# 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。

SE に Cisco DCNM をインストールする場合は、DCNM ISO 仮想アプライアンス（.iso）インストーラをインストールします。



# 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。アップグレードを開始する前に、`pgevent.dll`（`dcm db パス \db\lib\pgevent.dll` にあります）を必ず削除してください。

### 手順

**ステップ 1** Cisco DCNM サービスを停止します。

サーバで実行されている DCNM SAN クライアントと Device Manager のすべてのインスタンスを閉じていることを確認します。

**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** 最新のリリース リストで、リリース 11.5(1) 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。

インストーラー ファイルの形式は、`dcnm-installer-x64.11.5.1.exe` 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。

次のメッセージが表示されます。

```
Please close the DCNM Installation wizard gracefully using "Done" option
on last installation step and wait for the installation wizard to close automatically.
Do not restart the system or forcefully terminate the Installation wizard while it is
still in progress."
```

[OK] をクリックして作業を続行します。

**[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 PostgresSQL 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、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 クレデンシャル (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** インストーラを閉じたり、ウィザードを終了したりしないでください。**[終了（Done）]** をクリックします。

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 3 セクションの指示に従ってください。
- プライマリ サーバーとセカンダリ サーバーの両方が同じ DCNM バージョンであることを確認してください。

**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。

次のメッセージが表示されます。

```
Please close the DCNM Installation wizard gracefully using "Done" option
on last installation step and wait for the installation wizard to close automatically.
Do not restart the system or forcefully terminate the Installation wizard while it is
still in progress."
```

[OK] をクリックして作業を続行します。

**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。

（注） **/home** SELinux で保護されたパスに DCNM をインストールしないでください。

# 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。

サーバで稼働している DCNM SAN クライアントおよびデバイス マネージャのすべてのインスタンスを閉じます。

**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。

（注） RHEL 8.x をアンインストールする場合は、**./Uninstall_DCNM -i silent** コマンドを使用します。ただし、RHEL 8.x は Web UI によるアンインストールをサポートしていません。

**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 te 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    /* for uninstalling RHEL 7.x */
[dcnm-linux]# ./Uninstall_DCNM -i silent /* for uninstalling RHEL 8.x */
[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** 最新のリリース リストで、リリース 11.5(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-x64.11.5.1.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。

**Note** `/home` SELinux で保護されたパスに DCNM をインストールしないでください。

### Before you begin

DISPLAY 変数は 1 に設定されていることを確認します。

- 以下のコマンドを使用して、DISPLAY 変数が 1 に設定されているか確認します。

  **echo $DISPLAY**
- 以下のコマンドを使用して、DISPLAY 変数を 1 に設定します。

  **export DISPLAY=:1**

### 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。

次のメッセージが表示されます。

```
Please close the DCNM Installation wizard gracefully using "Done" option
on last installation step and wait for the installation wizard to close automatically.
Do not restart the system or forcefully terminate the Installation wizard while it is
still in progress."
```

[OK] をクリックして作業を続行します。

**[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。

**Note** インストールの場所は、必要なディスク領域がプロビジョニングされているパーティション内である必要があります。展開に十分なディスク領域があることを確認します。

[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 PostgresSQL 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 クレデンシャル (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。

**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：

**Note** `/home` SELinux で保護されたパスに DCNM をインストールしないでください。

### 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 12 の指示に従ってください。
- DISPLAY 変数は 1 に設定されていることを確認します。
  - 以下のコマンドを使用して、DISPLAY 変数が 1 に設定されているか確認します。

    **echo $DISPLAY**
  - 以下のコマンドを使用して、DISPLAY 変数を 1 に設定します。

    **export DISPLAY=:1**
- プライマリ サーバーとセカンダリ サーバーの両方が同じ DCNM バージョンであることを確認してください。

### 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。

次のメッセージが表示されます。

```
Please close the DCNM Installation wizard gracefully using "Done" option
on last installation step and wait for the installation wizard to close automatically.
```

```
Do not restart the system or forcefully terminate the Installation wizard while it is
still in progress."
```

[OK] をクリックして作業を続行します。

**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。

**Note** `/home` SELinux で保護されたパスに DCNM をインストールしないでください。

### Before you begin

Linux に Cisco DCNM をインストールする前に、/tmp ディレクトリに対する実行権限があることを確認します。

### 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:\\oraclexe\\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 vaires
#-----------------------------------------------------

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。

**Procedure**

**ステップ 1** 次のサイトに移動します。 http://software.cisco.com/download/http://software.cisco.com/download/

ダウンロード可能な Cisco DCNM の最新リリース ソフトウェアのリストが表示されます。

**ステップ 2** [製品の選択 (Select a Product)] 検索ボックスに「**Cisco Data Center Network Manager**」と入力します。

**[検索 (Search)]** アイコンをクリックします。

**ステップ 3** 検索結果から **[Data Center Network Manager]** をクリックします。

ダウンロード可能な Cisco DCNM の最新リリース ソフトウェアのリストが表示されます。

**ステップ 4** 最新リリースのリストで、11.5(1) を選択します。

**ステップ 5** DCNM 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。

**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 (Hosts and Clusters)]** に移動し、OVF テンプレートが展開されているホストを選択します。

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

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

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

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

次のいずれかの方法で OVA ファイルを選択できます。

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

[次へ（Next）] をクリックします。

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

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

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

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

- [名前 (Name)] フィールドに、OVF の適切な名前を入力します。

  **Note** VM 名がインベントリ内で固有であることを確認します。

- [参照 (Browse)] タブで、適切な ESXi ホストの下の展開場所として **[データセンター (Datacenter]** を選択します。

**[次へ (Next)]** をクリックします。

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

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

  コンセプト実証には [小規模 (Small)]、時間の増加が予想されないスイッチ 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、

- **[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。

[Next] をクリックします。

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

[Next] をクリックします。

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

a) ドロップダウン リストから仮想ディスク形式を選択します。

使用可能なディスクの形式は次のとおりです。

**Note** 仮想アプライアンス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。

b) ドロップダウン リストから VM ストレージ ポリシーを選択します。

デフォルトでは、ポリシーは選択されていません。

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

**[次へ (Next)]** をクリックします。

**ステップ 11** [ネットワークの選択 (Select Networks)] ページで、OVF テンプレートで使用されているネットワークをインベントリのネットワークにマッピングします。

- **dcnm-mgmt network**

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

- **enhanced-fabric-mgmt**

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

  **Note** このネットワークは、Cisco DCNM SAN OVA / ISO 展開ではオプションです。

- **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** このネットワークは、Cisco DCNM SAN OVA / ISO 展開には適用されません。

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」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。

[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。

**[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

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 25 を参照してください。

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

[コンソール (Console)] タブに表示されている URL を貼り付け、[Enter] キーを押します。初期メッセージが表示されます。

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

### Procedure

**ステップ 1** **[Cisco DCNM へようこそ (Welcome to Cisco DCNM)]** 画面から、**[開始 (Get Started)]** をクリックします。

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

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

[Next] をクリックします。

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

**[インストール モード (Install Mode)]** タブで、ドロップダウン リストから OVA DCNM アプライアンスの **[SAN のみ (SAN Only)]** インストール モードを選択します。

**[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 Systems、Inc.** または **IBM** を選択できます。

**[次へ (Next)]** をクリックします。

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

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

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

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

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

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

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

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

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

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

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

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

**[次へ (Next)]** をクリックします。

**ステップ 5** **[システム設定 (System Settings)]** で、DCNM アプライアンスの設定を行います。

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

  IPv6 アドレスを使用して DNS サーバを設定することもできます。

  リリース 11.3(1) から、1 個以上の DNS サーバと NTP サーバを設定できます。
- **[NTP サーバ アドレス リスト（NTP Server Address List）]** フィールドでは、NTP サーバの IP アドレスを入力します。

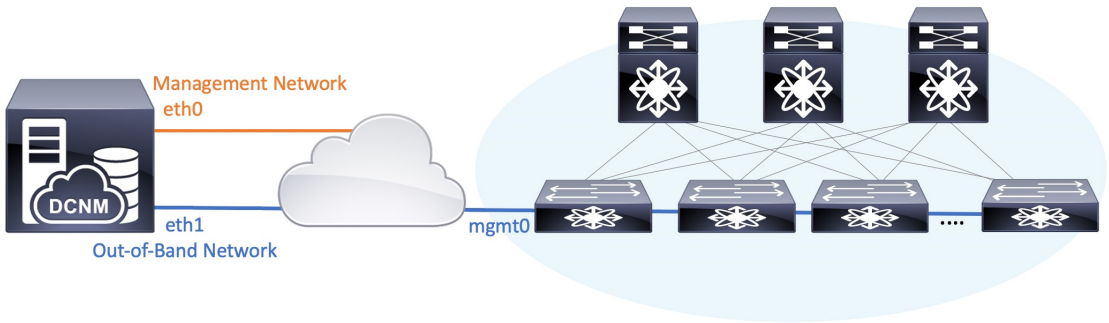
  値は IP または IPv6 アドレスか RFC 1123 に準拠した名前である必要があります。

  リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。
- **タイムゾーン** ドロップダウン リストから、DCNM を展開しているタイムゾーンを選択します。

[Next] をクリックします。

**ステップ 6** **[ネットワーク設定 (Network Settings)]** タブで、DCNM Web UI に到達するために使用されるネットワーク パラメータを構成します。

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



**Note** SAN OVA / ISO 展開用の Cisco DCNM では、それぞれの環境で、要件に基づいて eth0 のみ、または eth0 と eth1 の両方を（同じまたは異なるサブネットに）設定できます。eth0 または eth1 インターフェイスを介した管理/モニタリング用のスイッチへの IP 到達可能性を確立します。SAN Insights ストリーミングは、eth0 インターフェイスと eth1 インターフェイスの両方でサポートされます。ただし、それぞれのスイッチからのIP到達可能性を持つ DCNM インターフェイスにストリーミングが設定されていることを確認します。詳細については、『*OVA* と *ISO* 向けの展開設定ガイド』の「SAN Insights の設定」を参照してください。

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

管理IPアドレスのみが設定されている場合、eth0 管理インターフェイスが管理およびアウトオブバンド通信に使用されます。これは、ファブリックおよび SAN インサイトの操作に適用されることに注意してください。

**Note** 管理ネットワークに IPv6 アドレスを使用することもできます。ただし、SAN Insights ストリーミングは IPv4 アドレス設定でのみサポートされます。

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

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

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

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

c) (Optional) OVA / ISO 展開用の Cisco DCNM SAN には**インバンド ネットワーク**設定は必要ありません。

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。 eth0 インターフェイスと eth1 インターフェイスの両方が設定されている場合は、同じコマンドを使用して単一のインターフェイスを使用するようにスタティック ルートを設定できます。詳細については、DCNM インストール後のネットワーク プロパティを参照してください。

[次へ（Next）] をクリックします。

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

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

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

**[次へ (Next)]** をクリックします。

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

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

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

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

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

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

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

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

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

### What to do next

適切なクレデンシャルを使用して DCNM Web UI にログオンします。

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

# 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。

SE に Cisco DCNM をインストールする場合は、DCNM ISO 仮想アプライアンス（.iso）インストーラをインストールします。

# 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/http://software.cisco.com/download/

ダウンロード可能な Cisco DCNM の最新リリース ソフトウェアのリストが表示されます。

**ステップ 2** [製品の選択 (Select a Product)] 検索ボックスに「Cisco Data Center Network Manager」と入力します。

[検索 (Search)] アイコンをクリックします。

**ステップ 3** 検索結果から **[Data Center Network Manager]** をクリックします。

ダウンロード可能な Cisco DCNM の最新リリース ソフトウェアのリストが表示されます。

**ステップ 4** 最新リリースのリストで、11.5(1) を選択します。

**ステップ 5** DCNM ISO 仮想アプライアンス インストーラを検索し、**[ダウンロード (Download)]** アイコンをクリックします。

**ステップ 6** VMWare (ovf) および KVM (domain Xml) 環境の DCNM 仮想アプライアンスの定義ファイルで DCNM VM テンプレートを検索し、**[ダウンロード (Download)]** をクリックします。

**ステップ 7** インストール時に簡単に見つけることができるように、dcnm.iso ファイルをディレクトリに保存します。

### What to do next

KVM またはベアメタル サーバに DCNM をインストールすることを選択できます。詳細については KVM 上での DCNM ISO 仮想アプライアンスのインストール, on page 38 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 31 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。

**Note** **appmgr** コマンドはシェル（Bash）によって実行され、一部の文字は解釈が異なります。したがって、特殊文字を含むコマンド自体で指定されたパスワードは引用符で囲む必要があります。代わりに、**appmgr change_pwd ssh root** を実行してプロンプトにパスワードを入力することもできます。

**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。

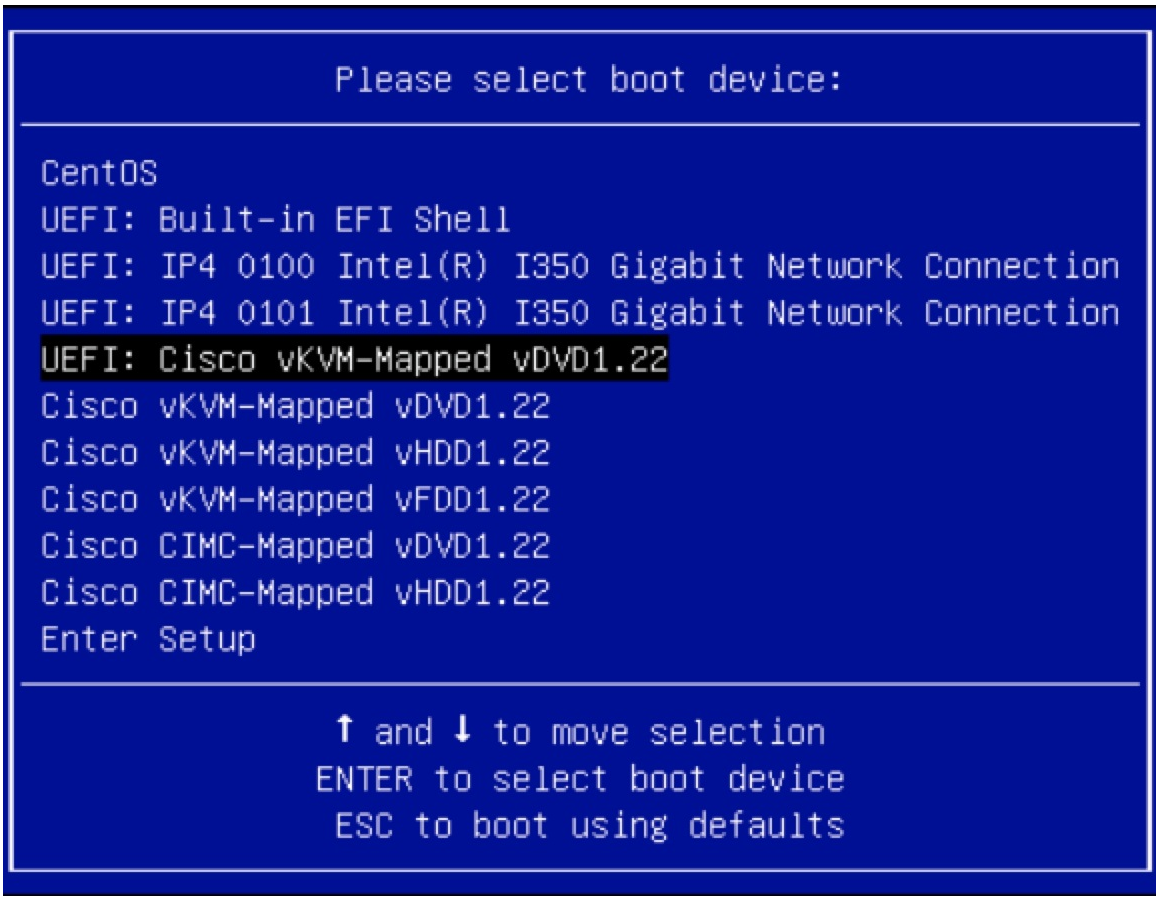
[UCS KVM コンソール (UCS KVM Console)] ウィンドウの使用方法の詳細については、次の URL にある『リリース 3.1 ユーザー ガイド Cisco UCS サーバ設定ユーティリティ』を参照してください。

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/ucsscu/user/guide/31/UCS_SCU/booting.html#wp1078073

**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。

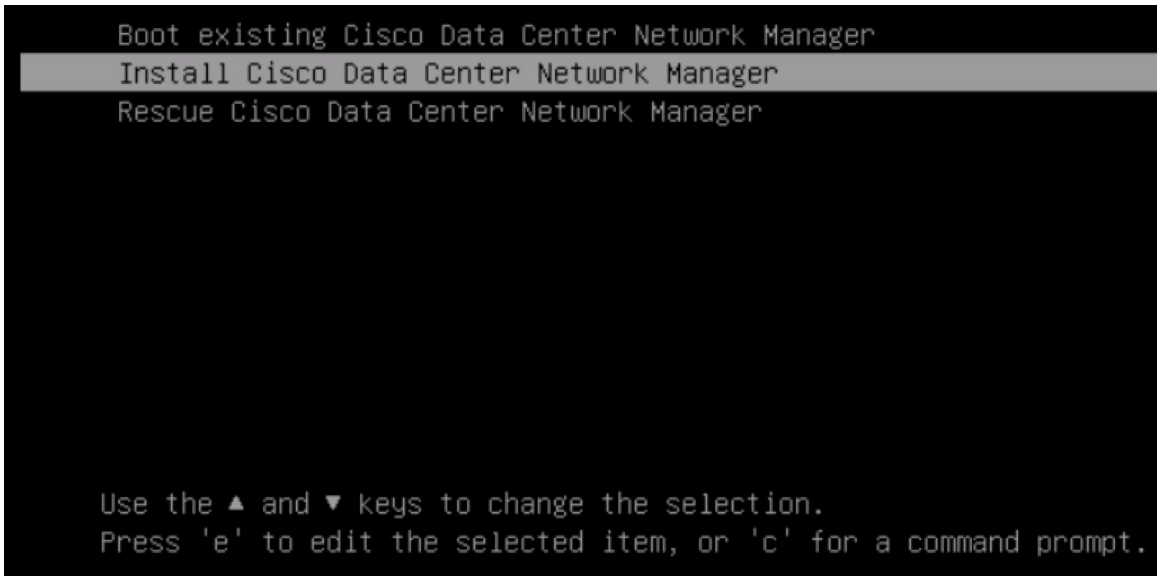
UEFI は、2 TB 以上のディスクを搭載したシステムでは必須です。



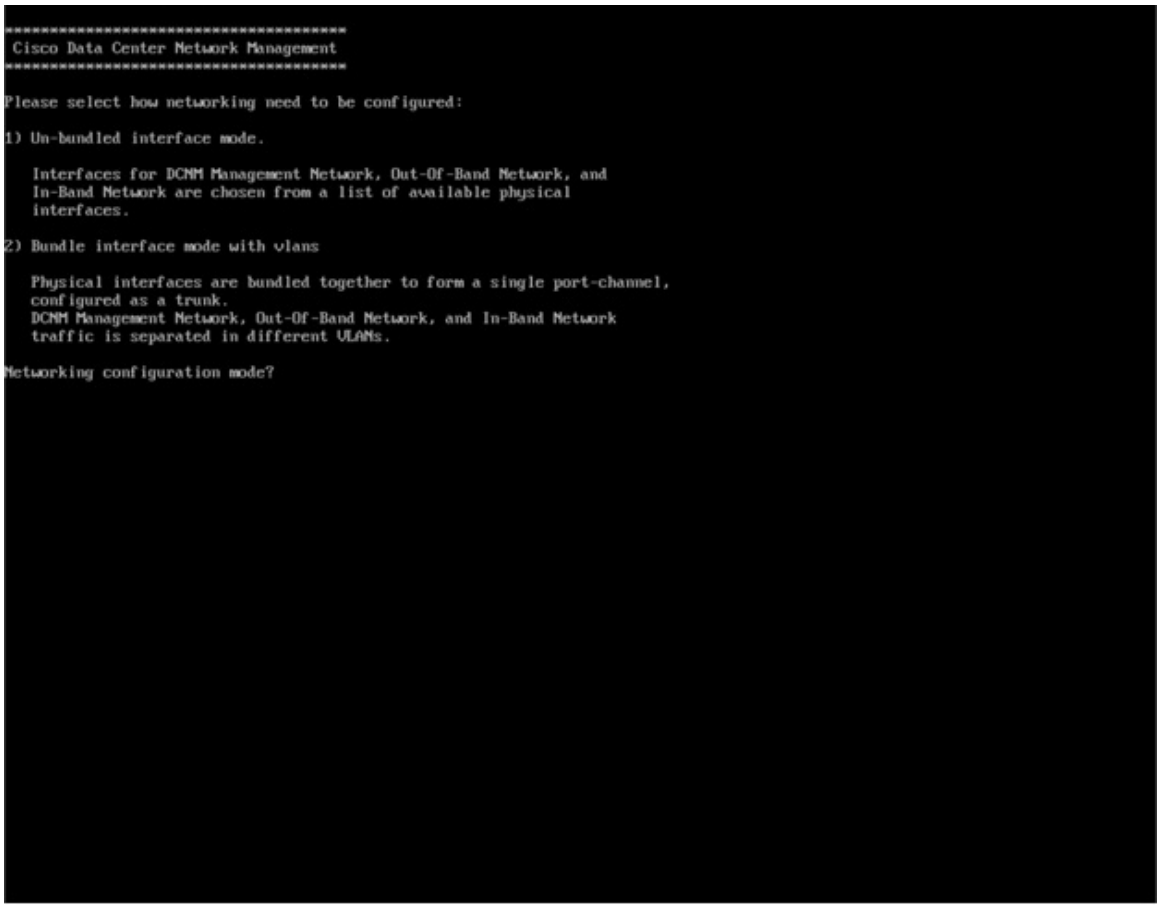

ディスク サイズが 2 TB 以上で、4K セクター サイズ ドライバを使用している Cisco UCS の場合は、UEFI 起動オプションが必要です。詳細については、「UEFI 起動モード」を参照してください。

**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。




**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。



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

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

**ステップ 11** 1 を入力した場合は、バンドルされていないインターフェイス モードで Cisco DCNM ISO をインストールするため、ネットワークのインターフェイスを選択します。利用可能なインターフェイスのリストが画面に表示されます。

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

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

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

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

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

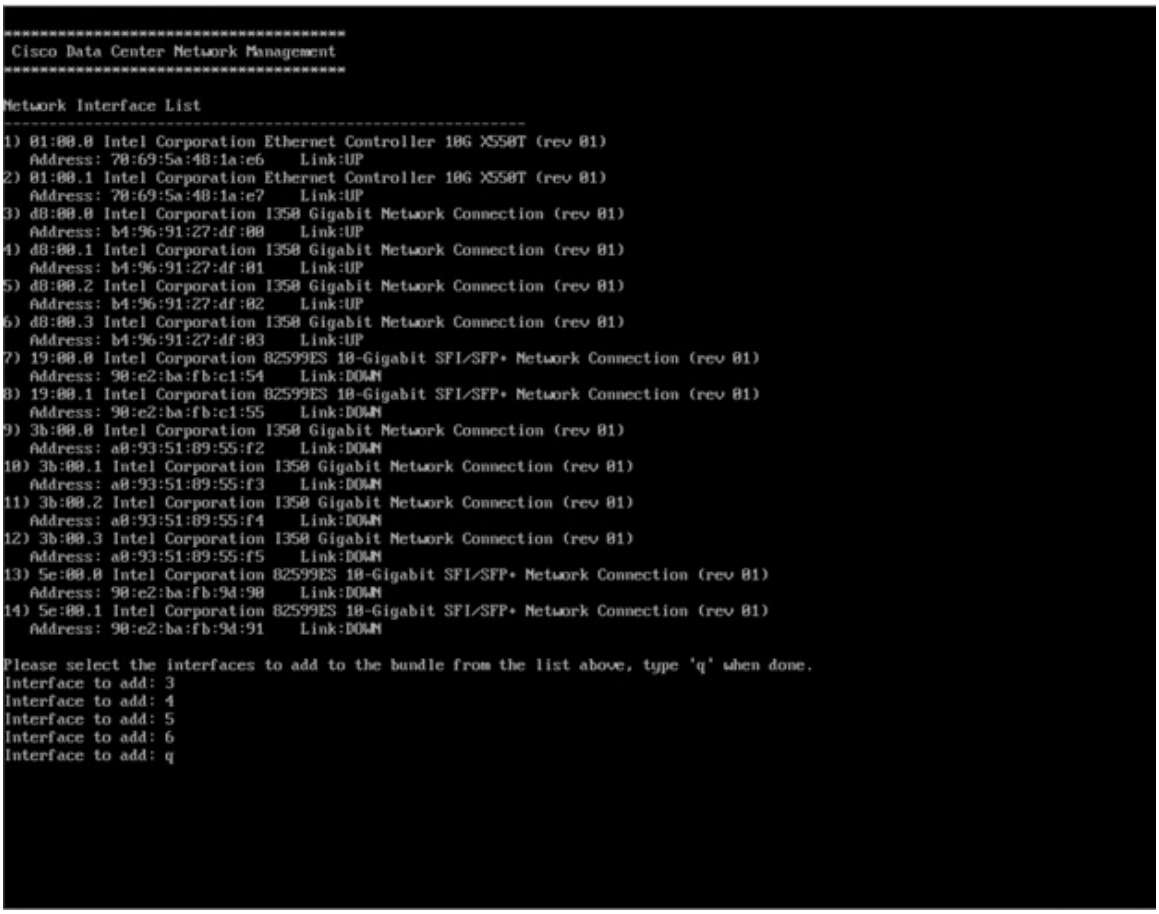
ただし、**appmgr update network-properties** コマンドを使用して、必要に応じてインストール後にネットワーク プロパティを編集できます。詳細については、「DCNM インストール後のネットワーク プロパティ」を参照してください。

**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。

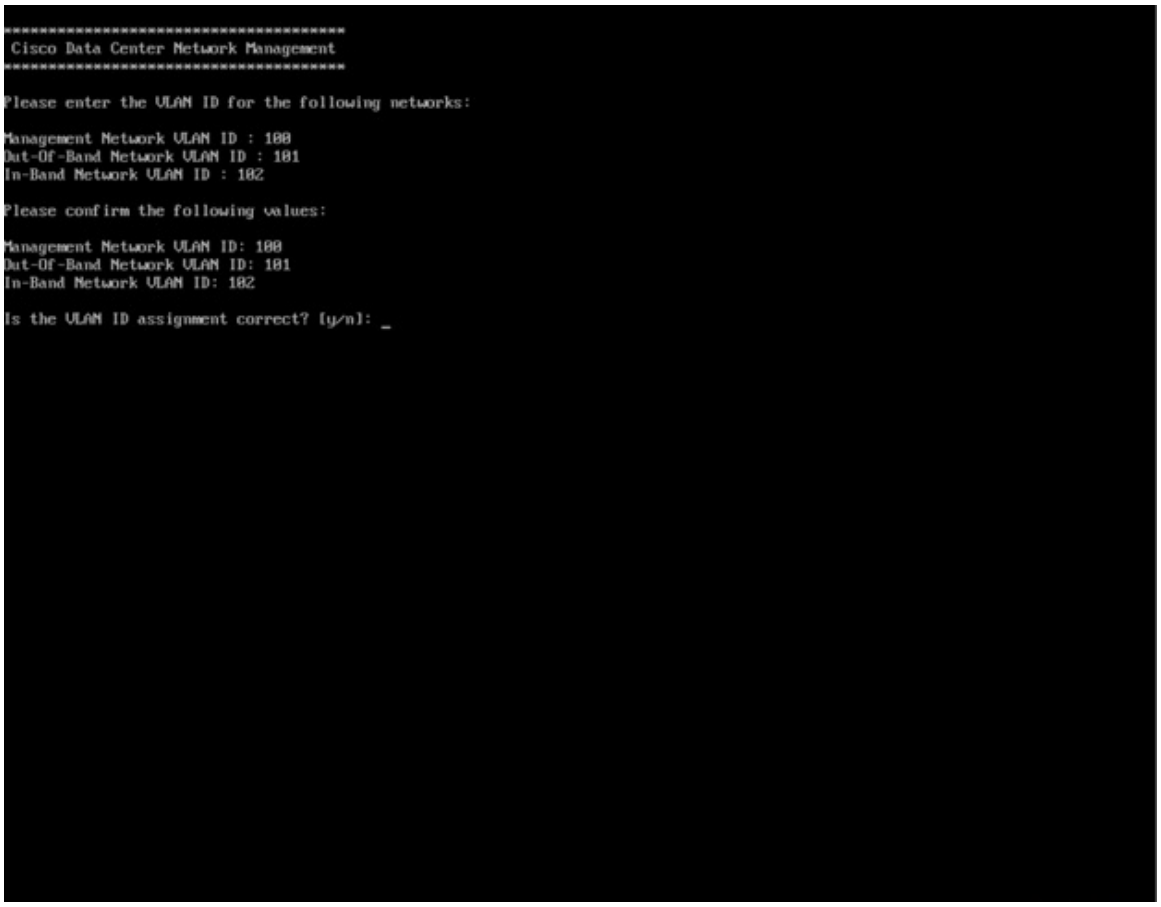
バンドルに追加する必要があるすべてのインターフェイスを入力した後に **q** を入力します。




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。




**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

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」」セクションを参照してください。

# KVM 上での DCNM ISO 仮想アプライアンスのインストール

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

**Procedure**

**ステップ 1** を解凍し抽出し、**dcnm-kvm-vm.xml** ファイルを検索します。

**ステップ 2** KVM を実行している RHEL サーバのこのファイルを ISO として同じ場所にアップロードします。

**ステップ 3** SCP ファイル転送端末を経由して、KVM を実行している RHEL サーバに接続します。

**ステップ 4** および **dcnm-kvm-vm.xml** RHEL サーバ にアップロードします。

**ステップ 5** ファイル転送セッションを閉じます。

**ステップ 6** SSH 端末を経由して、KVM を実行している RHEL サーバに接続します。

**ステップ 7** ISO およびドメイン XML の両方がダウンロードされている場所に移動します。

**ステップ 8** **virsh** コマンドを使用して、VM (または KVM 用語とも呼ばれるドメイン) を作成します。

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

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

**ステップ 9** VNC サーバを有効にして、必要なファイアウォール ポートを開きます。

**ステップ 10** SSH セッションを閉じます。

**ステップ 11** VNC 端末を経由して、KVM を実行している RHEL サーバに接続します。

**ステップ 12** **[アプリケーション (Applications)] > [システム ツール (System Tools)] > [仮想マシン マネージャ (VMM) (Virtual Machine Manager (VMM))]** に移動します。

VM が仮想マシン マネージャで作成されます。

**ステップ 13** 仮想マシン マネージャから、一覧で VM を選択して VM を編集します。**[編集 (Edit)] > [仮想マシンの詳細 (Virtual Machine Details)] > [仮想ハードウェアの詳細を表示する (Show virtual hardware details)]** をクリックします。

**ステップ 14** [仮想ハードウェアの詳細 (Virtual Hardware Details)] で、**[ハードウェアの追加 (Add Hardware)] > [ストレージ (Storage)]** に移動します。

**ステップ 15** 次の仕様で、デバイス タイプとともにハード ディスクを作成します。

- デバイス タイプ：IDE ディスク
- キャッシュ モード：デフォルト
- ストレージ形式：raw

500GB のストレージ サイズを使用することをお勧めします。

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

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

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

**ステップ 19** 仮想マシンの電源をオンにします。

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

オペレーティング システムがインストールされています。

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

[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。

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」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

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」」セクションを参照してください。

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

[コンソール (Console)] タブに表示されている URL を貼り付け、[Enter] キーを押します。初期メッセージが表示されます。

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

### Procedure

**ステップ 1** **[Cisco DCNM へようこそ (Welcome to Cisco DCNM)]** 画面から、**[開始 (Get Started)]** をクリックします。

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

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

[Next] をクリックします。

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

**[インストール モード (Install Mode)]** タブで、ドロップダウン リストから OVA DCNM アプライアンスの **[SAN のみ (SAN Only)]** インストール モードを選択します。

**[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 Systems、Inc.** または **IBM** を選択できます。

**[次へ (Next)]** をクリックします。

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

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

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

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

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

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

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

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

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

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

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

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

**[次へ (Next)]** をクリックします。

**ステップ 5** **[システム設定 (System Settings)]** で、DCNM アプライアンスの設定を行います。

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

  IPv6 アドレスを使用して DNS サーバを設定することもできます。

  リリース 11.3(1) から、1 個以上の DNS サーバと NTP サーバを設定できます。
- **[NTP サーバ アドレス リスト（NTP Server Address List）]** フィールドでは、NTP サーバの IP アドレスを入力します。

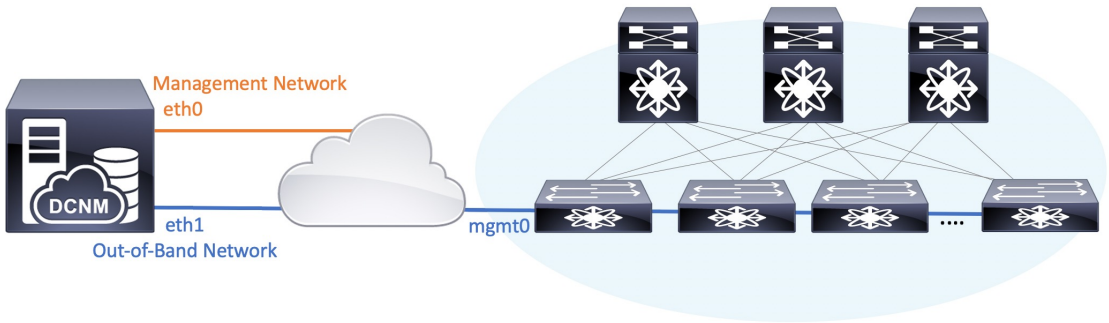
  値は IP または IPv6 アドレスか RFC 1123 に準拠した名前である必要があります。

  リリース 11.3(1) から、1 個以上の NTP サーバを設定できます。
- **タイムゾーン** ドロップダウン リストから、DCNM を展開しているタイムゾーンを選択します。

[Next] をクリックします。

**ステップ 6** **[ネットワーク設定 (Network Settings)]** タブで、DCNM Web UI に到達するために使用されるネットワーク パラメータを構成します。

***Figure 2: Cisco DCNM* 管理ネットワーク インターフェイス**



**Note** SAN OVA / ISO 展開用の Cisco DCNM では、それぞれの環境で、要件に基づいて eth0 のみ、または eth0 と eth1 の両方を（同じまたは異なるサブネットに）設定できます。eth0 または eth1 インターフェイスを介した管理/モニタリング用のスイッチへの IP 到達可能性を確立します。SAN Insights ストリーミングは、eth0 インターフェイスと eth1 インターフェイスの両方でサポートされます。ただし、それぞれのスイッチからのIP到達可能性を持つ DCNM インターフェイスにストリーミングが設定されていることを確認します。詳細については、『*OVA* と *ISO* 向けの展開設定ガイド』の「SAN Insights の設定」を参照してください。

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

管理IPアドレスのみが設定されている場合、eth0 管理インターフェイスが管理およびアウトオブバンド通信に使用されます。これは、ファブリックおよび SAN インサイトの操作に適用されることに注意してください。

**Note** 管理ネットワークに IPv6 アドレスを使用することもできます。ただし、SAN Insights ストリーミングは IPv4 アドレス設定でのみサポートされます。

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

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

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

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

c) (Optional) OVA / ISO 展開用の Cisco DCNM SAN には**インバンド ネットワーク**設定は必要ありません。

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。 eth0 インターフェイスと eth1 インターフェイスの両方が設定されている場合は、同じコマンドを使用して単一のインターフェイスを使用するようにスタティック ルートを設定できます。詳細については、DCNM インストール後のネットワーク プロパティを参照してください。

[次へ（Next）] をクリックします。

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

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

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

**[次へ (Next)]** をクリックします。

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

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

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

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

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

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

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

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

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

### What to do next

適切なクレデンシャルを使用して DCNM Web UI にログオンします。

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

# 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。

（注） OVA/ISO 展開の場合、Cisco DCNM リリース 11.5(1) にアップグレードした後、SAN クライアントまたはデバイスマネージャを起動する前に証明書を更新する必要があります。証明書を更新するには、**appmgr afw update-cert-dcnm-client** コマンドを使用します。

# 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。

# カスタム SSL 証明書対応 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** 次のコマンドを使用して公開キーを抽出します。 コマンド

**keytool.exe -exportcert -file dcnmweb.crt -alias sme -keystore C:\[DCNM Install directory]\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.exe -importcert -trustcacerts -file dcnmweb.crt -keystore fmtrust.jks -storetype jks**

**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。

**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。

### Example

次のサンプル例は、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 "<<storepass-kwd>>"
c:\[DCNM install directory]\dcm\java\jdk11\bin>
keytool.exe -exportcert -file dcnmweb.crt -alias sme -keystore 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


// generate key store without password,  during the command,
just use random password  dcnm123
c:\[DCNM install directory]\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=rhel144, 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 directory]\dcm\java\jdk11\bin>dir
chain-cert.pem  dcnmweb.crt  java  jrunscript  rmid
dcnm.csr        fmtrust.jks  jjs   keytool     rmiregistry


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


c:\[DCNM install directory]\dcm\java\jdk11\bin> FabricManager.bat
```

# 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 “<<storepass-pwd>>”
[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  jjs         keytool  rmiregistry
dcnm.csr        java         jrunscript  rmid


// generate key store without password,  during the command.
[root@dcnm-lnx1 bin]# ./keytool -importcert -trustcacerts -file dcnmweb.crt
-keystore fmtrust.jks -storetype jks
Enter keystore password:       //Navigate to
/usr/local/cisco/dcm/fm/conf/serverstore.properties.
//Fetch the keystore password from dcnmtrustedclient.token field.
Re-enter new password:
Owner: CN=Lin, OU=cisco, O=cisco, L=sj, ST=ca, C=US
Issuer: CN=rhel144, 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 â../../../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
```

# 自己署名 DCNM 証明書を使用した Linux フェデレーション セットアップでの Cisco DCNM SAN クライアントの起動

11.4.1 以前では、静的パスワード **fmserver_1_2_3** は **fmtrust.jks** 展開のために DCNM によって使用されていました。したがって、SAN クライアントを Node1 または VNC から Node1 にダウンロードし、SAN クライアントを起動できます。その後、フェデレーション設定（Node1 / Node2 / Node3）の任意のサーバにログインできます。

11.4.1 以降、DCNM は固有の **dcnm.fmserver.token** パスワードを使用します。そのため、**fmtrust.jks** ファイルは、デフォルトではフェデレーション設定の各サーバで異なります。Node1 または VNC から Node1 に SAN クライアントをダウンロードし、Node2 または Node3 で SAN クライアントを起動しようとすると、失敗します。

フェデレーションセットアップでデフォルトの DCNM 自己署名証明書を使用している場合は、それぞれのサーバから SAN クライアントをダウンロードし、SAN クライアントを起動する必要があります。同じサーバによって管理されているファブリックを開く必要があります。

次に例を示します。

- Node1 または VNC から Node1 に SAN クライアントをダウンロードし、SAN クライアントを起動して Node1 にログインします
- Node2 または VNC から Node2 に SAN クライアントをダウンロードし、SAN クライアントを起動して Node2 にログインします
- Node3 または VNC から Node3に SAN クライアントをダウンロードし、SAN クライアントを起動して Node3 にログインします

（注） これは、デフォルトの DCNM 自己署名証明書を使用するすべての DCNM フェデレーションに適用されます。また、デフォルトの DCNM 自己署名証明書を使用した DCNM フェデレーションのアップグレードにも適用されます。

# カスタムSSL証明書対応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 を参照してください。

OVA/ISO 展開の場合、Cisco DCNM リリース 11.5(1) にアップグレードした後、SAN クライアントまたはデバイスマネージャを起動する前に証明書を更新する必要があります。証明書を更新するには、**appmgr afw update-cert-dcnm-client** コマンドを使用します。

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。

# Cisco SAN OVA/ISO サーバからの DCNM SAN クライアントの起動

Cisco DCNM SAN OVA/ISO サーバで 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。

（注） DCNM SAN OVA/ISO サーバに GUI パッケージ/ X11 または VNC をインストールしないでください。

### 始める前に

OVA/ISO 展開の場合、Cisco DCNM リリース 11.5(1) にアップグレードした後、SAN クライアントまたはデバイスマネージャを起動する前に証明書を更新する必要があります。証明書を更新するには、**appmgr afw update-cert-dcnm-client** コマンドを使用します。

### 手順

**ステップ 1** VNC がインストールされている DCNM サーバへの VNC（例：`vnc-lnx:2`）。

**ステップ 2** `vnc-lnx` で 2 つの端末を開きます。

**ステップ 3** 1 番目のデバイスでコマンド **xhost +** を実行します。

**ステップ 4** 2 番目のデバイスで、DCNM OVA サーバに SSH 接続します。

**ステップ 5** **DISPLAY=vnc-lnx:2.0** をエクスポートします。

**ステップ 6** 手順 ステップ 4 （50 ページ） で、デバイスから SAN クライアントを起動します。

# VNC を使用したファブリック マネージャおよびデバイス マネージャの起動

リリース 11.5(1) 以降、Cisco DCNM は、ローカル VNC サーバでデバイス マネージャとファブリック マネージャを使用するための環境をプロビジョニングします。この環境は、OVA/ISO 展開用の Cisco DCNM SAN のインストール時に設定されます。

OVA/ISO 展開の場合、Cisco DCNM リリース 11.5(1) にアップグレードした後、SAN クライアントまたはデバイスマネージャを起動する前に証明書を更新する必要があります。証明書を更新するには、**appmgr afw update-cert-dcnm-client** コマンドを使用します。

DCNM IP アドレスを VNC クライアント ソフトウェアに接続します。接続が確立されると、VNC クライアントに仮想デスクトップが表示されます。

メニュー バーで、**[アプリケーション（Applications）]** を選択します。**Cisco Systems, Inc.** を検索します。 関連するアプリケーションが表示されます。デバイスマネージャおよびファブリック マネージャ アプリケーションを選択して実行できます。

**Note** VNC クライアント/サーバ セッションは暗号化されません。

翻訳について
このドキュメントは、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。