LAN 動作モードのスイッチの追加、モード、リリース 12.2.1

目次

新規情報および変更情報

次の表は、この最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

リリース バージョン	特長	説明
NDFC リリース 12.2.1	PowerOn Auto Provisioning（POAP）を使用したファブリックへの事前プロビジョニングされたデバイスの自動インポートのサポート	この機能を有効にすると、NDFC は POAP を使用して事前にプロビジョニングされたデバイスをファブリックに自動的にインポートします。この機能を有効にするには、**[管理者（Admin）] > [システム設定（System Settings）] > [サーバー設定（Server Settings）] > [LAN ファブリック（LAN-Fabric）]** タブで、**[再プロビジョニング中に事前プロビジョニングされたスイッチを自動許可（Auto permit pre-provisioned switch during re-poap）]** オプションを使用します。この機能を使用すると、**[スイッチの追加（ブートストラップ）（Add Switches (Bootstrap)]** ページでユーザー名、パスワード、およびブートストラップ パラメータを再入力する必要がなくなります。 詳細については、「POAP を使用した事前POAP を使用した 事前プロビジョニングされたデバイスの自動インポート」を参照してください。
NDFC リリース 12.2.1	スイッチが通常モードからメンテナンス モードに、またはその逆にモードを変更するのを待機するためのサポートが追加されました	この機能をイネーブルにして NDFC からスイッチ変更モード要求を実行すると、指定したスイッチがメンテナンス モードになり、NDFC GUI はスイッチでモードが完全に変更されるまで待機します。 NDFC GUI がスイッチのモード変更要求を完了すると、スイッチは選択に基づいてモードをメンテナンス モードまたは通常モードに変更します。 「展開時にスイッチ モードがメンテナンスに変更されるのを待機する」オプションは、「ファブリックの概要 > スイッチ」ページ、管理 **> [インベントリ] > [スイッチ]** ページの [アクション] ドロップダウン リストから有効にするか、または **[トポロジ]** ページでファブリックをダブルクリックしてスイッチにアクセスすることで有効にできます。次に、スイッチを右クリックし、[詳細（More）] > [モードの変更（Change Mode）] の順にクリックして、[モードの変更（Change Mode）] ダイアログボックスにアクセスします。 詳細については、[スイッチがモードを変更するのを待つ（Waiting for a Switch to Change Modes）] を参照してください。

スイッチ

次の表で、**[**スイッチ（**Switches**）**]** ウィンドウに表示されるフィールドについて説明します。

フィールド	説明
スイッチ	スイッチの名前を指定します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。
ロール	スイッチに割り当てるロールを指定します。
シリアル番号（Serial Number）	スイッチのシリアル番号を指定します。
Fabric Name（ファブリック名）	スイッチに関連付けられているファブリック名を指定します。
Config Status	構成ステータスを指定します。ステータスは、In-Sync または Out-of-sync のいずれかになります。
動作ステータス	構成ステータスを指定します。ステータスは、In-Sync または Out-of-sync のいずれかになります。
検出ステータス	スイッチの検出ステータスを指定します。
モデル	スイッチ モデルを指定します。
vPC ロール	スイッチの vPCロール を指定します。
vPC ピア	スイッチの vPC ピアを指定します。

ファブリックへのスイッチの追加

UI パス：**[管理（Manage）] > [インベントリ（Inventory）] > [スイッチ（Switches）] > [アクション（Actions）] > [スイッチの追加（Add Switches）]**

各ファブリックのスイッチは一意であるため、1 つのファブリックに追加できるスイッチは 1 つだけです。

ヒ Cisco Nexus Dashboard には、ノードごとに 2 つの論理インターフェイス、つまり管理インターフェイス（bond1br）とファブリック（データ）インターフェイス（bond0br）があります。Cisco Nexus Dashboard ファブリック コントローラの場合、Nexus Dashboard 管理インターフェイスとファブリック インターフェイスは異なる IP サブネットに存在する必要があります。デフォルトでは、Nexus Dashboard サービスのルートはファブリック インターフェイス経由です。オペレータは、管理インターフェイス（bond1br）経由で到達する必要があるスイッチに接続するために、Nexus Dashboard 管理ネットワークにスタティック ルートを追加する必要があります。これにより、ポッドのルートが管理インターフェイスを出口インターフェイスとして使用するようになります。

ヒ NDFC の検出または追加のスイッチまたは LAN クレデンシャルのスイッチ ユーザー ロールに network-admin ロールがあることを確認してください。

ヒ SNMPv3 は、Nexus デバイスの検出に使用されます。スイッチでユーザーが作成されると、デフォルトでは SNMPv3 認証に同じユーザー名/パスワードが使用されます。

既存のファブリックにスイッチを追加するには、次の手順を実行します：

1. Nexus Dashboard Fabric Controller Web UI から、**[管理（Manage）] > [インベントリ（Inventory）] > [スイッチ（Switches）]** の順に選択します。
2. [スイッチ（Switches）] タブで、 **[アクション**

   （Actions）] > [スイッチの追加（Add Switches）]

   を選択します。**[スイッチの追加（Add Switches）]**

   ウィンドウが表示されます。

   同様に、[トポロジ（Topology）] ウィンドウでスイッチを追加できます。このウィンドウでファブリックを選択し、ファブリックを右クリックして **[スイッチの追加（Add Switches）]** をクリックします。

3. **[スイッチの追加]** ウィンドウで、**[ファブリックの選択（Choose Fabric）]** をクリックし、適切なファブリックをクリックして、
   [選択（Select）] をクリックします。

   [スイッチの追加（Add Switches）] ウィンドウにはデフォルトの検出タブがあり、他のタブは選択したファブリックに基づいて表示されます。

さらに、スイッチとインターフェイスを事前プロビジョニングできます。詳細については、「デバイスの事前プロビジョニング」および「イーサネット インターフェイスの事前プロビジョニング」を参照してください。

NDFC はデフォルト システム名（シリアル番号）のスイッチ検出のみをサポートします。

Nexus Dashboard ファブリック コントローラがピリオド文字（.）を含むホスト名を持つスイッチを検出すると、ドメイン名として扱われ、切り捨てられます。ピリオド文字（.）の前のテキストのみがホスト名と見なされます。例：

- ホスト名が **leaf.it.vxlan.bgp.org1-XYZ** の場合、Nexus Dashboard ファブリック コントローラは **leaf** のみを表示します
- ホスト名が **Leaf.it.vxlan.bgp.org1-XYZ** の場合、Nexus Dashboard ファブリック コントローラは **leafit-vxlan** のみを表示します

スイッチ名またはホスト名がファブリック内で一意であることを確認してください。

新しいスイッチの検出

新しいスイッチを検出する前に、そのスイッチのパスワードが 8 文字以上であることを確認します。NDFC では、
パスワードの長さが 8 文字未満の場合、次のエラーメッセージが表示される場合があります。そのスイッチのパスワードが 8 文字未満の場合は、NDFC ファブリックにスイッチを追加すると、
「追加後処理中に予期しないエラーが発生する」 というメッセージです。

1. 新しい Cisco NX-OS デバイスの電源がオンになると、通常、そのデバイスにはスタートアップ構成も構成ステートもありません。その結果、NX-OS で電源が投入され、初期化後に POAP ループに入ります。デバイスは、mgmt0 インターフェイスを含むアップ状態のすべてのインターフェイスで DHCP 要求の送信を開始します。
2. デバイスと Nexus ダッシュボード ファブリック コントローラ間に IP 到達可能性がある限り、デバイスからの DHCP 要求は Nexus ダッシュボード ファブリック コントローラに転送されます。ゼロデイ デバイスを簡単に起動するには、前述のように、*ファブリック設定*でブート ストラップ オプションを有効にする必要があります。
3. ファブリックに対してブートストラップが有効になっている場合、デバイスからの DHCP 要求は Nexus Dashboard Fabric Controller によって処理されます。Nexus Dashboard Fabric Controller によってデバイスに割り当てられた一時IPアドレスは、デバイス モデル、デバイス NX-OS バージョンなどを含むスイッチに関する基本情報を学習するために使用されます。
4. Nexus Dashboard ファブリック コントローラ UI で、**[**スイッチ（**Switch**）**] > [**アクション（**Actions**）**] > [**スイッチの追加（**Add Switches**）**]** の順に選択します。 **[**スイッチの追加（**Add Switches**）**]** ウィンドウにデフォルトのタブが表示されます。
5. **[**ブートストラップ（**Bootstrap**）（**POAP**）**]** ラジオ ボタンを選択します。

   前述のように、Nexus Dashboard Fabric Controller はデバイスからシリアル番号、モデル番号、およびバージョンを取得し、それらを [インベントリ管理（Inventory Management）] ウィンドウに表示します。また、IP アドレス、ホスト名、およびパスワードを追加するオプションが使用可能になります。スイッチ情報が取得されない場合は、ウィンドウを更新します。

ウィンドウの左上には、*エクスポート*と*インポート*のオプションがあり、
スイッチ情報を含む .csv ファイルをエクスポートおよびインポートできます。インポート　　オプションを使用してデバイスを事前プロビジョニングすることもできます。

   Cisco NDFC リリース 12.1.1e から、事前プロビジョニングされたブートストラップ スイッチの場合、シリアル番号にダミー値を追加できます。ネットワークを正常に構成したら、[スイッチ（Switches）] タブで適切なスイッチ番号を使用してシリアル番号を変更できます。

Nexus 9000 シリーズ スイッチのシリアル番号のみを変更できます。

   スイッチの横にあるチェックボックスを選択し、スイッチのクレデンシャル（IP アドレスとホスト名）を入力します。

   デバイスの IP アドレスに基づいて、**[IP** アドレス（**IP Address**）**]** フィールドに IPv4 または IPv6 アド

レスを追加できます。
デバイスは事前にプロビジョニングできます。デバイスを事前プロビジョニングするには、「デバイスの事前プロビジョニング」の項を参照してください。

6. **[**管理者パスワード（**Admin Password**）**]** フィールドと **[**管理者パスワードの確認（Confirm Admin Password）] フィールドに、管理者パスワードを入力し、確認します。

   この管理者パスワードは、POAP ウィンドウに表示されるすべてのスイッチに適用されます。

   新しいユーザを指定できます。ラジオ ボタン **[**新規ユーザーの指定（**Specify a new user**）**]** を選択し、**[**ユーザー名（**Username**）**]**、**[**パスワード（**Password**）**]** を入力して、ドロップダウンリストから **[**認証プロトコル（**Authentication Protocol**）**]** を選択します。

   スイッチの検出に管理者のログイン情報を使用しない場合は、
   代わりに、AAA 認証（つまり、検出のみに RADIUS またはTACACS ログイン情報）を使用します。

7. （任意）スイッチの検出に検出クレデンシャルを使用します。
   a. **[**ディスカバリ ログイン情報の追加（**Add Discovery Credentials**）**]** アイコンをクリックして、スイッチのディスカバリ ログイン情報を入力します。
   b. **[**ディスカバリ ログイン情報（**Discovery Credentials**）**]** ウィンドウで、ディスカバリ ユーザー名やパスワードなどのディスカバリ ログイン情報を入力します。

      [OK] をクリックして、ディスカバリ ログイン情報を保存します。

      ディスカバリ ログイン情報が指定されていない場合は、Nexus Dashboard Fabric Controller は管理者ユーザーとパスワードを使用してスイッチを検出します。

8. 画面右上の **[**ブートストラップ（**Bootstrap**）**]** をクリックします。

   Nexus Dashboard Fabric Controller は管理IPアドレスおよび その他のログイン情報をスイッチにプロビジョニングします。この単純化された POAP プロセスでは、すべてのポートが開かれます。

9. 最新情報を入手するには、**[**トポロジの更新（**Refresh Topology**）**]** ボタンをクリックします。追加されたスイッチは、POAP サイクルを実行します。スイッチをモニタし、POAP 完了を確認します。
10. 追加されたスイッチが POAP を完了すると、ファブリック ビルダ トポロジページが追加されたスイッチで更新され、検出された物理接続が示されます。スイッチに適切なロールを設定し、ファブリック レベルで Deploy Config 操作を実行します。ファブリック設定、スイッチロール、トポロジなどが Fabric Builder によって評価され、スイッチの適切な意図された設定が保存操作の一部として生成されます。保留中の設定は、新しいスイッチをインテントと同期させるために新しいスイッチに導入する必要がある設定のリストを提供します。

    ファブリックで変更が発生して Out-of-Sync が発生した場合は、変更を展開する必要があります。このプロセスは、*「既存スイッチの検出」*の項で説明したものと同じです。

    ファブリックの作成中に、（
    [管理性（**Manageability**）**]** タブ）で、各スイッチの AAA サーバーのパスワードを更新する必要があります。
    そうでない場合、スイッチの検出は失敗します。

    SNMP を使用してデバイスを検出するときに、認証に AAA サーバーを使用するように

設定している場合は、コマンド *sync-snmp-password <password> <username>* が NDFC を介してスイッチ上で実行され、キャッシュされたユーザーが生成されます。提供者

> authentication は MD5 を デフォルトで活用します。 次の ように、 スイッチ AV ペアでの SNMPv3 認証とプライバシープロトコル属性を指定することもできます。
>
> *snmpv3:auth=SHA priv=AES-128*

11. 保留中の設定が展開されると、すべてのスイッチの **[**進捗（**Progress**）**]** 列に 100% と表示されます。
12. **[**閉じる（**Close**）**]** をクリックして、ファブリック ビルダ トポロジに戻ります。
13. **[**トポロジの更新（**Refresh Topology**）**]** をクリックして、更新を表示します。すべてのスイッチは、機能していることを示す緑色でなければなりません。
14. スイッチとリンクは、Nexus Dashboard Fabric Controllerで検出されます。設定は、さまざまなポリシー（ファブリック、トポロジ、スイッチ生成ポリシーなど）に基づいて構築されます。スイッチ イメージ（およびその他の必要な）設定がスイッチで有効になっている。
15. Nexus Dashboard Fabric Controller GUI では、検出されたスイッチは*スタンドアロン* ファブリック トポロジで確認できます。このステップまでで、POAP の基本設定は完了です。**[**管理（**Manage**）**] > [**インベントリ（**Inventory**）**] > [**スイッチ（**Switches**）**]** を介してインターフェイスを設定する必要があります。スイッチを選択すると、スライドイン ペインが表示されます。**[**起動 **(Launch)]** アイコンをクリックします。**[**スイッチの概要（**Switches Overview**）**]** タブで、**[**インターフェイス（**Interface**）**]** タブをクリックして追加設定を行いますが、次に限定されません。

    - vPC ペアリング
    - ブレークアウト インターフェイス
    - ポート チャネル、およびポートへのメンバーの追加

    vPC のペアリング/ペアリング解除または advertise-pip オプションを有効または無効にするか、マルチサイト構成を更新する場合は、**[**構成の展開（**Deploy Config**）**]** 操作を使用する必要があります。操作の終了時に、nve インターフェイスで **shutdown** または **no shutdown** コマンドを設定するように求めるエラーが表示されます。vPC 設定を有効にした場合のエラー スクリーンショットのサンプル。

    解決するには、 **[**インターフェイス（**Interfaces**）**] > [**アクション（**Actions**）**] > [**展開（**Deploys**）**]** タブに移動し、nve インターフェイスでシャットダウン操作を展開してから、No Shutdown 構成を実行します。これを次の図に示します。上矢印は No Shutdown 操作に対応し、下矢印はShutdown 操作に対応します。

スイッチを右クリックすると、さまざまなオプションを表示できます。

- ロールの設定：スイッチにロールを割り当てます（スパイン、ボーダー ゲートウェイなど）。

    - スイッチのロールの変更は、構成の展開を実行する前にのみ許可されます。
    - スイッチのロールは、スイッチ上にオーバーレイがない場合に変更できますが、スイッチ操作の項で指定された許可されたスイッチ ロール変更のリストに従ってのみ変更できます。

- モード：メンテナンス モードとアクティブ/操作モード。
- **vPC** ペアリング：vPC のスイッチを選択し、そのピアを選択します。

  vPC ペアの仮想リンクを作成するか、既存の物理リンクを vPC ペアの仮想リンクに変更できます。

- インターフェイスの管理：スイッチ インターフェイスに構成を展開します。
- ポリシーの表示/編集：スイッチ ポリシーを参照し、必要に応じて編集します。
- 履歴：スイッチの展開履歴を表示します。
- 履歴：スイッチの展開およびポリシーの変更履歴を表示します。

  [ポリシー変更履歴（**Policy Change History**）]タブには、追加、更新、削除などの変更を行ったユーザとともにポリシーの履歴が一覧表示されます。

  ポリシーの [ポリシー変更履歴（**Policy Change History**）] タブで、[生成された構成（**Generated Config**）] 列の [詳細な履歴（**Detailed History**）] をクリックして、前後の生成された構成を表示します。

  次の表に、ポリシー テンプレート インスタンス（PTI）の前後に生成される構成の概要を示します。

PTI の操作	前に生成された構成	後に生成された構成
追加	Empty	構成が含まれています
更新	変更前の構成が含まれています	変更後の構成が含まれています
マーク - 削除	削除する設定が含まれます。	色を変更して削除する構成が含まれます。
削除	構成が含まれています	Empty

ヒ ポリシーまたはプロファイル テンプレートが適用されると、テンプレートのアプリケーションごとにインスタンスが作成されます。これは、ポリシー テンプレート インスタンスまたは PTI と呼ばれます。

- [構成のプレビュー（Preview Config）] : 保留中の構成と、実行中の構成と予想される構成の比較を表示します。
- 構成の展開 - スイッチ構成ごとに展開します。
- 検出：このオプションを使用して、スイッチのクレデンシャルを更新し、スイッチをリロードし、スイッチを再検出し、ファブリックからスイッチを削除できます。

新しいファブリックが作成され、ファブリック構成スイッチがNexus Dashboard Fabric Controller で検出され、アンダーレイ設定がそれらのスイッチでプロビジョニングされ、Nexus Dashboard Fabric Controller との間の設定が同期されます。その他のタスクは、次のとおりです。

- vPC、ループバック インターフェイス、サブインターフェイス設定などの インターフェイス 構成をプロビジョニングします。
- ネットワークを作成し、スイッチに展開します。

既存のスイッチのディスバリ

Cisco Nexus Dashboard Fabric Controller Web UI で既存のスイッチを検出するには、次の手順を実行します。

1. [スイッチの追加（**Add Switches**）] をクリックした後、[スイッチの検出（**Discover Switches**）] をクリックして、1 つ以上の既存のスイッチをファブリックに追加します。

   この場合、既知のクレデンシャルと事前プロビジョニングされた IP アドレスを持つスイッチがファブ

リックに追加されます。

2. スイッチの IP アドレス（シード IP）、ユーザ名、およびパスワード（**[ユーザ名（Username）]** フィールドと **[パスワード（Password）]** フィールド）は、ユーザによる入力として提供されます。**[構成の保持（Preserve Config）]** チェックボックスがデフォルトで選択されています。これは、ファブリックへのデバイスのブラウンフィールド インポートに対してユーザが選択するオプションです。デバイス設定がインポート プロセスの一部としてクリーンアップされるグリーンフィールド インポートの場合、ユーザーは **[構成の保持（Preserve Config）]** チェックボックスを選択しないでください。

   Easy_Fabric_eBGP は、ファブリックへのデバイスのブラウンフィールドインポートをサポートしていません。

3. **[スイッチの検出（Discover Switches）]** をクリックします。

   [スイッチの追加（Add Switches）] ウィンドウが表示されます。**[最大ホップ（Max Hops）]** フィールドに 2 が入力されているため（デフォルト）、指定された IP アドレス（リーフ 91）を持つスイッチとそのスイッチからの 2 つのホップが **[スイッチの追加（Add Switches）]** の結果に入力されます。

4. Cisco Nexus Dashboard Fabric Controller がスイッチに対して正常なシャローディスカバリを実行できた場合、ステータス列に **[管理性（Manageable）]** と表示されます。該当するスイッチの横にあるチェックボックスをオンにして、**[スイッチの追加（Add Switches）]** をクリックします。

   この例では 1 つのスイッチの検出について説明しますが、複数のスイッチを同時に検出できます。

   スイッチ検出プロセスが開始されます。**[進行状況（Progress）]** 列には、選択したすべてのスイッチの進行状況が表示されます。完了時に各スイッチの完了を表示します。

   選択したすべてのスイッチがインポートされるか、エラー メッセージが表示されるまで、画面を閉じないでください（また、スイッチを再度追加してください）。

   エラー メッセージが表示された場合は、画面 を閉じます。[ファブリック トポロジ（fabric topology）] 画面が表示されます。エラー メッセージは、画面の右上に表示されます。
   必要に応じてエラーを解決し、[アクション（Actions）] パネルの **[スイッチの追加（Add Switches）]** をクリックしてインポート プロセスを再度開始します。

   Cisco Nexus Dashboard Fabric Controller がすべてのスイッチを検出し、[進行状況（Progress）] 列にすべてのスイッチの完了が表示されたら、画面を閉じます。*[スタンドアロン* ファブリック トポロジ（Standalone fabric topology）] 画面が再び表示されます。追加されたスイッチのスイッチ アイコンが表示されます。

   スイッチの検出中に次のエラーが発生することがあります。

5. 最新のトポロジ ビューを表示するには、**[トポロジの更新（Refresh topology）]** をクリックします。

   すべてのスイッチが追加され、ロールが割り当てられると、ファブリック トポロジにはスイッチとスイッチ間の接続が含まれます。

6. デバイスを検出したら、各デバイスに適切なロールを割り当てます。ロールの詳細については、[スイッチ ロールの割り当て（Assigning Switch Roles）] を参照してください。

   表示用に階層レイアウトを選択すると（[アクション（Actions）] パネルで）、トポロジはロールの割り当てに従って自動的に配置され、リーフ デバイスが下部に、スパイン デバイスが上部に接続され、境界デバイスが上部に配置されます。

vPC スイッチ ロール の割り当て：スイッチのペアを vPC スイッチ ペアとして指定するには、スイッチを右クリックし、スイッチのリストから vPC ピア スイッチを選択します。

AAA サーバー パスワード：（**[**管理性（**Manageability**）**]** タブで）AAA サーバー情報を入力した場合は、各スイッチで AAA サーバー パスワードを更新する必要があります。そうでない場合、スイッチの検出は失敗します。

Cisco Nexus Dashboard Fabric Controller を使用して新しい vPC ペアが正常に作成および展開されると、コマンドがスイッチに存在する場合でも、no ip redirects CLI のいずれかのピアが同期しなくなることがあります。この非同期は、実行構成で CLI を表示するためのスイッチの遅延が原因で発生し、構成のコンプライアンスに相違が生じます。**[**構成の展開（**Config Deployment**）**]** ウィンドウでスイッチを再同期して、差分を解決します。

7. **[**保存（**Save**）**]** をクリックします。

テンプレートとインターフェイスの設定は、スイッチのアンダーレイ ネットワーク構成を形成します。また、ファブリック構成の一部として入力されたフリーフォーム CLI（[詳細（Advanced）]タブで入力されたリーフおよびスパイン スイッチのフリー フォーム設定）も展開されます。

構成のコンプライアンス：プロビジョニングされた構成とスイッチの構成が一致しない場合、**[**ステータス（**Status**）**]** 列に非同期が表示されます。たとえば、CLI を使用してスイッチの機能を手動で有効にすると、設定が一致しなくなります。

Cisco Nexus Dashboard Fabric Controller からファブリックにプロビジョニングされた設定が正確であることを確認したり、逸脱（アウトオブバンド変更など）を検出したりするために、Nexus Dashboard Fabric Controller の構成コンプライアンスエンジンは、必要な修復構成を報告し、提供します。

[展開構成（**Deploy Config**）**]** をクリックすると、**[**構成の展開（**Config Deployment**）**]** ウィンドウが表示されます。

ステータスが非同期の場合は、デバイスの Nexus Dashboard Fabric Controller との構成に不整合があることを示しています。

[再同期（Re-sync）] 列のスイッチごとに [再同期（Re-sync）] ボタンが表示されます。大規模なアウトオブバンド変更がある場合、または設定変更が Nexus Dashboard Fabric Controller に正しく登録されていない場合に、このオプションを使用して Nexus Dashboard Fabric Controller 状態を再同期します。再同期操作は、スイッチに対して完全な CC 実行を実行し、「show run」および「show run all」コマンドをスイッチから再収集します。再同期プロセスを開始すると、進行状況メッセージが画面に表示されます。再同期中に、実行構成がスイッチから取得されます。スイッチの Out-of-Sync/In-Sync ステータスは、Nexus Dashboard Fabric Controller で定義されたインテントに基づいて再計算されます。

[構成のプレビュー（**Preview Config**）**]** 列エントリ（特定の行数で更新）をクリックします。[構成のプレビュー (Config Preview)] 画面が表示されます。

[保留中の構成（**PendingConfig**）**]** タブには、正常な展開の保留中の構成が表示されます。

[並べて比較（**Side-by-sideComparison**）**]** タブには、現在の構成と予想される構成が一緒に表示されます。

マルチラインバナー motd 構成は、**switch_freeform** を使用するスイッチごと、またはリーフ/スパイン自由形式構成を使用するファブリックごとのいずれかで、自由形式の構成ポリシーを使用して Cisco Nexus Dashboard Fabric Controller で構成できます。複数行のバナー motdが構成された後、ファブリック トポロジ画面（の右上）で**[**構成の展開（**Deploy Config**）**]**オプションを実行して、ポ

リシーを展開します。そうしないと、ポリシーがスイッチに適切に展開されない可能性があります。バナー ポリシーは、単一行のバナー設定のみを設定します。また、作成できるバナーは 1 つだけです。
関連するフリーフォーム設定/ポリシー。バナー motd を構成するための複数のポリシーはサポートされていません。

8. 画面 を閉じます。

   構成が正常にプロビジョニングされた後（すべてのスイッチで 100% の進捗が表示された場合）、画面を閉じます。

   ファブリック トポロジが表示されます。構成が成功すると、スイッチのアイコンが緑色に変わります。

   スイッチ アイコンが赤色の場合は、スイッチと Nexus Dashboard Fabric Controller 構成が同期していないことを示します。スイッチでの展開が保留中の場合、スイッチは青色で表示されます。保留状態は、保留中の展開または保留中の再計算があることを示します。スイッチをクリックし、**[**プレビュー（**Preview**）**]** または [構成の展開（Deploy Config）] オプションを使用して保留中の展開を確認するか、[構成の展開（Deploy Config）] をクリックしてスイッチの状態を再計算できます。

   CLI の実行で警告またはエラーが発生した場合は、通知が表示されます **[**ファブリック ビルダ（**FabricBuilder**）**]** ウィンドウに表示されます。重大な警告またはエラーには、**[**解決（**Resolve**）**]** オプションがあります。

   [構成の展開（**Deploy Config**）**]** オプションの使用例は、スイッチ レベルの自由形式の設定です。詳細について参照してください。

ブート ストラップ メカニズムを使用したスイッチの追加

新しい Cisco NX-OS デバイスの電源がオンになると、通常、そのデバイスにはスタートアップ構成も構成ステートもありません。その結果、NX-OS で電源が投入され、初期化後に POAP ループに入ります。デバイスは、mgmt0 インターフェイスを含むアップ状態のすべてのインターフェイスで DHCP 要求の送信を開始します。

Nexus Dashboard ファブリック コントローラ リリース 12.0.1a 以降、POAP はユーザーが検証したキー交換とパスワードなしの ssh を使用して、構成ファイルへのアクセスを特定のスイッチに制限します。したがって、デバイスが POAP を試行するたびに、**[**スイッチの追加（**Add Switch**）**] > [**ブート ストラップ（**Bootstrap**）**]** で新しいキーを受け入れる必要があります。

デバイスと Nexus Dashboard Fabric Controller 間に IP 到達可能性がある場合、デバイスからの DHCP 要求は Nexus Dashboard Fabric Controller に転送されます。ゼロデイ デバイスを簡単に起動するには、ブートストラップ オプションを [ファブリック設定（Fabric Settings）] で有効にする必要があります。

ファブリックに対してブートストラップが有効になっている場合、デバイスからの DHCP 要求は Nexus Dashboard Fabric Controller によって処理されます。Nexus Dashboard Fabric Controller によってデバイスに割り当てられた一時IPアドレスは、デバイス モデル、デバイス NX-OS バージョンなどを含むスイッチに関する基本情報を学習するために使用されます。

1. **[**管理（**Manage**）**] > [**インベントリ（**Inventory**）**] > [**スイッチ（**Switches**）**] > [**スイッチの追加（**Add Switches**）**]** の順に選択します。
2. **[**ブートストラップ（**Bootstrap**）（**POAP**）**]** ラジオ ボタンを選択します。
3. **[**アクション（**Actions**）**]** をクリックし、スイッチを追加します。

   [追加（**Add**）**]** オプションを使用してスイッチを 1 つずつ追加するか、**[**インポート（**Import**）**]** オプシ

ョンを使用して複数のスイッチを同時に追加できます。
[追加（Add）] オプションを使用する場合は、必要な詳細をすべて入力してください。

注：スイッチが表示されるまでに時間がかかる場合があります。

4. 必要なスイッチを選択します。
5. **[編集（Edit）]** をクリックします。

   [ブートストラップ スイッチの編集（Edit bootstrap switch）] ダイアログが表示されます。
6. 次の必須詳細情報を入力します。
7. **[保存（Save）]** をクリックします。
8. スイッチを選択します。
9. **[管理者パスワード（Admin password）]** フィールドに管理者パスワードを入力します。
10. **[選択したスイッチをインポート（Import Selected Switches）]** をクリックします。

返品許可（RMA）

ここでは、Cisco Nexus Dashboard Fabric Controller Easy Fabric モードを使用する場合に、ファブリック内の物理スイッチを交換する方法について説明します。

前提条件

- スイッチの交換時に、中断を最小限に抑えてファブリックが稼働していることを確認します。
- POAP RMA フローを使用するには、ファブリックをブートストラップ（POAP）用に設定します。
- 必要に応じて、再計算と展開を複数回実行し、FEX が展開されているスイッチの RMA の FEX 構成をコピーします。

注意事項と制約事項

- リリース 12.1.3 以降、Cisco Nexus ダッシュボード ファブリック コントローラは、Catalyst 9000 シリーズ スイッチで RMA 機能をサポートします。ただし、この機能は、Stackwise または Stackwise Virtual を搭載した Catalyst スイッチではサポートされていません。
- スイッチを交換するには、ファブリックから古いスイッチを取り外し、ファブリック内の新しいスイッチを検出します。
- Cisco Nexus 7000 シリーズスイッチをアップグレードする前にGIRが有効になっている場合、Cisco Nexus 7000 Series スイッチと Nexus Dashboard Fabric Controller は、RMA 手順の開始時に **system mode maintenance** コマンドをスイッチにプッシュします。このコマンドは、デフォルトのメンテナンス モード プロファイルに存在する設定をスイッチに適用します。Cisco Nexus 7000 シリーズ スイッチでのグレースフル挿入および取り外し（GIR）の実行の詳細については、「GIRの構成」を参照してください。
- スイッチを交換する場合は、交換用スイッチが元のデバイスと同じモデルであることを確認してください。不一致がある場合は、NDFC は不一致を示す警告を表示します。
- NDFC と Nexus Dashboard Orchestrator の統合では、NDFC へのスイッチの RMA 後、Nexus Dashboard Orchestrator でネットワークと VRF の手動インポートを実行して、NDFC でスキーマの差分を表示する必要があります。NDFC で RMA を実行した後、Nexus Dashboard Orchestrator ファブリックの更新後、Nexus Dashboard Orchestrator はシリアル番号の変更を確認します。NDFC では、シリアル番号を

同期させるためにスイッチを再インポートする必要があります。

POAP/PnP を使用した RMA のプロビジョニング

RMAをプロビジョニングするには、次の手順に従います。

1. **[**ファブリックの概要（**Fabric Overview**）**]** ページに移動します。
2. デバイスをメンテナンス モードにします。デバイスをメンテナンス モードに移動します。
   a. デバイスを選択し、**[**アクション（**Actions**）**] > [**詳細（**More**）**] > [**モードの 変更（**Change Mode**）**]** の順に選択します。
   b. **[**モード（**Mode**）**]** ドロップダウンリストで、**[**メンテナンス（**Maintenance**）**]** を選択します。
   c. **[**保存して展開（**Save and Deploy**）**]** をクリックします。
3. ネットワーク内のデバイスを物理的に交換します。物理接続は、交換用スイッチの元のスイッチと同じ場所で行う必要があります。
4. スイッチの電源をオンにし、POAP/PnP を使用してデバイスをオンボーディングします。
5. デバイスを選択し、**[**アクション（**Actions**）**] > [**詳細（**More**）**] >[RMA** のプロビジョニング（**Provision RMA**）**]** をクリックします。RMA フローが開始されます。
6. **[**管理者パスワード（**Admin password**）**]** フィールドに管理者パスワードを入力し、

   [RMA のプロビジョニング（**Provision RMA**）**]** をクリックします。（オプション）

   検出用の AAA ユーザーとパスワードを設定できます。

7. 交換用デバイスを選択し、**[**アクション（**Actions**）**] > [**詳細（**More**）**] > [RMA** のプロビジョニング（**Provision RMA**）**]** を選択します。
8. **[**管理者パスワード（**Admin password**）**]** フィールドに管理者パスワードを入力し、**[RMA** のプロビジョニング（**Provision RMA**）**]** をクリックします。

スイッチが NDFC IP とは異なるサブネット上にある場合は、POAP を使用するように DHCP リレーを設定する必要があります。DHCP リレーのスイッチでは、3 つの IP リダイレクト 回線 （ 各 ND ノード IP に 1 つ ）。 設定 について は 、DHCP リレーについては、「 概要」の「Creating Network for Standalone Fabrics」の項を参照してください。
LAN 動作モード設定のファブリックの概要。

RMA の手動プロビジョニング

このフローは、ブートストラップが不可能な場合（または望ましくない場合）に使用します。手動 RMA をプロビジョニングするには、次の手順に従います。

1. デバイスをメンテナンス モード（オプション）にします。
2. ネットワーク内のデバイスを物理的に交換します。
3. コンソールからログインし、管理 IP とログイン情報を設定します。
4. AAA を使用している場合は、スイッチで AAA コマンドを構成します。

新しく構成された AAA ユーザーの LAN および検出ログイン情報を NDFC で更新します。

5. Cisco Nexus Dashboard Fabric Controller が新しいデバイスを再検出することを許可します（または、**[検出（Discovery）] > [再検出（Rediscover）]** を手動で選択できます）。
6. **[アクション（Actions）] > [展開（Deploy）]** を使用して、期待される構成を展開します。
7. ブレイクアウト ポートまたは FEX ポートが使用中の場合、構成を復元するために再度展開します。
8. 展開が正常に完了し、デバイスが「同期中」になった場合、デバイスを通常モードに戻します。
9. AAA を使用している場合は、適切な TACACS ユーザー アカウントを使用して LAN および検出ログイン情報を更新します。
10. [再計算と展開（Recalculate and Deploy）] を実行して、ファブリックが引き続き同期していることを確認します。

ローカル認証を持つユーザの **RMA**

このタスクは、非 POAP スイッチにのみ適用されます。

ローカル認証を持つユーザの RMA を実行するには、次の手順を使用します。

1. 新しいスイッチがオンラインになったら、スイッチに SSH 接続し、「username」コマンドを使用してクリア テキスト パスワードでローカル ユーザ パスワードをリセットします。SNMP パスワードを再同期するには、ローカル ユーザ パスワードをリセットします。パスワードは、転送不可能な形式で構成ファイルに保存されます。
2. RMA が完了するまで待ちます。

事前プロビジョニングのサポート

Cisco NDFC は、事前のデバイス構成のプロビジョニングをサポートしています。これは特に、デバイスが調達されたものの、まだお客様に配送されていない、または受領されていないシナリオに当てはまります。発注書には通常、デバイスのシリアル番号、デバイス モデルなどに関する情報が含まれており、これらの情報を使用して、デバイスをネットワークに接続する前に NDFC でデバイス構成を準備できます。簡易ファブリックと外部/Classic_LAN ファブリック、および VXLAN EVPN ファブリックに対して、Cisco NX-OS デバイスの事前プロビジョニングがサポートされています。

デバイスの事前プロビジョニング

デバイスをファブリックに追加する前にプロビジョニングできます。

はじめる前に

- **[**ファブリックの編集（**Edit Fabric**）**] > [**ブートストラップ（**Bootstrap**）**]** タブの **[**ブートストラップの有効化（**Enable Bootstrap**）**]** チェックボックスがオンになっていることを確認します。
- **[**ローカル **DHCP** サーバーの有効化（**Enable Local DHCP Server**）**]** チェックボックスをオンにします。

事前プロビジョニングされたデバイスは、Nexus Dashboard ファブリック コントローラ で次の設定をサポートします。

- 基本管理
- vPC ペアリング
- ファブリック内リンク
- イーサネット ポート
- ポートチャネル
- vPC
- ST FEX
- AA FEX
- ループバック
- オーバーレイ ネットワーク設定

事前プロビジョニングされたデバイスは、Nexus Dashboard ファブリック コントローラ の次の設定をサポートしていません。

- ファブリック間リンク
- Sub-interface
- インターフェイス ブレークアウト構成

デバイスにブレークアウト リンクが事前プロビジョニングされている場合は、ブレークアウト PTI を生成するために、**[**新しいデバイスを事前プロビジョニングに追加（**Add a new device to pre-provisioning**）**]** ページの **[**データ（**Data**）**]** フィールドで、対応するブレークアウト コマンドをスイッチのモデルとゲートウェイとともに指定する必要があります。

ヒ 事前プロビジョニング ペイロードのデータ キーのインターフェイス ブレークアウト CLI には、スイッチからの「show running-configuration」出力にあるとおりの形式が

含まれている必要があります。

次のガイドラインに注意してください。

- 複数のブレイクアウト コマンドは、セミコロン（;）で区切ることができます。
- データ JSON オブジェクトのフィールドの定義は次のとおりです。

フィールド	説明
modulesModel	（必須）スイッチ モジュールのモデル情報を指定します。
ゲートウェイ	（必須）スイッチの管理 VRF のデフォルト ゲートウェイを指定します。このフィールドは、デバイスを事前プロビジョニングするインテントを作成するために必要です。デバイスの事前プロビジョニングの一環としてインテントを作成するために、Nexus Dashboard ファブリック コントローラと同じサブネット内にある場合でも、ゲートウェイを入力する必要があります。
ブレイクアウト	（オプション）スイッチで提供される breakout コマンドを指定します。
portMod	（オプション）ブレイクアウト インターフェイスのポート モードを指定します。

[データ（**Data**）**]** フィールドの値の例を次に示します。

- {" modulesModel" : [" N9K-C93180LC-EX"], " gateway" : " 10.1.1.1/24" }
- {" modulesModel" : [" N9K-C93180LC-EX"]," breakout" : " interface breakout module 1 port 1 map 10g-4x" , " portMode" : " hardware profile portmode 4x100G+28x40G" , " gateway" : " 172.22.31.1/24" }
- {" modulesModel" : [" N9K-X9736C-EX" , " N9K-X9732C-FX" , " N9K-C9516-FM-E2" , " N9K-C9516-FM-E2" , " N9K-C9516-FM-E2" , " N9K-C9516-FM-E2" , " N9K-SUP-B+" , " N9K-SC-A" , " N9K-SC-A"], " gateway" : " 172.22.31.1/24" }
- {" breakout" :" interface breakout module 1 port 50 map 10g-4x" , " gateway" : " 172.16.1.1/24" , " modulesModel" : [" N9K-C93180YC-EX "]}
- {" modulesModel" : [" N9K-X9732C-EX" , " N9K-X9732C-EX" , " N9K-C9504-FM-E" , " N9K-C9504-FM-E" , " N9K-SUP-B" , " N9K-SC-A" , " N9K-SC-A"], " gateway" : " 172.29.171.1/24" , " breakout" :" interface breakout module 1 port 1,11,19 map 10g-4x; interface breakout module 1 port 7 map 25g-4x" }
- {" modulesModel" : [" N9K-C93180LC-EX"] 、 " gateway" : " 10.1.1.1/24" ," breakout" : " interface breakout module 1 port 1-4 map 10g-4x" 、 " portMode" : " hardware profile portmode 48x25G + 2x100G + 4x40G" }

1. **[**管理（**Manage**）**] > [**インベントリ（**Inventory**）**] > [**スイッチ（**Switches**）**]** の順にクリックします。
2. [スイッチ（Switch）] をクリックします。
3. **[**アクション（**Actions**）**] > [**スイッチを追加（**Add Switches**）**]** をクリックします。**[**スイッチの追加

（**Add Switches**）] ページが表示

されます。

4. **[**ファブリックの選択（**Choose Fabric**）**]**をクリックします。
   [ファブリックの選択（**Select Fabric**）**]** ダイアログボックスが表示されます。
5. ファブリックを選択し、**[**選択

   （**Select**）**]** をクリックします。

   [スイッチの追加（**Add**

   Switches）**]** ページが表示されま

   す。
6. **[**事前プロビジョニング（**Pre-provision**）**]** ラジオ ボタンを選択します。
7. **[**スイッチ ログイン情報（**Switch Credentials**）**]** の **[**管理者パスワード（**Admin password**）**]** フィールドに管理者パスワードを入力します。
8. ページの **[**事前プロビジョニングするスイッチ（**Switches to Pre-**

   provision）**]** 領域で、**[**アクション（**Actions**）**] > [**追加（**Add**）**]** の順にク

   リックします。**[**スイッチの事前プロビジョニング（**Pre-provision a**

   switch）**]** ダイアロブボックスが表示されます。
9. 表の説明に従って、必須フィールドに入力します。

フィールド	説明
シリアル番号（**Serial Number**）	スイッチのシリアル番号を指定します。
モデル	スイッチのモデル番号を指定します。
バージョン	スイッチのバージョン番号を指定します。
[IPアドレス（**IP Address**）**]**	スイッチの IP アドレスを指定します。
ホスト名	スイッチのホスト名を指定します。
イメージポリシー	ドロップダウン リストからイメージ ポリシーを指定します。
スイッチ ロール	ドロップダウン リストからスイッチ ロールを指定します。
ゲートウェイ（**Gateway**）	ゲートウェイ IP アドレスを指定します。
データ	JSON オブジェクトのデータを指定します。

10. **[**保存（**Save**）**]** をクリックします。
11. **[**アクション（**Actions**）**] > [**追加（**Add**）**]** をクリックして、スイッチを追加します。

    [追加（**Add**）**]** オプションを使用してスイッチを 1 つずつ追加するか、**[**インポート（**Import**）**]** オプションを使用して複数のスイッチを同時に追加できます。

[アクション（**Actions**）] > [追加（**Add**）] オプションを使用する場合は、[スイッチの事前プロビジョニング（**Pre-provision a switch**）] 必要な詳細をすべて入力してください。

12. [保存（**Save**）] をクリックします。

    [スイッチのログイン情報（ **Switch Credential**）] ページが表示されます。

13. [管理者パスワード（**Admin password**）] フィールドに管理者パスワードを入力します。
14. 事前プロビジョニングするスイッチをクリックします。
15. [事前プロビジョニング（**Pre-provision**）] をクリックします。

    事前プロビジョニングされたスイッチが追加されます。
    物理デバイスを持ち込むには、手動の RMA または POAP（PowerOn 自動プロビジョニング）RMA の手順に従います。

    詳細については、「返品許可（RMA）」を参照してください。 POAP RMA 手順を使用する場合は、存在しないデバイスへの接続がないことが予想されるため、接続がないためにデバイスをメンテナンス モードにできないというエラー メッセージを無視します。

POAP を使用した事前プロビジョニングされたデバイスの自動インポート

事前にプロビジョニングされたデバイスをファブリックに自動的にインポートできます。[管理（ **Admin**）]、[システム設定（**System Settings**）]、[サーバー設定（**Server Settings**）]、[**LAN-Fabric** （LAN-Fabric）] タブの [再プロビジョニング中に事前プロビジョニングされた スイッチを自動許可する（**Auto permit pre-provisionedswitch during re-poap**）] オプションを有効にすると、NDFC は PowerOn Auto Provisioning（POAP）を使用して、事前にプロビジョニングされたデバイスをファブリックに自動的にインポートします。[スイッチの追加（ブートストラップ）（**Add Switches (Bootstrap)**）] ページでユーザー名、パスワード、およびブートストラップ パラメータを再入力する必要がなくなります。

たとえば、実際のデバイスを受け取る前にテストデバイスを事前にプロビジョニングし、後でテストデバイスを実際のデバイスと交換する必要がある場合があります。

事前プロビジョニングされたデバイスの自動インポートの構成

1. [管理者（**Admin**）] > [システム設定（**System Settings**）] > [サーバー設定（**Server Settings**）] > [**LAN-Fabric**（**LAN-Fabric**）] に移動します。
2. [再プロビジョニング中に事前プロビジョニングされたスイッチを自動許可する（**Auto permit pre-provisionedswitch during re-poap**）] チェックボックスをオンにします。

   ヒ

   デフォルトでは、[再プロビジョニング中に事前プロビジョニングされたスイッチを自動許可する（**Auto admin pre-provisioned switch during re-poap**）] オプションは有効になっていません。

3. [保存（**Save**）] をクリックします。
4. [管理（**Manage**）] > [ファブリック（**Fabrics**）] に移動します。
5. VXLAN EVPN ファブリックをダブル

   クリックします。[ファブリックの概

要（**Fabric Overview**）] ページが表

示されます。

6. **[**アクション（**Actions**）] > **[**ファブリックの編集（**Edit Fabric**）] をクリックします。
7. **[VXLAN EVPN** マルチサイト（**VXLAN EVPN Multi-Site**）] をクリックします。

   [ファブリックの種類の選択（**Select Type of Fabric**）] ダイアログボックスが表示されます。

8. **[**データセンター **VXLAN EVPN**（**Data Center VXLAN EVPN**）] をクリックし、**[**選択（**Select**）] をクリックします。
9. **[**ブートストラップ（**Bootstrap**）] タブをクリックします。
10. **[**ブートストラップの有効化（**Enable Bootstrap**）] チェックボックスをオンにします。
11. **[**ローカル **DHCP** サーバーの有効化（**Enable Local DHCP Server**）] チェックボックスをオンにします。
12. **[DHCP** スコープ開始アドレス（**DHCP Scope Start Address**）]、**[DHCP**スコープ終了アドレス（**DHCP Scope End Address**）]、および **[**スイッチ管理デフォルト ゲートウェイ（**Switch Mgmt Default Gateway**）] フィールドに値を入力します。
13. **[**保存（**Save**）] をクリックします。
14. 「ファブリックの概要」に移動します。
15. **[**アクション（**Actions**）] > **[**スイッチを追加（**Add Switches**）] をクリックします。
    [スイッチの追加（**Add Switches**）] ページが表示されます。
16. **[**事前プロビジョニング（**Pre-provision**）] ラジオ ボタンを選択します。
17. **[**スイッチ ログイン情報（**Switch Credentials**）]領域 の **[**管理者パスワード（**Admin password**）] フィールドに管理者パスワードを入力します。
18. ページの **[**事前プロビジョニングするスイッチ（**Switches to Pre-**

    provision）] 領域で、**[**アクション（**Actions**）] > **[**追加（**Add**）] の順にク

    リックします。**[**スイッチの事前プロビジョニング（**Pre-provision a**

    switch）] ダイアロブボックスが表示されます。

19. 表の説明に従って、必須フィールドに入力します。

フィールド	説明
シリアル番号（**Serial Number**）	スイッチのシリアル番号を指定します。 テストデバイスに無効なシリアル番号を指定し、後で実際のデバイスが到着したときにシリアル番号を置き換えることができます。
モデル	スイッチのモデル番号を指定します。
バージョン	スイッチのバージョン番号を指定します。
[IPアドレス（**IP Address**）]	スイッチの IP アドレスを指定します。
ホスト名	スイッチのホスト名を指定します。

イメージポリシー	ドロップダウン リストからイメージ ポリシーを指定します。
スイッチ ロール	ドロップダウン リストからスイッチ ロールを指定します。
ゲートウェイ（**Gateway**）	ゲートウェイ IP アドレスを指定します。
データ	JSON オブジェクトのデータを指定します。

20. **[**選択したスイッチをインポート（**Import Selected Switches**）**]** をクリックします。

    NDFC はこのデバイスのエントリを自動的に保存し、後で NDFC はデバイスをファブリックに追加します。

    事前プロビジョニングされたデバイスがファブリックに自動的にインポートされ、**[**選択したスイッチのインポート（**Import Selected Switches**）**]** オプションがグレー表示されます。

    [ファブリックの概要（**Fabric Overview**）**] > [**スイッチ（**Switch**）**]** ページで、選択したデバイスのスイッチのステータスが **[**到達不能（**Unreachable**）] から **[OK]**
    [OK] に変わります。

イーサネット インターフェイスの事前プロビジョニング

始める前に：

ファブリックに事前にプロビジョニングされたデバイスがあることを確認してください。詳細については、「 デバイスの事前 プロビジョニング」を参照してください。

[LAN インターフェイス（**LAN Interface**）**]** ウィンドウでイーサネット インターフェイスを事前プロビジョニングできます。この事前プロビジョニング機能は、Easy、外部、および eBGP ファブリックでサポートされています。イーサネット インターフェイスを追加できるのは、

NDFC で検出される前に、事前にプロビジョニングされたデバイスだけです。

ネットワーク/VRF を接続する前に、イーサネット インターフェイスを
ポート チャネル、vPC、ST FEX、AAFEX、ループバック、サブインターフェイス、トンネル、
イーサネット、および SVI 構成に追加する前に、事前プロビジョニングする必要があり
ます。

1. [LAN ファブリック（LAN Fabrics）] ウィンドウから事前にプロビジョニングされたデバイスを含

   むファブリックをダブルクリックします。**[**ファブリックの概要（**Fabric Overview**）**]** ウィンドウ

   が表示されます。

2. **[**インターフェイス（**Interfaces**）**]** タブで、**[**アクション

   （**Actions**）**] > [**インターフェイスの作成（**Create**

   Interface）**]** をクリックします。**[**インターフェイスの作

   成（**Create Interfaces**）**]** ウィンドウが表示されます。

3. **[**インターフェイスの作成（**Create Interface**）**]** ウィンドウで、必要なすべての詳細を入力します。

   [タイプ（**Type**）**]** : ドロップダウン リストから **[**イーサネット（**Ethernet**）**]** を選択します。

   [デバイスの選択（**Select a device**）**]** : 事前にプロビジョニングされたデバイスを選択します。

   すでに管理されているデバイスにイーサネット インターフェイスを追加することはでき
   ません。

   [インターフェイス名（**Interface Name**）**]** : モジュール タイプに基づいて有効なインターフェイス名を入力します。たとえば、Ethernet1/1、eth1/1、または e1/1 です。同じ名前のインターフェイスが、追加後にデバイスで使用できるようになります。

   [ポリシー（**Policy**）**]** : インターフェイスに適用する必要があるポリシーを選択します。

4. **[**保存（**Save**）**]** をクリックします。
5. **[**プレビュー（**Preview**）**]** をクリックして、追加後にスイッチに展開される予定の構成を確認します。

   デバイスは事前にプロビジョニングされているため、**[**展開（**Deploy**）**]** ボタンはイーサ
   ネット インターフェイスでは無効になっています。

vPC ペアの事前プロビジョニング

始める前に：

[ファブリックの設定（Fabric Settings）] で**[**ブートストラップ（**Bootstrap**）**]**が有効になっていることを確認します。

1. 両方のデバイスをファブリックにインポートします。詳細については、「デバイスの事前プロビジョニング」を参照してください。

   事前にプロビジョニングされ、既存のファブリックに追加された 2 台の Cisco Nexus 9000 シリーズ デバイス。**[**スイッチの追加（**Add Switches**）**]** を **[**アクション（**Actions**）**]** ドロップダウン リスト

から追加します。[インベントリ管理（**Inventory Management**）] 画面で、[パワーオン自動プロビジョニング（**PowerOn Auto Provisioning**、**POAP**）] をクリックします。

デバイスは、ファブリック内に灰色の/未検出デバイスとして表示されます。

2. 右クリックして、他の到達可能なデバイスと同様に、これらのデバイスの適切な役割を選択します。
3. 物理ピア リンクまたは MCT を持つデバイス間に vPC ペアリングを作成するには、次の手順を実行します。
   a. ピア リンクを形成する物理イーサネット インターフェイスをプロビジョニングします。

      leaf1-leaf2 間の vPC ピア リンクは、各デバイスのインターフェイス Ethernet1/44-45 で構成されます。[管理（**Manage**）] > [ファブリック（**Fabrics**）] > [インターフェイス（**Interfaces**）] を選択して、イーサネット インターフェイスを事前プロビジョニングします。

      詳細については、「イーサネット インターフェイスの事前プロビジョニング」を参照してください。

   b. これらのインターフェイス間に事前にプロビジョニングさ

      れたリンクを作成します。[リンク（Links）] タブで、[ア

      クション（Actions）] > [作成（Create）] をクリックし

      ます。

      2 つのリンクを作成します。1 つは、leaf1-Ethernet1/44 から leaf2-Ethernet1/44 へ、もう 1 つは、leaf1-Ethernet1/45 から leaf2-Ethernet1/45 へのリンクです。

      リンク テンプレートとして **int_pre_provision_intra_fabric_link** を選択していることを確認してください。送信元インターフェイスと宛先インターフェイスのフィールド名は、前の手順で事前にプロビジョニングされたイーサネット インターフェイスと一致している必要があります。

      リンクが作成されると、それらは [リンク（**Links**）] タブ（[ファブリックの概要（**Fabric Overview**）] ウィンドウ）にリスト表示されます。

   c. [トポロジ（**Topology**）] ウィンドウで、スイッチを右クリックし、ドロップダウン リストから [**vPC** ペアリング（**vPC Pairing**）] を選択します。

      vPC ペアを選択し、事前プロビジョニングされたデバイスの [vPC ペアリング（vPC pairing）] をクリックします。

   d. [再計算と展開（**Recalculate & Deploy**）] をクリックして、事前にプロビジョニングされたデバイスに必要な目的の vPC ペアリング構成を生成します。

      完了すると、デバイスは正しくペアリングされ、デバイスの vPC ペアリング インテントが生成され、ポリシーが生成されます。

      > デバイスはまだ動作していないため、構成コンプライアンスはこれらのデバイスの同期（IN-SYNC）または非同期（OUT-OF-SYNC）ステータスを返しません。
      >
      > これは、CC がデバイスからの実行コンフィギュレーションを順番に要求するためです。を使用してインテントと比較し、コンプライアンスステータスを計算して報告します。

vPC ホスト インターフェイスの事前プロビジョニング

1. 事前プロビジョニングされたデバイスに物理イーサネット インターフェイスを作成します。

   スイッチの通常の vPC ペアと同様の vPC ホスト インターフェイスを追加します。詳細については、「イーサネット インターフェイスの事前 プロビジョニング」を参照してください。

   たとえば、leaf1-leaf2 は、事前プロビジョニングされた vPC デバイス ペアを表します。ただし、イーサネット インターフェイス 1/1 は、leaf1 と leaf2 の両方で事前プロビジョニングされているものとします。

2. vPC ホスト トランク インターフェイスを作成します。

   vPC ホスト インターフェイスが作成され、ステータスが **[未検出（Not discovered）]** と表示されます。**[プレビュー（Preview）]** と **[展開（Deploy）]** アクションは、どちらもデバイスが存在する必要があるため、結果を生成しません。

事前にプロビジョニングされたデバイスへのオーバーレイのアタッチ

オーバーレイ VRF とネットワークは、他の検出されたデバイスと同様に、事前にプロビジョニングされたデバイスにアタッチできます。

オーバーレイ ネットワークは、事前にプロビジョニングされたリーフの vPC ペア（leaf1-leaf2）にアタッチされます。また、leaf1-leaf2 で作成され、事前にプロビジョニングされた vPC ホスト インターフェイス ポート チャネルにもアタッチされます。

デバイスに到達できないため、事前にプロビジョニングされたデバイスのプレビューおよび展開操作は無効になっています。事前にプロビジョニングされたデバイスに到達できるようになると、他の検出されたデバイスと同様に、すべての操作が有効になります。

[ファブリックの概要（**Fabric Overview**）**]** ウィンドウで、**[**ポリシー（**Policies**）**]** タブをクリックし、**[**アクション（**Actions**）**] > [**ポリシーの編集（**Edit Policy**）**]** をクリックします。オーバーレイ ネットワーク/VRF アタッチメント情報を含む、事前にプロビジョニングされたデバイス用に生成されたインテント全体を表示できます。

スイッチのプレビュー

UI ナビゲーション

- **[**管理（**Manage**）**] > [**インベントリ（**Inventory**）**] > [**スイッチ（**Switches**）**]** の順に選択します。
- **[**管理（**Manage**）**] > [**ファブリック（**Fabrics**）**]**の順に選択します。ファブリックをクリックして **[**ファブリック サマリ（**Fabric Summary**）**]** スライドイン ペインを開きます。
  [起動（**Launch**）**]** アイコンをクリックします。 **[**ファブリックの概要（**Fabric Overview**）**] > [**スイッチ（**Switches**）**]** を選択します。

スイッチを追加した後、保留中の設定、実行構成の並列比較、およびスイッチの予想される設定を含むスイッチをプレビューできます。複数のスイッチを選択して、同じインスタンスでプレビューできます。**[**プレビュー（**Preview**）**]** ウィンドウに、スイッチの正常な展開の保留中の構成が表示されます。

スイッチをプレビューし、保留中の構成と再同期するには、次の手順を実行します。

1. **[**スイッチ（**Switches**）**]** ウィンドウで、スイッチの横にあるチェックボックスを使用して、プレビューするスイッチを選択します。**[**アクション（**Actions**）**]** ドロップダウンリストから、**[**プレビュー（**Preview**）**]** を選択します。

   [構成のプレビュー（**Preview Config**）**]** ウィンドウが表示されます。このウィンドウには、スイッチ名（そのIPアドレス、ロール、シリアル番号、ファブリックのステータス（同期中、同期外、または使用不可）。保留中の構成。ステータスの説明。進捗状況など）のスイッチ設定情報が表示されます。

2. 構成のみをプレビューするには、表示された情報を表示して、**[**閉じる（**Close**）**]** をクリックします。
3. 保留中の構成でスイッチを再同期するには、**[**再同期（**Resync**）**]** をクリックします。経過表示バーに再同期の進捗が表示されます。**[**閉じる（**Close**）**]** をクリックして、**[**構成のプレビュー（**Preview Config**）**]** ウィンドウを閉じます。
4. 保留中の構成と比較を表示するには、
   [保留中の構成（**Pending Config**）**]** 列のそれぞれのリンクをクリックします。

   または、**[**ファブリックの概要アクション（**Fabric Overview Actions**）**]** ドロップダウン リストで、**[**構成の再計算（**Recalculate Config**）**]** を選択します。**[**構成の展開（**Deploy Configuration**）**]** ウィンドウが表示されます。スイッチの構成ステータスが表示されます。**[**保留中の構成（**Pending Config**）**]** 列のそれぞれのリンクをクリックして、保留中の構成を表示することもできます。

   [保留中の構成（**Pending Config**）**]** ウィンドウが表示されます。このウィンドウの **[**保留中の構成（**Pending Config**）**]** タブには、スイッチの保留中の構成が表示されます。**[**並べて比較（**Side-by-Side Comparison**）**]** タブには、実行中の構成と予想される構成が並べて表示されます。

   [保留中の構成（**Pending Config**）**]** ウィンドウを閉じます。

設定の導入

この展開オプションは、スイッチのローカル操作です。つまり、スイッチの予想される構成またはインテントが現在の実行構成に対して評価され、構成のコンプライアンス チェックが実行されて、スイッチが **In-Sync** または **Out-of-Sync** ステータスを取得します。スイッチが同期していない場合、ユーザには、その特定のスイッチで実行されているすべての設定のプレビューが提供されます。これらの設定は、それぞれのスイッチに対してユーザが定義した意図とは異なります。

1. 必要なスイッチを選択し、 **[**アクション（**Actions**）**] > [**展開（**Deploy**）**]** を選択してスイッチに設定を展開します。**[**構成の展開（**Deploy Configuration**）**]** ウィンドウが表示されます。
2. **[**再同期（**Resync**）**]** をクリックして構成を同期します。
3. **[**展開（**Deploy**）**]** をクリックします。

   [ステータス（Status）] カラムには、「FAILED」または「SUCCESS」の状態が表示されます。FAILED ステータスの場合は、問題の解決に失敗した理由を調査します。
4. **[**閉じる（**Close**）**]** をクリックして、ウィンドウを切り替えます。

ディスカバリ

この章は、次の項で構成されています。

クレデンシャル情報の更新

検出スイッチを更新するには、検出ログイン情報の更新を使用します。

1. 必要なスイッチを選択し、 **[**アクション（**Actions**）**] > [**検出（**Discovery**）**] >**

   [ログイン情報の更新（**Update Credentials**）**]** の順に選択します。**[**検出のログ

   イン情報の更新（**Update Discovery Credentials**）**]** ウィンドウが表示されま

   す。

2. **[**検出ログイン情報の更新（**Update Discovery Credentials**）**]**ウィンドウで、検出ユーザー名やパスワードなどの検出ログイン情報を入力します。
3. **[**更新（**Update**）**]** をクリックして、検出ログイン情報を保存します。

   ディスカバリ ログイン情報が指定されていない場合は、Nexus Dashboard Fabric Controller は管理者ユーザーとパスワードを使用してスイッチを検出します。

再検出

スイッチを再検出し、そのステータスを確認できます。

スイッチを再検出するには、次の手順を実行します。

- 必要なスイッチを選択し、 **[**アクション（**Actions**）**] > [**検出（**Discovery**）**] > [**再検出（**Rediscover**）**]** を選択してスイッチを再検出します。

  [検出ステータス（**Discovery Status**）**]** 列にステータスが **[**再検出中（**Rediscovering**）**]**として表示され、検出後にステータスが表示されます。

検出 **IP** アドレスの変更に関する注意事項と制約事項

Cisco Nexus Dashboard ファブリック コントローラ リリース 12.0.1a から、ファブリックに存在するデバイスの検出 IP アドレスを変更できます。

注意事項と制約事項

以下は、検出 IP アドレスの変更に関する注意事項と制約事項です。

- 検出 IP アドレスの変更は、管理インターフェイスを介して検出された NX-OS スイッチおよびデバイスでサポートされます。
- 検出 IP アドレスの変更は、次のようなテンプレートでサポートされます。
  - データセンター VXLAN EVPN
  - BGP ファブリック
  - 外部
  - 従来の LAN

- LAN モニター

- 検出 IP アドレスの変更は、管理モードとモニタ モードの両方でサポートされています。
- Cisco Fabric Controller UI で検出 IP アドレスを変更できるのは、**network-admin** ロールを持つユーザだけです。
- 検出 IPアドレスは、他のデバイスでは使用できず、変更が完了したときに到達可能である必要があります。
- 管理対象ファブリック内のデバイスの検出 IP アドレスを変更している間、スイッチは移行モードになります。
- vPC ピアにリンクされているスイッチの IP アドレス（vPC ピアなどの対応する変更）を変更すると、それに応じてドメイン設定が更新されます。
- ファブリック構成は元の IP アドレスを復元し、復元後の同期外れを報告し、同期ステータスを取得するにはデバイスの構成インテントを手動で更新する必要があります。
- 元のデバイス検出 IP を使用していたファブリック コントローラの復元は、スイッチを到達不能ポスト復元として報告します。検出 IP アドレスの変更手順は、復元後に繰り返す必要があります。
- 元の検出 IP アドレスに関連付けられているデバイス アラームは、IPアドレスの変更後に消去されます。

検出 IP アドレスの変更

始める前に：

デバイスで管理 IP アドレスとルート関連の変更を行い、Nexus Dashboard ファブリック コントローラからデバイスの到達可能性を確認する必要があります。

Cisco Nexus Dashboard ファブリック コントローラ Web UI から検出 IP アドレスを変更するには、次の手順を実行します。

1. **[**管理（**Manage**）**] > [**ファブリック（**Fabrics**）**]** の順に選択します。
2. ファブリック名をクリックして、必要なスイッチを

   表示します。**[**ファブリック サマリ（**Fabric**

   summary）**]** スライドイン ペインが表示されます。

3. **[**起動（**Launch**）**]** アイコンをクリックして、**[**ファブリックの概要（**Fabric Overview**）**]** ウィンドウを表示します。
4. **[**スイッチ（**Switches**）**]**タブで、メイン ウィンドウの **[**アクション（**Action**）**]** ボタンの横に

   ある **[**最新表示（**Refresh**）**]** アイコンをクリックします。IP アドレスが変更されたスイッチは、

   [検出ステータス（**Discovery Status**）**]** 列で到達不能状態になります。

5. **[**スイッチ（**Switch**）**]** 列の横にあるチェックボックスをクリックし、スイッチを選択します。

   ヒ　複数のスイッチではなく、個々のスイッチの IP アドレスを変更できます。

6. [スイッチ（Switches）] タブ領域で **[**アクション（**Actions**）**] > [**検

   出 **IP** の変更（**Change Discovery IP**）**]** を選択します。**[**検出 **IP** の変

   更（**Change Discovery IP**）**]** ウィンドウが表示されます。

同様に、**[管理（Manage）] > [インベントリ（Inventory）] > [スイッチ（Switches）]** タブから移動できます。必要なスイッチを選択し、**[アクション（Actions）] > [検出（Discovery）] > [検出 IP の変更（Change Discovery IP）]** をクリックします。

7. **[新規 IP アドレス（New IP Address）]** テキスト フィールドに適切な IP アドレスを入力し、**[OK]** をクリックします。
   a. 正常に更新するには、新しい IP アドレスが Nexus Dashboard Fabric Controller から到達可能である必要があります。
   b. 次の手順に進む前に、検出 IP アドレスを変更する必要があるデバイスに対して上記の手順を繰り返します。
   c. ファブリックが管理対象モードの場合、デバイス モードは移行モードに更新されます。
8. ファブリックの **[アクション（Actions）]** ドロップダウン リストから、**[構成の再計算（Recalculate Config）]** をクリックして、デバイスの Nexus Dashboard Fabric Controller 構成インテントの更新プロセスを開始します。同様に、トポロジ ウィンドウで構成を再計算できます。**[トポロジ（Topology）]** を選択し、スイッチを右クリックして **[構成の再計算（Recalculate Config）]** をクリックします。

   デバイス管理関連の構成の Nexus Dashboard ファブリック コントローラ構成インテントが更新され、スイッチのデバイス モード ステータスが通常モードに変更されます。スイッチの構成ステータスは **[同期中（In-Sync）]** と表示されます。

ヒ 古いスイッチの IP アドレスに関連付けられた PM レコードは消去され、新しいレコードの収集は変更後 1 時間かかります。

VRFの更新

スイッチの Discovery VRF を更新するには、次の手順を実行します。

VRF の更新オプションを有効にする と、
スイッチの検出 IP アドレスを持つインターフェイスに関連付けられた VRF が、スイッチのインポート中にNDFCで自動的に検出されます。必要なスイッチの VRF 設定は、適切なユーザー ロールで上書きできます。

1. 必要なスイッチを選択し、 **[アクション（Actions）] > [検出**

   （Discovery）] > [VRFの更新（Update VRF）] の順に選択します。**[検**

   出 VRF の更新（Update Discovery VRF）] ウィンドウが表示されます。

2. **[検出 VRF の更新（Update Discovery VRF）]** ウィンドウで、ドロップダウン リストから **[新規 VRF（New VRF）]**と**[インターフェイス（Interface）]** を選択します。
3. **[OK]** をクリックして、新しい VRF の詳細を保存します。

検出ステータス

次の表に、スイッチ ディスカバリ ステータス文字列とその説明を示します。

タイプ	**Discovery** ステータス文字列	説明
検出	検出中（Discovering）	スイッチは検出中です。初期検出に適用されます
Discovery	OK	スイッチは良好な状態です
Discovery	再検出中	スイッチは再検出中です
Discovery	デバイスをシャットダウンしています	スイッチがシャットダウンしています
Discovery	到達不要	スイッチ IP が ping できない
Discovery	IP アドレスの変更	スイッチの IP の更新中
Discovery	スイッチ キーの不一致	スイッチ RMA が進行中です。
Discovery	検出タイムアウト	スイッチの検出が設定された検出タイムアウト（デフォルト：5 分）内に完了しませんでした
Discovery	セッション エラー（コード：100）。再試行しています。	sim-master サービスが内部サーバー エラーを返したため、検出に失敗しました
Discovery	セッション エラー（コード：101）。再試行しています。	SIM マスター サービスの準備ができていないため、検出に失敗しました
Discovery	セッション エラー（コード：102）。再試行しています。	ジョブの実行中に sim-master サービスが再起動されたため、検出に失敗しました
Discovery	セッション エラー（コード：103）。再試行しています。	SIM マスター サービスに到達できないため、検出に失敗しました
Discovery	セッション エラー（コード：104）。再試行しています。	sim-agent サービスの再起動後に検出に失敗しました
Discovery	セッション エラー（コード：105）。再試行しています。	構成テンプレート サービスの準備ができていないため、検出に失敗しました
Discovery	セッション エラー（コード：106）。再試行しています。	LAN 検出ログイン情報が見つからないため、検出に失敗しました
Discovery	SSH セッション エラー	sim-agentで SSH セッション エラー（または）HTTP タイムアウトが発生したため、検出に失敗しました
SNMP	未知のユーザー名または不良なパスワード	SNMP ユーザー名および/またはパスワードが正しくありません
SNMP	タイムアウト（Timeout）	SNMP がタイムアウトを返します（デフォルト：10 秒）
SNMP	IP 接続に失敗しました	セッションの作成中に SNMP ConnectException が発生しました

SNMP	IP SNMP ソケット タイムアウト	セッションの作成中に SNMP SocketTimeoutException が発生しました
タイプ	**Discovery** ステータス文字列	説明
SNMP	IP GetSocket が失敗しました	セッションの作成中に SNMP IOException が発生しました

スイッチ ロールの割り当て

Nexus Dashboard Fabric Controller のスイッチにロールを割り当てることができます。

1. 必要なスイッチを選択し、**[アクション（Actions）] > [セット ロール]** を選択します。
2. **[ロールの選択]** ウィンドウが表示されます。必要なロールを選択し、**[選択（Select）]**

   をクリックします。確認ウィンドウが表示されます。

ヒ [ロール ステータス（Role Status）] 列に新しいロールの割り当てを表示するには、スイッチを再検出する必要があります。

NDFC 展開の実行時にボーダーデバイスに L2-VNI/SVI を追加する必要がある場合は、次の パス に従い ます 。[ネットワーク （ ファブリック レベル）] を選択 し、[展開する必要があるネットワークを選択] > [編集] > [詳細] > [境界上の L3 ゲートウェイ] を有効にします。

Cisco Nexus Dashboard Fabric Controller では、次のロールがサポートされています。

- スパイン
- リーフ
- 境界
- ボーダースパイン
- ボーダーゲートウェイ
- ボーダー ゲートウェイ スパイン
- スーパー スパイン
- ボーダー スーパー スパイン
- ボーダー ゲートウェイ スーパー スパイン
- アクセス
- 集約
- エッジ ルータ
- コア ルータ
- TOR

スーパー スパイン スイッチ ロールのサポート

スーパー スパインは、複数のスパイン リーフ POD を相互接続するために使用されるデバイスです。スーパー スパインを使用した追加の相互接続オプションがあります。スーパー スパインを介して相互接続された同じ Easy ファブリック内に複数のスパイン リーフ POD を持つことができ、同じ IGP ドメインがスーパー スパインを含むすべての POD にまたがって拡張されます。このような展開では、BGP RR と RP（該当する場合）がスーパー スパイン レイヤでプロビジョニングされます。スパイン レイヤは、リーフとスーパー スパイン間の疑似相互接続になります。VTEP にボーダー機能がある場合は、オプションでスーパー スパインでホストできます。

NDFC では、次のスーパー スパイン スイッチのロールがサポートされています。

- スーパースパイン
- ボーダースーパースパイン
- ボーダー ゲートウェイ スーパー スパイン

ボーダー スーパー スパインは、スーパー スパイン、RR、RP（オプション）、ボーダー リーフの機能を含む複数の機能を処理します。同様に、ボーダー ゲートウェイのスーパー スパインは、スーパー スパイン、RR、RP（オプション）、およびボーダー ゲートウェイにサービスを提供します。スーパー スパインまたは RR レイヤでボーダー機能をオーバーロードすることはお勧めしません。代わりに、ボーダー リーフまたはボーダー ゲートウェイを外部接続用のスーパー スパイン レイヤに接続します。スーパー スパイン レイヤは、RR または RP 機能との相互接続として機能します。

NDFC のスーパー スパイン スイッチのロールの特徴は次のとおりです。

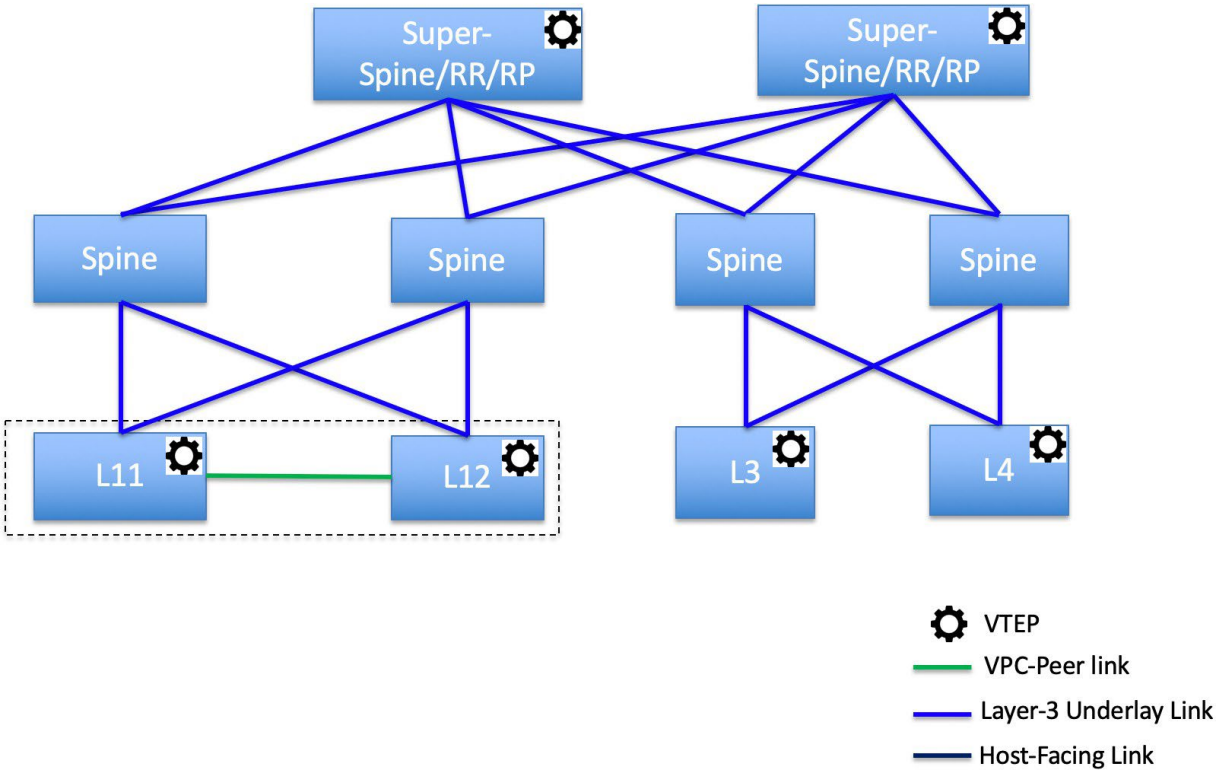
- Easy ファブリックでのみサポートされます。
- Cisco NDFC リリース 12.1.1e 以降、**BGP** ファブリック テンプレートを使用した IPv6 アンダーレイの eBGP ルーテッド ファブリックで、スーパー スパイン スイッチ ロールとボーダー スーパー スパイン スイッチ ロールもサポートされています。
- スパインとボーダーにのみ接続できます。有効な接続は次のとおりです。
  - スパインからスーパー スパインへ
  - スパインからボーダー スーパー スパインおよびボーダー ゲートウェイ スーパー スパインへ
  - スーパー スパインからボーダー リーフおよびボーダー ゲートウェイ リーフへ
- RR または RP（該当する場合）機能は、ファブリックに存在する場合、常にスーパー スパイン上で構成されます。スーパー スパインでも最大 4 つの RR および RP がサポートされます。
- ボーダー スーパー スパインおよびボーダー ゲートウェイ スーパー スパインのロールは、ファブリック間接続でサポートされます。
- スーパー スパインでは vPC 構成はサポートされていません。
- スーパー スパインは IPv6 アンダーレイ構成をサポートしていません。
- スイッチにスーパー スパイン ロールがある場合、スイッチのブラウンフィールド インポート中に、次のエラーが表示されます。

  シリアル番号：[スーパー スパイン/ボーダー スーパー スパイン/ボーダー ゲートウェイ スーパースパイン] ロールは、保持された構成の yes オプションではサポートされていません。

スーパー スパイン スイッチでサポートされるトポロジ

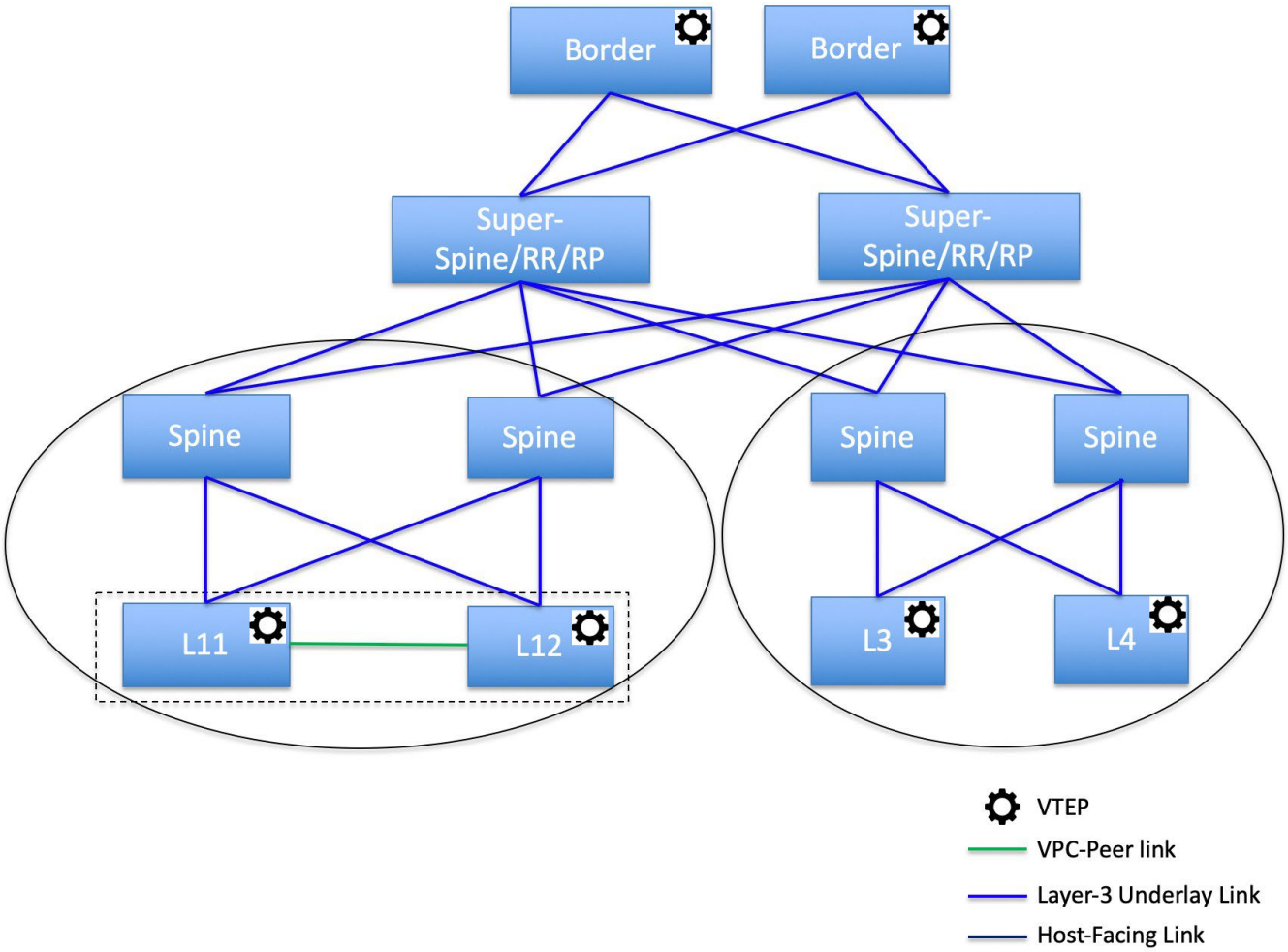
NDFC は、スーパー スパイン スイッチで次のトポロジをサポートします。

トポロジ **1**：スパイン リーフ トポロジのスーパー スパイン スイッチ



このトポロジでは、リーフ スイッチはスパインに接続され、スパインはスーパー スパイン スイッチに接続されます。このスイッチはスーパー スパイン、ボーダー スーパー スパイン、およびボーダー ゲートウェイ スーパー スパインであり得ます。

トポロジ **2**：ボーダーに接続されたスーパー スパイン スイッチ



このトポロジでは、2 つのスーパー スパイン スイッチに接続されているスパイン スイッチがあり、それらに接続されている 4 つのリーフ スイッチがあります。これらのスーパー スパイン スイッチは、ボーダーまたはボーダー ゲートウェイ リーフ スイッチに接続されます。

vPC セットアップの作成

外部ファブリック内のスイッチのペアに対して vPC セットアップを作成できます。スイッチの役割が同じで、相互に接続されていることを確認します。

1. 2 つの指定された **vPC** スイッチのいずれかを右クリックし、**[vPC** ペアリング**]** を選択します。

   [vPC ピアの選択（**Select vPC peer**）**]** ダイアログボックスが表示されます。潜在的なピア スイッチのリストが含まれます。vPC ピア スイッチの**[**推奨（**Recommended**）**]**列が **[true]** に更新されていることを確認します。

   ヒ

   または、**[**アクション（**Actions**）**]** ペインから表形式ビューに移動することもできます。**[**スイッチ（**Switches**）**]** タブでスイッチを選択し、**[vPC Pairing**（**vPC** ペアリング）**]**をクリックして vPC ペアを作成、編集、またはペアリング解除します。ただし、このオプションは、Cisco Nexus スイッチを選択した場合にのみ使用できます。

2. vPC ピアスイッチの横にあるオプションボタンをクリックし、**[vPC** ペア テンプレート（**vPC Pair Template**）**]** ドロップダウンリストから **vpc_pair** を選択します。ここには、**VPC_PAIR** テンプレートサブタイプのテンプレートのみが表示されます。

   [vPC ドメイン（**vPC Domain**）**]** タブと **[vPC** ピアリンク（**vPC Peerlink**）**]** タブが表示されます。vPC 設定を作成するには、タブのフィールドに入力する必要があります。各フィールドの説明は、右端に表示されます。

   [vPC ドメイン（**vPC Domain**）**]** タブ：vPC ドメインの詳細を入力します。

   [vPC+]：スイッチが FabricPath vPC+ セットアップの一部である場合は、このチェックボックスをオンにして
   [FabricPath スイッチ **ID]** フィールドに入力します。

   [VTEP の構成（**Configure VTEPs**）**]**：2 つの vPC ピア VTEP の送信元ループバック IP アドレスと、NVE 設定のループバック インターフェイス セカンダリ IP アドレスを入力します。

   [NVE インターフェイス（**NVE interface**）]：NVE インターフェイスを入力します。 vPC ペアリングでは、送信元ループバック インターフェイスのみが設定されます。追加構成には、自由形式のインターフェイス マネージャを使用します。

   [NVE ループバック構成（NVE loopback configuration）]：IP アドレスをマスクで入力します。 vPC ペアリングは、ループバック インターフェイスのプライマリおよびセカンダリ IP アドレスのみを構成します。追加構成には、自由形式のインターフェイス マネージャを使用します。

   [vPC ピアリンク（**vPC Peerlink**）**]**タブ：vPCピアリンクの詳細を入力します。

   [スイッチポート モード（**Switch Port Mode**）**]**：**trunk** または **access** または **fabricpath** を選択します。

   トランクを選択すると、対応するフィールド（**[**トランク許可 **VLAN**（**Trunk Allowed VLANs**）**]** および **[**ネイティブ **VLAN**（**Native VLAN**）**]**）が有効になります。**access** を選択すると、**[VLAN** にアクセス（**Access VLAN**）**]** フィールドが有効になります。**fabricpath** を選択すると、トランクおよびアクセスポート関連のフィールドは無効になります。

3. **[**保存（**Save**）**]** をクリックします。

   vPC セットアップが作成されます。

vPC セットアップの詳細を更新するには、次の手順を実行します。

a. vPC スイッチを右クリックし、[vPC ペアリング] を

選択します。**[vPC** ピア（**vPC peer**）**]** ダイアログ

ボックスが表示されます。

b. 必要に応じて、次のフィールドを更新します。

フィールドを更新すると、**[**ペアリング解除（**Unpair**）**]** アイコンが **[**保存（**Save**）**]** に変わります。

c. **[**保存（**Save**）**]** をクリックして更新を完了します。

vPC ペアを作成すると、**[vPC** の概要（**vPC Overview**）**]** ウィンドウで vPC の詳細を表示できます。

vPC セットアップの展開解除

1. **vPC** スイッチを右クリックし、**[vPC** ペアリング**]** を

   選択します。vPC ピア画面が表示されます。

2. 画面の右下にある **[**ペアリング解除（**Unpair**）**]** をクリックします。

   vPC ペアが削除され、ファブリック トポロジ ウィンドウが表示されます。

3. **[**構成の展開（**Deploy Config**）**]** をクリックします。
4. **[**構成の再計算（**Recalculate Config**）**]** 列の値をクリックします。

   [構成プレビュー**]** ダイアログボックスで保留中の構成を表示します。vPC 機能、vPC ドメイン、vPC ピアリンク、vPC ピアリンク メンバー ポート、ループバックセカンダリ IP、およびホスト vPC のペアリングを解除すると、スイッチの次の設定の詳細が削除されます。ただし、ホスト vPC とポート チャネルは削除されません。必要に応じて、**[**インターフェイス（**Interfaces**）**]** ウィンドウからこれらのポート チャネルを削除します。

同期していない場合は、ファブリックを再同期します。

ペアリングを解除すると、次の機能の PTI のみが削除されますが、構成の展開中に設定がクリアされません。NVE 設定、LACP 機能、ファブリック パス機能、nv オーバーレイ機能、ループバック プライマリ ID です。ホスト vPC の場合、

ポート チャネルとそのメンバー ポートはクリアされません。 これらの ポート チャネルを削除 でき ます

必要に応じて、**[**インターフェイス（**Interfaces**）**]** ウィンドウからこれらのポート チャネルを削除します。ペアリングを解除した後でも、スイッチでこれらの機能を引き続き使用できます。

fabricpath から VXLAN に移行する場合は、VXLAN 設定を展開する前にデバイスの設定をクリアする必要があります。

より高い

スイッチでのアクションの実行

モード変更

スイッチのモードを変更するには、次の手順を実行します。

1. **[管理（Manage）] > [**ファブリック（**Fabrics**）**]** に移動します。
2. VXLAN EVPN ファブリックをクリックします。

   [ファブリック サマリ（Fabric summary）] スライドイン ペインが表示されます。

3. **[起動 (Launch)]** アイコンをクリックします。

   [ファブリックの概要（**Fabric Overview**）**]** ページが表示されます。

4. **[**スイッチ（**Switches**）**]** タブをクリックします。
5. モードを変更するスイッチのチェックボックスをクリックします。
6. **[**アクション（**Actions**）**] > [**詳細

   （**More**）**]> [**モードの 変更（**Change**

   Mode）**]** の順に選択します。**[**モードの変

   更（**Change Mode**）**]** ダイアログボックス

   が表示されます。

7. ドロップダウンリストから **[**メンテナンス（**Maintenance**）**]** をクリックしてメンテナンスモードに変更するか、**[**通常（**Normal**）**]** をクリックして通常モードに変更します。
8. **[**今すぐ展開（**Deploy Now**）**]** をクリックしてモードを今すぐ変更するか、**[**後で展開（**Deploy Later**）**]** をクリックしてモードを後で変更します。

スイッチによるモード変更の待機

[ファブリックの概要（ **Fabric Overview**）**] > [**スイッチ（**Switches** ）**]** ページから **[**展開時にスイッチモードの変更を待機する（ **Wait for switch mode change to maintenance on deploy**） **]** オプションを有効にするか、**[**管理（ **Manage**）**] > [**インベントリ（**Inventory**）**] > [**スイッチ（**Inventory**）**]** ページの **[**アクション（**Actions**）**]** ドロップダウン リストを有効にするか、スイッチ（**Switches**）**]** ページの [管理（Manage）] > [インベントリ（Inventory）] > [スイッチ（Switches）] ページの **[**アクション（ **Actions**）**]** ドロップダウン リストから有効にするか、またはファブリックをダブルクリックして **[**トポロジ（**Topology**）**]** ページのスイッチにアクセスします。次に、スイッチを右クリックし、**[**詳細（**More**）**] > [**モードの変更（**Change Mode**）**]** の順にクリックして、**[**モードの変更（**Change Mode**）**]** ダイアログボックスにアクセスします。

スイッチによるモード変更待機の制限事項

- サポートは Cisco NX-OS デバイスに対してのみ提供されます。
- Catalyst または Catalyst 9K スイッチはサポート対象外です。Cisco NX-OS 以外のデバイスのモードを変更しようとすると、エラー メッセージが表示されます。
- 変更制御を使用してスイッチのモードを変更することはできません。

スイッチのモードの変更待機を有効にするには、次の手順を実行します。

1. **[**管理（**Manage**）**] > [**ファブリック（**Fabrics**）**]** に移動します。
2. VXLAN EVPN ファブリックをクリックします。

   [ファブリック サマリ（Fabric summary）] スライドイン ペインが表示されます。

3. **[**起動 **(Launch)]** アイコンをクリックします。

   [ファブリックの概要（**Fabric Overview**）**]** ページが表示されます。
4. **[**スイッチ（**Switches**）**]** タブをクリックします。
5. モードを変更するスイッチのチェックボックスをクリックします。
6. **[**アクション（**Actions**）**] > [**モードの変

   更（**Change Mode**）**]** をクリックしま

   す。**[**モードの変更（**Change Mode**）**]**

   ダイアログボックスが表示されます。

7. ドロップダウンリストから **[**メンテナンス（**Maintenance**）**]** をクリックしてメンテナンスモードに変更するか、**[**通常（**Normal**）**]** をクリックして通常モードに変更します。
8. **[**展開時にスイッチ モードのメンテナンスへの変更を待機する（**Wait for switch mode change to maintenance on deploy**）**]** チェックボックスをクリックします。
9. **[**今すぐ展開（**Deploy Now**） **]** ボタンをクリックして、スイッチ モードを変更します。

   [展開時にスイッチ モードの変更のメンテナンスに待機する（**Wait for switch mode change to maintenance on deploy**）**]** チェックボックスを有効にしたため、**[**後で展開（**Deploy Later**）**]** オプションがグレー表示されます。NDFC は、このチェックボックスに対するユーザーの最後のアクションを保持します。

モード変更プロセスが完了するまでに 2 ~ 3 分かかる場合があります。

RMA のプロビジョニング

スイッチのモードを変更するには、次の手順を実行します。

1. 必要なスイッチのチェックボックスをオンにします。
2. [アクション（Actions）] > **[RMA** のプロ

   ビジョニング（**Provision RMA**）**]** をク

   リックします。**[RMA** のプロビジョニン

   グ（**Provision RMA]** ページが表示され

   ます。

   [RMA のプロビジョニング（**Provision RMA**）**]** ページには、電源がオンになってから 5～10 分後に交換デバイスが表示されます。

シリアル番号の変更

スイッチのシリアル番号を変更できます。デバイスの事前プロビジョニング中に、スイッチのシリアル番

号にダミー値を指定できます。ネットワークを正常に構成したら、シリアル番号をスイッチの適切なシリアル番号に変更できます。

スイッチのシリアル番号を変更する前に、メイン ウィンドウで **[**アクション（**Actions**）**] > [**再計算と展開（**Recalculate and Deploy**）**]** をクリックして、スイッチに最新のデータを保存します。

シリアル番号の変更は、Nexus 9000 シリーズ スイッチでのみサポートされています。シリアル番号を実際の番号に変更した後は、電源オンのブートストラップ時に、デバイスの POAP を再度実行することをお勧めします。

実行開始のコピー（Copy Run Start）

既存のスイッチ構成をコピーして構成を開始するには、次の手順を実行します。

1. 必要なスイッチのチェックボックスをオンにします。
2. **[**アクション（**Actions**）**] > [**詳細（**More**）**] > [**コピー実行（**Copy Run**）**] > [**開始（**Start**）**]**の順にクリックします。

   [実行構成をスタートアップ構成にコピー（**Copy Running Config to Startup Config**）**]** ページが表示されます。
   [進捗状況（**Progress**）**]** 列には進行中のプロセスが表示され、ステータスの説明には **[**進行中の展開**]** と表示されます。

   確認用のダイアログボックスが表示されます。

3. [OK] をクリックします。

   ステータスの説明列には、**[**展開完了（**Deployment completed**）**]** と [進捗状況（progress）] 列が緑色で表示されます。

4. **[**閉じる（**Close**）**]** ボタンをクリックして、ページを閉じます。

リロード

1. 必要なスイッチをリロードするには、**[**アクション（**Actions**）**]**

   > [詳細（**More**）**] > [**リロード（**Reload**）**]** を選択します。確認

   用のダイアログボックスが表示されます。

2. **[**確認（**Confirm**）**]** をクリックします。

復元スイッチ

Cisco Nexus Dashboard ファブリック コントローラ GUIから外部ファブリックおよび LAN クラシック ファブリックの Cisco Nexus スイッチを復元できます。スイッチ レベルで復元する情報は、ファブリック レベルのバックアップから抽出されます。スイッチ レベルの復元では、ファブリック レベルのインテントおよびファブリック設定を使用して適用されたその他の設定は復元されません。スイッチ レベルのインテントのみが復元されます。したがって、スイッチを復元すると、ファブリック レベルのインテントが復元されないため、同期がとれなくなる可能性があります。ファブリック レベルの復元を実行して、インテントも復元します。復元は一度に 1 つしか実行できません。スイッチが検出されたファブリックが MSD ファブリックの一部である場合、スイッチを復元することはできません。

1. **[**アクション（**Actions**）**] > [**詳細（**More**）**] > [**リロード（**Reload**）**]** を選択します。

   [スイッチの復元（**Restore Switch**）**]** ページが表示され、**[**バックアップの選択（**Select a Backup**）**]** タブが表示されます。

   [バックアップの選択（**Select a Backup**）**]**タブには、ファブリック バックアップの詳細が表示されます。収集する情報は次のとおりです。

フィールド	説明
バックアップ日	バックアップの日時を指定します。
バックアップ バージョン	バックアップ名を指定します。
バックアップ タグ	スイッチのバージョン番号を指定します。
NDFC バージョン	NDFC バージョンの詳細を指定します。
バックアップのタイプ	バックアップのタイプ（手動または自動）を指定します。

   自動、手動、またはゴールデンバックアップを選択できます。これらのバックアップは色分けされています。自動バックアップは青色で示されます。

   手動バックアップは濃い青色で示されます。ゴールデン バックアップはオレンジ色で示されます。自動バックアップの名前にはバージョンのみが含まれます。一方、手動バックアップには
   手動バックアップを開始したときに指定したタグ名と、バックアップ名のバージョンがあります。バックアップにカーソルを合わせると、名前が表示されます。

   アーカイブの制限に達した後でも、削除しないバックアップにマークを付けることができます。これらのバックアップはゴールデン バックアップです。ファブリックのゴールデン バックアップは削除できません。ただし、Cisco Nexus Dashboard Fabric Controller は、最大 10 個のゴールデン バックアップのみをアーカイブします。

2. 必要なバックアップのラジオ ボタンをクリックして、ゴールデンとしてマークします。
3. **[**アクション（**Actions**）**] > [**ゴールデンとしてマーク（**Mark as Golden**）**]** をクリックします。

   確認用のダイアログボックスが表示されます。

4. **[**確認（**Confirm**）**]** をクリックします。
5. ゴールデン バックアップから削除するバックアップのオプション ボタンをクリックします。
6. **[**アクション（**Actions**）**] > [**ゴールデ

   ンとして削除（**Remove as**

   Golden）**]** の順にクリックします。

   確認用のダイアログボックスが表示

   されます。

7. **[**確認
   （**Confirm**）**]**
   をクリックし
   ます。

   ヒント：

この情報の大部分はファブリックレベルであり、スイッチレベルの復元の手順に直接影響する場合と影響しない場合があります。

8. **[次へ（Next）]** をクリックして、**[プレビューの復元（Restore Preview）]** の手順に進みます。

   スイッチ名、スイッチ シリアル、IP アドレス、ステータス、サポートされている復元、デルタ構成、および VRF の詳細に関する情報を表示できます。

9. （オプション）**[構成の取得（Get Config）]** をクリックして、デバイス構

   成の詳細をプレビューします。**[構成のプレビュー（Config Preview）]** ダ

   イアログが表示されます。このウィンドウには 3 つのタブがあります。

フィールド	説明
バックアップ設定	このタブには、選択したデバイスのバックアップ構成が表示されます。
現在の構成	このタブには、選択したデバイスの現在の実行構成が表示されます。
1 対 **1** での比較	このタブには、スイッチの現在の実行構成と、予想される構成が表示されます。

10. **[インテントの復元（Restore Intent）]** をクリックして、復元のステータ

    スの復元手順に進みます。スイッチの復元ステータスと説明が表示されま

    す。

11. 復元プロセスが完了したら、**[完了（Finish）]** をクリックします。

・ファブリック構成が変更されているため、以前のステップに戻ることができません

。

・復元に失敗した場合、スイッチは以前の構成にロールバックします。

コマンドの表示

次の手順では、Nexus Dashboard ファブリック コントローラのコマンドを表示します。

1. **[**アクション（**Actions**）**] > [**詳細（**More**）**] >**

   [show コマンド（**Show Command**）**]** を選択

   します。**[**スイッチの **show** コマンド（**Switch**

   Show Commands）**]** ページが表示されます。

2. ドロップダウン リストから必要なコマンドを選択し、テキスト フィールドに必要な情報を入力します。
3. CLI の出力を表示するには **[**実行（**Execute**）**]** をクリックし、出力をクリアします。
4. **[**出力の消去（**Clear Output**）**]** をクリックします。

Exec Commands

EXEC モードで使用可能なコマンドには、デバイスの状態および構成情報を表示する show コマンド、clear コマンド、ユーザーが構成に保存しない処理を実行するその他のコマンドがあります。

次の手順では、Nexus Dashboard Fabric Controller で EXEC コマンドの実行方法を表示します。

1. **[**アクション（**Actions**）**] > [**詳細（**More**）**] >**

   [Exec コマンド（**Exec Commands**）**]** 選択し

   ます。**[**スイッチの **show** コマンド（**Switch**

   Show Commands）**]** ページが表示されます。

2. **[**テンプレート（**Template**）**]** ドロップダウンリストから、**[exec_freeform]** または **[exec_elam_capture]** を選択します。
3. **Freeform CLI** で **exec_freeform** および必要な IP アドレスのコマンドを入力します。
4. **[**展開（**Deploy**）**]** をクリックして、EXEC コマンドを実行します。
5. **[CLI** 実行ステータス（**CLI Execution Status**）**]** ページで、展開のステータスを確認できます。
6. **[**コマンド（**Command**）**]** 列の **[**詳細なステータス（**Detailed Status**）**]**をクリックして詳細を表示します。
7. **[**コマンド実行の詳細（**Command Execution Details**）**]** ウィンドウで、**[CLI** 応答（**CLI Response**）**]** 列の情報をクリックして、出力または応答を表示します。

スイッチの削除

1 つ以上の既存のスイッチを削除できます。

1. **[**アクション（**Actions**）**] > [**詳細

   （**More**）**] > [**削除（**Delete**）**]** スイッチを

選択します。確認用のダイアログボックス

が表示されます。

2. **[**確認（**Confirm**）**]** をクリックします。

拡張されたロールベースのアクセス制御

Cisco Nexus ダッシュボード ファブリック コントローラ SAN コントローラリリース 12.0.1(a) からは、すべての RBAC が Nexus ダッシュボードにあります。ユーザロールとアクセスは、NDFC 上のファブリックの Nexus ダッシュボードから定義されます。

Nexus Dashboard の管理者ロールは、NDFC のネットワーク管理者ロールと見なされます。

DCNM には、さまざまなアクセスと操作を実行するための 5 つのロールがありました。ユーザーがアクセスする場合、ネットワークステージロールを持つファブリックは、ネットワークステージロールとして他のすべてのファブリックにアクセスできます。したがって、ユーザー名は DCNM でのロールによって制限されます。

Cisco NDFC リリース 12.0.1(a) には同じ 5 つのロールがありますが、Nexus ダッシュボードの統合により詳細な RBAC を実行できます。ユーザーがネットワークステージロールとしてファブリックにアクセスする場合、同じユーザーは、管理者またはオペレーターロールなどの他のユーザーロールを使用して別のファブリックにアクセスできます。したがって、ユーザーは NDFC のさまざまなファブリックでさまざまなアクセス権を持つことができます。

NDFC RBAC は、次のロールをサポートします。

- NDFC アクセス管理者
- NDFC 承認者の変更
- NDFC 展開者の変更
- NDFC デバイス アップグレード管理者
- NDFC ネットワーク管理者
- NDFC ネットワーク オペレータ
- NDFC ネットワーク ステージャ

DCNM では、下位互換性のために次のロールがサポートされています。

- グローバル管理者 (ネットワーク管理者にマッピング)
- サーバー管理者（ネットワーク管理者にマッピング）

ヒ どのウィンドウでも、ログインしているユーザーロールで実行できないアクションはグレー表示されます。

NDFC アクセス管理者

NDFC アクセス管理者ロールを持つユーザーは、すべてのファブリックの**[**インターフェイス マネージャ（**Interface Manager**）**]**
アクセス権を持つすべてのファブリックの

NDFC アクセス管理者は、次のアクションを実行できます。

- レイヤ 2 ポート チャネル、および vPC を追加、編集、削除、展開します。
- ホスト vPC、およびイーサネット インターフェイスを編集します。
- 管理インターフェイスからの保存、プレビュー、および展開。
- LAN クラシックおよび IPFM ファブリックのインターフェイスを編集します。

nve、管理、トンネル、サブインターフェイス、SVI、インターフェイス グループ、およびループバック
interfaces

ただし、Cisco Nexus Dashboard Fabric Controller アクセス管理者ロールを持つユーザーは、次のアクションを実行できません。

- レイヤ 3 ポート チャネル、ST FEX、AA FEX、ループバック インターフェイス、nve インターフェイス、およびサブインターフェイスは編集できません。
- レイヤ 3、ST FEX、AA FEX のメンバー インターフェイスおよびポート チャネルは編集できません。
- Easy ファブリック用に、アンダーレイとリンクから関連付けられたポリシーを持つインターフェイスは編集できません。
- ピア リンク ポート チャネルを編集できません。
- 管理インターフェイスを編集できません。
- トンネルを編集できません。

ヒ ファブリックまたは Cisco Nexus Dashboard Fabric Controller が展開フリーズ モードの場合、このロールのアイコンとボタンはグレー表示されます。

NDFC 承認者の変更

NDFC 変更承認者ロールは、NDFC リリース 12.1.3 で導入された変更制御およびロールバック機能の一部として使用できるようになりました。詳細については、「変更制御とロールバック」を参照してください。

NDFC 承認者の変更権限を持つユーザーは、変更制御チケットを承認できます。

NDFC 承認者の変更ロールが割り当てられたユーザーは、特定のチケットに関連付けられている変更を再確認し、それらの変更を承認または拒否できます。

NDFC 展開者の変更

NDFC 展開の変更ロールは、NDFC リリース 12.1.3 で導入された変更制御およびロールバック機能の一部として使用できるようになりました。 詳細については、「変更制御とロールバック」を参照してください。

NDFC Change Deployer 権限を持つユーザは、変更制御チケットを展開できます。

NDFC 承認者変更ロールを持つユーザーによって変更制御チケットが承認されると、**NDFC** 展開者変更ロールが割り当てられているすべてのユーザーがそのチケットを使用できるようになり、変更管理ワークフローで展開段階に移動した変更を展開できます。

NDFC デバイス アップグレード管理者

NDFC デバイス アップグレード管理者ロールを持つユーザーは、**[**イメージ管理（**Image Management**）**]** ウィンドウでのみ操作を実行できます。

詳細については、「イメージ管理：LAN」のセクションを参照してください。

NDFC ネットワーク管理者

NDFC ネットワーク管理者ロールを持つユーザーは、Cisco Nexus Dashboard Fabric Controller ですべての操作を実行できます。

Cisco Nexus Dashboard Fabric Controlle リリース 12.1.1e から、このロールを持つユーザーは、ネットワークおよび VRF の MSD ファブリックのすべての操作を実行できます。

NDFC ネットワーク管理者ロールを持つユーザーは、Cisco Nexus Dashboard Fabric Controller の特定のファブリックまたはすべてのファブリックをフリーズできます。

ヒ NDFC の検出または追加のスイッチまたは LAN クレデンシャルのスイッチ ユーザー ロールに network-admin ロールがあることを確認してください。

NDFC ネットワーク オペレータ

ネットワーク オペレータは、ファブリック ビルダー、ファブリック設定、構成のプレビュー、ポリシー、およびテンプレートを表示できます。ただし、ネットワーク オペレータは次の操作を実行できません。

- ファブリック内のスイッチの予期される構成を変更できません。
- スイッチに構成を展開できません。
- ライセンス、追加ユーザの作成などの管理オプションにアクセスできません。

ネットワーク オペレータとネットワーク ステージャの違いは、ネットワーク ステージャとして、既存のファブリックのインテントのみを定義できますが、それらの設定を展開できないことです。

ネットワーク ステージャロールを持つユーザがステージングした変更および編集を展開できるのは、ネットワーク管理者だけです。

NDFC ネットワーク ステージャ

NDFC ネットワーク ステージャ ロールを持つユーザーは、Cisco Nexus Dashboard Fabric Controller で構成を変更できます。**NDFC** ネットワーク管理者ロールを持つユーザーは、これらの変更を後で展開できます。ネットワーク ステージャは、次のアクションを実行できます。

- インターフェイス構成の編集
- ポリシーの表示または編集
- インターフェイスの作成
- ファブリック設定の変更
- テンプレートの編集または作成

ただし、ネットワーク ステージャは次のアクションを実行できません。

- スイッチに設定を展開できません。
- Cisco Nexus Dashboard Fabric Controller Web UI または REST API から展開関連のアクションを実行できません。
- ライセンス、追加ユーザの作成などの管理オプションにアクセスできません。
- メンテナンス モードの切り替えはできません。
- 展開フリーズ モードでファブリックを移動したり、展開モードから解放したりすることはできません。
- パッチをインストールします。
- スイッチをアップグレードできません。

- ファブリックを作成または削除できません。
- スイッチをインポートまたは削除できません。

デフォルトの認証ドメインの選択

Nexus Dashboard のデフォルトのログイン画面では、認証用のローカルドメインが選択されます。ドロップダウンリストから利用可能なドメインを選択することで、ログイン時にドメインを変更できます。

Nexus Dashboard は、ローカルおよびリモート認証をサポートしています。Nexus Dashboard のリモート認証プロバイダーには、RADIUS と TACACS が含まれます。認証のサポートの詳細については、https://www.cisco.com/c/en/us/td/docs/dcn/nd/2x/user-guide/cisco-nexus-dashboard-user- を参照してください。
guide-211.pdf を参照してください。

次の表に、DCNM アクセスと NDFC アクセス間の RBAC の比較を示します。

DCNM 11.5(x)	**NDFC 12.0.x** および **12.1.x**
• ユーザーのロールは 1 つです。 • すべての API とリソースは、この 1 つのロールでアクセスされます。	• ユーザーは、セキュリティドメインの Nexus Dashboard ごとに異なるロールを持つことができます。 • セキュリティドメインには単一の Nexus Dashboard が含まれ、各 Nexus Dashboard には単一の NDFC ファブリックが含まれます。
DCNM のオプションへのアクセスを無効化または制限することにより、単一のロールがユーザーに関連付けられます。	単一のロールでは、選択したページに特権リソースのみが表示され、NDFC のその他のオプションでは、選択したリソースに関連付けられたセキュリティドメインに基づいて、制限されたアクセスがグレー表示されます。
シェル、ロール、およびオプションのアクセス制約を含む DCNM AV ペア形式。	シェル、ドメインを含む Nexus Dashboard AV ペアフォーマット。
展開タイプ LAN、SAN、または PMN に基づいてサポートされるロール。	network-admin、network-operator、device-upg-admin、network-stager、access-admin などのサポートされているロールは NDFC にあります。下位互換性のためのレガシーロールのサポート。DCNM のネットワーク管理者としての Nexus Dashboard 管理ロール。

次の表では、DCNM 11.5(x) AV ペアの形式について説明します。

Cisco DCNM Role	**RADIUS Cisco-AV-Pair** の値	**TACACS+** シェル **Cisco-AV-Pair** ペアの値

ネットワークオペレータ	shell:roles = " network-operator" dcnm-access=" group1 group2 group5"	cisco-av-pair=shell:roles=" network-operator" dcnm-access=" group1 group2 group5"
Cisco DCNM Role	**RADIUS Cisco-AV-Pair** の値	**TACACS+** シェル **Cisco-AV-Pair** ペアの値
ネットワーク管理者	shell:roles = " network-admin" dcnm-access=" group1group2 group5"	cisco-av-pair=shell:roles=" network-admin" dcnm-access=" group1 group2 group5"

次の表では、NDFC 12.x AV ペアの形式について説明します。

ユーザー ロール	**AVPair** 値
NDFC アクセス管理者	access-admin
NDFC デバイスアップグレード管理者	device-upg-admin
NDFC ネットワーク管理者	ネットワーク管理者
NDFC ネットワークオペレータ	network-operator
NDFC ネットワークステージャ	network-stager

AV ペア文字列の形式は、特定のユーザーに対して読み取り/書き込みロールを設定するか、読み取り専用ロールを設定するか、または読み取り/書き込みロールと読み取り専用ロールの組み合わせを設定するかによって異なります。通常の文字列にはドメインが含まれており、その後にスラッシュ（/）で区切って読み取り専用ロールからは切り離された読み取り/書き込みロールが続きます。個々のロールはパイプ（|）で区切られています。

shell:domains=<domain>/<writeRole1>|<writeRole2>/<readRole1>|<readRole2>

強化された **RBAC** のユースケース

NDFC にはさまざまなファブリックがあります。デフォルトでは、ユーザーはすべてのファブリックの管理者です。たとえば、ユーザー名 **Cisco** は、Fabric-A への 管理者ロール アクセスと、別の Fabric-B へのステージャ ロール アクセスを持つことができます。

Nexus Dashboard では、すべてのセキュリティ ポリシーはセキュリティ ドメインの一部です。ユーザーを作成し、これらのセキュリティ ドメインへのアクセスを許可できます。

ユーザーを作成し、特定のロールを定義するには、次の手順を実行します。

1. セキュリティ ドメインにユーザーを作成するには：
   a. 管理者ロールで Nexus Dashboard にログインし、**[**管理（**Administrative**）**]** タブに移動します。
   b. **[**セキュリティ ドメイン（**Security Domain**）**]** タブで、[セキュリティ ドメインの作成（**Create Security Domain**）] をクリックし、次のセキュリティ ドメインを作成します。
      - **all**：network-admin ロールに類似しています。このドメインには、Nexus Dashboard および NDFC サービス アプリケーションへの管理アクセス権があります。
      - **cisco-admin**：Fabric-A への完全なネットワーク管理者アクセス
      - **cisco-stager**：Fabric-B へのネットワーク ステージャのみのアクセス
2. ローカル ユーザー **Cisco** を作成するには。
   a. **[**ユーザー（**Users**）**] > [**ローカル（**Local**）**]** に移動します。
   b. **[**ローカル（**Local**）**]** タブで、**[**ローカル

      ユーザーの作成（**Create Local User**）**]**

      をクリックします。**[**ローカル ユーザーの

      作成（**Create Local User**）**]** ウィンドウが

      表示されます。

   c. [ユーザー ID（User ID）] テキスト フィールドに **Cisco** と入力し、それぞれのフィールドに適切なパスワードを設定します。
   d. Cisco ユーザーを作成したら、**[**ローカル（**Local**）**]** ウィンドウに移動し、省略記号アイコン（**Cisco**
      ユーザー名の行を選択し、**[**ユーザーの編集

      （**Edit User**）**]** をクリックします。**[**ユーザ

      ーの編集（**Edit User**）**]** ウィンドウが表示

      されます。

3. **[**ユーザーの編集（**Edit User**）**]** ウィンドウには、デフォルトで、**all** セキュリティ ドメインが存在します。**[**セキュリティ ドメインの追加（**Add Security Domain**）**]** をクリックします。
   他のセキュリティ ドメインを追加するロール。

   [セキュリティ ドメインとロールの追加（**Add Security Domain and Roles**）**]** ウィンドウが表示されます。

   a. オプションのドロップダウン リストから **cisco-admin** ドメインを選択し、**[NDFC** アクセス管理者

（**NDFC Access Admin**）]
チェックボックスをオンにして、**[**保存（**Save**）**]** をクリックします。

b. 手順 **a** を繰り返して、**cisco-stager** ドメインを **[NDFC** ネットワーク ステージャ（NDFC Network Stager）] ロール用に追加します。

c. セキュリティ ドメインをそれぞれのファブリック サイトに関連付けるには、次の手順を実行します。

Nexus Dashboard で、**[**サイト（**Sites**）**]** ウィンドウに移動します。**Fabirc-A** サ

イト名をクリックします。スライドイン ペインが表示されます。Fabric-A サイト

の **all** セキュリティ ドメインを表示できます。

d. Fabric-A の network-admin として Cisco ユーザーを追加するには、省略記号アイコンと [サイトの編集（Edit Site）] をクリックします。

e. **all** セキュリティ ドメインを削除し、**network-admin** ドメインを追加して、変更を保存します。

同様に、network-stager ドメインでも追加できます。

f. Nexus Dashboard からログアウトし、**Cisco** ユーザーとして再度ログインします。

ユーザー ロール Cisco は、権限に基づいて Nexus Dashboard の NDFC 関連オプションのみを表示できます。
これは、権限に基づくものです。Nexus Dashboard サービスに制限されたユーザー アクセス。

g. NDFC アプリケーションへのナビゲーション。

ユーザー Cisco は、NDFC 上の 2 つのサイトで操作を実行できます。これは、ユーザーが Fabric-A の network-admin ロール、および Fabric-B の network-stager ロールとして割り当てられているためです。

network-admin ロールは、Fabric-A のインターフェイスを作成して展開できます。
network-stager ロールは、Fabric-B のインターフェイスを作成できますが、展開へのアクセスは制限されます。

Nexus Dashboard のセキュリティ ドメイン

ユーザー ログインに関するアクセス制御情報には、ユーザー ID、パスワードなどの認証データが含まれます。認証データに基づいて、リソースに適宜アクセスできます。Cisco Nexus Dashboard の管理者は、セキュリティ ドメインを作成し、さまざまなリソース タイプ、リソース インスタンスをグループ化し、それらをセキュリティ ドメインにマッピングできます。管理者は各ユーザーの AV ペアを定義します。これにより、Cisco Nexus Dashboard のさまざまなリソースに対するユーザーのアクセス権限が定義されます。ファブリックを作成すると、Nexus ダッシュボードに同じファブリック名でサイトが作成されます。これらのサイトは、**[Nexus**ダッシュボード（**Nexus Dashboard**）**] > [**サイト（**Sites**）**]**で作成および表示できます。

Cisco Nexus Dashboard Fabric Controller REST API は、この情報を使用して、認可を確認することによってアクションを実行します。

ヒ

REST API にアクセスすると、渡されたペイロードを JSON 形式で確認できます。ペイロードが適切な JSON 形式であることを確認します。

Cisco Nexus Dashboard Fabric Controller リリース 11.x からアップグレードすると、各ファブリックは同じ名前の自動生成サイトにマッピングされます。これらすべてのサイトは、Nexus Dashboard のすべてのセキュリティ ドメインにマッピングされます。

すべてのリソースは、他のドメインに割り当てられたりマッピングされたりする前に、すべてのドメインに配置されます。すべてのセキュリティ ドメインには、Nexus ダッシュボードで使用可能なすべてのセキュリティ ドメインは含まれません。

AV ペア

セキュリティ ドメインのグループと各ドメインの読み取りおよび書き込みロールは、AV ペアを使用して指定されます。管理者は、各ユーザの AV ペアを定義します。AV ペアは、Nexus ダッシュボードのさまざまなリソースに対するユーザのアクセス権限を定義します。

AV ペアの形式は次のとおりです。

```
avpair

" shell:domains=security-domain/write-role-1|write-role-2,security-domain/write-role-1|write-role2/read-role-1|read-role-2" ``
```

次に例を示します。

```
" avpair" :

" shell:domains=all/network-admin/app-user|network-operator"
```

この例では、ユーザをスーパーユーザーにします。「all/admin/」の例は避けることをお勧めします。

write ロールには read ロールも含まれます。したがって、all/network-admin/ と all/network-admin/network-admin は同じです。

ヒ

Cisco Nexus Dashboard Fabric Controller リリース 12.0.1a から、 Cisco Nexus Dashboard Fabric Controller リリース11.x で作成した既存の AV ペア形式がサポートされます。ただし、新しい AV ペアを作成する場合は、上記の形式を使用します。shell:domains にスペースが含まれていないことを確認します。

AAA サーバ上での Cisco NX-OS のユーザ ロールおよび SNMPv3 パラメータの指定

AAA サーバー上で VSA cisco-AV-pair を使用して、次の形式で Cisco NX-OS デバイスのユーザーロールマッピングを指定できます。

```
shell:roles=" roleA roleB ..."
```

cisco-AV-pair 属性にロール オプションを指定しなかった場合のデフォルトのユーザ ロールは、network-operator です。

次のように SNMPv3 認証とプライバシー プロトコル属性を指定することもできます。

```
shell:roles=" roleA roleB..."  snmpv3:auth=SHA priv=AES-128
```

SNMPv3 認証プロトコルに指定できるオプションは、SHA と MD5 です。プライバシー プロトコルに指定できるオプションは、AES-128 と DES です。cisco-AV-pair 属性にこれらのオプションを指定しなかった場合のデフォルトの認証プロトコルは、MD5 と DES です。

セキュリティ ドメインの作成

Cisco Nexus Dashboard からセキュリティ ドメインを作成するには、次の手順を実行します。

1. Cisco Nexus Dashboard にログインします。
2. **[管理（Administrative）] > [セキュリティ（Security）]** の順に選択します。
3. **[セキュリティ ドメイン（Security Domain）]** タブに移動します。
4. **[セキュリティ ドメインの作成（Create Security Domain）]** をクリックします。
5. 必要な詳細を入力し、**[作成（Create）]** をクリックします。

ユーザーの作成

Cisco Nexus Dashboard からユーザーを作成するには、次の手順を実行します。

1. Cisco Nexus Dashboard にログインします。
2. **[管理（Administrative）] > [ユーザー（Users）]** の順に選択します。
3. **[ローカル ユーザーの作成（Create Local User）]** をクリックします。
4. 必要な詳細を入力し、**[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。
5. ドロップダウン リストからドメインを選択します。

6. 適切なチェックボックスをオンにして、Cisco Nexus Dashboard Fabric Controller サービスの読み取りまたは書き込みロールを割り当てます。
7. **[**保存（**Save**）**]** をクリックします。

著作権

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本マニュアルに組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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

Cisco およびCisco のロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。
商標または登録商標です。シスコの商標の一覧は、http://www.cisco.com/ go/trademarks でご確認いただけます。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。（1110R）。