



SAN 展開リリース 11.3(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：2019年12月20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.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org>)

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

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: <http://www.cisco.com/go/trademarks>. 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. (1110R)

© 2019 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	概要 1
	はじめに 1
	Installation Options 3
	展開オプション 3
	Cisco DCNM のアップグレード 4
	システム要件 5

第 2 章	注意事項と制約事項 13
	注意事項と制約事項 13

第 3 章	前提条件 15
	一般的な前提条件 15
	はじめる前に 15
	初回のセットアップルーチン 17
	スイッチを設定するための準備 17
	デフォルトのログイン 19
	セットアップ オプション 19
	セットアップ情報の指定 20
	帯域外管理の設定 20
	帯域内管理の設定 25
	setup コマンドの使用法 28
	Cisco MDS 9000 ファミリのスイッチの始動 28
	スイッチへのアクセス 29
	Linux で DCNM をインストールするための前提条件 30

Linux で DCNM をインストールするための前提条件	31
ウイルス対策の除外対象	32
DCNM サーバの Oracle データベース	32
Oracle SQLPlus コマンドライン ツール	33
init.ora ファイル	33
Oracle データベースのバックアップ	33
Oracle データベースの準備	34
Oracle へのログイン	34
SYSTEM テーブルスペースの拡張	35
セッション数とプロセス数の 150 への増加	35
開いているカーソルの数の 1000 への増加	36
コマンドプロンプトを使用して Oracle DB ユーザーを作成する	37
SCAN 機能タイプ DB を使用して Oracle RAC に接続する	37
フェデレーションセットアップ用のデータベース	38
バックアップおよび復元用のリモート Oracle データベース ユーティリティ スクリプト	38
バックアップおよび復元用のローカル PostgreSQL データベース ユーティリティ スクリプト	39

第 4 章

Cisco DCNM のインストール	41
Windows への Cisco DCNM のインストール	41
Windows で Cisco DCNM をアンインストールする	41
Cisco DCNM Windows インストーラおよびプロパティ ファイルのダウンロード	42
GUI を使用した Windows への Cisco DCNM のインストール	43
GUI を使用したサーバフェデレーション環境への Cisco DCNM Windows のインストール	47
サイレントインストールを通して Cisco DCNM Windows をインストールする	48
Linux への Cisco DCNM のインストール	50
Linux への Cisco DCNM のアンインストール	50
Cisco DCNM Linux インストーラおよびプロパティ ファイルのダウンロード	51
GUI を使用した Linux への Cisco DCNM のインストール	52
GUI を使用したサーバフェデレーション環境への Cisco DCNM Linux のインストール	55
サイレントインストールを通して Cisco DCNM Linux をインストールする	56

オープン仮想アプライアンスで DCNM をインストールする	58
オープン仮想アプライアンス ファイルのダウンロード	58
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	59
スタンドアロンモードでの Cisco DCNM OVA のインストール	64
ネイティブ HA モードでの Cisco DCNM OVA のインストール	68
ISO 仮想アプライアンスで DCNM をインストールする	77
ISO 仮想アプライアンス ファイルのダウンロード	77
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	78
KVM 上での DCNM ISO 仮想アプライアンスのインストール	85
スタンドアロンモードでの Cisco DCNM ISO のインストール	87
ネイティブ HA モードで Cisco DCNM ISO をインストールする	91
SAN クライアントおよびデバイス マネージャの起動	100
Web UI からの SAN Client および Device Manager の起動	100
DCNM サーバから SAN クライアントおよびデバイス マネージャを起動する	100
SSL が有効な Windows 展開のための DCNM SAN からの DCNM SAN クライアントの起動	101
SSL が有効な Linux 展開のための DCNM SAN からの DCNM SAN クライアントの起動	103
SSL が有効な OVA/ISO 展開のための DCNM SAN からの DCNM SAN クライアントの起動	105
第 5 章 Cisco DCNM のアップグレード	107
Cisco DCNM のアップグレード	107
CA 署名済み証明書の保持	108
Windows で Cisco SAN にアップグレードする	109
Windows で Cisco DCNM をアンインストールする	109
GUI を使用した Cisco DCNM Linux のアップグレード	110
GUI を使用した Cisco DCNM Windows フェデレーションのアップグレード	111
サイレント インストールを通して Cisco DCNM Windows をアップグレードする	111
サイレントインストールを通して Cisco DCNM Windows フェデレーションをアップグレードする	112
Linux で Cisco SAN にアップグレードする	113

Linux への Cisco DCNM のアンインストール	113
GUI を使用した Cisco DCNM Linux のアップグレード	114
GUI を使用した Cisco DCNM Linux フェデレーションのアップグレード	115
サイレントインストールを通して Cisco DCNM Linux をアップグレードする	116
サイレントインストールを通して Cisco DCNM Linux フェデレーションをアップグレードする	116
OVA/ISO での Cisco SAN へのアップグレード	118
10.4(x) SAN OVA/ISO/Windows から新しい DCNM 11.3(1) OVA/ISO への PM データ移行	119
11.1(1) および 11.2(1) 以降から 11.3(1) OVA/ISO の新規インストールへの PM データの移行	120
11.1(1) および 11.2(1) Linux 以降から 11.3(1) OVA/ISO の新規インストールへの PM データの移行	123

第 6 章

ファイアウォール背後での Cisco DCNM の実行	127
ファイアウォール背後での Cisco DCNM の実行	127
カスタム ファイアウォールの設定	139

第 7 章

ユーザーとスキーマ	143
新規ユーザーの作成	143
既存ユーザーの新しくスキーマを作成する	144

第 8 章

証明書	145
CA 署名済み証明書の保持	145
Cisco DCNM の証明書を設定する	146
自己署名 SSL 証明書の使用	146
Windows でキーツールを使用して証明書要求が生成される場合 SSL 証明書を使用する	147
Linux でキーツールを使用して証明書要求が生成されたときに SSL 証明書を使用する	148
Linux で OpenSSL を使用して証明書要求が生成される場合 SSL 証明書を使用する	149
証明書の管理 (Certificate Management)	150
証明書管理のベスト プラクティス	151

インストールされた証明書の表示	151
CA 署名付き証明書のインストール	152
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	153
アップグレード後に証明書を復元する	154
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	155
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	156
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	157
インストールした証明書の確認	158

 第 9 章

Cisco DCNM サーバのセキュアなクライアント通信	161
Cisco DCNM サーバのセキュアなクライアント通信	161
RHEL または Windows 上のフェデレーションの Cisco DCNM で SSL/HTTPS を有効化する	161

 第 10 章

DCNM 展開後にユーティリティ サービスを管理する	163
DCNM インストール後のネットワーク プロパティ	163
スタンドアロンモードの DCNM 上でネットワーク プロパティの変更	164
DCNM インストール後に DCNM サーバパスワードを変更する	166
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	167
ユーティリティ サービスの詳細	167
ネットワーク管理	167
オーケストレーション	168
電源オン自動プロビジョニング	168
アプリケーションとユーティリティ サービスの管理	169
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	169
ユーティリティ サービスの停止、開始、リセット	170
IPv6 の SFTP サーバアドレスの更新	171



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 3](#)
- [展開オプション, on page 3](#)
- [Cisco DCNM のアップグレード, on page 4](#)
- [システム要件 \(5 ページ\)](#)

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 MDS 9000 スイッチの完全な設定とステータスモニタリング機能に加えて、Cisco DCNM-SAN は強力なちゃんえるトラブルシューティングツールを提供します。深い健全性と設定の分析機能では、固有の MDS 9000 スイッチ機能 (ファイバチャネルおよびトレースルート) を活用します。

リリース 11.1(1) から、Cisco DCNM では Cisco UCS ブレードサーバもモニタできるようになりました。

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 Server

Cisco DCNM-SAN Server コンポーネントは、Cisco DCNM-SAN を実行する前に起動する必要があります。Cisco DCNM-SAN サーバはサービスとしてインストールされます。このサービスを管理するには、[Control Panel] の [Windows Services] を使用します。Cisco DCNM-SAN Server は物理および論理ファブリックを検出し、SNMP トラップ、Syslog メッセージ、および Performance Manager しきい値イベントをリッスンします。

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。MDS9000 ファブリックも設定できます。

Cisco DCNM-SAN クライアント

DCNM-SAN Client では、Cisco MDS 9000 ファミリースイッチ、サードパーティ製スイッチ、ホスト、ストレージデバイスなどのネットワーク ファブリックのマップが表示されます。Cisco DCNM-SAN クライアントは、Cisco DCNM SAN 機能にアクセスするために複数のメニューを提供します。

Device Manager

デバイス マネージャは、Cisco DCNM Web UI に埋め込まれています。スイッチが検出された後、[インベントリ (Inventory)] > [スイッチ (Switches)] > [デバイス マネージャ (Device Manager)] に移動し、デバイス マネージャを起動します。

Cisco DCNM-SAN は、デバイス マネージャを自動的にインストールします。Device Manager は、1 台のスイッチに対し 2 つのビューを表示します。

- **Device View** : スイッチ設定を図にして示し、統計情報と設定情報へのアクセスを提供します。
- **Summary View** : スイッチ、ファイバチャネル、IP 隣接デバイスの xE ポート (スイッチ間リンク)、Fx ポート (ファブリック ポート)、Nx ポート (接続されたホストとストレージ) の概要を表示します。表を作成したり、印刷したり、タブ区切りの形式でファイルに概要やリアルタイムの統計情報を保存できます。

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。パフォーマンス マネージャは、伸縮可能な検索時間シリーズ データベースにデータを保存します。DCNM は伸縮可能な検索への API アクセスをサポートしていません。

Installation Options

Cisco DCNM ソフトウェア イメージは、Cisco DCNM インストーラ、しよめ証明書、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。

DCNM Windows インストーラ

このインストーラは、実行可能ファイル (.exe) として使用できます。

DCNM Linux インストーラ

このインストーラはバイナリ (.bin) ファイルとして使用できます。

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。

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。

外部 Oracle を備えたスタンドアロン

セットアップに多くのスイッチがある場合、またはセットアップが一定時間にわたって増加すると予想される場合は、外部 Oracle サーバを使用することを推奨します。この展開モードでは、デフォルトのインストールセットアップが必要です。その後、外部 Oracle を使用するように DCNM を設定する手順を実行します。スケーラビリティの詳細については、https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/11_0_1/scalability_guide/b_scale_guide_dcnm_11.html を参照してください。

DCNM フェデレーション

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。DCNM フェデレーションセットアップ内のすべてのノードは、多くの SAN デバイスのグループを管理できます。単一のクライアントインターフェイスは、すべてのデバイスを管理できます。フェデレーションモードは、復元力とスケーラビリティのために使用されます。これにより、20,000 個の FC ポートをモニタできます。DCNM Windows および Linux インストーラは、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つように、フェデレーションモードで展開できます。Cisco DCNM-SAN フェデレーションの場合、データベース URL (プロパティ) は、フェデレーション内のすべての Cisco DCNM-SAN ノードで同じである必要があります。

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。ただし、SAN OVA/ISO のアップグレードパスはありません。

リリース 11.3(1) 以降では、Cisco DCNM OVA および ISO は SAN 機能に対してサポートされています。

次の表は、リリース 11.3(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: Cisco DCNM SAN 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 11.3(1) にアップグレードするアップグレードタイプ
11.2(1)	<p>Windows 向け：インラインアップグレード</p> <p>Linux向け：インラインアップグレード</p> <p>OVA/ISO 向け：</p> <ol style="list-style-type: none"> 新しい 11.3(1) SAN のみのインストール。 パフォーマンス マネージャの収集を停止します。 <p>Note 古いパフォーマンス マネージャ データは、11.3(1) の既存のパフォーマンス マネージャ データを置き換えます。</p>

現在のリリース番号	リリース 11.3(1) にアップグレードするアップグレードタイプ
11.1(1)	Windows 向け：インラインアップグレード Linux向け：インラインアップグレード OVA\ISO 向け： <ol style="list-style-type: none"> 新しい 11.3(1) SAN のみのインストール。 パフォーマンス マネージャの収集を停止します。 <p>Note 古いパフォーマンス マネージャ データは、11.3(1) の既存のパフォーマンス マネージャ データを置き換えます。</p>
10.4(2) OVA 10.4 (1) OVA	11.3(1) OVA\ISO 向け： <ol style="list-style-type: none"> 新しい 11.3(1) SAN のみのインストール。 パフォーマンス マネージャの収集を停止します。 <p>Note 古いパフォーマンス マネージャ データは、11.3(1) の既存のパフォーマンス マネージャ データを置き換えます。</p>

システム要件

ここでは、Cisco DCNM リリース 11.3(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。

Java の要件

Cisco DCNM サーバは、次のディレクトリに JRE 11.0.2 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 11.3(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。

- SAN 展開：
 - Microsoft Windows 2016
 - Microsoft Windows 2012 R2
 - Red Hat Enterprise Linux リリース 7.3、7.4、7.6、7.7

- CentOS Linux リリース 7.6 と統合したオープン仮想アプライアンス (OVA)
- CentOS Linux リリース 7.6 と統合した ISO 仮想アプライアンス (ISO)

Cisco DCNM リリース 11.3(1) では、次のデータベースをサポートします。

- Oracle11g Express (XE)、標準、エンタープライズ エディション、および Oracle 11g Real Application Clusters (RAC)
- Oracle 12c エンタープライズ エディション (従来)—(非プラグ接続型インストール)



(注) Cisco DCNM リリース 11.3(1) では、Oracle 12c プラグ接続型データベースバージョンのインストールはサポートされていません。

- Oracle 12c RAC (非プラグ接続型インストール)
- PostgreSQL 9.4.5



(注) データベース サイズは、パフォーマンス マネージャ 収集が有効になっている DCNM が管理するノード数およびポート数に応じて増加します。データベースのサイズを制限することはできません。Oracle データベースを選択する場合、表スペースの制限の問題により、Oracle SE またはエンタープライズ エディションを使用することをお勧めします。



(注) メンテナンス、トラブルシューティング、リカバリを含む Oracle データベースに関連するすべてのサポートに責任を負います。毎日または毎週など、定期的にデータベースのバックアップを取得し、すべてのデータが保持されているようにすることをお勧めします。



(注) ISO/OVA i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。

Cisco DCNM リリース 11.2(1) から、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 ¹
Cisco UCS C240M4	UCSC-C240-M4S	RAID 運用のために Cisco ハードウェア RAID コントローラ [UCSC-MRAID12G-1GB/2 GB] を備えた 32G / 500G 16-vCPU コア (小規模)

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 ¹
Cisco UCS C240M4	UCSC-C240-M4L	RAID 運用のために Cisco ハードウェア RAID コントローラ [UCSC-MRAID12G-GB/2 GB] を備えた 32G / 500G 16-vCPU コア (大規模)
Cisco UCS C240 M5S	UCSC-C240-M5SX	RAID 運用のために Cisco ハードウェア RAID コントローラ [UCSC-SAS-M5 を備えた 32G / 500G 16-vCPU コア (小規模)
Cisco UCS C220 M5L	UCSC-C220-M5L	32G / 500G RAID 運用のために Cisco ハードウェア RAID コントローラ [UCSC-SAS-M5 を備えた 16-vCPU コア (小規模)

¹ 16vCPUs、64G RAM、および 500 GB のハードディスクを搭載した Cisco DCNM コンピューティング ノードをインストールします。32G RAM サーバでコンピューティング ノードをインストールしないようにしてください。



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

Cisco DCNM の VMware Snapshot サポート

スナップショットでは、スナップショットを撮影した時点の仮想マシン全体の状態をキャプチャします。仮想マシンの電源をオンにして、電源をオフにすると、スナップショットを取得できます。



(注) vCenter サーバは、Cisco DCNM OVA インストーラを展開するために必須です。

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 チェック ボックスが選択されていないことを示すスナップショットに注意してください。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.11.3.1 ×

Name VM Snapshot taken powered on 12/8/2019

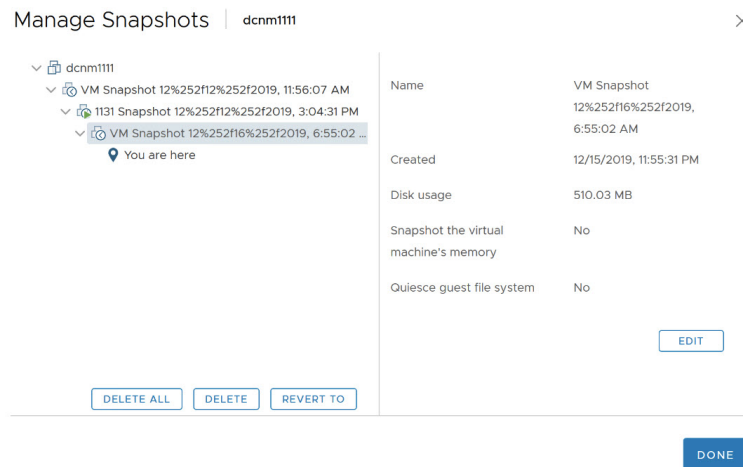
Description

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。



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。

表 2: 従来の LAN、LAN ファブリック、SAN OVA 展開のスナップショット サポート

VMware vSphere Hypervisor (ESXi)	6.0	6.5	6.7	6.7 更新 3
VMware vCenter サーバ	6.0	6.5	6.7	6.7 更新 3

サーバリソース要件

配置	展開タイプ	小規模 (Lab または POC)	大規模 (生産)	大規模 (生産)	コンピューティング
SAN	Windows	CPU : 8 vCPUs RAM : 24 GB DISK : 500 GB	CPU : 16 vCPUs RAM : 32 GB DISK : 500 GB	N/A	N/A
	Windows (スタンドアロンまたは VM)	CPU : 8 vCPUs RAM : 24 GB DISK : 500 GB	CPU : 16 vCPUs RAM : 32 GB DISK : 500 GB	SAN Insights を使用 : • CPU : 32 vCPUs • RAM : 128 GB • DISK : 2 TB	N/A
	• OVA スタンドアロン • ISO スタンドアロン	CPU : 8 vCPUs RAM : 24 GB DISK : 500 GB	CPU : 16 vCPUs RAM : 32 GB DISK : 500 GB	CPU : 32 vCPUs RAM : 128 GB DISK : 2 TB (SAN Insights を使用)	N/A



(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。

root パーティションに十分なディスクスペースがあることを確認するか、インストールまたはアップグレード中に /tmp ディレクトリが取り付け可能な別のディスクの取り付けます。

DCNM セットアップにディスクスペースを追加できます。SSH を使用して DCNM サーバにログオンします。 **appmgr system scan-disks-and-extend-fs** コマンドを使用して、ディスク ファイルシステムを拡張します。



- (注)
- リリース 11.3(1) から、Cisco DCNM Windows 展開では、SAN Insights 機能はサポートされていません。
 - Cisco DCNM 小規模展開では、SAN Insights 機能はサポートされていません。
 - 2 TB のディスク スペースがある中規模展開で SAN Insights 機能を使用できます。
 - フェデレーション ノードはそれぞれ 3 つの大規模な設定ノードで構成されています。
 - Cisco DCNM リリース 11.2(1) 以降では、プライマリ ノードからのみフェデレーション ノードを同期します。

クライアント要件

Cisco DCNM SAN デスクトップクライアントおよび Cisco デバイス マネージャは、Microsoft Windows 10、Microsoft Windows 2012、Microsoft Windows 2016、Red Hat Linux をサポートします。次の表に、これらのクライアントシステムの最小ハードウェア要件を示します。

表 3: クライアントのハードウェア要件

ハードウェア	最小要件
RAM (空き)	6 GB 以上
CPU 速度	3 GHz 以上の速さ
ディスク容量 (空き容量)	20 GB

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。

一部の Cisco DCNM 機能はライセンスが必要です。ライセンス付与されている機能を使用する前に、各 Nexus 管理または MDS 管理プラットフォームに Cisco DCNM ライセンスをインストールする必要があります。DCNM のライセンスに関する詳細は、https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/11_x/licensing/cisco_dcnm_licensing_guide_11_x.html を参照してください。

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 79.0.3945.79
- Mozilla Firefox バージョン 71.0 (32/64 ビット)
- Microsoft Internet Explorer バージョン 11.706 更新バージョン 11.0.120

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 11.3(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 4: 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 • 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 および Cisco DCNM-SAN サーバ暗号化 : 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 13](#)

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。

新規インストール

- Windows および Linux インストーラの場合、インストーラはシステムに Cisco DCNM-SAN および Cisco SMI-S エージェントをインストールします。
- リリース 11.3(1) から、OVA および ISO に Cisco DCNM SAN 展開をインストールできます。

アップグレード

- Windows および Linux インストーラの場合、デフォルトは最新の Cisco DCNM バージョンにアップグレードすることです。
- Network Insights アプリケーションを実行する必要がある場合、3 個のコンピューティングノードをインストールする必要があります。



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。

- [一般的な前提条件, on page 15](#)
- [Linux で DCNM をインストールするための前提条件, on page 30](#)
- [Linux で DCNM をインストールするための前提条件, on page 31](#)
- [DCNM サーバの Oracle データベース, on page 32](#)
- [バックアップおよび復元用のリモート Oracle データベース ユーティリティ スクリプト, on page 38](#)
- [バックアップおよび復元用のローカル PostgreSQL データベース ユーティリティ スクリプト, on page 39](#)

一般的な前提条件

この項では、次のトピックについて取り上げます。

はじめる前に

Cisco DCNM をインストールする前に、Cisco DCNM システムで次の前提条件が満たされていることを確認します。

- Cisco DCNM をインストールする前に、ホスト名が次の場所にあるホスト ファイルの IP アドレスにマッピングされていることを確認します。
 - Microsoft Windows : `C:\WINDOWS\system32\drivers\etc\hosts`
 - Linux : `/etc/hosts`



Note Cisco DCNM のデータベースとして Oracle RAC が選択されている場合は、データベース ホスト IP アドレスと仮想 IP アドレスがホスト名を使用してホストファイルに追加されていることを確認します。

- RHEL の場合、共有メモリの最大サイズは 256 MB 以上である必要があります。共有メモリの最大サイズを 256 MB に設定するには、次のコマンドを使用します。

sysctl -w kernel.shmmax=268435456

この設定 (`kernel.shmmax=268435456`) を `/etc/sysctl.conf` ファイルに保存する必要があります。この設定が存在しなかったり、268435456 未満に設定されていたりすると、サーバシステムの再起動後に Cisco DCNM サーバが失敗します。詳細については、次の URL を参照してください。

<http://www.postgresql.org/docs/8.3/interactive/kernel-resources.html>

サーバシステムは、DNS サーバに登録されている必要があります。DCNM アプリケーションをホストするサーバは、DCNM のみを実行するために専用とする必要があります。メモリリソースとシステムリソースを使用する他のアプリケーションと共有することはできません。

- リモート PostgreSQL データベース サーバを使用しているときに、Cisco DCNM ホストの IP アドレスが PostgreSQL インストールディレクトリに存在する `pg_hba.conf` ファイルに追加されていることを確認します。エントリが追加されたら、データベースを再起動します。
- Cisco DCNM をインストールするユーザには、ユーザアカウントを作成し、サービスを起動するためのすべての管理者権限が必要です。また、すべてのポートへのアクセス権も必要です。詳細については、「[ファイアウォール背後での Cisco DCNM の実行, on page 127](#)」を参照してください。
- 最初にサーバを接続する場合、Cisco DCNM は正しい Sun Java 仮想マシンバージョンがローカルワークステーションにインストールされているか確認します。Cisco DCNM デスクトップクライアントは、インストール中にバージョン 1.8(x) を検索します。必要な場合は、Sun Java Virtual Machine ソフトウェアをインストールします。



Note Cisco DCNM インストーラを起動する場合に、`console` コマンドオプションはサポートされません。



Note Cisco DCNM インストーラを GUI モードで使用するには、VNC または XWindows を使用してリモートサーバにログインする必要があります。Telnet または SSH を使用して Cisco DCNM を GUI モードでインストールすることはできません。

Cisco DCNM を使用してネットワーク スイッチを管理する前に、次のタスクを実行する必要があります。

- 管理するスイッチごとに、スーパーバイザ モジュールを搭載します。
- スーパーバイザ モジュールには、セットアップルーチンまたは CLI を使用して次の値を設定します。
 - mgmt0 インターフェイスに割り当てられる IP アドレス
 - SNMP クレデンシャル (v3 ユーザー名とパスワード、または v1/v2 コミュニティ)、ファブリック内のすべてのスイッチで同じユーザー名とパスワードを保持します。

初回のセットアップルーチン

MDS または Nexus の Cisco NXOS ベース スイッチに初めてアクセスすると、セットアッププログラムが実行され、IP アドレスや、スイッチがスーパーバイザ モジュールのイーサネット インターフェイスを介して通信するために必要なその他の設定情報を入力するよう求められます。この情報は、スイッチを設定および管理するために必要です。すべての Cisco Nexus または Cisco MDS スイッチにおいて、デフォルト ユーザーはネットワーク管理者 (Admin) です。デフォルトのユーザーはどの時点でも変更できません。Cisco Nexus または Cisco MDS のすべてのスイッチに、強固なパスワードを明示的に設定する必要があります。セットアップ方法は、新しいスイッチを追加するサブネットによって異なります。

- 帯域外管理：スーパーバイザ モジュールの前面パネルのイーサネットポートを介したネットワーク接続を提供します。
- 帯域内管理：スイッチ管理用の IP over Fibre Channel (IPFC) を提供します。帯域内管理機能はネットワーク管理システム (Network Management System) に透過的です。



Note Cisco Nexus スイッチまたは Cisco MDS スイッチの IP アドレスは、CLI または USB キーまたは POAP を使用して設定できます。

スイッチを設定するための準備

Cisco Nexus または Cisco MDS 9000 ファミリのスイッチを初めて設定する際には、事前に次の情報を用意しておく必要があります。

- 次に示す管理者パスワード
 - 管理者パスワードの作成（必須）
 - その他のログインアカウントおよびパスワードの作成（任意）
- スイッチ管理インターフェイスの IP アドレス：管理インターフェイスには、帯域外イーサネット インターフェイスまたは帯域内のファイバチャネルインターフェイス（推奨）を使用できます。
- スイッチ管理インターフェイスのサブネット マスク（任意）
- 次の IP アドレス
 - 送信先プレフィックス、送信先プレフィックスのサブネットマスク、およびネクストホップの IP アドレス（IP ルーティングをイネーブルにする場合）。さらに、デフォルトネットワークの IP アドレスも用意します（任意）。
 - あるいは、デフォルトネットワークの IP アドレスも用意します（任意）。
- スイッチの SSH サービス：この任意のサービスをイネーブルにする場合は、SSH キーのタイプ（dsa/rsa/rsa1）とキービット数（768 ～ 2048）を選択します。
- DNS IP アドレス（任意）
- デフォルト ドメイン名（任意）
- NTP サーバの IP アドレス（任意）
- SNMP コミュニティストリング（任意）
- スイッチ名：これは、スイッチプロンプトに使用されます（任意）。



Note SNMP アクセスをイネーブルにする場合は、必ず IP ルート、IP デフォルト ネットワーク アドレス、および IP デフォルト ゲートウェイアドレスを設定してください。IP ルーティングがイネーブルの場合、スイッチは IP ルートとデフォルト ネットワーク IP アドレスを使用します。IP ルーティングがディセーブルの場合、スイッチはデフォルト ゲートウェイ IP アドレスを使用します。



Note インストール時に Cisco DCNM-SAN Server が特定のインターフェイスにバインドするように設定されている場合を除き、Cisco DCNM-SAN Server のホスト名エントリが DNS サーバに存在していることを確認する必要があります。

デフォルトのログイン

すべての Cisco Nexus および Cisco MDS 9000 ファミリ スイッチにおいて、デフォルトユーザーはネットワーク管理者 (admin) です。デフォルトのユーザはどの時点でも変更できません。(『Security Configuration Guide, Cisco DCNM for SAN』を参照)。

Cisco MDS 9000 ファミリのいずれのスイッチにも、安全なパスワードを強制するオプションがあります。パスワードが簡潔である場合 (短く、解読しやすい場合)、パスワード設定は拒否されます。安全なパスワードを設定するようにしてください (セキュリティ設定ガイドの SAN 用 Cisco DCNM を参照してください)。パスワードの設定後に、その新しいパスワードを忘れてしまった場合は、パスワードを回復することもできます (『Security Configuration Guide, Cisco DCNM for SAN』を参照)。

**Note**

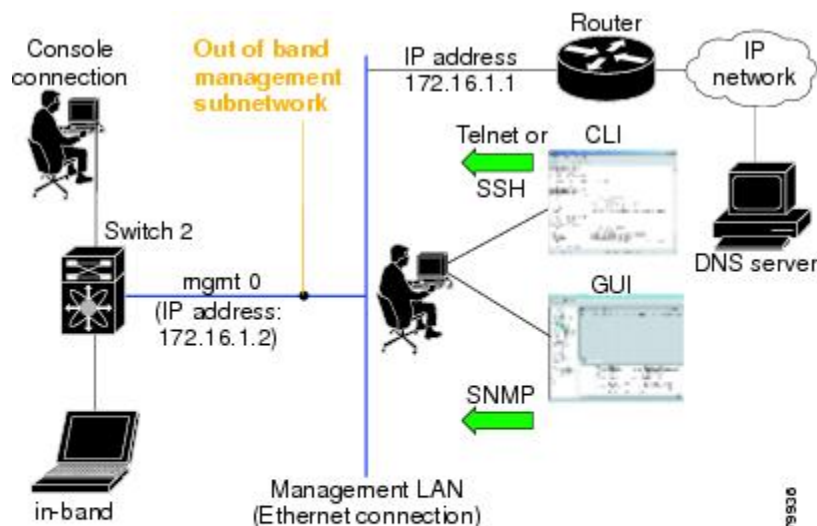
次のパスワード要件に従います。要件に従わない場合、DCNM アプリケーションは適切に機能しない場合があります。

- 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。
- 展開モード用の 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> & \$ % ‘ “ ^ = < > ; :

セットアップオプション

セットアップ方法は、新しいスイッチを追加するサブネットによって異なります。スイッチ外部からの管理接続を有効にするには、Cisco MDS 9000 ファミリ スイッチまたは Cisco Nexus スイッチに IP アドレスを設定する必要があります (Figure 1: スイッチへの管理者アクセス, on page 20 を参照)。

Figure 1: スイッチへの管理者アクセス



セットアップ情報の指定

ここでは、帯域外と帯域内の両方の管理について、初回のスイッチ設定方法を説明します。



Note 任意のプロンプトで **Ctrl+C** キーを押すと、残りの設定オプションを飛ばして、設定手順を先に進めることができます。管理者用の新しいパスワードの入力は必須の手順であり、飛ばすことはできません。



Tip 以前に設定した項目の値を再度入力しない場合や、入力を省略する場合は、**Enter** キーを押します。デフォルトの回答が見つからない場合（たとえば、スイッチ名）、スイッチは以前の設定を使用して、次の質問にスキップします。

帯域外管理の設定

次の手順でインバンドおよびアウトオブバンド設定の両方に **Yes** を入力することで、両方を一緒に設定できます。

Procedure

ステップ 1 スイッチの電源を入れます。Cisco Nexus と Cisco MDS 9000 ファミリ スイッチは自動的に起動します。

Do you want to enforce secure password standard (Yes/No)?

ステップ 2 Yes と入力して、安全なパスワードを強制します。

a) 管理者パスワードを入力します。

Enter the password for admin: **2008asdf*1kjh17**

Note パスワードはアルファベット、数字、特殊文字(-_#@&\$ など)の組み合わせを含むことができます。展開モード用の 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> & \$ % ‘ “ ^ = < > ; :

b) 管理者パスワードを確認します。

Confirm the password for admin: **2008asdf*1kjh17**

Tip パスワードが簡潔である場合（短く、解読しやすい場合）、パスワード設定は拒否されます。サンプル設定のように、強力なパスワードを設定してください。パスワードは大文字と小文字が区別されます。

ステップ 3 **yes** を入力して、セットアップ モードを開始します。

Note このセットアップユーティリティでは、手順に従って、システムの基本的な設定を行います。セットアップで設定されるのは、システムの管理に必要な接続のみです。

Please register Cisco MDS 9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. MDS devices must be registered to receive entitled support services. Press Enter anytime you want to skip any dialog. Use ctrl-c at anytime to skip away remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): **yes**

セットアップユーティリティでは、手順に従って、基本的な設定プロセスを完了できます。どのプロンプトでも、**Ctrl + C** キーを押すと、設定プロセスが終了します。

ステップ 4 管理者に新しいパスワードを入力します (Admin がデフォルトです)。

Enter the password for admin: **admin**

ステップ 5 **yes** (no がデフォルトです) を入力して、追加のアカウントを作成します。

Create another login account (yes/no) [n]: **yes**

初期セットアップを設定する際に、管理者アカウントに加えて、追加のユーザー アカウント (ネットワーク管理者ロール) を作成できます。デフォルトのロールと権限については、『Security Configuration Guide, Cisco DCNM for SAN』を参照してください。

Note ユーザ ログイン ID には、数字以外の文字を含める必要があります。

a) ユーザ ログイン ID [administrator] を入力します。

Enter the user login ID: **user_name**

- b) ユーザ パスワードを入力します。

Enter the password for user_name: **user-password**

パスワードはアルファベット、数字、特殊文字(-_#@&\$ など)の組み合わせを含むことができます。展開モード用の 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> & \$ % ‘ “ ^ = < > ; :

- c) ユーザ パスワードを確認します。

Confirm the password for user_name: **user-password**

- ステップ 6** **yes** を入力して SNMPv3 アカウントを追加します (デフォルトは **no**) 。

Configure read-only SNMP community string (yes/no) [n]: **yes**

- a) ユーザー名を入力します (デフォルトは **Admin** です)。

SNMPv3 user name [admin]: **admin**

- b) SNMPv3 パスワードを入力します (8 文字以上) 。デフォルトは **admin123** です。

SNMPv3 user authentication password: **admin_pass**

- ステップ 7** **yes** (**no** がデフォルトです) を入力して、読み取り専用または読み取り書き込み SNMP コミュニティ文字列を設定します。

Configure read-write SNMP community string (yes/no) [n]: **yes**

- a) SNMP コミュニティ スtring を入力します。

SNMP community string: **snmp_community**

- ステップ 8** スイッチの名前を入力します。

Enter the switch name: **switch_name**

- ステップ 9** **yes** (**yes** がデフォルトです) を入力して、アウトオブバンド管理を設定します。

Continue with Out-of-band (mgmt0) management configuration? [yes/no]: **yes**

- a) mgmt0 IP アドレスを入力します。

Mgmt0 IPv4 address: **ip_address**

- b) mgmt0 サブネット マスクを入力します。

Mgmt0 IPv4 netmask: **subnet_mask**

- ステップ 10** **yes** (**yes** がデフォルトです) を入力して、デフォルト ゲートウェイ (推奨) を設定します。

Configure the default-gateway: (yes/no) [y]: **yes**

- a) デフォルト ゲートウェイ IP アドレスを入力します。

IPv4 address of the default gateway: **default_gateway**

- ステップ 11** **yes** (**no** がデフォルトです) を入力して、インバンド管理、静的ルート、デフォルトネットワーク、DNS、ドメイン名などの高度な IP オプションを設定します。

Configure Advanced IP options (yes/no)? [n]: **yes**

- a) インバンド管理設定プロンプトで **no** (no がデフォルトです) を入力します。
Continue with in-band (VSAN1) management configuration? (yes/no) [no]: **no**
- b) **yes** (no がデフォルトです) を入力して、IP ルーティング機能を有効にします。
Enable the ip routing? (yes/no) [n]: **yes**
- c) **yes** (no がデフォルトです) を入力して、静的ルート (推奨) を設定します。
Configure static route: (yes/no) [n]: **yes**
送信先プレフィックスを入力します。
Destination prefix: **dest_prefix**
送信先プレフィックス マスクを入力します。
Destination prefix mask: **dest_mask**
ネクストホップ IP アドレスを入力します。
Next hop ip address: **next_hop_address**
Note SNMP アクセスを有効にする場合は、必ず IP ルート、デフォルト ネットワーク IP アドレス、およびデフォルト ゲートウェイ IP アドレスを設定してください。IP ルーティングがイネーブルの場合、スイッチは IP ルートとデフォルト ネットワーク IP アドレスを使用します。IP ルーティングがディセーブルの場合、スイッチはデフォルト ゲートウェイ IP アドレスを使用します。
- d) **yes** (no がデフォルトです) を入力して、デフォルト ネットワーク (推奨) を設定します。
Configure the default network: (yes/no) [n]: **yes**
デフォルト ネットワーク IP アドレスを入力します。
Note デフォルト ネットワーク IP アドレスは、で入力した送信先プレフィックスです。
Default network IP address [dest_prefix]: **dest_prefix**
- e) **yes** (no がデフォルトです) を入力して、DNS IP アドレスを設定します。
Configure the DNS IPv4 address? (yes/no) [n]: **yes**
DNS IP アドレスを入力します。
DNS IPv4 address: **name_server**
- f) **yes** (no がデフォルトです) を入力して、デフォルトのドメイン名を設定します。
Configure the default domain name? (yes/no) [n]: **yes**
デフォルト ドメイン名を入力します。
Default domain name: **domain_name**

ステップ 12 **yes** を入力して、Telnet サービスをイネーブルにします (デフォルトは no)。
Enable the telnet server? (yes/no) [n]: **yes**

ステップ 13 **yes** (no がデフォルトです) を入力して、サービスを有効にします。
Enabled SSH server? (yes/no) [n]: **yes**

ステップ 14 SSH キーのタイプを入力します。

```
Type the SSH key you would like to generate (dsa/rsa)? dsa
```

ステップ 15 指定範囲内でキーのビット数を入力します。

```
Enter the number of key bits? (768 to 2048): 768
```

ステップ 16 **yes** (**no** がデフォルトです) を入力して、NTP サーバを設定します。

```
Configure NTP server? (yes/no) [n]: yes
Configure clock? (yes/no) [n] :yes
Configure clock? (yes/no) [n] :yes
Configure timezone? (yes/no) [n] :yes
Configure summertime? (yes/no) [n] :yes
Configure the ntp server? (yes/no) [n] : yes
```

a) NTP サーバの IP アドレスを入力します。

```
NTP server IP address: ntp_server_IP_address
```

ステップ 17 **noshut** (**shut** がデフォルトです) を入力して、デフォルトのスイッチ ポート インターフェイスをシャット状態に設定します。

```
Configure default switchport interface state (shut/noshut) [shut]: noshut
```

ステップ 18 **on** (**on** がデフォルトです) を入力して、スイッチポート トランク モードを設定します。

```
Configure default switchport trunk mode (on/off/auto) [on]: on
```

ステップ 19 **no** と入力して、スイッチ ポートのモード F を設定します (**on** がデフォルト)。

```
Configure default switchport port mode F (yes/no) [n] : no
```

ステップ 20 **permit** (**deny** がデフォルトです) を入力して、デフォルトゾーン ポリシー設定を拒否します。

```
Configure default zone policy (permit/deny) [deny]: permit
```

デフォルトゾーンのすべてのメンバーへのトラフィックフローを許可します。

ステップ 21 **yes** (**no** がデフォルトです) を入力して、完全ゾーン設定宛先を無効にします(「SAN 向け Cisco DCNM、ファブリック設定ガイド」を参照してください)。フルゾーンセット配布機能について、スイッチ全体のデフォルトをディセーブルにします。

```
Enable full zoneset distribution (yes/no) [n]: yes
```

新しい設定を参照します。ここまでに入力した設定を確認して修正します。

ステップ 22 設定に満足した場合は、**no** (**no** がデフォルトです) を入力します。

```
The following configuration will be applied:
username admin password admin_pass role network-admin
username user_name password user_pass role network-admin
snmp-server community snmp_community ro
switchname switch
interface mgmt0
  ip address ip_address subnet_mask
  no shutdown
ip routing
ip route dest_prefix dest_mask dest_address
ip default-network dest_prefix
ip default-gateway default_gateway
```



```

ip name-server name_server
ip domain-name domain_name
telnet server enable
ssh key dsa 768 force
ssh server enable
ntp server ipaddr ntp_server
system default switchport shutdown
system default switchport trunk mode on
system default port-channel auto-create
zone default-zone permit vsan 1-4093
zoneset distribute full vsan 1-4093
Would you like to edit the configuration? (yes/no) [n]: no

```

ステップ 23 yes と入力すると（デフォルトは yes）、この設定を保存して使用できます。

```
Use this configuration and save it? (yes/no) [y]: yes
```

Caution ここで、設定を保存しておかないと、次のスイッチ再起動時に設定が更新されません。yes を入力して、新しい設定を保存し、キックスタートとシステムイメージも自動設定されていることを確認します。

帯域内管理の設定

帯域内管理の論理インターフェイスは VSAN 1 です。この管理インターフェイスはファイバチャネルインフラストラクチャを使用して IP トラフィックを伝送します。VSAN 1 のインターフェイスはファブリック内のすべてのスイッチで作成されます。各スイッチには、同じサブネットワークの IP アドレスで設定されている VSAN 1 インターフェイスが必要です。IP ネットワークへのアクセスを提供するスイッチを指すデフォルトルートをファイバチャネルファブリックのスイッチすべてに対して設定します（『Fabric Configuration Guide, Cisco DCNM for SAN』を参照）。



Note 次の手順を入力して、インバンドとアウトオブバンドの両方の設定をまとめて設定できます。

Procedure

ステップ 1 スイッチの電源を入れます。Cisco MDS 9000 ファミリのスイッチは自動的にブートします。

ステップ 2 管理者の新しいパスワードを入力します。

```
Enter the password for admin: 2004asdf*1kj18
```

パスワードはアルファベット、数字、特殊文字(-_#@&\$ など)の組み合わせを含むことができます。パスワードはアルファベット、数字、特殊文字(-_#@&\$ など)の組み合わせを含むことができます。展開モード用の 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 yes を入力して、セットアップ モードを開始します。

```

This setup utility will guide you through the basic configuration of the system. Setup
configures only enough connectivity for management of the system.
Please register Cisco MDS 9000 Family devices promptly with your supplier. Failure to
register may affect response times for initial service calls.
MDS devices must be registered to receive entitled support services.
Press Enter incase you want to skip any dialog. Use ctrl-c at anytime to skip away
remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes

```

セットアップユーティリティでは、手順に従って、基本的な設定プロセスを完了できます。どのプロンプトでも、**Ctrl-C** キーを押すと、設定プロセスが終了します。

ステップ 4 追加のアカウントを作成しない場合、**no** (**no** がデフォルトです) を入力します。

```
Create another login account (yes/no) [no]: no
```

ステップ 5 読み取り専用または読み書きの SNMP コミュニティ スtring を設定します。

a) **no** (**no** がデフォルトです) を入力して、読み取り専用 SNMP コミュニティ 文字列を設定しないようにします。

```
Configure read-only SNMP community string (yes/no) [n]: no
```

ステップ 6 スイッチの名前を入力します。

Note スイッチの名前は、英数字 32 文字以内で指定してください。デフォルトは **switch** です。

```
Enter the switch name: switch_name
```

ステップ 7 設定プロンプトで **no** (**yes** がデフォルトです) を入力して、アウトオブバンド管理を設定します。

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no]: no
```

ステップ 8 **yes** (**yes** がデフォルトです) を入力して、デフォルトゲートウェイを設定します。

```
Configure the default-gateway: (yes/no) [y]: yes
```

a) デフォルトゲートウェイ IP アドレスを入力します。

```
IP address of the default gateway: default_gateway
```

ステップ 9 **yes** (**no** がデフォルトです) を入力して、インバンド管理、静的ルート、デフォルトネットワーク、DNS、ドメイン名などの高度な IP オプションを設定します。

```
Configure Advanced IP options (yes/no)? [n]: yes
```

a) インバンド管理設定プロンプトで **yes** (**no** がデフォルトです) を入力します。

```
Continue with in-band (VSAN1) management configuration? (yes/no) [no]: yes
```

VSAN 1 IP アドレスを入力します。

```
VSAN1 IP address: ip_address
```

サブネットマスクを入力します。

```
VSAN1 IP net mask: subnet_mask
```

b) **no** (**yes** がデフォルトです) を入力して、IP ルーティング機能を有効にします。

```
Enable ip routing capabilities? (yes/no) [y]: no
```

- c) **no** (yes がデフォルトです) を入力して、静的ルートを設定します。
Configure static route: (yes/no) [y]: **no**
- d) **no** (yes がデフォルトです) を入力して、デフォルト ネットワークを設定します。
Configure the default-network: (yes/no) [y]: **no**
- e) **no** (yes がデフォルトです) を入力して、DNS IP アドレスを設定します。
Configure the DNS IP address? (yes/no) [y]: **no**
- f) **no** (no がデフォルトです) を入力して、デフォルトのドメイン名設定をスキップします。
Configure the default domain name? (yes/no) [n]: **no**

ステップ 10 **no** (yes がデフォルトです) を入力して、Telnet サービスを無効にします。

Enable the telnet service? (yes/no) [y]: **no**

ステップ 11 **yes** (no がデフォルトです) を入力して、サービスを有効にします。

Enabled SSH service? (yes/no) [n]: **yes**

ステップ 12 生成する SSH キータイプ (「SAN 向け Cisco DCNM、セキュリティ設定ガイド」を参照してください) を入力します。

Type the SSH key you would like to generate (dsa/rsa/rsa1)? **rsa**

ステップ 13 指定範囲内でキーのビット数を入力します。

Enter the number of key bits? (768 to 1024): **1024**

ステップ 14 **no** (no がデフォルトです) を入力して、NTP サーバを設定します。

Configure NTP server? (yes/no) [n]: **no**

ステップ 15 **shut** (shut がデフォルトです) を入力して、デフォルトのスイッチ ポート インターフェイスをシャット状態に設定します。

Configure default switchport interface state (shut/noshut) [shut]: **shut**

Note 管理イーサネットインターフェイスはこの時点ではシャットダウンされません。シャットダウンされるのはファイバチャネル、iSCSI、FCIP、およびギガビットイーサネットインターフェイスだけです。

ステップ 16 **auto** (off がデフォルトです) を入力して、スイッチポート トランク モードを設定します。

Configure default switchport trunk mode (on/off/auto) [off]: **auto**

ステップ 17 **deny** (deny がデフォルトです) を入力して、デフォルト ゾーン ポリシー設定を拒否します。

Configure default zone policy (permit/deny) [deny]: **deny**

デフォルトゾーンのすべてのメンバーへのトラフィックフローを拒否します。

ステップ 18 **no** (no がデフォルトです) を入力して、完全ゾーン設定配信を無効にします。

Enable full zoneset distribution (yes/no) [n]: **no**

この手順では、完全ゾーンセット配信機能のスイッチ全体のデフォルトを無効にします。

新しい設定を参照します。入力した設定を確認し、編集します。

ステップ 19 設定に満足した場合は、**no** (**no** がデフォルトです) を入力します。

```
The following configuration will be applied:
username admin password admin_pass role network-admin
snmp-server community snmp_community rw
switchname switch
interface vsan1
  ip address ip_address subnet_mask
  no shutdown
ip default-gateway default_gateway
no telnet server enable
ssh key rsa 1024 force
ssh server enable
no system default switchport shutdown
system default switchport trunk mode auto
no zone default-zone permit vsan 1-4093
no zoneset distribute full vsan 1-4093
Would you like to edit the configuration? (yes/no) [n]: no
```

ステップ 20 **yes** (**yes** がデフォルト) と入力すると、この設定を使用および保存できます。

```
Use this configuration and save it? (yes/no) [y]: yes
```

Caution ここで、設定を保存しておかないと、次のスイッチ再起動時に設定が更新されません。**yes** を入力して、新しい設定を保存します。キックスタートイメージとシステムイメージも自動的に設定されるようにします。

setup コマンドの使用法

あとで初回の設定を変更する場合は、EXEC モードで **setup** コマンドを実行します。

```
switch# setup
---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup always assumes a predefined defaults irrespective
of the current system configuration when invoked from CLI.
Press Enter incase you want to skip any dialog. Use ctrl-c at anytime
to skip away remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes
```

セットアップユーティリティでは、手順に従って、基本的な設定プロセスを完了できます。

Cisco MDS 9000 ファミリのスイッチの始動

ここでは、スイッチの始動など、ハードウェアインストール時に完了しておく必要のある作業手順をまとめます。これらの作業を完了しないと、スイッチを設定できません。



Note 初回のスイッチ始動時には CLI を使用する必要があります。

Procedure

ステップ 1 新しい Cisco MDS 9000 ファミリ スイッチの物理的な接続を確認します。次の接続を確認してください。

- コンピュータ 端末（または 端末サーバ）に コンソール ポート が物理的に接続されている。
- 管理 10/100 イーサネット ポート（mgmt0）が外部ハブ、スイッチ、またはルータに接続されている。

Tip 後で使用するためにホスト ID 情報を控えておいてください（たとえば、ライセンス機能をイネーブルにする場合など）。ホスト ID 情報は、スイッチに同梱されている Proof of Purchase 文書に記載されています。

ステップ 2 デフォルトのコンソール ポートのパラメータが、スイッチ コンソール ポートに接続されたコンピュータ 端末（または 端末サーバ）のパラメータと同じであることを確認します。

- 9600 ボー
- 8 データ ビット
- 1 ストップ ビット
- パリティなし

ステップ 3 スイッチの電源を入れます。

スイッチは自動的にブートし、ターミナル ウィンドウに `switch#` プロンプトが表示されます。

スイッチへのアクセス

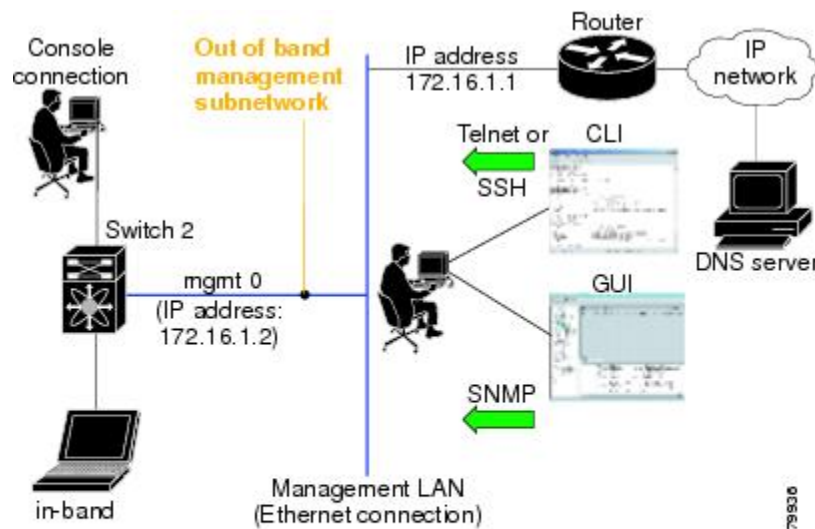
初期設定後は、次の 3 つのいずれかの方法でスイッチにアクセスできます。

- シリアル コンソール アクセス：シリアル ポート接続を使用して CLI にアクセスできます。
- 帯域内 IP（IPFC）アクセス：Telnet または SSH を使用して Cisco DCNM-SAN 9000 ファミリのスイッチにアクセスできます。または SNMP を使用して Cisco DCNM-SAN アプリケーションに接続できます。
- 帯域外（10/100BASE-T イーサネット）アクセス：Telnet または SSH を使用して Cisco MDS 9000 ファミリのスイッチにアクセスできます。または SNMP を使用して Cisco DCNM-SAN アプリケーションに接続できます。

初回の設定後は、次の 3 つのいずれかの方法でスイッチにアクセスできます ([Figure 2: スイッチ アクセスのオプション, on page 30](#) を参照)。

- シリアル コンソール アクセス：シリアル ポート接続を使用して CLI にアクセスできます。
- 帯域内 IP (IPFC) アクセス：Telnet または SSH を使用して Cisco MDS 9000 ファミリのスイッチにアクセスできます。または Cisco DCNM-SAN を使用してスイッチにアクセスできます。
- 帯域外 (10/100BASE-T イーサネット) アクセス：Telnet または SSH を使用して Cisco MDS 9000 ファミリのスイッチにアクセスできます。または Cisco DCNM-SAN を使用してスイッチにアクセスできます。

Figure 2: スイッチ アクセスのオプション



Linux で DCNM をインストールするための前提条件

- 初期インストール時に、Windows サーバで実行されているすべてのセキュリティおよびウイルス対策ツールを無効にします。
- Cisco DCNM サーバまたは Cisco DCNM データベース サーバ上で他の管理アプリケーションを実行しないでください。
- Cisco DCNM をインストールする前に、ホスト名が `C:\WINDOWS\system32\drivers\etc\hosts` の下のホスト ファイルの IP アドレスにマッピングされていることを確認します。
- Windows で、リモート Cisco DCNM インストールまたはアップグレードが VNC を使用したコンソールを通して、またはコンソールモード (RDC が `/Console` オプションとともに

使用されていることを確認します) のリモートデスクトップクライアント (RDC) を通して完了する必要があります。このデータベースではすべてのインストールとアップグレードにローカル コンソールが必要なため、このプロセスは、デフォルトの PostgreSQL データベースが Cisco DCNM で使用されている場合に重要です。

- Telnet Client アプリケーションはデフォルトでは Microsoft Windows Vista にインストールされていません。Telnet Client をインストールするには、[スタート (Start)] > [プログラム (Programs)] > [コントロール パネル (Control Panel)] > [Windows 機能のオンまたはオフをクリックする (Click Turn Windows features on or off)] を選択します (UAC をオンにした場合、権限を提供して続行します)。[Telnet Client] チェック ボックスをオンにして、[OK] をクリックします。
- Cisco DCNM と同じ PC で CiscoWorks を実行できますが、Java 要件は異なります。Cisco DCNM に最新の Java バージョンをインストールする場合は、CiscoWorks に必要な以前の Java バージョンが上書きされないようにしてください。両方の Java バージョンは PC 上で共存できます。
- フェデレーション セットアップのすべてのノードに対して、同じオペレーティング システムを使用していることを確認します。
- フェデレーション セットアップで、サーバ時間がフェデレーション セットアップのすべてのノードで同期されていることを確認します。時間が同期されていない場合、サーバが通信できません。NTPサーバを使用して、すべてのノードで時間を同期することを推奨します。
- Windows 2016 サーバに Cisco DCNM をインストールする前に、Windows Defender アプリケーションをアンインストールし、Windows 2016 サーバを再起動してください。

Linux で DCNM をインストールするための前提条件

- RHEL の場合、共有メモリの最大サイズは 256 MB 以上である必要があります。最大共有メモリを 256 MB に設定するには、次のコマンドを使用します。 `sysctl -w kernel.shmmax=268435456`。 `/etc/sysctl.conf` ファイルに `kernel.shmmax=268435456` 値を保存します。この値が正しくない場合、サーバシステムの再起動後に Cisco DCNM サーバに障害が発生します。詳細については、次の URL を参照してください。
<http://www.postgresql.org/docs/8.4/interactive/kernel-resources.html>
- サーバシステムは、DNS サーバに登録されている必要があります。
- その他のプログラムはサーバ上で実行する必要はありません。
- RHEL のインストール時に、推奨言語として英語を選択していることを確認します。
- フェデレーション セットアップのすべてのノードに対して、同じオペレーティング システムを使用していることを確認します。
- フェデレーション セットアップで、サーバ時間がフェデレーション セットアップのすべてのノードで同期されていることを確認します。時間が同期されていない場合、サーバが

通信できません。NTPサーバを使用して、すべてのノードで時間を同期することを推奨します。

- Linux スタンドアロンサーバで Cisco DCNM リリース 11.2(1) からアップグレードした後は、Web UI を起動して SAN クライアントをダウンロードする前に、ブラウザのキャッシュと Java コンソールキャッシュを消去していることを確認してください。Java コンソールには、以前のバージョンの SAN クライアントデータが記憶されています。Java コンソールキャッシュを消去しないと、ダウンロードした最新の SAN クライアントを使用できなくなります。

ウイルス対策の除外対象

Cisco DCNM のスキャンには、データベースファイルのスキャンが含まれます。このプロセスは、動作中の DCNM のパフォーマンスを阻害します。Linux RHEL サーバで Cisco DCNM をスキャン中、ディレクトリ `/usr/local/cisco/dcm/db` and `/var/lib/dcnm` を除外します。

詳細については、<https://wiki.postgresql.org> を参照してください。



Note ポートの使用またはブロックにより障害が発生する可能性があるため、DCNM のインストール中にウイルス対策のスキャンを停止することをお勧めします。インストール後、特定のガイドラインがあるウイルス対策アプリケーションを有効またはインストールすることで、スキャンの一部となる DCNM ディレクトリを避けることができます。

DCNM サーバの Oracle データベース

ここでは、DCNM サーバのインストールに必要なデータベースについて詳しく説明します。



Note このセクションは、Cisco DCNM ネイティブ HA のインストールには適用されません。

Cisco DCNM では、次のデータベースをサポートします。

- Oracle Database 11g
- Oracle データベース 12c
- Oracle RAC 11g および 12c

必要に応じて、ローカルデータベースから外部 Oracle データベースに変更できます。



Note Cisco DCNM は、AL32UTF8 文字セットを使用して設定されます。

Cisco DCNM データベースのサイズは制限されず、DCNM が Performance Manager コレクションを有効にして管理するノードとポートの数に基づいて増加します。データベースのサイズを制限することはできません。表スペースの制限により、Oracle XE の代わりに Oracle SE またはエンタープライズ エディションを使用することを推奨します。

この項の内容は、次のとおりです。

Oracle SQLPlus コマンドライン ツール

ここで示す Oracle データベースの手順を実行するには、SQL*Plus コマンドライン ツールを使用する必要があります。SQL*Plus 実行可能ファイルは、通常、Oracle ホーム ディレクトリの下に bin ディレクトリにインストールされています。

Linux の環境変数

Linux を使用している場合は、SQL*Plus コマンドライン ツールを使用する前に、ORACLE_HOME および ORACLE_SID 環境変数を正しい値に設定する必要があります。

たとえば、Linux で Oracle 11g を使用している場合は、次のコマンドを実行して、これらの環境変数をデフォルトの Oracle ホーム ディレクトリと SID に設定します (bash シェルを使用している場合)。

```
export ORACLE_HOME=<usr_home_directory>/app/oracle/product/11.2.0/  
(or identify the Oracle home on the Oracle installed server)  
export ORACLE_SID=XE
```

init.ora ファイル

init.ora ファイルでは、起動パラメータを指定します。次の表に示すように、このファイルのデフォルトの名前と格納場所はプラットフォームによって異なります。

Table 5: init.ora ファイルの名前とデフォルトの格納場所

Oracle バージョン	オペレーティングシステム	init.ora ファイルの場所
12c	Microsoft Windows	C:\app\Administrator\virtual\product\12.2.0\dbhome_1\srvm\admin\init.ora
	Linux	/usr/lib/oracle/orcl/app/oracle/product/12.2.0/db_1/Srvm/initorclora
11g	Microsoft Windows	C:\app\Administrator\product\11.1.0\db_1\dfs\initORCL.ora
	Linux	/usr/lib/oracle/orcl/app/oracle/product/11.1.0/db_1/dfs/initORCL.ora

Oracle データベースのバックアップ

Cisco DCNM サーバディレクトリ DCNM_SERVER_Install/dcm/dcnm/bin から Oracle バックアップ/復元スクリプトをコピーします。

Linux の場合、スクリプト名は `backup-remote-oracledb.sh/restore-remote-oracledb.sh` であり、`DB_HOME` 変数を編集して Oracle インストールを指定します。

Windows の場合、スクリプト名は `backup-remote-oracledb.bat/restore-remote-oracledb.bat` であり、`DB_HOME` 変数を編集して Oracle インストールを指定します。

Oracle DBHOME に次のパスを使用します。

- Linux の場合 : `/usr/lib/oracle/xe/app/oracle/product/10.2.0/server`
`/usr/lib/oracle` を Oracle インストール パスに置き換えます。
- Windows の場合: `C:\oraclexe\app\oracle\product\10.2.0\server`
`C:\oraclexe` を Oracle インストール パスに置き換えます。

Oracle データベースの準備

Oracle データベースを準備できます。

Procedure

- ステップ 1** セッション数とプロセス数をそれぞれ 150 に増やします。詳細については、[セッション数とプロセス数の 150 への増加, on page 35](#)を参照してください。
- ステップ 2** 開いているカーソルの数を 1000 に増やします。詳細については、[開いているカーソルの数の 1000 への増加, on page 36](#)を参照してください。
-

Oracle へのログイン

SQL*Plus コマンドライン ツールを使用して Oracle データベースにログインできます。

Before you begin

データベース管理者のユーザ名とパスワードを確認します。

Procedure

- ステップ 1** SQL*Plus 実行可能ファイルを実行します。
コマンドプロンプトが表示されます。
- ステップ 2** `connect` コマンドを入力します。
ユーザ名プロンプトが表示されます。
- ステップ 3** データベース管理者のユーザ名を入力します。
パスワードプロンプトが表示されます。

ステップ 4 指定したユーザ名のパスワードを入力します。

たとえば、Oracle 管理者のユーザ名が `system` でパスワードが `oracle` である場合は、次のように入力してログインします。

Example:

```
Username: sys as sysdba  
Password: oracle
```

What to do next

SQL*Plus の使用の詳細については、使用している Oracle データベース バージョンのマニュアルを参照してください。

SYSTEM テーブルスペースの拡張

SYSTEM テーブルスペースを拡張できます。

Procedure

ステップ 1 Oracle データベースにログインするには、SQL*Plus コマンドライン ツールを使用します。詳細については、[Oracle SQLPlus コマンドライン ツール, on page 33](#)を参照してください。

ステップ 2 次のコマンドを入力します。

```
select file_name, bytes, autoextensible, maxbytes  
from dba_data_files where tablespace_name='SYSTEM';
```

ステップ 3 次のコマンドを入力します。

```
alter database datafile filename autoextend on next 100m maxsize 2000m;
```

file_name は前の手順で **select** コマンドの出力ファイル名です。

SYSTEM テーブルスペースが拡張されます。

ステップ 4 **exit** コマンドを入力します。

セッション数とプロセス数の 150 への増加

同じ Oracle データベースに設定されている DCNM インスタンスごとに、カーソルとプロセス数を 150 と 1000 よりも大きくする必要があります。

たとえば、2つの DCNM スタンドアロン (非 HA) インスタンスが同じ Oracle データベースを使用するように設定されている場合は、いずれかの DCNM インスタンスが通常の動作中に発生したパフォーマンスの低下または SQL 例外エラーに応じて、カーソルとプロセスを約 300 および 2000 に増やす必要があります。

Procedure

ステップ 1 `init.ora` ファイルが存在し、このファイルに使用中の Oracle データベース インストールに該当する 1 行が含まれていることを確認します。それ以外の行が含まれている場合は削除します。

詳細については、[init.ora ファイル, on page 33](#)を参照してください。

ステップ 2 Oracle データベースにログインするには、SQL*Plus コマンドライン ツールを使用します。詳細については、[Oracle SQLPlus コマンドライン ツール, on page 33](#)を参照してください。

ステップ 3 `shutdown` コマンドを入力してシステムをシャット ダウンします。このコマンドが失敗する場合は、`shutdown abort` コマンドを使用します。

ステップ 4 次のコマンドを入力します。

```
startup pfile='init_file_name';
```

`init_file_name` は、使用中の Oracle データベース インストールの `init.ora` ファイル名です。詳細については、[init.ora ファイル, on page 33](#)を参照してください。

ステップ 5 次のコマンドを入力して、セッション数を 150 に設定します。

```
alter system set sessions = 150 scope=spfile;
```

ステップ 6 `shutdown` コマンドを入力してシステムをシャット ダウンします。このコマンドが失敗する場合は、`shutdown abort` コマンドを使用します。

ステップ 7 `startup` コマンドを入力して、システムを起動します。

ステップ 8 次のコマンドを入力して、セッション数とプロセス数が 150 に変更されていることを確認します。

```
show parameter sessions
```

ステップ 9 `exit` コマンドを入力して、終了します。

開いているカーソルの数の 1000 への増加

開いているカーソルの数を 1000 に増やすことができます。

Procedure

ステップ 1 `init.ora` ファイルが存在し、このファイルに使用中の Oracle データベース インストールに該当する 1 行が含まれていることを確認します。それ以外の行がファイルに含まれている場合は削除します。

詳細については、[init.ora ファイル, on page 33](#)を参照してください。

ステップ 2 Oracle データベースにログインするには、SQL*Plus コマンドライン ツールを使用します。詳細については、[Oracle SQLPlus コマンドライン ツール, on page 33](#)を参照してください。

ステップ3 shutdown コマンドを入力してシステムをシャットダウンします。このコマンドが失敗する場合は、**shutdown abort** コマンドを使用します。

ステップ4 次のコマンドを入力します。

```
startup pfile='init_file_name'
```

init_file_name は、使用中の Oracle データベース インストールの *init.ora* ファイル名です。詳細については、[init.ora ファイル](#), on page 33を参照してください。

ステップ5 次のコマンドを入力して、開いているカーソルの数を 1000 に設定します。

```
alter system set open_cursors = 1000 scope=spfile;
```

ステップ6 shutdown コマンドを入力してシステムをシャットダウンします。このコマンドが失敗する場合は、**shutdown abort** コマンドを使用します。

ステップ7 startup コマンドを入力して、システムを起動します。

ステップ8 次のコマンドを入力して、開いているカーソルの数が 1000 に変更されていることを確認します。

```
show parameter open_cursors
```

ステップ9 exit コマンドを入力して、終了します。

コマンドプロンプトを使用して Oracle DB ユーザーを作成する

コマンドプロンプトを使用して Oracle DB ユーザーを作成するには、次の手順に従います。

```
export ORACLE_SID=XE
export ORACLE_HOME=/usr/lib/oracle/xe/app/oracle/product/10.2.0/server
cd $ORACLE_HOME/bin
sqlplus
sys as sysdba
create user dcnmdbusername identified by dcnmdbuserpassword default tablespace users
temporary tablespace temp;
grant connect, resource to dcnmdbusername;
grant create session to dcnmdbusername;
grant dba to dcnmdbusername;
```



Note Oracle_SID および Oracle_Home を設定していることを確認し、DB ユーザー名とパスワードフィールドの値を入力します。



Note DBA アカウントが作成できない場合、DML/DDI/スキーマ権限を持つアカウントで十分です。

SCAN 機能タイプ DB を使用して Oracle RAC に接続する

SCAN 機能タイプ DB を使用して Oracle RAC に接続するには、次のコマンドを入力します。

```
# appmgr update -u jdbc:oracle:thin:@//[ip_addr]:1521/[service name] -n [username] -p [password]
```

フェデレーションセットアップ用のデータベース

Cisco DCNM は、Cisco DCNM-SAN フェデレーションとして展開できます。Cisco DCNM-SAN フェデレーションの場合、データベース URL (プロパティ) は、フェデレーション内のすべての Cisco DCNM-SAN ノードで同じである必要があります。



Note フェデレーションを形成するためにマルチキャストアドレスを指定していないことを確認します。

バックアップおよび復元用のリモート Oracle データベースユーティリティスクリプト

プラットフォームに関係なく、Cisco DCNM がインストールされており (Windows または Linux)、リモート Oracle データベースをバックアップおよび復元するには、次のスクリプトを作成します。

Linux プラットフォームにインストールされている Oracle データベースのユーティリティスクリプト:

1. backup-remote-oracledb.sh
2. restore-remote-oracledb.sh

Windows プラットフォームにインストールされている Oracle データベースのユーティリティスクリプトは次のとおりです。

1. backup-remote-oracledb
2. restore-remote-oracledb

Cisco DCNM ホストは、リモート Oracle データベースを使用して実行するように設定されています。ハウスキーピングの一環として、DCNM ユーティリティスクリプトをリモート Oracle データベースにコピーし、DCNM データベーススキーマを復元することができます。

ユーティリティスクリプトを実行するには、データベース管理者のクレデンシャルが必要です。これらのスクリプトでは、次のプロンプトが表示されます。

1. DCNM データベース パスワード (ユーザー名はすでに存在します)
2. 管理者ユーザーのユーザー名/パスワード。

DBA ユーザークレデンシャルを入力する際には、「sys」として「sys」を入力しないようにしてください。一部のバージョンの Oracle では、スペースが存在するとバックアップ/復元が失敗する可能性があります。代わりに、ユーザーはシステムや sysdba などのユーザー名にスペースがない有効なユーザークレデンシャルを提供する必要があります。管理者クレデンシャルは保存またはキャッシュされないため、機密性の高いクレデンシャル情報は漏洩しません。



Note `dcnm/bin`のユーザー スクリプトは、管理者ユーザーのみが実行できます。

バックアップおよび復元用のローカル PostgreSQL データベース ユーティリティ スクリプト

RHEL マシンにインストールされているローカル PostgreSQL データベースのユーティリティ スクリプトは次のとおりです。

1. `backup-pgsql-dcnm-db.sh`
2. `restore-pgsql-dcnm-db.sh`

Windows マシンにインストールされているローカル PG データベースのユーティリティ スクリプトは次のとおりです。

1. `backup-pgsql-dcnm-db.bat`
2. `restore-pgsql-dcnm-db.bat`



第 4 章

Cisco DCNM のインストール

この章は、次の項で構成されています。

- [Windows への Cisco DCNM のインストール \(41 ページ\)](#)
- [Linux への Cisco DCNM のインストール \(50 ページ\)](#)
- [オープン仮想アプライアンスで DCNM をインストールする \(58 ページ\)](#)
- [ISO 仮想アプライアンスで DCNM をインストールする \(77 ページ\)](#)
- [SAN クライアントおよびデバイス マネージャの起動 \(100 ページ\)](#)

Windows への Cisco DCNM のインストール

Windows に Cisco DCNM をインストールするには、次のタスクを実行します。

Windows で Cisco DCNM をアンインストールする

Windows で Cisco DCNM をアンインストールするには、次の手順を実行します。



(注) 同じ順番でこれらの手順に従うことをお勧めします。

始める前に

同じサーバを使用して異なるバージョンの DCNM をインストールする前に、Cisco DCNM i インスタンスを完全に削除する必要があります。

手順

- ステップ 1** Cisco DCNM サービスを停止します。
- ステップ 2** Postgres データベースをアンインストールします。
- ステップ 3** Cisco DCNM をアンインストールします。

- ステップ 4 C:\Users\Administrator に移動し、**cisco_mds9000** フォルダを削除します。
- ステップ 5 C:\Program Files\Zero G Registry に移動し、**ゼロ G レジストリ** フォルダを削除します。
- ステップ 6 C:\Users\Administrator に移動し、**installanywhere** フォルダを削除します。
- ステップ 7 Cisco DCNM インストールに必要なすべてのポートが空いており、利用できることを確認します。
- ステップ 8 Cisco DCNM ディレクトリを削除します。
- ステップ 9 Windows VM を再起動します。

Cisco DCNM Windows インストーラおよびプロパティ ファイルのダウンロード

Windows に DCNM をインストールする最初の手順は、`dcnm.exe` ファイルをダウンロードすることです。



Note フェデレーションアプリケーション機能を使用する予定の場合は、`dcnm.exe` 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、 を選択します。
- ステップ 5 DCNM Windows インストーラを見つけて、**[ダウンロード (Download)]** アイコンをクリックします。
インストーラ ファイルの形式は、 です。
- ステップ 6 DCNM サイレント インストーラのプロパティ ファイルを検索し、**[ダウンロード (Download)]** アイコンをクリックします。
このファイルは、サイレント インストール時に使用されます。

ステップ7 インストールを開始したときに簡単に見つけることができるように、両方のファイルをディレクトリに保存します。

GUI を使用した Windows への Cisco DCNM のインストール

GUI を使用して DCNM Windows 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 ダウンロードした dcnm .exe ファイルを検索します。

dcnm.exe ファイルをダブルクリックします。

[InstallAnywhere] 進捗バーが表示され、進行状況が表示されます。

ステップ2 [はじめに (Introduction)] 画面の指示を読みます。

OEM ベンダー ドロップダウンリストからベンダーを選択します。

- Cisco Data Center Network Manager
- IBM : IBM Data Center Network Manager をインストールする場合。

[次へ (Next)] をクリックします。

ステップ3 フェデレーションセットアップで DCNM がセカンダリ アプライアンスとしてインストールされている場合、[既存のフェデレーションにサーバを追加する (Add server to existing federation)] チェックボックスをオンにします。

ステップ4 [セキュア暗号 (Secure Ciphers)] チェックボックスをオンにすると、強力な暗号を持つスイッチだけが DCNM によって検出されます。

ステップ5 初めて DCNM-SAN および SMI-S をインストールする場合、インストールする場所を選択します。[インストール場所 (Install Location)] フィールドで、[選択 (Choose)] をクリックして、適切なフォルダパスを提供します。DCNM がフェデレーションセットアップの一部としてインストールされている場合、[デフォルト フォルダの復元 (Restore Default Folder)] をクリックします。

[次へ (Next)] をクリックします。

ステップ6 DCNM サーバに適切な RDBMS を選択します。

要求に基づいてデータベースを選択します。

- PostgreSQL のインストール : dcnm.exe にバンドルされている PostgreSQL データベースをインストールします。
- 既存の PostgreSQL 9.4
- 既存の Oracle 10g/11g/12c

- 既存の Oracle 10g/11g/12c RAC

[サービス名 (Service Name)] フィールドに、Oracle RAC サーバのサービス名を入力します。最大3つの IP アドレスを入力します。[OK] をクリックします。DB URL が生成されます。

Cisco DCNM インストーラによって RDBMS がすでにインストールされていることが検出された場合は、[DB URL] フィールドにホスト名が表示されます。

既存の PostgreSQL を使用した Cisco DCNM インストールでは、同じユーザー名によって所有されている DCNM ユーザー名と同じ名前の既存のスキーマが必要です。DCNM ユーザー名のスキーマが存在しない場合、または同じ dcnmuser 名のスキーマを所有していない場合は、「public」という名前のデフォルトのスキーマで表が作成されます。

Note デフォルトのパブリック スキーマで作成された表を使用して DCNM サーバをアップグレードすることはできません。

Note Oracle では、新しいユーザが作成された場合に、ユーザ名と同じ名前のスキーマ名が自動的に作成されます。

[DCNM DB ユーザー (DCNM DB User)] フィールドに、Cisco DCNM がデータベースにアクセスするために使用するユーザー名を入力します。[DCNM DB Password] フィールドに、指定したデータベース ユーザアカウントのパスワードを入力します。**[既存のフェデレーションにサーバを追加する (Add Server to an existing federation)]** を選択する場合、対応する RDBMS オプションを選択して、データベース URL を変更します。フェデレーション内のすべてのサーバが同じデータベースを参照しているため、プライマリサーバの dcnmuser 名とパスワードを指定する必要があります。

[次へ (Next)] をクリックします。Oracle データベースの制限を確認し、[OK] をクリックします。

[次へ (Next)] をクリックします。

ステップ 7 [ポート設定オプション (Port Configuration Options)] 画面で、Cisco DCNM のインターフェイスと Web ポートを選択します。

- [Server IP Address] リストから、Cisco DCNM サーバで使用する IP アドレスを選択します。このリストには、サーバシステムのネットワーク インターフェイスに現在割り当てられている IP アドレスだけが表示されます。
- Cisco DCNM-SAN Web サーバがリスンするポートを変更する場合は、[SAN Web Server Port] フィールドに新しいポート番号を入力します。デフォルトでは、Cisco DCNM-SAN Web サーバは TCP ポート 443 をリスンします。

Note Cisco DCNM のインストール中に、一般的に使用されていないポート番号を使用します。たとえば、87 と 23 は、予約または制限された Web ポートです。

[次へ (Next)] をクリックします。

ステップ 8 [DCNM のアーカイブフォルダを選択する (Choose archive Folder for DCNM)] 画面で、フォルダパスを提供し、デバイス設定ファイル、ユーザーの基本設定などを保存します。

次のいずれかを実行します。

- **[選択 (Choose)]** をクリックして、DCNM LAN アーカイブ ディレクトリを保存するパスを選択します。

Note リモートシステムを選択する必要がある場合、UNIC パスを提供します。
例：//Server/Share/directorypath.

- **[デフォルト フォルダの復元 (Restore Default Folder)]** をクリックし、デフォルトフォルダを保持します。

Note このフォルダが、フェデレーションセットアップのすべてのノードからアクセス可能であることを確認します。

[次へ (Next)] をクリックします。

ステップ 9 [ローカル ユーザー クレデンシヤル (Local User Credentials)] 画面で、DCNM SAN および DCNM LAN アプライアンスの両方にアクセスするための有効なユーザー名とパスワードを入力します。

- **[管理ユーザー名 (Admin Username)]** フィールドに、Cisco DCNM サーバのユーザーの名前を入力します。インストーラによって、Cisco DCNM サーバのユーザが作成され、そのユーザに管理者ロールが割り当てられます。
- **[Password]** フィールドにそのユーザのパスワードを入力し、**[Confirm Password]** フィールドにそのパスワードを再入力します。

次のパスワード要件に従います。要件に準拠していない場合、DCNM アプリケーションが正常に機能しない可能性があります。

- 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。
- 展開モード用の 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> & \$ % ‘ “ ^ = < > ; :

[次へ (Next)] をクリックします。

ステップ 10 [認証設定 (Authentication Settings)] 画面で、Cisco DCNM サーバが Cisco DCNM クライアントにログオンするユーザーを認証するために使用する認証方式を選択します。次のいずれかを選択できます。

- **ローカル** : Cisco DCNM クライアント ユーザーは、Cisco DCNM サーバのユーザー アカウントによってのみ認証されます。
- **RADIUS** : Cisco DCNM クライアント ユーザーは、RADIUS サーバによって認証されます。
- **TACACS+** : Cisco DCNM クライアント ユーザーは、TACACS+ サーバによって認証されます。

DCNM のインストール後に LDAP 認証を設定できます。

Note TACACS/RADIUS/LDAP を有効にすると、ローカルユーザー「admin」にアクセスできなくなります。これはデフォルトの動作です。

TACACS/RADIUS/LDAP サーバが到達不能またはダウンしている場合にのみ、ローカルユーザーが検証され、ログインできるようになります。

LDAP/RADIUS/TACACS サーバが到達可能で、TACACS/LDAP/RADIUS で認証に失敗した場合は、ローカルにフォールバックしません。

ステップ 11 [RADIUS] または [TACACS+] を選択した場合は、次の手順を実行します。

- a) [primary server address] フィールドに、サーバの IPv4 アドレスをドット付き 10 進数形式で入力します。
- b) [primary server key] フィールドに、サーバの共有秘密キーを入力します。
- c) (Optional) Cisco DCNM がサーバと通信可能なことを確認する場合は、**[検証 (Verify)]** をクリックします。
- d) [secondary server address] フィールドに、サーバの IPv4 アドレスをドット付き 10 進数形式で入力します。
- e) [secondary server key] フィールドに、サーバの共有秘密キーを入力します。
- f) (Optional) Cisco DCNM がサーバと通信可能なことを確認する場合は、**[検証 (Verify)]** をクリックします。
- g) [tertiary server address] フィールドに、サーバのアドレスをドット付き 10 進数形式で入力します。
- h) [第三次サーバキー (tertiary server key)] フィールドに、サーバの共有秘密キーを入力します。
- i) (Optional) Cisco DCNM がサーバと通信可能なことを確認する場合は、**[検証 (Verify)]** をクリックします。

[次へ (Next)] をクリックします。

ステップ 12 [ショートカット フォルダの選択 (Choose Shortcut Folder)] 画面で、DCNM アイコンを作成するパスを指定します。

サーバシステムにログイン可能なすべてのユーザーにショートカットが作成されるようにする場合は、**[すべてのユーザーにアイコンを作成する (Create Icons for All Users)]** 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 13 [インストール前の概要 (Pre-Installation Summary)] 画面で、インストール設定を確認します。

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。

[次へ (Next)] をクリックします。

ステップ 14 確認ウィンドウで、**[はい (Yes)]** をクリックし、DCNM インストールを開始します。

進捗バーの説明では、インストール中の進行状況を示します。

ステップ 15 [インストール完了 (Install Complete)] 画面で、インストールが完了したコンポーネントが一覧表示されます。**[完了 (Done)]** をクリックし、DCNM サーバを開始します。

Note [インストール完了 (Install Complete)] 画面で **[終了 (Done)]** をクリックします。[終了 (Done)] をクリックしなかった場合、installvariables.properties および dcnm_installer.log が生成されません。これにより、DCNM セットアップの次のアップグレード/アンインストールが制限されます。

システムに DCNM が展開されるまで待ちます。

サイレントインストールが完了すると、プロンプトが返されます。

ステップ 16 ブラウザを開き、https://<<DCNM_server_IP_Address>> を入力します。

[Return] キーを押して、LAN および SAN 管理用の Windows で CISCO DCNM の Web インターフェイスを起動します。

GUI を使用したサーバ フェデレーション環境への Cisco DCNM Windows のインストール

サーバ フェデレーション環境で DCNM をインストールするには：

Before you begin

プライマリ サーバで DCNM をインストールしていることを確認します。[GUI を使用した Windows への Cisco DCNM のインストール, on page 43](#) セクションの指示に従ってください。

Procedure

ステップ 1 セカンダリ サーバで DCNM をインストールしながら、**[既存のフェデレーションにサーバを追加する (Add server to existing federation)]** チェックボックスをオンにします。

これにより、フェデレーションセットアップでセカンダリ アプライアンスとして DCNM をインストールします。[事前インストール概要 (Pre-installation Summary)] 画面には、[フェデレーション設定 (Federation Settings)] でフェデレーション ステータスとノードを表示します。

ステップ 2 [セキュア暗号 (Secure Ciphers)] チェックボックスをオンにすると、セキュア暗号がプライマリで有効になっている場合にのみ、強力な暗号を持つスイッチだけが DCNM によって検出されます。

Cisco DCNM は、スイッチに接続するときに強力な暗号と脆弱な暗号の両方を使用します。uses both strong and weak ciphers when connecting to switches. ユーザーがネットワークに強力な暗号のみを使用する場合は、このチェックボックスをオンにします。DCNM は強力な暗号をサポートしていないスイッチに接続できないため、チェックボックスを選択する前にネットワーク内のスイッチが強力な暗号をサポートしていることを確認します。

ステップ 3 対応する RDBMS オプションを選択して、データベース URL を変更します。

Note フェデレーション内のすべてのサーバは同じデータベースを参照するため、プライマリサーバの DCNM ユーザー名とパスワードを指定する必要があります。また、プライマリサーバのデータベースユーザー名とパスワードを指定する必要があります。

データベースのユーザー名とパスワードは、フェデレーションを形成するすべてのサーバインストールで同じです。同様に、DCNMのユーザー名とパスワードは、フェデレーションを形成するすべてのサーバインストールで同じです。

サイレントインストールを通して Cisco DCNM Windows をインストールする

Cisco DCNM は、リモート認証モードではなく、ローカル認証モードでのみサイレントインストールをサポートしています。

サイレントインストールを使用して DCNM ウィンドウ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 解凍し、`installer.properties` ファイルを展開して開き、次のプロパティを更新します。

```
#-----BASIC Properties-----
DCNM_IP_ADDRESS=<ip_address_of_host_machine>
USER_INSTALL_DIR=C:\\Program Files\\Cisco Systems
INSTALLATION_TYPE=NEW_INSTALL
#INSTALLATION_TYPE=UPGRADE
SAN_FEDERATION=FALSE
#SAN_FEDERATION=TRUE
```

ステップ 2 データベースパラメータを設定します。

PostgreSQL データベースを使用している場合は、次のブロックを編集します。

```
#-----DATABASE Properties-----
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#-----
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE

PG_DB_PATH=C:\\Program Files\\Cisco Systems\\dcm\\db

#-----New Postgres-----
DCNM_DB_URL=jdbc\:postgresql://localhost\:5432/dcmdb
DCNM_DB_NAME=dcmdb
SELECTED_DATABASE=postgresql
DCNM_DB_USERNAME=dcnmuser
DCNM_DB_USER_PASSWORD=dcnmuser
```

Oracle データベースを使用している場合は、次のブロックを編集します。


```
#-----DATABASE Properties-----
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#-----
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE

ORA_DB_PATH=C:\\oraclexe\\app\\oracle\\product\\10.2.0\\server
```

ステップ 3 DCNM のユーザー クレデンシャルを設定します。

```
#-----User Configuration-----
#DCNM User Configuration Properties
#If you want to use special characters in DCNM_ADMIN
#credentials, Please use escape character(\) before
#the symbol [For eg. Password "an$6x12" must be specified as "an\$6x12" ].
#-----
DECRYPT_PASSWORDS=FALSE
DCNM_ADMIN_USER=admin
DCNM_ADMIN_USER_PASSWORD=admin123

#-----User Configuration-----
```

ステップ 4 セキュアな暗号方式を有効にします。

```
#-----Secure Ciphers-----
#DCNM uses both strong and weak ciphers when connecting to switches
#If user wants to use only strong ciphers for connection, please set
#property to TRUE. Make sure your switches support strong ciphers before
#setting the property as DCNM will not be able to connect to switches which
#support only weak ciphers.
#-----
SECURE_CIPHER=FALSE
#SECURE_CIPHER=TRUE
#-----
```

ステップ 5 IBM Raven を設定し、IBM Data Center Network Managerをインストールします。

```
#-----IBM Raven Support-----
#Set true if Vendor is IBM, by default false
#-----
IBM_INSTALL=FALSE /*Does not install IBM Data Center Network Manager*/
#-----
```

ステップ 6 Cisco DCNM Windows ソフトウェアをダウンロードしたディレクトリに移動し、次のコマンドを使用して適切なインストーラを実行します。

```
dcnm-release.exe -i silent -f path_of_installer.properties_file
```

タスク マネージャ プロセスでインストールのステータスを確認できます。

ステップ 7 ブラウザを開き、https://<<DCNM_server_IP_Address>> を入力します。

[Return] キーを押して、SAN 管理用の CISCO Dcnm の Web インターフェイスを起動します。

Linux への Cisco DCNM のインストール

Linux に Cisco DCNM をインストールするには、次のタスクを実行します。

Linux への Cisco DCNM のアンインストール

Linux で Cisco DCNM をアンインストールするには、次の手順を実行します。



(注) 同じ順番でこれらの手順に従うことをお勧めします。

始める前に

同じサーバを使用して異なるバージョンの DCNM をインストールする前に、Cisco DCNM インスタンスを完全に削除する必要があります。

手順

- ステップ 1 `/root/Stop_DCNM_Servers` コマンドを使用して DCNM サーバで DCNM サービスを停止します。
- ステップ 2 `<<dcnm_directory_location>/db/uninstall-postgresql` コマンドを使用して Postgres データベースをアンインストールします。
- ステップ 3 `/root/Uninstall_DCNM` コマンドを使用して、Cisco DCNM サーバをアンインストールします。
- ステップ 4 `rm -rf .cisco_mds9000` コマンドを使用して、非表示の `.cisco_mds9000` ファイルを削除します。
- ステップ 5 `rm -rf /var/.com.zerog.registry.xml` コマンドを使用して、ゼロ G レジストリを削除します。
- ステップ 6 `rm -rf InstallAnywhere` コマンドを使用して、非表示の `InstallAnywhere` フォルダを削除します。
- ステップ 7 Cisco DCNM インストールに必要なすべてのポートが空いており、利用できることを確認します。
- ステップ 8 `rm -rf /usr/local/cisco/*` を使用して DCNM ディレクトリを削除します。他のディレクトリに保存した場合は、DCNM ディレクトリを削除します。
- ステップ 9 RHEL システムを再起動します。

Linux への Cisco DCNM のアンインストール

次の例は、Linux で Cisco DCNM をアンインストールするために実行する必要があるコマンドのリストを示しています。

```
[dcnm-linux]# /root/Stop_DCNM_Servers
[dcnm-linux]# /<<dcnm_installed_dir>>/db/uninstall-postgresql
[dcnm-linux]# /root/Uninstall_DCNM
[dcnm-linux]# rm -rf .cisco_mds9000
[dcnm-linux]# rm -rf /var/.com.zerog.registry.xml
[dcnm-linux]# rm -rf .InstallAnywhere
[dcnm-linux]# rm -rf /usr/local/cisco/*
[dcnm-linux]# restart
[dcnm-linux]#
```

Cisco DCNM Linux インストーラおよびプロパティ ファイルのダウンロード

Linux に DCNM をインストールする最初の手順は、`dcnm.bin` ファイルをダウンロードすることです。



Note

フェデレーションアプリケーション機能を使用する予定の場合は、`dcnm.bin` 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、[リリース 11.1(1) (Release 11.1(1))] を選択します。
- ステップ 5** DCNM Linux 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。
インストーラ ファイルの形式は、`dcnm-installer-x64.11.1.1.bin` です。
- ステップ 6** DCNM サイレント インストーラのプロパティ ファイルを検索し、[ダウンロード (Download)] アイコンをクリックします。
このファイルは、サイレント インストール時に使用されます。
- ステップ 7** インストールを開始したときに簡単に見つけることができるように、両方のファイルをディレクトリに保存します。

GUI を使用した Linux への Cisco DCNM のインストール

GUI を使用して DCNM Linux 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** ダウンロードした `dcnm-installer-x64.<release-name>.bin` ファイルを検索します。
`dcnm.bin` インストーラ ファイルを実行します。
[InstallAnywhere 進捗バーが表示され、進行状況が示されます。
- ステップ 2** [はじめに (Introduction)] 画面の指示を読みます。
[OEM ベンダー (OEM Vendor)] ドロップダウン リストからベンダーを選択します。
- Cisco Data Center Network Manager
 - IBM : IBM Data Center Network Manager をインストールする場合。
- [次へ (Next)] をクリックします。
- ステップ 3** フェデレーションセットアップで DCNM がセカンダリ アプライアンスとしてインストールされている場合、[既存のフェデレーションにサーバを追加する (Add server to existing federation)] チェックボックスをオンにします。
- ステップ 4** [セキュア暗号 (Secure Ciphers)] チェックボックスをオンにすると、強力な暗号を持つスイッチだけが DCNM によって検出されます。
- ステップ 5** 初めて DCNM-SAN および SMI-S をインストールする場合、インストールする場所を選択します。[インストール場所 (Install Location)] フィールドで、[選択 (Choose)] をクリックして、適切なフォルダパスを提供します。DCNM がフェデレーションセットアップの一部としてインストールされている場合、[デフォルト フォルダの復元 (Restore Default Folder)] をクリックします。
- [次へ (Next)] をクリックします。
- ステップ 6** DCNM サーバに適切な RDBMS を選択します。
要求に基づいてデータベースを選択します。
- PostgreSQL のインストール : `dcnm.bin` とともにバンドルされている PostgreSQL データベースをインストールします。
 - 既存の PostgreSQL 9.4 : クリーン スキーマを使用してすでに設定されている既存の PostgreSQL データベース。
 - 既存の Oracle 10g/11g/12c : クリーン スキーマを使用してすでに設定されている既存の Oracle データベース。
 - 既存の Oracle 10g/11g/12c RAC : クリーン スキーマを使用してすでに設定されている既存の Oracle データベース。

[サービス名 (Service Name)] フィールドに、Oracle RAC サーバのサービス名を入力します。最大 3 つの IP アドレスを入力します。[OK] をクリックします。DB URL が生成されます。

Cisco DCNM インストーラによって RDBMS がすでにインストールされていることが検出された場合は、[DB URL] フィールドにホスト名が表示されます。

Note 既存の PostgreSQL を使用した Cisco DCNM インストールでは、同じユーザー名によって所有されている DCNM ユーザー名と同じ名前の既存のスキーマが必要です。DCNM ユーザー名のスキーマが存在しない場合、または同じ dcnmuser 名のスキーマを所有していない場合は、「public」という名前のデフォルトのスキーマで表が作成されます。

表がデフォルトスキーマで作成されている場合は、Cisco DCNM のアップグレード後に認証の問題が発生する可能性があります。同じユーザー名で所有する DCNM ユーザー名として、同じ名前を持つスキーマを作成する必要があります。手順については、[ユーザーとスキーマ, on page 143](#)を参照してください。

Note Oracle では、新しいユーザが作成された場合に、ユーザ名と同じ名前のスキーマ名が自動的に作成されます。

[DCNM DB ユーザー (DCNM DB User)] フィールドに、Cisco DCNM がデータベースにアクセスするために使用するユーザー名を入力します。[DCNM DB パスワード (DCNM DB Password)] フィールドに、指定したデータベースユーザーアカウントのパスワードを入力します。[既存のフェデレーションにサーバを追加する (Add Server to an existing federation)] を選択する場合、対応する RDBMS オプションを選択して、データベース URL を変更します。フェデレーション内のすべてのサーバが同じデータベースを参照しているため、プライマリサーバの dcnmuser 名とパスワードを指定する必要があります。

[次へ (Next)] をクリックします。Oracle データベースの制限を確認し、[OK] をクリックします。

[次へ (Next)] をクリックします。

ステップ 7 [ポート設定オプション (Port Configuration Options)] 画面で、Cisco DCNM のインターフェイスと Web ポートを選択します。

- [Server IP Address] リストから、Cisco DCNM サーバで使用する IP アドレスを選択します。このリストには、サーバシステムのネットワーク インターフェイスに現在割り当てられている IP アドレスだけが表示されます。
- Cisco DCNM-SAN Web サーバがリッスンするポートを変更する場合は、[SAN Web Server Port] フィールドに新しいポート番号を入力します。デフォルトでは、Cisco DCNM-SAN Web サーバは TCP ポート 443 をリッスンします。

Note Cisco DCNM のインストール中に、空いているポート番号を使用します。たとえば、87 と 23 は、予約または制限された Web ポートです。

[次へ (Next)] をクリックします。

ステップ 8 [DCNM のアーカイブフォルダを選択する (Choose archive folder for DCNM)] 画面で、フォルダパスを提供し、デバイス設定ファイル、ユーザーの基本設定などを保存します。

次のいずれかを実行します。

- **[選択 (Choose)]** をクリックして、DCNM アーカイブ ディレクトリを保存するパスを選択します。

Note リモート システムを選択する必要がある場合、UNIC パスを提供します。

例：//Server/Share/directorypath.

- **[デフォルト フォルダの復元 (Restore Default Folder)]** をクリックし、デフォルト フォルダを保持します。

[次へ (Next)] をクリックします。

ステップ 9 [ローカル ユーザー クレデンシヤル (Local User Credentials)] 画面で、DCNM SAN アプライアンスの両方にアクセスするための有効なユーザー名とパスワードを入力します。

- **[管理ユーザー名 (Admin Username)]** フィールドに、Cisco DCNM サーバのユーザーの名前を入力します。インストーラによって、Cisco DCNM サーバのユーザーが作成され、そのユーザーに管理者ロールが割り当てられます。
- **[Password]** フィールドにそのユーザーのパスワードを入力し、**[Confirm Password]** フィールドにそのパスワードを再入力します。

次のパスワード要件に従います。要件に準拠していない場合、DCNM アプリケーションが正常に機能しない可能性があります。

- 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。
- 展開モード用の 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> & \$ % ‘ “ ^ = < > ; :

[次へ (Next)] をクリックします。

ステップ 10 [認証設定 (Authentication Settings)] 画面で、Cisco DCNM サーバが Cisco DCNM クライアントにログオンするユーザーを認証するために使用する認証方式を選択します。次のいずれかを選択できます。

- **ローカル** : Cisco DCNM クライアントユーザーは、Cisco DCNM サーバのユーザー アカウントによってのみ認証されます。
- **RADIUS** : Cisco DCNM クライアントユーザーは、RADIUS サーバによって認証されます。
- **TACACS+** : Cisco DCNM クライアントユーザーは、TACACS+ サーバによって認証されます。

ステップ 11 [RADIUS] または [TACACS+] を選択した場合は、次の手順を実行します。

- a) [primary server address] フィールドに、サーバの IPv4 アドレスをドット付き 10 進数形式で入力します。
- b) [primary server key] フィールドに、サーバの共有秘密キーを入力します。
- c) (Optional) Cisco DCNM がサーバと通信可能なことを確認する場合は、[検証 (Verify)] をクリックします。
- d) [secondary server address] フィールドに、サーバの IPv4 アドレスをドット付き 10 進数形式で入力します。
- e) [secondary server key] フィールドに、サーバの共有秘密キーを入力します。
- f) (Optional) Cisco DCNM がサーバと通信可能なことを確認する場合は、[検証 (Verify)] をクリックします。
- g) [tertiary server address] フィールドに、サーバのアドレスをドット付き 10 進数形式で入力します。
- h) [第三次サーバ キー (tertiary server key)] フィールドに、サーバの共有秘密キーを入力します。
- i) (Optional) Cisco DCNM がサーバと通信可能なことを確認する場合は、[検証 (Verify)] をクリックします。

[次へ (Next)] をクリックします。

[リンクの選択 (Choose Link)] フォルダはスキップされ、デフォルトではその場所は /root ディレクトリになります。

ステップ 12 [インストール前の概要 (Pre-Installation Summary)] 画面で、インストール設定を確認します。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。

[次へ (Next)] をクリックします。

ステップ 13 確認ウィンドウで、[はい (Yes)] をクリックし、DCNM インストールを開始します。進捗バーの説明では、インストール中の進行状況を示します。

ステップ 14 [インストール完了 (Install Complete)] 画面で、インストールが完了したコンポーネントが一覧表示されます。[完了 (Done)] をクリックし、DCNM サーバを開始します。

システムに DCNM が展開されるまで待ちます。

ステップ 15 ブラウザを開き、`https://<<DCNM_server_IP_Address>>` を入力します。

[Return] キーを押して、SAN 管理用の CISCO Dcnm の Web インターフェイスを起動します。

GUI を使用したサーバ フェデレーション環境への Cisco DCNM Linux のインストール

サーバ フェデレーション環境で DCNM をインストールするには：

Before you begin

プライマリサーバでDCNMをインストールしていることを確認します。GUIを使用したLinuxへのCisco DCNMのインストール, on page 52 の指示に従ってください。

Procedure

ステップ 1 セカンダリサーバでDCNMをインストールしながら、**[既存のフェデレーションにサーバを追加する (Add server to existing federation)]** チェックボックスをオンにします。

これにより、フェデレーションセットアップでセカンダリ アプライアンスとしてDCNMをインストールします。[事前インストール概要 (Pre-installation Summary)] 画面には、[フェデレーション設定 (Federation Settings)] でフェデレーションステータスとノードを表示します。

ステップ 2 [セキュア暗号 (Secure Ciphers)] チェックボックスをオンにすると、セキュア暗号がプライマリで有効になっている場合にのみ、強力な暗号を持つスイッチだけがDCNMによって検出されます。

Cisco DCNMは、スイッチに接続するときに強力な暗号と脆弱な暗号の両方を使用します。uses both strong and weak ciphers when connecting to switches. ネットワークに強力な暗号のみを使用する場合は、このチェックボックスをオンにします。DCNMは強力な暗号をサポートしていないスイッチに接続できないため、チェックボックスを選択する前にネットワーク内のスイッチが強力な暗号をサポートしていることを確認します。

ステップ 3 対応する RDBMS オプションを選択して、データベース URL を変更します。

Note フェデレーション内のすべてのサーバは同じデータベースを参照するため、プライマリサーバのDCNMユーザー名とパスワードを指定する必要があります。また、プライマリサーバのデータベースユーザー名とパスワードを指定する必要があります。

データベースのユーザー名とパスワードは、フェデレーションを形成するすべてのサーバインストールで同じです。同様に、DCNMのユーザー名とパスワードは、フェデレーションを形成するすべてのサーバインストールで同じです。

サイレントインストールを通して Cisco DCNM Linux をインストールする

Cisco DCNMは、リモート認証モードではなく、ローカル認証モードでのみサイレントインストールをサポートしています。

サイレントインストールを使用してDCNM Linux ウィンドウ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 installer.properties ファイルを解凍、抽出して開き、次のプロパティを更新します。

```
#-----BASIC Properties-----
DCNM_IP_ADDRESS=<ip_address_of_host_machine>
USER_INSTALL_DIR=/usr/local/cisco/dcm
INSTALLATION_TYPE=NEW_INSTALL
#INSTALLATION_TYPE=UPGRADE
SAN_FEDERATION=FALSE
#SAN_FEDERATION=TRUE
```

ステップ 2 データベース パラメータを設定します。

PostgreSQL データベースを使用している場合は、次のブロックを編集します。

```
#-----New Postgress-----
PG_DB_PATH=/usr/local/cisco/dcm/db

#PG_DB_PATH=/opt/dctest/cisco/dcm/db /*non-default installation directory*/
#BACKUP_FILE=/opt/dctest/cisco/dcm/dcnm/bin/<backup-filename> /*non-default backup file
directory*/

DCNM_DB_URL=jdbc\:postgresql\://localhost\:5432/dcmdb
DCNM_DB_NAME=dcmdb
SELECTED_DATABASE=postgresql
DCNM_DB_USERNAME=dcnmuser
DCNM_DB_USER_PASSWORD=dcnmuser
#CLEAN_DATABASE=TRUE
```

Oracle データベースを使用している場合は、次のブロックを編集します。

```
#-----DATABASE Properties-----
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#-----
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE
ORA_DB_PATH=C:\oracle\app\oracle\product\10.2.0\server
```

ステップ 3 DCNM のデータパスを設定します。

```
#-----DATA PATH-----
#Data path is the folder location where DCNM LAN related
#information like Config archives, templates etc. are stored.
# In DCNM LAN Cluster mode this folder has to be a shared folder.
#For linux and windows it will be different as the folder structure varies
#-----
DATA_PATH=/usr/local/cisco/dcm/dcnm
#-----DATA PATH-----
```

ステップ 4 DCNM のユーザー クレデンシャルを設定します。

```
#-----User Configuration-----
#DCNM User Configuration Properties
#If you want to use special characters in DCNM_ADMIN
#credentials,Please use escape character(\) before
#the symbol [For eg. Password "an$6x12" must be specified as "an\$6x12" ].
#-----
```

```

DECRYPT_PASSWORDS=FALSE
DCNM_ADMIN_USER=admin
DCNM_ADMIN_USER_PASSWORD=admin123

#-----User Configuration-----

```

ステップ 5 セキュアな暗号方式を有効にします。

```

#-----Secure Ciphers-----
#DCNM uses both strong and weak ciphers when connecting to switches
#If user wants to use only strong ciphers for connection, please set
#property to TRUE. Make sure your switches support strong ciphers before
#setting the property as DCNM will not be able to connect to switches which
#support only weak ciphers.

#-----
SECURE_CIPHER=FALSE
#SECURE_CIPHER=TRUE
#-----

```

ステップ 6 IBM Raven を設定し、IBM Data Center Network Managerをインストールします。

```

#-----IBM Raven Support-----
#Set true if Vendor is IBM, by default false
#-----

IBM_INSTALL=FALSE /*Does not install IBM Data Center Network Manager*/
#-----

```

ステップ 7 Cisco DCNM Linux ソフトウェアをダウンロードしたディレクトリに移動し、次のコマンドを使用して適切なインストーラを実行します。

```
dcnm-release.bin -i silent -f path_of_installer.properties_file
```

インストールのステータスを確認するには、コマンド **ps -ef | grep 'LAX'** を使用します。サイレントインストールが完了すると、プロンプトが返されます。

ステップ 8 ブラウザを開き、**https://<<DCNM_server_IP_Address>>** を入力します。

[Return]キーを押して、SAN 管理用の Linux で Cisco DCNM の Web インターフェイスを起動します。

オープン仮想アプライアンスで DCNM をインストールする

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/>。
- 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、[11.3(1)] を選択します。
- ステップ 5** 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 6** `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)]、時間の増加が期待されないスイッチ 50 個未満のその他の小規模環境の場合は [小規模 (small-scale)] を選択します。

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

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

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

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

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

SAN Insights 機能を展開する場合は、この設定を選択することを推奨します。

[次へ (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。

[次へ (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で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。

- 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。
- 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 (Show datastores from Storage DRS clusters)**] をオンにします。
- 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。

Note enhanced-fabric-inband ネットワークを設定しない場合、エンドポイントロケータおよびテレメトリ機能は操作できません。

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

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

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

- 両方の OVA には、同じサブネット内に管理アクセス (eth0)、拡張ファブリック管理 (eth1)、およびインバンド管理 (eth2) インターフェイスが必要です。
- 各 OVA には、異なるサブネットに eth0 と eth2 のインターフェイスが必要です。
- 両方の OVA は、同じ管理パスワードを使用して展開する必要があります。これは、両方の OVA がアプリケーション アクセスのため互いに重複していることを確認するためです。パスワードには次の文字を使用しないでください。

[次へ (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。

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

DCNM インストーラは、DCNM VM フォルダに `_deviceImage-0.iso` を作成し、その ISO を VM に永続的にマウントします。この ISO が削除されるか、CD/DVD が切断されると、VM は起動しません。VM は緊急モードに入り、次のメッセージが表示されます。管理用の `root` パスワードを指定します。VM がダウンしている場合は、CD/DVD ドライブの接続を解除できます。ただし、再度電源をオンにすると、VM は緊急モードに入り、プロンプトを表示します。

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 64](#) 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 68](#) 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。
- 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。
[Continue] をクリックします。
- ステップ 3 [管理 (Administration)] タブで、Cisco DCNM オープン仮想アプライアンスのすべて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ます。
次のパスワード要件に従います。要件に準拠していない場合、DCNM アプリケーションが正常に機能しない可能性があります。
 - 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> " & \$ % ' ^ = < > ; : ` \ | / , . *

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

[次へ (Next)] をクリックします。

ステップ 4 [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 [SAN のみ (SAN Only)] インストール モードを選択します。

クラスタ モードで Cisco DCNM を展開する場合は、[クラスタ モードを有効にする (Enable Clustered Mode)] チェックボックスをオンにします。

コンピューティング ノードが Cisco DCNM [Web UI] > [アプリケーション (Applications)] > [コンピューティング (Compute)] に表示されます。後でコンピューティング ノードをクラスタに追加できます。You can add the compute nodes to a Cluster, later.

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

[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。

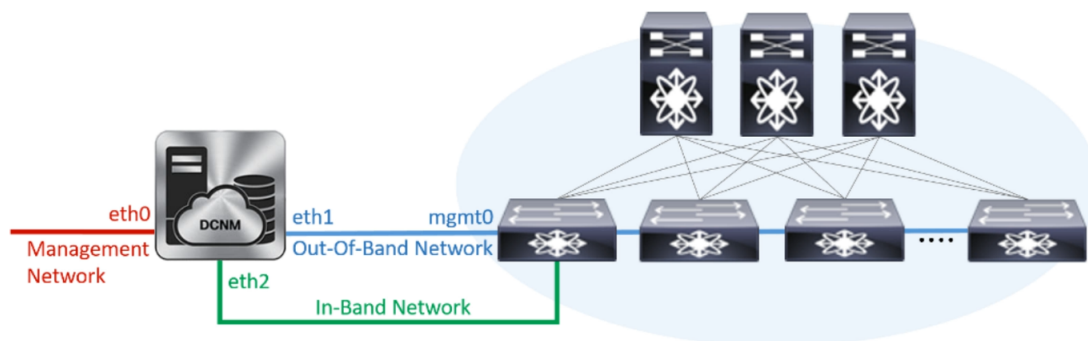
- [完全修飾ホスト名 (Fully Qualified Hostname)] フィールドで、RFC1123 セクション 2.1 の通りに、完全修飾ドメイン名 (FQDN) のホスト名を入力します。
- [DNS サーバアドレス (DNS Server Address)] フィールドで、DNS IP アドレスを入力します。
リリース 11.2(1) から、IPv6 アドレスを使用した DNS サーバも設定できます。
- [NTP サーバ (NTP Server)] フィールドに、NTP サーバの IP アドレスを入力します。
値は IP または IPv6 アドレスか RFC 1123 に準拠し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 DNS サーバと NTP サーバを設定できます。

[次へ (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、ネットワーク パラメータを設定します。

Figure 3: 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、自動入力 IP アドレスとデフォルトゲートウェイ 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 ゲートウェイを設定します。

- b) [アウトオブバンドネットワーク (Out-of-Band Network)] 領域で、IP アドレス、ゲートウェイ IP アドレスを入力します。DCNM が IPv6 ネットワークにある場合、IPv6 アドレスを使用してネットワークを設定します。

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

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

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

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

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

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

[Next] をクリックします。

- ステップ 7** [アプリケーション (Applications)] タブの [IPv4 サブネット (IPv4 Subnet)] フィールドで、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 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。

手順 [ステップ 4, on page 65](#) 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。

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

アドレスは eth1 サブネットから利用可能で小さい IP アドレスのプレフィックスである必要があります。例：eth1 サブネットがインストール中に 10.1.1.0/24 に設定された場合、10.1.1.240/28 を使用します。

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

- b. [アウトオブバンド IPv6 ネットワーク アドレス プール (Out-of-Band IPv6 Network Address Pool)] で、クラスタモードで使用するアウトオブバンド IPv6 ネットワークからアドレス プールを入力します。アドレス プールは IPv6 サブネットである必要があります。

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

アドレスは利用可能な IP アドレスの eth2 サブネットより小さい IP アドレスのプレフィックスである必要があります。例：eth2 サブネットがインストール中に 11.1.1.0/24 に設定された場合、11.1.1.240/28 を使用します。

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

- d. [インバンド IPv6 ネットワーク アドレス プール (In-Band IPv6 Network Address Pool)] で、クラスタモードで使用するインバンド IPv6 ネットワークからアドレス プールを入力します。アドレス プールは IPv6 サブネットである必要があります。

[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>>:2443
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 setup inband-route --subnet switches-fabric-links-IP-subnet/mask
dcnm# appmgr setup inband-route --subnet switch-loopback-IP-subnet>/mask
```

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 setup inband-route --subnet 10.0.0.0/24
dcnm# appmgr setup inband-route --subnet 40.1.1.0/24
```

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。
- b) [Cisco DCNM インストーラ (Cisco DCNM Installer)] 画面で、[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。

[Continue] をクリックします。

- c) [管理 (Administration)] タブで、Cisco DCNM オープン仮想アプライアンスのすべて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ます。

次のパスワード要件に従います。要件に準拠していない場合、DCNM アプリケーションが正常に機能しない可能性があります。

- 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。
- Linux、Windows、OVA、および ISO プラットフォームでは、DCNM パスワードに次の特殊文字を使用しないでください。

<SPACE> " & \$ % ' ^ = < > ; : \ | / , . *

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

[次へ (Next)] をクリックします。

- d) [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 DCNM アプライアンスのインストールモードを選択します。

Check the **Enable Clustered Mode** checkbox, if you want to deploy Cisco DCNM in Cluster mode.

コンピューティング ノードが Cisco DCNM [Web UI] > [アプリケーション (Applications)] > [コンピューティング (Compute)] に表示されます。後でコンピューティング ノードをクラスターに追加できます。You can add the compute nodes to a Cluster, later.

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

[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。

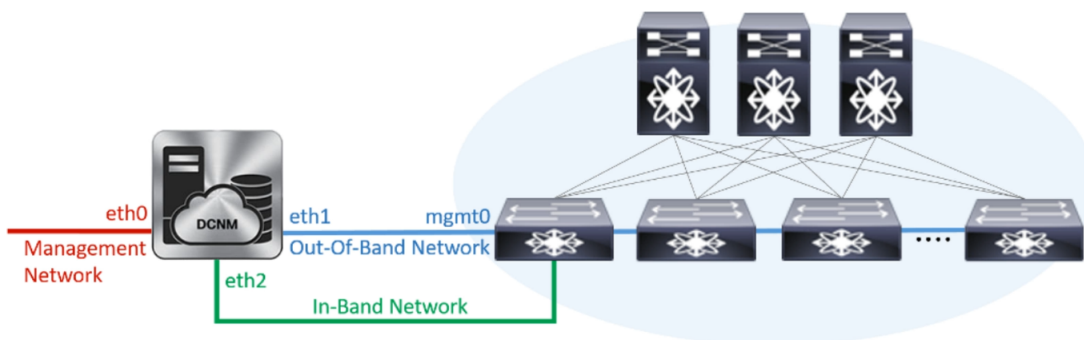
- [完全修飾ホスト名 (Fully Qualified Hostname)] フィールドで、RFC1123 セクション 2.1 の通りに、完全修飾ドメイン名 (FQDN) のホスト名を入力します。
- [DNS サーバアドレス (DNS Server Address)] フィールドで、DNS IP アドレスを入力します。
リリース 11.2(1) から、IPv6 アドレスを使用した DNS サーバも設定できます。
- [NTP サーバ (NTP Server)] フィールドに、NTP サーバの IP アドレスを入力します。
値は IP または IPv6 アドレスか RFC 1123 に準拠し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 DNS サーバと NTP サーバを設定できます。

[次へ (Next)] をクリックします。

f) [ネットワーク設定 (Network Settings)] タブで、ネットワーク パラメータを設定します。

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、自動入力された IP アドレスとデフォルトゲートウェイ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 ゲートウェイを設定します。

- [アウトオブバンドネットワーク (Out-of-Band Network)] 領域で、IP アドレス、ゲートウェイ IP アドレスを入力します。DCNM が IPv6 ネットワークにある場合、IPv6 アドレスを使用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。

- [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 VIP アドレスとゲートウェイ IP アドレスを入力します。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。

- [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 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。

Note プライマリ HA およびセカンダリ HA ノードの両方で同じ IP サブネットを設定していることを確認します。

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 163](#)」を参照してください。

[Next] をクリックします。

- g) [HA 設定 (HA Settings)] タブに確認メッセージが表示されます。

```
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。

- h) [アプリケーション (Applications)] タブの [IPv4 サブネット (IPv4 Subnet)] フィールドで、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 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。

手順 [2.d, on page 69](#) 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。

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

アドレスは eth1 サブネットから利用可能で小さい IP アドレスのプレフィックスである必要があります。例：eth1 サブネットがインストール中に 10.1.1.0/24 に設定された場合、10.1.1.240/28 を使用します。

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

2. [アウトオブバンド IPv6 ネットワーク アドレス プール (Out-of-Band IPv6 Network Address Pool)] で、クラスタ モードで使用するアウトオブバンド IPv6 ネットワークからアドレス プールを入力します。アドレス プールは IPv6 サブネットである必要があります。

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

アドレスは利用可能な IP アドレスの eth2 サブネットより小さい IP アドレスのプレフィックスである必要があります。例：eth2 サブネットがインストール中に 11.1.1.0/24 に設定された場合、11.1.1.240/28 を使用します。

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

4. [インバンド IPv6 ネットワーク アドレス プール (In-Band IPv6 Network Address Pool)] で、クラスタ モードで使用するインバンド IPv6 ネットワークからアドレス プールを入力します。アドレス プールは IPv6 サブネットである必要があります。

[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。
- 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) [管理 (Administration)] タブで、Cisco DCNM オープン仮想アプライアンスのすべて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ます。

Note セカンダリ ノードのパスワードは、手順 2.c, on page 69 で入力したプライマリの管理パスワードと同じである必要があります。

[次へ (Next)] をクリックします。

- d) [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 ノードに対して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。

[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。

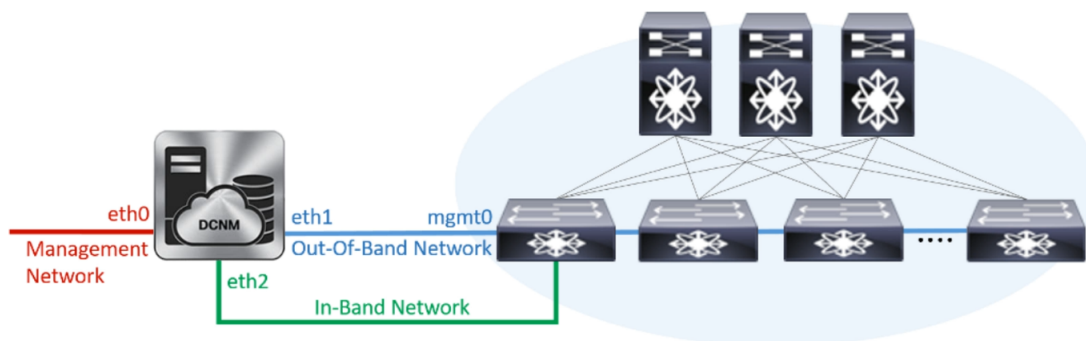
- [完全修飾ホスト名 (Fully Qualified Hostname)] フィールドで、RFC1123 セクション 2.1 の通りに、完全修飾ドメイン名 (FQDN) のホスト名を入力します。
- [DNS サーバアドレス (DNS Server Address)] フィールドで、DNS IP アドレスを入力します。
リリース 11.2(1) から、IPv6 アドレスを使用した DNS サーバも設定できます。
- [NTP サーバ (NTP Server)] フィールドに、NTP サーバの IP アドレスを入力します。
値は IP または IPv6 アドレスか RFC 1123 に準拠し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 DNS サーバと NTP サーバを設定できます。

[次へ (Next)] をクリックします。

- f) [ネットワーク設定 (Network Settings)] タブで、ネットワーク パラメータを設定します。

Figure 5: 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、自動入力された IP アドレスとデフォルトゲートウェイ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。

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 ゲートウェイを設定します。

- [アウトオブバンドネットワーク (Out-of-Band Network)] 領域で、IP アドレス、ゲートウェイ IP アドレスを入力します。DCNM が IPv6 ネットワークにある場合、IPv6 アドレスを使用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 HA セットアップが正常に完了するために、IP アドレス、IP アドレス ゲートウェイ、および IPv6 アドレスがプライマリ ノードで設定されているものと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。

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。

アウトオブバンド管理ネットワークの IPv6 アドレスを設定することもできます。

- [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 IP アドレスおよびゲートウェイ IP アドレスを入力します。インバンド ネットワークにより、前面パネルのポートを介してデバイスへ到達可能になります。

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

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

- [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 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。

Note プライマリ HA およびセカンダリ HA ノードの両方で同じ IP サブネットを設定していることを確認します。

[次へ (Next)] をクリックします。

- g) [アプリケーション (Applications)] タブの [IPv4 サブネット (IPv4 Subnet)] フィールドで、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 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。

Note プライマリ HA およびセカンダリ HA ノードの両方で同じ IP サブネットを設定していることを確認します。

[次へ (Next)] をクリックします。

- h) [HA 設定 (HA Settings)] タブで、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。
- 管理ネットワーク VIP アドレス、VIPv6 アドレス、および OOB ネットワーク VIP アドレスを適切に入力します。

Note IPv6 アドレスを使用して管理ネットワークを設定している場合は、管理ネットワークの VIPv6 アドレスを設定していることを確認します。

- VIP の IPv6 アドレスを設定するには、OOB ネットワーク VIPv6 アドレスと入力します。
- [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 VIP アドレスを入力します。

これは、インバンドネットワークの VIP アドレスです。[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。

- 必要に応じて HA ping IP アドレスを入力します。

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 IP アドレスを設定して、スプリットブレインのシナリオを避ける必要があります。このアドレスは、拡張ファブリック管理ネットワークに属している必要があります。

[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 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>>:2443
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 setup inband-route --subnet switches-fabric-links-IP-subnet/mask
dcnm# appmgr setup inband-route --subnet switch-loopback-IP-subnet>/mask
```

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 setup inband-route --subnet 10.0.0.0/24
dcnm# appmgr setup inband-route --subnet 40.1.1.0/24
```

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、[11.3(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 85](#) 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 78](#) を参照してください。

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

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

```

Note インバンド インターフェイスを設定しない場合、エンドポイント ロケータおよび テレメトリ機能は操作できません。

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

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) 01:00:0 Intel Corporation Ethernet Controller 106 X550T (rev 01)
   Address: 78:69:5a:40:1a:e6   Link:UP
2) 01:00:1 Intel Corporation Ethernet Controller 106 X550T (rev 01)
   Address: 78:69:5a:40:1a:e7   Link:UP
3) d8:00:0 Intel Corporation 1350 Gigabit Network Connection (rev 01)
   Address: b4:96:91:27:df:00   Link:UP
4) d8:00:1 Intel Corporation 1350 Gigabit Network Connection (rev 01)
   Address: b4:96:91:27:df:01   Link:UP
5) d8:00:2 Intel Corporation 1350 Gigabit Network Connection (rev 01)
   Address: b4:96:91:27:df:02   Link:UP
6) d8:00:3 Intel Corporation 1350 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 1350 Gigabit Network Connection (rev 01)
   Address: a8:93:51:89:55:f2   Link:DOWN
10) 3b:00:1 Intel Corporation 1350 Gigabit Network Connection (rev 01)
   Address: a8:93:51:89:55:f3   Link:DOWN
11) 3b:00:2 Intel Corporation 1350 Gigabit Network Connection (rev 01)
   Address: a8:93:51:89:55:f4   Link:DOWN
12) 3b:00:3 Intel Corporation 1350 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:98   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 87 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 91 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 **dcnm-va-ovf-kvm-files.11.3.1.zip** 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 **dcnm-va.11.3.1.iso** 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。必要な場合、インバンド インターフェイス (eth2) も設定できます。

Note インバンド インターフェイス (eth2) を設定しない場合、エンドポイント ロケータおよびテレメトリ機能は操作できません。

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

- 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 87](#) 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 91](#) 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。

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。

[Continue] をクリックします。

ステップ 3 [管理 (Administration)] タブで、Cisco DCNM オープン仮想アプライアンスのすべて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ます。

次のパスワード要件に従います。要件に準拠していない場合、DCNM アプリケーションが正常に機能しない可能性があります。

- 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> " & \$ % ' ^ = < > ; : ' \ | / , . *

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

[次へ (Next)] をクリックします。

ステップ 4 [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 [SAN のみ (SAN Only)] インストール モードを選択します。

クラスタ モードで Cisco DCNM を展開する場合は、[クラスタ モードを有効にする (Enable Clustered Mode)] チェックボックスをオンにします。

コンピューティング ノードが Cisco DCNM [Web UI] > [アプリケーション (Applications)] > [コンピューティング (Compute)] に表示されます。後でコンピューティング ノードをクラスタに追加できます。You can add the compute nodes to a Cluster, later.

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

[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。

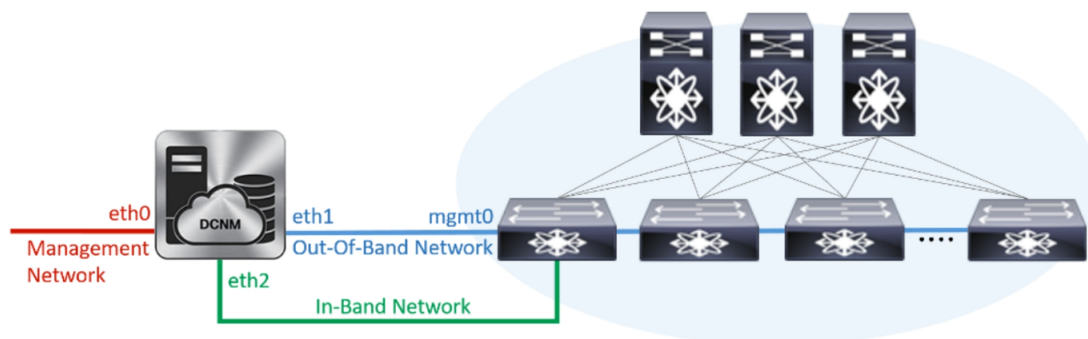
- [完全修飾ホスト名 (Fully Qualified Hostname)] フィールドで、RFC1123 セクション 2.1 の通りに、完全修飾ドメイン名 (FQDN) のホスト名を入力します。
- [DNS サーバアドレス (DNS Server Address)] フィールドで、DNS IP アドレスを入力します。
リリース 11.2(1) から、IPv6 アドレスを使用した DNS サーバも設定できます。
- [NTP サーバ (NTP Server)] フィールドに、NTP サーバの IP アドレスを入力します。
値は IP または IPv6 アドレスか RFC 1123 に準拠し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 DNS サーバと NTP サーバを設定できます。

[次へ (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、ネットワーク パラメータを設定します。

Figure 6: 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、自動入力 IP アドレスとデフォルトゲートウェイ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 ゲートウェイを設定します。

- b) [アウトオブバンドネットワーク (Out-of-Band Network)] 領域で、IP アドレス、ゲートウェイ IP アドレスを入力します。DCNM が IPv6 ネットワークにある場合、IPv6 アドレスを使用してネットワークを設定します。

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

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

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

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

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

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

[Next] をクリックします。

ステップ 7 [アプリケーション (Applications)] タブの [IPv4 サブネット (IPv4 Subnet)] フィールドで、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 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。

手順 [ステップ 4, on page 87](#) 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。

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

アドレスは eth1 サブネットから利用可能で小さい IP アドレスのプレフィックスである必要があります。例：eth1 サブネットがインストール中に 10.1.1.0/24 に設定された場合、10.1.1.240/28 を使用します。

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

- b. [アウトオブバンド IPv6 ネットワーク アドレス プール (Out-of-Band IPv6 Network Address Pool)]で、クラスタモードで使用するアウトオブバンド IPv6 ネットワークからアドレス プールを入力します。アドレス プールは IPv6 サブネットである必要があります。

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

アドレスは利用可能な IP アドレスの eth2 サブネットより小さい IP アドレスのプレフィックスである必要があります。例：eth2 サブネットがインストール中に 11.1.1.0/24 に設定された場合、11.1.1.240/28 を使用します。

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

- d. [インバンド IPv6 ネットワーク アドレス プール (In-Band IPv6 Network Address Pool)]で、クラスタモードで使用するインバンド IPv6 ネットワークからアドレス プールを入力します。アドレス プールは IPv6 サブネットである必要があります。

[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>>:2443
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 にログインします。

[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 setup inband-route --subnet switches-fabric-links-IP-subnet/mask
dcnm# appmgr setup inband-route --subnet switch-loopback-IP-subnet>/mask
```

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 setup inband-route --subnet 10.0.0.0/24
dcnm# appmgr setup inband-route --subnet 40.1.1.0/24
```

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。
- b) [Cisco DCNM インストーラ (Cisco DCNM Installer)] 画面で、[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。

[Continue] をクリックします。

- c) [管理 (Administration)] タブで、Cisco DCNM オープン仮想アプライアンスのすべて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ます。

次のパスワード要件に従います。要件に準拠していない場合、DCNM アプリケーションが正常に機能しない可能性があります。

- 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。
- Linux、Windows、OVA、および ISO プラットフォームでは、DCNM パスワードに次の特殊文字を使用しないでください。

<SPACE> " & \$ % ' ^ = < > ; : ` \ | / , . *`

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

[次へ (Next)] をクリックします。

- d) [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 DCNM アプライアンスのインストール モードを選択します。

Check the **Enable Clustered Mode** checkbox, if you want to deploy Cisco DCNM in Cluster mode.

コンピューティング ノードが Cisco DCNM [Web UI] > [アプリケーション (Applications)] > [コンピューティング (Compute)] に表示されます。後でコンピューティング ノードをクラスタに追加できます。You can add the compute nodes to a Cluster, later.

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

[次へ (Next)] をクリックします。

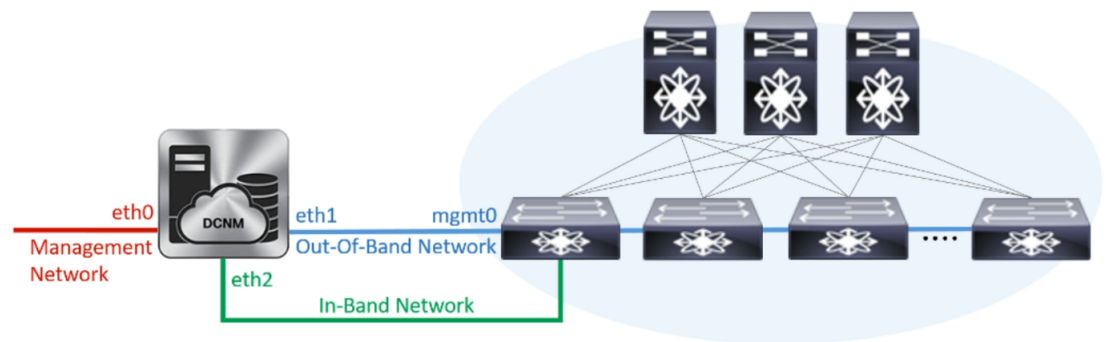
- e) [システム設定 (System Settings)] で、DCNM アプライアンスの設定を行います。
- [完全修飾ホスト名 (Fully Qualified Hostname)] フィールドで、RFC1123 セクション 2.1 の通りに、完全修飾ドメイン名 (FQDN) のホスト名を入力します。
 - [DNS サーバアドレス (DNS Server Address)] フィールドで、DNS IP アドレスを入力します。
リリース 11.2(1) から、IPv6 アドレスを使用した DNS サーバも設定できます。
 - [NTP サーバ (NTP Server)] フィールドに、NTP 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 DNS サーバと NTP サーバを設定できます。

[次へ (Next)] をクリックします。

- f) [ネットワーク設定 (Network Settings)] タブで、ネットワーク パラメータを設定します。

Figure 7: 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、自動入力された IP アドレスとデフォルトゲートウェイ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 ゲートウェイを設定します。

- [アウトオブバンドネットワーク (Out-of-Band Network)] 領域で、IP アドレス、ゲートウェイ IP アドレスを入力します。DCNM が IPv6 ネットワークにある場合、IPv6 アドレスを使用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。

- [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 VIP アドレスとゲートウェイ IP アドレスを入力します。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。

- [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 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。

Note プライマリ HA およびセカンダリ HA ノードの両方で同じ IP サブネットを設定していることを確認します。

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 163](#)」を参照してください。

[Next] をクリックします。

- g) [HA 設定 (HA Settings)] タブに確認メッセージが表示されます。

```
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。

- h) [アプリケーション (Applications)] タブの [IPv4 サブネット (IPv4 Subnet)] フィールドで、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 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。

手順 [2.d, on page 92](#) 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。

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

アドレスは eth1 サブネットから利用可能で小さい IP アドレスのプレフィックスである必要があります。例：eth1 サブネットがインストール中に 10.1.1.0/24 に設定された場合、10.1.1.240/28 を使用します。

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

2. [アウトオブバンド IPv6 ネットワーク アドレス プール (Out-of-Band IPv6 Network Address Pool)] で、クラスタモードで使用するアウトオブバンド IPv6 ネットワークからアドレス プールを入力します。アドレス プールは IPv6 サブネットである必要があります。

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

アドレスは利用可能な IP アドレスの eth2 サブネットより小さい IP アドレスのプレフィックスである必要があります。例：eth2 サブネットがインストール中に 11.1.1.0/24 に設定された場合、11.1.1.240/28 を使用します。

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

4. [インバンド IPv6 ネットワーク アドレス プール (In-Band IPv6 Network Address Pool)] で、クラスタモードで使用するインバンド IPv6 ネットワークからアドレス プールを入力します。アドレス プールは IPv6 サブネットである必要があります。

[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。
- 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) [管理 (Administration)] タブで、Cisco DCNM オープン仮想アプライアンスのすべて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ます。

Note セカンダリ ノードのパスワードは、手順 [2.c, on page 92](#) で入力したプライマリの管理パスワードと同じである必要があります。

[次へ (Next)] をクリックします。

- d) [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 ノードに対して選択したものと同一インストール モードを選択します。

Note プライマリ ノードと同じインストール モードを選択しない場合、HA のインストールは失敗します。

[次へ (Next)] をクリックします。

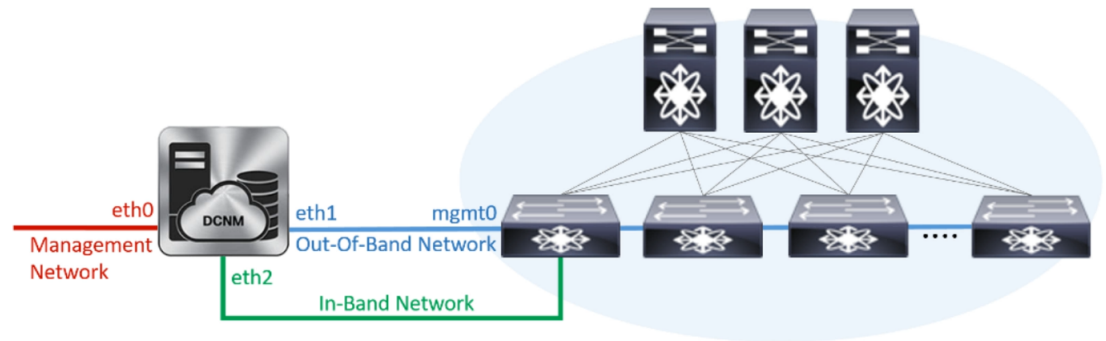
- e) [システム設定 (System Settings)] で、DCNM アプライアンスの設定を行います。
 - [完全修飾ホスト名 (Fully Qualified Hostname)] フィールドで、RFC1123 セクション 2.1 の通りに、完全修飾ドメイン名 (FQDN) のホスト名を入力します。
 - [DNS サーバアドレス (DNS Server Address)] フィールドで、DNS IP アドレスを入力します。
リリース 11.2(1) から、IPv6 アドレスを使用した DNS サーバも設定できます。
 - [NTP サーバ (NTP Server)] フィールドに、NTP 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 DNS サーバと NTP サーバを設定できます。

[次へ (Next)] をクリックします。

- f) [ネットワーク設定 (Network Settings)] タブで、ネットワーク パラメータを設定します。

Figure 8: 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、自動入力された IP アドレスとデフォルトゲートウェイ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。

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 ゲートウェイを設定します。

- [アウトオブバンドネットワーク (Out-of-Band Network)] 領域で、IP アドレス、ゲートウェイ IP アドレスを入力します。DCNM が IPv6 ネットワークにある場合、IPv6 アドレスを使用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 HA セットアップが正常に完了するために、IP アドレス、IP アドレス ゲートウェイ、および IPv6 アドレスがプライマリ ノードで設定されているものと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。

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。

アウトオブバンド管理ネットワークの IPv6 アドレスを設定することもできます。

- [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 IP アドレスおよびゲートウェイ IP アドレスを入力します。インバンドネットワークにより、前面パネルのポートを介してデバイスへ到達可能になります。

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

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

- [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 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。

Note プライマリ HA およびセカンダリ HA ノードの両方で同じ IP サブネットを設定していることを確認します。

[次へ (Next)] をクリックします。

- g) [アプリケーション (Applications)] タブの [IPv4 サブネット (IPv4 Subnet)] フィールドで、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 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。

Note プライマリ HA およびセカンダリ HA ノードの両方で同じ IP サブネットを設定していることを確認します。

[次へ (Next)] をクリックします。

- h) [HA 設定 (HA Settings)] タブで、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。
- 管理ネットワーク VIP アドレス、VIPv6 アドレス、および OOB ネットワーク VIP アドレスを適切に入力します。

Note IPv6 アドレスを使用して管理ネットワークを設定している場合は、管理ネットワークの VIPv6 アドレスを設定していることを確認します。

- VIP の IPv6 アドレスを設定するには、OOB ネットワーク VIPv6 アドレスと入力します。
- [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 VIP アドレスを入力します。

これは、インバンドネットワークの VIP アドレスです。[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。

- 必要に応じて HA ping IP アドレスを入力します。

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 IP アドレスを設定して、スプリットブレインのシナリオを避ける必要があります。このアドレスは、拡張ファブリック管理ネットワークに属している必要があります。

[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 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>>:2443
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

適切なクレデンシアルを使用して 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 setup inband-route --subnet switches-fabric-links-IP-subnet/mask
dcnm# appmgr setup inband-route --subnet switch-loopback-IP-subnet>/mask
```

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 setup inband-route --subnet 10.0.0.0/24
dcnm# appmgr setup inband-route --subnet 40.1.1.0/24
```

SAN クライアントおよびデバイス マネージャの起動

ここでは、Cisco DCNM SAN クライアントとデバイス マネージャを起動するためのさまざまな方法について説明します。

Web UI からの SAN Client および Device Manager の起動

Cisco DCNM SAN クライアントとデバイス マネージャを Cisco DCNM Web UI から起動するには、次の手順を実行します。

手順

ステップ 1 Cisco DCNM SAN 展開をインストールした後、Cisco DCNM Web UI にログインします。

ステップ 2 歯車アイコンをクリックし、**[DCNM SAN および DM (DCNM SAN & DM)]** をクリックします。

dcnm-client.zip をディレクトリに保存します。

ステップ 3 dcnm-client.zip の内容を dcnm-clientzip/bin ディレクトリに抽出します。

ステップ 4 SAN クライアントとデバイス マネージャを起動するには、次のようにします。

- **Windows 環境で DCNM を起動する場合は、次のようにします。**

FMClient.bat ファイルをダブルクリックして、CISCO DCNM SAN クライアントを起動します。

DeviceManager.bat をダブルクリックして、CISCO Dcnm デバイス マネージャを起動します。

- **Linux 環境で DCNM を起動する場合は、次のようにします。**

./FMClient.sh スクリプトを実行して、SAN クライアントを起動します。

./Devicemanager.sh スクリプトを実行して、デバイス マネージャを起動します。

DCNM サーバから SAN クライアントおよびデバイス マネージャを起動する

デフォルトでは、DCNM をインストールするときに、SAN クライアントとデバイス マネージャが Cisco DCNM サーバとともにインストールされます。Cisco DCNM SAN クライアントとデバイス マネージャを Cisco DCNM サーバから起動するには、次の手順を実行します。

Procedure

- ステップ 1** DCNM サーバにログインします。
- ステップ 2** Cisco Systems\dcm\fm\bin\ ディレクトリに移動します。
- ステップ 3** SAN クライアントとデバイス マネージャを起動するには、次のようにします。

- **Windows 展開の場合:**

FabricManager.bat ファイルをダブルクリックして、Cisco DCNM SAN クライアントを起動します。

DeviceManager.bat ファイルをダブルクリックして、Cisco DCNM デバイス マネージャを起動します。

- **Linux 展開の場合:**

./FabricManager.sh スクリプトを実行して、Cisco DCNM SAN クライアントを起動します。

./DeviceManager.sh スクリプトを実行して、Cisco DCNM デバイス マネージャを起動します。

SSL が有効な Windows 展開のための DCNM SAN からの DCNM SAN クライアントの起動

DCNM サーバに設定されたカスタム SSL を使用して Windows 向け Cisco DCNM をインストールすると、SAN クライアントを起動できなくなります。証明書を変更して、SAN クライアントを正常に起動します。

証明書を変更し、Windows 展開から DCNM SAN クライアントを起動するには、次の手順を実行します。

Procedure

- ステップ 1** **keytool.exe -exportcert -file dcnmweb.crt -alias sme C:[DCNM Install directory]\cisco\dcm\wildfly-14.0.1.Final\Standalone\configuration\fmserver.jks** コマンドを使用して公開キーを抽出します。

```
// extract public key from the new fmserver.jks and save it to dcnmweb.crt, alias "sme",  
password "fmserver_1_2_3"  
c:[DCNM install directory]\dcm\java\jdk11\bin>keytool.exe -exportcert -file dcnmweb.crt  
-alias sme C:[DCNM Install  
directory]\cisco\dcm\wildfly-14.0.1.Final\Standalone\configuration\fmserver.jks  
Enter keystore password:  
Certificate stored in file <dcnmweb.crt>  
c:[DCNM install directory]\dcm\java\jdk11\bin>dir
```

```
chain-cert.pem dcnmweb.crt jjs          keytool  rmiregistry
dcnm.csr       java          jrunscript  rmid
```

ステップ 2 **keytool.exe -importcert -trustcacerts -file dcnmweb.crt -keystore fmtrust.jks -storetype jks** コマンドを使用してキー ストアを生成します。

```
// generate key store without password, during the command, just use random password
dcnm123
c:\[DCNM install dirrectory]\dcm\java\jdk11\bin>keytool.exe -importcert -trustcacerts
-file dcnmweb.crt -keystore fmtrust.jks -storetype jks
Enter keystore password:
Re-enter new password:
Owner: CN=Lin, OU=cisco, O=cisco, L=sj, ST=ca, C=US
Issuer: CN=rhell144, OU=DCBu, O=Cisco, L=BGL, ST=KA, C=IN
Serial number: 1086
Valid from: Wed Nov 13 12:17:23 PST 2019 until: Thu Nov 12 12:17:23 PST 2020
Certificate fingerprints:
    SHA1: F8:19:CB:79:FC:93:08:54:74:9A:BC:F3:8F:CB:9C:A7:22:56:3D:0F
    SHA256:
8F:06:1F:72:15:FD:12:B5:E9:43:E4:61:0E:00:E0:1C:96:CE:9C:90:82:3C:5C:EA:A1:49:A8:A9:66:9B:86:31
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.16.840.1.113730.1.13 Criticality=false
0000: 16 1D 4F 70 65 6E 53 53 4C 20 47 65 6E 65 72 61 ..OpenSSL Genera
0010: 74 65 64 20 43 65 72 74 69 66 69 63 61 74 65 ted Certificate

#2: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: C9 1E 9B 17 EF AE E4 AF 7A E3 88 BC 2D C9 B9 E9 .....z....
0010: FC EC 40 82 ..@.
]
]#3: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:false
PathLen: undefined
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 9A 9E B4 98 95 8C 9F FB 0B 57 A5 6D 78 EB 8D C1 .....W.mx...
0010: BB 80 00 DE ....
]
]

Trust this certificate? [no]: yes
Certificate was added to keystore
c:\[DCNM install dirrectory]\dcm\java\jdk11\bin>dir
chain-cert.pem dcnmweb.crt java jrunscript rmid
dcnm.csr fmtrust.jks jjs keytool rmiregistry
```

ステップ 3 新しく作成した **fmtrust.jks** を `\fm\lib\fm` ディレクトリにコピーします。

```
c:\[DCNM install dirrectory]\dcm\java\jdk11\bin>cp fmtrust.jks ..\..\fm\lib\fm
cp: overwrite â..\..\fm\lib\fm\fmtrust.jks? y
```

ステップ 4 Web UI または DCNM サーバからダウンロードした **dcnm-client** を見つけます。

ステップ 5 `bin\fmtrust.jks` を解凍して、新しく作成した **fmtrust.jks** ファイルに置き換えます。

ステップ 6 **FabricManager.bat** のバッチ ファイルを実行して、CISCO DCNM SAN クライアントを起動します。

SSL が有効な Linux 展開のための DCNM SAN からの DCNM SAN クライアントの起動

DCNM サーバでカスタム SSL が設定された Linux に Cisco DCNM をインストールすると、SAN クライアントを起動できません。SAN クライアントを正常に起動するには、証明書を変更する必要があります。

証明書を変更し、Linux 展開から DCNM SAN クライアントを起動するには、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公開キーを抽出します。

```
./keytool -exportcert -file dcnmweb.crt -alias sme -keystore  
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks
```

ステップ 2 次のコマンドを使用してキー ストアを生成します。

```
./keytool -importcert -trustcacerts -file dcnmweb.crt -keystore fmtrust.jks -storetype jks
```

ステップ 3 新しく作成した **fmtrust** を /fm/lib/fm ディレクトリにコピーします。

ステップ 4 Web UI または DCNM サーバからダウンロードした **dcnm-client** を見つけます。

ステップ 5 /bin ディレクトリ内の **fmtrust.jks** を、新しく作成した **fmtrust.jks** ファイルに置き換えます。

ステップ 6 **./FabricManager.sh** スクリプトを実行して、Cisco DCNM SAN クライアントを起動します。

Example

次のサンプル例は、証明書を変更し、Linux 展開から DCNM SAN クライアントを起動するコマンドを示しています。

```
// extract public key from the new fmserver.jks and save it to dcnmweb.crt,  
alias "sme", password "fmserver_1_2_3"  
[root@dcnm-lnx1 bin]# ./keytool -exportcert -file dcnmweb.crt -alias sme  
-keystore /usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks  
Enter keystore password:  
Certificate stored in file <dcnmweb.crt>  
[root@dcnm-M5-2-lnx1 bin]# ls  
chain-cert.pem dcnmweb.crt jjjs keytool rmiregistry  
dcnm.csr java jrunscript rmid
```

```

// generate key store without password, during the command,
just use random password dcnml23
[root@dcnm-lnx1 bin]# ./keytool -importcert -trustcacerts -file dcnmweb.crt
-keystore fmtrust.jks -storetype jks
Enter keystore password:
Re-enter new password:
Owner: CN=Lin, OU=cisco, O=cisco, L=sj, ST=ca, C=US
Issuer: CN=rhell144, OU=DCBu, O=Cisco, L=BGL, ST=KA, C=IN
Serial number: 1086
Valid from: Wed Nov 13 12:17:23 PST 2019 until: Thu Nov 12 12:17:23 PST 2020
Certificate fingerprints:
    SHA1: F8:19:CB:79:FC:93:08:54:74:9A:BC:F3:8F:CB:9C:A7:22:56:3D:0F
    SHA256: 8F:06:1F:72:15:FD:12:B5:E9:43:E4:61:0E:00:E0:1C:96:CE:9C:90:82:
           3C:5C:EA:A1:49:A8:A9:66:9B:86:31
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.16.840.1.113730.1.13 Criticality=false
0000: 16 1D 4F 70 65 6E 53 53 4C 20 47 65 6E 65 72 61 ..OpenSSL Genera
0010: 74 65 64 20 43 65 72 74 69 66 69 63 61 74 65 ted Certificate

#2: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: C9 1E 9B 17 EF AE E4 AF 7A E3 88 BC 2D C9 B9 E9 .....z...-...
0010: FC EC 40 82 ..@.
]
]

#3: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:false
PathLen: undefined
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 9A 9E B4 98 95 8C 9F FB 0B 57 A5 6D 78 EB 8D C1 .....W.mx...
0010: BB 80 00 DE ....
]
]

Trust this certificate? [no]: yes
Certificate was added to keystore
[root@dcnm-M5-2-lnx1 bin]# ls
chain-cert.pem dcnmweb.crt java jrunscript rmid
dcnm.csr fmtrust.jks jjs keytool rmiregistry
[root@dcnm-M5-2-lnx1 bin]# pwd
/usr/local/cisco/dcm/java/jdk11/bin

[root@dcnm-M5-2-lnx1 bin]#

[root@dcnm-M5-2-lnx1 bin]# cp fmtrust.jks ../../fm/lib/fm
cp: overwrite ../../fm/lib/fm/fmtrust.jks? y

[root@dcnm-M5-2-lnx1 dcm]# cd fm/download/
[root@dcnm-M5-2-lnx1 download]# pwd
/usr/local/cisco/dcm/fm/download
[root@dcnm-M5-2-lnx1 download]# ls

```



```
dcnm-clientzip.zip
// for remote access, in fm/download/dcnm-clientzip.zip,
replace bin/fmtrust.jks with this new fmtrust.jks
```

```
[root@dcnm-M5-2-lnx1 bin]# ./ FabricManager.sh
```

SSL が有効な OVA/ISO 展開のための DCNM SAN からの DCNM SAN クライアントの起動

DCNM サーバに設定されたカスタム SSL を使用して Cisco DCNM SAN OVA/ISO をインストールすると、SAN クライアントを起動できなくなります。CA 署名付き証明書をインストールしてから、Web UI から DCNM SAN クライアントをダウンロードして起動します。

Cisco DCNM SAN OVA/ISO サーバに CA 署名付き証明書をインストールする方法については、[CA 署名付き証明書のインストール \(152 ページ\)](#) を参照してください。

Web UI を起動します。DCNM SAN クライアントをダウンロードします。DCNM SAN クライアントとデバイス マネージャを起動します。



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 107](#)
- [CA 署名済み証明書の保持, on page 108](#)
- [Windows で Cisco SAN にアップグレードする \(109 ページ\)](#)
- [Linux で Cisco SAN にアップグレードする \(113 ページ\)](#)
- [OVA/ISO での Cisco SAN へのアップグレード \(118 ページ\)](#)

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。ただし、SAN OVA/ISO のアップグレードパスはありません。

リリース 11.3(1) 以降では、Cisco DCNM OVA および ISO は SAN 機能に対してサポートされています。

次の表は、リリース 11.3(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 6: Cisco DCNM SAN 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 11.3(1) にアップグレードするアップグレードタイプ
11.2(1)	<p>Windows 向け：インラインアップグレード</p> <p>Linux向け：インラインアップグレード</p> <p>OVA\ISO 向け：</p> <ol style="list-style-type: none"> 1. 新しい 11.3(1) SAN のみのインストール。 2. パフォーマンス マネージャの収集を停止します。 <p>Note 古いパフォーマンス マネージャ データは、11.3(1) の既存のパフォーマンス マネージャ データを置き換えます。</p>
11.1(1)	<p>Windows 向け：インラインアップグレード</p> <p>Linux向け：インラインアップグレード</p> <p>OVA\ISO 向け：</p> <ol style="list-style-type: none"> 1. 新しい 11.3(1) SAN のみのインストール。 2. パフォーマンス マネージャの収集を停止します。 <p>Note 古いパフォーマンス マネージャ データは、11.3(1) の既存のパフォーマンス マネージャ データを置き換えます。</p>
10.4(2) OVA 10.4 (1) OVA	<p>11.3(1) OVA\ISO 向け：</p> <ol style="list-style-type: none"> 1. 新しい 11.3(1) SAN のみのインストール。 2. パフォーマンス マネージャの収集を停止します。 <p>Note 古いパフォーマンス マネージャ データは、11.3(1) の既存のパフォーマンス マネージャ データを置き換えます。</p>

CA 署名済み証明書の保持

アップグレード後に CA 署名付き SSL 証明書を保持する必要がある場合は、次の手順を実行します。

キーストアのパスワードまたはエイリアスを変更する場合は、次の場所にある **standalone-san** ドキュメントで更新する必要があることに注意してください。

```
< DCNM_install_root >  
\dcm\wildfly-14.0.1.Final\standalone\configuration\standalone-san.xml
```

keystore タグとエイリアスのパスワードを更新します。

```
<keystore key-password>="fmserver_1_2_3 key-alias="updated-key-alias"  
keystore-password="updated-password"  
path="<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks">
```

Procedure

ステップ 1 次の場所から署名付き証明書をバックアップします。

- Windows の場合 :
 <DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks
- Linux の場合 :
 <DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks

ステップ 2 Cisco DCNM リリース 11.3(1) にアップグレードします。

ステップ 3 アップグレード後、Cisco DCNM のアップグレードされたバージョンと同じ場所に証明書をコピーします。

Note [ステップ 1, on page 109](#)に記載されているのと同じ場所に証明書をロードする必要があります。

ステップ 4 DCNM サービスを再起動します。

Windows で Cisco SAN にアップグレードする

ここでは、Windows の Cisco DCNM SAN を最新バージョンにアップグレードする手順について説明します。

Windows で Cisco DCNM をアンインストールする

Windows で Cisco DCNM をアンインストールするには、次の手順を実行します。



(注) 同じ順番でこれらの手順に従うことをお勧めします。

始める前に

同じサーバを使用して異なるバージョンの DCNM をインストールする前に、Cisco DCNM i インスタンスを完全に削除する必要があります。

手順

-
- ステップ 1 Cisco DCNM サービスを停止します。
 - ステップ 2 Postgres データベースをアンインストールします。
 - ステップ 3 Cisco DCNM をアンインストールします。
 - ステップ 4 C:\Users\Administrator に移動し、**cisco_mds9000** フォルダを削除します。
 - ステップ 5 C:\Program Files\Zero G Registry に移動し、**ゼロ G レジストリ** フォルダを削除します。
 - ステップ 6 C:\Users\Administrator に移動し、**installanywhere** フォルダを削除します。
 - ステップ 7 Cisco DCNM インストールに必要なすべてのポートが空いており、利用できることを確認します。
 - ステップ 8 Cisco DCNM ディレクトリを削除します。
 - ステップ 9 Windows VM を再起動します。
-

GUI を使用した Cisco DCNM Linux のアップグレード

開始する前に、Cisco DCNM 11.1(1) または 11.2(1) がアップ状態であり実行中であることを確認します。

Procedure

-
- ステップ 1 DCNM サービスを停止します。
 - ステップ 2 リリース 実行可能ファイルの Cisco DCNM ソフトウェアを実行します。
アップグレード通知ウィンドウが表示されます
 - ステップ 3 **[OK]** をクリックして、アップグレードを開始します。
 - ステップ 4 アップグレードが完了したら、**[完了 (Done)]** をクリックします。
Cisco DCNM リリース サービスは自動的に開始されます。
-

GUI を使用した Cisco DCNM Windows フェデレーションのアップグレード

開始する前に、Cisco DCNM 11.1(1) または 11.2(1) がアップ状態であり実行中であることを確認します。



Note プライマリとセカンダリの両方のデータベース プロパティが同じであることを確認します。

Procedure

- ステップ 1** プライマリおよびセカンダリ DCNM サービスの両方を停止します。
- ステップ 2** プライマリ サーバで、Cisco DCNM リリース 実行可能ファイルを実行します。
アップグレード通知ウィンドウが表示されます。
- ステップ 3** **[OK]** をクリックして、アップグレードを開始します。
- ステップ 4** プライマリ サーバでアップグレードが完了したら、**[完了 (Done)]** をクリックします。
Cisco DCNM リリース サービスはプライマリおよびセカンダリ サーバで自動的に開始されます。
- ステップ 5** セカンダリ サーバで、Cisco DCNM リリース 実行可能ファイルを実行します。
アップグレード通知ウィンドウが表示されます。
- ステップ 6** **[OK]** をクリックして、アップグレードを開始します。
- ステップ 7** セカンダリ サーバでアップグレードが完了したら、**[完了 (Done)]** をクリックします。
Cisco DCNM リリース サービスはセカンダリ サーバで自動的に開始されます。

サイレントインストールを通して Cisco DCNM Windows をアップグレードする

開始する前に、Cisco DCNM 11.1(1) または 11.2(1) がアップ状態であり実行中であることを確認します。



Note Cisco DCNM は、リモート認証モードではなく、ローカル認証モードでのみサイレントインストールおよびアップグレードをサポートしています。

Procedure

ステップ 1 DCNM サービスを停止します。

ステップ 2 インストーラのプロパティ ファイルを開き、次のプロパティを更新します。

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE

ORA_DB_PATH=C:\oracle\app\oracle\product\10.2.0\server
#-----Use Existing Oracle-----
DCNM_DB_URL=jdbc\:oracle\:thin\:@<ip_address_of_oracle_machine>:1521:XE
DCNM_DB_NAME=XE
SELECTED_DATABASE=oracle
DCNM_DB_USERNAME=oracledbadmin1
DCNM_DB_USER_PASSWORD=oracledbadmin1
```

ステップ 3 Cisco DCNM ソフトウェアをダウンロードしたディレクトリに移動し、次のコマンドを使用して適切なインストーラを実行します。

```
dcnm-release.exe -i silent -f <path_of_installer.properties>
```

Cisco DCNM リリース サービスは、アップグレードの完了後に開始されます。

タスク マネージャ プロセスでアップグレードのステータスを確認できます。

サイレントインストールを通して Cisco DCNM Windows フェデレーションをアップグレードする

開始する前に、Cisco DCNM 11.1(1) または 11.2(1) がアップ状態であり実行中であることを確認します。



Note Cisco DCNM は、リモート認証モードではなく、ローカル認証モードでのみサイレントインストールおよびアップグレードをサポートしています。



Note プライマリとセカンダリの両方のデータベース プロパティが同じであることを確認します。

Procedure

ステップ 1 プライマリおよびセカンダリ DCNM サービスの両方を停止します。

ステップ 2 プライマリ サーバで、`installer.properties` ファイルを開き、次のプロパティを更新します。

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
```


ステップ 3 Cisco DCNM ソフトウェアをダウンロードしたディレクトリに移動し、次のコマンドを使用して適切なインストーラを実行します。

```
dcnm-release.exe -i silent -f <path_of_installer.properties>
```

タスク マネージャ プロセスでアップグレードのステータスを確認できます。

Cisco DCNM リリース サービスはプライマリおよびセカンダリ サーバで自動的に開始されます。

ステップ 4 セカンダリ サーバで、`installer.properties` ファイルを開き、次のプロパティを更新します。

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE

ORA_DB_PATH=C:\\oraclexe\\app\\oracle\\product\\10.2.0\\server
#-----Use Existing Oracle-----
DCNM_DB_URL=jdbc\:oracle\:thin\:@<ip_address_of_oracle_machine>\:1521\:XE
DCNM_DB_NAME=XE
SELECTED_DATABASE=oracle
DCNM_DB_USERNAME=oracledbadmin1
DCNM_DB_USER_PASSWORD=oracledbadmin1
```

ステップ 5 Cisco DCNM ソフトウェアをダウンロードしたディレクトリに移動し、次のコマンドを使用して適切なインストーラを実行します。

```
dcnm-release.exe -i silent -f <path_of_installer.properties>
```

タスク マネージャ プロセスでアップグレードのステータスを確認できます。

Cisco DCNM リリース サービスはセカンダリ サーバで自動的に開始されます。

Linux で Cisco SAN にアップグレードする

ここでは、Linux の Cisco DCNM SAN を最新バージョンにアップグレードする手順について説明します。

Linux への Cisco DCNM のアンインストール

Linux で Cisco DCNM をアンインストールするには、次の手順を実行します。



(注) 同じ順番でこれらの手順に従うことをお勧めします。

始める前に

同じサーバを使用して異なるバージョンの DCNM をインストールする前に、Cisco DCNM i インスタンスを完全に削除する必要があります。

手順

-
- ステップ 1 `/root/Stop_DCNM_Servers` コマンドを使用して DCNM サーバで DCNM サービスを停止します。
 - ステップ 2 `<<dcnm_directory_location>/db/uninstall-postgresql` コマンドを使用して Postgres データベースをアンインストールします。
 - ステップ 3 `/root/Uninstall_DCNM` コマンドを使用して、Cisco DCNM サーバをアンインストールします。
 - ステップ 4 `rm -rf .cisco_mds9000` コマンドを使用して、非表示の `.cisco_mds9000` ファイルを削除します。
 - ステップ 5 `rm -rf /var/.com.zerog.registry.xml` コマンドを使用して、ゼロ G レジストリを削除します。
 - ステップ 6 `rm -rf .InstallAnywhere` コマンドを使用して、非表示の `InstallAnywhere` フォルダを削除します。
 - ステップ 7 Cisco DCNM インストールに必要なすべてのポートが空いており、利用できることを確認します。
 - ステップ 8 `rm -rf /usr/local/cisco/*` を使用して DCNM ディレクトリを削除します。他のディレクトリに保存した場合は、DCNM ディレクトリを削除します。
 - ステップ 9 RHEL システムを再起動します。
-

Linux への Cisco DCNM のアンインストール

次の例は、Linux で Cisco DCNM をアンインストールするために実行する必要があるコマンドのリストを示しています。

```
[dcnm-linux]# /root/Stop_DCNM_Servers
[dcnm-linux]# /<<dcnm_installed_dir>>/db/uninstall-postgresql
[dcnm-linux]# /root/Uninstall_DCNM
[dcnm-linux]# rm -rf .cisco_mds9000
[dcnm-linux]# rm -rf /var/.com.zerog.registry.xml
[dcnm-linux]# rm -rf .InstallAnywhere
[dcnm-linux]# rm -rf /usr/local/cisco/*
[dcnm-linux]# restart
[dcnm-linux]#
```

GUI を使用した Cisco DCNM Linux のアップグレード

開始する前に、Cisco DCNM 11.1(1) または 11.2(1) がアップ状態であり実行中であることを確認します。

Procedure

-
- ステップ 1 DCNM サービスを停止します。
 - ステップ 2 リリース 実行可能ファイルの Cisco DCNM ソフトウェアを実行します。

アップグレード通知ウィンドウが表示されます

ステップ 3 **[OK]** をクリックして、アップグレードを開始します。

ステップ 4 アップグレードが完了したら、**[完了 (Done)]** をクリックします。

Cisco DCNM リリース サービスは自動的に開始されます。

What to do next

Linux スタンドアロン サーバで Cisco DCNM リリース 11.2(1) からアップグレードした後は、Web UI を起動して SAN クライアントをダウンロードする前に、ブラウザのキャッシュと Java コンソール キャッシュを消去していることを確認してください。Java コンソールには、以前のバージョンの SAN クライアントデータが記憶されています。Java コンソール キャッシュを消去しないと、ダウンロードした最新の SAN クライアントを使用できなくなります。

GUI を使用した Cisco DCNM Linux フェデレーションのアップグレード

開始する前に、Cisco DCNM 11.1(1) または 11.2(1) がアップ状態であり実行中であることを確認します。



Note

プライマリとセカンダリの両方のデータベース プロパティが同じであることを確認します。

Procedure

ステップ 1 プライマリおよびセカンダリ DCNM サービスの両方を停止します。

ステップ 2 プライマリ サーバで、Cisco DCNM リリース 実行可能ファイルを実行します。

アップグレード通知ウィンドウが表示されます。

ステップ 3 **[OK]** をクリックして、アップグレードを開始します。

ステップ 4 プライマリ サーバでアップグレードが完了したら、**[完了 (Done)]** をクリックします。

Cisco DCNM リリース サービスはプライマリおよびセカンダリ サーバで自動的に開始されます。

ステップ 5 セカンダリ サーバで、Cisco DCNM リリース 実行可能ファイルを実行します。

アップグレード通知ウィンドウが表示されます。

ステップ 6 **[OK]** をクリックして、アップグレードを開始します。

ステップ 7 セカンダリ サーバでアップグレードが完了したら、**[完了 (Done)]** をクリックします。

Cisco DCNM リリース サービスはセカンダリ サーバで自動的に開始されます。

サイレントインストールを通して Cisco DCNM Linux をアップグレードする

開始する前に、Cisco DCNM 11.1(1) または 11.2(1) がアップ状態であり実行中であることを確認します。



Note Cisco DCNM は、リモート認証モードではなく、ローカル認証モードでのみサイレントインストールおよびアップグレードをサポートしています。



Note 既存の DCNM セットアップの場合と同じように、リリースには同じデータベースを使用する必要があります。

Procedure

ステップ 1 DCNM サービスを停止します。

ステップ 2 `installer.properties` ファイルを開き、次のプロパティを更新します。

```
INSTALLATION_TYPE=UPGRADE
USE_EXISTING_DB=TRUE
```

ステップ 3 Cisco DCNM ソフトウェアをダウンロードしたディレクトリに移動し、次のコマンドを使用して適切なインストーラを実行します。

```
dcnm-release.bin -i silent -f <path_of_installer.properties>
```

Cisco DCNM リリース サービスは、アップグレードの完了後に開始されます。

コマンド `ps -ef | grep 'LAX'` を使用して、アップグレードプロセスのステータスを確認できます。サイレントインストールが完了すると、プロンプトが返されます。

サイレントインストールを通して Cisco DCNM Linux フェデレーションをアップグレードする

開始する前に、Cisco DCNM 11.1(1) または 11.2(1) がアップ状態であり実行中であることを確認します。



Note Cisco DCNM は、リモート認証モードではなく、ローカル認証モードでのみサイレントインストールおよびアップグレードをサポートしています。



Note プライマリとセカンダリの両方のデータベース プロパティが、以前のリリース セットアップと同じであることを確認します。

Procedure

ステップ 1 プライマリおよびセカンダリ DCNM サービスの両方を停止します。

ステップ 2 プライマリ サーバで、`installer.properties` ファイルを開き、次のプロパティを更新します。

```
INSTALLATION_TYPE=UPGRADE  
USE_EXISTING_DB=TRUE
```

ステップ 3 Cisco DCNM ソフトウェアをダウンロードしたディレクトリに移動し、次のコマンドを使用して適切なインストーラを実行します。

```
dcnm-release.bin -i silent -f <path_of_installer.properties>
```

コマンド `ps -ef | grep 'LAX'` を使用して、アップグレードプロセスのステータスを確認できます。サイレントインストールが完了すると、プロンプトが返されます。

Cisco DCNM リリース サービスはプライマリおよびセカンダリ サーバで自動的に開始されません。

ステップ 4 プライマリ サーバで、アップグレードが完了したら、**Done** をクリックします。

Cisco DCNM リリース サービスはプライマリおよびセカンダリ サーバで自動的に開始されません。

ステップ 5 セカンダリ サーバで、`installer.properties` ファイルを開き、次のプロパティを更新します。

```
INSTALLATION_TYPE=UPGRADE  
USE_EXISTING_DB=TRUE
```

ステップ 6 Cisco DCNM ソフトウェアをダウンロードしたディレクトリに移動し、次のコマンドを使用して適切なインストーラを実行します。

```
dcnm-release.bin -i silent -f <path_of_installer.properties>
```

コマンド `ps -ef | grep 'LAX'` を使用して、アップグレードプロセスのステータスを確認できます。サイレントインストールが完了すると、プロンプトが返されます。

Cisco DCNM リリース サービスはセカンダリ サーバで自動的に開始されます。

OVA/ISO での Cisco SAN へのアップグレード

リリース 11.3(1) から、OVA/ISO に Cisco DCNM SAN をインストールできます。ただし、以前のリリースの DCNM をリリース 11.3(1) に移行することはできません。代わりに、OVA または ISO で SAN 用 Cisco DCNM の新規インストールを実行し、Performance Manager データを古いバージョンからインポートします。

PM データの移行

OVA/ISO の DCNM SAN へのアップグレードパスはありません。ただし、Cisco DCNM 11.3(1) の新規インストールでは、次のリリースから Performance Manager データを移行することができます。

- 11.2(1) SAN から 11.3(1) SAN OVA/ISO
- 11.1(1) SAN から 11.3(1) SAN OVA/ISO
- 10.4(2) SAN OVA から 11.3(1) SAN OVA/ISO



(注) Performance manager データを移行する前に、Cisco DCNM 11.3(1) で Performance Manager が停止していることを確認します。アップグレードが完了したら、Performance Manager のデータ収集を開始する必要があります。



(注) Cisco DCNM 11.3(1) で新たに収集されたデータは、移行した Performance Manager 収集データに置換されます。

古いリリースからの SAN Insights データ

古いリリースからの SAN Insights データは大きすぎるため、2 週間ごとに更新されます。SAN Insight データを新しい DCNM 11.3(1) OVA/ISO インストールに移行しないことをお勧めします。

ファブリックでパフォーマンスモニタリングを使用している場合は、この項の手順を使用して Performance Manager データを移行します。ただし、この手順では、Elasticsearch データベース内のすべての内容がコピーされます。したがって、この手順を実行する前に、次のコマンドを使用して DCNM にデータをストリーミングしている各スイッチの SAN Insights データを削除します。

```
<DCNM Install Location>\dcm\fm\bin\FMGeneric.bat com.cisco.dcbu.analytics.CleanupSanInsightES
<switchname_in_lowercase> <switch_ip_address>
```

```
C:\Program Files\CiscoDCNM\dcm\fm\bin\FMGeneric.bat
com.cisco.dcbu.analytics.CleanupSanInsightES mds9396t-174145 xxx.xx.xxx.xxx
```

ここでは、新しくインストールされた Cisco DCNM 11.3(1) アプライアンスに PM データを移行する手順について説明します。

10.4(x) SAN OVA/ISO/Windows から新しい DCNM 11.3(1) OVA/ISO への PM データ移行

リリース 10.4(1) OVA または 10.4(2) OVA では、パフォーマンス マネージャは RRD をデータベースとして使用してすべての raw データを保存します。Cisco DCNM は、RRD ファイルを柔軟なデータベースに移行するためのインライン移行プロセスを提供します。

10.4(1) または 10.4(2) OVA データを 11.3(1) OVA/ISO に移行するには、次の手順を実行します。

手順

ステップ 1 DCNM 10.4 (1) または 10.4(2) サーバを停止します。

Windows の場合 : C:\Program Files\cisco それ Systems\dcm\dcm\bin に移動します。stopLANSANServer.bat をダブルクリックして、サービスを停止します。

Linux の場合 : /root へのログオンします。/root/Stop_DCNM_Servers コマンドを使用して、サービスを停止します。

ステップ 2 RRD ファイルが配置されている /usr/local/cisco/dcm/fm/pm/db に移動します。

RRD ファイルを安全な場所にコピーします。

Windows の場合 : [RRD] ファイル フォルダを右クリックし、[コピー (Copy)] をクリックします。安全なディレクトリに内容を貼り付けます。

Linux : コピー /usr/local/cisco/dcm/fm/pm/db/<<rrd_directory>> を実行して、すべての RRD ファイルを安全なディレクトリにコピーします。

ステップ 3 新しくインストールされた DCNM 11.3 (1) SAN OVA/ISO サーバで、同じファブリックを検出します。

ステップ 4 ファブリック検出の後、[SAN 収集 (SAN Collections)] を有効にして、パフォーマンス マネージャの収集を開始します。

Cisco DCNM [Web UI] > [管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバステータス (Server Status)] > [パフォーマンス コレクタ (Performance Collector)] を選択します。
[ステータス (Status)] 列を確認します。

Cisco DCNM Web UI からパフォーマンス マネージャがデータを収集するために、DCNM サーバを 60 ~ 70 分許可します。

ステップ 5 `appmgr root-access permit` コマンドを使用して、DCNM サーバへの root アクセスを提供します。

ステップ 6 11.3(1) DCNM サーバで、/usr/local/cisco/dcm/fm/pm/db/ ディレクトリに移動します。
古い DCNM からこのディレクトリに RRD ファイルをコピーします。

11.1(1) および 11.2(1) 以降から 11.3(1) OVA/ISO の新規インストールへの PM データの移行

ステップ 7 `chmod -R 777` コマンドを使用して、すべての RRD ファイルに対する読み取りおよび書き込み権限を変更します。

ステップ 8 [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。

パフォーマンス コレクタ サービスを特定します。

ステップ 9 [アクション (Actions)] 列で、[サービスの停止 (Stop Service)] アイコンをクリックして、パフォーマンス コレクタ サービスを停止します。[サービスの再起動 (Re(Start) Service)] アイコンをクリックして、収集を開始します。

DCNM Server	Actions	Service Name	Status
10.106.177.26 10.106.177.36		Database Server	Running
localhost		Search Indexer	Last updated: 2019-12-02 22:30:00
localhost		Performance Collector	Running. Collecting 188 entities. 99% response in last hour. last DB update: 2019/12/02 22:57
10.106.177.158		Performance Collector	Running. Collecting 77 entities. 100% response in last hour. last DB update: 2019/12/02 22:57
10.106.177.152		SMI-S Agent	Running
10.106.177.152		Nexus Pipeline	Running
10.106.177.152		Elasticsearch	Running
10.106.177.152		SAN Insights	Running

RRD ファイルの量によっては、移行にかかる時間が長くなることがあります。データの移行後に、移行したすべての RRD ファイルが `db_backup` にコピーされます。Web UI から履歴データを表示できます。

11.1(1) および 11.2(1) 以降から 11.3(1) OVA/ISO の新規インストールへの PM データの移行



(注) Windows フェデレーションのデータをリリース 11.3(1) SAN OVA/ISO 展開を移行できません。

新規インストール 11.3(1) OVA では、同じファブリックを検出し、パフォーマンス マネージャを有効にします。古いデータを 11.3(1) にインポートするとき、データを 11.3(1) の既存のデータに置換します。

11.1(1) または 11.2(1) DCNM Windows パフォーマンス マネージャデータを 11.3(1) SAN OVA/ISO 展開に移行するには、次の手順を実行します。

手順

ステップ 1 古い DCNM バージョンで伸縮検索サービスを停止します。

11.1(1) および 11.2(1) 以降から 11.3(1) OVA/ISO の新規インストールへの PM データの移行

```

    creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/
    creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/

    creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IIDbdw/

    creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IIDbdw/0/

    creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IIDbdw/0/index/

    inflating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IIDbdw/0/index/segments_11

    extracting:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IIDbdw/0/index/write.lock

    extracting:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IIDbdw/0/index/_lay.dii

    inflating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IIDbdw/0/index/_lay.dim

    .
    ..
    ...
    ending: inflating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/CmZQjhtS-WGxyPOTlkrw/_state/state-13.st
    extracting:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/node.lock

    creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/_state/
    inflating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/_state/global-7.st
    extracting:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/_state/node-0.st
Started AFW Server Processes
Started AFW Agent Processes
dcnm11-3-1#

```

データが移行されるまでおよそ 30 分間待ちます。

ステップ 7 `docker ps` コマンドを使用して伸縮検索のステータスを確認します。

```

dcnm11-3-1# docker ps
CONTAINER ID        IMAGE                                     COMMAND
CREATED           STATUS          PORTS                    NAMES
8dfa2935cb0d      127.0.0.1:5000/afwapiproxy:2.0         "/bin/entry.sh"
20 seconds ago    Up 17 seconds  0.0.0.0:443->443/tcp     AfwApiProxy
6839a3d88cb4      127.0.0.1:5001/saninsightpost:1.0      "java -Xms1G -Xmx7..."
20 seconds ago    Up 17 seconds
saninsightpost_Cisco_afw.9hfm7g3g016y7as0f8e4e288m.qk3gw8a4wmlg7pg8k4rsx4qme
6bbdff07fc8a      127.0.0.1:5001/epltwo:2.0              "/bin/sh -c /usr/l..."
22 seconds ago    Up 19 seconds
epttwo_Cisco_afw.9hfm7g3g016y7as0f8e4e288m.0newc0fzplfrqt08i8xjdx5h
896336c7689a      127.0.0.1:5001/saninsightcol:1.0       "/bin/pipeline.sh "
23 seconds ago    Up 20 seconds
saninsightcol_Cisco_afw.9hfm7g3g016y7as0f8e4e288m.vzqkxe8owuf9y18icawns3abw
9bc609916781      127.0.0.1:5001/dcnmelastic:5.6.7_11.2.2 "/docker-entrypoin..."

```

```

25 seconds ago      Up 22 seconds      9200/tcp, 9300/tcp
elasticsearch_Cisco_afw.9hfm7g3g0l6y7as0f8e4e288m.owdosoyelrco3rr4790429zky
ee78966aef89        127.0.0.1:5000/registry:2      "/sbin/entry.sh"
26 seconds ago      Up 23 seconds
registry_cisco_afw.1.xwsd9lty6oajfp7ukfvw2iutd
cc635ab41796        registry:2                  "/sbin/entry.sh"
42 seconds ago      Up 40 seconds      AfwAppRegistry

```

ステップ 8 `apmgr restart all` コマンドを使用して DCNM サーバを再起動します。

DCNM が安定し、新しいパフォーマンスマネージャデータに接続するまで 10 分待機します。

11.1(1) および 11.2(1) Linux 以降から 11.3(1) OVA/ISO の新規インストールへの PM データの移行



(注) Linux フェデレーションのデータをリリース 11.3(1) SAN OVA/ISO 展開を移行できません。

新規インストール 11.3(1) OVA では、同じファブリックを検出し、パフォーマンスマネージャを有効にします。古いデータを 11.3(1) にインポートするとき、データを 11.3(1) の既存のデータに置換します。

11.1(1) または 11.2(1) DCNM Linux パフォーマンスマネージャデータを 11.3(1) SAN OVA/ISO 展開に移行するには、次の手順を実行します。

手順

ステップ 1 古い DCNM バージョンで伸縮検索サービスを停止します。

Web UI で、[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。パフォーマンスマネージャの収集を停止します。

ステップ 2 \\DCNM_Install_Directory\dcm\elasticsearch\data\にあるパフォーマンスマネージャ収集ディレクトリ ファイルのバックアップを取得します。

すべてのファイルを圧縮し、ファイルを安全な場所に保存します。

(注) 圧縮したファイルには root フォルダとノードおよびデータが入ったすべてのサブフォルダが必要です。

```

[root@dcnm]# unzip -l nodes.zip
Archive:  nodes.zip
  Length   Date       Time    Name
-----
0         10-15-2019 04:34   nodes/
0         10-15-2019 04:34   nodes/0/
0         10-15-2019 04:34   nodes/0/indices/
0         10-15-2019 04:34   nodes/0/indices/5AJ72Xv0SXXkfxaD9IDMbdw/
0         10-15-2019 04:34   nodes/0/indices/5AJ72Xv0SXXkfxaD9IDMbdw/0/
0         10-15-2019 04:34   nodes/0/indices/5AJ72Xv0SXXkfxaD9IDMbdw/0/index/

```

```

615 10-15-2019 04:33 nodes/0/indices/5AJ72Xv0SXXfXaD9IDMbdw/0/index/segments_11
0 10-10-2019 00:28 nodes/0/indices/5AJ72Xv0SXXfXaD9IDMbdw/0/index/write.lock
82 10-15-2019 03:58 nodes/0/indices/5AJ72Xv0SXXfXaD9IDMbdw/0/index/_lay.dii
.
.
.
2037 10-10-2019 00:28 nodes/0/indices/CMzGQjhtS-W3xyPoTlktnw/_state/state-13.st
0 10-10-2019 00:12 nodes/0/node.lock
0 10-15-2019 04:34 nodes/0/_state/
4668 10-10-2019 00:24 nodes/0/_state/global-7.st
71 10-10-2019 00:12 nodes/0/_state/node-0.st
-----
129921151 487 files
[root@dcnm]#

```

ステップ 3 `zip -r myPMData.zip ./` コマンドを使用して、すべてのファイルを圧縮し、ファイルを安全な場所に保存します。

(注) 圧縮したファイルには root フォルダとノードおよびデータが入ったすべてのサブフォルダが必要です。

```

[root@dcnm]# zip -r nodes.zip nodes
adding: nodes/ (stored 0%)
adding: nodes/0/ (stored 0%)
adding: nodes/0/indices/ (stored 0%)
adding: nodes/0/indices/CMzGQjhtS-W3xyPoTlktnw/ (stored 0%)
adding: nodes/0/indices/CMzGQjhtS-W3xyPoTlktnw/3/ (stored 0%)
adding: nodes/0/indices/CMzGQjhtS-W3xyPoTlktnw/3/index/ (stored 0%)
adding: nodes/0/indices/CMzGQjhtS-W3xyPoTlktnw/3/index/_114o.fdx (deflated 2%)
adding: nodes/0/indices/CMzGQjhtS-W3xyPoTlktnw/3/index/_lbsm.fnm (deflated 87%)
adding: nodes/0/indices/CMzGQjhtS-W3xyPoTlktnw/3/index/_lcs1.si (deflated 23%)
adding: nodes/0/indices/CMzGQjhtS-W3xyPoTlktnw/3/index/_lbsm.si (deflated 38%)
.
.
.
adding: nodes/0/indices/5AJ72Xv0SXXfXaD9IDMbdw/2/_state/ (stored 0%)
adding: nodes/0/indices/5AJ72Xv0SXXfXaD9IDMbdw/2/_state/state-0.st (deflated 5%)
adding: nodes/0/indices/5AJ72Xv0SXXfXaD9IDMbdw/_state/ (stored 0%)
adding: nodes/0/indices/5AJ72Xv0SXXfXaD9IDMbdw/_state/state-3.st (deflated 9%)
adding: nodes/0/node.lock (stored 0%)
adding: nodes/0/_state/ (stored 0%)
adding: nodes/0/_state/global-7.st (deflated 72%)
adding: nodes/0/_state/node-0.st (deflated 7%)
[root@dcnm]#

```

ステップ 4 11.3(1) DCNM サーバでは、`appmgr root-access permit` コマンドを使用して root アクセスを DCNM サーバに提供します。

ステップ 5 圧縮したファイルを新しくインストールした DCNM 11.3(1) SAN OVA\ISO サーバにコピーします。

(注) 圧縮したファイル コンテンツを安全なディレクトリにコピーできます。

ステップ 6 DCNM 11.3 (1) Linux SAN アプライアンスでパフォーマンス マネージャを停止します。

ステップ 7 `appmgr migrate-pm-es-data` コマンドを使用してパフォーマンス マネージャ データを移行します。

(注) 古いバージョンの DCNM パフォーマンス マネージャ データが移行された後、元の 11.3(1) パフォーマンス マネージャ データが消去されます。

```

dcnm11-3-1# appmgr migrate-pm-es-data nodes.zip
stop elasticsearch
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Archive: nodes.zip
  creating: /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/
    creating:
  /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/
    creating:
  /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/
    creating:
  /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDMdw/
    creating:
  /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDMdw/0/
    creating:
  /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDMdw/0/index/
    inflating:
  /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDMdw/0/index/segments_11
    extracting:
  /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDMdw/0/index/write.lock
    extracting:
  /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDMdw/0/index/_lay.dii
    inflating:
  /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDMdw/0/index/_lay.dim
    .
    ..
    ...
    ending: inflating:
  /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/CmzCQjhtS-W3xyP0t1ktrw/_state/state-13.st
    extracting:
  /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/node.lock
    creating:
  /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/_state/
    inflating:
  /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/_state/global-7.st
    extracting:
  /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/_state/node-0.st
Started AFW Server Processes
Started AFW Agent Processes
dcnm11-3-1#

```

データが移行されるまでおよそ 30 分間待ちます。

ステップ 8 docker ps コマンドを使用して伸縮検索のステータスを確認します。

```

dcnm11-3-1# docker ps
CONTAINER ID        IMAGE                                     COMMAND
CREATED            STATUS              PORTS              NAMES
8dfa2935cb0d       127.0.0.1:5000/afwapiproxy:2.0         "/bin/entry.sh"
20 seconds ago    Up 17 seconds      0.0.0.0:443->443/tcp  AfwApiProxy
6839a3d88cb4       127.0.0.1:5001/saninsightpost:1.0      "java -Xms1G -Xmx7..."
20 seconds ago    Up 17 seconds

```

```

saninsightpost_Cisco_afw.9hfm7g3g016y7as0f8e4e288m.qk3gw8a4wmlg7pg8k4rsx4qme
6bbdff07fc8a      127.0.0.1:5001/epltwo:2.0      "/bin/sh -c /usr/l..."
22 seconds ago    Up 19 seconds
epltwo_Cisco_afw.9hfm7g3g016y7as0f8e4e288m.0newc0fzplfrqt08i8xjdx5h
896336c7689a      127.0.0.1:5001/saninsightcol:1.0  "/bin/pipeline.sh "
23 seconds ago    Up 20 seconds
saninsightcol_Cisco_afw.9hfm7g3g016y7as0f8e4e288m.vzqkxe8owuf9y18icawns3abw
9bc609916781      127.0.0.1:5001/dcnmelastic:5.6.7_11.2.2  "/docker-entrypoin..."
25 seconds ago    Up 22 seconds      9200/tcp, 9300/tcp
elasticsearch_Cisco_afw.9hfm7g3g016y7as0f8e4e288m.owdosoyelrco3rr4790429zky
ee78966aef89      127.0.0.1:5000/registry:2      "/sbin/entry.sh"
26 seconds ago    Up 23 seconds
registry_cisco_afw.1.xwsd91ty6oajfp7ukfvw2iutd
cc635ab41796      registry:2      "/sbin/entry.sh"
42 seconds ago    Up 40 seconds      AfwAppRegistry

```

ステップ 9 `appmgr restart all` コマンドを使用して DCNM サーバを再起動します。

DCNM が安定し、新しいパフォーマンスマネージャデータに接続するまで 10 分待機します。



第 6 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 127](#)
- [カスタム ファイアウォールの設定 \(139 ページ\)](#)

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、Cisco DCNMSAN クライアント、Cisco デバイスマネージャ接続はファイアウォールを通過します。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。

Cisco DCNM リリース 11.0(1) 以降では、DCNM SAN クライアントは、HTTPS ポート 443 で DCNM SAN サーバとの通信を開始します。ただし、DCNM SAN クライアントとデバイス マネージャは両方ともデバイスと直接通信します。デバイス マネージャは DCNM SAN サーバ UI を使用して起動でき、DCNM SAN サーバのコンテキスト内で動作します。デバイス マネージャとデバイスとの通信は、個別に実行されている場合と同様に変わりません。

DCNM SNMP サーバの DCNM SNMP プロキシ サービスは、DCNM SAN クライアントまたはデバイス マネージャ、DCNM サーバの間の SNMP 通信に設定可能な TCP ポート (デフォルトは 9198) を使用します。

UDP SNMP_TRAP ローカル ポートは、Cisco DCNM-SAN およびデバイス マネージャの両方で 1163 ~ 1170 の間です。Cisco DCNM-SAN Client および Device Manager は、使用可能な最初の UDP ポートを使用して、SNMP 応答を送受信します。

次のステートメントのコメント解除によって、デバイス マネージャが SNMP 応答に使用する UDP ポートを選択できます。

- Windows デスクトップでは、C:\Program Files\Cisco Systems\MDS9000\bin ディレクトリの DeviceManager.bat ファイル内の次のステートメントをアンコメントします。

```
rem JVMARGS=%JVMARGS% -Dsnmp.localport=[localport]
```

[localport] が空いているローカルポートの値の場合。



Note Windows VM で `netstat -nab` コマンドを実行して、`javaw.exe` プロセスで使用されているポートを表示します。

- LINUX デスクトップでは、`$HOME/.cisco_mds9000/bin` ディレクトリの `DeviceManager.sh` ファイル内の次のステートメントをアンコメントします。

```
# JVMARGS=$JVMARGS -Dsnmp.localport=[localport]
```

[localport] が空いているローカルポートの値の場合。

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、DCNM Web クライアント、DCNM SAN クライアント、デバイス マネージャ、SSH クライアント、および DCNM サーバ間の通信に使用されるすべてのポートの一覧を示します。

ポート番号	プロトコル	サービス名	通信方向	備考
22	TCP	SSH	SSH から DCNM SAN 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 SAN サーバ	Cisco DCNM Web クライアント、Cisco DCNM SAN クライアントから Cisco DCNM サーバ
1099	TCP	Java RMI	クライアントから DCNM SAN サーバ	Cisco DCNM SAN クライアントからサーバ
1163 ~ 1170	UDP	SNMP_TRAP	デバイスから SAN クライアントおよびデバイス マネージャ	Cisco DCNM SAN クライアントと Cisco デバイス マネージャは、同じ範囲のポートを使用します。

ポート番号	プロトコル	サービス名	通信方向	備考
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。 サーバに到達するために、インストール中に DCNM SAN OVA/ISO にのみ必要です。DCNM SAN サーバは、インストールが完了した後このポートを閉じます。
3528	TCP	JBOSS	クライアントから DCNM SAN サーバ	Wildfly JBOSS CORBA-IIOP
3529	TCP	JBOSS	クライアントから DCNM SAN サーバ	Wildfly JBOSS CORBA-IIOP SSL

ポート番号	プロトコル	サービス名	通信方向	備考
9198	UDP/TCP	SNMP		Cisco DCNM SNMP プロキシ サービスは、 Cisco DCNM SAN クライアントまた は Cisco デバイス マネージャと Cisco DCNM サー バ間の SNMP 通 信に TCP ポート (デフォルトでは 9198) を使用しま す。

ポート番号	プロトコル	サービス名	通信方向	備考
			<p>SAN クライアント、デバイスマネージャから DCNM SAN サーバ</p> <p>SNMP プロキシが使用可能な場合は、Cisco DCNM SAN クライアントが空いているローカルポート (UDP) または 9198 (TCP) をランダムに選択します。ポートは、<code>client -Dsnmp.localport</code> を使用して変更できます。</p> <p>SNMP プロキシが使用可能な場合は、Cisco デバイスマネージャが空いているローカルポート (UDP) または 9198 (TCP) をランダムに選択します。ポートは、<code>server.properties</code> ファイルで変更できます。</p> <p>DCNM SNMP プロキシは、SAN クライアントまたはデバイスマネージャが管理対象デバイスに直接到達できず、管理対象デバイスから DCNM SAN サーバに送信される</p>	

ポート番号	プロトコル	サービス名	通信方向	備考
			SNMP 応答を SAN クライアントおよびデバイスマネージャにリレーできる場合に使用されます。DCNM SAN クライアントとデバイスマネージャは、SNMP 応答を取得するために DCNM SAN サーバポート 9198(または任意のポートが設定されている)に到達する必要があります。	
61616	TCP	メッセージ	DCNM SAN クライアントから DCNM SAN サーバ	

次の表に、Cisco DCNM サーバと、ファイアウォールのどちらかでホスト可能な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一覧表示します。

Port Number	プロトコル	Service Name	コミュニケーション方向	備考
49	TCP/UDP	TACACS+	Cisco DCNM SAN サーバから ACS 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 および UDP	DNS	Cisco DCNM SAN サーバから DNS 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	Cisco DCNM SAN 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
1521	TCP	Oracle	DCNM SAN サーバから Oracle データベースサーバ	<p>これは、Oracle サーバが 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必要です。Oracle サーバは、別のポートでリスンするように設定されている場合があります。その場合は、対象のポートを考慮する必要があります。</p> <p>Note DCNM SAN のインストール時に Oracle サーバポートを選択できません。インストール後や後で変更することはできません。</p>

Port Number	プロトコル	Service Name	コミュニケーション方向	備考
5432	TCP	postgres	Postgres サーバへの Cisco DCNM SAN 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必要です。

Port Number	プロトコル	Service Name	コミュニケーション方向	備考
9198	UDP/TCP	SNMP	DCNM SAN クライアント、デバイス マネージャから DCNM SAN サーバ	

Port Number	プロトコル	Service Name	コミュニケーション方向	備考
				<p>Cisco DCNM SNMP プロキシサービスは、Cisco DCNM SAN クライアントまたは Cisco デバイスマネージャと Cisco DCNM サーバ間の SNMP 通信のため、DCNM SAN サーバで TCP ポート (デフォルトでは 9198) を使用します。</p> <p>SNMP プロキシに到達するために、Cisco DCNM SAN クライアントが空いているローカルポート (UDP) または 9198 (TCP) をランダムに選択します。ポートは、client <code>-Dsnmp.localportoption</code> を使用して変更できます。</p> <p>SNMP プロキシに到達するために、Cisco デバイスマネージャが空いているローカルポート (UDP) または 9198 (TCP) をランダムに選択します。ポートは、<code>server.properties</code> ファイルで変更できます。</p> <p>DCNM SNMP プ</p>

Port Number	プロトコル	Service Name	コミュニケーション方向	備考
				ロキシは、SAN クライアントまたはデバイス マネージャが管理対象デバイスに直接到達できず、管理対象デバイスから DCNM SAN サーバに送信される SNMP 応答を SAN クライアントおよびデバイス マネージャにリレーできる場合に使用されます。DCNM SAN クライアントとデバイス マネージャは、SNMP 応答を取得するために DCNM SAN サーバポート 9198(または任意のポートが設定されている)に到達する必要があります。

次の表に、Cisco 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の一覧を示します。

Port Number	プロトコル	Service Name	通信方向	備考
22	TCP	SSH	両方向	サーバからデバイス：デバイス管理用。 デバイスからサーバ：SCP (POAP)
67	UDP	DHCP	デバイスから DCNM SAN サーバ	

Port Number	プロトコル	Service Name	通信方向	備考
69	TCP	TFTP	デバイスから DCNM SAN サー バ	POAP に必須
161	TCP および UDP	SNMP	DCNM SAN サー バからデバイス	UDP ポート 161 の代わりに、ポ ート 161 で TCP を 使用するために server.properties 経由で設定されて いる Cisco DCNM
514	UDP	Syslog	デバイスから DCNM SAN サー バ	
2162	UDP	SNMP_TRAP	デバイスから DCNM SAN サー バ	
5989	TCP	SMI-S エージェン ト	両方向	サーバからデバイ スへ。これは、ス トレージデバイ スがリッスンする 場所です。 アプリケーション から DCNM サー バ : DCNM サー バがストレージ プロキシとして動 作している場合。 サーバからのスト レージデバイス ポート番号は、ス トレージデバイ スがリッスンして いる場所によつて 異なります。 5989、5888、また はその他のポート である可能性があ ります。

Port Number	プロトコル	Service Name	通信方向	備考
57500	TCP	gRPC	デバイスから DCNM SAN サー バ	SAN テレメトリ ストリーミング

カスタム ファイアウォールの設定



(注) これは、DCNM OVA/ISO 展開にのみ適用されます。

Cisco DCNM サーバは、DCNM ローカル ファイアウォールと呼ばれる IPTables ルールのセットを展開します。これらのルールは、Cisco DCNM 操作に必要な TCP/UDP ポートを開きます。OS インターフェイスにアクセスし、SSH を経由して、ルールを変更することなく内蔵ローカルファイアウォールを操作することはできません。攻撃に対して脆弱になったり、DCNM の通常の機能に影響を及ぼす可能性があるため、ファイアウォールルールを変更しないで下さい。

指定の展開またはネットワークに対応するため、Cisco DCNM では CLI を使用してリリース 11.3(1) から独自のファイアウォールルールを設定できます。



(注) これらのルールは幅広い粒度が細かく、内蔵ローカルファイアウォールルールを優先します。したがって、メンテナンス期間はこれらのルールを慎重に設定します。

カスタム ファイアウォールを設定するために、DCNM サーバまたはアプリケーションを停止または再起動する必要はありません。



注意 IPTable は、設定している順番でルールに優先順位を付けます。従って、最初により粒度の細かいルールをインストールする必要があります。ルールの順番が要求通りにするため、テキストエディタにすべてのルール作成し、希望の順番で CLI を実行することができます。ルールを調整する必要がある場合、すべてのルールを取り消し、希望の順番でルールを設定できます。

カスタム ファイアウォールで次の操作を実行できます。



(注) SSH を使用して Cisco DCNM サーバですべてのコマンドを実行します。

カスタム ファイアウォール CLI

appmgr user-firewall コマンドを使用して、カスタム ファイアウォール CLI チェーン ヘルプと例を表示します。

```
dcnm# appmgr user-firewall
dcnm# appmgr user-firewall - h
```

カスタム ファイアウォールのルールを設定する

appmgr user-firewall {add | del} コマンドを使用して、カスタム ファイアウォールルールを設定します。

```
appmgr user-firewall {add|del} proto {tcp|udp} port {<port><port range n1:n2>}
[{in|out} <interface name>] [srcip <ip-address> [/<mask>]] [dstip <ip-address>
[/<mask>]] action {permit|deny}
```



(注) カスタム ファイアウォールルールは、ローカルファイアウォールルールを優先します。従って、機能が破損していないか注意して確認します。

例：例のカスタム ファイアウォール ルール

- dcnm# **appmgr user-firewall add proto tcp port 7777 action deny**

このルールは、すべてのインターフェイスですべての TCP ポート 7777 トラフィックをドロップします。

- dcnm# **appmgr user-firewall add proto tcp port 443 in eth1 action deny**

このルールは、インターフェイス eth1 ですべての TCP ポート 443 着信トラフィックをドロップします。

- dcnm# **appmgr user-firewall add proto tcp port 7000:7050 srcip 1.2.3.4 action deny**

このルールは、IP アドレス 1.2.3.4. から発信されている TCP ポート範囲 10000 ~ 10099 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のみ動作します。

ルールをすぐに適用するには、**appmgr user-firewall user-policy-install** コマンドを使用してスタンバイ ノードでカスタム ファイアウォールルールをインストールします。

カスタム ファイアウォールの削除

appmgr user-firewall flush-all コマンドを使用して、すべてのカスタム ファイアウォールを削除します。

カスタム ファイアウォールを永久に削除するには、**appmgr user-firewall commit** コマンドを使用します。



第 7 章

ユーザーとスキーマ

この章では、*Cisco Data Center Network Manager* のユーザーとユーザー固有のスキーマの作成について説明します。

- [新規ユーザーの作成, on page 143](#)
- [既存ユーザーの新しくスキーマを作成する, on page 144](#)

新規ユーザーの作成

新規ユーザーを作成するには、次の作業を実行します。

Procedure

- ステップ 1 DCNM アプライアンスの SSH 端末にログオンします。
 - ステップ 2 `create user username` コマンドを使用して、新規ユーザーを作成します。
 - ステップ 3 パスワードプロンプトで有効なパスワードを入力します。
 - ステップ 4 `create schemausernameauthorizationusername` を使用して、ユーザーと同じ名前を持つ新規スキーマを作成します。
 - ステップ 5 `grant all on schemausername to username` を使用して、スキーマですべての権限を有効にします。
-

Example

次の例は、新規ユーザーを作成するためのコマンドのサンプル出力を示しています。

```
dcnm# create user user1
password: password
dcnm# create schema user1 authorization user1;
dcnm# grant all on schema user1 to user1;
```

既存ユーザーの新しくスキーマを作成する

このタスクを実行して、既存のユーザーに対して同じ作成された新しいスキーマを保持します。

Procedure

- ステップ 1 DCNM アプライアンスの SSH 端末にログオンします。
 - ステップ 2 **drop userusernamecascade** コマンドを使用して、既存のユーザーをドロップします。
 - ステップ 3 **drop schemausernamecascade** コマンドを使用して、ユーザー名と同じ名前の既存のスキーマをドロップします。
 - ステップ 4 **create user username** コマンドを使用して、新規ユーザーを作成します。
 - ステップ 5 パスワードプロンプトで有効なパスワードを入力します。
 - ステップ 6 **create schemausernameauthorizationusername** コマンドを使用して、ユーザーと同じ名前の新しいスキーマを作成します。
 - ステップ 7 **grant all on schemausername to username** を使用して、スキーマですべての権限を有効にします。
-

Example

次の例は、新規ユーザーを作成するためのコマンドのサンプル出力を示しています。

```
dcnm# drop user user_old cascade
dcnm# drop schema user_old cascade
dcnm# create user user_new
password: password
dcnm# create schema user_new authorization user_new;
dcnm# grant all on schema user_new to user_new;
```




第 8 章

証明書

- CA 署名済み証明書の保持, on page 145
- Cisco DCNM の証明書を設定する, on page 146
- 証明書の管理 (Certificate Management) (150 ページ)

CA 署名済み証明書の保持

アップグレード後に CA 署名付き SSL 証明書を保持する必要がある場合は、次の手順を実行します。

キーストアのパスワードまたはエイリアスを変更する場合は、次の場所にある **standalone-san** ドキュメントで更新する必要があることに注意してください。

```
< DCNM_install_root >  
\dcm\wildfly-14.0.1.Final\standalone\configuration\standalone-san.xml
```

keystore タグとエイリアスのパスワードを更新します。

```
<keystore key-password>="fmserver_1_2_3 key-alias="updated-key-alias"  
keystore-password="updated-password"  
path="<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks">
```

Procedure

ステップ 1 次の場所から署名付き証明書をバックアップします。

- Windows の場合 :
<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks
- Linux の場合 :
<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks

ステップ 2 Cisco DCNM リリース 11.3(1) にアップグレードします。

ステップ 3 アップグレード後、Cisco DCNM のアップグレードされたバージョンと同じ場所に証明書をコピーします。

Note ステップ 1, on page 145 に記載されているのと同じ場所に証明書をロードする必要があります。

ステップ 4 DCNM サービスを再起動します。

Cisco DCNM の証明書を設定する

ここでは、Cisco DCNM で証明書を設定する 3 つの方法について説明します。

キーストアのパスワードまたはエイリアスを変更する場合は、次の場所にある **standalone-san** ドキュメントで更新する必要があることに注意してください。

```
< DCNM_install_root >
\dcm\wildfly-14.0.1.Final\standalone\configuration\standalone-san.xml
```

keystore タグのパスワードと **key-alias** タグのエイリアスを次のように更新します。

```
<keystore key-password>="fmserver_1_2_3 key-alias="updated-key-alias"
keystore-password="updated-password"
path="<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks">
```

ここでは、次の内容について説明します。

自己署名 SSL 証明書の使用

Procedure

ステップ 1 DCNM サービスを停止します。

ステップ 2 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-14.0.1.Final\standalone\configuration\fmserver.jks
~
```

```
< DCNM_install_root >
\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks.old
```

ステップ 3 コマンドプロンプトから、に移動します。<DCNM install root>\dcm\java\jdk11\bin\

ステップ 4 次のコマンドを使用して、自己署名証明書を生成します。

```
keytool -genkey -trustcacerts -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore
<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks -storepass
fmserver_1_2_3 -validity 360 -keysize 2048
```

ステップ 5 DCNM サービスを開始します。

Windows でキーツールを使用して証明書要求が生成される場合 SSL 証明書を使用する

Procedure

ステップ 1 DCNM サービスを停止します。

ステップ 2 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-14.0.1.Final\standalone\configuration\fmserver.jks
~
< DCNM_install_root >
\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks.old
```

ステップ 3 From command prompt, navigate to <DCNM install root>\dcm\java\jdk11\bin\

ステップ 4 次のコマンドを使用して、DCNM キーストアで公開秘密キーペアを生成します。

```
keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore
"<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks" -storepass
fmserver_1_2_3 -validity 360 -keysize 2048
```

ステップ 5 [ステップ 4, on page 147](#) で生成された公開キーから証明書署名要求 (CSR) を生成します。

```
keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install
root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3
```

Note dcnm csr ファイルは、/usr/local/cisco/dcm/java/jdk11/bin にあるキーツールディレクトリに作成されます。

ステップ 6 CSR を CA に送信し、Base-64 形式で署名付き証明書チェーンをダウンロードします。これにより、.p7b ファイルが作成されます。

CA は、証明書と署名証明書を PKCS 7 形式 (.p7b ファイル) または PEM (.pem) ファイルの証明書チェーンとして提供することがあります。CA が提供した PKCS7 形式の場合は、[ステップ 7, on page 147](#) に移動して PEM 形式に変換します。CA が PEM 形式を提供した場合は、[ステップ 8, on page 147](#) に進みます。

ステップ 7 Openssl を使用して、PKCS 7 証明書チェーンを X509 証明書チェーンに変換します。

```
openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem
```

Note 上記のコマンドで、ユーザーが cert-chain.p7b の正しい場所への絶対パスまたは相対パスのいずれかを提供していることを確認します。

ステップ 8 次の手順に従って、最初に中間証明書をインポートし、次に root 証明書をインポートし、署名付き証明書を最後にインポートします。

```
keytool -importcert -trustcacerts -file cert-chain.pem -keystore
"<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks" -storepass
fmserver_1_2_3 -alias sme
```

Note 上記のコマンドで、ユーザーが cert-chain.pem ファイルの正しい場所への絶対パスまたは相対パスのいずれかを提供していることを確認します。

ステップ 9 DCNM サービスを開始します。

Linux でキーツールを使用して証明書要求が生成されたときに SSL 証明書を使用する

Procedure

ステップ 1 `appmgr stop dcnm` コマンドを使用して、DCNM サービスまたは DCNM アプリケーションを停止します。

ステップ 2 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-14.0.1.Final/standalone/configuration/fmserver.jks
```

目的

```
< DCNM_install_root
>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks.old
```

ステップ 3 コマンドプロンプトから、適切なフォルダに移動します。

```
<DCNM install root>/dcm/java/jdk11/bin/
```

ステップ 4 次のコマンドを使用して、DCNM キーストアで公開秘密キーペアを生成します。

```
./keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore
<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -storepass
fmserver_1_2_3 -validity 360 -keysize 2048
```

ステップ 5 [ステップ 7, on page 148](#) で生成されている公開キーから、証明書署名要求 (CSR) を生成します。

```
./keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install
root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks" -storepass fmserver_1_2_3
```

Note dcnm csr ファイルは、/usr/local/cisco/dcm/java/jdk11/binにあるキーツールディレクトリに作成されます。

ステップ 6 CSR を CA に送信し、Base-64 形式で署名付き証明書チェーンをダウンロードします。これにより、.p7b ファイルが作成されます。

CA は、証明書と署名証明書を PKCS 7 形式 (.p7b ファイル) または PEM (.pem) ファイルの証明書チェーンとして提供することがあります。PKCS 7 形式で CA が証明書チェーンを提供した場合は、[ステップ 7, on page 148](#) に移動して PEM 形式に変換します。PEM 形式で CA が証明書チェーンを提供した場合、[ステップ 8, on page 149](#) に移動します。

ステップ 7 OpenSSL を使用して、PKCS 7 証明書チェーンを X509 証明書チェーンに変換します。

```
openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem
```

Note 上記のコマンドで、ユーザーが `cert-chain.p7b` の正しい場所への絶対パスまたは相対パスのいずれかを提供していることを確認します。

ステップ 8 次の手順に従って、最初に中間証明書をインポートし、次に root 証明書をインポートし、署名付き証明書を最後にインポートします。

```
./keytool -importcert -trustcacerts -file cert-chain.pem -keystore  
<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -storepass  
fmserver_1_2_3 -alias sme
```

Note 上記のコマンドで、ユーザーが `cert-chain.pem` ファイルの正しい場所への絶対パスまたは相対パスのいずれかを提供していることを確認します。

ステップ 9 `apmgrp start dcnm` コマンドを使用して、サーバのアプリケーションを開始します。

Linux で OpenSSL を使用して証明書要求が生成される場合 SSL 証明書を使用する

Open SSL を使用して生成された証明書要求を使用して Cisco DCNM で SSL 証明書を設定するには、次の手順を実行します。

Procedure

ステップ 1 `apmgrp stop dcnm` コマンドを使用して、DCNM サービスまたは DCNM アプリケーションを停止します。

ステップ 2 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-14.0.1.Final/standalone/configuration/fmserver.jks  
~
```

```
< DCNM_install_root  
>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks.old
```

ステップ 3 コマンドプロンプトから `<DCNM_install_root>/dcm/java/jdk11/bin/` に移動します。

ステップ 4 OpenSSL を使用して RSA 秘密キーを生成します。

```
openssl genrsa -out dcnm.key 2048
```

ステップ 5 次のコマンドを使用して、自己署名証明書 (CSR) を生成します。

```
openssl req -new -key dcnm.key -sha256 -out dcnm.csr
```

ステップ 6 CSR を証明書認定機関に送信し、Base-64 形式で署名付き証明書チェーンをダウンロードします。これにより、`.p7b` ファイルが作成されます。

CA は、証明書と署名証明書を PKCS 7 形式 (`.p7b` ファイル) または PEM (`.pem`) ファイルの証明書チェーンとして提供することがあります。CA が PKCS 7 形式を提供している場合は、[ステッ](#)

プ 7, on page 150 に移動して PEM 形式に変換します。CA が PEM 形式を提供している場合は、ステップ 8, on page 150 に進みます。

ステップ 7 PKCS 7 証明書チェーンを X509 証明書チェーンに変換します。
`openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem`

ステップ 8 X509 証明書チェーンと秘密キーを PKCS 12 形式に変換します。
`openssl pkcs12 -export -in cert-chain.pem -inkey dcnm.key -out dcnm.p12 -password pass
 fmsvrer_1_2_3 -name sme`

Note 上記のコマンドで `dcnm.key` および `dcnm.p12` ファイルの正しい場所に、ユーザーが絶対パスまたは相対パスのどちらかを提供するようにします。

ステップ 9 中間証明書、root 証明書、および署名付き証明書を同じ順序でインポートします。
`./keytool -importkeystore -srckeystore dcnm.p12 -srcstoretype PKCS12 -destkeystore
 <DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmsvrer.jks -deststoretype
 JKS -alias sme`

Note 上記のコマンドで、`cert-chain.pem`、`dcnm.key`、および `dcnm.p12` の正しい場所に対して絶対パスまたは相対パスを提供していることを確認します。

ステップ 10 `appmgr start dcnm` コマンドを使用して、サーバの DCNM サービス、または DCNM アプリケーションを起動します。

証明書の管理 (Certificate Management)



(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。



(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。
- 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 = fmserver_1_2_3
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#

```

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 */

```

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。

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。

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。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=dcnml.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=dcnml.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11.3(1)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 11.3(1)にアップグレードすると、CA 署名付き証明書のバックアップが作成されます。

Cisco DCNM スタンドアロンアプライアンスが正常にアップグレードされたら、SSH を使用して DCNM サーバにログインします。

- 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 署名証明書を確認します。

システムは、CA 証明書を用意しており、ブラウザで確認できます。

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

Cisco DCNM ネイティブ HA セットアップでは、証明書はアクティブ ノードとスタンバイ ノードの両方にインストールされます。アクティブ ノードでのみ証明書を復元する必要があります。証明書はスタンバイ ノードと自動的に同期されます。

Cisco DCNM スタンドアロン展開をリリース 11.3(1)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。

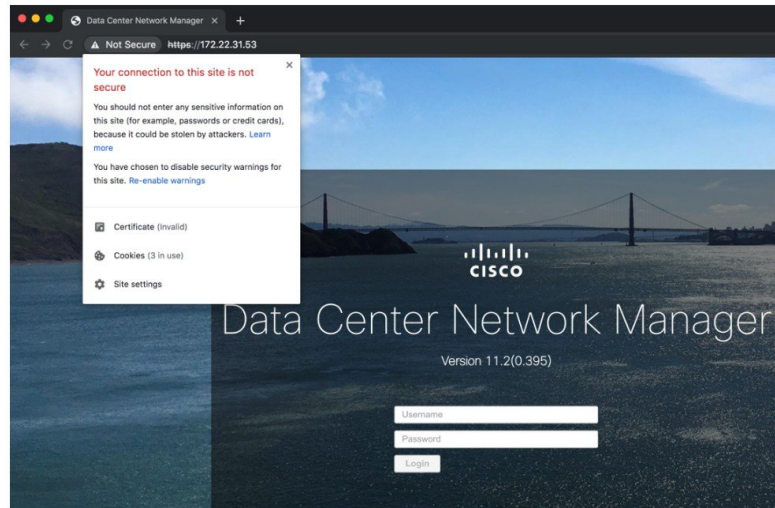
インストールした証明書の確認

`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。

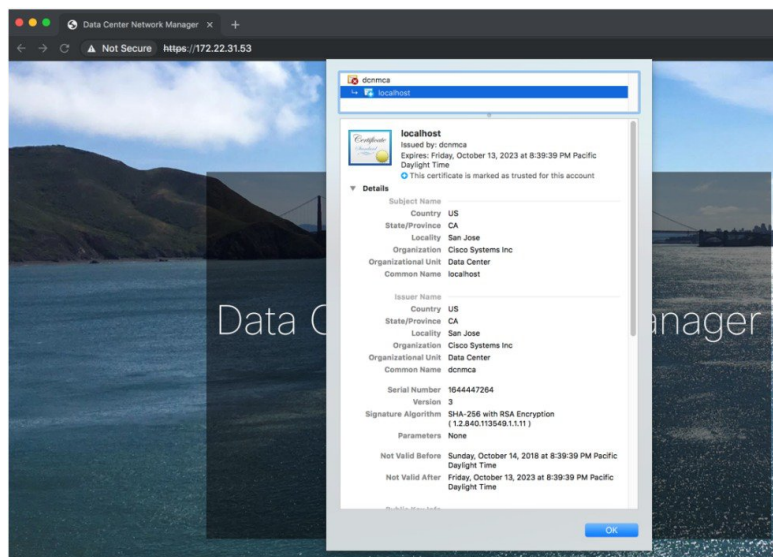
ブラウザのプロバイダ Web サイトで、ブラウザの固有情報を参照することをお勧めします。

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。



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 161](#)

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。

RHELまたはWindows上のフェデレーションのCiscoDCNMでSSL/HTTPSを有効化する

フェデレーションの Cisco DCNM 向け RHEL または Windows 上で SSL/HTTPS を有効にするには、次の手順を実行します。

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、次のいずれかを実行します。

- インストーラの実行中に、[HTTPS] を選択して、HTTP モードで実行することを選択します。
 - サイレントインストールしている間、インストーラの実行中に [HTTPs] を選択します。
-



第 10 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 7: 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、 ² を選択します。	ネットワーク管理

² [展開中にユーザーによって入力された管理パスワードを参照するようにユーザーが選択する (User choice refers to the administration password entered by the user during the deployment)]

この章は、次の項で構成されています。

- [DCNM インストール後のネットワーク プロパティ \(163 ページ\)](#)
- [ユーティリティ サービスの詳細, on page 167](#)
- [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 169](#)
- [IPv6 の SFTP サーバアドレスの更新, on page 171](#)

DCNM インストール後のネットワーク プロパティ

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

- dcnm-mgmt network (eth0) インターフェイス

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

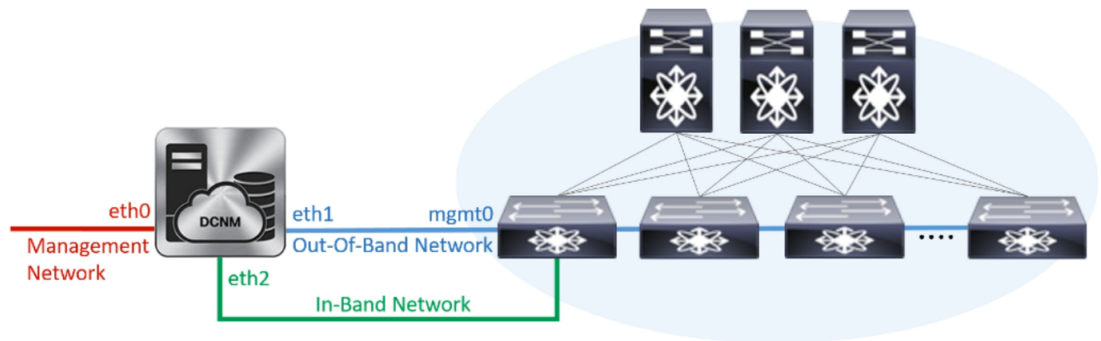
- enhanced-fabric-mgmt (eth1) インターフェイス

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

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

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

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



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

次の項で説明するように、パラメータを変更できます。

スタンドアロン モードの DCNM 上でネットワーク プロパティの変更



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

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

Procedure

ステップ 1 次のコマンドを使用して、コンソールのセッションを開始します。

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

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

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

ステップ 3 次のコマンドを使用して、変更を表示し確認します。

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

ステップ 4 変更を確認した後、次のコマンドを使用して設定を適用します。

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

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

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

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

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

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

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

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

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

PLEASE STOP ALL APPLICATIONS MANUALLY
*****

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
server signaled
INFO : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave
the 'tentative' state
```

DCNM インストール後に DCNM サーバパスワードを変更する

```

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#

```

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
```

ユーティリティ サービスの詳細

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

ネットワーク管理

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



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

オーケストレーション

RabbitMQ

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



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

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

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

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

電源オン自動プロビジョニング

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

- DHCP サーバ

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

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



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:

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

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

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

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

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

ユーティリティ サービスの停止、開始、リセット

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

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

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

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

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

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

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



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

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

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



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

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

IPv6 の SFTP サーバアドレスの更新

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

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

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

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

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

