Data Center VXLAN EVPN、リリース 12.2.2/12.2.3

目次

新規情報および変更情報

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

リリース バージョン	特長	説明
NDFC リリース 12.2.3	**[BGP 認証キー暗号化タイプ（BGP Authentication Key Encryption Type）]** フィールドでの Cisco 暗号化タイプ 6 のサポート	Data Center VXLAN EVPN ファブリック タイプを作成するときに、**[BGP 認証キー暗号化タイプ（BGP Authentication Key Encryption Type）]** フィールドで Cisco 暗号化タイプ 6 をサポートできるようになりました。IPv4 使用例の詳細は、「データ センター VXLAN EVPN テンプレートを使用したVXLAN EVPN ファブリックの作成」を参照してください。
NDFC リリース 12.2.3	**[リーフ-ToR ペアリングで許可される VLAN を設定（Set Allowed Vlan On Leaf-ToR Pairing）]** フィールドの導入	Data Center VXLAN EVPN ファブリック タイプを作成する場合、新しい **[リーフ-ToR ペアリングで許可される VLAN を設定（Set Allowed Vlan On Leaf-ToR Pairing）]** フィールドを使用して、リーフと ToR ペアリング ポート チャネルのトランク許可 VLAN を none または all に設定できます。IPv4 使用例の詳細は、「データ センター VXLAN EVPN テンプレートを使用したVXLAN EVPN ファブリックの作成」を参照してください。
NDFC リリース 12.2.3	**[自由形式（Freeform）]** タブの導入	Data Center VXLAN EVPN ファブリック タイプを作成すると、自由形式の構成フィールドが 1 つの **[自由形式（Freeform）]** タブに統合されるようになりました。IPv4 使用例の詳細は、「データ センター VXLAN EVPN テンプレートを使用したVXLAN EVPN ファブリックの作成」を参照してください。
NDFC リリース 12.2.3	800 Gb のインターフェイス速度の QoS キューイング ポリシーをサポートします。	**[AI/ML QOS & Queuing Policy]** オプションを有効にすると、新しい **[AI_Fabric_QOS_800G]** フィールドが追加され、800 Gb のインターフェイス速度の QoS キューイング ポリシーが有効になります。詳細については、「詳細情報」のセクションを参照してください。
NDFC リリース 12.2.3	**[ToR の vPC 遅延復元時間（秒）（vPC Delay Restore Time for ToR（In Seconds））]** フィールドの導入	ToR スイッチの vPC 遅延復元期間を秒単位で指定するには、新しい **[ToR の vPC 遅延復元時間（秒）（vPC Delay Restore Time for ToR（In Seconds））]** フィールドを使用できます。詳細については、「vPC」を参照してください。

リリース バージョン	特長	説明
NDFC リリース 12.2.2	QKD サーバまたは事前共有キーを使用した MACsec でのファブリック間リンクを使用したファブリック接続のサポート	この機能を使用すると、量子キー流通（QKD）サーバを使用して Media Access Control Security（MACsec）とファブリック間リンクを使用して 2 つのファブリックを接続し、暗号化キーを安全に交換するか、事前共有されたキーを提供できます。 NDFC 12.2.2 以降、NDFC は、次のファブリック タイプのファブリック間リンクの MACsec のサポートを追加しました。 • データ センター VXLAN EVPN • 拡張クラシック LAN • 外部接続ネットワーク NDFC 12.2.2 より前のバージョンでは、NDFC は Data CenterVXLAN EVPN および BGP のファブリック内リンクの MACsec をサポートしていました。 このリリースでは、NDFC は MACsec パラメータを **[詳細（Advanced）]** タブから新しい **[セキュリティ（Security）]** タブに移動しました。詳細については、「セキュリティ」を参照してください。 量子鍵伝送（QKD）サーバを使用した MACsec の詳細については、「QKD を使用して、2 つのファブリックを MACsec と接続する」を参照してください。

リリース バージョン	特長	説明
NDFC リリース 12.2.2	PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN EVPN ファブリックの作成のサポートが追加されました	NDFC の以前のリリースでは、NDFC は入力レプリケーション（IR）で IPv6 アンダーレイをサポートしていました。NDFC 12.2.2 リリース以降、NDFC はマルチキャス トレプリケーションのサポートを追加しました。以前は、NDFC はスタンドアロン VXLANv4 ファブリックをサポートしていました。NDFC 12.2.2 以降、NDFC は VXLANv6 を使用したマルチサイト ドメイン（MSD）ファブリックの作成をサポートしています。 NDFC 12.2.2 より前のバージョンでは、NDFC はテナント ルーテッド マルチキャスト（TRM）IPv4 をサポートしていました。NDFC 12.2.2 では、NDFC は、IPv4 または IPv6 のマルチキャストトラフィックの転送を有効にするために、**[VRF の作成（Create VRF）]** ページに新しいタブ **TRM** を使用して TRMv6 のサポートを追加しました。既存の IPv4 TRM フィールドは、**[詳細（Advanced）]** タブから **[TRM]** タブに移動されます。 この機能は、次のファブリック タイプで使用できます。 • データセンター VXLAN EVPN ファブリック • BGP（eBGB EVPN）ファブリック • VXLAN EVPN マルチサイト ファブリック 詳細は、次のトピックを参照してください。 • Data Center VXLAN EVPN テンプレートを使用した VXLAN EVPN ファブリックの作成 • VRF の作成 • PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN EVPN ファブリックの構成。

VXLAN EVPN ファブリックのプロビジョニング

Cisco Nexus Dashboard Fabric Controller では、Nexus 9000 および 3000 シリーズ スイッチにおける 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、拡張「Easy」ファブリック ワークフローを提供しています。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構成により、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希望するアンダーレイ 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、Nexus Dashboard Fabric Controller 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 Nexus Dashboard Fabric Controller 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。

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

[アクション（Actions）] ドロップダウン リストの下の、[管理（Manage）] > [ファブリック（Fabrics）] > [ファブリックの作成（Create Fabric）]。

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。

[アクション（Actions）] ドロップダウン リストの下の、**[管理（Manage）]** > **[インベントリ（Inventory）]** > **[インターフェイス（Interfaces）]** > **[新しいインターフェイスの作成（Create New Interface）]** を選択します。

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。

[アクション（Actions）] ドロップダウン リストで、**[管理（Manage）]** > **[インベントリ（Inventory）]** > **[スイッチ（Switches）]**、**[スイッチの追加（Add Switches）]** を選択します。

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。
- Nexus Dashboard Fabric Controller のファブリックからプロビジョニングを削除します。

[管理（Manage）] > **[インベントリ（Inventory）]** > **[スイッチ（Switches）]** > **[スイッチの概要（Switch Overview）]** > **[サービス（Services）]** メニュー オプション。

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。ファブリック コントローラからオーバーレイ 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による展開の詳細については、LAN の動作モードでのファブリックの概要についての「ネットワーク」および「VRF」のセクションで扱われています。

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 Nexus Dashboard Fabric Controller 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
  - **guestshell** コマンドを実行する機能。これには、Nexus Dashboard Fabric Controller トラッカーのため、**run guestshell** によりプレフィックスが付けられます。
- 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 Nexus Dashboard Fabric Controller 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 クレデンシャルは、デバイスごと、ユーザーごとに Nexus Dashboard Fabric Controller 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 クレデンシャルが設定されていない場合、Nexus Dashboard Fabric Controller 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 クレデンシャルを設定し、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構成コンプライアンス 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

  [設定の再計算（Recalculate Config）] 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設定が生成されます。**[構成のプレビュー（Preview Config）]** をクリックして、生成された構成をプレビューし、ファブリック レベルで展開します。そのため、ファブリックのサイズによっては、**[構成の展開（Deploy Config）]** 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、**[スイッチに構成を展開（Deploy config to Switches）]**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。

- 永続的な構成の差分は、コマンドライン：system nve infra-vlanintforce 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、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-vlanintforce コマンドは常に diff として機能しれます。

  Nexus Dashboard Fabric Controllerのインテントには、次の行が含まれています。

  ```
  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構成を編集して 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。**[構成のプレビュー（Config Preview）]** ウィンドウの **[並べて比較（Side-by-side）]** タブを使用して、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 Nexus Dashboard Fabric Controller 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。

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

「double-wide」なしで arp-ether 領域を構成すると、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 Nexus Dashboard Fabric Controller のポリシーとマッチしないため、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。

Data Center VXLAN EVPN テンプレートを使用した VXLAN EVPN ファブリックの作成

このトピックでは、**データ センター VXLAN EVPN** テンプレートを使用して新しい VXLAN EVPN ファブリックを作成する方法について説明し、IPv4 アンダーレイについて説明します。

Data Center VXLAN EVPN ファブリックは、IPv6 アンダーレイで作成できます。IPv6 アンダーレイは、VXLAN EVPN テンプレートでサポートされます。IPv6 アンダーレイの詳細については、「VXLANv6 ファブリックの構成」および「PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN EVPN ファブリックの構成」を参照してください。

1. **[LAN ファブリック（LAN Fabrics)]** ページ に移動します：

   [管理（Manage）] > [ファブリック（Fabrics）]

2. **[アクション（Action）] > [ファブリックを作成（ Create Fabric）]** をクリックします。

   [ファブリックの作成（Create Fabric）] ウィンドウが表示されます。

3. **[ファブリック名（Fabric Name）]** フィールドにファブリックの一意の名前を入力し、**[ファブリックの選択（Choose Fabric）]** をクリックします。

   使用可能なすべてのファブリック テンプレートのリストが表示されます。

4. ファブリック テンプレートの使用可能なリストから、データセンター VXLAN EVPN テンプレートを選択し、**[選択（Select）]** をクリックします。

5. ファブリックを作成するために必要なフィールド値を入力します。

   画面のタブとそのフィールドについては、次のセクションで説明されています。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。

   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、「VXLAN EVPN マルチサイト」のトピックを参照してください。

   - 一般的なパラメータ
   - Replication
   - vPC
   - Protocols
   - セキュリティ
   - 詳細設定
   - Freeform（NDFC 12.2.3 リリースのみ）
   - 関連資料
   - 管理性（Manageability）
   - ブートストラップ

- コンフィギュレーションのバックアップ
- Flow Monitor

6. 必要な構成が完了したら **[保存（Save）]** をクリックします。
   - [ファブリック（Fabric）] をクリックして、スライドイン ペインに概要を表示します。
   - **[起動（Launch）]** アイコンをクリックして、**[ファブリックの概要（Fabric Overview）]** を表示します。

一般的なパラメータ

デフォルトでは、**[全般パラメータ（General Parameters）]** タブが表示されます。次のテーブルにこのタブのフィールドが説明されています。

フィールド	説明
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。これは、既存のファブリックと同じである必要があります。
IPv6 アンダーレイの有効化（Enable IPv6 Underlay）	Pv6 アンダーレイ機能を有効にします。詳細については、「データ センター VXLAN EVPN」の「VXLANv6 ファブリックの構成」および「PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN EVPN ファブリックの構成」を参照してください。
IPv6 リンクローカル アドレスを有効にする	|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	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	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 サブネット IPv6 マスク	ファブリック インターフェイスの IPv6 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	ファブリック、OSPF、または IS-IS で使用される IGP です。

フィールド	説明
ルートリフレクタ（RR）（Route-Reflectors）	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 として展開する際、Nexus Dashboard Fabric Controller 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（Increasing the count）*：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（Decreasing the count）*：4 つのルート リフレクタを 2 つに減らすとき、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。 1. ドロップダウンボックスの値を 2 に変更します。 2. 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。 3. 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。 4. ファブリック トポロジ ウィンドウで **[構成の展開（Deploy Config）]** をクリックします。 RR と RP は、最初の **[保存と展開（Save & Deploy）]** 操作を実行する前に事前選択できます。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	エニーキャスト ゲートウェイ MAC アドレスを指定します。
パフォーマンス モニタリングの有効化	オンにすると、パフォーマンス モニタリングが有効になります。 スイッチのコマンド ライン インターフェイスからインターフェイス カウンタをクリアしないでください。インターフェイス カウンタをクリアすると、パフォーマンス モニターにトラフィック使用率に関する誤ったデータが表示される可能性があります。カウンタをクリアする必要があり、スイッチに clear counters コマンドと clear counters snmp コマンドの両方がある場合（すべてのスイッチに clear counters snmp コマンドがあるわけではない）、main コマンドと SNMP コマンドの両方を同時に実行してください。たとえば、clear counters interface ethernet slot/port コマンドを実行し、clear counters

フィールド	説明
	interface ethernet slot/port snmp コマンドを実行する必要があります。これにより、1 回限りのスパイクが発生する可能性があります。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な構成が完了したら **[保存（Save）]** をクリックします。

Replication

[レプリケーション（Replication）] タブのフィールドについては、次の表で説明します。ほとんどのフィールドは、シスコが推奨するベスト プラクティスの構成に基づいて自動的に生成されますが、必要に応じてフィールドを更新できます。

フィールド	説明
レプリケーションモード	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。**[マルチキャスト（Multicast）]** レプリケーションを選択すると、**[入力レプリケーション（Ingress Replication）]** 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。 IPv4 または IPv6 のテナント ルーテッド マルチキャスト（TRM）のレプリケーション モードとして **[マルチキャスト（Multicast）]** を選択します。 IPv4 の使用例の詳細については、このトピックを参照してください。 IPv6 の使用例の詳細については、「PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN EVPN ファブリックの構成」を参照してください。
マルチキャスト グループ サブネット	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。 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、モードを入力レプリケーションに変更することはできません。 古いマルチキャスト グループ プールは、既存のネットワーク（および TRM が有効になっている場合は VRF）によって参照され、使用されている場合は、スパインまたはリーフの自由形式に使用することをお勧めします。**[レプリケーション（Replication）] > [マルチキャスト グループ サブネット（Multicast Group Subnet）]** 設定で、新しいまたは更新されたマルチキャスト グループ プールを使用します。これにより、新しいすべてのネットワークに新しいマルチキャスト プールまたは更新されたマルチキャスト プールが使用されるようになります。

フィールド	説明
IPv6 マルチキャスト グループ サブネット	プレフィックス範囲が 112 ~ 126 の IPv6 マルチキャスト アドレスを入力します。
IPv4 テナント ルーテッド マルチキャスト（TRM）の有効化	VXLAN EVPN ファブリックで EVPN/MVPN を介してオーバーレイ IPv4 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 IPv4 を使用したテナント 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。
IPv6 テナント ルーテッド マルチキャスト（TRM）の有効化	VXLAN EVPN ファブリックで EVPN/MVPN を介してオーバーレイ IPv6 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 IPv6 を使用したテナント 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 IPv6 アドレス	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（Multicast Group Subnet ）]** 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、Configuring Tenant Routed Multicast の「Overview of Tenant Routed Multicast」の項を参照してください。
TRM VRF のデフォルト MDT IPv6 アドレス	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 **[IPv6 マルチキャスト グループ サブネット（IPv6 Multicast Group Subnet ）]** 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更新する場合、**[IPv6 マルチキャスト グループ サブネット（IPv6 Multicast Group Subnet）]** で指定した IP プレフィックスから選択された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、Configuring Tenant Routed Multicast の「Overview of Tenant Routed Multicast」の項を参照してください。
ランデブーポイント	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	レプリケーションでサポートされている 2 つのマルチモード、ASM（エニーソース マルチキャスト [ASM]）またはBiDir（双方向 PIM [BIDIR-PIM]）の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。  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 **[詳細（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	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。

フィールド	説明
アンダーレイ プライマリ RP ループバック ID（Underlay Primary RP Loopback ID）	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。 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）	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。 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	2 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。
アンダーレイ サード バックアップ RP ループバック ID	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。
MVPN VRI ID 範囲	NDFC 12.2.2 以降、vPC ごとに一意の MVPN VRI ID を割り当てるには、このフィールドを使用します。 このフィールドは、次の使用例で必要です。 • VLAN モードなしのレイヤ 3 VNI で VXLANv4 アンダーレイを設定し、TRMv4 または TRMv6 を有効にします。 • VXLANv6 アンダーレイを構成し、TRMv4 または TRMv6 を有効にします。 MVPN VRI ID は、マルチサイト ファブリック内でいずれかのサイト ID と同じにはできません。 VRI IDは 、MSD 内のすべてのサイト内で一意である 必要があります。
MVPN VRI ID の再割り当ての有効化	NDFC リリース 12.2.2 以降では、このチェックボックスを有効にして、ワンタイム VRI ID の再割り当てを生成します。NDFC は、該当する各スイッチに対して、上記の MVPN VRI ID 範囲内で新しい MVPN ID を自動的に割り当てます。これは 1 回限りの操作であるため、操作の実行後、このフィールドはオフになります。 VRI ID の変更は中断を伴うため、それに応じて計画してください。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な設定が完了したら **[保存（Save）]** をクリックします。

vPC

次の表では、[VPC] タブのフィールドについて説明します。ほとんどのフィールドは、シスコが推奨するベスト プラクティスの構成に基づいて自動的に生成されますが、必要に応じてフィールドを更新できます。

フィールド	説明
vPC ピア リンク 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 として設定（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	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 自動リカバリ時間（秒単位）	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（秒単位）	vPC 遅延復元期間を秒単位で指定します。
vPC 遅延復元時間（秒単位）	NDFC リリース 12.2.3 で追加された新しいフィールド。ToR スイッチの 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 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。この機能を無効にするには、チェックボックスをオフにします。
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。
すべての vPC ペアに対して同じ 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 ペアに対して同じ 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	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。

フィールド	説明
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。  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	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。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な構成が完了したら **[保存（Save）]** をクリックします。

プロトコル

[プロトコル（Protocols）] タブのフィールドについては、次の表で説明します。ほとんどのフィールドは、シスコが推奨するベスト プラクティスの構成に基づいて自動的に生成されますが、必要に応じてフィールドを更新できます。

フィールド	説明
ルーティング ループバック ID	loopback0 は通常ファブリック 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 と設定されます。
アンダーレイ VTEP ループバック 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 エニーキャスト ループバック ID	ループバック インターフェイス ID はグレー表示されています。VXLANv6 ファブリックの vPC ピアリングにのみ使用されます。
アンダーレイ ルーティング プロトコル タグ	ネットワークのタイプを定義するタグ。
OSPFエリアID	OSPF がファブリック内で IGP として使用されている場合の OSPF エリア ID。  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	OSPF 認証を有効にする場合、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	キー ID が入力されます。
OSPF 認証キー	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。  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。

フィールド	説明
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 ネットワーク ポイントツーポイントの有効化	番号付きのファブリック インターフェイスでネットワーク ポイントツーポイントを有効にします。
IS-IS 認証の有効化	IS-IS 認証を有効にする場合、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、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	CiscoisisAuth などのキーチェーン名を入力します。
IS-IS 認証キー ID	キー ID が入力されます。
IS-IS 認証キー	Cisco Type 7 暗号化キーを入力します。 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 オーバーロード ビットの設定（Set IS-IS Overload Bit）	有効にすると、リロード後の一定時間、オーバーロード ビットを設定します。
IS-IS オーバーロード ビット経過時間	経過時間（秒）の後にオーバーロード ビットをクリアできます。
BGPの有効化認証	BGP 認証を有効にする場合、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、[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。 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	暗号化タイプを選択します。 • 3DES 暗号化タイプの場合は 3 • Cisco 暗号化タイプ 6 の場合は 6（NDFC 12.2.3 以降でのみ使用可能） • Cisco 暗号化タイプ 7 の場合は7
BGP認証キー	暗号化タイプに基づいて暗号化キーを入力します。 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。

フィールド	説明
PIM Hello 認証の有効化	ファブリック内のスイッチのすべてのファブリック内インターフェイスで PIM hello 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。このチェックボックスは、マルチキャスト レプリケーション モードでのみ編集できます。このチェックボックスは、IPv4 アンダーレイに対してのみ有効です。
PIM Hello 認証キー	PIM hello 認証キーを指定します。詳細については、「PIM Hello 認証キーの取得」を参照してください。 PIM Hello 認証キーを取得するには、次の手順を実行します。 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)# **interface e1/32** switch(config-if)# **ip pim hello-authentication ah-md5 pimHelloPassword** この例では、**pimHelloPassword** が使用されたクリアテキスト パスワードです。 3. **show run interface** コマンドを入力して、PIM hello 認証キーを取得します。 switch(config-if)# **show run interface e1/32 | grep pim** ip pim sparse-mode ip pim hello-authentication ah-md5 3 d34e6c5abc7fecf1caa3b588b09078e0 この例では、**d34e6c5abc7fecf1caa3b588b09078e0** がファブリック設定で指定される PIM hello 認証キーです。
BFDの有効化	ファブリック内のすべてのスイッチで**機能 bfd** を有効にする場合に、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。 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：機能 bfd 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イメージについては、*Compatibility Matrix for Cisco* を参照してください。

フィールド	説明
iBGP の BFD の有効化（Enable BFD for iBGP）	チェックボックスをオンにすると、iBGP ネイバーの BFD が有効になります。このオプションは、デフォルトで無効です。
OSPF の BFD の有効化（Enable BFD for OSPF）	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 の BFD の有効化（Enable BFD for ISIS）	チェックボックスをオンにすると、ISIS 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 OSPF の場合はグレー表示されます。

PIM の BFD の有効化（Enable BFD for PIM）	チェックボックスをオンにすると、PIM 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、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 認証の有効化	BFD 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。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。 **[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	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 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。
iBGP ピアテンプレート構成	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。

フィールド	説明
	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 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。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な設定が完了したら [保存（Save）] をクリックします。

セキュリティ

[セキュリティ（Security）] タブは次のテーブルで説明されています。

フィールド	説明
セキュリティ グループの有効化	このチェックボックスをオンにして、IPv4 専用アンダーレイで **[CLI オーバーレイ モード（CLI Overlay Mode）]** を使用するセキュリティ グループを有効にします。セキュリティ グループの詳細については、「VXLAN EVPN ファブリックのセキュリティの構成」を参照してください。
セキュリティ グループ名プレフィックス	新しいセキュリティ グループを作成するときに使用するプレフィックスを指定します。

フィールド	説明
セキュリティグループタグ（SGT）ID 範囲（オプション）	必要に応じて、セキュリティ グループのタグ ID を指定します。
セキュリティ グループの事前プロビジョニング	非適用 VRF のセキュリティ グループ構成を生成するには、このチェックボックスをオンにします。
MACsec の有効化（Enable MACsec）	ファブリックで 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 構成は、ファブリック内リンクで MACsec が有効になるまで生成されません。**[再計算して展開（Recalculate and Deploy）]** 操作を実行して MACsec 構成を生成し、スイッチに構成を展開します。
[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。
MACsec プライマリ キー文字列	プライマリ DCI 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. 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。 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	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 キーの文字列	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。 **[QKD の有効化（Enable QKD）]** オプションを無効にした場合は、**[MACsec フォールバック キー文字列（MACsec Fallback Key String）]** オプション を 指定する 必要 があります。
MACsec フォールバック暗号化アルゴリズム	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。

フィールド	説明
DCI MACsec の有効化	DCI リンクで 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。 **[DCI MACsec の有効化（Enable DCI MACsec）]** オプションを有効にして、**[リンク MACsec 設定の使用（Use Link MACsec Setting）]** オプションを無効にすると、NDFCはファブリック設定を使用して、DCI リンクで MACsec を構成します。 量子鍵伝送（QKD）サーバを使用した MACsec の詳細については、「QKD を使用して、2 つのファブリックを MACsec と接続する」を参照してください。
QKD の有効化	暗号化用の量子キーを生成するために QKDサーバを有効にするには、このチェックボックスをオンにします。 **[QKD を有効にする（Enable QKD）]** オプションを有効にしないことにした場合、NDFC はキーを生成するための QKD サーバを使用する代わりに提供された事前共有キーを使用します。**[QKD の有効化（Enable QKD）]** オプションが無効の場合、QKD に対してすべてのフィールドがグレーになります。
DCI MACsec 暗号スイート	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。
DCI MACsecプライマリキー文字列	プライマリ DCI 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。 デフォルトのキー ライフタイムは無期限です。
DCI MACsec プライマリ暗号化アルゴリズム	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。

フィールド	説明
DCI MACsecフォールバック キー文字列	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。  **[QKD の有効化（Enable QKD）]** オプションが 選択されていない場合 、この パラメータ は必須です。
DCI MACsec フォールバック暗号化アルゴリズム	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。
QKD プロファイル名	暗号プロファイル名を指定します。 暗号化プロファイルの最大サイズは 63 です。
KMEサーバー IP	キー管理エンティティ（KME）サーバの IPv4アドレスを指定します。
KMEサーバ ポート番号	KME サーバが使用するポート番号を指定します。
トラストポイントラベル	認証タイプのトラストポイント ラベルを指定します。 最大サイズは 64 です。
証明書を無視する	着信証明書の検証をスキップするには、このチェックボックスをオンにします。
MACsec ステータスレポート タイマー	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。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な構成が完了したら **[保存（Save）]** をクリックします。

高度

次のテーブルに**[詳細（Advanced）]** タブのフィールドが説明されています。ほとんどのフィールドは、シスコが推奨するベスト プラクティスの構成に基づいて自動的に生成されますが、必要に応じてフィールドを更新できます。

フィールド	説明
VRF テンプレート（VRF Template）	VRF 作成のための VRF 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）	ネットワークVRF 作成のための VRF テンプレートを指定します。
VRF拡張テンプレート	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。
ネットワーク拡張テンプレート	ネットワークを他のファブリックに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。

フィールド	説明
オーバーレイ モード	config-profile または CLI を使用した VRF/ネットワーク構成です。デフォルトは config-profile です。詳細については、「オーバーレイ モード」を参照してください。
L3VNI（VLAN なし）の許可	NDFC リリース 12.2.2 以降では、ボックスをオンにして、VLAN 機能なしのレイヤ 3 VNI を有効にします。 詳細については、「VLAN なしのレイヤ 3 VNI」を参照してください。
L3VNI VLAN なしを有効にする	NDFC リリース 12.2.1 以降、VRF のデフォルト値を設定するボックスをオンにします。このファブリック レベル フィールドの設定は、**[VRF レベルで L3VNI w/o VLAN を有効にする（Enable L3VNI w/o VLAN）]** のデフォルト値です。 詳細については、以下を参照してください。 • VLAN なしの レイヤ 3 VNI • 「LAN 操作モードのセットアップのファブリック概要」について の「VRF の作成」の項
プライベート VLAN（PVLAN）の有効化	スパイン スイッチとスーパー スパイン スイッチを除くスイッチでプライベート VLAN（PVLAN）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、「LAN 動作モード設定のファブリックの概要」の「プライベート VLAN の作成」の項を参照してください。
PVLAN セカンダリ ネットワーク テンプレート	PVLAN セカンダリ ネットワークのテンプレートを選択します。デフォルトは **Pvlan_Secondary_Network** です。
サイト ID	このファブリックを MSD 内で移動する場合のファブリックの 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。
ファブリック内インターフェイス MTU	ファブリック内インターフェイスに 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 インターフェイスに MTU を指定します。この値は偶数にする必要があります。
デフォルトでのホスト インターフェイスのシャットダウン解除（Unshut Host Interfaces by Default）	デフォルトでホスト インターフェイスのシャットダウンを解除するには、このチェックボックスをオンにします。
電源モード	適切な電源モードを選択します。
CoPP プロファイル	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 ホールドダウン タイマー	NVE 送信元インターフェイス ホールドダウン時間を指定します。

フィールド	説明
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	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フォーマットを入力します。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。ネットワーク名の名前反感の詳細については、「LAN 動作モード設定用ファブリックの概要について」の「スタンドアロン ファブリック用におネットワークを作成する」の項を参照してください。構文は **[<string> | $$VLAN_ID$$] $$VNI$$ [<string>| $$VLAN_ID$$]** で、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。 次のリストで構文内の変数について説明します。 • **$$VNI$$**：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、Nexus Dashboard Fabric Controller 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、ネットワーク名の注意事項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は、Site_VNI12345_VLAN1234 です。 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 • 構成プロファイルベースのオーバーレイ
オーバーレイ ネットワーク インターフェイス アタッチメントのスキップ	ブラウンフィールドとホスト ポートの再同期の場合にオーバーレイ ネットワーク インターフェイスの接続をスキップするには、このチェックボックスをオンにします。
ブートストラップされたスイッチの CDP の有効化	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。

フィールド	説明
VXLAN OAM の有効化	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。チェックボックスをオフにすると、VXLAN OAM 機能が無効になります。 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。 Cisco 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。 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 を有効化（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。 • **[NX-API]** オプションが有効または無効になっている場合、EPL 機能にはわずかな動作の変更があります。詳細については、「NX-API 構成での EPL の動作」の項を参照してください。 • **[NX-API]** オプションを無効にすると、レイヤ 4 からレイヤ 7 サービス構成機能の動作が変更されます。詳細については、「レイヤ 4 ～ レイヤ 7 サービスの注意事項と制限事項」を参照してください。
NX-API HTTPS ポート番号	**[NX-APIの有効化（Enable NX-API）]** オプションが有効になっている場合、フィールドがアクティブになります。 NX-API HTTPS ポート番号を入力します。デフォルト値は 443 です。
HTTP ポートでの NX-API の有効化	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～L7 サービス）、VXLAN OAM など、NX-API を使用し、Cisco Nexus Dashboard Fabric Controller がサポートするアプリケーションは、HTTP ではなく HTTPS の使用を開始します。 **[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。

フィールド	説明
NX-API HTTP ポート番号	**[HTTP NX-APIの有効化（Enable NX-API）]** オプションが有効になっている場合、フィールドがアクティブになります。 NX-API HTTPS ポート番号を入力します。デフォルト値は 80 です。
L4-L7 サービス リダイレクトの有効化	L4 ~ L7 サービスの使用例に基づいて、スイッチで次の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。 • ポリシーベース リダイレクト（PBR） • 拡張ポリシーベース リダイレクト（ePBR） • サービス レベル コントラクト（SLA）
厳密な構成コンプライアンスの有効化	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。これにより、双方向のコンプライアンス チェックが有効になり、インテント/期待されている構成に存在せず、実行構成内で追加された構成には、フラグが付けられます。デフォルトでは、この機能は無効になっています。
AAA IP 認証の有効化	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 Nexus Dashboard Fabric Controller をサポートするために必要です。
トラップホストとしての NDFC の有効化（Enable NDFC as Trap Host）	SNMP トラップの宛先として Nexus ダッシュボード ファブリック コントローラを有効にするには、このチェックボックスをオンにします。通常、ネイティブHA Nexusダッシュボードファブリックコントローラの導入では、eth1 VIP IPアドレスがスイッチのSNMPトラップ宛先として設定されます。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。
ボーダー ゲートウェイ advertise-pip	エニーキャスト ボーダー ゲートウェイ PIP が VTEP としてアドバタイズされるようにします。MSD ファブリックの「構成の再計算」で有効です。
グリーンフィールドクリーンアップ オプション	Preserve-Config=No で Nexus Dashboard Fabric Controller にインポートされたスイッチで、スイッチ リロードなしでの、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。
高精度時間プロトコル（PTP）を有効化（Enable Precision Time Protocol（PTP））	ファブリック全体で PTP をイネーブルにします。このチェックボックスをチェックすると、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 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、「データ センター VXLAN EVPN ファブリックの高精度時間プロトコル」の「データ センター VXLAN EVPN ファブリックの高精度時間プロトコル」項を参照してください。

フィールド	説明
PTP 送信元ループバック ID（PTP Source Loopback Id）	すべての PTP パケットの送信元 IP アドレスとして使用されるループバック インターフェイス ID ループバックを指定します。有効な値の範囲は 0 ~ 1023 です。PTP ループバック ID を RP、ファントム RP、NVE、または MPLS ループバック ID と同じにすることはできません。そうでない場合は、エラーが生成されます。PTP ループバック ID は、BGP ループバックまたは Nexus ダッシュボード ファブリック コントローラから作成されたユーザー定義ループバックと同じにすることができます。 展開設定中に 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、「MPLS SR および LDP ハンドオフ」を参照してください。
アンダーレイ MPLS ループバック ID	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	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。
デフォルトのキューイング ポリシーの有効化	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。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 Nexus Dashboard Fabric Controller Web UI から、**[管理（Manage）] > [テンプレート（Templates）]** 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]**）。ファイルを選択します。**[アクション（Actions）]** ドロップダウンリストから、**[テンプレート コンテンツの編集（Edit template content）]** を選択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 シリーズ NX-OS Quality of Service 構成ガイド*』を参照してください。

フィールド	説明
N9K クラウド スケール プラットフォーム 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 プラットフォームのキューイング 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。
AI/MLQOS およびキューイング ポリシーを有効にする	NDFCリリース12.2.1 以降では、このボックスをオンにして、BGPファブリックで AI/ML QoS およびキューイング ポリシーを有効にします。詳細については、「AI/ML QoS 分類およびキューイング ポリシー」を参照してください。 このオプションは、次のいずれかのオプションも有効にした場合は使用できません。 • **[vPC]** タブの **[ファブリック vPC ピアリングの Qos の有効化（Enable Qos for Fabric vPC-Peering）]** オプション • **[詳細（Advanced）]** タブの **[デフォルト キューイング ポリシーの有効化（Enable Default Queuing Policies）]** オプション

フィールド	説明
AI/ML の QOS とキューイング ポリシー	このフィールドは、上記の **[AI/ML QOS およびキューイングポリシーの有効化（ Enable 人工知能/ML QOS and Queuing Policies）]** オプションをオンにした場合に使用できます。 NDFC リリース 12.2.1 以降では、ファブリック内の特定のスイッチの主要なファブリック リンク速度に基づいて、ドロップダウン リストからキューイング ポリシーを選択します。詳細については、「AI/ML QoS 分類 およびキューイング ポリシー」を参照してください。 オプションは、次のとおりです。 • **AI_Fabric_QOS_800G**：NDFC リリース 12.2.3 で追加された新しいフィールド。800 Gb のインターフェイス速度の QoS キューイング ポリシーを有効にします。 • **AI_Fabric_QOS_400G**：400 Gb のインターフェイス速度の QoS キューイング ポリシーを有効にします。 • **AI_Fabric_QOS_100G**：100 Gb のインターフェイス速度の QoS キューイング ポリシーを有効にします。 • **AI_Fabric_QOS_25G**：25 Gb のインターフェイス速度の QoS キューイング ポリシーを有効にします。
優先順位フロー制御ウォッチドッグ間隔	このフィールドは、上記の **[AI/ML QOS およびキューイングポリシーの有効化（ Enable 人工知能/ML QOS and Queuing Policies）]** オプションをオンにした場合に使用できます。NDFC リリース 12.2.2 以降では、AI/ML 機能を有効にすると、PFC が有効になっているすべての構成済みデバイス、ファブリック内リンク、およびすべてのホスト インターフェイスで priority-flow-control watchdog-interval on が有効になります。このリリースでは、**[Priority flow control watch-dog interval]** フィールドも追加されています。ここで、**[Priority flow control watch-dog interval]** フィールドをシステム以外のデフォルト値（デフォルトは 100 ミリ秒）に設定できます。有効な値は <101-1000> です。
リアルタイムのインターフェイス統計情報収集の有効化	リアルタイムのインターフェイス統計情報の収集を有効にするには、このチェックボックスをオンにします。
インターフェイス統計情報のロード間隔	インターフェイス統計負荷の間隔を秒単位で入力します（最小：5、最大：300）。
スパニング ツリー ルート ブリッジ プロトコル	ルート ブリッジを構成するためのプロトコルをドロップダウン リストから選択します。 使用可能なプロトコルは次のとおりです。 • **rpvst**：VLAN ごとの高速スパニング ツリー • **mst**：多重スパニング ツリー • **unmanaged**（デフォルト）：STP ルートは NDFC によって管理されていません。 レイヤ 2 ToR には mst プロトコルを使用することをお勧めします。

フィールド	説明
スパニングツリー VLAN 範囲（Spanning Tree VLAN Range）	VLAN 範囲を指定します。デフォルト値は 1 ~ 3967 です。
MST インスタンス範囲（MST Instance Range）	MST インスタンス範囲を指定します。デフォルト値は 0 です。
スパニング ツリー ブリッジ優先度（Spanning Tree Bridge Priority）	スパニング ツリーのブリッジ優先度を 4096 の倍数で指定します。
Leaf-ToR ペアリングでの許可 VLAN の設定	このフィールドは、NDFC リリース 12.2.3 で導入されました。leaf-ToR ペアリング ポート チャネルのトランク許可 VLAN を none または all に設定します。デフォルト値は none です。
 次のフィールドは NDFC リリース 12.2.2 の **[詳細（Advanced）]** タブで使用できますが、NDFC リリース 12.2.3 では [自由形式（Freeform）] タブに移動されます。	
リーフ フリーフォーム構成（Leaf Freeform Config）	**リーフ**、**境界**、および**境界ゲートウェイ**のロールを持つスイッチに追加する必要のある CLI を追加します。
スパイン自由形式構成	**スパイン**、**境界スパイン**、**境界ゲートウェイ スパイン**、および**スーパー スパイン** 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構成	ファブリック内リンクに追加する必要がある CLI を追加します。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な設定が完了したら **[保存（Save）]** をクリックします。

自由形式

このフィールドは、NDFC リリース 12.2.3 で導入されました。

このタブのフィールドは次のとおりです。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。

フィールド	説明
リーフインターフェイス前の自由形式構成	[実行コンフィギュレーションの表示（Show Running Configuration）] からキャプチャされたすべてのリーフ スイッチに対して、インターフェイス構成の前に追加の CLI を入力します。
スパイン自由形式構成	[実行コンフィギュレーションの表示（Show Running Configuration）] からキャプチャされたすべてのスパイン スイッチに対して、インターフェイス構成の前に追加の CLI を入力します。
ToR インターフェイス前の自由形式構成	[実行コンフィギュレーションの表示（Show Running Configuration）] からキャプチャされたすべての ToR に対して、インターフェイス構成の前に追加された追加の CLI を入力します。

フィールド	説明
リーフ自由形式構成	[実行中の構成の表示（Show Running Configuration）] からキャプチャされたすべてのリーフ スイッチおよび階層 2 リーフ スイッチに対して、インターフェイス構成後に追加された追加の CLI を入力します。
スパインのインターフェイス後の自由形式構成	[実行コンフィギュレーションの表示（Show Running Configuration）] からキャプチャされたすべてのスパイン スイッチに対して、インターフェイス構成後に追加の CLI を入力します。
ToR インターフェイス後の自由形式構成	[実行コンフィギュレーションの表示（Show Running Configuration）] からキャプチャされたすべての ToR に対して、インターフェイス構成の後に追加の CLI を入力します。
ファブリック内リンクの追加構成	ファブリック内リンクに追加する CLI を追加します。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な設定が完了したら **[保存（Save）]** をクリックします。

関連資料

[リソース（Resources）] タブのフィールドについては、次の表で説明します。ほとんどのフィールドは、シスコが推奨するベスト プラクティスの構成に基づいて自動的に生成されますが、必要に応じてフィールドを更新できます。

ループバック IP 範囲フィールドのファブリック設定を編集した後、サブネット範囲を拡張することでループバック IP アドレス範囲を拡張できますが、ループバック IP アドレス範囲を完全に変更することはできません。この制限は、**[リソース（Resources）]** タブのこれらのフィールドに適用されます。

- **アンダーレイ ルーティング ループバック IP 範囲**
- **アンダーレイ VTEP ループバック IP 範囲**
- **アンダーレイ RP ループバック IP 範囲**
- **アンダーレイ サブネット IP 範囲**

フィールド	説明
アンダーレイ IP アドレスの手動割り当て（Manual Underlay IP Address Allocation）	VXLAN ファブリック管理を Nexus Dashboard Fabric Controller に移行する場合は、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、Nexus Dashboard Fabric Controller. 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。 • 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	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	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	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	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。
アンダーレイ MPLS ループバック IP 範囲	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。
アンダーレイルーティングループバック IPv6 範囲	Loopback0 の IPv6 アドレス範囲を指定します。
アンダーレイ VTEP ループバック IPv6 範囲	Loopback1 およびエニーキャスト ループバックの IPv6 アドレス範囲を指定します。
アンダーレイサブネット IPv6範囲（Underlay Subnet IPv6 Range）	番号付きおよびピアリンク SVI IP を割り当てる IPv6 アドレス範囲を指定します。
IPv6 アンダーレイの BGP ルータ ID 範囲（BGP Router ID Range for IPv6 Underlay）	IPv6 アンダーレイの BGP ルータ ID 範囲を指定します。
レイヤ2 VXLAN VNI範囲	ファブリックのオーバーレイ VXLAN VNI 範囲を指定します（最小：1、最大：16777214）。

フィールド	説明
レイヤ3 VXLAN VNI範囲	ファブリックのオーバーレイ VRF VNI 範囲を指定します（最小：1、最大：16777214）。
ネットワーク VLAN 範囲（Network VLAN Range）	スイッチごとのオーバーレイ ネットワークの VLAN 範囲（最小：2、最大：4094）。
VRF VLAN 範囲（VRF VLAN Range）	スイッチごとのオーバーレイ レイヤ 3 VRF の VLAN 範囲（最小：2、最大：4094）。
サブインターフェイス Dot1q 範囲	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	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。Back2Back＆ToExternal を選択すると、VRF Lite IFC が自動作成されます。
ピアの自動展開	このチェックボックスは、VRF Lite 展開で利用できます。このチェックボックスをオンにすると、自動作成された VRF Lite IFC では、**[VRF Lite]** タブセットの **[ピアの構成自動生成（Auto Generate Configuration for Peer）]** フィールドが設定されます。 VRF Lite IFC 設定にアクセスするには、**[リンク（Links）]** タブに移動し、特定のリンクを選択してから、**[アクション（Actions）] > [編集（Edit）]** を選択します。 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。この構成は、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。自動作成された IFC を編集し、**[ピアの構成を自動生成（Auto Generate Configuration for Peer）]** をオンまたはオフにすることができます。この設定は常に優先されます。
Auto Deploy デフォルト VRF	このチェックボックスをオンにすると、自動作成された VRF Lite IFC に対して **[デフォルト VRF での構成自動生成（Auto Generate Configuration on default VRF）]** フィールドが自動的に有効になります。 このチェックボックスは、**[VRF Lite の展開（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。**[デフォルト VRF での構成の自動生成（Auto Generate Configuration on default VRF）]** フィールドを設定すると、ボーダー デバイスの物理インターフェイスが自動的に構成され、ボーダー デバイスとエッジ デバイスまたは別の VXLAN EVPN ファブリック内の別のボーダー デバイスとの間に EBGP 接続が確立されます。

フィールド	説明
ピアの Auto Deploy デフォルト VRF	このチェックボックスをオンにすると、**[デフォルト VRF での NX-OS ピアの構成の自動生成（Auto Generate Configuration for NX-OS Peer on default VRF）]** フィールドが、自動作成された VRF Lite IFC に対して自動的に有効になります。このチェックボックスは、**[VRF Lite の展開（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。**[デフォルト VRF の NX-OS ピアの構成自動生成（Auto Generate Configuration for NX-OS Peer on default VRF）]** フィールドを設定すると、ピア NX-OS スイッチの物理インターフェイスと EBGP コマンドが自動的に構成されます。 IFC リンクの **[デフォルト VRF での構成自動生成（Auto Generate Configuration on default VRF）]** および **[デフォルト VRF での NX-OS ピアの構成自動生成（Auto Generate Configuration for NX-OS Peer on default VRF）]** フィールドにアクセスするには、[リンク（Links）] タブに移動し、特定のリンクを選択し、**[アクション（Actions）] > [編集（Edit）]** を選択します。
BGP ルートマップ名の再配布	デフォルト VRF で BGP ルートを再配布するためのルート マップを定義します。
VRF Lite サブネット IP 範囲	これらのフィールドには、DCI サブネットの詳細が事前に入力されています。必要に応じて、次のフィールドを更新します。 ページ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、各ファブリックが独自の範囲を持ち、アンダーレイ範囲と重複しないようにしてください。これにより、重複のリスクを回避できます。一度に更新できる値の範囲は 1 つだけです。
VRF Lite サブネット マスク	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、レイヤ 2 およびレイヤ 3 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、**[保存（Save）]** をクリックして
サービス ネットワーク VLAN 範囲	[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。
VRF Lite IFC を介した VRF 拡張での一意の IP の自動割り当て（Auto Allocation of Unique IP on VRF Extension over VRF Lite IFC)	VRF Lite IFC を介した VRF 拡張の送信元および接続インターフェイスのサブネットを持つ一意の IPv4 アドレスを自動的に割り当てます。 有効にすると、システムは、VRF 接続の拡張ごとに、送信元インターフェイスと接続先インターフェイスの一意の IP アドレスを自動的に入力します。この機能を無効にすると、システムは VRF 拡張の送信元インターフェイスと接続先インターフェイスに同じ IP アドレスを自動的に入力します。これらの IP アドレスは VRF が接続されたリソース マネージャに割り当てられます。リソース マネージャは、これらが 同じ VRF で他の目的に使用されないようにします。

フィールド	説明
Per VRF Per VTEP Loopback IPv4 Auto-Provisioning	システムが VRF 接続に使用する VTEP のループバック アドレスを IPv4 形式で自動プロビジョニングします。 このオプションは、デフォルトで無効になっています。有効にすると、システムは、VTEP ループバック インターフェイスに割り当てた IP プールから IPv4 アドレスを割り当てます。 1. **[Per VRF Per VTEP Loopback IPv4 Auto-Provisioning]** または **[Per VRF Per VTEP Loopback IPv6 Auto-Provisioning]** オプションを有効にします。 2. ファブリック設定を保存します。 3. **[再計算と展開（Recalculate and Deploy）]** 操作を実行します。 4. **[VRF アタッチメント（VRF Attachments）]** に移動します。 5. 特定の VRF がすでに接続されている場合は、**[アクション（Actions）] > [クイック接続（Quick Attach）]** をクリックします。これにより、VRF に新しいループバックが生成されます。 VRF 拡張がすでに有効になっており、たとえばボーダー デバイスの VRF Lite が構成されている場合は、ファブリック設定を有効にする前に、それぞれの VRF 接続とボーダー デバイスにアクセスして、VRF 拡張を再度接続する必要があります。たとえば、VRF Corp は Border-1 に接続され、VRF Lite を使用して外部ドメインに拡張されます。この場合、**[クイック アタッチ（Quick Attach）]** を実行し、VRF で新しいループバックをプロビジョニングすると、元の VRF-Lite 拡張が切り離されます。その後、VRF アタッチメントを選択し、VRF-Lite 拡張機能を編集して再接続してから、関連するすべての構成を展開できます。
ループバックの VRF ごと、VTEP IPv4 ごとの IP プール	各 VRF の VTEP のループバック インターフェイスに割り当てられる IPv4 アドレスのプール。
VRF ごと、VTEP ごとのループバック IPv6 自動プロビジョニング	システムが VRF 接続に使用する VTEP のループバック アドレスを IPv6 形式で自動プロビジョニングします。 このオプションは、デフォルトで無効になっています。有効にすると、システムは、VTEP ループバック インターフェイスに割り当てた IP プールから IPv6 アドレスを割り当てます。
ループバックの VRF ごと、VTEP ごとの IP プール	各 VRF の VTEP のループバック インターフェイスに割り当てられる IPv6 アドレスのプール。
サービス レベル コントラクト（SLA）ID 範囲	スイッチごとの SLA ID 範囲（最小：1、最大：2147483647）。
追跡対象オブジェクト ID 範囲	スイッチごとのトラッキング対象オブジェクト ID 範囲（最小：1、最大：512）。
サービス ネットワーク VLAN 範囲	スイッチごと、オーバーレイ サービス ネットワーク VLAN 範囲（最小：2、最大：4094）。

フィールド	説明
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 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。
特定の vPC/ポート チャネル識別子範囲の活用	リーフ-ToRスイッチペアリングの vPC 識別子のカスタム範囲を指定します。最小許容値は 1、最大許容値は 4099 です。
vPC/ポート チャネル識別子範囲	リーフ ToR スイッチ ペアリングの vPC 識別子を自動割り当てするためのカスタム vPC 識別子範囲を指定します。最小許容値は 1、最大許容値は 4099 です。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な構成が完了したら **[保存（Save）]** をクリックします。

管理性

次の表では、**[管理性（Manageability）]** タブのフィールドについて説明します。ほとんどのフィールドは、シスコが推奨するベスト プラクティスの構成に基づいて自動的に生成されますが、必要に応じてフィールドを更新できます。

フィールド	説明
インバンド管理	これを有効にすると、フロント パネル インターフェイスを介してスイッチを管理できます。アンダーレイ ルーティング ループバック インターフェイスは、検出に使用されます。有効にすると、アウトオブバンド（OOB）mgmt0 インターフェイスを介してスイッチをファブリックに追加することはできなくなります。インバンド管理を通じて easy ファブリックを管理するには、NDFC Web UI で **[データ（Data）]** を選択し、**[管理（Admin）] > [システム設定（System Settings）] > [サーバ設定（Server Settings）] > [管理（Admin）]** を選択していることを確認します。この設定では、インバンド管理とアウトオブバンド接続（mgmt0）の両方がサポートされます。詳細については、「インバンド管理、インバンド POAP 管理、セキュア POAP の構成」の「Easy ファブリックのインバンド管理およびインバンド POAP」の項を参照してください。
DNS サーバー IP（DNS Server IPs）	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 サーバー VRF（DNS Server VRFs）	すべての DNS サーバに 1 つの VRF を指定するか、DNS サーバーごとに 1 つの VRF を指定します。
NTP サーバ IP	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 を指定します。
Syslog サーバー IP（Syslog Server IPs）	syslog サーバーの 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 サーバーの重要度（Syslog Server Severity）	syslog サーバーごとに 1 つの syslog 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。

フィールド	説明
Syslog サーバー VRF（Syslog Server VRFs）	すべての syslog サーバーに 1 つの VRF を指定するか、syslog サーバーごとに 1 つの VRF を指定します。
AAA フリーフォーム構成（AAA Freeform Config）	AAA フリーフォーム構成を指定します。 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 **AAAConfigurations** である **switch_freeform** PTI が作成されます。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な設定が完了したら **[保存（Save）]** をクリックします。

ブートストラップ

次の表では、**[ブートストラップ（Bootstrap）]** タブのフィールドについて説明します。ほとんどのフィールドは、シスコが推奨するベスト プラクティスの構成に基づいて自動的に生成されますが、必要に応じてフィールドを更新できます。

フィールド	説明
ブートストラップの有効化	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。 Cisco NDFC リリース 12.1.1e 以降、スイッチを追加し、POAP 機能を使用するには、**[ブートストラップを有効にする（Enable Bootstrap）]** および **[ローカル DHCP サーバーを有効にする（Enable Local DHCP Server）]** チェックボックスをオンにします。詳細については、「インバンド管理、インバンド POAP 管理、セキュア POAP の構成」の「Easy ファブリックのインバンド管理およびインバンド POAP」の項を参照してください。 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：**[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]** および **[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** フィールドに外部 DHCP サーバーに関する情報を入力します。 • [ローカル DHCP サーバー（Local DHCP Server）]：**[ローカル DHCP サーバー（Local DHCP Server）]** チェックボックスをオンにして、残りの必須フィールドに詳細を入力します。
ローカル DHCP サーバーの有効化	ローカル DHCP サーバを介した自動 IP アドレス割り当ての有効化を開始するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、**[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、Nexus ダッシュボード ファブリック コントローラは自動 IP アドレス割り当てにリモートまたは外部DHCPサーバを使用します。

フィールド	説明
DHCP バージョン	このドロップダウンリストから [DHCPv4] または [DHCPv6] を選択します。[DHCPv4] を選択すると、**[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]** フィールドは無効になります。DHCPv6 を選択すると、**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** は無効になります。 Cisco Nexus 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）と DHCP スコープ終了アドレス（DHCP Scope End Address）	スイッチ 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	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	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：*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	スイッチの Mgmt0 インターフェイスの IPv6 プレフィックスを指定します。プレフィックスは 112 ～ 126 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。
DHCPv4/DHCPv6 マルチサブネット スコープ	1 行に 1 つのサブネット範囲を入力して、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すると、このフィールドは編集可能になります。 スコープの形式は次の順で定義する必要があります。 **[DHCP スコープ開始アドレス、DHCP スコープ終了アドレス、スイッチ管理デフォルト ゲートウェイ、スイッチ管理サブネット プレフィックス（DHCP Scope Start Address, DHCP Scope End Address, Switch Management Default Gateway, Switch Management Subnet Prefix）]** 例：10.6.0.2、10.6.0.9、16.0.0.1、24

フィールド	説明
ブートストラップ フリーフォーム 構成	（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 フリーフォームの設定（Bootstrap Freeform Config）]** フィールドで定義された設定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、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。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な設定が完了したら［保存（Save）］をクリックします。

コンフィギュレーションのバックアップ

次の表では、**[構成バックアップ（Configuration Backup）]** タブのフィールドについて説明します。ほとんどのフィールドは、シスコが推奨するベスト プラクティスの構成に基づいて自動的に生成されますが、必要に応じてフィールドを更新できます。

フィールド	説明
毎時ファブリック バックアップ	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。
スケジュール済みバックアップ	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。
予定時刻	スケジュールされたバックアップ時間を 24 時間フォーマットで指定します。**[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。 NDFC で保持されるファブリック バックアップの数は、**[管理（Admin）] > [システム設定（System Settings）] > [サーバ設定（Server Settings）] > [LAN ファブリック（LAN Fabric）] > [ファブリックごとの最大バックアップ数（Maximum Backups per Fabric）]** で決定されます。保持できるアーカイブ ファイルの数は、**[サーバのプロパティ（Server Properties）]** ウィンドウの **[デバイスごとに保持されるアーカイブ ファイル数（# Number of archived files per device to be retained）：]** フィールドに表示されます。

フィールド	説明
	 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。 1. **[概要（Overview）] > [トポロジ（Topology）]** を選択します。 2. 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。 3. ファブリック内のスイッチを右クリックし、**[構成のプレビュー（Preview Config）]** を選択します。 4. このファブリックの **[構成のプレビュー（Preview Config）]** ウィンドウで、**[すべて再同期（Re-Sync All）]** 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。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な設定が完了したら **[保存（Save）]** をクリックします。

Flow Monitor

次の表では、**[フローモニター（Flow Monitor）]** タブのフィールドについて説明します。ほとんどのフィールドは、シスコが推奨するベスト プラクティスの構成に基づいて自動的に生成されますが、必要に応じてフィールドを更新できます。

フィールド	説明
NetFlow を有効にする	このチェック ボックスをオンにして、このファブリックの VTEP で Netflow を有効にします。デフォルトでは、Netflow は無効になっています。有効にすると、NetFlow 設定は、NetFlow をサポートするすべての VTEPS に適用されます。  ファブリックで Netflow が有効になっている場合、ダミーの no_netflow PTI を使用して、特定のスイッチで Netflow を使用しないように選択することができます。 netflow がファブリック レベルで有効になっていない場合、インターフェイス、ネットワーク、または vrf レベルで netflow を有効にすると、エラー メッセージが生成されます。Cisco NDFC の NetFlow サポートの詳細については、Understanding LAN Fabrics の「Netflow Support」の項を参照してください。

[ネットフロー エクスポータ（Netflow Exporter）] エリアで、**[アクション（Actions）] > [追加（Add）]** の順にクリックして、1 つ以上の Netflow エクスポータを追加します。このエクスポータは、NetFlow データの受信側です。このページのフィールドは次のとおりです。

- **[エクスポータ名（Exporter Name）] -** エクスポータの名前を指定します。
- **[IP]**：エクスポータの IP アドレスを指定します。

- **[VRF]**：エクスポータがルーティングされる VRF を指定します。
- **[送信元インターフェイス（Source Interface）]**：送信元インターフェイス名を指定します。
- **[UDP ポート（UDP Port）]**：Netflow データがエクスポートされる UDP ポートを指定します。

[保存（Save）] をクリックしてエクスポータを構成します。破棄するには **[キャンセル（Cancel）]** をクリックします。既存のエクスポータを選択し、**[アクション（Actions）] > [編集（Edit）]** または **[アクション（Actions）] > [削除（Delete）]** を選択して、関連するアクションを実行することもできます。

[ネットフロー レコード（Netflow Exporter）] エリアで、**[アクション（Actions）]** > **[追加（Add）]** の順にクリックして、1 つ以上のネットフロー レコードを追加します。この画面のフィールドは次のとおりです。

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

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

[Netflow モニター（Netflow Monitor）] 領域で、**[アクション（Actions）] > [追加（Add）]** の順にクリックして、1 つ以上の Netflow モニターを追加します。このページのフィールドは次のとおりです。

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

各 netflow モニタで参照されるレコード名とエクスポータは、「**Netflow レコード（Netflow Record）**」と「**Netflow エクスポータ（Netflow Exporter）**」で定義する必要があります。

[保存（Save）] をクリックして、モニターを構成します。破棄するには **[キャンセル（Cancel）]** をクリックします。既存のモニタを選択し、**[アクション（Actions）] > [編集（Edit）]** または **[アクション（Actions）] > [削除（Delete）]** を選択して、関連するアクションを実行することもできます。

次の作業：必要に応じて別のタブで構成を完了するか、このファブリックに必要な設定が完了したら **[保存（Save）]** をクリックします。

VLAN なしの レイヤ 3 VNI

NDFC リリース 12.2.1 以降、VLAN 機能のないレイヤ 3 VNI が Nexus Dashboard ファブリック コントローラでサポートされるようになりました。この機能により、レイヤ 3 VNI 構成では、VRF ごとの VLAN は必要なくなりました。

以下は、ファブリックで VLAN なしのレイヤ 3 VNI 機能を有効にするための上位レベルのプロセスです。

1. （オプション）新しいファブリックを構成する場合は、[**L3VNI を有効にする（Enable L3VNI w/o VLAN）**] フィールドをオンにして、ファブリック レベルで VLAN なしのレイヤ 3 VNI 機能を有効にします。このファブリック レベルのフィールドの設定は、以下で説明するように、VRF レベルの関連フィールドに影響します。
2. VRF を作成または編集するときに、**[VLAN なしで L3VNI を有効にする（Enable L3VNI w/o VLAN）]** フィールドをオンにして、VRF レベルで VLAN なしのレイヤ 3 VNI 機能を有効にします。このフィールドのデフォルト設定は、以下の要素に基づいて決まります。
    - 既存の VRF の場合、デフォルト設定は無効になっています（**[VLAN なしで L3VNI を有効にする（Enable L3VNI w/o VLAN）]** ボックスはオフになっています）。
    - 新しく作成された VRF の場合、上記のように、デフォルト設定はファブリック設定から継承されます。
    - このフィールドは、VXLAN ファブリックごとの変数です。VXLAN EVPN マルチサイト ファブリックから作成された VRF の場合、このフィールドの値は子ファブリックのファブリック設定から継承されます。必要に応じて、子ファブリックの VRF を編集して値を変更できます。

      詳細については、「LAN 動作モード設定のファブリックの概要について」の「VRF の作成」セクションを参照してください。

次の条件が満たされた場合、VRF アタッチメント（新規または編集済み）は、VLAN モードなしの新しいレイヤ 3 VNI を使用します。

- **VLAN なしの L3VNI を有効にする**機能は VRF レベルで有効になっています。
- スイッチはこの機能をサポートしており、スイッチは正しいリリースで実行されています（注意事項と制限事項：VLANなしのレイヤ3 VNIを参照）。

これらの条件が満たされると、VRF アタッチメントでは VLAN は無視されます。

注意事項と制限事項：VLAN なしのレイヤー 3 VNI

VLAN 機能のないレイヤー 3 の注意事項と制限事項は次のとおりです。

- VLAN なしのレイヤ 3 VNI 機能は、Nexus 9000 スイッチの -EX、-FX、および -GX バージョンでサポートされています。この機能を VRF レベルで有効にすると、この機能をサポートしていないスイッチモデルでは VRF の機能設定は無視されます。
- Campus VXLAN EVPN ファブリックで使用する場合、この機能はそのタイプのファブリック内の Cisco Nexus 9000 シリーズ スイッチでのみサポートされます。この機能は、Campus VXLAN EVPN ファブリック内の Cisco Catalyst 9000 シリーズ スイッチではサポートされていません。これらのスイッチでは、レイヤ 3 VNI 構成に VLAN が必要です。
- この機能は、NXOS リリース 10.3.1 以降で動作するスイッチでサポートされます。この機能を VRF レベルで有効にすると、10.3.1 より前の NX-OS イメージを実行しているスイッチでは VRF の機能設定は無視されます。

- データセンター VXLAN EVPN ファブリックでブラウンフィールド インポートを実行するときに、1 つのスイッチ構成が VRF レベルで **VLAN なしの L3VNI を有効にする**構成になっている場合、スイッチモデルとイメージがこの機能をサポートしていれば、この VRF に関連付けられている同じファブリック内の残りのスイッチにも同じ設定を構成する必要があります。
- 以前のリリースから NDFC 12.2.1 にアップグレードする場合、すでに構成されている VRF とファブリックは、VLAN 機能なしのレイヤ 3 VNI が無効になっている（**[VLAN なしの L3VNI を有効にする（Enable L3VNI w/o VLAN）]** ボックスがオフになっている）既存の 12.2.1 より前の設定を保持します。NDFC リリース 12.2.1 に完全にアップグレードしたら、必要に応じてこれらの設定を手動で変更して、VLAN 機能なしのレイヤ 3 VNI を有効にすることができます。

AI/ML QoS 分類およびキューイング ポリシー

ここでは、NDFC リリース12.2.1 で導入された AI/ML QoS 分類およびキューイング ポリシー機能について説明します。

- AI/ML QoS 分類およびキューイング ポリシーについて
- 注意事項と制限事項：AI/ML QoS 分類およびキューイング ポリシー
- AI/ML QoS 分類およびキューイング ポリシーの構成
- カスタム QoS テンプレートを使用したポリシーの作成

AI/ML QoS 分類およびキューイング ポリシーについて

NDFC リリース 12.2.1 以降では、人工知能（AI）および機械学習（ML）トラフィックに使用できる低遅延、高スループット、およびロスレス ファブリック構成の構成がサポートされています。

この機能によって次のことが可能になります。

- ほとんどまたはすべてのリンクが 400Gb、100Gb、または 25Gb の速度で動作する、同種のインターフェイス速度のネットワークを簡単に構成できます。
- ホスト インターフェイスの優先キューイング ポリシーを上書きするカスタマイズを提供します。

AI/ML QoS ポリシーを適用すると、NDFC はQoS およびシステム キューイング ポリシーを使用してファブリック間リンクを自動的に事前構成し、優先順位フロー制御（PFC）も有効にします。VXLAN EVPN ファブリックで AI/ML　QoS 機能を有効にすると、ネットワーク仮想（NVE）インターフェイスに AI/ML QoS ポリシーが接続されます。

この機能を有効にするには、次の領域を活用します。

- BGP ファブリックを設定する場合、機能を有効にし、インターフェイス速度に基づいてキューイング ポリシー パラメータを設定するための新しいフィールドを使用できます。詳細については、「詳細情報」のセクションを参照してください。
- 次の AI/ML 固有のスイッチ テンプレートを使用して、ホスト インターフェイスで使用できるカスタム デバイス ポリシーを作成することもできます。
  - **AI_Fabric_QOS_Classification_Custom**：カスタム キューイングポリシーをインターフェイスに適用するために使用できるインターフェイス テンプレート。
  - **AI_Fabric_QOS_Queuing_Custom**：ユーザー定義のキューイング ポリシー構成に使用できるスイッチ テンプレート。

    これらのカスタム分類およびキューイング テンプレートで定義されたポリシーは、さまざまなホスト インターフェイス ポリシーで使用できます。詳細については、「カスタム QoS テンプレートを使用したポリシーの作成」を参照してください。

NDFC リリース 12.2.2 以降では、AI/ML 機能を有効にすると、プライオリティ フロー制御（PFC）が有効になっているすべての構成済みデバイス、ファブリック内リンク、およびすべてのホスト インターフェイスで priority-flow-control watchdog-interval on が有効になります。PFC ウォッチドッグ間隔は、no-drop キュー内のパケットが指定された時間内にドレインされているかどうかを検出するためのものです。このリリースでは、**[詳細（Advanced）]** タブ に **[優先フロー制御ウォッチドッグ間隔（Priority flow control watch-dog interval）]** フィールドも追加されています。Data Center VXLAN EVPN ファブリックまたはその他のファブリックを作成または編集し、AI/ML が有効になっている場合、**[優先フロー制御ウォッチドッグ間隔（ Priority flow control watch-dog interval ）]** フィールドをシステム以外のデフォルト値

（デフォルトは 100 ミリ秒）に設定できます。Cisco NX-OS の PFC ウォッチドッグ間隔の詳細については、『 *Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide*』の 「 Configuring a Priority Flow Control Watchdog Interval」を参照してください。

以前のリリースからアップグレードを実行し、**[再計算と展開（Recalculate and Deploy）]** を実行すると、構成に追加の **priority-flow-control watchdog-interval** が表示される場合があります。

注意事項と制限事項：AI/ML QoS 分類およびキューイング ポリシー

次に、AI/ML QoS およびキューイング ポリシー機能の注意事項と制限事項を示します。

- この機能は、インターフェイスごとの速度設定を自動化するしません。
- この機能は、Cisco Nexus 9300-FX2、9300-FX3、9300-GX、および 9300-GX2 シリーズ スイッチなど、Cisco Cloud スケール テクノロジーを使用した Nexus デバイスでのみサポートされます。
- この機能は、ToR ロールが割り当てられているデバイスを含むファブリックではサポートされていません。

AI/ML QoS 分類およびキューイング ポリシーの構成

AI/ML QoS およびキューイング ポリシーを構成するには、次の手順を実行します。

1. ファブリック レベルで AI/ML QoS およびキューイング ポリシーを有効にします。

   a. 通常どおりにファブリックを作成します。

   b. これらの指示の [詳細（Advanced）] タブで、ファブリック レベルで AI/ML QoS およびキューイング ポリシーを構成するために必要な選択を行います。

   c. 残りのタブで、必要に応じて残りのファブリック レベルの設定を行います。

   d. 必要なファブリック レベルの構成がすべて完了したら、**[保存（Save）]** をクリックし、**[再計算と展開（Recalculate and Deploy）]** をクリックします。

      プロセスのこの時点で、ネットワーク QoS およびキューイング ポリシーが各デバイスで構成され、分類ポリシーが NVE インターフェイス（該当する場合）で構成され、優先順位フロー制御および分類ポリシーがすべてのファブリック内リンク インターフェイスで構成されます。

2. ホスト インターフェイスの場合は、そのホスト インターフェイスに関連付けられたポリシーを編集して、優先順位フロー制御、QoS 、およびキューイングを選択的に有効にします。

   詳細については、「LAN 動作モードのインターフェイスの追加 」を参照してください。

   a. 前のステップで AI/ML QoS およびキューイング ポリシーを有効にしたファブリック内で、**[インターフェイス（Interfaces）]** タブをクリックします。

      このファブリック内の構成済みインターフェイスが表示されます。

   b. AI/ML QoS およびキューイング ポリシーを有効にするホスト インターフェイスを見つけ、そのホスト インターフェイスの横にあるボックスをクリックして選択し、**[アクション（Actions）] > [編集（Edit）]** の順にクリックします。

      [インターフェイスの編集（Edit Interfaces）] ページが表示されます。

c. **[ポリシー（Policy）]** フィールドで、このインターフェイスに関連付けられているポリシーに、このホスト インターフェイスで AI/ML QoS およびキューイング ポリシーを有効にするために必要なフィールドが含まれていることを確認します。

   たとえば、次のポリシー テンプレートには、必要な AI/ML QoS およびキューイング ポリシー フィールドが含まれています。

   - int_access_host
   - int_dot1q_tunnel_host
   - int_pvlan_host
   - int_routed_host
   - int_trunk_host

d. **[優先順位フロー制御の有効化（ Enable 優先順位 フロー control ）]** フィールドを見つけ、このフィールドの横にあるボックスをクリックして、このホスト インターフェイスの優先順位フロー制御を有効にします。

e. **[QoS 構成の有効化（Enable QoS Configuration）]** フィールドで、このフィールドの横にあるボックスをクリックして、このホスト インターフェイスの AI/ML QoS を有効にします。

   これにより、AI/ML キューイングがファブリック レベルで有効になっている場合、このインターフェイスで QoS 分類が有効になります。

f. 前のステップで **[QoS 構成の有効化（ Enable QoS Configuration）]** フィールドの横にあるボックスをオンにし、「カスタムQoS テンプレートを 使用したポリシーの作成」に記載されているステップを使用してカスタム QoS ポリシーを作成した場合は、必要に応じて、**[このインターフェイスのカスタム QoS ポリシー（Custom QoS Policy for this interface）]** フィールドにカスタム QoS 分類ポリシーを入力し、このホスト インターフェイスにカスタム QoS ポリシーを関連付けます。

   このフィールドを空白のままにすると、NDFC はデフォルトの QOS_CLASSIFICATIONポリシーを使用します（ 使用可能な場合）。

g. 「カスタム QoS テンプレートを使用したポリシーの作成」の手順を使用してカスタム キューイング ポリシーを作成した場合は、必要に応じて、**[このインターフェイスのカスタム キューイング ポリシー（Custom Queuing Policy for this interface）]** フィールドにそのカスタム キューイング ポリシーを入力して、そのカスタム キューイング ポリシーをこのホスト インターフェイスに関連付けます。

h. このホスト インターフェイスの AI/ML QoS およびキューイング ポリシーの構成が完了したら、**[保存（Save）]** をクリックします。

カスタム QoS テンプレートを使用したポリシーの作成

必要に応じて、次の手順に従ってカスタム QoS テンプレートを使用してポリシーを作成します。テンプレート の一般的な情報については、「テンプレート」を参照してください。

1. AI/ML QoS およびキューイング ポリシーを有効にしたファブリック内で、**[スイッチ（Switches）]** をクリックし、AI/ML QoS およびキューイング ポリシーを有効にしたホスト インターフェイスがあるスイッチをダブルクリックします。

   そのスイッチの **[スイッチの概要（Switch Overview）]** ページが表示されます。

2. **[ポリシー（Policies）]** タブをクリックします。

3. **[アクション（Actions）] > [ポリシーの追加（Add Policy）]** をクリックします。

   [ポリシーの作成（Create Policy）] ページが表示されます。

4. 優先順位を設定し、新しいポリシーの説明を入力します。

   このポリシーの優先順位は、ホスト インターフェイスに設定された優先順位よりも低くする必要があることに注意してください。

5. **[テンプレートの選択（Select Template）]** フィールドで、**[ポリシーが選択されていません（No Policy Selected）]** テキストをクリックします。

   [ポリシー テンプレートの選択（Select Policy Template）] ページが表示されます。

6. リストから適切なカスタム分類またはキューイング テンプレートを選択し、**[選択（Select）]** をクリックします。

   次のテンプレートは、NDFC リリース12.2.1 で導入された AI/ML QoS およびキューイング ポリシー機能に固有です。次のテンプレートを活用して、1 つ以上のホスト インターフェイスで使用できるポリシーを作成します。

   - **AI_Fabric_QOS_Classification_Custom**：カスタム キューイングポリシーをインターフェイスに適用するために使用できるインターフェイス テンプレート。
   - **AI_Fabric_QOS_Queuing_Custom：**ユーザー定義のキューイング ポリシー構成に使用できるスイッチ テンプレート。

7. 選択したテンプレートで必要な QoS 分類またはキューイング構成を行い、**[保存（Save）]** をクリックします。

これらの手順を使用して作成されたカスタム QoS ポリシーは、ホスト インターフェイスの QoS およびキューイング ポリシーを構成するときに使用できるようになります。

データ センター VXLAN EVPN ファブリックの高精度時間プロトコル

[データ センター VXLAN EVPN（Data Center VXLAN EVPN）] 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、『*Cisco Nexus 9000 シリーズ NX-OS システム管理コンフィギュレーション ガイド*』の「*PTP の構成*」の項、および『*Cisco Nexsus Dashboard Insights ユーザ ガイド*』を参照してください。

Nexus Dashboard Fabric Controller 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。

[構成の展開（Deploy Config）] 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ます。トラフィックがこのファブリックを出るときには 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 -> _すでに作成されているループバック インターフェイス（loopback0）、またはファブリック設定でユーザーが作成したループバック インターフェイスの IP アドレス

ptp domain 1 -> _ファブリック設定で指定された PTP ドメイン ID_

interface Ethernet1/59 -> _コア側インターフェイス_
  ptp

interface Ethernet1/50 -> _ホスト側インターフェイス_
  --t_tag
  ttag ストリップ
```

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。

データ センター VXLAN EVPN および BGP ファブリックでの MACsec サポート

MACsec は、ファブリック内リンクの Data Center VXLAN EVPN および BGP 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。

NDFC 12.2.2 以降、NDFC は、QKD サーバを使用してキーを生成するか、事前共有キーを使用して、ファブリック間リンクの MACsec、DCI MACsec のサポートを追加しました。詳細については、「QKD を使用して 2 つのファブリックを MACsec と接続する」を参照してください。

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。

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 が有効になっているリンクの MACsec ステータスが **[リンク（Links）]** ページに表示されます。
- 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。

次の項では、Nexus Dashboard Fabric Controller 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

このセクションで説明するプロセスは、データ センター VXLAN EVPN および BGP ファブリックのファブリック内リンクの MACsec を構成するためのものです。

ファブリック内リンクおよび量子鍵伝送（QKD）サーバを使用した MACsec の構成の詳細については、「QKD を使用して、2 つのファブリックを MACsec と接続する」を参照してください。

1. **[管理（Manage）] > [ファブリック（Fabrics）]** に移動します。
2. 既存のデータ センター VXLAN EVPN ファブリックで **[アクション（Actions）] > [作成（Create）]** をクリックして新しいファブリックを作成するか、**[アクション（Actions）] > [ファブリックの編集（Edit Fabric）]** をクリックします。
3. **[セキュリティ（Security）]** タブをクリックし、MACsec の詳細を指定します。

フィールド	説明
MACsec の有効化（Enable MACsec）	ファブリックで 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 構成は、ファブリック内リンクで MACsec が有効になるまで生成されません。**[再計算して展開（Recalculate and Deploy）]** 操作を実行して MACsec 構成を生成し、スイッチに構成を展開します。
[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。
MACsec プライマリ キー文字列	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。 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	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 キーの文字列	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	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。
DCI MACsec の有効化	DCI リンクで DCI 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。 **[DCI MACsec の有効化（Enable DCI MACsec）]** オプションを有効にして、**[リンク MACsec 設定の使用（Use Link MACsec Setting ）]** オプションを無効に すると、NDFC はファブリック設定を使用して、DCI リンクで DCI MACsec を構成します。

フィールド	説明
QKD の有効化	暗号化用の量子キーを生成するために QKDサーバを有効にするには、このチェックボックスをオンにします。 **[QKD を有効にする（Enable QKD）]** オプションを有効にしないことにした場合、NDFC はキーを生成するための QKD サーバを使用する代わりに事前共有キーを生成します。**[QKD を有効にする（Enable QKD）]** オプションを無効にする場合、QKD に関するすべてのフィールドはグレー表示されます。
DCI MACsec 暗号スイート	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。
DCI MACsecプライマリキー文字列	プライマリ DCI 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。 デフォルトのキー ライフタイムは無期限です。
DCI MACsec プライマリ暗号化アルゴリズム	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。
DCI MACsecフォールバック キー文字列	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。 **[QKD の有効化（Enable QKD）]** オプション を 無効 にした 場合は、**[DCI MACsec フォールバック キー文字列（DCI MACsec Fallback Key String）]** オプション を 指定する 必要 があります。
DCI MACsec フォールバック暗号化アルゴリズム	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。
QKD プロファイル名	暗号プロファイル名を指定します。 最大サイズは 63 です。

フィールド	説明
KMEサーバー IP	キー管理エンティティ（KME）サーバの IPv4アドレスを指定します。
KMEサーバ ポート番号	KME サーバが使用するポート番号を指定します。
トラストポイント ラベル	認証タイプのトラストポイント ラベルを指定します。 最大サイズは 64 です。
証明書を無視する	着信証明書の検証をスキップするには、このチェックボックスをオンにします。
MACsec ステータス レポート タイマー	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。

4. **[保存（Save）]** をクリックします。
5. ファブリックをクリックして、サイド パネルに **[概要（Summary）]** を表示します。
6. **[起動（Launch）]** アイコンをクリックして、**[ファブリックの概要（Fabric Overview）]** ページを開きます。
7. **[ファブリックの概要（Fabric Overview）] > [リンク（Links）]** タブをクリックします。
8. MACsec を有効にするファブリック内リンクを選択し、**[アクション（Actions）] > [編集（Edit）]** の順にクリックします。VRF-Lite ファブリック間リンクの作成の詳細については、「VRF-Lite ファブリック間リンクの作成」を参照してください。

   [リンク管理 - リンクの編集（Link Management- Edit Link）] ページが表示されます。
9. **[リンク管理 - リンクの編集（Link Management - Edit Link）]** ページで、**[セキュリティ（Security）]** タブに移動し、必要なパラメータを入力します。

フィールド	説明
MACsec の有効化（Enable MACsec）	VRF-Lite ファブリック間リンク接続（IFC）リンクで MACsec を有効にするには、チェックボックスをオンにします。 **[MACsec の有効化（Enable MACsec）]** オプションを有効にして、**[リンク MACsec 設定の使用（Use Link MACsec Setting）]** オプションを無効にすると、NDFC はファブリック設定を使用して、VRF-Lite IFC で MACsec を構成します。 MACsec がリンクで構成されると、NDFC によって次の構成が生成されます。 • これが MACsec を有効にする最初のリンクの場合のスイッチレベル MACsec 構成。 • リンクの MACsec 構成。
送信元 MACsec ポリシー/キーチェーン名プレフィックス	ポリシーのプレフィックスと、送信元での MACsec 構成のキーチェーン名を指定します。 デフォルト値は **DCI** で、値を変更できます。

フィールド	説明
宛先 MACsec ポリシー/キーチェーン 名プレフィックス	ポリシーのプレフィックスと、宛先での MACsec 構成のキーチェーン名を指定します。 デフォルト値は **DCI** で、値を変更できます。
QKD の有効化	暗号化用の量子キーを生成するために QKDサーバを有効にするには、このチェックボックスをオンにします。  **[QKD を有効にする（Enable QKD）]** オプションを有効にしないことにした場合、NDFC はキーを生成するための QKD サーバを使用する代わりに、ユーザーによって提供された事前共有キーを使用します。**[QKD の有効化（Enable QKD）]** オプションが無効の場合、QKD に対してすべてのフィールドがグレーになります。
リンク MACsec 設定の使用	ファブリック設定を使用する代わりに、リンク設定を使用するためのオーバーライド オプションとしてこのチェックボックスをオンにします。
[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。
MACsec プライマリ キー文字列	プライマリ DCI 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。  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	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 キーの文字列	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。  **[QKD の有効化（Enable QKD）]** が 選択されていない場合 、この パラメータ は必須です。

フィールド	説明
MACsec フォールバック暗号化アルゴリズム	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。
送信元の QKD プロファイル名	送信元の暗号プロファイル名を指定します。 最大サイズは 63 です。
送信元 KME サーバ IP	キー管理エンティティ（KME）サーバの送信元 IPv4 アドレスを指定します。
送信元 KME サーバ ポート番号	KME サーバの送信元ポート番号を指定します。
送信元トラストポイントのラベル	送信元認証タイプのトラストポイント ラベルを指定します。 最大サイズは 64 です。
宛先 QKD プロファイル名	宛先暗号プロファイル名を指定します。
宛先KME サーバ IP	KME サーバに宛先 IPv4 アドレスを指定します。
接続先 KME サーバ ポート番号	KME サーバが使用する宛先ポート番号を指定します。
宛先トラストポイントラベル	宛先認証タイプのトラストポイント ラベルを指定します。 最大サイズは 64 です。
証明書を無視する	受信した証明書の検証をスキップする場合は指定します。

10. **[保存（Save）]** をクリックします。
11. **[ファブリックの概要（Fabric Overview）] > [スイッチ（Switches）]** タブから、**[アクション（Actions）] > [再計算と展開（Recalculate and Deploy）]** を選択して、スイッチに MACsec 構成を展開します。

MACsec の無効化

このセクションで説明するプロセスは、データ センター VXLAN EVPN および BGP ファブリックのファブリック間リンクで MACsec を無効にするためのものです。

量子キー配布（QKD）サーバとのファブリック間リンクの MACsec を無効にする方法については、「QKD を使用して、2 つのファブリックを MACsec と接続する」を参照してください。

次の操作は、MACsec とを無効にします。

- QKD または事前共有キーを使用して、ファブリック間リンクで MACsec を無効にします。
- これが MACsec が有効になっている最後のリンクである場合、NDFC はスイッチからスイッチレベルの MACsec 構成を削除します。
  1. **[ファブリックの概要（Fabric Overview）] > [リンク（Links）]** タブに移動します。
  2. ファブリック間リンクで MACsec を無効にするリンクを選択します。

3. **[リンク管理 - リンクの編集（Link Management - Edit Link）]** ページから、**[セキュリティ（Security）]** タブに移動し、**[MACsec の有効化（Enable MACsec）]** オプションを選択解除します。
4. **[保存（Save）]** をクリックします。
5. **[ファブリックの概要（Fabric Overview）] > [スイッチ（Switches）]** タブから、**[アクション（Actions）] > [展開（Deploy）]** を選択して、スイッチから MACsec 構成を削除します。

IGP アンダーレイを使用した VXLAN EVPN ファブリックのプロビジョニング

Cisco Nexus Dashboard Fabric Controller では、Nexus 9000 および Nexus 3000 シリーズ スイッチにおける VXLAN 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、拡張「Easy」ファブリック ワークフローを導入しました。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希望するアンダーレイ プロビジョニング オプションに合わせて調整できます。

VXLAN BGP EVPN ファブリックの作成と展開については、「VXLAN EVPN ファブリック プロビジョニング」を参照してください。

IPv4 アンダーレイを使用した VXLAN EVPN ファブリックの作成

新しい VXLAN EVPN ファブリックを作成するには、「データセンター　VXLAN EVPN テンプレートを使用した VXLAN EVPN ファブリックの作成」を参照してください。

IPv6 アンダーレイを使用した VXLAN EVPN ファブリックの作成

この手順では、IPv6 アンダーレイを使用して VXLAN EVPN ファブリックを作成する方法を示します。IPv6 アンダーレイを使用して VXLAN ファブリックを作成するためのフィールドのみが記載されていることに注意してください。残りのフィールドについては、「Data Center VXLAN EVPN テンプレートを使用した VXLAN EVPN ファブリックの作成」を参照してください。

NDFC 12.2.2 以降、NDFC は、IPv6 PIMv6 アンダーレイを使用してデータセンター VXLAN EVPN ファブリックと BGP VXLAN ファブリックを構成するためのサポートを追加しました。詳細については、「PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN　EVPN ファブリックの構成」を参照してください。

1. **[管理（Manage）] > [ファブリック（Fabrics）]**の順に選択します。
2. **[アクション（Actions）]** ドロップダウンリストから、**[ファブリックの作成（Create Fabric）]** を選択します。

   [ファブリックの作成（Create Fabric）] ウィンドウが表示されます。
3. **[ファブリック名（Fabric Name）]** フィールドにファブリック名を入力します。
4. **[ファブリックの選択（Pick Fabric）]** フィールドで、**[ファブリックの タイプの選択（Select Type of Fabric）]** ドロップダウン リストから **[Data Center VXLAN EVPN]** を選択します。
5. **[選択（Select）]** をクリックします。
6. デフォルトでは、**[全般パラメータ（General Parameters）]** タブが表示されます。**[一般パラメータ（General Parameters）]** タブの IPv6 アンダーレイを構成するフィールドは以下の通りです。

フィールド	説明
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。2 バイトの BGP ASN または 4 バイトの BGP ASN のいずれかを入力できます。
IPv6 アンダーレイの有効化（Enable IPv6 Underlay）	**[IPv6 アンダーレイの有効化（Enable IPv6 Underlay）]** チェックボックスをオンにします。
IPv6 リンクローカル アドレスを有効にする	**[IPv6 リンク ローカル アドレスを有効にする（Enable IPv6 Link-Local Address）]** チェックボックスをオンにして、リーフスパイン インターフェイスとスパイン ボーダー インターフェイス間のファブリックでリンクローカル アドレスを使用します。このチェックボックスをオンにすると、**[アンダーレイ サブネット IPv6 マスク（Underlay Subnet IPv6 Mask ）]**フィールドは編集できなくなります。デフォルトでは、**[IPv6 リンク ローカル アドレスを有効にする（Enable IPv6 Link-Local Address）]** フィールドが有効になっています。
ファブリック インターフェイスの番号付け	IPv6 アンダーレイは、**p2p** ネットワークのみをサポートします。したがって、**[ファブリック インターフェイスの番号付け（Fabric Interface Numbering）]** ドロップダウン リストは無効になっています。
アンダーレイ サブネット IPv6 マスク（Underlay Subnet IPv6 Mask）	ファブリック インターフェイスの IPv6 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	ファブリックで使用される IGP を指定します。VXLANv6 の場合、OSPFv3 または IS-IS です。
IPv6 アンダーレイの有効化（Enable IPv6 Underlay）	**[IPv6 アンダーレイの有効化（Enable IPv6 Underlay）]** チェックボックスをオンにします。
IPv6 リンクローカル アドレスを有効にする	**[IPv6 リンク ローカル アドレスを有効にする（Enable IPv6 Link-Local Address）]** チェックボックスをオンにして、リーフスパイン インターフェイスとスパイン ボーダー インターフェイス間のファブリックでリンクローカル アドレスを使用します。このチェックボックスをオンにすると、**[アンダーレイ サブネット IPv6 マスク（Underlay Subnet IPv6 Mask ）]**フィールドは編集できなくなります。デフォルトでは、**[IPv6 リンク ローカル アドレスを有効にする（Enable IPv6 Link-Local Address）]** フィールドが有効になっています。 IPv6 アンダーレイは、**p2p** ネットワークのみをサポートします。したがって、**[ファブリック インターフェイスの番号付け（Fabric Interface Numbering）]** ドロップダウン リストは無効になっています。
アンダーレイ サブネット IPv6 マスク（Underlay Subnet IPv6 Mask）	ファブリック インターフェイスの IPv6 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	ファブリックで使用される IGP を指定します。VXLANv6 の場合、OSPFv3 または IS-IS です。

7. **[レプリケーション（Replication）]** タブに移動します。マルチキャスト レプリケーション モードの IPv6 アンダーレイを構成するためのフィールドは次のとおりです。

フィールド	説明
レプリケーション モード	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 [入力レプリケーション（Ingress Replication）] または [マルチキャスト レプリケーション（Multicast replication）] です。[入力レプリケーション（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。マルチキャスト レプリケーションを選択すると、入力レプリケーション 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。 IPv4 または IPv6 のテナント ルーテッド マルチキャスト（TRM）のレプリケーション モードとして **[マルチキャスト（Multicast）]** を選択します。 IPv4 使用例の詳細は、「データ センター VXLAN EVPN テンプレートを使用した VXLAN EVPN ファブリックの作成」を参照してください。 IPv6 の使用例の詳細については、「PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN EVPN ファブリックの構成」を参照してください。
IPv6 マルチキャスト グループ サブネット	プレフィックス範囲が 112 ～ 126 の IPv6 マルチキャスト アドレスを入力します。
IPv4 テナント ルーテッド マルチキャスト（TRM）の有効化	VXLAN EVPN ファブリックで EVPN/MVPN を介してオーバーレイ IPv4 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 IPv4 を使用したテナント 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。
IPv6 テナント ルーテッド マルチキャスト（TRM）の有効化	VXLAN EVPN ファブリックで EVPN/MVPN を介してオーバーレイ IPv6 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 IPv6 を使用したテナント 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 IPv6 アドレス	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（Multicast Group Subnet ）]** 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、Configuring Tenant Routed Multicast の「Overview of Tenant Routed Multicast」の項を参照してください。
TRM VRF のデフォルト MDT IPv6 アドレス	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 **[IPv6 マルチキャスト グループ サブネット（IPv6 Multicast Group Subnet ）]** 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、**[IPv6 マルチキャスト グループ サブネット（IPv6 Multicast Group Subnet）]** で指定した IP プレフィックスから選択された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、Configuring Tenant Routed Multicast の「Overview of Tenant Routed Multicast」の項を参照してください。

フィールド	説明
MVPN VRI ID 範囲	NDFC 12.2.2 以降、vPC ごとに一意の MVPN VRI ID を割り当てるには、このフィールドを使用します。 このフィールドは、次の使用例で必要です。 • VLAN モードなしのレイヤ 3 VNI で VXLANv4 アンダーレイを設定し、TRMv4 または TRMv6 を有効にします。 • VXLANv6 アンダーレイを構成し、TRMv4 または TRMv6 を有効にします。  MVPN VRI ID は、マルチサイト ファブリック内でいずれかのサイト ID と同じにはできません。 VRI IDは 、MSD 内のすべてのサイト内で一意である 必要があります。
MVPN VRI ID の再割り当ての有効化	NDFC リリース 12.2.2 以降では、このチェックボックスを有効にして、ワンタイム VRI ID の再割り当てを生成します。NDFC は、該当する各スイッチに対して、上記の MVPN VRI ID 範囲内で新しい MVPN ID を自動的に割り当てます。これは 1 回限りの操作であるため、操作の実行後、このフィールドはオフになります。  VRI ID の変更は中断を伴うため、それに応じて計画してください。

8. **[VPC]** タブに移動します。

フィールド	説明
vPC ピア キープ アライブオプション	**[管理（management）]** または **[ループバック（loopback）]** 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には、**管理**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には、PKA のために使用される、アンダーレイ ルーティング ループバック（IPv6 アドレスを持つ）を選択します。どちらのオプションも IPv6 アンダーレイでサポートされています。

9. **[プロトコル（Protocols）]** タブに移動します。

フィールド	説明
アンダーレイ エニーキャスト ループバック ID	IPv6 アンダーレイのアンダーレイ エニーキャスト ループバック ID を指定します。IPv6 アドレスはセカンダリとして構成できないため、追加のループバック インターフェイスが各 vPC デバイスに割り当てられます。その IPv6 アドレスが VIP として使用されます。

10. **[リソース（Resources）]** タブに移動します。

フィールド	説明
アンダーレイ IP アドレスの手動割り当て（Manual Underlay IP Address Allocation）	ダイナミック アンダーレイ IP アドレス割り当てを無効にするには、このチェックボックスをオンにします。動的アンダーレイ IP アドレス フィールドは無効になっています。
アンダーレイ ルーティング ループバック IPv6 範囲	プロトコル ピアリングのループバック IPv6 アドレスを指定します。
アンダーレイ VTEP ループバック IPv6 範囲	VTEP のループバックIPv6 アドレスを指定します。
アンダーレイ サブネット IPv6範囲（Underlay Subnet IPv6 Range）	番号付きおよびピアリンク SVI の IP を割り当てる IPv6 アドレス範囲を指定します。このフィールドを編集するには、**[IPv6 リンクローカル アドレスの有効化（Enable IPv6 Link-Local Address）]** チェックボックスをオフにします（**[全般パラメータ（General Parameters）]** タブ ）。
IPv6 アンダーレイの BGP ルータ ID 範囲（BGP Router ID Range for IPv6 Underlay）	BGP ルータ ID を割り当てるアドレスの範囲を指定します。ルーターに使用される IPv4 アドレッシングは、BGP およびアンダーレイ ルーティング プロトコル用です。

11. **[ブートストラップ（Bootstrap）]** タブに移動します。

フィールド	説明
ブートストラップの有効化	**[ブートストラップの有効化（Enable Bootstrap）]** チェックボックスをオンにします。このチェックボックスが選択されていない場合、このタブの他のフィールドは編集できません。
ローカル DHCP サーバの有効化	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、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した場合にのみ、**[DHCP 範囲開始アドレス（DHCP Scope Start Address）]** および **[DHCP 範囲終了アドレス（DHCP Scope End Address）]** フィールドが編集可能になります。
DHCP バージョン	ドロップダウン リストから **[DHCPv4]** を選択する必要があります。

12. **[詳細（Advanced）]** タブまで移動します。

フィールド	説明
L3VNI（VLAN なし）の許可	NDFC リリース 12.2.2 以降では、VLAN を構成せずにレイヤ 3 VNI を構成できるようにするには、このチェックボックスをオンにします。
TCAM 割り当ての有効化	TRMv6 を有効にする場合に 768 以上に TCAM を割り当てるには、このオプションをオンにします。|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。 詳細については、「PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN EVPN ファブリックの構成」を参照してください。

13. **[保存（Save）]** をクリックし、ファブリックの作成を完了します。

次の作業：LAN 動作モードのスイッチの追加の「ファブリックへのスイッチの追加」の項を参照してください。

スイッチの追加

スイッチは、任意の時点で単一のファブリックに追加できます。ファブリックにスイッチを追加し、既存または新しいスイッチを検出するには、「LAN 動作モードのスイッチの追加」の「ファブリックへのスイッチの追加」の項を参照してください。

スイッチ ロールの割り当て

Nexus ダッシュボード ファブリック コントローラのスイッチにロールを割り当てるには、Add Switches for LAN Operational Modeの「Assigning Switch Roles」セクションを参照してください。

vPC ファブリック ピアリング

vPC ファブリック ピアリングは、vPC ピア リンクの物理ポートを無駄にすることなく、拡張デュアル ホーミング アクセス ソリューションを提供します。この機能は、従来の vPC のすべての特性を保持します。詳細については、「*vPC ファブリック ピアリングについての情報*」のセクション（『*Cisco Nexus 9000 シリーズ NX-OS VXLAN 構成ガイド*』）を参照してください。

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 NDFC は、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 vPC ファブリック ピアリングをサポートします。この機能は、**Data Center VXLAN EVPN** および **BGP ファブリック** ファブリック テンプレートに適用されます。

BGP ファブリック 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。

注意事項と制約事項

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 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、また FX および FX2 で終わる Cisco Nexus 9000 シリーズ スイッチだけが vPC ファブリック ピアリングをサポートします。
- 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/GX/GX2 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。詳細については、「*vPC ファブリック ピアリングの注意事項と制約事項*」のセクション（『*Cisco Nexus 9000 シリーズ NX-OS VXLAN 構成ガイド*』）を参照してください。
- 他の Cisco Nexus 9000 シリーズ スイッチを使用している場合、**[再計算と展開（Recalculate & 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、**[再計算と展開（Recalculate & Deploy）]** 中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 NDFC での 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、**[再計算と展開（Recalculate & 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。機能構成中に TCAM リージョンを更新するには、構成端末で hardware access-list tcam ingress-flow redirect512 コマンドを使用します。

ファブリック vPC ピアリングの QoS

Data Center VXLAN EVPN 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、スパインの QoS を有効にすることができます。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、「Data Center VXLAN EVPN」の「Data Center VXLAN EVPN テンプレートを使用した VXLAN EVPN ファブリックを作成する」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：

> 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アカウントの対象となっていない構成をフィルタリングして除去し、構成を PTI 説明付きの **switch_freeform** に設定します。
- 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では、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。

> 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 **[再計算と展開（Recalculate & Deploy）]** 後にファブリック設定からの QoS を有効にした場合、QoS 構成が重複するため、ファブリックの vPC ピアリング構成がすでに存在する場合に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、「Data Center VXLAN EVPN」の「Data Center VXLAN EVPN テンプレートを使用した VXLAN EVPN ファブリックを作成する」を参照してください。

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	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 NDFC 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。

1. **[管理（Manage）] > [ファブリック（Fabrics）]**の順に選択します。

   [LAN ファブリック（LAN Fabrics）] ウィンドウが表示されます。

2. **データセンター VXLAN EVPN** または **BGP ファブリック** 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。

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

   ピア選択のためのウィンドウが表示されます。

   または、**[ファブリックの概要（Fabric Overview）]** ウィンドウ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、**[アクション（Actions）] > [vPC ペアリング（vPC Pairing）]** をクリックして、vPC ペアを作成、編集、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）。

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。

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、**[再計算とデプロイ（Recalculate & Deploy）]** 中に警告またはエラーが発生します。

6. **[保存（Save）]** をクリックします。

7. **[トポロジ（Topology）]** ウィンドウで、**[再計算と展開（Recalculate & Deploy）]** を選択します。

   [構成の展開（Deploy Configuration）] ウィンドウが表示されます。

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。

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。

10. ウィンドウを閉じます。

11. **[再計算と展開（Recalculate & 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。トポロジ ウィンドウからスイッチをリロードすることもできます。詳細については、「*vPC ファブリック ピアリングの注意事項と制約事項*」および「*vPC から vPC ファブリック ピアリングへの移行*」のセクション（『*Cisco Nexus 9000 シリーズ NX-OS VXLAN 構成ガイド*』）を参照してください。

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

はじめる前に

- 物理ピア リンクから仮想ピア リンクへの変換は、スイッチのメンテナンス ウィンドウ中に実行します。
- 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。
  - Cisco Nexus 9300-EX、および 9300-FX/FXP/FX2/FX3/GX/GX2 プラットフォーム スイッチ。詳細については、「*vPC ファブリック ピアリングの注意事項と制約事項*」のセクション（『*Cisco Nexus 9000 シリーズ NX-OS VXLAN 構成ガイド*』）を参照してください。

Cisco NDFC Web UI から物理ピア 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。

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

   [LAN ファブリック（LAN Fabrics）] ウィンドウが表示されます。

2. **データセンター VXLAN EVPN** または **BGP ファブリック** 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。

3. **[トポロジ（Topology）]** ウィンドウで、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。

   または、**[ファブリックの概要（Fabric Overview）]** ウィンドウ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、**[アクション（Actions）] > [vPC ペアリング（vPC Pairing）]** をクリックして、vPC ペアを作成、編集、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）。

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、**[再計算とデプロイ（Recalculate & Deploy）]** 中に警告またはエラーが発生します。

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。

6. **[保存（Save）]** をクリックします。

[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。

7. **[トポロジ（Topology）]** ウィンドウで、**[再計算と展開（Recalculate & Deploy）]** を選択します。

   [構成の展開（Deploy Configuration）] ウィンドウが表示されます。

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。

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。

10. ウィンドウを閉じます。

11. **[再計算と展開（Recalculate & 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

はじめる前に

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。

Cisco NDFC 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。

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

   [LAN ファブリック（LAN Fabrics）] ウィンドウが表示されます。

2. **データセンター VXLAN EVPN** または **BGP ファブリック** 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。

3. **[トポロジ（Topology）]** ウィンドウで、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。

   または、**[ファブリックの概要（Fabric Overview）]** ウィンドウ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、**[アクション（Actions）] > [vPC ペアリング（vPC Pairing）]** をクリックして、vPC ペアを作成、編集、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。

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。

5. **[保存（Save）]** をクリックします。

6. **[トポロジ（Topology）]** ウィンドウで、**[再計算と展開（Recalculate & Deploy）]** を選択します。

   [構成の展開（Deploy Configuration）] ウィンドウが表示されます。

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。

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。

9. ウィンドウを閉じます。

10. **[再計算と展開（Recalculate & 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。

オーバーレイ モード

CLI または設定プロファイル モードで VRF またはネットワークをファブリック レベルで作成できます。VXLAN EVPN マルチサイト ファブリックのメンバー ファブリックのオーバーレイ モードは、メンバー ファブリック レベルで個別に設定されます。オーバーレイ モードは、オーバーレイ構成をスイッチに展開する前にのみ変更できます。オーバーレイ構成を展開すると、すべての VRF/ネットワーク アタッチメントを削除しない限り、モードを変更できません。

Cisco DCNM リリース 11.5(x) からアップグレードする場合、既存の config-profile モードは同じように機能します。スイッチに構成プロファイル ベースのオーバーレイがある場合は、**[config-profile]** オーバーレイ モードでのみインポートできます。cli オーバーレイ モードでインポートすると、ブラウンフィールド インポートの際にエラーが発生します。

ブラウンフィールド インポートで、オーバーレイが **config-profile** モードとして展開されている場合は、**config-profile** モードでのみインポートできます。ただし、オーバーレイが **cli** として展開されている場合は、**config-profile** または **cli** のいずれかのモードでインポートできます。

ファブリック内の VRF またはネットワークのオーバーレイモードを選択するには、次の手順を実行します。

1. **[ファブリックの編集（Edit Fabric）]** ウィンドウに移動します。
2. **[詳細（Advanced）]** タブに移動します。
3. **[オーバーレイ モード（Overlay Mode）]** ドロップダウンリストから、**[config-profile]** または **[cli]** を選択します。

   デフォルト モードは **[config-profile]** です。

VRF の作成

次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。

1. **[管理（Manage）] > [ファブリック（Fabrics）]**の順に選択します。

2. ファブリックをクリックして、**[ファブリック（Fabric）]** スライドイン ペインを開きます。
3. **[起動（Launch）]** アイコンをクリックします。
4. **[ファブリックの概要（Fabric Overview）] > [VRF（VRFs）] > [VRF（VRFs）]** を選択します。
5. **［管理（Manage）] > [ファブリック（Fabrics）]**の順に選択します。
6. ファブリックをダブルクリックして、**[ファブリックの概要（Fabric Overview）]** ページを開きます。

   [VRF の作成（Create VRF）] ページが表示されます。

7. **[VRF の作成（Create VRF）]** ページで、必須のフィールドに必要な詳細を入力します。使用可能なフィールドは、ファブリック タイプによって異なります。

   [VRF の作成（Create VRF）] ページのフィールドは次のとおりです。

フィールド	説明
VRF Name	VRF 名を自動的に設定させること、または自分で入力することができます。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。 MSD ファブリックの場合、VRF またはネットワークの値はファブリックと同じです。
VRF ID	VRF の ID を指定する、または自分で入力することができます。
VLAN ID	ネットワークの対応するテナント VLAN ID を指定する、または自分で入力することができます。ネットワークに新しい VLAN を提案する場合は、**[VLAN の提案（Propose VLAN)]** をクリックします。
VRF テンプレート（VRF Template)	デフォルトのユニバーサル 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。
VRF拡張テンプレート	デフォルトの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。

8. 必要に応じて、必要なフィールド値を入力するか、事前に入力されたフィールドを編集します。

   ページのタブとそのフィールドについては、次のセクションで説明されています。

   - 一般的なパラメータ
   - 作成するAdvanced
   - TRM
   - Route Target

9. VRF を作成するには **[作成（Create）]** を、VRF を破棄するには **[キャンセル（Cancel）]** をクリックします。

   VRF 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 VRF が **[VRF（VRFs）]** 水平タブに表示されます。VRF が作成されたがまだ展開されていないため、ステータスは **NA** です。VRF が作成されたので、ファブリック内のデバイスにネットワークを作成して展開できます。

一般的なパラメータ

[一般パラメータ（General Parameters）] タブには以下のフィールドがあります。

フィールド	説明
VRF VLAN 名	VRF の VLAN 名を入力します。
VRF インターフェイスの説明	VRF インターフェイスの説明を入力します。
VRFの説明	VRF の説明を入力します。

詳細

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。このタブのフィールドは自動入力されます。**[詳細（Advanced)]** タブには以下のフィールドがあります。

フィールド	説明
VRF インターフェイス MTU	VRF インターフェイス MTU を指定します。
ループバック ルーティング タグ	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。
ダイレクトルートマップの再配布	再配布直接ルート マップ名を指定します。
最大 BGP パス	最大 BGP パスを指定します。有効な値の範囲は 1 ～ 64 です。
最大 iBGP パス	iBGP パスの最大数を指定します。有効な値の範囲は 1 ～ 64 です。
IPv6 リンクローカル オプションの有効化	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。
L3VNI VLAN なしを有効にする	NDFC リリース 12.2.1 以降、チェックボックスをオンにして、VLAN 機能なしでレイヤ 3 VNI を有効にします。このチェックボックスがオフの場合、レイヤ 3 VNI 設定には VRF ごとの VLAN が必要です。 このフィールドのデフォルト設定は、以下の要素に基づいて決まります。 • 既存の VRF の場合、デフォルト設定は無効になっています（**[VLAN なしで L3VNI を有効にする（Enable L3VNI w/o VLAN）]** ボックスはオフになっています)。 • 新しく作成された VRF の場合、デフォルト設定はファブリック設定から継承されます。 • このフィールドは、VXLAN ファブリックごとの変数です。VXLAN EVPN マルチサイト ファブリックから作成された VRF の場合、このフィールドの値は子ファブリックのファブリック設定から継承されます。必要に応じて、子ファブリックの VRF を編集して値を変更できます。
アドバタイズホストルート	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。

フィールド	説明
デフォルトルートをアドバタイズ	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（Advertise Default Route）]** 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が /32 ルートになります。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	スタティック 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 ネバーパスワード	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	ドロップダウンリストから、暗号化タイプを選択します。
NetFlow を有効にする	VRF-Lite サブインターフェイスで Netflow モニタリングを有効にすることができます。これは、ファブリックで Netflow が有効になっている場合にのみサポートされることに注意してください。
Netflow Monitor	VRF-lite の Netflow 構成のモニタを指定します。 VRF-Lite サブインターフェイスで Netflow を有効にするには、VRF レベルおよび VRF 拡張レベルで Netflow を有効にする必要があります。拡張を編集して Netflow モニタリングを有効にする場合は、VRF アタッチメントの **[Enable_IFC_Netflow]** チェックボックスをオンにします。 詳細については、「LAN ファブリックについて」の「Netflow のサポート」の項を参照してください。

TRM

NDFC 12.2.2 以降、テナント ルーテッド マルチキャスト（TRM）IPv6 を構成するための **[TRM]** タブが追加されました。既存の IPv4 TRM フィールドは、**[詳細（Advanced）]** タブから **[TRM]** タブに移動されました。

TRMv6 の構成に関する詳細については、「PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN EVPN ファブリックの構成」を参照してください。

TRM の詳細については、「テナント ルーテッド マルチキャストの構成」を参照してください。

フィールド	説明
IPv4 TRM の有効化	IPv4 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。 IPv4 TRM を有効にし、RP アドレスを指定する場合には、**[アンダーレイ マルチキャスト アドレス（Underlay Mcast Address）]** フィールドでアンダーレイ マルチキャスト アドレスを入力する必要があります。

フィールド	説明
RP なし	チェックボックスをオンにすると、RP フィールドを無効にします。このチェックボックスを編集するには、TRMv4 を有効にする必要があります。 **[No RP]** を有効にすると、**[RP 外部（Is RP External）]**、**[RP アドレス（RP Address）]**、**[RP ループバック ID（RP Loopback ID）]**、および **[オーバーレイ マルチキャスト グループ（Overlay Mcast Groups）]** フィールドが無効になります。
RP 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オンにします。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（Is RP External）]** が有効にされていない場合、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	VRF に関連付けられるマルチキャスト 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。 ファブリック設定ページの **[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	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。
TRMv6 の有効化	TRMv6 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。
TRMv6 RP なし	PIM-SSM のみが使用されるため、TRMv6 の RP フィールドを無効にするには、このチェックボックスをオンにします。
TRMv6 RP 外部	TRMv6 の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オンにします。
TRMv6 RP アドレス	TRMv6 RP マルチキャスト トラフィックの IPv6 アドレスを入力します。
オーバーレイ IPv6 マルチキャスト グループ	指定した TRMv6 RP の IPv6 マルチキャスト グループ サブネットを指定します。値は「ipv6 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 ff00::/8 が使用されます。
MVPN 間の有効化	自律システム（AS）境界を通過するには、このチェックボックスをオンにして、マルチキャスト VPN（MVPN）アドレス ファミリ ルートの inter-AS キーワードを使用します。このオプションは、TRM オプションを有効にした場合に適用されます。
IPv4/IPv6 TRM BGW MSite の有効化	BGW マルチサイトで IPv4 または IPv6 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。

ルートターゲット

フィールド	説明
RT自動生成の無効化	IPv4、IPv6 VPN/EVPN/MVPN のこのチェックボックスをオンにします。
インポート	インポートする 1 つの VPN ルート ターゲットまたは VPN ルート ターゲットのカンマ区切りリストを指定します。
エクスポート	エクスポートする 1 つの VPN ルート ターゲットまたは VPN ルート ターゲットのカンマ区切りリストを指定します。
EVPNのインポート	インポートする 1 つの EVPN ルート ターゲットまたは EVPN ルート ターゲットのカンマ区切りリストを指定します。
EVPNのエクスポート	エクスポートする 1 つの EVPN ルート ターゲットまたは EVPN ルート ターゲットのカンマ区切りリストを指定します。
MVPNのインポート	インポートする 1 つの MVPN ルート ターゲットまたは MVPN ルート ターゲットのカンマ区切りリストを指定します。
MVPNのエクスポート	エクスポートする 1 つの MVPN ルート ターゲットまたは MVPN ルート ターゲットのカンマ区切りリストを指定します。 デフォルトでは、**[MVPN のインポート（Import MVPN）]** フィールドと **[MVPN のエクスポート（Export MVPN）]** フィールドは無効になっています。 これらのフィールドを有効にするには、**[IPv4 TRM 有効化（IPv4 TRM Enable）]** または **[TRMv6 有効化（TRMv6 Enable）]** チェックボックスをオンにします。

VRF アタッチメント

UI ナビゲーション

次のオプションは、スイッチ ファブリック、VXLAN EVPN ファブリック、VXLAN EVPN マルチサイト ファブリックにのみ適用されます。

- **[管理（Manage）] > [ファブリック（Fabrics）]**の順に選択します。ファブリックをクリックして、**[ファブリック（Fabric）]** スライドイン ペインを開きます。**[起動（Launch）]** アイコンをクリックします。**[ファブリックの概要（Fabric Overview）] > [VRF（VRFs）] > [VRF アタッチメント（VRF Attachments）]** を選択します。
- **[管理（Manage）] > [ファブリック（Fabrics）]**の順に選択します。ファブリックをダブルクリックして、**[ファブリックの概要（Fabric Overview）] > [VRF（VRFs）] > [VRF アタッチメント（VRF Attachments）]** を開きます。

このウィンドウで、VRFとの間でアタッチメントをアタッチまたはデタッチします。VRF アタッチメントをインポートまたはエクスポートすることもできます。

VRF アタッチメント テーブルのフィールドと説明

フィールド	説明
VRF Name	VRF の名前を指定します。
VRF ID	VRF の ID を指定します。
VLAN ID	VLAN ID を指定します。

スイッチ	スイッチの名前を示します。
ステータス	VRF アタッチメントのステータス（pending、NA、deployed、out-of-sync など）を指定します。
添付ファイル	VRF アタッチメントがアタッチされるか、デタッチされるかを指定します。
スイッチ ロール	スイッチのロールを指定します。たとえば、Campus VXLAN EVPN ファブリック テンプレートを使用して作成されたファブリックの場合、スイッチ ロールはリーフ、スパイン、またはボーダーのいずれかとして指定されます。
Fabric Name（ファブリック名）	VRF がアタッチまたはデタッチされるファブリックの名前を指定します。
ループバック ID	ループバック ID を指定します
ループバック IPV4 アドレス	ループバック IPv4 アドレスを指定します。
ループバック IPV6 アドレス	ループバック IPv6 アドレスを指定します。 IPv6 アドレスはアンダーレイではサポートされていません。

テーブル ヘッダーをクリックすると、エントリがそのパラメータのアルファベット順にソートされます。

次の表に、**[アクション（Actions）]** ドロップダウン リストのアクション項目を示します。これは、**[ファブリックの概要（Fabric Overview）]** ウィンドウの **[VRF（VRFs）]** タブにある、**[VRF アタッチメント（VRF Attachments）]** 水平タブに表示されます。

VRF アタッチメントのアクションと説明

アクション項目	説明
履歴	選択したVRFの展開およびポリシー変更履歴を表示できます。 **[接続履歴（Deployment History）]** タブでは、ホスト名、VRF 名、コマンド、ステータス、ステータスの説明、ユーザ、完了時間など、ネットワーク VRF アタッチメントの展開履歴の詳細を表示できます。 **[ポリシー変更履歴（Policy Change History）]** タブでは、ポリシーの変更履歴の詳細（ポリシー ID、テンプレート、説明、PTI 操作、生成された設定、エンティティの名前とタイプ、作成日、シリアル番号、ユーザー、ソースなど）を表示できます。 VRF アタッチメントの履歴を表示するには、VRF 名の横にあるチェックボックスをオンにして、**[履歴（History）]** を選択します。**[履歴（History）]** ウィンドウが表示されます。必要に応じて、**[展開履歴（Deployment History）]** または **[ポリシー変更履歴（Policy Change History）]** タブをクリックします。また、**[展開履歴（Deployment History）]** タブの **[コマンド（Commands）]** 列の **[詳細履歴（Detailed History）]** リンクをクリックして、ホストのコマンド実行の詳細（構成、ステータスおよび CLI レスポンスを含みます）を表示することもできます。

編集	選択した VRF にアタッチするインターフェイスなどの VRF アタッチメント パラメータを表示または編集できます。 VRF 接続情報を編集するには、編集する VRF 名の横にあるチェックボックスをオンにします。**[編集（Edit）]** を選択します。**[VRF接続の編集（Edit VRF Attachment）]** ウィンドウで、必要な値を編集し、VRF 接続をアタッチまたはデタッチします。**[編集（Edit）]** リンクをクリックしてスイッチの CLI 自由形式構成を編集し、**[保存（Save）]** をクリックして変更を適用します。または **[キャンセル（Cancel）]** をクリックして変更を破棄します。編集した VRF アタッチメントは、**[ファブリックの概要（Fabric Overview）]** ウィンドウの **[VRF（VRFs）]** タブにある、**[VRF アタッチメント（VRF Attachments）]** 水平タブのテーブルに表示されます。
プレビュー	選択した VRF のVRF アタッチメントの設定をプレビューできます。 このアクションは、展開済みまたは NA ステータスのアタッチメントには使用できません。 VRF をプレビューするには、VRF 名の横にあるチェックボックスをオンにして、**[アクション（Actions）]** ドロップダウン リストから **[プレビュー（Preview）]** アクションを選択します。ファブリックの **[構成のプレビュー（Preview Configuration）]** ウィンドウが表示されます。 VRF アタッチメントの詳細をプレビューできます。これには VRF 名、ファブリック名、スイッチ名、シリアル番号、IP アドレス、ロール、VRF ステータス、保留設定、および設定の進行状況などが含まれます。また、**[保留中の構成（Pending Config）]** 列のラインのリンクをクリックして、構成が保留中のラインを確認することもできます。[閉じる（Close）] をクリックします。
展開	選択した VRF の VRF アタッチメント（たとえば、インターフェイス）の保留中の設定を展開できます。 このアクションは、展開済みまたは NA ステータスのアタッチメントには使用できません。 VRF を展開するには、VRF 名の隣にあるチェックボックスをオンにして、**[アクション（Actions）]** ドロップダウン リストから **[展開（Deploy）]** を選択します。ファブリックの **[構成の展開（Deploy Configuration）]** ウィンドウが表示されます。 VRF名、ファブリック名、スイッチ名、シリアル番号、IP アドレス、ロール、VRF ステータス、保留中の設定、設定の進行状況などの詳細を表示できます。また、**[保留中の構成（Pending Config）]** 列のラインのリンクをクリックして、構成が保留中のラインを確認することもできます。**[Deploy]** ボタンをクリックします。展開のステータスと進行状況は、**[VRF ステータス（VRF Status）]** 列と **[進行状況（Progress）]** 列に表示されます。展開が正常に完了したら、ウィンドウを閉じます。

インポート	選択したファブリックの VRF アタッチメントに関する情報をインポートできます。 VRF アタッチメント情報をインポートするには、**[インポート（Import）]** を選択します。ディレクトリを参照し、VRF アタッチメント情報を含む .csv ファイルを選択します。**[開く（Open）]** をクリックし、**[OK]** をクリックします。VRF 情報がインポートされ、**[ファブリックの概要（Fabric Overview）]** ウィンドウの **[VRF（VRFs）]** タブにある **[VRF アタッチメント（VRF Attachments）]** 水平タブに表示されます。
エクスポート	VRF アタッチメントについての情報を .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、LAN がアタッチされているかどうか、関連付けられている VLAN、シリアル番号、インターフェイス、VRF アタッチメント用に保存したフリーフォームの設定など、各 VRF に関する情報が含まれています。 VRF アタッチメント情報をエクスポートするには、**[エクスポート（Export）]** アクションを選択します。VRF 情報を保存するローカル システム ディレクトリの場所を選択し、**[保存（Save）]** をクリックします。VRF 情報ファイルがローカル ディレクトリにエクスポートされます。ファイルがエクスポートされた日時がファイル名に付加されます。
クイックアタッチ	選択した VRF にアタッチメントをすぐにアタッチできます。複数のエントリを選択し、それらを同じインスタンスの VRF にアタッチできます。 アタッチメントを VRF にすばやくアタッチするには、**[アクション（Actions）]** ドロップダウン リストから **[クイック アタッチ（Quick Attach）]** アクションを選択します。アタッチ アクションが成功したことを通知するメッセージが表示されます。
クイック デタッチ	選択した VRF をアタッチメント（ファブリックなど）からすぐにデタッチすることができます。複数のエントリを選択し、それらを同じインスタンスのアタッチメントからデタッチすることができます。 アタッチメントを VRF にすばやくデタッチするには、**[アクション（Actions）]** ドロップダウン リストから **[クイック デタッチ（Quick Detach）]** アクションを選択します。デタッチ アクションが成功したことを通知するメッセージが表示されます。

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

ネットワークを作成する前に、ファブリックの VRF が作成されていることを確認します。ただし、**[ネットワーク作成（Create Network）]** ページでレイヤ 2 を選択した場合は、VRF は必要ありません。詳細については、LAN 動作モード設定のファブリックの概要の「VRF」セクションを参照してください。

Cisco Nexus Dashboard Fabric Controller Web UIからネットワークを作成するには、次の手順を実行します。

1. **[ネットワーク（Networks）]** タブで、**[アクション（Actions）] > [作成（Create）]** をクリックします。

   [ネットワークの作成（Create Network）] ページが表示されます。

2. **[ネットワークの作成（Create Network）]** で、必須のフィールドに必要な詳細を入力します。使用可能なフィールドは、ファブリック タイプによって異なります。

画面のタブとそのフィールドについては、次のセクションで説明されています。

[ネットワークの作成（Create Network）] ページのフィールドは次のとおりです。

フィールド	説明
ネットワーク ID とネットワーク名	ネットワークのレイヤ 2 VNI および名前を指定します。ネットワーク名には、アンダースコア（_）およびハイフン（-）以外の特殊文字または空白が含まれないようにしてください。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。
レイヤ2のみ	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。
VRF Name	ドロップダウン リストから、仮想ルーティングおよび転送（VRF）を選択できます。 新しい VRF を作成する場合は、**[VRF の作成（Create VRF)]** 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。
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。ネットワークに新しい VLAN を提案する場合は、**[VLAN の提案（Propose VLAN)]** をクリックします。
ネットワークテンプレート（Network Template）	デフォルトのユニバーサル 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	デフォルトの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。
マルチキャストIPの生成	新しいマルチキャスト グループ アドレスを生成し、デフォルト値を上書きする場合をクリックします。

画面のタブとそのフィールドについては、次のセクションで説明されています。

- 一般的なパラメータ
- 詳細設定

[一般パラメータ（General Parameters）] タブには以下のフィールドがあります。

フィールド	注説明：ネットワークがレイヤ 2 以外のネットワークである場合は、ゲートウェイの IP アドレスを指定する必要があります。
IPv4 ゲートウェイ/ネットマスク	IPv4 アドレスとサブネットを指定します。 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。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。 + 注：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、Nexus Dashboard Fabric Controller はエラーを表示せず、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 リスト	IPv6 アドレスとサブネットを指定します。
VLAN 名	VLAN 名を入力します。
インターフェイスの説明	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	レイヤ 3 インターフェイスの MTU を入力します。範囲は 68 ~ 9216 です。1
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。
IPv4 セカンダリ GW3	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 GW4	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。

3. 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。**[詳細（Advanced)]** タブには以下のフィールドがあります。

フィールド	説明
ARP 抑制	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	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。 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。

フィールド	説明
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 です。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。 Cisco NDFC リリース 12.1.2e 以降、オーバーレイ ネットワーク用に最大 16 台の DHCP リレー サーバがサポートされます。DHCP リレー サーバ情報を含めるには、次の手順を実行します。 a. **[DHCP リレー サーバ情報（DHCP Relay Server Information）]** フィールドで、**[アクション（Actions）]** > **[追加（Add）]** の順にクリックします。 **[項目の追加（Add Item）]** ページが表示されます。..**[サーバの IP V4 アドレス（Server IP V4 Address）]** および **[サーバの VRF（Server VRF）]** の詳細を入力して、**[保存（Save）]** をクリックします。.. 上記の手順を繰り返して、必要な数の DHCP リレー サーバ情報を追加します。 NDFC リリース 12.1.2e 以降にアップグレードすると、出荷時のオーバーレイ テンプレートを使用して定義された既存の DHCP サーバ構成は、新しい構造に自動的にアップデートされます。構成情報が失われることはありません。
DHCPv4 サーバ 3	次の DHCP サーバの DHCP リレー IP アドレスを入力します。
DHCPv4 Server3 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（最小：0、最大：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	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。
IPv4 TRM の有効化	IPv4 での 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 マルチキャストの構成」を参照してください。
IPv6 TRM の有効化	IPv6 での 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 マルチキャストの構成」を参照してください。
L2 VNI ルートターゲットの両方の有効化	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。
NetFlow を有効にする	ネットワーク上で Netflow モニタリングを有効にします。これは、ファブリックで Netflow がすでに有効になっている場合にのみサポートされます。

フィールド	説明
インターフェイス VLAN Netflow モニタ	VLAN インターフェイスのレイヤ 3 レコードに指定された Netflow モニタを指定します。これは、ファブリックの **[Netflow レコード（Netflow Record）]** で **[レイヤ 2 レコード（Is Layer 2 Record）]** が有効になっていない場合にのみ適用されます。
Vlan Netflow モニタ	レイヤ 3 の [Netflow レコード（Netflow Record）] のファブリック設定で定義された**モニター名を指定します。**
ボーダー上の L3 ゲートウェイの有効化	チェックボックスをオンにすると、ボーダー スイッチでレイヤ 3 ゲートウェイが有効になります。

4. **[作成（Create）]** をクリックします。

   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。

ネットワーク接続

次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。

- **[管理（Manage）] > [ファブリック（Fabrics）]**の順に選択します。ファブリックをクリックして、**[ファブリック（Fabric）]** スライドイン ペインを開きます。**[起動（Launch）]** アイコンをクリックします。**[ファブリックの概要（Fabric Overview）] > [ネットワーク（Networks）] > [ネットワーク アタッチメント（Network Attachments）]** を選択します。
- **[管理（Manage）] > [ファブリック（Fabrics）]**の順に選択します。ファブリックをダブルクリックして、**[ファブリックの概要（Fabric Overview）] > [ネットワーク（Networks）]> [ネットワーク接続（Network Attachments）]** を開きます。

このウィンドウを使用して、ファブリックやインターフェイスをネットワークにアタッチします。

ネットワーク接続テーブルのフィールドと説明

フィールド	説明
ネットワーク名（Network Name）	ネットワークの名前を指定します。
ネットワーク ID（Network ID）	ネットワークのレイヤ 2 VNI を指定します。
VLAN ID	VLAN ID を指定します。
スイッチ	スイッチの名前を示します。
ポート	インターフェイスのポートを指定します。
ステータス	ネットワーク接続のステータス（保留中（pending）、NA など）を指定します。
添付ファイル	ネットワーク接続が接続または切断されているかどうかを指定します。

スイッチ ロール	スイッチのロールを指定します。たとえば、Campus VXLAN EVPN ファブリック テンプレートを使用して作成されたファブリックの場合、スイッチ ロールはリーフ、スパイン、またはボーダーのいずれかとして指定されます。
Fabric Name（ファブリック名）	ネットワークが接続または切断されるファブリックの名前を指定します。

次の表に、**[ファブリックの概要（Fabric Overview）]** ウィンドウの **[ネットワーク（Networks）]** タブの **[ネットワーク アタッチメント（Network Attachments）]** 水平タブに表示される **[アクション（Actions）]** ドロップダウン リストのアクション項目を示します。

ネットワーク接続のアクションと説明

アクション項目	説明
履歴	選択したネットワークの展開およびポリシー変更履歴を表示できます。 **[接続履歴（Deployment History）]** タブでは、ホスト名、ネットワーク名、VRF 名、コマンド、ステータス、ステータスの説明、ユーザ、完了時間など、ネットワーク接続の展開履歴の詳細を表示できます。 **[ポリシー変更履歴（Policy Change History）]** タブでは、ポリシーの変更履歴の詳細（ポリシー ID、テンプレート、説明、PTI 操作、生成された設定、エンティティの名前とタイプ、作成日、シリアル番号、ユーザー、ソースなど）を表示できます。 ネットワーク接続の履歴を表示するには、ネットワーク名の横にあるチェックボックスをオンにして、**[履歴（History）]** アクションを選択します。**[履歴（History）]** ウィンドウが表示されます。必要に応じて、**[展開履歴（Deployment History）]** または **[ポリシー変更履歴（Policy Change History）]** タブをクリックします。**[展開履歴（Deployment History）]** タブの **[コマンド（Commands）]** 列の **[詳細履歴（Detailed History）]** リンクをクリックすれば、ホストのコマンド実行の詳細（構成、ステータスおよび CLI レスポンスを含みます）を表示することができます。

編集	選択したネットワークに接続するインターフェイスなどのネットワーク接続パラメータを表示または編集できます。 ネットワーク接続情報を編集するには、 1. 編集するネットワーク名の横にあるチェックボックスをオンにして、**[アクション（Actions）] > [編集（Edit）]** を選択します。 2. **[ネットワーク アタッチメントの編集（Edit Network Attachment）]** ウィンドウが表示されます。 ○ ネットワーク接続の接続または切断 ○ **[編集（Edit）]** リンクをクリックして、スイッチの CLI 自由形式構成を編集します。 ○ 必要な値の編集 NDFC リリース 12.2.3 以降、**[スイッチ ロール（Switch Role）]** 列に表示されている**境界**または**境界ゲートウェイ**を持つスイッチ上の VXLAN ファブリックでネットワーク接続を編集するときに、**[ルートターゲットのインポート（Import Route Target）]** および **[ルートターゲットのエクスポート（Export Route Target）]** フィールドのスイッチ レベルで、カンマ区切りルート ターゲットをインポートまたはエクスポートできます。これは、Nexus 9000 と Catalyst 9000 スイッチの両方でサポートされています。 **[保存（Save）]** をクリックして変更内容を保存するか、または **[キャンセル（Cancel）]** をクリックして変更内容を取り消します。 編集したネットワーク接続は、**[ファブリックの概要（Fabric Overview）]** ウィンドウの **[ネットワーク（Networks）]** タブの **[ネットワーク接続（Network Attachments）]** 水平タブの表に表示されます。
プレビュー	選択したネットワークのネットワーク接続の構成をプレビューできます。 このアクションは、展開済みまたは NA ステータスのアタッチメントには使用できません。 ネットワークをプレビューするには、ネットワーク名の横にあるチェックボックスをオンにして、**[アクション（Actions）]** ドロップダウン リストから **[プレビュー（Preview）]** アクションを選択します。ファブリックの **[構成のプレビュー（Preview Configuration）]** ウィンドウが表示されます。 ネットワーク名、ファブリック名、スイッチ名、シリアル番号、IP アドレスおよびロール、ネットワーク ステータス、保留中の構成、および構成の進行状況など、ネットワーク接続の詳細をプレビューできます。また、**[保留中の構成（Pending Config）]** 列のラインのリンクをクリックして、構成が保留中のラインを確認することもできます。**[閉じる（Close）]** をクリックします。

展開	選択したネットワークのネットワーク接続（たとえば、インターフェイス）の保留中の構成を展開できます。 このアクションは、展開済みまたは NA ステータスのアタッチメントには使用できません。 ネットワークを展開するには、ネットワーク 名の横にあるチェックボックスをオンにして、**[アクション（Actions）]** ドロップダウン リストから **[展開（Deploy）]** アクションを選択します。ファブリックの **[構成の展開（Deploy Configuration）]** ウィンドウが表示されます。 ネットワーク名、ファブリック名、スイッチ名、シリアル番号、IP アドレスおよびロール、ネットワーク ステータス、保留中の構成、および構成の進行状況などの詳細をプレビューできます。また、**[保留中の構成（Pending Config）]** 列のラインのリンクをクリックして、構成が保留中のラインを確認することもできます。**[Deploy]** ボタンをクリックします。展開のステータスと進行状況は、**[ネットワーク ステータス（Network Status）]** 列と **[進行状況（Progress）]** 列に表示されます。展開が正常に完了したら、ウィンドウを閉じます。
インポート	選択したファブリックのネットワーク接続に関する情報をインポートできます。 ネットワーク接続情報をインポートするには、**[インポート（Import）]** を選択します。ディレクトリを参照し、ネットワーク接続情報を含む CSV ファイルを選択します。**[開く（Open）]** をクリックし、**[OK]** をクリックします。ネットワーク情報がインポートされ、**[ファブリックの概要（Fabric Overview）]** ウィンドウの **[ネットワーク（Networks）]** タブの **[ネットワーク接続（Network Attachments）]** 水平タブに表示されます。
エクスポート	ネットワーク接続についての情報を 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、LAN が接続されているかどうか、関連付けられている VLAN、シリアル番号、インターフェイス、およびネットワーク接続用に保存した自由形式の構成の詳細など、各ネットワークに関する情報が含まれています。 ネットワーク アタッチメント情報をエクスポートするには、**[エクスポート（Export）]** アクションを選択します。ネットワーク情報を保存するローカル システム ディレクトリの場所を選択し、**[保存（Save）]** をクリックします。ネットワーク情報ファイルがローカル ディレクトリにエクスポートされます。ファイルがエクスポートされた日時がファイル名に付加されます。
クイックアタッチ	選択したネットワークにすぐに接続できます。複数のエントリを選択し、それらを同じインスタンスのネットワークに接続できます。 このアクションを使用して、インターフェイスをネットワークに接続することはできません。 アタッチメントをネットワークにすばやくアタッチするには、**[アクション（Actions）]** ドロップダウン リストから **[クイック アタッチ（Quick Attach）]** アクションを選択します。アタッチ アクションが成功したことを通知するメッセージが表示されます。

クイック デタッチ	選択したネットワークを、たとえばファブリックなどの接続から即座に切り離すことができます。複数のエントリを選択し、それらを同じインスタンスの接続から切り離すことができます。 アタッチメントをネットワークからすばやくデタッチするには、**[アクション（Actions）]** ドロップダウン リストから **[クイック デタッチ（Quick Detach）]** アクションを選択します。デタッチ アクションが成功したことを通知するメッセージが表示されます。 クイック デタッチ後、展開がない場合、スイッチのステータスは計算されません。展開後、構成コンプライアンスはエンティティレベル（インターフェイスまたはオーバーレイ）で呼び出しを行います。

ブラウンフィールド VXLAN BGP EVPN ファブリックの管理

このユースケースは、既存の VXLAN BGP EVPN ファブリックを Cisco NDFC に移行する方法を示しています。移行には、既存のネットワーク設定の Nexus Dashboard Fabric Controller への移行が含まれます。

通常、ファブリックは手動の CLI 構成またはカスタム自動化スクリプトによって作成および管理されます。これで、Nexus Dashboard Fabric Controller を使用してファブリックの管理を開始できます。移行後、ファブリック アンダーレイとオーバーレイ ネットワークは NDFC によって管理されます。

VXLAN EVPN マルチサイト ファブリックの移行については、*ボーダー ゲートウェイ スイッチを使用した VXLAN EVPN マルチサイト ファブリックの移行*を参照してください。

前提条件

- NDFC サポート対象の NX-OS ソフトウェア バージョン詳細については、『Nexus Dashboard ファブリック コントローラ、リリース ノート』を参照してください。
- アンダーレイ ルーティング プロトコルは OSPF または IS-IS です。
- 次のファブリック全体のループバック インターフェイス ID は重複してはなりません。
  - IGP/BGP のルーティング ループバック インターフェイス。
  - VTEP ループバック ID
  - ASM がマルチキャスト レプリケーションに使用されている場合のアンダーレイ ランデブー ポイント ループバック ID。
- BGP 構成では、「router-id」を使用します。これはルーティング ループバック インターフェイスの IP アドレスです。
- iBGP ピア テンプレートが構成されている場合は、リーフ スイッチとルート リフレクタで構成する必要があります。リーフ リフレクタとルート リフレクタの間で使用する必要があるテンプレート名は同じにするべきです。
- BGP ルート リフレクタおよびマルチキャスト ランデブー ポイント（該当する場合）機能が、スパイン スイッチに実装されていること。リーフ スイッチはこの機能をサポートしていません。
- VXLAN BGP EVPN ファブリックの概念と、Nexus Dashboard Fabric Controller の観点から見たファブリックの機能に関する知識。
- ファブリック スイッチ ノードの動作は安定していて機能しており、すべてのファブリック リンクがアップ状態であること。
- vPC スイッチとピア リンクは、移行前にアップ状態になっていること。構成の更新が進行中でないこと、保留中の変更がないことを確認してください。
- IP アドレスとログイン情報を使用して、ファブリック内のスイッチのインベントリ リストを作成します。Nexus Dashboard Fabric Controller は、この情報を使用してスイッチに接続します。
- 現在使用している他のコントローラ ソフトウェアをすべてシャットダウンして、VXLAN ファブリックに対してそれ以上の構成変更が行われないようにします。または、コントローラ ソフトウェア（存在する場合）からネットワーク インターフェイスを切断して、スイッチでの変更が行なわれないようにします。
- スイッチ オーバーレイ構成には、出荷されている NDFC ユニバーサル オーバーレイ プロファイルで定義された必須構成が含まれている必要があります。スイッチで見つかった追加のネットワークまたは

VRF オーバーレイ関連の構成は、ネットワークまたは VRF NDFC エントリに関連付けられた自由形式の構成に保持されます。

- ブラウンフィールド移行を成功させるには、VLAN 名やルート マップ名などのオーバーレイ ネットワークと VRF プロファイルのすべてのパラメータが、ファブリック内のすべてのデバイスで一貫している必要があります。

注意事項と制約事項

- 共有ボーダー ファブリックは、ブラウンフィールド移行ではサポートされません。
- すべてのスイッチを NDFC ファブリックに追加して、ファブリック全体に対してブラウンフィールド インポートを完了する必要があります。
- スイッチ上で terminal color を構成する、またはこの構成のバリエーションを構成する（terminal color persist など）ことで、ブラウンフィールドのインポートが失敗する可能性があります。
- CDP デバイス ID を設定する cdp format device-id <system-name> コマンドはサポートされていないため、ブラウンフィールド インポート中にスイッチを追加するとエラーが発生します。サポートされている形式は、cdp format device-id <serial-number>（デフォルト形式）のみです。
- **[ファブリックの作成（Create Fabric）]** ウィンドウで、**[詳細設定（Advanced）] > [オーバーレイ モード（Overlay Mode）]** ファブリック設定で、オーバーレイの移行方法を決定します。デフォルトの config-profile が設定されている場合、VRF およびネットワーク オーバーレイ構成プロファイルは、移行プロセスの一部としてスイッチに展開されます。さらに、重複するオーバーレイ CLI 構成の一部を削除するための diffs 機能があります。これらはネットワークに影響を与えません。
- CLI が設定されている場合、**[オーバーレイ モード（Overlay Mode）]** ドロップダウン リストから選択した VRF およびネットワーク オーバーレイの構成は、整合性の違いに対応するための変更をほとんど、または全く行う必要なく、そのままスイッチに残されます。
- NDFC のブラウンフィールド インポートは、簡素化された NX-OS VXLAN EVPN 構成 CLI をサポートします。詳細については、『Cisco Nexus 9000 シリーズ NX-OS VXLAN 構成ガイド、リリース 10.2(x)』を参照してください。
- 次の機能はサポートされていません。
  - スーパー スパイン ロール
  - ToR
  - eBGP アンダーレイ
  - レイヤ 3 ポートチャネル
- 移行前に、スイッチ構成のバックアップを取り、保存します。
- 移行が完了するまで、スイッチの構成を変更してはなりません（このドキュメントで指示されている場合を除く）。変更すると、重大なネットワークの問題が発生する可能性があります。
- Cisco Nexus Dashboard Fabric Controller への移行は、Cisco Nexus 9000 スイッチでのみサポートされています。
- ボーダー スパインとボーダー ゲートウェイ スパインのロールは、ブラウンフィールド移行でサポートされています。
- まず、設定を更新する際のガイドラインについての注意を述べます。次に、各 VXLAN ファブリック設定タブについて説明します。
  - 一部の値（BGP AS 番号、OSPF など）は、既存のファブリックへの基準ポイントと見なされるので、入力する値は既存のファブリックの値と一致させる必要があります。

- 一部のフィールド（IP アドレス範囲、VXLAN ID 範囲など）の場合、自動入力または設定で入力された値は、将来の割り当てにのみ使用されます。移行中は、既存のファブリック値が優先されます。
- 一部のフィールドは、既存のファブリックに存在しない可能性のある新しい機能（advertise-pip など）に関連しています。必要に応じて有効または無効にします。
- ファブリックの移行が完了した後で、必要に応じて設定を更新できます。

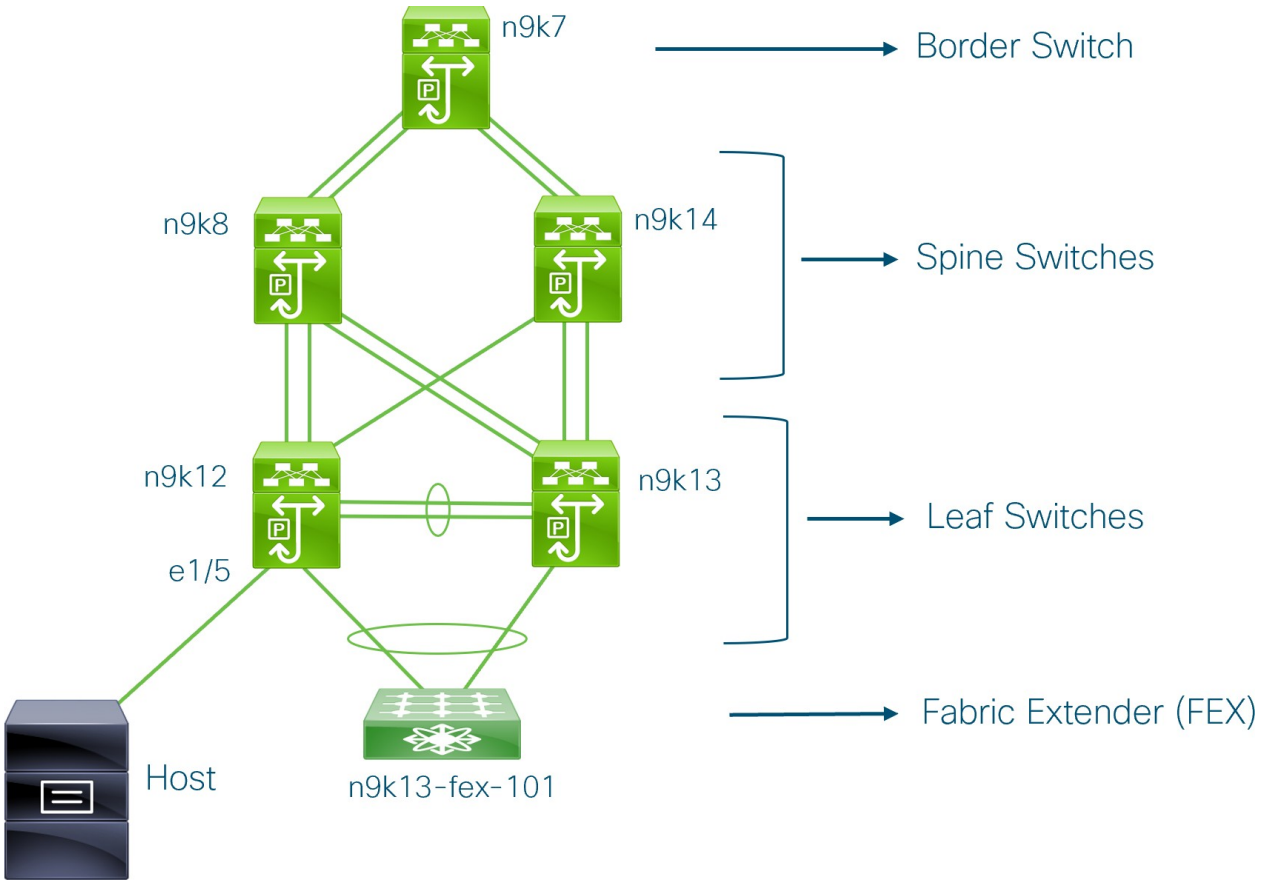
ファブリック トポロジの概要

このユース ケースの例では、次のハードウェアおよびソフトウェア コンポーネントを使用します。

- 5 台の Cisco Nexus 9000 シリーズ スイッチ
- 1 基のファブリック エクステンダ（FEX）
- 1 台のホスト

サポートされるソフトウェア イメージに関する詳細については、*Compatibility Matrix for Cisco NDFC* を参照してください。

既存のファブリックの移行を開始する前に、そのトポロジを見てみましょう。



1 台のボーダー スイッチ、2 台のスパイン スイッチ、2 台のリーフ スイッチ、およびファブリック エクステンダつまり FEX があることがわかります。

1 台のホストが、インターフェイス イーサネット 1/5 を介して n9k12 リーフ スイッチに接続されています。

NDFC ブラウンフィールド展開タスク

ブラウンフィールド移行には、次のタスクが含まれます。

1. 既存の VXLAN BGP EVPN ファブリックの確認
2. Data Center VXLAN EVPN テンプレートを使用した VXLAN EVPN ファブリックの作成
3. スイッチの追加と VXLAN ファブリック管理の NDFC への移行

既存の VXLAN BGP EVPN ファブリックの確認

コンソール端末から **n9k12** スイッチのネットワーク接続を確認してみましょう。

1. ファブリックのネットワーク仮想インターフェイスまたは NVE を確認します。

```
n9k12# show nve vni summary
Codes: CP - Control Plane        DP - Data Plane
       UC - Unconfigured

Total CP VNIs: 84   [Up: 84, Down: 0]
Total DP VNIs: 0   [Up: 0, Down: 0]
```

   コントロール プレーンには 84 の VNI があり、アップ状態になっています。ブラウンフィールド移行の前に、すべての VNI がアップ状態になっていることを確認してください。

2. vPC の整合性と障害を確認します。

```
n9k12# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 2
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : secondary
Number of vPCs configured         : 40
ピア ゲートウェイ                 : 有効
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled, timer is off.(timeout = 300s)
Delay-restore status              : Timer is off.(timeout = 60s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router    : Disabled
.
.
.
```

3. **[n9k-12]** スイッチの EVPN ネイバーを確認します。

```
n9k12# show bgp l2vpn evpn summary
BGP summary information for VRF default, address family L2VPN EVPN
BGP router identifier 192.168.0.4, local AS number 65000
BGP table version is 637, L2VPN EVPN config peers 2, capable peers 2
243 network entries and 318 paths using 57348 bytes of memory
BGP attribute entries [234/37440], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [2/8]

Neighbor        V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.0.0     4 65000     250      91     637    0    0 01:26:59 75
192.168.0.1     4 65000     221      63     637    0    0 00:57:22 75
```

スパイン スイッチに対応する 2 つのネイバーがあることがわかります。

ASN が 65000 であることに注意してください。

4. VRF 情報を確認します。

```
n9k12# show run vrf internet

!Command: show running-config vrf Internet
!Running configuration last done at: Fri Aug 9 01:38:02 2019
!Time: Fri Aug 9 02:48:03 2019

version 7.0(3)I7(6) Bios:version 07.59

interface Vlan347
  vrf member Internet

interface Vlan349
  vrf member Internet

interface Vlan3962
  vrf member Internet

interface Ethernet1/25
  vrf member Internet

interface Ethernet1/26
  vrf member Internet
vrf context Internet
  description Internet
  vni 16777210
  ip route 204.90.141.0/24 204.90.140.129 name LC-Networks
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
router ospf 300
  vrf Internet
    router-id 204.90.140.3
    redistribute direct route-map allow
    redistribute static route-map static-to-ospf
```

```
router bgp 65000
  vrf Internet
    address-family ipv4 unicast
      advertise l2vpn evpn
```

The VRF **Internet** is configured on this switch.

n9k-12 スイッチに接続されているホストは、VRF **Internet** の一部です。

この VRF に関連付けられた VLAN を表示できます。

具体的には、ホストは **Vlan349** の一部です。

5. レイヤ 3 インターフェイス情報を確認します。

```
n9k12# show run interface vlan349

!Command: show running-config interface Vlan349
!Running configuration last done at: Fri Aug 9 01:38:02 2019
!Time: Fri Aug 9 02:49:27 2019

version 7.0(3)I7(6) Bios:version 07.59
```

```
interface Vlan349
  no shutdown
  vrf member Internet
  no ip redirects
  ip address 204.90.140.134/29
  no ipv6 redirects
  fabric forwarding mode anycast-gateway
```

IP アドレスが **204.90.140.134** であることに注意してください。この IP アドレスは、エニーキャスト ゲートウェイ IP として構成されます。

6. 物理インターフェイスの情報を確認します。このスイッチは、インターフェイス イーサネット 1/5 を介してホストに接続されています。

```
n9k12# show run interface ethernet1/5

!Command: show running-config interface Ethernet1/5
!Running configuration last done at: Fri Aug 9 01:38:02 2019
!Time: Fri Aug 9 02:50:05 2019

version 7.0(3)I7(6) Bios:version 07.59

interface Ethernet1/5
  description to host
  switchport mode trunk
  switchport trunk native vlan 349
  switchport trunk allowed vlan 349,800,815
  spanning-tree bpduguard enable
  mtu 9050
```

このインターフェイスがホストに接続されており、VLAN 349 で構成されていることがわかります。

7. ホストからエニーキャスト ゲートウェイの IP アドレスへの接続を確認します。

```
host# ping 204.90.140.134 count unlimited interval 1
PING 204.90.140.134 (204.90.140.134): 56 data bytes
64 bytes from 204.90.140.134: icmp_seq=0 ttl=254 time=1.078 ms
64 bytes from 204.90.140.134: icmp_seq=1 ttl=254 time=1.129 ms
64 bytes from 204.90.140.134: icmp_seq=2 ttl=254 time=1.151 ms
64 bytes from 204.90.140.134: icmp_seq=3 ttl=254 time=1.162 ms
64 bytes from 204.90.140.134: icmp_seq=4 ttl=254 time=1.84 ms
64 bytes from 204.90.140.134: icmp_seq=5 ttl=254 time=1.258 ms
```

```
64 bytes from 204.90.140.134: icmp_seq=6 ttl=254 time=1.273 ms
64 bytes from 204.90.140.134: icmp_seq=7 ttl=254 time=1.143 ms
```

既存のブラウンフィールド ファブリックを Nexus Dashboard Fabric Controlle に移行する間、ping コマンドをバックグラウンドで実行させています。

スイッチの追加と VXLAN ファブリック管理の NDFC への移行

スイッチを検出して、新しく作成したファブリックに追加しましょう。

1. 新しく作成されたファブリック名をダブルクリックして **[ファブリックの概要（Fabric Overview）]** 画面を表示します。

   [スイッチ（Switches）] タブをクリックします。

2. **[アクション（Actions）]** ドロップダウン リストから、**[スイッチの追加（Add Switches）]** を選択します

   [スイッチの追加（Add Switches）] ウィンドウが表示されます。

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

3. **[スイッチの追加 - ファブリック（Add Switches - Fabric）]** 画面で、**[シード スイッチの詳細（Seed Switch Details）]** を入力します。

   [シード IP（Seed IP）] フィールドにスイッチの IP アドレスを入力します。検出するスイッチのユーザー名とパスワードを入力します。

   デフォルトでは、**[最大ホップ数（Max Hops）]** フィールドの値は **2** です。指定された IP アドレスを持つスイッチと、そこから 2 ホップ離れたスイッチは、検出が完了すると入力されます。

   [構成を保持（Preserve Config）] チェックボックスを必ずオンにしてください。これにより、スイッチの現在の構成が保持されます。

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

   指定された IP アドレスを持つスイッチと、そこから最大 2 ホップ離れたスイッチ（最大ホップ数の設定による）が、[スキャンの詳細（Scan Details）] セクションに表示されます。

5. ファブリックにインポートする必要がある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。

   1 回の試行で同時に複数のスイッチを検出することをお勧めします。スイッチは適切にケーブル接続し NDFC 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。

   スイッチを複数回インポートする場合は、ブラウンフィールド インポート プロセスを続行する前に、すべてのスイッチがファブリックに追加されていることを確認してください。

6. **[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、選択したすべてのスイッチの進行状況が表示されます。完了時には、スイッチごとに **[完了（done）]** と表示されます。

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

   エラー メッセージが表示された場合は、画面を閉じます。[ファブリック トポロジ（fabric topology）] 画面が表示されます。エラー メッセージは、画面の右上に表示されます。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。

7. インポートが成功すると、進行状況バーにすべてのスイッチの **[完了（Done）]** が表示されます。**[閉じる（Close）]** をクリックします。

   ウィンドウを閉じると、ファブリック トポロジ ウィンドウが再び表示されます。スイッチは移行モードになり、移行モードのラベルがスイッチ アイコンに表示されます。

   この時点では、グリーンフィールド移行や*新しい*スイッチの追加を行わないでください。移行プロセス中の新しいスイッチの追加はサポートされていません。ネットワークに望ましくない結果をもたらす可能性があります。ただし、移行プロセスの完了後には、新しいスイッチを追加できます。

8. すべてのネットワーク要素が検出されると、接続されたトポロジの **[トポロジ（Topology）]** ウィンドウに表示されます。各スイッチには、デフォルトで**リーフ** ロールが割り当てられます。

   いくつかのスイッチでスイッチ ディスカバリ プロセスが失敗し、ディスカバリ エラー メッセージが表示されることがあります。それでも、そのようなスイッチは引き続きファブリック トポロジに表示されます。このようなスイッチはファブリックから削除し（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）]** をクリックします）、再度インポートする必要があります。

   既存のファブリック内のすべてのスイッチが NDFC で検出されるまで、次の手順に進まないでください。

   表示用に階層レイアウトを選択すると（[アクション（Actions）] パネルで）、トポロジはロールの割り当てに従って自動的に配置され、リーフ スイッチが下部に、接続されたスパイン スイッチがその上に、ボーダー スイッチが上部に配置されます。

   > Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x) イメージのスイッチでサポートされるロールは、ボーダー リーフ、ボーダー スパイン、リーフ、およびスパインです。

9. スイッチを選択し、**[アクション（Actions）] > [ロールの設定（Set Role）]** をクリックします。[ロールの選択] 画面で、**[境界（Border）]** を選択し、**[選択（Select）]** をクリックします。

   同様に、**[スパイン（Spine）]** ロールを **[n9k-14]** および **[n9k-8]** スパイン スイッチで設定します。

   > 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。

   vPC ペアリング（vPC Pairing） ：vPC ペアリングは、レイヤ 3 vPC ピア キープ アライブが使用されているスイッチに対して行う必要があります。vPC ピア キープ アライブが管理オプションによって確立されると、vPC 構成はスイッチから自動的に取得されます。このペアリングは、移行が完了した後にのみ GUI に反映されます。

   a. スイッチ アイコンを右クリックし、[vPC ペアリング（vPC Pairing）] をクリックして、vPC スイッチ ペアを設定します。

      [vPC ピアの選択（Select vPC peer）] 画面が表示されます。vPC ピアになり得るスイッチが一覧表示されます。

   b. 適切なスイッチを選択し、[OK] をクリックします。ファブリック トポロジが再び起動します。vPC ペアが形成されます。

   > 現在のファブリックからすべてのスイッチを追加したかどうかを確認します。スイッチを追加し忘れた場合は、ここで追加してください。既存のスイッチをすべてインポートしたことを確認したら、次のステップである [保存して展開（Save and Deploy）] オプションに進みます。

10. [ファブリックの概要（Fabric Overview）] の **[アクション（Actions）]** ドロップダウン リストから、**[再計算と展開（Recalculate and Deploy）]** を選択します。

    [再計算と展開（Recalculate and Deploy）] をクリックすると、NDFC はスイッチ設定を取得し、現在実行中の設定から現在予想される設定までのすべてのスイッチの状態を入力します。これが意図された状態で、NDFC で維持されます。

構成の不一致がある場合は、**[保留中の構成（Pending Config）]** 列に相違の行数が表示されます。[保留中の構成（Pending Config）] 列をクリックして、**[保留中の構成（Pending Config）]** を表示し、実行構成と**並べて比較**します。**[展開（Deploy）]** をクリックして、設定を適用します。

アンダーレイおよびオーバーレイ ネットワークの移行後、**[構成の展開（Deploy Configuration）]** 画面が表示されます。

- ブラウンフィールド移行では、オーバーレイ構成の一貫性を維持するなど、既存のファブリックでベスト プラクティスに従う必要があります。
- ブラウンフィールド移行は、スイッチから実行中の構成を収集し、これらに基づいて NDFC 構成の意図を構築し、整合性チェックなどを行うため、完了するまでに時間がかかる場合があります。
- 移行中に見つかったエラーまたは不整合は、ファブリック エラーで報告されます。スイッチは引き続き移行モードのままです。これらのエラーを修正し、**[展開（Deploy）]** をクリックし、エラーが報告されなくなるまで繰り返して、移行を再度完了する必要があります。

11. 構成が生成されたら、**[構成のプレビュー（Preview Config）]** 列のリンクをクリックして確認します。

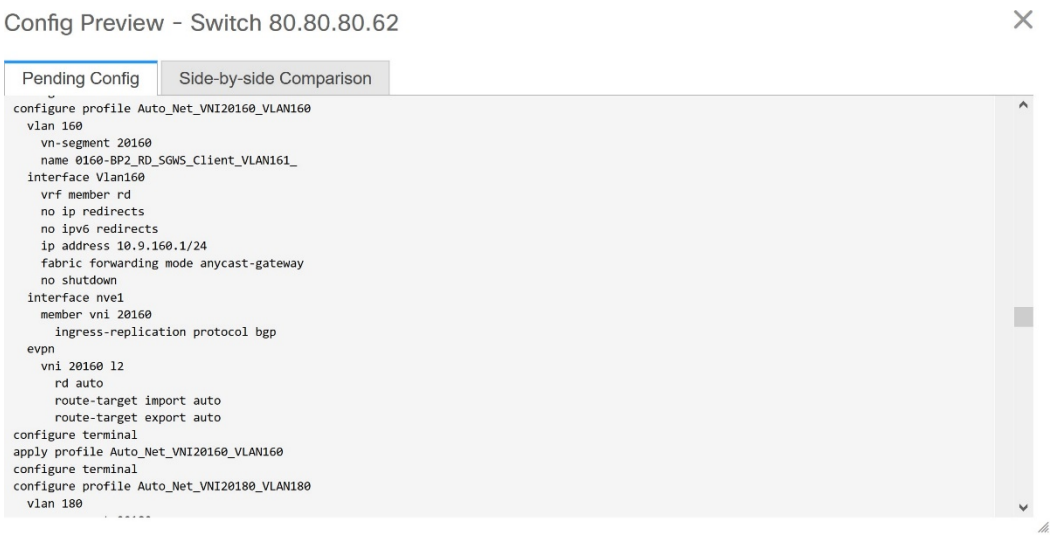
スイッチへの展開に進む前に、構成をプレビューすることを強くお勧めします。[構成のプレビュー（Preview Configuration）] 列のエントリをクリックします。**[構成のプレビュー（Preview Config）]** 画面が表示されます。スイッチの保留中の設定が一覧表示されます。

[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。

[保留中の構成（Pending Config）] タブには、現在の実行構成から現在期待または意図されている構成に移行するために、スイッチに展開する必要がある一連の構成が表示されます。

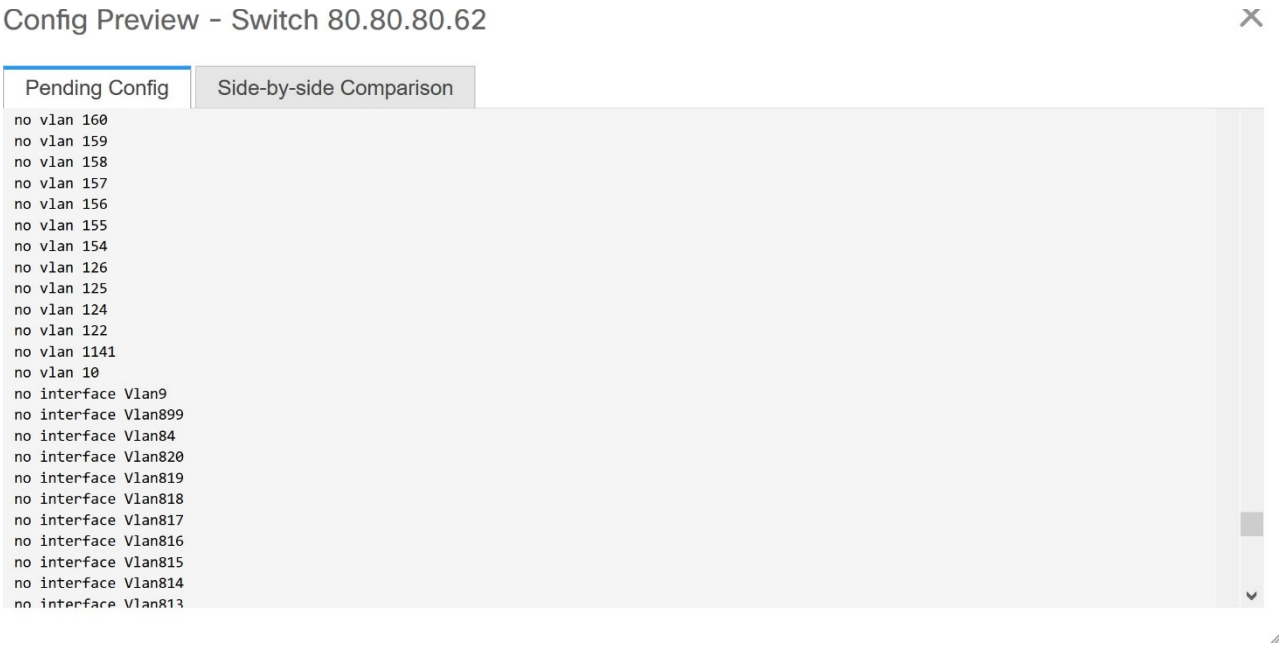
[保留中の構成（Pending Config）] タブには、スイッチに展開される多くの構成行が表示される場合があります。通常、ブラウンフィールド インポートが成功すると、これらの行が、オーバーレイ ネットワーク構成のためにスイッチにプッシュされた構成プロファイルに対応することになります。既存のネットワークおよび VRF 関連のオーバーレイ設定はスイッチから削除されないことに注意してください。

構成プロファイルは、スイッチの VXLAN 構成を管理するために NDFC に必要な構成です。ブラウンフィールド インポート プロセス中には、スイッチにすでに存在する元の VXLAN 構成と同じ情報がキャプチャされます。次の図では、**vlan 160** の構成プロファイルが適用されています。



インポート プロセスの一環として、構成プロファイルが適用された後、元の CLI ベースの基準構成はスイッチから削除されます。これらは、差分の最後に表示される「no」CLI です。スイッチの VXLAN 構成は、構成プロファイルに保持されます。次の画像では、構成が削除されることがわかります。具体的には、**no vlan 160** が削除されます。

オーバーレイ モードが CLI ではなく **config-profile** に設定されている場合、CLI ベースの設定は削除できます。



[並べて比較（Side-by-Side Comparison）] タブには、実行中の構成と予想される構成が並べて表示されます。

12. 構成を確認したら、**[構成プレビュー スイッチ（Config Preview Switch）]** ウィンドウを閉じます。
13. **[構成の展開（Deploy Config）]** をクリックして、構成をスイッチに展開します。

    [ステータス（Status）] 列に **[失敗（FAILED）]** と表示された場合は、失敗の理由を調査して問題に対応してください。

    最終的に、プログレスバーは、各スイッチについて **100%** を示します。プロビジョニングが正しく行われ、構成が正常に達成されたら、画面を閉じます。

    表示されるファブリック トポロジ画面では、インポートされたすべてのスイッチ インスタンスが緑色で表示され、設定が成功したことを示します。また、**[移行モード（Migration Mode）]**ラベルは、どのスイッチ アイコンでも表示されなくなります。

    NDFC は VXLAN-EVPN ファブリックを正常にインポートしました。

    [VXLAN ファブリック管理から NDFC への移行後（Post-transitioning of VXLAN fabric management to NDFC）]：これで、VXLAN ファブリック管理から NDFC への移行プロセスが完了します。これで、新しいスイッチを追加し、ファブリックにオーバーレイ ネットワークをプロビジョニングできます。詳細については、構成ガイドのファブリック トピックの該当するセクションを参照してください。

    詳細については、「LAN 動作モード設定のファブリックの概要」を参照してください。

ブラウンフィールド移行の構成プロファイルのサポート

Cisco NDFC は、構成プロファイルでプロビジョニングされる VXLAN オーバーレイを使用した、ファブリックのブラウンフィールド インポートをサポートしています。このインポート プロセスは、構成プロ

ファイルに基づいてオーバーレイ構成のインテントを再作成します。アンダーレイの移行は、通常のブラウンフィールド移行で実行されます。

この機能は、NDFC バックアップを復元できない場合に、既存の Easy ファブリックを回復するために使用できます。この場合、最新の NDFC リリースをインストールし、ファブリックを作成してから、スイッチをファブリックにインポートする必要があります。

この機能は、NDFC アップグレードには推奨されないことに注意してください。詳細については、*NDFC Installation and Upgrade Guide* を参照してください。

以下は、構成プロファイルのサポートに関するガイドラインです。

- **Data Center VXLAN EVPN** テンプレートでは、構成プロファイルのブラウンフィールド移行がサポートされています。
- スイッチの構成プロファイルは、デフォルトのオーバーレイ **Universal** プロファイルのサブセットである必要があります。**Universal** プロファイルの一部ではない追加の構成行が存在する場合、不要なプロファイルの更新が表示されます。この場合、構成を再計算して展開した後、**並べて比較**機能を使用して差分を確認し、変更を展開します。
- VXLAN オーバーレイ構成プロファイルと通常の CLI を組み合わせたスイッチでのブラウンフィールド移行はサポートされていません。この状態が検出されると、エラーが生成され、移行が中止されます。すべてのオーバーレイは、構成プロファイルまたは通常の CLI のいずれか一方だけを使用する必要があります。

ブラウンフィールド移行後のリーフまたはスパインの PIM-BIDIR 構成を手動で追加する

ブラウンフィールド移行後、新しいスパインまたはリーフ スイッチを追加する場合は、PIM-BIDIR 機能を手動で設定する必要があります。

次の手順は、新しいリーフまたはスパインの PIM-BIDIR 機能を手動で設定する方法を示しています。

1. ブラウンフィールド移行によって追加された RP 用に作成された **base_pim_bidir_11_1** ポリシーを確認します。各 ip pim rp-address_RP_IP_group-list_MULTICAST_GROUP_bidir コマンドで使用する RP IP およびマルチキャスト グループを確認します。
2. 各 **base_pim_bidir_11_1** ポリシーを新しいリーフまたはスパインの **[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウから追加し、各 **base_pim_bidir_11_1** ポリシーの構成をプッシュします。

ボーダーゲートウェイスイッチを使用した VXLAN EVPN Multi-Site ファブリックの移行

ボーダー ゲートウェイ スイッチを備えた既存の VXLAN EVPN Multi-Site ファブリックを NDFC に移行する場合は、次のガイドラインに注意してください。

- **自動** IFC 作成関連のファブリック設定をすべてオフにします。設定を確認し、次のようにチェックがオフになっていることを確認します。
    - **データセンター VXLAN EVPN** ファブリック

      [リソース（Resources）] タブの **[両方を自動展開（Auto Deploy Both）]** チェックボックスをオフにします。

- VXLAN EVPN Multi-Site ファブリック

  [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フ（**[DCI]** タブ）。

- アンダーレイ マルチサイト ピアリング：サイト間のアンダーレイ拡張の eBGP ピアリングおよび対応するルーテッド インターフェイスは、**switch_freeform** および **routed_inerfaces**、オプションで **interface_freeform** 構成でキャプチャされます。この構成には、マルチサイトのすべてのグローバル構成が含まれます。EVPN マルチサイトのループバックも、適切なインターフェイス テンプレートを介してキャプチャされます。

- オーバーレイ マルチサイト ピアリング：eBGP ピアリングは、**switch_freeform** の一部としてキャプチャされます。唯一の関連する構成がルータ bgp の下にあるためです。

- ネットワークまたは VRF を含むオーバーレイ：対応するインテントは、**extension_type = MULTISITE** のボーダー ゲートウェイのプロファイルでキャプチャされます。

1. 必要なファブリック設定を使用して、データセンター VXLAN EVPN および Multi-Site Interconnect Network ファブリックを含む、必要なすべてのファブリックを作成します。上記のように [Auto VRF-Lite] 関連オプションを無効にします。詳細については、*VXLAN EVPN ファブリックの作成*および*外部ファブリック*セクションを参照してください。

2. すべてのスイッチを必要なすべてのファブリックにインポートし、それに応じてロールを設定します。

3. 各ファブリックで **[再計算と展開（Recalculate and Deploy）]** をクリックし、ブラウンフィールド移行プロセスが 'Deployment' フェーズに到達することを確認します。ここでは、**[構成の展開（Deploy Configuration）]** をクリックしないでください。

4. ガイドラインに示すように、必要なファブリック設定で **VXLAN EVPN Multi-Site** ファブリックを作成し、**[自動マルチサイト IFC（Auto MultiSite IFC）]** 関連オプションを無効にします。詳細については、「*VXLAN EVPN マルチサイト ファブリックの作成*」を参照してください。

5. すべてのメンバーファブリックを VXLAN EVPN Multi-Site に移動します。この手順が正常に完了するまで、先に進まないでください。詳細については、「*VXLAN EVPN マルチサイト親ファブリック下でのメンバー 1 ファブリックの移動*」を参照してください。

   > 各イージー ファブリックのオーバーレイ ネットワークと VRF の定義は対称にして、それらが VXLAN EVPN マルチサイトに正常に追加されるようにする必要があります。不一致が見つかった場合、エラーが報告されます。これらは、ファブリックのオーバーレイ情報を更新して修正し、VXLAN EVPN マルチサイトに追加する必要があります。

6. 展開された構成の IP アドレスと設定に一致するように、すべてのマルチサイト アンダーレイ IFC を作成します。

   > 必要に応じて、追加のインターフェイス構成を、**[詳細（Advanced）]** セクションの [送信元/宛先インターフェイス（Source/Destination interface ）] フリーフォーム フィールドに追加する必要があります。

   詳細については、*マルチサイト オーバーレイ IFC の構成*を参照してください。

7. 展開された構成の IP アドレスと設定に一致するように、すべてのマルチサイト オーバーレイ IFC を作成します。IFC リンクを追加する必要があります。詳細については、*マルチサイト オーバーレイ IFC の構成*を参照してください。

8. VRF-Lite IFC もある場合は、それらも作成します。

設定プロファイルがスイッチにすでに存在する、ブラウンフィールド移行の場合、VRF-Lite IFC はステップ #3 で自動的に作成されます。

9. VXLAN EVPN Multi-Site ファブリックでテナント ルーテッド マルチキャスト（TRM）が有効になっている場合は、VXLAN EVPN Multi-Site のすべての TRM 関連 VRF およびネットワーク エントリを編集し、TRM パラメータを有効にします。

   この手順は、ファブリックで TRM が有効になっている場合に実行する必要があります。TRM が有効になっていない場合でも、各ネットワーク エントリを編集して保存する必要があります。

10. ここで、VXLAN EVPN Multi-Site ファブリックの **[再計算して展開（Recalculate and Deploy）]** をクリックしますが、**[構成の展開（Deploy Configuration）]** はまだクリックしないでください。

11. 各メンバー ファブリックに移動し、**[再計算と展開（Recalculate and Deploy）]** をクリックしてから、**[構成の展開（Deploy Configuration）]** をクリックします。

これでブラウンフィールド移行は完了です。通常の NDFC オーバーレイ ワークフローを使用して、BGW のすべてのネットワークまたは VRF を管理できるようになりました。

アンダーレイ IFC 用のレイヤ 3 ポート チャネルを持つボーダー ゲートウェイ スイッチ（BGW）を備えた既存の VXLAN EVPN Multi-Site ファブリックを移行する場合は、次の手順を実行してください。

VXLAN EVPN Multi-Site ファブリックを移行する前に、子ファブリックが VXLAN EVPN Multi-Site に追加されていることを確認します。

1. VXLAN EVPN Multi-Site 子ファブリックをクリックし、**[ファブリック（Fabrics）] > [インターフェイス（Interfaces）]** に移動して、BGW を表示します。アンダーレイ IFC に使用する適切なレイヤ 3 ポート チャネルを選択します。

2. **[ポリシー（Policy）]** 列で、ドロップダウン リストから **int_port_channel_trunk_host_11_1** を選択します。関連付けられたポート チャネル インターフェイス メンバーを入力し、**[保存（Save）]** をクリックします。

3. VXLAN EVPN Multi-Site ファブリックの**表形式ビュー**に移動します。レイヤ 3 ポート リンクを編集し、マルチサイト アンダーレイ IFC リンク テンプレートを選択し、送信元と宛先の IP アドレスを入力します。これらの IP アドレスは、スイッチの既存の構成値と同じです。

4. 上記の手順 7 から 11 までの手順を実行します。

VXLANv6 ファブリックの構成

IPv6 のみのアンダーレイで Easy ファブリックを作成できます。IPv6 アンダーレイは、**Data Center VXLAN EVPN** テンプレートでのみサポートされます。

NDFC 12.2.2 以降、NDFC は、IPv6 アンダーレイ、PIMv6、および TRMv6 のサポートを使用してすべての VXLAN EVPN ファブリック テンプレートを構成するためのサポートを追加しました。詳細については、「PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN EVPN ファブリックの構成」を参照してください。

IPv6 アンダーレイ ファブリックでは、ファブリック内リンク、ルーティング ループバック、vPC ピア リンク SVI、および VTEP の NVE ループバック インターフェイスが IPv6 アドレスで構成されます。EVPN BGP ネイバー ピアリングも、IPv6 アドレッシングを使用して確立されます。

IPv6 アンダーレイの注意事項と制約事項

- IPv6 アンダーレイは、Cisco NX-OS リリース 9.3(1) 以降を搭載した Cisco Nexus 9000 シリーズ スイッチでサポートされています。
- VXLANv6 は、Cisco Nexus 9332C、Cisco Nexus C9364C、および EX、GX、FX、FX2、FX3、または FXP で終わる Cisco Nexus モジュールのみでサポートされます。

VXLANv6 は、IPv6 アンダーレイを備えた VXLAN ファブリックとして定義されます。

- VXLANv6 では、スパインでサポートされるプラットフォームは、すべての Cisco Nexus 9000 シリーズおよび Cisco Nexus 3000 シリーズ プラットフォームです。
- IPv6 ファブリックでサポートされるオーバーレイ ルーティング プロトコルは BGP EVPN です。
- 物理マルチシャーシ EtherChannel トランク（MCT）機能を備えた vPC は、NDFC の IPv6 アンダーレイ ネットワークでサポートされています。vPC ピア キープアライブ オプションは、IPv4 または IPv6 アドレスを使用したループバックまたは管理インターフェイスで設定できます。
- VXLANv6 ファブリックではブラウンフィールド移行がサポートされています。IPv6 アドレスを使用した L3 vPC キープアライブは、ブラウンフィールド移行ではサポートされないことに注意してください。この vPC 構成は、移行後に削除されます。ただし、IPv4 アドレスを使用した L3 vPC キープアライブはサポートされています。
- DHCPv6 は、IPv6 アンダーレイ ネットワークでサポートされています。
- 次の機能は、VXLAN IPv6 アンダーレイではサポートされていません。
  - ISIS、OSPF、および BGP 認証
  - デュアルスタック アンダーレイ
  - vPC ファブリック ピアリング
  - DCI SR-MPLS または MPLS-LDP ハンドオフ
  - BFD
  - スーパー スパイン スイッチ ロール
  - NGOAM

IPv6 アンダーレイを使用した VXLAN EVPN ファブリックの作成

この手順では、IPv6 アンダーレイを使用して VXLAN EVPN ファブリックを作成する方法を示します。IPv6 アンダーレイを使用して VXLAN ファブリックを作成するためのフィールドのみが記載されていることに注意してください。残りのフィールドについては、「Data Center VXLAN EVPN テンプレートを使用した VXLAN EVPN ファブリックの作成」を参照してください。

NDFC 12.2.2 以降、NDFC は、IPv6 PIMv6 アンダーレイを使用してデータセンター VXLAN EVPN ファブリックと BGP VXLAN ファブリックを構成するためのサポートを追加しました。詳細については、「PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN　EVPN ファブリックの構成」を参照してください。

1. **[管理（Manage）] > [ファブリック（Fabrics）]**の順に選択します。
2. **[アクション（Actions）]** ドロップダウンリストから、**[ファブリックの作成（Create Fabric）]** を選択します。

   [ファブリックの作成（Create Fabric）] ウィンドウが表示されます。
3. **[ファブリック名（Fabric Name）]** フィールドにファブリック名を入力します。
4. **[ファブリックの選択（Pick Fabric）]** フィールドで、**[ファブリックの タイプの選択（Select Type of Fabric）]** ドロップダウン リストから **[Data Center VXLAN EVPN]** を選択します。
5. **[選択（Select）]** をクリックします。
6. デフォルトでは、**[全般パラメータ（General Parameters）]** タブが表示されます。**[一般パラメータ（General Parameters）]** タブの IPv6 アンダーレイを構成するフィールドは以下の通りです。

フィールド	説明
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。2 バイトの BGP ASN または 4 バイトの BGP ASN のいずれかを入力できます。
IPv6 アンダーレイの有効化（Enable IPv6 Underlay）	**[IPv6 アンダーレイの有効化（Enable IPv6 Underlay）]** チェックボックスをオンにします。
IPv6 リンクローカル アドレスを有効にする	**[IPv6 リンク ローカル アドレスを有効にする（Enable IPv6 Link-Local Address）]** チェックボックスをオンにして、リーフスパイン インターフェイスとスパイン ボーダー インターフェイス間のファブリックでリンクローカル アドレスを使用します。このチェックボックスをオンにすると、**[アンダーレイ サブネット IPv6 マスク（Underlay Subnet IPv6 Mask ）]**フィールドは編集できなくなります。デフォルトでは、**[IPv6 リンク ローカル アドレスを有効にする（Enable IPv6 Link-Local Address）]** フィールドが有効になっています。
ファブリック インターフェイスの番号付け	IPv6 アンダーレイは、p2p ネットワークのみをサポートします。したがって、**[ファブリック インターフェイスの番号付け（Fabric Interface Numbering）]** ドロップダウン リストは無効になっています。
アンダーレイ サブネット IPv6 マスク（Underlay Subnet IPv6 Mask）	ファブリック インターフェイスの IPv6 アドレスのサブネット マスクを指定します。

フィールド	説明
アンダーレイ ルーティング プロトコル	ファブリックで使用される IGP を指定します。VXLANv6 の場合、OSPFv3 または IS-IS です。
IPv6 アンダーレイの有効化（Enable IPv6 Underlay）	**[IPv6 アンダーレイの有効化（Enable IPv6 Underlay）]** チェックボックスをオンにします。
IPv6 リンクローカル アドレスを有効にする	**[IPv6 リンク ローカル アドレスを有効にする（Enable IPv6 Link-Local Address）]** チェックボックスをオンにして、リーフスパイン インターフェイスとスパイン ボーダー インターフェイス間のファブリックでリンクローカル アドレスを使用します。このチェックボックスをオンにすると、**[アンダーレイ サブネット IPv6 マスク（Underlay Subnet IPv6 Mask ）]**フィールドは編集できなくなります。デフォルトでは、**[IPv6 リンク ローカル アドレスを有効にする（Enable IPv6 Link-Local Address）]** フィールドが有効になっています。 IPv6 アンダーレイは、**p2p** ネットワークのみをサポートします。したがって、**[ファブリック インターフェイスの番号付け（Fabric Interface Numbering）]** ドロップダウン リストは無効になっています。
アンダーレイ サブネット IPv6 マスク（Underlay Subnet IPv6 Mask）	ファブリック インターフェイスの IPv6 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	ファブリックで使用される IGP を指定します。VXLANv6 の場合、OSPFv3 または IS-IS です。

7. **[レプリケーション（Replication）]** タブに移動します。マルチキャスト レプリケーション モードの IPv6 アンダーレイを構成するためのフィールドは次のとおりです。

フィールド	説明
レプリケーション モード	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 [入力レプリケーション（Ingress Replication）] または [マルチキャスト レプリケーション（Multicast replication）] です。[入力レプリケーション（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。マルチキャスト レプリケーションを選択すると、入力レプリケーション 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。 IPv4 または IPv6 のテナント ルーテッド マルチキャスト（TRM）のレプリケーション モードとして **[マルチキャスト（Multicast）]** を選択します。 IPv4 使用例の詳細は、「データ センター VXLAN EVPN テンプレートを使用した VXLAN EVPN ファブリックの作成」を参照してください。 IPv6 の使用例の詳細については、「PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN EVPN ファブリックの構成」を参照してください。
IPv6 マルチキャスト グループ サブネット	プレフィックス範囲が 112 ~ 126 の IPv6 マルチキャスト アドレスを入力します。

フィールド	説明
IPv4 テナント ルーテッド マルチキャスト（TRM）の有効化	VXLAN EVPN ファブリックで EVPN/MVPN を介してオーバーレイ IPv4 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 IPv4 を使用したテナント 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。
IPv6 テナント ルーテッド マルチキャスト（TRM）の有効化	VXLAN EVPN ファブリックで EVPN/MVPN を介してオーバーレイ IPv6 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 IPv6 を使用したテナント 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 IPv6 アドレス	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（Multicast Group Subnet ）]** 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、Configuring Tenant Routed Multicast の「Overview of Tenant Routed Multicast」の項を参照してください。
TRM VRF のデフォルト MDT IPv6 アドレス	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 **[IPv6 マルチキャスト グループ サブネット（IPv6 Multicast Group Subnet ）]** 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、**[IPv6 マルチキャスト グループ サブネット（IPv6 Multicast Group Subnet）]** で指定した IP プレフィックスから選択された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、Configuring Tenant Routed Multicast の「Overview of Tenant Routed Multicast」の項を参照してください。
MVPN VRI ID 範囲	NDFC 12.2.2 以降、vPC ごとに一意の MVPN VRI ID を割り当てるには、このフィールドを使用します。 このフィールドは、次の使用例で必要です。 • VLAN モードなしのレイヤ 3 VNI で VXLANv4 アンダーレイを設定し、TRMv4 または TRMv6 を有効にします。 • VXLANv6 アンダーレイを構成し、TRMv4 または TRMv6 を有効にします。 MVPN VRI ID は、マルチサイト ファブリック内で VRI IDは 、MSD 内のすべてのサイト内で一意である 必要があります。
MVPN VRI ID の再割り当ての有効化	NDFC リリース 12.2.2 以降では、このチェックボックスを有効にして、ワンタイム VRI ID の再割り当てを生成します。NDFC は、該当する各スイッチに対して、上記の MVPN VRI ID 範囲内で新しい MVPN ID を自動的に割り当てます。これは 1 回限りの操作であるため、操作の実行後、このフィールドはオフになります。 VRI ID の変更は中断を伴うため、それに応じて計画してください。

8. **[VPC]** タブに移動します。

フィールド	説明
vPC ピア キープ アライブオプション	**[管理（management）]** または **[ループバック（loopback）]** 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には、**管理**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には、PKA のために使用される、アンダーレイ ルーティング ループバック（IPv6 アドレスを持つ）を選択します。どちらのオプションも IPv6 アンダーレイでサポートされています。

9. **[プロトコル（Protocols）]** タブに移動します。

フィールド	説明
アンダーレイ エニーキャスト ループバック ID	IPv6 アンダーレイのアンダーレイ エニーキャスト ループバック ID を指定します。IPv6 アドレスはセカンダリとして構成できないため、追加のループバック インターフェイスが各 vPC デバイスに割り当てられます。その IPv6 アドレスが VIP として使用されます。

10. **[リソース（Resources）]** タブに移動します。

フィールド	説明
アンダーレイ IP アドレスの手動割り当て（Manual Underlay IP Address Allocation）	ダイナミック アンダーレイ IP アドレス割り当てを無効にするには、このチェックボックスをオンにします。動的アンダーレイ IP アドレス フィールドは無効になっています。
アンダーレイ ルーティング ループバック IPv6 範囲	プロトコル ピアリングのループバック IPv6 アドレスを指定します。
アンダーレイ VTEP ループバック IPv6 範囲	VTEP のループバックIPv6 アドレスを指定します。
アンダーレイ サブネット IPv6範囲（Underlay Subnet IPv6 Range）	番号付きおよびピアリンク SVI の IP を割り当てる IPv6 アドレス範囲を指定します。このフィールドを編集するには、**[IPv6 リンクローカル アドレスの有効化（Enable IPv6 Link-Local Address）]** チェックボックスをオフにします（**[全般パラメータ（General Parameters）]** タブ ）。
IPv6 アンダーレイの BGP ルータ ID 範囲（BGP Router ID Range for IPv6 Underlay）	BGP ルータ ID を割り当てるアドレスの範囲を指定します。ルーターに使用される IPv4 アドレッシングは、BGP およびアンダーレイ ルーティング プロトコル用です。

11. **[ブートストラップ（Bootstrap）]** タブに移動します。

フィールド	説明
ブートストラップの有効化	**[ブートストラップの有効化（Enable Bootstrap）]** チェックボックスをオンにします。このチェックボックスが選択されていない場合、このタブの他のフィールドは編集できません。

フィールド	説明
ローカル DHCP サーバの有効化	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、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した場合にのみ、**[DHCP 範囲開始アドレス（DHCP Scope Start Address）]** および **[DHCP 範囲終了アドレス（DHCP Scope End Address）]** フィールドが編集可能になります。
DHCP バージョン	ドロップダウン リストから **[DHCPv4]** を選択する必要があります。

12. **[Advanced]** タブまで移動します。

フィールド	説明
L3VNI（VLAN なし）の許可	NDFC リリース 12.2.2 以降では、VLAN を構成せずにレイヤ 3 VNI を構成できるようにするには、このチェックボックスをオンにします。
TCAM 割り当ての有効化	TRMv6 を有効にする場合に 768 以上に TCAM を割り当てるには、このオプションをオンにします。|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。 詳細については、「PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN EVPN ファブリックの構成」を参照してください。

13. **[保存（Save）]** をクリックし、ファブリックの作成を完了します。

次の作業：「LAN 動作モードのスイッチの追加」の「ファブリックへのスイッチの追加」の項を参照してください。

PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN EVPN ファブリックの構成

PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN EVPN ファブリックの作成について

NDFC 12.2.2 リリース以降、NDFC は次をサポートします。

- アンダーレイでの Protocol Independent Multicast（PIM）IPv6 を使用した VXLAN EVPN ファブリックの構成（PIMv6）
- 同じサブネット内または異なるサブネット内の送信者と受信者間、または仮想トンネルエンドポイント（VTEP）間でマルチキャストトラフィックを転送するためのテナント ルーテッド マルチキャスト（TRM）IPv6 の構成

この機能は、次のファブリック タイプを作成または編集する場合にサポートされます。

- データセンター VXLAN EVPN ファブリック
- BGP（eBGB EVPN）ファブリック
- VXLAN EVPN マルチサイト ファブリック

ここでは、PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN EVPN ファブリックの構成について説明します。

- PIMv6 アンダーレイと TRMv6 を使用して VXLAN EVPN ファブリックを作成する利点

- PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN ファブリックの構成でサポートされるロール
- PIMv6 アンダーレイを使用した VXLAN EVPN ファブリックでサポートされるプラットフォーム
- TRMv6 でサポートされるプラットフォーム
- 注意事項と制限事項：PIMv6 アンダーレイおよび TRMv6 を使用した VXLANv6
- データ センター VXLAN EVPN ファブリック用の PIMv6 アンダーレイおよび TRMv6 を使用した VXLANv6 の構成
- TRMv6 の構成

PIMv6 アンダーレイと TRMv6 を使用して VXLAN EVPN ファブリックを作成する利点

- マルチサイト ファブリックをサポート
- IPv6 マルチキャスト トラフィックのルーティングをサポート
- MSD メンバー ファブリックで IPv4 または IPv6 のアンダーレイ タイプをサポート
- TRM IPv6 をサポート
- すべての BGW ロールをサポート
- IPv4 または IPv6アドレスをサポート
- リンク ローカルおよび BGP 番号をサポート

PIMv6 アンダーレイおよび TRMv6 を使用した VXLAN ファブリックの構成でサポートされるロール

ファブリックタイプ	ロール（Roles）
データセンター VXLAN EVPN ファブリック	リーフ、スパイン、ボーダー、ボーダー ゲートウェイ、ボーダー スパイン、ボーダー ゲートウェイ スパイン、ToR
BGP ファブリック	リーフ、スパイン、ボーダー、ボーダー ゲートウェイ、ボーダー スパイン、ボーダー ゲートウェイ スパイン、スーパー スパイン、ボーダー スーパー スパイン、ボーダー ゲートウェイ スーパー スパイン

PIMv6 アンダーレイを使用した VXLAN EVPN ファブリックでサポートされるプラットフォーム

- BGW 向け Cisco NX-OS バージョン 10.4.3
- BGW 以外の Cisco NX-OS バージョン 1.4.2
- Cisco Nexus 9300 FX、FX2、FX3、GX、GX2、および Cisco Nexus C9332D-H2R ToR スイッチはリーフ VTEP としてサポートされます
- X9716D-GX ライン カードを持つ Cisco Nexus 9500 は、スパイン（EoR）でのみサポートされます。
- X9736C-FX ライン カードを持つ Cisco Nexus 9500 は、スパイン（EoR）でのみサポートされます。

行の最後（EoR）には、グローバル構成モードで以下のコマンドのいずれかを使用して、デフォルト以外のテンプレートを構成する必要があります。system routing template-multicast-heavy および system routing template-multicast-ext-heavy。

- ファブリック ピアリング（VMCT）は、IPv6 マルチキャスト アンダーレイではサポートされません。VMCT は、Cisco Nexus 9300 EX/FX/FX2/FX3/GX/GX2 スイッチ上の Cisco NX-OS 10.3.2 以降、および Cisco Nexus C9332D-H2R スイッチ上の Cisco NX-OS 10.4.1 以降の IPv6 入力レプリケーション（IR）アンダーレイでサポートされます。

TRMv6 でサポートされるプラットフォーム

- TRMv6
  - Cisco Nexus 9300 EX
  - Cisco Nexus 9300 FX、FX2、FX3、GX、および GX2 ToR
- BGW
  - Cisco Nexus 9300 FX3、GX、および GX2 ToR

注意事項と制限事項：PIMv6 アンダーレイおよび TRMv6 を使用した VXLANv6

VXLANv6 は次をサポートしていません。

- vPC ボーダー ゲートウェイはサポートされません。
- vPC ファブリック ピアリングにサポートはありません。
- アンダーレイ マルチキャスト RP モードの双方向転送はサポートされません。
- 双方向フォワーディング検出（BFD）にサポートはありません。
- PIMv6 hello 認証の Mp サポート。
- IR を使用した IPv6 アンダーレイの制限により、データ センター VXLAN EVPN ファブリックではどのタイプのスーパー スパイン ロールもサポートされません。
- CloudSec
- プライベート VLAN（PVLAN）はサポートされていません。
- OR3F での IPv4 と IPv6 の混在はサポートされません。
- IPv6 マルチサイト ループバック インターフェイスおよび Cisco Data Center Interconnect（DCI）インターフェイス アドレス サブネット プールは、アンダーレイ タイプに基づいています。
- 子ファブリックが MSD の一部である場合、IPv4 と IPv6 の間で子ファブリックを変更することはできません。
- 子ファブリックが MSD ファブリックの一部である場合の IPv4 アドレスから IPv6 アドレスへの変更。
- DCI は入力レプリケーション（IR）を使用します。
- アンダーレイとして IR を使用する VXLANv6 は、MSD ファブリックではサポートされていません。

データ センター VXLAN EVPN ファブリック用の PIMv6 アンダーレイおよび TRMv6 を使用した VXLANv6 の構成

1. IPv6 アンダーレイのデータ センター VXLAN EVPN ファブリックを作成または編集します。詳細については、「IPv6 アンダーレイを使用した VXLAN EVPN ファブリックの作成」を参照してください。
2. **[一般パラメータ（General Parameters）]** タブに移動し、**[IPv6 アンダーレイの有効化（Enable IPv6 Underlay）]** および **[IPv6 リンク - ローカル アドレスの有効化（Enable IPv6 Link-Local Address）]** オプションをオンにします。詳細については、「データ センター VXLAN EVPN テンプレートを使用した VXLAN EVPN ファブリックを作成する」の「一般パラメータ」の項を参照してください。

3. TRMv4 または TRMv6 を構成する場合は、**[レプリケーション（Replication）]** タブに移動し、次のフィールドを有効にします。
   - **IPv4 テナント ルーテッド マルチキャスト（TRM）の有効化**
   - **IPv6 テナント ルーテッド マルチキャスト（TRMv6）の有効化**
   - **MVPN VRI ID 範囲**

     詳細については、「データ センター VXLAN EVPN テンプレートを使用した VXLAN EVPN ファブリック を作成する」の「レプリケーション」の項を参照してください。
4. **[詳細（Advanced）]** タブに移動し、**[VXLAN あり/なしの L3 の許可（Allow L3 VNIw/o VXLAN）]** オプションを有効にします。
5. TRMv6 を有効にする場合は、**[TCAM 割り当ての有効化（Enable TCAM Allocation）]** オプションをオンにします。

   TCAM リージョンを TRMv6 に割り当てる必要があります。これには、接続されているスイッチのリロードが必要です。

   詳細については、「データ センター VXLAN EVPN テンプレートを使用した VXLAN EVPN ファブリック を作成する」の「詳細情報」の項を参照してください。
6. **[保存（Save）]** をクリックし、ファブリックの作成を完了します。

TRMv6 の構成

1. VRF を作成または編集します。詳細については、「LAN 動作モード設定のファブリックの概要」の「VRF の作成」の項を参照してください。
2. **[TRM]** タブに移動し、TRMv4 または TRMv6 のどちらを有効にするかに応じて必須フィールドに入力します。

   TCAM リージョンを TRMv6 に割り当てる必要があります。これには、接続されているスイッチのリロードが必要です。
3. VRF を作成するには **[作成（Create）]** を、VRF を破棄するには **[閉じる（Close）]** をクリックします。

著作権

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

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

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

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

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

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

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

Cisco およびCisco のロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。

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