マルチサイト外部ネットワーク、リリース12.1.3

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または、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 12.1.3	整理し直したコンテンツ	このドキュメント内のコンテンツは元来 『*Cisco NDFC-Fabric Controller Configuration Guide*』または『*Cisco NDFC-SAN Controller Configuration Guide*』で提供されました。リリース 12.1.3 以降、このコンテンツは現在、本ドキュメントでのみ提供されており、これらのドキュメントでは提供されなくなっています。
NDFC リリース 12.1.3	ファブリック タイプ名前の変更	マルチサイト インターコネクト ネットワーク ファブリック タイプは、マルチサイト外部ネットワークに名前が変更されました。

External_Fabric に関連付けられたファブリックテンプレート

このドキュメントでの External_Fabric への参照は、次の 3 つのファブリック テンプレートのいずれかを指します。

- マルチサイト外部ネットワーク
- 外部接続ネットワーク
- カスタムネットワーク

ファブリックのタイプは **External_Fabric**で、次の場合、ファブリック テンプレート名で表示されます。

1. DCNM 11.5(4) からのアップグレードと復元。
2. NDFC 12.0.2f/12.1.1e からのアップグレード

既存のすべての機能リストは、以前のリリースと同様に機能し続けます。必要に応じて、ファブリックを編集し、**[カスタム ネットワーク（Flexible Network）]**、**[外部接続ネットワーク（External Connectivity Network）]**、**[マルチサイト外部ネットワーク（Multi-Site External Network）]** の 3 つのオプションのいずれかを選択できます。これらのオプションのいずれかを選択せずにファブリック設定を編集すると、デフォルトのオプションである **[カスタム ネットワーク（Custom Network）]** が選択されます。必要に応じて、機能を損なうことなく、これらの 3 つのオプションを切り替えることができます。ファブリックのタイプは、**EXT_FABRIC_TYPE** という変数の nvPairs に保存されます。これは、ファブリックの作成時にペイロードでオプションで指定できます。指定しない場合、**[カスタム ネットワーク（Custom Network）]** のデフォルトオプションが選択されます。

外部ファブリック

外部ファブリックにスイッチを追加できます。汎用ポインタ：

NDFC は「no router bgp」を生成しません。変更する場合は、スイッチに移動して「no feature bgp」を実行します。それ以外何もせずに ASN を更新した場合は、その後で再同期します。

- 外部ファブリックは、モニタ専用または管理モードのファブリックです。
- Cisco Nexus Dashboard Fabric Controller Release 12.0.1、Cisco IOS XR ファミリ デバイス、Cisco ASR 9000 シリーズ Aggregation Services Routers および Cisco Network Convergence System（NCS）5500 シリーズは、管理モードおよびモニタ モードの外部ファブリックでサポートされます。NDFC は設定を生成してこれらのスイッチにプッシュすることができ、設定コンプライアンスもこれらのプラットフォームで有効になります。
- Cisco Nexus Dashboard Fabric Controller リリース 12.1.1e から、管理モードとモニタ モードの両方で Cisco 8000 シリーズ ルータを外部ファブリックに追加することもできます。構成コンプライアンスもサポートされます。
- 外部ファブリックのスイッチをインポート、削除、および削除できます。
- ファブリック間接続（IFC）の場合、外部ファブリックの宛先スイッチとしてCisco 9000、7000、および5600シリーズスイッチを選択できます。
- 存在しないスイッチを宛先スイッチとして使用できます。
- 外部ファブリックをサポートするテンプレートは、External_Fabricです。
- 外部ファブリックが VXLAN EVPN マルチサイト ファブリックメンバーである場合、VXLAN EVPN マルチサイト トポロジ画面には、外部ファブリックとそのデバイス、およびメンバー ファブリックとそのデバイスが表示されます。

  外部ファブリック トポロジ画面から表示すると、Nexus Dashboard Fabric Controller の管理対象でないスイッチへの接続はすべて、**Undiscovered** というラベルの付いたクラウドアイコンで表されます。

- マルチサイトまたはVRF-lite IFCを設定するには、VXLANファブリック内の境界デバイスのリンクを手動で設定するか、または自動的にDeploy Border Gateway MethodまたはVRF Lite IFC Deploy Methodを使用します。ボーダーデバイスのリンクを手動で設定する場合は、コアルータロールを使用してマルチゲートウェイeBGPアンダーレイをボーダーゲートウェイデバイスからコアルータに設定し、エッジルータロールを使用してVRF-Lite Interを設定することを推奨します。 -ボーダーデバイスからエッジデバイスへのファブリック接続（IFC）。
- Cisco Nexus 7000シリーズスイッチとCisco NX-OSリリース6.2（24a）をLANクラシックまたは外部ファブリックで使用している場合は、ファブリック設定でAAA IP認証を有効にしてください。
- 外部ファブリックでは、次の非Nexusデバイスを検出できます。
  - [IOS XE ファミリ デバイス（IOS XE family devices）] : Cisco CSR 1000v、Cisco IOS XE ジブラルタ 16.10.x、Cisco ASR 1000 シリーズ ルータ、および Cisco Catalyst 9000 シリーズ スイッチ
  - [IOS-XR ファミリ デバイス（IOS XR family devices）] : ASR 9000 シリーズ ルータ、IOS XR リリース 6.5.2 および Cisco NCS 5500 シリーズ ルータ、IOS XR リリース 6.5.3
  - Arista 4.2（任意のモデル）
- 外部ファブリックに追加する前に、Cisco CSR 1000vを除くすべてのNexus以外のデバイスを設定します。
- Nexus以外のデバイスをボーダーとして設定できます。外部ファブリックの非 Nexus デバイスと、easy fabric の

Cisco Nexus デバイス間で IFC を作成できます。これらのデバイスでサポートされるインターフェイスは次のとおりです。

- ルート化済み
- サブインターフェイス
- ループバック

- Cisco ASR 1000シリーズルータおよびCisco Catalyst 9000シリーズスイッチをエッジルータとして設定し、VRF-lite IFCを設定し、簡単なファブリックを使用してボーダーデバイスとして接続できます。
- VDCをリロードする前に、ファブリックで管理VDCを検出します。それ以外の場合、リロード操作は行われません。
- Cisco CSR 1000vを使用して、シスコデータセンターをパブリッククラウドに接続できます。使用例については、*「Cisco Data Centerとパブリック クラウドの接続」*の章を参照してください。
- 外部ファブリックで **switch_user** ポリシーを追加し、ユーザー名とパスワードを指定する場合、パスワードは **show run** コマンドで表示される暗号化された文字列である必要があります。

  次に例を示します。

  ```
  username admin password 5
  $5$I4sapkBh$S7B7UcPH/iVTihLKH5sgldBeS3O2X1StQsvv3cmbYd1 role network-admin
  ```

  この場合、入力するパスワードは次のようになります。

  5$5$I4sapkBh$S7B7UcPH/iVTihLKH5sgldBeS3O2X1StQsvv3cmbYd1

- Cisco Network Insights for Resources（NIR）リリース2.1以降、およびフロー テレメトリの場合、**feature lldp** コマンドは、必要な設定の 1 つです。

  Cisco Nexus Dashboard Fabric Controller は、Easy Fabric 展開、つまり eBGP ルーテッド ファブリックまたは VXLAN EVPN ファブリックの場合にのみ、**機能 lldp** をスイッチにプッシュします。

  したがって、NIR ユーザーは、次のシナリオですべてのスイッチで**機能 lldp**を有効にする必要があります。

  - モニタモードまたは管理モードの外部ファブリック
  - モニタモードまたは管理モードのLANクラシックファブリック
- バックアップ/復元は、外部ファブリック上の Nexus デバイスでのみサポートされます。

> ファブリックまたはスイッチの復元を実行する前に、ターゲット デバイスがサポートされていることを確認します。ターゲット デバイスがサポートされていない場合、スイッチごとの復元はブロックされ、ファブリック全体の復元中にはサポートされていないものとして表示されます。

VXLAN EVPN マルチサイト ファブリックの下の外部ファブリックの移動

外部ファブリックをメンバーとして関連付けるには、VXLAN EVPN マルチサイト ファブリック ページに移動する必要があります。

1. **[トポロジ（Topology）]** で、VXLAN EVPN マルチサイト親ファブリック内をクリックします。**[アクション（Actions）]** ドロップダウンリストで、**[ファブリックの移動（Move Fabrics）]** を選択します。

   [ファブリックの移動（Move Fabric）] 画面が表示されます。ファブリックのリストが含まれています。外部ファブリックは、スタンドアロンファブリックとして表示されます。

2. 外部ファブリックの横にあるオプションボタンを選択し、[Add]をクリックします。

   右上の [スコープ（Scope）] ドロップダウン ボックスで、VXLAN EVPN マルチサイト ファブリックの下に外部ファブリックが表示されていることがわかります。

VXLAN EVPN マルチサイト ファブリック トポロジでの外部ファブリックの説明

VXLAN EVPN Multi-Siteトポロジ画面には、VXLAN EVPN Multi-Site メンバーファブリックと外部ファブリックが一緒に表示されます。外部ファブリック External65000 は、VXLAN EVPN マルチサイトトポロジの一部として表示されます。

VXLAN ファブリックのネットワークまたは VRF を展開すると、 展開ページ（VXLAN EVPN マルチサイト トポロジ ビュー）には、相互に接続されている VXLAN と外部ファブリックが表示されます。

外部ファブリックの作成

Cisco Fabric Controller Web UIを使用して外部ファブリックを作成するには、次の手順を実行します。

1. **[LAN] > [ファブリック（Fabrics）] > [ファブリック（Fabrics）]** を選択します。
2. **[アクション（Actions）]** ドロップダウンリストから、**[ファブリックの作成（Create Fabric）]** を選択します。
3. ファブリックの一意の名前を入力して、 **[ファブリックを選択（Choose Fabric）]**をクリックします。
4. ドロップダウンリストから、**[External_Fabric]** テンプレートを選択します。

   この画面のフィールドは次のとおりです。

   - **[BGP AS #]** : BGP AS番号を入力します。
   - **[ファブリック モニタ モード（Fabric Monitor Mode）]** : Nexus Dashboard Fabric Controller にファブリックを管理させる場合は、このチェックボックスをオフにします。モニタ専用の外部ファブリックを有効にする場合には、チェックボックスをオンのままにします。

     Cisco Nexus Dashboard ファブリック コントローラ リリース 12.1.1e から、管理モードとモニタ モードの両方で Cisco 8000 シリーズ ルータを外部ファブリックに追加することもできるようになりました。

     VXLANファブリックからこの外部ファブリックへのファブリック間接続を作成すると、BGP AS番号が外部またはネイバーファブリックAS番号として参照されます。

     外部ファブリックが **[ファブリック モニタ モードのみ（Fabric Monitor Mode Only）]** に設定されている場合は、そのスイッチに設定を展開できません。**[Deploy Config]**をクリックすると、エラーメッセージが表示されます。

     ファブリックで検出する前に、Nexus以外のデバイスの設定をプッシュする必要があります。モニタモードでは設定をプッシュできません。

   - **[パフォーマンス モニタリングの有効化（Enable Performance Monitoring）]** : NX-OS スイッチでのみパフォーマンス モニタリングを有効にするには、このチェックボックスをオンにします。

スイッチのコマンド ライン インターフェイスからインターフェイス カウンタをクリアしないでください。インターフェイス カウンタをクリアすると、パフォーマンス モニターにトラフィック使用率に関する誤ったデータが表示される可能性があります。カウンタをクリアする必要があり、スイッチに clear counters コマンドと clear counters snmp コマンドの両方がある場合（すべてのスイッチに clear counters snmp コマンドがあるわけではない）、main コマンドと SNMP コマンドの両方を同時に実行してください。たとえば、clear counters interface ethernet slot/port コマンドを実行し、clear counters interface ethernet slot/port snmp コマンドを実行する必要があります。これにより、1 回限りのスパイクが発生する可能性があります。

1. **[詳細（Advanced）]**タブのフィールドに値を入力します。

   - **電源モード（Power Supply Mode）** ：適切な電源モードを選択します。
   - **[MPLS ハンドオフの有効化（Enable MPLS Handoff）]** : MPLS ハンドオフ機能を有効にするには、このチェックボックスをオンにします。詳細については、「MPLS SR および LDP ハンドオフ」を参照してください。
   - **[アンダーレイ MPLS ループバック ID（Underlay MPLS Loopback Id）]** : アンダーレイ MPLS ループバック ID を指定します。デフォルト値は 101 です。

- **[AAA IP 認証の有効化（Enable AAA IP Authorization）]**：AAA サーバーで IP 認証が有効になった後に、AAA IP 認証を有効にします。
- **[Nexus Dashboard ファブリック コントローラをトラップ ホストとして有効にする（Enable Nexus Dashboard Fabric Controller as Trap Host）]：** Nexus Dashboard ファブリック コントローラをトラップ ホストとして有効にするには、このチェックボックスをオンにします。
- **[ブートストラップ スイッチの CDP を有効にする（Enable CDP for Bootstrapped Switch）]**：チェックボックスをオンにして、ブートストラップ スイッチの CDP を有効にします。
- **[NX-API の有効化（Enable NX-API）]**：HTTPS での NX-API の有効化を指定します。このチェックボックスは、デフォルトでオフになっています。
- **[HTTP での NX-API の有効化（Enable NX-API on HTTP）]**：HTTP での NX-API の有効化を指定します。このチェックボックスは、デフォルトでオフになっています。HTTP を使用するには、**[NX-API の有効化（Enable NX-API）]** チェック ボックスをオンにします。このチェックボックスをオフにすると、エンドポイント ロケータ（EPL）、レイヤ 4 ~ レイヤ 7 サービス、VXLAN OAM など、NX-API を使用し、Cisco Nexus Dashboard Fabric Controller がサポートするアプリケーションは、HTTP ではなく HTTPS を使用するようになります。

> **[NX-API の有効化（Enable NX-API）]** と **[HTTP での NX-API の有効化（Enable NX-API on HTTP）]** チェックボックスをオンにすると、アプリケーションは HTTP を使用します。

- **[インバンド管理（Inband Mgmt）]**：外部およびクラシック LAN ファブリックの場合、このノブを使用すると Nexus Dashboard Fabric Controller は、インバンド接続（スイッチ ループバック、ルーテッド インターフェイス、または SVI インターフェイス経由で到達可能）でのスイッチのインポートおよび管理が可能になり、またアウトオブバンド接続（つまり、スイッチ mgmt0 インターフェイス経由で到達可能）でのスイッチの管理が可能になります。唯一の要件は、インバンド管理対象スイッチの場合、 Nexus ダッシュボード ファブリック コントローラから Nexus ダッシュボード データ インターフェイス（インバンド インターフェイス）を介してスイッチに IP が到達可能であることです。この目的のために、Nexus Dashboard Fabric Controller でスタティックルートが必要になる場合があります。これは、**[管理（Administration）] > [カスタマイズ（Customization）] > [ネットワーク設定（Network Preferences）]** で構成できます。インバンド管理を有効にした後、検出中に、インバンド管理を使用してインポートするすべてのスイッチの IP を指定し、最大ホップ数を 0 に設定します。 Nexus ダッシュボード ファブリック コントローラは、インバンド管理されたスイッチ IP が Nexus ダッシュボード データ インターフェイスを介して到達可能であるかを検証する事前チェックを行います。事前チェックをパスした後、 Nexus ダッシュボード ファブリック コントローラはインターフェイスが属する VRF に加えて、指定された検出 IP を持つそのスイッチ上のインターフェイスを検出し、学習します。スイッチのインポート/検出のプロセスの一部として、この情報は Nexus ダッシュボード ファブリック コントローラに入力される目的のベースラインにキャプチャされます。詳細については、「インバンド管理、インバンド POAP 管理、セキュア POAP の構成」 の「外部ファブリックおよび LAN クラシック ファブリックのインバンド管理」の項を参照してください。

> ブートストラップまたは POAP は、アウトオブバンド接続、つまりスイッチ mgmt0 を介して到達可能なスイッチでのみサポートされます。Nexus Dashboard Fabric Controller 上のさまざまな POAP サービスは通常、eth1 またはアウトオブバンド インターフェイスにバインドされます。Nexus Dashboard Fabric Controller の eth0 / eth1 インターフェイスが同じ IP サブネットに存在するシナリオでは、POAP サービスは両方のインターフェイスにバインドされます。

- **[精密時間プロトコル（PTP）の有効化（Enable Precision Time Protocol（PTP））]**：ファブリック全体で PTP を有効にします。このチェックボックスを選択すると、PTP はグローバルで、およびコア向きのインターフェイスで有効化されます。**[PTP 送信元ループバック ID（PTP Source Loopback Id）]** フィールドと **[PTP ドメイン ID（PTP Domain Id）]** フィールドも編集できます。詳細については、フレキシブル ネットワーク内の「外部ファブリックの正確な時刻のプロトコル」セクションを参照してください。
- **[PTP 送信元ループバック ID（PTP Source Loopback Id）]**：すべての PTP パケットの送信元 IP アドレスとして使用されるループバック インターフェイス ID ループバックを指定します。有効な値の範囲は 0 ~ 1023 です。PTP ループバック ID を RP、ファントム RP、NVE、または MPLS ループバック ID と同じにすることはできません。そうでない場合は、エラーが生成されます。PTP ループバック ID は、BGP ループバックまたは Nexus ダッシュボード ファブリック コントローラから作成されたユーザー定義ループバックと同じにすることができます。保存して展開中に PTP ループバック ID が見つからない場合は、次のエラーが生成されます：PTP ソース IP に使用するループバック インターフェイスが見つかりません。PTP機能を有効にするには、すべてのデバイスでPTPループバックインターフェイスを作成してください。
- **[PTP ドメイン ID]**：単一のネットワーク上の PTP ドメイン ID を指定します。有効な値の範囲は 0 ~ 127 です。
- **[ファブリック自由形式（Fabric Freeform）]**：この自由形式フィールドを使用して、外部ファブリックで検出されたすべてのデバイスに構成をグローバルに適用できます。ファブリック内のデバイスは同じデバイスタイプに属している必要があり、ファブリックはモニタモードになっていません。さまざまなデバイスタイプがあります。
  - NX-OS
  - IOS XE
  - IOS XR
  - その他

  デバイスタイプに応じて、設定を入力します。ファブリック内の一部のデバイスがこれらのグローバル設定をサポートしていない場合、導入中に同期がとれなかったり、失敗したりします。したがって、適用する設定がファブリック内のすべてのデバイスでサポートされていることを確認するか、これらの設定をサポートしていないデバイスを削除します。

- **AAA Freeform Config**：このフリーフォームフィールドを使用して、外部ファブリックで検出されたすべてのデバイスにAAA設定をグローバルに適用できます。

2. 次の説明に従って、**[リソース（Resources）]** タブに値を入力します。
   - **[サブインターフェイス Dot1q 範囲（Subinterface Dot1q Range）]**：サブインターフェイス 802.1Q 範囲とアンダーレイ ルーティング ループバック IP アドレス範囲が自動入力されます。
   - **[アンダーレイ MPLS ループバック IP 範囲（Underlay MPLS Loopback IP Range）]**：アンダーレイ MPLS SR または LDP ループバック IP アドレス範囲を指定します。

     IP 範囲は一意である必要があります。つまり、他のファブリックの IP 範囲と重複しないようにする必要があります。

3. 次に示すように、**[構成のバックアップ（Configuration Backup）]** タブに入力します。

   このタブのフィールドは次のとおりです。
   - **[毎時ファブリック バックアップ（Hourly Fabric Backup）]**：ファブリック構成とインテントの毎時バックアップを有効にします。

新しいファブリック設定とインテントの1時間ごとのバックアップを有効にできます。前の時間に構成のプッシュがある場合、Nexus Dashboard Fabric Controller はバックアップを取得します。外部ファブリックの場合、VXLAN ファブリックのように、スイッチの構成全体は Nexus Dashboard Fabric Controller のインテントに変換されません。したがって、外部ファブリックでは、インテントと実行コンフィギュレーションの両方がバックアップされます。

インテントとは、Nexus Dashboard Fabric Controller に保存されているが、まだスイッチにプロビジョニングされていない構成を指します。

時間単位のバックアップは、その時間の最初の 10 分間にトリガーされます。

- **[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]**：毎日のバックアップを有効にします。このバックアップは、構成のコンプライアンスによって追跡されないファブリック デバイスの実行構成の変更を追跡します。
- **[スケジュール済みの時間（Scheduled Time）]**：スケジュールされたバックアップ時間を 24 時間形式で指定します。[**スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]** チェックボックス**をオンにすると、このフィールドが有効になります。**

  両方のチェックボックスをオンにして、両方のバックアップ プロセスを有効にします。

  [保存（Save）]をクリックすると、バックアップ プロセスが開始されます。

  スケジュールされたバックアップは、指定した時刻に最大 2 分の遅延でトリガーされます。スケジュールされたバックアップは、構成の展開ステータスに関係なくトリガーされます。

  ファブリック トポロジ ウィンドウでファブリック バックアップを開始することもできます。**[アクション（Actions）]** ペインで **[今すぐバックアップ（Backup Now）]** をクリックします。

  バックアップには、実行構成と Nexus Dashboard Fabric Controller によってプッシュされたインテントが含まれます。構成への準拠により、実行構成が Nexus Dashboard Fabric Controller の構成と同じになります。外部ファブリックでは、一部の構成のみがインテントの一部であり、残りの構成は Nexus Dashboard Fabric Controller によって追跡されないことに注意してください。したがって、バックアップの一部として、Nexus Dashboard Fabric Controller のインテントと、スイッチからの実行構成の両方がキャプチャされます。

4. **[ブートストラップ（Bootstrap）]** タブをクリックします。

   - **[ブートストラップの有効化（Enable Bootstrap）]：ブートストラップ機能を有効にします。**

     ブートストラップをイネーブルにした後、次のいずれかの方法を使用して、DHCP サーバで IP アドレスの自動割り当てをイネーブルにできます。

     - [外部 DHCP サーバ（External DHCP Server）]：**[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]** および **[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** フィールドに外部 DHCP サーバに関する情報を入力します。
     - [ローカル DHCP サーバー（Local DHCP Server）]：**[ローカル DHCP サーバー（Local DHCP Server）]** チェックボックスをオンにして、残りの必須フィールドに詳細を入力します。

Cisco NDFC リリース 12.1.1e から、外部ファブリックにインバンド POAP またはアウトオブバンド POAP を選択できるようになりました。

- **[インバンド POAP を有効にする（Enable Inband POAP）]**：インバンド POAP を有効にするには、このチェック ボックスをオンにします。

> このオプションを有効にするには、**[インバンド管理（Inband Mgmt）]** を **[詳細（Advanced）]** タブで有効にする必要があります。

- **[ローカル DHCP サーバの有効化（Enable Local DHCP Server）]**：ローカル DHCP サーバを介した自動 IP アドレス割り当ての有効化を開始するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、残りのすべてのフィールドが編集可能になります。
- **[DHCP バージョン（DHCP Version）]**：このドロップダウンリストから [DHCPv4] または [DHCPv6] を選択します。[DHCPv4] を選択すると、**[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]** フィールドは無効になります。DHCPv6 を選択すると、**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** は無効になります。

> Cisco Nexus Dashboard Fabric Controller の IPv6 POAP は、Cisco Nexus 7000 シリーズ スイッチではサポートされていません。Cisco Nexus 9000 および 3000 シリーズ スイッチは、スイッチが L2 隣接 (eth1またはアウトオブバンド サブネットは /64 である必要があります）である場合、またはいずれかの IPv6 / 64 サブネットに存在する L3 隣接IPv6 POAP をサポートします。/64 以外のサブネット プレフィックスはサポートされません。

このチェックボックスをオンにしない場合、Nexus ダッシュボード ファブリック コントローラは自動 IP アドレス割り当てにリモートまたは外部DHCPサーバを使用します。

- **[DHCP スコープ開始アドレス（DHCP Scope Start Address）]** および **[DHCP スコープ終了アドレス（DHCP Scope End Address）]**：スイッチのアウトオブバンド POAP に使用される IP アドレス範囲の最初と最後の IP アドレスを指定します。
- **[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]**：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。
- **[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]**：スイッチの Mgmt0 インターフェイスのプレフィックスを指定します。プレフィックスの範囲は 8 ~ 30 です。
- *DHCP 範囲および管理デフォルト ゲートウェイ IP アドレスの仕様（DHCP scope and management default gateway IP address specification）*：管理デフォルト ゲートウェイ IP アドレスを 10.0.1.1 に、サブネット マスクを 24 に指定した場合、DHCP 範囲が指定したサブネット、10.0.1.2 ~ 10.0.1.254 の範囲内であることを確認してください。
- **[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]**：スイッチの Mgmt0 インターフェイスの IPv6 プレフィックスを指定します。プレフィックスは 112 ~ 126 である必要があります。このフィールドは DHCP の IPv6 が有効な場合に編集できます。
- **[AAA 構成を有効化（Enable AAA Config）]**：デバイスの起動時に [詳細（Advanced）] タブから AAA 構成を含めるには、このチェックボックスをオンにします。
- **[ブートストラップ自由形式の構成（Bootstrap Freeform Config）]**：（任意）必要に応じて追加のコマンドを入力します。たとえば、AAAまたはリモート認証関連の設定を使用している場合は、このフィールドにこれらの設定を追加してインテントを保存します。デバイスが起動すると、**[ブートストラップ自由形式の構成（Boostrap Freeform Config）]** フィールドで定義されたインテントが含まれます。

running-config をコピーして **[フリーフォームの設定（freeform config）]** フィールドに、NX-OS スイッチの実行設定に示されているように、正しいインデントでコピーアンドペーストします。freeform config は running config と一致する必要があります。詳細については、ファブリック スイッチでのフリーフォーム設定の有効化を参照してください。

- **[DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）]**：1 行に 1 つのサブネット スコープを入力するフィールドを指定します。**[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すると、このフィールドは編集可能になります。

  スコープの形式は次の順で定義する必要があります。

  [DHCP スコープ開始アドレス、DHCP スコープ終了アドレス、スイッチ管理デフォルト ゲートウェイ、スイッチ管理サブネット プレフィックス（DHCP Scope Start Address, DHCP Scope End Address, Switch Management Default Gateway, Switch Management Subnet Prefix）]

  例：10.6.0.2、10.6.0.9、16.0.0.1、24

5. **[フロー モニタ（Flow Monitor）]** タブをクリックします。このタブのフィールドは次のとおりです。

   - **[NetFlow を有効にする（Enable NetFlow）]**：このチェックボックスをオンにして、このファブリックの VTEP で NetFlow を有効にします。デフォルトでは、NetFlow は無効になっています。有効にすると、NetFlow 設定は、NetFlow をサポートするすべての VTEPS に適用されます。

     注：ファブリックで NetFlow が有効になっている場合、ダミーの no_netflow PTI を使用することで、特定のスイッチでは NetFlow を使用しないように選択できます。

     NetFlow がファブリック レベルで有効になっていない場合、インターフェイス、ネットワーク、または VRF レベルで NetFlow を有効にすると、エラー メッセージが生成されます。Cisco NDFC の NetFlow サポートの詳細については、「NetFlow Support」の「LAN ファブリックについて 」セクションを参照してください。

     [NetFlow エクスポータ（NetFlow Exporter）] エリアで、**[アクション（Actions）] > [追加（Add）]** の順にクリックして、1 つ以上の NetFlow エクスポータを追加します。このエクスポータは、NetFlow データの受信側です。この画面のフィールドは次のとおりです。
     - **[エクスポータ名（Exporter Name）] -** エクスポータの名前を指定します。
     - **[IP]**：エクスポータの IP アドレスを指定します。
     - **[VRF]**： エクスポータがルーティングされる VRF を指定します。
     - **[送信元インターフェイス（Source Interface）]：**送信元インターフェイス名を入力します。
     - **[UDP ポート（UDP Port）]**：NetFlow データがエクスポートされる UDP ポートを指定します。

     [保存（Save）] をクリックしてエクスポータを構成します。破棄するには **[キャンセル（Cancel）]** をクリックします。既存のエクスポータを選択し、**[アクション（Actions）] > [編集（Edit）]** または **[アクション（Actions）] > [削除（Delete）]** を選択して、関連するアクションを実行することもできます。**[NetFlow レコード（NetFlow Record）]** エリアで、**[アクション（Actions）] > [追加（Add）]** の順にクリックして、1 つ以上の NetFlow レコードを追加します。この画面のフィールドは次のとおりです。

- **[レコード名（Record Name）]** - レコードの名前を指定します。
- **[レコード テンプレート（Record Template）]** : レコードのテンプレートを指定します。レコード テンプレート名の 1 つを入力します。リリース 12.0.2 では、次の 2 つのレコード テンプレートを使用できます。カスタム NetFlow レコード テンプレートを作成できます。テンプレート ライブラリに保存されているカスタム レコード テンプレートは、ここで使用できます。
  - **[netflow_ipv4_record]** : IPv4 レコード テンプレートを使用します。
  - **netflow_l2_record -** レイヤ 2 レコード テンプレートを使用します。
- **[レイヤ 2 レコード（Is Layer2 Record）] :** レコードが Layer2 NetFlow の場合は、このチェックボックスをオンにします。

  [保存（Save）] をクリックしてレポートを構成します。**[キャンセル（Cancel）]** をクリックして破棄します。既存のレコードを選択し、**[アクション（Actions）] > [編集（Edit）]** または **[アクション（Actions）] > [削除（Delete）]** を選択して、関連するアクションを実行することもできます。

  [NetFlow モニター（NetFlow Monitor）] エリアで、**[アクション（Actions）] > [追加（Add）]** の順にクリックして、1 つ以上の NetFlow モニターを追加します。この画面のフィールドは次のとおりです。

- **[モニター名（Monitor Name）]** : モニターの名前を指定します。
- **[レコード名（Record Name）]** : モニターのレコードの名前を指定します。
- **[エクスポータ 1 の名前（Exporter1 Name）]** - NetFlow モニターのエクスポータの名前を指定します。
- **[エクスポータ 2 の名前（Exporter2 Name）]** : （オプション）NetFlow モニタの副次的なエクスポータの名前を指定します。

各 NetFlow モニタで参照されるレコード名とエクスポータは、**[Netflow レコード（Netflow Record）]**と **[Netflow エクスポータ（Netflow Exporter）]**で定義する必要があります。**[保存（Save）]** をクリックして、モニターを構成します。破棄するには **[キャンセル（Cancel）]** をクリックします。既存のモニタを選択し、**[アクション（Actions）] > [編集（Edit）]** または **[アクション（Actions）] > [削除（Delete）]** を選択して、関連するアクションを実行することもできます。

6. **[保存（Save）]** をクリックします。

   外部ファブリックが作成されると、外部ファブリックトポロジページが表示されます。

   外部ファブリックを作成したら、スイッチを追加します。

外部ファブリックへのスイッチの追加

各ファブリックのスイッチは一意であるため、各スイッチは 1 つのファブリックにのみ追加できます。外部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. **[LAN] [スイッチ（Switches）]** を選択します。[アクション（Actions）] ドロップダウン リストから、**[スイッチの追加（Add Switches）]** を選択します

   [LAN] > [ファブリック（Fabrics）] からファブリックにスイッチを追加することもできます。ファブリックを選択し、**[概要（Summary）]** を表示します。**[スイッチ（Switches）]** タブの **[アクション（Actions）]**ドロップダウン リストから、**[スイッチの追加（Add Switches）]** を選択して、選択したファブリックにスイッチを追加します。

   [トポロジ（Topology）] から、[ファブリック（Fabric）] を右クリックし、**[スイッチの追加（Add Switches）]** を選択します。

2. 新しいスイッチを検出するには、**[検出（Discover）]** を選択します。既存のスイッチをファブリックに追加するには、**[ネイバー スイッチを移動する（Move Neighbor Switches）]** を選択します。
3. **[検出（Discover）]** オプションを選択した場合は、次の手順を実行します。

   a. スイッチの IP アドレス（シード IP）を入力します。

   b. **[認証プロトコル（Authentication Protocol）]** フィールドで、ドロップダウン リストから、ファブリックにスイッチを追加するための適切なプロトコルを選択します。

   c. **[デバイス タイプ（Device Type）]** ドロップダウン リストからデバイス タイプを選択します。

      オプションは、**[NX-OS]**、**[IOS XE]**、**[IOS XR]** および **[その他（Other）]** です。

      - Cisco Nexus スイッチを検出するには、**[NX-OS]** を選択します。
      - CSR デバイスを検出するには、**[IOS XE]** を選択します。
      - ASR デバイスを検出するには、**[IOS XR]** を選択します。
      - Cisco 以外のデバイスを検出するには、**[その他（Other）]** を選択します。

        他の非 Nexus デバイスの追加の詳細については、*外部ファブリックへの非 Nexus デバイスの追加*の項を参照してください。

        Cisco CSR 1000v を除くすべての Nexus 以外のデバイスの設定コンプライアンスは無効です。

   d. スイッチ管理者ユーザ名およびパスワードを入力します。

   e. 画面の下部にある **[スイッチの検出（Discovery Switches）]** をクリックします。

      [スキャン詳細（Scan Details）] セクションが間もなく表示されます。[最大ホップ（Max Hops）] フィールドに 2 が入力されているため、指定された IP アドレスを持つスイッチとその 2 ホップのスイッチが入力されます。

      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、**[スイッチをファブリックに追加する（Add Switches into fabric）]** をクリックします。

      複数のスイッチを同時に検出できます。スイッチは適切にケーブル接続して、Nexus Dashboard Fabric Controller サーバーに接続する必要があり、スイッチのステータスは管理可能である必要があります。

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、進行状況が表示されます。Nexus Dashboard ファブリック コントローラがスイッチを検出したら、**[閉じる（Close）]** をクリックして、前の画面に戻ります。

4. **[ネイバー スイッチを移動する（Move Neighbor Switches）]** オプションを選択した場合は、スイッチを選択して **[スイッチを移動する（Move Switch）]** をクリックします。

   選択したスイッチが外部ファブリックに移動します。

外部ファブリック向けスイッチ設定

外部ファブリック スイッチの設定は、VXLAN ファブリック スイッチの設定とは異なります。スイッチをダブルクリックして [スイッチの概要（Switch Overview）] 画面を表示し、オプションを編集/変更します。

次のオプションがあります。

[ロールの設定（Set Role）]：デフォルトでは、外部ファブリック スイッチにロールは割り当てられません。ファブリックに必要なロールを割り当てることができます。Multi-Site Inter-Fabric Connection（IFC）のコア ルータ ロールと、外部ファブリックと VXLAN ファブリック境界デバイス間の VRF Lite IFC のエッジ ルータ ロールを割り当てます。

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。

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。

[モードの変更（Change Modes）]：スイッチのモードを [アクティブ（Active）] から [動作（Operational）] 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。

ストレート FEX、アクティブ/アクティブ FEX、およびインターフェイスのブレークアウトは、外部ファブリック スイッチ インターフェイスではサポートされません。

[ポリシーの表示/編集（View/edit Policies）]：スイッチでポリシーを追加、更新、および削除します。スイッチに追加するポリシーは、テンプレート ライブラリで使用可能なテンプレートのテンプレート インスタンスです。ポリシーを作成したら、[ポリシーの表示/編集（View / edit Policies）] 画面で使用できる [展開（Deploy）] オプションを使用してスイッチに展開します。

履歴：スイッチの展開履歴を表示します。

[構成の再計算（Recalculate Config）]：保留中の構成と、実行構成および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。

[アクション（Actions）] ドロップダウン リストから **[展開（Deploy）]** 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、スイッチの設定を形成します。

[展開（Deploy）] をクリックすると、**[構成の展開（Deploy Configuration）]** 画面が表示されます。

画面の下部にある **[構成（Config）]** をクリックして、保留中の構成をスイッチに展開します。 次の**[展開の進行状況（Deploy Progress）]** 画面に、構成の展開の進行状況とステータスが表示されます。

展開が完了したら、**[閉じる（Close）]** をクリックします。

外部ファブリック内のスイッチがデフォルトのクレデンシャルを受け入れない場合は、次のいずれかの操作を実行する必要があります。

- インベントリから外部ファブリックのスイッチを削除し、再検出します。

- LAN ディスカバリは SNMP と SSH の両方を使用するため、両方のパスワードを同じにする必要があります。スイッチの SNMP パスワードと一致するように SSH パスワードを変更する取得されます。SNMP 認証が失敗すると、検出は認証エラーで停止します。SNMP 認証は成功したが SSH 認証が失敗した場合、Nexus Dashboard Fabric Controller で検出は続行されますが、スイッチのステータスに SSH エラーの警告が表示されます。

新しいスイッチの検出

新しいスイッチを検出するには、次の手順を実行します。

1. Nexus Dashboard Fabric Controller サーバーにケーブル接続されていることを確認してから、外部ファブリックの新しいスイッチの電源をオンにします。

   Cisco NX-OS を起動し、スイッチのクレデンシャルを設定します。

2. スイッチで **write**、**erase**、および **reload** コマンドを実行します。

   [はい（Yes）] または [いいえ（No）] の選択を求める両方の CLI コマンドに対して **[はい（Yes）]** を選択します。

3. Nexus ダッシュボード ファブリック コントローラ UI で、[外侮ファブリック（External Fabric）] を選択します。**[ファブリックの編集（Edit Fabric）]** を **[アクション（Actions）]** ドロップダウン リストから 選択します。

   [ファブリックの編集（Edit Fabric）] 画面が表示されます。

4. **[ブートストラップ（Bootstrap）]** タブをクリックし、DHCP 情報を更新します。
5. **[ファブリックの編集（Edit Fabric）]** 画面の右下の **[保存（Save）]** をクリックして、設定を保存します。
6. ファブリックをダブルクリックして **[ファブリックの概要（Fabric Overview）]** を表示します。
7. **[スイッチ（Switches）]** タブで、**[アクション（Actions）]** ドロップダウン リストから **[スイッチの追加（Add Switches）]** を選択します。
8. **[POAP]** タブをクリックします。

   前の手順では、reload コマンドをスイッチで実行していました。スイッチが再起動してリブートすると、Nexus Dashboard Fabric Controller はスイッチからシリアル番号、モデル番号、およびバージョンを取得し、[インベントリ管理（Inventory Management）] 画面に表示します。また、管理 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、画面の右上にある [更新（Refresh）] アイコンを使用して画面を更新します。

   

   画面の左上には、エクスポートとインポートのオプションが表示され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。

   スイッチの横にあるチェックボックスをオンにして、スイッチのクレデンシャル（IP アドレスとホスト名）を追加します。

   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。

9. **[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。

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。

10. 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。

    - 使用できるディスカバリクレデンシャルは、AAA 認証ベースのクレデンシャル（RADIUS または TACACS）です。
    - 検出クレデンシャルは、デバイス設定のコマンドに変換されません。このクレデンシャルは、主にスイッチを検出するリモート ユーザー（または管理ユーザー以外）を指定するために使用されます。デバイス構成の一部としてコマンドを追加する場合は、ファブリック設定の **[ブートストラップ（Bootstrap）]** タブにある **[ブートストラップ自由形式構成（Bootstrap Freeform Config）]** フィールドにコマンドを追加します。また、**[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウからそれぞれのポリシーを追加できます

11. 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。

    追加されたスイッチが POAP を完了すると、ファブリック ビルダー トポロジ画面に、追加されたスイッチと物理接続が表示されます。

12. スイッチをモニタし、POAP 完了を確認します。
13. **[設定の展開]** を、**[アクション（Actions）]** ドロップダウンリストでクリックして（**[ファブリックの概要（Fabric Overview）]** 画面）、保留中の設定（テンプレートやインターフェイス設定など）をスイッチに展開します。

    - スイッチと Nexus Dashboard Fabric Controller の間に同期の問題がある場合、スイッチ アイコンが赤色で表示され、ファブリックが同期していないことを示します。ファブリックの変更が原因で同期が外れた場合は、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。
    - 検出ログイン情報が、デバイス構成のコマンドに変換されることはありません。このクレデンシャルは、主にスイッチを検出するリモート ユーザー（または管理ユーザー以外）を指定するために使用されます。デバイス構成の一部としてコマンドを追加する場合は、ファブリック設定の **[ブートストラップ（Bootstrap）]** タブにある **[ブートストラップ自由形式構成（Bootstrap Freeform Config）]** フィールド

にコマンドを追加します。また、**[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウからそれぞれのポリシーを追加できます。

ファブリックの作成時に、**[管理性（Manageability）]** タブに AAA サーバー情報を入力した場合は、各スイッチの 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。

14. 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。
15. [トポロジ（Topology）] 画面で、**[トポロジの更新（Refresh Topology）]** アイコン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。

    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。
16. 展開された設定を表示するには、右クリックして [履歴（History）] を選択します。

    詳細を確認するには、**[ステータス（Status）]** 列の **[成功（Success）]** リンクをクリックしてください。例：
17. Nexus Dashboard Fabric Controller UI 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。すべてのインターフェイスがトランク ポートに設定されます。追加設定を行うには、**[LAN] > [インターフェイス（Interfaces）]**オプションを使用してインターフェイスを構成する必要があります。以下の構成が含まれますが、これらに限定されません。

    - vPC ペアリング。
    - ブレークアウト インターフェイス

      ブレークアウト インターフェイスのサポートは、9000 シリーズ スイッチで使用できます。

    - ポート チャネル、およびポートへのメンバーの追加。

スイッチ（新規または既存）を検出した後、いつでも次のことが行えます。POAP プロセスを使用して構成を再度プロビジョニングします。このプロセスにより、既存の設定が削除され、新しい設定がプロビジョニングされます。また、POAP を呼び出さずに設定を段階的に展開することもできます。

非 Nexus デバイスを外部ファブリックに追加する

Cisco Nexus Dashboard Fabric Controller リリース 12.0.1a 以降では、管理対象モードでも外部ファブリックに Cisco IOS XR デバイスを追加できます。外部ファブリックで次の Cisco IOS XR デバイスを管理できます。

- Cisco ASR 9000 シリーズ ルータ
- Cisco NCS 5500 シリーズ ルータ、IOS XR リリース6.5.3

Cisco Nexus Dashboard ファブリック コントローラ リリース 12.1.1e から、管理モードとモニタ モードの両方で Cisco 8000 シリーズ ルータを外部ファブリックに追加することもできるようになりました。

外部ファブリックで Nexus 以外のデバイスを検出し、これらのデバイスの設定コンプライアンスも実行できます。詳細については、「外部ファブリックの構成コンプライアンス」の項を参照してください。

Cisco Nexus Dashboard Fabric Controller がサポートする非Nexus デバイスについては、*Cisco Compatibility Matrix*を参照してください。

デフォルトでは、Cisco Nexus スイッチのみが SNMP 検出をサポートします。したがって、すべての非 Nexus デバイスを外部ファブリックに追加する前に設定してください。非 Nexus デバイスの設定には、SNMP ビュー、グループ、およびユーザーの設定が含まれます。詳細については、「Nexus 以外のデバイスの検出の構成」の項を参照してください。

Cisco CSR 1000v は SSH を使用して検出されます。Cisco CSR 1000v は、SNMP がセキュリティ上の理由でブロックされているクラウドでもインストールできるため、SNMP のサポートは必要ありません。外部ファブリックに Cisco CSR 1000v、Cisco IOS XE Gibraltar 16.10.xを追加する使用例については、「*Cisco Data Centerとパブリック クラウドの接続*」の章を参照してください。

ただし、Cisco Nexus Dashboard Fabric Controller がアクセスできるのは、システム名、シリアル番号、モデル、バージョン、インターフェイス、稼働時間などの基本的なデバイス情報に限られます。ホストが CDP または LLDP の一部である場合、Cisco Nexus Dashboard Fabric Controller は非 Nexus デバイスを検出しません。

ファブリックトポロジウィンドウで非 Nexus デバイスを右クリックすると多くのオプションが表示されますが、非Nexus デバイスに適用されない設定は空白で表示されます。ASR 9000 シリーズ ルータおよび Arista スイッチのインターフェイスは追加または編集できません。

Cisco Catalyst 9000 シリーズスイッチや Cisco ASR 1000 シリーズ ルータなどの IOS XE デバイスは外部ファブリックに追加できます。

外部ファブリックでのコンプライアンスの構成

外部ファブリックを使用すると、Nexus スイッチ、Cisco IOS XE デバイス、Cisco IOS XR デバイス、および Arista をファブリックにインポートできます。展開のタイプに制限はありません。LAN クラシック、VXLAN、FabricPath、vPC、HSRP などを使用できます。スイッチが外部ファブリックにインポートされるとき、非中断となるようにスイッチの設定が保持されます。スイッチユーザ名やmgmt0インターフェイスなどの基本ポリシーのみが、スイッチのインポート後に作成されます。

外部ファブリックでは、DCNM で定義されているインテントに対して、構成コンプライアンス（CC）により、このインテントが対応するスイッチに存在することが保証されます。

このインテントがスイッチに存在しない場合、CCはOut-of-Syncステータスを報告します。さらに、このインテントをスイッチにプッシュしてステータスを同期中に変更するために生成された保留中の設定があります。スイッチ上にあるが、Nexus Dashboard Fabric Controller で定義されたインテントではない追加の構成は、インテント内の設定との競合がない限り、CCによって無視されます。

前述のように、ユーザ定義のインテントが Nexus Dashboard Fabric Controller に追加され、同じトップレベルコマンドの下にスイッチの追加構成がある場合、CC は Nexus Dashboard Fabric Controller で定義されたインテントがスイッチに存在することのみを確認します。Nexus Dashboard Fabric Controller 上のこのユーザー定義インテントがスイッチから削除する目的で全体として削除され、対応する構成がスイッチに存在する場合、CC はスイッチの OUT-OF-SYNC ステータスをレポートし、**[保留中の構成（Pending Config）]** を作成してスイッチからその構成を削除します。この**保留中の構成**には、トップレベルのコマンドの削除が含まれています。このアクションにより、このトップレベルコマンドでスイッチで行われた他のアウトオブバンド設定も削除されます。この動作を上書きすることを選択した場合は、自由形式ポリシーを作成し、関連する最上位コマンドを自由形式ポリシーに追加することを推奨します。

この動作を例で見てみましょう。

1. Nexus Dashboard Fabric Controller のユーザーがスイッチに定義し、スイッチに展開した **switch_freeform** ポリシー。
2. 実行構成の **router bgp** の下に、ユーザー定義 Nexus Dashboard Fabric Controllerインテントの**予期される構成**に存在しない追加構成があります。Nexus Dashboard Fabric Controller 上で、ユーザー定義のインテントなしでスイッチに存在する追加の構成を削除する **[保留中の構成（Pending Config）]** はありません。
3. 手順 1 で作成された switch_freeform ポリシーを削除することで、Nexus Dashboard Fabric Controller によって以前にプッシュされたインテントがから削除された場合の**保留中の構成**と**並列比較**。
4. 最上位の **router bgp** コマンドを使用して **switch_freeform** ポリシーを作成する必要があります。これにより、CC は以前に Nexus Dashboard Fabric Controller からプッシュされた目的のサブ構成のみを削除するために必要な構成を生成できます。
5. 削除された構成は、以前に Nexus Dashboard Fabric Controller からプッシュされた構成のサブセットのみです。

   外部ファブリックのスイッチのインターフェイスでは、Nexus Dashboard Fabric Controller はインターフェイス全体を管理するか、まったく管理しません。CC は次の方法でインターフェイスをチェックします。

   - 任意のインターフェイスについて、ポリシーが定義され、関連付けられている場合、このインターフェイスは管理対象と見なされます。このインターフェイスに関連付けられているすべての設定は、関連付けられたインターフェイス ポリシーで定義する必要があります。これは、論理インターフェイスと物理インターフェイスの両方に適用されます。それ以外の場合、CCは、インターフェイスに行われたアウトオブバンド更新を削除して、ステータスを[In-Sync]に変更します。
   - アウトオブバンドで作成されたインターフェイス（ポートチャネル、サブインターフェイス、SVI、ループバックなどの論理インターフェイスに適用）は、通常の検出プロセスの一部として Nexus Dashboard Fabric Controller によって検出されます。ただし、これらのインターフェイスにはインテントがないため、CC はこれらのインターフェイスの **[OUT-OF-SYNC]** ステータスをレポートしません。
   - どのインターフェイスにも、Nexus Dashboard Fabric Controller に関連付けられたモニタ ポリシーが常に存在する可能性があります。この場合、CC は **[同期中（In-Sync）]** または **[同期外（Out-of-Sync）]** 構成構成ステータスを**レポート**するときに、インターフェイスの構成を無視します。

構成コンプライアンスで無視される特別な構成 CLI

次の構成 CLI は、構成コンプライアンス チェック中に無視されます。

- 「ユーザー名」とともに「パスワード」が含まれている CLI
- 「snmp-server user」で始まるすべての CLI

上記に一致する CLI は保留中の差分に表示されず、[ファブリック ビルダー（Fabric Builder）] ウィンドウで [保存して展開（Save & Deploy）] をクリックしても、そのような設定はスイッチにプッシュされません。これらの CLI は、並列比較ウィンドウにも表示されません。

このような構成 CLI を展開するには、次の手順を実行します。

1. **[LAN] > [ファブリック（Fabrics）]** を選択します。

   ファブリック名をダブルクリックして **[ファブリックの概要（Fabric Overview）]** 画面を表示します。

2. [スイッチ（Switch）] タブで、スイッチ名をダブルクリックして、**[スイッチの概要（Switch Overview）]** 画面を表示します。

   [ポリシー（Policies）] タブには、選択したファブリック内のスイッチに適用されているすべてのポリシーが一覧表示されます。

3. [ポリシー（Policies）] タブで、**[アクション（Actions）]** ドロップダウン リストから **[ポリシーの追加（Add Policy）]** を選択します。
4. 必要な構成を持つポリシー テンプレート インスタンス（PTI）を追加します**switch_freeform** テンプレートを選択し、**[保存（Save）]** をクリックします。
5. 作成したポリシーを選択し、**[構成のプッシュ（Push Config）]**（**[アクション（Actions）]** ドロップダウン リスト）を選択して、構成をスイッチに展開します。

NDFC を使用した Cisco IOS XR デバイスの管理

一般に、ワークロードには、データセンター ファブリック内のデータセンター ドメイン外のサービスとの通信が必要です。これには、インターネットおよび WAN からアプリケーションおよびサービスにアクセスするユーザーの通信が含まれます。境界デバイスを備えた VXLAN EVPN ファブリックは、North-South 接続のハンドオフと見なされます。これらの境界デバイスは、WAN およびインターネット接続のバックボーン ルータである IOS XR ルータとピアにあります。

DCNM リリース 11.5(x) では、管理者ロールを持つユーザーは、モニタリング、自動化、コンプライアンスなどの機能を使用して VXLAN EVPN ファブリックを制御できます。IOS XR ルータは、モニタ対象モードでのみモニタリングできます。したがって、これらのデバイス間の構成を管理および自動化し、異なるサービス間の通信の構成コンプライアンスのバランスをとってチェックするするために、単一のファブリック コントローラに必要な要件です。

NDFC リリース 12.0.1a 以降、管理者ロールを持つユーザーは、自動化とコンプライアンスの確認に限定された IOS XR ルータを管理できます。境界スイッチと IOS XR ルータ間の eBGP VRF Lite ハンドオフを自動化および管理するために、新しいテンプレートとポリシーが導入されています。NDFC を使用すると、外部ファブリックの Cisco Nexus スイッチと同様に、IOS XR デバイスの構成コンプライアンスを確認できます。

Nexus 以外のすべてのデバイスの場合、SNMPv3 認証では MD5 プロトコル オプションのみがサポートされます。

エッジ ルータとしての IOS XR の構成

IOS XR のボーダー デバイスをエッジ ルータとして使用して Cisco Nexus 9000 ファブリックから VRF Lite を拡張するには、「*Cisco Nexus 9000 ベースのボーダーと非 Nexus デバイス間の VRF Lite*」の項を参照してください。

詳細については、NDFC を使用した ASR 9000 の管理と構成のビデオを参照してください。

ディスカバリ用の非 Nexus デバイスの設定

Cisco Nexus Dashboard Fabric Controller で非 Nexus デバイスを検出する前に、スイッチ コンソールで構成します。

ディスカバリ用の IOS XE デバイスの構成

障害が発生した場合、またはデバイスの設定に問題がある場合は、シスコのテクニカル アシスタンスセンター（TAC）に連絡してください。Nexus Dashboard Fabric Controller の Cisco XE デバイスを検出する前に、以下のステップを実行します。

1. スイッチ コンソールで次の SSH コマンドを実行します。

```
switch (config)# hostname <hostname>
switch (config)# ip domain name <domain_name>
switch (config)# crypto key generate rsa
switch (config)# ip ssh time-out 90
switch (config)# ip ssh version 2
switch (config)# line vty 1 4
switch (config-line)# transport input ssh
switch (config)# username admin privilege secret <password>
switch (config)# aaa new-model
switch (config)# aaa authentication login default local
switch (config)# aaa authorization exec default local none
```

2. スイッチで SNMP コマンドを実行する前に、IP アドレス、ユーザー名、および SNMP 関連の構成がスイッチで定義されていることを確認します。スイッチ コンソールで次の SNMP コマンドを実行します。

```
aaa new-model
aaa session-id common
 ip domain name cisco
username admin privilege 15 secret 0 xxxxx
snmp-server group group1 v3 auth read view1 write view1
snmp-server view view1 mib-2 included
snmp-server view view1 cisco included
```

```
snmp-server user admin group1 v3 auth md5 xxxxx priv des xxxxx
line vty 0 4
privilege level 15
transport input all
line vty 5 15
privilege level 15
transport input all
line vty 16 31
transport input ssh
```

検出用 Arista デバイスの構成

次のコマンドを使用して、特権 EXEC モードを有効化します。

```
switch> enable
switch#


switch# show running confiruation | grep aaa          /* 承認を表示する場合*/
aaa authorization exec default local
```

Arista デバイスを構成するには、スイッチ コンソールで次のコマンドを実行します。

```
switch# configure terminal
switch (config)# username ndfc privilege 15 role network-admin secret cisco123
snmp-server view _view_name_ SNMPv2 included
snmp-server view _view_name_ SNMPv3 included
snmp-server view _view_name_ default included
snmp-server view _view_name_ entity included
snmp-server view _view_name_ if included
snmp-server view _view_name_ iso included
snmp-server view _view_name_ lldp included
snmp-server view _view_name_ system included
snmp-server view sys-view default included
snmp-server view sys-view ifmib included
snmp-server view sys-view system included
snmp-server community private ro
snmp-server community public ro
snmp-server group _group_name_ v3 auth read _view_name_
snmp-server user username _group_name_ v3 auth md5 _password_ priv aes _password_
```

SNMP パスワードはユーザ名のパスワードと同じにする必要があります。ユーザーは、**show run** コマンドを実行して構成設定を確認し、**show snmp view** コマンドを実行して SNMP ビューの出力を表示できます。

show run コマンド [ソース]

```
switch (config)# snmp-server engineID local f5717f444ca824448b00
snmp-server view _view_name_ SNMPv2 included
snmp-server view _view_name_ SNMPv3 included
snmp-server view _view_name_ default included
snmp-server view _view_name_ entity included
snmp-server view _view_name_ if included
snmp-server view _view_name_ iso included
snmp-server view _view_name_ lldp included
snmp-server view _view_name_ system included
snmp-server view sys-view default included
snmp-server view sys-view ifmib included
snmp-server view sys-view system included
snmp-server community private ro
snmp-server community public ro
snmp-server group _group_name_ v3 auth read _view_name_
snmp-server user _user_name group_name_ v3 localized f5717f444ca824448b00 auth
md5 be2eca3fc858b62b2128a963a2b49373 priv aes
be2eca3fc858b62b2128a963a2b49373
!
spanning-tree mode mstp
!
service unsupported-transceiver labs f5047577
!
aaa authorization exec default local
!
no aaa root
!
username admin role network-admin secret sha512
$6$5ZKs/7.k2UxrWDg0$FOkdVQsBTnOquW/9AYx36YUBSPNLFdeuPlse9XgyHSdEOYXtPyT/
0sMUYYdkMffuljgn/d9rx/Do71XSbygSn/
username cvpadmin role network-admin secret sha512
$6$fLGFj/PUcuJT436i$Sj5G5c4y9cYjl/BZswjjmZW0J4npGrGqlyG3ZFk/ULza47Kz.d31q13jXA
7iHM677gwqQbFSH2/3oQEaHRq08.
username ndfc privilege 15 role network-admin secret sha512
$6$M48PNrCdg2ElTEdG$iiB880nvFQQlrWoZwOMzdt5EfkuClraNqtEMRS0TJUhNKCQnJN.VD
LFsLAmP7kQBo.C3ct4/.n.2eRlcP6hij/
```

show snmp view コマンド [ソース]

```
configure terminal# show snmp view
view_name SNMPv2 - included
view_name SNMPv3 - included
```

```
view_name default - included
view_name entity - included
view_name if - included
view_name iso - included
view_name lldp - included
view_name system - included
sys-view default - included
sys-view ifmib - included
sys-view system - included
leaf3-7050sx#show snmp user

User name : _user_name_
Security model : v3
Engine ID : f5717f444ca824448b00
Authentication : MD5
Privacy : AES-128
Group : _group_name_
```

ディスカバリ用の Cisco IOS XR デバイスの構成と確認

IOS XR デバイスを構成するには、スイッチ コンソールで次のコマンドを実行します。

```
switch# configure terminal
switch (config)# snmp-server viewview_namecisco included
snmp-server view _view_name_ mib-2 included
snmp-server group _group_name_ v3 auth read _view_name_ write _view_name_
snmp-server user _user_name group_name_ v3 auth md5 password priv des56 password
SystemOwner
```

次に、スイッチで IOS XR デバイスを構成する例を示します。

```
RP/0/RSP0/CPU0:ios(config)#snmp-server view view_name cisco included
RP/0/RSP0/CPU0:ios(config)#snmp-server view view_namemib-2 included
RP/0/RSP0/CPU0:ios(config)#snmp-server group group_name v3 auth read view_name
write view_name
RP/0/RSP0/CPU0:ios(config)#snmp-server user user_name_group_name_ v3 auth md5
password priv des56 passwordSystemOwner
RP/0/RSP0/CPU0:ios(config)#commit Day MMM DD HH:MM:SS Timezone
```

IOS XR デバイスを確認するには、次のコマンドを実行します。

```
RP/0/RSP0/CPU0:ios(config)#
RP/0/RSP0/CPU0:ios(config)#show run snmp-server Day MMM DD HH:MM:SS Timezone
```

```
snmp-server user user_name group1 v3 auth md5 encrypted 10400B0F3A4640585851 priv
des56 encrypted 000A11103B0A59555B74 SystemOwner
snmp-server view _view_name_cisco included
snmp-server view _view_name_mib-2 included
snmp-server group group_name v3 auth read view_name write view_namev3 auth read
_view_name_ write _view_name_
```

外部ファブリックで非 Nexus デバイスの検出

始める前に：

外部ファブリックに追加する前に、非 Nexus のデバイスの設定がプッシュされていることを確認します。モニタ モードでは、ファブリックの設定をプッシュできません。

ファブリック トポロジ ウィンドウで外部ファブリックに非 Nexus デバイスを追加するには、次の手順を実行します。

1. **[アクション（Actions）]** ペインで **[スイッチの追加（Add switches）]** をクリックします。
2. **[既存スイッチの検出（Discover Existing Switches）]** タブの次のフィールドに値を入力します。

フィールド	説明
シードIP	スイッチのIP アドレスを入力します。スイッチのIP アドレスの範囲を入力することにより、複数のスイッチをインポートできます。たとえば 10.10.10.40-60 です。スイッチは適切にケーブル接続して、Nexus Dashboard Fabric Controller サーバーに接続する必要があり、スイッチのステータスは管理可能である必要があります。
デバイス タイプ	• C、IOS XRisco CSR 1000v、Cisco ASR 1000 シリーズ ルータ、または Cisco Catalyst 9000 シリーズ スイッチを追加するには、ドロップダウンリストから **[IOS XE]** を選択します。 • ASR 9000 シリーズ ルータ、Cisco NCS 5500 シリーズ ルータ リリース 6.5.3 または Cisco 8000 シリーズ ルータを追加するには、ドロップダウンリストから **[IOS XR]** を選択します。 Cisco IOS XR デバイスを追加するには、管理対象モードで、ファブリック設定で **[一般パラメータ（General Parameters）]** に移動し **[ファブリック モニタ モード（Fabric Monitor Mode）]** チェックボックスをオフにします。 • シスコ以外のデバイス（Arista スイッチなど）を追加するには、ドロップダウンリストから **[その他（Other）]** を選択します。
ユーザ名	ユーザ名を入力します。
[パスワード（Password）]	パスワードを入力します。

すでに検出されているデバイスを検出しようとすると、エラー メッセージが表示されます。
パスワードが設定されていない場合は、**[LAN クレデンシャル（LAN Credentials）]** ウィンドウでデバイスのパスワードを設定します。Cisco Nexus Dashboard Fabric Controller Web UI から**[LAN クレデンシャル（LAN Credentials）]** ウィンドウに移動するには、**[管理（Administration）] > [LAN クレデンシャル（LAN Credentials）]** を選択します。

3. **[検出の開始（Start Discovery）]** をクリックします。

   [スキャンの詳細（Scan Details）] セクションが表示され、スイッチの詳細が入力されます。

4. インポートするスイッチに隣接するチェックボックスをオンにします。
5. **[ファブリックにインポート（Import into fabric）]** をクリックします。

   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、進行状況が表示されます。

   デバイスの検出には時間がかかります。検出の進行状況が **[100%]** または **[完了（done）]** になった後、デバイスの検出に関するポップアップ メッセージが右下に表示されます。次に例を示します。**[<ip-address> 検出用に追加されました。（<ip-address> added for discovery.）]**

スイッチをファブリックにインポートしようとした後で、「基本的なスイッチ設定の（シード インターフェイス）インテントの作成中にエラーが発生しました（Error while creating the (Seed interface) intent for basic switch configurations）」というようなエラー メッセージが表示されることがあります。構成の［保存/展開（Save/Deploy）］を使用して再試行してください。これは、スイッチをファブリックにインポートしようとする前に、スイッチに権限が適切に設定されていないことが原因である可能性があります。「IOS XE デバイスを検出できるように構成する」の手順を使用してスイッチの権限を設定し、スイッチをファブリックに再度インポートしてください。

6. **[閉じる（Close）]** をクリックします。

   ファブリック トポロジ ウィンドウにスイッチが表示されます。

7. 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。
8. **[ファブリックの概要（Fabric Overview）]** をクリックします。

   スイッチとリンクのウィンドウが表示され、スキャンの詳細を確認できます。検出が進行中の場合、検出ステータスは赤色で **[検出中（discovering）]** と表示され、その横に警告アイコンが表示されます。

9. デバイスの詳細を表示します。

   デバイスの検出後：

   - 検出ステータは緑色の **[OK]** に変わり、横のチェックボックスがオンになります。
   - **[ファブリック ステータス（Fabric Status）]** 列のデバイスの値が **[同期中（In-Sync）]** に変わります。

スイッチが **[到達不能（Unreachable）]** 検出ステータスの場合、残りの列にはスイッチの最後の使用可能な情報が保持されます。たとえば、スイッチ がスイッチが到達不可能になる前に**[実行中（RUNNING）]** トラッカー ステータスであった場合、このスイッチの **[トラッカー ステータス（Tracker Status）]** 列の値は、スイッチが **[到達不可能（Unreachable）]** 検出ステータスに**なっ**たにもかかわらず、**[実行中（RUNNING）]** のままになります。

次に行う作業：

適切なロールを設定します。デバイスを右クリックし、**[ロールの設定（Set role）]** を選択します。これらのデバイスを管理対象モードで追加した場合は、ポリシーも追加できます。

Nexus 以外のデバイスから外部ファブリックへの管理

Nexus Dashboard Fabric Controller 12.0.1a 以降、IOS XR は管理対象モードでサポートされます。

IOS XE および IOS XR スイッチでは、外部ファブリックで Nexus スイッチを処理する場合と同様に、構成コンプライアンスが有効になります。詳細については、外部ファブリックの設定コンプライアンスの項を参照してください。

Nexus Dashboard Fabric Controller は、IOS XR デバイスの展開の最後にコミットを送信します。

Nexus Dashboard Fabric Controller には、IOS XR デバイス用のテンプレートがいくつか用意されています。IOS-XR スイッチをエッジ ルータにして、ボーダーとの eBGP ピアリングを確立するには、 **ios_xr_Ext_VRF_Lite_Jython.template** を使用します。これにより、VRF の構成、VRF の eBGP ピアリング、およびサブインターフェイスが作成されます。同様に、**[ios_xe_Ext_VRF_Lite_Jython]** を使用して、IOS XE スイッチをエッジ ルータとして使用し、ボーダーとの eBGP ピアリングを確立できます。

vPC セットアップの作成

vPC ペアリング

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。

   

   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。

   - 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。

   - 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。

   - **[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**に構成がクリアされません。NVE 構成、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。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 チャネルを削除できます。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。

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。

シスコが採用している 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）。