCP ファイル転送端末を経由して、KVM を実行している RHEL サーバに接続します。
  - Step 4** および **dcnm-kvm-vm.xml** RHEL サーバにアップロードします。
  - Step 5** ファイル転送セッションを閉じます。
  - Step 6** SSH 端末を経由して、KVM を実行している RHEL サーバに接続します。
  - Step 7** ISO およびドメイン XML の両方がダウンロードされている場所に移動します。
  - Step 8** **virsh** コマンドを使用して、VM (または KVM 用語とも呼ばれるドメイン) を作成します。

**need info on dcnm-kvm-vm-huge.xml**

```
sudo virsh define [{"dcnm-kvm-vm-huge.xml | dcnm-kvm-vm-compute.xml |
dcnm-kvm-vm-large.xml | dcnm-kvm-vm-small.xml"}]
```

- Step 9** VNC サーバを有効にして、必要なファイアウォールポートを開きます。
- Step 10** SSH セッションを閉じます。
- Step 11** VNC 端末を経由して、KVM を実行している RHEL サーバに接続します。
- Step 12** [アプリケーション (Applications)] > [システム ツール (System Tools)] > [仮想マシン マネージャ (VMM) (Virtual Machine Manager (VMM))] に移動します。  
VM が仮想マシン マネージャで作成されます。
- Step 13** 仮想マシン マネージャから、一覧で VM を選択して VM を編集します。[編集 (Edit)] > [仮想マシンの詳細 (Virtual Machine Details)] > [仮想ハードウェアの詳細を表示する (Show virtual hardware details)] をクリックします。
- Step 14** [仮想ハードウェアの詳細 (Virtual Hardware Details)] で、[ハードウェアの追加 (Add Hardware)] > [ストレージ (Storage)] に移動します。
- Step 15** 次の仕様で、デバイス タイプとともにハードディスクを作成します。
  - デバイス タイプ: IDE ディスク
  - キャッシュ モード: デフォルト
  - ストレージ形式: raw

500GB のストレージサイズを使用することをお勧めします。

**Step 16** 仮想マシンの編集ウィンドウで [IDE CDROM] を選択し、[接続 (Connect)] をクリックします。

**Step 17** dcnm-va.iso に移動し、[OK] をクリックします。

**Step 18** 両方の NIC を選択し、作成されている適切なネットワークを割り当てます。

**Step 19** 仮想マシンの電源をオンにします。

**Note** VM の電源をオンにする前に、選択した展開設定に基づき、CPU やメモリなど VM に予約されている適切なリソースがあることを確認します。

オペレーティング システムがインストールされています。

**Step 20** [Cisco 管理ネットワーク管理 (Cisco Management Network Management)] 画面で、ネットワークのインターフェイスを選択します。利用可能なインターフェイスのリストが画面に表示されます。

[ネットワーク インターフェイス リスト (Network Interface List)] から [管理インターフェイス (eth0) (Management Interface (eth0))] および [アウトオブバンドインターフェイス (eth1) (Out-of-Band interface (eth1))] を選択します。また、必要に応じてインバンドインターフェイス (eth2) を設定することもできます。

**Note** インバンドインターフェイス (eth2) 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。

ただし、`appmgr update network-properties` コマンドを使用して、必要に応じてインストール後にネットワーク プロパティを編集できます。詳細については、「[DCNM インストール後のネットワーク プロパティ, on page 163](#)」を参照してください。

**Step 21** [y] を押して、インストールを確認して続行します。

**Step 22** 管理ネットワークを設定します。[IP アドレス (IP address)]、[サブネット (Subnet)]、[マスク (Mask)]、[ゲートウェイ (Gateway)] と入力します。[y] を押して、インストールを続行します。

インストールが完了した後、システムが再起動し、DCNM アプライアンスが設定されていることを示すメッセージが画面に表示されます。

```
*****
Please point your web browser to
http://<IP-address>:<port-number>
to complete the application
*****
```

ブラウザに URL をコピーして貼り付け、Web インストーラを使用してインストールを完了します。

### What to do next

スタンドアロンモードまたはネイティブ HA モードで DCNM をインストールするように選択できます。詳細については、または [ネイティブ HA モードで Cisco DCNM ISO をインストールする, on page 59](#) を参照してください。

## Windows Hyper-V 上での DCNM ISO 仮想アプライアンスのインストール

Hyper-v Manager は、仮想化プラットフォームに管理アクセスを提供します。DCNM ISO 仮想アプライアンスは、Hyper-v manager を使用してインストールできます。

適切なクレデンシャルを使用して Windows Server Manager を起動します。Hyper-v Manager を起動するには、メニューバーから [ツール (Tools)] > [Hyper-v Manager] を選択します。



(注) Windows Hyper-V 上の DCNM ISO 仮想アプライアンスは、クラスタ化モードをサポートしていません。

Windows Hyper-V 上で Cisco DCNM ISO 仮想アプライアンスをインストールするには、次のタスクを実行します。

### 仮想スイッチの作成

Cisco DCNM では、ネットワーク インターフェイスに 3 つの仮想スイッチが必要です。

- dcnm-mgmt network (eth0) インターフェイス
- enhanced-fabric-mgmt (eth1) インターフェイス
- enhanced-fabric-inband (eth2) インターフェイス

Hyper-V Manager で仮想スイッチを作成するには、次の手順を実行します。

#### Procedure

**Step 1** [アクション (Action)] ペインで、[仮想スイッチ マネージャ (Virtual Switch Manager)] をクリックします。

Windows Hyper-V ウィンドウの仮想スイッチ マネージャが表示されます。

**Step 2** 左側のペインの [仮想スイッチ (Virtual switch)] の下で、[新しい仮想ネットワーク スイッチ (New virtual network switch)] をクリックして仮想スイッチを作成します。

**Step 3** DCNM 管理ネットワーク用の仮想スイッチを作成します。

- a) [外部 (External)] を選択し、[仮想スイッチの作成 (Create Virtual Switch)] をクリックします。
- b) [名前 (Name)] フィールドに、**eth0** インターフェイスの適切な名前を入力します。

**Note** 仮想スイッチ名がインベントリ内で固有であることを確認します。

- c) [外部ネットワーク (External network)] ドロップダウンリストから、サーバで使用可能な適切な物理インターフェイスを選択します。
- d) [Apply] をクリックします。

**Step 4** 拡張ファブリック管理インターフェイスの仮想スイッチを作成します。

- a) [外部 (External)] を選択し、[仮想スイッチの作成 (Create Virtual Switch)] をクリックします。
- b) [名前 (Name)] フィールドに、**eth1** インターフェイスの適切な名前を入力します。

**Note** 仮想スイッチ名がインベントリ内で固有であることを確認します。

- c) [外部ネットワーク (External network)] ドロップダウンリストから、サーバで使用可能な適切な物理インターフェイスを選択します。
- d) [Apply] をクリックします。

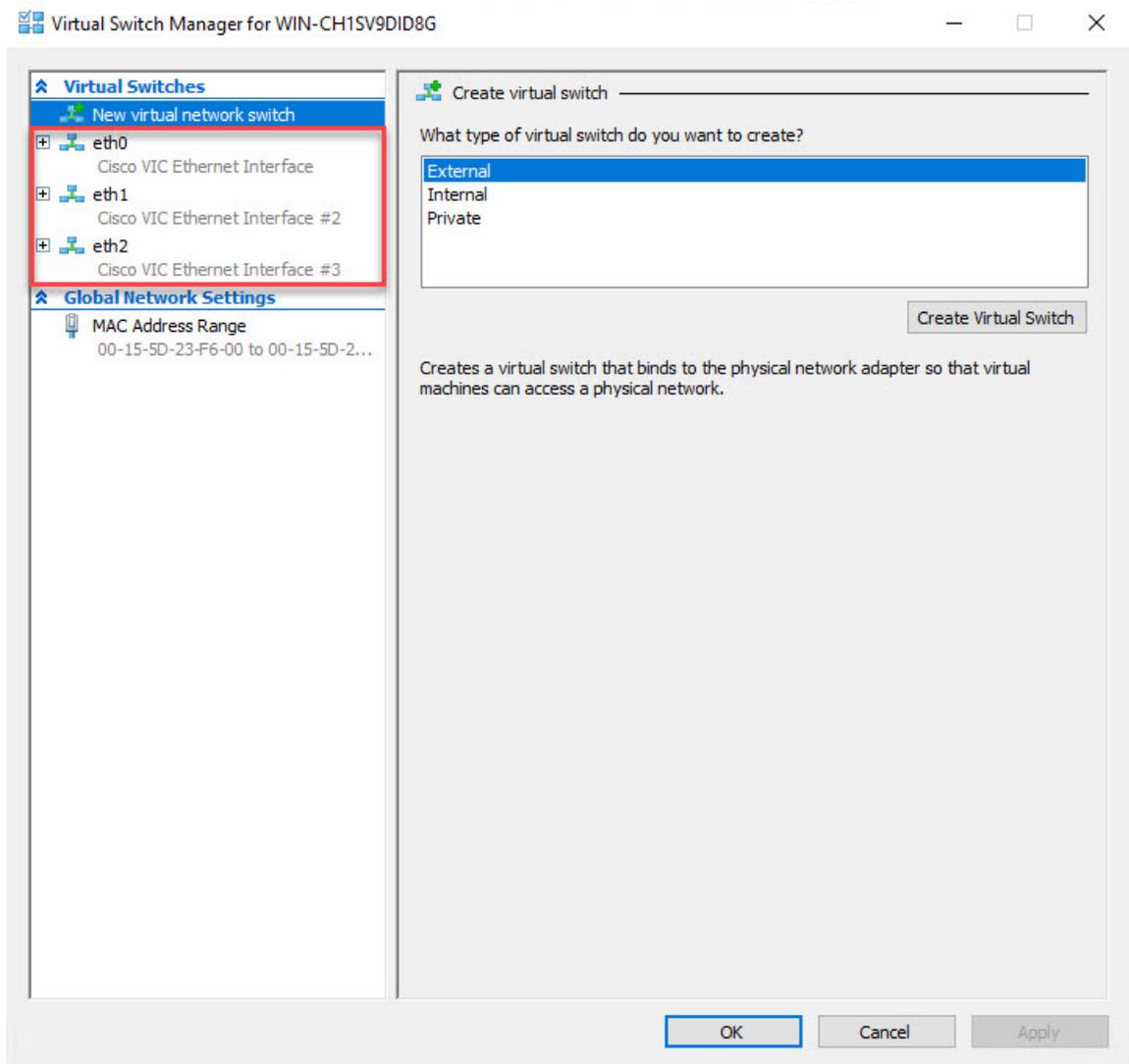
**Step 5** 拡張ファブリック インバンド インターフェイスの仮想スイッチを作成します。

- a) [外部 (External)] を選択し、[仮想スイッチの作成 (Create Virtual Switch)] をクリックします。
- b) [名前 (Name)] フィールドに、**eth2** インターフェイスの適切な名前を入力します。

**Note** 仮想スイッチ名がインベントリ内で固有であることを確認します。

- c) [外部ネットワーク (External network)] ドロップダウンリストから、サーバで使用可能な適切な物理インターフェイスを選択します。
- d) [Apply] をクリックします。

次の図に示すように、すべてのインターフェイスが左側のペインの仮想スイッチの下に表示されます。



### What to do next

ISOをマウントするための仮想マシンを作成します。詳細については、[仮想マシンの作成, on page 46](#)を参照してください。

## 仮想マシンの作成

ネイティブ HA セットアップ用のスタンドアロンまたはプライマリ ノードおよびセカンダリ ノードのいずれかに仮想マシンを作成するには、次の手順を実行します。

## Before you begin

Cisco DCNM をネイティブ HA モードでインストールしている場合は、2 つの仮想マシンを作成する必要があります。1 つはプライマリ ノード用、もう 1 つはセカンダリ ノード用です。

## Procedure

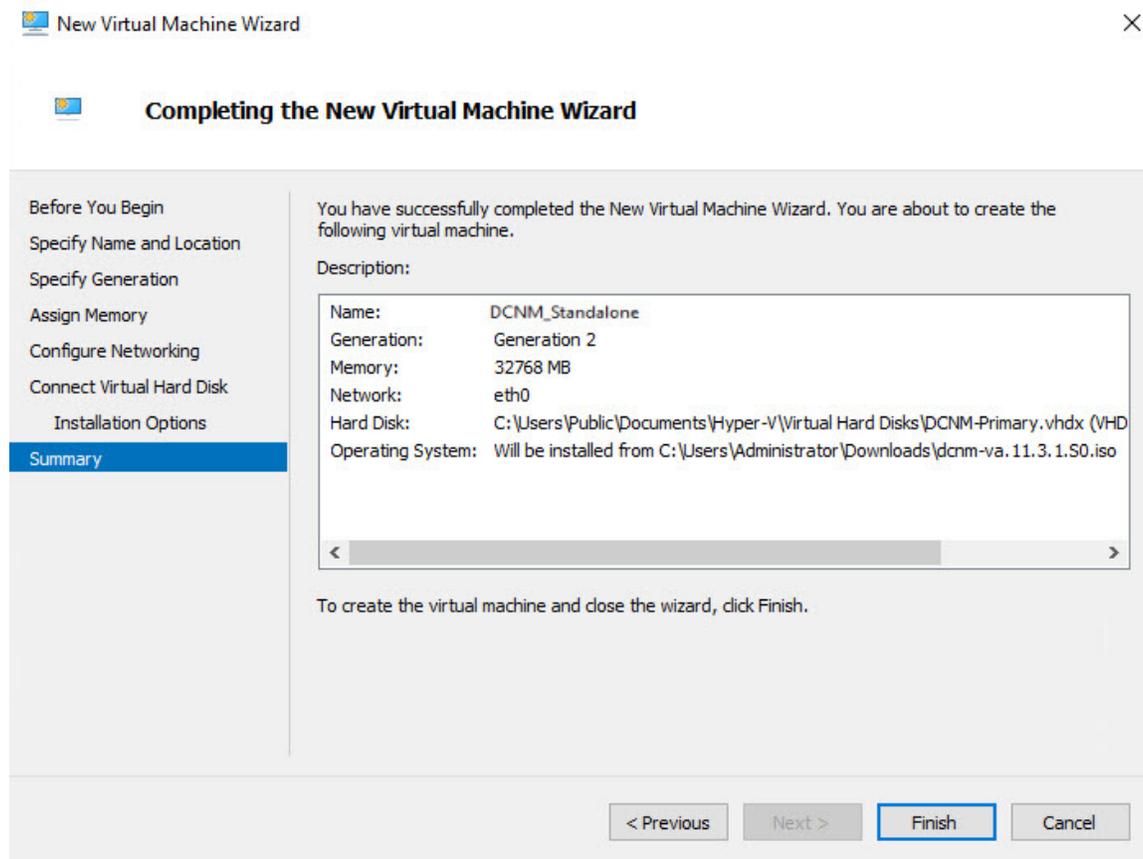
- 
- Step 1** [アクション (Actions)] ペインの [新規 (New)] ドロップダウン リストから、[仮想マシン (Virtual Machine)] を選択します。
- [New Virtual Machine] ウィザードが表示されます。
- Step 2** 開始する前に、[次へ (Next)] をクリックします。
- Step 3** [名前と場所の指定 (Specify Name and Location)] 画面で、アクティブな DCNM ノードの名前を入力します。
- [次へ (Next)] をクリックします。
- Step 4** [世代の指定 (Specify Generation)] 画面で、[第二世代 (Generation 2)] を選択します。
- この仮想マシンは、新しい仮想化機能をサポートし、UEFI ベースのファームウェアを備えており、64 ビットのオペレーティング システムを必要とします。
- [次へ (Next)] をクリックします。
- Step 5** [メモリの割り当て (Assign Memory)] 画面の [起動メモリ (Startup memory)] フィールドに **32768 MB** と入力し、仮想マシンに 32GB メモリを設定します。
- 推奨される設定を確認するには、「システム要件」の [概要, on page 1](#) の章を参照してください。
- [次へ (Next)] をクリックします。
- Step 6** [設定ネットワークング (Configuration Networking)] 画面で、[接続 (Connection)] ドロップダウン リストから、この VM のインターフェイスを選択します。[Eth0](管理ネットワーク インターフェイス) を選択します。
- [次へ (Next)] をクリックします。
- Step 7** [仮想ハード ディスクの接続 (Connect Virtual Hard Disk)] 画面で、仮想ハード ディスクを作成します。
- [仮想ハード ディスクの作成 (Create a virtual hard disk)] を選択します。
  - ハード ディスクの適切な名前、場所、およびサイズを入力します。
- Note** 仮想ハード ディスクのデフォルト名は、[名前と場所の指定 (Specify Name and Location)] 画面で指定した仮想マシン名から取得されます。
- ハード ディスクのサイズは 500 GB 以上にする必要があります。
- [次へ (Next)] をクリックします。

**Step 8** [インストール オプション (Installation Options)] 画面で、[ブート可能なイメージファイルからオペレーティング システムとしてインストールする (Install as operating system from a bootable image file)] を選択します。

[イメージファイル (.iso) (Image file (.iso))] フィールドで、[参照 (Browse)] をクリックします。ディレクトリに移動し、DCNM ISO イメージを選択します。

[次へ (Next)] をクリックします。

**Step 9** [概要 (Summary)] 画面で、設定の詳細を確認します。



[終了 (Finish)] をクリックして、DCNM アクティブノードを作成します。

新しく作成された仮想マシンは、Hyper-V Manager の仮想マシンブロックに表示されます。

**Step 10** 仮想マシンを右クリックし、[設定 (Settings)] を選択します。

DCNM ノードに [設定 (Settings)] 画面が表示されます。

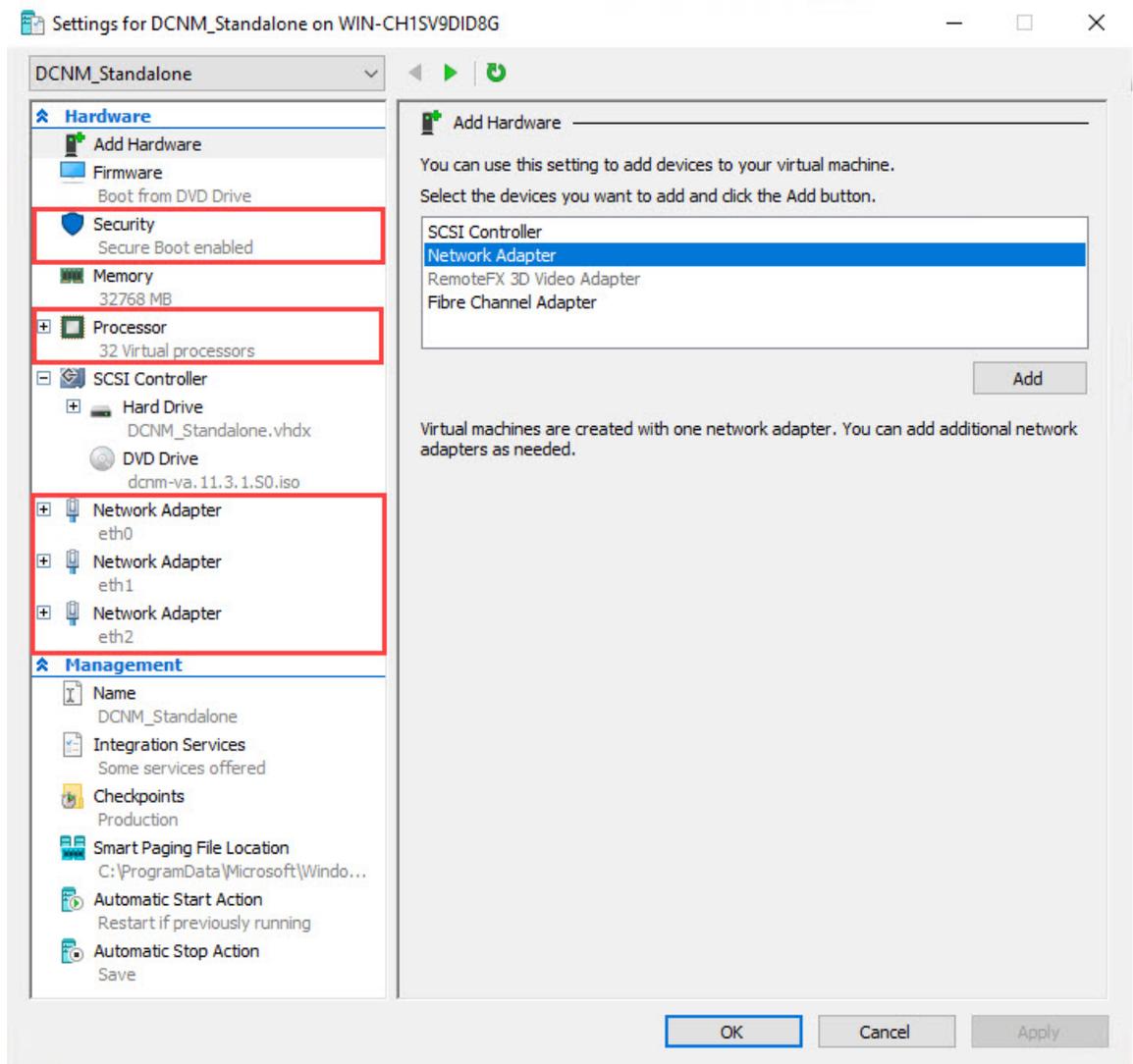
**Step 11** 左側のペインのハードウェアブロックで、[ハードウェアの追加 (Add Hardware)] をクリックします。

**Step 12** メインペインで、[ネットワーク アダプタ (Network Adapter)] を選択し、[追加 (Add)] をクリックします。

**Step 13** [ネットワーク アダプタ (Network Adapter)] 画面で、仮想スイッチのネットワーク アダプタを作成します。

- [仮想スイッチ (Virtual Switch)] ドロップダウン リストから、[eth1] 仮想スイッチを選択します。[適用 (Apply)] をクリックします。
- [仮想スイッチ (Virtual Switch)] ドロップダウン リストから、[eth2] 仮想スイッチを選択します。[適用 (Apply)] をクリックします。

3つのネットワーク アダプタは、すべて [ハードウェア (Hardware)] セクションの下の左側のペインに表示されます。



**Step 14** 左側のペインで、[セキュリティ (Security)] を選択します。

メイン ペインの [テンプレート (template)] ドロップダウン リストから、[MICROSOFT UEFI 証明機関 (MICROSOFT UEFI Certificate Authority)] を選択します。

**Note** 第2世代 Hyper-V 仮想マシンを選択した場合、このテンプレートは必須です。

[Apply] をクリックします。

### Step 15

[設定 (Settings)] 画面で、[プロセッサ (Processor)] をクリックします。

メインペインの [仮想プロセッサの数 (Number of virtual processors)] フィールドで、**32** と入力し、[32vCPUs] を選択します。[適用 (Apply)] をクリックします。

[OK] をクリックして、DCNM ノードの設定を確定します。

### What to do next

Windows Hyper-V に Cisco DCNM ISO をインストールします。詳細については、[DCNM ISO 仮想アプライアンスのインストール](#), on page 50 を参照してください。

## DCNM ISO 仮想アプライアンスのインストール

ネイティブ HA セットアップのためスタンドアロンまたはプライマリ ノードとセカンダリ ノードのいずれかに DCNM ISO 仮想アプライアンスを設定するには、次の手順を実行します。

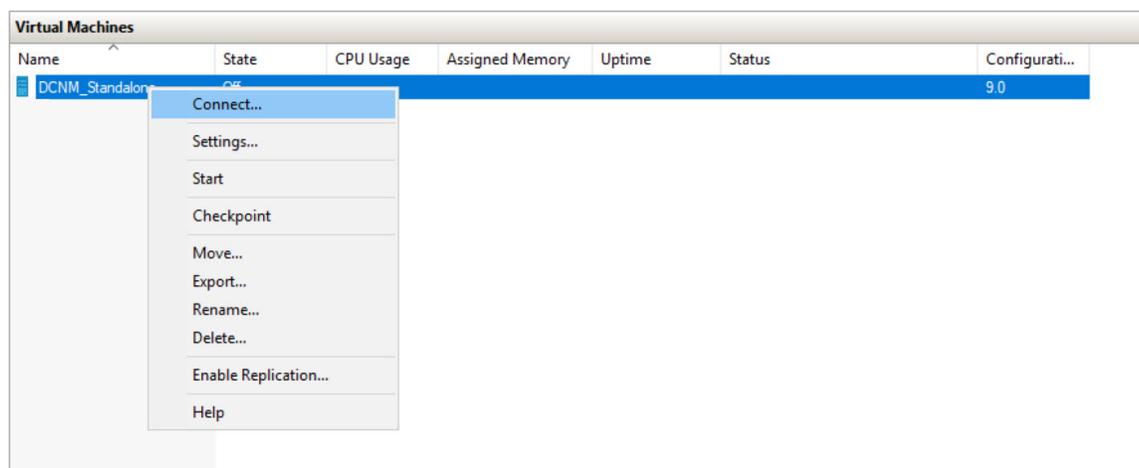
### Before you begin

適切なセキュリティ設定を使用して、仮想マシンが正しく設定されていることを確認します。

### Procedure

#### Step 1

[仮想マシン (Virtual Machines)] ブロックから、[アクティブ ノード (Active node)] を右クリックして [接続 (Connect)] を選択します。

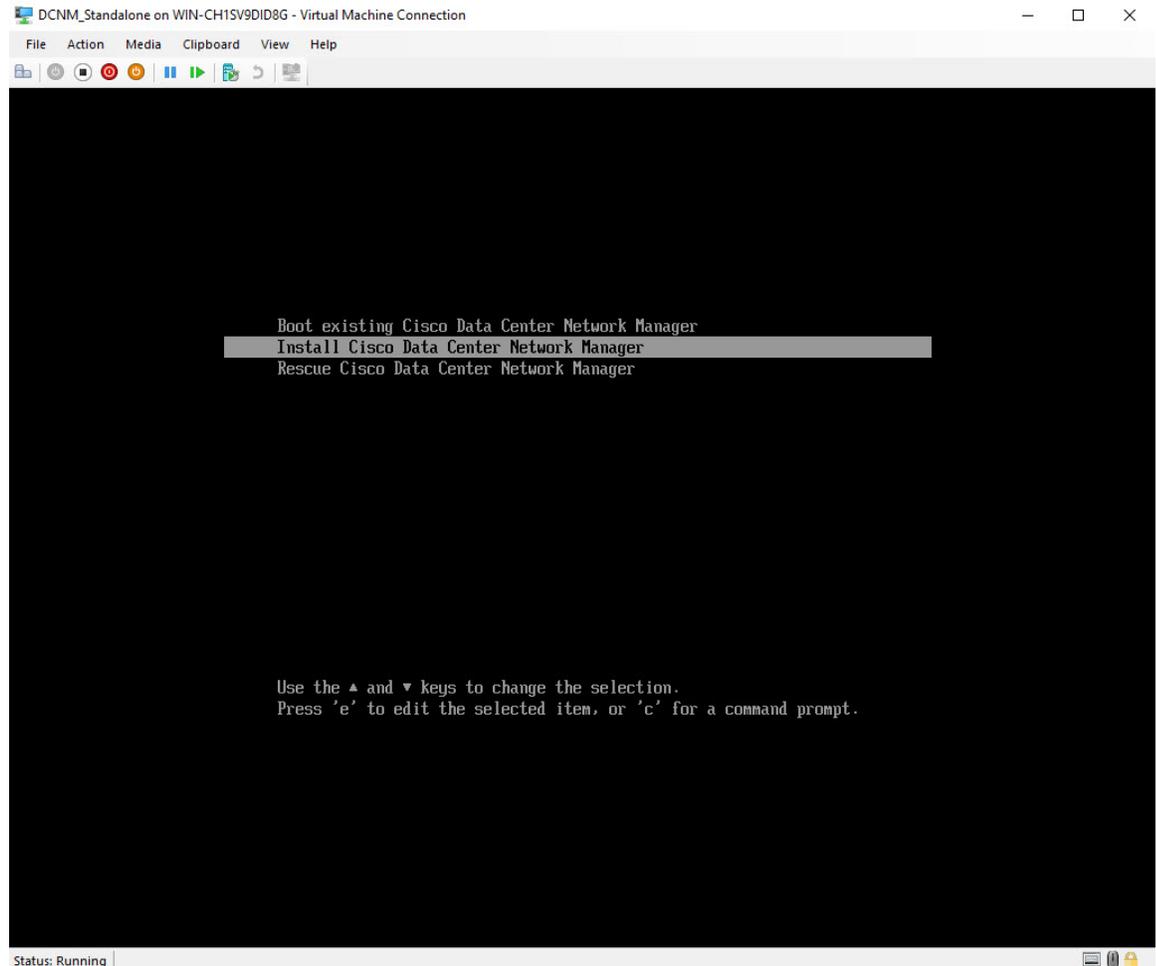


#### Step 2

[仮想マシン接続 (Virtual Machine Connection)] 画面のメニューバーから、[メディア (Media)] > [DVD ドライブ (DVD Drive)] を選択して、選択したイメージを確認します。

[Start] をクリックします。DCNM サーバが起動します。

- Step 3** 上下矢印キーを使用して、**[Cisco Data Center Network Manager のインストール (Install Cisco Data Center Network Manager)]** を選択します。[Enter]キーを押して、CISCO DCNM アクティブノードをインストールします。



- Step 4** [Cisco 管理ネットワーク管理 (Cisco Management Network Management)] 画面で、ネットワークのインターフェイスを選択します。利用可能なインターフェイスのリストが画面に表示されます。
- [ネットワーク インターフェイス リスト (Network Interface List)] から[管理インターフェイス (eth0) (Management Interface (eth0))] および [アウトオブバンド インターフェイス (eth1) (Out-of-Band interface (eth1))] を選択します。また、必要に応じて [In-band interface (eth2) (インバンド インターフェイス (eth2))] を設定することもできます。

```

DCNM_Standalone on WIN-CH1S1V9DID8G - Virtual Machine Connection
File Action Media Clipboard View Help
Cisco Data Center Network Management
Network Interface List
-----
1)
Address: 15.54.23.24 Link:UP
2)
Address: 15.54.23.25 Link:UP
3)
Address: 15.54.23.26 Link:UP

Please select the interfaces to use from the list above:
Management Interface (eth0) [ ] : 1
Out-Of-Band Interface (eth1) : 2

Configure In-Band Interface (eth2)? [y/n]: y
In-Band Interface (eth2) : 3

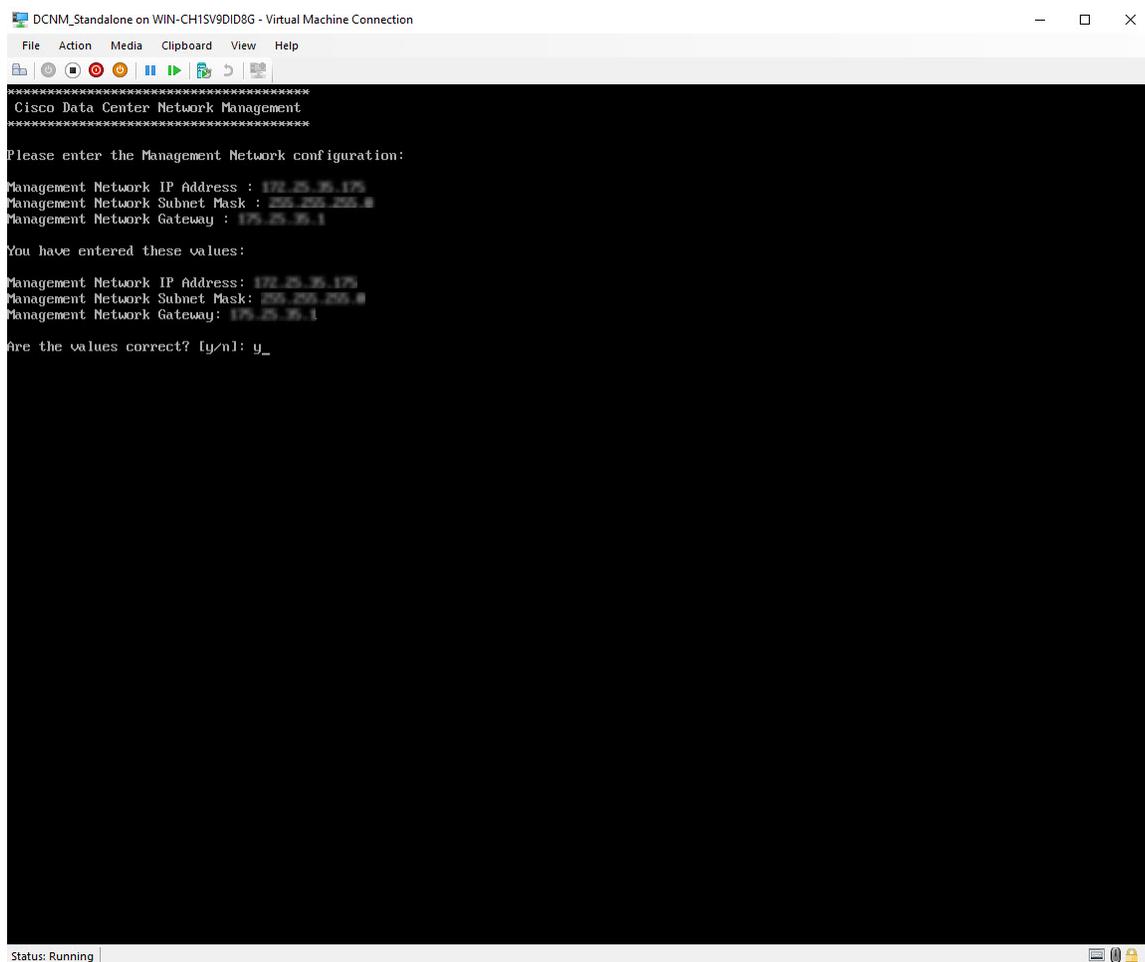
Please confirm the following selection:
Management Interface (eth0):
1)
Address: 15.54.23.24 Link:UP
Out-Of-Band Interface (eth1):
2)
Address: 15.54.23.25 Link:UP
In-Band Interface (eth2):
3)
Address: 15.54.23.26 Link:UP

Is the interface assignment correct? [y/n]: y_

```

選択したインターフェイスを確認します。[y] を押して、インストールを確認して続行します。

- Step 5** Cisco DCNM の管理ネットワークを設定します。[IP アドレス (IP address)]、[サブネット (Subnet)]、[マスク (Mask)]、[ゲートウェイ (Gateway)] と入力します。
- 値を確認し、[y] を押してインストールを続行します。



```
DCNM_Standalone on WIN-CH15V9DID8G - Virtual Machine Connection
File Action Media Clipboard View Help
Cisco Data Center Network Management
Please enter the Management Network configuration:
Management Network IP Address : 172.25.35.175
Management Network Subnet Mask : 255.255.255.0
Management Network Gateway : 172.25.35.1
You have entered these values:
Management Network IP Address: 172.25.35.175
Management Network Subnet Mask: 255.255.255.0
Management Network Gateway: 172.25.35.1
Are the values correct? [y/n]: y_
Status: Running
```

インストールが完了した後、システムが再起動し、DCNM アプライアンスが設定されていることを示すメッセージが画面に表示されます。

```
*****
Please point your web browser to
http://<IP-address>:<port-number>
to complete the application
*****
```

ブラウザに URL をコピーして貼り付け、Web インストーラを使用してインストールを完了します。

### What to do next

スタンドアロンモードまたはネイティブ HA モードで DCNM をインストールするように選択できます。詳細については、[スタンドアロンモードでの Cisco DCNM ISO のインストール, on page 54](#) または [ネイティブ HA モードで Cisco DCNM ISO をインストールする, on page 59](#) を参照してください。

## スタンドアロン モードでの Cisco DCNM ISO のインストール

[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。

Web インストーラから Cisco DCNM のインストールを完了するには、次の手順を実行します。

### Procedure

**Step 1** [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。

**Caution** 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。

**Step 2** [Cisco DCNM インストーラ (Cisco DCNM Installer)] 画面で、[新規インストール - スタンドアロン (Fresh Installation - Standalone)] オプション ボタンを選択します。

[Next] をクリックします。

**Step 3** [インストール モード (Install Mode)] タブで、DCNM 導入タイプを選択します。

[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 OVA DCNM アプライアンスの [LAN ファブリック (LAN Fabric)] インストール モードを選択します。

クラスタモードで Cisco DCNM を展開する場合は、[クラスタ モードを有効にする (Enable Clustered Mode)] チェックボックスをオンにします。コンピューティング ノードが Cisco DCNM [Web UI] > [アプリケーション (Applications)] > [コンピューティング (Compute)] に表示されます。アプリケーションはコンピューティング ノードで実行されます。後でコンピューティング ノードをクラスタに追加できます。You can add the compute nodes to a Cluster, later.

コンピューティング クラスタが必要な場合は、仮想アプライアンスの設定時に 3NIC があることを確認します。後で NIC をインストールすることはサポートされていません。3つのNICがない場合は、[クラスタモードの有効化 (Enable Clustered Mode)] は使用できません。

**Note** [クラスタ モードを有効にする (Enable Clustered Mode)] がオンになっている場合、設定、コンプライアンス、EPL、NIA などのアプリケーションはコンピューティング ノードがインストールされるまで動作しません。

[Next] をクリックします。

**Step 4** [管理 (Administration)] タブで、パスワードに関する情報を入力します。

- [管理者のパスワード] フィールドで、Cisco DCNM のアプリケーションに接続するために使用されるパスワードを入力してください。

パスワードは、`%^=&:.*\'' <SPACE>` を除くすべての特殊文字を使用できます。

[管理者パスワードの確認] フィールドにパスワードをもう一度入力します。

- **[データベースパスワード (Database Password)]** フィールドに、PostgreSQL データベースのパスワードを入力します。

すべての特殊文字は `%"$^=;.*\'' <SPACE>` を除き、パスワードに使用できます。

**[管理者パスワードの確認]** フィールドにパスワードをもう一度入力します。

**Note** **[データベースパスワード (Database Password)]** フィールドを空白のままにすると、管理者パスワードが PostgreSQL のパスワードと見なされます。

- **[Superuser Password (root)]** フィールドに、スーパーユーザーが root 権限にアクセスするためのパスワードを入力します。

**[スーパーユーザーパスワード (Superuser Password)]** フィールドにもう一度パスワードを入力します。

**Note** スーパーユーザーパスワードが空白のままの場合は、管理者パスワードをスーパーユーザーパスワードと見なします。ただし、セキュリティ上の理由から、強力なパスワードを設定することを推奨します。

入力したパスワードを表示するには、**[入力したパスワードを表示する (Show passwords in clear text)]** チェックボックスをオンにします。

**[次へ (Next)]** をクリックします。

**Step 5** **[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。

IPv6 アドレスを使用して DNS サーバを設定することもできます。

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。

**Note** Network Insights アプリケーションを使用している場合は、DNS サーバが有効で到達可能であることを確認します。

- **[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。

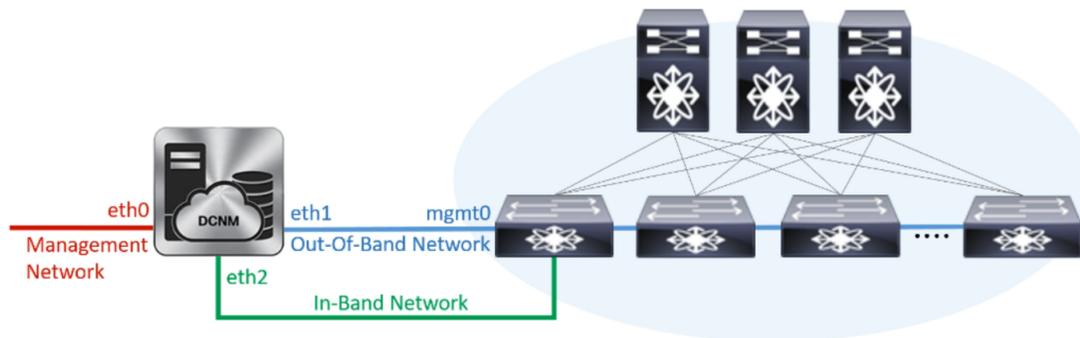
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **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。

**Step 6** **[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。

Figure 4: Cisco DCNM 管理ネットワーク インターフェイス



- a) [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。

**Note** Cisco DCNM リリース 11.2(1) から、管理ネットワークの IPv6 アドレスも使用できません。

(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。

- b) [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。

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。

**Note** 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。

- c) (Optional) [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。

ステップ [Step 3, on page 54](#) でクラスタの有効化モードを選択した場合、このフィールドは必須です。

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。

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。

**Note** 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。

コンピューティングクラスタが必要な場合は、仮想アプライアンスの設定時に3NICがあることを確認します。後でNICをインストールすることはサポートされていません。3NICがなく、[クラスタモードを有効にする (Enable Clustered Mode)] が使用できない場合、eth2 インターフェイスを構成できません。

ただし、`appmgr update network-properties` コマンドを使用して、必要に応じてインストール後にネットワークプロパティを編集できます。詳細については、「[DCNM インストール後のネットワークプロパティ, on page 163](#)」を参照してください。

[Next] をクリックします。

**Step 7** [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]、および [クラスタモード設定] を構成します。

**Note** デバイスコネクタは、デフォルトで有効になります。

デバイスコネクタは、クラウドベース管理プラットフォームであるCisco Intersightの機能を実現する組み込み管理コントローラです。

a) (Optional) [プロキシサーバー (Proxy Server)] フィールドで、プロキシサーバーのIPアドレスを入力します。

プロキシサーバーはRFC1123 準拠名でなければなりません。

**Note** デフォルトで、ポート80がプロキシサーバに使用されます。<proxy-server-ip>:<port>を使用して、プロキシサーバに異なるポートを使用します。

プロキシサーバが認証を必要とする場合、関連するユーザー名とパスワードを [プロキシサーバーユーザー名 (Proxy Server Username)] と [プロキシサーバーパスワード (Proxy Server Password)] フィールドに入力します。

b) [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。

すべてのアプリケーションがこのサブネットからのIPアドレスを使用します。

c) [クラスタモード設定 (Clustered mode configuration)] 領域で、ネットワーク設定を構成して、クラスタモードでDCNMインスタンスを展開します。クラスタモードで、アプリケーションは個別のコンピューティングノードで実行されます。

手順 [Step 3, on page 54](#) で [クラスタモードを有効にする (Enable Clustered Mode)] チェックボックスをオンにしている場合、[クラスタモード設定 (Cluster Mode configuration)] 領域が表示されます。

**Note** [クラスタモード (Clustered mode)] では、Cisco DCNM アプリケーションは別のDCNMコンピューティングノード実行します。

• [アウトオブバンドIPv4ネットワークアドレスプール (Out-of-Band IPv4 Network Address Pool)] で、クラスタモードで使用するアウトオブバンドIPv4ネットワークからアドレスプールを入力します。

オプションで、[アウトオブバンド IPv6 ネットワーク アドレス プール (Out-of-Band IPv6 Network Address Pool)] フィールドに IPv6 アドレス プールを入力することもできます。

- [インバンド IPv4 ネットワーク アドレス プール (In-Band IPv4 Network Address Pool)] で、クラスタ モードで使用するインバンド IPv4 ネットワークからアドレス プールを入力します。

オプションで、[インバンド IPv6 ネットワーク アドレス プール (In-Band IPv6 Network Address Pool)] フィールドに IPv6 アドレス プールを入力することもできます。

アドレスは eth1 サブネットから利用可能で小さい IP アドレスのプレフィックスである必要があります。例: eth1 サブネットがインストール中に 10.1.1.0/24 に設定された場合、10.1.1.240/28 を使用します。このサブネットは、最小で /28 (16 アドレス) および最大で /24 (256 アドレス) である必要があります。また、east-west プール以上にししないでください。このサブネットは、スイッチとの通信のためコンテナに割り当てられます。

[次へ (Next)] をクリックします。

**Step 8** [概要 (Summary)] タブで、設定の詳細を確認します。

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 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
*****
```

**Note** 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。

**Note** インストールが進行中に管理 IP アドレスを使用して DCNM Web UI にアクセスする場合、エラー メッセージがコンソールに表示されます。

```
*****
*Preparing Appliance*
*****
```

## What to do next

適切なクレデンシヤルを使用して DCNM Web UI にログオンします。

[設定 (Settings)] アイコンをクリックし、[DCNM の詳細 (About DCNM)] を選択します。展開したインストールタイプを表示して確認できます。

デバイス管理にインバンド管理 (eth2) IP アドレスを設定している場合、スタンドアロン サーバにログインし、次のコマンドを使用して、サーバの eth2 からスイッチにインバンドネットワーク到達可能性を設定します。

```
dcnm# appmgr update network-properties add route ipv4 eth2 <ipv4-network-ip-address/prefix>
```

例: 10.0.0.x/30 サブネットを介して接続しているすべてのファブリック リンクを備えた 4 つのスイッチがある場合、およびサブネット 40.1.1.0/24 のインバンド到達可能性に対してすべてのスイッチがループバック インターフェイスで設定されている場合、次のコマンドを使用します。

```
dcnm# appmgr update network-properties session start
dcnm# appmgr update network-properties add route ipv4 eth2 10.0.0.0/24
dcnm# appmgr update network-properties add route ipv4 eth2 40.1.1.0/24
dcnm# appmgr update network-properties session apply
```

## ネイティブ HA モードで Cisco DCNM ISO をインストールする

ネイティブ HA は ISO または OVA インストールのみを使用した DCNM アプライアンスでサポートされています。

デフォルトでは、Cisco DCNM を使用した組み込み型 PostgreSQL データベース エンジンです。ネイティブ HA 機能は、Cisco DCNM アプライアンスによって、リアルタイムで同期されている組み込みデータベースを使用したアクティブおよびスタンバイ アプリケーションとして実行可能です。したがって、アクティブ DCNM が機能していない場合、スタンバイ DCNM は同じデータベースデータを引き継ぎ、操作を再開します。

DCNM のネイティブ HA をセットアップするには、次の作業を実行します。

### Procedure

- Step 1** 2 つの DCNM 仮想アプライアンス (OVA または ISO のいずれか) を展開します。  
例えば、**dcnm1** および **dcnm2** として示します。
- Step 2** **dcnm1** をプライマリ ノードとして設定します。 **dcnm1** 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。

**Caution** 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 **SYSTEMRESOURCEERROR** 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)] タブで、[新規インストール - HA プライマリ (Fresh Installation - HA Primary)] オプション ボタンを選択して、**dcnm1** をプライマリ ノードとしてインストールします。

[Next] をクリックします。

- c) [インストール モード (Install Mode)] タブで、DCNM 導入タイプを選択します。

[インストール モード (Installation mode)] ドロップダウン リストから DCNM アプライアンスの[LAN ファブリック (LAN Fabric)] インストール モードを選択します。

クラスタ モードで Cisco DCNM を展開する場合は、[クラスタ モードを有効にする (Enable Clustered Mode)] チェックボックスをオンにします。コンピューティング ノードが Cisco DCNM [Web UI] > [アプリケーション (Applications)] > [コンピューティング (Compute)] に表示されます。アプリケーションはコンピューティング ノードで実行されます。後でコンピューティング ノードをクラスタに追加できます。You can add the compute nodes to a Cluster, later.

コンピューティング クラスタが必要な場合は、仮想アプライアンスの設定時に 3NIC あることを確認します。後で NIC をインストールすることはサポートされていません。3つのNICがない場合は、[クラスタモードの有効化 (Enable Clustered Mode)] は使用できません。

**Note** [クラスタ モードを有効にする (Enable Clustered Mode)] がオンになっている場合、設定、コンプライアンス、EPL、NIA などのアプリケーションはコンピューティング ノードがインストールされるまで動作しません。

[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。

- [管理者のパスワード] フィールドで、Cisco DCNM のアプリケーションに接続するために使用されるパスワードを入力してください。

パスワードは、`%^=;*\' <SPACE>` を除くすべての特殊文字を使用できます。

[管理者パスワードの確認] フィールドにパスワードをもう一度入力します。

- [データベース パスワード (Database Password)] フィールドに、PostgreSQL データベースのパスワードを入力します。

すべての特殊文字は `%^=;*\' <SPACE>` を除き、パスワードに使用できます。

[管理者パスワードの確認] フィールドにパスワードをもう一度入力します。

**Note** [データベース パスワード (Database Password)] フィールドを空白のままにすると、管理者パスワードが PostgreSQL のパスワードと見なされます。

- [Superuser Password (root)] フィールドに、スーパーユーザーが root 権限にアクセスするためのパスワードを入力します。

[スーパーユーザー パスワード (Superuser Password)] フィールドにもう一度パスワードを入力します。

**Note** スーパーユーザー パスワードが空白のままの場合は、管理者パスワードをスーパーユーザーパスワードと見なします。ただし、セキュリティ上の理由から、強力なパスワードを設定することを推奨します。

入力したパスワードを表示するには、[入力したパスワードを表示する (Show passwords in clear text)] チェックボックスをオンにします。

[次へ (Next)] をクリックします。

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。

**Note** Network Insights アプリケーションを使用している場合は、DNS サーバが有効で到達可能であることを確認します。

- [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。

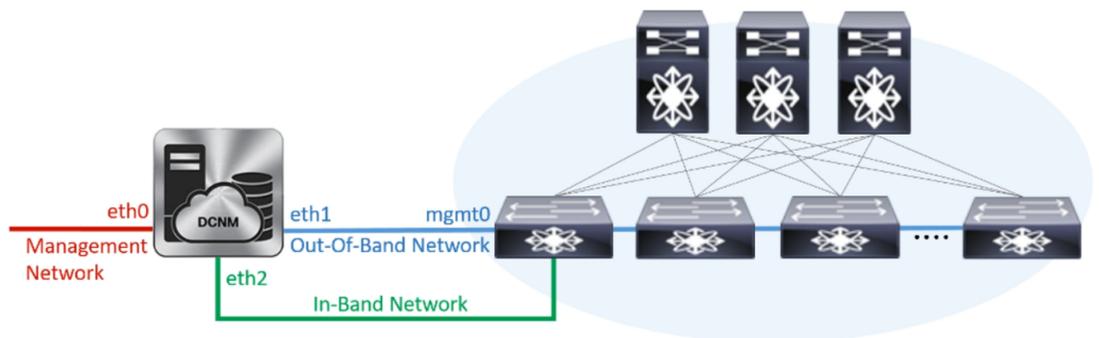
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **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。

Figure 5: 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。

**Note** Cisco DCNM リリース 11.2(1) から、管理ネットワークの IPv6 アドレスも使用できます。

(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。

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。

**Note** 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。

[クラスタを有効にする (Enable Cluster)] モードを選択した場合、このフィールドは必須です。

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。

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。

**Note** 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。

コンピューティングクラスタが必要な場合は、仮想アプライアンスの設定時に 3NIC があることを確認します。後で NIC をインストールすることはサポートされていません。3 NICs がなく、[クラスタ モードを有効にする (Enable Clustered Mode)] が使用できない場合、eth2 インターフェイスを構成できません。

ただし、`appmgr update network-properties` コマンドを使用して、必要に応じてインストール後にネットワーク プロパティを編集できます。詳細については、「[DCNM インストール後のネットワーク プロパティ, on page 163](#)」を参照してください。

[Next] をクリックします。

- g) [アプリケーション (Applications)] タブで、[デバイス コネクタ] と [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。

**Note** デバイス コネクタは、デフォルトで有効になります。

デバイス コネクタは、クラウドベース管理プラットフォームである Cisco Intersight の機能を実現する組み込み管理コントローラです。

1. **[プロキシ サーバー (Proxy Server)]** フィールドで、プロキシサーバーの IP アドレスを入力します。

プロキシサーバーは RFC1123 準拠名でなければなりません。

**Note** デフォルトで、ポート 80 がプロキシサーバーに使用されます。  
<proxy-server-ip>:<port> を使用して、プロキシサーバーに異なるポートを使用します。

プロキシサーバーが認証を必要とする場合、関連するユーザー名とパスワードを **[プロキシサーバー ユーザー名 (Proxy Server Username)]** と **[プロキシサーバーパスワード (Proxy Server Password)]** フィールドに入力します。

2. **[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。

すべてのアプリケーションがこのサブネットからの IP アドレスを使用します。デフォルトで、

手順 2.c, on page 60 で **[クラスタ モードを有効にする (Enable Clustered Mode)]** チェックボックスをオンにしている場合、**[クラスタ モード設定 (Cluster Mode configuration)]** 領域が表示されます。

**Note** **[クラスタ モード (Clustered mode)]** では、Cisco DCNM アプリケーションは別の DCNM コンピューティング ノード実行します。

3. **[クラスタ モード設定 (Clustered mode configuration)]** 領域で、ネットワーク設定を構成して、クラスタモードで DCNM インスタンスを展開します。クラスタモードで、アプリケーションは個別のコンピューティング ノードで実行されます。

- **[アウトオブバンド IPv4 ネットワーク アドレス プール (Out-of-Band IPv4 Network Address Pool)]** で、クラスタモードで使用するアウトオブバンド IPv4 ネットワークからアドレスプールを入力します。

オプションで、**[アウトオブバンド IPv6 ネットワーク アドレス プール (Out-of-Band IPv6 Network Address Pool)]** フィールドに IPv6 アドレスプールを入力することもできます。

- **[インバンド IPv4 ネットワーク アドレス プール (In-Band IPv4 Network Address Pool)]** で、クラスタモードで使用するインバンド IPv4 ネットワークからアドレスプールを入力します。

オプションで、**[インバンド IPv6 ネットワーク アドレス プール (In-Band IPv6 Network Address Pool)]** フィールドに IPv6 アドレスプールを入力することもできます。

アドレスは eth1 サブネットから利用可能で小さい IP アドレスのプレフィックスである必要があります。例: eth1 サブネットがインストール中に 10.1.1.0/24 に設定された場合、

10.1.1.240/28 を使用します。このサブネットは、最小で /28 (16 アドレス) および最大で /24 (256 アドレス) である必要があります。また、east-west プール以上にしないでください。このサブネットは、スイッチとの通信のためコンテナに割り当てられます。

- h) **[HA 設定 (HA Settings)]** タブで、確認メッセージが表示します。

```
You are installing the primary DCNM HA node.
Please note that HA setup information will need to
be provided when the secondary DCNM HA node is
installed.
```

**[次へ (Next)]** をクリックします。

- i) **[概要 (Summary)]** タブで、設定の詳細を確認します。

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 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。

セカンダリ ノードをインストールするまで、セットアップが完了していないことを示す警告メッセージが表示されます。

```
WARNING: DCNM HA SETUP IS NOT COMPLETE!
Your Cisco Data Center Network Manager software has been installed on
this HA primary node.
However, the system will be ready to be used only after installation
of the secondary node has been completed.
Thank you.
```

- Step 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。

**Caution** 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 **SYSTEMRESOURCEERROR** 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 セカンダリ (Fresh Installation - HA Secondary)]** オプション ボタンを選択して、**dcnm2** をセカンダリ 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 ノードに選択したのと同じインストールモードを選択します。

**Note** 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。

クラスタ モードで Cisco DCNM プライマリを構成している場合は、**[クラスタ モードを有効にする (Enable Clustered Mode)]** チェックボックスをオンにします。

[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。

**Note** 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。

**Note** Network Insights アプリケーションを使用している場合は、DNS サーバが有効で到達可能であることを確認します。

- **[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。

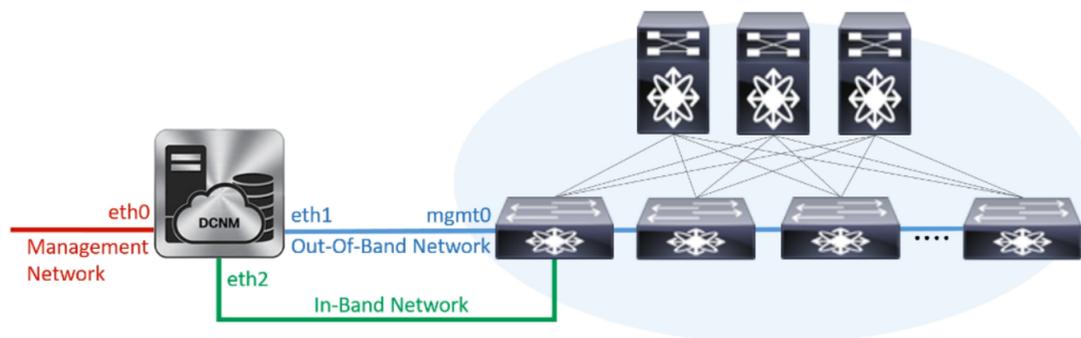
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **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。

Figure 6: 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。

**Note** 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。

**Note** 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。

**Note** 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。

**Note** 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。

**Note** 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]、および [クラスタ モード設定] 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。
  2. [クラスタ モード設定 (Clustered mode configuration)] 領域で、ネットワーク設定を構成して、クラスタ モードで DCNM インスタンスを展開します。クラスタ モードで、アプリケーションは個別のコンピューティング ノードで実行されます。
    - [アウトオブバンド IPv4 ネットワーク アドレス プール (Out-of-Band IPv4 Network Address Pool)] で、クラスタ モードで使用するアウトオブバンド IPv4 ネットワークからアドレス プールを入力します。

オプションで、[アウトオブバンド IPv6 ネットワーク アドレス プール (Out-of-Band IPv6 Network Address Pool)] フィールドに IPv6 アドレス プールを入力することもできます。
    - [インバンド IPv4 ネットワーク アドレス プール (In-Band IPv4 Network Address Pool)] で、クラスタ モードで使用するインバンド IPv4 ネットワークからアドレス プールを入力します。

オプションで、[インバンド IPv6 ネットワーク アドレス プール (In-Band IPv6 Network Address Pool)] フィールドに IPv6 アドレス プールを入力することもできます。

IP アドレスがプライマリ ノードで構成されたものと同じプールに属することを確認します。

- 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VIPv6アドレス (Management Network VIPv6 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。
- Note** 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 VIPv6 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 VIPv6 アドレス (Out-of-Band Network VIPv6 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 VIPv6 アドレス (In-Band Network VIPv6 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。

**Note** [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。

**Note** 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
*****
```

**Note** 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。

### What to do next

適切なクレデンシャルを使用して DCNM Web UI にログオンします。

[設定 (Settings)] アイコンをクリックし、[DCNM の詳細 (About DCNM)] を選択します。展開したインストールタイプを表示して確認できます。

デバイス管理にインバンド管理 (eth2) IP アドレスを設定している場合、スタンドアロン サーバにログインし、次のコマンドを使用して、サーバの eth2 からスイッチにインバンドネットワーク到達可能性を設定します。

```
dcnm# appmgr update network-properties add route ipv4 eth2 <ipv4-network-ip-address/prefix>
```

例: 10.0.0.x/30 サブネットを介して接続しているすべてのファブリック リンクを備えた 4 つのスイッチがある場合、およびサブネット 40.1.1.0/24 のインバンド到達可能性に対してすべてのスイッチがループバック インターフェイスで設定されている場合、次のコマンドを使用します。

```
dcnm# appmgr update network-properties session start
dcnm# appmgr update network-properties add route ipv4 eth2 10.0.0.0/24
dcnm# appmgr update network-properties add route ipv4 eth2 40.1.1.0/24
dcnm# appmgr update network-properties session apply
```

## Cisco APIC SE への Cisco DCNM SE ISO のインストール

Cisco Application Services Engine に DCNM と APIC の両方をインストールできます。APIC ASE PID を発注し、後で同じ ASE に Cisco DCNM リリース 11.3(1) または 11.4(1) をインストールすることを選択した場合は、次のエラーメッセージが表示されます。

```

storage.reset()
File "/usr/lib/python2.7/site-packages/blivet/__init__.py", line 511, in reset
  self.devicetree.populate(cleanupOnly=cleanupOnly)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 2256, in populate
  self._populate()
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 2323, in _populate
  self.addUdevDevice(dev)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1293, in addUdevDevice
  self.handleUdevDeviceFormat(info, device)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 2809, in handleUdevDeviceFormat
  self.handleUdevLUMPVFormat(info, device)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1651, in handleUdevLUMPVFormat
  self.handleUgLvS(vg_device)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1588, in handleUgLvS
  addLU(lv)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1531, in addLU
  addRequiredLU(origin_device_name, "failed to locate origin lv")
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1432, in addRequiredLU
  addLU(lv_info.name)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1531, in addLU
  addRequiredLU(origin_device_name, "failed to locate origin lv")
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1432, in addRequiredLU
  addLU(lv_info.name)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1531, in addLU
  addRequiredLU(origin_device_name, "failed to locate origin lv")
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1432, in addRequiredLU
  addLU(lv_info.name)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1531, in addLU
  addRequiredLU(origin_device_name, "failed to locate origin lv")
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1432, in addRequiredLU
  addLU(lv_info.name)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1531, in addLU
  addRequiredLU(origin_device_name, "failed to locate origin lv")
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1432, in addRequiredLU
  addLU(lv_info.name)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1558, in addLU
  exists=True, **lv_kwargs)
File "/usr/lib/python2.7/site-packages/blivet/devices/lvm.py", line 554, in __init__
  exists=exists)
File "/usr/lib/python2.7/site-packages/blivet/devices/dm.py", line 73, in __init__
  parents=parents, sysfsPath=sysfsPath)
File "/usr/lib/python2.7/site-packages/blivet/devices/storage.py", line 131, in __init__
  Device.__init__(self, name, parents=parents)
File "/usr/lib/python2.7/site-packages/blivet/devices/device.py", line 84, in __init__
  raise ValueError("%s is not a valid name for this device" % name)
ValueError: 18fc8614ba7b7c8c8279b588de8861b578bc356b3151834ead1482f9ab94339b is not a valid name for this device
anaconda! :main* 2:shell 3:log 4:storage-log 5:program-log          Switch tab: Alt+Tab | Help: F1

```

既存の APIC ASE に Cisco DCNM 11.3(1) または 11.4(1) をインストールするには、次の手順を実行します。

## 手順

- Step 1** プロンプトで、**CTRL-ALT-F2** を押して別のコンソールに移動します。  
シェル プロンプトが表示されます。
- Step 2** **lsblk -d** コマンドを使用して、ディスクのリストを取得します。
- Step 3** 各ディスクに次のコマンドを実行します。  
(注) UNIGEN 16GB ディスクでこのコマンドを実行しないでください。

**dd if=/dev/zero of=/dev/<disk> bs=10M count=1**

```

root@se-appliance$ lsblk -d
NAME HCTL          TYPE VENDOR   MODEL          REV TRAN
sda  0:2:0:0          disk Cisco    UCSC-RAID12G-2GB 5.10
sdb  0:2:1:0          disk Cisco    UCSC-RAID12G-2GB 5.10
sdc  0:2:2:0          disk Cisco    UCSC-RAID12G-2GB 5.10

```

```
sdd 0:2:3:0    disk Cisco    UCSC-RAID12G-2GB 5.10
sde 0:2:4:0    disk Cisco    UCSC-RAID12G-2GB 5.10
sdf 2:0:0:0    disk ATA      Micron_5100_MTFD H072 sata
sdg 1:0:0:0    disk UNIGEN   PHF16H0CM1-ETG  PMAP usb
root@se-appliance$
```

**Step 4** Cisco Applications Service Engine を再起動します。

**Step 5** Cisco DCNM ISO リリース 11.3(1) または 11.4(1) をインストールします。

詳細については、以下の URL を参照してください。

- 詳細については、『[Cisco DCNM 向け Cisco Application Services Engine インストール ガイド、リリース 11.3\(1\)](#)』を参照してください。
- 詳細については、『[Cisco Application Services Engine Installation Guide For Cisco DCNM、リリース 11.4\(1\)](#)』を参照してください。

## 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:
Install mode: LAN Fabric
Standalone node. HA not enabled.
dcnm#
```

### 手順

**Step 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
```

**Step 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。

**Step 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 **SYSTEMRESOURCEERROR** 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 セカンダリ (Fresh Installation - HA Secondary)] オプション ボタンを選択して、**dcnm2** をセカンダリ 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 ノードと同一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。

クラスタ モードで Cisco DCNM プライマリを構成している場合は、[クラスタ モードを有効にする (Enable Clustered Mode)] チェックボックスをオンにします。

[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。

(注) Network Insights アプリケーションを使用している場合は、DNS サーバが有効で到達可能であることを確認します。

- **[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。

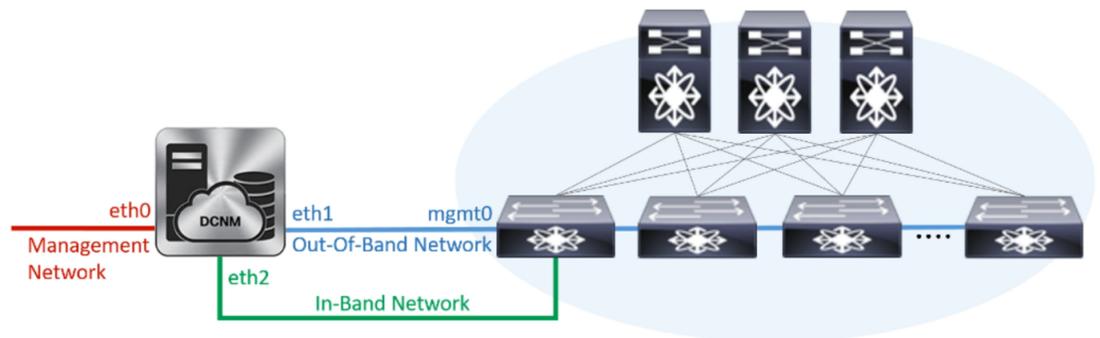
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **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 7: 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]**、および **[クラスタ モード設定]** 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。

2. **[クラスタ モード設定 (Clustered mode configuration)]** 領域で、ネットワーク設定を構成して、クラスタ モードで DCNM インスタンスを展開します。クラスタ モードで、アプリケーションは個別のコンピューティング ノードで実行されます。

- **[アウトオブバンド IPv4 ネットワーク アドレス プール (Out-of-Band IPv4 Network Address Pool)]** で、クラスタ モードで使用するアウトオブバンド IPv4 ネットワークからアドレス プールを入力します。

オプションで、**[アウトオブバンド IPv6 ネットワーク アドレス プール (Out-of-Band IPv6 Network Address Pool)]** フィールドに IPv6 アドレス プールを入力することもできます。

- **[インバンド IPv4 ネットワーク アドレス プール (In-Band IPv4 Network Address Pool)]** で、クラスタ モードで使用するインバンド IPv4 ネットワークからアドレス プールを入力します。

オプションで、**[インバンド IPv6 ネットワーク アドレス プール (In-Band IPv6 Network Address Pool)]** フィールドに IPv6 アドレス プールを入力することもできます。

IP アドレスがプライマリ ノードで構成されたものと同じプールに属していることを確認します。

- 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VIPv6アドレス (Management Network VIPv6 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 VIPv6 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VIPv6アドレス (Out-of-Band Network VIPv6 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VIPv6アドレス (In-Band Network VIPv6 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（古いスタンドアロンノード）：

```

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

```

## Cisco DCNM コンピューティングノードのインストール

[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。Cisco DCNM OVA と ISO の両方の展開にコンピューティングノードをインストールできます。



**Note** コンピューティングノードを使用すると、アプリケーション負荷が、通常の 1 または 2 (HA がある場合) ノードではなく、すべてのコンピューティングノードで共有されるため、ユーザーは DCNM を拡張できます。



**Note** DCNM のインストール中に [クラスター化モードを有効にする] が選択された場合、構成コンプライアンス、EPL、NIA、NIR などのアプリケーションは、計算ノードをインストールするまで機能しません。

NIR/NIA アプリケーションがより大規模に有効になっている場合、つまり 250 のスイッチと 10000 のハードウェア テレメトリ フローがある場合、DCNM Computes ノードは 10Gig リンクを使用し、すべての eth0、eth1、および eth2 インターフェイスに接続する必要があります。

Web インストーラから Cisco DCNM コンピューティング ノードのインストールを完了するには、次の手順を実行します。

### Before you begin

コンピューティング ノードをインストールするには、16 個の vCPUs、64 GB の RAM、および 500 GB のハードディスクがあることを確認します。

デフォルトでは、**ComputeHuge** 構成には 32vCPU と 2GB ディスクの 128GB RAM があります。この構成は Cisco Network Insights アプリケーションを使用する場合にお勧めします。

### Procedure

- 
- Step 1** [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。
- Step 2** [Cisco DCNM インストーラ (Cisco DCNM Installer)] 画面で、[新規インストール - スタンドアロン (Fresh Installation - Standalone)] オプション ボタンを選択します。
- [Continue] をクリックします。
- Step 3** [インストール モード (Install Mode)] タブのドロップダウン リストから、[コンピューティング (Compute)] を選択して DCNM インスタンスを展開します。
- Note** OVF テンプレートまたは ISO ハイパーバイザを構成する間に、[コンピューティング (Compute)] feature-id="dcnm-11-4-1">または [ComputeHuge] を選択した場合、[コンピューティング (Compute)] オプションはドロップダウン リストに表示されます。
- [Next] をクリックします。
- Step 4** [管理 (Administration)] タブで、パスワードに関する情報を入力します。
- [管理者のパスワード] フィールドで、Cisco DCNM のアプリケーションに接続するために使用されるパスワードを入力してください。
- パスワードは、%\$^=;.\*'" <SPACE> を除くすべての特殊文字を使用できます。
- [管理者パスワードの確認] フィールドにパスワードをもう一度入力します。
- 入力したパスワードを表示するには、[入力したパスワードを表示する (Show passwords in clear text)] チェックボックスをオンにします。
- [次へ (Next)] をクリックします。
- Step 5** [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。

**Note** Network Insights アプリケーションを使用している場合は、DNS サーバが有効で到達可能であることを確認します。

- **[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。

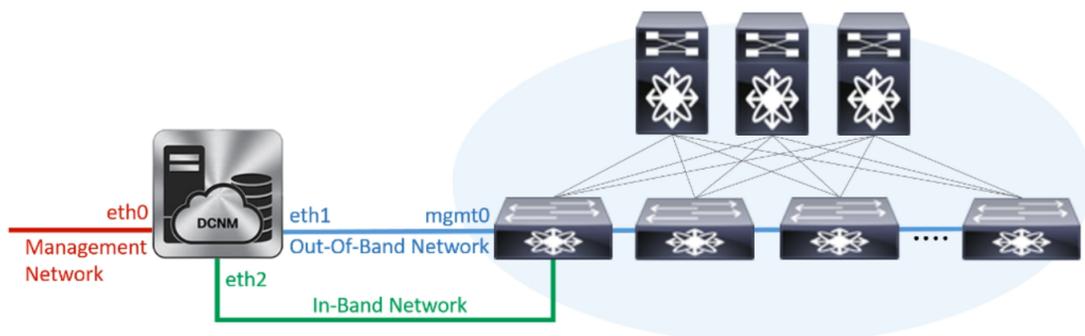
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **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。

- Step 6** **[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。

Figure 8: Cisco DCNM 管理ネットワーク インターフェイス



- a) **[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。

**Note** Cisco DCNM リリース 11.2(1) から、管理ネットワークの IPv6 アドレスも使用できます。

(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。

- b) **[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。

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。

**Note** 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。

- c) **[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。

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。

**Note** 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。

ただし、**appmgr update network-properties** コマンドを使用して、必要に応じてインストール後にネットワーク プロパティを編集できます。詳細については、「[DCNM インストール後のネットワーク プロパティ, on page 163](#)」を参照してください。

[Next] をクリックします。

- Step 7** **[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。

すべてのアプリケーションがこのサブネットからの IP アドレスを使用します。

[次へ (Next)] をクリックします。

- Step 8** **[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 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。

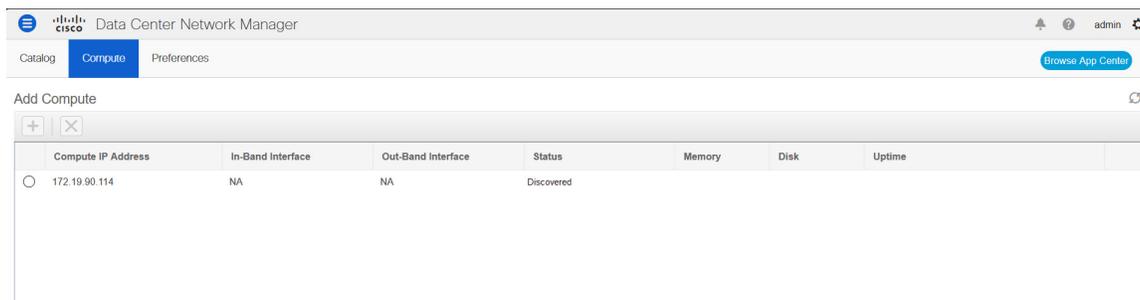
DCNM コンピューティング ノードにアクセスするための URL を含む成功メッセージが表示されます。

```
*****
Your Cisco DCNM Compute Node has been installed.
Click on the following link to go to DCNM GUI's Application page:
DCNM GUI's Applications
You will be redirected there in 60 seconds.
Thank you
*****
```

## What to do next

適切なクレデンシヤルを使用して DCNM Web UI にログオンします。

[**アプリケーション (Applications)**] タブには、インストールした DCNM 展開で実行中のすべてのサービスが表示されます。[**コンピューティング (Compute)**] タブをクリックすると、CISCO Dcnm Web UI で検出された状態の新しいコンピューティングが表示されます。



クラスタにコンピューティングノードを追加するために、詳細については、展開固有の『Cisco DCNM コンフィギュレーションガイド』の「[クラスタノードへのコンピューティングの追加](#)」を参照してください。



**Note** DCNM をインストールする間にクラスタされたモードを有効にしなかった場合は、**appmgr afw config-cluster** コマンドを使用して、コンピューティングクラスタを有効にします。手順については、『Cisco DCNM LAN ファブリック コンフィギュレーションガイド』の「[コンピューティングクラスタを有効にする](#)」を参照してください。

コンピューティングノードがスケジュールされていないパワーサイクルを通過し、再起動するとき、Elasticsearch コンテナは起動しません。一部のファイルシステムが破損している可能性があります。この問題を解決するために、**fsck -y** コマンドを使用して、セーフモードでコンピューティングノードをリブートしてください。



## 第 5 章

# Cisco DCNM のアップグレード

この章では、Cisco DCNM のアップグレードについて説明します。次の項を含みます。

- [インラインアップグレードを使用して ISO または OVA をアップグレードする \(81 ページ\)](#)

## インラインアップグレードを使用して ISO または OVA をアップグレードする

既存の DCNM に新しい DCNM を提供することで、インラインアップグレードで DCNM をアップグレード可能になります。インラインアップグレード後、DCNM アプリケーションを起動する前にブラウザ キャッシュを消去するようにしてください。

Cisco DCNM をインストールするとき、デフォルトで自己署名付き証明書がインストールされています。ただし、最新の Cisco DCNM リリースにアップグレードした後は、証明書を復元する必要があります。



- 
- (注) 証明書の復元は、破壊的なメカニズムです。アプリケーションを停止して再起動する必要があります。アップグレードされたシステムが安定している場合にのみ、証明書を復元します。つまり、Cisco DCNM Web UI にログインできる必要があります。

アップグレード後に証明書を復元するには、[アップグレード後に証明書を復元する \(137 ページ\)](#) を参照してください。

ここでは、インラインアップグレード方式を使用して DCNM をアップグレードする手順について説明します。



- 
- (注) クラシック LAN 展開のアップグレードでは、DCNM リリースにアップグレードすると、展開は自動的に LAN ファブリック展開モードに変換されます。
-

# スタンドアロン モードでの DCNM 仮想アプライアンスのインラインアップグレード

既存の DCNM に新しい DCNM を提供することで、インラインアップグレードで DCNM をアップグレード可能になります。インラインアップグレード後、DCNM アプリケーションを起動する前にブラウザ キャッシュを消去するようにしてください。

スタンドアロン モードで DCNM 仮想アプライアンスをアップグレードするには、次の作業を実行します。

## Before you begin

Cisco DCNM セットアップがクラスタ モードの場合は、必ず Network Insights - Resources (NIR) 2.x アプリケーションを停止してください。Cisco DCNM Web UI で、[アプリケーション (Applications)] > [カタログ (Catalog)] を選択します。NIR アプリで、[停止 (Stop)] アイコンをクリックしてアプリケーションを停止します。カタログからアプリケーションを削除するには、[削除 (Delete)] をクリックします。

## Procedure

**Step 1** Cisco DCNM アプライアンス コンソールにログインします。

**Caution** システム要件が最小リソース要件を満たしていない場合、コンソールまたは SSH 経由で DCNM にログオンするたびに、**SYSTEM RESOURCE ERROR** が表示されます。コンソール/ SSH 経由で DCNM にシステム要件のログオンを変更します。

- OVA のインストールの場合：ホスト用に展開された OVF テンプレートで、右クリックして [設定 (Settings)] > [Web コンソールの起動 (Launch Web Console)] を選択します。
- ISO のインストールの場合：KVM コンソールまたは UCS (ベア メタル) コンソールを選択します。

**Caution** SSH セッションからインラインアップグレードを実行しないでください。セッションがタイムアウトし、アップグレードが不完全になることがあります。

または

次のコマンドを実行してスクリーンセッションを作成します。

```
dcnm# screen
```

これにより、コマンドを実行できるセッションが作成されます。このコマンドは、ウィンドウが表示されていない場合、または切断された場合でも実行し続けます。

**Step 2** **appmgr backup** コマンドを使用してアプリケーション データのバックアップを取得します。

```
dcnm# appmgr backup
```

DCNM サーバの外部にある安全な場所にバックアップ ファイルをコピーします。

**Step 3** **su** コマンドを使用して、`/root/` ディレクトリにログオンします。

```
dcnm# su
Enter password: <<enter-password>>
```

**Note** ISO をディレクトリにマウントする前に、`/root/` フォルダーにアクセスできることを確認します。

**Step 4** **mkdir /mnt/iso** コマンドを使用して、**iso** という名前のフォルダを作成します。

```
dcnm# mkdir /mnt/iso
```

**Step 5** `/mnt/iso/packaged-files/scripts/` に移動して `./inline-upgrade.sh` スクリプトを実行します。

```
dcnm# cd /mnt/iso/packaged-files/scripts/
dcnm# ./inline-upgrade.sh Do you want to continue and perform the inline upgrade to ? [y/n]:
y
```

**Note** Cisco DCNM リリース 11.2(1) からアップグレードする場合にのみ、新しい `sysadmin` パスワードを入力するように求められます。

**Step 6** プロンプトで新しい `sysadmin` ユーザー パスワードを入力します。

**Note** Cisco DCNM リリース 11.2(1) からアップグレードする場合にのみ、新しい `sysadmin` パスワードを入力するように求められます。

```
Enter the password for the new sysadmin user: <<sysadmin_password>>
Enter it again for verification: <<sysadmin_password>>
```

アップグレードが完了すると、アプライアンスが再起動します。再起動後、`SSH \root` アクセスはデフォルトで無効になっています。**sysadmin** ユーザーを使用します。

以前の `Elasticsearch` バージョンは、11.5(1) でサポートされている `Elasticsearch` バージョンと互換性がないため、リリース 11.5(1) にアップグレードした後で、`Elasticsearch` データのインデックスを再作成する必要があります。

次のメッセージが生成されます。

```
*****
WARNING: Elasticsearch indices for historical Performance Monitoring (PM)
data need to be reindexed manually.
Check DCNM installation and upgrade guide for more details.
*****
```

確認メッセージが表示されます。**[y]** を入力して、アップグレードを続行してください。

アップグレードの完了後に、システムがリブートします。

**Step 7** **appmgr status all** コマンドを使用して、DCNM アプリケーションが機能していることを確認します。

```
dcnm# appmgr status all
```

**Step 8** Cisco DCNM リリース 11.4(1) が正常にインストールされていることを確認するには、**appmgr show version** コマンドを使用します。

```
dcnm# appmgr show version
```

```
Cisco Data Center Network Manager
```

```
Version: 11.4(1)
Install mode: LAN Fabric
Standalone node. HA not enabled.
```

### What to do next

適切なクレデンシャルを使用して DCNM Web UI にログインします。



**Note** リリース11.3(1)では、sysadmin と root ユーザーのパスワードは同一ではありません。にアップグレードすると、sysadmin および root ユーザーのパスワードは保持されます。

ただし、アップグレード後にCisco DCNMでバックアップと復元を実行すると、sysadmin ユーザーは root ユーザーからパスワードを継承するため、両方のユーザーが同じパスワードを持ちます。復元が完了したら、両方のユーザーのパスワードを変更できます。

[設定 (Settings)] アイコンをクリックし、[DCNM の詳細 (About DCNM)] を選択します。展開したインストールタイプを表示して確認できます。

古いPMデータはElasticsearchに保持されます。Elasticsearchは、Cisco DCNM Web UI、[ダッシュボード (Dashboard)]、[ヘルス (Health)] と [管理 (Administration)]、[DCNMサーバ (DCNM Server)]、[サーバステータス (Server Status)] の順に選択すると、再インデックスが必要と表示されます。

古い Performance Manager (PM) データを破棄し、DCNM リリース 11.4(1) へのアップグレードを続けるように選択できます。Performance Managerデータをドロップする方法については、を参照してください。

Performance Manager データを保存することを選択した場合は、Cisco TAC に連絡してサポートを受けることを推奨します。

Cisco DCNM リリース 11.5(1) にアップグレード後に Cisco Nexus 9000 スイッチを構成する Cisco DCNM リリース 11.3(1) またはリリース 11.4(1) 管理対象 VXLAN BGP EVPN ファブリックを正常にオンボードするには、「[VXLAN BGP EVPN、外部、および MSD ファブリックの DCNM 11.5 \(1\) アップグレード後](#)」を参照してください。

## ネイティブ HA モードでの DCNM 仮想アプライアンスのインラインアップグレード

既存の DCNM に新しい DCNM を提供することで、インラインアップグレードで DCNM をアップグレード可能になります。インラインアップグレード後、DCNMアプリケーションを起動する前にブラウザ キャッシュを消去するようにしてください。

ネイティブ HA モードで DCNM 仮想アプライアンスをアップグレードするには、次の作業を実行します。

## Before you begin

- Cisco DCNM 11.1(1)、Cisco DCNM 11.2(1) の両方または Cisco DCNM 11.3(1) Active と Standby ピアが起動して実行中であることを確認します。
- クラスタ モードで Cisco DCNM をアップグレードする前に、Network Insights - Resources (NIR) 2.x アプリケーションを停止します。Cisco DCNM Web UI で、[アプリケーション (Applications)] > [カタログ (Catalog)] を選択します。NIR アプリで、[停止 (Stop)] アイコンをクリックしてアプリケーションを停止します。カタログからアプリケーションを削除するには、[削除 (Delete)] をクリックします。



**Note** クラスタ モードでの Cisco DCNM のインラインアップグレードは、リリース 11.2(1) 以降でサポートされています。リリース 11.1(1) では、クラスタ モードの DCNM のインラインアップグレードはサポートされていません。

- **appmgr show ha-role** コマンドを使用して、アクティブ サーバとスタンバイ サーバが動作していることを確認します。

例:

アクティブ ノードで次の操作を実行します。

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

スタンバイ ノードで次の操作を実行します。

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

## Procedure

**Step 1** ファイルを解凍し、ファイルを /root/ フォルダに、アップグレードする DCNM セットアップの Active と Standby ノードの両方でアップロードします。

**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。

**Step 2** Cisco DCNM アプライアンス コンソールにログインします。

**Caution** システム要件が最小リソース要件を満たしていない場合、コンソールまたは SSH 経由で DCNM にログオンするたびに、**SYSTEM RESOURCE ERROR** が表示されます。コンソール/SSH 経由で DCNM にシステム要件のログオンを変更します。

- OVA のインストールの場合: ホスト用に展開された OVF テンプレートで、右クリックして [設定 (Settings)] > [Web コンソールの起動 (Launch Web Console)] を選択します。
- ISO のインストールの場合: KVM コンソールまたは UCS (ベア メタル) コンソールを選択します。

**Caution** SSHセッションからインラインアップグレードを実行しないでください。セッションがタイムアウトし、アップグレードが不完全になることがあります。

または

次のコマンドを実行してスクリーンセッションを作成します。

```
dcnm1# screen
dcnm2# screen
```

これにより、コマンドを実行できるセッションが作成されます。このコマンドは、ウィンドウが表示されていない場合、または切断された場合でも実行し続けます。

**Step 3** アクティブおよびスタンバイの両方のアプライアンスで **appmgr backup** コマンドを使用して、アプリケーションデータのバックアップを取得します。

```
dcnm1# appmgr backup
dcnm2# appmgr backup
```

DCNM サーバの外部にある安全な場所にバックアップ ファイルをコピーします。

**Step 4** アクティブノードで、インラインアップグレードを実行します。

a) **mkdir /mnt/iso** コマンドを使用して、**iso** という名前のフォルダを作成します。

```
dcnm1# mkdir /mnt/iso
```

b) DCNM ISO ファイルを /mnt/iso フォルダで Active ノードにマウントします。

c) **/mnt/iso/packaged-files/scripts/** に移動し、**./inline-upgrade.sh** スクリプトを実行します。

```
dcnm1# cd /mnt/iso/packaged-files/scripts/
dcnm1# ./inline-upgrade.sh
```

**Note** 一部のサービスがまだ実行されている場合は、サービスが停止することを示すプロンプトが表示されます。プロンプトが表示されたら、**y** を押して続行します。

d) プロンプトで新しい **sysadmin** ユーザー パスワードを入力します。

**Note** Cisco DCNM リリース 11.1(1) またはリリース 11.2(1) からアップグレードする場合にのみ、新しい **sysadmin** パスワードを入力するように求められます。

```
Enter the password for the new sysadmin user: <<sysadmin_password>>
Enter it again for verification: <<sysadmin_password>>
```

アップグレードが完了すると、アプライアンスが再起動します。再起動後、SSH \root アクセスはデフォルトで無効になっています。**sysadmin** ユーザーを使用します。

以前の Elasticsearch バージョンは、11.5(1) でサポートされている Elasticsearch バージョンと互換性がないため、リリース 11.5(1) にアップグレードした後で、Elasticsearch データのインデックスを再作成する必要があります。

次のメッセージが生成されます。

```
*****
WARNING: Elasticsearch indices for historical Performance Monitoring (PM)
data need to be reindexed manually.
Check DCNM installation and upgrade guide for more details.
*****
```

確認メッセージが表示されます。[y] を入力して、アップグレードを続行してください。

アップグレードの完了後に、システムがリブートします。

- e) **appmgr status all** コマンドを使用して、DCNM アプリケーションが機能していることを確認します。

```
dcnm1# appmgr status all
```

**Note** スタンバイ ノードのアップグレードに進む前に、すべてのサービスが Cisco DCNM アクティブ ノードで稼働していることを確認します。

- f) **appmgr show ha-role** コマンドを使用して、アクティブ ノードのロールを確認します。現在のロールはアクティブとして表示される必要があります。

```
dcnm1# appmgr show ha-role
```

```
Native HA enabled.
Deployed role: Active
Current role: Active
```

**Warning** アクティブ ノードの現在のロールがアクティブでない限り、スタンバイ ノードのアップグレードを続行しないことをお勧めします。

**Step 5** スタンバイ ノードで、インラインアップグレードを実行します。

- a) **mkdir /mnt/iso** コマンドを使用して、**iso** という名前のフォルダを作成します。

```
dcnm2# mkdir /mnt/iso
```

- b) DCNM ISO ファイルを /mnt/iso フォルダで Standby ノードでマウントします。

- c) /mnt/iso/packaged-files/scripts/ に移動し、**./inline-upgrade.sh** スクリプトを実行します。

```
dcnm2# cd /mnt/iso/packaged-files/scripts/
dcnm2# ./inline-upgrade.sh --standby
```

**Note** 一部のサービスがまだ実行されている場合は、サービスが停止することを示すプロンプトが表示されます。プロンプトが表示されたら、[y] を押して続行します。

- d) プロンプトで新しい sysadmin ユーザー パスワードを入力します。

**Note** Cisco DCNM リリース 11.1(1) またはリリース 11.2(1) からアップグレードする場合にのみ、新しい sysadmin パスワードを入力するように求められます。

```
Enter the password for the new sysadmin user: <<sysadmin_password>>
Enter it again for verification: <<sysadmin_password>>
```

アップグレードが完了すると、アプライアンスが再起動します。再起動後、SSH \root アクセスはデフォルトで無効になっています。**sysadmin** ユーザーを使用します。

アップグレードが完了すると、アプライアンスが再起動します。次のコマンドを使用して、アプライアンスのロールを確認します。

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

### What to do next

適切なクレデンシャルを使用して DCNM Web UI にログインします。



**Note** リリース 11.3(1) では、`sysadmin` と `root` ユーザーのパスワードは同一ではありません。にアップグレードすると、`sysadmin` および `root` ユーザーのパスワードは保持されます。

ただし、アップグレード後に Cisco DCNM でバックアップと復元を実行すると、`sysadmin` ユーザーは `root` ユーザーからパスワードを継承するため、両方のユーザーが同じパスワードを持ちます。復元が完了したら、両方のユーザーのパスワードを変更できます。

**[設定 (Settings)]** アイコンをクリックし、**[DCNM の詳細 (About DCNM)]** を選択します。展開したインストールタイプを表示して確認できます。

古い PM データは Elasticsearch に保持されます。Elasticsearch は、Cisco DCNM Web UI、**[ダッシュボード (Dashboard)]**、**[ヘルス (Health)]** と **[管理 (Administration)]**、**[DCNM サーバ (DCNM Server)]**、**[サーバステータス (Server Status)]** の順に選択すると、再インデックスが必要と表示されます。

古い Performance Manager (PM) データを破棄し、DCNM リリース 11.4(1) へのアップグレードを続行するように選択できます。Performance Manager データをドロップする方法については、を参照してください。

Performance Manager データを保存することを選択した場合は、Cisco TAC に連絡してサポートを受けることを推奨します。

を使用して、両方のアプライアンスのロールを確認します。 **appmgr show ha-role**

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

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

**appmgr status all** コマンドを使用して、すべてのアプリケーションのステータスを確認します。

Cisco DCNM リリース 11.5(1) にアップグレード後に Cisco Nexus 9000 スイッチを構成する Cisco DCNM リリース 11.3(1) またはリリース 11.4(1) 管理対象 VXLAN BGP EVPN ファブリックを正常にオンボードするには、「[VXLAN BGP EVPN、外部、および MSD ファブリックの DCNM 11.5 \(1\) アップグレード後](#)」を参照してください。

# DCNM コンピューティングノードのインラインアップグレード

DCNM コンピューティングノードをインラインアップグレードを使用してアップグレードできます。インラインアップグレードでは、新しい DCNM バージョンを既存のコンピューティングノードに強制することによって、コンピューティングノードをアップグレードできます。



**Note** Cisco DCNM リリース 11.3(1) の Cisco アプリケーションサービスのコンピューティングノードをインラインアップグレード手順を使用してアップグレードできます。詳細については、『<https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/products-installation-guides-list.html>』を参照してください。

スタンドアロンとネイティブの両方の HA モードで DCNM コンピューティングノードをアップグレードするには、次の作業を実行します。

## Before you begin

DCNM コンピューティングノードをアップグレードする前に、スタンドアロンノードまたはネイティブ HA モードのいずれかの Cisco DCNM サーバをリリースにアップグレードする必要があります。

## Procedure

**Step 1** Cisco DCNM コンピューティングコンソールにログオンします。

**Caution** SSHセッションからインラインアップグレードを実行しないでください。セッションがタイムアウトし、アップグレードが不完全になることがあります。

**Caution** システム要件が最小リソース要件を満たしていない場合、コンソールまたは SSH 経由で DCNM にログオンするたびに、**SYSTEM RESOURCE ERROR** が表示されます。コンソール/SSH 経由で DCNM にシステム要件のログオンを変更します。

または

次のコマンドを実行して、コンピューティングノードにスクリーンセッションを作成します。

```
dcnm-compute# screen
```

これにより、コマンドを実行できるセッションが作成されます。このコマンドは、ウィンドウが表示されない場合や切断された場合でも実行され続けます。

**Step 2** すべてのコンピューティングで `mkdir /mnt/iso` コマンドを使用して、`iso` という名前のフォルダを作成します。

```
dcnm-compute# mkdir /mnt/iso
```

**Step 3** DCNM ISO ファイルを `/mnt/iso` フォルダのコンピューティングノードでフォルダにマウントします。

すべてのコンピューティングノードに ISO をマウントします。

**Step 4** /mnt/iso/packaged-files/scripts に移動して `./inline-upgrade.sh` スクリプトを実行します。

**Note** 一部のサービスがまだ実行されている場合は、サービスを停止するように促すプロンプトが表示されます。プロンプトが表示されたら、**y** を押して続行します。

**Note** Cisco DCNM リリース 11.1(1) またはリリース 11.2(1) からアップグレードする場合にのみ、新しい `sysadmin` パスワードを入力するように求められます。

**Step 5** プロンプトで新しい `sysadmin` ユーザー パスワードを入力します。

```
Enter the password for the new sysadmin user:<<sysadmin_password>>
Enter it again for verification:<<sysadmin_password>>
```

アップグレードが完了すると、コンピューティング ノードが再起動します。再起動後、SSH \root アクセスはデフォルトで無効になっています。 `sysadmin` ユーザーを使用します。

**Step 6** `appmgr show version` コマンドを使用して、Cisco DCNM リリース へのアップグレードが正常に行われたことを確認します。

```
dcnm-compute# appmgr show version

Cisco Data Center Network Manager
Version:
Install mode: Compute
```

### What to do next

クラスタ内の 3 つのコンピューティング ノードすべてをアップグレードする必要があります。

アップグレードプロセスが完了すると、各コンピューティング ノードが再起動し、自動的にクラスタに参加します。Cisco DCNM Web UI で、[アプリケーション (Applications)] > [コンピューティング (Compute)] の順に選択して、コンピューティング ノードが [結合済み (Joined)] として表示されるかどうかを確認します。

Cisco DCNM リリース 11.5(1) にアップグレード後に Cisco Nexus 9000 スイッチを構成する Cisco DCNM リリース 11.3(1) またはリリース 11.4(1) 管理対象 VXLAN BGP EVPN ファブリックを正常にオンボードするには、「[VXLAN BGP EVPN、外部、および MSD ファブリックの DCNM 11.5 \(1\) アップグレード後](#)」を参照してください。



## 第 6 章

# Cisco DCNM Classic LAN 展開のアップグレード

- 概要 (91 ページ)
- ファブリックの移行 (92 ページ)
- アップグレード後の LAN ファブリックでサポートされるスイッチ ロール (94 ページ)
- LAN ファブリックの従来の LAN テンプレート (95 ページ)
- クラシック LAN 展開から LAN ファブリック展開へのアップグレード (98 ページ)
- LAN クラシック ファブリック テンプレートの機能 (102 ページ)

## 概要

Cisco DCNM リリース 11.4(1) 以降では、クラシック LAN の導入はサポートされていません。クラシック LAN 展開を DCNM リリース 11.4(1) にアップグレードする場合、使用できるアップグレードオプションは DCNM リリース 11.4(1) LAN ファブリック展開のみで、DCNM インラインアップグレードプロセス中に自動的に実行されます。

次の表に、への従来の LAN 展開のアップグレードの概要を示します。

古いリリースから Cisco DCNM リリース 11.4 (1) へのインラインアップグレードを実行すると、**LAN\_Classic** および **Fabric\_Group** ファブリック テンプレートを使用した LAN ファブリック モードへの自動変換が実行されます。



- (注) アップグレードを進める前に、Cisco DCNM LAN ファブリックの機能を理解しておくことをお勧めします。詳細については、『』 『』を参照してください。

### 前提条件

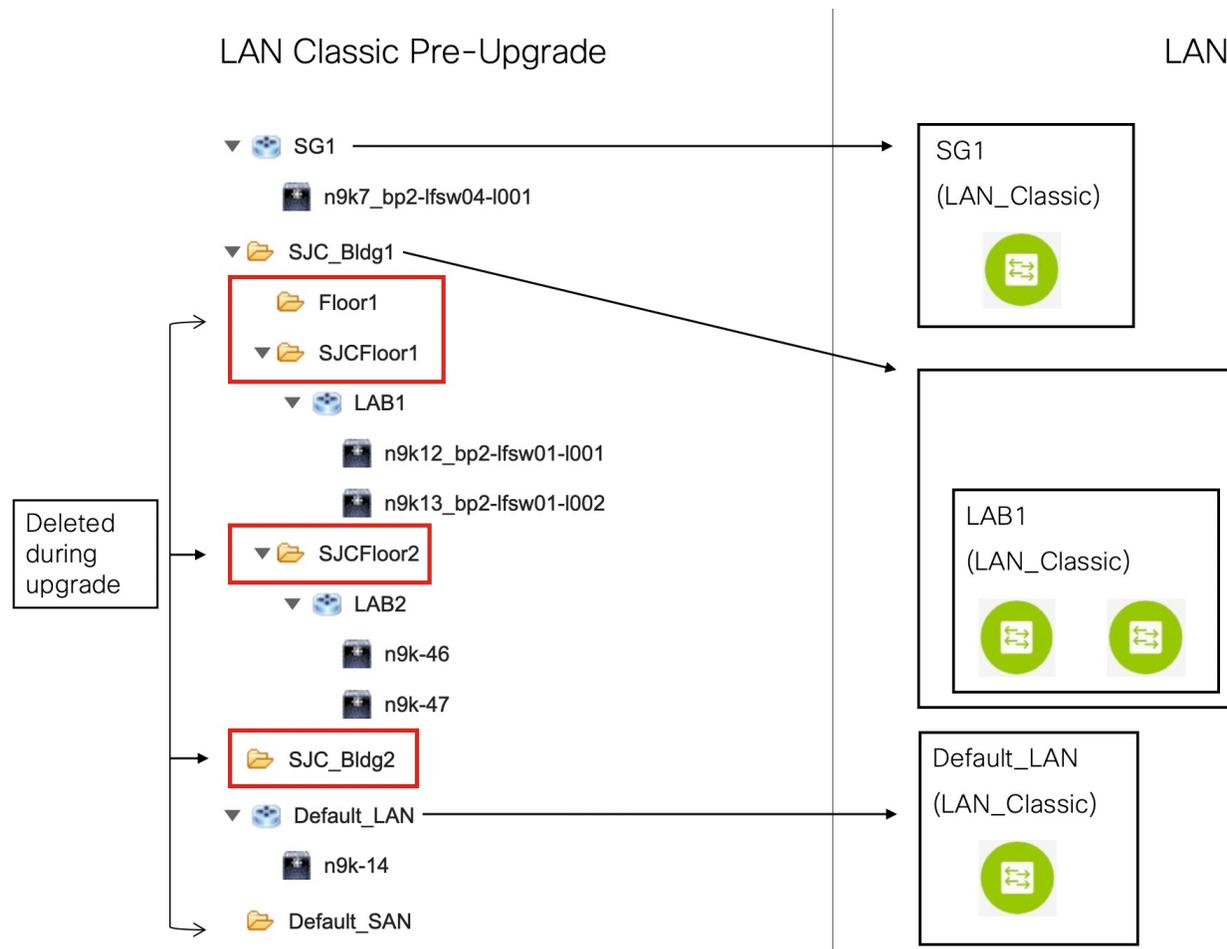
- 「Cisco DCNM LAN Fabric Verified Scalability」セクションを参照して、既存の導入ニーズが満たされていることを確認します。『*Verified Scalability Guide for Cisco DCNM*』を参照してください。

### 注意事項と制約事項

- クラシック LAN 展開では、インバンド インターフェイスを使用してスイッチを管理している場合、LAN ファブリック展開へのアップグレードはサポートされません。管理 (mgmt0) インターフェイスを使用してスイッチを管理するように変更してから、アップグレードする必要があります。
- インバンド インターフェイス管理のサポートは、将来のリリースで使用可能になる予定です。
- Cisco Nexus 7000 シリーズ スイッチの VDC 自動プロビジョニング (VOAP) は、LAN ファブリック インストール モードではサポートされません。
- 次の設定は、クラシック LAN から LAN ファブリック展開に移行されません。
  - アーカイブ ジョブの設定。  
アップグレード後に、ファブリックの設定からファブリックのバックアップを設定する必要があります。
  - CLI ジョブ。
  - POAP DHCP 設定。  
アップグレード後に、POAP のファブリック設定を構成する必要があります。

## ファブリックの移行

クラシック LAN からの DCNM アップグレードでは、クラシック LAN スイッチおよびコンテナグループに一致するように、LAN ファブリックにファブリック インスタンスが自動的に作成されます。ネストされたグループ化が存在する場合、LAN ファブリックモードへのインラインアップグレードでは、2 レベルの階層のみが保持されます。すべての中間グループまたは空のグループが自動的に削除されます。参考として、次の図を参照してください。



移行動作のサマリは、次のとおりです。

- スイッチを保持するスイッチグループのみが、LAN\_Classicファブリックテンプレートを使用してファブリックインスタンスに移行されます。この例では、**SG1**、**LAB1**、**LAB2**、および**Default\_LAN**が移行されます。
- アップグレード中に維持される階層のレベルは2つだけです。中間グループが削除され、最下位レベルのスイッチグループが階層の最上位に昇格されます。

この例では、次のようになります。

- **SJC\_Bldg1** は、クラシック LAN で有効なスイッチグループを持つ最上位のテナグループです。したがって、**SJC\_Bldg1** のファブリックインスタンスが LAN ファブリックで作成され、**Fabric\_Group** テンプレートが使用されます。
- **LAB1** および **LAB2** のファブリックインスタンスは、LAN ファブリックの **LAN\_Classic** ファブリックテンプレートを使用して作成されます。これらのファブリックインスタンスは、**SJC\_Bldg1** のメンバーファブリックになります。
- 中間の **SJC\_Floor1** および **SJC\_Floor2** テナは、LAN ファブリックに引き継がれません。

- 有効なスイッチグループがないテナグループは移行されません。この例では、**Floor1** と **SJC\_Bldg2** は移行されません。
  - スイッチグループは、**LAN\_Classic** ファブリック テンプレートを使用してスタンドアロン ファブリック インスタンスに移行されます。この例では、**Default\_LAN** は **LAN\_Classic** ファブリック テンプレートを使用して LAN ファブリックに移行されます。
  - 移行後、デバイスは **LAN\_Classic** ファブリック テンプレートに関連付けられたファブリックで **移行モード** になります。ファブリックは **ファブリック モニタ モード** になります。
- 次の手順の詳細については、「従来の LAN 展開から LAN ファブリック展開へのアップグレード」を参照してください。

## アップグレード後の LAN ファブリックでサポートされるスイッチ ロール

クラシック LAN インストール モードでサポートされているスイッチ ロールの一部は、LAN ファブリックでは使用できません。次の表に、従来の LAN のスイッチ ロールと LAN ファブリックの同等のスイッチ ロールを示します。

クラシック LAN (アップグレード前)	LAN ファブリック (アップグレード後)
ボーダー PE	ボーダー
エッジ	エッジ ルータ
FEX ホスト 管理 VDC	アクセス

これらのロールは、アップグレード後に LAN ファブリックの同等のロールに自動的にマッピングされることに注意してください。

次のスイッチの役割は、アップグレード後も LAN ファブリックで同じです。

- スパイン
- リーフ
- ボーダー スパイン
- ボーダー
- ボーダーゲートウェイ
- エッジ ルータ
- コア ルータ

- アクセス
- 集約

## LAN ファブリックの従来の LAN テンプレート

`templateType = CLI` のテンプレートは、`templateType = POLICY` に変換されます。これらのテンプレートは、[制御 (Control)] > [テンプレート ライブラリ (Template Library)] に表示されます。必要に応じて、[ポリシーの表示/編集 (View / Edit Policies)] ウィンドウから PTI を作成できます。

Templates

<input type="checkbox"/>	Name	Supported Platforms	Tags	Template ...	Template ...
<input type="checkbox"/>	aaa_radius	N9K		POLICY	DEVICE
<input type="checkbox"/>	aaa_radius_deadtime	N9K		POLICY	DEVICE
<input type="checkbox"/>	aaa_radius_key	N9K		POLICY	DEVICE
<input type="checkbox"/>	aaa_radius_src_interface	N9K		POLICY	DEVICE
<input type="checkbox"/>	aaa_radius_use_vrf	N9K		POLICY	DEVICE
<input type="checkbox"/>	aaa_tacacs	N9K		POLICY	DEVICE
<input type="checkbox"/>	aaa_tacacs_key	N9K		POLICY	DEVICE
<input type="checkbox"/>	aaa_tacacs_src_interface	N9K		POLICY	DEVICE
<input type="checkbox"/>	aaa_tacacs_use_vrf	N9K		POLICY	DEVICE

## View/Edit Policies for n9k-46(FDO231003AX)

<input type="button" value="+"/> <input type="button" value="✎"/> <input type="button" value="✕"/> <input type="button" value="View"/> <input type="button" value="View All"/> <input type="button" value="Push Config"/> <input type="button" value="Current Switch Config"/>					
<input type="checkbox"/>	Policy ID	Template	Description	Generated Config	Entity
<input type="checkbox"/>	POLICY-28720	host_11_1		<a href="#">View</a>	SWITC
<input type="checkbox"/>	POLICY-28730	nfm_switch_user		<a href="#">View</a>	SWITC
<input type="checkbox"/>	POLICY-28740	snmp_server_host_trap		<a href="#">View</a>	SWITC
<input type="checkbox"/>	POLICY-28700	switch_freeform	management vrf configuration	<a href="#">View</a>	SWITC
<input type="checkbox"/>	POLICY-28660	int_mgmt_11_1		<a href="#">View</a>	mgmt0
<input type="checkbox"/>	POLICY-28670	mgmt_interface_11_1		<a href="#">View</a>	mgmt0
<input type="checkbox"/>	POLICY-28680	no_shut_interface		<a href="#">View</a>	mgmt0
<input type="checkbox"/>	POLICY-28690	int_eth		<a href="#">View</a>	mgmt0
<input type="checkbox"/>	POLICY-28650	device_type		<a href="#">View</a>	SWITC



(注) 自動的に更新されるポリシーを確認する必要がある場合は、元のファイルのバックアップがDCNMの /usr/local/cisco/dcm/dcnm/data/templates/ ディレクトリに保存されます。

クラシック LAN で使用可能なテンプレート言語の一部は、LAN ファブリックのインストールではサポートされていません。次に例を示します。

- カスタム プロンプト処理
- コマンド実行ロジック
- 派生/継承テンプレート



(注) LAN ファブリックを使用するには、テンプレートを適切に編集する必要があります。

## サポートされていないテンプレート言語コンテンツ

次のクラシック LAN テンプレート言語機能は、LAN ファブリック インストール モードではサポートされていません。

このコンテンツを使用する既存のテンプレートはサポートされていないことに注意してください。互換性のあるテンプレートを作成するには、それらを確認または編集する必要があります。

### 1. インタラクティブ コマンド処理

インタラクティブ コマンドを処理するためのテンプレート コンテンツの一部として、プロンプトと応答を含めます。

次に例を示します。

```
##template variables
string srcFile;
string srcDir;
string password;
string vrf;
##

##template content
copy scp://root@10.127.117.65/$$srcFile$$ bootflash: vrf $$vrf$$ <prompt:'(yes/no)?',
response:'yes'> <prompt:'(y/n)?[n]',
response:'y'> <prompt:'password:',
response:'$$password$$'>
```

### 2. 動的な決定

設定テンプレートは、特殊な内部変数 **LAST\_CMD\_RESPONSE** を提供します。

次に例を示します。

```
##template content
show vlan id $$vlan_id$$
if($$LAST_CMD_RESPONSE$$ contains
    "not found"){
    vlan $$vlan_id$$
}
else{
}
```

### 3. テンプレート参照

この場合、テンプレートは別のテンプレートから参照されます。

派生テンプレート:

```
##template properties
[snip]
imports = baseTemplate1,baseTemplate2;

##
```

テンプレートの詳細については、『Cisco DCNM Classic LAN Configuration Guide, Release 11.3(1)』および『Cisco DCNM LAN Fabric Configuration Guide, Release 11.4(1)』を参照してください。

# クラシック LAN 展開から LAN ファブリック展開へのアップグレード

## 手順

---

- Step 1** すべてのスイッチがアップグレード前に Cisco DCNM から到達可能であることを確認してください。
- (注) ネストされたスイッチグループが DCNM 11.3(1) にあり、テレメトリがそれらで有効になっている場合、アップグレード前にこれらのスイッチグループのテレメトリを無効にする必要があります。
- Step 2** LAN ファブリック展開にアップグレードするためのインラインアップグレード手順に従ってください。
- 詳細については、「[インラインアップグレードを通じた ISO または OVA のアップグレード \(Upgrading ISO or OVA through Inline Upgrade\)](#)」を参照してください。
- Step 3** アップグレード後に、DCNM インストールタイプは自動的に LAN ファブリックに変更され、適切なファブリックインスタンスが作成されます。ファブリックの詳細については、[ファブリックの移行 \(92 ページ\)](#) を参照してください。



## Fabric Builder

Fabric Builder creates a managed and controlled SDN fabric. Select an existing fabric below or define a new *VXLAN* fabric, add switches, set the roles of the switches and deploy settings to devices.

Create Fabric

### Fabrics (5)

Default\_LAN  

Type: External  
Technology: LANClassic

LAB1  

Type: External  
Technology: LANClassic

LAB2  

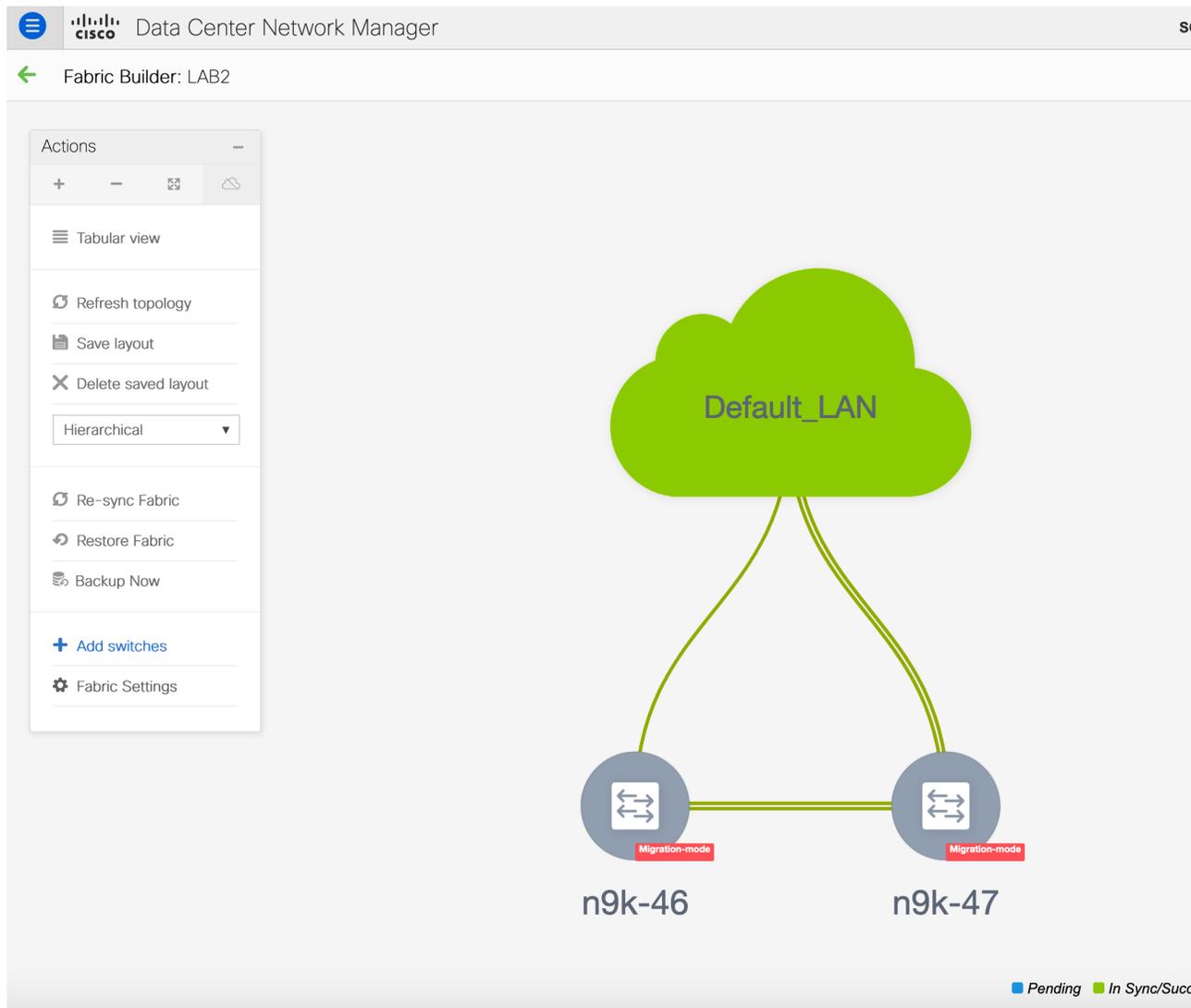
Type: External  
Technology: LANClassic

SJC\_Bldg1  

Type: Multi-Fabric Domain  
Technology: SwitchGroup  
Member Fabrics: LAB1, LAB2

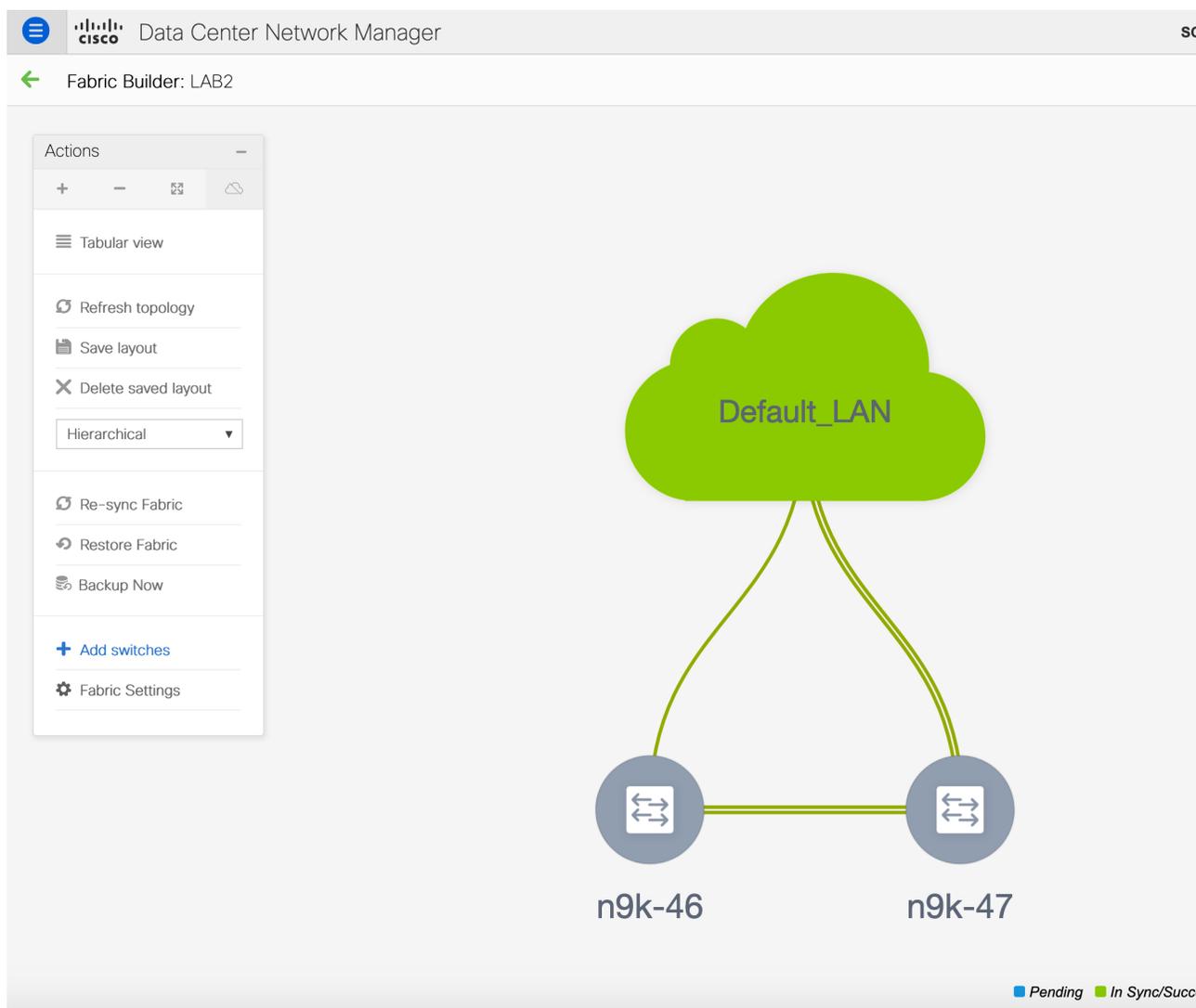
**Step 4** スイッチは **移行モード** になります。各 **LAN\_Classic** ファブリックにナビゲーションして、[保存して展開 (**Save & Deploy**)] をクリックします。

(注) ファブリックはデフォルトで、[**モニタモード (Monitor Mode)**] になっています。このモードのためにエラーメッセージが表示されますが、無視できます。



The screenshot shows the Cisco DCNM Config Deployment interface. At the top, there is a navigation bar with the Cisco logo and the text "Data Center". Below this, the main heading is "Config Deployment". Underneath, it says "Step 1. Configuration Preview". A prominent error message is displayed in a white box with a red 'X' icon: "This Fabric, LAB2 is in read-only mode. No configuration deployments are permitted. Please review Fabric settings." A blue "Close" button is located to the right of the message. Below the message is a table with the following headers: "Switch Name", "IP Address", "Switch Serial", "Preview Config", "Status", and "Re-sync". The table content is empty, with the text "No data available" displayed below the headers. At the bottom of the interface, there is a blue "Deploy Config" button.

Switch Name	IP Address	Switch Serial	Preview Config	Status	Re-sync
No data available					



このステップでは、最小の構成インテントがスイッチに対してキャプチャされることを確認します。スイッチはすべての接続の問題やエラーが解決するまで、[移行モード (Migration Mode)] のままになります。スイッチをこのモードから外すには、その後の[保存して展開 (Save & Deploy)] 操作が必要です。

## LAN クラシック ファブリック テンプレートの機能

LAN\_Classic テンプレートの次の機能は、External\_Fabric\_11\_1 テンプレートと同じサポートを提供します。

サポートされる機能は次のとおりです。

- 設定コンプライアンス

- ファブリック/スイッチのバックアップまたは復元
- ネットワーク インサイト
- パフォーマンス モニタリング
- VMM
- トポロジ ビュー
- Kubernetes の可視化
- RBAC

詳細については、機能固有のセクションを参照してください。





## 第 7 章

# 展開のベスト プラクティス

- [Cisco DCNM およびコンピューティング展開のベストプラクティス \(105 ページ\)](#)

## Cisco DCNM およびコンピューティング展開のベストプラクティス

この章では、クラスタモードおよびクラスタ解除モードで、Cisco DCNM OVA および ISO を展開するためのベストプラクティスについて説明します。次のセクションでは、Cisco DCNM のインストール中の IP アドレスと関連する IP プールの設定に推奨される設計について説明します。

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 に接続 (SSH、SCP、HTTP、HTTPS) を提供します。

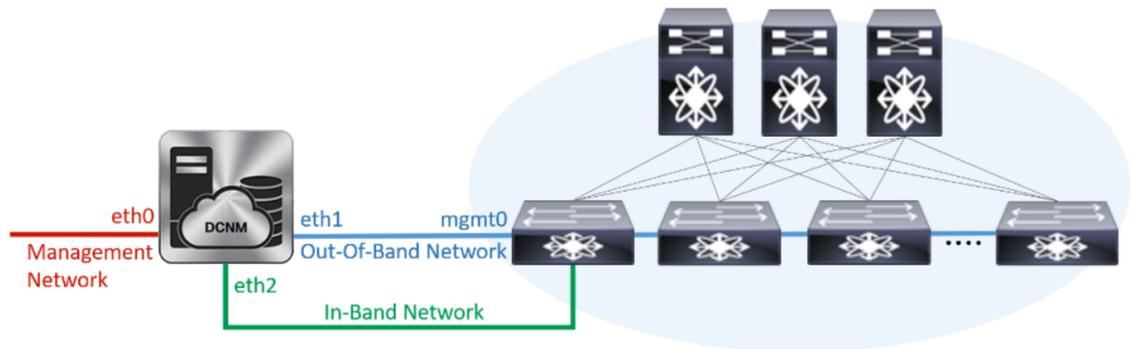
- `enhanced-fabric-mgmt (eth1)` インターフェイス

このネットワークは、アウトオブバンドまたは `mgmt0` インターフェイスを介して、Cisco Nexus スイッチのファブリック管理を強化します。

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

このネットワークは、前面パネルポートを通して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 インターフェイスは、エンドポイント ロケータ (EPL) や Network Insights Resources (NIR) などのアプリケーションに使用されます。

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。



## ベストプラクティスを使用するためのガイドライン

次に、DCNMおよびコンピューティングを展開するためのベストプラクティスを使用する際に注意すべきガイドラインを示します。

- このドキュメントで指定されているIPアドレスは、サンプルアドレスです。セットアップに実稼働ネットワークで使用されているIPアドレスが反映されていることを確認します。
- eth2 インターフェイスサブネットが、eth0 インターフェイスと eth1 インターフェイスに関連付けられているサブネットと異なっていることを確認します。
- eth0 と eth1 の両方のインターフェイスが同じサブネット上にあるため、DHCPは同じIPアドレスを返しますが、2つの応答は同じです。
- Cisco DCNM ネイティブ HA は、アクティブおよびスタンバイアプリケーションとして動作する2つのCisco DCNM アプライアンスで構成されます。アクティブとスタンバイの両方のアプライアンスの組み込みデータベースは、リアルタイムで同期されます。クラスタモードのCisco DCNM およびコンピューティング ノードの eth0、eth1、および eth2 インターフェイスは、レイヤ2 隣接である必要があります。
- Cisco DCNM 展開環境でのクラスタモードの詳細については、使用している展開タイプの『[Cisco DCNM 設定ガイド](#)』の「アプリケーション」の章を参照してください。

## Cisco DCNM で冗長性の展開

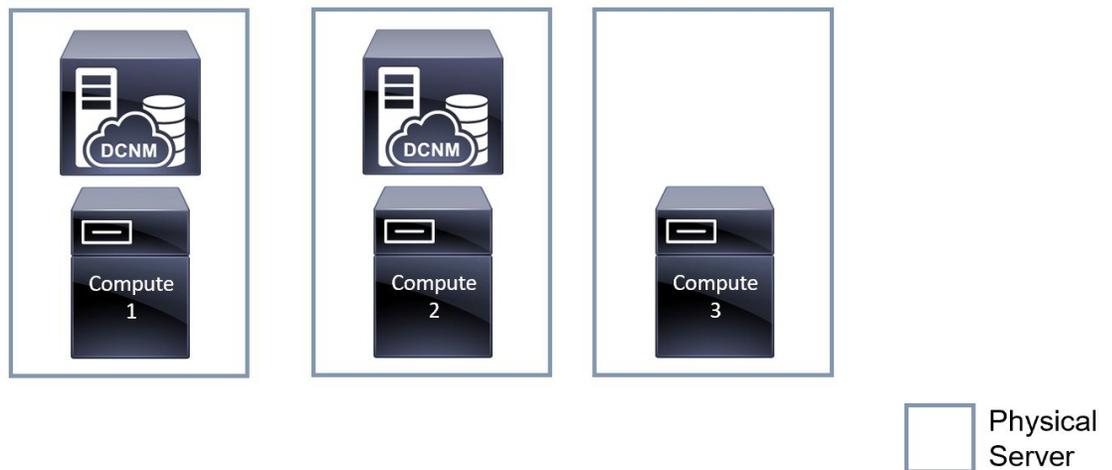
ここでは、DCNM 動作の冗長性のための推奨される展開方法について説明します。一般的な前提として、DCNM とコンピューティング ノードは仮想マシンとしてインストールされます。UCS (ベアメタル) 上の仮想アプライアンスで Cisco DCNM ISO のインストール中に、すべての DCNM とコンピューティングに個別のサーバがあります。

### 展開 1: 最小冗長性設定

Cisco DCNM クラスタモードのインストールで最小限の冗長性を確保するための推奨設定は、次のとおりです。

- サーバ 1 の DCNM アクティブノードとコンピューティング ノード 1
- サーバ 2 の DCNM スタンバイ ノードとコンピューティング ノード 2
- サーバ 3 のコンピューティング ノード 3
- 排他的ディスクに展開されたコンピューティング VM
- 物理サーバのメモリまたは CPU のオーバーサブスクリプションなし

図 9: Cisco DCNM クラスタ モード: 物理サーバから VM へのマッピング

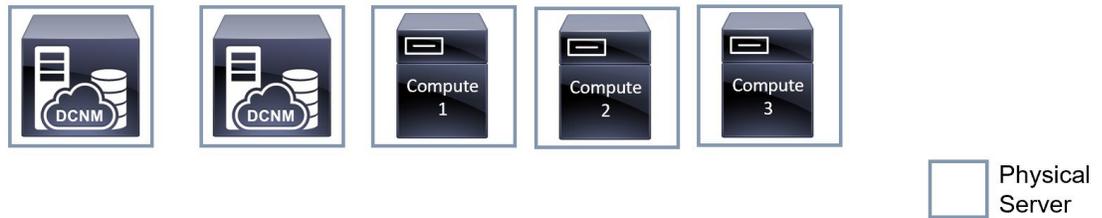


## 展開 2: 冗長性の最大設定

DCNM クラスタモードのインストールで最大限の冗長性を確保するための推奨設定は、次のとおりです。

- サーバ 1 の DCNM アクティブ ノード (アクティブ)
- サーバ 2 の DCNM スタンバイ ノード
- サーバ 3 のコンピューティング ノード 1
- サーバ 4 のコンピューティング ノード 2
- サーバ 5 のコンピューティング ノード 3

図 10: Cisco DCNM クラスタ モード: 物理サーバから VM へのマッピング



## Cisco DCNM での IP アドレスの設定

ここでは、Cisco DCNM およびコンピューティングノードのすべてのインターフェイスの IP アドレス設定に対して、ベストプラクティスと推奨される展開について説明します。

### シナリオ 1: 3つのイーサネットインターフェイスはすべて異なるサブネットにあります

このシナリオでは、異なるサブネット上の DCNM の 3 つのイーサネットインターフェイスすべてを考慮します。

次に例を示します。

- eth0 – 172.28.8.0/24
- eth1 – 10.0.8.0/24
- eth2 – 192.168.8.0/24

可能な展開は次のとおりです。

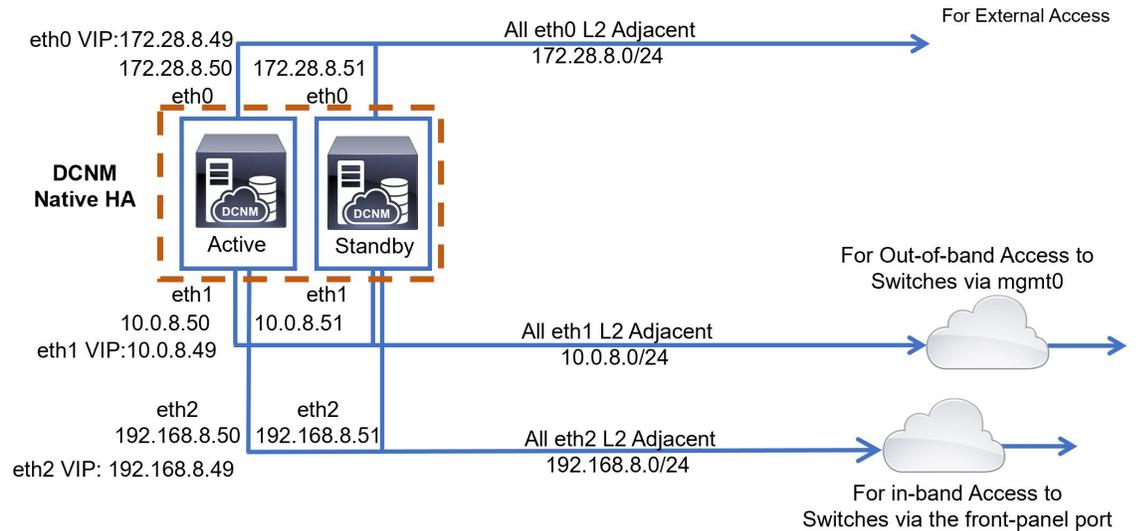
- [Cisco DCNM クラスタ解除モード \(109 ページ\)](#)
- [Cisco DCNM クラスタ モード \(110 ページ\)](#)

### Cisco DCNM クラスタ解除モード

図 11: コンピューティング クラスタを使用しない Cisco DCNM スタンドアロン展開



図 12: コンピューティング クラスタを使用しない Cisco DCNM HA 展開



## Cisco DCNM クラスタ モード

図 13: コンピューティング クラスタを使用した Cisco DCNM スタンドアロン展開

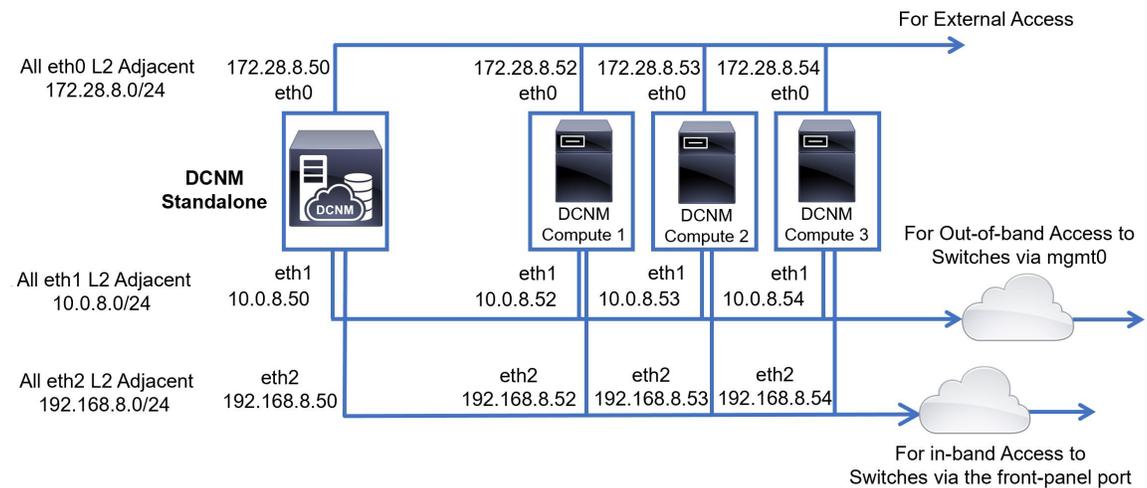
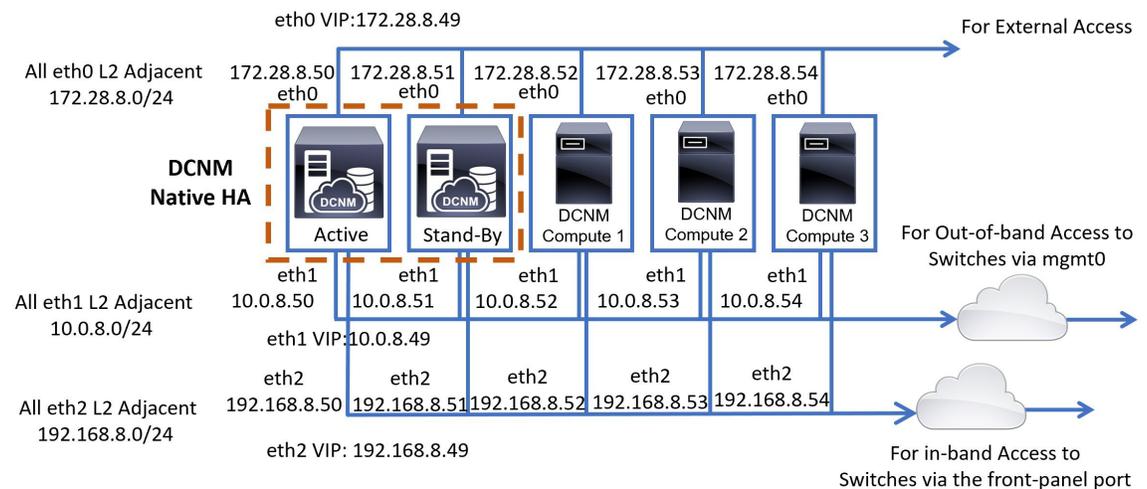


図 14: コンピューティング クラスタを使用した Cisco DCNM HA の展開



## シナリオ 2: 異なるサブネットの eth2 インターフェイス

このシナリオでは、eth0 と eth1 のインターフェイスが同じサブネット内にあり、DCNM とコンピューティングの eth2 インターフェイスが異なるサブネットにあることを考慮してください。

次に例を示します。

- eth0 – 172.28.8.0/24
- eth1 – 172.28.8.0/24
- eth2 – 192.168.8.0/24

可能な展開は次のとおりです。

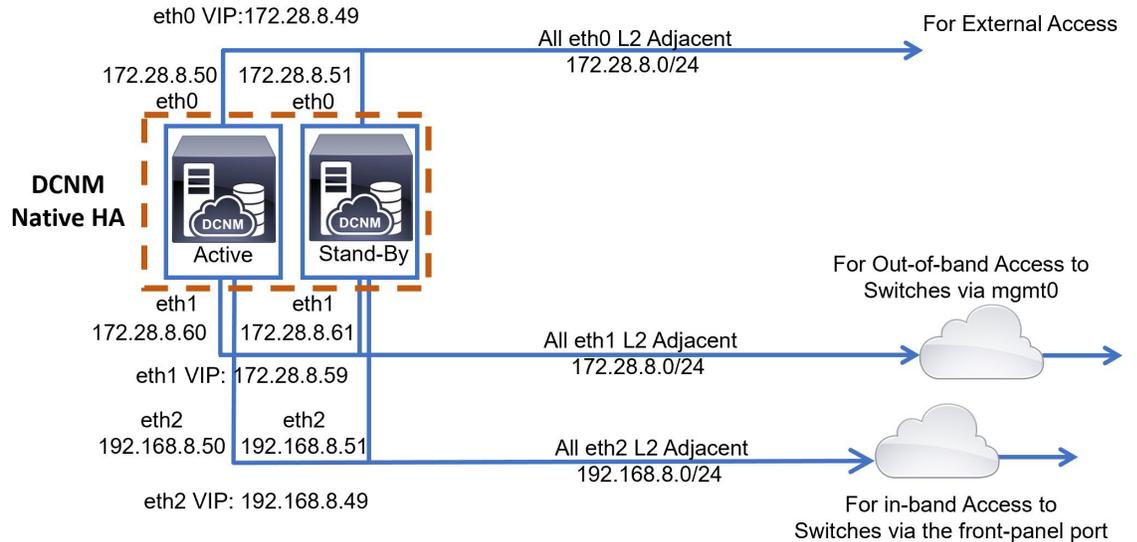
- Cisco DCNM クラスタ解除モード (111 ページ)
- Cisco DCNM クラスタ モード (112 ページ)

**Cisco DCNM クラスタ解除モード**

図 15: コンピューティング クラスタを使用しない Cisco DCNM スタンドアロン展開 (HA なし)



図 16: コンピューティング クラスタを使用しない Cisco DCNM ネイティブ HA 展開



## Cisco DCNM クラスタ モード

図 17: コンピューティング クラスタを使用した Cisco DCNM スタンドアロン展開

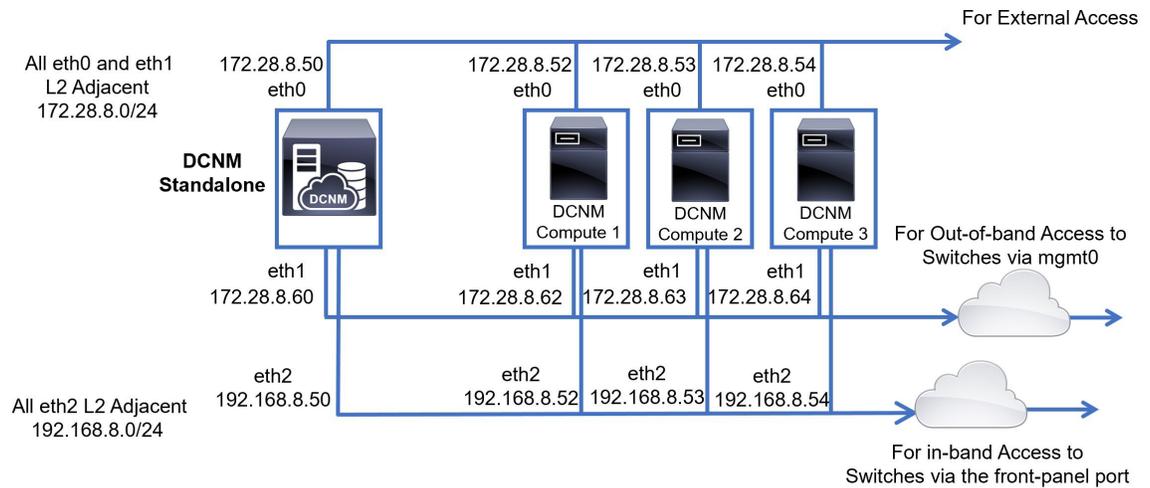
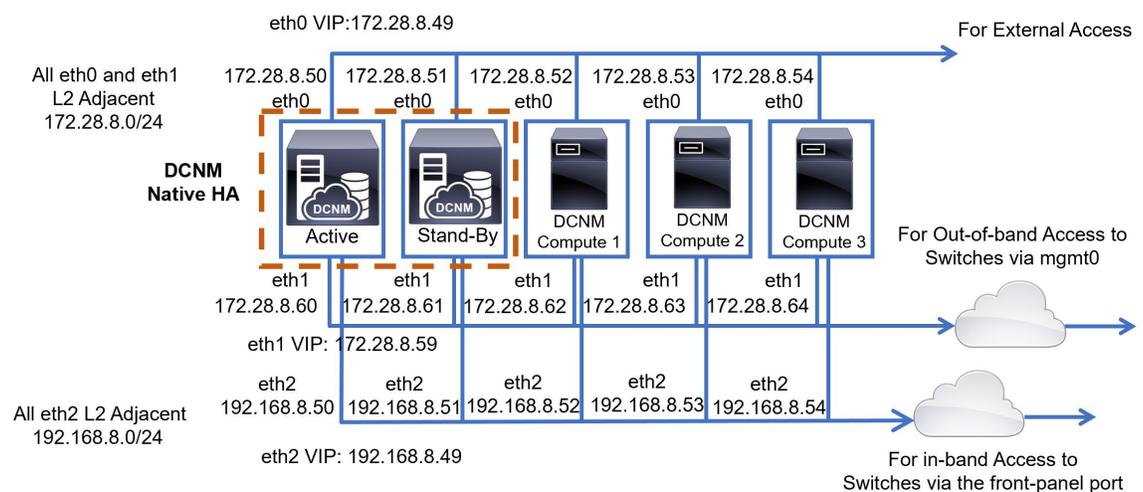


図 18: コンピューティング クラスタを使用した Cisco DCNM ネイティブ HA 展開



## Cisco DCNM およびコンピューティングノードの物理接続

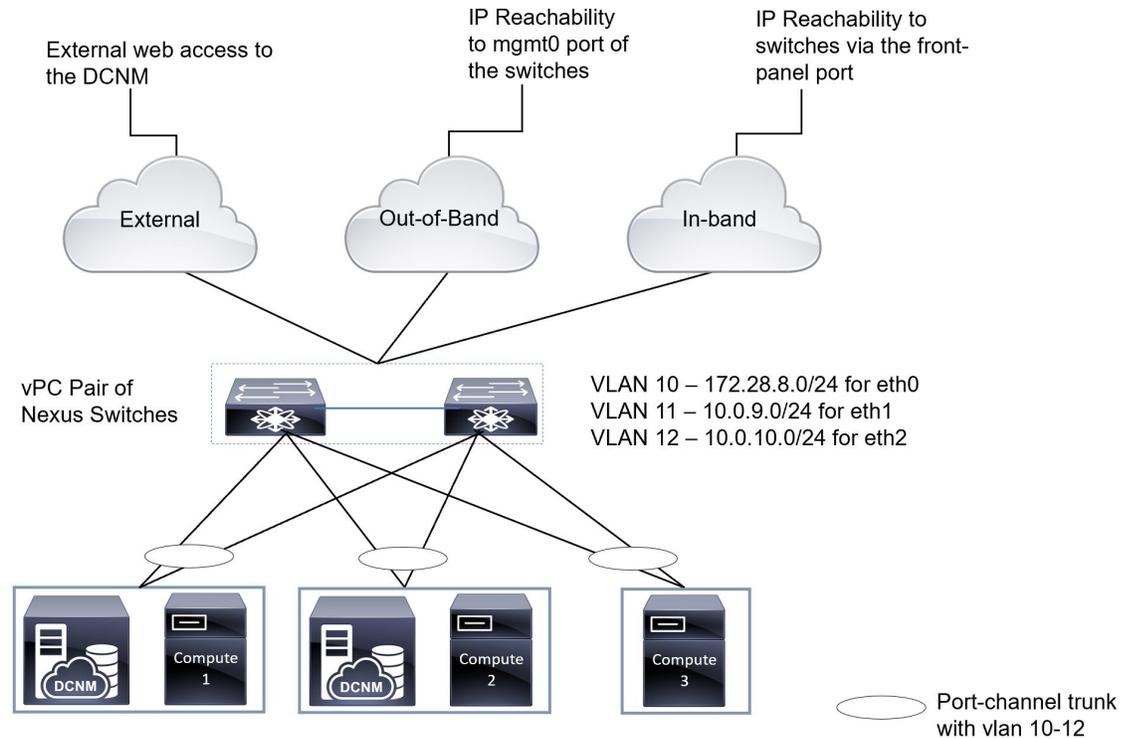
ここでは、仮想マシンとベアメタルインストールの両方での Cisco DCNM およびコンピューティングノードの物理的な接続について説明します。

## 仮想マシン

次の図は、3つのサーバ冗長性設定でサポートされている DCNM およびコンピューティングノードの物理的な接続を示しています。物理サーバは、ポートチャネルを介してスイッチの vPC ペアに接続されている必要があります。これにより、単一のリンクに障害が発生したり、単一のスイッ

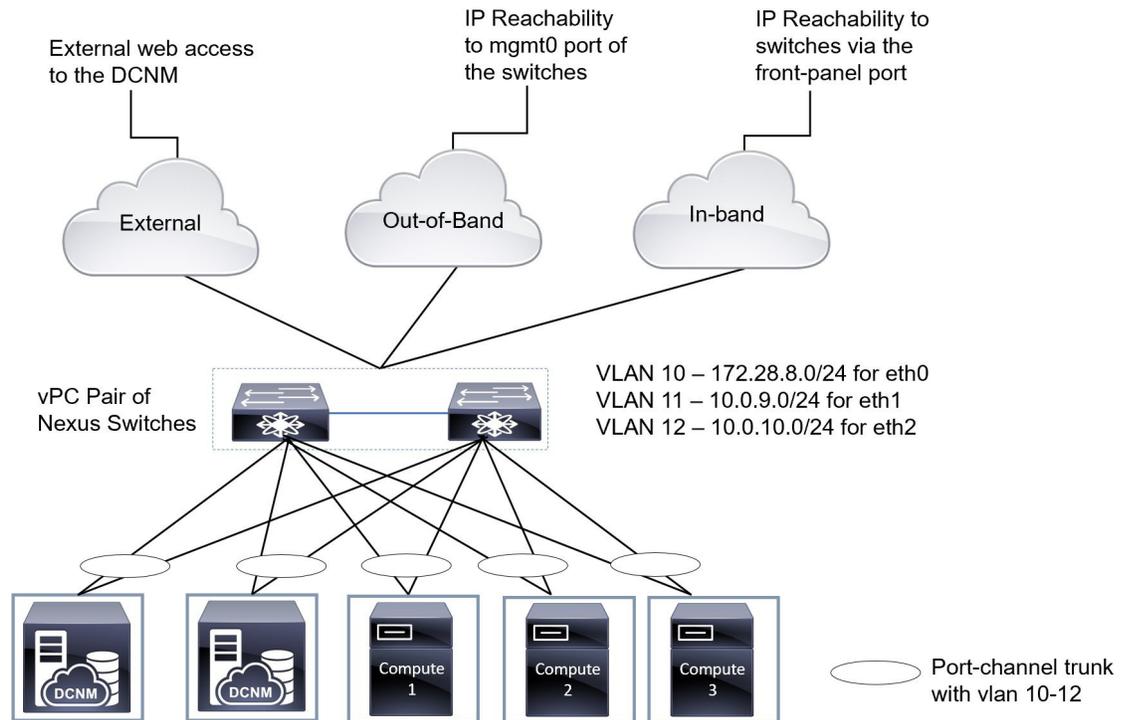
チで障害が発生したりすると、適切な耐障害性が得られます。スイッチの vPC ペアは、物理サーバへの管理接続を提供するインフラ vPC ペアと見なされます。

図 19: 3 台のサーバを使用した *Cisco DCNM VM* の物理接続



次の図は、5つのサーバ冗長性設定での VM インストールでサポートされている Cisco DCNM と、コンピューティングノードの物理的な接続を示しています。

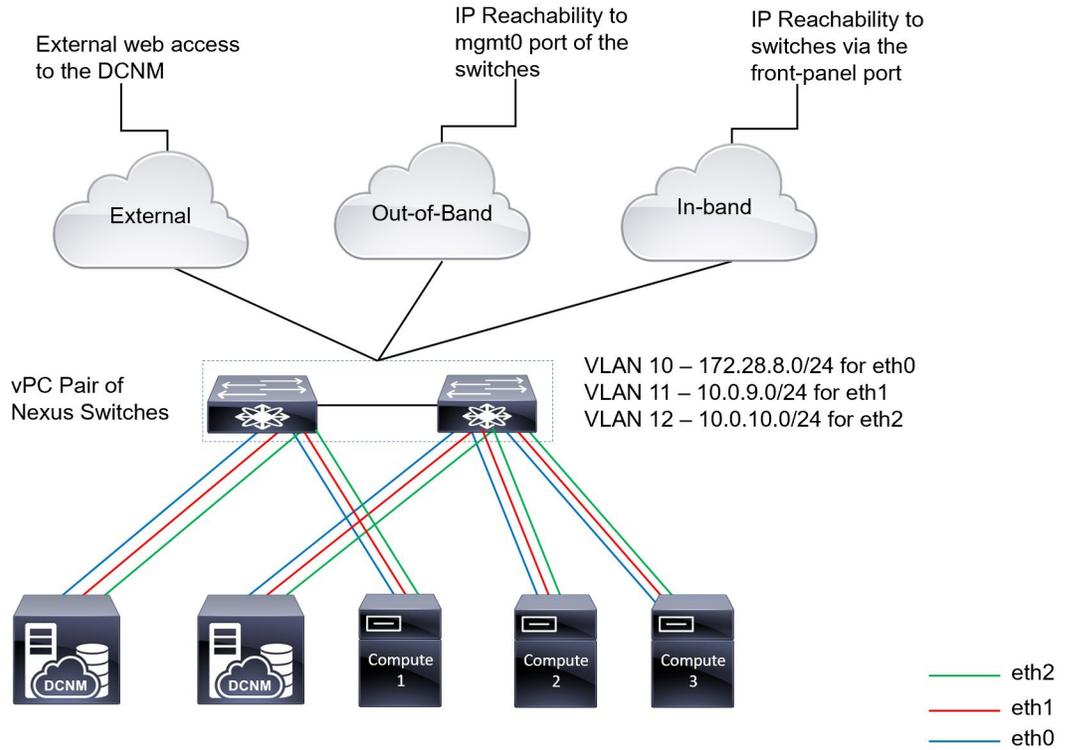
図 20:5 台のサーバを使用した Cisco DCNM VM の物理接続



### ベア メタルのインストール

ベア メタルで Cisco DCNM をインストールするには、5 台のサーバが必要です。次の図は、Cisco DCNM およびコンピューティングノードの物理的な接続を示しています。各サーバには、それぞれ eth0、eth1、および eth2 インターフェイスにマッピングされる 3 つの物理インターフェイスがあることに注意してください。物理サーバが Cisco UCS VIC 1455 仮想インターフェイスカードなどの管理対象ネットワーク アダプタで構成されている場合は、仮想マシンと同様に、サーバからスイッチへのポート チャネル接続を確立できます。

図 21: Cisco DCNM とコンピューティング ベア メタルの物理接続







## 第 8 章

# ディザスタ リカバリ (バックアップおよび復元)

この章は、次の項で構成されています。

- [スタンドアロン DCNM セットアップでの Cisco DCNM およびアプリケーションデータのバックアップおよび復元, on page 117](#)
- [ネイティブ HA セットアップでの Cisco DCNM およびアプリケーションデータのバックアップおよび復元, on page 119](#)
- [Cisco DCNM シングル HA ノードのリカバリ \(120 ページ\)](#)
- [管理者アカウントの回復 \(123 ページ\)](#)
- [SRM を使用した HA の災害回避 \(124 ページ\)](#)

## スタンドアロン DCNM セットアップでの Cisco DCNM およびアプリケーションデータのバックアップおよび復元

分析およびトラブルシューティングのために、Cisco DCNM アプリケーションデータのバックアップを作成できます。



**Note** リリース11.3(1)では、sysadmin と root ユーザーのパスワードは同一ではありません。にアップグレードすると、sysadmin および root ユーザーのパスワードは保持されます。

ただし、アップグレード後にCisco DCNMでバックアップと復元を実行すると、sysadmin ユーザーは root ユーザーからパスワードを継承するため、両方のユーザーが同じパスワードを持ちます。復元が完了したら、両方のユーザーのパスワードを変更できます。

Cisco DCNM およびアプリケーションデータのバックアップを作成するには、次の作業を実行します。

## Procedure

---

- Step 1** SSH を使用して Cisco DCNM アプライアンスにログインします。
- Step 2** **appmgr backup** コマンドを使用してアプリケーション データのバックアップを取得します。
- ```
dcnm# appmgr backup
```
- リリース 11.4(1) 以降、Cisco DCNM では、バックアップをリモート scp サーバに保存できる cron ジョブを設定できます。スケジュールバックアップを設定するために、**appmgr backup schedule** コマンドを使用します。
- ```
dcnm# appmgr backup schedule [day] <hh<hh>:<mm>
[destination <user>@<host>:<dir>]]
```
- バックアップ ファイルを安全な場所にコピーし、DCNM アプライアンスをシャットダウンします。
- Step 3** インストールされている VM を右クリックし、**[電源 (Power)] > [電源オフ (Power Off)]** を選択します。
- Step 4** 新しい DCNM アプライアンスを展開します。
- Step 5** VM の電源がオンになったら、**[コンソール (Console)]** タブをクリックします。
- DCNM アプライアンスが設定されていることを示すメッセージが画面に表示されます。
- 復元プロセスを続行するには、ブラウザに URL をコピーして貼り付けます。
- Step 6** DCNM Web インストーラ UI で、**[開始 (Get Started)]** をクリックします。
- Step 7** Cisco DCNM インストーラの画面で、オプション ボタンを選択します。
- [Step 2, on page 118](#) で生成されたバックアップ ファイルを選択します。
- DCNM の展開を続行します。
- Step 8** **[概要 (Summary)]** タブで、設定の詳細を確認します。
- 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 仮想アプライアンス 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。
- Step 9** データが復元されたら、**appmgr status all** コマンドを使用してステータスを確認します。
-

# ネイティブ HA セットアップでの Cisco DCNM およびアプリケーション データのバックアップおよび復元

分析およびトラブルシューティングのために、Cisco DCNM アプリケーション データのバックアップを作成できます。



**Note** リリース11.3(1) では、sysadmin と root ユーザーのパスワードは同一ではありません。にアップグレードすると、sysadmin および root ユーザーのパスワードは保持されます。

ただし、アップグレード後にCisco DCNMでバックアップと復元を実行すると、sysadmin ユーザーは root ユーザーからパスワードを継承するため、両方のユーザーが同じパスワードを持ちます。復元が完了したら、両方のユーザーのパスワードを変更できます。

ネイティブ HA セットアップでデータのバックアップと復元を実行するには、次の作業を実行します。

## Before you begin

アクティブ ノードが動作しており、機能していることを確認します。

## Procedure

- Step 1** アクティブ ノードが動作しているかどうかを確認します。それ以外の場合は、フェールオーバーをトリガします。
- Step 2** SSH を使用して Cisco DCNM アプライアンスにログインします。
- Step 3** アクティブおよびスタンバイの両方のアプライアンスで **appmgr backup** コマンドを使用して、アプリケーション データのバックアップを取得します。
- ```
dcnm1# appmgr backup
dcnm2 appmgr backup
```
- リリース11.4(1) 以降、Cisco DCNM では、バックアップをリモート scp サーバに保存できる cron ジョブを設定できます。スケジュールバックアップを設定するために、**appmgr backup schedule** コマンドを使用します。
- ```
dcnm# appmgr backup schedule [day] <hh<hh>:<mm>
[destination <user>@<host>:[<dir>]]
```
- アクティブおよびスタンバイの両方のアプライアンスのバックアップ ファイルを安全な場所にコピーし、DCNM アプライアンスをシャットダウンします。
- Step 4** インストールされている VM を右クリックし、[電源 (Power)] > [電源オフ (Power Off)] を選択します。
- Step 5** 新しい DCNM アプライアンスをネイティブ HA モードで展開します。

- Step 6** アクティブおよびスタンバイアプライアンスの両方で、VMの電源をオンにした後、[**コンソール (Console)**] タブをクリックします。
- DCNM アプライアンスが設定されていることを示すメッセージが画面に表示されます。
- 復元プロセスを続行するには、ブラウザに URL をコピーして貼り付けます。
- Step 7** DCNM Web インストーラ UI で、[**開始 (Get Started)**] をクリックします。
- Step 8** Cisco DCNM インストーラの画面で、オプション ボタンを選択します。
- ステップ [Step 3, on page 119](#) で生成されたバックアップ ファイルを選択します。
- パラメータの値は、バックアップ ファイルから読み取られ、自動入力されます。必要に応じて値を変更します。
- DCNM の展開を続行します。
- Step 9** [概要 (Summary)] タブで、設定の詳細を確認します。
- 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 仮想アプライアンス 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。
- Step 10** データが復元されたら、`apmr status all` コマンドを使用してステータスを確認します。
- 

## Cisco DCNM シングル HA ノードのリカバリ

ここでは、シナリオについて詳しく説明し、Cisco DCNM シングル HA ノードをリカバリする手順について説明します。

次の表では、Cisco DCNM ネイティブ HA セットアップで、1 つまたは両方のノードで障害が発生した場合のすべてのリカバリ手順について詳しく説明します。

障害のタイプ	回復するノード/データベース	使用可能なプライマリバックアップ	セカンダリバックアップが使用可能	リカバリ手順
プライマリ ノードが失われました。 セカンダリ ノードがプライマリになりました (フェールオーバーのため)。	プライマリ ノード	—	—	<ol style="list-style-type: none"> <li>1. セカンダリ ノードをプライマリ ノードに変換します。</li> <li>2. 新しいセカンダリ ノードの設定</li> </ol>
プライマリおよびセカンダリサーバデータベースが失われます。セカンダリ ノードがプライマリになりました (フェールオーバーのため)	プライマリ データベース	—	—	アクティブなセカンダリノードが再起動し、スタンバイプライマリノードと同期します。
アクティブなセカンダリ ノードが失われました。フェールオーバーが原因でプライマリ ノードがアクティブになっています。	セカンダリ ノード	—	×	新しいセカンダリ ノードの設定
アクティブなセカンダリ ノードが失われました。フェールオーバーが原因でプライマリ ノードがアクティブになっていません。	セカンダリ ノード	—	対応	Web インストーラを使用して、新しいセカンダリ ノードを設定します。[復元用のバックアップ ファイルを含む新規インストール (Fresh installation with backup file for restore)] を選択します。HA 設定画面で、[セカンダリ DCNM ノードのみを復元する (Restore secondary DCNM node only)] を選択します。
セカンダリ スタンバイ ノードが失われます。	セカンダリ ノード	—	×	新しいセカンダリ ノードの設定

障害のタイプ	回復するノード/データベース	使用可能なプライマリバックアップ	セカンダリバックアップが使用可能	リカバリ手順
セカンダリスタンバイノードが失われます	セカンダリノード	—	対応	Web インストーラを使用して、新しいセカンダリノードを設定します。[復元用のバックアップファイルを含む新規インストール (Fresh installation with backup file for restore)] を選択します。HA 設定画面で、[セカンダリ DCNM ノードのみを復元する (Restore secondary DCNM node only)] を選択します。
プライマリノードがアクティブです。セカンダリスタンバイデータベースが失われました。	セカンダリデータベース	—	—	プライマリノードは、セカンダリノードと同期するために再起動します。

### セカンダリノードからプライマリノードへの変換

セカンダリノードをプライマリノードに変換するには、次の手順を実行します。

1. セカンダリノードで SSH を使用して DCNM サーバにログインします。
2. `appmgr stop all` コマンドを使用して、セカンダリノード上のすべてのアプリケーションを停止します。
3. `ha-setup.properties` ファイルに移動します。
4. セカンダリノードをプライマリノードとして設定するには、ノード ID を 1 に設定します。

```
NODE_ID 1
```

セカンダリノードのノード ID を 1 に変更した後、サーバを再起動します。古いセカンダリが新しいプライマリノードとして再起動します。失われたプライマリをセカンダリノードとして試し、新しいセカンダリノードを設定します。

### でのセカンダリノードの設定

セカンダリノードをから設定するには、次の手順を実行します。

1. スタンドアロン Cisco DCNM をインストールします。失われたセカンダリノードと同じ設定を使用します。



- (注) プライマリ ノードが失われ、古いセカンダリ ノードがプライマリ ノードに変換された場合は、失われたプライマリ設定で新しいスタンドアロン ノードを設定します。
- SSH を使用して新しい DCNM スタンドアロン サーバにログインし、**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 root-access permit** を使用して、新しいノードの **/root** ディレクトリへのアクセスを提供します。
  - SSH を使用してプライマリ ノードにログオンし、**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 root-access permit** を使用して、プライマリ ノードの **/root** ディレクトリへのアクセスを提供します。
  - プライマリ ノードで、**/root/.DO\_NOT\_DELETE** ファイルを編集します。プライマリ ノードで **NATIVE\_HA\_STATUS** パラメータを **NOT\_TRIGGERED** に設定します。
  - appmgr setup native-ha active** コマンドを使用して、プライマリ ノードをアクティブとして設定します。
  - appmgr setup native-ha secondary** コマンドを使用して、セカンダリ ノードをスタンバイとして設定します。

## 管理者アカウントの回復

network-admin ユーザ/パスワード クレデンシャルを持っている場合は、Cisco DCNM Web UI から他のユーザのログインとパスワードの回復ができます。Step 5 (124 ページ) を参照してください。

Cisco DCNM Web UI ユーザーまたはパスワードを回復するには、次の手順を実行します。

### 始める前に

パスワードを変更する権限があることを確認します。

### 手順

**Step 1** SSH を起動し、**/root** ユーザとして DCNM サーバにログインします。

```
[root@dcnm]#
```

**Step 2** **/usr/local/cisco/dcm/fm/bin** フォルダに移動します。

```
[root@dcnm]# cd /usr/local/cisco/dcm/fm/bin  
[root@dcnm bin]#
```

**Step 3** `addUser.sh` スクリプトを実行して、新しいネットワーク管理者ユーザを作成します。新しいユーザ名、パスワード、データベースパスワードを指定します。

```
[root@dcnm bin]# ./addUser.sh <user> <password> <dbpassword>
```

次のメッセージが生成され、新しいユーザが作成されます。

```
----- OUTPUT -----
----insertUser-----
----username-----john123
----role-----network-admin
----insertUser-----done...
      Added user : john123 successful!
----- END -----
```

**Step 4** 新しいユーザで Cisco DCNM Web UI にログインします。

**Step 5** [管理 (Administration)] > [管理ユーザー (Management Users)] > [ローカル (Local)] を選択します。

新しいユーザがリストに表示されます。

**Step 6** パスワードを回復するユーザを選択し、[編集 (Edit)] アイコンをクリックします。

**Step 7** [ユーザの編集 (Edit User)] ウィンドウで、ユーザのロールとパスワードを変更します。

180 日後に期限切れになるようにパスワードを設定することもできます。

**Step 8** [Apply] をクリックして変更内容を保存します。

## SRM を使用した HA の災害回避

Cisco DCNM リリース 11.5(1) は、VM Site Recovery Manager (SRM) に正常に導入できます。SRM は、フェールオーバーとフェールバックの自動オーケストレーションを提供するダウンタイムを最小限に抑えるディザスタ リカバリ ソフトウェアです。



(注) このドキュメントでは、高度なワークフローについて説明します。詳細については、<https://docs.vmware.com/en/Site-Recovery-Manager/index.html> を参照してください。

DCNM を設定して SRM に移行するには、次のタスクを実行します。

1. サイト 1 で実行されている vCenter、SRM、VM レプリケータ マネージャを実行する管理サーバ (ESXi 6.7) を設定します。
2. 同様に、サイト 2 で実行する vCenter、SRM、VM レプリケータ マネージャを実行する管理サーバ (ESXi 6.7) を設定します。

VRM は、あるサイトから別のサイトに VM を複製するのに役立ちます。



(注) すべての VM を同じサイトにまとめて展開する必要があります。DCNM VM を移行する場合（計画的リカバリまたはディザスタ リカバリ）、すべての DCNM VM をリカバリ サイトに移行する必要があります。

3. 同期する Site1 を Site2 に複製します。
4. Site1 および Site2 を Site Recovery Manager に移行します。
5. リカバリ サイトに VM を展開します。

互換性:

- ESXi 6.7
- SRM 8.3

DCNM HA ディザスタ リカバリ用に SRM を設定するには、次のタスクを実行します。

1. SRM を起動します。
2. Site1 と Site2 をペアリングします。レプリケーションが完了すると、両方のサイトが同期されます。
3. [詳細の表示 (View Details)] をクリックします。  
[概要 (Summary)] ページが開きます。
4. [概要 (Summary)] タブで、
  1. [ネットワーク マッピング (Network Mappings)] をクリックし、Site1 と Site2 の両方で VM が使用するネットワークをマッピングします。
  2. [フォルダ マッピング (Folder Mappings)] をクリックします。vCenter が VM に使用するすべてのフォルダをマッピングします。
  3. [リソースマッピング (Resource Mappings)] をクリックします。Site1 の各コンポーネントのリソースを Site2 のコンポーネントにマッピングします。[リバースマッピング (Reverse Mapping)] で [Yes] を選択します。
  4. [プレースホルダ データストア (Placeholder Datastores)] をクリックします。ホスト/クラスタを正しいデータストアにマッピングします。たとえば、ホスト/クラスタ内の VM は、マッピングされたデータストアに複製されます。



(注) VM が正しいデータストアに複製されていることを確認します。そうでない場合、リカバリ プランは失敗します。

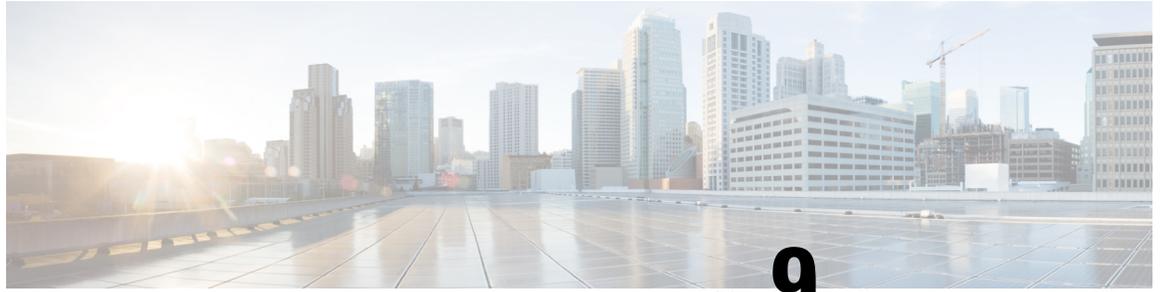
5. [レプリケーション (Replications)] タブでは、

1. vSphere Replication を使用して、ソースサイトからターゲットサイトに VM を複製します。
  2. 左側のペインで、[Outgoing] をクリックします。site2 と同期されたすべてのデータが表示されます。
  3. Site1 にあり、Site2 にすべてのレプリケーションがある場合、このタブは空になります。
  4. 左側のペインで、[Incoming] をクリックします。Site2 と同期しているすべての VM のステータスが表示されます。
  5. 許容できる最大データ損失を決定するために、レプリケーションの設定時にリカバリ ポイント目標 (RPO) 値を設定します。
  6. [新規 (New)] をクリックして、レプリケーションレイテンシを設定し、目標リカバリ ポイントを設定します。VM の前にある矢印をクリックして、VM の設定データを表示します。
6. [保護グループ (Protection Groups)] タブ:
- 1 つのリカバリ プランは 1 つ以上の保護グループに適用されます。リカバリ プランは、Site Recovery Manager に含まれる保護グループ内の仮想マシンをリカバリする方法を指定します。
7. [リカバリ プラン (Recovery Plans)] タブで、
- 保護サイトとリカバリサイトで Site Recovery Manager を設定した後、リカバリ プランを作成、テスト、および実行できます。
1. リカバリ プランを作成または変更する場合は、計画された移行またはディザスタ リカバリに使用する前に、それをテストしてください。
  2. 保護されたサイトからリカバリサイトに仮想マシンを移行するために、計画された状況でリカバリプランを実行できます。保護されたサイトで予期しないイベントが発生し、データが失われる可能性がある場合は、計画外の状況でリカバリプランを実行することもできます。
  3. リカバリ プランを作成、テスト、および実行することで、リカバリ中の Site Recovery Manager のアクションをカスタマイズできます。
  4. このプランをリカバリ モードで実行すると、保護サイトで VM のシャットダウンが試行され、リカバリサイトで VM のリカバリが試行されます。
  5. 次のいずれかのリカバリ タイプを選択できます。
    - **計画的移行:** 最近の変更をリカバリサイトに複製し、エラーが発生した場合はリカバ리를キャンセルします。計画的移行中は、リソース集中的な操作を実行しないでください。
    - **ディザスタ リカバリ:** 最新の変更をリカバリサイトに複製しようとしませんが、それ以外は最新のストレージ同期データを使用します。エラーが発生した場合でも、リカバ리를続行します。

6. [実行 (Run)] の後ろの [...] をクリックし、[再保護 (Reprotect)] をクリックして VM を保護するか、[キャンセル (Cancel)] をクリックしてリカバリ プランを停止します。

Site Recovery Manager がリカバリを実行すると、仮想マシンがリカバリ サイトで起動します。保護されたサイトがオンラインに戻ったときに **reprotect** を実行すると、レプリケーションの方向が逆になり、リカバリサイトのリカバリされた仮想マシンが元の保護されたサイトに保護されます。





## 第 9 章

# 証明書

- [の証明書管理 \(129 ページ\)](#)

## の証明書管理



(注) このセクションでは、DCNM OVA/ISO の展開にのみ適用されます。

リリース 11.2(1) 以降、Cisco DCNM では新しい方法と新しい CLI で、システム上で証明書のインストール、アップグレード後の復元、検証が可能です。アクティブノードからスタンバイノードに証明書をエクスポートして、ネイティブ HA セットアップの両方のピアに同じ証明書があることを確認できます。

Cisco DCNM ネイティブ HA セットアップでは、アクティブノードに CA 証明書をインストールし、サービスを開始すると、証明書はスタンバイノードと自動的に同期されます。アクティブノードとスタンバイノードの両方で同じ内部証明書が必要な場合は、アクティブノードからスタンバイノードに証明書をエクスポートする必要があります。これにより、Cisco ネイティブ HA セットアップの両方のピアの証明書が同じになります。



(注) リリース 11.3(1) 以降では、証明書の管理に **sysadmin** ロールを使用する必要があります。

Cisco DCNM は、次の 2 つの証明書を保存します。

- 自己署名証明書 (Cisco DCNM サーバとさまざまなアプリケーション間の内部通信用)
- Web UI などの外部世界と通信するための CA (認証局) 署名付き証明書。



(注) CA 署名付き証明書をインストールするまで、Cisco DCNM は外部ネットワークと通信するため自己署名証明書を保持します。

## 証明書管理のベストプラクティス

Cisco DCNM での証明書管理のガイドラインとベストプラクティスを次に示します。

- Cisco DCNM は、証明書を表示、インストール、復元、およびエクスポートまたはインポートするための CLI ベースのユーティリティを提供します。これらの CLI は SSH コンソールから使用でき、**sysadmin** ユーザーのみがこれらのタスクを実行できます。
- Cisco DCNM をインストールするとき、デフォルトで自己署名付き証明書がインストールされています。この証明書は、外部との通信に使用されます。Cisco DCNM のインストール後に、CA 署名付き証明書をシステムにインストールする必要があります。
- Cisco DCNM ネイティブ HA セットアップでは、DCNM アクティブ ノードに CA 署名付き証明書をインストールすることを推奨します。CA 署名付き証明書は、自動的にスタンバイノードと同期されます。ただし、アクティブノードとスタンバイノードの両方で同じ内部および CA 署名付き証明書を保持する場合は、アクティブノードから証明書をエクスポートして、スタンバイノードにインポートする必要があります。アクティブノードとスタンバイノードの両方に同じ証明書セットがあります。



(注) コンピューティング ノードは内部的に管理された証明書を使用するため、クラスタ展開のコンピューティングノードには何のアクションも必要ありません。

- CN (共通名) を使用して Cisco DCNM で CSR を生成します。CN として VIP FQDN (仮想 IP アドレス FQDN) を指定して、CA 署名付き証明書をインストールします。FQDN は、Cisco DCNM Web UI にアクセスするために使用される管理サブネット VIP (eth0 の VIP) インターフェイスの完全修飾ドメイン名です。
- Cisco DCNM をアップグレードする前に CA 署名付き証明書がインストールされている場合は、Cisco DCNM をアップグレードした後に、CA 署名付き証明書を復元する必要があります。



(注) インラインアップグレードまたはバックアップと復元を実行する場合は、証明書のバックアップを取得する必要はありません。

## インストールされた証明書の表示

次のコマンドを使用して、インストールされた証明書の詳細を表示できます。

**appmgr afw show-cert-details**

**appmgr afw show-cert-details** コマンドの次のサンプル出力では、**CERTIFICATE 1** は外部ネットワークおよび Web ブラウザに提供されている証明書を示します。**CEERTIFICATE 2** は内部で使用されている証明書を示します。

```

dcnm# appmgr afw show-cert-details

****CERTIFICATE 1****
[Certificate available to web gateway. This certificate is offered to webclients]:
-----Web gateway certificate-----
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 4202 (0x106a)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=IN, ST=KA, L=BGL, O=xyz, OU=ABC, CN=<FQDN/IP>
    Validity
      Not Before: Jun  4 13:55:25 2019 GMT
      Not After : Jun  3 13:55:25 2020 GMT
    Subject: C=IN, ST=KA9, L=BGL9, O=XYZ123, OU=ABC123, CN=<FQDN/IP>
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:bb:52:1e:7f:24:d7:2e:24:62:5a:83:cc:e4:88:
-----Certificate output is truncated to first 15 lines-----

****CERTIFICATE 2****
[Certificate available in keystore(jks). CA signed certificate is installed here till DCNM
version 11.1.x]
If you have upgraded from DCNM version 11.1.x to later version please see installation guide
to restore
CA signed certificate to upgraded version.
-----Keystore certificate-----
alias = sme, storepass = <<storepass-pwd>>
Alias name: sme
Creation date: Oct 14, 2018
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
Owner: CN=localhost, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Issuer: CN=dcnmca, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Serial number: 62044620
Valid from: Sun Oct 14 20:39:39 PDT 2018 until: Fri Oct 13 20:39:39 PDT 2023
Certificate fingerprints:
  MD5:  E5:F8:AD:17:4D:43:2A:C9:EE:35:5F:BE:D8:22:7D:9C
  SHA1: 38:66:F1:CD:10:61:27:E7:43:85:10:41:3D:A3:4B:5C:C9:CC:17:5E
  SHA256:
E0:87:D8:34:71:18:FE:8C:AB:18:0B:D7:85:B1:91:A8:4B:75:A3:91:BA:90:83:46:72:87:FE:FE:FE:04:F0:E1
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
-----Certificate output is truncated to first 15 lines-----
dcnm#

```



- (注) <<storepass-pwd>> は、DCNM サーバのインストール時に生成されるパスワード文字列です。この文字列は <install dir>/dcn/fm/conf/serverstore.properties ディレクトリにあります。storepass-pwd の dcnm.fmserver.token 値を取得します。

インストール後、Web UI は **CERTIFICATE 1** を参照します。**CERTIFICATE 1** が利用できない場合、次の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再起動する必要があります。



- (注) Cisco DCNM で同じ一連のコマンドに従い、このシナリオをトラブルシューティングするようにしてください。

Cisco DCNM スタンドアロン アプライアンスで、次のコマンドを実行して、すべてのアプリケーションを停止および開始し、**CERTIFICATE 1** をトラブルシューティングします。

```
dcnm# appmgr stop all /* stop all the applications running on Cisco DCNM */
dcnm# appmgr start all /* start all the applications running on Cisco DCNM */
```

Cisco DCNM ネイティブ HA アプライアンスで、次のコマンドを実行して、すべてのアプリケーションを停止および開始し、**CERTIFICATE 1** をトラブルシューティングします。

例えば、**dcnm1** でアクティブ ノードを示し、**dcnm2** でスタンバイ ノードを示します。

両方のノードで実行しているアプリケーションを停止します。

```
dcnm2# appmgr stop all /* stop all the applications running on Cisco DCNM Standby Node */
dcnm1# appmgr stop all /* stop all the applications running on Cisco DCNM Active Node */
```

両方のノードでアプリケーションを開始します。

```
dcnm1# appmgr start all /* start all the applications running on Cisco DCNM Active Node*/
dcnm2# appmgr start all /* start all the applications running on Cisco DCNM Standby Node*/
```



- (注) 管理 IP アドレスを使用して、Cisco DCNM Web UI を起動する前にブラウザ キャッシュを消去します。

**CERTIFICATE 1** は、ブラウザのセキュリティ設定に表示されます。

## CA 署名付き証明書のインストール

標準のセキュリティ慣行として CA 署名付き証明書をインストールすることをお勧めします。CA 署名付き証明書が認識され、ブラウザによって検証されます。CA 署名付き証明書を手動で検証することもできます。



- (注) 認証局は、企業の署名機関でもかまいません。

### Cisco DCNM スタンドアロン セットアップで CA 署名済み証明書をインストールする

Cisco DCNM に CA 署名付き証明書をインストールするには、次の手順を実行します。

#### Procedure

- Step 1** SSH 端末を経由して DCNM サーバにログオンします。

**Step 2** `appmgr afw gen-csr` コマンドを使用して、Cisco DCNM サーバで CSR を生成します。

**Note** CSR は Cisco DCNM に固有のものであり、対応する CSR 署名付き証明書のみが所定の Cisco DCNM にインストールされている必要があります。

```
dcnm# appmgr afw gen-csr
Generating CSR...
..
...
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:CA
Locality Name (eg, city) [Default City]:San Jose
Organization Name (eg, company) [Default Company Ltd]:Cisco
Organizational Unit Name (eg, section) []:DCBG
Common Name (eg, your name or your server's hostname) []:dcnmhost.cisco.com
Email Address []:dcnm@cisco.com

Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []: /* This field is not mandatory */
An optional company name []: /* This field is not mandatory */
...
```

CSR ファイル `dcnmweb.csr` が `/var/tmp/` ディレクトリに作成されます。

```
***** CA certificate installation not completed yet. Please do followings. *****
CSR is generated and placed at /var/tmp/dcnmweb.csr.
Please download or copy the content to your certificate signing server.
```

**Step 3** この CSR を証明書署名サーバに送信します。

**Note** CA 署名サーバは、組織に対してローカルです。

**Step 4** 認証局によって署名された証明書を取得します。

認証局 (CA) は、プライマリ、中間 (Issuing/Subordinate) 証明書、およびルート証明書の 3 つの証明書を返します。3 つの証明書すべてを `one.pem` ファイルに結合し、DCNM にインポートします。

**Step 5** 新しい CA 署名付き証明書を Cisco DCNM サーバにコピーします。

証明書が Cisco DCNM サーバの `/var/tmp` ディレクトリにあることを確認します。

**Step 6** 次のコマンドを使用して、Cisco DCNM に CA 署名付き証明書をインストールします。

**Note** 以下に示すように、同じ順序で次のコマンドを実行することを推奨します。

```
dcnm# appmgr stop all /* Stop all applications running on Cisco DCNM
dcnm# appmgr afw install-CA-signed-cert <CA-signed certificate directory>
/* CA-signed certificate with full or relative path */
Making the signed certificate available to web gateway...
```

```
CA signed certificate CA-signed-cert.pem is installed. Please start all applications as
followings:
On standalone setup execute: 'appmgr start all'
```

**Step 7** `appmgr start all` コマンドを使用して、Cisco DCNM で新しい証明書ですべてのアプリケーションを再起動します。

```
dcnm# appmgr start all
```

**Step 8** **appmgr afw show-cert-details** コマンドを使用して、新しくインストールした CA 署名証明書を確認します。

システムは、CA 証明書を用意しており、ブラウザで確認できます。

**Note** CSR は Cisco DCNM に固有のものであり、対応する CSR 署名付き証明書のみが所定の Cisco DCNM にインストールされている必要があります。

## DCNM ネイティブ HA セットアップで CA 署名済み証明書をインストールする

Cisco DCNM に CA 署名付き証明書をインストールするには、次の手順を実行します。



**Note** 以下に示すように、同じ順序で次のコマンドを実行することを推奨します。

### Procedure

**Step 1** アクティブ ノードで、SSH 端末を経由して DCNM サーバにログオンします。

**Note** 例えば、Cisco DCNM 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。

**Step 2** **appmgr afw gen-csr** コマンドを使用して、CISCO DCNM サーバで CSR を生成します。

**Note** CSR は Cisco DCNM に固有のものであり、対応する CSR 署名付き証明書のみが所定の Cisco DCNM にインストールされている必要があります。

```
dcnm1# appmgr afw gen-csr
Generating CSR....
..
...
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:CA
Locality Name (eg, city) [Default City]:San Jose
Organization Name (eg, company) [Default Company Ltd]:Cisco
Organizational Unit Name (eg, section) []:DCBG
Common Name (eg, your name or your server's hostname) []:dcnmhost.cisco.com
/* Provide a VIP FQDN name of the eth0 interface*/
Email Address []:dcnm@cisco.com

Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []: /* This field is not mandatory */
An optional company name []: /* This field is not mandatory */
...
```

**Note** アクティブ ノードで CSR を生成するケースでは、プロンプトで共通名を促される場合に、eth0 インターフェイスの VIP FQDN 名を提供することをお勧めします。

この FQDN は、Cisco DCNM Web UI を起動するためにブラウザで入力した Web サーバアドレスである必要があります。

CSR ファイル `dcnmweb.csr` が `/var/tmp/` ディレクトリに作成されます。

```
***** CA certificate installation not completed yet. Please do followings. *****
CSR is generated and placed at /var/tmp/dcnmweb.csr.
Please download or copy the content to your certificate signing server.
```

**Step 3** この CSR を証明書署名サーバに送信します。

**Note** CA 署名サーバは、組織に対してローカルです。

CA 署名サーバは、組織内の CA 署名期間または組織のローカル CA にすることができます。

**Step 4** 認証局によって署名された証明書を取得します。

**Step 5** 新しい CA 署名付き証明書を Cisco DCNM サーバにコピーします。

証明書が Cisco DCNM サーバの `/var/tmp` ディレクトリにあることを確認します。

**Step 6** スタンバイ ノードで、SSH 端末を経由して DCNM サーバにログオンします。

**Step 7** スタンバイ ノードで、`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。

```
dcnm2# appmgr stop all /* Stop all applications running on Cisco DCNM Standby Node
dcnm2#
```

**Step 8** アクティブ ノードで、`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。

```
dcnm1# appmgr stop all /* Stop all applications running on Cisco DCNM Active Node
dcnm2#
```

**Step 9** アクティブ ノードで、`appmgr afw install-CA-signed-cert` コマンドを使用して Cisco DCNM に CA 署名付き証明書をインストールします。

```
dcnm1# appmgr afw install-CA-signed-cert <CA-signed certificate directory>
/* CA-signed certificate with full or relative path */
Making the signed certificate available to web gateway....
```

CA signed certificate `CA-signed-cert.pem` is installed. Please start all applications as followings:

On standalone setup execute: `'appmgr start all'`

**Step 10** アクティブ ノードで、`appmgr start all` コマンドを使用して、Cisco DCNM 上で新しい証明書とともにすべてのアプリケーションを再起動します。

```
dcnm1# appmgr start all /* Start all applications running on Cisco DCNM Active Node
```

先に進む前に、Cisco DCNM アクティブ ノードのすべてのサービスが動作していることを確認します。

**Note** Cisco DCNM Web UI にログオンし、証明書の詳細が正しいことを確認します。

**Step 11** スタンバイ ノードで、`appmgr start all` コマンドを使用して、Cisco DCNM 上で新しい証明書とともにすべてのアプリケーションを再起動します。

```
dcnm2# appmgr start all /* Start all applications running on Cisco DCNM Standby Node
```

これにより、スタンバイノードはアクティブノードと新しいピア関係を確立できます。したがって、アクティブノードに新しくインストールされている CA 署名付き証明書は、スタンバイノードで同期されます。

**Step 12** アクティブおよびスタンバイノードの両方で **appmgr afw show-cert-details** コマンドを使用して、新しくインストールした CA 署名証明書を確認します。

システムは、CA 証明書を用意しており、ブラウザで確認できます。

**Note** 証明書情報が表示されない場合、数分待機することをお勧めします。セカンダリノードは、アクティブノードとの同期に少し時間がかかります。

ネイティブ HA セットアップの両方のピアで、同じ内部および CA 署名付き証明書を保持する場合、最初にアクティブノードの証明書をインストールします。アクティブノードに証明書をインストールした後、アクティブノードから証明書をエクスポートし、同じ証明書をスタンバイノードにインポートします。

## アクティブノードからスタンバイノードへ証明書をエクスポートする

次の手順は Cisco DCNM ネイティブ HA セットアップのみに適用されます。アクティブノードにインストールされている CA 署名付き証明書は、常にスタンバイノードに同期されています。ただし、内部の証明書はアクティブノードとスタンバイノードの両方で異なります。両方のピアで同じ証明書セットを保持する場合、このセクションで説明されている手順を実行する必要があります。



**Note** 内部証明書はシステム内部のため、証明書をエクスポートしないように選択できます。これらの証明書は、機能に影響を与えることなく、アクティブノードおよびスタンバイノードで別に行うことができます。

アクティブノードから CA 署名付き証明書をエクスポートし、スタンバイノードに証明書をインポートするには、次の手順を実行します。

### Procedure

**Step 1** アクティブノードで、SSH 端末を経由して DCNM サーバにログオンします。

**Step 2** **appmgr afw export-import-cert-ha-peer export** コマンドを使用して、証明書バンドルを作成します。

```
dcnm1# appmgr afw export-import-cert-ha-peer export
```

**Step 3** 証明書バンドルをスタンバイ ノードをコピーします。

**Note** スタンバイ ノード上の証明書を、SSH 端末で指定されている場所にコピーしていることを確認します。

**Step 4** スタンバイ ノードで、**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。

```
dcnm2# appmgr stop all /* Stop all applications running on Cisco DCNM Standby Node
dcnm2#
```

**Step 5** **appmgr afw export-import-cert-ha-peer import** コマンドを使用して、スタンバイ ノードに証明書をインポートします。

証明書バンドルがインポートされ、スタンバイ ノードにインストールされます。

**Step 6**

**Step 7** スタンバイ ノードで、**appmgr start all** コマンドを使用して、Cisco DCNM 上で新しい証明書とともにすべてのアプリケーションを再起動します。

```
dcnm2# appmgr start all /* Start all applications running on Cisco DCNM Standby Node
```

これにより、スタンバイ ノードでアプリケーションが起動したときに、新しいインポートされた証明書が有効になります。

**Step 8** スタンバイ ノードで、**appmgr afw show-cert-details** コマンドを使用して、新しくインポートされた CA 署名付き証明書を確認します。

これで、システムはアクティブ ノードとスタンバイ ノードの両方で同じ証明書を使用できるようになりました。

## アップグレード後に証明書を復元する

このメカニズムは、インラインアップグレードプロセスのみを使用した Cisco DCNM アップグレード手順に適用されます。この手順は、同じバージョンの Cisco DCNM アプライアンスでのデータのバックアップと復元には必要ありません。

証明書の復元は破壊的なメカニズムであることに注意してください。アプリケーションを停止して再起動する必要があります。復元は、アップグレードされたシステムが安定している際にのみ実行する必要があります。つまり、Cisco DCNM Web UI にログインする必要があります。Cisco DCNM ネイティブ HA セットアップでは、アクティブ ノードとスタンバイ ノードの両方でピア関係が確立されている必要があります。



(注) 証明書は、次の状況でのみ復元する必要があります。

- アップグレード前に CA 署名付き証明書がシステムにインストールされている場合。
- 11.2(1) より前のバージョンからバージョン 11.2(1) 以降にアップグレードしている場合。

Cisco DCNM をアップグレードした後は、復元する前に **CERTIFICATE 1** が CA 署名付き証明書であるか必ず証明書を確認する必要があります。それ以外の場合は、証明書を復元する必要があります。

次のサンプル出力に示すように、**appmgr afw show-cert-details** を使用して証明書を確認します。

```

dcnm# appmgr afw show-cert-details
****CERTIFICATE 1****
[Certificate available to web gateway. This certificate is offered to webclients]:
-----Web gateway certificate-----
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1575924977762797464 (0x15decf6aec378798)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, ST=CA, L=San Jose, O=Enterprise CA inc, OU=Data Center, CN=dcnm1.ca.com

    Validity
      Not Before: Dec  9 20:56:17 2019 GMT
      Not After : Dec  9 20:56:17 2024 GMT
      Subject: C=US, ST=CA, L=San Jose, O= Enterprise CA inc, OU=Data Center,
CN=dcnm1.ca.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:cf:6e:cd:c6:a9:30:08:df:92:98:38:49:9c:2a:
-----Certificate output is truncated to first 15 lines-----

****CERTIFICATE 2****
[Certificate available in keystore(jks). CA signed certificate is installed here till DCNM
version 11.1.x]
If you have upgraded from DCNM version 11.1.x to later version please see installation guide
to restore
CA signed certificate to upgraded version.
-----Keystore certificate-----
Alias name: sme
Creation date: Oct 14, 2018
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
Owner: CN=localhost, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Issuer: CN=dcnmca, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Serial number: 62044620
Valid from: Sun Oct 14 20:39:39 PDT 2018 until: Fri Oct 13 20:39:39 PDT 2023
Certificate fingerprints:
  SHA1: 38:66:F1:CD:10:61:27:E7:43:85:10:41:3D:A3:4B:5C:C9:CC:17:5E
  SHA256:
E0:87:D8:34:71:18:FE:8C:AB:18:0B:D7:85:B1:91:A8:4B:75:A3:91:BA:90:83:46:72:87:FE:FE:FE:04:F0:E1
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
-----Certificate output is truncated to first 15 lines-----
dcnm#

```

## アップグレード後に Cisco DCNM スタンドアロンセットアップで証明書を復元する

Cisco DCNM スタンドアロン展開をリリースにアップグレードした後に証明書を復元するには、次の手順を実行します。

## Procedure

- Step 1** **Note** リリースにアップグレードすると、CA 署名付き証明書のバックアップが作成されます。
- Cisco DCNM スタンドアロン アプライアンスが正常にアップグレードされたら、SSH を使用して DCNM サーバにログインします。
- Step 2** 次の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 stop all
```
- Step 3** 次のコマンドを使用して、証明書を復元します。
- ```
appmgr afw restore-CA-signed-cert
```
- Step 4** [はい (yes)] と入力し、以前インストールした証明書を復元することを確認します。
- Step 5** 次のコマンドを使用して、すべてのアプリケーションを開始します。
- ```
appmgr start all
```
- Step 6** **appmgr afw show-cert-details** コマンドを使用して、新しくインストールした CA 署名証明書を確認します。
- システムは、CA 証明書を用意しており、ブラウザで確認できます。

## アップグレード後に Cisco DCNM ネイティブ HA セットアップで証明書を復元する

Cisco DCNM ネイティブ HA セットアップでは、証明書はアクティブ ノードとスタンバイ ノードの両方にインストールされます。アクティブ ノードでのみ証明書を復元する必要があります。証明書はスタンバイ ノードと自動的に同期されます。

Cisco DCNM スタンドアロン展開をリリースにアップグレードした後に証明書を復元するには、次の手順を実行します。

## Procedure

- Step 1** SSH を使用して Cisco DCNM サーバにログインします。
- 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。
- Step 2** スタンバイ ノードで、**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。
- ```
dcnm2# appmgr stop all /* Stop all applications running on Cisco DCNM Standby Node
```
- Step 3** アクティブ ノードで、**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。
- ```
dcnm1# appmgr stop all /* Stop all applications running on Cisco DCNM Active Node
```

**Step 4** `appmgr afw restore-CA-signed-cert` コマンドを使用して、アクティブ ノードの証明書を復元します。

```
dcnm1# appmgr afw restore-CA-signed-cert
```

**Step 5** [はい (yes)] と入力し、以前インストールした証明書を復元することを確認します。

**Step 6** アクティブ ノードで、`appmgr start all` コマンドを使用してすべてのアプリケーションを起動します。

```
dcnm1# appmgr start all /* Start all applications running on Cisco DCNM Active Node
```

先に進む前に、Cisco DCNM アクティブ ノードのすべてのサービスが動作していることを確認します。

**Note** Cisco DCNM Web UI にログオンし、証明書の詳細が正しいことを確認します。

**Step 7** スタンバイ ノードで、`appmgr start all` コマンドを使用してすべてのアプリケーションを起動します。

```
dcnm2# appmgr start all /* Start all applications running on Cisco DCNM Standby Node
```

しばらく待ってから、スタンバイ ノードがアクティブ ノードと同期します。

**Step 8** アクティブおよびスタンバイ ノードの両方で `appmgr afw show-cert-details` コマンドを使用して、新しくインストールした CA 署名証明書を確認します。

システムは、CA 証明書を用意しており、ブラウザで確認できます。

## 以前にインストールされた CA 署名付き証明書の回復と復元

CA 署名付き証明書のインストール、復元、管理は、サードパーティの署名サーバが関係しているため、時間がかかるプロセスです。これにより、誤った証明書をインストールすることとなるミスが生じる場合があります。このようなシナリオでは、最新のインストールまたはアップグレードの前にインストールされた証明書を復元することをお勧めします。

以前にインストールされた CA 署名付き証明書を回復して復元するには、次の手順を実行します。

### 手順

**Step 1** SSH 端末を経由して DCNM サーバにログオンします。

**Step 2** `/var/lib/dcnm/afw/apigateway/` ディレクトリに移動します。

```
dcnm# cd /var/lib/dcnm/afw/apigateway/
dcnm# ls -ltr /* View the contents of the folder
total 128
-rw----- 1 root root 1844 Nov 18 13:14 dcnmweb.key.2019-11-20T132939-08:00
-rw-r--r-- 1 root root 1532 Nov 18 13:14 dcnmweb.crt.2019-11-20T132939-08:00
-rw----- 1 root root 1844 Nov 20 10:15 dcnmweb.key.2019-11-20T132950-08:00
-rw-r--r-- 1 root root 1532 Nov 20 10:15 dcnmweb.crt.2019-11-20T132950-08:00
-rw----- 1 root root 1844 Dec 22 13:59 dcnmweb.key
-rw-r--r-- 1 root root 1532 Dec 22 13:59 dcnmweb.crt
```

..  
..  
..

**dcnmweb** と **dcnmweb** は、現在、システムにインストールされているキーと証明書ファイルです。同様のファイル名は、タイムスタンプサフィックスを使用して、最近のアップグレードまたは復元の前にインストールされているキーと証明書のペアを識別するのに役立ちます。

- Step 3** **appmgr stop all** コマンドを使用して、Cisco DCNM 上で実行されているすべてのアプリケーションを停止します。
- Step 4** **dcnmweb.key** および **dcnmweb.crt** ファイルのバックアップをとります。
- Step 5** 復元する古いキーと証明書のペアを特定します。
- Step 6** キーと証明書のペアを **dcnmweb.key** および **dcnmweb.crt** として (タイムスタンプサフィックスなしで) コピーします。
- Step 7** **appmgr start all** コマンドを使用して、Cisco DCNM 上で実行されているすべてのアプリケーションを開始します。
- Step 8** **appmgr afw show-cert-details** コマンドを使用して、証明書の詳細を確認します。CERTIFICATE 1 は CA 署名付き証明書です。

(注) CA 署名付き証明書が Cisco DCNM Web UI に表示されない場合、または DCNM サーバがエラーメッセージを送信した場合は、システムを再起動する必要があります。

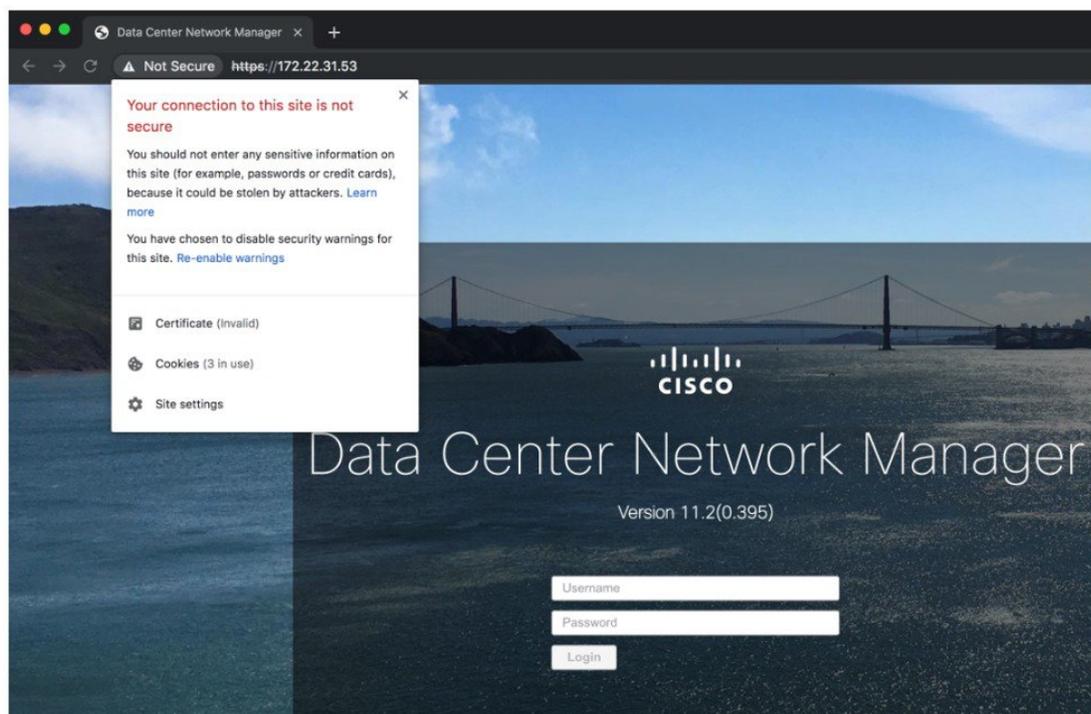
## インストールした証明書の確認

**appmgr afw show-cert-details** コマンドを使用してインストールした証明書を確認でき、Web ブラウザによって証明書が有効か否か確認します。Cisco DCNM はすべての標準ブラウザ (Chrome、IE、Safari、Firefox) をサポートします。しかし、各ブラウザでは証明書情報が異なって表示されます。

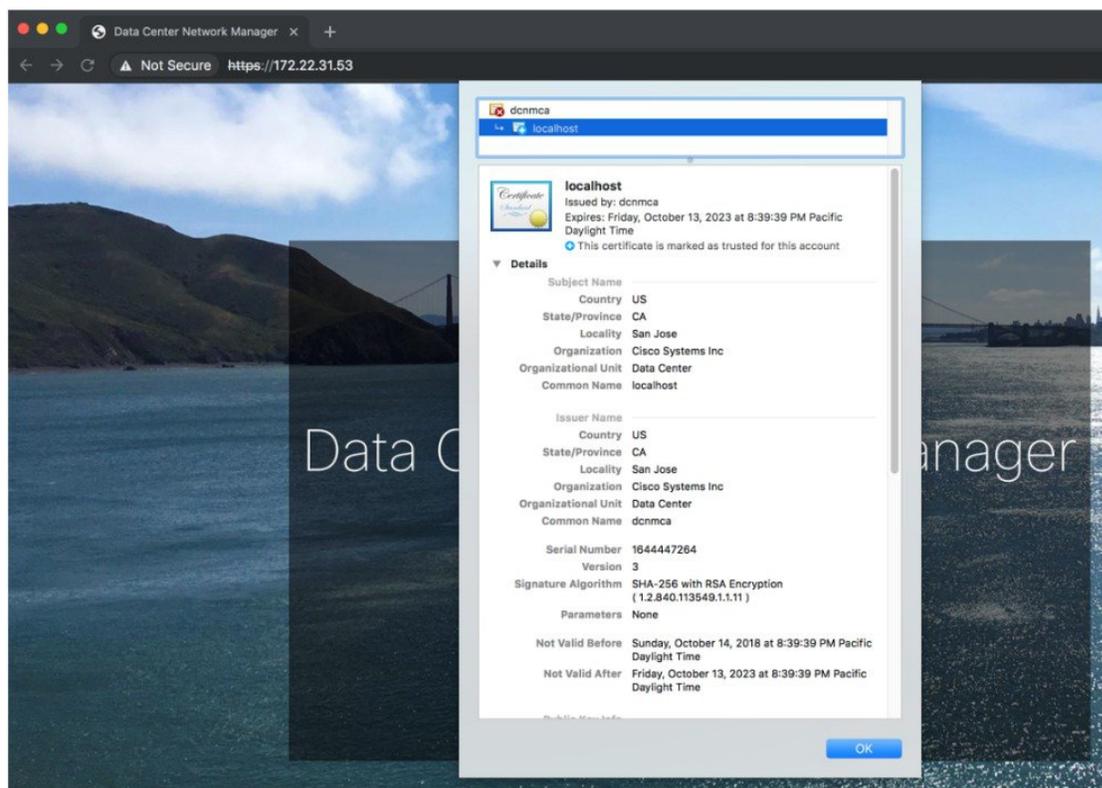
ブラウザのプロバイダ Web サイトで、ブラウザの固有情報を参照することをお勧めします。

次のスニペットは、証明書を確認するための Chrome ブラウザ バージョン 74.0.3729.169 の例です。

1. URL **https://<dcnm-ip-address>** または **https://<FQDN>** をブラウザのアドレス バーに入力します。  
Return キーを押します。
2. 証明書の種類に基づき、URL フィールドの左側のアイコンにロック アイコン [  ] またはアラート アイコン [  ] が表示されます。  
アイコンをクリックします。



3. カードで、[証明書 (Certificate)] フィールドをクリックします。  
証明書の情報が示されます。



表示されている情報は、`appmgr afw show-cert-details` を使用して証明書の詳細を確認したときに、証明書 1 に表示されている詳細と一致している必要があります。





## 第 10 章

# ファイアウォール背後での Cisco DCNM の実行

この章では、ファイアウォールの背後で Cisco DCNM を実行する方法について説明します。

- [ファイアウォール背後での Cisco DCNM の実行, on page 145](#)
- [カスタム ファイアウォールの設定 \(148 ページ\)](#)

## ファイアウォール背後での Cisco DCNM の実行

通常、企業 (外部) およびデータセンターはファイアウォールによって分離されます。つまり、DCNM はファイアウォールの背後に設定されます。Cisco DCNM Web クライアントと SSH 接続は、そのファイアウォールを通過する必要があります。また、ファイアウォールは、DCNM サーバと DCNM 管理対象デバイス間に配置できます。

すべての Cisco DCNM ネイティブ HA ノードは、ファイアウォールの同じ側にある必要があります。内部 DCNM ネイティブ HA ポートは一覧表示されていません。ネイティブ HA ノード間でファイアウォールを設定することは推奨されていません。



**Note** DCNM で LAN デバイスを追加または検出すると、検出プロセスの一部として java が使用されます。ファイアウォールがプロセスをブロックすると、TCP 接続ポート 7 が検出プロセスとして使用されます。`cdp.discoverPingDisable` サーバプロパティが `true` に設定されていることを確認します。[Web UI]、[Administration]、[DCNM Server]、[Server Properties] の順に選択して、サーバプロパティを設定します。

入力トラフィックがクライアントから入力される場合のスタンダードポートは、ローカルファイアウォールを無効にするまで変更できません。

次の表に、Cisco DCNM Web クライアント、SSH クライアント、および Cisco DCNM サーバ間の通信に使用されるすべてのポートを示します。

| Port Number | プロトコル | Service Name | コミュニケーション方向          | 備考                                                 |
|-------------|-------|--------------|----------------------|----------------------------------------------------|
| 22          | TCP   | SSH          | クライアントから<br>DCNM サーバ | 外部への SSH アクセスはオプションです。                             |
| 443         | TCP   | HTTPS        | クライアントから<br>DCNM サーバ | これは DCNM Web サーバに到達するために必要です。                      |
| 2443        | TCP   | HTTPS        | クライアントから<br>DCNM サーバ | サーバに到達するために、インストール中に必要です。インストール完了後、DCNM はポートを閉じます。 |

次の表に、Cisco DCNM サーバとその他のサービス間の通信に使用されるすべてのポートを示します。



**Note** サービスは、ファイアウォールのいずれかの側でホストできます。

| Port Number | プロトコル   | Service Name | コミュニケーション方向           | 備考                             |
|-------------|---------|--------------|-----------------------|--------------------------------|
| 49          | TCP/UDP | TACACS+      | DNS サーバから<br>DCNM サーバ | ACS サーバは、ファイアウォールのいずれかの側になります。 |
| 53          | TCP/UDP | DNS          | DNS サーバから<br>DCNM サーバ | DNS サーバは、ファイアウォールのいずれかの側になります。 |
| 123         | UDP     | NTP          | DCNM サーバから<br>NTP サーバ | NTP サーバは、ファイアウォールのいずれかの側になります。 |

| Port Number | プロトコル | Service Name | コミュニケーション方向                | 備考                                                                                            |
|-------------|-------|--------------|----------------------------|-----------------------------------------------------------------------------------------------|
| 5000        | TCP   | Docker レジストリ | DCNM サーバへの着信               | DCNM コンピューティングノードからの要求をリッスンしている DCNM サーバ上の Docker レジストリ サービス。                                 |
| 5432        | TCP   | postgres     | DCNM サーバから Postgres DB サーバ | DCNM のデフォルトインストールでは、このポートは必要ありません。<br><br>これは、Postgres が DCNM ホストマシンの外部にインストールされている場合にのみ必要です。 |

次の表に、DCNM サーバと管理対象デバイス間の通信に使用されるすべてのポートを示します。

| Port Number | プロトコル | Service Name | コミュニケーション方向     | 備考                                                           |
|-------------|-------|--------------|-----------------|--------------------------------------------------------------|
| 22          | TCP   | SSH          | 両方向             | DCNM サーバからデバイス： デバイス管理用。<br><br>デバイスから DCNM サーバ： SCP (POAP)。 |
| 67          | UDP   | DHCP         | デバイスから DCNM サーバ |                                                              |
| 69          | TCP   | TFTP         | デバイスから DCNM サーバ | POAP に必須                                                     |

| Port Number   | プロトコル       | Service Name | コミュニケーション方向     | 備考                                                                                                  |
|---------------|-------------|--------------|-----------------|-----------------------------------------------------------------------------------------------------|
| 161           | TCP および UDP | SNMP         | サーバから DCNM デバイス | TCP を使用するための <code>server.properties</code> 経由で設定されている DCNM は、UDP ポート 161 の代わりに TCP ポート 161 を使用します。 |
| 514           | UDP         | Syslog       | デバイスから DCNM サーバ |                                                                                                     |
| 2162          | UDP         | SNMP_TRAP    | デバイスから DCNM サーバ |                                                                                                     |
| 33000 ~ 33499 | TCP         | gRPC         | デバイスから DCNM サーバ | LAN テレメトリ ストリーミング                                                                                   |

## カスタム ファイアウォールの設定



(注) これは、DCNM OVA/ISO 展開にのみ適用されます。

Cisco DCNM サーバは、DCNM ローカル ファイアウォールと呼ばれる IPTables ルールのセットを展開します。これらのルールは、Cisco DCNM 操作に必要な TCP/UDP ポートを開きます。OS インターフェイスにアクセスし、SSH を経由して、ルールを変更することなく内蔵ローカルファイアウォールを操作することはできません。攻撃に対して脆弱になったり、DCNM の通常の機能に影響を及ぼす可能性があるため、ファイアウォールルールを変更しないで下さい。

指定の展開またはネットワークに対応するため、Cisco DCNM では CLI を使用してリリース 11.3(1) から独自のファイアウォールルールを設定できます。



(注) これらのルールは幅広い粒度が細かく、内蔵ローカルファイアウォールルールを優先します。したがって、メンテナンス期間はこれらのルールを慎重に設定します。

カスタム ファイアウォールを設定するために、DCNM サーバまたはアプリケーションを停止または再起動する必要はありません。



**注意** IPTableは、設定している順番でルールに優先順位を付けます。従って、最初により粒度の細かいルールをインストールする必要があります。ルールの順番が要求通りにするため、テキストエディタにすべてのルール作成し、希望の順番で CLI を実行することができます。ルールを調整する必要がある場合、すべてのルールを取り消し、希望の順番でルールを設定できます。

カスタム ファイアウォールで次の操作を実行できます。



(注) SSH を使用して Cisco DCNM サーバですべてのコマンドを実行します。

### カスタム ファイアウォール CLI

**appmgr user-firewall** コマンドを使用して、カスタム ファイアウォール CLI チェーン ヘルプと例を表示します。

```
dcnm# appmgr user-firewall
dcnm# appmgr user-firewall - h
```

### カスタム ファイアウォールのルールを設定する

**appmgr user-firewall {add | del}** コマンドを使用して、カスタム ファイアウォールルールを設定します。

```
appmgr user-firewall {add|del} proto {tcp|udp} port {<port><port range n1:n2>}
[{in|out} <interface name>] [srcip <ip-address> [/<mask>]] [dstip <ip-address> [/<mask>]]
action {permit|deny}
```



(注) カスタムファイアウォールルールは、ローカルファイアウォールルールを優先します。従って、機能が破損していないか注意して確認します。

### 例: 例のカスタム ファイアウォール ルール

- dcnm# **appmgr user-firewall add proto tcp port 7777 action deny**

このルールは、すべてのインターフェイスですべてのTCPポート7777トラフィックをドロップします。

- dcnm# **appmgr user-firewall add proto tcp port 443 in eth1 action deny**

このルールは、インターフェイス eth1 ですべてのTCPポート443着信トラフィックをドロップします。

- dcnm# **appmgr user-firewall add proto tcp port 7000:7050 srcip 1.2.3.4 action deny**

このルールは、IPアドレス1.2.3.4. から発信されているTCPポート範囲10000～10099 tトラフィックをドロップします。

### カスタム ファイアウォール ルールの保持

**appmgr user-firewall commit** コマンドを使用して、再起動時にカスタム ファイアウォール ルールを保持します。



---

(注) ルールを変更するたびにこのコマンドを実行して、再起動時にルールを保持する必要があります。

---

### ネイティブ HA スタンバイ ノードでカスタム ファイアウォール ルールをインストールする

Cisco DCNM ネイティブ HA セットアップでは、アクティブ ノードで **appmgr user-firewall commit** を実行するとき、ルールがスタンバイ ノードに自動的に同期されます。ただし、新しいルールはシステム再起動後にのみ動作します。

ルールをすぐに適用するには、**appmgr user-firewall user-policy-install** コマンドを使用してスタンバイ ノードでカスタム ファイアウォール ルールをインストールします。

### カスタム ファイアウォールの削除

**appmgr user-firewall flush-all** コマンドを使用して、すべてのカスタム ファイアウォールを削除します。

カスタム ファイアウォールを永久に削除するには、**appmgr user-firewall commit** コマンドを使用します。



## 第 11 章

# Cisco DCNM サーバのセキュアなクライアント通信

• [Cisco DCNM サーバのセキュアなクライアント通信, on page 151](#)

## Cisco DCNM サーバのセキュアなクライアント通信

この項では、Cisco Data Center Network Manager Servers で HTTPS を使用方法について説明します。



**Note** CA 署名済み SSL 証明書を追加する前に、Cisco DCNM で SSL/HTTPS を有効にする必要があります。したがって、下に記載されている順番で手順を実行します。

この項では、次のトピックについて取り上げます。

## 仮想アプライアンスの HA 環境で Cisco DCNM 上の SSL/HTTPS を有効にする

HA モードの Cisco DCNM の仮想アプライアンスで SSL/HTTPS を有効にするには、次のことを実行します。

### Procedure

**Step 1** 自己署名 SSL 証明書を使用してプライマリ サーバを設定します。

**Note** CA 署名付き証明書では、各サーバに独自の証明書が生成されます。証明書が両方のサーバで共通の署名証明書チェーンによって署名されていることを確認します。

**Step 2** セカンダリ サーバでキーストアを検索します。

**Step 3** 次の場所にあるキーストアの名前を変更します

```
< DCNM_install_root
>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks
```

～

```
< DCNM_install_root
>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks.old
```

**Step 4** プライマリ サーバからセカンダリ サーバに生成された fmserver.jks ファイルを、フォルダにコピーします。

```
<dcnm-home> /dcm/wildfly-10.1.0.Final/standalone/configuration/
<dcnm-home>/dcm/fm/conf/cert/
```

---

### What to do next

自己署名付き証明書を作成した場合、SSL 証明書をキーストアにインポートした場合、/usr/local/cisco/dcm/wildfly-10.1.0.Final/standalone/configuration にある新しい fmserver.jks を /etc/elasticsearch にコピーする必要があります。fmserver.jks ファイルを elasticsearch ディレクトリにコピーしない場合、アラームとポリシーを取得できません。elasticsearch データベースを安定化させるため、Cisco DCNM [Web UI モニタ (Web UI Monitor)] > [アラーム (Alarms)] > [アラーム ポリシー (Alarm Policies)] でアラーム ポリシーを設定できません。



## 第 12 章

# ハイアベイラビリティ環境でのアプリケーションの管理

この章では、Cisco プログラマブル ファブリック ソリューション用に、Cisco DCNM オープン仮想アプライアンス展開でハイアベイラビリティ (HA) 環境を設定する方法について説明します。また、Cisco DCNM オープン仮想アプライアンス内にバンドルされている各アプリケーションの HA 機能に関する詳細も含まれています。



(注) DCNM で適切な HA 機能を実現するには、NTP サーバがアクティブ ピアとスタンバイ ピア間で同期されている必要があります。

この章は、次の項で構成されています。

- [Information About Application Level HA in the Cisco DCNM オープン仮想アプライアンスのアプリケーション レベル HA に関する情報, on page 153](#)
- [ネイティブ HA フェールオーバーおよびトラブルシューティング, on page 155](#)
- [アプリケーション ハイアベイラビリティ, on page 157](#)

## Information About Application Level HA in the Cisco DCNM オープン仮想アプライアンスのアプリケーションレベル HA に関する情報

Cisco DCNM オープン仮想アプライアンスで実行されるアプリケーションの HA を確保するために、2つの仮想アプライアンスを実行できます。1つはアクティブ モードで、もう一方はスタンバイ モードで実行できます。



**Note** このドキュメントでは、これらのアプライアンスをそれぞれ OVA-A と OVA-B と呼びます。

このシナリオでは、次のようになります。

1. すべてのアプリケーションは、両方のアプライアンスで実行されます。  
アプリケーションデータは常に同期されるか、アプリケーションが共通のデータベースを共有します (該当する場合)。
2. 2つのアプライアンスで実行されているアプリケーションのうち1つのみがクライアント要求を処理します。最初は、OVA-A で実行されているアプリケーションです。アプリケーションは、次のいずれかが発生するまで続行します。
  - OVA 上のアプリケーションがクラッシュします。
  - OVA 上のオペレーティングシステムがクラッシュします。
  - OVA-A は何らかの理由で電源がオフになっています。
3. この時点で、他のアプライアンス (OVA-B) で実行されているアプリケーションが引き継がれます。  
DHCP の場合、最初のノードで障害が発生すると、2番目のノードが IP アドレスの提供を開始します。
4. OVA-A への既存の接続はドロップされ、新しい接続は OVA-B にルーティングされます。  
このシナリオでは、ノード (OVA-A) の 1 つが最初にアクティブノードと呼ばれ、OVA-B がスタンバイノードと呼ばれている理由を示しています。

## 自動フェールオーバー

アプリケーション レベルと仮想マシン (VM) レベルおよびスイッチオーバー プロセスは次のとおりです。

- ロードバランシングソフトウェア (DCNM/AMQP) によって管理されているアプリケーションのいずれかが OVA-A でダウンした場合、クライアント要求を処理するアクティブノードは障害を検出し、後続の要求をスタンバイノード (OVA-B) にリダイレクトします。このプロセスは、アプリケーションレベルのスイッチオーバーを提供します。
- アクティブノード (OVA A) に障害が発生した場合、または何らかの理由で電源がオフになった場合、スタンバイノード (OVA-B) は障害を検出し、OVA-B で Cisco DCNM/AMQP の VIP アドレスを有効にします。また、IP アドレスに関連付けられている新しい MAC アドレスを示すために、ローカルスイッチに追加 ARP を送信します。VIP を使用しないアプリケーションの場合、OVA-B で実行されている DHCPD は OVA-A 上の DHCPD の障害を検出し、それ自体をアクティブにします。OVA で実行されている LDAP は、LDAP がアクティブ-アクティブとして展開されているため、実行を継続します。したがって、VM レベルのフェールオーバーは、4つのすべてのアプリケーション (DCNM/AMQP/DHCP/LDAP) に対して行われます。

## 手動でトリガされたフェールオーバー

アプリケーションレベルのフェールオーバーは、手動でトリガすることもできます。たとえば、OVA-B で AMQP を実行し、OVA-A でその他のアプリケーションを実行する場合があります。この場合、OVA-A の SSH 端末にログインし、`appmgr stop amqp` コマンドを使用して AMQP を停止することができます。

このフェールオーバーは、[自動フェールオーバー, on page 154](#) で説明されているのと同じプロセスをトリガします。AMQP 仮想 IP アドレスへの後続の要求は、OVA B にリダイレクトされます。

## ネイティブ HA フェールオーバーおよびトラブルシューティング

ネイティブ HA の特性により、ホストのロールはアクティブからスタンバイ、またはスタンバイからアクティブに切り替えることができます。

ここでは、さまざまな使用例でのトラブルシューティングについて説明します。

### アクティブホストからスタンバイホストへのネイティブ HA フェールオーバー

アクティブホストからスタンバイホストへのネイティブ HA フェールオーバーが発生した場合は、次の手順を実行します。

1. DCNM Web UI にログインし、[管理者 (Administrator)] > [ネイティブ HA (NATIVE HA)] に移動します。
2. HA のステータスを確認します。DCNM HA ステータスが [OK] モードでない場合は、フェールオーバー操作を実行できません。

[フェールオーバー (Failover)] をクリックします。Cisco DCNM サーバがシャットダウンし、DCNM スタンバイ アプライアンスが動作可能になります。

3. Cisco DCNM Web UI を更新します。

DCNM サーバが動作可能になったら、DCNM Web UI にログインできます。



**Note** フェールオーバーをトリガーするには、アクティブホストで `appmgr stop all` または `appmgr stop ha-apps` を実行しないようにすることを推奨します。Cisco DCNM HA ステータスが [OK] モードでない場合、フェールオーバーの前にスタンバイ DCNM アプライアンスがアクティブなアプライアンスと同期されないため、フェールオーバーによってデータの損失が発生する可能性があります。

### DCNM アプリケーション フレームワークに関する問題

DCNM Web UI にアクセスできず、フェールオーバー操作が必要な場合は、Linux コンソールで次のいずれかのコマンドを実行します。

**appmgr failover:** このコマンドは、HA ハートビート フェールオーバーをトリガーします。

または

**reboot-h now:** このコマンドは、Linuxホストの再起動をトリガーします。これにより、フェールオーバーが発生します。

ただし、両方の HA ピアが同期していない場合、その他のすべての方法でデータ損失のリスクが発生するため、DCNM Web UI を使用してフェールオーバーを実行することをお勧めします。

### DCNM の停止と再起動

DCNM を完全に停止して再起動するには、次の手順を実行します。

1. スタンバイ アプライアンスで、**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。
2. **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かどうかを確認します。
3. アクティブ アプライアンスで、**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。
4. **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かどうかを確認します。
5. 展開されたアクティブ ホストで、**appmgr start all** コマンドを使用してすべてのアプリケーションを起動します。

すべてのアプリケーションが実行されているかどうかを確認します。DCNM Web UI にログオンして、動作しているかどうかを確認します。

6. 展開されたスタンバイ ホストで、**appmgr start all** コマンドを使用してすべてのアプリケーションを起動します。

Web UI で、[管理 (Administration)] > [ネイティブ HA (NATIVE HA)] に移動し、HA ステータスに [OK] と表示されていることを確認します。

### スタンバイ ホストの再起動

スタンバイ ホストのみを再起動するには、次の手順を実行します。

1. スタンバイ ホストで、**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。
2. **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たかどうかを確認します。
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。

Web UI で、[管理 (Administration)] > [ネイティブ HA (NATIVE HA)] に移動し、HA ステータスに [OK] と表示されていることを確認します。

## アプリケーションハイアベイラビリティ

ここでは、すべての Cisco プログラマブル ファブリック HA アプリケーションについて説明します。

Cisco DCNM オープン仮想アプライアンスには2つのインターフェイスがあります。1つはオープン仮想アプライアンス管理ネットワークに接続し、もう1つは強化されたプログラマブル ファブリックネットワークに接続しています。仮想IPアドレスは、両方のインターフェイスに対して定義されます。

- オープン仮想アプライアンス管理ネットワークから、DCNM REST API、DCNM インターフェイス、および AMQP には VIP アドレスを使用してアクセスします。
- 拡張されたファブリック管理ネットワークから、LDAP と DHCP に直接アクセスします。

次の3つの仮想 IP のみが定義されています。

- DCNM REST API (DCNM 管理ネットワーク上)
- DCNM REST API (拡張ファブリック管理ネットワーク上)
- AMQP (dcnm 管理ネットワーク上)



**Note** HA で DCNM オープン仮想アプライアンスでは VIP を設定しますが、VIP は DCNM、REST API のアクセスに使用することを目的としています。GUI アクセスの場合でも、DCNM HA ピアの個別 IP アドレスを使用し、同じものを使用して DCNM SAN Java クライアントなどを起動することを推奨します。

プログラマブルファブリックアプリケーションとそれに対応する HA メカニズムの完全なリストについては、次の表を参照してください。

| プログラマブルファブリックアプリケーション       | HA メカニズム                  | 仮想 IP の使用 | 注                        |
|-----------------------------|---------------------------|-----------|--------------------------|
| Data Center Network Manager | DCNM クラスタリング/<br>フェデレーション | 対応        | 各ネットワークに1つずつ定義された2つのVIP  |
| RabbitMQ                    | RabbitMQ ミラーリング<br>キュー    | 対応        | OVA 管理ネットワークで定義された1つのVIP |
| リポジトリ                       | —                         | —         | 外部リポジトリを使用する必要があります      |

## データセンターのネットワーク管理

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、[http://\[host/ip\]](http://[host/ip]) でブラウザからアクセスできます。



**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。

### HA の実装

両方の OVA で動作する Cisco DCNM は、HA 用のクラスタモードとフェデレーションモードで設定されます。Cisco DCNM フェデレーションは、SAN デバイスの HA メカニズムです。SAN デバイスのグループは、DCNM フェデレーションセットアップの各ノードで管理できます。すべてのデバイスは、単一のクライアントインターフェイスを使用して管理できます。

Cisco DCNM UI で自動フェールオーバーを有効にするには、**Admin > Federation** を選択します。自動フェールオーバーを有効にし、OVA A で実行されている Cisco DCNM に障害が発生した場合、自動フェールオーバーは、OVA A から OVA B に自動的に管理されるファブリックおよび shallow-discovered LAN のみを移動します。

### DCNM 仮想 IP の使用状況

オープン仮想アプライアンス HA セットアップには、デフォルトの HTTP ポートに Cisco DCNM の 2 つの VIP アドレス (各ネットワークに 1 つずつ) があります。これらの VIP は、オープン仮想アプライアンス管理ネットワークおよび拡張ファブリック管理ネットワーク上の DCNM RESTful サービスにアクセスするために使用できます。たとえば、Cisco UCS Director などの外部システムは、オープン仮想アプライアンス管理ネットワークの VIP を指定することができ、要求がアクティブな Cisco DCNM に転送されます。同様に、拡張ファブリック管理ネットワーク内のスイッチは、POAP プロセス中に拡張ファブリック管理ネットワーク上の VIP アドレスにアクセスします。

Cisco DCNM の実際の IP アドレスに直接接続し、クラスタ/フェデレーションセットアップの DCNM の場合と同じように使用することもできます。



**Note** DCNM REST API にアクセスする場合にのみ、VIP アドレスを使用することを推奨します。Cisco DCNM Web または SAN クライアントにアクセスするには、サーバの IP アドレスを使用して接続する必要があります。

### ライセンス

Cisco DCNM では、最初のインスタンスのライセンスと、2 番目のインスタンスに対応する予備のライセンスがあることを推奨します。

### アプリケーションのフェールオーバー

[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [ネイティブ HA (Native HA)] を選択して、オープン仮想アプライアンス HA ペアが設定されている場合に、Cisco DCNM UI で自動フェールオーバー オプションを有効にします。このプロセスにより、OVA A で実行されている DCNM に障害が発生した場合、DCNM A によって管理されているすべてのファブリックおよび shallow-discovered LAN は、所定の期間 (通常は、OVA A の DCNM の障害発生後約 5 分後) に DCNM B により自動的に管理されます。

Cisco DCNM VIP アドレスは引き続き OVA A に存在します。Representational State Transfer Web Services (REST) コールは、最初に OVA A の VIP アドレスに到達し、OVA B で実行されている Cisco DCNM にリダイレクトされます。

### アプリケーション フェールバック

OVA A で Cisco DCNM が起動すると、VIP アドレスによって REST 要求が DCNM A に自動的にリダイレクトされます。

### 仮想 IP のフェールオーバー

OVA A の Cisco DCNM REST API に設定されている VIP アドレスは、次の 2 つの理由により失敗する可能性があります。

- OVA A で実行されているロードバランシング ソフトウェアが失敗します。
- OVA A が失敗します。

Cisco DCNM の VIP アドレスは、自動的に OVA B に移行されます。唯一の違いは、フェールオーバー後に使用される DCNM です。

- ロードバランシング ソフトウェアの障害が発生した場合、OVA-B の VIP アドレスは要求を DCNM A に送信します。
- OVA A 障害が発生した場合、OVA B の VIP アドレスは要求を DCNM B に送信します。

自動フェールオーバーにより、DCNM A によって管理されているすべてのファブリックおよび shallow-discovered LAN の所有権が自動的に DCNM B に変更されます。

### 仮想 IP フェールバック

OVA A が起動され、Cisco DCNM が実行されている場合、VIP アドレスはスタンバイ ノードで実行されたままになります。OVA B から OVA A への仮想 IP アドレスのフェールバックは、次の順序でのみ発生します。

1. OVA A が起動します。
2. Cisco DCNM は、OVA A 上で動作します。
3. OVA B がダウンするか、OVA B でロードバランシング ソフトウェアが失敗します。

# 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。



**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。

## HA の実装

オープン仮想アプライアンスで HA を有効にすると、オープン仮想アプライアンス管理ネットワークに VIP アドレスが作成されます。vCloud Director などのオーケストレーションシステムでは、その AMQP ブローカを VIP アドレスに設定します。

オープン仮想アプライアンスで HA を有効にすると、各ノードで実行する RabbitMQ ブローカも、他のノードで実行されているブローカと重複するように設定されます。両方の OVA は、RabbitMQ クラスタの「ディスク ノード」として機能します。これは、永続キューに保存されているすべての永続メッセージが複製されることを意味します。RabbitMQ ポリシーにより、すべてのキューがすべてのノードに自動的に複製されます。

## アプリケーションのフェールオーバー

RabbitMQ A に障害が発生すると、OVA の VIP アドレスは、後続の AMQP 要求を RabbitMQ にリダイレクトします。

## アプリケーション フェールバック

RabbitMQ A が起動すると、VIP アドレスが自動的に AMQP 要求の RabbitMQ への指示を開始します。

## 仮想 IP のフェールオーバー

OVA A で AMQP ブローカに対して設定された VIP アドレスは、次の 2 つの理由により失敗する可能性があります。

- OVA A で実行されているロードバランシング ソフトウェアが失敗します。
- OVA A が失敗します。

いずれの場合も、AMQP の VIP アドレスは自動的に OVA B に移行されます。唯一の違いは、フェールオーバー後に使用される AMQP ブローカです。

- ロードバランシング ソフトウェアの障害では、OVA B の VIP アドレスによって要求が RabbitMQ に転送されます。
- OVA A で障害が発生した場合、OVA B の VIP アドレスによって、要求が RabbitMQ B に送信されます。

### 仮想 IP フェールバック

OVA A が起動し、AMQP A が実行されている場合、VIP アドレスは OVA B で実行され続けます (要求を AMQP A に指示します)。RabbitMQ VIP の OVA B から OVA A へのフェールバックは、次の順序でのみ発生します。

1. OVA A が起動します。
2. RabbitMQ は、OVA A で実行されます。
3. OVA B がダウンするか、OVA B でロードバランシング ソフトウェアが失敗します。

## リポジトリ

すべてのリポジトリがリモートである必要があります。





## 第 13 章

# 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 \(163 ページ\)](#)
- [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 \(177 ページ\)](#)
- [ユーティリティ サービスの詳細, on page 182](#)
- [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 183](#)
- [IPv6 の SFTP サーバアドレスの更新, on page 186](#)

## 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。

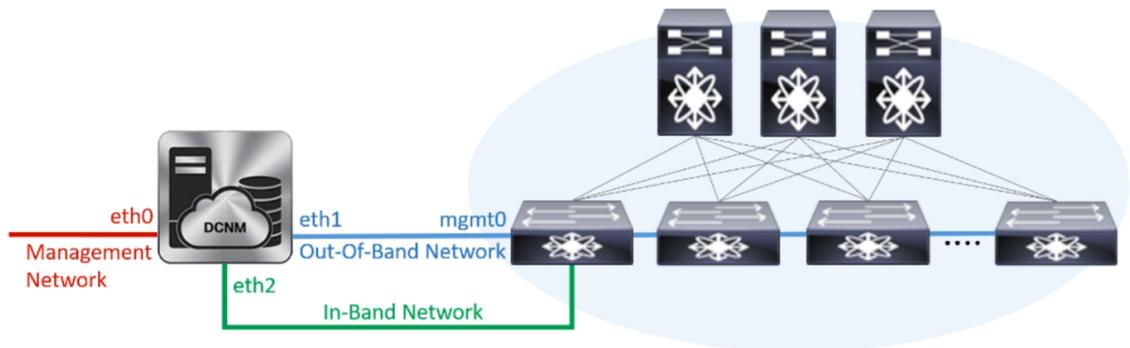
- enhanced-fabric-mgmt (eth1) インターフェイス

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

- Step 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
```
- Step 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>
```
- Step 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}
```
- Step 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

- Step 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。
- Step 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**
- Step 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**
- Step 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}**
- Step 5** スタンバイ ノードで、ステップ [Step 4, on page 167](#) 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。
- Step 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。

- Step 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**
- Step 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。
- Step 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**
- Step 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**
- Step 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

```

## 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

```
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

```

## 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

```

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"
```

## DCNM インストール後に DCNM サーバパスワードを変更する

```

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 ~]#

```

## 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

- 
- Step 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。
- Step 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> " & \$ % ' ^ = < > ; : ` \ | / , . \*`

**Step 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

- Step 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。
- Step 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。
- Step 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

---

- Step 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。
- Step 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。
- Step 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。
- Step 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。
- Step 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:
Install mode: LAN Fabric
Standalone node. HA not enabled.
dcnm#
```

## 手順

- 
- Step 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
```
- Step 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。
- Step 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 **SYSTEMRESOURCEERROR** 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 セカンダリ (Fresh Installation - HA Secondary)] オプション ボタンを選択して、**dcnm2** をセカンダリ 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。

クラスタ モードで Cisco DCNM プライマリを構成している場合は、[クラスタ モードを有効にする (Enable Clustered Mode)] チェックボックスをオンにします。

[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。

(注) Network Insights アプリケーションを使用している場合は、DNS サーバが有効で到達可能であることを確認します。

- [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。

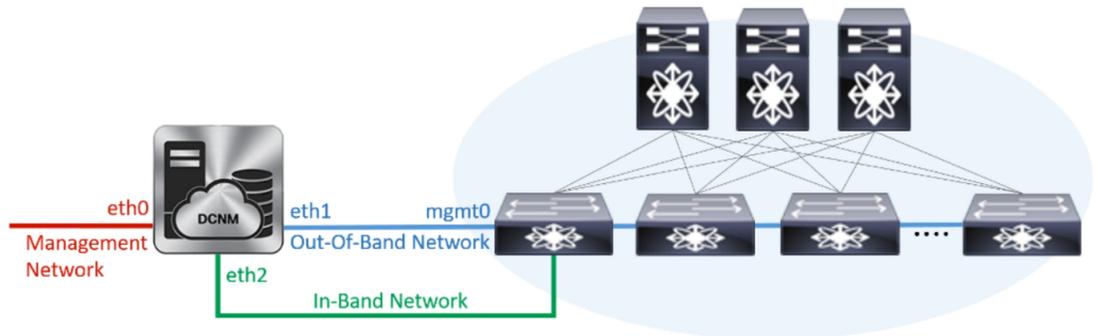
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **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 22: 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]、および [クラスタ モード設定] 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。
2. [クラスタ モード設定 (Clustered mode configuration)] 領域で、ネットワーク設定を構成して、クラスタ モードで DCNM インスタンスを展開します。クラスタ モードで、アプリケーションは個別のコンピューティング ノードで実行されます。

- [アウトオブバンド IPv4 ネットワーク アドレス プール (Out-of-Band IPv4 Network Address Pool)] で、クラスタ モードで使用するアウトオブバンド IPv4 ネットワークからアドレス プールを入力します。

オプションで、[アウトオブバンド IPv6 ネットワーク アドレス プール (Out-of-Band IPv6 Network Address Pool)] フィールドに IPv6 アドレス プールを入力することもできます。

- [インバンド IPv4 ネットワーク アドレス プール (In-Band IPv4 Network Address Pool)] で、クラスタ モードで使用するインバンド IPv4 ネットワークからアドレス プールを入力します。

オプションで、[インバンド IPv6 ネットワーク アドレス プール (In-Band IPv6 Network Address Pool)] フィールドに IPv6 アドレス プールを入力することもできます。

IP アドレスがプライマリ ノードで構成されたものと同じプールに属することを確認します。

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VIPv6アドレス (Management Network VIPv6 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 VIPv6 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 VIPv6 アドレス (Out-of-Band Network VIPv6 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 VIPv6 アドレス (In-Band Network VIPv6 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。

- [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（古いスタンドアロンノード）：

```
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。

## 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

Rabbit MQ 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錆巢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ワークを定義します。

- 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

- Step 1** SSH セッションを開きます。
- ssh root DCNM network IP address** コマンドを入力します。
  - 管理パスワードを入力してログインします。

- Step 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  dhcpd

```

## 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。

## 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
```



## 第 14 章

# DCNM 検証を行う Tetration エージェント

Tetration ソフトウェア エージェントは、ホストシステムで実行される小さなソフトウェアアプリケーションです。その主な機能は、ネットワークフロー情報をモニタおよび収集することです。また、システムで実行されているネットワーク インターフェイスやアクティブなプロセスなど、その他のホスト情報も収集します。エージェントによって収集された情報は、さらなる分析処理のために Tetration クラスタ内で実行されている一連のコレクタにエクスポートされます。

- [DCNM 検証を行う Tetration エージェント \(187 ページ\)](#)

## DCNM 検証を行う Tetration エージェント

Linux プラットフォームで詳細可視性適用エージェントを展開する場合は、インストーラ スクリプトを使用することをお勧めします。

### 始める前に

インストールされたエージェントを Tetration クラスタに接続する場合は、**ACTIVATION\_KEY** および **HTTPS\_PROXY** パラメータが必要です。インストーラ スクリプトを使用すると、自動的に **ACTIVATION\_KEY** が入力されますが、HTTPS\_PROXY 情報をスクリプトに直接挿入する必要があります。

手動展開を使用する場合は、**ACTIVATION\_KEY** と **HTTPS\_PROXY** の両方のパラメータを手動で挿入します。詳細については、「[Tetration SaaS のユーザー設定](#)」を参照してください。

### 手順

- Step 1** クレデンシャルを使用して Cisco TetrationOS ソフトウェアの Web UI にログインします。
- Step 2** [設定 (Settings)] メニューから [エージェント設定 (Agent Config)] を選択して、[エージェント設定 (Agent Config)] ウィンドウを表示します。
- Step 3** [ソフトウェア エージェント ダウンロード (Software Agent Download)] タブに移動します。
- Step 4** [Select Platform (プラットフォームの選択)] セクションで [Linux] を選択します。
- Step 5** [Select Agent Type (エージェントタイプの選択)] セクションで [Deep Visibility] または [Enforcement] を選択します。

**Step 6** [Download Installer (インストーラのダウンロード)] ボタンをクリックし、ファイルをローカルディスクに保存します。

**Step 7** ルート権限で DCNM にログインします。インストーラ シェル スクリプトをコピーし、スクリプトを実行します。

(注) エージェントがすでにインストールされている場合、インストーラ スクリプトは続行されません。

インストーラ スクリプト コマンドおよびその構文は、次のとおりです。

```
$ tetration_linux_installer.sh [-skip-pre-check] [-noInstall]
    [-logFile=filename] [-proxy=proxy_string>] [-skip-ipv6-check]
    [-help] [-version] [-sensor-version=version_info] [-ls] [-file=filename]
    [-save=filename] [-new]
```

<b>-skip-pre-check</b>	インストール前のチェックをスキップします。
<b>-noInstall</b>	センサー パッケージはダウンロードされず、システムにインストールされません。
<b>-logFile filename</b>	filename で指定されたファイルにログを書き込みます。
<b>-proxy proxy_string</b>	HTTPS_PROXY の値を設定します。クラスタとの通信にプロキシサーバが必要な場合は、これを使用します。文字列は <code>http://proxy:port</code> の形式にする必要があります。
<b>-skip-ipv6-check</b>	IPv6 検証をスキップします。
<b>-help</b>	このヘルプ情報を出力します。
<b>-version</b>	現在のスクリプトのバージョンを印刷します。
<b>-sensorVersion version_info</b>	特定のセンサー バージョンをダウンロードします。デフォルトは最新バージョンです。version_info エントリの例は <code>-sensor-version = 3.1.1.53.devel</code> です。
<b>ls</b>	システムで使用可能なすべてのセンサー バージョンを一覧表示します (3.1 より前のパッケージは一覧表示しません)。これはリストのみです。パッケージをダウンロードしません。
<b>-file filename</b>	クラスタからダウンロードする代わりに、センサーのインストールに使用するローカル zip ファイルを指定します。
<b>-save filename</b>	Tetration クラスタからインストーラの zip ファイルをダウンロードし、ファイル名を付けてローカルに保存します。
<b>-new</b>	Tetration エージェントがこのローカルマシンにすでにインストールされている場合は、すべてのコピーをアンインストールまたは削除します。

**Step 8** 次のコマンドを実行して、エージェントがインストールされていることを確認します。

```
sudo rpm -q tet-sensor
```

エントリは次のように表示されます。

```
$ sudo rpm -q tet-sensor
```

tet-sensor-3.1.1.50-1.el6.x86\_64

(注) DCNM ネイティブ HA クラスタ展開には、DCNM プライマリ、DCNM セカンダリ、および3つのコンピューティングノードの5つのノードがあります。DCNM クラスタを完全に可視化するために、これらの各ノードに Tetration エージェントをインストールします。

図 23: DCNM クラスタを使用する Tetration エージェント

The screenshot shows the Cisco Tetration 'SOFTWARE AGENT LIST' interface. The table lists several agents, with the 'epi-compute2' agent highlighted in yellow. The table columns are: Hostname, Agent Type, IP Addresses, SW Version, Platform, First Check-In, Last Check-In, and VRF.

Hostname	Agent Type	IP Addresses	SW Version	Platform	First Check-In	Last Check-In	VRF
epi-compute3	Enforcement	172.28.188.28 172.28.188.188 172.28.188.28 172.28.188.28 172.28.188.28 ...16 more	3.3.2.23-enforcer	CentOS-7.7	May 6 2020 03:31:33 am (PDT)	May 11 2020 01:51:57 pm (PDT)	DCNM
epi-compute2	Enforcement	172.28.188.28 172.28.188.188 172.28.188.28 172.28.188.28 172.28.188.28 ...15 more	3.3.2.23-enforcer	CentOS-7.7	May 6 2020 03:31:21 am (PDT)	May 11 2020 01:47:58 pm (PDT)	DCNM
epi-compute1	Enforcement	172.28.188.28 172.28.188.188 172.28.188.28 172.28.188.28 172.28.188.28 ...27 more	3.3.2.23-enforcer	CentOS-7.7	May 6 2020 03:31:09 am (PDT)	May 11 2020 01:55:24 pm (PDT)	DCNM
epi-haSecondary	Enforcement	172.28.188.27 172.28.188.188 172.28.188.27 172.28.188.27 172.28.188.27 ...8 more	3.3.2.23-enforcer	CentOS-7.7	May 6 2020 03:25:17 am (PDT)	May 11 2020 01:41:22 pm (PDT)	DCNM
epi-primary	Enforcement	172.28.188.28 172.28.188.28 172.28.188.28 172.28.188.28	3.3.2.23-enforcer	CentOS-7.7	May 6 2020 03:24:55 am (PDT)	May 11 2020 02:01:04 pm (PDT)	DCNM





## 第 15 章

# TACACS+ サーバ経由で認証をセットアップ

- TACACS+ Server 経由のリモート認証 (191 ページ)

## TACACS+ Server 経由のリモート認証

リリース 11.5(1) 以降、Cisco DCNM には、TACACS+ サーバ経由で認証を設定するための **appmgr** コマンドが用意されています。DCNM は TACACS+ サーバに接続して、アクセスが許可されているかどうかを判断します。成功すると、アクセスが許可されます。TACACS+ サーバに到達できない場合、システムはローカル認証に戻ります。

この機能によって認証されるユーザは、**root** ユーザ、**sysadmin** ユーザ、および **poap** ユーザです。すべてのユーザをリモートサーバで設定する必要があります。

リモート認証は、SSH セッションでのみサポートされます。**su** コマンドは常にローカル認証を使用します。アプライアンス コンソールからのログインでは、ユーザがシステムからロックアウトされないように、常にローカル認証が使用されます。

### リモート認証の削除

リモート認証を削除するには、次のコマンドを使用します。

```
appmgr remote-auth set none
```



(注) **appmgr remote-auth set** コマンドは、常に古い設定を新しい設定に置き換えます。

### TACACS+ を使用したリモート認証の設定

TACACS+ を使用してリモート認証を設定するには、次のコマンドを使用します。

```
appmgr remote-auth set tacacs [ auth {pap | chap | ascii } ] {server <addr> <secret> }
```

値は次のとおりです。

- **auth** は、認証タイプを定義します。指定しない場合、デフォルトは PAP です。ASCII および MSCHAP もサポートされます。

- **addr** はサーバのアドレスです。サーバアドレスは、ホスト名、IPv4 アドレス、または IPv6 アドレス形式にすることができます。ポート番号を指定することもできます。例：  
**my.tac.server.com:2049**

IPv6 アドレスは、RFC2732 に準拠した完全修飾 IPv6 形式でなければなりません。IPv6 アドレスは [] で囲む必要があります。そうしないと、機能が正しく機能しません。

次に例を示します。

- [2001:420:1201:2::a] – 正解
- 2001:420:1201:2::a – 不正解

- **secret** は、DCNM と TACACS+ サーバ間で共有される秘密です。スペースを含むシークレットは許可されません/サポートされません。

### リモート認証の有効化または無効化

リモート認証を有効または無効にするには、次のコマンドを使用します。

```
appmgr remote-auth { enable | disable }
```

### リモート認証パスワードの表示

リモート認証パスワードを表示するには、次のコマンドを使用します。

```
appmgr remote-auth show
```

サンプル出力:

```
dcnm# appmgr remote-auth show
Remote Authentication is DISABLED

dcnm# appmgr remote-auth show
Remote Authentication is ENABLED
Protocol: tacacs+
Server: 172.28.11.77, secret: *****
Authentication type: ascii
```

dcnm#

デフォルトでは、[-S or --show-secret] キーワードを使用しない限り、共有秘密はクリアテキストで表示されません。

### 例

1. 172.28.11.77 をリモート認証サーバとして設定し、cisco123 を共有秘密として使用します。

```
dcnm# appmgr remote-auth set tacacs server 172.28.11.77 cisco123
dcnm# appmgr remote-auth enable
```

2. 認証タイプとして MSCHAP を使用し、172.28.11.77 をリモート認証サーバとして設定し、Cisco 123 を共有秘密として設定します。

```
dcnm# appmgr remote-auth set tacacs auth mschap 172.28.11.77 cisco123
dcnm# appmgr remote-auth enable
```

- 異なる共有秘密を持つ3つのサーバを設定します。

```
dcnm# appmgr remote-auth set tacacs server tac1.cisco.com:2049 cisco123 server
tac2.cisco.com Cisco_123 server tac3.cisco.com Cisco_123
dcnm# appmgr remote-auth enable
```

- 認証設定を無効にするか、削除します。

```
dcnm# appmgr remote-auth set tacacs none
```

- 設定を削除せずにリモート認証を無効にします。

```
dcnm# appmgr remote-auth disable
```

- 現在のリモート認証設定を有効にします。

```
dcnm# appmgr remote-auth enable
```

### リモート認証と POAP

リモート認証がイネーブルの場合、POAP ユーザのローカルパスワードは TACACS サーバのパスワードと同じである必要があります。それ以外の場合、POAP は失敗します。

ローカルの POAP パスワードを同期するには、TACACS サーバでパスワードを設定または変更した後、次のコマンドを使用します。

#### **appmgr change\_pwd ssh poap**

Cisco DCNM ネイティブ HA セットアップでは、このコマンドはアクティブ ノードでのみ実行します。

### DCNM ネイティブ HA セットアップでのリモート認証

既存のスタンドアロンセットアップにセカンダリ HA ノードを追加する前、および **appmgr update ssh-peer-trust** コマンドを実行する前に、リモート認証を無効にする必要があります。

