Cisco Nexusダッシュボード ファブリック コントローラ インストールおよびアップグレード ガイド、リリース 12.0.1a

初版：2021 年 9 月 30 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/

目 次

第 1 章 **概要 1**

概要 1

展開オプション 3

展開プロファイル 4

第 2 章 **システム要件 7**

システム要件 7

第 3 章 **注意事項と制約事項 11**

注意事項と制約事項 11

第 4 章 **前提条件 13**

前提条件 13

第 5 章 **Cisco Nexusダッシュボード ファブリック コントローラ のインストール 15**

App Store を使用した Nexusダッシュボード ファブリック コントローラ サービスのインストール 15

Nexusダッシュボード ファブリック コントローラ サービスの手動インストール 17

第 6 章 **Cisco Nexusダッシュボード ファブリック コントローラ のアップグレード 21**

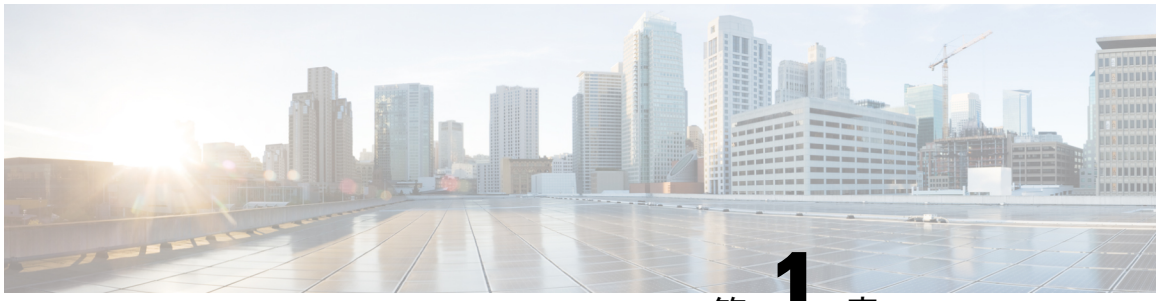
アップグレード パス 21

Nexusダッシュボード ファブリック コントローラ アップグレード ツールのダウンロード 25

アップグレード ツールを使用したバックアップ 26

Cisco Nexusダッシュボード ファブリック コントローラ のアップグレード 30

Feature Manager 32
機能セット全体での変更 33
アップグレード後の作業 34



第 1 章

概要

- 概要 （1 ページ）
- 展開オプション （3 ページ）
- 展開プロファイル （4 ページ）

概要

（注） Cisco Data Center Network Manager（DCNM）は、リリース 12.0.1a から CiscoNexusダッシュボード ファブリック コントローラ（NDFC）に名前が変更されました。

Cisco Nexusダッシュボード ファブリック コントローラ は、シスコが提供するデータ センターの LAN ファブリック、SAN、および IP Fabric for Media（IPFM）ネットワークにまたがるすべての NX-OS 展開向けの包括的な管理ソリューションです。Cisco Nexusダッシュボード ファブリック コントローラ は、IOS-XE スイッチ、IOS-XR ルータ、シスコ以外のデバイスなど、他のデバイスもサポートしています。マルチファブリック コントローラである Cisco Nexusダッシュボードファブリック コントローラ は、VXLAN EVPN、クラシック 3 層、LAN 向けのルーテッド ベース ファブリックなどの複数の展開モデルを管理すると同時に、これらすべての環境ですぐに使用できる制御、管理、モニタリング、および自動化機能を提供します。さらに、Cisco Nexusダッシュボード ファブリック コントローラ は SAN コントローラとして有効にすると、NX-OS モードで Cisco MDS スイッチと Cisco Nexus ファミリ インフラストラクチャを自動化します。

Nexusダッシュボード ファブリック コントローラ は主に3つの主要な市場セグメントの制御と管理に焦点を当てています。

- スタンドアロン NX-OS を実行する Cisco Nexus スイッチをサポートするVXLAN、マルチサイト、クラシック イーサネット、および外部ファブリックを含む LAN ネットワーキング。IOS-XR、IOS-XE、および隣接するホスト、コンピューティング、仮想マシン、およびコンテナ管理システムもサポートします。

- スタンドアロン NX-OS を実行する Cisco MDS および Cisco Nexus スイッチの SAN ネットワーキング（ストレージアレイ、さらにはホスト、コンピューティング、仮想マシン、およびコンテナ管理システムとの統合を含む）。
- スタンドアロン NX-OS として動作する Cisco Nexus スイッチを実行するマルチキャストビデオ実稼働ネットワークのメディア制御、およびサードパーティ製メディア制御システムの追加統合。

以前は、DCNM は、OVA または ISO を介して展開された VM、ISO を介して展開された物理アプライアンス、または認定された Windows または Linux マシンにインストールされたソフトウェアで実行されるアプリケーション サーバでした。Cisco Nexusダッシュボード ファブリック コントローラ リリース 12は、Cisco Nexus Dashboard 仮想アプライアンスまたは物理アプライアンス上で排他的に実行されるアプリケーションとして使用できます。

OVA を使用した仮想 Nexus Dashboard の展開は仮想 Nexus Dashboard （vND）展開とも呼ばれ、物理アプライアンス（サービス エンジン）への Nexus Dashboard の展開は物理 Nexus Dashboard（pND）展開と呼ばれます。要件に基づいて Nexus Dashboard を展開するには、『Cisco Nexus Dashboard Deployment Guide』を参照してください。

リリース 12.0.1a 以降、Cisco Nexusダッシュボード ファブリック コントローラ にはシングル インストール モードがあります。単一のインストールで複数のペルソナから選択できます。Nexusダッシュボード ファブリック コントローラ リリース 12.0.1a のインストール後、次のペルソナのいずれかを選択できます。

- ファブリック検出：LAN 展開を検出、モニタ、および可視化します。
- ファブリック コントローラ：メディア展開用のクラシック イーサネット（vPC）、ルーテッド、VXLAN、および IP ファブリック用のLANコントローラ。
- SAN コントローラ：MDS および Nexus スイッチ用の SAN コントローラ。ストリーミング テレメトリによる拡張 SAN 分析。

すべてのフィーチャ/サービスはモジュール化され、より小さなマイクロサービスに分割され、必要なマイクロサービスは機能セットまたはインストールモードに基づいて調整されます。したがって、いずれかの機能またはマイクロサービスがダウンした場合は、そのマイクロサービスのみが再起動され、中断が最小限に抑えられます。

両方のサーバのリソースを有効に活用していなかった以前の DCNM アクティブ/スタンバイ HA モデルとは対照的に、Cisco Nexusダッシュボード ファブリック コントローラ ではマイクロサービスの展開に3つのノードすべてを利用するアクティブ/アクティブ HA 展開モデルを展開しています。これにより、遅延と有効なリソース使用率が大幅に向上します。

NDFC を仮想 Nexus Dashboard インスタンス上で実行するには、外部サービス IP アドレスが指定されているインターフェイスに関連付けられたポートグループで無差別モードを有効にする必要があります。デフォルトでは、LAN 展開では、Nexus Dashboard 管理インターフェイス サブネットに 2 つの外部サービス IP アドレスが必要です。したがって、関連付けられたポートグループの無差別モードを有効にする必要があります。インバンド管理または EPL が有効になっている場合は、Nexus Dashboard データ インターフェイス サブネットで外部サービス IP アドレスを指定する必要があります。また、Nexus Dashboard のデータ/ファブリック インター

フェイス ポート グループに対して、無差別モードを有効にする必要があります。NDFC SAN コントローラの場合、無差別モードは、ポート グループに関連付けられた Nexus Dashboard データ インターフェイスでのみ有効にする必要があります。

詳細については、「Cisco Nexus Dashboard Fabric Controller（旧 DCNM）」を参照してください。

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでは、偏向のないとは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFPのドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

変更履歴

次の表は、このマニュアルの改訂履歴を示したものです。

表 *1*：変更履歴

日付	説明
2021 年 9 月 30 日	Cisco Nexusダッシュボード ファブリック コントローラ 12.0.1a のリリース ノート

展開オプション

Cisco Nexusダッシュボード ファブリック コントローラ では、次の展開オプションを使用できます。

- シングル ノードの NDFC（非 HA クラスタ）

  シングル ノードの Nexus Dashboard では、次のペルソナを使用して NDFC を展開できます。

  - SAN Insights を使用した SAN コントローラ
  - IP Fabric for Media（IPFM）展開用のファブリック コントローラ
  - ラボ/非実稼働環境用のファブリック コントローラ（25 台以下のスイッチ）

- 3ノード クラスタの NDFC（アクティブ-アクティブ HA モード）

  3 ノード Nexus Dashboard では、次のペルソナを使用して NDFC を展開できます。

  - ファブリック検出

- ファブリック コントローラ
- SAN Insights を使用した SAN コントローラ

注 NDFC 展開の場合、Nexus Dashboard ノードの管理インターフェイスとデータ/ファブリック インターフェイスに異なるサブネットが必要です。また、3 ノードの Nexus Dashboard クラスタでは、すべての Nexus Dashboard ノードがレイヤ 2 に隣接している必要があります。つまり、3 つの Nexus Dashboard ノードは、すべて同じ管理ネットワークとデータ ネットワークに属している必要があります。

要約すると、Nexusダッシュボード ファブリック コントローラ は重複するサブネットを使用する管理ネットワークとデータ ネットワークで展開される Nexus Dashboard ノードではサポートされません。

この展開では、3 つの ND ノードすべてがマスターとして機能します。3 ノード HA はアクティブ/アクティブ ソリューションです。つまり、すべてのノードがNexus Dashboard ファブリック コントローラのマイクロサービスの実行に使用されます。ノードに障害が発生すると、障害が発生したノードで実行されている Nexus Dashboard ファブリック コントローラ マイクロサービスは、他の 2 つのノードに移動されます。Nexus Dashboard ファブリック コントローラは、1 つのノード障害状態で正常に動作します。ノード障害時に移行する必要があるサービスが短時間中断することが予想されます。ただし、サービスの移行が完了すると、サポートされるスケールは引き続き機能します。ただし、1 つのノードで障害が発生しているシステムは望ましい状況ではないため、できるだけ早く修正する必要があります。3 ノード クラスタは 2 ノードの障害に耐えられず、すべての Nexus Dashboard ファブリック コントローラ サービスが中断されます。

ESXi 環境での仮想 Nexus Dashboard OVA導入では、Nexus Dashboard 管理および Nexus Dashboard データ/ファブリック インターフェイス ポート グループに関連付けられたポート グループで無差別モードを有効にする必要があります。そうしないと、SNMP トラップ、イメージ管理、エンドポイント ロケータ、SAN インサイトなどの一部の機能が動作しません。

展開プロファイル

ペルソナに基づいて Cisco Nexusダッシュボード ファブリック コントローラ をインストールするときに、展開プロファイルを選択できます。NDFC アプリケーションを展開すると、Nexus Dashboardに、クラスタ フォームファクタ用に選択された展開プロファイルが表示されます。以下に明示的に記載されていない限り、通常はこれをオーバーライドする必要はありません。

次の推奨事項を参考にして、適切なプロファイルを選択してください。

• **virtual-demo**

この展開プロファイルは、NDFC アプリケーション OVA を使用して導入された仮想 Nexus Dashboard クラスタで実行するアプリケーション用に選択する必要があります。

(注) Nexus Dashboard で NDFC アプリケーションを有効にしている場合にのみ、このプロファイルを上書きできます。

サポートされる展開ペルソナには、次のものが含まれます

- シングル ノードでのファブリック検出
- シングル ノード クラスタでのファブリック コントローラの展開
- シングル ノード クラスタの IPFM を使用したファブリック コントローラ
- シングル ノードでの SAN Insights を使用した SAN コントローラの展開

(注) virtual-demo プロファイルは、純粋にデモ用であり、実稼働環境で使用することは意図されていません。

• **virtual-app**

この展開プロファイルは、NDFC アプリケーション OVA を使用して導入された仮想 Nexus Dashboard クラスタで実行するアプリケーション用に選択する必要があります。NDFC アプリケーションが仮想 Nexus Dashboard で有効になっている場合、デフォルトでこのプロファイルが選択されます。

サポートされる展開ペルソナには、次のものが含まれます

- 3 ノード クラスタのファブリック コントローラ
- シングル または 3 ノード クラスタの IPFM を使用するファブリック コントローラ
- シングル または 3 ノード クラスタの SAN コントローラ

(注) SAN Insights は、この展開プロファイルではサポートされていません。

• **virtual-data**

この展開プロファイルは、データ OVA を使用して展開された仮想 Nexus Dashboard クラスタで実行される NDFC アプリケーション用に選択する必要があります。このプロファイルは、SAN Insights で SAN コントローラ ペルソナに使用する必要があります。デフォル

トでは、NDFC アプリケーションがデータ ノード仮想 Nexus Dashboard で有効になっている場合、このプロファイルが選択されます。

サポートされる展開ペルソナには、次のものが含まれます

- シングル または 3 ノード クラスタの SAN コントローラ

注 SAN Insights は、シングルまたは 3 マスター クラスタ ノードのこの展開プロファイルでサポートされます

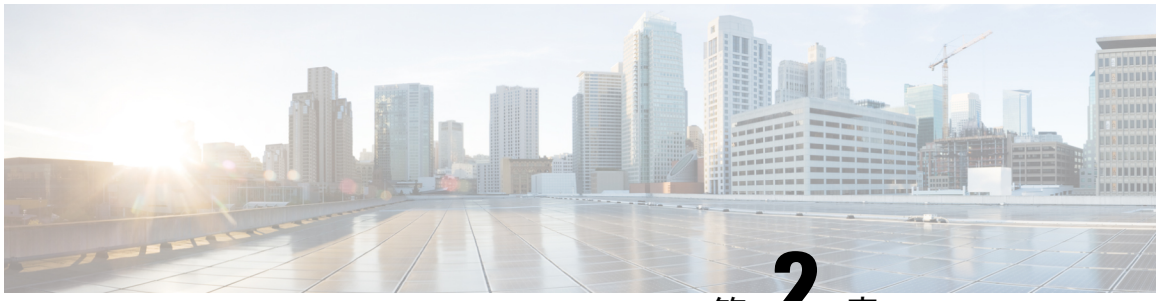
- **物理**

この展開プロファイルは、物理 Nexus Dashboard クラスタで実行する NDFC アプリケーション用に選択する必要があります。デフォルトでは、このプロファイルは、NDFCアプリケーションが物理 Nexus Dashboard で有効になっている場合に選択されます。

サポートされる展開ペルソナには、次のものが含まれます

- 3ノード クラスタのファブリック コントローラ
- シングル または 3 ノード クラスタの IPFM を使用するファブリック コントローラ
- シングル または 3 ノード クラスタの SAN コントローラ

注 SAN Insights は、この展開プロファイルでサポートされます。



第 2 章

システム要件

• システム要件 （7 ページ）

システム要件

この章では、Cisco Nexus Dashboard ファブリック コントローラ アーキテクチャのテスト済みおよびサポート対象のハードウェアとソフトウェアの仕様を示します。アプリケーションは英語ロケールのみです。

次のセクションでは、Cisco Nexusダッシュボード ファブリック コントローラ、リリース 12.0.1a を正しく機能させるためのさまざまなシステム要件について説明します。

（注） 基盤となるサードパーティ ソフトウェアを個別にアップグレードしないことを推奨します。必要なソフトウェア コンポーネントはすべて、インライン アップグレード手順で更新されます。Nexusダッシュボード ファブリック コントローラ アップグレードの外部のコンポーネントのアップグレードで機能上の問題を生じさせます。

• Cisco Nexus Dashboard バージョンの互換性 （7 ページ）
• Nexus Dashboard サーバ リソース（CPU/メモリ）要件 （8 ページ）
• サポートされている遅延 （9 ページ）
• サポートされる Web ブラウザ （9 ページ）
• その他のサポート対象のソフトウェア （9 ページ）

Cisco Nexus Dashboard バージョンの互換性

Cisco Nexusダッシュボード ファブリック コントローラ（NDFC）には、Nexus Dashboard バージョン **2.1(1e)** 以降が必要です。NDFC 2.1(1e) より前のバージョンの Nexus 2.1(1e) に 12.0.1a をアップロードしようとすると、NDFC アプリケーションをアップロードできません。Nexus Dashboard の正しいバージョンをダウンロードするには、ソフトウェア ダウンロード：Nexus Dashboard にアクセスしてください。

Nexus Dashboard サーバ リソース（CPU/メモリ）要件

表 *2 : ND* 上で *NDFC* を実行するためのサーバ リソース（*CPU*/メモリ）要件

展開タイプ	ノードタイプ	CPU	メモリ	ストレージ（スループット：40～50 MB/s）
ファブリック検出	仮想ノード（vND）：アプリケーション OVA	16vCPU	64 GB	550GB SSD
	物理ノード（pND） （PID：SE-NODE-G2）	2 X 10コア2.2G Intel Xeon Silver CPU	256 GB の RAM	4 X 2.4 TB HDD 400 GB SSD 1.2 TB NVME ドライブ
ファブリック コントローラ	仮想ノード（vND）：アプリケーション OVA	16vCPU	64 GB	550GB SSD
	物理ノード（pND） （PID：SE-NODE-G2）	2 X 10コア2.2G Intel Xeon Silver CPU	256 GB の RAM	4 X 2.4 TB HDD 400 GB SSD 1.2 TB NVME ドライブ
SAN コントローラ	仮想ノード（vND）：アプリケーション OVA （SAN Insights なし）	16vCPU	64 GB	550GB SSD
	データ ノード（vND）：データ OVA （SAN Insights を使用）	32vCPU	128GB	3TB SSD
	物理ノード（pND） （PID：SE-NODE-G2）	2 X 10コア2.2G Intel Xeon Silver CPU	256 GB の RAM	4 X 2.4 TB HDD 400 GB SSD 1.2 TB NVME ドライブ

サポートされている遅延

Cisco Nexusダッシュボード ファブリック コントローラ は Cisco Nexus Dashboard 上に展開されるため、遅延係数は Cisco Nexus Dashboard に依存します。遅延については、『Cisco Nexus Dashboard Deployment Guide』を参照してください。

サポートされる Web ブラウザ

Cisco Nexusダッシュボード ファブリック コントローラ は次の Web ブラウザをサポートします。

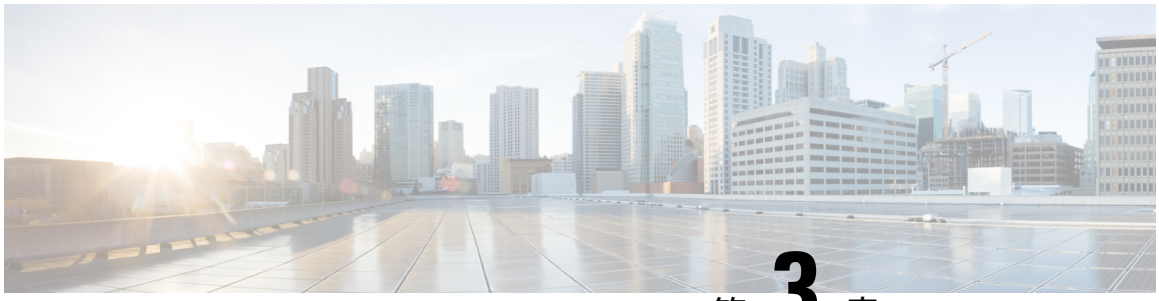
- Google Chrome バージョン：92.0.4515.159
- Mozilla Firefox バージョン：91.0.2（64 ビット）
- Microsoft Edge バージョン：92.0.902.84

その他のサポート対象のソフトウェア

次の表に、Cisco Nexus Dashboard ファブリック コントローラ リリース 12.0.1a 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。

コンポーネント	機能
セキュリティ	• ACS バージョン 4.0、5.1、5.5、および 5.8 • ISE バージョン 2.6 • ISE バージョン 3.0 • Telnet 無効：SSH バージョン 1、SSH バージョン 2、グローバル適用 SNMP プライバシー暗号化。 • Webクライアント：TLS 1、1.1、および1.2を使用したHTTPS • TLS 1.3

システム要件



第 3 章

注意事項と制約事項

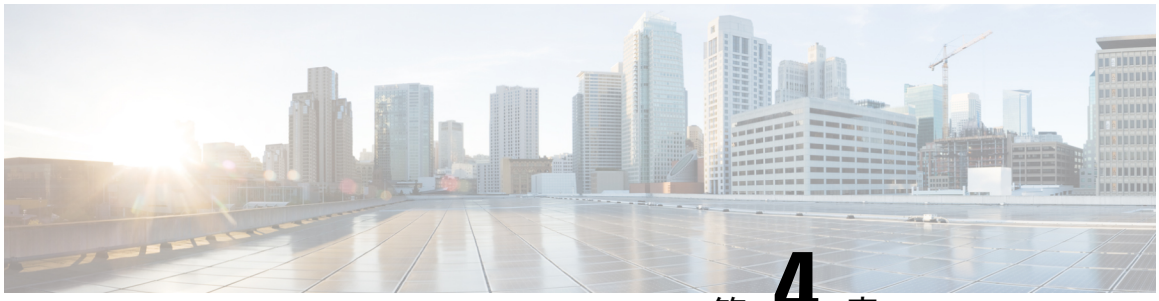
Cisco Nexusダッシュボード ファブリック コントローラ のインストールとアップグレードのための注意事項と制約事項は以下のとおりです。

- 注意事項と制約事項 （11 ページ）

注意事項と制約事項

基盤となるサードパーティ ソフトウェアを個別にアップグレードしないことを推奨します。必要なソフトウェア コンポーネントはすべて、インライン アップグレード手順で更新されます。Nexusダッシュボード ファブリック コントローラ アップグレードの外部のコンポーネントのアップグレードで機能上の問題を生じさせます。

注意事項と制約事項



第 4 章

前提条件

この章では、*Cisco Nexus*ダッシュボード ファブリック コントローラ 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。

- 前提条件 （13 ページ）

前提条件

Cisco Nexus Dashboard に Cisco Nexusダッシュボード ファブリック コントローラ をインストールする前に、次の前提条件を満たしている必要があります。

Nexusダッシュボード

ここで説明する追加の要件と Nexusダッシュボード ファブリック コントローラ サービスのインストールに進む前に、『*Cisco Nexus Dashboard Deployment Guide*』の説明に従って、Cisco Nexus Dashboard クラスタを展開し、そのファブリック接続を設定する必要があります。

Nexusダッシュボード ファブリック コントローラ リリース	Nexus Dashboard の最小リリース
リリース 12.0.1a	Cisco Nexus Dashboard、リリース 2.1.1e 以降 （注） Linux KVM の Cisco Nexus Dashboard クラスタは Nexusダッシュボード ファブリック コントローラ リリース 12.0.1a をサポートしていません。

Nexus ダッシュボードのネットワーク

最初に Nexus ダッシュボードを設定するときは、2 つの Nexus ダッシュボード インターフェイスに 2 つの IP アドレスを指定する必要があります。1 つはデータ ネットワークに接続し、もう 1 つは管理ネットワークに接続します。データ ネットワークは、ノードのクラスタリングおよびシスコ ファブリック トラフィックに使用されます。管理ネットワークは、Cisco Nexus Dashboard Web UI、CLI、または API への接続に使用されます。

ノード内の管理インターフェイスとデータインターフェイスは、Nexusダッシュボードファブリック コントローラ の異なるサブネットに属している必要があります。ノード間のインターフェイスは、同じレイヤ 2 ネットワーク（または同じレイヤ 3 サブネット）内にある必要があります。

Nexusダッシュボード ファブリック コントローラ に対して 150ms を超えないラウンドトリップ時間（RTT）で、両方のネットワークでノード間の接続が必要です。同じ Nexus Dashboard クラスタで実行されている他のアプリケーションの RTT 要件は低くなる可能性があり、同じ Nexus Dashboard クラスタに複数のアプリケーションを展開する場合は、常に最も低い RTT 要件を使用する必要があります。詳細については、『Cisco Nexus Dashboard Deployment Guide』を参照することを推奨します。

Nexusダッシュボード ファブリック コントローラ が Nexus ダッシュボードに展開されると、次の表に示すように 2 つのネットワークのそれぞれが異なる目的で使用されます。

Nexusダッシュボード ファブリック コントローラ Traffic Type	Nexus ダッシュボードのネットワーク
Cisco Nexusダッシュボード ファブリック コントローラとの間のすべてのトラフィック	データ ネットワーク
クラスタ間通信	データ ネットワーク
監査ログ ストリーミング（Splunk/syslog）	管理ネットワーク
リモート バックアップ	管理ネットワーク

Nexus Dashboard クラスタのサイジング

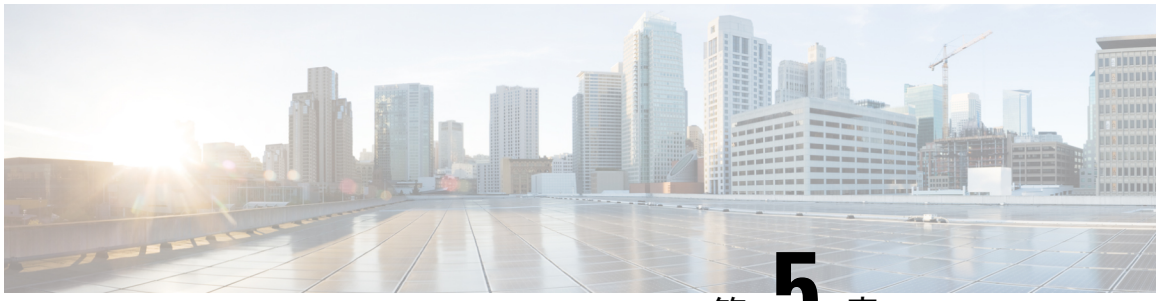
Nexus Dashboard は、サービスの共同ホスティングをサポートします。実行するサービスの種類と数によっては、クラスタに追加のワーカーノードを展開する必要があります。クラスタのサイジング情報と、特定の使用例に基づく推奨ノード数については、『Cisco Nexus Dashboard Capacity Planning』を参照してください。

Nexusダッシュボード ファブリック コントローラ に加えて他のアプリケーションもホストする予定の場合は、クラスタのサイジングツールの推奨事項に基づいて追加のNexusダッシュボードノードを展開して設定します。これについては、『Cisco Nexus Dashboard User Guide』（Nexus Dashboard Web UI から直接入手可能）にも記載されています。

Network Time Protocol（NTP）

Nexusダッシュボード ファブリック コントローラ はクロックの同期に NTP を使用するため、環境で NTP サーバを設定する必要があります。

すべてのノードのクロックは、同じ秒内で同期する必要があります。1 秒を超える 2 つのノード間の差分は、ノード間のデータベース整合性メカニズムに影響する可能性があります。



第 5 章

Cisco Nexusダッシュボード ファブリック コントローラ のインストール

この章は、次の項で構成されています。

- App Store を使用した Nexusダッシュボード ファブリック コントローラ サービスのインストール （15 ページ）
- Nexusダッシュボード ファブリック コントローラ サービスの手動インストール （17 ページ）

App Store を使用した Nexusダッシュボード ファブリック コントローラ サービスのインストール

既存のCisco Nexus Dashboard クラスタに Cisco Nexusダッシュボード ファブリック コントローラ をインストールするには、次の手順を実行します。

始める前に

- Cisco Nexus Dashboard の必要なフォーム ファクタがインストールされていることを確認します。手順については、『Cisco Nexus Dashboard Deployment Guide』を参照してください。
- 前提条件 （13 ページ） に記載されている要件とガイドラインを満たしていることを確認します。
- Cisco DC App Center は、管理ネットワークを介して直接、またはプロキシ設定を使用して Nexus Dashboard から到達可能である必要があります。Nexus Dashboard のプロキシ設定については、『Nexus Dashboard User Guide』を参照してください。

  DC App Center への接続を確立できない場合は、このセクションをスキップして、Nexus ダッシュボード ファブリック コントローラ サービスの手動インストール （17 ページ） の手順に従ってください。

- Cisco Nexus Dashboard で、サービスに IP プール アドレスが割り当てられていることを確認します。詳細については、『*Cisco Nexus Dashboard User Guide*』の「Cluster Configuration」の項を参照してください。

手順

ステップ 1 適切なクレデンシャルを使用して、Cisco **Nexus Dashboard** Web UIを起動します。

ステップ 2 左側のナビゲーション ペインで **[管理コンソール（Admin Console）] > [サービス（Services）]** メニューをクリックし、[Services Catalog] ウィンドウを開きます。

ステップ 3 [App Store] タブで Nexusダッシュボード ファブリック コントローラ カードを特定し、**[インストール（Install）]** をクリックします。

ステップ 4 [ライセンス契約（License Agreement）] 画面で、[CISCO APP CENTER AGREEMENT] を読み、**[同意してダウンロード（Agree and Download）]** をクリックします。

アプリケーションが Nexus Dashboard にダウンロードされ、展開されるまで待ちます。

アプリケーションがすべてのノードおよびすべてのサービスに完全に展開されるまでには、最大 30 分かかります。

Nexusダッシュボード ファブリック コントローラ アプリケーションが**サービス カタログ**に表示されます。ステータスは **[初期化中（Initializing）]** として表示されます。

ステップ 5 Nexusダッシュボード ファブリック コントローラ アプリケーションが初期化されたら、Nexusダッシュボード ファブリック コントローラアプリケーション カードで **[有効（Enable）]** をクリックします。

[Cisco Nexus Dashboard ファブリック コントローラを有効にする（Enable Cisco Nexus Dashboard Fabric Controller）] ウィンドウが表示されます。

ステップ 6 **[展開プロファイル（Deployment Profile）]** フィールドをクリックして、さまざまなプロファイルを表示します。

展開プロファイルには、Cisco Nexusダッシュボード ファブリック コントローラ に必要なリソースプロファイルが含まれています。詳細については、展開プロファイル （4 ページ）を参照してください。

ステップ 7 **[有効化（Enable）]**をクリックします。

サービスが有効になると、Nexusダッシュボード ファブリック コントローラ カードのボタンに **[開く（Open）]** と表示されます。

すべてのポッドとコンテナが稼働するまで待ちます。

ステップ 8 **[開く（Open）]** をクリックして、Cisco Nexus Dashboard ファブリック コントローラ Web UI を起動します。

（注） シングル サインオン（SSO）機能を使用すると、Nexus Dashboard で使用したものと同じクレデンシャルを使用してアプリケーションにログインできます。

Nexus Dashboard ファブリック コントローラ Web UI が新しいブラウザで開きます。**[フィーチャ管理]** ウィンドウが表示されます。

（注） 外部サービスプールの IP アドレスが設定されていない場合は、エラー メッセージが表示されます。**[Nexus Dashboard] Web UI > [インフラストラクチャ（Infrastructure）] > [クラスタ設定（Cluster Configuration）]** に移動します。[外部サービス プール（External Service Pools）]セクションで管理サービスとデータサービスの IP アドレスを設定します。詳細については、『*Cisco Nexus* ダッシュボード ユーザ ガイド』の「クラスタ設定」の項を参照してください。

[ファブリック検出（Fabric Discovery）]、[ファブリック コントローラ（Fablic Controller）]、および [SAN コントローラ（SAN Controller）] の 3 つのカードが表示されます。

ステップ 9 要件に基づいて、展開を選択します。

[フィーチャ（Features）] のリストから、Nexusダッシュボード ファブリック コントローラ の展開で有効にする必要がある機能を選択します。

（注） 表示されるフィーチャのリストは、カードで選択した展開に基づいています。

ステップ 10 **[適用（Apply）]** をクリックして、選択したフィーチャで Nexusダッシュボード ファブリック コントローラ を展開します。

インストールが完了すると、展開カードとすべてのフィーチャのステータスが **[開始（Started）]** になります。

Nexusダッシュボード ファブリック コントローラ サービスの手動インストール

既存の Cisco Nexus Dashboard クラスタにC isco Nexusダッシュボード ファブリック コントローラを手動でアップロードしてインストールするには、次の手順を実行します。

始める前に

- Cisco Nexus Dashboard の必要なフォーム ファクタがインストールされていることを確認します。手順については、『Cisco Nexus Dashboard Deployment Guide』を参照してください。
- 前提条件 （13 ページ） に記載されている要件とガイドラインを満たしていることを確認します。
- Cisco Nexus Dashboard で、サービスに IP プール アドレスが割り当てられていることを確認します。詳細については、『*Cisco Nexus Dashboard User Guide*』の「Cluster Configuration」の項を参照してください。

手順

ステップ 1 次のサイトに移動します。https://dcappcenter.cisco.com

[Cisco DC のアプリケーション センター] ページが開きます。

[すべてのアプリケーション（All apps）] セクションで、すべてのアプリケーションは Cisco Nexus Dashboard でサポートされています。

ステップ 2 Cisco Nexusダッシュボード ファブリック コントローラ リリース 12.0.1aアプリケーションを見つけ、**[ダウンロード（Download）]** アイコンをクリックします。

ステップ 3 [ライセンス契約（License Agreement）] 画面で、[CISCO APP CENTER AGREEMENT] を読み、**[同意してダウンロード（Agree and Download）]** をクリックします。

Nexus ダッシュボードにインポート/アップロードする必要があるときに見つけやすいように、Nexusダッシュボード ファブリック コントローラ アプリケーションをディレクトリに保存します。

ステップ 4 適切なクレデンシャルを使用してCisco Nexusダッシュボードを起動します。

ステップ 5 Cisco Nexus Dashboard にインストールされているサービスを表示するには、**[管理コンソール（Admin Console）] > [サービス（Services）] > [インストール済みのサービス（Installed Services）]**の順に選択します。

ステップ 6 **[アクション（Actions）]** ドロップダウン リストから、**[サービスのアップロード（Upload Service）]** を選択します。

ステップ 7 **[ロケーション（Location）]** トグルボタンを選択し、[リモート（Remote）] または [ローカル（Local）] を選択します。

リモート ディレクトリまたはローカル ディレクトリからサービスをアップロードできます。

- **[リモート（Remote）]** を選択した場合は、**[URL]** フィールドに、Nexusダッシュボード ファブリック コントローラアプリケーションが保存されているディレクトリへの絶対パスを入力します。
- **[ローカル（Local）]** を選択した場合は、**[参照（Browse）]** をクリックして、Nexusダッシュボード ファブリック コントローラ アプリケーションが保存されている場所に移動します。アプリケーションを選択し、**[開く（Open）]** をクリックします。

ステップ 8 [アップロード（Upload）] をクリックします。

Nexusダッシュボード ファブリック コントローラ アプリケーションがサービス カタログに表示されます。ステータスは [初期化中（Initializing）] として表示されます。

アプリケーションが Nexus Dashboard にダウンロードされ、展開されるまで待ちます。

アプリケーションがすべてのノードおよびすべてのサービスに完全に展開されるまでには、最大 30 分かかります。

Nexusダッシュボード ファブリック コントローラ アプリケーションが**サービス カタログ**に表示されます。ステータスは **[初期化中（Initializing）]** として表示されます。

ステップ 9 Nexusダッシュボード ファブリック コントローラ アプリケーションが初期化されたら、Nexusダッシュボード ファブリック コントローラアプリケーション カードで **[有効（Enable）]** をクリックします。

[Cisco Nexus Dashboard ファブリック コントローラを有効にする（Enable Cisco Nexus Dashboard Fabric Controller）] ウィンドウが表示されます。

ステップ 10 **[展開プロファイル（Deployment Profile）]** フィールドをクリックして、さまざまなプロファイルを表示します。

展開プロファイルには、Cisco Nexusダッシュボード ファブリック コントローラ に必要なリソースプロファイルが含まれています。詳細については、展開プロファイル （4 ページ）を参照してください。

ステップ 11 **[有効化（Enable）]**をクリックします。

サービスが有効になると、Nexusダッシュボード ファブリック コントローラ カードのボタンに **[開く（Open）]** と表示されます。

すべてのポッドとコンテナが稼働するまで待ちます。

ステップ 12 **[開く（Open）]** をクリックして、Cisco Nexus Dashboard ファブリック コントローラ Web UI を起動します。

（注） シングル サインオン（SSO）機能を使用すると、Nexus Dashboard で使用したものと同じクレデンシャルを使用してアプリケーションにログインできます。

Nexus Dashboard ファブリック コントローラ Web UI が新しいブラウザで開きます。**[フィーチャ管理]** ウィンドウが表示されます。

（注） 外部サービスプールの IP アドレスが設定されていない場合は、エラー メッセージが表示されます。**[Nexus Dashboard] Web UI > [インフラストラクチャ（Infrastructure）] > [クラスタ設定（Cluster Configuration）]** に移動します。[外部サービス プール（External Service Pools）]セクションで管理サービスとデータサービスの IP アドレスを設定します。詳細については、『*Cisco Nexus* ダッシュボード ユーザ ガイド』の「クラスタ設定」の項を参照してください。

[ファブリック検出（Fabric Discovery）]、[ファブリック コントローラ（Fablic Controller）]、および [SAN コントローラ（SAN Controller）] の 3 つのカードが表示されます。

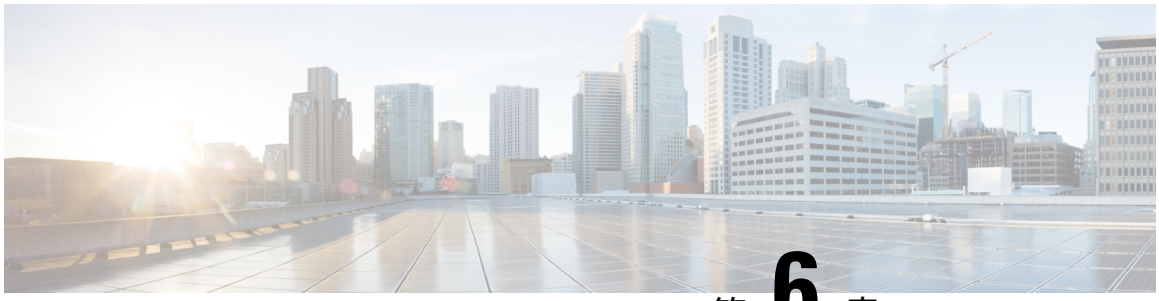
ステップ 13 要件に基づいて、展開を選択します。

[フィーチャ（Features）] のリストから、Nexusダッシュボード ファブリック コントローラ の展開で有効にする必要がある機能を選択します。

（注） 表示されるフィーチャのリストは、カードで選択した展開に基づいています。

ステップ 14 **[適用（Apply）]** をクリックして、選択したフィーチャで Nexusダッシュボード ファブリック コントローラ を展開します。

インストールが完了すると、展開カードとすべてのフィーチャのステータスが**[開始（Started）]**になります。



第 6 章

Cisco Nexusダッシュボード ファブリック コントローラ のアップグレード

この章では、Cisco Nexusダッシュボード ファブリック コントローラ 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。

- アップグレード パス （21 ページ）
- Nexusダッシュボード ファブリック コントローラ アップグレード ツールのダウンロード （25 ページ）
- アップグレード ツールを使用したバックアップ （26 ページ）
- Cisco Nexusダッシュボード ファブリック コントローラ のアップグレード （30 ページ）
- Feature Manager （32 ページ）
- アップグレード後の作業 （34 ページ）

アップグレード パス

次の表は、リリース 12.0.1a 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。

[ソフトウェアのダウンロード（Software Download）] に移動して、アップグレード ツール スクリプトをダウンロードします。

現在のリリース番号	展開タイプ	リリース 12.0.1a にアップグレードするアップグレード タイプ
11.5(3)	すべて	未サポート

現在のリリース番号	展開タイプ	リリース12.0.1aにアップグレードするアップグレード タイプ
11.5(2)	Windows および Linux での SAN の展開	• **DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip** を使用したバックアップ • Nexusダッシュボード ファブリック コントローラ**Web UI > [操作（Operations）] > [バックアップと復元（Backup & Restore）]** での復元
	OVA/ISO/SE での SAN 展開	• **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** を使用したバックアップ • Nexusダッシュボード ファブリック コントローラ**Web UI > [操作（Operations）] > [バックアップと復元（Backup & Restore）]** での復元
	OVA/ISO/SE での LAN ファブリックの展開	• **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** を使用したバックアップ • Nexusダッシュボード ファブリック コントローラ**Web UI > [操作（Operations）] > [バックアップと復元（Backup & Restore）]** での復元

現在のリリース番号	展開タイプ	リリース 12.0.1a にアップグレードするアップグレード タイプ
11.5(1)	Windows および Linux での SAN の展開	• **DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip** を使用したバックアップ • Nexusダッシュボードファブリック コントローラ **Web UI > [操作（Operations）] > [バックアップと復元（Backup & Restore）]** での復元
	OVA/ISO/SE での SAN 展開	• **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** を使用したバックアップ • Nexusダッシュボードファブリック コントローラ **Web UI > [操作（Operations）] > [バックアップと復元（Backup & Restore）]** での復元
	OVA/ISO/SE での LAN ファブリックの展開	• **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** を使用したバックアップ • Nexusダッシュボードファブリック コントローラ **Web UI > [操作（Operations）] > [バックアップと復元（Backup & Restore）]** での復元
	OVA/ISO でのメディア コントローラの展開	• **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO.zip** を使用したバックアップ • Nexusダッシュボードファブリック コントローラ **Web UI > [操作（Operations）] > [バックアップと復元（Backup & Restore）]** での復元

アップグレードのペルソナ互換性

適切なアップグレードツールを使用することで、次の表に示すように、新しく展開されたCisco Nexusダッシュボード ファブリック コントローラ にペルソナの DCNM リリース 11.5 (1) またはリリース 11.5 (2) からバックアップされたデータを復元できます。

DCNM 11.5(x) から のバックアップ[1]	アップグレード後の **NDFC 12.0.1a** でのペルソナの有効化
OVA/ISO/SE での DCNM 11.5(x) LAN ファブリックの展開	ファブリック コントローラ + ファブリック ビルダー

DCNM 11.5(x) から のバックアップ[1]	アップグレード後の NDFC 12.0.1a でのペルソナの有効化
OVA/ISO/SE でのDCNM 11.5(x) PMN の展開	ファブリック コントローラ +メディアの IP ファブリック（IPFM）
OVA/ISO/SE での DCNM 11.5(x) SAN の展開	SAN コントローラ
Linux での DCNM 11.5(x) SAN の展開	SAN コントローラ
Windows での DCNM 11.5（x）SAN の展開	SAN コントローラ

[1] 11.5(x) のすべての参照は、11.5(1) または 11.5(2) に対するものです。DCNM 11.5(3) から NDFC 12 へのアップグレードはサポートされていません。

アップグレード後の機能の互換性

次の表に、NDFC、リリース 12.0.1a へのアップグレード後に DCNM 11.5(x) バックアップから復元される機能に関連する警告を示します。

DCNM 11.5(x) の機能	アップグレードのサポート
設定済みのマルチサイト オーケストレーター	サポート対象外
Nexus Insights の設定	サポート対象外
設定されたプレビュー フィーチャー	サポート対象外
SAN インストールの LAN スイッチ	サポート対象外
IPv6 で検出されたスイッチ	サポート対象外
Container Orchestrator フィーチャー	サポート対象外
vCenter コンピューティング フィーチャ	サポート対象外
DCNM トラッカー	サポート対象外
SAN CLI テンプレート	11.5(x) から 12.0.1a に引き継がれない
イメージ/イメージ管理データの切り替え	11.5(x) から 12.0.1a に引き継がれない
スロードレイン データ	11.5(x) から 12.0.1a に引き継がれない
Infoblox 設定	11.5(x) から 12.0.1a に引き継がれない
エンドポイント ロケーションの設定	リリース 12.0.1a へのアップグレード後に、エンドポイント ロケータ（EPL）を再設定する必要があります。ただし、履歴データは最大 500 MB まで保持されます。

DCNM 11.5(x) の機能	アップグレードのサポート
アラーム ポリシーの設定	11.5(x) から 12.0.1a に引き継がれない
パフォーマンス管理データ	アップグレード後、最大 90 日間の CPU/メモリ/インターフェイス統計情報が復元されます。

Nexusダッシュボード ファブリック コントローラ アップグレード ツールのダウンロード

Cisco DCNM から Nexusダッシュボード ファブリック コントローラ にアップグレードするアップグレード ツールをダウンロードするには、次の手順を実行します。

始める前に

- Cisco DCNM リリース 11.5(x) セットアップの展開タイプを特定します。

手順

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

ダウンロード可能な Cisco Nexusダッシュボード ファブリック コントローラ の最新リリース ソフトウェアのリストが表示されます。

ステップ 2 最新のリリース リストで、リリース 12.0.1a を選択します。

ステップ 3 Cisco DCNM 11.5(x) の展開タイプに基づいて、**DCNM_To_NDFC_Upgrade_Tool** を見つけ、**[ダウンロード（Download）]** アイコンをクリックします。

次の表に、DCNM 11.5(x) 展開タイプと、ダウンロードする必要がある対応する Nexusダッシュボード ファブリック コントローラ アップグレード ツールを示します。

表 3 :『DCNM 11.5(x) Deployment type and Upgrade Tool Compatibility Matrix』

DCNM 11.5(x) 展開タイプ	アップグレード ツール名
ISO/OVA	DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
Linux	DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
Windows	DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip

ステップ 4 **sysadmin** クレデンシャルを使用して、11.5(x) サーバに適切な**アップグレード ツール**を保存します。

アップグレード ツールを使用したバックアップ

DCNM 11.5 上のすべてのアプリケーションとデータのバックアップを取得するために **DCNM_To_NDFC_Upgrade_Tool** を実行するには、次の作業を実行します。

始める前に

- Cisco DCNM リリース 11.5(1) では、バックアップを実行する前に、各ファブリックを検証してください。[Cisco DCNM **[Web UI]-[管理（Administration）]-[クレデンシャル管理（Credentials Management）]-[SANクレデンシャル（SAN Credentials）]**を選択します。各ファブリックを選択し、**[検証（Validate）]** をクリックしてクレデンシャルを検証してからバックアップを作成します。
- 適切なアップグレード ツールを DCNM 11.5(x) セットアップのサーバにコピーしたことを確認します。
- アップグレードツールの実行権限が有効になっていることを確認します。実行可能権限を有効にするために **chmod +x .** を使用します。

```
[root@dcnm]# chmod +x ./DCNM12UpgradeToolOVAISO
```

手順

ステップ 1 Cisco DCNM リリース 11.5(x) アプライアンス コンソールにログインします。

ステップ 2 次のコマンドを実行してスクリーン セッションを作成します。

```
dcnm# screen
```

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

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

```
dcnm# su
Enter password: <<enter-password>>
[root@dcnm]#
```

ステップ 4 **./DCNM_To_NDFC_Upgrade_Tool** 個マンdのを使用してアップグレードツールを実行します。

OVA / ISO の場合：

```
[root@dcnm]# ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO /* for OVA/ISO
```

Windows/Linux の場合：

```
root@dcnm]# unzip DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
[root@dcnm-rhel]# cd DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/
[root@dcnm-rhel DCNM_To_NDFC_Upgrade_Tool_LIN_WIN]# ls
DCNMBackup.bat  DCNMBackup.sh  jar
[root@rhel DCNM_To_NDFC_Upgrade_Tool_LIN_WIN]# ./DCNMBackup.sh        /* Enter this
command for Linux appliance */
OR
```

```
[root@rhel DCNM_To_NDFC_Upgrade_Tool_LIN_WIN]# ./DCNMBackup.bat          /* Enter this
command for Windows appliance */
```

アップグレード ツールは DCNM アプライアンスのデータを分析し、Cisco Nexusダッシュボード ファブリック コントローラ Release 12.0.1a にアップグレードできるかどうかを判断します。

（注） このツールを使用して生成されたバックアップは、アップグレード後にデータを復元するために使用できます。

ステップ 5 バックアップを続行するプロンプトで、**y** を押します。

```
********************************************************************************
Welcome to DCNM-to-NDFC Upgrade Tool for OVA/ISO.
This tool will analyze this system and determine whether you can move to NDFC 12.0.1a
or not.
If upgrade to NDFC 12.0.1a is possible, this tool will create files to be used for
performing the upgrade.
NOTE: only backup files created by this tool can be used for upgrading, older backup
files created with 'appmgr backup'
CAN NOT be used for upgrading to NDFC 12.0.1a

Thank you!
********************************************************************************

Continue? [y/n]: y

Collect operational data (e.g. PM, EPL)? [y/n]: y

Does this DCNM 11.5(1) have DCNM Tracker feature enabled on any switch on any fabric?
[y/n]: n
```

ステップ 6 バックアップ ファイルに対する暗号キーを入力します。

（注） バックアップ ファイルを復元するときに、この暗号キーを指定する必要があります。暗号キーは安全な場所に保存してください。暗号キーを失うと、バックアップを復元できません。

```
Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring the backup file generated
by this tool.

Please enter the encryption key:       /* enter the encryption key for the backup file
*/
Enter it again for verification:       /* re-enter the encryption key for the backup file
 */

...
...
Creating backup file
Done.
Backup file: backup11_dcnm-172-23-87-224_20210928-093355.tar.gz          /* backup file
name*/
[root@dcnm]#
```

暗号化されたバックアップ ファイルが作成されます。

ステップ 7 バックアップ ファイルを安全な場所にコピーし、アプリケーション 11.5(x) DCNM アプライアンスをシャットダウンします。

例

DCNM バックアップ ツールを使用したバックアップの例

- **DCNM 11.5(x) OVA/ISO アプライアンスでのバックアップの取得**

```
[root@dcnm]# chmod +x DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
[root@dcnm]# ./DCNM_To_NDFC_Upgrade_Tool_OVA_ISO
********************************************************************************

Welcome to DCNM-to-NDFC Upgrade Tool for OVA/ISO.

This tool will analyze this system and determine whether you can move to
NDFC 12.0.1a or not.

If upgrade to NDFC 12.0.1a is possible, this tool will create files
to be used for performing the upgrade.

NOTE:
only backup files created by this tool can be used for upgrading,
older backup files created with 'appmgr backup' CAN NOT be used
for upgrading to NDFC 12.0.1a

Thank you!

********************************************************************************

Continue? [y/n]: y

Collect operational data (e.g. PM, EPL)? [y/n]: y

Does this DCNM 11.5(1) have DCNM Tracker feature enabled on any switch on any fabric?
 [y/n]: n

Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring
the backup file generated by this tool.

Please enter the encryption key:      /* enter the encryption key for the backup
file */
Enter it again for verification:      /* re-enter the encryption key for the backup
 file */

Adding backup header
Collecting DB table data
Collecting DB sequence data
Collecting stored credentials
Collecting Custom Templates
Collecting CC files
Collecting L4-7-service data
Collecting CVisualizer data
Collecting EPL data
Collecting PM data - WARNING: this will take a while!
Collecting AFW app info
Decrypting stored credentials
Creating backup file
Done.
Backup file: backup11_dcnm-172-23-87-224_20210913-012857.tar.gz        /* backup
file name*/
[root@dcnm]#
```

- **DCNM 11.5(x) Windows/Linux アプライアンスでのバックアップの実行**

```
[root@dcnm]# chmod +x DCNM_To_NDFC_Upgrade_Tool_LIN_WIN
[root@dcnm]# unzip DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
Archive:  DCNM_To_NDFC_Upgrade_Tool_LIN_WIN.zip
    creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/
    creating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/bcprov-jdk15on-1.68.jar
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/DCNMBackup.java
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.oracle
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/slf4j-simple-1.7.21.jar
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jnm.jar
   inflating:
DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/not-going-to-be-commons-ssl-0.3.20.jar
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.postgres
   inflating:
DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/jarchivelib-0.7.1-jar-with-dependencies.jar
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/tables.info.oracle
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/sequences.info.postgres
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/jar/log4j.properties
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.sh
   inflating: DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/DCNMBackup.bat

[root@dcnm-rhel]# cd DCNM_To_NDFC_Upgrade_Tool_LIN_WIN/
[root@dcnm-rhel DCNM_To_NDFC_Upgrade_Tool_LIN_WIN]# ls
DCNMBackup.bat  DCNMBackup.sh  jar
[root@rhel DCNM_To_NDFC_Upgrade_Tool_LIN_WIN]# ./DCNMBackup.sh        /* Enter this
 command for Linux appliance */
OR
[root@rhel DCNM_To_NDFC_Upgrade_Tool_LIN_WIN]# ./DCNMBackup.bat       /* Enter this
 command for Windows appliance */

Enter DCNM root directory [/usr/local/cisco/dcm]:

Initializing, please wait...

Note: ./jar/DCNMBackup.java uses unchecked or unsafe operations.
Note: Recompile with -Xlint:unchecked for details.
********************************************************************************

Welcome to DCNM-to-NDFC Upgrade Tool for Linux/Windows.

This tool will analyze this system and determine whether you can move to NDFC 12.0.1a
 or not.

If upgrade to NDFC 12.0.1a is possible, this tool will create files to be used for
performing the upgrade.

Thank you!

********************************************************************************

This tool will backup config data. Exporting Operational data like Performance(PM)
might take some time.

Do you want to export operational data also? [y/N]: y
********************************************************************************

Sensitive information will be encrypted using an encryption key.
This encryption key will have to be provided when restoring the backup file generated
 by this tool.

Please enter the encryption key:       /* enter the encryption key for the backup
file */
Enter it again for verification:       /* re-enter the encryption key for the backup
 file */
```

Cisco Nexusダッシュボード ファブリック コントローラ のアップグレード

```
2021-09-13 14:36:31 INFO  DCNMBackup:223 - Inside init() method
2021-09-13 14:36:31 INFO  DCNMBackup:245 - Loading properties....
2021-09-13 14:36:31 INFO  DCNMBackup:301 - Inside checkLANSwitches...
2021-09-13 14:36:32 INFO  DCNMBackup:315 - LAN Switch count: 0
2021-09-13 14:36:32 INFO  DCNMBackup:342 - Inside exportDBTables...
2021-09-13 14:36:32 INFO  DCNMBackup:358 - Exporting ---------> statistics
2021-09-13 14:36:32 INFO  DCNMBackup:358 - Exporting ---------> sequence
...
...
...
2021-09-13 14:49:48 INFO  DCNMBackup:1760 - ###### Total time to export Hourly data:
 42 seconds.


2021-09-13 14:49:48 INFO  DCNMBackup:1767 - Exporting SanPort Daily entries.
2021-09-13 14:49:48 INFO  DCNMBackup:1768 - Total number of ports: 455
2021-09-13 14:49:48 INFO  DCNMBackup:1769 - This might take a while, please wait...
2021-09-13 14:50:23 INFO  DCNMBackup:1791 - Total number of Json data entries in
backup/es/pmdb_sanportratedata_daily.data ==> 13751
2021-09-13 14:50:23 INFO  DCNMBackup:1795 - ###### Total time to export Daily data:
 34 seconds.


2021-09-13 14:50:23 INFO  DCNMBackup:1535 - ###### Total time to export PM data: 81
 seconds.


2021-09-13 14:50:23 INFO  DCNMBackup:879 - Creating final tar.gz file....
2021-09-13 14:50:30 INFO  DCNMBackup:892 - Final tar.gz elapsed time: 7049 in ms
2021-09-13 14:50:30 INFO  DCNMBackup:893 - Backup done.
2021-09-13 14:50:30 INFO  DCNMBackup:894 - Log file: backup.log
2021-09-13 14:50:30 INFO  DCNMBackup:895 - Backup file:
backup11_rhel77-160_20210913-149215.tar.gz        /* backup file name*/
[root@rhel DCNM_To_NDFC_Upgrade_Tool_LIN_WIN]#
```

Cisco Nexusダッシュボード ファブリック コントローラのアップグレード

DCNM リリース 11.5(1) から Cisco Nexusダッシュボード ファブリック コントローラ リリース 12.0.1a にアップグレードするには、次の手順を実行します。

ここにコンテキストを表示

始める前に

- 11.5(x) アプライアンスから作成されたバックアップ ファイルにアクセスできることを確認します。

  暗号化キーがない場合、バックアップ ファイルから復元することはできません。

- Cisco Nexus Dashboard の必要なフォーム ファクタがインストールされていることを確認します。手順については、『Cisco Nexus Dashboard Deployment Guide』を参照してください。

- Cisco Nexusダッシュボード ファブリック コントローラ の新規インストールをインストールしたことを確認します。Cisco Nexusダッシュボード ファブリック コントローラ のインストール手順については、次を参照してください。
  - Nexusダッシュボード ファブリック コントローラ サービスの手動インストール （17 ページ）.
  - App Store を使用した Nexusダッシュボード ファブリック コントローラ サービスのインストール （15 ページ）

手順

ステップ 1 **[Nexus Dashboard] > [Services]** で、Cisco Nexusダッシュボード ファブリック コントローラ カードを特定し、**[開く（Open）]** をクリックします。

Nexusダッシュボード ファブリック コントローラ Web UI では、**[フィーチャ管理（Feature Management）]** 画面が表示されます。

新しくインストールされた Nexusダッシュボード ファブリック コントローラ でペルソナが選択されていないことに注意してください。

ステップ 2 [復元（Restore）] をクリックします。

[オペレーション（Operations）] > [バックアップと復元（Backup & Restore）] ウィンドウが開きます。

ステップ 3 [復元（Restore）] をクリックします。

[今すぐ復元（Restore now）] ウィンドウが表示されます。

ステップ 4 **[種類（Type）]** で、復元する形式を選択します。

- 設定データのみを復元するには、**[設定のみ（Config only）]** を選択します。
- このアプリケーションに以前のバージョンのデータをすべて復元するには、**[完全（Full）]** を選択します。

ステップ 5 バックアップ ファイルを保存した適切な宛先を選択します。

- ファイルがローカル ディレクトリに保存されている場合は、**[ファイルのアップロード（Upload File）]** を選択します。
  1. バックアップ ファイルが保存されるディレクトリ
  2. バックアップ ファイルを **[今すぐ復元（Restore now）]** ウィンドウにドラッグアンドドロップします。

     または

[参照（Browse）]をクリックします。バックアップ ファイルが保存されるディレクトリに移動します。バックアップ ファイルを選択して、**[開く（Open）]**をクリックします。

3. バックアップ ファイルに対する**暗号キー**を入力します。

- バックアップ ファイルがリモート ディレクトリに保存されている場合は、**[SCP からインポート（Import from SCP）]** を選択します。

1. **[SCP サーバ（SCP Server）]** フィールドに、SCP サーバの IP アドレスを入力します。
2. **[ファイル パス（File Path）]** フィールドに、バックアップ ファイルへの相対ファイル パスを入力します。
3. **ユーザ名**と**パスワード**を該当するフィールドに入力します。
4. **[暗号キー（Encryption Key）]** フィールドにバックアップ ファイルに対する暗号キーを入力します。

ステップ 6 [復元（Restore）] をクリックします。

進行状況バーが表示され、完了したパーセンテージ、操作の説明が表示されます。アップグレードの進行中は、Web UI がロックされます。復元が完了すると、バックアップ ファイルが **[バックアップと復元（Backup & Restore）]** 画面のテーブルに表示されます。復元に必要な時間は、バックアップ ファイルのデータによって異なります。

（注） Cisco Nexus ダッシュボードで IP プール アドレスを割り当てていない場合は、エラーが表示されます。詳細については、『*Cisco Nexus Dashboard User Guide*』の「Cluster Configuration」の項を参照してください。

正常に復元されると、次のような通知バナーが表示されます。

```
Reload the page to see latest changes.
```

[ページの再ロード（Reload the page）] をクリックするか、ブラウザ ページを更新して復元を完了し、Cisco Nexusダッシュボード ファブリック コントローラ Web UIの使用を開始します。

Feature Manager

展開のタイプに基づいてバックアップを復元した後、リリースは次のいずれかのパーソナリティで展開されます。Nexusダッシュボード ファブリック コントローラ12.0.1a

- ファブリック コントローラ
- SAN コントローラ

Feature Management のステータスが **[開始中（Starting）]** に変わります。また、有効にするフィーチャを選択できます。**[フィーチャ（Feature）]**チェックボックスと**[保存して続行（Save & Continue）]** をクリックします。

DCNM 11.5(x) バージョンからデータをインポートした新しいCisco Nexusダッシュボード ファブリック コントローラ Release 12.0.1a は、Web UI で使用できます。

（注） NDFC リリース 12.0.1a へのアップグレードに関して、DCNM 11.5(x) で有効になっているフィーチャに関連する警告があります。詳細については、アップグレード後の機能の互換性（24 ページ）を参照してください。

機能セット全体での変更

Nexusダッシュボード ファブリック コントローラ 12 では、ある機能セットから別の機能セットに切り替えることができます。**[設定（Settings）]>[機能管理（Feature Management）]** を選択します。次の表で、目的の機能セットとアプリケーションを選択します。[保存して続行（Save and Continue）] をクリックします。ブラウザを更新して、新しい機能セットとアプリケーションで Cisco Nexusダッシュボード ファブリック コントローラ の使用を開始します。

特定の導入でサポートされる機能/アプリケーションがいくつかあります。機能セットを変更すると、これらの機能の一部は新しい展開でサポートされません。次の表に、機能セットを変更できる前提条件と基準の詳細を示します。

表 *4:* 展開間でサポートされるスイッチング

送信元/宛先	ファブリック検出	ファブリック コントローラ	SAN コントローラ
ファブリック検出	-	ファブリック検出の展開では、モニタモードファブリックのみがサポートされます。機能セットを変更すると、ファブリック コントローラ導入でファブリックを使用できます。	サポート対象外
ファブリック コントローラ	ファブリックセットを変更する前に、既存のファブリックを削除する必要があります。	Easy Fabric から IPFM ファブリック アプリケーションに変更する場合は、既存のファブリックを削除する必要があります。	サポート対象外

送信元/宛先	ファブリック検出	ファブリック コントローラ	SAN コントローラ
SAN コントローラ	サポート対象外	サポート対象外	-

アップグレード後の作業

次の項では、Cisco NDFC、リリース 12.0.1a へのアップグレード後に実行する必要があるタスクについて説明します。

SAN コントローラのアップグレード後のタスク

バックアップからデータを復元すると、すべての server-smart ライセンスが **OutofCompliance** になります。

ポリシーを使用してスマートライセンスに移行するには、Nexusダッシュボード ファブリック コントローラ を起動します。Web UI で、**[Operations]**、**[License Management]**、**[Smart]** タブの順に選択します。SLP を使用して CCSM との信頼を確立します。手順については、『*Cisco Nexus*ダッシュボード ファブリック コントローラ *Configuration Guides*』の「*License Management*」の章を参照してください。

ファブリック コントローラのアップグレード後のタスク

DCNM 11.5(x) から Cisco NDFC 12.0.1a にアップグレードする場合、次の機能は引き継がれません。

- エンドポイント ロケータを再設定する必要があります
- IPAM 統合を再設定する必要があります
- アラーム ポリシーを再設定する必要があります
- カスタム トポロジを再作成して保存する必要があります
- ファブリックで PM 収集を再度有効にする必要があります
- スイッチ イメージをアップロードする必要があります

Nexus ダッシュボードでのトラップ IP の管理 Nexusダッシュボード ファブリック コントローラ

リリース 11.5(x) の展開タイプ	11.5(x)では、トラップ IP アドレスは	LAN デバイス管理の接続性	12.0.1a では、トラップ IP アドレスはに属します	結果
LAN ファブリック メディア コントローラ	eth1（またはHA システムの場合は vip1）	管理	管理サブネットに属する	[Honored][2]
LAN ファブリック メディア コントローラ	eth0（またはHA システムの場合は vip0）	管理	管理サブネットに属していない	無視されます。管理プールの別の IP がトラップ IP として使用されます
LAN ファブリック メディア コントローラ	eth0（またはHA システムの場合は vip0）	データ	データ サブネットに属する	Honored
LAN ファブリック メディア コントローラ	eth0（またはHA システムの場合は vip0）	データ	データ サブネットに属していない	無視されます。データ プールの別のIPがトラップ IP として使用されます

リリース 11.5(x) の展開タイプ	11.5(x) では、トラップ IP アドレスは	LAN デバイス管理の接続性	12.0.1a では、トラップ IP アドレスはに属します	結果
SAN 管理	OVA/ISO – • trap.registaddress（設定されている場合） • eth0（trap.registaddress が設定されていない場合） Windows/Linux – • trap.registaddress（設定されている場合） • イベント-マネージャ アルゴリズムに基づくインターフェイス（trap.registaddress が設定されていない場合）	N/A	データ サブネットに属する	Honored
		N/A	データ サブネットに属していない	無視されます。データ プールの別のIPがトラップ IP として使用されます

[2] 設定に違いはありません。対応不要です。

* ***Honored***：設定に違いはありません。対応不要です。

****Ignored***：設定の違いが作成されます。***Web UIの[LAN]-[Fabrics]-[Fabrics]*** で、*[Fabric]*をダブルクリックして***[Fabric Overview]*** を表示します。***[ファブリック アクション（Fabrics Actions）]*** ドロップダウン リストから、***[設定の再計算（Recalculate Config）]*** を選択します。***[設定の展開（Deploy Config）]*** をクリックします。

ファブリック、インターフェイス、およびリンクのテンプレートの変更

Nexusダッシュボード ファブリック コントローラリリース 12.0.1a では、次のファブリック、インターフェイス、およびリンクテンプレート名が変更され、**_11_1** 文字列が削除されています。

ファブリック テンプレート:

- Easy_Fabric.template
- External_Fabric.template
- MSD_Fabric.template

インターフェイス ポリシー テンプレート：

- int_access_host.template
- int_dot1q_トンネル_ホスト。テンプレート
- int_routed_host.template
- int_trunk_host.template
- int_intra_fabric_num_link.template
- int_intra_fabric_unnum_link.template
- int_intra_vpc_peer_keep_alive_link.template
- int_loopback.template
- int_mgmt.template
- int_monitor_ethernet.template
- int_monitor_port_channel.template
- int_nve.template
- int_port_channel_aa_fex.template
- int_port_channel_fex.template
- int_port_channel_access_host.template
- int_port_channel_dot1q_tunnel_host.template
- int_port_channel_trunk_host.template
- int_subif.template
- int_vpc_access_host.template
- int_vpc_dot1q_tunnel.template
- int_vpc_trunk_host.template
- int_vpc_peer_link_po.template

リンク **IFC** テンプレート**:**

- ext_fabric_setup.template
- ext_multisite_underlay_setup.template

設定コンプライアンスの変更

Configuration Compliance（CC）関連のファイルも次のように変更されます。

- 設定コンプライアンスは **内部** NDFC テンプレートになりました。
- DCNM 11.5(x) のパス n ファイルシステム

  `/usr/local/cisco/dcm/dcnm/model-config`

表 *5 : DCNM 11.5* から *NDFC* テンプレート名へのマッピング

DCNM 11.5(x) のテンプレート名	**NDFC 12.0.1a** のテンプレート名 詳細については、『[3]』を参照してください。
compliance_case_insensitive_clis	compliance_case_insensitive_clis
ipv6_clis	compliance_ipv6_clis
strict_cc_exclude_clis	compliance_strict_cc_exclude_clis

[3] Cisco NDFC Fabric Controller Configuration Guide