Control

この章は次のトピックで構成されています。

ファブリック

このマニュアルでは、次の用語を使用しています。

- グリーンフィールド展開：新しい VXLAN EVPN ファブリックおよび eBGP ベースのルーテッド ファブリックのプロビジョニングに適用されます。
- ブラウンフィールド展開：既存の VXLAN EVPN ファブリックに適用されます。
  - **[Easy_Fabric_11_1]** ファブリック テンプレートを使用して、CLI で構成された VXLAN EVPN ファブリックを DCNM に移行します。
  - **[Easy_Fabric_11_1]** ファブリック テンプレートを使用した Cisco DCNM への NFM 移行。

アップグレードについては、『*LAN* ファブリックの展開用 *Cisco DCNM* インストールおよびアップグレードガイド』を参照してください。

ここでは、次の内容について説明します。

VXLAN BGP EVPN ファブリックのプロビジョニング

DCNM 11 では、Nexus 9000 および 3000 シリーズ スイッチでの VXLAN BGP EVPN 構成の統合アンダーレイおよびオーバーレイ プロビジョニングのための拡張「Easy」ファブリック ワークフローを導入しています。ファブリックの設定は、強力で柔軟でカスタマイズ可能なテンプレートベースのフレームワークによって実現されます。最小限のユーザー入力に基づいて、シスコ推奨のベストプラクティス設定により、ファブリック全体を短時間で立ち上げることができます。[ファブリック設定（Fabric Settings）]で公開されている一連のパラメータにより、ユーザーはファブリックを好みのアンダーレイ プロビジョニング オプションに合わせて調整できます。

ファブリック内の境界デバイスは通常、適切なエッジ/コア/WANルータとのピアリングを介して外部接続を提供します。これらのエッジ/コア ルータは、DCNM によって管理またはモニタできます。これらのデバイスは、外部ファブリックと呼ばれる特別なファブリックに配置されます。同じDCNM コントローラが、複数のVXLAN BGP EVPNファブリックを管理できると同時に、マルチサイト ドメイン（MSD）ファブリックと呼ばれる特別な構造を使用して、これらのファブリック間のレイヤ 2 およびレイヤ 3 DCI アンダーレイおよびオーバーレイ構成を簡単にプロビジョニングし、管理できます。

このドキュメントでは、「スイッチ」と「デバイス」という用語は同じ意味で使用されていることにご注意ください。

VXLAN BGP EVPN ファブリックを作成および展開するための DCNM GUI の機能は次のとおりです。

[制御（Control）] > [ファブリック ビルダ（Fabric Builder）] メニューオプション（**[ファブリック（Fabrics）]** サブメニューの下）。

ファブリックの作成、編集、および削除：

- 新しい VXLAN、MSD、および外部 VXLAN ファブリックを作成します。
- ファブリック間の接続を含む、VXLANおよびMSDファブリック トポロジを表示します。
- ファブリック設定を更新します。
- 更新された変更を保存し、展開します。
- ファブリックを削除します（デバイスが削除された場合）。

新しいスイッチでのデバイス検出とプロビジョニングの起動設定：

- ファブリックにスイッチ インスタンスを追加します。
- POAP設定を使用して、新しいスイッチに起動設定とIPアドレスをプロビジョニングします。
- スイッチ ポリシーを更新し、更新された変更を保存し、展開します。
- ファブリック内およびファブリック間リンク（ファブリック間接続（IFC）とも呼ばれる）を作成します。

[制御（Control）] > [インターフェイス（Interfaces）] メニューオプション（**[ファブリック（Fabrics）]** サブメニューの下）。

アンダーレイのプロビジョニング：

- ポートチャネル、vPC スイッチ ペア、ストレート スルー FEX（ST-FEX）、アクティブ-アクティブ FEX（AA-FEX）、ループバック、サブインターフェイスなどを作成、展開、表示、編集、削除します。
- ブレイクアウト ポートとアンブレイクアウト ポートを作成します。
- インターフェイスをシャットダウンして起動します。
- ポートを再検出し、インターフェイスの設定履歴を表示します。

[制御（Control）] > [ネットワーク（Networks）] および **[制御（Control）] > [VRF]** メニューオプション（**[ファブリック（Fabrics）]** サブメニューの下）。

オーバーレイ ネットワークのプロビジョニング

- （ファブリックの作成で指定された範囲から）新しいオーバーレイ ネットワークと VRF を作成します。
- ファブリックのスイッチでオーバーレイ ネットワークと VRF をプロビジョニングします。
- スイッチからネットワークと VRF を展開解除します。
- DCNM でファブリックからプロビジョニングを削除します。

[制御（Control）] > [サービス（Serviecs）] メニューオプション（**[ファブリック（Fabrics）]** サブメニューの下）。

L4 ～ 7 サービス アプライアンスを接続できるサービス リーフの設定のプロビジョニング。詳細については、「*L4* ～ *L7*サービスの基本的なワークフロー」を参照してください。

この章では、単一の VXLAN BGP EVPN ファブリックの設定プロビジョニングについて主に説明します。MSD ファブリックを使用した複数のファブリックでのレイヤ 2/レイヤ 3 DCI の EVPN Multi-Site プロビジョニングについては、別の章で説明します。DCNM からオーバーレイ ネットワークおよび VRF を簡単にプロビジョニングできる方法の展開の詳細については、「ネットワークおよび VRF の作成と展開 」で説明されています。

VXLAN BGP EVPN ファブリック プロビジョニングのガイドライン

- スイッチを DCNM に正しくインポートするには、検出/インポート用に指定されたユーザーに次の権限が必要です。
  - スイッチへの SSH アクセス
  - SNMPv3 クエリを実行する権限
  - show run、show interfaces などを含む **show** コマンドを実行する権限

- スイッチ検出ユーザーには、スイッチの設定を変更する権限は必要ありません。主に読み取りアクセスに使用されます。
- 無効なコマンドが DCNM によってデバイスに展開された場合、たとえば、ファブリック設定の無効なエントリが原因で無効なキーチェーンを持つコマンドが生じた場合には、この問題を示すエラーが生成されます。このエラーは、無効なファブリックエントリを修正した後もクリアされません。エラーをクリアするには、無効なコマンドを手動でクリーンアップまたは削除する必要があります。

  コマンドの実行に関連するファブリックエラーは、失敗したのと同じコマンドが後続の展開で成功した場合にのみ、自動的にクリアされることに注意してください。
- LAN クレデンシャルは、デバイスへの書き込みアクセスを実行する必要があるすべてのユーザーに設定する必要があります。LAN ログイン情報は、デバイスごと、ユーザーごとに DCNM に設定する必要があります。ユーザーがデバイスを Easy ファブリックにインポートし、そのデバイスに LAN ログイン情報が設定されていない場合、DCNM はこのデバイスを移行モードに移動します。ユーザーがそのデバイスに適切な LAN ログイン情報を設定し、その後で [保存と展開（Save & Deploy）] を選択すると、デバイス インポート プロセスが再トリガーされます。
- **[保存と展開（Save & Deploy）]** ボタンをクリックすると、ファブリック全体のインテントの再生成と、ファブリック内のすべてのスイッチの設定コンプライアンス チェックがトリガーされます。このボタンは以下の場合に必須ですが、それらに限定されません。
  - スイッチまたはリンクが追加された、またはトポロジが変更されたとき
  - ファブリック全体で共有する必要があるファブリック設定が変更されたとき
  - スイッチが取り外された、または削除されたとき
  - 新しい vPC のペアリングまたはペアリングの解除が実行されたとき
  - デバイスのロールが変更されたとき

  [保存と展開（Save & Deploy）] をクリックすると、ファブリックの変更が評価され、ファブリック全体の構成が生成されます。生成された構成をプレビューし、ファブリック レベルで展開できます。そのため、ファブリックのサイズによっては、**[保存と展開（Save & Deploy）]** に時間がかかることがあります。

  スイッチのアイコンを右クリックして、**[構成の展開（Deploy Config）]** オプションを選択すれば、スイッチごとの構成を展開できます。このオプションは、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。
- 永続的な設定の差分は、コマンドライン**system nve infra-vlan** *int* **force**で確認できます。永続的な差分は、スイッチにフリーフォームの設定を介してこのコマンドを展開すると、発生します。スイッチは展開時に **force** キーワードを必要としますが、DCNM 内でスイッチ

から取得された実行構成では**force**キーワードは表示されません。したがって、**system nve infra-vlan** *int* **force** コマンドは常に diff として表示されます。

DCNM のインテントには次の行が含まれます：

```
system nve infra-vlan int force
```

実行設定には次の行が含まれいます：

```
system nve infra-vlan int
```

永続的な差分を修正する回避策として、最初の展開後にフリーフォームの設定を編集して **force** キーワードを削除し、 **system nve infra-vlan** *int* になるようにします。

force キーワードは最初の展開に必要ですが、展開が成功した後では削除する必要があります。**[比較（Side-by-side）]** タブ（**[設定のプレビュー（Config Preview）]** ウィンドウ）を使用して、差分を確認できます。

永続的な差分は、スイッチの消去書き込みおよびリロードの後にも表示されます。**force** キーワードを含めるように DCNM のインテントを更新し、最初の展開後に **force** キーワードを削除する必要があります。

- スイッチに、**hardware access-list tcam region arp-ether 256** コマンドが含まれている場合、このコマンドは、**double-wide** キーワードなしでは非推奨になり、次の警告が表示されます。

  警告：「double-wide」なしで arp-ether 領域を設定すると、非 vxlan パケットのドロップが発生する可能性があります。（WARNING: Configuring the arp-ether region without "double-wide" is deprecated and can result in silent non-vxlan packet drops.）arp-ether リージョンの TCAM スペースを分割する場合は、「double-wide」キーワードを使用します。

  元の **hardware access-list tcam region arp-ether 256** コマンドは DCNM のポリシーと一致しないため、この構成は**switch_freeform** ポリシーでキャプチャされます。**hardware access-list tcam region arp-ether 256 double-wide** コマンドがスイッチにプッシュされると、元の **tcam** コマンド（**double-wide** キーワードを含まないもの）は削除されます。

  hardware access-list tcam region arp-ether 256 コマンドを **switch_freeform** ポリシーから手動で削除する必要があります。それ以外の場合、設定コンプライアンスには永続的な差分が表示されます。

  スイッチでの **hardware access-list** コマンドの例を次に示します。

```
switch(config)# show run | inc arp-ether
switch(config)# hardware access-list tcam region arp-ether 256
Warning: Please save config and reload the system for the configuration to take
effect
switch(config)# show run | inc arp-ether
hardware access-list tcam region arp-ether 256
switch(config)#
switch(config)# hardware access-list tcam region arp-ether 256 double-wide
Warning: Please save config and reload the system for the configuration to take
effect
switch(config)# show run | inc arp-ether
hardware access-list tcam region arp-ether 256 double-wide
```

  元の **tcam** コマンドが上書きされていることがわかります。

新規 VXLAN BGP EVPN ファブリックの作成

この手順では、新しい VXLAN BGP EVPN ファブリックを作成する方法を示します。

この手順には、IPv4 アンダーレイの説明が含まれています。IPv6 アンダーレイについては、Easy Fabric の IPv6 アンダーレイ サポート, on page 76 を参照してください。

1. **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

   [ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。初めてログインしたときには、**[ファブリック（Fabrics）]** セクションにはまだエントリはありません。ファブリックを作成すると、**[ファブリック ビルダ（Fabric Builder）]** ウィンドウに表示されます。長方形のボックスが各ファブリックを表します。

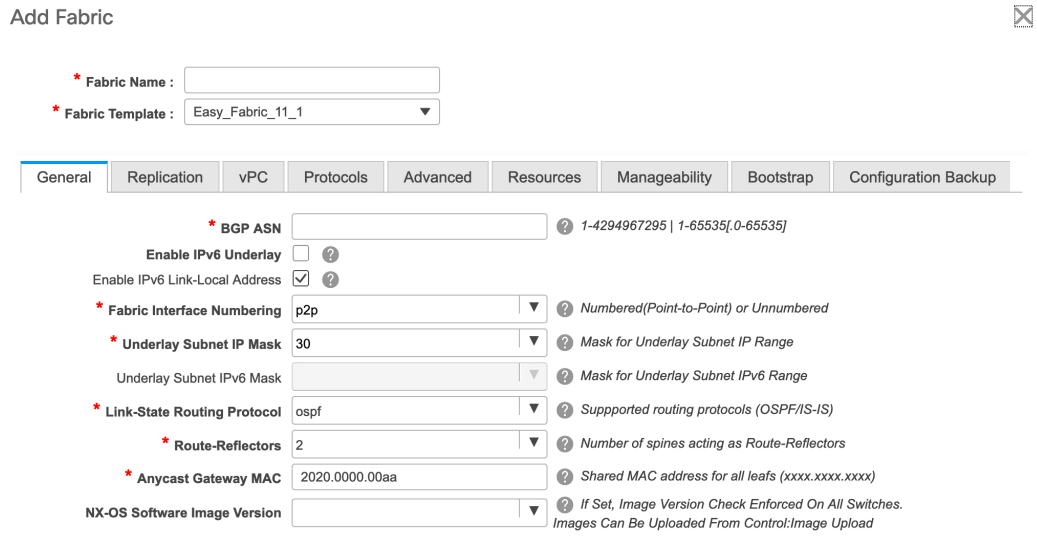
   スタンドアロンまたはメンバーファブリックには、Switch_Fabric（タイプフィールド）、AS 番号（ASN フィールド）、および複製モード（複製モード フィールド）が含まれます。

2. **[ファブリックの作成（Create Fabric）]** をクリックすると、**[ファブリックの追加（Add Fabric）]** 画面が表示されます。

   フィールドについて説明します。

   [ファブリック名（Fabric Name）]：ファブリックの名前を入力します。

   [ファブリック テンプレート（Fabric Template）]：ドロップダウンメニューから、**[Easy_Fabric_11_1]** ファブリック テンプレートを選択します。スタンドアロン ファブリックを作成するためのファブリック設定が表示されます。



画面のタブとそのフィールドについては、以降のポイントで説明します。オーバーレイおよびアンダーレイ ネットワーク パラメータは、これらのタブに含まれています。

Note MSDファブリックの潜在的なメンバーファブリックとしてスタンドアロンファブリックを作成する場合（EVPN マルチサイト テクノロジーを介して接続されるファブリックのオーバーレイ ネットワークのプロビジョニングに使用）、メンバー ファブリックの作成前に、トピック「VXLAN BGP EVPN ファブリックのマルチサイト ドメイン」を参照してください。

3. デフォルトでは **[全般（General）]** タブが表示されます。このタブのフィールドは次のとおりです。

   [BGP ASN]：ファブリックが関連付けられている BGP AS 番号を入力します。

   [IPv6 アンダーレイの有効化（Enable IPv6 Underlay）]：IPv6 アンダーレイ機能を有効にします。詳細については、Easy Fabric の IPv6 アンダーレイ サポート, on page 76を参照してください。

   [IPv6 リンクローカル アドレスの有効化（Enable IPv6 Link-Local Address）]：IPv6 リンクローカル アドレスを有効にします。

   [ファブリック インターフェイスの番号付け（Fabric Interface Numbering）]：ポイントツーポイント（[p2p]）またはアンナンバードネットワークのどちらを使用するかを指定します。

   [アンダーレイ サブネット IP マスク（Underlay Subnet IP Mask）]：ファブリック インターフェイスの IP アドレスのサブネットマスクを指定します。

   [アンダーレイ ルーティング プロトコル（Underlay Routing Protocol）]：ファブリック、OSPF、または IS-IS で使用される IGP。

   [ルートリフレクタ（RR）（Route-Reflectors（RRs））]：BGP トラフィックを転送するためのルート リフレクタとして使用されるスパイン スイッチの数。ドロップダウン リスト ボックスで [なし（None）] を選択します。デフォルト値は 2 です。

   スパイン デバイスを RR として展開するには、DCNM はスパイン デバイスをシリアル番号に基づいてソートし、2つまたは4つのスパインデバイスをRRとして指定します。スパイン デバイスを追加しても、既存の RR 設定は変更されません。

   カウントの増加：ルート リフレクタを任意の時点で 2 から 4 に増やすことができます。設定は、RR として指定された他の 2 つのスパイン デバイスで自動的に生成されます。

   カウントの削減：4 つのルート リフレクタを 2 つに減らす場合は、不要なルート リフレクタ デバイスをファブリックから削除します。カウントを 4 から 2 に減らすには、次の手順に従います。

   a. ドロップダウンボックスの値を 2 に変更します。

   b. ルート リフレクタとして指定するスパイン スイッチを特定します。

      ルート リフレクタの場合、**[rr_state]** ポリシーのインスタンスがスパイン スイッチに適用されます。ポリシーがスイッチに適用されているかどうかを確認するには、スイッチを右クリックし、[ポリシーの表示/編集（View/edit policies）] を選択しま

す。[ポリシーの表示/編集（View/Edit Policies）] 画面の [テンプレート（Template）] フィールドで [rr_state] を検索します。画面に表示されます。

c. ファブリックから不要なスパインデバイスを削除します（スパイン スイッチアイコンを右クリックし、[検出（Discovery）] > [ファブリックから削除（Remove from fabric）] の順に選択します）。

既存の RR デバイスを削除すると、次に使用可能なスパイン スイッチが交換 RR として選択されます。

d. ファブリック トポロジ ウィンドウで **[保存と展開（Save & Deploy）]** をクリックします。

最初の [保存と展開（Save & Deploy）] 操作を実行する前に、RR と RP を事前に選択できます。詳細については、「ルートリフレクタおよびランデブーポイントとしてのスイッチの事前選択」を参照してください。

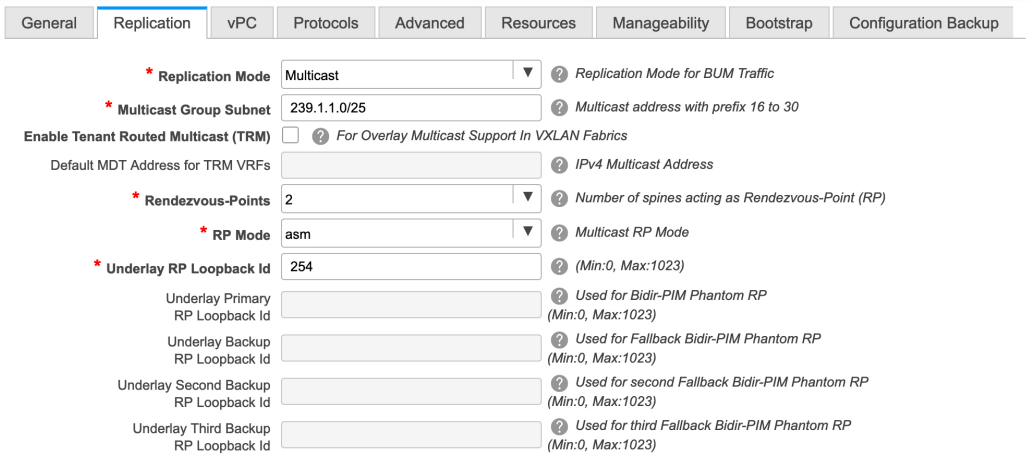
[エニーキャスト ゲートウェイ MAC（Anycast Gateway MAC）]：エニーキャスト ゲートウェイ MAC アドレスを指定します。

[NX-OSソフトウェア イメージ バージョン（NX-OS Software Image Version）]：リストからイメージを選択します。

イメージアップロードオプションを使用してCisco NX-OS ソフトウェアイメージをアップロードすると、アップロードされたイメージがこのフィールドにリストされます。イメージを選択してファブリック設定を保存すると、システムはファブリック内のすべてのスイッチに選択したバージョンがあることを確認します。一部のデバイスでイメージが実行されない場合、指定されたイメージへのインサービス ソフトウェア アップグレード（ISSU）を実行するように警告するプロンプトが表示されます。警告には、[解決（Resolve）] ボタンも付いています。これにより、[ファブリック設定（Fabric Settings）] で指定された指定の NX-OS イメージへのデバイス アップグレード/ダウングレードに対して不一致のスイッチが自動的に選択されたイメージ管理画面が表示されます。すべてのデバイスが指定されたイメージを実行するまで、展開プロセスは完了しません。

ファブリック スイッチに複数のタイプのソフトウェア イメージを展開する場合は、イメージを指定しないでください。イメージが指定されている場合は削除します。

4. **[レプリケーション（Replication）]** タブをクリックします。ほとんどのフィールドは自動生成されます。必要に応じてフィールドを更新できます。



[レプリケーション モード（Replication Mode）]：BUM（ブロードキャスト、不明なユニキャスト、マルチキャスト）トラフィックのファブリックで使用されるレプリケーションのモードです。選択肢は[レプリケーションの入力（Ingress Replication）]または[マルチキャスト（Multicast）]です。[レプリケーションの入力（Ingress replication）]を選択すると、マルチキャスト関連のフィールドは無効になります。

ファブリックのオーバーレイ プロファイルが存在しない場合は、ファブリック設定をあるモードから別のモードに変更できます。

[マルチキャスト グループ サブネット（Multicast Group Subnet）]：マルチキャスト通信に使用される IP アドレス プレフィックスです。オーバーレイ ネットワークごとに、このグループから一意の IP アドレスが割り当てられます。

DCNM 11.1(1) リリースでは、現在のモードのポリシー テンプレート インスタンスが作成されている場合、レプリケーション モードの変更は許可されません。たとえば、マルチキャスト関連のポリシーを作成して展開する場合、モードを入力に変更することはできません。

[テナント ルーテッド マルチキャスト（TRM）の有効化（Enable Tenant Routed Multicast（TRM））]：VXLAN BGP EVPN ファブリックで EVPN/MVPN を介してオーバーレイ マルチキャスト トラフィックをサポートできるようにするテナント ルーテッド マルチキャスト（TRM）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。

[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]：テナント ルーテッド マルチキャスト トラフィックのマルチキャスト アドレスが入力されます。デフォルトでは、このアドレスは [マルチキャスト グループ サブネット] フィールドで指定された IP プレフィックスから取得されます。いずれかのフィールドをアップデートする場合、**[マルチキャスト グループ サブネット（Multicast Group Subnet）]** で指定した IP プレフィックスから選択された TRM アドレスであることを確認してください。

詳細については、テナント ルーテッド マルチキャストの概要, on page 176を参照してください。

[ランデブーポイント（Rendezvous-Points）]：ランデブーポイントとして機能するスパイン スイッチの数を入力します。

[RPモード（RP mode）]：ASM（エニーソース マルチキャスト（ASM）の場合）または BiDir（双方向 PIM（BIDIR-PIM）の場合）の 2 つのサポート対象のマルチキャスト モードから選択します。

[ASM] を選択すると、[BiDir] 関連のフィールドは有効になりません。[BiDir] を選択すると、[BiDir] 関連フィールドが有効になります。

Note BIDIR-PIM は、Cisco のクラウド スケール ファミリ プラットフォーム 9300-EX および 9300-FX/FX2、およびソフトウェア リリース 9.2(1) 以降でサポートされています。

ファブリック オーバーレイの新しい VRF を作成すると、このアドレスが [アドバンス（Advanced）] タブの [アンダーレイ マルチキャスト アドレス（Underlay Multicast Address）] フィールドに入力されます。

[アンダーレイ RP ループバック ID（Underlay RP Loopback ID）]：ファブリック アンダーレイでのマルチキャスト プロトコル ピアリングの目的で、ランデブーポイント（RP）に使用されるループバック ID です。

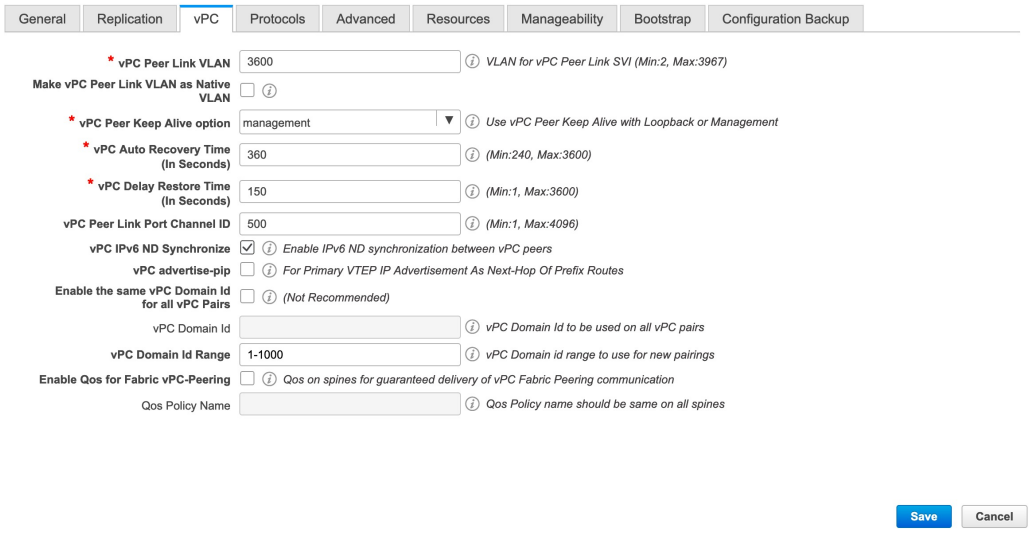
次の 2 つのフィールドは、レプリケーションのマルチキャスト モードとして [BIDIR-PIM] を選択した場合に有効になります。

[アンダーレイ プライマリ RP ループバック ID（Underlay Primary RP Loopback ID）]：ファブリック アンダーレイでマルチキャスト プロトコル ピアリングのためにファントム RP に使用されるプライマリ ループバック ID です。

[アンダーレイ バックアップ RP ループバック ID（Underlay Backup RP Loopback ID）]：ファブリック アンダーレイでマルチキャスト プロトコル ピアリングを目的として、ファントム RP に使用されるセカンダリ ループバック ID です。

[アンダーレイ セカンド バックアップ RP ループバック ID（Underlay Second Backup RP Loopback Id）] および [アンダーレイ サード バックアップ RP ループバック ID（Underlay Third Backup RP Loopback Id）]：2 番目と 3 番目のフォールバック Bidir-PIM ファントム RP に使用されます。

5. **[vPC]** タブをクリックします。ほとんどのフィールドは自動生成されます。必要に応じてフィールドを更新できます。



[vPC ピア リンク VLAN（vPC Peer Link VLAN）]：vPC ピア リンク SVI に使用される VLAN です。

[vPC ピア リンク VLAN をネイティブ VLAN とする（Make vPC Peer Link VLAN as Native VLAN）]：vPC ピア リンク VLAN をネイティブ VLAN として有効にします。

[vPC ピア キープアライブ オプション（vPC Peer Keep Alive option）]：管理またはループバック オプションを選択します。管理ポートおよび管理 VRF に割り当てられた IP アドレスを使用する場合は、[管理（management）] を選択します。ループバック インターフェイス（および非管理 VRF）に割り当てられた IP アドレスを使用する場合は、ループバックを選択します。

IPv6 アドレスを使用する場合は、ループバック ID を使用する必要があります。

[vPC 自動回復時間（vPC Auto Recovery Time）]：vPC 自動回復タイムアウト時間を秒単位で指定します。

[vPC 遅延復元時間（vPC Delay Restore Time）]：vPC 遅延復元期間を秒単位で指定します。

[vPC ピア リンク ポートチャネル ID（vPC Peer Link Port Channel ID）：vPC ピア リンクのポートチャネル ID を指定します。デフォルトでは、このフィールドの値は 500 です。

[vPC IPv6 ND 同期（vPC IPv6 ND Synchronize）]：vPC スイッチ間の IPv6 ネイバー探索同期を有効にします。デフォルトでチェックボックスはオンになっています。機能を無効にするにはチェックボックスをクリアします。

[vPC advertise-pip]：アドバタイズ PIP 機能を有効にします。

特定の vPC でアドバタイズ PIP 機能をイネーブルにすることもできます。詳細については、vPC で PIP をアドバタイズする, on page 228を参照してください。

[すべての vPC ペアに同じ vPC ドメイン ID を有効にする（Enable the same vPC Domain Id for all vPC Pairs）]：すべての vPC ペアに同じ vPC ドメイン ID を有効にします。この

フィールドを選択すると、[vPC ドメイン ID（vPC Domain Id）] フィールドが編集可能になります。

[vPC ドメイン ID（vPC Domain Id）]：すべての vPC ペアで使用される vPC ドメイン ID を指定します。

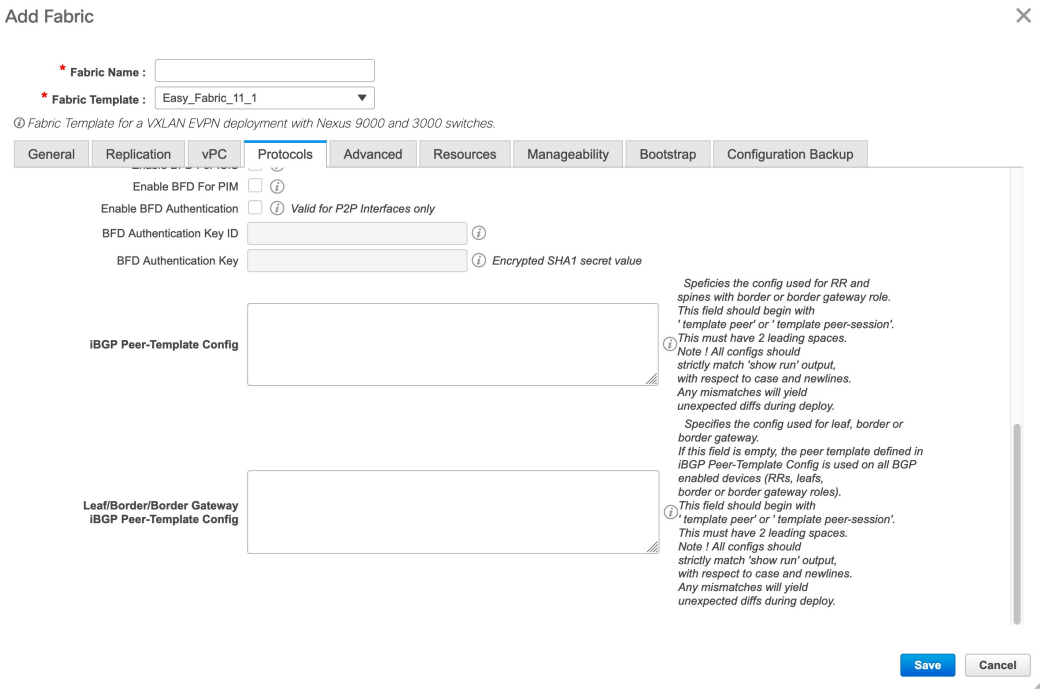
[vPC ドメイン ID の範囲（vPC Domain Id Range）]：新しいペアリングに使用する vPC ドメイン ID の範囲を指定します。

[ファブリック vPC ピアリングの QoS を有効にする（Enable QoS for Fabric vPC-Peering）]：スパインの QoS を有効にして、vPC ファブリック ピアリング通信の配信を保証します。詳細については、ファブリック vPC ピアリングの QoS, on page 219を参照してください。

Note ファブリック設定の vPC ファブリック ピアリングとキューイング ポリシーの QoS オプションは相互に排他的です。

[QoS ポリシー名（QoS Policy Name）]：すべてのファブリック vPC ピアリング スパインで同じにする必要がある QoS ポリシー名を指定します。デフォルト名は [spine_qos_for_fabric_vpc_peering] です。

6. **[プロトコル（Protocols）]** タブをクリックします。ほとんどのフィールドは自動生成されます。必要に応じてフィールドを更新できます。



[アンダーレイ ルーティング ループバック ID（Underlay Routing Loopback Id）]：通常は loopback0 がファブリック アンダーレイ IGP ピアリングに使用されるため、ループバック インターフェイス ID は 0 に設定されます。

[アンダーレイ VTEP ループバック ID（Underlay VTEP Loopback Id）]：loopback1 は VTEP ピアリングの目的で使用されるため、ループバック インターフェイス ID は 1 に設定されます。

[アンダーレイ ルーティング プロトコル タグ（Underlay Routing Protocol Tag）]：ネットワークのタイプを定義するタグです。

[OSPF エリア ID（OSPF Area ID）]：OSPF エリア ID です（OSPF がファブリック内で IGP として使用されている場合）。

Note OSPF または IS-IS 認証フィールドは、[全般（**General**）] タブの**[アンダーレイ ルーティング プロトコル（Underlay Routing Protocol）]** フィールドでの選択に基づいて有効になります。

[OSPF 認証の有効化（Enable OSPF Authentication）]：OSPF 認証を有効にするには、このチェックボックスをオンにします。無効にするにはチェックボックスをオフにします。このフィールドを有効にすると、OSPF 認証キー ID フィールドおよび OSPF 認証キー フィールドが有効になります。

[OSPF 認証キー ID（OSPF Authentication Key ID）]：キー ID が入力されます。

[OSPF 認証キー（OSPF Authentication Key）]：OSPF 認証キーは、スイッチからの 3DES キーである必要があります。

Note プレーン テキスト パスワードはサポートされていません。スイッチにログインし、暗号化キーを取得して、このフィールドに入力します。詳細については、「認証キーの取得」の項を参照してください。

[IS-IS レベル（IS-IS Level）]：このドロップダウンリストから IS-IS レベルを選択します。

[IS-IS 認証の有効化（Enable IS-IS Authentication）]：IS-IS 認証を有効にするにはチェックボックスをオンにします。無効にするにはチェックボックスをオフにします。このフィールドを有効にすると、IS-IS 認証フィールドが有効になります。

[IS-IS 認証キーチェーン名（IS-IS Authentication Keychain Name）]：CiscoisisAuth などのキーチェーン名を入力します。

[IS-IS 認証キー ID（IS-IS Authentication Key ID）：キー ID が入力されます。

[IS-IS 認証キー（IS-IS Authentication Key）]：Cisco Type 7 暗号化キーを入力します。

Note プレーン テキスト パスワードはサポートされていません。スイッチにログインし、暗号化キーを取得して、このフィールドに入力します。詳細については、「認証キーの取得」の項を参照してください。

[BGP 認証の有効化（Enable BGP Authentication）]：BGP 認証を有効にするにはチェックボックスをオンにします。無効にするにはチェックボックスをオフにします。このフィールドを有効にすると、[BGP 認証キー暗号化タイプ（BGP Authentication Key Encryption Type）] および [BGP 認証キー（BGP Authentication Key）] フィールドが有効になります。

Note このフィールドを使用して BGP 認証を有効にする場合は、[iBGP Peer-Template Config] フィールドを空白のままにして、設定が重複しないようにします。

[BGP 認証キー暗号化タイプ（BGP Authentication Key Encryption Type）]：3DES 暗号化タイプの場合は 3、Cisco 暗号化タイプの場合は 7 を選択します。

[BGP 認証キー（BGP Authentication Key）]：暗号化タイプに基づいて暗号化キーを入力します。

Note プレイン テキスト パスワードはサポートされていません。スイッチにログインし、暗号化されたキーを取得して、[BGP 認証キー（BGP Authentication Key）] フィールドに入力します。詳細については、「認証キーの取得」の項を参照してください。

[PIM hello 認証の有効化（Enable PIM Hello Authentication）]：PIM hello認証を有効にします。

[PIM Hello 認証キー（PIM Hello Authentication Key）]：PIM hello 認証キーを指定します。

[BFD の有効化（Enable BFD）]：ファブリック内のすべてのスイッチで機能 [bfd] 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。この機能は、IPv4 アンダーレイでのみ有効で、範囲はファブリック内にあります。

Cisco DCNM リリース 11.3(1) 以降、ファブリック内の BFD はネイティブにサポートされます。ファブリック設定では、BFD機能はデフォルトで無効になっています。有効にすると、デフォルト設定のアンダーレイ プロトコルに対して BFD が有効になります。カスタムの必須BFD構成は、スイッチごとの自由形式またはインターフェイスごとの自由形式ポリシーを使用して展開する必要があります。

[BFD の有効化（Enable BFD）] チェックボックスをオンにすると、次の構成がプッシュされます。

```
feature bfd
```

Note BFD が有効になっている DCNM リリース 11.2(1) から DCNM リリース 11.3(1) にアップグレードすると、次の設定がすべての P2P ファブリック インターフェイスにプッシュされます。

```
no ip redirects
no ipv6 redirects
```

BFD機能の互換性については、それぞれのプラットフォームのマニュアルを参照してください。サポートされているソフトウェア画像については、「*Cisco DCNM* の互換性マトリクス」を参照してください。

[iBGP 向け BFD の有効化（Enable BFD for iBGP）]：iBGP ネイバーの BFD 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。このオプションは、デフォルトで無効です。

[OSPF 向け BFD の有効化（Enable BFD for OSPF）]：このチェックボックスをオンにすると、OSPF アンダーレイ インスタンスの BFD が有効になります。このオプションはデフォルトで無効になっており、リンクステートプロトコルがISISの場合はグレー表示されます。

[ISIS 向け BFD の有効化（Enable BFD for ISIS）]：このチェックボックスをオンにして、ISIS アンダーレイ インスタンスの BFD を有効にします。このオプションはデフォルトで無効になっており、リンク ステート プロトコルが OSPF の場合はグレー表示されます。

[PIM 向け BFD の有効化（Enable BFD for PIM）]：PIM の BFD 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。このオプションはデフォルトで無効になっており、レプリケーション モードが [入力（Ingress）] の場合はグレー表示されます。

BFD グローバル ポリシーの例を次に示します。

```
router ospf <ospf tag>
   bfd

router isis <isis tag>
  address-family ipv4 unicast
    bfd

ip pim bfd

router bgp <bgp asn>
  neighbor <neighbor ip>
    bfd
```

[BGP 認証の有効化（Enable BGP Authentication）]：BGP 認証を有効にするにはチェックボックスをオンにします。このフィールドを有効にすると、[BFD 認証キー ID（BFD Authentication Key ID）] フィールドと [BFD 認証キー（BFD Authentication Key）] フィールドが編集可能になります。

Note [全般（General）] タブの [ファブリック インターフェイスの番号付け（Fabric Interface Numbering）] フィールドが [番号付けなし（unnumbered）] に設定されている場合、BFD 認証はサポートされません。BFD 認証フィールドは自動的にグレー表示されます。BFD 認証は、P2P インターフェイスに対してのみ有効です。

[BFD 認証キー ID（BFD Authentication Key ID）]：インターフェイス認証の BFD 認証キー ID を指定します。デフォルト値は 100 です。

[BFD 認証キー（BFD Authentication Key）]：BFD 認証キーを指定します。

BFD 認証パラメータを取得する方法については、暗号化された BFD 認証キーの取得, on page 242 を参照してください。

[iBGP ピアテンプレート構成（iBGP Peer-Template Config）]：リーフ スイッチに iBGP ピア テンプレート構成を追加して、リーフ スイッチとルート リフレクタの間に iBGP セッションを確立します。

BGP テンプレートを使用する場合は、テンプレート内に認証構成を追加し、[BGP 認証の有効化（Enable BGP Authentication）] チェックボックスをオフにして、構成が重複しないようにします。

構成例では、パスワード 3 の後に 3DES パスワードが表示されます。

```
router bgp 65000
    password 3 sd8478fswerdfw3434fsw4f4w34sdsd8478fswerdfw3434fsw4f4w
```

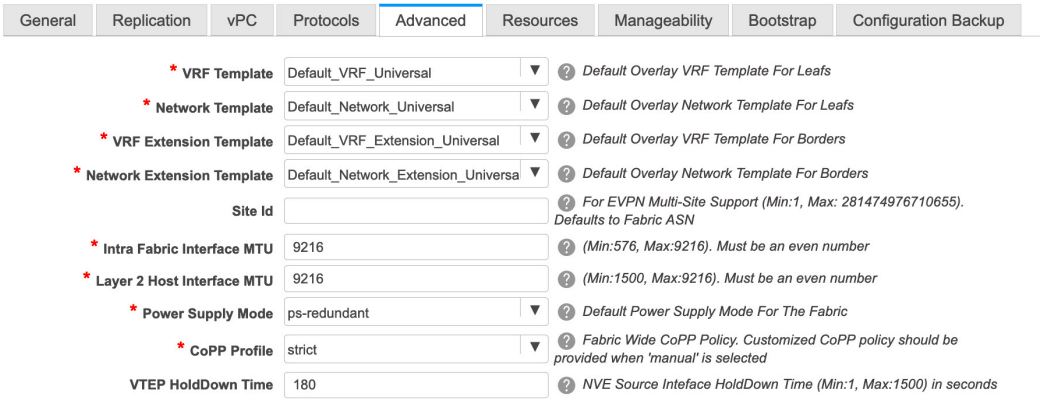
Cisco DCNM リリース 11.3(1) までは、リーフまたはボーダー ロール デバイスの iBGP 定義の iBGP ピア テンプレートと BGP RR は同じでした。DCNM リリース 11.4(1) 以降、次のフィールドを使用してさまざまな構成を指定できます。

- [iBGP ピアテンプレート構成（iBGP Peer-Template Config）]：境界ロールを持つ RR およびスパインに使用される構成を指定します。

- [リーフ/境界/境界ゲートウェイ iBGP ピアテンプレート構成（Leaf/Border/Border Gateway iBGP Peer-Template Config）]：リーフ、境界、または境界ゲートウェイに使用される構成を指定します。このフィールドが空の場合、[iBGP ピアテンプレート構成（iBGP Peer-Template Config）] で定義されたピア テンプレートがすべての BGP 対応デバイス（RR、リーフ、境界、または境界ゲートウェイ ロール）で使用されます。

ブラウンフィールド移行では、スパインとリーフが異なるピアテンプレート名を使用する場合、[iBGP ピアテンプレート構成（iBGP Peer-Template Config）] フィールドと [リーフ/境界/境界ゲートウェイ iBGP ピアテンプレート構成（Leaf/Border/Border Gateway iBGP Peer-Template Config）] フィールドの両方をスイッチ構成に従って設定する必要があります。スパインとリーフが同じピア テンプレート名とコンテンツを使用する場合（「route-reflector-client」CLIを除く）、ファブリック設定の [iBGP ピアテンプレート構成（iBGP Peer-Template Config）] フィールドのみを設定する必要があります。iBGP ピアテンプレートのファブリック設定が既存のスイッチ構成と一致しない場合、エラーメッセージが生成され、移行は続行されません。

7. [Advanced] タブをクリックします。ほとんどのフィールドは自動生成されます。必要に応じてフィールドを更新できます。



VRFテンプレートおよびVRF拡張テンプレート：VRFを作成するためのVRFテンプレートと、他のファブリックへのVRF拡張を有効にするためのVRF拡張テンプレートを指定します。

[ネットワーク テンプレート（Network Template）] と [ネットワーク拡張テンプレート（Network Extension Template）]：ネットワークを作成するためのネットワーク テンプレートと、他のファブリックにネットワークを拡張するためのネットワーク拡張テンプレートを指定します。

[サイト ID（Site ID）]：このファブリックを MSD 内で移動する場合の ID です。メンバー ファブリックが MSD の一部であるためには、サイト ID が必須です。MSD の各メンバー ファブリックには、一意のサイト ID があります。

[イントラ ファブリック インターフェイス MTU（Intra Fabric Interface MTU）]：ファブリック内インターフェイスの MTU を指定します。この値は偶数にする必要があります。

[レイヤ 2 ホスト インターフェイス MTU（Layer 2 Host Interface MTU）]：レイヤ 2 ホスト インターフェイスの MTU を指定します。この値は偶数にする必要があります。

電源モード（Power Supply Mode）：適切な電源モードを選択します。

[CoPP プロファイル（CoPP Profile）]：ファブリックの適切なコントロールプレーン ポリシング（CoPP）プロファイルポリシーを選択します。デフォルトでは、strict オプションが入力されます。

[VTEP HoldDown 時間（VTEP HoldDown Time）]：NVE 送信元インターフェイスのホールドダウン時間を指定します。

[ブラウンフィールド オーバーレイ ネットワーク名の形式（Brownfield Overlay Network Name Format）]：ブラウンフィールドのインポートまたは移行時にオーバーレイ ネットワーク名を作成するために使用する形式を入力します。ネットワーク名は、アンダースコア（_）およびハイフン（-）を除く特殊文字または空のスペースが含まれないようにしてください。ブラウンフィールドの移行が開始されたら、ネットワーク名を変更しないでください。ネットワーク名の命名規則については、「スタンドアロン ファブリックのネットワークの作成」の項を参照してください。構文は**[<string> | $$VLAN_ID$$] $$VNI$$ [<string>| $$VLAN_ID$$]**です。デフォルト値は **[Auto_Net_VNI$$VNI$$_VLAN$$VLAN_ID$$]** です。ネットワークを作成すると、指定した構文に従って名前が生成されます。次の表で構文内の変数について説明します。

変数	説明
$$VNI$$	スイッチ構成で検出されたネットワーク VNI ID を指定します。これは、一意のネットワーク名を作成するために必要な必須キーワードです。
$$VLAN_ID$$	ネットワークに関連付けられた VLAN ID を指定します。 VLAN ID はスイッチに固有であるため、DCNM はネットワークが検出されたスイッチの 1 つから VLAN ID をランダムに選択し、名前に使用します。 VLAN ID が VNI のファブリック全体で一貫していない限り、これを使用しないことを推奨します。
<string>	この変数はオプションであり、ネットワーク名のガイドラインを満たす任意の数の英数字を入力できます。

オーバーレイ ネットワーク名の例：Site_VNI12345_VLAN1234

Note グリーンフィールド展開では、このフィールドを無視します。ブラウンフィールド オーバーレイ ネットワーク名の形式は、次のブラウンフィールド インポートに適用されます。

- CLI ベースのオーバーレイ
- 構成プロファイルが Cisco DCNM リリースで作成された構成プロファイルベースのオーバーレイ

  10.4(2) で作成された構成プロファイルベースのオーバーレイ

[ブートストラップ スイッチの CDP の有効化（Enable CDP for Bootstrapped Switch）]：ブートストラップ スイッチの管理（mgmt0）インターフェイスで CDP を有効にします。デフォルトでは、ブートストラップ スイッチの場合、mgmt0 インターフェイスで CDP は無効にされています。

[VXLAN OAM の有効化（Enable VXLAN OAM）]：ファブリック内のデバイスの VXLAM OAM機能を有効にします。この設定はデフォルトでイネーブルになっています。VXLAN OAM 機能を無効にするにはチェックボックスをクリアします。

ファブリック内の特定のスイッチで VXLAN OAM 機能を有効にし、他のスイッチで無効にする場合は、自由形式構成を使用して、ファブリック設定で OAM を有効にし、OAM を無効にすることができます。

Note Cisco DCNM の VXLAN OAM 機能は、単一のファブリックまたはサイトでのみサポートされます。

[テナント DHCP の有効化（Enable Tenant DHCP）]：機能 dhcp および関連する構成をファブリック内のすべてのスイッチでグローバルに有効にするには、このチェックボックスをオンにします。これは、テナント VRF の一部であるオーバーレイ ネットワークの DHCP をサポートするための前提条件です。

Note オーバーレイ プロファイルで DHCP 関連のパラメータを有効にする前に、**[テナント DHCP の有効化（Enable Tenant DHCP）]** が有効であることを確認します。

[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、デフォルトでオンになっています。

[ポートの HTTP で NX-API を有効化する（Enable on NX-API on HTTP）]：HTTP 上の NX-API の有効化を指定します。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は、デフォルトでオンになっています。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（L4ーL7 サービス）、VXLAN OAM など、NX-API

を使用し、Cisco DCNM がサポートするアプリケーションは、HTTP ではなく HTTPS の使用を開始します。

Note [NX-API の有効化（Enable NX-API）] チェックボックスと [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。

[ポリシーベース ルーティング（PBR）の有効化（Enable Policy-Based Routing（PBR））]：指定したポリシーに基づいてパケットのルーティングを有効にするにはこのチェックボックスを選択します。Cisco NX-OS リリース 7.0(3)I7(1) 以降では、この機能は Nexus 9000 クラウド スケール（Tahoe）ASIC を搭載した Cisco Nexus 9000 シリーズ スイッチで動作します。この機能は、レイヤ 4 ～ レイヤ 7 サービス ワークフローとともに使用されます。レイヤ 4 ～ レイヤ 7 サービスの詳細については、「レイヤ 4 ～ レイヤ 7 サービス」の章を参照してください。

[厳密な構成コンプライアンスの有効化（Enable Strict Config Compliance）]：このチェックボックスをオンにして、厳密な構成コンプライアンス機能を有効にします。デフォルトで、この機能は無効になっています。詳細については、「厳密な構成コンプライアンス」を参照してください。

[AAA IP 認証の有効化（Enable AAA IP Authorization）]：IP 認証がリモート認証サーバーで有効になっている場合に、AAA IP 認証を有効にします。これは、スイッチにアクセスできる IP アドレスを顧客が厳密に制御できるシナリオで DCNM をサポートするために必要です。

[NDFC をトラップ ホストとして有効化（Enable NDFC as Trap Host）]：DCNM を SNMP トラップの接続先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。通常、ネイティブ HA DCNM の展開では、スイッチの eth1 VIP IP アドレスが SNMP トラップ接続先として構成されます。デフォルトでは、このチェックボックスは有効になっています。

[グリーンフィールド クリーンアップ オプション（Greenfield Cleanup Option）]：Preserve-Config=No で DCNM にインポートされたスイッチのスイッチ クリーンアップ オプションを有効にします。このオプションは、通常、スイッチのクリーンアップ時間を短縮するために、Cisco Nexus 9000v スイッチを使用するファブリック環境でのみ推奨されます。グリーンフィールド導入の推奨オプションは、ブートストラップを使用するか、または再起動によるクリーンアップです。つまり、このオプションはオフにする必要があります。

[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オンにすると、PTP がグローバルに有効になり、コアに面するインターフェイスで有効になります。また、**[PTP 送信元ループバック ID（PTP Source Loopback Id）]** および **[PTP ドメイン ID（PTP Domain Id）]** フィールドが編集可能になります。詳細については、Easy ファブリック向け高精度時間プロトコル, on page 61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、DCNM から BGP ループバックまたは作成元の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 送信元 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ます。

[PTP ドメイン ID（PTP Domain 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。

[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、「VXLAN BGP EVPN ファブリックでの境界プロビジョニングの使用例：MPLS SR および LDP ハンドオフ」の章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。

[TCAM 割り当ての有効化（Enable TCAM Allocation）]：TCAM コマンドは、有効にすると VXLAN および vPC ファブリック ピアリングに対して自動的に生成されます。

[デフォルト キューイング ポリシーの有効化（Enable Default Queuing Policies）]：このファブリック内のすべてのスイッチにQoSポリシーを適用するには、このチェックボックスをオンにします。すべてのスイッチに適用したQoSポリシーを削除するには、このチェックボックスをオフにし、すべての設定を更新してポリシーへの参照を削除し、保存して展開します。Cisco DCNM リリース 11.3(1) 以降、さまざまな Cisco Nexus 9000 シリーズスイッチに使用できる定義済みのQoS設定が含まれています。このチェックボックスをオンにすると、適切な QoS 設定がファブリック内のスイッチにプッシュされます。システム キューイングは、設定がスイッチに展開されると更新されます。インターフェイスごと自由形式ブロックに必要な設定を追加することにより、必要に応じて、定義されたキューイング ポリシーを使用してインターフェイス マーキングを実行できます。

Cisco DCNM リリース 11.4(1) 以降、ポリシー テンプレートの QoS 5 の DSCP マッピングが 40 から 46 に変更されました。11.4(1) にアップグレードされた DCNM 11.3(1) 展開の場合、展開する必要がある差分が表示されます。

テンプレート エディタでポリシー ファイルを開いて、実際のキューイング ポリシーを確認します。Cisco DCNM Web UI から、**[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択します。ポリシー ファイル名でキューイング ポリシーを検索します（例：[queuing_policy_default_8q_cloudscale]）。ファイルを選択し、**[テンプレートの変更/表示（Modify/View template）]** アイコンをクリックしてポリシーを編集します。

プラットフォーム特有の詳細については、『*Cisco Nexus 9000 Series NX-OS Quality of Service* コンフィグレーション ガイド』を参照してください。

[N9K クラウド スケール プラットフォームのキューイング ポリシー（N9K Cloud Scale Platform Queuing Policy）]：ファブリック内の EX、FX、および FX2 で終わるすべての Cisco Nexus 9200 シリーズスイッチおよび Cisco Nexus 9000 シリーズスイッチに適用するキューイング ポリシーをドロップダウン リストから選択します。有効な値は [queuing_policy_default_4q_cloudscale] および [queuing_policy_default_8q_cloudscale] です。FEX には [queuing_policy_default_4q_cloudscale] ポリシーを使用します。FEX がオフラインの場合にのみ、[queuing_policy_default_4q_cloudscale] ポリシーから [queuing_policy_default_8q_cloudscale] ポリシーに変更できます。

[N9K R シリーズ プラットフォーム キューイング ポリシー（N9K R-Series Platform Queuing Policy）]：ドロップダウンリストから、ファブリック内の R で終わるすべての Cisco Nexus スイッチに適用するキューイング ポリシーを選択します。有効な値は [queuing_policy_default_r_series] です。

[その他の N9K プラットフォーム キューイング ポリシー（Other N9K Platform Queuing Policy）]：ドロップダウンリストからキューイングポリシーを選択し、ファブリック内にある、上記 2 つのオプションで説明したスイッチ以外の他のすべてのスイッチに適用します。有効な値は [queuing_policy_default_other] です。

[MACsec の有効化（Enable MACsec）]：ファブリックの MACsec を有効にします。詳細については、Easy ファブリックおよび eBGP ファブリックでの MACsec サポート, on page 173を参照してください。

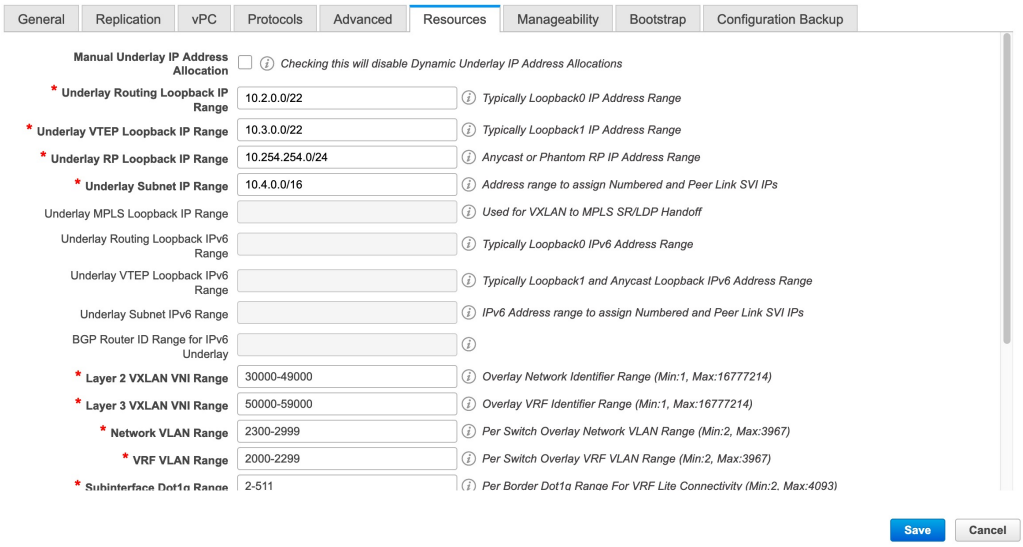
[自由形式の CLI（Freeform CLIs）]：ファブリック レベルの自由形式の CLI は、ファブリックの作成または編集中に追加できます。ファブリック全体のスイッチに適用できます。インデントなしで、実行コンフィギュレーションに表示されている設定を追加する必要があります。VLAN、SVI、インターフェイス構成などのスイッチ レベルの自由形式の構成は、スイッチでのみ追加する必要があります。詳細については、「ファブリック スイッチでのフリーフォーム設定の有効化」を参照してください。

[リーフの自由形式の構成（Leaf Freeform Config）]：リーフ、ボーダー、およびボーダーゲートウェイのロールを持つスイッチに追加する CLI です。

[スパインの自由形式の設定（Spine Freeform Config）]：スパイン、ボーダー スパイン、ボーダーゲートウェイ スパイン、および スーパー スパインのロールを持つスイッチに追加する必要がある CLI を追加します。

[ファブリック内リンクの追加設定（Intra-fabric Links Additional Config）]：ファブリック内リンクに追加する CLI を追加します。

8. [リソース（Resources）] タブをクリックします。



[手動アンダーレイ IP アドレスの割り当て（Manual Underlay IP Address Allocation）]：VXLAN ファブリック管理を移行する場合は、このチェックボックスをオンにしないでください。

- デフォルトでは、DCNM は定義されたプールから動的にアンダーレイ IP アドレス リソース（ループバック、ファブリック インターフェイスなど）を割り当てます。このチェックボックスをオンにすると、割り当て方式が静的に切り替わり、動的 IP アドレス範囲フィールドの一部が無効になります。
- 静的割り当ての場合、REST API を使用してアンダーレイ IP アドレス リソースをリソース マネージャ（RM）に入力する必要があります。

  詳細については、『Cisco REST API 参照ガイド、リリース 11.2(2)』を参照してください。スイッチをファブリックに追加した後、REST APIを呼び出してから [保存して展開（Save & Deploy）] オプションを使用する必要があります。
- マルチキャスト レプリケーションに BIDIR-PIM 機能が選択されている場合、[アンダーレイ RP ループバック IP 範囲（Underlay RP Loopback IP Range）] フィールドは有効のままになります。
- 静的割り当てから動的割り当てに変更しても、現在の IP リソースの使用情況は維持されます。それ以後の IP アドレス割り当て要求のみが動的プールから取得されます。

[アンダーレイ ルーティング ループバック IP 範囲（Underlay Routing Loopback IP Range）]：プロトコル ピアリングのループバック IP アドレスを指定します。

[アンダーレイ VTEP ループバック IP 範囲（Underlay VTEP Loopback IP Range）]：VTEP のループバック IP アドレスを指定します。

[アンダーレイ RP ループバック IP 範囲（Underlay RP Loopback IP Range）]：エニーキャストまたはファントム RP の IP アドレス範囲を指定します。

[アンダーレイ サブネット IP 範囲（Underlay Subnet IP Range）]：インターフェイス間のアンダーレイ P2P ルーティング トラフィックの IP アドレスです。

[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 ループバック IP アドレス範囲を指定します。

Easy A の境界と Easy B の間の eBGP では、アンダーレイ ルーティング ループバックとアンダーレイ MPLS ループバック IP 範囲は一意の範囲である必要があります。他のファブリックの IP 範囲と重複しないようにしてください。重複すると、VPNv4 ピアリングが起動しません。

[レイヤ 2 VXLAN VNI 範囲（Layer 2 VXLAN VNI Range）] および [レイヤ 3 VXLAN VNI 範囲（Layer 3 VXLAN VNI Range）]：ファブリックの VXLAN VNI ID を指定します。

[ネットワーク VLAN 範囲（Network VLAN Range）] および **[VRF VLAN 範囲（VRF VLAN Range）]**：レイヤ 3 VRF およびオーバーレイ ネットワークの VLAN 範囲です。

[サブインターフェイス Dot1q 範囲（Subinterface Dot1q Range）]：L3 サブインターフェイスを使用する場合のサブインターフェイスの範囲を指定します。

[VRF Lite の展開（VRF Lite Deployment）]：ファブリック間接続を拡張するための VRF Lite 方式を指定します。

[VRF Lite サブネット IP 範囲（VRF Lite Subnet IP Range）] フィールドは、VRF LITE IFC が自動作成されるときに VRF LITE に使用される IP アドレス用に予約されたリソースを指定します。Back2BackOnly、ToExternalOnly、または Back2Back & ToExternal を選択すると、VRF LITE IFC が自動作成されます。

[自動展開両方（Auto Deploy Both）]：このチェックボックスは、対称 VRF Lite 展開に適用されます。このチェックボックスをオンにすると、自動作成された IFC の自動展開フラグが true に設定され、対称 VRF Lite 構成がオンになります。

このチェックボックスは、[VRF Lite 展開（VRF Lite Deployment）] フィールドが [手動（Manual）] に設定されていない場合に選択または選択解除できます。この場合、ユーザは自動作成された IFC の [自動展開（auto-deploy）] フィールドを明示的にオフにし、ユーザ入力には常に優先順位が与えられます。このフラグは、新しい自動作成 IFC にのみ影響し、既存の IFC には影響しません。

[VRF Lite サブネット IP 範囲（VRF Lite Subnet IP Range）] および [VRF Lite サブネットマスク（VRF Lite Subnet Mask）]：これらのフィールドには、DCI サブネットの詳細が入力されます。必要に応じて、次のフィールドを更新します。

画面に表示される値は自動的に生成されます。IP アドレス範囲、VXLAN レイヤ 2/レイヤ 3 ネットワーク ID 範囲、または VRF/ネットワーク VLAN 範囲を更新する場合は、次のことを確認します。

Note 値の範囲を更新する場合は、他の範囲と重複しないようにしてください。一度に更新できる値の範囲は 1 つだけです。複数の値の範囲を更新する場合は、別のインスタンスで実行します。たとえば、L2 と L3 の範囲を更新する場合は、次の手順を実行する必要があります。

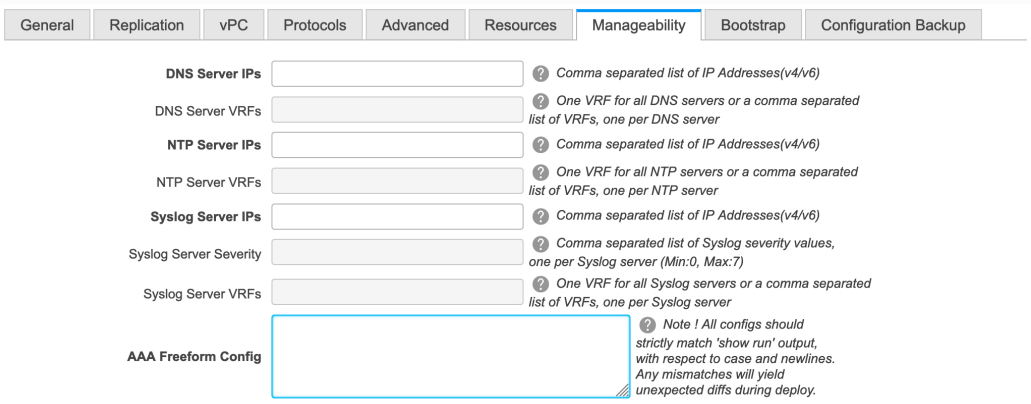
a. L2 範囲を更新し、[保存（Save）] をクリックします。

b. [ファブリックの編集（Edit Fabric）] オプションをもう一度クリックし、L3 範囲を更新して [保存（Save）] をクリックします。

[サービス ネットワーク VLAN 範囲（Service Network VLAN Range）]：[サービス ネットワーク VLAN 範囲（Service Network VLAN Range）] フィールドで VLAN 範囲を指定します。これはスイッチごとのオーバーレイ サービス ネットワーク VLAN 範囲です。最小許容値は 2 で、最大許容値は 3967 です。

[ルート マップ シーケンス番号範囲（Route Map Sequence Number Range）]：ルートマップのシーケンス番号の範囲を指定します。最小許容値は 1 で、最大許容値は 65534 です。

9. **管理能力（Manageability）** 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。

[DNS サーバ IP（DNS Server IPs）]：ドメイン ネーム システム（DNS) サーバの IP アドレス（v4/v6）のカンマ区切りリストを指定します。

[DNS サーバ VRF（DNS Server VRFs）]：すべての DNS サーバに 1 つの VRF を指定するか、DNS サーバごとに 1 つの VRF を、カンマ区切りリストで指定します。

[NTP サーバ IP（NTP Server IPs）]：NTP サーバの IP アドレス（v4/v6）のカンマ区切りリストを指定します。

[NTP サーバ VRF（NTP Server VRFs）]：すべての NTP サーバに 1 つの VRF を指定するか、NTP サーバごとに 1 つの VRF を、カンマ区切りリストで指定します。

[Syslog サーバ IP（Syslog Server IPs）]：syslog サーバの IP アドレスのカンマ区切りリスト（v4/v6）を指定します（使用する場合）。

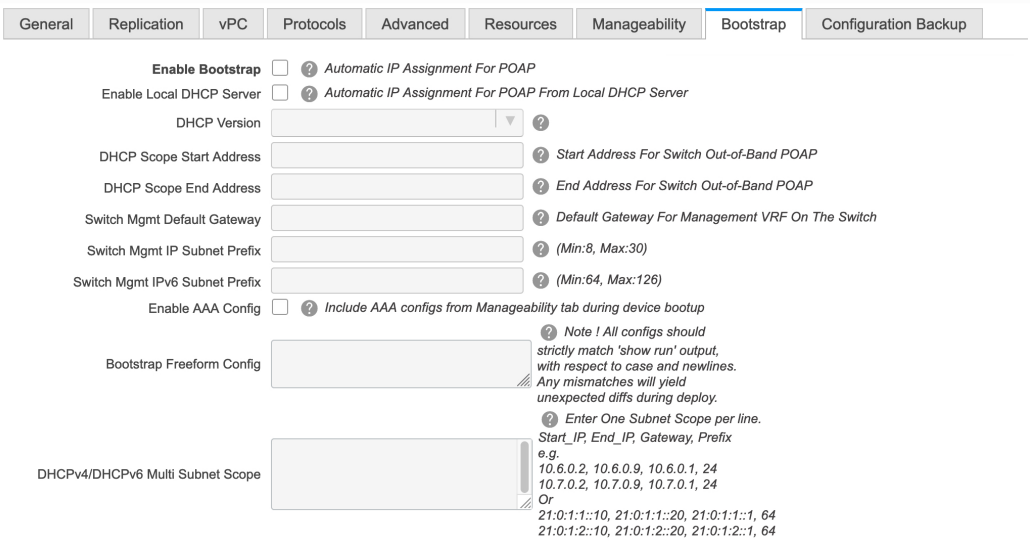
[Syslog サーバのシビラティ（重大度）（Syslog Server Severity）]：syslog サーバごとに 1 つの syslog シビラティ（重大度）値のカンマ区切りリストを指定します。最小値は 0 で、最大値は 7 です。高いシビラティ（重大度）を指定するには、大きい数値を入力します。

[Syslog サーバ VRF（Syslog Server VRFs）]：すべての syslog サーバに 1 つの VRF を指定するか、syslog サーバごとに 1 つの VRF を指定します。

[AAA 自由形式の構成（AAA Freeform Config）：AAA 自由形式の構成を指定します。

ファブリック設定で AAA 構成が指定されている場合は、ソースが [UNDERLAY_AAA]、説明が [AAA 構成（AAA Configurations）] の [switch_freeform PTI] が作成されます。

10. **[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）]：このチェックボックスを選択し、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使用すると、新しいデバイスを day-0 段階で簡単にインポートし、既存のファブリックに組み込むことができます。ブートストラップは NX-OS POAP 機能を活用します。

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）]** 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（Local DHCP Server）：[ローカル DHCP サーバ（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。

ローカル DHCP サーバーの有効化（Enable Local DHCP Server）：ローカル DHCP サーバーを介した自動 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、**[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）]** フィールドが編集可能になります。

このチェックボックスをオンにしない場合、DCNM 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 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）]** フィールドが無効になります。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。

Note Cisco Nexus 9000 および 3000 シリーズ スイッチは、スイッチがレイヤ 2 隣接（eth1 またはアウトオブバンド サブネットが /64 である必要がある）、または一部の IPv6 /64 サブネットにある L3 隣接である場合にのみ、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。

[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。プレフィックスは 8 ～ 30 の間である必要があります。

DHCP スコープ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 スコープ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 ー 126 の範囲で指定する必要があります。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 構成の有効化（Enable AAA Config）]：ブートストラップ後のデバイス起動構成の一部として [管理可能性（Manageability）] タブから AAA 構成を含めます。

[ブートストラップ フリーフォームの構成（Bootstrap Freeform Config）]：（オプション）必要に応じて追加のコマンドを入力します。たとえば、デバイスにプッシュするいくつかの追加の設定が必要であり、ポストデバイスブートストラップが使用可能である場合、このフィールドでキャプチャして要求のとおりに保存することが可能です。デバイスの起動後、**[ブートストラップ自由形式の構成（Bootstrap Freeform Config）** フィールドで定義された構成を含めることができます。

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、スイッチのフリーフォーム設定エラーの解決, on page 353を参照してください。

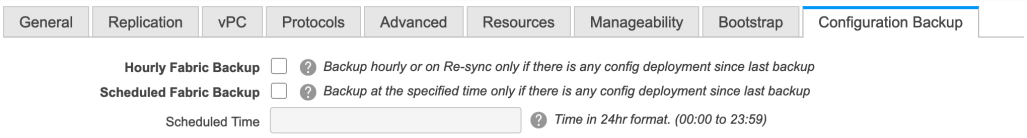
[DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）]：1行に1つのサブネット スコープを入力して、フィールドを指定します。**[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）]** チェックボックスをオンにした後で、このフィールドは編集可能になります。

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

11. [構成のバックアップ（Configuration Backup）]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。



[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。

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。

バックアップ構成ファイルは、DCNM にある次のパスに保存されます：`/usr/local/cisco/dcm/dcnm/data/archive`

保持できるアーカイブファイルの数は、[サーバ プロパティ（Server Properties）] ウィンドウの [保持するデバイスあたりのアーカイブ ファイル数（# Number of archived files per device to be retained:）] フィールドで設定します。

Note 即時バックアップをトリガーするには、次の手順を実行します。

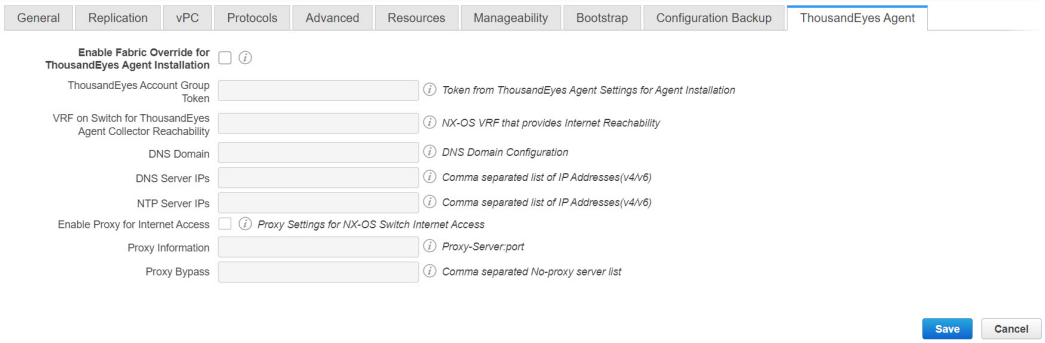
a. **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。[Fabric Builder] 画面が表示されます。

b. 特定のファブリック ボックス内をクリックします。[ファブリック トポロジ (fabric topology)] 画面が表示されます。

c. 画面左側の [アクション（Actions）] ペインで、[ファブリックの再同期（Re-Sync Fabric）] をクリックします。

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。

12. **[ThousandEyes Agent]** タブをクリックします。この機能は、Cisco DCNM リリース 11.5（3）でのみサポートされています。詳細については、「Cisco DCNM での ThousandEyes Enterprise Agent のグローバル設定の構成」を参照してください。



このタブのフィールドは次のとおりです。

Note ThousandEyes Agent のファブリック設定はグローバル設定を上書きし、そのファブリック内のスイッチにインストールされているすべての ThousandEyes エージェントに同じ構成を適用します。

- **[ThousandEyes Agent インストールのファブリック オーバーライドを有効にする（Enable Fabric Override for ThousandEyes Agent Installation）]**：チェック ボックスを選択して、ファブリックで ThousandEyes Enterprise Agent を有効にします。

- **[ThousandEyes アカウント グループ トークン（ThousandEyes Account Group Token）]** : インストール用の ThousandEyes Enterprise Agent アカウント グループ トークンを指定します。
- **[ThousandEyes Agent コレクタ到達可能性のスイッチ上の VRF（VRF on Switch for ThousandEyes Agent Collector Reachability）]** : インターネットの到達可能性を提供する VRF データを指定します。
- **[ドメイン ネーム システム（DNS） ドメイン（DNS Domain）]** : スイッチのドメイン ネーム システム（DNS） ドメイン構成を指定します。
- **[ドメイン ネーム システム（DNS） サーバ IP（DNS Server IPs）]** : ドメイン ネーム システム（DNS） サーバの IP アドレス（v4/v6）のカンマ区切りリストを指定します。DNS サーバには、最大 3 つの IP アドレスを入力できます。
- **[NTP サーバ IP（NTP Server IPs）]** : Network Time Protocol (NTP) サーバの IP アドレス（v4/v6）のコンマ区切りリストを指定します。NTP サーバには、最大 3 つの IP アドレスを入力できます。
- **[プロキシを有効にする（Enable Proxy）]** : チェックボックスをオンにして、NX-OS スイッチのインターネット アクセスのプロキシ設定を選択します。
- **[プロキシ情報（Proxy Information）]** : プロキシ サーバのポート情報を指定します。
- **[プロキシ バイパス（Proxy Bypass）]** : プロキシをバイパスするサーバ リストを指定します。

13. 関連情報を入力して更新したら、**[保存（Save）]**をクリックします。画面の右下に、ファブリックが作成されたことを示すメモが短時間表示されます。ファブリックが作成されると、ファブリックのページが表示されます。画面左上に生地名が表示されます。

    (同時に、新しく作成されたファブリック インスタンスが **[ファブリック ビルダ（Fabric Builder）]** 画面に表示されます。**[ファブリック ビルダ（Fabric Builder）]** 画面に移動するには、**[アクション（Actions）]** ペインの上にある左矢印（**[←]**）ボタン [画面の左側] をクリックします。

    [アクション（Actions）] ペインでは、さまざまな機能を実行できます。それらの 1 つは、ファブリックにスイッチを追加する **[スイッチの追加（Add switches）]** オプションです。ファブリックを作成したら、ファブリック デバイスを追加する必要があります。オプションについて説明します：

    - **[表形式の表示（Tabular View）]** : デフォルトでスイッチはトポロジ表示として映されます。このオプションを使用して、表形式のビューでスイッチを表示します。
    - **[トポロジの更新（Refresh topology）]** : トポロジを更新できます。
    - **[レイアウトの保存（Save Layout）]** : トポロジのカスタム 表示を保存します。トポロジに特定のビューを作成し、使いやすいように保存できます。
    - **[保存されたレイアウトの削除（Delete saved layout）]** : トポロジのカスタム 表示を削除します。

- **[トポロジ表示（Topology views）]**：保存されたレイアウトの表示オプションは、階層型、ランダム、およびカスタムから選択できます。
  - **[階層型（Hierarchical）]**：トポロジのアーキテクチャ表示を表示。CLOS トポロジの構成方法に関するノードを示すさまざまなスイッチロールを定義できます。
  - **[ランダム（Random）]**：ノードはウィンドウ上にランダムに配置されます。DCNMは、推測を行い、近接するノードをインテリジェントに配置しようとします。
  - **[カスタム保存レイアウト（Custom saved layout）]**：ノードを好きなようにドラッグできます。好きな位置に配置したら、レイアウトの保存をクリックして位置を記憶することができます。次回トポロジにアクセスすると、DCNMにより最後に保存したレイアウト位置に基づいてノードが描画されます。
- **[ファブリックの復元（Restore Fabric）]**：ファブリックを以前のDCNM構成状態に復元できます（1か月前、2か月前など）。詳細については、「ファブリックの復元」セクションを参照します。
- **[今すぐバックアップ（Backup Now）]**：**[今すぐバックアップ（Backup Now）]**をクリックして、ファブリックバックアップを手動で開始できます。タグの名前を入力して、**[OK]**をクリックします。**[ファブリック設定（Fabric Settings）]**ダイアログボックスの**[構成バックアップ（Configuration Backup）]**タブで選択した設定に関係なく、このオプションを使用してバックアップを開始できます。
- **[ファブリックの再同期Resync Fabric（Resync Fabric）]**：大規模なアウトオブバンド変更がある場合、または構成変更がDCNM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DCNM状態を再同期します。再同期操作は、ファブリック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ウィンドウに表示されます。再同期中に、実行構成がスイッチから取得されます。次に、スイッチのOut-of-Sync/In-Syncステータスは、DCNMで定義された意図または予想される構成と、スイッチから取得された現在実行中の構成に基づいて再計算されます。
- **[スイッチを追加（Add Switches）]**：ファブリックにスイッチインスタンスを追加しすることを許可します。
- **[ファブリック設定（Fabric Settings）]**：ファブリック設定を表示または編集できます。
- **[クラウド（Cloud）]**アイコン：**[クラウド（Cloud）]**アイコンをクリックして、**[未検出（Undiscovered）]**のクラウドを表示（または非表示に）します。

  アイコンをクリックすると、未検出のクラウドと、選択したファブリックトポロジへのリンクは表示されません。

  [未検出（Undiscovered）]クラウドを表示するために**[クラウド（Cloud）]**アイコンをまたクリックします。

[範囲（SCOPE）]：右上の[範囲（SCOPE）]ドロップダウンボックスを使用して、ファブリックを切り替えることができます。現在のファブリックは、強調表示されます。MSD とそのメンバーファブリックが明確に表示され、メンバーファブリックはMSDファブリックの下にくぼんで表示されます。

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。

[アクション（Actions）]パネルから**[スイッチの追加（Add Switches）]**オプションをクリックして、DCNMで作成されたファブリックにスイッチを追加します。**[インベントリ管理（Inventory Management）]**画面が表示されます。画面には2つのタブがあり、1つは既存のスイッチを検出するためのもので、もう1つは新しいスイッチを検出するためのものです。両方のオプションについて説明します。

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 , on page 46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, on page 51を参照してください。

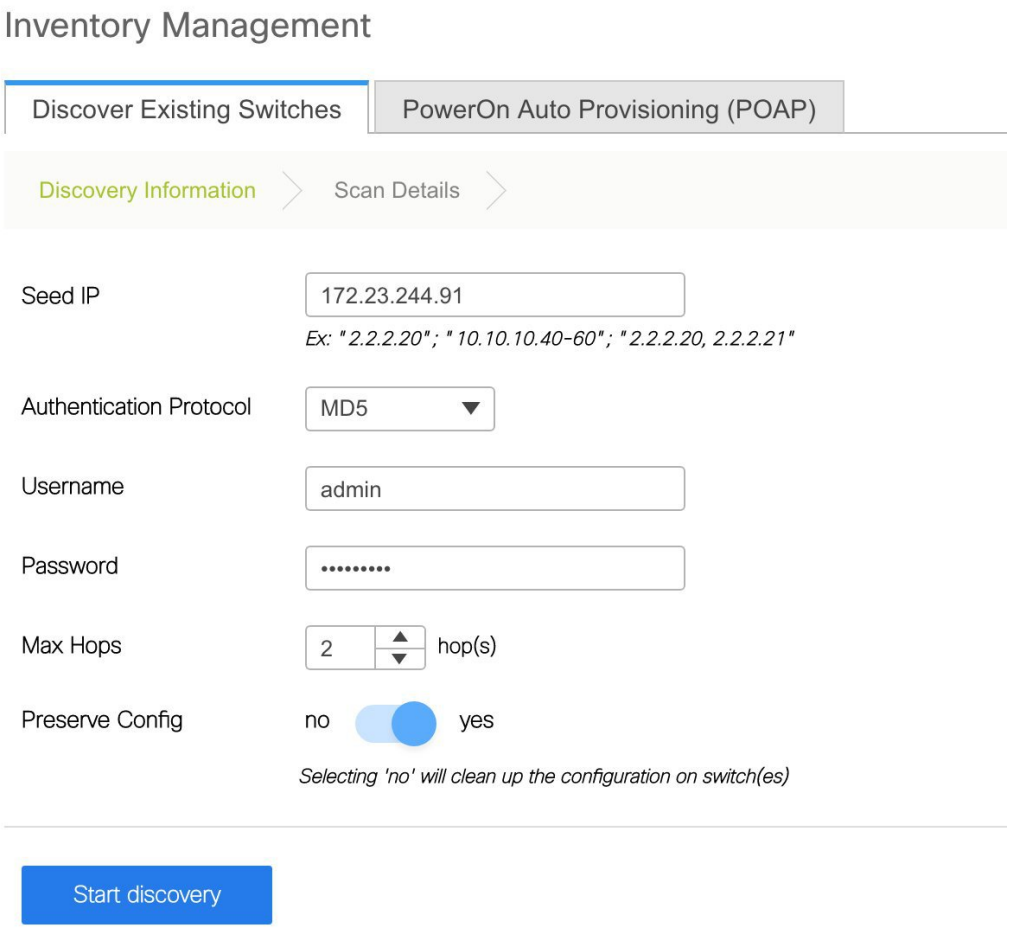
Note DCNM でピリオド文字（.）を含むホスト名を持つスイッチが検出されると、ドメイン名として扱われ、切り捨てられます。ピリオド文字（.）の前のテキストのみがホスト名と見なされます。次に例を示します。

- ホスト名が **[leaf.it.vxlan.bgp.org1-XYZ]** の場合、DCNM で **[leaf]** のみが表示されます。
- ホスト名が **[leaf-itvxlan.bgp.org1-XYZ]** の場合、DCNM で **[leafit-vxlan]** のみが表示されます。

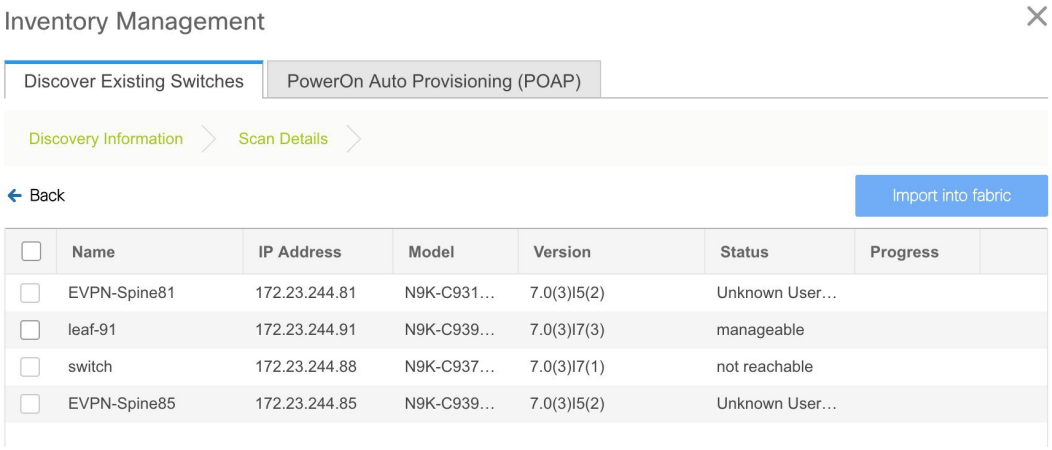
既存のスイッチの検出

1. **[スイッチの追加（Add Switches）]**をクリックした後、**[既存のスイッチの検出（Discover Existing Switches）]**タブを使用して、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。スイッチの IP アドレス（シード IP）、管理者名、ユーザー名、およびパスワード（**[ユーザー名（Username）]**フィールドと**[パスワード（Password）]**フィールド）は、ユーザーによる入力として提供されます。**[構成の保持（Preserve Config）]**ノブは、デフォルトで**[yes]**に設定されています。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。デバイス構成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）]**ノブを**[no]**に設定する必要があります。

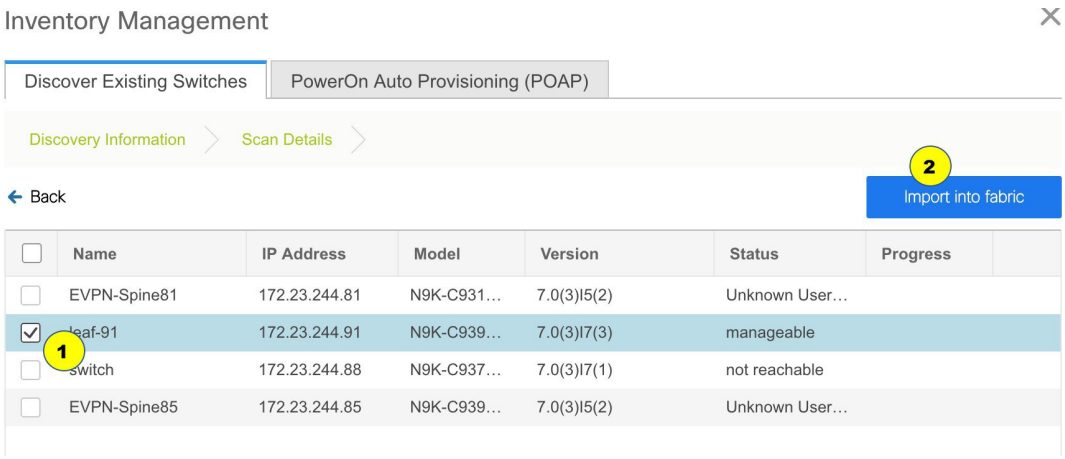
Note Easy_Fabric_eBGP は、ファブリックへのデバイスのブラウンフィールドインポートをサポートしていません。



2. [検出の開始（Start discovery）] をクリックします。**[スキャン詳細（Scan Details）]** ウィンドウ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（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 **[スキャン詳細（Scan Details）]** の結果に入力されます。



3. DCNM がスイッチに対して正常なシャロー検出を実行できた場合、ステータスに **[管理性（Manageable）]** と表示されます。適切なスイッチの横にあるチェックボックスをオンにして、**[ファブリックにインポート（Import into fabric）]** 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。

Note 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。

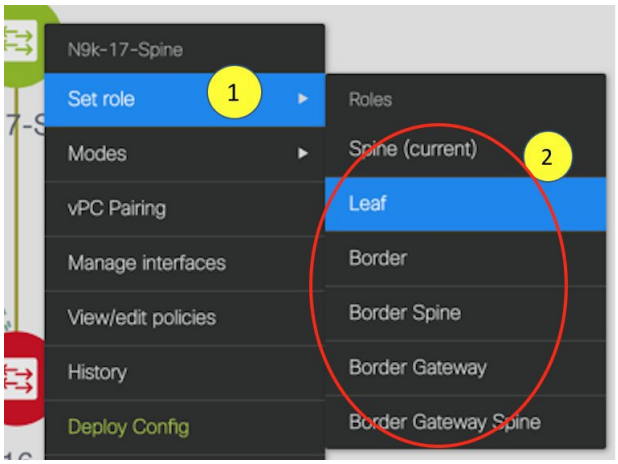
DCNM がすべてのスイッチを検出し、[進行状況（Progress）] 列にすべてのスイッチの **[done]** が表示されたら、画面を閉じます。*[*スタンドアロン ファブリック トポロジ（Standalone fabric topology）] 画面が再び表示されます。追加されたスイッチのスイッチアイコンが表示されます。

Note 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。

4. 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。

5. 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。このためには、デバイスをクリックし、**[ロールの設定]** オプションを使用して適切なロールを設定します。代わりに、表形式のビューを使用して、一度に複数のデバイスに同じロールを割り当てることもできます。



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 パスワード：（**[管理性（Manageability）]** タブで）AAA サーバ情報を入力した場合は、各スイッチで AAA サーバ 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 DCNM 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。

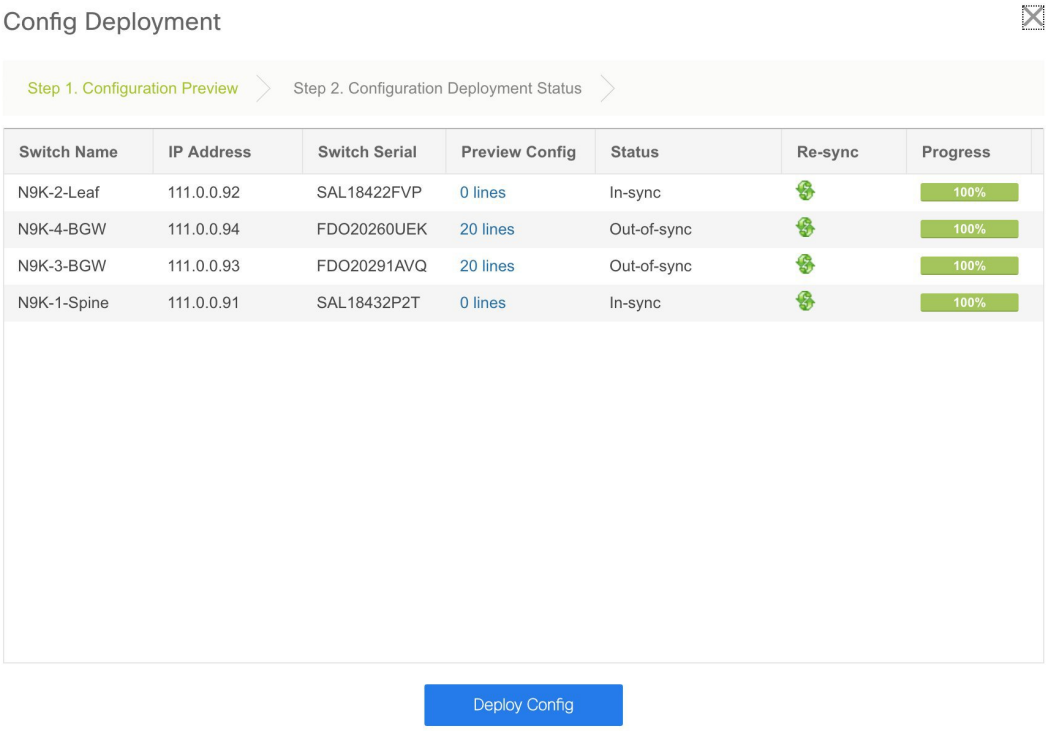
6. 画面の右上にある **[保存と展開（Save & Deploy）]** をクリックします。

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。自由形式構成の詳細については、「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。

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 DCNM からファブリックにプロビジョニングされた構成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、DCNM 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。

[保存と展開（Save & Deploy）] 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 DCNM 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 DCNM 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 DCNM 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、DCNM 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。

[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。

DCNM 11 では、複数行のバナー motd 構成がサポートされています。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 DCNM 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 **[保存と展開（Save & Deploy）]** 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、自由形式の設定/ポリシー

に関連するバナーは1つだけ作成できます。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。

7. 画面 を閉じます。

   構成展開の画面で、画面下部の [構成の展開（Deploy Config）] をクリックして、保留中の構成をスイッチに展開開始します。[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。

   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、スイッチと DCNM の構成が同期していないことを示します。スイッチで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、**[保存と展開（Save & Deploy）]** をクリックしてスイッチの状態を再計算できます。

Note CLI の実行で警告またはエラーが発生した場合は、**[Fabric Builder]** ウィンドウに通知が表示されます。自動解決可能な警告またはエラーには、**[解決（Resolve）]** オプションがあります。

スイッチのリロードまたはRMA操作の後にリーフスイッチが起動すると、DCNMは、スイッチとそれに接続されている FEX デバイスの構成をプロビジョニングします。DCNM が FEX（ホスト インターフェイス）構成をプロビジョニングした後に FEX 接続が起動し、構成が一致しない場合があります。不一致を解決するには、ファブリック トポロジ画面で **[保存と展開（Save & Deploy）]** を再度クリックします。

Cisco NX-OS リリース 11.4(1) 以降、**[トポロジ（Topology）]** ウィンドウの **[FEX]** チェックボックスをオフにすると、FEX デバイスは **[ファブリック ビルダ（Fabric Builder）]** トポロジ ウィンドウでも非表示になります。**Fabric Builder** で FEX を表示するには、このチェックボックスをオンにする必要があります。このオプションはすべてのファブリックに適用でき、セッションごとに保存されるか、DCNMからログアウトするまで保存されます。ログアウトしてDCNMにログインすると、FEXオプションはデフォルトにリセットされます。つまり、デフォルトで有効になります。詳細については、パネルを表示を参照してください。

[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。

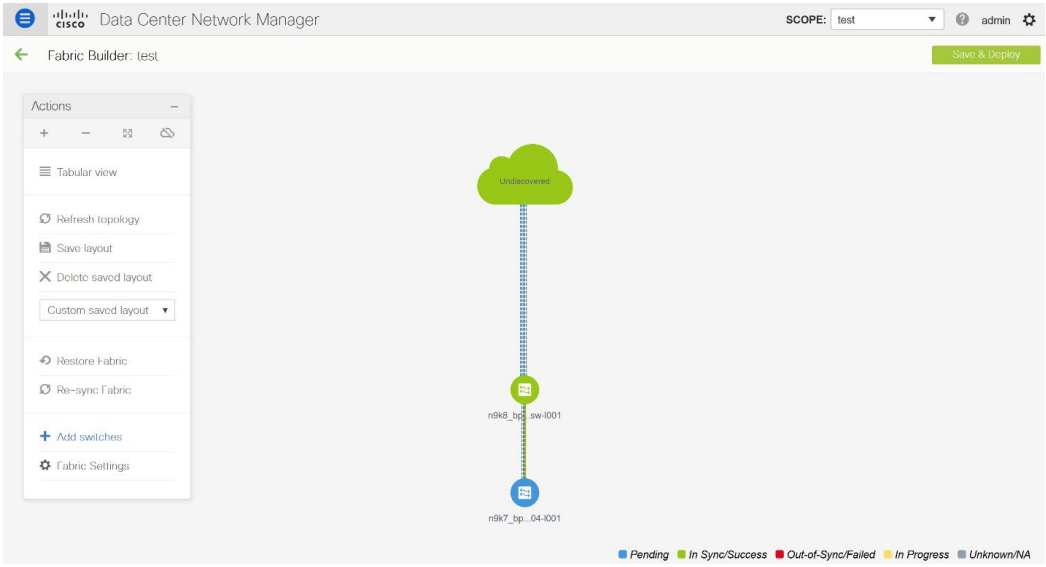
新しいスイッチの検出

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 DCNM の間に IP 到達可能性がある限り、デバイスからの DHCP 要求は DCNM 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 DCNM によって処理されます。DCNM 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. DCNM GUI で、ファブリックに移動します（**[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** をクリックし、ファブリックをクリックします）。ファブリック トポロジが表示されます。



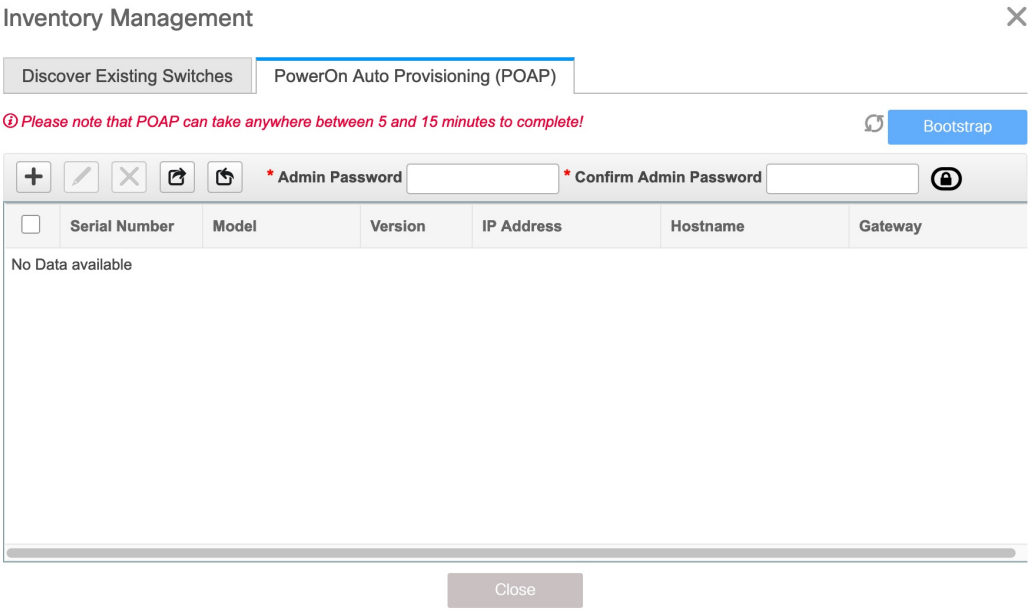
ファブリック トポロジ ウィンドウに移動し、**[アクション（Actions）]** パネルから **[スイッチの追加（Add switches）]** オプションをクリックします。[インベントリ管理（Inventory Management）] ウィンドウが表示されます。

5. **[POAP]** タブをクリックします。

前述のように、DCNM 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。

Note

- ウィンドウの左上には、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するためのエクスポートおよびインポートオプションがあります。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。

リリース 11.2(1) 以降、デバイスを事前にプロビジョニングできます。デバイスの事前プロビジョニングについては、デバイスの事前プロビジョニング , on page 46 を参照してください。

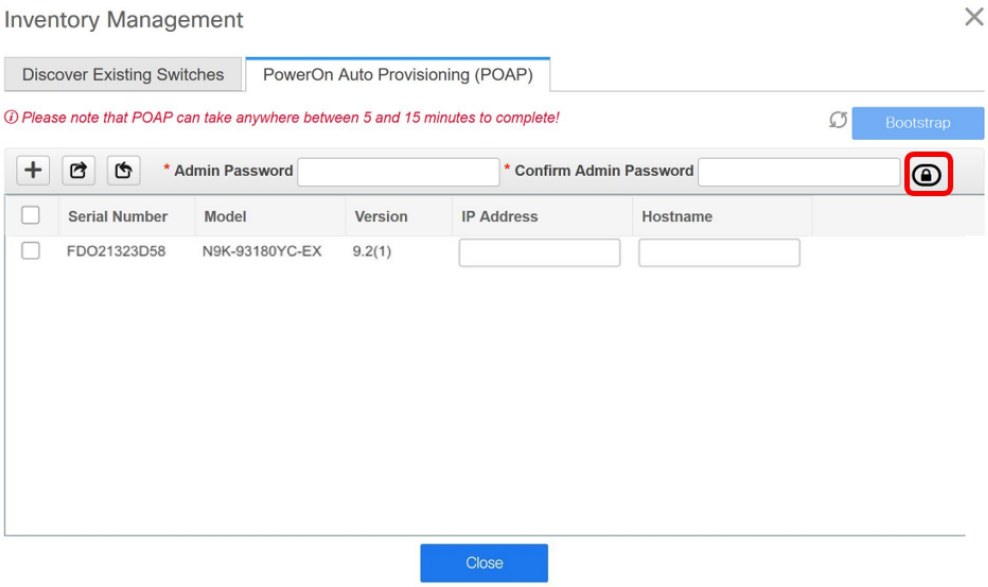
6. **[管理者パスワード（Admin Password）]** フィールドと **[管理者パスワードの確認（Confirm Admin Password）]** フィールドに、新しいパスワードを入力します。

   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。

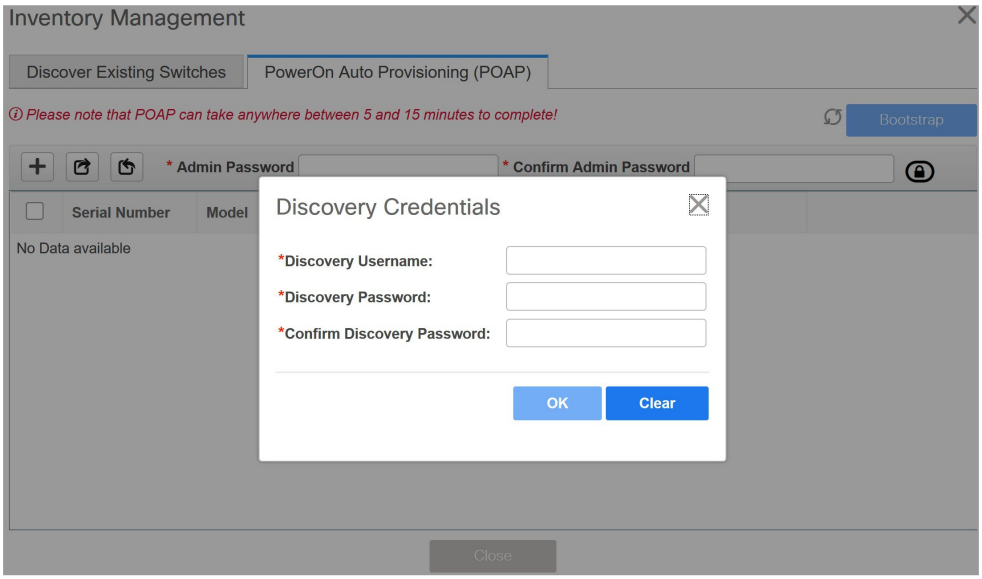
Note 管理者クレデンシャルを使用してスイッチを検出しない場合は、代わりに AAA 認証（RADIUS または TACACS クレデンシャル）を使用できます。

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 クレデンシャルの追加（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 クレデンシャルを入力します。



b. **[ディスカバリ クレデンシャル（Discovery Credentials）]** ウィンドウで、ディスカバリ ユーザ名やパスワードなどのディスカバリ クレデンシャルを入力します。



[OK] をクリックして、ディスカバリ クレデンシャルを保存します。

検出クレデンシャルが指定されていない場合は、DCNM は管理者ユーザ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。

DCNM は管理IPアドレスおよびその他のクレデンシャル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 [保存と展開（Save & Deploy）] 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。

Note 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時に、**[管理性（Manageability）]** タブに AAA サーバ情報を入力した場合は、各スイッチの AAA サーバ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。

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。

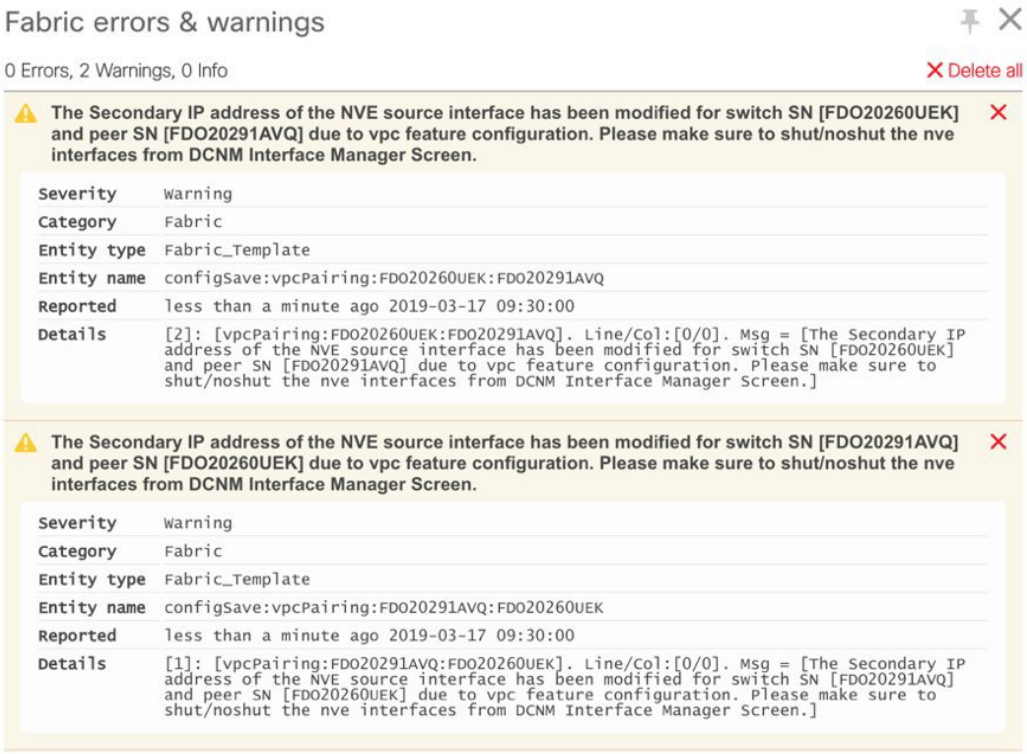
14. スイッチとリンクが DCNM で検出されます。設定は、さまざまなポリシー（ファブリック、トポロジ、スイッチ生成ポリシーなど）に基づいて構築されます。スイッチイメージ（およびその他の必要な）設定がスイッチで有効になっている。

15. DCNM 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 は基本設定で完了します。追加構成を行うには、**[制御（Control）] > [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設定する必要があります。以下が含まれますが、これらに限定されません。

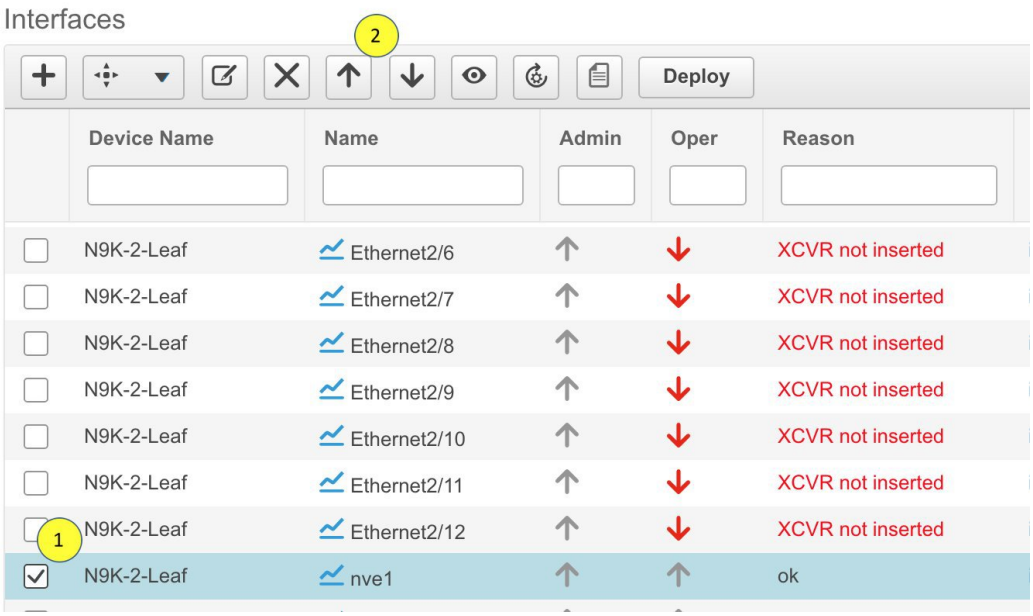
    - vPC ペアリング。
    - ブレークアウト インターフェイス。
    - ポートチャネル、およびポートへのメンバーの追加。

    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、**[保存と展開（Save & Deploy）]** 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、[制御（Control）]>[インターフェイス（Interfaces）]画面に移動し、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）。

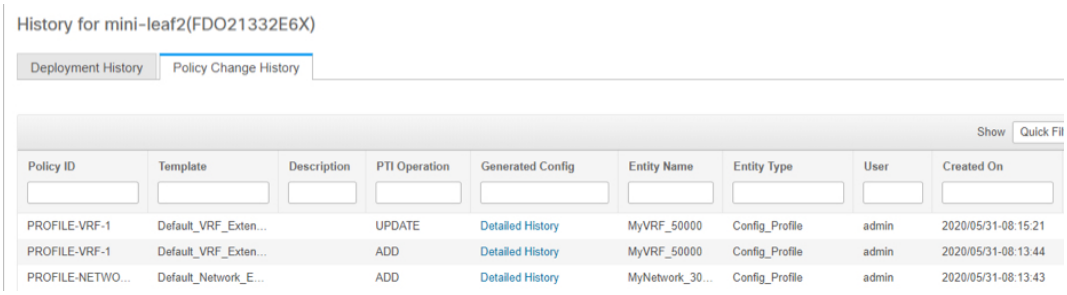
Note

- スイッチのロールの変更は、**[保存と展開（Save & Deploy）]** を実行する前にのみ許可されます。
- DCNM 11.1(1) 以降、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, on page 186 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。

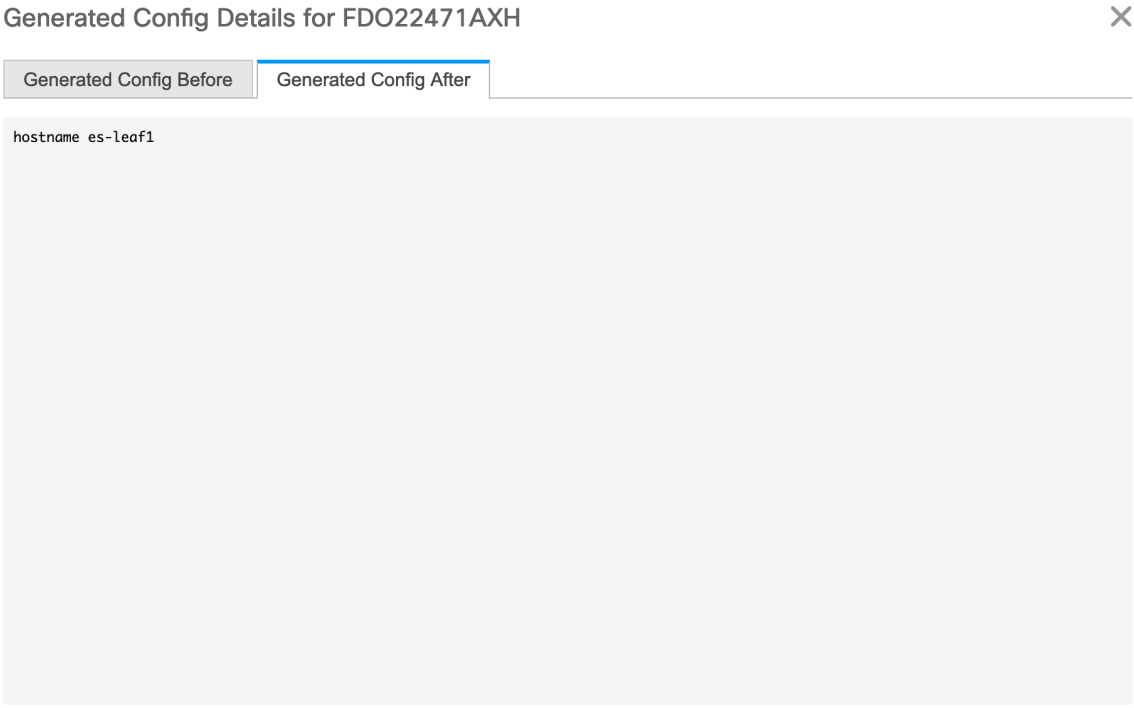
- **モード**：メンテナンス モードとアクティブ/操作モード。
- **vPC** ペアリング：vPC のスイッチを選択し、そのピアを選択します。

  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	生成後の構成
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

Note 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。
- **展開構成** - 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 DCNM で検出され、アンダーレイ構成がそれらのスイッチでプロビジョニングされ、DCNM との間の構成が同期されます。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。[「インターフェイス」を参照してください]。
- ネットワークを作成し、スイッチに展開します。[「ネットワークおよび VRF の作成と展開 」を参照してください]。

DCNM 11 での事前プロビジョニングのサポート

Cisco DCNM 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 DCNM でデバイス構成を準備できます。Easy ファブリックと外部/Classic_LAN ファブリックの両方で、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

Cisco DCNM リリース 11.2 以降、デバイスを事前にプロビジョニングできます。

Note ファブリック設定の [ブートストラップ（Bootstrap）] タブに DHCP の詳細を確実に入力してください。

- 事前プロビジョニングされたデバイスは、DCNM で次の構成をサポートします。
  - 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、DCNM で次の構成をサポートしません。
  - 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）]** ウィンドウの **[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。

  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。
    - **modulesModel** ：（必須）スイッチ モジュールのモデル情報を指定します。
    - **gateway** ：（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、DCNM 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。
    - **breakout**：（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。
    - **portMode**：（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"}

Procedure

ステップ 1 **[制御（Control）] > [Fabric Builder]**の順にクリックします。

[ファブリック ビルダ（Fabric Builder）] 画面が表示されます。

ステップ 2 ファブリック ボックス内をクリックします。

ステップ 3 [アクション（Actions）] パネルで、**[スイッチの追加（Add switches）]** オプションをクリックします。

[インベントリ管理（Inventory Management）] 画面が表示されます。

ステップ 4 **[POAP]** タブをクリックします。

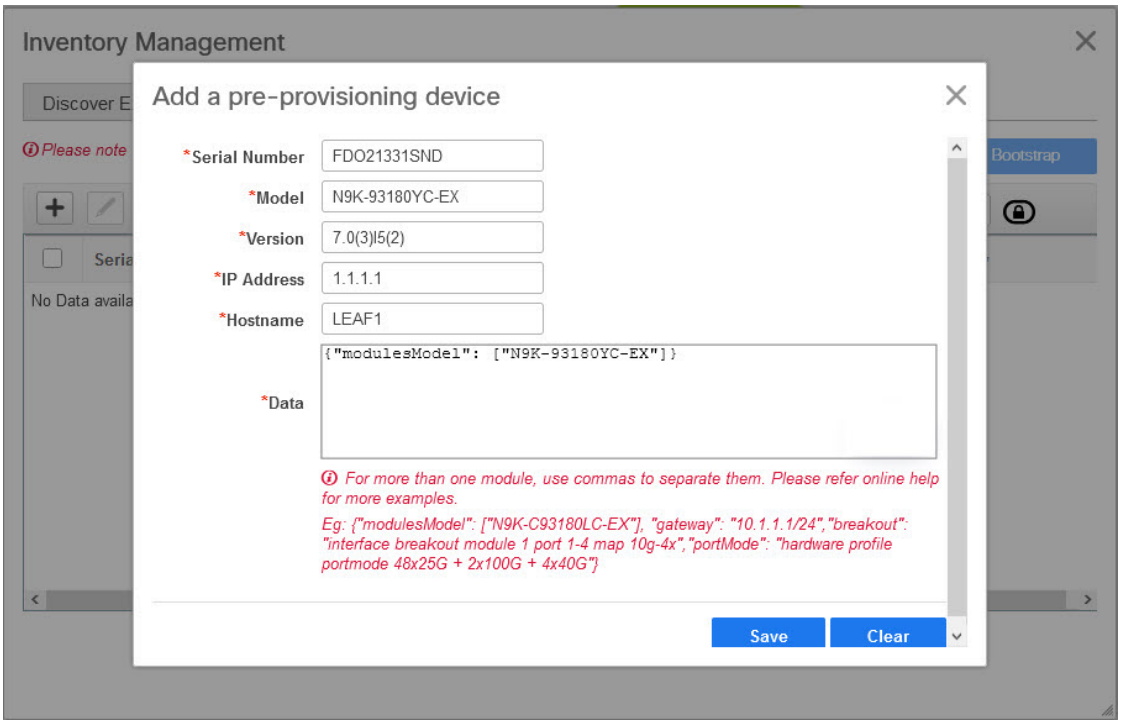
ステップ 5 **[POAP]** タブで、次の手順を実行します。

a. 画面左上の [+] をクリックします。

[新しいデバイスの追加（Add a new device）] 画面が表示されます。

b. スクリーンショットに示されているように、デバイスの詳細を入力します。

c. [保存（Save）] をクリックします。



IP アドレス：新しいデバイスの IPv4 または IPv6 アドレスを指定します。

シリアル番号：デバイスのシリアル番号。シリアル番号は Cisco Build of Material Purchase にあり、事前プロビジョニング機能の使用中にこれらの値を参照できます。

データ フィールドの詳細については、ガイドラインで提供されている例を参照してください。

デバイスの詳細がPOAP画面に表示されます。事前プロビジョニング用にデバイスをさらに追加できます。

ウィンドウの左上には、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するための **[エクスポート（Export）]** および **[インポート（Import）]** アイコンがあります。

[インポート（Import）] オプションを使用して複数のデバイスを事前プロビジョニングすることができます。

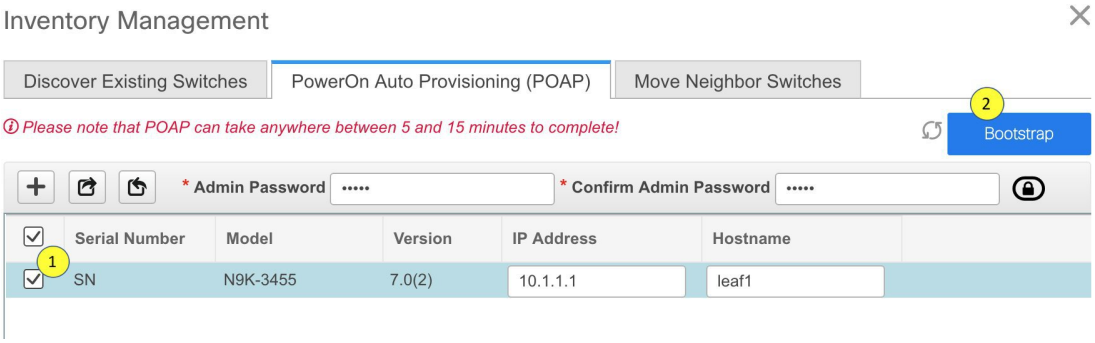
すべての必須フィールド（シリアル番号、モデル、バージョン、IpAddress、ホスト名、およびデータ フィールド [JSON オブジェクト]）を使用して、.csv ファイルに新しいデバイスの情報を追加します。

[データ（Data）] 列は、ファブリック テンプレートからハードウェア タイプを識別するためのモジュールのモデル名で構成されます。A.csv ファイルのスクリーンショット：

	A	B	C	D	E	F	G
1	#SerialNumber(Eg:FD01344GH5)	#Model(Eg:N9k-C9236C)	#Version(Eg:7.0(3)12(3))	#IPAddress of the device	#HostName	#Data(JSON Field contains model name of the modules	
2	Serial Number	Model	Version	IP Address	Hostname	Data	
3	FDO21331SND	N9K-93180YC-EX	7.0(3)I5(2)	1.1.1.1	leaf1	{"modulesModel":["N9K-93180YC-EX"]}	
4	FDO21351N3X	N9K-C9236C	7.0(3)I4(1)	11.1.1.1	spine1	{"modulesModel":["N9K-C9236C"]}	
5	FDO21491A5K	N9K-C93240YC-FX2	7.0(3)I7(3)	12.1.1.1	leaf2	{"modulesModel":["N9K-C93240YC-FX2"]}	
6							

ステップ 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、管理パスワードを入力します。

ステップ 7 デバイスを選択して、画面右上の **[ブートストラップ（Bootstrap）]** をクリックします。



Leaf1 デバイスがファブリック トポロジに表示されます。

[アクション（Actions）] パネルで、**[表形式ビュー（Tabular View）]** をクリックします。事前にプロビジョニングされたすべてのスイッチのステータスが **[検出ステータス（Discovery Status）]** 列に **[ok]** と表示されるまで、ファブリックを展開できません。

Note スイッチが [到達不能（Unreachable）] 検出ステータスの場合、スイッチの最後の使用可能な情報が他の列に保持されます。

Leaf1 をファブリックに接続すると、スイッチには IP アドレス 10.1.1.1 がプロビジョニングされます。

ステップ 8 **ファブリック ビルダ** に移動し、デバイスのロールを設定します。

次のいずれかのテンプレートを使用して、リンク内ポリシーを作成します。

- **int_pre_provision_intra_fabric_link** は、DCNM に割り当てられた IP アドレスを使用して、ファブリック内インターフェイス構成を自動的に生成します
- **int_intra_fabric_unnum_link_11_1** 番号付けなしのリンクを使用している場合
- **int_intra_fabric_num_link_11_1** IP アドレスをリンク内に手動で割り当てる場合

[保存して展開（Save & Deploy）] をクリックします。

スイッチの構成は、対応する PTI に取り込まれ、**[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウに表示されます。

ステップ 9 物理デバイスを持ち込むには、手動の RMA または POAP RMA の手順に従います。

詳細については、返品許可（RMA）, on page 246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。

ホスト ポートをプロビジョニングするために 1 つ以上のスイッチがオンラインになった後、ファブリックで**[保存と展開（Save & Deploy）]**をクリックする必要があります。このアクションは、ホストポート接続用にオーバーレイをプロビジョニングする前に実行する必要があります。

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

DCNM リリース 11.4(1) 以降、**[インターフェイス（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。DCNM 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にのみ、イーサネット インターフェイスを追加できます。

（注） ネットワーク/VRF をアタッチする前に、イーサネットインターフェイスを事前にプロビジョニングしてから、ポートチャネル、vPC、ST FEX、AA FEX、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 構成に追加する必要があります。

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 （46 ページ）を参照してください。

手順

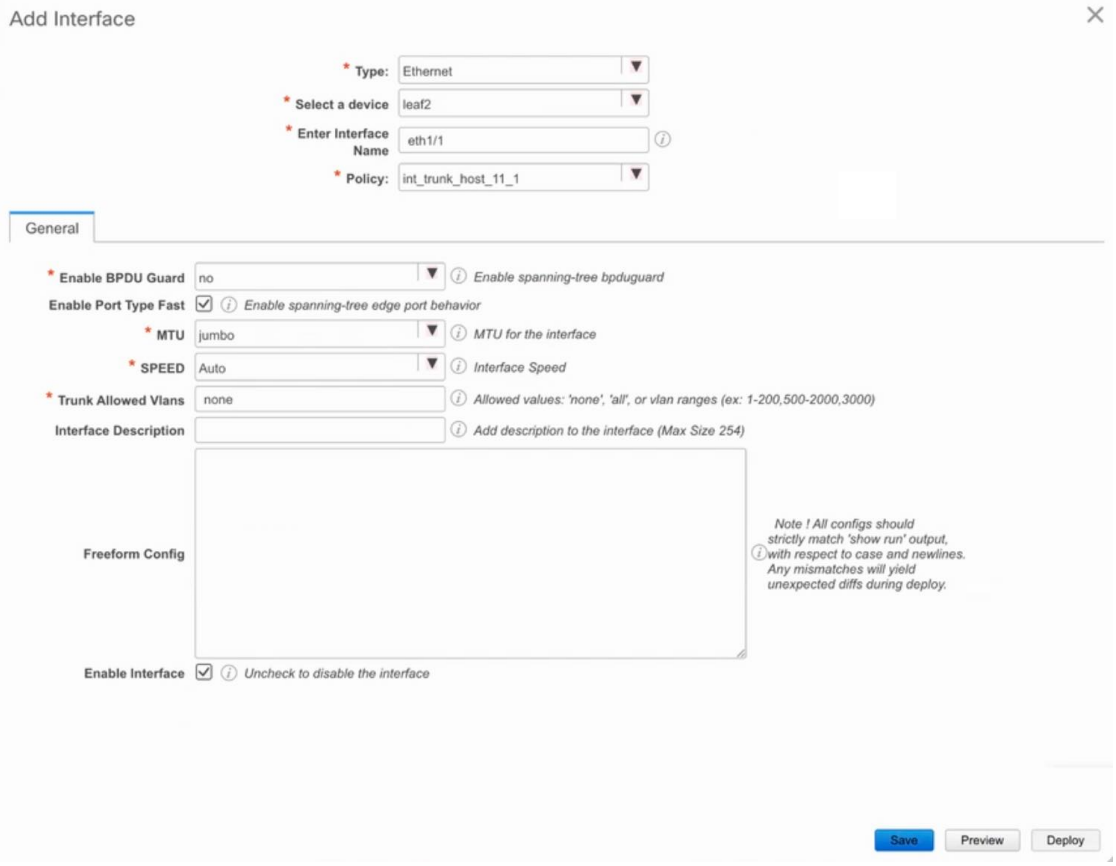
ステップ 1 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウから事前にプロビジョニングされたデバイスを含むファブリックに移動します。

ステップ 2 事前にプロビジョニングされたデバイスを右クリックし、**[インターフェイスの管理（Manage Interfaces）]** を選択します。

[制御（Control）] > [ファブリック（Fabrics）] > [インターフェイス（Interfaces）] を選択して、[インターフェイス（Interfaces）] ウィンドウに移動することもできます。[範囲（Scope）] ドロップダウンリストから、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選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 **[インターフェイスの追加（Add 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）]：この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。

（注） DCNM で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の入力（Enter 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。

詳細については、インターフェイスの追加 （258 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 **[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。

（注） 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

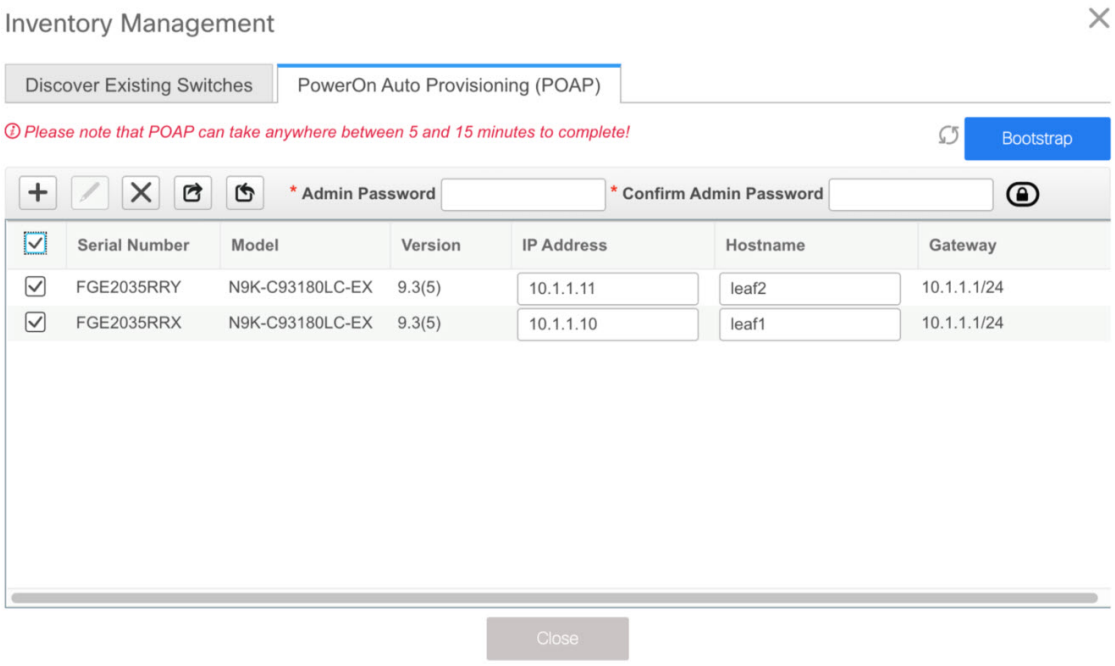
[ファブリックの設定（Fabric Settings）] で**[ブートストラップ（Bootstrap）]**が有効になっていることを確認します。

手順

ステップ 1 両方のデバイスをファブリックにインポートします。

手順については、「**デバイスの事前プロビジョニング**」を参照してください。

次の例は、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 デバイスを表示するイメージを示します。[アクション（Action）] パネルで **[スイッチの追加（Add Switches）]** を選択します。**[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。

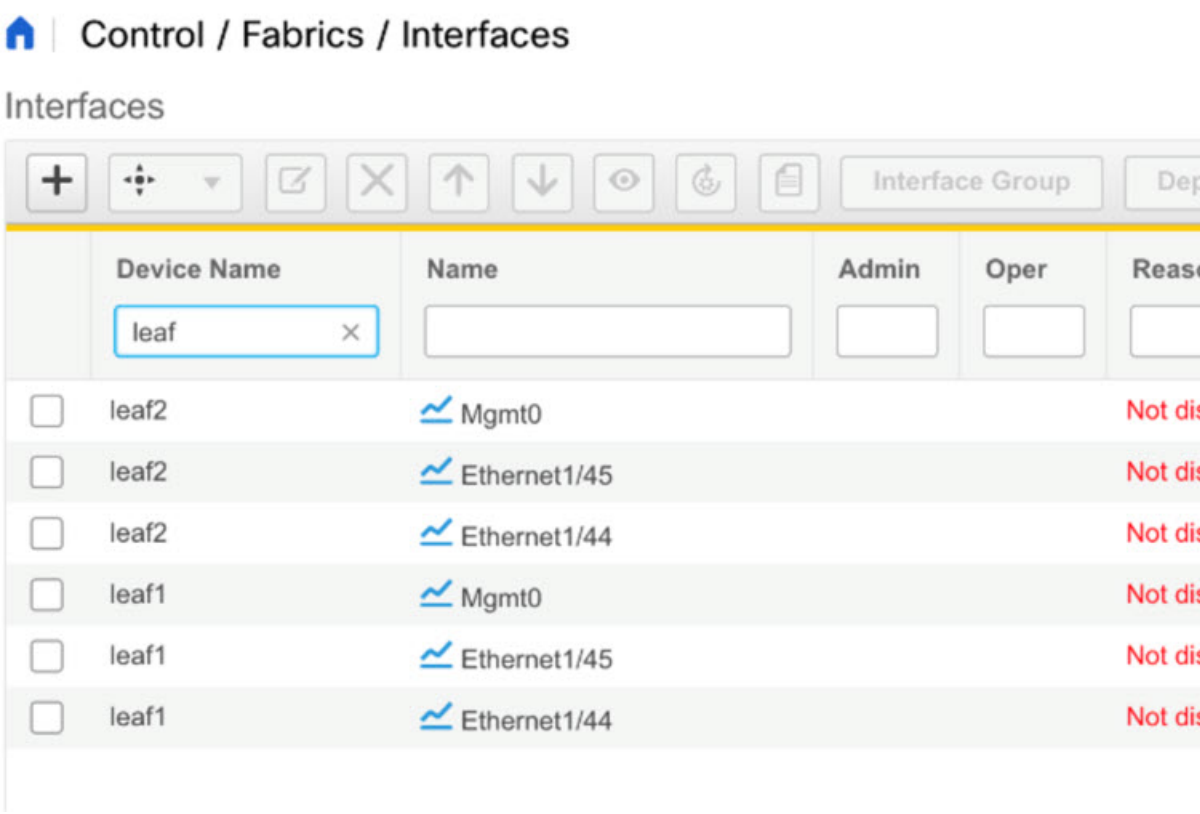
ステップ 2 右クリックして、他の到達可能なデバイスと同様に、これらのデバイスの適切な役割を選択します。

ステップ 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。**[制御（Control）] > [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。

手順については、「**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。

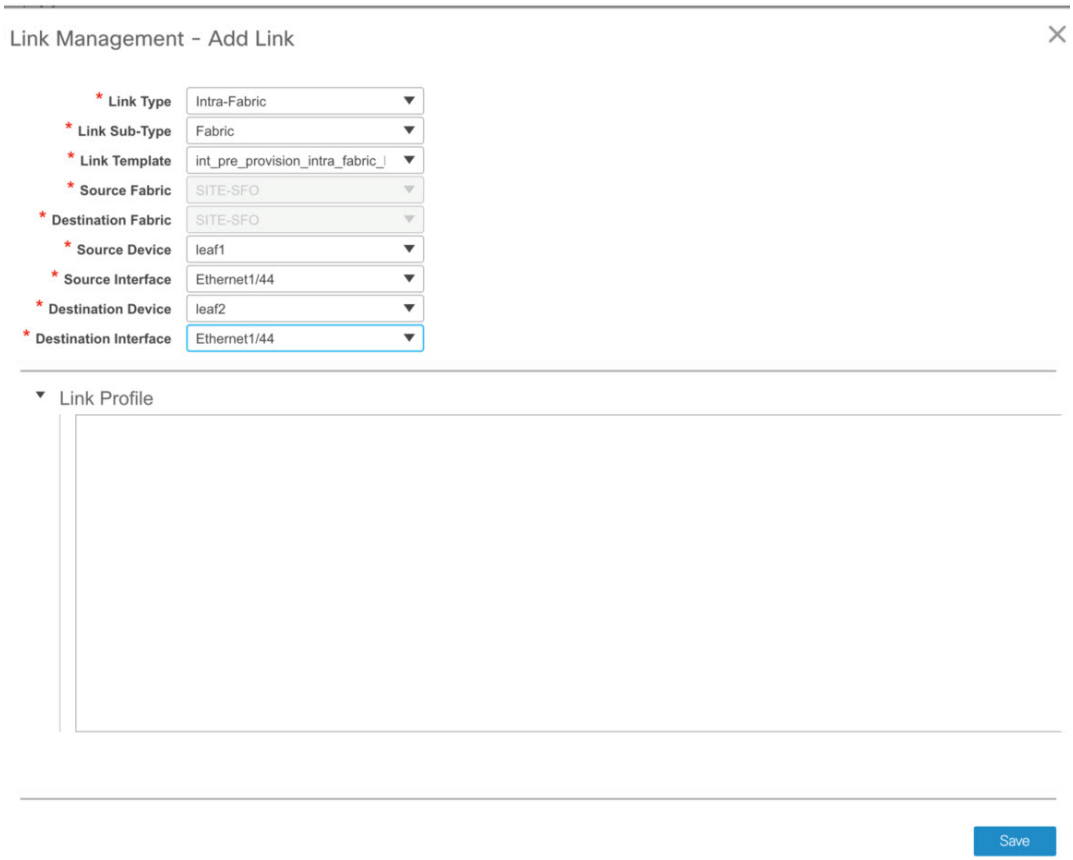
ファブリック ビルダ表示で、**[追加（Add）]** リンクを右クリックするか、ファブリック ビルダの表形式ビューの [リンク] タブで **[追加（+）（Add(+)）]** アイコンをクリックします。

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。

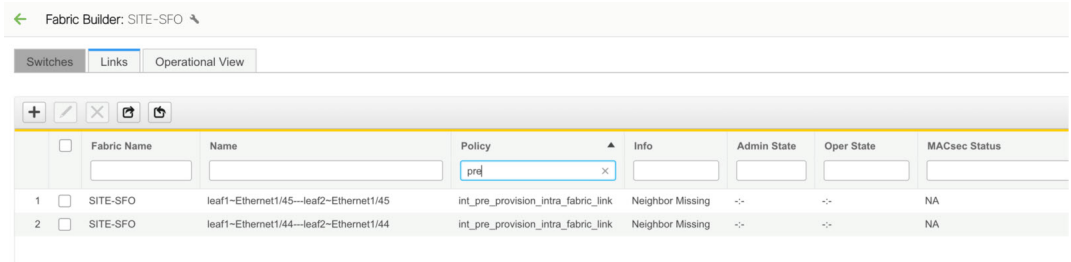
リンク テンプレートとして **int_pre_provision_intra_fabric_link** を選択していることを確認してください。送信元インターフェイスと宛先インターフェイスのフィールド名は、前の

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。

事前にプロビジョニングされたリンク作成の例を次のイメージに示します。



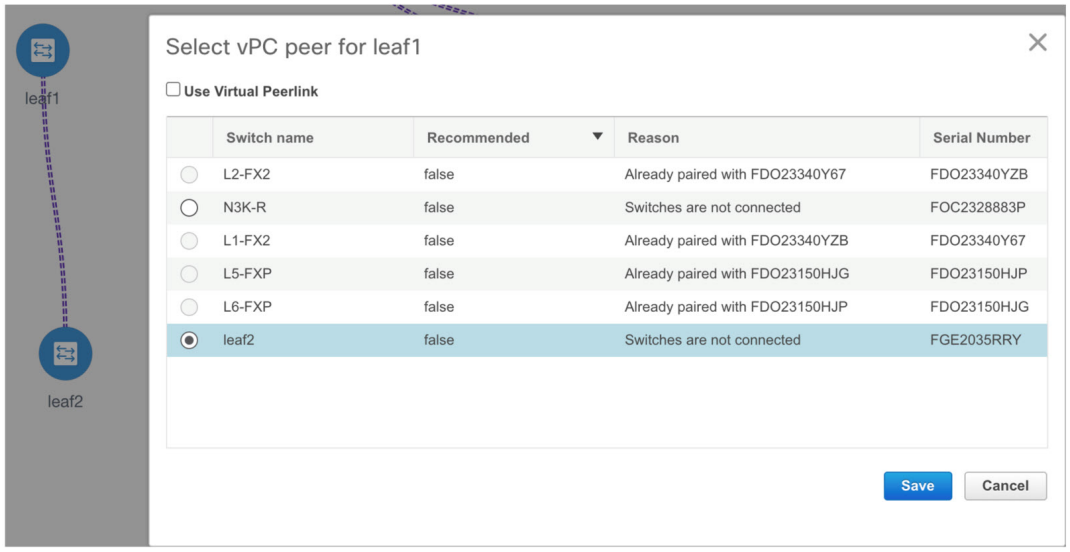
リンクが作成されると、次のイメージに示すように、[ファブリック ビルダ（Fabric builder）] の下の [リンク（Links）] タブにリスト表示されます。



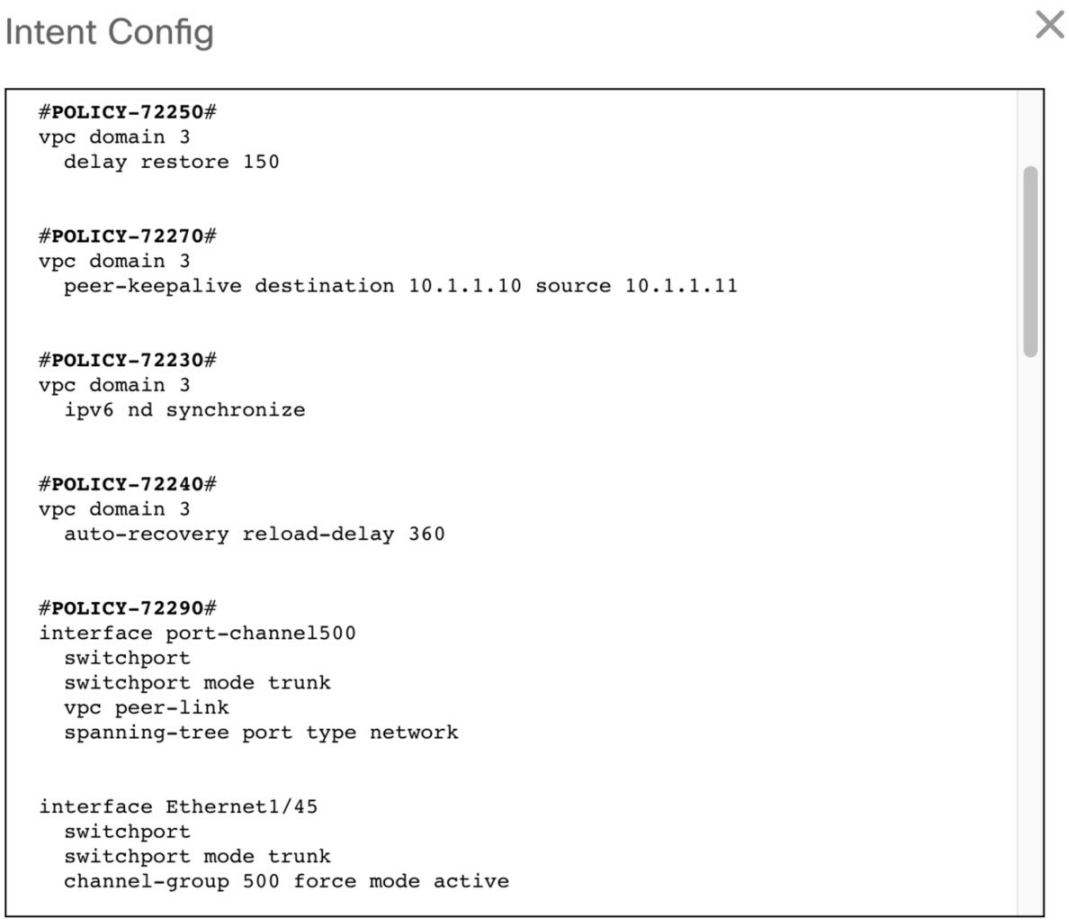
c) [ファブリック トポロジ（Fabric topology）] で、スイッチを右クリックし、ドロップダウンリストから [vPC ペアリング（vPC Pairing）] を選択します。

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) **[保存と展開（Save & 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ます。ポリシーは、次の図に示すように生成されます。



（注） 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。

CC は、インテントと計算結果を比較し、コンプライアンス ステータスを報告するため、デバイスからの実行構成を必要としているので、こうなることが予想されます。

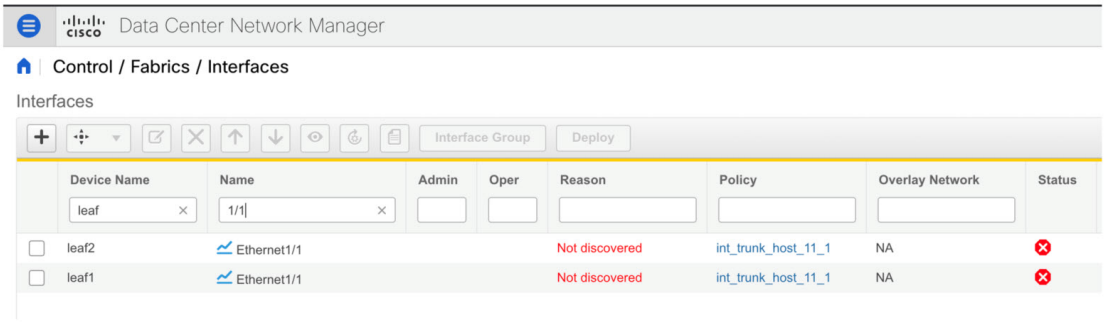
vPC ホスト インターフェイスの事前プロビジョニング

手順

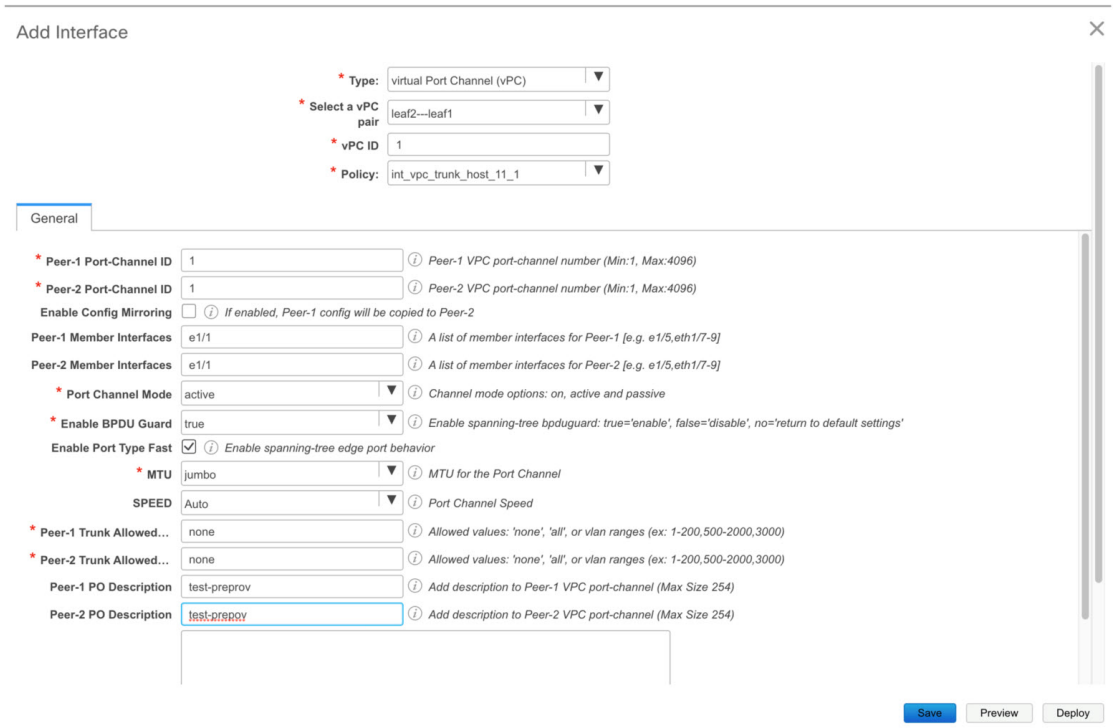
ステップ 1 事前プロビジョニングされたデバイスに物理イーサネットインターフェイスを作成します。通常の vPC ペアまたはスイッチと同様の vPC ホスト インターフェイスを追加します。

手順については、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 （51 ページ）を参照してください。

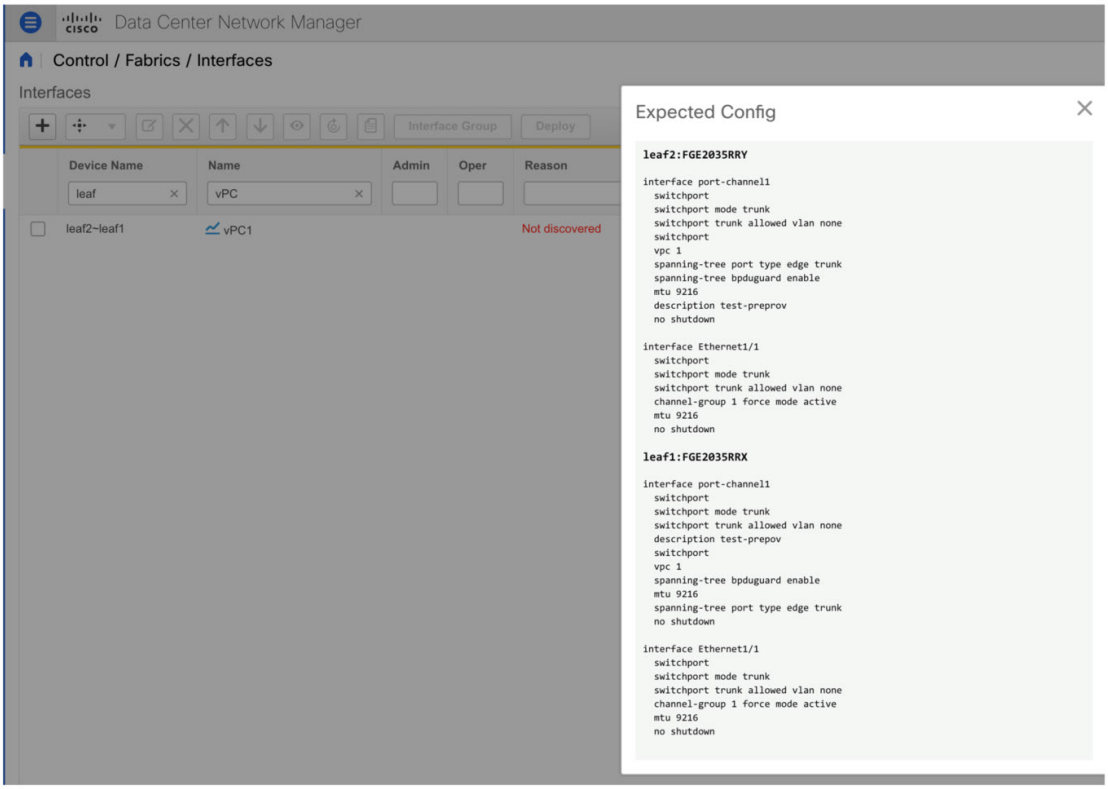
たとえば、leaf1-leaf2 は、事前プロビジョニングされた vPC デバイス ペアを表します。ただし、イーサネット インターフェイス 1/1 は、leaf1 と leaf2 の両方のデバイスで事前プロビジョニングされているものとします。



ステップ 2 次の図に示すように、vPC ホスト トラック インターフェイスを作成します。



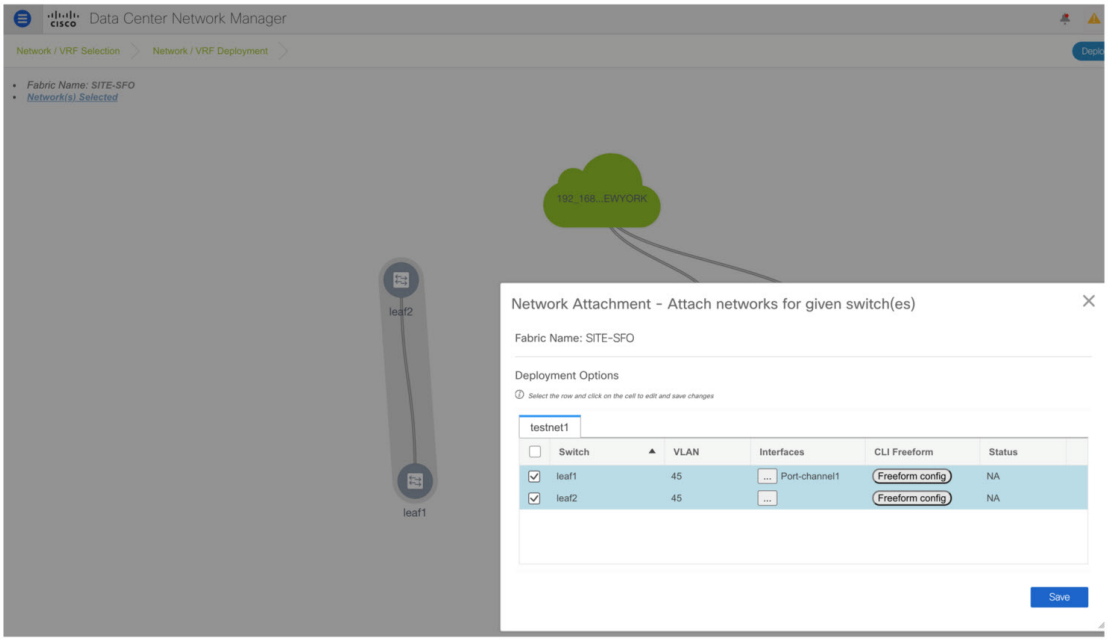
[プレビュー（Preview）] アクションと **[展開（Deploy）]** アクションは、どちらもデバイスが存在する必要があるため、結果を生成しません。vPC ホストインターフェイスが作成され、次のイメージで示すように、ステータスが **[未検出（Not discovered）]** と表示されます。



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

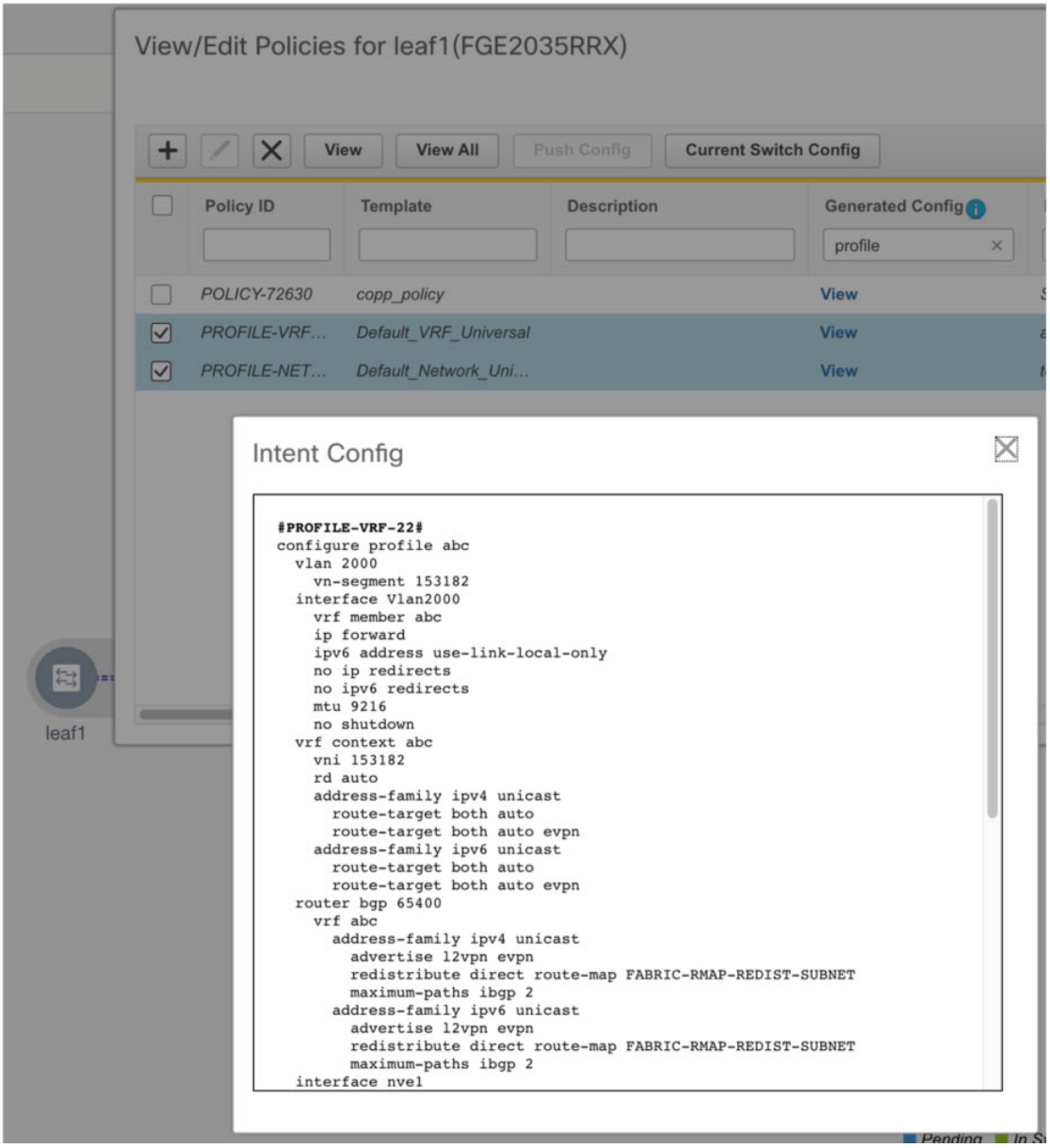
オーバーレイ VRF とネットワークは、他の検出されたデバイスと同様に、事前にプロビジョニングされたデバイスにアタッチできます。

次の例では、オーバーレイ ネットワークが、事前にプロビジョニングされたリーフの vPC ペア（leaf1-leaf2）にアタッチされる様子を示しています。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。

次のイメージに示すように、**[ファブリック ビルダ（Fabric Builder）] > [ポリシーの表示/編集（View/Edit Policies）]** で、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。



Easy ファブリック向け高精度時間プロトコル

Easy_Fabric_11_1 テンプレートのファブリック設定で、**[高精度時間プロトコル（PTP）を有効化（Enable Precision Time Protocol（PTP）]** チェックボックスをオンにして、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。また、**[PTP ループバック ID（PTP Loopback Id）]** および **[PTP ドメイン ID（PTP Domain Id）]** フィールドは編集可能です。

PTP機能は、ファブリック内のすべてのデバイスがクラウド規模のデバイスである場合にのみ機能します。ファブリック内にクラウドスケール以外のデバイスがあり、PTPが有効になっていない場合は、警告が表示されます。クラウドスケールデバイスは、Cisco Nexus 93180YC-EX、

Cisco Nexus 93180YC-FX、Cisco Nexus 93240YC-FX2、および Cisco Nexus 93360YC-FX2 スイッチがあります。

ローカル エリア ネットワーク（LAN）の展開、特に VXLAN EVPN ベースのファブリック展開では、PTP をグローバルに有効にする必要があります。また、コア側のインターフェイスで PTP を有効にする必要があります。インターフェイスは、VM や Linux ベースのマシンのような外部 PTP サーバに対して構成できます。したがって、インターフェイスを編集して、グランドマスター クロックと接続する必要があります。

グランドマスター クロックは Easy ファブリックの外部で構成する必要があり、IP 到達可能です。グランドマスター クロックへのインターフェイスは、[interface freeform config] を使用して PTP で有効にする必要があります。

[保存して展開（Save & Deploy）] をクリックすると、すべてのコア側インターフェイスが PTP 構成で自動的に有効になります。このアクションにより、すべてのデバイスがグランドマスター クロックに確実に PTP 同期されます。さらに、ホスト、ファイアウォール、サービス ノード、またはその他のルータに接続されている境界デバイスやリーフ上のインターフェイスなど、コア側でないインターフェイスについては、ttag 関連の CLI を追加する必要があります。ttag は、VXLAN EVPN ファブリックに入るすべてのトラフィックに追加され、トラフィックがこのファブリックを出るときに ttag を削除する必要があります。

PTP の構成例を次に示します。

```
feature ptp

ptp source 100.100.100.10 -> IP address of the loopback interface (loopback0) that is
already created or user created loopback interface in the fabric settings

ptp domain 1 -> PTP domain ID specified in fabric settings

interface Ethernet1/59 -> Core facing interface
  ptp

interface Ethernet1/50 -> Host facing interface
  ttag
  ttag-strip
```

次のガイドラインは PTP で適用可能です。

- ファブリック内のすべてのスイッチに Cisco NX-OS リリース 7.0(3)I7(1) 以降のバージョンが搭載されている場合、ファブリックで PTP 機能をイネーブルにできます。それ以外の場合、次のエラー メッセージが表示されます。

  すべてのスイッチに NX-OS リリース 7.0(3)I7(1) 以降のバージョンがある場合、PTP 機能をファブリックで有効にできます。このファブリックで PTP を有効にするには、スイッチを NX-OS リリース 7.0(3)I7(1) 以降のバージョンにアップグレードしてください。

- NIR のハードウェア テレメトリ サポートでは、PTP 構成が前提条件です。

- PTP 構成を含む既存のファブリックに非クラウド スケール デバイスを追加すると、次の警告が表示されます。

  すべてのデバイスがクラウド スケール スイッチである場合、TTAG はファブリック全体で有効になるため、新しく追加された非クラウド スケール デバイスでは有効にできません。

- ファブリックにクラウド スケール デバイスと非クラウド スケール デバイスの両方が含まれている場合、PTP を有効にしようとすると、次の警告が表示されます。

  すべてのデバイスがクラウド スケール スイッチであり、非クラウド スケール デバイスが原因で有効になっていない場合、TTAG はファブリック全体で有効になります。

DCNM のスーパー スパイン 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。DCNM リリース 11.3(1) より前は、スーパー スパインを介して複数の VXLAN EVPN Easy ファブリックをインターコネクトできました。ただし、これらのスーパー スパインは外部ファブリックの一部である必要がありました。各 Easy ファブリック内で、適切な IGP がアンダーレイ接続に使用されます。外部ファブリックのスーパー スパイン レイヤーと Easy ファブリックのスパイン レイヤ間の eBGP は、複数の VXLAN EVPN Easy ファブリックをインターコネクトするための推奨される方法です。eBGP ピアリングは、ファブリック間リンク、またはそれぞれのスイッチでのインターフェイスと eBGP 構成の適切な組み合わせを介して構成できます。

DCNM リリース 11.3(1) 以降では、スーパー スパインを使用した追加のインターコネクトのオプションがあります。スーパー スパインを介してインターコネクトされた同じ 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。

DCNM では、次のスーパー スパイン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推奨されていません。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。

DCNM 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_Fabric_11_1]** テンプレートでのみ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 GW スーパー スパインへ

- スーパースパイン、ボーダー スーパー スパイン、ボーダー GW スーパー スパインからボーダーリーフおよびボーダー GW リーフ

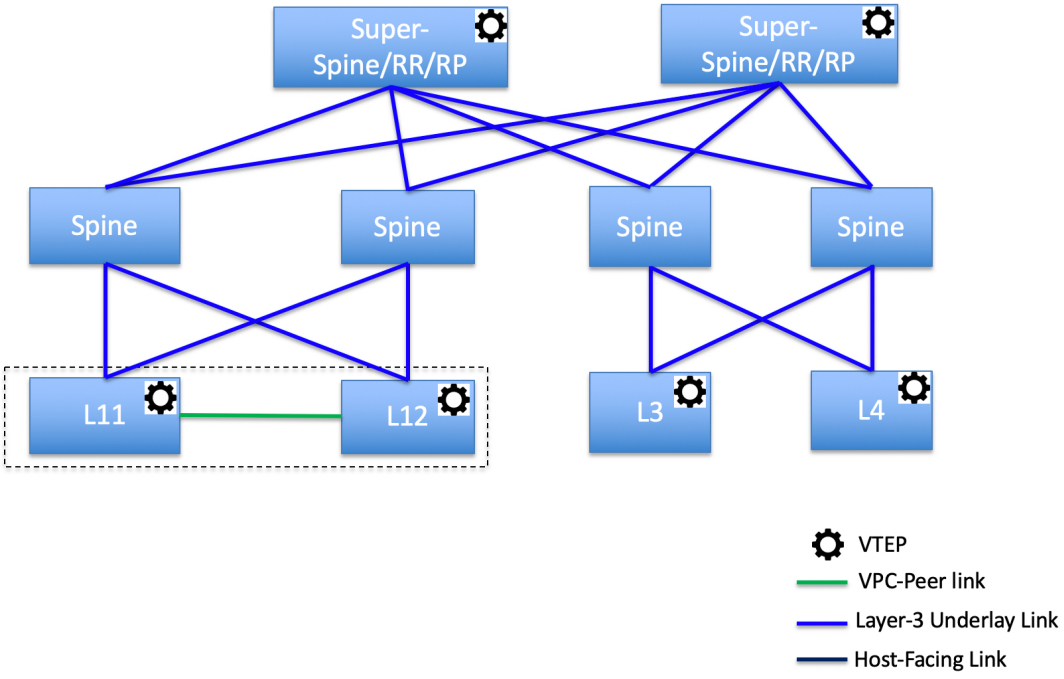
- RR または RP は、ファブリックに存在する場合、常にスーパー スパイン上で構成される必要があります。スーパー スパインでサポートされる RR および RP の数は 4 です。
- ボーダー スーパー スパインおよびボーダー GW スーパー スパインのロールは、ファブリック間接続でサポートされます。
- スーパー スパインでは vPC 構成はサポートされていません。
- スーパー スパインは IPv6 アンダーレイ構成をサポートしていません。
- スイッチにスーパースパイン ロールがある場合、スイッチのブラウンフィールドインポート中に、次のエラーが表示されます。

  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

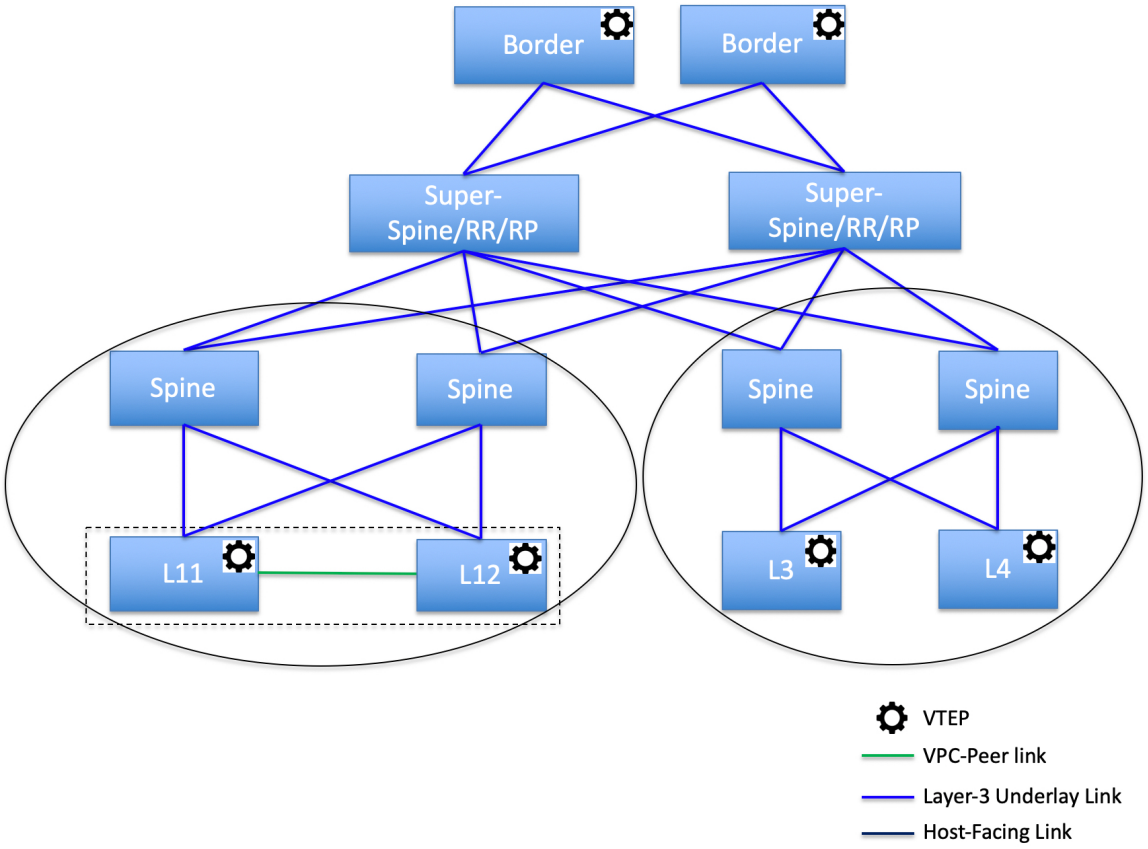
DCNM は、スーパー スパイン スイッチで次のトポロジをサポートします。

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、ボーダーゲートウェイ スーパー スパインです。

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。

スーパー スパイン スイッチを既存の VXLAN BGP EVPN ファブリックへ追加する

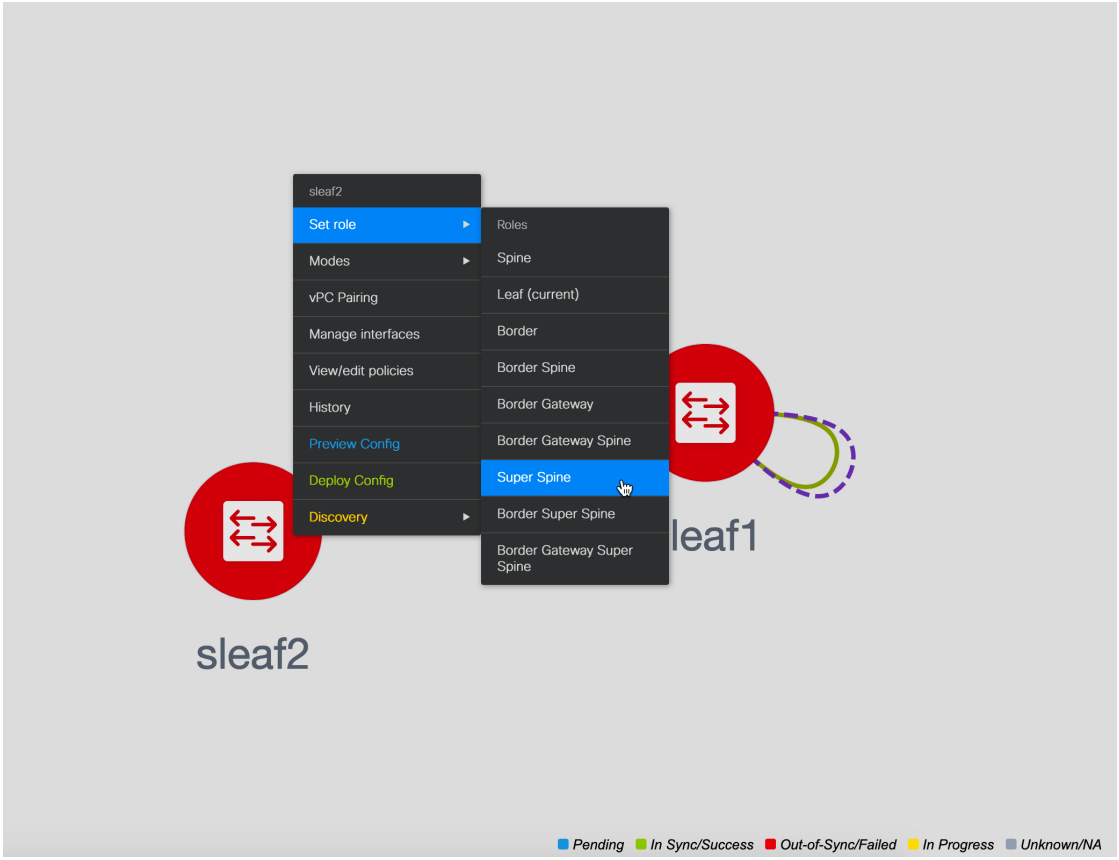
Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** に移動します。

ステップ 2 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウで、アクション パネルの **[スイッチの追加（Add Switches）]** をクリックします。

詳細については、ファブリックへのスイッチの追加, on page 32を参照してください。

ステップ 3 既存のスイッチまたは新しく追加されたスイッチを右クリックし、**[ロールの設定（Set role）]** オプションを使用して適切なスーパー スパイン ロールを設定します。



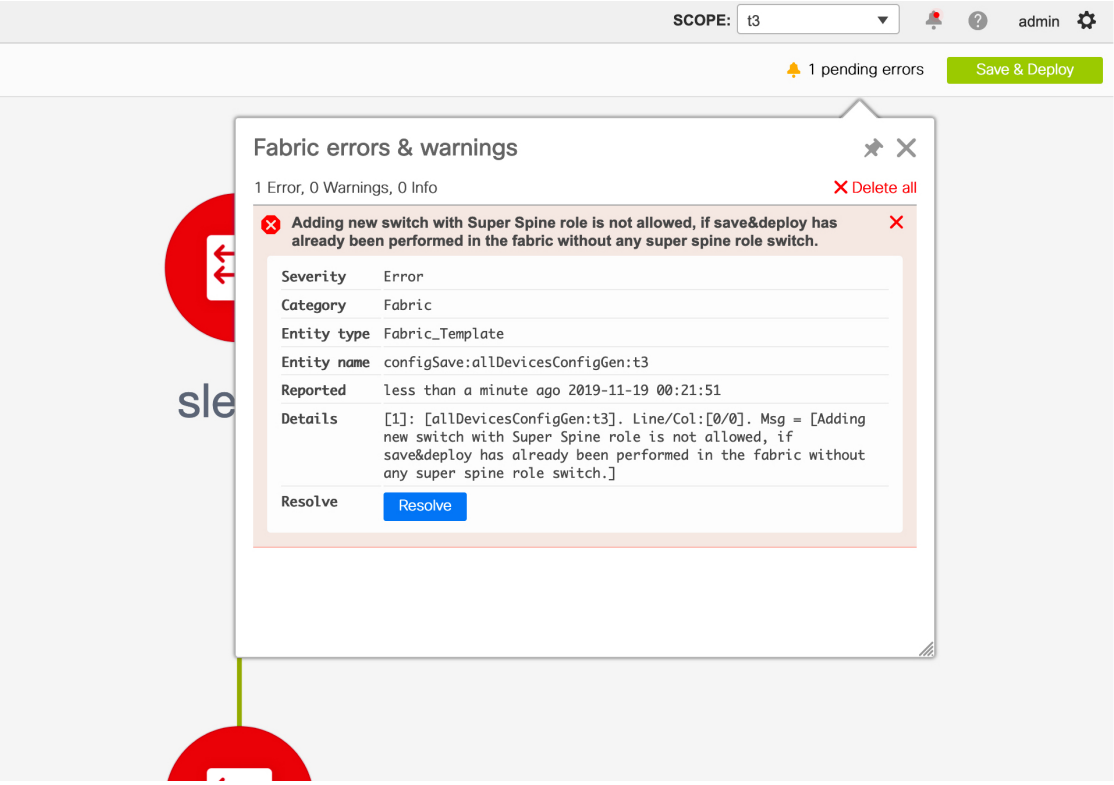
Note **[スーパー スパイン（Super Spine）]** ロールがファブリックに存在する場合、ファブリック内の他の可能なスパイン ロールは、ボーダー スーパー スパインまたはボーダー ゲートウェイ スーパー スパインです。ボーダー スパインまたはボーダー ゲートウェイ スパイン ロール (これらのスイッチ ロールにはスーパーが存在しない) が使用されている場合、[保存してデプロイ] をクリックした後にエラーが生成されます。ボーダー スパインとボーダーゲートウェイ スパインのロールが既存のファブリックにすでに存在する場合は、それらのスイッチを削除して、正しいボーダー スーパー スパインまたはボーダーゲートウェイ スーパー スパインのロールを追加して戻す必要があります。

ステップ 4 [保存して展開（Save & Deploy）] をクリックします。

次のエラーが表示されます。

スーパー スパイン ロールを使用して新しいスイッチを追加することは、スーパー スパイン ロール スイッチなしでファブリックで保存と展開がすでに実行されている場合は許可されません。

ステップ 5 エラーをクリックし、**[解決（Resolve）]** ボタンをクリックします。



続行するかどうかを確認するダイアログ ボックスが表示されます。**[はい（Yes）]** をクリックすると、DCNM によって次のアクションが実行されます。

- 無効な接続はホスト ポートに変換されます。
- スパインからリーフへの既存の BGP ネイバーシップを削除します。
- すべてのスパイン スイッチから RR または RP を削除します。

デバイスでの TCAM 構成の変更

POAP でブートストラップ機能を使用して、X9500 ラインカードを搭載した Cisco Nexus 9300 シリーズ スイッチおよび Cisco Nexus 9500 シリーズ スイッチをオンボーディングしている場合、DCNM はスイッチ モデルに応じて次のポリシーをプッシュします。

- Cisco Nexus 9300 シリーズ スイッチ：**tcam_pre_config_9300** および **tcam_pre_config_vxlan**
- Cisco Nexus 9500 シリーズ スイッチ：**tcam_pre_config_9500** および **tcam_pre_config_vxlan**

DCNM でデバイスの TCAM カービングを変更するには、次の手順を実行します。

1. **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

2. ブートストラップ機能を使用してオンボードされた、指定されたスイッチを含むファブリックをクリックします。
3. **[ファブリック ビルダ（Fabric Builder）]** ウィンドウの **[アクション（Actions）]** メニューの下にある **[表形式ビュー（Tabular View）]** をクリックします。
4. 指定されたすべてのスイッチを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** アイコンをクリックします。
5. **tcam_pre_config** ポリシーを検索します。
6. TCAM構成が正しくないか、適用できない場合は、これらのポリシーをすべて選択し、[削除（Delete）] アイコンをクリックしてポリシーを削除します。
7. 1つまたは複数の tcam_config ポリシーを追加し、正しい TCAM 構成を提供します。ポリシーを追加する方法の詳細については、「複数のスイッチの *PTI* の追加」を参照してください。
8. それぞれのスイッチをリロードします。

スイッチがリーフ、ボーダー リーフ、ボーダーゲートウェイ リーフ、ボーダー スパイン、またはボーダーゲートウェイ スパインとして使用されている場合は、次のコマンドで **tcam_config** ポリシーを追加して展開します。

```
hardware access-list tcam region racl 1024
```

この構成は、NGOAMおよびVXLAN抑制ARP機能を機能させるためにスイッチで必要です。

この tcam_config ポリシーの優先度が **tcam_pre_config_vxlan** ポリシーよりも高く、**racl 1024** の構成ポリシーが **tcam_pre_config_vxlan** ポリシーの前に構成されるようにしてください。

（注） **tcam_pre_config_vxlan** ポリシーには、次の構成が含まれています。**hardware access-list tcam region arp-ether 256 double-wide**

ルート リフレクタおよびランデブー ポイントとしてのスイッチの事前選択

このタスクは、最初の **[保存と展開（Save & Deploy）]** 操作の前に、ルート リフレクタ（RR）およびランデブー ポイント（RP）としてスイッチを事前選択する方法を示しています。

（注） このシナリオは、2つ以上のスパインがあり、最初の保存と展開操作の前に RR と RP の事前選択を制御する場合に適用されます。

手順

ステップ 1 スイッチが正常にインポートされました。

ステップ 2 RR または RP として事前に選択する必要があるスパインまたはスーパー スパイン スイッチで **[ポリシーの表示/編集（View/Edit Policies）]** を使用して、**rr_state** または **rp_state** ポリシーを作成します。

（注）
- 2 つ以上のスパインがあり、ファブリック設定の RR または RP の最大数が 2 に設定されている場合は、RR と RP を異なるスパインに配布することが推奨されています。
- 4 つ以上のスパインがあり、ファブリック設定の RR または RP の最大数が 4 に設定されている場合は、RR と RP を異なるスパインに配布することが推奨されています。

ステップ 3 **[保存と展開（Save & Deploy）]** をクリックし、**[構成の展開（Deploy Config）]** をクリックします。

rr_state ポリシーを持つスパインは RR になり、**rp_state** ポリシーを持つスパインは RP になります。

ステップ 4 **[保存して展開（Save & Deploy）]** した後、事前に選択された RR および RP を新しいデバイスセットに置き換える場合は、同じ手順を実行する前に、古い RR および RP デバイスをファブリックから削除する必要があります。

vPC L3 ピア キープアライブ リンクの追加

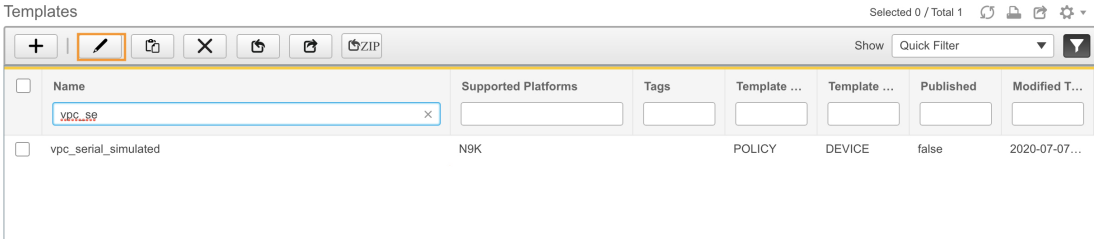
この手順は、vPC L3 ピア キープアライブ リンクを追加する方法を示しています。

（注）
- vPC L3 ピア キープアライブ リンクは、ファブリック vPC ピアリングではサポートされていません。
- ブラウンフィールド移行で、スイッチで L3 キープアライブが構成されている場合は、vPC ペアリングを手動で作成する必要があります。それ以外の場合、vPC 構成はスイッチから自動的に取得されます。

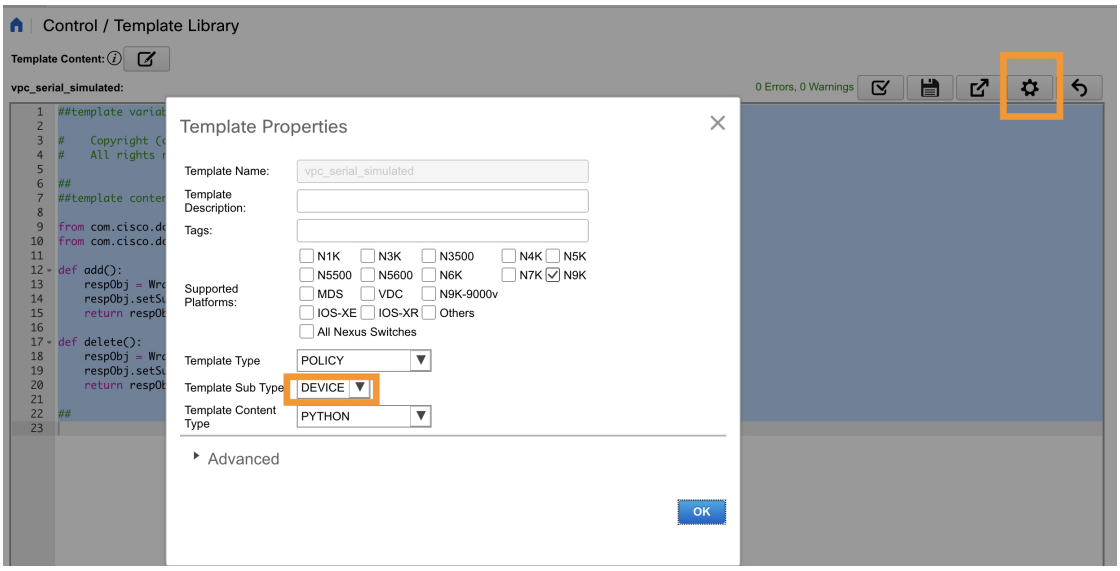
手順

ステップ 1 DCNM から、**[制御（Control）] > [テンプレート ライブラリ（Template Library）]** に移動します。

ステップ 2 **[vpc_serial_simulated]** ポリシーを検索して選択し、**[編集（Edit）]** アイコンをクリックします。



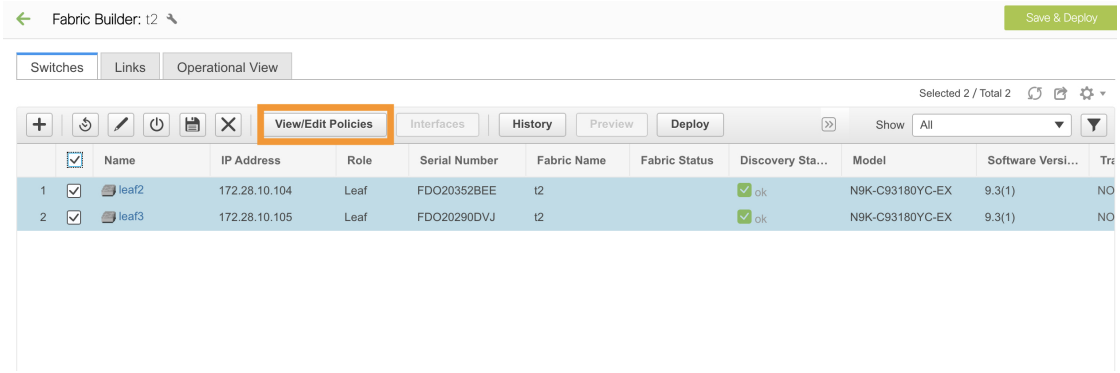
ステップ 3 テンプレート プロパティを編集し、**[テンプレート サブ タイプ（Template Sub Type）]** を **[デバイス（Device）]** に設定して、このポリシーが **[ポリシーの表示/編集（View/Edit Policies）]** に表示されるようにします。



ステップ 4 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウに移動し、vPC ペア スイッチを含むファブリックをクリックします。

ステップ 5 **[表形式ビュー（Tabular View）]** をクリックして vPC ペア スイッチを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** をクリックします。

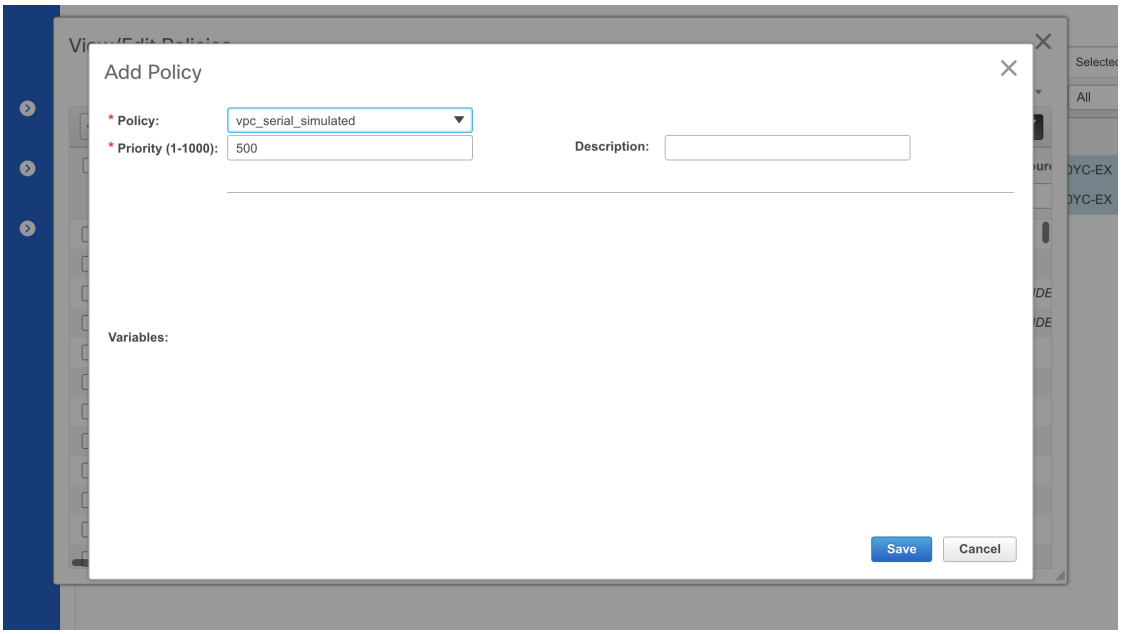
トポロジ内のスイッチを個別に右クリックして、**[ポリシーの表示/編集（View/Edit Policies）]** を選択することもできます。



ステップ 6 **[+]** をクリックしてポリシーを追加します。

ステップ 7 **[ポリシー（Policy）]** ドロップダウン リストから、**[vpc_serial_simulated]** ポリシーを選択し、優先度を追加します。[保存（Save）] をクリックします。

両方のスイッチが選択されている場合、このポリシーは両方の vPC ペア スイッチで作成されることに注意してください。

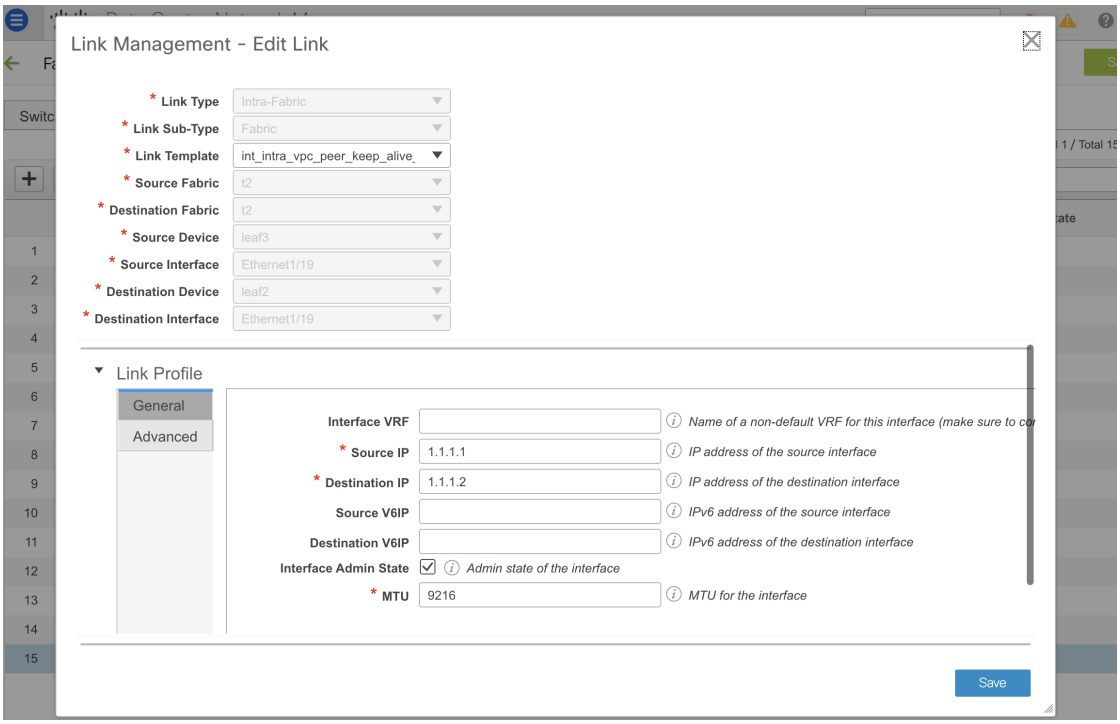


ステップ 8 **[表形式ビュー（Tabular View）]** に戻り、**[リンク（Links）]** タブをクリックします。

ステップ 9 vPC ピア キープ アライブである必要がある vPC ペア間のリンクを選択し、**[編集（Edit）]** をクリックします。

ステップ 10 **[リンク テンプレート（Link Template）]** ドロップダウンリストから、**[int_intra_vpc_peer_keep_alive_link_11_1]** を選択します。

残りのフィールドの値を入力します。デフォルト VRF のフィールドを空のままにして、**[保存（Save）]** をクリックします。

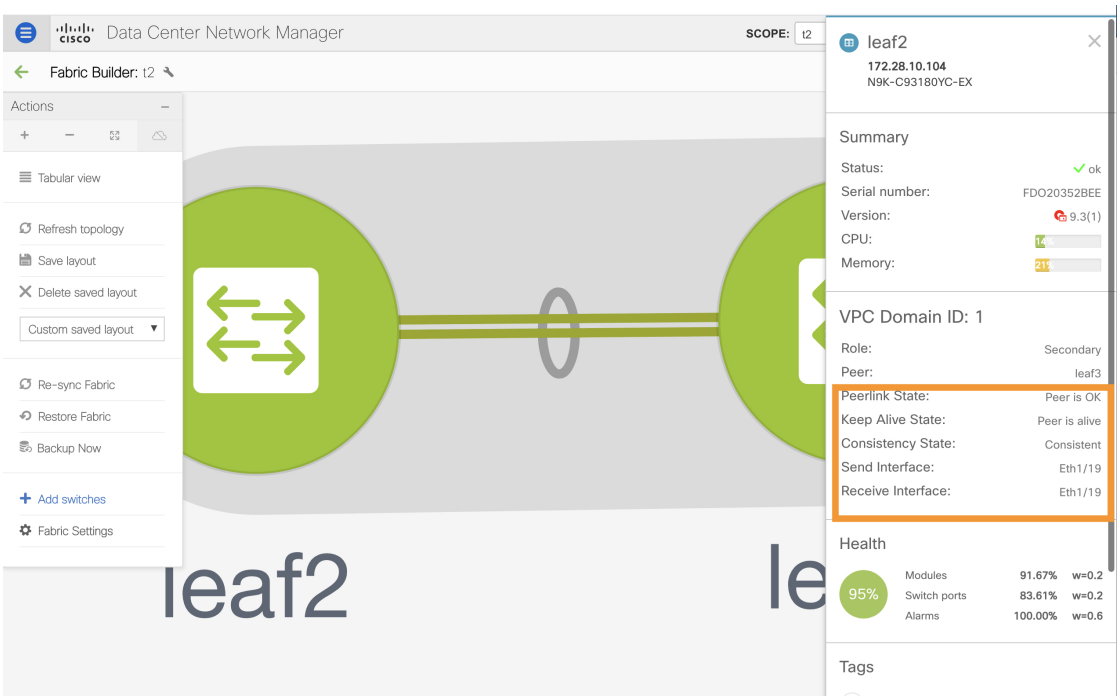


ステップ 11 **[保存と展開（Save & Deploy）]** をクリックし、いずれかのスイッチの **[構成のプレビュー（Preview Config）]** をクリックします。

```
vpc domain 1
  ip arp synchronize
  peer-gateway
  peer-switch
  delay restore 150
  peer-keepalive destination 1.1.1.1 source 1.1.1.2 vrf default
  auto-recovery reload-delay 360
  ipv6 nd synchronize
interface port-channel500
```

VRF がデフォルト以外の場合は、**switch_freeform** を使用してそれぞれの VRF を作成します。

トポロジに移動し、vPC ペア スイッチをクリックして詳細を表示します。

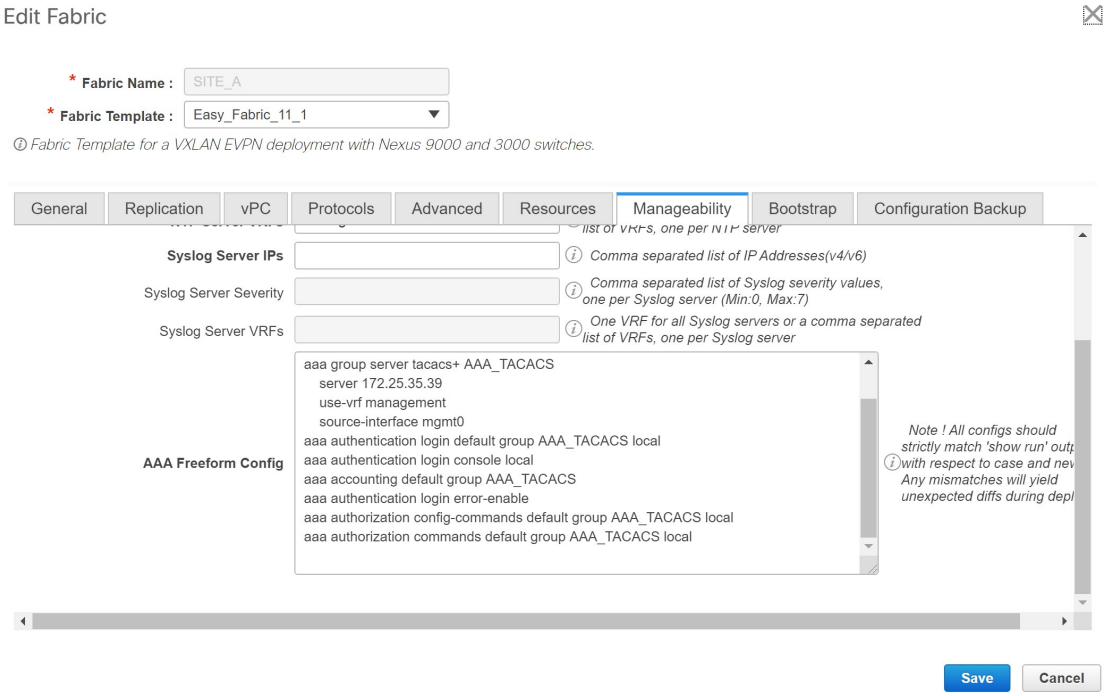


ファブリック内スイッチ向けのローカル認証を AAA 認証へ変更する

手順

ステップ 1 DCNM にログインし、**[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** に移動します。

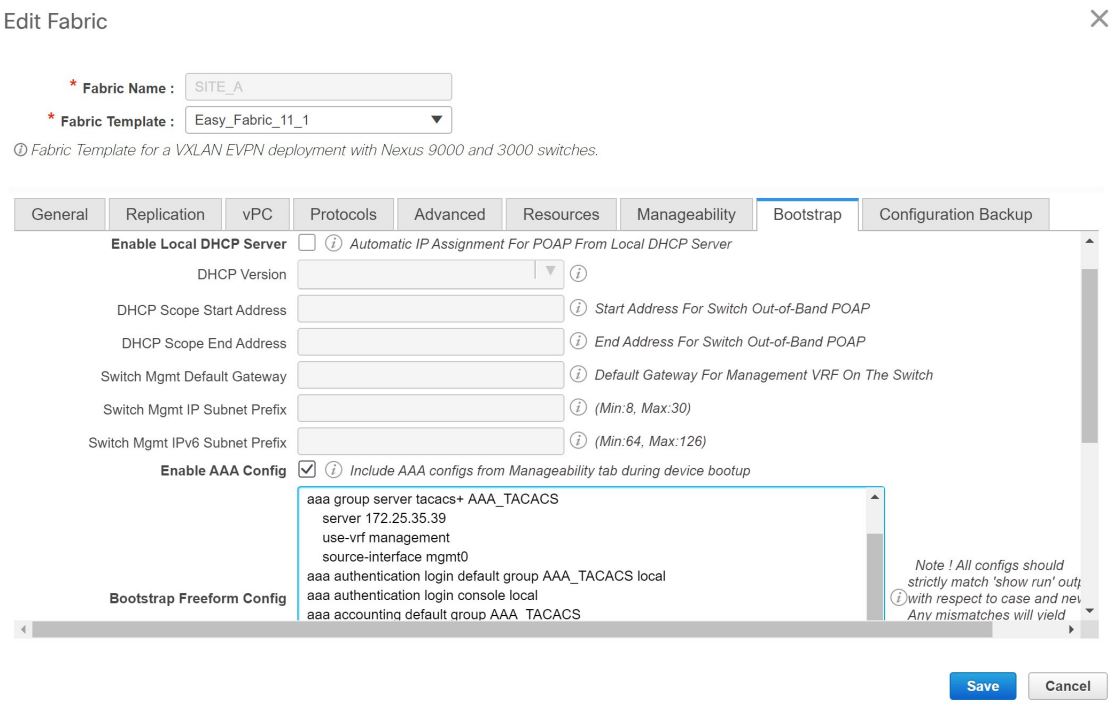
ステップ 2 ファブリックの **[編集（Edit）]** アイコンをクリックし、**[管理性（Manageability）]** タブの **[AAA 自由形式構成（AAA Freeform Config）]** フィールドに AAA 認証コマンドを追加します。



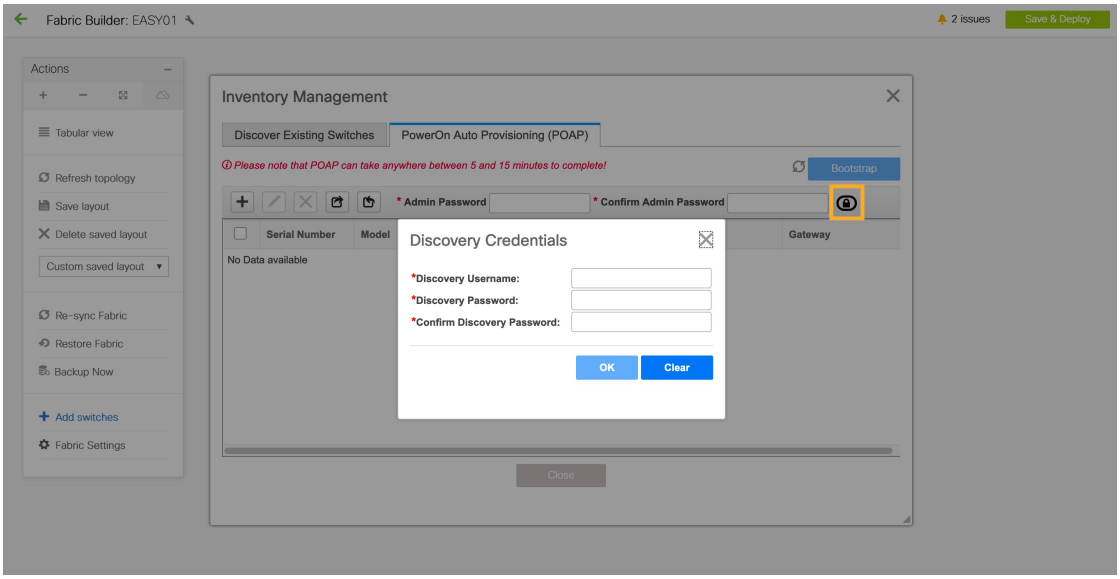
ステップ 3 **[ファブリック ビルダ（Fabric Builder）]** トポロジ ウィンドウで、**[スイッチの追加（Add Switches）]** をクリックします。このウィンドウの AAA ログイン情報を使用して、スイッチを DCNM に追加します。

ステップ 4 POAP 経由でスイッチをファブリックにインポートする場合は、スイッチに AAA 構成が必要です。

ファブリック設定に移動し、関連するコマンドを **[ブートストラップ自由形式構成（Bootstrap Freeform Config）]** に追加します。



ステップ 5 **[ファブリック ビルダ（Fabric Builder）]** トポロジ ウィンドウで、**[スイッチの追加（Add Switches）]** をクリックします。**[PowerON 自動プロビジョニング（POAP）（PowerON Auto Provisioning (POAP)）]** タブで、**[検出されるログイン情報の追加（Add discovery credentials）]** アイコンをクリックし、検出されるログイン情報を入力します。



スイッチの追加が完了したら、**[保存と展開（Save & Deploy）]** をクリックします。

Easy Fabric の IPv6 アンダーレイ サポート

Cisco DCNM リリース 11.3(1) から、IPv6 のみのアンダーレイで Easy fabric を作成できます。IPv6 アンダーレイは、**Easy_Fabric_11_1** テンプレートでのみサポートされています。詳細については、「*IPv6*アンダーレイを使用した*VXLAN*ファブリックの構成」を参照してください。

ブラウンフィールド展開：VXLAN ファブリック管理から DCNMへの移行

DCNM では、VXLAN BGP EVPN ファブリック管理を DCNM に移行するブラウンフィールド展開をサポートしています。移行には、既存のネットワーク構成の DCNM への移行が含まれます。詳細については、「ブラウンフィールド *VXLAN BGP EVPN* ファブリックの管理」を参照してください。

eBGP アンダーレイを使用したファブリックの構成

Easy_Fabric_eBGP ファブリック テンプレートを使用して、eBGP アンダーレイを使用するファブリックを作成できます。詳細については、「BGP ベースのルーテッド ファブリックの管理」および「グリーンフィールド VXLAN BGP EVPN ファブリックの管理」を参照してください。

外部ファブリックの作成

DCNM 11.1(1) リリースで、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：

- 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。DCNMは、Cisco IOS-XR ファミリ デバイスのモニタ モードのみをサポートします。
- 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MSDファブリックメンバーである場合、MSD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、非 DCNM 管理対象スイッチへの接続はすべて、**[未検出（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：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：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。
- Cisco DCNM リリース 11.4(1) 以降、非 Nexus デバイスをボーダーとして構成できます。外部ファブリックの非Nexusデバイスと簡易ファブリックの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 DCNM リリース 11.4(1) 以降、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構成し、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、入力したパスワードは5 $ 5 $ I4sapkBh $ S7B7UcPH / iVTihLKH5sgldBeS3O2X1StQsvv3cmbYd1です。

- 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コマンドは必須設定の1つです。

  シスコは、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、**lldp** 機能をスイッチにプッシュします。

  したがって、NIRユーザは、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（DCNM 11.4(1) 以降で該当）

ファブリック ビルダからの外部ファブリックの作成

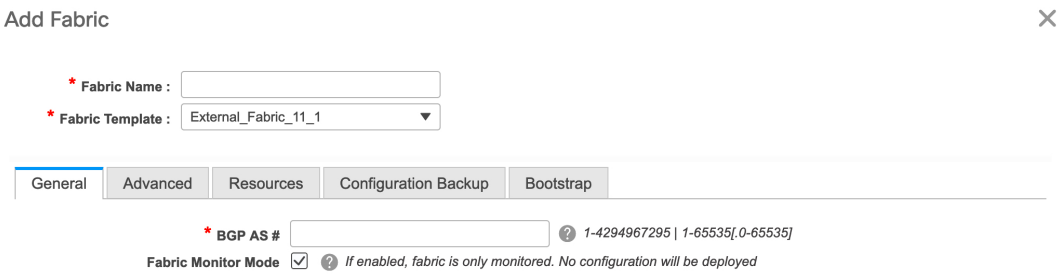
次の手順に従って、ファブリック ビルダから外部ファブリックを作成します。

1. **[制御（Control）] > [Fabric Builder]**の順にクリックします。[ファブリック ビルダ（Fabric Builder）] ページが表示されます。
2. **[ファブリックの作成（Create Fabric）]** ボタンをクリックします。[ファブリックの追加（Add Fabric）] 画面が表示されます。この画面のフィールドは次のとおりです。

   [ファブリック名（Fabric Name）]：外部ファブリックの名前を入力します。

   [ファブリック テンプレート（Fabric Template）]：*External_Fabric* を選択します。

   ファブリックテンプレートを選択すると、外部ファブリックを作成するファブリック作成画面が表示されます。
3. 次に示すように、**[全般（General）]** タブに入力します。



[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）]：DCNM でファブリックを管理する場合は、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。DCNM は、Cisco IOS-XR ファミリ デバイスのモニタ モードのみをサポートします。

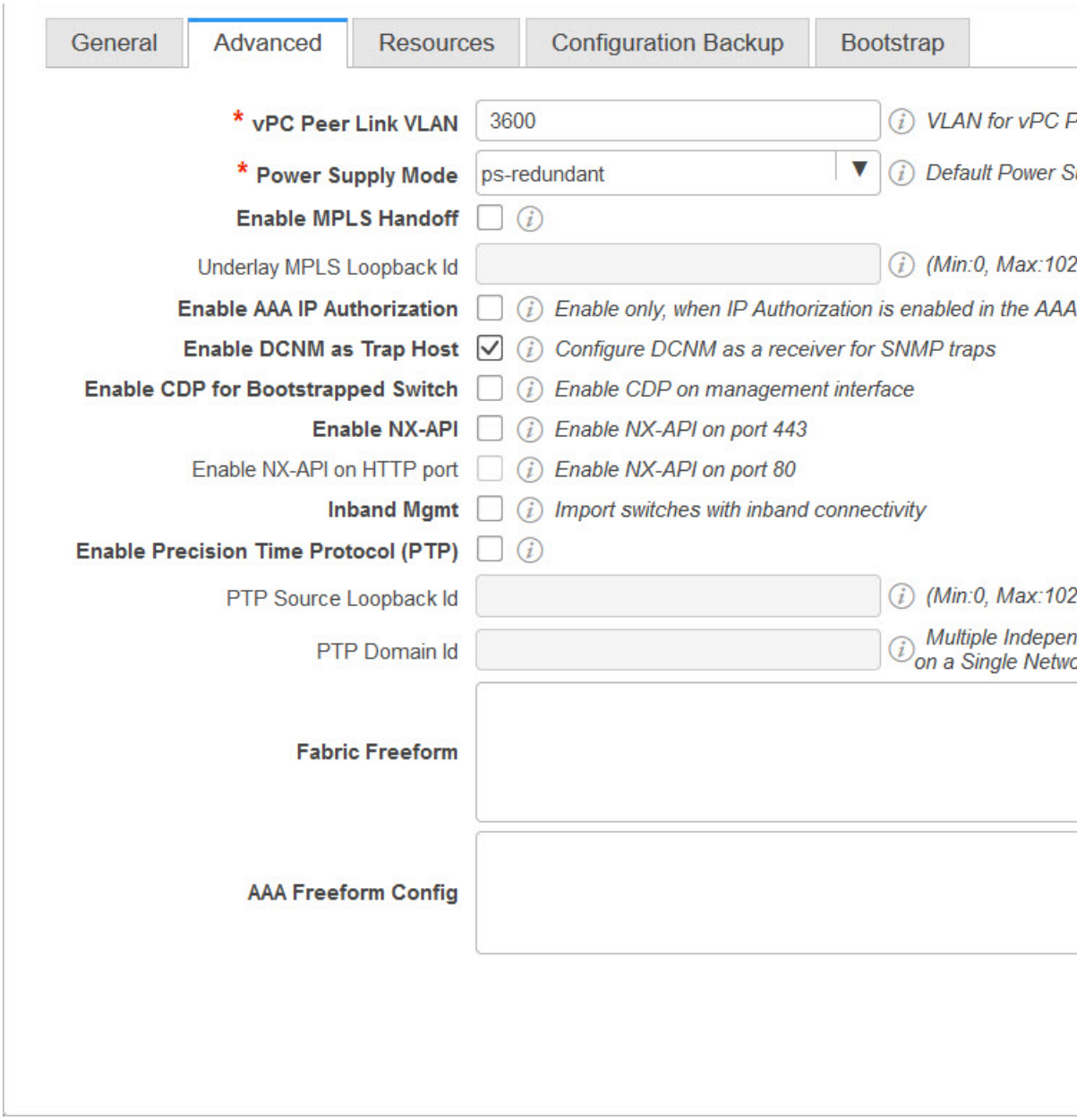
VXLANファブリックからこの外部ファブリックへのファブリック間接続を作成すると、BGP AS番号が外部またはネイバーファブリックAS番号として参照されます。

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。ファブリック トポロジ画面で **[保存して展開（Save & Deploy）]** 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。

ただし、次の設定（スイッチ アイコンを右クリックすると使用可能）が許可されます。

4. [詳細（Advanced）]タブのフィールドに値を入力します。



[vPC ピア リンク VLAN（vPC Peer Link VLAN）]：vPC ピア リンク VLAN ID は自動入力されます。正しい値を反映させてフィールドをアップデートします。

[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、「VXLAN BGP EVPN ファブリックでの境界プロビジョニングの使用例：MPLS SR および LDP ハンドオフ」の章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 認証が有効になっている場合に、AAA IP 認証を有効にします。

[トラップ ホストとして有効にする（Enable as Trap Host）]：トラップ ホストとして有効にする場合は、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（L4 ー L7 サービス）、VXLAN OAM など、NX-API を使用し、Cisco DCNM がサポートするアプリケーションは、HTTP ではなく HTTPS の使用を開始します。

Note [NX-API の有効化（Enable NX-API）] チェックボックスと [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 DCNM は、インバンド接続（スイッチ ループバック、ルーテッド、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、インバンド管理型スイッチの場合、eth2（別名インバンド インターフェイス）を介して DCNM からスイッチ IP に到達可能であることです。この目的のために、DCNM で静的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）]オプションで構成できます。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。DCNM は、インバンド管理されたスイッチ IP が eth2 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すると、DCNM 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 DCNM に入力される目的の基準設定にキャプチャされます。詳細については、外部ファブリックおよびLANクラシック ファブリックでのインバンド管理, on page 165を参照してください。

Note 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。DCNM 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。DCNM 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オンにすると、PTP がグローバルに有効になり、コアに面するインターフェイスで有効になります。また、[PTP 送信元ループバック ID（PTP Source Loopback Id）] および [PTP ドメイン ID（PTP Domain Id）] フィールドが編集可能になります。詳細については、外部ファブリックおよび LAN クラシック ファブリック向け高精度時間プロトコル（PTP）, on page 166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、DCNM から BGP ループバックまたは作成元の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。PTPループバックIDが保存と展開中に見つからない場合、次のエラーが生成されます。PTP送信元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。

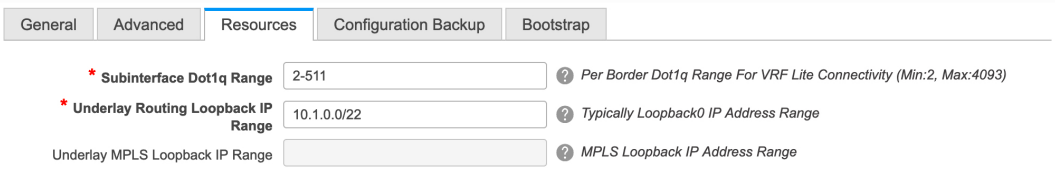
[PTP ドメイン ID（PTP Domain Id）]：単一のネットワーク上の PTP ドメイン ID を指定します。有効な値の範囲は 0 ～ 127 です。

[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。

5. 次に示すように、[リソース（Resources）]タブに入力します。



[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 ルーティング ループバック IP 範囲（Underlay Routing Loopback IP Range）]：プロトコル ピアリングのループバック IP アドレスを指定します。

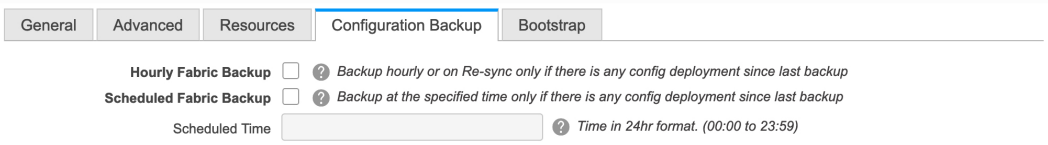
[アンダーレイ MPLS ループバック IP 範囲（Underlay MPLS Loopback IP Range）]：アンダーレイ MPLS SR または LDP ループバック IP アドレス範囲を指定します。

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。

[AAA IP 認証の有効化（Enable AAA IP Authorization）]：AAA サーバーで IP 認証が有効になっている場合に、AAA IP 認証を有効にします。

[トラップ ホストとして有効にする（Enable as Trap Host）]：トラップ ホストとして有効にする場合は、このチェックボックスをオンにします。

6. 次に示すように、[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、DCNM 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 ファブリックと比較して、スイッチの構成全体が DCNM 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、DCNM 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。

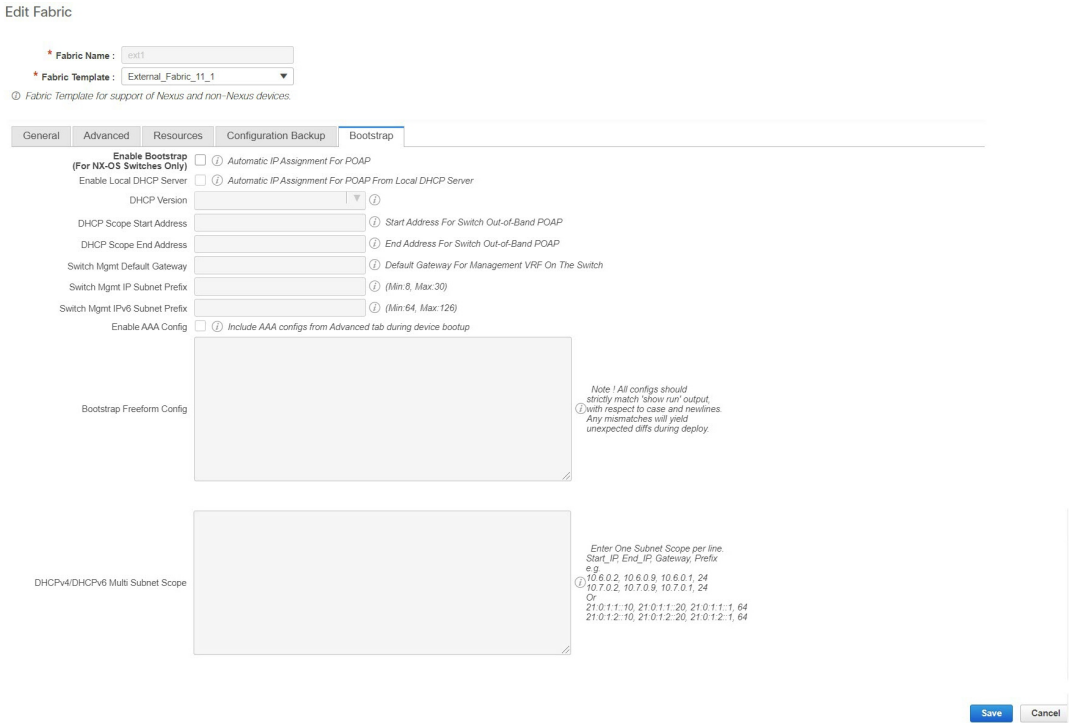
スケジュールされたバックアップは、指定した時刻に最大 2 分の遅延でトリガーされます。スケジュールされたバックアップは、構成の展開ステータスに関係なくトリガーされます。

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。

毎時バックアップとスケジュール済みバックアップのポインタ：

- バックアップには、実行構成と DCNM によってプッシュされたインテントが含まれます。構成コンプライアンスは、実行構成が DCNM 構成と同じになるようにします。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 DCNM によってトラック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、スイッチからの DCNM インテントと実行構成の両方がキャプチャされます。

7. **[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）]：このチェックボックスを選択し、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 サーバー（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）]** 外部 DHCP サーバーに関する情報を入力します。
- ローカル DHCPサーバ（Local DHCP Server）：[ローカル DHCP サーバ（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。

ローカル DHCP サーバーの有効化（Enable Local DHCP Server）：ローカル DHCP サーバーを介した自動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）]** フィールドが無効になります。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。

Note Cisco DCNM 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 が必須）、またはスイッチがいくつかの IPv6 /64 サブネット内に存在する L3 隣接である場合にのみ、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、DCNM 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。プレフィックスは 8 ～ 30 の間である必要があります。

DHCP スコープ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 スコープ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 ー 126 の範囲で指定する必要があります。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。

Bootstrap Freeform Config ：（オプション）必要に応じて他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、[Bootstrap Freeform Config]フィールドで定義されたインテントが含まれます。

NX-OSスイッチの実行コンフィギュレーションに示されているように、running-configを正しいインデントで自由形式の設定フィールドに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、スイッチのフリーフォーム設定エラーの解決, on page 353を参照してください。

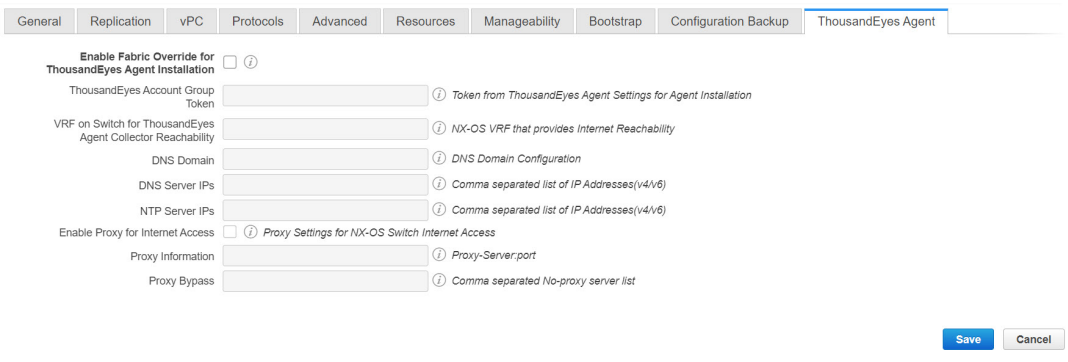
[DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）]：1 行に 1 つのサブネット スコープを入力して、フィールドを指定します。**[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）]**チェックボックスをオンにした後で、このフィールドは編集可能になります。

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

8. **[ThousandEyes Agent]** タブをクリックします。この機能は、Cisco DCNM リリース 11.5(3) でのみサポートされています。詳細については、「Cisco DCNM での ThousandEyes Enterprise Agent のグローバル設定の構成」を参照してください。



このタブのフィールドは次のとおりです。

Note ThousandEyes Agent のファブリック設定はグローバル設定を上書きし、そのファブリック内のスイッチにインストールされているすべての ThousandEyes エージェントに同じ構成を適用します。

- **[ThousandEyes Agent インストールのファブリック オーバーライドを有効にする（Enable Fabric Override for ThousandEyes Agent Installation）]** : チェック ボックスを選択して、ファブリックで ThousandEyes Enterprise Agent を有効にします。
- **[ThousandEyes アカウント グループ トークン（ThousandEyes Account Group Token）]** : インストール用の ThousandEyes Enterprise Agent アカウント グループ トークンを指定します。
- **[ThousandEyes Agent コレクタ到達可能性のスイッチ上の VRF（VRF on Switch for ThousandEyes Agent Collector Reachability）]** : インターネットの到達可能性を提供する VRF データを指定します。
- **[ドメイン ネーム システム（DNS） ドメイン（DNS Domain）]** : スイッチのドメイン ネーム システム（DNS） ドメイン構成を指定します。
- **[ドメイン ネーム システム（DNS） サーバ IP（DNS Server IPs）]** : ドメイン ネーム システム（DNS） サーバの IP アドレス（v4/v6）のカンマ区切りリストを指定します。DNS サーバには、最大 3 つの IP アドレスを入力できます。
- **[NTP サーバ IP（NTP Server IPs）]** : Network Time Protocol (NTP) サーバの IP アドレス（v4/v6）のコンマ区切りリストを指定します。NTP サーバには、最大 3 つの IP アドレスを入力できます。
- **[プロキシを有効にする（Enable Proxy）]** : チェックボックスをオンにして、NX-OS スイッチのインターネット アクセスのプロキシ設定を選択します。
- **[プロキシ情報（Proxy Information）]**: プロキシサーバーのポート情報を指定します。
- **[プロキシ バイパス（Proxy Bypass）]** : プロキシをバイパスするサーバー リストを指定します。

9. **[Save（保存）]** 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

1. [スイッチの追加（Add Switches）] をクリックします。インベントリ管理画面が表示されます。

   [表形式ビュー（Tabular View）] > [スイッチ（Switches）] > [+] をクリックして、スイッチを追加することもできます。

2. スイッチの IP アドレス（シード IP）を入力します。
3. **[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**です。

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

   該当するオプション ボタンをクリックします。Cisco CSR 1000v の追加の詳細については、「*Cisco* データセンターとパブリッククラウドの接続」の章を参照してください。

   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。
4. 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。
5. 画面の下部にある [検出の開始（Start discovery）] 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。
6. 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、[ファブリックにインポート（Import 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 DCNM 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。DCNM がスイッチを検出すると、画面が閉じ、ファブリック画面が再び表示されます。ファブリック画面の中央にスイッチ アイコンが表示されます。
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. 外部ファブリック スイッチの設定：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。スイッチアイコンを右クリックして、スイッチ オプションを設定または更新します。

   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。許可されるロールは、エッジ ルータとコア ルータです。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。

Note スイッチのロールの変更は、[保存と展開（Save & Deploy）] を実行する前にのみ許可されます。

モード：アクティブ/動作モード。

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。

[インターフェイスの管理（Manage Interfaces）]：スイッチインターフェイスに設定を展開します。

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（History）]：スイッチごとの導入履歴を表示します。

[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。

[展開設定（Deploy Config）]：スイッチ設定ごとに展開します。

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。

9. 画面の右上にある [保存と展開（Save & 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。

[保存と展開（Save & Deploy）] をクリックすると、[構成展開（Configuration Deployment）] 画面が表示されます。

10. 画面の下部にある [構成の展開（Deploy 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。

11. 展開が完了したら、画面を閉じます。

Note 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必要があります。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、DCNM 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。

MSDファブリックの下で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、MSDファブリックページに移動する必要があります。

1. [制御（Control）] > [ファブリック ビルダ（Fabric Builder）] をクリックして、ファブリック ビルダ画面に移動します。
2. MSD-Parent-Fabric ボックス内をクリックして、トポロジ画面に移動します。
3. トポロジ画面で、[アクション（Actions）] パネルに移動し、[ファブリックの移動（Move Fabrics）] をクリックします。

   [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。
4. 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[Scope]ドロップダウンボックスで、MSD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。
5. 画面の左上にある [←] をクリックして、ファブリック ビルダ画面に移動します。MSD ファブリック ボックスの [メンバー ファブリック（Member Fabrics）] フィールドに、外部ファブリックが表示されます。

MSDファブリックトポロジでの外部ファブリックの説明

MSDトポロジ画面には、MSD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、MSDトポロジの一部として表示されます。

Note 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（MSDトポロジビュー）に、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 スイッチの操作

外部ファブリック トポロジ画面で、画面の左側にある [Actions（アクション）] パネルの [表形式ビュー（Tabular view）] オプションをクリックします。[スイッチ | リンク（Switches | Links）] 画面が表示されます。

[スイッチ（Switches）] タブはスイッチ操作を管理するためのもので、[リンク（Links）] タブはファブリック リンクを表示するためのものです。各行は外部ファブリック内のスイッチを表し、シリアル番号を含むスイッチの詳細が表示されます。

表の上部にあるボタンについて、左から右に説明します。一部のオプションは、スイッチアイコンを右クリックしても使用できます。ただし、[スイッチ（Switches）] タブでは、ポリシーの追加や展開など、複数のスイッチの構成を同時にプロビジョニングできます。

- ファブリックにスイッチを追加します。このオプションは、トポロジ ページ（[アクション（Actions）] パネルの [スイッチの追加（Add switches）] オプション）でも使用できます。
- スイッチ検出プロセスを DCNM afresh により開始します。
- 認証プロトコル、ユーザー名、パスワードなどのデバイス ログイン情報を更新します。
- スイッチをリロードします。
- ファブリックからスイッチを削除します。
- ポリシーの表示/編集：複数のスイッチで同時に、ポリシーを追加、更新、および削除します。ポリシーはテンプレート ライブラリで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。

Note 複数のスイッチを選択してポリシー インスタンスを展開する場合、選択したすべてのスイッチに展開されます。

- [インターフェイスの管理（Manage Interfaces）]：スイッチ インターフェイスに設定を展開します。
- 履歴：選択されたスイッチで展開履歴を表示します。
- 展開：スイッチ構成を展開します。

外部ファブリック リンク

外部ファブリック リンクの表示と削除のみが可能です。リンクの作成や編集はできません。

外部ファブリックのリンクを削除するには、次の手順を実行します。

1. トポロジ画面に移動し、画面の左側にある [アクション（Actions）] パネルの [表形式ビュー（Tabular view）] オプションをクリックします。

   [スイッチ | リンク（Switches | Links）] 画面が表示されます。

2. 1 つ以上のチェックボックスをオンにして、左上の [削除（Delete）] アイコンをクリックします。

   リンクは削除されます。

ネイバー スイッチを外部ファブリックに移動

1. [スイッチの追加（Add Switches）] をクリックします。インベントリ管理画面が表示されます。
2. [ネイバー スイッチの移動（Move Neighbor Switches）] タブをクリックします。
3. スイッチを選択し、**[ネイバーの移動（Move Neighbor）]** をクリックします。

   ネイバーを削除するには、スイッチを選択して **[ネイバーの削除（Delete Neighbor）]** をクリックします。

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。

Procedure

ステップ 1 DCNM 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。

ステップ 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。

ステップ 3 DCNM UI で、**[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

[ファブリック ビルダ（Fabric Builder）] 画面が表示されます。これには、長方形のボックスが各ファブリックを表すファブリックのリストが含まれています。

ステップ 4 ファブリック ボックスの右上にある **[ファブリックの編集（Edit Fabric）]** アイコンをクリックします。

[ファブリックの編集（Edit Fabric）] 画面が表示されます。

ステップ 5 **[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。

ステップ 6 [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。

ステップ 7 [ファブリック ビルダ（Fabric Builder）]画面で、ファブリック ボックス内をクリックします。

[ファブリック トポロジ（fabric topology）] 画面が表示されます。

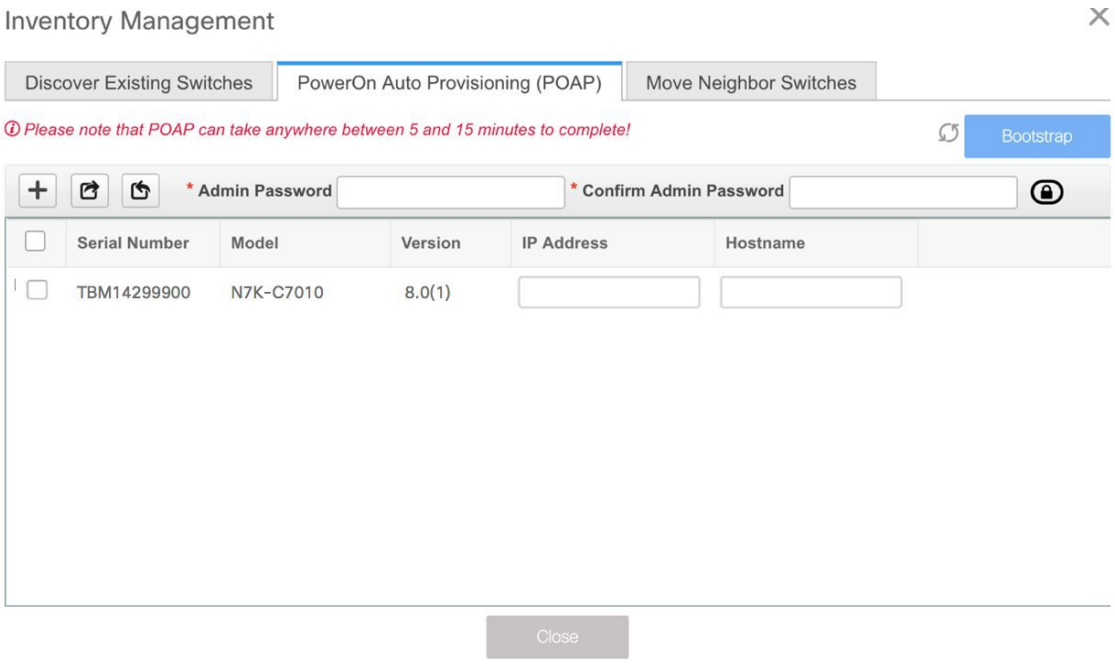
ステップ 8 ファブリック トポロジ画面で、画面の左側にある [アクション（Actions）] パネルから、**[スイッチの追加（Add switches）]** をクリックします。

インベントリ管理画面が表示されます。

ステップ 9 **[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、DCNM 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。

Note 画面の左上には、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するためのエクスポートおよびインポートオプションがあります。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。

リリース 11.2(1) 以降、事前にプロビジョニングデバイスが可能です。デバイスの事前プロビジョニングについては、デバイスの事前プロビジョニング , on page 46 を参照してください。

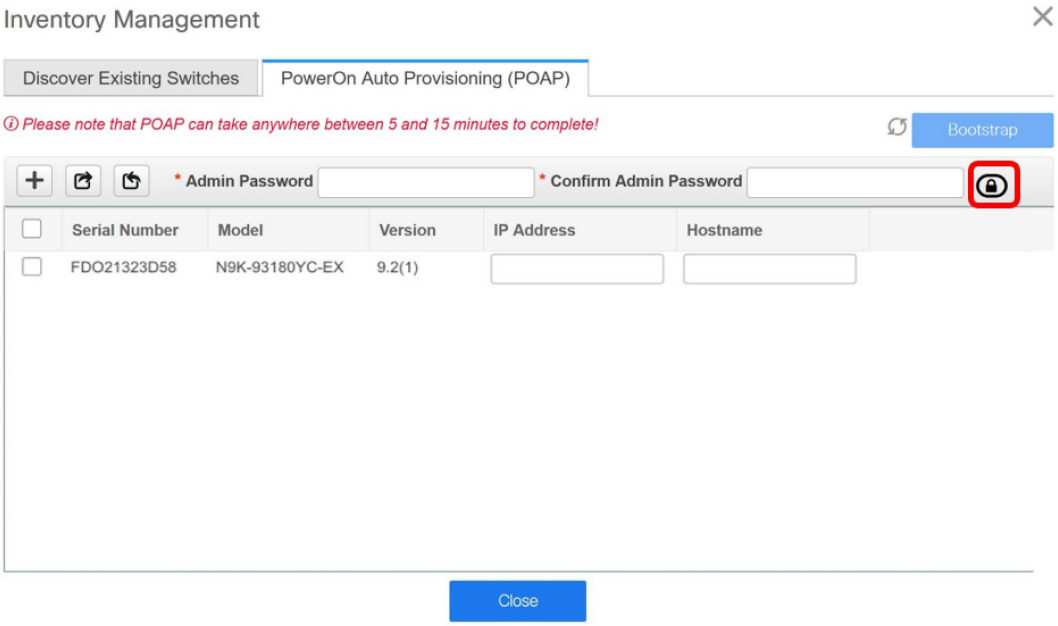
ステップ 10 **[管理者パスワード（Admin Password）]** フィールドと **[管理者パスワードの確認（Confirm Admin Password）]** フィールドに、新しいパスワードを入力します。

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。

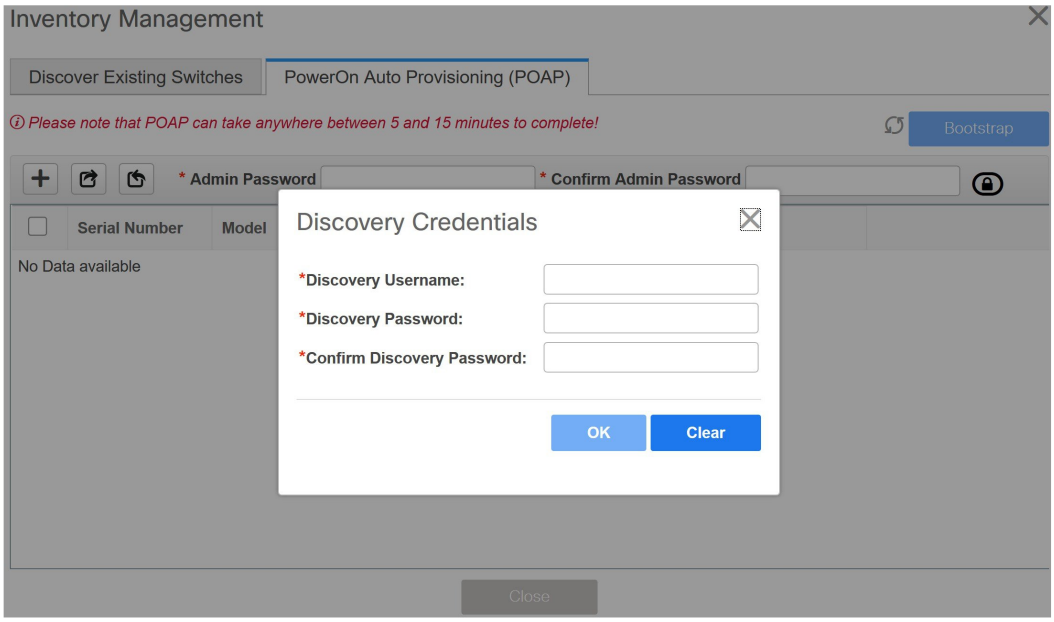
Note 管理者クレデンシャルを使用してスイッチを検出しない場合は、代わりに AAA 認証（RADIUS または TACACS クレデンシャル）を使用できます。

ステップ 11 (Optional) 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 クレデンシャルの追加（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 クレデンシャルを入力します。



b) **[ディスカバリ クレデンシャル（Discovery Credentials）]** ウィンドウで、ディスカバリ ユーザ名やパスワードなどのディスカバリ クレデンシャルを入力します。



[OK] をクリックして、ディスカバリ クレデンシャルを保存します。

検出クレデンシャルが指定されていない場合は、DCNMは管理者ユーザとパスワードを使用してスイッチを検出します。

Note

- 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。デバイス設定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 フリーフォーム設定（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。

ステップ 12 画面右上の **[ブートストラップ（Bootstrap）]** をクリックします。

DCNM は管理IPアドレスおよびその他のクレデンシャル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。

ステップ 13 ブートストラップが完了したら、**[インベントリ管理（Inventory Management）]** 画面を閉じて、ファブリック トポロジ画面に移動します。

ステップ 14 ファブリック トポロジ画面で、画面の左側にある **[アクション（Actions）]** パネルから、**[トポロジの更新（Refresh Topology）]** をクリックします。

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。

ステップ 15 スイッチをモニタし、POAP 完了を確認します。

ステップ 16 ファブリック ビルダ トポロジ画面の右上にある **[保存と展開（Save & Deploy）]** をクリックして、保留中の構成（テンプレートやインターフェイス構成など）をスイッチに展開します。

Note
- スイッチと DCNM 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。デバイス設定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 フリーフォーム設定（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 サーバ情報を入力した場合は、各スイッチの AAA サーバ 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。

ステップ 17 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。

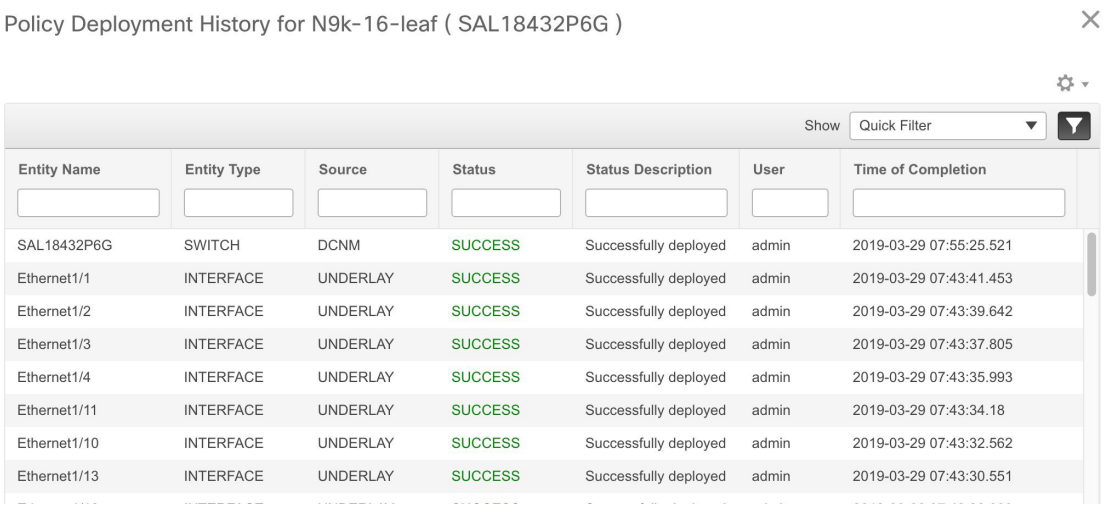
ステップ 18 **[閉じる（Close）]** をクリックして、ファブリック ビルダ トポロジに戻ります。

ステップ 19 **[トポロジの更新（Refresh Topology）]** をクリックして、更新を表示します。

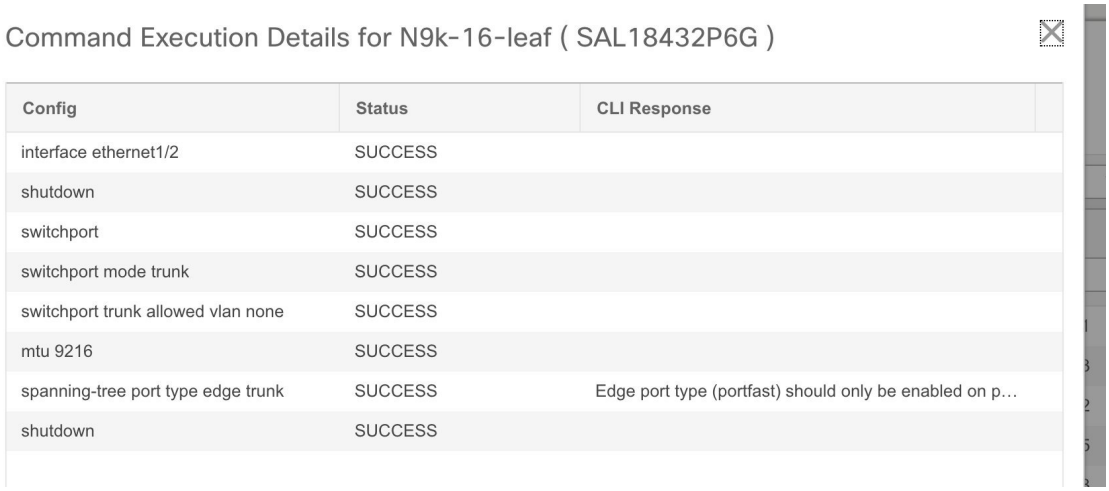
すべてのスイッチは、機能していることを示す緑色でなければなりません。

スイッチとリンクが DCNM 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。

ステップ 20 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。



詳細については、**[成功（Success）]** リンク（**[ステータス（Status）]** 列）をクリックします。例：



ステップ 21 DCNM UIでは、検出されたスイッチはファブリック 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。追加構成を行うには、**[制御（Control）] > [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設定する必要があります。以下が含まれますが、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。

Note スイッチ（新規または既存）を検出した後は、いつでも、POAP プロセスを使用してスイッチの設定を再度プロビジョニングできます。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

外部ファブリックで非 Nexus デバイスを検出できます。*Cisco DCNM Compatibility Matrix* には、Cisco DCNM がサポートする非Nexus デバイスが記載されています。

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設定」セクション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 DCNM 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 DCNM 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 DCNM、リリース 11.4(1) 以降、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。

検出用非 Nexus デバイスの構成

Cisco DCNM 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。

検出用の *IOS-XE* デバイスの設定

DCNM で Cisco IOS-XE デバイスを検出するには、次の手順を実行します。

手順

ステップ 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)# aaa authentication login default local
switch (config)# aaa authorization exec default local none
switch (config)# username admin privilege secret <password>
switch (config)# aaa new-model
switch (config)# session-id-common
```

ステップ 2 SNMP ウォークを実行するには、DCNM コンソールで次のコマンドを実行します。

```
snmpbulkwalk -v3 -u admin -A <password> -l AuthNoPriv -a MD5 ,switch-mgmt-IP>
        .1.3.6.1.2.1.2.2.1.2
```

ステップ 3 スイッチ コンソールで次の SNMP コマンドを実行します。

```
snmp-server user username group-name [remote host {v1 | v2c | v3 [encrypted] [auth {md5
 | sha} auth-password]} [priv des 256 privpassword] vrf vrf-name [access access-list]
```

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        /* to view the authorization*/
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 dcnm 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
```

（注） 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。

[show run] コマンドを実行して設定を確認し、[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

```
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/9AYx36YUBSPNLFdeuPIse9XgyHSdEOYXtPyT/0sMUYYdkMffuIjgn/d9rx/Do71XSbygSn/
username cvpadmin role network-admin secret sha512
$6$fLGFj/PUcuJT436i$Sj5G5c4y9cYjI/BZswjjmZW0J4npGrGqIyG3ZFk/ULza47Kz.d31q13jXA7iHM677gwqQbFSH2/3oQEaHRq08.
username dcnm privilege 15 role network-admin secret sha512
$6$M48PNrCdg2EITEdG$iiB880nvFQQlrWoZwOMzdt5EfkuCIraNqtEMRS0TJUhNKCQnJN.VDLFsLAmP7kQBo.C3ct4/.n.2eRlcP6hij/
```

Show SNMP View コマンド

```
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
```

検出用 *Cisco IOS-XR* デバイスの構成

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 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_name
snmp-server user user_name group_name v3 auth md5 password priv des56 password SystemOwner
```

（注） 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。

構成を確認するには、show run コマンドを実行します。

Cisco IOS-XR デバイスの構成と確認

```
RP/0/RSP0/CPU0:ios(config)#snmp-server view view_name cisco included
RP/0/RSP0/CPU0:ios(config)#snmp-server view view_name mib-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 password SystemOwner
RP/0/RSP0/CPU0:ios(config)#commit Day MMM DD HH:MM:SS Timezone
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_name
```

外部ファブリックで非 Nexus デバイスの検出

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。

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。

手順

ステップ 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。

[インベントリ管理（Inventory Management）] ダイアログボックスが表示されます。

ステップ 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。 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 スイッチは適切にケーブル接続しDCNM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	• Cisco 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。 • Cisco NCS 5500 シリーズ ルータ、IOS XR リリース 6.5.3 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。 • 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。

（注） 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 DCNM Web UI から **[LAN ログイン情報（LAN Credentials）]** ウィンドウに移動するには、**[管理（Administration）] > [LAN ログイン情報（LAN Credentials）]** を選択します。

ステップ 3 [検出の開始（Start Discovery）] をクリックします。

[詳細のスキャン（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。

ステップ 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。

ステップ 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.）]

ステップ 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。

ステップ 7 （任意） 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。

ステップ 8 （任意） **[アクション（Actions）]** ペインで **[表形式ビュー（Tabular view）]** 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の [検出中（discovering）] でありその横に警告アイコンが表示されます。

ステップ 9 （任意） デバイスの詳細を表示します。

デバイスの検出後：

- 検出ステータスが緑色の [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。

（注） スイッチが [到達不能（Unreachable）] 検出ステータスの場合、スイッチの最後の使用可能な情報が他の列に保持されます。

次のタスク

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。

デバイスの事前プロビジョニング

Cisco DCNM リリース 11.2 以降、デバイスを事前にプロビジョニングできます。

Note ファブリック設定の [ブートストラップ（Bootstrap）] タブに DHCP の詳細を確実に入力してください。

- 事前プロビジョニングされたデバイスは、DCNM で次の構成をサポートします。
  - 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、DCNM で次の構成をサポートしません。
  - 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）]** ウィンドウの **[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。

  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。
    - **modulesModel** ：（必須）スイッチ モジュールのモデル情報を指定します。
    - **gateway** ：（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、DCNM 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。
    - **breakout**：（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。
    - **portMode**：（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"}

Procedure

ステップ 1 **[制御（Control）] > [Fabric Builder]**の順にクリックします。

[ファブリック ビルダ（Fabric Builder）] 画面が表示されます。

ステップ 2 ファブリック ボックス内をクリックします。

ステップ 3 [アクション（Actions）] パネルで、**[スイッチの追加（Add switches）]** オプションをクリックします。

[インベントリ管理（Inventory Management）] 画面が表示されます。

ステップ 4 **[POAP]** タブをクリックします。

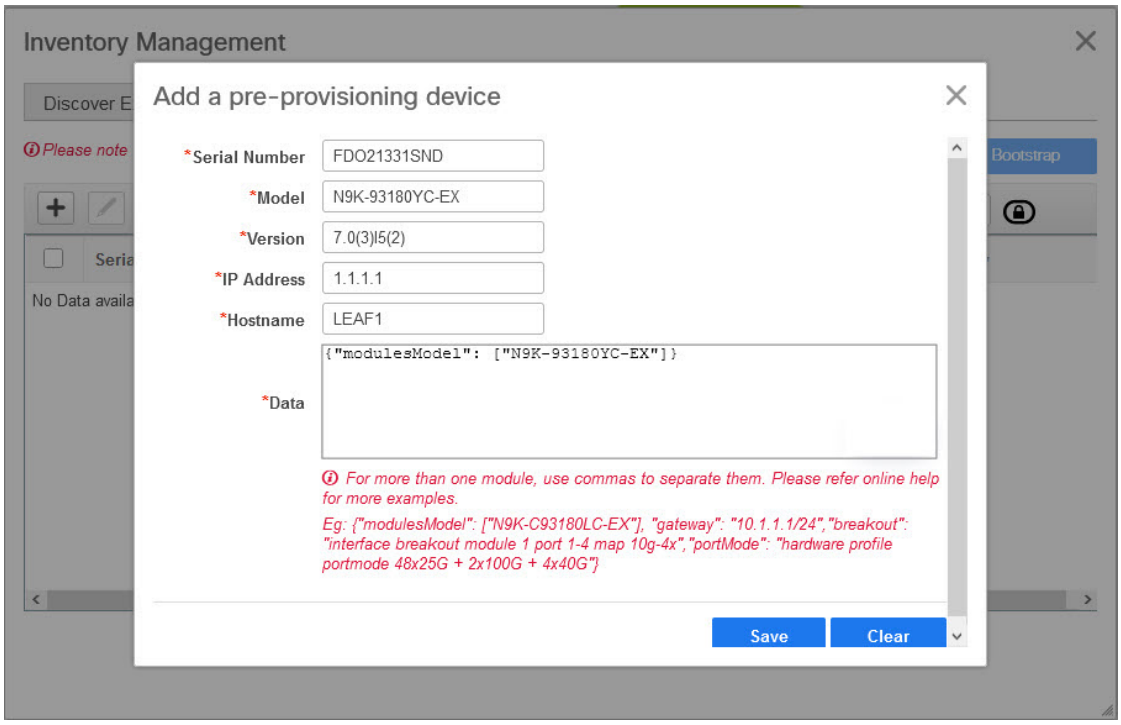
ステップ 5 **[POAP]** タブで、次の手順を実行します。

a. 画面左上の [+] をクリックします。

[新しいデバイスの追加（Add a new device）] 画面が表示されます。

b. スクリーンショットに示されているように、デバイスの詳細を入力します。

c. [保存（Save）] をクリックします。



IP アドレス：新しいデバイスの IPv4 または IPv6 アドレスを指定します。

シリアル番号：デバイスのシリアル番号。シリアル番号は Cisco Build of Material Purchase にあり、事前プロビジョニング機能の使用中にこれらの値を参照できます。

データ フィールドの詳細については、ガイドラインで提供されている例を参照してください。

デバイスの詳細が POAP 画面に表示されます。事前プロビジョニング用にデバイスをさらに追加できます。

ウィンドウの左上には、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するための **[エクスポート（Export）]** および **[インポート（Import）]** アイコンがあります。

[インポート（Import）] オプションを使用して複数のデバイスを事前プロビジョニングすることができます。

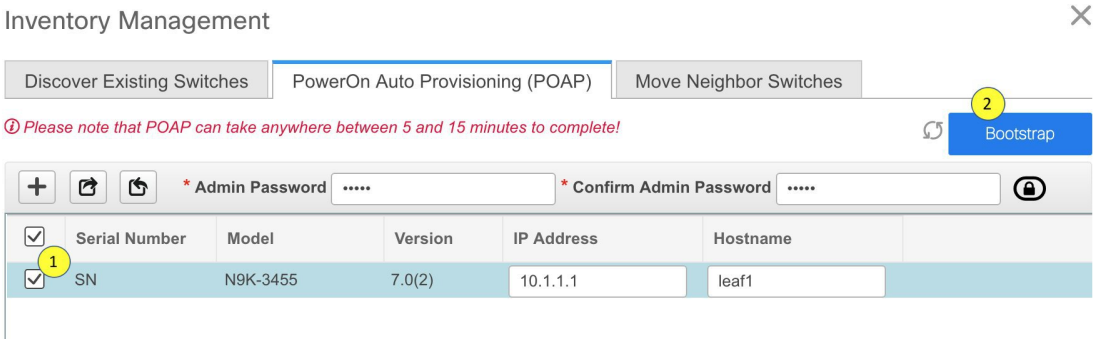
すべての必須フィールド（シリアル番号、モデル、バージョン、IpAddress、ホスト名、およびデータ フィールド [JSON オブジェクト]）を使用して、.csv ファイルに新しいデバイスの情報を追加します。

[データ（Data）] 列は、ファブリック テンプレートからハードウェア タイプを識別するためのモジュールのモデル名で構成されます。A.csv ファイルのスクリーンショット：

	A	B	C	D	E	F	G
1	#SerialNumber(Eg:FD01344GH5)	#Model(Eg:N9k-C9236C)	#Version(Eg:7.0(3)12(3))	#IPAddress of the device	#HostName	#Data(JSON Field contains model name of the modules	
2	Serial Number	Model	Version	IP Address	Hostname	Data	
3	FDO21331SND	N9K-93180YC-EX	7.0(3)I5(2)	1.1.1.1	leaf1	{"modulesModel":["N9K-93180YC-EX"]}	
4	FDO21351N3X	N9K-C9236C	7.0(3)I4(1)	11.1.1.1	spine1	{"modulesModel":["N9K-C9236C"]}	
5	FDO21491A5K	N9K-C93240YC-FX2	7.0(3)I7(3)	12.1.1.1	leaf2	{"modulesModel":["N9K-C93240YC-FX2"]}	
6							

ステップ 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、管理パスワードを入力します。

ステップ 7 デバイスを選択して、画面右上の **[ブートストラップ（Bootstrap）]** をクリックします。



Leaf1 デバイスがファブリック トポロジに表示されます。

[アクション（Actions）] パネルで、**[表形式ビュー（Tabular View）]** をクリックします。事前にプロビジョニングされたすべてのスイッチのステータスが **[検出ステータス（Discovery Status）]** 列に **[ok]** と表示されるまで、ファブリックを展開できません。

Note スイッチが [到達不能（Unreachable）] 検出ステータスの場合、スイッチの最後の使用可能な情報が他の列に保持されます。

Leaf1 をファブリックに接続すると、スイッチには IP アドレス 10.1.1.1 がプロビジョニングされます。

ステップ 8 **ファブリック ビルダ** に移動し、デバイスのロールを設定します。

次のいずれかのテンプレートを使用して、リンク内ポリシーを作成します。

- **int_pre_provision_intra_fabric_link** は、DCNM に割り当てられた IP アドレスを使用して、ファブリック内インターフェイス構成を自動的に生成します
- **int_intra_fabric_unnum_link_11_1** 番号付けなしのリンクを使用している場合
- **int_intra_fabric_num_link_11_1** IP アドレスをリンク内に手動で割り当てる場合

[保存して展開（Save & Deploy）] をクリックします。

スイッチの構成は、対応する PTI に取り込まれ、**[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウに表示されます。

ステップ 9 物理デバイスを持ち込むには、手動の RMA または POAP RMA の手順に従います。

詳細については、返品許可（RMA）, on page 246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。

ホスト ポートをプロビジョニングするために 1 つ以上のスイッチがオンラインになった後、ファブリックで**[保存と展開（Save & Deploy）]**をクリックする必要があります。このアクションは、ホストポート接続用にオーバーレイをプロビジョニングする前に実行する必要があります。

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

DCNM リリース 11.4(1) 以降、**[インターフェイス（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。DCNM 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にのみ、イーサネット インターフェイスを追加できます。

（注） ネットワーク/VRF をアタッチする前に、イーサネットインターフェイスを事前にプロビジョニングしてから、ポートチャネル、vPC、ST FEX、AA FEX、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 構成に追加する必要があります。

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 （46 ページ）を参照してください。

手順

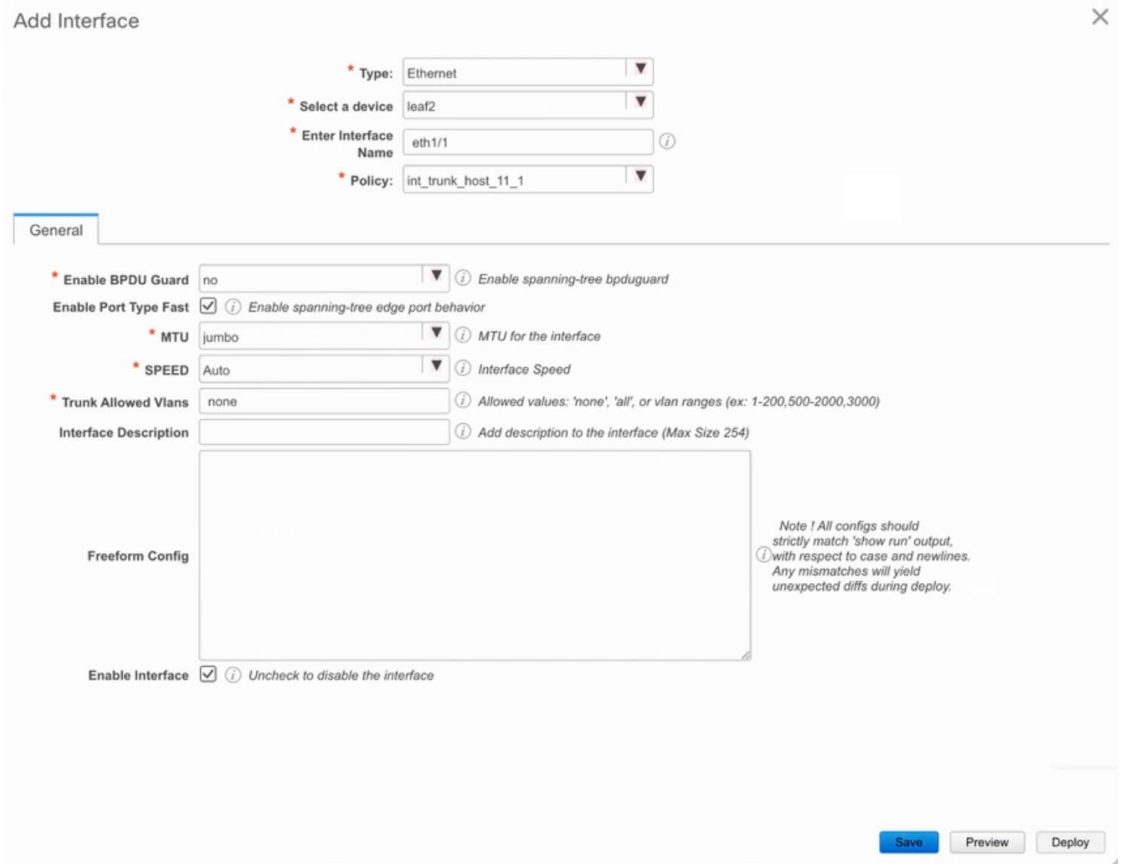
ステップ 1 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウから事前にプロビジョニングされたデバイスを含むファブリックに移動します。

ステップ 2 事前にプロビジョニングされたデバイスを右クリックし、**[インターフェイスの管理（Manage Interfaces）]** を選択します。

[制御（Control）] > [ファブリック（Fabrics）] > [インターフェイス（Interfaces）] を選択して、[インターフェイス（Interfaces）] ウィンドウに移動することもできます。[範囲（Scope）] ドロップダウンリストから、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選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 **[インターフェイスの追加（Add 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）]：この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。

（注） DCNM で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の入力（Enter 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。

詳細については、インターフェイスの追加 （258 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 **[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。

（注） 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 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。

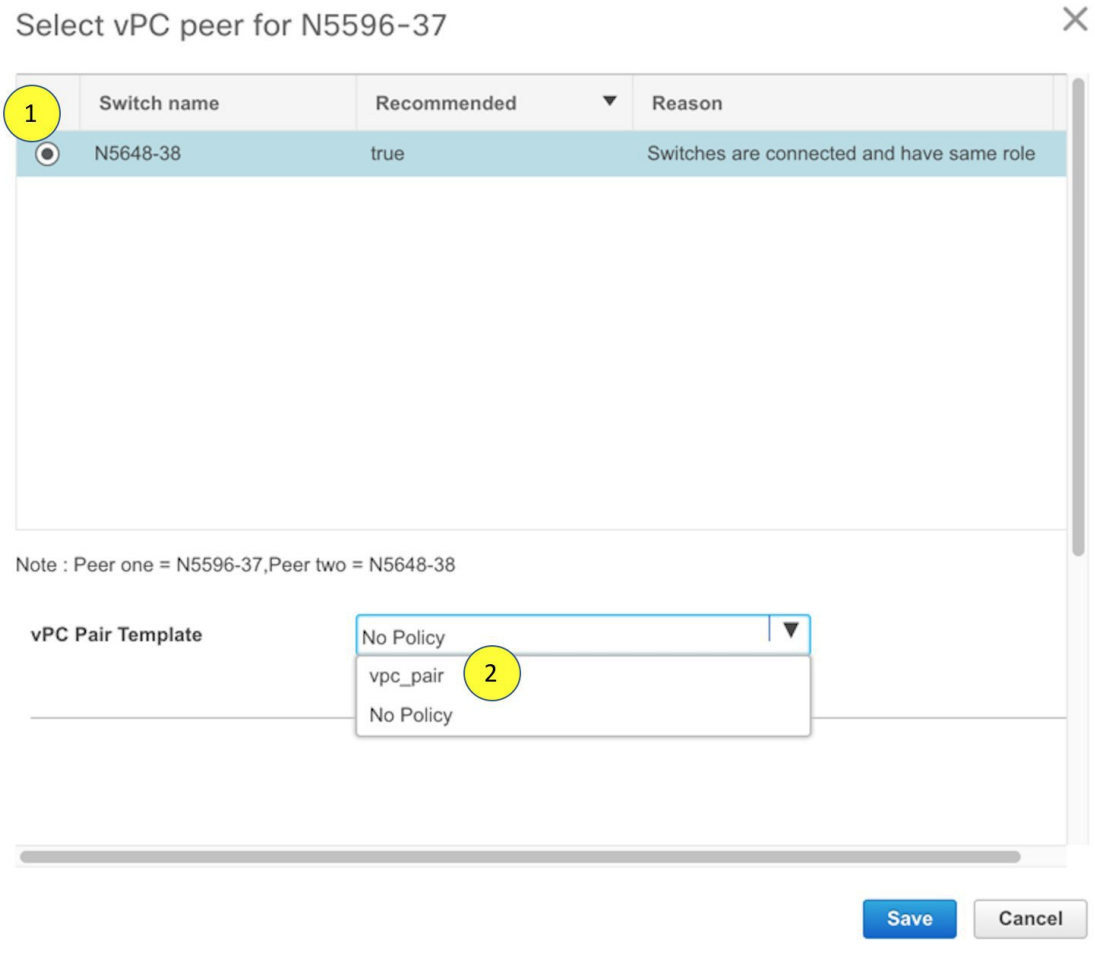
Procedure

ステップ 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。

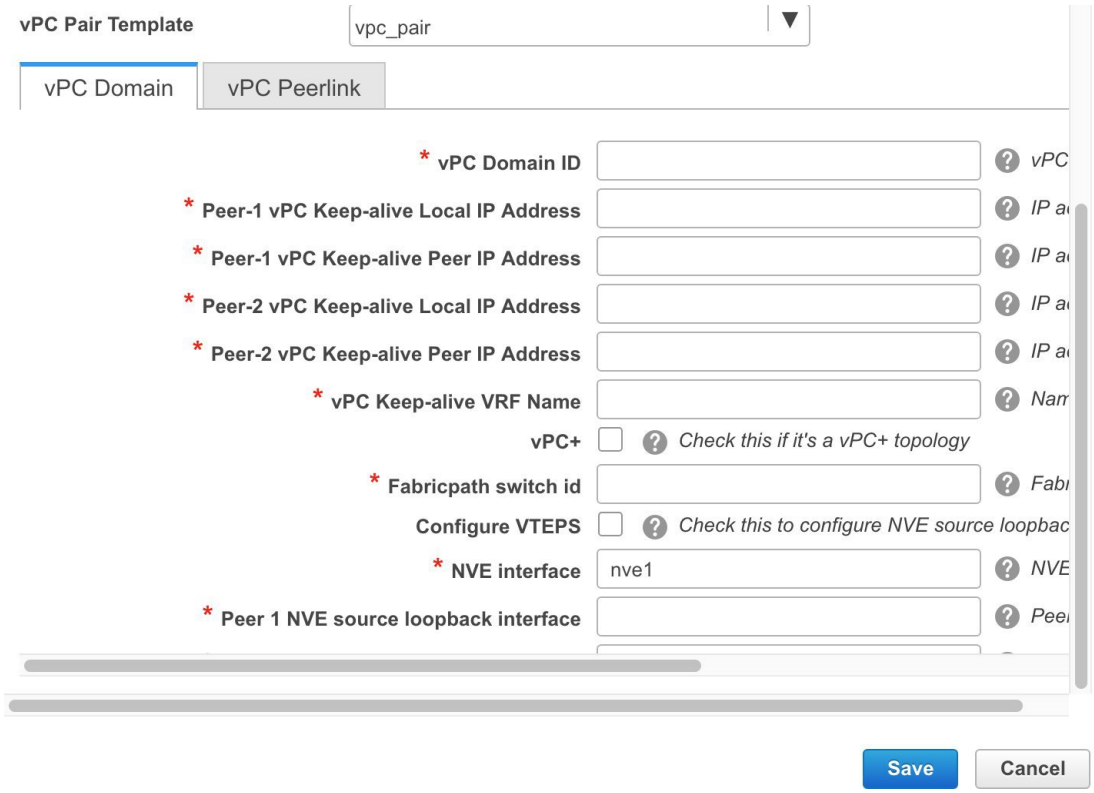
[vPC ピアの選択（Select vPC peer）] ダイアログボックスが表示されます。潜在的なピア スイッチのリストが含まれます。vPC ピア スイッチの**[推奨（Recommended）]**列が **[true]**に更新されていることを確認します。

Note 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。

ステップ 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。



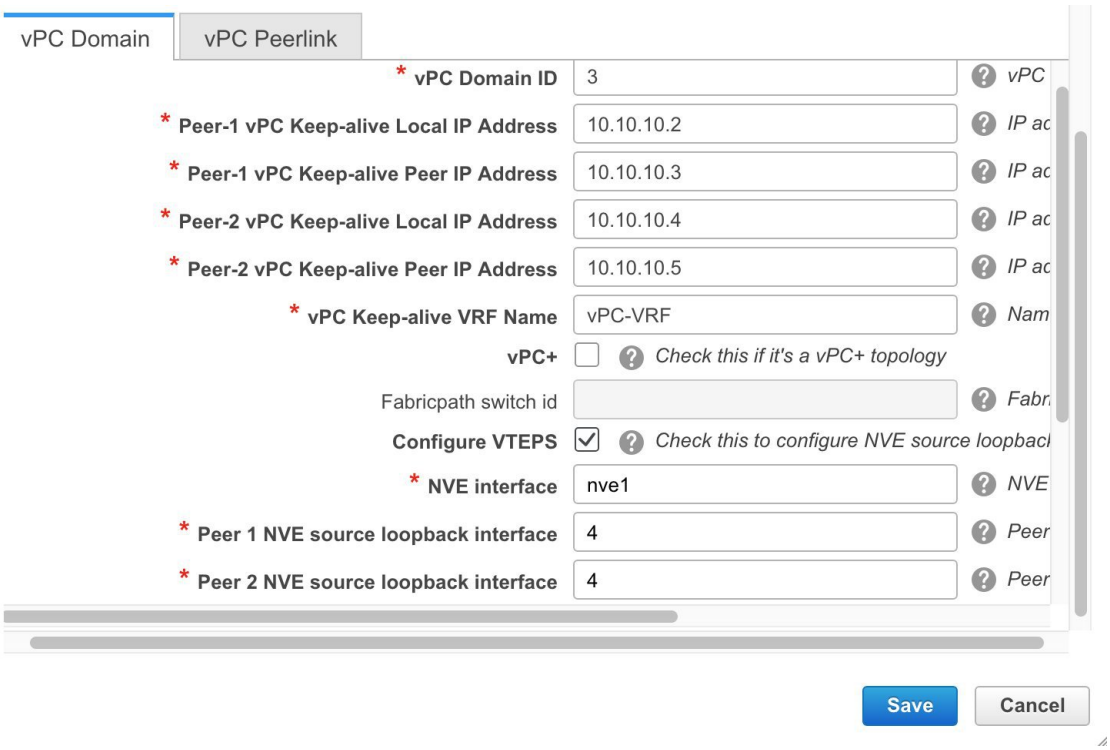
[vPC ドメイン（vPC Domain）] タブ：vPC ドメインの詳細を入力します。

[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。

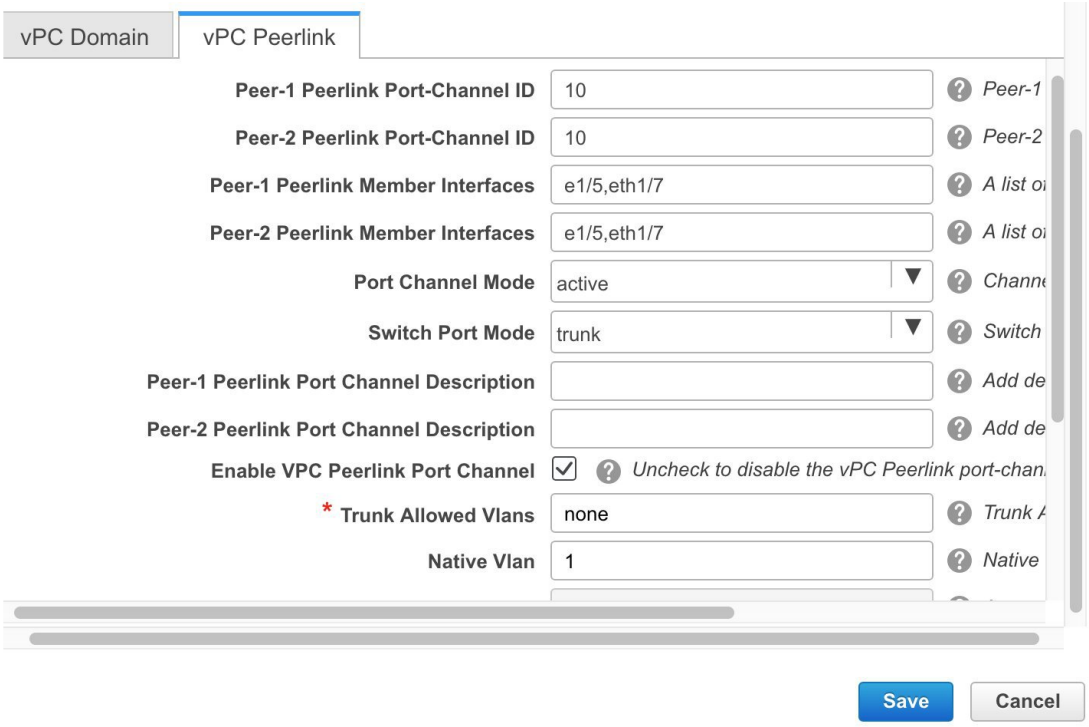
[NVE ループバック構成（NVE loopback configuration）]：IP アドレスをマスクで入力します。vPC ペアリングは、ループバック インターフェイスのプライマリおよびセカンダリ IP アドレスのみを構成します。追加構成には、自由形式のインターフェイスマネージャを使用します。



[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。

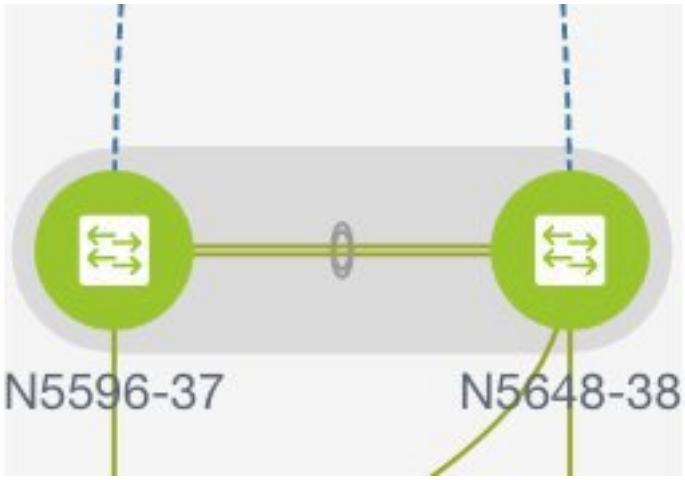
[スイッチポート モード（Switch Port Mode）]：**trunk** または **access** または **fabricpath** を選択します。

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。



ステップ 3 **[Save（保存）]** をクリックします。

[ファブリック トポロジ（fabric topology）] ウィンドウが表示されます。**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 セットアップの展開解除

Procedure

ステップ 1 **vPC** スイッチを右クリックし、**[vPC ペアリング（vPC Pairing)]** を選択します。

vPC ピア画面が表示されます。

ステップ 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。

ステップ 3 [保存して展開（Save & Deploy）] をクリックします。

[構成展開（Config Deployment）] ダイアログ ボックスが表示されます。

ステップ 4 (Optional) **[構成のプレビュー（Preview 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設定を表示します。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。

Note 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、**[保存と展開（Save & Deploy）]** の間に構成がクリアされません。NVE 構成、LACP 機能、FabricPath 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。

VXLAN BGP EVPN ファブリックのマルチサイト ドメイン

マルチサイト ドメイン（MSD）は、複数のメンバー ファブリックを管理するために作成されるマルチファブリック コンテナです。MSD は、メンバー ファブリック間で共有されるオーバーレイ ネットワークと VRF を定義するための単一の制御ポイントです。ファブリック（マルチファブリック オーバーレイ ネットワーク ドメインの一部として指定されている）をメンバー ファブリックとして MSD の下に移動すると、メンバー ファブリックは、MSD レベルで作成されたネットワークと VRF を共有します。このようにして、一度にさまざまなファブリックのネットワークと VRF を、一貫した仕方でプロビジョニングできます。複数のファブリック プロビジョニングに関連する時間と複雑さが大幅に削減されます。

サーバー ネットワークと VRF はメンバー ファブリック全体で（1 つの拡張ネットワークとして）共有されるため、新しいネットワークと VRF のプロビジョニング機能は MSD ファブリック レベルで提供されます。新しいネットワークと VRF の作成は、MSD に対してのみ許可されます。すべてのメンバー ファブリックは、MSD 用に作成された新しいネットワークと VRF を継承します。

DCNM 11.1(1) リリースでは、メンバー ファブリックに加えて、MSD ファブリックのトポロジ ビューが導入されています。このビューには、すべてのメンバー ファブリックと、それらが互いにどのように接続されているかが、1 つのビューとして表示されます。

また、MSD ファブリックの展開ビューも導入されています。各メンバー ファブリックの展開画面に個別にアクセスして展開する代わりに、単一のトポロジ展開画面から、メンバー ファブリックにオーバーレイ ネットワーク（および VRF）を展開できます。

Note

- DCNM 11.1(1) リリースでは、BGW の vPC サポートが追加されています。
- MSD 機能は、Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x) イメージを持つスイッチでサポートされていません。
- Cisco DCNM の VXLAN OAM 機能は、単一のファブリックまたはサイトでのみサポートされます。
- BGW vPC のペアリングを解除した後、メンバー ファブリックで **[保存と展開（Save & Deploy）]** を実行し、続いて MSD ファブリックの **[保存と展開（Save & Deploy）]** を実行します。

ファブリック固有の用語：

- **スタンドアロン ファブリック**：MSD の一部ではないファブリックは、MSD の観点からスタンドアロン ファブリックと呼ばれます。MSD の概念が登場する前は、すべてのファブリックはスタンドアロンと見なされていましたが、現在は、2 つ以上のファブリックを相互に接続できます。
- **メンバー ファブリック**：MSD の一部であるファブリックは、メンバー ファブリックまたはメンバーと呼ばれます。最初にスタンドアロン ファブリック（タイプ *Easy_Fabric*）を作成してから、それを MSD 内へ移動してメンバー ファブリックにします。

スタンドアロン ファブリックが MSD に追加されると、次のアクションが実行されます。

- スタンドアロン ファブリックの関連属性とネットワークおよびVRF 定義が、MSD でも同様にチェックされます。競合がある場合、MSD へのスタンドアロン ファブリックの追加は失敗します。競合がない場合、スタンドアロン ファブリックはMSD のメンバー ファブリックになります。競合がある場合、競合の詳細が MSD ファブリックの保留中のエラーログに記録されます。競合を解決してから、スタンドアロン ファブリックを MSD に再度追加してみることができます。
- MSD に存在していなかったスタンドアロン ファブリックからのすべての VRF およびネットワークの定義は、MSD にコピーされ、他の既存の各メンバー ファブリックに継承されます。
- MSD からの VRF（およびその定義、つまりスタンドアロン ファブリックには存在していない MSD の VRF、L2 および L3 VNI パラメータなど） は、メンバーになったばかりのスタンドアロン ファブリックに継承されます。

ファブリックとスイッチのインスタンス変数

MSD はネットワークおよび VRF 値のグローバル範囲をプロビジョニングしますが、ファブリック固有のパラメータや、スイッチ固有のパラメータもあります。そのようなパラメータは、ファブリック インスタンス変数およびスイッチ インスタンス変数と呼ばれます。

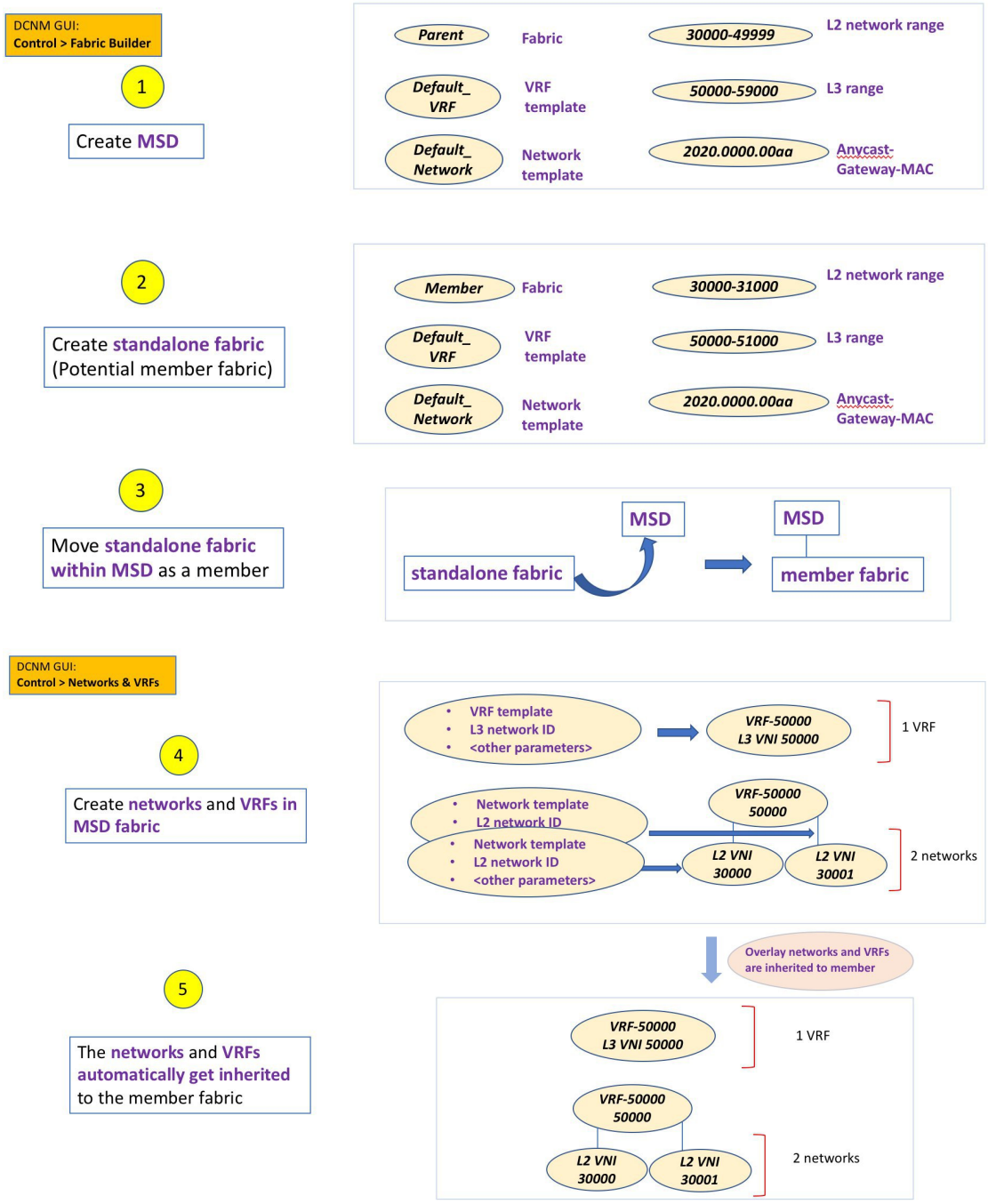
ファブリック インスタンスの値は、[VRFs and Networks] ウィンドウからのファブリック コンテキストでのみ編集または更新できます。ファブリック インスタンスの値を編集するには、**[範囲（SCOPE）]** ドロップダウンリストで適切なファブリックを選択する必要があります。ファブリック インスタンス変数の例には、BGP ASN、ネットワークごとのマルチキャスト グループまたは VRF などがあります。マルチキャスト グループ アドレスの編集方法については、メンバー ファブリックでのネットワークの編集, on page 140を参照してください。

スイッチインスタンスの値は、スイッチにネットワークを展開するときに編集できます。例としては、*VLAN ID* があります。

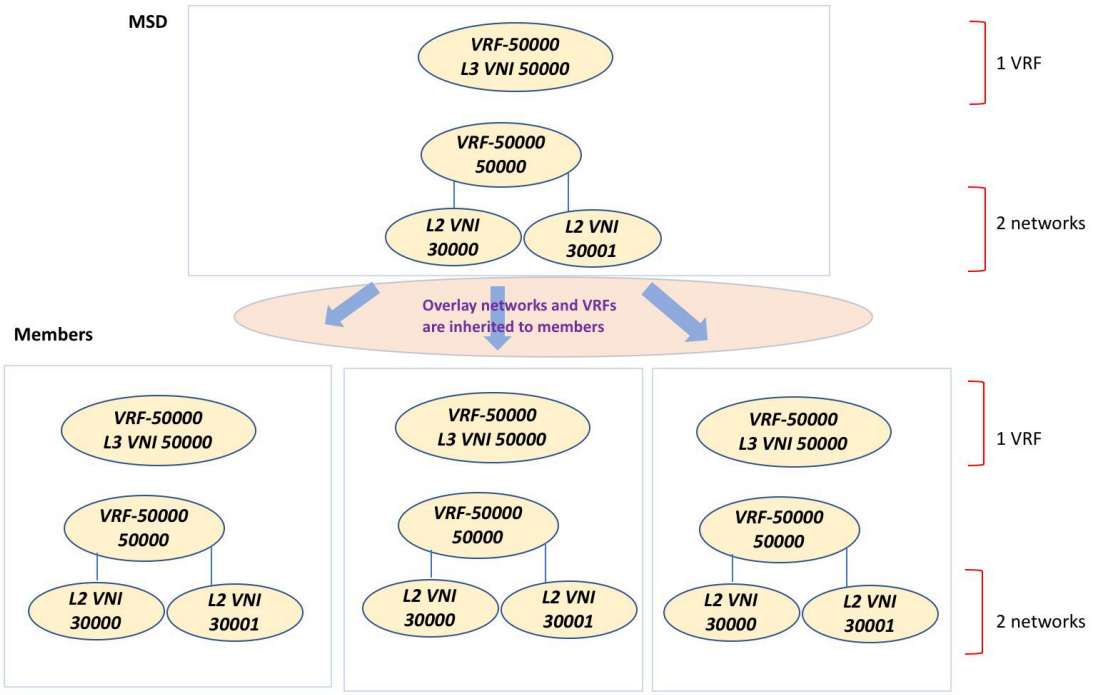
MSD およびメンバー ファブリックのプロセス フロー

MSDには複数のサイトがあります（したがって、MSDの下に複数のメンバー ファブリックがあります）。MSD用にVRFとネットワークが作成され、メンバー ファブリックに継承されます。たとえば、VRF-50000（および ID 50000 の L3 ネットワーク）と、ID 30000 および 30001 の L2 ネットワークが、MSD に対して一度に作成されます。

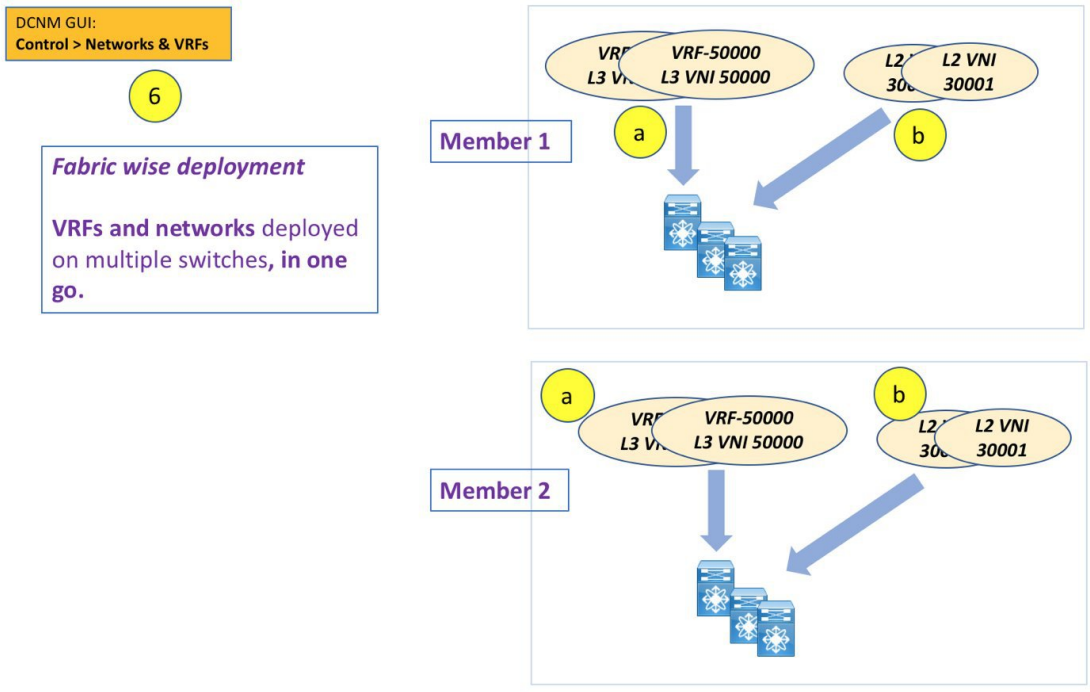
MSD とメンバー ファブリックの作成、および MSD からメンバー ファブリックへの継承プロセスの概要フロー チャート：



サンプル フローでは、MSD から 1 つのメンバーへの継承について説明しました。MSD には複数のサイトがあります（したがって、MSD の下に複数のメンバー ファブリックがあります）。MSD から複数のメンバーへのサンプル フロー：



この例では、VRF-50000（および ID 50000 の L3 ネットワーク）と、ID 30000 および 30001 の L2 ネットワークが、一度に作成されます。図に示すように、ネットワークと VRF はメンバー ファブリック スイッチに順次展開されます。



DCNM 11.1(1) では、単一の MSD 展開画面からオーバーレイ ネットワークをプロビジョニングできます。

Note 既存のネットワークと VRF を持つスタンドアロン ファブリックを MSD に移行すると、DCNM は適切な検証を行います。これについては、次のセクションで詳しく説明します。

ドキュメントの今後のセクションでは、以下について説明します。

- MSD ファブリックの作成。
- （潜在的なメンバーとしての）スタンドアロン ファブリックの作成と、メンバーとしての MSD の下でのその移行。
- MSD でのネットワークと VRF の作成、およびメンバー ファブリックへの継承。
- MSD およびメンバー ファブリック トポロジ ビューからのネットワークと VRF の展開。
- ファブリック移行のその他のシナリオ：
  - 既存のネットワークおよび VRF を持つスタンドアロン ファブリックの MSD ファブリックへの移行。
  - ある MSD のメンバー ファブリックの、別の MSD への移行。

MSD ファブリックの作成とメンバー ファブリックの関連付け

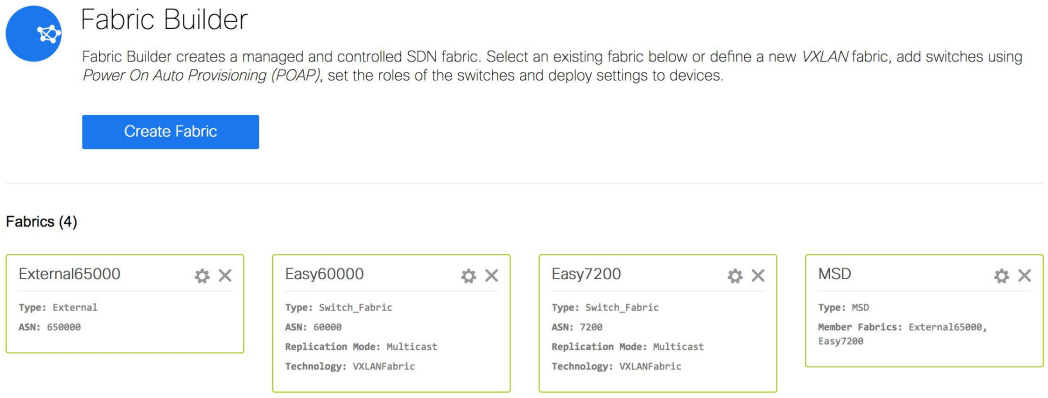
このプロセスは、次の 2 つのステップで説明されます。

1. MSD ファブリックを作成します。
2. 新しいスタンドアロン ファブリックを作成し、メンバー ファブリックとして MSD ファブリックの下に移動します。

MSD ファブリックの作成

1. **[制御（Control）] > [Fabric Builder]**の順にクリックします。

   [Fabric Builder] 画面が表示されます。初めて画面を表示したときに、[ファブリック（Fabrics）] セクションにはまだエントリはありません。ファブリックを作成すると、[ファブリック ビルダ（Fabric Builder）] 画面に表示されます。長方形のボックスが各ファブリックを表します。

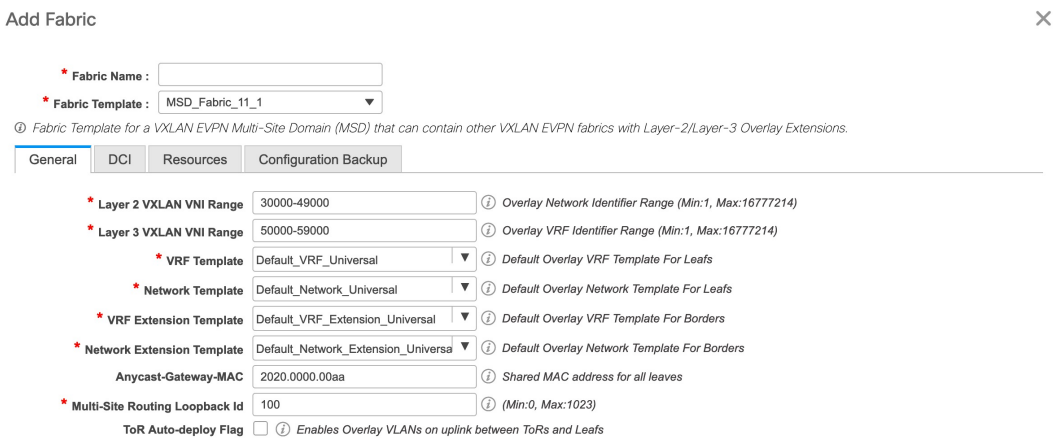


スタンドアロンまたはメンバー ファブリックには、*Switch_Fabric*（**タイプ** フィールド）、AS 番号（**ASN** フィールド）、および複製モード（**複製モード** フィールドのマルチキャストまたは複製の入力）が含まれます。MSD ファブリックはコンテナであり、デバイスまたはネットワーク トラフィックは関連付けられていないため、これらのフィールドはありません。

2. **[ファブリックの作成（Create Fabric）]** ボタンをクリックします。[ファブリックの追加（Add Fabric）] 画面が表示されます。該当するフィールドは次のとおりです。

   [ファブリック名（Fabric Name）]：ファブリックの名前を入力します。

   [ファブリック テンプレート（Fabric Template）]：このフィールドには、特定のタイプのファブリックを作成するためのテンプレート オプションがあります。*[MSD_Fabric]* を選択します。MSD 画面が表示されます。



画面のフィールドについて説明します。

[全般（General）] タブでは、すべてのフィールドにデータが自動入力されます。フィールドは、レイヤ 2 およびレイヤ 3 VXLAN セグメント識別子の範囲、デフォルトのネットワークおよび VRF テンプレート、およびエニーキャスト ゲートウェイの MAC アドレスで構成されます。必要に応じて、以下のフィールドを更新します。

[レイヤ 2 VXLAN VNI 範囲（Layer 2 VXLAN VNI Range）]：レイヤ 2 VXLAN セグメントの ID の範囲。

[レイヤ 3 VXLAN VNI 範囲（Layer 3 VXLAN VNI Range）]：レイヤ 3 VXLAN セグメントの ID の範囲。

[VRF テンプレート（VRF Template）]：デフォルトの VRF テンプレート。

[ネットワーク テンプレート（Network Template）]：デフォルトのネットワーク テンプレート。

[VRF 拡張テンプレート（VRF Extension Template）]：デフォルトの VRF 拡張テンプレート。

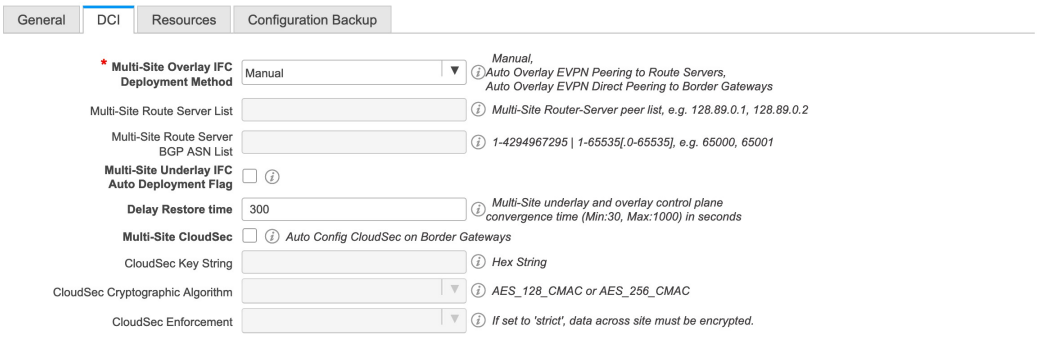
[ネットワーク拡張テンプレート（Network Extension Template）]：デフォルトのネットワーク拡張テンプレート。

[Anycast-Gateway-MAC]：エニーキャスト ゲートウェイ MAC アドレス。

[マルチサイト ルーティング ループバック ID（Multisite Routing Loopback Id）]：マルチサイト ルーティング ループバック ID は、このフィールドに入力されます。

[Tor 自動展開フラグ（ToR Auto-deploy Flag）]：このチェックボックスをオンにすると、MSD ファブリックで **[保存と展開（Save & Deploy）]** をクリックしたときに、Easy ファブリックのネットワークと VRF を外部ファブリックの ToR スイッチに自動展開できます。

3. **[DCI]** タブをクリックします。



該当するフィールドは次のとおりです。

[Multi-Site Overlay IFC Deploy Method（マルチサイト オーバーレイ IFC 展開方法）]：データ センターを BGW 経由、手動、バックツーバック、またはルート サーバー経由で接続する方法を選択します。

ルート サーバー経由で接続する場合は、ルート サーバーの詳細を入力する必要があります。

[マルチサイト ルート サーバー リスト（Multi-Site Route Server List）]：ルート サーバーの IP アドレスを指定します。複数を指定する場合は、IP アドレスをコンマで区切ります。

[マルチサイト ルート サーバー BGP ASN リスト（Multi-Site Route Server BGP ASN List）]：ルート サーバーの BGP AS 番号を指定します。複数のルート サーバーを指定する場合は、AS 番号をコンマで区切ります。

[マルチサイト アンダーレイ IFC 自動展開フラグ（Multi-Site Underlay IFC Auto Deployment Flag）]：チェックボックスをオンにして、自動構成を有効にします。手動構成の場合、チェックボックスをオフにします。

[復元時間の遅延（Delay Restore Time）]：マルチサイト アンダーレイおよびオーバーレイ コントロール プレーンのコンバージェンス時間を指定します。最小値は 30 秒で、最大値は 1000 秒です。

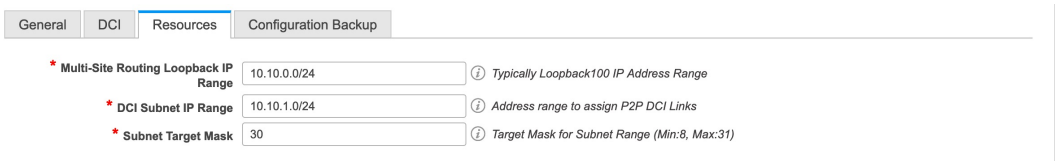
[マルチサイト（Multi-Site CloudSec）]：ボーダー ゲートウェイで CloudSec 構成を有効にします。このフィールドを有効にすると、CloudSec の残りの 3 つのフィールドが編集可能になります。詳細については、マルチサイト展開での CloudSec のサポート, on page 147を参照してください。

[マルチサイト eBGP パスワードを有効にする（Enable Multi-Site eBGP Password）]：マルチサイト アンダーレイ/オーバーレイ IFC の eBGP パスワードを有効にします。

[eBGP パスワード（eBGP Password）]：暗号化された eBGP パスワードの 16 進文字列を指定します。

[eBGP 認証キー暗号化タイプ （eBGP Authentication Key Encryption Type）]：BGP キー暗号化タイプを指定します。3DES の場合は **3**、Cisco の場合は **7** です。

4. [リソース（Resources）] タブをクリックします。

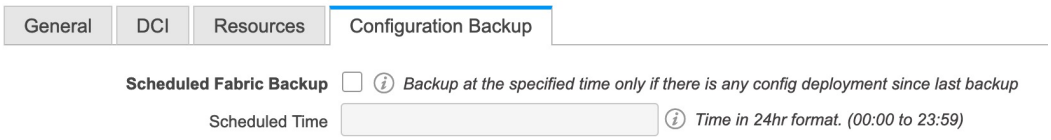


[マルチサイト ルーティング ループバック IP 範囲（MultiSite Routing Loopback IP Range）]：EVPN マルチサイト機能に使用されるマルチサイト ループバック IP アドレス範囲を指定します。

各メンバー サイトには、オーバーレイ ネットワークの到達可能性のためにループバック 100 IP アドレスが割り当てられている必要があるため、この範囲から各メンバー ファブリックに一意のループバック IPアドレスが割り当てられます。ファブリックごとのループバック IP アドレスは、特定のメンバー ファブリック内のすべての BGW に割り当てられます。

[DCI サブネット IP 範囲（DCI Subnet IP Range）] および **[サブネット ターゲット マスク（Subnet Target Mask）]**：データ センター インターコネクト（DCI）サブネットの IP アドレスとマスクを指定します。

5. [構成のバックアップ（Configuration Backup）] タブをクリックします。



[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]：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。

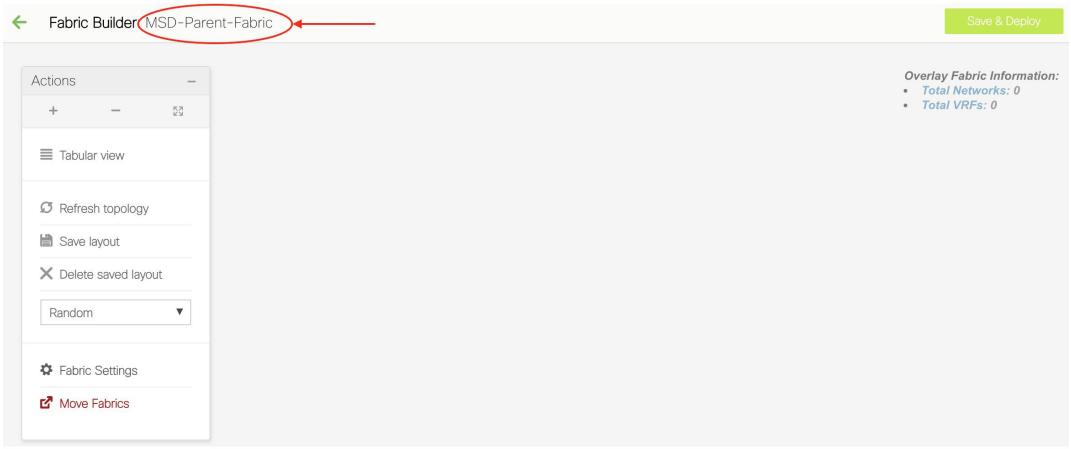
[保存（Save）]をクリックすると、バックアップ プロセスが開始されます。

バックアップ構成ファイルは、DCNM にある次のパスに保存されます：/usr/local/cisco/dcm/dcnm/data/archive

6. [保存（Save）] をクリックします。

画面の右下に、新しい MSD ファブリックが作成されたことを示すメッセージが短時間表示されます。ファブリック作成後、ファブリックのページが表示されます。画面の左上にファブリック名 *[MSD-Parent-Fabric]* が表示されます。

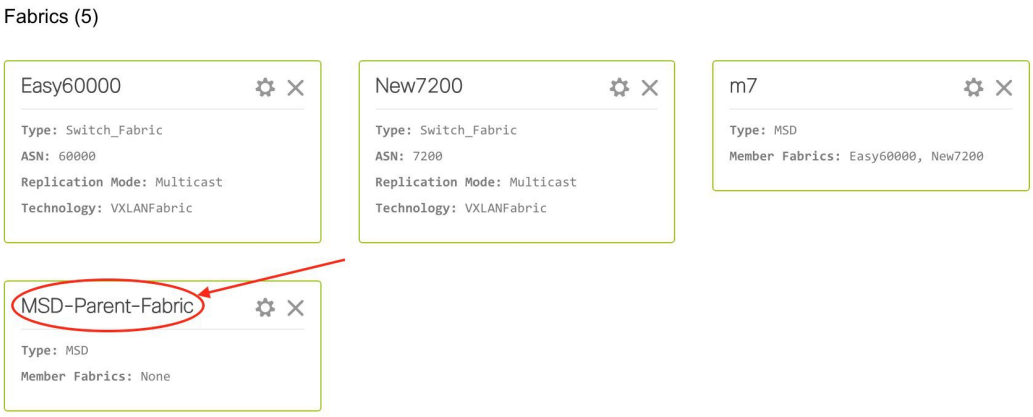
Note Cisco DCNM リリース 11.4(1) 以降、MSD ファブリック設定を更新すると、MSD に関連するロールを持つスイッチだけが更新されます。



MSD ファブリックはコンテナであるため、スイッチを追加することはできません。メンバーおよびスタンドアロン ファブリックの **[アクション（Actions）]** パネルで使用できる **[スイッチの追加（Add Switches）]** ボタンは、MSD ファブリックでは使用できません。

新しい MSD が作成されると、新しく作成された MSD ファブリック インスタンスが [ファブリック ビルダ（Fabric Builder）] ページに表示されます（長方形のボックスで表示）。[ファブリック ビルダ（Fabric Builder）] ページに移動するには、*[MSD-Parent-Fabric]* ページの左上にある **[←]** ボタンをクリックします。

MSD ファブリックは、*[MSD]* として **[タイプ（Type）]** フィールドに 表示されます。これには **[メンバー ファブリック（Member Fabrics）]** フィールドのメンバー ファブリック名が含まれています。メンバー ファブリックが作成されていない場合は、*[なし（None）]* が表示されます。



MSD ファブリックを作成し、メンバー ファブリックをその下に移動する手順は次のとおりです。

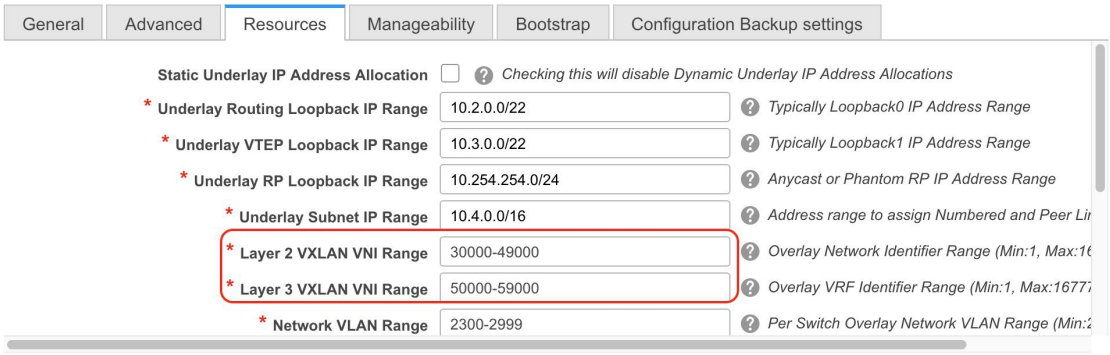
1. MSD ファブリックを作成します。
2. **新しいスタンドアロン ファブリックを作成し、メンバー ファブリックとして MSD ファブリックの下に移動します。**

ステップ 1 が完了しました。ステップ 2 については、次のセクションで説明します。

新しいファブリックを作成し、メンバーとして MSD ファブリックの下に移動する

新しいファブリックは、スタンドアロン ファブリックとして作成されます。新しいファブリックを作成したら、メンバーとして MSD の下に移動できます。ベスト プラクティスとして、（MSD の）メンバー ファブリックにする予定の新しいファブリックを作成するときは、ネットワークと VRF をファブリックに追加しないでください。ファブリックを MSD の下に移動してから、MSD のネットワークと VRF を追加します。そうすれば、メンバーと MSD ファブリック ネットワークおよび VRF パラメータ間の検証（または競合解決）の必要がなくなります。

新しいファブリックの作成については、Easy ファブリックの作成プロセスで説明されています。MSD ドキュメントでは、ファブリックの移動について説明されています。ただし、スタンドアロン（メンバーとなる可能性のある）ファブリックについては、いくつかの指針があります。



画面に表示される値は自動的に生成されます。新しいネットワークおよびVRFの作成に割り当てられるVXLAN VNI ID範囲(L2セグメントID範囲およびL3パーティションID範囲フィールド内)は、MSDファブリック セグメントID範囲からの値です。VXLAN VNI範囲、またはVRFおよびネットワーク VLAN範囲を更新する場合は、次のことを確認します。

- 値の範囲を更新する場合は、他の範囲と重複しないようにしてください。
- 一度に更新できる値の範囲は1つだけです。複数の値の範囲を更新する場合は、別のインスタンスで実行します。たとえば、L2とL3の範囲を更新する場合は、次の手順を実行する必要があります。
  1. L2範囲を更新し、[保存（Save）]をクリックします。
  2. [ファブリックの編集（Edit Fabric）]オプションをもう一度クリックし、L3範囲を更新して[保存（Save）]をクリックします。

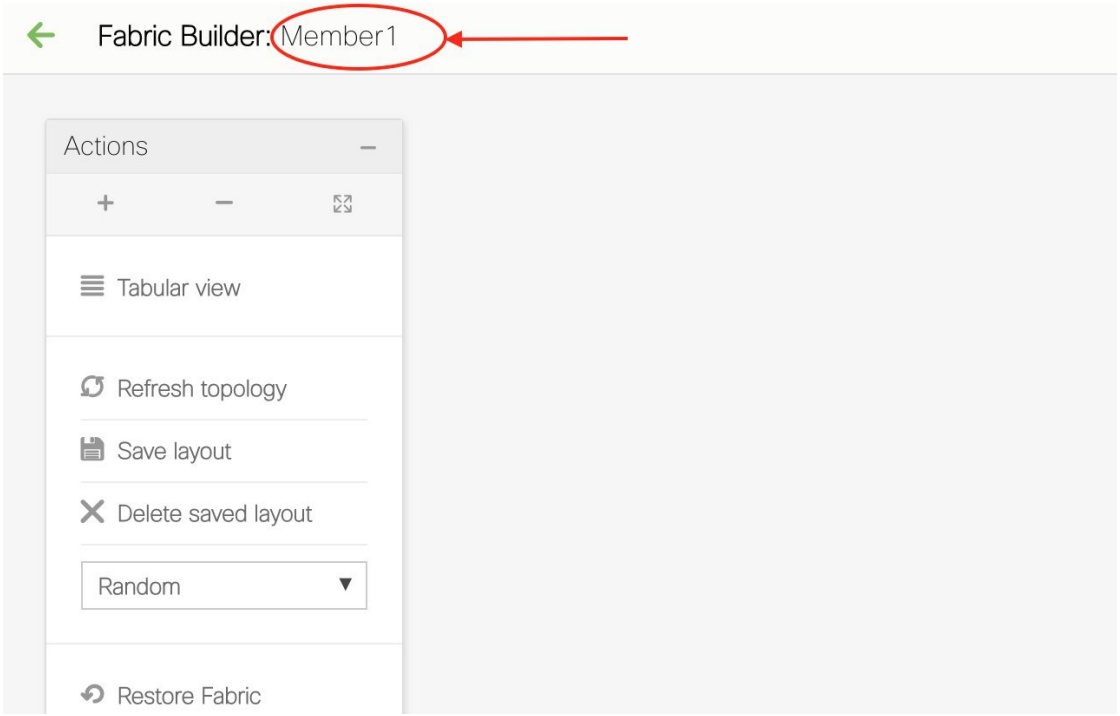
[エニーキャスト ゲートウェイ MAC（Anycast Gateway MAC）]、**[ネットワーク テンプレート（Network Template）]**、および**[VRF テンプレート（VRF Template）]**フィールドの値がMSDファブリックと同じであることを確認します。それ以外の場合、MSDへのメンバーファブリックの移動は失敗します。

その他の指針：

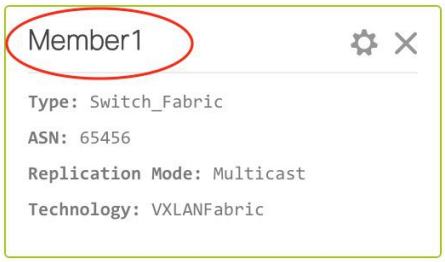
- [エニーキャスト ゲートウェイ MAC（Anycast Gateway MAC）]、[ネットワーク テンプレート（Network Template）]、および[VRF テンプレート（VRF Template）]フィールドの値がMSDファブリックと同じであることを確認します。それ以外の場合、MSDへのメンバーファブリックの移動は失敗します。
- メンバーファブリックにはサイトIDが設定されている必要があり、サイトIDはメンバー間で一意である必要があります。
- BGP AS番号は、メンバー ファブリックに対して一意である必要があります。
- loopback0のアンダーレイ サブネット範囲は一意である必要があります。
- loopback1のアンダーレイ サブネット範囲は一意である必要があります。

[保存（Save）]をクリックすると、ファブリックが作成されたことを示すメモが画面の右下に表示されます。ファブリックが作成されると、ファブリックのページが表示されます。画面左上にファブリック名が表示されます。

同時に、ファブリック ビルダ ページには、新しく作成されたファブリック *Member1* も表示されます。



同時に、ファブリック ビルダ ページには、新しく作成されたファブリック Member1 も表示されます。



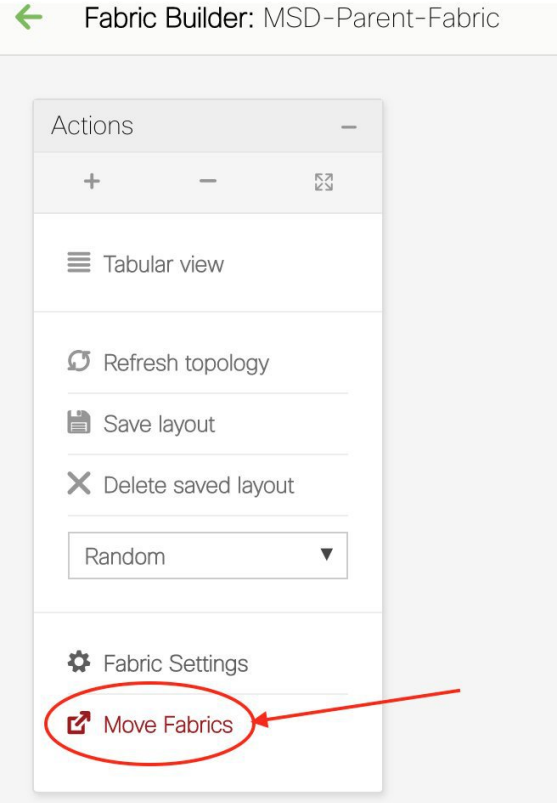
MSD-Parent-Fabric の下での Member1 ファブリックの移動

MSD ファブリックのページに移動して、その下のメンバー ファブリックを関連付ける必要があります。

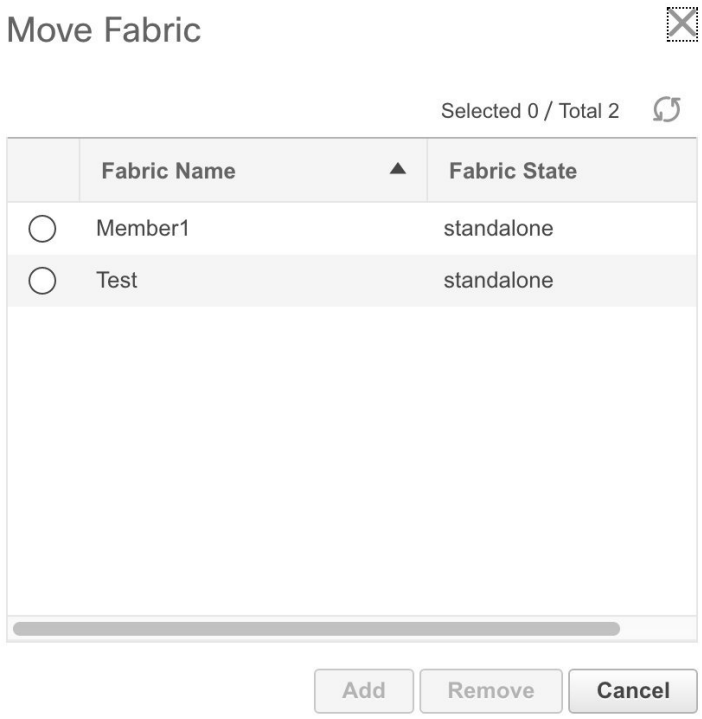
ファブリック ビルダ ページを表示している場合は、**MSD-Parent-Fabric** ボックス内をクリックして、MSD-Parent-Fabric ページに移動します。

Member1 ファブリック ページにいる場合は、MSD-Parent-Fabrics-Docs ファブリック ページに移動する必要があります。**[アクション（Actions）]** パネルの上にある **[←]** をクリックします。ファブリック ビルダ ページにアクセスします。**MSD-Parent-Fabric** ボックス内をクリックします。

1. MSD-Parent-Fabric ページで、**[アクション（Actions）]** パネルに移動し、**[ファブリックの移動（Move Fabrics）]** をクリックします。



[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。

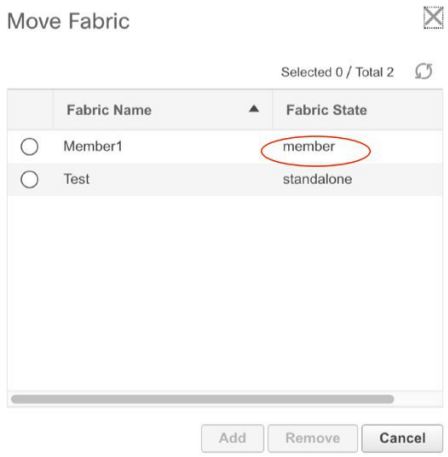


他の MSD コンテナ ファブリックのメンバー ファブリックは、ここには表示されません。

Member1 ファブリックは、依然としてスタンドアロン ファブリックです。ファブリックは、MSD ファブリックに関連付けられている場合にのみ、MSD ファブリックのメンバー ファブリックと見なされます。また、各スタンドアロンファブリックは、MSDファブリックの 1 つに関連付けるまで、MSD ファブリック メンバーの候補です。

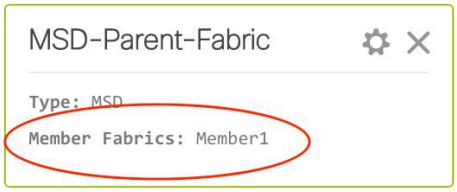
2. *Member1* ファブリックを MSD ファブリックに関連付けるため、**[Member1]** ラジオ ボタンを選択します。**[追加（Add）]** ボタンが有効になります。
3. [追加（Add）] をクリックします。

   すぐに、*Member1* ファブリックが MSD ファブリック *MSD-Parent-Fabric* に関連付けられたことを示すメッセージが画面の上部に表示されます。これで、MSD-Parent-Fabric ファブリック ページが再び表示されます。
4. **[ファブリックの移動（Move Fabrics）]** オプションをクリックして、ファブリックのステータスを確認します。ファブリックのステータスがスタンドアロンからメンバーに変更されたことがわかります。



5. この画面を閉じます。
6. [アクション（Actions）]パネルの上にある **[←]** をクリックして、ファブリック ビルダ ページに移動します。

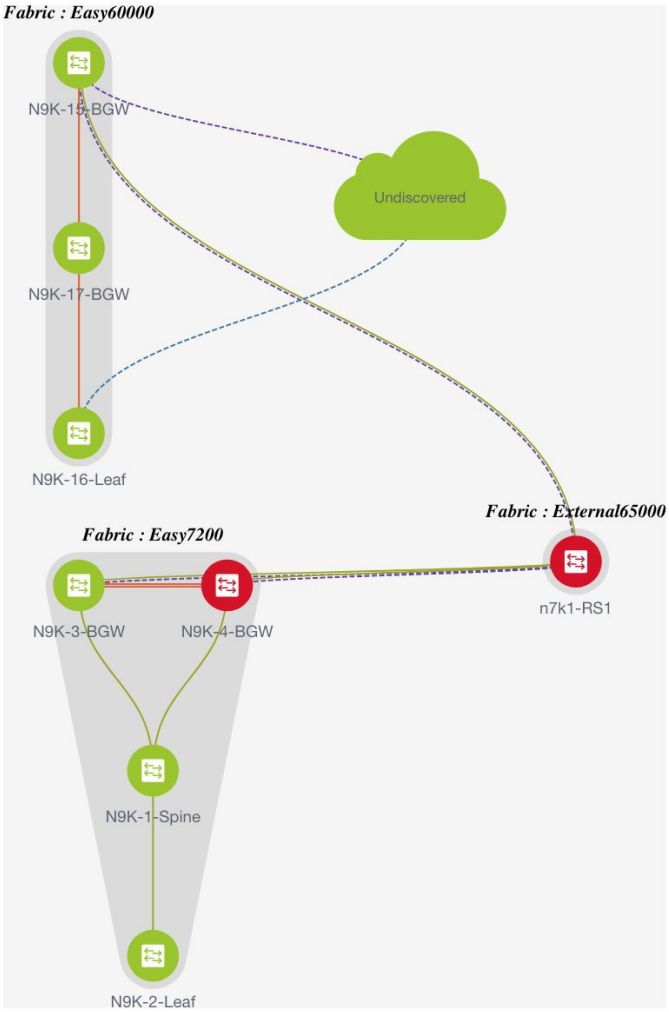
   Member1 が MSD ファブリックに追加され、**[メンバー ファブリック（Member Fabrics）]** フィールドに表示されることがわかります。



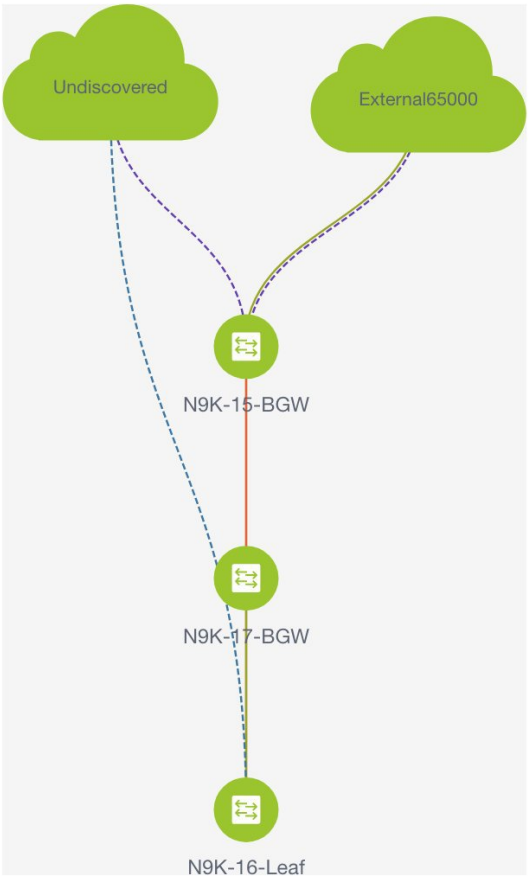
MSD ファブリックのトポロジ ビューのポインタ

- **[MSD ファブリック トポロジ ビュー（MSD fabric topology view）]**：メンバー ファブリックとそのスイッチが表示されます。境界は、各メンバーファブリックを定義します。ファブリックのすべてのファブリック デバイスは、境界に限定されます。

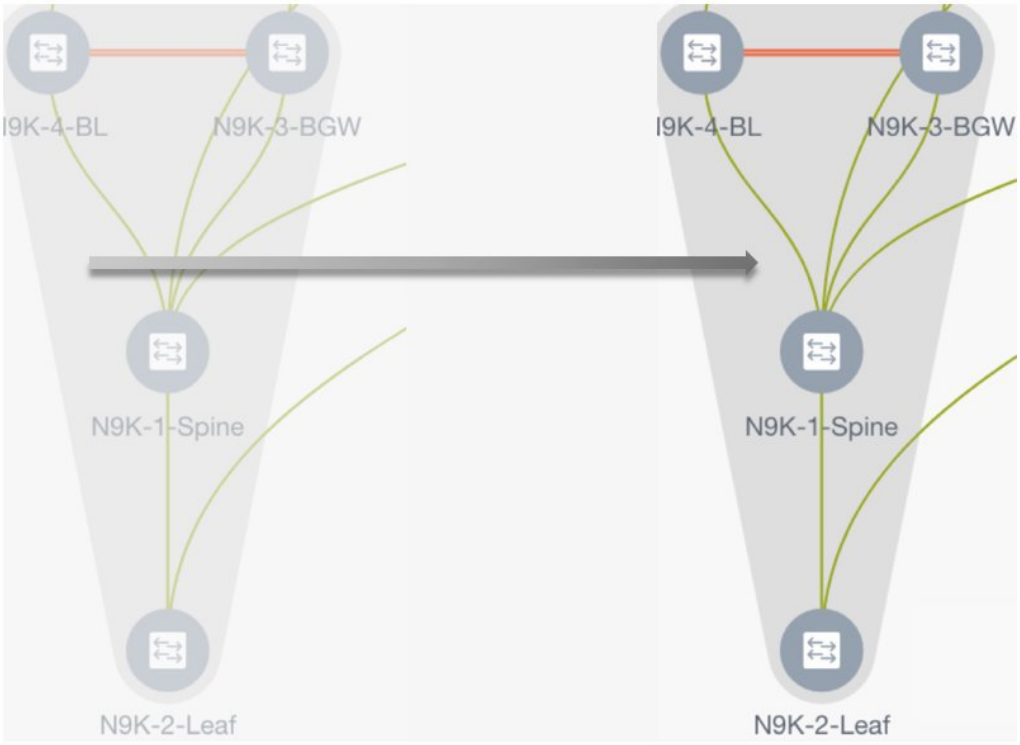
  ファブリック内リンクとマルチサイト（アンダーレイとオーバーレイ）、およびリモート ファブリックへの VRF Lite リンクを含むすべてのリンクが表示されます。



- **[メンバー ファブリック トポロジ ビュー（Member fabric topology view）]**：メンバー ファブリックとそのスイッチが表示されます。また、接続されている外部ファブリックが表示されます。



- 境界は、スタンドアロンVXLANファブリックと、MSDファブリック内の各メンバーファブリックを定義します。ファブリックのデバイスは、ファブリックの境界に限定されます。スイッチのアイコンはドラッグして移動できます。ユーザー体験を向上させるために、DNCM 11.2(1) リリースでは、スイッチに加えて、ファブリック全体を移動できます。ファブリックを移動するには、カーソルをファブリック境界内（スイッチアイコン上ではなく）に置き、目的の方向にドラッグします。



リンクの追加と編集

リンクを追加するには、トポロジ内の任意の場所を右クリックし、**[リンクの追加（Add Link）]** オプションを使用します。リンクを編集するには、リンクを右クリックし、**[リンクの編集（Edit Link）]** オプションを使用します。

または、**[アクション（Actions）]** パネルから **[表形式ビュー（Tabular view）]** オプションに移動することもできます。

異なるファブリックのボーダースイッチ間（ファブリック間）、または同じファブリック内のスイッチ間（ファブリック内）にリンクを追加する方法については、**ファブリックのリンク**のトピックを参照してください。

MSD ファブリックでのネットワークと VRF の作成と展開

スタンドアロンファブリックでは、ファブリックごとにネットワークとVRFが作成されます。MSD ファブリックでは、ネットワークと VRF は MSD ファブリック レベルで作成する必要があります。ネットワークと VRF は、すべてのメンバー ネットワークによって継承されます。メンバー ファブリックのネットワークおよび VRF を作成または削除することはできません。ただし、編集することはできます。

たとえば、2 つのメンバー ファブリックを持つ MSD ファブリックを考えてみます。MSD ファブリックに 3 つのネットワークを作成すると、3 つのネットワークすべてが自動的に両方のメンバー ファブリックで展開できるようになります。

メンバー ファブリックは MSD ファブリックのネットワークと VRF を継承しますが、ファブリックごとにネットワークと VRF を個別に展開する必要があります。

DCNM 11.1(1) リリースでは、ファブリックごとの展開ビューに加えて、MSD の展開ビューが導入されました。このビューでは、MSD 内のすべてのメンバー ファブリックのオーバーレイ ネットワークを一度に表示し、プロビジョニングできます。ただし、ファブリックごとにネットワークと VRF の構成を個別に適用して保存する必要があります。

Note ネットワークと VRF は、サーバー（またはエンドホスト）がその下でグループ化される共通の識別子（メンバー ファブリック全体で表現される）であり、同じファブリック、それとも異なるファブリックに属しているかにはかかわりなく、ネットワークと VRF ID に基づいてエンドホスト間でトラフィックを送信できるようにします。メンバー ファブリック全体で共通の表現があるため、ネットワークと VRF を一度にプロビジョニングできます。異なるファブリックのスイッチは物理的にも論理的にも異なるため、ファブリックごとに同じネットワークと VRF を個別に展開する必要があります。

たとえば、2 つのメンバー ファブリックを含む MSD にネットワーク 30000 と 30001 を作成すると、メンバーファブリック用にネットワークが自動的に作成され、展開に使用できるようになります。

DCNM 11.1(1) リリースでは、30000 および 30001 は、単一の（MSD ファブリック）展開画面を介して、すべてのメンバーファブリックのボーダーデバイスに展開できます。これ以前は、最初のメンバーのファブリック展開画面にアクセスし、ファブリックのボーダー デバイスに 30000 と 300001 を展開してから、2 番目のメンバー ファブリック展開画面にアクセスして、再度展開する必要がありました。

ネットワークと VRF は MSD で作成され、メンバー ファブリックに展開されます。手順は次のとおりです。

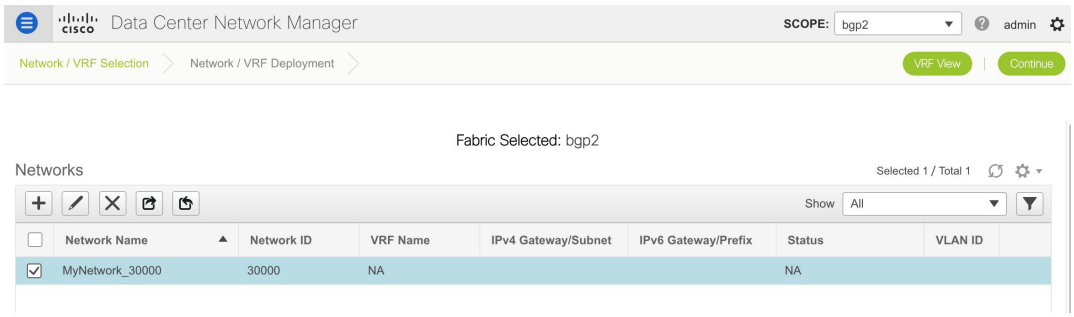
1. MSD ファブリックにネットワークと VRF を作成します。
2. メンバー ファブリックのデバイスにネットワークと VRF を展開します。1 回に付き 1 つのファブリックを展開します。

MSD ファブリックでのネットワークの作成

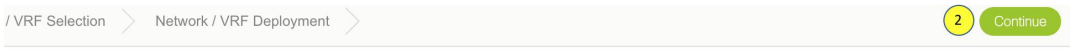
1. **[制御（Control）] > [ネットワーク（Networks）]**（**[ファブリック（Fabrics）]** サブメニューの下）をクリックします。

   [ネットワーク（Networks）] 画面が表示されます。

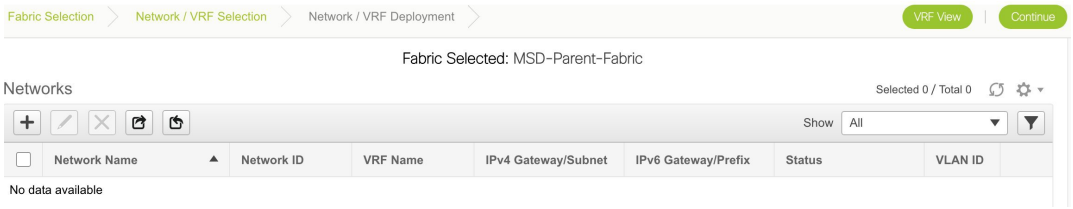
2. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[ネットワーク（Networks）]** 画面が更新され、選択したファブリックのネットワークが一覧表示されます。



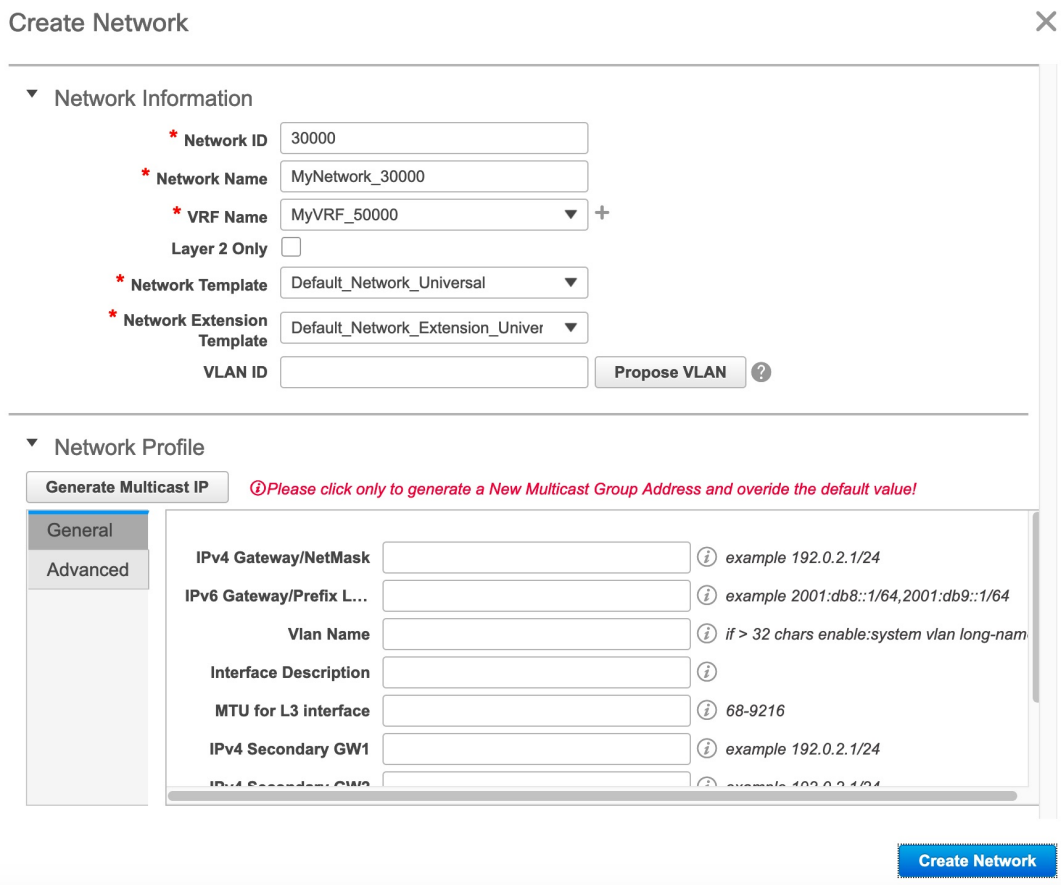
3. リストから *MSD-Parent-Fabric* を選択し、画面の右上にある **[続行（Continue）]** をクリックします。



[ネットワーク（Networks）]ページが表示されます。これには、MSDファブリック用に作成されたネットワークのリストが表示されます。最初、この画面にはエントリがありません。



4. 画面の左上部分（**[ネットワーク（Networks）]** の下）にある **[+]** ボタンをクリックして、ネットワークをMSDファブリックに追加します。[ネットワークの作成（Create Network）]画面が表示されます。ほとんどのフィールドは自動入力されます。



この画面のフィールドは次のとおりです。

[ネットワーク ID (Network ID)] と **[ネットワーク名 (Network Name)]**：ネットワークのレイヤ 2 VNI と名前を指定します。ネットワーク名には、アンダースコア（_）とハイフン（-）以外の空白や特殊文字は使用できません。

[VRF 名 (VRF Name)]：仮想ルーティングおよび転送（VRF）を選択できます。

VRF が作成されていない場合、このフィールドは空白になります。新しい VRF を作成する場合は、**[+]** ボタンをクリックします。VRF名には、アンダースコア（_）、ハイフン（-）、およびコロン（:）以外の空白文字や特殊文字は使用できません。

Note [ネットワーク（Networks）] ページの [VRF ビュー（VRF View）] ボタンをクリックして、VRF を作成することもできます。

[レイヤ 2 のみ (Layer 2 Only)]：ネットワークがレイヤ 2 のみであるかどうかを指定します。

[ネットワーク テンプレート（Network Template）]：ネットワーク テンプレートを選択できます。

[ネットワーク拡張テンプレート（Network Extension Template）]：このテンプレートを使用すると、メンバー ファブリック間のネットワークを拡張できます。

VLAN ID：ネットワークの対応するテナントVLAN IDを指定します。

[ネットワーク プロファイル（Network Profile）] のセクションには、[全般（General）] タブと [詳細（Advanced）] タブがあります。

[General] タブ

IPv4ゲートウェイ/ NetMask：IPv4アドレスとサブネットを指定します。

[IPv6ゲートウェイ/プレフィックス（IPv6 Gateway/Prefix）]：サブネットの IPv6 アドレスを指定します。

[Vlan 名（Vlan Name）]：VLAN 名を入力します。

VLAN が複数のサブネットにマッピングされている場合は、それらのサブネットのエニーキャスト ゲートウェイ IP アドレスを入力します。

[インターフェイスの説明（Interface Description）]：インターフェイスの説明を指定します。

[L3 インターフェイスの MTU（MTU for L3 interface）]：レイヤ 3 インターフェイスの MTU を入力します。

IPv4セカンダリGW1：追加のサブネットのゲートウェイIPアドレスを入力します。

[IPv4 セカンダリ GW2（IPv4 Secondary GW2）]：追加のサブネットのゲートウェイ IP アドレスを入力します。

[詳細（Advanced）]タブ：オプションとして、**[詳細（Advanced）]**タブをクリックしてプロファイルの詳細設定を指定できます。次のオプションがあります。

- ARP 抑制
- DHCPv4 サーバー 1 および DHCPv4 サーバー 2：最初と 2 番目の DHCP サーバーの DHCP リレー IP アドレスを入力します。
- DHCPv4サーバVRF：DHCPサーバのVRF IDを入力します。
- DHCP リレー インターフェイスのループバック ID：DHCP リレー インターフェイスのループバック ID を入力します。
- ルーティング タグ：ルーティング タグは自動入力されます。このタグは、各ゲートウェイの IP アドレス プレフィックスに関連付けられます。
- [TRM が有効（TRM enable）]：TRM 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。

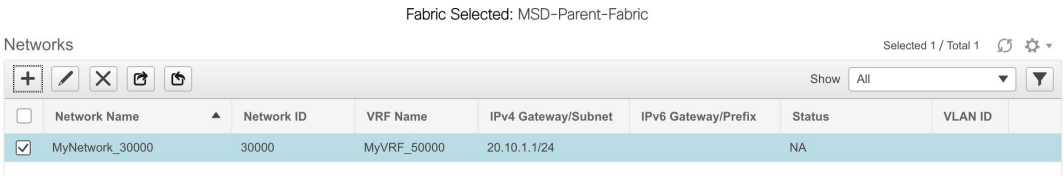
  詳細については、テナント ルーテッド マルチキャストの概要, on page 176を参照してください。
- L2 VNI ルート ターゲットの両方が有効：すべての L2 仮想ネットワークのルート ターゲットの自動インポートとエクスポートを有効にするには、このチェックボックスをオンにします。

Note Cisco DCNM リリース 11.5(1) 以降、**[ボーダーで L3 ゲートウェイを有効にする（Enable L3 Gateway on Border）]** フィールドは、MSD ネットワーク設定の一部として使用できません。ボーダー スイッチのレイヤ 3 ゲートウェイをファブリック レベルで有効にすることができます。詳細については、スタンドアロン ファブリック向けのネットワークの作成, on page 275を参照してください。

MSD ファブリック レベルで **[ボーダーで L3 ゲートウェイを有効にする（Enable L3 Gateway on Border）]** チェックボックスをオンにして、Cisco DCNM リリース 11.5(1) にアップグレードしようとすると、アップグレード中に MSD ファブリック レベルから自動的に削除されます。

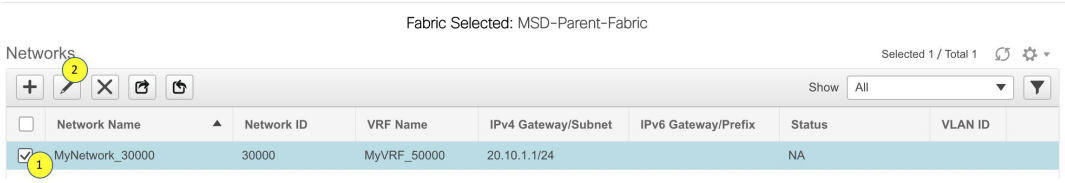
- [ネットワークの作成（Create Network）] 画面のサンプル：

5. [ネットワークの作成（Create Network）] をクリックします。画面の右下に、ネットワークが作成されたことを示すメッセージが表示されます。新しいネットワーク（*MyNetwork_30000*）は、表示される [ネットワーク（Networks）] ページに表示されます。

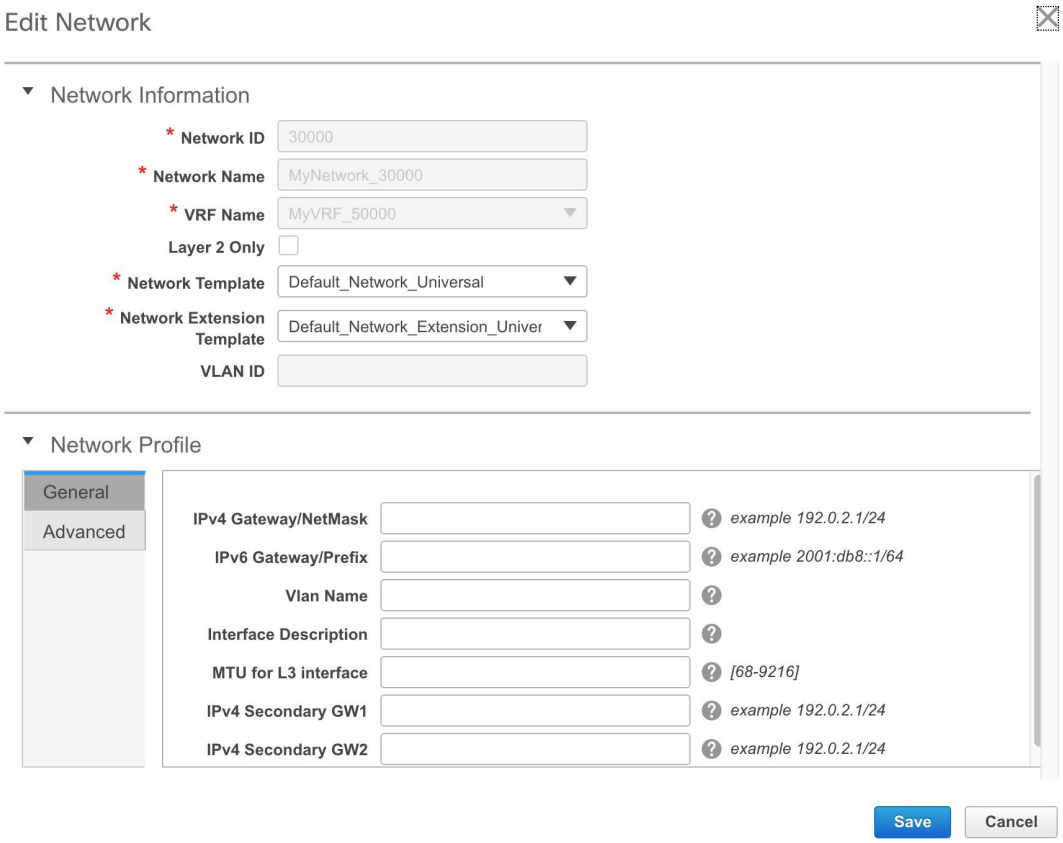


MSD ファブリックでのネットワークの編集

1. MSD ファブリックの [ネットワーク（Networks）] 画面で、編集するネットワークを選択し、画面の左上にある [編集（Edit）] アイコンをクリックします。



[ネットワークの編集（Edit Network）] 画面が表示されます。



MSD ファブリック ネットワークでは、**ネットワーク プロファイル**を一部だけ（**[一般（General）]** タブと **[詳細（Advanced）]** タブで）編集することができます。

2. 画面の右下の **[保存（Save）]** ボタンをクリックして、アップデートを保存します。

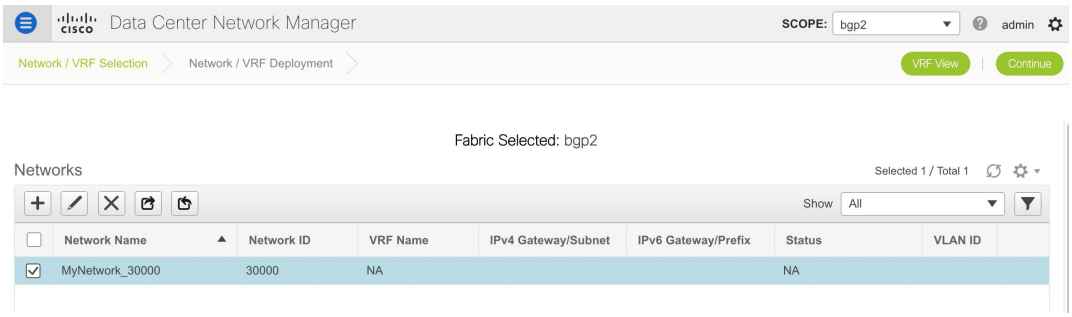
MSD-Parent-Fabric から Member1 へのネットワーク継承

MSD-Parent-Fabric ファブリックには、1 つのメンバー ファブリック *Member1* が含まれています。[ファブリックの選択（Select a Fabric）] ページに移動して、*Member1* ファブリックにアクセスします。

1. **[制御（Control）]** > **[ネットワーク（Networks）]**（**[ファブリック（Fabrics）]** サブメニューの下）をクリックします。

   [ネットワーク（Networks）] 画面が表示されます。

2. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[ネットワーク（Networks）]** 画面が更新され、選択したファブリックのネットワークが一覧表示されます。

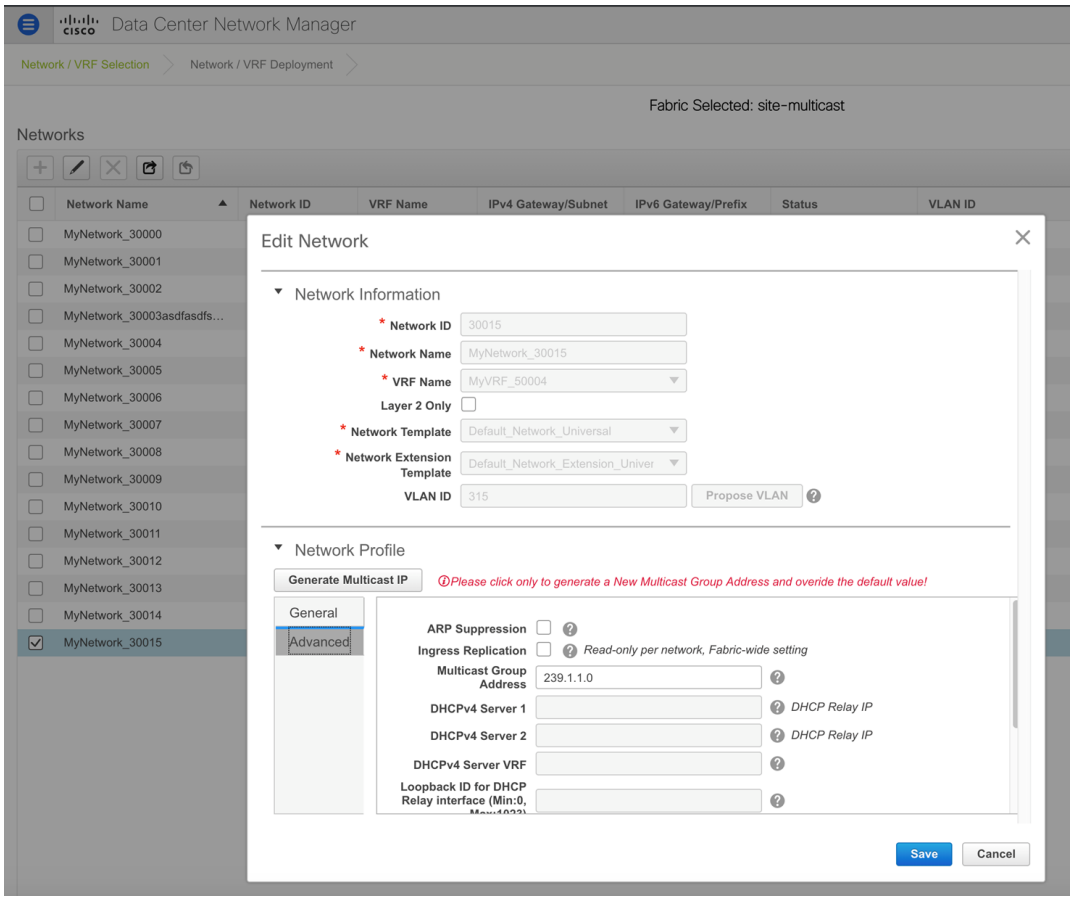


メンバー ファブリックでのネットワークの編集

MSD には複数のファブリックを含めることができます。これらのファブリックは、マルチキャストまたは入力レプリケーションを介して BUM トラフィックを転送します。すべてのファブリックが BUM トラフィックにマルチキャストを使用する場合でも、これらのファブリック内のマルチキャスト グループは同じである必要はありません。

MSD でネットワークを作成すると、すべてのメンバーファブリックに継承されます。ただし、マルチキャスト グループ アドレスは、ファブリック インスタンス ごとの変数です。マルチキャスト グループ アドレスを編集するには、メンバー ファブリックに移動してネットワークを編集する必要があります。**[マルチキャスト グループ アドレス（Multicast Group Address）]** フィールドの詳細については、スタンドアロン ファブリックのネットワークの作成を参照してください。

1. ネットワークを選択し、ウィンドウの左上にある **[編集（Edit）]** オプションをクリックします。**[ネットワークの編集（Edit Network）]** ウィンドウが表示されます。
2. 次のいずれかの方法でマルチキャスト グループ アドレスを更新します。
   - **[ネットワーク プロファイル（Network Profile）]** で、**[マルチキャスト IP の生成（Generate Multicast IP）]** ボタンをクリックして、選択したネットワークの新しいマルチキャスト グループ アドレスを生成し、**[保存（Save）]** をクリックします。
   - **[ネットワーク プロファイル（Network Profile）]** セクションの **[詳細（Advanced）]** タブをクリックし、マルチキャスト グループ アドレスを更新して、**[保存（Save）]** をクリックします。



Note **[マルチキャスト IP の生成（Generate Multicast IP）]** オプションは、メンバー ファブリック ネットワークでのみ使用でき、MSD ネットワークでは使用できません。

MSD およびメンバー ファブリックでのネットワークの削除

ネットワークを削除できるのは MSD ファブリックからだけであり、メンバー ファブリックからは削除できません。MSD ファブリック内のネットワークおよび対応する VRF を削除するには、次の手順に従います。

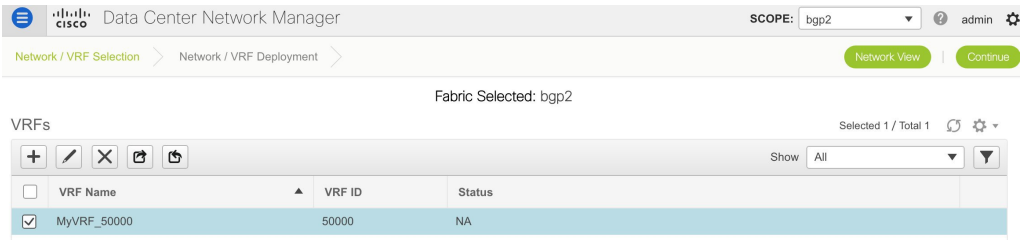
1. 削除する前に、それぞれのファブリック デバイスでネットワークを展開解除します。
2. MSD ファブリックからネットワークを削除します。ネットワークを削除するには、[ネットワーク（Networks）] 画面の左上にある削除（**[X]**）オプションを使用します。複数のネットワークを一度に削除することもできます。

Note MSD ファブリックからネットワークを削除すると、そのネットワークはメンバー ファブリックからも自動的に削除されます。

3. 削除する前に、それぞれのファブリック デバイスで VRF を展開解除します。
4. 画面の左上にある削除（**[X]**）オプションを使用して、MSD ファブリックから VRF を削除します。複数の VRF インスタンスを一度に削除することもできます。

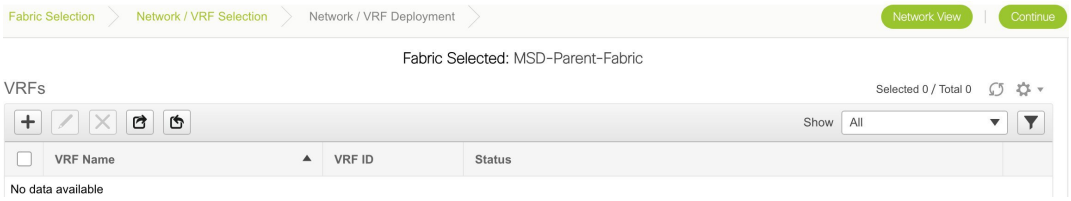
MSD ファブリックでの VRF の作成

1. MSD ファブリックの [ネットワーク（Networks）] ページで、画面の右上にある **[VRF ビュー（VRF View）]** ボタンをクリックして VRF を作成します。
   a. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[VRF（VRFs）]** 画面が更新され、選択したファブリックの VRF が一覧表示されます。



   b. ドロップダウン ボックスから MSD ファブリック（*MSD-Parent-Fabric*）を選択し、**[続行（Continue）]** をクリックします。[ネットワーク（Networks）] ページが表示されます。
   c. [ネットワーク（Networks）] ページの右上にある **[VRF ビュー（VRF View）]** をクリックします。

   [VRF] ページが表示されます。これには、MSD ファブリック用に作成された VRF のリストが表示されます。最初、この画面にはエントリがありません。



2. 画面の左上にある **[+]** ボタンをクリックして、VRF を MSD ファブリックに追加します。[VRF の作成 (Create VRF)] 画面が表示されます。ほとんどのフィールドは自動入力されます。

   この画面のフィールドは次のとおりです。

   VRF ID と **VRF 名**：VRF の ID と名前です。

   VRF ID は、テナントの VRF VNI または L3 VNI です。

Note 使いやすいように、ネットワークの作成時に VRF 作成オプションも使用できます。

[VRF テンプレート（VRF Template）]：これは *Default_VRF* テンプレートに入力されます。

[VRF 拡張テンプレート（VRF Extension Template）]：このテンプレートを使用すると、メンバー ファブリック間の VRF を拡張できます。

3. **[全般（General）]** タブ：VRF に関連付けられた VLAN の VLAN ID、対応するレイヤ 3 仮想インターフェイス、および VRF ID を入力します。

4. **[詳細（Advanced）]** タブ

   [ルーティング タグ（Routing Tag）]：VLAN が複数のサブネットに関連付けられている場合、このタグは各サブネットの IP プレフィックスに関連付けられます。このルーティング タグは、オーバーレイ ネットワークの作成にも関連付けられています。

   [再配布直接ルート マップ（Redistribute Direct Route Map）]：VRF でルートを再配布するためのルート マップ名を指定します。

   [最大 BGP パス（Max BGP Paths）] および **[最大 iBGP パス（Max iBGP Paths）**：最大 BGP および iBGP パスを指定します。

   [TRM の有効（TRM Enable）]：TRM 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。

   TRM を有効にする場合は、RP アドレスとアンダーレイ マルチキャスト アドレスを入力する必要があります。

   詳細については、テナント ルーテッド マルチキャストの概要, on page 176を参照してください。

   [RP が外部（Is RP External）]：ファブリックに対して RP が外部である場合、このチェックボックスを有効にします。このフィールドのチェックがオフの場合、RP はすべての VTEP に分散されます。

   RP アドレス：RP の IP アドレスを指定します。

   RP ループバック ID：**RP が外部** が有効化されていない場合、RP のループバック ID を指定します。

   [アンダーレイ マルチキャスト アドレス（Underlay Multicast Address）]：VRF に関連付けられたマルチキャスト アドレスを指定します。マルチキャスト アドレスは、ファブリック アンダーレイでマルチキャスト トラフィックを転送するために使用します。

Note ファブリック設定画面の **[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]** フィールドのマルチキャスト アドレスは、このフィールドに自動的に入力されます。この VRF に別のマルチキャスト グループ アドレスを使用する必要がある場合は、このフィールドを上書きできます。

[オーバーレイ マルチキャスト グループ（Overlay Multicast Groups）]：指定した RP のマルチキャスト グループ サブネットを指定します。値は「ip pim rp-address」コマンドのグループ範囲です。フィールドが空の場合、デフォルトで 224.0.0.0/24 が使用されます。

[IPv6 リンク ローカル オプションの有効化（Enable IPv6 link-local Option）]：このチェックボックスをオンにすると、VRF SVI で IPv6 リンク ローカル オプションが有効になります。このチェックボックスをオフにすると、IPv6 転送が有効になります。

[ホスト ルートのアドバタイズ（Advertise Host Routes）]：エッジ ルータへの /32 および /128 ルートのアドバタイズメントを制御するには、このチェックボックスをオンにします。

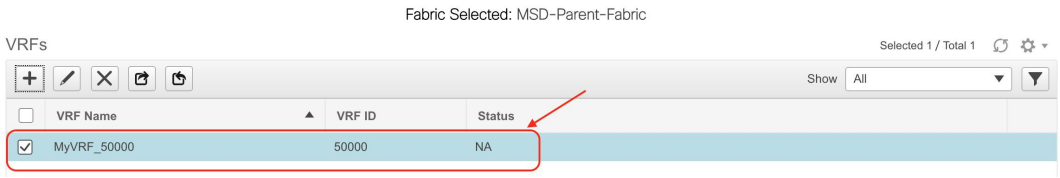
[デフォルト ルートのアドバタイズ（Advertise Default Route）]：このチェックボックスを選択して、ファブリック内のデフォルト ルートのアドバタイズを制御します。

サンプル スクリーンショット：

[Advanced] タブ：

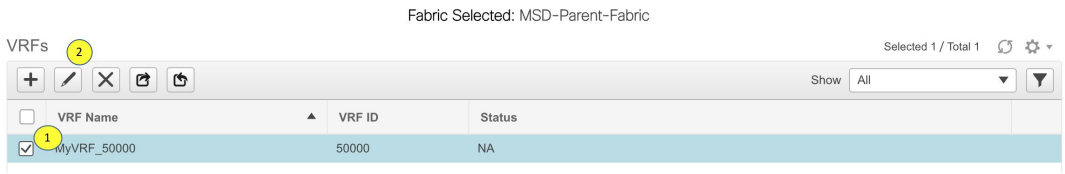
5. **[VRF の作成（Create VRF）]** をクリックします。

   MyVRF_50000 VRF が作成され、VRFs ページに表示されます。

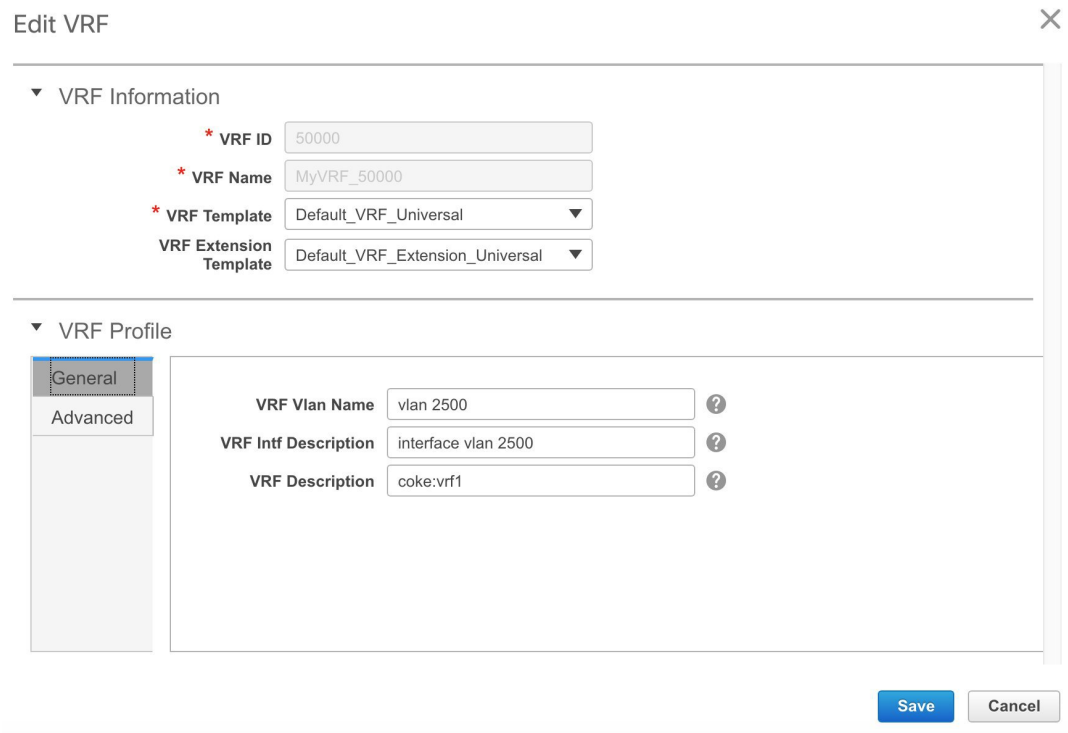


MSD ファブリックでの VRF の編集

1. MSD ファブリックの [VRF] 画面で、編集する VRF を選択し、画面の左上にある [編集（Edit）] アイコンをクリックします。



   [VRF の編集（Edit VRF）] 画面が表示されます。



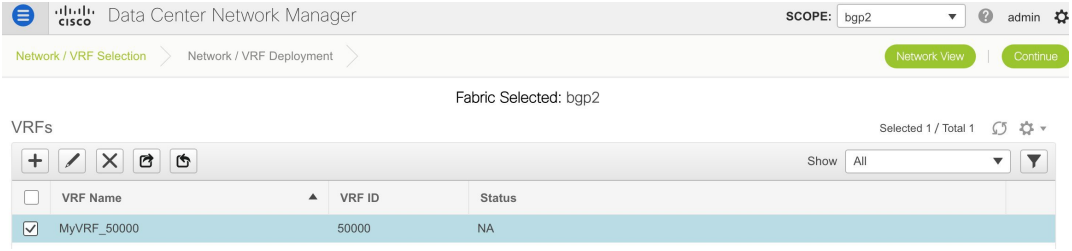
[VRF プロファイル（VRF Profile）] の部分（**[全般（General）]** タブと **[詳細（Advanced）]** タブ）を編集することができます。

2. 画面の右下の **[保存（Save）]** ボタンをクリックして、アップデートを保存します。

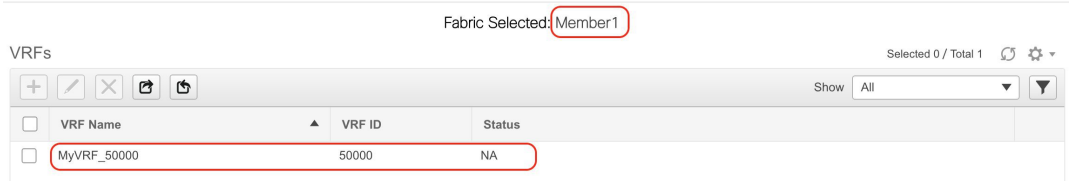
MSD-Parent-Fabric から Member1 への VRF 継承

MSD-Parent-Fabric には、1 つのメンバー ファブリック *Member1* が含まれています。メンバー ファブリック ページにアクセスするには、次の手順を実行します。

1. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[VRF（VRFs）]** 画面が更新され、選択したファブリックの VRF が一覧表示されます。



2. **[VRF ビュー（VRF View）]** ボタンをクリックします。[VRF] ページで、MSD 用に作成された VRF がそのメンバーに継承されていることがわかります。



MSD およびメンバー ファブリックでの VRF の削除

ネットワークを削除できるのは MSD ファブリックからだけであり、メンバー ファブリックからは削除できません。MSD ファブリック内のネットワークおよび対応する VRF を削除するには、次の手順に従います。

1. 削除する前に、それぞれのファブリック デバイスでネットワークを展開解除します。
2. MSD ファブリックからネットワークを削除します。
3. 削除する前に、それぞれのファブリック デバイスで VRF を展開解除します。
4. 画面の左上にある削除（**[X]**）オプションを使用して、MSD ファブリックから VRF を削除します。複数の VRF インスタンスを一度に削除することもできます。

Note MSD ファブリックから VRF を削除すると、メンバー ファブリックからも自動的に削除されます。

メンバー ファブリックでの VRF の編集

メンバー ファブリック レベルで VRF パラメータを編集することはできません。MSD ファブリックの VRF 設定を更新します。すべてのメンバー ファブリックが自動的に更新されます。

メンバー ファブリックでの VRF の削除

メンバーファブリック レベルで VRF を削除することはできません。MSD ファブリックで VRF を削除します。削除された VRF は、すべてのメンバー ファブリックから自動的に削除されます。

以下の手順 1 について説明します。手順 2 の情報については、次のサブセクションで説明します。

1. MSD ファブリックにネットワークと VRF を作成します。
2. メンバー ファブリックのデバイスにネットワークと VRF を展開します。1 回に付き 1 つのファブリックを展開します。

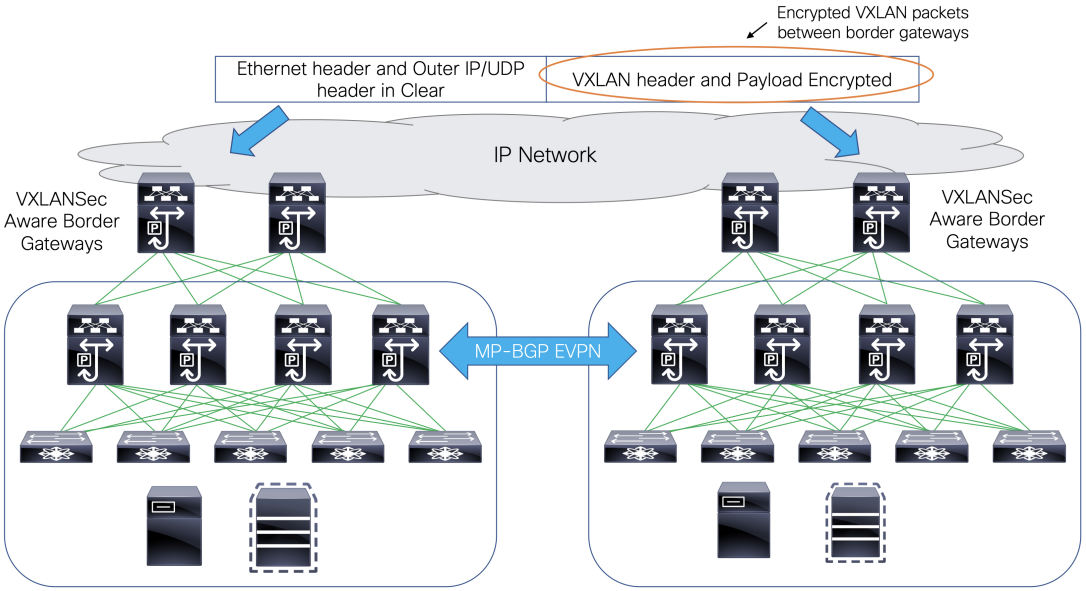
メンバー ファブリックでのネットワークと VRF の展開と展開解除

メンバー ファブリックは、MSD ファブリック用に作成されたネットワークと VRF を継承するため、開始する前に、MSD ファブリック レベルでネットワークを作成していることを確認してください。

Note メンバー ファブリックでのネットワークと VRF の展開（および展開解除）は、スタンドアロン ファブリックで説明したものと同じです。「ネットワークおよび VRF の作成と展開」を参照してください。

マルチサイト展開での CloudSec のサポート

CloudSec 機能は、異なるファブリック内のボーダー ゲートウェイ デバイス間の送信元から宛先へのパケット暗号化をサポートすることにより、マルチサイト展開で安全なデータセンター相互接続を可能にします。



CloudSec 機能は、Cisco NX-OS リリース 9.3(5) 以降を搭載した Cisco Nexus 9000 シリーズ FX2 プラットフォームでサポートされています。FX2 プラットフォームであり、Cisco NX-OS リリース 9.3(5) 以降を実行するボーダー ゲートウェイ、ボーダー ゲートウェイ スパイン、およびボーダー ゲートウェイ スーパースパインは、CloudSec 対応スイッチと呼ばれます。

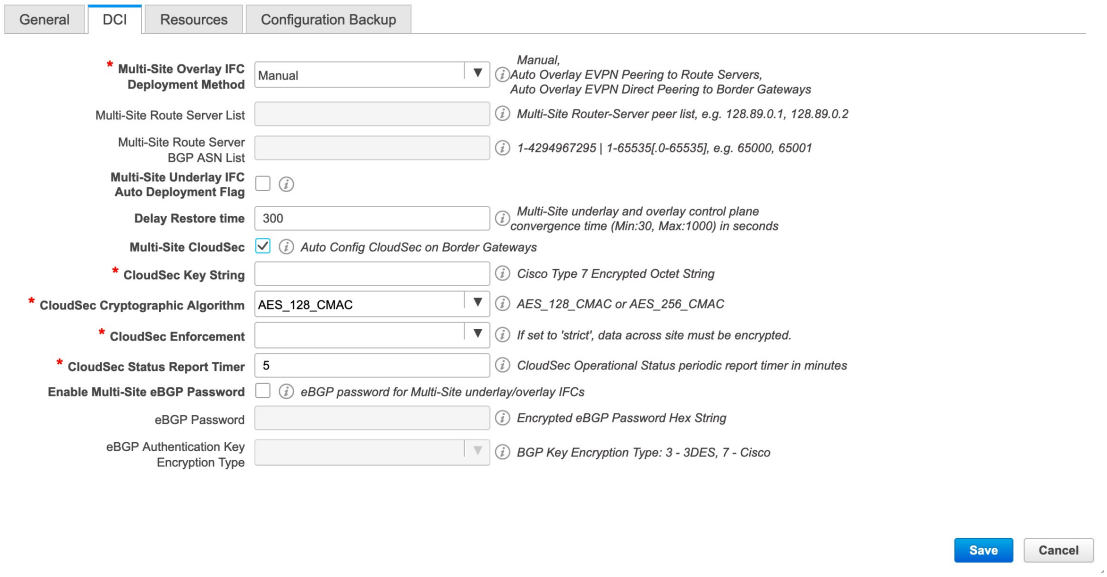
Cisco DCNM リリース 11.4(1) には、MSD ファブリックで CloudSec を有効にするオプションが用意されています。

（注） CloudSec セッションは、2 つの異なるサイトのボーダー ゲートウェイ（BGW）間の DCI を介したポイントツーポイントです。サイト間のすべての通信は、VIP の代わりにマルチサイト PIP を使用します。CloudSec を有効にするには、VIP から PIP に切り替える必要があります。これにより、サイト間のデータ フローのトラフィックが中断される可能性があります。したがって、CloudSec の有効または無効の切り替えは、メンテナンス ウィンドウ中に行うことをお勧めします。

CloudSec 機能を構成する方法を示すビデオを見ることもできます。「ビデオ：Cisco DCNM での CloudSec の構成」を参照してください。

MSD で CloudSec を有効にする

[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）] に移動します。**[ファブリックの作成（Create Fabric）]** をクリックして新しい MSD ファブリックを作成するか、**[ファブリックの編集（Edit Fabric）]** をクリックして既存の MSD ファブリックを編集することができます。



[DCI] タブで、CloudSec 構成の詳細を指定できます。

[マルチサイト（Multi-Site CloudSec）]：ボーダー ゲートウェイで CloudSec 構成を有効にします。このフィールドを有効にすると、CloudSec の残りのフィールドが編集可能になります。

[マルチサイト（Multi-Site CloudSec）]：ボーダー ゲートウェイで CloudSec 構成を有効にします。このフィールドを有効にすると、CloudSec の残りの 3 つのフィールドが編集可能になります。

Cloudsec が MSD レベルで有効になっている場合、DCNM は、すべての Cloudsec 対応ゲートウェイのアップリンクで、**dci-advertise-pip**（**evpn multisite border-gateway**の下） と 、**tunnel-encryption** も有効にします。

[保存と展開（Save & Deploy）] をクリックすると、ボーダーゲートウェイ スイッチの **[構成のプレビュー（Preview Config）]** ウィンドウでこれらの構成を確認できます。

[注（Note）]：ボーダーゲートウェイに vPC がある場合、または TRM が有効になっている場合、つまり、マルチサイト オーバーレイ IFC で TRM が有効になっている場合、CloudSec はサポートされません。このシナリオで CloudSec が有効になっている場合、適切な警告またはエラー メッセージが生成されます。

[CloudSec キー文字列（CloudSec Key String）]：16 進キー文字列を指定します。**AES_128_CMAC** を選択した場合は 66 文字の 16 進文字列を入力し、**AES_256_CMAC** を選択した場合は 130 文字の 16 進文字列を入力します。

[CloudSec 暗号化アルゴリズム（CloudSec Cryptographic Algorithm）]：**AES_128_CMAC** または **AES_256_CMAC** を選択します。

[CloudSec 強制（CloudSec Enforcement）]：CloudSec を厳密に強制するか、緩和するかを指定します。

[厳密（strict）]：MSD のファブリック内のすべてのボーダー ゲートウェイに CloudSec 構成を展開します。CloudSec をサポートしていないボーダー ゲートウェイがある場合、エラー メッセージが生成され、構成はどのスイッチにもプッシュされません。

[厳密（strict）] が選択されている場合、**tunnel-encryption must-secure** CLI が MSD 内の CloudSec 対応ゲートウェイにプッシュされます。

[緩和（loose）]：MSD のファブリック内のすべてのボーダー ゲートウェイに CloudSec 構成を展開します。CloudSec をサポートしていないボーダー ゲートウェイがある場合は、警告メッセージが生成されます。この場合、CloudSec 構成は、CloudSec をサポートするスイッチにのみ展開されます。**[緩和（loose）]** が選択されていて、**tunnel-encryption must-secure** CLI が存在する場合は削除されます。

（注） CloudSec をサポートするボーダー ゲートウェイを備えた MSD には、少なくとも 2 つのファブリックが必要です。CloudSec 対応デバイスを備えたファブリックが 1 つしかない場合は、次のエラー メッセージが生成されます。

CloudSec には、CloudSec をサポートできるサイトが少なくとも 2 つ必要です（CloudSec needs to have at least 2 sites that can support CloudSec）。

このエラーを解消するには、CloudSec をサポートするか、CloudSec を無効にできるサイトが少なくとも 2 つあるという条件を満たす必要があります。

[CloudSec ステータス レポート タイマー（CloudSec Status Report Timer）]：CloudSec 動作ステータス定期レポート タイマーを分単位で指定します。この値は、DCNM がスイッチから CloudSec ステータス データをポーリングする頻度を指定します。デフォルト値は 5 分で、範囲は 5 ～ 60 分です。

DCNM の CloudSec 機能を使用すると、MSD 内のすべてのゲートウェイが同じキーチェーン（および1つのキー文字列のみ）を持ち、ポリシーを持つようにすることができます。DCNM に1つのキーチェーン文字列を指定して、キーチェーン ポリシーを形成することができます。

DCNM は、すべてのデフォルト値を使用して encryption-policy を形成します。DCNM は、同じキー チェーン ポリシー、同じ暗号化ポリシー、および暗号化ピア ポリシーを各 CloudSec 対応ゲートウェイにプッシュします。各ゲートウェイには、CloudSec 対応で、同じキーチェーンと同じキー ポリシーを使用する encryption-peer ポリシーが、リモート ゲートウェイごとに 1 つあります。

MSD ファブリック全体に同じキーを使用したくない場合、またはすべてのサイトのサブセットでのみ CloudSec を有効にしたい場合は、**switch_freeform** を使用して、CloudSec 構成をスイッチに手動でプッシュできます。

switch_freeform のすべての CloudSec 構成をキャプチャします。

たとえば、次の設定は **switch_freeform** ポリシーに含まれています。

```
feature tunnel-encryption
evpn multisite border-gateway 600
  dci-advertise-pip
tunnel-encryption must-secure-policy
tunnel-encryption policy CloudSec_Policy1
tunnel-encryption source-interface loopback20
key chain CloudSec_Key_Chain1 tunnel-encryption
  key 1000
    key-octet-string 7 075e731f1a5c4f524f43595f507f7d737062677147524054590 70b0b0701585440
 cryptographic-algorithm AES_128_CMA
tunnel-encryption peer-ip 192.168.0.6
  keychain CloudSec_Key_Chain1 policy CloudSec_Policy1
```

次のような構成を生成するアップリンク インターフェイス ポリシーのフリーフォーム構成に **tunnel-encryption** を追加します。

```
interface ethernet1/13
  no switchport
  ip address 192.168.1.14/24 tag 54321
  evpn multisite dci-tracking
  tunnel-encryption
  mtu 9216
  no shutdown
```

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 （350ページ）を参照してください。

CloudSec 設定がスイッチに追加または削除されると、DCI アップリンクがフラップし、マルチサイト BGP セッション フラッピングがトリガーされます。既存のクロス サイト トラフィックがあるマルチサイトの場合、この移行中にトラフィックの中断が発生します。したがって、メンテナンス期間中に移行を行うことをお勧めします。

CloudSec 構成の MSD ファブリックを DCNM に移行する場合、Cloudsec 関連の構成は、**[switch_freeform]** およびインターフェイス自由形式構成でキャプチャされます。MSD ファブリック設定で Multi-Site Cloudsec をオンにする必要はありません。さらにファブリックを追加し、既存のものとキーを含む同じ CloudSec ポリシーを共有する CloudSec トンネルを確立する場合は、MSD ファブリック設定で CloudSec 構成を有効にすることができます。MSD ファブリック設定の CloudSec パラメータは、スイッチの既存の CloudSec 設定と一致する必要があります。CloudSec 構成は既にフリーフォーム構成に取り込まれており、MSD で CloudSec を有効にすると構成インテントも生成されます。したがって、二重のインテントが生じます。たとえば、MSD 設定で CloudSec キーを変更する場合、DCNM は **switch_freeform** の構成を変更しな

いため、CloudSec 自由形式構成を削除する必要があります。そうしないと、MSD ファブリック設定のキーがフリーフォーム構成のキーと競合します。

CloudSec の動作状態の表示

Cisco DCNM 11.5(1) 以降では、MSD ファブリックで CloudSec が有効になっている場合、**[CloudSec 操作ビュー（CloudSec Operational View）]** を使用して CloudSec セッションの操作ステータスを確認できます。

手順

ステップ 1 MSD ファブリックを選択します。

ファブリック トポロジ ウィンドウが表示されます。

ステップ 2 **[アクション（Actions）]** ペインで **[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 **[CloudSec 操作ビュー（CloudSec Operational View）]** タブを選択します。

ステップ 4 CloudSec が無効になっている場合、**[CloudSec 操作ビュー（CloudSec Operational View）]** タブは表示されません。

[操作ビュー（Operational View）] タブには、次のフィールドと説明があります。

フィールド	説明
Fabric Name（ファブリック名）	CloudSec セッションを持つファブリックを指定します。
セッション	CloudSec セッションに関係するファブリックとボーダー ゲートウェイ スイッチを指定します。
リンク ステータス	CloudSec セッションのステータスを指定します。この状態は次のいずれかになります。 • Up：スイッチ間で CloudSec セッションが正常に確立されています。 • Down：CloudSec セッションは動作していません。
稼働時間	CloudSec セッションの稼働時間を指定します。具体的には、最後の Rx および Tx セッションがフラップしてからの稼働時間であり、2 つのセッションのうち小さい方の値が表示されます。
動作理由	CloudSec セッション状態のダウン理由を指定します。

これらすべての列が並べ替え可能です。

（注） ファブリックで CloudSec が有効になった後、セッションが作成され、次のステータス ポーリングが発生するまでは、動作ステータスを使用できない場合があります。

CloudSec セッションのトラブルシューティング

CloudSec セッションが停止している場合は、プログラマブル レポートを使用してその詳細を確認できます。

手順

ステップ 1 **[アプリケーション（Applications）] > [プログラマブル レポート（Programmable report）]** に移動します。

ステップ 2 **[レポートの作成（Create Report）]** アイコンをクリックします。

ステップ 3 レポート名を指定し、レポートジョブを実行するMSDファブリックを選択して、**[次へ（Next）]** をクリックします。

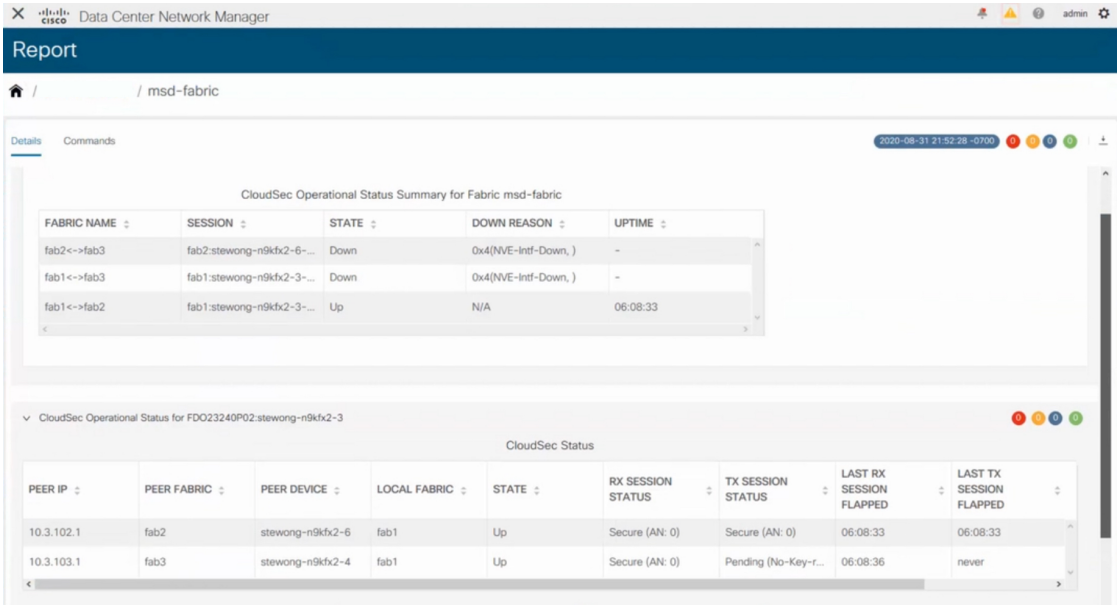
ステップ 4 **[テンプレート（Template）]** ドロップダウン リストから、**fabric_cloudsec_oper_status** を選択して **[ジョブの作成（Create Job）]** をクリックします。

レポートが正常に生成されると、ステータスは成功を示す緑色のチェックマークに変わります。

ステップ 5 [レポート（report）] をクリックして表示します。このレポートは、**CloudSec 操作ビュー（CloudSec Operation View）]** タブに似ています。

ステップ 6 CloudSecセッション ステータスの詳細を表示するには、**[詳細の表示（View Details）]** をクリックします。

ステップ 7 セッションの動作ステータスをクリックして、各ピア ファブリックおよびデバイスのCloudSecセッションに関する詳細情報を表示します。



MSD からのファブリックの削除

MSD ファブリックからファブリックを削除するには、次の手順を実行します。

Before you begin

削除するファブリックのボーダー スイッチに VRF が展開されていないことを確認してください。詳細については、メンバー ファブリックでのネットワークと VRF の展開と展開解除, on page 147を参照してください。

Note Cisco DCNM リリース 11.4(1) 以降、MSD から個々のファブリックを削除した後、アンダーレイおよびオーバーレイ IFC が削除されます。IFC が拡張されている場合、ファブリックの削除を禁止するエラーが報告されます。

Procedure

ステップ 1 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウで、MSD ファブリックをクリックします。

ステップ 2 **[アクション（Actions）]** メニューで **[ファブリックの移動（Move Fabric）]** をクリックします。

ステップ 3 **[ファブリックの移動（Move Fabric）]** ウィンドウで、削除するファブリックのそれぞれのラジオ ボタンを選択し、**[削除（Remove）]** をクリックします。

ファブリックの削除通知ウィンドウで、**[閉じる（Close）]** をクリックします。

ステップ 4 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウで MSD の **[保存と展開（Save & Deploy）]** をクリックします。

ステップ 5 **[構成の展開（Config Deployment）]** ウィンドウで **[展開構成（Deploy Config）]** をクリックします。

[閉じる（Close）] をクリックします。

ステップ 6 MSD から削除したファブリックに移動し、**[保存と展開（Save & Deploy）]** をクリックします。

ステップ 7 **[構成の展開（Config Deployment）]** ウィンドウで **[展開構成（Deploy Config）]** をクリックします。

[閉じる（Close）] をクリックします。

スタンドアロン ファブリック（既存のネットワークと VRF を使用）を MSD ファブリックに移動する

既存のネットワークと VRF を持つスタンドアロン ファブリックをメンバーとして MSD ファブリックに移動する場合は、共通のネットワーク（つまり、L2 VNI と L3 VNI 情報）、エニー

キャスト ゲートウェイ MAC、VRF とネットワーク テンプレートがファブリックと MSD 全体で同じであることを確認してください。DCNMは、スタンドアロンファブリック（ネットワークおよび VRF 情報）を MSD ファブリックの（ネットワークおよび VRF 情報）に対して検証して、エントリの重複を回避します。エントリの重複の例は、2 つの一般的なネットワーク名が異なるネットワーク ID を持っている場合です。競合があるかの検証後、スタンドアロンファブリックはメンバー ファブリックとして MSD ファブリックに移動されます。詳細：

- MSD ファブリックは、MSD ファブリックに存在しないスタンドアロン ファブリックのネットワークと VRF を継承します。それから、これらのネットワークと VRF は、メンバー ファブリックに継承されます。
- 新しく作成されたメンバー ファブリックは、MSD ファブリックのネットワークと VRF（新しく作成されたメンバー ファブリックには存在しないもの）を継承します。
- スタンドアロン ファブリックと MSD ファブリックの間に競合がある場合、検証によって、エラー メッセージが表示されます。更新後、メンバー ファブリックを MSD ファブリックに移動すると、移動は成功します。ページの上部に移動が成功したことを示すメッセージが表示されます。

メンバー ファブリックをスタンドアロン ステータスに戻すと、ネットワークと VRF はそのまま残りますが、独立したファブリックのように、MSD ファブリックの範囲外で関連したままになります。

LAN クラシック テンプレートを使用したスイッチ管理

Cisco DCNM リリース 11.4(1) 以降、**[LAN_Classic]** および **[Fabric_Group]** テンプレートを使用して、以前 DCNM クラシック LAN 展開で管理していたスイッチを管理できます。

[LAN_Classic] ファブリック テンプレートは、Cisco Nexus スイッチを管理するための汎用ファブリック テンプレートです。

ガイドラインと制約事項

- **[LAN_Classic]** ファブリック テンプレートを使用するファブリックは、**[External_Fabric_11_1]** ファブリック テンプレートを使用するように変更してから、関連するすべての機能を使用することができます。これはサポートされている唯一のファブリック テンプレートの変換であり、元に戻すことはできません。
- **[LAN_Classic]** ファブリックは、MSD ファブリックのメンバーとして追加できます。
- **[LAN_Classic]** ファブリックでは、Cisco Nexus スイッチのみがサポートされています。
- **[ToR]** ロールを持つスイッチがファブリック内にある場合、TOR Auto-Deploy 機能は **[LAN_Classic]** メンバー ファブリックでサポートされます。詳細については「*ToR* スイッチの構成とネットワークの展開」を参照してください。
- 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。

- **[LAN_Classic]** テンプレートの次の機能は、**[External_Fabric_11_1]** テンプレートと同じサポートを提供します。

  サポートされる機能は次のとおりです。

  - 設定コンプライアンス
  - ファブリックのバックアップまたは復元
  - ネットワーク インサイト
  - パフォーマンス モニタリング
  - VMM
  - トポロジ ビュー
  - Kubernetes の可視化
  - RBAC

  詳細については、機能固有のセクションを参照してください。

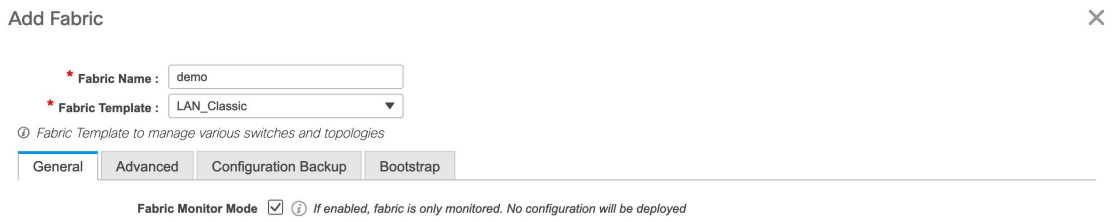
LAN クラシック ファブリックの作成

手順

ステップ 1 **[制御（Control）]** > **[ファブリック（Fabrics）]** > **[ファブリック ビルダ（Fabric Builder）]** に移動します。

ステップ 2 [ファブリックの作成（Create Fabric）] をクリックします。

ステップ 3 ファブリック名を入力し、**[ファブリック テンプレート（Fabric Template）]** ドロップダウンリストから **[LAN_Classic]** を選択します。



ステップ 4 デフォルトでは **[全般（General）]** タブが表示されます。このタブのフィールドは次のとおりです。

[ファブリック モニタ モード（Fabric Monitor Mode）]：DCNM がファブリックを管理する場合は、このチェックボックスをオフにします。ファブリックのモニタリングのみを有効にする場合は、チェックボックスをオンのままにします。この状態では、スイッチに構成を展開できません。

ファブリックで検出する前に、デバイスの構成をプッシュする必要があります。モニタ モードでは構成をプッシュできません。

ステップ 5 [Advanced] 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。

[vPC ピア リンク VLAN（vPC Peer Link VLAN）]：vPC ピア リンク VLAN ID は自動入力されます。正しい値を反映させてフィールドをアップデートします。

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、「VXLAN BGP EVPN ファブリックでの境界プロビジョニングの使用例：MPLS SR および LDP ハンドオフ」の章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 サーバで IP 認証が有効になっている場合に、AAA IP 認証を有効にします。

[トラップホストとして有効にする（Enable as Trap Host）]：トラップホストとして有効にする場合は、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 の有効化（Enable CDP for Bootstrapped Switch）]：管理インターフェイスで CDP を有効にします。

[NX-API の有効化（Enable NX-API）]：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。

[ポートの HTTP で NX-API を有効化する（Enable on NX-API on HTTP）]：HTTP 上の 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、レイヤ 4 ～ レイヤ 7 サービス（L4 ー L7 サービス）、VXLAN OAM など、NX-API を使用し、Cisco DCNM がサポートするアプリケーションは、HTTP ではなく HTTPS の使用を開始します。

（注） [NX-API の有効化（Enable NX-API）] チェックボックスと [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 DCNM は、インバンド接続（スイッチ ループバック、ルーテッド、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、インバンド管理型スイッチの場合、eth2（別名インバンドインターフェイス）を介して DCNM からスイッチ IP に到達可能であることです。この目的のために、DCNM で静的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）]オプションで構成できます。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。DCNM は、インバンド管理されたスイッチ IP が eth2 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すると、DCNM 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 DCNM に入力される目的の基準設定にキャプチャされます。詳細については、外部ファブリックおよび LAN クラシック ファブリックでのインバンド管理 （165 ページ）を参照してください。

（注） 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。DCNM 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。DCNM 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オンにすると、PTP がグローバルに有効になり、コアに面するインターフェイスで有効になります。また、[PTP 送信元ループバック ID（PTP Source Loopback Id）] および [PTP ドメイン ID（PTP Domain Id）] フィールドが編集可能になります。詳細については、外部ファブリックおよび LAN クラシック ファブリック向け高精度時間プロトコル（PTP） （166 ページ）を参照してください。

[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。

[AAA 自由形式の構成（AAA Freeform Config）]：AAA 自由形式の構成を指定します。

ステップ 6 [リソース（Resources）] 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。

[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 ルーティング ループバック IP 範囲（Underlay Routing Loopback IP Range）]：プロトコル ピアリングのループバック IP アドレスを指定します。

[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。

ステップ 7 [設定（Configuration）] 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。

[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。

[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。

[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。

（注） 毎時またはスケジュールされたバックアップは、次の CC の毎時実行後にのみ実行されます。バックアップは、スケジュールされた時間が経過した後にのみ実行され、その時間が経過した後に CC が実行されるたびに実行されます。

バックアップと復元のプロセスは、外部ファブリックのプロセスに似ています。外部ファブリックのバックアップおよび復元に関する詳細については、ファブリックのバックアップと復元 （313 ページ） を参照してください。

ステップ 8 **[ブートストラップ（Bootstrap）]** 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。

ブートストラップの有効化（NX-OS スイッチのみ）（Enable Bootstrap）（For NX-OS Switches Only） ：Cisco Nexus スイッチのみに対してブートストラップ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。

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 サーバー（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）]** フィールドの外部 DHCP サーバーについての情報を入力します。
- [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有効にして、残りの必須フィールドに詳細を入力します。

ローカル DHCP サーバーの有効化（Enable Local DHCP Server） ：ローカル DHCP サーバーを介した自動 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）]** フィールドが無効になります。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。

（注） Cisco DCNM 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 が必須）、またはスイッチがいくつかの IPv6 /64 サブネット内に存在する L3 隣接である場合にのみ、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、DCNM は自動 IP アドレス割り当てにリモートまたは外部 DHCP サーバーを使用します。

[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。プレフィックスは 8 ～ 30 の間である必要があります。

DHCP スコープ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 スコープ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 ー 126 の範囲で指定する必要があります。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 構成の有効化（Enable AAA Config）]：AAA 構成を有効にします。これには、デバイスの起動時に **[詳細（Advanced）]** タブからの AAA 構成が含まれます。

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構成を使用している場合は、このフィールドにこれらの構成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、[Bootstrap 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 **[自由形式の構成（freeform config）]** フィールドに正しいインデントでペーストします。NX-OS スイッチの実行構成に表示されているように正しく行ってください。freeform config は running config と一致する必要があります。詳細については、「スイッチでの自由形式の構成エラーの解決」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 スコープを入力して、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した後で、このフィールドは編集可能になります。

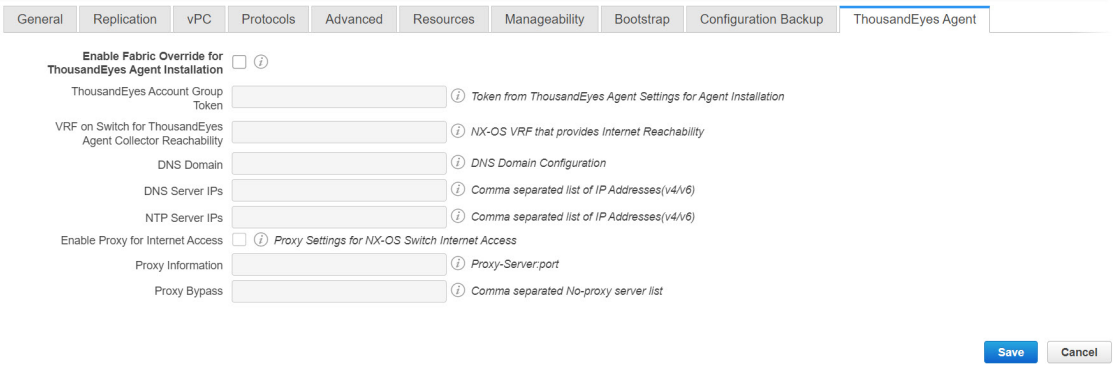
スコープの形式は次の順で定義する必要があります。

[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

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。

ステップ 9 **[ThousandEyes Agent]** タブをクリックします。この機能は、Cisco DCNM リリース 11.5（3）でのみサポートされています。詳細については、「Cisco DCNM での ThousandEyes Enterprise Agent のグローバル設定の構成」を参照してください。



このタブのフィールドは次のとおりです。

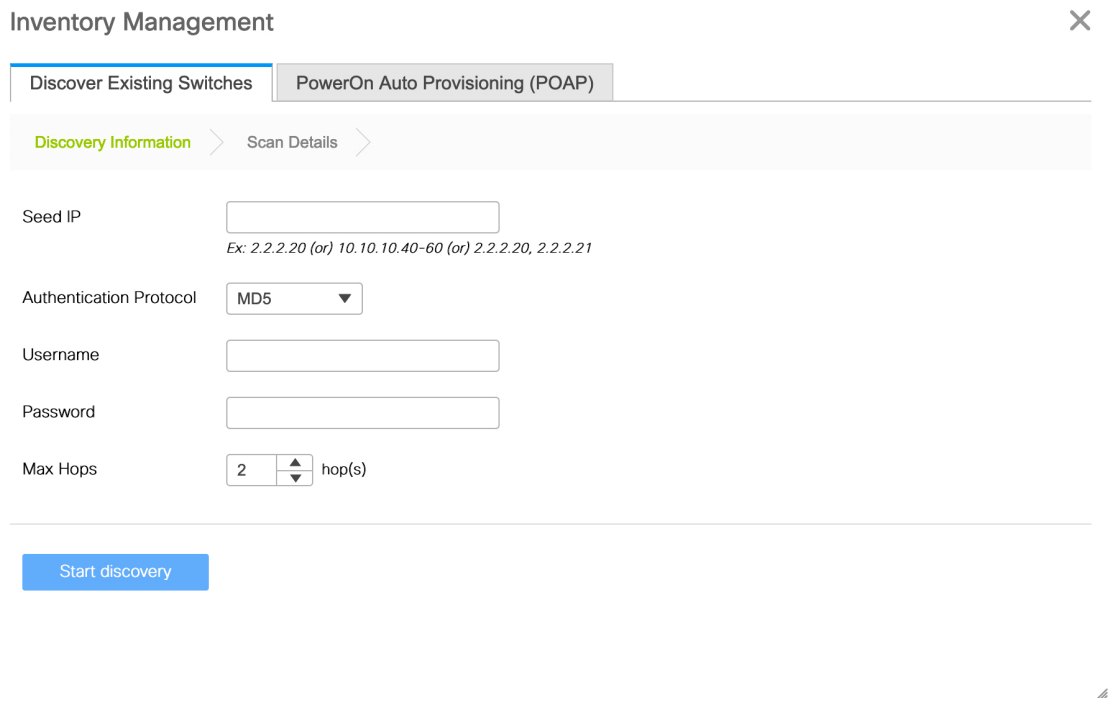
（注） ThousandEyes Agent のファブリック設定はグローバル設定を上書きし、そのファブリック内のスイッチにインストールされているすべての ThousandEyes エージェントに同じ構成を適用します。

- **[ThousandEyes Agent インストールのファブリック オーバーライドを有効にする（Enable Fabric Override for ThousandEyes Agent Installation）]**：チェック ボックスを選択して、ファブリックで ThousandEyes Enterprise Agent を有効にします。
- **[ThousandEyes アカウント グループ トークン（ThousandEyes Account Group Token）]**：インストール用の ThousandEyes Enterprise Agent アカウント グループ トークンを指定します。
- **[ThousandEyes Agent コレクタ到達可能性のスイッチ上の VRF（VRF on Switch for ThousandEyes Agent Collector Reachability）]**：インターネットの到達可能性を提供する VRF データを指定します。
- **[ドメイン ネーム システム（DNS） ドメイン（DNS Domain）]**：スイッチのドメイン ネーム システム（DNS） ドメイン構成を指定します。
- **[ドメイン ネーム システム（DNS） サーバ IP（DNS Server IPs）]**： ドメイン ネーム システム（DNS） サーバの IP アドレス（v4/v6）のカンマ区切りリストを指定します。DNS サーバには、最大 3 つの IP アドレスを入力できます。
- **[NTP サーバ IP（NTP Server IPs）]**： Network Time Protocol (NTP) サーバの IP アドレス（v4/v6）のコンマ区切りリストを指定します。NTP サーバには、最大 3 つの IP アドレスを入力できます。
- **[プロキシを有効にする（Enable Proxy）]**：チェックボックスをオンにして、NX-OS スイッチのインターネット アクセスのプロキシ設定を選択します。
- **[プロキシ情報（Proxy Information）]**：プロキシ サーバのポート情報を指定します。
- **[プロキシ バイパス（Proxy Bypass）]**：プロキシをバイパスするサーバ リストを指定します。

LAN クラシック ファブリックへのスイッチの追加

手順

ステップ 1 スイッチの **[追加（Add）]** をクリックします。**[インベントリ管理（Inventory Management）]** ウィンドウが表示されます。



[表形式ビュー（Tabular View）] > **[スイッチ（Switches）]** > **[+]** をクリックして、スイッチを追加することもできます。

ステップ 2 スイッチの IP アドレス（**[シード IP（Seed IP）]**）を入力します。

ステップ 3 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。

ステップ 4 画面の下部にある **[検出の開始（Start discovery）]** 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。

ステップ 5 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、**[ファブリックにインポート（Import 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 DCNM 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。DCNM がスイッチを検出すると、画面が閉じ、ファブリック画面が再び表示されます。ファブリック画面の中央にスイッチ アイコンが表示されます。

ステップ 6 最新のトポロジ表示を表示するには、トポロジの **[更新（Refresh）]** をクリックします。

詳細については、以下を参照してください。

- 既存のスイッチの検出 （32 ページ）
- 新しいスイッチの検出 （39 ページ）

ファブリック グループの作成とメンバー ファブリックの関連付け

この手順は、**[Fabric_Group]** を作成し、**[LAN_Classic]** ファブリックを追加する方法を示しています。**[Fabric_Group]** テンプレートは、視覚化のために **[LAN_Classic]** ファブリックをグループ化するために使用されます。

次の機能は **[Fabric_Group]** ではサポートされていません。

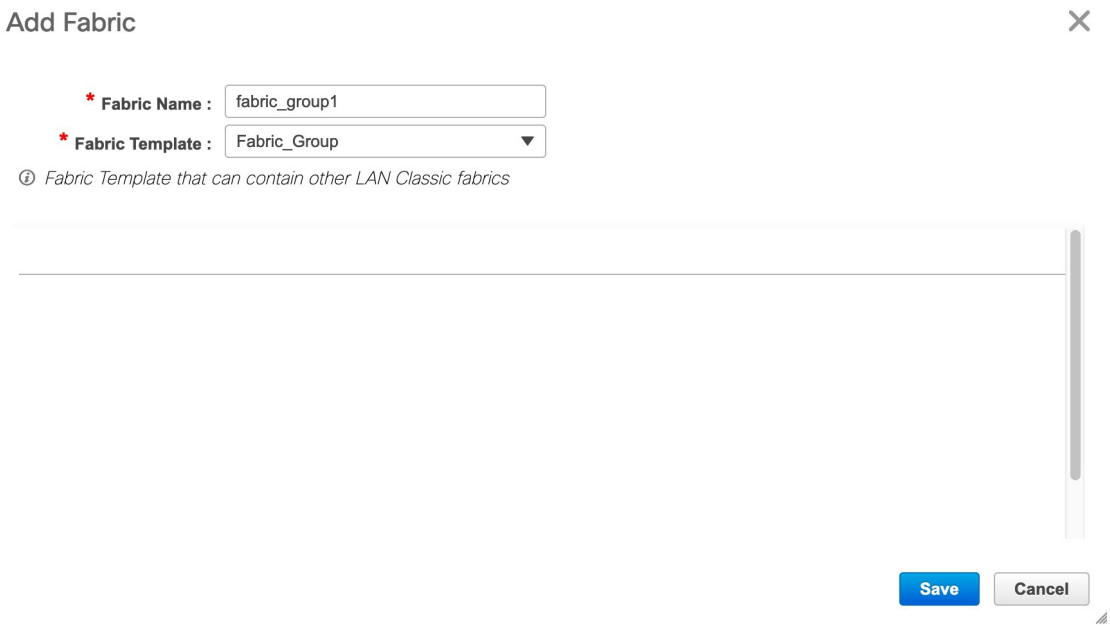
- ファブリックのバックアップと復元
- VXLAN オーバーレイまたは IFC 展開
- ファブリック テンプレートを他のファブリック テンプレートから、または他のファブリック テンプレートに変更する
- **[Fabric_Group]** は構成を管理しないため、**[保存と展開（Save & Deploy）]** をクリックするとエラーが報告されます。

手順

ステップ 1 **[制御（Control）]** > **[ファブリック（Fabrics）]** > **[ファブリック ビルダ（Fabric Builder）]** に移動します。

ステップ 2 [ファブリックの作成（Create Fabric）] をクリックします。

ステップ 3 ファブリック名を入力し、**[ファブリック テンプレート（Fabric Template）]** ドロップダウンリストから **[Fabric_Group]** を選択します。



ステップ 4 [保存（Save）] をクリックします。

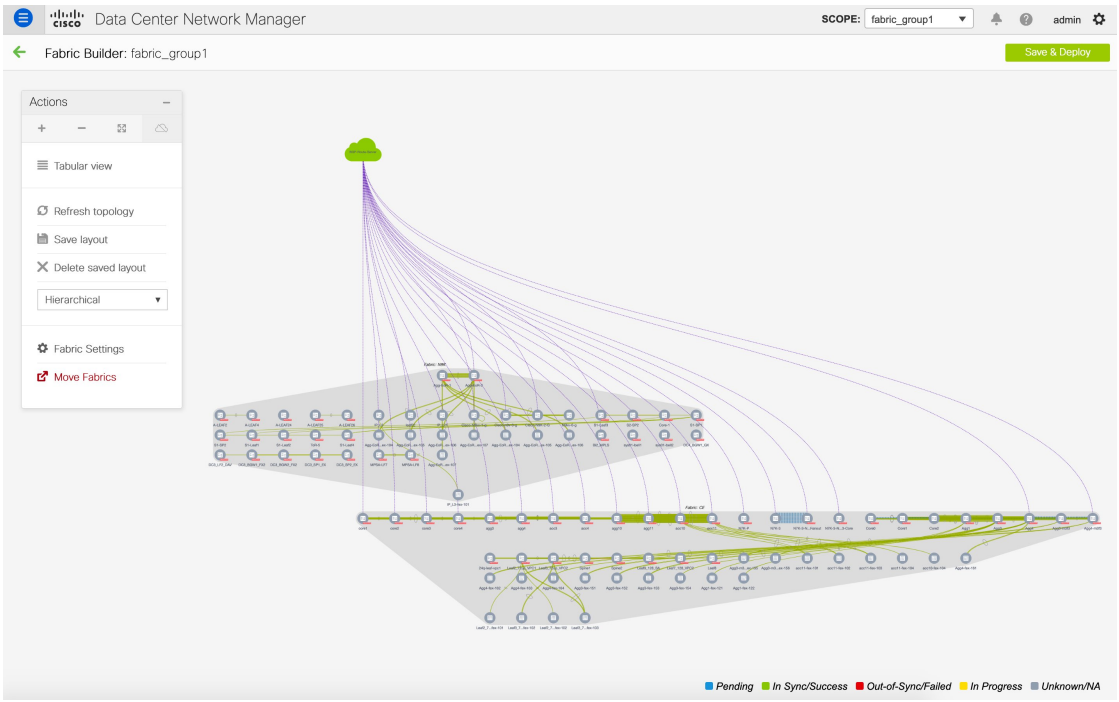
ステップ 5 **[アクション（Actions）]** パネルで、**[ファブリックの移動（Move Fabrics）]** をクリックします。

ステップ 6 **[ファブリックの移動（Move Fabric）]** ウィンドウで **[LAN_Classic]** ファブリックを選択します。

（注） ファブリック グループ内の **[LAN_Classic]** ファブリックのみを選択して追加できます。

ステップ 7 [追加（Add）] をクリックします。

同様に、メンバー ファブリックを選択して **[削除（Remove）]** をクリックすることで、メンバー ファブリックを削除できます。



LAN クラシック ファブリック テンプレートのファブリック内接続のサポート

[LAN_Classic] ファブリックは、次の条件で VRF-Lite、Multi-Site、および MPLS IFC をサポートします。

- DCI/VRF-Lite および Multi-Site IFC の接続先として **[LAN_Classic]** ファブリックがサポートされていますが、必要な情報を提供することで手動でのみ作成できます。**[Easy_Fabric_11_1]** および **[MSD_Fabric_11_1]** ファブリックで自動展開オプションが有効になっている場合でも、これらは自動的に作成されません。
- 存在しない（メタ）スイッチを **[LAN_Classic]** ファブリックに追加することはできません。メタ スイッチは、DCNM が検出できないスイッチまたはデバイスのプレースホルダです。
- 「エッジ ルータ」および「コア ルータ」スイッチ ロールの基本 BGP 構成は、自動生成されません。これらは、**[switch_freeform]** ポリシーまたはその他の適切な手段を使用して構成します。
- ファブリック設定で MPLS ハンドオフが有効になっている場合、MPLS 基本構成は、「エッジ ルータ」および「コア ルータ」スイッチ ロールに対して自動生成されます。

外部ファブリックおよびLANクラシックファブリックでのインバンド管理

リリース 11.5(1) 以降 Cisco DCNM では、ブラウンフィールド展開でのみ、外部および LAN クラシック ファブリックのインバンド接続のスイッチをインポートまたは検出できます。ファブリック設定を構成または編集しながら、ファブリックごとにインバンド管理を有効にします。POAP を使用してインバンド接続のスイッチをインポートまたは検出することはできません。

設定後、ファブリックはインバンド管理の VRF に基づいてスイッチの検出を試みます。ファブリック テンプレートは、シード IP を使用してインバンド スイッチのVRFを決定します。同じシード IP に複数の VRF がある場合、シードインターフェイスのインテントは学習されません。インテント/設定を手動で作成する必要があります。

ファブリック設定を構成/編集した後、保存して展開する必要があります。インバンド管理対象スイッチをファブリックにインポートした後は、インバンド管理設定を変更できません。このチェックボックスをオフにすると、次のエラー メッセージが生成されます。

```
Inband IP <<IP Address>> cannot be used to import the switch,
please enable Inband Mgmt in fabric settings and retry.
```

スイッチをファブリックにインポートしたら、インターフェイスを管理してインテントを作成する必要があります。スイッチをインポートするインターフェイスのインテントを作成します。インターフェイス コンフィギュレーションを編集/更新します。このインバンド管理スイッチのインターフェイス IP を変更しようとすると、エラー メッセージが生成されます。

```
Interface <<interface_name>> is used as seed or next-hop egress interface
for switch import in inband mode.
IP/Netmask Length/VRF changes are not allowed for this interface.
```

インターフェイスの管理中に、インバンド管理を使用してインポートされたスイッチでは、スイッチのシード IP を変更できません。次のエラーが生成されます。

```
<<switch-name>>: Mgmt0 IP Address (<ip-address>) cannot be changed,
when is it used as seed IP to discover the switch.
```

ネクストホップ インターフェイスのポリシーを作成します。サードパーティ製デバイスから DCNM へのルートには、ECMP ルートと呼ばれる複数のインターフェイスが含まれる場合があります。ネクストホップインターフェイスを検索し、スイッチのインテントを作成します。インターフェイス IP および VRF の変更は許可されません。

インバンド管理が有効になっている場合、イメージ管理中に、ISSU、EPLD、RPM、および SMU インストール フローで、スイッチ上のイメージをコピーするために eth2 IP アドレスが使用されます。

ファブリック内のインバンド接続を使用してスイッチをインポートし、後でファブリック設定でインバンド管理を無効にすると、次のエラー メッセージが生成されます。

```
The fabric <<fabric name>> was updated with below message:
Fabric Settings cannot be changed for Inband Mgmt, when switches are already imported
using inband Ip. Please remove the existing switches imported using Inband Ip from the
fabric,
then change the Fabric Setttings.
```

ただし、同じファブリックに、インバンド接続とアウトオブバンド接続の両方を使用してインポートされたスイッチを含めることができます。

外部ファブリックおよびLANクラシックファブリック向け高精度時間プロトコル（PTP）

リリース11.5(1)から、**[External_Fabric_11_1]**または**[LAN_Classic]**テンプレートのファブリック設定で、**[高精度時間プロトコル（PTP）を有効化（Enable Precision Time Protocol（PTP））]**チェックボックスをオンにして、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。また、**[PTPループバックID（PTP Loopback Id）]**および**[PTPドメインID（PTP Domain Id）]**フィールドは編集可能です。

PTP機能は、NX-OSバージョン7.0(3)I7(1)以降のCisco Nexus 9000シリーズクラウドスケールスイッチでサポートされます。ファブリック内にクラウドスケール以外のデバイスがあり、PTPが有効になっていない場合は、警告が表示されます。クラウドスケールデバイスの例としては、Cisco Nexus 93180YC-EX、Cisco Nexus 93180YC-FX、Cisco Nexus 93240YC-FX2、およびCisco Nexus 93360YC-FX2スイッチがあります。詳細については、https://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html#~productsを参照してください。

Note PTPグローバル設定は、Cisco Nexus 3000シリーズスイッチでサポートされます。ただし、PTPおよびttagの設定はサポートされていません。

詳細については、『*Cisco Nexus 9000*シリーズ*NX-OS*システム管理構成ガイド』の「*PTP*の構成」の章、および『*Cisco DCNM*ユーザーガイド（「リソースアプリケーション向け*Cisco Network Insights*」』を参照してください。

外部およびLANクラシックファブリック展開の場合、PTPをグローバルに有効にし、コア側のインターフェイスでPTPを有効にする必要があります。インターフェイスは、VMやLinuxベースのマシンのような外部PTPサーバに対して構成できます。したがって、インターフェイスを編集して、グランドマスタークロックと接続する必要があります。PTPおよびTTAG構成を外部およびLANクラシックファブリックで動作させるには、**host_port_resync**ポリシーを使用してDCNMにスイッチ構成を同期する必要があります。詳細については、アウトオブバンドスイッチインターフェイス構成とDCNMの同期, on page 168を参照してください。

グランドマスタークロックはEasyファブリックの外部で構成する必要があり、IP到達可能です。グランドマスタークロックへのインターフェイスは、[interface freeform config]を使用してPTPで有効にする必要があります。

[保存して展開（Save & Deploy）]をクリックすると、すべてのコア側インターフェイスがPTP構成で自動的に有効になります。このアクションにより、すべてのデバイスがグランドマスタークロックに確実にPTP同期されます。さらに、ホスト、ファイアウォール、サービスノード、またはその他のルータに接続されている境界デバイスやリーフ上のインターフェイスなど、コア側でないインターフェイスについては、ttag関連のCLIを追加する必要があります。ttagは、VXLAN EVPNファブリックに入るすべてのトラフィックに追加され、トラフィックがこのファブリックを出るときにttagを削除する必要があります。

次に、PTPの構成例を示します。`feature ptp`

```
feature ptp

ptp source 100.100.100.10 -> IP address of the loopback interface (loopback0)
that is already created, or user-created loopback interface in the fabric settings

ptp domain 1 -> PTP domain ID specified in fabric settings

interface Ethernet1/59 -> Core facing interface
  ptp

interface Ethernet1/50 -> Host facing interface
  ttag
  ttag-strip
```

次のガイドラインはPTPで適用可能です。

- ファブリック内のすべてのスイッチにCisco NX-OSリリース7.0(3)I7(1)以降のバージョンが搭載されている場合、ファブリックでPTP機能をイネーブルにできます。それ以外の場合、次のエラー メッセージが表示されます。

  ```
  PTP feature can be enabled in the fabric, when all the switches have
  NX-OS Release 7.0(3)I7(1) or higher version. Please upgrade switches to
  NX-OS Release 7.0(3)I7(1) or higher version to enable PTP in this fabric.
  ```

- NIRのハードウェア テレメトリ サポートでは、PTP構成が前提条件です。
- PTP構成を含む既存のファブリックに非クラウド スケール デバイスを追加すると、次の警告が表示されます。

  ```
  TTAG is enabled fabric wide, when all devices are cloud-scale switches
  so it cannot be enabled for newly added non cloud-scale device(s).
  ```

- ファブリックにクラウドスケール デバイスと非クラウドスケール デバイスの両方が含まれている場合、PTPを有効にしようとすると、次の警告が表示されます。

  ```
  TTAG is enabled fabric wide when all devices are cloud-scale switches
  and is not enabled due to non cloud-scale device(s).
  ```

- ホスト構成の同期がすべてのデバイスで実行されると、すべてのデバイスに対してTTAG構成が生成されます。新しく追加されたすべてのデバイスでホスト構成の同期が実行されない場合、新しく追加されたデバイスのTtag構成は生成されません。

  構成が同期されていない場合は、次の警告が表示されます。

  ```
  TTAG on interfaces with PTP feature can only be configured for cloud-scale devices.
  It will not be enabled on any newly added switches due to the presence of non
  cloud-scale devices.
  ```

- PTPおよびTTAG構成は、ホスト インターフェイスに展開されます。
- PTPおよびTTAG構成は、同じファブリック内のスイッチ間でサポートされます（ファブリック内リンク）。PTPはファブリック間リンク用に作成され、ttagは他のファブリック（スイッチ）がDCNMによって管理されていない場合に作成されます。ファブリック間リンクは、両方のファブリックがDCNMによって管理されている場合、PTPまたはttag構成をサポートしません。
- TTAG設定は、ブレークアウト後にデフォルトで設定されます。リンクが検出され、ブレークアウト後に接続されたら、[保存および展開（Save & Deploy）]を実行して、ポート

のタイプ（ホスト、ファブリック内リンク、またはファブリック間リンク）に基づいて正しい構成を生成します。

アウトオブバンド スイッチ インターフェイス構成と DCNM の同期

DCNM リリース 11.5(1) 以降、DCNM の外部で（CLI を介して）作成されたすべてのインターフェイス レベルの構成を DCNM に同期し、DCNM から管理できます。また、vPC ペア構成は自動的に検出され、ペアリングされます。これは、External_Fabric_11_1 および LAN_Classic ファブリックにのみ適用されます。vPC ペアリングは **vpc_pair** ポリシーで実行されます。

（注） DCNM がスイッチを管理している場合は、すべての構成変更が DCNM から開始されることを確認し、スイッチで直接変更を行わないようにします。

インターフェイス構成が DCNM インテントに同期されると、スイッチ構成が参照と見なされます。つまり、同期アップの終了時に、スイッチに存在する内容が DCNM インテントに反映されます。再同期操作の前にそれらのインターフェイスに展開されていないインテントが DCNM にある場合、それらは失われます。

ガイドライン

- Easy_Fabric_11_1、External_Fabric_11_1、および LAN_Classic テンプレートを使用するファブリックでサポートされます。
- Cisco Nexus スイッチでのみサポートされます。
- 再同期前にファブリック アンダーレイ関連ポリシーが関連付けられていないインターフェイスでサポートされます。たとえば、IFC インターフェイスとファブリック内リンクは再同期の対象になりません。
- 再同期の前に関連付けられているカスタム ポリシー（Cisco DCNM に付属していないポリシー テンプレート）がないインターフェイスでサポートされます。
- 再同期前に Cisco DCNM の機能やアプリケーションによってインテントが排他的に所有されていないインターフェイスでサポートされます。
- インターフェイス グループが関連付けられていないスイッチでサポートされます。
- インターフェイスモード（スイッチポートからルーテッド、トランクからアクセスなど）の変更は、そのインターフェイスに接続されたオーバーレイではサポートされません。

同期アップ機能は、次のインターフェイス モードおよびポリシーでサポートされます。

インターフェイス モード	ポリシー

トランク（スタンドアロン、po、および vPC PO）	• int_trunk_host_11_1 • int_port_channel_trunk_host_11_1 • int_vpc_trunk_host_11_1
アクセス（スタンドアロン、po、および vPC PO）	• int_access_host_11_1 • int_port_channel_access_host_11_1 • int_vpc_access_host_11_1
dot1q-tunnel	• int_dot1q_tunnel_host_11_1 • int_port_channel_dot1q_tunnel_host_11_1 • int_vpc_ dot1q_tunnel_host_11_1
ルーテッド	int_routed_host_11_1
loopback	int_freeform
sub-interface	int_subif_11_1
FEX (ST, AA)	• int_port_channel_fex_11_1 • int_port_channel_aa_fex_11_1
ブレイクアウト	interface_breakout
nve	int_freeform（External_Fabric_11_1/LAN_Classic のみ）
SVI	int_freeform（External_Fabric_11_1/LAN_Classic のみ）
mgmt0	int_mgmt_11_1

Easyファブリックでは、インターフェイスの再同期によって、インターフェイス上のアクセス VLAN または許可された VLAN に基づいて、ネットワーク オーバーレイ接続が自動的に更新されます。

再同期操作が完了すると、スイッチ インターフェイスのインテントを通常の DCNM 手順で管理できます。

スイッチ インターフェイス構成と DCNM の同期

始める前に

- インターフェイスの再同期を試みる前に、ファブリックのバックアップを作成することをお勧めします。
- **[External_Fabric_11_1]** および **[LAN_Classic]** ファブリックで vPC ペアリングが正しく機能するには、両方のスイッチがファブリック内にあり、機能している必要があります。

- スイッチが **[同期（In-Sync）]** しており、スイッチ モードが**[移行モード（Migration-mode）]** または **[メンテナンス モード（Maintenance-mode）]** でないことを確認します。

手順

ステップ 1 DCNM で、**[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** に移動し、ファブリックをクリックします。

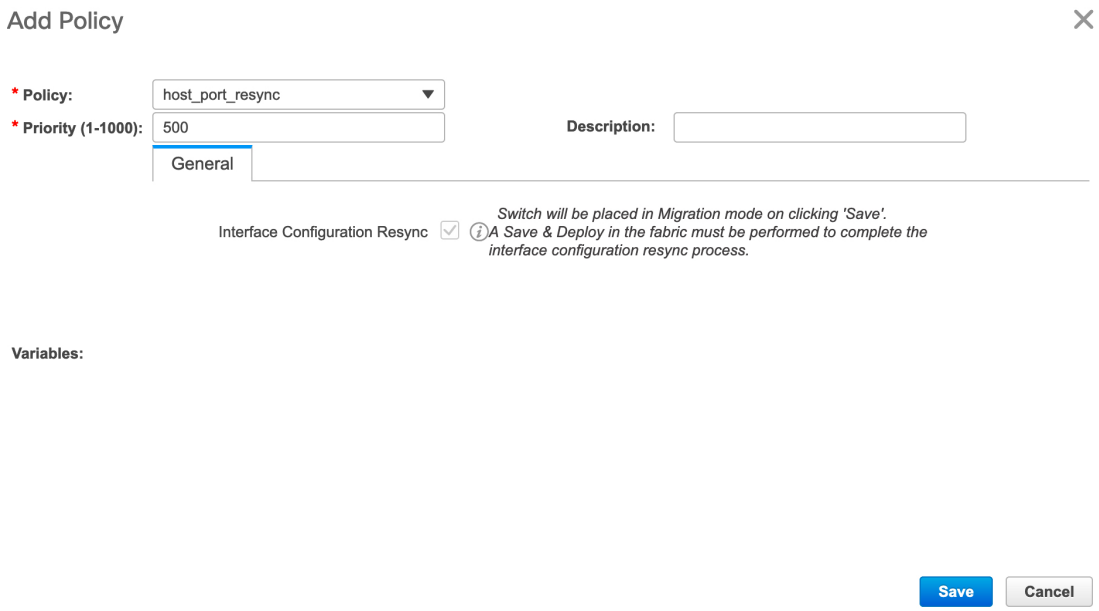
ステップ 2 スイッチがファブリックに存在し、vPC ペアリングが完了していることを確認します。これらは **[トポロジ（Topology）]** 表示に示されています。**[アクション（Actions）]** パネルで **[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 **[表形式ビュー（Tabular view）]** から、インターフェイス インテントの再同期が必要な 1 つ以上のスイッチを選択して、**[ポリシー（Policies）]** をクリックします。

（注）
- スイッチのペアが **no_policy** または **vpc_pair** のいずれかを使用してすでにペアリングされている場合は、ペアの一方のスイッチのみを選択します。
- スイッチのペアがまだペアリングされていない場合は、両方のスイッチを選択します。

ステップ 4 **[ポリシー（Policies）]** ウィンドウで、**[ポリシーの追加（Add Policy）]** アイコンをクリックします。

ステップ 5 **[ポリシーの追加（Add Policy）]** ウィンドウで、**[host_port_resync]** を **[ポリシー（Policy）]** ドロップダウンリストから選択します。[保存（Save）] をクリックします。



ステップ 6 スイッチの **[モード（Mode）]** 列をチェックして、それらが **[移行（Migration）]** を報告していることを確認します。vPC ペアの場合、両方のスイッチが **Migration-mode** になります。

- この手順の後、**[トポロジ（Topoplogy）]** ビューのスイッチは **Migration-mode** になります。
- いずれかのスイッチを移行モードにしただけでも、vPC ペアの両方のスイッチが移行モードになります。
- スイッチが意図せずに再同期モードになった場合は、**[host_port_resync]** ポリシー インスタンスを識別して **[ポリシー（Policies）]** ウィンドウから削除することで、通常モードに戻すことができます。

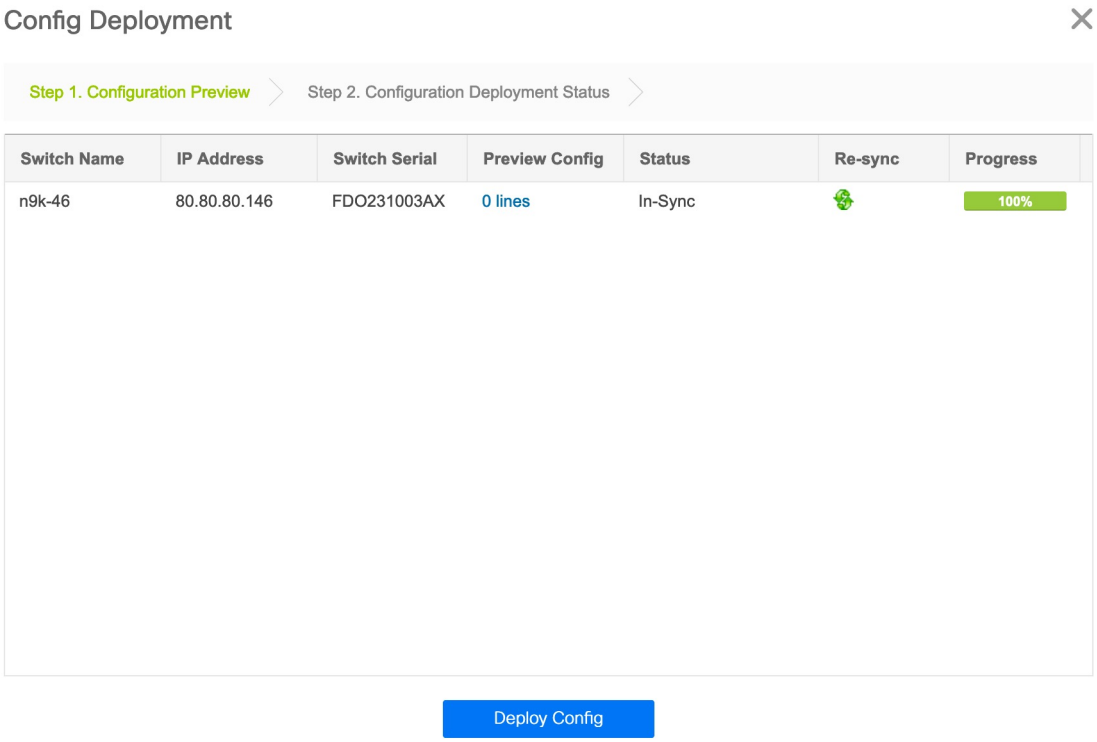
ステップ 7 構成の変更を DCNM に同期する準備ができたら、**[表形式ビュー（Tabular view）]** に移動して必要なスイッチを選択し、**[スイッチの再検出（Rediscover switch）]** をクリックして、DCNM が新しいインターフェイスやその他の変更を認識していることを確認します。

ステップ 8 **[保存と展開（Save & Deploy）]** をクリックして、再同期プロセスを開始します。

（注） このプロセスは、スイッチ構成のサイズと関連するスイッチの数によっては、完了するまでに時間がかかる場合があります。

ステップ 9 再同期操作中にエラーが検出されなかった場合は、**[構成展開（Config Deployment）]** ウィンドウが表示されます。インターフェイス インテントは DCNM で更新されます。

（注） External_Fabric_11_1 または LAN_Classic ファブリックが **[監視モード（Monitored Mode）]** の場合、ファブリックが読み取り専用モードであることを示すエラー メッセージが表示されます。このエラー メッセージは、再同期プロセスが失敗したことを意味するものではないため、無視してかまいません。



[構成展開（Config Deployment）] ウィンドウを閉じると、スイッチが自動的に **[移行モード（Migration-mode）]** を終えたことが観察できます。ペアになっていなかった、または **no_policy** を使用してペアになっていた vPC ペアのスイッチは、ペアとして表示され、**vpc_pair** ポリシーに関連付けられます。

（注） スイッチ用に作成された **host_port_resync** ポリシーは、再同期プロセスが正常に完了すると自動的に削除されます。

次のタスク

次の制限は、スイッチ インターフェイス構成を DCNM に同期した後に適用されます。

- ポートチャネル メンバーシップ（ポリシーが存在する場合）はサポートされていません。
- オーバーレイがアタッチされているインターフェイスのモードの変更（トランクからアクセスなど）はサポートされていません。
- **インターフェイス グループ**に属するインターフェイスの再同期はサポートされていません。
- **External_Fabric_11_1** および **LAN_Classic** テンプレートの vPC ペアリングは、**vpc_pair** ポリシーで更新する必要があります。

- オーバーレイがアタッチされているインターフェイスのモードの変更はサポートされていません。
- **Easy_Fabric** ファブリックでは、VXLAN オーバーレイ インターフェイスのアタッチは、許可された VLAN に基づいて自動的に実行されます。

Easy ファブリックおよび eBGP ファブリックでの MACsec サポート

Cisco DCNM リリース 11.5（1）からMACsec は、ファブリック内リンクの Easy Fabric および eBGP ファブリックでサポートされます。MACsec を設定するには、ファブリックおよび必要な各ファブリック内リンクで MACsec を有効にする必要があります。CloudSec とは異なり、MACsec の自動設定はサポートされていません。

MACsec は、Cisco NX-OS リリース 7.0(3)I7(8) および 9.3(5) 以降のスイッチでサポートされます。

（注） MACsec のサポートは、Cisco DCNM リリース 11.5(1) のプレビュー機能です。

ガイドライン

- リンクの物理インターフェイスで MACsec を設定できない場合は、**[保存（Save）]** をクリックするとエラーが表示されます。次の理由により、デバイスおよびリンクで MACsec を設定できません。
  - NX-OS の最小バージョンが満たされていません。
  - インターフェイスは MACsec に対応していません。
- ファブリック設定の MACsec グローバル パラメータは、いつでも変更できます。
- MACsec と CloudSec は BGW デバイス上で共存できます。
- MACsec はボーダー リーフではサポートされていません。
- MACsec が有効になっているリンクの MACsec ステータスが **[リンク（Links）]** ウィンドウに表示されます。
- MACsec が設定されたデバイスのブラウンフィールド移行は、スイッチおよびインターフェイスの自由形式の設定を使用してサポートされます。

  サポートされているプラットフォームとリリースを含むMACsec設定の詳細については、『Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイド』の「*MACsec* の設定」の章を参照してください。

次のセクションでは、 DCNM で MACsec を有効または無効にする方法を示します：

MACsec の有効化

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** に移動します。

ステップ 2 既存の Easy または eBGP ファブリックで **[ファブリックの作成（Create Fabric）]** をクリックして新しいファブリックを作成するか、**[ファブリックの編集（Edit Fabric）]** をクリックします。

ステップ 3 **[アドバンスト（Advanced）]** タブをクリックし、MACsec の詳細を指定します。

[MACsec の有効化（Enable MACsec）]：ファブリックの MACsec 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。

[MACsec プライマリ キー文字列（MACsec Primary Key String）]：プライマリ MACsec セッションの確立に使用される Cisco Type 7 暗号化オクテット文字列を指定します。AES_256_CMAC の場合、キー文字列の長さは 130、AES_128_CMAC の場合、キー文字列の長さは 66 である必要があります。これらの値が正しく指定されていない場合、ファブリックの保存時にエラーが表示されます。

（注） デフォルトのキー ライフタイムは無期限です。

[MACsec プライマリ暗号化アルゴリズム（MACsec Primary Cryptographic Algorithm）]：プライマリ キー文字列に使用する暗号化アルゴリズムを選択します。**AES_128_CMAC** または **AES_256_CMAC** です。デフォルト値は **AES_128_CMAC** です。

プライマリ セッションが失敗した場合にバックアップ セッションを開始するように、デバイスのフォールバック キーを設定できます。

[MACsec フォールバック キー文字列（MACsec Fallback Key String）]：フォールバック MACsec セッションの確立に使用される Cisco Type 7 暗号化オクテット文字列を指定します。AES_256_CMAC の場合、キー文字列の長さは 130、AES_128_CMAC の場合、キー文字列の長さは 66 である必要があります。これらの値が正しく指定されていない場合、ファブリックの保存時にエラーが表示されます。

[MACsec フォールバック暗号化アルゴリズム（MACsec Fallback Cryptographic Algorithm）]：フォールバック キー文字列に使用する暗号化アルゴリズムを選択します。AES_128_CMAC または AES_256_CMAC です。デフォルト値は AES_128_CMAC です。

[MACsec 暗号スイート（MACsec Cipher Suite）]：MACsec ポリシーの次の MACsec 暗号スイートのいずれかを選択します。

- GCM-AES-128
- GCM-AES-256
- GCM-AES-XPN-128
- GCM-AES-XPN-256

デフォルト値は **GCM-AES-XPN-256** です。

（注） ファブリックの展開が完了した後、MACsec 設定はスイッチに展開されません。スイッチに MACsec 設定を展開するには、ファブリック内リンクで MACsec を有効にする必要があります。

[MACsec ステータス レポート タイマー（MACsec Status Report Timer）]：MACsec 動作ステータス定期レポート タイマーを分単位で指定します。

ステップ 4 ファブリックをクリックし、**[アクション（Actions）]** パネルで **[表形式ビュー（Tabular View）]** をクリックしてから、**[リンク（Links）]** をクリックします。

ステップ 5 MACsec を有効にするファブリック内リンクを選択し、**[リンクのアップデート（Update Link）]** をクリックします。

ステップ 6 **[リンク管理 - リンクの編集（Link Management – Edit Link）]** ウィンドウで、**[リンク プロファイル（Link Profile）]** セクションの **[アドバンスト（Advanced）]** をクリックし、**[MACsec の有効化（Enable MACsec）]** チェックボックスをオンにします。

MACsec がファブリック内リンクで有効になっているが、ファブリック設定では有効になっていない場合、**[保存（Save）]** をクリックするとエラーが表示されます。

MACsec がリンクで設定されると、次の設定が生成されます。

- MACsec を有効にする最初のリンクである場合は、MACsec グローバル ポリシーを作成します。
- リンクの MACsec インターフェイス ポリシーを作成します。

ステップ 7 **[保存（Save）]** をクリックし、**[保存と展開（Save & Deploy）]** をクリックして、MACsec 構成を展開します。

MACsec の無効化

ファブリック内リンクで MACsec を無効にするには、**[リンク管理 – リンクの編集（Link Management – Edit Link）]** ウィンドウに移動し、**[MACsec の有効化（Enable MACsec）]** チェックボックスをオフにして、**[保存（Save）]** をクリックし、**[保存と展開（Save & Deploy）]** をクリックします。このアクションは、次を実行します。

- リンクから MACsec インターフェイスポリシーを削除します。
- これが MACsec が有効になっている最後のリンクである場合、MACsec グローバル ポリシーもデバイスから削除されます。

リンクで MACsec を無効にした後でのみ、**[ファブリックの設定（Fabric Settings）]** に移動し、**[MACsec の有効化（Enable MACsec）]** チェックボックス（**[詳細（Advanced）]** タブ）をオフにして、ファブリックで MACsec を無効にすることができます。MACsec が有効になっているファブリック内にファブリック内リンクがある場合、**[保存と展開（Save & Deploy）]** をクリックするとエラーが表示されます。

テナント ルーテッド マルチキャストの概要

テナント ルーテッド マルチキャスト（TRM）は、BGP ベースの EVPN コントロール プレーンを使用する VXLAN ファブリック内でのマルチキャスト転送を有効にします。TRM は、ローカルまたは VTEP 間で同じサブネット内または異なるサブネット内の送信元と受信側の間にマルチテナント対応のマルチキャスト転送を実装します。

TRM を有効にすると、アンダーレイでのマルチキャスト転送が活用され、VXLAN でカプセル化されたルーテッド マルチキャスト トラフィックが複製されます。デフォルト マルチキャスト配信ツリー（デフォルト MDT）は、VRF ごとに構築されます。これは、レイヤ 2 仮想ネットワーク インスタンス（VNI）のブロードキャストおよび不明ユニキャスト トラフィック、およびレイヤ 2 マルチキャスト複製グループの既存のマルチキャスト グループに追加されます。オーバーレイ内の個々のマルチキャスト グループ アドレスは、複製および転送のためにそれぞれのアンダーレイ マルチキャスト アドレスにマッピングされます。BGP ベースのアプローチを使用する利点は、TRM を備えた BGP EVPN VXLAN ファブリックが、すべてのエッジ デバイスまたは VTEP に RP が存在する完全な分散型オーバーレイ ランデブー ポイント（RP）として動作できることです。

マルチキャスト対応のデータセンターファブリックは、通常、マルチキャストネットワーク全体の一部です。マルチキャスト送信元、受信側、およびマルチキャスト ランデブー ポイントはデータセンター内に存在する可能性がありますが、キャンパス内にある場合や WAN 経由で外部から到達可能である場合もあります。TRM を使用すると、既存のマルチキャスト ネットワークをシームレスに統合できます。ファブリック外部のマルチキャスト ランデブー ポイントを活用できます。さらに、TRM では、レイヤ 3 物理インターフェイスまたはサブインターフェイスを使用したテナント対応外部接続が可能です。

詳細については、次のトピックを参照してください。

- テナント ルーテッド マルチキャストに関する注意事項と制限事項
- レイヤ 3 テナント ルーテッド マルチキャストの注意事項と制約事項
- レイヤ 2/レイヤ 3 テナント ルーテッド マルチキャスト（混合モード）の注意事項と制約事項

VXLAN EVPN マルチサイトのテナント ルーテッド マルチキャストの概要

マルチサイトを使用したテナント ルーテッド マルチキャストは、マルチサイト経由で接続された複数の VXLAN EVPN ファブリック間でのマルチキャスト転送を可能にします。

次の 2 つのユース ケースがサポートされています。

- ユース ケース 1：TRM は、さまざまなサイトの送信元と受信者に、レイヤ 2 およびレイヤ 3 マルチキャスト サービスを提供します。
- ユース ケース 2：TRM 機能を VXLAN ファブリックからファブリック外部の送信元受信者に拡張します。

TRM Multi-Site は、BGP ベースの TRM ソリューションを拡張したもので、複数の VTEP を持つ複数の TRM サイトが相互に接続して、最も効率的な方法でサイト間でマルチキャスト サー

ビスを提供できるようにします。各TRMサイトは独立して動作しており、各サイトのボーダーゲートウェイは各サイトをつなぐことができます。サイトごとに複数のボーダーゲートウェイを設定できます。特定のサイトで、BGWはEVPNおよびMVPNルートを交換するために、他のサイトのルートサーバまたはBGWとピアリングします。BGWで、BGPはローカルVRF/L3VNI/L2VNIにルートをインポートし、ルートが学習された場所に応じて、それらのインポートされたルートをファブリックまたはWANにアドバタイズします。

VXLAN EVPN マルチサイト オペレーションのテナント ルーテッド マルチキャスト

VXLAN EVPN マルチサイトでの TRM の操作は次のとおりです。

- 各サイトはエニーキャスト VTEP BGW で表されます。BGW 間での DF の選択により、パケットの重複がなくなります。
- ボーダーゲートウェイ間のトラフィックは、入力複製メカニズムを使用します。トラフィックは VXLAN ヘッダーとともにカプセル化され、その後に IP ヘッダーが続きます。
- 各サイトは、パケットのコピーを 1 つだけ受信します。
- サイト間のマルチキャスト送信元および受信者情報は、TRM が設定されたボーダー ゲートウェイ上の BGP プロトコルによって伝播されます。
- 各サイトの BGW はマルチキャスト パケットを受信し、ローカル サイトに送信する前にパケットを再カプセル化します。

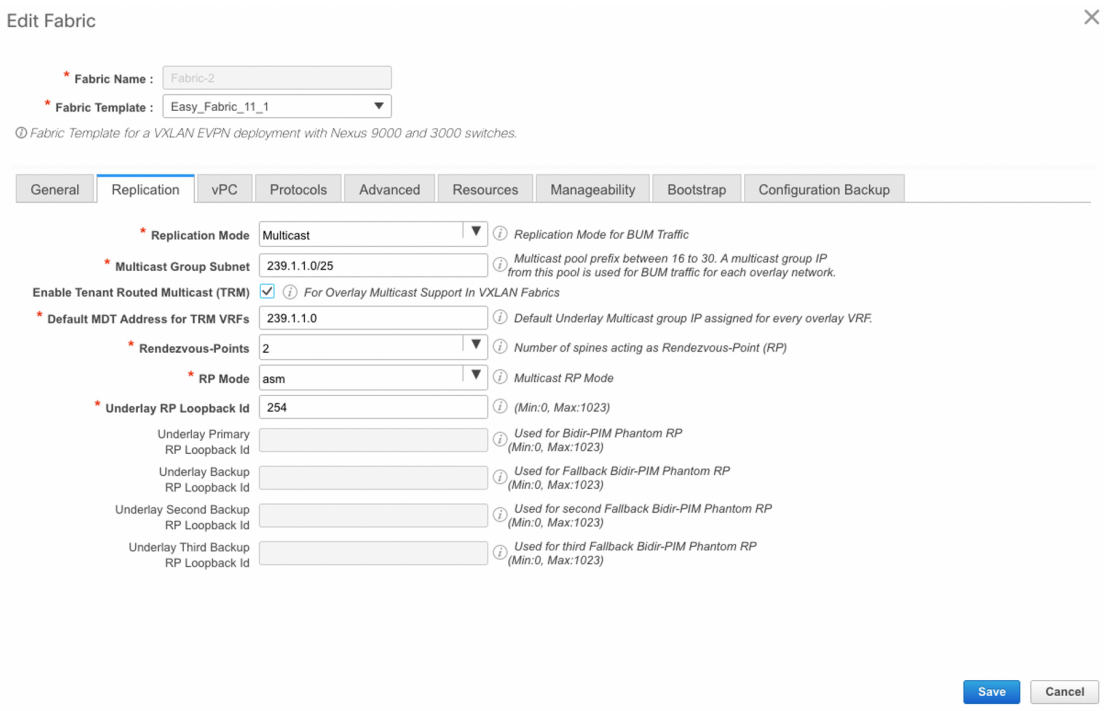
VXLAN EVPNマルチサイトでのTRMのガイドラインと制限事項については、「テナント ルーテッド マルチキャストの設定」を参照してください。

Cisco DCNM を使用したシングル サイト向け TRM の構成

この項では、VXLAN EVPN ファブリックが Cisco DCNM を使用してすでにプロビジョニングされていることを前提としています。

Procedure

ステップ 1 選択した Easy ファブリックの TRM を有効にします。ファブリック テンプレートが **[Easy_Fabric_11_1]** の場合は、[ファブリック（Fabric）]設定をクリックし、**[複製（Replication）]** タブに移動して、**[テナント ルーテッド マルチキャスト（TRM）の有効化（Enable Tenant Routed Multicast (TRM)）]** フィールドをオンにします。さらに、デフォルトの MDT マルチキャスト グループ フィールドには、デフォルト値が自動入力されます。



[テナント ルーテッド マルチキャスト（TRM）の有効化（Enable Tenant Routed Multicast（TRM））]：VXLAN BGP EVPN ファブリックで EVPN/MVPN を介してオーバーレイ マルチキャスト トラフィックをサポートできるようにするテナント ルーテッド マルチキャスト（TRM）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。

[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]：テナント ルーテッド マルチキャスト トラフィックのマルチキャスト アドレスが入力されます。デフォルトでは、このアドレスは [マルチキャスト グループ サブネット] フィールドで指定された IP プレフィックスから取得されます。いずれかのフィールドをアップデートする場合、**[マルチキャスト グループ サブネット（Multicast Group Subnet）]** で指定した IP プレフィックスから選択された TRM アドレスであることを確認してください。

[保存（Save）] をクリックして、ファブリックの設定を保存します。この時点で、すべてのスイッチは保留状態になるため、「青色」になります。**[保存して展開（Save and Deploy）]** をクリックして、以下を有効にします。

- 機能 ngmvpn の有効化（Enable feature ngmvpn）：BGP ピアリング向け次世代マルチキャスト VPN（ngMVPN）コントロール パネルを有効にします。
- IP マルチキャスト マルチパス s-g-hash next-hop-based の構成（Configure ip multicast multipath s-g-hash next-hop-based）：VRF で有効化された TRM 向けマルチパス ハーシング アルゴリズムです。
- IP IGMP スヌーピング VXLAN の構成（Configure ip igmp snooping vxlan）：VXLAN VLAN の IGMP スヌーピングを有効化します。
- IP マルチキャスト overlay-spt-only の構成（Configure ip multicast Overlay-spt-only）：すべての MPVN 対応 Cisco Nexus 9000 スイッチで MVPN ルートタイプ 5 を有効にします。

- MVPN BGP AFI ピアリングの設定と確立（Configure and Establish MVPN BGP AFI Peering）：これは、BGP RR とリーフ間のピアリングに必要です。

Easy_Fabric_eBGP ファブリック テンプレートを使用して作成された VXLAN EVPN ファブリックの場合は、[EVPN] タブに **[テナント ルーテッド マルチキャスト（TRM）の有効化（Enable Tenant Routed Multicast（TRM））]** フィールドと **[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]** フィールドが表示されます。

ステップ 2 VRF の TRM を有効にします。

[制御（Control）] > [VRF] に移動し、選択した VRF を編集します。**[詳細（Advanced）]** タブに移動し、次の TRM 設定を編集します。

TRM の有効化：TRM を有効にするためにチェックボックスを選択します。TRM を有効化する場合、RP アドレスおよびアンダーレイ マルチキャスト アドレスを入力する必要があります。

RP が外部：ファブリックに対して RP が外部である場合、このチェックボックスを有効にします。このフィールドのチェックがオフの場合、RP はすべての VTEP に分散されます。

Note RP が外部の場合、適切なオプションを選択します。RP が外部の場合、RP ループバック ID がグレー化されます。

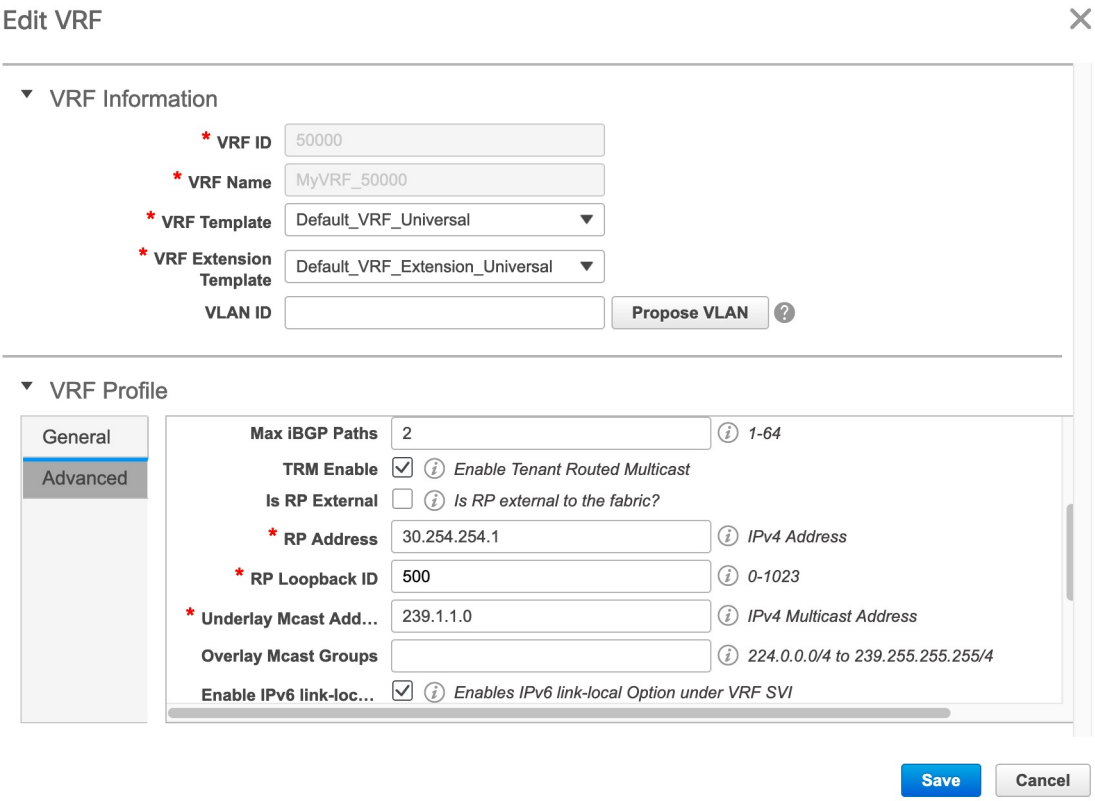
RP アドレス：RP の IP アドレスを指定します。

RP ループバック ID：**RP が外部** が有効化されていない場合、RP のループバック ID を指定します。

[アンダーレイ マルチキャスト アドレス（Underlay Multicast Address）]：VRF に関連付けられたマルチキャストアドレスを指定します。マルチキャストアドレスは、ファブリック アンダーレイでマルチキャスト トラフィックを転送するために使用します。

Note ファブリック設定画面の **[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]** フィールドのマルチキャスト アドレスは、このフィールドに自動的に入力されます。ユーザーはこの VRF に別のマルチキャスト グループ アドレスを使用する必要がある場合は、このフィールドを上書きできます。

[オーバーレイ マルチキャスト グループ（Overlay Multicast Groups）]：指定した RP のマルチキャスト グループ サブネットを指定します。値は「ip pim rp-address」コマンドのグループ範囲です。フィールドが空の場合、デフォルトで 224.0.0.0/24 が使用されます。



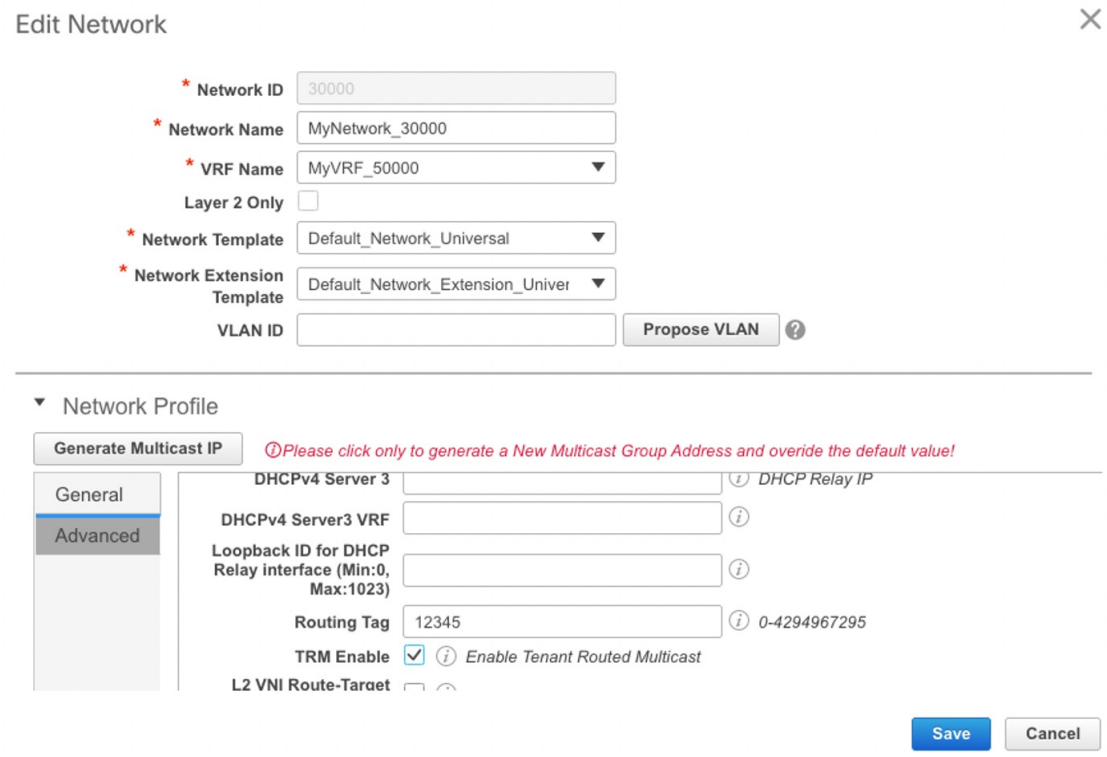
[Save] をクリックして設定を保存します。スイッチは保留状態に入り、青色になります。これらの設定で次のことが有効化されます。

- L3VNI SVI で PIM を有効にします。
- MVPN AFI のルートターゲットのインポートおよびエクスポート。
- VRF 向け RP およびその他のマルチキャスト構成。
- 分散 RP の上記の RP アドレスと RP ループバック ID を使用するループバック インターフェイス。

ステップ 3 ネットワークの TRM を有効にします。

[制御（Control）]>[ネットワーク（Networks）] に移動します。選択したネットワークを編集し、[詳細（Advanced）] タブに移動します。次の TRM 設定を編集します。

[TRM が有効（TRM enable）]：TRM 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。



[Save] をクリックして設定を保存します。スイッチは保留状態、つまり青色になります。TRM 設定により、次のことが可能になります。

- L2VNI SVI で PIM を有効にします。
- PIM ポリシーを **なし（none）** で作成して、VLAN 内の PIM ルータとの PIM ネイバーシップを回避します。**なし（none）** キーワードは、すべての ipv4 アドレスを拒否するように設定されたルートマップで、エニーキャスト IP を使用した PIM ネイバーシップ ポリシーの確立を回避します。

Cisco DCNM を使用したマルチサイト向け TRM の構成

このセクションでは、マルチサイト ドメイン（MSD）がすでに Cisco DCNM によって展開されており、TRM を有効にする必要があることを前提としています。

Procedure

ステップ 1 BGW で TRM を有効にします。

[制御（Control）] > [VRF] に移動します。[スコープ（Scope）] で正しい DC ファブリックが選択されていることを確認し、VRF を編集します。[Advanced] タブまで移動します。TRM 設定の編集すべての DC ファブリックとその VRF に対してこのプロセスを繰り返します。

TRM の有効化：TRM を有効にするためにチェックボックスを選択します。TRM を有効化する場合、RP アドレスおよびアンダーレイ マルチキャスト アドレスを入力する必要があります。

RP が外部：ファブリックに対して RP が外部である場合、このチェックボックスを有効にします。このフィールドのチェックがオフの場合、RP はすべての VTEP に分散されます。

Note RP が外部の場合、適切なオプションを選択します。RP が外部の場合、RP ループバック ID がグレー化されます。

RP アドレス：RP の IP アドレスを指定します。

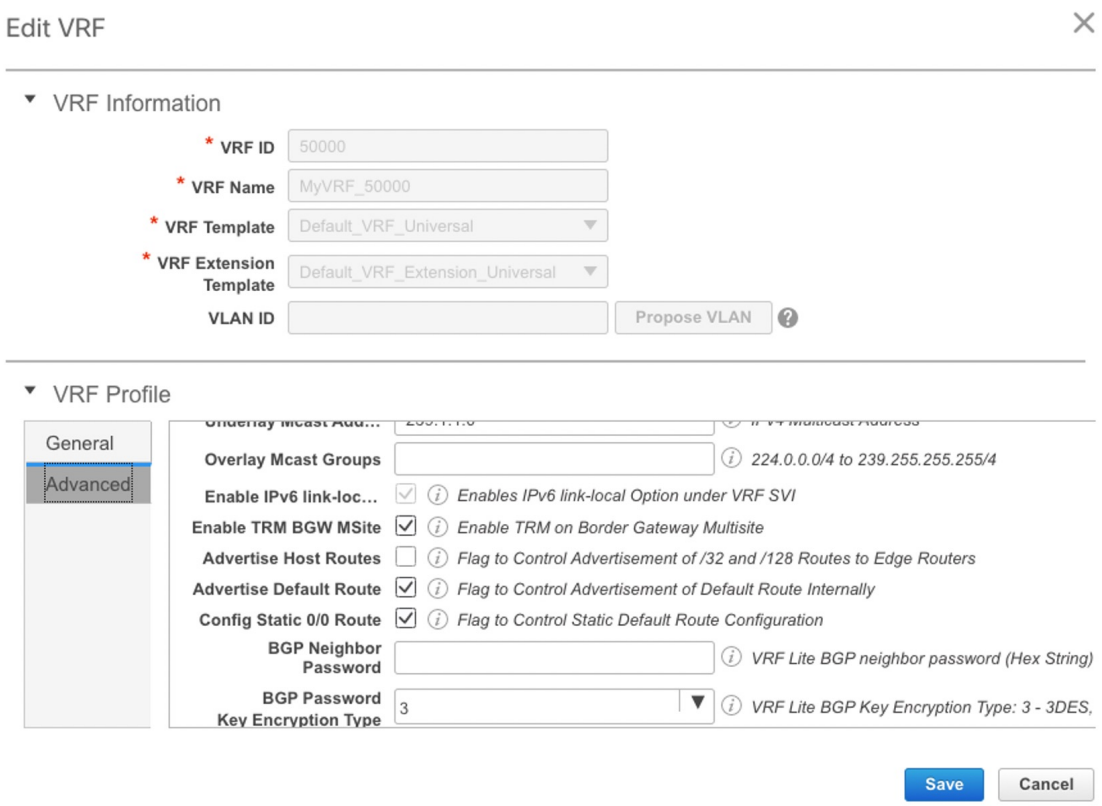
RP ループバック ID：**RP が外部** が有効化されていない場合、RP のループバック ID を指定します。

[アンダーレイ マルチキャスト アドレス（Underlay Multicast Address）]：VRF に関連付けられたマルチキャストアドレスを指定します。マルチキャストアドレスは、ファブリック アンダーレイでマルチキャスト トラフィックを転送するために使用します。

Note ファブリック設定画面の **[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]** フィールドのマルチキャスト アドレスは、このフィールドに自動的に入力されます。ユーザはこの VRF に別のマルチキャスト グループ アドレスを使用する必要がある場合は、このフィールドを上書きできます。

[オーバーレイ マルチキャスト グループ（Overlay Multicast Groups）]：指定した RP のマルチキャスト グループ サブネットを指定します。値は「ip pim rp-address」コマンドのグループ範囲です。フィールドが空の場合、デフォルトで 224.0.0.0/24 が使用されます。

[TRM BGW MSite の有効化（Enable TRM BGW MSite）]：境界ゲートウェイ マルチサイトで TRM 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。

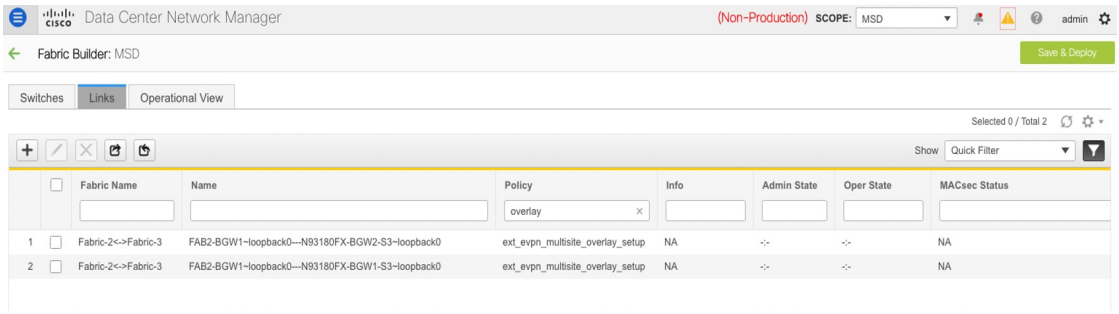


[保存（Save）] をクリックして、設定を保存します。スイッチは保留状態に入り、青色になります。これらの設定で次のことが有効化されます。

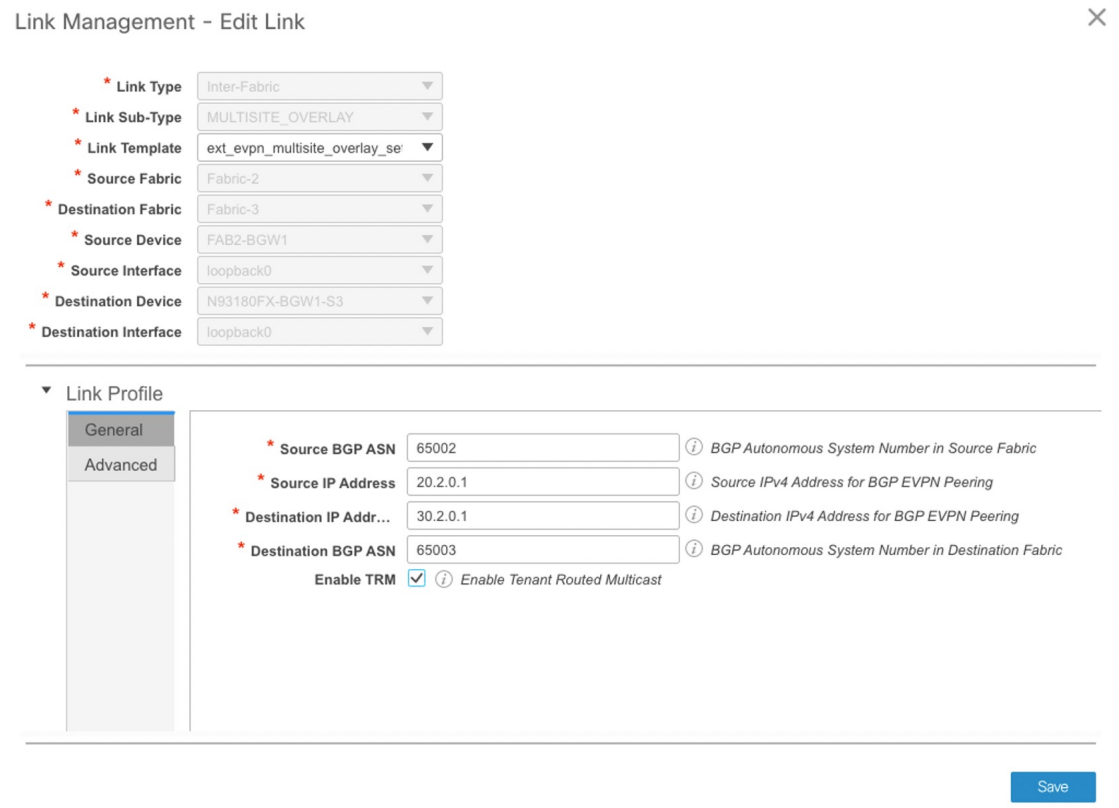
- 機能 ngmvpn の有効化：BGP ピアリング向け次世代マルチキャスト VPN（ngMVPN）コントロール パネルを有効にします。
- L3VNI SVIでPIMをイネーブルにします。
- L3VNI マルチキャスト アドレスを構成します。
- MVPN AFI のルートターゲットのインポートおよびエクスポート。
- VRF 向け RP およびその他のマルチキャスト構成。
- 分散 RP のループバック インターフェイス。
- レイヤ 2 VNI を拡張するためのマルチサイト BUM 入力レプリケーション方式を有効化します。

ステップ 2 BGW 間の MVPN AFI を確立します。

[制御（Control）] > [ファブリック（Fabrics）] に移動します。MSD ファブリックを選択します。**[表形式ビュー（Tabular view）]** をクリックし、**[リンク（Links）]** をクリックします。ポリシー：[オーバーレイ（Overlays）] でフィルタします。



[TRM の有効化（Enable TRM）] チェックボックスをオンにして、各オーバーレイ ピアリングを選択および編集し、TRM を有効にします。



[Save] をクリックして設定を保存します。スイッチは保留状態、つまり青色になります。TRM 設定により、BGW 間、または BGW とルート サーバ間の MVPN ピアリングが有効になります。

SSH キー RSA ハンドリング

ブートストラップのシナリオ

スイッチの実行構成にキー長変数値が 1024 以外の **ssh key rsa** コマンドがある場合、ブートストラップ中に **ssh key rsa** *key-length* **force** コマンドを必要な値（1024 以外の任意の値）を使用してブートストラップ自由形式構成に追加する必要があります。

グリーンフィールドとブラウンフィールドのシナリオ

ssh key rsa *key-length* **force** コマンドを使用して、キー長変数を 1024 以外の値に変更します。

ただし、Cisco Nexus 9000 リリース 9.3(1) および 9.3(2) では、ASCII 再生プロセス中にデバイスが起動しているときに、**ssh key rsa** *key-length* **force** コマンドが失敗します。詳細については、CSCvs40704 を参照してください。

インテントとスイッチの両方の実行構成に同じコマンドがある場合、構成は同期していると見なされます。たとえば、**ssh key rsa 2048** コマンドがインテントと実行構成の両方に存在する場合、ステータスは同期中と見なされます。ただし、アウトオブバンドの変更として **ssh key rsa 2040** コマンドがスイッチにプッシュされたシナリオを検討してください。インテントのキー長値は 2048 ですが、デバイスのキー長値は 2040 です。このような場合、スイッチは非同期としてマークされます。

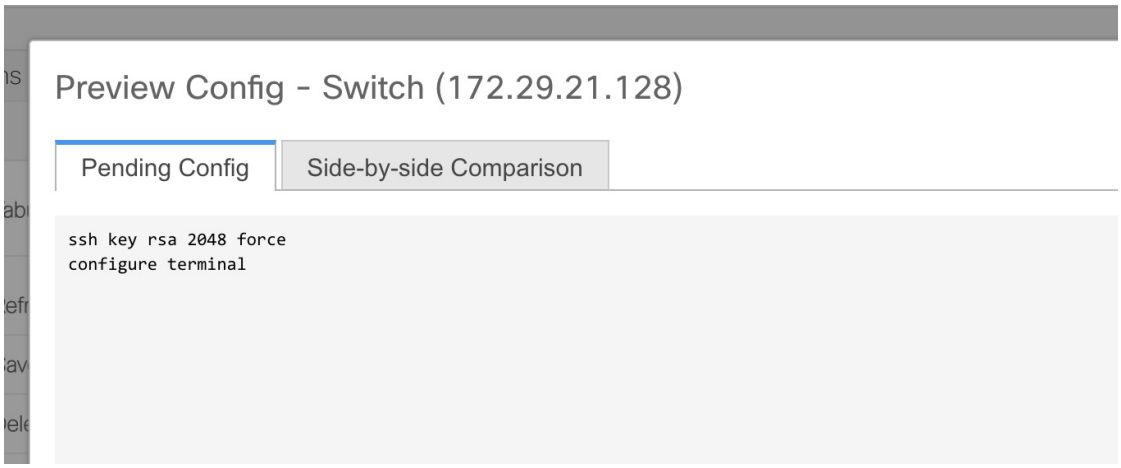
[保留中構成（Pending Config）] タブに表示される差分（厳格構成コンプライアンス モードと非厳格構成コンプライアンス モードの両方）は、**ssh key rsa** コマンドに変更を加える前に **feature ssh** コマンドを使用して SSH 機能を無効にする必要があるため、DCNM からスイッチに展開できません。これにより、DCNM への接続が切断されます。このようなシナリオでは、差分がないようにインテントを変更することで差分を解決できます。

厳格構成コンプライアンス モードの場合：

- **[ファブリック ビルダ（Fabric Builder）]** ウィンドウの **[表形式ビュー（Tabular View）]** で **[ポリシーの表示/編集（View/Edit Policies）]** をクリックして、**ssh key rsa 2048 force** コマンドを持つポリシー テンプレート インスタンス（PTI）を削除します。

- **[ポリシーの表示/編集（View/Edit Policies）]** をクリックして、**ssh key rsa 2040 force** コマンドで新しい PTI を作成します。

厳格構成コンプライアンス モードなしの場合：



- **[ファブリック ビルダ（Fabric Builder）]** ウィンドウの **[表形式ビュー（Tabular View）]** で **[ポリシーの表示/編集（View/Edit Policies）]** をクリックして、**ssh key rsa 2048 force** コマンドを持つ PTI を削除します。

- デバイスからのアウトオブバンドの変更に一致する目的で、**ssh key rsa 2040 force** コマンドを使用して switch_freeform PTI を作成します。

スイッチ操作

さまざまなオプションを表示するには、スイッチを右クリックします。

[ロールの設定（Set Role）]：スイッチにロールを割り当てます。次のロールのいずれかをスイッチに割り当てることができます。

- スパイン
- リーフ（デフォルト ロール）
- 境界
- ボーダースパイン
- ボーダーゲートウェイ
- アクセス
- 集約

- エッジ ルータ
- コア ルータ
- 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 スパイン
- ToR

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。同じデバイス タイプの 1 つ以上のデバイスを選択し、**[ロールの設定（Set Role）]** をクリックしてデバイスのロールを設定します。デバイス タイプは次のとおりです。

- NX-OS
- IOS XE
- IOS XR
- その他

Note ロールを設定する前に、スイッチをメンテナンス モードからアクティブ モードまたは動作モードに移動したことを確認します。

[保存と展開（Save & Deploy）] を実行する前にのみ、スイッチのロールを変更できます。

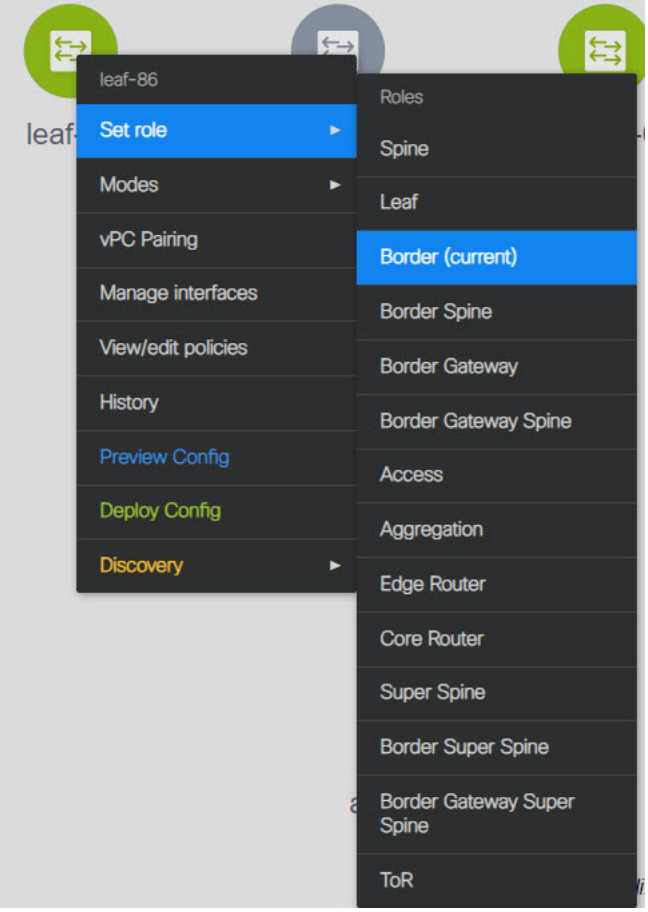
非 Nexus デバイスには、次のいずれかのロールを割り当てることができます。

- スパイン
- リーフ
- アクセス（このロールは、Cisco ASR 1000 シリーズ ルータおよび Cisco Catalyst 9000 シリーズ スイッチでのみ使用できます)。
- エッジ ルータ（VRF-Lite にはこのロールを使用します）。
- コア ルータ
- スーパースパイン
- 設定のプレビュー
- ToR（このロールは、Cisco Catalyst 9000 シリーズ スイッチでのみ使用できます）。

DCNM 11.1(1) リリースから、スイッチにオーバーレイがない場合、スイッチのロールを既存のロールから必要なロールにシフトできます。**[保存して展開（Save and Deploy）]** をクリックして、更新後の構成を生成します。スイッチ ロールには、次のシフトが許可されています。

- リーフからボーダー

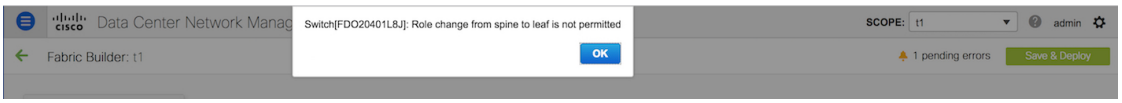
- ボーダーからリーフ
- リーフからボーダーゲートウェイ
- ボーダーゲートウェイからリーフ
- ボーダーからボーダーゲートウェイ
- ボーダーゲートウェイからボーダー
- スパインからボーダー スパイン
- ボーダー スパインからスパイン
- スパインからボーダーゲートウェイ スパイン
- ボーダーゲートウェイ スパインからスパイン
- ボーダー スパインからボーダーゲートウェイ スパイン
- ボーダーゲートウェイ スパインからボーダー スパイン



スイッチ ロールをリーフ ロールからスパイン ロールに、スパイン ロールからリーフ ロールに変更することはできません。

上記の Easy ファブリックで許可されているスイッチ ロールの変更に従ってスイッチ ロールが変更されていない場合、**[保存して展開（Save and Deploy）]** をクリックした後に次のエラーが表示されます。

```
Switch[<serial-number>]: Role change from <switch-role> to <switch-role> is not permitted.
```



その後、スイッチ ロールを以前に設定されたロールに変更するか、新しいロールを設定して、ファブリックを構成できます。

[保存して展開（Save and Deploy）] をクリックする前にポリシー テンプレート インスタンスを作成しておらず、オーバーレイがない場合は、スイッチのロールを他の必要なロールに変更できます。

vPC ペアの一部である vPC スイッチのスイッチ ロールを変更すると、**[保存して展開（Save and Deploy）]** をクリックすると次のエラーが表示されます。

```
Switches role should be the same for VPC pairing. peer1 <serial-number>: [<switch-role>],
 peer2 <serial-number>: [<switch-role>]
```

このシナリオを回避するには、vPC ペアの両方のスイッチのスイッチ ロールを同じロールに変更します。

DCNM での EXEC モード コマンドの実行

初めてログインしたときに、Cisco NX-OS ソフトウェアでは EXEC モードが開始されます。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、ユーザがデバイス コンフィギュレーション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。

次の手順は、DCNM でEXECコマンドを実行する方法を示しています。

手順

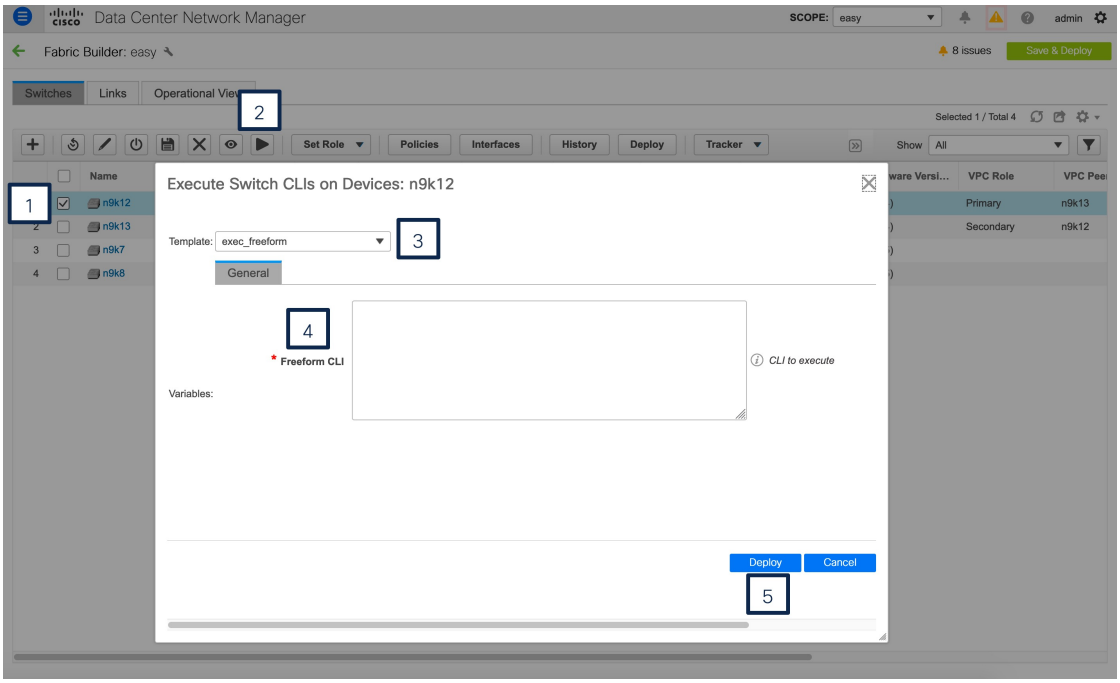
ステップ 1 DCNM から、**[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** の順に移動します。

ステップ 2 ファブリックをクリックし、**[アクション（Actions）]** メニューで **[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 1 つまたは複数のスイッチを選択し、**[再生（Play）]** ボタン（コマンド実行）をクリックします。

ステップ 4 **[テンプレート（Template）]** ドロップダウンリストから、**[exec_freeform]** を選択します。

ステップ 5 コマンドを **[自由形式 CLI（Freeform CLI）]** フィールドに入力します。



ステップ 6 **[展開（Deploy）]** をクリックして、EXEC コマンドを実行します。

ステップ 7 **[CLI 実行ステータス（CLI Execution Status）]** ウィンドウで、展開のステータスを確認できます。**[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。

ステップ 8 **[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。

ファブリック マルチ スイッチ操作

ファブリック トポロジ ウィンドウの **[アクション（Actions）]** ペインから **[表形式ビュー（Tabular View）]** をクリックします。表形式ビューには、次のタブがあります。

- 表形式ビュー：スイッチ
- 表形式ビュー：リンク
- 表形式ビュー：操作ビュー

表形式ビュー：スイッチ

このタブでスイッチ操作を管理できます。各行はファブリック内のスイッチを表し、シリアル番号を含むスイッチの詳細が表示されます。

このタブから実行できるアクションの一部は、ファブリック トポロジ ウィンドウでスイッチを右クリックしたときにも使用できます。ただし、**[スイッチ（Switches）]** タブでは、ポリシーの展開など、複数のスイッチの設定を同時にプロビジョニングできます。

[スイッチ（Switches）] タブには、ファブリックで検出されたすべてのスイッチに関する次の情報が表示されます。

- 名前：スイッチ名を指定します。
- IP アドレス：スイッチの IP アドレスを指定します。
- ロール：スイッチのロールを指定します。
- シリアル番号：スイッチのシリアル番号を入力します。
- ファブリック名：スイッチが検出されたファブリックの名前を指定します。
- ファブリック ステータス：スイッチが検出されたファブリックのステータスを指定します。
- 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。
- ソフトウェア バージョン：スイッチのソフトウェア バージョンを指定します。
- ThousandEyes ステータス：ThousandEyes Enterprise Agent のステータスを指定します。
- 最終更新日：スイッチが最後に更新された日時を示します。
- モード：スイッチの現在のモードを指定します。
- 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。

[スイッチ（Switches）] タブには、次のアイコンとボタンがあります。

- スイッチの追加：このアイコンをクリックして、ファブリックに既存または新規のスイッチを検出します。**[インベントリ管理（Inventory Management）]** ダイアログボックスが表示されます。

  このオプションは、ファブリック トポロジ ウィンドウでも使用できます。[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。

  詳細については、次の項を参照してください。

  - ファブリックへのスイッチの追加：簡易ファブリックへのスイッチの追加について説明します。
  - 新しいスイッチの検出：外部ファブリックへの Cisco Nexus スイッチの追加に関する情報を提供します。
  - 非 Nexus デバイスを外部ファブリックに追加：外部ファブリックへの非 Nexus スイッチの追加に関する情報を提供します。

- スイッチの再検出：スイッチ検出プロセスを DCNM afresh により開始します。
- ディスカバリ クレデンシャルの更新：認証プロトコル、ユーザ名、パスワードなどのデバイス クレデンシャルを更新します。
- 構成の保存とリロード：構成を保存して、スイッチをリロードします。

Note このオプションは、ファブリックがフリーズモードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。

- コピー実行からスタートアップ構成：Cisco DCNM、リリース 11.4(1) 以降、1 つ以上のスイッチに対して、オンデマンドのコピー実行コンフィギュレーションからスタートアップ構成への動作を実行できます。

Note このオプションは、ファブリックがフリーズモードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。

- スイッチの削除：ファブリックからスイッチを削除します。

Note このオプションは、ファブリックがフリーズモードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。

- プレビュー：保留中の設定と、実行中の設定と予想される設定の並べた比較をプレビューできます。
- ポリシーの：ポリシーを追加、更新、および削除します。ポリシーはテンプレート ライブラリで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、 ウィンドウで使用できる **[展開（Deploy）]** オプションを使用してスイッチに展開します。複数のポリシーを選択して表示できます。

Note 複数のスイッチを選択してポリシー インスタンスを展開する場合、選択したすべてのスイッチに展開されます。

- **[ThousandEyes Agent]**：スイッチで ThousandEyes Enterprise Agent を起動、停止、インストール、またはアンインストールできます。単一または複数のスイッチを選択し、**[ThousandEyes エージェント（ThousandEyes Agent）]** ドロップダウンリストから必要な操作を選択します。

Note ThousandEyes Enterprise Agent アクションを実行するために複数のスイッチを選択する場合は、選択したスイッチのステータスが同じであることを確認してください。

- インターフェイスの：スイッチ インターフェイスに構成を展開します。
- 履歴：このボタンを使用して、展開履歴とポリシー変更履歴を表示します。1 つ以上のスイッチを選択し、**[履歴（History）]** をクリックします。

  [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	生成後の構成
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	削除する構成が含まれます	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

Note 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。このインスタンスは、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。

- 展開：スイッチ構成を展開します。Cisco DCNM リリース 11.3(1) 以降では、**[展開（Deploy）]** ボタンを使用して複数のデバイスの構成を展開できます。

Note

- このオプションは、ファブリックがフリーズ モードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。
- MSD ファブリックでは、Border Gateway、Border Gateway Spine、Border Gateway Super-Spine、または外部ファブリック スイッチにのみ構成を展開できます。

- ロールの設定：同じデバイスタイプの 1 つ以上のデバイスを選択し、**[ロールの設定（Set Role）]** をクリックしてデバイスのロールを設定します。デバイス タイプは次のとおりです。
  - NX-OS
  - IOS XE
  - IOS XR
  - その他

  ロールを設定する前に、スイッチをメンテナンス モードからアクティブ モードまたは動作モードに移動したことを確認します。ロールの設定の詳細については、スイッチ操作の項を参照してください。
- vPC ペアリング：スイッチを選択し、**[vPC ペアリング（vPC Pairing）]** 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。詳細については、次の項を参照してください。
  - vPC セットアップの作成：外部ファブリックで vPC ペアを作成する方法について説明します。
  - vPC ファブリック ピアリング：簡単なファブリックで vPC ペアを作成する方法について説明します。

表形式ビュー：リンク

異なるファブリックの境界スイッチ間（ファブリック間）、または同じファブリック内のスイッチ間（ファブリック内）にリンクを追加できます。DCNM による管理対象のスイッチに対してのみ、ファブリック間接続（IFC）を作成できます。

物理的に接続する前にスイッチ間のリンクを定義する必要があるシナリオがあります。リンクは、ファブリック間リンクまたはファブリック内リンクです。そうすることで、リンクを追加する意図を表現して表すことができます。インテントのあるリンクは、実際に機能するリンクに変換されるまで、異なる色で表示されます。リンクを物理的に接続すると、接続済みとして表示されます。

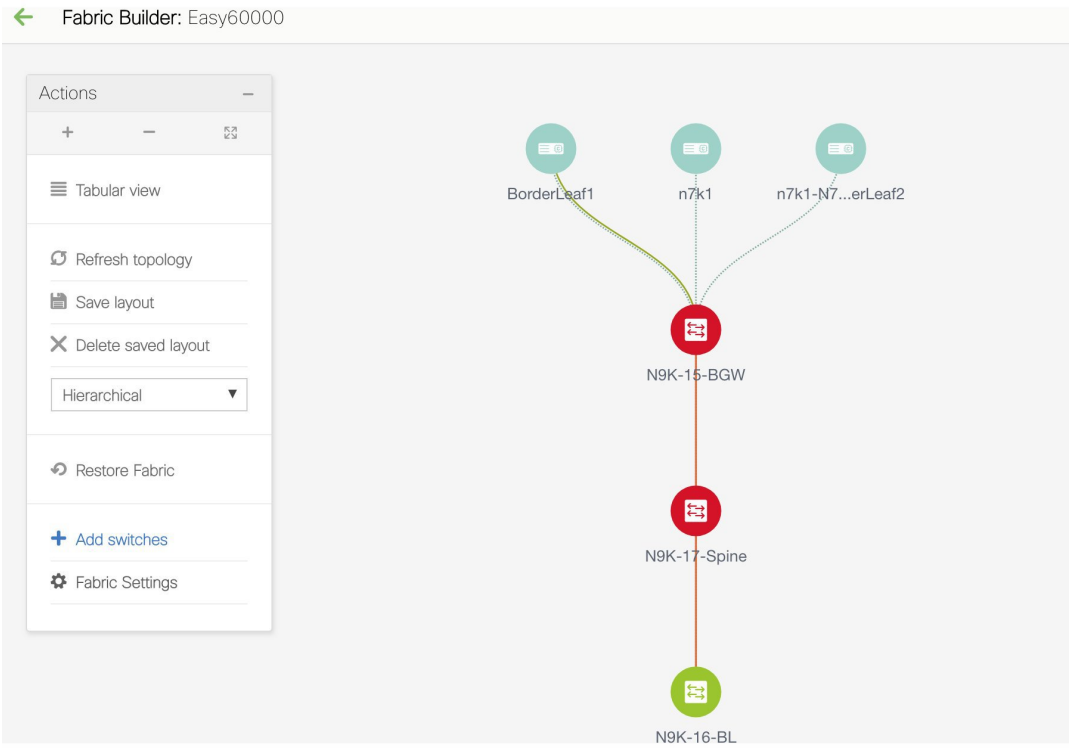
管理リンクは、ファブリックトポロジでは赤色のリンクとして表示される場合があります。このようなリンクを削除するには、リンクを右クリックし、**[リンクの削除（Delete Link）]** をクリックします。

Cisco DCNM リリース 11.1(1) 以降で、ボーダー スイッチのスイッチ ロールに、ボーダー スパイン ロールとボーダーゲートウェイ スパイン ロールが追加されます。

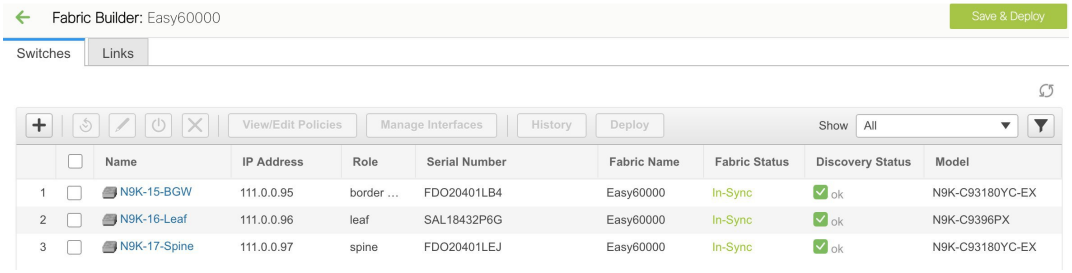
事前プロビジョニングされたデバイスを宛先デバイスとして選択することで、既存のデバイスと事前プロビジョニングされたデバイス間のリンクを作成できます。

ファブリック間リンクの作成

1. [制御（Control）] > [ファブリック ビルダ（Fabric Builder）] をクリックして、ファブリック ビルダ画面に移動します。
2. ファブリックを表す長方形のボックス内をクリックします。[ファブリック トポロジ(fabric topology)] 画面が表示されます。
3. ウィンドウの左側に表示される [アクション（Actions）] パネルの [表形式ビュー（Tabular view）] をクリックします。

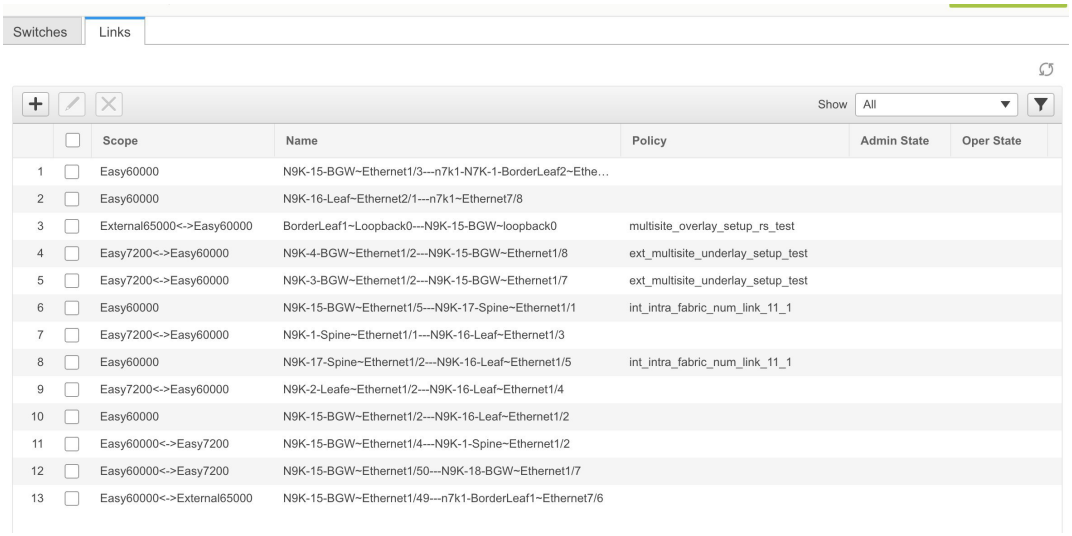


[スイッチ（Switches）] タブと [リンク（Links）] タブのあるウィンドウが表示されます。ファブリック スイッチとリンクをテーブルにリストします。



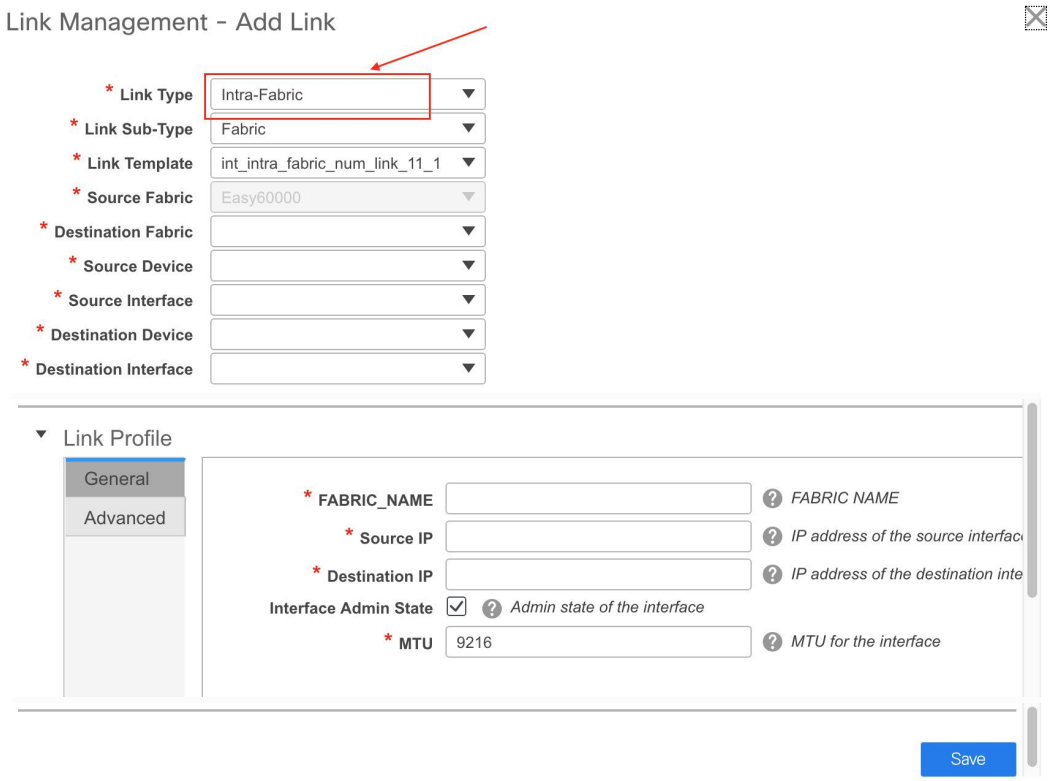
4. [リンク（Links）] タブをクリックします。リンクのリストを確認できます。

   まだリンクを作成していない場合、リストは空です。



5. 画面の左上にある [追加（+）（Add (+)）] ボタンをクリックしてリンクを追加します。

   [リンクの追加（Add Link）] 画面が表示されます。デフォルトでは、リンク タイプとして [ファブリック内（Intra-Fabric）] オプションが選択されています。



該当するフィールドは次のとおりです。

リンク タイプ：ファブリック内の2つのスイッチ間にリンクを作成するには、[ファブリック内（Intra-Fabric）] を選択します。

リンク サブタイプ：このフィールドは、これがファブリック内のリンクであることを示す「ファブリック」に入力されます。

リンク テンプレート：次のリンク テンプレートのいずれかを選択できます。

- int_intra_fabric_num_link_11_1：リンクが IP アドレスが割り当てられた 2 つのイーサネット インターフェイス間にある場合は、int_intra_fabric_num_link_11_1 を選択します。
- int_intra_fabric_unnum_link_11_1：リンクが 2 つの IP アンナンバード インターフェイス間にある場合は、int_intra_fabric_unnum_link_11_1 を選択します。
- int_intra_vpc_peer_keep_alive_link_11_1：リンクが vPC ピア キープアライブ リンクの場合は、int_intra_vpc_peer_keep_alive_link_11_1 を選択します。
- int_pre_provision_intra_fabric_link：リンクが2つの事前プロビジョニングされたデバイス間にある場合は、int_pre_provision_intra_fabric_link を選択します。**[保存と展開（Save & Deploy）]** をクリックすると、アンダーレイ サブネット IP プールから IP アドレスが選択されます。

これに対応して、[リンク プロファイル（Link Profile）] セクションのフィールドが更新されます。

送信元ファブリック：送信元ファブリックが既知であるため、このフィールドにファブリック名が入力されます。

宛先ファブリック：宛先ファブリックを選択します。ファブリック内リンクの場合、送信元と宛先のファブリックは同じです。

送信元デバイスと送信元インターフェイス：送信元デバイスと送信元インターフェイスを選択します。

宛先デバイスと宛先インターフェイス：宛先デバイスと宛先インターフェイスを選択します。

Note 既存のデバイスと事前プロビジョニングされたデバイスの間にリンクを作成する場合は、事前プロビジョニングされたデバイスを宛先デバイスとして選択します。

[リンク プロファイル（Link Profile）]セクションの **[全般（General）]** タブ

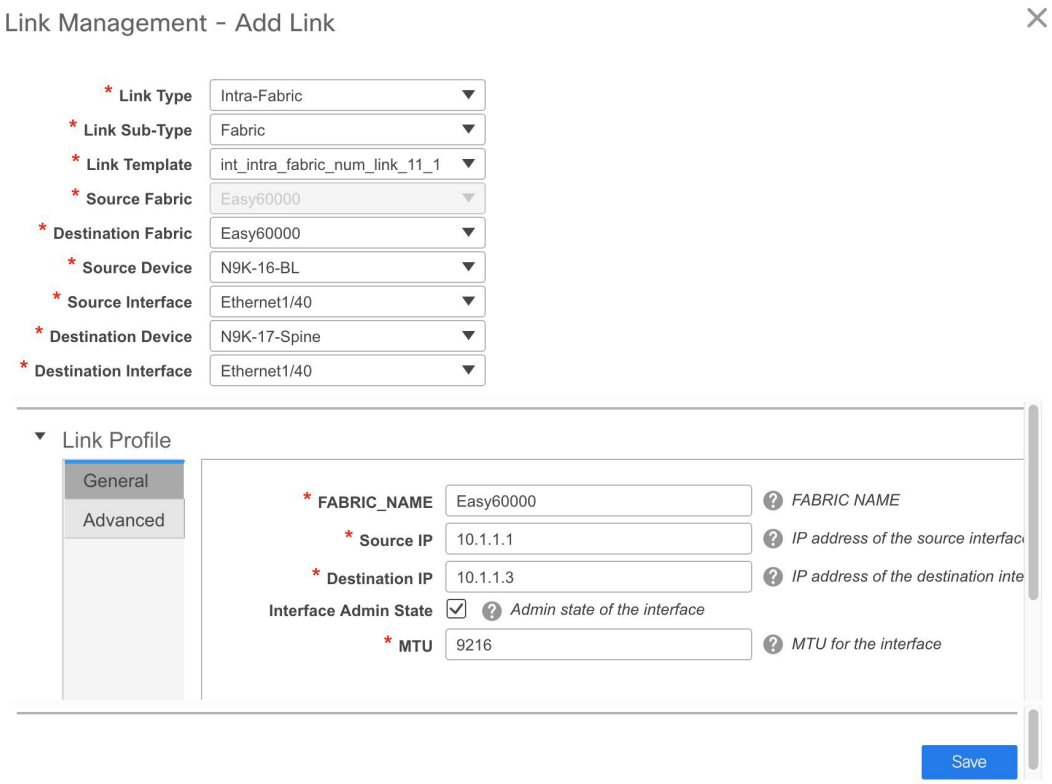
インターフェイス VRF：このインターフェイスのデフォルト以外の VRF の名前。

送信元 IP および宛先 IP：送信元と宛先インターフェイスの送信元 IP および宛先 IP アドレスをそれぞれ指定します。

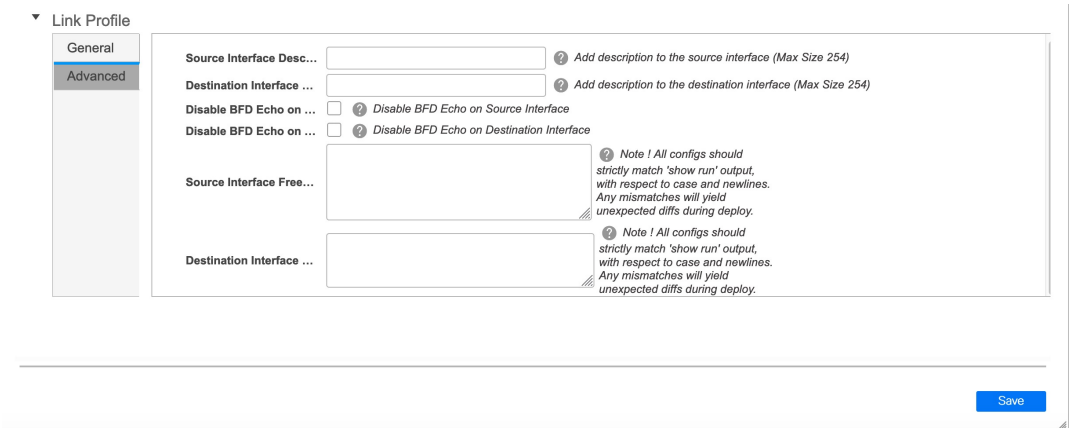
Note **[int_pre_provision_intra_fabric_link]** テンプレートを選択すると、[送信元 IP] フィールドと [接続先 IP] フィールドは表示されません。

インターフェイスの管理状態（Interface Admin State）：このチェックボックスをオンまたはオフにして、インターフェイスの管理状態を有効または無効にします。

MTU：2 つのインターフェイスの最大伝送単位（MTU）を指定します。



[詳細（Advanced）] タブ



[送信元インターフェイスの説明（Source Interface Description）] および [宛先インターフェイスの説明（Destination Interface Description）] : 後で使用するためのリンクについて説明します。たとえば、リンクがリーフ スイッチとルート リフレクタ デバイスの間にある場合は、これらのフィールドに情報を入力できます（リーフ スイッチからRR1へのリンク、およびRR1からリーフ スイッチへのリンク）。この説明は設定に変換されますが、スイッチにはプッシュされません。**[保存と展開（Save & Deploy）]** の後、実行構成に反映されます。

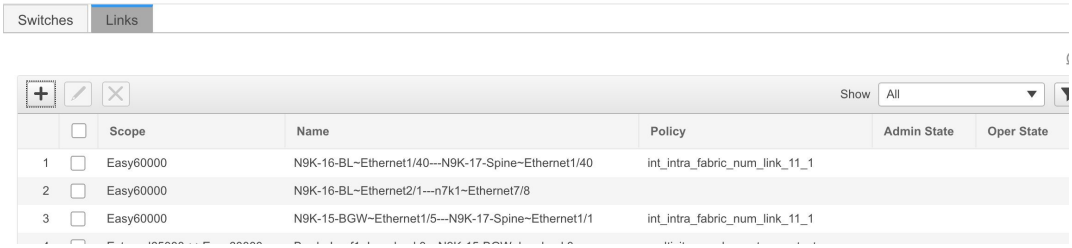
[送信元インターフェイスの BFD エコーの無効化（Disable BFD Echo on Source Interface）] および **[宛先インターフェイスの BFD エコーの無効化（Disable BFD Echo on Destination Interface）]**：送信元および宛先インターフェイスでBFDエコーパケットを無効にします。

BFD エコー フィールドは、ファブリック設定で BFD を有効にした場合にのみ適用されることに注意してください。

送信元インターフェイス フリーフォーム CLI および宛先インターフェイス フリーフォーム CLI（Source Interface Freeform CLIs and Destination Interface Freeform CLIs）：送信元と宛先インターフェイスに特別なフリーフォーム構成を入力してください。スイッチの実行構成に表示されている設定を、インデントなしで追加する必要があります。詳細な説明と例については、「ファブリック スイッチでの自由形式構成」セクションを参照してください。

6. 画面の下部にある [保存（Save）] をクリックします。

   リンク タブに新しいリンクが表示されます。



7. **[保存と展開（Save & Deploy）]** をクリックして、リンク構成をスイッチに展開します。

   [構成展開（Config Deployment）] 画面が表示されます。スイッチの構成ステータスが表示されます。[構成のプレビュー（Preview 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。[構成のプレビュー（Preview Config）]列のリンクをクリックすると、[構成プレビュー（Config Preview）] ウィンドウが表示されます。スイッチの保留中の設定が一覧表示されます。[並べて表示（Side-by-Side）] タブには、実行構成と予想される構成が並べて表示されます。

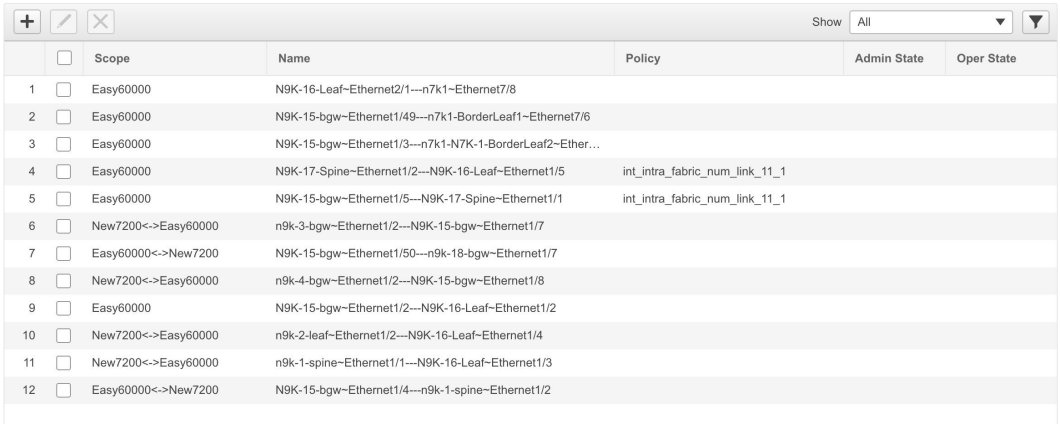
8. プレビュー画面を閉じて、[構成の展開（Deploy Config）] をクリックします。保留中の構成が展開されます。

9. すべての行で進行状況が 100% であることを確認したら、画面の下部にある [閉じる（Close）] をクリックします。[リンク（Links）] 画面が再び表示されます。

   画面の左上にある [<-] をクリックして、ファブリック トポロジに移動します。 ファブリック トポロジでは、2 つのデバイス間のリンクが表示されます。

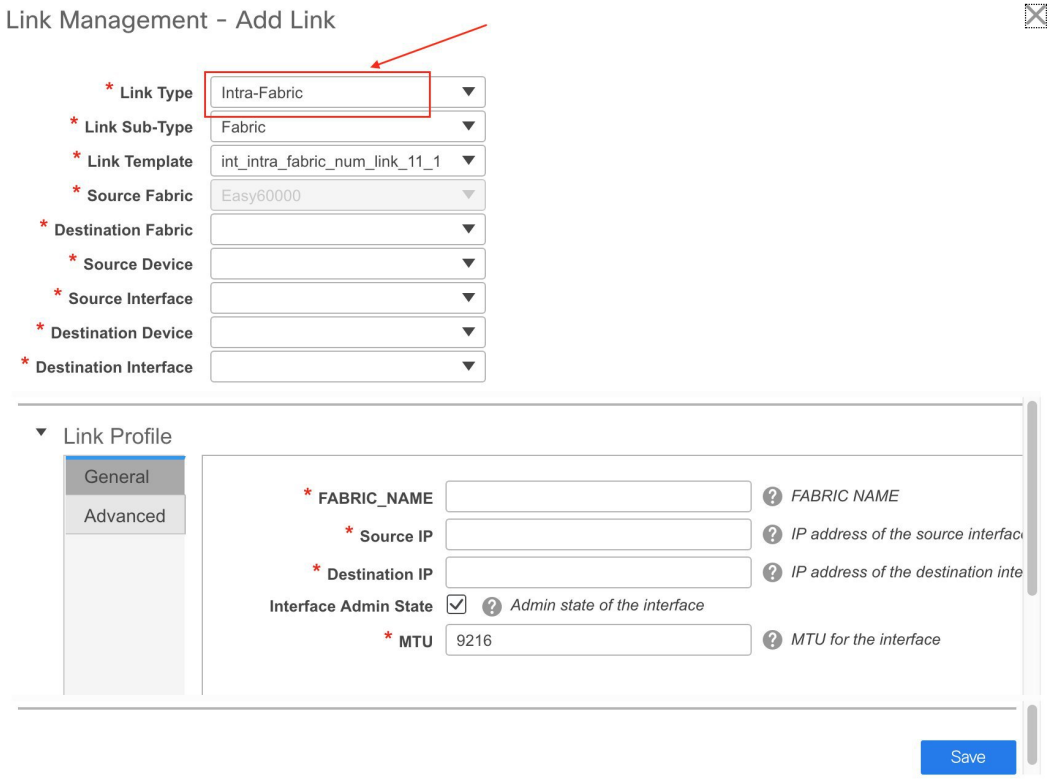
ファブリック内リンクの作成

1. [スイッチ | リンク（Switches | Links）] ページの [リンク（Links）] タブをクリックします。以前に作成されたリンクのリストが表示されます。リンクには、ファブリック内リンク（ファブリック内のスイッチ間）、およびファブリック間リンク（BGW 間、または異なるファブリックのボーダー リーフスイッチ/スパイン スイッチ間）が含まれます。

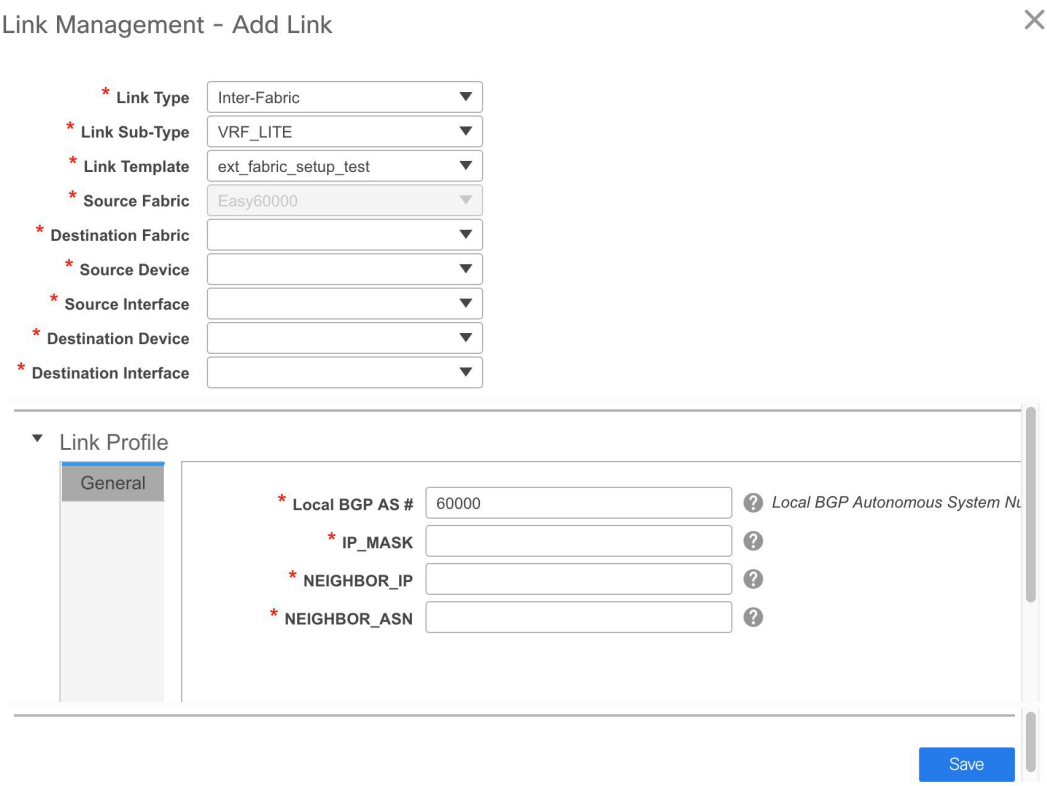


2. 画面の左上にある [追加（+）（Add (+)）] ボタンをクリックしてリンクを追加します。[リンクの追加（Add Link）] 画面が表示されます。

   デフォルトでは、リンク タイプとして [ファブリック内（Intra-Fabric）] オプションが選択されています。



3. IFC を作成しているため、[Link Type] ドロップダウン ボックスから [ファブリック間（Inter-Fabric）] を選択します。画面がそれに応じて変化します。



ファブリック間リンク作成のフィールドについて説明します。

リンク タイプ：ファブリック間（Inter-Fabric） を選択して、2 つのファブリック間の境界スイッチを介したファブリック間接続を作成します。

リンク サブタイプ：このフィールドは IFC タイプを入力します。ドロップダウン リストから **[VRF_LITE]**、**[MULTISITE_UNDERLAY]**、または **[MULTISITE_OVERLAY]** を選択します。

マルチサイト オプションについては、マルチサイトの使用例で説明します。

VXLAN MPLS 相互接続の詳細については、「*VXLAN BGP EVPN* ファブリック *-MPLS SR* および *LDP* ハンドオフの境界プロビジョニングの使用例」の章を参照してください。

ルーテッドファブリックの相互接続については、「*eBGP* アンダーレイを使用したファブリックの構成（*Configuring a Fabric with eBGP Underlay*）」の章の「ルーテッド ファブリックと外部ファブリック間のファブリック間リンクの作成（*Creating Inter-Fabric Links between a Routed Fabric and an External Fabric*）」の項を参照してください。

リンク テンプレート：リンク テンプレートが入力されます。

テンプレートには、選択内容に基づいて、対応するパッケージ済みのデフォルト テンプレートが自動的に入力されます。

Note ユーザ定義テンプレートを追加、編集、削除できます。詳細については、「制御」の章の「テンプレート ライブラリ」のセクションを参照してください。

[送信元ファブリック]：このフィールドには、送信元ファブリック名が事前に入力されています。

[宛先ファブリック]：このドロップダウンボックスから宛先ファブリックを選択します。

[送信元デバイスと宛先インターフェイス]：宛先デバイスに接続する送信元デバイスとイーサネット インターフェイスを選択します。

[宛先デバイスと宛先インターフェイス]：送信元デバイスに接続する宛先デバイスとイーサネット インターフェイスを選択します。

送信元デバイスと送信元インターフェイスの選択に基づいて、Cisco Discovery Protocol 情報（使用可能な場合）に基づいて宛先情報が自動入力されます。宛先外部デバイスが宛先ファブリックの一部であることを確認するために、追加の検証が実行されます。

[リンク プロファイル] セクションの **[全般]** タブ。

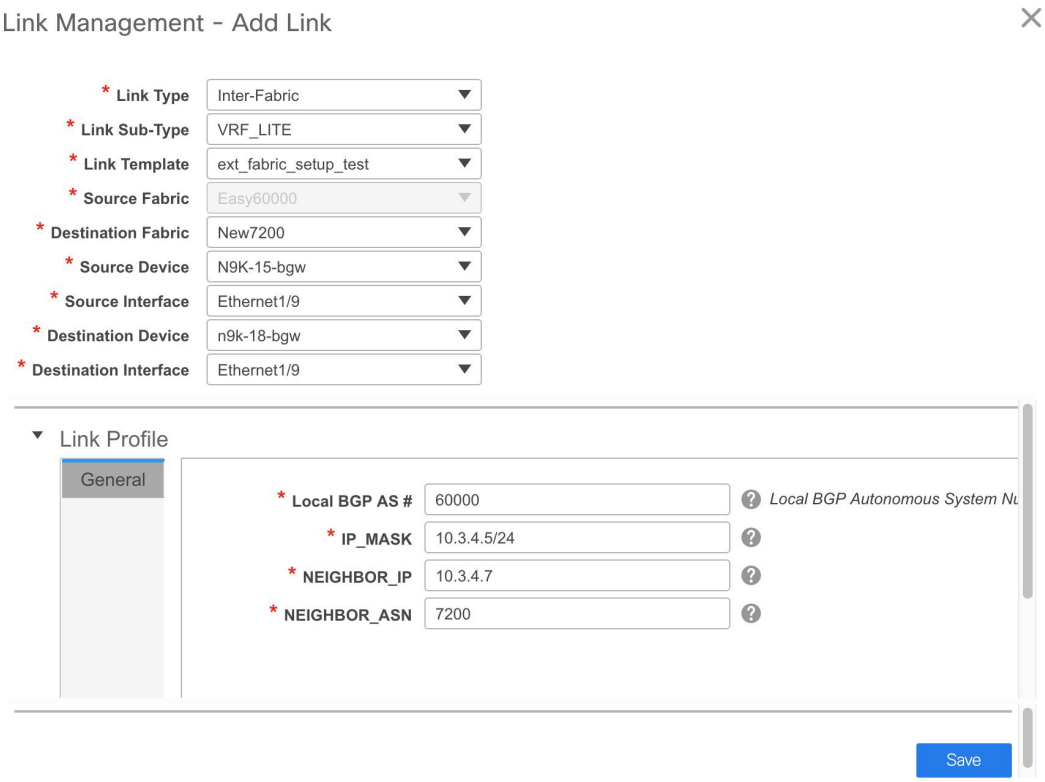
ローカル BGP AS # ：このフィールドには、送信元ファブリックの AS 番号が自動入力されます。

IP_MASK：宛先デバイスに接続する送信元インターフェイスの IP アドレスをこのフィールドに入力します。

NEIGHBOR_IP：宛先インターフェイスの IP アドレスをこのフィールドに入力します。

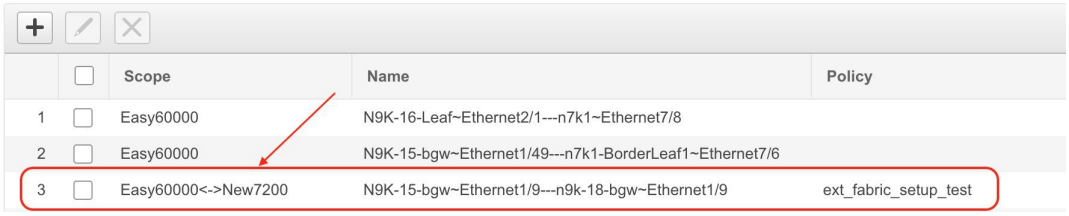
NEIGHBOR_ASN：このフィールドには、宛先デバイスの AS 番号が自動入力されます。

[リンクの追加（Add Link）] 画面に入力すると、次のようになります。



4. 画面の下部にある [保存（Save）] をクリックします。

   [スイッチ | リンク（Switches | Links）] 画面が再び表示されます。IFC が作成され、リンクのリストに表示されていることがわかります。



5. [保存と展開（Save & Deploy）] をクリックして、リンク構成をスイッチに展開します。

   [構成展開 (Config Deployment)] 画面が表示されます。スイッチの構成ステータスが表示されます。[構成のプレビュー（Preview 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。[構成のプレビュー（Preview Config）]列のリンクをクリックすると、[構成プレビュー（Config Preview）] ウィンドウが表示されます。スイッチの保留中の設定が一覧表示されます。[並べて表示（Side-by-Side）] タブには、実行構成と予想される構成が並べて表示されます。

6. プレビュー画面を閉じて、[構成の展開（Deploy Config）] をクリックします。保留中の構成が展開されます。

7. すべての行で進行状況が 100％ であることを確認したら、画面の下部にある [閉じる（Close）] をクリックします。[リンク（Links）] 画面が再び表示されます。
8. 画面の左上にある [<-] をクリックして、ファブリック トポロジに移動します。ファブリック トポロジでは、2 つのデバイス間のリンクが表示されます。

   2 つのファブリックが MSD のメンバー ファブリックである場合は、MSD トポロジにもリンクが表示されます。

ToExternalOnly メソッドまたは MSD ファブリック経由のマルチサイト機能を使用して VRF Lite 機能を有効にすると、（VXLAN ファブリック）ボーダー/BGW デバイスと接続された（外部ファブリック）エッジ ルータ/コア デバイス間で IFC が自動的に作成されます。ER/コア/ボーダー/BGW デバイスを削除すると、DCNM でそのスイッチとの間で対応する IFC（リンク PTI）が削除されます。その後、DCNM は次の保存および展開操作で、残りのデバイスから対応する IFC 構成（存在する場合）を削除します。また、IFC およびオーバーレイ拡張を備えたデバイスをそれらの IFC から削除する場合は、それらの IFC に対応するすべてのオーバーレイ拡張を展開して、スイッチを削除できるようにする必要があります。

VRF 拡張を展開解除するには、[制御（Control）] > [ネットワークと VRF（Networks & VRFs）] をクリックして、VXLAN ファブリックと拡張 VRF を選択し、VRF 展開画面で VRF を展開解除します。

IFC を削除するには、[制御（Control）] > [ファブリック ビルダ（Fabric Builder）] をクリックし、ファブリック トポロジ画面に移動し、[表形式ビュー（Tabular view）] をクリックして、[リンク（Links）] タブから IFC を削除します。

ファブリック スイッチ名が一意であることを確認します。同じ名前のスイッチに VRF 拡張を導入すると、設定が誤ってしまいます。

新しいファブリックが作成され、DCNM でファブリックスイッチが検出され、これらのスイッチでアンダーレイ ネットワークがプロビジョニングされ、DCNM とスイッチ間の構成が同期されます。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。インターフェイスを参照してください。
- オーバーレイ ネットワークと VRF を作成し、スイッチに展開します。「ネットワークおよび VRF の作成と展開」を参照してください。

リンクのエクスポート

1. **[制御（Control）]> > [ファブリック ビルダ（Fabric Builder）]** の順に選択し、1 つのファブリックを選択します。

   ファブリック トポロジ ウィンドウが表示されます。
2. **[アクション（Actions）]** パネルで **[表形式ビュー（Tabular view）]** をクリックします。

   [スイッチ（Switches）] タブと **[リンク（Links）]** タブのあるウィンドウが表示されます。
3. **[リンク（Links）]** タブをクリックします。

リンクのリストを確認できます。まだリンクを作成していない場合、リストは空です。

4. **[リンクのエクスポート（Export Links）]** アイコンをクリックしてリンクを CSV ファイルにエクスポートします。

   リンクの次の詳細がエクスポートされます。リンクテンプレート、送信元ファブリック、宛先ファブリック、送信元デバイス、宛先デバイス、送信元スイッチ名、宛先スイッチ名、送信元インターフェイス、宛先インターフェイス、および nvPairs。nvPairs フィールドは JSON オブジェクトで構成されます。

リンクのインポート

リンクの詳細を含む CSV ファイルをインポートして、ファブリックに新しいリンクを追加できます。CSV ファイルには、リンクテンプレート、送信元ファブリック、宛先ファブリック、送信元デバイス、宛先デバイス、送信元スイッチ名、宛先スイッチ名、送信元インターフェイス、宛先インターフェイス、および nvPairs の詳細が含まれている必要があります。

Note

- 既存のリンクは更新できません。
- **[リンクのインポート（Import Links）]** アイコンは、外部ファブリックでは無効です。

1. **[制御（Control）]**> > **[ファブリック ビルダ（Fabric Builder）]** の順に選択し、1 つのファブリックを選択します。

   ファブリック トポロジ ウィンドウが表示されます。

2. **[アクション（Actions）]** パネルで **[表形式ビュー（Tabular view）]** をクリックします。

   [スイッチ（Switches）] タブと **[リンク（Links）]** タブのあるウィンドウが表示されます。

3. **[リンク（Links）]** タブをクリックします。

   リンクのリストを確認できます。まだリンクを作成していない場合、リストは空です。

4. **[リンクのインポート（Import Links）]** アイコンをクリックします。

   ファイル サーバ ディレクトリが開きます。

5. ディレクトリを参照し、インポートする CSV ファイルを選択します。

6. [開く（Open）] をクリックします。

   確認の画面が表示されます。

7. **[はい（Yes）]** をクリックして、選択したファイルをインポートします。

ファブリック リンクの詳細の表示

ファブリック ビルダのトポロジ表示で、アンダーレイを展開するリンク間の IP サブネット、MTU、速度の不一致などのファブリック リンクに関する情報を表示できます。Cisco DCNM Web クライアントからリンクの詳細を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** の順に選択し、1 つのファブリックを選択します。

ファブリックのトポロジ表示が表示されます。

ステップ 2 いずれかのリンクをダブルクリックします。

詳細ウィンドウが表示されます。このリンクを使用して接続されているデバイス、サマリ、およびデータトラフィックを表示できます。

ステップ 3 **[さらに詳細を表示（Show more details）]** をクリックします。

リンクで接続されている 2 つのデバイスの比較表が表示されます。これには、デバイスの次のパラメータが含まれます。デバイス名、名前、管理ステータス、動作ステータス、理由、ポリシー、オーバーレイ ネットワーク、ステータス、PC、vPC ID、速度、MTU、モード、VLAN、IP またはプレフィックス、VRF、ネイバー、および説明。

Note
- ハイパーリンクのあるデバイス名をクリックすると、ファブリック リンクのトラフィックの詳細を表示できます。または、詳細ウィンドウでこれらのトラフィックの詳細を表示できます。詳細については、「ファブリック リンクのトラフィックの詳細の表示」セクションを参照してください。
- ハイパーリンクのあるポリシーをクリックすると、ファブリック リンクの予想される構成を表示できます。

ステップ 4 **[戻る（Back）]** アイコンをクリックして、詳細ウィンドウに戻ります。

Note **[閉じる（Close）]** アイコンをクリックして、詳細ウィンドウを終了できます。

ファブリック リンクのトラフィック詳細の表示

ファブリック リンクの詳細ウィンドウで、トラフィックの詳細を表示する方法を選択できます。期間、形式に基づいてトラフィックの詳細を表示し、この情報をエクスポートできます。

[期間（Duration）] ドロップダウンリストでは、次のリンクのデータ トラフィックを表示することができます。

- 24 時間
- 週

- 月
- 年

表示：**[表示（Show）]** をクリックし、ドロップダウン リストから **[チャート（Chart）]**、**[表（Table）]**、または **[チャートと表（Chart and Table）]** を選択して、トラフィックの詳細を表示する方法を表示します。ブラウザ ウィンドウを拡大して、**[チャートと表形式（Chart and Table）]** フォーマットで詳細を表示します。

[チャート（Chart）] を選択した場合、トラフィック チャートにカーソルを合わせると、Y 軸に沿って、対応する時間の Rx 値と Tx 値が X 軸に沿って表示されます。時間範囲セレクターのスライダを動かすことで、X 軸の持続時間の値を変更できます。Rx および Tx チェック ボックスをオンまたはオフにして、Y 軸の値を選択できます。

（注） 期間として**週**、**月**、または**年**を選択すると、Y 軸に沿ってピーク受信およびピーク送信の値を表示することもできます。

[表（Table）] を選択して、交通情報を表形式で表示します。

[チャート タイプとチャートのオプション（Chart Type and Chart Options）]：**[チャート タイプ（Chart Type）]** ドロップダウン リストから **[エリア チャート（Area Chart）]** または **[ライン チャート（Line Chart）]** を選択します。

次のチャート オプションを選択できます。

- **塗りつぶしのパターンを表示**
- **データ マーカーを表示**
- **Y軸(対数目盛)**

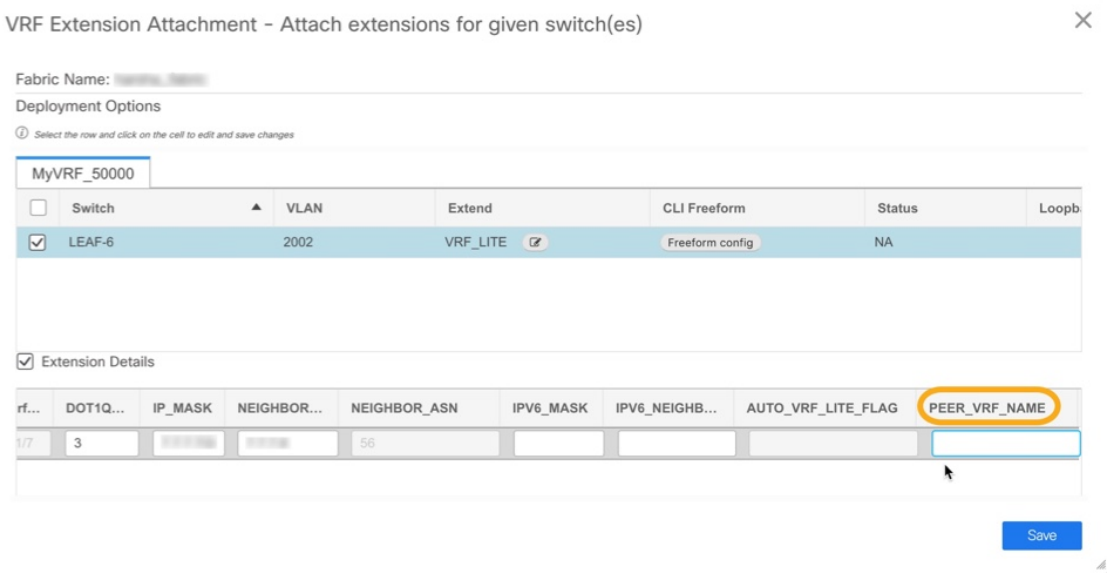
アクション：**[アクション（Actions）]** ドロップダウン リストから適切なオプションを選択して、トラフィック情報をエクスポートまたは印刷します。

シンメトリック自動 VRF Lite

- **[リンク管理（Link Management）]** ダイアログボックスの **[自動展開フラグ（Auto Deploy Flag）]** 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、管理対象デバイスのリンクの両端で、VRF lite 展開が有効になります。
- バックツーバック シナリオで VRF lite を拡張する場合、VRF はピア ファブリックにすでに存在している必要があり、VRF 名は同じである必要があります。VRF がピア ファブリック内にない場合に、VRF Lite を拡張しようとすると、エラー メッセージが表示されます。
- Easy ファブリックと外部ファブリックの間で VRF Lite を拡張する場合、VRF 名は、送信元ファブリック、デフォルト、または別の VRF 名と同じにすることができます。ただし、サブインターフェイスの子 PTI および外部ファブリックでの VRF の作成またはピアリン

グには送信元があります。したがって、**[ポリシーの表示/編集（View/Edit policies）]**ウィンドウからポリシーを編集または削除することはできません。

- DCNM アップグレードを実行し、ポリシーが IFC にアタッチされていないことに気付いた場合は、ポリシーと VRF を編集して、それらを再度アタッチします。
- IPv6 アドレスの他に、IP マスク、IPv4 アドレス、ネイバー IP アドレスも入力して、対称 VRF lite を使用してトップダウンから VRF を展開します。
- 両方のファブリックに構成を展開します。



- VXLAN ファブリックの **[リンク（Link）]** タブで IFC を編集または削除できます。自動構成 IFC に関する追加の考慮事項は、次回の保存および展開時に IFC が再生成されないようにするために、モードを手動モードに戻すか、関連するデバイスでのみ構成を保存することです。
- バックツーバック シナリオでは、ファブリックの 1 つで VRF lite IFC を削除すると、VRF lite はピア ファブリックからも削除されます。
- Easy ファブリックと外部ファブリックの間の VRF ライトを削除する場合は、トップダウン方式を使用して Easy ファブリック内の拡張を削除します。拡張は外部ファブリックから自動的に削除されます。
- 両方のファブリックに構成を展開します。

VRF Lite でのユースケースについては、「*VXLAN BGP EVPN* ファブリックでのボーダー プロビジョニングのユースケース：*VRF Lite*」の章を参照してください。

レイヤ 3 ポートチャネル

Cisco DCNM リリース 11.3(1) 以降、レイヤ 3 ポートチャネルは外部リンクおよびインターフェイスでサポートされます。**[インターフェイス（Interfaces）]** ウィンドウでは、ポートチャネルおよび対応するレイヤ 3 ポートチャネル インターフェイス テンプレートを選択できます。このテンプレートを使用すると、レイヤ3インターフェイス関連のすべての構成を指定する機能など、レイヤ 3 ポートチャネルに関連するさまざまなオプションを構成できます。レイヤ 3 ポートチャネルは、Easy ファブリックと外部ファブリックでのみサポートされます。

VRF_LITE を使用した外部接続も、レイヤ 3 ポートチャネルを使用してサポートされます。物理ルーテッドインターフェイスおよびレイヤ3ポートチャネルインターフェイスの場合、MTU を設定できます。

Cisco DCNM でレイヤ 3 ポートチャネルを使用して対称 VRF Lite を拡張する方法を示すビデオも視聴できます。「レイヤ 3 ポートチャネルを使用した対称 VRF Lite の拡張」ビデオを参照してください。

インターフェイス上にレイヤ 3 ポートチャネルを構成する

Cisco DCNM Web UI からインターフェイス上にレイヤ 3 ポートチャネル を構成するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）]** > **[ファブリック（Fabrics）]** > **[インターフェイス（Interfaces）]** の順に選択します。

[インターフェイス（Interfaces）] ウィンドウが表示されます。

ステップ 2 [インターフェイスの追加（Add Interface）] をクリックします。

[Add Interface] ダイアログボックスが表示されます。

ステップ 3 **[ポートチャネル（Port Channel）]** のタイプとデバイスを選択します。

port-channel ID が自動入力されます。

ステップ 4 **[int_l3_port_channel]** ポリシーを選択します。

それに伴い **[全般（General）]** エリアにあるフィールドが変更されます。

ステップ 5 フィールドに値を入力し、**[保存（Save）]** をクリックします。

保存された設定のみがデバイスにプッシュされます。インターフェイスの追加中は、最初の保存後にのみポリシー属性を変更できます。既に使用している ID を使用しようとすると **Resource could not be allocated** エラーが表示されます。

ステップ 6 (Optional) **[プレビュー（Preview）]** オプションをクリックして、展開する構成をプレビューします。

ステップ 7 **[展開（Deploy）]** をクリックして、指定した論理インターフェイスを展開します。

新しく追加したインターフェイスが画面に表示されます。左上にあるブレークアウトオプションを使用してインターフェイスのブレークアウト、およびブレークアウト解除ができます。

IOS XE デバイス向けのインターフェイス上にレイヤ 3 ポートチャネルを構成する

IOS XE デバイス向けのインターフェイス上にレイヤ 3 ポートチャネル を構成するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [インターフェイス（Interfaces）]** の順に選択します。

[インターフェイス（Interfaces）] ウィンドウが表示されます。

ステップ 2 [インターフェイスの追加（Add Interface）] をクリックします。

[Add Interface] ダイアログボックスが表示されます。

ステップ 3 **[ポートチャネル（Port Channel）]** のタイプとデバイスを選択します。

port-channel ID が自動入力されます。

ステップ 4 **[ios_xe_int_l3_port_channel]** ポリシーを選択します。

それに伴い **[全般（General）]** エリアにあるフィールドが変更されます。

ステップ 5 フィールドに値を入力し、**[保存（Save）]** をクリックします。

保存された設定のみがデバイスにプッシュされます。インターフェイスの追加中は、最初の保存後にのみポリシー属性を変更できます。既に使用しているIDを使用しようとすると **Resource could not be allocated** エラーが表示されます。

（注） Cisco Catalyst 9000 シリーズ スイッチのポートチャネル ID の範囲は 1 ～ 128 で、Cisco ASR 1000 シリーズ ルータの範囲は 1 ～ 64 です。

ステップ 6 （任意） **[プレビュー（Preview）]** オプションをクリックして、展開する構成をプレビューします。

ステップ 7 **[展開（Deploy）]** をクリックして、指定した論理インターフェイスを展開します。

新しく追加したインターフェイスが画面に表示されます。

非 Nexus デバイスの物理インターフェイスへのポリシーの展開

Cisco DCNM リリース 11.4(1) からの非 Nexus デバイスをサポートするためのポリシーがさらに追加されました。非Nexusデバイスを外部ファブリックにインポートすると、ポートの数に基

づいてデフォルトでいくつかの物理インターフェイスが作成されます。ポリシーは、管理ポートに対してのみ作成されます。Cisco Catalyst 9000 シリーズ スイッチの場合、管理ポートは GigabitEthernet0/0 であり、Cisco ASR 1000 シリーズ ルータの場合、管理ポートは GigabitEthernet0 です。

次の表に、さまざまな 非 Nexus デバイスに追加されたポリシーを示します。

デバイス	ポリシー
Cisco CSR 1000v シリーズ ルータ	ギガビットイーサネット
Cisco IOS-XE デバイス	• GigabitEthernet_mgmt • ios_xe_int_access_host • ios_xe_int_freeform • ios_xe_int_routed_host • ios_xe_int_trunk_host （注） GigabitEthernet0/0 である管理ポートにのみ GigabitEthernet_mgmt ポリシーを使用します。

Cisco DCNM Web UI の **[インターフェイス（Interfaces）]** ウィンドウで物理インターフェイスにポリシーを展開するには、次の手順を実行します。

始める前に

非 Nexus デバイスを外部ファブリックにインポートして検出します。ファブリックがモニタ モードになっていないことを確認してください。

手順

ステップ 1 ポリシーを展開するインターフェイスのチェックボックスをオンにします。

ステップ 2 **[構成の編集（Edit Configuration）]** アイコンをクリックします。

ステップ 3 ドロップダウンリストから **[ポリシー（Policy）]** を選択します。

有効なオプションは次のとおりです。

- **ギガビットイーサネット**
- **GigabitEthernet_mgmt**
- **ios_xe_int_access_host**
- **ios_xe_int_freeform**
- **ios_xe_int_routed_host**
- **ios_xe_int_trunk_host**

（注）
- 選択したオプションに基づいて、**[全般（General）]** エリアの下のフィールドは異なります。
- **ios_xe_int_routed_host** ポリシーを選択した場合は、VRF が帯域外で手動で構成されているか、**[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウで **ios_xe_switch_freeform** ポリシーを使用していることを確認してください。
- DCNM は NVE または BDI インターフェイスをサポートしていません。ただし、それらを手動またはアウトオブバンドですでに作成している場合は、**ios_xe_int_freeform** ポリシーを使用して構成を定義します。

ステップ 4 すべての必須フィールドに値を入力します。

（注） デバイスに基づいて速度を選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 **[プレビュー（Preview）]** をクリックし、保留中の構成をプレビューします。

ステップ 7 **[展開（Deploy）]** をクリックして、インターフェイスのポリシーを展開します。

サブインターフェイス上にレイヤ 3 ポートチャネルを構成する

Cisco DCNM Web UI からインターフェイス上にレイヤ 3 ポートチャネル を構成するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）]** > **[ファブリック（Fabrics）]** > **[インターフェイス（Interfaces）]** の順に選択します。

[インターフェイス（Interfaces）] ウィンドウが表示されます。

ステップ 2 レイヤ 3 ポートチャネル インターフェイスを選択します。

ステップ 3 [インターフェイスの追加（Add Interface）] をクリックします。

[Add Interface] ダイアログボックスが表示されます。

ステップ 4 **[サブインターフェイス（Subinterface）]** タイプを選択します。

サブインターフェイス ID とポリシーが自動入力され、**[全般（General）]** エリアのフィールドがそれに応じて変更されます。

ステップ 5 フィールドに値を入力し、**[保存（Save）]** をクリックします。

保存された設定のみがデバイスにプッシュされます。

ステップ 6 (Optional) **[プレビュー（Preview）]** オプションをクリックして、展開する構成をプレビューします。

ステップ 7 **[展開（Deploy）]** をクリックして、指定した論理インターフェイスを展開します。

確認ウィンドウが表示され、新しく追加されたサブインターフェイスがリストに表示されます。

ファブリック間接続のためのレイヤ 3 ポートチャネルの構成

[ファブリック ビルダ（Fabric Builder）] ウィンドウからレイヤ 3 ポートチャネル リンクを構成するには、次の手順を実行します。

Before you begin

インターフェイスにレイヤ 3 ポートチャネルが作成されていることを確認します。

Procedure

ステップ 1 VRF-Lite を拡張する Easy ファブリックまたは外部ファブリックを選択します。

ファブリック トポロジ ウィンドウが表示されます。

ステップ 2 **[アクション（Actions）]** ペインで **[表形式ビュー（Tabular view）]** をクリックします。

このファブリックのすべてのコンポーネントは、ステータスとその他の詳細とともにさまざまなタブに表示されます。

ステップ 3 **[リンク（Links）]** タブを選択します。

ステップ 4 **[リンクの追加（Add Link）]** アイコンをクリックします。

[リンクの追加（Add Link）] ダイアログボックスが表示されます。

ステップ 5 **[Inter-Fabric]** リンク タイプを選択します。

ステップ 6 **[VRF_LITE]** リンク サブタイプを選択します。

ステップ 7 **[テンプレートのリンク（Link Template）]** ドロップダウンリストから [テンプレートのリンク（link template）] を選択します。

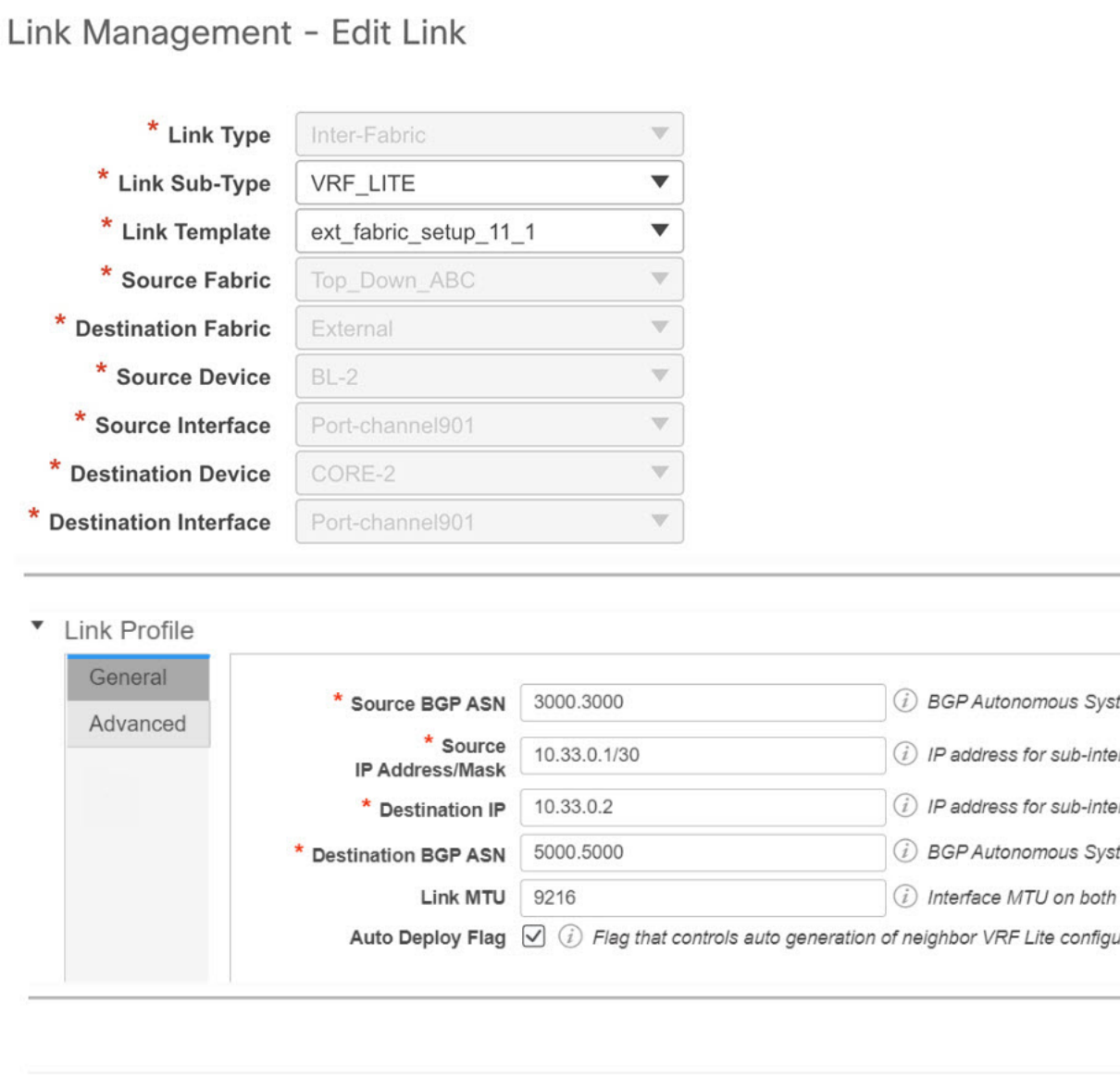
有効な値は、**[ext_fabric_setup_11_1]** および **[service_link_trunk]** です。

ステップ 8 それに応じて、他のすべてのフィールドに詳細を入力します。

ステップ 9 必要に応じて、**[リンク プロファイル（Link Profile）]** エリアのフィールドに詳細を入力します。

MTU を設定できます。**[Ext_VRF_Lite_Jython]** 自動展開テンプレートは、ファブリック内のデバイスの VRF-Lite 構成に使用されます。

ステップ 10 [保存（Save）] をクリックします。



What to do next

トップダウン フローを使用してレイヤ 3 ポートチャネルで VRF Lite IFC を作成した後、VRF Lite を使用して VRF を拡張すると、レイヤ 3 ポートチャネルにサブインターフェイスが作成されます。VRF が拡張された後でも、レイヤ 3 ポートチャネル リンクを編集できます。ただし、レイヤ 3 ポートチャネルは、ファブリック内リンクではサポートされていません。

表形式ビュー：操作ビュー

Cisco DCNM 11.3(1) から、ファブリックの運用サポートが提供されます。この機能は、次の情報を提供します。

- ファブリックの稼働状況
- アラームとイベント通知

[操作表示（Operational View）] タブで操作ステータス情報を表示できます。Cisco DCNM の上部ペインにある **[ヘルプ（Help）]** アイコンの横にある **[アラートと通知（Alerts and Notifications）]** アイコンをクリックすると、アラートとイベント通知を表示できます。

動作ステータスの表示

[ファブリック ビルダ（Fabric Builder）] ウィンドウからファブリックの動作ステータスを表示するには、次の手順を実行します。

手順

ステップ 1 ファブリックを選択します。
ファブリック トポロジ ウィンドウが表示されます。

ステップ 2 **[アクション（Actions）]** ペインで **[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 **[操作表示（Operational View）]** タブを選択します。

[操作表示（Operational View）] タブには、次のフィールドと説明があります。

フィールド	説明
Fabric Name（ファブリック名）	リンクのあるファブリックを指定します。
Name	リンクの名前を指定します。
Is Present	リンクが存在するかどうかを指定します。有効な値は **true** と **false** です。

フィールド	説明
リンクステータス	論理的リンクのステータスを指定します。論理リンクは、次のいずれかの状態になります。 • **[確立済み（Established）]**：リンクが **[確立済み（Established）]** 状態の場合、ピアは更新メッセージを送信して、BGP ピアにアドバタイズされた各ルートに関する情報を交換します。エラーが発生し、状態が **[Idle]** に変わると、通知が送信されます。**[確立（Established）]** 状態にできるのは、BGP ルーティング プロトコルを使用するリンクのみです。 • **[Idle]**：ピア間でエラーが発生した場合、BGP プロトコルを使用するリンクは [アイドル（Idle）] 状態になります。 • **[UP]**：ピア間でリンクが正常に確立されると、ISIS プロトコルを使用するリンクは **[UP]** 状態になります。 • **[FULL]**：ピア間でリンクが正常に確立されると、OSPF プロトコルを使用するリンクは **[FULL]** 状態になります。 • **[peer-alive]**：vPC ピア スイッチのバイタリティをモニタするピア キープアライブ リンクとしてリンクを指定します。
リンクタイプ	論理リンクのタイプを指定します。リンクは次のタイプにすることができます。 • **BGP** • **ISIS** • **OSPF** • **[VPC_KEEPALIVE]**
稼働時間	リンク タイプの稼働時間を指定します。

これらすべての列が並べ替え可能です。

論理リンクの表示

[トポロジ（Topology）] ウィンドウに論理リンクが表示されます。Cisco DCNM Web UI から論理リンクを表示するには、次の手順を実行します。

手順

ステップ 1 **[トポロジ（Topology）]** を選択します。

[トポロジ（Topology）] ウィンドウが表示されます。

ステップ 2 [表示（Show）] ペインの **[論理リンク（Logical Links）]** チェック ボックスをオンにします。

デバイス間の論理リンクは青色で表示されます。

（注） リンクの色は、状態に基づいて変化します。

ステップ 3 （任意） リンクにカーソルを合わせると、リンク タイプが表示されます。

アラートとイベント通知の表示

アラートおよびイベント通知には、正常性スコア、トポロジ ノード表示、アラーム ビュー、アラーム ポリシー、および通知サービスが含まれます。イベントは、ネットワーク、デバイス、またはCisco DCNMに影響を与えるアクションです。アラートは、イベントの一部としてトリガーされて表示される通知です。

ToR スイッチのサポート

Cisco DCNM 11.3(1)以降、トップオブラック（ToR）スイッチのサポートがDCNMに追加されました。外部ファブリックにレイヤ 2 ToR スイッチを追加でき、それらを Easy ファブリックのリーフ スイッチに接続できます。詳細については「*ToR* スイッチの構成とネットワークの展開」を参照してください。

vPC ファブリック ピアリング

2 台のスイッチの仮想ピア リンクを作成するか、既存の物理ピア リンクを仮想ピア リンクに変更できます。Cisco DCNM リリース 11.2(1) で vPC ファブリック ピアリングをサポートするのは、グリーンフィールド展開だけです+ ただし、グリーンフィールド展開とブラウンフィールド展開の両方で、Cisco DCNM リリース 11.3(1) の vPC ファブリック ピアリングがサポートされます。この機能は、**Easy_Fabric_11_1** および **Easy_Fabric_eBGP** ファブリック テンプレートに適用されます。

（注） **Easy_Fabric_eBGP** ファブリックは、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。

ガイドラインと制約事項

次に、vPC ファブリック ピアリングの注意事項と制限事項を示します。

- vPC ファブリック ピアリングは、Cisco DCNM リリース 11.2(1) および Cisco NX-OS リリース 9.2(3) からサポートされています。

- Cisco Nexus N9K-C9332C スイッチ、Cisco Nexus N9K-C9364C スイッチ、Cisco Nexus N9K-C9348GC-FXP スイッチ、および FX で終わる Cisco Nexus 9000 シリーズ スイッチ、FX2 だけが vPC ファブリック ピアリングをサポートします。
- Cisco DCNM リリース 11.4(1) 以降、Cisco Nexus N9K-C93180YC-FX3S および N9K-C93108TC-FX3P プラットフォーム スイッチは vPC ファブリック ピアリングをサポートします。
- Cisco Nexus 9300-EX 、および 9300-FX/FXP/FX2/FX3 プラットフォーム スイッチは、vPC ファブリック ピアリングをサポートします。Cisco Nexus 9200 および 9500 プラットフォーム スイッチは、vPC ファブリック ピアリングをサポートしていません。
- 他の Cisco Nexus 9000 シリーズ スイッチを使用している場合、**[保存して展開（Save & Deploy）]** 中に警告が表示されます。これらのスイッチは将来のリリースでサポートされるため、警告が表示されます。
- **[仮想ピアリンクを使用（Use Virtual Peerlink）]** オプションを使用して、vPC ファブリック ピアリングをサポートしていないスイッチをペアリングしようとすると、ファブリックの展開時に警告が表示されます。
- オーバーレイの有無にかかわらず、物理ピア リンクを仮想ピア リンクに、またはその逆に変換することができます。
- ボーダー ゲートウェイのリーフ ロールを持つスイッチは、vPC ファブリック ピアリングをサポートしていません。
- vPC ファブリック ピアリングは、Cisco Nexus 9000 シリーズ モジュラ シャーシおよび FEX ではサポートされていません。これらのいずれかをペアリングしようとすると、**[保存して展開中（Save & Deploy）]** にエラーが表示されます。
- ブラウンフィールド展開とグリーンフィールド展開は、Cisco DCNM リリース 11.3(1) の vPC ファブリック ピアリングをサポートします。
- ただし、物理ピア リンクを使用して接続されているスイッチをインポートし、**[保存して展開（Save & Deploy）]** 後に物理ピア リンクを仮想ピア リンクに変換することはできます。機能の設定中に TCAM リージョンを更新するには、構成端末で **hardware access-list tcam ingress-flow redirect** *512* コマンドを使用します。

ファブリック vPC ピアリングの QoS

Cisco DCNM リリース 11.4(1) 以降、**Easy_Fabric_11_1** ファブリック設定で、vPC ファブリック ピアリング通信の配信を保証するためにスパインで QoS を有効にできます。さらに、QoS ポリシー名を指定できます。

グリーンフィールド展開については、次のガイドラインに注意してください。

- QoS が有効で、ファブリックが新しく作成された場合：
  - スパインまたはスーパー スパイン ネイバーが仮想 vPC である場合に、スーパー スパインが存在しているなら、スーパー スパインからリーフまたはボーダーからスパインなどの無効なリンクからのネイバーが優先されないようにします。

- Cisco Nexus 9000 シリーズ スイッチ モデルに基づいて、**switch_freeform** ポリシー テンプレートを使用して、推奨されるグローバル QoS 構成を作成します。
- スパインから正しいネイバーへのファブリック リンクで QoS を有効にします。

- QoS ポリシー名が編集されている場合は、ポリシー名の変更がすべての場所（グローバルとリンクなど）に適用されることを確認してください。
- QoS が無効になっている場合は、QoS ファブリック vPC ピアリングに関連するすべての設定を削除します。
- 変更がない場合は、既存の PTI を尊重します。

グリーンフィールド展開の詳細については、「新しい *VXLAN BGP EVPN* ファブリックの作成」セクションを参照してください。

ブラウンフィールド展開については、次のガイドラインに注意してください。

ブラウンフィールドのシナリオ 1：

- QoS が有効で、ポリシー名が指定されている場合：

（注） QoS は、グローバル QoS およびネイバー リンク サービス ポリシーのポリシー名が、すべてのファブリック vPC ピアリング接続スパインで同じ場合にのみ有効にする必要があります。

  - ポリシー名に基づいてスイッチから QoS 構成をキャプチャし、ポリシー名に基づいて説明されていない構成からそれをフィルタリングし、構成を PTI 説明付きの **switch_freeform** に入れます。
  - ファブリック インターフェイスのサービス ポリシー構成も作成します。
  - グリーンフィールド構成は、ブラウンフィールド構成を尊重する必要があります。

- QoS ポリシー名が編集されている場合は、既存のポリシーとブラウンフィールドの追加構成も削除し、推奨される構成でグリーンフィールド フローに従います。
- QoS が無効になっている場合は、QoS ファブリック vPC ピアリングに関連するすべての設定を削除します。

（注） 生じ得る、またはエラーのために不一致が生じたユーザー構成のクロスチェックは行われず、ユーザーには差分が表示される場合があります。

ブラウンフィールドのシナリオ 2：

- QoSが有効になっていて、ポリシー名が指定されていない場合、QoS設定は、アカウントの対象となっていない、スイッチの自由形式設定の一部です。
- ブラウンフィールドの **[保存して展開（Save & Deploy）]** 後にファブリック設定から QoS が有効になっている場合、QoS構成が重複し、ファブリック vPC ピアリング構成がすでに存在する場合は相違が表示されます。

ブラウンフィールド展開の詳細については、「新しい *VXLAN BGP EVPN* ファブリックの作成」セクションを参照してください。

フィールドと説明+

スイッチの vPC ペアリング ウィンドウを表示するには、ファブリック トポロジ ウィンドウでスイッチを右クリックし、**[vPC ペアリング（vPC Pairing）]** を選択します。スイッチの vPC ペアリング ウィンドウには、次のフィールドがあります。

フィールド	説明
仮想ピアリンクを使用	スイッチ間の仮想ピア リンクを有効または無効にすることができます。
スイッチ名	ファブリック内のすべてのピア スイッチを指定します。 （注） ピア スイッチをペアリングしていない場合は、ファブリック内のすべてのスイッチを表示できます。ピア スイッチをペアリングすると、vPC ペアリング ウィンドウにはピア スイッチだけが表示されます。
推奨	ピア スイッチを選択したスイッチとペアリングできるかどうかを指定します。有効な値は **true** と **false** です。推奨されるピア スイッチは **true** に設定されます。
理由	選択したスイッチとピア スイッチ間の vPC ペアリングが可能または不可能な理由を指定します。
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。

[vPC ペアリング（vPC Pairing）] オプションを使用して、次のことを実行できます。

仮想ピア リンクの作成

Cisco DCNM Web UI で仮想ピア リンクを作成するには、次の手順を実行します。

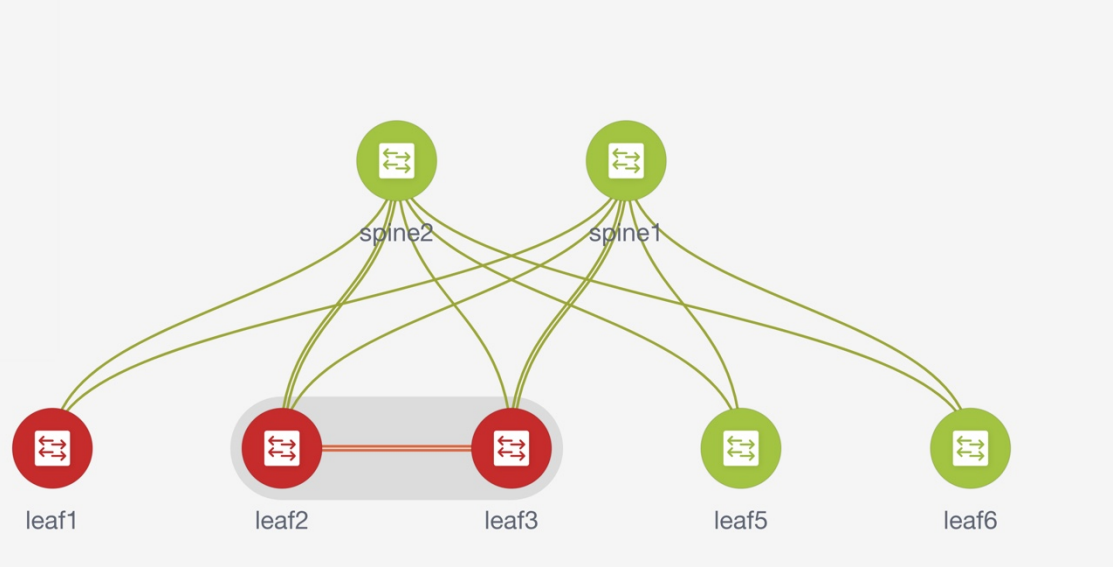
Procedure

ステップ 1　**[制御（Control）] > [ファブリック（Fabrics）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

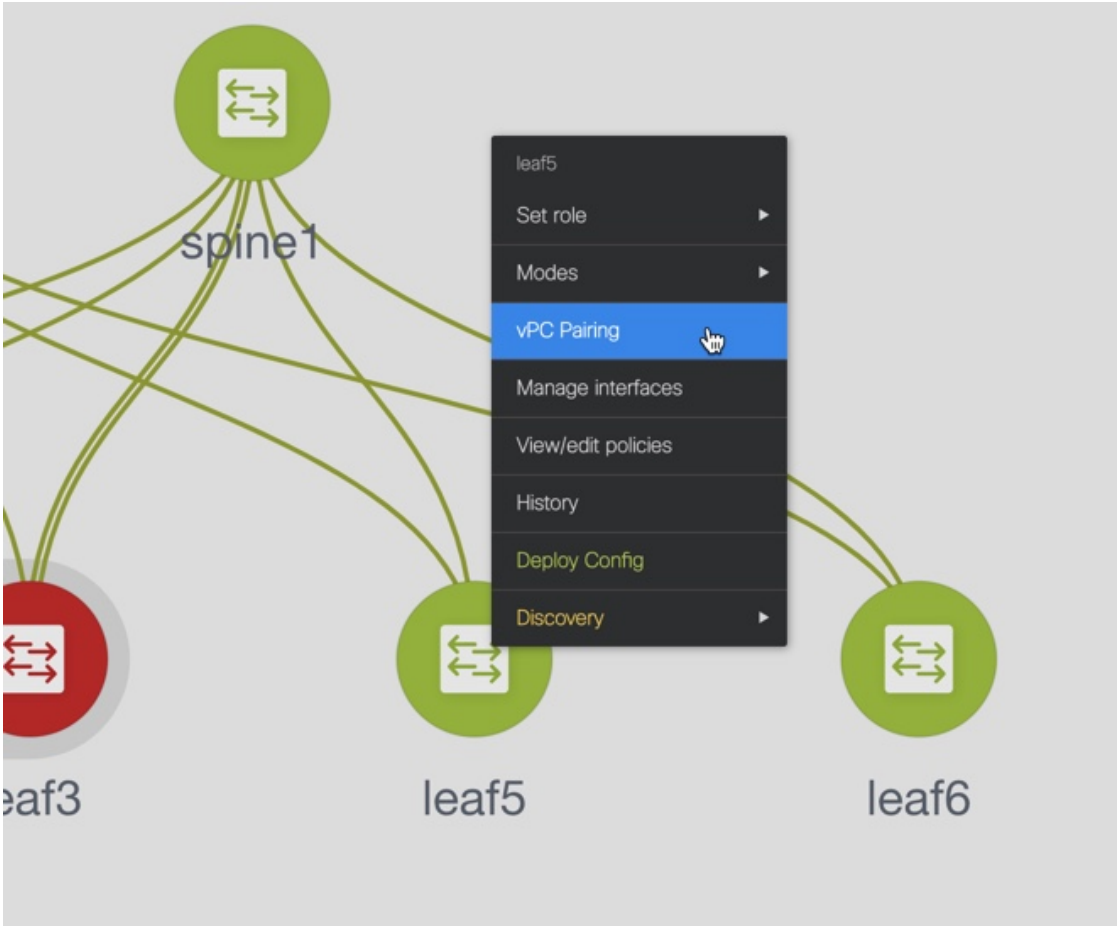
ステップ 2　**Easy_Fabric_11_1** または **Easy_Fabric_eBGP** ファブリック テンプレートを使用してファブリックを選択します。

ファブリック トポロジ ウィンドウが表示されます。



ステップ 3　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。

ピア選択のためのウィンドウが表示されます。



Note 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。

ボーダー ゲートウェイ リーフ ロールを持つスイッチを選択すると、次のエラーが表示されます。

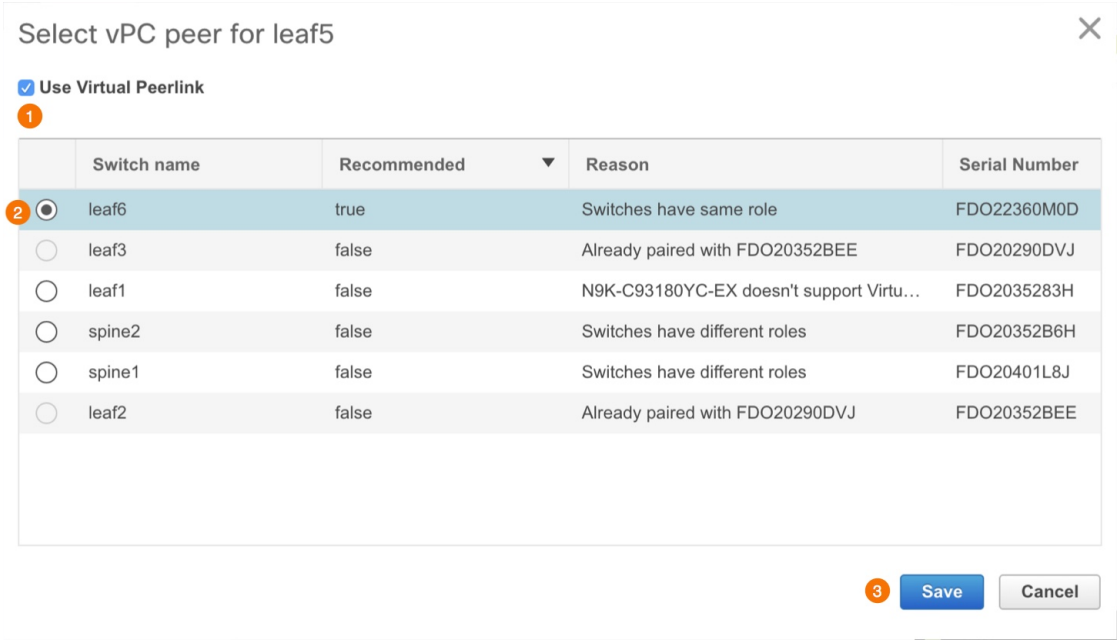
`<switch-name> にはネットワーク/VRF がアタッチされています（<switch-name> has a Network/VRF attached）。vPC ペアリング/ペアリング解除の前にネットワーク/VRF をデタッチしてください（Please detach the Network/VRF before vPC Pairing/Unpairing）。`

ステップ 4 **[仮想ピアリンクを使用（Use Virtual Peerlink）]** チェック ボックスをオンにします。

ステップ 5 ピア スイッチを選択し、**[推奨（Recommended）]** 列をチェックして、ペアリングが可能かどうかを確認します。

値が **true** の場合、ペアリングが可能です。推奨が **false** の場合でも、スイッチをペアリングすることは可能です。ただし、**[保存と展開（Save & Deploy）]** 中に警告またはエラーが発生します。

ステップ 6 [保存（Save）] をクリックします。



ステップ 7 **[ファブリック トポロジ（Fabric Topology）]** ウィンドウで、**[保存と展開（Save & Deploy）]** をクリックします。

[構成展開（Config Deployment）] ウィンドウが表示されます。

ステップ 8 **[構成のプレビュー（Preview Config）]** 列のスイッチに関連するフィールドをクリックします。

そのスイッチの **[構成のプレビュー（Config Preview）]** ウィンドウが表示されます。

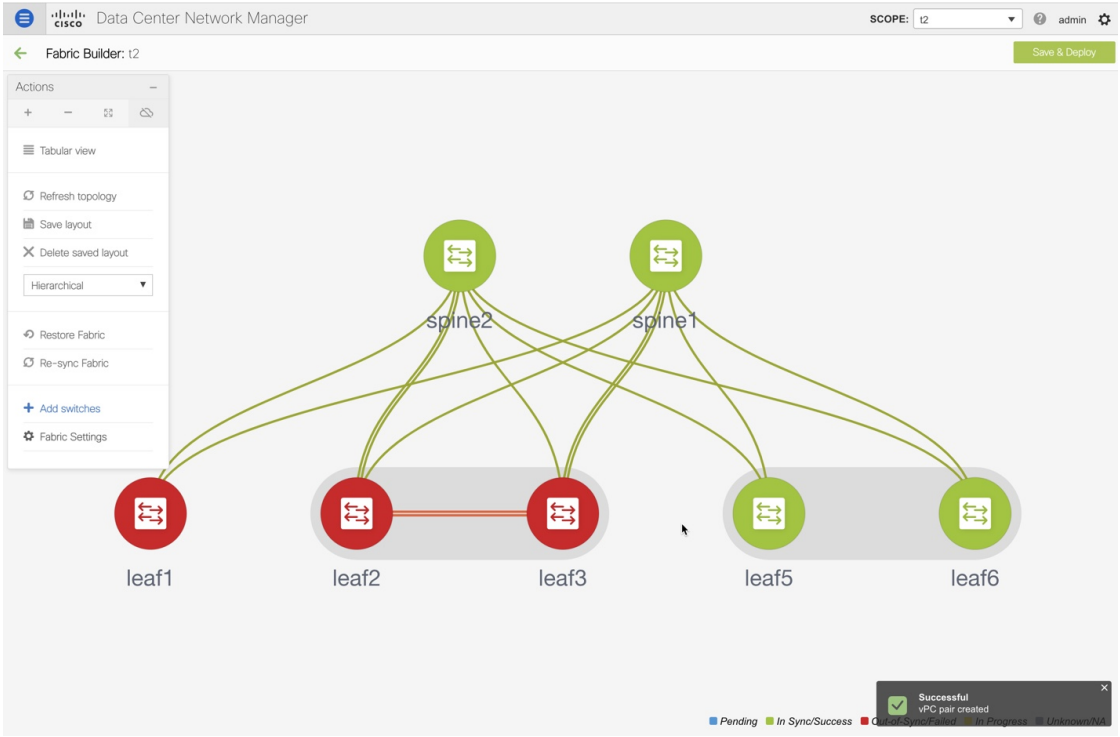
ステップ 9 vPC リンクの詳細が、保留中の構成と、元の構成を横に並べて表示されます。

ステップ 10 ウィンドウを閉じます。

ステップ 11 **[保存と展開（Save & Deploy）]** アイコンの横にある保留中のエラーアイコンをクリックして、エラーと警告を表示します（存在する場合）。

TCAM に関連する警告が表示された場合は、**[解決（Resolve）]** アイコンをクリックします。スイッチのリロード確認用のダイアログボックスが表示されます。[OK] をクリックします。ファブリック トポロジ ウィンドウの **[表形式ビュー（Tabular view）]** からスイッチをリロードすることもできます。

vPC ファブリック ピアリングを介して接続されているスイッチは、灰色の雲で囲まれています。



物理ピア リンクから仮想ピア リンクへの変換

Cisco NDFC Web UI で物理ピア リンクを仮想ピア リンクに変換するには、次の手順を実行します。

Before you begin

- スイッチのメンテナンス ウィンドウ中に、物理ピア リンクから仮想ピア リンクへの変換を計画します。
- スイッチが vPC ファブリック ピアリングをサポートしていることを確認します。以下のスイッチのみが vPC ファブリック ピアリングをサポートします。
  - Cisco Nexus N9K-C9332C スイッチ、Cisco Nexus N9K-C9364C スイッチ、および Cisco Nexus N9K-C9348GC-FXP スイッチ。
  - FX、FX2、および FX2-Z で終わる Cisco Nexus 9000 シリーズ スイッチ。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 **Easy_Fabric_11_1** または **Easy_Fabric_eBGP** ファブリック テンプレートを使用してファブリックを選択します。

ステップ 3 物理ピア リンクを使用して接続されている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。

ピア選択のためのウィンドウが表示されます。

Note 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。

ボーダー ゲートウェイ リーフ ロールを持つスイッチを選択すると、次のエラーが表示されます。

`<switch-name> にはネットワーク/VRF がアタッチされています（<switch-name> has a Network/VRF attached）。vPC ペアリング/ペアリング解除の前にネットワーク/VRF をデタッチしてください（Please detach the Network/VRF before vPC Pairing/Unpairing）。`

ステップ 4 **[推奨（Recommended）]** 列をチェックして、ペアリングが可能かどうかを確認します。

値が **true** の場合、ペアリングが可能です。推奨が **false** の場合でも、スイッチをペアリングすることは可能です。ただし、**[保存と展開（Save & Deploy）]** 中に警告またはエラーが発生します。

ステップ 5 **[仮想ピアリンクを使用（Use Virtual Peerlink）]** チェック ボックスをオンにします。

[ペア解除（Unpair）] アイコンが **[保存（Save）]** に変わります。

ステップ 6 [保存（Save）] をクリックします。

Note **[保存（Save）]** をクリックすると、展開しなくても、スイッチ間の物理 vPC ピア リンクが自動的に削除されます。

ステップ 7 **[ファブリック トポロジ（Fabric Topology）]** ウィンドウで、**[保存と展開（Save & Deploy）]** をクリックします。

[構成展開（Config Deployment）] ウィンドウが表示されます。

ステップ 8 **[構成のプレビュー（Preview Config）]** 列のスイッチに関連するフィールドをクリックします。

そのスイッチの **[構成のプレビュー（Config Preview）]** ウィンドウが表示されます。

ステップ 9 vPC リンクの詳細が、保留中の構成と、元の構成を横に並べて表示されます。

ステップ 10 ウィンドウを閉じます。

ステップ 11 **[保存と展開（Save & Deploy）]** アイコンの横にある保留中のエラーアイコンをクリックして、エラーと警告を表示します（存在する場合）。

TCAM に関連する警告が表示された場合は、**[解決（Resolve）]** アイコンをクリックします。スイッチのリロード確認用のダイアログボックスが表示されます。[OK] をクリックします。ファブリック トポロジ ウィンドウの **[表形式ビュー（Tabular view）]** からスイッチをリロードすることもできます。

ピア スイッチ間の物理ピア リンクが赤に変わります。このリンクを削除します。スイッチは仮想ピア リンクを介してのみ接続されるようになり、灰色の雲に囲まれて表示されます。

仮想ピア リンクから物理ピア リンクへの変換

Cisco DCNM Web UI で仮想ピア リンクを物理ピア リンクに変換するには、次の手順を実行します。

Before you begin

vPC ファブリック ピアリングを無効にする前に、物理ピア リンクを使用してスイッチを接続します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 **[Easy_Fabric_11_1]** または **[Easy_Fabric_eBGP]** ファブリック テンプレートを使用してファブリックを選択します。

ステップ 3 仮想ピア リンクを介して接続されている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。

ピア選択のためのウィンドウが表示されます。

Note 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。

ステップ 4 **[仮想ピアリンクを使用（Use Virtual Peerlink）]** チェック ボックスをオフにします。

[ペア解除（Unpair）] アイコンが **[保存（Save）]** に変わります。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 **[ファブリック トポロジ（Fabric Topology）]** ウィンドウで、**[保存と展開（Save & Deploy）]** をクリックします。

[構成展開（Config Deployment）] ウィンドウが表示されます。

ステップ 7 **[構成のプレビュー（Preview Config）]**列のスイッチに関連するフィールドをクリックします。

そのスイッチの **[構成のプレビュー（Config Preview）]** ウィンドウが表示されます。

ステップ 8 vPC ピア リンクの詳細が、保留中の構成と、元の構成を横に並べて表示されます。

ステップ 9 ウィンドウを閉じます。

ステップ 10 **[保存と展開（Save & Deploy）]** アイコンの横にある保留中のエラーアイコンをクリックして、エラーと警告を表示します （存在する場合）。

TCAM に関連する警告が表示された場合は、**[解決（Resolve）]** アイコンをクリックします。スイッチのリロード確認用のダイアログボックスが表示されます。[OK] をクリックします。ファブリック トポロジ ウィンドウの **[表形式ビュー（Tabular view）]** からスイッチをリロードすることもできます。

灰色の雲で表される仮想ピア リンクが表示されなくなり、代わりにピア スイッチが物理ピア リンクを介して接続されます。

vPC で PIP をアドバタイズする

ファブリック設定では、**vPC advertise-pip** チェックボックスをオンにして、ファブリック内のすべての vPC で PIP アドバタイズ機能を有効にすることができます。Cisco DCNM リリース 11.4（1）以降、**vpc_advertise_pip_jython** ポリシーを使用して、ファブリック内の特定の vPC で PIP のアドバタイズ機能を有効にできます。

次のガイドラインに注意してください。

- Advertising-pip がグローバルに有効になっていない場合、または vPC ピアがファブリック ピアリングを使用していない場合にのみ、特定のピアで vpc_advertise_pip_jython ポリシーを作成できます。
- **vpc advertise-pip** を有効にしても、現在の動作には影響しません。
- ファブリックのアドバタイズ ピップを無効化しても、このポリシーには影響しません。
- スイッチのペアリングを解除すると、このポリシーが削除されます。
- このポリシーは、作成されたピア スイッチから手動で削除できます。

手順

ステップ 1 **[ファブリック ビルダー（Fabric Builder）]** ウィンドウでファブリックをクリックし、vPC のあるスイッチを右クリックして **[表示 / ポリシーを編集（View/Edit Policies）]** を選択します。

ステップ 2 **[追加（Add）]** をクリックして **vpc_advertise_pip_jython** ポリシー テンプレートを選択し、必須パラメータ データを入力します。

（注） このポリシーを 1 つの vPC ピアに追加すると、両方のピアで vpc アドバタイズのそれぞれのコマンドが作成されます。

ステップ 3 **[保存（Save）]** をクリックして、このポリシーを展開します。

ThousandEyes Enterprise Agent

モニタ対象のネットワーク内でユーザが特定のウェブサイトにアクセスするとき、ThousandEyes Enterprise Agent はネットワークとアプリケーション レイヤのパフォーマンス データを収集します。テストの実行、ネットワーク パスと接続の詳細なアスペクトのチェック、ネットワーク ルーティングのステータス チェック、インテント、実行構成などの変更のモニタを行うために、データは使用されます。

リリース 11.5(3) から、ThousandEyes Enterprise Agent は Cisco DCNM と統合されています。

ThousandEyes Enterprise Agent は、NX-OS バージョン 9.3(7) および 10.2(1) 以降のリリースを備えた Cisco Nexus 3000-R シリーズおよび Cisco Nexus 9000 クラウド スケール シリーズでサポートされています。

これは、次のファブリック テンプレートでサポートされています。

- Easy_Fabric_11_1
- Easy_Fabric_eBGP
- External_Fabric_11_1
- LAN_Classic

Cisco DCNM **[Web UI]** > **[制御（Control）]** > **[ThousandEyes]** > **[構成（Configure）]** を使用して、ThousandEyes Enterprise Agent のグローバル設定を構成できます。

このセクションの内容は次のとおりです。

TCAM および CoPP ポリシーの構成

スイッチに ThousandEyes Enterprise Agent 機能をインストールする前に、関連するポリシーを Cisco Nexus 3000-R シリーズおよび Cisco Nexus 9000 クラウド 拡張 シリーズ スイッチに追加してください。

Cisco DCNM Web UI からスイッチで TCAM および CoPP ポリシーを構成するには、次の手順を実行します。

Procedure

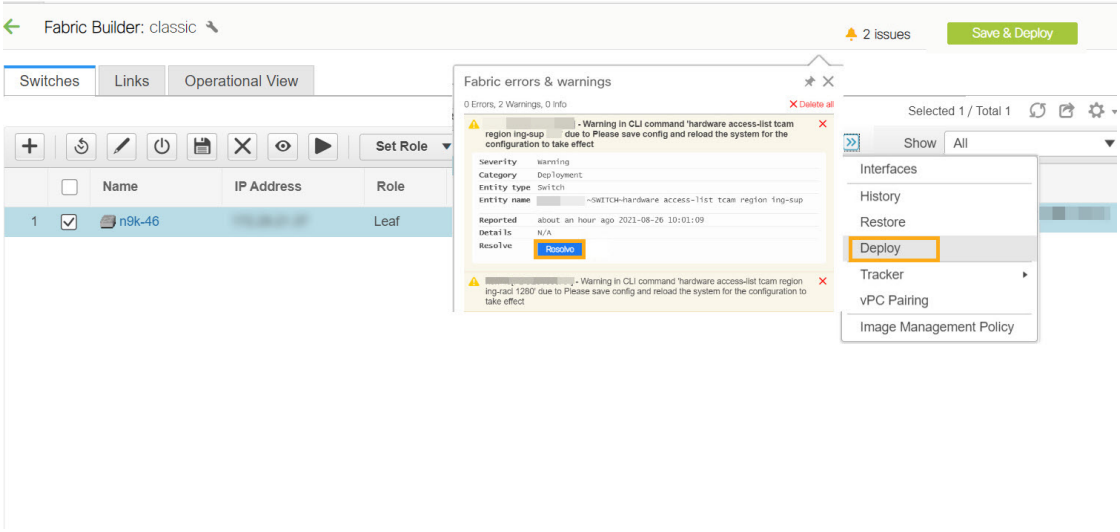
ステップ 1 DCNM Web UI から、**[制御（Control）]** > **[ファブリック ビルダー（Fabric Builder）]** を選択し、ファブリックを選択して、**[アクション（Actions）]** ウィンドウで **[Tabular View]** をクリックします。

[スイッチ（Switches）] タブが表示されます。

ステップ 2 **[スイッチ（Switches）]** タブで 1 つまたは複数のスイッチを選択し、**[ポリシー（Policies）]** ボタンをクリックします。

ステップ 3 **[追加（Add）]** アイコンをクリックします。

ステップ 4 Cisco Nexus 9000 EX、FX、および FX2 シリーズ スイッチの TCAM ポリシーを追加するには、次の手順を実行します。



- EX シリーズ スイッチには ThousandEyes_Agent_N9K_EX_tcam_config を、FX および FX2 シリーズ スイッチには ThousandEyes_Agent_N9K_FX_FEX2_tcam_config を選択します。
- **[優先度（Priority）]** フィールドに値 200 を入力し、**[保存（Save）]** をクリックします。
- **[スイッチ（Switches）]** タブで、ポリシーを追加するスイッチを選択します。**[展開する（Deploy）]** をクリックして、設定をスイッチに展開します。

Note スイッチに TCAM の変更を反映させるためにスイッチをリロードする必要があることを示す警告メッセージが表示されます。**[解決（Resolve）]**をクリックしてスイッチをリロードします。

ステップ 5 Easy_Fabric_11_1 および Easy_Fabric_eBGP テンプレートに CoPP ポリシーを追加するには、次の手順を実行します。

- DCNM Web UI から、**[Control（制御）] > [Fabric Builder（ファブリック ビルダー）] > [Fabric Settings（ファブリック設定）]** を選択し、**[Advanced（詳細設定）]** タブをクリックします。
- **[CoPP プロファイル（CoPP Profile）]** フィールドで手動を選択します。

ステップ 6 サポートされているすべてのスイッチとファブリック テンプレートにポリシーを展開するには、次の手順を実行します。

- 適切なスイッチを選択し、**[再生（Play）]** ボタンをクリックします。

  [デバイスでのスイッチ CLI の実行（Execute Switch CLIs on Devices）] ウィンドウが表示されます。

- [テンプレート（Template）] ドロップダウン リストから **ThousandEyes_Agent_Copy_CoPP** を選択し、[展開（Deploy）] をクリックします。
- **[スイッチ（Switches）]** タブで、適切なスイッチを選択します。**[ポリシー（New Policy）]** をクリックします。

[ポリシー（Policy）] ウィンドウが表示されます。

- **[追加（Add）]** アイコンをクリックします。
- [ポリシー（Priority）] ドロップダウン リストから **[ThousandEyes_Agent_CoPP]** を選択します。
- [優先度（Priority）] フィールドに値 210 を入力し、**[保存（Save）]** をクリックします。
- **[スイッチ（Switches）]** タブで、ポリシーを追加するスイッチを選択します。**[保存（Save）]** をクリックして、構成をスイッチに展開します。

ThousandEyes Enterprise エージェント アクションの実行

管理モードのファブリックに対してのみ、ThousandEyes Enterprise Agent アクションを実行できます。

Note ThousandEyes Enterprise Agent をスイッチにインストールする前に、TCAM および COPP ポリシーがスイッチに設定されていることを確認してください。

DCNM Web UI を使用して ThousandEyes Enterprise Agent を起動、停止、インストール、またはアンインストールするには、次の手順を実行します。

Procedure

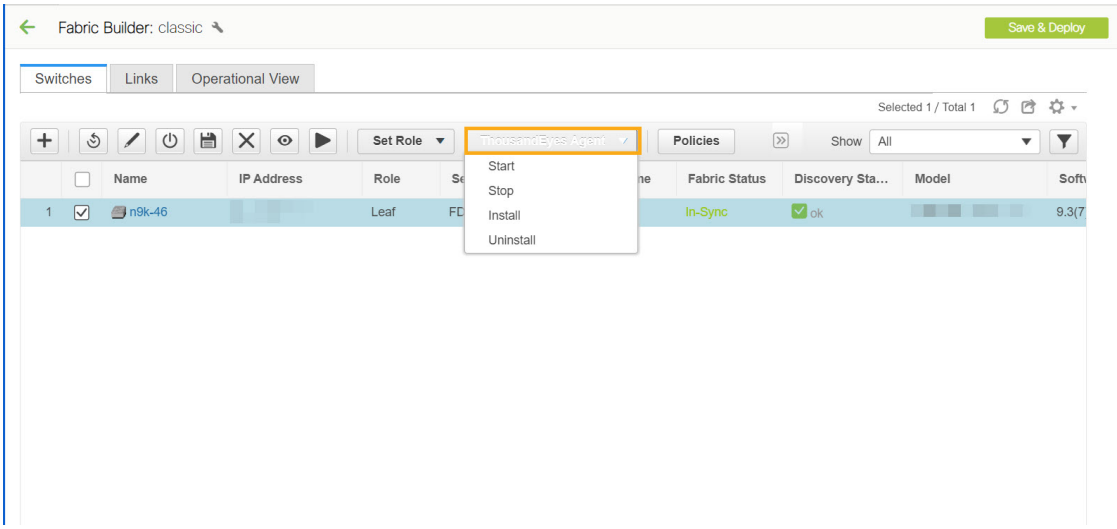
ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。長方形のボックスは、各ファブリックを表します。

ステップ 2 ファブリックを選択し、**[アクション（Actions）]** ウィンドウの **[表形式のビュー（Tabular View）]** をクリックします。

[スイッチ（Switches）] タブが表示されます。

ステップ 3 単一または複数のスイッチを選択し、**[ThousandEyes エージェント（ThousandEyes Agent）]** ドロップダウン リストから必要なアクションをクリックします。



次の操作を実行できます。

- **[インストール（Install）]** – ThousandEyes Enterprise Agent をインストールしますインストール後、[ThousandEyes Agent Status] 列に RUNNING と表示されます。
- **[開始（Start）]** – 以前に停止した、スイッチ上の ThousandEyes Enterprise Agent を開始します。

  Note スイッチでエージェントを開始する前に、ThousandEyes Enterprise Agent をインストールする必要があります。

- **[停止（Stop）]** – スイッチの ThousandEyes Enterprise Agent を停止します。
- **[アンインストール（Uninstall）]** – スイッチから ThousandEyes Enterprise Agent をアンインストールします。アクションを実行するとポップアップ ウィンドウが表示され、メッセージが表示されます - **ThousandEyes アクションが完了しました。ステータスを確認してください！**

  DCNM から ThousandEyes Enterprise Agent をアンインストールしても、ThousandEyes ポータルのアカウント グループ トークン番号はクリアされません。スイッチ上の既存の ThousandEyes Enterprise Agent アカウント グループ トークンを削除するには、ThousandEyes Enterprise Agent の削除セクションを参照してください。

ThousandEyes Enterprise Agent ステータス

ThousandEyes Enterprise Agent のステータス メッセージは次のとおりです。

- **[NOT_INSTALLED]**：ThousandEyes Enterprise Agent はスイッチにインストールされません。
- **[RUNNING]**：ThousandEyes Enterprise Agent はスイッチでアクティブです。
- **[STOPPED]**：ThousandEyes Enterprise Agent をスイッチで停止します。

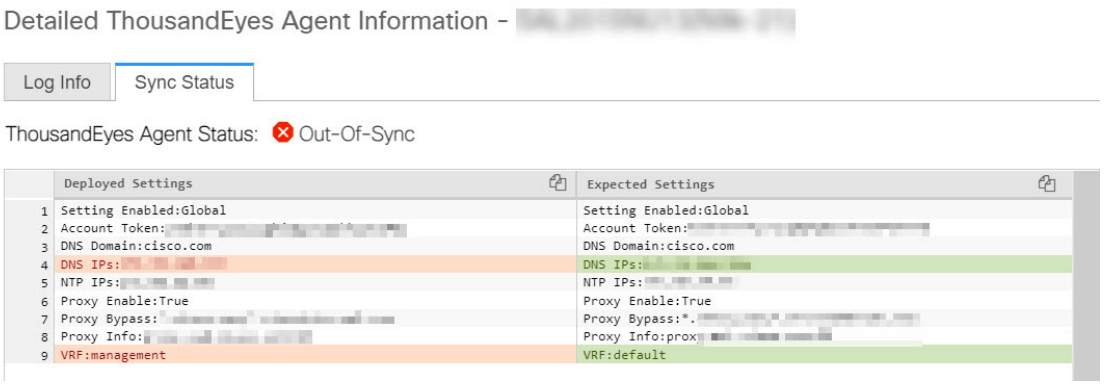
- **[UNSUPPORTED_VERSION]**：ThousandEyes Enterprise Agent は、スイッチの NX-OS バージョンではサポートされていません。
- **[UNSUPPORTED_PLATFORM]**：ThousandEyes Enterprise Agent は、選択したスイッチ プラットフォームでサポートされていません。
- **NA**：ThousandEyes Enterprise Agent グローバル設定は DCNM で構成されていません

1. **[ThousandEyes ステータス（ThousandEyes Status）]** をクリックして、ThousandEyes Enterprise Agent の情報を表示します。

   [ThousandEyes Agent の詳細情報（Detailed ThousandEyes Agent Information）] ページが表示されます。

   - **[ログ情報（Log Info）]** タブには、ランタイム エージェントのステータスまたはスイッチのエラー ログが表示されます。
   - **[同期ステータス（Sync Status）]** タブには、スイッチの展開された設定と予想される設定の詳細が表示されます。

ThousandEyes Enterprise Agent の構成がその時点での DCNM の有効な構成と異なる場合、DCNM は構成の不一致（**[In-Sync]**、**[Out-Of-Sync]**）を示します。構成が一致しない場合は、ThousandEyes Enterprise Agent をアンインストール、削除、およびインストールして、構成を同期させる必要があります。



ThousandEyes Enterprise Agent の削除

ThousandEyes Enterprise ポータルで既存の ThousandEyes Enterprise Agent エントリを削除するには、[古いエージェント エントリの削除（Removing Old Agent Entries）]セクションの手順を参照してください。

DCNM のスイッチから既存の ThousandEyes Enterprise Agent アカウント グループ トークンを削除するには、次の手順を実行します。

Procedure

ステップ 1 Cisco DCNM Web UI から、**[制御（Control）] > [Fabric Builder]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。長方形のボックスは、各ファブリックを表します。

ステップ 2 ファブリックを選択し、**[アクション（Actions）]** ウィンドウの **[表形式のビュー（Tabular View）]** をクリックします。

[スイッチ（Switches）] タブが表示されます。

ステップ 3 適切なスイッチを選択して ThousandEyes Enterprise Agent を削除し、**[再生（Play）]** ボタン（コマンドの実行）をクリックします。

[デバイスでのスイッチ CLI の実行（Execute Switch CLIs on Devices）] ウィンドウが表示されます。

ステップ 4 [テンプレート（Template）] ドロップダウン リストから **[ThousandEyes_Agent_Identity_Delete]** を選択し、**[展開（Deploy）]** をクリックします。

ポリシーの表示と編集

Cisco DCNM は、一連のスイッチをグループ化する機能を提供し、グループに一連のアンダーレイ構成をプッシュできます。このリリースでは、ポリシーテンプレートを作成し、選択した複数のスイッチに適用できます。

ポリシーを表示、追加、展開、または編集するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

ステップ 2 使用可能なファブリックを選択し、**[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 [スイッチ（switches）] タブで複数のスイッチを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** をクリックします。

Note **[ポリシーの表示/編集（View/Edit Policies）]**は、MSD ファブリックに対して有効になっていません。

ポリシーの表示

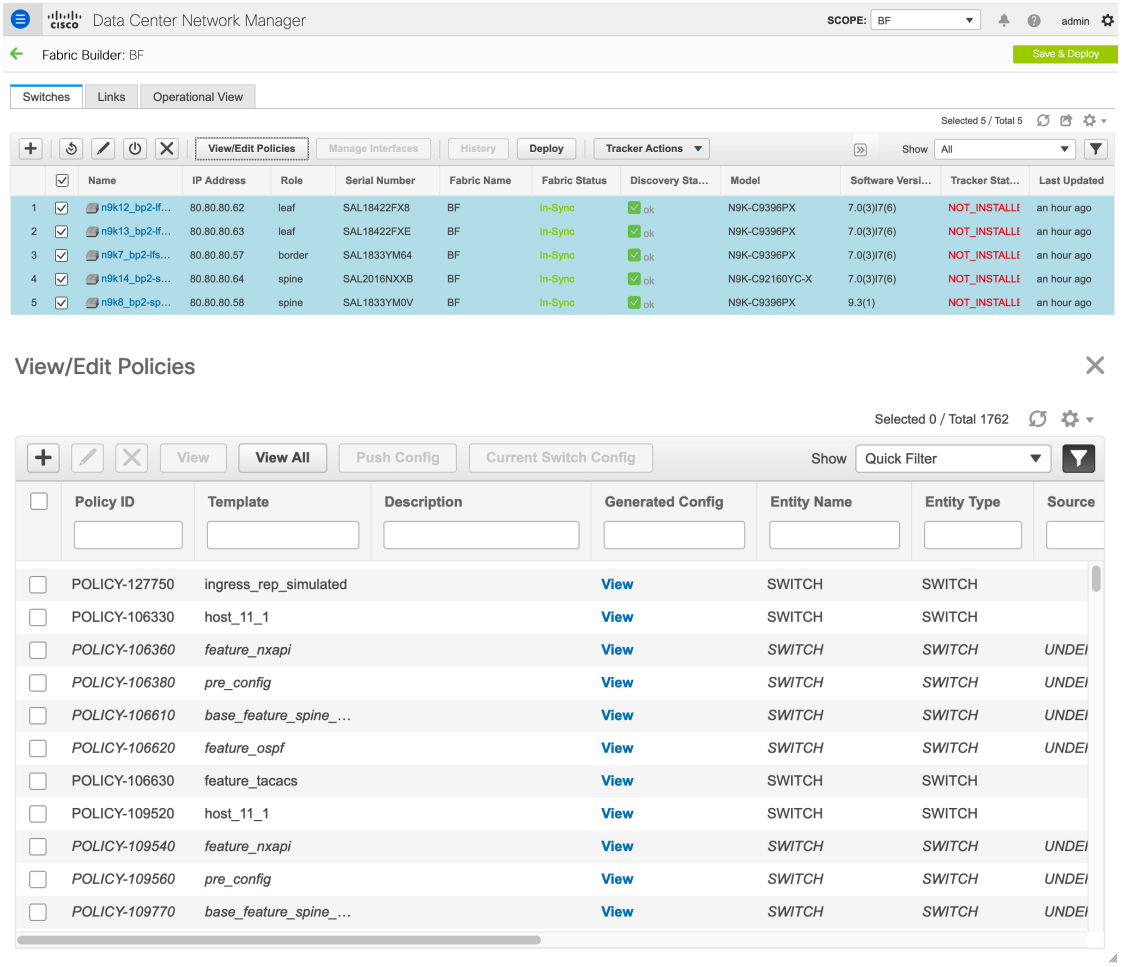
Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

ステップ 2 使用可能なファブリックを選択し、**[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 [スイッチ（switches）] タブで複数のスイッチを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** をクリックします。

ポリシーは、複数のスイッチのポリシー テーブルの表示または編集にリストされます。

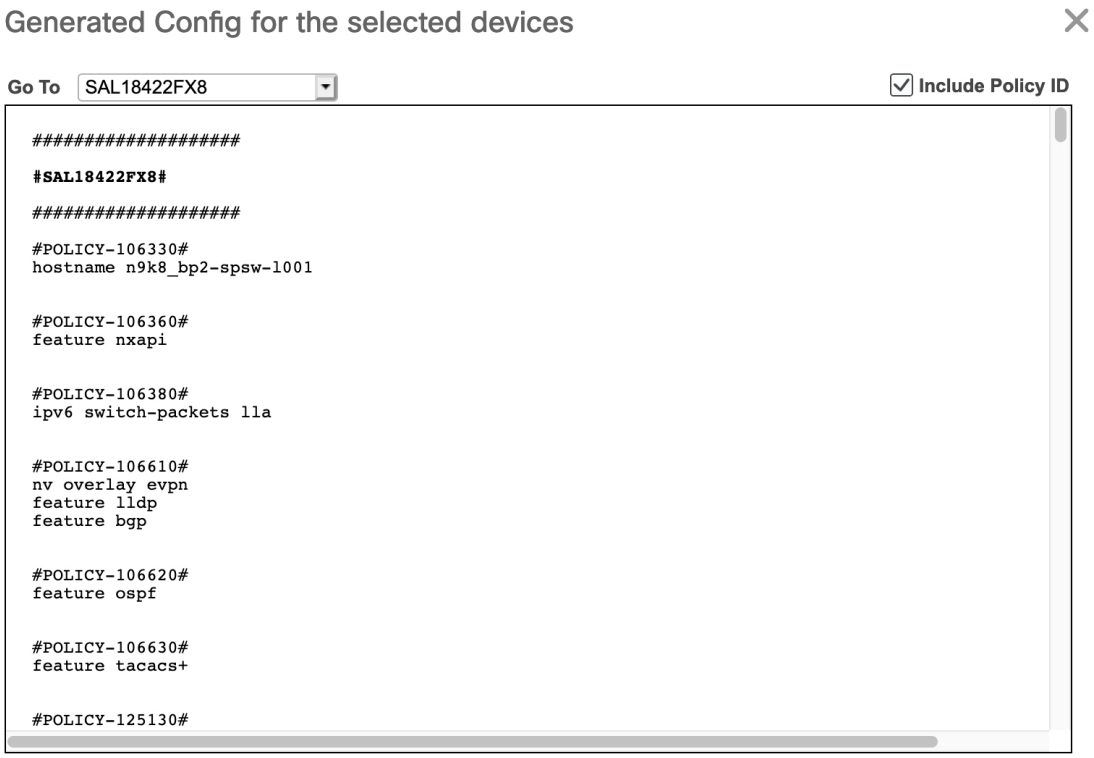


Note **[生成された構成（Generated Config）]** 列の下にある **[表示（View）]** ボタンにカーソルを合わせると、デバイスに対して生成された構成を表示できます。さらに、この列の下の検索フィールドに構成を入力して、ポリシーをフィルタリングできます。

ステップ 4 ポリシーを選択し、**[表示（View）]** ボタンをクリックしてその構成を表示します。

Note Python ポリシーは、ロジックを配置し、CLI ポリシーを制御するために使用されます。DCNM リリース 11.3(1) 以降、複数の CLI 子ポリシーが Python ポリシーごとに集約されます。

ステップ 5 **[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウで、**[すべてを表示（View All）]** をクリックして、ポリシーを使用してスイッチにプッシュされたすべての構成を表示します。



[移動先：（Go To:）] このドロップダウンリストからデバイスを選択して、その開始構成に移動します。

このオプションは、複数のデバイスのポリシーを表示する場合にのみ適用されます。

ポリシー ID を含める：（Include Policy ID:） すべてのポリシーのポリシー ID を表示するには、このチェックボックスをオンにします。デフォルトでは、このチェックボックスはオンです。

ポリシーの追加

Procedure

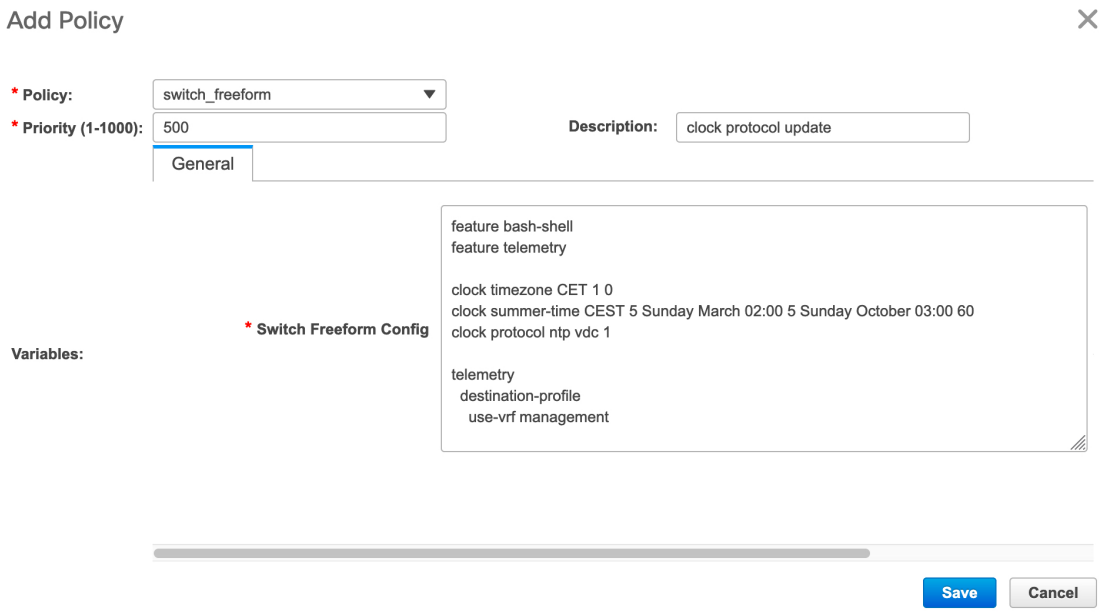
ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

ステップ 2 使用可能なファブリックを選択し、[表形式ビュー（Tabular view）] をクリックします。

ステップ 3 **[スイッチ（Switches）]** タブで 1 つまたは複数のスイッチを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** ボタンをクリックします。

ステップ 4 [追加（Add）] アイコンをクリックします。

ステップ 5 ポリシーテンプレートを選択し、必須パラメータ データを入力して、**[保存（Save）]** をクリックします。n 個のデバイスの選択に基づいて、各デバイスごとに PTI が追加されます。



[ポリシー（Policy]：このドロップダウンリストからポリシーを選択します。

[優先順位（Priority）]：ポリシーの優先順位を指定します。適用可能な値は 1 ～ 1000 です。デフォルト値は 500 です。**[優先順位（Priority）]** フィールドの数値が小さいほど、生成された構成およびPOAP スタートアップ構成の優先順位が高いことを意味します。たとえば、機能は 50、ルート マップは 100、vpc-domain は 200 です。

[説明（Description）]：（オプション）ポリシーの説明を指定します。このフィールドは、複数の自由形式ポリシーを差別化するために使用されます。**[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウに **[説明（Description）]** 列が追加され、説明に基づいてポリシーをフィルタリングまたは検索するために使用できます。

ポリシーの展開

Procedure

ステップ 1 **[制御（Control）]** > **[ファブリック ビルダ (Fabric Builder)]** を選択します。

ステップ 2 使用可能なファブリックを選択し、[表形式ビュー（Tabular view）] をクリックします。

ステップ 3 [スイッチ（switches）] タブで複数のスイッチを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** ボタンをクリックします。

ステップ 4 複数のポリシーを選択し、> **[構成をプッシュ（Push Config）]** をクリックします。選択した PTI の構成がスイッチのグループにプッシュされます。

- 外部ファブリックがモニタ モードの場合、**[構成をプッシュ（Push Config）]** オプションは無効になっています。
- このオプションは、ファブリックが凍結モードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。

ポリシーの編集

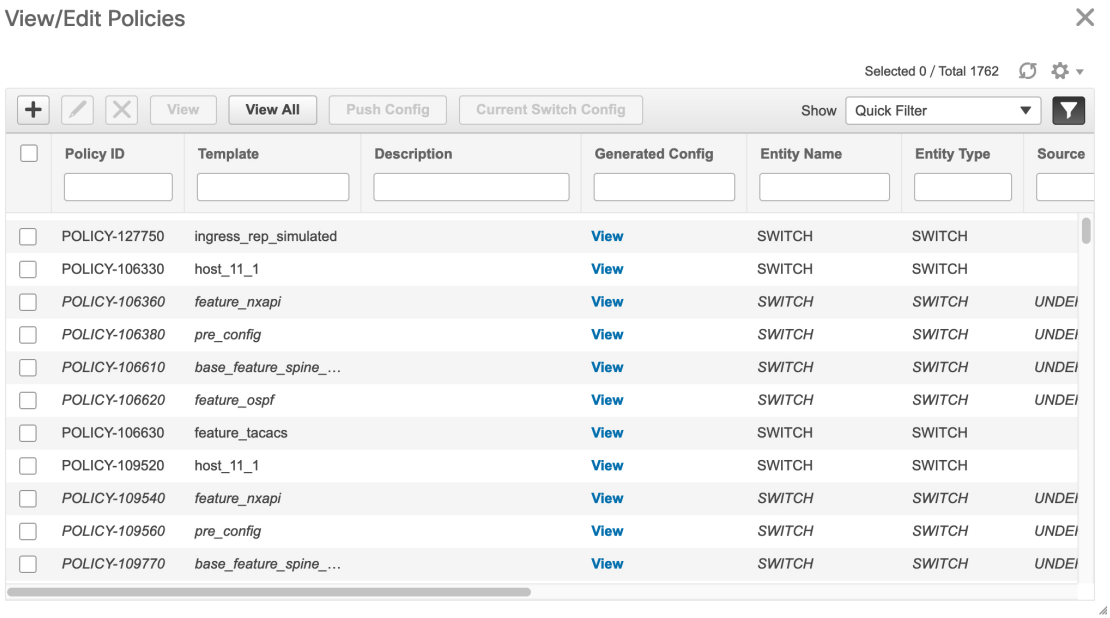
Note 複数のポリシーの編集はサポートされていません。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

ステップ 2 使用可能なファブリックを選択し、**[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 [スイッチ（switches）] タブで複数のスイッチを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** ボタンをクリックします。

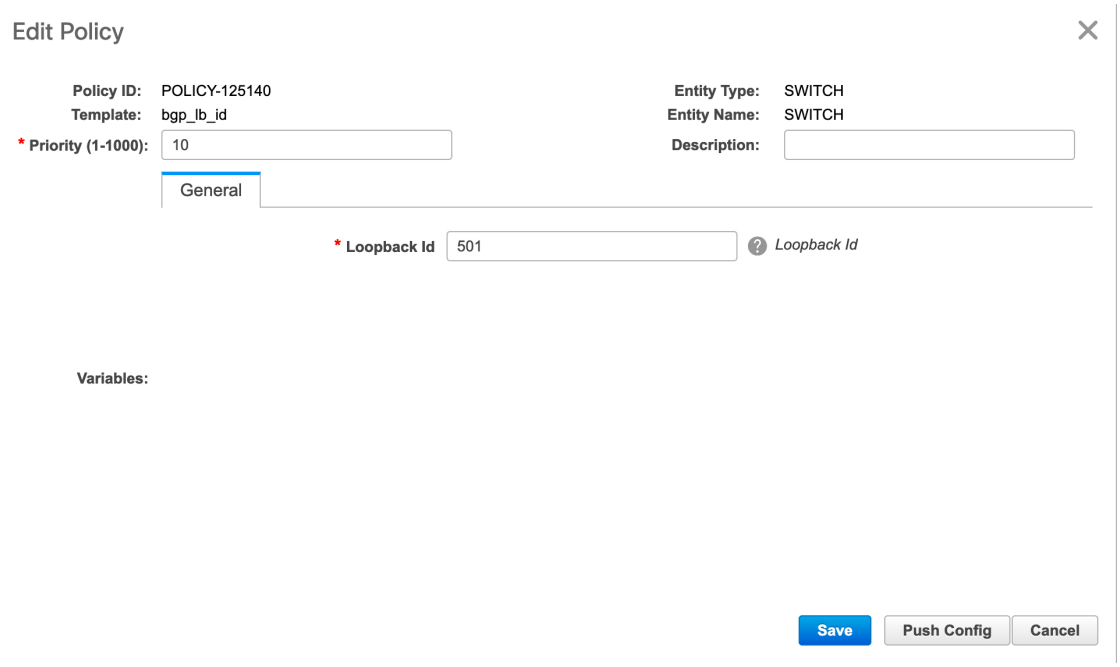


Note イタリック体のフォントのポリシーは編集できません。これらのポリシーの **[編集可能（Editable）]** 列と **[削除済みマーク（Mark Deleted）]** 列の値は **[false]** です。

ステップ 4 PTI を選択し、**[編集（Edit）]** をクリックして必要なデータを変更し、**[保存（Save）]** をクリックして PTI を保存します。

ステップ 5 PTI を選択し、**[編集（Edit）]** をクリックして必要なデータを変更し、>**[構成をプッシュ（Push Config）]** をクリックしてポリシー構成をデバイスにプッシュします。

Note
- このオプションは、ファブリックが凍結モードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。
- Python ポリシーの構成をプッシュすると、Warning（注意）が表示されます。
- mark-deleted ポリシーを編集、削除、または構成をプッシュすると、Warning（注意）が表示されます。mark-deleted ポリシーは、**[削除済みマーク（Mark Deleted）]** 列で **[true]** に設定されています。**[削除済みマーク（Mark Deleted）]** ポリシーのスイッチの自由形式の子ポリシーが **[ポリシーの表示/編集（View/Edit Policies）]** ダイアログボックスに表示されます。**Python** の switch_freeform ポリシーのみを編集できます。**Template_CLI** switch_freeform_config ポリシーは編集できません。



現在のスイッチ構成

Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

ステップ 2 使用可能なファブリックを選択し、**[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 [スイッチ（switches）] タブで複数のスイッチを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** をクリックします。

ステップ 4 **[現在のスイッチ構成（Current Switch Config）]** をクリックします。

[実行構成（Running Config）] ダイアログ ボックスに現在のスイッチ構成が表示されます。

Note ユーザーロールがデフォルトでプロンプトの有効化にアクセスできない場合、**[現在のスイッチ構成（Current Switch Config）]** をクリックしても、Cisco CSR 1000v の実行構成は表示されません。

認証キーの取得

3DES 暗号化 OSPF 認証キーの取得

1. スイッチに SSH 接続します。
2. 未使用のスイッチインターフェイスで、次を有効にします。

```
config terminal
    feature ospf
    interface Ethernet1/1
       no switchport
       ip ospf message-digest-key 127 md5 ospfAuth
```

この例では、**ospfAuth** は暗号化されていないパスワードです。

（注） このステップ 2 は、新しいキーを設定する場合に必要です。

3. **show run interface Ethernet1/1** コマンドを入力してパスワードを取得します。

```
Switch # show run interface Ethernet1/1
   interface Ethernet1/1
     no switchport
     ip ospf message-digest key 127 md5 3 sd8478f4fsw4f4w34sd8478fsdfw
     no shutdown
```

md5 3 の後の文字のシーケンスは、暗号化されたパスワードです。

4. **[OSPF 認証キー（OSPF Authentication Key）]** フィールドの暗号化されたパスワードを更新します。

暗号化された IS-IS 認証キーの取得

キーを取得するには、スイッチにアクセスできる必要があります。

1. スイッチに SSH 接続します。
2. 一時キーチェーンを作成します。

```
config terminal
   key chain isis
   key 127
   key-string isisAuth
```

この例では、**isisAuth** はプレーンテキスト パスワードです。これは、CLI が受け入れられた後に Cisco タイプ 7 パスワードに変換されます。

3. **show run | section "key chain"** コマンドを入力してパスワードを取得します。

```
key chain isis
   key 127
       key-string 7 071b245f5a
```

key-string 7 の後の文字のシーケンスは、暗号化されたパスワードです。設定を保存します。

4. [OSPF 認証キー（OSPF Authentication Key）] フィールドの暗号化されたパスワードを更新します。
5. ステップ 2 で行った不要な設定を削除します。

3DES 暗号化 BGP 認証キーの取得

1. スイッチに SSH 接続し、存在しないネイバーの BGP 設定を有効にします。

（注） 存在しないネイバー設定は、パスワードを取得するための一時的な BGP ネイバー設定です。

```
router bgp
   neighbor 10.2.0.2 remote-as 65000
   password bgpAuth
```

この例では、**bgpAuth** は暗号化されていないパスワードです。

2. パスワードを取得するには、show run bgp コマンドを入力します。サンプル出力：

```
neighbor 10.2.0.2
   remote-as 65000
   password 3 sd8478fswerdfw3434fsw4f4w34sdsd8478fswerdfw3434fsw4f4w3
```

パスワード 3 の後の文字のシーケンスは、暗号化されたパスワードです。

3. **[BGP 認証キー（BGP Authentication Key）]** フィールドの暗号化されたパスワードを更新します。
4. BGP ネイバー設定を削除します。

暗号化された BFD 認証キーの取得

1. スイッチに SSH 接続します。
2. 未使用のスイッチインターフェイスで、次を有効にします。

```
switch# config terminal
switch(config)# int e1/1
switch(config-if)# bfd authentication keyed-SHA1 key-id 100 key cisco123
```

この例では、**cisco123** は暗号化されていないパスワードで、キー ID は **100** です。

（注） このステップ 2 は、新しいキーを設定する場合に必要です。

3. キーを取得するには、**show running-config interface** コマンドを入力します。

```
switch# show running-config interface Ethernet1/1

interface Ethernet1/1
description connected-to- switch-Ethernet1/1
no switchport
mtu 9216
bfd authentication Keyed-SHA1 key-id 100 hex-key 636973636F313233
no ip redirects
ip address 10.4.0.6/30
no ipv6 redirects
ip ospf network point-to-point
ip router ospf 100 area 0.0.0.0
no shutdown
```

BFD キー ID は **100** で、暗号化キーは **636973636F313233** です。

4. **[BFD 認証キー（BFD Authentication Key ID）]** フィールドと **[BFD 認証キー（BFD Authentication Key）]** フィールドのキー ID とキーを更新します。

カスタム メンテナンス モードのプロファイル ポリシー

DCNM を使用してスイッチをメンテナンス モードにすると、メンテナンス モード プロファイルでは、BGP および OSPF 分離 CLI の固定セットのみが構成されます。Cisco DCNM リリース 11.3(1) 以降では、メンテナンス モードおよび通常モード プロファイル用にカスタマイズされた構成で **[custom_maintenance_mode_profile]** PTI を作成し、PTI をスイッチに展開してから、スイッチをメンテナンス モードに移行できます。

カスタム メンテナンス モードのプロファイル ポリシーの作成と展開

Procedure

ステップ 1 **[制御（Control）]** > **[ファブリック ビルダ（Fabric Builder）]** を選択し、**[表形式ビュー（Tabular View）]** をクリックして、**[名前（Name）]** 列でスイッチを選択する、または、**[制御（Control）]** > **[ファブリック ビルダ（Fabric Builder）]** を選択してスイッチを右クリックします。

ステップ 2 **[ポリシーの表示/編集（View/Edit Policies）]** をクリックして、**[+]** をクリックして新しいポリシーを追加します。**[ポリシーの追加（Add Policy）]** ウィンドウが表示されます。

ステップ 3 **[ポリシー（Policy）]** ドロップダウンリストから **[custom_maintenance_mode_profile]** を選択します。

ステップ 4 **[メンテナンス モード プロファイル コンテンツ（Maintenance mode profile contents）]** に、必要な構成 CLI を入力します。

例：

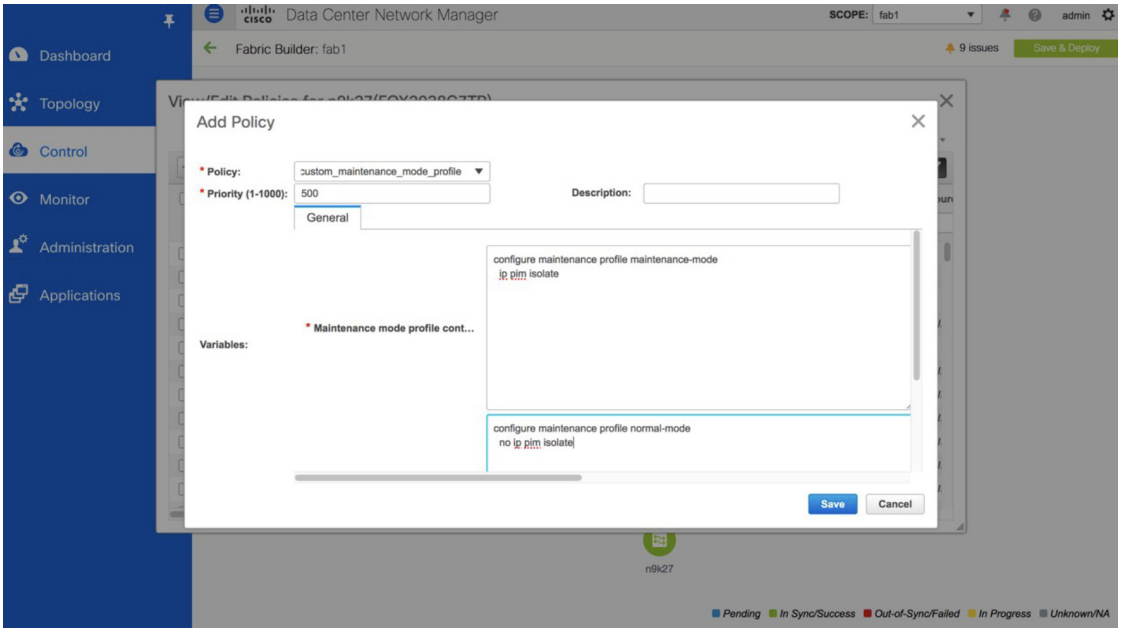
```
configure maintenance profile maintenance-mode
ip pim isolate
```

[通常モード プロファイル コンテンツ（Normal mode profile contents）] に、必要な構成 CLI を入力します。

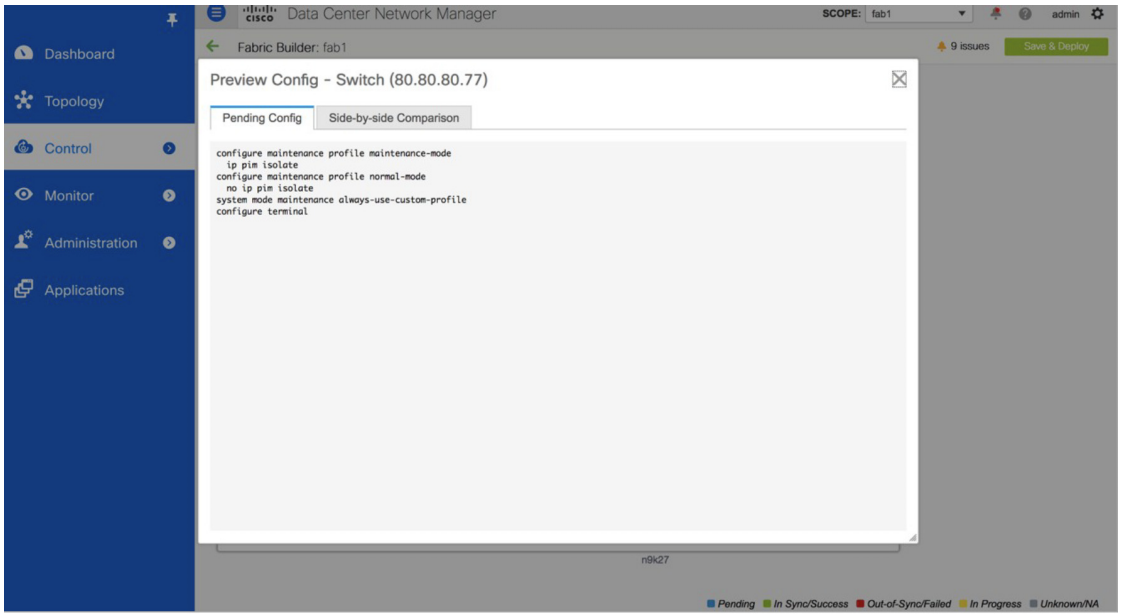
例：

```
configure maintenance profile normal-mode
no ip pim isolate
```

ステップ 5 [保存（Save）] をクリックします。



ステップ 6 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウでスイッチを右クリックし、**[構成の展開（Deploy Config）]** を選択します。**[保留中の構成（Pending Config）]** ウィンドウで構成を確認し、構成をスイッチに展開します。



ステップ 7 次に、スイッチを右クリックし、**[モード（Modes）] > [メンテナンス モード（Maintenance Mode）]** を選択して、スイッチをメンテナンス モードに移動します。

カスタム メンテナンス モード のプロファイル ポリシーの削除

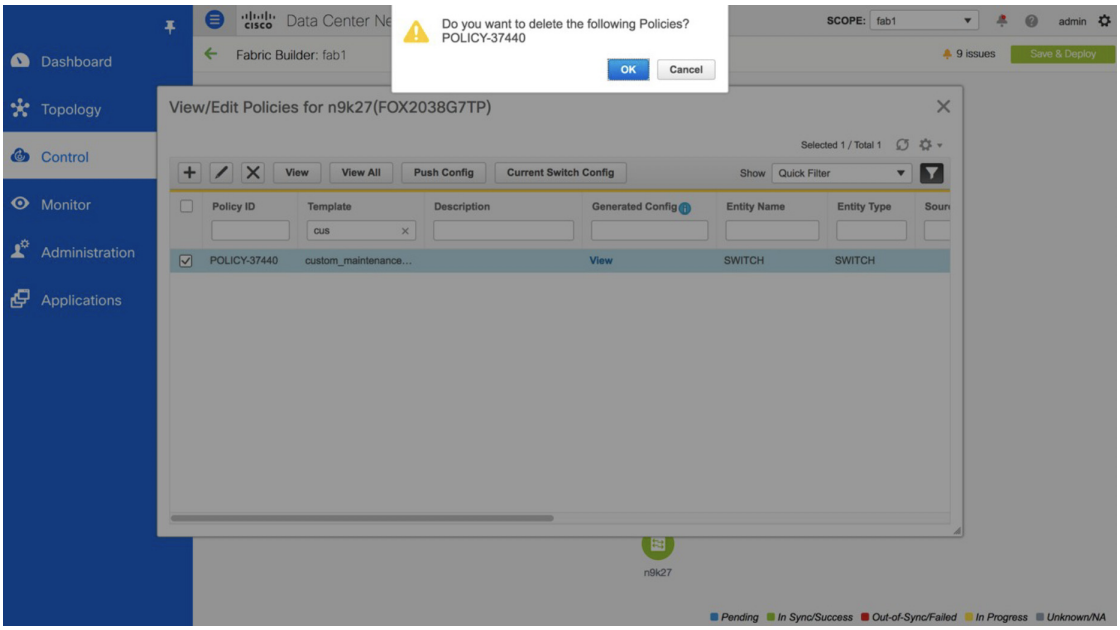
Procedure

ステップ 1 カスタム メンテナンス モード プロファイル ポリシーを削除する前に、スイッチをアクティブ/動作モードまたは通常モードに移行する必要があります。これを行うには、**[ファブリック ビルダ（Fabric Builder）]** ウィンドウでスイッチを右クリックし、**[モード（Modes）] > [アクティブ/（Active/）] > [動作モード（Operational Mode）]** の順に選択します。

ステップ 2 スイッチがアクティブ/動作モードまたは通常モードに移動した後、**[ファブリック ビルダ（Fabric Builder）]** ウィンドウで **[表形式ビュー（Tabular View）]** をクリックし、**[名前（Name）]** 列でスイッチを選択するか、**[ファブリック ビルダ（Fabric Builder）]** ウィンドウでスイッチを右クリックします。

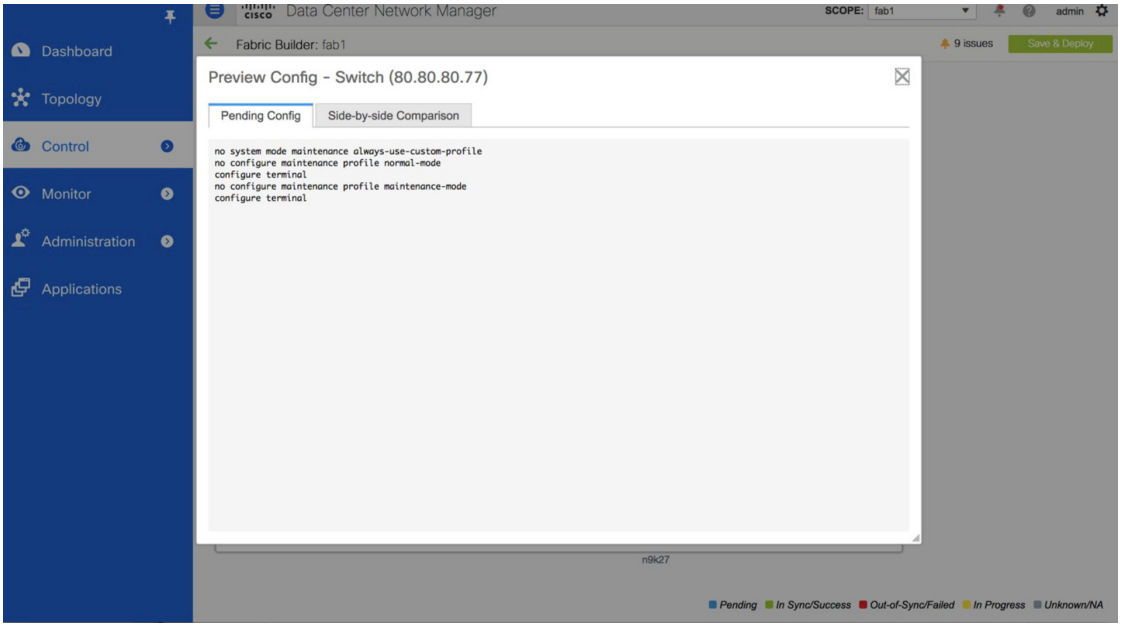
ステップ 3 **[ポリシーの表示/編集（View/Edit Policies）]** をクリックし、削除する必要がある **[custom_maintenance_mode_profile]** ポリシーを選択します。

ステップ 4 **[X]** をクリックしてポリシーを削除します。



ステップ 5 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウでスイッチを右クリックし、**[構成の展開（Deploy Config）]** を選択します。**[保留中の構成（Pending Config）]** ウィンドウで構成を確認し、構成をスイッチに展開します。

```
no system mode maintenance always-use-custom-profile
no configure maintenance profile normal-mode
no configure maintenance profile maintenance-mode
configure terminal
```



返品許可（RMA）

ここでは、Cisco DCNM Easy ファブリック 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、保存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

- 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。たとえば、Cisco Nexus 9300-EX スイッチを Cisco Nexus 9300-FX スイッチに交換する場合は、ファブリックから 9300-EX スイッチを取り外し、同じファブリック内の 9300-FX 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、DCNM は、DCNM 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。

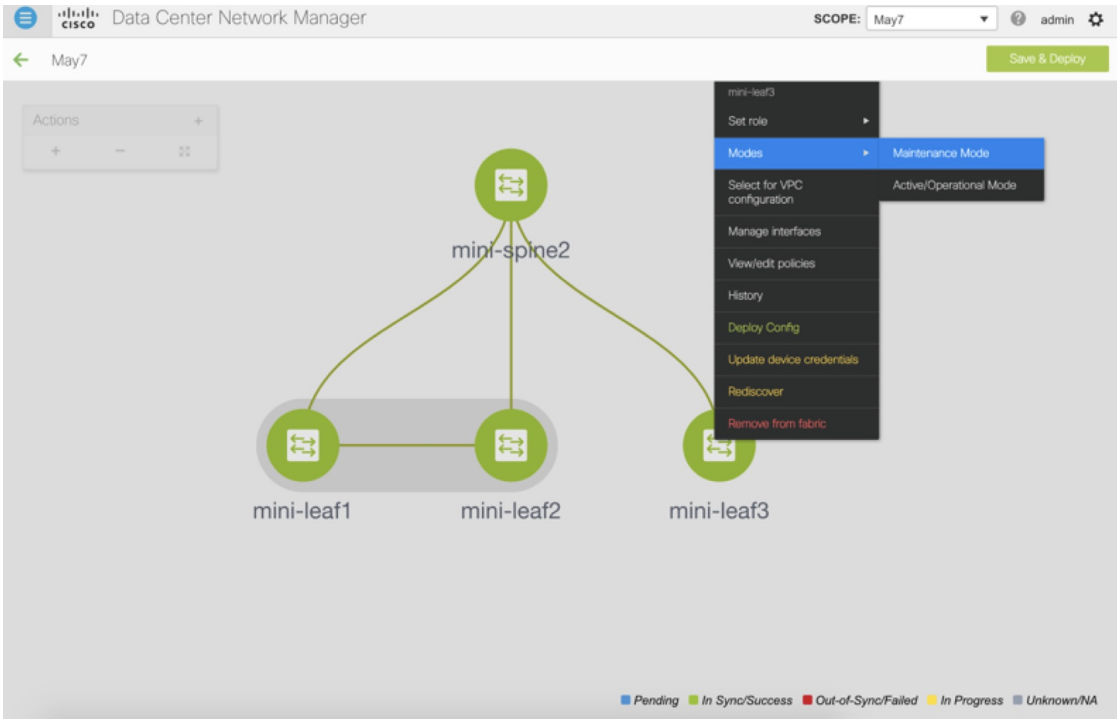
POAP RMA フロー

Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

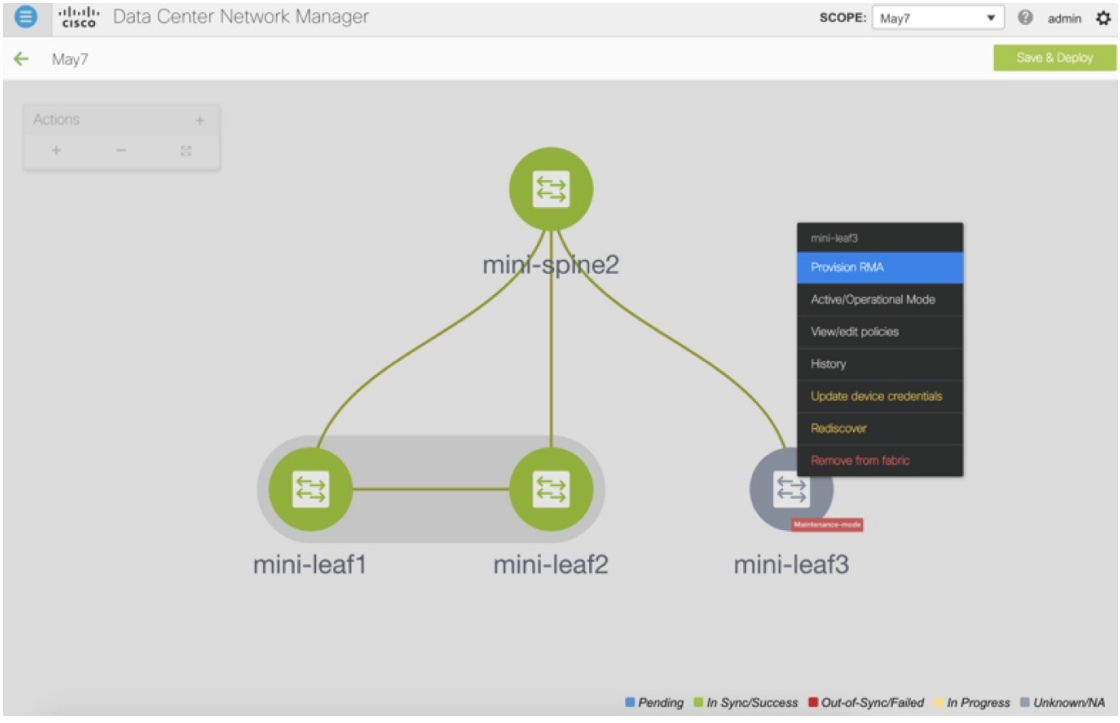
ステップ 2 RMA を実行するファブリックをクリックします。

ステップ 3 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 モードに移行するには、デバイスで右クリックし、**[モード（Modes）] > [メンテナンス モード（Maintenance Mode）]** を選択します。

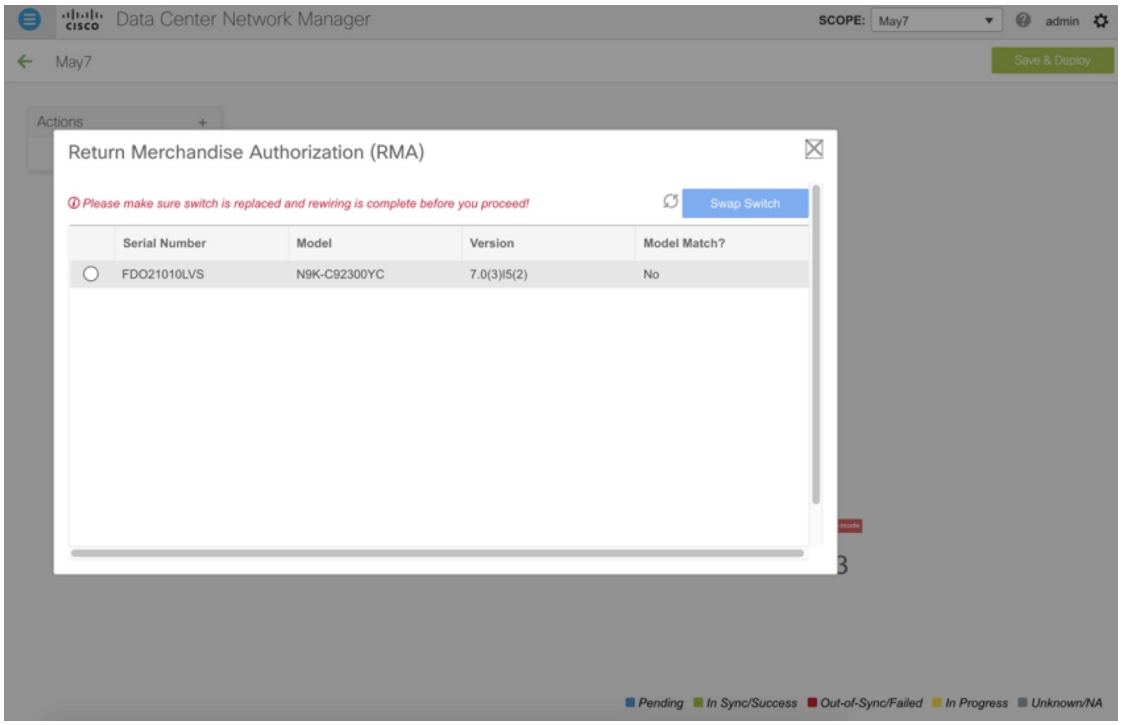


ステップ 4 ネットワークのデバイスを物理的に交換します。物理接続は、交換用スイッチの元のスイッチと同じ場所で行う必要があります。

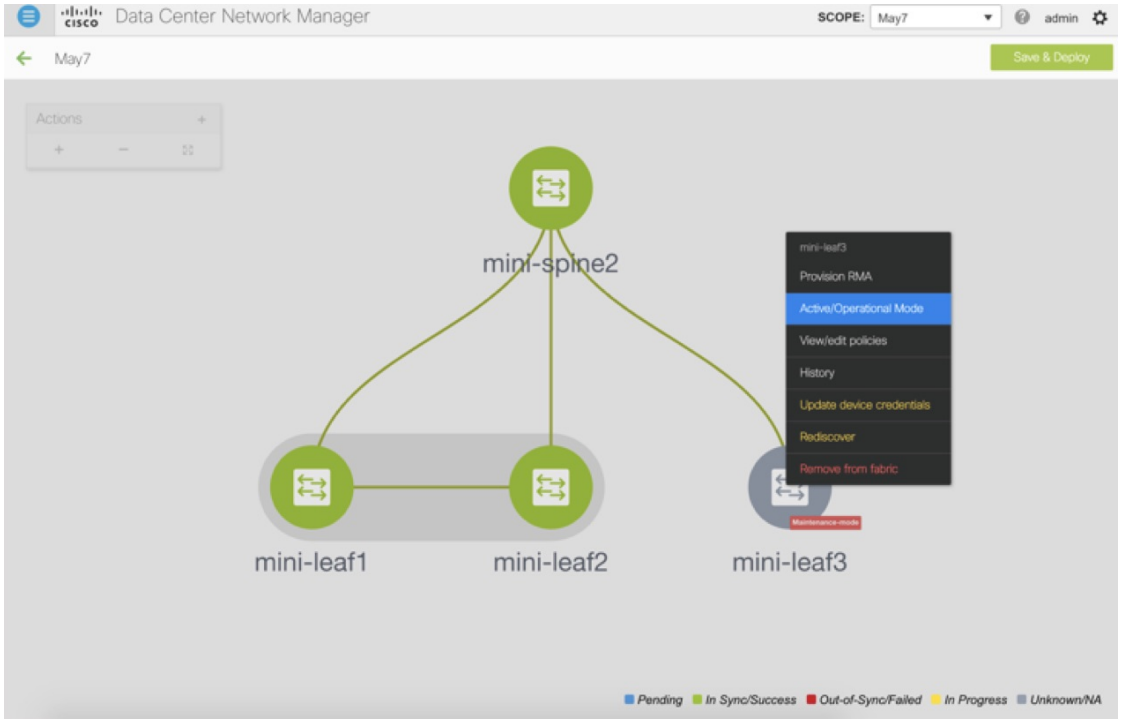
ステップ 5 RMA フローをプロビジョニングし、交換用デバイスを選択します。



ステップ 6 [RMA のプロビジョニング（Provision RMA）] UIには、電源がオンになってから 5ー10 分後に交換デバイスが表示されます。



ステップ 7 正しい交換用デバイスを選択し、**[スイッチの交換（Swap Switch）]** をクリックします。これにより、そのデバイスの完全な「予想される」構成で POAP が開始されます。合計 POAP 時間は、通常、約 10 ～ 15 分です。

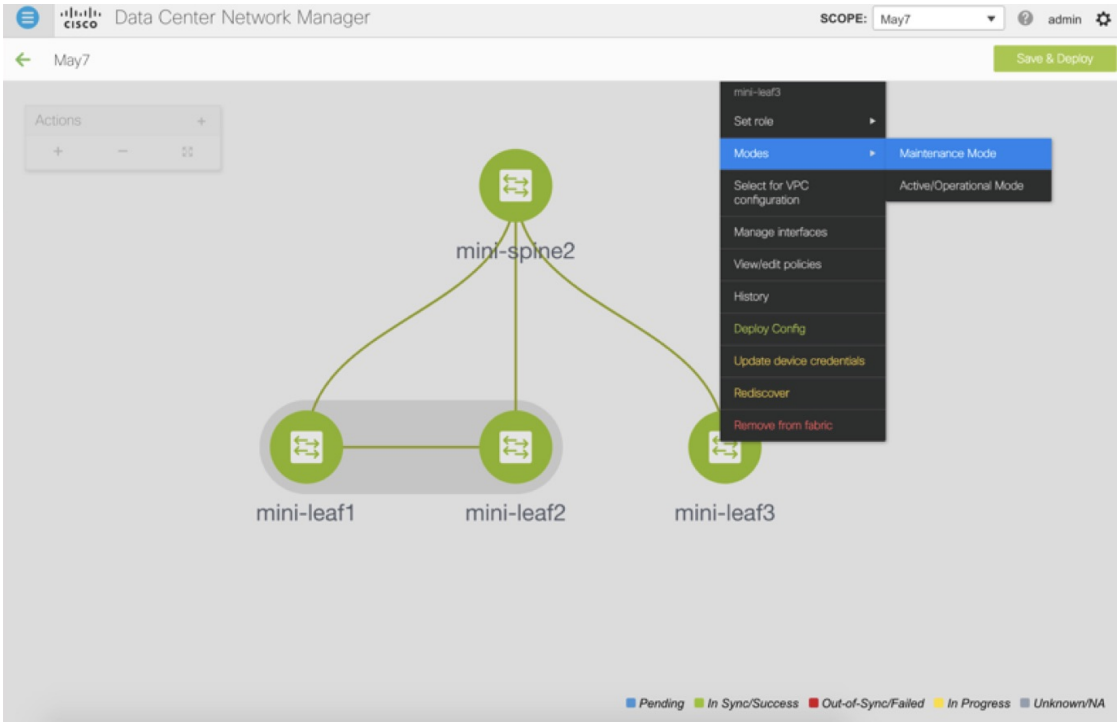


手動 RMA フロー

このフローは、最初の Cisco DCNM 11.0(1) リリースで *IPv6* のみ である場合など、「ブートストラップ」が不可能な（または望ましくない）場合に使用します。

Procedure

ステップ 1 デバイスをメンテナンス モード（オプション）にします。

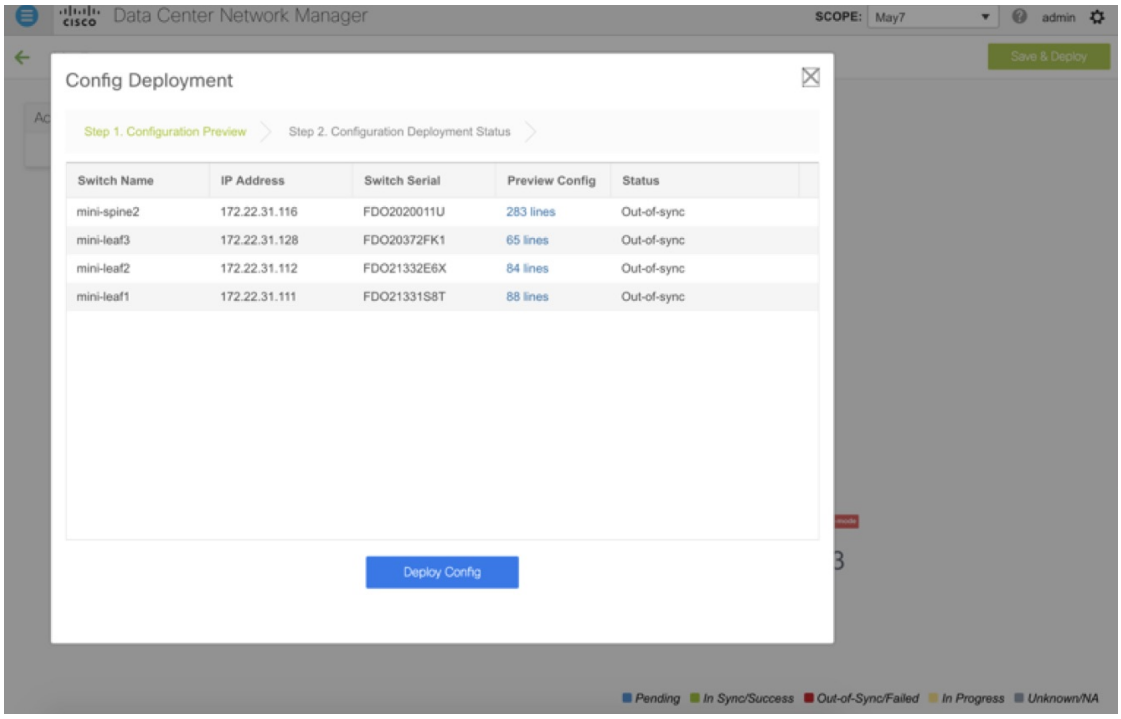


ステップ 2 ネットワーク内のデバイスを物理的に交換します。

ステップ 3 コンソールからログインし、管理 IP とクレデンシャルを設定します。

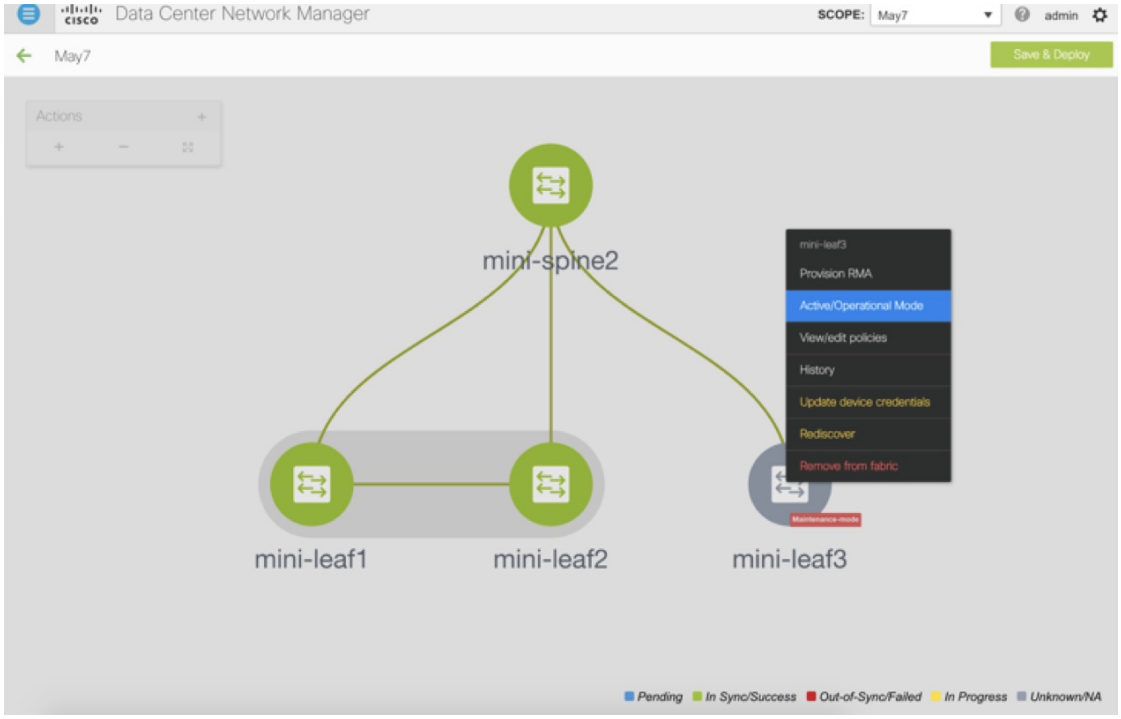
ステップ 4 Cisco DCNM は新しいデバイスを再検出します（または、**[検出（Discovery）] > [再検出（Rediscover）]** を手動で選択できます）。

ステップ 5 **[展開（Deploy）]** を使用して、必要な設定を展開します。



ステップ 6 設定によっては、ブレイクアウト ポートまたは FEX ポートが使用中の場合、設定を完全に復元するために再度展開する必要があります。

ステップ 7 展開が正常に完了し、デバイスが「同期中」になったら、デバイスを通常モードに戻す必要があります。



カスタム メンテナンス モード のプロファイル ポリシー

ローカル認証を持つユーザの RMA

Note 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。

Procedure

ステップ 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。これは、SNMP パスワードを再同期するために必要であり、転送不可能な形式で構成ファイルに保存されます。

ステップ 2 RMA が完了するまで待ちます。

ステップ 3 スイッチの新しい SNMP MD5 キーを使用して、スイッチの Cisco DCNM switch_snmp_user ポリシーを更新します。

インターフェイス

[インターフェイス（Interfaces）] オプションは、スイッチで検出されたすべてのインターフェイス、仮想ポート チャネル（vPC）、およびデバイスに存在しない目的のインターフェイスを表示します。

次の機能を使用できます。

- ポート チャネル、vPC、 Straight-through FEX、Active-Active FEX、ループバック、およびサブインターフェイスを作成、展開、表示、編集、および削除します。

（注）

- 次の機能は、Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x)イメージを使用したスイッチのブラウンフィールド移行ではサポートされていません。
  - X9500 ラインカードを搭載した Cisco Nexus 9300 シリーズ スイッチおよびCisco Nexus 9500 シリーズ スイッチ以外のスイッチでの FEX
  - AA-FEX

  FEX のプラットフォーム サポートについては、プラットフォームと NX-OS のマニュアルを参照して、機能の互換性を確認してください。
- ファブリック内リンクやファブリック間リンクなどのファブリック リンクに関連付けられているインターフェイスを編集するには、リンクに関連付けられたインターフェイスの編集 （261 ページ） を参照してください。
- **flowcontrol** または **priority-flow-control** の設定は、HIF ポートまたはメンバーとしての HIF ポートではサポートされません。

- Cisco Cloud Services Router 1000v シリーズ（Cisco CSR 1000v シリーズ）のトンネル インターフェイスを作成します。
- ブレイクアウト ポートとアンブレイクアウト ポートを作成します。
- インターフェイスをシャットダウンして起動します。
- ポートを再検出し、インターフェイスの設定履歴を表示します。
- インターフェイスおよび vPC にホストポリシーを適用します。たとえば、int_trunk_host_11_1、int_access_host_11_1 などです。
- インターフェイスの情報（管理ステータス、動作ステータス、理由、ポリシー、速度、MTU、モード、VLAN、IP/プレフィックス、VRF、ポートチャネル、インターフェイスのネイバーなど）を表示します。

（注）

- **[ネイバー（Neighbor）]** 列には、検出された接続スイッチ、インテント リンク、および Virtual Machine Manager（VMM）接続の詳細が表示されます。対応するスイッチをクリックすると、その **[スイッチ（Switch）]** のダッシュボードに移動できます。ただし、インテント リンクと VMM リンクはハイパーリンクされておらず、対応する **[スイッチ（Switch）]** ダッシュボードに移動できません。
- [名前（Name）] 列のグラフ アイコンをクリックして、過去 24 時間のインターフェイス パフォーマンス チャートを表示します。ただし、オーバーレイ ネットワークに関連付けられている VLAN インターフェイスのパフォーマンス データは、このグラフには表示されないことに注意してください。

[ステータス（Status）] 列に、次のいずれかのステータスが表示されます。

- 青：保留中
- 緑：同期/成功
- 赤: 非同期/失敗
- 黄色：進行中
- グレー：不明/ NA

- インターフェイスがアウトオブバンドで作成された場合、このインターフェイスを削除するには、ファブリックの再同期を実行するか、構成コンプライアンスのポーリングを待機する必要があります。そうしないと、Config Compliance は正しい差分を生成しません。

ただし、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を追加または編集することはできません。

特定のフィールド（[デバイス名（Device Name）]など）の情報をフィルタリングおよび表示できます。次の表で、このページに表示されるボタンを説明します。

（注）

- 適切な vPC ペア構成を含む、インターフェイス オプションから展開する前に、適切な構成がファブリック ビルダ オプションを介して展開されていることを確認します。ファブリックの展開の前にインターフェイスを追加または編集すると、デバイスで構成が失敗することがあります。
- ファブリック ビルダ トポロジ画面からインターフェイスを管理することもできます。スイッチを右クリックし、[インターフェイスの管理（Manage Interfaces）] オプションを選択します。スイッチごとにインターフェイスを管理できます。スイッチが vPC ペアの一部である場合、両方のピアからのインターフェイスがページに表示されます。
- インターフェイス マネージャから構成を展開する前に、vPCペアリングを含むアンダーレイをファブリックに展開します。

フィールド	説明
追加（Add）	ポートチャネル、vPC、Straight-through FEX、Active-Active FEX、ループバックおよびサブインターフェイスなどの論理インターフェイスを追加できます。
ブレークアウト、ブレークアウト解除	ブレークアウト状態のインターフェイスまたはブレークアウト解除インターフェイスを、ブレークアウトにできます。
編集	インターフェイスに関連付けられているポリシーを編集および変更できます。
削除	[インターフェイス（Interfaces）] 画面から作成された論理インターフェイスを削除できます。オーバーレイとアンダーレイからアタッチされたポリシーを持つインターフェイスは削除できません。
シャットダウンなし	インターフェイスを有効にできます（シャットダウンまたは管理起動なし）。
シャットダウン	インターフェイスをシャットダウンできます。
表示する	interface show コマンドを表示できます。show コマンドを使用するには、テンプレート ライブラリに show テンプレートが必要です。
再検出	選択したインターフェイスのコンプライアンス ステータスを再検出または再計算できます。

フィールド	説明
インターフェイス履歴	インターフェイス展開履歴の詳細を表示できます。
展開	保存したインターフェイス設定を展開または再展開できます。

Cisco DCNM リリース 11.4(1) 以降で、**[インターフェイス（Interfaces）]** ウィンドウでサポートされるさまざまなユーザーロールとこれらのロールの操作について、次の表で説明します。

操作	ユーザ ロール		
	network-admin	**network-operator**	**network-stager**
追加	保存、プレビュー、展開	ブロック	保存、プレビュー
サブ会議	サポート対象	ブロック済み	ブロック済み
ブレークアウト解除	サポート対象	ブロック済み	ブロック済み
編集	保存、プレビュー、展開	プレビュー	保存、プレビュー
削除	保存、プレビュー、展開	ブロック	保存、プレビュー
シャットダウン	保存、プレビュー、展開	ブロック	保存、プレビュー
シャットダウンなし	保存、プレビュー、展開	ブロック	保存、プレビュー
表示	サポート対象	サポート対象	サポート対象
再検出	サポート対象	サポート対象	サポート対象
展開	プレビュー、展開	ブロック済み	ブロック済み

次の表に、Cisco DCNM リリース 11.5(1) からの **[インターフェイス（Interfaces）]** ウィンドウのホスト側ポートでの新しいユーザーロール access-admin 操作のサポートを示します。

操作	ユーザ ロール
	Role: access-admin
追加	保存、プレビュー、展開
サブ会議	ブロック済み
ブレークアウト解除	ブロック済み

操作	ユーザ ロール
	Role: access-admin
編集	保存、プレビュー、展開 （注） Access-admin ユーザー ロールは、Easy ファブリックのファブリック間リンクやファブリック内リンクなどのリンク ポリシーに関連付けられたインターフェイスを編集できません。このユーザーロールは、LAN クラシック ファブリックのインターフェイスを編集できます。
削除	保存、プレビュー、展開
シャットダウン	保存、プレビュー、展開
シャットダウンなし	保存、プレビュー、展開
表示	サポート対象
再検出	サポート対象
展開	プレビュー、展開

Cisco DCNM リリース 11.4(1) 以降、DCNM で展開を無効にしたり、ネットワーク管理者としてファブリックをフリーズしたりできます。ただし、ファブリックをフリーズする場合、またはファブリックがモニタ モードの場合、すべてのアクションを実行することはできません。

次の表に、ファブリックをフリーズするとき、およびファブリックのモニタ モードを有効にするときに実行できるアクションを示します。

操作	DCNM モード	
	フリーズ モード	モニタ モード
追加	保存、プレビュー	ブロック
サブ会議	ブロック済み	ブロック済み
ブレークアウト解除	ブロック済み	ブロック済み
編集	保存、プレビュー	ブロック
削除	保存、プレビュー	ブロック
シャットダウン	保存、プレビュー	ブロック

操作	DCNM モード	
	フリーズ モード	モニタ モード
シャットダウンなし	保存、プレビュー	ブロック
表示	サポート対象	サポート対象
再検出	サポート対象	サポート対象
展開	ブロック済み	ブロック済み

関連付けられた操作のボタンは、それに応じてグレー表示されます。

構成プロファイルの一部である SVI で管理操作（shutdown/no shutdown）を実行すると、連続した**保存して展開**操作で **no interface vlan** コマンドが生成されます。

ポリシーのない SVI の場合、管理操作の実行時、つまり **Interface Manager** から shutdown /no shutdown コマンドがプッシュされると、**int_vlan_admin_state** ポリシーが SVI に関連付けられます。

たとえば、**switch_freeform** から SVI を作成して展開します。

```
interface vlan1234
  description test
  no shutdown
  no ip redirects
  no ipv6 redirects
```

インターフェイス マネージャから SVI をシャットダウンすると、**int_vlan_admin_state** ポリシーが SVI に関連付けられます。

保留中の差分は次のように表示されます。

```
interface Vlan1234
  shutdown
  no ip redirects
  no ipv6 redirects
  description test
  no shutdown
```

自由形式の設定から **no shutdown CLI** を削除します。

ユーザが SVI で管理操作を実行した場合、デバイスには実行構成のインターフェイスがあります。したがって、ネットワーク切断後の **interface vlan** は引き続き存在し、インターフェイスが検出されます。**Interface Manager** からインターフェイスを手動で削除する必要があります。

この項の内容は、次のとおりです。

インターフェイスの追加

Cisco DCNM Web UIからインターフェイスを追加するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

右上に **[範囲（Scope）]** オプションが表示されます。特定のファブリックのインターフェイスを表示する場合は、リストからファブリック ウィンドウを選択します。

ステップ 2 **[追加（Add）]** をクリックして、論理インターフェイスを追加します。

[インターフェイスの追加（Add Interface）] ウィンドウが表示されます。

ステップ 3 **[タイプ（Type）]** ドロップダウン リストで、インターフェイス タイプを選択します。

有効な値は、ポートチャネル、仮想ポートチャネル（vPC）、ストレート（ST）FEX、アクティブ-アクティブ（AA）FEX、ループバック、、トンネルイーサネット、およびスイッチ仮想インターフェイス（SVI） です。インターフェイス タイプを選択すると、それぞれのインターフェイス ID フィールドが表示されます。

- DCNMを通じてポートチャネルを作成する場合は、同じ速度のインターフェイスを追加します。さまざまな速度のインターフェイスから作成されたポート チャネルは起動しません。たとえば、2 つの *10* ギガビット イーサネット ポートを持つポート チャネルが有効です。ただし、*10* ギガビット イーサネット + *25* ギガビット イーサネット ポートの組み合わせを持つポート チャネルは無効です。
- vPC ホストを追加するには、ファブリック トポロジで（ファブリック ビルダを介して）vPC スイッチを指定し、**[保存して展開（Save and Deploy）]**オプションを使用して vPC およびピアリンク構成を展開する必要があります。vPC ペアの構成が展開されると、[vPC ペアの選択（Select a vPC pair）] ドロップダウンボックスに表示されます。

  int_vpc_trunk_host_11_1 ポリシーを使用して vPC を作成できます。
- サブインターフェイスを追加する場合は、[追加（Add）] ボタンをクリックする前に、インターフェイス テーブルからルーテッド インターフェイスを選択する必要があります。
- [インターフェイス（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、eBGP、および外部ファブリックでサポートされています。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 （51 ページ）を参照してください。

ステップ 4 **[デバイスの選択（Select a Device）]** フィールドで、デバイスを選択します。

デバイスは、ファブリックおよびインターフェイスタイプに基づいてリストされます。外部ファブリック デバイスは、ST FEX および AA FEX には表示されません。vPC またはアクティブからアクティブ FEX の場合は、vPC スイッチペアを選択します。

ステップ 5 選択したインターフェイスに基づいて、表示される各インターフェイス ID フィールド（**ポートチャネル ID**、**vPC ID**、**ループバック ID**、および **サブインターフェイス ID**）に ID 値を入力します。

この値は上書きできます。新しい値は、リソース マネージャ プールで使用可能な場合にのみ使用されます。それ以外の場合は、エラーになります。

ステップ 6 **[ポリシー（Policy）]** フィールドで、インターフェイスに適用するポリシーを選択します。

このフィールドには、インターフェイスのタイプに基づいてフィルタリングされた、*interface interface_edit_policy* のインターフェイス Python ポリシーのみが表示されます。

_upg インターフェイス ポリシーを作成しないでください。たとえば、**vpc_trunk_host_upg**、**port_channel_aa_fex_upg**、**port_channel_trunk_host_upg**、および **trunk_host_upg** オプションを使用してポリシーを作成することはできません。

（注） ポリシーは、**[タイプ（Type）]** ドロップダウンリストで選択したインターフェイス タイプと、**[デバイスの選択（Select a Device）]** ドロップダウンリストで選択したデバイスに基づいてフィルタリングされます。

ステップ 7 **[全般（General）]** タブの必須フィールドに値を入力します。

フィールドは、選択したインターフェイス タイプによって異なります。

（注） Cisco DCNM Release 11.5(1) 以降では、vPC の作成時に Peer-1 の構成を Peer-2 にミラーリングできます。**[構成ミラーリングの有効化（Enable Config Mirroring）]** チェックボックスをオンにすると、[Peer-2] フィールドがグレー表示されます。[Peer-1] フィールドに入力した設定は、[Peer-2] フィールドにコピーされます。

ステップ 8 [保存（Save）] をクリックして、設定を保存します。

（注） インターフェイスに QoS ポリシーを適用するには、参照を使用してインターフェイスの自由形式を作成します。

保存された設定のみがデバイスにプッシュされます。インターフェイスの追加中は、最初の保存後にのみポリシー属性を変更できます。すでに使用されている ID を使用しようとすると、リソースが割り当てられないというエラーが発生します。

ステップ 9 （任意）**[プレビュー（Preview）]** オプションをクリックして、展開する構成をプレビューします。

ステップ 10 **[展開（Deploy）]** をクリックして、指定した論理インターフェイスを展開します。

新しく追加したインターフェイスが画面に表示されます。

サブ会議

[ブレークアウト（Breakout）] アイコン  の横にあるドロップダウン矢印をクリックして、使用可能なブレイクアウト オプションのリストを表示します。使用可能なオプションは、

10g-4x、**25g-4x**、**50g-2x**、**50g-4x**、**100g-2x**、**100g-4x**、**200g-2x**、および**Unbreakout**です。必要なオプションを選択します。

インターフェイスの編集

Cisco DCNM Web UIからインターフェイスを編集するには、次の手順を実行します。

（注） **[インターフェイスの編集（Edit Interface）]**では、ポリシーを変更したり、ポートチャネルまたはvPCからインターフェイスを追加または削除したりできます。

手順

ステップ1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

画面の左上にあるブレークアウトオプションを使用してインターフェイスのブレークアウト、およびブレークアウト解除ができます。

ステップ2 インターフェイスまたはvPCを編集するには、インターフェイス チェックボックスをオンにします。

複数のインターフェイスを編集するには、対応するチェックボックスをオンにします。複数のポート チャネルおよびvPCを編集することはできません。異なるタイプのインターフェイスを同時に編集することはできません。

ステップ3 インターフェイスを編集するには、**[編集（Edit）]** をクリックします。

[構成の編集（Edit Configuration）]ウィンドウに表示される変数は、テンプレートとそのポリシーに基づいています。適切なポリシーを選択します。ポリシーをプレビューし、同じように保存して展開します。このウィンドウには、インターフェイスの種類に基づいてフィルタリングされた、*interface_edit_policy*タグが付いたインターフェイスPythonポリシーのみが表示されます。

vPCのセットアップでは、2つのスイッチは、編集ウィンドウに表示されるスイッチ名の順序になります。たとえば、スイッチ名が *LEAF1:LEAF2* と表示されている場合、Leaf1はピア スイッチ1、Leaf2はピア スイッチ2です。

スイッチへのオーバーレイ ネットワークの展開中に、ネットワークをトランク インターフェイスに関連付けることができます。トランクインターフェイスとネットワークの関連付けは、**[インターフェイス（Interfaces）]**画面に反映されます。このようなインターフェイスを更新できます。

[制御（Control）]>[インターフェイス（Interfaces）]画面から作成されていないインターフェイスポリシーの場合、一部の構成を編集できますが、ポリシー自体は変更できません。編集できないポリシーとフィールドはグレー表示されます。

次に、編集できないポリシーの例を示します。

- ループバック インターフェイス ポリシー：int_fabric_loopback_11_1 ポリシーは、ループバック インターフェイスを作成するために使用されます。ループバック IP アドレスと説明は編集できますが、int_fabric_loopback_11_1 ポリシーインスタンスは編集できません。
- ファブリック アンダーレイ ネットワーク インターフェイス ポリシー（int_fabric_num_11_1 など）およびファブリック オーバーレイ ネットワーク インターフェイス（NVE）ポリシー。
- vPC に関連付けられたポート チャネルおよびメンバーポートを含む、ポート チャネルおよびポート チャネルのメンバー ポートに関連付けられたポリシー。
- ネットワークおよび VRF の作成時に作成された SVI。関連付けられた VLAN がインターフェイス リストに表示されます。

リンクに関連付けられたインターフェイスの編集

リンクには、ファブリック内リンクとファブリック間リンクの2種類があります。名前が示すように、ファブリック内リンクは同じ Easy ファブリック内のデバイス間に設定され、通常はスパイン リーフ接続に使用されます。ファブリック間リンクは、Easy ファブリックと、通常は他の外部または Easy ファブリック間に設定されます。外部 WAN や DC I接続に使用されます。ポリシーは、リンクの両端に適用される設定を効果的に示す各リンクに関連付けられます。つまり、リンク ポリシーは、リンクを形成する2つのインターフェイスに関連付けられた個々の子インターフェイス ポリシーの親になります。このシナリオでは、リンク ポリシーを編集して、説明、IPアドレス、インターフェイスごとの自由形式の設定などのインターフェイス ポリシー フィールドを編集する必要があります。次の手順は、リンクに関連付けられたインターフェイスを編集する方法を示しています。

Procedure

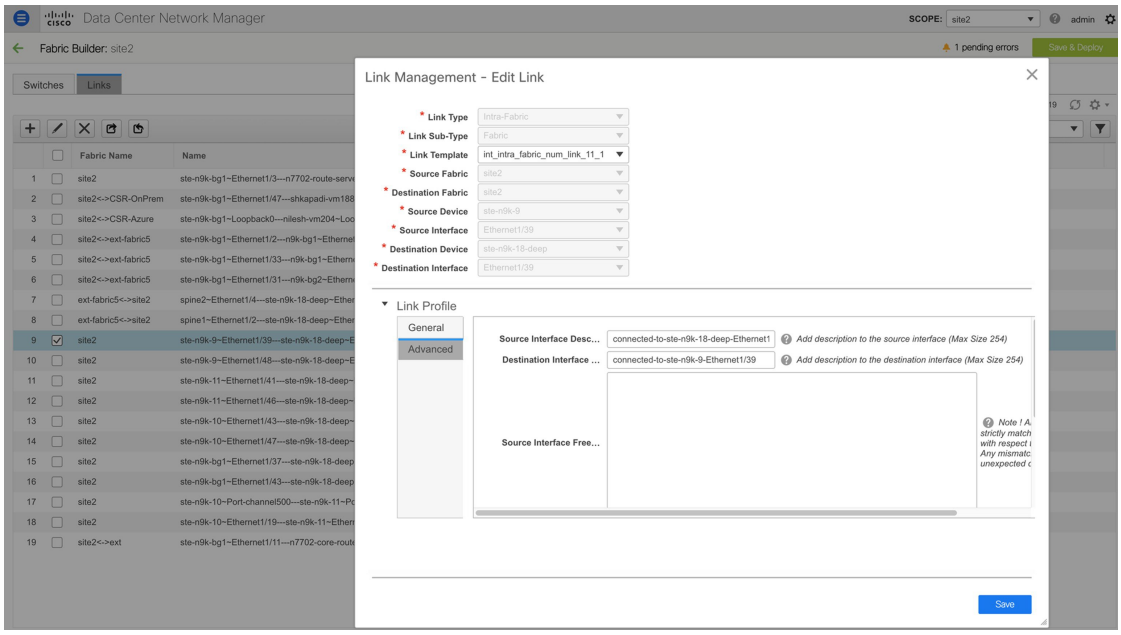
ステップ 1 **[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** を選択し、リンクを含むファブリックを選択します。

ステップ 2 **[アクション（Actions）]** パネルで **[表形式ビュー（Tabular view）]** をクリックします。

[スイッチ（Switches）] タブと **[リンク（Links）]** タブのあるウィンドウが表示されます。

ステップ 3 **[リンク（Links）]** タブをクリックします。

ステップ 4 編集するリンクを選択し、**[リンクの更新（Update Link）]** アイコンをクリックします。



要件に基づいてリンクを更新し、**[保存（Save）]** をクリックします。

インターフェイスの削除

Cisco DCNM Web UI からインターフェイスを削除するには、次の手順を実行します。

（注） このオプションを使用すると、論理ポート、ポート チャネル、および vPC のみを削除できます。オーバーレイまたはアンダーレイ ポリシーがアタッチされていない場合は、インターフェイスを削除できます。

ポート チャネルまたは vPC が削除されると、対応するメンバー ポートにデフォルトのポリシーが関連付けられます。デフォルト ポリシーは、`server.properties` ファイルで設定できます。

手順

ステップ 1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 インターフェイスを選択します。

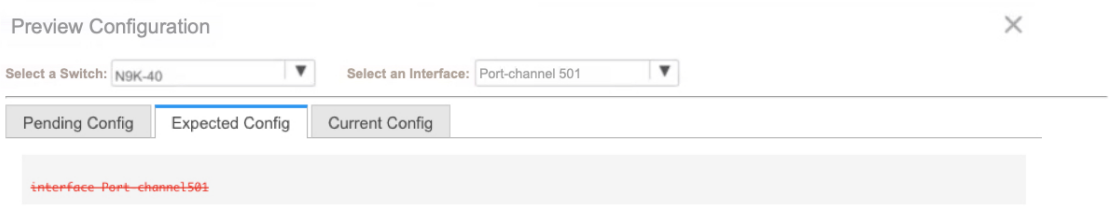
ステップ 3 [削除（Delete）] をクリックします。

ファブリック アンダーレイで作成された論理インターフェイスは削除できません。

ステップ 4 **[Save（保存）]** をクリックします。

ステップ 5 （任意）インターフェイスを削除する前に、**[プレビュー（Preview）]** をクリックしてすべての変更を表示します。

削除は、**[予期される構成（Expected Config）]** タブの下に取り消し線付きの赤色で強調表示されます。



ステップ 6 **[展開（Deploy）]** をクリックして、インターフェイスを削除します。

インターフェイスのシャットダウンと起動

Cisco DCNM Web UI からインターフェイスをシャットダウンして起動するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）]** > **[インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 シャットダウンまたは起動するインターフェイスを選択します。

ステップ 3 **[シャットダウン（Shutdown）]**をクリックして、選択したインターフェイスを無効にします。たとえば、ネットワークからホストを分離したり、ネットワーク内でアクティブでないホストを分離したりできます。

変更を保存、プレビュー、および展開できる確認ウィンドウが表示されます。**[保存（Save）]** をクリックして、変更の展開をプレビューします。

ステップ 4 **[シャットダウンなし（No Shutdown）]** をクリックして、選択したインターフェイスを起動します。

変更を保存、プレビュー、および展開できる確認ウィンドウが表示されます。**[保存（Save）]** をクリックして、変更をプレビューまたは展開します。

インターフェイス構成の表示

Cisco DCNM Web UI からインターフェイス構成コマンドを表示して実行するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

構成を表示するインターフェイスを選択します。

ステップ 2 **[インターフェイス表示コマンド（Interface Show Commands）]** ウィンドウで、**[表示（Show）]** ドロップダウンボックスからアクションを選択し、**[実行（Execute）]** をクリックします。インターフェイス構成が、画面の右側の **[出力（Output）]** セクションに表示されます。

Show コマンドの場合は、インターフェイスで対応する **show** テンプレート、またはポートチャネルや vPC などのインターフェイス サブタイプを **[テンプレート ライブラリ（Template Library）]** で定義する必要があります。

インターフェイスの再検出

Cisco DCNM Web UI からインターフェイスを再検出するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 再検出するインターフェイスを選択します。

ステップ 3 **[再検出（Rediscover）]** をクリックして、選択されたインターフェイスを再検出します。たとえば、インターフェイスを編集または有効にした後、インターフェイスを再検出できます。

インターフェイス履歴の表示

Cisco DCNM Web UI からインターフェイス履歴を表示するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 インターフェイスを選択します。

ステップ 3 **[インターフェイス履歴（Interface History）]** をクリックして、インターフェイスでの構成履歴を表示します。

ステップ 4 **[ステータス（Status）]** をクリックして、その構成インスタンスに設定されている各コマンドを表示します。

インターフェイス構成の展開

Cisco DCNM Web UIからインターフェイス構成を展開するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 展開するインターフェイスを選択します。

（注） 複数のインターフェイスを選択し、保留中の設定を展開できます。

ステップ 3 **[展開（Deploy）]** をクリックして、インターフェース用に保存されている構成を展開または再展開します。

インターフェイス設定を展開すると、インターフェイス ステータス情報が更新されます。ただし、全体的なスイッチレベルの状態は保留状態（青色）になることがあります。インターフェイス、リンク、ポリシーテンプレートの更新、トップダウンなどのいずれかのモジュールからインテントが変更されると、スイッチ レベルの全体的な状態は保留状態になります。保留状態では、スイッチに保留中の設定またはスイッチ レベルの再計算がある場合があります。スイッチ レベルの再計算は、次の場合に発生します。

- スイッチをプレビューまたは展開します
- 保存および展開中
- 毎時同期中

スイッチをプレビューまたは展開して、状態を確認し、保留状態の根本原因を理解します。ファブリック全体の再計算のために保存して展開します。

[展開（Deploy）] をクリックする前に **[プレビュー（Preview）]** をクリックし、構成をプレビューします。

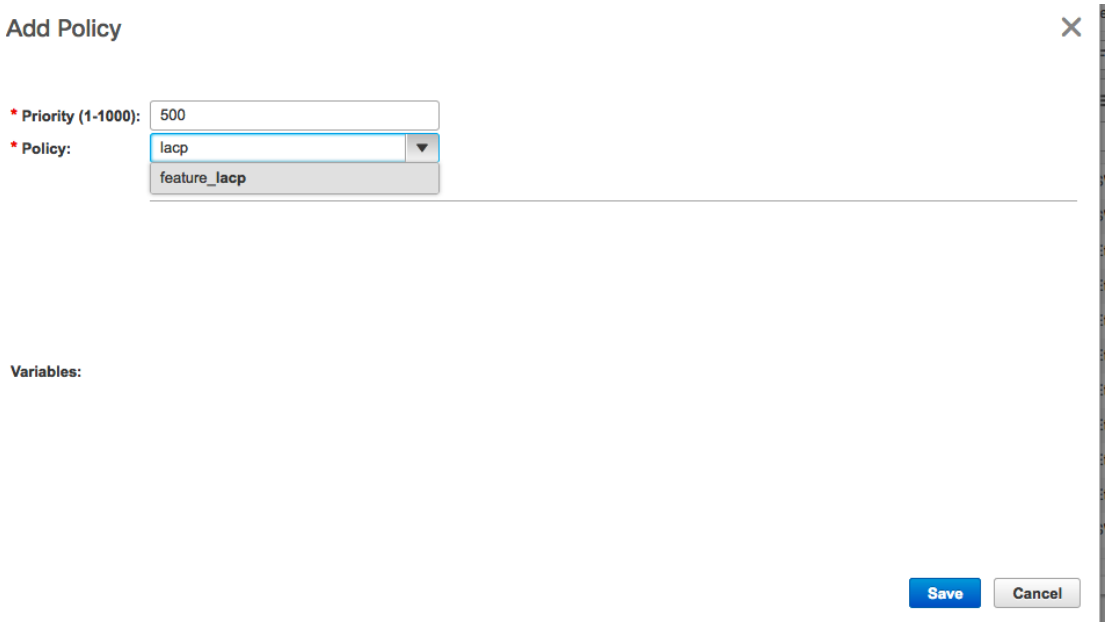
外部ファブリック インターフェイスの作成

外部ファブリック デバイスのポート チャネル、vPC、サブインターフェイス、およびループバック インターフェイスを追加および編集できます。ストレート FEX およびアクティブ-アクティブ FEX 機能は追加できません。

ブレークアウト ポート機能は、外部ファブリックの Cisco Nexus 9000、3000、および 7000 シリーズ スイッチでのみサポートされます。

外部ファブリック デバイスにインターフェイスを追加すると、リソース マネージャはデバイスと同期しません。そのため、ID フィールドに入力された値（ポート チャネルID、vPC ID、ループバック ID など）がスイッチで事前に設定されていないことを確認します。

外部ファブリックでポート チャネルを設定する場合は、ポート チャネルが設定されるスイッチに **feature_lacp** ポリシーを追加して展開する必要があります。



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。ファブリック トポロジ画面で **[保存して展開（Save & Deploy）]** をクリックすると、エラー メッセージが表示されます。ただし、次の設定（スイッチ アイコンを右クリックすると使用可能）が許可されます。

vPC ペアリング：vPC スイッチ ペアを指定できますが、これは参照用です。

ポリシーの表示/編集：ポリシーを追加できますが、スイッチに展開することはできません。

インターフェイスの管理：インターフェイスを追加する目的のみを作成できます。インターフェイスを展開、編集、または削除しようとすると、エラー メッセージが表示されます。

インターフェイスグループ

Cisco DCNM リリース 11.5(1) 以降、ファブリック レベルでホスト側のインターフェイスをグループ化できるインターフェイス グループを作成できます。具体的には、物理イーサネット インターフェイス、L2 ポート チャネル、および vPC のインターフェイス グループを作成できます。インターフェイス グループのインターフェイスに複数のオーバーレイ ネットワークを接続または接続解除できます。

ガイドライン

- インターフェイス グループは、**Easy_Fabric_11_1** テンプレートを使用するファブリックでのみサポートされます。
- インターフェイス グループは、ファブリックに固有です。たとえば、2つのファブリック（Fab1 と Fabric 2）を考えます。Fab1 のインターフェイス グループ IG1 は、Fab 2 には適用されません。
- インターフェイス グループは、特定のタイプのインターフェイスのみを持つことができます。たとえば、物理イーサネット トランク インターフェイスの場合は IG1、L2 トランク ポート チャネルの場合は IG2、vPC ホスト トランク ポートの場合は IG3 など、3 つのタイプのインターフェイスをグループ化する場合は、3つの個別のインターフェイス グループが必要です。
- インターフェイス グループは、事前プロビジョニングされたインターフェイスを使用して作成することもできます。
- インターフェイス グループは、リーフ ロールを持つスイッチに限定されます。これらは、Border、BGW、およびその他の関連バリアントなどの他のロールではサポートされません。
- インターフェイス グループの一部である L2 ポート チャネルおよび vPC の場合、インターフェイス グループに関連付けられているネットワークがない場合でも、それらはインターフェイス グループから関連付け解除されるまで削除できません。同様に、オーバーレイ ネットワークを持たないがIGの一部であるトランク ポートは、アクセス ポートに変換できません。つまり、インターフェイス グループの一部であるインターフェイスのポリシーは変更できません。ただし、ポリシーの特定のフィールドは編集できます。
- リーフ スイッチの L4～L7 サービス設定では、サービス接続に使用されるトランク ポートをインターフェイス グループの一部にすることはできません。
- イージーファブリックのファブリック単位のバックアップを実行すると、そのファブリックで作成されたインターフェイス グループがある場合、関連するすべてのインターフェイス グループの状態がバックアップされます。
- イージーファブリックにインターフェイス グループが含まれている場合、このファブリックは MSO にインポートできません。同様に、イージー ファブリックが MSO に追加されている場合は、イージーファブリック内のスイッチに属するインターフェイスのインターフェイス グループを作成できません。
- **[インターフェイス グループ（Interface Group）]** ボタンは、管理者およびステージャ ユーザに対してのみ有効です。他のすべてのユーザの場合、このボタンは無効になります。
- **[インターフェイス グループ（Interface Group）]** ボタンは、次の状況では無効になります。
  - **[SCOPE]** ドロップダウン リストから **[データセンター（Data Center）]** を選択します。
  - スイッチのないファブリックを選択します。

- vPC、ポートチャネル、およびイーサネット以外の他のインターフェイスを選択します。
- インターフェイスに別の送信元からのポリシーがアタッチされている場合：
  - インターフェイスがポート チャネルまたは vPC のメンバーである場合。
  - ポート チャネルが vPC のメンバーである場合。
  - インターフェイスにアンダーレイまたはリンクからのポリシーがある場合。

（注） 異なるタイプのインターフェイスを選択すると、**[インターフェイス グループ（Interface Group）]** ボタンが有効になります。ただし、インターフェイス グループに対して異なるタイプのインターフェイスを作成または保存しようとすると、エラーが表示されます。

インターフェイス グループの作成

手順

ステップ 1 DCNM から、**[制御（Control）]>[ファブリック（Fabrics）]>[インターフェイス（Interfaces）]** に移動します。

ステップ 2 **[範囲（SCOPE）]** ドロップダウン リストから、ファブリックを選択します。

ステップ 3 グループ化する必要があるインターフェイスを選択し、**[インターフェイスグループ（Interface Group）]** をクリックします。

ステップ 4 4.**[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウで、**[インターフェイス グループの選択（Select Interface Group）]** フィールドにインターフェイス グループ名を入力してカスタム インターフェイス グループを作成し、**[カスタムの作成（Create custom）]** をクリックします。インターフェイス グループ名の最大長は 64 文字です。

すでにインターフェイス グループを作成している場合は、**[インターフェイス グループの選択（Select Interface Group）]** ドロップダウン リストから選択します。また、インターフェイスがすでにインターフェイス グループの一部である場合は、**[インターフェイス グループの選択（Select Interface Group）]** ドロップダウンリストから新しいグループを選択することで、そのインターフェイスを別のインターフェイス グループに移動できます。

（注） インターフェイスは、1つのインターフェイス グループにのみ属することができます。

インターフェイス グループは、**[インターフェイス （Interfaces）]** ウィンドウまたは **[ネットワーク（Networks）]** ウィンドウから作成できます。詳細については、インターフェイス グループへのネットワークの接続 （270 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

[インターフェイス（Interfaces）] ウィンドウの **[インターフェイス グループ（Interfaces Groups）]** 列にインターフェイス グループ名が表示されます。

インターフェイス グループからのインターフェイスの削除

手順

ステップ 1 DCNM から、**[制御（Control）] > [ファブリック（Fabrics）] > [インターフェイス（Interfaces）]** に移動します。

ステップ 2 **[範囲（SCOPE）]** ドロップダウン リストから、ファブリックを選択します。

ステップ 3 インターフェイス グループから関連付けを解除するインターフェイスを選択し、**[インターフェイス グループ（Interface Group）]** をクリックします。

ステップ 4 **[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウで、**[インターフェイス グループの選択（Select Interface Group）]** ドロップダウンリストで何も選択されていないことを確認し、**[クリア（Clear）]** をクリックします。

関連付けられたすべてのインターフェイスをクリアするかどうかを確認するダイアログボックスが表示されます。**[はい（Yes）]** をクリックして続行します。これらのインターフェイスに接続されているネットワークがある場合、**[クリア（Clear）]** をクリックすると、それらのネットワークも切断されます。

インターフェイス グループへのネットワークの接続

手順

ステップ 1 DCNM から、**[制御（Control）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** に移動します。

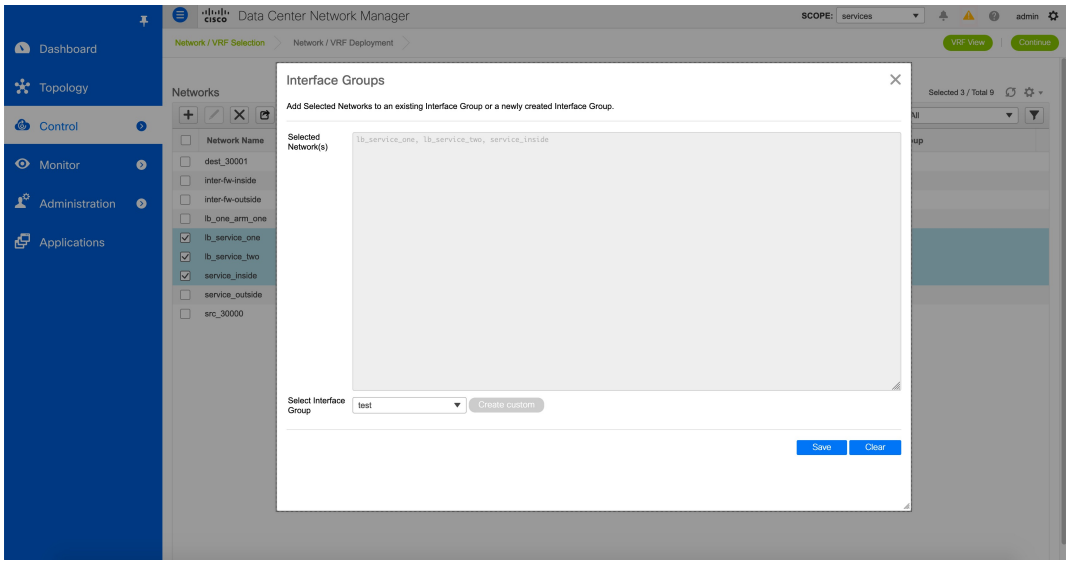
ステップ 2 **[範囲（SCOPE）]** ドロップダウン リストから、ファブリックを選択します。

ステップ 3 **[ネットワーク（Networks）]** ウィンドウで、インターフェイス グループに接続する必要があるネットワークを選択し、**[インターフェイス グループ（Interface Group）]** をクリックします。

（注）
- オーバーレイ ネットワークは、複数のインターフェイス グループに属することができます。
- VLAN ID を持つネットワークのみを選択できます。それ以外の場合は、適切なエラー メッセージが表示されます。

ステップ 4 **[インターフェイス グループ（Interface Groups）]** ウィンドウで、次の操作を実行できます。

- **[インターフェイス グループの選択（Select Interface Group）]** ドロップダウン リストから既存のインターフェイス グループを選択し、**[保存（Save）]** をクリックします。



たとえば、3つのネットワークとインターフェイス グループ **test** を選択し、**[保存（Save）]** ボタンをクリックすると、次の操作がバックグラウンドで実行されます。

1. DCNM は、インターフェイス グループ **[test]** の一部であるインターフェイスを取得します。
2. DCNM は、3 つのネットワークがインターフェイス グループ **[test]** に追加されることを決定します。したがって、これらのネットワークは、インターフェイス グループ **test** の一部であるすべてのインターフェイスに自動接続されます。
3. インターフェイスごとに、DCNM は 選択したネットワークごとに **[switchport trunk allowed vlan add xxxx]** コマンドを 3 回プッシュします。

   （注）　DCNM は、重複する構成インテントがないことを保証します。

[クリア（Clear）] ボタンをクリックすると、DCNM により **[switchport trunk allowed vlan remove xxx]** 構成インテントがプッシュされます。

- **[インターフェイス グループの選択（Select Interface Group）]** フィールドにインターフェイス グループ名を入力してカスタム インターフェイス グループを作成し、**[カスタムの作成（Create custom）]** をクリックします。**[Save（保存）]** をクリックします。

  このオプションを選択する場合は、**[インターフェイス（Interfaces）]** ウィンドウでこのインターフェイス グループにインターフェイスを追加してください。その結果、DCNM は次の操作を実行します。

  1. インターフェイス グループに属していない既存のすべてのオーバーレイ ネットワークをこれらのインターフェイスから削除します。
  2. インターフェイス グループの一部であるが、まだこれらのインターフェイスに接続されていない新しいオーバーレイ ネットワークを追加します。

インターフェイス グループへのインターフェイスの関連付けの詳細については、インターフェイス グループの作成 （268 ページ） を参照してください。

ステップ 5 **[続行（Continue）]** をクリックし、**[保存して展開（Save & Deploy）]** をクリックして、選択したネットワークをスイッチに展開します。

インターフェイス グループからのネットワークの接続解除

この手順では、[ネットワーク（Networks）] ウィンドウでインターフェイス グループからネットワークの接続を解除する方法を示します。また、**[インターフェイス（Interfaces）]** ウィンドウでインターフェイス グループからインターフェイスを削除すると、ネットワークの接続を解除できます。詳細については、「インターフェイス グループからのインターフェイスの削除」を参照してください。

手順

ステップ 1 1. DCNM から、**[制御（Control）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** に移動します。

ステップ 2 **[範囲（SCOPE）]** ドロップダウン リストから、ファブリックを選択します。

ステップ 3 **[ネットワーク（Networks）]** ウィンドウで、インターフェイス グループに接続解除する必要があるネットワークを選択し、**[インターフェイス グループ（Interface Group）]** をクリックします。

ステップ 4 **[インターフェイス グループ（Interface Group）]** ウィンドウで、**[インターフェイス グループの選択（Select Interface Group）]** ドロップダウン リストからインターフェイスグループを選択し、**[クリア（Clear）]** をクリックしてネットワークの接続を解除します。

ステップ 5 （任意） **[制御（Control）] > [ファブリック（Fabrics）] > [インターフェイス（Interfaces）]** に移動します。

[オーバーレイ ネットワーク（Overlay Network）] 列の下に、対応するインターフェイスの未接続ネットワークが赤色で表示されます。ネットワークをクリックすると、取り消し線が引かれた設定が表示されます。

ステップ 6 **[ファブリック ビルダ（Fabric Builder）]** または **[ネットワーク（Networks）]** ウィンドウに移動し、**[保存と展開（Save & Deploy）]** をクリックします。

インターフェイス グループの削除

インターフェイス グループは、使用されていないときに自動的に削除されます。インターフェイス グループにマッピングされたインターフェイスおよびネットワークがない場合、DCNM はインターフェイス グループの暗黙的な削除を実行します。このチェックは、**[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウで **[クリア（Clear）]** ボタンをクリッ

クするたびに実行されます。インターフェイスグループを明示的にクリーンアップする必要がある例外シナリオが存在する場合があります。

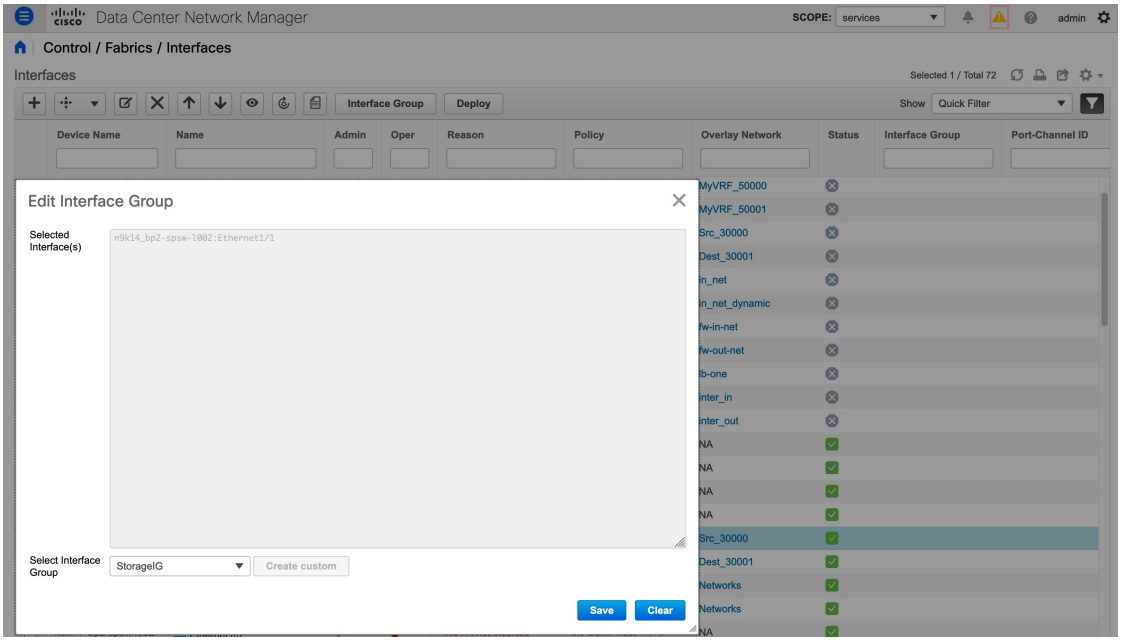
たとえば、インターフェイス グループ **storageIG** を作成し、それにインターフェイスを追加します。後で、インターフェイス マッピングを別のグループに変更します。したがって、インターフェイスを選択し、**[インターフェイス グループ（Interface Group）]** をクリックして **[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウを開きます。**diskIG** という名前の別のインターフェイス グループを選択します。現在、**storageIG** インターフェイス グループには、関連付けられているメンバー インターフェイスまたはネットワークがありません。この場合は、次の手順を実行します。

手順

ステップ 1 インターフェイスグループに属していないインターフェイスを選択します。

ステップ 2 インターフェイスを選択し、**[インターフェイス グループ（Interface Group）]** をクリックして **[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウを開きます。

ステップ 3 **[インターフェイス グループの選択（Select Interface Group）]** ドロップダウン リストから **StorageIG** インターフェイス グループを選択します。



ステップ 4 [Clear] をクリックします。

ネットワークおよび VRF の作成と展開

オーバーレイ ネットワークと VRF プロビジョニングの手順は次のとおりです。

1. ファブリックにネットワークと VRF を作成します。

2. ファブリック スイッチでネットワークと VRF を展開します。

Note 展開の説明の後に、オーバーレイネットワークとVRFの展開解除と削除について説明します。最後に、外部ファブリックの作成と、VXLANから外部ファブリックへのファブリック拡張について説明します。

インターフェイス グループの作成とネットワークの接続については、インターフェイスグループ, on page 266 を参照してください。

次のオプションのいずれかを使用して、ネットワークおよびVRF ウィンドウに移動できます。

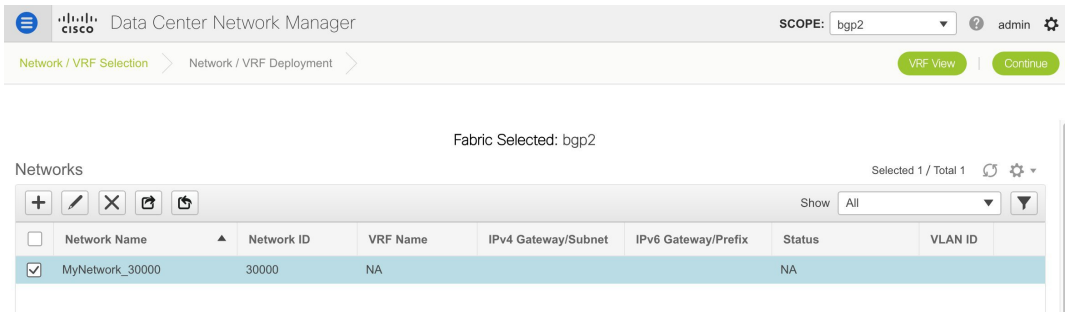
- ホームページから： Cisco DCNM Web UI のランディングページで **[ネットワークと VRF（Networks & VRFs）]** ボタンをクリックします。
- [制御（Control）] メニューから：Cisco DCNM Web UI のホームページから、**[制御（Control）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** を選択して、**[ネットワーク（Networks）]** ウィンドウに移動します。**[制御（Control）] > [ファブリック（Fabrics）] > [VRF]** を選択して、**[VRF]** ウィンドウに移動します。
- ファブリック トポロジ ウィンドウから：ファブリック トポロジ ウィンドウの任意の場所を右クリックします。**[オーバーレイ表示（Overlay View）] > [VRF 表示（VRF View）]** または **[オーバーレイ表示（Overlay View）] > [ネットワーク表示（Network View）]** を選択します。このオプションはスイッチ ファブリック、Easy ファブリック、および MSD ファブリックにのみ適用可能です。

[VRF 表示（VRF View）] または **[ネットワーク表示（Network View）]** ボタンをクリックすると、両方のウィンドウでネットワーク表示と VRF 表示を切り替えることができます。ネットワークまたは VRF ウィンドウを開いているとき、ネットワークまたは VRF を作成する前に、**[範囲（Scope）]** ドロップダウンリストから適切なファブリックを選択していることを確認してください。

ファブリックのネットワークと VRF の表示

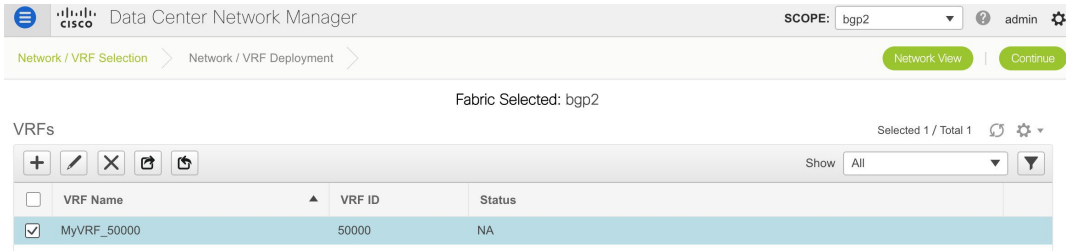
- メイン メニューから **[制御（Control）] > [ネットワーク（Networks）]** をクリックします。

  [ネットワーク（Networks）] 画面が表示されます。（画面の右上にある）[範囲（SCOPE）] ドロップダウンボックスには、DCNM インスタンスによって管理されるすべてのファブリックがアルファベット順に一覧表示されます。[範囲（SCOPE）]から正しいファブリックを選択できます。ファブリックを選択すると、**[ネットワーク（Networks）]** 画面が更新され、選択したファブリックのネットワークが一覧表示されます。



- メイン メニューから **[制御（Control）] > [VRF]** をクリックします。

  VRF 画面が表示されます。（画面の右上にある）SCOPE ドロップダウン ボックスには、DCNM インスタンスによって管理されるすべてのファブリックがアルファベット順に一覧表示されます。[範囲（SCOPE）] から正しいファブリックを選択できます。ファブリックを選択すると、**[VRF]** 画面が更新され、選択したファブリックの VRF が一覧表示されます。



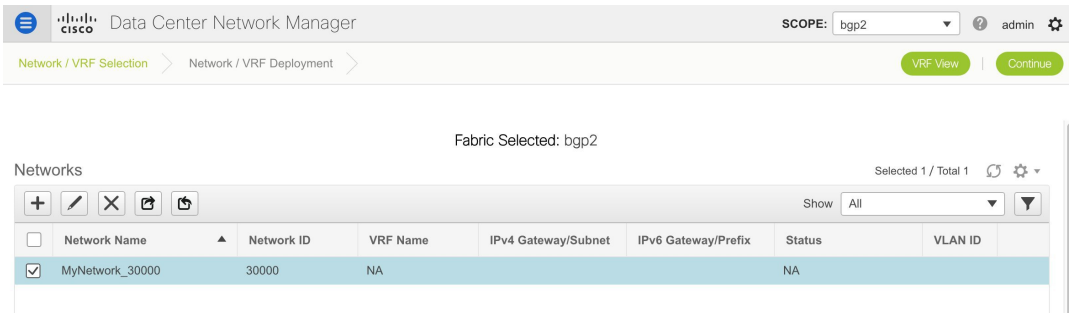
Note **[ネットワーク（Networks）]** または **[VRF]** ウィンドウは、Easy ファブリックまたは MSD ファブリックにのみ適用されます。

スタンドアロン ファブリック向けのネットワークの作成

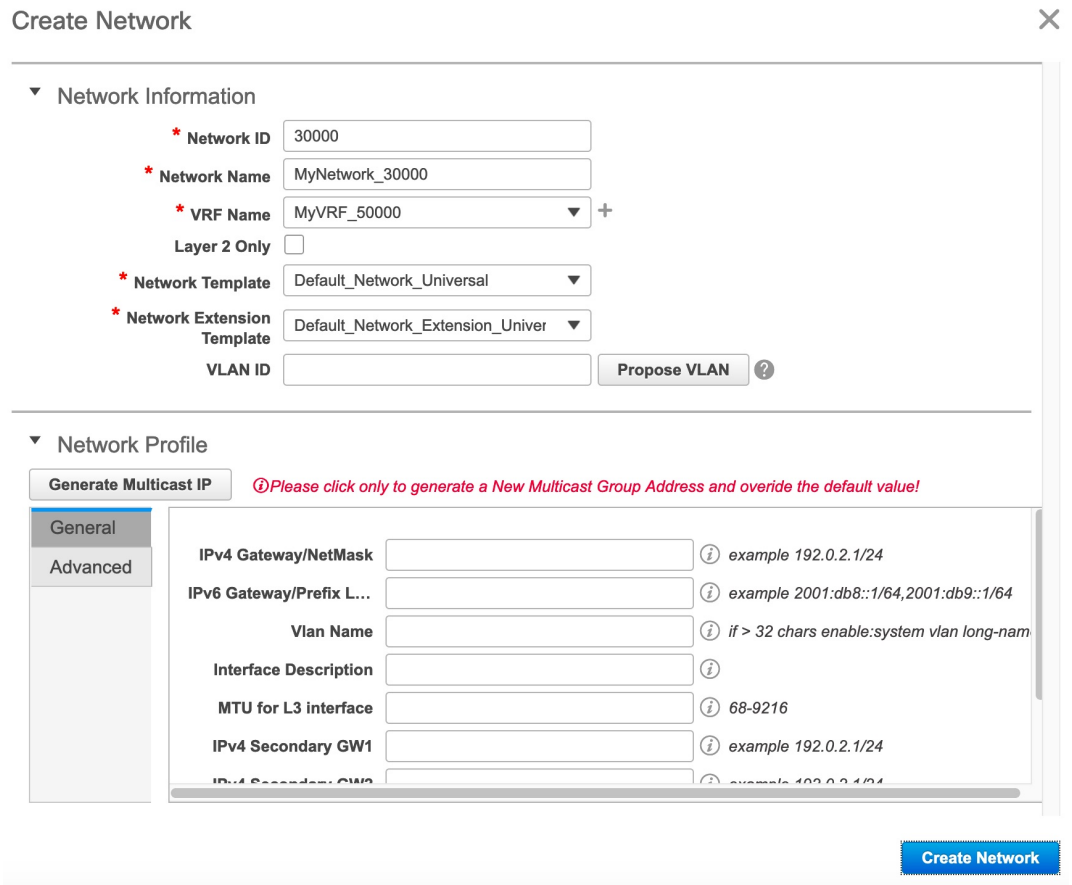
1. **[制御（Control）] > [ネットワーク（Networks）]**（**[ファブリック（Fabrics）]** サブメニューの下）をクリックします。

   [ネットワーク（Networks）] 画面が表示されます。

2. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[ネットワーク（Networks）]** 画面が更新され、選択したファブリックのネットワークが一覧表示されます。



3. 画面の左上部分（**[ネットワーク（Networks）]** の下）にある **[+]** ボタンをクリックして、ネットワークをファブリックに追加します。[ネットワークの作成（Create Network）]画面が表示されます。ほとんどのフィールドは自動入力されます。



この画面のフィールドは次のとおりです。

[ネットワーク ID（Network ID）] と **[ネットワーク名（Network Name）]**：ネットワークのレイヤ 2 VNI と名前を指定します。ネットワーク名には、アンダースコア（_）とハイフン（-）以外の空白や特殊文字は使用できません。対応するレイヤ 3 VNI（または VRF VNI）は、VRF の作成時に生成されます。

[VRF 名（VRF Name）]：仮想ルーティングおよび転送（VRF）を選択できます。

VRF が作成されていない場合、このフィールドは空白になります。新しい VRF を作成する場合は、**[+]** ボタンをクリックします。VRF名には、アンダースコア（_）、ハイフン（-）、およびコロン（:）以外の空白文字や特殊文字は使用できません。

[レイヤ 2 のみ（Layer 2 Only）]：ネットワークがレイヤ 2 のみであるかどうかを指定します。

[ネットワーク テンプレート (Network Template)]：ユニバーサル テンプレートが自動入力されます。これはリーフ スイッチにのみ適用されます。

[ネットワーク拡張テンプレート (Network Extension Template)]：ユニバーサル拡張テンプレートが自動入力されます。これにより、このネットワークを別のファブリックに拡張できます。メソッドは VRF Lite、Multi Site などです。このテンプレートは、境界リーフ スイッチおよび BGW に適用できます。

[VLAN ID]：ネットワークの対応するテナントVLAN IDを指定します。

VLAN ID のデフォルト範囲は 2 から 3967 です。DCNM リリース 11.5(2) 以降、デフォルト値 3967 以上の VLAN 範囲を使用できます。予約済み VLAN 範囲は異なる範囲で設定する必要があります。スイッチ コマンドで「**system vlan <vlan> reserve**」を入力します。スタートアップ構成で構成を保存し、新しい予約済み VLAN 範囲を反映させてスイッチをリロードします。

Cisco DCNM Web UI から、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** の順に選択し、**RM.TOP_DOWN_NETWORK_VLAN.MAX** および **RM.TOP_DOWN_VRF_VLAN.MAX** に値 4094 として入力し、**[変更の適用（Apply Changes）]** をクリックし DCNM を再起動します。DCNM が起動したら、3967 以上の VLAN 値を使用して VRF とネットワークを作成できます。

[ネットワーク プロファイル（Network Profile）] セクションには、*[全般（General）]* タブと *[詳細（Advanced）]* タブがあります。

[General] タブ

IPv4 ゲートウェイ/ネットマスク (IPv4 Gateway/NetMask)]：IPv4 アドレスとサブネットを指定します。

Note ネットワーク テンプレートの IPv4 ゲートウェイと IPv4 セカンダリ GW1 または GW2 フィールドに同じ IP アドレスを構成した場合、DCNM はエラーを表示しないので、この構成は保存できます。

ただし、このネットワーク設定がスイッチにプッシュされると、スイッチは設定を許可しないため、障害が発生します。

[IPv6ゲートウェイ/プレフィックス（IPv6 Gateway/Prefix）]：サブネットの IPv6 アドレスを指定します。

MyNetwork_30000 に属するサーバーおよび別の仮想ネットワークに属するサーバーからの L3 トラフィックを転送するためのエニーキャスト ゲートウェイ IP アドレスを指定しま

す。デフォルトでエニーキャスト ゲートウェイ IP アドレスは、ネットワークが存在するファブリックのすべてのスイッチの MyNetwork_30000 で同じです。

[Vlan 名（Vlan Name）]：VLAN 名を入力します。

[インターフェイスの説明 (Interface Description)]：インターフェイスの説明を指定します。このインターフェイスはスイッチの仮想インターフェイス（SVI）です。

[L3 インターフェイスの MTU（MTU for L3 interface）]：レイヤ 3 インターフェイスの MTU を入力します。

IPv4セカンダリGW1：追加のサブネットのゲートウェイIPアドレスを入力します。

IPv4セカンダリGW2：追加のサブネットのゲートウェイIPアドレスを入力します。

[詳細（Advanced）]タブ：オプションとして、**[詳細（Advanced）]**タブをクリックしてプロファイルの詳細設定を指定できます。

[ARP 抑制 (ARP Suppression)]：ARP 抑制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。

[入力レプリケーション（Ingress Replication）]：レプリケーション モードが入力レプリケーションの場合、チェックボックスはオンになります。

Note 入力レプリケーションは、[詳細（Advanced）]タブの読み取り専用オプションです。ファブリック設定を変更すると、このフィールドは更新されます。

[マルチキャスト グループ アドレス（Multicast Group Address）]：ネットワークのマルチキャスト IP アドレスが自動入力されます。

マルチキャストグループアドレスは、ファブリックインスタンスごとの変数です。サポートされるアンダーレイ マルチキャスト グループの数は 128 に限られます。すべてのネットワークがすべてのスイッチに展開されている場合は、L2 VNI またはネットワークごとに異なるマルチキャストグループを使用する必要はありません。したがって、ファブリック内のすべてのネットワークのマルチキャストグループは同じままです。新しいマルチキャスト グループ アドレスが必要な場合は、**[マルチキャスト IP の生成 (Generate Multicast IP)]**ボタンをクリックして生成できます。

DHCPv4サーバ1：最初のDHCPサーバのDHCPリレーIPアドレスを入力します。

DHCPv4サーバ2：次のDHCPサーバのDHCPリレーIPアドレスを入力します。

[DHCPv4 サーバー VRF（DHCPv4 Server VRF）]：DHCP サーバーの VRF ID を入力します。

Loopback ID for DHCP Relay interface（Min：0、Max：1023）：DHCPリレーインターフェイスのループバックIDを指定します。

[ルーティング タグ（Routing Tag）]：ルーティングタグは自動入力されます。このタグは、各ゲートウェイの IP アドレス プレフィックスに関連付けられます。

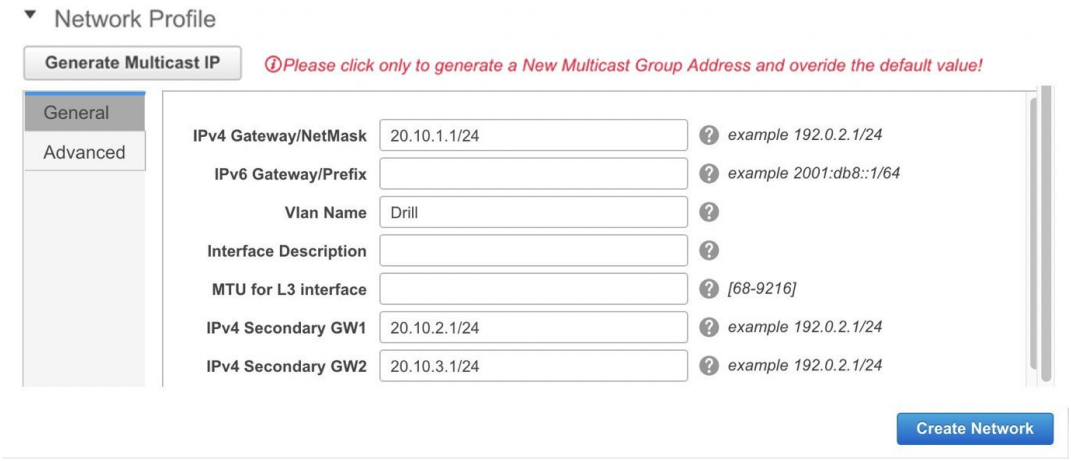
[TRM が有効（TRM enable）]：TRM を有効にするには、このチェックボックスをオンにします。

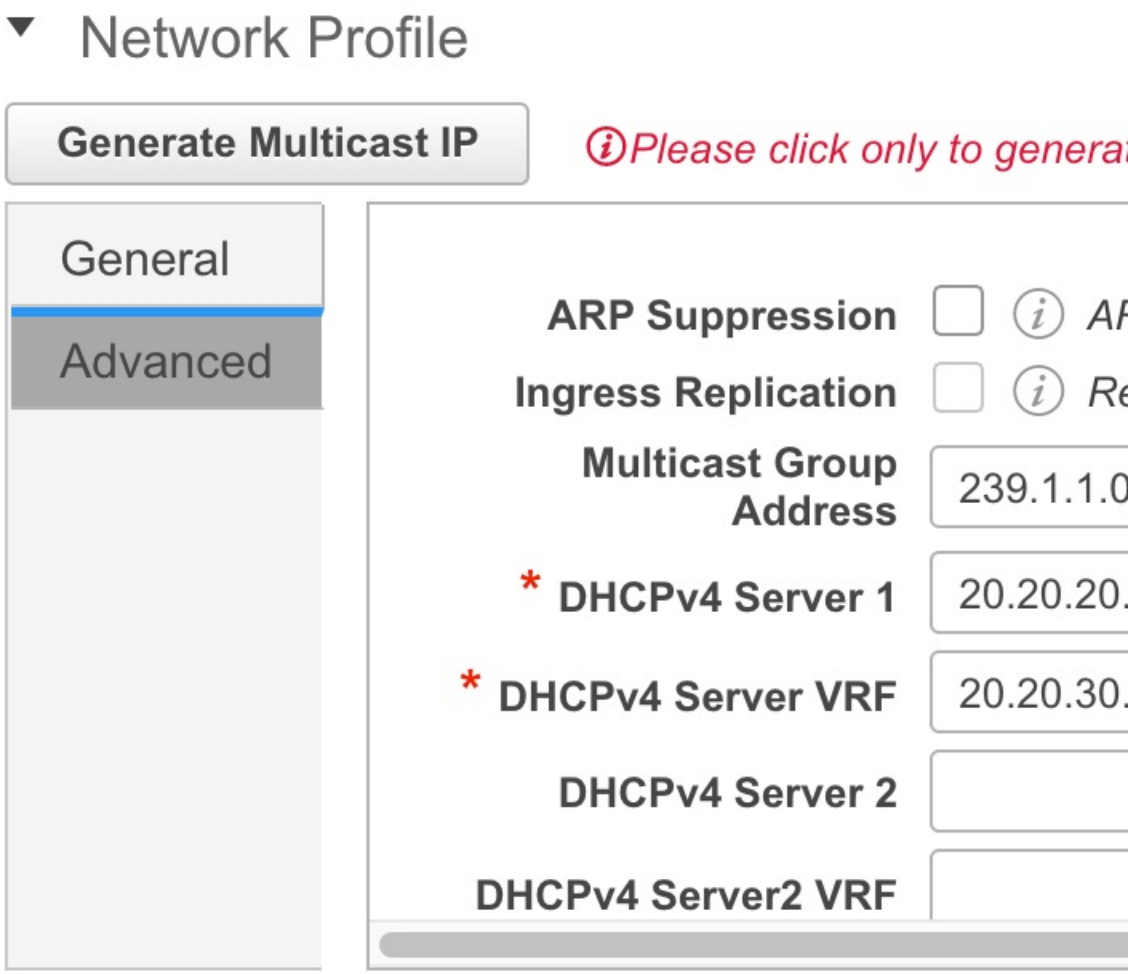
詳細については、テナント ルーテッド マルチキャストの概要, on page 176を参照してください。

[L2 VNI ルート ターゲットの両方が有効（L2 VNI Route Target Both Enable）]：すべての L2 仮想ネットワークのルート ターゲットの自動インポートとエクスポートを有効にするには、このチェックボックスをオンにします。

[境界でのL3ゲートウェイの有効化（Enable L3 Gateway on Border）]：チェックボックスをオンにすると、境界スイッチでレイヤ3ゲートウェイが有効になります。

[ネットワークの作成（Create Network）] 画面のサンプルを以下に示します。





4. [ネットワークの作成（Create Network）]をクリックします。画面の右下に、ネットワークが作成されたことを示すメッセージが表示されます。

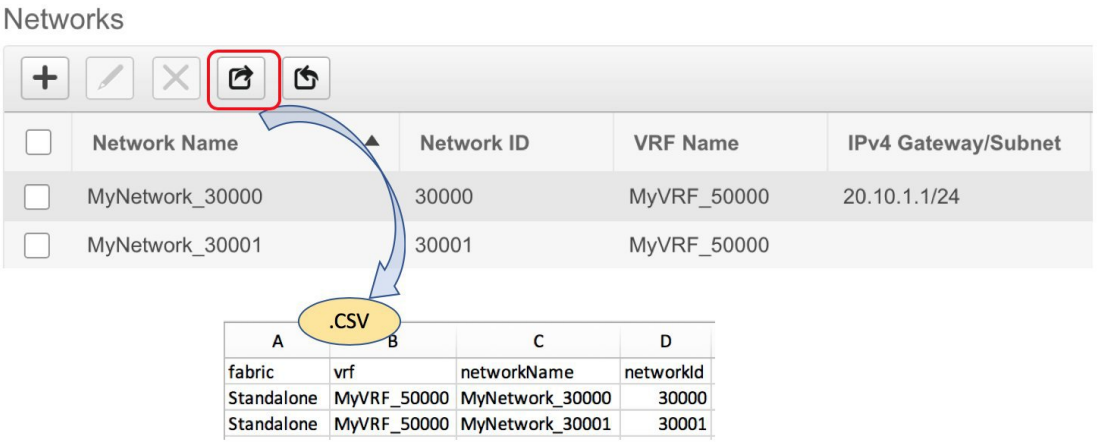
   新しいネットワークは、表示される **[ネットワーク (Networks)]** ページに表示されます。

ネットワークは作成されていますが、まだスイッチに展開されていないため、ステータスは *NA* です。これでネットワークは作成されました。必要であればさらにネットワークを作成し、ファブリック内のデバイスにネットワークを展開できます。

ネットワーク情報のエクスポートとインポート

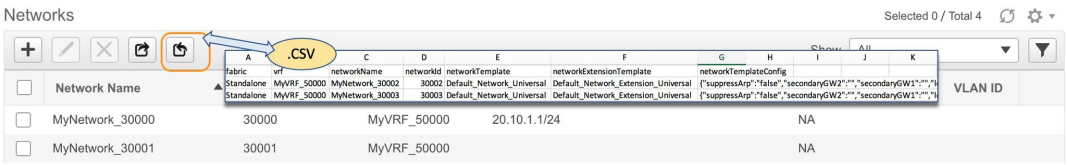
ネットワーク接続についての情報は、.CSV ファイルにエクスポートすることが可能です。エクスポートされたファイルには、所属するファブリック、関連付けられている VRF、ネットワークの作成に使用されたネットワーク テンプレート、およびネットワークの作成時に保存したその他のすべての設定の詳細が含まれます。

[ネットワーク（Networks）]画面で、[エクスポート（Export）]アイコンをクリックして、ネットワーク情報を .CSV ファイルとしてエクスポートします。



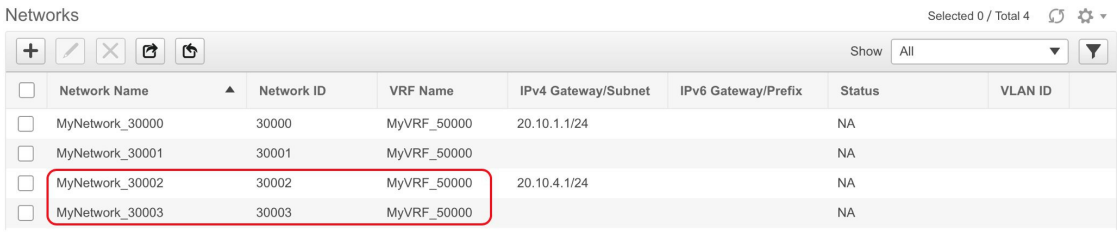
エクスポートされた .CSV ファイルは参照用に使用することや、新しいネットワークを作成するためのテンプレートとして使用することができます。ネットワークをインポートするには、次の手順を実行します。

1. .CSV ファイル内の新しいレコードをアップデートします。[networkTemplateConfig] フィールドに JSON オブジェクトが含まれていることを確認します。画面の右下にあるメッセージ部に、エラーメッセージと成功メッセージが表示されます。このスクリーンショットは、インポートされる 2 つの新しいネットワークを示しています。



2. [ネットワーク（Networks）]画面で、[インポート（Import）]アイコンをクリックし、.CSV ファイルを DCNM にインポートします。

インポートされたネットワークが[ネットワーク（Networks）]画面に表示されていることがわかります。



スタンドアロン ファブリック向けのネットワークの編集

Cisco DCNM Web UI からスタンドアロン ファブリック向けのネットワークを編集するには、以下の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ネットワーク（Networks）]** をクリックします。

[ネットワーク（Networks）] ウィンドウが表示されます。

ステップ 2 **[範囲（SCOPE）]** ドロップダウンリストから [ファブリック（Fabric）] を選択します。

[ネットワーク（Networks）] ウィンドウが更新され、ファブリック内のネットワークが一覧表示されます。

ステップ 3 ネットワークを選択します。

ステップ 4 [編集（Edit）] アイコンをクリックします。

[ネットワークの編集（Edit Network）] ウィンドウが表示されます。

ステップ 5 必要に応じて、**[ネットワーク プロファイル（Network Profile）]** エリアの **[全般（General）]** タブと **[詳細（Advanced）]** タブのフィールドを更新します。

Note ネットワーク名を編集できます。編集したネットワーク名は、**[ネットワーク（Networks）]** ウィンドウの **[ネットワーク名（Network Name）]** 列に表示されます。ネットワークの作成時に使用した元の名前が **[ディスプレイ名（Display Name）]** 列に表示されます。**[ネットワーク（Networks）]** ウィンドウの **[ディスプレイ名（Display Name）]** 列から元のネットワーク名を表示するには、**[設定（Settings）]** をクリックします。**[列（Columns）]** ドロップダウンリストを展開し、**[ディスプレイ名（Display Name）]** オプションを選択します。[閉じる（Close）] をクリックします。ネットワーク トポロジ表示で元のネットワーク名を表示することもできます。

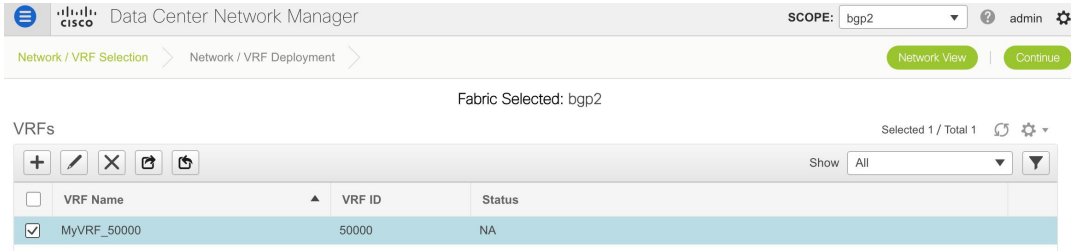
ステップ 6 ウィンドウの右下の **[保存（Save）]** ボタンをクリックして、アップデートを保存します。

スタンドアロン ファブリック向けの VRF の作成

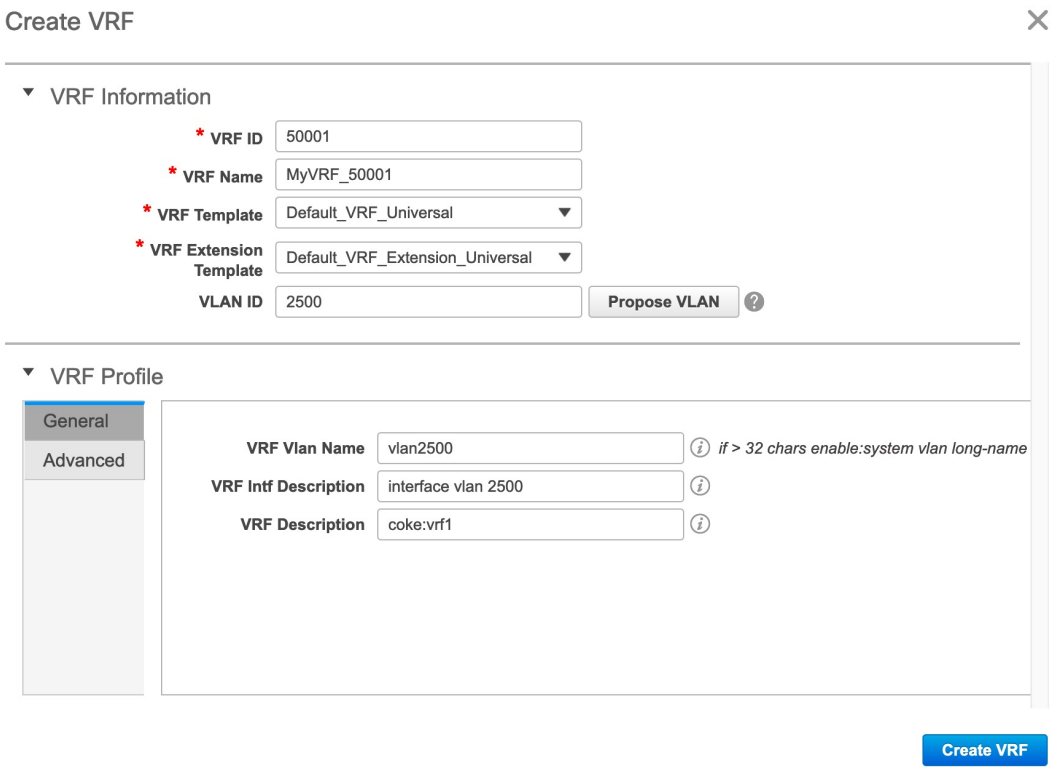
1. **[制御（Control）] > [VRF]（[ファブリック（Fabrics）]** サブメニューの下）をクリックします。

   [VRF] 画面が表示されます。

2. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[VRF]** 画面が更新され、選択したファブリックの VRF が一覧表示されます。



3. **[+]** ボタンをクリックして、スタンドアロン ファブリックに VRF を追加します。[VRF の作成 (Create VRF)] 画面が表示されます。ほとんどのフィールドは自動入力されます。



この画面のフィールドは次のとおりです。

[VRF ID] と **[VRF 名（VRF Name）]**：VRF の ID と名前です。

Note 使いやすいように、ネットワークの作成時に VRF 作成オプションも使用できます。

[VRF テンプレート（VRF Template）]：このテンプレートは VRF の作成に適用でき、リーフスイッチにのみ適用できます。

[VRF 拡張テンプレート（VRF Extension Template）]：テンプレートは、VRF を他のファブリックに拡張する場合に適用され、ボーダー デバイスに適用されます。

[VRF プロファイル（VRF Profile）] セクションのフィールドに入力します。

[全般（General）] タブ：VRF に関連付けられた VLAN の VLAN ID、対応するレイヤ 3 仮想インターフェイス、および VRF ID を入力します。

VLAN ID のデフォルト範囲は 2 から 3967 です。DCNM リリース 11.5(2) 以降、デフォルト値 3967 以上の VLAN 範囲を使用できます。予約済み VLAN 範囲は異なる範囲で設定する必要があります。スイッチ コマンドで「**system vlan <vlan> reserve**」を入力します。スタートアップ構成で構成を保存し、新しい予約済み VLAN 範囲を反映させてスイッチをリロードします。

Cisco DCNM Web UI から、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** の順に選択し、**[RM.TOP_DOWN_NETWORK_VLAN.MAX]** および **[RM.TOP_DOWN_VRF_VLAN.MAX]** に値 4094 として入力し、**[変更の適用（Apply Changes）]** をクリックし DCNM を再起動します。DCNM が起動したら、3967 以上の VLAN 値を使用して VRF とネットワークを作成できます。

[詳細（Advanced）] タブ：タブのフィールドは自動入力されます。

[VRF インターフェイス MTU（VRF Intf MTU）]：VRFインターフェイスMTUを指定します。

[ルーティング タグ（Routing Tag）]：VLAN が複数のサブネットに関連付けられている場合、このタグは各サブネットの IP プレフィックスに関連付けられます。このルーティング タグは、オーバーレイ ネットワークの作成にも関連付けられています。

[再配布直接ルート マップ（Redistribute Direct Route Map）]：VRF でルートを再配布するためのルート マップ名を指定します。

[最大 BGP パス（Max BGP Paths）] および **[最大 iBGP パス（Max iBGP Paths）**：最大 BGP および iBGP パスを指定します。

[TRM の有効（TRM Enable）]：TRM 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。

TRM を有効にする場合は、RP アドレスとアンダーレイ マルチキャスト アドレスを入力する必要があります。

詳細については、テナント ルーテッド マルチキャストの概要, on page 176を参照してください。

[RP が外部（Is RP External）]：ファブリックに対して RP が外部である場合、このチェックボックスを有効にします。このフィールドのチェックがオフの場合、RP はすべての VTEP に分散されます。

RP アドレス：RP の IP アドレスを指定します。

RP ループバック ID：**RP が外部** が有効化されていない場合、RP のループバック ID を指定します。

[アンダーレイ マルチキャスト アドレス（Underlay Multicast Address）]：VRF に関連付けられたマルチキャスト アドレスを指定します。マルチキャスト アドレスは、ファブリック アンダーレイでマルチキャスト トラフィックを転送するために使用します。

Note ファブリック設定画面の **[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]** フィールドのマルチキャスト アドレスは、このフィールドに自動的に入力されます。この VRF に別のマルチキャスト グループ アドレスを使用する必要がある場合は、このフィールドを上書きできます。

[オーバーレイ マルチキャスト グループ（Overlay Multicast Groups）]：指定した RP のマルチキャスト グループ サブネットを指定します。値は「ip pim rp-address」コマンドのグループ範囲です。フィールドが空の場合、デフォルトで 224.0.0.0/24 が使用されます。

[IPv6 リンク ローカル オプションの有効化（Enable IPv6 link-local Option）]：このチェックボックスをオンにすると、VRF SVI で IPv6 リンク ローカル オプションが有効になります。このチェックボックスをオフにすると、IPv6 転送が有効になります。

[TRM BGW マルチサイトの有効化（Enable TRM BGW MSite）]：チェックボックスをオンにして、ボーダー ゲートウェイ マルチサイトで TRM を有効にします。

[ホスト ルートのアドバタイズ（Advertise Host Routes）]：エッジ ルータへの /32 および /128 ルートのアドバタイズメントを制御するには、このチェックボックスをオンにします。

[デフォルトルートのアドバタイズ（Advertise Default Route）]：このチェックボックスをオンにすると、デフォルトルートのアドバタイズメントが内部的に制御されます。

異なる VXLAN ファブリック内（両方のファブリックにサブネットが存在する）のエンドホスト間のサブネット間通信を許可するには、関連付けられている VRF の **デフォルト ルートのアドバタイズ**機能を無効にする（**[デフォルト ルートのアドバタイズ（Advertise Default Route）]** チェックボックスをオフにする）必要があります。これにより、両方のファブリックでホストの /32 ルートが表示されます。たとえば、ファブリック 1 のホスト 1（VNI 30000、VRF 50001）は、ホスト ルートが両方のファブリックに存在する場合にのみ、ファブリック 2 のホスト 2（VNI 30001、VRF 50001）にトラフィックを送信できます。サブネットが 1 つのファブリックにのみ存在する場合は、サブネット間通信にはデフォルト ルートだけで十分です。

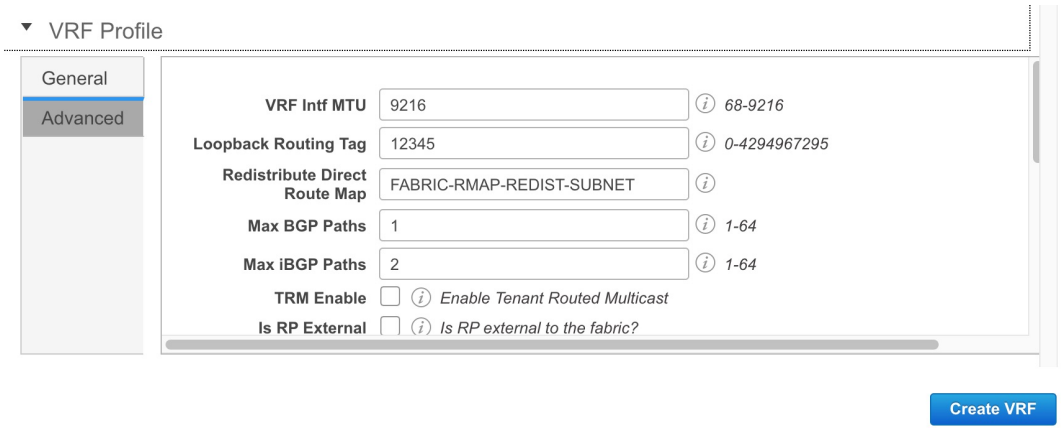
[静的 0/0 ルートの構成（Config Static 0/0 Route）]：静的デフォルトルートの構成を制御するには、このチェックボックスをオンにします。

[BGP ネイバーパスワード（BGP Neighbor Password）]：VRF Lite BGP のネイバー パスワードを指定します。

[BGP パスワード キー暗号化タイプ（BGP Password Key Encryption Type）]：このドロップダウン リストから暗号化タイプを選択します。

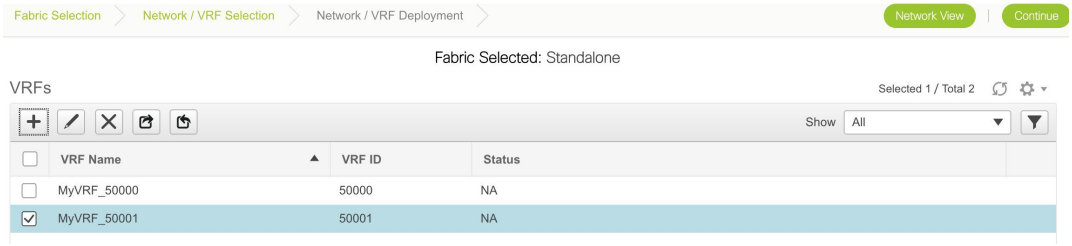
VRF の作成画面のサンプル スクリーンショット：

[Advanced] タブ：



4. **[VRF の作成（Create VRF）]** をクリックします。

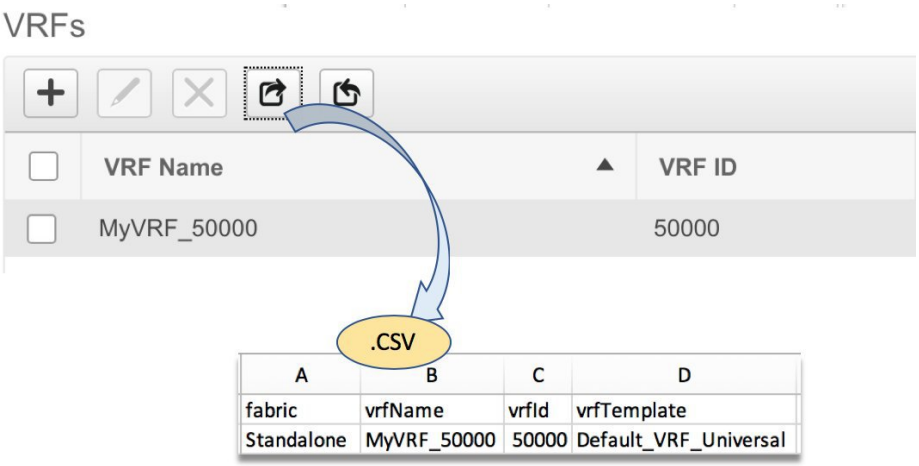
   MyVRF_50001 VRF が作成され、VRFs ページに表示されます。



[VRF 情報のエクスポートとインポート（Export and Import VRF Information）]

VRF 接続についての情報は、.CSV ファイルにエクスポートすることが可能です。エクスポートされたファイルには、含まれるファブリック、VRF 作成に使用されたテンプレート、および VRF の作成時に保存したその他のすべての構成の詳細を含む、各 VRF に関連する情報が格納されています。

[VRF] 画面で、[エクスポート（Export）] アイコンをクリックして、VRF 情報を .CSV ファイルとしてエクスポートします。



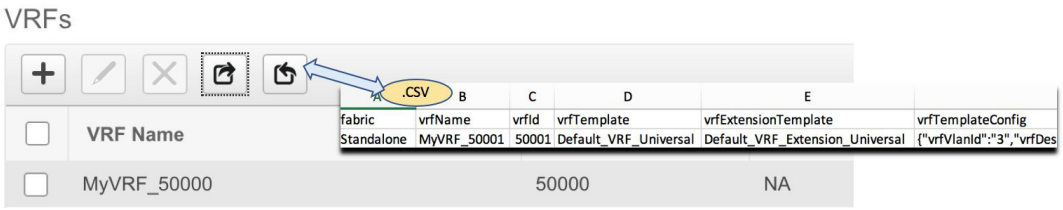
エクスポートされた .CSV ファイルは参照用に使用することや、新しい VRF を作成するためのテンプレートとして使用することができます。VRF をインポートするには、次の手順を実行します。

1. .CSV ファイル内の新しいレコードをアップデートします。**[vrfTemplateConfig]** フィールドに JSON オブジェクトが含まれていることを確認します。
2. [VRF] 画面で、**[インポート（Import）]** アイコンをクリックし、.CSV ファイルを DCNM にインポートします。

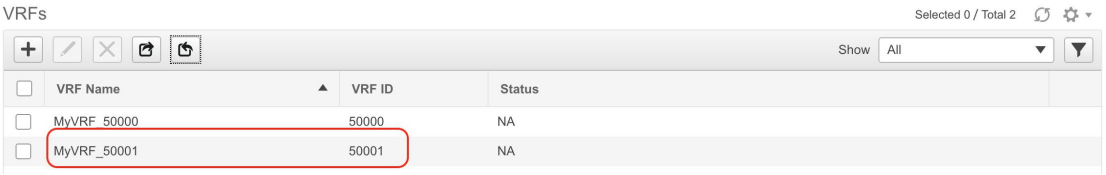
   画面の右下にあるメッセージ部に、エラーメッセージと成功メッセージが表示されます。このスクリーンショットは、インポートされる新しい VRF を示しています。

Note [VRF] ウィンドウの **[インポート（Import）]** オプションまたは DCNM API を使用して VRF を作成すると、次のエラーが表示される場合があります。「インスタンス名が指定されていません。」

このエラーは、タグ付けの問題が原因です。このエラーを削除するには、DCNM Web UI で VRF を編集してから展開します。

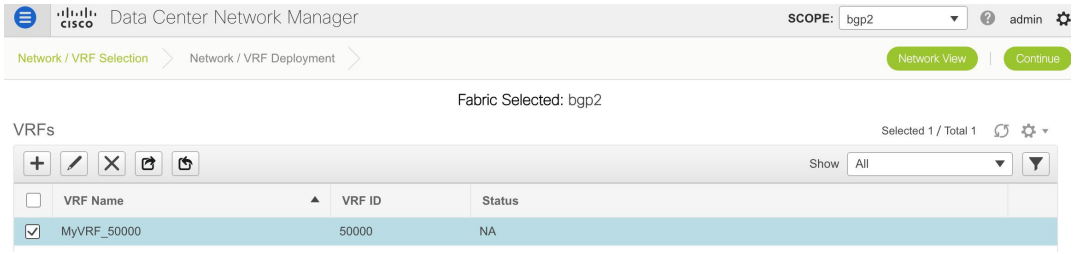


インポートされた VRF が [VRF] 画面に表示されていることがわかります。

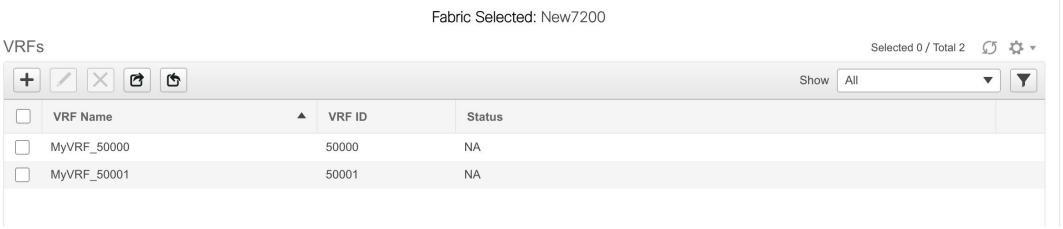


スタンドアロン ファブリック向けの VRF の編集

1. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[VRF（VRFs）]** 画面が更新され、選択したファブリックの VRF が一覧表示されます。



2. **[ファブリックの選択（Select a Fabric）]** ドロップダウンリストから *[スタンドアロン（Standalone）]* を選択し、画面の右上にある **[続行（Continue）]** をクリックします。[ネットワーク（Networks）] ページが表示されます。
3. 画面右上の **[VRF の表示（VRF View）]** をクリックします。VRF ページが表示されます。



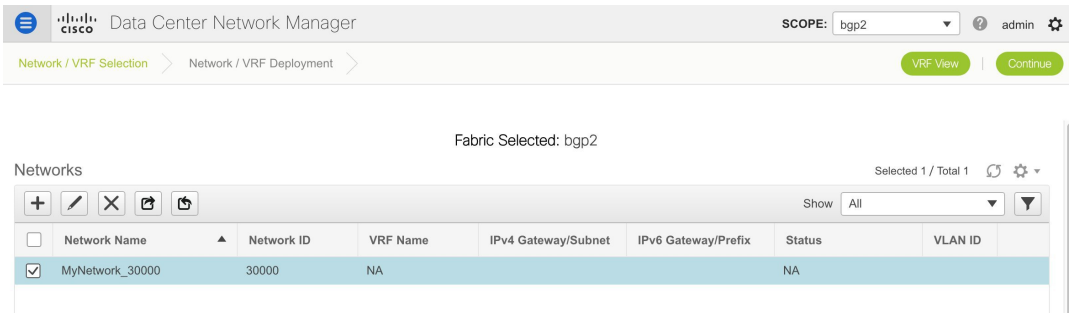
4. **[VRF]** を選択し、画面の左上にある **[編集（Edit）]** オプションをクリックします。**[VRF の編集（Edit VRF）]** 画面が表示されます。
5. 必要に応じて、**[VRF プロファイル（VRF Profile）]** セクションの **[全般（General）]** タブと **[詳細（Advanced）]** タブのフィールドを更新します。
6. 画面の右下の **[保存（Save）]** ボタンをクリックして、アップデートを保存します。

スタンドアロンおよび MSD ファブリック向けネットワークの展開

開始の前に：ファブリックのネットワークが作成されていることを確認します。

1. **[制御（Control）]>[ネットワーク（Networks）]**（**[ファブリック（Fabrics）]** サブメニューの下）をクリックします。

   [ネットワーク（Networks）] 画面が表示されます。
2. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[ネットワーク（Networks）]** 画面が更新され、選択したファブリックのネットワークが一覧表示されます。



3. 展開するネットワークを選択します。この場合、両方のネットワークの横にあるチェックボックスをオンにして、画面の右上にある **[続行（Continue）]** をクリックします。

   [ネットワークの展開（Network Deployment）] ページが表示されます。このページでは、スタンドアロン ファブリックのネットワーク トポロジを確認できます。

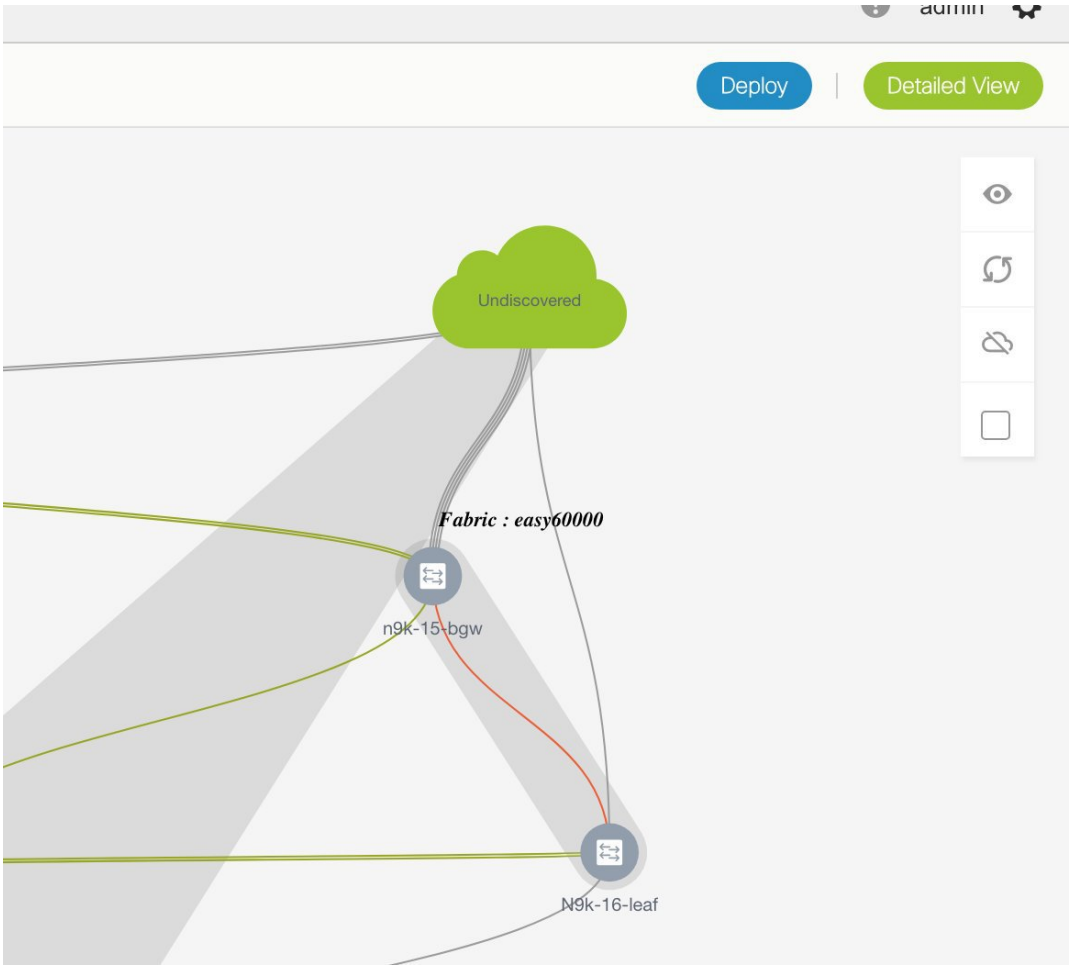
複数のスイッチにネットワークを同時に展開できます。選択したデバイスは、同じロール（リーフ、ボーダーゲートウェイなど）を持つ必要があります。

Note MSD ファブリックでは、すべてのメンバー ファブリックがこの画面から表示されます。

画面の右下に、展開のさまざまな段階を表すカラー コードが表示されます。それに応じてスイッチ アイコンの色が変わります。保留中 の状態は青色、プロビジョニングが進行中の場合の 進行中 は黄色、正常に展開された場合は緑色などです。 DCNM 11.3(1) 以降、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、**[保存と展開（Save & Deploy）]** をクリックしてスイッチの状態を再計算できます。

オーバーレイ ネットワーク（/VRF）のプロビジョニング ステータスは、コンテキスト固有です。これは、プロビジョニング用に選択したネットワークとトポロジ内の関連するスイッチの組み合わせです。この例では、ネットワーク *MyNetwork_30000* および *MyNetwork_30001* が、このファブリック内のどのスイッチにもまだ展開されていないことを意味します。

[未検出のクラウド（Undiscovered cloud）] の表示：この画面に **[未検出（Undiscovered）]** クラウドを表示（または非表示）するには、画面の右上にある垂直パネルのクラウドアイコンをクリックします。アイコンをクリックすると、**[未検出（Undiscovered）]** クラウドと、選択したファブリック トポロジへのリンクは表示されません。**[未検出（Undiscovered）]** クラウドを表示するためにアイコンを再度クリックします。



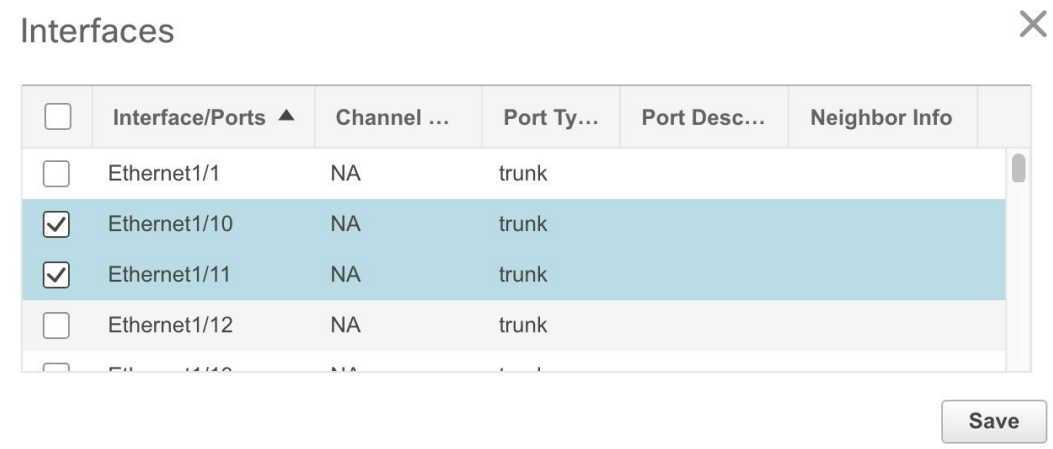
画面上でマウスの左ボタンをクリックし、希望する方向に移動することにより、画面上でトポロジを移動できます。カーソル ローラーを移動することで、スイッチ アイコンを比例して拡大または縮小できます。タッチパッドで対応する代替手段を使用することもできます。

4. **[インターフェイス（Interfaces）]** 列で **[...]** をクリックします。

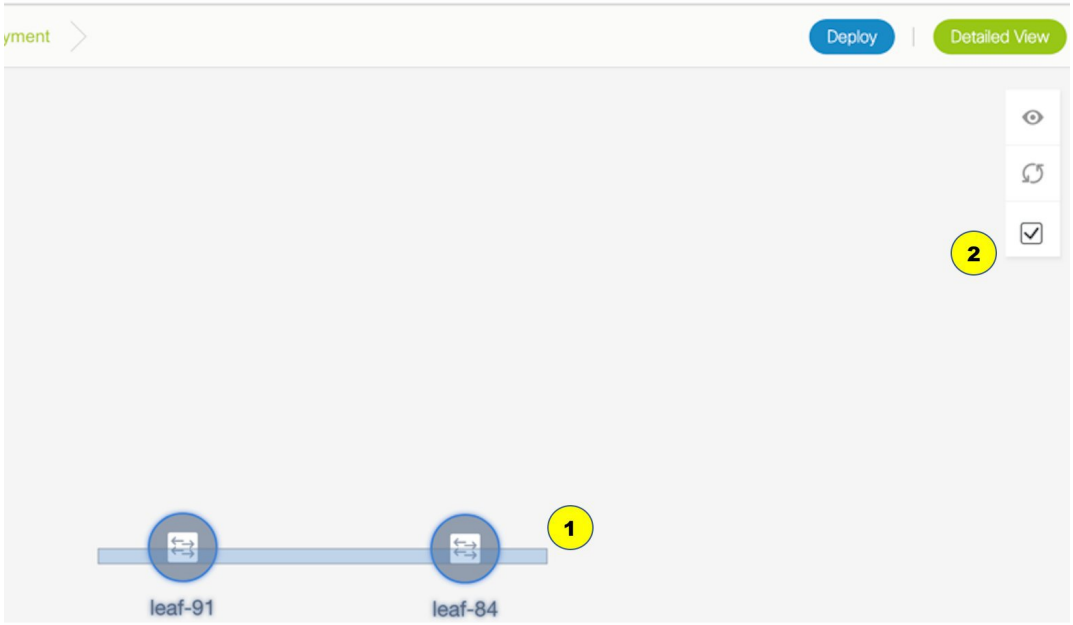
   [インターフェイス（Interfaces）] ボックスが開きます。インターフェイスまたはポートチャネルが一覧表示されます。インターフェイス/ポートチャネルを選択して、選択したネットワークに関連付けることができます。インターフェイスごとに、ポートタイプと説明、チャネル番号、および接続されたネイバーインターフェイスの詳細が表示されます。

   Cisco DCNM リリース 11.5(1) 以降、**[インターフェイス（Interfaces）]** ウィンドウには、インターフェイス グループの一部であるインターフェイスが表示されません。具体的には、トランク ポート、アクセス ポート、および dot1q トンネル ポートです。

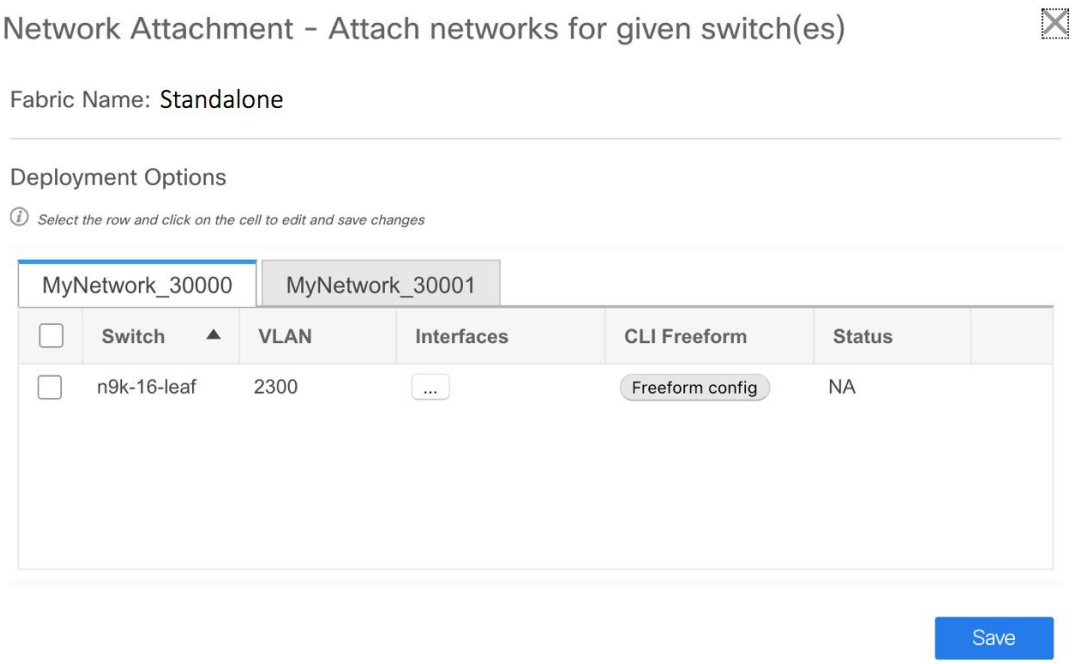
   スイッチへのネットワーク接続を実行しようとしたときに、インターフェイスがインターフェイス グループの一部である場合、適切なエラーが表示されます。



5. スイッチをダブルクリックして、スイッチにネットワークを展開します。複数のスイッチにネットワークを展開するには、画面の右上にあるパネルから [複数選択（Multi-Select）] をクリックし（トポロジが静的な状態に凍結します）、スイッチ間でカーソルをドラッグします。



すぐに [ネットワーク接続（Network Attachment）] ダイアログ ボックスが表示されます。



タブは、展開されている各ネットワークを表します（最初のネットワークがデフォルトで表示されます）。各ネットワーク タブに、スイッチが表示されます。各行はスイッチを表します。

[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、すべてのスイッチを選択します。ネットワークは、スイッチでプロビジョニングする準備ができています。

VLAN：必要に応じて VLAN ID を更新します。

VLAN ID を更新して、ネットワークの展開プロセスを完了しても、古い VLAN は自動的に削除されません。プロセスを完了するには、ファブリック トポロジ画面に移動し（**[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** をクリックし、対応するファブリック ボックス内をクリックして画面に移動します）、[保存して展開（Save and Deploy）] オプションを使用する必要があります。

特定のネットワークの VLAN ID を更新する場合、元の VLAN ID は接続されたトランク インターフェイスから自動的に削除されません。古いまたは元の VLAN ID を削除するには、ファブリック ビルダのファブリック内から **[保存して展開（Save and Deploy）] + [構成展開（Config Deploy）** 操作を実行する必要があります。このためには、ファブリック トポロジ画面に移動し（**[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** をクリックし、対応するファブリック ボックス内をクリックして画面に移動します）、**[保存して展開**（Save and Deploy）] 操作を実行する必要があります。構成コンプライアンスによって必要な構成が削除されていることを確認してから、**[構成の展開（Deploy Config）]** 操作を実行して構成を削除します。

インターフェイス：列の [...] をクリックして、選択したネットワークに関連付けられたインターフェイスを追加します。

VLAN からトランク ポートへのマッピング：選択したトランク ポートには、ポートで許可された VLAN として VLAN が含まれます。

VLAN から vPC ドメインへのマッピング：VLAN を vPC ドメインのポートチャネルに関連付ける場合は、インターフェイスのリストからポートチャネルを追加します。vPC ポートチャネルには、許可された VLAN として VLAN が含まれています。

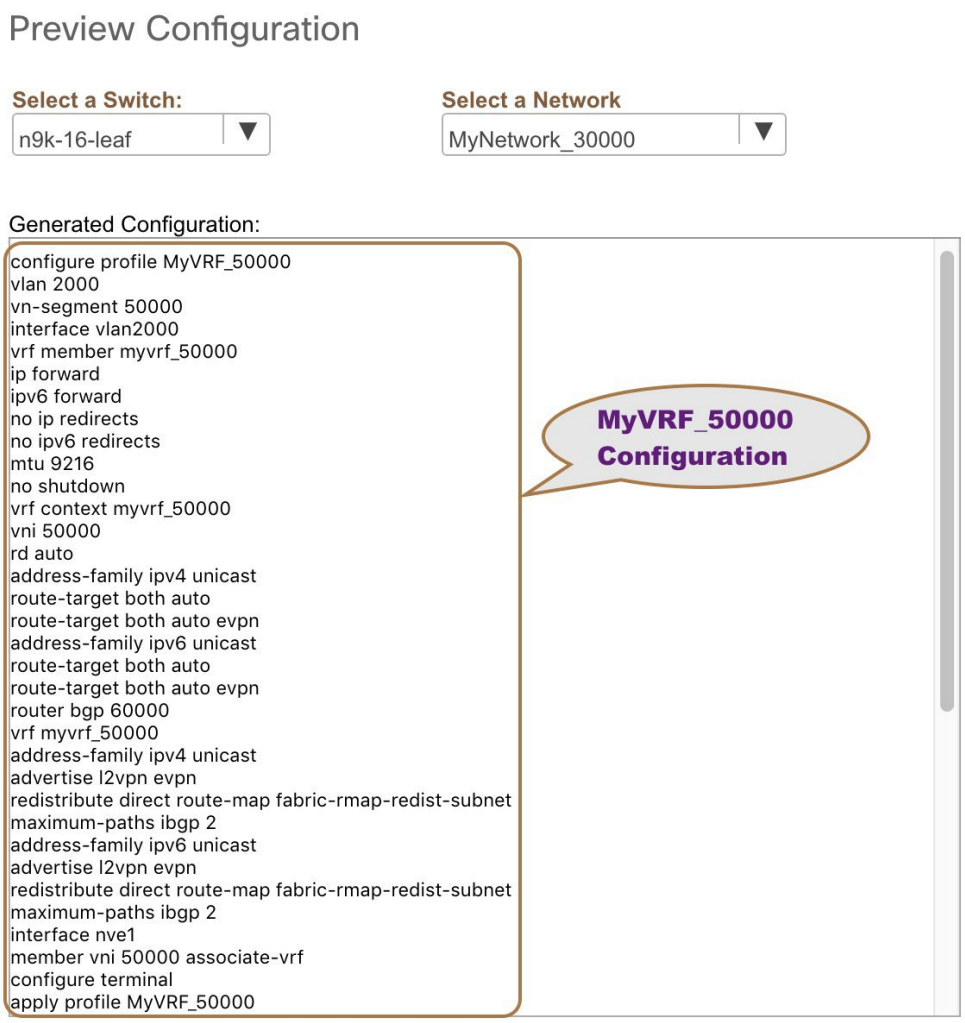
自由形式構成：[自由形式構成（Freeform config）]をクリックして、スイッチで追加の構成を有効にします。構成が保存されると、[自由形式構成（Freeform config）]ボタンが強調表示されます。

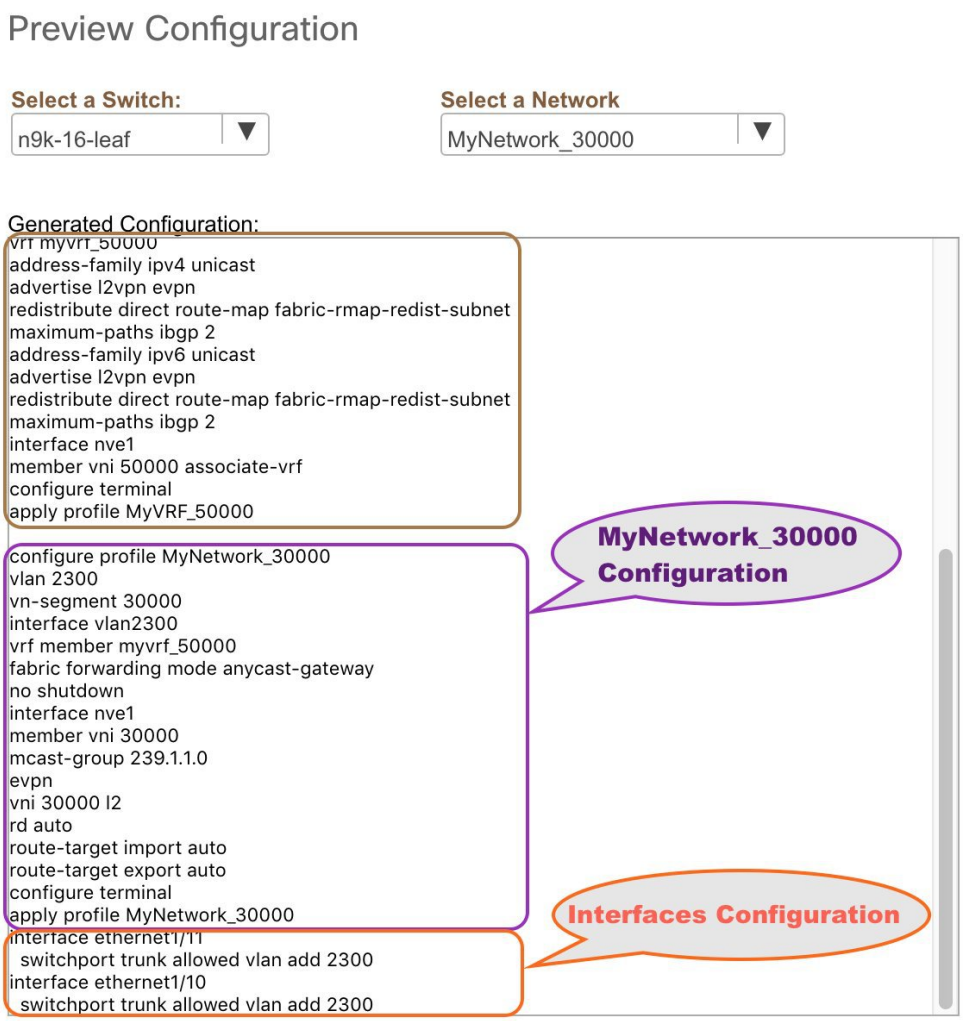
6. 他のネットワーク タブを選択し、同じ選択を行います。
7. **[保存（Save）]**（画面の右下部分）をクリックして、構成を保存します。

Note インターフェイスの追加と削除は、[スイッチの展開（Switches Deploy）]画面の**[インターフェイス（Interfaces）]**列に表示されます。インターフェイス関連の更新（トランク ポートの追加または削除など）はスイッチにプロビジョニングされますが、正しい構成はプレビュー画面に反映されません。トランクまたはアクセス ポートを追加または削除すると、プレビューには、そのネットワーク下のインターフェイスの構成の追加または削除が表示されます。

[トポロジ（Topology）] ウィンドウが再び表示されます。画面の右上にある垂直パネルの *[更新（Refresh）]* をクリックします。スイッチ アイコンの青色は、展開が保留中であることを示します。 DCNM 11.3(1) 以降、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、**[保存と展開（Save & Deploy）]** をクリックしてスイッチの状態を再計算できます。

8. *[プレビュー（Preview）]*（[複数選択（Multi-Select）] オプションの上にある目のアイコン）をクリックして、構成をプレビューします。*MyNetwork_30000* と *MyNetwork_30001* は VRF *50000* のネットワークであるため、構成には VRF 構成とそれに続くネットワーク構成が含まれます。


Preview Configuration
Select a Switch:
n9k-16-leaf
Select a Network
MyNetwork_30000
Generated Configuration:
configure profile MyVRF_50000
vlan 2000
vn-segment 50000
interface vlan2000
vrf member myvrf_50000
ip forward
ipv6 forward
no ip redirects
no ipv6 redirects
mtu 9216
no shutdown
vrf context myvrf_50000
vni 50000
rd auto
address-family ipv4 unicast
route-target both auto
route-target both auto evpn
address-family ipv6 unicast
route-target both auto
route-target both auto evpn
router bgp 60000
vrf myvrf_50000
address-family ipv4 unicast
advertise l2vpn evpn
redistribute direct route-map fabric-rmap-redist-subnet
maximum-paths ibgp 2
address-family ipv6 unicast
advertise l2vpn evpn
redistribute direct route-map fabric-rmap-redist-subnet
maximum-paths ibgp 2
interface nve1
member vni 50000 associate-vrf
configure terminal
apply profile MyVRF_50000
MyVRF_50000
Configuration

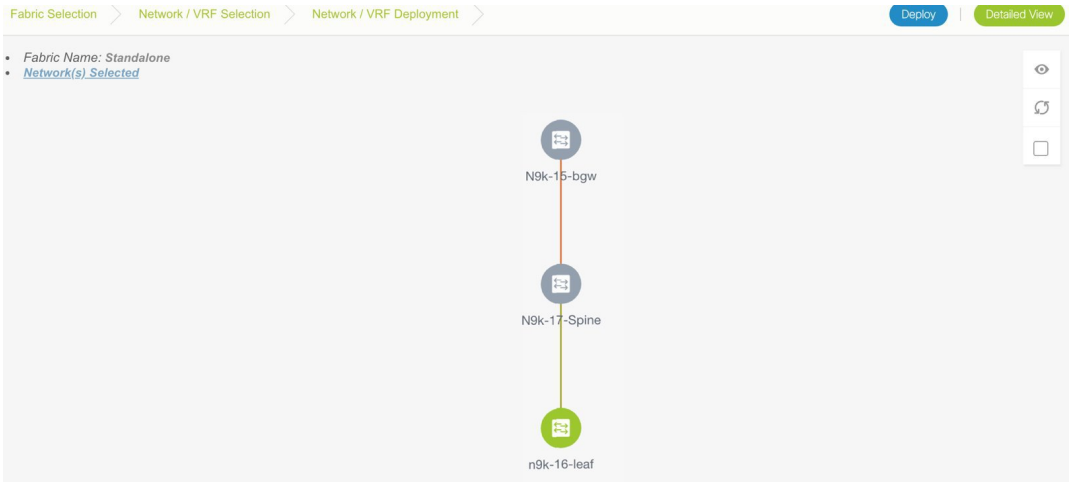


プレビュー画面では、画面上部の **[スイッチの選択（Select a switch）]** および **[ネットワークの選択（Select a network）]** ドロップダウンボックスから選択して、他のネットワーク構成を表示できます。

構成を確認したら、画面を閉じます。[トポロジ（Topology）] 画面が再び表示されます。

9. 画面の右上にある **[展開（Deploy）]** をクリックします。スイッチアイコンの色が黄色に変わり、画面の右下に展開が進行中であることを示すメッセージが表示されます。ネットワークの展開が完了すると、スイッチアイコンの色が緑に変わり、展開が成功したことを示します。

Note **[展開（Deploy）]** をクリックして、展開する必要のある構成差分がない場合は、**[展開保留中のスイッチなし（No switches PENDING for deployment）]** と示すポップアップ ウィンドウが表示されます。



Note スイッチのステータスは、選択したネットワークまたは次の階層の VRF の集約ステータスによって決定されます：**[保留中（Pending）]**、**[進行中（In Progress）]**、**[同期していない/失敗（Out-of-Sync/Failed）]**、**[同期中/成功（In Sync/Success）]**、**[不明/NA（Unknown/NA）]**。たとえば、いずれかのネットワークまたは VRF のステータスが **Out-of-Sync/Failed** で、他のネットワークまたは VRF が **[保留中（Pending）]** または **[進行中（In Progress）]** のステータスでない場合、スイッチのステータスは **[同期していない/失敗（Out-of-Sync/Failed）]** です。ステータスが不明の場合、デフォルトのステータスは **[不明/NA（Unknown/NA）]** です。

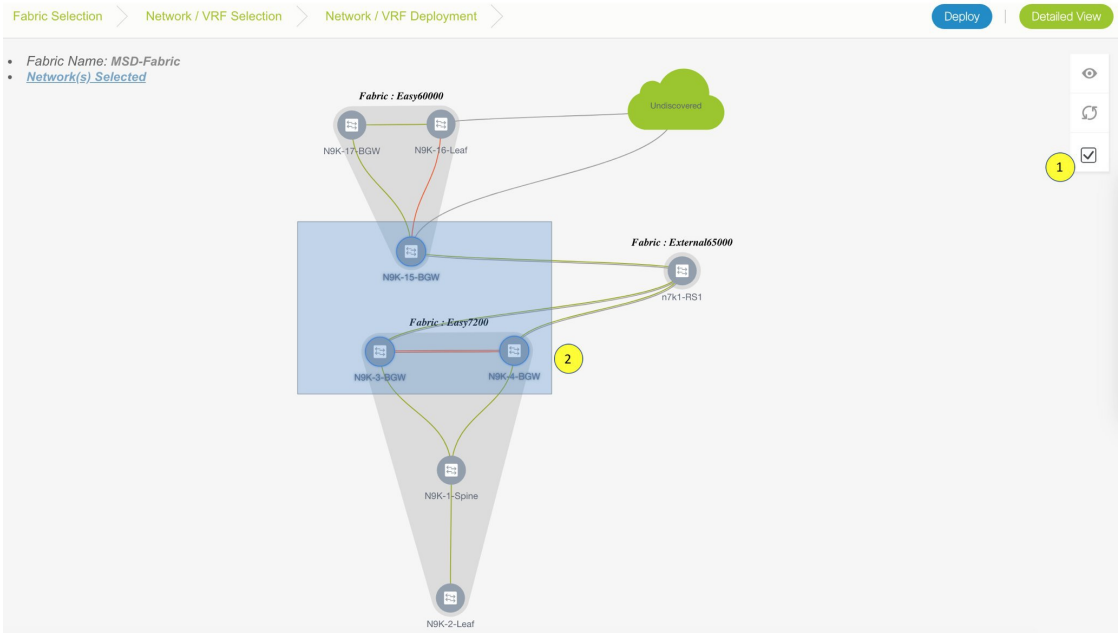
[ネットワーク（Network）] ページに移動して、すべてのネットワークの個々のステータスを表示します。

[MSD ファブリックのネットワーク展開（Network Deployment for an MSD Fabric）]

異なるメンバー ファブリック ボーダー デバイスに同じネットワークを展開しているシナリオを検討してください。1つのファブリックを選択し、そのボーダーデバイスにネットワークを展開してから、2 番目のファブリックを選択してネットワークを展開できます。

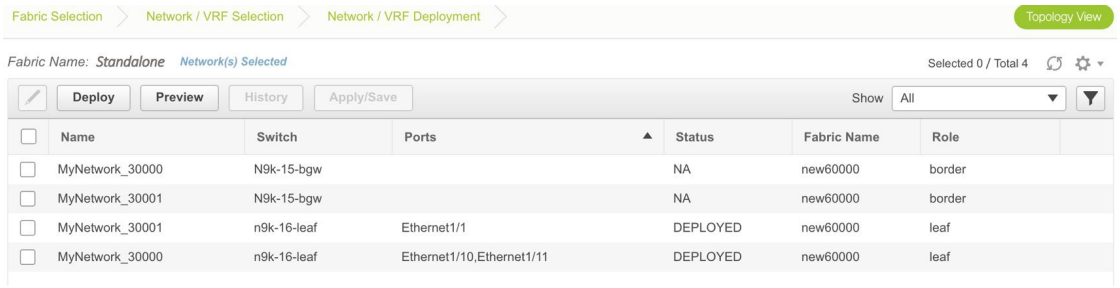
または、MSD ファブリックを選択し、すべてのメンバー ファブリック ボーダー デバイスの単一トポロジ表示からネットワークを展開できます。

これは、MSD ファブリックのトポロジ表示であり、2 つのメンバー ファブリック トポロジとそれらの接続が示されています。ファブリックの BGW にネットワークを一度に展開できます。



[詳細表示（Detailed view）]

[詳細表示（Detailed View）] オプションを使用して、ネットワークと VRF を展開することもできます。画面右上の **[詳細表示（Detailed View）]** をクリックします。[詳細表示（Detailed View）] ウィンドウが表示されます。これにより、表形式ビューでネットワークが一覧表示されます。



次のオプションがあります。

編集：ネットワークを選択し、画面の左上にある [編集（Edit）] アイコンをクリックします。

Note ネットワーク/スイッチ エントリを 1 つ選択して [編集（Edit）] をクリックすると、[ネットワーク接続（Network Attach）] ダイアログ ボックスが表示されます。[トポロジ表示（Topology View）] 画面と [詳細表示（Detailed View）] 画面の間で一貫性を維持するために、ネットワーク接続画面には、選択したネットワーク/スイッチ エントリだけでなく、すべてのネットワークが表示されます。

プレビュー：[プレビュー（Preview）] をクリックして、展開をする前に構成をプレビューします。プレビューできるのは保留中の構成のみであり、開始されていない構成や展開された構成はプレビューできません。

展開：[展開（Deploy）] をクリックして、ネットワークをスイッチにプロビジョニングします。

履歴：行を選択し、[履歴（History）] をクリックして、構成インスタンスとステータスを表示します。ネットワークおよび VRF に関する構成が表示されます。詳細については、任意のインスタンスの [ステータス（Status）] 列をクリックします。

テーブルのフィールドには、各行の構成インスタンス、関連するスイッチとファブリックの名前、スイッチのロール、トランク ポート（ある場合）、および展開ステータスが含まれています。

クイック アタッチ：ネットワークを選択し、**[クイック アタッチ（Quick Attach）]** をクリックします。 確認ウィンドウが表示されます。**[OK]** をクリックします。選択したスイッチにネットワークが接続されます。

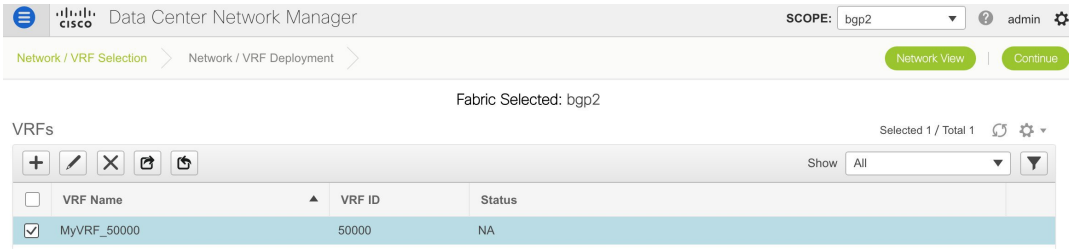
クイック アタッチ解除：ネットワークを選択し、**[クイック アタッチ解除（Quick Detach）]** をクリックします。 確認ウィンドウが表示されます。**[OK]** をクリックします。選択したスイッチからネットワークが切り離されます。

[詳細表示（Detailed View）] ページでは、ネットワーク プロファイルの構成履歴が表示されます。特定のトランク インターフェイスをそのネットワークに関連付けている場合、インターフェイス構成は別個の構成インスタンスとして表示されます。

Note 以前のリリース（DCNM 10.4[2] など）から DCNM 11.0(1) リリースにアップグレードすると、以前の DCNM リリースからのオーバーレイ ネットワークおよび VRF 展開履歴情報は保持されません。

スタンドアロンおよび MSD ファブリック向け VRF の展開

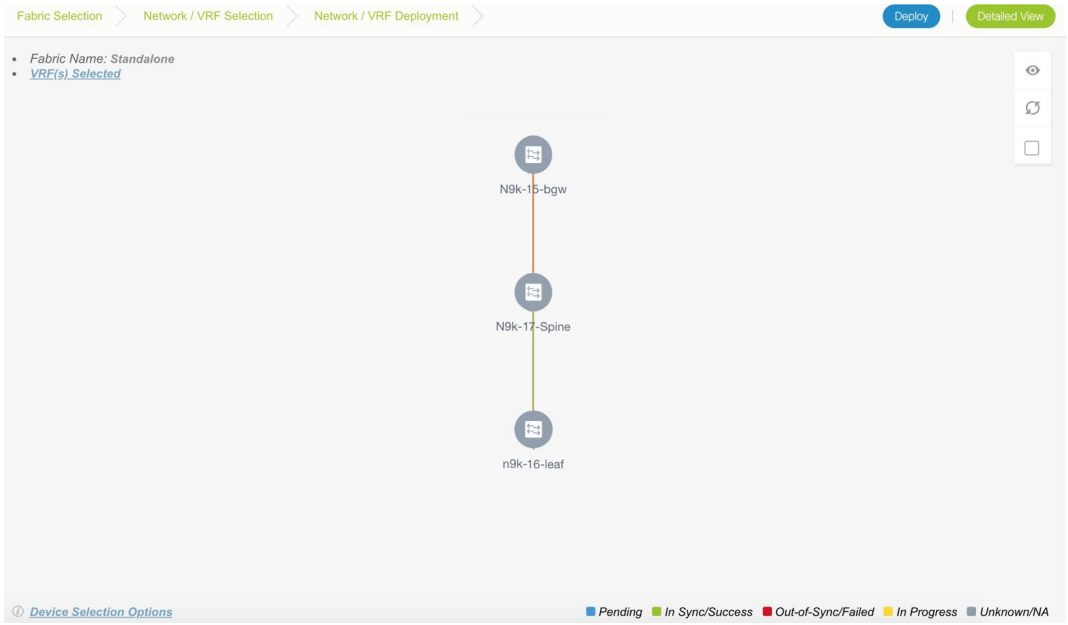
1. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[VRF（VRFs）]** 画面が更新され、選択したファブリックの VRF が一覧表示されます。



2. 展開する VRF の横にあるチェックボックスをオンにして、画面の右上にある [続行（Continue）] をクリックします。

[VRF 展開（VRF Deployment）] 画面が表示されます。このページでは、スタンドアロンファブリックのトポロジを確認できます。次の例は、リーフスイッチに VRF MyVRF_50000

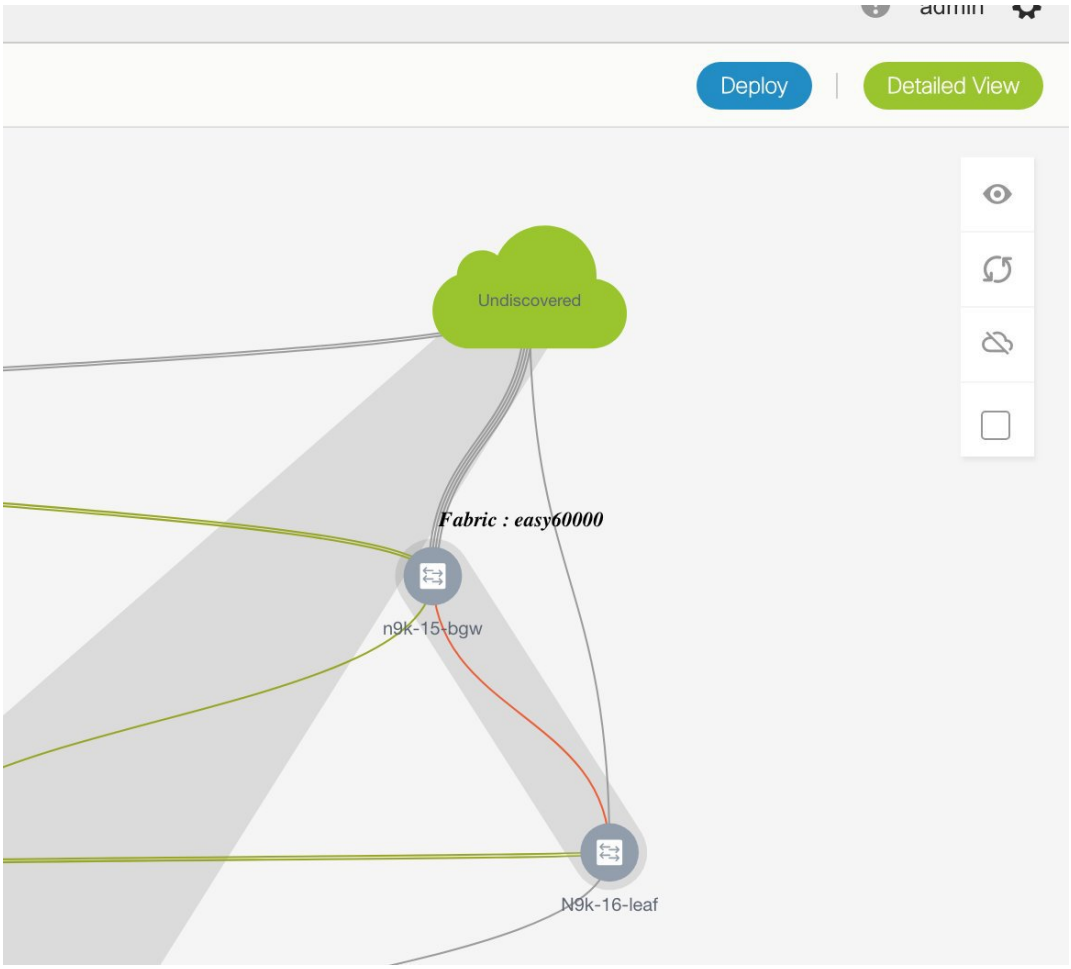
およびMyVRF_50001を展開する方法を示しています。複数のスイッチに同時にVRFを展開できますが、ロールは同じです（リーフ、ボーダーゲートウェイなど）。



画面の右下に、展開のさまざまな段階を表すカラーコードが表示されます。それに応じてスイッチ アイコンの色が変わります。保留中 の状態は青色、プロビジョニングが 進行中 の場合は黄色、失敗状態の場合は赤色、正常に展開された場合は緑色です。 DCNM 11.3(1) 以降、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、**[保存と展開（Save & Deploy）]** をクリックしてスイッチの状態を再計算できます。

オーバーレイ ネットワーク（または VRF）のプロビジョニング ステータスは、コンテキスト固有です。これは、プロビジョニング用に選択した VRF とトポロジ内の関連するスイッチの組み合わせです。この例では、VRF がこのファブリックのどのスイッチにもまだ展開されていないことを意味します。

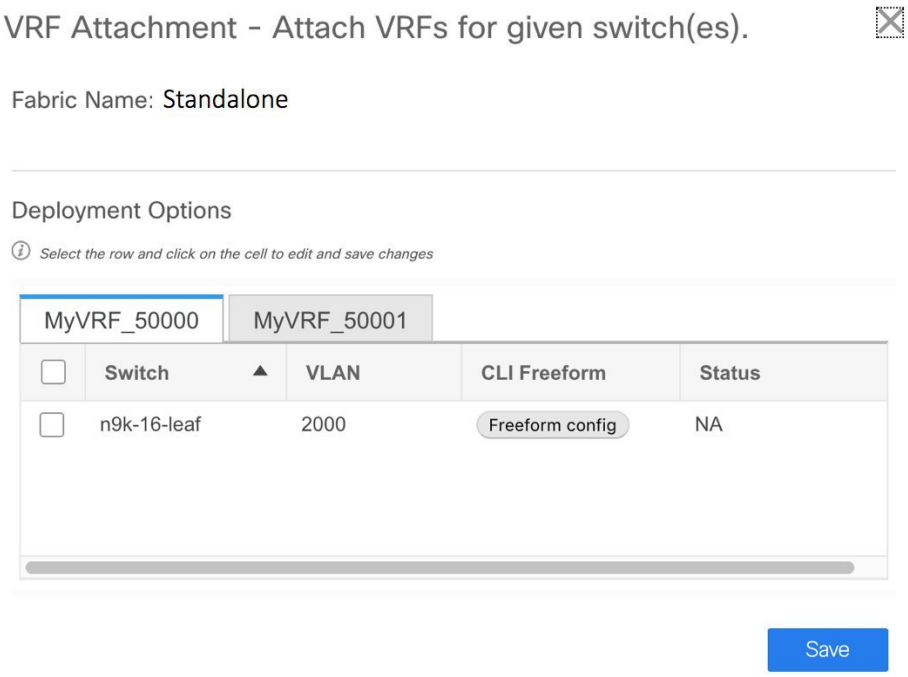
[未検出のクラウド（Undiscovered cloud）] の表示：この画面に **[未検出（Undiscovered）]** クラウドを表示（または非表示）するには、画面の右上にある垂直パネルのクラウドアイコンをクリックします。アイコンをクリックすると、**[未検出（Undiscovered）]** クラウドと、選択したファブリック トポロジへのリンクは表示されません。**[未検出（Undiscovered）]** クラウドを表示するためにアイコンを再度クリックします。



画面上でマウスの左ボタンをクリックし、希望する方向に移動することにより、画面上でトポロジを移動できます。カーソル ローラーを移動することで、スイッチ アイコンを比例して拡大または縮小できます。タッチパッドで対応する代替手段を使用することもできます。

3. スイッチをダブルクリックして、スイッチに VRF を展開します。[VRF アタッチメント（VRF Attachment）] 画面が表示されます。

Note 複数のスイッチに VRF を展開するには、画面の右上部分にあるパネルから [複数選択（Multi-Select）] オプションをクリックし（これにより、トポロジが静的な状態に凍結します）、スイッチ間でカーソルをドラッグします。



タブは、展開されている各 VRF を表します（最初に選択された VRF がデフォルトで表示されます）。各 VRF タブには、選択したスイッチが表示されます。各行はスイッチを表します。

VLAN ID：必要に応じて、VLAN 列内をクリックして VRF VLAN ID を更新します。

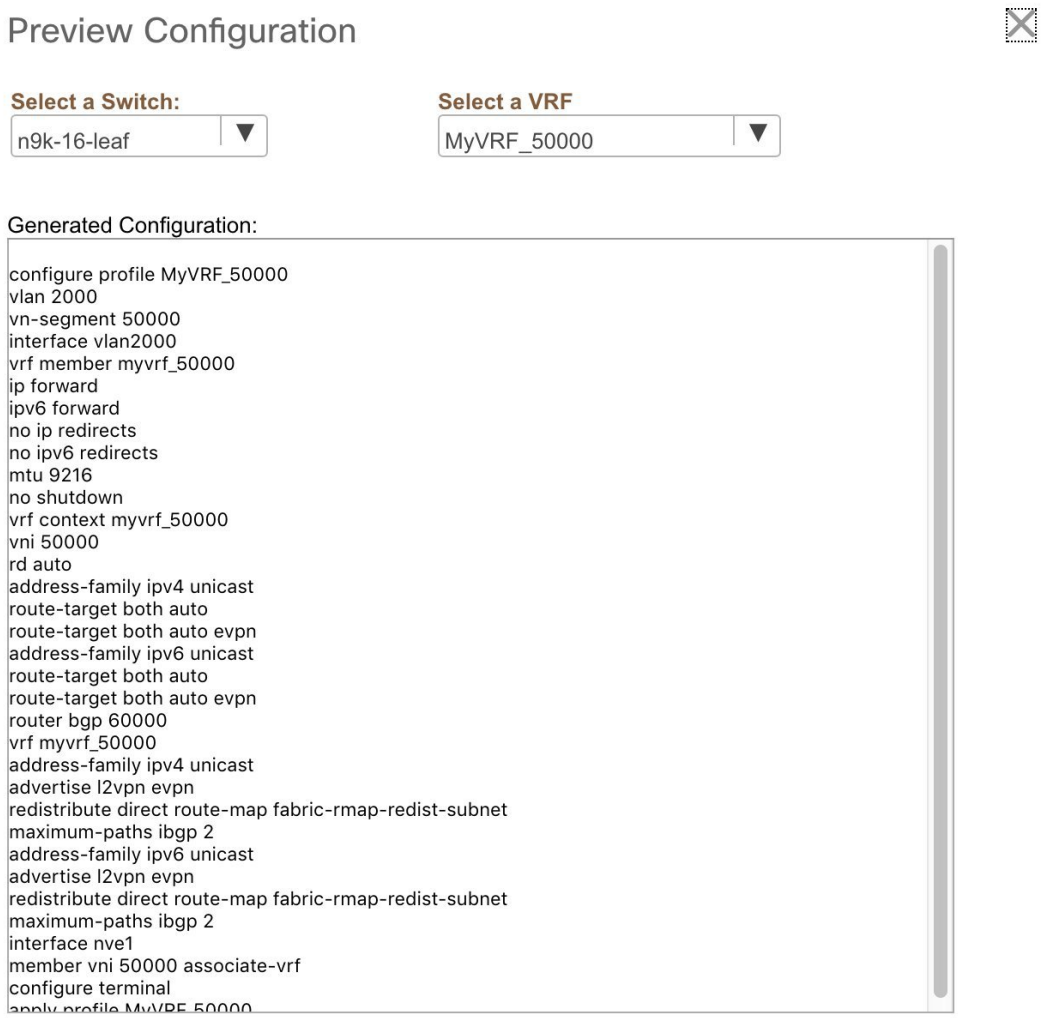
自由形式構成：[自由形式構成（Freeform config）] をクリックして、スイッチで追加の構成を有効にします。自由形式構成を保存すると、[自由形式構成（Freeform config）] ボタンが強調表示されます。

[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、すべてのスイッチを選択します。VRF MyVRF_50000 は、スイッチでプロビジョニングする準備ができています

4. 他の VRF タブを選択し、同じ選択を行います。
5. **[保存（Save）]**（画面の右下部分）をクリックして、VRF 構成を保存します。

   トポロジ画面が再び起動します。画面の右上にある垂直パネルの *[更新（Refresh）]* ボタンをクリックします。スイッチ アイコンの青色は、展開が保留中であることを示します。DCNM 11.3(1) 以降、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、**[保存と展開（Save & Deploy）]** をクリックしてスイッチの状態を再計算できます。

   [プレビュー（Preview）] ボタン（*[複数選択（Multi-Select）]* オプションの上にある目のアイコン）をクリックして、構成をプレビューします。



構成を確認したら、画面を閉じます。*[*トポロジ表示（*Topology View*）*]* 画面が表示されます。

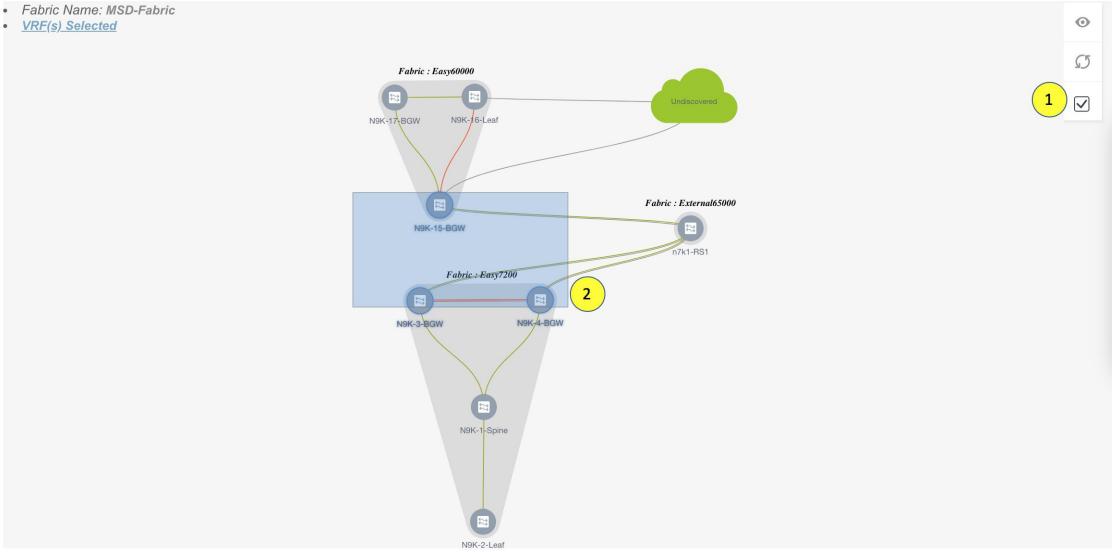
6. 画面右上の **[展開（Deploy）]** ボタンをクリックします。スイッチアイコンの色が黄色に変わり、画面の右下に展開が進行中であることを示すメッセージが表示されます。VRF の展開が完了すると、スイッチアイコンの色が緑に変わり、展開が成功したことを示します。

Note **[展開（Deploy）]** をクリックして、展開する必要のある構成差分がない場合は、**[展開保留中のスイッチなし（No switches PENDING for deployment）]** と示すポップアップ ウィンドウが表示されます。

[MSD ファブリックの VRF 展開（VRFs Deployment for an MSD Fabric）]

異なるメンバー ファブリック ボーダー デバイスに同じ VRF を展開しているシナリオを検討してください。1 つのファブリックを選択し、そのボーダー デバイスに VRF を展開してから、2 番目のファブリックを選択して VRF を展開できます。

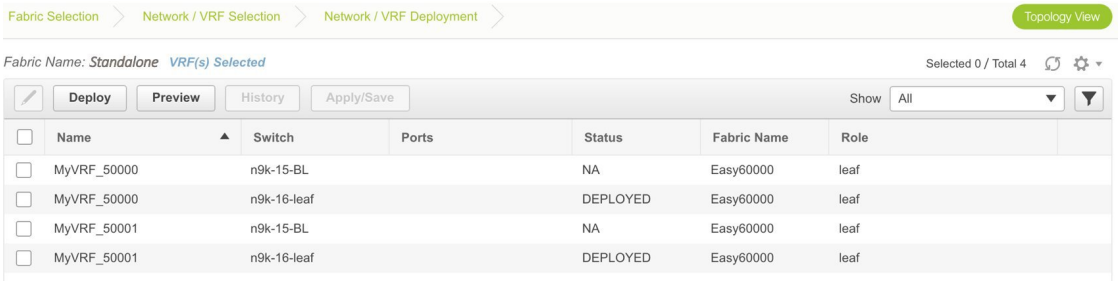
または、MSD ファブリックを選択し、すべてのメンバー ファブリック ボーダー デバイスの単一トポロジ表示から VRF を一度に展開できます。



詳細ビュー

[詳細表示（Detailed View）] ボタンを使用して、ネットワークと VRF を展開することもできます。

画面右上の **[詳細表示（Detailed View）]** をクリックします。[詳細表示（Detailed View）] 画面が表示されます。これにより、表形式ビューで VRF が一覧表示されます。



次のオプションがあります。

編集：VRF を選択し、画面の左上にある [編集（Edit）] アイコンをクリックします。

Note 1 つの VRF/スイッチ エントリを選択すると、VRF 接続画面が表示されます。[トポロジ表示（Topology View）] 画面と [詳細表示（Detailed View）] 画面の間で一貫性を維持するために、VRF 接続画面には、選択した VRF/スイッチエントリだけでなく、すべての VRF が表示されます。

プレビュー：[プレビュー（Preview）] をクリックして、展開をする前に構成をプレビューします。プレビューできるのは保留中の構成のみであり、開始されていない構成や展開された構成はプレビューできません。

展開：[展開（Deploy）] をクリックして、VRF をスイッチにプロビジョニングします。

履歴：行を選択し、[履歴（History）] をクリックして、構成インスタンスとステータスを表示します。ネットワークおよび VRF に関する構成が表示されます。詳細については、任意のインスタンスの [ステータス（Status）] 列をクリックします。

テーブルのフィールドには、各行の構成インスタンス、関連するスイッチとファブリックの名前、スイッチのロール、および展開ステータスが含まれています。

クイック アタッチ：VRF を選択し、**[クイック アタッチ（Quick Attach）]** をクリックします。確認ウィンドウが表示されます。**[OK]** をクリックします。選択したスイッチに VRF が接続されます。

クイック アタッチ解除：VRF を選択し、**[クイック アタッチ解除（Quick Detach）]** をクリックします。確認ウィンドウが表示されます。**[OK]** をクリックします。選択したスイッチから VRF が切り離されます。

Note 以前のリリース（DCNM 10.4[2] など）から DCNM 11.0(1) リリースにアップグレードすると、以前の DCNM リリースからのオーバーレイ ネットワークおよび VRF 展開履歴情報は保持されません。

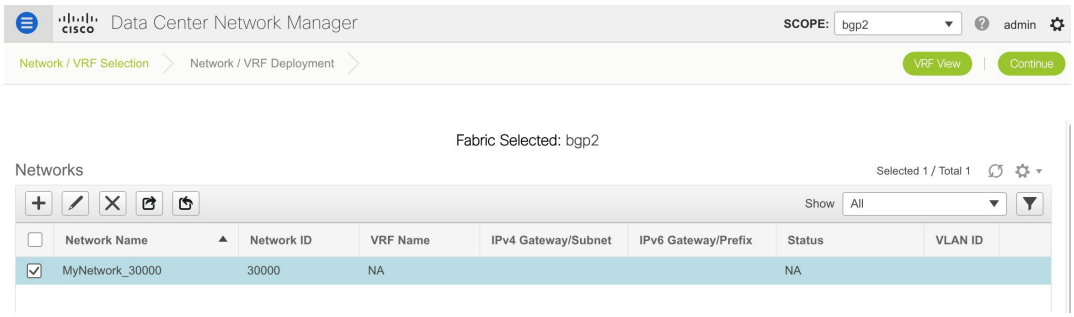
スタンドアロン ファブリック向けのネットワークの展開解除

展開画面から VRF とネットワークを展開解除できます。展開解除の DCNM 画面フローは、展開プロセスフローに似ています。展開画面（トポロジ表示）に移動して、ネットワークの展開を解除します。

1. **[制御（Control）]>[ネットワーク（Networks）]（[ファブリック（Fabrics）]** サブメニューの下）をクリックします。

   [ネットワーク（Networks）] 画面が表示されます。

2. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[ネットワーク（Networks）]** 画面が更新され、選択したファブリックのネットワークが一覧表示されます。



3. 展開解除するネットワークを選択し、[続行（Continue）] をクリックします。トポロジ表示が表示されます。
4. 複数のスイッチからネットワークを展開解除する場合は、[複数選択（Multi-Select）] ボタンを選択し、同じロールを持つスイッチ間でカーソルをドラッグします。[ネットワーク接続（Network Attachment）] 画面が表示されます。

   （単一のスイッチの場合、スイッチをダブルクリックすると、[ネットワーク接続（Network Attachment）] 画面が表示されます）。

   （単一のスイッチの場合、スイッチをダブルクリックすると、[スイッチ展開（Switches Deploy）] 画面が表示されます）。
5. [ネットワーク接続（Network Attachment）] 画面で、展開されたネットワークの [ステータス（Status）] 列が [展開済み（DEPLOYED）] と表示されます。必要に応じて、スイッチの横にあるチェックボックスをオフにします。各タブはネットワークを表すため、すべてのタブでこれを繰り返します。
6. **[保存（Save）]**（画面の右下部分）をクリックして、ネットワークの展開解除を開始します。トポロジ表示 が再び表示されます。

Note または、**[詳細表示（Detailed View）]** ボタンをクリックして、ネットワークを展開解除することもできます。

7. 画面を更新し、必要に応じて構成をプレビューし、**[展開（Deploy）]** をクリックしてスイッチのネットワーク構成を削除します。スイッチアイコンが緑色に変わったら、展開解除が成功したことを示します。
8. [ネットワーク（Networks）] ページに移動して、ネットワークが展開されていないかどうかを確認します。

スタンドアロン ファブリック向けの VRF の展開解除

展開画面から VRF を展開解除できます。展開解除の DCNM 画面フローは、展開プロセス フローに似ています。

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

2. **[範囲（SCOPE）]**から正しいファブリックを選択してください。ファブリックを選択すると、**[VRF]** 画面が更新され、選択したファブリックのネットワークが一覧表示されます。
3. 展開解除する VRF を選択し、**[続行（Continue）]** をクリックします。*[*トポロジ表示（*Topology View*）*]* ページが表示されます。
4. 複数のスイッチから VRF を展開解除する場合は、Multi-Select オプションを選択し、同じロールを持つスイッチ間でカーソルをドラッグします。[VRF アタッチメント（VRF Attachment）] 画面が表示されます。

   （単一のスイッチの場合、スイッチをダブルクリックすると、VRF 接続画面が表示されます）。
5. [スイッチの展開（Switches Deploy）] 画面で、展開された VRF の **[ステータス（Status）]** 列が [展開済み（DEPLOYED）] と表示されます。必要に応じて、スイッチの横にあるチェックボックスをオフにします。各タブは VRF を表すため、すべてのタブでこれを繰り返します。
6. **[保存（Save）]**（画面の右下部分）をクリックして、VRF の展開解除を開始します。トポロジ表示が再び表示されます。

Note または、**[詳細表示（Detailed View）]** ボタンをクリックして、VRF を展開解除することもできます。

7. 画面を更新し、必要に応じて構成をプレビューし、**[展開（Deploy）]**をクリックしてスイッチの VRF 構成を削除します。スイッチ アイコンが緑色に変わったら、展開解除が成功したことを示します。
8. [VRF] ページに移動して、ネットワークが展開されていないかどうかを確認します。

ネットワークおよび VRF の削除

MSD ファブリック内のネットワークおよび対応する VRF を削除するには、次の手順に従います。

1. ネットワークを展開解除します（まだ実行していない場合）。
2. ネットワークを削除します。
3. VRF を展開解除します（まだ実行していない場合）。
4. VRF を削除します。

複数の VLAN ID を単一の VNI に構成する

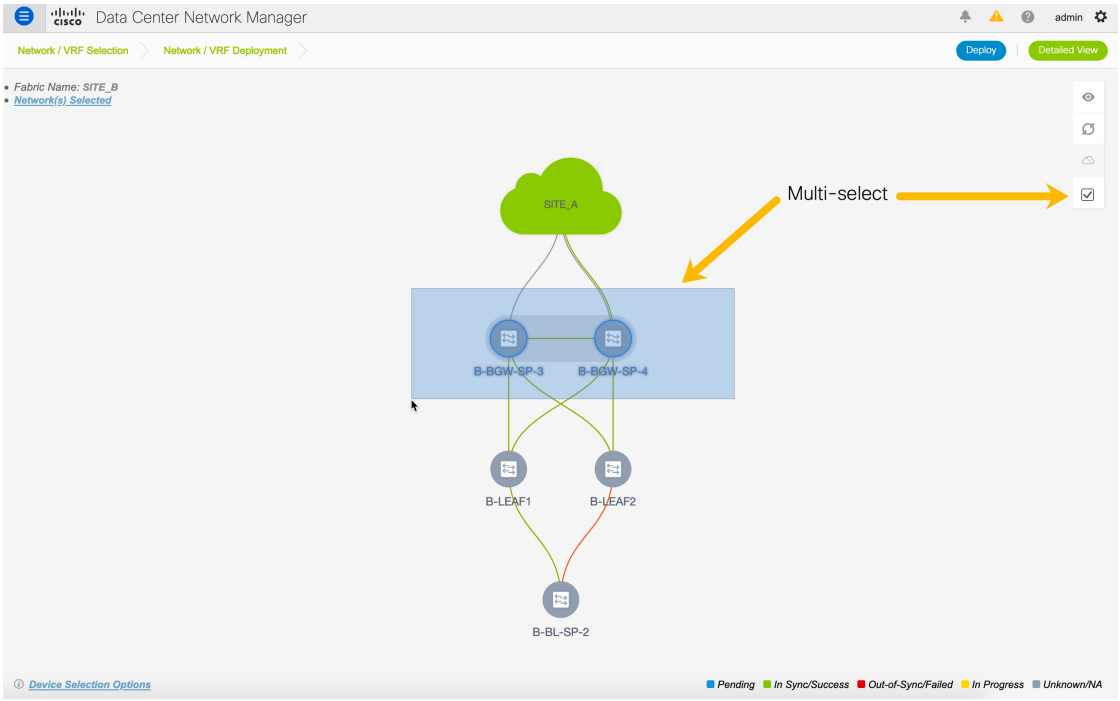
次の手順は、DCNM で複数の VLAN ID を単一の VNI にタグ付けする方法を示しています。

手順

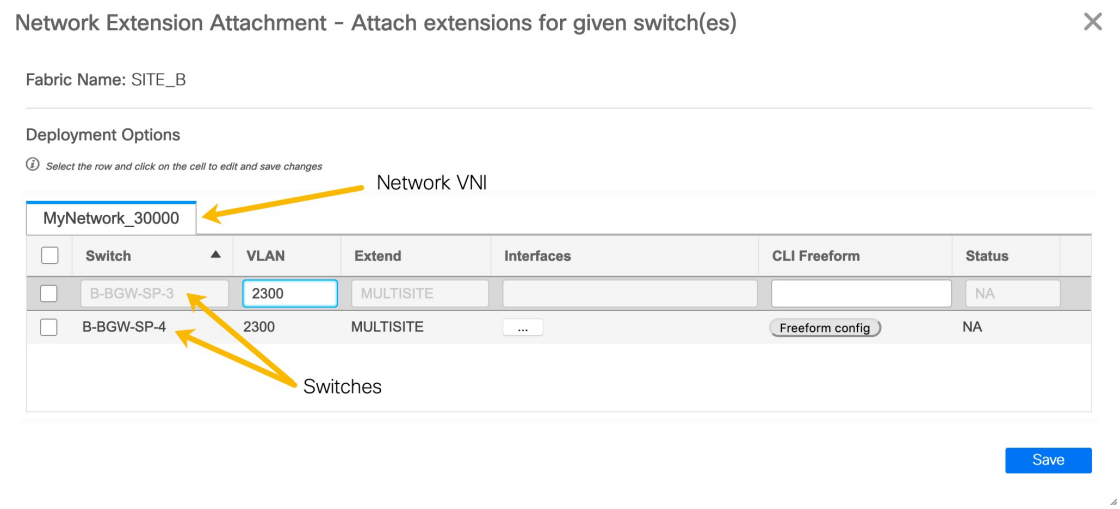
ステップ 1 **[制御（Control）] > [ネットワーク（Networks）]** に移動します。

ステップ 2 **[範囲（SCOPE）]** ドロップダウンリストからファブリックを選択し、ネットワークを選択します。**[続行（Continue）]**をクリックします。

ステップ 3 **[複数選択（Multi-Select）]** チェックボックスをオンにして、VLAN ID で更新する必要があるスイッチの上にカーソルをドラッグします。



ステップ 4 **[ネットワーク接続（Network Attachment）]** ウィンドウで、スイッチの VLAN ID を編集し、**[保存（Save）]** をクリックします。



ステップ 5 構成を展開するには、**[展開（Deploy）]** をクリックします。

Cisco DCNM の拡張された役割別のアクセス制御

Cisco DCNM リリース 11.4（1）から、次のロールベース アクセス コントロール（RBAC）の変更を確認できます。

- **network-operator** ユーザー ロールの Cisco DCNM Web UI および API への読み取り専用アクセス
- **network-stager** と呼ばれる新しいユーザー ロール。
- **network-admin**ロールを持つユーザーとして、DCNM 内の特定のファブリックまたはすべてのファブリックの展開をフリーズします。

Cisco DCNM リリース 11.5（1））から、新しいユーザー ロール、**device-upg-admin**、および **access-admin** が追加されていることがわかります。

（注） 選択したユーザー 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。

また、ネットワーク ステージャによって実行される操作の一部と、Cisco DCNM でファブリックを凍結する方法についてのビデオを見ることもできます。[拡張されたロールベース アクセス コントロール（RBAC）（Enhanced Role-based Access Control (RBAC)）]ビデオを参照してください。

Device-upg-admin ロール

[device-upg-admin] 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 （433 ページ）を参照してください。

Access-admin ロール

[access-admin] 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）]** ウィンドウでのみ操作を実行できます。

access-admin 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 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 インターフェイスを除く

ただし、access-admin 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。

（注） ファブリックまたは DCNM が deployment-freeze 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。

Network-Operator ロール

[network-operator] ロールを持つユーザーは、DCNM Web UI の次のメニューにアクセスできます。

- ダッシュボード
- トポロジ
- モニタ（Monitor）
- アプリケーション

Cisco DCNM リリース 11.4(1) 以降、このロールを持つユーザーは、**[制御（Control）]** メニューへの読み取り専用アクセスもできます。

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。

Network-Stager ロール

network-stager ロールを持つユーザーは、DCNM で構成を変更できます。network-admin 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を編集します。
- ポリシーを表示または編集します。
- インターフェイスを作成します。
- ファブリック設定を変更します。
- テンプレートを編集または作成します。

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。
- DCNM 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。

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、それらの構成を展開できないことです。

[network-stager] ロールを持つユーザー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。

ポリシー変更履歴の表示

異なるユーザーは、DCNM でスイッチの予期される構成を同時に変更できます。**[ポリシー変更履歴（Policy Change History）]** タブでこれらの段階的な変更履歴を表示できます。展開履歴は、DCNM からスイッチにプッシュまたは展開された変更をキャプチャします。

（注） 非 Nexus デバイスでは、展開履歴のみがサポートされます。

さまざまなユーザーによる変更を表示するには、次の手順を実行します。

手順

ステップ 1 **[network-admin]**、**[network-stager]**、または **[network-operator]** のユーザーロールで Cisco DCNM にログインします。

ステップ 2 ファブリック トポロジ ウィンドウに移動します。

ステップ 3 履歴を変更する対象のスイッチを右クリックします。

ステップ 4 **[履歴（History）]** を選択します。

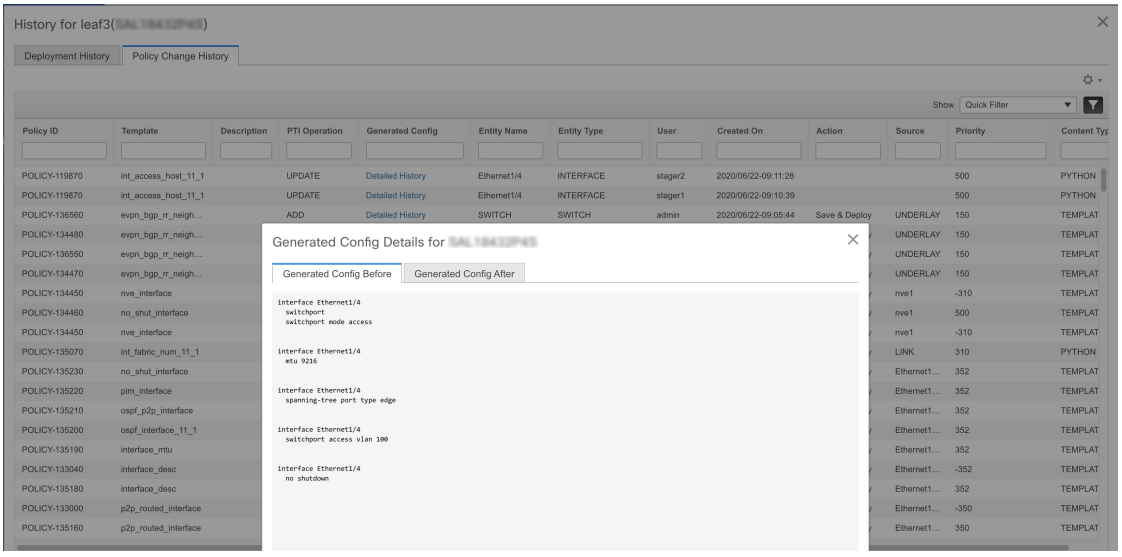
ステップ 5 **[ポリシー変更履歴（Policy Change History）]** タブをクリックします。

ステップ 6 **[生成された構成（Generated Config）]** 列で変更を加えたインターフェイスを検索します。

ステップ 7 **[PTI 操作（PTI Operation）]** 列には、さまざまなユーザーによって行われた変更の値 **[UPDATE]** が含まれます。

ステップ 8 **[ユーザー（User）]** 列まで水平にスクロールします。タイムスタンプ付きのユーザー名が表示されます。

構成可能なエンティティごとに、**[生成された構成（Generated Config）]** 列の下の詳細な履歴に、すべてのユーザーが行った構成変更の差分が表示されます。



Cisco DCNM でのファブリックの凍結

ネットワーク管理者は、LAN クラシック ファブリック、Easy ファブリック、および外部ファブリックの展開を無効にするか、凍結することができます。展開が凍結すると、DCNM からスイッチへの構成または書き込みアクセスが無効になります。ファブリックを凍結すると、スイッチをリロードしたり、メンテナンス モードに移行したり、メンテナンス モードを終了したり、ファブリック内でスイッチを追加または削除したりできなくなります。この機能は、メ

ンテナンス ウィンドウがスケジュールされていない限り、ネットワーク管理者が DCNM から物理ネットワークへの不注意な変更を無効にする完全な制御を提供します。

ファブリックの凍結

Cisco DCNM Web UI からのファブリックの展開を無効にするには、次の手順を実行します。

手順

ステップ 1 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウまたはファブリック トポロジ ウィンドウに移動します。

ステップ 2 スパナ（🔧）アイコンをクリックします。

スパナアイコンは、ファブリック トポロジウィンドウのファブリック名の横にあります。ファブリックのすべての展開を無効にするかどうかを尋ねる確認ウィンドウが表示されます。

ステップ 3 **[はい（Yes）]** をクリックします。

（注） ファブリックを凍結する前にスパナアイコンにカーソルを合わせると、ツールチップに **[展開有効化（Deployment Enabled）]** と表示されます。ファブリックを凍結した後にスパナアイコンにカーソルを合わせると、ツールチップに **[展開無効化（Deployment Disabled）]** と表示されます。

展開を無効にするか、ファブリックを凍結した後は、変更を保存、編集、またはプレビューすることはできますが、それらを展開することはできません。DCNM からこのファブリックへの展開関連のアクションはすべてグレー表示されます。

ファブリックのすべての展開を有効にするには、同じスパナ（⊗）アイコンをクリックして、ファブリックの凍結を解除します。

すべてのファブリックの凍結

ファブリックごとの展開凍結ノブに加えて、ネットワーク管理者は、DCNM 内のすべてのファブリックの展開を同時に凍結できます。

Cisco DCNM Web UI から DCNM セットアップですべてのファブリックを凍結するには、以下の手順を実行します。

手順

ステップ 1 **[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** を選択します。

ステップ 2 **[DEPLOYMENT_FREEZE]** フィールドを検索します。

ステップ 3 値を **[true]** に設定します。

デフォルト値は **false** です。

（注） DCNMを凍結すると、スイッチに変更を展開できません。ただし、network-adminロールやnetwork-stagerロールなどの適切なロールを持つユーザーは、適切なアクセス権を持ち、後の段階で展開するためにDCNMに変更を加えることができます。

ファブリックまたはDCNMを凍結したときに実行できないアクションはグレー表示されます。

ファブリックのバックアップと復元

このセクションでは、Cisco DCNM でのファブリックのバックアップと復元について説明します。

ファブリックのバックアップ

すべてのファブリック設定とインテントを自動または手動でバックアップできます。インテントである構成をCisco DCNMに保存できます。インテントは、スイッチにプッシュされる場合とされない場合があります。

DCNM は、次のファブリックをバックアップしません。

- モニタ専用モードの外部ファブリック：構成またはインテントを復元できないため、モニタ専用モードでの外部ファブリックのバックアップはサポートされていません。ただし、そのような外部ファブリックがMSDファブリックのメンバー ファブリックである場合、バックアップはMSD ファブリック レベルで取得されます。

（注） Cisco DCNMリリース11.4(1)以降、モニタ専用モードで外部ファブリックのバックアップを取得できますが、復元することはできません。外部ファブリックがモニタ専用モードでない場合は、このバックアップを復元できます。

- Cisco DCNMリリース11.4(1)より前のリリースの親MSDファブリック：MSDファブリック内のメンバー ファブリックの構成とインテントのみを個別にバックアップできます。

（注） Cisco DCNMリリース11.4(1)から、MSDファブリックのバックアップを取得できます。親ファブリックからバックアップを開始すると、バックアッププロセスはメンバーファブリックにも適用されます。ただし、DCNMは、メンバー ファブリックとMSDファブリックのすべてのバックアップ情報を1つのディレクトリにまとめて保存します。

Cisco DCNM リリース 11.4(1) 以降、バックアップは IFC に関連するインテントもキャプチャします。外部ファブリックをバックアップすると、チェックポイントがスイッチから DCNM にコピーされます。 バックアップ構成ファイルは、DCNM にある次のパスに保存されます：`/usr/local/cisco/dcm/dcnm/data/archive`

バックアップされた構成ファイルは、ファブリック名を持つ対応するディレクトリにあります。ファブリックの各バックアップは、手動または自動のどちらでバックアップされたかに関係なく、異なるバージョンとして扱われます。バックアップのすべてのバージョンは、対応するファブリック ディレクトリにあります。したがって、バックアップされたインテント構成ファイル、実行構成ファイル、および PTI は、次の場所にあります。`/usr/local/cisco/dcm/dcnm/data/archive/<fabric_name> /Version_x`、ここで `x` はバージョン番号です。有効な値は、1 から、**[archived.versions.limit]** フィールドで設定した制限までです。デフォルト値は 50 です。これは、50 個のバックアップのみがアーカイブされ、最も古いバックアップが削除されることを意味します。最小値は 10 です。10 未満の値を指定すると、10 に上書きされます。**[サーバーのプロパティ（Server Properties）]** ウィンドウで、アーカイブするバックアップファイルの数を設定できます。**[サーバーのプロパティ（Server Properties）]** ウィンドウで、**[ファブリックあたり保持されるアーカイブ ファイルの数：（# Number of archived files per fabric to be retained:）]** セクションを検索します。**[archived.versions.limit]** フィールドに値を入力します。

Cisco DCNM でMSD ファブリックをバックアップおよび復元する方法を示すビデオも視聴できます。「MSD ファブリックのバックアップと復元」のビデオを参照してください。

ファブリックの自動バックアップ

ファブリック構成およびインテントの毎時の自動バックアップ、またはスケジュール バックアップを有効にできます。自動バックアップには 2 つのタイプがあります。

バックアップには、ファブリック上の使用済みリソースに関するリソースマネージャの状態に加えて、インテントとファブリック設定に関連する情報が含まれます。DCNM は、構成のプッシュがある場合にのみバックアップします。DCNM は、最後の構成プッシュ後に手動バックアップをトリガーしなかった場合にのみ、自動バックアップをトリガーします。

自動バックアップには 2 つのタイプがあります。

- **[毎時のファブリック バックアップ（Hourly Fabric Backup）]**：毎時のバックアップを有効にすることができます。

（注） MSD ファブリックは、毎時バックアップをサポートしていません。

- **[スケジュール ファブリック バックアップ（Scheduled Fabric Backup）]**：定期的な間隔でファブリック バックアップをスケジュールできます。

（注） 外部ファブリックでは、DCNMは実行構成の変更もバックアップします。構成のプッシュは、展開後に行われます。変更を展開しなかった場合、インテントでそれらをバックアップすることはできません。

1時間ごと、およびスケジュールされたバックアップ プロセスは、次の定期的な構成コンプライアンス アクティビティ中にのみ発生し、最大 1 時間の遅延が発生する可能性があります。

ファブリックの毎時バックアップおよびスケジュール済みバックアップ

Cisco DCNM Web クライアントからファブリック構成およびインテントの自動バックアップを有効化するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

[ファブリック ビルダ（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 バックアップするファブリックの**[ファブリックの編集（Edit Fabric）]**アイコンをクリックします。

ステップ 3 [構成のバックアップ（Configuration Backup）] タブをクリックします。

ステップ 4 適切なチェックボックスをオンにして、バックアップの種類を選択します。

有効なオプションは、**[毎時のファブリック バックアップ（Hourly Fabric Backup）]** と **[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]** です。両方のバックアップを有効にする場合は、**[毎時のファブリック バックアップ（Hourly Fabric Backup）]** チェックボックスと**[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します。

（注） **[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場合は、**[スケジュール時刻（Scheduled Time）]** フィールドでスケジュール済みのバックアップ時刻を指定します。`HH:MM` フォーマットで値を入力します。

ステップ 5 [保存（Save）] をクリックします。

[保存（Save）] をクリックすると、DCNM はバックアップ プロセスを開始します。

ファブリックの手動バックアップ

ファブリック構成およびインテントの手動バックアップを有効にできます。**[ファブリックの編集（Edit Fabric）]** ダイアログ ボックスの **[構成バックアップ（Configuration Backup）]** タブで選択した設定に関係なく、このオプションを使用してバックアップを開始できます。MSD

ファブリックのメンバー ファブリックのスタンドアロン バックアップを開始することはできません。

Cisco DCNM Web UI からファブリック構成およびインテントの手動バックアップを開始するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 すぐにバックアップするファブリックをクリックします。

ファブリック トポロジ ウィンドウが表示されます。

ステップ 3 [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。

[今すぐバックアップ（Backup Now）] ダイアログが表示されます。

ステップ 4 **[タグ（Tag）]** フィールドにタグ名を入力します。

ステップ 5 [OK] をクリックします。

バックアップが正常にトリガーされたことを示す確認メッセージが表示されます。

（注） 確認メッセージは、バックアップが成功したかどうかではなく、バックアップがトリガーされたことのみを示しています。

ステップ 6 （任意） **[アクション（Actions）]** ペインで **[ファブリックの復元（Restore Fabric）]** をクリックして、手動バックアップが成功したかどうかを確認します。

手動バックアップは濃い青色で示されます。バックアップにカーソルを合わせると、名前に手順 *4* で言及したタグが付いており、手動バックアップであることを確認できます。

ゴールデン バックアップ

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 DCNM は最大 10 のゴールデン バックアップのみをアーカイブします。ファブリックの復元中に、バックアップをゴールデン バックアップとしてマークできます。Cisco DCNM でゴールデンとしてバックアップをマークするには、Cisco DCNM Web UI から次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** の順に選択し、1 つのファブリックを選択します。

ステップ 2 **[アクション（Actions）]** メニューから **[ファブリックの復元（Restore Fabric）]** をクリックします。

[ファブリックの復元（Restore Fabric）] ウィンドウが表示されます。

ステップ 3 バックアップを選択する期間を選択します。

有効な値は、**1m**、**3m**、**6m**、**YTD**、**1y**および**All**です。グラフを拡大できます。デフォルトでは、**1m** のバックアップ情報（1 ヵ月）が表示されます。カスタムの日付範囲を選択することもできます。バックアップ情報には、次の情報が含まれます。

- バックアップ日
- デバイスの総数
- 同期しているデバイスの数
- 同期されていないデバイスの数

ステップ 4 バックアップをクリックして、ゴールデンとしてマークするバックアップを選択します。

自動または手動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。自動バックアップは、**[ファブリックの設定（Fabric Settings）]** ダイアログボックスの **[構成のバックアップ（Configuration Backup）]** タブから開始します。手動バックアップを開始するには、ファブリック トポロジ ウィンドウの **[アクション（Actions）]** ペインから **[今すぐバックアップ（Backup Now）]** をクリックします。

ステップ 5 バックアップをゴールデン バックアップとしてマークするには、**[バックアップをゴールデン バックアップとしてマーク（Mark backup as golden backup）]** チェックボックスにチェックを入れます。

確認用のダイアログボックスが表示されます。

ステップ 6 **[はい（Yes）]** をクリックします。

ステップ 7 「ファブリックの復元」の項に記載されている残りのファブリック復元手順を続行するか、ウィンドウを終了します。

バックアップの検証

ファブリックの復元プロセスを開始すると、DCNMはすべてのバックアップを検証します。検証には、次のチェックが含まれます。

- 復元する DCNM リリース：Cisco DCNM リリース 11.3(1) および Cisco DCNM リリース 11.4(1) からのみバックアップを復元できます。したがって、Cisco DCNM リリース 11.3(1) から Cisco DCNM リリース 11.4(1) にアップグレードする場合、アップグレード前にアーカイブしたバックアップを復元できます。
- メンバーファブリックの構成：DCNMは、MSDファブリックのメンバーファブリックの名前またはIDをチェックします。バックアップ後にそれらを変更すると、復元は続行されません。
- テンプレートの検証：DCNMは、バックアップのテンプレートが現在のバージョンのテンプレートと一致するかどうかを確認します。テンプレートを削除または名前を変更すると、復元を続行できません。
- ファブリックのデバイス構成：バックアップ後にスイッチのインベントリに変更があった場合、復元することはできません。

ファブリックの復元

このセクションでは、さまざまなタイプのファブリックの復元について説明します。Cisco DCNM はファブリック レベルで構成の復元をサポートします。復元する構成のバックアップを取ります。

Easy Fabric の復元

Cisco DCNM で Easy ファブリックを復元するには、Cisco DCNM Web UI から以下の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** の順に選択し、1 つのファブリックを選択します。

ステップ 2 **[アクション（Actions）]** メニューから **[ファブリックの復元（Restore Fabric）]** を選択します。

[ファブリックの復元（Restore Fabric）] ウィンドウが表示されます。

ステップ 3 構成を復元する時間を選択します。

有効な値は、**1m**、**3m**、**6m**、**YTD**、**1y** および **All** です。グラフを拡大できます。デフォルトでは、**1m** のバックアップ情報（1 ヵ月）が表示されます。カスタムの日付範囲を選択することもできます。バックアップ情報には、次の情報が含まれます。

- バックアップ日
- デバイスの総数

- 同期しているデバイスの数
- 同期されていないデバイスの数

ステップ 4 復元するバックアップを選択します。

自動または手動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。自動バックアップは、**[ファブリックの設定（Fabric Settings）]** ダイアログボックスの **[構成のバックアップ（Configuration Backup）]** タブから開始します。手動バックアップを開始するには、ファブリック トポロジ ウィンドウの **[アクション（Actions）]** ペインから **[今すぐバックアップ（Backup Now）]** をクリックします。

Note ファブリックが MSD ファブリックのメンバーであり、バックアップが MSD ファブリック レベルで取得された場合、そのバックアップはここに表示されません。MSD ファブリックの一部になる前に取得されたファブリックのスタンドアロンバックアップのみがここに表示されます。

ステップ 5 バックアップをゴールデン バックアップとしてマークするには、**[バックアップをゴールデンバックアップとしてマーク（Mark backup as golden backup）]** チェックボックスにチェックを入れます。

ステップ 6 > **[次へ（Next）]** をクリックして、同期しているデバイスの選択したバックアップ情報を表示します。

スイッチ名、スイッチのシリアル番号、IP アドレス、と差分構成の詳細が表示されます。

Note ファブリックにデバイスを追加または削除すると、バックアップは無効になります。有効なバックアップのみを復元できます。

ステップ 7 **[構成の取得（Get Config）]** をクリックして、構成の詳細をプレビューします。

[構成のプレビュー（Config Preview）] ウィンドウが表示されます。このウィンドウには 2 つのタブがあります。

- **バックアップ構成（Backup Config）**：このタブには、選択したデバイスのバックアップ設定が表示されます。
- **[現在の構成（Current Config）]**：このタブには、選択したデバイスの現在の構成が表示されます。

ステップ 8 **[バックアップのサマリを表示（View Backup Summary）]** ウィンドウに戻ります。

ステップ 9 **[インテントの復元（Restore Intent）]** をクリックして、復元の手順に進みます。

[ステータスの復元（Restore Status）] ウィンドウが表示されます。次のステータスを表示できます。

- **[バックアップの検証（Validating Backup）]**

- **[ファブリック インテントの復元（Restoring fabric intent）]**
- **[アンダーレイ インテントの復元（Restoring underlay intent）]**
- **[インターフェイス インテントの復元（Restoring interface intent）]**
- **[オーバーレイ インテントの復元（Restoring overlay intent）]**

アクションのステータスの有効な値は、**[進行中（In Progress）]**、**[保留中（Pending）]**、または **[失敗（Failed）]**です。

Note **[検証のバックアップ（Validating Backup）]** のステータスが **[失敗（Failed）]** の場合、他の復元アクションはこのウィンドウにリストされません。

ステップ 10 インテントが復元されたら、**[次へ（Next）]** をクリックします。

[構成のプレビュー（Configuration Preview）] ウィンドウが表示されます。このウィンドウでは、次の詳細を表示できます。

- スイッチ名
- [IP アドレス（IP Address）]
- スイッチのシリアル番号
- 構成のプレビュー
- Status
- 進歩

ステップ 11 復元された構成を展開するには、**[展開（Deploy）]** をクリックします。

[構成展開ステータス（Configuration Deployment Status）] ウィンドウが表示されます。スイッチ名、IP アドレス、ステータス、ステータスの説明、進行状況の詳細を表示できます。

ステップ 12 復元プロセスが完了したら、**[閉じる（Close）]** をクリックします。

外部ファブリックの復元

外部ファブリックを復元すると、バックアップされたチェックポイントが DCNM からスイッチにコピーされます。Cisco DCNM で外部ファブリックを復元するには、Cisco DCNM Web UI から以下の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** の順に選択し、1 つのファブリックを選択します。

ステップ 2 [アクション（Actions）] メニューから **[ファブリックの復元（Restore Fabric）]** を選択します。

[ファブリックの復元（Restore Fabric）] ウィンドウが表示されます。

ステップ 3 構成を復元する時間を選択します。

有効な値は、**1m**、**3m**、**6m**、**YTD**、**1y**および**All**です。グラフを拡大できます。デフォルトでは、**1m** のバックアップ情報（1 ヵ月）が表示されます。

バックアップバージョンを選択すると、それを表す垂直バーがグレーになり、対応する情報が画面下部に表示されます。収集する情報は次のとおりです。

- バックアップ日
- DCNM Version
- デバイスの総数
- 同期しているデバイスの数
- 同期されていないデバイスの数

垂直バーの下にある日付スライドを再配置するか、画面の右上にある **[開始（From）]** ボックスと **[終了（To）]** ボックスを使用して、カスタムの日付範囲を選択できます。

ステップ 4 復元するバックアップを選択します。

自動または手動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。自動バックアップは、**[ファブリックの設定（Fabric Settings）]** ダイアログボックスの **[構成のバックアップ（Configuration Backup）]** タブから開始します。手動バックアップを開始するには、ファブリック トポロジ ウィンドウの **[アクション（Actions）]** ペインから **[今すぐバックアップ（Backup Now）]** をクリックします。

Note ファブリックが MSD ファブリックのメンバーであり、MSD ファブリックのバックアップが取られた場合、そのバックアップはここに表示されません。MSDファブリックの一部になる前に取得されたファブリックのスタンドアロンバックアップのみがここに表示されます。

ステップ 5 (Optional) バックアップをゴールデン バックアップとしてマークするには、**[バックアップをゴールデン バックアップとしてマーク（Mark backup as golden backup）]** チェックボックスにチェックを入れます。

ステップ 6 > **[次へ（Next）]** をクリックして、同期しているデバイスの選択したバックアップ情報を表示します。

スイッチ名、スイッチのシリアル番号、IPアドレス、ステータス、復元のサポート（デバイスがチェックポイントロールバックをサポートしているかどうかを示します）、デバイスの構成の詳細、および VRF が表示されます。

Note プラットフォームでのチェックポイントロールバック機能のサポートについては、それぞれのプラットフォームのドキュメントを参照してください。

デフォルトでは、管理 VRF は、復元プロセス中のコピー操作に使用されるため、VRF 列に表示されます。コピー操作に別の VRF を使用する場合は、VRF 列を更新します。すべてのデバイスに同じ VRF を更新するには、画面の左下にある [すべてのデバイスに適用（Apply for all devices）] オプションを使用します。サンプル スクリーンショット：

Note ファブリックにデバイスを追加または削除した場合、現在の日付から過去の日付にファブリックを復元することはできません。

ステップ 7 **[構成の取得（Get Config）]** をクリックして、デバイスの構成の詳細をプレビューします。

[構成のプレビュー（Config Preview）] ウィンドウが表示されます。このウィンドウには 3 つのタブがあります。

- **バックアップ構成（Backup Config）**：このタブには、選択したデバイスのバックアップ設定が表示されます。
- **現在の構成（Current Config）**：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。
- **[並列比較（Side-by-side Comparison）]**：このタブには、スイッチの現在の実行構成と、バックアップ構成（または予想される構成）が表示されます。

ステップ 8 **[バックアップのサマリを表示（View Backup Summary）]** ウィンドウに戻ります。

ステップ 9 **[インテントの復元（Restore Intent）]** をクリックして、復元の手順に進みます。

[ステータスの復元（Restore Status）] ウィンドウが表示されます。次のステータスを表示できます。

- **[バックアップの検証（Validating Backup）]**
- **[ファブリック インテントの復元（Restoring fabric intent）]**
- **[アンダーレイ インテントの復元（Restoring underlay intent）]**
- **[インターフェイス インテントの復元（Restoring interface intent）]**
- **[オーバーレイ インテントの復元（Restoring overlay intent）]**
- **[インテント再生（Intent Regeneration）]**

アクションのステータスの有効な値は、**[進行中（In Progress）]**、**[保留中（Pending）]**、**[完了（Completed）]** または **[失敗（Failed）]**です。

Note **[検証のバックアップ（Validating Backup）]** のステータスが **[失敗（Failed）]** の場合、他の復元アクションはこのウィンドウにリストされません。

ステップ 10 復元プロセスが完了したら、**[閉じる（Close）]** をクリックします。

MSD ファブリックの復元

MSD ファブリックを復元すると、MSD ファブリックに関連するオーバーレイ情報が復元されてから、子ファブリックに関連する情報が復元されます。MSD ファブリックのインベントリ

に変更がある場合、バックアップは無効と見なされ、復元はブロックされます。メンバーファブリックの復元プロセスを開始することはできません。ファブリックが現在 MSD ファブリックのメンバー ファブリックであることを示すエラーが表示されます。メンバー ファブリックを MSD ファブリックから移動して、以前のスタンドアロン バックアップを復元します。MSD ファブリックの復元には、ファブリック インテント、アンダーレイまたはインターフェイス インテント、オーバーレイ インテント、およびインテント再生成の復元が含まれます。

Cisco DCNM でMSD ファブリックをバックアップおよび復元する方法を示すビデオも視聴できます。「MSD ファブリックのバックアップと復元」のビデオを参照してください。

Cisco DCNM で Easy ファブリックを復元するには、Cisco DCNM Web UI から以下の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

ステップ 2 MSD ファブリックを選択します。

ステップ 3 **[アクション（Actions）]** メニューから **[ファブリックの復元（Restore Fabric）]** をクリックします。

[ファブリックの復元（Restore Fabri）]ウィザードが表示され、**[バックアップの選択（Select Backup）]**手順に進みます。

（注） このオプションは、対応するファブリック トポロジ ウィンドウから、MSD ファブリックのメンバー ファブリックには使用できません。

ステップ 4 構成を復元する時間を選択します。

有効な値は、**1m**、**3m**、**6m**、**YTD**、**1y**および**All**です。グラフを拡大できます。デフォルトでは、**1m** のバックアップ情報（1 ヵ月）が表示されます。カスタムの日付範囲を選択することもできます。バックアップ情報には、次の情報が含まれます。

- バックアップ日
- デバイスの総数
- 同期しているデバイスの数
- 同期されていないデバイスの数

ステップ 5 復元するバックアップを選択します。

自動または手動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。自動バックアップは、**[ファブリックの設定（Fabric Settings）]**ダイアログボッ

クスの **[構成のバックアップ（Configuration Backup）]** タブから開始します。手動バックアップを開始するには、ファブリック トポロジ ウィンドウの **[アクション（Actions）]** ペインから **[今すぐバックアップ（Backup Now）]** をクリックします。

（注） メンバー ファブリックを MSD ファブリックにインポートする前に取ったスタンドアロン バックアップは、ここには表示されません。MSD バックアップのみがここに表示されます。

ステップ 6 復元したいバックアップをクリックします。

[バックアップ サマリ（Backup Summary）] エリアが表示されます。収集する情報は次のとおりです。

- バックアップ取得時間：バックアップを取った時点のタイムスタンプ
- DCNM バージョン：バックアップを取った時点の DCNM バージョン
- バックアップ バージョン：バックアップのバージョン（手動バックアップの場合はタグ名も含みます。）
- ファブリックの総数：MSD ファブリックにインポートされたメンバー ファブリックの総数を指定します。
- Easy ファブリックの総数：Easy ファブリックであるメンバー ファブリックの数を指定します。
- 外部ファブリックの総数：外部ファブリックであるメンバーファブリックの数を指定します。
- デバイスの総数：すべてのメンバー ファブリック内のスイッチの総数を指定します。
- 同期ステータス以外のデバイスの数：同期していないデバイスの数を指定します。
- 不明なステータスのデバイスの数：ステータスが不明のデバイスの数を指定します。
- メンバー ファブリック：メンバー ファブリックの名前を指定します。[ゴールデン バックアップとしてバックアップをマーク付け（Mark backup as golden backup）] チェックボックス：（オプション）バックアップをゴールデン バックアップとしてマーク付けするには、**[ゴールデン バックアップとしてバックアップをマーク付け（Mark backup as golden backup）]** チェック ボックスをオンにします。

（注） 同期ステータス以外（Out-of-Sync）または不明な（Unknown）ステータスのデバイスがある場合、復元プロセスはブロックされます。

ステップ 7 **[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。

[Easy ファブリック（Easy Fabric）] タブには、スイッチ名、ファブリック名、スイッチ シリアル、IPアドレス、およびメンバーEasyファブリックのデルタ構成に関する情報があります。**[Easy ファブリック（Easy Fabric）]** タブには、スイッチ名、ファブリック名、スイッチのシリアル、IPアドレス、スイッチのステータス、構成、およびメンバーの外部ファブリックで復元がサポートされているかどうかに関する情報が含まれています。

（注） デバイスがファブリックに追加または削除された場合、バックアップは無効です。有効なバックアップのみを復元できます。

ステップ 8 **[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。

メンバー ファブリックの復元ステータスと説明が表示されます。メンバー ファブリック オプション ボタンをクリックして、そのファブリックのファブリック レベルの進行状況を表示します。進行状況は 5 秒ごとに自動的に更新されます。

ステップ 9 ステータスが成功したら、**[次へ（Next）]** をクリックします。

[構成のプレビュー（Configuration Preview）] ウィンドウが表示されます。このウィンドウでは、スイッチ名、IPアドレス、スイッチのシリアル番号、構成のプレビュー、ステータス、および進行状況の詳細を表示できます。

（注）
- **[次へ（Next）]** をクリックできるのは、ステータスが **[完了（Completed）]** の場合のみです。
- ファブリック設定が変更されているため、前の手順に戻ることはできません。
- 復元に失敗した場合、ファブリックは以前の構成にロール バックします。

ステップ 10 復元された構成を展開するには、**[展開（Deploy）]** をクリックします。

[構成展開ステータス（Configuration Deployment Status）] ウィンドウが表示されます。次の詳細情報を表示できます。

- スイッチ名
- [IP アドレス（IP Address）]
- Status
- ステータスの説明
- 進歩

ステップ 11 復元プロセスが完了したら、**[閉じる（Close）]** をクリックします。

スイッチの復元

Cisco DCNM リリース 11.5(1) 以降、Cisco DCNM Web UI 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。

Cisco DCNM でスイッチを復元するには、Cisco DCNM Web UI から以下の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

ステップ 2 外部ファブリック、または LAN クラシック ファブリックを選択します。

ステップ 3 構成を復元する Cisco Nexus スイッチを右クリックします。

ステップ 4 **[構成の復元（Restore Config）]** オプションを選択します。

または、**[アクション（Actions）]** ペインの **[表形式ビュー（Tabular view）]** をクリックして、**[スイッチ（Switches）]** タブに移動することもできます。チェックボックスをオンにして Cisco Nexus スイッチを選択し、**[復元（Restore）]** をクリックします。

非 Nexus スイッチの場合、**[構成の復元（Restore Config）]** オプションは表示されず、**[復元（Restore）]** ボタンはグレー表示されます。

このオプションは、**[network-operator]** ロールでログインした場合、またはファブリックがモニタ モードまたは凍結モードの場合は表示されません。

[スイッチの復元（Restore Switch）] ウィザードが表示され、**[バックアップの選択（Select Backup）]** 手順に進みます。

ステップ 5 構成を復元する時間を選択します。

有効な値は、**1m**、**3m**、**6m**、**YTD**、**1y** および **All** です。グラフを拡大できます。デフォルトでは、**1m** のバックアップ情報（1 ヵ月）が表示されます。カスタムの日付範囲を選択することもできます。

ステップ 6 復元するバックアップを選択します。

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。自動バックアップは、**[ファブリックの設定（Fabric Settings）]** ダイアログボックスの **[構成のバックアップ（Configuration Backup）]** タブから開始します。手動バックアップを開始するには、ファブリック トポロジ ウィンドウの **[アクション（Actions）]** ペインから **[今すぐバックアップ（Backup Now）]** をクリックします。

ステップ 7 復元するバックアップをクリックします。

[バックアップ サマリ（Backup Summary）] エリアが表示されます。収集する情報は次のとおりです。

- バックアップ取得時間：バックアップを取った時点のタイムスタンプ

- DCNM バージョン：バックアップを取った時点の DCNM バージョン
- バックアップバージョン：バックアップのバージョン（手動バックアップの場合はタグ名も含みます。）
- デバイスの総数：バックアップを取った時点のファブリック内のスイッチの総数を指定します。
- 同期ステータスのデバイスの数：同期しているデバイスの数を指定します。
- 同期ステータス以外のデバイスの数：同期していないデバイスの数を指定します。
- 不明なステータスのデバイスの数：ステータスが不明のデバイスの数を指定します。
- [ゴールデン バックアップとしてバックアップをマーク付け] チェックボックス：（オプション）バックアップをゴールデン バックアップとしてマーク付けするには、**[ゴールデン バックアップとしてバックアップをマーク付け（Mark backup as golden backup）]** チェック ボックスをオンにします。バックアップをゴールデン バックアップとしてマークすると、ファブリック レベルのバックアップもゴールデン バックアップとしてマークされます。

（注） 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。

ステップ 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。

ステップ 9 （任意）**[構成の取得（Get Config）]** をクリックして、デバイスの構成の詳細をプレビューします。

[構成のプレビュー（Config Preview）] ウィンドウが表示されます。このウィンドウには 3 つのタブがあります。

- **バックアップ構成（Backup Config）**：このタブには、選択したデバイスのバックアップ設定が表示されます。
- **現在の構成（Current Config）**：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。
- **並列比較**：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。

ステップ 10 **[復元（Restore）]** をクリックして、復元の **[ステータスの復元（Restore Status）]** 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。

ステップ 11 復元プロセスが完了したら、**[閉じる（Close）]** をクリックします。

（注）
- ファブリック設定が変更されているため、前の手順に戻ることはできません。
- 復元に失敗した場合、スイッチは以前の設定にロールバックします。

VXLAN BGP EVPN ファブリックの削除

[制御（Control）] > [ファブリック ビルダ (Fabric Builder)] を選択します。ファブリック ビルダ ページで、ファブリックを表す長方形のボックスの **[X]** をクリックします。ファブリックを削除する前に、次のことを確認してください。

- ファブリック デバイスは、ファブリック内またはファブリックからの移行、進行中のネットワークまたは VRF プロビジョニングなどの移行中でないようにしてください。移行が完了したら、ファブリックを削除します。
- まだファブリックに接続されているデバイスを削除します。最初に Cisco Nexus 9000 シリーズ以外のスイッチを削除してから、9000 シリーズ スイッチを削除します。

VXLAN BGP EVPN、外部ファブリック、MSD ファブリックの DCNM 11.5(1) アップグレードのポスト

DCNM リリース 11.5(1) にアップグレードした後は、次のガイドラインに注意してください。

- 以前の DCNM リリースからのアップグレードの一環として、ファブリックおよび関連するテンプレートは DCNM リリース 11.5(1) に引き継がれます。
- DCNM 11.3(1) 以降、以前の DCNM リリースのポリシー テンプレートの一部は廃止され、新しい DCNM リリースごとにアクティブに更新されます。これらのポリシー テンプレートは、使用中でないことが判明した場合、アップグレード後に自動的に削除されます。この削除により動作が影響を受けることはなく、DCNM テンプレート ライブラリで表示されるポリシーの数を削減することに役立ちます。
- **[ファブリック ビルダ（Fabric Builder）]** ウィンドウから各ファブリックに移動し、**[保存と展開（Save & Deploy）]** をクリックして変更を展開します。

  [保存と展開（Save & Deploy）] をクリック後、新規または予期しない保留中の構成が見つかった場合は、DCNM での構成コンプライアンス （329 ページ）を参照してください。

⚠

注意 この手順の一部として、いくつかの構成変更が想定されています。したがって、スケジュール済みのメンテナンス ウィンドウについてのみ、実行するようにしてください。

- リリース 11.2(1) からの DCNM アップグレード後、ファブリックにボーダーデバイス（ボーダー、ボーダースパイン、ボーダーゲートウェイなど）がある場合、次の相違点が表示されます。

```
route-map extcon-rmap-filter-v6 deny 20
  no match ip address prefix-list host-route-v6
route-map extcon-rmap-filter-v6 deny 20
  match ipv6 address prefix-list host-route-v6
```

  上記の構成は予期されるものであり、正しいルートマップ定義であることを意味します。この差分を展開することで、スイッチ構成を正常に行えます。アップグレードの前にファブリックがグリーンフィールドとして作成された場合、追加のアクションは必要ありません。デバイス上での誤ったルートマップ構成によってアップグレードが行われる前に、ファブリックがブラウンフィールドとして作成された場合、この構成は **switch_freeform** ポリシーでキャプチャされます。アップグレード後、展開の前に、自由形式ポリシーを編集して CLI **match ip address prefix-list host-route-v6** を削除する必要があります。

- Cisco DCNM 10.4(2) または 11.0(1) 以降では、マルチレベルのアップグレードの後、VRF テンプレートを **Default_VRF_Universal** または **Default_VRF_Extension_Universal** に変更して、**ipv6 address use-link-local-only** を有効にすることができます。

レベル 1 からレベル 2 へ ISIS 構成の変更

この手順は、VXLAN ファブリック展開で、スイッチの ISIS 構成をレベル 1 からレベル 2 に変更する方法を示しています。

1. **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。
2. **ファブリック ビルダ（Fabric Builder）** ウィンドウで、ファブリックをクリックします。
3. **[アクション（Actions）]** メニューで **[表形式ビュー（Tabular view）]** をクリックします。
4. **[テンプレート（Template）]** 検索フィールドですべての **base_isis** ポリシーを検索します。
5. すべての **base_isis** ポリシーを選択し、**[削除（Delete）]** アイコンをクリックしてポリシーを削除します。
6. [保存して展開（Save & Deploy）] をクリックします。

すべての **base_isis** ポリシーが削除されると、DCNM は移行されたブラウンフィールド ファブリックをグリーンフィールド ファブリックと見なし、スイッチに **base_isis_level2** ポリシーを作成します。

DCNM での構成コンプライアンス

特定のスイッチに定義されたインテント全体または予想される構成は、DCNM に保存されます。この構成を 1 つ以上のスイッチにプッシュする場合、構成コンプライアンス（CC）モジュールがトリガーされます。CC は、現在のインテント、現在の実行構成を取得し、現在の

実行構成から現在期待されている構成に移行するために必要な一連の構成を算出し、すべてが同期するようにします。

スイッチでソフトウェアまたはファームウェアのアップグレードを実行しても、スイッチの現在の実行構成は変更されません。アップグレード後、現在の実行構成が現在期待されている構成またはインテントを持っていないことを検出した場合、CC は非同期ステータスを報告します。構成の自動展開は行われません。展開される差分をプレビューしてから、1 つ以上のデバイスを同期状態に戻すことができます。

CC では、同期は常に DCNM からスイッチに対して行われます。逆方向の同期は行われません。そのため、Switchに対し、DCNM で定義されたインテントと競合するアウトオブバンドの変更を行うと、CC はこの差分をキャプチャし、デバイスが同期していないことを示します。保留中の差分は、アウトオブバンドで行われた構成を元に戻し、デバイスを同期状態に戻します。アウトオブバンド変更によるこのような競合がキャプチャされるのは、デフォルトで 60 分ごとに発生する定期的なCC実行時、またはファブリックごとまたはスイッチごとにRESYNC オプションをクリックしたときであることに注意してください。CC の REST API を使用して、スイッチ全体のアウトオブバンド変更をキャプチャすることもできます。詳細については、『*Cisco DCNM REST API* ガイド、リリース *11.2(1)* 』を参照してください。

Cisco DCNM リリース 11.2(1) 以降、展開される構成の使いやすさと読みやすさを向上させるために、DCNM の CC は以下のように拡張されました。

- DCNM でのすべての表示は、読みやすく理解しやすいものにされました。
- 繰り返される構成スニペットは表示されません。
- 保留中の構成には、正確に差分構成だけが表示されます。
- 並列比較による差分表示はより読みやすくなり、統合された検索またはコピー、および差分サマリー機能を備えています。

CC エンジンは、インテントをスイッチで実行中の構成と比較することで差分を計算し、インテントで定義されている構成がスイッチに存在することを確認します。インテントで定義されているコンポーネントまたは構成スニペットについて、CCエンジンは、必要に応じて、スイッチ構成をインテント構成と一致させる適切なコマンドを生成することにより、同じコンポーネントまたは構成スニペットがスイッチ上に存在することを保証します。

DCNMインテントが関連付けられていない、スイッチの最上位の構成コマンドでは、構成コンプライアンス（CC） のコンプライアンス チェックは行われません。ただし、以下のコマンドについては、DCNMインテントがない場合でも、CC はコンプライアンス チェックを実行し、削除を試みます。

- **configure profile**
- **apply profile**
- **interface vlan**
- **interface loopback**
- **interface Portchannel**
- サブインターフェイス、例えば **interface Ethernet** *X/Y.Z*

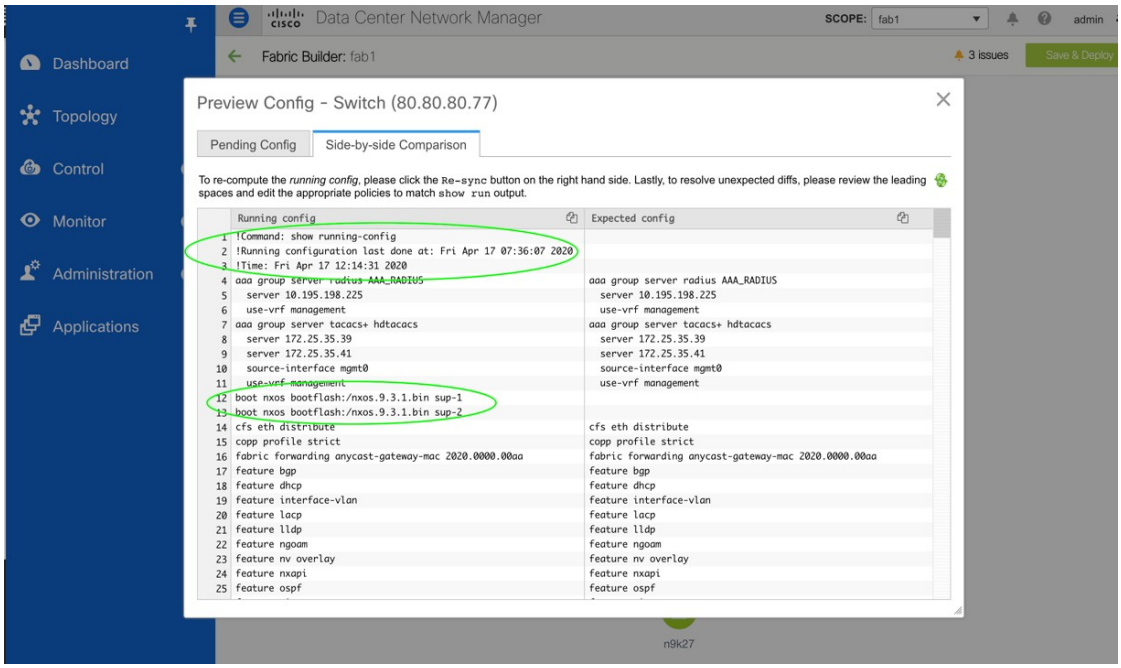
- **fex**
- **vlan** <*vlan-ids*>

CC は、*Easy_Fabric_11_1* および *Easy_Fabric_eBGP* ファブリック テンプレートが使用されている場合にのみ、コンプライアンスチェックを実行し、これらのコマンドの削除を試みます。*External_Fabric* テンプレートの場合、上記のコマンドも含めて、関連する DCNM インテントを持たないスイッチの最上位の構成コマンドでは、CC はコンプライアンス チェックを実行しません。

予期しない動作を避けるために、これらのコマンドをスイッチに展開する場合には、DCNM 自由形式構成テンプレートを使用して追加のインテントを作成することが推奨されています。

ここで、スイッチに存在する構成がインテントで定義された構成と関係していないシナリオを考えてみましょう。このような構成の例としては、インテントでキャプチャされていないがスイッチに存在する新しい機能、またはインテントでキャプチャされていない他の構成の特徴があります。構成コンプライアンスは、これらの構成の不一致を差分とは見なしません。このような場合、厳密な構成コンプライアンスは、インテントで定義されているすべての構成行がスイッチに存在する唯一の構成であることを保証します。ただし、厳密な CC チェックは、ブート文字列、rommon 構成、およびその他のデフォルト構成などの構成を無視します。このような場合、内部構成コンプライアンスエンジンは、これらの構成変更が差分として呼び出されないようにします。これらの差分は、**[保留中の構成（Pending Config）]** ウィンドウにも表示されません。ただし、並列比較差分ユーティリティは、2つをテキストファイルとして差分の比較を行います。diff の計算で使用される内部ロジックは利用しません。その結果、デフォルト構成の差分は、**並列比較（Side-by-side Comparison）**ウィンドウで赤で強調表示されます。

Cisco DCNM リリース 11.4(1) から、そのような差分は、**[並列比較（Side-by-side Comparison）]** ウィンドウで強調表示されません。**[実行中の構成（Running config）]** ウィンドウで強調表示される自動生成されたデフォルト構成は、**[期待される構成（Expected config）]** ウィンドウには表示されません。



[保留中の構成（Pending Config）] ウィンドウに表示される構成が **[並列比較（Side-by-side Comparison）]** ウィンドウでは赤で強調表示される場合があります。これは、その構成が **[実行中の構成（Running config）]** ウィンドウには表示されるものの、**[期待される構成（Expected config）]** ウィンドウには表示されない場合です。一方、**[保留中の構成（Pending Config）]** ウィンドウに表示される構成が **[並列比較（Side-by-side Comparison）]** ウィンドウでは緑で強調表示される場合もあります。これは、その構成が **[期待される構成（Expected config）]** ウィンドウには表示されるものの、**[実行中の構成（Running config）]** ウィンドウには表示されない場合です。**[保留中の構成（Pending Config）]** ウィンドウに構成が表示されない場合、**[並列比較（Side-by-side Comparison）]** ウィンドウに赤で構成が表示されることはありません。

すべての自由形式の構成は、スイッチの **show running configuration** の出力と厳密に一致する必要があり、構成からの逸脱は、**[保存と展開（Save & Deploy）]** の際に差分として表示されます。先頭のスペースによるインデントは守る必要があります。

通常、次の方法を使用して DCNM に構成スニペットを入力できます。

- ユーザー定義のプロファイルとテンプレート
- スイッチ、インターフェイス、オーバーレイ、および vPC フリーフォーム設定
- スイッチごとのネットワークおよび VRF フリーフォーム構成
- リーフ、スパイン、または iBGP 構成のファブリック設定

⚠

注意 設定形式は、対応するスイッチの **show running configuration** と同じである必要があります。そうなっておらず、構成の先頭のスペースが欠落していたり、正しくなかったりした場合、予期しない展開エラーが発生したり、保留中の構成が予測不能な状態になったりする可能性があります。予期しない差分または展開エラーが表示された場合は、ユーザー提供またはカスタムの構成スニペットに間違った値がないか確認してください。

予期しない保留中の構成が原因で DCNM に「非同期」ステータスが表示され、この構成が展開できないか、展開後も変化がない場合は、次の手順を実行して回復します。

1. **[保留中の構成（Pending Config）]** タブ（**[構成プレビュー（Pending Config）]** ウィンドウ）で強調表示されている構成の行を確認します。
2. **[並列比較（Side-by-side Comparison）]** タブで同じ行を確認します。このタブには、「intent」または「show run」、あるいはその両方の先頭スペースが異なっていて、差分になっていた場合、それが表示されます。先頭のスペースは、**[並列比較（Side-by-side Comparison）]** タブで強調表示されます。
3. 保留中の構成または非同期状態のスイッチが、「インテント」と「実行構成」の先頭のスペースが一致しない、識別可能な構成が原因である場合、インテント側のスペースが正しくないため、編集する必要があることを示しています。
4. カスタム ポリシーまたはユーザー定義ポリシーの不適切なスペースを編集するには、スイッチに移動して対応するポリシーを編集します。
    1. ポリシーのソースが **[アンダーレイ（UNDERLAY）]** の場合、ファブリック設定画面からこれを編集し、更新された構成を保存する必要があります。
    2. ソースが空白の場合は、そのスイッチの **[ポリシーの表示/編集（View/Edit policies）]** ウィンドウから編集できます。
    3. ポリシーのソースが **[オーバーレイ（OVERLAY）]** であるが、スイッチの自由形式構成から派生している場合。この場合、適切な **[オーバーレイ（OVERLAY）]** スイッチ自由形式構成に移動して更新します。
    4. ポリシーのソースが **[オーバーレイ（OVERLAY）]** またはカスタム テンプレートの場合は、次の手順を実行します。
        1. **[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** に移動し、**[template.in_use.check]** プロパティを **[false]** に設定します。これにより、プロファイルまたはテンプレートを編集できるようになります。
        2. **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** 編集ウィンドウから特定のプロファイルまたはテンプレートを編集し、更新されたプロファイル テンプレートを適切なスペースを設定して保存します。
        3. **[保存と展開（Save & Deploy）]** をクリックして、影響を受けるスイッチの差分を再計算します。

4. 構成が更新されたら、**[template.in_use.check]** プロパティを **[true]** に設定します。これは、特に **[保存と展開（Save & Deploy）]** 操作で、DCNM システムのパフォーマンスが低下するためです。

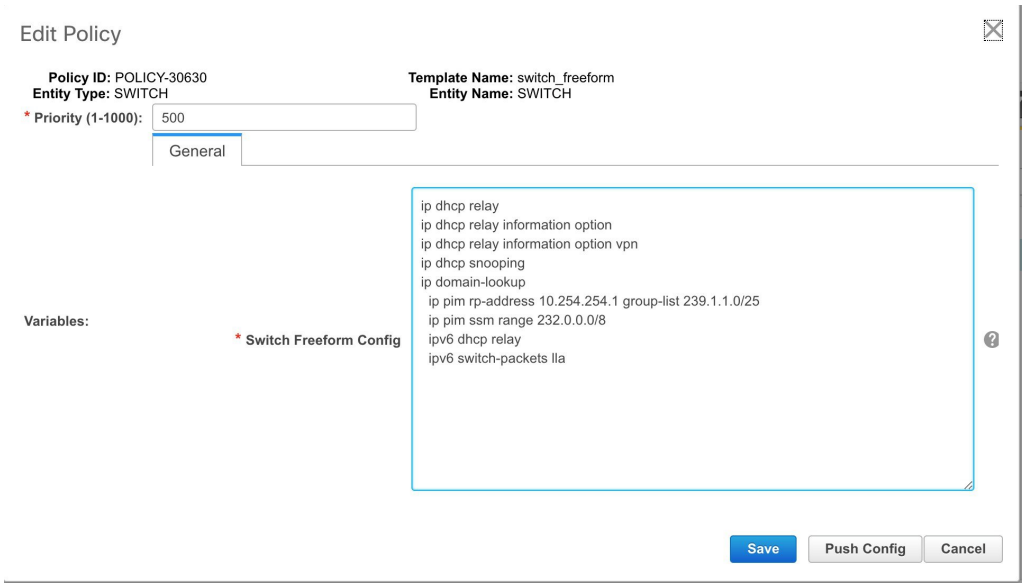
差分が解決されたことを確認するには、ポリシーを更新した後に**[保存と展開（Save & Deploy）]** をクリックして変更を検証します。

（注） DCNM は、特に複数のコマンド シーケンスの場合、コマンドの階層を意味するものであるため、先頭のスペースのみをチェックします。DCNM は、コマンド シーケンスの末尾のスペースをチェックしません。

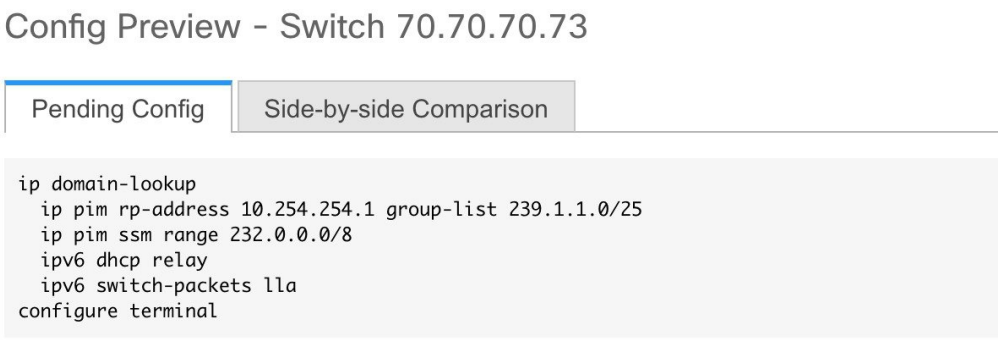
例 1: スイッチの自由形式ポリシーの構成コンプライアンス

スイッチの [自由形式構成（Freeform Config）] フィールドのスペースが正しくない例を考えてみましょう。

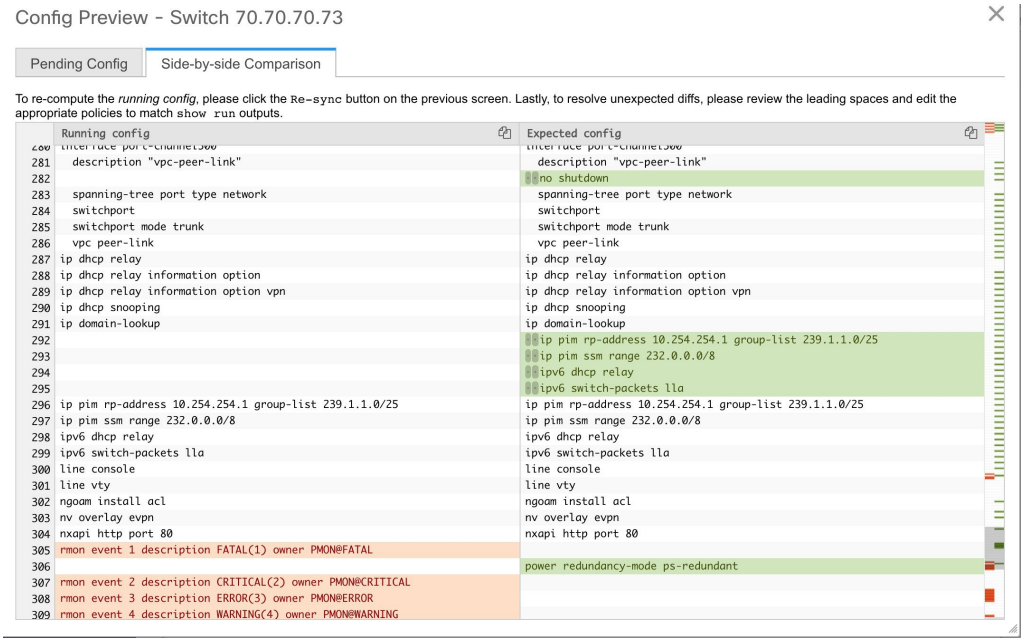
スイッチ自由形式ポリシーは、次のように作成されます。



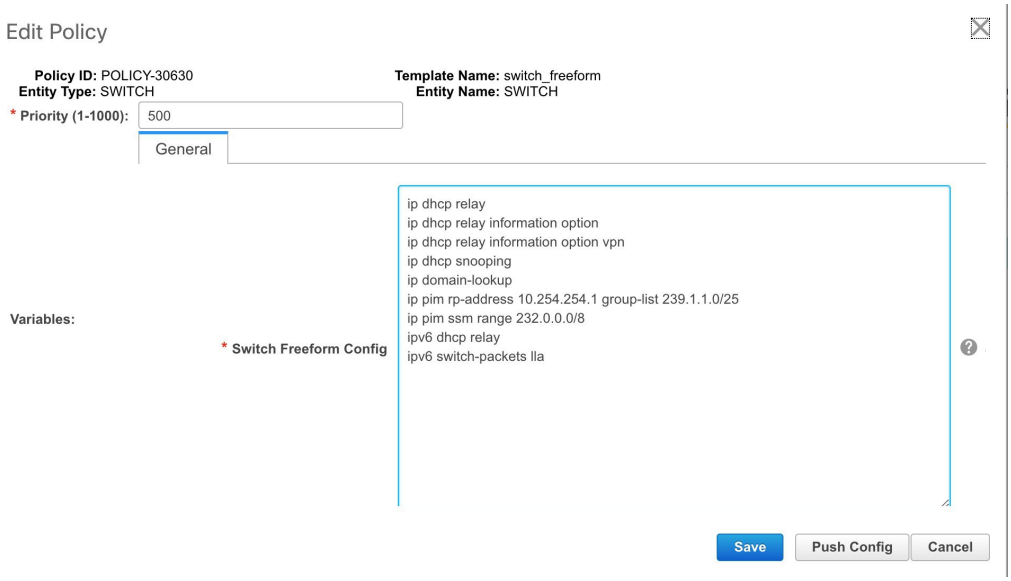
このポリシーがスイッチに正常に展開されると、DCNM は次のように永続的に差分をレポートします。



[並列比較（Side-by-side Comparison）] タブをクリックすると、差分の原因を確認できます。以下のように、**[ip pim rp-address]** 行の先頭には 2 文字のスペースがありますが、実行構成の先頭にはスペースがありません。

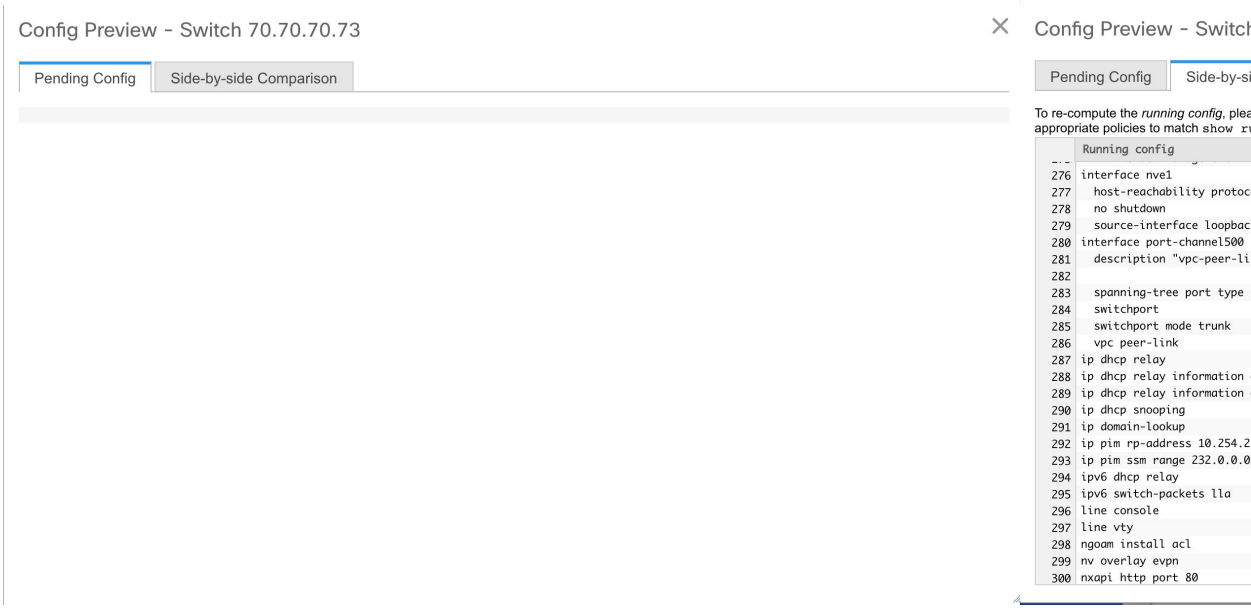


この相違を解決するには、対応するスイッチの自由形式ポリシーを編集して、スペースを合わせます。



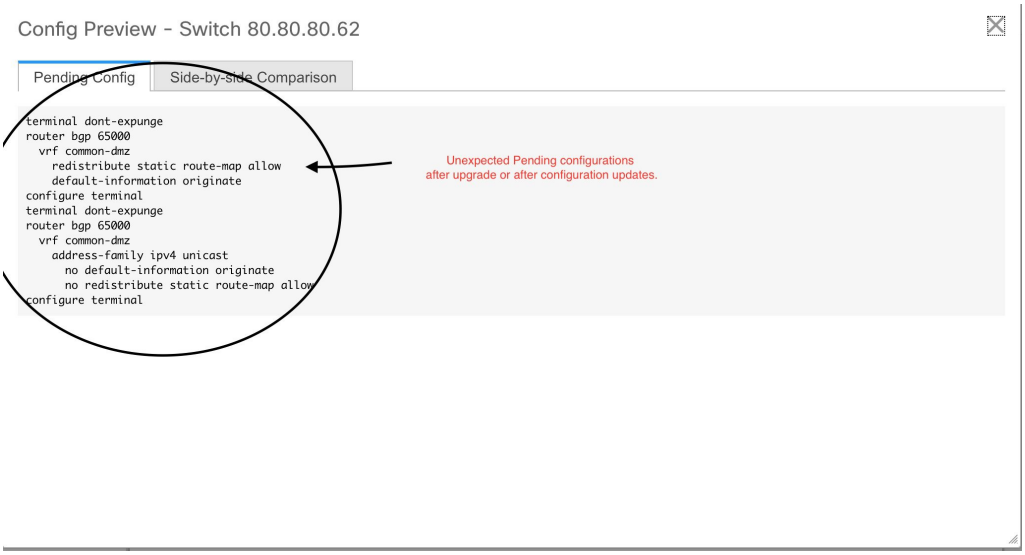
保存後、**[構成のプッシュ（Push Config）]** または **[保存と展開（Save & Deploy）]** オプションを使用して差分を再計算します。

以下に示すように、差分が解決されたことがわかります。**[並列比較（Side-by-side Comparison）]** タブで、先頭のスペースが更新されていることを確認します。

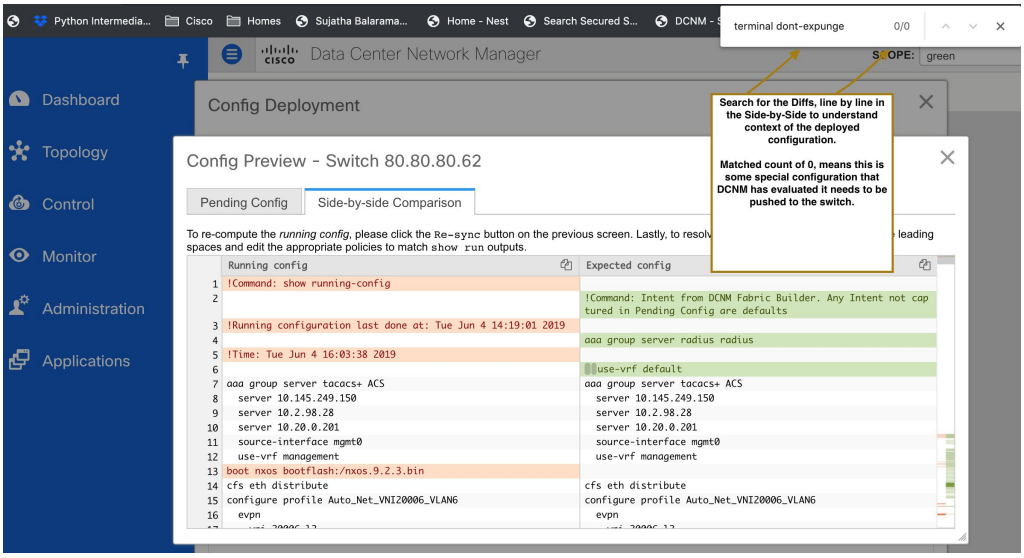


例 2：オーバーレイ構成での先頭スペース エラーの解決

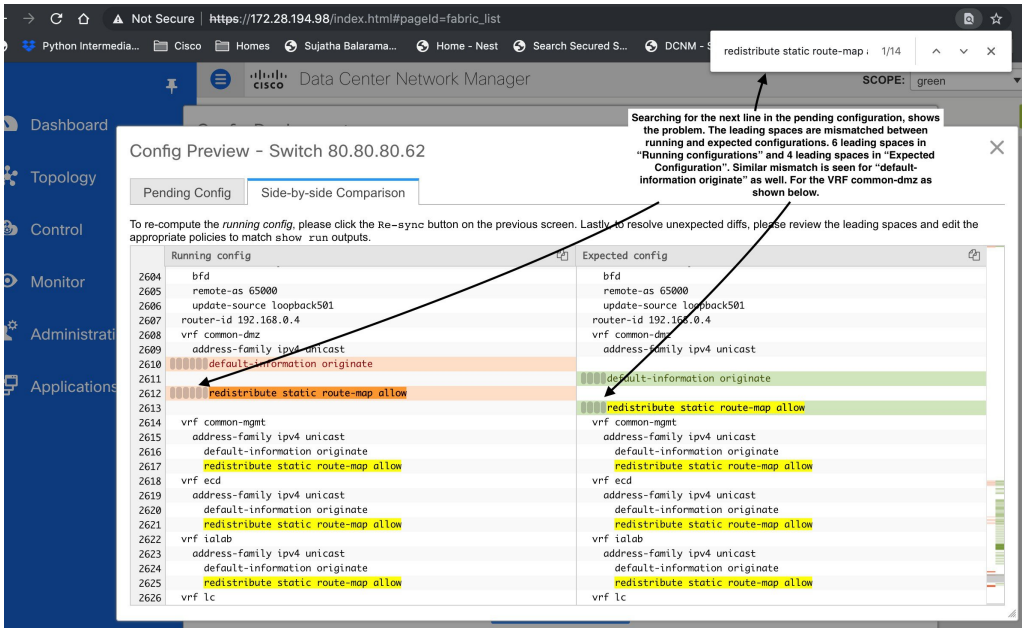
[保留中の構成（Pending Config）] タブに表示される先頭スペース エラーの例を考えてみましょう。



[並列比較（Side-by-side Comparison）] タブで、展開された構成のコンテキストを理解するために、行ごとの差分を検索します。

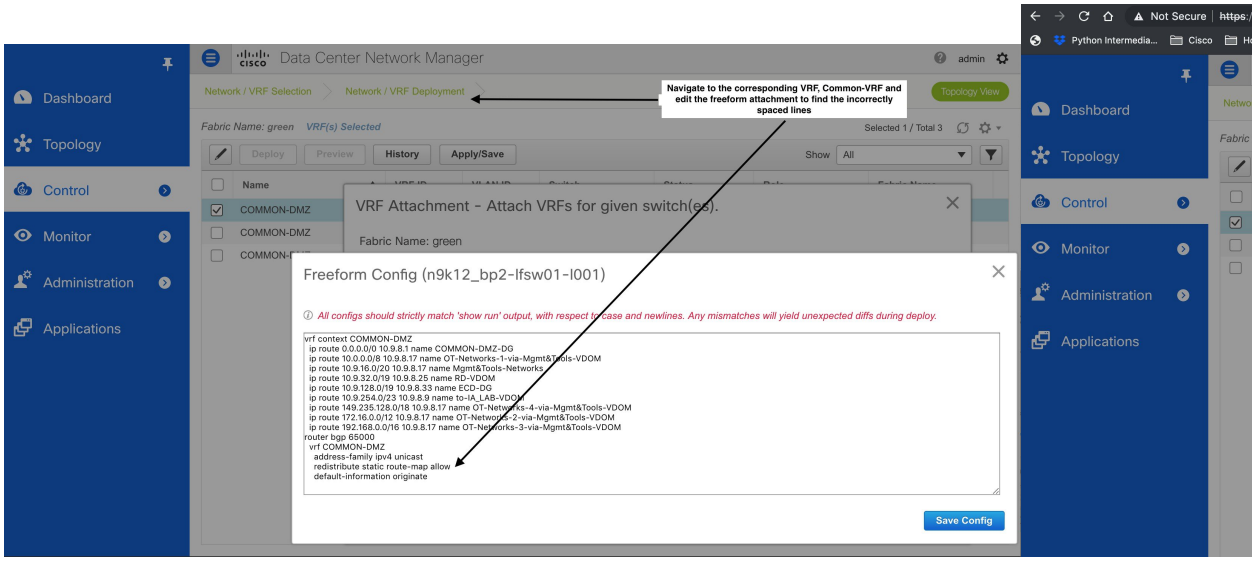


一致数が 0 の場合は、DCNM がスイッチにプッシュするために評価した特別な構成であることを意味します。



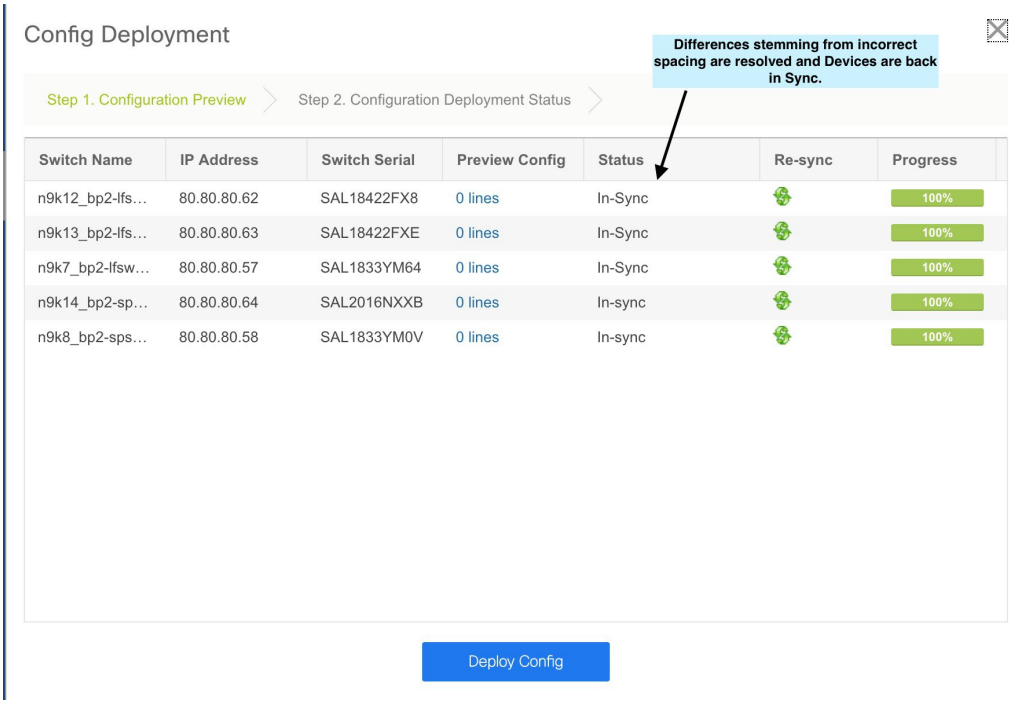
実行中の構成と期待される構成の間で、先頭のスペースが一致していないことがわかります。

それぞれの自由形式の構成に移動し、先頭のスペースを修正して、更新された構成を保存します。



ファブリックの **[ファブリック ビルダ（Fabric Builder）]** ウィンドウに移動し、**[保存と展開（Save & Deploy）]** をクリックします。

[構成展開（Config Deployment）] ウィンドウで、すべてのデバイスが同期していることがわかります。



外部ファブリックでのコンプライアンスの構成

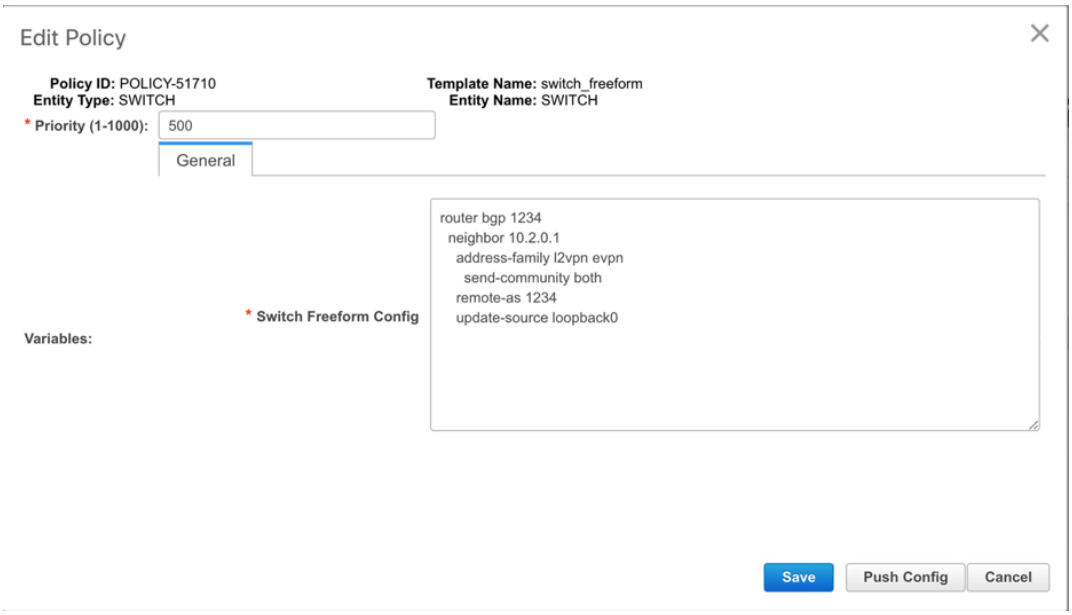
外部ファブリックを使用すると、Nexus スイッチをファブリックにインポートできます。展開のタイプに制限はありません。LAN クラシック、VXLAN、FabricPath、vPC、HSRP などを使用できます。スイッチが外部ファブリックにインポートされるとき、非中断となるようにスイッチの設定が保持されます。スイッチユーザ名やmgmt0インターフェイスなどの基本ポリシーのみが、スイッチのインポート後に作成されます。

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 **IN-SYNC** に変更するために生成された保留中の構成があります。スイッチ上にあるが、DCNM で定義されたインテントではない追加の構成は、インテント内の構成との競合がない限り、CC によって無視されます。

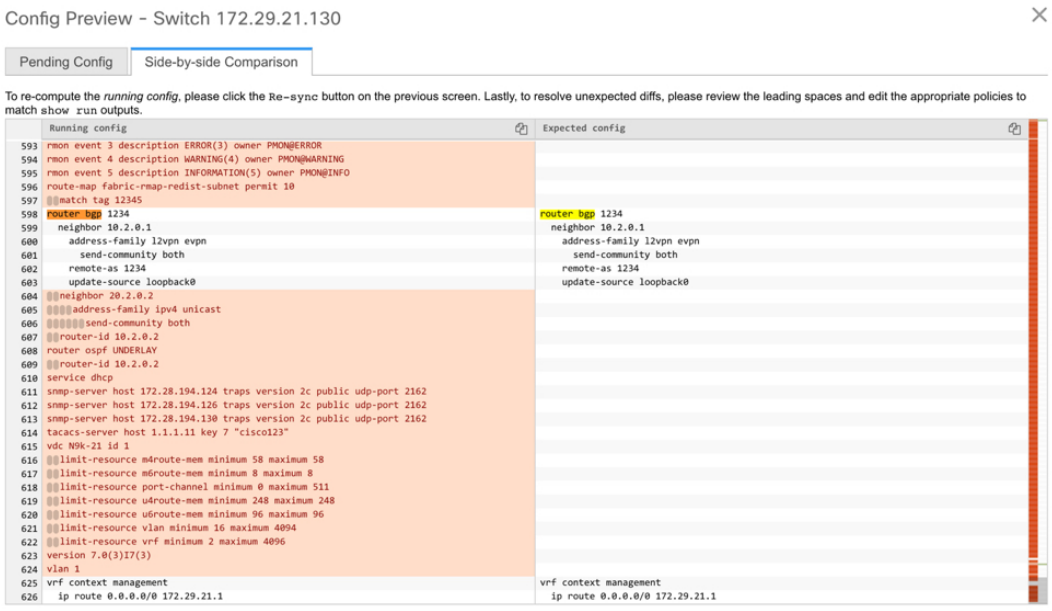
前述のように、ユーザー定義のインテントが DCNM に追加され、同じトップレベル コマンドの下にスイッチの追加構成がある場合、CC は DCNM で定義されたインテントがスイッチに存在することのみを確認します。DCNM 上のこのユーザー定義インテントがスイッチから削除する目的で全体として削除され、対応する構成がスイッチに存在する場合、CC はスイッチの **OUT-OF-SYNC** ステータスをレポートし、**保留中の構成** を作成してスイッチからその構成を削除します。この保留中の設定には、トップレベルのコマンドの削除が含まれています。このアクションにより、このトップレベルコマンドでスイッ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。

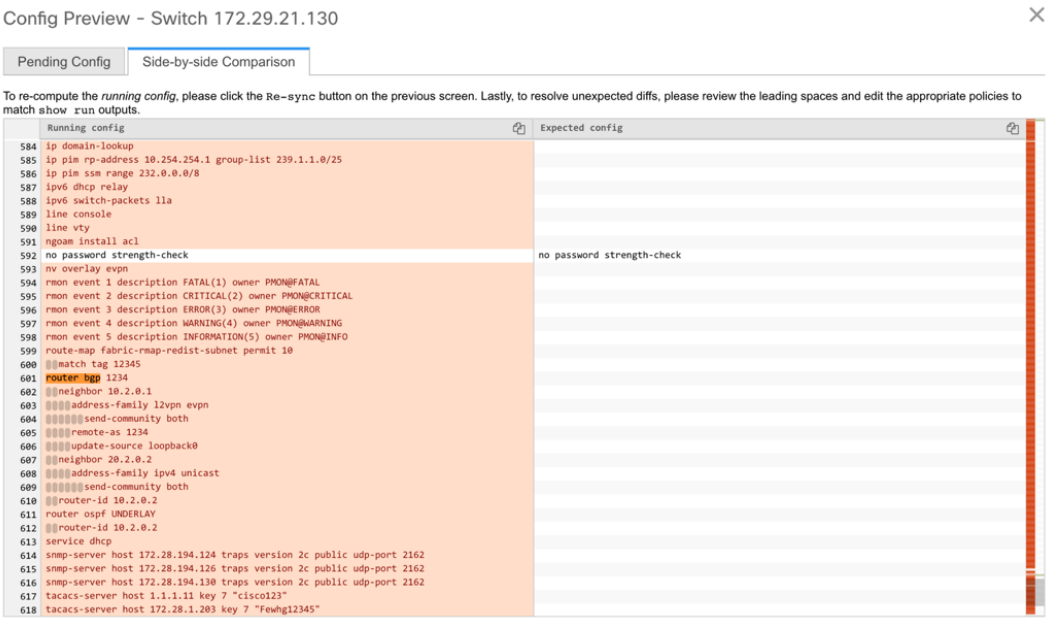
1. **switch_freeform** ポリシーはユーザーによって DCNM に定義され、スイッチに展開されています。

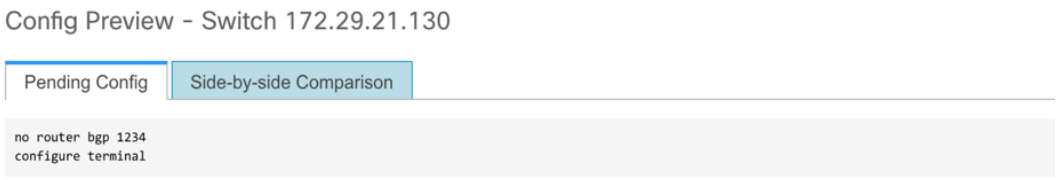


2. **実行構成** の **ルータ bgp** の下に、ユーザー定義 DCNM インテントの **予期される構成** に存在しない追加構成があります。DCNM でユーザー定義のインテントなしでスイッチに存在する追加の構成を削除する **保留中の構成** はありません。

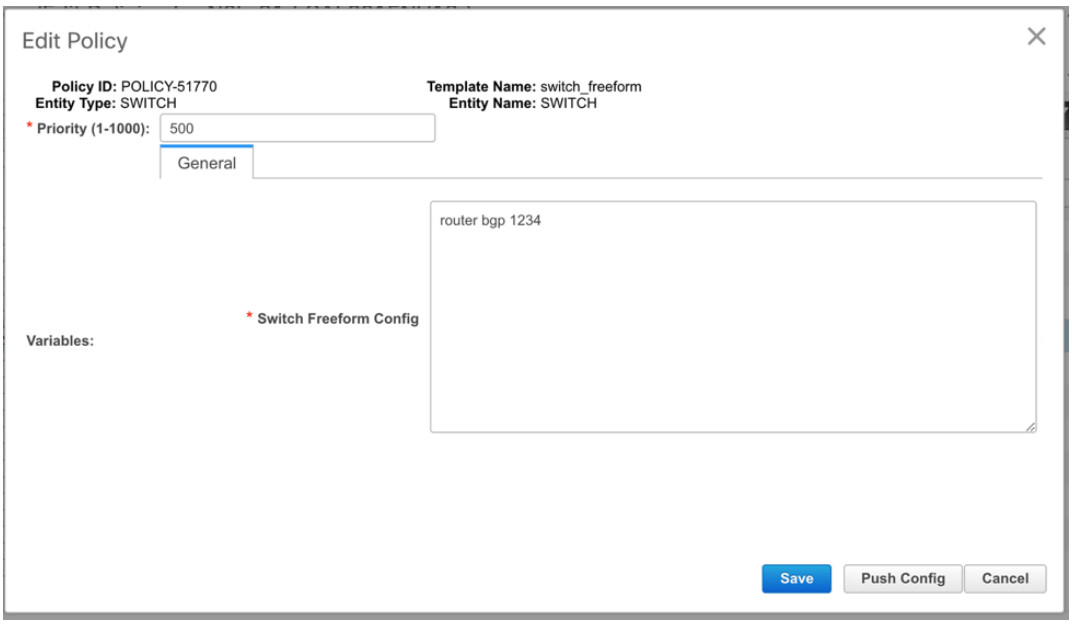


3. 手順 1 で作成された switch_freeform ポリシーを削除することで、DCNM によって以前にプッシュされたインテントが DCNM から削除された場合の **[保留中の構成（Pending Config）]** と **[サイドバイサイド比較（Side-by-side Comparison）]**。

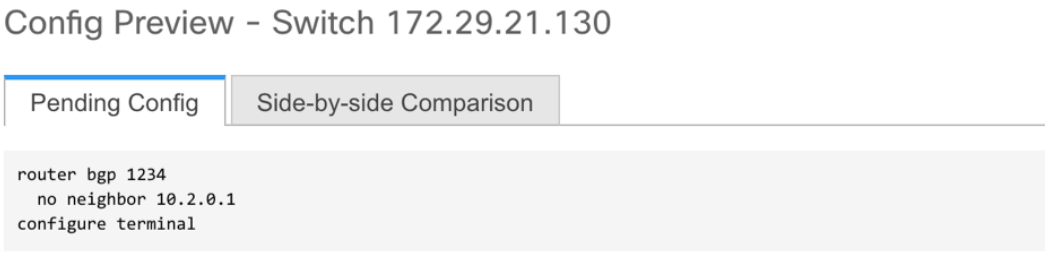


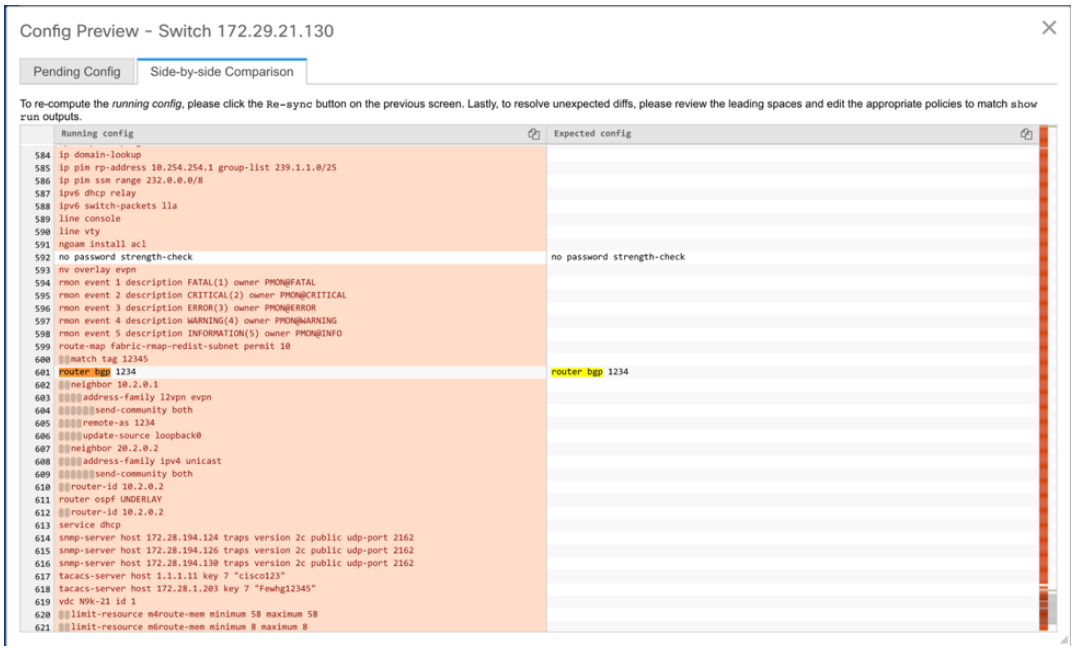


4. 最上位のrouter bgpコマンドを使用してswitch_freeformポリシーを作成する必要があります。これにより、CC は以前に DCNM からプッシュされた目的のサブ構成のみを削除するために必要な構成を生成できます。



5. 削除された構成は、以前に DCNM 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、DCNM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DCNM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でも、モニタポリシーはDCNMに常に関連付けられています。この場合、CC は **[IN-SYNC]** または **[OUT-OF-SYNC]** 構成コンプライアンス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（Fabric Builder）]** ウィンドウで **[保存と展開（Save & Deploy）]** をクリックしても、そのような構成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（Side-by-side Comparison）]**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. **[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** を選択し、**[表形式ビュー（Tabular View）]** をクリックして、**[名前（Name）]** 列でスイッチを選択する、または、**[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** を選択してデバイスを右クリックします。
2. **[ポリシーの表示/編集（View/Edit Policies）]** をクリックして、**[+]** をクリックして新しいポリシーを追加します。**[ポリシーの追加（Add Policy）]** ウィンドウが表示されます。
3. **[switch_freeform]** テンプレートを使用して、必要な構成 CLI を含む PTI を追加し、**[保存（Save）]** をクリックします。
4. 作成したポリシーを選択し、**[構成をプッシュ（Push Config）]** をクリックして、構成をスイッチに展開します。

大文字と小文字を区別しないコマンドの差分の解決

デフォルトでは、インテントを比較する際に DCNM で生成されるすべての差分（予期される構成と実行構成の差分）では、大文字と小文字が区別されます。ただし、スイッチには大文字と小文字を区別しないコマンドも多くあるため、これらのコマンドで相違点が存在するとしてフラグを付けるのは適切でない場合があります。これらの外れ値は、**compliance_case_insensitive_clis.txt** テキスト ファイルにキャプチャされます。

既存の **compliance_case_insensitive_clis.txt** ファイルに含まれていない追加のコマンドは、大文字と小文字を区別するものとして扱うべきです。構成の保留が、DCNM が予期している構成と実行構成との間の大文字と小文字の違いによって生じたものである場合、次の方法で、大文字と小文字の違いを無視するように DCNM を構成できます。

1. DCNM ファイル システムで次のファイルを変更します。

   `/usr/local/cisco/dcm/dcnm/model-config/compliance_case_insensitive_clis.txt`

   compliance_case_insensitive_clis.txt ファイルのサンプル エントリが次のように表示されます。

```
[root@dcnm98 model-config]# pwd
/usr/local/cisco/dcm/dcnm/model-config
[root@dcnm98 model-config]# cat compliance_case_insensitive_clis.txt
"^(no |)interface\s+Port(.)"
"^(no |)interface\s+Loo(.)"
"^(no |)interface\s+Eth(.)"
"^update-source\s+Loo(.)"
"^vrf\s+"
"^hardware profile portmode\s+"
"^(.*)route-map\s+(.)"
"^(.*)neighbor-policy(.)"
"(no |)encapsulation\s+(.)"
"(.*)alert-group\s+(.)"
"^streetaddress\s+(.)"
"^transport email\s+(.)"
"(no |)action\s+(.)"
"(no|)\s+\d*\s+remark.*"
[root@dcnm98 model-config]#
```

展開中に新しいパターンが検出され、それらが構成の保留をトリガーしている場合、これらのパターンをこのファイルに追加します。パターンは、有効な正規表現パターンである必要があります。

これにより、DCNMは、比較の実行中に、記述された構成パターンを大文字と小文字を区別しないものとして扱うことができます。

2. ファブリックについて、**[保存と展開（Save & Deploy）]** をクリックして、更新された比較出力を表示します。

スイッチのインポート後の構成コンプライアンスの解決

Cisco DCNM にスイッチをインポートした後、管理インターフェイス（mgmt0）の説明フィールドに余分なスペースがあるため、スイッチの構成コンプライアンスが失敗することがあります。

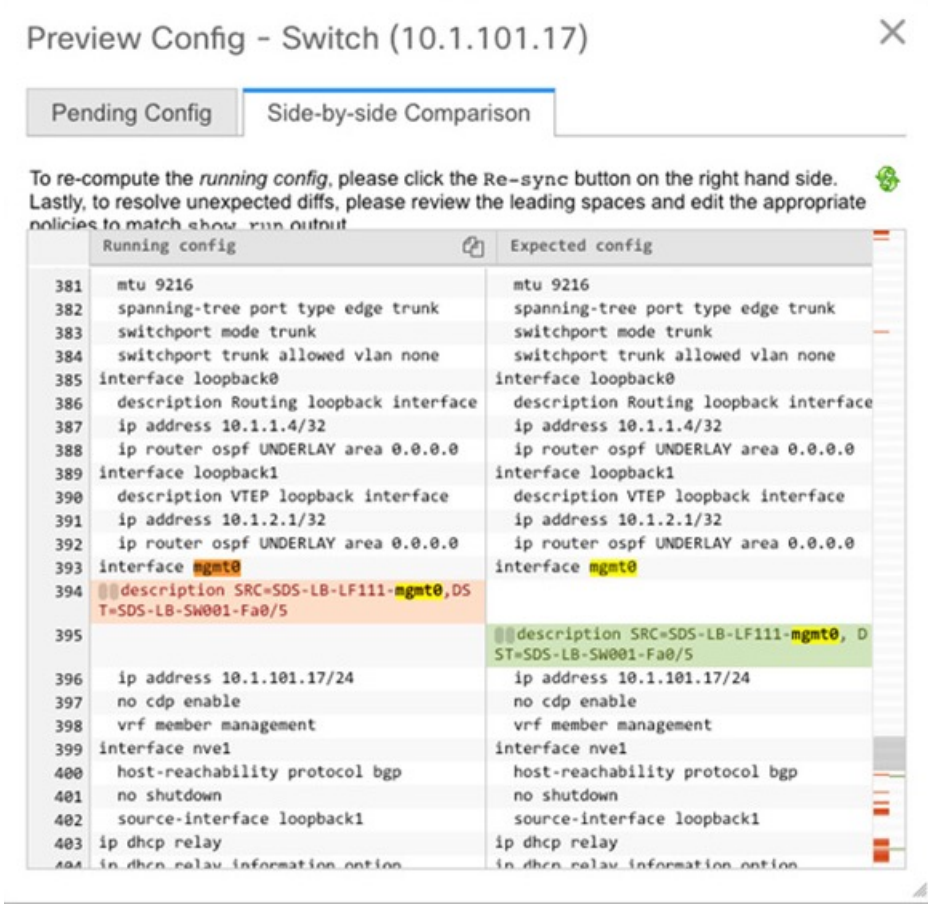
たとえば、スイッチをインポートする前に：

```
interface mgmt0
  description SRC=SDS-LB-LF111-mgmt0, DST=SDS-LB-SW001-Fa0/5
```

スイッチをインポートして構成プロファイルを作成したら、次の手順を実行します。

```
interface mgmt0
  description SRC=SDS-LB-LF111-mgmt0,DST=SDS-LB-SW001-Fa0/5
```

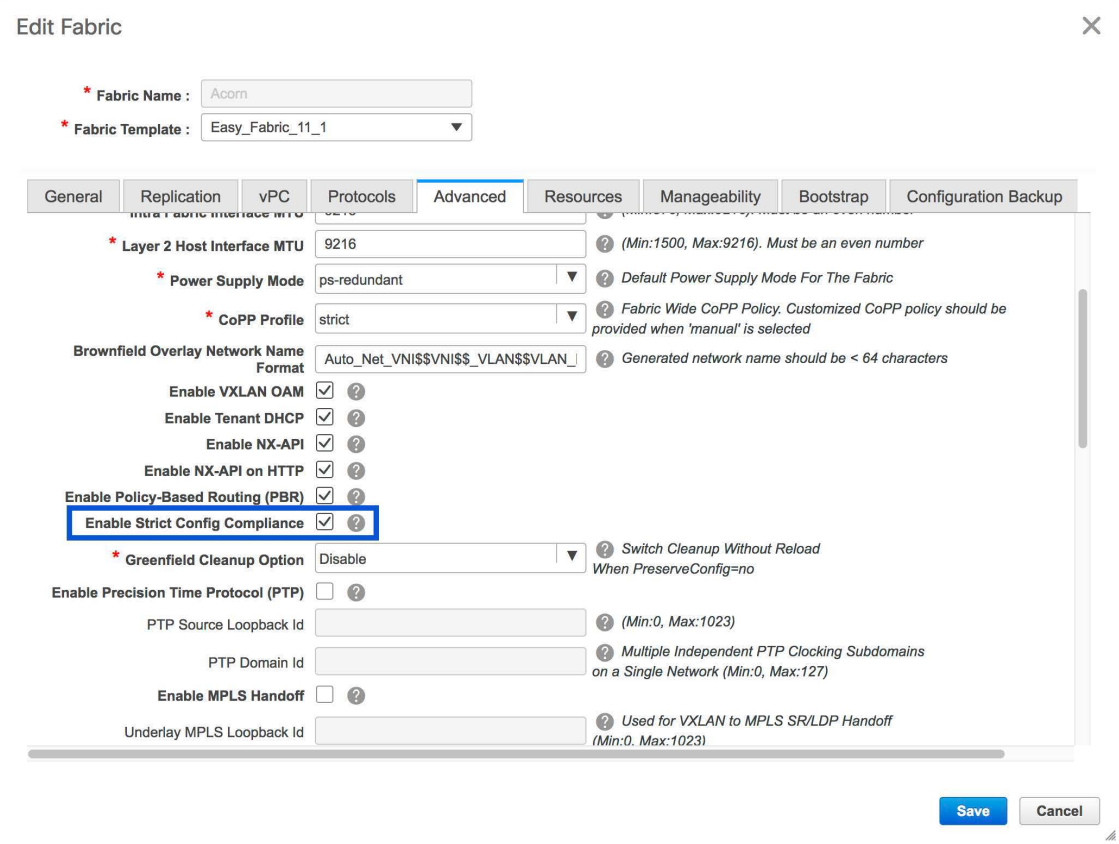
この例では、コンマ（,）の後のスペースが削除されています。



mgmt0インターフェイスを選択した後、インターフェイスマネージャに移動し、**[編集（Edit）]** アイコンをクリックします。説明の余分なスペースを削除してください。

厳密な構成コンプライアンス

Cisco DCNM リリース 11.3(1) から厳密な構成コンプライアンスは、スイッチ構成と関連するインテント間の相違をチェックし、スイッチに存在するが関連するインテントに存在しない構成の **no** コマンドを生成します。**[保存して展開（Save and Deploy）]** をクリックすると、関連付けられたインテントに存在しないスイッチ構成が削除されます。この機能を有効にするには、**[厳密な公正コンプライアンスを有効にする（Enable Strict Config Compliance）]** チェックボックスをオンにします。これは **[詳細設定（Advanced）]** タブ（**[ファブリックの追加（Add Fabric）]** または **[ファブリックの編集（Edit Fabric）]** ウィンドウ）にあります。デフォルトで、この機能は無効になっています。



厳密な構成コンプライアンス機能は、Easy Fabric テンプレート（Easy_Fabric_11_1 および Easy_Fabric_eBGP）でサポートされています。スイッチによって自動生成されるコマンド（vdc、rmon など）について差分が生成されないようにするために、CC はデフォルトのコマンドのリストを含むファイルを使用して、これらのコマンドに対して差分が生成されないようにします。このファイルは、**/usr/local/cisco/dcm/dcnm/model-config/strict_cc_exclude_clis.txt** にあります。

（注）

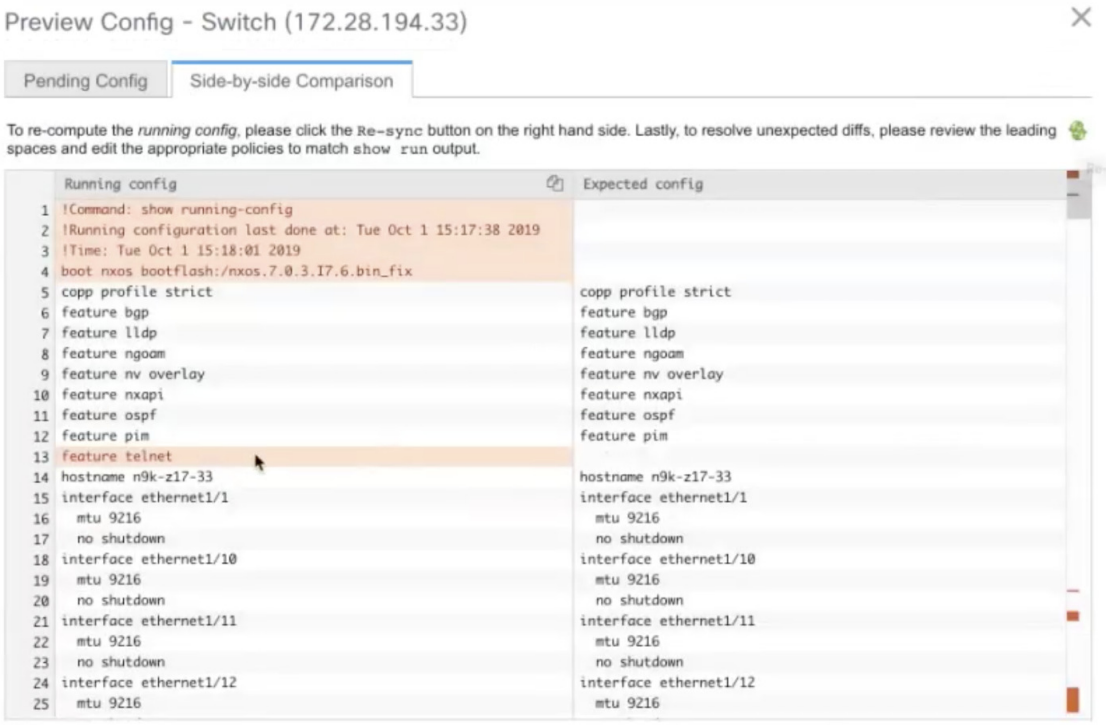
- 厳密な構成コンプライアンスを有効にした後に差分が生成された場合、**[ファブリック ビルダー（Fabric Builder）]** ウィンドウでスイッチアイコンが青色に変わります。

例：厳密な構成コンプライアンス

コマンドがスイッチで構成されているが、インテントに存在しない例を考えてみましょう。**feature telnet** このようなシナリオでは、CC チェックが実行された後、スイッチのステータスが**非同期**として表示されます。

次に、非同期スイッチの **[構成のプレビュー（Preview Config）]** をクリックします。厳密な構成コンプライアンス機能が有効になっているため、**[構成のプレビュー（Preview Config）]** ウィンドウの **[保留中の構成（Pending Config）]** の下に **feature telnet** コマンドの **no** 形式が表示されます。

[並べて比較（Side-by-Side Comparison）] タブには、実行構成と予想される構成の差が並べて表示されます。Cisco DCNM リリース 11.3(1)から**[再同期（Re-sync）]** ボタンは、構成のプレビューウィンドウの [並べて比較（Side-by-Side Comparison）] タブの右上隅にも表示されます。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 DCNM 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 DCNM 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、DCNMで定義されたインテントに基づいて再計算されます。

次に、**[構成のプレビュー（Preview Config）]**ウィンドウを閉じ、**[保存と展開（Save and Deploy）]**をクリックします。厳密な構成コンプライアンス機能により、**feature telnet** コマンドの **no** 形式をスイッチにプッシュすることによって、スイッチの実行構成がインテントから逸脱しないようにします。構成間の相違が強調表示されます。**feature telnet** コマンド以外の差分は、デフォルトのスイッチ構成およびブート構成であり、厳密なCCチェックでは無視されます。

Cisco DCNMリリース11.2(1)以前のリリースでは、[ファブリックのビルダー（Fabric Builder）]ウィンドウでスイッチを右クリックし、**[構成を展開（Deploy Config）]**を選択して**[構成展開（Config Deployment）]**ウィンドウを表示する必要がありました。次に、特定のスイッチの**[構成のプレビュー（Preview Config）]**をクリックして、そのスイッチの保留中の構成を表示する**[構成のプレビュー（Preview Config）]**ウィンドウを表示する必要がありました。これにより、ユーザは、プレビュー構成が誤ってスイッチに展開されていると考える可能性があります。Cisco DCNMリリース11.3(1)から**[ファブリックのビルダー（Fabric Builder）]**ウィンドウでスイッチを右クリックして**[構成のプレビュー（Preview Config）]**を選択すると、**[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、意図に準拠した構成を実現するためにスイッチにプッシュする必要がある保留中の構成が表示されます。

カスタム自由形式構成を DCNM に追加して、DCNM での目的の構成とスイッチ構成を同一にすることができます。その後、スイッチは同期中ステータスになります。DCNM にカスタム自由形式構成の追加方法の詳細については、「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。

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

DCNM では、次の方法でフリーフォーム ポリシーを使用してカスタム設定を追加できます。

1. ファブリック全体
   - ファブリック内のすべてのリーフ、ボーダー リーフ スイッチ上で一度に。
   - すべてのスパインとボーダー スパイン スイッチで一度に。
2. 特定のスイッチ上で。

リーフ スイッチは、リーフ、境界、および境界ゲートウェイのロールによって識別され、スパイン スイッチは、スパイン、境界スパイン、および境界ゲートウェイ スパインのロールによって識別されます。

Note 自由形式の CLI は、ファブリックを作成するときでも、ファブリックがすでに作成されているときでも展開できます。次に、既存のファブリックでの例を示します。ただし、これは新しいファブリックを作成するときでも参考にすることができます。

リーフおよびスパイン スイッチ上でのファブリック全体のフリーフォーム CLI の導入

1. **[制御（Control）] > [Fabric Builder]**の順にクリックします。[Fabric Builder] 画面が表示されます。長方形のボックスが各ファブリックを表します。
2. 既存のファブリックにカスタム構成を追加するには、**[ファブリックの編集（Edit Fabric）]** アイコン（長方形のボックスの右上部分）をクリックします。**[ファブリックの編集 (Edit Fabric)]** 画面が表示されます。

   （ファブリックを初めて作成する場合は、**[ファブリックの作成 (Create Fabric)]** をクリックします）。
3. **[詳細設定 (Advanced)]** タブをクリックし、次のフィールドを更新します。

   [リーフのフリーフォーム構成 (Leaf Freeform Config)]：このフィールドでは、ファブリック内のすべてのリーフ、境界リーフ、および境界リーフ スイッチの構成を追加します。

   [スパインのフリーフォーム構成 (Spine Freeform Config)] - このフィールドでは、ファブリック内のすべてのスパイン、境界スパイン、および境界ゲートウェイ スパイン スイッチの構成を追加します。

Note 目的の設定を正しいインデントでコピー アンド ペーストします。Nexus スイッチでの実行コンフィギュレーションを参考にしてください。詳細については、スイッチのフリーフォーム設定エラーの解決, on page 353を参照してください。

4. [保存（Save）] をクリックします。[ファブリック トポロジ (fabric topology)] 画面が表示されます。
5. 画面の右上にある **[保存して展開 (Save & Deploy)]** をクリックして、構成を保存して展開します。

   構成の遵守機能により、これらの CLI で示された目的の設定がスイッチ上に確実に存在するようにします。仮にそれらが削除されるか、ミスマッチが生じた場合には、ミスマッチとしてフラグが付けられ、デバイスが同期外れであることが示されるようにします。

*[*不完全な構成の遵守 *(Incomplete Configuration Compliance)]*：一部の Cisco Nexus 9000 シリーズ スイッチでは、**[保存して展開 (Save & Deploy)]** オプションを使用して保留中のスイッチ構成を構成しても、意図した構成とスイッチ構成の間にミスマッチが生じる場合があります。問題を解決するには、影響を受けるスイッチに **switch_freeform** ポリシーを追加します（「特定のスイッチへのフリーフォーム *CLI* の展開」の項を参照）。たとえば、次の永続的な保留設定を考えてみます。

```
line vty
logout-warning 0
```

上記の設定をポリシーに追加し、更新を保存したら、トポロジ画面で **[保存して展開 (Save and Deploy)]** をクリックして展開プロセスを完了します。

スイッチを同期状態に戻すには、上記の構成を保存した **switch_freeform** ポリシーで追加し、スイッチに展開します。

特定のスイッチへのフリーフォーム CLIの導入

1. **[制御（Control）] > [Fabric Builder]**の順にクリックします。[Fabric Builder] 画面が表示されます。
2. ファブリックを表す長方形のボックスをクリックします。[ファブリック トポロジ（fabric topology）] 画面が表示されます。

Note 新しいファブリックにフリーフォームのCLIをプロビジョニングするには、ファブリックを作成し、そのファブリックにスイッチをインポートしてから、フリーフォームの CLI を展開する必要があります。

3. スイッチ アイコンを右クリックし、**[ポリシーの表示/編集（View/edit policies）]** オプションを選択します。

[ポリシーの表示/編集（View/edit policies）] 画面が表示されます。

4. **[+]** をクリックします。**[ポリシーの追加（Add Policy）]** 画面が表示されます。

   [プライオリティ (Priority)] フィールドで、優先順位はデフォルトで500に設定されます。展開時に上位に表示する必要がある CLI には、（低い番号を指定して）高い優先順位を選択できます。たとえば、機能を有効にするコマンドは、コマンドリストの前に表示されます。

5. **[ポリシー]** フィールドから、**switch_freeform** を選択します。

6. **[フリーフォーム CLI (Freeform Config CLI)]** ボックスで CLI を追加または更新します。

   目的の設定を正しいインデントでコピーアンドペーストします。Nexus スイッチでの実行コンフィギュレーションを参考にしてください。詳細については、スイッチのフリーフォーム設定エラーの解決, on page 353を参照してください。

7. [保存（Save）] をクリックします。

   ポリシーが保存されると、そのスイッチの目的の設定に追加されます。

8. ポリシー画面を閉じます。ファブリック トポロジが再び起動します。

9. スイッチを右クリックし、**[構成の展開（Deploy Config）]** をクリックします。

   [保存して展開（Save ＆Deploy）] オプションは、展開にも使用できます。ただし、**[保存して展開（Save ＆Deploy）]** オプションを使用すると、すべてのファブリック スイッチで意図した構成と実行構成のミスマッチが特定されます。

switch_freeform ポリシー構成：

- ポリシーでは複数のインスタンスを作成できます。
- vPCスイッチペアの場合は、両方のvPCスイッチで一貫した **switch_freeform** ポリシーを作成します。
- **switch_freeform** ポリシーを編集してスイッチに展開すると、（[プレビュー（Preview）] オプションの **[並べて表示（Side-by-side）]** タブで）変更内容を確認できます。

フリーフォーム CLI の設定例

コンソール ラインの設定

この例では、一部のファブリック全体のフリーフォーム設定（すべてのリーフ スイッチとスパイン スイッチ）、および個々のスイッチ設定を展開します。

ファブリック全体のセッション タイムアウトの設定：

```
line console
  exec-timeout 1
```

特定のスイッチのコンソール速度設定：

```
line console
  speed 115200
```

ACL の設定

ACL 設定は通常、ファブリック全体ではなく、特定のスイッチ（リーフ/スパイン スイッチ）で設定されます。スイッチで ACL をフリーフォーム CLIとして設定する場合は、シーケンス番号を含める必要があります。それ以外の場合は、意図した設定と実行での設定が一致しなくなります。シーケンス番号の設定例：

```
ip access-list ACL_VTY
  10 deny tcp 172.29.171.67/32 172.29.171.36/32
  20 permit ip any any
ip access-list vlan65-acl
  10 permit ip 69.1.1.201/32 65.1.1.11/32
  20 deny ip any any

interface Vlan65
  ip access-group vlan65-acl in
line vty
  access-class ACL_VTY in
```

switch_freeform ポリシーでシーケンス番号なしで ACL を構成した場合は、スイッチの実行構成に示されているようにシーケンス番号でポリシーを更新します。

ポリシーを更新して保存したら、デバイスを右クリックし、スイッチごとに**[設定の展開(Deploy Config)]** オプションを選択して設定を展開します。または、ファブリック トポロジ画面 (Fabric Builder 内) の **[保存して展開]** オプションを使用して、ファブリックが構成遵守をトリガーし、構成のミスマッチを解決するようにします。

スイッチのフリーフォーム設定エラーの解決

実行設定を、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フリーフォーム設定にコピーアンドペーストします。フリーフォームの設定は、実行設定とマッチしている必要があります。それ以外の場合、DCNM の構成遵守は、スイッチを非同期としてマークします。

スイッチのフリーフォーム設定の例を見てみましょう。

```
feature bash-shell
feature telemetry

clock timezone CET 1 0
# Daylight saving time is observed in Metropolitan France from the last Sunday in March
 (02:00 CET) to the last Sunday in October (03:00 CEST)
clock summer-time CEST 5 Sunday March 02:00 5 Sunday October 03:00 60
clock protocol ntp

telemetry
  destination-profile
    use-vrf management
```

夏時間に関する強調表示された行は、**show running config** コマンドの出力には表示されないコメントです。したがって、インテントが実行設定とマッチしないため、設定コンプライアンスはスイッチを非同期としてマークします。

クロック プロトコルのスイッチの実行設定を確認します。

```
spine1# show run all | grep "clock protocol"
clock protocol ntp vdc 1
```

フリーフォームの設定に **vdc 1** がないことがわかります。

この例では、実行設定をフリーフォーム設定にコピーアンドペーストします。

更新されたフリーフォーム設定を次に示します。

```
feature bash-shell
feature telemetry

clock timezone CET 1 0
clock summer-time CEST 5 Sunday March 02:00 5 Sunday October 03:00 60
clock protocol ntp vdc 1

telemetry
  destination-profile
    use-vrf management
```

実行設定をコピーアンドペーストして展開すると、スイッチは同期されます。**[保存して展開（Save & Deploy）]** をクリックすると、**[構成プレビュー(Config Preview)]** ウィンドウの **[並べて比較 (Side-by-Side Comparison)]** により、定義済みのインテントと実行中の構成の違いに関する情報を表示します。

VMM ワークロードの自動化

VMM ワークロードの自動化は、VMware 環境で生成されたワークロード用の Cisco の Nexus スイッチでのネットワーク構成の自動化に関するものです。これは、Cisco DCNM リリース 11.4(1) のプレビュー機能です。

この自動化を示すビデオを見ることもできます。「ビデオ：Cisco DCNM での VMM ワークロードの自動化」を参照してください。

vCenter でのネットワークオブジェクトの概要

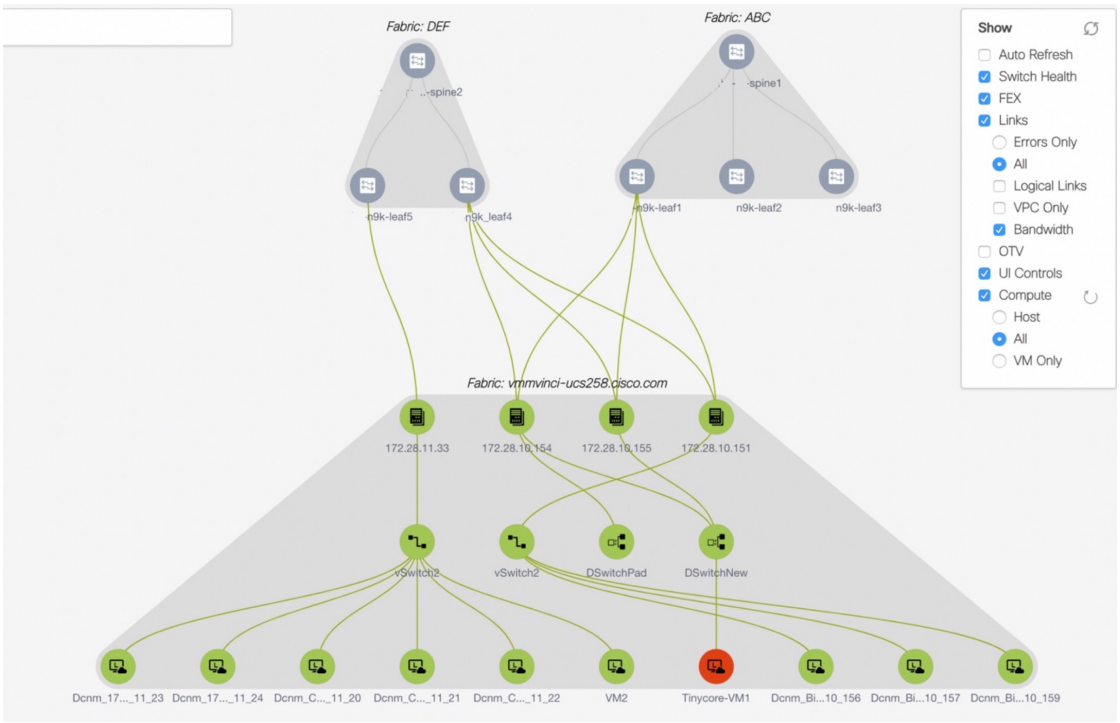
VMM ワークロードの自動化には、vCenter のネットワークオブジェクトを DCNM のネットワークオブジェクトにマッピングすることが含まれます。vCenter の次のネットワークオブジェクトが検討されます。

- 仮想スイッチ（VS）：通常の VS は、ソフトウェア ベースの切り替えを実行する ESXi ホストで実行されます。VS は複数のポート グループ（PG）を持つことができます。各 PG には、VLAN などのネットワークに接続するネットワークポート構成プロパティがあります。各 VS は、リーフスイッチに接続する複数のアップリンクポートを持つことができま

す。ESXi ホストで生成されたワークロードは、この VS で作成された PG に接続できます。

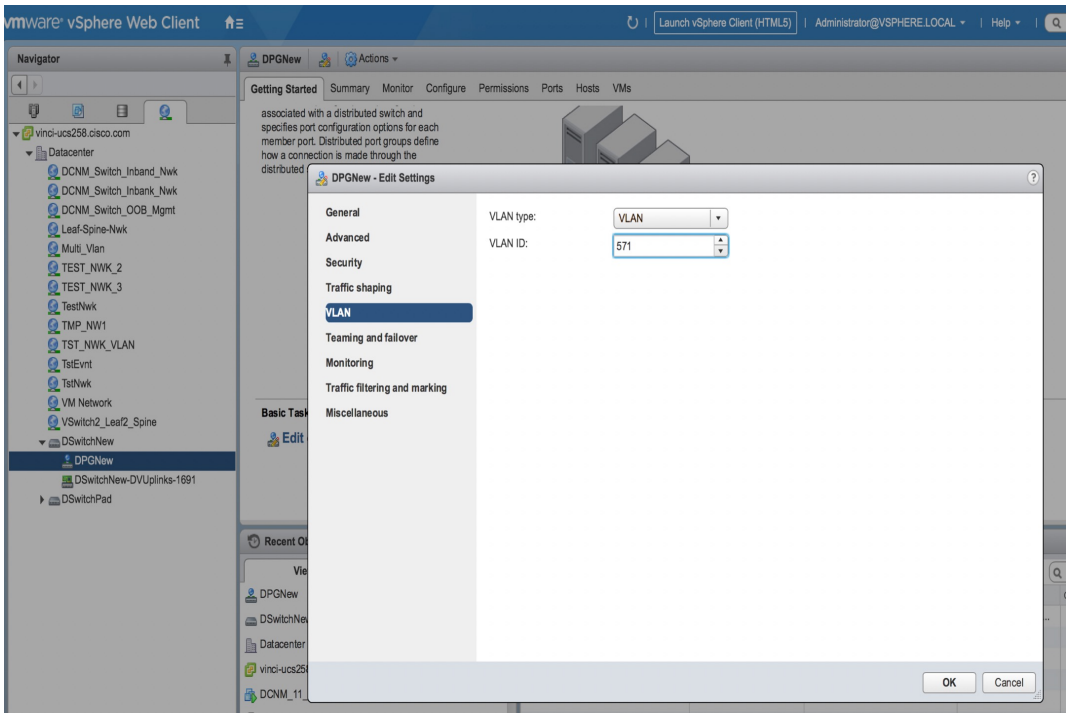
- 分散仮想スイッチ（DVS）：DVS は、複数の ESXi ホストにまたがる仮想スイッチです。通常の VS と同様に、DVS には分散ポート グループ（DPG）と呼ばれる複数のポート グループがあります。DPG には、VLAN など、ネットワークに接続するネットワークポート構成プロパティがあります。各 DVS は、リーフスイッチに接続できる複数のアップリンクポートを持つことができます。DVS のメンバーであるホストのいずれかで生成されたワークロードは、DPG に接続できます。このドキュメントおよび構成ファイルでは、DPG は分散仮想ポートグループ（DV-PG）とも呼ばれます。

DCNM の次のトポロジを考えてみましょう。

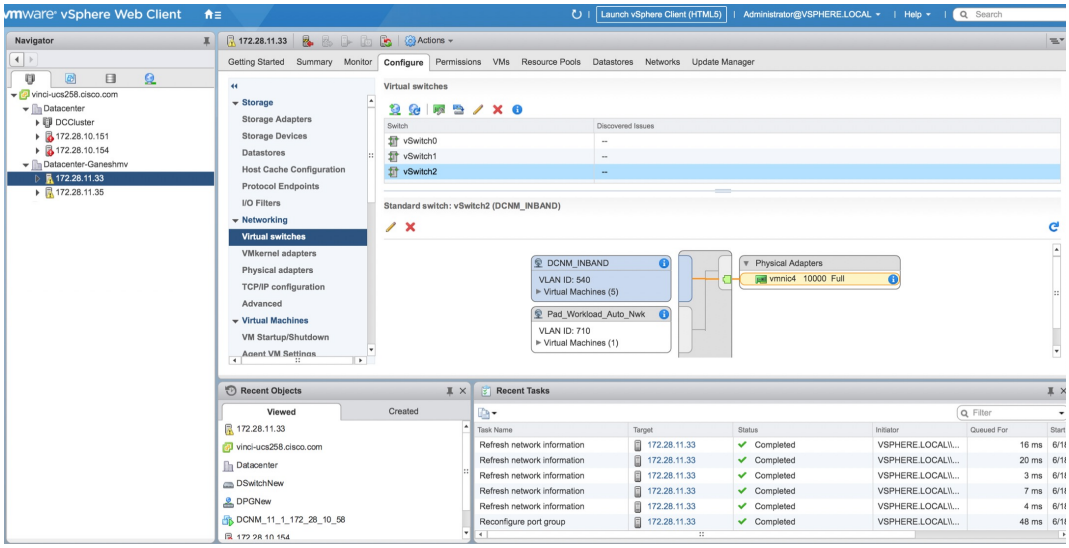


- セットアップには、IP アドレスを持つ 4 つのホストがあります。
  - 172.28.11.33
  - 172.28.10.154
  - 172.28.10.151
  - 172.28.10.155

- **DSwitchNew** という名前の DVS は、ホスト 172.28.10.154 と 172.289.10.155 にまたがって生成されます。この DVS には、図には示されていない **DPGNew** という名前の DPG があります。この DVS は、アップリンクポート <vmnic3, vmnic1> およびスイッチ インターフェイス <e1/25, e1/7> それぞれを介して、スイッチ n9k-leaf1 および n9k-leaf4 に接続します（図には示されていません）。571 の VLAN 値は、**DPG DPGNew** に関連付けられています。



- ホスト 172.28.11.33 には、vSwitch2 という名前の通常の vSwitch もあります。この VS には、DCNM_Inband という名前の PG があります。この VS は、アップリンクポート vmnic4 およびスイッチインターフェイス e1/23 を介してリーフスイッチ n9k-leaf5 に接続します。540 の VLAN 値は、PG **DCNM_Inband** に関連付けられています。



VMM ワークロード自動化の仕組み

ワークロードが生成されると、ネットワークまたはファブリックでのプロビジョニングが必要になります。vCenter で生成されたワークロードは、DPG または PG に関連付けられています。VMWare 内のこの DPG または PG は、対応する DCNM ネットワークにマッピングする必要が

あります。以前のトポロジの例として、ワークロードが PG **インバンド** を備えたホスト 172.28.11.33 で生成された場合、オーバーレイおよびアンダーレイ構成を含むネットワーク プロビジョニングは、関連するインターフェイス e1/23 を備えたリーフスイッチ n9k-leaf5 で発生する必要があります。

ネットワーク プロビジョニングを行うには、vCenter（DPG または PG）の各ネットワークオブジェクトを DCNM のネットワークオブジェクトにマッピングする必要があります。DCNM のネットワークオブジェクトには、次の特性があります。

- VRF Name
- VLAN ID
- IPv4/IPv6 サブネットおよびゲートウェイ情報
- セカンダリ IPv4/v6 およびゲートウェイ情報
- BGP-EVPN 構成

静的マッピングは、vCenter のネットワーク オブジェクトを DCNM のネットワーク オブジェクトにマッピングする構成ファイルで定義する必要があります。詳細については、VMM ワークロード自動化の構成ファイル （358 ページ）を参照してください。

構成ファイルにデータが入力されたら、ワークロード自動化モジュールを開始できます。このモジュールは、構成ファイル（conf.yml）で指定されたすべての vCenter をスキャンし、vCenter ごとに次の情報を収集します。

- すべてのデータセンターで構成されている DVS と DPG のリスト。
- すべてのデータセンターのすべてのホストで構成されている PG のリスト。
- 構成ファイルで指定されたすべての DPG または PG について、構成された VLAN と直接接続されたネイバー スイッチをそのインターフェイス情報と共に検索します。
- 構成ファイルで指定されている <DVS, DPG> または <Host, PG> はそれぞれ、DCNM で関連付けられたネットワークマッピングを取得します。

モジュールはすべての情報をマージし、DCNM API を呼び出して、前の手順のいずれかでネイバーとして検出されたすべてのスイッチのネットワークをプロビジョニングまたは修正します。

ネットワークまたはファブリックのプロビジョニングは、DCNM トップダウン プロビジョニングを使用し、次の手順で構成されます。

1. ネイバーとして検出された 1 つ以上のスイッチの関連インターフェースにネットワーク構成をアタッチします。このアタッチメントは、ワークロード自動化モジュールによって行われます。
2. 構成がアタッチされた後、スイッチにプッシュされた正確な CLI を確認できます。
3. 確認後、構成をスイッチに展開できます。この展開は、構成ファイルの設定に基づいてスクリプトで実行するか（デフォルトは **False**）、DCNM を介して実行できます。この手順の後、構成がスイッチに表示されます。

詳細については、https://pypi.org/project/vmm-workload-auto/ を参照してください。

VMM ワークロード自動化の構成ファイル

VMM ワークロードの自動化には、次の構成ファイルが使用されます。

- グローバル YML ファイル（conf.yml）：このファイルには、DCNM および vCenter のグローバル構成とアクセスまたは認証情報が含まれています。また、各 DCNM の CSV ファイルの場所は、このファイルで指定されます。詳細については、VMM ワークロード自動化の構成ファイル （358 ページ）を参照してください。
- CSV ファイル（sample.csv）：このファイルは、vCenter の <DVS, DVS-PG> または <Host, PG> DCNM を DCNM のネットワーク名にマッピングします。DCNM ごとに個別の CSV ファイルがあります。詳細については、vCenter および DCNM のネットワークのマッピング用 CSV ファイル （359 ページ）を参照してください。

DCNM および vCenter のマッピング用構成ファイル

構成ファイル（conf.yml）は、DCNM の IP アドレス、ユーザー名、およびパスワードを指定します。DCNM ごとに、IP アドレス、ユーザー名、パスワードなどの vCenter 情報のリストも指定されます。この conf.yml ファイルでは、複数の DCNM を指定できます。すべての DCNM インスタンスには、関連付けられた CSV ファイルがあります。マルチ DCNM の場合は、スクリプトが DCNM で実行されず、構成ファイルで指定されたすべての DCNM および vCenter に接続できるサーバーで実行される場合にのみ適用されます。

構成ファイルで指定する情報の階層は以下のとおりです。

```
Global config parameters
DCNM1
      DCNM1 config parameters including location of the CSV file
 vCenter1
  vCenter1 config parameters
  …
 vCenter2
              vCenter2 config parameters
  ….
DCNM2
       ….
  …
```

この構成ファイルの場所は、VMM ワークロード自動化スクリプトのインストール方法によって異なります。詳細については、VMM ワークロード自動化スクリプトのインストールを参照してください。このファイルには、サンプルエントリが含まれています。使用環境に合わせて変更してください。

構成ファイルには次のエントリがあります。

LogFile：ワークロード自動化モジュールがエラーとデバッグ情報を記録するために使用する絶対パスを含むログファイルの名前を指定します。ディレクトリにログファイルを作成するための書き込み権限があることを確認してください。たとえば、/tmp/workloadauto.log です。

ListenPort：ワークロード自動化モジュールが REST API をリッスンするために使用するポート（9590など）を指定します。このポートが他のアプリケーションによって使用されていないことを確認してください。**sudo netstat -tulpn** コマンドを実行して同じことを確認できます。

AutoDeploy：ネットワークを接続した後、スクリプトがスイッチに構成を自動的に展開するかどうかを指定します。デフォルトでは、構成を確認してDCNMに展開できるように**False**に設定されています。

NwkMgr：DCNM 情報を含むトップレベル セクションを指定します。複数の DCNM インスタンスの場合は、適切な値でフィールドを繰り返します。例については、複数の DCNM を処理する conf_multiple_dcnm.yml ファイルを参照してください。

Ip：DCNM の IP アドレスを指定します（例：172.28.10.156）。

User：DCNM へのログインに使用するユーザー名を指定します（例：admin）。

Password：DCNM のパスワードを指定します。

CsvFile：この DCNM の CSV ファイルの場所の絶対パスを指定します。
（例：/etc/vmm_workload_auto/sample.csv）

ServerCntrlr：サーバー コントローラ、つまり vCenter/vSphere の情報を指定します。この DCNM に該当する複数の vCenter については、このセクションが繰り返されます。例については、DCNM の下に複数の vCenter が含まれている conf_multiple_vcenter.yml ファイルを参照してください。

Ip：vCenter の IP アドレスを指定します。

タイプ：サーバー コントローラのタイプを指定します。デフォルトは vCenter です。

ユーザー：vCenter へのログインに使用するユーザー名を指しますたとえば、administrator@vsphere.local とします。

パスワード：vCenter のパスワードを指します。

次の例は、conf.yml ファイルの内容を示しています。

```
LogFile: /tmp/workloadauto.log
ListenPort: 9590
AutoDeploy: false
NwkMgr:
- Ip: 172.28.10.151
  User: admin
  Password: C1sco_123
  CsvFile: /etc/sample.csv
  ServerCntrlr:
    - Ip: 172.28.10.194
      Type: vCenter
      User: administrator@vsphere.local
      Password: Cisc0!23
```

vCenter および DCNM の ネットワークのマッピング用 CSV ファイル

CSV ファイルには、vCenter のネットワーク オブジェクトから DCNM で作成されたネットワークへのマッピングが含まれています。このファイルには、次のエントリが CSV 形式で含まれています。つまり、コンマ区切りのエントリです。CSV ファイルを作成する理由は、vSphere

の PG（または DPG）と DCNM のネットワーク名との間のマッピングを指定するためです。1 対 1 のマッピングです。ただし、PG または DPG は単独では識別できない（一意ではない）ため、マッピングするには追加の DVS 名またはホスト名が必要です。

CSV ファイルは、次のフィールドを含みます。

vCenter：vCenter の IP アドレスを指定します

Dvs：DVS の名前を指定します。

Dvs_pg：DVS の DVS PG（DPG）を指定します。

ホスト（Host）：ホスト/サーバー（IP アドレス）を指定します。

Host_pg：ホストのポート グループを指定します。

ファブリック（Fabric）：DCNM のファブリックを指定します。

ネットワーク（Network）：DCNM ですでに作成されているネットワークの名前を指定します。

ネットワーク オブジェクトは、次のいずれかの一意のペアによって識別されます。<DVS, DVS_PG> または <Host, Host_PG>

次の例を考えて見ましょう。

vCenter Params					**DCNM Params**	
vCenter	**DVS**	**DVPortGroup/ネットワーク**	**ESXi ホスト**	**ポート グループ/ネットワーク**	**Fabric Name（ファブリック名）**	**ネットワーク名（Network Name）**
172.28.12.123	DVS1	DPG1			Fab1	ネットワーク 10
172.28.12.123	DVS1	DPG1			Fab2	ネットワーク 30
172.28.12.123			172.28.12.11	PG10	Fab1	ネットワーク 20
172.28.12.123			172.28.12.12	PG20	Fab1	ネットワーク 20

このテーブルには、vCenter 172.28.12.123 のマッピングがあります。次の 4 つのエントリがあります。

- 最初のエントリは、DVS1 の DPG1 について、DCNM のネットワークがファブリック「Fab1」の「Network10」であることを指定します。DVS のホストが複数のファブリックのスイッチに接続できる場合があります。各ファブリックのネットワーク名は異なる場合があるため、ファブリック名も必要です。表の例では、2番目のエントリにそのようなケースの 1 つを示しています。
- 2番目のエントリは同じものを指定します。<DVS1, DPG1>ペアは、ファブリック「Fab2」のネットワーク 30 にマッピングされています。
- 3 番目のエントリは、ホスト 172.28.12.11 の PG10 の場合、DCNM のネットワークがファブリック「Fab1」の「Network20」であることを指定します。

- 4 番目のエントリは、ホスト 172.28.12.11 の PG20 の場合、DCNM のネットワークがファブリック「Fab1」の「Network20」であることを指定します。

前の表に見られるように、ネットワーク オブジェクトは、次のいずれかの一意のペアによって識別されます。<DVS, DVS_PG> または <Host, Host PG> DVS、DVS_PG に指定された値がある場合、<Host, Host_PG> の値はブランクです。つまり、<DVS, DVS_PG> と <Host, Host_PG> は相互に排他的な値です。

上記の表を CSV 形式で指定すると、CSV ファイルでは以下のように表示されます。

```
172.28.12.123,DVS1,DPG1,,,Fab1,Network10
172.28.12.123,DVS1,DPG1,,,Fab2,Network30
172.28.12.123,,,172.28.12.11,PG10,Fab1,Network20
172.28.12.123,,,172.28.12.12,PG20,Fab1,Network20
```

より多くの例を考えてみましょう：

- **172.28.10.184,DSwitchPad,DSPad-PG2,,,DEF,MyNetwork_30000**

  CSV ファイルのこの行では、vCenter の IP アドレスを 172.28.10.184 として指定し、<DVS, DVS PG> 値はそれぞれ DSwitchPad、DSPad-PG2 です。DVS、DVS-PG の値が指定されているため、この例に示すように、Host、Host-PG の値はブランクです。ファブリック名は DEF で、DCNM のネットワークは MyNetwork_30000 です。

- **172.28.10.184,,,172.28.11.33,Pad_Workload_Auto_Nwk,DEF,MyNetwork_60000**

  この例では、<DVS, DVS-PG> はブランクで、値 <Host, Host_PG> は、それぞれ 172.28.11.33 および Pad_Workload_Auto_Nwk として指定されます。DCNM のファブリックは DEF で、DCNM のネットワーク名は MyNetwork_60000 です。

CSV ファイルの例は次のとおりです。

```
vCenter,Dvs,Dvs_pg,Host,Host_pg,Fabric,Network
172.28.10.184,DSwitchNew,DPGNew,,,DEF,MyNetwork_30000
172.28.10.184,DSwitchNew,DPGNew,,,ABC,MyNetwork_30000
172.28.10.184,,,172.28.11.33,Pad_Workload_Auto_Nwk,DEF,MyNetwork_60000
```

VMM ワークロード自動化モジュールのインストールと開始

PIP インストールまたはインストール スクリプトを使用して、VMM ワークロード自動化モジュールをインストールできます。

PIP インストールの使用

始める前に

このインストール方法は、**pip インストール** に精通しており、プロキシの設定方法や Python パッケージで競合が発生した場合の処理方法を知っているユーザー向けです。

手順

ステップ 1 このモジュールを仮想環境で実行するか、物理サーバーで実行するかを決定します。サーバーでこれを実行する場合は、pip インストールを実行するための書き込み権限があることを確認してください。

ステップ 2 http_proxy、https_proxy、および no_proxy を適切に設定します。

次に例を示します。

```
export http_proxy=http://proxy.esl.cisco.com:80
export https_proxy=https://proxy.esl.cisco.com:80
export no_proxy=127.0.0.1,172.28.10.0/24
```

この例では、no_proxy で指定されている 172.28.10.0 が DCNM の管理サブネットです。

ステップ 3 モジュールを https://pypi.org/ からダウンロードしてインストールします。

```
pip3 install vmm-workload-auto
```

同様に、次のコマンドを使用してモジュールをアンインストールできます。**pip3 uninstall vmm-workload-auto**

ステップ 4 デフォルトでは、**pip** コマンドでオプションを指定して上書きしない限り、インストールは次のディレクトリで行われます。

パッケージは以下にインストールされます。`/usr/local/lib/python3.7/site-packages/vmm_workload_auto-0.1.1.dist-info`

構成ファイルは `/usr/local/lib/python3.7/site-packages/etc/vmm_workload_auto` にインストールされます。

ソース コードは `/usr/local/lib/python3.7/site-packages/workload_auto` にあります。

ステップ 5 `/usr/local/lib/python3.7/site-packages/etc/vmm_workload_auto` の構成ファイルを編集します。

詳細については、DCNM と vCenter をマッピングするための構成ファイルを参照してください。

conf.yml ファイルに指定されている CSV ファイルのパスが正しいことを確認してください。

ステップ 6 VMM ワークロード自動化モジュールを開始します。

Python モジュールのエントリ ポイントは、`/usr/local/bin/vmm_workload_auto` です。

次のように実行できます。

```
/usr/local/bin/vmm_workload_auto
```

または

```
vmm_workload_auto
```

/usr/local/bin/ がすでに **$PATH** にある場合。

コマンドライン オプションとして構成ファイルを指定します。

```
/usr/local/bin/vmm_workload_auto
--config=/usr/local/lib/python3.7/site-packages/etc/vmm_workload_auto/conf.yml
```

インストール スクリプトの使用

インストール スクリプトの使用は、**pip install** を使用したくないユーザのための代替方法です。インストール スクリプトはインストールを実行し、Python モジュールを開始します。

手順

ステップ 1 https://pypi.org/project/vmm-workload-auto/ に移動し、 latest.tar.gz ファイルをダウンロードします。

ステップ 2 解凍します。次に例を示します。

```
tar -xvf vmm_workload_auto-0.1.0.tar.gz
```

ステップ 3 config/conf.yml と config/sample.csv を作業環境に合わせて変更します。

ステップ 4 セットアップ スクリプトを「source setup.sh」として実行します。

ステップ 5 インストール スクリプトは、最初に conf.yaml および .csv ファイルを編集するようにユーザに促します。次に、スクリプトは、ユーザにプロキシおよびその他の詳細を求めるプロンプトを表示します。すべてが完了すると、スクリプトは Python パッケージをインストールし、モジュールを自動的に開始します。

ステップ 6 スクリプトのインストールについては、https://pypi.org/project/vmm-workload-auto/ にある README ファイルのインストール セクションを参照してください。

インストール後

ワークロード自動化モジュールを実行したら、DCNM ネットワーク ウィンドウに移動して、ネットワーク接続が完了しているかどうかを確認します。構成ファイル（conf.yml）で **AutoDeploy** が **false** に設定されている場合は、構成を確認して展開します。

REST API を使用する追加の機能

ワークロード自動化モジュールは、次の REST API も提供します。

（注） REST API は、VMM ワークロード自動化モジュールの実行後に別のウィンドウで実行されます。REST API を実行する前に、自動化モジュールが実行されていることを確認してください。

- 更新：CSV ファイルが変更された場合、更新操作を実行する必要があります。この操作により、ファイルが再読み取りされ、必要に応じて新しい構成が適用されます。更新 API は次のとおりです。

```
curl -XPOST http://127.0.0.1:{port}/workload_auto/refresh
```

- 再同期：DVS-PG、PG、VLAN、またはネイバー スイッチに変更がある場合は、再同期操作が必要です。変更が見つかった場合、それに応じて構成が再適用されます。再同期 API は次のとおりです。

```
curl -XPOST http://127.0.0.1:{port}/workload_auto/resync
```

- クリーン：モジュールを使用して以前に実行されたネットワーク プロビジョニングをクリーンアップするには、クリーンアップ操作が必要です。クリーン API は次のとおりです。

```
curl -XPOST http://127.0.0.1:{port}/workload_auto/clean
```

vCenter のイベント

DCNM リリース 11.4(1) では、リアルタイム イベント処理はモジュールを使用して実行されません。さまざまな関連イベントと、このモジュールに対するその重要性は次のとおりです。

更新

更新 API により、モジュールは CSV ファイルを再度読み取り、ネットワーク構成を 1 つ以上の関連スイッチに適用できます。更新の操作は、次のイベントに対して実行する必要があります。

- PG の追加：この PG の DCNM で関連付けられたネットワークを指定するエントリを CSV ファイルに作成します。エントリが追加されたら、更新 REST API を呼び出します。
- DPG の追加：この DPG の DCNM で関連付けられたネットワークを指定するエントリを CSV ファイルに作成します。エントリが追加されたら、更新 REST API を呼び出します。

Resync

再同期 API により、モジュールはネットワーク オブジェクトとその関連プロパティを再度検出できます。この再同期操作の結果として、ネットワーク構成が新規または変更されたスイッチまたはインターフェイスに適用されます。次のイベントに対して再同期操作を実行します。

- DVS へのホストの追加
- DPG または PG の VLAN を変更します。
- トポロジの変更：以下のいずれかの情報が変更された場合は、Resync REST API を発行してトポロジを再検出し、REST API を適用します。
  - ネイバースイッチの変更：これは、接続されているリーフスイッチが新しいスイッチに置き換えられた場合、または別のスイッチに再配線された場合に発生する可能性があります。

- インターフェイスの変更：これは、スイッチ内の別のインターフェイスへの再配線が原因で発生する可能性があります。
- ホスト pNIC の変更。
- 追加の接続を追加：これは、次の場合に発生する可能性があります。
  - ホストの通常のインターフェイスは、ホストからスイッチに追加のインターフェイスを接続することにより、ポートチャネルになります。
  - vPC ペアを形成する別のスイッチに接続するホストの追加インターフェイス。

操作の必要はありません

次のイベントの場合、アクションを実行する必要はありません。

- スタンドアロン ホストを追加します。
- vSwitch を追加します。
- DVS を追加します。
- DVS を削除します。

マッピングの変更

CSV でのマッピング変更のさまざまなシナリオは次のとおりです。

- 新しいマッピングが追加された場合は、CSV ファイルにマッピングを追加した後に更新 API を実行します。
- vCenter ネットワークから DCNM ネットワークへのマッピングを変更する必要がある場合は、クリーンな REST API を実行し、CSV ファイルのマッピングを変更して、更新 REST API を実行します。
- 既存のマッピングを削除する必要がある場合は、クリーンな REST API を実行し、CSV ファイル内のマッピングを削除して、更新 API を実行します。

その他のイベント

カテゴリに属さないその他のイベントと操作は次のとおりです。

- DVS から削除されたホスト：ホストが DVS から削除された場合、関連するリーフスイッチと接続されたインターフェイスのネットワーク構成を削除する必要があります。これは、この DVS のすべての DPG に対して行う必要があります。DCNM に移動し、適切なネットワークを接続解除します。
- DPG または PG の削除：この DPG または PG に関連付けられているスペック ファイルで指定されたすべてのネットワーク マッピングについて、関連するスイッチおよびインターフェイスのネットワーク構成を削除します。DCNM に移動し、適切なネットワークを接続解除します。

- ポート ダウンまたはスイッチ ダウン：ポートまたはスイッチが永続的にオフラインになる場合は、構成をアウトオブバンドで削除する必要があります。スイッチにホストから到達できないが、まだDCNMによって管理されている場合は、DCNMに移動し、適切なネットワークを接続解除します。

管理

管理メニューには、次のサブメニューがあります。

リソース

Cisco DCNM では、リソースを管理できます。次の表で、このページに表示されるフィールドを説明します。

フィールド	説明
スコープタイプ	リソースが管理される範囲レベルを指定します。範囲タイプは、**[ファブリック（Fabric）]**、**[デバイス（Device）]**、**[DeviceInterface]**、**[DevicePair]**、**[ファブリック（Fabric）]**、および **[リンク（Link）]** です。
範囲	リソース使用範囲を指定します。有効な値は、スイッチのシリアル番号またはファブリック名です。シリアル番号を持つリソースは一意であり、スイッチのシリアル番号でのみ使用できます。
リソースの割り当て	リソースをデバイス、デバイス インターフェイス、またはファブリックで管理するかどうかを指定します。有効な値は、ID タイプ、サブネット、または IP アドレスです。
割り当て先	リソースが割り当てられるエンティティ名を指定します。
[リソース タイプ（Resource Type)]	リソース タイプを指定します。有効な値は、**TOP_DOWN_VRF_LAN**、**TOP_DOWN_NETWORK_VLAN**、**LOOPBACK_ID**、**VPC_ID** などです。
割り当てされましたか？	リソースが割り当てられているかどうかを指定します。リソースが特定のエンティティに永続的に割り当てられている場合、値は **True** に設定されます。リソースがエンティティに予約されており、永続的に割り当てられていない場合、値は **False** に設定されます。
割り当て日時	リソース割り当ての日時を指定します。

リソースの割り当て

Cisco DCNM Web UI からリソースを割り当てるには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 リソースを割り当てるファブリックで、**[ファブリックの編集（Edit Fabric）]** アイコンをクリックします。

[ファブリックの編集（Edit Fabric）] ダイアログボックスが表示されます。

（注） または、ファブリック トポロジ ウィンドウから **[ファブリックの編集（Edit Fabric）]** ダイアログボックスに移動できます。**[アクション（Actions）]** ペインで **[ファブリック設定（Fabric Settings）]** をクリックします。

ステップ 3 **[リソース（Resources）]** タブを選択します。

ステップ 4 **[手動アンダーレイ IP アドレスの割り当て（Manual Underlay IP Address Allocation）]** チェックボックスをオフにします。

このチェックボックスをオンにすると、**[リソース割り当て（Resource Allocation）]** ウィンドウを使用して、すべてのリソースに IP アドレスを手動で提供します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 **[制御（Control）] > [管理（Management）] > [リソース（Resources）]** を選択します。

[**リソースの割り当て（Resource Allocation**）] ウィンドウが表示されます。このウィンドウには、選択した範囲の下にあるすべてのリソースが一覧表示されます。

ステップ 7 **[リソースの割り当て（Allocate Resource）]** アイコンをクリックします。

[リソースの割り当て（Allocate Resource）] ダイアログボックスが表示されます。

ステップ 8 ドロップダウン リストからプール タイプ、プール名、およびスコープ タイプを適宜選択します。

プール タイプのオプションは、**[ID]**、**[IP]**、および **[SUBNET]** です。選択したプールタイプに基づいて、**[プール名（Pool Name）]** ドロップダウン リストの値が変更されます。

ステップ 9 **[シリアル番号（Serial Number）]** ドロップダウンリストから、シリアル番号を選択します。

このフィールドは、ファブリック範囲タイプを除くすべての範囲タイプに表示されます。

ステップ 10 **[エンティティ名（Entity Name）]** フィールドにエンティティ名を入力します。

組み込みヘルプには、さまざまなスコープ タイプの名前の例が示されています。

ステップ 11 **[リソース（Resource）]** フィールドに ID、IP アドレス、またはサブネットを入力します。ステップ *3* で選択したプール タイプに従う必要があります。

ステップ 12 **[保存（Save）]** をクリックしてリソースを割り当てます。

リソース割り当ての例

例 1：IP を loopback 0 と loopback 1 に割り当てる

```
#loopback 0 and 1
    L0_1: #BL-3
        pool_type: IP
        pool_name: LOOPBACK0_IP_POOL
        scope_type: Device Interface
        serial_number: BL-3(FDO2045073G)
        entity_name: FDO2045073G~loopback0
        resource : 10.7.0.1


    # L1_1: #BL-3
    #     pool_type: IP
    #     pool_name: LOOPBACK1_IP_POOL
    #     scope_type: Device Interface
    #     serial_number: BL-3(FDO2045073G)
    #     entity_name: FDO2045073G~loopback1
    #     resource : 10.8.0.3
```

例 2：サブネットの割り当て

```
#Link subnet
    Link0_1:
        pool_type: SUBNET
        pool_name: SUBNET
        scope_type: Link
        serial_number: F3-LEAF(FDO21440AS4)
        entity_name: FDO21440AS4~Ethernet1/1~FDO21510YPL~Ethernet1/3
        resource : 10.9.0.0/30
```

例 3：IP をインターフェイスに割り当てる

```
    #Interface IP
    INT1_1: #BL-3
        pool_type: IP
        pool_name: 10.9.0.8/30
        scope_type: Device Interface
        serial_number: BL-3(FDO2045073G)
        entity_name: FDO2045073G~Ethernet1/17
        resource : 10.9.0.9
```

例 4：エニーキャスト IP の割り当て

```
    #ANY CAST IP
    ANYCAST_IP:
        pool_type: IP
        pool_name: ANYCAST_RP_IP_POOL
        scope_type: Fabric
        entity_name: ANYCAST_RP
        resource : 10.253.253.1
```

例 5：ループバック ID の割り当て

```
#LOOPBACK ID
LID0_1: #BL-3
    pool_type: ID
    pool_name: LOOPBACK_ID
    scope_type: Device
    serial_number: BL-3(FDO2045073G)
    entity_name: loopback0
    resource : 0
```

リソースの解放

Cisco DCNM Web UI からリソースを解放するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [リソース（Resources）]** を選択します。

[**リソースの割り当て（Resource Allocation**）] ウィンドウが表示されます。このウィンドウには、選択した範囲の下にあるすべてのリソースが一覧表示されます。

ステップ 2 削除するリソースを選択します。

（注） 複数のリソースを選択すると、複数のリソースを同時に削除できます。

ステップ 3 **[リソースの解放（Release Resource(s)]** アイコンをクリックします。

確認用のダイアログボックスが表示されます。

ステップ 4 **[はい（Yes）]** をクリックして、リソースを解放します。

VMware サーバの追加、編集、再検出、削除

この項の内容は、次のとおりです。

VirtualCenter サーバを追加

Cisco DCNM から仮想センター サーバを追加できます。

Procedure

ステップ 1 **[制御（Control）] > [管理（Management）] > [仮想マシン マネージャ（Virtual Machine Manager）]** を選択します。

Cisco DCNM-LAN によって管理されている VMware Server（存在する場合）のリストがテーブルに表示されます。

ステップ 2 [追加（Add）] をクリックします。

[vCenter の追加（Add VCenter）] ウィンドウが表示されます。

ステップ 3 この VMware **[VirtualCenter サーバ（Virtual Center Server）]** の IP アドレスを入力します。

ステップ 4 この VMware Server の**[ユーザー名（User Name）]**と**[パスワード（Password）]**を入力します。

ステップ 5 **[Add（追加）]** をクリックすると、このVMware Server の管理が開始されます。

VMware サーバを削除

Cisco DCNM から VMware サーバを削除できます。

Procedure

ステップ 1 **[コントロール > マネジメント > 仮想マシン マネージャ（Control > Management > Virtual Machine Manager）]** を選択。

ステップ 2 VMware サーバのデータ収集を中止するために、削除したい VMware サーバの隣にあるチェック ボックスを選択して、**[削除（Delete）]** をクリックします。

VMware サーバの編集

Cisco DCNM Web クライアントから VMware サーバを編集できます。

Procedure

ステップ 1 **[コントロール > 管理 > 仮想マシン マネージャ（Control > Management > Virtual Machine Manager）]** を選択します。

ステップ 2 編集する VMware サーバーの隣のチェックボックスをオンにして、**[Edit（編集）]** VirtualCenter アイコンをクリックします。

[vCenter の編集（Edit VCenter）] ダイアログ ボックスが表示されます。

ステップ 3 **[ユーザー名（User Name）]** と **[パスワード（Password）]** を入力します。

ステップ 4 管理対象または管理対象外のステータスを選択します。

ステップ 5 [適用（Apply）] をクリックし、変更を保存します。

VMware サーバの再検出

Cisco DCNM から VMware サーバを再検出できます。

Procedure

ステップ 1 **[制御（Control）] > [管理（Management）] > [仮想マシン マネージャ（Virtual Machine Manager）]** を選択します。

ステップ 2 再検出する VMware の隣のチェックボックスを選択します。

ステップ 3 **[再検出（Rediscover）]** をクリックします。

「再検出操作が完了するまでお待ちください」という警告が記載されたダイアログボックスが表示されます。

ステップ 4 ダイアログ ボックスで [OK] をクリックします。

コンテナ オーケストレータ

Cisco DCNM Web UI で、**[制御（Control] > [管理（Management）] > [コンテナ オーケストレータ（Container Orchestrator）]** を選択します。コンテナ タイプを追加、削除、編集、および再検出できます。

Cisco DCNM を使用してコンテナ可視化を使用する方法を示すビデオも視聴できます。「ビデオ：Cisco DCNM でのコンテナ可視化の使用」を参照してください。

次の表に、[Container Orchestrator] ウィンドウのフィールドと説明が記載されています。

フィールド	説明
コンテナタイプ	オーケストレータのタイプを表示します。
クラスタIP	Kubernetes クラスタの IP アドレスを表示します。
クラスタ名	クラスタの名前を指定します。
管理対象（Managed）	クラスタが管理されていることを指定します。

フィールド	説明
Status	クラスタのステータスを表示します。 • **[証明書の期限切れ（Cert expired）]** は、証明書の期限が切れていることを意味します。正しい証明書を再度追加する必要があります。 • **[到達不能（Not reachable）]** は、DCNM が Kubernetes クラスタに到達できないことを意味します。 • **[Ok]** は、クラスタが正しく機能していることを意味します。 • **[検出中（Discovering）]** は、クラスタが検出中であることを意味します。 • **[空白（Blank）]**は、クラスタが管理されていないことを意味します。 （注） 注：ステータスが空の場合、クラスタが管理されていないことを意味します。
User	Kubernetes クラスタのロールを指定します
最終更新時刻	前回の変更からの経過時間を表示します。

次の表は、[コンテナ オーケストレータ（Container Orchestrator）] ウィンドウで実行できるアクションについて説明しています。

フィールド	説明
追加（Add）	**[追加（Add）]**アイコンをクリックして、新しいクラスタをコンテナ オーケストレーションに追加します。コンテナは 4 つまで追加できます。
削除	Kubernetes クラスタを選択し、**[削除（Delete）]** アイコンをクリックして削除します。
編集	Kubernetes クラスタを選択し、**[編集（Edit）]** アイコンをクリックしてクラスタの詳細を編集します。
再検出	Kubernetes クラスタを選択し、**[再検出（Rediscover）]** をクリックしてクラスタを更新します。

コンテナ オーケストレータでは、次のアクションを実行できます。

コンテナ オーケストレータの追加

Cisco DCNM Web UI からコンテナ オーケストレータを追加するには、次の手順を実行します。

始める前に

VM ベースの Kubernetes クラスタを追加するには、コンテナ オーケストレータの可視化機能を有効にする前に、Cisco DCNM で VMM が正常に構成されていることを確認してください。VM ベースの Kubernetes クラスタが実行されている VM をホストする VMM に vCenter を追加する必要があります。

ホスト名がすべてのクラスタ ノードで一意であることを確認してください。

ベアメタル ベースのクラスタには VMM は必要ありません。ベアメタル ベースのクラスタの場合、次を実行します。

- **[Web UI] > [管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバーのプロパティ（Server Properties）]** の順に選択してサーバー プロパティを編集し、DCNM で LLDP を有効にします。**[cdp.discover-lldp]** フィールドに **[true]** を入力して、LLDP を有効にします。
- ファブリックのすべてのリーフスイッチで LLDP 機能が有効化されていることを確認してください。
- Kubernetes クラスタで、すべてのベアメタルノードで LLDP および SNMP サービスが有効になっていることを確認します。
- Cisco UCS が Intel NIC を使用している場合、FW-LLDP が原因で LLDP ネイバーシップの確立に失敗します。

  回避策：Intel® イーサネットコントローラ（800 および 700 シリーズなど）に基づく選択されたデバイスでは、ファームウェアで実行される LLDP エージェントを無効にします。LLDP を無効にするには、次のコマンドを使用します。

  echo 'lldp stop' > /sys/kernel/debug/i40e/<bus.dev.fn>/command

  特定のインターフェイスの *bus.dev.fn* を見つけるには、次のコマンドを実行し、インターフェイスに関連付けられた ID を選択します。ID は、以下のサンプル出力で強調表示されています。

```
[ucs1-lnx1]# dmesg | grep enp6s0
[ 12.609679] IPv6: ADDRCONF(NETDEV_UP): enp6s0: link is not ready
[ 12.612287] enic 0000:06:00.0 enp6s0: Link UP
[ 12.612646] IPv6: ADDRCONF(NETDEV_UP): enp6s0: link is not ready
[ 12.612665] IPv6: ADDRCONF(NETDEV_CHANGE): enp6s0: link becomes ready
[ucs1-lnx1]#
```

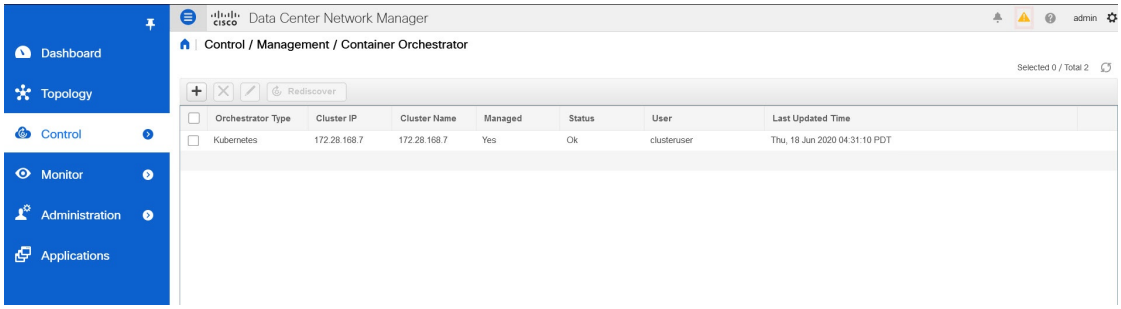
（注） LLDP 機能は、ベアメタルクラスタノードが接続されているファブリックスイッチで有効になっています。また、ボーダーゲートウェイスイッチに接続することもできます。

クラスタが検出された後にKubernetesクラスタが接続されているファブリックが検出された場合、トポロジを正しく表示するためにクラスタを再検出する必要があります。

LLDP の設定後にベアメタルベースの Kubernetes クラスタが検出された場合、トポロジを正しく表示するためにベアメタルクラスタを再検出する必要があります。

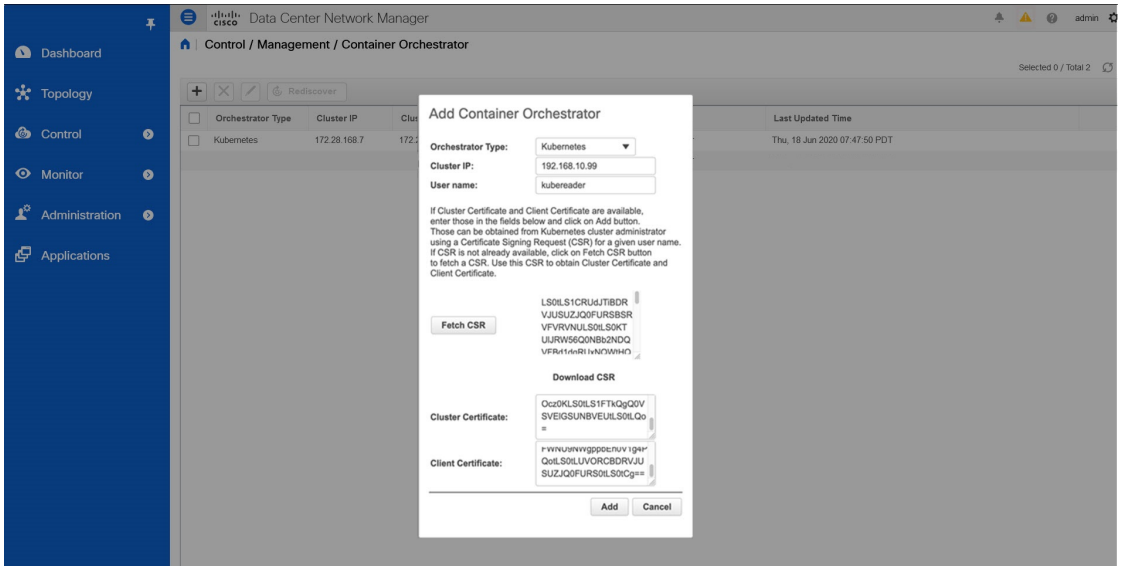
手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [コンテナ オーケストレータ（Container Orchestrator）]** の順に選択します。



ステップ 2 [追加（Add）] をクリックします。

[コンテナ オーケストレータの追加（Add Container Orchestrator）] が表示されます。



ステップ 3 **[オーケストレータ（Orchestrator）]** ドロップダウンリストから、**[Kubernetes]** を選択します。

ステップ 4 **[クラスター IP（Cluster IP）** フィールドに、Kubernetes クラスタのマスター ノードの IP アドレスを入力します。

ステップ 5 **[ユーザー名（User Name）]** フィールドに、Kubernetes に接続する API クライアントのユーザー名を入力します。

ステップ 6 **[CSR の取得（Fetch CSR）]** をクリックして、Kubernetes ビジュアライザ アプリケーションから証明書署名要求（CSR）を取得します。

（注） このオプションは、有効なクラスタ IP アドレスとユーザー名を入力するまで無効になっています。

SSL 証明書を取得していない場合にのみ、**[CSR の取得（Fetch CSR）]** を使用してください。有効な証明書がすでにある場合は、CSR を取得する必要はありません。

[CSR のダウンロード（Download CSR）] をクリックします。証明書の詳細は、ディレクトリ内の **<username>.csr** に保存されます。CSR の内容をファイル **[kubereader.csr]** に貼り付けます。ここで、*kubereader* は、Kubernetes に接続する API クライアントのユーザー名です。

CSR ファイル名は命名規則 <<*username*> > に従う必要があります。

（注） 証明書は Kubernetes クラスタで生成されるため、証明書を生成するには Kubernetes 管理者権限が必要です。

証明書 **[genk8clientcert.sh]** を生成するスクリプトは、DCNM サーバの `./root/packaged-files/scripts/genk8sclientcert.sh` の場所にあります。

ステップ 7 Kubernetes クラスタコントローラノードにログインします。

（注） 証明書を生成するには、管理者権限が必要です。

ステップ 8 `[genk8clientcert.sh]` と `[kubereader.csr]` を DCNM サーバーの場所から Kubernetes クラスタ コントローラ ノードにコピーします。

（注） 「vnc カットアンドペースト」操作を実行して、すべての文字が正しくコピーされるようにします。

ステップ 9 **genk8sclientcert.sh** スクリプトを使用して、ユーザー名の CSR を生成します。

```
(k8s-root)# ./genk8sclientcert.sh kubereader 10.x.x.x
```

値は次のとおりです。

- `kubereader` は、Kubernetes に接続する API クライアントのユーザー名です。（手順 ステップ 5 （374 ページ） で定義）。
- `10.x.x.x` は DCNM サーバーの IP アドレスです。

証明書が正常に生成されると、次のメッセージが表示されます。

```
------------------------------------------------------------
The K8s CA certificate is copied into k8s_cluster_ca.crt file.
    This to be copied into "Cluster CA" field.
The client certificate is copied into kubereader_10.x.x.x.crt file.
    This to be copied into "Client Certificate" field.
------------------------------------------------------------
```

同じ場所に 2 つの新しい証明書が生成されます。

- k8s_cluster_ca.crt
- *username_dcnm-IP*.crt

例：kubereader_10.x.x.x.crt （ここで、kubereader はユーザー名で、10.x.x.x は DCNM IP アドレスです）

ステップ 10 **cat** コマンドを使用して、これら 2 つのファイルから証明書を抽出します。

```
dcnm(root)# cat kubereader_10.x.x.x.crt
dcnm(root)# cat k8s_cluster_ca.crt
```

Cisco DCNM に Kubernetes クラスタを追加するユーザに、これらの 2 つの証明書を提供します。

ステップ 11 kubereader_10.x.x.x.crt の内容を **[クライアント証明書（Client Certificate）]** フィールドにコピーします。

（注） 「vnc カットアンドペースト」操作を実行して、すべての文字が正しくコピーされるようにします。

ステップ 12 k8s_cluster_ca.crt の内容を **[クラスタ証明書（Cluster Certificate）]** フィールドにコピーします。

（注） 「vnc カットアンドペースト」操作を実行して、すべての文字が正しくコピーされるようにします。

ステップ 13 **[追加（Add）]** をクリックして、コンテナ オーケストレータを追加します。

[キャンセル（Cancel）] をクリックして、コンテナ オーケストレータの追加を破棄します。

コンテナ オーケストレータの削除

Cisco DCNM Web UI からコンテナ オーケストレータを削除するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [コンテナ オーケストレータ（Container Orchestrator）]** の順に選択します。

ステップ 2 削除する **[コンテナ オーケストレータ（Container Orchestrator）]** を選択します。

一度に複数のクラスタを選択できます。

[削除（Delete）] をクリックします。

（注） クラスタを削除すると、すべてのデータが削除されます。クラスタは、トポロジビューからも削除されます。

ステップ 3 確認メッセージで **[はい（Yes）]** をクリックして、コンテナ オーケストレータを削除します。

[いいえ（No）] をクリックして破棄します。

コンテナ オーケストレータの編集

Cisco DCNM Web UI からコンテナを編集するには、以下の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [コンテナ オーケストレータ（Container Orchestrator）]** の順に選択します。

ステップ 2 変更する**[コンテナ オーケストレータ（Container Orchestrator）]** を選択します。[編集（Edit）] をクリックします。

[コンテナ オーケストレータの編集（Edit Container Orchestrator）] ウィンドウが表示されます。

ステップ 3 値を適切に変更します。

クラスタとクライアントの証明書を更新できます。Kubernetes クラスタの管理ステータスを更新することもできます。管理ステータスの更新を選択した場合、証明書は必要ありません。

ステップ 4 [適用（Apply）] をクリックし、変更を保存します。

[キャンセル（Cancel）] をクリックして破棄します。

Kubernetes クラスタの再検出

Cisco DCNM Web UI からKubernetes クラスタを再検出するには、以下の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [コンテナ オーケストレータ（Container Orchestrator）]** の順に選択します。

ステップ 2 再検出する**[コンテナ オーケストレータ（Container Orchestrator）]** を選択します。

一度に複数のクラスタを選択できます。

[再検出（Rediscover）] をクリックします。

このアクションでは、コンテナ情報を更新するのに時間がかかる場合があります。

OpenStack ビジュアライザ

Cisco DCNM Web UI で、**[制御（Control）] > [管理（Management）] > [OpenStack ビジュアライザ（OpenStack Visualizer）]** を選択します。OpenStack クラスタを追加、削除、編集、および再検出できます。これはプレビュー機能であることに注意してください。

[トポロジ（Topology）] で OpenStack クラスタを表示する方法については、OpenStack ワークロードの可視性 を参照してください。

次のテーブルでは、**[OpenStack ビジュアライザ（OpenStack Visualizer）]** ウィンドウのフィールドと説明を説明します。

フィールド	説明
クラスタ タイプ	クラスタのタイプを指定します。
クラスタIP	クラスタのコントローラのIPアドレスを指定します。
管理対象（Managed）	クラスタが管理対象か非管理対象かを指定します。
Status	クラスタのステータスを指定します。
ユーザ名	クラスタのユーザー名を指定します。
プロジェクト名	プロジェクト名を指定します。
[リージョン（Region）]	リージョンを指定します。
ユーザ ドメイン	ユーザー ドメインを指定します。
プロジェクト ドメイン	プロジェクト ドメインを指定します。
最終更新時刻	最後に更新された日時を示します。

次の表は、**[OpenStack ビジュアライザ（OpenStack Visualizer）]** ウィンドウで実行できるアクションについて説明しています。

フィールド	説明
追加（Add）	**[追加（Add）]** アイコンをクリックして、新しいOpenStackクラスタをコンテナオーケストレーションに追加します。
削除	OpenStack クラスタを選択し、**[削除（Delete）]** アイコンをクリックして削除します。
編集	OpenStack クラスタを選択し、**[編集（Edit）]** アイコンをクリックしてクラスタの詳細を編集します。
再検出	OpenStack クラスタを選択し、**[再検出（Rediscover）]** をクリックしてクラスタを更新します。

OpenStack クラスタの追加

このタスクは、OpenStack クラスタを追加する方法を示しています。

始める前に

- **[管理 (Administration)] > [DCNM サーバー (DCNM Server)] > [サーバー ステータス (Server Status)]** を選択します。**[cdp.discover-lldp]** プロパティが **[True]** に設定されていることを確認し、**[変更の適用（Apply Changes）]** をクリックします。

  OpenStack クラスタで、すべてのベアメタルノードで LLDP サービスが有効になっていることを確認します。LLDP機能は、ベアメタルクラスタノードが接続されているファブリックスイッチで有効になっています。また、ボーダーゲートウェイスイッチに接続することもできます。

- 再同期タイマーは、**[openstackviz.resync.timer]** プロパティを使用して変更できます。デフォルト値は 60 分です。この値を 60 分未満に設定できないことに注意してください。再同期機能は、OpenStack プラグインを再起動し、すべての OpenStack クラスタを再検出します。

- Intel® イーサネットコントローラに基づく、選択されたデバイス（例：800 および 700 シリーズ）については、ファームウェアで実行される Link Layer Discovery Protocol（LLDP）エージェントを無効にします。同じことを行うには、次のコマンドを使用します。

  ```
  # echo 'lldp stop' > /sys/kernel/debug/i40e/bus.dev.fn/command
  ```

  特定のインターフェイスの *bus.dev.fn* を見つけるには、次のコマンドを実行し、インターフェイスに関連付けられた ID を選択します。ID は、以下の出力で強調表示されています。

  ```
  # dmesg | grep eth0
  [ 8.269557] enic 0000:6a:00.0 eno5: renamed from eth0
  [ 8.436639] i40e 0000:18:00.0 eth0: NIC Link is Up, 40 Gbps Full Duplex, Flow Control:
   None
  [ 10.968240] i40e 0000:18:00.0 ens1f0: renamed from eth0
  [ 11.498491] ixgbe 0000:01:00.1 eno2: renamed from eth0
  ```

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [OpenStack ビジュアライザ（OpenStack Visualizer）]** の順に移動します。

ステップ 2 **[追加（Add）]** アイコンをクリックして、OpenStack クラスタを追加します。

- クラスタ情報（VM やホスト情報など）を取得するには、少なくとも読み取りアクセス許可が必要です。

- DCNM リリース 11.5(1) では、単一のプロジェクトとリージョンでのみクラスタを追加できます。

ステップ 3 **[OpenStack クラスタの追加（Add OpenStack Cluster）]** ウィンドウで、次の詳細情報を指定します。

- **[オーケストレータ タイプ（Orchestrator Type）]**：オーケストレータのタイプを指定します。デフォルトでは、このドロップダウンリストから OpenStack が選択されています。
- **[サーバー IP（Server IP）]**：OpenStack クラスタのコントローラの IP アドレスを指定します。
- **[ポート（Port）]**：ポート番号を指定します。
- **[バージョン（Version）]**：バージョンを指定します。
- **[ユーザー名（Username）]** および **[パスワード（Password）]**：OpenStack クラスタのユーザー名とパスワードを指定します。
- **[プロジェクト（Project）]**：プロジェクト名を指定します。
- **[リージョン（Region）]**：リージョンを指定します。デフォルトのリージョンは **[RegionOne]** です。
- **[ユーザ ドメイン（User Domain）]**：ユーザ ドメインを指定します。デフォルトのユーザ ドメインは **[default]** です。
- **[プロジェクト ドメイン（Project Domain）]**：プロジェクト ドメインを指定します。デフォルトのプロジェクト ドメインは **[default]** です。
- **[AMQP エンドポイント（AMQP Endpoint）]**：AMQP エンドポイントのアドレス詳細を含む multi-valued フィールドを、コロン（：）区切りで指定します。値はフォーマット：**[username:password:port]** で指定される必要があります。フィールドは次の情報で指定されます。
  - **[username]**：AMQP エンドポイントのユーザー名を指定します。
  - **[password]**：AMQP エンドポイントのパスワードを指定します。
  - **[port]**：AMQP エンドポイントのポート番号を指定します。

  このフィールドのデフォルト値は **[guest:guest:5672]** です。

ステップ 4 [追加（Add）] をクリックします。

検出後、ステータスは **[検出中（Discovering）]** から **[OK]** に変わります。OpenStack クラスタから受信した情報は適切に編成され、メインの **[トポロジ（Topology）]** ウィンドウに表示されます。**[表示（Show）]** ペインに **[OpenStack]** というラベルの付いた追加のメニュー項目が表示されます。

OpenStack クラスタの編集

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [OpenStack ビジュアライザ（OpenStack Visualizer）]** の順に移動します。

ステップ 2 変更する OpenStack クラスタを選択します。[編集（Edit）] をクリックします。

[OpenStack クラスタの編集（Edit OpenStack Cluster）] ウィンドウでは、次のフィールドを編集できます。

- **[ユーザー名（Username）]** および **[パスワード（Password）]**：OpenStack クラスタのユーザー名とパスワードを指定します。
- **[管理対象（Managed）]**：**[管理対象外（unmanaged）]** を選択して、OpenStack クラスタを管理対象外にできます。
- **[AMQP エンドポイント（AMQP Endpoint）**：AMQP エンドポイントのアドレス詳細を含む multi-valued フィールドを、コロン（：）区切りで指定します。値はフォーマット：**[username:password:port]** で指定される必要があります。フィールドは次の情報で指定されます。
  - **[username]**：AMQP エンドポイントのユーザー名を指定します。
  - **[password]**：AMQP エンドポイントのパスワードを指定します。
  - **[port]**：AMQP エンドポイントのポート番号を指定します。

  このフィールドのデフォルト値は **[guest:guest:5672]** です。

ステップ 3 [適用（Apply）] をクリックし、変更を保存します。

[キャンセル（Cancel）] をクリックして破棄します。

OpenStack クラスタの削除

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [OpenStack ビジュアライザ（OpenStack Visualizer）]** の順に移動します。

ステップ 2 変更する OpenStack クラスタを削除します。[削除（Delete）] をクリックします。

インベントリ ビューからクラスタを削除すると、OpenStack プラグインはクラスタからの変更通知のフェッチと受信を停止し、削除されたクラスタとの接続をシャットダウンして、すべてのソフトウェア リソースを解放します。

ステップ 3 確認メッセージで **[はい（Yes）]** をクリックして、OpenStack クラスタを削除します。

[いいえ（No）] をクリックして破棄します。

OpenStack クラスタの再検出

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [OpenStack ビジュアライザ（OpenStack Visualizer）]** の順に移動します。

ステップ 2 再検出する特定のクラスタまたはすべてのクラスタを選択します。**[再検出（Rediscover）]** をクリックします。

[テンプレート ライブラリ（Template Library）]

Cisco DCNM Web クライアントを使用して、異なる Cisco Nexus および Cisco MDS プラットフォームで設定されているテンプレートを追加、編集、または削除できます。Cisco DCNM Web クライアントのホームページから、**[制御（Control）] > [テンプレート ライブラリ（Template Library）] > [テンプレート（Templates）]** を選択します。Cisco DCNM Web クライアントで構成されているテンプレートごとに、次のパラメータが表示されます。テンプレートは JavaScript をサポートします。テンプレートの JavaScript 関数を使用して、テンプレートの構文で算術演算と文字列操作を実行できます。

次の表で、このページに表示されるフィールドを説明します。

Table 1: テンプレート操作

フィールド	説明
Add Template	新しいテンプレートを追加できます。
テンプレートの変更/表示	テンプレート定義を表示し、必要に応じて変更できます。
テンプレートに名前を付けて保存	選択したテンプレートを別の名前で保存できます。必要に応じて、テンプレートを編集できます。
テンプレートの削除（Delete Template）	テンプレートの削除を許可します
テンプレートのインポート	ローカル ディレクトリからテンプレートを 1 つずつインポートできます。

フィールド	説明
テンプレートのエクスポート	ローカル ディレクトリの場所にテンプレート設定をエクスポートできます。
テンプレート Zip ファイルのインポート	.zip 形式でバンドルされた複数のテンプレートを含む .zip ファイルをインポートできます ZIP ファイル内のすべてのテンプレートが抽出され、個々のテンプレートとしてテーブルにリストされます。

Note サーバーの再起動後にテンプレートのロード中に問題が発生した場合は、**[テンプレート Zip ファイルのインポート]** の横に通知が表示されます。通知をクリックして、**[テンプレートの読み込み中の問題]** ウィンドウにエラーを表示します。エラーのあるテンプレートは、**[テンプレート（Templates）]** ウィンドウに表示されません。このようなテンプレートをインポートするには、エラーを修正してインポートします。

Cisco DCNM Release 11.4(1) から **network-operator** ロールでのみテンプレートのみを表示できます。このロールでテンプレートを作成、編集、または保存することはできません。ただし、**network-stager** ロールを使用してテンプレートを作成または編集できます。

Table 2: テンプレートのプロパティ

フィールド	説明
テンプレート名（Template Name）	構成されたテンプレートの名前が表示されます。
[テンプレートの説明（Template Description）]	テンプレートの構成中に提供される説明を表示します。
タグ（Tags）	テンプレートに割り当てられたタグを表示し、タグに基づいてテンプレートをフィルタリングするのに役立ちます。
サポートされるプラットフォーム	テンプレートと互換性のあるサポートされている Cisco Nexus プラットフォームを表示します。テンプレートでサポートされているプラットフォームのチェック ボックスをオンにします。 **Note** 複数のプラットフォームを選択できます。
テンプレートのタイプ	テンプレートのタイプが表示されます。
テンプレート サブ タイプ	テンプレートに関連付けられたサブタイプを指定します。
テンプレートのコンテンツ タイプ	Jython または Template CLI のどちらであるかを指定します。

Table 3: 詳細テンプレートのプロパティ

フィールド	説明
実装	実装する抽象テンプレートを表示します。
依存関係	スイッチの特定の機能を指定します。
作成日：	テンプレートを公開するかどうかを指定します。
インポート	インポートのベース テンプレートを指定します。

さらに、メニュー バーから **[制御] > [テンプレート ライブラリ] > [テンプレート]** を選択し、次のこともできます。

- **[フィルタを表示]** をクリックして、ヘッダーに基づいたテンプレートをフィルタ処理します。
- **[印刷]** をクリックして、テンプレートのリストを印刷します。
- **[Excel にエクスポート]** をクリックして、テンプレートのリストを Microsoft Excel スプレッドシートにエクスポートします。

この項の内容は、次のとおりです。

テンプレート構造

構成テンプレートの内容は、主に4つの部分で構成されます。テンプレートのコンテンツの編集については、**[テンプレート コンテンツ（Template Content）]** の横にある **[ヘルプ（Help）]** アイコンをクリックします。

この項の内容は、次のとおりです。

テンプレートの形式

ここでは、テンプレートの基本情報について説明します。次の表に、使用可能なフィールドの詳細を示します。

プロパティ名	説明	有効な値	任意かどうか
名前（name）	テンプレートの名前	テキスト	いいえ
説明	テンプレートに関する簡単な説明	テキスト（Text）	はい

プロパティ名	説明	有効な値	任意かどうか
userDefined	ユーザがテンプレートを作成したかどうかを示します。ユーザが作成した場合、値は「true」です。	「true」または「false」	はい
supportedPlatforms	この設定テンプレートをサポートするデバイスプラットフォームのリスト。すべてのプラットフォームをサポートするには、[All]を指定します。	N1K、N3K、N3500、N4K、N5K、N5500、N5600、N6K、N7K、N9K、MDS、VDC、N9K-9000v、IOS-XE、IOS-XR、その他、すべてのNexusスイッチのリストがカンマで区切られています。	いいえ

プロパティ名	説明	有効な値	任意かどうか
templateType	使用するテンプレートのタイプを指定します。	• CLI • POAP **Note** POAP オプションは、Cisco DCNM ローカル エリア ネットワーク（LAN）ファブリックの展開には適用されません。 • ポリシー • SHOW • プロファイル • ファブリック • [抽象（ABSTRACT）] • レポート	はい

プロパティ名	説明	有効な値	任意かどうか
templateSubType	テンプレートに関連付けられたサブタイプを指定します。		

プロパティ名	説明	有効な値	任意かどうか
		• CLI • なし • POAP • なし • VXLAN • FABRICPATH • VLAN • PMN **Note** POAP オプションは、Cisco DCNM ローカル エリア ネットワーク（LAN）ファブリックの展開には適用されません。 • ポリシー • VLAN • interface-vlan • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORTCHANNEL • INTERFACE_FC • INTERFACE_MGMT	

プロパティ名	説明	有効な値	任意かどうか
		• INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VPC • INTERFACE_PORTCHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • SHOW • VLAN • interface-vlan • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORTCHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VPC • INTERFACE_PORTCHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • プロファイル • VXLAN	

プロパティ名	説明	有効な値	任意かどうか
		• ファブリック • 該当なし • [抽象（ABSTRACT）] • VLAN • interface-vlan • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORT_CHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_SAN_PORT_CHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • レポート • アップグレード • GENERIC	

プロパティ名	説明	有効な値	任意かどうか
contentType			はい

プロパティ名	説明	有効な値	任意かどうか
		• CLI • TEMPLATE_CLI • POAP • TEMPLATE_CLI **Note** POAP オプションは、Cisco DCNM ローカル エリア ネットワーク（LAN）ファブリックの展開には適用されません。 • ポリシー • TEMPLATE_CLI • PYTHON • SHOW • TEMPLATE_CLI • プロファイル • TEMPLATE_CLI • PYTHON • ファブリック • PYTHON • [抽象（ABSTRACT）]	

プロパティ名	説明	有効な値	任意かどうか
		• TEMPLATE_CLI • PYTHON • レポート • PYTHON	
実装（Implement）	抽象テンプレートを実装するために使用されます。	テキスト（Text）	はい
依存関係	スイッチの特定の機能を選択するために使用されます。	テキスト（Text）	はい
公開	テンプレートを読み取り専用としてマークし、変更を回避するために使用されます。	「true」または「false」	はい

テンプレート変数

このセクションには、テンプレートに使用されるパラメータの宣言された変数、データ型、デフォルト値、および有効な値の条件が含まれます。これらの宣言された変数は、動的コマンド生成プロセス中にテンプレート コンテンツ セクションの値の置換に使用されます。また、これらの変数は、意思決定およびテンプレート コンテンツ セクションの反復ブロックで使用されます。変数には事前定義されたデータ型があります。変数に関する説明を追加することもできます。次の表に、使用可能なデータ型の構文と使用方法を示します。

変数の型	有効値	反復可能?
boolean	true|false	いいえ
enum	`Example: running-config, startup-config`	いいえ
浮動	浮動小数点形式	いいえ
floatRange	`Example: 10.1,50.01`	はい
整数型（Integer）	任意の数値	いいえ

変数の型	有効値	反復可能?
integerRange	「-」で区切られた連続する番号 「,」で区切られた個別の番号 `Example: 1-10,15,18,20`	はい
インターフェイス	形式：<if type><slot>[/<sub slot>]/<port> `Example: eth1/1, fa10/1/2 etc.`	いいえ
interfaceRange	`Example: eth10/1/20-25, eth11/1-5`	はい
IPアドレス	IPv4 または IPv6 アドレス	いいえ

ipAddressList	IPv4、IPv6、または両方のタイプのアドレスの組み合わせのリストを作成できます。
	`Example 1: 172.22.31.97, 172.22.31.99, 172.22.31.105, 172.22.31.109`
	`Example 2: 2001:0db8:85a3:0000:0000:8a2e:0370:7334, 2001:0db8:85a3:0000:0000:8a2e:0370:7335, 2001:0db8:85a3:1230:0000:8a2f:0370:7334`
	`Example 3: 172.22.31.97, 172.22.31.99, 2001:0db8:85a3:0000:0000:8a2e:0370:7334, 172.22.31.254`
		はい

ipAddressWithoutPrefix	`Example: 192.168.1.1`
	または
	`Example: 1:2:3:4:5:6:7:8`
		いいえ

ipV4Address	IPv4 アドレス	いいえ
ipV4AddressWithSubnet	`Example: 192.168.1.1/24`	いいえ
ipV6Address	[IPv6 アドレス（IPv6 address）]	いいえ

変数の型	有効値	反復可能?
ipV6AddressWithPrefix	Example: 1:2:3:4:5:6:7:8 22	いいえ
ipV6AddressWithSubnet	IPv6アドレスとサブネット	いいえ
ISISNetAddress	Example: 49.0001.00a0.c96b.c490.00	いいえ
long	Example: 100	いいえ
MAC アドレス	14 または 17 文字長の MAC アドレス形式	いいえ

string	変数の説明などに使用される自由テキスト
	
	Example:
	string scheduledTime
	{
	regularExpr=^([01]\d|2[0-3]):([0-5]\d)$;
	}
		いいえ

string[]	Example: {a,b,c,str1,str2}	はい

構造体	単一の変数にバンドルされているパラメータのセット。
	
	struct <structure name declaration > {
	<parameter type> <parameter 1>;
	<parameter type> <parameter 2>;
	…..
	} [<structure_inst1>] [,
	<structure_inst2>] [,
	<structure_array_inst3 []>];
	
	struct interface_detail {
	string inf_name;
	string inf_description;
	ipAddress inf_host;
	enum duplex {
	validValues = auto, full, half;
	};
	}myInterface,
	myInterfaceArray[];
		いいえ
		Note 構造体変数が配列として宣言されている場合、変数は反復型です。

wwn （Cisco DCNM Web Client でのみ使用可能）	Example: 20:01:00:08:02:11:05:03	いいえ

可変メタ プロパティ

テンプレート変数セクションで定義されている各変数には、一連のメタ プロパティがあります。メタ プロパティは、主に変数に定義されている検証ルールです。

次の表に、使用可能な変数タイプに適用されるさまざまなメタ プロパティを示します。

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
boolean	ブール値。 Example: true	はい											
enum			はい										
浮動	符号付き実数。 Example: 75.56, -8.5	はい	はい	はい	はい	はい							
floatRange	符号付き実数の範囲 Example: 50.5 - 54.75	はい	はい	はい	はい	はい							
integer	符号付き実数 Example: 50, -75	はい	はい		はい	はい							

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
integerRange	符号付き実数の範囲 Example: 50-65	はい	はい		はい	はい							
インターフェイス	インターフェイス/ポートを指定します Example: Ethernet 5/10	はい	はい				はい	はい	はい	はい			
interfaceRange		はい	はい				はい	はい	はい	はい			
IPアドレス	IPv4 または IPv6 形式の IP アドレス	はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
pAdtsLi		はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
	IPv4、IPv6、または両方のタイプのアドレスの組み合わせのリストを作成できます。 Example 1: 10.2.2.3.97, 10.2.2.3.99, 10.2.2.3.105, 10.2.2.3.109 Example 2: [redacted], [redacted], [redacted] Example 3: 10.2.2.3.97, 10.2.2.3.99, [redacted], 10.2.2.3.254 **Note** リス												

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
		ト内のアドレスは、ハイフンではなくカンマで区切ります。											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
[illegible]	IPv4 または IPv6 アドレス（プレフィックス/サブネットは不要）。												
[illegible]	IPv4 アドレス	はい											
[illegible]	IPv4 アドレスとサブネット	はい											
[illegible]	[IPv6 アドレス（IPv6 addrs）]	はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
[illegible]	プレフィックス付き IPv6 アドレス	はい											
[illegible]	IPv6 アドレスとサブネット	はい											
[illegible]	Example: [illegible]												
long	Example: 100	はい			はい	はい							
MAC アドレス	MAC アドレス												
string	リテラル文字列 Example for string Regular expression: string [illegible] { [illegible] }	はい									はい	はい	はい

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
string[]	カンマ（,）で区切られた文字列リテラル Example: {string1, string2}	はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
構造体	単一の変数にバンドルされているパラメータのセット。 struct <structure name declaration > { <parameter type> <parameter 1>; <parameter type> <parameter 2>; ….. } [structvar1] [, <structvar2> [, <structvar3> []>];												
wwn	WWN アドレス												

例：メタ プロパティの使用

```
##template variables

integer VLAN_ID {
min = 100;
max= 200;
};

string USER_NAME {
defaultValue = admin123;
minLength = 5;
};

struct interface_a{
 string inf_name;
 string inf_description;
 ipAddress inf_host;
 enum duplex {
  validValues = auto, full, half;
 };
}myInterface;

##
```

可変注釈

注釈を使用して変数をマーキングする変数プロパティを設定できます。

Note 可変注釈は、POAP でのみ使用できます。ただし、注釈はテンプレートタイプ「CLI」には影響しません。

テンプレート変数セクションでは、次の注釈を使用できます。

注釈キー	有効な値	説明
AutoPopulate	テキスト（Text）	あるフィールドから別のフィールドに値をコピーします。
DataDepend	テキスト	
説明	[テキスト（Text）]	ウィンドウに表示されるフィールドの説明
DisplayName	テキスト（Text） **Note** スペースがある場合は、テキストを引用符で囲みます。	ウィンドウに表示されるフィールドの表示名

注釈キー	有効な値	説明
列挙体	Text1、Text2、Text3 など	選択するテキストまたは数値をリストします
IsAlphaNumeric	「true」または「false」	文字列には、英数字を使用します。
IsAsn	「true」または「false」	
IsDestinationDevice	「true」または「false」	
IsDestinationFabric	「true」または「false」	
IsDestinationInterface	「true」または「false」	
IsDestinationSwitchName	「true」または「false」	
IsDeviceID	「true」または「false」	
IsDot1qId	「true」または「false」	
IsFEXID	「true」または「false」	
IsGateway	「true」または「false」	IPアドレスがゲートウェイかどうかを検証します。
IsInternal	「true」または「false」	フィールドを内部にし、ウィンドウに表示しません。 **Note** この注釈は、ipAddress変数にのみ使用します。
IsManagementIP	「true」または「false」 **Note** この注釈は、変数「ipAddress」に対してのみマークする必要があります。	

注釈キー	有効な値	説明
is_mandatory	「true」または「false」	値をフィールドに強制的に渡す必要があるかどうかを検証します
IsMTU	「true」または「false」	
IsMultiCastGroupAddress	「true」または「false」	
IsMultiLineString	「true」または「false」	文字列フィールドを複数行の文字列テキスト領域に変換します
IsMultiplicity	「true」または「false」	
IsPassword	「true」または「false」	
IsPositive	「true」または「false」	値が正であるかどうかを確認します。
IsReplicationMode	「true」または「false」	
IsShow	「true」または「false」	ウィンドウのフィールドを表示または非表示にします
IsSiteId	「true」または「false」	
IsSourceDevice	「true」または「false」	
IsSourceFabric	「true」または「false」	
IsSourceInterface	「true」または「false」	
IsSourceSwitchName	「true」または「false」	
IsSwitchName	「true」または「false」	
IsRMID	「true」または「false」	
IsVPCDomainID	「true」または「false」	
IsVPCID	「true」または「false」	
IsVPCPeerLinkPort	「true」または「false」	
IsVPCPeerLinkPortChannel	「true」または「false」	

注釈キー	有効な値	説明
IsVPCPortChannel	「true」または「false」	
[パスワード（Password）]	テキスト（Text）	パスワードフィールドを検証します
PeerOneFEXID	「true」または「false」	
PeerTwoFEXID	「true」または「false」	
PeerOnePCID	「true」または「false」	
PeerTwoPCID	「true」または「false」	
PrimaryAssociation		
ReadOnly	「true」または「false」	フィールドを読み取り専用にします
ReadOnlyOnEdit	「true」または「false」	
SecondaryAssociation	テキスト（Text）	
セクション		
UsePool	「true」または「false」	
UseDNSReverseLookup		
ユーザ名	テキスト（Text）	ウィンドウにユーザ名フィールドを表示します。
警告	テキスト（Text）	Description 注釈をオーバーライドするテキストを提供します。

例：**AutoPopulate** 注釈

```
##template variables
string BGP_AS;
 @(AutoPopulate="BGP_AS")
  string SITE_ID;
##
```

例：**DisplayName**注釈

```
##template variables
@(DisplayName="Host Name", Description = "Description of the host")
String hostname;
@(DisplayName="Host Address", Description = " test description" IsManagementIP=true)
```

```
ipAddress hostAddress;
##
```

例：IsMandatory注釈

```
##template variables
@(IsMandatory="ipv6!=null")
ipV4Address ipv4;
@(IsMandatory="ipv4!=null")
ipV6Address ipv6;
##
```

例：IsMultiLineString注釈

```
##template variables
@(IsMultiLineString=true)
string EXTRA_CONF_SPINE;
##
```

IsShow注釈

```
##template variables
boolean isVlan;
@(IsShow="isVlan==true")
integer vlanNo;
##

##template variables
boolean enableScheduledBackup;
@(IsShow="enableScheduledBackup==true",Description="Server time")
string scheduledTime;
##
The condition "enableScheduledBackup==true" evaluates to true/false

##template variables
@(Enum="Manual,Back2BackOnly,ToExternalOnly,Both")
string VRF_LITE_AUTOCONFIG;
@(IsShow="VRF_LITE_AUTOCONFIG!=Manual",  Description="Target Mask")
integer DCI_SUBNET_TARGET_MASK
##
The condition "VRF_LITE_AUTOCONFIG!=Manual" matches string comparison to evaluate to
true or false
```

例：警告の注釈

```
##template variables
@(Warning="This is a warning msg")
  string SITE_ID;
##
```

テンプレートの内容

この項には、テンプレートで使用する構成コマンドと、すべてのパラメータが含まれています。これらのコマンドには、テンプレート変数セクションで宣言された変数を含めることができます。コマンド生成プロセス中に、変数の値がテンプレートの内容に適切に置き換えられます。

Note 使用するコマンドは、任意のデバイスのグローバル構成コマンド モードで入力するのと同じように指定する必要があります。コマンドを指定するときは、コマンド モードを考慮する必要があります。

テンプレートの内容は、変数の使用によって決まります。

- スカラ変数：反復に使用できない値の範囲または配列を取得しません（変数タイプテーブルでは、iterate-ableが「No」としてマークされています）。スカラ変数はテンプレートの内容内で定義する必要があります。

```
Syntax: $$<variable name>$$
Example: $$USER_NAME$$
```

- 反復変数：ブロックの反復に使用されます。これらのループ変数は、次に示すように、繰り返しブロック内でアクセスする必要があります。

```
Syntax:@<loop variable>
Example:
foreach val in $$INTEGER_RANGE_VALUE$$ {
@val
}
```

- スカラー構造体変数：構造体メンバー変数は、テンプレートの内容からアクセスできます。

```
Syntax: $$<structure instance name>.<member variable name>$$
Example: $$myInterface.inf_name$$
```

- 配列構造変数：構造体のメンバー変数は、テンプレートの内容からアクセスできます。

```
Syntax: $$<structure instance name>.<member variable name>$$
Example: $$myInterface.inf_name$$
```

テンプレート変数に加えて、次のステートメントを使用して、条件付きコマンドと反復コマンドの生成を使用できます。

- if-else if-else ステートメント：その中の変数に割り当てられた値に基づいて、設定コマンドのセットの包含/除外を論理的に決定します。

```
Syntax: if(<operand 1>  <logical operator>  <operand 2>){
command1 ..
command2..
..
}
else  if (<operand 3> <logical operator> <operand 4> )
{
Command3 ..
Command4..
..
}
else
{
```

```
Command5 ..
Command6..
..
}
Example: if-else if-else statement
if($$USER_NAME$$ == 'admin'){
Interface2/10
no shut
}
else {
Interface2/10
shut
}
```

- foreach ステートメント：コマンドのブロックを反復するために使用されます。反復は、割り当てられたループ変数値に基づいて実行されます。

```
Syntax:
foreach <loop index variable> in $$<loop variable>$$ {
@<loop index variable> ..
}
Example: foreach Statement
foreach ports in $$MY_INF_RANGE$${
interface @ports
no shut
}
```

- オプションパラメータ：デフォルトでは、すべてのパラメータが必須です。パラメータをオプションにするには、パラメータに注釈を付ける必要があります。

変数セクションには、次のコマンドを含めることができます。

- **@(IsMandatory=false)**
- **Integer frequency;**

  テンプレートの内容の項では、「if」条件チェックを使用せずに、パラメータに値を割り当てることで、コマンドを除外または含めることができます。オプションのコマンドは、次のように構成できます。

- **probe icmp [frequency frequency-value] [timeout seconds] [retry-count retry-count-value]**

テンプレート コンテンツ エディタ

テンプレート コンテンツ エディタには、次の機能があります。

- 構文の強調表示: エディタは、Python スクリプトのさまざまなタイプのステートメント、キーワードなどの構文を強調表示します。
- オートコンプリート: 入力を開始すると、エディタはテンプレートのデータ型、注釈、またはメタプロパティを提案します。
- 行に移動: スクロールする代わりに、テンプレート コンテンツ エディタで正確な行に移動できます。Mac の場合は **Command-L**、Windows の場合は **Ctrl-L** を押し、ポップアップ ウィンドウに移動先の行番号を入力します。

エディタで行数より大きい値を入力すると、エディタ ウィンドウの最後の行に移動します。

- テンプレートの検索と置換: Mac の場合は **Command-F**、Windows の場合は **Ctrl-F** を押し、**検索対象**フィールドに検索語を入力し、検索ウィンドウで検索のタイプを選択します。エディタで次の検索を実行できます。
  - **RegExp 検索**：エディタで正規表現検索を実行できます。
  - **CaseSensitive 検索** ：エディタで大文字と小文字を区別した検索を実行できます。
  - **単語全体の検索 : 単語全体の検索を実行して、エディタで正確な単語を見つけることができます。**たとえば、"play" という単語の通常の検索では、"display" などの単語の一部である結果が返されますが、単語全体の検索では、"play" という単語に完全に一致する場合にのみ結果が返されます。
  - **選択範囲で検索** : 選択したコンテンツで検索を実行できます。検索を絞り込みたいコンテンツを選択し、検索語を入力します。

  置換オプションを使用するには、検索ウィンドウで + アイコンを選択します。**[置換後の文字列（Replace with）]** フィールドに置換する単語を入力します。**[置換]** を選択すると、選択した単語を 1 回だけ置き換えることができます。選択した単語の出現箇所をすべて置換するには、**[すべて]** を選択します。
- コードの折りたたみ: エディタでコード ブロックを展開またはグループ化するには、行番号の横にある矢印をクリックします。
- その他の機能: エディタは、コード、閉じ括弧を自動的にインデントし、対応する括弧を強調表示します。

テンプレート エディタの設定

[テンプレート エディタの設定（Template Editor Settings）] をクリックすると、テンプレート エディタの次の機能を編集できます。

- **[テーマ（Theme）]** : ドロップダウン リストからエディタに必要なテーマを選択します。
- **KeyBinding**：エディタをカスタマイズするには、**KeyBinding** ドロップダウン リストからエディタ モードを選択します。 **Vim** と **Ace** モードがサポートされています。デフォルトは **Ace** です。
- **[フォント サイズ（Font Size）]** : エディタに必要なフォント サイズを選択します。

高度な機能

次に、テンプレートの構成に使用できる高度な機能を示します。

- 割り当て操作

構成テンプレートは、テンプレートコンテンツセクション内の変数値の割り当てをサポートします。変数の宣言されたデータ型の値が検証されます。不一致がある場合、値は割り当てられません。

割り当て操作は、次のガイドラインに従って使用できます。

- 左側の演算子は、テンプレートパラメータまたはforループパラメータのいずれかである必要があります。
- 正しい値の演算子は、テンプレートパラメータ、ループパラメータ、引用符で囲まれたリテラル文字列値、または単純な文字列値のいずれかの値です。

ステートメントがこれらのガイドラインに従っていない場合、またはこの形式に適合しない場合は、割り当て操作とは見なされません。これは、他の通常の行と同様に、コマンド生成時に置き換えられます。

```
Example: Template with assignment operation
##template properties
name =vlan creation;
userDefined= true;
supportedPlatforms = All;
templateType = CLI;
published = false;
##
##template variables
integerRange vlan_range;
@(internal=true)
integer vlanName;
##
##template content
foreach vlanID in $$vlan_range$${
vlan @vlanID
$$vlanName$$=@vlanID
name myvlan$$vlanName$$
}
##
```

- Evaluate メソッド

設定テンプレートは、Java ランタイムが提供する Java スクリプト環境を使用して、算術演算（ADD、SUBTRACT など）、文字列操作などを実行します。

テンプレートリポジトリパスでJavaScriptファイルを見つけます。このファイルには、算術文字列関数の主要なセットが含まれています。カスタム JavaScript メソッドを追加することもできます。

これらのメソッドは、次の形式の設定テンプレート コンテンツ セクションから呼び出すことができます。

```
Example1:
$$somevar$$ = evalscript(add, "100", $$anothervar$$)
```

また、次のようなif条件の内部で *evalscript* を呼び出すことができます。

```
if($$range$$ > evalscript(sum, $$vlan_id$$,  -10)){
```

```
do something...
}
```

Java スクリプト ファイルのバックエンドにあるメソッドを呼び出すことができます。

- 動的な決定

  構成テンプレートは、特殊な内部変数LAST_CMD_RESPONSEを提供します。この変数には、コマンド実行中のデバイスからの最後のコマンド応答が格納されます。これは、デバイスの状態に基づいてコマンドを提供するための動的な決定を行うために、構成テンプレートのコンテンツで使用できます。

Note ifブロックの後には、空の場合もある新しい行でelseブロックを続ける必要があります。

VLAN がデバイス上に存在しない場合の VLAN の作成例。

```
Example: Create VLAN
##template content
show vlan id $$vlan_id$$
if($$LAST_CMD_RESPONSE$$ contains "not found"){
vlan $$vlan_id$$
}
else{
}
##
```

この特別な暗黙的変数は、「IF」ブロックでのみ使用できます。

- テンプレート参照

  すべての変数を定義した基本テンプレートを作成できます。この基本テンプレートは、複数のテンプレートにインポートできます。基本テンプレートの内容は、拡張テンプレートの適切な場所に置き換えられます。インポートしたテンプレートパラメータと内容は、拡張テンプレート内でアクセスできます。

```
Example: Template Referencing
Base template:
##template properties
 name =a vlan base;
 userDefined= true;
 supportedPlatforms = All;
 templateType = CLI;
 published = false;
 timestamp = 2015-07-14 16:07:52;
 imports = ;
##
##template variables
 integer vlan_id;
##
##template content
 vlan $$vlan_id$$
##

Derived Template:
##template properties
 name =a vlan extended;
 userDefined= true;
```

```
 supportedPlatforms = All;
 templateType = CLI;
 published = false;
 timestamp = 2015-07-14 16:07:52;
 imports = a vlan base,template2;
##
##template variables
 interface vlanInterface;
##
##template content
 <substitute a vlan base>
 interface $$vlanInterface$$
 <substitute a vlan base>
##
```

拡張テンプレートを起動すると、基本テンプレートのパラメータ入力も取得されます。また、置換された内容は、完全な CLI コマンドの生成に使用されます。

レポート テンプレート

Cisco DCNM 11.3(1) リリース以降、新しいテンプレート タイプ、REPORT が追加されました。このテンプレートには、[UPGRADE] と [GENERIC] の 2 つのサブタイプがあります。テンプレートの種類は python です。

アップグレード

UPGRADEテンプレートは、ISSU前後のシナリオに使用されます。これらのテンプレートは、ISSU ウィザードに表示されます。

ISSU 前後の処理の詳細については、DCNM にパッケージ化されているデフォルトのアップグレード テンプレートを参照してください。デフォルトのアップグレード テンプレートは issu_vpc_check です。

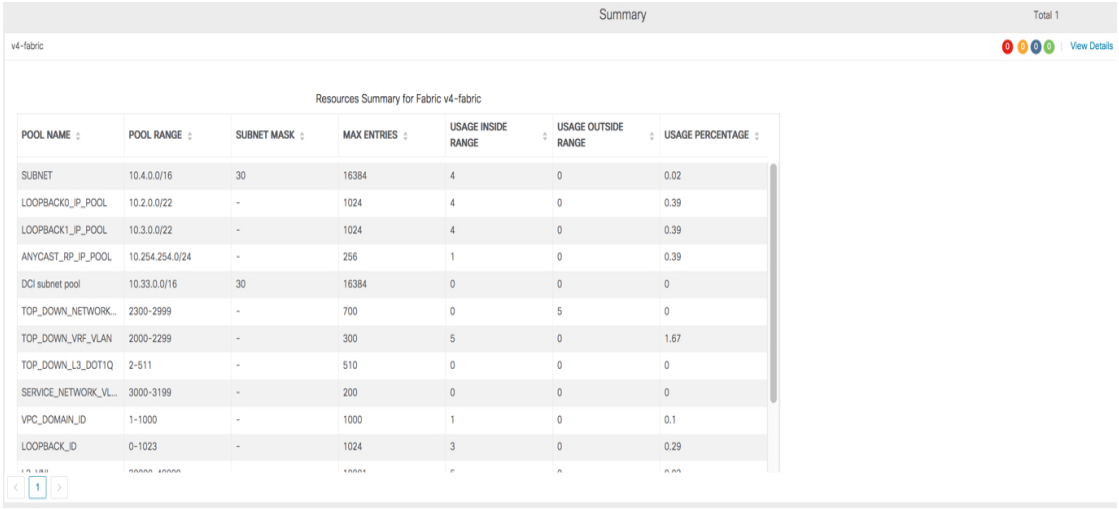
GENERIC

GENERIC テンプレートは、リソース、スイッチ インベントリ、SFP、NVE VNI カウンタに関する情報の収集など、一般的なレポート シナリオに使用されます。このテンプレートを使用して、トラブルシューティング レポートを生成することもできます。

リソース レポート

このレポートには、特定のファブリックのリソース使用状況に関する情報が表示されます。

[サマリ（Summary）]セクションには、すべてのリソース プールと現在の使用率が表示されます。より多くの列を表示するには、ウィンドウの下部にある水平スクロール バーを使用します。



POOL NAME：プールの名前を指定します。

POOL RANGE：プールの IP アドレス範囲を指定します。

SUBNET MASK：サブネット マスクを指定します。

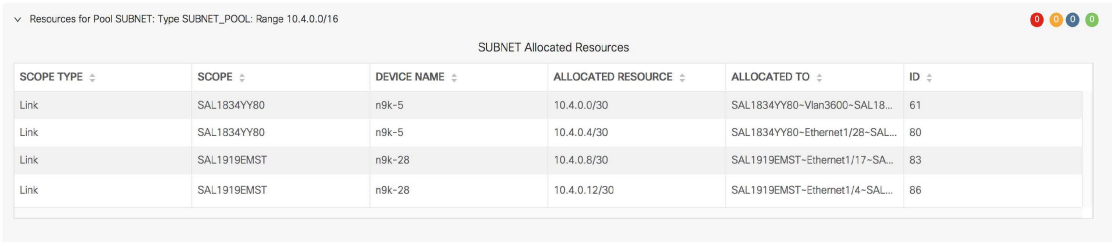
MAX ENTRIES：プールから割り当て可能な最大エントリ数を示します。

USAGE INSIDE RANGE：プール範囲内に割り当てられている現在のエントリ数を指定します。

USAGE OUTSIDE RANGE：プール範囲外に設定されている現在のエントリ数を指定します。

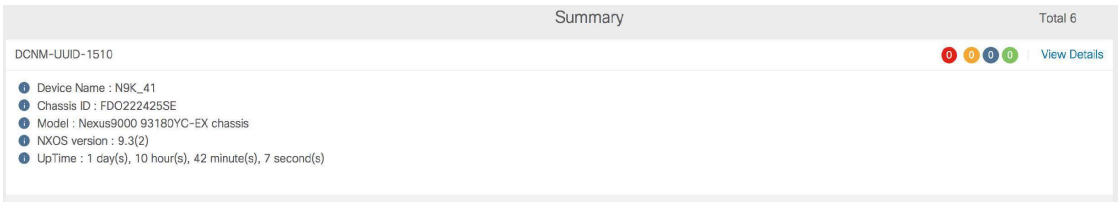
USAGE PERCENTAGE：これは、(範囲内での使用数/最大エントリ数) *100 という式を使用して計算されます。

[詳細の表示（View Details）]をクリックして、各リソースプールに割り当てられた、または設定されたリソースのビューを表示します。たとえば、SUBNET の詳細セクションには、サブネット内で割り当てられたリソースに関する情報が含まれます。

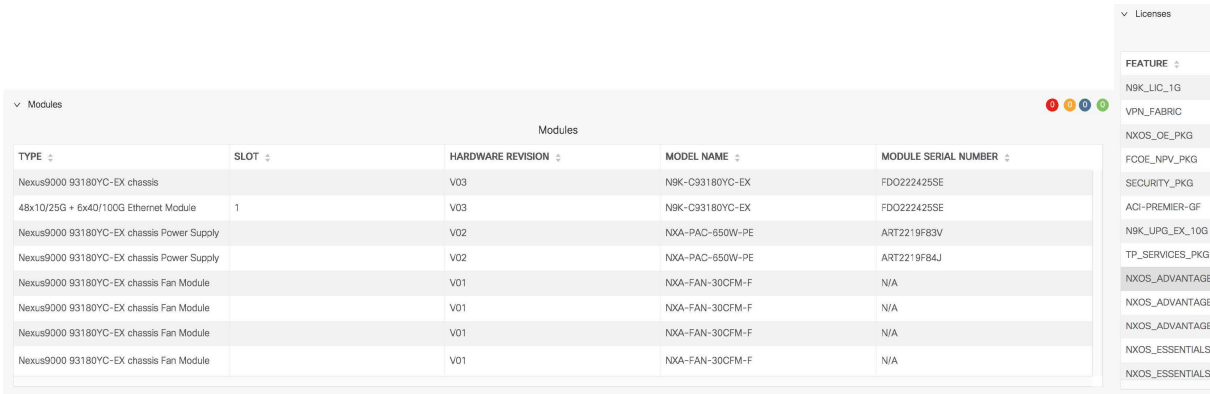


スイッチ インベントリ レポート

このレポートは、スイッチ インベントリに関する概要を提供します。

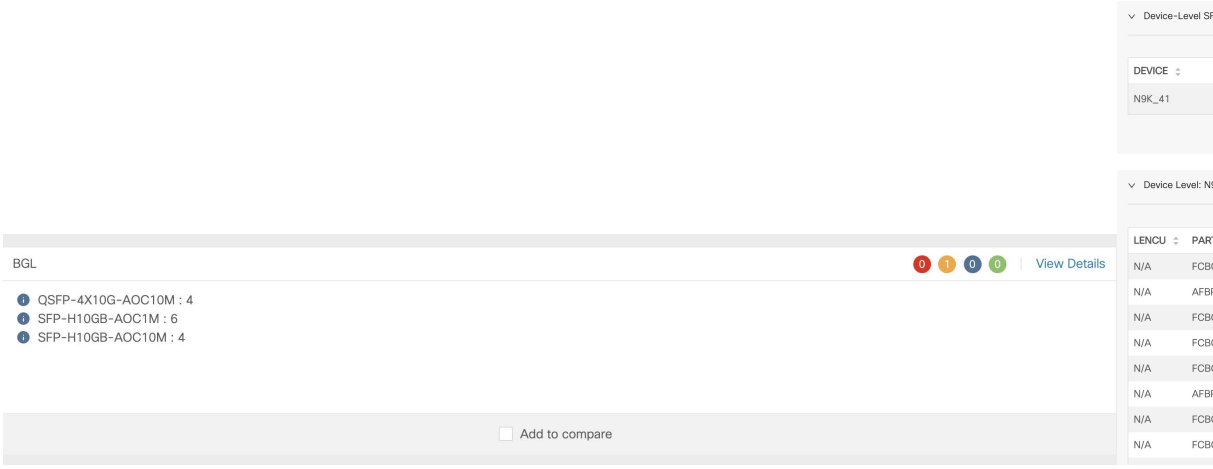


[詳細の表示（View Details）] をクリックして、モジュールとライセンスに関する詳細情報を表示します。



SFPレポート

このレポートは、ファブリックおよびデバイス レベルでの SFP の使用率に関する情報を提供します。



（注） スイッチインベントリおよび SFP レポートは、Cisco Nexus デバイスでのみサポートされます。

トラブルシューティング レポート

これらのレポートは、トラブルシューティングのシナリオに役立つように生成されます。現在、定義済みのトラブルシューティング レポートは **NVE VNI** カウンタ レポートのみです。**NVE VNI カウンタ** レポートの生成では、ネットワーク トラフィックに基づいて上位ヒットの VNI を特定するための定期的なチェックが実行されます。大規模なセットアップでは、レポートの生成頻度を 60 分以上に制限することをお勧めします。

NVE VNI カウンタ レポート

このレポートは、ファブリック内の各 VNI の **show nve vni counters** コマンド出力を収集します。

最も古いレポートと最新のレポートを比較すると、**[サマリ（Summary）]** セクションには上位 10 件のヒット VNI が表示されます。上位ヒット VNI は、次のカテゴリに表示されます。

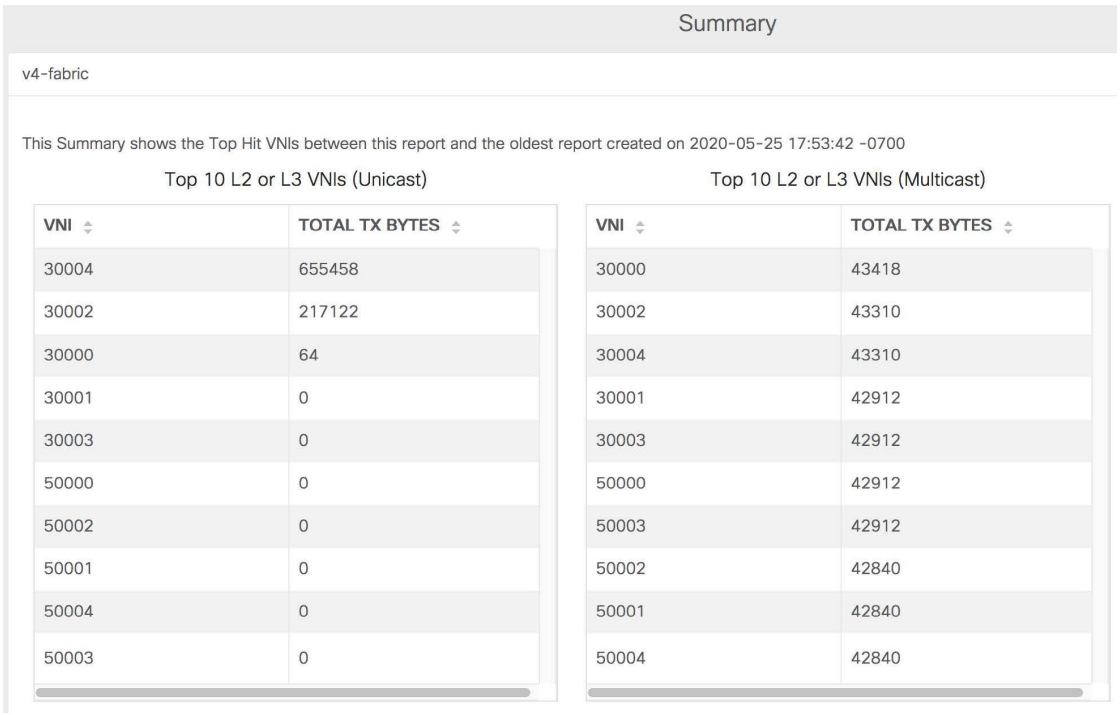
- ユニキャスト トラフィック用の L2 または L3 VNI
- マルチキャスト トラフィック用の L2 または L3 VNI
- ユニキャスト トラフィック用の L2 のみの VNI
- マルチキャスト トラフィック用の L2 のみの VNI
- ユニキャスト トラフィック用の L3 のみの VNI
- マルチキャスト トラフィック用の L3 のみの VNI

最も古いレポートは、現在のレポートタスクで保存された最初のレポートを参照します。現在のレポートと比較する必要がある最初のレポートとして特定のレポートを選択する場合は、選択したレポートが最初で最も古いレポートになるように、選択したレポートよりも古いすべてのレポートを削除します。

たとえば、昨日の午前 8 時、午後 4 時、および午後 11 時に 3 つのレポートが実行されたとします。今日のレポートの最初の最も古いレポートとして午後 11 時にレポートを使用する場合は、昨日の午前 8 時と午後 4 時に実行されました。

定期レポートの場合、最も古いレポートは、期間の開始時刻に実行される最初のレポートです。日次および週次レポートの場合、現在のレポートが以前に生成されたレポートと比較されます。

[サマリ（Summary）] セクションには、送信された合計バイト数と VNI に関する情報を含むカラムごとのレポートが表示されます。より多くの列を表示するには、ウィンドウの下部にある水平スクロール バーを使用します。


Summary

v4-fabric

This Summary shows the Top Hit VNIs between this report and the oldest report created on 2020-05-25 17:53:42 -0700

Top 10 L2 or L3 VNIs (Unicast)

VNI	TOTAL TX BYTES
30004	655458
30002	217122
30000	64
30001	0
30003	0
50000	0
50002	0
50001	0
50004	0
50003	0

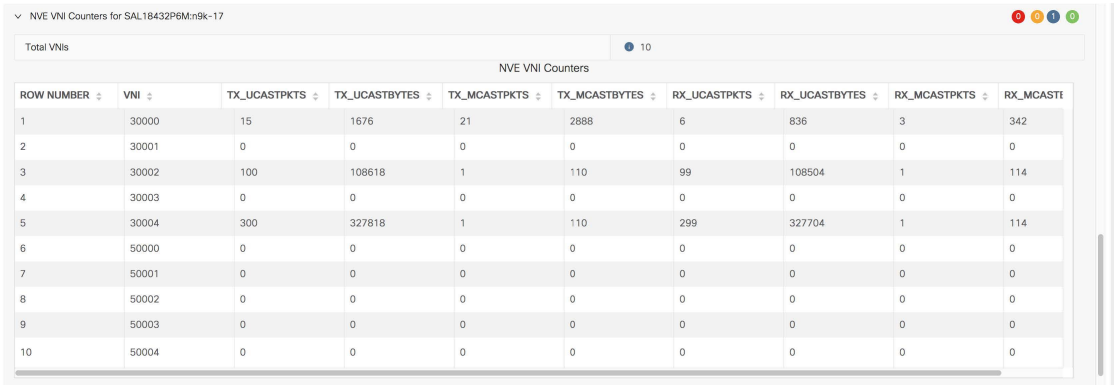
Top 10 L2 or L3 VNIs (Multicast)

VNI	TOTAL TX BYTES
30000	43418
30002	43310
30004	43310
30001	42912
30003	42912
50000	42912
50003	42912
50002	42840
50001	42840
50004	42840

VNI
30004
30002
30000
30001
30003

（注） NVE VNI カウンタ レポートの**[サマリ（Summary）]**セクションでは、スイッチのリロード後またはスイッチのカウンタのクリア後にレポートが生成された場合、[合計送信バイト数（TOTAL TX BYTES）]列に負の数が表示されます。番号は、後続のレポートで正しく表示されます。回避策として、スイッチをリロードするか、カウンタをクリアする前に、古いレポートをすべて削除するか、新しいジョブを作成することを推奨します。

詳細については、**[詳細の表示（View Details）]**をクリックしてください。このセクションでは、スイッチごとに NVE VNI とカウンタを示します。


NVE VNI Counters for SAL18432P6M:n9k-17

Total VNIs 10

NVE VNI Counters

ROW NUMBER	VNI	TX_UCASTPKTS	TX_UCASTBYTES	TX_MCASTPKTS	TX_MCASTBYTES	RX_UCASTPKTS	RX_UCASTBYTES	RX_MCASTPKTS	RX_MCASTE
1	30000	15	1676	21	2888	6	836	3	342
2	30001	0	0	0	0	0	0	0	0
3	30002	100	108618	1	110	99	108504	1	114
4	30003	0	0	0	0	0	0	0	0
5	30004	300	327818	1	110	299	327704	1	114
6	50000	0	0	0	0	0	0	0	0
7	50001	0	0	0	0	0	0	0	0
8	50002	0	0	0	0	0	0	0	0
9	50003	0	0	0	0	0	0	0	0
10	50004	0	0	0	0	0	0	0	0

レポートの表示方法の詳細については、プログラム可能レポート を参照してください。

テンプレート機能のレポート

generateReport メソッド

レポートの生成中に generateReport メソッドが呼び出されます。レポートにはレポート導入ロジックが含まれます。このメソッドは、任意のコンテキスト オブジェクトを受け入れ、WrappersResp オブジェクトを返します。WrappersResp の詳細については、リンクを参照してください。

検証メソッド

検証メソッドはオプションです。テンプレートでこのメソッドが定義されている場合、プログラマブル レポート アプリケーションはこのメソッドを呼び出して、ジョブの作成中に事前検証チェックを実行します。このメソッドは、選択されたデバイスまたはファブリックの数に関係なく、ジョブが作成され、1 回だけ呼び出された場合にのみ呼び出されます。検証を通過すると、このメソッドは SuccessRetCode を持つ WrappersResp オブジェクトを返します。検証が失敗した場合、このメソッドはエラー リストとともに FailureRetCode を返します。

正常な検証と失敗した検証の例は次のとおりです。

*正常な検証

```
def validate(context):
    respObj = WrappersResp.getRespObj()

 ## Validation logic here

    respObj.setSuccessRetCode()
    return respObj
```

*失敗した検証

```
def validate(context):
    respObj = WrappersResp.getRespObj()

 ## Validation logic here

    respObj.setFailureRetCode()
    respObj.addErrorReport(template_name,error)
    return respObj
```

コンテキスト パラメータの内容に基づいて検証を実行することもできます。

コンテキスト パラメータ

コンテキスト パラメータは、次の属性で構成されます。

- ユーザー名：ジョブを作成したユーザーの名前
- ユーザーロール：ジョブを作成したユーザーのロール
- Job ID
- 再発：現在、1 回、毎日、毎週、毎月、オンデマンド、定期
- 期間：繰り返しが定期的な場合、期間には選択した頻度が表示されます。

ジョブ コンテキスト API の詳細については、「ジョブ コンテキスト情報」セクションを参照してください。

レポート Python ライブラリ

REPORT には次のコンポーネントがあります。

- 要約
  - キーと値
  - メッセージ - 推論
- 詳細/セクション
  - キーと値
  - JSON ドキュメント – カード
  - JSON ドキュメントの配列 – テーブル
- コマンド ログ

レポート JSON モデルを生成するための Python ライブラリが提供されています。これらの API を使用するには、次のインポート ステートメントをテンプレートに追加する必要があります。

```
from reportlib.preport import Report
```

レポート API

レポートの作成

「レポート」オブジェクトを作成するには、この API を使用します –

```
report = Report (“Report title”)
```

サマリの追加

各レポートには概要を含めることができます。これは python の辞書です。概要を追加するには、この API を使用します –

```
summary = report.add_summary ()
```

[概要へのコンテンツの追加（Adding Content to the Summary）]

概要にコンテンツを追加するには、次の API を使用します。

キーと値 -

```
summary [‘NXOS Version’] = ‘8.4(1)’
```

メッセージとインターフェイス -

```
summary.add_message (“Simple message”)
```

Note Cisco DCNM リリース 11.4(1) では、概要の値として JSON オブジェクトを追加することはサポートされていません。次の例はサポートされていません -

```
summary["info"] = {"key":"value","key-2":"value-2"}
```

[概要でテーブルの追加（Adding tables in Summary）]

概要にテーブルを追加するには、この API を使用します –

```
table = summary.add_table(title,_id)
```

title： テーブルのタイトル。

_id： テーブルの一意の識別子。

[テーブルへの行の追加（Adding rows to the table）]

テーブルに行を追加するには、この API を使用します –

```
table.append(value, _id)
```

値：JSON オブジェクトです。ネストされた JSON はサポートされません。

_id：行の一意の識別子です。

[セクションの追加（Adding a Section）]

セクションは、レポートコンテンツの論理グループです。セクションは、必要な情報を表示するためにユーザーが作成および構成します。セクションを追加するには、この API を使用します。

```
section = report.add_section ("Section title",_id)
```

_id：セクションの一意の識別子。

[セクションのキーと値へのコンテンツの追加（Adding Content to a Section Key and Values）]

セクションに単純なキーと値のペアを追加するには、この API を使用します。

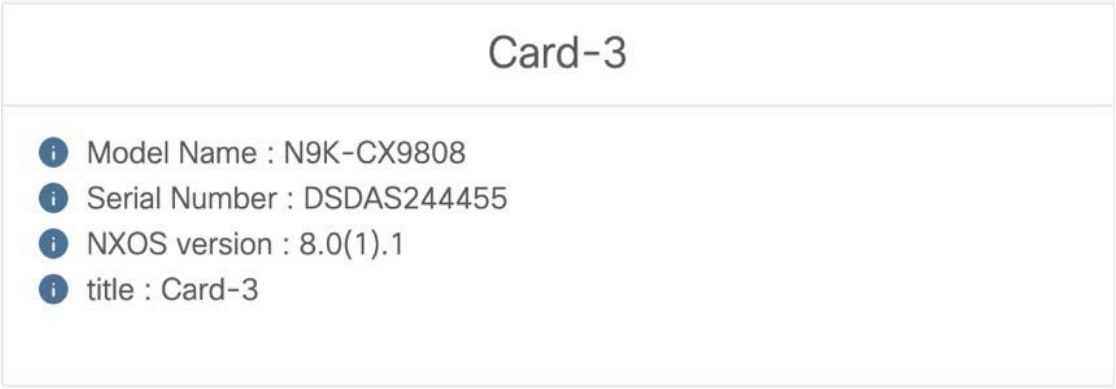
```
section['key'] = 'value'
```

[JSON ドキュメント – カード（JSON Document – Cards）]

JSON ドキュメントは、単純なキーと値のペアが追加されるのと同じ方法で追加できます。

Note ネストされた JSON は、Cisco DCNM リリース 11.4(1) ではサポートされていません。

カード ウィジェットとして表示される JSON ドキュメントの例を次に示します。



JSON ドキュメントの配列 – テーブル

テーブルを作成し、このテーブルに行を追加するには、この API を使用します。

```
section.append(key, dictionary, _id)
```

_id：テーブルの行を識別する一意の識別子。*_id* が重複すると、一意の id 違反エラーが発生します。

例：

```
section.append('Switch Details', {'name': 'N5K'},'DSDAS244455')
```

この API を使用したテーブルの作成には、次の制限があります。

- すべての JSON ドキュメントには、同じキー/列のセットが必要です。列の数または列名が異なると、テーブルが Web UI に表示されない場合があります。
- ネストされた JSON はサポートされません。

[Formatters]

Formatter は、ユーザー インターフェイスに表示される値の追加の書式設定を有効にします。たとえば、値を ERROR、SUCCESS、WARNING、および INFO としてマークできます。これらの値は色分けされ、Web UI に表示されます。エラーは赤、警告は黄色、情報は青、成功は緑で表示されます。

形式を構成するには、この API を使用します。

```
Formatter.add_marker(value,marker)
```

値：マーカーを追加する値

マーカー：Marker.ERROR、Marker.SUCCESS、Marker.WARNING、および Marker.INFO

例：

```
Formatter.add_marker (“NXOS version”,Marker.INFO)
```

グラフ

概要とセクションの両方にグラフを追加できます。

チャートを概要に追加するには、この API を使用します-

```
report = Report("title")
summary = report.add_summary()
summary.add_chart(ChartType, _id)
```

ChartType：ChartTypes.COLUMN_CHART、ChartTypes.PIE_CHART、および ChartTypes.LINE_CHART

_id：チャートの一意の ID

チャートをセクションに追加するには、この API を使用します。

```
report = Report("title")
section = report.add_section ("section_title",_id)
section.add_chart(ChartType, _id)
```

ChartType：ChartTypes.COLUMN_CHART、ChartTypes.PIE_CHART、および ChartTypes.LINE_CHART

_id：チャートの一意の ID

Note インポート セクションでクラスがインポートされていることを確認します。

円グラフ

円グラフで情報を表示するには、この API を使用します。

タイトルとサブタイトルを設定するには：

```
pie_chart.set_title("Chart title")
pie_chart.set_subtitle("Sub title")
```

値を追加するには：

```
pie_chart.add_value("key",value)
```

キー：文字列キー

値：数字の値

[列チャート（Column chart）]

縦棒グラフで情報を表示するには、この API を使用します。

タイトルとサブタイトルのタイトルを設定するには：

```
column_chart.set_title("Chart title")
column_chart.set_subtitle("Sub title")
```

X 軸と Y 軸のタイトルを設定するには

```
column_chart.set_xAxis_title("X-Axis title")
column_chart.set_yAxis_title("y-Axis title")
```

値を追加するには：

```
bar_chart.add_value("key",value,category)
```

キー：文字列キー

値：数字の値

カテゴリ：縦棒グラフは、データをカテゴリと呼ばれる論理グループに分割します。指定されたキーには、各カテゴリの値が必要です。たとえば、デバイス数がキーで、ファブリック名がカテゴリです。チャートには、各ファブリックのデバイス数が必要です。

折れ線グラフ

折れ線グラフで情報を表示するには、この API を使用します。

タイトルとサブタイトルのタイトルを設定するには：

```
line_chart.set_title("Chart title")
line_chart.set_subtitle("Sub title")
```

X 軸と Y 軸のタイトルを設定するには

```
line_chart.set_xAxis_title("X-Axis title")
line_chart.set_yAxis_title("y-Axis title")
```

値を追加するには：

```
line_chart.add_value("key",value,category)
```

キー：文字列キー

値：数字の値

カテゴリ：折れ線グラフは、データをカテゴリと呼ばれる論理グループに分割します。指定されたキーには、各カテゴリの値が必要です。たとえば、「デバイス数」がキーで、「ファブリック名」がカテゴリです。チャートには、ファブリックまたはカテゴリごとのデバイス数が必要です。

[デバイスでの CLI の実行（Running CLIs on a Device）]

デバイスでの CLI の実行を構成するには、この API を使用します。

```
from reportlib.preport import show
cli_responses = show(serial_number,*commands)
```

serial_number：コマンドを実行する必要があるデバイスのシリアル番号。VDC インスタンスの場合、シリアル番号は **[serial_number:vdc_name]** です。

**commands*：デバイスで実行されるコマンド。これらは可変引数です。

例：

- 単一のスイッチでコマンドを実行する：

```
cli_responses = show("FOX1816G0S9",'show version | xml', 'show inventory | xml', 'show
license usage | xml')
```

- 複数のスイッチでコマンドを実行する：

```
cli_responses = show( ["FOX1816G0S9","SSI15470HJ5"],'show version | xml', 'show
inventory | xml', 'show     license usage | xml')
```

[コマンドを表示して応答を保存（Show commands and store responses）]

show コマンドを構成し応答を保存するには、この API を使用します。

```
from reportlib.preport import show_and_store
cli_responses = show_and_store(report,serial_number,*commands)
```

report：以前に作成されたレポート オブジェクト。

serial_number：コマンドを実行するデバイスのシリアル番号。VDC の場合、シリアル番号は *serial_number:vdc_name* である必要があります。シリアル番号のリストを追加して、複数のデバイスで同じコマンド セットを実行できます。

commands：デバイスで実行するコマンド。これらは可変引数です。複数のコマンドを指定できます。

例：

- 単一のスイッチでコマンドを実行する：

```
cli_responses = show_and_store(report, “FOX1816G0S9”, 'show version | xml', 'show
inventory | xml', 'show license usage | xml')
```

- 複数のスイッチでコマンドを実行する：

```
cli_responses = show_and_store(report, [“FOX1816G0S9”,”SSI15470HJ5”], 'show version
 | xml', 'show inventory | xml', 'show license usage | xml')
```

Note この API は、デバイスからの応答をレポートとともに elasticsearch に保存します。すべての応答を保存すると、使用可能なストレージ スペースが減少する可能性があるため、この API を使用するときは注意することをお勧めします。

[戻り値（Return value）]

上記の API は、応答のリストを返します。各応答は、次の構造を持つディクショナリです。

```
{
'status': 'success' | 'failed,
'response':<response from device>,
'command':<cli command>,
'serial_number': <device serial number>
}
```

複数のスイッチの場合、応答はスイッチごとに個別のエントリを持つ応答のリストです。

例：

```
[
{
'status': 'success',
'response':<response from device>,
'command':’show version’,
'serial_number': ‘FOX1816G0S9’
},
{
'status': 'success',
'response':<response from device>,
'command':’show version’,
'serial_number': ‘SSI15470HJ5’
}
]
```

[ジョブ コンテキスト情報（Job context information）]

アプリケーションからジョブをスケジュールしているときに繰り返しを表示するには、この API を使用します。

```
get_recurrence(context)
```

戻り値は、NOW、ONCE、DAILY、WEEKLY、MONTHLY、ONDEMAND、および PERIODIC です。

ジョブが定期的にスケジュールされ、特定の期間に関する情報を取得する必要がある場合は、この API を使用します。

```
period = get_period(context)
```

period.get_period()：期間を返します。

period. get_time_unit()：時間単位（HOURS、MINUTES）を返します。

[履歴レポートによる分析（Analysis with Historical Reports）]

[以前生成されたレポートを取得（Retrieve previously generated reports）]

過去に生成されたレポートを取得するには、*get_previous_reports()* メソッドを使用します。これは、現在のデータと履歴データに基づいて分析を実行するために使用できます。この API は、レポートが作成された時間の降順でレポートのリストを返します。

```
List of reports = get_previous_reports(context,entity,count)
```

コンテキスト：generateReport（コンテキスト）メソッドから入力として受け取ったオブジェクト

エンティティ：serial_number またはファブリック名

カウント：取得するレポートの数

[最も古いレポートを取得（Get oldest report）]

最も古いレポートを取得するには、この API を使用します。

```
oldest_report = get_oldest_report(context,entity)
```

コンテキスト：generateReport（コンテキスト）メソッドから入力として受け取ったオブジェクト

エンティティ：serial_number またはファブリック名

上記の両方の API は、情報を取得するために次の API を使用して Report オブジェクトを返します。

- 概要を取得する：*report.get_summary()*
- セクションの取得：*report.get_section(_id)*。*_id* は *[*セクションの追加（*Adding a Section*）*]* で説明したセクションの一意の識別子です。

[XML ユーティリティ（XML Utilities）]

XML ユーティリティは、xml.etree.elementtree（https://docs.python.org/2/library/xml.etree.elementtree.html）に基づいています。

[getxmltree]

指定されたタグの下にある XML ツリーを返すには、この API を使用します。

```
from reportlib.preport import getxmltree
xml_element_tree = getxmltree(xml_string,tag)
```

xml_string：デバイスからの XML 応答。

タグ：XML タグ。このタグの下の完全な XML は、ElementTree として返されます。

xml_element_tree：xml.etree.ElementTree オブジェクトを返す API

[getxmlrows]

CLI 応答に行が含まれている場合に行の配列を取得するには、この API を使用します。

```
from reportlib.preport import getxmlrows
rows = getxmlrows(xml_tree,tag_xpath)
```

xml_tree：xml.etree.ElementTree オブジェクト。

tag_xpath：XML レコードの xpath。
https://docs.python.org/2/library/xml.etree.elementtree.html#xpath-support を参照してください。

行：行の配列

[getnodevalue]

XML ノード値を読み取るには、この API を使用します。

```
from reportlib.preport import getnodevalue
value = getnodevalue(xml_tree,node_xpath)
```

xml_tree：**xml.etree.ElementTree** オブジェクト

node_xpath：XML レコードの xpath。
https://docs.python.org/2/library/xml.etree.elementtree.html#xpath-support を参照してください。

[ノードの存在を確認する（Check for existence of node）]

この API は、指定されたタグが XML ツリーに存在するかどうかに応じて、True または False を返します。

```
from reportlib.preport import
has_tag has_tag(xml_tree,tag)
```

xml_tree：**xml.etree.ElementTree** オブジェクト

[WrappersResp]

各レポートは**WrappersResp** タイプのオブジェクトを返す必要があります。これは、以下に示す API を使用して開始できます。これを com.cisco.dcbu.vinci.rest.services.jython import WrappersResp からインポートします。

```
respObj = WrappersResp.getRespObj()
```

WrapperResp のリターン コードは、レポートが正常に実行されたかどうかを示します。

- すべてのコマンドが実行され、必要な情報が抽出された場合、レポートは成功 API - *respObj.setSuccessRetCode()* を返します。
- コマンドの失敗などの例外が発生した場合、レポートは失敗 API - *respObj.setFailureRetCode()* を返します。

エラーコードを設定すると、レポートの実行に問題があり、レポートが生成されないことを示します。

エラーのあるレポートを返すには、Formatter を使用してエラーをマークし、*WrapperResp* を *Success* に設定します。詳細については、「*Formatters*」を参照してください。

発生する可能性のあるエラーについては、この API を使用してエラーの理由を指定できます。

```
respObj.addErrorReport(template_name,error_message)
```

作成したレポート オブジェクトは、次に示すように *WrappersResp* の値に設定する必要があります。

```
respObj.setValue(report)
```

ロガー

ロガーは、レポートテンプレートからのメッセージのログを有効にします。ロガーを使用して記録される情報は、「/usr/local/cisco/dcm/fm/logs/preport_jython.log」に記録されます。

```
Logger.info("message")
Logger.debug("message")
Logger.error("message")
Logger.trace("message")
Logger.warn("message")
```

テンプレートの追加

Cisco Web UI からユーザー定義のテンプレートを作成し、ジョブをスケジュールするには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択します。

[テンプレート プロパティ（Template Properties）] ウィンドウに、テンプレートの名前、その説明、サポートされるプラットフォーム、およびタグが表示されます。

ステップ 2 **[追加（Add）]** をクリックして新しいテンプレートを追加します。

[テンプレートのプロパティ（Properties）] ウィンドウが表示されます。

ステップ 3 [テンプレート名、詳細、タグとサポートされているプラットフォームを指定。（Specify a template name, description, tags, and supported platforms for the new template.）]

ステップ 4 テンプレートの**[テンプレート タイプ（Template Type）]**を指定します。

ステップ 5 テンプレートの**[テンプレート サブ タイプ（Template Sub Type）]**と**[テンプレート コンテンツ タイプ（Template Content Type）]**を選択します。

ステップ 6 **[詳細（Advanced）]** タブをクリックして、**[実装（Advanced）]**、**[依存関係（Dependencies）]**、**[公開（Published）]**、**[インポート（Imports）]**などの他のプロパティを編集します。**[発行済み（Published）]** を選択して、テンプレートを読み取り専用にします。公開されたテンプレートは編集できません。

ステップ 7 **[インポート（Imports）] > [テンプレート名（Template Name）]** リストから、テンプレートチェックボックスを選択します。

基本テンプレート コンテンツは、**[テンプレート コンテンツ（Template Content）]** ウィンドウに表示されます。ベース テンプレートには、テンプレート プロパティ、テンプレート変数、およびテンプレート コンテンツが表示されます。他のテンプレートにこのテンプレートをインポートすることができます。そして、基本テンプレートの内容は、拡張テンプレートの適切な場所に置き換えられます。拡張テンプレートを起動すると、基本テンプレートのパラメータ入力も取得されます。また、置換された内容は、完全な CLI コマンドの生成に使用されます。

Note 基本テンプレートは CLI テンプレートです。

ステップ 8 **[OK]** をクリックしてテンプレートのプロパティを保存するか、ウィンドウの右上隅にあるキャンセル アイコンをクリックして変更を元に戻します。

Note **[テンプレート プロパティ（Template Property）]** をクリックして、テンプレート プロパティを編集できます。

ステップ 9 **[テンプレート コンテンツ（Template Content）]** をクリックして、テンプレートの構文を編集します。構成テンプレートの構造については、「テンプレートの構造」の項を参照してください。

ステップ 10 **[テンプレート構文の検証]** をクリックして、テンプレート値を検証します。

エラーまたは警告メッセージが表示された場合は、エラーおよび警告フィールドをクリックして、**検証テーブル（Validation Table）**で検証の詳細を確認できます。

Note 警告のみがある場合は、テンプレートの保存を続行できます。ただし、エラーが発生した場合は、続行する前にテンプレートを編集してエラーを修正する必要があります。[開始行（Start Line）] 列の下の行番号をクリックして、テンプレートの内容でエラーを見つけます。テンプレート名がないテンプレートを検証すると、エラーが発生します。

ステップ 11 **[保存（Save）]** をクリックして、テンプレートを保存します。

ステップ 12 **[保存して閉じる（Save and Exit）]** をクリックし構成を保存して、構成テンプレート画面に戻ります。

テンプレートの変更

ユーザ定義のテンプレートを編集できます。ただし、定義済みのテンプレートおよびすでに公開されているテンプレートは編集できません。

Procedure

ステップ 1 **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** から、テンプレートを選択します。

ステップ 2 **[テンプレートの変更/表示（Modify/View template）]** をクリックします。

ステップ 3 テンプレートの説明とタグを編集します。

編集したテンプレートの内容が右側のペインに表示されます。

ステップ 4 **[インポート（Imports）] > [テンプレート名（Template Name）]** リストから、テンプレートチェックボックスを選択します。

基本テンプレート コンテンツは、**[テンプレート コンテンツ（Template Content）]** ウィンドウに表示されます。**[テンプレート コンテンツ（Template Content）]** ウィンドウで、要件に基づいてテンプレート コンテンツを編集できます。テンプレートのコンテンツの編集については、**[テンプレート コンテンツ（Template Content）]** ウィンドウの横にある [ヘルプ（Help）] アイコンをクリックします。

ステップ 5 テンプレートでサポートされているプラットフォームを編集します。

ステップ 6 **[テンプレートシンタックスの検証（Validate Template Syntax）]** をクリックして、テンプレート値を検証します。

ステップ 7 **[保存（Save）]** をクリックして、テンプレートを保存します。

ステップ 8 **[保存して閉じる（Save and Exit）]** をクリックし構成を保存して、構成テンプレート画面に戻ります。

テンプレートのコピー

Cisco DCNM Web UI からテンプレートをコピーするには、以下の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択して、テンプレートを選択します。

ステップ 2 **[テンプレートに名前を付けて保存（Save Template As）]** をクリックします。

ステップ 3 テンプレート名、説明、タグ、およびその他のパラメータを編集します。

編集したテンプレートのコンテンツが右側のペインに表示されます。

ステップ 4 **[インポート（Imports）] > [テンプレート名（Template Name）]** リストから、テンプレートチェックボックスを選択します。

基本テンプレート コンテンツは、**[テンプレート コンテンツ（Template Content）]** ウィンドウに表示されます。**[テンプレート コンテンツ（Template Content）]** ウィンドウで、要件に基づいてテンプレート コンテンツを編集できます。テンプレートのコンテンツの編集については、**[テンプレート コンテンツ（Template Content）]** ウィンドウの横にある [ヘルプ（Help）] アイコンをクリックします。

ステップ 5 テンプレートでサポートされているプラットフォームを編集します。

ステップ 6 **[テンプレートシンタックスの検証（Validate Template Syntax）]** をクリックして、テンプレート値を検証します。

ステップ 7 **[保存（Save）]** をクリックして、テンプレートを保存します。

ステップ 8 **[保存して閉じる（Save and Exit）]** をクリックし構成を保存して、構成テンプレート画面に戻ります。

テンプレートの削除

ユーザ定義テンプレートを削除できます。ただし、事前定義されたテンプレートは削除できません。Cisco DCNM リリース 11.0(1) 以降、複数のテンプレートを一度に削除できます。

Cisco DCNM Web UI からテンプレートを削除するには、以下の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択します。

ステップ 2 チェックボックスを使用してテンプレートを選択し、**[テンプレートの削除（Remove template）]** アイコンをクリックします。

テンプレートは警告メッセージなしで削除されます。

What to do next

DCNM Web UI のテンプレート リストからテンプレートが削除されます。DCNM サービスを再起動すると、削除されたテンプレートが **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** ページに表示されます。

テンプレートを永久的に削除するには、ローカル ディレクトリ `Cisco Systems\dcm\dcnm\data\templates\` に位置するテンプレートを削除します。

テンプレートのインポート

Cisco DCNM Web UI からテンプレートをインポートするには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択し、**[インポート テンプレート（Import Template）]** をクリックします。

ステップ 2 コンピュータに保存されているテンプレートを参照して選択します。

必要に応じて、テンプレートパラメータを編集できます。詳細については、テンプレートの変更, on page 430を参照してください。

Note テンプレート内の「\n」は、インポートおよび編集されると改行文字と見なされますが、ZIP ファイルとしてインポートされると正常に機能します。

ステップ 3 **[テンプレート構文の検証]** をクリックして、テンプレートを検証します。

ステップ 4 **[保存（Save）]** をクリックしてテンプレートを保存するか、**[保存して終了（Save and Exit）]** をクリックしてテンプレートを保存して終了します。

テンプレートのエクスポート

Cisco DCNM Web UI からテンプレートをエクスポートするには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択します。

ステップ 2 チェック ボックスを使用してテンプレートを選択し、**[テンプレートのエクスポート（Export Template）]** アイコンをクリックします。

ブラウザは、テンプレートを開くか、ディレクトリに保存するように要求します。

イメージ管理

デバイスを最新のソフトウェアバージョンに手動でアップグレードすると、時間がかかり、エラーが発生しやすくなります。迅速で信頼性の高いソフトウェアアップグレードを実現するために、イメージ管理はアップグレードの計画、スケジューリング、ダウンロード、およびモニタリングに関連する手順を自動化します。画像管理は、Cisco Nexus スイッチと でのみサポートされます。

（注） アップグレードする前に、Cisco Nexus 9000 シリーズ スイッチおよび Cisco Nexus 3000 シリーズ スイッチの POAP ブート モードが無効になっていることを確認します。POAP を無効にするには、スイッチ コンソールで [no boot poap enable] コマンドを実行します。ただし、アップグレード後に有効にすることができます。

[画像管理（Image Management）] メニューには、次のサブメニューとオプションが含まれています：

表 *4:* 画像管理メニュー

サブメニュー	オプション	操作	
イメージのアップロード	[スマート イメージ管理（Smart Image Management）]	イメージのアップロード	
		イメージの削除	
インストールとアップグレード	アップグレード履歴 ウィンドウ名：**ソフトウェア アップグレード タスク**	表示	
		削除	
		新規インストール	新しい ISSU インストール
			EPLD インストール
		インストールの終了	
	スイッチ レベルの履歴	デバイス アップグレード タスクを表示	
		スイッチ レベル履歴テーブルの更新	
パッケージ [SMU/RPM]	パッケージ	パッケージおよびパッチのインストール	
		パッケージおよびパッチのアンインストール	
		パッケージおよびパッチのアクティブ化	
		非アクティブ化	
画像管理ポリシー	画像管理ポリシー	画像管理ポリシーの追加	
		画像管理ポリシーの削除	

ユーザー ロールが **network-admin** または **device-upg-admin** であり、次の操作を実行するために DCNM をフリーズしていないことを確認します。

- イメージをアップロードまたは削除します。
- イメージのインストール、削除、またはイメージのインストールを終了します。
- パッケージおよびパッチをインストールまたはアンインストールします。
- パッケージおよびパッチをアクティブ化または非アクティブ化します。
- 画像管理ポリシーを追加または削除します（network-admin ユーザー ロールにのみ適用）。
- 管理ポリシーを表示します。

ユーザ ロールが network-admin、network-stager、network-operator、または device-upg-admin の場合は、任意のイメージインストールまたはデバイスアップグレードタスクを表示できます。DCNM がフリーズ モードの場合は、それらを表示することもできます。

[スマート イメージ管理（Smart Image Management）]

この機能により、POAP およびスイッチのアップグレード中に使用されるイメージをアップロードまたは削除できます。（This feature allows you to upload or delete images that are used during POAP and switch upgrade.） **[パッケージ（Packages）]** ウィンドウで、インストールに使用される RPM および SMU をアップロードまたは削除することもできます。 Cisco DCNM Web UI ホームページから **スマート イメージ管理（Image and Configuration Servers Smart Image Management）]** ウィンドウを表示するには、**コントロール（Repositories Control）] > [イメージ管理（Image Management）] > [イメージをアップロード（Image Upload）]** を選択します。

[**スマート イメージ管理**（Image and Configuration Servers Smart Image Management）] ウィンドウで、次の詳細を表示できます。

フィールド	説明
[プラットフォーム（Platform）]	プラットフォームの名前を指定します。イメージ、RPM、または SMU は、次のように分類されます。 • N9K/N3k • N6K • N7K • N77K • N5K • その他 • サード パーティ N9K プラットフォームと N3K プラットフォームのイメージは同じです。 アップロードされたイメージが既存のプラットフォームのいずれにもマッピングされていない場合、プラットフォームは [その他（Other）] になります。 プラットフォームは RPM の [サード パーティ（Third Party）] になります。
イメージ名	アップロードしたイメージ、RPM、または SMU のファイル名を指定します。
[イメージ タイプ（Image Type）]	イメージ、[EPLD、（EPLD,）]RPM、または SMU のファイル タイプを指定します。

フィールド	説明
[イメージのサブタイプ（Image Subtype）]	イメージ、EPLD、RPM、またはSMUのファイルタイプを指定します。 ファイルタイプ EPLD は [epld] です。イメージのファイル タイプは、[nxos]、[system] または [kickstart] です。RPM のファイルタイプは [feature] で、SMU のファイル タイプは [patch] です。
NXOS バージョン	Cisco スイッチのみの NXOS イメージ バージョンを指定します。
イメージ バージョン	Cisco 以外のデバイスを含むすべてのデバイスのイメージ バージョンを指定します。
サイズ（バイト）	イメージ、RPM、または SMU ファイルのサイズをバイト単位で指定します。
Checksum	イメージのチェックサムを指定します。チェックサムは、イメージ、RPM、または SMU のファイルに破損がないかどうかをチェックします。Cisco の Web サイトからダウンロードしたファイルと [イメージのアップロード（Image Upload）] ウィンドウでアップロードしたファイルのチェックサム値が同じかどうかを確認することで、信頼性を検証できます。

すべての列を並べ替えることができます。

イメージのアップロード

Cisco DCNM Web UI からサーバにさまざまなタイプの画像をアップロードするには、次の手順を実行します。

Note デバイスは、POAP またはイメージのアップグレード中にこれらのイメージを使用します。RPMとSMU は、**[パッケージ（Packages）]** ウィンドウで使用されます。すべての画像、RPM、およびSMU が **[画像管理ポリシー（Image Management Policies）]** ウィンドウで使用されます。

画像をアップロードするには、ユーザー ロールが **network-admin** または **device-upg-admin** である必要があります。**network-stager** ユーザ ロールでは、この操作を実行できません。

Procedure

ステップ 1 **[制御（Control）] > [画像管理（Image Management）] > [画像のアップロード（Image Upload）]** を選択します。

のスマート画像管理（Smart Image Management）] ウィンドウが表示されます。

ステップ 2 **[画像のアップロード（Image Upload）]** をクリックします。

[アップロードするファイルを選択（Select File to Upload）] ダイアログボックスが表示されます。

ステップ 3 **[ファイルの選択（Choose file）]** をクリックして、デバイスのローカル リポジトリからファイルを選択します。

ステップ 4 ファイルを選択し、**[アップロード（Upload）]**をクリックする。

ZIP ファイルもアップロードできます。シスコ DCNM は画像ファイルを処理して検証し、それに応じて既存のプラットフォームで分類します。**N9K/N3K**、**N6K**、**N7K**、**N77K**、または **N5K** プラットフォームに該当しない場合、イメージファイルは **サードパーティ**または**その他**のプラットフォームに分類されます。**サードパーティ** プラットフォームは、RPM にのみ適用されます。

ステップ 5 [OK] をクリックします。

[EPLD 画像、（EPLD images,）]RPM、および SMU はリポジトリにある次のパスにアップロードされます：**/var/lib/dcnm/upload/<platform_name>**

すべての NX-OS、キックスタートおよびシステム 画像はリポジトリにある次のパスにアップロードされます：**/var/lib/dcnm/images** と **/var/lib/dcnm/upload/<platform_name>**

ファイル サイズとネットワーク帯域幅によっては、アップロードに時間がかかります。

Note すべての Cisco Nexus シリーズ スイッチのイメージをアップロードできます。

Cisco Nexus 9000 シリーズ スイッチの EPLD イメージのみをアップロードできます。

ネットワークの速度が遅い場合は、Cisco DCNM の待機時間を 1 時間に増やして、画像のアップロードを完了します。Cisco DCNM Web UI からの待機時間を増やすには、次の手順を実行します。

a. **[管理者 (Administrator)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** を選択します。

b. **csrf.refresh.time** プロパティを検索し、値を **60** に設定します。

Note 値は分単位です。

c. [Apply Changes] をクリックします。

d. Cisco DCNM サーバを再起動します。

イメージの削除

Cisco DCNM Web UI から画像をリポジトリから削除するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [画像管理（Image Management）] > [画像のアップロード（Image Upload）]** を選択します。

のスマート画像管理（Smart Image Management）] ウィンドウが表示されます。

ステップ 2 リストから既存の画像を選択し、**[画像の削除（Delete Image）]** アイコンをクリックします。

確認ウィンドウが表示されます。

ステップ 3 [はい（Yes）] をクリックして、イメージを削除します。

[インストールとアップグレード（Install & Upgrade）]

[インストールおよびアップグレード（Install & Upgrade）] メニューには、次のサブメニューが含まれています。

アップグレード履歴

この機能により、In-Service Software Upgrade（ISSU）を使用して Cisco Nexus プラットフォーム スイッチをアップグレードできます。このアップグレード手順は、デバイス構成に基づいて、中断を伴う場合もあれば、中断しない場合もあります。アップグレードに必要なキックスタート、システム、または NX-OS イメージ SSIデバイス上のイメージ リポジトリまたはファイル システムから選択できます。リポジトリからイメージを選択するには、**[コントロール] > [イメージ管理] > [イメージ アップロード]** タブから同じイメージをアップロードする必要があります。

次の表では、**[制御] > [イメージ管理] > [アップグレード履歴]** 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
タスク ID（Task Id）	タスクのシリアル番号を指定します。最新のタスクが上部に表示されます。 **Note** ネイティブ HA でフェールオーバーがトリガーされると、タスク ID シーケンス番号が 32 ずつ増加します。
タスクタイプ	タスクのタイプを指定します。 • 互換性 • アップグレード
[オーナー（Owner）]	Role-Based Authentication Control（RBAC）に基づいて、このタスクを開始した所有者を指定します。

フィールド	説明
デバイス	このタスク用に選択されたすべてのデバイスを表示します。
[ジョブ ステータス（Job Status）]	ジョブのステータスを指定します。 • 計画済み • In Progress（進行中） • Completed（完了） • 例外ありで完了 **Note** ジョブが 1 つまたは複数のデバイスで失敗した場合、ステータスフィールドには失敗を示す COMPLETED WITH EXCEPTION が表示されます。
作成時刻	タスクが作成された時間を指定します。
スケジュール	タスクの実行を指定する時刻を指定します。タスクを後で実行するようにスケジュールすることもできます。
完了時刻	タスクが完了した時間を指定します。
備考	タスクの実行中に所有者が追加したコメントを表示します。

Note Cisco DCNM の新規インストール後、このページにはエントリがありません。

次を実行します。

表示

Cisco DCNM Web UI からイメージ アップグレード履歴を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [画像管理（Image Management）] > [インストールおよびアップグレード（Install & Upgrade）] > [アップグレード履歴（Upgrade History）]**を選択し、タスク 識別子 チェックボックスを選択します。

一度に 1 つのタスクのみを選択します。

ステップ 2 [表示（View）] をクリックします。

[インストール タスクの詳細（Installation Task Details）] ウィンドウが表示されます。

ステップ 3 [設定（Settings）] をクリックします。**[列（Columns）]** メニューを展開し、表示する詳細を選択します。

このウィンドウには次の情報が表示されます。

- キックスタートとシステム イメージのローケーション
- 互換性チェック ステータス
- インストールステータス
- プレ ISSU レポート ステータスとポスト ISSU レポート ステータス
- 説明
- レポートサマリー
- バージョン チェック結果
- ログ

列は、表示することを選択したタスクに応じて変わります。EPLD タスクのスイッチ名、IP アドレス、プラットフォームの詳細、イメージ名、およびインストール ステータスを表示できます。レポート ステータスには、レポートの概要も含まれます。 レポートの概要には、ISSU 前の詳細レポートと ISSU 後のレポートへのハイパーリンクが含まれています。これらのハイパーリンクをクリックすると、レポートを表示するための新しいタブまたはウィンドウに移動します。レポート サマリーには、レポート テンプレートで定義したコマンドも含まれます。

ステップ 4 デバイスを選択します。

タスクの詳細ステータスが表示されます。完了したタスクについては、デバイスからの応答が表示されます。

アップグレード タスクが進行中の場合は、インストール プロセスのライブ ログが表示されます。

Note
- このウィンドウが表示されている場合、このテーブルは、進行中のジョブについて 30 秒ごとに自動更新されます。
- アップグレードされた EPLD 情報が表示されるまでに時間がかかります。スイッチが到達可能になるまで、5 分ごとにスイッチから DCNM に更新をフェッチするジョブがスケジュールされています。

削除

Cisco DCNM Web UI からタスクを削除するために、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [画像管理（Image Management）] > [インストールおよびアップグレード（Install & Upgrade）] > [アップグレード履歴（Upgrade History）]**を選択し、**[タスク 識別子（Task ID）]** チェックボックスを選択します。

ステップ 2 [削除（Delete）] をクリックします。

ステップ 3 **[OK]** をクリックして、ジョブの削除を確認します。

新規インストール

Cisco DCNM に ISSU および EPLD イメージをインストールできます。

新しい *ISSU* インストール

Cisco DCNM から検出されたデバイスをアップグレードするには、次の手順を実行します。

Before you begin

ISSU 前および ISSU 後のレポートが必要な場合は、**[テンプレート ライブラリ]** ウィンドウにレポート テンプレートを追加します。ISSU 前後の処理の詳細については、DCNM にパッケージ化されているデフォルトのアップグレード テンプレートを参照してください。デフォルトのアップグレード テンプレートは **issu_vpc_check** です。

Procedure

ステップ 1 **[制御（Control）]> [イメージ管理（Image Management）]> [インストールおよびアップグレード（Install & Upgrade）] > [アップグレード履歴（Upgrade History）]**を選択します。

ステップ 2 **[新しいインストール（New Installation）] > [ISSU]** を選択して、デバイス上のキックスタートおよびシステム イメージをインストールまたはアップグレードします。

デフォルトの VDC を持つデバイスが **[スイッチの選択（Select Switches）]** ウィンドウに表示されます。

Note フリーズモードまたはモニタリング モードのファブリックの一部であるスイッチは、ここにリストされていません。**[デバイス範囲（Device Scope）]** ドロップダウン メニューから、フリーズ モードまたはモニタ モードでファブリックを選択する場合、エラー メッセージが表示されます。

ステップ 3 スイッチ名の左側にあるチェック ボックスをオンにします。

複数のスイッチを選択して。

ステップ 4 [次へ（Next）] をクリックします。

[ISSU 前後のレポート（Pre-Post ISSU Reports）] ウィンドウが表示されます。

Note プレポストISSU レポートは、SANおよびメディア コントローラのインストールではサポートされていません。

ステップ 5 (Optional) **[ISSU 前後のレポートのスキップ（Skip Pre-Post ISSU Reports）]** チェックボックスをオンにして、スイッチの ISSU 前後のレポートをスキップし、ステップ *8* に進みます。

デフォルトでは、このチェックボックスはオフになっています。

ステップ 6 **[レポート テンプレートの選択]** ドロップダウン リストからレポート テンプレートを選択します。

[制御（Control）] > [テンプレート ライブラリ（Template Library）] ウィンドウにリストされている **UPGRADE** サブタイプを持つ **REPORT** テンプレート タイプのテンプレートのみが、**[レポート テンプレートの選択（Select Report Template）]** ドロップダウン リストに表示されます。

ステップ 7 ステップ *6* で選択したテンプレートに基づいて、**[全般]** タブの必須フィールドに入力します。

ステップ 8 [次へ（Next）] をクリックします。

[ソフトウェア イメージの指定（Specify Software Images）] ウィンドウが表示されます。このタブには、前の画面で選択したスイッチが表示されます。アップグレードするイメージも選択できます。

- **[自動ファイル選択]** チェック ボックスを使用すると、イメージ バージョン、およびアップグレードされたイメージを選択したデバイスに適用できるパスを指定できます。
- **[ファイル サーバーの選択]**を無効にし、デフォルトのサーバーが使用されます。
- **[イメージ バージョン]** フィールドで、**[イメージのアップロード]** ウィンドウに表示されるイメージのバージョンを指定します。
- **[パス]** フィールドは無効になり、デフォルトのイメージ パスが使用されます。

ステップ 9 **[キックスタート イメージ]** 列で **[イメージを選択]** をクリックします。

[ソフトウェア イメージ ブラウザ（Software Image Browser）] ダイアログボックスが表示されます。

Note
- Cisco Nexus 9000 シリーズ スイッチでは、Cisco NX-OS オペレーティング システムをロードするためにシステム イメージのみが必要です。したがって、これらのデバイスのキックスタート イメージを選択するオプションは無効になっています。
- **[ソフトウェア イメージ ブラウザ]** ダイアログ ボックスの表示に問題がある場合は、ブラウザのフォント サイズを小さくして再試行してください。

ステップ 10 **[システム イメージ]** 列で **[イメージの選択]** をクリックします。

[ソフトウェア イメージ ブラウザ（Software Image Browser）] ダイアログボックスが表示されます。

ステップ 11 **[ソフトウェア イメージ ブラウザ（Software Image Browser）]** ダイアログボックスで、**[ファイル サーバー（File Server）]** または **[スイッチ ファイル システム（Switch File System）]** からイメージを選択できます。

ファイル サーバーを選択した場合：

a) **[ファイル サーバーの選択]** リストから、イメージが保存されている Default_SCP_Repository のファイル サーバーを選択します。

b) **[画像の選択]** リストから、適切な画像を選択します。同じプラットフォームの他のすべての選択したデバイスに同じイメージを使用するには、チェック ボックスをオンにします。

例：プラットフォーム タイプ N9K-C93180YC-EX および N9K-C93108TC-EX の場合、ロジックはプラットフォーム（N9K）とサブプラットフォームの 3 つの文字（C93）に一致します。すべてのプラットフォーム スイッチで同じロジックが使用されます。

Note **ファイル サーバー**を選択すると、BIN 拡張子を持つファイルのみが一覧表示されます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバーを再起動します。デフォルトでは **true** に設定されています。

Note **[イメージのアップロード（Image Upload）]** ウィンドウに存在するイメージファイルのみが選択できます。他のパスにあるイメージは選択できません。

c) [VRF の選択（**Select Vrf**）] ドロップダウン リストから VRF を選択します。

Note このフィールドは、Cisco MDS スイッチには表示されません。

この VRF は、他の選択されたデバイスに対してデフォルトで選択されています。デフォルト値は **[management]** です。

d) [OK] をクリックします。

このイメージは、同じプラットフォーム タイプの他のすべての選択されたデバイスに対して選択されます。

[ファイル システムの切り替え] を選択した場合：

a) **[イメージの選択（Select Image）]** リストから、デバイスのフラッシュ メモリにある適切なイメージを選択します。

Note **スイッチ ファイル システム（Switch File System）]** を選択すると、BIN 拡張子を持つファイルのみが一覧表示されます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバーを再起動します。デフォルトでは **true** に設定されています。

b) **[OK]** をクリックしキックスタート イメージを選択するか、**[キャンセル（Cancel）]** をクリックして **[ソフトウェア イメージの指定（Specify Software Images）]** ダイアログ ボックスに戻ります。

ステップ 12 **[Vrf]** 列では、仮想ルーティングおよびフォワーディング（VRF）の名前を示します。

ステップ 13 **[使用可能なスペース（Available Space）]**列で、スイッチの**プライマリ スーパーバイザ**モジュールと**セカンダリ スーパーバイザ** モジュールに使用可能なスペースを指定します。

[使用可能なスペース] 列には、スイッチで使用可能なメモリが MB で表示されます (1 MB 未満の場合は、KB として表示およびマークされます。

ブートフラッシュ ブラウザでは、スイッチ ブートフラッシュにあるすべてのファイルとディレクトリのファイル名、サイズ、最新の変更日を表示します。ファイルを削除するには、ファイルを選択して **[削除]** をクリックし、スイッチの空き容量を増やします。

ステップ 14 **[選択されたファイルのサイズ]**列には、サーバーから選択されたイメージのサイズが表示されます。

選択したイメージの合計サイズがスイッチの使用可能なスペースより大きい場合、ファイルサイズは赤でマークされます。スイッチにイメージをコピーしてインストールするためのスペースを増やすことをお勧めします。

ステップ 15 スイッチをドラッグ アンド ドロップして、アップグレード タスク シーケンスを並べ替えます。

ステップ 16 (Optional) デバイス上の Cisco NX-OS ソフトウェア バージョンと、選択したアップグレードされたイメージとの互換性をチェックする場合は、**[バージョンの互換性をスキップ（Skip Version Compatibility）]** チェックボックスをオフにします。

ステップ 17 すべてのラインカードを同時にアップグレードするには、**[パラレル ライン カードのアップグレードの選択（Select Parallel Line Card upgrade）]** を選択します。

パラレル ライン カードのアップグレードは、Cisco MDS デバイスには適用されません。

ステップ 18 **[アップグレード オプション]** 列の **[オプション]** をクリックして、アップグレードのタイプを選択します。

[アップグレードオプション] ウィンドウに2つのアップグレードオプションが表示されます。**アップグレード オプション 1** のドロップダウン リストには、次のオプションがあります。

- **中断**
- **Bios force**
- **無停止を許可**
- **無停止を強制**

中断は、Cisco Nexus 9000 シリーズ スイッチのデフォルト値です。アップグレード オプションは、他のスイッチには**適用されません**。

[アップグレード オプション1] の下で **[無停止を許可（Allow Non Disruptive）]** を選択し、スイッチが無停止アップグレードをサポートしていない場合、中断アップグレードが実行されます。

アップグレード オプション 1 で **[無停止を強制（Force non-disruptive）]** を選択すると、互換性チェックが無停止アップグレードに必須であるため、**[バージョン互換性の確認（Skip Version Compatibility）]** チェック ボックスがオフになります。選択したスイッチが無停止アップグ

レードをサポートしていない場合、スイッチの選択を確認するよう求める警告メッセージが表示されます。スイッチを選択または削除するには、チェックボックスを使用します。

[アップグレード オプション 2] のドロップダウン リストには、**[アップグレード オプション 1]** で **[無停止を許可]** または **[無停止を強制]** を選択すると、次のオプションがあります。

- **北米**
- **バイオスフォース**

アップグレード オプション 1 で **Disruptive** または **Bios-force** を選択すると、**アップグレード オプション 2** では **アップグレード オプション 2** は無効になります。

選択したすべてのデバイスに選択したオプションを使用するには、**[他のすべての選択したデバイスにこのオプションを使用する]** チェック ボックスをオンにして、**[OK]** をクリックします。

Note
- アップグレード オプションは、Cisco Nexus 3000 シリーズおよび 9000 シリーズ スイッチにのみ適用されます。
- アップグレードに **[無停止を許可]** オプションを選択しても、無停止アップグレードが保証されるわけではありません。互換性チェックを実行して、デバイスが無停止アップグレードをサポートしていることを確認します。

ステップ 19 [次へ（Next）] をクリックします。

[バージョンの互換性をスキップ] を選択しなかった場合、Cisco DCNM は互換性チェックを実行します。

チェックが完了するまで待つか、**[後でインストールを終了]** をクリックするかを選択できます。

インストール ウィザードが閉じられ、互換性タスクが **[制御] > [イメージ管理] > [インストールとアップグレード] > [アップグレード履歴タスク]** で作成されます。

イメージの互換性のチェックにかかる時間は、構成とデバイスの負荷によって異なります。

互換性検証 ステータス列には、検証のステータスが表示されます。

[バージョン互換性をスキップ（Skip Version Compatibility）] を選択してバージョン互換性チェックをスキップすると、Cisco DCNM はデバイスの名前だけを表示します。**[現在のアクション]** 列には **[完了]** と表示され、**互換性検証]** 列には **[スキップされました]** と表示されます。

ISSU 前レポート ステータス（Pre-ISSU Report Status）] 列は、ISSU 前レポートが生成されたかどうかを示します。**[互換性ステータス]** 列で、互換性ログとレポートの概要を表示できます。レポート サマリーのハイパーリンクをクリックして、ISSU 前チェックの詳細レポートを表示します。

Note インターネットの帯域幅によっては、ステータスが Web UI に反映されるまでに時間がかかる場合があります。

スイッチの選択を確認し、それに応じてアップグレードするスイッチをオンまたはオフにすることができます。

ステップ 20 **[後でインストールを終了]** をクリックして、後でアップグレードを実行します。

ステップ 21 [次へ（Next）] をクリックします。

ステップ 22 デバイスのアップグレード前に実行構成をスタートアップ構成に保存するには、このチェックボックスをオンにします。

ステップ 23 アップグレードプロセスは、すぐに実行するか、後で実行するようにスケジュールできます。

a. デバイスを今すぐアップグレードするには、**[今すぐ展開（Deploy Now）]** を選択します。

b. **[展開時間の選択（Choose time to Deploy）]** を選択し、後でアップグレードを実行するための時刻を MMM/DD/YYYY HH:MM:SS 形式で指定します。

時刻はサーバーに相対的です。選択した展開時刻が過去の場合、ジョブはすぐに実行されます。

ステップ 24 アップグレード対象として選択したデバイスとラインカードに基づいて、実行モードを選択できます。

a. **[順次]** を選択して、選択した順序でデバイスをアップグレードします。

Note デバイスをメンテナンス モードにすると、このオプションは無効になります。

b. **[同時]** を選択して、すべてのデバイスを同時にアップグレードします。

ステップ 25 **[終了（Finish）]** をクリックし、アップグレード プロセスを開始します。

インストール ウィザードが閉じ、**[制御] > [イメージ管理] > [インストールとアップグレード] > [アップグレード履歴]** ページにアップグレードするタスクが作成されます。

What to do next

スイッチで ISSU を完了したら、スイッチが再起動し、SNMP エージェントが安定するまで 20 分間待機します。DCNM は、Cisco DCNM Web UI にスイッチの新しいバージョンを表示するために、投票サイクルを検出します。

EPLD インストール

Cisco DCNM は、Cisco Nexus 9000 シリーズ スイッチでの 2 種類の EPLD 画像のインストールまたはアップグレードをサポートしています。

- EPLD 画像からすべてのモジュールをアップグレードします。
- EPLD 画像から特定のモジュールのみをアップグレードします。

リポジトリから画像を選択するには、**[制御（Control）] > [画像管理（Image Management）] > [画像のアップロード（Image Upload）]** からアップロードします。

Cisco DCNM で EPLD 画像をインストールまたはアップグレードするには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [画像管理（Image Management）] > [インストールとアップグレード（Install & Upgrade）] > [アップグレード履歴（Upgrade History）]** を選択します。

ステップ 2 **[新規インストール（New Installation）] > [EPLD]** を選択します。

[スイッチの選択（Select Switches）] ウィンドウに Cisco Nexus 9000 シリーズ スイッチが表示されます。

（注） フリーズモードまたは監視モードのファブリックの一部であるスイッチは、ここにリストされていません。**[デバイス範囲（Device Scope）]** ドロップダウン メニューから、フリーズモードまたはモニタ モードでファブリックを選択する場合、エラー メッセージが表示されます。

ステップ 3 スイッチ名の左側にあるチェックボックスをチェックします。

複数のデバイスを選択できます。

ステップ 4 [次へ（Next）] をクリックします。

[EPLD 画像の指定（Specify EPLD Images）] ウィンドウが表示されます。このタブには、前の画面で選択したスイッチが表示され、アップグレードする EPLD 画像を選択できます。

ステップ 5 **[EPLD 画像（Select Image）]** 列で **[画像の選択（EPLD image）]** をクリックします。

[EPLD 画像ブラウザ（EPLD Image Browser）] ダイアログ ボックスが表示されます。

ステップ 6 ファイル サーバまたはスイッチ ファイル システムから EPLD 画像 ファイルを選択します。

[ファイル サーバ（File Server）] を選択した場合：

a) **[画像の選択（Select Image）]** リストから適切な画像を選択します。

（注）
- **[ファイル サーバ（File Server）]** を選択すると、IMG 拡張子を持つファイルのみがリストされます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバーを再起動します。デフォルトでは **true** に設定されています。
- **[イメージのアップロード（Image Upload）]** ウィンドウに存在するイメージ ファイルのみが選択できます。他のパスにある画像は選択できません。

b) **[OK]** をクリックして EPLD 画像を選択するか、**[キャンセル（Cancel）]** をクリックして、**[ソフトウェア画像の指定（Specify Software Images）]** ウィンドウに戻ります。

[ファイル システムの切り替え] を選択した場合：

a) **[イメージの選択（Select Image）]** リストから、デバイスのフラッシュ メモリにある適切なイメージを選択します。

（注） **[ファイル システムの切り替え（Switch File System）]** を選択すると、IMG 拡張子を持つファイルのみが一覧表示されます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバーを再起動します。デフォルトでは **true** に設定されています。

b) **[OK]** をクリックし EPLD 画像を選択するか、**[キャンセル（Cancel）]** をクリックして **[ソフトウェア画像の指定（Specify Software Images）]** ダイアログ ボックスに戻ります。

ステップ 7 [VRF の選択（Select Vrf）] ドロップダウン リストから VRF を選択します。

有効な値は、管理、デフォルト、およびキープアライブです。

ステップ 8 （任意） 選択した他のすべてのデバイスに VRF を使用するには、**[その他すべての選択されたデバイスにこの VRF を使用する（Use this Vrf for other all selected devices）]** チェックボックスをオンにします。

ステップ 9 （任意） 選択した他のすべてのデバイスにこの画像を使用するには、**[同じプラットフォーム タイプのその他すべての選択されたデバイスにこの画像を使用するUse this image for other all selected devices of same platform type]** チェックボックスをオンにします。

ステップ 10 **[Vrf]** 列では、仮想ルーティングおよびフォワーディング（VRF）の名前を示します。

ステップ 11 **[使用可能なスペース（Available Space）]** 列で、スイッチの**プライマリ スーパーバイザ** モジュールと**セカンダリ スーパーバイザ** モジュールに使用可能なスペースを指定します。

[使用可能なスペース（Available Space）] 列には、スイッチで使用可能なメモリが MB 単位で表示されます（1 MB 未満の場合は、KB として表示およびマークされます）。

ブートフラッシュ ブラウザでは、スイッチ ブートフラッシュにあるすべてのファイルとディレクトリのファイル名、サイズ、最新の変更日を表示します。ファイルを削除するには、ファイルを選択して **[削除]** をクリックし、スイッチの空き容量を増やします。

ステップ 12 選択した画像の合計サイズが、**[選択されたファイルのサイズ（Selected Files Size）]** 列のスイッチで使用可能なスペースより大きいかどうかを確認します。

[選択されたファイルのサイズ（Selected Files Size）] 列には、サーバから選択した画像のサイズが表示されます。

選択したイメージの合計サイズがスイッチの使用可能なスペースより大きい場合、ファイル サイズは赤でマークされます。スイッチにイメージをコピーしてインストールするためのスペースを増やすことをお勧めします。

（注） 返されるはずのバージョンが返されない場合、EPLDのアップグレードは失敗します。

ステップ 13 スイッチをドラッグアンドドロップして、アップグレード タスクの順序を並び替えます。

ステップ 14 **[モジュール オプション（Module Options）]** 列のハイパーリンクをクリックして、対応するスイッチのモジュールを選択して EPLD モジュールをアップグレードします。

[モジュール オプション（Module Options）] ダイアログ ボックスが表示されます。デフォルト値は **[すべて（All）]** で、選択したスイッチのすべての EPLD モジュールをインストールまたはアップグレードします。

ステップ 15 モジュールを選択します。

ステップ 16 [OK] をクリックします。

ステップ 17 **[FPGA リージョン（FPGA Region）]** 列の下のハイパーリンクをクリックして、FPGA リージョンを選択します。

有効なオプションは、**[プライマリ（Primary）]** および **[ゴールデン（Golden）]** です。

ゴールデン アップグレードを選択した場合は、BIOS が更新され、すべての前提条件が満たされていることを確認してください。詳細については、「*Cisco Nexus 9000* シリーズ *FPGA/EPLD* アップグレード リリース ノート」を参照してください。

ステップ 18 **[終了（Finish）]** をクリックし、アップグレード プロセスを開始します。

インストール ウィザードが閉じ、アップグレードするタスクが **[制御（Control）] > [画像管理（Image Management）] > [インストールおよびアップグレード（Install & Upgrade）] > [アップグレード履歴（Upgrade History）]** ウィンドウで作成されます。EPLD アップグレード タスクは、タスク タイプによって識別できます。

次のタスク

スイッチのアップグレードが完了したら、スイッチが再起動し、SNMP エージェントが安定するまで 20 分間待機します。Cisco DCNM は、Cisco DCNM Web UI の **[スイッチ レベル履歴（Switch Level History）]** ウィンドウにスイッチの新しいバージョンを表示するために、ポーリング サイクルを検出します。

[イベント（Events）] ウィンドウで EPLD ゴールデン アップグレード通知を表示できます。Cisco DCNM Web UI のホームページから、**[モニタ（Monitor）] > [スイッチ（Switch）] > [イベント（Events）]** を選択します。

インストールの終了

[互換性チェック（Compatibility Check）] ページで完了したタスクのインストールを完了することを選択できます。次のタスクを実行して、デバイスのアップグレードプロセスを完了します。

Procedure

ステップ 1 **[制御（Control）] > [イメージ管理（Image Management）] > [インストールとアップグレード（Install & Upgrade）] > [アップグレード履歴（Upgrade History）]** を選択し、互換性チェックが完了したタスクを選択します。

一度に 1 つのタスクのみを選択します。

ステップ 2 **[インストールの終了（Finish Installation）]** をクリックします。

[ソフトウェア インストール ウィザード（Software Installation Wizard）] が表示されます。

ステップ 3 スイッチの選択を確認し、それに応じてアップグレードするスイッチをオンまたはオフにすることができます。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 デバイスのアップグレード前に実行構成をスタートアップ構成に保存するには、このチェックボックスをオンにします。

ステップ 6 チェックボックスをオンにして、アップグレードの前にデバイスをメンテナンス モードにします。このオプションは、メンテナンス モードをサポートするデバイスに対してのみ有効です。

ステップ 7 アップグレードプロセスは、すぐに実行するか、後で実行するようにスケジュールできます。

a. デバイスを今すぐアップグレードするには、**[今すぐ展開（Deploy Now）]** を選択します。

b. **[展開時間の選択（Choose time to Deploy）]** を選択し、後でアップグレードを実行するための時刻を MM/DD/YYYY HH:MM:SS 形式で指定します。

ステップ 8 アップグレード対象として選択したデバイスとライン カードに基づいて、実行モードを選択できます。

a. **[順次（Sequential）]** を選択して、選択された順序でデバイスをアップグレードします。

Note デバイスをメンテナンス モードにすると、このオプションは無効になります。

b. **[同時（Concurrent）]** を選択して、すべてのデバイスを同時にアップグレードします。

ステップ 9 **[終了（Finish）]** をクリックして、アップグレード プロセスを完了します。

スイッチ レベルの履歴

アップグレードプロセスの履歴をスイッチ レベルで表示できます。スイッチの現在のバージョンとその他の詳細を表示できます。

次の表では、**[制御（Control）] > [画像管理（Image Management）] > [インストールとアップグレード（Install & Upgrade）] > [スイッチ レベル履歴（Switch Level History）]** 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
スイッチ名	スイッチの名前を指定します
IP アドレス	スイッチの IP アドレスを指定します
プラットフォーム	Cisco Nexus スイッチ プラットフォームを指定します

フィールド	説明
現在のバージョン	スイッチ ソフトウェアの現在のバージョンを指定します。

スイッチ名の横にあるラジオボタンをクリックしてスイッチを選択し、そのアップグレード履歴を表示します。**[表示（View）]** をクリックして、選択したスイッチのアップグレード タスク履歴を表示します。

次の表では、**[制御（Control）] > [画像管理（Image Management）] > [インストールとアップグレード（Install & Upgrade）] > [スイッチ レベル履歴（Switch Level History）] > [デバイス アップグレード タスクの表示（View Device Upgrade Tasks）]** 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
オーナー（Owner）	アップグレードを開始した所有者を指定します。
[ジョブ ステータス（Job Status）]	ジョブのステータスを指定します。 • 計画済み • In Progress（進行中） • Completed（完了）
キックスタート画像	スイッチのアップグレードに使用するキックスタート イメージを指定します。
システムのイメージ（System Image）	スイッチのアップグレードに使用するシステム画像を指定します。
完了時刻	アップグレードが正常に完了した日時を指定します。
ステータスの説明	ジョブのインストールログ情報を指定します。

パッケージ

画像管理は、必要なパッケージとパッチのインストールまたはアンインストールにも役立ちます。スイッチにインストールされているすべての RPM パッケージと SMU パッチが **[パッケージ [SMU/RPM]（Package [SMU/RPM]）]** ウィンドウに表示されます。パッケージまたはパッチに対して次のアクションを実行できるようになりました。

- インストール
- アンインストール
- 有効化

• 非アクティブ化

この操作を実行するには、管理者権限が必要です。次のテーブルは、**[制御（Control）] > [画像管理（Image Management）] > [パッケージ [SMU/RPM]（Package [SMU/RPM]）] > [インストール履歴（Installation History）]**に現れるフィールドを説明します。

フィールド	説明
Switch Name	ファイルがインストールされているスイッチの名前を指定します。
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。
IP Address	デバイスの IP アドレスを指定します。
リリース	スイッチのリリース OS バージョンを指定します。
Name	ファイルの名前を指定します。
バージョン	ファイルのバージョンを指定します。
[タイプ（Type）]	ファイルが基本パッケージ、非基本パッケージ、またはパッチのいずれであるかを指定します。
ステータス	パッケージまたはパッチがアクティブ化されているかどうかを指定します。有効な値は**[アクティブ（active）]**と**[非アクティブ（inactive）]**です。

[パッケージ（Package）] ウィンドウで次のタスクを実行することができます。

パッケージおよびパッチのインストール

Cisco DCNM Web UI からパッケージまたはパッチをインストールするには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [画像管理（Image Management）] > [パッケージ [SMU/RPM]（Package [SMU/RPM]）]** を選択し、**[インストール]** アイコンをクリックします。

[デバイスの選択（Select Devices）] ウィンドウが表示されます。

Note フリーズモードまたは監視モードのファブリックの一部であるスイッチは、ここにリストされていません。**[デバイス範囲（Device Scope）]** ドロップダウンメニューから、フリーズモードまたはモニタモードでファブリックを選択する場合、エラーメッセージが表示されます。

スイッチが移行モードの場合、チェック ボックスは無効になります。

ステップ 2 スイッチ名の左側にあるチェックボックスを選択します。

複数のスイッチを選択できます。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 **[パッケージ / パッチ（Packages/Patches）]** 列の **[パッケージの選択（Select Packages）]**

[パッケージ/パッチ ブラウザ（Packages/Patches Browser）] ダイアログ ボックスが表示されます。

ステップ 5 **[ファイル サーバ（File Server）]** または **[スイッチ ファイル システム（Switch File System）]** からファイルを選択します。

ファイル サーバを選択した場合:

a) **[画像の選択（Select Image）]** リストから、デバイスにインストールする必要がある適切なパッケージまたはパッチを選択します。

特定のプラットフォーム用にアップロードされたパッケージまたはパッチは、このファイルセレクターにリストされます。インストールするファイルを複数選択できますが、インストールでスイッチのリロードが必要な場合は、パッチまたはパッケージを 1 つだけ選択してください。

同じプラットフォームの他のすべての選択されたデバイスに同じパッケージを使用するには、チェックボックスをオンにします。

このパッケージまたはパッチ画像は、他の選択されたデバイスに対してデフォルトで選択されています。

b) **[OK]** をクリックしてパッチ画像を選択します。

c) ドロップダウン リストから VRF を選択します。

この VRF は、選択した他のすべてのデバイスに使用できます。

この VRF は、他の選択されたデバイスに対してデフォルトで選択されています。

[ファイル システムの切り替え（Switch File System）] を選択した場合：

a) **[画像の選択（Select Image）]** リストから、デバイスのフラッシュ メモリにある適切なファイル画像を選択します。

デバイスにインストールするファイルを複数選択できますが、インストールでデバイスのリロードが必要な場合は、パッチまたはパッケージを 1 つだけ選択してください。**[ファイル システムの切り替え（Switch File System）]** を選択すると、RPM または SMU 拡張子を持つファイルのみがリストされます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバーを再起動します。デフォルトでは **true** に設定されています。

b) [**OK**] をクリックします。

ステップ 6 [Finish] をクリックします。

[パッケージ（Packages）] ウィンドウで、スイッチにインストールされているパッケージのリストを表示できます。

Note パッケージをインストールすると、それもアクティブ化されます。

パッケージおよびパッチのアンインストール

アンインストールプロセスでは、選択したパッケージまたはパッチが非アクティブ化され、その後削除されます。非ベースRPMパッケージとSMUパッチのみを削除できます。ベースRPMパッケージをアンインストールすると、非アクティブ化されるだけです。ベースRPMパッケージは削除できません。アンインストールでデバイスの再ロードが必要な場合は、パッチまたはパッケージを 1 つだけ選択します。

Cisco DCNM Web UIからデバイスのパッケージまたはパッチをアンインストールするには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control ）] > [画像管理（Image Management）] > [パッケージ [SMU/RPM]（Package [SMU/RPM]）]** を選択します。

ステップ 2 パッケージまたはパッチを選択し、**[アンインストール（Uninstall）** アイコンをクリックします。

確認ウィンドウが表示されます。

ステップ 3 [OK] をクリックします。

一度に複数のパッケージまたはパッチをアンインストールできますが、選択したすべてのパッケージまたはパッチのステータスは同じである必要があります。

パッケージおよびパッチのアクティブ化

非アクティブなパッケージまたはパッチをアクティブ化できます。Cisco DCNM Web UI からパッケージまたはパッチをアクティブ化にするには、次の手順を実行します。

Procedure

ステップ 1 **[[制御（Control ）] > [画像管理（Image Management）] > [パッケージ [SMU/RPM]（Package [SMU/RPM]）]** を選択します。

ステップ 2 非アクティブなパッケージまたはパッチを選択し、**[アクティブ化（Activate）]** アイコンをクリックします。

確認用のダイアログボックスが表示されます。

ステップ 3 [OK] をクリックします。

[インストール タスクの詳細（Installation Task Details）] ダイアログ ボックスが表示されます。**[ステータス（Status）]** 列の下のハイパーリンクをクリックして、インストール ステータスの詳細を表示できます。

非アクティブ化

アクティブなパッケージまたはパッチを非アクティブ化できます。Cisco DCNM Web UI からパッケージまたはパッチを非アクティブ化にするには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control ）] > [画像管理（Image Management）] > [パッケージ [SMU/RPM]（Package [SMU/RPM]）]** を選択します。

ステップ 2 1 つ以上のアクティブなパッケージまたはパッチを選択し、**[非アクティブ化（Deactivate）]** アイコンをクリックします。

確認用のダイアログボックスが表示されます。

ステップ 3 **[OK]**をクリックします。

画像管理ポリシー

イメージ管理ポリシーには、RPM または SMU とともに NX-OS イメージの目的の情報が含まれます。ポリシーは、特定のプラットフォームに属することも、さまざまなタイプのプラットフォームに対して包括的に属することもあります。包括タイプのポリシーには、1 つ以上のプラットフォームのポリシーを含めることができます。スイッチのプラットフォームに関係なく、包括的なイメージ管理ポリシーをスイッチのグループに関連付けることができます。包括タイプのポリシーでは、プラットフォームごとに1つのプラットフォーム ポリシーのみを選択できます。スイッチに適用されたポリシーに基づいて、Cisco DCNM では必要な NXOS と RPM または SMU がスイッチに存在するかどうかが確認されます。スイッチ上のポリシーとイメージの間に不一致があると、ファブリック警告が生成されます。

次のテーブルに **[ポリシー（Policies）]** ウィンドウのフィールドと詳細があります。

フィールド	説明
ポリシー名（Policy Name）	ポリシー名を指定します。
ポリシータイプ	ポリシー タイプが **[プラットフォーム（PLATFORM）]** か **[Cisco Umbrella（UMBRELLA）]** かを指定します。
リリース	プラットフォーム ポリシーのプラットフォーム リリースを指定します。包括的なポリシーの場合、フィールドは空です。

フィールド	説明
[ポリシー/パッケージ名（Policy / Package Name）]	パッチまたは、パッケージ名を指定します。プラットフォーム ポリシーにはパッケージ名が表示され、Cisco 包括ポリシーには関連するプラットフォーム ポリシーが表示されます。
プラットフォーム	プラットフォーム ポリシーのプラットフォームを指定します。
[ポリシーの説明（Policy Description）]	ユーザー定義のポリシーの説明を指定します。

[ポリシー（Policies）] ウィンドウで次のタスクを実行することができます。

画像管理ポリシーの追加

Cisco DCNM Web UI から画像管理ポリシーを追加するには、次の手順を実行します。

Before you begin

画像ポリシーを作成する前に、**[画像のアップロード（Images Upload）]** タブで画像をアップロードします。画像のアップロードに関しては、「イメージのアップロード, on page 436」セクションを参照してください。

Procedure

ステップ 1 **[制御（Control）]** > **[画像管理（Image Management）]** > **[画像管理ポリシー（Image Management Policies）]** の順に選択します。

[ポリシー（Policies）] ウィンドウが表示されます。

ステップ 2 [追加（Add）] アイコンをクリックします。

[イメージ管理ポリシーの作成（Create Image Management Policy）] ダイアログボックスが表示されます。

ステップ 3 ポリシー タイプの選択

有効な値は**プラットフォーム**と**包括的** です。

ステップ 4 a) **プラットフォーム** ポリシータイプを選択すると、**[画像管理ポリシーの作成（Create Image Management Policy）]** ダイアログ ボックスに次のフィールドが表示されます。

フィールド	アクション
ポリシー名（Policy Name）	ポリシー名を入力します。

フィールド	アクション
プラットフォーム	プラットフォーム ドロップダウンリストからプラットフォームを選択します。オプションは、**[画像のアップロード（Image Upload）]** ウィンドウでアップロードした画像に基づいて入力されます。[リリース（Release）] ドロップダウンリストのオプションは、選択したプラットフォームに基づいて自動的に入力されます。
リリース	[リリース（Release）] ドロップダウンリストから NX-OS バージョンを選択します。**[パッケージ名（Package Name）]** のオプションは、選択したリリースに基づいて自動的に入力されます。
パッケージ名	（オプション）パッケージを選択します。
[ポリシーの説明（Policy Description）]	（任意）ポリシーの説明を入力します。

b) **包括的な**ポリシー タイプを選択すると、**[画像管理ポリシーの作成（Create Image Management Policy）]** ダイアログ ボックスに次のフィールドが表示されます。

フィールド	アクション
ポリシー名	ポリシー名を入力します。
プラットフォーム ポリシー	この包括的なポリシーの下にあるプラットフォーム ポリシーを選択します。プラットフォームごとに 1 つのポリシーのみを選択します。
[ポリシーの説明（Policy Description）]	（任意）ポリシーの説明を入力します。

ステップ 5 [OK] をクリックします。

確認ウィンドウが表示されます。

What to do next

デバイスにポリシーをアタッチします。詳細については、デバイスへのイメージ管理ポリシーのアタッチ, on page 457セクションを参照してください。

デバイスへのイメージ管理ポリシーのアタッチ

Cisco DCNM Web UI から画像管理ポリシーをアタッチするには、次の手順を実行します。

Before you begin

[画像管理ポリシー（Image Management Policies）] ウィンドウで、ポリシーをアタッチするスイッチ プラットフォームの画像管理ポリシーを作成します。詳細については、画像管理ポリシーの追加, on page 456を参照してください。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 ファブリックを選択します。

ファブリック トポロジ ウィンドウが表示されます。

ステップ 3 **[アクション（Actions）]** ペインで **[表形式ビュー（Tabular view）]** をクリックします。

ステップ 4 **[スイッチ（Switches）]** タブで、画像管理ポリシーをアタッチするスイッチを選択します。

ステップ 5 **[画像管理ポリシー（Image Management Policies）]** アイコンをクリックします。

[ポリシーをデバイスにアタッチする（Attach Policy to Device）] ダイアログ ボックスが表示されます。このダイアログ ボックスには、選択したスイッチの IP アドレス、スイッチ名、シリアル番号、およびポリシー名が表示されます。

ステップ 6 イメージ管理ポリシーを適用するスイッチを選択します。

ステップ 7 [追加（Add）] アイコンをクリックします。

選択したプラットフォームに対してポリシーが作成されていない場合は、警告が表示されます。

ステップ 8 **[ポリシーの選択（Selec Policy）]** ドロップダウン リストからポリシーを選択します。

[画像管理ポリシー（Image Management Policies）] ウィンドウにリストされている、選択したスイッチと互換性のあるすべてのプラットフォーム ポリシーと包括的なポリシーが、ドロップダウン リストに表示されます。選択したポリシーに、選択したスイッチのプラットフォームに関連する情報が含まれていることを確認してください。デフォルト以外の VDC にはポリシーを適用しないでください。

ステップ 9 [OK] をクリックします。

[ポリシーをデバイスにアタッチする（Attach Policy to Device）] ダイアログ ボックスで、スイッチのポリシー名が更新されます。

ステップ 10 (Optional) ファブリック トポロジ ウィンドウに移動します。

ステップ 11 (Optional) **[アクション（Actions）]** ペインで **[ファブリックの再同期（Re-sync Fabric）]** をクリックします。

または、スケジュールされた CC チェックを待って、目的の NX-OS 画像、RPM、または SMU がスイッチにインストールされているかどうかを確認できます。

ステップ 12 (Optional) 保留中のエラーを確認し、**[解決（Resolve）]** をクリックして解決します。

スイッチからポリシーを削除するには、上記の手順に従って*[ステップ 6（Step 6）]* まで実行し、**[ステップ 7（Step 7）]** で *[*削除（*Delete*）*]* アイコンをクリックします。

画像管理ポリシーの削除

Cisco DCNM Web UI から画像管理ポリシーを削除するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [画像管理（Image Management）] > [画像管理ポリシー（Image Management Policies）]** の順に選択します。

[ポリシー（Policies）] ウィンドウが表示されます。

ステップ 2 **削除**アイコンをクリックします。

確認用のダイアログボックスが表示されます。

Note
- 包括的なポリシーで使用されているプラットフォーム ポリシーは削除できません。このようなプラットフォーム ポリシーを削除する前に、包括的なポリシーを削除してください。
- 使用中のポリシーは削除できません。削除する前にデバイスからポリシーを切断します。

ステップ 3 **[OK]**をクリックします。

エンドポイント ロケータ

エンドポイントロケータ（EPL）機能により、データセンター内のエンドポイントをリアルタイムで追跡できます。追跡には、エンドポイントのネットワーク ライフ履歴のトレースと、エンドポイントの追加、削除、移動などに関連する傾向へのインサイトの取得が含まれます。

エンドポイント ロケータに関する情報は、単一のランディング ページまたはダッシュボードに表示されます。ダッシュボードには、すべてのアクティブなエンドポイントに関するデータがほぼリアルタイムで（30秒ごとに更新されて）1つのペインに表示されます。このランディング ページに表示されるデータは、**[範囲（Scope）]** ドロップダウン リストで選択した範囲によって異なります。

- エンドポイント ロケータ
- エンドポイント ロケータの監視

ThousandEyes Enterprise Agent

ThousandEyes は Network Intelligence SaaS プラットフォームであり、これによりユーザはグローバルの監視ポイントを使用して、DNS 解決、ブラウザの応答特性、ネットワーク パスと接続の詳細なアスペクト、ネットワーク ルーティングのステータス、VoIP ストリーミング接続の品質を監視するための様々なテストを実行することができます。

モニタ対象のネットワーク内でユーザが特定のウェブサイトにアクセスするとき、ThousandEyes Enterprise Agent はネットワークとアプリケーション レイヤのパフォーマンス データを収集します。テストの実行、ネットワーク パスと接続の詳細なアスペクトのチェック、ネットワーク ルーティングのステータス チェック、インテント、実行構成などの変更のモニタを行うために、データは使用されます。

Cisco DCNM リリース 11.5(3) 以降、ThousandEyes Enterprise Agent は Cisco DCNM と統合されています。

Cisco DCNM **[Web UI]**> > **[制御（Control）]**> > **[ThousandEyes]**> > **[構成（Configure）]** を使用して、ThousandEyes Enterprise Agent のグローバル設定を構成できます。

Cisco DCNM での ThousandEyes Enterprise Agent のグローバル設定の構成

DCNM のスイッチで ThousandEyes Enterprise Agent アクションを実行するには、最初に Cisco DCNM で ThousandEyes Enterprise Agent のグローバル設定を構成する必要があります。

ThousandEyes ポータルからアカウント グループ トークンを取得したことを確認します。

管理者の資格情報を使用して ThousandEyes ポータルにログインします。**[Cloud & Enterprise Agents] > [エージェント設定（Agent Settings）]** に移動し、関連するエージェント名を選択して **[新規 Enterprise Agent の追加（Add New Enterprise Agent）]** をクリックし、**[アカウント グループ トークン（Account Group Token）]** フィールドからトークンをコピーします。

ThousandEyes Enterprise Agent は、DCNM のすべてのファブリックでサポートされています。グローバル設定ですべてのファブリックに対して ThousandEyes Enterprise Agent を構成し、新しいファブリックを作成するときに個々のファブリックに対しても構成できます。個々のファブリックを構成すると、グローバル設定が上書きされ、選択したファブリックに適用されます。選択したファブリックに ThousandEyes Enterprise Agent を構成する前に、グローバル設定が構成されていることを確認してください。

Procedure

ステップ 1 **[制御（Control）] > [ThousandEyes] > [構成（Configure）]** を選択します。

[ThousandEyes 構成（ThousandEyes Configuration）] ウィンドウが表示されます。

ステップ 2 **[ThousandEyes エージェントのインストールを有効にする（Enable ThousandEyes Agent Installation）]** チェック ボックスをオンにして、すべてのフィールドを有効にします。

ステップ 3 次のフィールドには適切なデータを入力します。

- **ThousandEyes アカウント グループ トークン**：インストール用の ThousandEyes Enterprise Agent アカウント グループ トークンを入力します。**[ThousandEyes エージェント設定（ThousandEyes Agent Settings）]** をクリックして、ThousandEyes ポータルにログインします。
- **ThousandEyes Agent Collector Reachability のスイッチ上の VRF**：インターネットの到達可能性を提供する VRF データを入力します。
- **DNS ドメイン**：スイッチの DNS ドメイン構成を入力します。
- **DNS サーバ IP**： Domain Name System（DNS）サーバの IP アドレス（v4/v6）のコンマ区切りリストを入力します。DNS サーバには、最大 3 つの IP アドレスを入力できます。
- **NTP サーバ IP**： Network Time Protocol (NTP) サーバの IP アドレス（v4/v6）のコンマ区切りリストを入力します。NTP サーバには、最大 3 つの IP アドレスを入力できます。
- **プロキシを有効にする**：チェックボックスをオンにして、NX-OS スイッチのインターネット アクセスのプロキシ設定を有効にします。
- **プロキシ情報**：プロキシ サーバのポート情報を入力します。
- **プロキシ バイパス**：プロキシをバイパスするサーバ リストを入力します。

ステップ 4 [保存（Save）] をクリックします。

ThousandEyes Enterprise Agent をインストールする前に、サポートされているスイッチのポリシーを追加するには、「TCAM および CoPP ポリシーの構成」セクションの手順を参照してください。

スイッチで ThousandEyes Enterprise エージェントの操作を実行するには、「ThousandEyes Enterprise エージェント アクションの実行」セクションの手順を参照してください。

レイヤ 4 ～ レイヤ 7 サービス

Cisco DCNM リリース 11.3(1) は、レイヤ 4～レイヤ 7 （L4～L7）サービス デバイスをデータセンター ファブリックに挿入する機能を展開し、これらのサービス デバイスにトラフィックを選択的にリダイレクトすることもできます。サービス ノードを追加し、サービス ノードとサービス リーフ スイッチの間にルート ピアリングを作成し、これらのサービス ノードにトラフィックを選択的にリダイレクトできます。

Cisco Web UI で、**[制御（Control）] > [サービス（Services）]** を選択します。サービス ノードの構成については、レイヤ 4 ～ レイヤ 7 サービス を参照してください。

クロス サイト スクリプティング（XSS）脅威および緩和

クロスサイト スクリプティング（XSS）攻撃は、インジェクションの一種です。悪意のあるスクリプトが、安全で信頼されている Web サイトに投入されます。XSS 攻撃は、攻撃者が Web アプリケーションを使用して悪意のあるコードを送信すると発生します。悪意のあるコードは、ブラウザ スクリプトの形式で別のエンドユーザーに送信されます。

攻撃者はXSSを使用して、疑いを持たないユーザーに悪意のあるスクリプトを送信できます。ブラウザは、スクリプトが信頼されるべきではないことを認識できず、スクリプトを実行します。ブラウザはスクリプトが信頼できる送信元からのものであると考えるため、悪意のあるスクリプトは、ブラウザが保持し、そのサイトで使用されるCookie、セッショントークン、またはその他の機密情報にアクセスできます。

XSS 攻撃は、DCNM へのアクセスが確立されたときに発生します。システムにアクセスし、悪意のある文字列をデータとして DCNM に投入できる承認が与えられたことにより、このブラウザ上の疑いを持たないユーザーによって読み取り可能となりました。そのため、悪意のあるコードが実行されます。 OWASP XSS チートシート は、XSS を引き起こす可能性のある特殊文字の完全なリストを提供します。

クロスサイトスクリプト（XSS）の脅威、およびポリシーフィールドでの特殊文字の取り扱い

さまざまなポリシーフィールドでは、従来、特殊文字を含む文字列を含む値が使用されてきました。

例

```
Port mode = “40G+10G”
Shared secret = <A password having many special characters>
Description = “NYC & SFO, >100G”
```

（注） 「説明」など、一部のフィールドには特殊文字が含まれていない場合があります。「ポート モード」や「共有秘密」などの他のフィールドには、NXOS CLI コマンド形式に関連付けられているか、システムのインターワーキングに必要なため、特殊文字が必要です。

DCNM 11.5(1) での処理

DCNM リリース 11.5(1) は、OWASP ガイドラインに基づいて特殊文字のポリシー関連フィールド コンテンツをサニタイズ（無害化）し、クロス サイト スクリプティング（XSS）攻撃を回避します。ポリシー テンプレート変数の値は、XSS 文字の特別なセットについてスキャンされ、エラーとして報告されます。一部の特殊文字はポリシーで必要になるため、NXOS 要件に従って、DCNM リリース 11.5(2) は特殊文字を許可するメカニズムを提供します。

次の図は、典型的なエラー メッセージを示しています。

DCNM 11.5(2) での処理

Cisco DCNM リリース 11.5(2) には、サニタイズ動作を制御するサーバー プロパティ **ef.sanitize.state** が用意されています。次のキーワードは、機能を説明します。

- **Strict**—OWASP ガイドラインに従って、XSS 脅威文字のコンテンツをサニタイズします。

  これは、例外がないことを意味します。**@ & + \ + % = < >** などの特殊文字はすべて、XSS エラーの原因になります。

- **Default** — 削減された文字セットのコンテンツをサニタイズします。

  使用可能な文字は次のとおりです。**@ % & \ + ‘ = .**

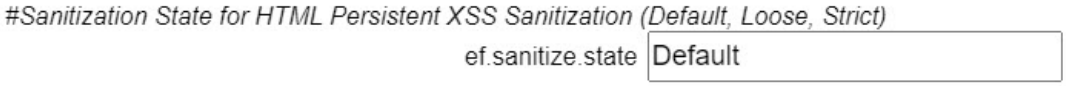
  ただし、これにより、**$** または **< >** のプレフィックス付きの許可された文字がサニタイズされます。

  例：**$@** または **<>@** は許可されていません。ただし、**@** は使用できます。

- **Loose** — サニタイズを完全に無効にします。

Cisco DCNM Web UI でサーバー プロパティをアップデートするには、**[管理（Administration）]** > **[サーバー プロパティ（Server Properties]** を選択します。

このサーバー プロパティのデフォルト値は **Default** です。



Strict モードは、XSS の脆弱なデータが Cisco DCNM に保存されるのを防ぐため、XSS に対する効率的な防御を提供します。ただし、従来のテンプレートが使用されている実用的な理由や、特殊文字の使用が義務付けられている NXOS CLI コマンドの場合は、次のメカニズムのいずれかを使用します。

- 特殊文字を許可するには、次の手順を使用してプロパティ値を **Loose** に設定します。ただし、これにより XSS の脅威が増加します。この場合、次の点に注意してください。
  - データセンター VPN 内など、安全なマシンを使用して DCNM にアクセスできます。これにより、悪意のあるユーザが DCNM に簡単に到達することがなくなります。

- これらの操作には管理者権限が必要なため、**admin** ロールを持つユーザはパスワードのセキュアな管理に取り組みます。

- **[テンプレート コンテンツ（Template Content）]**に XSS の安全でないコンテンツを直接含むカスタム ポリシー テンプレートを作成し、これらのポリシーをスイッチに展開します。

例

以下の CLI を GUI **switch_freeform** ポリシーに追加すると、XSS 脅威緩和の実施により、ポリシーを保存するとエラーが発生します。

```
ip as-path access-list ORIGIN-ACL seq 10 permit "^$"
```

XSS 脅威を軽減するには、次のいずれかを実行します。

- カスタム テンプレートを作成します。手順については、「テンプレートの追加 （429 ページ）.

  次の例は、サンプルのカスタム テンプレートを示しています。

```
##template properties
name =ip_as_path;
description = IP AS Path Custom Template;
tags = ;
userDefined = true;
supportedPlatforms = All;
templateType = POLICY;
templateSubType = DEVICE;
contentType = TEMPLATE_CLI;
implements = ;
dependencies = ;
published = false;
imports = ;
##
##template variables
##

##template content
ip as-path access-list ORIGIN-ACL seq 10 permit "^$"
##
```

- [ポリシーの表示/編集（View/Edit Policies）] から、スイッチにこのテンプレートを使用してポリシーを追加します。

- 新しいポリシーをスイッチに展開します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。