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

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 （5 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。

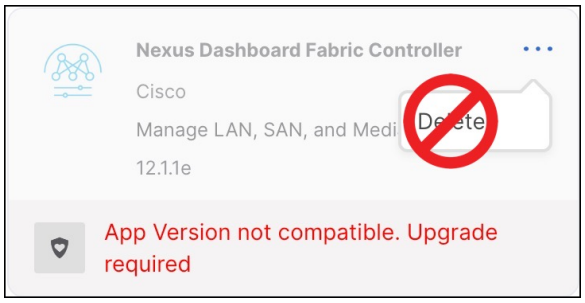
- Nexus Dashboard リリース 2.2(1) またはそれ以降を実行して、リリース 3.0(1) に直接アップグレードする必要があります。

（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 （8 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 （8 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 （11 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 （1 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。

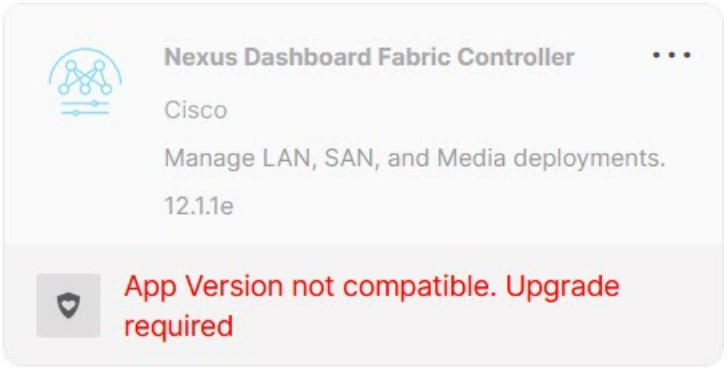
（注）
Nexus Dashboard のアップグレードを開始する前に、前のステップで説明したように、NDFC サービスが無効になっていることを確認してください。

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 *1*：『*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 （14 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
  - App Store を使用した NDFC のインストール
- 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 *2:* 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。