グリーンフィールド VXLAN BGP EVPN ファブリックの管理

この章では、グリーンフィールド VXLAN BGP EVPN ファブリックを管理する方法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 （1 ページ）
- 新規 VXLAN BGP EVPN ファブリックの作成, on page 5
- ファブリックへのスイッチの追加, on page 31
- eBGP EVPN を使用した VXLAN EVPN の展開 （45 ページ）

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、「ネットワークと 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 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。

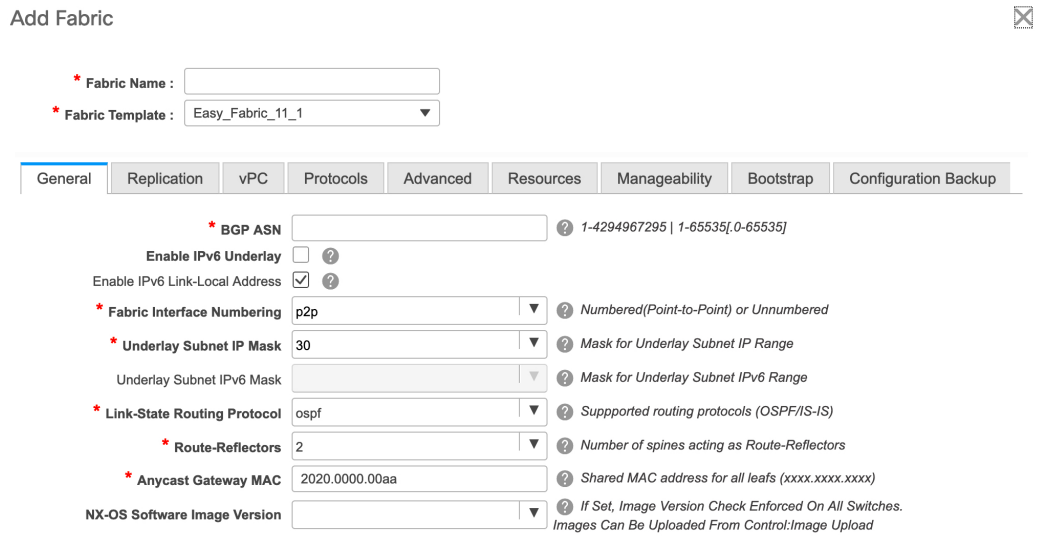
   スタンドアロンまたはメンバーファブリックには、Switch_Fabric（タイプフィールド）、AS 番号（ASN フィールド）、および複製モード（複製モード フィールド）が含まれます。

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。

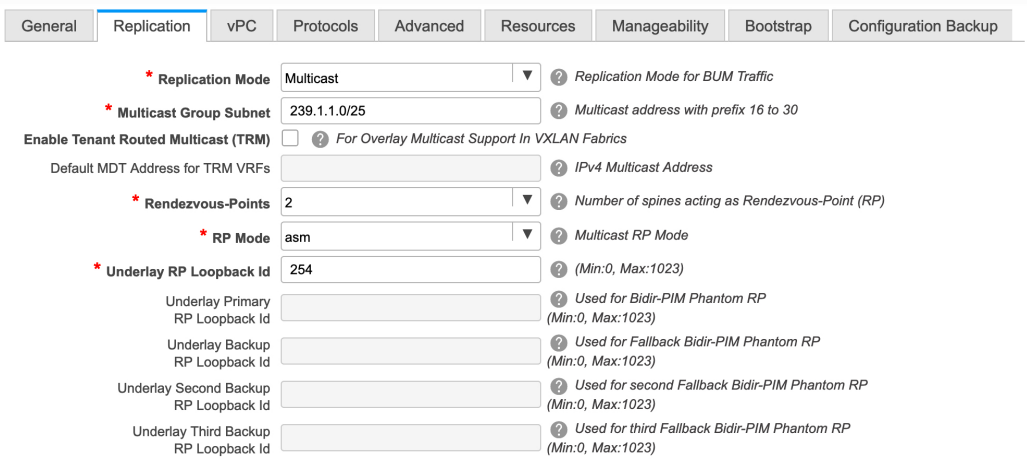
[NX-OSソフトウェア イメージ バージョン（NX-OS Software Image Version）]：リストからイメージを選択します。

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。

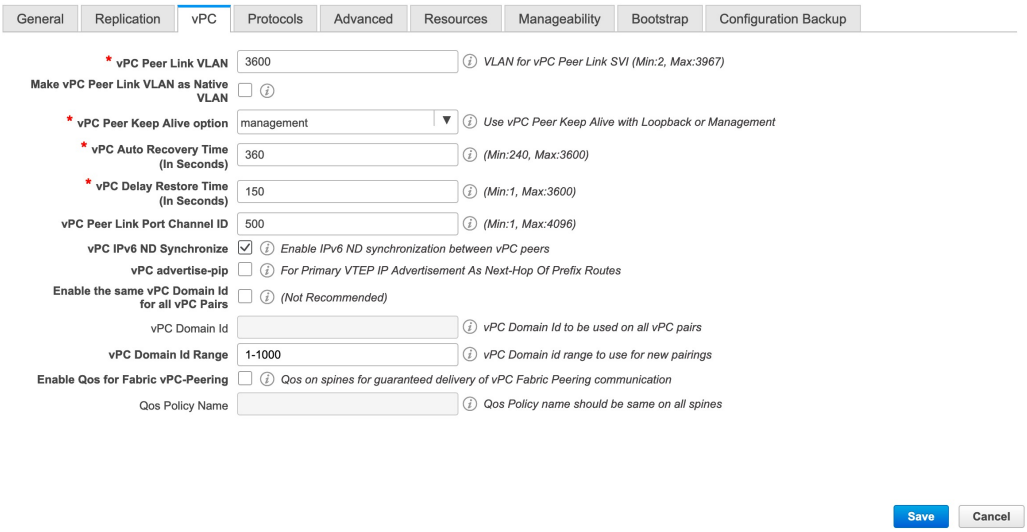
次の 2 つのフィールドは、レプリケーションのマルチキャスト モードとして [BIDIR-PIM] を選択した場合に有効になります。

[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。

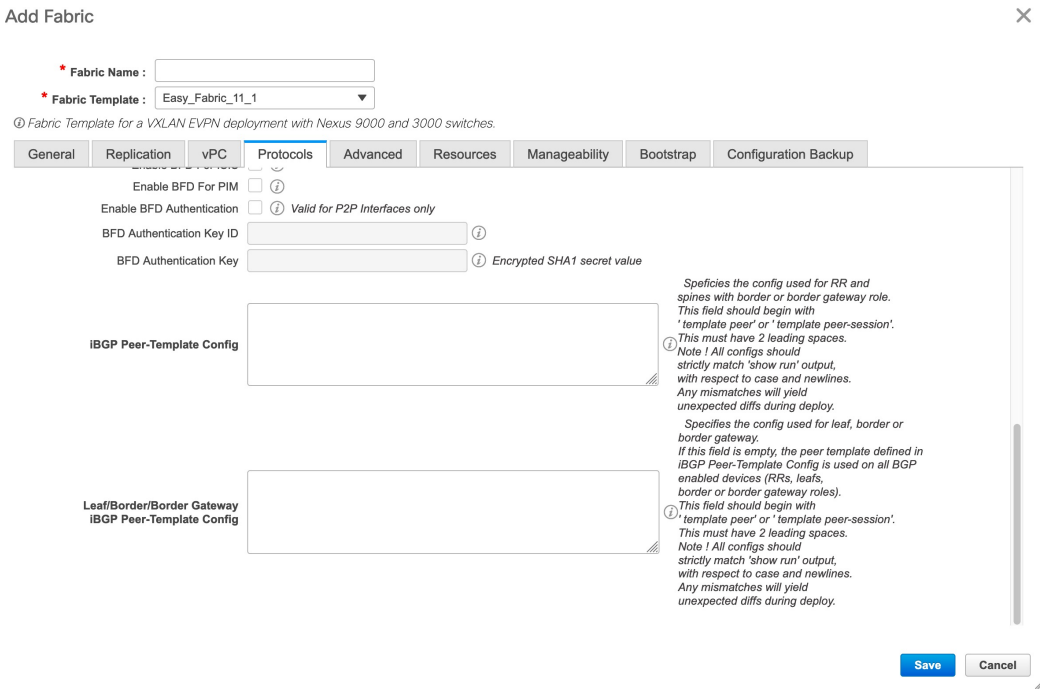
[vPC ドメイン ID の範囲（vPC Domain Id Range）]：新しいペアリングに使用する vPC ドメイン ID の範囲を指定します。

[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 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
```

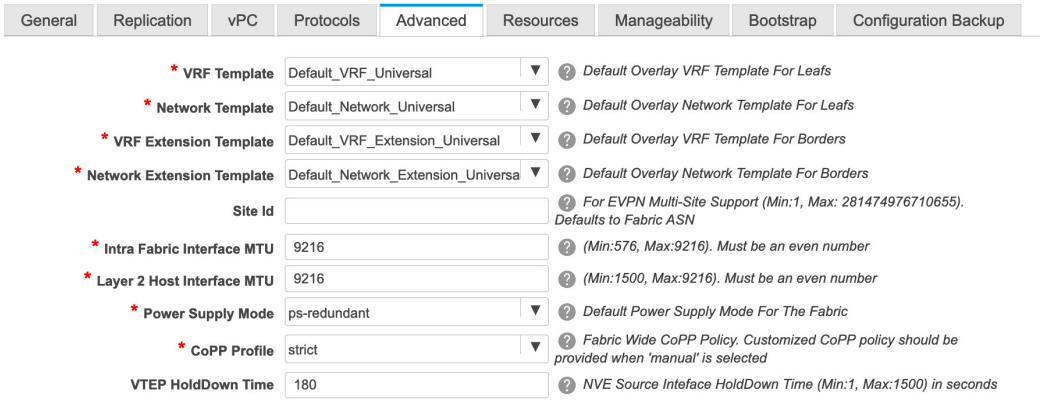
Cisco DCNM リリース 11.3(1) までは、リーフまたはボーダー ロール デバイスの iBGP 定義の iBGP ピア テンプレートと BGP RR は同じでした。DCNM リリース 11.4(1) 以降、次のフィールドを使用してさまざまな構成を指定できます。

- [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、「厳格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。

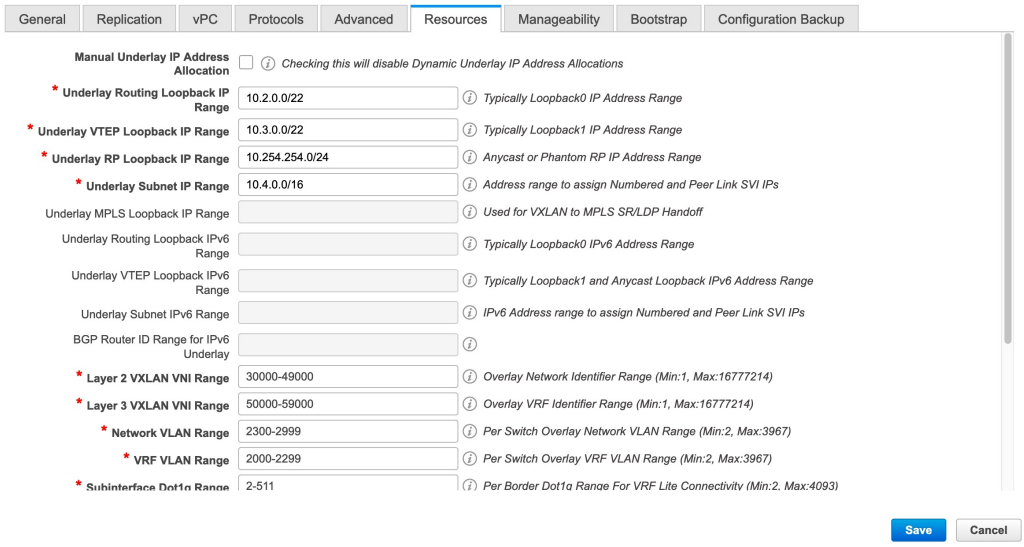
[自由形式の CLI（Freeform CLIs）]：ファブリック レベルの自由形式の CLI は、ファブリックの作成または編集中に追加できます。ファブリック全体のスイッチに適用できます。インデントなしで、実行コンフィギュレーションに表示されている設定を追加する必要があります。VLAN、SVI、インターフェイス構成などのスイッチ レベルの自由形式の構成は、スイッチでのみ追加する必要があります。詳細については、「ファブリック スイッチでのフリーフォーム設定の有効化」を参照してください。

[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。

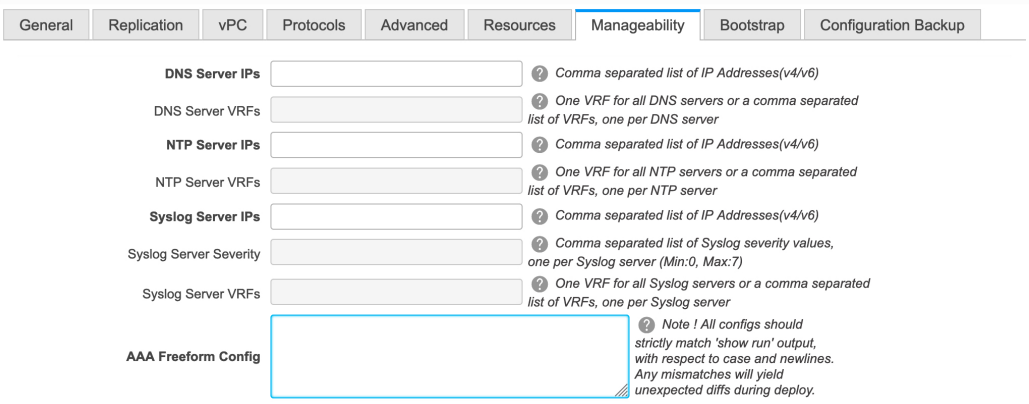
a. L2 範囲を更新し、[保存（Save）] をクリックします。

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）。

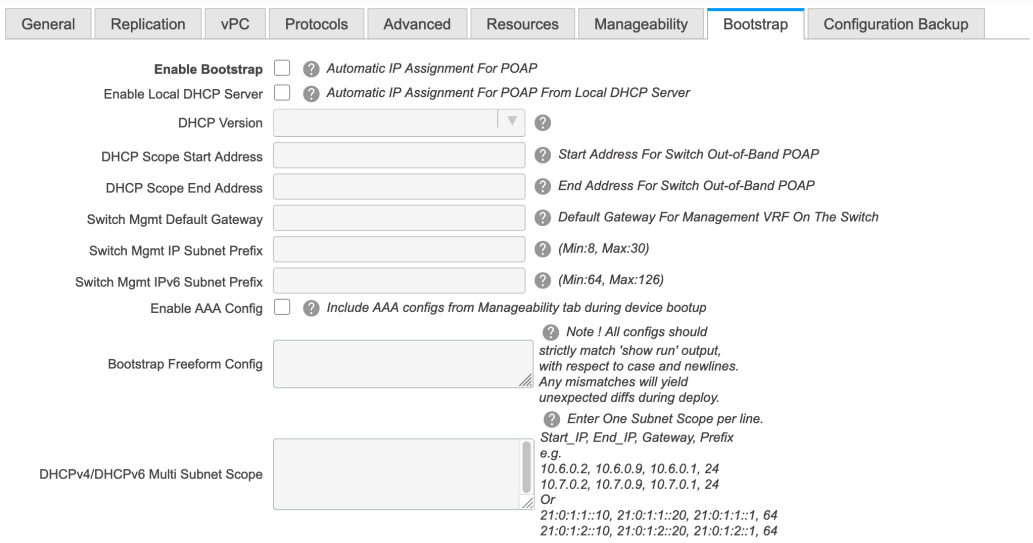
[Syslog サーバのシビラティ（重大度）（Syslog Server Severity）]：syslog サーバごとに 1 つの syslog シビラティ（重大度）値のカンマ区切りリストを指定します。最小値は 0 で、最大値は 7 です。高いシビラティ（重大度）を指定するには、大きい数値を入力します。

[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。

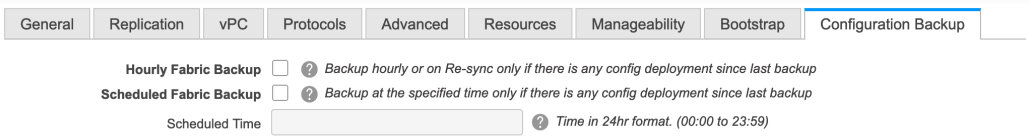
[DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）]：1行に1つのサブネット スコープを入力して、フィールドを指定します。**[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）]** チェックボックスをオンにした後で、このフィールドは編集可能になります。

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。

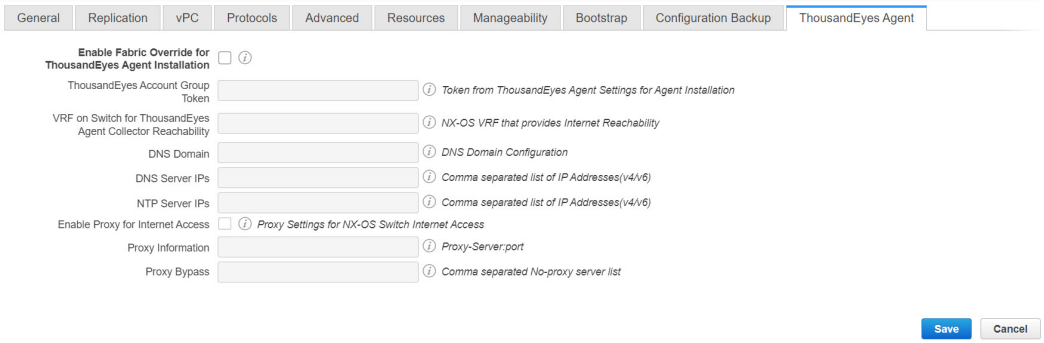
a. **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。[Fabric Builder] 画面が表示されます。

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、「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およびイーサネットインターフェイスの事前プロビジョニングを参照してください。

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。

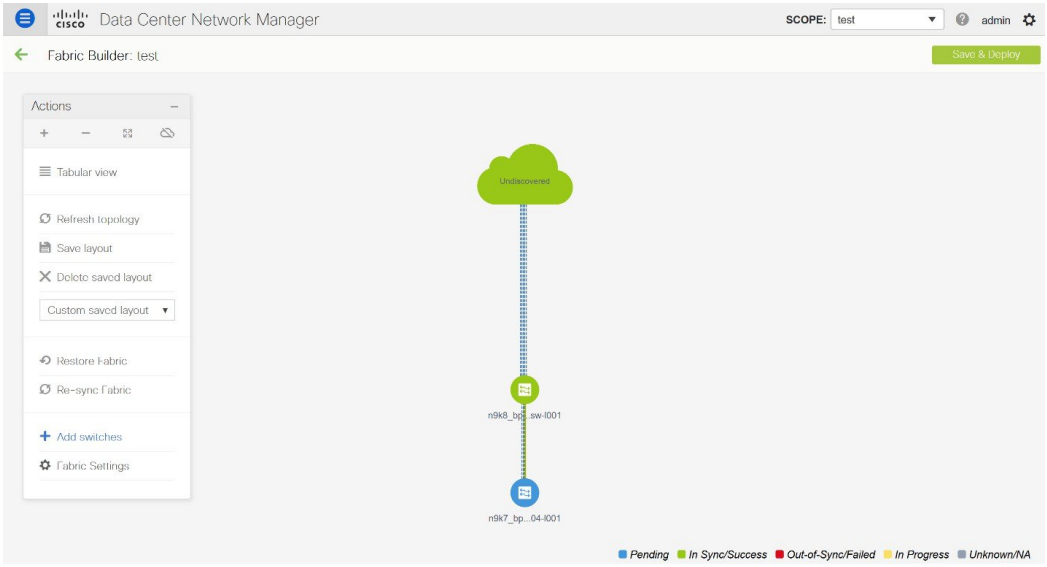
- ホスト名が **[leaf.it.vxlan.bgp.org1-XYZ]** の場合、DCNM で **[leaf]** のみが表示されます。
- ホスト名が **[leaf-itvxlan.bgp.org1-XYZ]** の場合、DCNM で **[leafit-vxlan]** のみが表示されます。

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。



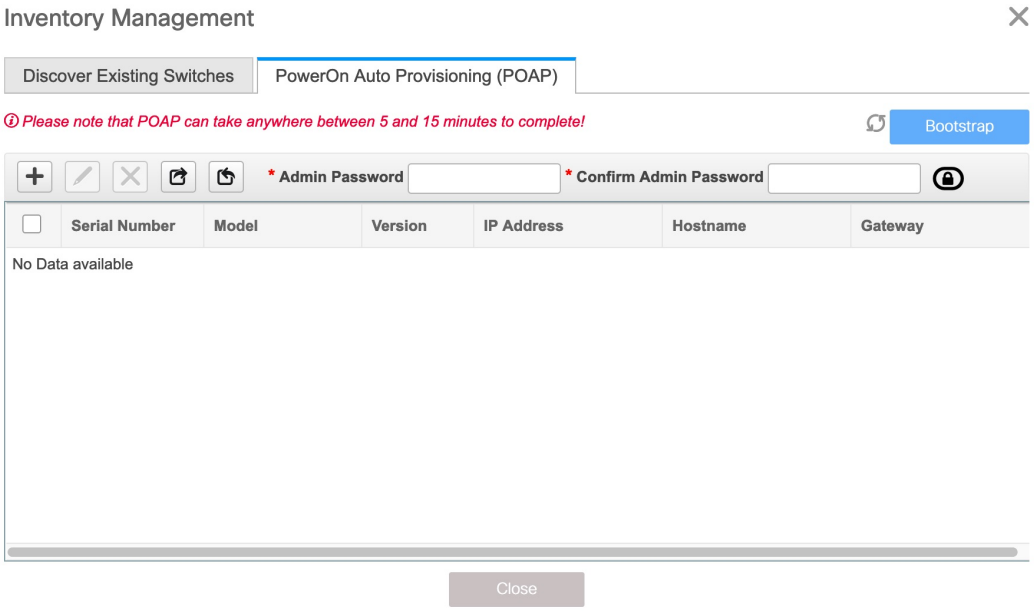
ファブリック トポロジ ウィンドウに移動し、**[アクション（Actions）]** パネルから **[スイッチの追加（Add switches）]** オプションをクリックします。[インベントリ管理（Inventory Management）] ウィンドウが表示されます。

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 を参照してください。

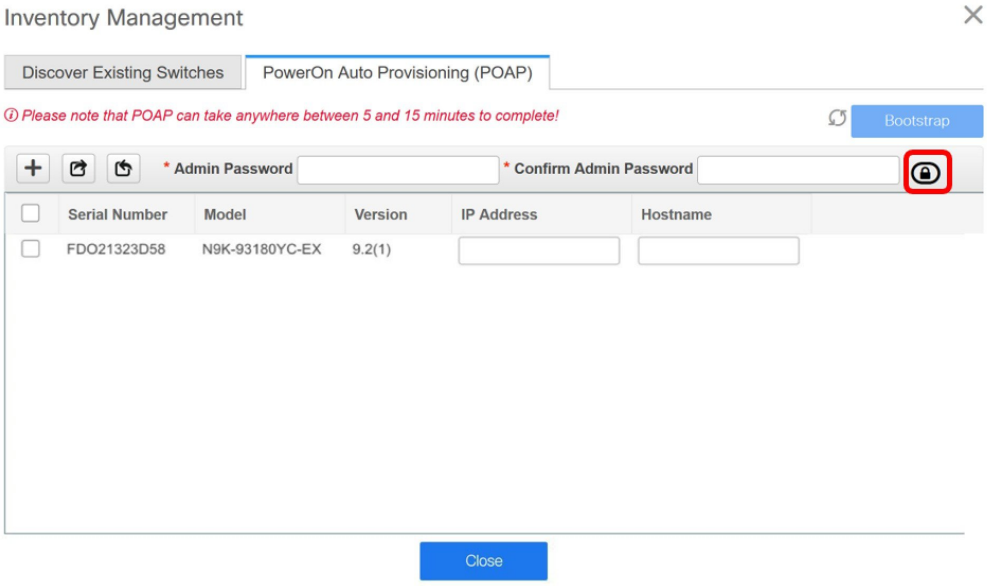
6. **[管理者パスワード（Admin Password）]** フィールドと **[管理者パスワードの確認（Confirm Admin Password）]** フィールドに、新しいパスワードを入力します。

   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。

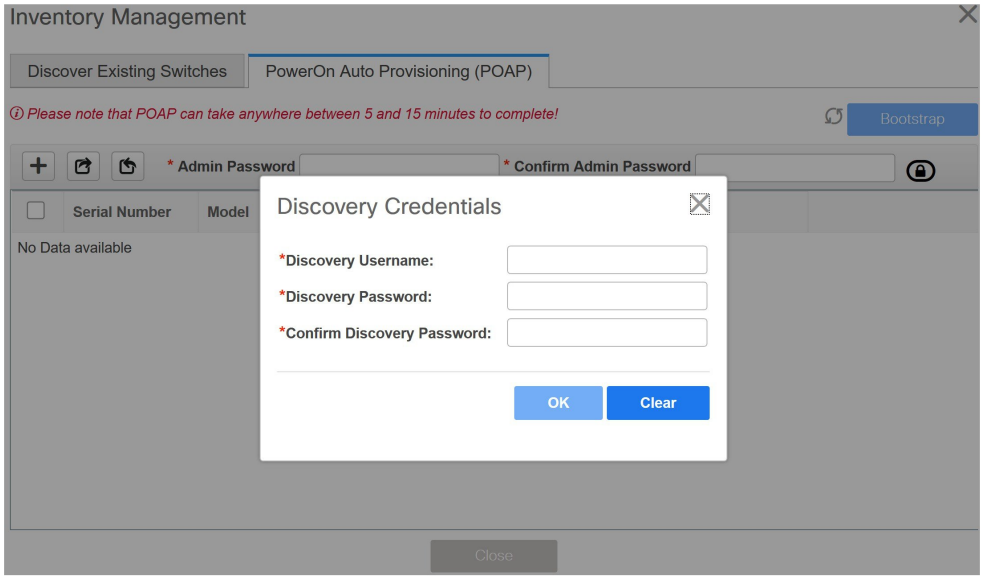
Note 管理者クレデンシャルを使用してスイッチを検出しない場合は、代わりに AAA 認証（RADIUS または TACACS クレデンシャル）を使用できます。

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。

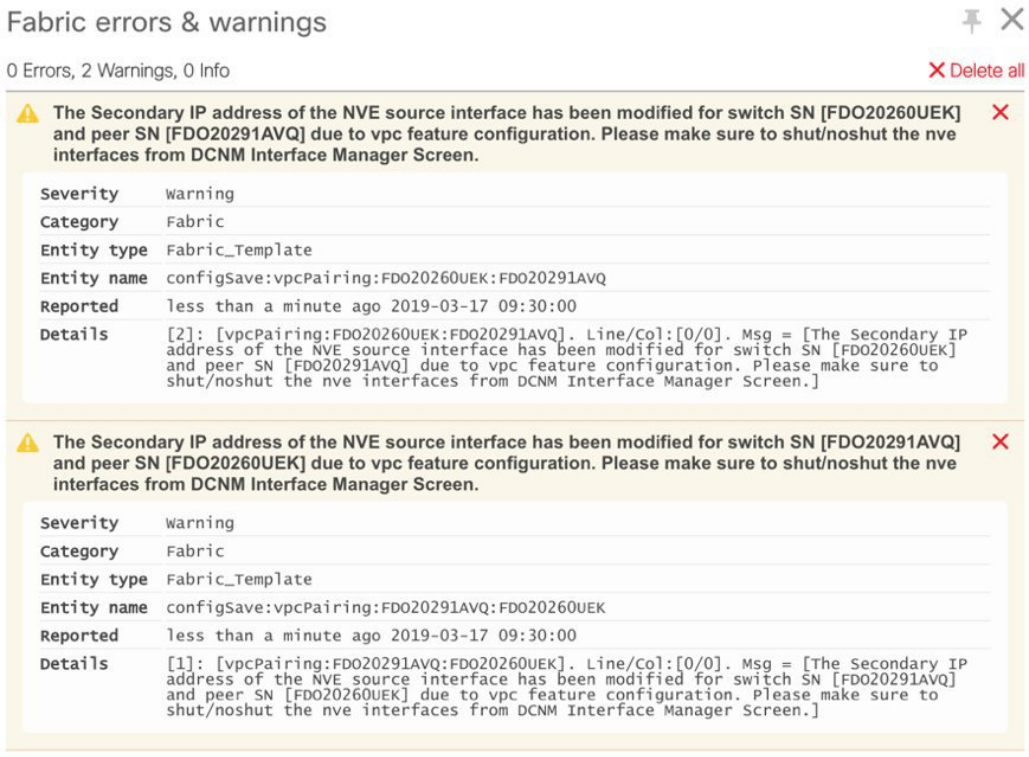
13. **[トポロジの更新（Refresh Topology）]** をクリックして、更新を表示します。すべてのスイッチは、機能していることを示す緑色でなければなりません。

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。

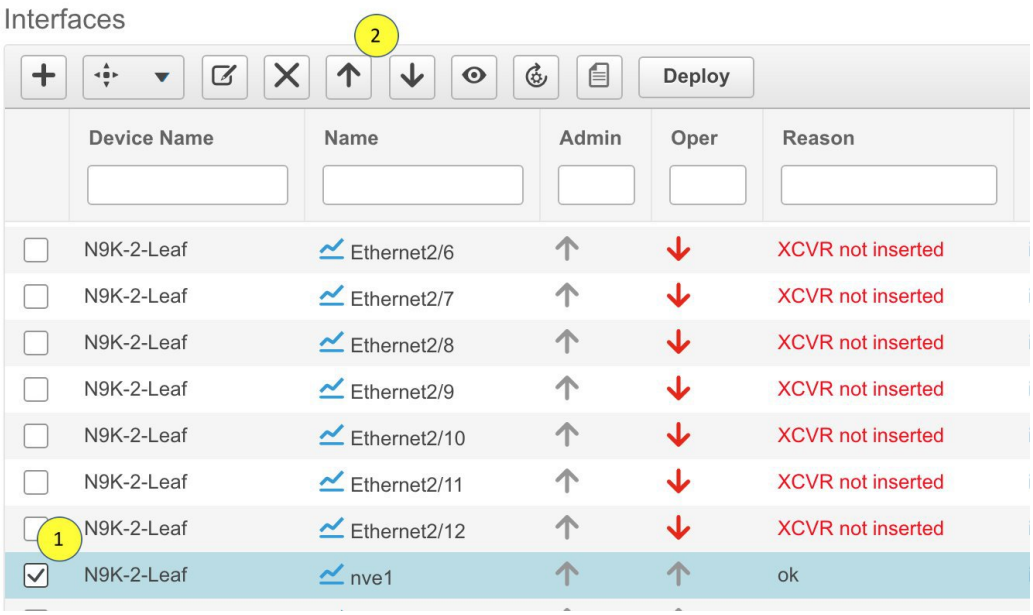
15. DCNM GUIでは、検出されたスイッチは スタンドアロン ファブリック トポロジで確認できます。このステップまでで、POAP は基本設定で完了します。追加構成を行うには、**[制御（Control）] > [インターフェイス（Interfaces）]** オプションを使用してインターフェイスを設定する必要があります。以下が含まれますが、これらに限定されません。

    - 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）。

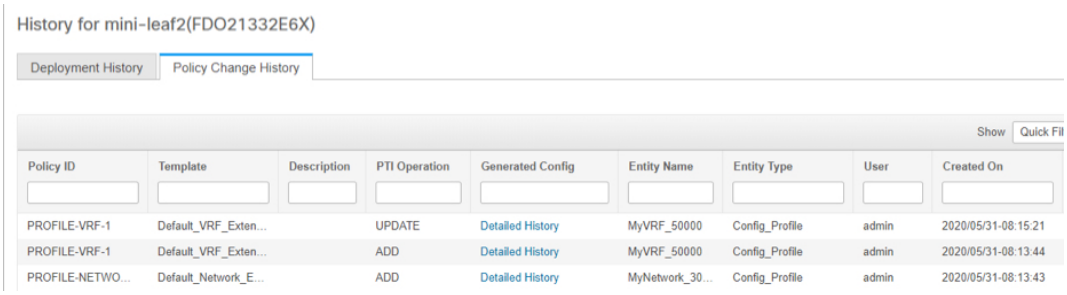
Note

- 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 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。

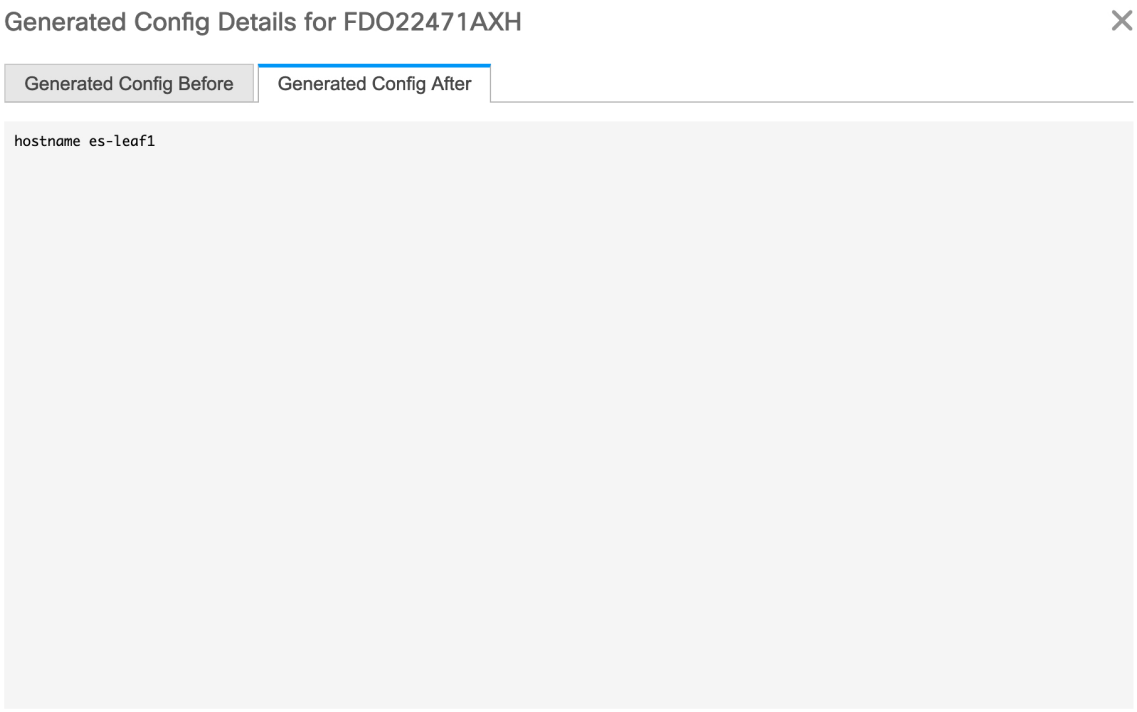
- **モード**：メンテナンス モードとアクティブ/操作モード。
- **vPC** ペアリング：vPC のスイッチを選択し、そのピアを選択します。

  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。

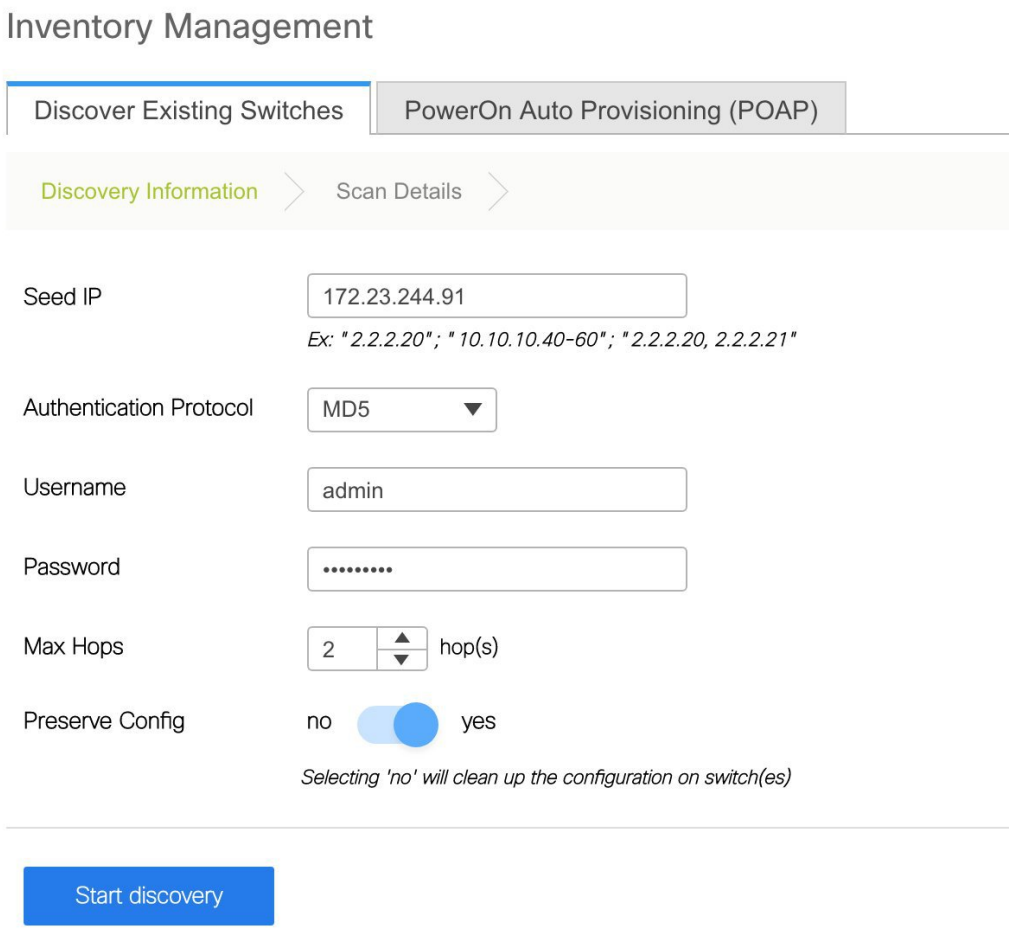
新しいファブリックが作成され、ファブリック構成スイッチが DCNM で検出され、アンダーレイ構成がそれらのスイッチでプロビジョニングされ、DCNM との間の構成が同期されます。その他のタスクは、次のとおりです。

- 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]。

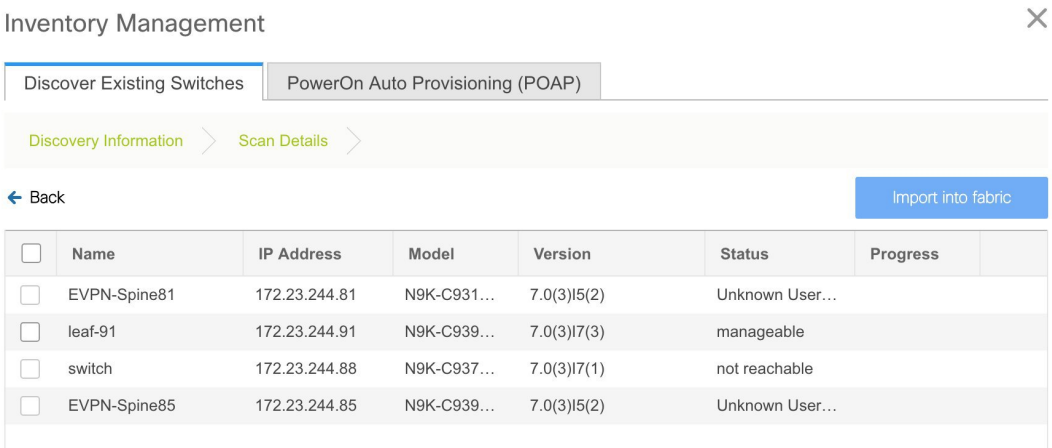
既存のスイッチの検出

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。

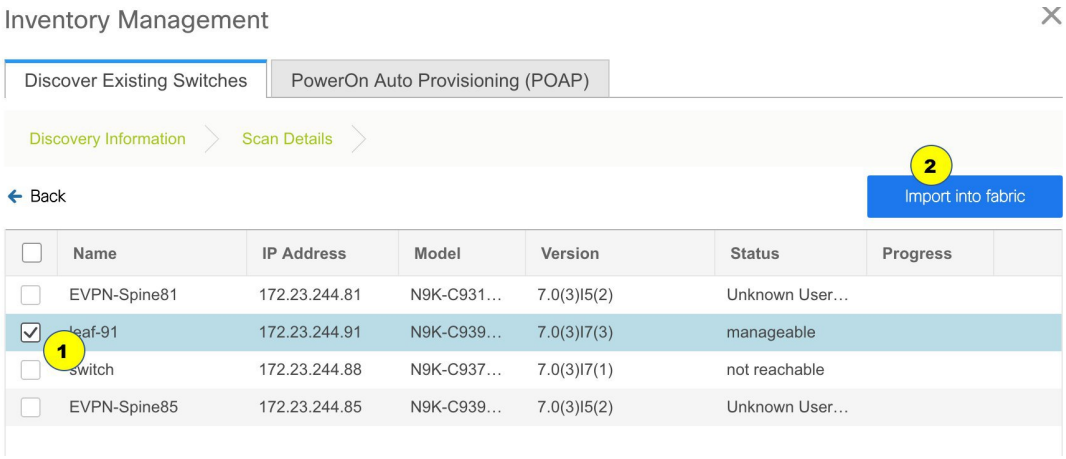
Note Easy_Fabric_eBGP は、ファブリックへのデバイスのブラウンフィールドインポートをサポートしていません。



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。

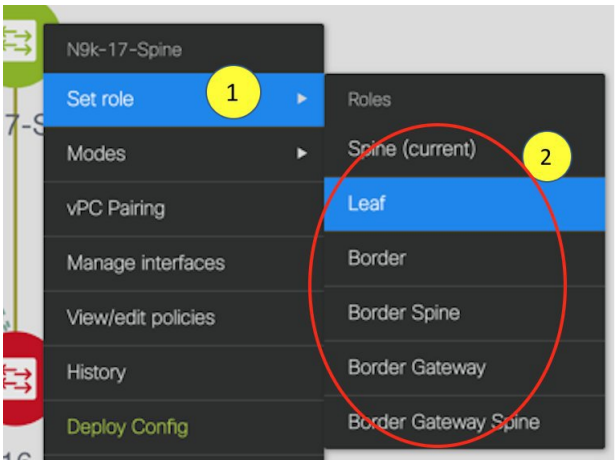
DCNM がすべてのスイッチを検出し、[進行状況（Progress）] 列にすべてのスイッチの **[done]** が表示されたら、画面を閉じます。*[*スタンドアロン ファブリック トポロジ（Standalone fabric topology）] 画面が再び表示されます。追加されたスイッチのスイッチアイコンが表示されます。

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。

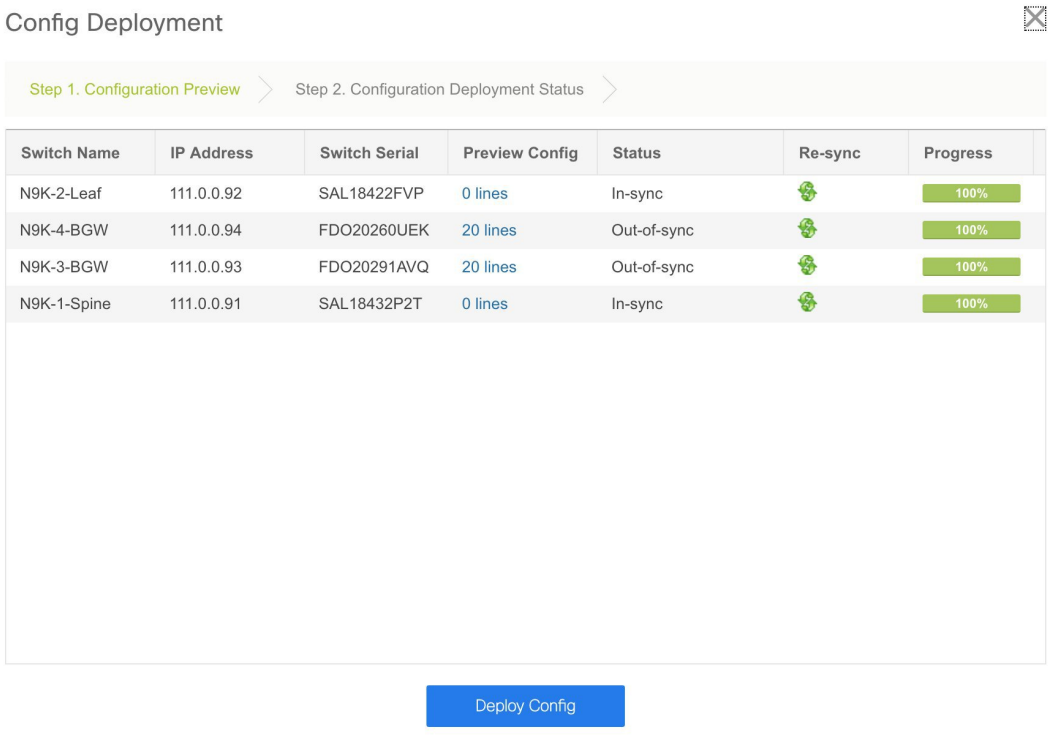
6. 画面の右上にある **[保存と展開（Save & Deploy）]** をクリックします。

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 スイッチでの自由形式構成の有効化」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 スイッチでの自由形式構成の有効化」を参照してください。

eBGP EVPN を使用した VXLAN EVPN の展開

eBGP ベースのアンダーレイを使用した eBGP の新しい VXLAN EVPN の作成

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

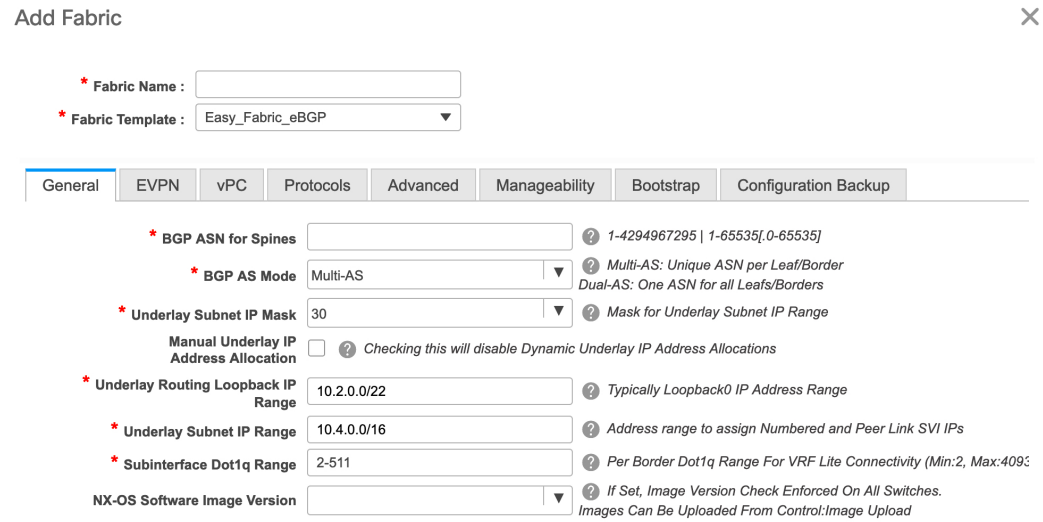
   [ファブリック ビルダ（Fabric Builder）]画面が表示されます。初めてログインしたときには、**[ファブリック（Fabrics）]**セクションにはまだエントリはありません。ファブリックを作成すると、**[ファブリック ビルダ（Fabric Builder）]**画面に表示されます。長方形のボックスが各ファブリックを表します。

2. [ファブリックの作成（Create Fabric）] 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。

   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_eBGP]**ファブリックテンプレートを選択します。スタンドアロンルーテッド 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。



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。

   [スパインの BGP ASN（BGP ASN for Spines）]：ファブリックのスパイン スイッチの BGP AS 番号を入力します。

   [BGP AS モード（BGP AS Mode）]：**[Multi-AS]** または **[Dual-AS]** を選択します。

   Multi-AS ファブリックでは、スパイン スイッチには一意の BGP AS 番号があり、各リーフ スイッチには一意の AS 番号があります。2 つのリーフ スイッチが vPC スイッチ ペアを形成している場合、それらは同じ AS 番号を持ちます。

   [Dual-AS] ファブリックでは、スパイン スイッチには一意の BGP AS 番号があり、リーフスイッチには一意の AS 番号があります。

   ファブリックは、スパイン スイッチの AS 番号によって識別されます。

   [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。

   [手動アンダーレイ IP アドレス割り当て（Manual Underlay IP Address Allocation）]：[動的アンダーレイ IP アドレス割り当て（Dynamic Underlay IP Address Allocation）] を無効にするには、このチェックボックスをオンにします。

   [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 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。

   [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。

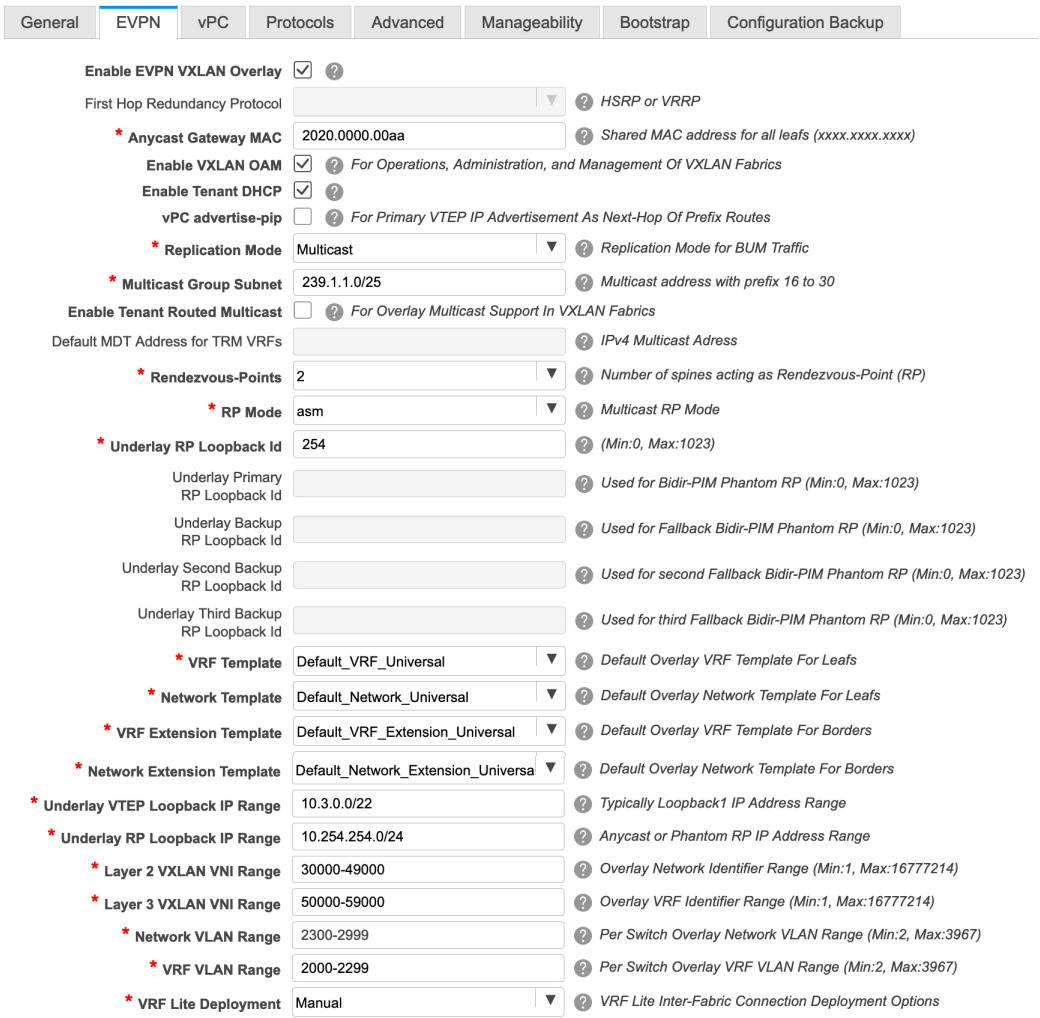
   [NX-OSソフトウェア イメージ バージョン（NX-OS Software Image Version）]：ドロップダウンリストからイメージを選択します。

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。イメージを選択すると、システムはスイッチに選択したバージョンがあるかどうかを確認します。選択されていない場合、エラー メッセージが表示されます。[解決（Resolve）] をクリックすることで、エラーを解決できます。イメージ管理画面が表示され、ISSU オプションを処理できます。その代わりに、リリース ナンバーを削除した後で保存することも可能です。

このフィールドでイメージを指定する場合、ファブリックのすべてのスイッチはそのイメージを実行する必要があります。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。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. **[EVPN]** をクリックします。このタブのほとんどのフィールドは自動入力されます。該当するフィールドは次のとおりです。



[EVPN VXLAN オーバーレイを有効にする（Enable EVPN VXLAN Overlay）]：ファブリックの VXLAN オーバーレイ プロビジョニングを有効にします。

このオプションを選択すると、ルーテッドファブリックを VXLAN 対応のファブリックに変換できます。ファブリックで VXLAN が有効になっている場合、オーバーレイ ネットワークまたは VRF を作成して展開できます。ネットワークまたは VRF を作成して展開する手順は、Easy_Fabric_11_1 の場合と同じです。詳細については、『*Cisco DCNM LAN* ファブリックの構成ガイド』の「ネットワークおよび *VRF* の作成と展開」章を参照してください。

[ルーテッド ファブリック（Routed Fabric）]：ルーテッド ファブリック（VXLAN カプセル化のない IP ファブリック）を作成するためには、EVPN VXLAN オーバーレイ フィールドの有効化を無効にする必要があります。ルーテッドファブリックでは、ネットワークを作成して展開できます。詳細については、ルーテッドファブリックのネットワークの概要を参照してください。

eBGP ルーテッドまたは eBGP VXLAN ファブリックを作成する場合、ファブリックは eBGP をコントロール プレーンとして使用して、ファブリック内接続を構築します。ス

パイン スイッチとリーフ スイッチ間のリンクは、上側で eBGP ピアリングが構築されたポイント ツー ポイント（p2p）番号付き IP アドレスで自動構成されます。

ファブリック内にネットワークまたはVRFが作成されている場合、**[EVPN VXLAN オーバーレイを有効にする（Enable EVPN VXLAN Overlay）]** チェック ボックスを選択して、VXLAN EVPN モードとルーテッド ファブリック モードを切り替えることはできません。ファブリック設定を変更するには、これらのネットワークまたはVRFを削除する必要があります。

Routed_Network_Universal テンプレートは、ルーテッドファブリックにのみ適用されることに注意してください。ルーテッド ファブリックを EVPN VXLAN ファブリックに変換する場合は、ネットワーク テンプレートとネットワーク拡張テンプレートを、EVPN VXLAN に定義されているものに設定します：**Default_Network_Universal** と **Default_Network_Universal** です。EVPN VXLAN ファブリック用にカスタマイズされたテンプレートがある場合は、それを使用することも選択できます。

[ファースト ホップ冗長性プロトコル（First Hop Redundancy Protocol）]：FHRP プロトコルを指定します。**hsrp** または **vrrp** のいずれかを選択します。このフィールドは、ルーテッド ファブリックにのみ適用されます。

Note

- ネットワークの作成後に、このファブリック設定を変更することはできません。変更する場合は、すべてのネットワークを削除してから、FHRP設定を変更する必要があります。
- [EVPN] タブ セクションの残りのフィールドは、EVPN VXLAN オーバーレイを有効にする場合にのみ適用されます。

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

[VXLAN OAM を有効にする（Enable VXLAN OAM）]：既存のスイッチの VXLAN 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、ファブリック設定でOAMを無効にしておいて、自由形式構成でOAMを有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 を有効にする（Enable Tenant DHCP）]：テナント DHCP サポートを有効にします。

[vPC advertise-pip]：アドバタイズ PIP 機能を有効にするには、[vPC advertise-pip] チェックボックスをオンにします。

[レプリケーション モード（Replication Mode）]：ファブリック、入力レプリケーション、またはマルチキャストで使用されるレプリケーションのモードです。

[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。

[テナント ルーテッド マルチキャストを有効にする（Enable Tenant Routed Multicast）]：ファブリック オーバーレイ マルチキャスト プロトコルとしてテナント ルーテッド マルチキャスト（TRM）を有効にするには、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。

[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 スイッチの台数を入力します。

[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、サポート対象の 2 つのマルチキャスト モードからいずれかを選択します。[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。

[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。デフォルトは 254 です。

[双方向（bidir）]を選択すると、以下のフィールドが有効になります。RP カウントに応じて、2 つまたは 4 つのファントム RP ループバック ID フィールドが有効になります。

- **[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（つまりバックアップ）ループバック ID です。

次のループバック ID オプションは、RP カウントが 4 の場合にのみ適用されます。

- **[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）]**：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、第二のバックアップ ループバック ID です。

- **[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）]**：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、第三のバックアップ ループバック ID です。

[VRF テンプレート（VRF Template）] および **[VRF 拡張テンプレート（VRF Extension Template）]**：VRF を作成するための VRF テンプレートと、他のファブリックで 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。

[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 アドレス範囲を指定します。

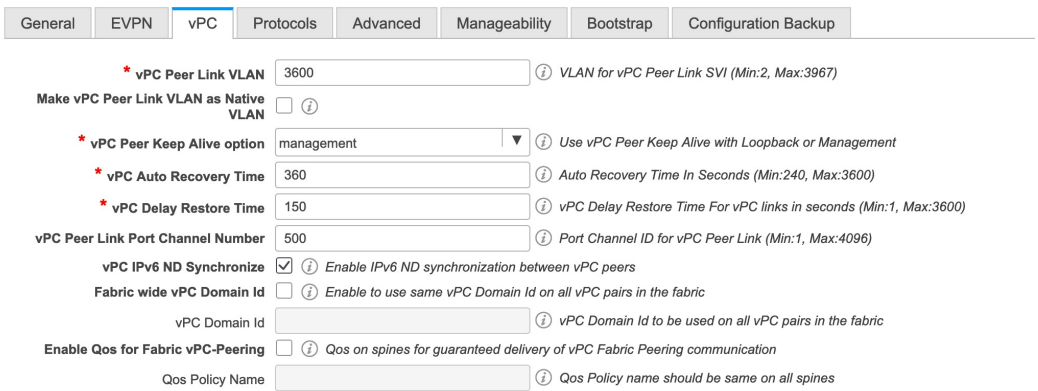
[アンダーレイ RP ループバック IP 範囲（Underlay RP Loopback IP Range）]：エニーキャストまたはファントム RP の IP アドレス範囲を指定します。

[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。

[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。[手動（Manual）] オプションのみがサポートされています。

5. **[vPC]** 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 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 遅延復元時間を秒単位で指定します。

[vPC ピア リンク ポートチャネル番号（vPC Peer Link Port Channel Number）]：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。

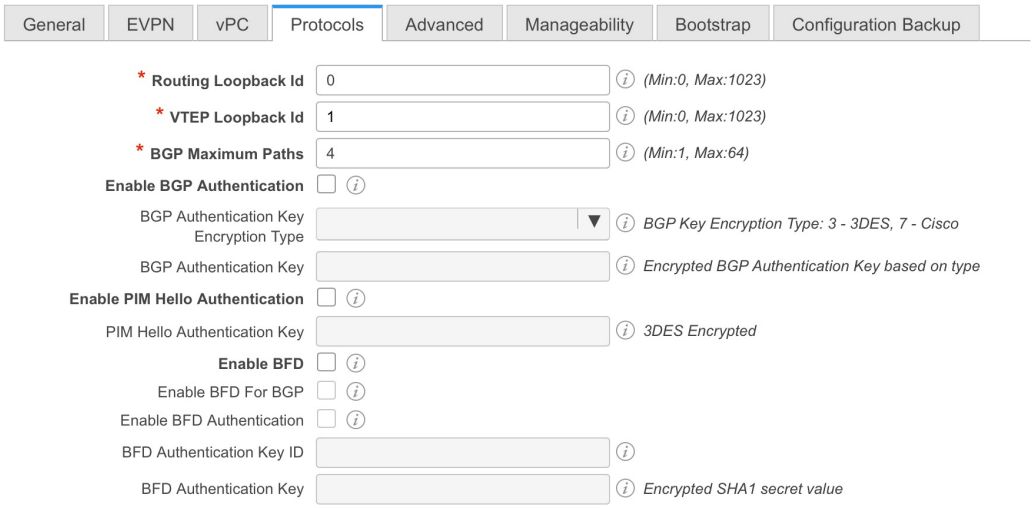
[ファブリック全体の vPC ドメイン ID（Fabric wide vPC Domain Id）]：ファブリック内のすべての vPC ペアで同じ vPC ドメイン ID の使用を有効にします。このフィールドを選択すると、[vPC ドメイン ID（vPC Domain Id）] フィールドが編集可能になります。

[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。

[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。

[QoS ポリシー名（QoS Policy Name）]：すべての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。

6. **[プロトコル（Protocols）]** 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。



[ルーティング ループバック ID（Routing Loopback Id）]：ループバック インターフェイス ID は、デフォルトで 0 として設定されます。BGP ルータ ID として使用されます。

[VTEP ループバック ID（VTEP Loopback Id）]：loopback1 は通常 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。

[BGP 最大パス（BGP Maximum Paths）]：BGP 最大パスを指定します。

[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。

[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、次の構成がすべての 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。

[BGP 向け BFD の有効化（Enable BFD for BGP）]：BGP 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。

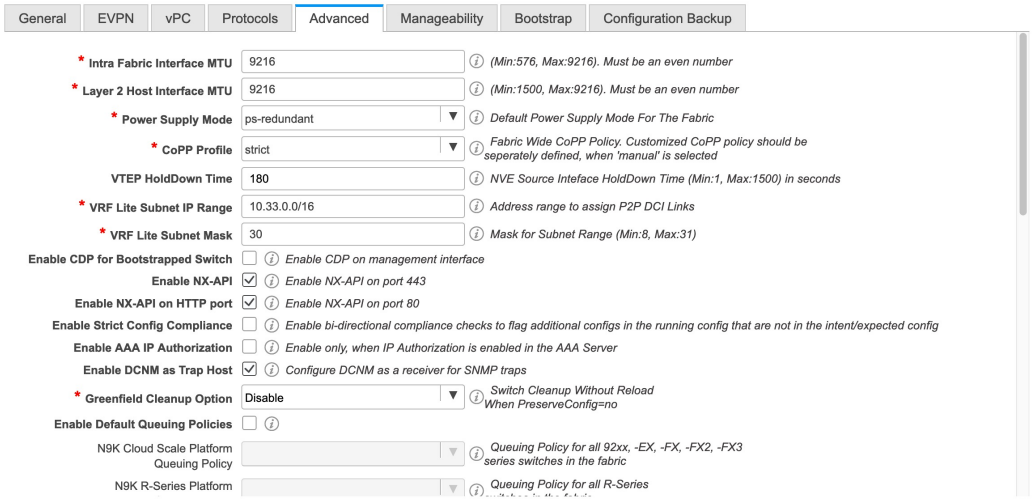
[BGP 認証の有効化（Enable BGP Authentication）]：BGP 認証を有効にするにはチェックボックスをオンにします。このフィールドを有効にすると、[BFD 認証キー ID（BFD Authentication Key ID）] フィールドと [BFD 認証キー（BFD Authentication Key）] フィールドが編集可能になります。

[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。

[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、『*Cisco DCNM LAN* ファブリック構成ガイド』の「暗号化された *BFD* 認証キーの取得」を参照してください。

7. [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。



[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。

[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。

[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、デフォルトでオンになっています。

[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。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。

[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。

厳密な構成コンプライアンスについては、*Enhanced Monitoring and Monitoring Fabrics Guide*を参照してください。

Note ファブリックで厳密な構成コンプライアンスが有効になっている場合、Cisco DCN M のリソースで Network Insights を展開することはできません。

[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。

[グリーンフィールド クリーンアップ オプション（Greenfield Cleanup Option）]：スイッチをリロードせずにスイッチのグリーンフィールドクリーンアップ オプションを有効にします。このオプションは、通常、Cisco Nexus 9000v スイッチを使用するデータセンター環境でのみ推奨されます。

[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。

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。

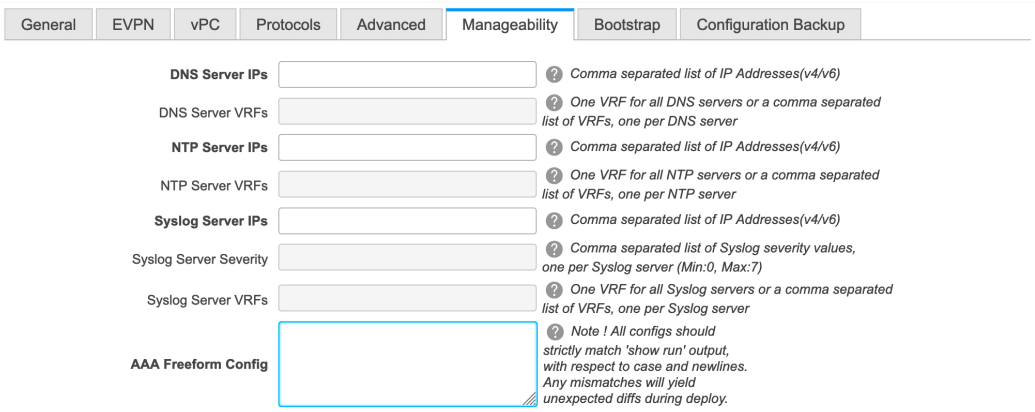
[その他の N9K プラットフォーム キューイング ポリシー（Other N9K Platform Queuing Policy）]：ドロップダウンリストからキューイング ポリシーを選択し、ファブリック内にある、上記 2 つのオプションで説明したスイッチ以外の他のすべてのスイッチに適用します。有効な値は [queuing_policy_default_other] です。

[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構成（Spine Freeform Config）]：スパイン、ボーダー スパイン、およびボーダーゲートウェイ 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. **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 サーバー IP（DNS Server IPs）]：DNS サーバーの IP アドレス（v4/v6）のカンマ区切りリストを指定します。

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

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

[NTP サーバー VRF（NTP Server VRFs）]：すべての NTP サーバーに 1 つの VRF を指定するか、NTP サーバーごとに 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）。

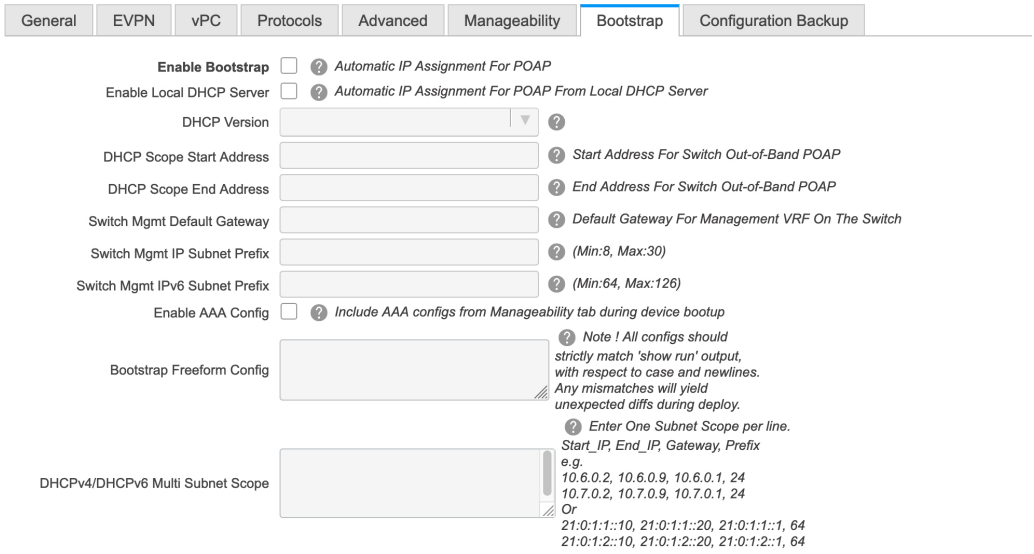
[Syslog サーバのシビラティ（重大度）（Syslog Server Severity）]：syslog サーバごとに 1 つの syslog シビラティ（重大度）値のカンマ区切りリストを指定します。最小値は 0 で、最大値は 7 です。高いシビラティ（重大度）を指定するには、大きい数値を入力します。

[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、**switch_freeform** PTI で、ソースが **UNDERLAY_AAA**、説明が **AAA Configurations** であるものが作成されます。

9. **[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（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、**[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 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。

[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 [管理性（Manageability）] タブから AAA 構成を含めるには、このチェックボックスをオンにします。

[ブートストラップ自由形式の構成（Bootstrap Freeform Config）]：（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、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する必要があります。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、スイッチでのフリーフォーム構成エラーの解決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構成の有効化に記されています。

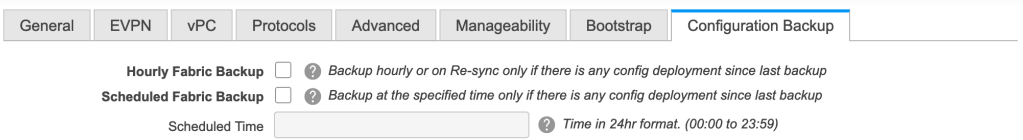
[DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）]：1行に1つのサブネット スコープを入力して、フィールドを指定します。**[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）]** チェックボックスをオンにした後で、このフィールドは編集可能になります。

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

10. **[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。

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。

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。

[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。

Note 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。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。

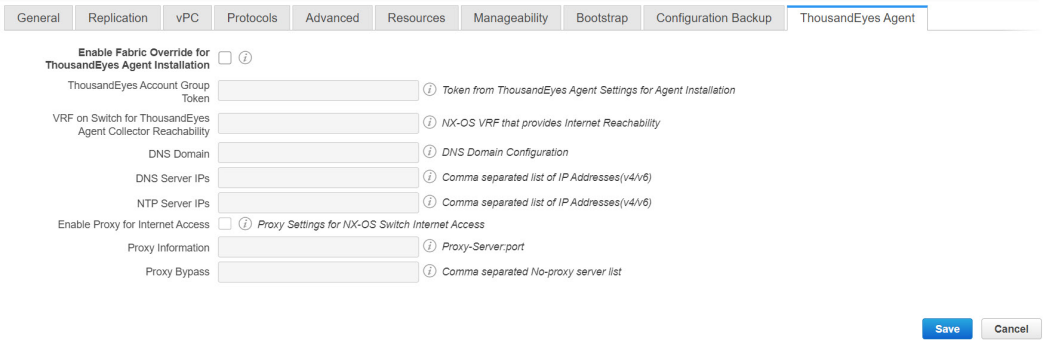
b. 特定のファブリック ボックス内をクリックします。[ファブリック トポロジ (fabric topology)] 画面が表示されます。

c. 画面左側の **[アクション（Actions）]** パネルで、**[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。

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。

11. **[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、「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。

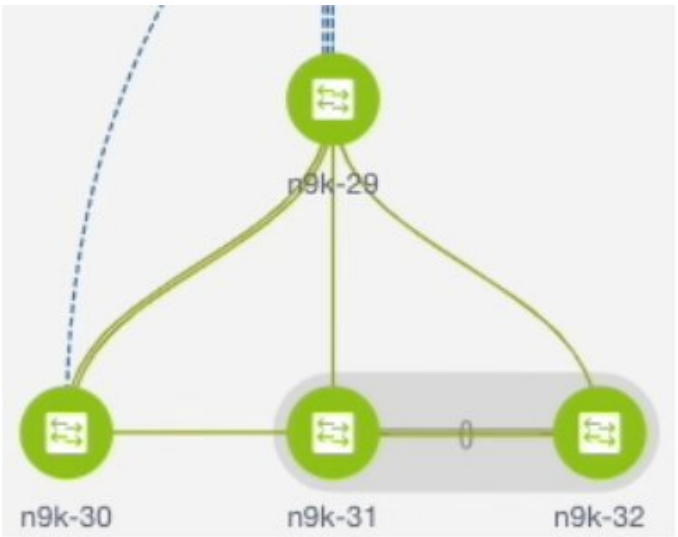
- **[ThousandEyes Agent インストールのファブリック オーバーライドを有効にする（Enable Fabric Override for ThousandEyes Agent Installation）]** : チェック ボックスを選択して、ファブリックで ThousandEyes Enterprise Agent を有効にします。
- **[ThousandEyes アカウント グループ トークン（ThousandEyes Account Group Token）]** : インストール用の ThousandEyes Enterprise Agent トークン ID を指定します。
- **[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ー リストを指定します。

eBGP アンダーレイを備えた VXLAN ファブリック：ポインタ

- すべてのリーフスイッチには共通の AS 番号があるため、リーフ オーバーレイ ポリシーとアンダーレイ ポリシーを一度にすべてのリーフスイッチに展開します。
- ブラウンフィールド移行は、eBGP ファブリックではサポートされていません。
- リーフスイッチの AS 番号は、作成後に再計算と展開（Recalculate & Deploy）操作を実行した後は変更できません。変更が必要になった場合は、**leaf_bgp_asn** ポリシーを削除し、再計算と展開（Recalculate & Deploy）操作を実行して、この AS に関連する BGP 構成を削除する必要があります。次に、新しい AS 番号を使用して、leaf_bgp_asn ポリシーを追加できます。

- Multi-ASモードとDual-ASモードを切り替える場合は、モードを変更する前に、手動で追加されたすべてのBGPポリシー（リーフスイッチのLeaf_bgp_asnおよびebgpオーバーレイ ポリシーを含む）を削除し、**[保存と展開（Save & Deploy）]**操作を実行します。
- デバイスにebgpオーバーレイ ポリシーが存在する場合、リーフスイッチのleaf_bsp_asnポリシーを変更または削除することはできません。最初にebgpオーバーレイ ポリシーを削除してから、leaf_bgp_asnポリシーを削除する必要があります。
- サポートされているロールは、リーフ、スパイン、ボーダー リーフです。
- ボーダー デバイスでは、VRF-Liteは手動モードでサポートされます。外部接続のマルチサイト サポートはありません。
- TRMはサポートされています。
- 機能ファブリックのリーフスイッチとスパインスイッチにポリシーを適用する必要があります。
- VXLAN対応ファブリックの場合、Easy Fabricと同じ方法でオーバーレイ ネットワークとVRFを作成して展開できます。詳細については、『*Cisco DCNM LAN* ファブリックの構成ガイド』の「ネットワークおよび *VRF* の作成と展開」章を参照してください。

ファブリック アンダーレイ eBGP ポリシーの展開



トポロジは、eBGPアンダーレイが有効化されたVXLANファブリックを表示します。DCNMでは、**[Easy_Fabric_eBGP]**テンプレートを持つファブリックが作成されます。1つのスパインスイッチ（n9k-29）と3つのリーフスイッチ（n9k-30、およびvPCスイッチ ペア：n9k-31とn9k-32）がインポートされています。

ファブリックには次の 2 種類があります。

- **マルチ AS モード ファブリックの作成**：マルチ AS モード ファブリックでは、スパイン スイッチには共通の BGP AS 番号があり、各リーフ スイッチには一意の BGP AS 番号があります。Dual-AS から Multi-AS モードへのファブリック変換にも同じ手順を使用します。
- **[Dual-AS モード ファブリックの作成（Creating a Dual-AS mode fabric）]**：Dual-AS モードファブリックの作成については、別の手順が説明されています。Multi-AS から Dual-AS モードへのファブリック変換にも同じ手順を使用します。

  Dual-AS ファブリックでは、すべてのスパイン スイッチには共通の BGP AS 番号があり、すべてのリーフスイッチには共通の BGP AS 番号があります（スパイン スイッチの BGP AS 番号とは異なります）。次のセクションで説明するように、ポリシーを展開する必要があります。

ファブリック アンダーレイ eBGP ポリシーを展開するには、各リーフ スイッチに **leaf_bgp_asn** ポリシーを手動で追加して、スイッチで使用される BGP AS 番号を指定する必要があります。後ほど **[保存と展開（Save & Deploy）]** 操作を実施すると、リーフスイッチとスパイン スイッチ間の物理インターフェイス上に eBGP ピアリングが生成され、アンダーレイの到達可能性情報が交換されます。

1. 画面左側の **[表形式ビュー（Tabular View）]** をクリックします。**Switches | Links** 画面が表示されます。
2. リーフスイッチ（たとえば、n9k-30 チェックボックス）を選択し、**[ポリシーの表示/編集（View/Edit Policies）]** をクリックします。[ポリシーの表示/編集（View/edit policies）] 画面が表示されます。

（注） Dual-AS モードで eBGP ファブリックを作成する場合（または Multi-AS モードから Dual-AS モードに変更する場合）、すべてのリーフスイッチを選択します。これは、共通の BGP AS 番号があるためです。

3. [追加（Add）] 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。
4. [ポリシー（Policy）] ドロップダウンボックスから、**leaf_bgp_asn** を選択し、**[BGP AS #]** フィールドに BGP AS 番号を入力します。
5. [保存（Save）] をクリックします。
6. vPC スイッチに対してこの手順を繰り返します。vPC スイッチ ペアの場合は、両方のスイッチを選択し、**leaf_bgp_asn** ポリシーを適用します。

（注） 前の手順で説明したように、Dual-AS モードでファブリックを作成（または Dual-AS モードに変換）し、それらすべてに BGP AS 番号を割り当てている場合、この手順は必要ありません。

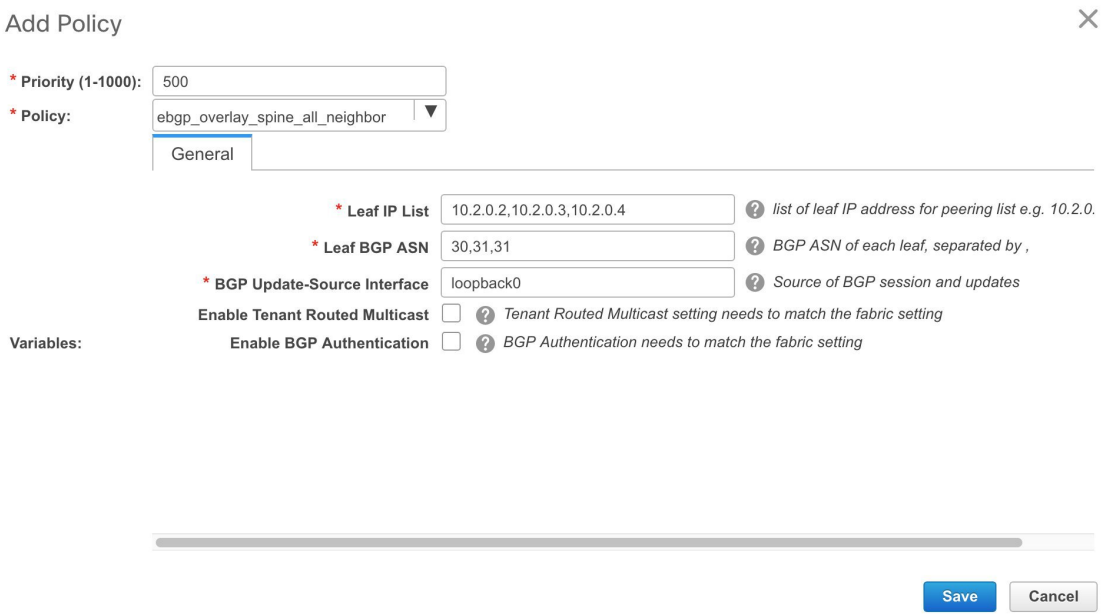
7. **[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウを閉じます
8. トポロジ画面で、画面の右上にある **[保存と展開（Save & Deploy）]** をクリックします。
9. **構成展開** ウィザードに従って構成を展開します。

ファブリック オーバーレイ eBGP ポリシーの展開

オーバーレイ ピアリングの eBGP オーバーレイ ポリシーは手動で追加する必要があります。DCNM は、リーフおよびスパイン スイッチに手動で追加して EVPN オーバーレイ ピアリングを形成できる eBGP リーフおよびスパイン オーバーレイ ピアリング ポリシー テンプレートを提供します。

スパイン スイッチ オーバーレイ ポリシーの展開

ebgp_overlay_spine_all_neighbor ポリシーをスパイン スイッチ n9k-29 に追加します。このポリシーは、すべてのスパイン スイッチで同じフィールド値を共有するため、一度にすべてのスパイン スイッチに展開できます。



この画面のフィールドは次のとおりです。

[リーフ IP リスト（Leaf IP List）]：リーフ スイッチ ルーティング ループバック インターフェイスの IP アドレス。

10.2.0.2 は、リーフスイッチ n9k-30 のループバック 0 ピアリング IP アドレスです。10.2.0.3 および 10.2.0.4 は、vPC スイッチ ペア n9k-31 および n9k-32 の IP アドレスです。

[リーフ BGP ASN（Leaf BGP ASN）]：リーフ スイッチの BGP AS 番号。vPC スイッチの AS 番号は同じ 31 であることに注意してください。

（注） デュアル AS モードでファブリックを作成する場合（またはデュアル AS モードに変換する場合）、すべてのリーフスイッチが属する共通の BGP AS 番号でこのフィールドを更新する必要があります。

[BGP アップデート送信元インターフェイス（BGP Update-Source Interface）]：BGP アップデートの送信元インターフェイスです。このフィールドでは loopback0、つまり、アンダーレイ ルーティングのループバック インターフェイスを使用できます。

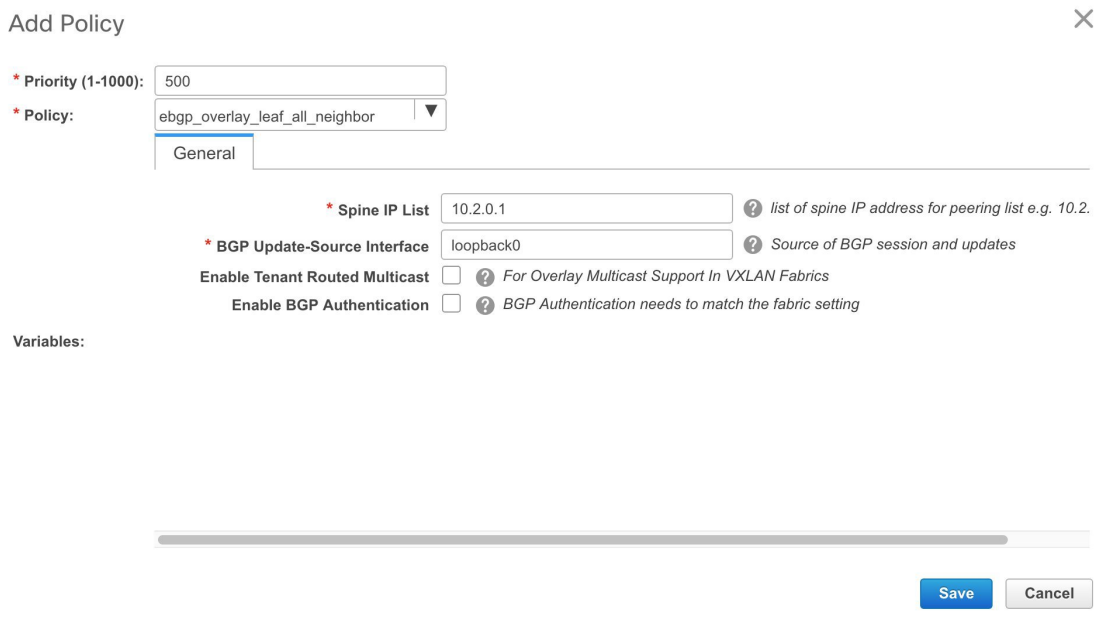
[テナント ルーテッド マルチキャストを有効にする（Enable Tenant Routed Multicast）]：チェックボックスをオンにして、オーバーレイ マルチキャスト トラフィックを処理するための TRM を有効にします。TRM の有効化は、ファブリック設定と一致する必要があります。

[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。

BGP 認証は、ファブリック設定と一致する必要があります。BGP 認証の詳細については、「認証キーの取得」セクションを参照してください。

リーフ スイッチ オーバーレイ ポリシーの展開

すべてのリーフ スイッチに **ebgp_overlay_leaf_all_neighbor** ポリシーを追加して、スパイン スイッチへの eBGP オーバーレイ ピアリングを確立します。このポリシーは、すべてのリーフ スイッチで同じフィールド値を共有するため、一度にすべてのリーフ スイッチに展開できます。



この画面のフィールドは次のとおりです。

[スパイン IP リスト（Spine IP List）]：スパイン スイッチ ルーティング ループバック インターフェイスの IP アドレス。

10.2.0.1 は、スパイン スイッチ n9k-29 のループバック 0 ピアリング IP アドレスです。

[BGP アップデート送信元インターフェイス（BGP Update-Source Interface）]：BGP アップデートの送信元インターフェイスです。このフィールドでは loopback0、つまり、アンダーレイ ルーティングのループバック インターフェイスを使用できます。

[テナント ルーテッド マルチキャストを有効にする（Enable Tenant Routed Multicast）]：チェックボックスをオンにして、オーバーレイ マルチキャスト トラフィックを処理するための TRM を有効にします。TRM の有効化は、ファブリック設定と一致する必要があります。

[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。

BGP 認証は、ファブリック設定と一致する必要があります。BGP 認証の詳細については、「認証キーの取得」セクションを参照してください。

画面の右上にある **[保存と展開（Save & Deploy）]** をクリックして、構成展開ウィザードごとに構成を展開します。または、**[ポリシーの表示/編集（View/Edit Policy）]** オプションを使用し、**[構成のプッシュ（Push Config）]** をクリックして構成を展開します。

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。