ファブリック

LAN ファブリック

このマニュアルでは、次の用語を使用しています。

- グリーンフィールド展開：新しい VXLAN EVPN ファブリックおよび eBGP ベースのルーテッド ファブリックのプロビジョニングに適用されます。
- ブラウンフィールド展開：既存の VXLAN EVPN ファブリックに適用されます。
  - Easy_Fabric ファブリック テンプレートを使用して、CLI で設定された VXLAN EVPN ファブリックを Nexusダッシュボード ファブリック コントローラ に移行します。
  - Easy_Fabric ファブリック テンプレートを使用した Nexusダッシュボード ファブリック コントローラ Cisco への NFM 移行。

アップグレードについては、『*Cisco Nexus*ダッシュボードファブリック コントローラ *Installation and Upgrade Guide for LAN Controller Deployment*』を参照してください。

次の表では、**LAN > [ファブリック（Fabrics）]** で表示されるフィールドを説明します。

フィールド	説明
Fabric Name（ファブリック名）	ファブリックの名前を表示します。
ファブリック テクノロジー	ファブリック テンプレートに基づくファブリック テクノロジーを表示します。
ファブリックタイプ	ファブリックのタイプ（スイッチ ファブリック、LANモニタ、または外部）を表示します。
ASN	ファブリックの ASN を表示します。
ファブリック ヘルス	ファブリックのヘルスを表示します。

次の表に、[アクション（Actions）] メニューのドロップダウンリストで、**[LAN] > [ファブリック（Fabrics）]**に表示されるアクション項目を示します。

アクション項目	説明
ファブリックの作成	[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。手順については、ファブリックの作成 （6 ページ）を参照してください。
ファブリックの編集	編集するファブリックを選択します。[アクション（Actions）] ドロップダウン リストから、**[ファブリックの編集（Edit Fabric）]** を選択します。必要な変更を行って、**[保存（Save）]** をクリックします。変更を廃棄するには **[閉じる（Close）]** をクリックします。
ファブリックを削除	削除するファブリックを選択します。ドロップダウン リストから、**[ファブリックの削除（Delete Fabric）]** を選択します。**[確認（Confirm）]** をクリックして、ファブリックを削除します。

ここでは、次の内容について説明します。

ファブリック サマリ

[ファブリック（Fabric）] をクリックして、サイド キック パネルを開きます。次のセクションでは、ファブリックの概要を表示します。

ヘルス：ファブリックのヘルスを示します。

アラーム：カテゴリに基づいてアラームを表示します。

ファブリック情報：このセクションでは、ファブリックに関する基本情報を提供します。

インベントリ：このセクションでは、スイッチの設定とスイッチの状態に関する情報を提供します。

右上隅にある**[起動（Launch）]**アイコンをクリックして、ファブリックの概要を表示します。

ファブリックを作成するための前提条件

- vSphereクライアントのESXiホスト設定を更新して、無差別モードでの変更の上書きを受け入れます。詳細については、「無差別モードでの変更のオーバーライド」を参照してください。
- Nexus Dashboardで永続IPアドレスを設定します。詳細については、『*Cisco Nexus Dashboard User Guide*』の「Cluster Configuration」の項を参照してください。

ファブリック テンプレートの概要

次の表に、ファブリック テンプレートの概要に関する情報を示します。

ファブリックのテンプレート	[説明（Description）]	詳細な手順
Easy_Fabric	IGP（OSPF、IS-IS）を使用したVXLAN BGP EVPN展開およびNexus 9000および3000スイッチへのiBGP展開用のファブリック テンプレート。IPv4とIPV6両方のアンダーレイがサポートされています。	新規 VXLAN BGP EVPN ファブリックの作成 （11 ページ）
Easy_Fabric_IOS_XE	Catalyst 9000スイッチを使用したVXLAN BGP EVPN展開用のファブリック テンプレート。	Cisco Catalyst 9000 シリーズ スイッチ向け Easy ファブリックの作成 （74 ページ）
Easy_Fabric_eBGP	Nexus 9000および3000スイッチを使用したeBGPベースのルーテッド ファブリック展開用のファブリック テンプレート。このテンプレートは、アンダーレイ プロトコルとオーバーレイ プロトコルの両方として使用されるeBGPを使用したeBGP VXLAN BGP EVPN展開もサポートします。	eBGPベースのアンダーレイを使用した eBGP の新しい VXLAN EVPN の作成

ファブリックのテンプレート	[説明（Description）]	詳細な手順
External_Fabric	Nexus および Nexus 以外のデバイスをサポートするファブリック テンプレート。非 Nexus デバイスのサポートには、他の Cisco デバイス（IOS-XE、IOS-XR）およびサードパーティのスイッチが含まれます。このテンプレートには、コア ルータとエッジ ルータの BGP 構成を管理する機能があります。このテンプレートの使用例としては、以下のものがあります。クラシック階層 2/3 層 vPC またはファブリック パスのようなネットワーク、Nexus 3k/9k 以外の Nexus スイッチの VXLAN EVPN 展開、コア/エッジ デバイスでの VRF-Lite、および監視モードでの NDFC の使用（監視モードを試してから、最終的に管理モードに移行したい場合に有用）。	外部ファブリックの作成 （87 ページ）
LAN_Classic	従来の 2 または 3 層、vPC やファブリック パス データセンター トポロジを含む、さまざまな Nexus ベースのグリーンフィールドおよびブラウンフィールドの展開を監視および管理するためのファブリック テンプレート。	LAN ファブリック （1 ページ）
Fabric_Group	他の LAN_Classic ファブリックを含むファブリック テンプレートにより、Classic LAN ファブリックのグループとその相互接続を視覚化できます。	LAN ファブリック （1 ページ）

ファブリックのテンプレート	[説明（Description）]	詳細な手順
LAN_Monitor	モニタリングのみを目的としてファブリック ディスカバリ ペルソナをサポートするファブリック テンプレート。Nexus Dashboard Insights（NDI）は、そのようなファブリックで動作できます。構成のプロビジョニングまたはイメージ管理はサポートされていません。	LAN ファブリック （1 ページ）
MSD_Fabric	VXLAN BGP EVPN マルチサイト ドメイン（MSD）展開用のファブリック テンプレート。これには、レイヤ 2/レイヤ 3 オーバーレイ DCI 拡張を備えた他の VXLAN BGP EVPN ファブリックを含めることができます。	MSD ファブリックの作成とメンバー ファブリックの関連付け
[IPFM_Classic]	メディア用 IP ファブリック (IPFM) の既存の展開用のファブリック テンプレート。IPFM により、メディア コンテンツ プロバイダーと放送局は、柔軟でスケーラブルな IP ベースのインフラストラクチャを使用できます。	IPFM クラシック ファブリックの作成 （113 ページ）
Easy_Fabric_IPFM	メディア用 IP ファブリック（IPFM）ファブリックのグリーンフィールド展開を容易にするファブリック テンプレート。IPFM により、メディア コンテンツ プロバイダーと放送局は、柔軟でスケーラブルな IP ベースのインフラストラクチャを使用できます。	IPFM Easy ファブリックの作成（117 ページ）

無差別モードの ESXi ネットワーキングのオーバーライド

NDFC を仮想 Nexus Dashboard（vND）インスタンス上で実行するには、外部サービス IP アドレスが指定されている Nexus Dashboard インターフェイスに関連付けられているポートグループで無差別モードを有効にする必要があります。 vND は、Nexus Dashboard 管理インターフェ

イスとデータインターフェイスで構成されています。デフォルトでは、LAN展開では、Nexus Dashboard管理インターフェイス サブネットに2つの外部サービスIPアドレスが必要です。したがって、関連付けられたポートグループの無差別モードを有効にする必要があります。インバンド管理またはエンドポイントロケータ（EPL）が有効になっている場合は、Nexus Dashboardデータ インターフェイス サブネットで外部サービスIPアドレスを指定する必要があります。また、Nexus ダッシュボードデータ/ファブリック インターフェイス ポート グループの無差別モードを有効にする必要があります。NDFC SANコントローラの場合、無差別モードは、ポート グループに関連付けられたNexus Dashboardデータインターフェイスでのみ有効にする必要があります。NDFC SAN コントローラの場合、無差別モードは、ポート グループに関連付けられたNexus Dashboardデータ インターフェイスでのみ有効にする必要があります。詳細については、Cisco Nexus ダッシュボード導入ガイドを参照してください。

手順

ステップ1 **vSphere** クライアントにログインします。

ステップ2 ESXi ホストに移動します。

ステップ3 ホストを右クリックし、**[Settings（設定）]** を選択します。

サブメニューが表示されます。

ステップ4 **[ネットワーキング（Networking）] > [仮想スイッチ（Virtual Switches）]** を選択します。

すべての仮想スイッチがブロックとして表示されます。

ステップ5 VM ネットワークの **[設定を編集（Edit Settings）]** をクリックします。

ステップ6 [セキュリティ（Security）] タブに移動します。

ステップ7 **無差別モード**の設定を次のように更新します。

- **[オーバーライド（Override）]** チェックボックスをオンにします。
- ドロップダウン リストから **[承認（Accept）]** を選択します。

ステップ8 [OK] をクリックします。

ファブリックの作成

Cisco Nexusダッシュボード ファブリック コントローラ Web UI を使用してファブリックを作成するには、次の手順を実行します。

手順

ステップ1 **[LAN] > [ファブリック（Fabrics）] > [ファブリック（Fabrics）]** の順に選択します。

ステップ 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。

ステップ 3 ファブリック名を入力し、**[テンプレートの選択（Choose Template）]** をクリックします。

LAN_Monitor テンプレートのみを使用できます。

ステップ 4 ファブリック要件に基づいて、ファブリックテンプレートのいずれかを選択し、**[選択（Select）]** をクリックします。

ステップ 5 ファブリック設定の値を指定し、**[保存（Save）]** をクリックします。

VXLAN BGP EVPN ファブリックのプロビジョニング

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

ファブリック内の境界デバイスは通常、適切なエッジ/コア/WANルータとのピアリングを介して外部接続を提供します。これらのエッジ/コア ルータは、Nexusダッシュボード ファブリック コントローラ 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ダッシュボード ファブリック コントローラ が、複数のVXLAN BGP EVPNファブリックを管理できると同時に、Multi-Site 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設定を簡単にプロビジョニングし、管理できます。

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

VXLAN BGP EVPN ファブリックを作成および展開するための Nexusダッシュボード ファブリック コントローラ GUI の機能は次のとおりです。

[LAN] > [ファブリック（Fabrics）] > [LAN ファブリック（LAN Fabris）] で、**[ファブリックの作成（Create Fabric）]** を **[アクション（Actions）]** ドロップダウン リストで選択します。

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。

[LAN] > [インターフェイス（Interfaces）]> [LAN ファブリック（LAN Fabrics）] で、**[新しいインターフェイスの作成（Create New Interface）]** を **[アクション（Actions）]** ドロップダウンリストで選択します。

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。

[LAN] > [スイッチ（Switches）] > [LAN ファブリック（LAN Fabris）] で、**[追加（Add）]** を **[アクション（Actions）]** ドロップダウン リストで選択します。

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ダッシュボード ファブリック コントローラ でファブリックからプロビジョニングを削除します。

[LAN] > [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の展開の詳細については、「ネットワークおよび「VRF」のセクションの、ネットワークの作成と VRF の作成の説明で扱われています。

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ダッシュボード ファブリック コントローラ 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ダッシュボード ファブリック コントローラ トラッカーのための **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ダッシュボード ファブリック コントローラ 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ダッシュボード ファブリック コントローラ 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ダッシュボード ファブリック コントローラ 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設定コンプライアンス チェックがトリガーされます。このボタンは以下の場合に必須ですが、それらに限定されません。
  - スイッチまたはリンクが追加された、またはトポロジが変更されたとき
  - ファブリック全体で共有する必要があるファブリック設定が変更されたとき
  - スイッチが取り外された、または削除されたとき
  - 新しい vPC のペアリングまたはペアリングの解除が実行されたとき

- デバイスのロールが変更されたとき

[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。**[設定のプレビュー（Preview Config）]** をクリックして、生成された設定をプレビューし、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、**[設定の展開（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、**[スイッチに設定を展開（Deploy config to Switches）]**オプションを選択すれば、スイッチごとの設定を展開できます。このオプションは、スイッチのローカル操作です。つまり、スイッチの予想される構成またはインテントが現在の実行構成に対して評価され、構成のコンプライアンス チェックが実行されて、スイッチが **In-Sync** または **Out-of-Sync** ステータスを取得します。スイッチが同期していない場合、ユーザには、その特定のスイッチで実行されているすべての設定のプレビューが提供されます。これらの設定は、それぞれのスイッチに対してユーザが定義した意図とは異なります。

- 永続的な設定の差分は、コマンドライン**system nve infra-vlan** *int* **force**で確認できます。永続的な差分は、スイッチにフリーフォームの設定を介してこのコマンドを展開すると、発生します。スイッチは展開時に **force** キーワードを必要としますが、Nexusダッシュボード ファブリック コントローラ 内でスイッチから取得された実行設定では **force** キーワードは表示されません。したがって、**system nve infra-vlan** *int* **force** コマンドは常に diff として表示されます。

  Nexusダッシュボード ファブリック コントローラ のインテントには次の行が含まれます：

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

  実行設定には次の行が含まれいます：

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

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

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

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

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

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

元の **hardware access-list tcam region arp-ether 256** コマンドは Nexusダッシュボード ファブリック コントローラ のポリシーとマッチしないため、この設定は **switch_freeform** ポリシーでキャプチャされます。**hardware access-list tcam region arp-ether 256 double-wide** コマンドがスイッチにプッシュされると、元の **tcam** コマンド（**double-wide** キーワードを含まないもの）は削除されます。

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

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

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

元の **tcam** コマンドが上書きされていることがわかります。

新規 VXLAN BGP EVPN ファブリックの作成

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

この手順には、IPv4 アンダーレイの説明が含まれています。IPv6 アンダーレイについては、Easy ファブリックの IPv6 アンダーレイ サポート, on page 33 を参照してください。

1. [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。

2. ファブリックの一意の名前を入力します。

   [テンプレートを選択（Choose Template）] をクリックして、ファブリックのテンプレートを選択します。

   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。

3. ファブリック テンプレートの使用可能なリストから、**Easy_Fabric** テンプレートを選択します。

   [選択（Select）] をクリックします。

   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、以降のポイントで説明します。オーバーレイおよびアンダーレイ ネットワーク パラメータは、これらのタブに含まれています。

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

4. 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。このタブのフィールドは次のとおりです。

   [BGP ASN]：ファブリックが関連付けられている BGP AS 番号を入力します。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）]：IPv6 アンダーレイ機能を有効にします。詳細については、Easy ファブリックの IPv6 アンダーレイ サポート, on page 33を参照してください。

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

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

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

   [アンダーレイ 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（Underlay Routing Protocol）]：ファブリック、OSPF、または IS-IS で使用される IGP。

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

   スパイン デバイスを RR として展開するには、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。Nexusダッシュボード ファブリック コントローラスパイン 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 つに減らす場合に、不要なルート リフレクタ デバイスをファブリックから削除します。カウントを 4 から 2 に減らすには、次の手順に従います。

   a. ドロップダウンボックスの値を 2 に変更します。

b. ルート リフレクタとして指定するスパイン スイッチを特定します。

ルート リフレクタの場合、[rr_state] ポリシーのインスタンスがスパイン スイッチに適用されます。ポリシーがスイッチに適用されているかどうかを確認するには、スイッチを右クリックし、[ポリシーの表示/編集（View/edit policies）] を選択します。[ポリシーの表示/編集（View/Edit Policies）] 画面の [テンプレート（Template）] フィールドで [rr_state] を検索します。画面に表示されます。

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

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

d. ファブリック トポロジ ウィンドウで [Config の展開（Deploy Config）] をクリックします。

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

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

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

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

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

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

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

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

[テナント ルーテッド マルチキャスト（TRM）の有効化（Enable Tenant Routed Multicast（TRM））]：VXLAN BGP EVPN ファブリックで EVPN/MVPN を介してオーバーレイ マルチキャスト トラフィックをサポートできるようにするテナント ルーテッド マルチキャスト（TRM）を有効にするには、このチェックボックスをオンにします。

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

詳細については、テナント ルーテッド マルチキャストの概要, on page 33を参照してください。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   特定の vPC で アドバタイズ PIP 機能をイネーブルにすることもできます。.

   [すべての vPC ペアに同じ vPC ドメイン ID を有効にする（Enable the same vPC Domain Id for all vPC Pairs）]：すべての vPC ペアに同じ vPC ドメイン ID を有効にします。このフィールドを選択すると、[vPC ドメイン ID（vPC Domain Id）] フィールドが編集可能になります。

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

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

   [ファブリック vPC ピアリングの QoS を有効にする（Enable QoS for Fabric vPC-Peering）]：スパインの QoS を有効にして、vPC ファブリック ピアリング通信の配信を保証します。.

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

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

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

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

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

   [アンダーレイ エニーキャスト ループバック ID（Underlay Anycast Loopback Id）]：ループバック インターフェイス ID はグレー表示され、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（Underlay Routing Protocol Tag）]：ネットワークのタイプを定義するタグです。

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

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

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

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

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

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

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

[IS-IS ネットワーク ポイントツーポイントの有効化（Enable IS-IS Network Point-to-Point）]：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（Enable IS-IS Authentication）]：IS-IS 認証を有効にするには、チェックボックスをオンにします。無効にするにはチェックボックスをオフにします。このフィールドを有効にすると、IS-IS 認証フィールドが有効になります。

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

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

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

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

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

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

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

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

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

[PIM Hello 認証の有効化（Enable PIM Hello Authentication）]：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 Authentication Key）]：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。

a. スイッチに SSH 接続します。

b. 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。

c. 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（Enable BFD）]：ファブリック内のすべてのスイッチで機能 [bfd] を有効にするには、このチェックボックスをオンにします。この機能は、IPv4 アンダーレイでのみ有効で、範囲はファブリック内にあります。

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

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

```
feature bfd
```

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。*Nexus*ダッシュボード ファブリック コントローラ

[iBGP 向け BFD の有効化（Enable BFD for iBGP）]：iBGP ネイバーの BFD を有効にするには、このチェックボックスをオンにします。このオプションはデフォルトでは無効になっています。

[OSPF 向け BFD の有効化（Enable BFD for OSPF）]：このチェックボックスをオンにすると、OSPF アンダーレイ インスタンスの BFD が有効になります。このオプションはデ

フォルトで無効になっており、リンクステートプロトコルがISISの場合はグレー表示されます。

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

[PIM 向け BFD の有効化（Enable BFD for PIM）]：PIM の BFD を有効にするには、このチェックボックスをオンにします。このオプションはデフォルトで無効になっており、レプリケーション モードが [入力（Ingress）] の場合はグレー表示されます。

BFD グローバル ポリシーの例を次に示します。

```
router ospf <ospf tag>
   bfd

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

ip pim bfd

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

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

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

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

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

BFD 認証パラメータを取得する方法について。.

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

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

構成例では、パスワード 3 の後に 3DES パスワードが表示されます。

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

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。

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

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

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

   [オーバーレイ モード（Overlay Mode）]：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, on page 51を参照してください。

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

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

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

[デフォルトでホストインターフェイスをシャットダウンしない（Unshut Host Interfaces by Default）]：このチェック ボックスをオンにすると、デフォルトでホスト インターフェイスをシャットダウンしなくなります。

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

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

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

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

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

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

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

- CLI ベースのオーバーレイ
- 構成プロファイルベースのオーバーレイ

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

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

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

Note Cisco Nexusダッシュボード ファブリック コントローラの VXLAN OAM 機能は、単一のファブリックまたはサイトでのみサポートされます。

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

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

[NX-API の有効化（Enable NX-API）]：HTTPS での NX-API の有効化を指定します。このチェックボックスは、デフォルトでオンになっています。

[ポートの HTTP で NX-API を有効化する（Enable on NX-API on HTTP）]：HTTP 上の NX-API の有効化を指定します。HTTP を使用するには、[NX-API の有効化（Enable NX-API）] チェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。このチェックボックスをオフにすると、エンドポイント ロケータ（EPL）、レイヤ 4 ～ レイヤ 7 サービス（L4 ー L7 サービス）、VXLAN OAM など、NX-API を使用し、Cisco 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。 Nexusダッシュボード ファブリック コントローラ

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

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

[厳密な構成コンプライアンスの有効化（Enable Strict Config Compliance）]：このチェックボックスをオンにして、厳密な構成コンプライアンス機能を有効にします。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（Enable AAA IP Authorization）]：IP 認証がリモート認証サーバ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Nexusダッシュボード ファブリック コントローラをサポートするために必要で、カスタマがスイッチにアクセス可能な IP アドレスの厳密なコントロールをもつ場合のシナリオで必要です。

[NDFC をトラップ ホストとして有効化（Enable NDFC as Trap Host）]：Nexusダッシュボード ファブリック コントローラ を SNMPトラップの宛先として有効にするには、このチェックボックスをオンにします。通常、ネイティブ HA の導入では、スイッチの eth1 VIP IP アドレスが SNMP トラップ宛先として構成されます。Nexusダッシュボード ファブリック コントローラデフォルトでは、このチェックボックスは有効になっています。

[エニーキャストボーダーゲートウェイのアドバタイズ-pip（Anycast Border Gateway advertise-pip）]：エニーキャスト ボーダー ゲートウェイの PIP を VTEP としてアドバタイズできるようにします。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（Greenfield Cleanup Option）]：Preserve-Config=No でインポートされたスイッチのスイッチ クリーンアップ オプションを有効にします。Nexusダッシュボード ファブリック コントローラこのオプションは、通常、スイッチのクリーンアップ時間を短縮するために、Cisco Nexus 9000v スイッチを使用するファブリック環境でのみ推奨されます。グリーンフィールド導入の推奨オプションは、ブートストラップを使用するか、または再起動によるクリーンアップです。つまり、このオプションはオフにする必要があります。

[精密時間プロトコル（PTP）の有効化（Enable Precision Time Protocol (PTP)）]：ファブリック全体で PTP を有効にします。このチェックボックスをオンにすると、PTP がグローバルに有効になり、コアに面するインターフェイスで有効になります。また、**[PTP 送信元ループバック ID（PTP Source Loopback Id）]** および **[PTP ドメイン ID（PTP**

Domain Id）] フィールドが編集可能になります。詳細については、「PTP情報」を参照してください。Easy ファブリック向け高精度時間プロトコル, on page 46

[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作成元のユーザ定義ループバックと同じにすることができます。Nexusダッシュボード ファブリック コントローラ

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、『External/WAN Layer 3 Connectivity for VXLAN BGP EVPN Fabrics』の MPLS SR および LDP ハンドオフ 章を参照してください。

[アンダーレイ MPLS ループバック ID（Underlay MPLS Loopback Id）]：アンダーレイ MPLS ループバック ID を指定します。デフォルト値は 101 です。

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

[デフォルト キューイング ポリシーの有効化（Enable Default Queuing Policies）]：このファブリック内のすべてのスイッチにQoSポリシーを適用するには、このチェックボックスをオンにします。すべてのスイッチに適用したQoSポリシーを削除するには、このチェックボックスをオフにし、すべての設定を更新してポリシーへの参照を削除し、保存して展開します。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 Web UI から、[操作（Operations）] > [テンプレート（Templates）] の順に選択します。Nexusダッシュボード ファブリック コントローラポリシー 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 Series NX-OS Quality of Service* コンフィグレーション ガイド』を参照してください。

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

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

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

[MACsec の有効化（Enable MACsec）]：ファブリックの MACsec を有効にします。詳細については、「MACsec の有効化」を参照してください。MACsec の有効化, on page 72

[自由形式の CLI（Freeform CLIs）]：ファブリック レベルの自由形式の CLI は、ファブリックの作成または編集中に追加できます。ファブリック全体のスイッチに適用できます。インデントなしで、実行コンフィギュレーションに表示されている設定を追加する必要があります。VLAN、SVI、インターフェイス構成などのスイッチ レベルの自由形式の構成は、スイッチでのみ追加する必要があります。詳細については、「ファブリック スイッチでのフリーフォーム設定の有効化」を参照してください。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 , on page 66を参照してください。

[リーフの自由形式の構成（Leaf Freeform Config）]：リーフ、境界、および境界ゲートウェイの役割を持つスイッチに追加する必要がある CLI です。

[スパイン自由形式の構成（Spine Freeform Config）]：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 スパインのロールを持つスイッチに追加する必要がある CLI を追加します。

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

9. [リソース（Resources）] タブをクリックします。

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

- デフォルトでは、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。Nexusダッシュボードファブリック コントローラ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（Underlay Routing Loopback IP Range）]：プロトコル ピアリングのループバック IP アドレスを指定します。

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

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

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

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

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

[アンダーレイ ルーティング ループバック IPv6 範囲（Underlay Routing Loopback IPv6 Range）：Loopback0 IPv6 アドレス範囲を指定します。

Underlay VTEP Loopback IPv6 Range：Loopback1およびAnycast Loopback IPv6 Address Range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（Layer 2 VXLAN VNI Range）] および [レイヤ 3 VXLAN VNI 範囲（Layer 3 VXLAN VNI Range）]：ファブリックの VXLAN VNI ID を指定します。

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

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

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

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

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

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

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

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

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

a. L2 範囲を更新し、[保存（Save）] をクリックします。

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

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

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

10. **管理能力（Manageability）** タブをクリックします。

このタブのフィールドは次のとおりです。

[インバンド管理（Inband Management）]：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、**[設定（Settings）] > [サーバー設定（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、Easy ファブリックでのインバンド管理とインバンド POAP, on page 141を参照してください。

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

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

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

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

[Syslog サーバの重大度（Syslog Server Severity）]：syslog サーバごとに 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。高い重大度を指定するには、大きい数値を入力します。

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

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

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

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

[ブートストラップの有効化（Enable Bootstrap）]：ブートストラップ機能を有効にします。ブートストラップは easy day-0 のインポートを可能にし、既存のファブリックで新規デバイスを立ち上げることができます。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、Easy ファブリックでのインバンド管理とインバンド POAP, on page 141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（External DHCP Server）：[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）] および [スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）] フィールドに外部 DHCP サーバに関する情報を入力します。
- ローカル DHCPサーバ（Local DHCP Server）：[ローカル DHCP サーバ（Local DHCP Server）] チェックボックスをオンにして、残りの必須フィールドに詳細を入力します。

ローカル DHCP サーバの有効化（Enable Local DHCP Server）：ローカル DHCP サーバを介した自動IPアドレス割り当ての有効化を開始するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、**[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。

[DHCP バージョン（DHCP Version）]：このドロップダウンリストから [DHCPv4] または [DHCPv6] を選択します。DHCPv4 を選択すると、**[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]** フィールドが無効になります。DHCPv6 を選択すると、**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** は無効になります。

Note Cisco Nexus 9000 および 3000 シリーズ スイッチは、スイッチがレイヤ 2 隣接（eth1 またはアウトオブバンド サブネットが /64 である必要がある）、または一部の IPv6 /64 サブネットにある L3 隣接である場合にのみ、IPv6 POAP をサポートします。/64 以外のサブネット プレフィックスはサポートされません。

[DHCP スコープ開始アドレス（DHCP Scope Start Address）] および [DHCP スコープ終了アドレス（DHCP Scope End Address）]：スイッチのアウトオブバンド POAP に使用される IP アドレス範囲の最初と最後の IP アドレスを指定します。

[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]：スイッチの管理 VRF のデフォルト ゲートウェイを指定します。

スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）：スイッチの Mgmt0 インターフェイスのプレフィックスを指定します。プレフィックスは 8 ～ 30 の間である必要があります。

DHCP スコープおよび管理デフォルト ゲートウェイ *IP* アドレスの仕様（*DHCP scope and management default gateway IP address specification*）：管理デフォルト ゲートウェイ IP アドレスを 10.0.1.1 に、サブネット マスクを 24 に指定した場合、DHCP スコープが指定したサブネット、10.0.1.2 ～ 10.0.1.254 の範囲内であることを確認してください。

[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]：スイッチの Mgmt0 インターフェイスの IPv6 プレフィックスを指定します。プレフィックスは 112 ー 126 の範囲で指定する必要があります。このフィールドは DHCP の IPv6 が有効な場合に編集できます。

[AAA 構成の有効化（Enable AAA Config）]：ブートストラップ後のデバイス起動構成の一部として [管理可能性（Manageability）] タブから AAA 構成を含めます。

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

スコープの形式は次の順で定義する必要があります。

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

例：10.6.0.2、10.6.0.9、16.0.0.1、24

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

running-config をコピーして **[フリーフォームの設定（freeform config）]** フィールドに、NX-OS スイッチの実行設定に示されているように、正しいインデントでコピーアンドペーストします。freeform config は running config と一致する必要があります。詳細については、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 , on page 66を参照してください。

12. [構成のバックアップ（Configuration Backup）] タブをクリックします。このタブのフィールドは次のとおりです。

    [毎時ファブリック バックアップ（Hourly Fabric Backu）]：ファブリック構成とインテントの毎時バックアップを有効にします。

    時間単位のバックアップは、その時間の最初の 10 分間にトリガーされます。

    [スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]：毎日のバックアップを有効にします。このバックアップは、構成のコンプライアンスによって追跡されないファブリック デバイスの実行構成の変更を追跡します。

    [スケジュール済みの時間（Scheduled Time）]：スケジュールされたバックアップ時間を 24 時間形式で指定します。[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）] チェックボックスをオンにすると、このフィールドが有効になります。

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

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

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

NDFC で保持されるファブリック バックアップの数は、**[設定（Settings）] > [サーバー設定（Server Settings）] > [LAN ファブリック（LAN Fabric）] > [ファブリックあたりの最大バックアップ数（Maximum Backups per Fabric）]**によって決定されます。

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

Note 即時バックアップをトリガーするには、次の手順を実行します。

a. **[LAN] > [トポロジ（Topology）]** を選択してください。

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

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

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

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

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

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

NetFlow がファブリック レベルで有効になっていない場合、インターフェイス、ネットワーク、または VRF レベルで NetFlow を有効にすると、エラー メッセージが生成されます。Cisco NDFC の Netflow サポートについては、Netflow サポート, on page 133 を参照してください。

[Netflow エクスポータ（Netflow Exporter）]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 エクスポータを追加します。このエクスポータは、NetFlow データの受信側です。この画面のフィールドは次のとおりです。

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

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

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

[Netflow レコード（Netflow Record）] 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 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。
- **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。この画面のフィールドは次のとおりです。

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

各 netflow モニター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。**[キャンセル（Cancel）]** をクリックして破棄します。既存のモニターを選択し、**[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。

14. [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。

eBGP アンダーレイを使用したファブリックの構成

Easy_Fabric_eBGP ファブリック テンプレートを使用して、eBGP アンダーレイを使用するファブリックを作成できます。詳細については、*eBGP* アンダーレイを使用したファブリックの構成を参照してください。

Easy ファブリックの IPv6 アンダーレイ サポート

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、**Easy_Fabric** テンプレートでのみサポートされています。詳細については、*VXLANv6* ファブリックの構成を参照してください。

テナント ルーテッド マルチキャストの概要

テナント ルーテッド マルチキャスト（TRM）は、BGP ベースの EVPN コントロール プレーンを使用する VXLAN ファブリック内でのマルチキャスト転送を有効にします。TRM は、ローカルまたは VTEP 間で同じサブネット内または異なるサブネット内の送信元と受信側の間にマルチテナント対応のマルチキャスト転送を実装します。

TRM を有効にすると、アンダーレイでのマルチキャスト転送が活用され、VXLAN でカプセル化されたルーテッド マルチキャスト トラフィックが複製されます。デフォルト マルチキャスト配信ツリー（デフォルト MDT）は、VRF ごとに構築されます。これは、レイヤ 2 仮想ネットワーク インスタンス（VNI）のブロードキャストおよび不明ユニキャスト トラフィック、およびレイヤ 2 マルチキャスト複製グループの既存のマルチキャスト グループに追加されます。オーバーレイ内の個々のマルチキャスト グループ アドレスは、複製および転送のためにそれぞれのアンダーレイ マルチキャスト アドレスにマッピングされます。BGP ベースのアプローチを使用する利点は、TRM を備えた BGP EVPN VXLAN ファブリックが、すべてのエッジ デバイスまたは VTEP に RP が存在する完全な分散型オーバーレイ ランデブー ポイント（RP）として動作できることです。

マルチキャスト対応のデータセンターファブリックは、通常、マルチキャストネットワーク全体の一部です。マルチキャスト送信元、受信側、およびマルチキャスト ランデブー ポイントはデータセンター内に存在する可能性がありますが、キャンパス内にある場合や WAN 経由で

外部から到達可能である場合もあります。TRM を使用すると、既存のマルチキャスト ネットワークをシームレスに統合できます。ファブリック外部のマルチキャスト ランデブー ポイントを活用できます。さらに、TRM では、レイヤ 3 物理インターフェイスまたはサブインターフェイスを使用したテナント対応外部接続が可能です。

詳細については、次のトピックを参照してください。

- テナント ルーテッド マルチキャストに関する注意事項と制限事項
- レイヤ 3 テナント ルーテッド マルチキャストの注意事項と制約事項
- レイヤ 2/レイヤ 3 テナント ルーテッド マルチキャスト（混合モード）の注意事項と制約事項

VXLAN EVPN マルチサイトのテナント ルーテッド マルチキャストの概要

マルチサイトを使用したテナント ルーテッド マルチキャストは、マルチサイト経由で接続された複数の VXLAN EVPN ファブリック間でのマルチキャスト転送を可能にします。

次の 2 つのユース ケースがサポートされています。

- ユース ケース 1：TRM は、さまざまなサイトの送信元と受信者に、レイヤ 2 およびレイヤ 3 マルチキャスト サービスを提供します。
- ユース ケース 2：TRM 機能を VXLAN ファブリックからファブリック外部の送信元受信者に拡張します。

TRM Multi-Site は、BGP ベースの TRM ソリューションを拡張したもので、複数の VTEP を持つ複数の TRM サイトが相互に接続して、最も効率的な方法でサイト間でマルチキャスト サービスを提供できるようにします。各 TRM サイトは独立して動作しており、各サイトのボーダー ゲートウェイは各サイトをつなぐことができます。サイトごとに複数のボーダー ゲートウェイを設定できます。特定のサイトで、BGW は EVPN および MVPN ルートを交換するために、他のサイトのルートサーバまたは BGW とピアリングします。BGW で、BGP はローカル VRF/L3VNI/L2VNI にルートをインポートし、ルートが学習された場所に応じて、それらのインポートされたルートをファブリックまたは WAN にアドバタイズします。

VXLAN EVPN マルチサイト オペレーションのテナント ルーテッド マルチキャスト

VXLAN EVPN マルチサイトでの TRM の操作は次のとおりです。

- 各サイトはエニーキャスト VTEP BGW で表されます。BGW 間での DF の選択により、パケットの重複がなくなります。
- ボーダーゲートウェイ間のトラフィックは、入力複製メカニズムを使用します。トラフィックは VXLAN ヘッダーとともにカプセル化され、その後に IP ヘッダーが続きます。
- 各サイトは、パケットのコピーを 1 つだけ受信します。
- サイト間のマルチキャスト送信元および受信者情報は、TRM が設定されたボーダー ゲートウェイ上の BGP プロトコルによって伝播されます。

- 各サイトの BGW はマルチキャスト パケットを受信し、ローカル サイトに送信する前にパケットを再カプセル化します。

VXLAN EVPN マルチサイトでの TRM のガイドラインと制限事項については、「テナント ルーテッド マルチキャストの設定」を参照してください。

Cisco Nexusダッシュボード ファブリック コントローラを使用したシングル サイト向け TRM の構成

この項では、VXLAN EVPN ファブリックが Cisco Nexusダッシュボード ファブリック コントローラを使用してすでにプロビジョニングされていることを前提としています。

手順

ステップ 1 選択した Easy ファブリックの TRM を有効にします。ファブリック テンプレートが [Easy_Fabric] の場合は、[ファブリックの概要（Fabric Overview）] > [アクション（Actions）] ドロップダウンから [ファブリックの編集（Edit Fabric）] オプションを選択します。[レプリケーション（Replication）] タブをクリックします。このタブのフィールドは次のとおりです。

[テナント ルーテッド マルチキャスト（TRM）の有効化（Enable Tenant Routed Multicast（TRM））]：VXLAN BGP EVPN ファブリックで EVPN/MVPN を介してオーバーレイ マルチキャスト トラフィックをサポートできるようにするテナント ルーテッド マルチキャスト（TRM）を有効にするには、このチェックボックスをオンにします。

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

[保存（Save）]をクリックして、ファブリックの設定を保存します。この時点で、すべてのスイッチは保留状態になるため、「青色」になります。[ファブリックの概要（Fabric Overview）] > [アクション（Actions）] ドロップダウンリストから、[構成の再計算（Recalculate Config）] を選択し、[構成の展開（Deploy Config）] を選択して、次を有効にします。

- 機能 ngmvpn の有効化（Enable feature ngmvpn）：BGP ピアリング向け次世代マルチキャスト VPN（ngMVPN）コントロール パネルを有効にします。
- IP マルチキャスト マルチパス s-g-hash next-hop-based の構成（Configure ip multicast multipath s-g-hash next-hop-based）：VRF で有効化された TRM 向けマルチパス ハーシング アルゴリズムです。
- IP IGMP スヌーピング VXLAN の構成（Configure ip igmp snooping vxlan）：VXLAN VLAN の IGMP スヌーピングを有効化します。

- IP マルチキャスト overlay-spt-only の構成（Configure ip multicast Overlay-spt-only）：すべての MPVN 対応 Cisco Nexus 9000 スイッチで MVPN ルートタイプ 5 を有効にします。
- MVPN BGP AFI ピアリングの設定と確立（Configure and Establish MVPN BGP AFI Peering）：これは、BGP RR とリーフ間のピアリングに必要です。

Easy_Fabric_eBGP ファブリック テンプレートを使用して作成された VXLAN EVPN ファブリックの場合は、[EVPN] タブに [テナント ルーテッド マルチキャスト（TRM）の有効化（Enable Tenant Routed Multicast）] フィールドと [TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）] フィールドが表示されます。

ステップ 2 VRF の TRM を有効にします。

[ファブリックの概要（Fabric Overview）] > [VRF] > [VRF] に移動し、選択した VRF を編集します。[詳細（Advanced）] タブに移動し、次の TRM 設定を編集します。

TRM の有効化：TRM を有効にするためにチェックボックスを選択します。TRM を有効化する場合、RP アドレスおよびアンダーレイ マルチキャスト アドレスを入力する必要があります。

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

（注） RP が外部の場合、適切なオプションを選択します。RP が外部の場合、RP ループバック ID がグレー化されます。

RP アドレス：RP の IP アドレスを指定します。

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

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

オーバーレイ Mcast 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。

[Save] をクリックして設定を保存します。スイッチは保留状態に入り、青色になります。これらの設定で次のことが有効化されます。

- L3VNI SVI で PIM を有効にします。
- MVPN AFI のルートターゲットのインポートおよびエクスポート。
- VRF 向け RP およびその他のマルチキャスト構成。
- 分散 RP の上記の RP アドレスと RP ループバック ID を使用するループバック インターフェイス。

ステップ 3 ネットワークの TRM を有効にします。

[ファブリックの概要（Fabric Overview）] > [ネットワーク（Networks）] > [ネットワーク（Networks）] に移動します。選択したネットワークを編集し、[詳細（Advanced）] タブに移動します。次の TRM 設定を編集します。

TRM の有効化：TRM を有効にするためにチェックボックスを選択します。

[Save] をクリックして設定を保存します。スイッチは保留状態、つまり青色になります。TRM 設定により、次のことが可能になります。

- L2VNI SVI で PIM を有効にします。
- PIM ポリシーを **なし（none）** で作成して、VLAN 内の PIM ルータとの PIM ネイバーシップを回避します。**なし（none）** キーワードは、すべての ipv4 アドレスを拒否するように設定されたルートマップで、エニーキャスト IP を使用した PIM ネイバーシップ ポリシーの確立を回避します。

Cisco Nexusダッシュボード ファブリック コントローラ を使用したマルチサイト向け TRM の構成

このセクションでは、マルチサイト ドメイン（MSD）がすでに Cisco Nexusダッシュボード ファブリック コントローラによって展開されており、TRM を有効にする必要があることを前提としています。

手順

ステップ 1 BGW で TRM を有効にします。

[ファブリックの概要（Fabric Overview）] > [VRF] > [VRF] に移動します。[スコープ（Scope）] で正しい DC ファブリックが選択されていることを確認し、VRF を編集します。[Advanced] タブまで移動します。TRM 設定の編集すべての DC ファブリックとその VRF に対してこのプロセスを繰り返します。

TRM の有効化：TRM を有効にするためにチェックボックスを選択します。TRM を有効化する場合、RP アドレスおよびアンダーレイ マルチキャスト アドレスを入力する必要があります。

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

（注） RP が外部の場合、適切なオプションを選択します。RP が外部の場合、RP ループバック ID がグレー化されます。

RP アドレス：RP の IP アドレスを指定します。

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

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

オーバーレイ Mcast 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。

[TRM BGW MSite の有効化（Enable TRM BGW MSite）]：境界ゲートウェイ マルチサイトで TRM を有効にするには、このチェックボックスをオンにします。

[保存（Save）] をクリックして、設定を保存します。スイッチは保留状態に入り、青色になります。これらの設定で次のことが有効化されます。

- 機能 ngmvpn の有効化：BGP ピアリング向け次世代マルチキャスト VPN（ngMVPN）コントロール パネルを有効にします。
- L3VNI SVIでPIMをイネーブルにします。
- L3VNI マルチキャスト アドレスを構成します。
- MVPN AFI のルートターゲットのインポートおよびエクスポート。
- VRF 向け RP およびその他のマルチキャスト構成。
- 分散 RP のループバック インターフェイス。
- レイヤ 2 VNI を拡張するためのマルチサイト BUM 入力レプリケーション方式を有効化します。

ステップ 2 BGW 間の MVPN AFI を確立します。

MSD 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）] ウィンドウを開きます。**[リンク（Link）]** を選択します。ポリシー：[オーバーレイ（Overlays）] でフィルタします。

[TRM の有効化（Enable TRM）] チェックボックスをオンにして、各オーバーレイ ピアリングを選択および編集し、TRM を有効にします。

[Save] をクリックして設定を保存します。スイッチは保留状態、つまり青色になります。TRM 設定により、BGW 間、または BGW とルート サーバ間の MVPN ピアリングが有効になります。

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、**Easy_Fabric** および **Easy_Fabric_eBGP** ファブリック テンプレートに適用されます。

（注） **Easy_Fabric_eBGP** ファブリックは、ブラウンフィールドインポートをサポートしていません。

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。機能の設定中に TCAM リージョンを更新するには、構成端末で **hardware access-list tcam ingress-flow redirect** *512* コマンドを使用します。

ファブリック vPC ピアリングの QoS

Easy_Fabric 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、ファブリックを新しく作成した場合：
  - 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 設定を作成します。
  - 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（つまり、グローバルとリンク）に適用されることを確認してください。
- QoS が無効になっている場合は、QoS ファブリック vPC ピアリングに関連するすべての設定を削除します。
- 変更がない場合は、既存の PTI を尊重します。

グリーンフィールド展開の詳細については、新規 VXLAN BGP EVPN ファブリックの作成（11 ページ）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、以下のガイドラインに注意してください。

ブラウンフィールドのシナリオ 1：

- QoS が有効で、ポリシー名が指定されている場合：

（注） QoS は、グローバル QoS およびネイバー リンク サービス ポリシーのポリシー名が、すべてのファブリック vPC ピアリング接続スパインで同じ場合にのみ有効にする必要があります。

  - ポリシー名に基づいてスイッチから QoS 設定をキャプチャし、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設定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。

（注） 生じ得る、またはエラーのために不一致が生じたユーザー構成のクロスチェックは行われず、ユーザーには差分が表示される場合があります。

ブラウンフィールドのシナリオ 2：

- QoS が有効になっていて、ポリシー名が指定されていない場合、QoS 設定は、アカウントの対象となっていない、スイッチの自由形式設定の一部です。
- ブラウンフィールドの **[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 ピアリング設定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、新規 VXLAN BGP EVPN ファブリックの作成（11 ページ）を参照してください。

フィールドと説明

スイッチの vPC ペアリング ウィンドウを表示するには、ファブリック トポロジ ウィンドウでスイッチを右クリックし、**[vPC ペアリング（vPC Pairing）]** を選択します。スイッチの vPC ペアリング ウィンドウには、次のフィールドがあります。

フィールド	説明
[仮想ピアリンクを使用（Use Virtual Peerlink）]	スイッチ間の仮想ピア リンクを有効または無効にすることができます。
スイッチ名	ファブリック内のすべてのピア スイッチを指定します。 （注） ピア スイッチをペアリングしていない場合は、ファブリック内のすべてのスイッチを表示できます。ピア スイッチをペアリングすると、vPC ペアリング ウィンドウにはピア スイッチだけが表示されます。

フィールド	説明
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。
Reason	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	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。

Procedure

ステップ 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。

ステップ 2 **Easy_Fabric** または **Easy_Fabric_eBGP** ファブリック テンプレートを使用してファブリックを選択します。

ステップ 3 **[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。

Note 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 ペアの作成、編集、またはペアリング解除を行います。ただし、このオプションは、Cisco Nexus スイッチを選択した場合にのみ使用できます。

ボーダー ゲートウェイ リーフ ロールを持つスイッチを選択すると、次のエラーが表示されます。

`<switch-name> にはネットワーク/VRF がアタッチされています（<switch-name> has a Network/VRF attached）。vPC ペアリング/ペアリング解除の前にネットワーク/VRF をデタッチしてください（Please detach the Network/VRF before vPC Pairing/Unpairing）。`

ステップ 4 **[仮想ピアリンクを使用（Use Virtual Peerlink）]** チェック ボックスをオンにします。

ステップ 5 ピア スイッチを選択し、**[推奨（Recommended）]** 列をチェックして、ペアリングが可能かどうかを確認します。

値が **true** の場合、ペアリングが可能です。推奨が **false** の場合でも、スイッチをペアリングすることは可能です。ただし、**[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。

ステップ 6 [保存（Save）] をクリックします。

ステップ 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。

ステップ 8 **[構成のプレビュー（Preview Config）]** 列のスイッチに関連するフィールドをクリックします。

そのスイッチの **[構成のプレビュー（Config Preview）]** ウィンドウが表示されます。

ステップ 9 vPC リンクの詳細が、保留中の構成と、元の構成を横に並べて表示されます。

ステップ 10 ウィンドウを閉じます。

ステップ 11 **[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

Cisco NDFC Web UI で物理ピア リンクを仮想ピア リンクに変換するには、次の手順を実行します。

Before you begin

- 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。

Procedure

ステップ 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。

ステップ 2 **Easy_Fabric** または **Easy_Fabric_eBGP** ファブリック テンプレートを使用してファブリックを選択します。

ステップ 3 **[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。

Note 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 ペアの作成、編集、またはペアリング解除を行います。ただし、このオプションは、Cisco Nexus スイッチを選択した場合にのみ使用できます。

ボーダー ゲートウェイ リーフ ロールを持つスイッチを選択すると、次のエラーが表示されます。

`<switch-name> にはネットワーク/VRF がアタッチされています（<switch-name> has a Network/VRF attached）。vPC ペアリング/ペアリング解除の前にネットワーク/VRF をデタッチしてください（Please detach the Network/VRF before vPC Pairing/Unpairing）。`

ステップ 4 **[推奨（Recommended）]** 列をチェックして、ペアリングが可能かどうかを確認します。

値が **true** の場合、ペアリングが可能です。推奨が **false** の場合でも、スイッチをペアリングすることは可能です。ただし、**[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。

ステップ 5 **[仮想ピアリンクを使用（Use Virtual Peerlink）]** チェック ボックスをオンにします。

[ペア解除（Unpair）] アイコンが **[保存（Save）]** に変わります。

ステップ 6 [保存（Save）] をクリックします。

Note **[保存（Save）]** をクリックすると、展開しなくても、スイッチ間の物理 vPC ピア リンクが自動的に削除されます。

ステップ 7 **[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。

ステップ 8 **[構成のプレビュー（Preview Config）]** 列のスイッチに関連するフィールドをクリックします。

そのスイッチの **[構成のプレビュー（Config Preview）]** ウィンドウが表示されます。

ステップ 9 vPC リンクの詳細が、保留中の構成と、元の構成を横に並べて表示されます。

ステップ 10 ウィンドウを閉じます。

ステップ 11 **[再計算して展開（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

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。

Before you begin

vPC ファブリック ピアリングを無効にする前に、物理ピア リンクを使用してスイッチを接続します。

Procedure

ステップ 1 **[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。

ステップ 2 **Easy_Fabric** または **Easy_Fabric_eBGP** ファブリック テンプレートを使用してファブリックを選択します。

ステップ 3 **[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。

Note 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 ペアの作成、編集、またはペアリング解除を行います。ただし、このオプションは、Cisco Nexus スイッチを選択した場合にのみ使用できます。

ステップ 4 **[仮想ピアリンクを使用（Use Virtual Peerlink）]** チェック ボックスをオフにします。

[ペア解除（Unpair）] アイコンが **[保存（Save）]** に変わります。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 **[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。

ステップ 7 **[構成のプレビュー（Preview Config）]** 列のスイッチに関連するフィールドをクリックします。

そのスイッチの **[構成のプレビュー（Config Preview）]** ウィンドウが表示されます。

ステップ 8 vPC ピア リンクの詳細が、保留中の構成と、元の構成を横に並べて表示されます。

ステップ 9 ウィンドウを閉じます。

ステップ 10 **[再計算して展開（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。

Easy ファブリック向け高精度時間プロトコル

[Easy_Fabric] 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ダッシュボード ファブリック コントローラの展開、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、トラフィックがこのファブリックを出るときに ttag を削除する必要があります。

PTP の構成例を次に示します。

```
feature ptp

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

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

interface Ethernet1/59 -> Core facing interface
  ptp

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

次のガイドラインは PTP で適用可能です。

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

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

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

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

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

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

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

スーパー スパイン スイッチ ロールのサポート

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

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

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

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

NDFC のスーパー スパイン スイッチのロールの特徴は次のとおりです。

- Easy ファブリックでのみサポートされます。
- Cisco NDFC リリース 12.1.1e 以降、**Easy_Fabric_eBGP** テンプレートを使用した IPv6 アンダーレイの eBGP ルーテッド ファブリックで、スーパー スパイン スイッチ ロールとボーダー スーパー スパイン スイッチ ロールもサポートされています。
- スパインとボーダーにのみ接続できます。有効な接続は次のとおりです。
  - スパインからスーパー スパインへ
  - スパインからボーダー スーパー スパインおよびボーダー ゲートウェイ スーパー スパインへ
  - スーパー スパインからボーダー リーフおよびボーダー ゲートウェイ リーフへ
- RR または RP（該当する場合）機能は、ファブリックに存在する場合、常にスーパー スパイン上で設定されます。スーパー スパインでも最大 4 つの RR および RP がサポートされます。
- ボーダー スーパー スパインおよびボーダー ゲートウェイ スーパー スパインのロールは、ファブリック間接続でサポートされます。

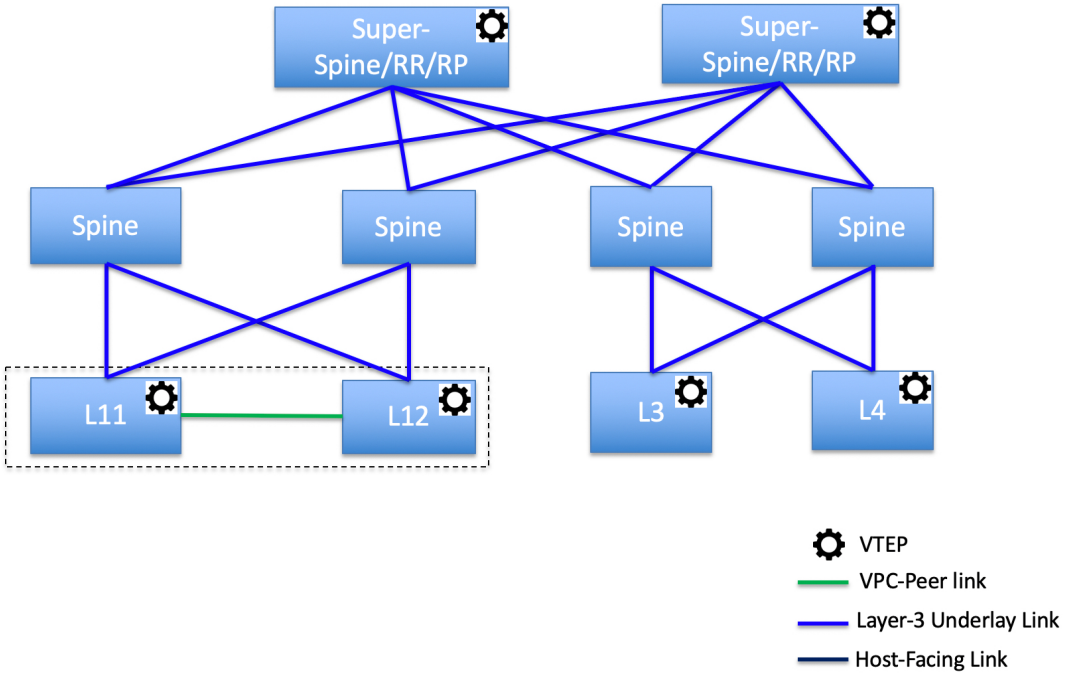
- スーパー スパインでは vPC 構成はサポートされていません。
- スーパー スパインは IPv6 アンダーレイ構成をサポートしていません。
- スイッチにスーパー スパイン ロールがある場合、スイッチのブラウンフィールドインポート中に、次のエラーが表示されます。

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

スーパー スパイン スイッチでサポートされるトポロジ

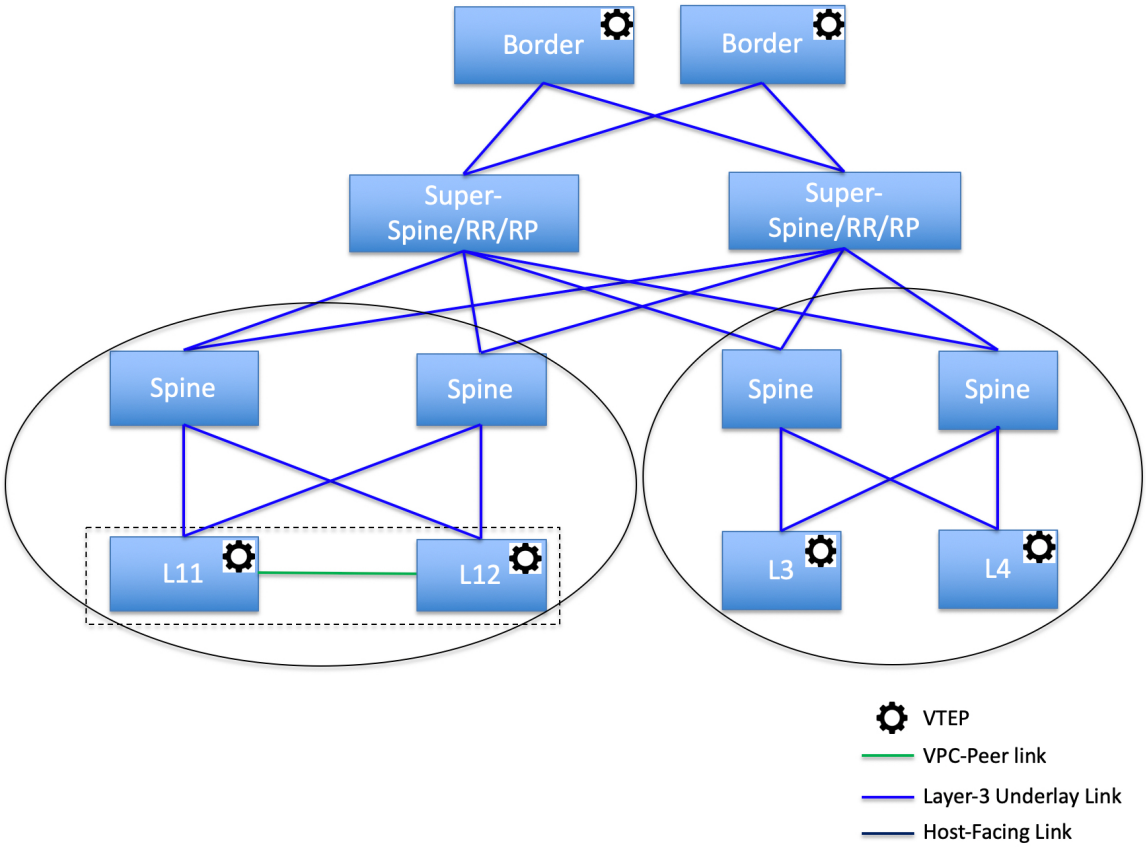
NDFC は、スーパー スパイン スイッチで次のトポロジをサポートします。

トポロジ 1：スパイン リーフ トポロジのスーパー スパイン スイッチ



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

トポロジ 2：ボーダーに接続されたスーパー スパイン スイッチ



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

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

スーパー スパイン スイッチを既存の VXLAN BGP EVPN ファブリックに追加するには、次の手順を実行します。

Procedure

ステップ 1 **[LAN]** > **[ファブリック（Fabrics）]** を選択します。必要なファブリックをダブルクリックします。

[ファブリックの概要（Fabric Overview）] ウィンドウが表示されます。

ステップ 2 **[スイッチ（Switches）]** タブで、**[アクション（Actions）]** > **[スイッチの追加（Add Switches）]** をクリックします。

詳細については、ファブリックへのスイッチの追加を参照してください。

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

Note
- ファブリックに**スーパースパイン**ロールが存在する場合、新しいデバイスにボーダー スーパー スパインとボーダー ゲートウェイ スーパー スパインのロールを割り当てることができます。
- スーパー スパインまたはそのバリエーション ロールのいずれかが割り当てられていない場合、非ボーダー スパインに接続されていれば、新しいデバイスにそのロールを割り当てることができます。**[再計算と展開（Recalculate & Deploy）]** の後、エラーが出ますが、これは以下の手順に示すように、**[解決（Resolve）]** ボタンをクリックすることで解決できます。

ステップ 4 **[ファブリックの概要（Fabric Overview）]** ウィンドウで、**[アクション（Actions）]** > **[再計算と展開（Recalculate & Deploy）]** をクリックします。

次のエラー メッセージが表示されます。

スーパー スパイン ロールは、既存のファブリックでは中断を生じさせるため許可できません。[イベント分析（Event Analytics）] に移動し、解決ボタンをクリックして続行してください。

ステップ 5 **[イベント分析（Event Analytics）]**>**[アラーム（Alarms）]**を選択し、**[ID]** をクリックします。

[アラーム ID（Alarm ID）] スライドイン ペインが表示されます。

ステップ 6 [解消（Resolve）] をクリックします。

[アクションの確認（Confirm action）] ダイアログボックスが表示されます。

ステップ 7 [確認（Confirm）] をクリックします。

ステップ 8 **[ファブリックの概要（Fabric Overview）]** ウィンドウで、**[アクション（Actions）]** > **[再計算と展開（Recalculate & Deploy）]** をクリックします。

デバイスがボーダー スパインまたはボーダー ゲートウェイ スパインに接続されている場合は、スーパー スパイン、ボーダー スーパー スパイン、またはボーダー ゲートウェイ スーパー スパインのロールを持つデバイスを追加しないでください。このアクションでは、構成を再計算して展開した後、エラーが発生します。ボーダー スパイン ロールを持つ既存のデバイスを使用するには、デバイスを削除し、適切なロールを持つデバイスを追加します。

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。MSD 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、オーバーレイ設定をスイッチに展開する前にのみ変更できます。オーバーレイ設定を展開すると、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。

（注） Cisco リリース 12.0.1a より前のリリースからアップグレードした後は、既存の設定プロファイルモードは同じように機能します。Nexusダッシュボード ファブリック コントローラ

スイッチに設定プロファイルベースのオーバーレイがある場合は、設定プロファイルオーバーレイ 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、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** としてデプロイされている場合は、**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。

アウトオブバンド スイッチ インターフェイスの構成の同期

（CLI を介して）Nexusダッシュボード ファブリック コントローラ の外部で行われたインターフェイス レベルの構成は、Nexusダッシュボード ファブリック コントローラ に同期して Nexusダッシュボード ファブリック コントローラ から管理できます。また、vPC ペア構成は自動的に検出され、ペアリングされます。これは、External_Fabric および LAN_Classic ファブリックにのみ適用されます。vPC ペアリングは **vpc_pair** ポリシーで実行されます。

（注） Nexusダッシュボード ファブリック コントローラ がスイッチを管理している場合は、すべての構成変更が Nexusダッシュボード ファブリック コントローラ から開始されることを確認し、スイッチで直接変更を行わないようにします。

インターフェイス構成が Nexusダッシュボード ファブリック コントローラ インテントに同期されると、スイッチ構成が参照と見なされます。つまり、同期アップの終了時に、スイッチに存在する内容が Nexusダッシュボード ファブリック コントローラ インテントに反映されます。再同期操作の前にそれらのインターフェイスに展開されていないインテントがある場合、それらは失われます。Nexusダッシュボード ファブリック コントローラ

ガイドライン

- Easy_Fabric、External_Fabric、および LAN_Classic テンプレートを使用するファブリックでサポートされます。
- Cisco Nexus スイッチでのみサポートされます。
- 再同期前にファブリック アンダーレイ関連ポリシーが関連付けられていないインターフェイスでサポートされます。たとえば、IFC インターフェイスとファブリック内リンクは再同期の対象になりません。
- 再同期の前に関連付けられているカスタム ポリシー（Cisco Nexusダッシュボード ファブリック コントローラ に付属していないポリシー テンプレート）がないインターフェイスでサポートされます。
- 再同期前に Cisco Nexusダッシュボード ファブリック コントローラ の機能やアプリケーションによってインテントが排他的に所有されていないインターフェイスでサポートされます。
- インターフェイス グループが関連付けられていないスイッチでサポートされます。
- インターフェイスモード（スイッチポートからルーテッド、トランクからアクセスなど）の変更は、そのインターフェイスに接続されたオーバーレイではサポートされません。

同期アップ機能は、次のインターフェイス モードおよびポリシーでサポートされます。

インターフェイス モード	ポリシー
トランク（スタンドアロン、po、および vPC PO）	• int_trunk_host • int_port_channel_trunk_host • int_vpc_trunk_host
アクセス（スタンドアロン、po、および vPC PO）	• int_access_host • int_port_channel_access_host • int_vpc_access_host
dot1q-tunnel	• int_dot1q_tunnel_host • int_port_channel_dot1q_tunnel_host • int_vpc_ dot1q_tunnel_host
ルーテッド	int_routed_host
loopback	int_freeform
sub-interface	int_subif
FEX (ST, AA)	• int_port_channel_fex • int_port_channel_aa_fex

ブレイクアウト	interface_breakout
nve	int_freeform（External_Fabric/LAN_Classic のみ）
SVI	int_freeform（External_Fabric/LAN_Classic のみ）
mgmt0	int_mgmt

Easyファブリックでは、インターフェイスの再同期によって、インターフェイス上のアクセス VLAN または許可された VLAN に基づいて、ネットワーク オーバーレイ接続が自動的に更新されます。

再同期操作が完了すると、スイッチ インターフェイスのインテントを通常の Nexusダッシュボード ファブリック コントローラ 手順で管理できます。

スイッチ インターフェイスの構成の同期

NDFCからすべてのスイッチ設定を展開することをお勧めします。一部のシナリオでは、アウトオブバンドでスイッチインターフェイスの構成を変更する必要がある場合があります。これにより、構成のずれが発生し、スイッチが同期外と報告されます。

NDFCは、アウトオブバンドインターフェイス構成を、変更を戻して同期し、そのインテントに合わせることをサポートしています。

注意事項と制約事項

次の制限は、スイッチ インターフェイス構成を NDFC に同期した後に適用されます。

- ポート チャネル メンバーシップの変更（ポリシーが存在する場合）はサポートされていません。
- オーバーレイがアタッチされているインターフェイスのモードの変更（トランクからアクセスなど）はサポートされていません。
- **インターフェイス グループ**に属するインターフェイスの再同期はサポートされていません。
- **External_Fabric** および **LAN_Classic** テンプレートの vPC ペアリングは、**vpc_pair** ポリシーで更新する必要があります。
- この機能は、Easy ファブリック、外部ファブリック、および LAN クラシック ファブリックでサポートされています。
- 再同期は一連のスイッチに対して実行でき、必要に応じて繰り返すことができます。
- **Easy_Fabric** ファブリックでは、VXLAN オーバーレイ インターフェイスのアタッチは、許可された VLAN に基づいて自動的に実行されます。

始める前に

- インターフェイスの再同期を試みる前に、ファブリックのバックアップを作成することをお勧めします。
- **External_Fabric** および **LAN_Classic** ファブリックで vPC ペアリングが正しく機能するには、両方のスイッチがファブリック内にあり、機能している必要があります。
- スイッチが**同期**しており、スイッチモードが**移行**または**メンテナンス**でないことを確認します。
- **[アクション（Actions）]** ドロップリストから**[検出（Discovery）]**>**[再検出（Rediscover）]** を選択して、NDFC が新しいインターフェイスやその他の変更を認識していることを確認します。

手順

ステップ 1 **[LAN]** > **[ファブリック（Fabrics）]**を選択し、ファブリックをダブルクリックします。

[ファブリックの概要（Fabric Overview）] ウィンドウが表示されます。

ステップ 2 **[スイッチ（Switch）]** タブをクリックして、スイッチがファブリックに存在し、vPC ペアリングが完了していることを確認します。

ステップ 3 **[ポリシー（Policies）]** タブをクリックし、インターフェイス インテントの再同期が必要な 1 つ以上のスイッチを選択します。

（注）
- スイッチのペアが **no_policy** または **vpc_pair** のいずれかを使用してすでにペアリングされている場合は、ペアの一方のスイッチのみを選択します。
- スイッチのペアがまだペアリングされていない場合は、両方のスイッチを選択します。

ステップ 4 **[アクション (Actions)]** ドロップダウンリストから **[ポリシーの追加 (Add Policy)]** を選択します。

[ポリシーの作成（Create Policy）] ウィンドウを表示します。

ステップ 5 **[ポリシーの作成（Create Policy）]** ウィンドウで、**host_port_resync** を **[ポリシー（Policy）]** ドロップダウン リストから選択します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 スイッチの **[モード（Mode）]** 列をチェックして、それらが **[移行（Migration）]** を報告していることを確認します。vPC ペアの場合、両方のスイッチが **Migration-mode** になります。

- この手順の後、**[トポロジ（Topoplogy）]** ビューのスイッチは **Migration-mode** になります。
- いずれかのスイッチを移行モードにしただけでも、vPC ペアの両方のスイッチが移行モードになります。

- スイッチが意図せずに再同期モードになった場合は、**host_port_resync** ポリシー インスタンスを識別して **[ポリシー（Policies）]** タブから削除することで、通常モードに戻すことができます。

ステップ 8 構成の変更を NDFC に同期する準備ができたら、**[スイッチ（Switches）]** タブに移動し、必要なスイッチを選択します。

ステップ 9 **[再計算と展開（Recalculate & Deploy）]** をクリックして、再同期プロセスを開始します。

（注） このプロセスは、スイッチ構成のサイズと関連するスイッチの数によっては、完了するまでに時間がかかる場合があります。

ステップ 10 再同期操作中にエラーが検出されなかった場合は、**[構成の展開（Deploy Configuration）]** ウィンドウが表示されます。インターフェイス インテントは NDFC で更新されます。

（注） External_Fabric または LAN_Classic ファブリックが**監視モード**の場合、ファブリックが読み取り専用モードであることを示すエラー メッセージが表示されます。このエラー メッセージは、再同期プロセスが失敗したことを意味するものではないため、無視してかまいません。

[構成の展開（Deploy Configuration）] ウィンドウを閉じると、スイッチが自動的に**移行モード**を終えたことが観察できます。ペアになっていなかった、または **no_policy** を使用してペアになっていた vPC ペアのスイッチは、ペアとして表示され、**vpc_pair** ポリシーに関連付けられます。

（注） スイッチ用に作成された **host_port_resync** ポリシーは、再同期プロセスが正常に完了すると自動的に削除されます。

コンフィグ コンプライアンス チェック

特定のスイッチに定義されたインテント全体または予想される構成は、NDFC に保存されます。この構成を 1 つ以上のスイッチにプッシュする場合、構成コンプライアンス（CC）モジュールがトリガーされます。CC は、現在のインテント、現在の実行構成を取得し、現在の実行構成から現在期待されている構成に移行するために必要な一連の構成を算出し、すべてが同期するようにします。

スイッチでソフトウェアまたはファームウェアのアップグレードを実行しても、スイッチの現在の実行構成は変更されません。アップグレード後、現在の実行構成が現在期待されている構成またはインテントを持っていないことを検出した場合、CC は非同期ステータスを報告します。構成の自動展開は行なわれません。展開される差分をプレビューしてから、1 つ以上のデバイスを同期状態に戻すことができます。

CC では、同期は常に NDFC からスイッチに対して行われます。逆方向の同期は行なわれません。そのため、Switchに対し、NDFC で定義されたインテントと競合するアウトオブバンドの変更を行うと、CC はこの差分をキャプチャし、デバイスが同期していないことを示します。保留中の差分は、アウトオブバンドで行われた構成を元に戻し、デバイスを同期状態に戻しま

す。アウトオブバンド変更によるこのような競合がキャプチャされるのは、デフォルトで 60 分ごとに発生する定期的なCC実行時、またはファブリックごとまたはスイッチごとにRESYNC オプションをクリックしたときであることに注意してください。Cisco NDFC リリース 12.1.1e 以降、定期的な CC は 24 時間ごとに実行されます。この間隔は、30 ～ 3600 分の範囲でカスタマイズできます。この構成は、**[サーバー（Server）] > [サーバー設定（Server Settings）] > [LAN ファブリック（LAN-Fabric）]**に移動して行うことができます。CC の REST API を使用して、スイッチ全体のアウトオブバンド変更をキャプチャすることもできます。詳細については、*Cisco NDFC REST API Guide* を参照してください。

展開される構成の使いやすさと読みやすさを向上させるために、NDFC の CC は以下のように拡張されました。

- NDFC でのすべての表示は、読みやすく理解しやすいものにされました。
- 繰り返される構成スニペットは表示されません。
- 保留中の構成には、正確に差分構成だけが表示されます。
- 並列比較による差分表示はより読みやすくなり、統合された検索またはコピー、および差分サマリー機能を備えています。

NDFC インテントが関連付けられていない、スイッチの最上位の構成コマンドでは、CC のコンプライアンス チェックは行なわれません。ただし、以下のコマンドについては、NDFCインテントがない場合でも、CC はコンプライアンス チェックを実行し、削除を試みます。

- **configure profile**
- **apply profile**
- **interface vlan**
- **interface loopback**
- **interface Portchannel**
- サブインターフェイス、例えば **interface Ethernet** *X/Y.Z*
- **fex**
- **vlan** <*vlan-ids*>

CC は、**Easy_Fabric** および **Easy_Fabric_eBGP** テンプレートが使用されている場合にのみ、コンプライアンス チェックを実行し、これらのコマンドの削除を試みます。**External_Fabric** および **LAN_Classic** テンプレートの場合、上記のコマンドも含めて、関連する NDFC インテントを持たないスイッチの最上位の設定コマンドでは、CC はコンプライアンス チェックを実行しません。

予期しない動作を避けるために、これらのコマンドをスイッチに展開する場合には、NDFCフリーフォーム構成テンプレートを使用して追加のインテントを作成することをお勧めします。

ここで、スイッチに存在する構成がインテントで定義された構成と関係していないシナリオを考えてみましょう。このような構成の例としては、インテントでキャプチャされていないがスイッチに存在する新しい機能、またはインテントでキャプチャされていない他の構成の特徴が

あります。構成コンプライアンスは、これらの構成の不一致を差分とは見なしません。このような場合、厳密な構成コンプライアンスは、インテントで定義されているすべての構成行がスイッチに存在する唯一の構成であることを保証します。ただし、厳密な CC チェックは、ブート文字列、rommon 構成、およびその他のデフォルト構成などの構成を無視します。このような場合、内部構成コンプライアンスエンジンは、これらの構成変更が差分として呼び出されないようにします。これらの差分は、**[保留中の構成（Pending Config）]** ウィンドウにも表示されません。ただし、並列比較差分ユーティリティは、2 つをテキストファイルとして差分の比較を行ないます。diff の計算で使用される内部ロジックは利用しません。その結果、デフォルト構成の差分は、**並列比較（Side-by-side Comparison）** ウィンドウで赤で強調表示されます。

NDFC では、そのような差分は、**並列比較（Side-by-side Comparison）** ウィンドウで強調表示されません。**[実行中の構成（Running config）]** ウィンドウで強調表示される自動生成されたデフォルト構成は、**[期待される構成（Expected config）]** ウィンドウには表示されません。

[保留中の構成（Pending Config）] ウィンドウに表示される構成が **[並列比較（Side-by-side Comparison）]** ウィンドウでは赤で強調表示される場合があります。これは、その構成が **[実行中の構成（Running config）]** ウィンドウには表示されるものの、**[期待される構成（Expected config）]** ウィンドウには表示されない場合です。一方、**[保留中の構成（Pending Config）]** ウィンドウに表示される構成が **[並列比較（Side-by-side Comparison）]** ウィンドウでは緑で強調表示される場合もあります。これは、その構成が **[期待される構成（Expected config）]** ウィンドウには表示されるものの、**[実行中の構成（Running config）]** ウィンドウには表示されない場合です。**[保留中の構成（Pending Config）]** ウィンドウに構成が表示されない場合、**[並列比較（Side-by-side Comparison）]** ウィンドウに赤で構成が表示されることはありません。

すべての自由形式の構成は、スイッチの **show running configuration** の出力と厳密に一致する必要があり、構成からの逸脱は、**[再計算と展開（Recalculate & Deploy）]** の際に差分として表示されます。先頭のスペースによるインデントは守る必要があります。

通常、次の方法を使用して NDFC に構成スニペットを入力できます。

- ユーザー定義のプロファイルとテンプレート
- スイッチ、インターフェイス、オーバーレイ、および vPC フリーフォーム設定
- スイッチごとのネットワークおよび VRF フリーフォーム構成
- リーフ、スパイン、または iBGP 構成のファブリック設定

注意 設定形式は、対応するスイッチの **show running configuration** と同じである必要があります。そうなっておらず、構成の先頭のスペースが欠落していたり、正しくなかったりした場合、予期しない展開エラーが発生したり、保留中の構成が予測不能な状態になったりする可能性があります。予期しない差分または展開エラーが表示された場合は、ユーザー提供またはカスタムの構成スニペットに間違った値がないか確認してください。

予期しない保留中の構成が原因でNDFCに「非同期」ステータスが表示され、この構成が展開できないか、展開後も変化がない場合は、次の手順を実行して回復します。

1. **[保留中の構成（Pending Config）]** タブ（**[構成プレビュー（Pending Config）]** ウィンドウ）で強調表示されている構成の行を確認します。
2. **[並列比較（Side-by-side Comparison）]** タブで同じ行を確認します。このタブには、「intent」または「show run」、あるいはその両方の先頭スペースが異なっていて、差分になっていた場合、それが表示されます。先頭のスペースは、**[並列比較（Side-by-side Comparison）]** タブで強調表示されます。
3. 保留中の構成または非同期状態のスイッチが、「インテント」と「実行構成」の先頭のスペースが一致しない、識別可能な構成が原因である場合、インテント側のスペースが正しくないため、編集する必要があることを示しています。
4. カスタム ポリシーまたはユーザー定義ポリシーの不適切なスペースを編集するには、スイッチに移動して対応するポリシーを編集します。
    1. ポリシーのソースが **[アンダーレイ（UNDERLAY）]** の場合、ファブリック設定画面からこれを編集し、更新された構成を保存する必要があります。
    2. ソースが空白の場合は、そのスイッチの **[ポリシーの表示/編集（View/Edit policies）]** ウィンドウから編集できます。
    3. ポリシーのソースが **[オーバーレイ（OVERLAY）]** であるが、スイッチの自由形式構成から派生している場合。この場合、適切な **[オーバーレイ（OVERLAY）]** スイッチ自由形式構成に移動して更新します。
    4. ポリシーのソースが **[オーバーレイ（OVERLAY）]** またはカスタム テンプレートの場合は、次の手順を実行します。
        1. **[設定（Settings）] > [サーバー設定（Server settings）]** を選択し、**template.in_use.check** プロパティを **false** に設定し、**[使用中テンプレートのオーバーライド（Template In-Use Override）]** チェックボックスをオフにして **[保存（Save）]** します。これにより、プロファイルまたはテンプレートを編集できるようになります。
        2. **[操作（Operations）] > [テンプレート（Templates）] > [テンプレート プロパティの編集（Edit template properties）]** 編集ウィンドウから特定のプロファイルまたはテンプレートを編集し、更新されたプロファイル テンプレートを適切なスペースを設定して保存します。
        3. **[再計算と展開（Recalculate & Deploy）]** をクリックして、影響を受けるスイッチの差分を再計算します。
        4. 構成が更新されたら、**template.in_use.check** プロパティを **true** に設定し、**[使用中テンプレートのオーバーライド（Template In-Use Override）]** チェック ボックスをオンにして **[保存（Save）]** します。これは、特に **[再計算と展開（Recalculate & Deploy）]** 操作で、NDFC システムのパフォーマンスが低下するためです。

差分が解決されたことを確認するには、ポリシーを更新した後に **[再計算と展開（Recalculate & Deploy）]** をクリックして変更を検証します。

（注） NDFC は、特に複数のコマンド シーケンスの場合、コマンドの階層を意味するものであるため、先頭のスペースのみをチェックします。NDFC は、コマンド シーケンスの末尾のスペースをチェックしません。

例 1: スイッチの自由形式ポリシーの構成コンプライアンス

スイッチの [自由形式構成（Freeform Configuration）] フィールドのスペースが正しくない例を考えてみましょう。

スイッチの自由形式ポリシーを作成します。

このポリシーがスイッチに正常に展開されると、NDFC は永続的な差分を報告します。

[並列比較（Side-by-side Comparison）] タブをクリックすると、違いの原因を確認できます。 **ip pim rp-address** 行の先頭には 2 文字のスペースがありますが、実行構成の先頭にはスペースがありません。

この相違を解決するには、対応するスイッチの自由形式ポリシーを編集して、スペースを合わせます。

保存後、**[構成のプッシュ（Push Config）]** または **[再計算と展開（Recalculate & Deploy）]** オプションを使用して差分を再計算します。

差分が解決されたことがわかります。**[並列比較（Side-by-side Comparison）]** タブで、先頭のスペースが更新されていることを確認します。

例 2：**オーバーレイ構成での先頭スペース エラーの解決**

[保留中の構成（Pending Config）] タブに表示される先頭スペース エラーの例を考えてみましょう。

[並列比較（Side-by-side Comparison）] タブで、展開された構成のコンテキストを理解するために、行ごとの差分を検索します。

一致数が 0 の場合は、NDFC がスイッチにプッシュするために評価した特別な構成であることを意味します。

実行中の構成と期待される構成の間で、先頭のスペースが一致していないことがわかります。

それぞれの自由形式の構成に移動し、先頭のスペースを修正して、更新された構成を保存します。

ファブリックの **[ファブリックの概要（Fabric Overview）]** ウィンドウに移動し、**[再計算と展開（Recalculate & Deploy）]** をクリックします。

[構成の展開（Deply Configuration）] ウィンドウで、すべてのデバイスが同期していることがわかります。

外部ファブリックでのコンプライアンスの構成

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

外部ファブリックでは、で定義されているインテントに対して、設定コンプライアンス（CC）により、このインテントが対応するスイッチに存在することが保証されます。Nexusダッシュボードファブリック コントローラこのインテントがスイッチに存在しない場合、CCはOut-of-Syncステータスを報告します。さらに、このインテントをスイッチにプッシュしてステータスを同期中に変更するために生成された保留中の設定があります。スイッチ上にあるが、で定義されたインテントではない追加の設定は、インテント内の設定との競合がない限り、CCによって無視されます。Nexusダッシュボード ファブリック コントローラ

前述のように、ユーザ定義のインテントがに追加され、同じトップレベルコマンドの下にスイッチの追加設定がある場合、CCはで定義されたインテントがスイッチに存在することのみを確認します。Nexusダッシュボード ファブリック コントローラNexusダッシュボード ファブリック コントローラこのユーザ定義インテントがスイッチから削除する目的で全体として削除され、対応する設定がスイッチに存在する場合、CCはスイッチの同期外れステータスを報告し、 config。Nexusダッシュボード ファブリック コントローラこの保留中の設定には、トップレベルのコマンドの削除が含まれています。このアクションにより、このトップレベルコマンドでスイッチで行われた他のアウトオブバンド設定も削除されます。この動作を上書きすることを選択した場合は、自由形式ポリシーを作成し、関連する最上位コマンドを自由形式ポリシーに追加することを推奨します。

この動作を例で見てみましょう。

1. ユーザがスイッチに定義し、スイッチに展開したswitch_freeformポリシー。Nexusダッシュボード ファブリック コントローラ
2. 実行コンフィギュレーションのルータbgpの下に、ユーザ定義インテントの予期される設定に存在しない追加設定があります。Nexusダッシュボード ファブリック コントローラユーザ定義のインテントなしでスイッチに存在する追加の設定を削除する保留中の設定はありません。Nexusダッシュボード ファブリック コントローラ
3. ステップ1で作成されたswitch_freeformポリシーを削除することで、によって以前にプッシュされたインテントがから削除された場合の保留中の設定とサイドバイサイド比較Nexusダッシュボードファブリック コントローラNexusダッシュボードファブリック コントローラ
4. 最上位のrouter bgpコマンドを使用してswitch_freeformポリシーを作成する必要があります。これにより、CCは以前にプッシュされた目的のサブ設定のみを削除するために必要な設定を生成できます。Nexusダッシュボード ファブリック コントローラ
5. 削除された設定は、以前にプッシュされた設定のサブセットのみです。Nexusダッシュボード ファブリック コントローラ

外部ファブリックのスイッチのインターフェイスでは、インターフェイス全体を管理するか、まったく管理しません。Nexusダッシュボード ファブリック コントローラCC は次の方法でインターフェイスをチェックします。

- 任意のインターフェイスについて、ポリシーが定義され、関連付けられている場合、このインターフェイスは管理対象と見なされます。このインターフェイスに関連付けられているすべての設定は、関連付けられたインターフェイスポリシーで定義する必要があります。これは、論理インターフェイスと物理インターフェイスの両方に適用されます。それ以外の場合、CCは、インターフェイスに行われたアウトオブバンド更新を削除して、ステータスを[In-Sync]に変更します。
- アウトオブバンドで作成されたインターフェイス（ポートチャネル、サブインターフェイス、SVI、ループバックなどの論理インターフェイスに適用）は、通常の検出プロセスの一部としてによって検出されます。Nexusダッシュボード ファブリック コントローラただし、これらのインターフェイスにはインテントがないため、CCはこれらのインターフェイスのOut-of-Syncステータスを報告しません。
- どのインターフェイスでも、モニタ ポリシーは Nexusダッシュボード ファブリック コントローラ に常に関連付けられています。この場合、CCはIn-SyncまたはOut-of-Sync設定コンプライアンスステータスを報告するときに、インターフェイスの設定を無視します。

構成コンプライアンスで無視される特別な構成 CLI

次の構成 CLI は、構成コンプライアンス チェック中に無視されます。

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

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

このような構成 CLI を展開するには、次の手順を実行します。

手順

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

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

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

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

ステップ 3 [ポリシー（Policies）] タブで、**[アクション（Actions）]** ドロップダウン リストから **[ポリシーの追加（Add Policy）]** を選択します。

ステップ 4 **switch_freeform** テンプレートを使用して、必要な構成 CLI を含むポリシー テンプレート インスタンス（PTI）を追加し、**[保存（Save）]** をクリックします。

ステップ 5 作成したポリシーを選択し、**[構成のプッシュ（Push Config）]**（**[アクション（Actions）]** ドロップダウン リスト）を選択して、構成をスイッチに展開します。

大文字と小文字を区別しないコマンドの差分の解決

デフォルトでは、インテントを比較する際にNDFCで生成されるすべての差分（予期される構成と実行構成の差分）では、大文字と小文字が区別されます。ただし、スイッチには大文字と小文字を区別しないコマンドも多くあるため、これらのコマンドで相違点が存在するとしてフラグを付けるのは適切でない場合があります。これらは、**compliance_case_insensitive_clis.txt** テンプレートに取り込まれます。これは**[操作（Operations）]** > **[テンプレート（Templates）]** の下にあります。

Cisco NDFC リリース 12.0.1a 以降、**compliance_case_insensitive_clis.txt** ファイルは、他の 2 つの **compliance_strict_cc_exclude_clis.txt** および **compliance_ipv6_clis.txt** ファイルとともに、出荷されるテンプレートの一部になりました。

すべてのテンプレートは、**[操作（Operations）]** > **[テンプレート（Templates）]** の下にあります。テンプレートを変更するには、**[使用中のテンプレートの上書き（Template In-Use Override）]** チェックボックスをオフにします（**[LAN ファブリック（LAN-Fabric）]** タブ、**[サーバー設定（Server Settings）]** ウィンドウ）。

既存の **compliance_case_insensitive_clis.txt** ファイルに含まれていない追加のコマンドは、大文字と小文字を区別するものとして扱うべきです。構成の保留が、NDFCが予期している構成と実行構成との間の大文字と小文字の違いによって生じたものである場合、次の方法で、大文字と小文字の違いを無視するように NDFC を設定できます。

1. **[使用中のテンプレートの上書き（Template In-Use Override）]** チェックボックスをオフにします（**[LAN ファブリック（LAN-Fabric）]** タブ、**[サーバー設定（Server Settings）]** ウィンドウ）。
2. **[操作（Operations）]** > **[テンプレート（Templates）]**に移動し、**compliance_case_insensitive_clis.txt** ファイルを検索します。
3. **compliance_case_insensitive_clis.txt** ファイルのサンプル エントリが表示されます。

```
[root@dcnm98 model-config]# pwd
/usr/local/cisco/dcm/dcnm/model-config
[root@dcnm98 model-config]# cat compliance_case_insensitive_clis.txt
"^(no |)interface\s+Port(.)"
"^(no |)interface\s+Loo(.)"
"^(no |)interface\s+Eth(.)"
"^update-source\s+Loo(.)"
"^vrf\s+"
"^hardware profile portmode\s+"
"^(.*)route-map\s+(.)"
"^(.*)neighbor-policy(.)"
"(no |)encapsulation\s+(.)"
"(.*)alert-group\s+(.)"
"^streetaddress\s+(.)"
"^transport email\s+(.)"
"(no |)action\s+(.)"
"(no|)\s+\d*\s+remark.*"
[root@dcnm98 model-config]#
```

4. 展開中に新しいパターンが検出され、それらが構成の保留をトリガーしている場合、これらのパターンをこのファイルに追加します。パターンは、有効な正規表現パターンである必要があります。
5. これにより、NDFC は、比較の実行中に、記述された構成パターンを大文字と小文字を区別しないものとして扱うことができます。
6. ファブリックについて、**[再計算と展開（Recalculate & Deploy）]** をクリックして、更新された比較出力を表示します。

スイッチのインポート後の構成コンプライアンスの解決

Cisco NDFC にスイッチをインポートした後、管理インターフェイス（mgmt0）の説明フィールドに余分なスペースがあるため、スイッチの構成コンプライアンスが失敗することがあります。

たとえば、スイッチをインポートする前に：

```
interface mgmt0
  description SRC=SDS-LB-LF111-mgmt0, DST=SDS-LB-SW001-Fa0/5
```

スイッチをインポートして構成プロファイルを作成したら、次の手順を実行します。

```
interface mgmt0
  description SRC=SDS-LB-LF111-mgmt0,DST=SDS-LB-SW001-Fa0/5
```

mgmt0 インターフェイスを選択した後、インターフェイスマネージャに移動し、**[編集（Edit）]** アイコンをクリックします。説明の余分なスペースを削除してください。

厳格な構成コンプライアンス

厳密な構成コンプライアンスは、スイッチ構成と関連するインテント間の相違をチェックし、スイッチに存在するが関連するインテントに存在しない構成の **no** コマンドを生成します。**[再計算と展開（Recalculate and Deploy）]** をクリックすると、関連付けられたインテントに存在しないスイッチ構成が削除されます。この機能を有効にするには、**[厳密な公正コンプライア**

ンスを有効にする（**Enable Strict Config Compliance**）**]** チェック ボックスをオンにします。これは **[**詳細設定（**Advanced**）**]** タブ（**[**ファブリックの作成（**Create Fabric**）**]** または **[**ファブリックの編集（**Edit Fabric**）**]** ウィンドウ）にあります。デフォルトで、この機能は無効になっています。

厳密な構成コンプライアンス機能は、Easy ファブリック テンプレート（**Easy_Fabric** および **Easy_Fabric_eBGP**）でサポートされています。スイッチによって自動生成されるコマンド（vdc、rmon など）について差分が生成されないようにするために、CC はデフォルトのコマンドのリストを含むファイルを使用して、これらのコマンドに対して差分が生成されないようにします。このファイルは、**[**操作（**Operations**）**]** > **[**テンプレート（**Templates**）**]**、**compliance_strict_cc_exclude_clis.txt** テンプレートで維持されます。

例：厳密な構成コンプライアンス

feature telnet コマンドがスイッチで構成されているが、インテントに存在しない例を考えてみましょう。このようなシナリオでは、CC チェックが実行された後、スイッチのステータスが **Out-of-sync** として表示されます。

次に、非同期スイッチの **[**構成のプレビュー（**Preview Config**）**]** をクリックします。厳密な構成コンプライアンス機能が有効になっているため、**[**構成のプレビュー（**Preview Config**）**]** ウィンドウの **[**保留中の構成（**Pending Config**）**]** の下に **feature telnet** コマンドの **no** 形式が表示されます。

[並べて比較（**Side-by-Side Comparison**）**]** タブには、実行構成と予想される構成の差が並べて表示されます。**[**再同期（**Re-sync**）**]** ボタンは、**[**構成のプレビュー（**Preview Config**）**]** ウィンドウの [並べて比較（Side-by-Side Comparison）] タブの右上隅にも表示されます。大規模なアウトオブバンド変更がある場合、または設定変更が NDFC に正しく登録されていない場合に、このオプションを使用して NDFC 状態を再同期します。

再同期操作は、スイッチに対して完全な CC 実行を実行し、「show run」および「show run all」コマンドをスイッチから再収集します。再同期プロセスを開始すると、進行状況メッセージが表示されます。再同期中に、実行構成がスイッチから取得されます。スイッチの Out-of-Sync/In-Sync ステータスは、NDFC で定義されたインテントに基づいて再計算されます。

次に、**[**構成のプレビュー（**Preview Config**）**]** ウィンドウを閉じ、**[**再計算と展開（**Recalculate and Deploy**）**]** をクリックします。厳密な構成コンプライアンス機能により、**feature telnet** コマンドの **no** 形式をスイッチにプッシュすることによって、スイッチの実行構成がインテントから逸脱しないようにします。構成間の差分が強調表示されます。**feature telnet** コマンド以外の差分は、デフォルトのスイッチ構成およびブート構成であり、厳密な CC チェックでは無視されます。

[ファブリックの概要（**Fabric Overview**）**]** ウィンドウでスイッチを右クリックして **[**構成のプレビュー（**Preview Config**）**]** を選択すると、**[**構成のプレビュー（**Preview Config**）**]** ウィンドウが表示されます。このウィンドウには、インテントに準拠した構成を実現するためにスイッチにプッシュする必要がある保留中の構成が表示されます。

カスタムの自由形式構成を NDFC に追加して、NDFC での目的の構成とスイッチ構成を同一にすることができます。その後、スイッチは In-Sync ステータスになります。NDFC でカスタム

の自由形式構成を追加する方法の詳細については、ファブリック スイッチでのフリーフォーム設定の有効化 （66 ページ）を参照してください。

ファブリック スイッチでのフリーフォーム設定の有効化

Nexusダッシュボード ファブリック コントローラ では、次の方法でフリーフォーム ポリシーを使用してカスタム設定を追加できます。

1. ファブリック全体
   - ファブリック内のすべてのリーフ、ボーダー リーフ、およびボーダー ゲートウェイ リーフ スイッチ。
   - すべてのスパイン、スーパー スパイン、ボーダー スパイン、ボーダー スーパー スパイン、ボーダー ゲートウェイ スパイン、およびボーダー スイッチ。
2. グローバル レベルの特定のスイッチ。
3. ネットワークごとまたは VRF レベルごとの特定のスイッチ。

リーフ スイッチは、Leaf、Border、および Border Gateway のロールによって識別されます。スパイン スイッチは、Spine、Border Spine、Border Gateway Spine、Super Spine、Border Super Spine、および Border Gateway Super Spine のロールによって識別されます。

Note 自由形式の CLI は、ファブリックを作成するときでも、ファブリックがすでに作成されているときでも展開できます。次に、既存のファブリックでの例を示します。ただし、これは新しいファブリックを作成するときでも参考にすることができます。

リーフおよびスパイン スイッチ上でのファブリック全体のフリーフォーム CLI の導入

1. **[LAN] > [ファブリック (Fabrics)] > [ファブリック (Fabrics)]** を選択します。
2. ファブリックを選択し、**[ファブリックの編集 (Edit Fabric)]** を **[アクション (Actions)]** ドロップダウン リストから選択します。

   （ファブリックを初めて作成する場合は、**[ファブリックの作成 (Create Fabric)]** をクリックします）。
3. **[詳細設定 (Advanced)]** タブをクリックし、次のフィールドを更新します。

   [リーフのフリーフォーム設定 (Leaf Freeform Config)]：このフィールドでは、ファブリック内のすべてのリーフ、ボーダー リーフ、およびボーダー ゲートウェイ リーフ スイッチの設定を追加します。

   [スパインのフリーフォーム設定 (Spine Freeform Config)]：このフィールドでは、ファブリック内のすべてのスパイン、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、およびボーダー ゲートウェイ スーパー スパイン スイッチの設定を追加します。

Note 目的の設定を正しいインデントでコピー アンド ペーストします。Nexus スイッチでの実行コンフィギュレーションを参考にしてください。詳細については、スイッチのフリーフォーム設定エラーの解決, on page 69を参照してください。

4. [保存（Save）] をクリックします。[ファブリック トポロジ (fabric topology)] 画面が表示されます。
5. **[設定の展開 (Deploy Config)]** を **[アクション (Actions)]** ドロップダウン リストからクリックし、設定を保存して展開します。

   コンフィギュレーションコンプライアンス機能により、これらのCLIで示された目的の設定がスイッチ上に確実に存在するようにします。仮にそれらが削除されるか、ミスマッチが生じた場合には、ミスマッチとしてフラグが付けられ、デバイスが同期外れであることが示されるようにします。

[不完全な設定コンプライアンス (Incomplete Configuration Compliance)]：一部の Cisco Nexus 9000 シリーズ スイッチでは、**[設定の展開 (Deploy Config)]** オプションを使用して保留中のスイッチ設定を設定しても、意図した設定とスイッチ設定の間にミスマッチが生じる場合があります。問題を解決するには、該当するスイッチに **switch_freeform** ポリシーを追加します（特定のスイッチへのフリーフォーム *CLI* の導入の項を参照）。たとえば、次の永続的な保留設定を考えてみます。

```
line vty
logout-warning 0
```

上記の設定をポリシーに追加し、更新を保存したら、トポロジ画面で **[設定の展開 (Deploy Config)]** をクリックして展開プロセスを完了します。

スイッチを同期状態に戻すには、上記の設定を **switch_freeform** ポリシーに追加し、スイッチに展開します。

特定のスイッチへのフリーフォーム CLIの導入

1. **[LAN] > [ファブリック (Fabrics)] > [ファブリック (Fabrics)]** を選択します。
2. ファブリックを選択し、**[ファブリックの編集 (Edit Fabric)]** を **[アクション (Actions)]** ドロップダウン リストから選択します。
3. **[ポリシー (Policies)]** タブをクリックします。**[アクション (Actions)]** ドロップダウンリストから **[ポリシーの追加 (Add Policy)]** を選択します。

   [ポリシーの作成 (Create Policy)] 画面が表示されます。

Note 新しいファブリックにフリーフォームのCLIをプロビジョニングするには、ファブリックを作成し、そのファブリックにスイッチをインポートしてから、フリーフォームの CLI を展開する必要があります。

4. **[プライオリティ (Priority)]** フィールドで、優先順位はデフォルトで500に設定されます。展開時に上位に表示する必要がある CLI には、（低い番号を指定して）高い優先順位を選択できます。たとえば、機能を有効にするコマンドは、コマンドリストの前に表示されます。
5. **[説明 (Description)]** フィールドに、このポリシーの説明を入力します。
6. **[テンプレート名 (Template Name)]** フィールドから、**[freeform_policy]** を選択します。
7. **[フリーフォーム CLI (Freeform Config CLI)]** ボックスで CLI を追加または更新します。

   目的の設定を正しいインデントでコピーアンドペーストします。Nexus スイッチでの実行コンフィギュレーションを参考にしてください。詳細については、スイッチのフリーフォーム設定エラーの解決, on page 69を参照してください。
8. [保存（Save）] をクリックします。

   ポリシーが保存されると、そのスイッチの目的の設定に追加されます。
9. [ファブリックの概要（Fabric Overview）] ウィンドウで、**[スイッチ（Switches）]** タブをクリックし、必要なスイッチを選択します。
10. **[スイッチ（Switch）]** タブで、**[アクション（Actions）]** ドロップダウン リストをクリックし、**[展開（Deploy）]** を選択します。

freeform_policy ポリシー設定のポインタ：

- ポリシーでは複数のインスタンスを作成できます。
- vPCスイッチペアの場合は、両方のvPCスイッチで一貫した **freeform_policy** ポリシーを作成します。
- **freeform_policy** ポリシーを編集してスイッチに展開すると、変更内容が表示されます（[プレビュー (Preview)] オプションの **[サイドバイサイド (Side-by-side)]** タブ）。

フリーフォーム CLI の設定例

コンソール ラインの設定

この例では、一部のファブリック全体のフリーフォーム設定（すべてのリーフ スイッチとスパイン スイッチ）、および個々のスイッチ設定を展開します。

ファブリック全体のセッション タイムアウトの設定：

```
line console
```

```
  exec-timeout 1
```

特定のスイッチのコンソール速度設定：

```
line console
  speed 115200
```

IP プレフィックス リスト/ルートマップ設定 (IP Prefix List/Route-map configuration)

IP プレフィックス リストおよびルートマップ設定は、通常、ボーダー デバイスで設定されます。これらの設定は、スイッチ上で一度定義し、必要に応じて複数の VRF に適用できるものであるため、グローバルです。この設定の目的は、switch_freeform ポリシーにキャプチャして保存できます。前述のように、ポリシーに保存されている設定は **show run** 出力と一致する必要があることに注意してください。これは、NX-OS スイッチが CLI で設定されたときにシーケンス番号を自動的に生成するプレフィックスリストに特に関係しています。スニペットの例を次に示します。

ACL の設定

ACL 設定は通常、ファブリック全体ではなく、特定のスイッチ（リーフ/スパイン スイッチ）で設定されます。スイッチで ACL をフリーフォーム CLIとして設定する場合は、シーケンス番号を含める必要があります。それ以外の場合は、意図した設定と実行での設定が一致しなくなります。シーケンス番号の設定例：

```
ip access-list ACL_VTY
  10 deny tcp 172.29.171.67/32 172.29.171.36/32
  20 permit ip any any
ip access-list vlan65-acl
  10 permit ip 69.1.1.201/32 65.1.1.11/32
  20 deny ip any any

interface Vlan65
  ip access-group vlan65-acl in
line vty
  access-class ACL_VTY in
```

freeform_policy ポリシーでシーケンス番号なしで ACL を設定した場合は、スイッチの実行設定に示されているようにシーケンス番号でポリシーを更新します。

ポリシーを更新して保存したら、デバイスを右クリックし、スイッチごとに**[設定の展開(Deploy Config)]** オプションを選択して設定を展開します。

スイッチのフリーフォーム設定エラーの解決

実行設定を、NX-OSスイッチの実行設定に示されているように、正しいインデントでフリーフォーム設定にコピーアンドペーストします。フリーフォームの設定は、実行設定とマッチしている必要があります。それ以外の場合、Nexusダッシュボード ファブリック コントローラの設定コンプライアンスは、スイッチを非同期としてマークします。

スイッチのフリーフォーム設定の例を見てみましょう。

```
feature bash-shell
feature telemetry
```

```
clock timezone CET 1 0
# Daylight saving time is observed in Metropolitan France from the last Sunday in March
 (02:00 CET) to the last Sunday in October (03:00 CEST)
clock summer-time CEST 5 Sunday March 02:00 5 Sunday October 03:00 60
clock protocol ntp

telemetry
  destination-profile
    use-vrf management
```

夏時間に関する強調表示された行は、**show running config** コマンドの出力には表示されないコメントです。したがって、インテントが実行設定とマッチしないため、設定コンプライアンスはスイッチを非同期としてマークします。

クロック プロトコルのスイッチの実行設定を確認します。

```
spine1# show run all | grep "clock protocol"
clock protocol ntp vdc 1
```

フリーフォームの設定に **vdc 1** がないことがわかります。

この例では、実行設定をフリーフォーム設定にコピーアンドペーストします。

更新されたフリーフォーム設定を次に示します。

```
feature bash-shell
feature telemetry

clock timezone CET 1 0
clock summer-time CEST 5 Sunday March 02:00 5 Sunday October 03:00 60
clock protocol ntp vdc 1

telemetry
  destination-profile
    use-vrf management
```

実行設定をコピーアンドペーストして展開すると、スイッチは同期されます。**[設定の再計算 (Recalculate Config)]** をクリックし、**[保留中の設定 (Pending Config)]** カラムをクリックします。**[サイドバイサイドで比較 (Side-by-Side Comparison)]** により、定義済みのインテントと実行設定の違いに関する情報を表示します。

VRF/ネットワーク単位での特定のスイッチへのフリーフォーム CLI の導入

1. **[LAN] > [ファブリック (Fabrics)] > [ファブリック (Fabrics)]** を選択します。
2. ファブリックを選択し、**[ファブリックの編集 (Edit Fabric)]** を **[アクション (Actions)]** ドロップダウン リストから選択します。
3. **[VRFs]** タブをクリックします。**[アクション (Actions)]** ドロップダウンリストから、**[作成 (Create)]** を選択します。

   [VRF の作成 (Create VRF)] 画面が表示されます。
4. 個々のスイッチを選択します。VRFアタッチメントフォームが表示され、選択したスイッチがリストされます。vPC ペアの場合、ペアに属する両方のスイッチが表示されます。

5. [CLI フリーフォーム (CLI Freeform)]列で、**[フリーフォーム設定 (Freeform config)]** というラベルのボタンを選択します。このオプションを使用すると、VRF プロファイル設定とともにスイッチに展開する追加の設定を指定できます。
6. **[フリーフォーム設定 (Free Form Config)]** CLI ボックスで CLI を追加または更新します。目的の設定を正しいインデントでコピーアンドペーストします。Nexus スイッチでの実行コンフィギュレーションを参考にしてください。詳細については、スイッチでのフリーフォーム設定エラーの解決を参照してください。
7. **[構成の展開（Deploy Config）]** をクリックします。

Note VRF ごとにスイッチごとの設定が指定されていない場合、**[フリーフォーム設定 (Freeform config)]** ボタンはグレーになります。いくつかの設定がユーザーによって保存されると、ボタンは青色になります。

ポリシーを保存したら、[VRF アタッチメント (VRF Attachment)] ポップアップで**[保存 (Save)]** をクリックして、そのスイッチにVRFを展開するインテントを保存します。スイッチ横の左側のチェックボックスがオンになっていることを確認します。

8. ここで、オプションで **[プレビュー (Preview)]** をクリックして、スイッチにプッシュされる設定を確認します。
9. **[設定の展開 (Deploy Config)]** をクリックして、設定をスイッチにプッシュします。

同じ手順を使用して、ネットワークごとに、スイッチ設定を定義できます。

Easy ファブリックおよび eBGP ファブリックでの MACsec サポート

MACsec は、ファブリック内リンクの Easy Fabric および eBGP ファブリックでサポートされます。MACsec を設定するには、ファブリックおよび必要な各ファブリック内リンクで MACsec を有効にする必要があります。CloudSec とは異なり、MACsec の自動設定はサポートされていません。

MACsec は、Cisco NX-OS リリース 7.0(3)I7(8) および 9.3(5) 以降のスイッチでサポートされます。

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）]** ウィンドウに表示されます。
- MACsec が設定されたデバイスのブラウンフィールド移行は、スイッチおよびインターフェイスの自由形式の設定を使用してサポートされます。

  サポートされているプラットフォームとリリースを含むMACsec設定の詳細については、『Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイド』の「*MACsec* の設定」の章を参照してください。

次の項では、Nexusダッシュボード ファブリック コントローラ で MACsec を有効または無効にする方法を示します。

MACsec の有効化

手順

ステップ 1 **[LAN] > [ファブリック（Fabrics）]** に移動します。

ステップ 2 既存の Easy または eBGP ファブリックで **[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。

ステップ 3 **[アドバンスト（Advanced）]** タブをクリックし、MACsec の詳細を指定します。

[MACsec の有効化（Enable MACsec）]：ファブリックの MACsec を有効にするには、このチェックボックスをオンにします。

[MACsec プライマリ キー文字列（MACsec Primary Key String）]：プライマリ MACsec セッションの確立に使用される Cisco Type 7 暗号化オクテット文字列を指定します。AES_256_CMAC の場合、キー文字列の長さは 130、AES_128_CMAC の場合、キー文字列の長さは 66 である必要があります。これらの値が正しく指定されていない場合、ファブリックの保存時にエラーが表示されます。

（注） デフォルトのキー ライフタイムは無期限です。

[MACsec プライマリ暗号化アルゴリズム（MACsec Primary Cryptographic Algorithm）]：プライマリ キー文字列に使用する暗号化アルゴリズムを選択します。**AES_128_CMAC** または **AES_256_CMAC** です。デフォルト値は **AES_128_CMAC** です。

プライマリ セッションが失敗した場合にバックアップ セッションを開始するように、デバイスのフォールバック キーを設定できます。

[MACsec フォールバック キー文字列（MACsec Fallback Key String）]：フォールバック MACsec セッションの確立に使用される Cisco Type 7 暗号化オクテット文字列を指定します。AES_256_CMAC の場合、キー文字列の長さは 130、AES_128_CMAC の場合、キー文字列の長さは 66 である必要があります。これらの値が正しく指定されていない場合、ファブリックの保存時にエラーが表示されます。

[MACsec フォールバック暗号化アルゴリズム（MACsec Fallback Cryptographic Algorithm）]：フォールバック キー文字列に使用する暗号化アルゴリズムを選択します。AES_128_CMAC または AES_256_CMAC です。デフォルト値は AES_128_CMAC です。

[MACsec 暗号スイート（MACsec Cipher Suite）]：MACsec ポリシーの次の MACsec 暗号スイートのいずれかを選択します。

- GCM-AES-128
- GCM-AES-256
- GCM-AES-XPN-128
- GCM-AES-XPN-256

デフォルト値は **GCM-AES-XPN-256** です。

（注） ファブリックの展開が完了した後、MACsec 設定はスイッチに展開されません。スイッチに MACsec 設定を展開するには、ファブリック内リンクで MACsec を有効にする必要があります。

[MACsec ステータス レポート タイマー（MACsec Status Report Timer）]：MACsec 動作ステータス定期レポート タイマーを分単位で指定します。

ステップ 4 ファブリックをクリックして、サイド キックに **[概要（Summary）]** を表示します。サイド キックをクリックして展開します。**[リンク（Links）]** タブをクリックします。

ステップ 5 MACsec を有効にするファブリック内リンクを選択し、**[アクション（Actions）]>[編集（Edit）]** の順にクリックします。

ステップ 6 **[リンク管理 - リンクの編集（Link Management – Edit Link）]** ウィンドウで、**[リンク プロファイル（Link Profile）]** セクションの **[アドバンスト（Advanced）]** をクリックし、**[MACsec の有効化（Enable MACsec）]** チェックボックスをオンにします。

MACsec がファブリック内リンクで有効になっているが、ファブリック設定では有効になっていない場合、**[保存（Save）]** をクリックするとエラーが表示されます。

MACsec がリンクで設定されると、次の設定が生成されます。

- MACsec を有効にする最初のリンクである場合は、MACsec グローバル ポリシーを作成します。
- リンクの MACsec インターフェイス ポリシーを作成します。

ステップ 7 [ファブリックのアクション（Fabric Actions）]ドロップダウンリストから、**[設定の展開（Deploy Config）]** を選択して、MACsec 設定を展開します。

MACsec の無効化

ファブリック内リンクで MACsec を無効にするには、**[リンク管理-リンクの編集（Link Management – Edit Link）]** ウィンドウに移動し、**[MACsec の有効化（Enable MACsec）]** チェックボックスをオフにして、**[保存（Save）]** をクリックします。[ファブリックのアクション

（Fabric Actions）]ドロップダウンリストから、**[設定の展開（Deploy Config）]** を選択して、MACsec 設定を無効にします。このアクションは、次を実行します。

- リンクから MACsec インターフェイスポリシーを削除します。
- これが MACsec が有効になっている最後のリンクである場合、MACsec グローバル ポリシーもデバイスから削除されます。

リンクでMACsecを無効にした後でのみ、**[ファブリックの設定（Fabric Settings）]**に移動し、**[MACsec の有効化（Enable MACsec）]** チェックボックス（**[詳細（Advanced）]**タブ）をオフにして、ファブリックでMACsecを無効にすることができます。MACsec が有効になっているファブリック内にファブリック内リンクがある場合、**[アクション（Actions）] > [設定の再計算（Recalculate Config）]**を**[ファブリックのアクション（Fabric Actions）]** ドロップダウン リストでクリックすると、エラーが表示されます。

Cisco Catalyst 9000 シリーズ スイッチ向け Easy ファブリックの作成

Easy_Fabric_IOS_XE ファブリック テンプレートを使用して、Easy ファブリックに Cisco Catalyst 9000 シリーズ スイッチを追加できますこのファブリックに追加できるのは、Cisco Catalyst 9000 IOS XE スイッチだけです。このファブリックは、アンダーレイ プロトコルとして OSPF、およびオーバーレイ プロトコルとして BGP EVPN をサポートします。このファブリック テンプレートを使用すると、Nexusダッシュボード ファブリック コントローラ でCisco Catalyst 9000 IOS-XE スイッチで構成される VXLAN EVPN ファブリックのすべての設定を管理することを許可します。このファブリックのバックアップと復元は、Easy_Fabric と同じです。

ガイドライン

- EVPN VXLAN 分散型エニーキャスト ゲートウェイは、各 SVI が同じエニーキャスト ゲートウェイ MAC で構成されている場合にサポートされます。
- StackWise Virtual がサポートされています。
- ブラウンフィールドはサポートされていません。
- 以前のバージョンからのアップグレードはサポートされていません（ただし、11.5 のプレビュー機能です）。
- IPv6アンダーレイ、VXLANマルチサイト、エニーキャストRP、およびTRMはサポートされていません。
- ISIS、入力レプリケーション、アンナンバードファブリック内リンク、4バイトBGP ASN、およびゼロタッチ プロビジョニング（ZTP）はサポートされていません。

（注） 設定のコンプライアンスについては、外部ファブリックでのコンプライアンスの構成（61 ページ） を参照してください。

Cisco Catalyst 9000 シリーズ スイッチ向け Easy ファブリックの作成

UI ナビゲーション：**[LAN] > [ファブリック（Fabrics）]** を選択します。

Cisco Catalyst 9000 シリーズ スイッチの easy ファブリックを作成するには、次の手順を実行します。

1. **[ファブリックの作成（Create Fabric）]** を **[アクション（Actions）]** ドロップダウン リストから 選択します。
2. ファブリック名を入力し、**[テンプレートの選択（Choose Template）]** をクリックします。

   [ファブリック テンプレートの選択（Select Fabric Template）] ダイアログが表示されます。
3. **Easy_Fabric_IOS_XE** ファブリック テンプレートを選択し、**[選択]** をクリックします。
4. 必要なフィールドに情報を入力し、**[保存（Save）]** をクリックします。

（注） BGP ASN は唯一の必須フィールドです。

Cisco Catalyst 9000 シリーズ スイッチを IOS-XE Easy ファブリックに追加する

Cisco Catalyst 9000 シリーズ スイッチは、SNMP を使用して検出されます。したがって、Cisco Catalyst 9000 シリーズ スイッチをファブリックに追加する前に、SNMP ビュー、グループ、およびユーザを構成する必要があります。詳細については、「検出用 IOS-XE デバイスの構成」の項を参照してください。検出用の IOS-XE デバイスの設定 （103 ページ）

StackWise Virtual スイッチの場合、ファブリックに追加する前にStackWise Virtual 関連の構成を行います。

UI ナビゲーション

次のナビゲーション パスのいずれかを選択して、[スイッチの追加（Add Switches）] ウィンドウでスイッチを追加します。

- **[LAN] > [ファブリック（Fabrics）]** を選択します。リストから Easy_Fabric_IOS_XE ファブリック テンプレートを使用するファブリックを選択し、[アクション（Actions）] をクリックして、[スイッチの追加（Add Switches] を選択します。
- **[LAN] > [ファブリック（Fabrics）]** を選択します。リストから Easy_Fabric_IOS_XE ファブリック テンプレートを使用するファブリックを選択します。[スイッチ（Switches）] タブをクリックします。[アクション（Actions）] をクリックし、[スイッチの追加（Add Switches）] を選択します。
- **[LAN] [スイッチ（Switches）]** を選択します。[アクション（Actions）] をクリックし、[スイッチの追加（Add Switches）] を選択します。[ファブリックの選択（Choose Fabric）] をクリックし、IOS-XE VXLAN ファブリックを選択して、[選択（Select）] をクリックします。

始める前に

デフォルトのクレデンシャルが設定されていない場合は、[LAN クレデンシャル管理（LAN Credentials Management）] ウィンドウでデバイスのデフォルトのクレデンシャルを設定します。Cisco Web UI から [LAN クレデンシャル管理（LAN Credentials Management）] ウィンドウに移動するには、[設定（Settings）] [LAN クレデンシャル管理（LAN Credentials Management）] を選択します。Nexusダッシュボード ファブリック コントローラ >

手順

ステップ 1 次のフィールドに値を入力します。

フィールド	説明
シードIP	スイッチの IP アドレスを入力します。 IP アドレスの範囲を入力することにより、複数のスイッチをインポートできます。たとえば、10.10.10.40 ～ 60 スイッチは適切にケーブル接続され、Cisco サーバに到達可能である必要があり、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。Nexusダッシュボード ファブリック コントローラ
認証プロトコル（Authentication Protocol）	ドロップダウンリストから認証プロトコルを選択します。
ユーザ名	スイッチのユーザ名を入力します。
[パスワード（Password）]	スイッチのパスワードを入力します。

（注） スイッチの検出後にのみ、検出および LAN クレデンシャルを変更できます。

ステップ 2 **[スイッチの検出（Discover Switches）]** をクリックします。

スイッチの詳細が入力されます。

Cisco Nexusダッシュボード ファブリック コントローラでは、StackWise Virtual で動作する Cisco Catalyst 9500 スイッチのインポートをサポートしています。Cisco Catalyst 9500 スイッチのペアを仮想スイッチに形成する StackWise Virtual の構成は、インポートの前に行う必要があります。StackWise Virtual の構成方法の詳細については、必要なリリースの『High Availability Configuration Guide（Catalyst 9500 スイッチ）』の「Cisco StackWise Virtual の構成」の章を参照してください。https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-9/configuration_guide/ha/b_169_ha_9500_cg/configuring_cisco_stackwise_virtual.html

ステップ 3 インポートするスイッチに隣接するチェックボックスをオンにします。

管理可能なステータスのスイッチのみをインポートできます。

ステップ 4 **[スイッチの追加（Add Switches）]** をクリックします。

スイッチの検出プロセスが開始され、[スイッチ（Switches）] タブの [検出ステータス（Discovery Status）] 列で検出ステータスが更新されます。

ステップ 5 （任意）デバイスの詳細を表示します。

デバイスの検出後、検出ステータスが緑色の [OK] に変わります。

次のタスク

1. 適切なロールを設定します。サポートされるロールは次のとおりです。
   - リーフ
   - スパイン
   - 境界

   ロールを設定するには、スイッチを選択して [アクション（Actions）] をクリックします。**[ロールの設定（Set role）]** を選択します。ロールを選択し、[選択（Select）] をクリックします。

（注） スイッチを検出すると、Nexus ダッシュボード ファブリック コントローラ は通常、デフォルト ロールとして [リーフ] を割り当てます。

2. 構成を再計算し、構成をスイッチに展開します。

構成の再計算と展開

設定を再計算し、IOS-XE Easy Fabric のスイッチに展開するには、次の手順を実行して設定を再計算します。

始める前に

IOS-XE Easy Fabric でスイッチのロールを設定します。

手順

ステップ 1 **[ファブリックの概要（Fabric Overview）]** から **[アクション（Actions）]** をクリックします。

ステップ 2 **[構成の再計算（Recalculate Config）]** を選択します。

スイッチで構成の再計算が開始されます。

IOS-XE イージー ファブリック内に Cisco Catalyst スイッチの DCI リンクを作成する

IOS-XE Easy Fabric のボーダー ロールを持つ Cisco Catalyst 9000 シリーズ スイッチと、別のファブリックの別のスイッチの間で VRF-Lite IFC を作成できます。他のスイッチは、外部ファブリック、LAN クラシック ファブリック、または Easy Fabric の Nexus スイッチにすることができます。外部ファブリックまたは IOS-XE Easy Fabric の Catalyst 9000 スイッチも使用できます。リンクは IOS-XE Easy Fabric からのみ作成できます。

詳細については、リンク （172 ページ）およびテンプレート （Templates）を参照してください。

（注） IOS-XE Easy Fabric の DCI リンクを作成する場合、宛先デバイスが Nexus スイッチの場合にのみ自動展開がサポートされます。

IOS-XE Easy Fabric のリンクを作成するには、次の手順を実行します。

1. ファブリックの概要の **[リンク（Links）]** タブに移動します。

   以前に作成されたリンクのリストが表示されます。このリストには、ファブリック内のスイッチ間のファブリック間リンクと、このファブリック内の境界スイッチと他のファブリック内のスイッチ間のファブリック内リンクが含まれています。

   ファブリック間リンクは、BGW およびボーダー リーフ/スパインとは別に、外部ファブリックのエッジ ルータ スイッチもサポートします。

2. **[アクション (Actions)]** をクリックし、**[作成 (Create)]** を選択します。

   [リンクの作成（Create Link）] ウィンドウが表示されます。デフォルトでは、リンク タイプとして **[ファブリック内（Intra-Fabric）]** オプションが選択されています。

3. **[リンク タイプ（Link Type）]** ドロップダウン ボックスから **[ファブリック間（Inter-Fabric）]** を選択します。フィールドはそれに応じて変更されます。

4. リンクサブタイプとしてVRF_LITE、VRF_LITE IFCのext_fabric_setupテンプレート、およびソースファブリックとしてIOS-XEファブリックを選択します。

   リンク テンプレート：リンク テンプレートが入力されます。

   テンプレートには、選択内容に基づいて、対応するパッケージ済みのデフォルト テンプレートが自動的に入力されます。VRF_LITE IFC に使用するテンプレートは ext_fabric_setup です。

（注） ext_routed_fabric テンプレートのみを追加、編集、または削除できます。詳細については、テンプレートを参照してください。

5. [Source Fabric] ドロップダウンリストから、ソースファブリックとしてIOS-XEファブリックを選択します。

6. [宛先ファブリック（Destination Fabric）] ドロップダウン リストから宛先ファブリックを選択します。
7. 宛先デバイスに接続する送信元デバイスとイーサネット インターフェイスを選択します。
8. 送信元デバイスに接続する宛先デバイスとイーサネット インターフェイスを選択します。
9. 必要に応じて、他のフィールドに値を入力します。
10. **[Save（保存）]** をクリックします。

（注） 作成アクションの代わりに、**編集**アクションを使用し、既存のファブリック間リンクを使用して VRF-Lite IFC を作成することもできます。**VRF_Lite** リンク サブタイプを選択します。デフォルトでは、[Edit]を選択すると、[Link-Type]、[Source Fabric]、[Destination Fabric]、[Source Device]、[Destination Device]、[Source Interface]、および[Destination Interface]フィールドのデータが[Edit Link]ウィンドウに自動的に入力されます。

リンクサブタイプとしてVRF_LITE、VRF_LITE IFCのext_fabric_setupテンプレート、およびソースファブリックとしてIOS-XEファブリックを選択します。

手順を完了するには、上記のステップ 4 ー 10 を繰り返します。

IOS-XE Easy ファブリックに Cisco Catalyst 9000 シリーズ スイッチの VRF を作成する

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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（VRFs）]**を選択します。
- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。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（VRFs）]** を開きます。

IOS-XE Easy ファブリック用の VRF を作成できます。

Cisco Nexus ダッシュボード ファブリック コントローラ Web UIから VRF を作成するには、次の手順を実行します。

1. **[アクション (Actions)]** をクリックし、**[作成 (Create)]** を選択します。

   [VRF の作成（Create VRF）] ウィンドウが表示されます。
2. 必須のフィールドに必要な詳細情報を入力します。一部のフィールドにはデフォルト値があります。

   このウィンドウのフィールドは次のとおりです。

[VRF名（VRF Name）]：仮想ルーティングおよび転送（VRF）の名前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。

VRF ID：VRF の ID を設定させること、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 を設定させること、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)]：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。IOS_XE Easy Fabric のデフォルトテンプレートは、**IOS_XE_VRF** テンプレートです。

[VRF 拡張テンプレート (VRF Extension Template)]：ユニバーサル拡張テンプレートが自動入力されます。これにより、このネットワークを別のファブリックに拡張できます。IOS_XE Easy Fabric のデフォルトテンプレートは、**IOS_XE_VRF** テンプレートです。

VRF プロファイルのセクションには、**[一般 (General)]** タブと **[詳細 (Advanced)]** タブがあります。

3. **[一般 (General)]** タブには以下のフィールドがあります。

   [VRF の説明（VRF Description）]：VRFの説明を入力します。

   [VRF インターフェイスの説明（VRF Intf Description）]：VRFインターフェイスの説明を入力します。

4. **[詳細 (Advanced)]** タブをクリックすると、オプションとして、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。

   [再配布直接ルート マップ（Redistribute Direct Route Map）]：再配布直接ルート マップ名を指定します。

   [最大 BGP パス（Max BGP Paths）]：最大 BGP パスを指定します。有効な値の範囲は 1 ー 64 です。

   [最大 iBGP パス（Max iBGP Paths）]：最大 iBGP パスを指定します。有効な値の範囲は 1 ー 64 です。

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

   [デフォルト ルートのアドバタイズ（Advertise Default Route）]：このチェックボックスをオンにすると、デフォルト ルートのアドバタイズメントが内部的に制御されます。

   [スタティック 0/0 ルートの設定（Config Static 0/0 Route）]：スタティック デフォルト ルートの設定を制御するには、このチェックボックスをオンにします。

5. 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。

次の作業

VRF をアタッチします。

VRF_LITE 拡張を選択するループバック インターフェイスを作成します。

VRF のアタッチおよびデタッチの詳細については、VRF アタッチメント （191 ページ） を参照してください。

IOS-XE Easy ファブリックで VRF を Cisco Catalyst 9000 シリーズ スイッチに接続する

IOS-XE イージー ファブリックの Cisco Catalyst 9000 シリーズ スイッチに VRF を接続するには、VRF アタッチメント （191 ページ） を参照してください。

（注） 横にあるチェックボックスをオンにして、CAT9000 シリーズ スイッチに対応するVRFを選択します。

（注） 同様に、ループバック インターフェイスを作成し、VRF_LITE 拡張を選択できます。

次の作業

次のように設定を展開します。

1. **[ファブリック概要（Fabric Overview）]** で **[アクション（Actions）]** をクリックします。
2. **[スイッチに設定を展開する（Deploy config to Switches）]** を選択します。
3. 設定のプレビューが完了したら、**[展開（Deploy）]** をクリックします。
4. 導入が完了したら、**[閉じる（Close）]** をクリックします。

IOS-XE Easy ファブリックにネットワークの作成および展開

次のステップでは、IOS-XE Easy Fabricsでネットワークを作成して展開します。

（注）
- ネットワークテンプレートおよびネットワーク拡張テンプレートは、IOS-XE簡易ファブリック用に作成されたデフォルトのIOS_XE_Networkテンプレートを使用します。

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、簡易ファブリック、およびMSDファブリックにのみ適用されます。

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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。**[ファブリック概要（Fabric Overview）]** > **[ネットワーク（Networks）]** を選択します。
- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。ファブリックをダブルクリックして、**[ファブリック概要（Fabric Overview）]** > **[ネットワーク（Networks）]** を開きます。

IOS-XE Easy Fabricのネットワークの作成

Cisco Web UIからIOX-XE Easy Fabricのネットワークを作成するには、次の手順を実行します。
Nexusダッシュボード ファブリック コントローラ

1. [Networks]水平タブで、[Actions]をクリックし、[Create]を選択します。

   [ネットワークの作成 (Create Network)] ウィンドウが表示されます。

2. 必須のフィールドに必要な詳細情報を入力します。

   このウィンドウのフィールドは次のとおりです。

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

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

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

   VRF が作成されていない場合、このフィールドは空白になります。新しい VRF を作成する場合は、**[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：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：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。VRF Lite拡張がサポートされています。このテンプレートは、境界リーフスイッチに適用できます。

   [Generate Multicast IP]：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は、[Generate Multicast IP]をクリックします。

   ネットワーク プロファイルのセクションには、**[一般 (General)]** タブと **[詳細 (Advanced)]** タブがあります。

3. **[一般 (General)]** タブには以下のフィールドがあります。

（注） 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/ NetMask：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 アドレスを設定した場合、Nexusダッシュボード ファブリック コントローラ はエラーを表示しないので、この設定は保存できます。

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：サブネットのIPv6アドレスを指定します。

[Vlan 名（Vlan Name）]：VLAN 名を入力します。

[Vlan インターフェイスの説明（Vlan Interface Description）]：インターフェイスの説明を指定します。このインターフェイスはスイッチの仮想インターフェイス（SVI）です。

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。

4. **[詳細 (Advanced)]** タブをクリックすると、オプションとして、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。

   [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、デフォルトではすべてのネットワークで同じです。このネットワークに新しいマルチキャストグループアドレスが必要な場合は、[マルチキャストIPの生成（Generate Multicast IP）]ボタンをクリックして生成できます。

   DHCPv4サーバ1：最初のDHCPサーバのDHCPリレーIPアドレスを入力します。

   DHCPv4サーバVRF：DHCPサーバのVRF IDを入力します。

   DHCPv4サーバ2：次のDHCPサーバのDHCPリレーIPアドレスを入力します。

   DHCPv4 Server2 VRF：DHCPサーバのVRF IDを入力します。

   Loopback ID for DHCP Relay interface（Min：0、Max：1023）：DHCPリレーインターフェイスのループバックIDを指定します。

[境界でのL3ゲートウェイの有効化（Enable L3 Gateway on Border）]：チェックボックスをオンにすると、境界スイッチでレイヤ3ゲートウェイが有効になります。

5. [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。

IOS-XE Easy Fabricsでのネットワークの展開

IOS-XEイージーファブリックでは、次のようにネットワークを展開できます。

- ネットワーク設定は、次のように[Fabric Overview]ウィンドウで展開することもできます。
  1. ファブリックの概要で[アクション（Actions）]をクリックします。
  2. **[スイッチに設定を展開する（Deploy config to Switches）]** を選択します。
  3. 設定のプレビューが完了したら、**[展開（Deploy）]** をクリックします。
  4. 展開が完了したら、**[閉じる（Close）]** をクリックします。
- IOS-XE Easy Fabricでネットワークを展開するには、を参照してください。ネットワーク接続 （204 ページ）

外部ファブリック

外部ファブリックにスイッチを追加できます。汎用ポインタ：

NDFC は「no router bgp」を生成しません。変更する場合は、スイッチに移動して「no feature bgp」を実行します。何もなく、ASN を更新する場合は、その後で再同期します。

- 外部ファブリックは、モニタ専用または管理モードのファブリックです。
- Cisco Nexus Dashboard Fabric Controller Release 12.0.1、Cisco IOS-XR ファミリ デバイス、Cisco ASR 9000 シリーズ Aggregation Services Routers および Cisco Network Convergence System（NCS）5500 シリーズは、管理モードおよびモニタ モードの外部ファブリックでサポートされます。NDFC は設定を生成してこれらのスイッチにプッシュすることができ、設定コンプライアンスもこれらのプラットフォームで有効になります。
- Cisco Nexus Dashboard Fabric Controller リリース 12.1.1e から、管理モードとモニタ モードの両方でCisco 8000 シリーズルータを外部ファブリックに追加することもでき、構成コンプライアンスもサポートされます。
- 外部ファブリックのスイッチをインポート、削除、および削除できます。

- ファブリック間接続（IFC）の場合、外部ファブリックの宛先スイッチとしてCisco 9000、7000、および5600シリーズスイッチを選択できます。
- 存在しないスイッチを宛先スイッチとして使用できます。
- 外部ファブリックをサポートするテンプレートは、External_Fabricです。
- 外部ファブリックがMSDファブリックメンバーである場合、MSDトポロジ画面には、外部ファブリックとそのデバイス、およびメンバーファブリックとそのデバイスが表示されます。

  外部ファブリックトポロジ画面から表示すると、非管理対象スイッチへの接続はすべて、Undiscoveredというラベルの付いたクラウドアイコンで表されます。Nexusダッシュボード ファブリック コントローラ
- マルチサイトまたはVRF-lite IFCを設定するには、VXLANファブリック内の境界デバイスのリンクを手動で設定するか、または自動的にDeploy Border Gateway MethodまたはVRF Lite IFC Deploy Methodを使用します。ボーダーデバイスのリンクを手動で設定する場合は、コアルータロールを使用してマルチゲートウェイeBGPアンダーレイをボーダーゲートウェイデバイスからコアルータに設定し、エッジルータロールを使用してVRF-Lite Interを設定することを推奨します。 -ボーダーデバイスからエッジデバイスへのファブリック接続（IFC）。
- Cisco Nexus 7000シリーズスイッチとCisco NX-OSリリース6.2（24a）をLANクラシックまたは外部ファブリックで使用している場合は、ファブリック設定でAAA IP認証を有効にしてください。
- 外部ファブリックでは、次の非Nexusデバイスを検出できます。
  - IOS-XEファミリデバイス：Cisco CSR 1000v、Cisco IOS XEジブラルタ16.10.x、Cisco ASR 1000シリーズルータ、およびCisco Catalyst 9000シリーズスイッチ
  - IOS-XRファミリデバイス：ASR 9000シリーズルータ、IOS XRリリース6.5.2およびCisco NCS 5500シリーズルータ、IOS XRリリース6.5.3
  - Arista 4.2（任意のモデル）
- 外部ファブリックに追加する前に、Cisco CSR 1000vを除くすべてのNexus以外のデバイスを設定します。
- Nexus以外のデバイスをボーダーとして設定できます。外部ファブリックの非Nexusデバイスと簡易ファブリックのCisco Nexusデバイス間でIFCを作成できます。これらのデバイスでサポートされるインターフェイスは次のとおりです。
  - ルート化済み
  - サブインターフェイス
  - ループバック

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

  次に例を示します。

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

  この場合、入力したパスワードは5 $ 5 $ I4sapkBh $ S7B7UcPH / iVTihLKH5sgldBeS3O2X1StQsvv3cmbYd1です。
- Cisco Network Insights for Resources（NIR）リリース2.1以降、およびフローテレメトリの場合、feature lldpコマンドは必須設定の1つです。

  シスコは、Easy Fabric導入、つまりeBGPルーテッドファブリックまたはは VXLAN EVPNファブリックの場合にのみ、lldp機能をスイッチにプッシュします。Nexusダッシュボードファブリック コントローラ

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

  - モニタモードまたは管理モードの外部ファブリック
  - モニタモードまたは管理モードのLANクラシックファブリック

MSDファブリックの下での外部ファブリックの移動

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

1. [Topology]で、MSD-Parent-Fabric内をクリックします。**[アクション（Actions）]** ドロップダウンリストで、**[ファブリックの移動（Move Fabrics）]** を選択します。

   [ファブリックの移動（Move Fabric）] 画面が表示されます。ファブリックのリストが含まれています。外部ファブリックは、スタンドアロンファブリックとして表示されます。
2. 外部ファブリックの横にあるオプションボタンを選択し、[Add]をクリックします。

   右上の[Scope]ドロップダウンボックスで、MSDファブリックの下に外部ファブリックが表示されていることがわかります。

MSDファブリックトポロジでの外部ファブリックの説明

MSDトポロジ画面には、MSDメンバーファブリックと外部ファブリックが一緒に表示されます。外部ファブリックExternal65000は、MSDトポロジの一部として表示されます。

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

外部ファブリックの作成

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

手順

ステップ 1 **[LAN] > [ファブリック（Fabrics）] > [ファブリック（Fabrics）]** の順に選択します。

ステップ 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。

ステップ 3 ファブリック名を入力し、**[テンプレートの選択（Choose Template）]** をクリックします。

ステップ 4 ドロップダウンリストから、[External_Fabric template]を選択します。

この画面のフィールドは次のとおりです。

BGP AS # ：BGP AS番号を入力します。

[ファブリックモニタモード（Fabric Monitor Mode）]：ファブリックを管理する場合は、このチェックボックスをオフにします。Nexusダッシュボードファブリック コントローラモニタ専用の外部ファブリックを有効にする場合には、チェックボックスをオンのままにします。

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

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

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

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

[Enable Performance Monitoring]：NX-OSスイッチでのみパフォーマンスモニタリングを有効にします。

ステップ 5 [詳細（Advanced）]タブのフィールドに値を入力します。

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

[MPLS ハンドオフの有効化（Enable MPLS Handoff）]：MPLS ハンドオフ機能を有効にするには、このチェックボックスをオンにします。詳細については、VXLAN BGP EVPN ファブリックの外部/WAN レイヤ 3 接続について扱っている MPLS SR および LDP ハンドオフ 章を参照してください。

[アンダーレイ MPLS ループバック ID（Underlay MPLS Loopback Id）]：アンダーレイ MPLS ループバック ID を指定します。デフォルト値は 101 です。

[Enable AAA IP Authorization]：IP認証がAAAサーバで有効になっている場合に、AAA IP認証を有効にします。

[トラップホストとして有効にする（Enable as Trap Host）]：トラップホストとして有効にする場合は、このチェックボックスをオンにします。Nexusダッシュボード ファブリック コントローラNexusダッシュボード ファブリック コントローラ

[ブートストラップスイッチのCDPを有効にする（Enable CDP for Bootstrapped Switch）]：ブートストラップスイッチのCDPを有効にします。

[NX-APIの有効化（Enable NX-API）]：HTTPSでのNX-APIの有効化を指定します。このチェックボックスは、デフォルトでオフになっています。

[Enable NX-API on HTTP]：HTTPでのNX-APIの有効化を指定します。このチェックボックスは、デフォルトでオフになっています。HTTP を使用するには、[NX-API の有効化（Enable NX-API）]チェックボックスをオンにします。このチェックボックスをオフにすると、エンドポイントロケータ（EPL）、レイヤ4～レイヤ7サービス（L4ーL7サービス）、VXLAN OAM など、NX-API を使用し、Cisco Nexusダッシュボード ファブリック コントローラ がサポートするアプリケーションは、HTTP ではなく HTTPS の使用を開始します。

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

インバンド管理：外部および従来のLANファブリックの場合、このノブを使用して、アウトバンド接続（別名スイッチmgmt0インターフェイスを介して到達可能）。Nexusダッシュボード ファブリック コントローラ唯一の要件は、インバンド管理型スイッチの場合、eth2（別名インバンドインターフェイス）を介してスイッチからIPに到達できることです。Nexusダッシュボード ファブリック コントローラこの目的のために、でスタティックルートが必要になる場合があります。これは、[管理（Administration）]-[カスタマイズ（Customization）]-[ネットワーク設定（Network Preferences）]オプションで設定できます。Nexusダッシュボード ファブリック コントローラインバンド管理を有効にした後、検出中に、インバンド管理を使用してインポートするすべてのスイッチの IP を指定し、最大ホップ数を 0 に設定します。Nexusダッシュボード ファブリック コントローラ にはインバンド管理対象スイッチ IP が eth2 インターフェイス経由で到達可能であることを検証する事前チェックがあります。事前チェックをパスすると、Nexusダッシュボード ファブリック コントローラはインターフェイスが属する VRF に加えて、指定された検出 IP を持つそのスイッチ上のインターフェイスを検出し、学習します。スイッチのインポート/検出のプロセスの一部として、この情報はNexusダッシュボード ファブリック コントローラに入力される目的のベースラインにキャプチャされます。詳細については、外部

ファブリックおよびLANクラシック ファブリックでのインバンド管理 （137ページ）を参照してください。

（注） ブートストラップまたはPOAPは、アウトオブバンド接続、つまりスイッチmgmt0を介して到達可能なスイッチでのみサポートされます。Nexusダッシュボード ファブリック コントローラ上のさまざまなPOAPサービスは通常、eth1またはアウトオブバンドインターフェイスにバインドされます。eth0 / eth1インターフェイスが同じIPサブネットに存在するシナリオでは、POAPサービスは両方のインターフェイスにバインドされます。Nexusダッシュボード ファブリック コントローラ

[精密時間プロトコル（PTP）の有効化（Enable Precision Time Protocol (PTP)）]：ファブリック全体でPTPを有効にします。このチェックボックスをオンにすると、PTPがグローバルに有効になり、コアに面するインターフェイスで有効になります。また、[PTP送信元ループバックID（PTP Source Loopback Id）]および[PTPドメインID（PTP Domain Id）]フィールドが編集可能になります。詳細については、外部ファブリックおよびLANクラシック ファブリック向け高精度時間プロトコル（PTP） （135ページ）を参照してください。

[PTP送信元ループバックID（PTP Source Loopback Id）]：すべてのPTPパケットの送信元IPアドレスとして使用されるループバック インターフェイスIDループバックを指定します。有効な値の範囲は0～1023です。PTPループバックIDをRP、ファントムRP、NVE、またはMPLSループバックIDと同じにすることはできません。そうでない場合は、エラーが生成されます。PTPループバックIDは、BGPループバックまたは作成元のユーザ定義ループバックと同じにすることができます。Nexusダッシュボード ファブリック コントローラPTPループバックIDが保存と展開中に見つからない場合、次のエラーが生成されます。PTP送信元IPに使用するループバックインターフェイスが見つかりません。PTP機能を有効にするには、すべてのデバイスでPTPループバックインターフェイスを作成してください。

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

ファブリック自由形式：この自由形式フィールドを使用して、外部ファブリックで検出されたすべてのデバイスに設定をグローバルに適用できます。ファブリック内のデバイスは同じデバイスタイプに属している必要があり、ファブリックはモニタモードになっていません。さまざまなデバイスタイプがあります。

- NX-OS
- IOS-XE
- IOS-XR
- その他

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

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

ステップ6 次に示すように、[リソース（Resources）]タブに入力します。

サブインターフェイスDot1q範囲：サブインターフェイス802.1Q範囲とアンダーレイルーティングループバックIPアドレス範囲が自動入力されます。

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

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

ステップ7 次に示すように、[Configuration Backup]タブに入力します。

このタブのフィールドは次のとおりです。

[毎時ファブリック バックアップ（Hourly Fabric Backu）]：ファブリック構成とインテントの毎時バックアップを有効にします。

新しいファブリック設定とインテントの1時間ごとのバックアップを有効にできます。前の時間に設定のプッシュがある場合、はバックアップを取得します。Nexusダッシュボード ファブリック コントローラ外部ファブリックの場合、VXLANファブリックと比較して、スイッチの設定全体がインテントオンに変換されません。Nexusダッシュボードファブリック コントローラしたがって、外部ファブリックでは、インテントと実行コンフィギュレーションの両方がバックアップされます。

インテントとは、に保存されているが、まだスイッチにプロビジョニングされていない設定を指します。Nexusダッシュボード ファブリック コントローラ

時間単位のバックアップは、その時間の最初の 10 分間にトリガーされます。

[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]：毎日のバックアップを有効にします。このバックアップは、構成のコンプライアンスによって追跡されないファブリック デバイスの実行構成の変更を追跡します。

[スケジュール済みの時間（Scheduled Time）]：スケジュールされたバックアップ時間を 24 時間形式で指定します。[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]チェックボックスをオンにすると、このフィールドが有効になります。

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

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

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

ファブリック トポロジ ウィンドウでファブリック バックアップを開始することもできます。[Actions]ペインで[Backup Fabric]をクリックします。

バックアップには、実行コンフィギュレーションとによってプッシュされたインテントが含まれます。Nexusダッシュボード ファブリック コントローラ設定に準拠すると、実行コンフィギュレーションが設定と同じになります。Nexusダッシュボードファブリック コントローラ外部ファブリックでは、一部の設定のみがインテントの一部であり、残りの設定はによって追跡されないことに注意してください。Nexusダッシュボードファブリック コントローラしたがっ

て、バックアップの一部として、スイッチからのインテントと実行コンフィギュレーションの両方がキャプチャされます。Nexusダッシュボード ファブリック コントローラ

ステップ 8 **[ブートストラップ（Bootstrap）]** タブをクリックします。

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

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

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

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

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

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

ローカル DHCP サーバの有効化（Enable Local DHCP Server）：ローカル DHCP サーバを介した自動 IP アドレス割り当ての有効化を開始するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、残りのすべてのフィールドが編集可能になります。

[DHCP バージョン（DHCP Version）]：このドロップダウンリストから [DHCPv4] または [DHCPv6] を選択します。DHCPv4 を選択すると、**[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]** フィールドが無効になります。DHCPv6 を選択すると、**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** は無効になります。

（注） NexusダッシュボードファブリックコントローラCisco IPv6 POAP は、Cisco Nexus 7000 シリーズ スイッチではサポートされていません。Cisco Nexus 9000 および 3000 シリーズ スイッチは、スイッチが L2 隣接（eth1 またはアウトオブバンド サブネットは /64 が必須）、またはスイッチがいくつかの IPv6 /64 サブネット内に存在する L3 隣接である場合にのみ、IPv6 POAP をサポートします。/64 以外のサブネット プレフィックスはサポートされません。

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

[DHCPスコープ開始アドレス（DHCP Scope Start Address）]および[DHCPスコープ終了アドレス（DHCP Scope End Address）]：スイッチアウトオブバンドPOAPに使用されるIPアドレス範囲の最初と最後のIPアドレスを指定します。

[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]：スイッチの管理 VRF のデフォルト ゲートウェイを指定します。

スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）：スイッチの Mgmt0 インターフェイスのプレフィックスを指定します。プレフィックスは 8 ～ 30 の間である必要があります。

DHCP スコープおよび管理デフォルト ゲートウェイ *IP* アドレスの仕様（*DHCP scope and management default gateway IP address specification*）：管理デフォルト ゲートウェイ IP アドレスを 10.0.1.1 に、サブネット マスクを 24 に指定した場合、DHCP スコープが指定したサブネット、10.0.1.2 ～ 10.0.1.254 の範囲内であることを確認してください。

[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]：スイッチの Mgmt0 インターフェイスの IPv6 プレフィックスを指定します。プレフィックスは 112 ー 126 の範囲で指定する必要があります。このフィールドは DHCP の IPv6 が有効な場合に編集できます。

[Enable AAA Config]：デバイスの起動時に[Advanced]タブからAAA設定を含めるには、このチェックボックスをオンにします。

Bootstrap Freeform Config ：（オプション）必要に応じて他のコマンドを入力します。たとえば、AAAまたはリモート認証関連の設定を使用している場合は、このフィールドにこれらの設定を追加してインテントを保存します。デバイスが起動すると、[Bootstrap Freeform Config] フィールドで定義されたインテントが含まれます。

NX-OSスイッチの実行コンフィギュレーションに示されているように、running-configを正しいインデントで自由形式の設定フィールドにコピーアンドペーストします。freeform config は running config と一致する必要があります。詳細については、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 （66 ページ）を参照してください。

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

スコープの形式は次の順で定義する必要があります。

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

例：10.6.0.2、10.6.0.9、16.0.0.1、24

ステップ 9 **[フロー モニター（Flow Monitor）]**タブをクリックします。このタブのフィールドは次のとおりです。

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

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

NetFlow がファブリック レベルで有効になっていない場合、インターフェイス、ネットワーク、または VRF レベルで NetFlow を有効にすると、エラー メッセージが生成されます。Cisco NDFC の Netflow サポートについては、Netflow サポート （133 ページ） を参照してください。

[Netflow エクスポータ（Netflow Exporter）]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 エクスポータを追加します。このエクスポータは、NetFlow データの受信側です。この画面のフィールドは次のとおりです。

- **[エクスポータ名（Exporter Name）]**：エクスポータの名前を指定します。
- **[IP]**：エクスポータの IP アドレスを指定します。
- **[VRF]**：エクスポータがルーティングされる VRF を指定します。
- **[送信元インターフェイス（Source Interface）]**：送信元インターフェイス名を入力します。
- **[UDP ポート（UDP Port）]**：NetFlow データがエクスポートされる UDP ポートを指定します。

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

[Netflow レコード（Netflow Record）] 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 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。
- **[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（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 モニタを追加します。この画面のフィールドは次のとおりです。

- **[モニタ名（Monitor Name）]**：モニタの名前を指定します。
- **[レコード名（Record Name）]**：モニタのレコードの名前を指定します。
- **[エクスポータ 1 の名前（Exporter1 Name）]**：Netflow モニタ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。

ステップ 10 **[Save（保存）]** をクリックします。

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

外部ファブリックを作成したら、スイッチを追加します。

外部ファブリックへのスイッチの追加

各ファブリックのスイッチは一意であるため、各スイッチは1つのファブリックにのみ追加できます。外部ファブリックにスイッチを追加するには、次の手順を実行します。

手順

ステップ 1 **[LAN] [スイッチ（Switches）]** を選択します。[アクション（Actions）] ドロップダウン リストから、**[スイッチの追加（Add Switches）]** を選択します

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

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

ステップ 2 新しいスイッチを検出するには、**[検出（Discover）]** を選択します。既存のスイッチをファブリックに追加するには、**[ネイバー スイッチを移動する（Move Neighbor Switches）]** を選択します。

ステップ 3 **[検出（Discover）]** オプションを選択した場合は、次の手順を実行します。

a) スイッチの IP アドレス（シード IP）を入力します。

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

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

オプションは、**NX-OS**、**IOS XE**、**IOS XR** および**その他**です。

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

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

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

d) スイッチ管理者ユーザ名およびパスワードを入力します。

e) 画面の下部にある **[ディスカバリ スイッチ（Discovery Switches）]** をクリックします。

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

該当するスイッチの横にあるチェックボックスをオンにし、**[スイッチをファブリックに追加する（Add Switches into fabric）]** をクリックします。

複数のスイッチを同時に検出できます。スイッチは適切にケーブル接続しサーバ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。Nexusダッシュボード ファブリック コントローラ

スイッチ検出プロセスが開始されます。**[進行状況（Progress）]** 列には、進行状況が表示されます。Nexusダッシュボード ファブリック コントローラ でスイッチが検出されたら、**[閉じる（Close）]** をクリックして前の画面に戻ります。

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

選択したスイッチが外部ファブリックに移動します。

外部ファブリック向けスイッチ設定

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

次のオプションがあります。

[ロールの設定（Set Role）]：デフォルトでは、外部ファブリック スイッチにロールは割り当てられません。許可されるロールは、エッジ ルータとコア ルータです。Multi-Site Inter-Fabric Connection（IFC）のコア ルータ ロールと、外部ファブリックと VXLAN ファブリック境界デバイス間の VRF Lite IFC のエッジ ルータ ロールを割り当てます。

（注） スイッチのロールの変更は、**構成の展開**を実行する前にのみ許可されます。

vPC ペアリング：vPC のスイッチを選択し、そのピアを選択します。

[モードの変更（Change Modes）]：スイッチのモードを [アクティブ（Active）] から [操作（Operational）] に変更できます。

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

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

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

[履歴（History）]：スイッチごとの導入履歴を表示します。

[設定の再計算（Recalculate Config）]：保留中の設定と、実行中の設定と予想される設定の比較を表示します。

[展開設定（Deploy Config）]：スイッチ設定ごとに展開します。

[検出（Discovery）]：このオプションを使用して、スイッチのクレデンシャルを更新し、スイッチをリロードし、スイッチを再検出し、ファブリックからスイッチを削除できます。

[アクション（Actions）] ドロップダウン リストから **[展開（Deploy）]** をクリックします。テンプレートとインターフェイスの設定は、スイッチの設定を形成します。

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

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

導入が完了したら、**[閉じる（Close）]** をクリックします。

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

- インベントリから外部ファブリックのスイッチを削除し、再検出します。
- LANディスカバリはSNMPとSSHの両方を使用するため、両方のパスワードを同じにする必要があります。スイッチのSNMPパスワードと一致するようにSSHパスワードを変更する必要があります。SNMP認証が失敗すると、検出は認証エラーで停止します。SNMP認証は成功したがSSH認証が失敗した場合、Nexusダッシュボード ファブリック コントローラ で検出は続行されますが、スイッチのステータスにSSHエラーの警告が表示されます。

新しいスイッチの検出

新しいスイッチを検出するには、次の手順を実行します。

Procedure

ステップ 1 Nexusダッシュボード ファブリック コントローラ サーバーにケーブル接続されていることを確認してから、外部ファブリックの新しいスイッチの電源をオンにします。

Cisco NX-OS を起動し、スイッチのクレデンシャルを設定します。

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

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

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

[ファブリックの編集（Edit Fabric）] 画面が表示されます。

ステップ 4 **[ブートストラップ（Bootstrap）]** タブをクリックし、DHCP 情報を更新します。

ステップ 5 **[保存（Save）]**（**[ファブリックの編集（Edit Fabric）]** 画面の右下）をクリックして、設定を保存します。

ステップ 6 ファブリックをダブルクリックして**[ファブリックの概要（Fabric Overview）]**を表示します。

ステップ 7 **[スイッチ（Switches）]** タブで、**[アクション（Actions）]** ドロップダウンリストから **[スイッチの追加（Add Switches）]** を選択します。

ステップ 8 **[POAP]** タブをクリックします。

前の手順では、reload コマンドをスイッチで実行していました。スイッチが再起動してリブートすると、Nexusダッシュボード ファブリック コントローラ はスイッチからシリアル番号、モデル番号、およびバージョンを取得し、[インベントリ管理（Inventory Management）] 画面

に表示します。また、管理 IP アドレス、ホスト名、およびパスワードを追加するオプションが使用可能になります。スイッチ情報が取得されない場合は、画面の右上にある [更新（Refresh）] アイコンを使用して画面を更新します。

Note 画面の左上には、スイッチ情報を含む.csvファイルをエクスポートおよびインポートするためのエクスポートおよびインポートオプションがあります。インポート オプションを使用してデバイスを事前プロビジョニングすることもできます。

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

デバイスの IP アドレスに基づいて、**[IP アドレス（IP Address）]** フィールドに IPv4 または IPv6 アドレスを追加できます。

デバイスは事前にプロビジョニングできます。

ステップ 9 **[管理者パスワード（Admin Password）]** フィールドと **[管理者パスワードの確認（Confirm Admin Password）]** フィールドに、新しいパスワードを入力します。

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

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

ステップ 10 (Optional) スイッチの検出に検出クレデンシャルを使用します。

a) **[ディスカバリ クレデンシャルの追加（Add Discovery Credentials）]** アイコンをクリックして、スイッチのディスカバリ クレデンシャルを入力します。

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

[OK] をクリックして、ディスカバリ クレデンシャルを保存します。

検出クレデンシャルが指定されていない場合は、Nexusダッシュボード ファブリック コントローラ は管理者ユーザとパスワードを使用してスイッチを検出します。

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

ステップ 11 画面右上の **[ブートストラップ（Bootstrap）]** をクリックします。

Nexusダッシュボード ファブリック コントローラ は管理IPアドレスおよびその他のクレデンシャルをスイッチにプロビジョニングします。この単純化されたPOAPプロセスでは、すべてのポートが開かれます。

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

ステップ 12 スイッチをモニタし、POAP 完了を確認します。

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

Note
- スイッチと Nexusダッシュボード ファブリック コントローラ の間に同期の問題がある場合、スイッチアイコンが赤色で表示され、ファブリックが同期していないことを示します。ファブリックの変更が原因で同期が外れた場合は、変更を展開する必要があります。このプロセスは、「既存スイッチの検出」の項で説明したものと同じです。
- 検出クレデンシャルは、デバイス設定のコマンドに変換されません。このクレデンシャルは、主にスイッチを検出するリモートユーザー（または管理ユーザー以外）を指定するために使用されます。デバイス設定の一部としてコマンドを追加する場合は、ファブリック設定の **[ブートストラップ（Bootstrap）]** タブにある **[ブートストラップ フリーフォーム設定（Bootstrap Freeform Config）]** フィールドにコマンドを追加します。また、**[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウからそれぞれのポリシーを追加できます。

ファブリックの作成時に、**[管理性（Manageability）]** タブに AAA サーバ情報を入力した場合は、各スイッチの AAA サーバ パスワードを更新する必要があります。そうでない場合、スイッチの検出は失敗します。

ステップ 14 保留中の設定が展開されると、すべてのスイッチの **[進捗（Progress）]** 列に 100% と表示されます。

ステップ 15 [トポロジ（Topology）] 画面で、**[トポロジの更新（Refresh Topology）]** アイコンをクリックして更新を表示します。

すべてのスイッチは、機能していることを示す緑色でなければなりません。

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

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

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

ステップ 17 Nexusダッシュボード ファブリック コントローラ UIでは、検出されたスイッチはファブリック トポロジで確認できます。

このステップまでで、POAP の基本設定は完了です。すべてのインターフェイスがトランクポートに設定されます。追加設定を行うには、**[LAN] > [Interfaces]**オプションを使用してインターフェイスを設定する必要があります。以下の設定が含まれますが、これらに限定されません。

- vPC ペアリング。
- ブレークアウト インターフェイス

  ブレークアウトインターフェイスのサポートは、9000 シリーズスイッチで使用できます。
- ポート チャネル、およびポートへのメンバーの追加。

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

非 Nexus デバイスを外部ファブリックに追加する

Cisco Nexusダッシュボード ファブリック コントローラ リリース 12.0.1a 以降では、管理対象モードでも外部ファブリックに Cisco IOS-XR デバイスを追加できます。外部ファブリックでは、次の Cisco IOS-XR デバイスを管理できます。

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

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

外部ファブリックでNexus以外のデバイスを検出し、これらのデバイスの設定コンプライアンスも実行できます。詳細については、外部ファブリックでのコンプライアンスの構成（61 ページ）セクションを参照してください。

*Cisco Nexus*ダッシュボード ファブリック コントローラ *Compatibility Matrix* には、Cisco Nexus ダッシュボード ファブリック コントローラ がサポートする非Nexus デバイスが記載されています。

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

Cisco CSR 1000v は SSH を使用して検出されます。Cisco CSR 1000v は、SNMP がセキュリティ上の理由でブロックされているクラウドでもインストールできるため、SNMP のサポートは必要ありません。外部ファブリックに Cisco CSR 1000v、Cisco IOS XE Gibraltar 16.10.xを追加する

使用例については、「*Cisco Data Center*とパブリッククラウドの接続」の章を参照してください。

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

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

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

外部ファブリックでのコンプライアンスの構成

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

外部ファブリックでは、で定義されているインテントに対して、設定コンプライアンス（CC）により、このインテントが対応するスイッチに存在することが保証されます。Nexusダッシュボードファブリックコントローラこのインテントがスイッチに存在しない場合、CCはOut-of-Syncステータスを報告します。さらに、このインテントをスイッチにプッシュしてステータスを同期中に変更するために生成された保留中の設定があります。スイッチ上にあるが、で定義されたインテントではない追加の設定は、インテント内の設定との競合がない限り、CCによって無視されます。Nexusダッシュボード ファブリック コントローラ

前述のように、ユーザ定義のインテントがに追加され、同じトップレベルコマンドの下にスイッチの追加設定がある場合、CCはで定義されたインテントがスイッチに存在することのみを確認します。Nexusダッシュボード ファブリック コントローラNexusダッシュボード ファブリック コントローラこのユーザ定義インテントがスイッチから削除する目的で全体として削除され、対応する設定がスイッチに存在する場合、CCはスイッチの同期外れステータスを報告し、 config。Nexusダッシュボード ファブリック コントローラこの保留中の設定には、トップレベルのコマンドの削除が含まれています。このアクションにより、このトップレベルコマンドでスイッチで行われた他のアウトオブバンド設定も削除されます。この動作を上書きすることを選択した場合は、自由形式ポリシーを作成し、関連する最上位コマンドを自由形式ポリシーに追加することを推奨します。

この動作を例で見てみましょう。

1. ユーザがスイッチに定義し、スイッチに展開したswitch_freeformポリシー。Nexusダッシュボード ファブリック コントローラ
2. 実行コンフィギュレーションのルータbgpの下に、ユーザ定義インテントの予期される設定に存在しない追加設定があります。Nexusダッシュボード ファブリック コントローラ

ユーザ定義のインテントなしでスイッチに存在する追加の設定を削除する保留中の設定はありません。Nexusダッシュボード ファブリック コントローラ

3. ステップ1で作成されたswitch_freeformポリシーを削除することで、によって以前にプッシュされたインテントがから削除された場合の保留中の設定とサイドバイサイド比較Nexusダッシュボードファブリック コントローラNexusダッシュボードファブリック コントローラ

4. 最上位のrouter bgpコマンドを使用してswitch_freeformポリシーを作成する必要があります。これにより、CCは以前にプッシュされた目的のサブ設定のみを削除するために必要な設定を生成できます。Nexusダッシュボード ファブリック コントローラ

5. 削除された設定は、以前にプッシュされた設定のサブセットのみです。Nexusダッシュボード ファブリック コントローラ

   外部ファブリックのスイッチのインターフェイスでは、インターフェイス全体を管理するか、まったく管理しません。Nexusダッシュボード ファブリック コントローラCC は次の方法でインターフェイスをチェックします。

   - 任意のインターフェイスについて、ポリシーが定義され、関連付けられている場合、このインターフェイスは管理対象と見なされます。このインターフェイスに関連付けられているすべての設定は、関連付けられたインターフェイス ポリシーで定義する必要があります。これは、論理インターフェイスと物理インターフェイスの両方に適用されます。それ以外の場合、CCは、インターフェイスに行われたアウトオブバンド更新を削除して、ステータスを[In-Sync]に変更します。
   - アウトオブバンドで作成されたインターフェイス（ポートチャネル、サブインターフェイス、SVI、ループバックなどの論理インターフェイスに適用）は、通常の検出プロセスの一部としてによって検出されます。Nexusダッシュボード ファブリック コントローラただし、これらのインターフェイスにはインテントがないため、CCはこれらのインターフェイスのOut-of-Syncステータスを報告しません。
   - どのインターフェイスでも、モニタ ポリシーは Nexusダッシュボード ファブリック コントローラに常に関連付けられています。この場合、CCはIn-SyncまたはOut-of-Sync設定コンプライアンスステータスを報告するときに、インターフェイスの設定を無視します。

構成コンプライアンスで無視される特別な構成 CLI

次の構成 CLI は、構成コンプライアンス チェック中に無視されます。

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

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

このような構成 CLI を展開するには、次の手順を実行します。

手順

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

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

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

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

ステップ 3 [ポリシー（Policies）] タブで、**[アクション（Actions）]** ドロップダウン リストから **[ポリシーの追加（Add Policy）]** を選択します。

ステップ 4 **switch_freeform** テンプレートを使用して、必要な構成 CLI を含むポリシー テンプレート インスタンス（PTI）を追加し、**[保存（Save）]** をクリックします。

ステップ 5 作成したポリシーを選択し、**[構成のプッシュ（Push Config）]**（**[アクション（Actions）]** ドロップダウン リスト）を選択して、構成をスイッチに展開します。

ディスカバリ用の非 Nexus デバイスの設定

Cisco Nexusダッシュボード ファブリック コントローラ で非 Nexus デバイスを検出する前に、スイッチ コンソールで設定します。

検出用の *IOS-XE* デバイスの設定

Nexusダッシュボード ファブリック コントローラ で Cisco IOS-XE デバイスを検出するには、次の手順を実行します。

手順

ステップ 1 スイッチ コンソールで次の SSH コマンドを実行します。

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

ステップ 2 SNMP ウォークを実行するには、Nexusダッシュボード ファブリック コントローラ コンソールで次のコマンドを実行します。

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

ステップ 3 スイッチ コンソールで次の SNMP コマンドを実行します。

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

検出用 *Arista* デバイスの構成

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

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

（注） SNMP パスワードはユーザ名のパスワードと同じにする必要があります。

[show run] コマンドを実行して設定を確認し、[show snmp view] コマンドを実行して SNMP ビューの出力を表示できます。

Show Run コマンド

```
switch (config)# snmp-server engineID local f5717f444ca824448b00
snmp-server view view_name SNMPv2 included
snmp-server view view_name SNMPv3 included
snmp-server view view_name default included
snmp-server view view_name entity included
snmp-server view view_name if included
snmp-server view view_name iso included
snmp-server view view_name lldp included
snmp-server view view_name system included
snmp-server view sys-view default included
snmp-server view sys-view ifmib included
snmp-server view sys-view system included
snmp-server community private ro
snmp-server community public ro
snmp-server group group_name v3 auth read view_name
snmp-server user user_name group_name v3 localized f5717f444ca824448b00 auth md5
be2eca3fc858b62b2128a963a2b49373 priv aes be2eca3fc858b62b2128a963a2b49373
!
spanning-tree mode mstp
```

```
!
service unsupported-transceiver labs f5047577
!
aaa authorization exec default local
!
no aaa root
!
username admin role network-admin secret sha512
$6$5ZKs/7.k2UxrWDg0$FOkdVQsBTnOquW/9AYx36YUBSPNLFdeuPIse9XgyHSdEOYXtPyT/0sMUYYdkMffuIjgn/d9rx/Do71XSbygSn/
username cvpadmin role network-admin secret sha512
$6$fLGFj/PUcuJT436i$Sj5G5c4y9cYjI/BZswjjmZW0J4npGrGqIyG3ZFk/ULza47Kz.d31ql3jXA7iHM677gwqQbFSH2/3oQEaHRq08.
username NDFC privilege 15 role network-admin secret sha512
$6$M48PNrCdg2EITEdG$iiB880nvFQQlrWoZwOMzdt5EfkuCIraNqtEMRS0TJUhNKCQnJN.VDLFsLAmP7kQBo.C3ct4/.n.2eRlcP6hij/
```

Show SNMP View コマンド

```
configure terminal# show snmp view
view_name SNMPv2 - included
view_name SNMPv3 - included
view_name default - included
view_name entity - included
view_name if - included
view_name iso - included
view_name lldp - included
view_name system - included
sys-view default - included
sys-view ifmib - included
sys-view system - included
leaf3-7050sx#show snmp user

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

検出用 *Cisco IOS-XR* デバイスの構成

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

```
switch# configure terminal
switch (config)# snmp-server view view_name cisco included
snmp-server view view_name mib-2 included
snmp-server group group_name v3 auth read view_name write view_name
snmp-server user user_name group_name v3 auth md5 password priv des56 password SystemOwner
```

（注） SNMP パスワードはユーザ名のパスワードと同じにする必要があります。

構成を確認するには、show run コマンドを実行します。

Cisco IOS-XR デバイスの構成と確認

```
RP/0/RSP0/CPU0:ios(config)#snmp-server view view_name cisco included
RP/0/RSP0/CPU0:ios(config)#snmp-server view view_name mib-2 included
```

```
RP/0/RSP0/CPU0:ios(config)#snmp-server group group_name v3 auth read view_name write
view_name
RP/0/RSP0/CPU0:ios(config)#snmp-server user user_name group_name v3 auth md5 password
priv des56 password SystemOwner
RP/0/RSP0/CPU0:ios(config)#commit Day MMM DD HH:MM:SS Timezone
RP/0/RSP0/CPU0:ios(config)#
RP/0/RSP0/CPU0:ios(config)#show run snmp-server Day MMM DD HH:MM:SS Timezone snmp-server
 user user_name group1 v3 auth md5 encrypted 10400B0F3A4640585851 priv des56 encrypted
000A11103B0A59555B74 SystemOwner
snmp-server view view_name cisco included
snmp-server view view_name mib-2 included
snmp-server group group_name v3 auth read view_name write view_name
```

外部ファブリックで非 Nexus デバイスの検出

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

始める前に

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

手順

ステップ 1 [アクション（Actions）] ペインで [スイッチの追加（Add switches）] をクリックします。

ステップ 2 [既存スイッチの検出（Discover Existing Switches）] タブの次のフィールドに値を入力します。

フィールド	説明
シードIP	スイッチの IP アドレスを入力します。 IPアドレスの範囲を入力することにより、複数のスイッチをインポートできます。たとえば、10.10.10.40 ～ 60 スイッチは適切にケーブル接続しサーバ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。Nexus ダッシュボード ファブリック コントローラ

フィールド	説明
デバイス タイプ	• Cisco CSR 1000v、Cisco ASR 1000 シリーズ ルータ、または Cisco Catalyst 9000 シリーズ スイッチを追加するには、ドロップダウンリストから [IOS XE] を選択します。 • ASR 9000 シリーズ ルータ、Cisco NCS 5500 シリーズ ルータ、IOS XR リリース 6.5.3 または Cisco 8000 シリーズ ルータを追加するには、ドロップダウンリストから [IOS XR] を選択します。 （注） 管理対象モードで Cisco IOS XR デバイスを追加するには、ファブリック設定の [全般パラメータ（General Parameters）] タブに移動し、[ファブリック モニタ モード（Fabric Monitor Mode）] チェックボックスをオフにします。 • シスコ以外のデバイス（Arista スイッチなど）を追加するには、ドロップダウンリストから [その他（Other）] を選択します。
ユーザ名	ユーザ名を入力します。
[パスワード（Password）]	パスワードを入力します。

（注） すでに検出されているデバイスを検出しようとすると、エラーメッセージが表示されます。

パスワードが設定されていない場合は、[LAN クレデンシャル（LAN Credentials）] ウィンドウでデバイスのパスワードを設定します。Cisco Web UI から [LAN クレデンシャル（LAN Credentials）] ウィンドウに移動するには、[管理（Administration）] > [LAN クレデンシャル（LAN Credentials）] を選択します。Nexusダッシュボード ファブリック コントローラ

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

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

ステップ 4 インポートするスイッチに隣接するチェックボックスをオンにします。

ステップ 5 [ファブリックにインポート（Import into fabric）] をクリックします。

スイッチ検出プロセスが開始されます。**[進行状況（Progress）]** 列には、進行状況が表示されます。

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

ステップ 6 [閉じる（Close）] をクリックします。

ファブリック トポロジ ウィンドウにスイッチが表示されます。

ステップ 7 （任意） 最新のトポロジ ビューを表示するには、**[トポロジの更新（Refresh topology）]** をクリックします。

ステップ 8 （任意） **[ファブリックの概要（Fabric Overview）]** をクリックします。

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

ステップ 9 （任意） デバイスの詳細を表示します。

デバイスの検出後：

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

（注） スイッチが [到達不能（Unreachable）] 検出ステータスの場合、スイッチの最後の使用可能な情報が他の列に保持されます。たとえば、スイッチが到達不能になる前にトラッカー ステータスが [実行中（RUNNING）] であった場合、スイッチが [到達不能（Unreachable）] 検出ステータスであっても、このスイッチの [トラッカー ステータス（Tracker Status）] 列の値は [実行中（RUNNING）] のままになります。

次のタスク

適切なロールを設定します。デバイスを右クリックし、[ロールの設定（Set role）] を選択します。

これらのデバイスを管理対象モードで追加した場合は、ポリシーも追加できます。

外部ファブリックでの 非 Nexus デバイスの管理

Nexusダッシュボード ファブリック コントローラ 12.0.1a 以降、IOS-XR は管理対象モードでサポートされます。

（注） IOS-XE および IOS-XR スイッチでは、外部ファブリックで Nexus スイッチを処理する場合と同様に、構成コンプライアンスが有効になります。詳細については、外部ファブリックでのコンプライアンスの構成 （61 ページ）を参照してください。

Nexusダッシュボード ファブリック コントローラは、IOS-XR デバイスの展開の最後にコミットを送信します。

Nexusダッシュボード ファブリック コントローラは、IOS-XR デバイス用のいくつかのテンプレートを提供します。IOS-XR スイッチの **[ios_xr_Ext_VRF_Lite_Jython.template]** を使用して、境界との eBGP ピアリングを確立します。これにより、VRF の構成、VRF の eBGP ピアリング、およびサブインターフェイスが作成されます。同様に、**[ios_xe_Ext_VRF_Lite_Jython]** を使用して、IOS-XE スイッチをエッジ ルータとして使用し、境界との eBGP ピアリングを確立できます。

vPC セットアップの作成

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

Procedure

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

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

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

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

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

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

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

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

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

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

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

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

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

ステップ 3 **[Save（保存）]** をクリックします。

vPC セットアップが作成されます。

vPC セットアップの詳細を更新するには、次の手順を実行します。

a. vPC スイッチを右クリックし、[vPC ペアリング] を選択します。

[vPC ピア（vPC peer）] ダイアログボックスが表示されます。

b. 必要に応じて、次のフィールドを更新します。

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

c. **[保存（Save）]** をクリックして更新を完了します。

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

vPC セットアップの展開解除

Procedure

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

vPC ピア画面が表示されます。

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

vPC ペアが削除され、ファブリック トポロジ ウィンドウが表示されます。

ステップ 3 **[構成の展開（Deploy Config）]** をクリックします。

ステップ 4 (Optional) **[構成の再計算（Recalculate Config）]**列の値をクリックします。

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

Note 同期していない場合は、ファブリックを再同期します。

ペアリングを解除すると、次の機能のPTIのみが削除されますが、**構成の展開中**に設定がクリアされません。NVE設定、LACP機能、ファブリック パス機能、nvオーバーレイ機能、ループバック プライマリ ID です。ホスト vPC の場合、ポート チャネルとそのメンバー ポートはクリアされません。必要に応じて、**[インターフェイス（Interfaces）]** ウィンドウからこれらのポートチャネルを削除できます。ペアリングを解除した後でも、スイッチでこれらの機能を引き続き使用できます。

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

IPFM ファブリック

このセクションでは、IP Fabric for Media（IPFM）に関連するファブリックの構成方法について説明します。IPFM ファブリック機能は、LAN ファブリックの一部です。IPFM ファブリック機能を有効にするには、**[設定（Settings）]** > **[機能管理（Feature Management）]** で LAN ファブリックの次の機能を有効にする必要があります。

- IP Fabric for Media：メディア コントローラに対応するマイクロサービスを開始します。
- PTP モニタリング：必要に応じて有効にします。ただし、IPFM とは独立していますが、IPTP には PTP モニタリングが使用されます。
- パフォーマンス モニタリング：基本インターフェイス モニタリングを提供します。

Nexusダッシュボード ファブリック コントローラバージョン 12.0.1a 以降、IPFM ファブリック テンプレートには次のタイプがあります。

- IPFM クラシック ファブリック：IPFM_Classic ファブリック テンプレートを使用して、既存の IPFM ファブリックからスイッチを導入します。このテンプレートは、管理 VRF/インターフェイスやホスト名などの基本的なスイッチ構成のみをインポートできる外部またはLANクラシック ファブリックのように動作します。ファブリックの属性を読み取り/書き込みまたは読み取り専用に設定できます。読み取り専用ファブリックの場合は、モニタ モードを有効にします。このテンプレートは、IPFM_Classic および Generic_Multicast テクノロジーをサポートします。

- IPFM Easy ファブリック：Easy_Fabric_IPFM テンプレートを使用して、Easy ファブリック管理で新しい IPFM ファブリックを作成し、IPFM ファブリックのアンダーレイ ネットワークを構築します。

（注） IPFM Easy ファブリックは、グリーンフィールド展開のみをサポートします。

NDFC 展開に 35 を超えるスイッチがある場合は、3 ノード クラスタを展開することをお勧めします。開始する前に仮想Nexusダッシュボードクラスタを使用している場合は、テレメトリ用に永続的なIPアドレスおよび必要な設定が有効になっていることを確認してください。Cisco Nexus Dashboard ファブリックコントローラ導入ガイドを参照してください。

新規インストールの場合は、要件に応じて IPFM Easy ファブリックまたは IPFM クラシック ファブリックを選択できます。

IPFM ファブリックの作成

IPFM ファブリックを作成するには、次の手順を実行します。

1. 適切なテンプレートを使用して必要な IPFM ファブリックを作成し、パラメータを設定します。IPFM_Classic テンプレートの詳細については、IPFM クラシック ファブリックの作成（113 ページ）を参照してください。Easy_Fabric_IPFM テンプレートの詳細については、IPFM Easy ファブリックの作成 （117 ページ）を参照してください。
2. ファブリックにスイッチを追加し、スイッチのロールを設定します（IPFM ファブリックではスパインとリーフのみがサポートされます）。スイッチの追加、既存および新規スイッチの検出、ロールの割り当て、およびスイッチの導入の詳細については、スイッチを参照してください。

（注） IPFM Easy ファブリックは、グリーンフィールド展開のみをサポートします。

3. ファブリックの [ファブリックの概要（Fabric Overview）] ウィンドウで、[アクション（Actions）] ドロップダウンリストから [構成の再計算（Recalculate Config）] を選択します。次に、[構成の展開（Deploy Configuration）] ウィンドウで、[展開（Deploy）] ボタンをクリックして構成を展開します。詳細については、ファブリックの概要 （163 ページ）を参照してください。

   IPFM Easy ファブリック：各スイッチのアンダーレイ構成は、ファブリック構成、スイッチ ロール、およびスイッチ プラットフォームに基づいて計算されます。

   IPFMクラシック ファブリック：ファブリックのインターフェイスを Nexus ダッシュボード ファブリック コントローラで管理する場合は、host_port_resync/Interface Config Resync を実行して、スイッチの移行プロセスを完了します。ホスト ポートの再同期の詳細については、アウトオブバンド スイッチ インターフェイスの構成の同期 （52 ページ）を参照してください。

IPFM ファブリックを編集または削除する場合は、IPFM ファブリックの編集 （126ページ）またはIPFM ファブリックの削除 （127 ページ）を参照してください。

4. 必要に応じて既存のインターフェイスを編集します。詳細については、IPFM ファブリック インターフェイスの編集 （131 ページ）を参照してください。新しい論理インターフェイスの詳細については、IPFM ファブリックのインターフェイスの作成 （127ページ）を参照してください。

IPFM クラシック ファブリックの作成

ここでは、**[IPFM_Classic ファブリック（IPFM_Classic fabric）]** テンプレートから IPFM クラシック ファブリックを作成する手順について説明します。

手順

ステップ 1 **[LAN ファブリック（LAN Fabrics）]** ウィンドウで、**[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。

（注） 初めてログインすると、**[LAN ファブリック（Lan Fabrics）]** ウィンドウに IPFM ファブリックのエントリが表示されません。ファブリックが作成されると、**[LAN ファブリック（Lan Fabrics）]** ウィンドウに表示されます。

ステップ 2 **[ファブリックの作成（Create Fabric）]** ウィンドウで、ファブリック名を入力し、**[テンプレートの選択（Choose Template）]** をクリックします。

[ファブリック テンプレートの選択（Select Fabric Template）] ウィンドウが表示されます。

ステップ 3 **IPFM_Classic** ファブリック テンプレートを検索またはスクロールして選択します。[選択（Select）] をクリックします。

[ファブリックの作成（Create Fabric）] ウィンドウは次の要素を表示します。

ファブリック名（Fabric Name）：入力したファブリック名を表示します。

テンプレートの選択（Pick Template）：選択したテンプレートの型を表示します。テンプレートを変更するには、そのテンプレートをクリックします。**[ファブリック テンプレートの選択（Select Fabric Template）]** ウィンドウが表示されます。現在の手順を繰り返します。

[全般パラメータ（General Parameters）]、[詳細（Advanced）]、および [ブートストラップ（Bootstrap）] タブ：IPFM クラシック ファブリックを作成するためのファブリック構成を表示します。

ステップ 4 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。このタブのフィールドは次のとおりです。

ファブリック テクノロジー（Fabric Technology）：ドロップダウンリストから次のいずれかのテクノロジーを選択します。

- **[IPFM_Classic]**

- **[Generic_Multicast]**

ファブリック モニタ モード（Fabric Monitor Mode）：ファブリックのみをモニタし、構成を展開しない場合は、このチェックボックスをオンにします。

パフォーマンス モニタを有効化（Enable Performance Monitoring）：ファブリックのパフォーマンスをモニタするにはこのチェックボックスをオンにします。

ステップ 5 [Advanced] タブをクリックします。このタブのフィールドは次のとおりです。

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

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

NDFC をトラップ ホストとして有効にする（Enable NDFC as Trap Host）：Nexus ダッシュボードファブリック コントローラをトラップ ホストとして有効にするには、このチェックボックスをオンにします。

ブートストラップ スイッチの CDP の有効化（Enable CDP for Bootstrapped Switch）：管理インターフェイスで CDP を有効にします。

インバンド管理（Inband Mgmt）：外部およびクラシック LAN ファブリックの場合、このノブを使用するとNexusダッシュボードファブリック コントローラは、インバンド接続（スイッチ ループバック、ルーテッド、または SVI インターフェイス経由で到達可能）でのスイッチのインポートおよび管理が可能になり、またアウトオブバンド接続（スイッチmgmt0インターフェイス経由で到達可能）でのスイッチの管理が可能になります。唯一の要件は、インバンド管理対象スイッチの場合、Nexusダッシュボード ファブリック コントローラからeth2（つまり、インバンド インターフェイス）を介してスイッチに IP が到達可能であることです。インバンド管理を有効にした後、検出中に、インバンド管理を使用してインポートするすべてのスイッチの IP を指定し、最大ホップ数を 0 に設定します。Nexusダッシュボード ファブリック コントローラにはインバンド管理対象スイッチ IP が eth2 インターフェイス経由で到達可能であることを検証する事前チェックがあります。事前チェックをパスすると、Nexusダッシュボード ファブリック コントローラはインターフェイスが属する VRF に加えて、指定された検出 IP を持つそのスイッチ上のインターフェイスを検出し、学習します。スイッチのインポート/検出のプロセスの一部として、この情報はNexusダッシュボードファブリック コントローラに入力される目的のベースラインにキャプチャされます。詳細については、外部ファブリックおよび LAN クラシック ファブリックでのインバンド管理 （137 ページ）を参照してください。

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

ファブリック フリーフォーム（Fabric Freeform）：この自由形式フィールドを使用して、外部ファブリックで検出されたすべてのデバイスに構成をグローバルに適用できます。

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

ステップ 6 **[ブートストラップ（Bootstrap）]** タブをクリックします。このタブのフィールドは次のとおりです。

ブートストラップの有効化（NX-OS スイッチのみ）（Enable Bootstrap）（For NX-OS Switches Only） ：Cisco Nexus スイッチのみに対してブートストラップ機能を有効にするにはこのチェックボックスをオンにします。このチェックボックスをオンにすると、POAP の自動 IP 割り当てが有効になります。

ブートストラップをイネーブルにした後、次の方法を使用して、POAP の自動 IP アドレス割り当てに対して DHCP サーバをイネーブルにできます。

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

ローカル DHCP サーバの有効化（Enable Local DHCP Server） ：ローカル DHCP サーバを介した自動 IP アドレス割り当ての有効化を開始するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、残りのすべてのフィールドが編集可能になります。

DHCP バージョン（DHCP Version） ：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。

（注） Nexusダッシュボード ファブリック コントローラCisco IPv6 POAP は、Cisco Nexus 7000 シリーズ スイッチではサポートされていません。Cisco Nexus 9000 および 3000 シリーズ スイッチは、スイッチが L2 隣接（eth1 またはアウトオブバンド サブネットは /64 が必須）、またはスイッチがいくつかの IPv6 /64 サブネット内に存在する L3 隣接である場合にのみ、IPv6 POAP をサポートします。/64 以外のサブネット プレフィックスはサポートされていません。

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

DHCP スコープ開始アドレス（DHCP Scope Start Address） および **DHCP スコープ終了アドレス（DHCP Scope End Address）** ：スイッチ アウトオブバンド POAP に使用される IP アドレス範囲の最初と最後の IP アドレスを指定します。

スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway） ：スイッチの管理 VRF のデフォルト ゲートウェイを指定します。

スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix） ：スイッチの Mgmt0 インターフェイスのプレフィックスを指定します。プレフィックスは 8 ～ 30 の間である必要があります。

DHCP スコープおよび管理デフォルト ゲートウェイ IP アドレスの仕様（DHCP scope and management default gateway IP address specification）：管理デフォルト ゲートウェイ IP アドレスを 10.0.1.1 に、サブネット マスクを 24 に指定した場合、DHCP スコープが指定したサブネット、10.0.1.2 ～ 10.0.1.254 の範囲内であることを確認してください。

スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）：スイッチの Mgmt0 インターフェイスの IPv6 プレフィックスを指定します。プレフィックスは 64 ～ 126 の間である必要があります。このフィールドは DHCP の IPv6 が有効な場合に編集できます。

ブートストラップ自由形式の構成（Bootstrap Freeform Config）：（任意）必要に応じて追加のコマンドを入力します。たとえば、AAA またはリモート認証関連の構成を使用している場合は、このフィールドにこれらの構成を追加してインテントを保存する必要があります。デバイスが起動すると、**[ブートストラップ自由形式の構成（Boostrap Freeform Config）]** フィールドで定義されたインテントが含まれます。

running-config をコピーして **[自由形式の構成（freeform config）]** フィールドに正しいインデントでペーストします。NX-OS スイッチの実行構成に表示されているように正しく行ってください。freeform config は running-config と一致する必要があります。スイッチでの自由形式の構成エラーの解決（*Resolving Freeform Config Errors in Switches*）について詳細は、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 （66 ページ）を参照してください。

DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）：1 行に 1 つのサブネット スコープを入力するフィールドを指定します。このフィールドは、**[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）]** チェックボックスをオンにした後に編集できます。

スコープの形式は次のように定義される必要があります。

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）

たとえば、16.0.0.2、10.6.0.9、10.6.0.1、24 です。

ステップ 7 **[Save（保存）]** をクリックします。

IPFM クラシック ファブリックが作成され、**[LAN ファブリック（Lan Fabrics）]** ウィンドウのテーブルに表示されます。

次のタスク

ファブリックの作成後、[構成の再計算（Recalculate Config）] を実行し、スイッチに構成を行ってください。詳細については、ファブリックの概要 （163 ページ）を参照してください。

その後必要に応じて、インターフェイスを編集または作成してください。詳細については、IIPFM ファブリックのインターフェイス構成 を参照してください。

IPFM Easy ファブリックの作成

ここでは、[IPFM_Easy ファブリック（IPFM_Easy fabric）] テンプレートから IPFM Easy ファブリックを作成する手順について説明します。

手順

ステップ 1 **[LAN ファブリック（LAN Fabrics）]** ウィンドウで、**[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。

（注） 初めてログインしたときには、[LAN ファブリック（Lan Fabrics）] テーブルにはまだエントリはありません。ファブリックが作成されると、**[LAN ファブリック（Lan Fabrics）]** ウィンドウに表示されます。

ステップ 2 **[ファブリックの作成（Create Fabric）]** ウィンドウで、ファブリック名を入力し、**[テンプレートの選択（Choose Template）]** をクリックします。

[ファブリック テンプレートの選択（Select Fabric Template）] ウィンドウが表示されます。

ステップ 3 **Easy_Fabric_IPFM** テンプレートを検索またはスクロールして選択します。[選択（Select）] をクリックします。

[ファブリックの作成（Create Fabric）] ウィンドウは次の要素を表示します。

ファブリック名（Fabric Name）：入力したファブリック名を表示します。

テンプレートの選択（Pick Template）：選択したテンプレートの型を表示します。テンプレートを変更するには、そのテンプレートをクリックします。**[ファブリック テンプレートの選択（Select Fabric Template）]** 画面が表示されます。現在の手順を繰り返します。

[全般パラメータ（General Parameters）]、**[マルチキャスト（Multicast）]**、**[プロトコル（Protocols）]**、**[詳細（Advanced）]**、**[管理能力（Manageability）]**、および **[ブートストラップ（Bootstrap）]** タブ：IPFM Easy Fabric を作成するためのファブリック設定を表示します。

ステップ 4 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。このタブのフィールドは次のとおりです。

[ファブリックインターフェイスの番号付け（Fabric Interface Numbering）：]：番号付き（ポイントツーポイント、つまり **p2p**）ネットワークのみをサポートします。

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

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

[ファブリック ルーティング ループバック ID（Fabric Routing Loopback 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。有効な値の範囲は 0 ～ 1023 です。

[手動ファブリック IP アドレス割り当て（Manual Fabric IP Address Allocation）]：ファブリック IP アドレスの動的割り当てを無効にします。

- デフォルトでは、Nexusダッシュボード ファブリック コントローラ は定義されたプールからアンダーレイ 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）を動的に割り当てます。このチェックボックスをオンにすると、割り当て方式が静的に切り替わり、動的 IP アドレス範囲フィールドの一部が無効になります。
- 静的割り当ての場合、REST API を使用してアンダーレイ IP アドレス リソースをリソース マネージャ（RM）に入力する必要があります。
- 詳細については、『*Cisco Nexus*ダッシュボード ファブリック コントローラ *REST API Reference Guide, Release 12.0.1a*』を参照してください。スイッチをファブリックに追加した後、REST APIを呼び出してから **[保存して展開（Save & Deploy）]** オプションを使用する必要があります。
- 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。

[ファブリック ルーティング ループバック IP 範囲（Fabric Routing Loopback IP Range）]：プロトコル ピアリングのループバック IP アドレスの範囲を指定します。

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

[パフォーマンス モニタリングの有効化（Enable Performance Monitoring）]：ファブリックのパフォーマンスをモニタするには、このチェックボックスをオンにします。

ステップ 5 **[マルチキャスト（Multicast）]** タブをクリックします。このタブのフィールドは次のとおりです。

[NBM パッシブモードの有効化（Enable NBM Passive Mode）]：このチェックボックスをオンにすると、NBM モードが pim-passive になります。NBM パッシブ モードを有効にすると、スイッチはすべての RP および MSDP 設定を無視します。これは必須のチェックボックスです。このチェックボックスをオンにすると、残りのフィールドとチェックボックスは無効になります。詳細については、「Configuring an NBM VRF for Static Flow Provisioning」セクション（『*Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide, Release 10.2(x)*』）を参照してください。

[ASMの有効化（Enable ASM）]：（*、G）結合を送信する受信者を持つグループを有効にするには、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をオンにすると、ASM 関連のセクションが有効になります。

[デフォルト VRF のための NBM フロー ASM グループ（SPT しきい値無限あり/なし）（NBM Flow ASM Groups for default VRF（w / wo SPT-Threshold Infinity））]：このセクションは、ASM 関連の情報で構成されます。

- セクションを縮小または展開するには、このセクションのタイトルの横にある展開矢印をクリックします。

- **[アクション（Actions）]** ドロップダウンリストを使用して、テーブル内の ASM グループを追加、編集、または削除します。
  - **[追加（Add）]**：**[項目の追加（Add Item）]** ウィンドウを開きます。**[項目の追加（Add Item）]** ウィンドウで、次の手順を実行します。
    1. フィールドに適切な値を入力し、次のようにチェックボックスをオンまたはオフにします。
       - **[Group_Address]**：NBM フロー ASM グループ サブネットの IP アドレスを指定します。
       - **[プレフィックス（Prefix）]**：ASM グループ サブネットのサブネット マスク長を指定します。サブネット マスク長の有効な値の範囲は 4 ー 32 です。たとえば、239.1.1.0 / 25 はプレフィックス付きのグループ アドレスです。
       - **Enable_SPT_Threshold**：SPT しきい値の無限を有効にするには、このチェックボックスをオンにします。
    2. **[保存（Save）]** をクリックして、設定した NBM フロー ASM グループをテーブルに追加するか、**[キャンセル（Cancel）]** をクリックして値を破棄します。
  - **[編集（Edit）]**：グループアドレスの横にあるチェックボックスをオンにし、**[項目の編集（Edit Item）]** ウィンドウを開きます。編集項目を開き、ASM グループパラメータを編集します。**[保存（Save）]** をクリックしてテーブルの値を更新するか、**[キャンセル（Cancel）]** をクリックして値を破棄します。
  - **[削除（Delete）]**：テーブルからASMグループを削除するには、グループ アドレスの横にあるチェックボックスをオンにし、このオプションを選択します。
- テーブルには、グループ アドレス、プレフィックス、および SPT 有効化しきい値の値が表示されます。

RP ループバック ID（RP Loopback Id）：ファブリック アンダーレイでのマルチキャスト プロトコル ピアリングの目的で、ランデブー ポイント（RP）に使用されるループバック ID。有効な値の範囲は 0 ～ 1023 です。

ファブリック RP ループバック IP 範囲（Fabric RP Loopback IP Range）：RP ループバック IP アドレス範囲を指定します。

ステップ 6 **[プロトコル（Protocols）]** タブをクリックします。このタブのフィールドは次のとおりです。

ファブリック ルーティング プロトコル タグ（Fabric Routing Protocol Tag）：ファブリックのルーティング プロセス タグを指定します。

OSPF エリア ID（OSPF Area 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。

（注） [OSPF] または [IS-IS] 認証フィールドは、**[ファブリック ルーティング プロトコル（Fabric Routing Protoco）l]** フィールド（**[全般パラメータ（General Parameters）]** タブ）での選択に基づいて有効になります。

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

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

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

（注） 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 （124 ページ） セクションを参照してください。

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

[IS-IS ネットワーク ポイントツーポイントの有効化（Enable IS-IS Network Point-to-Point）]：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（Enable IS-IS Authentication）]：IS-IS 認証を有効にするには、チェックボックスをオンにします。無効にするには、チェックボックスをオフにします。このフィールドを有効にすると、[IS-IS] 認証フィールドが有効になります。

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

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

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

（注） 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 （124 ページ） セクションを参照してください。

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

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

ステップ 7 [Advanced] タブをクリックします。このタブのフィールドは次のとおりです。

[イントラ ファブリック インターフェイス MTU（Intra Fabric Interface MTU）]：ファブリック内インターフェイスの MTU を指定します。この値は偶数にする必要があります。有効な値の範囲は 576 ～ 9216 です。これは必須フィールドです。

[レイヤ 2 ホスト インターフェイス MTU（Layer 2 Host Interface MTU）]：レイヤ 2 ホスト インターフェイスの MTU を指定します。この値は偶数にする必要があります。有効な値の範囲は 1500 ～ 9216 です。

[Power Supply Mode]：ドロップダウンリストから、ファブリックのデフォルトモードとなる適切な電源モードを選択します。これは必須フィールドです。

[ブートストラップ スイッチの CDP を有効にする（Enable CDP for Bootstrapped Switch）]：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。

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

[NDFC をトラップ ホストとして有効化（Enable NDFC as Trap Host）]：Nexusダッシュボード ファブリック コントローラ を SNMPトラップの宛先として有効にするには、このチェックボックスをオンにします。通常、ネイティブHA 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。

[精密時間プロトコル (PTP) の有効化 (Enable Precision Time Protocol (PTP))]：ファブリック全体でPTPを有効にします。このチェックボックスをオンにすると、PTPはグローバルに、およびファブリック内インターフェイスで有効になります。また、**[PTP 送信元ループバック ID（PTP Source Loopback Id）]** および **[PTP ドメイン ID（PTP Domain Id）]** フィールドが編集可能になります。詳細については、Easy ファブリック向け高精度時間プロトコル （46 ページ）を参照してください。

[PTP 送信元ループバック ID（PTP Source Loopback Id）]：すべての PTP パケットの送信元 IP アドレスとして使用されるループバック インターフェイス ID ループバックを指定します。有効な値の範囲は 0 ～ 1023 です。PTP ループバック ID を RP ループバック ID と同じにすることはできません。そうした場合は、エラーが表示されます。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。PTP ループバックが作成されていない場合は、自動的に作成されます。

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

[PTP プロファイル（PTP Profile）]：リストからPTPプロファイルを選択します。PTPプロファイルは、ISL リンクでのみ有効になります。サポートされている PTP プロファイルは、IEEE-1588v2、SMPTE-2059-2、および AES67-2015 です。

[リーフの自由形式の設定（Leaf Freeform Config）]：リーフ、境界、および境界ゲートウェイの役割を持つスイッチに追加する必要がある CLI です。

[スパインの自由形式の設定（Spine Freeform Config）]：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 スパインのロールを持つスイッチに追加する必要がある CLI を追加します。

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

ステップ 8 **管理能力（Manageability）** タブをクリックします。このタブのフィールドは次のとおりです。

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

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

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

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

[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 サーバーの重大度（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。高い重大度を指定するには、大きい数値を入力します。

[Syslog サーバー 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 フリーフォームの設定（AAA Freeform Config）：AAA フリーフォームの設定を指定します。

ファブリック設定で AAA 設定が指定されている場合は、**switch_freeform** PTI で、ソースが **UNDERLAY_AAA** で説明が **AAAConfigurations** であるものが作成されます。

ステップ 9　**[ブートストラップ（Bootstrap）]** タブをクリックします。このタブのフィールドは次のとおりです。

[ブートストラップの有効化（Enable Bootstrap）]：ブートストラップ機能を有効にします。ブートストラップを使用すると、新しいデバイスを day-0 段階で簡単にインポートし、既存のファブリックに組み込むことができます。ブートストラップは NX-OS POAP 機能を活用します。

ブートストラップを有効にした後、次のいずれかの方法を使用して、DHCP サーバーで IP アドレスの自動割り当てを有効にできます。

- 外部 DHCP サーバー（External DHCP Server）：**[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]** および **[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** フィールドに外部 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（Enable Local DHCP Server）：ローカル DHCP サーバーを介した自動 IP アドレス割り当ての有効化を開始するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、**[DHCP スコープ開始アドレス（DHCP Scope Start Address）]** および **[DHCP スコープ終了アドレス（DHCP Scope End Address）]** フィールドが編集可能になります。

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

[DHCP バージョン（DHCP Version）]：このドロップダウンリストから [DHCPv4] または [DHCPv6] を選択します。[DHCPv4] を選択すると、**[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]** フィールドは無効になります。DHCPv6 を選択すると、**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** フィールドは無効になります。

（注） Cisco Nexus 9000 および 3000 シリーズ スイッチは、スイッチが L2 隣接（eth1 またはアウトオブバンド サブネットは /64 が必須）、またはスイッチがいくつかの IPv6 /64 サブネット内に存在する L3 隣接である場合にのみ、IPv6 POAP をサポートします。/64 以外のサブネット プレフィックスはサポートされていません。

[DHCP スコープ開始アドレス（DHCP Scope Start Address）]：スイッチのアウトオブバンド POAP に使用する IP アドレス範囲の最初の IP アドレスを指定します。

[DHCP スコープ終了アドレス（DHCP Scope End Address）]：スイッチのアウトオブバンド POAP に使用する IP アドレス範囲の最後の IP アドレスを指定します。

[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]：スイッチの管理 VRF のデフォルト ゲートウェイを指定します。

スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）：スイッチの Mgmt0 インターフェイスのプレフィックスを指定します。プレフィックスは 8 ～ 30 の間である必要があります。

DHCP スコープおよび管理デフォルト ゲートウェイ *IP* アドレスの仕様（*DHCP scope and management default gateway IP address specification*）：管理デフォルト ゲートウェイ IP アドレスを 10.0.1.1 に、サブネット マスクを 24 に指定した場合、DHCP スコープが、指定したサブネット、10.0.1.2 ～ 10.0.1.254 の範囲内であることを確認してください。

[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]：スイッチの Mgmt0 インターフェイスの IPv6 プレフィックスを指定します。プレフィックスは 64 ～ 126 の間である必要があります。このフィールドは DHCP の IPv6 が有効な場合に編集できます。

[AAA 設定の有効化（Enable AAA Config）]：ブートストラップ後のデバイス起動設定の一部として **[管理可能性（Manageability）]** タブから AAA 設定を含めます。

[ブートストラップ フリーフォームの設定（Bootstrap Freeform Config）]：（オプション）必要に応じて追加のコマンドを入力します。たとえば、デバイスにプッシュするいくつかの追加の設定が必要であり、ポスト デバイス ブートストラップが使用可能である場合、このフィールドでキャプチャして要求のとおりに保存することが可能です。デバイスの起動後、**[ブートストラップ 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 **[自由形式の構成（freeform config）]** フィールドに正しいインデントでペーストします。NX-OS スイッチの実行構成に表示されているように正しく行ってください。freeform config は running-config と一致する必要があります。スイッチでの自由形式の構

成エラーの解決（*Resolving Freeform Config Errors in Switches*）について詳細は、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 （66 ページ）を参照してください。

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

スコープの形式は次の順で定義する必要があります。

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

例：16.0.0.2、10.6.0.9、10.6.0.1、24

ステップ 10 **[Save（保存）]** をクリックします。

IPFM Easy ファブリックが作成され、**[LAN ファブリック（Lan Fabrics）]** ウィンドウのテーブルに表示されます。

次のタスク

ファブリックの作成後、[構成の再計算（Recalculate Config）] を実行し、スイッチに構成を行ってください。詳細については、ファブリックの概要 （163 ページ）を参照してください。

その後必要に応じて、インターフェイスを編集または作成してください。詳細については、IIPFM ファブリックのインターフェイス構成 を参照してください。

認証キーの取得

3DES 暗号化 OSPF 認証キーの取得

1. スイッチに SSH 接続します。
2. 未使用のスイッチインターフェイスで、次を有効にします。

```
config terminal
    feature ospf
    interface Ethernet1/1
       no switchport
       ip ospf message-digest-key 127 md5 ospfAuth
```

この例では、**ospfAuth** は暗号化されていないパスワードです。

（注） このステップ 2 は、新しいキーを設定する場合に必要です。

3. **show run interface Ethernet1/1** コマンドを入力してパスワードを取得します。

```
Switch # show run interface Ethernet1/1
   interface Ethernet1/1
```

```
no switchport
ip ospf message-digest key 127 md5 3 sd8478f4fsw4f4w34sd8478fsdfw
no shutdown
```

md5 3 の後の文字のシーケンスは、暗号化されたパスワードです。

4. **[OSPF 認証キー（OSPF Authentication Key）]** フィールドの暗号化されたパスワードを更新します。

暗号化された IS-IS 認証キーの取得

キーを取得するには、スイッチにアクセスできる必要があります。

1. スイッチに SSH 接続します。
2. 一時キーチェーンを作成します。

```
config terminal
   key chain isis
   key 127
   key-string isisAuth
```

この例では、**isisAuth** はプレーンテキスト パスワードです。これは、CLI が受け入れられた後に Cisco タイプ 7 パスワードに変換されます。

3. **show run | section “key chain”** コマンドを入力してパスワードを取得します。

```
key chain isis
   key 127
       key-string 7 071b245f5a
```

key-string 7 の後の文字のシーケンスは、暗号化されたパスワードです。設定を保存します。

4. [OSPF 認証キー（OSPF Authentication Key）] フィールドの暗号化されたパスワードを更新します。
5. ステップ 2 で行った不要な設定を削除します。

3DES 暗号化 BGP 認証キーの取得

1. スイッチに SSH 接続し、存在しないネイバーの BGP 設定を有効にします。

（注） 存在しないネイバー設定は、パスワードを取得するための一時的な BGP ネイバー設定です。

```
router bgp
   neighbor 10.2.0.2 remote-as 65000
   password bgpAuth
```

この例では、**bgpAuth** は暗号化されていないパスワードです。

2. パスワードを取得するには、show run bgp コマンドを入力します。サンプル出力：

```
neighbor 10.2.0.2
   remote-as 65000
   password 3 sd8478fswerdfw3434fsw4f4w34sdsd8478fswerdfw3434fsw4f4w3
```

パスワード 3 の後の文字のシーケンスは、暗号化されたパスワードです。

3. **[BGP 認証キー（BGP Authentication Key）]** フィールドの暗号化されたパスワードを更新します。
4. BGP ネイバー設定を削除します。

暗号化された BFD 認証キーの取得

1. スイッチに SSH 接続します。
2. 未使用のスイッチインターフェイスで、次を有効にします。

```
switch# config terminal
switch(config)# int e1/1
switch(config-if)# bfd authentication keyed-SHA1 key-id 100 key cisco123
```

この例では、**cisco123** は暗号化されていないパスワードで、キー ID は **100** です。

（注） このステップ 2 は、新しいキーを設定する場合に必要です。

3. キーを取得するには、**show running-config interface** コマンドを入力します。

```
switch# show running-config interface Ethernet1/1

interface Ethernet1/1
description connected-to- switch-Ethernet1/1
no switchport
mtu 9216
bfd authentication Keyed-SHA1 key-id 100 hex-key 636973636F313233
no ip redirects
ip address 10.4.0.6/30
no ipv6 redirects
ip ospf network point-to-point
ip router ospf 100 area 0.0.0.0
no shutdown
```

BFD キー ID は **100** で、暗号化キーは **636973636F313233** です。

4. **[BFD 認証キー（BFD Authentication Key ID）]** フィールドと **[BFD 認証キー（BFD Authentication Key）]** フィールドのキー ID とキーを更新します。

IPFM ファブリックの編集

[LAN ファブリック（LAN Fabrics）] ウィンドウで、編集するファブリックを選択します。**[アクション（Actions）]** ドロップダウン リストから、**[ファブリックの編集（Edit Fabric）]** を選択します。必要に応じてテンプレートのフィールドを編集します**[Save（保存）]** をクリックします。

（注） ファブリックの設定を変更したら、[構成の再計算（Recalculate Config）] を実行し、構成をスイッチに展開します。

IPFM ファブリックの削除

[LAN ファブリック（LAN Fabrics）] ウィンドウで、削除するファブリックを選択します。**[アクション（Actions）]** ドロップダウン リストから、**[ファブリックの削除（Delete Fabric）]** を選択します。ファブリックを削除するかどうかを確認するメッセージが表示されたら、**[確認（Confirm）]** をクリックします。

IIPFM ファブリックのインターフェイス構成

Cisco Nexusダッシュボード ファブリック コントローラ Web UI では、ファブリック内の各スイッチに IPFM 外部リンクを設定できます。外部デバイスは、IPFM External-Link としてマーキングすることで、このインターフェイスを介してネットワークに接続できます。

（注） Nexusダッシュボード ファブリック コントローラのネットワーク オペレータ ロールを持つユーザは、インターフェイス設定を保存、展開、展開解除、または編集できません。

Nexusダッシュボード ファブリック コントローラリリース 12.0.1a 以降、IPFM ファブリックのインターフェイスはNexusダッシュボードファブリック コントローラインターフェイス マネージャによって管理されます。

IPFM のデフォルトのインターフェイス ポリシーは int_ipfm_l3_port です。

IPFM ファブリックの非ファブリック イーサネット インターフェイス ポリシー テンプレートは、int_ipfm_l3_port、int_ipfm_access_host、および int_ipfm_trunk_host です。

IPFM ファブリックのポート チャネル インターフェイス ポリシー テンプレートは、int_ipfm_port_channel_access_host、int_ipfm_port_channel_trunk_host、int_ipfm_port_channel_access_member、および int_ipfm_port_channel_trunk_member です。

IPFM ファブリックのスイッチ仮想インターフェイス（SVI）テンプレートは int_ipfm_vlan です。

IPFM ファブリックのインターフェイスの作成

ここでは、使用可能な IPFM ファブリック インターフェイス テンプレートから選択したテンプレートに基づいて、IPFM ファブリックの新しいインターフェイスを作成する手順について説明します。

（注） IPFM ファブリックは V6 アンダーレイをサポートしません。

手順

ステップ 1 ファブリックの**[ファブリックの概要（Fabric Overview）]**ウィンドウに移動し、**[インターフェイス（Interfaces）]**タブをクリックします。

ステップ 2 **[新しいインターフェイスの作成（Create new interface）]**を**[アクション（Actions）]**drop-down list.[インターフェイスの編集 (Edit interface)] を [アクション (Actions)] ドロップダウン リストから 選択します。

[新しいインターフェイス（New Interfaces）] ウィンドウが表示されます。

ステップ 3 IPFM のインターフェイス タイプとして、[ポートチャネル（Port Channel）]、[ループバック（Loopback）]、または [SVI] を選択します。

ステップ 4 ドロップダウン リストからデバイスを選択します。ファブリックの一部であるスイッチ（スパインおよびリーフ）がドロップダウン リストに表示されます。

ステップ 5 インターフェイス タイプの選択に基づいて、[ポートチャネル ID（Port Channel ID）]、[ループバック ID（Loopback ID）,または [VLAN ID] を入力します。

ステップ 6 **[ポリシー未選択（No Policy Selected）]** リンクをクリックして、IPFM に固有のポリシーを選択します。**[アタッチするポリシーの選択（Select Attached Policy Template）]** ダイアログ ボックスで、必要なインターフェイス ポリシー テンプレートを選択し、**[保存（Save）]** をクリックします。

ステップ 7 **[ポリシー オプション（Policy Options）]**領域に適切な値を入力します。ポリシーに基づいて、それに応じた[ポリシーオプション（Policy Options）]フィールドが表示されることに注意してください。

- **[タイプ：ポートチャネル（Type - Port Channel）]**

  [ポートチャネル メンバー インターフェイス（Port Channel Member Interfaces）]：メンバー インターフェイスのリストを指定します（例：e1/5、eth1/7-9）。

  [ポートチャネル モード（Port Channel Mode）]：次のチャネル モード オプションとして、[オン（on）]、[アクティブ（active）]、または [パッシブ（passive）] のいずれかを選択します。

  [BPDU ガードの有効化（Enable BPDU Guard）]：スパニングツリー ブリッジ プロトコル データ ユニット（BPDU）ガードのオプションとして、次のいずれかを選択します。

  - true：bdpuguard を有効にします
  - false：bpduguard を無効にします
  - no：デフォルト設定に戻します。

  [ポート タイプ高速の有効化（Enable Port Type Fast）]：このチェックボックスをオンにすると、スパニングツリー エッジ ポートの動作が有効になります。

  [MTU]：ポートチャネルまたはインターフェイスの最大伝送ユニット（MTU）を指定します。インターフェースでの MTU の有効な値の範囲は 576 ～ 9216 です。

  [速度（SPEED）]：ポートチャネルの速度またはインターフェイスの速度を指定します。

[アクセス VLAN（Access Vlan）]：アクセス ポートの VLAN を指定します。

[トランク許可された VLAN（Trunk Allowed Vlans）]：次のいずれかの値を入力します。

- なし
- all
- VLANの範囲（1ー200、500ー2000、3000 など）

[PTP の有効化（Enable PTP）]：IPFM ファブリックのホスト インターフェイスの高精度時間プロトコル（Precision Time Protocol、PTP）を有効にします。PTP の詳細については、IPFM ファブリックの PTP 構成 （131 ページ） を参照してください。

[PTPプロファイル（PTP Profile）]：ドロップダウン リストから PTP プロファイルとして **[IEEE-1588v2]**、**[SMPTE-2059-2]**、または **[AES67-2015]** のいずれかを選択します。

[PTP VLAN（PTP Vlan）]：PTP が有効な場合のメンバー インターフェイスの PTP VLAN を指定します。

[ポートチャネルの説明（Port Channel Description）]：ポートチャネルの説明を入力します。

[フリーフォームの設定（Freeform Config）]：必要に応じて、ポートチャネルの追加 CLI を入力します。

[ポートチャネルの有効化（Enable Port Channel）]：ポートチャネルを有効にするには、このチェックボックスをオンにします。

- **[タイプ：ループバック（Type - Loopback）]**

[インターフェイス VRF（Interface VRF）]：インターフェイス VRF の名前を入力します。デフォルトの VRF の場合は **default** と入力します。

[ループバック IP（Loopback IP）]：ループバック インターフェイスの IPv4 アドレスを入力します。

[ループバック IPv6 アドレス（Loopback IPv6 address）]：VRFがデフォルト以外の場合、ループバック インターフェイスの IPv6 アドレスを入力します。デフォルトVRFの場合は、フリーフォームで IPv6 アドレスを追加します。

[ルートマップ タグ（Route-Map TAG）]：インターフェイス IP に関連付けられたルートマップ タグを入力します。

[インターフェイスの説明 (Interface Description)]：インターフェイスの説明を入力します。説明は最大 254 文字です。

[フリーフォームの設定（Freeform Config）]：必要に応じて、ループバック インターフェイスの追加 CLI を入力します。

[インターフェイスの有効化（Enable Interface）]：インターフェイスを有効にするには、このチェックボックスをオンにします。

- **[タイプ：SVI（Type - SVI）**

[インターフェイス VRF（Interface VRF）]：インターフェイス VRF の名前を入力します。デフォルトの VRF の場合は **default** と入力します。

[VLAN インターフェイス IP（VLAN Interface IP）]：VLAN インターフェイスの IP アドレスを入力します。

[IP ネットマスク長（IP Netmask Length）]：IP アドレスで使用される IP ネットマスク長を指定します。有効な値の範囲は 1 ～ 31 です。

[ルーティング TAG（Routing TAG）]：インターフェイス IP に関連付けられたルーティング タグを入力します。

[MTU]：ポートチャネルまたはインターフェイスの最大伝送ユニット（MTU）を指定します。インターフェースでの MTU の有効な値の範囲は 576 ～ 9216 です。

[IP リダイレクトの無効化（Disable IP redirects）]：インターフェイスで IPv4 と IPv6 の両方のリダイレクトを無効にします。

[IPFM 外部リンク (IPFM External-Link)]：インターフェイスを外部ルーターに接続することを指定するには、このチェックボックスをオンにします。

[インターフェイスの説明 (Interface Description)]：インターフェイスの説明を入力します。説明は最大 254 文字です。

[フリーフォームの設定（Freeform Config）]：必要に応じて、VLAN インターフェイスの追加 CLI を入力します。

[インターフェイス管理状態（Interface Admin State）]：インターフェイスの管理状態を有効にするには、このチェックボックスをオンにします。

ステップ 8 要件に基づいて、次のいずれかのボタンをクリックします。

- [保存 (Save)]：設定の変更を保存するには、**[保存 (Save)]** をクリックします。
- [プレビュー (Preview)]：**[プレビュー (Preview)]** をクリックすると、**[インターフェイス設定のプレビュー (Preview interfaces configuration)]** ウィンドウが開いて、詳細が表示されます。
- [展開 (Deploy)]：インターフェイスを設定するには、**[展開 (Deploy)]** をクリックします。

次のタスク

インターフェイスを編集する場合は、IPFM ファブリック インターフェイスの編集 （131 ページ） を参照してください。

インターフェイスの準備ができたら、IPFM ファブリックを設定するためのポリシーを追加します。詳細については、「IPFM ファブリックを構成するポリシーの追加 （132 ページ）」を参照してください。

IPFM ファブリックの *PTP* 構成

Precision Time Protocol（PTP）は、コンピュータ ネットワーク全体でクロックを同期するために使用されるプロトコルです。インターフェイスの作成時に **[PTP の有効化（Enable PTP）]** チェックボックスをオンにすると、PTP はファブリック全体およびすべてのファブリック内インターフェイスで有効になります。IPFM ファブリックでサポートされる PTP プロファイルは、**IEEE-1588v2**、**SMPTE-2059-2**、および **AES67-2015** です。

非ファブリック イーサネット インターフェイスのインターフェイスごとの PTP プロファイルについては、次の点に注意してください。

- 各非ファブリック イーサネット インターフェイスで PTP を有効化し、PTP プロファイルを選択する必要があります。
- PTP プロファイルは、ファブリック レベルのものとは異なる場合があります。
- 非ファブリック イーサネット インターフェイスで PTP を設定するには、ファブリック設定で PTP を有効にする必要があります。

ファブリック設定で PTP が無効になっている場合、PTP 設定はすべてのインターフェイス（ファブリック インターフェイスと非ファブリック インターフェイスの両方）から削除されます。

IPFM ファブリックの PTP モニタリングの詳細については、PTP（モニタリング） を参照してください。

IPFM ファブリック インターフェイスの編集

ここでは、既存の IPFM ファブリック インターフェイスのテンプレートを編集する手順について説明します。**[ポリシーオプション (Policy Options)]** 領域では、テンプレートを変更することや、編集可能なパラメータの値を編集することができます。

手順

ステップ 1 ファブリックの **[ファブリックの概要 (Fabric Overview)]** ウィンドウに移動し、**[インターフェイス (Interfaces)]** タブをクリックします。

ステップ 2 **[インターフェイスの編集 (Edit interface)]** を **[アクション (Actions)]** ドロップダウン リストから選択します。

[インターフェイスの編集 (Edit interface)] ウィンドウが表示されます。

ステップ 3 この手順は任意です。ポリシーを変更するには、ポリシー リンクをクリックし、IPFM に固有のポリシーを選択します。

[アタッチするポリシーの選択 (Select Attached Policy Template)] ダイアログ ボックスで、必要なインターフェイス ポリシー テンプレートを選択し、**[保存 (Save)]** をクリックします。

ステップ 4 **[ポリシーオプション (Policy Options)]** 領域で必要な値を編集します。ポリシーに基づいて、それに応じた [ポリシーオプション (Policy Options)] フィールドが表示されることに注意してください。パラメータの詳細については、IPFM ファブリックのインターフェイスの作成（127 ページ）を参照してください。

次のフィールドは int_ipfm_l3_port ポリシーに固有であることに注意してください。

[IPFM ユニキャスト帯域幅パーセンテージ (IPFM Unicast Bandwidth Percentage)]：ユニキャストトラフィック専用の帯域幅の割合を指定します。残りのパーセンテージは、マルチキャストトラフィック用に自動的に予約されます。このフィールドを空白のままにすると、グローバル ユニキャストの帯域幅予約が適用されます。

[IPFM 外部リンク (IPFM External-Link)]：インターフェイスを外部ルーターに接続することを指定するには、このチェックボックスをオンにします。

[境界ルーター (Border Router)]：このチェックボックスをオンにすると、インターフェイスで境界ルーターの設定が有効になります。インターフェイスは PIM ドメインの境界です。

[インターフェイスの説明 (Interface Description)]：インターフェイスの説明を入力します。説明は最大 254 文字です。

ステップ 5 要件に基づいて、次のいずれかのボタンをクリックします。

- [保存 (Save)]：設定の変更を保存するには、**[保存 (Save)]** をクリックします。
- [プレビュー (Preview)]：**[プレビュー (Preview)]** をクリックすると、**[インターフェイス設定のプレビュー (Preview interfaces configuration)]** ウィンドウが開いて、詳細が表示されます。
- [展開 (Deploy)]：インターフェイスを設定するには、**[展開 (Deploy)]** をクリックします。

次のタスク

IPFM ファブリックを設定するためのポリシーを追加します。詳細については、IPFM ファブリックを構成するポリシーの追加 （132 ページ）を参照してください。

IPFM ファブリックを構成するポリシーの追加

すべてのリーフまたはスパインで均一ではない設定の場合、IPFM ファブリックの設定を完了するのに役立つ追加のテンプレートが提供されます。

たとえば、9300 スイッチで NAT を有効にすると、ipfm_tcam_nat_9300 ポリシーを作成して、スイッチに必要な NAT TCAM を設定できます。

テレメトリには ipfm_telemetry ポリシーを使用し、VRF 設定（routing、pim、asm）には ipfm_vrf ポリシーを使用します。

手順

ステップ 1 使用するファブリックの **[ファブリックの概要（Fabric Overview）]** ウィンドウに移動し、**[ポリシー（Policies）]** タブをクリックします。

ステップ 2 [アクション（Actions）] ドロップダウンリストから [ポリシーの追加（Add Policy）] を選択します。

[ポリシーの作成（Create Policy）] ウィンドウを表示します。

ステップ 3 [スイッチの選択（Select Switches）] フィールドの右矢印をクリックします。

[スイッチの選択（Select Switches）] ダイアログボックスが表示されます。

ステップ 4 1 つ以上のスイッチを選択し、[選択（Select）] をクリックします。

ステップ 5 [ポリシーの作成（Create Policy）] ウィンドウで [テンプレートの選択（Choose Template）] をクリックします。

ステップ 6 [ポリシー テンプレートの選択（Select a Policy Template）] ダイアログ ボックスで、IPFM ファブリックに必要なテンプレート（ipfm_tcam_nat_9300 など）を選択します。[選択（Select）] をクリックします。

ステップ 7 テンプレートの優先順位を入力します。有効な値の範囲は、1 ～ 1000 です。

ステップ 8 TCAM 関連のフィールドに値を入力します。TCAM サイズを 256 単位で入力し、[保存（Save）] をクリックします。

IPFM ファブリックのポリシーの編集

IPFM ファブリック内の任意のスイッチのポリシーを編集できます。

手順

ステップ 1 ファブリックの **[ファブリックの概要（Fabric Overview）]** ウィンドウに移動し、**[ポリシー（Policies）]** タブをクリックします。

ステップ 2 テンプレートを検索します。

ステップ 3 [アクション（Actions）] ドロップダウンリストからポリシーを選択し、[ポリシーの編集（Edit Policy）] を選択します。

[ポリシーの編集（Edit Policy）] ウィンドウが表示されます。

ステップ 4 必要な変更を行って、[保存（Save）] をクリックします。

Netflow サポート

ファブリック レベルで Netflow を構成すると、ネットワーク フローとデータを収集、記録、エクスポート、監視して、どのネットワーク トラフィック フローとボリュームでさらに分析とトラブルシューティングを行ったらよいかを判断できます。Cisco NDFC リリース 12.0.2 から、Easy ファブリック、Easy ファブリックの eBGP、外部ファブリック、および LAN クラシックのテンプレートで Netflow を設定できます。

ファブリックに対して Netflow を有効にした後、ネットワークまたはインターフェイス（VLAN、SVI、物理インターフェイス、サブインターフェイス、またはポートチャネル）で Netflow を

構成できます。インターフェイスまたはネットワークで Netflow を有効にする前に、指定されたモニタ名がファブリック設定で定義されていることを確認してください。

Netflow がファブリック レベルで有効になっている場合、**no_netflow** ポリシーを持つスパイン/スーパー スパインまたはスイッチを除き、ファブリック内の Netflow 対応スイッチ（FX/GX/EX）の構成が生成されます。マルチサイト ドメイン構成では、Netflow は、マルチサイト ドメイン全体ではなく、Easy ファブリックごとに構成されます。

（注） NDFC は **Netflow モニタ**名を検証しません。

以下は、他のネットワーク要素での Netflow 設定のガイドラインです。

- VRF Lite IFC の場合、オーバーレイ モードに関係なく、構成プロファイル内に Netflow 構成はありません。
- ネットワークの場合、オーバーレイ モードに関係なく、構成プロファイル内に Netflow 構成はありません。
- トランク ポート、アクセス ポート、dot1q トンネル、レイヤ 2 ポート チャネル、および VPC ポートでは、レイヤ 2 インターフェイスの Netflow を構成できます。
- SVI、ルーテッド ホスト、L3 ポート チャネル、およびサブインターフェイスでは、レイヤ 3 インターフェイスの Netflow を構成できます。
- VLAN の Netflow 構成では、**vlan_netflow** レコード テンプレートを使用します。ブラウンフィールド展開では、VLAN の Netflow 構成はスイッチの自由形式です。
- SVI（ルーテッド トラフィックの場合）または VLAN 構成（スイッチド トラフィックの場合）の下では、Netflow を有効にできます。
- IPv6 フロー モニタリングを構成するには、**switch_freeform** または**インターフェイスの自由形式**を使用します。
- トランクまたはルーテッド ポートの下の Netflow 設定は、**インターフェイスの自由形式**です。
- ホスト ポートの再同期の場合、Netflow 構成はインターフェイスの自由形式でキャプチャされます。
- ファブリック内リンクまたはマルチサイト アンダーレイ IFC では Netflow の明示的なサポートはありません。自由形式構成を使用できることに注意してください。

ブラウンフィールド展開の Netflow サポート

ブラウンフィールド展開の場合、エクスポート、記録、および監視のグローバル Netflow 構成は、テレメトリのユース ケースが原因でキャプチャされません。ブラウンフィールドインポートの後、グローバル レベルの Netflow コマンドが削除されないようにするために、次のアクションを実行できます。

- 厳密な CC をオンにしないでください。
- **スイッチの自由形式**に Netflow グローバル構成を含めます。
- スイッチ構成に合わせたファブリック設定で Netflow を有効にします。

  スイッチのインターフェイスおよび VLAN レベルの Netflow 構成は、**自由形式**でキャプチャされます。
- SVI の Netflow 構成は、ネットワークに関連付けられた **switch_freeform** でキャプチャされます。
- トランク ポートまたはルーテッド ポートの Netflow 構成は、**インターフェイスの自由形式**に置かれます。
- VLAN の Netflow 構成は、**switch_freeform** に置かれます。
- VRF-Lite 拡張のサブインターフェイス構成は、 **int_freeform** に置かれます。

外部ファブリックおよびLANクラシックファブリック向け高精度時間プロトコル（PTP）

[External_Fabric] または **[LAN_Classic]** テンプレートのファブリック設定で、**[高精度時間プロトコル（PTP）を有効化（Enable Precision Time Protocol（PTP）]** チェックボックスをオンにして、ファブリック全体で PTP を有効にします。このチェックボックスを選択すると、PTP はグローバルで、およびコア向きのインターフェイスで有効化されます。また、**[PTP ループバック ID（PTP Loopback Id）]** および **[PTP ドメイン ID（PTP Domain Id）]** フィールドは編集可能です。

PTP 機能は、NX-OS バージョン 7.0(3)I7(1) 以降の Cisco Nexus 9000 シリーズ クラウド スケール スイッチでサポートされます。ファブリック内にクラウドスケール以外のデバイスがあり、PTP が有効になっていない場合は、警告が表示されます。クラウドスケールデバイスの例としては、Cisco Nexus 93180YC-EX、Cisco Nexus 93180YC-FX、Cisco Nexus 93240YC-FX2、および Cisco Nexus 93360YC-FX2 スイッチがあります。詳細については、https://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.htmlを参照してください。

Note PTP グローバル設定は、Cisco Nexus 3000 シリーズ スイッチでサポートされます。ただし、PTP および ttag の設定はサポートされていません。

詳細については、『*Cisco Nexus 9000* シリーズ *NX-OS* システム管理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 Nexus Dashboard Insights*（*Cisco Nexus*ダッシュボード ファブリック コントローラ 用）ユーザー ガイド』を参照してください。

外部および LAN クラシック ファブリック展開の場合、PTP をグローバルに有効にし、コア側のインターフェイスで PTP を有効にする必要があります。インターフェイスは、VM や Linux ベースのマシンのような外部 PTP サーバに対して構成できます。したがって、インターフェイスを編集して、グランドマスター クロックと接続する必要があります。PTP および TTAG 設

定を外部およびLANクラシック ファブリックで動作させるには、**host_port_resync**ポリシーを使用してNexusダッシュボード ファブリック コントローラ にスイッチ設定を同期する必要があります。詳細については、アウトオブバンド スイッチ インターフェイスの構成の同期, on page 52を参照してください。

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

[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、トラフィックがこのファブリックを出るときにttagを削除する必要があります。

次に、PTPの設定例を示します。`featureptp`

```
feature ptp

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

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

interface Ethernet1/59 -> Core facing interface
  ptp

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

次のガイドラインはPTP で適用可能です。

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

  ```
  PTP feature can be enabled in the fabric, when all the switches have
  NX-OS Release 7.0(3)I7(1) or higher version. Please upgrade switches to
  NX-OS Release 7.0(3)I7(1) or higher version to enable PTP in this fabric.
  ```

- NIR のハードウェア テレメトリ サポートでは、PTP 構成が前提条件です。
- PTP 構成を含む既存のファブリックに非クラウド スケール デバイスを追加すると、次の警告が表示されます。

  ```
  TTAG is enabled fabric wide, when all devices are cloud-scale switches
  so it cannot be enabled for newly added non cloud-scale device(s).
  ```

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

  ```
  TTAG is enabled fabric wide when all devices are cloud-scale switches
  and is not enabled due to non cloud-scale device(s).
  ```

- ホスト構成の同期がすべてのデバイスで実行されると、すべてのデバイスに対して TTAG 構成が生成されます。新しく追加されたすべてのデバイスでホスト構成の同期が実行されない場合、新しく追加されたデバイスの Ttag 構成は生成されません。

  構成が同期されていない場合は、次の警告が表示されます。

  ```
  TTAG on interfaces with PTP feature can only be configured for cloud-scale devices.
  It will not be enabled on any newly added switches due to the presence of non
  cloud-scale devices.
  ```

- PTP および TTAG 構成は、ホスト インターフェイスに展開されます。
- PTP および TTAG 構成は、同じファブリック内のスイッチ間でサポートされます（ファブリック内リンク）。PTP はファブリック間リンク用に作成され、ttagは他のファブリック（スイッチ）が Nexusダッシュボード ファブリック コントローラ によって管理されていない場合に作成されます。ファブリック間リンクは、両方のファブリックが Nexusダッシュボード ファブリック コントローラ によって管理されている場合、PTP または ttag 設定をサポートしません。
- TTAG 設定は、ブレークアウト後にデフォルトで設定されます。リンクが検出され、ブレークアウト後に接続されたら、**[構成の展開（Deploy Config）]** を実行して、ポートのタイプ（ホスト、ファブリック内リンク、またはファブリック間リンク）に基づいて正しい設定を生成します。

ブラウンフィールド展開：VXLANファブリック管理からNexusダッシュボード ファブリック コントローラ への移行

Nexusダッシュボード ファブリック コントローラ では、VXLAN BGP EVPN ファブリック管理を Nexusダッシュボード ファブリック コントローラ に移行するブラウンフィールド展開をサポートしています。移行には、既存のネットワーク設定のNexusダッシュボード ファブリック コントローラ への移行が含まれます。詳細については、「ブラウンフィールド *VXLAN BGP EVPN* ファブリックの管理」を参照してください。

外部ファブリックおよびLANクラシック ファブリックでのインバンド管理

ブラウンフィールド展開でのみ、外部および LAN クラシック ファブリックのインバンド接続のスイッチをインポートまたは検出できます。ファブリック設定を構成または編集しながら、ファブリックごとにインバンド管理を有効にします。POAP を使用してインバンド接続のスイッチをインポートまたは検出することはできません。

設定後、ファブリックはインバンド管理の VRF に基づいてスイッチの検出を試みます。ファブリック テンプレートは、シード IP を使用してインバンド スイッチのVRFを決定します。同じシード IP に複数の VRF がある場合、シードインターフェイスのインテントは学習されません。インテント/設定を手動で作成する必要があります。

ファブリック設定を構成/編集した後、**構成を展開する**必要があります。インバンド管理対象スイッチをファブリックにインポートした後は、インバンド管理設定を変更できません。このチェックボックスをオフにすると、次のエラー メッセージが生成されます。

```
Inband IP <<IP Address>> cannot be used to import the switch,
please enable Inband Mgmt in fabric settings and retry.
```

スイッチをファブリックにインポートしたら、インターフェイスを管理してインテントを作成する必要があります。スイッチをインポートするインターフェイスのインテントを作成します。インターフェイス コンフィギュレーションを編集/更新します。このインバンド管理スイッチのインターフェイス IP を変更しようとすると、エラー メッセージが生成されます。

```
Interface <<interface_name>> is used as seed or next-hop egress interface
for switch import in inband mode.
IP/Netmask Length/VRF changes are not allowed for this interface.
```

インターフェイスの管理中に、インバンド管理を使用してインポートされたスイッチでは、スイッチのシード IP を変更できません。次のエラーが生成されます。

```
<<switch-name>>: Mgmt0 IP Address (<ip-address>) cannot be changed,
when is it used as seed IP to discover the switch.
```

ネクストホップ インターフェイスのポリシーを作成します。サードパーティ製デバイスからNexusダッシュボード ファブリック コントローラ へのルートには、ECMP ルートと呼ばれる複数のインターフェイスが含まれる場合があります。ネクストホップインターフェイスを検索し、スイッチのインテントを作成します。インターフェイス IP および VRF の変更は許可されません。

インバンド管理が有効になっている場合、イメージ管理中に、ISSU、EPLD、RPM、および SMU インストール フローで、スイッチ上のイメージをコピーするために eth2 IP アドレスが使用されます。

ファブリック内のインバンド接続を使用してスイッチをインポートし、後でファブリック設定でインバンド管理を無効にすると、次のエラー メッセージが生成されます。

```
The fabric <<fabric name>> was updated with below message:
Fabric Settings cannot be changed for Inband Mgmt, when switches are already imported
using inband Ip. Please remove the existing switches imported using Inband Ip from the
fabric,
then change the Fabric Settings.
```

ただし、同じファブリックに、インバンド接続とアウトオブバンド接続の両方を使用してインポートされたスイッチを含めることができます。

外部ファブリックおよびLANクラシック ファブリックでのインバンドPOAP管理

Power On Auto Provisioning（POAP）は、ネットワークに初めて導入された Cisco Nexus スイッチにおいて、ソフトウェアイメージのアップグレードと構成ファイルのインストールのプロセスを自動化します。POAP を使用すると、手動構成を実行せずにデバイスを起動できます。

POAP 機能が有効なデバイスが起動し、スタートアップ構成が見つからない場合、デバイスは POAP モードに入り、DHCP サーバーを検索し、インターフェイス IP アドレス、ゲートウェイ、および DNS サーバーの IP アドレスを使用して自身のブートストラップを実行します。デ

バイスはTFTPサーバーのIPアドレスを取得し、構成スクリプトをダウンロードします。このスクリプトは、スイッチが適切なソフトウェアイメージと構成ファイルをダウンロードしてインストールできるようにします。

NexusスイッチのPOAP（Power On Auto Provisioning）機能を使用することにより、NDFC（Nexus Dashboard Fabric Controller）は新しいデータセンターの展開を自動化し、全体の時間と労力を削減します。

NDFC 12.1.1e から、外部ファブリックと LAN クラシック ファブリックは、インバンド インターフェイスから POAP を介して行われるスイッチの追加をサポートしています。

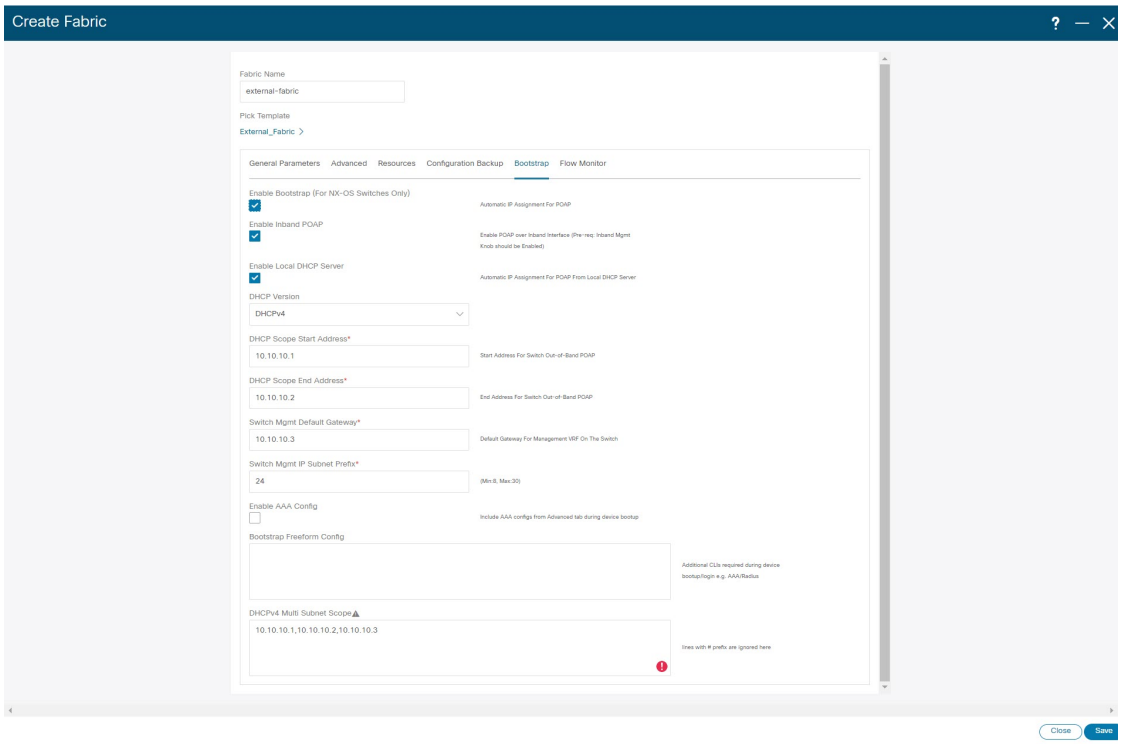
インバンド POAP は、**外部**および **LAN クラシック** テンプレートを使用したファブリックのすべてのロールでサポートされています。

以下は、インバンド POAP 管理を使用するための前提条件です。

- 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、**[サーバー設定（サーバー設定）] > [管理（Admin）]** に移動し、**[データ（Data）]** を **[LAN デバイス管理接続（LAN Device Management Connectivity）]** ドロップダウンから選択します。そうしないと、エラー メッセージが表示されます。**[データ（Data）]** を選択した場合は、必要な「データ サービス IP」が Nexus ダッシュボードの **[外部サービス プール（External Service Pools）]** タブで使用できることを確認してください。
- Cisco Nexus ダッシュボードのスイッチ インバンド インターフェイスに到達できるように、適切なデータ ネットワーク ルートを設定します。Nexus Dashboard で、**[管理コンソール（Admin Console）]** > **[インフラストラクチャ（Infrastructure）]** > **[クラスタ構成（Cluster Configuration）]** を選択します。**[全般（General）]** タブで、ルートの IP アドレスを入力します。
- ファブリック設定に記載されている定義済み DHCP サブネット スコープの各サブネットには、リバース トラフィックの有効なルートが必要です。
- DHCP リレー機能が中間ルータに設定されていることを確認します。次に、インバンド POAP 管理の注意事項および制限事項を示します。
  - インバンド POAP は、NX-OS スイッチでのみサポートされています。
  - **[ブートストラップ（Bootstrap）]** タブのインバンド POAP は、**[インバンド管理（Inband Management）]** が **[詳細（Advanced）]** タブで有効になっている場合にのみサポートされます。
  - ローカルDHCPサーバーとして、または外部DHCPサーバー上で、NDFCを使用してインバンド POAP を有効にすることができます。
  - インバンド POAP は、マルチ サブネット スコープをサポートします。

インバンド POAP によるスイッチの追加

インバンドPOAPを介してスイッチを追加する前に、前提条件とガイドラインに従っていることを確認してください。



手順

ステップ 1 外部または LAN クラシック ファブリックを作成します。外部ファブリックの作成 （87 ページ）を参照してください。

ステップ 2 **[詳細設定（Advanced）]** タブで、**[インバンド管理（Inband Mgmt）]** チェック ボックスをオンにします。

ステップ 3 [ブートストラップ（Bootstrap）] タブで、次の操作を行います。

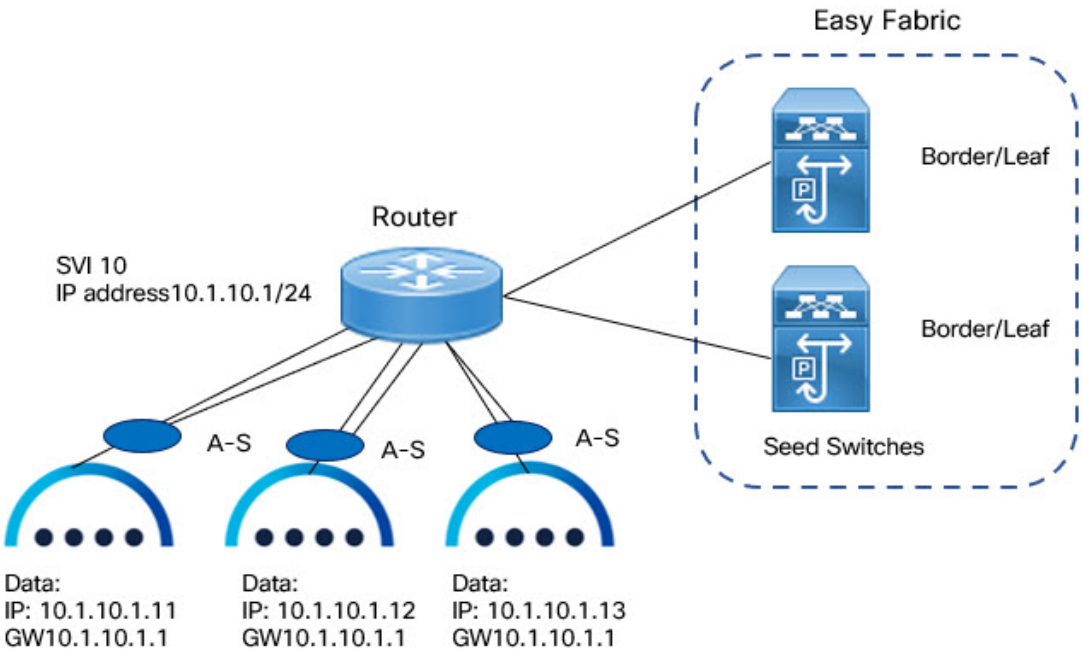
1. NX-OS スイッチの場合のみ、**[ブートストラップの有効化（Enable Bootstrap）]** チェック ボックス（**[ブートストラップ（Boostrap）]** タブ）をオンにします。
2. [インバンド POAP の有効化（Enable Inband POAP）] チェック ボックスをオンにします。
3. ローカル DHCP サーバーが必要な場合は、**[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）]** チェック ボックスをオンにします。必要な DHCP スコープを入力します。無効にする場合、外部 DHCP サーバーがスイッチのブートストラップで使用できる必要があります。

ステップ 4 ファブリックにスイッチを追加するには、デバイスの事前プロビジョニングを参照してください。

（注） インバンド インターフェイス、ルーティング IP、ホスト名など、すべてのスイッチに必要な詳細が追加されていることを確認します。

Easy ファブリックでのインバンド管理とインバンド POAP

Cisco NDFC リリース 12.1.1e 以降、Easy ファブリックのインバンド接続とインバンド POAP を使用してスイッチを管理できます。インバンド管理では、デバイスの Loopaback0 インターフェイスがファブリック設定で使用されます。



インバンド POAP または事前プロビジョニングとインバンド POAP を使用したグリーンフィールドまたはブラウンフィールド展開のいずれかで、Easy ファブリックに対応していてインバンド管理が有効になっているスイッチを追加できます。

- ブラウンフィールド展開の場合は、**[構成の保持（Preserve Config）]** チェック ボックスをオンにします。
- グリーンフィールド展開の場合は、**[構成の保持（Preserve Config）]** チェック ボックスをオフにします。

シードスイッチは外部ルータに接続し、ファブリック内の他のスイッチへの管理接続を提供します。ファブリックへの接続を提供するために外部ルータに接続されたスイッチは、シードスイッチと呼ばれます。外部ルータに接続するシードスイッチのインターフェイスは、ブートストラップ インターフェイスと呼ばれます。

インバンド管理の前提条件

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、**[サーバー設定（Server settings）] > [管理（Admin）]** に移動し、**[データ（Data）]** を **[LAN デバイス管理（LAN Device Management）] [接続（Connectivity）]** から選択します。**[データ（Data）]** を選択する際には、必要な **[データ サービス IP（Data Service IPs）]** がNexus Dashboardの **[外部サービス プール（External Service Pools）]** タブで使用できることを確認してください。このサーバー設定は、インバンド接続とアウトオブバンド接続の両方に必要です。Cisco Nexus Dashboardのデータ インターフェイス経由で以下の静的ルートを設定します。

Cisco Nexus Nexus Dashboardで、外部ルートおよびデータ インターフェイス経由のルートに必要な静的ルートIPアドレスを入力します。

インバンドPOAPでは、シード スイッチに接続されている外部ルータのIPアドレスに次の機能が必要です。

- 外部ルータのルート
- Easyファブリックのルーティング ループバック サブネット範囲のルート
- Easyファブリックのアンダーレイ ルーティング サブネット範囲のルート

インバンドPOAPでは、外部ルータに接続されたシード スイッチに次の機能が必要です。

- DHCPリレー機能
- eBGPピアリング

インバンド管理およびインバンドPOAP用のスイッチを追加するには、新しいスイッチの検出を参照してください。

注意事項と制約事項

インバンド管理に関する注意事項および制約事項は次のとおりです。

- インバンドインターフェイスで**インバンド管理**が有効になっていることを確認します。同じファブリックでインバンド スイッチとアウトオブバンド スイッチを同時にサポートすることはできません。
- これは、IPv4アンダーレイおよびOSPFルーティング プロトコルでのみサポートされます。
- ファブリックの作成後に、スイッチ管理をインバンドからアウトオブバンドに、またはその逆に変更できます。
- インバンド マネージド スイッチでは、次のロールがサポートされています。
  - スパイン
  - リーフ
  - 境界
  - ボーダースパイン

- ボーダーゲートウェイ
- ボーダー ゲートウェイ スパイン

- インバンド管理は、番号付きおよび番号なしの両方のファブリック インターフェイスの番号付けでサポートされています。
- 同じロール スイッチがシード スイッチとして割り当てられていることを確認します。スパインのロール スイッチがシード スイッチとして割り当てられている場合、そのファブリック内のすべてのスパインのロールスイッチをシードスイッチとして割り当てる必要があります。スイッチは、シード スイッチとして割り当てることをお勧めします。
- スイッチをファブリックに追加するときは、スイッチがメンテナンス モードになっていないことを確認してください。
- ファブリックが作成された場合にのみ、ブラウンフィールド展開にスイッチを追加できます（**[構成の保持（Preserve Config）]** チェックボックスをオンにします）。さらにスイッチを追加するには、インポート スイッチ オプションでインバンド POAP を使用します。
- vPC スイッチ mgmt0 インターフェイスが設定されていない場合は、**[vPC ピア キープ アライブ（vPC Peer Keep Alive）]** オプションをループバックに設定します。

インバンド POAP に関する注意事項および制約事項は次のとおりです。

- ファブリックのインバンドPOAPは、インバンド管理が有効になっている場合にのみ有効にできます。
- インバンド POAP では、ファブリックまたはコアに面したインターフェイスが、シード スイッチとスパイン スイッチに対して一貫してケーブル接続されている必要があります。
- ファブリック内のすべてのスパイン スイッチは、同じファブリック インターフェイス番号のセットを使用する必要があります。
- ファブリックにシード スイッチである一連のリーフ スイッチがある場合、スイッチは同じファブリック インターフェイス番号を使用する必要があります。
- シード スイッチには、外部ルータとの eBGP ピアリングが必要です。したがって、外部ルータは必要な eBGP ルート ピアリング機能を備えている必要があり、Easy ファブリックで使用されるサブネット用に構成されたDHCP リレーと静的ルート用の外部ルータの構成を表示します。
- DHCP リレーは、インバンド インターフェイスでシード スイッチを接続する外部ルータ インターフェイスで構成する必要があります。構成されている DHCP リレーの宛先が、Cisco Nexus ダッシュボードのすべてのクラスタ ノード データ インターフェイスで同じであることを確認します。
- DHCP サーバーは、内部 NDFC または外部サーバーにすることができます。

Easy ファブリックでのインバンド POAP の有効化

Easy ファブリックでインバンド POAP を有効にするには、次の手順を実行します。

手順

ステップ 1 **[管理性（Manageability）]** タブで、**[インバンド管理（Inband Management）]** チェックボックスをオンにします。

ステップ 2 **[ブートストラップ（Bootstrap）]** タブで、次の操作を行います。

a) **[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。

b) **[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て、NDFC を DHCP サーバーとして割り当て、すべてのファブリック シードスイッチのブートストラップ インターフェイスの DHCP スコープを入力します。

[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）] を選択し、[一般パラメータ（General Parameters）] 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）] ドロップダウン リストで [番号なし（unnumbered）] を選択した場合は、次の詳細を追加します。

- [ブートストラップ シードスイッチ ループバック インターフェイス ID（Bootstrap Seed Switch Loopback Interface ID）]
- [スイッチ ループバック DHCP スコープ開始アドレス（Switch Loopback DHCP Scope Start Address）]
- [スイッチ ループバック DHCP スコープ終了アドレス（Switch Loopback DHCP Scope End Address）]

c) 外部ルータから NDFC への接続を提供するには、[外部 DHCP サーバー IP アドレス（External DHCP Server IP Addresses）] チェックボックスをオンにします。

[外部 DHCP サーバーの IP アドレス（External DHCP Server IP Addresses）] を選択した場合は、コンマ区切りのリストで最大 3 つの IPv4 アドレスを追加できます。

（注） シードと外部ルータの間に eBGP ピアリングを設定するには、ブートストラップ シード スイッチのループバック インターフェイス IP アドレスを追加します。この IP は、ループバック ID 範囲のサブセット内にある必要があります。

d) **[シード スイッチ ファブリック インターフェイス（Seed Switch Fabric Interfaces）]** テキスト フィールドにシード スイッチ インターフェイスを入力します。

e) **[スパイン スイッチ ファブリック インターフェイス（Spine Switch Fabric Interfaces）]** テキスト フィールドにスパイン スイッチ インターフェイスを入力します。

（注） スパイン スイッチがシード スイッチである場合、リストは**[シード スイッチ ファブリック インターフェイス（Seed Switch Fabric Interfaces）]** テキスト フィールドと一貫している必要があります。

ステップ 3 番号なしのインターフェイスを持つファブリックの場合は、次の手順を実行します。

a) **[一般パラメータ（General Parameters）]** で、**[番号なし（unnumbered）]** を **[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 リストから選択します。

b) **[ブートストラップ（Bootstrap）]** タブでは：

[ブートストラップ シード スイッチ ループバック インターフェイス ID（Bootstrap Seed Switch Loopback Interface ID）]：ループバック ID は、ファブリックのデフォルト ルータ IP です。このループバック ID は、既存のファブリック ループバック ID と重複してはなりません。

[スイッチ ループバック DHCP スコープ開始アドレス（Switch Loopback DHCP Scope Start Address）]：この IP アドレスは、ブートストラップ スイッチに割り当てるルーティング ループバック アドレス範囲の DHCP プールの開始アドレスです。この IP アドレスは、**[アンダーレイ ルーティング ループバック IP 範囲（Underlay Routing Loopback IP Range）]**. の既存の IP アドレスと重複していてはなりません。

[スイッチ ループバック DHCP スコープ終了アドレス（Switch Loopback DHCP Scope End Address）]：DHCP プールの終了アドレスです。

ブラウンフィールド展開用のスイッチのインポート

始める前に

スイッチを追加する前に、前提条件の手順に従っていることを確認してください。

手順

ステップ 1 テンプレート **Easy_Fabric** を使用してファブリックを作成します。この説明については、ファブリックの作成 （6 ページ） を参照してください。

シード スイッチ、スパイン スイッチ、その他のスイッチの順序でスイッチを追加します。スパイン スイッチはシード スイッチとして追加できます。

ステップ 2 各ファブリックのブラウンフィールド展開の **[インバンド管理（Inband Management）]**（**[管理性（Manageability）]** タブ）でインバンド管理を有効にして、ファブリックをインポートします。

ステップ 3 **[構成の保存（Preserve Config）]** チェック ボックスを使用して、スイッチをファブリックに追加します。

ステップ 4 **[ホスト名（hostname）]**、**[ロール（Role）]** を入力し、**[シード スイッチ（Seed Switch）]** を有効にして、適切な IP アドレスを入力します。

ステップ 5 すべてのシード スイッチの IP アドレスを入力し、**[選択したスイッチのインポート（Import Selected Switches）]** をクリックして、それらをファブリックに追加します。

ステップ 6 **[ポリシー（Policy）]** タブに移動し、**[アクション（Actions）]>[ポリシーの追加（Add Policy）]** をクリックします。**ext_bgp_neighbor** ポリシーを選択して、シード スイッチが eBGP ピアリングを確立するようにします。必要な詳細を入力し、**[保存（Save）]** をクリックします。

ステップ 7 適切なスイッチのロールを割り当てます。

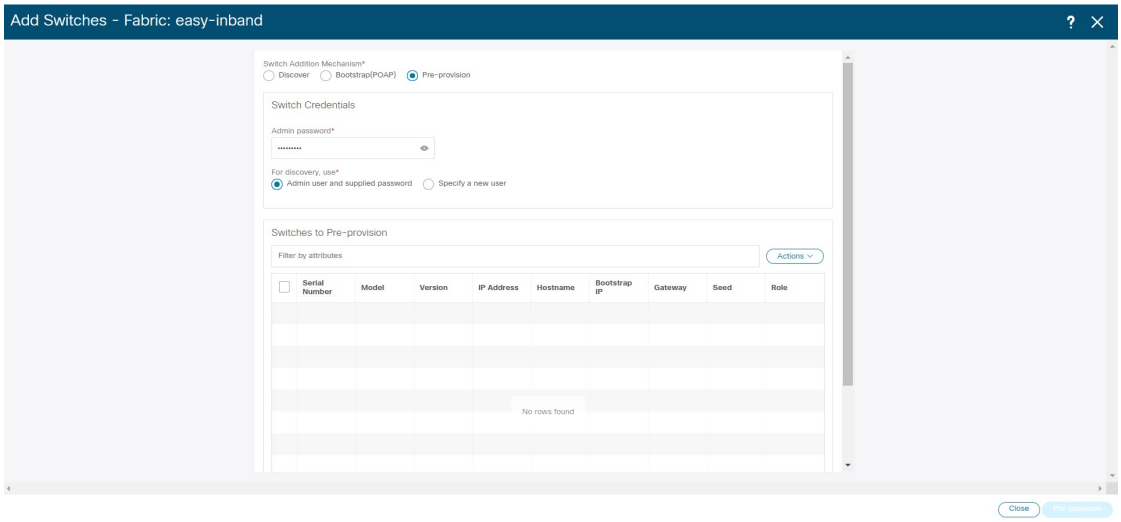
手順については、ブート ストラップ メカニズムを使用したスイッチの追加を参照してください。

インバンド POAP によるスイッチの事前プロビジョニング

手順

ステップ 1 **[スイッチ（Switches）]** タブで、**[アクション（Actions）] > [スイッチの追加（Add Switches）]** を選択します。

[スイッチの追加（Add Switches）] ウィンドウが表示されます。



ステップ 2 **[事前プロビジョニング（Pre-provision）]** オプション ボタンを選択します。

ステップ 3 **[事前プロビジョニングを行うスイッチ（Switches to Pre-provision）]** テーブルで、**[アクション（Actions）] > [追加（Add）]** をクリックします。

[スイッチの事前プロビジョニング（Pre-provision a switch）] ウィンドウが表示されます。

ステップ 4 シリアル番号、モデル、IP アドレスなどの適切な詳細を入力し、**[追加（Add）]** をクリックします。

ステップ 5 一度に 1 台のスイッチのみ入力して、必要な情報を入力します。複数のスイッチがある場合。

ステップ 6 **[スイッチをファブリックにインポートする（Import Switches to Fabric）]** をクリックしてスイッチを追加します。

Easy ファブリックのポリシーの追加

手順

ステップ 1 **[LAN] > [ファブリック（Fabrics）]** ウィンドウに移動し、適切な Easy Fabric をダブルクリックしてポリシーを追加します。

[ファブリックの概要（Fabric Overview）] ウィンドウが表示されます。

ステップ 2 **[ファブリックの概要（Fabric Overview）]** タブで、**[ポリシー（Policy）]** タブをクリックします。

ステップ 3 **[スイッチ（Switch）]** ウィンドウから適切なスイッチを選択し、**[テンプレートの選択（Choose Template）]** をクリックします。

ステップ 4 **ext_bgp_neighbor policy** を選択し、**[選択（Select）]** をクリックします。

[ポリシーの作成（Create Policy）] ウィンドウを表示します。

ステップ 5 **[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）] ウィンドウを表示します。

ステップ 6 ウィンドウに適切な詳細を入力し、**[保存（Save）]** をクリックします。

ステップ 7 **[ファブリックの概要（Fabric Overview）]** ウィンドウで、**[アクション（Actions）] > [再計算と展開（Recalculate and Deploy）]** をクリックします。

ファブリック管理モードの変更

ファブリックはアウトオブバンドからインバンド管理に、またはその逆に変更できます。

手順

ステップ 1 ファブリック管理をアウトオブバンドからインバンド管理に変更するには、次の手順を実行します。

a) インバンド管理の前提条件の手順に従っていることを確認します。

b) **[ファブリックの編集（Edit Fabric）]** ウィンドウで、**[インバンド管理（Inband Mgmt）]**（**[詳細（Advanced）]** タブ）を有効にして、**[保存（Save）]** をクリックします。

c) **[ファブリックの概要（Fabric Overview）] > [スイッチ（Switches）]** タブで、スイッチを選択し、**[アクション（Actions）] >[モードの変更（Change Mode）]** を選択します。モード列に **[移行（Migration）]** と表示されます。

d) スイッチを選択します。**[アクション（Actions）] >[再計算と展開（Recalculate and Deploy）]** をクリックします。

スイッチの検出 IP アドレスは、BGP ルーティング ループバック IP に変更されます。

検出 VRF はデフォルトを表示し、検出インターフェイスは BGP ルーティング ループバック インターフェイスに更新されます。

e) **[検出ステータス（Discovery Status）]** 列にステータスが **[OK]** と表示されていることを確認し、**[アクション（Actions）] > [再計算して展開（Recalculate and Deploy）]** をクリックします。

ステップ 2 ファブリック管理をインバンド管理からアウトオブバンドに変更するには、次の手順を実行します。

a) アウトオブバンドの前提条件手順に従っていることを確認します。
b) スイッチにアウトオブバンド IP アドレスを設定します。この IP は、NDFC データまたは管理インターフェイスから到達可能である必要があります。
c) ファブリックを選択し、**[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。
d) **[詳細設定（Advanced）]** タブで、**[インバンド管理（Inband Management）]** チェック ボックスをオフにして、**[保存（Save）]** をクリックします。
e) **[ファブリックの概要（Fabric Overview）] > [スイッチ（Switches）]** タブで、スイッチを選択し、**[アクション（Actions ）] > [モードの変更（Change Mode）]** を選択すると、モード列に **[移行（Migration）]** が表示されます。
f) スイッチを選択します。**[アクション（Actions）] > [再計算と展開（Recalculate and Deploy）]** をクリックします。

スイッチの検出 IP アドレスが mgmt0 IP に変更されます。

検出 VRF には管理が表示され、検出インターフェイスは mgmt0 に更新されます。

g) **[検出ステータス（Discovery Status）]** 列にステータスが **[OK]** と表示されていることを確認し、**[アクション（Actions）] > [再計算して展開（Recalculate and Deploy）]>** をクリックします。

拡張されたロールベースのアクセス制御

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

Nexus ダッシュボードの管理者ロールは、NDFC のネットワーク管理者ロールと見なされます。

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

Cisco NDFC リリース 12.0.1(a) には同じ 5 つのロールがありますが、Nexus ダッシュボードの統合により詳細な RBAC を実行できます。ユーザーがネットワークステージロールとしてファブリックにアクセスする場合、同じユーザーは、管理者またはオペレーターロールなどの他の

ユーザーロールを使用して別のファブリックにアクセスできます。したがって、ユーザーはNDFC のさまざまなファブリックでさまざまなアクセス権を持つことができます。

NDFC RBAC は、次のロールをサポートします。

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

次の表では、NDFC でのユーザーロールとその権限について説明します。

ロール	権限
NDFC アクセス管理者	読み取り/書き込み 参照先
NDFC デバイス アップグレード管理者	読み取り/書き込み
NDFC ネットワーク管理者	読み取り/書き込み
NDFC ネットワーク オペレータ	読み取り
NDFC ネットワーク ステージャ	読み取り/書き込み

DCNM では、下位互換性のために次のロールがサポートされています。

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

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

NDFC ネットワーク管理者

NDFC ネットワーク管理者ロールを持つユーザは、Cisco Nexus Dashboard ファブリック コントローラですべての操作を実行できます。

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

NDFC ネットワーク管理者ロールを持つユーザーは、Cisco Nexus ダッシュボード ファブリック コントローラ の特定のファブリックまたはすべてのファブリックをフリーズできます。

（注） スイッチの検出または追加のスイッチを行うスイッチ ユーザーのロール、または NDFC の LAN クレデンシャルには、network-admin ロールが必要であることを確認してください。

NDFC デバイス アップグレード管理者

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

詳細については、「イメージ管理」の項を参照してください。

NDFC アクセス管理者

NDFC アクセス管理者ロールを持つユーザは、すべてのファブリックの**[インターフェイス マネージャ（Interface Manager）]** ウィンドウでのみ操作を実行できます。

NDFC アクセス管理者は、次のアクションを実行できます。

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

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

ただし、Cisco Nexus Dashboard ファブリック コントローラ アクセス ロールを持つユーザは、次のアクションを実行できません。

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

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

NDFC ネットワーク ステージャ

NDFC ネットワーク ステージャ ロールを持つユーザは、Cisco Nexus ダッシュボード ファブリック コントローラで設定を変更できます。**NDFC ネットワーク管理者**ロールを持つユーザは、これらの変更を後で展開できます。ネットワーク ステージャは、次のアクションを実行できます。

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

ただし、ネットワーク ステージャは次のアクションを実行できません。

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

NDFC ネットワーク オペレータ

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

- ファブリック内のスイッチの予期される構成を変更できません。
- スイッチに構成を展開できません。

- ライセンス、追加ユーザの作成などの管理オプションにアクセスできません。

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

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

デフォルトの認証ドメインの選択

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

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

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

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

次の表では、DCNM 11.5(x) AV ペアの形式について説明します。

Cisco DCNM Role	RADIUS Cisco-AV-Pair の値	TACACS+ シェル Cisco-AV-Pair ペアの値
network-operator	shell:roles = "network-operator" dcnm-access="group1 group2 group5"	cisco-av-pair=shell:roles="network-operator" dcnm-access="group1 group2 group5"
Network-Admin	shell:roles = "network-admin" dcnm-access="group1group2 group5"	cisco-av-pair=shell:roles="network-admin" dcnm-access="group1 group2 group5"

次の表では、NDFC 12.x AV ペアの形式について説明します。

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

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

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

強化された RBAC のユースケース

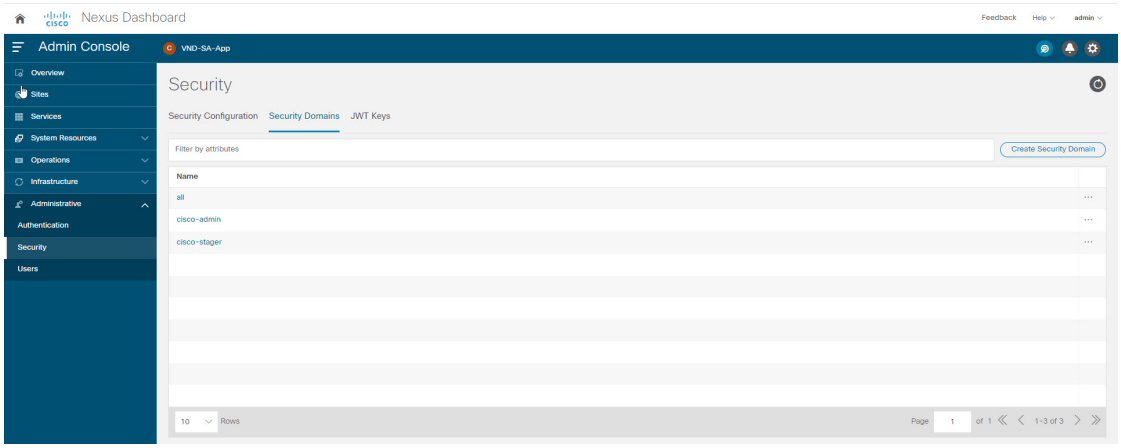
NDFCにはさまざまなファブリックがあります。デフォルトでは、ユーザーはすべてのファブリックの管理者です。たとえば、ユーザー名 **Cisco** は、Fabric-A への 管理者ロール アクセスと、別の Fabric-B へのステージャ ロール アクセスを持つことができます。

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

ユーザーを作成し、特定のロールを定義するには、次の手順を実行します。

手順

ステップ 1 セキュリティ ドメインにユーザーを作成するには：



a) 管理者ロールで Nexus Dashboard にログインし、**[管理（Administrative）]** タブに移動します。

b) **[セキュリティ ドメイン（Security Domain）]** タブで、**[セキュリティ ドメインの作成（Create Security Domain）]** をクリックし、次のセキュリティ ドメインを作成します：

- **all**：network-admin ロールに類似しています。このドメインには、Nexus Dashboard および NDFC サービス アプリケーションへの管理アクセス権があります。
- **cisco-admin**：Fabric-A への完全なネットワーク管理者アクセス
- **cisco-stager**：Fabric-B へのネットワーク ステージャのみのアクセス

ステップ 2 ローカル ユーザー **Cisco** を作成するには。

a) **[ユーザー（Users）]** > **[ローカル（Local）]**に移動します

b) **[ローカル（Local）]** タブで、**[ローカル ユーザーの作成（Create Local User）]** をクリックします。

[ローカル ユーザーの作成（Create Local User）] ウィンドウが表示されます。

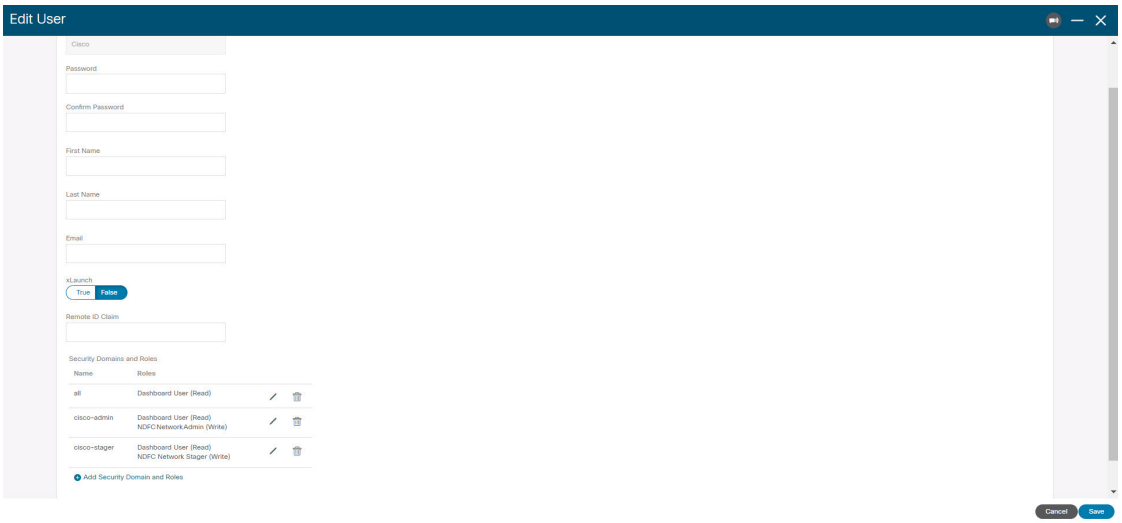
c) [ユーザー ID（User ID）] テキスト フィールドに **Cisco** と入力し、それぞれのフィールドに適切なパスワードを設定します。

d) Cisco ユーザーを作成したら、**[ローカル（Local）]** ウィンドウに移動し、**省略記号**アイコン（**Cisco** ユーザー名の行）をクリックしてから、**[ユーザーの編集（Edit User）]** をクリックします。

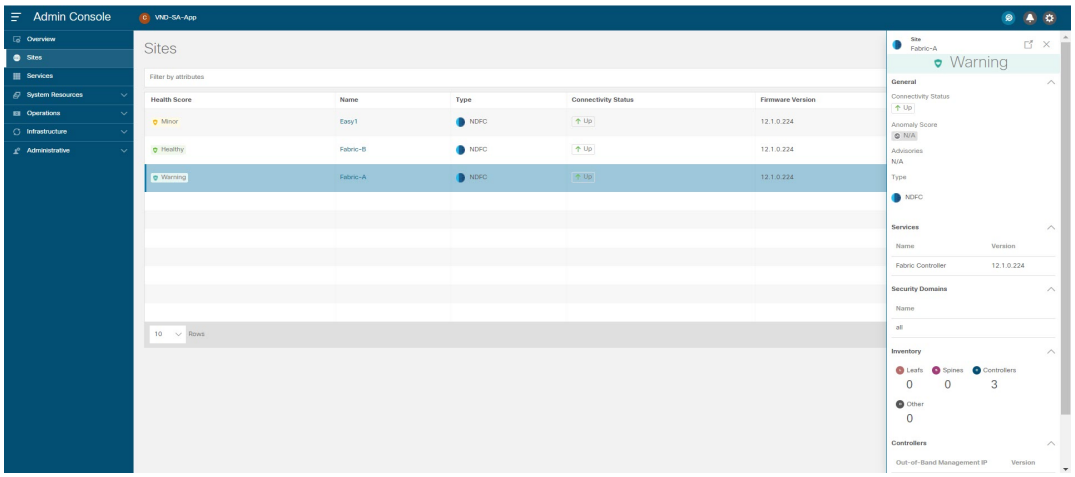
[ユーザーの編集（Edit User）] ウィンドウが表示されます。

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

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



1. オプションのドロップダウン リストから **cisco-admin** ドメインを選択し、**[NDFC アクセス管理者（NDFC Access Admin）]** チェックボックスをオンにして、**[保存（Save）]** をクリックします。
2. 手順 **a** を繰り返して、**cisco-stager** ドメインを **[NDFC ネットワーク ステージャ（NDFC Network Stager）]** ロール用に追加します。
3. セキュリティ ドメインをそれぞれのファブリック サイトに関連付けるには、次の手順を実行します。



Nexus ダッシュボードで、**[サイト（Sites）]** ウィンドウに移動します。**Fabirc-A** サイト名をクリックします。

スライドイン ペインが表示されます。Fabric-A サイトの **all** セキュリティ ドメインを表示できます。

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

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

   同様に、network-stager ドメインでも追加できます。

6. Nexus ダッシュボードからログアウトし、**Cisco** ユーザーとして再度ログインします。

   （注） ユーザー ロール Cisco は、権限に基づいて、Nexus ダッシュボードで NDFC 関連のオプションのみを表示できます。Nexus Dashboard サービスに制限されたユーザー アクセス。

7. NDFC アプリケーションへのナビゲーション。

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

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

Nexus Dashboard のセキュリティ ドメイン

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

Cisco Nexus ダッシュボード ファブリック コントローラ REST API は、この情報を使用して、認可を確認することによってアクションを実行します。

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

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

AV ペア

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

AV ペアの形式は次のとおりです。

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

例：`"avpair":`

`"shell:domains=all/network-admin/app-user|network-operator"`「`all/admin/`」はユーザをスーパーユーザにするため、`all/admin/` を使用した例を避けるのが最善です。

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

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

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

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

```
shell:roles="roleA roleB …"
```

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

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

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

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

セキュリティ ドメインの作成

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

1. Cisco Nexus Dashboard にログインします。
2. **[管理（Administrative）] > [セキュリティ（Security）]** の順に選択します。
3. **[セキュリティ ドメイン（Security Domain）]** タブに移動する
4. **[セキュリティ ドメインの作成（Create Security Domain）]** をクリックします。

5. 必要な詳細を入力し、**[作成（Create）]** をクリックします。

ユーザの作成

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

1. Cisco Nexus Dashboard にログインします。
2. **[管理（Administrative）] > [ユーザー（Users）]** の順に選択します。
3. **[ローカル ユーザーの作成（Create Local User）]** をクリックします。
4. 必要な詳細を入力し、**[セキュリティ ドメインの追加（Add Security Domain）]** をクリックします。
5. ドロップダウン リストからドメインを選択します。
6. 適切なチェックボックスをオンにして、Cisco Nexus Dashboard ファブリック コントローラ サービスの読み取りまたは書き込みロールを割り当てます。
7. [保存（Save）] をクリックします。

バックアップ ファブリック

選択したファブリックのバックアップを [ファブリック（Fabric）] ウィンドウから設定できます。同様に、**[ファブリックの概要（Fabric Overview）]** ウィンドウでバックアップを設定できます。メイン ウィンドウで**[ファブリックの概要（Fabric Overview）]**>**[アクション（Actions）]** を選択し、**[バックアップ ファブリック（Backup Fabric）]** をクリックします。

すべてのファブリック設定とインテントを自動または手動でバックアップできます。インテントであるCisco Nexus Dashboard ファブリック コントローラ の設定を保存できます。インテントは、スイッチにプッシュされる場合とされない場合があります。

Cisco Nexus Dashboard ファブリック コントローラは、次のファブリックをバックアップしません。

- モニタ専用モードの外部ファブリック：モニタ専用モードの外部ファブリックのバックアップを作成できますが、復元はできません。外部ファブリックがモニタ専用モードでない場合は、このバックアップを復元できます。
- 親 MSD ファブリック：MSD ファブリックのバックアップを作成できます。親ファブリックからバックアップを開始すると、バックアップ プロセスはメンバー ファブリックにも適用されます。ただし、Cisco Nexus Dashboard ファブリック コントローラは、メンバー ファブリックと MSD ファブリックのすべてのバックアップ情報を 1 つのディレクトリにまとめて保存します。

バックアップされた構成ファイルは、ファブリック名を持つ対応するディレクトリにあります。ファブリックの各バックアップは、手動または自動のどちらでバックアップされたかに関

係なく、異なるバージョンとして扱われます。バックアップのすべてのバージョンは、対応するファブリック ディレクトリにあります。

ファブリック設定およびインテントのスケジュール バックアップを有効にできます。

バックアップには、ファブリック上の使用済みリソースに関するリソースマネージャの状態に加えて、インテントとファブリック設定に関連する情報が含まれます。Cisco Nexus Dashboard ファブリック コントローラは、設定プッシュがある場合にのみバックアップされます。Cisco Nexus Dashboard ファブリック コントローラは、最後の設定プッシュ後に手動バックアップをトリガーしなかった場合にのみ、自動バックアップをトリガーします。

ゴールデン バックアップ

アーカイブの制限に達した後でも、削除しないバックアップにマークを付けることができます。これらのバックアップはゴールデン バックアップです。ファブリックのゴールデン バックアップは削除できません。ただし、Cisco Nexus Dashboard ファブリック コントローラは、最大 10 個のゴールデンバック アップのみをアーカイブします。ファブリックの復元中に、バックアップをゴールデン バックアップとしてマークできます。バックアップをゴールデン バックアップとしてマークするには、Web UI から次の手順を実行します。

手順

ステップ 1 ファブリックを選択し、**[Fabrics] > [Fabric Overview] >[More] > [Backup Fabric]** の順に選択します。

[バックアップ（Backup）] タブが表示されます。

ステップ 2 メイン ウィンドウで、**[アクション（Actions）]** > **[バックアップの構成（Configure Backup）]** を選択します。

[スケジュールされたアーカイブ（Scheduled Archive）] ウィンドウが表示されます。

ステップ 3 バックアップを選択する期間を選択します。

有効な値は、**1m**、**3m**、**6m**、**YTD**、**1y**および**All**です。グラフを拡大できます。デフォルトでは、**1m** のバックアップ情報（1 ヵ月）が表示されます。カスタムの日付範囲を選択することもできます。バックアップ情報には、次の情報が含まれます。

- バックアップ日
- デバイスの総数
- 同期しているデバイスの数
- 同期されていないデバイスの数

ステップ 4 バックアップをクリックして、ゴールデンとしてマークするバックアップを選択します。

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

ンバックアップはオレンジ色で示されます。自動バックアップの名前にはバージョンのみが含まれます。一方、手動バックアップには、手動バックアップを開始したときに指定したタグ名と、バックアップ名のバージョンがあります。バックアップにカーソルを合わせると、名前が表示されます。自動バックアップは、**[ファブリックの概要（Fabric Overview）]** ウィンドウの **[バックアップ（Backup）]** タブから開始します。手動バックアップを開始するには、[バックアップ（Backup）] タブの **[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。

ステップ 5 スイッチウィンドウに移動し、必要なスイッチ名のチェックボックスを選択し、**[スイッチ（Switch）]** > **[スイッチの概要（Switch Overview）]** > **[バックアップ（Backup）]** > **[アクション（Backup Actions）]を選択して、**>**[ゴールデンバックアップとしてマーク（Mark as golden backup）]** を選択します。

確認用のダイアログボックスが表示されます。

ステップ 6 **[はい（Yes）]** をクリックします。

ステップ 7 「ファブリックの復元」の項に記載されている残りのファブリック復元手順を続行するか、ウィンドウを終了します。

ファブリックの復元

次の表で、**[バックアップの復元（Restore Backup）]** タブに表示される列について説明します。

フィールド	説明
バックアップ日	バックアップの日付を指定します。
バックアップ バージョン	バックアップのバージョンを指定します。
バックアップ タグ	バックアップ名を指定します。
NDFC バージョン	NDFC のバージョンを指定します。
バックアップのタイプ	バックアップ タイプがゴールデン バックアップであるかどうかを指定します。

次の表では、**[アクション（Action）]** に表示されるフィールドおよび説明について記述します。

アクション	説明
ゴールデンとしてマーク	既存のバックアップをゴールデンバック アップとしてマークするには、**[ゴールデンとしてマーク]** を選択します。確認ウィンドウが表示されたら、**[確認（Confirm）]** をクリックします。詳細は「ゴールデン バックアップ」の項を参照してください。

アクション	説明
ゴールデンとして削除	ゴールデンバックアップから既存のバックアップを削除するには、**[ゴールデンとして削除（Remove as gold）]** を選択します。確認ウィンドウが表示されたら、**[確認（Confirm）]** をクリックします。

VXLAN OAM

Nexusダッシュボード ファブリック コントローラ では、VXLAN OAM は VXLAN ファブリック、eBGP VXLAN ファブリック、外部、および LAN クラシック ファブリック テクノロジーでサポートされます。VXLAN EVPN ベースのファブリック トポロジでは、フローの到達可能性や実際のパスなどの詳細を追跡できます。

ガイドライン

- OAM トレースを使用する前に、スイッチで OAM を有効にする必要があります。

（注） VXLAN OAM IPv6 は、Irvine リリース以降でサポートされます。

- HTTP ポートの NX-API および NX-API を有効にする必要があります。
- vPC advertise-pip を有効にする必要があります。
- スイッチ間 OAM の場合、VRF が、それらの VRF の下で IPv4 および IPv6 アドレスを持つループバック インターフェイスとともに設定されていることを確認します。
- ホスト間 OAM の場合、IPv6 の設定と同時に、VLAN を使用するネットワークが設定されていることを確認してください。
- Cisco NDFC リリース 12.1.1e から、IPv6 アンダーレイは VXLAN OAM でサポートされます。IPv6 アンダーレイを介した VXLAN OAM サポートを有効にするには、次のいずれかの手順を実行します。
  - **[トポロジ（Topology）]** ウィンドウで：
    - **[アクション（Actions）]** > **[ファブリックの追加（Add Fabric）]**を選択します。
    - **[一般パラメータ（General Parameters）]** タブで、**[IPv6 アンダーレイを有効にする（Enable IPv6 Underlay）]** チェックボックスをオンにします。
  - **[LAN ファブリック（LAN Fabrics）]** ウィンドウで：
    - **[アクション（Actions）]**>**[ファブリックの作成（Create Fabric）]**を選択します。
    - **[一般パラメータ（General Parameters）]** タブで、**[IPv6 アンダーレイを有効にする（Enable IPv6 Underlay）]** チェックボックスをオンにします。

（注） IPv4 アンダーレイから IPv6 アンダーレイへの変更は、既存のファブリック設定ではサポートされていません

ファブリック設定を IPv4 アンダーレイから IPv6 アンダーレイに変更するには、既存のファブリックを削除し、アンダーレイ IPV6 を有効にして新しいファブリックを作成します。

UI ナビゲーション

- **[トポロジ（Topology）]** ウィンドウで、**[アクション（Actions）]** をクリックします。ドロップダウン リストから **[VXLAN OAM]** オプションを選択します。
- **[LAN ファブリック（LAN Fabrics）]** ウィンドウから：**[LAN] > [ファブリック（Fabrics）]** を選択します。ファブリックのファブリック概要ウィンドウに移動します。[Actions] をクリックします。ドロップダウン リストから **[VXLAN OAM]** オプションを選択します。

[VXLAN OAM] ウィンドウが表示されます。左側の **[パス トレース設定（Path Trace Settings）]** ペインには、**[スイッチ間（Switch to Switch）]** タブと **[ホスト間（Host to Host）]** タブが表示されます。Nexus ダッシュボード ファブリック コントローラは、これら 2 つのオプションの送信元と宛先スイッチ間のトポロジ上のルートを強調表示します。

[スイッチ間（Switch to Switch）] オプションは、VTEP-to-VTEP の使用例の VXLAN OAM ping および traceroute テスト結果を提供します。**[スイッチ間（Switch to Switch）]** オプションを使用して検索を有効にするには、次の値を入力します。

- **[送信元スイッチ（Source Switch）]** ドロップダウンリストから、送信元スイッチを選択します。
- **[接続先スイッチ（Destination Switch）]** ドロップダウンリストから接続先スイッチを選択します。
- **VRF** ドロップダウンリストから VRF を選択するか詳細を入力します。
- 検索結果にすべてのパスを含めるには、**[含まれるすべてのパス（All Path Included）]** チェックボックスをオンにします。

[ホスト間（Host to Host）] オプションは、送信元ホストに接続されているVTEPまたはスイッチから、宛先ホストに接続されている VTEP またはスイッチへの特定のフローがたどる正確なパスの VXLAN OAM パストレース結果を提供します。**[ホスト間（Host to Host）]** の使用例には、次の 2 つのオプションがあります。

- ネットワークの VRF または SVI は、VXLAN EVPN ファブリック内のスイッチでインスタンス化されます。このようなシナリオでは、エンドホストの IP アドレス情報が必要です。
- 特定のネットワークのレイヤ 2 設定は、VXLAN EVPN ファブリック内のスイッチでインスタンス化されます。このようなシナリオでは、エンドホストの MAC アドレス情報と IP アドレス情報の両方が必要です。

[ホスト間（Host to Host）] オプションを使用して検索を有効にするには、次の値を入力します。

- **[送信元ホスト（Source Host）]** フィールドに、送信元ホストの IPv4/IPv6 アドレスを入力します。
- **[接続先ホスト IP（Destination Host IP）]** フィールドに、接続先ホストの IPv4/IPv6 アドレスを入力します。
- **[VRF]** フィールドで、ドロップダウン リストから [VRF] を選択するか、ホストに関連付けられている VRF 名を入力します。
- **[送信元ポート]** フィールドで、ドロップダウン リストからレイヤ 4 送信元ポート番号を選択するか、その値を入力します。
- **[宛先ポート]** フィールドで、宛先ポート番号を選択するか、その値を入力します。
- **[プロトコル（Protocol）]** フィールドで、ドロップダウン リストからプロトコル値を選択するか、その値を入力します。これはレイヤ 4 プロトコルで、通常は TCP または UDP です。
- **[レイヤ 2 のみ（Layer 2 only）]** チェックボックスをオンにして、一部のネットワーク（レイヤ 2 VNI）に対してレイヤ 2 専用モードで展開されている VXLAN-EVPN ファブリックを検索します。この検索オプションを使用する場合は、これらのネットワークのファブリックで SVI または VRF をインスタンス化しないでください。このオプションをオンにすると、送信元 MAC アドレス、宛先 MAC アドレス、および VNI の詳細も入力する必要があります。

スイッチからスイッチまたはホストからホストへのパス トレースを表示するには、**[パス トレースの実行（Run Path Trace）]** をクリックします。

トポロジ内の順方向パスと逆方向パスも表示できます。パス トレースの概要が **[サマリ（Summary）]** タブに表示されます。**[フォワード パス（Forward Path）]** タブまたは **[リバース パス（Reverse Path）]** タブで、順方向および逆方向のパスの詳細を表示できます。必要に応じて、属性で結果をフィルタリングします。

ファブリックの概要

ファブリック レベルの **[アクション（Actions）]** ドロップダウン リストでは、次の操作を実行できます。

Actions	説明
ファブリックの編集	• ファブリックを編集するには、**[アクション（Actions）]** > **[ファブリックの編集（Edit Fabric）]** を選択します。 • [ファブリックの編集（Edit fabric）] ウィンドウが表示されたら、必要な変更を行い、**[保存（Save）]** をクリックします。

Actions	説明
スイッチの追加	詳細については、[スイッチの追加（Add Switches）] を参照してください。
構成の再計算	詳細については、「構成の再計算と展開」の項を参照してください。
設定のプレビュー	詳細については、「構成のプレビュー」の項を参照してください。
展開構成	• 構成変更を展開するには、**[アクション（Actions）]**>**[構成の展開（Deploy Config）]**を選択します。 • 進行状況ウィンドウが表示され、確認メッセージが表示されます。
[詳細（More）]	
展開の有効化	• [ファブリックの概要（Fabrics Overview）]から、メインタブの **[アクション（Actions）]** を選択し、**[詳細（More）]** > **[展開の有効化（Deployment Enable）]** を選択します。 • 確認ウィンドウが表示されます。[OK] をクリックします。
展開の無効化	• [ファブリックの概要（Fabrics Overview）]から、メインタブの **[アクション（Actions）]** を選択し、**[詳細（More）]** > **[展開の無効化（Deployment Disable）]** を選択します。 • 確認ウィンドウが表示されます。[OK] をクリックします。
バックアップ ファブリック	詳細については、「バックアップ ファブリック」の項を参照してください。
ファブリックの復元	詳細については、「ファブリックの復元」の項を参照してください。
VXLAN OAM	詳細については、VXLAN OAM （161 ページ） の項を参照してください。 （注） この機能は、VXLAN OAM をサポートする VXLAN ファブリック、eBGP VXLAN ファブリック、外部、および LAN クラシック ファブリック テクノロジーの場合のみ、[アクション（Actions）] ドロップダウン リストに表示されます。

Actions	説明
エンドポイント ロケータの構成	エンドポイントロケータ（EPL）機能により、データセンター内のエンドポイントをリアルタイムで追跡できます。詳細については、エンドポイント ロケータ （283 ページ）を参照してください。

[ファブリックの概要（Fabric Overview）] には、ファブリックですべての操作を表示および実行できるタブがあります。

概要

[概要（Overview）] タブは、次の情報をカードとして表示します。

- ファブリック情報
- ファブリック

  子ファブリックがある場合に表示されます。例：マルチサイト ファブリック
- イベント分析
- スイッチの構成
- スイッチ
  - スイッチの状態
  - スイッチの設定
  - ロールの切り替え
  - スイッチ ハードウェア バージョン（Switch Hardware Version）
- VXLAN

  VXLAN ファブリックにのみ表示
  - ルーティング ループバック
  - VTEP ループバック
  - マルチサイト ループバック
  - NVE Int ステータス
  - ネットワーク/VRF の定義
  - 拡張ネットワーク/VRF
- [ホスト（Hosts）]

  このタブは、IPFM ファブリックを設定した場合にのみ表示されます。

- [フロー（Flows）]

  このタブは、IPFM ファブリックを設定した場合にのみ表示されます。

- レポート

[ホスト（Hosts）]

ホスト カードには、次の詳細が表示されます。

- **円グラフ**：各スライスには固有の色があり、ホストの役割と数（送信者、受信者、ARP など）が表示されます。選択した IPFM ファブリックのホスト タイプ（[送信者（Sender）] など）をクリックして、スライスを表示または非表示にします。

  詳細を表示するには、**[ファブリックの概要（Fabric Overview）]**>**[ホスト（Hosts）]**>**[検出されたホスト（Discovered Hosts）]** を選択します。

- **障害**：障害が存在する場合、ポリサーのドロップを含む障害の数が表示されます。詳細を表示するには、**[障害（Faults）]** をクリックして、**[ホスト]**>**[検出ホスト（Hosts Discovered Hosts）]** タブを開きます。

ホストの詳細については、ホスト （213 ページ） を参照してください。

[フロー（Flows）]

フロー カードには、次の詳細が表示されます。

- **円グラフ**：各スライスには固有の色があり、アクティブ、非アクティブ、送信者のみ、受信者のみなどのマルチキャスト フロー クラスと数が表示されます。[アクティブ（Active）] などのフロー クラスをクリックして、スライスを表示または非表示にします。

  詳細を表示するには、**[ファブリックの概要（Fabric Overview）]**>**[フロー（Flow）]**>**[フロー ステータス（Flow Status）]** を選択します。

- **グループ（Groups）**：マルチキャスト フロー グループの数を表示します。この情報は、IPFM ファブリック トポロジにも表示されます。

フローの詳細については、[フロー（Flows）] （229 ページ） を参照してください。

スイッチ

このタブでスイッチ操作を管理できます。各行はファブリック内のスイッチを表し、シリアル番号を含むスイッチの詳細が表示されます。

このタブから実行できるアクションの一部は、ファブリック トポロジ ウィンドウでスイッチを右クリックしたときにも使用できます。ただし、**[スイッチ（Switches）]** タブでは、ポリシーの展開など、複数のスイッチの設定を同時にプロビジョニングできます。

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

[スイッチ（Switches）] タブには、ファブリックで検出されたすべてのスイッチに関する次の情報が表示されます。

- 名前：スイッチ名を指定します。
- IP アドレス：スイッチの IP アドレスを指定します。
- ロール：スイッチのロールを指定します。
- シリアル番号：スイッチのシリアル番号を入力します。
- ファブリック名：スイッチが検出されたファブリックの名前を指定します。
- ファブリック ステータス：スイッチが検出されたファブリックのステータスを指定します。
- 検出ステータス：スイッチの検出ステータスを指定します。
- モデル：スイッチ モデルを指定します。
- ソフトウェア バージョン：スイッチのソフトウェア バージョンを指定します。
- 最終更新日：スイッチが最後に更新された日時を示します。
- モード：スイッチの現在のモードを指定します。
- vPC ロール：スイッチの vPC ロールを指定します。
- vPC ピア：スイッチの vPC ピアを指定します。

[スイッチ（Switches）] タブの [アクション（Action）] ドロップダウン リストには、次の操作が含まれています。

- **[スイッチの追加（Add switches）]**：このアイコンをクリックして、ファブリック内の既存または新規のスイッチを検出します。[Inventory Management] ダイアログボックスが表示されます。

  このオプションは、ファブリック トポロジ ウィンドウでも使用できます。[アクション（Actions）] ペインで [スイッチの追加（Add switches）] をクリックします。

  詳細については、次の項を参照してください。

  - ファブリックへのスイッチの追加：簡易ファブリックへのスイッチの追加について説明します。
  - 新しいスイッチの検出：外部ファブリックへの Cisco Nexus スイッチの追加に関する情報を提供します。

- 外部ファブリックへの非 Nexus デバイスの追加：外部ファブリックへの非 Nexus スイッチの追加に関する情報を提供します。

- プレビュー：保留中の設定と、実行中の設定と予想される設定の並べた比較をプレビューできます。
- 展開：スイッチ構成を展開します。Cisco Nexusダッシュボード ファブリック コントローラ リリース 11.3(1) 以降では、[展開（Deploy）] ボタンを使用して複数のデバイスの構成を展開できます。

（注）
- このオプションは、ファブリックがフリーズ モードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。
- MSD ファブリックでは、Border Gateway、Border Gateway Spine、Border Gateway Super-Spine、または外部ファブリック スイッチにのみ構成を展開できます。

- 検出：次の操作を実行できます。
  - ディスカバリ クレデンシャルの更新：認証プロトコル、ユーザ名、パスワードなどのデバイス クレデンシャルを更新します。
  - スイッチの再検出：スイッチ検出プロセスを Nexusダッシュボード ファブリック コントローラ afresh により開始します。

- ロールの設定：同じデバイスタイプの 1 つ以上のデバイスを選択し、[ロールの設定（Set Role）] をクリックしてデバイスのロールを設定します。デバイス タイプは次のとおりです。
  - NX-OS
  - IOS XE
  - IOS XR
  - その他

  ロールを設定する前に、スイッチをメンテナンス モードからアクティブ モードまたは動作モードに移動したことを確認します。ロールの設定の詳細については、「スイッチの動作」の項を参照してください。
- vPC ペアリング：スイッチを選択し、[vPC ペアリング（vPC Pairing）]をクリックしてvPC ペアを作成、編集、またはペアリング解除します。ただし、このオプションは、Cisco Nexus スイッチを選択した場合にのみ使用できます。詳細については、次の項を参照してください。

- 外部ファブリックでの vPC セットアップの作成：外部ファブリックで vPC ペアを作成する方法について説明します。
- vPC ファブリック ピアリング：簡単なファブリックで vPC ペアを作成する方法について説明します。

（注） 注: NDFC 12 では、スパイン、ボーダー スパイン、ボーダー ゲートウェイ スパイン、スーパー スパイン、ボーダー スーパー スパイン、およびボーダー ゲートウェイ スーパー スパインのロールで vPC ペアリングを作成できません。

- vPC の概要
- その他：その他の操作は [その他（More）] で提供されます。
- 表示コマンド：選択したスイッチで [表示（Show）] コマンドを実行します。ドロップダウン リストからコマンドを選択します。[変数（Variables）] フィールドに適切な値を入力し、**[実行（Execute）]** をクリックします。右側の列で [表示（Show）] コマンドを実行すると、出力が表示されます。
- 実行コマンド: 最初にログインするとき、Cisco NX-OS ソフトウェアは EXEC モードに切り替えます。EXEC モードで使用可能なコマンドには、デバイスの状態および構成情報を表示する show コマンド、clear コマンド、ユーザがデバイス コンフィギュレーションに保存しない処理を実行するその他のコマンドがあります。
- RMA のプロビジョニング：Cisco Nexusダッシュボード ファブリック コントローラ Easy Fabric モードを使用する場合、ファブリック内の物理スイッチを交換できます。
- **シリアル番号の変更**：スイッチが事前にプロビジョニングされている場合、スイッチのシリアル番号を変更できます。

  デバイスの事前プロビジョニング中に、スイッチのシリアル番号にダミー値を指定できます。ポリシー、リンク、インターフェイス、vrfs、またはネットワークの形式で事前プロビジョニングデバイスのネットワークを構成した後、ダミーのシリアル番号を必要な適切なシリアル番号に変更できます。スイッチのシリアル番号を変更する前に、メイン ウィンドウで**[アクション（Actions）] > [再計算と展開（Recalculate and deploy）]** をクリックして、スイッチに最新のデータを保存します。

（注） シリアル番号の変更は、Nexus 9000 シリーズ スイッチでのみ許可されています。

- コピー実行の開始：1つ以上のスイッチに対して、オンデマンドのコピー実行コンフィギュレーションからスタートアップ構成への動作を実行できます。

（注） このオプションは、ファブリックがフリーズモードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。

- リロード：選択したスイッチをリロードします。

（注） このオプションは、ファブリックがフリーズモードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。

- スイッチの削除：ファブリックからスイッチを削除します。

  このオプションは、ファブリックがフリーズモードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。

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

- モードの変更：スイッチのモードを [標準（Normal）] から [管理（Managed）] に変更できます。

  設定を保存してすぐに展開するか、後でスケジュールするかを選択できます。

検出 IP アドレスの変更に関する注意事項と制約事項

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

注意事項と制約事項

以下は、検出 IP アドレスの変更に関する注意事項と制約事項です。

- 検出 IP アドレスの変更は、管理インターフェイスを介して検出された NX-OS スイッチおよびデバイスでサポートされます。
- 検出 IP アドレスの変更は、次のようなテンプレートでサポートされます。
  - Easy_Fabric
  - Easy_Fabric_eBGP

- 外部
- LAN_Classic
- LAN_Monitor

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

検出 IP アドレスの変更

始める前に

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

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

手順

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

ステップ 2 ファブリック名をクリックして、必要なスイッチを表示します。

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

ステップ 3 **[起動（Launch）]** アイコンをクリックして、**[ファブリックの概要（Fabric Overview）]** ウィンドウを表示します。

ステップ 4 **[スイッチ（Switches）]**タブで、メイン ウィンドウの **[アクション（Action）]** ボタンの横にある **[最新表示（Refresh）]** アイコンをクリックします。

IP アドレスが変更されたスイッチは、**[検出ステータス（Discovery Status）]** 列で**到達不能**状態になります。

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

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

ステップ 6 [スイッチ（Switches）] タブ領域で **[アクション（Actions）]** > **[検出 IP の変更（Change Discovery IP）]** を選択します。

[検出 IP の変更（Change Discovery IP）] ウィンドウが表示されます。

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

ステップ 7 **[新規 IP アドレス（New IP Address）]** テキスト フィールドに適切な IP アドレスを入力し、**[OK]** をクリックします。

a) 正常に更新するには、新しい IP アドレスが Nexus Dashboard ファブリック コントローラから到達可能である必要があります。
b) 次の手順に進む前に、検出 IP アドレスを変更する必要があるデバイスに対して上記の手順を繰り返します。
c) ファブリックが管理対象モードの場合、デバイス モードは移行モードに更新されます。

ステップ 8 ファブリックの **[アクション（Actions）]** ドロップダウン リストから、**[構成の再計算（Recalculate Config）]** をクリックして、デバイスの Nexus Dashboard ファブリック コントローラ構成インテントの更新プロセスを開始します。同様に、トポロジ ウィンドウで構成を再計算できます。**[トポロジ（Topology）]** を選択し、スイッチを右クリックして **[構成の再計算（Recalculate Config）]** をクリックします。

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

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

リンク

異なるファブリックの境界スイッチ間（ファブリック間）、または同じファブリック内のスイッチ間（ファブリック内）にリンクを追加できます。Nexusダッシュボードファブリック コントローラ による管理対象のスイッチに対してのみ、ファブリック間接続（IFC）を作成できます。

物理的に接続する前にスイッチ間のリンクを定義する必要があるシナリオがあります。リンクは、ファブリック間リンクまたはファブリック内リンクです。そうすることで、リンクを追加する意図を表現して表すことができます。インテントのあるリンクは、実際に機能するリンクに変換されるまで、異なる色で表示されます。リンクを物理的に接続すると、接続済みとして表示されます。

管理リンクは、ファブリックトポロジでは赤色のリンクとして表示される場合があります。このようなリンクを削除するには、リンクを右クリックし、**[リンクの削除（Delete Link）]** をクリックします。

境界スイッチのスイッチ ロールに、Border Spine ロールと Border Gateway Spine ロールが追加されます。

事前プロビジョニングされたデバイスを宛先デバイスとして選択することで、既存のデバイスと事前プロビジョニングされたデバイス間のリンクを作成できます。

次の表では、**[リンク（Links）]** タブのフィールドについて説明します。

フィールド	説明
Fabric Name（ファブリック名）	ファブリックの名前を指定します。
名前	リンクの名前を指定します。 以前に作成されたリンクのリストが表示されます。このリストには、ファブリック内のスイッチ間のファブリック間リンクと、このファブリック内の境界スイッチと他のファブリック内のスイッチ間のファブリック内リンクが含まれています。
ポリシー	リンク ポリシーを指定します。
[情報（Info）]	リンクに関する詳細情報を提供します。
Admin State	リンクの管理状態を表示します。
Oper State	リンクの動作ステートを表示します。

次の表に、**[ファブリックの概要（Fabric Overview）]>[リンク（Links）]>[リンク（Links）]** に表示されるアクション項目（[アクション（Actions）] メニューのドロップダウンリスト）を示します。

アクション項目	説明
作成（Create）	次のリンクを作成できます。 • ファブリック内リンクの作成, on page 176 • ファブリック間リンクの作成, on page 174
編集	選択したファブリックを編集できます。

アクション項目	説明
削除	選択したファブリックを削除できます。
インポート	リンクの詳細を含むCSVファイルをインポートして、ファブリックに新しいリンクを追加できます。CSVファイルには、リンクテンプレート、送信元ファブリック、宛先ファブリック、送信元デバイス、宛先デバイス、送信元スイッチ名、宛先スイッチ名、送信元インターフェイス、宛先インターフェイス、およびnvPairsの詳細が含まれている必要があります。 **Note** • 既存のリンクは更新できません。 • [リンクのインポート（Import Links）]アイコンは、外部ファブリックでは無効です。
エクスポート	リンクを選択し、**[エクスポート（Export）]** を選択してリンクを CSV ファイルにエクスポートします。 リンクの次の詳細がエクスポートされます。リンク テンプレート、送信元ファブリック、宛先ファブリック、送信元デバイス、宛先デバイス、送信元スイッチ名、宛先スイッチ名、送信元インターフェイス、宛先インターフェイス、および nvPairs。nvPairs フィールドは JSON オブジェクトで構成されます。

ファブリック間リンクの作成

[リンク（Links）]タブをクリックします。リンクのリストを確認できます。まだリンクを作成していない場合、リストは空です。

ファブリック内リンクを作成するには、次の手順を実行します。

手順

ステップ 1 [アクション（Actions）] ドロップダウンリストから、**[作成（Create）]** を選択します。

[リンク管理 - リンクの作成（Link Management-Create Link）] ページが表示されます。

ステップ 2 IFC を作成しているため、[リンク タイプ（Link Type）] ドロップダウンボックスから **[ファブリック内（Intra-Fabric）]** を選択します。画面がそれに応じて変化します。

該当するフィールドは次のとおりです。

リンク タイプ：ファブリック内の 2 つのスイッチ間にリンクを作成するには、[ファブリック内（Intra-Fabric）] を選択します。

リンク サブタイプ：このフィールドは、これがファブリック内のリンクであることを示す「ファブリック」に入力されます。

リンク テンプレート：次のリンク テンプレートのいずれかを選択できます。

- **int_intra_fabric_num_link**：リンクが IP アドレスが割り当てられた 2 つのイーサネット インターフェイス間にある場合は、int_intra_fabric_num_link を選択します。
- **int_intra_fabric_unnum_link**：リンクが 2 つの IP アンナンバードインターフェイス間にある場合は、int_intra_fabric_unnum_link を選択します。
- int_intra_vpc_peer_keep_alive_link：リンクがvPCピアキープアライブリンクの場合は、int_intra_vpc_peer_keep_alive_linkを選択します。
- **int_pre_provision_intra_fabric_link**：リンクが2つの事前プロビジョニングされたデバイス間にある場合は、**int_pre_provision_intra_fabric_link** を選択します。[保存して展開（Save & Deploy）] をクリックすると、アンダーレイ サブネット IP プールから IP アドレスが選択されます。

これに対応して、[リンク プロファイル（Link Profile）] セクションのフィールドが更新されます。

送信元ファブリック：送信元ファブリックが既知であるため、このフィールドにファブリック名が入力されます。

宛先ファブリック：宛先ファブリックを選択します。ファブリック内リンクの場合、送信元と宛先のファブリックは同じです。

送信元デバイスと送信元インターフェイス：送信元デバイスと送信元インターフェイスを選択します。

宛先デバイスと宛先インターフェイス：宛先デバイスと宛先インターフェイスを選択します。

（注） 既存のデバイスと事前プロビジョニングされたデバイスの間にリンクを作成する場合は、事前プロビジョニングされたデバイスを宛先デバイスとして選択します。

[リンク プロファイル（Link Profile）]セクションの **[全般（General）]** タブ

インターフェイス VRF：このインターフェイスのデフォルト以外の VRF の名前。

送信元 IP および宛先 IP：送信元と宛先インターフェイスの送信元 IP および宛先 IP アドレスをそれぞれ指定します。

（注） int_pre_provision_intra_fabric_link template を選択すると、[送信元 IP] フィールドと [宛先 IP] フィールドは表示されません。

インターフェイスの管理状態（Interface Admin State）：このチェックボックスをオンまたはオフにして、インターフェイスの管理状態を有効または無効にします。

MTU：2 つのインターフェイスの最大伝送単位（MTU）を指定します。

[送信元インターフェイスの説明（Source Interface Description）] および [宛先インターフェイスの説明（Destination Interface Description）]：後で使用するためのリンクについて説明します。

たとえば、リンクがリーフ スイッチとルート リフレクタ デバイスの間にある場合は、これらのフィールドに情報を入力できます（リーフ スイッチから RR 1 へのリンク、および RR 1 からリーフ スイッチへのリンク）。この説明は設定に変換されますが、スイッチにはプッシュされません。保存して展開すると、実行構成に反映されます。

[送信元インターフェイスの BFD エコーの無効化（Disable BFD Echo on Source Interface）] および **[宛先インターフェイスの BFD エコーの無効化（Disable BFD Echo on Destination Interface）]**：送信元および宛先インターフェイスで BFD エコー パケットを無効にします。

BFD エコー フィールドは、ファブリック設定で BFD を有効にした場合にのみ適用されることに注意してください。

送信元インターフェイス フリーフォーム CLI および宛先インターフェイス フリーフォーム CLI（Source Interface Freeform CLIs and Destination Interface Freeform CLIs）：送信元と宛先インターフェイスに特別なフリーフォーム構成を入力してください。スイッチの実行構成に表示されている設定を、インデントなしで追加する必要があります。詳細については、「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。

ステップ 3 画面の下部にある **[保存（Save）]** をクリックします。

IFC が作成され、リンクのリストに表示されていることがわかります。

ステップ 4 [ファブリックの概要アクション（Fabric Overview Actions）] ドロップダウンリストで、**[構成の再計算（Recalculate Config）]** を選択します。

[構成の展開（Deploy Configuration）] 画面が表示されます。

スイッチの構成ステータスが表示されます。**[保留中の構成（Pending Config）]** 列のそれぞれのリンクをクリックして、保留中の構成を表示することもできます。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）] 画面を閉じます。

ステップ 5 **[ファブリックの概要アクション（Fabric Overview Actions）]** ドロップダウンリストから、**[構成の展開（Deploy Config）]** を選択します。

保留中の構成が展開されます。

すべての行で進行状況が 100% であることを確認したら、画面の下部にある **[閉じる（Close）]** をクリックします。[リンク（Links）] 画面が再び表示されます。ファブリック トポロジでは、2 つのデバイス間のリンクが表示されます。

ファブリック内リンクの作成

[リンク（Links）] タブをクリックします。リンクのリストを確認できます。まだリンクを作成していない場合、リストは空です。

（注） 外部ファブリックでは、ファブリック間リンクが BGW、ボーダー リーフ/スパイン、およびエッジ ルータ スイッチをサポートします。

ファブリック間リンクを作成するには、次の手順を実行します。

手順

ステップ 1 [アクション（Actions）] ドロップダウンリストから、**[作成（Create）]** を選択します。

[リンク管理 - リンクの作成（Link Management-Create Link）] ページが表示されます。

ステップ 2 IFC を作成しているため、[Link Type] ドロップダウン ボックスから **[ファブリック間（Inter-Fabric）]** を選択します。画面がそれに応じて変化します。

ファブリック間リンク作成のフィールドについて説明します。

リンク タイプ：ファブリック間（Inter-Fabric） を選択して、2 つのファブリック間の境界スイッチを介したファブリック間接続を作成します。

リンク サブタイプ：このフィールドは IFC タイプを入力します。ドロップダウン リストから [VRF_LITE]、[MULTISITE_UNDERLAY]、または[MULTISITE_OVERLAY] を選択します。

マルチサイト オプションについては、マルチサイトの使用例で説明します。

VXLAN MPLS 相互接続については、MPLS SR および LDP ハンドオフ の章を参照してください。

ルーテッドファブリックの相互接続については、「*eBGP* アンダーレイを使用したファブリックの構成（*Configuring a Fabric with eBGP Underlay*）」の章の「ルーテッド ファブリックと外部ファブリック間のファブリック間リンクの作成（*Creating Inter-Fabric Links between a Routed Fabric and an External Fabric*）」の項を参照してください。

リンク テンプレート：リンク テンプレートが入力されます。

テンプレートには、選択内容に基づいて、対応するパッケージ済みのデフォルトテンプレートが自動的に入力されます。

（注） ユーザ定義テンプレートを追加、編集、削除できます。詳細については、「制御」の章の「テンプレート」の項を参照してください。

[送信元ファブリック]：このフィールドには、送信元ファブリック名が事前に入力されています。

[宛先ファブリック]：このドロップダウンボックスから宛先ファブリックを選択します。

[送信元デバイスと宛先インターフェイス]：宛先デバイスに接続する送信元デバイスとイーサネット インターフェイスを選択します。

[宛先デバイスと宛先インターフェイス]：送信元デバイスに接続する宛先デバイスとイーサネット インターフェイスを選択します。

送信元デバイスと送信元インターフェイスの選択に基づいて、Cisco Discovery Protocol 情報（使用可能な場合）に基づいて宛先情報が自動入力されます。宛先外部デバイスが宛先ファブリックの一部であることを確認するために、追加の検証が実行されます。

[リンク プロファイル] セクションの **[全般]** タブ。

ローカル BGP AS # ：このフィールドには、送信元ファブリックの AS 番号が自動入力されます。

IP_MASK：宛先デバイスに接続する送信元インターフェイスの IP アドレスをこのフィールドに入力します。

NEIGHBOR_IP：宛先インターフェイスの IP アドレスをこのフィールドに入力します。

NEIGHBOR_ASN：このフィールドには、宛先デバイスの AS 番号が自動入力されます。

ステップ 3 画面の下部にある **[保存（Save）]** をクリックします。

IFC が作成され、リンクのリストに表示されていることがわかります。

ステップ 4 [ファブリックの概要アクション（Fabric Overview Actions）] ドロップダウンリストで、**[構成の再計算（Recalculate Config）]** を選択します。

[構成の展開（Deploy Configuration）] 画面が表示されます。

スイッチの構成ステータスが表示されます。**[保留中の構成（Pending Config）]** 列のそれぞれのリンクをクリックして、保留中の構成を表示することもできます。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）] 画面を閉じます。

ステップ 5 **[ファブリックの概要アクション（Fabric Overview Actions）]** ドロップダウンリストから、**[構成の展開（Deploy Config）]** を選択します。

保留中の構成が展開されます。

すべての行で進行状況が 100％ であることを確認したら、画面の下部にある **[閉じる（Close）]** をクリックします。[リンク（Links）] 画面が再び表示されます。ファブリック トポロジでは、2 つのデバイス間のリンクが表示されます。

2 つのファブリックがMSDのメンバー ファブリックである場合は、MSD トポロジにもリンクが表示されます。

次のタスク

2 つのファブリックが MSD のメンバー ファブリックである場合は、MSD トポロジにもリンクが表示されます。

ToExternalOnly メソッドまたは MSD ファブリック経由のマルチサイト機能を使用して VRF Lite 機能を有効にすると、（VXLAN ファブリック）ボーダー/BGW デバイスと接続された（外部ファブリック）エッジ ルータ/コア デバイス間で IFC が自動的に作成されます。ER/コア/ボー

ダー/BGWデバイスを削除すると、Nexusダッシュボードファブリック コントローラ でそのスイッチとの間で対応する IFC（リンク PTI）が削除されます。その後、Nexusダッシュボード ファブリック コントローラ は次の保存および展開操作で、残りのデバイスから対応する IFC 設定（存在する場合）を削除します。また、IFC およびオーバーレイ拡張を備えたデバイスをそれらの IFC から削除する場合は、それらの IFC に対応するすべてのオーバーレイ拡張を展開して、スイッチを削除できるようにする必要があります。

VRF 拡張を展開解除するには、VXLAN ファブリックと拡張 VRF を選択し、VRF 展開画面で VRF を展開解除します。

IFC を削除するには、[リンク（Links）] タブから IFC を削除します。

ファブリック スイッチ名が一意であることを確認します。同じ名前のスイッチに VRF 拡張を導入すると、設定が誤ってしまいます。

新しいファブリックが作成され、Nexusダッシュボード ファブリック コントローラ でファブリックスイッチが検出され、これらのスイッチでアンダーレイ ネットワークがプロビジョニングされ、Nexusダッシュボード ファブリック コントローラ とスイッチ間の設定が同期されます。その他のタスクは、次のとおりです。

- vPC、ループバック インターフェイス、サブインターフェイス設定などのインターフェイス構成をプロビジョニングします。インターフェイスを参照してください。
- オーバーレイ ネットワークと VRF を作成し、スイッチに展開します。「ネットワークおよび VRF の作成と展開」を参照してください。

プロトコル ビュー

このタブには、選択したファブリック内のリンクのプロトコルが表示されます。

次の表では、**[プロトコル ビュー（Protocol View）]** タブのフィールドについて説明します。

フィールド	説明
Fabric Name（ファブリック名）	ファブリックの名前を指定します。
名前	リンクの名前を指定します。
存在する（Is Present）	リンクが存在するかどうかを指定します。
リンクタイプ	リンクのタイプを指定します。
リンクステータス	リンクの状態を示します。
稼働時間	リンクがアップしてからの時間を指定します。

インターフェイス

ここでは、次の内容について説明します。

- インターフェイス

- インターフェイスグループ

ポリシー

Nexusダッシュボード ファブリック コントローラ は、一連のスイッチをグループ化する機能を提供し、グループに一連のアンダーレイ構成をプッシュできます。

[LAN] > [ポリシー（Policies）] を選択して、ポリシーのリストを表示します。

次の表では、**LAN > [ポリシー（Policies）]** で表示されるフィールドを説明します。

フィールド	説明
ポリシー ID	ポリシー ID を指定します。
スイッチ	スイッチ名を指定します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。
テンプレート	テンプレート名を指定します。
説明	説明を指定します。 （注） Cisco NDFC リリース 12.1.1e から、スイッチのシリアル番号の変更が許可され、古いシリアル番号と新しいシリアル番号の両方がこの列に表示されます。
エンティティ名	エンティティ名を指定します。
エンティティ タイプ（Entity Type）	エンティティ タイプを指定します。
送信元	送信元を指定します。
優先順位（Priority）	プライオリティを指定します。
コンテンツ タイプ	コンテンツ タイプの種類を指定します。
Fabric Name（ファブリック名）	ファブリック名を指定します。
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。
編集可能	ポリシーが編集可能かどうかを示すブール値を指定します。
削除済みマーク	ポリシーが削除対象としてマークされているかどうかを示すブール値を指定します。

次の表で、**LAN > [ポリシー（Policies）]** で表示される **[アクション（Actions）]** メニュー ドロップダウン リストの アクション項目について説明します。

アクション項目	説明
Add Policy	ポリシーを追加するには、「ポリシーの追加」を参照してください。
ポリシーの編集	テーブルからポリシーを選択し、**[ポリシーの編集（Edit Policy）]** を選択してポリシーを変更します。 （注） • イタリック体のフォントのポリシーは編集できません。これらのポリシーの **[編集可能（Editable）]** 列と **[削除済みマーク（Mark Deleted）]** 列の値は false です。 • **[削除済みマーク（Mark Deleted）]** 値が *true* に設定されているポリシーを編集すると、警告が表示されます。**[削除済みマーク（Mark Deleted）]** ポリシーのスイッチの自由形式の子ポリシーが [ポリシー（Policies）] ダイアログボックスに表示されます。**Python** の switch_freeform ポリシーのみを編集できます。**Template_CLI** switch_freeform_config ポリシーは編集できません。
ポリシーの削除	テーブルからポリシーを選択し、**[ポリシーの削除（Delete Policy）]** を選択してポリシーを削除します。 （注） **[削除済みマーク（Mark Deleted）]** の値が *true* に設定されているポリシーを削除すると、警告が表示されます。
生成された構成	すべてのユーザが行った構成変更の差分を表示するには、テーブルからポリシーを選択し、**[生成された構成（Generated Config）]** を選択します。

アクション項目	説明
構成のプッシュ	テーブルからポリシーを選択し、**[構成のプッシュ（Push Config）]** を選択してポリシー構成をデバイスにプッシュします。 （注） • このオプションは、ファブリックがフリーズモードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。 • Python ポリシーの設定をプッシュすると、警告が表示されます。 • **[削除済みマーク（Mark Deleted）]** 値が *true* に設定されているポリシーの設定をプッシュすると、警告が表示されます。

イベント分析

イベント分析には、次のトピックが含まれます。

アラーム

このタブには、さまざまなカテゴリに対して生成されたアラームが表示されます。このタブには、ID（オプション）、重大度、障害ソース、名前、カテゴリ、確認応答、作成時刻、最終更新日（オプション）、ポリシー、メッセージなどの情報が表示されます。このタブで [更新間隔（Refresh Interval）] を指定できます。1 つ以上のアラームを選択し、[ステータスの変更（Change Status）] ドロップダウンリストを使用して、アラームのステータスを確認または確認解除できます。また、1 つ以上のアラームを選択し、[削除（Delete）] ボタンをクリックしてアラームを削除できます。

イベント

このタブには、スイッチに対して生成されたイベントが表示されます。このタブには、Ack、確認済みユーザ、グループ、スイッチ、重大度、ファシリティ、タイプ、カウント、最終確認、説明などの情報が表示されます。1つ以上のイベントを選択し、[ステータスの変更（Change Status）] ドロップダウンリストを使用して、そのステータスを確認または確認解除できます。また、1 つ以上のアラームを選択し、[削除（Delete）] ボタンをクリックしてアラームを削除できます。すべてのイベントを削除する場合は、[すべてを削除（Delete All）] ボタンをクリックします。

次の表で、**[操作（Operations）] > [イベント分析（Event Analytics）] > [イベント（Events）]** に表示されるフィールドについて説明します。

フィールド	説明
グループ	ファブリックを指定します。
スイッチ	スイッチのホスト名を指定します。
重大度	イベントの重大度を指定します。
施設	イベントを作成するプロセスを指定します。 イベント ファシリティには、NDFC と syslog ファシリティとの 2 つのカテゴリがあります。 Nexusダッシュボードファブリック コントローラ ファシリティは、Nexusダッシュボード ファブリック コントローラ 内部サービスによって生成されたイベントと、スイッチによって生成された SNMP トラップを表します。syslog ファシリティは、syslog メッセージを作成したマシン プロセスを表します。
タイプ	スイッチ/ファブリックの管理方法を指定します。
数	イベントが発生した回数を提供します。
作成時刻	イベントが作成された時刻を指定します。
前回の検出	イベントが最後に実行された時刻を指定します。
説明	イベントに提供される説明を指定します。
Ack	イベントを確認するかどうかを指定します。

次の表では、**[操作（Actions）]** メニュー ドロップダウン リストで、**[操作（Operations）] > [イベント分析（Event Analytics）] > [イベント（Events）]** に表示されるアクション項目について説明します。

アクション項目	説明
確認応答あり	テーブルから 1 つ以上のイベントを選択し、**[確認（Acknowledge）]**アイコンを選択して、ファブリックのイベント情報を確認します。 ファブリックのイベントを確認すると、確認アイコンが [グループ（Group）] の横の [Ack] 列に表示されます。
未確認	テーブルから 1 つ以上のイベントを選択し、**[確認解除（Unacknowledge）]** アイコンを選択して、ファブリックのイベント情報を確認します。

アクション項目	説明
削除	イベントを選択し、**[削除（Delete）]** をクリックします。
イベントのセットアップ	では新しいイベントを設定できます。詳細については、イベントのセットアップを参照してください。

アカウンティング

Cisco Nexusダッシュボード ファブリック コントローラ Web UI でアカウンティング情報を表示できます。

次の表では、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アカウンティング（Accounting）] >** に表示されるフィールドについて説明します。

フィールド	説明
ソース（Source）	送信元 SGT を指定します。
User Name	ユーザ名を指定します。
時間	イベントが作成された時刻を指定します。
説明	説明を表示します。
グループ	グループの名前を指定します。

次の表では、**[操作（Actions）]** ドロップダウンリストのアクション項目について説明します。これらの項目は、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アカウンティング（Accounting）]** に表示されます。

アクション項目	説明
削除	リストからアカウンティング情報を削除するには、行を選択して **[削除（Delete）]** を選択します。

[最近のタスク（Recent Tasks）]

UI パス ：**[LAN] > [ファブリック（Fabric）] > [ファブリックの概要（Fabric Overview）] > [イベント分析（Event Analytics）] > [最近のタスク（Recent Tasks）]**

[最近のタスク（Recent Tasks）] タブでは、イベント分析に対して行われた変更を表示できます。

（注） デバイスを再起動すると、最近のタスクの詳細が消去されます。

次の表では、**[最近のタスク（Recent Tasks）]** タブに表示されるフィールドについて説明します。

フィールド	説明
ファブリック	ファブリックの名前を指定します。
タスク名（Task Name）	ファブリックで最近実行された操作の名前を指定します。
タスクの説明	ファブリックで実行されるタスクの説明を指定します。
Duration	タスクの期間を指定します。
完了（Completed）/進行中（Progress）	タスクが 100% 完了したか、まだ進行中かなど、進行状況の詳細を指定します。

VRF

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、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。

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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] を選択します。 >
- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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] を開きます。 >

（注） オーバーレイモード CLI は Easy ファブリックおよび eBGP Vxlan ファブリックにのみ使用可能です。

オーバーレイ VRF を作成するには、ファブリックの VRF を作成し、ファブリック スイッチに展開します。VRF を接続または展開する前に、オーバーレイ モードを設定します。オーバーレイ モードの選択方法の詳細については、オーバーレイ モード （51 ページ）を参照してください。

[VRF] 水平タブで VRF の詳細を表示し、[VRF 接続（VRF Attachments）] 水平タブで VRF 接続の詳細を表示できます。

この項の内容は、次のとおりです。

VRF

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、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。

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

- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。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（VRFs）]** を開きます。

このタブを使用して、VRFを作成、編集、削除、インポート、およびエクスポートします。レイヤ2を使用してネットワークを作成する場合を除き、VRFの作成後にのみネットワークを作成できます。

表 *1: VRF* 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 ステータス	VRF 展開のステータスが NA、非同期、保留中、展開済みなどのいずれであるかを指定します。
VRF ID	VRF の ID を指定します。

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、**[VRF]**水平タブ（**[VRF（VRFs）]** タブ、**[ファブリックの概要（Fabric Overview）]** ウィンドウ内）に表示されます。

表 *2: VRF* のアクションと説明

アクション項目	説明
作成（Create）	新しい VRF を作成できます。詳細については、VRF の作成 （187 ページ）を参照してください。
編集	選択した VRF を編集できます。 VRF 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て、**[編集（Edit）]** を選択します。**[VRF の編集（Edit VRF）]** ウィンドウでは、パラメータを編集し、**[保存（Save）]** をクリックして変更を保持するか、**[キャンセル（Cancel）]** をクリックして変更を破棄できます。

アクション項目	説明
インポート	ファブリックの VRF 情報をインポートできます。 VRF 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 情報を含む .csv ファイルを選択します。[開く（Open）] をクリックします。VRF 情報がインポートされ、**[ファブリック概要（Fabric Overview）]** ウィンドウの **[VRF]** タブに表示されます。
エクスポート	.csv ファイルに VRF 情報を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、VRF の作成時に保存した設定の詳細など、各 VRF に関する情報が含まれています。 VRF 情報をエクスポートするには、**[エクスポート（Export）]** 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 Nexusダッシュボード ファブリック コントローラ から選択し、**[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。 （注） エクスポートされた .csv ファイルは参照用に使用することや、新しい VRF を作成するためのテンプレートとして使用することができます。
削除	選択した VRF を削除できます。 VRF を削除するには、削除する VRF の横にあるチェックボックスをオンにし、**[削除（Delete）]** を選択します。複数の VRF エントリを選択し、同じインスタンスで削除できます。VRF の削除を求める警告メッセージが表示されます。**[確認（Confirm）]** をクリックして削除するか、**[キャンセル（Cancel）]** をクリックしてVRFを保持します。選択した VRF が正常に削除されたことを示すメッセージが表示されます。

VRF の作成

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、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。

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

- **[LAN] > [ファブリック（Fabrics）]**を選択します。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（VRFs）]** を開きます。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI を使用して VRF を作成するには、次の手順を実行します。

手順

ステップ 1 **[アクション (Actions)]** をクリックし、**[作成 (Create)]** を選択します。

[VRF の作成（Create VRF）] ウィンドウが表示されます。

ステップ 2 必須のフィールドに必要な詳細情報を入力します。使用可能なフィールドは、ファブリック タイプによって若干異なります。

このウィンドウのフィールドは次のとおりです。

[VRF名（VRF Name）]：仮想ルーティングおよび転送（VRF）の名前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。

（注） 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 を設定させること、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 を設定させること、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)]：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 (VRF Extension Template)]：ユニバーサル拡張テンプレートが自動入力されます。これにより、このネットワークを別のファブリックに拡張できます。メソッドは VRF Lite、Multi Site などです。このテンプレートは、境界リーフ スイッチおよびBGWに適用できます。

VRF プロファイルのセクションには、**[一般パラメータ（General Parameters）]** タブ、**[詳細（Advanced）]** タブ、**[ルート ターゲット（Route Target）]** タブがあります。

a) **[一般 (General)]** タブには以下のフィールドがあります。

[VRF VLAN 名（VRF Vlan Name）]：VRF の VLAN 名を入力します。

[VRF の説明（VRF Description）]：VRFの説明を入力します。

[VRF インターフェイスの説明（VRF Intf Description）]：VRFインターフェイスの説明を入力します。

b) **[詳細 (Advanced)]** タブをクリックすると、オプションとして、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。

[VRF インターフェイス MTU（VRF Intf MTU）]：VRFインターフェイスMTUを指定します。

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

[再配布直接ルート マップ（Redistribute Direct Route Map）]：再配布直接ルート マップ名を指定します。

[最大 BGP パス（Max BGP Paths）]：最大 BGP パスを指定します。有効な値の範囲は 1 ー 64 です。

[最大 iBGP パス（Max iBGP Paths）]：最大 iBGP パスを指定します。有効な値の範囲は 1 ー 64 です。

[TRM の有効（TRM Enable）]：TRM を有効にするには、このチェックボックスをオンにします。

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

NO RP - 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。

NO RP を有効にすると、RP 外部、RP アドレス、RP ループバック ID、およびオーバーレイ マルチキャスト グループが VRF アタッチメントで無効になります。

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

RP アドレス：RP の IP アドレスを指定します。

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

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

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

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

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

[TRM BGW マルチサイトの有効化（Enable TRM BGW MSite）]：チェックボックスをオンにして、ボーダー ゲートウェイ マルチサイトで TRM を有効にします。

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

[デフォルト ルートのアドバタイズ（Advertise Default Route）]：このチェックボックスをオンにすると、デフォルト ルートのアドバタイズメントが内部的に制御されます。

異なる VXLAN ファブリック内（両方のファブリックにサブネットが存在する）のエンドホスト間のサブネット間通信を許可するには、関連付けられている VRF の **デフォルト ルートのアドバタイズ**機能を無効にする（**[デフォルト ルートのアドバタイズ（Advertise Default Route）]** チェックボックスをオフにする）必要があります。これにより、両方のファブリックでホストの /32 ルートが表示されます。たとえば、ファブリック 1 のホスト 1（VNI 30000、VRF 50001）は、ホスト ルートが両方のファブリックに存在する場合にのみ、ファブリック 2 のホスト 2（VNI 30001、VRF 50001）にトラフィックを送信できます。サブネットが 1 つのファブリックにのみ存在する場合は、サブネット間通信にはデフォルト ルートだけで十分です。

[スタティック 0/0 ルートの設定（Config Static 0/0 Route）]：スタティック デフォルト ルートの設定を制御するには、このチェックボックスをオンにします。

[BGP ネイバーパスワード（BGP Neighbor Password）：VRF Lite BGP のネイバー パスワードを指定します。

[BGP パスワード キー暗号化タイプ（BGP Password Key Encryption Type）]：このドロップダウン リストから暗号化タイプを選択します。

[Netflow の有効化（Enable Netflow）]：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 モニター（Netflow Monitor）]：VRF-lite の Netflow 構成のモニターを指定します。

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。

Cisco NDFC の Netflow サポートについては、Netflow サポート （133 ページ） を参照してください。

c) [ルート ターゲット（Route Target）] タブのフィールドは次のとおりです。

[RT 自動生成を無効にする（Disable RT Auto-Generate）]：チェックボックスをオンにして、IPv4、IPv6 VPN/EVPN/MVPN の RT 自動生成を無効にします。

[インポート（Import）]：インポートする VPN ルート ターゲットのコンマ区切りリストを指定します。

[エクスポート（Export）]：エクスポートする VPN ルート ターゲットのコンマ区切りリストを指定します。

[EVPN のインポート（Import EVPN）]：インポートする EVPN ルート ターゲットのコンマ区切りリストを指定します。

[EVPN のエクスポート（Export EVPN）]：エクスポートする EVPN ルート ターゲットのコンマ区切りリストを指定します。

[MVPN のインポート（Import MVPN）]：インポートする MVPN ルート ターゲットのコンマ区切りリストを指定します。

[MVPN のエクスポート（Export MVPN）]：エクスポートする MVPN ルート ターゲットのコンマ区切りリストを指定します。

（注） デフォルトでは、[MVPN のインポート（Import MVPN）] および [MVPN のエクスポート（Export MVPN）] テキスト フィールドはグレー表示されています。これらのテキスト フィールドを有効にするには、**[TRM 有効（TRM Enable）]** チェックボックスをオンにして、有効にする必要があります（**[詳細（Advanced）]** タブ）。

ステップ 3 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。

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、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。

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

表 *3: 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	スイッチ名を指定します。
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、Easy Fabric IOS XE 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。 （注） 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、**[VRF アタッチメント（VRF Attachments）]**水平タブ（**[VRF（VRFs）]** タブ、**[ファブリックの概要（Fabric Overview）]** ウィンドウ内）に表示されます。

表 *4 : 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。 **[展開履歴（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、ユーザー、完了時刻など、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）]** 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。また、**[詳細履歴（Detailed History）]** リンク（**[コマンド（Commands）]** 列、**[展開履歴（Deployment History）]** タブ）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 アタッチメント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て、**[編集（Edit）]** アクションを選択します。**[VRF アタッチメントの編集（Edit VRF Attachment）]** ウィンドウで、必要な値を編集し、VRFアタッチメントをアタッチまたはデタッチし、**[編集（Edit）]** リンクをクリックしてスイッチの CLI フリーフォーム設定を編集し、**[保存（Save）]** をクリックして変更を適用するか、**[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、**[VRF アタッチメント（VRF Attachments）]** 水平タブ（**[VRF（VRFs）]** タブ、**[ファブリックの概要（Fabric Overview）]** ウィンドウ）の表に表示されます。

アクション項目	説明
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。 （注） 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、**[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。 （注） 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 名の横にあるチェックボックスをオンにして、**[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。 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。[導入（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。

アクション項目	説明
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、**[VRF アタッチメント（VRF Attachments）]** 水平タブ（**[VRF（VRFs）]** タブ、**[ファブリックの概要（Fabric Overview）]** ウィンドウ）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Nexus ダッシュボード ファブリック コントローラ から選択し、**[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、**[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。 アタッチメントから VRF を素早くデタッチするには、**[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。

ネットワーク

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、簡易ファブリック、および MSD ファブリックにのみ適用されます。

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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。**[ファブリック概要（Fabric Overview）]** > **[ネットワーク（Networks）]** を選択します。
- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。ファブリックをダブルクリックして、**[ファブリック概要（Fabric Overview）]** > **[ネットワーク（Networks）]** を開きます。

（注） 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、レイヤ 2 を選択した場合は、VRF は必要ありません。VRF の詳細については、VRF （185 ページ）を参照してください。

オーバーレイ ネットワークを作成するには、ファブリックのネットワークを作成し、ファブリック スイッチに展開します。ネットワークを展開する前に、オーバーレイ モードを設定します。オーバーレイ モードの選択方法の詳細については、オーバーレイ モード （51 ページ）を参照してください。

インターフェイス グループの作成とネットワークの接続については、インターフェイスグループ を参照してください。

[ネットワーク（Networks）] 水平タブでネットワークの詳細を表示し、**[ネットワーク接続（Network Attachments）]** 水平タブでネットワーク接続の詳細を表示できます。

この項の内容は、次のとおりです。

ネットワーク

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、**[ネットワーク (Networks)]** ウィンドウに表示されるものです。

表 *5:* ネットワーク アクションと説明

アクション項目	説明
作成（Create）	ファブリックの新しいネットワークを作成できます。新しいネットワークの作成手順については、スタンドアロン ファブリック向けのネットワークの作成（201 ページ）を参照してください。

アクション項目	説明
編集	選択したネットワークパラメータを表示または編集できます。 ネットワーク情報を編集するには、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、**[編集 (Edit)]** を選択します。**[ネットワークの編集 (Edit Network)]** ウィンドウで、必要な値を編集し、**[送信 (Submit)]** をクリックして変更を適用するか、**[キャンセル (Cancel)]** をクリックしてホストエイリアスを破棄します。編集したネットワークは、**[ネットワーク (Networks])** タブ (**[ファブリックの概要 (Fabric Overview)]**ウィンドウ) のテーブルに表示されます。
インポート	ファブリックのネットワーク情報をインポートできます。 ネットワーク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、ホストIPアドレスおよび対応する一意のネットワーク情報を含む `.csv` ファイルを選択します。[開く（Open）] をクリックします。ホストエイリアスがインポートされ、**[ネットワーク (Networks)]** タブ (**[ファブリックの概要 (Fabric Overview)]** ウィンドウ) に表示されます。

アクション項目	説明
エクスポート	ネットワーク接続についての情報は、.csv ファイルにエクスポートすることが可能です。エクスポートされたファイルには、所属するファブリック、関連付けられている VRF、ネットワークの作成に使用されたネットワーク テンプレート、およびネットワークの作成時に保存したその他のすべての設定の詳細が含まれます。 ネットワーク情報をエクスポートするには、**[エクスポート (Export)]** を選択します。Nexusダッシュボード ファブリック コントローラ からの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。ファイル名には、ファイルがエクスポートされた日時が付加されます。3. （注） エクスポートされた .csv ファイルは参照用に使用することや、新しいネットワークを作成するためのテンプレートとして使用することができます。ファイルをインポートする前に、.csv ファイルの新しいレコードを更新します。[networkTemplateConfig] フィールドに JSON オブジェクトが含まれていることを確認します。画面の右下にあるメッセージ部に、エラーメッセージと成功メッセージが表示されます。
削除	ネットワークは削除できます。 ファブリックのネットワークを削除するには、削除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、**[削除 (Delete)]** を選択します。同じインスタンスであれば、複数のネットワーク エントリを選択して削除できます。

アクション項目	説明
インターフェイス グループの追加	ネットワークはインターフェイスグループに追加できます。複数のネットワークエントリを選択し、それらを同じインスタンスのインターフェイス グループに追加できます。 選択したネットワークを必要なインターフェイスグループに追加するには、**[インターフェイス グループに追加 (Add to interface group)]** アクションをクリックします。 **[インターフェイス グループに追加 (Add to interface group)]** ウィンドウでネットワークのリンクをクリックし、選択したネットワークが **[選択したネットワーク (Selected Networks)]** ウィンドウに存在していることを確認して、ウィンドウを閉じます。ドロップダウン リストからインターフェイス グループを選択するか、**[新しいインターフェース グループの作成 (Create new interface group)]** をクリックします。 **[新しいインターフェース グループの作成 (Create new interface group)]** ウィンドウで、インターフェイス グループの名前を入力し、インターフェイス タイプを選択し、**[保存 (Save)]** をクリックして変更を保存し、ウィンドウを閉じます。または **[キャンセル (Cancel)]** をクリックして変更を破棄します。 **[インターフェイス グループに追加 (Add to interface group)]** ウィンドウで、**[保存 (Save)]** をクリックして変更を保存し、ウィンドウを閉じます。または **[キャンセル (Cancel)]** をクリックして変更を破棄します。 インターフェイス グループは、**[ネットワーク (Networks)]** タブ (**[ファブリックの概要 (Fabric Overview)]** ウィンドウ) の列に表示されます。

アクション項目	説明
インターフェイス グループからの削除	ネットワークはインターフェイスグループから削除できます。同じインスタンスの1つのインターフェイスグループから複数のネットワークエントリを選択し、削除できます。 選択したネットワークをインターフェイスグループから削除するには、**[インターフェイス グループから削除 (Remove from interface group)]** アクションをクリックします。 **[インターフェイス グループから削除 (Remove from interface group)]** ウィンドウでネットワークのリンクをクリックし、選択したネットワークが **[選択したネットワーク (Selected Networks)]** ウィンドウに存在していることを確認して、ウィンドウを閉じます。 **[インターフェイス グループから削除 (Remove from interface group)]** ウィンドウで、**[削除 (Remove)]** をクリックしてネットワークをインターフェイスグループから削除し、ウィンドウを閉じます。または **[キャンセル (Cancel)]** をクリックして変更を破棄します。 インターフェイス グループは、**[ネットワーク (Networks)]** タブ (**[ファブリックの概要 (Fabric Overview)]** ウィンドウ) の列から削除されます。

表 *6:* ネットワーク 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	ネットワークのレイヤ 2 VNI を指定します。
[VRF名（VRF Name）]	仮想ルーティングおよびフォワーディング（VRF）の名前を指定します。
IPv4 ゲートウェイ/サフィックス（IPv4 Gateway/Suffix）	IPv4 アドレスとサブネットを指定します。
IPv6 ゲートウェイ/サフィックス（IPv6 Gateway/Suffix）	IPv6 アドレスとサブネットを指定します。
ネットワークステータス	ネットワークのステータスを表示します。
VLAN ID	VLAN ID を指定します。
インターフェイス グループ	インターフェイス グループを指定します。

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

Cisco Nexusダッシュボード ファブリック コントローラ Web UI を使用してネットワークを作成するには、次の手順を実行します。

始める前に

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、レイヤ2を選択した場合は、VRFは必要ありません。VRFの詳細については、VRF（185 ページ）を参照してください。

手順

ステップ1 **[アクション (Actions)]** をクリックし、**[作成 (Create)]** を選択します。

[ネットワークの作成 (Create Network)] ウィンドウが表示されます。

ステップ2 必須のフィールドに必要な詳細情報を入力します。使用可能なフィールドは、ファブリック タイプによって若干異なります。

このウィンドウのフィールドは次のとおりです。

[ネットワーク ID (Network ID)] と **[ネットワーク名 (Network Name)]**：ネットワークのレイヤ 2 VNI と名前を指定します。ネットワーク名には、アンダースコア（_）とハイフン（-）以外の空白や特殊文字は使用できません。対応するレイヤ 3 VNI（またはVRF VNI）は、VRF の作成時に生成されます。

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

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

VRF が作成されていない場合、このフィールドは空白になります。新しい VRF を作成する場合は、**[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)]：ユニバーサル テンプレートが自動入力されます。これはリーフ スイッチにのみ適用されます。

[ネットワーク拡張テンプレート (Network Extension Template)]：ユニバーサル拡張テンプレートが自動入力されます。これにより、このネットワークを別のファブリックに拡張できます。メソッドは VRF Lite、Multi Site などです。このテンプレートは、境界リーフ スイッチおよびBGW に適用できます。

[マルチキャスト IP の生成 (Generate Multicast IP)]：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は、**[マルチキャスト IP の生成 (Generate Multicast IP)]** をクリックします。

ネットワーク プロファイルのセクションには、**[一般 (General)]** タブと **[詳細 (Advanced)]** タブがあります。

a) **[一般 (General)]** タブには以下のフィールドがあります。

（注） 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 Gateway/NetMask)]：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 アドレスを設定した場合、Nexusダッシュボード ファブリック コントローラ はエラーを表示しないので、この設定は保存できます。

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 Gateway/Prefix List) ：IPv6 アドレスとサブネットを指定します。

[VLAN 名 (Vlan Name)]：VLAN 名を入力します。

[インターフェイスの説明 (Interface Description)]：インターフェイスの説明を指定します。このインターフェイスはスイッチの仮想インターフェイス（SVI）です。

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

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

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

[IPv4 セカンダリ GW3 (IPv4 Secondary 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 (IPv4 Secondary 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。

b) **[詳細 (Advanced)]** タブをクリックすると、オプションとして、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。

[ARP 抑制 (ARP Suppression)]：ARP 抑制機能を有効にするには、このチェックボックスをオンにします。

[入力レプリケーション (Ingress Replication)]：レプリケーション モードが入力レプリケーションの場合、チェックボックスはオンになります。

（注） 入力レプリケーションは、**[詳細 (Advanced)]** タブの読み取り専用オプションです。ファブリック設定を変更すると、このフィールドは更新されます。

[マルチキャスト グループ アドレス (Multicast Group Address)]：ネットワークのマルチキャスト IP アドレスが自動入力されます。

マルチキャスト グループ アドレスは、ファブリック インスタンスごとの変数です。サポートされるアンダーレイ マルチキャスト グループの数は 128 に限られます。すべてのネットワークがすべてのスイッチに展開されている場合は、L2 VNI またはネットワークごとに異なるマルチキャスト グループを使用する必要はありません。したがって、ファブリック内のすべてのネットワークのマルチキャスト グループは同じままです。新しいマルチキャスト グループ アドレスが必要な場合は、**[マルチキャスト IP の生成 (Generate Multicast IP)]**ボタンをクリックして生成できます。

[DHCPv4 サーバー 1 (DHCPv4 Server 1)]：最初の DHCP サーバーの DHCP リレー IP アドレスを入力します。

[DHCPv4 サーバー VRF (DHCPv4 Server VRF)]：DHCP サーバーの VRF ID を入力します。

[DHCPv4 サーバー 2 (DHCPv4 Server 2)]：次の DHCP サーバーの DHCP リレー IP アドレスを入力します。

[DHCPv4 Server2 VRF]：DHCP サーバーの VRF ID を入力します。

[DHCPv4 サーバー 3 (DHCPv4 Server 3)]：次の DHCP サーバーの DHCP リレー IP アドレスを入力します。

[DHCPv4 Server3 VRF]：DHCP サーバーの 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 (Loopback ID for DHCP Relay interface) (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 (Routing Tag)]：ルーティングタグは自動入力されます。このタグは、各ゲートウェイの IP アドレス プレフィックスに関連付けられます。

[TRM が有効 (TRM enable)]：TRM を有効にするには、このチェックボックスをオンにします。

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

[L2 VNI ルート ターゲットの両方が有効 (L2 VNI Route Target Both Enable)]：すべての L2 仮想ネットワークのルート ターゲットの自動インポートとエクスポートを有効にするには、このチェックボックスをオンにします。

[Netflow の有効化（Enable Netflow）]：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。

[インターフェイス Vlan Netflow モニター（Interface Vlan Netflow Monitor）]：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 モニターを指定します。これは、**[レイヤ 2 レコード（Is Layer 2 Record）]** がファブリックの **[Netflow レコード（Netflow Record）]** で有効になっていない場合にのみ適用されます。

[Vlan Netflow モニター（Vlan Netflow Monitor）]：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。

[ボーダーの L3 ゲートウェイを有効にする (Enable L3 Gateway on Border)]：ボーダー スイッチでレイヤ 3 ゲートウェイを有効にするには、このチェックボックスをオンにします。

ステップ 3 [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

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、簡易ファブリック、および MSD ファブリックにのみ適用されます。

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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）][ネットワーク接続（Network Attachments）]を選択します。＞＞
- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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などの接続をネットワークに接続します。

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 [ネットワーク接続（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。

表 *7:* 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ID、テンプレート、説明、PTIオペレーション、作成済み構成、エンティティ名およびタイプ、作成日、シリアル番号、ユーザ、およびポリシーのソースなど、ポリシー変更履歴の詳細を表示できます。 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。また、**[詳細履歴（Detailed History）]** リンク（**[コマンド（Commands）]** 列、**[展開履歴（Deployment History）]** タブ）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、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、[編集（Edit）] アクションを選択します。[ネットワーク接続の編集（Edit Network Attachment）] ウィンドウで、必要な値を編集し、ネットワーク接続を接続または切断し、[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するか、[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）] 水平タブのテーブルに表示されます。

アクション項目	説明
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。 （注） このアクションは展開済みまたはNAステータスである接続向けに許可されません。 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、[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。 （注） このアクションは展開済みまたはNAステータスである接続向けに許可されません。 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、[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、詳細を確認できます。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。[導入（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が[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。

アクション項目	説明
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）]**をクリックして**[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。 ネットワーク接続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。Nexusダッシュボード ファブリック コントローラ からの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。ファイル名には、ファイルがエクスポートされた日時が付加されます。3.
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。 （注） 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。 ネットワークにすばやく接続するには、[クイック接続（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。

アクション項目	説明
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。 ネットワークからすばやく切断するには、[クイック切断（Quick Detach）] アクションを選択します。切断アクションが正常に行われたことを示すメッセージが表示されます。

表 *8:* 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	スイッチ名を指定します。
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、Easy Fabric IOS XE 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。

履歴

[履歴（History）] タブには、展開およびポリシーの変更履歴に関する情報が表示されます。**[LAN] > [ファブリック（Fabrics）]** を選択します。ファブリック名をダブルクリックして **[ファブリックの概要（Fabric Overview）]** ウィンドウを開き、**[履歴（History）]** タブをクリックします。

展開履歴の表示

選択したサービス ポリシーまたはルート ピアリングに関係するスイッチおよびネットワークの展開履歴が、[展開履歴（Deployment History）] タブに表示されます。展開履歴は、Nexusダッシュボード ファブリック コントローラからスイッチにプッシュまたは展開された変更をキャプチャします。展開履歴は、Nexusダッシュボードファブリック コントローラからスイッチにプッシュまたは展開された変更をキャプチャします。

次の表で、このページに表示されるフィールドを説明します。

フィールド	説明
ホスト名（シリアル番号）	ホスト名を指定します。
エンティティ名	エンティティ名を指定します。
エンティティ タイプ（Entity Type）	エンティティ タイプを指定します。
送信元	送信元を指定します。
コマンド	コマンドを指定します。
ステータス	ホストのステータスを指定します。
ステータスの説明	ステータスの説明を指定します。
ユーザ	ユーザを指定します。
完了までの時間	展開のタイムスタンプを指定します。

ポリシー変更履歴の表示

異なるユーザは、Nexusダッシュボード ファブリック コントローラ でスイッチの予期される設定を同時に変更できます。**[ポリシー変更履歴（Policy Change History）]** タブでポリシー変更の履歴を表示できます。

次の表で、このページに表示されるフィールドを説明します。

フィールド	説明
ポリシー ID	ポリシー ID を指定します。
テンプレート	使用するテンプレートを指定します。
説明	説明を指定します。
PTI の動作	ポリシー テンプレート インスタンス（PTI）を指定します。

フィールド	説明
生成された設定	設定履歴を指定します。**[詳細履歴（Detailed History）]** をクリックして、設定履歴を表示します。
エンティティ名	エンティティ名を指定します。
エンティティ タイプ（Entity Type）	エンティティ タイプを指定します。
作成日	ポリシーが作成された日付を指定します。
優先度	プライオリティ値を指定します。
シリアル番号	シリアル番号を指定します。
コンテンツ タイプ	コンテンツ タイプを指定します。
ユーザ	ユーザを指定します。
送信元	送信元を指定します。

リソース

Cisco Nexusダッシュボード ファブリック コントローラ では、リソースを管理できます。次の表で、このページに表示されるフィールドを説明します。

フィールド	説明
スコープタイプ	リソースが管理される範囲レベルを指定します。範囲タイプは、**ファブリック（Fabric）**、**デバイス（Device）**、**デバイス インターフェイス（Device Interface）**、**デバイス ペア（Device Pair）**、および **リンク（Link）** です。
範囲	リソース使用範囲を指定します。有効な値は、スイッチのシリアル番号またはファブリック名です。シリアル番号を持つリソースは一意であり、スイッチのシリアル番号でのみ使用できます。
デバイス名（Device Name）	デバイス名を指定します。
デバイス IP	デバイスの IP アドレスを指定します。
リソースの割り当て	リソースをデバイス、デバイス インターフェイス、またはファブリックで管理するかどうかを指定します。有効な値は、ID タイプ、サブネット、または IP アドレスです。
割り当て先	リソースが割り当てられるエンティティ名を指定します。

フィールド	説明
[リソース タイプ（Resource Type)]	リソース タイプを指定します。有効な値は、**TOP_DOWN_VRF_LAN**、**TOP_DOWN_NETWORK_VLAN**、**LOOPBACK_ID**、**VPC_ID** などです。
割り当てされましたか？	リソースが割り当てられているかどうかを指定します。リソースが特定のエンティティに永続的に割り当てられている場合、値は **True** に設定されます。リソースがエンティティに予約されており、永続的に割り当てられていない場合、値は **False** に設定されます。
割り当て日時	リソース割り当ての日時を指定します。
ID	ID を指定します。

リソースの割り当て

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からリソースを割り当てるには、次の手順を実行します。

手順

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

ステップ 2 ファブリック名をダブルクリックします。

[ファブリックの概要（Fabric Overview）] ウィンドウが表示されます。

ステップ 3 [リソース（Resources）] タブをクリックします。

ステップ 4 **[アクション（Actions）]> [リソースの割り当て（Allocate Resource）]** をクリックして、リソースを割り当てます。

[**リソースの割り当て（Allocate Resource**）] ウィンドウが表示されます。

ステップ 5 ドロップダウン リストからプール タイプ、プール名、およびスコープ タイプを適宜選択します。

プール タイプのオプションは、**ID_POOL**、**SUBNET_POOL**、および **IP_POOL** です。選択したプールタイプに基づいて、**[プール名（Pool Name）]** ドロップダウン リストの値が変更されます。

ステップ 6 **[エンティティ名（Entity Name）]** フィールドにエンティティ名を入力します。

組み込みヘルプには、さまざまなスコープ タイプの名前の例が示されています。

ステップ 7 **[リソース（Resource）]** フィールドに ID、IP アドレス、またはサブネットを入力します。ステップ *3* で選択したプール タイプに従う必要があります。

ステップ 8 **[保存（Save）]** をクリックしてリソースを割り当てます。

リソース割り当ての例

例 1：IP を loopback 0 と loopback 1 に割り当てる

```
#loopback 0 and 1
    L0_1: #BL-3
        pool_type: IP
        pool_name: LOOPBACK0_IP_POOL
        scope_type: Device Interface
        serial_number: BL-3(FDO2045073G)
        entity_name: FDO2045073G~loopback0
        resource : 10.7.0.1


    # L1_1: #BL-3
    #     pool_type: IP
    #     pool_name: LOOPBACK1_IP_POOL
    #     scope_type: Device Interface
    #     serial_number: BL-3(FDO2045073G)
    #     entity_name: FDO2045073G~loopback1
    #     resource : 10.8.0.3
```

例 2：サブネットの割り当て

```
#Link subnet
    Link0_1:
        pool_type: SUBNET
        pool_name: SUBNET
        scope_type: Link
        serial_number: F3-LEAF(FDO21440AS4)
        entity_name: FDO21440AS4~Ethernet1/1~FDO21510YPL~Ethernet1/3
        resource : 10.9.0.0/30
```

例 3：IP をインターフェイスに割り当てる

```
    #Interface IP
    INT1_1: #BL-3
        pool_type: IP
        pool_name: 10.9.0.8/30
        scope_type: Device Interface
        serial_number: BL-3(FDO2045073G)
        entity_name: FDO2045073G~Ethernet1/17
        resource : 10.9.0.9
```

例 4：エニーキャスト IP の割り当て

```
    #ANY CAST IP
    ANYCAST_IP:
        pool_type: IP
        pool_name: ANYCAST_RP_IP_POOL
        scope_type: Fabric
        entity_name: ANYCAST_RP
        resource : 10.253.253.1
```

例 5：ループバック ID の割り当て

```
    #LOOPBACK ID
```

```
LID0_1: #BL-3
    pool_type: ID
    pool_name: LOOPBACK_ID
    scope_type: Device
    serial_number: BL-3(FDO2045073G)
    entity_name: loopback0
    resource : 0
```

リソースの解放

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からリソースを解放するには、次の手順を実行します。

手順

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

ステップ 2 ファブリック名をダブルクリックします。

[ファブリックの概要（Fabric Overview）] ウィンドウが表示されます。

ステップ 3 [リソース（Resources）] タブをクリックします。

ステップ 4 削除するリソースを選択します。

（注） 複数のリソースを選択すると、複数のリソースを同時に削除できます。

ステップ 5 **[アクション（Actions）] [リソースの解放（Release(s)）]** をクリックして、リソースを解放します。

確認用のダイアログボックスが表示されます。

ステップ 6 **[確認（Confirm）]** をクリックして、リソースを解放します。

ホスト

Note このタブは、Nexus Dashboard ファブリック コントローラに IPFM を展開している場合にのみ、IPFM ファブリックで使用できます。

Nexusダッシュボード ファブリック コントローラUI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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）]**> **[ホスト（Hosts）]**を選択します。

ホストに関する情報は、**[ファブリックの概要（Fabric Overview）]** ウィンドウの **[概要（Overview）]** タブにもカードとして表示されます。これらのポリシーの詳細については、[ホスト（Hosts）], on page 166 を参照してください。

[ホスト（Hosts）] タブには次のタブが含まれます。

検出されたホストの概要

Nexusダッシュボード ファブリック コントローラUI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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)]** > **[ホスト (Hosts)]** > **[検出されたホストのサマリ (Discovered Hosts Summary)]**を選択します。
- **[LAN]** > **[ファブリック (Fabrics)]**を選択します。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)]** > **[ホスト (Hosts)]** > **[検出されたホストのサマリ (Discovered Hosts Summary)]**を開きます。

このウィンドウには、テレメトリによって入力されたすべてのホストのサマリを表示できます。

***Table 9: [検出されたホストのサマリ (Discovered Hosts Summary)]* テーブルのフィールドと説明**

フィールド	説明
VRF	ホストの VRF を指定します。
Host	ホストの IP アドレスを指定します。
[送信者/受信者 (Senders/Receivers)]	ホストデバイスが送信者または受信者としての役割を果たす回数を指定します。使用した場所を表示するには、カウントをクリックします。

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。

検出されたホスト

Nexusダッシュボード ファブリック コントローラUI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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。**[ファブリック概要（Fabric Overview）]** > **[ホスト（Hosts）]** > **[検出済みホスト（Discovered Hosts）]**を選択します。
- **[LAN]** > **[ファブリック (Fabrics)]**を選択します。ファブリックをダブルクリックして、**[ファブリック概要（Fabric Overview）]** > **[ホスト（Hosts）]** > **[検出済みホスト（Discovered Hosts）]**を開きます。

この画面には、テレメトリによって入力されたすべてのホストを表示できます。スイッチが検出されると、ファブリック内のすべてのスイッチがテレメトリを使用して定期的にNexusダッシュボード ファブリック コントローラ サーバにデータをプッシュします。シスコ Nexusダッシュボード ファブリック コントローラ サーバは、アクティブなフローごとに受信したイベントとフローの統計情報を表示します。

Table 10: 検出されたホスト テーブルのフィールドと説明

フィールド	説明
VRF	ホストの VRF を指定します。
Host	ホストの IP アドレスを指定します。
職務	ホストデバイスのロールを指定します。ホストのロールは次のいずれかになります。 • 送信者 • 外部送信者 • ダイナミック レシーバ • 外部レシーバ • スタティック レシーバ
マルチキャスト グループ	ホストが参加するフローのマルチキャストアドレスを指定します。
ソース言語	検出されたホストが参加するフローの送信元を指定します。
スイッチ	スイッチの名前を示します。
インターフェイス	送信側または受信側スイッチでホストが接続されているインターフェイスを指定します。
MAC アドレス	物理ホストの MAC アドレスを指定します（スイッチにそのホストの ARP エントリがある場合）。
ホスト検出時間	スイッチがホストを検出した日時を指定します。
障害の理由（Fault Reason）	検出されたホストが参加しているフローの失敗理由を指定します。

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。

ホスト ポリシー

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。ファブリック名をクリックして、**[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）]** > **[ホスト（Hosts）]** > **[ホスト ポリシー（Host Policies）]**を選択します。
- **[LAN]** > **[ファブリック (Fabrics)]**を選択します。ファブリック名をダブルクリックして、[ファブリックの概要（Fabric Overview）] [ホスト（Hosts）] [ホスト ポリシー（Host Policies）] を開きます。 > >

ホスト デバイスにポリシーを追加できます。[ホスト ポリシー（Host Policies）] に移動して、ホスト ポリシーを設定します。

（注） スイッチは、デフォルトのホスト ポリシーを使用して展開する必要があります。デフォルトのホスト ポリシーを編集して、許可または拒否することができます。[展開（Deployment）] ドロップダウンリストから、[選択したポリシーの展開（Deploy Selected Policies）] を選択して、デフォルト ポリシーをスイッチに展開します。また、デフォルト ポリシーを選択しなくても、[すべてのデフォルト ポリシーを展開（Deploy All Default Policies）] を選択することで、すべてのデフォルト ポリシーをすべての管理対象スイッチに展開できます。

デフォルトでは、ポリシーのシーケンス番号はによって自動生成され、マルチキャスト マスク/プレフィックスは /32 として取得されます。Nexusダッシュボード ファブリック コントローラシーケンス番号とマルチキャスト マスク/プレフィックスに必要な値を適切なフィールドに入力する場合は、[設定（Settings）] [サーバ設定（Server Settings）] [IPFM（IPFM）] タブの [ホスト ポリシーのマルチキャスト範囲のマスク/プレフィックスの有効化（Enable mask/prefix for the Host Policy）] チェックボックスがオンになっていることを確認します。次に、[ホスト ポリシー（Host Policies）] ウィンドウの [アクション（Actions）] ドロップダウンリストで使用可能な [ホスト ポリシーの作成（Create Host Policy）] および [ホスト ポリシーの編集（Edit Host Policy）] オプションの適切なフィールドに、シーケンス番号とマルチキャスト マスク/プレフィックスを入力できます。

スイッチにカスタム ホスト ポリシーを展開する前に、デフォルトのホスト ポリシーをスイッチに正しく展開する必要があります。そうしなかった場合、カスタムポリシーの展開に失敗します。カスタムポリシーを作成、編集、インポート、または展開する前に、すべてのスイッチにすべてのデフォルト ポリシーが正常に展開されていることを確認します。

（注） ユーザがネットワーク オペレータ ロールでNexusダッシュボード ファブリック コントローラにログインすると、ポリシーを作成、削除、編集、インポート、エクスポート、または展開するためのすべてのボタンまたはオプションが無効になります。このユーザはポリシー、展開ステータスまたは履歴を確認することのみ、可能です。

ポリシーが作成、編集、またはインポートされるたびに、ポリシーは自動的にスイッチに展開されます。ポリシーの横にある1つ以上のチェックボックスを選択し、[アクション（Actions）] ドロップダウンリストで適切なアクションを選択することで、ポリシーの展開または再展開を選択できます。ポリシーが展開された間にデバイスが再起動した場合、ポリシーは正常に展開されません。このような場合、[ホスト ポリシー（Host Policies）] ウィンドウの [展開ステータス（Deployment Status）] 列に [失敗（Failed）] メッセージが表示されます。

（注） カスタムまたはデフォルト以外の VRF を作成した場合、ホストおよびフロー ポリシーは VRF に対して自動的に作成されますが、このウィンドウのアクション オプションを使用して、ファブリック内のスイッチにホスト ポリシーを手動で展開します。

次の表で、[ホスト ポリシー（Host Policies）] ウィンドウに表示される [アクション（Actions）] ドロップダウンリストのアクション項目について説明します。

表 *11* : ホスト ポリシーのアクションと説明

アクション項目	説明
ホスト ポリシーの作成	新しいホスト ポリシーを作成できます。ホスト ポリシーの作成手順については、を参照してください。 ホスト ポリシーの作成 （223 ページ）
ホスト ポリシーの編集	選択したホスト ポリシー パラメータを表示または編集できます。 ホストポリシーを編集するには、削除するホストポリシーの横にあるチェックボックスをオンにして、[ホスト ポリシーの編集（Edit Host Policy）] を選択します。[ホスト ポリシーの編集（Edit Host Policy）] ウィンドウで、必要な値を編集し、[保存と展開（Save & Deploy）] をクリックしてポリシーを設定および展開するか、[キャンセル（Cancel）] をクリックしてホストポリシーを破棄します。編集したホスト ポリシーが [ホスト ポリシー（Host Policies）] ウィンドウのテーブルに表示されます。 （注） ホスト ポリシーに加えられた変更はすぐに適用されます。ポリシーがすでにデバイスに適用されている場合、変更が既存のフローに影響する可能性があります。

アクション項目	説明
ホストポリシーの削除	ユーザ定義のホスト ポリシーを削除できます。 （注） • ポリシーを削除する前に、すべてのスイッチからポリシーを展開解除します。Nexusダッシュボード ファブリック コントローラ • デフォルト ポリシーは、展開先のスイッチから展開解除できます。ただし、カスタム ポリシーは削除および展開解除できます。 • デフォルト ポリシーを展開解除すると、すべてのデフォルト ポリシーがデフォルトの権限（[許可（Allow）]）にリセットされます。 ホストポリシーを削除するには、削除するホストポリシーの横にあるチェックボックスをオンにし、[ホストポリシーの削除（Delete Host Policy）] を選択します。複数のホストポリシーエントリを選択し、同じインスタンスで削除できます。 ページの下部に、ホストポリシーの削除に成功したことを示すメッセージが表示されます。
消去	ポリシーチェックボックスを選択せずに、すべてのカスタム ポリシーを削除できます。 （注） • ポリシーを削除する前に、すべてのスイッチからポリシーを展開解除します。Nexusダッシュボード ファブリック コントローラ • デフォルトポリシーを展開解除できますが、デフォルト ポリシーは削除できません。カスタム ポリシーのみを削除および展開解除できます。

アクション項目	説明
インポート	ホスト ポリシーを CSV ファイルからにインポートできます。Nexusダッシュボード ファブリック コントローラ （注） インポート後、CSV ファイルからインポートされたすべてのポリシーは、すべての管理対象スイッチに自動的に適用されます。 ホスト ポリシー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、ホストポリシー設定情報を含む .csv ファイルを選択します。.csv ファイル内のフォーマットが正しくない場合、ポリシーはインポートされません。[開く（Open）] をクリックします。インポートされたポリシーは、ファブリック内のすべてのスイッチに自動的に展開されます。
エクスポート	ホストポリシーをNexusダッシュボードファブリック コントローラから .csv ファイルにエクスポートできます。 ホスト ポリシーをエクスポートするには、[エクスポート（Export）] を選択します。ホスト システムの詳細ファイル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ます。**[Save（保存）]** をクリックします。ホストポリシー 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。ファイル名には、ファイルがエクスポートされた日付が付加されます。エクスポート済みファイルのフォーマットは .csv です。
選択したポリシーの展開	選択したポリシーのみをスイッチに展開するには、このオプションを選択します。
すべてのカスタム ポリシーの展開	すべてのカスタムポリシーまたはユーザ定義ポリシーを単一インスタンスのスイッチに展開するには、このオプションを選択します。スイッチの再起動時にポリシーが展開されると、展開は失敗し、失敗ステータスメッセージが表示されます。
すべてのデフォルト ポリシーの展開	すべてのデフォルトポリシーをスイッチに展開するには、このオプションを選択します。
選択したポリシーの展開解除	選択したポリシーの展開解除をするにはこのオプションを選択します。 ポリシー名の横にある複数のチェックボックスを選択します。ドロップダウンリストからこのオプションを選択して、選択したポリシーの展開解除をします。

アクション項目	説明
すべてのカスタム ポリシーの展開解除	1 つのインスタンスですべてのカスタム ポリシーまたはユーザ定義ポリシーを展開解除するには、このオプションを選択します。
すべてのデフォルト ポリシーの展開解除	デフォルト ポリシーを展開解除するには、このオプションを選択します。
すべての失敗したポリシーのやり直し	ポリシーの展開は、さまざまな理由で失敗することがあります。失敗したすべてのポリシーを展開または展開解除するには、このオプションを選択します。 以前にスイッチで失敗したすべての展開は、それらのスイッチにのみ再度展開されます。以前スイッチの展開解除が失敗した場合、同じスイッチからのみ再度展開解除ができます。

アクション項目	説明
導入履歴	ドロップダウンリストから1つのポリシーを選択します。[展開履歴（Deployment History）] ペインで選択したポリシーの展開履歴を表示するには、このオプションを選択します。 ポリシー名が [ポリシー名（Policy Name）] フィールドに表示されます。ドロップダウンリストから、このポリシーが展開されたスイッチを選択します。 [展開履歴（Deployment History）] ペインには、次のフィールドが表示されます。 • ポリシー名：選択したポリシー名を指定します。 • VRF：選択したポリシーに VRF を指定します。 • スイッチ名：ポリシーの展開先のスイッチの名前を指定します。 • 展開ステータス：展開のステータスを表示します。展開が成功、失敗、または展開されなかった場合、表示されます。さらに詳細を確認するには、たとえば、展開ステータス **[成功（Success）]** をクリックします。展開ステータスについて詳細は、展開ステータス（222ページ）を参照してください。 • [アクション（Action）]：そのホストポリシーのスイッチで実行されるアクションを指定します。[作成（Create）] は、ポリシーがスイッチに展開されていることを意味します。[削除（Delete）] は、ポリシーがスイッチから展開解除されたことを意味します。 • 展開の日時：ホストポリシーが直近でアップデートされた日時を指定します。日時の表示形式は *Day MMM DD YYYY HH:MM:SS* タイムゾーン（*Timezone*） です。 • 失敗理由（Failed Reason）：ポリシーが正常に展開されなかった理由を示します。

表 *12*：ホスト ポリシー テーブルのフィールドと説明

フィールド	説明
VRF	ホストの VRF を指定します。[展開（Deployment）]、[展開解除（Undeployment）]、[ステータス（Status）]、および [履歴（History）] フィールドは、VRF に基づいています。
ポリシー名	ユーザの定義に従って、ホストのポリシー名を指定します。

フィールド	説明
レシーバ	受信側デバイスの IP アドレスを指定します。
マルチキャスト IP/マスク	ホストのマルチキャスト IP アドレスを指定します。
送信者	転送するデバイスの IP アドレスを指定します。
[ホストロール（Host Role）]	ホストデバイス ロールを指定します。ホストデバイス ロールは、次のいずれかです。 • **Sender** • **受信者** • **[受信者 - 外部（Receiver-External）]** • **[受信者 - ローカル（Receiver-Local）]**
オペレーション	ホスト ポリシーの動作かどうかを指定します。ポリシーには次の操作があります。 • **Permit** • **拒否**
シーケンス番号	マルチキャスト範囲が選択されている場合のカスタム ポリシーのシーケンス番号を指定します。
展開アクション（Deployment Action）	ホスト ポリシーのスイッチで実行されるアクションを指定します。 • **[作成（Create）]**：ポリシーがスイッチに展開されました。 • **[削除（Delete）]**：ポリシーがスイッチから展開解除されました。
展開ステータス	展開が成功したか、失敗したか、またはポリシーが展開されていないかを指定します。
最終更新日	ホスト ポリシーが最後に更新された日時を指定します。 日時の表示形式は *Day MMM DD YYYY HH:MM:SS* タイムゾーン（*Timezone*） です。

展開ステータス

次のテーブルは、展開ステータスで表示されるフィールドを説明しています。

表 *13 :* 展開ステータス フィールドおよび説明

フィールド	説明
ポリシー名	ホスト ポリシーの名前を指定します。
VRF	VRF の名前を指定します。
スイッチ名	VRF が展開されるスイッチを指定します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。
展開ステータス	展開のステータスを表示します。展開が**[成功（Success）]** または **[失敗（Failed）]** した場合、展開の失敗理由と共に、表示されます。
アクション	スイッチで実行されるアクション、たとえば **[作成（Create）]**、を指定します。
展開の日時	展開が初期化される日時を表示します。

この項の内容は、次のとおりです。

ホスト ポリシーの作成

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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）]** > **[ホスト（Hosts）]** > **[ホスト ポリシー（Host Policies）]**を選択します。
- **[LAN]** > **[ファブリック (Fabrics)]**を選択します。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）]** > **[ホスト（Hosts）]** > **[ホスト ポリシー（Host Policies）]** を開きます。

スイッチにカスタム ホスト ポリシーを展開する前に、デフォルトのホスト ポリシーをスイッチに正しく展開する必要があります。そうしなかった場合、カスタム ポリシーの展開に失敗します。カスタム ポリシーを追加する前に、すべてのスイッチにすべてのデフォルト ポリシーが正しく展開されていることを確認します。

Cisco Nexusダッシュボード ファブリック コントローラ からホスト ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 **[ホスト ポリシー（Host Policies）]** ウィンドウで、**[アクション（Actions）]** ドロップダウンリストから **[ホスト ポリシーの作成（Create Host Policy）]** を選択します。

ステップ 2 **[ホスト ポリシーの作成（Create Host Policy）]** ウィンドウで、次のフィールドにパラメータを指定します。

- **[VRF]**：**[VRF の選択 (Select a VRF)]** リンクをクリックして、**[VRF の選択 (Select a VRF)]** ウィンドウを開きます。デフォルトの VRF もウィンドウに表示されます。ホストの VRF を検索して選択し、**[保存 (Save)]** をクリックします。

  （注）
  - ポリシー名は VRF 間で繰り返すことができます。つまり、VRF 内でのみ一意なものとなります。
  - VRF 全体で、ホスト ポリシーは同じでも異なっていてもかまいません。

- **ポリシー名**：ホスト ポリシーの一意のポリシー名を指定します。
- **ホスト ロール**：ホストをマルチキャスト送信者または受信者として指定します。次のいずれかを選択します。
  - 送信者
  - 受信者 - ローカル（Receiver-Local）
  - 受信者 - 外部（Receiver-External）
- **送信者ホスト名（Sender Host Name）**：ポリシーが適用される送信者ホストを指定します。

  （注） リモート送信者として検出されたホストは、送信者ホストポリシーの作成に使用できます。

- **送信者 IP**：ホストの送信側の IP アドレスを指定します。このフィールドに *****（アスタリスク）記号または **0.0.0.0** を指定すると、この IP アドレスにワイルドカードを指定できます。
- **受信者ホスト名**：ポリシーが適用される受信者ホストを指定します。宛先ホストが検出された場合は、ドロップダウン リストからホスト名を選択できます。

  （注） 受信者または送信者のホストポリシーを作成するために、リモート受信者として検出されたホストを選択しないでください。ただし、リモート送信者として検出されたホストは、送信者ホスト ポリシーの作成に使用できます。

- **受信者 IP**：受信者ホストの IP アドレスを指定します。このフィールドは表示され、[ホスト ロール（Host Role）] が **[Receiver-Local]** に設定されている場合にのみ適用されます。このフィールドに *****（アスタリスク）記号または **0.0.0.0** を指定すると、この IP アドレスにワイルドカードを指定できます。

  （注） 受信者ホストポリシーの**受信者 IP**がワイルドカード（*****または**0.0.0.0**）の場合、**送信者 IP** もワイルドカード（***** または **0.0.0.0**）である必要があります。

- **マルチキャスト**：ホストポリシーのマルチキャストIPアドレスを指定します。このフィールドに*****（アスタリスク）記号を指定すると、このIPアドレスにワイルドカードを指定できます。これは **224.0.0.0/4** に変換されます。**[送信者IP（Sender IP）]** フィールドと **[受信**

者IP（**Receiver IP**）**]** フィールドにワイルドカード IP アドレスを指定する場合、マルチキャスト グループは常に必要です。つまり、***** または **0.0.0.0**としてマルチキャストを指定することはできません。

- **[許可/拒否（Permit/Deny）]**：ポリシーでトラフィック フローを許可する必要がある場合は、**[許可（Permit）]**をクリックします。ポリシーでトラフィック フローを許可しない場合は、**[拒否（Deny）]** をクリックします。

ステップ 3 **[保存して展開（Save＆Deploy）]**をクリックして、ポリシーを設定および展開します。**[キャンセル（Cancel）]** をクリックして新しいポリシーを破棄します。ウィンドウの一番下に、展開が完了したとのメッセージが,表示されます。ウィンドウの現在の展開ステータスを更新するには **[更新 (Refresh)]** をクリックします。導入の詳細を確認するには **[詳細の表示 (View Details)]** をクリックします。

ホスト エイリアス

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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）]** > **[ホスト（Hosts）]** > **[ホスト エイリアス（Host Alias）]**を選択します。
- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。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）]**>**[ホスト（Hosts）]**>**[ホスト エイリアス（Host Alias）]**を開きます。

Note このセクションは Nexusダッシュボード ファブリック コントローラ の IPFM モードおよび全般マルチキャスト モード、両方に適用が可能です。

Cisco Nexusダッシュボードファブリック コントローラでは、IPFM ファブリックの送信者ホストと受信者ホストのホスト エイリアスを作成できます。アクティブなマルチキャスト トラフィックの送受信デバイスは、ホストと呼ばれます。ホストエイリアス名を送信者と受信者のホストに追加すると、ホストを名前で識別しやすくなります。IPFM 展開を使用して、多数のホスト エイリアスを Cisco Nexusダッシュボード ファブリック コントローラにインポートすることもできます。

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、**[ホスト エイリアス（Host Alias）]** ウィンドウに表示されるものです。

Table 14: ホスト エイリアスのアクションと説明

アクション項目	説明
ホスト エイリアスの作成	新しいホストエイリアスを作成できます。新しいホストエイリアスの作成手順については、を参照してください。ホストエイリアスの作成, on page 227
ホスト エイリアスの編集	選択したホストエイリアスパラメータを表示または編集できます。 ホストエイリアスを編集するには、削除するホストエイリアスの横にあるチェックボックスをオンにし、[ホストエイリアスの編集（Edit Host Alias）]を選択します。[ホスト エイリアスの編集（Edit Host Alias）] ウィンドウで必要な値を編集し、[送信（Submit）] をクリックして変更を適用するか、[キャンセル（Cancel）] をクリックしてホスト エイリアスを破棄します。編集したホスト エイリアスが [ホスト エイリアス（Host Alias）] ウィンドウのテーブルに表示されます。
ホスト エイリアスの削除	ホスト エイリアスを削除できます。 ホストエイリアスを削除するには、削除するホストエイリアスの横にあるチェックボックスをオンにして、[ホスト エイリアスの削除（Delete Host Alias）] を選択します。複数のホスト エイリアス エントリを選択し、同じインスタンスで削除できます。
インポート	ファブリック内のデバイスのホストエイリアスをインポートできます。 ホスト エイリアス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、ホストIPアドレスと対応する一意のホスト名情報を含む [.csv] ファイルを選択します。[開く（Open）]をクリックします。ホストエイリアスがインポートされ、[ホスト エイリアス（Host Alias）] ウィンドウに表示されます。
エクスポート	ファブリック内のデバイスのホストエイリアスをエクスポートできます。 ホスト エイリアスをエクスポートするには、[エクスポート（Export）] を選択します。ホストエイリアス設定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。Nexusダッシュボード ファブリック コントローラホスト エイリアス コンフィギュレーション 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。ファイル名には、ファイルがエクスポートされた日時が付加されます。エクスポートされるファイルの形式は `.csv` です。

Table 15: ホスト エイリアス テーブルのフィールドと説明

フィールド	説明
VRF	ホストの VRF を指定します。
ホスト エイリアス	ホストを識別するように設定されているホスト名を指定します。
IP アドレス	エイリアス名で参照するスイッチに接続するホストの IP アドレスを指定します。
最終更新日時	ホスト エイリアスが最後に更新された日時を指定します。

この項の内容は、次のとおりです。

ホスト エイリアスの作成

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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）]** > **[ホスト（Hosts）]** > **[ホスト エイリアス（Host Alias）]**を選択します。
- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。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）]** > **[ホスト（Hosts）]** > **[ホスト エイリアス（Host Alias）]**を開きます。

Cisco Nexusダッシュボード ファブリック コントローラ が検出したファブリック内のデバイスに新しいホスト エイリアスを作成するには、次のタスクを実行します。

Cisco Nexusダッシュボード ファブリック コントローラ からホスト エイリアスを作成するには、次の手順を実行します。

Procedure

ステップ 1 **[ホスト エイリアス（Host Alias）]** ウィンドウで、**[アクション（Actions）]** ドロップダウン リストから **[ホスト エイリアスの作成（Create Host Alias）]** を選択します。

ステップ 2 **[ホスト エイリアスの作成（Create Host Alias）]** ウィンドウで、以下を入力します。

Note すべてのフィールドが必須です。

- **[VRF]**：ドロップダウン リストから VRF を選択します。デフォルト値は **[デフォルト（default）]** です。

  Note ホストと IP アドレスは VRF ごとに一意です。つまり、同じ IP アドレスを持つ同じホスト名が複数の VRF に存在できます。

- **[ホスト名（Host Name）]**：識別用の完全修飾ホスト名を入力します。
- **[IP アドレス（IP Address）]**：フローの一部であるホストの IP アドレスを入力します。

Note また、ホストが、直接接続された送信側または受信側リーフにデータを送信する前に、ホスト エイリアスを作成することもできます。

ステップ 3 [送信（Submit）] をクリックして変更を適用します。

ホスト エイリアスを破棄するには、**[キャンセル（Cancel）]** をクリックします。

新しいホスト エイリアスが **[ホスト エイリアス（Host Alias）]** ウィンドウのテーブルに表示されます。

適用されたホスト ポリシー

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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）]** > **[ホスト（Hosts）]** > **[適用されたホスト ポリシー（Applied Host Policies）]**を選択します。
- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。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）]** > **[ホスト（Hosts）]** > **[適用されたホスト ポリシー（Host Policies）]**を開きます。

このタブでは、ネットワーク全体に適用したポリシーを表示できます。

テーブルには、デフォルトの PIM ポリシー、ローカル受信者ポリシー、および送信者ポリシーが表示されます。IPFM は、ユーザー定義の PIM ポリシーまたはレシーバ外部ポリシーを表示しません。

Table 16: 適用されるホスト ポリシー テーブルのフィールドと説明

列名	説明
VRF	ホストの VRF を指定します。
ポリシー名/シーケンス番号	適用されるポリシーの名前を示します。
[ホストロール（Host Role）]	ホスト ロールを指定します。 ホスト デバイス ロールは、次のいずれかです。 • **PIM** • **Sender** • **受信者**

列名	説明
スイッチ	ポリシーが適用されるスイッチの名前を指定します。
インターフェイス	ポリシーが適用されるインターフェイスを指定します。
アクティブ	ポリシーがアクティブかどうかを指定します。
タイム スタンプ	ポリシーが作成/展開された日時を指定します。 形式は Day, MMM DD YYYY HH:MM:SS（タイムゾーン）です。

[フロー（Flows）]

Note このタブは、Nexus Dashboard ファブリック コントローラに IPFM を展開している場合にのみ、IPFM ファブリックで使用できます。

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。ファブリックをクリックして **[ファブリック サマリ（Fabric Summary）]** スライドイン ペインを開きます。**[起動（Launch）]** アイコンをクリックします。**[ファブリックの概要（Fabric Overview）]**> **[ホスト（Hosts）]** を選択します。
- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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）]** > **[ホスト（Hosts）]**を開きます。

フローに関する情報は、**[ファブリックの概要（Fabric Overview）]** ウィンドウの **[概要（Overview）]** タブにもカードとして表示されます。これらのポリシーの詳細については、[フロー（Flows）], on page 166 を参照してください。

[フロー（Flows）] タブは、次の水平タブで構成されます。

Flow Status

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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)]** > **[ホスト (Hosts)]** > **[フロー ステータス (Flow Status)]**を選択します。

- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。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)]** > **[ホスト (Hosts)]** > **[フロー ステータス (Flow Status)]**を開きます。

（注） このセクションは、Nexusダッシュボード ファブリック コントローラ の IPFM と汎用マルチキャスト モードの両方に適用されます。

Cisco Nexusダッシュボード ファブリック コントローラ では、フローステータスを図的および統計的に表示できます。

汎用マルチキャスト モードでは、スイッチは受信者エンドポイントの IP アドレスではなく、受信者インターフェイスの IP アドレスを報告します。この IP は、**[フロー ステータス (Flow Status)]** および **[トポロジ (Topology)]** ウィンドウにホストとして表示されます。[送信者（Sender）] フィールドと [受信者（Receiver）] フィールドでは、IP の末尾に青いドットと **Remote** という単語が付いており、これらの IP がリモート ホストであることを示しています。また、トラフィックのポリシングがないため、スイッチは「許可されたバイト/パケット」のみを報告し、「拒否されたバイト/パケット」は報告しません。

リリース 12.1.1e から、NAT タイプ「Egress」は ENAT に、NAT タイプ「Ingress」は INAT に名前が変更されました。Cisco NDFC は、**[フロー ステータス（Flow Status）]** テーブルで NAT の方向も示します。

- **MUNAT**：出力インターフェイスでのマルチキャストトラフィックが受信側インターフェイスでユニキャスト トラフィックに変換されることを示します。
- **UMNAT**：出力インターフェイスで受信したマルチキャスト トラフィックが送信側インターフェイスでユニキャスト トラフィックに変換されることを示します。

[受信者/送信者インターフェイス（Receiver/Sender Interface）] 列の **[ユニキャスト（Unicast）]** または **[マルチキャスト（Multicast）]** リンクをクリックして、このインターフェイスの IP ルート テーブルを表示します。

（注） すべてのプレ/ポスト マルチキャストおよび送信元 IP アドレス、ポスト グループ、ポスト S /DST ポート、プレ/ポスト NAT ポリシー ID、開始ノードと宛先ノードの詳細など、特定のフローの詳細をトポロジとともに表示するには、**アクティブ**なハイパーリンク（特定のマルチキャスト IP の **[フローリンク状態（Flow Link State）]** のもの）をクリックします。リリース 12.1.1e 以降、NAT インターフェイスの遷移タイプに関する詳細情報がテーブルに表示されます。

テーブルの右上にある **[テレメトリ同期ステータス（Telemetry Sync Status）]** リンクをクリックします。**[テレメトリ同期ステータス（Telemetry Sync Status）]** 画面には、同期ステータスと各スイッチの Telemetry コレクタの IP アドレス、および最後の同期のタイムスタンプが表示されます。Telemetry コレクタごとの負荷を表示するには、**Telemetry Collector == <<*IP Address***

of the collector>> フィルタを使用します。コレクタが現在処理しているフローに基づいて、コレクタのパフォーマンスのバランスをとることができます。

マルチキャスト NAT の可視化

Nexusダッシュボード ファブリック コントローラ は、マルチキャストフローの既存のフロー分類（アクティブ、非アクティブ、送信者のみ、または受信者のみ）に従います。入力および出力 NAT を複数使用すると、入力アドレスと出力アドレスを同じグループに変換できます。Nexusダッシュボード ファブリック コントローラ は送信者と受信者の組み合わせごとにこれらのフローを集約し、トポロジを通じて NAT ルールを可視化します。アクティブ フローのフロートポロジの詳細については、RTP/EDIフローモニタ （269ページ）を参照してください。

マルチキャスト NAT は IPFM ネットワークでサポートされます。通常のマルチキャストまたは汎用マルチキャストではサポートされません。

NATフローは、**[NAT検索 (NAT Search)]**フィールドを使用して検索できます。すべてのプレ/ポスト マルチキャストおよび送信元 IP アドレスは、**[フローステータス (Flow Status)]** ウィンドウには表示されません。アクティブなフロー ハイパーリンクをクリックすると、特定のフローの詳細をポップアップで表示できます。**NAT 検索**機能を使用すると、プレまたはポスト送信元/マルチキャスト グループの IP アドレスを入力し、関連するエントリをフィルタリングできます。検索された IP アドレスは、対応するポップアップ ウィンドウに表示されるプレまたはポストエントリの一部である可能性があるため、フィルタリングが適用されているメインテーブルに表示されない場合があります。

入力を含む NAT タイプの NAT フローの場合、送信元とグループは NAT 返還後の送信元および NAT 返還後のグループになります。出力を含む NAT タイプの場合、送信元とグループは NAT 変換前の送信元と NAT 変換前のグループになります。NAT ルールは、**[送信者のみ (Sender Only)]** タブと **[受信者のみ (Receiver Only)]** タブに表示されます。

NAT フローの場合、トポロジ グラフのパス トレースには、入力 NAT を持つスイッチ上の **NAT** バッジと、出力 NAT の受信者へのリンク上の **NAT** ラベルが表示されます。

NAT フローの場合、トポロジ グラフ パネルの下に、関連するすべての入力 NAT または出力 NAT 情報を示す追加のテーブルがあります。NATフロー情報は、**[トポロジ (Topology)]** ウィンドウでも確認できます。この情報は、**[フローリンク状態 (Flow Link State)]** 列のリンクをクリックすると表示されます。

VRF 名は、ホストとスイッチのスライドイン ペインにも表示されます。

たとえば、**sanjose-vrf**：**2.2.2.2** は、VRF が sanjose-vrf で、ホストが 2.2.2.2 であることを示します。

フローは、プレフィックスとして VRF 名を伝送します。VRF が**デフォルト**の場合、表示されません。

次の表に、NAT フィールドとその説明を示します。

表 *17 : NAT* フィールドと説明

フィールド	説明

NAT	NAT モード（入力、出力、または入力と出力）を示します。 入力 NAT タイプの場合、次の情報が表示されます。 入力 (S) (Ingress (S))：入力 NAT 変換が送信者スイッチ（ファーストホップルータ（FHR）とも呼ばれる）で実行されることを示します。 入力 (R) (Ingress (R))：入力 NAT 変換が受信者スイッチ（ラストホップルータ（LHR）とも呼ばれる）で実行されることを示します。 入力 (S、R) (Ingress (S, R))：入力 NAT 変換が送信者スイッチと受信者スイッチの両方で実行されることを示します。
プレソース（Pre-Source）	NAT 変換前の送信元 IP アドレスです。
ポストソース（Post-Source）	NAT 変換後の送信元 IP アドレスです。
プレグループ（Pre-Group）	NAT 変換前のマルチキャスト グループを示します。
ポストグループ（Post-Group）	NAT 変換後のマルチキャスト グループを示します。
ポスト S ポート（Post S Port）	NAT 変換後の送信元ポートを示します。
ポスト DST ポート（Post DST Port）	NAT 変換後の宛先ポートを示します。

次の表では、**[アクティブ (Active)]** タブのフィールドについて説明します。

表 *18 : [アクティブ (Active)]* タブのフィールドと説明

フィールド	説明
IPFM および汎用マルチキャスト モードの共通フィールド	
VRF	フローの VRF の名前を示します。
マルチキャストIP	フローのマルチキャスト IP アドレスを示します。 （注） [マルチキャスト IP アドレス (Multicast IP address)] の横にあるウェーブ リンクをクリックすると、フロー統計情報の図が表示されます。
フロー エイリアス (Flow Alias)	フロー エイリアスの名前を示します。

フロー リンク ステート (Flow Link State)	フロー リンクの状態を示します。 **アクティブ**なリンクをクリックすると、送信者と受信者のネットワーク図つまりトポロジが表示されます。 点線は、トラフィックのフローの方向を示します。情報を表示するには、ノードにカーソルを合わせます。右側のテーブルには、送信者と受信者に関する情報が表示されます。 ネットワーク図つまりトポロジのフローは、マルチキャスト IP と VRF を示します。VRF が**デフォルト**の場合、VRF はマルチキャスト IP とともに表示されません。
送信者	マルチキャスト グループの送信者の IP アドレスまたはホスト エイリアスを指定します。
NAT	フローが入力、出力、または入力と出力の両方であるかどうかを示します。
送信者スイッチ (Sender Switch)	送信者スイッチがリーフまたはスパインのいずれであるかを示します。
送信者インターフェイス (Sender Interface)	送信者が接続しているインターフェイスを示します。
受信者スイッチ (Receiver Switch)	受信者スイッチがリーフまたはスパインのいずれであるかを示します。
受信者インターフェイス（Receiving Interface）	受信者が接続しているインターフェイスを示します。
送信開始時間（Sender Start Time）	送信者が参加してからの時間を表示します。
受信者参加時間（Receiver Join Time）	受信者が参加した時刻を示します。
IPFM モードに固有のフィールド	
優先度	フローのフロー プライオリティを示します。
ポリシング (Policed)	フローがポリシーの対象とされるかどうかを示します。
レシーバ	グループに参加している受信者の IP アドレスまたはホスト エイリアスを示します。
帯域幅	トラフィックに割り当てられる帯域幅を示します。
QOS/DSCP	スイッチ定義の QoS ポリシーを示します。
ポリシー ID	マルチキャスト IP に適用されるポリシー ID を示します。
汎用マルチキャスト モード固有のフィールド	

受信者インターフェイス	グループに参加している受信者インターフェイスの IP アドレス示します。

次の表では、**[非アクティブ (Inactive)]** タブのフィールドについて説明します。

表 *19 : [非アクティブ (Inactive)]* タブのフィールドと説明

フィールド	説明
IPFM および汎用マルチキャスト モードの共通フィールド	
VRF	フローの VRF の名前を示します。
マルチキャストIP	フローのマルチキャスト IP アドレスを示します。 （注） マルチキャストIPアドレスの横にあるチャートリンクをクリックすると、フロー統計情報の図が表示されます。
フローエイリアス (Flow Alias)	フロー エイリアスの名前を示します。
NAT	フローが入力、出力、または入力と出力の両方であるかどうかを示します。
送信者	マルチキャスト グループの送信者の IP アドレスまたはホストエイリアスを指定します。
送信開始時間（Sender Start Time）	送信者が参加してからの時間を表示します。
受信者参加時間（Receiver Join Time）	受信者が参加した時刻を示します。
IPFM モードに固有のフィールド	
優先度	フローのフロー プライオリティを示します。
ポリシング (Policed)	フローがポリシーの対象とされるかどうかを示します。
レシーバ	グループに参加している受信者の IP アドレスまたはホスト エイリアスを示します。
帯域幅	トラフィックに割り当てられる帯域幅を示します。
QOS/DSCP	スイッチ定義の QoS ポリシーを示します。
ポリシー ID	マルチキャスト IP に適用されるポリシー ID を示します。

障害の理由（Fault Reason）	非アクティブ フローの理由を示します。 送信者と受信者の両方の mroute が次のいずれかの組み合わせで存在する場合、Cisco Nexusダッシュボード ファブリック コントローラ は非アクティブになるフローを決定します。 • 受信者 IIF がヌル • 受信者 OIF がヌル • 送信者 IIF がヌル • 送信者 OIF がヌル このシナリオでは、スイッチに障害の理由はありません。したがって、このような非アクティブ フローの障害理由はありません。
汎用マルチキャスト モード固有のフィールド	
受信者インターフェイス	グループに参加している受信者インターフェイスの IP アドレス示します。

次の表では、**[送信者のみ (Sender Only)]** タブのフィールドについて説明します。

表 *20 : [*送信者のみ *(Sender Only)]* タブのフィールドと説明

フィールド	説明
IPFM および汎用マルチキャスト モードの共通フィールド	
VRF	フローの VRF の名前を示します。
マルチキャストIP	フローのマルチキャスト IP アドレスを示します。
フロー エイリアス (Flow Alias)	フロー エイリアスの名前を示します。
フロー リンク ステート (Flow Link State)	フロー リンクの状態（許可または拒否）を示します。 **senderonly** リンクをクリックすると、送信者と受信者のネットワーク図つまりトポロジが表示されます。 点線は、トラフィックのフローの方向を示します。情報を表示するには、ノードにカーソルを合わせます。右側のテーブルには、送信者と受信者に関する情報が表示されます。 ネットワーク図つまりトポロジのフローは、マルチキャスト IP と VRF を示します。VRF が**デフォルト**の場合、VRF はマルチキャスト IP とともに表示されません。
送信者	送信者の名前を示します。
NAT	フローが入力、出力、または入力と出力の両方であるかどうかを示します。

フィールド	説明
IPFM および汎用マルチキャスト モードの共通フィールド	
送信者スイッチ (Sender Switch)	送信者スイッチの IP アドレスを示します。
送信者入力インターフェイス（Sender Ingress Interface）	送信者入力インターフェイスの名前を示します。
送信開始時間（Sender Start Time）	送信者スイッチが情報を送信してからの時間を表示します。
IPFM モードに固有のフィールド	
ポリシング (Policed)	フローがポリシーの対象とされるかどうかを示します。
ポリシー ID	マルチキャスト IP に適用されるポリシー ID を示します。
帯域幅	トラフィックに割り当てられる帯域幅を示します。
QOS/DSCP	スイッチ定義の QoS ポリシーを示します。
優先度	フローのフロー プライオリティを示します。

次の表では、**[受信者のみ (Receiver Only)]** タブのフィールドについて説明します。

表 *21 : [*受信者のみ *(Receiver Only)]* タブのフィールドと説明

フィールド	説明
IPFM および汎用マルチキャスト モードの共通フィールド	
VRF	フローの VRF の名前を示します。
マルチキャストIP	フローのマルチキャスト IP アドレスを示します。
フロー エイリアス (Flow Alias)	フロー エイリアスの名前を示します。
フロー リンク ステート (Flow Link State)	フロー リンクの状態（許可または拒否）を示します。 **receiveronly** リンクをクリックすると、送信者と受信者のネットワーク図つまりトポロジが表示されます。 点線は、トラフィックのフローの方向を示します。情報を表示するには、ノードにカーソルを合わせます。右側のテーブルには、送信者と受信者に関する情報が表示されます。 ネットワーク図つまりトポロジのフローは、マルチキャスト IP と VRF を示します。VRF が**デフォルト**の場合、VRF はマルチキャスト IP とともに表示されません。
送信元固有の送信者	マルチキャスト送信者の IP アドレスを示します。
レシーバ	受信者 ID を示します。マルチキャスト受信者がリモートの場合、**[リモート (Remote)]** ラベルがその名前の横に表示されます。

フィールド	説明
IPFM および汎用マルチキャスト モードの共通フィールド	
NAT	フローが入力、出力、または入力と出力の両方であるかどうかを示します。
受信者スイッチ (Receiver Switch)	受信者スイッチの IP アドレスを示します。
受信者インターフェイス（Receiving Interface）	宛先スイッチインターフェイスの名前を示します。
受信者参加時間（Receiver Join Time）	受信者が参加した時刻を示します。
IPFM モードに固有のフィールド	
帯域幅	トラフィックに割り当てられる帯域幅を示します。
ポリシー ID	マルチキャスト IP に適用されるポリシー ID を示します。
優先度	フローのフロー プライオリティを示します。
QOS/DSCP	スイッチ定義の QoS ポリシーを示します。

（注） スイッチで統計情報が有効になっている場合は、その統計情報のみがNexusダッシュボード ファブリック コントローラ に表示されます。

統計データをさまざまな形式で表示するには、統計表示領域の **[表示 (Show)]** ドロップダウンリストをクリックします。

統計データをエクスポートするには、矢印をクリックします。`.csv` または `.pdf` 形式でエクスポートできます。

（注） Cisco Nexusダッシュボード ファブリック コントローラ はフロー統計値を Nexusダッシュボードファブリック コントローラ サーバの内部メモリに保持します。したがって、Nexusダッシュボード ファブリック コントローラ の再起動または HA の切り替え後、フロー統計情報には以前に収集された値は表示されません。ただし、サーバの再起動または HA の切り替え後に収集されたフロー統計情報は表示できます。

Nexusダッシュボード ファブリック コントローラ で検出されたスイッチ間がアップリンクになる前に、新しいフローが参加すると、メッセージBW_UNAVAIL が表示されます。これは、デバイスの検出後にスイッチ間のアップリンクが Nexusダッシュボード ファブリック コントローラ により検出されると、解決されます。

フロー ポリシー

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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）]** > **[ホスト（Hosts）]** > **[フロー ポリシー（Flow Policies）]**を選択します。
- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。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）]** > **[ホスト（Hosts）]** > **[フロー ポシリー（Flow Policies）]** を開きます。

このウィンドウを使用して、フロー ポリシーを設定します。

（注） ユーザがネットワーク オペレータ ロールでNexusダッシュボード ファブリック コントローラにログインすると、ポリシーを追加、削除、変更、インポート、エクスポート、または展開するためのすべてのボタンまたはオプションが無効になります。このユーザはポリシー、展開ステータスまたは履歴を確認することのみ、可能です。

デフォルト ポリシーが [フロー ポリシー（Flow Policies）] タブに表示されます。デフォルトでは、これらのポリシーの帯域幅は 0 です。デフォルトのフロー ポリシーに一致するフローがそれに応じて帯域幅と QOS/DSCP パラメータを使用するように、帯域幅を設定できます。設定を保存すると、ポリシーがすべてのデバイスに展開されます。

（注） デフォルト ポリシーを展開解除すると、デフォルト値（Bandwidth:0gbps、DSCP:Best Effort、および Policer:Enabled）にリセットされます。

ポリシーは、作成、編集、またはインポートされるたびにスイッチに自動的に展開されます。[アクション（Actions）] ドロップダウンリストで適切なアクションを選択することで、ポリシーの展開または再展開を選択できます。ポリシーの展開中にデバイスが再起動された場合、ポリシーは正しく展開されません。この場合、[展開ステータス（Deployment Status）] 列に [失敗（Failed）] メッセージが表示されます。

スイッチにカスタム フロー ポリシーを展開する前に、デフォルトのフロー ポリシーをスイッチに正常に展開する必要があります。そうしなかった場合、カスタム ポリシーの展開に失敗します。カスタム ポリシーを追加、編集、インポート、または展開する前に、すべてのスイッチにすべてのデフォルト ポリシーが正常に展開されていることを確認します。

（注） カスタムまたはデフォルト以外の VRF を作成した場合、ホストおよびフロー ポリシーは VRF に対して自動的に作成されますが、このウィンドウのアクション オプションを使用して、ファブリック内のスイッチにフロー ポリシーを手動で展開します。

次の表で、このページに表示されるフィールドを説明します。

表 *22*: フロー ポリシー テーブルのフィールドと説明

フィールド	説明
VRF	フロー ポリシーの VRF の名前を示します。
ポリシー名	フロー ポシリー名を指定します。
マルチキャスト IP 範囲	トラフィックのマルチキャスト IP アドレスを指定します。[マルチキャスト範囲リスト（Multicast Range List）] ボックスに、マルチキャスト範囲の開始IPアドレスと終了IPアドレス、フロー優先度などの詳細を表示するには、[表示（View）] をクリックします。
帯域幅	トラフィックに割り当てられる帯域幅を示します。
QoS/DSCP	スイッチ定義の QoS ポリシーを示します。
展開アクション（Deployment Action）	ホスト ポリシーのスイッチで実行されるアクションを指定します。 • **[作成（Create）]**：ポリシーがスイッチに展開されました。 • **[削除（Delete）]**：ポリシーがスイッチから展開解除されました。
展開ステータス	フロー ポリシーが正常に展開されるか、展開されないか、または失敗するかを指定します。
使用中	フロー ポリシーが使用中かどうかを指定します。
Policer	フロー ポリシーを有効にするか無効にするかを指定します。 （注） フローポリシーの追加または編集では、デフォルトのポリサー状態は[有効（Enabled）] です。
最終更新日	フロー ポリシーが最後に更新された日時を指定します。 日時の表示形式は *Day MMM DD YYYY HH:MM:SS* タイムゾーン（*Timezone*） です。

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、[ファブリックの概要（Fabric Overview）] ウィンドウの [フロー（Flows）] タブの [フローポリシー（Flow Policies）] 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。

（注） 新しいフロー ポリシーまたは編集されたフロー ポリシーは、次の状況でのみ有効です。

- 新しいフローが既存のフロー ポリシーと一致する場合。
- フローが期限切れになり、新しいポリシーがすでに作成または編集されている場合、フロー ポリシーと一致します。

表 *23 :* フロー ポリシーのアクションと説明

フィールド	説明
フロー ポリシーの作成	新しいフローポリシーを作成できます。詳細については、フローポリシーの作成 （244 ページ）を参照してください。
フロー ポリシーの編集	選択したフロー ポリシー パラメータを表示または編集できます。 （注） スイッチにカスタム フロー ポリシーを展開する前に、デフォルトのフロー ポリシーをスイッチに正常に展開する必要があります。そうしなかった場合、カスタム ポリシーの展開に失敗します。カスタムポリシーを編集する前に、すべてのスイッチにすべてのデフォルトポリシーが正常に展開されていることを確認します。 VRF のフローポリシーを編集するには、VRF の横にあるチェックボックスをオンにして、[フロー ポリシーの編集（Edit Flow Policy）] アクションを選択します。[フロー ポリシーの編集（Edit Flow Policy）] ウィンドウで必要な変更を行い、[保存して展開（Save & Deploy）] をクリックして変更を展開するか、[キャンセル（Cancel）]をクリックして変更を破棄できます。 ウィンドウの一番下に、展開が完了したとのメッセージが,表示されます。ウィンドウの現在の展開ステータスを更新するには **[更新 (Refresh)]** をクリックします。導入の詳細を確認するには **[詳細の表示 (View Details)]** をクリックします。

フィールド	説明
フロー ポリシーの削除	ユーザ定義のフロー ポリシーを削除できます。 （注） • デフォルト フロー ポリシーは削除できません。 • ポリシーを削除する前に、すべてのスイッチからポリシーを展開解除します。Nexusダッシュボード ファブリック コントローラ • 削除するフロー ポリシーを複数選択できます。 フローポリシーを削除するには、VRFの横にあるチェックボックスをオンにして、[フロー ポリシーの削除（Delete Flow Policy）] アクションを選択します。スイッチからポリシーを展開解除するように求める警告メッセージが表示されます。[確認（Confirm）] をクリックして削除を続行し、ポリシーをスイッチに残します。または、[キャンセル（Cancel）] をクリックして削除操作を破棄します。
消去	単一のインスタンスですべてのフロー ポリシーを削除できます。 （注） ポリシーを削除する前に、すべてのスイッチからポリシーを展開解除します。Nexusダッシュボード ファブリック コントローラ すべてのフローポリシーを削除するには、[消去（Purge）]アクションを選択します。すべてのスイッチからポリシーを展開解除するように求める警告メッセージが表示されます。[確認（Confirm）]をクリックして削除を続行し、ポリシーをスイッチに残します。または、[キャンセル（Cancel）] をクリックして削除操作を破棄します。
インポート	csv ファイルからフロー ポリシーをインポートできます。 （注） スイッチにカスタム フロー ポリシーを展開する前に、デフォルトのフロー ポリシーをスイッチに正常に展開する必要があります。そうしなかった場合、カスタム ポリシーの展開に失敗します。カスタムポリシーをインポートする前に、すべてのスイッチにすべてのデフォルトポリシーが正常に展開されていることを確認します。 インポート後、csv ファイルからインポートされたすべてのポリシーは、すべての管理対象スイッチに自動的に適用されます。 フロー ポリシーをインポートするには、[インポート（Import）] アクションを選択します。ディレクトリを参照し、フロー ポリシー設定情報を含む .csv ファイルを選択します。.csv ファイル内のフォーマットが正しくない場合、ポリシーはインポートされません。[開く（Open）]をクリックします。インポートされたポリシーは、ファブリック内のすべてのスイッチに自動的に展開されます。

フィールド	説明
エクスポート	csv ファイルにフロー ポリシーをエクスポートできます。 フロー ポリシー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。フロー ポリシーの詳細ファイル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ます。**[Save（保存）]** をクリックします。フロー ポリシー 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。ファイル名には、ファイルがエクスポートされた日付が付加されます。エクスポート済みファイルのフォーマットは .csv です。
選択したポリシーの展開	選択したポリシーのみをデバイスに展開するには、このオプションを選択します。必要に応じて他のポリシーを展開できます。 ポリシー名の横にある複数のチェックボックスを選択します。選択したポリシーをスイッチに展開するには、このオプションを選択します。
すべてのカスタム ポリシーの展開	1 つのインスタンスですべてのカスタム ポリシーまたはユーザ定義ポリシーを展開するには、このオプションを選択します。 スイッチがリブートしている場合でも、ポリシーは展開されます。このような場合、展開は失敗し、[展開ステータス（Deployment Status）] 列に [失敗（Failed）] というステータス メッセージが表示されます。
すべてのデフォルト ポリシーの展開	すべてのデフォルト ポリシーをスイッチに展開するには、このオプションを選択します。
選択したポリシーの展開解除	選択したポリシーの展開解除をするにはこのオプションを選択します。 選択したポリシーを展開解除するには、VRF の横にある 1 つ以上のチェックボックスをオンにします。ドロップダウンリストからこのオプションを選択して、選択したポリシーの展開解除をします。
すべてのカスタム ポリシーの展開解除	1 つのインスタンスですべてのカスタム ポリシーまたはユーザ定義ポリシーを展開解除するには、このオプションを選択します。
すべてのデフォルト ポリシーの展開解除	単一のインスタンスですべてのデフォルトポリシーを展開解除するには、このオプションを選択します。
すべての失敗したポリシーのやり直し	ポリシーの展開または展開解除は、さまざまな理由で失敗することがあります。失敗したすべてのポリシーを展開するには、このオプションを選択します。 以前にスイッチで失敗したすべての展開は、それらのスイッチにのみ再度展開されます。以前スイッチの展開解除が失敗した場合、同じスイッチからのみ再度展開解除ができます。

フィールド	説明
導入履歴	[展開履歴（Deployment History）]ペインでスイッチ向けに選択したポリシーの展開履歴を表示するには、このオプションを選択します。 [展開履歴（Deployment History）] ペインには、次のフィールドが表示されます。 • ポリシー名：選択したポリシー名を指定します。 • VRF：選択したポリシーに VRF を指定します。 • スイッチ名：ポリシーの展開先のスイッチの名前を指定します。 • 展開ステータス：展開のステータスを表示します。展開が成功、失敗、または展開されなかった場合、表示されます。さらに詳細を確認するには、たとえば、展開ステータス **[成功（Success）]** をクリックします。展開ステータスについて詳細は、展開ステータス （243 ページ）を参照してください。 • [アクション（Action）]：そのフローポリシーのスイッチで実行されるアクションを指定します。 • 作成：ポリシーがスイッチに展開されていることを示します。 • 削除：ポリシーがスイッチから展開解除されたことを示します。 • 展開の日時：ホスト ポリシーが直近でアップデートされた日時を指定します。日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。 • 失敗理由（Failed Reason） ：ポリシーが正常に展開されなかった理由を示します。

展開ステータス

次のテーブルは、展開ステータスで表示されるフィールドを説明しています。

表 *24 :* 展開ステータス フィールドおよび説明

フィールド	説明
ポリシー名	フロー ポリシーの名前を示します。
VRF	VRF の名前を指定します。
スイッチ名	VRF が展開されるスイッチを指定します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。

フィールド	説明
展開ステータス	展開のステータスを表示します。展開が **[成功（Success）]** または **[失敗（Failed）]** した場合、展開の失敗理由と共に、表示されます。
アクション	スイッチで実行されるアクション、たとえば **[作成（Create）]**、を指定します。
展開の日時	展開が初期化される日時を表示します。

この項の内容は、次のとおりです。

フロー ポリシーの作成

（注） スイッチにカスタム ホスト ポリシーを展開する前に、デフォルトのホスト ポリシーをスイッチに正しく展開する必要があります。そうしなかった場合、カスタム ポリシーの展開に失敗します。カスタムポリシーを追加する前に、すべてのスイッチにすべてのデフォルト ポリシーが正しく展開されていることを確認します。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI を使用してフロー ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 **[アクション (Actions)]** をクリックし、**[フロー ポリシーの作成 (Create Flow Policy)]** を選択します。

[フロー ポリシーの作成 (Create Flow Policy)] ウィンドウが開きます。

ステップ 2 **[フロー ポリシーの作成 (Create Flow Policy)]** ウィンドウで、次のフィールドにパラメータを指定します。

- **[VRF]**：**[VRF の選択 (Select a VRF)]** リンクをクリックして、**[VRF の選択 (Select a VRF)]** ウィンドウを開きます。デフォルトの VRF もウィンドウに表示されます。ホストの VRF を検索して選択し、**[保存 (Save)]** をクリックします。

  （注）
  - ポリシー名は VRF 間で繰り返すことができます。つまり、VRF 内でのみ一意なものとなります。
  - VRF 全体で、ホスト ポリシーは同じでも異なっていてもかまいません。
  - ホスト ポリシーのシーケンス番号は VRF 単位です。

- **[ポリシー名 (Policy Name)]**：フロー ポリシーの一意のポリシー名を指定します。

- **[帯域幅 (Bandwidth)]**：フロー ポリシーに割り当てられる帯域幅を指定します。オプションボタンで、**[Gbps]**、**[Mbps]**、または **[Kbps]** を選択します。

ステップ 3 **[QoS/DSCP]** ドロップダウンリストから、適切な ENUM 値を選択します。

ステップ 4 フローのポリサーを有効または無効にするには、**[ポリサー (Policer)]** チェックボックスをオンにします。

ステップ 5 **[マルチキャスト IP 範囲 (Multicast IP Range)]** の **[開始 (From)]** および **[終了 (To)]** フィールドに、マルチキャスト範囲の開始 IP と 終了 IP のアドレスを入力します。有効な範囲は 224.0.0.0 ～ 239.255.255.255 です。

[フロー プライオリティ (Flow Priority)] ドロップダウン リストから、ポリシーのプライオリティを選択します。**[デフォルト (Default)]** または **[クリティカル (Critical)]** を選択できます。デフォルト値は **[デフォルト (Default)]** です。

フロー プライオリティは、次のシナリオで使用されます。

- エラー リカバリ：ユニキャスト ルーティング情報ベース（URIB）の到達可能性がフローに基づいて変更され、Re-Reverse-Path Forwarding（RPF）が実行されます。既存のフローのセットを再試行すると、**クリティカル (Critical)** プライオリティのフローからリカバリが開始されます。
- **[フローの再試行 (Flow Retry)]**：保留中のフローを再試行すると、クリティカル プライオリティのフローが最初に再試行されます。

[アクション (Action)]：アクションには、さまざまなアクションを実行するためのさまざまなアイコンがあります。正しい詳細を入力した場合は、目盛りのアイコンをクリックします。そうでない場合は、チェックマークのアイコンをクリックして、マルチキャストの範囲をポリシーに追加します。詳細を変更する場合は編集のアイコンをクリックします。行を削除する場合は、ビンのアイコンをクリックして行を削除します。別の行を追加するには、プラス (+) マークをクリックします。

ステップ 6 **[保存して展開 (Save & Deploy)]** をクリックして新しいポリシーを展開するか、**[キャンセル (Cancel)]** をクリックして変更を破棄します。ウィンドウの一番下に、展開が完了したとのメッセージが,表示されます。ウィンドウの現在の展開ステータスを更新するには **[更新 (Refresh)]** をクリックします。導入の詳細を確認するには **[詳細の表示 (View Details)]** をクリックします。

フロー エイリアス (Flow Alias)

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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）]** > **[フロー（Flows）]** > **[フロー エイリアス（Flow Alias）]**を選択します。

- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。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）]** > **[フロー（Flows）]** > **[フロー エイリアス（Flow Alias）]** を開きます。

このタブを使用して、フロー エイリアスを設定します。

（注） このセクションは、Nexusダッシュボード ファブリック コントローラ の IPFM と汎用マルチキャスト モードの両方に適用されます。

フロー エイリアス機能を使用して、マルチキャスト グループの名前を指定できます。マルチキャスト IP アドレスは覚えにくいため、マルチキャスト IP アドレスに名前を割り当てることで、名前に基づいてポリシーを検索および追加できます。

次の表で、この ウィンドウに表示されるフィールドについて説明します。

表 *25 :* フロー エイリアス テーブルのフィールドと説明

フィールド	説明
VRF	フローエイリアスの VRF を指定します。
ポリシー名	ポリシー名を指定します。
マルチキャスト IP 範囲	トラフィックのマルチキャスト IP アドレスを指定します。
説明	フロー エイリアスに追加された説明です。
最終更新日	フロー エイリアスが最後に更新された日付を示します

次の表では、**[アクション（Actions）]** ドロップダウン リストのアクション項目について説明します。これらは **[フロー エイリアス（Flow Alias）]** 水平タブに表示されるもので、**[フロー（Flows）]** タブ（**ファブリックの概要（Fabric Overview）]** ウィンドウ）にあります。

表 *26 :* フロー エイリアスのアクションと説明

アクション項目	説明
フロー エイリアスの作成	新しいフローエイリアスを作成できます。新しいフローエイリアスの作成手順については、フローエイリアスの作成（248 ページ）を参照してください。

アクション項目	説明
フロー エイリアスの編集	選択したフローエイリアスは、パラメータを表示または編集することができます。 フロー エイリアスを編集するには、削除するフロー エイリアスの横にあるチェックボックスをオンにし、**[フローエイリアスの編集（Edit Flow Alias）]** を選択します。**[フローエイリアスの編集（Edit Flow Alias）]** ウィンドウで、必要な値を編集し、**[送信（Submit）]** 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、フローエイリアスを破棄します。編集したフローエイリアスが **[フロー エイリアス（Flow Alias）]** ウィンドウのテーブルに表示されます。
フロー エイリアスの削除	フロー エイリアスは削除できます。 フローエイリアスを削除するには、削除するフローエイリアスの横にあるチェックボックスをオンにし、**[フロー エイリアスの削除（Delete Flow Alias）]** を選択します。複数のフローエイリアスエントリを選択して、同じインスタンスで削除することができます。
インポート	ファブリック内のデバイスのフローエイリアスはインポートできます。 フロー エイリアス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、フロー IP アドレスと対応する一意のフロー名情報を含む `.csv` ファイルを選択します。[開く（Open）] をクリックします。フロー エイリアスがインポートされ、**[フロー エイリアス（Flow Alias）]** ウィンドウに表示されます。
エクスポート	ファブリック内のデバイスのフロー エイリアスはエクスポートできます。 フロー エイリアスをエクスポートするには、**[エクスポート（Export）]** を選択します。フロー エイリアス設定を保存するローカルシステムディレクトリの場所をNexusダッシュボードファブリック コントローラから選択し、**[保存（Save）]** をクリックします。フロー エイリアスの設定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。ファイル名には、ファイルがエクスポートされた日時が付加されます。エクスポートされるファイルの形式は `.csv` です。

この項の内容は、次のとおりです。

フロー エイリアスの作成

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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）]** > **[フロー（Flows）]** > **[フロー エイリアス（Flow Alias）]**を選択します。
- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。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）]** > **[フロー（Flows）]** > **[フロー エイリアス（Flow Alias）]** を開きます。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI を使用してフロー エイリアスを作成するには、次の手順を実行します。

手順

ステップ 1 **[フロー エイリアス（Flow Alias）]** ウィンドウで、**[アクション（Actions）]** ドロップダウン リストから **[フロー エイリアスの作成（Create Flow Alias）]** を選択します。

ステップ 2 **[フロー エイリアスの作成（Create Flow Alias）]** ウィンドウで、以下を入力します。

（注） すべてのフィールドが必須です。

- **[VRF]**：ドロップダウン リストから VRF を選択します。デフォルト値は **[デフォルト（default）]** です。

  （注） ホストと IP アドレスは VRF ごとに一意です。つまり、同じ IP アドレスを持つ同じホスト名が複数の VRF に存在できます。

- **[フロー名（Flow Name）]**：フロー エイリアスを識別するための一意の完全修飾フロー名を入力します。
- **[マルチキャスト IP アドレス（Multicast IP Address）]**：フロー エイリアスのマルチキャスト IP アドレスを入力します。
- **[説明（Description）]**：フロー エイリアスの説明を入力します。

ステップ 3 [送信（Submit）] をクリックして変更を適用します。

フロー エイリアスを破棄するには、**[キャンセル（Cancel）]** をクリックします。

新しいフロー エイリアスが **[フロー エイリアス（Flow Alias）]** ウィンドウのテーブルに表示されます。

スタティック フロー

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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）]** > **[ホスト（Hosts）]** > **[スタティック フロー（Static Flow）]**を選択します。
- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。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）]** > **[ホスト（Hosts）]** > **[スタティック フロー（Static Flow）]**を開きます。

[スタティックフロー（Static Flow）] ウィンドウを使用してスタティック受信機を設定します。スタティック フローを作成する前に、**[オプションの選択（Select an Option）]** フィールドを使用してスイッチを選択します。

表 *27*：スタティック フロー アクションと説明

フィールド	説明
スタティック フローの作成	スタティックフローを作成できます。詳細については、スタティック フローの作成 （250 ページ）を参照してください。
スタティック フローの削除	スタティック フローを削除できます。 削除する必要があるスタティックフローを選択し、**[スタティックフローの削除（Delete Static Flow）]** アクションをクリックして、選択したスタティック フローを削除します。

表 *28*：スタティック フロー テーブルのフィールドと説明

フィールド	説明
VRF	スタティック フローの VRF を指定します。
グループ	スタティック フローのグループを指定します。
ソース言語	スタティック フローの送信元 IP アドレスを指定します。
[インターフェイス名（Interface Name）]	スタティック フローのインターフェイス名を指定します。スタティックフローの作成時に指定されていない場合は、**[N/A]** と表示されます。
展開アクション（Deployment Action）	ルールのスイッチで実行されるアクションを指定します。[作成（Create）]は、スタティック フローがスイッチに展開されたことを意味します。[Delete（削除）]は、スタティック フローがスイッチから展開解除されたことを意味します。
展開ステータス	スタティック フローが展開されているかどうかを示します。展開に失敗した場合は、情報アイコンにカーソルを合わせると、失敗の理由が表示されます。

フィールド	説明
最終更新日	スタティック フローが最後に更新された日時を示します。 日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。

スタティック フローの作成

選択したスイッチのスタティック フローを作成するには、次の手順を実行します。

始める前に

[ファブリック概要（Fabric Overview）] ウィンドウの **[スタティック フロー（Static Flow）]** タブでスイッチを選択してから、そのスイッチのスタティック フローを作成します。

手順

ステップ 1 **[アクション（Actions）]** をクリックし、**[スタティック フローの作成（Create Static Flow）]** を選択します。

[スタティック フローの作成（Create Static Flow）] ウィンドウが表示されます。

ステップ 2 **[スタティック フローの作成（Create Static Flow）]** ウィンドウで、次のフィールドにパラメータを指定します。

[スイッチ（Switch）]：スイッチ名を指定します。このフィールドは読み取り専用で、**[スタティック フロー（Static Flow）]** ウィンドウで選択されたスイッチに基づいています。

[グループ（Group）]：マルチキャスト グループを指定します。

[送信元（Source）]：送信元の IP アドレスを指定します。

[インターフェイス名（Interface Name）]：スタティック フローのインターフェイス名を指定します。このフィールドは任意です。インターフェイス名を指定しない場合、ホスト IP 0.0.0.0 が API に渡され、Null0 インターフェイスを使用して設定が作成されます。

ステップ 3 **[保存して展開（Save & Deploy）]** をクリックして、スタティック フローを保存します。

[キャンセル（Cancel）] をクリックして破棄します。

メトリック

[メトリック (Metric)] タブには、インフラストラクチャの正常性とステータスが表示されます。CPU 使用率、メモリ使用率、トラフィック、温度、インターフェイス、およびリンクの詳細を表示できます。

次の表では、**[CPU]** および **[メモリ (Memory)]** タブでの列の表示について説明します。

フィールド	説明
スイッチ名	スイッチの名前を指定します。
IP アドレス	スイッチの IP アドレスを指定します。
最小値 (Low Value (%))	スイッチの最小 CPU 使用率の値を示します。
平均値 (Avg. Value (%))	スイッチの平均 CPU 使用率の値を示します。
最大値 (High Value (%))	スイッチの最大 CPU 使用率の値を示します。
範囲プレビュー (Range Preview)	線形範囲のプレビューを示します。
前回の更新時刻	スイッチが最後に更新された日時を表示します。
最終日の表示 (Show last day)	**[最終日の表示 (Show last day)]** をクリックすると、選択した日、週、月、年のデータが表示され ます。

次の表では、**[トラフィック (Traffic)]** タブに表示される列について説明します。

フィールド	説明
スイッチ名	スイッチの名前を指定します。
平均Rx	平均 Rx 値を示します。
ピーク Rx (Peak Rx)	ピーク Rx 値を示します。
平均Tx	平均 Tx 値を示します。
ピーク Tx (Peak Tx)	ピーク Tx 値を示します。
平均Rx+Tx	Rx および Tx 値の平均を示します。
平均Errors	平均エラー値を示します。
ピーク エラー (Peak Errors)	ピーク エラー値を示します。
平均破棄	平均廃棄値を示します。
ピーク廃棄 (Peak Discards)	ピーク廃棄値を示します。
前回の更新時刻	最後に更新された日時を示します。
最終日の表示 (Show last day)	**[最終日の表示 (Show last day)]** をクリックすると、選択した日、週、月、年のデータが表示され ます。

次の表では、**[温度 (Temperature)]**タブに表示される列について説明します。

フィールド	説明
スイッチ名	スイッチの名前を指定します。
IP アドレス	平均 Rx 値を指します。

フィールド	説明
モジュール温度 (Temperature Module)	ピーク Rx 値を指します。
最低値 (Low Value (C))	最低温度の値を示します。
平均値 (Avg. Value (C))	平均温度の値を示します。
最高値 (High Value (C))	最高温度の値を示します。
最終日の表示 (Show last day)	**[最終日の表示 (Show last day)]** をクリックすると、選択した日、週、月、年のデータが表示され ます。

次の表では、**[インターフェイス (Interface)]** タブに表示される列について説明します。

フィールド	説明
スイッチ	スイッチの名前を示します。
インターフェイス	インターフェイスの名前を示します。
説明	インターフェイスの説明を示します。
スピード	インターフェイスの速度を示します。
ステータス	スイッチのリンクのステータスを示します。
受信	
平均	平均 Rx 値を示します。
平均% (Avg%)	Rx 値の平均パーセンテージを示します。
ピーク	ピーク Rx 値を示します。
ピーク % (Peak%)	ピークの Rx 値をパーセンテージで示します。
送信	
平均	平均 Tx 値を示します。
平均% (Avg%)	Tx 値の平均パーセンテージを示します。
ピーク	ピーク Tx 値を示します。
ピーク % (Peak%)	ピークの Tx 値をパーセンテージで示します。
Rx+Tx	Rx と Tx の合計値を示します。
エラー（Errors）	
入力平均 (In Avg.)	入力平均エラー値を示します。
出力平均 (Out Avg.)	出力ピーク エラー値を示します。
入力ピーク (In Peak)	入力ピーク エラー値を示します。
出力ピーク	出力ピーク エラー値を示します。

フィールド	説明
Discards	
入力平均 (In Avg.)	平均廃棄値を示します。
出力平均 (Out Avg.)	平均廃棄値を示します。
入力ピーク (In Peak)	入力ピーク廃棄値を示します。
出力ピーク (Out Peak)	出力ピーク廃棄値を示します。
最終日の表示 (Show last day)	**[最終日の表示 (Show last day)]** をクリックすると、選択した日、週、月、年のデータが表示され ます。

次の表では、**[リンク (Link)]** タブに表示される列について説明します。

フィールド	説明
スイッチ	スイッチの名前を示します。
VLAN	VLAN 名を指定します。
スピード	スイッチの速度を示します。
ステータス	スイッチのリンクのステータスを示します。
スピード	インターフェイスの速度を示します。
受信	
平均	平均 Rx 値を示します。
平均% (Avg%)	Rx 値の平均パーセンテージを示します。
ピーク	ピーク Rx 値を示します。
ピーク % (Peak%)	ピークの Rx 値をパーセンテージで示します。
送信	
平均	平均 Tx 値を示します。
平均% (Avg%)	Tx 値の平均パーセンテージを示します。
ピーク	ピーク Tx 値を示します。
ピーク % (Peak%)	ピークの Tx 値をパーセンテージで示します。
Rx+Tx	Rx と Tx の合計値を示します。
エラー（Errors）	
入力平均 (In Avg.)	入力平均エラー値を示します。
出力平均 (Out Avg.)	出力ピーク エラー値を示します。
入力ピーク (In Peak)	入力ピーク エラー値を示します。

フィールド	説明
出力ピーク	出力ピーク エラー値を示します。
Discards	
入力平均 (In Avg.)	平均廃棄値を示します。
出力平均 (Out Avg.)	平均廃棄値を示します。
入力ピーク (In Peak)	入力ピーク廃棄値を示します。
出力ピーク (Out Peak)	出力ピーク廃棄値を示します。
最終日の表示 (Show last day)	**[最終日の表示 (Show last day)]** をクリックすると、選択した日、週、月、年のデータが表示され ます。

マルチキャスト NAT

UDP ストリームのマルチキャスト NAT 変換は、Nexusダッシュボード ファブリック コントローラ IPFM モードでサポートされます。着信トラフィック（入力）、または出力リンクまたはインターフェイスに NAT を適用できます。入力 NAT の範囲はスイッチ全体ですが、出力 NAT は特定のインターフェイス用です。同じスイッチに入力 NAT と出力 NAT の両方を設定できます。ただし、特定のスイッチの同じフロー上に存在することはできません。出力 NAT には、同じフローを最大 40 回複製する機能があります。この機能を実現するために、スイッチにサービス反映インターフェイスが定義されています。複数または単一の出力ポートに使用されます。

（注） 入力および/または出力NAT変換は、送信者スイッチ（ファーストホップルータ（FHR）とも呼ばれる）と受信者スイッチ（ラスト ホップ ルータ（LHR）とも呼ばれる）でのみサポートされます。スパイン スイッチなどの中間ノードではサポートされません。

NAT について詳細は、『*Cisco Nexus 9000* シリーズ *NX-OS IP Fabric for Media* ソリューションガイド』を参照してください。

前提条件

- PIM スパース モードでループバック インターフェイスを設定します。フローが変換される場合、RPFチェックが失敗しないように、変換後の送信元はこのループバックのセカンダリ IP アドレスである必要があります。このループバックは、NAT 用のサービス反映インターフェイスとして構成されます。VRF ごとにルックバックを設定する必要があります。

  ループバック インターフェイスを構成する例を次に示します。

```
interface loopback10
ip router ospf 1 area 0
ip pim sparse-mode
ip address 192.168.1.1/32
```

```
ip address 172.16.1.10/32 secondary

ip service-reflect source-interface loopback10
```

- TCAM メモリ カービングを完了する必要があります。

  マルチキャスト NAT 用に TCAM を構成するコマンドは、次のとおりです。

  ```
  hardware access-list tcam region mcast-nat tcam-size
  ```

  マルチキャスト NAT をサポートするスイッチ モデルについては、『Cisco Nexus 9000 シリーズ NX-OS IP fabric for Media ソリューション ガイドの 』の「NBM でマルチキャスト サービス リフレクションを構成する 」を参照してください。

NAT モード

NAT モード オブジェクトは、スイッチおよび VRF ごとに作成されます。スイッチは、範囲に基づいてドロップダウンに入力されます。一覧表示するスイッチを選択し、対応する NAT モード オブジェクトを操作する必要があります。

[LAN] > [ファブリック（Fabrics）] を選択します。NATモードを設定するには、ファブリック名をダブルクリックし、[Multicast NAT]> [NAT Modes]をクリックします。

次の表では、**[NAT Modes（NAT モード）]** タブに表示されるフィールドについて説明します。

フィールド	説明
VRF	マルチキャストNATのVRFを指定します。VRFサポートはeNATには適用されませんが、iNATには適用されます。
グループ	NAT モードのマルチキャスト アドレスを指定します。
モード	入力または出力マルチキャスト NAT モードを指定します。
展開アクション（Deployment Action）	モードのスイッチで実行されるアクションを指定します。作成は、モードがスイッチで展開されていることを意味します。削除は、モードがスイッチから展開解除されていることを意味します。
展開ステータス	モードが展開されているか否かを指定します。展開に失敗した場合は、情報アイコンにカーソルを合わせて失敗の理由を表示します。
最終更新日	モードが最後に更新された日時を指定します。 日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。

次の表に、[NATモード（NAT Modes）]タブに表示されるアクションメニュードロップダウンリストのアクション項目を示します。

アクション項目	説明
NATモードの作成	NATモードを追加するには、[Create NAT Mode]を選択します。

アクション項目	説明
NATモードの削除	テーブルからモードを選択し、[Delete NAT Mode]を選択してモードを削除します。
インポート	CSVファイルからにNATモードをインポートできます。Nexusダッシュボード ファブリック コントローラ
エクスポート	NATモードをからCSVファイルにエクスポートできます。Nexusダッシュボードファブリック コントローラ
選択したNATモードの展開	テーブルからモードを選択し、[Deploy Selected NAT Modes]を選択して、選択したモードをスイッチに展開します。
すべてのNATモードの展開	[Deploy All NAT Modes]を選択して、すべてのモードをスイッチに展開します。
選択したNATモードの展開解除	テーブルからモードを選択し、[選択したNATモードの展開解除（Undeploy Selected NAT Modes）]を選択して、選択したモードをスイッチから展開解除します。
すべてのNATモードの展開解除	[Undeploy All NAT Modes]を選択して、スイッチからすべてのモードを展開解除します。
すべての失敗したNATモードをやり直す	失敗したすべてのモードを展開するには、[Redo All Failed NAT Modes]を選択します。

アクション項目	説明
導入履歴	テーブルからモードを選択し、[Deployment History]を選択して、選択したモードの展開履歴を表示します。 [展開履歴（Deployment History）] には、次のフィールドが表示されます。 • スイッチ名：モードが展開されたスイッチの名前を指定します。 • VRF：モードが展開されたVRFの名前を指定します。 • Group：NATモードのマルチキャストグループを指定します。 • Mode：NATモード（入力または出力）を指定します。 • 展開ステータス：展開のステータスを表示します。導入が成功したか失敗したかが表示されます。 • アクション：モードのスイッチで実行されるアクションを指定します。作成は、モードがスイッチで展開されていることを意味します。削除は、モードがスイッチから展開解除されていることを意味します。 • 展開日時：モードが最後に更新された日時を指定します。日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。 • 失敗理由：モードが正常に展開されなかった理由を示します。

NAT モードの追加

手順

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

ステップ 2 ファブリック名をダブルクリックします。

[ファブリックの概要（Fabric Overview）] ウィンドウが表示されます。

ステップ 3 **[マルチキャスト NAT（Multicast NAT）]** タブをクリックします。

ステップ 4 **[NAT モード（NAT Modes）]** タブをクリックします。

ステップ 5 **[アクション（Actions）] > [NAT モードの作成（Create NAT Mode）]** の順にクリックして、NAT モードを追加します。

[NAT モードの追加（Add NAT Mode）] ウィンドウが表示されます。

ステップ 6 **[NAT モードの追加（Add NAT Mode）]** ウィンドウで、次の情報を指定します。

[モード（Mode）] : マルチキャスト NAT モード（**入力**または**出力**）を選択します。

[選択済みスイッチ（Selected Switch）]: スイッチ名を指定します。このフィールドは読み取り専用で、**[NAT モード（NAT Modes）]** タブで選択したスイッチに基づいています。

[VRF]：NAT モードが属する VRF を選択します。

[グループ（Group/Mask）]：マスクでマルチキャスト グループを指定します。特定のスイッチでは、同じグループを出力 NAT にすることはできません。特定のグループまたはマスクが入力か出力かを識別する必要があります。

ステップ 7 **[保存して展開（Save & Deploy）]** をクリックして、NAT モードを保存して展開します。

NAT モードの削除

手順

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

ステップ 2 ファブリック名をダブルクリックします。

[ファブリックの概要（Fabric Overview）] ウィンドウが表示されます。

ステップ 3 **[マルチキャスト NAT（Multicast NAT）]** タブをクリックします。

ステップ 4 **[NAT モード（NAT Modes）]** タブをクリックします。

ステップ 5 削除する必要がある NAT モードを選択し、[アクション（Actions）] の [NAT モードの削除（Delete NAT Mode）] をクリックして NAT モードを削除します。

NAT モードが展開されていない場合、または失敗した場合は、この手順を省略できます。

ステップ 6 [確認（Confirm）] をクリックして、選択した NAT モードを削除します。

再循環マッピング

NDFCを使用すると、入力または出力インターフェイスのポート間で再循環パケットをマッピングできます。リリース 12.1.1e から、次の変換タイプの再循環マッピングを構成できます。

- マルチキャスト間

- マルチキャストからユニキャストへ
- ユニキャストからマルチキャストへ

[LAN] > [ファブリック（Fabrics）] を選択します。再循環マッピングを設定するには、ファブリック名をダブルクリックし、**[マルチキャスト NAT（Multicast NAT）] > [再循環マッピング（Recirc Mappings）]** をクリックします。

次の表は、**[再循環マッピング（Recirc Mappings）]** タブに表示されるフィールドについて説明しています。

フィールド	説明
VRF	再循環マッピングがルーティングされる VRF を指定します。
出力インターフェイス	マッピングの出力インターフェイスを指定します。
宛先/プレフィックス	宛先ユニキャスト インターフェイスの IP アドレスを指定します。
マップインターフェイス	マップ インターフェイスを指定します。 出力インターフェイスとマップ インターフェイスには、複数対 1 の関係があります。マッピングに複数の出力インターフェイスがある場合は、ハイパーリンクとして表示されます。インターフェイスの完全なリストを表示するには、ハイパーリンクをクリックします。
最大レプリケーション数	マップインターフェイスの最大レプリケーション数を指定します。
展開アクション（Deployment Action）	その出力インターフェイス マッピングに対してスイッチで実行されるアクションを指定します。[作成（Create）] は、出力インターフェイス マッピングがスイッチに展開されていることを意味します。[削除（Delete）] は、出力インターフェイス マッピングがスイッチから展開解除されたことを意味します。
展開ステータス	出力インターフェイス マッピングが展開されているかどうかを指定します。展開に失敗した場合は、情報アイコンにカーソルを合わせて失敗の理由を表示します。
最終更新日	出力インターフェイス マッピングが最後に更新された日時を指定します。 日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。

次の表は、**[アクション（Actions）]** メニューのドロップダウンリスト（**[再循環マッピング（Recirc Mappings）]** タブに表示されるもの）に表示されるアクションアイテムについて説明しています。

アクション項目	説明
NAT 再循環マッピングの作成	**[NAT 再循環マッピングの作成（Create NAT Recirc Mapping）]** を選択して、再循環マッピングを追加します。
NAT 再循環マッピングの編集	再循環マッピングを編集するには、テーブルからモードを選択し、**[NAT 再循環マッピングの編集（Edit NAT Recirc Mapping）]** を選択します。
NAT 再循環マッピングの削除	再循環マッピングを削除するには、テーブルからモードを選択し、**[NAT 再循環マッピングの削除（Delete NAT Recirc Mapping）]** を選択します。
インポート	NAT 出力インターフェイスマッピングを CSV ファイルから Nexus ダッシュボード ファブリック コントローラにインポートできます。
エクスポート	NAT 再循環マッピングは Nexus ダッシュボード ファブリック コントローラ から CSV ファイルにエクスポートできます。
選択した NAT 再循環マッピングを展開する	テーブルからモードを選択し、**[選択した NAT 再循環マッピングの展開（Deploy Selected NAT Recirc Mappings）]** を選択して、選択した再循環マッピングをスイッチに展開します。
すべての NAT 再循環マッピングの展開	**[すべての NAT 再循環マッピングの展開（Deploy All NAT Recirc Mapping）]** を選択して、すべての再循環マッピングをスイッチに展開します。
選択した NAT 再循環マッピングの展開解除	テーブルからモードを選択し、**[選択した NAT 再循環マッピングの展開解除（Undeploy Selected NAT Recirc Mappings）]** を選択して、選択した再循環マッピングをスイッチから展開解除します。
すべての NAT 再循環マッピングの展開解除	**[すべての NAT 再循環マッピングの展開解除（Undeploy All NAT Recirc Mapping）]** を選択して、すべての再循環マッピングをスイッチから展開解除します。

アクション項目	説明
失敗したすべてのNAT再循環マッピングをやり直す	**[失敗したすべての NAT 再循環マッピングをやり直す（Redo All Failed NAT Recirc Mapping）]** を選択して、失敗したすべての再循環マッピングを展開します。

アクション項目	説明
導入履歴	テーブルから再循環マッピングを選択し、**[展開履歴（Deployment History）]** を選択して、先ほど選択した再循環マッピングの展開履歴を表示します。 [展開履歴（Deployment History）] には、次のフィールドが表示されます。 • **[スイッチ名（Switch Name）]**：モードが展開されたスイッチの名前を指定します。 • **VRF**：選択した再循環マッピングの設定に使用する VRF を指定します。 • **[マップ インターフェイス（Map Interface）]**：再循環マッピングのマップインターフェイスを指定します。 • **[最大レプリケーション（Max Replications）]**：再循環マッピングの最大レプリケーション数を指定します。 • **[出力インターフェイス（Egress Interfaces）]** または **[宛先/プレフィックス（Destination/Prefix）]**：再循環マッピングが構成されているインターフェイスを指定します。 • **[展開ステータス（Deployment Status）]**：展開ステータスを表示します。導入が成功したか失敗したかが表示されます。失敗していた場合は、理由が表示されます。 • **[アクション（Action）]**：その再循環マッピングに対してスイッチで実行されるアクションを指定します。作成は、マッピングがスイッチに展開されたことを意味します。削除は、マッピングがスイッチから展開解除されたことを意味します。 • **[展開日時（Deployment Date/Time）]**：マッピングが最後に更新された日時を指定します。日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。

再循環マッピングの追加

手順

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

ステップ 2 ファブリック名をダブルクリックします。

[ファブリックの概要（Fabric Overview）] ウィンドウが表示されます。

ステップ 3 **[マルチキャスト NAT（Multicast NAT）] > [再循環マッピング（Recirc Mappings）]** タブをクリックします。

ステップ 4 **[選択したスイッチ（Selected Switch）]** ドロップダウン リストから、再循環マッピングを作成するスイッチを選択します。

ステップ 5 **[アクション（Actions）] > [再循環マッピングの作成（Create Recirc Mapping）]** をクリックして、選択したスイッチの再循環マッピングを追加します。

[再循環マッピングの追加（Add Recirc Mappings）] ウィンドウが表示されます。

ステップ 6 **[再循環マッピングの追加（Add Recirc Mappings）]** ウィンドウの **[選択済みのスイッチ（Selected Switch）]** フィールドで、スイッチ名を指定します。

このフィールドは読み取り専用で、[再循環マッピング（Recirc Mappings）] ウィンドウで選択されたスイッチに基づきます。

ステップ 7 **[VRF]** ドロップダウン リストから、再循環がルーティングされる VRF を選択します。

ステップ 8 [変換タイプ（Translation Type）] で、変換タイプのいずれかを選択します。

- マルチキャスト間
- マルチキャストからユニキャストへ
- ユニキャストからマルチキャストへ

ステップ 9 **[マルチキャスト間（Multicast-to-Multicast）]** 遷移タイプを選択した場合は、**[出力インターフェイス（Egress Interfaces）]** 領域で、次のいずれかを選択します。

- [すべて（All）]：すべてのインターフェイスを選択するには、[すべて] を選択します
- [1 つ以上選択（Select one or more）]：複数の出力インターフェイスを選択するには、**[1 つ以上選択（Select one or more）]** オプションを選択し、**[選択（Select）]** オプションをクリックしてインターフェイスを選択します。[選択（Select）] ウィンドウには、使用可能なインターフェイスが表示されます。つまり、他のマッピングですでに定義されているインターフェイスは除外されます。すべてのインターフェイスを選択するには、[すべて（All）]を選択します。[すべて（All）]を選択すると、個々の出力インターフェイスを選択するオプションは無効になります。

ステップ 10 移行タイプに基づいて、次の手順を実行します。

- **[マルチキャストからユニキャストへ（Multicast-to-Unicast）]** 移行タイプを選択した場合は**[宛先/プレフィックス（Destination/Prefix）]**フィールドに、宛先ユニキャストインターフェイスの IP アドレスを入力します。
- **[ユニキャストからマルチキャストへ（Unicast-to-Multicast）]** 移行タイプを選択した場合は**[宛先/プレフィックス（Destination/Prefix）]** フィールドに、宛先マルチキャスト インターフェイスの IP アドレスを入力します。

ステップ 11 **[マップ インターフェイス（Map Interface）]** ドロップダウン リストから、再循環マッピングを開始するインターフェイスを選択します。

インターフェイスは、出力インターフェイスまたはマップインターフェイスのいずれかで、両方は使用できません。すでに出力インターフェイスとして選択されているマップインターフェイスを選択すると、エラーが表示されます。

ステップ 12 **[最大レプリケーション（Max Replications）]** フィールドに、マップ インターフェイスの最大レプリケーション数を入力します。このフィールド値の範囲は 1 ～ 40 です。デフォルト値は 40 です。

ステップ 13 **[保存して展開（Save & Deploy）]** をクリックして、NAT モードを保存して展開します。

NAT ルール

NAT ルールは、イングレス NAT とエグレス NAT で同じですが、出力 NAT のレシーバ OIF も指定する必要があります。

[LAN] > [ファブリック（Fabrics）] を選択します。NATルールを設定するには、ファブリック名をダブルクリックし、[Multicast NAT]> [NAT Rules]をクリックします。

次の表では、**[NAT ルール（NAT Rules）]** タブに表示されるフィールドについて説明します。

フィールド	説明
VRF	マルチキャストNATのVRFを指定します。
モード	入力または出力の NAT モードを指定します。
事前変換グループ	NAT 変換前のマルチキャスト グループを示します。
変換後グループ	NAT 変換後のマルチキャスト グループを示します。
グループマスク	グループ マスクを指定します。
事前変換	NAT 変換前の送信元 IP アドレスです。
変換後の送信元	NAT 変換後の送信元 IP アドレスです。
送信元マスク	送信元マスクを指定します。
変換後の送信元ポート	NAT 変換後の送信元ポートを示します。範囲は、0 ～ 65535 です。値 0 は、UDP ソース ポートの変換がないことを意味します。

変換後の宛先ポート	NAT 変換後の宛先ポートを示します。値 0 は、UDP 宛先ポートの変換がないことを意味します。
静的 Oif	出力 NAT ルールをバインドする静的な発信インターフェイスを指定します。このドロップダウンには、[Egress Interface Mappings] ウィンドウで定義された出力インターフェイスが表示されます。このフィールドは入力モードには無効です。
展開アクション（Deployment Action）	ルールのスイッチで実行されるアクションを指定します。作成は、ルールがスイッチで展開されていることを意味します。削除は、ルールがスイッチから展開解除されていることを意味します。
展開ステータス	ルールが展開されているか否かを指定します。展開が失敗した場合、情報アイコンの上にマウスを置いて、失敗理由を表示します。
最終更新日	ルールが最後に更新された日時を指定します。 日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。

次の表では、[NATルール（NAT Rules）]タブに表示される[アクション（Actions）]メニュードロップダウンリストのアクション項目について説明します。

アクション項目	説明
NATルールの作成	NAT ルールを追加するには、**[NAT ルールの作成（Create NAT Rule）]** を選択します。
NATルールの削除	テーブルからモードを選択し、[Delete NAT Rule]を選択してルールを削除します。
インポート	CSVファイルからNATルールをにインポートできます。Nexusダッシュボード ファブリック コントローラ
エクスポート	NATルールをCSVファイルにエクスポートできます。Nexusダッシュボード ファブリック コントローラ
選択したNATルールの展開	テーブルからルールを選択し、[Deploy Selected NAT Rules]を選択して、選択したルールをスイッチに展開します。
すべてのNATルールの展開	[Deploy All NAT Rules]を選択して、すべてのルールをスイッチに展開します。

アクション項目	説明
選択したNATルールの展開解除	テーブルからルールを選択し、[Undeploy Selected NAT Rules]を選択して、選択したルールをスイッチに展開解除します。
すべてのNATルールの展開解除	[Undeploy All NAT Rules]を選択して、スイッチからすべてのルールを展開解除します。
失敗したすべてのNATルールをやり直し	[失敗したすべてのNATルールをやり直す（Redo All Failed NAT Rules）]を選択して、失敗したすべてのルールを展開します。
導入履歴	テーブルからルールを選択し、[Deployment History]を選択して、選択したルールの展開履歴を表示します。 [展開履歴（Deployment History）] には、次のフィールドが表示されます。 • スイッチ名：ルールが展開されたスイッチの名前を指定します。 • VRF：マッピングが属する VRF を指定します。 • 展開ステータス：展開のステータスを表示します。導入が成功したか失敗したかが表示されます。 • アクション：ルールのスイッチで実行されるアクションを指定します。作成は、ルールがスイッチで展開されていることを意味します。削除は、ルールがスイッチから展開解除されていることを意味します。 • 展開日時：ルールが最後に更新された日時を指定します。日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。 • 失敗理由：ルールが正常に展開されなかった理由を指定します。

NAT ルールの追加

手順

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

ステップ 2 ファブリック名をダブルクリックします。

[ファブリックの概要（Fabric Overview）] ウィンドウが表示されます。

ステップ 3 **[マルチキャスト NAT（Multicast NAT）]** タブをクリックします。

ステップ 4 **[NAT ルール（NAT Rules）]** タブをクリックします。

ステップ 5 **[アクション（Actions）] > [NAT ルールの作成（Create NAT Rule）]** をクリックして NAT ルールを追加します。

[NAT ルールの追加（Add NAT Rule）] ウィンドウが表示されます。

ステップ 6 **[NAT ルールの追加（Add NAT Rule）]** ウィンドウで、次の情報を指定します。

[変換タイプ（Translation Type）]：変換タイプのいずれかを選択します。

- マルチキャスト間
- マルチキャストからユニキャストへ
- ユニキャストからマルチキャストへ

[モード（Mode）]：NAT モード（**入力**または**出力**）を選択します。

このモードは、マルチキャストからユニキャストおよびユニキャストからマルチキャストへの変換タイプでは表示されません。

[選択済みスイッチ（Selected Switch）]: スイッチ名を指定します。このフィールドは読み取り専用で、**[NAT ルール（NAT Rules）]** タブで選択したスイッチに基づいています。

[VRF]：NAT ルールの VRF を選択します。デフォルトでは、**デフォルト** の VRFです。

[変換前グループ/ユニキャスト IP（Pre-Translation Group/Unicast IP）]：NAT の前のマルチキャストまたはユニキャスト グループを指定します。

[変換後グループ（Post-Translation Group）]：NAT 後のマルチキャストまたはユニキャストグループを指定します。

[グループ マスク（Group Mask）]：NAT ルールのマスク値を指定します。デフォルトでは 32 です。

[変換前の送信元（Pre-Translation Source）]：NAT の前の送信元 IP アドレスを指定します。

[変換後の送信元（Post-Translation Source）]：NAT 後の送信元 IP アドレスを指定します。

（注） RPF チェックが失敗しないようにするには、変換後の送信元 IP をループバック インターフェイスのセカンダリ IP アドレスにする必要があります。ただし、スイッチはプレ NAT レコードとポスト NAT レコードを別々に保持するのに対し、NDFC はユニキャストとマルチキャストのプレポスト エントリを単一のフローとしてマージします。

[送信元マスク（Source Mask）]：NAT ルールの送信元マスク値を指定します。デフォルトでは 32 です。

[変換後の送信元ポート（Post-Translation Source Port）]：送信元ポートはデフォルトで 0 です。値 0 は変換なしを意味します。

[変換後の宛先ポート（Post-Translation Destination Port）]：デフォルトでは宛先ポートは 0 です。値 0 は変換なしを意味します。

[スタティック Oif（Statis Oif）]：このフィールドは入力モードでは表示されません。出力モードでは、このフィールドには、Recirc Mappings 画面で定義された**出力インターフェイス**が表示されます。マッピングが定義されていない場合、フィールドは空です。

ステップ 7 **[保存と展開（Save & Deploy）]** をクリックして、NAT ルールを保存して展開します。

NAT ルールの削除

手順

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

ステップ 2 ファブリック名をダブルクリックします。

[ファブリックの概要（Fabric Overview）] ウィンドウが表示されます。

ステップ 3 **[マルチキャスト NAT（Multicast NAT）]** タブをクリックします。

ステップ 4 **[NAT ルール（NAT Rules）]** タブをクリックします。

ステップ 5 NATルールを削除するには、削除する必要があるNATモードを選択し、**[アクション（Actions）] > [NATルールの削除（Delete NAT Rule）]** をクリックします。

NAT ルールが展開されていない場合、または失敗していた場合は、この手順をスキップできます。

ステップ 6 **[確認（Confirm）]** をクリックして、選択したNATルールを削除します。

RTP/EDIフロー モニタ

（注） このタブは、Nexus Dashboard ファブリック コントローラに IPFM を展開している場合にのみ、IPFM ファブリックで使用できます。

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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）]** > **[RTP/EDI フロー モニタ（RTP/EDI Flow Monitor）]**を選択します。
- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。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）]** > **[RTP/EDI フロー モニタ（RTP/EDI Flow Monitor）]** を開きます。

（注） このセクションは、Nexusダッシュボード ファブリック コントローラ の IPFM と汎用マルチキャスト モードの両方に適用されます。

Cisco Nexusダッシュボード ファブリック コントローラ では、すべてのアクティブな RTP および EDI ストリームのビューを提供しています。また、RTP と EDI のドロップがあるアクティブなフローと、同じものに関する履歴レコードも一覧表示します。アクティブ IPFM フローの場合、Nexusダッシュボード ファブリック コントローラ はネットワークの損失を特定するための RTP および EDI トポロジを提供します。

（注） RTP/EDI フロー モニタを表示するには、スイッチでテレメトリを有効にする必要があります。詳細については、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。

これらのタブのフィールドの説明は次のとおりです。

フィールド	説明
スイッチ	スイッチの名前を示します。
インターフェイス	フローが検出されたインターフェイスを示します。
送信元 IP	フローの送信元 IP アドレスを示します。
送信元ポート	フローの送信元ポートを示します。
宛先 IP	フローの宛先 IP アドレスを示します。
宛先ポート	フローの宛先ポートを示します。

フィールド	説明
ビット レート	フローのビット レートを bps、kbps、mbps、gbps または tbp で示します。
パケットカウント	フローのパケット数を示します。
Packet Loss	失われたパケット数を示します。
損失開始	パケット損失が開始した時刻を示します。
損失終了	パケット損失が終了した時刻を示します。
開始時刻	フローが開始した時刻を示します。
プロトコル	フローで使用されているプロトコルを示します。

[テレメトリ スイッチ同期ステータス（Telemetry Switch Sync Status）] リンクをクリックすると、スイッチが同期しているかどうかを確認できます。**[テレメトリ同期ステータス（Telemetry Sync Status）]** ウィンドウの **[同期ステータス（Sync Status）]** フィールドにスイッチのステータスが表示され、**[最終同期時刻（Last Sync Time）]** フィールドに同期が最後に発生した時刻が表示されます。

[RTP/EDI フロー モニタ（RTP/EDI Flow monitor）] ウィンドウには、次のタブがあります。

- **アクティブなフロー**
- **パケット損失**
- **[ドロップ履歴（Drop History）]**

アクティブなフロー

[アクティブ フロー（Active Flows）] タブには、現在アクティブなフローが表示されます。これらのフローは、**[フロー（Flows）]>[フローステータス（Flow Status）]** に移動して表示することもできます。スイッチ リンクをクリックすると、エンドツーエンドフロー トポロジを表示できます。

[フロー トポロジ（Flow Topology）]

[フロー ステータス（Flow Status）] ウィンドウに表示されるアクティブなフローのフロートポロジが表示されます。マルチ キャスト NAT の可視化の詳細については、「Flow Status」を参照してください。

エンドツーエンド フロート ポロジを表示するには、スイッチ リンクをクリックします。

フロートポロジには、フローの方向が表示されます。アイコン内の矢印は、送信者から受信者へのフローの方向を示します。（**S**）と（**R**）が付いた IP アドレスは、それぞれ送信者と受信者のホストを示します。特定のフローに複数の受信者が存在する場合は、**[受信者の選択（Select Receiver）]** ドロップダウン リストから受信者を選択できます。

パケット ドロップが発生しているスイッチは、赤色の丸で囲まれています。

スイッチにカーソルを合わせると、次の詳細が表示されます。

- 名前
- IP address
- モデル
- パケット損失（存在する場合）

スイッチ間のリンクの横にある**ファイル**のアイコンをクリックすると、2 つのスイッチを接続しているインターフェイスのインターフェイス カウンタ エラーが表示されます。

ファイル アイコンをクリックすると、これらのスイッチ間でフローが参加しているインターフェイスに対して、**show interface <*interface name*> counters errors** コマンドが実行され、結果がポップインで表示されます。

パケット損失

[パケットドロップ（Packet Drop）] タブには、アクティブ フローのパケットドロップが表示されます。

[ドロップ履歴（Drop History）]

アクティブなRTPパケットドロップが確認されない場合、**[パケットドロップ（Packet Drop）]** タブのレコードは **[ドロップ履歴（Drop History）]** タブに移動されます。デフォルトでは、RTP ドロップ履歴は7日間保持されます。この設定をカスタマイズするには、**[IPFM履歴保持日数（IPFM history retention days）]**フィールド（**[設定（Settings）] > [サーバー設定（Server Settings）] > [IPFM]**）に必要な値を入力し、保存します。

（注） **[ドロップ履歴（Drop History）]** タブには、最後の 100,000 レコードのみが表示されます。

グローバル設定

Note このタブは、Nexus ダッシュボード ファブリック コントローラに IPFM を展開している場合にのみ、IPFM ファブリックで使用できます。ただし、汎用マルチキャスト ファブリック テクノロジーを使用する IPFM ファブリックは例外です（ここで作成された IPFM VRF は、IPFM と汎用マルチキャスト ファブリックの両方のホスト/フロー エイリアスを定義するために使用されます）。

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]を選択します。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）] > [グローバル構成（Global Config）] を選択します。 >

- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。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）] > [グローバル構成（Global Config）] を開きます。

Nexusダッシュボード ファブリック コントローラ では、2 つの主要な操作が可能です。

- ネットワークを監視します。
- ホストおよびフロー ポリシーを構成します。

Nexusダッシュボード ファブリック コントローラ は、テレメトリを使用して、フロー ステータス、検出されたホスト、適用されたホストポリシー、およびその他の操作をモニタします。スイッチによってトリガーされ、テレメトリを介して受信されたすべての操作（たとえば、フロー確立）は、定期的に新しいイベントをチェックし、適切な通知を生成します。Nexusダッシュボード ファブリック コントローラ

スイッチのリロード中に pmn.deploy-on-import-reload.enabled サーバ プロパティが true に設定されている場合、スイッチの coldStartSNMPtrap を受信すると、「Deployment Status=Successes」を示すグローバル構成、およびホストとフローポリシーが自動的にスイッチに展開されます。Nexusダッシュボード ファブリック コントローラスイッチ テレメトリを導入し、SNMP 設定をオンデマンドで導入するには、[テンプレート（Templates）] で利用可能なパッケージ化された [pmn_telemetry_snmp] CLI テンプレートを使用します。Nexusダッシュボード ファブリック コントローラ

[グローバル構成（Global Config）]に移動して、スイッチ グローバル構成と VRF を設定または変更します。

IPFM 導入でインストールする場合、[グローバル構成（Global Config）] を使用して、ポリシー、ユニキャスト帯域幅、Any Source Multicast（ASM）範囲、および VRF を展開できます。Nexusダッシュボード ファブリック コントローラ

Nexusダッシュボード ファブリック コントローラを IPFM で展開した後、帯域幅と ASM を設定します。帯域幅の残りの割合は、マルチキャスト トラフィックによって使用されます。はマスター コントローラのように動作し、ファブリック内のすべてのスイッチに帯域幅と ASM の構成を展開します。Nexusダッシュボード ファブリック コントローラ

Cisco Nexusダッシュボード ファブリック コントローラはファブリックからデータを取得するためにテレメトリを使用するため、フローステータスと Kafka 通知にリアルタイムの現在の状態が反映されない場合があります。定期的に新しいイベントをチェックし、適切な通知を生成します。詳細については、『Cisco Nexus ダッシュボード ファブリック コントローラの Kafka 通知、リリース 12.0.1a』を参照してください。

この項の内容は、次のとおりです。

スイッチのグローバル設定

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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。[Fabric Overview] [Global Config] [Switch Global Config]を選択します。 > >
- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。ファブリックをダブルクリックして、Fabric Overview Global Config Switch Global Configを開きます。 > >

グローバルパラメータを設定するには、[Switch Global Config]に移動します。

Note ネットワークオペレータロールを持つユーザは、ASMを保存、展開、展開解除、追加、または削除することはできません。Nexusダッシュボード ファブリック コントローラ

ユニキャスト帯域幅予約およびASM範囲を設定した後、次の操作を実行してこれらの設定をスイッチに展開できます。

グローバル設定を展開したら、ネットワーク内の各スイッチにWANを設定します。

Table 29: スイッチのグローバル設定テーブルのフィールドと説明

フィールド	説明
VRF	VRF の名前を指定します。このVRFは、IPFMと汎用マルチキャストファブリックの両方のIPFMホスト/フローポリシーとホスト/フローエイリアスを関連付けるために使用されます。
ユニキャスト帯域幅予約 %	ユニキャスト帯域幅設定のパーセンテージを示す数値を表示します。ステータスは、帯域幅の展開が成功したか、失敗したか、展開されていないかを示します。 帯域幅の専用のパーセンテージをユニキャスト トラフィックに割り当てるようにサーバを構成できます。残りのパーセンテージは、マルチキャスト トラフィックに自動的に予約されます。 数値リンクをクリックして、選択したVRFのユニキャスト帯域幅の展開履歴の詳細を表示し、[展開履歴（Deployment History）]ペインで切り替えます。詳細については、導入履歴, on page 276を参照してください。 [Failed]または[Success]リンクをクリックして、選択したVRFのユニキャスト帯域幅の展開ステータスの詳細を表示し、[Deployment Status]ペインで切り替えます。詳細については、展開ステータス, on page 276を参照してください。

フィールド	説明
受信者のみに帯域幅を予約	帯域幅予約ステータスは、帯域幅の展開が成功したか、失敗したか、または展開されていないかを示します。 Enabledステータスは、レシーバが存在する場合にのみ、ASMトラフィックがスパインにプッシュされることを示します。この機能は、Cisco NX-OSリリース9.3（5）以降のスイッチに適用されます。 [Enabled]リンクをクリックして、選択したVRFの予約帯域幅の導入履歴の詳細を表示し、[Deployment History]ペインで切り替えます。詳細については、導入履歴, on page 276を参照してください。 [失敗（Failed）]リンクをクリックして、選択したVRFの予約帯域幅の展開ステータスの詳細を表示し、[展開ステータス（Deployment Status）]ペインで切り替えます。詳細については、展開ステータス, on page 276を参照してください。

フィールド	説明
ASM / MASK	選択したVRFで有効になっているAny Source Multicast（ASM）グループの数を表示します。ステータスは、ASMとマスクの設定が正常に展開されたか、失敗したか、または展開されていないかを示します。 ASM は PIM ツリー構築モードの 1 つです。新しい送信元および受信者を検出する場合には共有ツリーを、受信者から送信元への最短パスを形成する場合は送信元ツリーを使用します。ASM はマルチキャスト送信元を検出します。 [ASM / MASK]フィールドのIPアドレスとサブネットマスクは、マルチキャスト送信元を定義します。 ASMの範囲は、IPアドレスとサブネットマスクを指定して設定します。 数値リンクをクリックして、選択したVRFのASM /マスクの導入履歴の詳細を表示し、[導入履歴（Deployment History）]ペインで切り替えます。詳細については、導入履歴, on page 276を参照してください。 [Failed]リンクをクリックして、選択したVRFのASM/マスクの導入ステータスの詳細を表示し、[Deployment Status]ペインで切り替えます。詳細については、展開ステータス, on page 276を参照してください。

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

次の表に、[Switch Global Config]ウィンドウに表示される[Actions]ドロップダウンリストのアクション項目を示します。

Table 30: スイッチのグローバル設定アクションと説明

アクション項目	説明
NBM VRF設定の編集	NBM VRF設定を編集できます。 編集を実行するには、このオプションを選択します。[Edit NBM VRF Config]ウィンドウが開きます。必要な値を編集し、[展開（Deploy）]をクリックします。

アクション項目	説明
すべて展開解除	すべてのスイッチに、ASM、ユニキャスト帯域幅、および予約帯域幅の設定を展開解除します。
ユニキャストBWの展開解除	ユニキャスト帯域幅設定のみを展開解除します。
予約BWの展開解除	予約帯域幅設定のみを展開解除します。
ASM /マスクの展開解除	ASM構成のみを展開解除します。
すべてやり直し失敗	選択した失敗した設定を再展開します。

導入履歴

次のテーブルは、[展開履歴（Deployment History）] で表示されるフィールドを説明しています。

Table 31: [展開履歴（Deployment History）] フィールドと説明

フィールド	説明
タイプ	タイプが[ユニキャスト帯域幅予約%（Unicast Bandwidth Reservation%）]、[レシーバ専用帯域幅の予約（Reserve Bandwidth to Receiver Only）]、または[ASM / MASK]のいずれであるかを指定します。
VRF	VRF の名前を指定します。
スイッチ名	設定が展開されたファブリックのスイッチ名を指定します。
展開ステータス	展開のステータスを表示します。展開が成功したか失敗したかが、展開が失敗した理由とともに表示されます。
アクション	**[作成（Create）]** または **[削除（Delete）]** など、スイッチで実行されるアクションを指定します。
展開の日時	展開が初期化される日時を表示します。

展開ステータス

次のテーブルは、展開ステータスで表示されるフィールドを説明しています。

Table 32: 展開ステータス フィールドおよび説明

フィールド	説明
タイプ	タイプが[ユニキャスト帯域幅予約%（Unicast Bandwidth Reservation%）]、[レシーバ専用帯域幅の予約（Reserve Bandwidth to Receiver Only）]、または[ASM / MASK]のいずれであるかを指定します。
VRF	VRF の名前を指定します。
スイッチ名	設定が展開されたファブリックのスイッチ名を指定します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。
展開ステータス	展開のステータスを表示します。展開が成功したか失敗したかが、VRF展開が失敗した理由とともに表示されます。
アクション	スイッチで実行されるアクション、たとえば**[作成（Create）]**、を指定します。
展開の日時	展開が初期化される日時を表示します。

IPFM VRF

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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。**Fabric Overview** > **Global Config** > **IPFM VRF** を選択します。
- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。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）]** > **[Global Config]** > **[IPFM VRF]**を開きます。

[IPFM VRF] ウィンドウを使用して、VRF を作成、編集、削除、および再展開します。各 VRF の展開ステータスと履歴を表示できます。

Table 33: IPFM VRF テーブルのフィールドと説明

フィールド	説明
名前	VRF の名前を指定します。

フィールド	説明
展開ステータス	VRF の展開が成功したか、失敗したか、またはVRF が展開されていないかを指定します。デフォルトVRFの場合、展開ステータスは**[該当なし（Not Applicable）]**と表示されます。 **[失敗（Failed）]** ステータスをクリックすると、展開ステータス, on page 276 の詳細情報が表示されます。
導入履歴	VRF の導入履歴を指定します。デフォルトVRF の場合、展開履歴は **[該当なし（Not Applicable）]** として表示されます。 展開履歴の詳細情報を表示するには、**[展開履歴]** の 導入履歴 をクリックします。
説明	説明を指定します。

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。

次の表では、**[ファブリックの概要（Fabric Overview）]** ウィンドウの [**グローバル Config（Global Config）]** タブにある **[IPFM VRF]** 水平タブに表示される **[アクション]** ドロップダウン リストのアクション項目について説明します。

Table 34: IPFM VRF アクションと説明

アクション項目	説明
VRFの作成	新しい VRF を作成できます。 VRF を作成するには、**[ファブリックの概要（Fabric Overview）]** ウィンドウの **[グローバル Config（Global Config）]** タブにある **[IPFM VRF]** 水平タブの **[アクション（Action）]** ドロップダウンリストから **[VRF の作成（Create VRF）]** を選択します。**[VRF の作成（Create VRF）]** ウィンドウで、VRF 名と説明を入力し、**[保存して展開（Save & Deploy）]** をクリックして変更を保持して展開するか、**[キャンセル（Cancel）]** をクリックして変更を破棄します。 **Note** カスタムまたはデフォルト以外のVRFを作成すると、そのVRFのデフォルトのホストおよびフローポリシーが自動的に作成されますが、ファブリック内のスイッチにポリシーを手動で展開する必要があります。ポリシーの手動展開の詳細については、ホストポリシー, on page 216 と「フローポリシー」を参照してください。
VRFの編集	選択した VRF を編集できます。 VRF 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て、**[VRF の編集（Edit VRF）]** を選択します。**[VRF の編集（Edit VRF）]** ウィンドウでは、説明のみを編集し、**[保存（Save）]** をクリックして変更を保持するか、**[キャンセル（Cancel）]** をクリックして変更を破棄できます。
VRFの削除	1 つ以上の VRF を削除できます。これにより、データベースからデータが削除され、スイッチでの展開がキャンセルされます。 VRF を削除するには、削除する VRF の横にあるチェックボックスをオンにし、**[VRF の削除（Delete VRF）]** を選択します。同じインスタンスであれば、複数の VRF エントリを選択して削除できます。
再展開	障害ステータスの VRF を選択して再展開できます。 VRF をスイッチに再展開するには、再度展開する VRF の横にあるチェックボックスをオンにして、**[再展開（Redeploy）]** を選択します。複数の VRF エントリを選択し、同じインスタンスに再展開できます。

導入履歴

次のテーブルは、**[展開履歴（Deployment History）]** ペインで表示されるフィールドを説明しています。

Table 35: [展開履歴（Deployment History）] フィールドと説明

フィールド	説明
タイプ	VRF のタイプを指定します。
VRF	VRF の名前を指定します。
スイッチ名	VRF が展開されるスイッチを指定します。
展開ステータス	展開のステータスを表示します。展開が**成功**したか、**失敗**したか、VRF 展開が失敗した理由、または**[該当なし（Not Applicable）]** のいずれかを示します。
アクション	**[作成（Create）]** または **[削除（Delete）]** など、スイッチで実行されるアクションを指定します。
展開の日時	展開が初期化される日時を表示します。

展開ステータス

次のテーブルは、**[展開ステータス（Deployment Status）]** ペインで表示されるフィールドを説明しています。

***Table 36:* 展開ステータス フィールドおよび説明**

フィールド	説明
タイプ	VRF のタイプを指定します。
VRF	VRF の名前を指定します。
スイッチ名	VRF が展開されるスイッチを指定します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。
展開ステータス	展開のステータスを表示します。展開が **[成功（Success）]** または **[失敗（Failed）]** した場合、展開の失敗理由と共に、表示されます。
アクション	スイッチで実行されるアクション、たとえば **[作成（Create）]**、を指定します。
展開の日時	展開が初期化される日時を表示します。

VRF（汎用マルチキャスト）

Note このタブは、IPFM が Nexusダッシュボード ファブリック コントローラ に導入されており、ファブリック テクノロジーが汎用マルチキャストである場合にのみ使用できます。

UI ナビゲーション

- **[LAN]** > **[ファブリック（Fabrics）]** を選択します。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。**[ファブリック概要（Fabric Overview）]** > **[VRF]** を選択します。
- **[LAN]** > **[ファブリック（Fabrics）]**を選択します。ファブリックをダブルクリックして、**[ファブリック概要（Fabric Overview）]** > **[VRF]** を開きます。

VRF ウィンドウを使用して、VRF を作成、編集、および削除します。

Table 37: VRF テーブルのフィールドと説明

フィールド	説明
名前	VRF の名前を指定します。
展開ステータス	汎用マルチキャスト VRF の場合、展開ステータスは **[該当なし（Not Applicable）]** と表示されます。
導入履歴	汎用マルチキャスト VRF の場合、展開ステータスは **[該当なし（Not Applicable）]** と表示されます。
説明	説明を指定します。

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、**[VRF]** ウィンドウに表示されるものです。

Table 38: VRF アクションと説明

アクション項目	説明
VRFの作成	新しい VRF を作成できます。 VRF を作成するには、**[ファブリック概要（Fabric Overview）]** ウィンドウにある **[VRF]** タブの **[アクション（Action）]** ドロップダウン リストから **[VRF の作成（Create VRF）]** を選択します。**[VRF の追加（Add VRF）]** ウィンドウで、VRF名と説明を入力し、**[保存（Save）]** をクリックして変更を保持するか、**[キャンセル（Cancel）]** をクリックして変更を破棄します。
VRFの編集	選択した VRF を編集できます。 VRF 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て、**[VRF の編集（Edit VRF）]** を選択します。**[VRF の編集（Edit VRF）]** ウィンドウでは、説明のみを編集し、**[保存（Save）]** をクリックして変更を保持するか、**[キャンセル（Cancel）]** をクリックして変更を破棄できます。
VRFの削除	選択した VRF を削除できます。 VRF を削除するには、削除する VRF の横にあるチェックボックスをオンにし、**[VRF の削除（Delete VRF）]** を選択します。同じインスタンスであれば、複数の VRF エントリを選択して削除できます。

仮想インフラストラクチャ

OpenStack VM の表示

次の表に、ウィンドウのフィールドと説明を示します。

フィールド	説明
VM 名	Kubernetes ポッドの名前を指定します。
コンピュータ名	Kubernetes ポッドの IP アドレスを表示します。
Fabric Name（ファブリック名）	ポッドのフェーズ（状態）を指定します。
IP アドレス	理由を指定します。
MAC アドレス	ポッドのアプリケーションを指定します。
物理 NIC	ポッドの名前空間を指定します。

フィールド	説明
ポート チャネル	ポッドのノード名を指定します。
スイッチ インターフェイス	ポッドに接続されているスイッチ インターフェイスを指定します。
スイッチ名	スイッチの名前を示します。
IPのスイッチ	スイッチの IP アドレスを指定します。
VLAN	VLAN を設定します。
ロック	クラスタがロック状態かどうかを指定します。
電源状態	openstack クラスタの電源状態を指定します。
状態を検出	openstack クラスタのネットワーク状態かどうかを指定します。
ステータス	openstack クラスタの状態を指定します。

エンドポイント ロケータ

エンドポイントロケータ（EPL）機能により、データセンター内のエンドポイントをリアルタイムで追跡できます。追跡には、エンドポイントのネットワーク ライフ履歴のトレースと、エンドポイントの追加、削除、移動などに関連する傾向へのインサイトの取得が含まれます。エンドポイントは少なくとも 1 つの IP アドレス (IPv4 および\または IPv6) と MAC アドレスをもつ任意のものです。EPL機能は、MAC専用エンドポイントを表示することもできます。デフォルトでは、MAC 専用エンドポイントは表示されません。その意味で、エンドポイントは仮想マシン（VM）、コンテナー、ベアメタル サーバー、サービス アプライアンスなどです。

Note

- EPLは、VXLAN BGP EVPN ファブリック展開でNexusダッシュボード ファブリック コントローラ LAN ファブリック インストール モードでのみサポートされます。VXLAN BGP EVPN ファブリックは、Easy ファブリック、Easy eBGP ファブリック、または外部ファブリック（管理モードまたはモニタ モード）として導入できます。EPL は、3 層のアクセス集約コア ベースのネットワーク展開ではサポートされません。
- EPL は、少なくとも 1 つの IP アドレス（IPv4 または IPv6）を持つエンドポイントを表示します。EPL は、MAC 専用エンドポイントを表示することもできます。EPL の設定時に **[MAC のみのアドバタイズメントを処理（Process MAC-Only Advertisements）]** チェックボックスをオンにして、MAC アドレスのみを持つ EVPN ルートタイプ 2 アドバタイズメントの処理を有効にします。L2VNI：MAC は、このようなすべてのエンドポイントの一意のエンドポイント ID です。EPL は、レイヤ 3 ゲートウェイがファイアウォール、ロードバランサ、またはその他のノード上にあるレイヤ2のみのネットワーク展開でエンドポイントを追跡できるようになりました。

EPL は、エンドポイント情報を追跡するために BGP の更新に依存します。したがって、通常Nexusダッシュボード ファブリック コントローラは、これらの更新を取得するためにBGPルートリフレクタ（RR）とピアリングする必要があります。このためには、Nexusダッシュボード ファブリック コントローラ から RR への IP 到達可能性が必要です。これは、Nexusダッシュボード ファブリック コントローラ データネットワーク インターフェイスへのインバンドネットワーク接続で実現できます。

エンドポイント ロケータの主な特徴は次のとおりです。

- デュアルホーム接続およびデュアルスタック（IPv4 + IPv6）エンドポイントのサポート
- 最大 2 つの BGP ルート リフレクタまたはルート サーバのサポート
- VRF、ネットワーク、レイヤ2 VNI、レイヤ3 VNI、スイッチ、IP、MAC、ポート、VLAN などのさまざまな検索フィルタで、すべてのエンドポイントのリアルタイムおよび履歴検索をサポートします。
- エンドポイントのライフタイム、ネットワーク、エンドポイント、VRF 日次ビュー、運用ヒートマップなどのインサイトに関するリアルタイムおよび履歴ダッシュボードのサポート。
- iBGP および eBGP ベースの VXLAN EVPN ファブリックのサポート。ファブリックは、イージーファブリックまたは外部ファブリックとして作成できます。EPLは、適切なBGP設定でスパインまたは RR を自動的に設定するオプションで有効にできます。
- 最大 4 つのファブリックに対して EPL 機能を有効にできます。
- EPL はマルチサイト ドメイン（MSD）でサポートされます。
- IPv6 アンダーレイはサポートされていません。
- ハイ アベイラビリティのサポート

- 最大 60 日間保存されるエンドポイントデータのサポート。最大 100 GB のストレージ容量。
- 新たに開始するためのエンドポイント データのオプションのフラッシュのサポート。
- サポートされる拡張性：ファブリックあたり最大 5 万個の固有エンドポイント。最大 4 つのファブリックがサポートされます。ただし、すべてのファブリックのエンドポイントの最大合計数は 50K を超えてはなりません。

  すべてのファブリックのエンドポイントの合計数が 50K を超えると、アラームが生成され、ウィンドウの右上にある **[アラーム（Alarms）]** アイコンの下にリストされます。このアイコンは、新しいアラームが生成されるたびに点滅し始めます。
- NDFC リリース 12.0.1a 以降、EPL を有効にするには、永続的または外部 IP アドレスが必要です。VXLAN ファブリックごとに、ファブリックのスパインとピアリングする BGP インスタンスを実行する特定のコンテナが生成されます。このコンテナには、スパイン上の iBGP ネイバーとして設定される永続的な IP が関連付けられている必要があります。ファブリックごとに異なるコンテナが使用されるため、EPL が有効になっている NDFC によって管理されるファブリックの数によって、EPL のために配布する必要がある永続的な IP アドレスの数が決まります。また、EPL は Nexus Dashboard データインターフェイス上でのみ iBGP セッションを確立します。
- 仮想 Nexus Dashboard の展開では、Nexus Dashboard 管理および/または IP スティッキ性が必要なデータ vNIC に関連付けられたポートグループで無差別モードを有効化し/受け入れます。永続的な IP アドレスがポッドに与えられます（たとえば、SNMP トラップ/Syslog レシーバー、ファブリックごとのエンドポイント ロケーター インスタンス、SAN Insights レシーバーなど）。Kubernetes のすべての POD は、複数の仮想インターフェースを持つことができます。特に IP スティッキ性については、外部サービス IP プールから適切な空き IP が割り当てられた POD に追加の仮想インターフェイスが関連付けられます。vNIC には、vND 仮想 vNIC に関連付けられた MAC アドレスとは異なる独自の一意の MAC アドレスがあります。さらに、POD から外部スイッチとの間のすべての通信は、北から南へのトラフィックフローのために同じボンドインターフェイスから出力されます。EPL コンテナは Nexus Dashboard データインターフェイスを使用します。データ vNIC は、bond0（bond0br とも呼ばれる）インターフェイスにマップします。デフォルトでは、VMware システムは、特定の vNIC からのトラフィックフローがその vNIC に関連付けられた送信元 MAC と一致するかどうかを確認します。NDFC の場合、トラフィックフローは、指定された POD の永続的 IP アドレスを使用して発信されます。そのため、VMware 側で必要な設定を有効にする必要があります。

開始する前に仮想 Nexus ダッシュボードクラスタを使用している場合は、永続的な IP アドレス、EPL 機能、および必要な設定が有効になっていることを確認してください。以下のリンクを参照。

Cisco Nexus Dashboard ファブリックコントローラ導入ガイド

Cisco Nexus Dashboard ファブリックコントローラのインストールとアップグレードガイド

EPL 接続オプション

様々な EPL 接続オプションのサンプル トポロジは次のとおりです。

DCNM クラスタ モード：物理サーバから VM へのマッピング

詳細については、 Cisco Nexus Dashboard Fabric Controller Verified Scalability Guideを参照してください。

エンドポイント ロケータの構成

Nexusダッシュボード ファブリック コントローラ の OVA または ISO インストールでは、次の 2 つのインターフェイスを使用します。

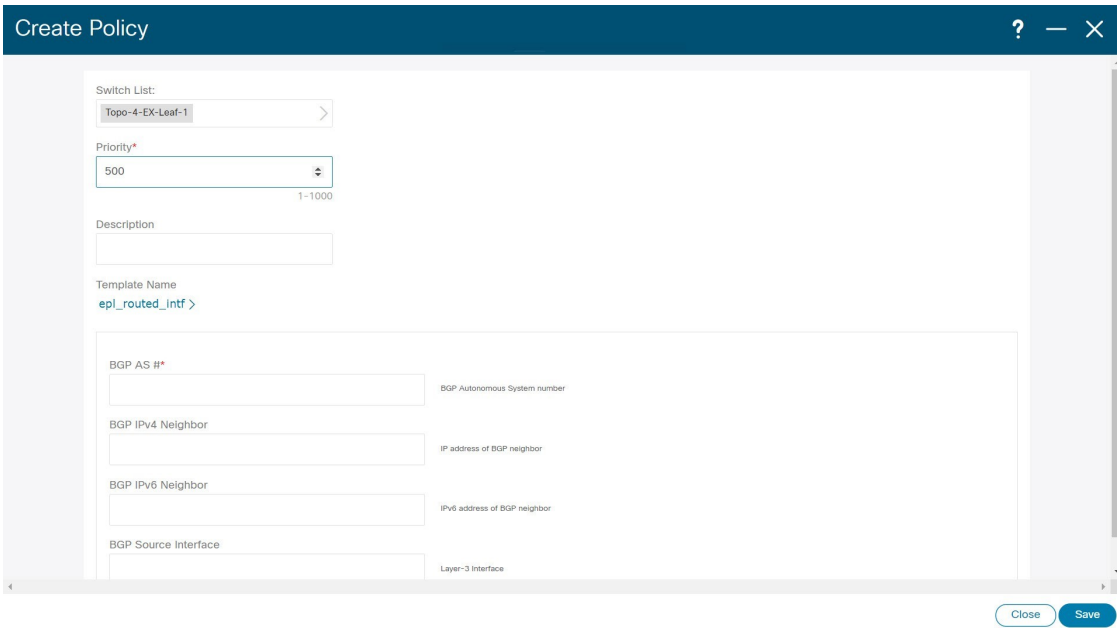
- 管理
- データ

（アウトオブバンドまたは OOO）スイッチ mgmt0 インターフェイスを介したスイッチの接続は、データ インターフェイスまたは管理インターフェイスによって行うことができます。詳細については、NDFC Installation and Upgrade Guide を参照してください。

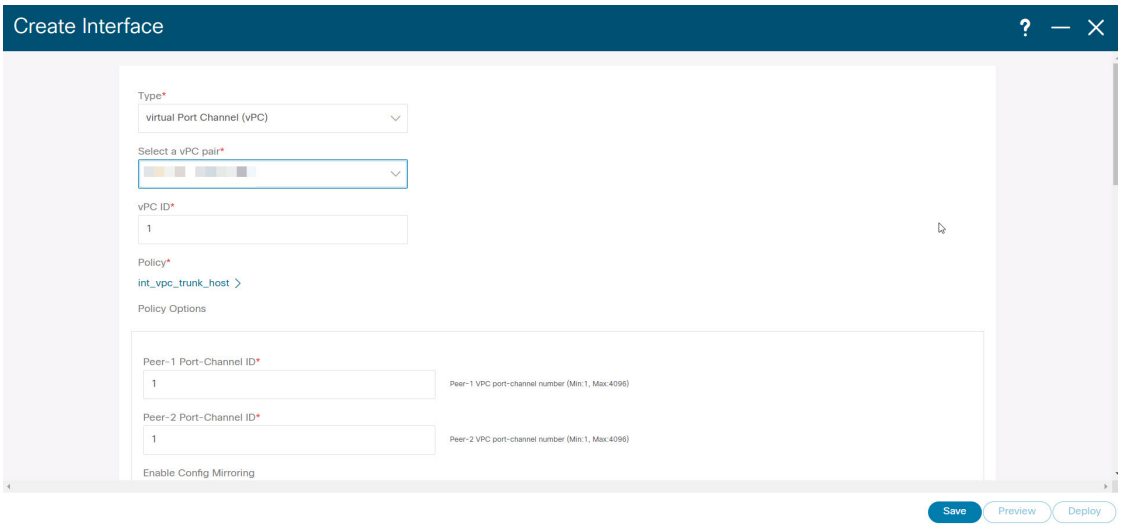
管理インターフェイスは、レイヤ 2 またはレイヤ 3 隣接の mgmt0 インターフェイスにより、デバイスに到達できるようにします。これにより、POAPを含むこれらのデバイスを管理およびモニタできます。Nexusダッシュボード ファブリック コントローラEPLでは、とルートリフレクタの間でBGPピアリングが必要です。Nexusダッシュボード ファブリック コントローラNexusデバイスのBGPプロセスは通常、デフォルトVRFで実行されるため、からファブリックへのインバンドIP接続が必要です。Nexusダッシュボード ファブリック コントローラデータ ネットワーク インターフェイスは、Nexusダッシュボードのインストール中に構成できます。構成されたインバンド ネットワーク構成を変更することはできません。

Note Nexusダッシュボード ファブリック コントローラ 上のデータ ネットワーク インターフェイスのセットアップは、ファブリック内のデバイスへのインバンド接続を必要とするアプリケーションの前提条件です。これには EPL とネットワーク インサイトのリソース（NIR）が含まれます。

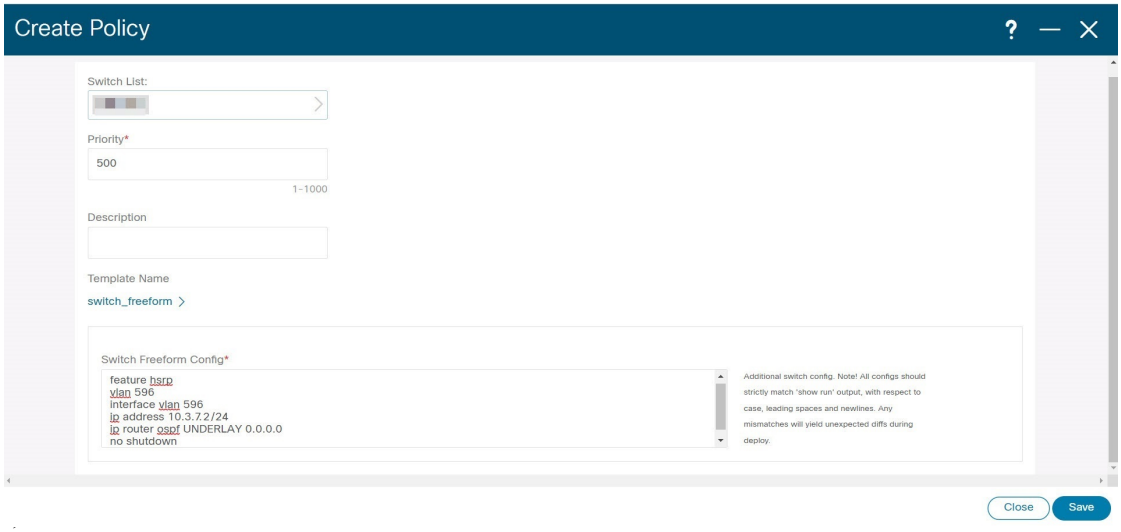
ファブリック側では、スタンドアロン Nexusダッシュボード ファブリック コントローラ 展開の場合、Nexus Dashboard データ ネットワーク ポートがリーフ上のフロントエンド インターフェイスの 1 つに直接接続されていれば、そのインターフェイスを **epl_routed_intf** テンプレートを使用して設定できます。ファブリック内のIGPとしてIS-ISまたはOSPFを使用する場合の、このシナリオの例を以下に示します。



ただし、冗長性を確保するために、がインストールされているサーバをデュアルホームまたはデュアル接続にすることをお勧めします。Nexusダッシュボード ファブリック コントローラ OVA導入では、ポートチャネルを介してサーバをスイッチに接続できます。Nexusダッシュボードファブリック コントローラこれにより、リンクレベルの冗長性が提供されます。ネットワーク側のノードレベルの冗長性を確保するために、サーバをリーフスイッチのvPCペアに接続することもできます。このシナリオでは、HSRP VIP が Nexusダッシュボード ファブリック コントローラ 上のデータ ネットワーク インターフェイスのデフォルトゲートウェイとして機能するようにスイッチを構成する必要があります。



terry-leaf3 上の HSRP 構成では、次の図に示すように、**switch_freeform** ポリシーを使用できま



SVI 596 に IP アドレス 10.3.7.2/24 を使用しながら、terry-leaf3 に同様の設定を展開できます。これにより、デフォルトゲートウェイが 10.3.7.3 に設定されたデータ ネットワーク インターフェイスを介して、Nexusダッシュボード ファブリック コントローラ からファブリックへのインバンド接続が確立されます。

物理または仮想とファブリック間のインバンド接続を確立した後、BGPピアリングを確立できます。Nexusダッシュボード ファブリック コントローラ

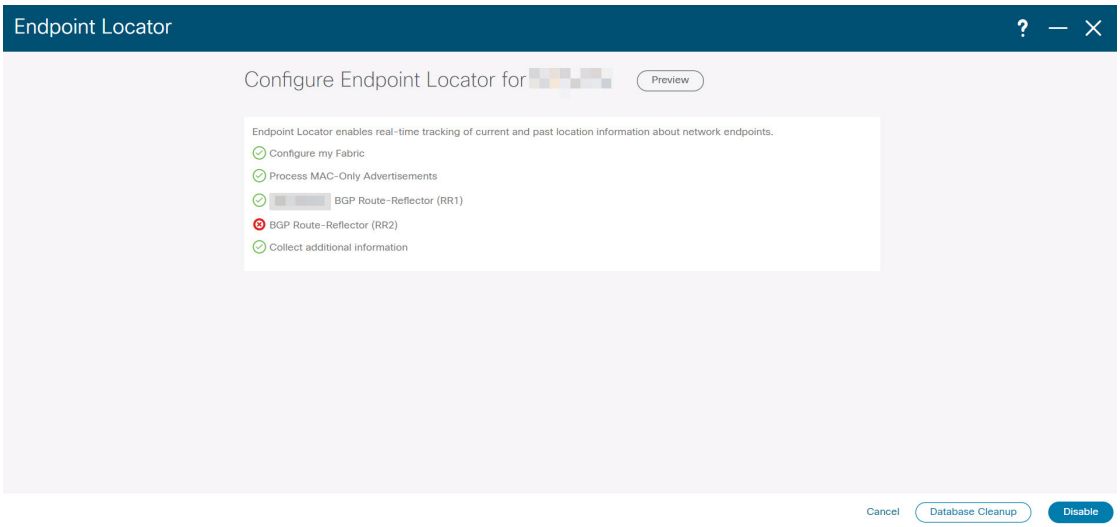
EPLの設定時に、ルートリフレクタ（RR）はBGPピアとして受け入れるように設定されます。Nexusダッシュボード ファブリック コントローラ同じ構成中、Nexusダッシュボード ファブリック コントローラは、データ ネットワーク インターフェイス ゲートウェイを介してスパイン/RR 上の BGP ループバック IP にルートを追加することによっても構成されます。

Note Cisco Nexusダッシュボード ファブリック コントローラ の EPL 機能をイネーブルにしていることを確認します。**[設定（Settings）] > [機能管理（Feature Management）] > [ファブリック コントローラ（Fabric Controller）]**を選択し、**[エンドポイント ロケータ（Endpoint Locator）]** チェックボックスをオンにします。追加された EPL の詳細をダッシュボードで表示できます。

Note シスコは、ASN、RR、IPなどのピアリングの確立に関する情報を収集するためにBGP RRを照会します。Nexusダッシュボード ファブリック コントローラ

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からエンドポイント ロケータを構成するには、[ファブリックの概要（Fabric Overview）]ページで、**[アクション（Actions）]> [その他（More）] > [エンドポイント ロケータの構成（Configure Endpoint Locator）]**を選択します。同様に、[トポロジ（Topology）] ページで EPL を構成し、必要なファブリックを右クリックして、**[その他（More）] > [エンドポイント ロケータの構成（Configure Endpoint**

Locator）]をクリックします。**[エンドポイント ロケータ（Endpoint Locator）]** ウィンドウが表示されます。



一度に1つのファブリックに対してEPLを有効にできます。

ドロップダウンリストから、RRをホストするファブリック上のスイッチを選択します。シスコはRRとピアリングします。Nexusダッシュボード ファブリック コントローラ

デフォルトでは、**[マイ ファブリックを構成（Configure My Fabric）]** オプションが選択されています。このノブは、EPL機能の有効化の一環として、選択したスパイン/ RRにBGP設定をプッシュするかどうかを制御します。EPL BGPネイバーシップのカスタムポリシーを使用してスパイン/RRを手動で設定する必要がある場合は、このオプションをオフにします。モニタされているだけで設定されていない外部ファブリックの場合、このオプションはグレー表示されます。Nexusダッシュボード ファブリック コントローラNexusダッシュボード ファブリック コントローラ

EPL機能の設定時にMAC専用アドバタイズメントの処理を有効にするには、[Process MAC-Only Advertisements]オプションを選択します。

Note [Process Mac-Only Advertisements]チェックボックスをオンまたはオフにしてEPLをファブリックで有効にし、後でこの選択を切り替える場合は、まずEPLを無効にしてから、[データベースのクリーンアップ（Database Clean-up）]をクリックしてエンドポイントデータを削除してから、EPLを再度有効にします。必要な[Macのみのアドバタイズメントの処理（Process Mac-Only Advertisements）]設定を使用します。

[追加情報の収集（Collect Additional Information）] で **[はい（Yes）]**を選択し、EPL 機能を有効にしながら PORT、VLAN、VRF などの追加情報の収集を有効にします。追加情報を収集するには、スイッチ、ToR、およびリーフでNX-APIがサポートされ、有効になっている必要があります。**[いいえ（No）]** オプションを選択すると、この情報は EPL によって収集および報告されません。

Note 外部ファブリックを除くすべてのファブリックでは、NX-APIがデフォルトで有効になっています。外部ファブリックの場合、External_Fabric_11_1ファブリックテンプレートの[Advanced]タブで[Enable NX-API]チェックボックスをオンにして、外部ファブリック設定でNX-APIを有効にする必要があります。

[i]アイコンをクリックすると、EPLを有効にしている間にスイッチにプッシュされる設定のテンプレートが表示されます。この設定は、外部モニタ対象ファブリックでEPLを有効にするために、スパインまたは境界ゲートウェイデバイスにコピーアンドペーストできます。

適切な選択を行い、さまざまな入力を確認したら、[送信（Submit）]をクリックしてEPLを有効にします。EPLの有効化中にエラーが発生した場合は、有効化プロセスが中止され、適切なエラーメッセージが表示されます。それ以外の場合、EPLは正常に有効化されます。

Nexus ダッシュボード データ サービスの IP は、BGP ネイバーとして使用されます。

エンドポイントロケータ機能を有効にすると、バックグラウンドでいくつかの手順が実行されます。選択したRRに接続し、ASNを決定します。Nexusダッシュボード ファブリック コントローラまた、BGPプロセスにバインドされているインターフェイスIPも決定します。また、eBGPアンダーレイの場合は、から開始されるBGP接続を受け入れる準備をするために、適切なBGPネイバーステートメントがRRまたはスパインに追加されます。Nexusダッシュボード ファブリック コントローラEPL ポッドに割り当てられている外部 Nexus ダッシュボード データ サービスの IP アドレスは、BGP ネイバーとして追加されます。EPLが正常に有効化されると、ユーザは自動的にEPLダッシュボードにリダイレクトされ、ファブリック内に存在するエンドポイントの運用上および探索的洞察が示されます。

EPL ダッシュボードの詳細については、エンドポイント ロケータの監視, on page 301を参照してください。

エンドポイントデータベースのフラッシュ

エンドポイントロケータ機能を有効にすると、すべてのエンドポイント情報をクリーンアップまたはフラッシュできます。これにより、エンドポイントに関する古い情報がデータベースに存在しないことを確認するために、クリーンな状態から開始できます。データベースがクリーンになると、BGPクライアントはBGP RRから学習したすべてのエンドポイント情報を再入力します。以前にEPL機能が無効にされていたファブリックでEPL機能を再度有効にしていない場合でも、エンドポイントデータベースをフラッシュできます。

Cisco Web UIからすべてのエンドポイントロケータ情報を消去するには、次の手順を実行します。Nexusダッシュボード ファブリック コントローラ

Procedure

ステップ 1 [Endpoint Locator]の[Configure]を選択し、[Database Clean-Up]をクリックします。

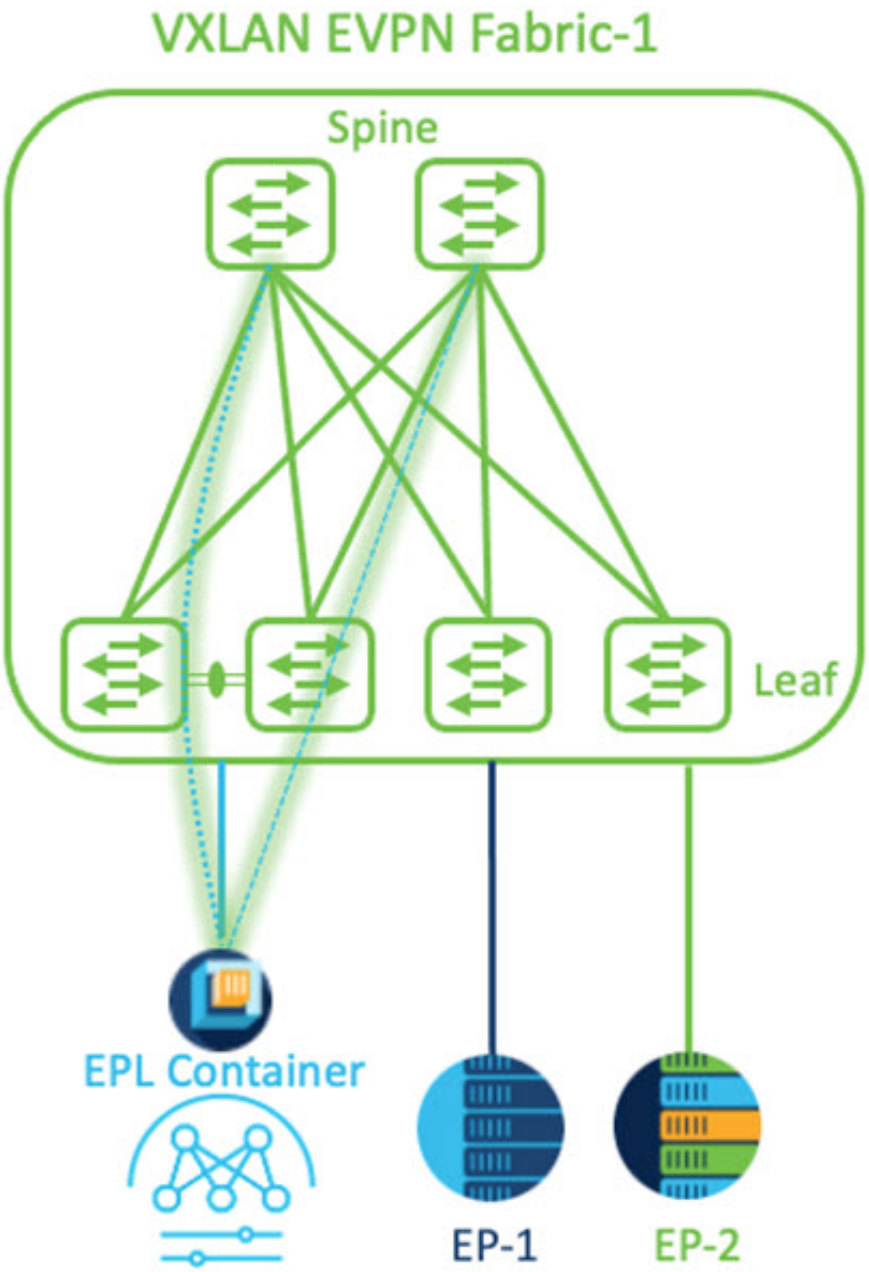
ステップ 2 [Delete]をクリックして続行するか、[Cancel]をクリックして中止します。

単一の VXLAN EVPN サイトのエンドポイント ロケータの構成

単一の VXLAN EVPN サイトのエンドポイント ロケータを構成するには、次の手順を実行します。

始める前に

次の図では、NDFC サービス アプリケーションは、リンクおよびノード レベルの冗長性を提供するため、リーフ スイッチの VPC ペアに接続されています。EPL コンテナで実行されている BGP インスタンスは、ファブリック スパインとの iBGP ピアリングを確立します。iBGP ピアリングは、スパイン ループバック アドレス（loopback0）と、EPL コンテナの永続的 IP アドレスの間で形成されます。スパインの loopback0 アドレスは VXLAN アンダーレイを介して到達可能であるため、EPL コンテナ IP にはスパインへの IP 到達可能性が必要です。IP 接続を提供できるリーフ スイッチに SVI を設定できます。SVI は非 VXLAN 対応 VLAN になり、アンダーレイにのみ参加します。



手順

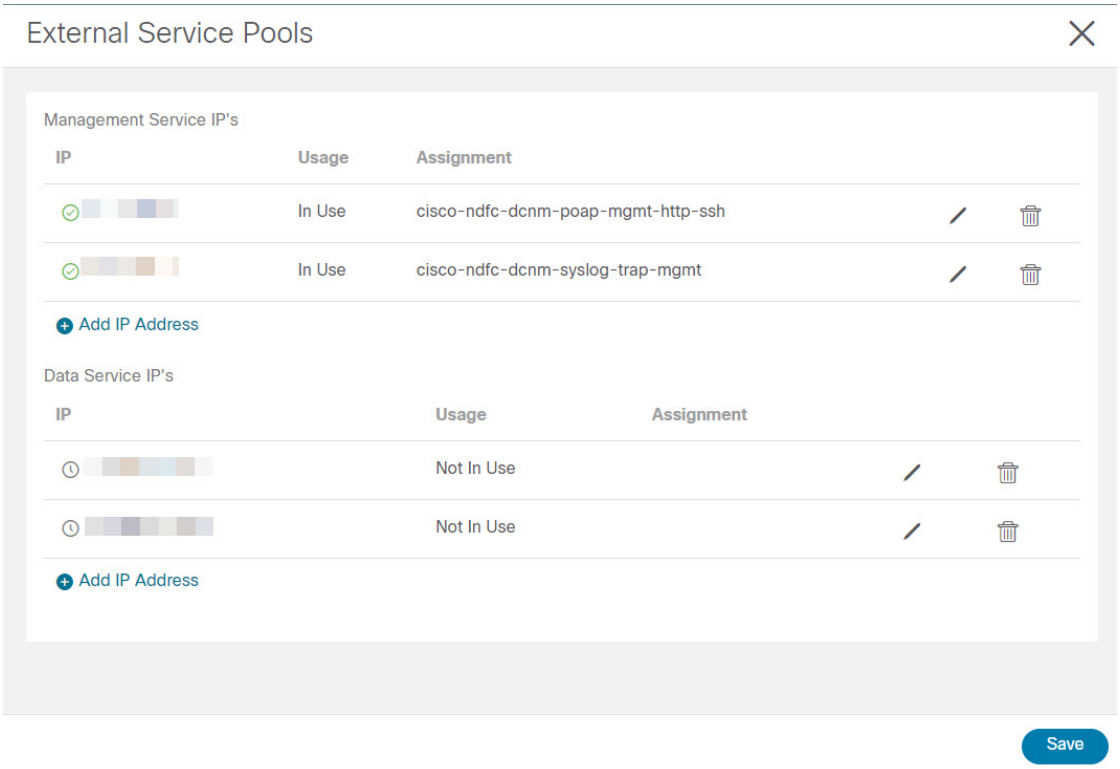
ステップ 1 Cisco Nexus Dashboard で永続 IP アドレスを構成する必要があります。Nexus Dashboard で、**[管理コンソール（Admin Console）]** > **[インフラストラクチャ（Infrastructure）]** > **[クラスタ構成（Cluster Configuration）]**を選択します。

ステップ 2 **[全般（General）]** タブの、**[外部サービス プール（External Service Pools）]** カードで、**[編集（Edit）]** アイコンをクリックします。

[外部サービスプール（External Service Pools）] ウィンドウが表示されます。

ステップ 3 **[データ サービス IP（Data Service IP's）]** に永続的 IP アドレスを入力し、**[チェック（check）]** アイコンをクリックします。

（注） IP アドレスは、Nexus ダッシュボード データ プールに関連付ける必要があります。単一のサイトの EP を視覚化および追跡するには、単一の永続的な IP アドレスが必要です。



ステップ 4 ND データ インターフェイスおよびアンダーレイ IP 接続に FHRP を使用するように SVI を構成します。

ファブリック リーフ 1 で **switch_freeform** ポリシーを使用できます。

自由形式ポリシーを作成するには、次の手順を実行します。

a) **[LAN]** > **[ファブリック（Fabrics）]** を選択し、必要なファブリックをダブルクリックします。

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

b) **[ポリシー（Policy）]** タブで、**[アクション（Actions）]** > **[ポリシーの追加（Add Policy）]** の順に選択します。

[ポリシーの追加（Add Policy）] ウィンドウが表示されます。

c) **[スイッチ リスト（Switch List）]** ドロップダウン リストから適切な Leaf1 スイッチを選択し、**[テンプレートの選択（Choose Template）]** をクリックします。

d) **[ポリシー テンプレートの選択（Select Policy Template）]** ウィンドウで、**switch_freeform** テンプレートを選択し、**[選択（Select）]** をクリックします。

FHRP 構成を適用し、テンプレートを保存します。

テンプレート構成を展開します。

この例では、ファブリック リーフ 1 で作成された HSRP ゲートウェイを備えた SVI 100 です。同様に、ファブリック リーフ 2 の手順を繰り返します。

以下の設定例をご覧ください：

```
feature hsrp
vlan 100
name EPL-Inband
interface Vlan100
  no shutdown
  no ip redirects
  ip address 192.168.100.252/24
  no ipv6 redirects
  ip router ospf 100 area 0.0.0.0
  hsrp 100
    ip 192.168.100.254
```

ステップ 5 Nexus ダッシュボード データ インターフェイスとファブリック スイッチ間の IP 到達可能性を確認します。

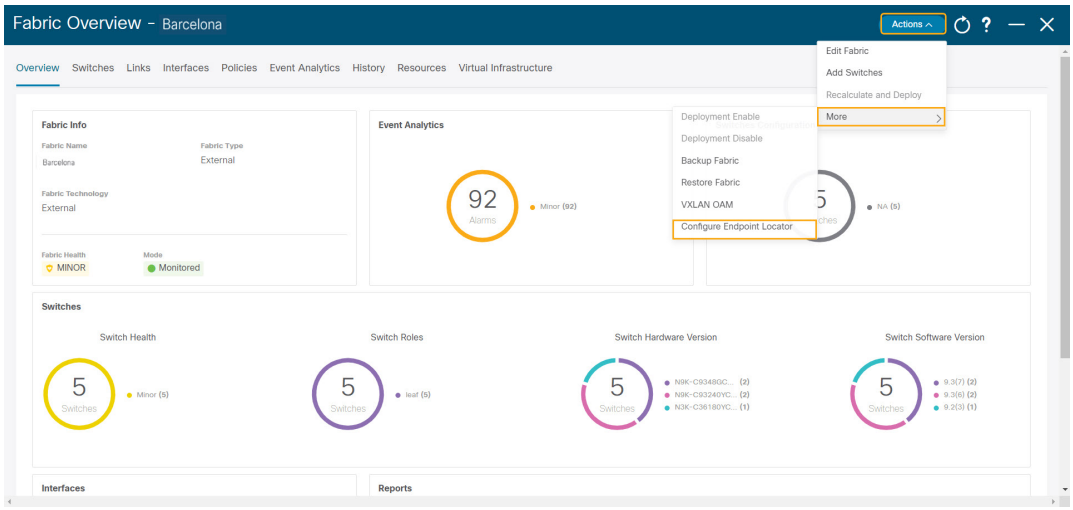
```
[rescue-user@ndfc-12-parth ~]$ ping 192.168.100.254 -c 2
PING 192.168.100.254 (192.168.100.254) 56(84) bytes of data.
64 bytes from 192.168.100.254: icmp_seq=1 ttl=255 time=1.95 ms
64 bytes from 192.168.100.254: icmp_seq=2 ttl=255 time=2.09 ms

--- 192.168.100.254 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 1.950/2.021/2.093/0.084 ms
[rescue-user@ndfc-12-parth ~]$
```

ステップ 6 ファブリック レベルで EPL を有効にします。

a) EPL を設定するには、**[LAN]** > **[ファブリック（Fabrics）]** > **[ファブリックの概要（Fabric Overview）]** を選択します。

b) **[ファブリックの概要（Fabric Overview）]** ウィンドウで、**[アクション（Actions）]** > **[その他（More）]** > **[エンドポイント ロケータの構成（Configure EndPoint Locator）]** を選択します



c) ドロップダウンリストから、スパイン/ルートリフレクタ RR をホストするファブリック上の適切なスイッチを選択します。

ノブ コントロールの **[マイ ファブリックの構成（Configure my Fabric）]** オプションを選択します。

これは、EPL 機能の有効化の一環として、選択したスパイン/ RR に BGP 設定をプッシュするかどうかを制御します。EPL BGP ネイバーシップのカスタム ポリシーを使用してスパイン/RR を手動で設定する必要がある場合は、このオプションをオフにします。モニタリングされているだけで構成されていない外部ファブリックの場合、このオプションはグレー表示されます。これらのファブリックは NDFC で構成されていないためです。

EPL 機能の設定時に MAC 専用アドバタイズメントの処理を有効にするには、**[MAC 専用アドバタイズメントを処理（Process MAC-Only Advertisements）]** オプションを選択します。

（注） **[MAC 専用アドバタイズメントを処理（Process Mac-Only Advertisements）]** チェックボックスをオンまたはオフにして EPL をファブリックで有効にしてから、後ほどこの選択を切り替える場合は、まず EPL を無効にしてから **[データベースのクリーンアップ（Database Clean-up）]** をクリックしてエンドポイント データを削除し、必要な **[Mac 専用アドバタイズメントを処理（Process Mac-Only Advertisements）]** 設定で EPL を再度有効にします。

[追加情報の収集（Collect Additional Information）] で **[はい（Yes）]** を選択し、EPL 機能を有効にしながら PORT、VLAN、VRF などの追加情報の収集を有効にします。追加情報を収集するには、スイッチ、ToR、およびリーフで NX-API がサポートされ、有効になっている必要があります。**[いいえ（No）]** オプションを選択すると、この情報は EPL によって収集および報告されません。

（注） 外部ファブリックを除くすべてのファブリックでは、NX-APIがデフォルトで有効になっています。外部ファブリックの場合、External_Fabric_11_1 ファブリック テンプレートで **[NX-API の有効化（Enable NX-API）]** チェックボックスをオンにして（**[詳細設定（Advanced）]**タブ）、外部ファブリック設定で NX-API を有効にする必要があります。

[プレビュー（Preview）]アイコンをクリックすると、EPL を有効にしている間にスイッチにプッシュされる設定のテンプレートが表示されます。この設定は、外部モニタ対象ファブリックでEPLを有効にするために、スパインまたは境界ゲートウェイデバイスにコピーアンドペーストできます。

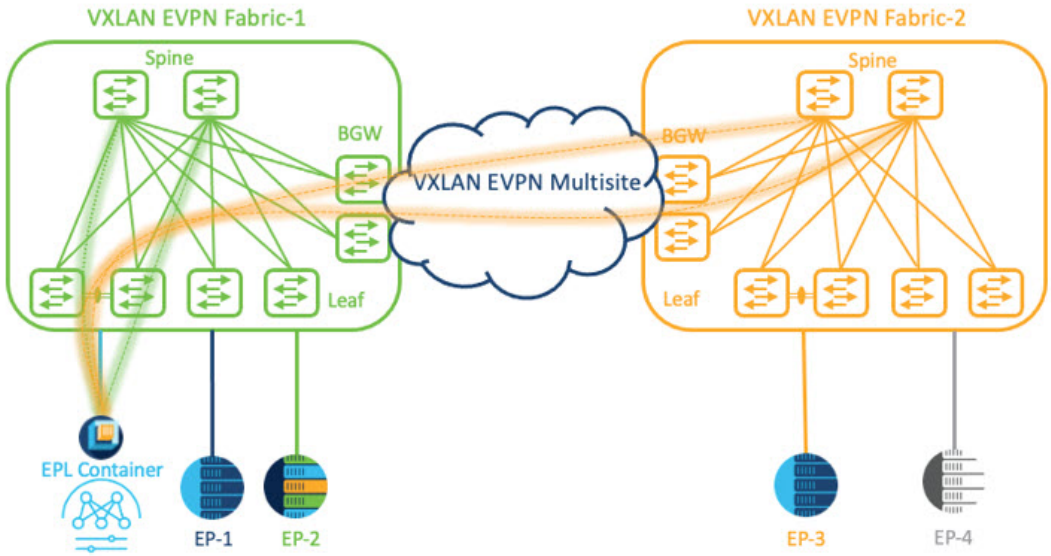
適切な選択を行い、さまざまな入力を確認したら、**[構成の保存（Save Config）]**をクリックして、EPL を有効にします。EPL の有効化中にエラーが発生した場合は、有効化プロセスが中止され、適切なエラーメッセージが表示されます。それ以外の場合、EPLは正常に有効化されます。EPL が有効になると、永続 IP が使用されます。

VXLAN EVPN マルチサイトを使用したマルチファブリックのエンドポイント ロケータの構成

マルチファブリック VXLAN EVPN マルチサイトのエンドポイント ロケータを構成するには、次の手順を実行します。

始める前に

次の図では、VXLAN EVPN マルチサイトを使用してマルチファブリックの EPL を有効にしています。BGP ピアリングは、各 VXLAN EVPN サイトのスパイン/RR と NDFC EPL コンテナの間で確立されます。永続的な IP は、VXLAN EVPN サイトの数に基づいて必要です。Cisco ND クラスタでホストされる NDFC アプリケーションは、サイト 1 にあります。リモート サイトに展開されたスパイン/RR に到達するためのルーティング情報は、マルチサイト全体で交換する必要があります。BGP セッションが形成されると、ファブリック 2 のローカル EP を可視化して追跡できます。



デフォルトでは、Nexus Dashboard データ インターフェイスおよびサイト 2 のスパイン/RR ループバックのプレフィックスは、BGW 全体にはアドバタイズされません。したがって、プレフィックスは、サイト全体でカスタム ルート マップとプレフィックス リストを使用して交換する必要があります。同時に、スパイン/RR ループバック プレフィックスは OSPF プロトコルの一部であり、BGW は BGP を使用して相互にピアリングするため、OSPF と BGP 間のルート再配布が必要です。

手順

ステップ 1 Cisco Nexus Dashboard で永続 IP アドレスを構成する必要があります。Nexus Dashboard で、**[管理コンソール（Admin Console）]**>**[インフラストラクチャ（Infrastructure）]**>**[クラスタ構成（Cluster Configuration）]**を選択します。

ステップ 2 **[全般（General）]** タブの、**[外部サービス プール（External Service Pools）]** カードで、**[編集（Edit）]** アイコンをクリックします。

[外部サービスプール（External Service Pools）] ウィンドウが表示されます。

ステップ 3 **[データ サービス IP（Data Service IP's）]** に永続的 IP アドレスを入力し、**[チェック（check）]** アイコンをクリックします。

（注） IP アドレスが Nexus ダッシュボード データ プールに関連付けられていることを確認します。2 つのメンバー ファブリックを持つマルチサイトの EP を可視化して追跡するには、2 つの永続的な IP アドレスが必要です。1 つの永続データ IP アドレスは EPL コンテナ IP として使用され、サイト 1 ファブリックとの BGP セッションが確立されます。サイト 2 ファブリックとのピアリングに使用できる新しい永続 IP アドレスが構成されます。

ステップ 4 VXLAN EVPN ファブリックのルート再配布を構成します。

ファブリック 1 のルート再配布

次の switch_freeform ポリシーは、ファブリック 1 BGW で使用できます。新しい **switch_freeform** ポリシーを作成するには、上記の例を参照してください。

下のサンプル構成例

```
ip prefix-list site-2-rr seq 5 permit 20.2.0.1/32 >> Site 2 RR
ip prefix-list site-2-rr seq 6 permit 20.2.0.2/32 >> Site 2 RR
ip prefix-list epl-subnet seq 5 permit 192.168.100.0/24 >> EPL Subnet

route-map bgp-to-ospf permit 10
   match ip address prefix-list site-2-rr
route-map ospf-to-bgp permit 10
   match ip address prefix-list epl-subnet

router ospf 100
   redistribute bgp 100 route-map bgp-to-ospf

router bgp 100
   address-family ipv4 unicast
       redistribute ospf 100 route-map ospf-to-bgp
```

ファブリック 2 のルート再配布

次の switch_freeform ポリシーは、ファブリック 2 BGW で使用できます。新しい **switch_freeform** ポリシーを作成するには、上記の例を参照してください。

下のサンプル構成例

```
ip prefix-list site-2-rr seq 5 permit 20.2.0.1/32 >> Site 2 RR
ip prefix-list site-2-rr seq 6 permit 20.2.0.2/32 >> Site 2 RR
ip prefix-list epl-subnet seq 5 permit 192.168.100.0/24 >> EPL Subnet

route-map bgp-to-ospf permit 10
  match ip address prefix-list epl-subnet
route-map ospf-to-bgp permit 10
  match ip address prefix-list site-2-rr

router ospf 200
  redistribute bgp 200 route-map bgp-to-ospf

router bgp 200
    address-family ipv4 unicast
        redistribute ospf 200 route-map ospf-to-bgp
```

ステップ 5 EPL を設定するには、**[LAN]** > **[ファブリック（Fabrics）]** > **[ファブリックの概要（Fabric Overview）]** を選択します。

ステップ 6 **[ファブリックの概要（Fabric Overview）]** ウィンドウで、**[アクション（Actions）]** > **[その他（More）]** > **[エンドポイント ロケータの構成（Configure EndPoint Locator）]** を選択します

ステップ 7 ドロップダウンリストから、スパイン/ルート リフレクタ RR をホストするファブリック上の適切なスイッチを選択します。

適切な選択を行い、さまざまな入力を確認したら、**[構成の保存（Save Config）]**をクリックして、EPL を有効にします。EPLの有効化中にエラーが発生した場合は、有効化プロセスが中止され、適切なエラーメッセージが表示されます。それ以外の場合、EPLは正常に有効化されます。EPL が有効になると、永続 IP が使用されます。

ファブリック 1 およびファブリック 2 で有効になっている EPL は正常に表示できます。EP を表示および追跡するには、エンドポイント ロケータの監視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 スイッチのエンドポイント ロケータの構成

ネットワーク管理者は、物理ピア リンクまたは仮想ピア リンクを使用して、スイッチのペア間に vPC を作成できます。 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オーバーヘッドのない、拡張された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。仮想ピア リンクの場合でも、リンクおよびノード レベルの冗長性のために、EPL は引き続きリーフ スイッチの vPC ペアに接続できます。ただし、EPL の最初のホップとして VXLAN VLAN（エニーキャスト ゲートウェイ）が使用されます。VXLAN VLAN はテナント VRF の一部になりますが、スパイン/RR の loopback0 アドレスは、VXLAN アンダーレイを介してのみ到達可能です。そのため、IP 通信を確立するために、テナント VRF とデフォルト VRF の間でルートリーキングが構成されます。詳細については、vPC ファブリック ピアリングの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 スイッチのエンドポイント ロケータを構成するには、次の手順を実行します。

手順

ステップ 1 Cisco Nexus Dashboard で永続 IP アドレスを構成する必要があります。Nexus Dashboard で、**[管理コンソール（Admin Console）]**>**[インフラストラクチャ（Infrastructure）]**>**[クラスタ構成（Cluster Configuration）]**を選択します。

ステップ 2 **[全般（General）]** タブの、**[外部サービス プール（External Service Pools）]** カードで、**[編集（Edit）]** アイコンをクリックします。

[外部サービスプール（External Service Pools）] ウィンドウが表示されます。

ステップ 3 **[データ サービス IP（Data Service IP's）]** に永続的 IP アドレスを入力し、**[チェック（check）]** アイコンをクリックします。

ステップ 4 vPC ファブリック ピアリング スイッチでテナント VRF およびエニーキャスト ゲートウェイを作成します。

2 つのイメージを追加

ステップ 5 テナント VRF とデフォルト VRF 間のルート リークを構成します。

テナント VRF からデフォルト VRF にアドバタイズします。

次の switch_freeform ポリシーは、ND が接続されているファブリック リーフで使用できます。

```
ip prefix-list vrf-to-default seq 5 permit 192.168.100.0/24 >> EPL subnet
route-map vrf-to-default permit 10
  match ip address prefix-list vrf-to-default
vrf context epl_inband
  address-family ipv4 unicast
    export vrf default map vrf-to-default allow-vpn
```

```
router ospf UNDERLAY
   redistribute bgp 200 route-map vrf-to-default
```

デフォルト VRF からテナント VRF にアドバタイズします。

次の switch_freeform ポリシーは、ND が接続されているファブリック リーフで使用できます。

```
ip prefix-list default-to-vrf seq 5 permit 20.2.0.3/32 >> Spine loopback IP
ip prefix-list default-to-vrf seq 6 permit 20.2.0.4/32 >> Spine loopback IP
route-map default-to-vrf permit 10
   match ip address prefix-list default-to-vrf
vrf context epl_inband
   address-family ipv4 unicast
       import vrf default map default-to-vrf
        router bgp 200
   address-family ipv4 unicast
       redistribute ospf UNDERLAY route-map default-to-vrf
```

ステップ 6 ファブリック レベルで EPL を有効にします。

a) EPL を設定するには、**[LAN]** > **[ファブリック（Fabrics）]** > **[ファブリックの概要（Fabric Overview）]** を選択します。

b) **[ファブリックの概要（Fabric Overview）]** ウィンドウで、**[アクション（Actions）]**>**[その他（More）]** > **[エンドポイント ロケータの構成（Configure EndPoint Locator）]** を選択します

c) ドロップダウンリストから、スパイン/ルートリフレクタ RR をホストするファブリック上の適切なスイッチを選択します。

適切な選択を行い、さまざまな入力を確認したら、**[構成の保存（Save Config）]**をクリックして、EPL を有効にします。EPLの有効化中にエラーが発生した場合は、有効化プロセスが中止され、適切なエラーメッセージが表示されます。それ以外の場合、EPLは正常に有効化されます。EPL が有効になると、永続 IP が使用されます。

外部ファブリックのエンドポイント ロケータの構成

Nexusダッシュボードファブリック コントローラ では、Easy ファブリックに加えて、外部ファブリックにインポートされるスイッチで構成される VXLAN EVPN ファブリックの EPL を有効にできます。外部ファブリックは、の **[ファブリック モニタ モード (Fabric Monitor Mode)]** フラグ **([外部ファブリック設定 (External Fabric Settings)])** の選択に基づいて、管理対象モードまたはモニタ対象モードにすることができます。Nexusダッシュボードファブリック コントローラからモニタのみされ、設定されていない外部ファブリックの場合、このフラグは無効になります。そのため、OOB 経由で、または CLI を使用して、スパインの BGP セッションを設定する必要があります。サンプル テンプレートを確認するには、 アイコンをクリックして、EPL を有効にしながら必要な設定を表示します。

[外部ファブリック設定 (External Fabric settings)] の **[ファブリック モニタ モード (Fabric Monitor Mode)]** チェックボックスがオフの場合でも、EPL はデフォルトの **[ファブリックの設定 (Configure my fabric)]** オプションを使用してスパイン/RRを設定できます。ただし、EPL を無効にすると、スパイン/RR のルータ bgp 設定ブロックが消去されます。これを防ぐには、BGP ポリシーを手動で作成し、選択したスパイン/RR にプッシュする必要があります。

eBGP EVPN ファブリックのエンドポイント ロケータの構成

VXLAN EVPN ファブリックの EPL は有効にできます。この場合、eBGP がアンダーレイ ルーティング プロトコルとして使用されます。eBGP EVPN ファブリック展開では、iBGP に似た従来の RR は存在しないことに注意してください。インバンド サブネットの到達可能性は、ルート サーバーとして動作するスパインにアドバタイズする必要があります。Cisco Nexusダッシュボード ファブリック コントローラ Web UIから eBGP EVPN ファブリックの EPL を設定するには、次の手順を実行します。

Procedure

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

eBGP を設定するファブリックを選択するか、**Easy_Fabric_eBGP** テンプレートを使用して eBGP ファブリックを作成します。

ステップ 2 すべてのリーフで一意の ASN を設定するには、**leaf_bgp_asn** ポリシーを使用します。

ステップ 3 各リーフに **ebgp_overlay_leaf_all_neighbor** ポリシーを追加します。

[スパイン IP リスト (Spine IP List)] にスパインの BGP インターフェイスの IP アドレス（通常は loopback0 の IP アドレス）を入力します。

[BGP アップデートソース インターフェイス (BGP Update-Source Interface)] にリーフの BGP インターフェイス（通常は loopback0）を入力します。

ステップ 4 **ebgp_overlay_spine_all_neighbor** ポリシーを各スパインに追加します。

[リーフ IP リスト (Leaf IP List)] にリーフの BGP インターフェイスの IP（通常は loopback0 の IP）を入力します。

[リーフの BGP ASN (Leaf BGP ASN)] に、**[リーフ IP リスト (Leaf IP List)]** と同じ順序でリーフのASNを入力します。

[BGP アップデートソース インターフェイス (BGP Update-Source Interface)] に、スパインの BGP インターフェイス（通常は loopback0）を入力します。

インバンド接続が確立された後も、EPL機能の有効化の状態はそれまでにリストされていたものと同じままです。EPL は、スパインで実行されているルート サーバーの iBGP ネイバーになります。

エンドポイント ロケータの監視

エンドポイント ロケータに関する情報は、単一のランディング ページまたはダッシュボードに表示されます。ダッシュボードには、すべてのアクティブなエンドポイントに関するデータがほぼリアルタイムで（30秒ごとに更新されて）1つのペインに表示されます。このダッシュボードに表示されるデータは、**[範囲（Scope）]** ドロップダウン リストで選択した範囲によっ

て異なります。Nexusダッシュボード ファブリック コントローラ 範囲階層はファブリックから始まります。ファブリックは、マルチサイト ドメイン（MSD）にグループ化できます。MSDのグループはデータセンターを構成します。エンドポイント ロケータ ダッシュボードに表示されるデータは、選択した範囲に基づいて集約されます。このダッシュボードから、[エンドポイント履歴（Endpoint History）]、[エンドポイント検索（Endpoint Search）]、および[エンドポイント寿命（Endpoint Life）] にアクセスできます。

エンドポイント ロケータの削除

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からエンドポイント ロケータを無効にするには、次の手順を実行します。

Procedure

ステップ 1 **[エンドポイント ロケータ（Endpoint Locator）] > [設定（Configure）]** を選択します。

[エンドポイント ロケータ（Endpoint Locator）] ウィンドウが表示されます。**[範囲（SCOPE）]** ドロップダウン リストから必要なディスクを選択します。選択したファブリックのファブリック設定詳細が表示されます。

ステップ 2 [無効（Disable）] をクリックします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。