



メディア コントローラ展開リリース 11.5(1) の Cisco DCNM インストールおよびアップグレードガイド

初版：2020年12月22日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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.

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)

© 2020 Cisco Systems, Inc. All rights reserved.



目次

Full Cisco Trademarks with Software License ?

第 1 章

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

Cisco DCNM のアップグレード 3

システム要件 4

第 2 章

注意事項と制約事項 11

注意事項と制約事項 11

第 3 章

前提条件 13

DCNM オープン仮想アプライアンスの前提条件 13

DCNM ISO 仮想アプライアンスの前提条件 14

Cisco DCNM 仮想アプライアンス HA の前提条件 15

HA モードで Cisco DCNM 仮想アプライアンスを展開する 15

仮想 IP アドレスの可用性 15

NTP サーバのインストール 15

第 4 章

Cisco DCNM のインストール 17

オープン仮想アプライアンスで DCNM をインストールする 17

オープン仮想アプライアンス ファイルのダウンロード 17

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	18
スタンドアロンモードでの Cisco DCNM OVA のインストール	23
ネイティブ HA モードでの Cisco DCNM OVA のインストール	27
ISO 仮想アプライアンスで DCNM をインストールする	35
ISO 仮想アプライアンス ファイルのダウンロード	35
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	36
KVM 上での DCNM ISO 仮想アプライアンスのインストール	43
Nexus ダッシュボードで DCNM ISO 仮想アプライアンスをインストールする	45
スタンドアロンモードでの Cisco DCNM ISO のインストール	46
ネイティブ HA モードで Cisco DCNM ISO をインストールする	50
Cisco APIC SE で Cisco DCNM SE ISO をインストールする	58
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	60

第 5 章

Cisco DCNM のアップグレード 67

Cisco DCNM のアップグレード	67
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	68
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	68
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	71
でパフォーマンス マネージャ データをドロップする	75

第 6 章

ディザスタ リカバリ (バックアップおよび復元) 79

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	79
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	80
Cisco DCNM シングル HA ノードのリカバリ	82

第 7 章

証明書 85

の証明書管理	85
証明書管理のベスト プラクティス	86
インストールされた証明書の表示	86

	CA 署名付き証明書のインストール	88
	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	88
	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	90
	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	92
	アップグレード後に証明書を復元する	93
	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	95
	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	95
	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	96
	インストールした証明書の確認	97
<hr/>		
第 8 章	ファイアウォール背後での Cisco DCNM の実行	101
	ファイアウォール背後での Cisco DCNM の実行	101
	カスタム ファイアウォールの設定	104
<hr/>		
第 9 章	Cisco DCNM サーバのセキュアなクライアント通信	107
	Cisco DCNM サーバのセキュアなクライアント通信	107
	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	107
<hr/>		
第 10 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	109
	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	109
	自動フェールオーバー	110
	手動でトリガされたフェールオーバー	111
	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	111
	アプリケーション ハイ アベイラビリティ	113
	データセンターのネットワーク管理	114
	RabbitMQ	116
	リポジトリ	117
<hr/>		
第 11 章	DCNM 展開後にユーティリティ サービスを管理する	119

DCNM インストール後のネットワーク プロパティ	119
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	120
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	122
DCNM インストール後に DCNM サーバパスワードを変更する	130
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	131
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	131
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	133
ユーティリティ サービスの詳細	138
電源オン自動プロビジョニング	138
アプリケーションとユーティリティ サービスの管理	138
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	139
ユーティリティ サービスの停止、開始、リセット	140

第 12 章	TACACS+ サーバ経由で認証をセットアップ	143
	TACACS+ Server 経由のリモート認証	143



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](#)
- [Cisco DCNM のアップグレード, on page 3](#)
- システム要件 (4 ページ)

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す。

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。

サポートされている遅延

Cisco DCNM メディア コントローラ 展開のサポートされている遅延は下記で定義されています。

- Native HA プライマリおよびセカンダリ アプライアンス間では、遅延は 50ms です。
- DCNM Native HA プライマリからスイッチ間では、遅延は 50ms 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。

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 root パスワードが必要です。 sysadmin ユーザーは sudo su 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 su は次のエイリアスです sudo su	リモート認証が設定されている場合でも、 su 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 root ユーザーだけです。	sysadmin もこのコマンドを実行できます。	-
appmgr root-access {permit deny ...} コマンド	root ユーザーのみがこのコマンドを実行できます	sysadmin 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	root 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	root または sysadmin ユーザーはこれらのコマンドを実行できます	root または sysadmin ユーザーはこれらのコマンドを実行できます	-

Cisco DCNM のアップグレード

Cisco DCNM リリース 11.0(1) より前に、DCNM OVA、および ISO は SAN 機能をサポートしていました。Cisco DCNM リリース 11.3(1) 以降では、OVA と ISO 仮想アプライアンスの両方に SAN 展開用の Cisco DCNM をインストールできます。

次の表は、リリース 11.5(1) にアップグレードするために従う必要があるアップグレードのタイプをまとめたものです。

Table 1: IP for Media (IPFM) 展開のアップグレードのタイプ

現在のリリース番号	リリース 11.5(1) にアップグレードするアップグレードタイプ
11.4(1)	インライン アップグレード
11.3(1)	インライン アップグレード
11.2(1)	インライン アップグレード
11.1 (1)	11.1(1) → 11.2(1) → 11.5(1) 11.1(1) → 11.3(1) → 11.5(1) 11.1(1) → 11.4(1) → 11.5(1) → インライン アップグレードを表します

システム要件

このセクションでは、Cisco DCNM リリース 11.5(1) を正しく機能させるためのさまざまなシステム要件について説明します。



(注) 基盤となるサードパーティソフトウェアを個別にアップグレードしないことを推奨します。必要なソフトウェアコンポーネントはすべて、インラインアップグレード手順で更新されます。DCNM アップグレード以外のコンポーネントをアップグレードすると、パフォーマンスの問題が発生します。

- [Java の要件 \(5 ページ\)](#)
- [サーバ要件 \(5 ページ\)](#)
- [サポートされている遅延](#)
- [データベースの要件 \(5 ページ\)](#)
- [ハイパーバイザ \(5 ページ\)](#)
- [サーバリソース要件 \(6 ページ\)](#)
- [Cisco DCNM の VMware Snapshot サポート \(6 ページ\)](#)
- [サポートされる Web ブラウザ \(8 ページ\)](#)
- [その他のサポート対象のソフトウェア \(9 ページ\)](#)

Java の要件

Cisco DCNM サーバは、次のディレクトリに JRE 1.0.8 を使用して配信されます。

DCNM_root_directory/java/jdk11

サーバ要件

Cisco DCNM リリース 11.5(1) では、次の 64 ビットオペレーティングシステム上の Cisco DCNM サーバがサポートされています。

- **IP for Media および LAN ファブリックの展開:**
 - CentOS Linux リリース 7.8 と統合した Open Virtual Appliance (OVA)
 - CentOS Linux リリース 7.8 と統合した ISO 仮想アプライアンス (ISO)

サポートされている遅延

Cisco DCNM メディア コントローラ 展開のサポートされている遅延は下記で定義されています。

- Native HA プライマリおよびセカンダリ アプライアンス間では、遅延は 50ms です。
- DCNM Native HA プライマリからスイッチ間では、遅延は 50ms です。

データベースの要件

Cisco DCNM リリース 11.2(1) では、次のデータベースをサポートします。

- PostgreSQL 10.15-OVA / ISO 展開向け



(注) ISO/OVA インストールは、組み込み型 PostgreSQL データベースのみをサポートします。

ハイパーバイザ

Cisco DCNM では、次のサーバプラットフォーム上のベアメタルサーバ(ハイパーバイザなし)での ISO のインストールがサポートされています。

サーバ	製品 ID (PID)	推奨される最小メモリ、ドライブ容量、CPU 数
Cisco UCS C240M4	UCSC-C240-M4S	32G / 500G 16 vCPU
Cisco UCS C240M4	UCSC-C240-M4L	32G / 500G 16 vCPU
Cisco UCS C240 M5S	UCSC-C240-M5SX	32G / 500G 16 vCPU
Cisco UCS C220 M5L	UCSC-C220-M5L	32G / 500G 16 vCPU



- (注) Cisco が Cisco UCS でのみテストしている場合でも、Cisco DCNM は適切な仕様の代理のコンピューティング ハードウェアで動作します。

サーバリソース要件



- (注) 仮想マシンの Cisco DCNM をインストールする場合、サーバリソース要件と同等のリソースを予約し、物理マシンを持つベースラインを確保する必要があります。

表 2: Cisco DCNM IPFM 展開のシステム要件

展開タイプ	小規模 (Lab または POC)	大規模 (生産)
OVA/ISO	CPU : vCPU x 8 RAM : 24 GB DISK : 500 GB	CPU : vCPU x 16 RAM : 32 GB DISK : 500 GB



- (注) 大規模かつコンピューティング展開の場合、ディスクを追加できます。ディスクのサイズは、最小 32GB から最大 1.5TB の範囲まで使用できます。

DCNM のインストールを完了し、DCNM アプリケーションを安定して継続的に動作させるために、ルートパーティションに十分なディスク領域を割り当てます。ディスク領域の要件については、アプリケーションのユーザーガイドを参照してください。インストールまたはアップグレード中に `/tmp` ディレクトリをマウントできる別のディスクをマウントできます。 `appmgr system scan-disks-and-extend-fs` コマンドを使用して、ディスク領域とディスク ファイル システムを追加することもできます。

Cisco DCNM の VMware Snapshot サポート

VMware vSphere Hypervisor (ESXi)	6.0	6.5	6.7	6.7 P01	7.0
VMware vCenter サーバ	6.0	6.5	6.7	6.7 P01	7.0



- (注) Cisco DCNM OVA インストーラを展開するには、VMware vCenter サーバが必要です。しかし、vCenter を使用せずに VMware ESXi に DCNM を直接インストールするには、DCNM ISO 展開を選択できます。正しい CPU、メモリ、ディスク、および NIC リソースがその VM に割り当てられていることを確認します。

VM でスナップショットを撮影するには、次の手順を実行します。

1. インベントリ内の仮想マシンを右クリックして、**[スナップショット (Snapshot)] > [スナップショットの撮影 (Take Snapshot)]** をクリックします。
2. **[スナップショットの撮影 (Take Snapshot)]** ダイアログボックスに、スナップショットの名前と説明を入力します。
3. **[OK]** をクリックし、スナップショットを保存します。

次のスナップショットを VM に使用できます。

- VM の電源がオフの状態。
- VM の電源がオンまたはアクティブの状態。



- (注) VM の電源がオンまたはオフのとき、Cisco DCNM はスナップショットをサポートします。仮想マシン メモリ オプションが選択されているとき、DCNM はスナップショットをサポートしません。

次の図に示すように、**仮想マシンのメモリのスナップショット** チェックボックスが選択されていないことを確認してください。ただし、VM の電源がオフになっている場合グレーになっています。

Take Snapshot | dcnm-va.11.x.1 ×

Name VM Snapshot taken powered on 12/8/2019,

Description

Snapshot the virtual machine's memory

Quiesce guest file system (Needs VMware Tools installed)

CANCEL OK

スナップショットの状態に VM を復元できます。

Manage Snapshots | dcnm1111 ×

dcnm1111

- VM Snapshot 12%252f12%252f2019, 11:56:07 AM
- 11:31 Snapshot 12%252f12%252f2019, 3:04:31 PM
- VM Snapshot 12%252f16%252f2019, 6:55:02 AM
 - You are here

Name	VM Snapshot 12%252f16%252f2019, 6:55:02 AM
Created	12/15/2019, 11:55:31 PM
Disk usage	510.03 MB
Snapshot the virtual machine's memory	No
Quiesce guest file system	No

DELETE ALL DELETE REVERT TO EDIT

DONE

仮想マシンを右クリックし、[スナップショットの管理 (Manage Snapshots)] を選択します。復元するスナップショットを選択し、[終了 (Done)] をクリックします。

サポートされる Web ブラウザ

Cisco DCNM は次の Web ブラウザをサポートします。

- Google Chrome バージョン: 86.0.4240.198
- Mozilla Firefox バージョン: 82.0.3 (64 ビット)
- Microsoft Edge バージョン: 86.0.622.63

その他のサポート対象のソフトウェア

次の表に、Cisco DCNM リリース 11.5(1) でサポートされているその他のソフトウェアを示します。

表 3: その他のサポート対象のソフトウェア

コンポーネント	機能
セキュリティ	<ul style="list-style-type: none">• ACS バージョン 4.0、5.1、5.5、および 5.8• ISE バージョン 2.6• ISE バージョン 3.0• Telnet 無効 : SSH バージョン 1、SSH バージョン 2、グローバル適用 SNMP プライバシー暗号化。• Web Client 暗号化 : TLS 1、1.1、1.2 を使用する HTTPS
OVA/ISO インストーラ	CentOS 7.6/Linux カーネル 3.10.x

Cisco DCNM は call-home イベント、ファブリック変更イベント、トラップおよびメールで転送されるイベントをサポートしています。



第 2 章

注意事項と制約事項

- [注意事項と制約事項, on page 11](#)

注意事項と制約事項

Cisco DCNM をインストールおよびアップグレードのガイドラインと制限は、次の通りです。

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> " & \$ % ' ^ = < > ; : ` \ | / , . *`
 - Cisco DCNM リリース 11.0(1) から、管理パスワードに許可されている文字は、OVA および ISO インストールに制限されています。従って、アップグレード中に、DCNM 11.0(1) または 11.1(1) に使用されている古いパスワードは無効です。ただし、アップグレード中は別のパスワードが許可されています。

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)

ただし、アップグレード後 Postgres DBMS は DCNM 10.4(2) で取得されているバックアップから復元されているため、DCNM リリース 10.4(2) で使用されているパスワードを使用して、Cisco DCNM Web UI にログオンする必要があります。

- 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、**pg_ctl** コマンドを使用します。**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。
- 基盤となるサードパーティ ソフトウェアを個別にアップグレードしないことを推奨します。必要なソフトウェア コンポーネントはすべて、インラインアップグレード手順で更新されます。DCNMアップグレードの外部のコンポーネントのアップグレードは、パフォーマンスの問題を生じさせます。

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。



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 13](#)
- [DCNM ISO 仮想アプライアンスの前提条件, on page 14](#)
- [Cisco DCNM 仮想アプライアンス HA の前提条件, on page 15](#)

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「サーバーリソースの要件」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す。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せん。
- 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

サポートされている遅延

Cisco DCNM メディア コントローラ 展開のサポートされている遅延は下記で定義されています。

- Native HA プライマリおよびセカンダリ アプライアンス間では、遅延は 50ms です。
- DCNM Native HA プライマリからスイッチ間では、遅延は 50ms です。

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で DCNM をインストールする \(17 ページ\)](#)
- [ISO 仮想アプライアンスで DCNM をインストールする \(35 ページ\)](#)
- [Cisco APIC SE で Cisco DCNM SE ISO をインストールする \(58 ページ\)](#)
- [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 \(60 ページ\)](#)

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

- ステップ 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。
- ステップ 2** 最新リリースのリストで、11.5(1) を選択します。
- ステップ 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。
- ステップ 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

- ステップ 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

- ステップ 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。
- ステップ 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。
- ステップ 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。
- ステップ 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。
- ステップ 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。
- ステップ 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。
- ステップ 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 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、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す。

[Next] をクリックします。

- ステップ 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。

- ステップ 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。

ステップ 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。

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 119](#)」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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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、[スタンドアロンモードでの Cisco DCNM OVA のインストール, on page 23](#) 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 27](#) 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

ステップ 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。

ステップ 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。

ステップ 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 アプリアランスの [メディア コントローラ (Media Controller)] インストール モードを選択します。

[Next] をクリックします。

ステップ 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。

ステップ 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。

- [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。

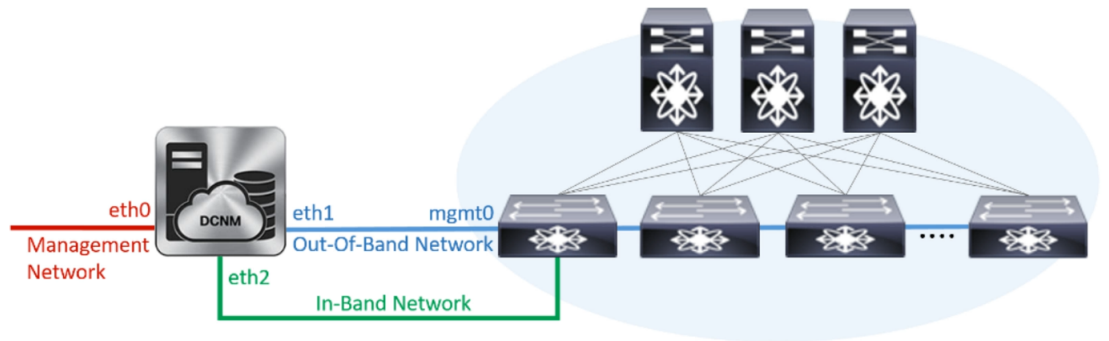
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **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。

ステップ 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。

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 119](#)」を参照してください。

[Next] をクリックします。

ステップ 7 [アプリケーション (Applications)] タブで、 、 および を構成します。

- a) [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。

ステップ 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

ステップ 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。

ステップ 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 **SYSTEM RESOURCE ERROR** と表示され、インストールが中止されます。システム要件を変更し、Web インストーラを起動してインストールを完了します。

b) [Cisco DCNM インストーラ (Cisco DCNM Installer)] 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[メディア コントローラ (Media Controller)] インストールモードを選択します。

[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。

- [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。

- [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。

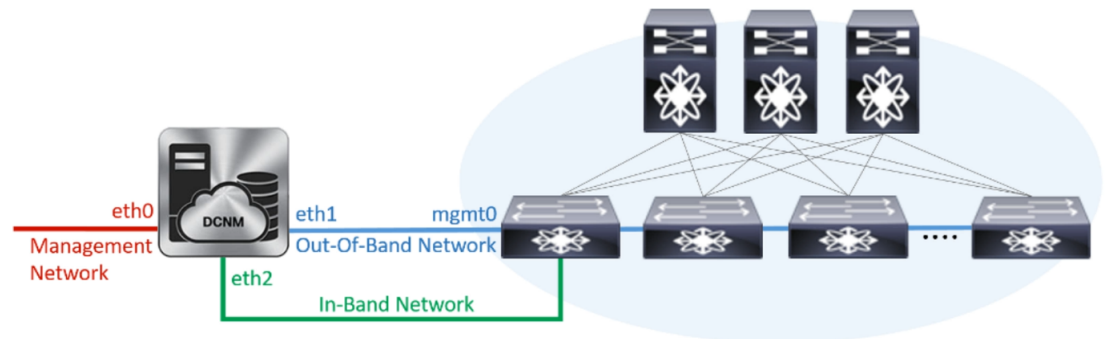
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **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。

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 119](#)」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、[内部アプリケーションサービス ネットワーク] を構成します。

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

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 27](#) 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。

- 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.

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

初期メッセージが表示されます。

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

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。

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。

[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。

- [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。

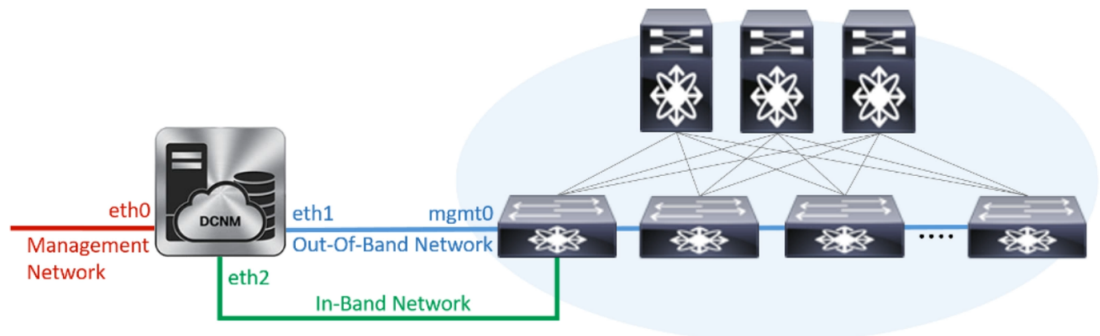
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **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] を構成します。
1. [内部アプリケーションサービス ネットワーク (Internal Application Services Network)] 領域で、DCNM に対して内部で実行するアプリケーションへアクセスするための **IPv4 IP サブネット フィールド** に IP サブネットを入力します。
- h) [HA 設定 (HA Settings)] タブで、セカンダリ ノードのシステム設定を行います。
- [プライマリ DCNM ノードの管理 IP アドレス (Management IP Address of primary DCNM node)] フィールドに、DCNM UI にアクセスするための適切な IP アドレスを入力します。
 - [VIP 完全修飾ホスト名 (VIP Fully Qualified Host Name)] フィールドで、RFC1123 セクション 2.1 の通りに、完全修飾ドメイン名 (FQDN) のホスト名を入力します。数字のみのホスト名はサポートされていません。
 - [管理ネットワーク VIP アドレス (Management Network VIP Address)] フィールドに、管理ネットワークの VIP として使用された IP アドレスを入力します。
オプションで、[管理ネットワークの IPv6 VIP アドレス (Management Network IPv6 Address)] フィールドに IPv6 VIP アドレスを入力することもできます。
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 IPv6 アドレスを設定していることを確認します。
 - [アウトオブバンドネットワーク VIP アドレス (Out-of-Band Network VIP Address)] フィールドにアウトオブバンドネットワークの VIP として使用される IP アドレスを入力します。
オプションで、[アウトオブバンドネットワークの IPv6 VIP アドレス (Out-of-Band Network IPv6 Address)] フィールドに IPv6 VIP アドレスを入力することもできます。
 - [インバンドネットワーク VIP アドレス (In-Band Network VIP Address)] フィールドにアウトオブバンドネットワークの VIP として使用される IP アドレスを入力します。

オプションで、[インバンドネットワークの 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

- ステップ 1** 次のサイトに移動します。 <http://software.cisco.com/download/>。
- ステップ 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。
- ステップ 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。
- ステップ 4** 最新リリースのリストで、11.5(1) を選択します。
- ステップ 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。

- ステップ 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。
- ステップ 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 43](#) 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 36](#) 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ネルまたはイーサネットチャ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

- ステップ 1** Cisco Integrated Management Controller (CIMC) を起動します。
- ステップ 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。
- ステップ 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。
- ステップ 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)]** の順にクリックします。
- ステップ 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に移動し、ISO イメージをロードします。
- ステップ 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。
- ステップ 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
- ステップ 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。

ステップ 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.
```

ステップ 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。

ステップ 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

```

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 119](#)」を参照してください。

ステップ 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) 81:00:0 Intel Corporation Ethernet Controller 10G X550T (rev 01)
   Address: 78:69:5a:48:1a:e6      Link:UP
2) 81:00:1 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: a8:93:51:89:55:f2      Link:DOWN
10) 3b:00:1 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: a8:93:51:89:55:f3      Link:DOWN
11) 3b:00:2 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: a8:93:51:89:55:f4      Link:DOWN
12) 3b:00:3 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: a8:93:51:89:55: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): _

```

ステップ 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。

ステップ 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、[スタンドアロン モードでの Cisco DCNM ISO のインストール](#), on

page 46 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 50 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

- ステップ 1 を解凍し抽出し、**dcnm-kvm-vm.xml** ファイルを検索します。
- ステップ 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。
- ステップ 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。
- ステップ 4 および **dcnm-kvm-vm.xml** RHEL サーバにアップロードします。
- ステップ 5 ファイル転送セッションを閉じます。
- ステップ 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。
- ステップ 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。
- ステップ 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}]
```

- ステップ 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。
- ステップ 10 SSH セッションを閉じます。
- ステップ 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。
- ステップ 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。

- ステップ 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。
- ステップ 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。
- ステップ 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。

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

- ステップ 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せん。

[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 119](#)」を参照してください。

- ステップ 21** [y] を押して、インストールを確認して続行します。
- ステップ 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、[スタンドアロン モードでの Cisco DCNM ISO のインストール, on page 46](#) 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 50](#) を参照してください。

Nexus ダッシュボードで DCNM ISO 仮想アプライアンスをインストールする

Nexus ダッシュボードに 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。

Before you begin

『Cisco Nexus ダッシュボード ハードウェア セットアップ ガイド』の説明に従って、ハードウェアとネットワークの接続を設定します。

Procedure

- ステップ 1 Cisco Integrated Management Controller (CIMC) を起動します。
- ステップ 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。
- ステップ 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。
- ステップ 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)] の順にクリックします。
- ステップ 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に移動し、ISO イメージをロードします。
- ステップ 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] をクリックして続行して、UCS ボックスを再起動します。
- ステップ 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。
- ステップ 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。
- ステップ 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。
- ステップ 10 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。
- ステップ 11 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。

提供された IP アドレスは、管理ネットワーク インターフェイス (eth0) の設定に使用されます。これで、システムがネットワーク経由で到達可能になります。

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 [スタンドアロン モードでの Cisco DCNM ISO のインストール, on page 46](#) 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 50](#) 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

ステップ 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。

ステップ 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。

ステップ 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 [メディア コントローラ (Media Controller)] インストール モードを選択します。

[Next] をクリックします。

ステップ 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。

ステップ 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。

- [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。

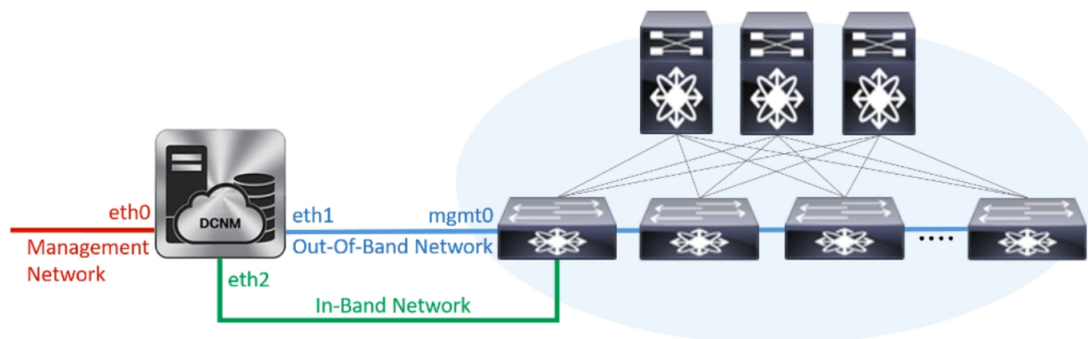
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **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。

ステップ 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



- [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。

- [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。

- (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。

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 119](#)」を参照してください。

[Next] をクリックします。

ステップ 7 [アプリケーション (Applications)] タブで、および を構成します。

a) [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。

ステップ 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 CiscoDCNM 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 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

ステップ 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。

ステップ 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 **SYSTEM RESOURCE ERROR** と表示され、インストールが中止されます。システム要件を変更し、Web インストーラを起動してインストールを完了します。

- b) **[Cisco DCNM インストーラ (Cisco DCNM Installer)]** 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**[メディア コントローラ (Media Controller)]** インストール モードを選択します。

[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。

- **[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。

- **[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。

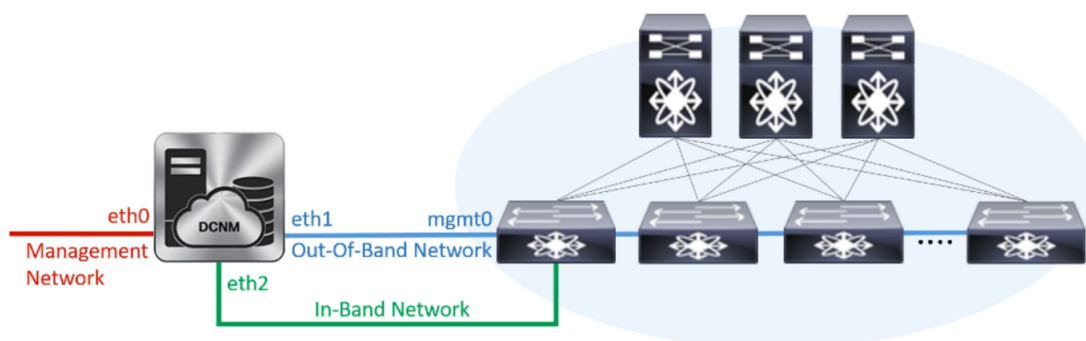
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **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。

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 119](#)」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、[内部アプリケーションサービス ネットワーク] を構成します。

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

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 51](#) 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。

- 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.
```

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

初期メッセージが表示されます。

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

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。

- 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。

[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。

- **[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。

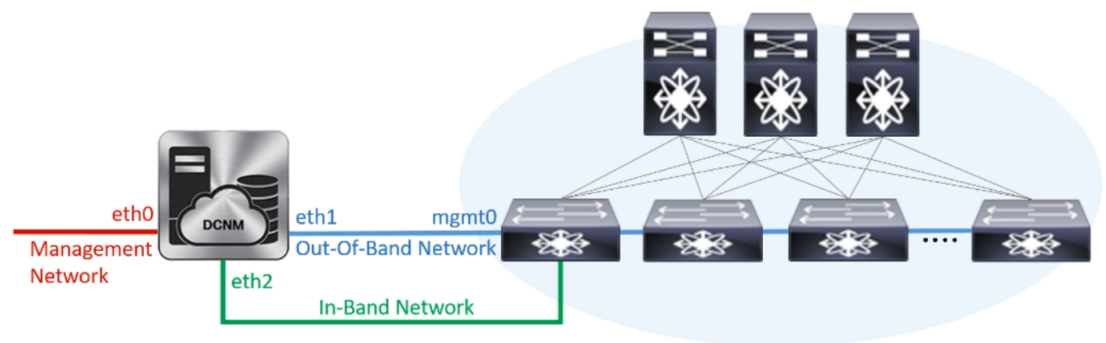
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **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せん。

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]** を構成します。

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

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

- **[プライマリ DCNM ノードの管理 IP アドレス (Management IP Address of primary DCNM node)]** フィールドに、DCNM UI にアクセスするための適切な IP アドレスを入力します。
- **[VIP 完全修飾ホスト名 (VIP Fully Qualified Host Name)]** フィールドで、RFC1123 セクション 2.1 の通りに、完全修飾ドメイン名 (FQDN) のホスト名を入力します。数字のみのホスト名はサポートされていません。

- **[管理ネットワーク VIP アドレス (Management Network VIP Address)]** フィールドに、管理ネットワークの VIP として使用された IP アドレスを入力します。

オプションで、**[管理ネットワークの IPv6 アドレス (Management Network IPv6 Address)]** フィールドに IPv6 VIP アドレスを入力することもできます。

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 IPv6 アドレスを設定していることを確認します。

- **[アウトオブバンドネットワーク VIP アドレス (Out-of-Band Network VIP Address)]** フィールドにアウトオブバンドネットワークの VIP として使用される IP アドレスを入力します。

オプションで、[アウトオブバンド ネットワークの 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 で Cisco DCNM SE ISO をインストールする

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.addDevDevice(dev)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1293, in addDevDevice
self.handleDevDeviceFormat(info, device)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 2889, in handleDevDeviceFormat
self.handleDevLUMPUFormat(info, device)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1651, in handleDevLUMPUFormat
self.handleLvs(vy_device)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1588, in handleLvs
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
anaconda1:~#

```

既存の APIC ASE に 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

ステップ 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。

ステップ 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。

ステップ 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$
```

ステップ 4 Cisco Applications Service Engine を再起動します。

ステップ 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](#)』を参照してください。
- 『[Cisco DCNM リリース 11.4\(1\) 向け Cisco Application Services Engine インストール ガイド](#)』

スタンドアロンセットアップからネイティブ HA セットアップへの変換

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

始める前に

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

```
dcnm# appmgr show version

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

手順

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

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

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

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

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

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

初期メッセージが表示されます。

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

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

b) [Cisco DCNM インストーラ (Cisco DCNM Installer)] 画面で、[新規インストール - HA セカンダリ (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。

[Next] をクリックします。

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

(注) すべてのパスワードは、プライマリ ノードの設定時に指定したパスワードと同じである必要があります。

e) [システム設定 (System Settings)] で、DCNM アプライアンスの設定を行います。

- [完全修飾ホスト名 (Fully Qualified Hostname)] フィールドで、RFC1123 セクション 2.1 の通りに、完全修飾ドメイン名 (FQDN) のホスト名を入力します。数字のみのホスト名はサポートされていません。

- [DNS サーバアドレス (DNS Server Address)] フィールドで、DNS IP アドレスを入力します。

リリース 11.2(1) から、IPv6 アドレスを使用した DNS サーバも設定できます。

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

- [NTP サーバアドレス リスト (NTP Server Address List)] フィールドでは、NTP サーバの IP アドレスを入力します。

値は IP または IPv6 アドレスか RFC 1123 に準拠した名前である必要があります。

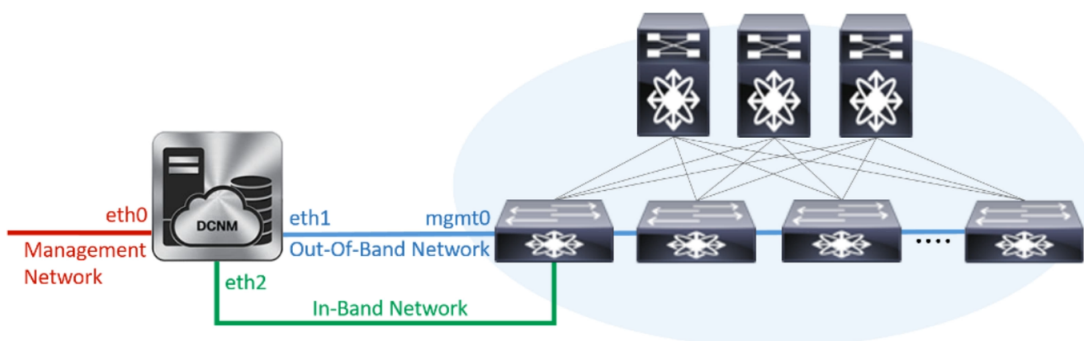
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **タイムゾーン** ドロップダウン リストから、DCNM を展開しているタイムゾーンを選択します。

[Next] をクリックします。

- f) **[ネットワーク設定 (Network Settings)]** タブで、DCNM Web UI に到達するために使用されるネットワーク パラメータを構成します。

図 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]** を構成します。
1. **[内部アプリケーションサービス ネットワーク (Internal Application Services Network)]** 領域で、DCNM に対して内部で実行するアプリケーションへアクセスするための **IPv4 IP サブネット フィールド** に IP サブネットを入力します。
- h) **[HA 設定 (HA Settings)]** タブで、セカンダリ ノードのシステム設定を行います。
- **[プライマリ DCNM ノードの管理 IP アドレス (Management IP Address of primary DCNM node)]** フィールドに、DCNM UI にアクセスするための適切な IP アドレスを入力します。
 - **[VIP 完全修飾ホスト名 (VIP Fully Qualified Host Name)]** フィールドで、RFC1123 セクション 2.1 の通りに、完全修飾ドメイン名 (FQDN) のホスト名を入力します。数字のみのホスト名はサポートされていません。
 - **[管理ネットワーク VIP アドレス (Management Network VIP Address)]** フィールドに、管理ネットワークの VIP として使用された IP アドレスを入力します。
オプションで、**[管理ネットワークの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
```




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。

- [Cisco DCNM のアップグレード, on page 67](#)
- [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 \(68 ページ\)](#)
- [パフォーマンス マネージャ データをドロップする, on page 75](#)

Cisco DCNM のアップグレード

Cisco DCNM リリース 11.0(1) より前に、DCNM OVA、および ISO は SAN 機能をサポートしていません。Cisco DCNM リリース 11.3(1) 以降では、OVA と ISO 仮想アプライアンスの両方に SAN 展開用の Cisco DCNM をインストールできます。

次の表は、リリース 11.5(1) にアップグレードするために従う必要があるアップグレードのタイプをまとめたものです。

Table 4: IP for Media (IPFM) 展開のアップグレードのタイプ

現在のリリース番号	リリース 11.5(1) にアップグレードするアップグレードタイプ
11.4(1)	インラインアップグレード
11.3(1)	インラインアップグレード
11.2(1)	インラインアップグレード
11.1 (1)	11.1(1) → 11.2(1) → 11.5(1) 11.1(1) → 11.3(1) → 11.5(1) 11.1(1) → 11.4(1) → 11.5(1) → インラインアップグレードを表します

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

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 にログインする必要があります。

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 \(93 ページ\)](#) 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 11.5(1) 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。

Procedure

- ステップ 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、**SYSTEMRESOURCEERROR** 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。

ステップ 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。

ステップ 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/ フォルダにアクセスできることを確認します。

ステップ 4 dcnm-va.11.5.1.iso.zip ファイルを解凍し、DCNM 11.5(1) ISO ファイルをアップグレードする DCNM セットアップ内の /root/ フォルダにアップロードします。

ステップ 5 **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
```

ステップ 6 /mnt/iso フォルダのスタンドアロンセットアップに DCNM 11.5(1) ISO ファイルをマウントします。

```
mount -o loop <DCNM 11.5(1) image> /mnt/iso
```

```
dcnm# mount -o loop dcnm-va.11.5.1.iso /mnt/iso
```

ステップ 7 /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 11.5(1)? [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。

ステップ 8 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。

11.2(1) および 11.3(1) でサポートされている Elasticsearch バージョンは、11.5(1) でサポートされている Elasticsearch と互換性がないため、リリース 11.5(1) にアップグレードする前に 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。

ステップ 9 `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
```

ステップ 10 Cisco DCNM リリース 11.5(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: 11.5(1)
Install mode: Media Controller
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 にログオンします。



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。11.5(1) 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、「[パフォーマンス マネージャ データをドロップする](#)」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。

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

- 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

ステップ 1 dcnm-va.11.5.1.iso.zip ファイルを解凍し、DCNM 11.5 (1) ISO ファイルを /root/ フォルダーに、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。

ステップ 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。

ステップ 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。

ステップ 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 11.5(1) 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。

```
dcnm1# mount -o loop dcnm-va.11.5.1.iso /mnt/iso
```

- 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。

```
dcnm1# Do you want to continue and perform the inline upgrade to 11.5(1)? [y/n]: y
```

- 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。

11.2(1) および 11.3(1) でサポートされている Elasticsearch バージョンは、11.5(1) でサポートされている Elasticsearch と互換性がないため、リリース 11.5(1) にアップグレードする前に 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。

ステップ 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 11.5(1) ISO ファイルを /mnt/iso フォルダーで Standby ノードでマウントします。

```
dcnm2# mount -o loop dcnm-va.11.5.1.iso /mnt/iso
```

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

```
dcnm2# cd /mnt/iso/package-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。

```
dcnm2# Do you want to continue and perform the inline upgrade to 11.5(1)? [y/n]: y
```

- 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 にログオンします。



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。11.5(1) 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、「[でパフォーマンス マネージャ データをドロップする](#)」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。

でパフォーマンス マネージャ データをドロップする



Note リリース 11.5(1) にアップグレードするとき 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。

Performance Manager (PM) データをドロップするには、次の手順を実行します。

Before you begin

- DCNM アプライアンスが動作していることを確認します。(スタンドアロンのアップグレード向け)
- フェデレーションを設定している場合は、DCNM フェデレーション設定のすべてのノードが動作していることを確認します。(フェデレーションセットアップ向け)

Procedure

ステップ 1 SSH セッションを起動し、次のコマンドを実行して PMDB インデックスを表示します。

Performance Manager データベースの PMDB インデックスを特定します。

でパフォーマンス マネージャ データをドロップする

次に例を示します。

```
dcnm-root-11-4# curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb
```

```

  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total  Spent    Left     Speed
100 2448    100 2448    0      0   4523      0  --:--:--  --:--:--  --:--:--  4524
green open pmdb_cpumemdata          rb-CJf-NR0my8M3mO-7QkA 5 1  7286  0
1.4mb 760.2kb
green open pmdb_ethintfratedata      P18gMKdPTkCODv0TomYAdw 5 1  9283  0
2.4mb 1.2mb

```

「pmdb_」というプレフィックスが付いたインデックスが表示されます。

ステップ 2 Cisco DCNM Web UI で、[管理 (Administration)] > [パフォーマンスの設定 (Performance Setup)] > [LAN コレクション (LAN Collection)] を選択します。

すべてのスイッチとコレクションを無効にするには、すべてのチェックボックスをオフにし、[適用 (Apply)] をクリックします。

Administration / Performance Setup / LAN Collections

For all selected licensed LAN Switches collect: Trunks Access Errors & Discards Temperature Sensor

Performance Default Polling Interval: 5 Mins

- Fab-1-externalfab
 - 9k_aragon
 - C93108TC-FX_116
 - C93108TC-FX_41
 - n3k_72
 - N77-TGEN-195
 - N9k_27
 - N9K-C9232C_28
 - N9K-C9364C_49
 - N9K-C9504_44
 - sugarbowl_56
 - suharbowl_57
- Fab-2-ClassicLAN
 - N3k_Utopia_70
 - switch
- Fab3-otherswitches
 - IND13-P1-A1
 - N6K-96Q-63
 - test
 - Default_LAN

ステップ 3 [管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバステータス (Server Status)] を選択します。

ステップ 4 Performance Collector サービスに対して、[アクション (Actions)] 列の停止アイコンをクリックして、データ収集を停止します。

DCNM Server	Actions	Service Name	Status
localhost		Database Server	Running
10.106.228.37	Re-init Elasticsearch DB Schema	dexer	Last updated: 2020-12-13 16:30:00
10.106.228.37	Stop Service, Clean up PM DB stale entry(s)	Performance Collector	Stopped
10.106.228.37		Agent	Running
10.106.228.37		Elasticsearch	Status:yellow, Docs: pmdb_*=0
0.0.0.0:123		NTPD Server	Running
0.0.0.0:67		DHCP Server	Running
0.0.0.0:2162		SNMP Traps	Running
0.0.0.0:514		Syslog Server	Running

ステップ 5 削除アイコンをクリックして、Performance Manager データベースを消去します。

このアクションにより、Performance Manager データベース内の古いエントリが削除されます。

ステップ 6 [再初期化 (reinitialize)] アイコンをクリックして、Elasticsearch データベーススキーマのインデックスを再作成します。

この操作は、Elasticsearch データベースの Performance Manager データを消去し、Performance Manager を再起動します。完了するまで数分かかる場合があります。

ステップ 7 [Continue] をクリックします。

Performance Collector サービスのステータスが [停止 (Stopped)] と表示されます。

ステップ 8 次のコマンドを使用して、すべての PMDB エントリを削除したことを確認します。

- リリース 11.1(1) からのアップグレード用
`curl https://127.0.0.1:33500/_cat/indices?pretty | grep pmdb`
- リリース 11.2 (1) からのアップグレード
`curl https://127.0.0.1:33500/_cat/indices?pretty | grep pmdb`
- リリース 11.3 (1) からのアップグレード用
`curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb`
- リリース 11.4(1) からのアップグレード用
`curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb`

次に例を示します。

```
dcnm-root-11-4# curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb
% Total    % Received % Xferd Average Speed   Time    Time     Time  Current
```

でパフォーマンス マネージャ データをドロップする

						Dload	Upload	Total	Spent	Left	Speed
100	2244	100	2244	0	0	3638	0	--:--:--	--:--:--	--:--:--	3636



第 6 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 79](#)
- [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 80](#)
- [Cisco DCNM シングル HA ノードのリカバリ \(82 ページ\)](#)

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。11.5(1) 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

ステップ 1 SSH を使用して Cisco DCNM アプライアンスにログインします。

ステップ 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。

ステップ 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。

ステップ 4 新しい DCNM アプライアンスを展開します。

ステップ 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。

ステップ 6 DCNM Web インストーラ UI で、[開始 (Get Started)] をクリックします。

ステップ 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。

[ステップ 2, on page 80](#) 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。

ステップ 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。

ステップ 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。11.5(1) 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

ステップ 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。

ステップ 2 SSH を使用して Cisco DCNM アプライアンスにログインします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 7 DCNM Web インストーラ UI で、[開始 (Get Started)] をクリックします。

ステップ 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 [ステップ 3, on page 81](#) 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。

ステップ 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。

ステップ 10 データが復元されたら、`appmr 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"> 1. セカンダリ ノードをプライマリ ノードに変換します。 2. 新しいセカンダリ ノードの設定
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。

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
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
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 ノードとしてみなし、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。

2. 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。
3. `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。
4. 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。
5. `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。
6. 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。
7. **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。
8. **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。



第 7 章

証明書

- の証明書管理 (85 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>/dcm/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

ステップ 1 SSH 端末を経由して DCNM サーバにログオンします。

ステップ 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.
```

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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'

```

ステップ 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
```

ステップ 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

ステップ 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。

ステップ 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.
```

ステップ 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。

ステップ 4 認証局によって署名された証明書を取得します。

ステップ 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。

ステップ 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。

ステップ 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#
```

ステップ 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#
```

ステップ 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'
```

ステップ 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。

- ステップ 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。

- ステップ 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

ステップ 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。

ステップ 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
```

ステップ 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。

ステップ 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#
```

ステップ 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。

ステップ 6

ステップ 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。

ステップ 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 にログインできる必要があります。

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

ステップ 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せん。

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。

ステップ 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
```

ステップ 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
```

ステップ 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。

ステップ 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
```

ステップ 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 confirms 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

ステップ 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。

ステップ 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
```

ステップ 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
```

ステップ 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
```

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 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

ステップ 1 SSH 端末を経由して DCNM サーバにログオンします。

ステップ 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。

ステップ 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。

ステップ 4 `dcnmweb.key` および `dcnmweb.crt` ファイルのバックアップをとります。

ステップ 5 復元する古いキーと証明書のペアを特定します。

ステップ 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。

ステップ 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。

ステップ 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。

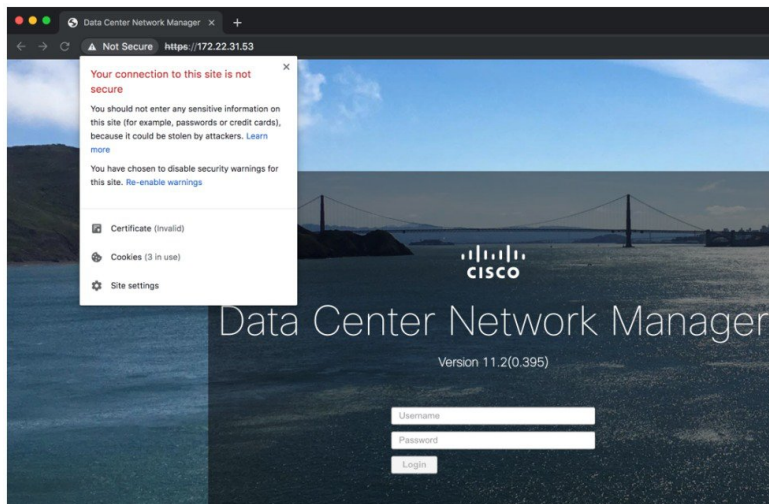
次のスニペットは、証明書を確認するための Chrome ブラウザバージョン 74.0.3729.169 の例です。

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。

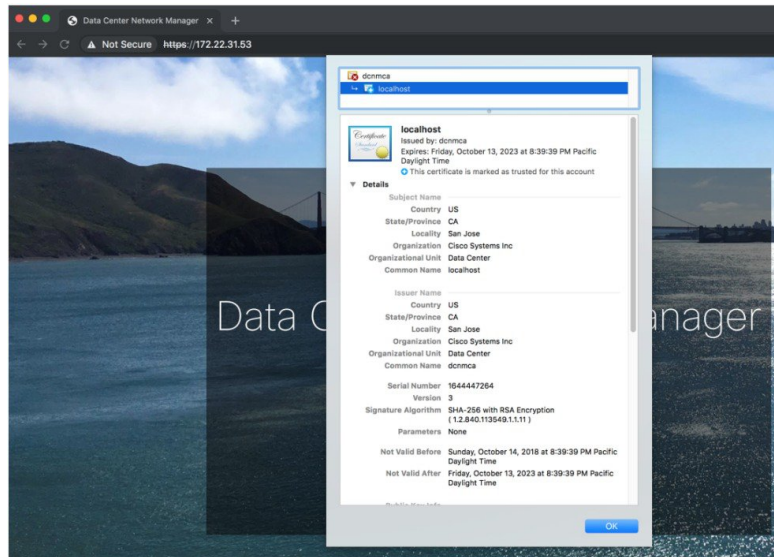
2. 証明書の種類に基づき、URL フィールドの左側のアイコンにロック アイコン [] またはアラート アイコン [] が表示されます。

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 8 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 101](#)
- [カスタム ファイアウォールの設定 \(104 ページ\)](#)

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 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 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 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 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 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 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。 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。 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 server.properties 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、メンテナンス期間に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 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。



CHAPTER 9

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。

- [Cisco DCNM サーバのセキュアなクライアント通信, on page 107](#)

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

ステップ 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。

ステップ 2 セカンダリ サーバでキーストアを検索します。

ステップ 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
```

ステップ 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 10 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 109](#)
- [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 111](#)
- [アプリケーションハイアベイラビリティ, on page 113](#)

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。
DCNM REST API および AMQP の場合、この移行は仮想 IP (VIP) アドレスを使用してアプライアンスのインターフェイス アドレスを非表示にするロードバランシング ソフトウェアによって行われます。
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 110](#)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

Cisco DCNMがネイティブHAモードで展開されている場合は、**appmgr restart all** または **appmgr restart ha-apps** を使用してアプリケーションを再起動しないことを推奨します。

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。DCNMHA 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/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、DCNMA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 クラスターの「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。

リポジットリ

すべてのリポジットリがリモートである必要があります。



第 11 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 5: Cisco DCNM ユーティリティ サービス

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

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

この章は、次の項で構成されています。

- [DCNM インストール後のネットワーク プロパティ \(119 ページ\)](#)
- [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 \(133 ページ\)](#)
- [ユーティリティ サービスの詳細, on page 138](#)
- [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 138](#)

DCNM インストール後のネットワーク プロパティ

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

- dcnm-mgmt network (eth0) インターフェイス

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

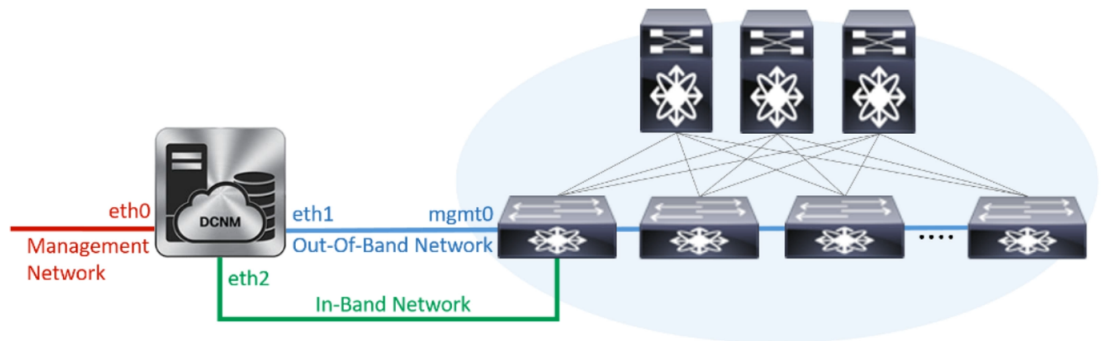
- enhanced-fabric-mgmt (eth1) インターフェイス

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

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

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

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



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



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

次の項で説明するように、パラメータを変更できます。

スタンドアロン モードの DCNM 上でネットワーク プロパティの変更



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

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

Procedure

ステップ 1 次のコマンドを使用して、コンソールのセッションを開始します。

appmgr update network-properties session start

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

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

ステップ 3 次のコマンドを使用して、変更を表示し確認します。

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

ステップ 4 変更を確認した後、次のコマンドを使用して設定を適用します。

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

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

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

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

```
dcnm# appmgr update network-properties session start

dcnm# appmgr update network-properties set ipv4 eth0 172.28.10.244 255.255.255.0
172.28.10.1
dcnm# appmgr update network-properties set ipv4 eth1 100.0.0.244 255.0.0.0
dcnm# appmgr update network-properties set ipv4 eth2 2.0.0.251 255.0.0.0 2.0.0.1
*****
WARNING: fabric/poap configuration may need to be changed
manually after changes are applied.
*****

dcnm# appmgr update network-properties session show changes
eth0 IPv4 addr 172.28.10.246/255.255.255.0 -> 172.28.10.244/255.255.255.0
eth1 IPv4 addr 1.0.0.246/255.0.0.0 -> 100.0.0.244/255.0.0.0
eth2 IPv4 addr 10.0.0.246/255.0.0.0 -> 2.0.0.251/255.0.0.0 2.0.0.1

dcnm# appmgr update network-properties session apply
*****
WARNING

Applications of both nodes of the DCNM HA system need to be stopped
for the changes to be applied properly.

PLEASE STOP ALL APPLICATIONS MANUALLY
*****

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
```

```

log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
server signaled
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave
the 'tentative' state
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave
the 'tentative' state
*****
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
*****

dcnm# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO:  Resource is stopped
Done.

Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
dcnm#

```

ネイティブ HA モードの DCNM 上でネットワーク プロパティの変更



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

次の手順で示されているように、同じ順番でコマンドを実行します。



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

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

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

Procedure

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

appmgr stop all

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

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

appmgr stop all

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

appmgr update network-properties session start

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

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

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

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

b) 次のコマンドを使用して、VIP IP アドレスを設定します。

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

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

c) 次のコマンドを使用して、ピア IP アドレスを設定します。

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

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

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

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

ステップ 5 スタンバイ ノードで、ステップ [ステップ 4, on page 123](#) で説明したコマンドを使用して、ネットワーク インターフェイスのパラメータを変更します。

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

appmgr update network-properties session apply

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

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

appmgr update network-properties session apply

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

appmgr start all

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

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

appmgr start all

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

appmgr update ssh-peer-trust

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

appmgr update ssh-peer-trust

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

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



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

```
[root@dcnm2 ~]# appmgr stop all
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.
Stopping and halting node rabbit@dcnm-dcnm2 ...
Note: Forwarding request to 'systemctl enable rabbitmq-server.service'.
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
[root@dcnm2 ~]#

[root@dcnm1 ~]# appmgr stop all
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.
Stopping and halting node rabbit@dcnm1 ...
Note: Forwarding request to 'systemctl enable rabbitmq-server.service'.
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
```

```

Stopped Application Framework...
[root@dcnm-1 ~]#

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

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

[root@dcnm1 ~]# appmgr update network-properties set ipv4 eth0 172.28.10.244 255.255.255.0
172.28.10.1
[root@dcnm1 ~]# appmgr update network-properties set ipv4 eth1 1.0.0.244 255.0.0.0 1.0.0.1
*****
WARNING: fabric/poap configuration may need to be changed
manually after changes are applied.
*****
[root@dcnm1 ~]# appmgr update network-properties set ipv4 eth2 2.0.0.244 255.0.0.0 2.0.0.1
[root@dcnm1 ~]# appmgr update network-properties set ipv4 peer0 172.29.10.238
[root@dcnm1 ~]# appmgr update network-properties set ipv4 peer1 1.0.0.238
[root@dcnm1 ~]# appmgr update network-properties set ipv4 peer2 2.0.0.238
[root@dcnm1 ~]# appmgr update network-properties set ipv4 vip0 172.28.10.239 255.255.255.0
[root@dcnm1 ~]# appmgr update network-properties set ipv4 vip1 1.0.0.239 255.0.0.0
[root@dcnm1 ~]# appmgr update network-properties set ipv4 vip2 2.0.0.239 255.0.0.0
[root@dcnm1 ~]# appmgr update network-properties set hostname local dcnm3.cisco.com
[root@dcnm1 ~]# appmgr update network-properties set hostname peer dcnm4.cisco.com
[root@dcnm1 ~]# appmgr update network-properties set hostname vip dcnm5.cisco.com
[root@dcnm1 ~]#

[root@dcnm2 ~]# appmgr update network-properties set ipv4 eth0 172.28.10.238 255.255.255.0
172.28.10.1
[root@dcnm2 ~]# appmgr update network-properties set ipv4 eth1 1.0.0.238 255.0.0.0 1.0.0.1
*****
WARNING: fabric/poap configuration may need to be changed
manually after changes are applied.
*****
[root@dcnm2 ~]# appmgr update network-properties set ipv4 eth2 2.0.0.238 255.0.0.0 2.0.0.1
[root@dcnm2 ~]# appmgr update network-properties set ipv4 peer0 172.29.10.244
[root@dcnm2 ~]# appmgr update network-properties set ipv4 peer1 1.0.0.244
[root@dcnm2 ~]# appmgr update network-properties set ipv4 peer2 2.0.0.244
[root@dcnm2 ~]# appmgr update network-properties set ipv4 vip0 172.28.10.239 255.255.255.0
[root@dcnm2 ~]# appmgr update network-properties set ipv4 vip1 1.0.0.239 255.0.0.0
[root@dcnm2 ~]# appmgr update network-properties set ipv4 vip2 2.0.0.239 255.0.0.0
[root@dcnm2 ~]# appmgr update network-properties set hostname local dcnm3.cisco.com
[root@dcnm2 ~]# appmgr update network-properties set hostname peer dcnm4.cisco.com
[root@dcnm2 ~]# appmgr update network-properties set hostname vip dcnm5.cisco.com
[root@dcnm2 ~]#

[root@dcnm2 ~]#
[root@dcnm1 ~]# appmgr update network-properties session show changes
eth0 IPv4 addr      172.28.10.246/255.255.255.0    -> 172.28.10.244/255.255.255.0
eth1 IPv4 addr      1.0.0.246/255.0.0.0           -> 1.0.0.244/255.0.0.0
eth1 IPv4 GW        /                               -> 1.0.0.1
eth2 IPv4 addr      /                               -> 2.0.0.244/255.0.0.0
eth2 IPv4 GW        /                               -> 2.0.0.1
Hostname            dcnm1.cisco.com                -> dcnm3.cisco.com
eth0 VIP            172.28.10.248/24                -> 172.28.10.239/24
eth1 VIP            1.0.0.248/8                     -> 1.0.0.239/8
eth2 VIP            /                               -> 2.0.0.239/8
Peer eth0 IP        172.28.10.247                  -> 172.29.10.238
Peer eth1 IP        1.0.0.247                      -> 1.0.0.238
Peer eth2 IP        /                               -> 2.0.0.238
Peer hostname       dcnm2.cisco.com                 -> dcnm4.cisco.com
VIP hostname        dcnm6.cisco.com                 -> dcnm5.cisco.com

```

ネイティブ HA モードの DCNM 上でネットワーク プロパティの変更

```
[root@dcnm1 ~]# appmgr update network-properties session show config
===== Current configuration =====
Hostname dcnm1.cisco.com
NTP Server      1.ntp.esl.cisco.com
DNS Server      171.70.168.183,1.0.0.246
eth0 IPv4 addr  172.28.10.246/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr  1.0.0.246/255.0.0.0
eth1 IPv4 GW
eth1 IPv6 addr
eth1 IPv6 GW
eth2 IPv4 addr  /
eth2 IPv4 GW
eth2 IPv6 addr
eth2 IPv6 GW
Peer hostname  dcnm2.cisco.com
Peer eth0 IP   172.28.10.247
Peer eth1 IP   1.0.0.247
Peer eth2 IP
Peer eth0 IPv6
Peer eth1 IPv6
eth0 VIP       172.28.10.248/24
eth1 VIP       1.0.0.248/8
eth2 VIP       /
eth0 VIPv6    /
eth1 VIPv6    /
VIP hostname  dcnm6.cisco.com

===== Session configuration =====
Hostname dcnm3.cisco.com
NTP Server      1.ntp.esl.cisco.com
DNS Server      171.70.168.183,1.0.0.246
eth0 IPv4 addr  172.28.10.244/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr  1.0.0.244/255.0.0.0
eth1 IPv4 GW    1.0.0.1
eth1 IPv6 addr
eth1 IPv6 GW
eth2 IPv4 addr  2.0.0.244/255.0.0.0
eth2 IPv4 GW    2.0.0.1
eth2 IPv6 addr
eth2 IPv6 GW
Peer hostname  dcnm4.cisco.com
Peer eth0 IP   172.29.10.238
Peer eth1 IP   1.0.0.238
Peer eth2 IP   2.0.0.238
Peer eth0 IPv6
Peer eth1 IPv6
eth0 VIP       172.28.10.239/24
eth1 VIP       1.0.0.239/8
eth2 VIP       2.0.0.239/8
eth0 VIPv6    /
eth1 VIPv6    /
VIP hostname  dcnm5.cisco.com
[root@dcnm1 ~]#

[root@dcnm2 ~]# appmgr update network-properties session show changes
eth0 IPv4 addr  172.28.10.247/255.255.255.0    ->    172.28.10.238/255.255.255.0
eth1 IPv4 addr  1.0.0.247/255.0.0.0              ->    1.0.0.238/255.0.0.0
```

```

eth1 IPv4 GW -> 1.0.0.1
eth2 IPv4 addr / -> 2.0.0.238/255.0.0.0
eth2 IPv4 GW -> 2.0.0.1
Hostname dcnm2.cisco.com -> dcnm4.cisco.com
eth0 VIP 172.28.10.248/24 -> 172.28.10.239/24
eth1 VIP 1.0.0.248/8 -> 1.0.0.239/8
eth2 VIP / -> 2.0.0.239/8
Peer eth0 IP 172.28.10.246 -> 172.29.10.244
Peer eth1 IP 1.0.0.246 -> 1.0.0.244
Peer eth2 IP -> 2.0.0.244
Peer hostname dcnm1.cisco.com -> dcnm3.cisco.com
VIP hostname dcnm6.cisco.com -> dcnm5.cisco.com
[root@dcnm2 ~]# appmgr update network-properties session show configuration
===== Current configuration =====
Hostname dcnm2.cisco.com
NTP Server 1.ntp.esl.cisco.com
DNS Server 171.70.168.183,1.0.0.247
eth0 IPv4 addr 172.28.10.247/255.255.255.0
eth0 IPv4 GW 172.28.10.1
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr 1.0.0.247/255.0.0.0
eth1 IPv4 GW
eth1 IPv6 addr
eth1 IPv6 GW
eth2 IPv4 addr /
eth2 IPv4 GW
eth2 IPv6 addr
eth2 IPv6 GW
Peer hostname dcnm1.cisco.com
Peer eth0 IP 172.28.10.246
Peer eth1 IP 1.0.0.246
Peer eth2 IP
Peer eth0 IPv6
Peer eth1 IPv6
eth0 VIP 172.28.10.248/24
eth1 VIP 1.0.0.248/8
eth2 VIP /
eth0 VIPv6 /
eth1 VIPv6 /
VIP hostname dcnm6.cisco.com

===== Session configuration =====
Hostname dcnm4.cisco.com
NTP Server 1.ntp.esl.cisco.com
DNS Server 171.70.168.183,1.0.0.247
eth0 IPv4 addr 172.28.10.238/255.255.255.0
eth0 IPv4 GW 172.28.10.1
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr 1.0.0.238/255.0.0.0
eth1 IPv4 GW 1.0.0.1
eth1 IPv6 addr
eth1 IPv6 GW
eth2 IPv4 addr 2.0.0.238/255.0.0.0
eth2 IPv4 GW 2.0.0.1
eth2 IPv6 addr
eth2 IPv6 GW
Peer hostname dcnm3.cisco.com
Peer eth0 IP 172.29.10.244
Peer eth1 IP 1.0.0.244
Peer eth2 IP 2.0.0.244
Peer eth0 IPv6
Peer eth1 IPv6

```

ネイティブ HA モードの DCNM 上でネットワーク プロパティの変更

```

eth0 VIP          172.28.10.239/24
eth1 VIP          1.0.0.239/8
eth2 VIP          2.0.0.239/8
eth0 VIPv6        /
eth1 VIPv6        /
VIP hostname      dcnm5.cisco.com
[root@dcnm2 ~]#

[root@dcnm1 ~]# appmgr update network-properties session apply
*****
                          WARNING
Applications of both nodes of the DCNM HA system need to be stopped
for the changes to be applied properly.
                          PLEASE STOP ALL APPLICATIONS MANUALLY
*****

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
server signaled
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave
the 'tentative' state
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave
the 'tentative' state
*****
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
*****
Please run 'appmgr update ssh-peer-trust' on the peer node.
*****
[root@dcnm1 ~]#

[root@dcnm2 ~]# appmgr update network-properties session apply
*****
                          WARNING
Applications of both nodes of the DCNM HA system need to be stopped
for the changes to be applied properly.
                          PLEASE STOP ALL APPLICATIONS MANUALLY
*****

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
afwnetplugin:0.1
server signaled
*****
Please run 'appmgr start afw; appmgr start all' to restart your nodes.

```

```
*****
*****
Please run 'appmgr update ssh-peer-trust' on the peer node.
*****
[root@dcnm2 ~]#
```

Step 7

```
[root@dcnm1 ~]# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO: Resource is stopped
Done.
Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
[root@dcnm1 ~]#
```

Waiting for dcnm1 to become active again.

```
[root@dcnm2 ~]# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO: Resource is stopped
Done.
Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
[root@dcnm2 ~]#
```

```
[root@dcnm1 ~]# appmgr update ssh-peer-trust
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh -o 'StrictHostKeyChecking=no'
'172.28.10.245'"
and check to make sure that only the key(s) you wanted were added.

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh -o 'StrictHostKeyChecking=no' '100.0.0.245'"
and check to make sure that only the key(s) you wanted were added.

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh -o 'StrictHostKeyChecking=no'
```

DCNM インストール後に DCNM サーバパスワードを変更する

```
'dcnm2.cisco.com'"
and check to make sure that only the key(s) you wanted were added.

[root@dcnm1 ~]#

[root@dcnm2 ~]# appmgr update ssh-peer-trust
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh -o 'StrictHostKeyChecking=no'
'172.28.10.244'"
and check to make sure that only the key(s) you wanted were added.

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh -o 'StrictHostKeyChecking=no' '100.0.0.244'"
and check to make sure that only the key(s) you wanted were added.

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh -o 'StrictHostKeyChecking=no'
'dcnm1.cisco.com'"
and check to make sure that only the key(s) you wanted were added.

[root@dcnm2 ~]#
```

DCNM インストール後に DCNM サーバパスワードを変更する

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

インストール後にパスワードを変更するには、次の手順を実行します。

Procedure

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

すべてのアプリケーションが稼働を停止するまで待ちます。

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

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

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

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

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

スタンドアロンセットアップで DCNM データベース パスワードを変更する

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

Procedure

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

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

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

プロンプトで新しいパスワードを入力します。

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

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

Example

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

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

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

Procedure

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

Example

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

```
dcnm1# appmgr stop all
dcnm2# appmgr stop all

dcnm1# appmgr change_pwd db <<new-password>>
dcnm2# appmgr change_pwd db <<new-password>>

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

スタンドアロンセットアップからネイティブ HA セットアップへの変換

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

始める前に

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

```
dcnm# appmgr show version

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

手順

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

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

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

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

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

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

初期メッセージが表示されます。

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

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

- b) [Cisco DCNM インストーラ (Cisco DCNM Installer)] 画面で、**[新規インストール - HA セカンダリ (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。

[Next] をクリックします。

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

(注) すべてのパスワードは、プライマリ ノードの設定時に指定したパスワードと同じである必要があります。

- e) **[システム設定 (System Settings)]** で、DCNM アプライアンスの設定を行います。

- **[完全修飾ホスト名 (Fully Qualified Hostname)]** フィールドで、RFC1123 セクション 2.1 の通りに、完全修飾ドメイン名 (FQDN) のホスト名を入力します。数字のみのホスト名はサポートされていません。

- **[DNS サーバ アドレス (DNS Server Address)]** フィールドで、DNS IP アドレスを入力します。

リリース 11.2(1) から、IPv6 アドレスを使用した DNS サーバも設定できます。

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

- **[NTP サーバ アドレス リスト (NTP Server Address List)]** フィールドでは、NTP サーバの IP アドレスを入力します。

値は IP または IPv6 アドレスか RFC 1123 に準拠した名前である必要があります。

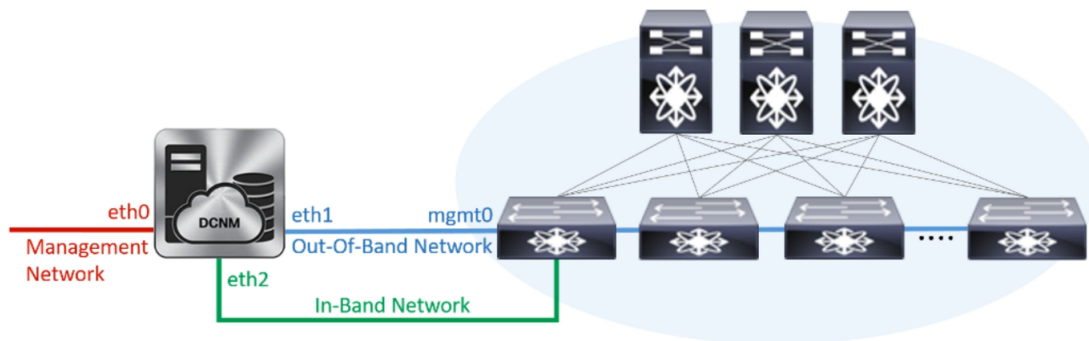
リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。

- **タイムゾーン** ドロップダウン リストから、DCNM を展開しているタイムゾーンを選択します。

[Next] をクリックします。

- f) **[ネットワーク設定 (Network Settings)]** タブで、DCNM Web UI に到達するために使用されるネットワーク パラメータを構成します。

図 8: Cisco DCNM 管理ネットワーク インターフェイス



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

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

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

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

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

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

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

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

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

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

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

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

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

[Next] をクリックします。

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

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

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

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

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

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

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

[次へ (Next)] をクリックします。

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

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

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

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

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

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

次のタスク

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

アクティブノード (古いスタンダオンノード) :

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

スタンバイノード (新しく展開されたノード) :

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

ユーティリティ サービスの詳細

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

電源オン自動プロビジョニング

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

- DHCP サーバ

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

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

**Note**

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

- リポジトリ

TFTP サーバは、POAP に使用される起動スクリプトをホストします。

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

アプリケーションとユーティリティ サービスの管理

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

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

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



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

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



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

このセクションの内容は次のとおりです。

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

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



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

Procedure

ステップ 1 SSH セッションを開きます。

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

ステップ 2 次のコマンドを使用して、ステータスをチェックします。

appmgr status all

Example:

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

```
dcnm# appmgr status all
```

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

```
DCNM Status
```

```
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
```

ユーティリティ サービスの停止、開始、リセット

```

=== ===== == == ===== ===== ===== = ===== ===== =====
27724 root      20  0  12.2g  3.9g 49328 S   0.0 16.6 60:24.10 java

Elasticsearch Status

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

Telemetry Manager Status

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

PMN Telemetry Status

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

TFTP Status

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

DHCP Status

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

AMQP Status

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

```

ユーティリティ サービスの停止、開始、リセット

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

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

```

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

```

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

```

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

```

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

```

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

```



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

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

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



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

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



第 12 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 \(143 ページ\)](#)

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

リモート認証が有効な場合、POAP ユーザー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 Cisco DCNM Native 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。

