Cisco Nexus Dashboard Fabric Controller のインストールとアップグレード ガイド、リリース 12.1.3

最終更新：2025 年 4 月 15 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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

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

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

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

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

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

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

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

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

© 2023 Cisco Systems, Inc. All rights reserved.

目 次

第 1 章

概要 1

概要 1

展開オプション 3

Nexus Dashboard Insights を使用した NDFC 管理モードの共同ホスティング 5

導入プロファイルの簡易化 7

クラスタ ノード間のレイヤ 3 到達可能性 8

第 2 章

Nexus Dashboard Fabric Controller のインストール 13

インストール要件とガイドライン 13

App Store を使用した NDFC のインストール 33

NDFC の手動インストール 35

第 3 章

Nexus Dashboard Fabric Controller のアップグレード 39

前提条件と注意事項のアップグレード 39

NDFC リリース 12.1.x からのアップグレード 46

DCNM（Data Center Network Manager）からのアップグレード 49

Cisco DCNM 11.5(4) からのアップグレード後のペルソナと機能の互換性 49

NDFC アップグレード ツールのダウンロード 51

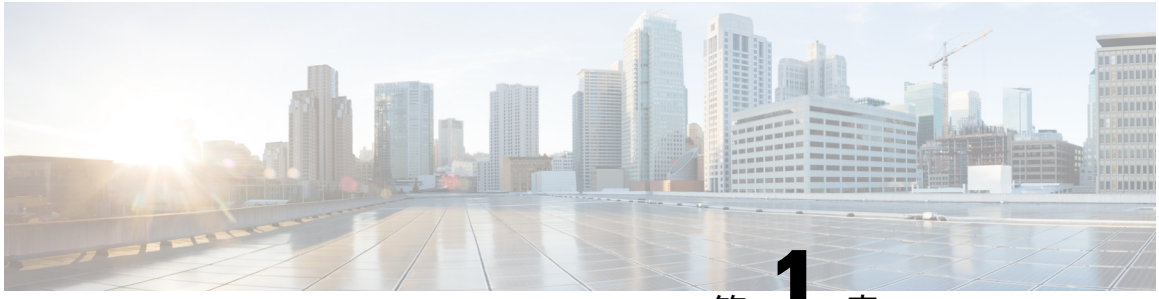
アップグレード ツールを使用した構成のバックアップ 52

Cisco DCNM 11.5（4）から Cisco NDFC リリース 12.1.3 へのアップグレード 57

アップグレード後の作業 60

Feature Manager 63

機能セット全体での変更 63



第 1 章

概要

- 概要 （1 ページ）
- 展開オプション （3 ページ）
- Nexus Dashboard Insights を使用した NDFC 管理モードの共同ホスティング （5 ページ）
- 導入プロファイルの簡易化 （7 ページ）
- クラスタ ノード間のレイヤ 3 到達可能性 （8 ページ）

概要

Cisco Nexus Dashboard Fabric Controller 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 Dashboard Fabric Controller 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 Dashboard Fabric Controller は、VXLAN EVPN、クラシック 3 層、FabricPath、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 NDFC を SAN コントローラとして有効にすると、ストレージ固有の機能と分析機能に重点を置いた 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。

- VXLAN、マルチサイト、クラシックイーサネット、外部ファブリックを含むLANネットワークは、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し、さらに IOS-XR、IOS-XE、隣接ホスト、計算機、仮想マシン、コンテナ管理システムにも対応します。
- 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 オーケストレーション 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 Dashboard Fabric Controlle、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 展開ガイド」を参照してください。

リリース 12 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。事後のインストールでは、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 Dashboard Fabric Controller リリース 12.1.3 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。

（注） Nexus Dashboard の特定のインスタンスでは、1 つのバージョンの NDFC サービスのみがアクティブになります。アクティブな NDFC サービスでは、特定のインスタンスで設定できるペルソナは 1 つだけです。

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機能の選択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。

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 NDFC ではマイクロサービスの展開にクラスタ内の 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。

Cisco NDFC リリース 12.1.2 以降、外部サービス IP アドレスが指定されている Nexus Dashboard 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**無効**にして、NDFC を仮想 Nexus Dashboard（vND）インスタンス上で実行することができます。vND は管理インターフェイスとデータ インターフェイスで構成されていることを思い出してください。デフォルトでは、LAN 展開で、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。同様に、デフォルトでは、SAN 展開で、Nexus Dashboard データ 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。

NDFC リリース 12.1.2 の前に、インバンド管理、エンドポイント ロケーター、または POAP 機能が NDFC で有効になっている場合、Nexus ダッシュボード データまたはファブリック 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した。この設定は、これらの機能が正しく動作するために必須でした。繰り返しますが、前述のように、vND 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はなくなりました。実際、顧客が以前のバージョンから移行している場合は、ND 2.3.1/NDFC 12.1.2 へのアップグレード後にポート グループの無差別モードを無効にすることをお勧めします。

（注）
- 無差別モードの無効化は、Cisco Nexus Dashboard リリース 2.3.1c からサポートされています。
- Nexus Dashboard ノードがデータ ネットワーク上でレイヤー 3 に隣接し、BGP が構成されており、データ インターフェイスを介してファブリック スイッチに到達できる場合は、無差別モードを無効にすることができます。
- Nexus Dashboard インターフェイスが管理およびデータ ネットワーク上でレイヤ 2 に隣接している場合でも、無差別モードを無効にできるようになりました。

（注） VMware ESXi 環境での無差別モードのデフォルト オプションは **[拒否]** です。つまり、無差別モードは無効になっています。

NDFC のこのリリースは、オンプレミス ネットワークとパブリック クラウド ネットワーク間のハイブリッド クラウド接続をサポートします。Cisco Nexus Dashboard Orchestrator を使用すると、NDFC 管理の VXLAN ファブリックとパブリック クラウドに展開された Cloud Application Policy Infrastructure Controller（cAPIC）の間で接続が調整されます。

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

展開オプション

Cisco Nexus Dashboard Fabric Controller では、次の導入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）
  - 実稼働環境用のファブリック ディスカバリ（50 台以下のスイッチ）
  - 実稼働環境用のファブリック コントローラ（50 台以下のスイッチ）
  - 実稼働環境向けのメディア コントローラ モードの IP ファブリックの Fabric Controller
  - 実稼働環境向けの SAN Controller（80 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）
  - ファブリック検出
  - ファブリック コントローラ
  - SAN Insights を使用したまたは使用しない SAN コントローラ
- 5ノード仮想の Nexus Dashboard（vND）クラスタの NDFC（アクティブ-アクティブ HA モード）
  - ファブリック検出
  - ファブリック コントローラ
- 3 ノードの物理 Nexus Dashboard（pND）クラスタでの NDFC（アクティブ-アクティブ HA モード）
  - Fabric Controller ペルソナの Nexus Dashboard Insights および NDFC（NDFC 管理モード）- 3 つの pND ノード（<= スイッチ）
- Red Hat Enterprise Linux（RHEL）上で実行されている Nexus Dashboard の NDFC
  - SAN Insights を使用したまたは使用しない SAN コントローラ
- KVM ハイパーバイザを使用した仮想 Nexus Dashboard（vND）の NDFC

  リリース 12.1.1e 以降、KVM ハイパーバイザを備えた仮想 Nexus Dashboard で、次のペルソナを使用して NDFC を展開できます。
  - Fabric Controller、Fabric Discovery、および SAN Controller のペルソナをサポートします。

Nexus Dashboard Capacity Planning を参照して、それぞれの展開をサポートするスイッチの数を決定します。

3 ノードおよび 5 ノードの展開では、3 つの Nexus Dashboard マスター ノードがあります。5 ノード展開では、追加の 2 つのノードがワーカー ノードとして機能します。3 ノードまたは 5 ノード クラスタ展開はアクティブ/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、そのノードで実行されているマイクロサービスが他のノードに移動します。Nexus Dashboard Fabric Controller は、1 つのノードの障害シナリオで正常に動作します。ただし、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されることが予想されます。サービスの移行が完了した後で、サポートされているスケールは、パフォーマンスが低下してもサポートされ続けます。最適な NDFC パフォーマンスを復元するには、1 つのノードに障害が発生した状態でシステムを実行すること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 ノードまたは 5 ノード クラスタは 2 つのマスター ノードの障害に耐えられず、すべての NDFC サービスが中断されます。

Nexus Dashboard Insights を使用した NDFC 管理モードの共同ホスティング

リリース 12.1.1e 以降、NDFC ファブリック コントローラと Nexus Dashboard Insights を同じ Nexus Dashboard クラスタで管理モードでホストしてファブリックを管理し、 Nexus Dashboard Insights をホストして同じファブリックをモニタリングできます。NDFC リリース 12.0.2f では、ファブリック ディスカバリ モードの NDFC、つまり、同じ Nexus Dashboard クラスタ上の NDI を使用したモニタモードがサポートされていることに注意してください。共同ホスティングには、最大 50 のスイッチの最大規模の 4 つの物理的な Nexus Dashboard ノードが必要でした。この機能は、対応するペアの Nexus Dashboard Insights リリース 12.1.1e を備えた NDFC リリースでもサポートされています。

（注） KVM に展開された Nexus Dashboard は、同じ Nexus Dashboard クラスタでの NDFC と Insights サービスの共同ホスティングをサポートしていません。

（注） 同じ Nexus Dashboard クラスタで NDFC と Insights を共同ホスティングするには、Nexus Dashboard ノードがレイヤ 2 で隣接している必要があります。共同ホスティング導入のためのレイヤ 3 隣接のサポートは、将来のリリースで展開される予定です。

次の表は、Nexus Dashboard とサービスの互換性のあるバージョンを示しています。

[サービス（Services）]	互換性バージョン
Nexusダッシュボード	3.0.1
Nexus Dashboard Insights	6.3.1
Nexusダッシュボードファブリック コントローラ	12.1.3

次の表は、Nexus Dashboard のシステム要件を示しています。

仕様	サポートされるスケール
物理的な Nexus Dashboard ノードの数	3
サポートされるスイッチの数	50
Nexus Dashboard Insights でサポートされるフローの数	1000

同じ Nexus Dashboard への NDFC と NDI のインストール

Cisco NDFC は、同じ Nexus Dashboard で Nexus Dashboard Insights と共同主催できます。

はじめる前に

- 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 展開ガイド.
- 『*Cisco NDFC* インストール ガイド』の「前提条件」に記載されている要件と注意事項を満たしていることを確認してください。
- 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 のプロキシ構成については、*Cisco Nexus Dashboard* ユーザー ガイド 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、『*Cisco NDFC* インストール ガイド』の「サービスの手動インストール」セクション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* ユーザー ガイド の「クラスタの構成」の項を参照してください。

Nexus Dashboard Insights のインストール

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。

NDFC のインストール

『*Cisco NDFC* インストール ガイド』を参照してください。

Nexus Dashboard で NDFC サイトを設定します。Cisco Nexus Dashboard 展開ガイド の「サイトの追加」セクションを参照してください。

NDI のインストール

同じ Nexus Dashboard セットアップで、Nexus Dashboard Insights サービスをインストールします。詳細については、『Cisco Nexus Dashboard Insights 導入ガイド』を参照してください。

インストール後

NDFC と NDI の互換性のあるバージョンを 5 ノードの物理 Nexus ダッシュボードにインストールした後、NDFC をファブリック（LAN）コントローラとして起動します。ファブリックを作成し、NDFC ファブリックでスイッチを検出してインポートします。Nexus Dashboard は、NDFC ファブリックと [サイト（Sites）] ページのリストをエンティティとして自動的に識別します。

（注） Nexus Dashboard サイトマネージャで、各サイトのパスワードを指定する必要があります。

導入プロファイルの簡易化

Nexus Dashboard の展開プロファイルの簡易化は、特定の展開規模に対するサービスの導入準備を合理化し、展開の相互接続を記憶するタスクを軽減することを目的としています。

Cisco Nexus Dashboard リリース 2.2.1 以降、リソース プロファイルの選択は、展開のユースケースに直接関連するいくつかのより直感的なパラメータに削減されました。スイッチやフローの数などのこれらのパラメータは、ファブリックのサイズとユースケースの意図を記述し、クラスタがサービスに必要なリソースをインテリジェントに決定できるようにします。パラメータは**「ネットワーク スケール」**として分類されます。

NDFCは、定義済みのプロファイルセットの中から適切なプロファイルを選択して、スケールに一致させます。

（注） ネットワーク スケール パラメータを変更した後、Nexus Dashboard でサービスを再起動する必要があります。

Cisco Nexus Dashboard でネットワーク スケール パラメータを表示または変更するには、次の手順を実行します。

1. Nexus Dashboard で、**[管理（Admin）]** > **[システム設定（System Settings）]** に移動します。
2. **[ネットワーク スケール（Network Scale）]** タイルで、ネットワーク スケール パラメータを変更するには、**[編集（Edit）]**アイコンをクリックします。
3. **[サイトの数（Number of Sites）]**フィールドに、この Nexus Dashboard クラスタが管理する、展開のサイトの目標数を入力します。
4. **[スイッチの数（Number of Switches）]**フィールドに、展開するスイッチ ノードの目標数を指定します。
5. **[1 秒あたりのフロー（Flows per second）]** フィールドで、LAN/IPFM/SAN-Insights の展開またはNDFC/NDI 共ホストセットアップでサポートされるスケールのサイト全体のフローの目標数を指定します。

リリース12.1.1eから、NDFC の展開プロファイルは、これらの展開プロファイルに対して異なる命名規則を使用します。これは、各プロファイルがサポートするスケールの数値に一致しています。

Nexus Dashboard の新規インストールでは、**ネットワーク スケール**は空です。ネットワーク スケールで1秒あたりのサイト、スイッチ、およびフローの数を定義することをお勧めします。このようなシナリオでは、サービスはクラスタ ノードの数に基づいてデフォルトのプロファイルを選択します。

使用可能なクラスタ コンピューティング キャパシティが必要な **[ネットワーク スケール（Network Scale）]** よりも少ない場合、Cisco NDFC のインストールではエラーが表示されま

す。Nexus Dashboard でネットワーク スケール値を解決し、NDFC のインストールに進む必要があります。エラーメッセージで指定された推奨事項は、是正アクションに関する有用な提案を示すことに注意してください。

Nexus Dashboard は、NDFC でサポートされているスケール値のプロファイル名を割り当てます。検証済みのスケール番号については、『Cisco NDFC 認証済みの拡張性、リリース 12.1.1e』を参照してください。

このリリースアップグレードすると、個々のコンテナが再起動され、新しく生成されたコンテナは新しいリソース要求と制限値で開始されます。

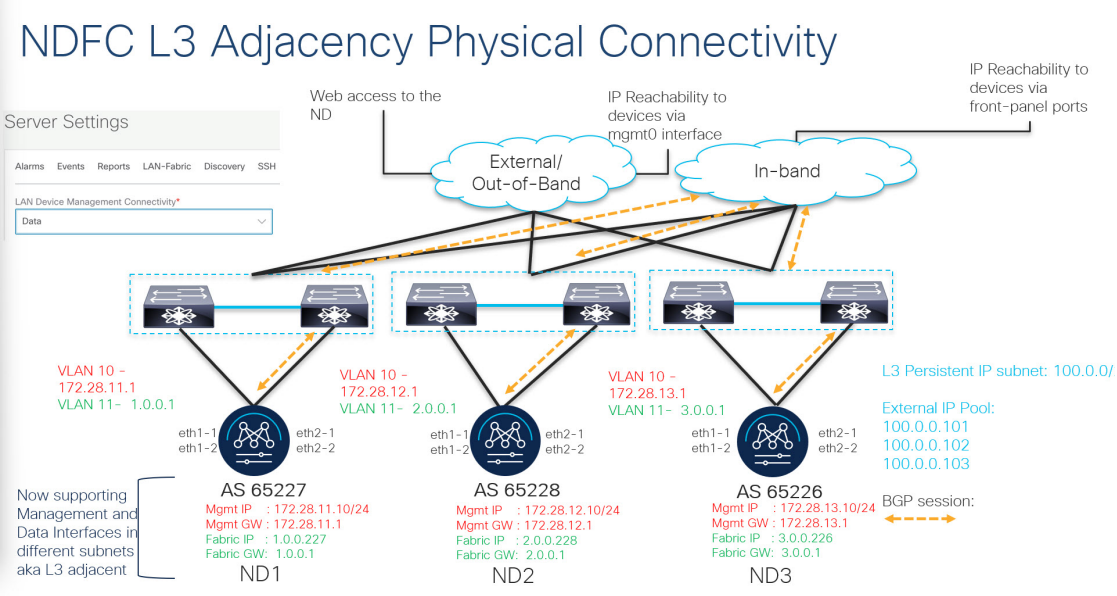
クラスタ ノード間のレイヤ 3 到達可能性

リリース 12.1.1e 以降、NDFC は、レイヤ 3 の隣接ノードを備えた Nexus Dashboard のサービスとして展開できます。サンプルの NDFC レイヤー 3 隣接物理接続トポロジを次の図に示します。

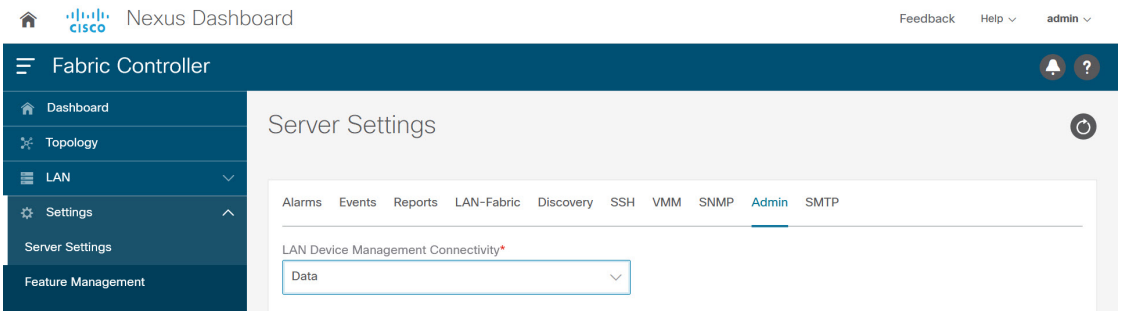
NDFC サービスが実行されている Nexus Dashboard ノード間でレイヤ 3 隣接を使用する場合、永続的な IP アドレスは、Nexus Dashboard データまたはファブリック インターフェイスを使用してアドバタイズされます。レイヤー 3 永続的 IP サブネット プールは一意である必要があり、Nexus Dashboard で BGP を使用してファブリックにアドバタイズされます。永続的 IP を必要とする EPL/SNMP トラップ/SCP などの Cisco NDFC ポッドは、Nexus Dashboard Data Interface のネクストホップで /32 BGP エントリとしてアドバタイズされます。また、Nexus Dashboard ノードとアップリンク スイッチ間の BGP セッションは、直接接続されたリンクを使用して設定する必要があります。

永続的な IP アドレスについては、NDFC の永続的な IP 要件を参照してください。

レイヤー 3 クラスター接続を展開するために、Nexus ダッシュボード ノードは、ノードのデータ ネットワーク ゲートウェイと共に BGP ローカルおよびリモート自律システム構成を使用して、データ インターフェイスを介して隣接ルーターとの eBGP セッションを確立します。Nexus ダッシュボード ノードは、Nexus ダッシュボード クラスタ構成中にセッションを確立するためにゲートウェイ IP を使用するため、隣接する BGP ピアはレイヤ 2 隣接関係である必要があります。レイヤ 2 隣接接続のないピアはサポートされていません。Nexus Dashboard のルートが正しく送信されるようにするには、BGP ネットワークを正しく構成する必要があります。



既存のレイヤ 2 隣接 Nexus Dashboard クラスタからレイヤ 3 隣接クラスタへのアップグレードまたは変更はサポートされていません。レイヤ 3 隣接を使用する場合、NDFC サービスは、スイッチ接続が Nexus Dashboard データ インターフェイスを介している場合にのみサポートされます。NDFC **[UI] > [設定（Settings）] > [管理（Admin）]** タブを選択します。**[LAN デバイス管理接続（LAN Device Management Connectivity）]** ドロップダウン リストから、**[データ（Data）]** を選択します。



Nexus Dashboard は eBGP を使用して、永続的 IP サブネットから取得した外部サービス IP を使用して NDFC 機能に到達するための /32 ルートの最新の到達可能性を公開します。ノードまたはネットワークに障害が発生した場合、回復が完了するまで外部 IP に到達できません（ネットワークがそれ自体を回復できる場合）。障害が発生したノードのマイクロサービスがクラスタ上の既存のノードの 1 つで起動された後、そのノードからの eBGP ピアリングは、対応する /32 永続的 IP 到達可能性をネットワークの残りの部分に自動的にアドバタイズすることによって、サービスの中断を自動修復します。

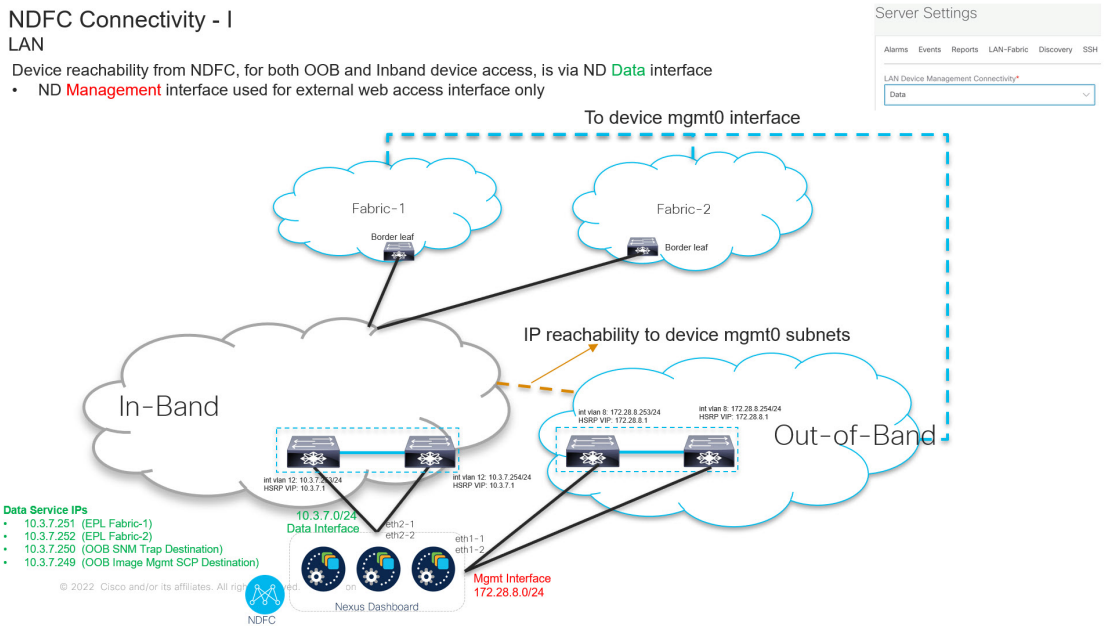
次の表は、レイヤ 3 の隣接するクラスタ ノードの接続に関するさまざまなシナリオに関する情報を提供します。

ネットワークの詳細	サポート提供
レイヤ 2 隣接からレイヤ 3 隣接への変更またはアップグレード	サポートされていません。必要に応じて、クラスタを再度展開する必要があります。
レイヤ 3 隣接からレイヤ 2 隣接への変更またはアップグレード	サポートされていません。必要に応じて、クラスタを再度展開する必要があります。
管理インターフェイスを介したNDFCからスイッチへの接続	サポート対象 （スイッチによって開始されたNDFCへのトラフィックは、データ インターフェイス経由でルーティングされます）
データ インターフェイスを介した NDFC からスイッチへの接続	サポート対象
管理インターフェイス上の Nexus Dashboard BGP トラフィック	未サポート
データ インターフェイスを介した Cisco Nexus Dashboard BGP トラフィック	サポート対象
Nexus Dashboard BGP ピア L2 隣接	サポート対象
Nexus Dashboard BGP ピア L3 隣接	未サポート

詳細については、「*Cisco Nexus Dashboard ユーザー ガイド*」を参照してください。

付録

次の画像は、異なる NDFC 接続を示しています

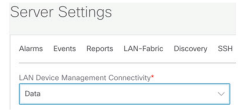


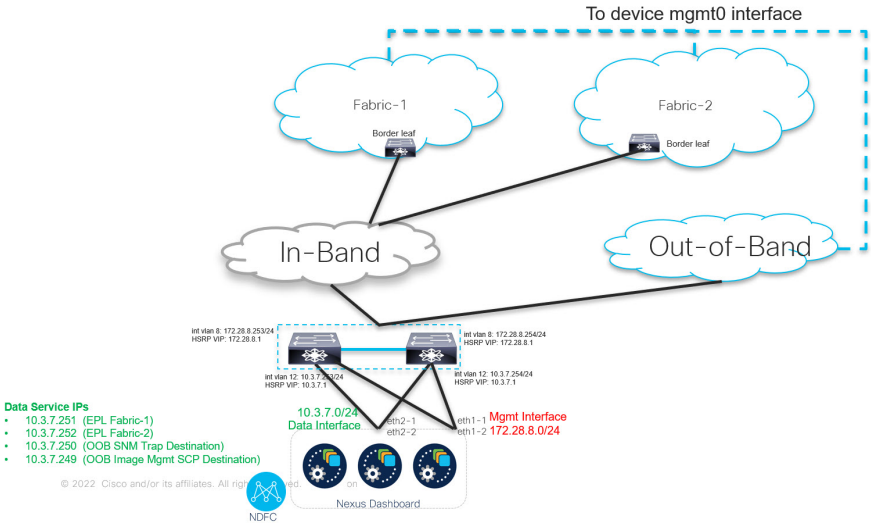
NDFC Connectivity - II

LAN

Device reachability from NDFC, for both OOB and Inband device access, is via ND Data interface

- ND Management interface used for external web access interface only



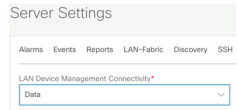


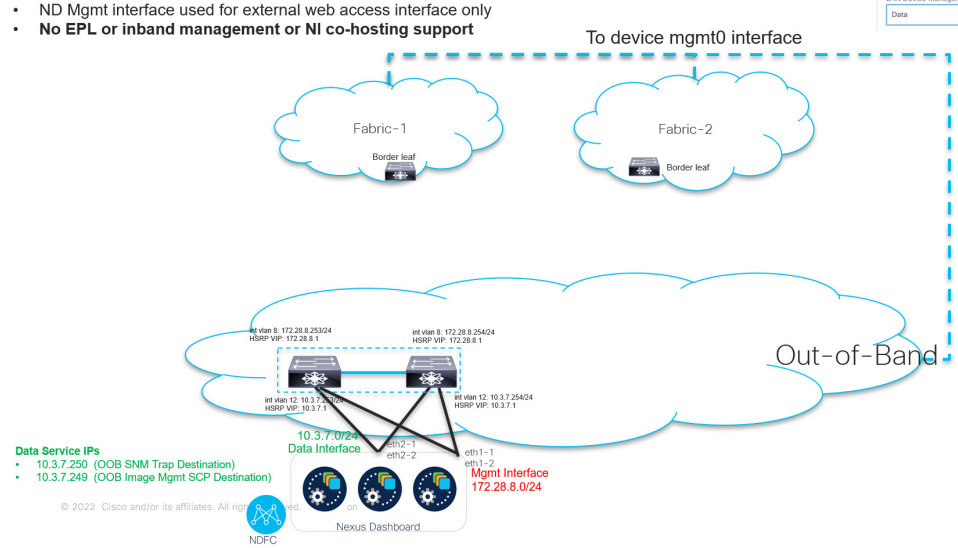
NDFC Connectivity - III

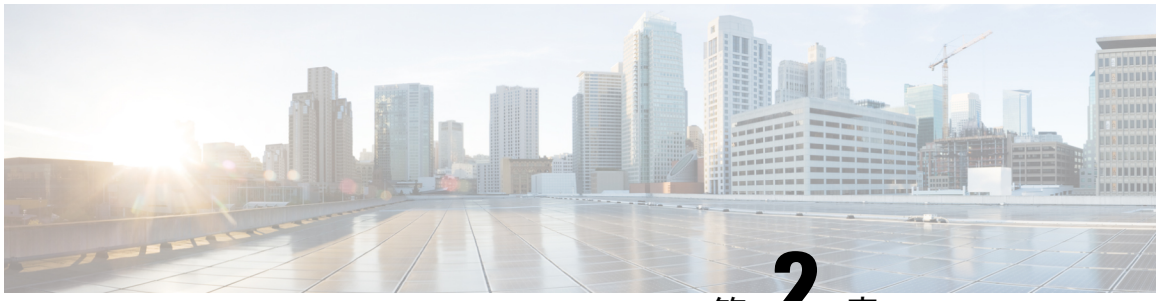
LAN

Device reachability from NDFC for OOB device access is via ND Data interface

- ND Mgmt interface used for external web access interface only
- **No EPL or inband management or NI co-hosting support**







第 2 章

Nexus Dashboard Fabric Controller のインストール

- インストール要件とガイドライン （13 ページ）
- App Store を使用した NDFC のインストール （33 ページ）
- NDFC の手動インストール （35 ページ）

インストール要件とガイドライン

次のセクションでは、Nexus Dashboard Fabric Controller を展開するためのさまざまな要件を説明します。

Network Time Protocol（NTP）

Nexus ダッシュボード ノードは、NTP サーバーと同期している必要があります。ただし、Nexus ダッシュボード ノード間で最大 1 秒の遅延が発生する可能性があります。Nexus ダッシュボード ノード間の遅延が 1 秒以上の場合、NDFC クラスタでの動作が不安定になる可能性があります。

IPv4 および IPv6 のサポート

Nexus Dashboard の以前のリリースでは、クラスタ ノードの純粋な IPv4 構成またはデュアル スタック IPv4/IPv6（管理ネットワークのみ）構成がサポートされていました。リリース 3.0(1) 以降、Nexus Dashboard は、クラスタ ノードおよびサービスの純粋な IPv4、純粋な IPv6、またはデュアル スタック IPv4/IPv6 構成をサポートします。

IP 構成を定義するとき、以下のガイドラインが適用されます。

- クラスタ内のすべてのノードとネットワークは、純粋な IPv4、純粋な IPv6、またはデュアル スタック IPv4/IPv6 のいずれかの均一な IP 構成を持つ必要があります。
- クラスタを純粋な IPv4 モードで展開し、デュアル スタック IPv4/IPv6 または純粋な IPv6 に切り替える場合は、クラスタを再展開する必要があります。
- デュアル スタック構成の場合：

- 外部（データと管理）ネットワークと内部（アプリケーションとサービス）ネットワークの両方がデュアル スタック モードである必要があります。

  IPv4 データ ネットワークやデュアル スタック管理ネットワークなどの部分的な構成はサポートされていません。

- 物理的なサーバーの CIMC にも IPv6 アドレスが必要です。
- ノードの初期起動時にノードの管理ネットワークに IPv4 または IPv6 アドレスを構成できますが、クラスタのブートストラップ ワークフロー中に両方のタイプの IP を指定する必要があります。

  管理 IP は、初めてノードにログインしてクラスタのブートストラップ プロセスを開始するために使用されます。

- すべての内部証明書は、IPv4 と IPv6 の両方のサブジェクト代替名（SAN）を含むように生成されます。
- Kubernetes 内部コア サービスは IPv4 モードで開始されます。
- DNS は、IPv4 と IPv6 の両方にサービスを提供して転送し、両方のタイプのレコードをサーバーに提供します。
- ピア接続用の VxLAN オーバーレイは、データ ネットワークの IPv4 アドレスを使用します。

  IPv4 パケットと IPv6 パケットは両方とも、VxLAN の IPv4 パケット内にカプセル化されます。

- UI は、IPv4 と IPv6 の両方の管理ネットワーク アドレスでアクセスできます。

- 純粋な IPv6 構成の場合：
  - 純粋な IPv6 モードは、物理および仮想フォーム ファクタのみでサポートされます。

    AWS、Azure、または既存の Red Hat Enterprise Linux（RHEL）システムに展開されたクラスタは、純粋な IPv6 モードをサポートしません。

  - ノードを最初に構成するときに、IPv6 管理ネットワーク アドレスを指定する必要があります。

    ノード（物理、仮想、またはクラウド）が起動した後、これらの IP を使用して UI にログインし、クラスタのブートストラップ プロセスを続行します。

  - 前述の内部アプリケーションおよびサービス ネットワークに IPv6 CIDR を提供する必要があります。
  - 前述のデータ ネットワークと管理ネットワークに IPv6 アドレスとゲートウェイを提供する必要があります。
  - すべての内部証明書は、IPv6 サブジェクト代替名 (SAN) を含むように生成されます。
  - すべての内部サービスは IPv6 モードで開始されます。

- ピア接続用の VxLAN オーバーレイは、データ ネットワークの IPv6 アドレスを使用します。

  IPv6 パケットは、VxLAN の IPv6 パケット内にカプセル化されます。

- すべての内部サービスは IPv6 アドレスを使用します。

Nexus Dashboard

ここで説明する追加の要件と Nexus Dashboard Fabric Controller サービスのインストールに進む前に、 *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。

（注） ファブリック コントローラ サービスは、展開されている Nexus ダッシュボード クラスターの 2 つのマスター ノードの障害から回復できません。その結果、Nexus ダッシュボード クラスタに少なくとも 1 つのスタンバイ ノードを維持し、NDFC 設定の定期的なバックアップを作成することをお勧めします。これは、使用しているリリースの *Cisco NDFC-Fabric* コントローラ構成ガイドの**操作 > の バックアップと復元**の章で説明されているとおりです。

Nexus ダッシュボード クラスタの 2 つの マスター ノードに機能不全が発生した場合は、使用しているリリースの *Cisco Nexus* ダッシュボード ユーザー ガイドの「**2 つのマスター ノードをスタンバイ ノードに置き換えるトラブルシューティング**」セクションで説明されている手順に従って、クラスタと NDFC構成を回復できます。

NDFC リリース	Nexus Dashboard の最小リリース
リリース 12.1.3	Cisco Nexus Dashboard リリース 3.0.1

NDFC 展開では、次の Nexus ダッシュボード フォーム ファクターがサポートされています。

- Cisco Nexus Dashboardの物理アプライアンス(.iso)
- VMware ESX (.ova)

  このリリースは、ESXi 7.0 をサポートします。

- Linux KVM (.qcow2)

  このリリースは、CentOS 7.9 および RHEL 8.6 をサポートします。

- 既存の Red Hat Enterprise Linux（SAN コントローラのペルソナのみ）

  このリリースは、Red Hat Enterprise Linux（RHEL）8.6 をサポートします。

Nexus Dashboard クラスタのサイジング

目的のスケールに必要な Nexus ダッシュボード クラスタ ノードの数については、NDFC のリリース固有の検証済み拡張性ガイドを参照してください。

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 Dashboard システム技術情報

Nexus Dashboard 上で NDFC を実行するためのサーバー技術情報要件に関する情報を次の表に示しています。Nexus Dashboard キャパシティプラン を参照して、それぞれの展開をサポートするスイッチの数を決定します。

Cisco Nexus Dashboard は、さまざまなフォーム ファクタを使用して展開できます。NDFC は、次のフォーム ファクタで展開できます：

- pND - 物理 Nexus ダッシュボード
- vND - 仮想 Nexus ダッシュボード
- rND - RHEL Nexus ダッシュボード

表 *1 : Nexus Dashboard* 上で *NDFC* を実行するためのサーバー技術情報要件

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/秒）
ファブリック検出	仮想ノード（vND）：アプリケーション ノード	16 vCPU	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
	物理ノード（pND） （PID: ND-NODE-L4）	2.8GHz AMD CPU	256 GB の RAM	4 x 2.4 TB HDD 960 GB SSD 1.6 TB NVME ドライブ

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/秒）
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 ノード	16 vCPU	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
	物理ノード（pND） （PID: ND-NODE-L4）	2.8GHz AMD CPU	256 GB の RAM	4 x 2.4 TB HDD 960 GB SSD 1.6 TB NVME ドライブ

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/秒）
SAN コントローラ	仮想ノード（vND）：アプリケーション ノード （SAN Insights を使用）	16 vCPU （物理予約と一緒）	64 GB （物理予約と一緒）	550GB SSD
	アプリ ノード（rND） （SAN Insights を使用）	16 vCPU （物理予約と一緒）	64 GB （物理予約と一緒）	550GB SSD
	データ ノード（vND）：データ ノード （SAN Insights を使用）	32 vCPU （物理予約と一緒）	128GB （物理予約と一緒）	3 TB SSD
	データ ノード (rND) （SAN Insights を使用）	32 vCPU （物理予約と一緒）	128 GB （物理予約と一緒）	3 TB 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
	物理ノード（pND） （PID: ND-NODE-L4）	2.8GHz AMD CPU	256 GB の RAM	4 x 2.4 TB HDD 960 GB SSD 1.6 TB NVME ドライブ

Nexus Dashboard システム技術情報

Nexus Dashboard 上で NDFC を実行するためのサーバー技術情報要件に関する情報を次の表に示しています。Nexus Dashboard キャパシティプラン を参照して、それぞれの展開をサポートするスイッチの数を決定します。

Cisco Nexus Dashboard は、さまざまなフォーム ファクタを使用して展開できます。NDFC は、次のフォーム ファクタで展開できます：

- pND - 物理 Nexus ダッシュボード
- vND - 仮想 Nexus ダッシュボード

表 *2 : Nexus Dashboard* 上で *NDFC* を実行するためのサーバー技術情報要件

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/秒）
ファブリック検出	仮想ノード（vND）：アプリケーション ノード	16 vCPU	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
	物理ノード（pND）（PID: ND-NODE-L4）	2.8GHz AMD CPU	256 GB の RAM	4 x 2.4 TB HDD 960 GB SSD 1.6 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 ノード	16 vCPU	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
	物理ノード（pND）（PID: ND-NODE-L4）	2.8GHz AMD CPU	256 GB の RAM	4 x 2.4 TB HDD 960 GB SSD 1.6 TB NVME ドライブ

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/秒）
SAN コントローラ	仮想ノード（vND）：アプリケーション ノード （SAN Insights を使用）	16 vCPU （物理予約と一緒）	64 GB （物理予約と一緒）	550GB SSD
	データ ノード（vND）：データ ノード （SAN Insights を使用）	32 vCPU （物理予約と一緒）	128GB （物理予約と一緒）	3 TB 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
	物理ノード（pND） （PID: ND-NODE-L4）	2.8GHz AMD CPU	256 GB の RAM	4 x 2.4 TB HDD 960 GB SSD 1.6 TB NVME ドライブ

Nexus ダッシュボードのネットワーク

最初に Nexus Dashboard を設定するときは、各ノードで 2 つの Nexus Dashboard 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、通常、ノードのクラスタリングと、物理ネットワークへの North-South 接続に使用されます。管理ネットワークは一般的に、Cisco Nexus Dashboard Web UI、CLI、または API への接続に使用されます。

Nexus Dashboard ファブリック コントローラを有効にする場合、Nexus Dashboard ノードの管理インターフェイスとデータ インターフェイスが異なるために必要なサブネットの数は、リリースに応じて決まります。

- NDFC リリース 12.1.3 より前のリリースでは、Nexus Dashboard ノードの管理インターフェイスとデータ インターフェイスは異なるサブネットに存在する必要があります。外部サービス プールの IP アドレスは、展開のタイプに応じて、特定のサブネット プールから取得される場合があります。

- LAN 展開の場合、これらの外部サービス IP は、構成された設定に応じて、Nexus Dashboard の管理サブネット プールまたはデータ サブネット プールから取得される場合があります。
- SAN 展開の場合、外部サービス IP は Nexus ダッシュボード データ サブネット プールから取得されます。

- NDFC リリース 12.1.3 では、LAN 展開要件は変更されませんが、SAN 展開では同じサブネット内の管理インターフェイスとデータ インターフェイスがサポートされるようになりました。Nexus Dashboardノードの管理インターフェイスとデータ インターフェイスが同じサブネットにある場合、外部サービス プールのIPアドレスも同じ単一のサブネットから取得されます。

  SAN展開でも、以前と同様に個別のサブネットが引き続きサポートされることに注意してください。

Cisco Nexus Dashboard ファブリック コントローラを有効にする場合、Nexus Dashboard ノードの管理インターフェイスとデータインターフェイスは異なるサブネットに存在する必要があります。同じ Nexus Dashboard クラスタに属する異なるノードは、レイヤ 2 隣接またはレイヤ 3 隣接のいずれかにすることができます。詳細については、クラスタ ノード間のレイヤ3到達可能性 （8 ページ）を参照してください。

両方のネットワークで、Nexus Dashboard Orchestrator に対して 50ms を超えないラウンドトリップ時間（RTT）での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 Fabric Controller Deployment Guide*』を参照してください。

Nexus Dashboard Fabric Controller ポート

Nexus Dashboard（ND）クラスタ ノードに必要なポートに加えて、Nexus Dashboard Fabric Controller（NDFC）サービスには次のポートが必要です。

（注） 次のポートは、NDFC サービスからスイッチへの IP 到達可能性を提供するインターフェイスに応じて、Nexus Dashboard 管理ネットワークおよび/またはデータ ネットワーク インターフェイスに適用されます。

表 *3 : Nexus Dashboard Fabric Controller* ポート

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
SSH	22	TCP	発信	SSH は、デバイスにアクセスするための基本的なメカニズムです。
SCP	22	TCP	発信	NDFC バックアップ ファイルをリモート サーバーにアーカイブする SCP クライアント。
SMTP	25	TCP	発信	SMTP ポートは、NDFC の [サーバー設定（Server Settings）] メニューから構成できます。 これはオプションの機能です。
DHCP	67	UDP	入力	NDFC ローカル DHCP サーバーがブートストラップ/POAP 用に構成されている場合。 これは、LAN 展開にのみ適用されます。 （注） POAP の目的でローカル DHCP サーバーとして NDFC を使用する場合、すべての ND マスター ノードの IP を DHCP リレーとして構成する必要があります。ND ノードの管理 IP またはデータ IP が DHCP サーバーにバインドされるかどうかは、NDFC サーバー設定の LAN デバイス管理接続によって決定されます。
DHCP	68	UDP	発信	
SNMP	161	TCP/UDP	アウト	NDFC からデバイスへの SNMP トラフィック。

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
HTTPS/HTTP（NX-API）	443/80	TCP	発信	NX-API HTTPS/HTTP クライアントは、構成可能でもあるポート 443/80 でデバイスの NX-API サーバーに接続します。これは、LAN 展開にのみ適用されます。 NX-API はオプション機能であり、次のような NDFC 機能の限られたセットで使用されます。 • エンドポイント ロケータ（EPL）（「**NX-API 構成での EPL の動作**」を参照） • 「**L4-L7 サービスの注意事項と制限事項**」で説明されているレイヤ 4 ～レイヤ 7 VXLAN、拡張クラシック LAN、eBGP、キャンパス ファブリックなどの適切なファブリックの **[詳細（Advanced）]** タブで NX-API 機能を有効にする必要があります。
HTTPS（vCenter、Kubernetes、OpenStack、Discovery）	443	TCP	発信	NDFC は、VMware vCenter や OpenStack などの登録済み VMM ドメインと、Kubernetes などのコンテナ オーケストレーターから取得した情報を関連付けることにより、統合されたホストおよび物理ネットワーク トポロジ ビューを提供します。 これはオプションの機能です。

（注） 次のポートは、一部の NDFC サービスで使用される永続的 IP とも呼ばれる外部サービス IP に適用されます。これらの外部サービス IP は、構成された設定に応じて、Nexus Dashboard の管理サブネット プールまたはデータ サブネット プールから取得される場合があります。

表 *4 : Nexus Dashboard Fabric Controller* 永続的 *IP* ポート

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
SCP	22	TCP	入力	SCP は、デバイスと NDFC サービス間でファイルを転送するさまざまな機能によって使用されます。NDFC SCP サービスは、ダウンロードとアップロードの両方の SCP サーバーとして機能します。SCP は、POAP 関連ファイルをダウンロードするために、デバイス上の POAP クライアントによっても使用されます。 NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
TFTP（POAP）	69	TCP	入力	POAP 経由のデバイス ゼロタッチ プロビジョニングにのみ使用されます。デバイスは、基本的なインベントリ情報を NDFC に送信して (NDFC への制限付きの書き込み専用アクセス)、セキュアな POAP 通信を開始できます。NDFC ブートストラップまたは POAP は、TFTP または HTTP/HTTPS 用に構成できます。 NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。 これは、LAN 展開にのみ適用されます。

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
HTTP（POAP）	80	TCP	入力	POAP 経由のデバイス ゼロタッチ プロビジョニングにのみ使用されます。デバイスは、基本的なインベントリ情報を NDFC に送信して (NDFC への制限付きの書き込み専用アクセス)、セキュアな POAP 通信を開始できます。NDFC ブートストラップまたは POAP は、TFTP または HTTP/HTTPS 用に構成できます。 NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。 これは、LAN 展開にのみ適用されます。

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
BGP	179	TCP	入力 / 出力	エンドポイント ロケーターの場合、有効になっているファブリックごとに、独自の永続的な IP を使用して EPL サービスが生成されます。このサービスは、常に Nexus Dashboard データ インターフェイスに関連付けられています。エンドポイント情報を追跡するために必要な BGP アップデートを取得するために、ファブリック上の適切な BGP エンティティ（通常は BGP ルート リフレクタ）と NDFC EPL サービスはピアを行います。 この機能は、VXLAN BGP EVPN ファブリックの展開にのみ適用されます。 これは、LAN 展開にのみ適用されます。
HTTPS（POAP）	443	TCP	入力	セキュア POAP は、ポート 443 の NDFC HTTPS サーバーを介して実現されます。HTTPS サーバーは SCP-POAP サービスにバインドされ、そのポッドに割り当てられたのと同じ永続的 IP を使用します。 NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。 これは、LAN 展開にのみ適用されます。

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
Syslog	514	UDP	入力	NDFC が Syslog サーバーとして構成されている場合、デバイスからの Syslog は、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的な IP に向けて送信されます。 NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。
SCP	2022	TCP	発信	NDFC POAP-SCP ポッドの永続的な IP から、Nexus Dashboard Insights を実行している別の ND クラスターにテクニカル サポート ファイルを転送します。 NDFC の SCP-POAP サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の LAN デバイス管理接続設定によって制御されます。

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続 （特に明記されていない限り、**LAN** と **SAN** の両方の展開に適用されます）
SNMP トラップ	2162	UDP	入力	デバイスから NDFC への SNMP トラップは、SNMP-Trap/Syslog サービス ポッドに関連付けられた永続的な IP に向けて送信されます。 NDFC の SNMP-Trap-Syslog サービスには、管理サブネットまたはデータ サブネットのいずれかに関連付けられた永続的な IP があります。これは、NDFC サーバー設定の [LAN デバイス管理接続（LAN Device Management Connectivity）] 設定によって制御されます。
GRPC（テレメトリ）	33000	TCP	入力	NDFC 永続的 IP に関連付けられた GRPC トランスポートを介して SAN データ (ストレージ、ホスト、フローなど) を受信する SAN Insights Telemetry サーバー。 これは、SAN 展開でのみ有効です。
GRPC（テレメトリ）	50051	TCP	入力	メディア展開用の IP ファブリックおよび一般的な LAN 展開用の PTP のマルチキャスト フローに関連する情報は、ソフトウェアテレメトリを介して、NDFC GRPC レシーバー サービス ポッドに関連付けられた永続的 IP にストリーミングされます。 これは、LAN およびメディア展開でのみ有効です。

NDFC 遅延要件

Cisco Nexus Dashboard Fabric Controller 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。遅延に関する詳細は、『*Nexus Dashboard Fabric Controller Deployment Guide*』を参照してください。

NDFC ネットワーク接続

- **ローカル エリア ネットワーク（LAN） デバイス管理接続** – ファブリック ディスカバリおよびファブリック コントローラ機能は、ND クラスタ アプライアンスの管理ネットワークとデータ ネットワークの両方を介してデバイスを管理できます。
- 管理ネットワークを使用する場合は、NDFC が管理ネットワークで管理またはモニタリングする必要があるデバイスのすべてのサブネットへのルートを追加します。
- データ ネットワークを使用する場合、タッチレス デイ 0 デバイスの起動に NDFC で事前にパッケージ化された DHCP サーバーを使用する場合、POAP が有効になっているすべてのデバイスのすべてのサブネットへのルートを追加します。
- SAN コントローラ ペルソナでは、すべてのデバイスが Nexus ダッシュボード クラスタ ノードのデータ ネットワーク経由で到達可能である必要があります。

NDFC 永続 IP アドレス

- Nexus ダッシュボード クラスタがネットワークのレイヤ 3 分離を介して展開されている場合は、すべての ND ノードで BGP を構成する必要があります。
- すべての永続 IP は、Nexus ダッシュボード ノードのサブネットの一部にならないように構成する必要があります。これは、ローカル エリア ネットワーク（LAN）デバイス管理接続がデータである場合にのみサポートされます。これは、Nexus ダッシュボードインサイトと NDFC を共同ホストするクラスタではサポートされていません。
- Nexus ダッシュボード クラスターが同じサブネット内のすべてのノードで展開されている場合、永続的な IP は同じサブネットからのものとして構成できます。

  この場合、永続的な IP は、NDFC サーバー設定のローカル エリア ネットワーク（LAN）デバイス管理接続設定に基づいて選択されたネットワークに属している必要があります。

  詳細については、NDFC の永続的な IP 要件を参照してください。

（注） このリリースでは、純粋な IPv4、純粋な IPv6、またはデュアル スタック IPv4/IPv6 で NDFC がサポートされているため、次の永続 IP 要件は IP ファミリごとにあります。

たとえば、デュアル スタック モードで展開しており、次の表に管理ネットワークに 2 つの IP アドレスが必要であると記載されている場合、これは 2 つの IPv4 アドレスと 2 つの IPv6 アドレスを意味します。

管理インターフェイス	データ インターフェイス	永続的 IP
レイヤ 2 隣接	レイヤ 2 隣接	LAN 展開タイプで [**LAN デバイス管理の接続性（LAN Device Management Connectivity）**] が [管理（Management）]（デフォルト）に設定されたレイヤー 2 モードで動作している場合 • SNMP/Syslog および SCP サービス用の管理ネットワーク内の 2 つの IP • [**EPL**] が有効になっている場合、各ファブリックのデータネットワークに 1 つの追加 IP • [**メディア用の IP ファブリック（IP Fabric for Media**）] が有効になっている場合、テレメトリ用の管理ネットワークに 1 つの追加の IP LAN 展開タイプで [**LAN デバイス管理の接続性（LAN Device Management Connectivity**）] が [データ（Data）]（デフォルト）に設定されたレイヤー 2 モードで動作している場合 • SNMP/Syslog および SCP サービス用のデータネットワーク内の 2 つの IP • [**EPL**] が有効になっている場合、各ファブリックのデータネットワークに 1 つの追加 IP • [**メディア用の IP ファブリック（IP Fabric for Media**）] が有効になっている場合、テレメトリ用のデータネットワークに 1 つの追加の IP SAN Controller 展開タイプの場合： • SSH 用の 1 つの IP • SNMP/Syslog 用の 1 つの IP • SAN Insights の機能に対して、Nexus Dashboard クラスタ ノードごとに 1 つの IP

管理インターフェイス	データ インターフェイス	永続的 IP
レイヤ 3 隣接	レイヤ 3 隣接	LAN 展開タイプのレイヤ 3 モードで動作している場合： • [**LAN デバイス管理の接続性（LAN Device Management Connectivity**）] が [データ（Data）] に設定されている必要があります • SNMP/Syslog および SCP サービス用の 2 つの IP • [**EPL**] が有効になっている場合、各ファブリックのデータネットワークに 1 つの追加 IP • すべての永続的 IP は、管理サブネットまたはデータ サブネットと重複していない別のプールの一部である必要があります。 永続的 IP のレイヤ 3 モードの詳細については、ユーザー ガイドの「永続的 IP」のセクションを参照してください。 SAN Controller 展開タイプの場合： • SSH 用の 1 つの IP • SNMP/Syslog 用の 1 つの IP • SAN Insights の機能に対して、Nexus Dashboard クラスタ ノードごとに 1 つの IP メディア用の IP ファブリックはレイヤ 3 モードではサポートされていません

POAP 関連の要件

- デバイスは POAP をサポートしている必要があります。
- デバイスにスタートアップ構成がない必要があります。または、スタートアップ構成をバイパスして POAP モードに入るように **boot poap enable** コマンドを設定する必要があります。
- 範囲が定義された DHCP サーバー。POAP の場合、事前にパッケージ化された NDFC DHCP サーバーまたは外部 DHCP サーバーを使用できます。
- POAP スクリプトとデバイスの構成ファイルを格納するスクリプト サーバーにアクセスできる必要があります。

- ソフトウェアおよびイメージ リポジトリ サーバーを使用して、デバイスのソフトウェア イメージを保存する必要があります。

Web ブラウザの互換性

Cisco Nexus Dashboard Fabric Controller GUI は、次の Web ブラウザでサポートされています。

- Google Chromeバージョン101.0.4951.64
- Microsoft Edge バージョン 101.0.1210.47（64 ビット）
- Mozilla Firefox バージョン 100.0.1（64 ビット）

その他のサポート対象のソフトウェア

次の表に、Cisco Nexus Dashboard Fabric Controller リリース 12.1.3 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 Client：TLS 1、1.1、1.2 および 1.3 を使用した HTTPS

App Store を使用した NDFC 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 リリース 12.1.3 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 展開ガイド.
- Cisco DC App Center は、直接管理ネットワークを介して、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 のプロキシ構成については、*Cisco Nexus Dashboard ユーザー ガイド* 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、NDFC の手動インストール （35 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 ユーザー ガイド* 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 リリース 12.1.3 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 **[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 6 **[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 Dashboard ユーザー ガイド* の「*Cluster Configuration*」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 7 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 8 **[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。

NDFC の手動インストール

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 コントローラリリース 12.1.3 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 展開ガイド.
- 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* ユーザー ガイド 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 12.1.3 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 **[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 10 **[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 Dashboard ユーザー ガイド* の「*Cluster Configuration*」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。

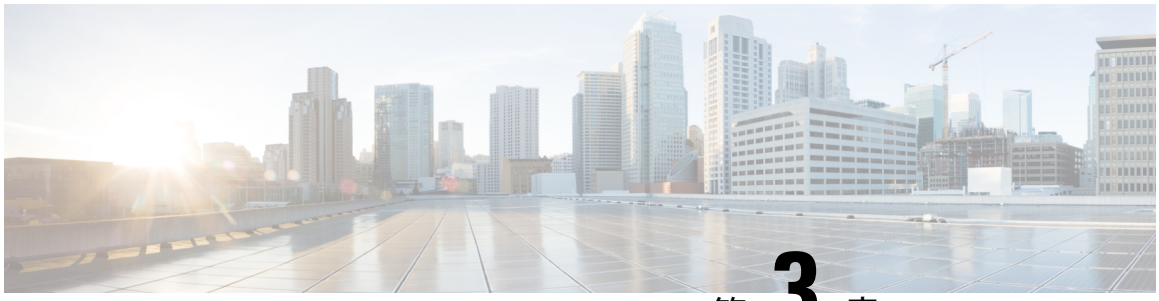
ステップ 11 要件に基づいて、展開を選択します。

[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 12 **[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 3 章

Nexus Dashboard Fabric Controller のアップグレード

- 前提条件と注意事項のアップグレード （39 ページ）
- NDFC リリース 12.1.x からのアップグレード （46 ページ）
- DCNM（Data Center Network Manager）からのアップグレード （49 ページ）

前提条件と注意事項のアップグレード

次のセクション では、既存の Nexus Dashboard Fabric Controller （NDFC）または以前の DCNM ソフトウェアをこのリリースにアップグレードするためのさまざまな要件について説明します。

- 現在の Nexus ダッシュボードクラスタが正常であることを確認します。

  Nexus ダッシュボードの**管理コンソール（Admin Console）**の **[概要（Overview）]** ページでシステムのステータスを確認するか、`rescue-user` としてノードの1つにログインし、`acs health` コマンドを実行して `All components are healthy` が返ってくることを確認します。

- VMware ESX に展開された仮想 Nexus Dashboard クラスタをアップグレードする場合は、ESX のバージョンがターゲット リリースで引き続きサポートされていることを確認します。

（注） ESX サーバーをアップグレードする必要がある場合は、Nexus Dashboard をターゲット リリースにアップグレードする前に行う必要があります。

1. 既存の Nexus Dashboard ノード VM を実行している場合に通常行うように、ESX ホストの 1 つをアップグレードします。
2. ホストがアップグレードされた後、Nexus Dashboard クラスタが正常に動作していることを確認します。
3. 他の ESX ホストで 1 つずつアップグレードを繰り返します。
4. すべての ESX ホストがアップグレードされ、既存の Nexus Dashboard クラスタが正常な状態になったら、次のセクションの説明に従って、Nexus Dashboard をターゲット リリースにアップグレードします。

- リリース 12.1.1 からアップグレードする場合は、既存のすべてのスイッチで VRF が正しく設定されていることを確認します。

  詳細情報とコンテキストについては、以下の 既存のスイッチでの VRF の検出 （43 ページ） セクションを参照してください。

- DCNM リリース 11.5.4 からアップグレードするときに NDFC 構成のバックアップを作成してから、NDFC の別のリリース（NDFC 12.1.3 など）で復元すると、初期セットアップ中の状況によっては、「範囲が使い果たされたため、VLAN またはループバック ID/IP の割り当てに失敗しました」などのエラーメッセージが表示されることがあります。これは、複数のネットワークまたは VRF またはネットワークと VRF の組み合わせに同じデフォルト VLAN が指定されていて、同じスイッチに接続されている場合に発生することがあります。これにより、2 番目に接続されたエンティティのデフォルト VLAN が -1 に設定されます。この問題を解決するには、そのスイッチで使用するオーバーライド VLAN を指定する必要があります。

- アップグレードを続行する前に、データを保護し、潜在的なリスクを最小限に抑えるために、アップグレードの前に Nexus Dashboard と Nexus Dashboard Fabric Controller の構成バックアップを実行する必要があります。

- DCNM リリース 11.5.4 からアップグレードする場合、DCNM で使用される `trap-ip` は Nexus Dashboard 管理 IP またはデータ IP アドレスであってはなりません。代わりに、IP を Nexus Dashboard の永続 IP アドレス プールで構成する必要があります。

  詳細については、「*Nexus Dashboard* インフラストラクチャの管理」の「永続 IP の構成」の項を参照してください。

- すべてのプレビュー/ベータ機能を無効にし、関連するデータを削除する必要があります。

  [設定（Settings）] > [機能管理（Feature Management）] ページで、すべてのベータ機能を無効にします。

[設定（Settings）] > **[サーバ設定（Server Settings）]** > **[LAN ファブリック（LAN Fabric）]** ページで、**[プレビュー機能の有効化（Enable Preview Features）]** が無効になっていることを確認します。

（注） ベータ機能を無効にしても、作成された構成は削除されません。たとえば、ECL プレビュー機能を有効にして、ECL ファブリックを作成/検出した場合、この機能を無効にしても、既存の構成は削除されません。この場合、機能を無効にすることに加えて、アップグレードの前に構成を削除する必要もあります。

- Nexus Dashboard から、現在有効になっているバージョンを除くすべての NDFC バージョンを削除したことを確認します。

  アップグレード中に同じクラスタに複数の NDFC リリース イメージを共存させてはなりません。次のリリースにアップグレードする前に、Nexus Dashboard の **[サービス（Services）]** ページに移動し、NDFC サービス タイルの **[...]** メニューをクリックして、**[バージョン（Versions）]** を選択してすべての非アクティブなバージョンを削除します。

- Nexus Dashboard でファブリック コントローラ サービスに十分な外部 IP アドレスが構成されていることを確認します。

  IP が別のサービスによって消費されている場合など、使用可能な IP が不足している場合、NDFC サービスは開始できません。

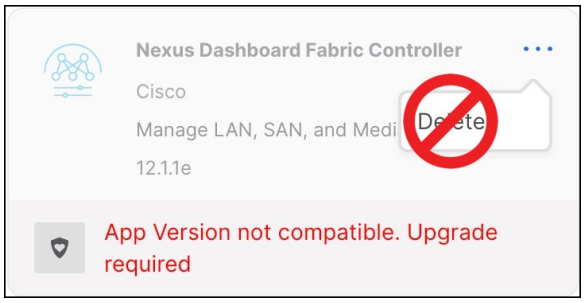
- Nexus Dashboard リリース 2.2(1) またはそれ以降を実行して、リリース 3.0(1) に直接アップグレードする必要があります。

（注） NDFC リリース 12.0.2 以前からアップグレードする場合、直接アップグレードはサポートされません。最初にリリース 12.1.1 にアップグレードしてから、リリース 12.1.3 にアップグレードする必要があります。詳細については、下のアップグレードワークフローの表を参照してください。

- リリース 3.0(1) 以降にアップグレードする前に、クラスタで実行されているすべてのサービスを無効にする必要があります。

（注） Nexus Dashboard をリリース 3.0(1) にアップグレードした後は、Nexus Dashboard のアップグレード前に無効にした既存の NDFC バージョンを再度有効にしないでください。

また、サービスの既存のバージョンを削除しないでください。互換性のない アプリ バージョンが表示される場合があります。アップグレードが必要です。エラー：



- アップグレードが進行中にワーカーまたはスタンバイ ノードを追加するなど、設定変更がクラスタに対して行われていないことを確認します。
- Nexus Dashboard および Nexus Dashboard Fabric Controller では、ソフトウェアのダウングレードをサポートしていません。

  以前のリリースにダウングレードするには、新しいクラスタを展開してサービスを再インストールする必要があります。
- 基盤となるサードパーティ ソフトウェアを個別にアップグレードしないことを推奨します。必要なソフトウェア コンポーネントはすべて、インライン アップグレード手順で更新されます。Nexus Dashboard Fabric Controller 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。

既存のスイッチでの VRF の検出

（注） 次の情報は、リリース 12.1.1 からの NDFC アップグレードに適用されます。リリース 12.1.2 からアップグレードする場合は、このサブセクションをスキップできます。

NDFC から スイッチへの到達可能性は、Nexus Dashboard クラスタのルート構成によって制御されます。デフォルトでは、すべての NDFC ポッドのデフォルトゲートウェイが Nexus Dashboard のデータ インターフェイス ゲートウェイに設定されています。ただし、永続的な IP（外部サービス IP）を持つポッドの場合、デフォルト ゲートウェイは、永続的な IP プールに関連付けられた特定の管理またはデータ インターフェイスに基づいて設定されます。

- ポッドが管理サブネットからの外部サービス IP を使用している場合、そのデフォルトゲートウェイは Nexus Dashboard の管理インターフェイスゲートウェイに設定されます。
- ポッドがデータ サブネット プールからの外部サービス IP を使用している場合、そのデフォルト ゲートウェイは Nexus Dashboard のデータ インターフェイスゲートウェイに設定されます。

NDFC の検出ポッドはスイッチへの IP 到達可能性を必要とし、永続的な IP がないため、ポッドのスイッチへの到達可能性は、スイッチから NDFC サービスをホストしている Nexus Dashboard クラスタへのルーティングがどのように構成されているかによって異なります。ただし、ポッドの操作の中には、スイッチから NDFC への逆到達可能性が必要なものもあります。たとえば、NDFC がスイッチのトラップ ホスト宛先として設定されている場合、そのスイッチの NDFC syslog-trap 外部サービス IP 構成に加えて、この IP に到達可能な VRF を指定する必要があります。同様に、スイッチが SCP コピー コマンドを実行してイメージ管理目的でイメージをコピーする場合、スイッチが SCP の宛先 IP（NDFC の poap-scp ポッドに関連付けられた外部サービス IP）に到達するように VRF を指定する必要があります。その結果、すべてのスイッチについて、スイッチから NDFC への接続に使用できる VRF を関連付ける必要があります。

NDFC の **[LAN デバイス管理接続（LAN Device Management Connectivity）]** が `[管理（Management）]`（デフォルト設定）に設定されている場合、POAP-SCP および SNMP-Trap ポッドは管理外部サービス IP プールから永続的な IP を取得します。この場合、スイッチの `mgmt0` IP アドレスを使用して NDFC にスイッチをインポートする必要があります。これは、Nexus Dashboard の管理インターフェイスを介して NDFC から到達可能である必要があります。レイヤ3経由で到達可能なスイッチの場合、これには、Nexus Dashboard の **[管理（Administration）]** > **[システム設定（System Settings）]** > **[ルート（ Routes）]** > **[管理ネットワーク ルート（Management Network Routes）]**（以前は、**[インフラストラクチ ャ（Infrastructure）** > **] [クラスタ構成（Cluster Configuration）]**）でスタティック ルートを構成する必要があります。これらのスイッチの場合、スイッチに関連付けられている VRF は管理に設定されます。

一方、NDFC の **[LAN デバイス管理の接続性（LAN Device Management Connectivity）]** が `[データ（Data）]` に設定されている場合、POAP-SCP および SNMP-Trap ポッドはデータ外部サービス IP プールから永続的な IP を取得し、Nexus Dashboard データ インターフェイスを介して到達可能になります。この場合、VRF がスイッチに適切に入力されるように、**[LAN デバイス管理の接続性がデータに設定されている場合は、LAN 検出に常に VRF をすべての Nexus スイッチに**

入力させる（**When LAN Device Management Connectivity is set to Data, rely on LAN discovery to always populate VRF for all Nexus Switches**）] オプションを有効にする必要があります 。

NDFC リリース 12.1.1 では、上記のオプションはデフォルトで無効になっていました。つまり、NDFC にインポートされたスイッチの VRF は「デフォルト」に設定されていました。この場合、前面パネルのインターフェイスを介してスイッチから NDFC への到達可能性を有効にするか、POAP-SCP および SNMP-Trap ポッドに関連付けられた永続的な IP が到達可能になるように、スイッチの検出 VRF を更新する必要がありました。ただし、イメージ管理またはトラップ関連機能を使用せず、スイッチから NDFC への到達可能性を有効にしていない場合、NDFC とスイッチ間の通信が継続されるため、Nexus Dashboard の管理またはデータ インターフェイスのいずれかを介して機能し続けるため、スイッチから NDFC への逆方向通信が機能していないことに気づきません。

リリース 12.1.2 以降、**[LAN デバイス管理の接続性がデータに設定されている場合は、LAN 検出に常に VRF をすべての Nexus スイッチに入力させる（When LAN Device Management Connectivity is set to Data, rely on LAN discovery to always populate VRF for all Nexus Switches）]** オプションがデフォルトで有効になります。したがって、NDFC はスイッチ検出中にスイッチ構成から検出 VRF を適切に入力します。

デフォルト設定の変更の結果として、リリース 12.1.1 からアップグレードする場合、VRF がスイッチで設定されていないという問題が発生する可能性があり、GUI または API を使用して VRF を手動で更新して、。既存のスイッチを NDFC に適切な到達可能性を確立する必要があります既存のスイッチの VRF をすでに明示的に構成している場合は、アップグレード中に保持されますが、VRF が現在「デフォルト」に設定されているスイッチは、スイッチが削除され再追加しない限り、**[LAN デバイス管理の接続性がデータに設定されている場合は、LAN 検出に常に VRF をすべての Nexus スイッチに入力させる（When LAN Device Management Connectivity is set to Data, rely on LAN discovery to always populate VRF for all Nexus Switches）]** 設定のデフォルト値の変更に関係なく更新されません。

アップグレード ワークフローの概要

次の表は、現在の NDFC リリースからリリース 12.1.3 にアップグレードするために必要なアップグレード ワークフローをまとめたものです。

現在のリリース	現在のリリースでの Nexus Dashboard バージョン	リリース 12.1.3 にアップグレードする場合のアップグレード ワークフロー
12.1.2	2.3.x	1. **[操作（Operations）] > [バックアップと復元（Backup and Restore）]** ページから構成バックアップを作成します。 2. **[Nexus Dashboard]** で **[Nexus Dashboard ファブリックコントローラ（Nexus Dashboard Fabric Controller）]** サービスを無効にする 3. **Nexus Dashboard** をリリース 3.0.1 にアップグレードします。 4. **NDFC** サービスをリリース 12.1.3 にアップグレードします。 詳細な手順については、NDFC リリース 12.1.x からのアップグレード （46 ページ）を参照してください。
12.1.1e	2.2.x	1. **[操作（Operations）] > [バックアップと復元（Backup and Restore）]** ページから構成バックアップを作成します。 2. **[Nexus Dashboard]** で **[Nexus Dashboard ファブリックコントローラ（Nexus Dashboard Fabric Controller）]** サービスを無効にする 3. **Nexus Dashboard** をリリース 3.0.1 にアップグレードします。 4. **NDFC** サービスをリリース 12.1.3 にアップグレードします。 詳細な手順については、NDFC リリース 12.1.x からのアップグレード （46 ページ）を参照してください。
12.0.2f	2.1.2d	直接アップグレードはサポートされていません。 このドキュメントに戻ってリリース 12.1.3 にアップグレードする前に、『*Nexus Dashboard Fabric Controller のインストールとアップグレードガイド、リリース 12.1.2e*』で説明されているように、NDFC をリリース 12.1.2 にアップグレードすることをお勧めします。

現在のリリース	現在のリリースでの Nexus Dashboard バージョン	リリース 12.1.3 にアップグレードする場合のアップグレード ワークフロー
12.0.1a	2.1.1e	直接アップグレードはサポートされていません。 このドキュメントに戻ってリリース 12.1.3 にアップグレードする前に、『*Nexus Dashboard Fabric Controller のインストールとアップグレードガイド、リリース 12.1.2e*』で説明されているように、NDFC をリリース 12.1.2 にアップグレードすることをお勧めします。
11.5(4)	該当なし	1. **DCNM_To_NDFC_Upgrade_Tool_OVA_ISO** を使用してバックアップする 2. **Nexus Dashboard** バージョン 3.0.1 のインストール 3. **[NDFC]** リリース 12.1.3 のインストール 4. **[Web UI] > [操作（Operations）] > [バックアップと復元（Backup & Restore）]** での復元 詳細な手順については、DCNM（Data Center Network Manager）からのアップグレード （49 ページ）を参照してください。

NDFC リリース 12.1.x からのアップグレード

次の手順では、リリース 12.1.x からリリース 12.1.3 にアップグレードする方法について説明します。

始める前に

次の条件が満たされていることを確認します。

- 前提条件と注意事項のアップグレード （39 ページ） の説明に従って、アップグレード ワークフローを理解し、前提条件を満たしていること。

手順

ステップ 1 既存の設定をバックアップします。

通常の方法で、**[操作（Operations）]>[バックアップと復元（Backup & Restore）]** ページからバックアップできます。

ローカルでバックアップを取る場合、必要に応じて後で使用するためにコピーをダウンロードして保存します。リモートでバックアップする場合、セキュアなリモートの場所にバックアップ ファイルを保存します。

バックアップの詳細については、『*Cisco NDFC* 構成ガイド』の「バックアップと復元」章を参照してください。

ステップ 2 既存の NDFC サービスを無効にします。

サービスを無効にするには、Nexus Dashboard の **[サービス（Services）]** ページに移動し、NDFC タイルのアクション メニュー（**...**）から **[無効化（Disable）]** を選択します。

ステップ 3 Nexus Dashboard をリリース 3.0.1 にアップグレードします。

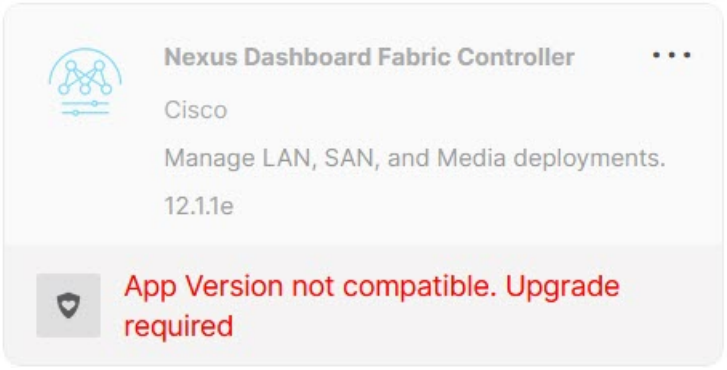
（注）
Nexus Dashboard のアップグレードを開始する前に、前のステップで説明したように、NDFC サービスが無効になっていることを確認してください。

追加の前提条件と注意事項を含む、Nexus Dashboard のアップグレードの詳細については、『*Nexus Dashboard* 展開ガイド』を参照してください。

ステップ 4 Nexus Dashboard のアップグレードが完了したら、ND UI の **[サービス（Services）]** ページに移動します。

（注）
NDFC の現在のバージョンを再有効化または削除してはなりません。メッセージを無視して、次のステップに進みます。

この時点で、NDFC サービス タイルに次のエラーが表示されます。



ステップ 5 Cisco App Store を使用して NDFC サービスをアップグレードします。

（注）
App Storeでは、サービスの最新バージョンにのみアップグレードできます。このリリースにアップグレードするときに、より新しいリリースが App Store で入手可能な場合は、このステップをスキップし、次のステップの説明に従って新しいサービスイメージを手動でアップロードする必要があります。

a) **[Nexus Dashboard] > [サービス（Services）]** ページに移動します。

b) **[App Store]** タブを選択します。
c) App Store の NDFC タイルで、**[更新（Update）]**をクリックします。
d) **ライセンス契約**に同意します。

これにより、NDFC イメージのダウンロードとインストールが開始されます。

e) **[インストール済みサービス（Installed Services）**] タブを選択し、イメージがダウンロードされてインストールされるまで待ちます。

ステップ 6 イメージを手動でアップロードして NDFC サービスをアップグレードします。

（注）
上記のように、すでに App Store を使用してアップグレードしている場合は、このステップをスキップしてください。

新しいリリースのイメージを手動でアップロードすることで、サービスをアップグレードすることを選択できます。

a) アップグレード イメージを入手します。

このリリースのイメージは、Cisco App Center からダウンロードできます。

オプションで、環境内の Web サーバでイメージをホストするように選択できます。イメージをNexus Dashboard クラスタにアップロードする場合、イメージに直接URLを指定するオプションがあります。

b) **[Nexus Dashboard] > [サービス（Services）]** ページに移動します。
c) **[インストール済みサービス (Installed Services)]** タブを選択します。
d) **[アクション（Actions）]** メニューから、**[サービスのアップロード（Upload Service）]** を選択します。
e) 前のサブステップでダウンロードした画像を選択し、**[アップロード（Upload）]**をクリックします。

環境内のサーバでイメージをホストしている場合は、ローカルマシンからイメージをアップロードするか、完全な URL を提供するかを選択できます。

f) イメージがアップロードされ初期化されるまで待ちます。

サービスがすべてのノードに複製され完全に展開されるまでには、最大30分かかります。

ステップ 7 新しいイメージを有効にします。

a) **[Nexus Dashboard Fabric Controller]** タイルで、アクションメニュー（**...**）をクリックし、**[利用可能なバージョン（Available Versions）]**を選択します。
b) 12.1.3 バージョンの横にある **[有効（Enable）]** をクリックします。

（注）
アップグレードが完了する前にサービスのデータが失われる可能性があるため、この時点では以前のバージョンを削除しないでください。

ステップ 8 アップグレード プロセスが完了するまで待ちます。

プロセスが完了すると、NDFC のタイルの **[開く（Open）**] ボタンが使用可能になります。

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 9 **[開く（Open）]** をクリックして、Nexus Dashboard Fablic Controller リリース 12.1.3 UI を起動します。

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ログイン情報を使用してアプリケーションにログインできます。

注意
アップグレード後は以前のNDFCイメージを削除しないでください。これは、クラスタが再起動した場合にサービスの中断が発生する可能性があります。Cisco TAC に連絡して、この問題に関するサポートを受けてください。

DCNM（Data Center Network Manager）からのアップグレード

次のセクションには、ソフトウェアが Nexus Dashboard プラットフォームに移動し、Nexus Dashboard Fabric Controller に名前が変更される前の、DCNM の 11.x リリースからのアップグレードに固有の情報が含まれています。

（注） 現在のリリースがすでに Nexus Dashboard に展開されている場合は、次のサブセクションをスキップしてください。

Cisco DCNM 11.5(4) からのアップグレード後のペルソナと機能の互換性

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、ペルソナのために新しく展開された Cisco Nexus Dashboard Fabric Controller に、DCNM リリース 11.5(4) からバックアップされたデータを復元できます。

DCNM 11.5（4）からのバックアップ	アップグレード後の NDFC 12.1.3 でのペルソナの有効化
OVA/ISO/SE での DCNM 11.5（4）ローカル エリア ネットワーク（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
OVA/ISO/SE でのDCNM 11.5（4）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）

DCNM 11.5（4）からのバックアップ	アップグレード後の NDFC 12.1.3 でのペルソナの有効化
OVA/ISO/SE での DCNM 11.5（4）SAN の展開	SAN コントローラ
Linux での DCNM 11.5（4）SAN の展開	SAN コントローラ
Windows での DCNM 11.5（4）SAN の展開	SAN コントローラ

アップグレード後の機能の互換性

次の表に、NDFC、リリース 12.1.3 へのアップグレード後に DCNM 11.5(4) 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（4）の機能	アップグレードのサポート
構成された Nexus Dashboard Insights 詳細については、Cisco Nexus Dashboard ユーザー ガイドを参照してください。	サポート対象
コンテナ オーケストレータ (K8s) ビジュアライザ	サポート対象
vCenter による VMM の可視性	サポート対象
構成された Nexus Dashboard Orchestrator	未サポート
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
DCNM トラッカー	サポート対象外
ファブリックのバックアップ	未サポート
レポート定義とレポート	未サポート
スイッチのイメージとイメージ管理ポリシー	サポート対象外
SAN CLI テンプレート	11.5（4）から繰り越されない 12.1.3
POAP および CLI テンプレート	11.5（4）から繰り越されない 12.1.3 **回避策**：アップグレードの前に、これらのテンプレートをコピーします。アップグレード/移行が完了したら、これらのテンプレートを NDFC に再適用します。

DCNM 11.5（4）の機能	アップグレードのサポート
イメージ/イメージ管理データの切り替え	11.5（4）から繰り越されない 12.1.3
低速ドレイン データ	11.5（4）から繰り越されない 12.1.3
Infoblox 設定	11.5（4）から繰り越されない 12.1.3
エンドポイント ロケーションの設定	リリース 12.1.3 へのアップグレード後に、エンドポイント ロケータ（EPL）を再構成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。
アラーム ポリシーの設定	11.5（4）から繰り越されない 12.1.3
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。

（注） SAN インサイトおよび VMM ビジュアライザの機能は、復元後に有効になりません。**[設定（Settings）] > [機能管理（Feature Management）]** のチェック ボックスをオンにして、**[保存（Save）]** をクリックして、復元後にこれらの機能を有効にする必要があります。

NDFC 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 NDFC ダウンロード ページを参照してください。https://software.cisco.com/download/home/281722751/type/282088134/

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 12.1.3 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 *5*：『*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 ツールを使用した構成のバックアップ

大規模な DCNM のバックアップ スクリプトを実行する前に、Performance Management の収集を停止します。Performance Management の収集を停止するには、次の手順を実行します。

- **[管理 (Administration)]** > > **[DCNM サーバ (DCNM Server)]** > > **[サーバ ステータス (Server Status)]** を選択します。
- **Performance Collector** の **[サービスの停止]** をクリックし、数秒待ちます。
- ステータスを確認するには、右上の**更新**アイコンをクリックします。**Stopped** と表示されていることを確認します。

バックアップ ツールは、過去 90 日間の Performance Management データを収集します。

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。

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。

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。

OVA / ISO の場合：

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

Windows/Linux の場合：

```
[root@dcnm]# chmod +x ./DCNM_To_NDFC_Upgrade_Tool_LIN_WIN
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 12.1.3 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、NDFC 12.1.3上にのみ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 12.1.3 or
 not.
If upgrade to NDFC 12.1.3 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 12.1.3
```

```
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 12.1.3 or not.

If upgrade to NDFC 12.1.3 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 12.1.3

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 12.1.3
 or not.

If upgrade to NDFC 12.1.3 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 */
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 DCNM 11.5（4）から Cisco NDFC リリース 12.1.3 へのアップグレード

DCNM リリース 11.5（4）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12.1.3 にアップグレードするには、次の手順を実行します。

始める前に

- 11.5（4）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。DCNM 11.5（4）ですべてのアプリケーションとデータをバックアップする手順については、を参照してくださいアップグレードツールを使用した構成のバックアップ （52 ページ）。

（注） 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 NDFC 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 NDFC のインストール手順については、次を参照してください：
  - NDFC の手動インストール （35 ページ）
  - App Store を使用した NDFC のインストール （33 ページ）
- 既存の設定で Cisco Smart Software Management（CSSM）に直接接続するスマート ライセンスを使用している場合は、Nexus Dashboard に CSSM Web サイトに到達するために必要なルートがあることを確認する必要があります。

  https://smartreceiver.cisco.com 上の IP アドレスのサブネットが、NDFC を実行している Nexus Dashboard のルート テーブルに追加されていることを確認します。**[管理者（Admin）]** > **[システム設定（System Settings）]** > **[システムの問題（System Issues）]** に移動します。**[管理ネットワーク ルート（Management Network Routes）]** エリアの **[編集**

（**Edit**）] アイコンをクリックし、管理ネットワーク ルートの IP アドレス/サブネットを追加し、**[保存（Save）]** をクリックして確認します。

https://smartreceiver.cisco.com に ping を送信すると、最新のサブネットを見つけることができます。例：

```
$ ping smartreceiver.cisco.com
PING smartreceiver.cisco.com (146.112.59.81): 56 data bytes
64 bytes from 146.112.59.81: icmp_seq=0 ttl=52 time=48.661 ms
64 bytes from 146.112.59.81: icmp_seq=1 ttl=52 time=44.730 ms
64 bytes from 146.112.59.81: icmp_seq=2 ttl=52 time=48.188 ms
```

さらに、NDFC は新しい製品インスタンスと見なされるため、信頼を再確立する必要があります。期限切れの信頼トークンを使用してバックアップを作成した場合は、アップグレード後にスマート ライセンス設定ウィザードを手動で実行し、有効なトークンを入力する必要があります。

手順

ステップ 1 正しいログイン情報を使用して Cisco **Nexus ダッシュボード Web UI** にログオンします。

ステップ 2 One View ドロップダウン リストから Nexus ダッシュボード ファブリック コントローラを選択します。

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 3 [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 4 [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 5 **[種類（Type）]** で、復元する形式を選択します。

（注）
DCNM リリース 11.5（4）で作成されたバックアップに基づいて、**[構成のみ（Config only）]** または **[完全（Full）]** 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。

  [構成のみ（Config only）] または **[完全（Full）]** バックアップ ファイルのいずれかを選択できます。

- 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。

[完全（Full）] バックアップ ファイルを選択する必要があります。

ステップ 6 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 サーバーからインポート（Import from SCP Server）]** または **[SFTP サーバーからインポート（Import from SFTP Server）]** を選択します。
  1. **[サーバー（Server）]** フィールドに、サーバーの 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 7 **[外部サービス IP 構成を無視（Ignore External Service IP Configuration ）]** オプションがオフになっていることを確認します。

このオプションは、アップグレード時には使用されません。

ステップ 8 [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。

アップグレード後の作業

次の項では、Cisco NDFC、リリース 12.1.3 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、**[オペレーション (Operations)] > [ライセンス管理 (License Management)] > [スマート (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 12.1.3 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	12.1.3 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 構成の違いは、ありません。対応不要です。
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）	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。 構成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。**[構成の展開（Deploy Config）]** をクリックします。
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 構成の違いは、ありません。対応不要です。

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	12.1.3 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	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 構成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。**[構成の展開（Deploy Config）]**をクリックします。

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	12.1.3 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 構成の違いは、ありません。対応不要です。
		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

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、Nexusダッシュボードファブリック コントローラ リリース 12.1.3 は次のいずれかのペルソナで展開されます。

- 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。

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シスコ 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。

特定の展開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 *6*: 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
SAN コントローラ	サポート対象外	サポート対象外	-

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。