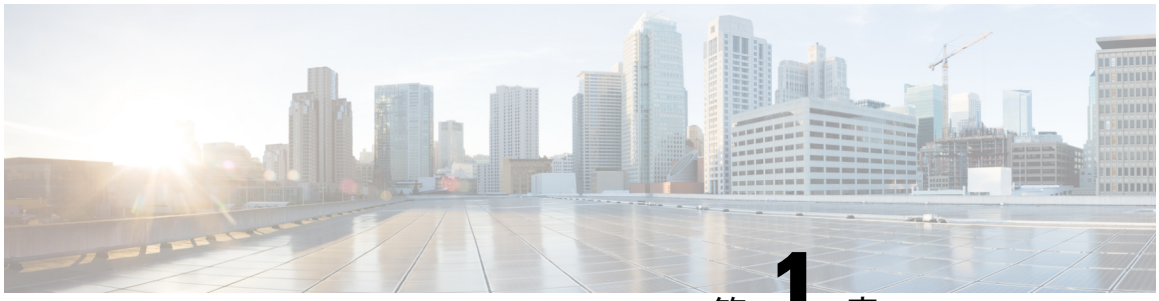
Cisco NDFC ファブリック コントローラ 構成ガイド、リリース 12.0.x

初版：2021 年 9 月 30 日

最終更新：2022 年 2 月 7 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。



第 1 章

概要

Web UI を理解する

Cisco Nexusダッシュボード ファブリック コントローラ Web UIを初めて起動すると、**[機能管理（Feature Management）]** ウィンドウが開きます。展開タイプを選択すると、左側のペインにパーソナリティに関連するメニューが表示されます。

上部ペインには、次の UI 要素が表示されます。

- **[ホーム（Home）]** アイコン：クリックして Nexus ダッシュボードセットアップの 1 つのビューを表示します。
- **[Nexus ダッシュボード（Nexus Dashboard）]**：クリックして、Nexus ダッシュボードセットアップの 1 つのビューを表示します。
- **フィードバック**：Cisco Nexusダッシュボード ファブリック コントローラ に関するフィードバックを提供できます。この説明については、ユーザフィードバック （3 ページ） を参照してください。
- **[ヘルプ（Help）]**：**[ヘルプ（Help）]** をクリックすると、次のオプションを含むドロップダウンリストが表示されます。
  - **Nexusダッシュボードについて**：Cisco Nexusダッシュボード ファブリック コントローラ が導入されているCisco Nexusダッシュボードのバージョンを表示します。
  - **ウェルカム画面**：最新情報を表示します。Web UI を起動するたびに、このページを表示するかどうかを選択できます。
  - **[ヘルプセンター（Help Center）]**：クリックすると、[ヘルプセンター（Help Center）] ページが表示されます。このページからさまざまな製品ドキュメントにアクセスできます。

ページの最後までスクロールして、Nexus Dashboard にインストールされているサービスを表示します。サービスをクリックして **[ヘルプセンター（Help Center）]** を表示します。

- **[ユーザーロール（User Role）]**：現在ログインしているユーザーのロール（**admin**など）が表示されます。ユーザー名をクリックすると、次のオプションを含むドロップダウンリストが表示されます。
  - **[ユーザー設定（User Preferences）]**：ログインするたびにウェルカム画面を表示するかどうかを設定できます。
  - **[パスワードの変更（Change Password）]**：現在のログインユーザのパスワードを変更できます。

    ネットワーク管理者ユーザの場合、他のユーザのパスワードを変更できます。
  - **[ログアウト（Logout）]**：Web UI を終了し、ログイン画面に戻ります。
- **[Cisco Nexusダッシュボード ファブリック コントローラ Persona]**：展開ペルソナを指定します – **ファブリックコントローラ**、**SAN コントローラ**、または**ファブリック検出**。
- **[アラートと通知（Alerts and Notifications）]**：Cisco Nexusダッシュボード ファブリック コントローラ の上部ペインにある **[ヘルプ（Help）]** アイコンの横にある[アラートと通知（Alerts and Notifications）]アイコンをクリックすると、アラートとイベント通知を表示できます。
- **[アラーム（Alarms）]**：**[アラーム（Alarms）]**アイコンは、[アラーム（Alarm）]がある場合、またはCisco Nexusダッシュボード ファブリック コントローラ 展開のしきい値を超えた場合に点滅します。メッセージを表示するには、点滅している **[アラーム（Alarms）]** アイコンをクリックします。次のアラームが表示されます。
  - **[インターフェイスの制限を超えた（Interfaces Limit Exceeded）]**：すべてのファブリックのエンドポイントの最大数が 100K を超えると、アラームアイコンが点滅し、メッセージが表示されます。
  - **[高可用性（HA）状態（High Availability (HA) State）]**：HA 状態通知は、ネイティブ HA セットアップが同期されていない場合、ノードの 1 つまたは両方が停止、障害、または準備ができていない可能性がある場合、または[アラーム（Alarms）]アイコンが点滅している場合に表示されます。HA 設定が同期されている場合、通知は 30 分（ポーリングサイクル中）またはログアウトして Cisco Nexusダッシュボード ファブリック コントローラ Web UI にログインしたときにクリアされます。
  - **[アプリケーション ダウン（Application down）]**：1 つ以上のアプリケーションがダウンしている場合は、エラーが表示されます。アプリケーションがオンラインまたはオフラインになると、アラーム メッセージが表示されます。

UI の一般的なアイコン：

- **ハンバーガー** アイコン-ホーム画面の製品名の横にある**ハンバーガー** アイコンをクリックすれば、ホーム画面のメニュー項目を最小化することや、メニュー項目を詳細に表示することができます。
- **更新** アイコン：更新アイコンをクリックすると、画面が更新されます。

ユーザフィードバック

Cisco Nexusダッシュボードファブリック コントローラ では、アプリケーションに関するフィードバックを提供できます。この機能を使用して、新しい機能/拡張機能を要求できます。要求は Cisco Nexusダッシュボード ファブリック コントローラ のマーケティング エンジニアに送信されます。エンジニアは要件を評価し、今後のリリースに機能または拡張機能を含めます。

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

手順

ステップ 1 **[フィードバック (Feedback)]** をクリックします。これはNexusダッシュボードファブリック コントローラ アプリケーションの右上隅にあります。

これを初めて使用する場合は、Cisco Nexus ダッシュボードで DNS とプロキシ サーバーを設定する必要があります。

ステップ 2 接続を確立するには、ブラウザで **[Cisco Nexus ダッシュボード (Cisco Nexus Dashboard)]** に移動し、次の手順を実行します。

a) Cisco Nexus ダッシュボードの Web UIで、**[インフラストラクチャ (Infrastructure)]** > **[クラスタ設定 (Cluster Configuration)]** を選択します。

[クラスタ設定全般 (Cluster Configuration General)] タブが表示されます。

b) **[プロキシ設定 (Proxy Configuration)]** 領域で、**[編集 (Edit)]** アイコンをクリックします。

c) **[サーバー (Servers)]** 領域で、**[サーバーの追加 (Add Server)]** をクリックします。

d) プロトコルのタイプとして、**[HTTP]** または **[HTTPS]** を選択します。

e) **[サーバー (Server)]** フィールドに、IP アドレスを入力します。

f) **[ユーザー名 (Username)]** と **[パスワード (Password)]** をそれぞれのフィールドに入力します。

g) 「ティック」アイコンをクリックして確定します。削除するには、「間違い」アイコンをクリックします。

h) **[無視するホスト (Ignore Hosts)]** 領域で、**[無視するホストの追加 (Add Ignore Host)]** をクリックします。

i) **[ホスト名 (Hostname)]** を入力し、「ティック」アイコンをクリックして確定します。削除するには、「間違い」アイコンをクリックします。

j) **[保存 (Save)]** をクリックして、プロキシ サーバーを設定します。

（注） プロキシ設定が Nexusダッシュボード ファブリック コントローラ アプリケーションに反映されるまで、最大 5 分間待ってください。

ステップ 3 Cisco Nexusダッシュボード ファブリック コントローラ Web UIで、**[フィードバック (Feedback)]** をクリックします。

ステップ 4 **[フィードバック (Feedback)]** パネルで、星をクリックして Nexusダッシュボード ファブリック コントローラ についての感想をお聞かせください。

ステップ 5 **[提案する (Make a suggestion)]** フィールドに、提案/フィードバックを入力します。

ステップ 6 フィードバックについてシスコと連絡を取ることにした場合は、**[シスコからフィードバックについての連絡を受けてもよい (Cisco may contact me about my Feedback)]** チェックボックスをオンにします。

ステップ 7 **[名前 (Name)]** と **[電子メール (Email)]** のフィールドに名前と電子メールを入力します。

Nexus Dashboard Insights を使用した NDFC 管理モードの共同ホスティング

リリース 12.1.1e 以降、NDFC と Nexus Dashboard Insights を同じ Nexus Dashboard クラスタで管理モードでホストしてファブリックを管理し、 Nexus Dashboard Insights をホストして同じファブリックをモニタリングできます。NDFC リリース 12.0.2f では、ファブリック ディスカバリ モードの NDFC、つまり、同じ Nexus Dashboard クラスタ上の NDI を使用したモニタモードがサポートされていることに注意してください。これには、最大 50 のスイッチの最大規模の 4 つの物理的な Nexus Dashboard ノードが必要でした。この機能は、対応するペアの Nexus Dashboard Insights リリース 12.1.1e を備えた NDFC リリースでもサポートされています。

（注） KVM に展開された Nexus Dashboard は、同じ Nexus Dashboard クラスタでの NDFC と Insights サービスの共同ホスティングをサポートしていません。

（注） 同じ Nexus Dashboard クラスタで NDFC と Insights を共同ホスティングするには、Nexus Dashboard ノードがレイヤ 2 で隣接している必要があります。共同ホスティング導入のためのレイヤ 3 隣接のサポートは、将来のリリースで展開される予定です。

次の表は、Nexus Dashboard とサービスの互換性のあるバージョンを示しています。

[サービス（Services）]	互換性バージョン
Nexusダッシュボード	2.2.1h
Nexus ダッシュボード Insights	6.1.2

[サービス（Services）]	互換性バージョン
Nexus Dashboard Fabric Controller	12.1.1e

次の表は、Nexus Dashboard のシステム要件を示しています。

仕様	サポートされるスケール
物理的な Nexus Dashboard ノードの数	5
サポートされるスイッチの数	50
Nexus Dashboard Insights でサポートされるフローの数	10000

同じ Nexus Dashboard への NDFC と NDI のインストール

Cisco NDFC は、同じ Nexus Dashboard で Nexus Dashboard Insights と共同主催できます。

はじめる前に

- Cisco Nexus Dashboard の必要なフォーム ファクタがインストールされていることを確認します。手順については、『Cisco Nexus Dashboard Deployment Guide』を参照してください。
- 『Cisco NDFC インストールおよびアップグレードガイド、リリース 12.1.1e』の「前提条件」セクションに記載されている要件とガイドラインを満たしていることを確認してください。
- Cisco DC App Center は、管理ネットワークを介して直接、またはプロキシ設定を使用して Nexus Dashboard から到達可能である必要があります。Nexus Dashboard のプロキシ設定については、『Nexus Dashboard ユーザー ガイド』を参照してください。
- DC のアプリケーションセンターへの接続を確立できない場合は、このセクションをスキップして、『Nexus Dashboard ファブリック コントローラ サービスを手動でインストールする』で説明されている手順に従ってください。
- Cisco Nexus Dashboard で、サービスに IP プール アドレスが割り当てられていることを確認します。詳細については、『Cisco Nexus Dashboard ユーザー ガイド』の「クラスタの設定」の項を参照してください。

Nexus Dashboard Insights のインストール

Cisco Nexus Dashboard の必要なフォームファクタがインストールされていることを確認します。手順については、『Cisco Nexus Dashboard Deployment Guide』を参照してください。

NDFC のインストール

「Cisco Nexus Dashboard ファブリックコントローラのインストール」を参照してください。

Nexus Dashboard で NDFC サイトを設定します。手順については、『Cisco Nexus Dashboard ユーザーガイド』の「サイトの追加」セクションを参照してください。

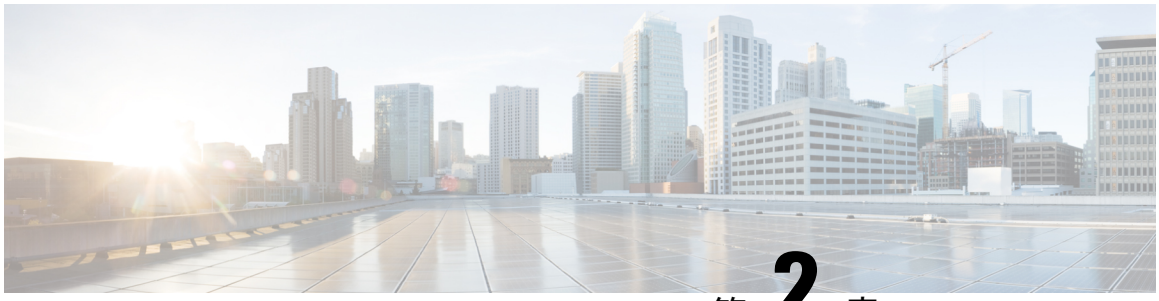
NDI のインストール

同じ Nexus Dashboard セットアップで、Nexus Dashboard Insights サービスをインストールします。詳細については、『Cisco Nexus Dashboard Insights 導入ガイド』を参照してください。

インストール後

NDFC と NDI の互換性のあるバージョンを 5 ノードの物理 Nexus ダッシュボードにインストールした後、NDFC をファブリック（LAN）コントローラとして起動します。ファブリックを作成し、NDFC ファブリックでスイッチを検出してインポートします。Nexus Dashboard は、NDFC ファブリックと [サイト（Sites）] ページのリストをエンティティとして自動的に識別します。

（注） Nexus Dashboard サイトマネージャで、各サイトのパスワードを指定する必要があります。



第 2 章

ダッシュボード

ダッシュボードの目的は、ネットワーク管理者とストレージ管理者がデータセンタースイッチングの健全性とパフォーマンスに関する特定の領域に集中できるようにすることです。この情報は、24 時間のスナップショットとして提供されます。

LAN スイッチングの機能ビューは、デフォルトで選択されたスコープのコンテキストで情報を表示する 7 つの動的ダッシュレットで構成されます。

Cisco Web Nexusダッシュボード ファブリック コントローラ UI で使用できるさまざまなスコープは次のとおりです。

概要

左側のメニューバーから **[ダッシュボード（Dashboard）]** > **[概要（Overview）]**を選択します。**[概要（Overview）]** ウィンドウに次のダッシュレットが表示されます。ダッシュレットにドーナツの概要が表示されます。

[概要（Overview）] ダッシュボード ウィンドウに表示されるデフォルトのダッシュレットは次のとおりです。

ダッシュレット	説明
ファブリック ヘルス	問題のファブリック ヘルス サマリーと、ファブリックの総数を示すドーナツの数を表示します。 **[重大（Critical）]** および **[正常（Healthy）]** のファブリック ヘルス ステータスを表示します。
イベント分析	重大度が**重大**、**エラー**、および**警告**のイベントを表示します。

ダッシュレット	説明
スイッチの構成	スイッチ モデルや対応するカウントなど、スイッチのインベントリ サマリー情報を表示します。
スイッチ	
スイッチの状態	スイッチのヘルスサマリー **Critical**（**重大**）と**正常**（**Healthy**）を対応するカウントとともに表示します。
ロールの切り替え	スイッチ ロールのサマリーと対応するカウントを表示します。アクセス、スパイン、およびリーフ デバイスの数を表示します。
スイッチ ハードウェア バージョン（Switch Hardware Version）	スイッチのモデルと対応するカウントを表示します。
スイッチ ソフトウェア バージョン	スイッチのソフトウェア バージョンと対応するカウントを表示します。
レポート	スイッチ レポートを表示します。

vCenter VM の表示

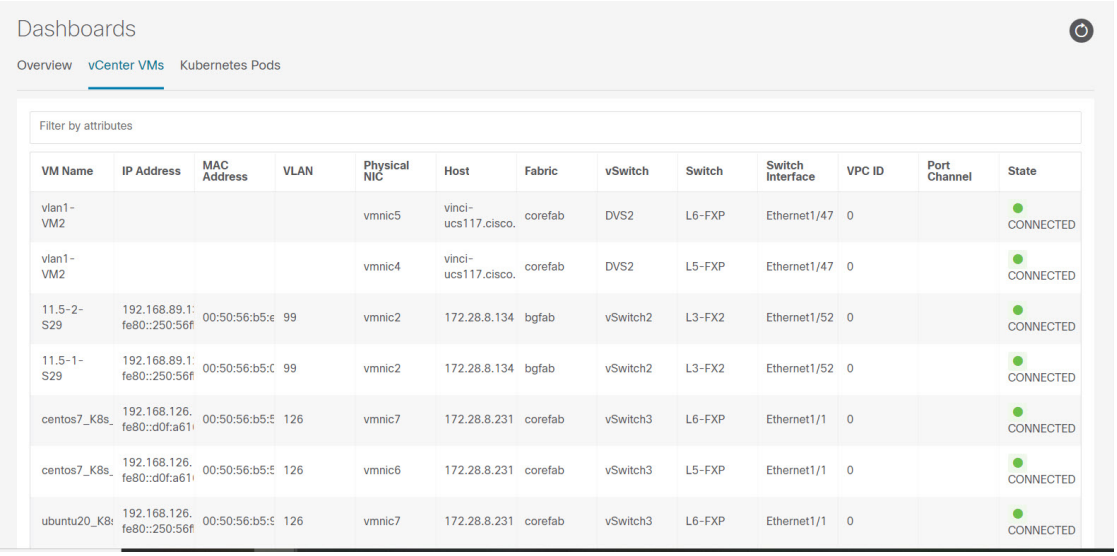
UI パス：**Dashboard** > **vCenter VMs**

（注） ダッシュボードおよびトポロジ ウィンドウで、追加された vCenter クラスタの仮想マシンの詳細を表示できます。**[ダッシュボード（Dashboard）]** > **[vCenter VM（vCenter VMs）]** に移動します。

[vCenter VM] タブには、VM の次の詳細が表示されます。

- VM 名、その IP アドレス、および MAC アドレス
- VM がホストされているコンピュータの名前
- VM に接続されているスイッチ名、スイッチの IP アドレス、MAC アドレス、およびインターフェイス
- ポート チャネル ID および vPC ID（VPC に接続されている場合）
- 構成された VLAN VM：
- VM の電源状態
- コンピュート ホストの物理 NIC

[属性によるフィルタリング（filter by attributes）] 検索フィールドを使用して、



を検索およびフィルタリングできます。

[ファブリック（Fabric）] ウィンドウでVMを表示するには、**[LAN]**>**[ファブリック（Fabrics）]** に移動し、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）]** ウィンドウで、**[仮想インフラストラクチャ（Virtual Infrastructure）]** > **[仮想マシン VM（Virtual Machine VMs）]** を選択します。

[スイッチ（Switch）] ウィンドウで VM を表示するには、**[LAN]** > **[スイッチ（Switches）]** に移動し、必要なスイッチをダブルクリックします。**[スイッチの概要（Switch Overview）]** ウィンドウで、**[仮想インフラストラクチャ（Virtual Infrastructure）]** > **[仮想マシン VM（Virtual Machine VMs）]** を選択します。

Kubernetes ポッドの表示

（注） これは、Nexus Dashboard Fabric Controller、Release 12.0.1a のフィーチャのプレビューです。ラボセットアップでのみ、ベータ版としてマークされたこの機能を使用することをお勧めします。実稼働環境でこれらのフィーチャを使用しないでください。

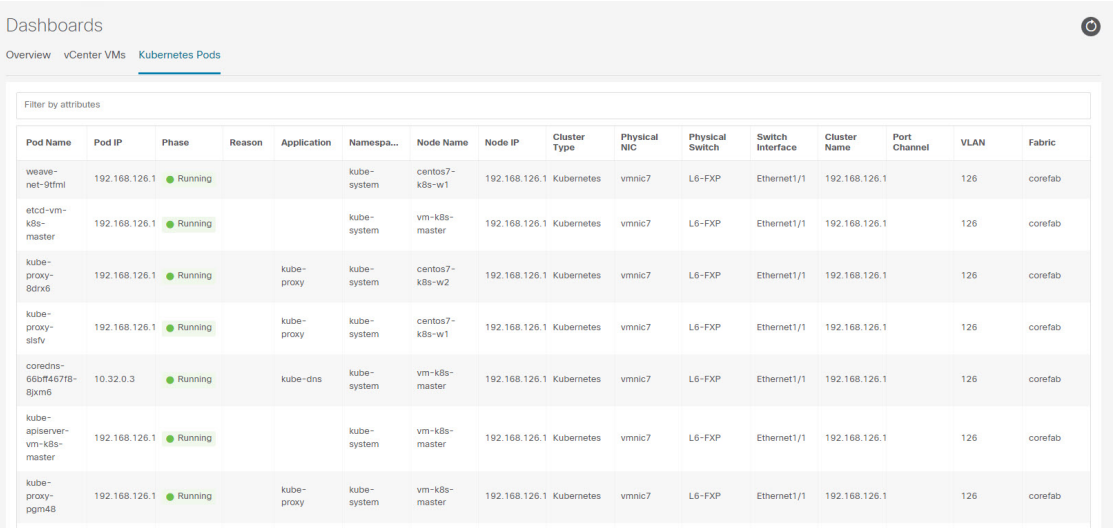
UI パス： **[ダッシュボード]** > **[Kubernetesポッド]**

[ファブリック（Fabrics）] ウィンドウで Kubernetes ポッドを表示し、**[LAN]** > **[ファブリック（Fabrics）]**に移動し、必要なファブリックをダブルクリックし、**[ファブリックの概要（Fabric Overview）]** ウィンドウに移動し、**[仮想インフラストラクチャ（Virtual Infrastructure）]** > **[Kubernetes ポッド（Kubernetes Pods）]**をクリックします。

[スイッチ（Switch）] ウィンドウでKubernetesポッドを表示し、**[LAN]** > **[スイッチ（Switches）]** に移動し、必要なスイッチをダブルクリックし、**[スイッチの概要（Switch Overview）]** ウィン

ドウに移動し、**[仮想インフラストラクチャ（Virtual Infrastructure）] > [Kubernetes ポッド（Kubernetes Pods）]** をクリックします。

属性フィルタ検索フィールドでを使用して、kubernetes ポッドを検索およびフィルタリングできます。



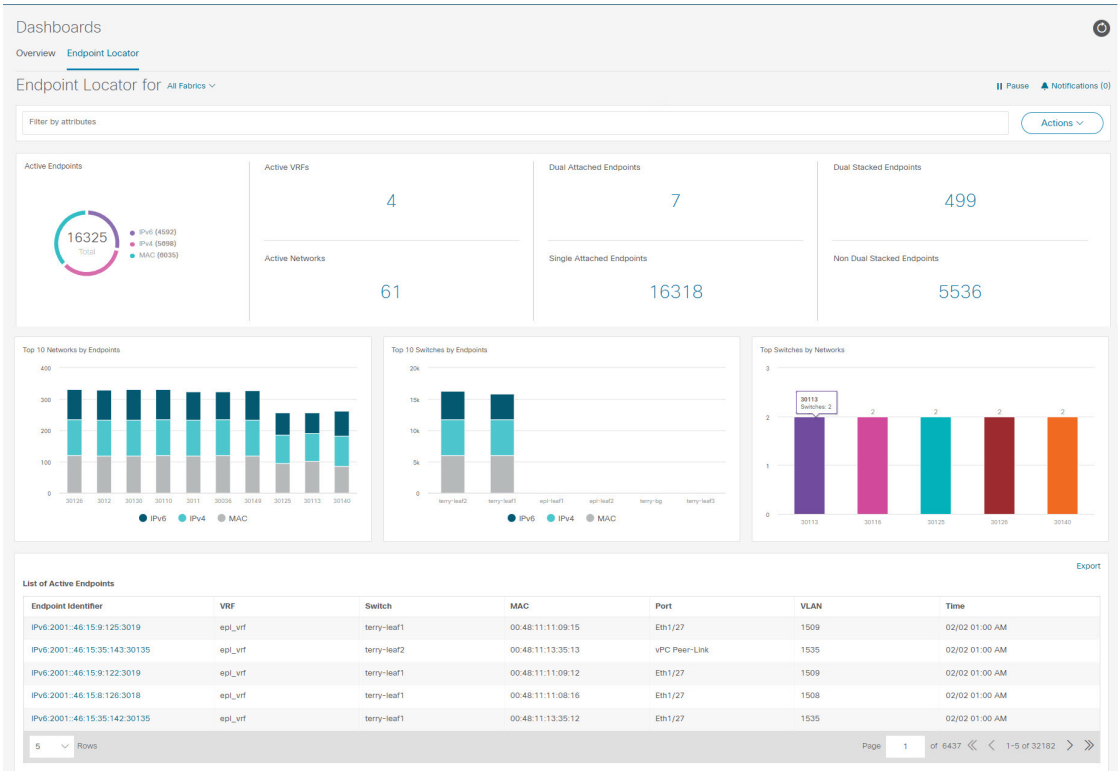
次の表に、ウィンドウのフィールドと説明を示します。

フィールド	説明
ポッド名	Kubernetes ポッドの名前を指定します。
ポッド IP	Kubernetes ポッドの IP アドレスを表示します。
フェーズ	ポッドのフェーズ（状態）を指定します。
理由	理由を指定します。
アプリケーション	ポッドのアプリケーションを指定します。
名前空間	ポッドの名前空間を指定します。
ノード名	ポッドのノード名を指定します。
ノード IP	ノードの IP アドレスを指定します。
クラスタ タイプ	クラスタのタイプを表示します。
物理 NIC	ノードの物理 NIC を表示します。
物理スイッチ	クラスタ ノードに接続されている物理スイッチを指定します。
スイッチ インターフェイス	クラスタ ノー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。

フィールド	説明
クラスタ名	クラスタの名前を指定します。
ポート チャネル	ポート チャネルを指定します（クラスタ ノードが VPC に接続されている場合）。
VLAN	VLAN を設定します。
ファブリック	ファブリック名を指定します。

エンドポイント ロケータ ダッシュボード

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 ロケータの詳細を確認するには、**[ダッシュボード（Dashboard）]>[エンドポイント ロケータ（Endpoint Locator）]** を選択します。**エンドポイント ロケータ** ダッシュボードが表示されます。



（注） 規模が拡大すると、システムがエンドポイント データを収集してダッシュボードに表示するまでに時間がかかる場合があります。エンドポイントの一括追加または削除では、EPL ダッシュボードに表示されるエンドポイント情報が最新のエンドポイントデータを更新して表示するまでに数分かかります。

- **[属性によるフィルター（filter by attributes）]** 検索バー フィールドで使用可能なオプションを使用して、検索を開始できます。

  また、それぞれのドロップダウン リストを使用して、特定の**スイッチ、VRF、ネットワーク**、および**タイプ**のエンドポイント ロケータの詳細をフィルタリングおよび表示することもできます。フィルター属性としてエンドポイントの MAC タイプを選択できます。ネットワークの名前は、**[ネットワーク（Network）]** ドロップダウン リストにも表示されます。デフォルトでは、選択したオプションはこれらのフィールドで**[すべて（All）]**です。**[ホスト IP/MAC/VM 名の検索（Search Host IP/MAC/VM Name）]**フィールドにホスト IP アドレス、MAC アドレス、または仮想マシンの名前を入力して、特定のデバイスのエンドポイント データを表示することができます。

- **[すべてのファブリック（All fabrics）]** ドロップダウン リストをクリックして、すべてのファブリックまたは必要なファブリックのエンドポイント ロケータの詳細を表示できます。

  エンドポイント関連の異常がある場合は、アラームが生成されます。**[一時停止（Pause）]** アイコンをクリックすると、ほぼリアルタイムでのデータの収集と表示が一時的に停止します。デフォルトでは、**[実行（Run）]**が選択されています。通知の詳細を表示する**[通知（Notification）]** アイコンをクリックします。

- **[アクション（Actions）]** > **[エンドポイント検索（Endpoint Search）]**をクリックします。詳細については、エンドポイント検索 （16 ページ） を参照してください。

- **[アクション（Actions）]** > **[エンドポイントの寿命（Endpoint Life）]**をクリックします。詳細については、エンドポイントの寿命 （17 ページ） を参照してください。

- **[アクション（Actions）]**>**[再同期（Resync）]**をクリックして、現在ルート リフレクター（RR）にあるデータに同期します。ただし、履歴データは保持されます。これはコンピューティング集約型のアクティビティであるため、**[再同期（Resync）]** を複数回クリックしないことを推奨します。

  特定のシナリオでは、次のようなネットワークの問題により、データポイントデータベースが同期せず、エンドポイントの数などの情報が正しく表示されないことがあります。

  - エンドポイントが同じスイッチの下でポート間を移動し、ポート情報を更新するのに時間がかかる。
  - 孤立したエンドポイントが 2 番目の VPC スイッチに接続され、孤立したエンドポイントではなくなりました。
  - NX-API は最初は有効になっておらず、後で有効になります。
  - NX-API は、最初は構成ミスが原因で失敗します。
  - ルート リフレクタ（RR）の変更。
  - スイッチの管理 IP が更新されます。

- **[通知（Notifications）]** アイコンをクリックして、最新の通知のリストを表示します。

[エンドポイント ロケータ通知（Endpoint Locator Notifications）] ウィンドウが表示されます。

通知が生成された時刻、通知の説明、シビラティ（重大度）などの情報が表示されます。

通知は、IPアドレスの重複、MAC専用アドレスの重複、ファブリックからのVRFの消失、スイッチからのすべてのエンドポイントの消失、エンドポイントの移動、ファブリックのエンドポイントがゼロになる、エンドポイントがスイッチに接続されたとき、新しいVRFが検出されたとき、RR BGP 接続ステータスが変更されたときなどのイベントに対して生成されます。RR connected ステータスは、Nexusダッシュボード ファブリック コントローラ が BGP を介して RR に接続できることを示します（Nexusダッシュボード ファブリック コントローラ および RR は BGP ネイバーです）。RR 切断ステータスは、RR が切断され、基盤となる BGP が機能していないことを示します。

属性によるフィルター検索バーフィールドで使用可能なオプションを使用して、検索を開始できます。

ウィンドウの上側ペインには、次の情報が表示されます。

ウィンドウの上側ペインには、選択したスコープのアクティブ エンドポイント、アクティブ VRF、アクティブ ネットワーク、デュアル アタッチ エンドポイント、デュアル アタッチ エンドポイントの数が表示されます。デュアル接続エンドポイント、シングル接続エンドポイント、デュアルスタックエンドポイントの数の表示のサポートが追加されました。デュアル接続エンドポイントは、少なくとも2つのスイッチの背後にあるエンドポイントです。デュアルスタックエンドポイントは、少なくとも 1 つの IPv4 アドレスと 1 つの IPv6 アドレスを持つエンドポイントです。

- データの履歴分析が実行され、前の日に偏差が発生したかどうかを示す文が各タイルの下部に表示されます。

  エンドポイント履歴 ウィンドウに移動するには、EPL ダッシュボードの上部ペインで任意のタイルをクリックします。

ウィンドウの「中央のペイン」には、次の情報が表示されます。

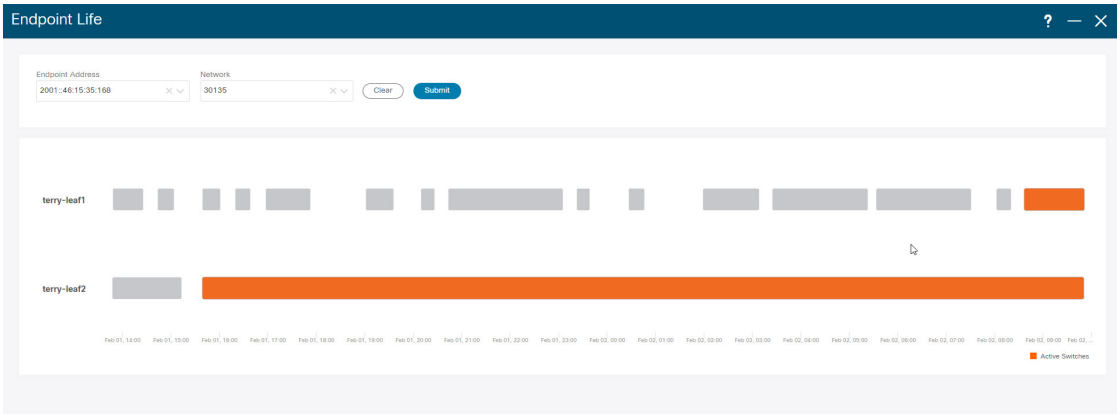
- **エンドポイント別の上位 10 個のネットワーク**：エンドポイントの数が最も多い上位 10 個のネットワークを示す円グラフが表示されます。円グラフにカーソルを合わせると、詳細情報が表示されます。必要なセクションをクリックして、IPv4、IPv6、および MAC アドレスの数を表示します。
- **エンドポイント別の上位 10 個のスイッチ**：最も多くのエンドポイントに接続されている上位10個のスイッチを示す円グラフが表示されます。円グラフにカーソルを合わせると、詳細情報が表示されます。必要なセクションをクリックして、IPv4、IPv6、および MAC アドレスの数を表示します。
- **ネットワーク別の上位スイッチ**：特定のネットワークに関連付けられているスイッチの数を示す棒グラフが表示されます。たとえば、スイッチのvPCペアがネットワークに関連付けられている場合、ネットワークに関連付けられているスイッチの数は 2 です。

ウィンドウの「下部ペイン」には、アクティブなエンドポイントのリストが表示されます。

仮想マシンが設定されている場合は、VM の名前が **[ノード名（Node Name）]** フィールドに表示されます。VM の名前が EPL ダッシュボードに反映されるまでに最大 15 分かかることに注意してください。それまでは、EPL ダッシュボードの **[ノード名（Node Name）]** フィールドに **[データなし（No DATA）]** と表示されます。

[エクスポート（Export）] をクリックして、アクティブなエンドポイントのリストを .csv 形式でダウンロードします。

必要なエンドポイント識別子をクリックすると、スライドインペインが表示され、関連する詳細が表示されます。**[エンドポイントの寿命（Endpoint Life）]** をクリックします。選択したエンドポイント ID の **[エンドポイントの寿命（Endpoint Life）]** ウィンドウが表示されます。詳細については、エンドポイントの寿命 （17 ページ） を参照してください。



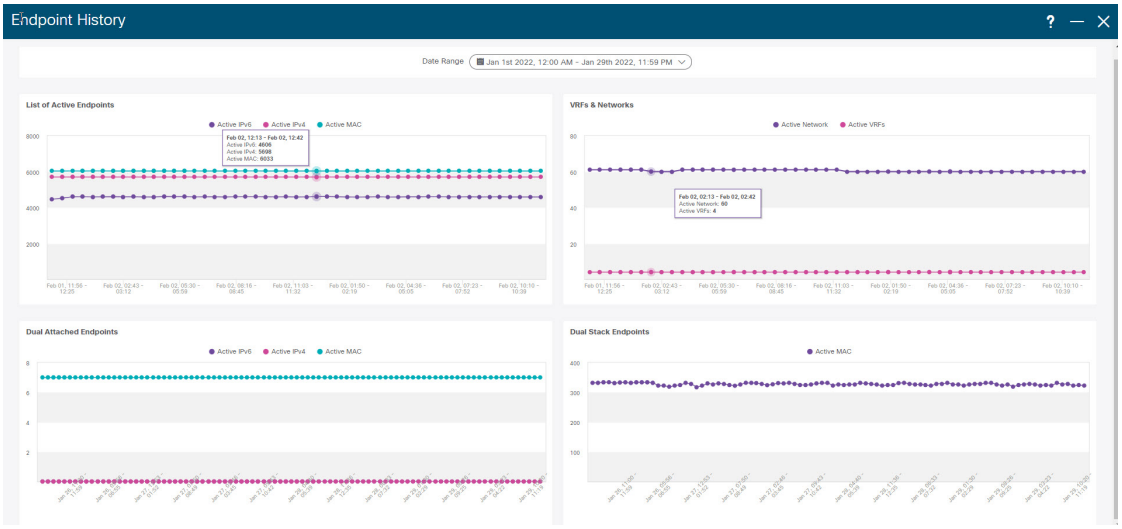
特定の IP アドレスを検索するには、**[エンドポイント ID（Endpoint Identifier）]** 列の検索アイコンをクリックします。

EPL が最初に有効になり、**[MAC-Only アドバタイズメントの処理（Process MAC-Only Advertisements）]** チェックボックスがオンになっているシナリオを考えます。次に、**[MAC-Only アドバタイズメントの処理（Process MAC-Only Advertisements）]** チェックボックスを選択せずに、EPL を無効にしてから再度有効にします。ElasticSearch のキャッシュデータは EPL を無効にしても削除されないため、MAC エンドポイント情報は EPL ダッシュボードに表示されたままになります。ルートリフレクタが切断された場合も、同じ動作が見られます。規模に応じて、エンドポイントはしばらくしてから EPL ダッシュボードから削除されます。場合によっては、古い MAC 専用エンドポイントの削除に最大 30 分かかることがあります。ただし、最新のエンドポイントデータを表示するには、**[再同期（Resync）]** アイコンをクリックします。

エンドポイント履歴

[エンドポイント履歴（Endpoint History）] ウィンドウに移動するには、EPL ダッシュボードの上部ペインで任意のタイルをクリックします。さまざまな時点でのアクティブエンドポイント、VRF およびネットワーク、デュアル接続エンドポイント、デュアルスタック MAC エンドポイントの数を示すグラフが表示されます。ここに表示されるグラフは、選択したファブリックに存在するエンドポイントだけでなく、すべてのエンドポイントを示します。エンドポイン

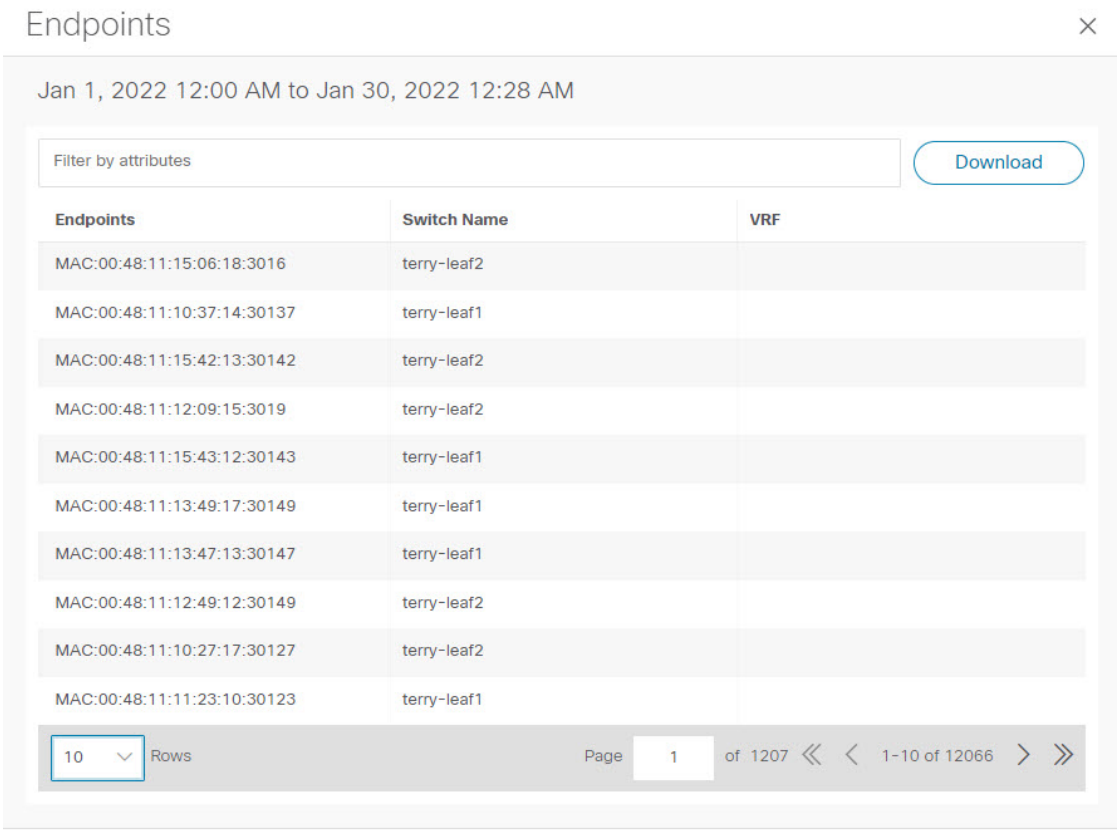
ト履歴情報は、過去 30 日間の最大 100 GB のストレージ容量に使用できます。



特定のポイントでグラフにカーソルを合わせると、詳細情報が表示されます。グラフのポイントは 30 分間隔でプロットされます。各グラフの下部にある色分けされたポイントをクリックして、特定の要件のグラフを表示することもできます。たとえば、**active (IPv4)** のみが強調表示され、他のポイントが強調表示されないように、上記の[アクティブエンドポイント（Active Endpoints）] ウィンドウで **active (IPv4)** 以外のすべての色分けされたポイントをクリックします。このようなシナリオでは、アクティブな IPv4 エンドポイントのみがグラフに表示されます。また、グラフの下部にある、色分けされたポイントのうち必要なものをクリックすると、特定の要件のグラフが表示されます。たとえば、**active (IPv4)** にカーソルを合わせると、アクティブな IPv4 エンドポイントのみがグラフに表示されます。

グラフ内の任意のポイントをクリックすると、その時点に関する詳細情報を示すウィンドウが表示されます。たとえば、**[アクティブエンドポイント（Active Endpoints）]** グラフで特定のポイントをクリックすると、**[エンドポイント（Endpoints）]** ウィンドウが表示されます。このウィンドウには、エンドポイントに関する情報とともに、エンドポイントに関連付けられているスイッチおよび VRF の名前が表示されます。データを CSV ファイルとしてダウンロード

するには、**[ダウンロード（Download）]** をクリックします。



エンドポイント検索

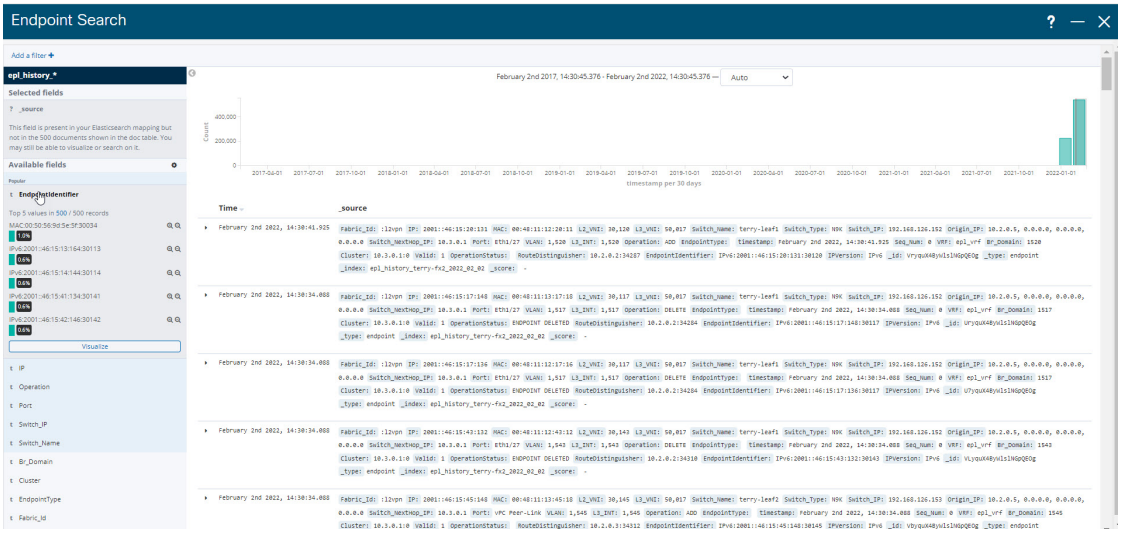
UI パス：**[ダッシュボード（Dashboard）]** > **[エンドポイント ロケータ（Endpoint Locator）]**.

[エンドポイント ロケータ（Endpoint Locator）] ウィンドウで、**[アクション（Actions）]** > **[エンドポイント検索（Endpoint Search）]**をクリックして、日付範囲で指定された期間のエンドポイント イベントを示すリアルタイム プロットを表示します。

（注） 時計アイコンの時刻は変更できません。ツールチップを無視して時間を変更してください。

ここに表示される結果は、左側のメニューにある **[選択済みフィールド（Selected fields）]** の下に表示されるフィールドによって異なります。**[使用可能なフィールド（Available fields）]** の下にあるフィールドを **[選択済みフィールド（Selected fields）]** に追加して、必須フィールドを

使用して検索を開始できます。



エンドポイントの寿命

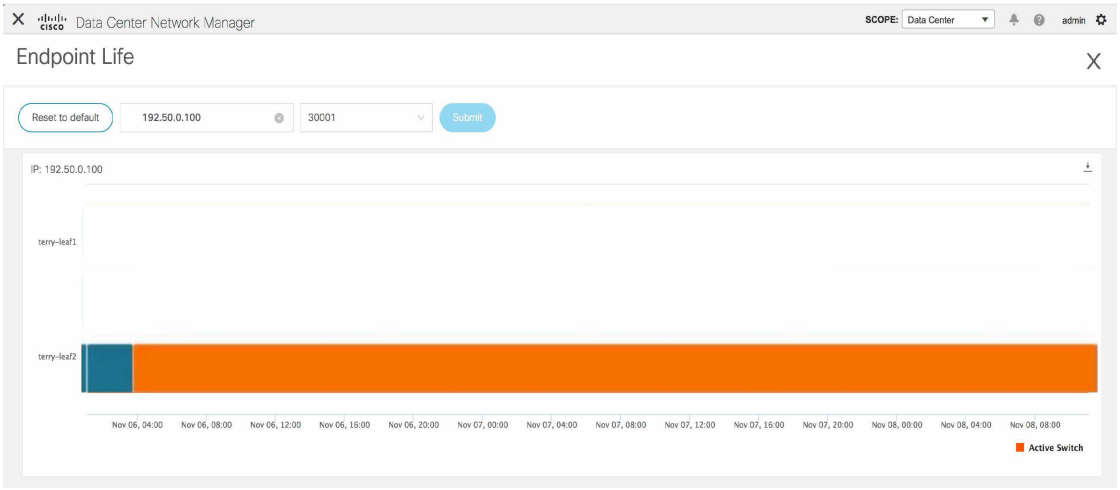
ファブリック内に存在する特定のエンドポイントのタイムライン全体を表示するには、[アクション（Actions）] > [エンドポイントの寿命（Endpoint Life）]をクリックします。

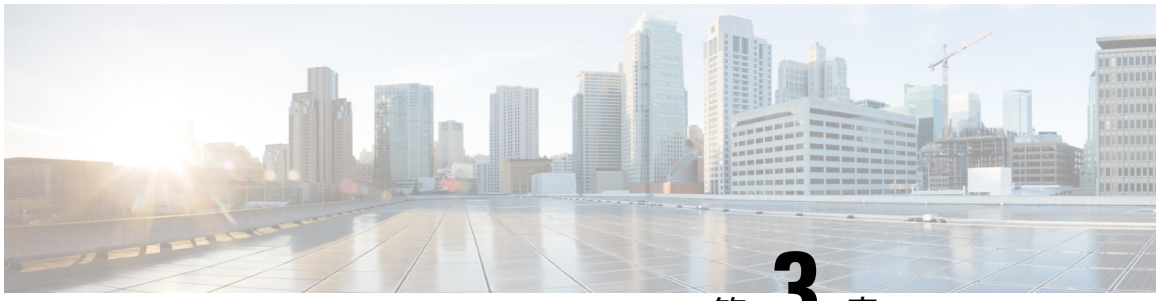
エンドポイントの IP または MAC アドレスと VXLAN ネットワーク識別子（VNI）を指定して、エンドポイントが存在していたスイッチのリストを、関連する開始日と終了日を含めて表示します。**[送信（Submit）]** をクリックします。`

IPv4 または IPv6 アドレスを使用して検索を開始し、IPv4/IPv6エンドポイントの**エンドポイント寿命**グラフを表示します。MACアドレスを使用して検索を開始し、MAC専用エンドポイントの**エンドポイント寿命**グラフを表示します。

表示されるウィンドウは、基本的には特定のエンドポイントのエンドポイントの寿命です。オレンジ色のバーは、そのスイッチのアクティブエンドポイントを表します。エンドポイントがネットワークによってアクティブと見なされる場合、エンドポイントには帯域があります。エンドポイントがデュアルホーム接続されている場合は、エンドポイントの存在を報告する2つの水平バンドがあり、各スイッチ（通常はスイッチのvPCペア）に 1 つのバンドがあります。エンドポイントが削除または移動された場合は、このウィンドウでエンドポイントの削除と移

動の履歴を確認することもできます。





第 3 章

トポロジ

UI ナビゲーション : [トポロジ（Topology）] をクリックします。

[トポロジ（Topology）] ウィンドウには、スイッチ、リンク、ファブリックエクステンダ、ポート チャネル設定、仮想ポート チャネルなど、さまざまなネットワーク要素に対応する色分けされたノードとリンクが表示されます。このウィンドウを使用して、次のタスクを実行します。

- これらの各要素の詳細を表示するには、対応する要素の上にカーソルを移動します。
- トポロジのナビゲーションを表示するには、上部のパンくずリストを表示します。
- デバイスまたは要素をクリックすると、右側にスライドインペインが表示され、デバイスまたは要素に関する詳細情報が表示されます。トポロジの詳細を表示するには、ノードをダブルクリックしてノード トポロジを開きます。たとえば、**[トポロジ（Topology）]** ウィンドウでファブリック トポロジとそのコンポーネントを表示するには、ファブリック ノードをダブルクリックしてから、表示する要素（ホスト、マルチキャスト グループ、マルチキャスト フローなど）をダブルクリックし、ファブリック タイプを表示します。
- ファブリックのファブリック サマリを表示する場合は、ファブリック ノードをクリックします。**[ファブリック サマリ（Fabric Summary）]** スライドイン ペインから、**[ファブリックの概要（Fabric Overview）]** ウィンドウを開きます。または、ファブリックを右クリックして **[詳細表示（Detailed View）]** を選択し、**[ファブリックの概要（Fabric Overview）]** ウィンドウを開きます。[ファブリックの概要（Fabric Overview）]ウィンドウの詳細については、ファブリックの概要 （194 ページ） を参照してください。
- 同様に、スイッチをクリックすると、設定されたスイッチ名、IP アドレス、スイッチ モデル、およびステータス、シリアル番号、正常性、最後にポーリングされた CPU 使用率、最後にポーリングされたメモリ使用率などのその他のサマリー情報が **[スイッチ（Switch）]** スライドインペインに表示されます。 -inペイン。詳細を表示するには、**[起動（Launch）]** アイコンをクリックして、**[スイッチの概要（Switch Overview）]** ウィンドウを開きます。[スイッチの概要（Switch Overview）] ウィンドウの詳細については、スイッチ （333 ページ） を参照してください。
- **[アクション（Actions）]** ドロップダウン リストからアクションを選択し、トポロジで選択した要素に基づいてさまざまなアクションを実行します。

たとえば、データセンター トポロジ ビューを開くと、[アクション（Actions）] ドロップダウン リストで使用できるアクションは [ファブリックの追加（Add Fabric）] のみです。ただし、ファブリック トポロジ ビューを開くと、ドロップダウン リストでさらに多くのオプションを使用できます。たとえば、LAN ファブリックの の場合、使用可能なアクションは、[詳細表示（Detailed View）]、[ファブリックの編集（Edit Fabric）]、[スイッチの追加（Add Switches）]、[構成の再計算（Recalculate Config）]、[構成のプレビュー（Preview Config）]、[構成の展開（Deploy Config）]、[リンクの展開（Deploy Link）]、[展開の無効化（Distribution Disable）]、[ファブリックのバックアップ（Restore Fabric）]、[ファブリックの復元（Restore Fabric）]、[VXLAN OAM]、および[ファブリックの削除（Delete Fabric）]です。 SAN ファブリックの 。IPFM ファブリックの場合、使用可能なアクションは、詳細ビュー、ファブリックの編集、スイッチの追加、設定の再計算、設定のプレビュー、設定の展開、およびファブリックの削除です。

- トポロジ内の要素に対してアクションを実行するには、アクション ドロップダウン リストにリストされている要素以外の要素を右クリックします。これにより、適切なウィンドウが開き、要素に基づいてタスクを実行できます。たとえば、ファブリックを右クリックすると、さまざまな設定、ファブリックの削除、バックアップと復元などのタスクを実行できます。
- VXLAN OAM オプションは、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。手順については、VXLAN OAM （192 ページ）を参照してください。

IPFM ファブリック トポロジは、Nexusダッシュボード ファブリック コントローラ IP for Media Fabric（IPFM）によって実行される操作に固有であり、IPFMモードと汎用マルチキャスト モードの両方に適用できます。

（注） 入力ノードと出力ノードを含むフロー トポロジでは、ノード アイコンの矢印は、入力ノードまたは送信者（**(S)** で示される）から出力ノードまたは受信者（**(R)** で示される）へのフローの方向を示します。

この項の内容は、次のとおりです。

トポロジの検索

効果的な検索を行うには、検索バーで検索属性と検索条件の組み合わせを使用します。検索属性と検索条件の組み合わせを検索バーに入力すると、対応するデバイスがトポロジ内で強調表示されます。

等号（=）、不等号（**!=**）、次を含む（**contains**）、次を含まない（**!contains**）などの検索条件を適用できます。

LAN ファブリックに使用できる検索属性は、ASN、ファブリック タイプ、ファブリック名、およびファブリック テクノロジーです。検索に使用できるファブリック タイプ属性には、スイッチ ファブリック、マルチファブリック ドメイン、外部、LAN モニタなどがあります。検索に使用できるファブリック テクノロジー属性には、fabricpath ファブリック、VXLAN ファブリック、VLANファブリック、外部、LANクラシック、IPFMクラシック、IPFMファブリック、スイッチ グループ、マルチファブリック ドメイン、eBGP VXLAN ファブリック、eBGP ルーテッドファブリック、MSOサイトグループ、メタ ファブリック、LANモニタ ファブリック、および IOS-XE VXLAN ファブリックなどがあります。

IPFM ファブリックの場合、スイッチまたはホスト名、スイッチまたはホストの IP アドレス、スイッチの MAC、およびスイッチのシリアル番号を検索できます。Generic Multicast モードでは、このウィンドウでレシーバ インターフェイス名または IP アドレスを検索することもできます。

トポロジにデバイスが表示されたら、そのデバイスをダブルクリックしてトポロジ内をさらに移動します。たとえば、検索したファブリックがトポロジに表示されている場合は、ファブリック（クラウド アイコン）をダブル クリックしてトポロジ内を移動します。さらに、ファブリックがトポロジに表示された後、条件とVPCピア、IPアドレス、モデル、モード、スイッチ、スイッチロール、検出ステータス、ソフトウェアバージョン、アップタイム、シリアルなどの条件とさまざまな検索持続性に基づいて検索を続行できます。

（注） トポロジの特定のレベルではフィルタのみが許可されます。つまり、フィルタは検索の代わりに使用されます。これらのレベルのトポロジリストには、限られた数のエンティティが表示されます。 たとえば、Easy Fabric Networks は 50 のネットワークに制限されています。追加の要素またはエンティティを表示するには、フィルタを使用する必要があります。

トポロジの表示

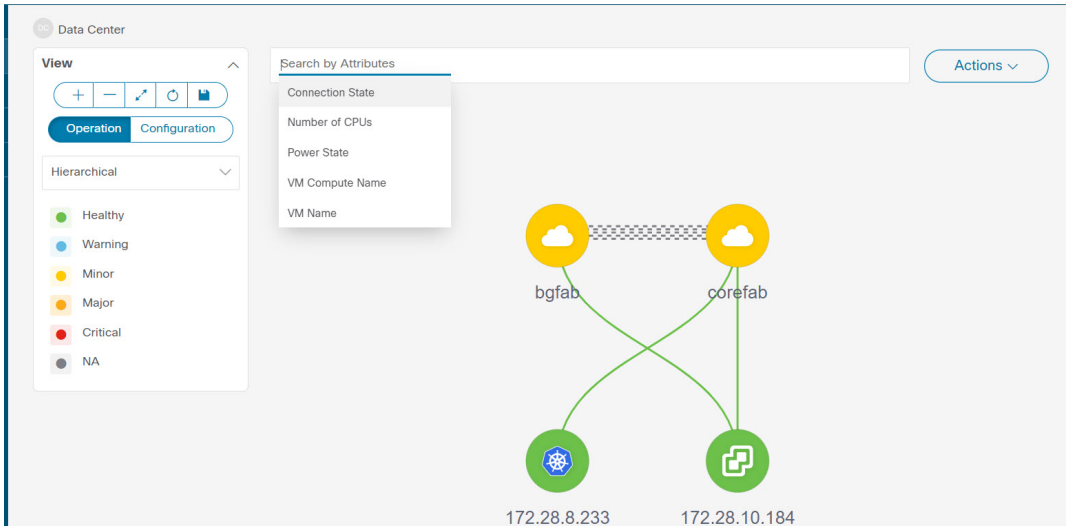
移動するには、空白の任意の場所をクリックしたまま、カーソルを上下左右にドラッグします。スイッチをドラッグするには、トポロジの空白領域をクリックしてカーソルを移動します。

スイッチを複数選択する場合、マウスドラッグを放してスイッチの選択を終了する前に、修飾キー（cmd/ctrl）を放す必要があります。

[表示（View）] ペインでは、デバイスとリンクに関する次の情報を表示できます。

- レイアウトオプション：画面に合わせてレイアウトを拡大、縮小、または調整できます。トポロジを更新したり、トポロジへの変更を保存したりすることもできます。詳細については、ズーム、パン、ドラッグ （38 ページ）を参照してください。
- 論理リンク：LAN トポロジの場合は、**[論理リンクの表示（Show Logical Links）]** トグルスイッチを使用して論理リンクを表示できます。

- [操作/構成（Operation/Configuration）]：LAN トポロジでは、操作または構成も選択できます。
- [レイアウトの選択（Select Layout）]ドロップダウン リスト：このドロップダウン リストからトポロジのレイアウトを選択し、レイアウト オプションで**[トポロジ レイアウトの保存（Save Topology Layout）]** をクリックします。詳細については、レイアウト （38 ページ）を参照してください。
- ステータス：すべてのデバイスまたはリンクのステータスが異なる色で表示されます。LAN トポロジの構成ステータスと動作ステータスも表示できます。詳細については、ステータス （39 ページ）を参照してください。

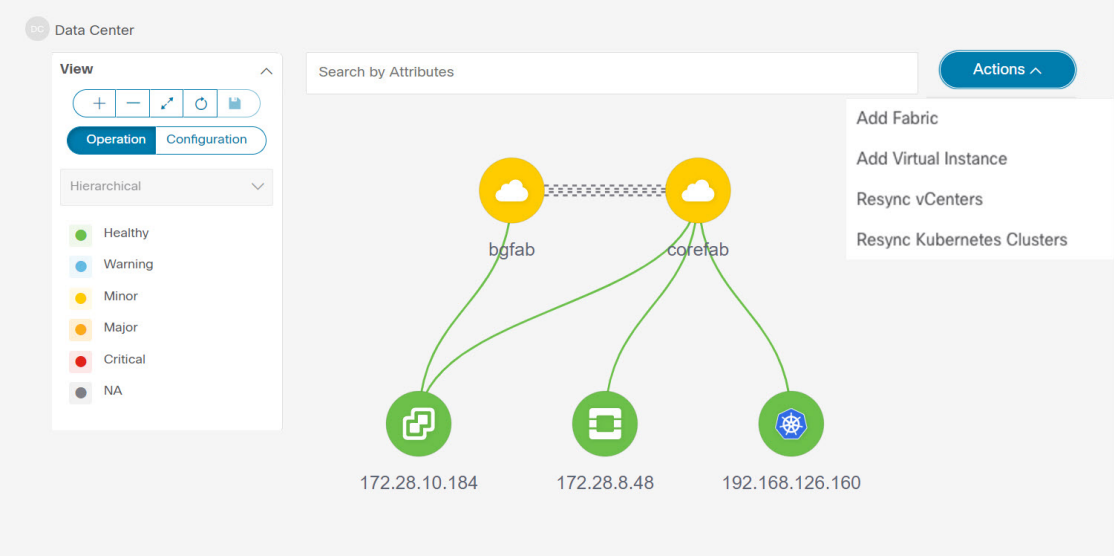


ノードのトポロジは、複数のスコープで表示されます。各スコープは、階層順に表示されます。スコープ階層はトピックパス（パンくずリスト）として表示され、必要なスコープに移動できます。スコープは次のとおりです。

- Data Center
- クラスタ（VCenter）
- リソースリスト（DVS、コンピューティング、および VM）
- Resource

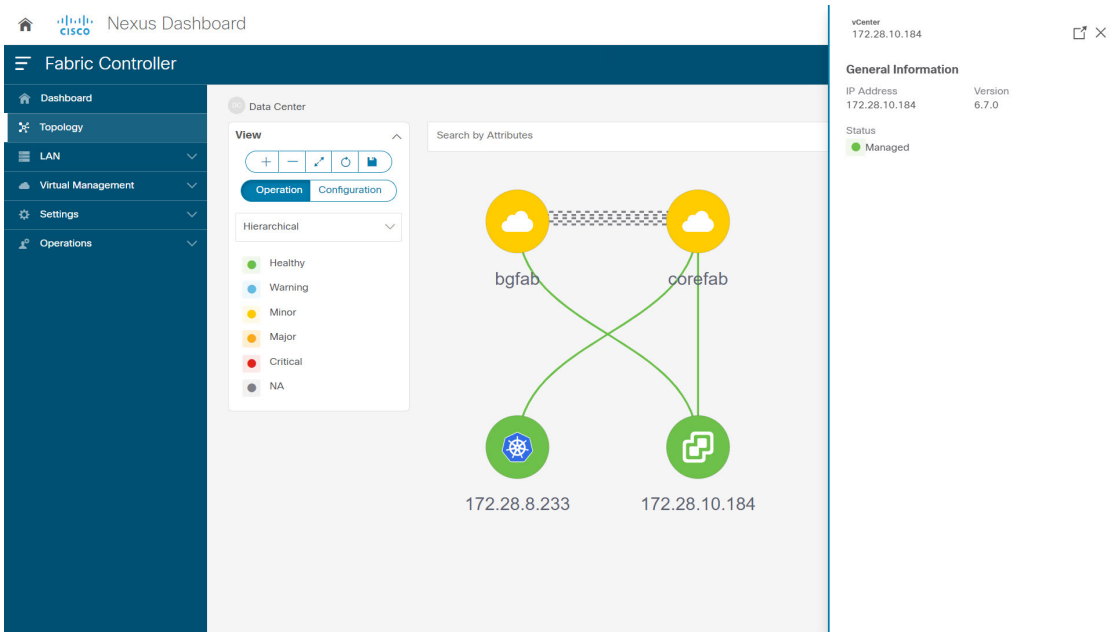
（注）

- **[トポロジ（Topology）]** ウィンドウでは、FEX の操作と構成ステータスが計算されないため、FEXはグレー（**[未知（Unknown）]** または **[該当なし（NA）]**）で表示されます。
- あるポートから別のポートにケーブルを移動した後、古いファブリックリンクは**[トポロジ（Topology）]** ウィンドウに保持され、リンクがダウンしていることを示す赤色で表示されます。削除が意図的なものであった場合は、リンクを右クリックして削除します。スイッチを手動で再検出すると、そのスイッチへのすべてのリンクが削除され、再学習されます。

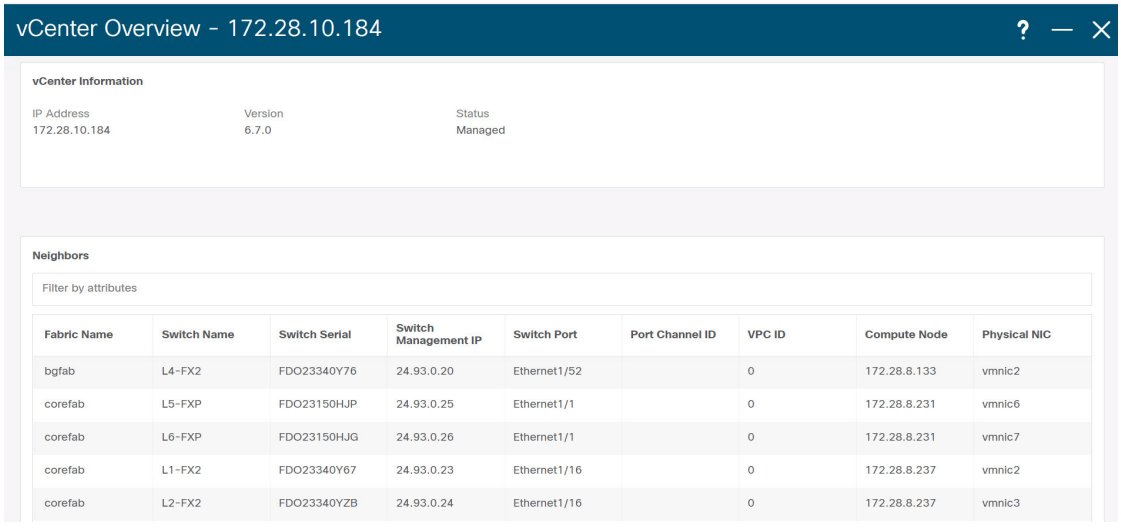


vCenter の可視化の表示

vCenter視覚化ノードをクリックすると、スライドインパネルが表示されます。**[起動（Launch）]** アイコンをクリックして、vCenter の概要ウィンドウを表示します。



このウィンドウには、vCenter IP アドレス、vCenter のステータス、クラスタに関連付けられたファブリック、スイッチ名、スイッチ IP、スイッチ ポート、VPC ID、コンピューティング ノード、および物理 NIC などのデータが要約されています。

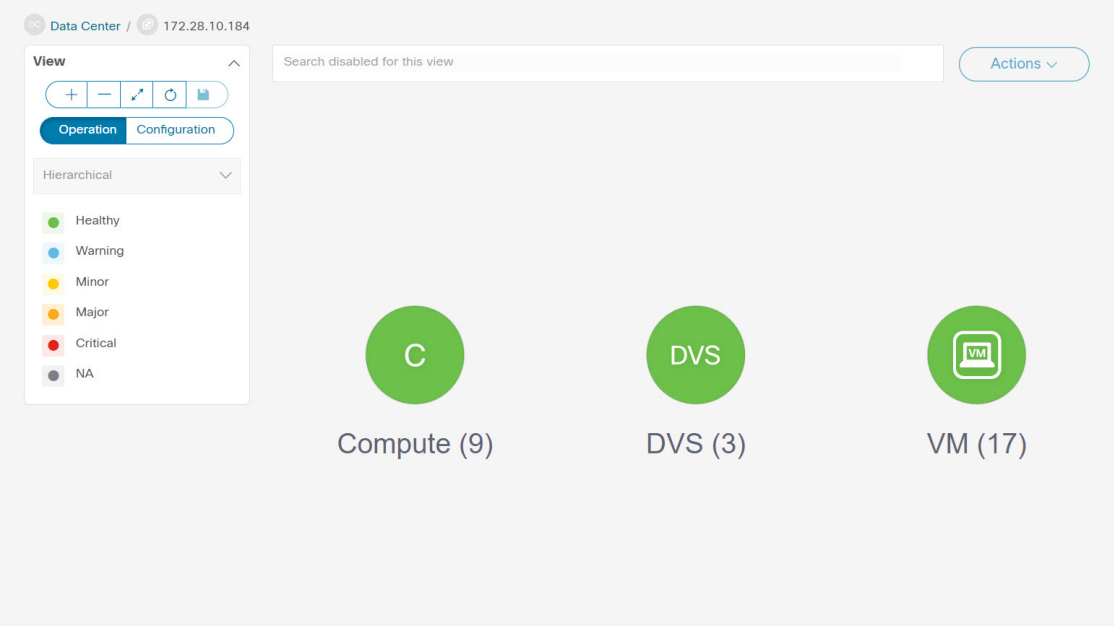


Fabric Name	Switch Name	Switch Serial	Switch Management IP	Switch Port	Port Channel ID	VPC ID	Compute Node	Physical NIC
bgfab	L4-FX2	FDO23340Y76	24.93.0.20	Ethernet1/52		0	172.28.8.133	vmnic2
corefab	L5-FXP	FDO23150HJP	24.93.0.25	Ethernet1/1		0	172.28.8.231	vmnic6
corefab	L6-FXP	FDO23150HJG	24.93.0.26	Ethernet1/1		0	172.28.8.231	vmnic7
corefab	L1-FX2	FDO23340Y67	24.93.0.23	Ethernet1/16		0	172.28.8.237	vmnic2
corefab	L2-FX2	FDO23340YZB	24.93.0.24	Ethernet1/16		0	172.28.8.237	vmnic3

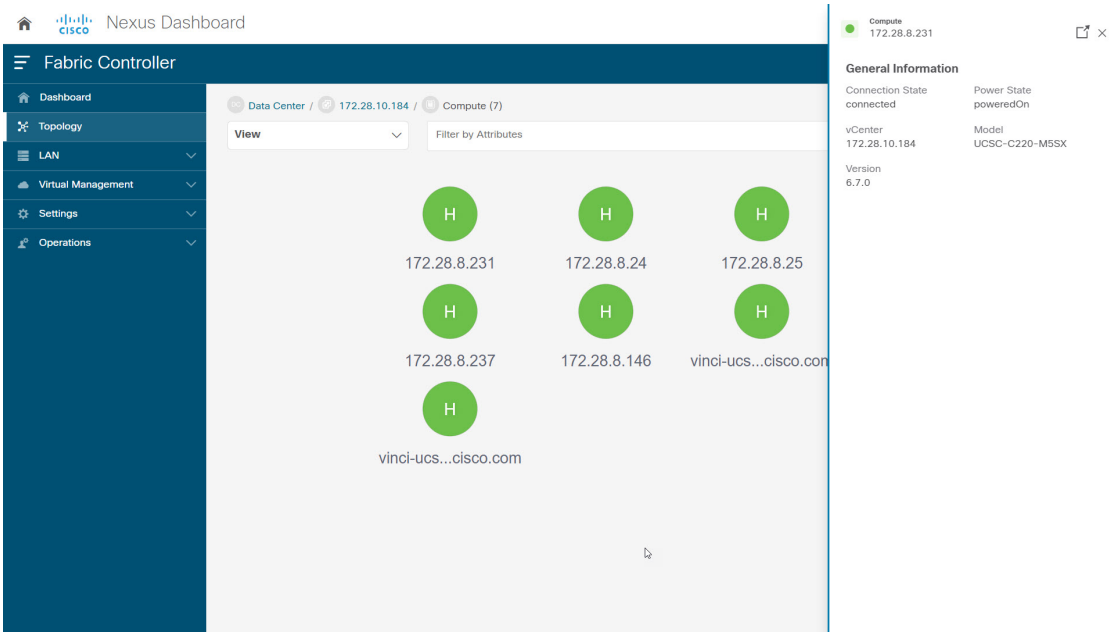
vCenter クラスタ ノードをダブルクリックして、コンピューティング、DVS、VM などの関連する vCenter クラスタ リソースを表示します。各ノードはブラケットで囲まれて表示され、vCenter インスタンス内の特定のノードの数を示します。

Compute、DVS、またはVMsをダブルクリックして、必要なリソースタイプとそのトポロジのリストを表示します。

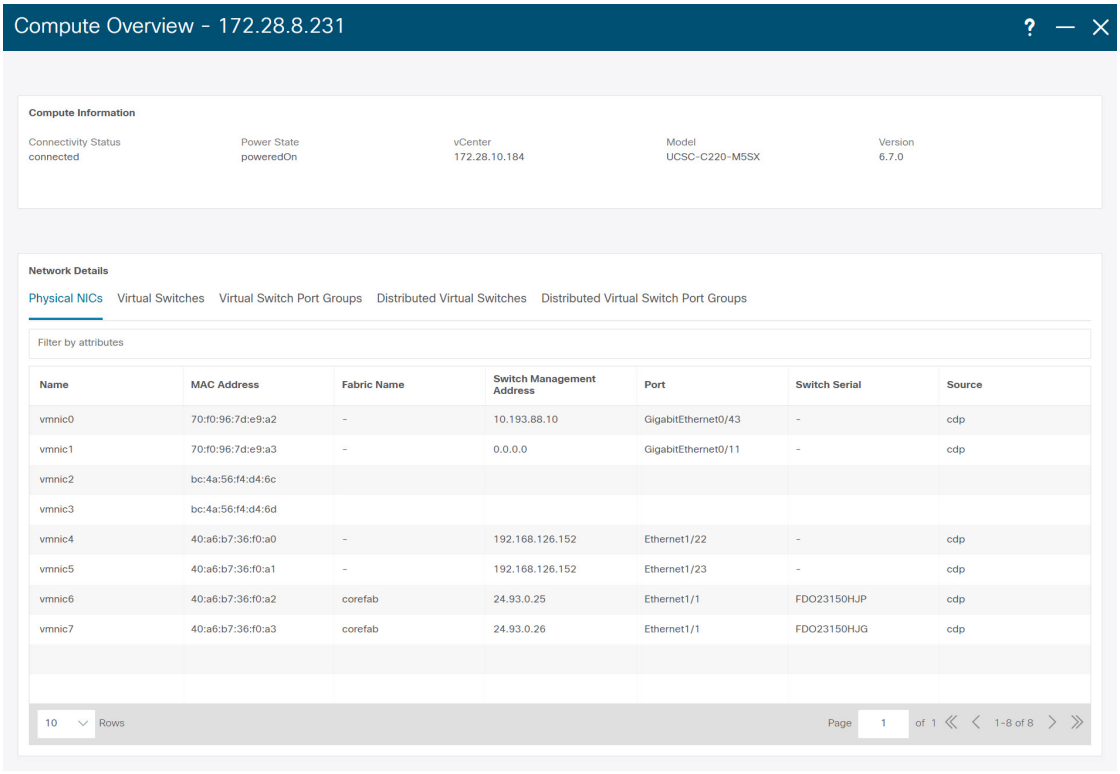
（注） DVS をダブルクリックすると、関連するコンピュートホストが DVS の下に表示されます。



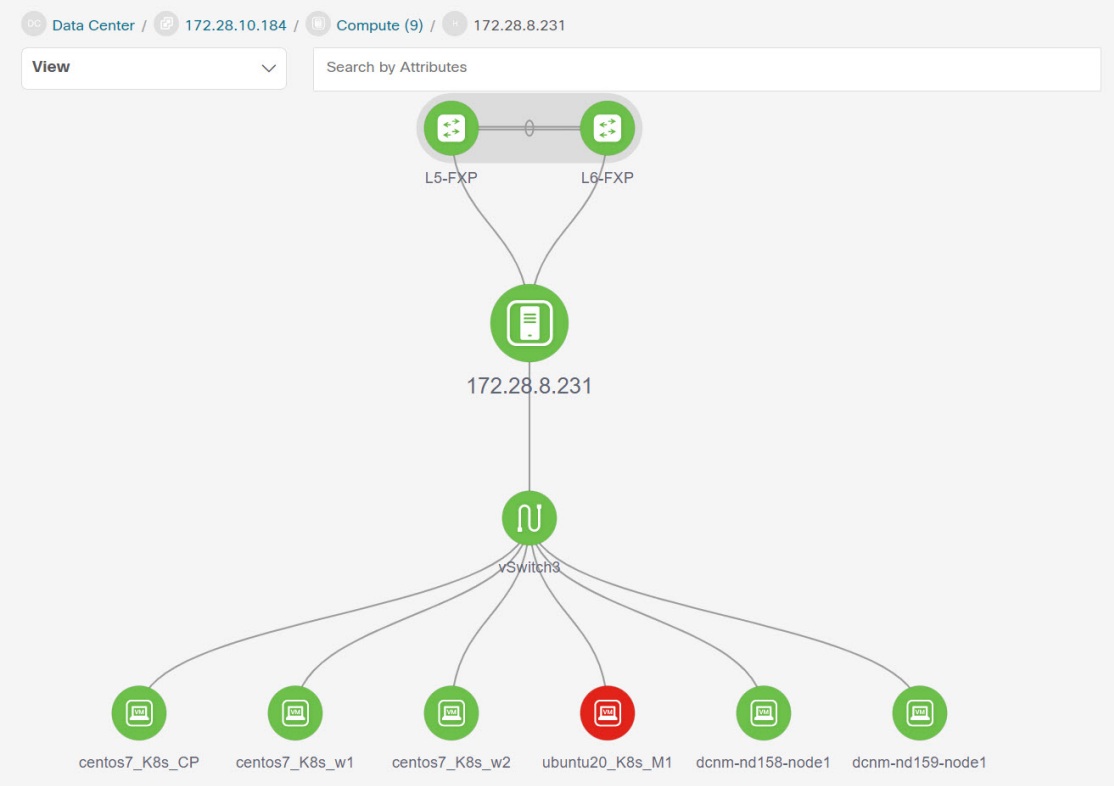
ノードをクリックすると、スライドインパネルが表示され、**[起動（Launch）]** アイコンをクリックして **[コンピューティングの概要（Compute Overview）]** ウィンドウを表示します。



ノードに関連付けられた電源状態、メモリサイズ、IP アドレス、MAC アドレスなどの情報を表示する [コンピューティング情報（Compute information）] タブと [ネットワークの詳細（Network details）] タブを表示できます。



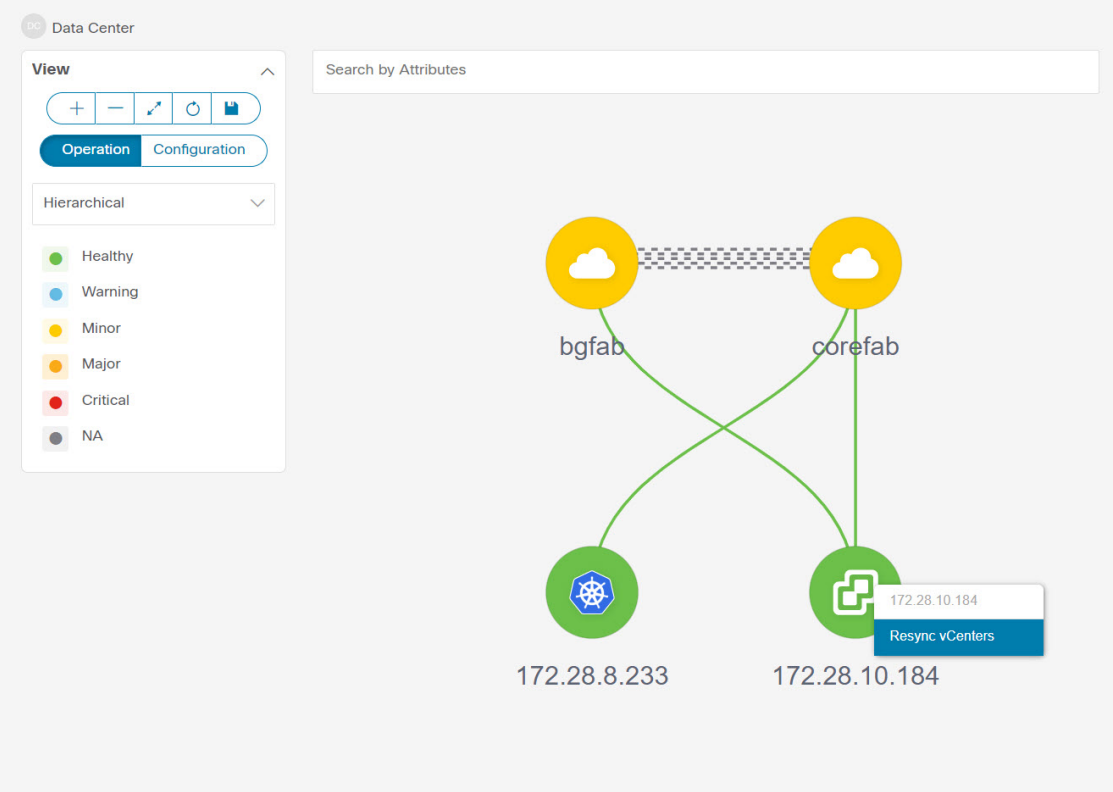
必要なノードを検索するには、**属性による検索**を使用して検索できます。特定のノードをダブルクリックして、vCenter ノードの完全なトポロジを表示します。



vCenter の再同期

再同期は、オンボードされたすべての vCenter クラスタの状態を同期します。vCenter クラスタを再同期するには、[トポロジウィンドウ（topology window）] を右クリックし、**[vCenter の再同期（Resync vCenters）]** を選択して **[確認（Confirm）]** をクリックします。個々の vCenter ク

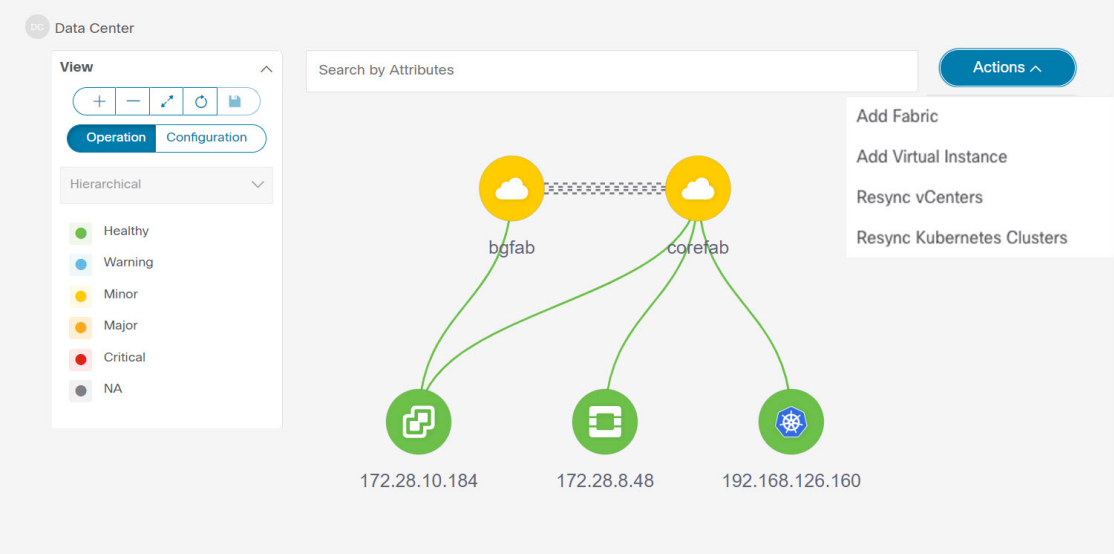
ラスタを同期するには、再検出フローを選択します。



Kubernetes クラスタの表示

トポロジは複数の範囲で表示でき、各範囲は階層順とナビゲーショントピックパスで表示されます。これらの範囲は次のとおりです。

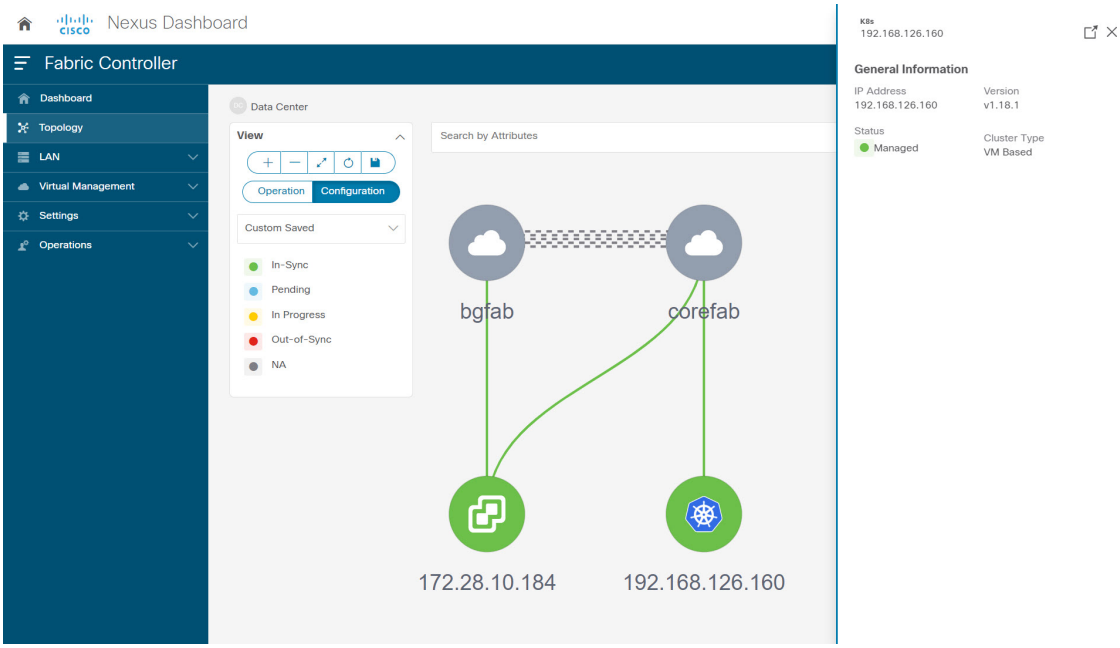
- データセンター、クラスタ（Kubernetes）
- リソースリスト（コンピューティング、およびポッド）
- リソース（コンピューティングとポッド）



Kubernetes クラスタには、2 つのタイプがあります。

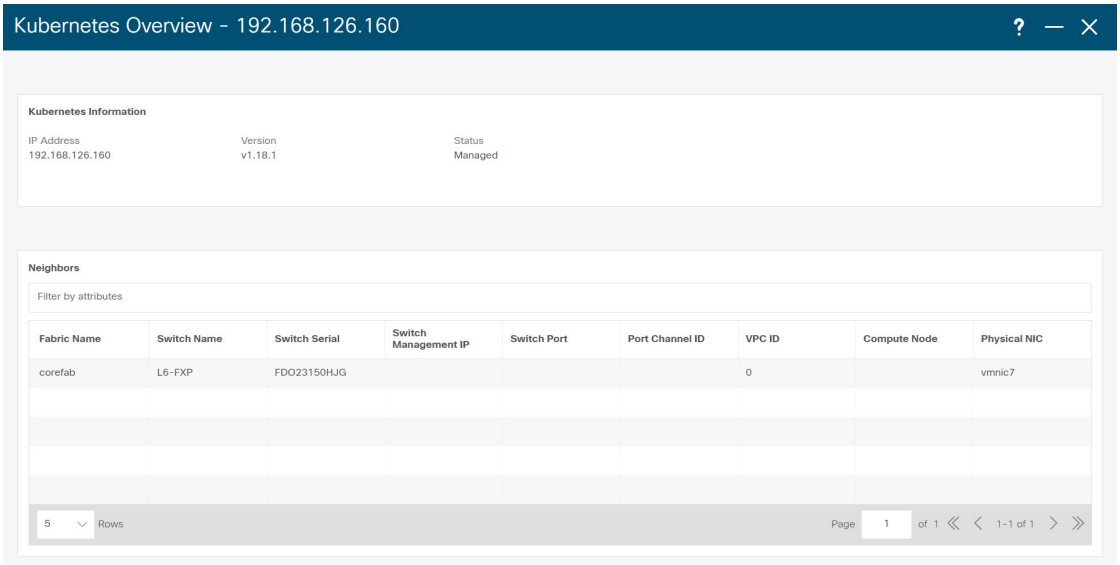
- VM ベースの Kubernetes クラスタは、vCenter によって管理される VM 上でホストされます。
- スイッチに直接接続されているベアメタルにインストールされた Kubernetes。

Kubernetes クラスタノードをクリックすると、スライドインパネルが表示されます。**起動**アイコンをクリックして、**Kubernetes の概要**ウィンドウを表示します。

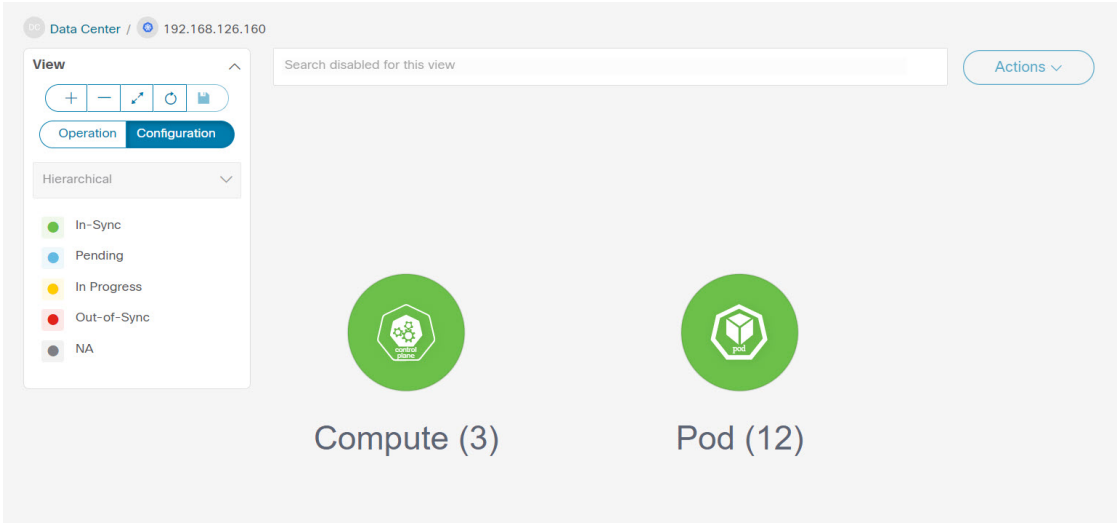


このウィンドウには、vCenter IP アドレス、vCenter のステータス、クラスタに関連付けられたファブリック、スイッチ名、スイッチ IP、スイッチポート、VPC ID、コンピューティングノー

ド、および物理 NIC などのデータが要約されています。

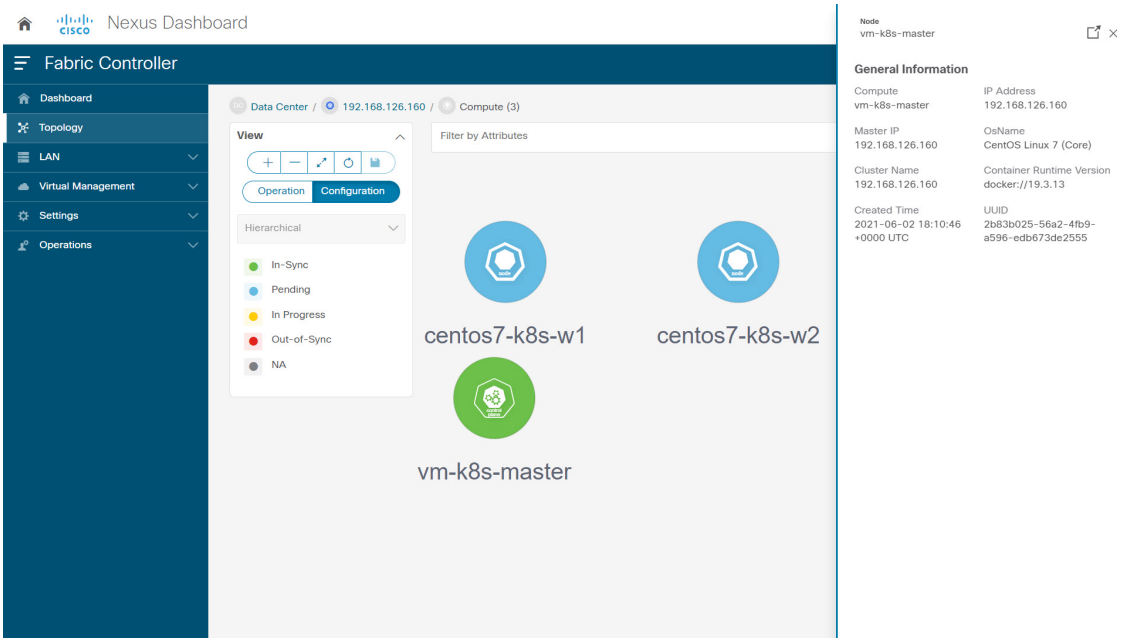


Kubernetes クラスタノードをダブルクリックして、コンピューティングやポッドなどの関連する Kubernetes クラスタリソースを表示します。各ノードはブラケットで囲まれて表示され、Kubernetes クラスタ内の特定のノードの数を示します。

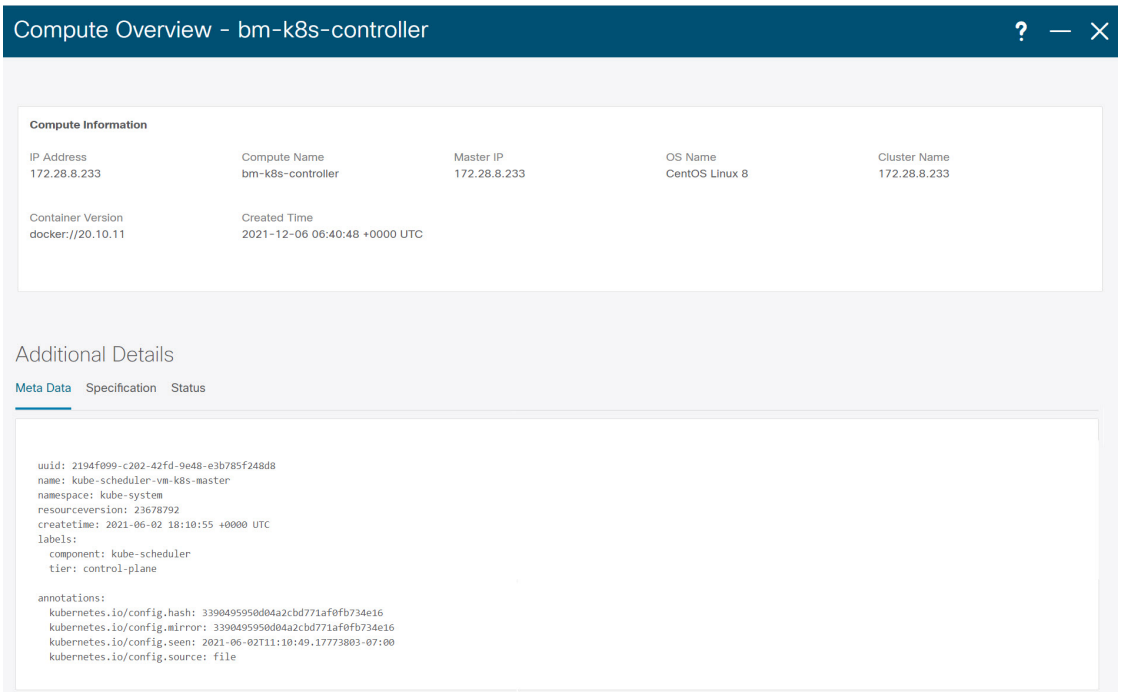


適切なリソース（コンピューティングまたはポッド）グループをダブルクリックして、Kubernetes クラスタ内のコンピューティングとポッドのリストを表示します。**[属性によるフィルタ処理**

（**Filter by Attributes**）] を使用して特定のノードを検索できます。



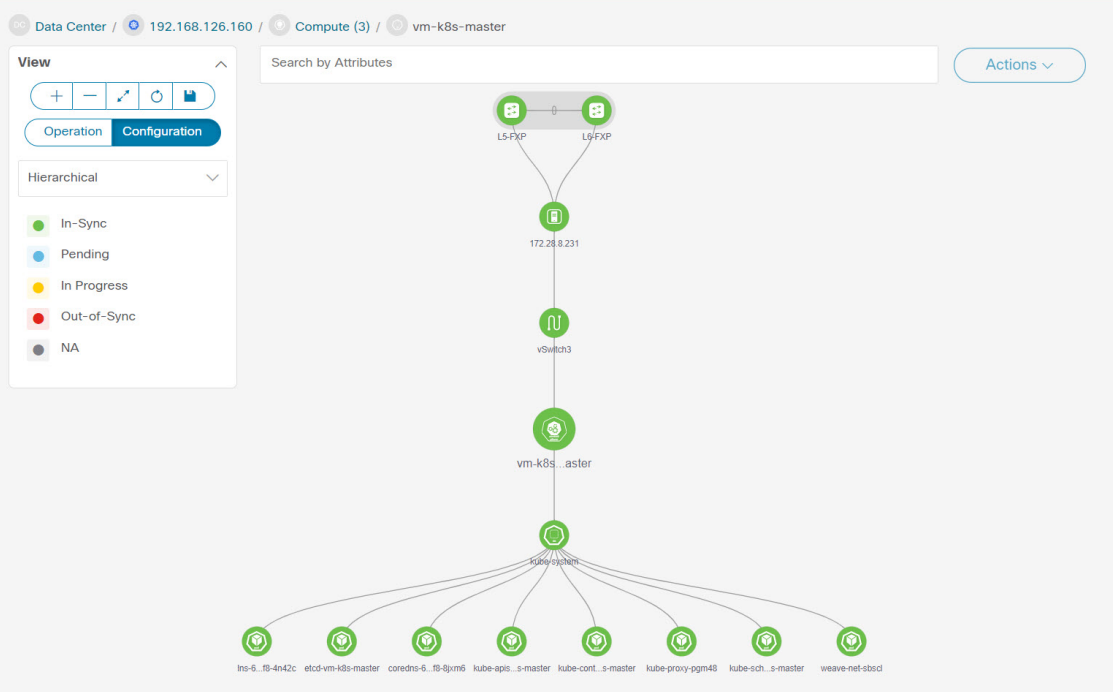
[ノード（Nodes）] をクリックして、ノードに関する詳細を表示します。ノードの概要を示すサイドパネルが表示されます。**[起動（Launch）]** アイコンをクリックして、選択したノードのメタデータ、仕様、およびステータス情報を表示します。



メタデータタブは、Kubernetes ノードまたはポッド名で構成されます。[仕様（Specification）] タブには、ノードまたはポッドの目的の設計または構成が含まれます。[ステータス] タブには、ノードまたはポッドの実行状態の情報が表示されます。

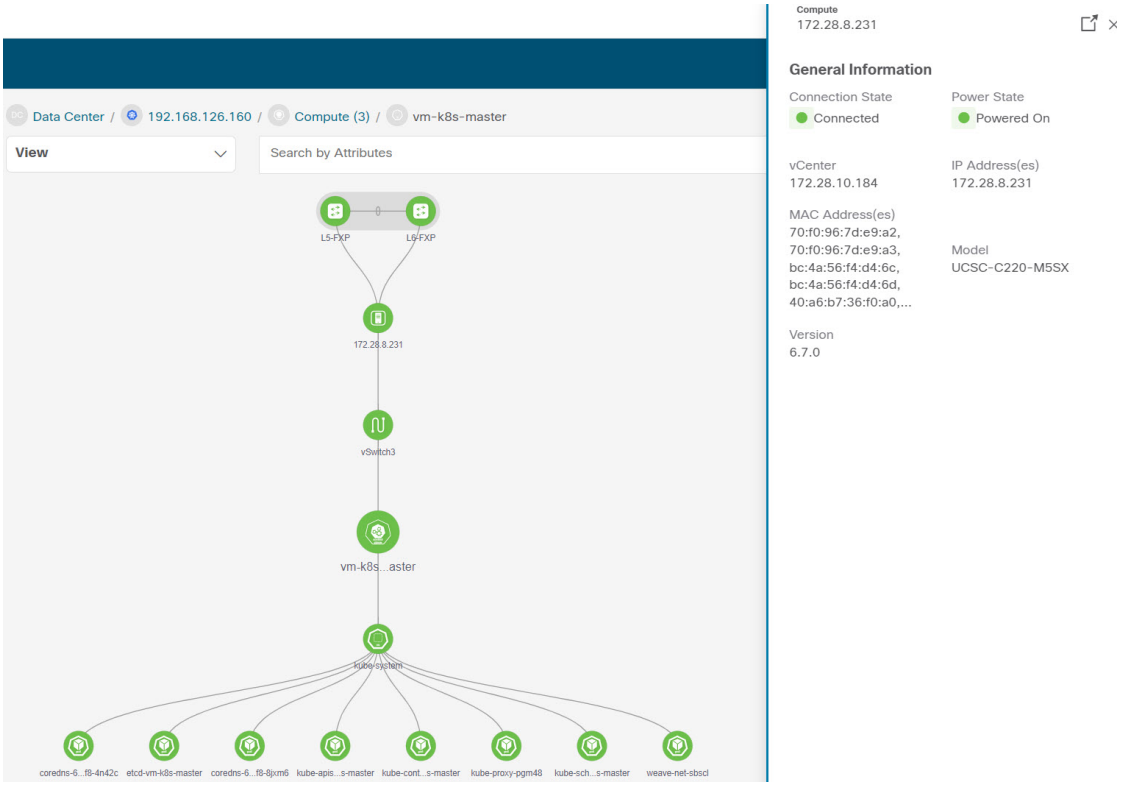
[コンピューティング（Compute）]または[ポッド（Pod）]をクリックして、特定のコンピューティングまたはポッドノードの詳細を表示します。**[属性別フィルタ処理（Filter by Attributes）]**を使用して、必要なノードを検索できます。

特定のノードをダブルクリックして、vCenter ノードの完全なトポロジを表示します。



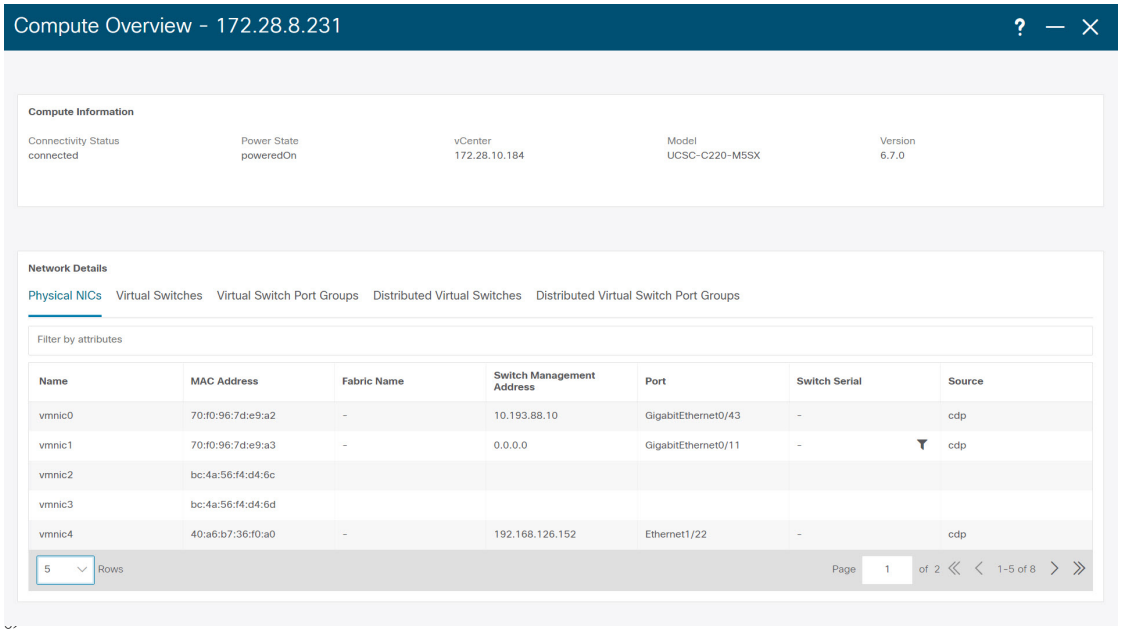
クラスタノードをクリックすると、スライドインパネルが表示されます。**起動**アイコンをクリックして、Kubernetes クラスタノードの概要ウィンドウを表示します。[コンピュータ情報（Compute information）]タブと[ネットワークの詳細（Network details）]タブを表示するには。

ポッドノードをクリックすると、スライドインパネルが表示されます。**起動**アイコンをクリックして、Kubernetes ポッドの概要ウィンドウを表示します。



[コンピュータ情報（Compute Information）]：接続ステータス、電源の状態、vCenter IP、モデル、およびバージョンを表示します。

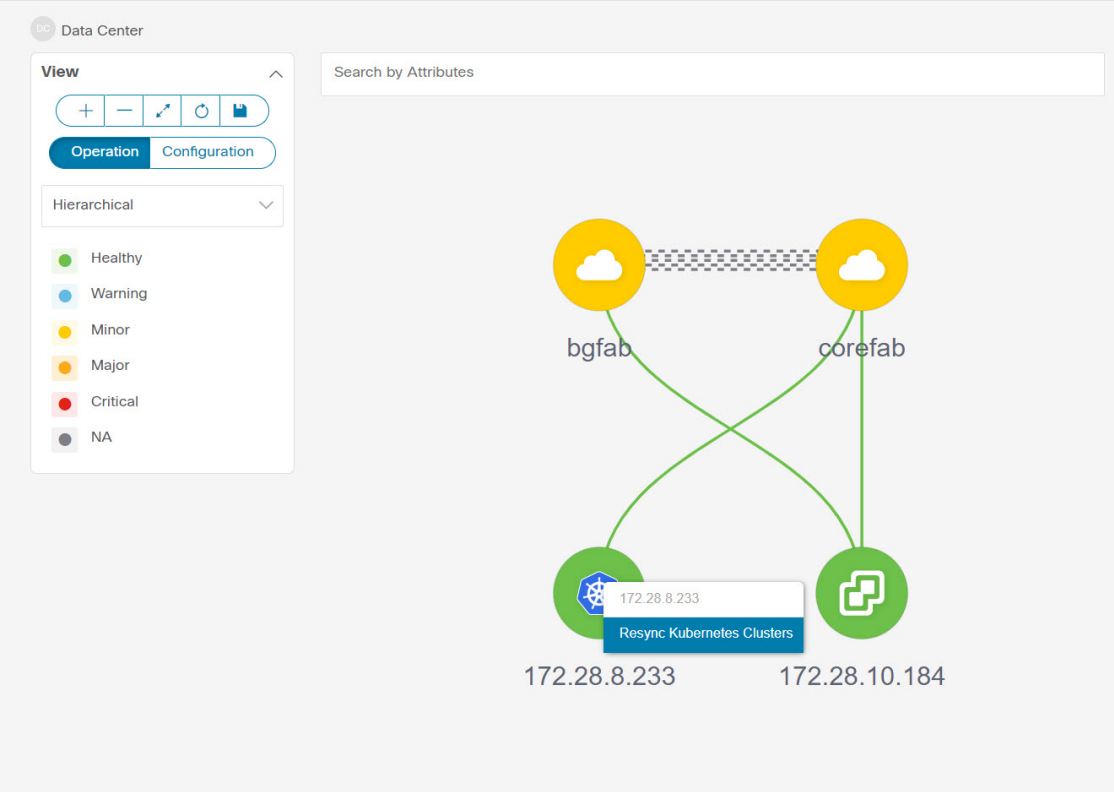
[ネットワークの詳細（Network Details）]：物理 NIC、仮想スイッチ、仮想スイッチポートグループ、分散仮想スイッチ、分散仮想スイッチポートグループなどの表形式の情報を表示しま



Kubernetes クラスタの再同期

kubernetes クラスタを再同期するには、[トポロジ（Topology）] ウィンドウを右クリックし、**[Kubernetes クラスタの再同期（Resync Kubernetes Clusters）]** をクリックして、**[確認（Confirm）]** をクリックします。

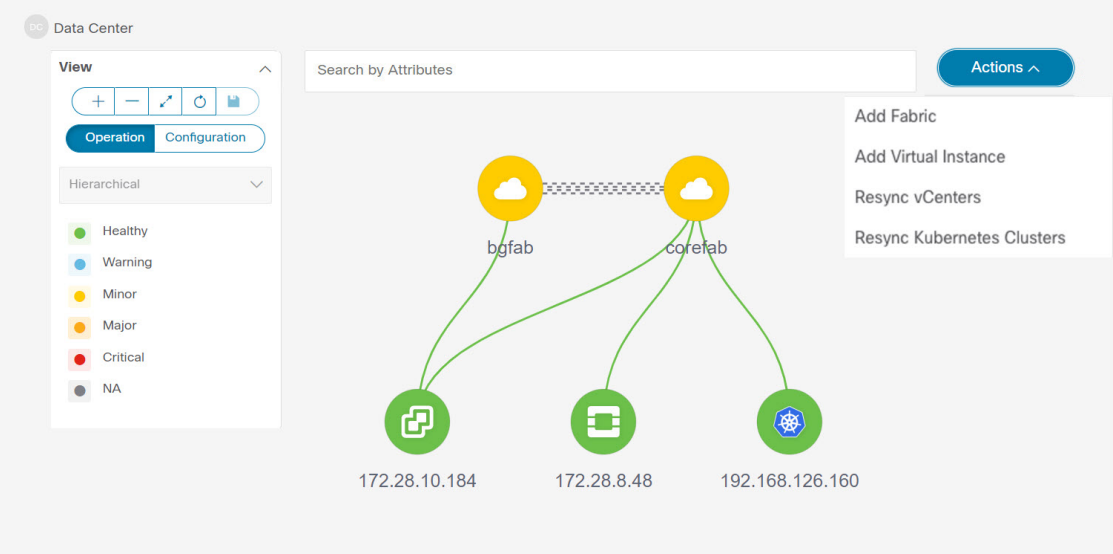
再同期は、オンボードされたすべての Kubernetes クラスタの状態を同期します。



OpenStack クラスタの表示

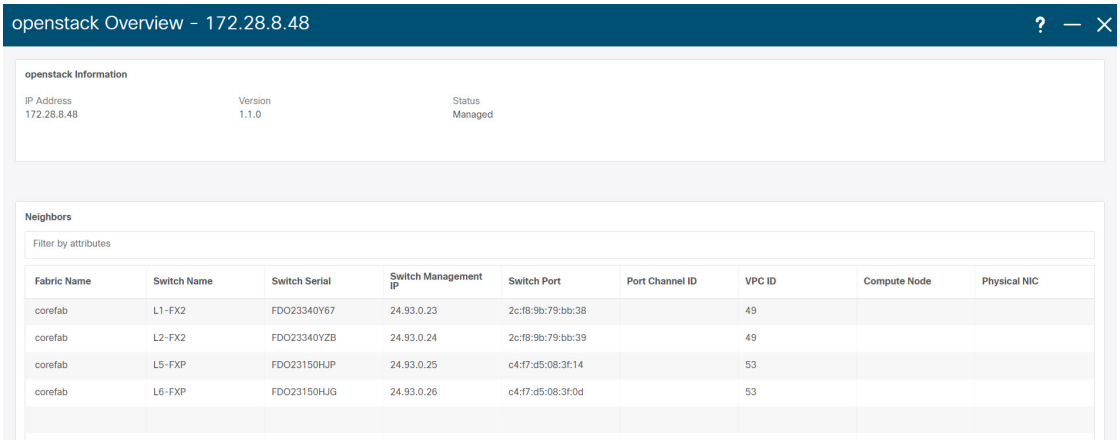
ノードのトポロジは、複数のスコープで表示されます。各スコープは、階層順に表示されます。スコープ階層はトピックパス（パンくずリスト）として表示され、必要なスコープに移動できます。スコープは次のとおりです。

- Data Center
- クラスタ（Openstack）
- リソースリスト（コンピューティング、および VM）
- Cluster



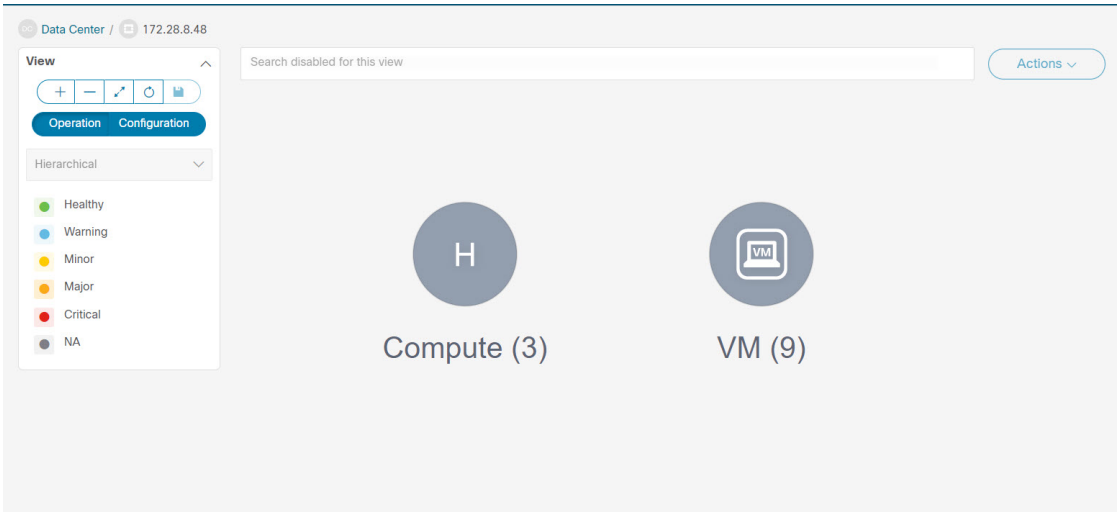
[Openstack クラスタノード（Openstack cluster node）]をクリックすると、スライドインパネルが表示されます。**[起動（Launch）]**アイコンをクリックして、[Openstack クラスタ（Openstack cluster）] ウィンドウを表示します。

このウィンドウには、Openstack クラスタの IP アドレス、vCenter のステータス、クラスタに関連付けられたファブリック、スイッチ名、スイッチ IP、スイッチ ポート、VPC ID、コンピューティング ノード、物理 NIC などのデータが要約されています。



[Openstack クラスタノード（Openstack cluster node）] をダブルクリックして、関連付けられている VM とコンピューティングノードを表示します。各ノードはブラケットで囲まれて表示さ

れ、vCenter インスタンス内の特定のノードの数を示します。



コンピューティングまたはVMグループのアイコンをダブルクリックして、クラスタ内の特定のコンピューティングまたは VM のリストを表示します。

[属性別フィルタ処理（Filter by Attributes）] を使用して、必要なノードを検索できます。

特定のノードをダブルクリックして、Openstack クラスタノードの完全なトポロジを表示します。

IPFM - マルチキャスト フロー

汎用マルチキャストは、2 層スパインまたはリーフトポロジに限定されません。関係するすべてのスイッチが Cisco NX-OS リリース 9.3(5) を搭載したCisco Nexus 9000 シリーズ スイッチである場合、フロー分類とパストレースは特定のトポロジに限定されません。汎用マルチキャストは、デフォルト VRF でサポートされます。

（注）
- インベントリからデバイスを削除すると、そのスイッチのポリシー展開ステータスが削除されます。ただし、スイッチのポリシー構成もクリアします。

マルチキャストルーティングをイネーブルにするには、次の手順を実行します。

1. Nexusダッシュボード ファブリック コントローラ Web UI から、**[設定（Settings）]** > **[サーバー設定（Server Settings）]** を選択します。
2. **[IPFM]** タブをクリックし、**[ホストポリシーでマルチキャスト範囲のマスク/プレフィックスを有効にする（Enable mask/prefix for the multicast range in Host Policy）]** チェックボックスをオンにします。
3. [保存（Save）] をクリックします。

マルチキャスト フロー トポロジを表示するには、次の手順を実行します。

1. **[トポロジ（Topology）]** ウィンドウで IPFM ファブリックをダブルクリックします。
2. [マルチキャスト フロー（Multicast Flows）]ノードをダブルクリックします。
3. 必要なマルチキャスト フローをダブルクリックします。

   マルチキャスト フロー トポロジが表示されます。

   マルチキャスト フロー トポロジには、スパイン、リーフ、および送信者と受信者のホストが含まれます。移動する点線は、IPFM ファブリック トポロジ内のトラフィックのフローを示しています。アイコン内の矢印はフローの方向を示し、**(S)** と **(R)** が付いた IP アドレスはそれぞれ送信側と受信側のホストを示します。

ズーム、パン、ドラッグ

ズームインまたはズームアウトするには、ウィンドウの左下にあるコントロールを使用するか、マウスのホイールを使用します。

移動するには、空白の任意の場所をクリックしたまま、カーソルを上下左右にドラッグします。

スイッチをドラッグするには、トポロジの空白領域をクリックしてカーソルを移動します。

レイアウト

トポロジは、トポロジの配置方法を記憶する **[レイアウトの保存（Save Layout）]** オプションとともに、さまざまなレイアウトをサポートします。

- **[Hierarchical]** および **[Hierarchical Left-Right]**：トポロジのアーキテクチャ ビューを提供します。CLOS トポロジの設定方法に関するノードを示すさまざまなスイッチ ロールを定義できます。

Note 大規模なセットアップを実行する場合、リーフ層のすべてのスイッチを簡単に表示できるようになるのは困難です。これを軽減するために、Nexusダッシュボード ファブリック コントローラ は 16 のスイッチごとにリーフ層を分割します。

- **Circular** および **Tiered-Circular**：ノードを円形または同心円状に描画します。
- **[ランダム（Random）]**：ノードはウィンドウにランダムに配置されます。Nexusダッシュボード ファブリック コントローラ は、推測を行い、近接するノードをインテリジェントに配置しようとします。
- **カスタム保存レイアウト**：ノードは、必要に応じてドラッグできます。必要に応じて配置した後、**[保存（Save）]** をクリックして位置を保持します。次回トポロジにアクセスすると、Nexusダッシュボード ファブリック コントローラ により最後に保存したレイアウト位置に基づいてノードが描画されます。

レイアウトを選択する前に、Nexusダッシュボード ファブリック コントローラ はカスタム レイアウトが適用されているかどうかを確認します。カスタム レイアウトが適用されている場合は、それを使用します。Nexusダッシュボード ファブリック コントローラカスタム レイアウトが適用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 はスイッチが異なる階層に存在するかどうかを確認し、階層レイアウトまたは階層左右レイアウトを選択します。他のすべてのレイアウトが失敗した場合は、強制指向レイアウトが選択されます。

ステータス

各ノードとリンクの色分けは、その状態に対応しています。動作の色とその意味を次のリストに示します。

- 緑：要素が正常に機能し、意図したとおりに機能していることを示します。
- 青：要素が警告状態にあり、それ以上の問題を防ぐために注意が必要であることを示します。
- 黄色：要素に小さな問題があることを示します。
- オレンジ：要素に重大な問題があり、それ以上の問題を回避するには注意が必要であることを示します。
- 赤：要素が重大な状態にあり、すぐに対処する必要があることを示します。
- グレー：要素を特定するための情報がないか、要素が検出されたことを示します。

設定の色とその意味を次のリストに示します。

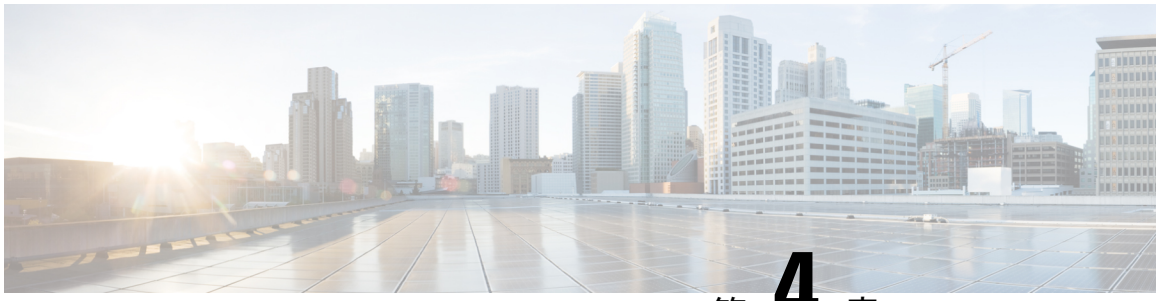
- 緑：要素が目的の設定と同期していることを示します。
- 青：要素に保留中の展開があることを示します。
- 黄色：アクティブな展開が進行中であることを示します。
- 赤：要素が意図した構成と同期していないことを示します。
- グレー：情報が不足しているか、設定の同期計算がサポートされていないことを示します。

Note

- **[トポロジ（Topology）]** ウィンドウでは、FEXの操作と構成ステータスが計算されないため、FEXはグレー（**[不明（Unknown）]** または **[n/a]**）で表示されます。
- あるポートから別のポートにケーブルを移動した後、古いファブリックリンクは**[トポロジ（Topology）]** ウィンドウに保持され、リンクがダウンしていることを示す赤色で表示されます。削除が意図的なものであった場合は、リンクを右クリックして削除します。スイッチを手動で再検出すると、そのスイッチへのすべてのリンクが削除され、再学習されます。

第 I 部

LAN



第 4 章

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 （48 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（53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（116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（639ページ）

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 （129 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 （43 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 （43 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 （43 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 （704 ページ）
[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 （154 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（158 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、MACアドレス変更、および不正送信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、MACアドレスの変更、および不正送信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 *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 75 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 , on page 699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 75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 75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 93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。

変数	説明
<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 88

[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, on page 731 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 114

[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 108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。

[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。

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 108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 175 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（53 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 （53 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。
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。

フィールド	説明
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。

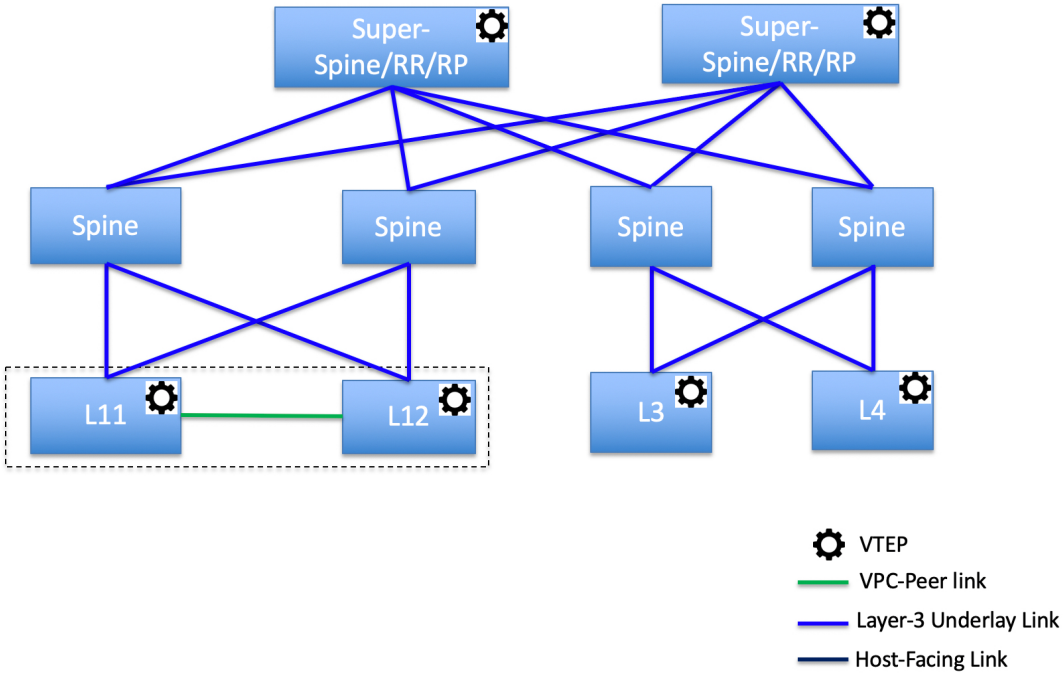
- Easy ファブリックでのみサポートされます。
- スパインとボーダーにのみ接続できます。有効な接続は次のとおりです。
  - スパインからスーパー スパインへ
  - スパインからボーダー スーパー スパインおよびボーダー ゲートウェイ スーパー スパインへ
  - スーパー スパインからボーダー リーフおよびボーダー ゲートウェイ リーフへ
- RR または RP（該当する場合）機能は、ファブリックに存在する場合、常にスーパー スパイン上で設定されます。スーパー スパインでも最大 4 つの RR および RP がサポートされます。
- ボーダー スーパー スパインおよびボーダー ゲートウェイ 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

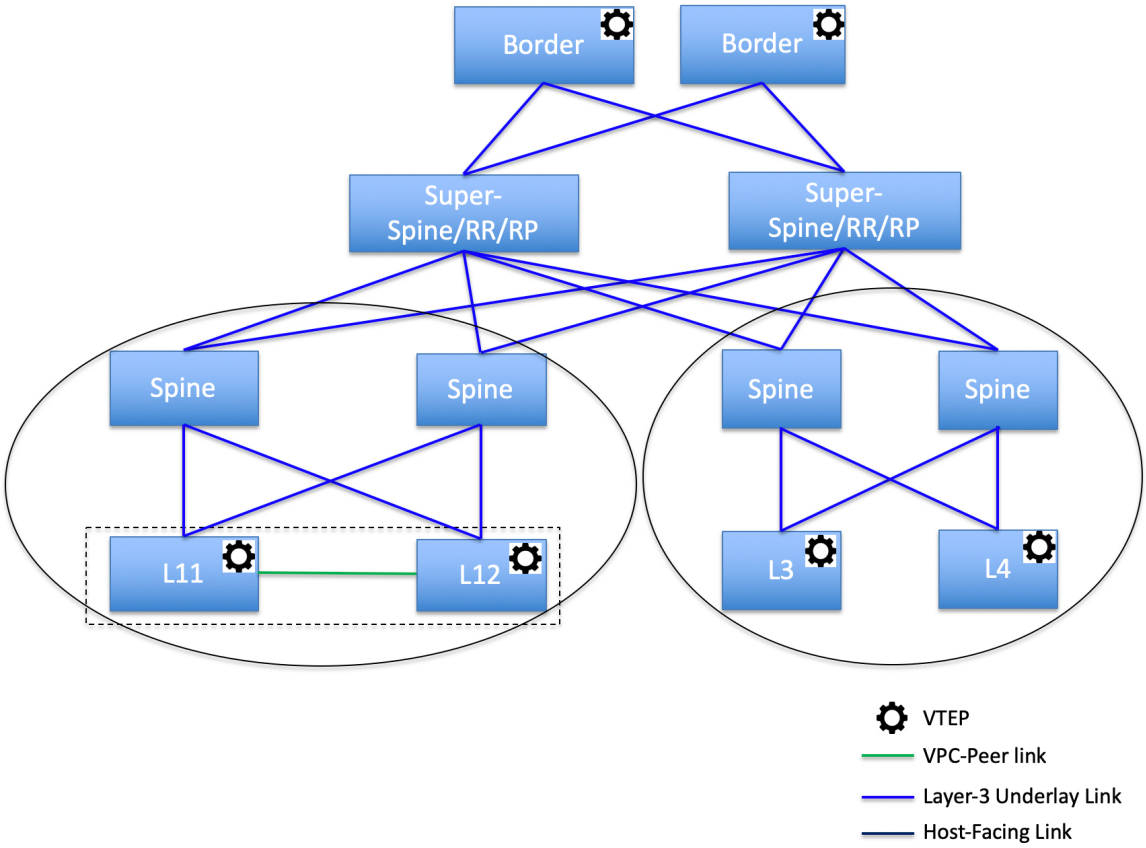
NDFC は、スーパー スパイン スイッチで次のトポロジをサポートします。

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, on page 334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。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 （108 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 111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 111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（102 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 （145 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 （203 ページ）およびテンプレート （Templates） （513 ページ）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 （Templates） 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 （221 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 （221 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 （234 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。
- 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。

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 （731 ページ） 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 （179 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） （176 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。

[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 （108 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 （175 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 8000 シリーズ ルータ

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（102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.d31q13jXA7iHM677gwqQbFSH2/3oQEaHRq08.
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
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 （102 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（154 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 （158 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（333 ページ）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 （194 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 （94 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 （168 ページ）またはIPFM ファブリックの削除 （168 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 （172 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 （169 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 （179 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 （108 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 （194 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 （166 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 （166 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 （88 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 （108 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 （194 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 （172 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 （172 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 （174 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） （367 ページ） 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（169 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 （174 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 Nexsus 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 94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。

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。

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

ユーザー ロール	AVPair 値
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

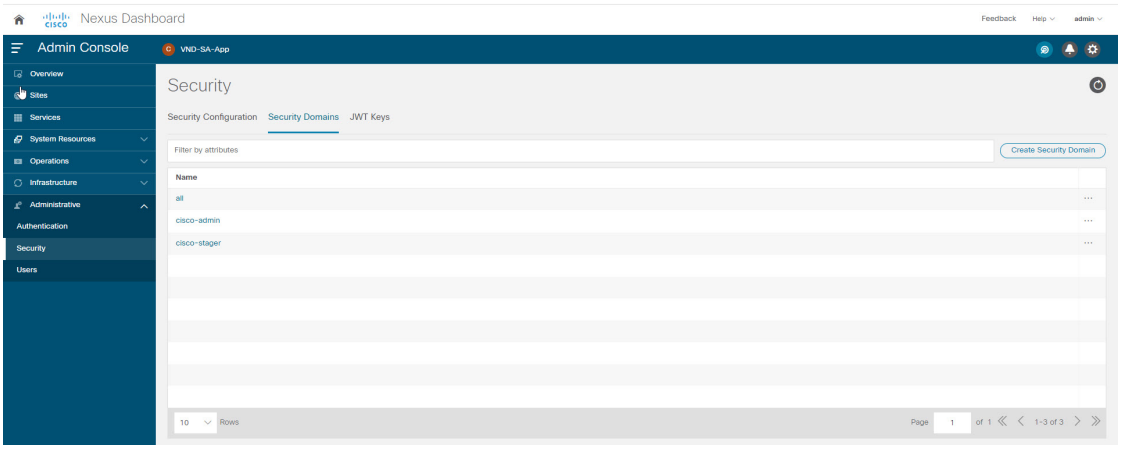
NDFCにはさまざまなファブリックがあります。デフォルトでは、ユーザーはすべてのファブリックの管理者です。たとえば、ユーザー名 **Cisco** は、Fabric-A への 管理者ロール アクセスと、別の Fabric-B へのステージャ ロール アクセスを持つことができます。

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。

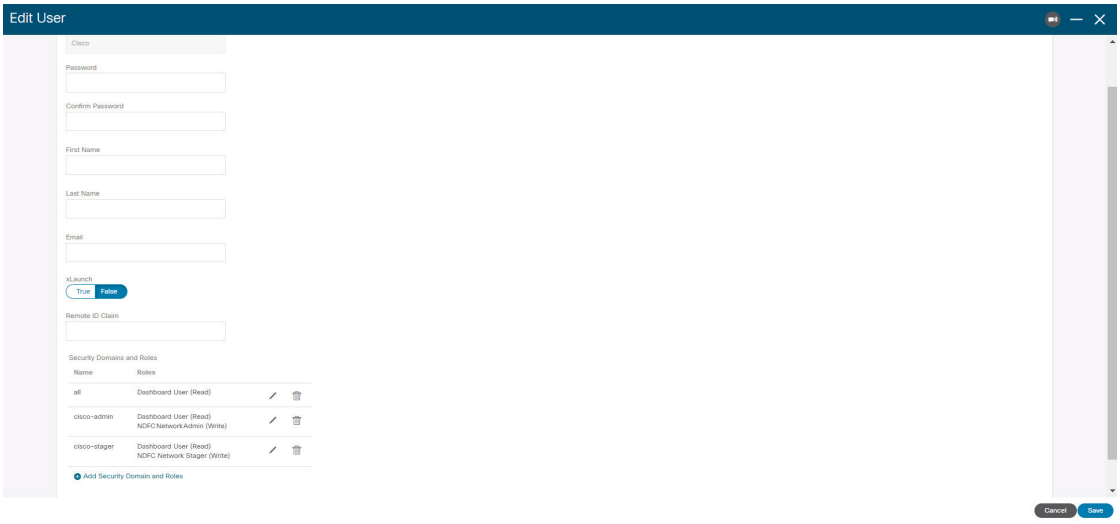
c) [ユーザー ID（User ID）] テキスト フィールドに **Cisco** と入力し、それぞれのフィールドに適切なパスワードを設定します。

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。

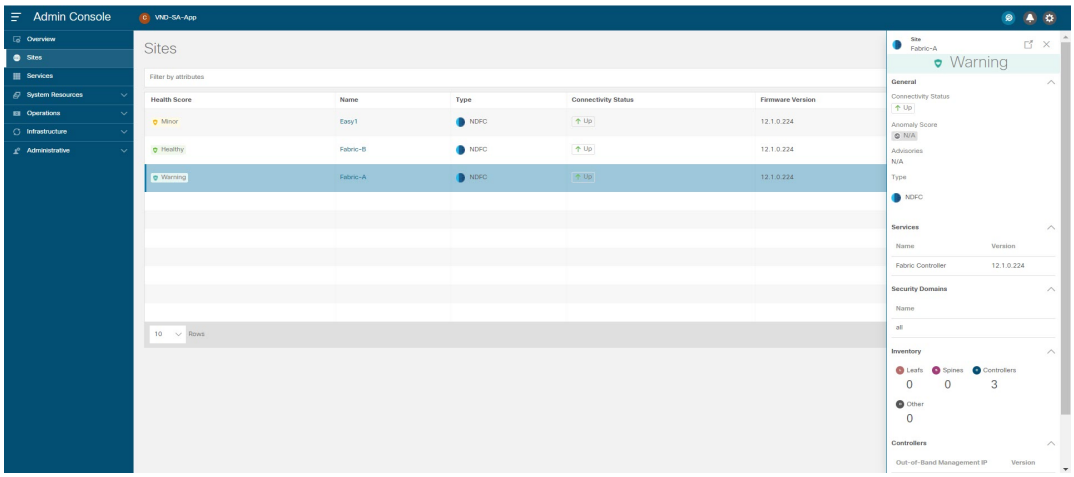
[ユーザーの編集（Edit User）] ウィンドウが表示されます。

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。
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。

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。
スイッチの追加	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。
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、「スイッチのプレビュー」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。

Actions	説明
VXLAN OAM	詳細については、VXLAN OAM （192 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。
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 （312 ページ）を参照してください。 （注） これは、Nexus Dashboard Fabric Controller、Release 12.0.1a のフィーチャのプレビューです。ラボセットアップでのみ、ベータ版としてマークされたこの機能を使用することをお勧めします。実稼働環境でこれらのフィーチャを使用しないでください。

[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 （243 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）]（259 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。

[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。
- 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 207 • ファブリック間リンクの作成, on page 205
編集	選択したファブリックを編集できます。
削除	選択したファブリックを削除できます。

アクション項目	説明
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 （731 ページ） 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 （Templates）」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。

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 （379 ページ）
- インターフェイスグループ （393 ページ）

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。

フィールド	説明
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。
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。

アクション項目	説明
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（474 ページ）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。

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 （93 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 （218 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。
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。

アクション項目	説明
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 (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。

[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。

[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 （175 ページ） を参照してください。

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 （215 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 （93 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 （393 ページ） 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（231 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（215 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 197 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 （253 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（252 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 257
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 197 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。

（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。

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 （298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	
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。
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	
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。
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。

フィールド	説明
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 （274 ページ）を参照してください。

フィールド	説明
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。

フィールド	説明
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。
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。

フィールド	説明
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 （273 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（278 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 （280 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。**出力** NAT モードでは、デフォルトの VRF が選択されます。これは編集できません。

[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。

出力インターフェイス マッピング

[LAN] > [ファブリック（Fabrics）] を選択します。出力インターフェイス 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）] > [出力インターフェイス マッピング（Egress Interface Mappings）] をクリックします。

次の表で、[出力インターフェイス マッピング（Egress Interface Mappings）] 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
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。
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。

次の表に、[出力インターフェイス マッピング（Egress Interface Mappings）] 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を示します。

アクション項目	説明
NAT 出力インターフェイスマッピングの作成	[NAT 出力インターフェイス マッピングの作成（Create NAT Egress Interface Mapping）] を選択して、出力インターフェイス マッピングを追加します。
NAT 出力インターフェイスマッピングの編集	テーブルからモードを選択し、[NAT 出力 インターフェイス マッピングの編集（Edit NAT Egress Interface Mapping）] を選択して出力インターフェイス マッピングを編集します。

アクション項目	説明
NAT 出力インターフェイス マッピングの削除	テーブルからモードを選択し、[出力インターフェイス マッピングの削除（Delete NAT Egress Interface Mapping）] を選択して出力インターフェイス マッピングを削除します。
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 出力インターフェイスマッピングを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。
選択した NAT 出力インターフェイス マッピングの展開	テーブルからモードを選択し、[選択した NAT 出力インターフェイス マッピングの展開（Deploy Selected NAT Egress Interface Mappings）] を選択して、選択した出力インターフェイス マッピングをスイッチに展開します。
すべての NAT 出力インターフェイス マッピングの展開	[すべての NAT 出力インターフェイス マッピングの展開（Deploy All NAT Egress Interface Mappings）] を選択して、すべての出力インターフェイス マッピングをスイッチに展開します。
選択した NAT 出力インターフェイス 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 出力インターフェイス マッピングの展開解除（Undeploy Selected NAT Egress Interface Mappings）] を選択して、選択した出力インターフェイス マッピングをスイッチから展開解除します。
すべての NAT 出力インターフェイス マッピングの展開解除	[すべての NAT 出力インターフェイス マッピングの展開解除（Undeploy All NAT Egress Interface Mappings）] を選択して、スイッチからすべての出力インターフェイス マッピングを展開解除します。
すべての失敗したNAT出力インターフェイス マッピングのやり直し	失敗したすべての出力インターフェイス マッピングを展開するには、[すべての失敗した NAT 出力インターフェイス マッピングのやり直し（Redo All Failed NAT Egress Interface Mappings）] を選択します。

アクション項目	説明
導入履歴	選択した出力インターフェイス マッピングの展開履歴を表示するには、テーブルからモードを選択し、[展開履歴（Deployment History）] を選択します。 [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。 • マップ インターフェイス：出力インターフェイス 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：出力インターフェイス 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：マッピングが展開される出力インターフェイス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。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：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：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。 • 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 出力インターフェイスマッピングの追加

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）]** タブをクリックします。

ステップ 4 **[出力インターフェイス マッピング（Egress Interface Mappings）]** タブをクリックします。

ステップ 5 **[アクション（Actions）] [NAT出力インターフェイス マッピングの作成（Create NAT Egress Interface Mapping）]** をクリックして、出力インターフェイス マッピングを追加します。

[出力インターフェイス マッピングの追加（Add Egress Interface Mappings）] ウィンドウが表示されます。

ステップ 6 **[出力インターフェイス マッピングの追加（Add Egress Interface Mappings）]** ウィンドウで、次の情報を指定します。

[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、**[出力インターフェイス マッピング（Egress Interface Mappings）]** ウィンドウで選択されたスイッチに基づきます。

[出力インターフェイス（Egress Interfaces）]：出力インターフェイスを指定します。1 つ以上の出力インターフェイスを選択できます。出力インターフェイスとマップ インターフェイスは、選択したスイッチに基づいて事前入力されます。

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。

[マップ インターフェイス（Map Interface）1]：マップ インターフェイスを指定します。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。

[最大レプリケーション（Max Replications）]：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。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 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 出力インターフェイス マッピングの編集

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 **[出力インターフェイス マッピング（Egress Interface Mappings）]** タブをクリックします。

ステップ 5 出力インターフェイス マッピングを編集するには、**[アクション（Actions）] [NAT出力インターフェイス マッピングの編集（Edit NAT Egress Interface Mapping）]** をクリックします。

[出力インターフェイス マッピングの編集（Edit Egress Interface Mappings）] ウィンドウが表示されます。

ステップ 6 **[出力インターフェイスマッピングの編集（Edit Egress Interface Mappings）]** ウィンドウで、次の情報を指定します。

出力インターフェイスと **[最大レプリケーション（Max Replications）]** フィールドを編集します。**[最大レプリケーション（Max Replications）]** の新しい値を 1 ー 40 の範囲内で指定します。

ステップ 7 **[保存して展開（Save & Deploy）]** をクリックして、出力インターフェイスマッピングを保存し、展開します。

出力インターフェイス マッピングの削除

出力インターフェイス マッピングをマッピングを削除しても、出力インターフェイス マッピングはスイッチから展開解除されません。そのため、Nexusダッシュボードファブリック コントローラ から削除する前に、スイッチから出力インターフェイス マッピングを展開解除してください。

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 **[出力インターフェイス マッピング（Egress Interface Mappings）]** タブをクリックします。

ステップ 5 選択した出力インターフェイスマッピングを削除するには、**[アクション（Actions）]> [NAT出力インターフェイスマッピングの削除（Delete NAT Egress Interface Mapping）]** をクリックします。

ステップ 6 **[確認（Confirm）]**をクリックして、選択した出力インターフェイスマッピングを削除します。

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。
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。

アクション項目	説明
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。

[モード（Mode）]：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 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（Pre-Translation Group）]：NAT の前のマルチキャスト 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 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。

[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。

[Statis Oif]：このフィールドは**入力**モードでは無効です。**出力**モードでは、定義された出力インターフェイス マッピングに基づいてインターフェイスに入力します。

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。
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。

フィールド	説明
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 305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 305を参照してください。
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 305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 305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 305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 305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 305 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 246 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。

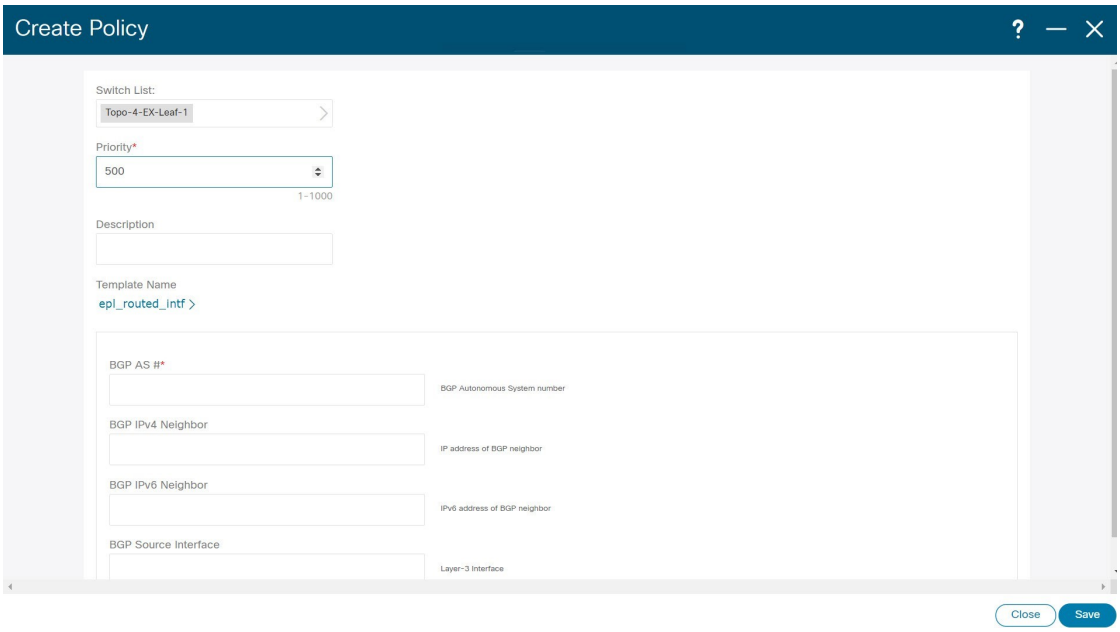
- 管理
- データ

（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。

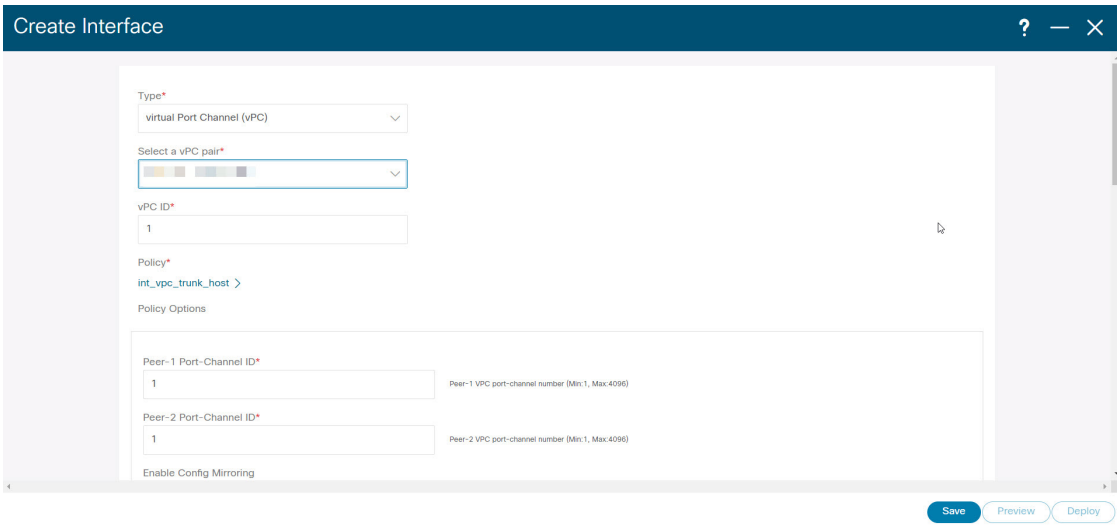
管理インターフェイスは、レイヤ 2 またはレイヤ 3 隣接の mgmt0 インターフェイスにより、デバイスに到達できるようにします。これにより、POAPを含むこれらのデバイスを管理およびモニタできます。Nexusダッシュボード ファブリック コントローラEPLでは、とルートリフレクタの間でBGPピアリングが必要です。Nexusダッシュボード ファブリック コントローラNexusデバイスのBGPプロセスは通常、デフォルトVRFで実行されるため、からファブリックへのインバンドIP接続が必要です。Nexusダッシュボード ファブリック コントローラデータ ネットワーク インターフェイスは、Nexus 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。

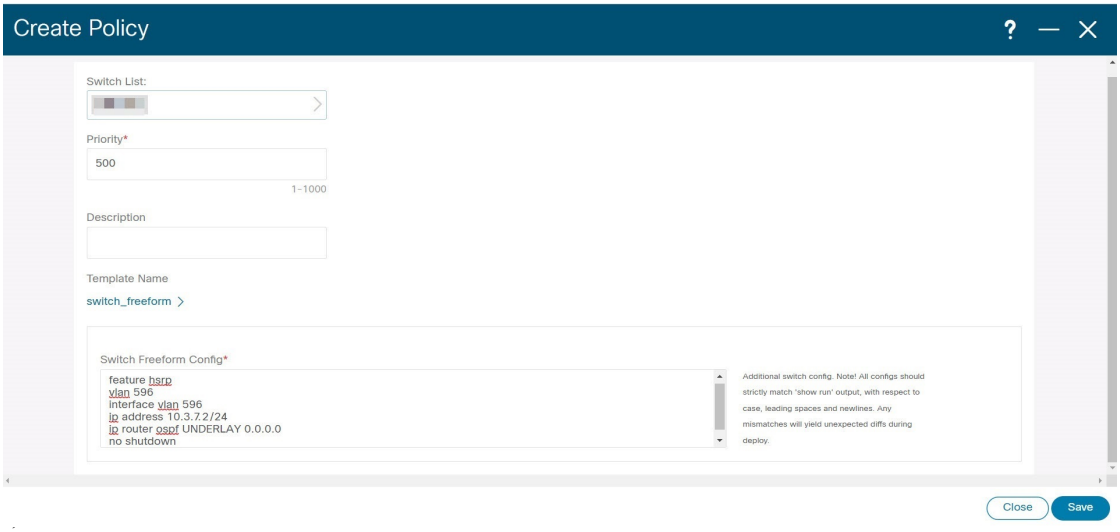
ファブリック側では、スタンドアロン Nexusダッシュボード ファブリック コントローラ 展開の場合、Nexus Dashboard データ ネットワーク ポートがリーフ上のフロントエンド インターフェイスの 1 つに直接接続されていれば、そのインターフェイスを **epl_routed_intf** テンプレートを使用して設定できます。ファブリック内のIGPとしてIS-ISまたはOSPFを使用する場合の、このシナリオの例を以下に示します。



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

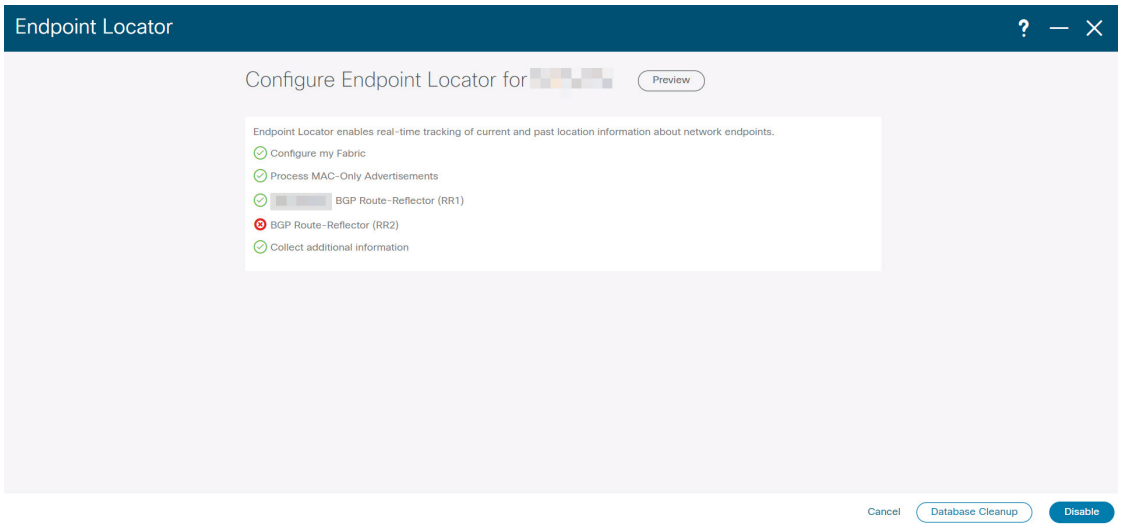
EPLの設定時に、ルートリフレクタ（RR）はBGPピアとして受け入れるように設定されます。Nexusダッシュボード ファブリック コントローラ同じ構成中、Nexusダッシュボード ファブリック コントローラは、データ ネットワーク インターフェイス ゲートウェイを介してスパイン/RR 上の BGP ループバック IP にルートを追加することによっても構成されます。

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 330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。

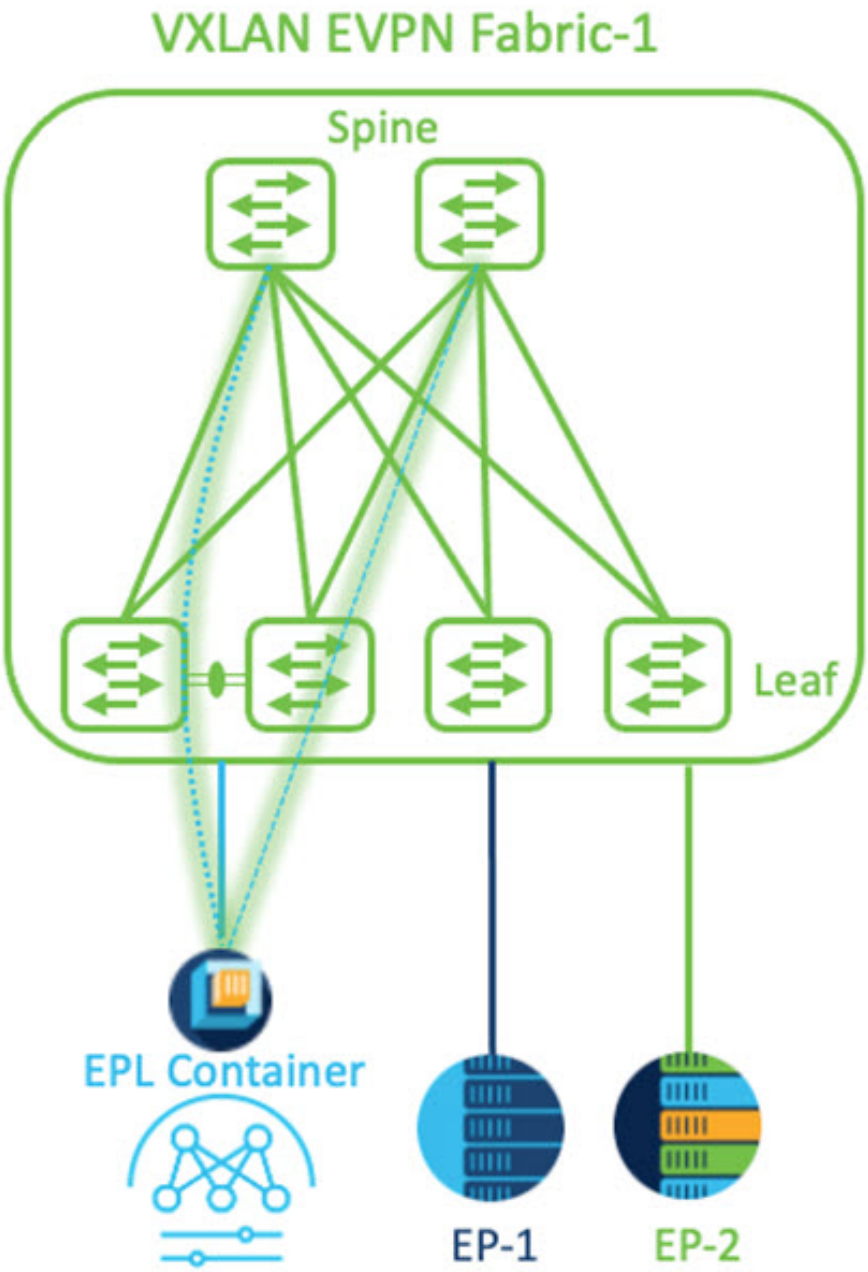
ステップ 2 [Delete]をクリックして続行するか、[Cancel]をクリックして中止します。

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

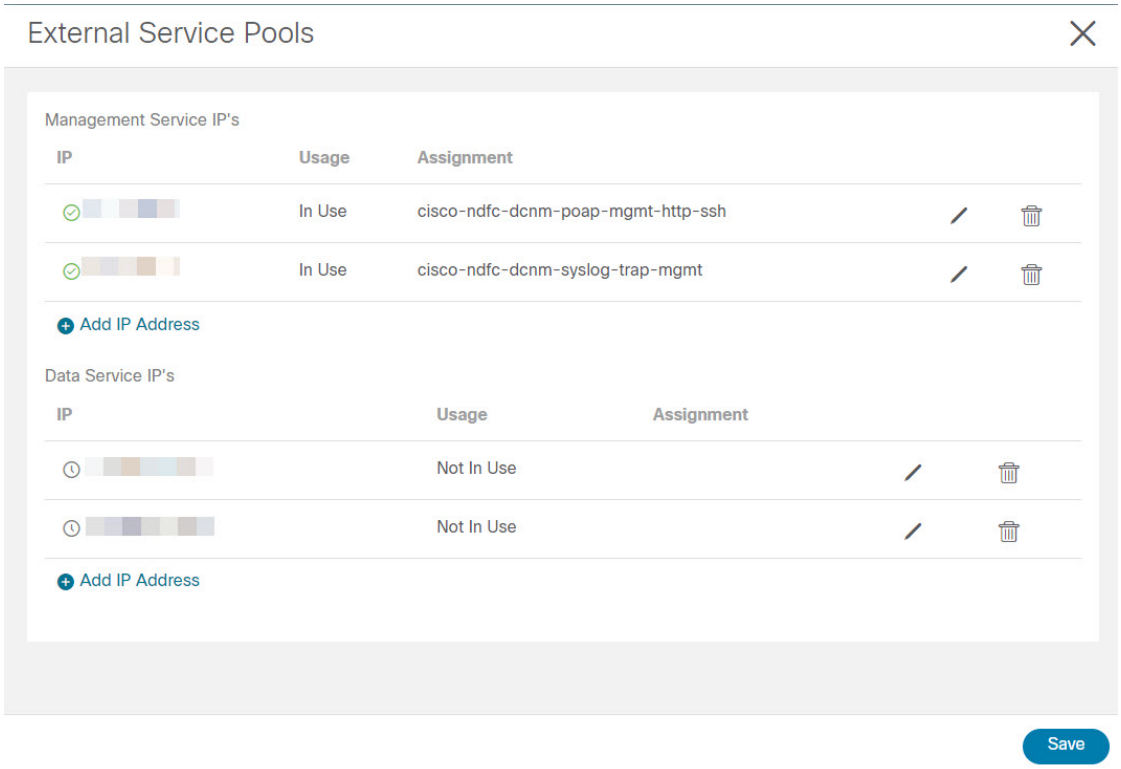
ステップ 1 Cisco Nexus Dashboard で永続 IP アドレスを構成する必要があります。Nexus Dashboard で、**[管理コンソール（Admin Console）]**>**[インフラストラクチャ（Infrastructure）]**>**[クラスタ構成（Cluster Configuration）]**を選択します。

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。

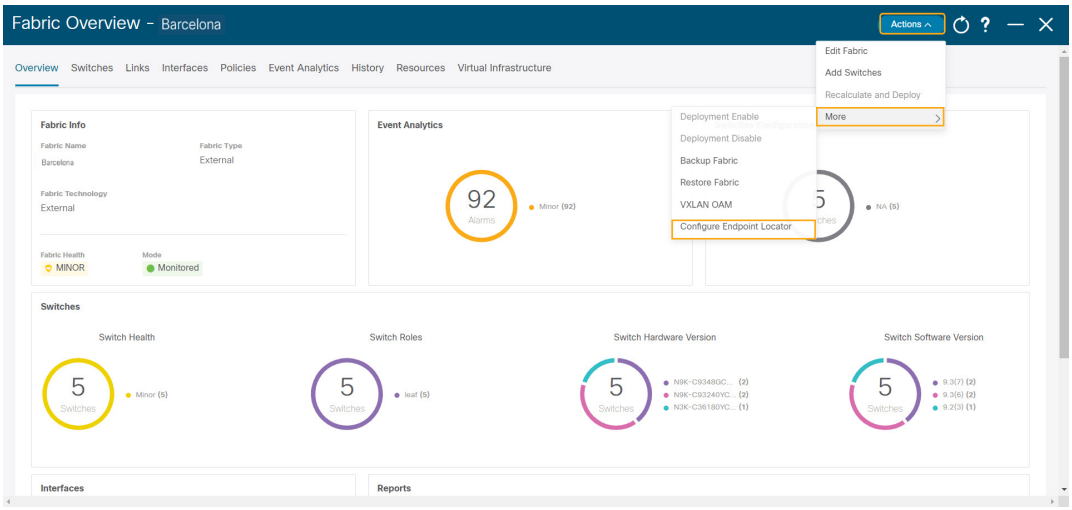
```
[rescue-user@ndfc-12-parth ~]$ ping 192.168.100.254 -c 2
PING 192.168.100.254 (192.168.100.254) 56(84) bytes of data.
64 bytes from 192.168.100.254: icmp_seq=1 ttl=255 time=1.95 ms
64 bytes from 192.168.100.254: icmp_seq=2 ttl=255 time=2.09 ms

--- 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。

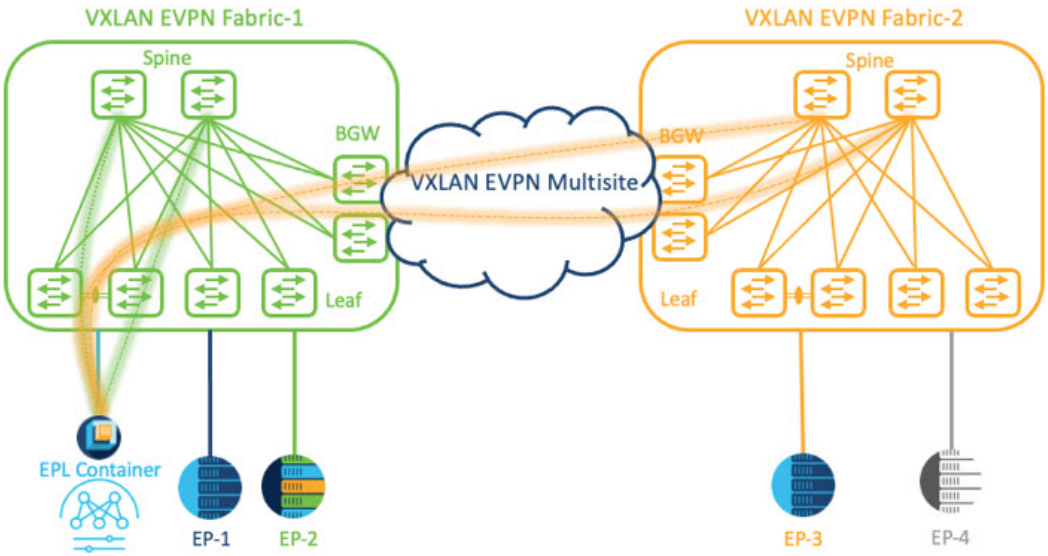
適切な選択を行い、さまざまな入力を確認したら、**[構成の保存（Save Config）]**をクリックして、EPL を有効にします。EPL の有効化中にエラーが発生した場合は、有効化プロセスが中止され、適切なエラーメッセージが表示されます。それ以外の場合、EPLは正常に有効化されます。EPL が有効になると、永続 IP が使用されます。

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。

（注） これは、Nexus Dashboard Fabric Controller、Release 12.0.1a のフィーチャのプレビューです。ラボセットアップでのみ、ベータ版としてマークされたこの機能を使用することをお勧めします。実稼働環境でこれらのフィーチャを使用しないでください。

エンドポイント ロケータの削除

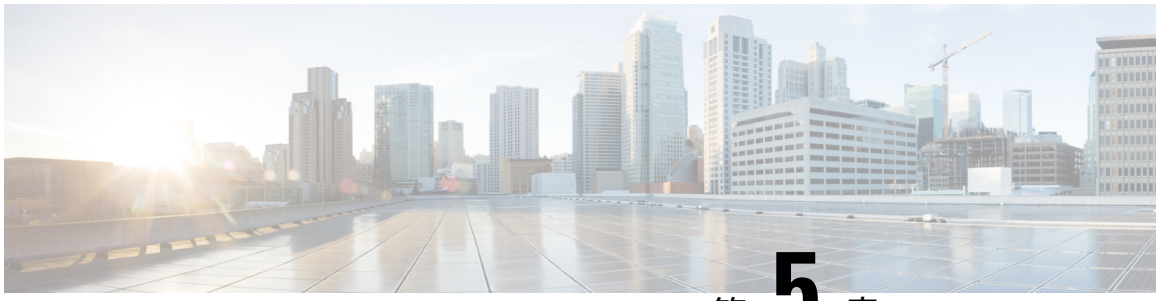
Cisco Nexusダッシュボード ファブリック コントローラ Web UI からエンドポイント ロケータを無効にするには、次の手順を実行します。

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。



第 5 章

スイッチ

スイッチ

次の表で、**[スイッチ（Switches）]** 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。

フィールド	説明
スイッチ	スイッチの名前を指定します。
[IPアドレス（IP Address）]	スイッチの IP アドレスを指定します。
ロール	スイッチに割り当てるロールを指定します。
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。
Fabric Name（ファブリック名）	スイッチに関連付けられているファブリック名を指定します。
Config Status	構成ステータスを指定します。 ステータスは、In-Sync または Out-of-sync のいずれかになります。
動作ステータス	構成ステータスを指定します。 ステータスは、In-Sync または Out-of-sync のいずれかになります。
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。
vPC ロール	スイッチの vPCロール を指定します。

フィールド	説明
vPC ピア	スイッチの vPC ピアを指定します。

ファブリックへのスイッチの追加

UI パス：**[LAN]** > **[スイッチ（Switches）]** > **[アクション（Actions）]** > **[スイッチの追加（Add Switches）]**

各ファブリックのスイッチは一意であるため、1 つのファブリックに追加できるスイッチは 1 つだけです。

Note Cisco Nexus Dashboard には、ノードごとに 2 つの論理インターフェイス、つまり管理インターフェイス（bond1br）とファブリック（データ）インターフェイス（bond0br）があります。Cisco Nexus Dashboard ファブリック コントローラの場合、Nexus Dashboard 管理インターフェイスとファブリック インターフェイスは異なる IP サブネットに存在する必要があります。デフォルトでは、Nexus Dashboard サービスのルートはファブリック インターフェイス経由です。オペレータは、管理インターフェイス（bond1br）経由で到達する必要があるスイッチに接続するために、Nexus Dashboard 管理ネットワークにスタティック ルートを追加する必要があります。これにより、ポッドのルートが管理インターフェイスを出口インターフェイスとして使用するようになります。

Note スイッチの検出または追加のスイッチを行な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。

既存のファブリックにスイッチを追加するには、次の手順を実行します。

1. Web Nexusダッシュボード ファブリック コントローラ UIから、**[LAN]** > **[スイッチ（Switches）]**を選択します。
2. **[スイッチ（Switches）]タブで、[アクション（Actions）]**>**[スイッチの追加（Add Switches）]** を選択します。

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

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

   [スイッチの追加（Add Switches）] ウィンドウにはデフォルトの [検出（Discover）] タブがあり、選択したファブリックに基づいて他のタブが表示されます。

さらに、スイッチとインターフェイスを事前プロビジョニングできます。詳細については、「デバイスの事前プロビジョニング」および「イーサネット インターフェイスの事前プロビジョニング」を参照してください。

Note Nexusダッシュボード ファブリック コントローラ でピリオド文字（.）を含むホスト名を持つスイッチが検出されると、ドメイン名として扱われ、切り捨てられます。ピリオド文字（.）の前のテキストのみがホスト名と見なされます。次に例を示します。

- ホスト名が **leaf.it.vxlan.bgp.org1-XYZ** の場合、Nexusダッシュボード ファブリック コントローラ で **leaf** のみが表示されます。
- ホスト名が **leaf-itvxlan.bgp.org1-XYZ** の場合、Nexusダッシュボードファブリック コントローラ で **leafit-vxlan** のみが表示されます。

Note スイッチ名またはホスト名がファブリック内で一意であることを確認してください。

新しいスイッチの検出

1. 新しい Cisco NX-OS デバイスの電源がオンになると、通常、そのデバイスにはスタートアップ構成も構成ステートもありません。その結果、NX-OS で電源が投入され、初期化後に POAP ループに入ります。デバイスは、mgmt0 インターフェイスを含むアップ状態のすべてのインターフェイスで DHCP 要求の送信を開始します。
2. デバイスと Nexusダッシュボードファブリック コントローラ の間にIP到達可能性がある限り、デバイスからのDHCP要求は Nexusダッシュボード ファブリック コントローラ に転送されます。ゼロデイ デバイスを簡単に起動するには、前述のように、**ファブリック設定**でブート ストラップ オプションを有効にする必要があります。
3. ファブリックに対してブートストラップが有効になっている場合、デバイスからの DHCP 要求は Nexusダッシュボード ファブリック コントローラ によって処理されます。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割り当てられた一時IP アドレスは、デバイス モデル、デバイス NX-OS バージョンなどを含むスイッチに関する基本情報を学習するために使用されます。
4. Nexusダッシュボード ファブリック コントローラ UIで、**[スイッチ（Switch）]** > **[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）] ウィンドウにデフォルトのタブが表示されます。
5. **[ブートストラップ（Bootstrap）（POAP）]** オプション ボタンを選択します。

   前述のように、Nexusダッシュボード ファブリック コントローラ はデバイスからシリアル番号、モデル番号、およびバージョンを取得し、それらを[インベントリ管理（Inventory Management）] ウィンドウに表示します。また、IP アドレス、ホスト名、およびパスワー

ドを追加するオプションが使用可能になります。スイッチ情報が取得されない場合は、ウィンドウを更新します。

Note

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

注：Nexus 9000 シリーズ スイッチのシリアル番号のみを変更できます。

スイッチの横にあるチェックボックスを選択し、スイッチのクレデンシャル（IP アドレスとホスト名）を入力します。

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

デバイスは事前にプロビジョニングできます。デバイスを事前プロビジョニングするには、「デバイスの事前プロビジョニング」の項を参照してください。

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

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

   新しいユーザを指定できます。ラジオ ボタン **[新規ユーザの指定（Specify a new user）]** を選択し、**[ユーザ名（Username）]**、**[パスワード（Password）]** を入力して、ドロップダウンリストから **[認証プロトコル（Authentication Protocol）]** を選択します。

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

7. （任意）スイッチの検出に検出クレデンシャルを使用します。

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

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

      [OK] をクリックして、ディスカバリ クレデンシャルを保存します。

      検出クレデンシャルが指定されていない場合は、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。

8. 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。

9. 最新情報を入手するには、**[トポロジの更新（Refresh Topology）]** ボタンをクリックします。追加されたスイッチは、POAP サイクルを実行します。スイッチをモニタし、POAP 完了を確認します。

10. 追加されたスイッチが POAP を完了すると、ファブリック ビルダ トポロジページが追加されたスイッチで更新され、検出された物理接続が示されます。スイッチに適切なロールを設定し、ファブリック レベルで Deploy Config 操作を実行します。ファブリック設定、スイッチロール、トポロジなどが Fabric Builder によって評価され、スイッチの適切な意図された設定が保存操作の一部として生成されます。保留中の設定は、新しいスイッチをインテントと同期させるために新しいスイッチに導入する必要がある設定のリストを提供します。

Note ファブリックで変更が発生して Out-of-Sync が発生した場合は、変更を展開する必要があります。このプロセスは、「既存スイッチの検出」の項で説明したものと同じです。

ファブリックの作成時に、**[管理性（Manageability）]** タブに AAA サーバ情報を入力した場合は、各スイッチの AAA サーバパスワードを更新する必要があります。そうでない場合、スイッチの検出は失敗します。

11. 保留中の設定が展開されると、すべてのスイッチの **[進捗（Progress）]** 列に 100％ と表示されます。

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

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

14. スイッチとリンクが 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。

15. Nexusダッシュボード ファブリック コントローラ GUIでは、検出されたスイッチはスタンドアロン ファブリック トポロジで確認できます。このステップまでで、POAP は基本設定で完了します。**LAN** > **スイッチ** を介してインターフェイスを設定する必要があります。スイッチを選択すると、スライドインペインが表示され、**[起動（Launch）]** アイコンをクリックします。**[スイッチの概要（Switches Overview）]** タブで、**[インターフェイス（Interface）]** タブをクリックして追加設定を行いますが、これに限定されません。

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

vPCのペアリング/ペアリング解除または advertise-pip オプションを有効または無効にするか、マルチサイト構成を更新する場合は、**[構成の展開（Deploy Config）]** 操作を使用する必要があります。操作の終了時に、nve インターフェイスで **shutdown** または **no shutdown** コマンドを設定するように求めるエラーが表示されます。vPC設定を有効にした場合のエラー スクリーンショットのサンプル。

解決するには、**[インターフェイス（Interfaces）]** > **[アクション（Actions）]** > **[展開（Deploys）]** タブに移動し、nve インターフェイスでシャットダウン操作を展開してから、No Shutdown 構成を実行します。これを次の図に示します。上矢印は No Shutdown 操作に対応し、下矢印はShutdown 操作に対応します。

スイッチを右クリックすると、さまざまなオプションを表示できます。

- **ロールの設定**：スイッチにロールを割り当てます（スパイン、ボーダーゲートウェイなど）。

Note

- スイッチのロールの変更は、**構成の展開**を実行する前にのみ許可されます。
- スイッチのロールは、スイッチ上にオーバーレイがない場合に変更できますが、スイッチ操作の項で指定された許可されたスイッチ ロール変更のリストに従ってのみ変更できます。

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

  vPCペアの仮想リンクを作成するか、既存の物理リンクをvPCペアの仮想リンクに変更できます。
- **インターフェイスの管理**：スイッチ インターフェイスに構成を展開します。
- **ポリシーの表示/編集**：スイッチ ポリシーを参照し、必要に応じて編集します。
- **履歴**：スイッチの展開履歴を表示します。
- **履歴**：スイッチの展開およびポリシーの変更履歴を表示します。

  [ポリシー変更履歴（Policy Change History）]タブには、追加、更新、削除などの変更を行ったユーザとともにポリシーの履歴が一覧表示されます。

  ポリシーの **[ポリシー変更履歴（Policy Change History）]** タブで、**[生成された構成（Generated Config）]** 列の **[詳細な履歴（Detailed History）]** をクリックして、前後の生成された構成を表示します。

  次の表に、ポリシーテンプレートインスタンス（PTI）の前後に生成される構成の概要を示します。

PTI の操作	前に生成された構成	生成後の構成
追加	Empty	構成が含まれています
更新	変更前の構成が含まれています	変更後の構成が含まれています
マーク - 削除	削除する設定が含まれます。	色を変更して削除する構成が含まれます。
削除	構成が含まれています	Empty

Note ポリシーまたはプロファイルテンプレートが適用されると、テンプレートのアプリケーションごとにインスタンスが作成されます。これは、ポリシー テンプレート インスタンスまたは PTI と呼ばれます。

- **[構成のプレビュー（Preview Config）]**：保留中の構成と、実行中の構成と予想される構成の比較を表示します。
- **展開構成** - スイッチ構成ごとに展開します。
- 検出：このオプションを使用して、スイッチのクレデンシャルを更新し、スイッチをリロードし、スイッチを再検出し、ファブリックからスイッチを削除できます。

新しいファブリックが作成され、ファブリック構成スイッチが 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、アンダーレイ設定がそれらのスイッチで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 との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。
- ネットワークを作成し、スイッチに展開します。

既存のスイッチの検出

Cisco Nexusダッシュボード ファブリック コントローラ Web UIで既存のスイッチを検出するには、次の手順を実行します。

手順

ステップ 1 **[スイッチの追加（Add Switches）]** をクリックした後、**[スイッチの検出（Discover Switches）]** をクリックして、1 つ以上の既存のスイッチをファブリックに追加します。

この場合、既知のクレデンシャルと事前プロビジョニングされた IP アドレスを持つスイッチがファブリックに追加されます。

ステップ 2 スイッチのIPアドレス（シードIP）、ユーザ名、およびパスワード（**[ユーザ名（Username）]** フィールドと **[パスワード（Password）]** フィールド）は、ユーザによる入力として提供されます。**[構成の保持（Preserve Config）]** チェックボックスがデフォルトで選択されています。これは、ファブリックへのデバイスのブラウンフィールドインポートに対してユーザが選択するオプションです。デバイス設定がインポートプロセスの一部としてクリーンアップされるグリーンフィールドインポートの場合、ユーザは**[構成の保持（Preserve Config）]**チェックボックスを選択しないでください。

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

ステップ 3 **[スイッチの検出（Discover Switches）]** をクリックします。

[スイッチの追加（Add Switches）] ウィンドウが表示されます。**[最大ホップ（Max Hops）]** フィールドに 2 が入力されているため（デフォルト）、指定された IP アドレス（リーフ 91）を持つスイッチとそのスイッチからの 2 つのホップが **[スイッチの追加（Add Switches）]** の結果に入力されます。

ステップ 4 Cisco Nexusダッシュボード ファブリック コントローラ がスイッチに対して正常なシャローディスカバリを実行できた場合、ステータス列に **[管理性（Manageable）]** と表示されます。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て、**[スイッチの追加（Add Switches）]** をクリックします。

この例では1つのスイッチの検出について説明しますが、複数のスイッチを同時に検出できます。

スイッチ検出プロセスが開始されます。**[進行状況（Progress）]** 列には、選択したすべてのスイッチの進行状況が表示されます。完了時に各スイッチの**完了**を表示します。

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

エラー メッセージが表示された場合は、画面を閉じます。[ファブリック トポロジ(fabric topology)] 画面が表示されます。エラー メッセージは、画面の右上に表示されます。必要に応じてエラーを解決し、[アクション（Actions）] パネルの **[スイッチの追加（Add Switches）]** をクリックしてインポート プロセスを再度開始します。

Cisco Nexusダッシュボードファブリック コントローラ がすべてのスイッチを検出し、**[進行状況（Progress）]** 列にすべてのスイッチの完了が表示されたら、画面を閉じます。*[*スタンドアロン ファブリック トポロジ（Standalone fabric topology）] 画面が再び表示されます。追加されたスイッチのスイッチ アイコンが表示されます。

（注） スイッチの検出中に次のエラーが発生することがあります。

ステップ 5 最新のトポロジ ビューを表示するには、**[トポロジの更新（Refresh topology）]** をクリックします。

すべてのスイッチが追加され、ロールが割り当てられると、ファブリック トポロジにはスイッチとスイッチ間の接続が含まれます。

ステップ 6 デバイスを検出したら、各デバイスに適切なロールを割り当てます。ロールの詳細については、「セット ロールの割り当て」を参照してください。

表示用に階層レイアウトを選択すると（[アクション（Actions）]パネルで）、トポロジはロールの割り当てに従って自動的に配置され、リーフ デバイスが下部に、スパイン デバイスが上部に接続され、境界デバイスが上部に配置されます。

vPC スイッチ ロールの割り当て：スイッチのペアを vPC スイッチ ペアとして指定するには、スイッチを右クリックし、スイッチのリストから vPC ピア スイッチを選択します。

AAA サーバ パスワード：（**[管理性（Manageability）]** タブで）AAA サーバ情報を入力した場合は、各スイッチで AAA サーバ パスワードを更新する必要があります。そうでない場合、スイッチの検出は失敗します。

Cisco Nexusダッシュボード ファブリック コントローラ を使用して新しい vPC ペアが正常に作成および展開されると、コマンドがスイッチに存在する場合でも、**no ip redirects CLI** のいずれかのピアが同期しなくなることがあります。この非同期は、実行構成でCLIを表示するためのスイッチの遅延が原因で発生し、構成のコンプライアンスに相違が生じます。**[構成の展開（Config Deployment）]** ウィンドウでスイッチを再同期して、差分を解決します。

ステップ 7 **[Save（保存）]** をクリックします。

テンプレートとインターフェイスの設定は、スイッチのアンダーレイ ネットワーク構成を形成します。また、ファブリック構成の一部として入力されたフリーフォーム CLI（[詳細（Advanced）]タブで入力されたリーフおよびスパイン スイッチのフリー フォーム設定）も展開されます。

構成のコンプライアンス：プロビジョニングされた構成とスイッチの構成が一致しない場合、**[ステータス（Status）]** 列に非同期が表示されます。たとえば、CLI を使用してスイッチの機能を手動で有効にすると、設定が一致しなくなります。

Cisco Nexusダッシュボード ファブリック コントローラ からファブリックにプロビジョニングされた設定が正確であることを確認したり、逸脱（アウトオブバンド変更など）を検出したりするために、Nexusダッシュボード ファブリック コントローラ の構成コンプライアンスエンジンは、必要な修復構成を報告し、提供します。

[展開構成（Deploy Config）] をクリックすると、**[構成の展開（Config Deployment）]** ウィンドウが表示されます。

ステータスが非同期の場合は、デバイスの Nexusダッシュボード ファブリック コントローラとの設定に不整合があることを示しています。

[再同期（Re-sync）] 列のスイッチごとに [再同期（Re-sync）] ボタンが表示されます。大規模なアウトオブバンド変更がある場合、または設定変更が Nexusダッシュボード ファブリック コントローラ 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 Nexusダッシュボード ファブリック コントローラ 状態を再同期します。再同期操作は、スイッチに対して完全な CC 実行を実行し、「show run」および「show run all」コマンドをスイッチから再収集します。再同期プロセスを開始すると、進行状況メッセージが画面に表示されます。再同期中に、実行構成がスイッチから取得されます。スイッチの Out-of-Sync/In-Sync ステータスは、Nexusダッシュボード ファブリック コントローラ で定義されたインテントに基づいて再計算されます。

[構成のプレビュー（Preview Config）] 列エントリ（特定の行数で更新）をクリックします。[構成のプレビュー (Config Preview)] 画面が表示されます。

[保留中の構成（PendingConfig）] タブには、正常な展開の保留中の構成が表示されます。

[並べて比較（Side-by-side Comparison）] タブには、現在の設定と予想される設定が一緒に表示されます。

マルチラインバナー motd 構成は、**switch_freeform** を使用するスイッチごと、またはリーフ/スパイン自由形式構成を使用するファブリックごとのいずれかで、自由形式の構成ポリシーを使用して Cisco Nexusダッシュボード ファブリック コントローラ で構成できます。複数行のバナー motdが構成された後、ファブリック トポロジ画面（の右上）で**[構成の展開（Deploy Config）]**オプションを実行して、ポリシーを展開します。そうしないと、ポリシーがスイッチに適切に展開されない可能性があります。**バナー** ポリシーは、単一行のバナー設定のみを設定します。また、自由形式の設定/ポリシーに関連するバナーは1つだけ作成できます。バナー motd を構成するための複数のポリシーはサポートされていません。

ステップ 8 **画面** を閉じます。

構成が正常にプロビジョニングされた後（すべてのスイッチで 100％ の進捗が表示された場合）、画面を閉じます。

ファブリック トポロジが表示されます。構成が成功すると、スイッチのアイコンが緑色に変わります。

スイッチアイコンが赤色の場合は、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 構成が同期していないことを示します。スイッチでの展開が保留中の場合、スイッチは青色で表示されます。保留状態は、保留中の展開または保留中の再計算があることを示します。スイッチをクリックし、**[プレビュー（Preview）]** または **[構成の展開（Deploy Config）]** オプションを使用して保留中の展開を確認するか、**[構成の展開（Deploy Config）]** をクリックしてスイッチの状態を再計算できます。

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

[構成の展開（Deploy Config）] オプションの使用例は、スイッチ レベルの自由形式の設定です。詳細については、 を参照してください。

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

新しいCisco NX-OSデバイスの電源がオンになると、通常、そのデバイスにはスタートアップ構成も構成ステートもありません。その結果、NX-OS で電源が投入され、初期化後に POAP ループに入ります。デバイスは、mgmt0 インターフェイスを含むアップ状態のすべてのインターフェイスで DHCP 要求の送信を開始します。

Nexus Dashboard ファブリック コントローラ リリース 12.0.1a 以降、POAP はユーザが検証したキー交換とパスワードなしの ssh を使用して、構成ファイルへのアクセスを特定のスイッチに

制限します。したがって、デバイスがPOAPを試行するたびに、**[スイッチの追加（Add Switch）] > [ブートストラップ（Bootstrap）]** で新しいキーを受け入れる必要があります。

デバイスと Nexusダッシュボード ファブリック コントローラ の間に IP 到達可能性がある場合、デバイスからのDHCP要求はNexusダッシュボードファブリック コントローラ に転送されます。ゼロデイ デバイスを簡単に起動するには、ブートストラップ オプションを [ファブリック設定（Fabric Settings）] で有効にする必要があります。

ファブリックに対してブートストラップが有効になっている場合、デバイスからのDHCP要求は Nexusダッシュボード ファブリック コントローラ によって処理されます。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割り当てられた一時IPアドレスは、デバイス モデル、デバイス NX-OS バージョンなどを含むスイッチに関する基本情報を学習するために使用されます。

1. **[LAN]> [スイッチ（Switches）]> [スイッチの追加（Add Switches）]** の順に選択します。
2. **[ブートストラップ（Bootstrap）（POAP）]** オプション ボタンを選択します。
3. **[アクション（Actions）]** をクリックし、スイッチを追加します。

   [追加（Add）] オプションを使用してスイッチを 1 つずつ追加するか、**[インポート（Import）]** オプションを使用して複数のスイッチを同時に追加できます。

   [追加（Add）] オプションを使用する場合は、必要な詳細をすべて入力してください。

   注：スイッチが表示されるまでに時間がかかる場合があります。
4. 必要なスイッチを選択します。
5. [編集（Edit）] をクリックします。

   [ブートストラップ スイッチの編集（Edit bootstrap switch）] ダイアログが表示されます。
6. 次の必須詳細情報を入力します。
7. [保存（Save）] をクリックします。
8. スイッチを選択します。
9. **[管理者パスワード（Admin password）]** フィールドに管理者パスワードを入力します。
10. **[選択したスイッチをインポート（Import Selected Switches）]** をクリックします。

返品許可（RMA）

ここでは、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に、ファブリック内の物理スイッチを交換する方法について説明します。

前提条件

- スイッチの交換時に、中断を最小限に抑えてファブリックが稼働していることを確認します。

- POAP RMA フローを使用するには、ファブリックをブートストラップ（POAP）用に設定します。
- 必要に応じて、再計算と展開を複数回実行し、FEX が展開されているスイッチの RMA の FEX 構成をコピーします。

注意事項と制約事項

- スイッチを交換するには、ファブリックから古いスイッチを取り外し、ファブリック内の新しいスイッチを検出します。たとえば、Cisco Nexus 9300-EX スイッチを Cisco Nexus 9300-FX スイッチに交換する場合は、ファブリックから 9300-EX スイッチを取り外し、同じファブリック内の 9300-FX スイッチを検出します。
- Cisco Nexus 7000 シリーズスイッチをアップグレードする前にGIRが有効になっている場合、Nexusダッシュボード ファブリック コントローラ は、Nexusダッシュボード ファブリック コントローラ RMA 手順の開始時に **system mode maintenance** コマンドをスイッチにプッシュします。このコマンドは、デフォルトのメンテナンス モード プロファイルに存在する設定をスイッチに適用します。Cisco Nexus 7000 シリーズ スイッチでのグレースフル挿入および取り外し（GIR）の実行の詳細については、「GIRの構成」を参照してください。

POAP RMA フロー

RMAをプロビジョニングするには、次の手順に従います。

手順

ステップ 1 「ファブリックの概要」に移動します。

ステップ 2 デバイスをメンテナンスモードにします。デバイスをメンテナンスモードにするには、デバイスを選択し、**[アクション（Actions）] > [その他（More）] > [モードの変更（Change Mode）]** をクリックします。[モード（Mode）] ドロップダウンリストで、**[メンテナンス（Maintenance）]** を選択します。

ステップ 3 ネットワークのデバイスを物理的に交換します。物理接続は、交換用スイッチの元のスイッチと同じ場所で行う必要があります。

ステップ 4 RMA フローを開始します。デバイスを選択し、**[アクション（Actions）] > [RMA のプロビジョニング（Provision RMA）]** をクリックします。

ステップ 5 管理者パスワードを設定します。

（任意）検出用の AAA ユーザとパスワードを設定できます。

ステップ 6 交換用デバイスを選択します。

ステップ 7 **[RMA のプロビジョニング（Provision RMA）]**をクリックします。

手動 RMA フロー

このフローは、ブートストラップが不可能な場合（または望ましくない場合）に使用します。

手動RMAをプロビジョニングするには、 の手順に従います。

手順

ステップ 1 デバイスをメンテナンス モード（オプション）にします。

ステップ 2 ネットワーク内のデバイスを物理的に交換します。

ステップ 3 コンソールからログインし、管理 IP とクレデンシャルを設定します。

ステップ 4 Cisco Nexusダッシュボード ファブリック コントローラ シスコは新しいデバイスを再検出します（または、**[Discovery] > [Rediscover]** を手動で選択できます）。

ステップ 5 **[展開（Deploy）]** を使用して、必要な設定を展開します。

ステップ 6 設定によっては、ブレイクアウト ポートまたは FEX ポートが使用中の場合、設定を完全に復元するために再度展開する必要があります。

ステップ 7 展開が正常に完了し、デバイスが「同期中」になったら、デバイスを通常モードに戻す必要があります。

ローカル認証を持つユーザの RMA

（注） このタスクは、非 POAP スイッチにのみ適用されます。

ローカル認証を持つユーザの RMA を実行するには、次の手順を使用します。

手順

ステップ 1 新しいスイッチがオンラインになったら、スイッチに SSH 接続し、「username」コマンドを使用してクリア テキスト パスワードでローカル ユーザ パスワードをリセットします。SNMP パスワードを再同期するには、ローカル ユーザ パスワードをリセットします。パスワードは、転送不可能な形式で構成ファイルに保存されます。

ステップ 2 RMA が完了するまで待ちます。

ステップ 3 スイッチの新しい SNMP MD5 キーを使用して、スイッチの Cisco Nexusダッシュボード ファブリック コントローラ `switch_snmp_user` ポリシーを更新します。

事前プロビジョニングのサポート

Cisco NDFC は、事前のデバイス構成のプロビジョニングをサポートしています。これは特に、デバイスが調達されたものの、まだお客様に配送されていない、または受領されていないシナ

リオに当てはまります。発注書には通常、デバイスのシリアル番号、デバイスモデルなどに関する情報が含まれており、これらの情報を使用して、デバイスをネットワークに接続する前にNDFC でデバイス構成を準備できます。Easy ファブリックと外部/Classic_LAN ファブリックの両方で、Cisco NX-OS デバイスの事前プロビジョニングがサポートされています。

デバイスの事前プロビジョニング

デバイスをファブリックに追加する前にプロビジョニングできます。ただし、ファブリック設定の [ブートストラップ（Bootstrap）] タブに DHCP の詳細を入力します。

事前プロビジョニングされたデバイスは、Nexus Dashboard ファブリック コントローラ で次の設定をサポートします。

- 基本管理
- vPC ペアリング
- ファブリック内リンク
- イーサネット ポート
- ポートチャネル
- vPC
- ST FEX
- AA FEX
- ループバック
- オーバーレイ ネットワーク設定

事前プロビジョニングされたデバイスは、Nexus Dashboard ファブリック コントローラ の次の設定をサポートしていません。

- ファブリック間リンク
- Sub-interface
- インターフェイス ブレークアウト構成

デバイスにブレークアウトリンクが事前プロビジョニングされている場合は、ブレークアウト PTI を生成するために、**[新しいデバイスを事前プロビジョニングに追加（Add a new device to pre-provisioning）]** ウィンドウの **[データ（Data）]** フィールドで、対応するブレークアウトコマンドをスイッチのモデルとゲートウェイとともに指定する必要があります。

（注） 事前プロビジョニング ペイロードの**データ** キーのインターフェイス ブレークアウト CLI には、スイッチからの「show running-configuration」出力にあるとおりの形式が含まれている必要があります。

次のガイドラインに注意してください。

- 複数のブレイクアウト コマンドは、セミコロン（;）で区切ることができます。
- データ JSON オブジェクトのフィールドの定義は次のとおりです。
  - **modulesModel** ：（必須）スイッチ モジュールのモデル情報を指定します。
  - **gateway** ：（必須）スイッチの管理 VRF のデフォルト ゲートウェイを指定します。このフィールドは、デバイスを事前プロビジョニングするインテントを作成するために必要です。デバイスの事前プロビジョニングの一環としてインテントを作成するために、Nexusダッシュボード ファブリック コントローラ と同じサブネット内にある場合でも、ゲートウェイを入力する必要があります。
  - **breakout**：（オプション）スイッチで提供される breakout コマンドを指定します。
  - **portMode**：（オプション）ブレイクアウト インターフェイスのポート モードを指定します。

[データ（Data）] フィールドの値の例を次に示します。

- {"modulesModel": ["N9K-C93180LC-EX"], "gateway": "10.1.1.1/24"}
- {"modulesModel": ["N9K-C93180LC-EX"],"breakout": "interface breakout module 1 port 1 map 10g-4x", "portMode": "hardware profile portmode 4x100G+28x40G", "gateway": "172.22.31.1/24" }
- {"modulesModel": ["N9K-X9736C-EX", "N9K-X9732C-FX", "N9K-C9516-FM-E2", "N9K-C9516-FM-E2", "N9K-C9516-FM-E2", "N9K-C9516-FM-E2", "N9K-SUP-B+", "N9K-SC-A", "N9K-SC-A"], "gateway": "172.22.31.1/24"}
- {"breakout":"interface breakout module 1 port 50 map 10g-4x" , "gateway": "172.16.1.1/24", "modulesModel": ["N9K-C93180YC-EX "]}
- {"modulesModel": ["N9K-X9732C-EX", "N9K-X9732C-EX", "N9K-C9504-FM-E", "N9K-C9504-FM-E", "N9K-SUP-B", "N9K-SC-A", "N9K-SC-A"], "gateway": "172.29.171.1/24", "breakout":"interface breakout module 1 port 1,11,19 map 10g-4x; interface breakout module 1 port 7 map 25g-4x"}
- {"modulesModel" : ["N9K-C93180LC-EX"]、 "gateway" : "10.1.1.1/24","breakout" : "interface breakout module 1 port 1-4 map 10g-4x"、 "portMode" : "hardware profile portmode 48x25G + 2x100G + 4x40G"}

1. **[LAN] > [スイッチ（Switches）] > [スイッチの追加（Add Switches）]** の順に選択します。
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。
3. [アクション（Actions）]をクリックし、スイッチを追加します。

   [追加（Add）] オプションを使用してスイッチを 1 つずつ追加するか、**[インポート（Import）]** オプションを使用して複数のスイッチを同時に追加できます。

   [追加（Add）] オプションを使用する場合は、必要な詳細をすべて入力してください。
4. スイッチを選択します。

5. **[管理者パスワード（Admin password）]** フィールドに管理者パスワードを入力します。
6. **[事前プロビジョニング（Pre-provision）]** をクリックします。

   事前プロビジョニングされたスイッチが追加されます。

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

   詳細については、「返品許可（RMA）」を参照してください。

   POAP RMA 手順を使用する場合は、存在しないデバイスへの接続がないことが予想されるため、接続がないためにデバイスをメンテナンス モードにできないというエラー メッセージを無視します。

イーサネット インターフェイスの事前プロビジョニング

[LAN インターフェイス（LAN Interface）] ウィンドウでイーサネット インターフェイスを事前プロビジョニングできます。この事前プロビジョニング機能は、Easy、外部、および eBGP ファブリックでサポートされています。NDFC で検出される前に、事前にプロビジョニングされたデバイスにのみ、イーサネット インターフェイスを追加できます。

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

始める前に

ファブリックに事前にプロビジョニングされたデバイスがあることを確認してください。詳細については、デバイスの事前プロビジョニング （346 ページ）を参照してください。

手順

ステップ 1 **[LAN ファブリック（LAN Fabrics）]** ウィンドウから事前にプロビジョニングされたデバイスを含むファブリック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 **[インターフェイス（Interfaces）]** タブで、**[アクション（Actions）]** > **[インターフェイスの作成（Create Interface）]**をクリックします。

[インターフェイスの作成（Create Interfaces）] ウィンドウが表示されます。

ステップ 3 **[インターフェイスの作成（Create Interface）]** ウィンドウで、必要なすべての詳細を入力します。

[タイプ（Type）]：ドロップダウン リストから **[イーサネット（Ethernet）]** を選択します。

[デバイスの選択（Select a device）]：事前にプロビジョニングされたデバイスを選択します。

（注） すでに管理されているデバイスにイーサネットインターフェイスを追加することはできません。

[インターフェイス名（Interface Name）]：モジュール タイプに基づいて有効なインターフェイス名を入力します。たとえば、Ethernet1/1、eth1/1、または e1/1 です。同じ名前のインターフェイスが、追加後にデバイスで使用できるはずです。

[ポリシー（Policy）]：インターフェイスに適用する必要があるポリシーを選択します。

詳細については、インターフェイスの追加 （385 ページ）を参照してください。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 **[プレビュー（Preview）]** をクリックして、追加後にスイッチに展開される予定の構成を確認します。

（注） デバイスは事前にプロビジョニングされているため、**[展開（Deploy）]** ボタンはイーサネット インターフェイスでは無効になっています。

vPC ペアの事前プロビジョニング

始める前に

ファブリックの設定で**ブートストラップ**が有効になっていることを確認します。

手順

ステップ 1 両方のデバイスをファブリックにインポートします。詳細については、デバイスの事前プロビジョニング （346 ページ）を参照してください。

事前にプロビジョニングされ、既存のファブリックに追加された 2 台の Cisco Nexus 9000 シリーズ デバイス。**[スイッチの追加（Add Switches）]** を **[アクション（Actions）]** ドロップダウン リストから追加します。**[インベントリ マネージャ（Inventory Management）] 画面で、[パワーオン自動プロビジョニング（PowerOn Auto Provisioning、POAP）]** をクリックします。

デバイスは、ファブリック内に灰色の/未検出デバイスとして表示されます。

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

ステップ 3 物理ピア リンクまたは MCT を持つデバイス間に vPC ペアリングを作成するには、次の手順を実行します。

a) ピア リンクを形成する物理イーサネット インターフェイスをプロビジョニングします。

leaf1-leaf2 間の vPC ピア リンクは、各デバイスのインターフェイス Ethernet1/44-45 で構成されます。**[LAN] > [ファブリック（Fabrics）] > [インターフェイス（Interfaces）]** を選択して、イーサネット インターフェイスを事前プロビジョニングします。詳細については、次を参照してください。

この説明については、イーサネット インターフェイスの事前プロビジョニング （348 ページ） を参照してください。

b) これらのインターフェイス間に事前にプロビジョニングされたリンクを作成します。

[リンク（Links）] タブで、**[アクション（Actions）]** > **[作成（Create）]** をクリックします。

2 つのリンクを作成します。1 つは、leaf1-Ethernet1/44 から leaf2-Ethernet1/44 へ、もう 1 つは、leaf1-Ethernet1/45 から leaf2-Ethernet1/45 へのリンクです。

リンク テンプレートとして **int_pre_provision_intra_fabric_link** を選択していることを確認してください。送信元インターフェイスと宛先インターフェイスのフィールド名は、前の手順で事前にプロビジョニングされたイーサネット インターフェイスと一致している必要があります。

リンクが作成されると、それらは **[リンク（Links）]** タブ（**[ファブリックの概要（Fabric Overview）]** ウィンドウ）にリスト表示されます。

c) **[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。

vPC ペアを選択し、事前プロビジョニングされたデバイスの [vPC ペアリング（vPC pairing）] をクリックします。

d) **[再計算と展開（Recalculate & Deploy）]** をクリックして、事前にプロビジョニングされたデバイスに必要な目的の vPC ペアリング設定を生成します。

完了すると、デバイスは正しくペアリングされ、デバイスの vPC ペアリング インテントが生成され、ポリシーが生成されます。

（注） デバイスはまだ動作していないため、構成コンプライアンスはこれらのデバイスの同期（IN-SYNC）または非同期（OUT-OF-SYNC）ステータスを返しません。

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

vPC ホスト インターフェイスの事前プロビジョニング

手順

ステップ 1 事前プロビジョニングされたデバイスに物理イーサネット インターフェイスを作成します。通常の vPC ペアまたはスイッチと同様の vPC ホスト インターフェイスを追加します。詳細については、イーサネット インターフェイスの事前プロビジョニング （348 ページ） を参照してください。

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

ステップ 2 vPC ホスト トラック インターフェイスを作成します。

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

事前にプロビジョニングされたデバイスへのオーバーレイのアタッチ

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

オーバーレイ ネットワークは、事前にプロビジョニングされたリーフの vPC ペア（leaf1-leaf2）にアタッチされます。また、leaf1-leaf2 で作成され、事前にプロビジョニングされた vPC ホスト インターフェイス ポート チャネルにもアタッチされます。

デバイスに到達できないため、事前にプロビジョニングされたデバイスの**プレビュー**および**展開**操作は無効になっています。事前にプロビジョニングされたデバイスに到達できるようになると、他の検出されたデバイスと同様に、すべての操作が有効になります。

[ファブリックの概要（Fabric Overview）] ウィンドウで、**[ポリシー（Policies）]** タブをクリックし、**[アクション（Actions）]** > **[ポリシーの編集（Edit Policy）]** の順に選択します。オーバーレイ ネットワーク/VRF アタッチメント情報を含む、事前にプロビジョニングされたデバイス用に生成されたインテント全体を表示できます。

スイッチのプレビュー

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]** > **[スイッチ（Switches）]** 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）]** > **[スイッチ（Switches）]** を選択します。

スイッチを追加した後、保留中の設定、実行構成の並列比較、およびスイッチの予想される設定を含むスイッチをプレビューできます。複数のスイッチを選択して、同じインスタンスでプレビューできます。**[プレビュー（Preview）]** ウィンドウに、スイッチの正常な展開の保留中の構成が表示されます。

スイッチをプレビューし、保留中の構成と再同期するには、次の手順を実行します。

Procedure

ステップ 1 **[スイッチ（Switches）]** ウィンドウで、スイッチの横にあるチェックボックスを使用して、プレビューするスイッチを選択します。**[アクション（Actions）]** ドロップダウンリストから、**[プレビュー（Preview）]** を選択します。

[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、スイッチ名（そのIPアドレス、ロール、シリアル番号、ファブリックのステータス（同期中、同期外、または使用不可）。保留中の構成。ステータスの説明。進捗状況など）のスイッチ設定情報が表示されます。

ステップ 2 構成のみをプレビューするには、表示された情報を表示して、**[閉じる（Close）]**をクリックします。

ステップ 3 保留中の構成でスイッチを再同期するには、**[再同期（Resync）]**をクリックします。経過表示バーに再同期の進捗が表示されます。**[閉じる（Close）]** をクリックして、**[構成のプレビュー（Preview Config）]** ウィンドウを閉じます。

ステップ 4 保留中の構成と比較を表示するには、**[保留中の構成（Pending Config）]** 列のそれぞれのリンクをクリックします。

または、**[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）]** ウィンドウが表示されます。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。

[保留中の構成（Pending Config）] ウィンドウが表示されます。このウィンドウの**[保留中の構成（Pending Config）]** タブには、スイッチの保留中の構成が表示されます。**[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が並べて表示されます。

[保留中の構成（Pending Config）] ウィンドウを閉じます。

設定の導入

この展開オプションは、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。

1. 必要なスイッチを選択し、**[アクション（Actions）]** > **[展開（Deploy）]** を選択してスイッチに設定を展開します。

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

2. **[再同期（Resync）]** をクリックして設定を同期します。

3. [展開（Deploy）] をクリックします。

   [ステータス（Status）] カラムには、「FAILED」または「SUCCESS」の状態が表示されます。FAILED ステータスの場合は、問題の解決に失敗した理由を調査します。

4. **[閉じる（Close）]** をクリックして、ウィンドウを切り替えます。

ディスカバリ

この章は、次の項で構成されています。

クレデンシャル情報の更新

検出スイッチを更新するには、検出ログイン情報の更新を使用します。

手順

ステップ 1 必要なスイッチを選択し、**[アクション（Actions）]** > **[検出（Discovery）]** > **[ログイン情報の構成（Update Credentials）]** の順に選択します。

[Database Credentials（データベースのログイン情報）] ウィンドウが表示されます。

ステップ 2 [検出ログイン情報の更新（Update Discovery Credentials）]ウィンドウで、検出ユーザ名やパスワードなどの検出ログイン情報を入力します。

ステップ 3 **[更新（Update）]** をクリックして、検出ログイン情報を保存します。

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。

再検出

スイッチを再検出し、そのステータスを確認できます。

スイッチを再検出するには、次の手順を実行します。

- 必要なスイッチを選択し、**[アクション（Actions）]** > **[検出（Discovery）]** > **[再検出（Rediscover）]** を選択してスイッチを再検出します。

  [検出ステータス（Discovery Status）] 列にステータスが **[再検出中（Rediscovering）]** として表示され、検出後にステータスが表示されます。

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。

セット ロールの割り当て

Nexusダッシュボード ファブリック コントローラ でスイッチにロールを割り当てることができます。

1. 必要なスイッチを選択し、**[アクション（Actions）]** > **[セット ロール]** を選択します。
2. **[ロールの選択]** ウィンドウが表示されます。適切なロールを選択し、**[選択（Select）]** をクリックします。

   確認ウィンドウが表示されます。

（注） **[ロール ステータス（Role Status）]** 列に新しいロールの割り当てを表示するには、スイッチを再検出する必要があります。

Nexusダッシュボードファブリック コントローラ 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
- 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
- アクセス
- 集約
- エッジ ルータ
- コア ルータ
- TOR

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。

スイッチでのアクションの実行

モード変更

スイッチのモードを変更するには、次の手順を実行します。

1. 必要なスイッチのチェックボックスを選択し、**[アクション（Actions）]**>**[詳細（More）]**>**[モードの変更（Change Mode）]** を選択します。

   [モードの変更（Change Mode）] ウィンドウが表示されます。

2. ドロップダウン リストから **[通常（Normal）]** または **[メンテナンス（Maintenance）]** を選択します。

3. **[今すぐ保存して展開（Save and Deploy Now）]** をクリックしてモードを変更するか、**[後で保存して展開（Save and Deploy Later）]** をクリックしてモードを後で変更します。

RMA のプロビジョニング

スイッチのモードを変更するには、次の手順を実行します。

1. 必要なスイッチのチェックボックスを選択し、**[アクション（Actions）]**>**[詳細（More）]**>**[RMA のプロビジョニング（Provision RMA）]** を選択します。

   [RMA のプロビジョニング（Provision RMA）] ウィンドウが表示されます。

2. [RMA のプロビジョニング（Provision RMA）] UIには、電源がオンになってから 5ー10 分後に交換デバイスが表示されます。

実行開始のコピー（Copy Run Start）

既存のスイッチ構成をコピーして構成を開始するには、次の手順を実行します。

1. 必要なスイッチのチェックボックスを選択し、**[アクション（Actions）]**>**[詳細（More）]**>**[実行開始のコピー（Copy Run Start）]** を選択します。

[実行構成をスタートアップ構成にコピー（Copy Running Config to Startup Config）] 画面が表示されます。[進捗状況（Progress）]列には進行中のプロセスが表示され、ステータスの説明には **[進行中の展開]** と表示されます。

2. 確認ウィンドウが表示されます。[OK] をクリックします。

   ステータスの説明列には、**[展開完了（Deployment completed）]** と [進捗状況（progress）] 列が緑色で表示されます。

3. [閉じる（Close）] をクリックしてウィンドウを閉じます。

リロード

必要なスイッチをリロードするには、**[アクション（Actions）]** > **[詳細（More）]** > **[リロード（Reload）]** を選択します。

確認ウィンドウが表示されます。**[確認（Confirm）]** をクリックします。

復元スイッチ

Cisco Nexusダッシュボード ファブリック コントローラ Web UIから外部ファブリックおよびLANクラシック ファブリックの Cisco Nexus スイッチを復元できます。スイッチ レベルで復元する情報は、ファブリック レベルのバックアップから抽出されます。スイッチ レベルの復元では、ファブリック レベルのインテントおよびファブリック設定を使用して適用されたその他の設定は復元されません。スイッチ レベルのインテントのみが復元されます。したがって、スイッチを復元すると、ファブリック レベルのインテントが復元されないため、同期がとれなくなる可能性があります。ファブリック レベルの復元を実行して、インテントも復元します。復元は一度に 1 つしか実行できません。スイッチが検出されたファブリックが MSD ファブリックの一部である場合、スイッチを復元することはできません。

1. **[アクション（Actions）]** > **[詳細（More）]** > **[リロード（Reload）]**を選択します。

   [スイッチの復元（Restore Switch）] ウィンドウが表示され、**[バックアップの選択（Select a Backup）]**タブが表示されます。詳細については、「バックアップ ファブリック」を参照してください。

2. [バックアップの選択（Select a Backup）]タブには、ファブリックバックアップの詳細が表示されます。収集する情報は次のとおりです。

   - バックアップ日（Backup Date）：バックアップの日時を指定します。
   - バックアップ バージョン（Backup Version）：バックアップのバージョン番号を指定します。
   - バックアップ タグ：バックアップの名前を指定します。
   - NDFC バージョン（NDFC Version）：NDFC バージョンの詳細を指定します。
   - バックアップ タイプ：バックアップのタイプ（手動または自動）を指定します。

     自動、手動、またはゴールデンバックアップを選択できます。これらのバックアップは色分けされています。自動バックアップは青色で示されます。手動バックアップは

濃い青色で示されます。ゴールデン バックアップはオレンジ色で示されます。自動バックアップの名前にはバージョンのみが含まれます。一方、手動バックアップには、手動バックアップを開始したときに指定したタグ名と、バックアップ名のバージョンがあります。バックアップにカーソルを合わせると、名前が表示されます。

3. 必要なバックアップのラジオ ボタンを選択してゴールデンとしてマークし、**[アクション（Actions）] > [ゴールデンとしてマーク（Mark as golden）]** の順に選択し、確認ウィンドウが表示さえ r たら、**[確認（Confirm）]** をクリックします。
4. ゴールデンから削除するバックアップのオプションボタンを選択し、**[アクション（Actions）]** の **[ゴールデンとして削除（Remove）]** 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。

   ゴールデンバックアップの詳細については、ゴールデン バックアップ を参照してください。

（注） この情報の大部分はファブリックレベルであり、スイッチレベルの復元の手順に直接影響する場合と影響しない場合があります。

5. **[次へ（Next）]** をクリックして、**[プレビューの復元（Restore Preview）]** の手順に進みます。
6. スイッチ名、スイッチシリアル、IPアドレス、ステータス、サポートされている復元、デルタ構成、および VRF の詳細に関する情報を表示できます。
7. （オプション）**[構成の取得（Get Config）]** をクリックして、デバイス構成の詳細をプレビューします。

   [構成のプレビュー（Config Preview）] ウィンドウが表示されます。このウィンドウには 3 つのタブがあります。

   - **バックアップ構成（Backup Config）**：このタブには、選択したデバイスのバックアップ設定が表示されます。
   - **現在の構成（Current Config）**：このタブには、選択したデバイスの現在の実行構成が表示されます。
   - **並列比較**：このタブには、スイッチの現在の実行構成と、予想される構成が表示されます。

8. **[インテントの復元（Restore Intent）]** をクリックして、復元の**ステータスの復元**手順に進みます。

   スイッチの復元ステータスと説明が表示されます。
9. 復元プロセスが完了したら、**[完了（Finish）]** をクリックします。

（注）
- ファブリック設定が変更されているため、前の手順に戻ることはできません。
- 復元に失敗した場合、スイッチは以前の設定にロールバックします。

コマンドの表示

次の手順では、Nexusダッシュボード ファブリック コントローラ のコマンドを表示します。

1. **[アクション（Actions）]** > **[詳細（More）]** > **[show コマンド（Show Command）]** を選択します。

   [Switch Show Commands] ウィンドウが表示されます。

2. ドロップダウン リストから必要なコマンドを選択し、テキスト フィールドに必要な情報を入力します。
3. CLI の出力を表示するには **[実行（Execute）]** をクリックし、出力をクリアするには **[出力のクリア（Clear Output）]** をクリックします。

Exec Commands

EXEC モードで使用可能なコマンドには、デバイスの状態および構成情報を表示する show コマンド、clear コマンド、ユーザがデバイス コンフィギュレーションに保存しない処理を実行するその他のコマンドがあります。

次の手順は、Nexusダッシュボード ファブリック コントローラ でEXECコマンドを実行する方法を示しています。

1. **[アクション（Actions）]** > **[詳細（More）]** > **[Exec コマンド（Exec Command）]** を選択します。

   [Switch Show Commands] ウィンドウが表示されます。

2. **[テンプレート（Template）]** ドロップダウンリストから、**[exec_freeform]** または **[exec_elam_capture]** を選択します。
3. **Freeform CLI** で **exec_freeform** および必要な IP アドレスのコマンドを入力します。
4. **[展開（Deploy）]** をクリックして、EXEC コマンドを実行します。
5. **[CLI 実行ステータス（CLI Execution Status）]** ウィンドウで、展開のステータスを確認できます。**[コマンド（Command）]** 列の **[詳細なステータス（Detailed Status）]**をクリックして詳細を表示します。
6. **[コマンド実行の詳細（Command Execution Details）]** ウィンドウで、**[CLI 応答（CLI Response）]** 列の情報をクリックして、出力または応答を表示します。

スイッチの削除

1 つ以上の既存のスイッチを削除できます。

[アクション（Actions）]>**[詳細（More）]**>**[削除（Delete）]**スイッチを選択します。確認ウィンドウが表示されます。**[確認（Confirm）]** をクリックします。

スイッチの概要

[スイッチの概要（Switch Overview）] ウィンドウの **[アクション（Actions）]** アイコンから、次の操作を実行できます。

- スイッチのプレビュー
- 設定の導入
- ディスカバリ
- セット ロールの割り当て
- vPC セットアップの作成
- スイッチでのアクションの実行

スイッチの概要の表示

[スイッチの概要（Switch Overview）] タブでは、スイッチの概要とともにスイッチに関する情報を表示できます。**[LAN]**>**[スイッチ（Switches）]**を移動し、必要なスイッチをクリックします。スライドイン ペインが表示されます。**[起動（Launch）]** アイコンをクリックして、**[スイッチの概要（Switch Overview）]** ウィンドウを表示します。

フィールド	説明
スイッチ情報	スイッチ名、IP アドレス、スイッチ モデルなどのスイッチ情報を指定します。
アラーム	選択したスイッチに設定されているアラームを指定します。
パフォーマンス	スイッチの CPU 使用率とメモリ使用率を指定します。
インターフェイス	インターフェイスの詳細を指定します。
モジュール/FEX	モジュールおよび FEX 情報を指定します。
レポート	レポートを指定します。

ハードウェア

このタブには、次の項を含みます。

モジュール

Cisco Nexus Dashboard ファブリック コントローラWeb UI からモジュールのインベントリ情報を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[LAN] > [スイッチ（Switch）] > [スイッチの概要（Switch Overview）] > [ハードウェア（Hardware）] > [モジュール（Modules）]** の順に表示できます。

[モジュール（Modules）] タブに、選択した範囲のすべてのスイッチとその詳細のリストが表示されます。

テーブルに必要な情報を表示し、**[属性によるフィルタ（Filter by Attributes）]** に詳細を入力できます。

ステップ 2 次の情報が表示されます。

- **[名前（Name）]** にはモジュール名が表示されます。
- **[モデル（Model）]** にモデル名が表示されます。
- **[シリアル番号（Serial Number）]** 列には、シリアル番号が表示されます。
- **[タイプ（Type）]** 列には、モジュールのタイプが表示されます。
- **Oper. Status** 列には、デバイスの動作状態が表示されます。
- **[スロット（Slot）]** 列には、スロット番号が表示されます。
- **[ハードウェア リビジョン（HW Revision）]** 列には、モジュールのハードウェア バージョンが表示されます。
- **[ソフトウェア リビジョン（Software Revision）]** 列には、モジュールのソフトウェア バージョンが表示されます。
- **[アセット ID（Asset ID）]** カラムには、モジュールのアセット ID が表示されます。

ブートフラッシュの表示

[ブートフラッシュ（Bootflash）] タブで次の情報を表示できます。

- **[プライマリ ブートフラッシュ サマリ（Primary Bootflash Summary）]** カードには、合計、使用済み、および使用可能な領域が表示されます。

- **[セカンダリ ブートフラッシュ サマリ（Secondary Bootflash Summary）]** カードには、合計、使用済み、および使用可能な領域が表示されます。
- **[ディレクトリ リスト（Directory List）]** 領域に、**プライマリ ブートフラッシュ**と**セカンダリ ブートフラッシュ**のチェックボックスが表示されます。

  この領域には、スイッチのブートフラッシュ上のすべてのファイルとディレクトリのファイル名、サイズ、および最終変更日が表示されます。**[アクション（Actions）] > [削除（Delete）]**を順に選択してファイルを削除し、スイッチで使用可能なスペースを増やします。

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。

フィールド	説明
[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 207 • ファブリック間リンクの作成, on page 205
編集	選択したファブリックを編集できます。
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。

PTP（モニタリング）

Note PTPモニタリングはアプリケーションとしてインストールでき、このアプリケーションはIPFM モードでのみ動作します。

UI ナビゲーション

- **[LAN]** > **[スイッチ（Switches）]** を選択します。スイッチをクリックして **[スイッチ（Switch）]** 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。**[スイッチの概要（Switch Overview）]** > **[PTP]** 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]** > **[スイッチ]** を開きます。スイッチをダブルクリックして、[Switch Overview] PTPを開きます。 >
- **[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 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）]** > **[スイッチ（Switches）]** を選択します。スイッチをクリックして**[スイッチ（Switch）]**スライドインペインを開き、**[起動（Launch）]**アイコンをクリックします。または、スイッチをダブルクリックして **[スイッチの概要（Switch Overview）]** を開くこともできます。**[スイッチの概要（Switch Overview）]** > **[PTP]** を選択します。

ここでは、Precision Time Protocol（PTP）モニタリングのプレビュー機能について説明します。PTP はネットワークに分散したノード間で時刻同期を行うプロトコルです。ローカル エリア ネットワークでは、サブナノ秒範囲のクロック精度を実現するため、測定および制御システムに適しています。

[スイッチの概要（Switch Overview）] ウィンドウの **[PTP]** タブでは、選択したスイッチに基づく PTP 関連情報を表示できます。**[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。**[同期ステータス（Sync Status）]** 列には、デバイスのステータスが表示されます。

このウィンドウには、次のタブが表示されます。

- **修正および平均パス遅延（Correction & Mean Path Delay）**
- **クロック ステータス（Clock Status）**

修正と平均パス遅延

[修正および平均パス遅延（Correction＆Mean Path Delay）] タブには、PTP の動作統計情報（平均パス遅延、修正、しきい値超過修正）を示すグラフが表示されます。プロットエリアをクリックしてドラッグし、ズームインし、**Shift** キーを押したままパンします。ズームをリセットするには、**[ズームのリセット]** ボタンをクリックします。

デフォルトでは、グラフは500ナノ秒（ns）のしきい値で表示されます。特定のしきい値に基づいてデータを表示することもできます。**[しきい値（Threshold）（ns）]**フィールドに、必要な値をナノ秒単位で入力し、**[適用（Apply）]**をクリックします。しきい値はNexusダッシュボード ファブリック コントローラ 設定で永続的であり、PTP 修正しきい値の Kafka 通知を生成するために使用されることに注意してください。

[日付（Date）]フィールドで、データを表示する適切な日付を選択できます。PTPデータは、過去7日間保存されます。保存データのデフォルト値は7日間です。この値を変更するには、**[設定（Settings）]> [サーバ設定（Server Settings）]> [IPFM（IPFM）]**に移動し、**[IPFM 履歴保持日数]**フィールドの更新値を設定します。

[期間（Period）]フィールドでは、データを表示する期間を選択することもできます。**[期間（Period）]**フィールドで選択できる値は、時間（1時間）、6時間、12時間、または日（24時間）です。

グラフの凡例をクリックすると、統計情報の表示/非表示を切り替えることができます。

修正がある場合は、**[しきい値を超えて修正（Corrections Beyond Threshold）]**リンクをクリックして、表形式で修正を表示できます。

手動で更新するには、**更新** アイコン をクリックします。

[クロックとポートの（Clock & Port Status）]

[クロックとポートのステータス（Clock & Port Status）]タブには、親クロック、グランドマスター クロック、およびポート ステータスのステータスが表示されます。

[ポート ステータス（Port Status）]テーブルには、ポートのステータスが表示されます。**[属性によるフィルタ（Filter by attributes）]**フィールドをクリックし、必要な属性を選択して、ポート ステータスをフィルタリングする条件を入力し、Enter キーを押します。

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 （379 ページ）
- インターフェイスグループ （393 ページ）

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。
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。

アクション項目	説明
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。

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。

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。

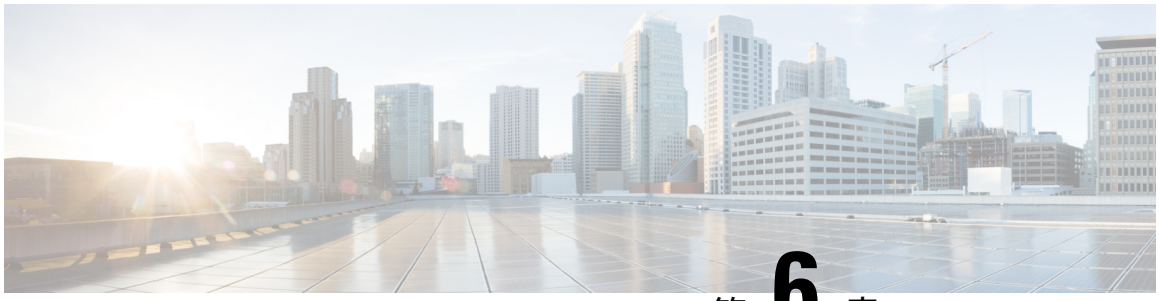
フィールド	説明
範囲	リソース使用範囲を指定します。有効な値は、スイッチのシリアル番号またはファブリック名です。シリアル番号を持つリソースは一意であり、スイッチのシリアル番号でのみ使用できます。
デバイス名（Device Name）	デバイス名を指定します。
デバイス IP	デバイスの IP アドレスを指定します。
リソースの割り当て	リソースをデバイス、デバイス インターフェイス、またはファブリックで管理するかどうかを指定します。有効な値は、ID タイプ、サブネット、または IP アドレスです。
割り当て先	リソースが割り当てられるエンティティ名を指定します。
[リソース タイプ（Resource 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。

L4～L7 サービスの構成

Cisco Nexus Dashboard ファブリック コントローラでは、レイヤ 4～レイヤ 7（L4～L7）サービス デバイスをデータ センター ファブリックに挿入する機能が導入されました。これらの L4～L7 サービス デバイスにトラフィックを選択的にリダイレクトすることもできます。L4～L7 サービス ノードを追加し、L4～L7 サービス ノードと L4～L7 サービス リーフ スイッチの間にルート ピアリングを作成してから、これらの L4～L7 サービス ノードにトラフィックを選択的にリダイレクトできます。

（注） これは、Nexus Dashboard Fabric Controller、Release 12.0.1a のフィーチャのプレビューです。ラボセットアップでのみ、ベータ版としてマークされたこの機能を使用することをお勧めします。実稼働環境でこれらのフィーチャを使用しないでください。

NDFC リリース 12.0.2a 以降、この機能を本番環境で使用できます。



第 6 章

ポリシー

ポリシーの表示と編集

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。
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。

フィールド	説明
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。

アクション項目	説明
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。
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。

ポリシーの追加

ポリシーを追加するには、次の手順を実行します。

手順

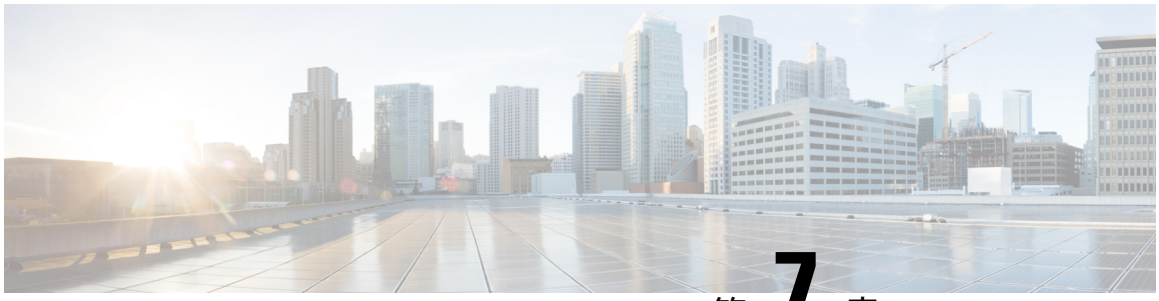
ステップ 1 **[アクション（Actions）] > [ポリシーの追加（Add Policy）]** の順に選択します。

[ポリシーの作成（Create Policy）] ウィンドウを表示します。

ステップ 2 必要なスイッチをクリックして選択し、**[選択（Select）]** をクリックします。

ステップ 3 **[テンプレートの選択（Choose Template）]** をクリックし、適切なポリシーテンプレートを選択して、**[選択（Select）]** をクリックします。

ステップ 4 テキスト フィールドに必須パラメータを入力し、**[保存（Save）]** をクリックします。



第 7 章

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 （379 ページ）
- インターフェイスグループ （393 ページ）

インターフェイス

[インターフェイス（Interfaces）] オプションは、スイッチで検出されたすべてのインターフェイス、仮想ポートチャネル（vPC）、およびデバイスに存在しない目的のインターフェイスを表示します。

無効なインターフェイスのエラーは、次のシナリオで発生します。

- インターフェイス モードの「ルーティング」は無効です。許可されるモードはトランク & アクセスです。
- すでに他のネットワークに割り当てられているアクセスポート。
- スイッチでは使用できないインターフェイス。

次の機能を使用できます。

- ポート チャネル、vPC、 Straight-through FEX、Active-Active FEX、ループバック、およびサブインターフェイスを作成、展開、表示、編集、および削除します。

（注）

- 次の機能は、Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x)イメージを使用したスイッチのブラウンフィールド移行ではサポートされていません。
  - X9500 ラインカードを搭載した Cisco Nexus 9300 シリーズ スイッチおよびCisco Nexus 9500 シリーズ スイッチ以外のスイッチでの FEX
  - AA-FEX

  FEX のプラットフォーム サポートについては、プラットフォームと NX-OS のマニュアルを参照して、機能の互換性を確認してください。
- ファブリック内リンクやファブリック間リンクなどのファブリック リンクに関連付けられているインターフェイスを編集するには、リンクに関連付けられたインターフェイスの編集 （389 ページ） を参照してください。
- **flowcontrol** または **priority-flow-control** の設定は、HIF ポートまたはメンバーとしての HIF ポートではサポートされません。

- Cisco Cloud Services Router 1000v シリーズ（Cisco CSR 1000v シリーズ）のトンネル インターフェイスを作成します。
- ブレイクアウト ポートとアンブレイクアウト ポートを作成します。
- インターフェイスをシャットダウンして起動します。
- ポートを再検出し、インターフェイスの設定履歴を表示します。
- インターフェイスおよびvPCにホストポリシーを適用します。たとえば、int_trunk_host、int_access_host などです。
- インターフェイスの情報（管理ステータス、動作ステータス、理由、ポリシー、速度、MTU、モード、VLAN、IP/プレフィックス、VRF、ポートチャネル、インターフェイスのネイバーなど）を表示します。

（注）

- **[ネイバー（Neighbor）]** 列には、検出された接続スイッチ、インテント リンク、および Virtual Machine Manager（VMM）接続の詳細が表示されます。

[ステータス（Status）] 列に、次のいずれかのステータスが表示されます。

- 青：保留中

- 緑：同期/成功
- 赤：非同期/失敗
- 黄色：進行中
- グレー：不明/ NA

- インターフェイスがアウトオブバンドで作成された場合、このインターフェイスを削除するには、ファブリックの再同期を実行するか、構成コンプライアンスのポーリングを待機する必要があります。そうしないと、Config Compliance は正しい差分を生成しません。

ただし、ASR 9000 シリーズ ルータおよび Arista スイッチのインターフェイスを追加または編集することはできません。

特定のフィールド（[デバイス名（Device Name）]など）の情報をフィルタリングおよび表示できます。次の表で、このページに表示されるボタンを説明します。

（注）

- 適切な vPC ペア構成を含む、インターフェイス オプションから展開する前に、適切な構成がファブリックに展開されていることを確認します。構成をファブリックに展開する前にインターフェイスを追加または編集すると、デバイスで構成が失敗することがあります。
- インターフェイス マネージャから構成を展開する前に、vPCペアリングを含むアンダーレイをファブリックに展開します。

フィールド	説明
インターフェイスの作成	ポート チャネル、vPC、Straight-through FEX、Active-Active FEX、ループバックなどの論理インターフェイスを追加できます。 詳細については、インターフェイスの追加 （385 ページ）を参照してください。
サブインターフェイスの作成	論理サブインターフェイスを追加できます。
インターフェイスの編集	インターフェイスに関連付けられているポリシーを編集および変更できます。 （注） Access-admin ユーザー ロールは、Easy ファブリックのファブリック間リンクやファブリック内リンクなどのリンク ポリシーに関連付けられたインターフェイスを編集できません。このユーザー ロールは、LAN クラシックおよび IPFM ファブリックのインターフェイスを編集できます。

フィールド	説明
インターフェイスのプレビュー	インターフェイス構成をプレビューできます。
インターフェイスの展開	保存したインターフェイス設定を展開または再展開できます。
シャットダウンなし	インターフェイスを有効にできます（シャットダウンまたは管理起動なし）。
シャットダウン	インターフェイスをシャットダウンできます。
インターフェイス グループの追加	インターフェイス グループにインターフェイスを追加できます。
インターフェイス グループからの削除	インターフェイス グループからインターフェイスを削除できます。
サブ会議	インターフェイスをブレークアウトできます。
ブレークアウト解除	ブレイクアウト状態のインターフェイスをブレイクアウト解除できます。
インターフェイスの再検出	選択したインターフェイスのコンプライアンス ステータスを再検出または再計算できます。
Show コマンド	interface show コマンドを表示できます。show コマンドを使用するには、テンプレートライブラリにshowテンプレートが必要です。
展開履歴	インターフェイス展開履歴の詳細を表示できます。
インターフェイスの削除	[インターフェイス（Interfaces）] 画面から作成された論理インターフェイスを削除できます。オーバーレイとアンダーレイからアタッチされたポリシーを持つインターフェイスは削除できません。

次の表に、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 11.5(1) からの **[インターフェイス（Interfaces）]** ウィンドウのホスト側ポートでの新しいユーザ ロールaccess-admin操作のサポートを示します。

操作	ユーザ ロール
	Role: access-admin
新しいインターフェイスの作成	保存、プレビュー、展開
サブ会議	ブロック済み
ブレークアウト解除	ブロック

操作	ユーザ ロール
	Role: access-admin
インターフェイスの編集	保存、展開
インターフェイスの削除	保存、展開
シャットダウン	保存、展開
シャットダウンなし	保存、展開
Show コマンド	出力のクリア、実行
インターフェイスの再検出	サポート対象
インターフェイスの展開	キャンセル、構成の展開

Nexusダッシュボード ファブリック コントローラ で展開を無効にしたり、ネットワーク管理者としてファブリックをフリーズしたりできます。ただし、ファブリックをフリーズする場合、またはファブリックがモニタ モードの場合、すべてのアクションを実行することはできません。

次の表に、ファブリックをフリーズするとき、およびファブリックのモニタ モードを有効にするときに実行できるアクションを示します。

操作	**Nexusダッシュボード ファブリック コントローラ[モード（Mode）]**	
	フリーズ モード	**モニタ モード**
追加	保存、プレビュー	ブロック
サブ会議	ブロック済み	ブロック済み
ブレークアウト解除	ブロック済み	ブロック済み
編集	保存、プレビュー	ブロック
削除	保存、プレビュー	ブロック
シャットダウン	保存、プレビュー	ブロック
シャットダウンなし	保存、プレビュー	ブロック
表示	サポート対象	サポート対象
再検出	サポート対象	サポート対象
展開	ブロック済み	ブロック済み

関連付けられた操作のボタンは、それに応じてグレー表示されます。

構成プロファイルの一部である SVI で管理操作（shutdown/no shutdown）を実行すると、連続した**保存して展開**操作で **no interface vlan** コマンドが生成されます。

ポリシーのない SVI の場合、管理操作の実行時、つまり **Interface Manager** から shutdown /no shutdown コマンドがプッシュされると、**int_vlan_admin_state** ポリシーが SVI に関連付けられます。

たとえば、**switch_freeform** から SVI を作成して展開します。

```
interface vlan1234
  description test
  no shutdown
  no ip redirects
  no ipv6 redirects
```

インターフェイス マネージャから SVI をシャットダウンすると、**int_vlan_admin_state** ポリシーが SVI に関連付けられます。

保留中の差分は次のように表示されます。

```
interface Vlan1234
  shutdown
  no ip redirects
  no ipv6 redirects
  description test
  no shutdown
```

自由形式の設定から **no shutdown CLI** を削除します。

ユーザが SVI で管理操作を実行した場合、デバイスには実行構成のインターフェイスがあります。したがって、ネットワーク切断後の **interface vlan** は引き続き存在し、インターフェイスが検出されます。**Interface Manager** からインターフェイスを手動で削除する必要があります。

次の表に、**[LAN] > [Interfaces] > [Interfaces]**に表示されるフィールドを示します。

フィールド	説明
Fabric Name（ファブリック名）	ファブリック名を指定します。
デバイス名（Device Name）	デバイス名を指定します。
インターフェイス	インターフェイス名を指定します。
Admin Status	インターフェイスの管理ステータスを指定します。ステータスは [Up] または [Down] です。
oper-status	インターフェイスの操作ステータス。ステータスは [Up] または [Down] です。
理由	理由を指定します。
ポリシー	ポリシー名を指定します。
オーバーレイ ネットワーク	オーバーレイ ネットワークを指定します。
同期ステータス	同期ステータスを指定します。インターフェイスのステータスが同期中か同期外かを指定します。

フィールド	説明
インターフェイス グループ	インターフェイスが属するインターフェイス グループを指定します。
ポートチャネルID	ポート チャネル ID を指定します。
vPC ID	vPC ID を指定します。
スピード	インターフェイスの速度を指定します。
[最大伝送ユニット（MTU）]	MTU のサイズを指定します。
モード（Mode）	インターフェイス モードを指定します。
VLAN	VLAN を設定します。
IP/プレフィックス	インターフェイスの IP/プレフィックスを指定します。
VRF	仮想ルーティングおよび転送（VRF）インスタンス
ネイバー	インターフェイス ネイバーを指定します。
説明	インターフェイスの説明を指定します。 （注） インターフェイスの説明が 64 文字を超える場合は、**snmp ifmib ifalias long**コマンドを使用してスイッチを構成する必要があります。

インターフェイスの追加

Cisco Nexusダッシュボード ファブリック コントローラ Web UIからインターフェイスを追加するには、次の手順を実行します。

手順

ステップ 1 **[LAN] > [インターフェイス（Interfaces）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 論理インターフェイスを追加するには、**[アクション（Actions）] > [新しいインターフェイスの作成（Create new interface）]** をクリックします。

[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 **[Type]** ドロップダウン リストから、インターフェイス タイプを選択します。

有効な値は、ポートチャネル、仮想ポートチャネル（vPC）、ストレート（ST）FEX、アクティブ-アクティブ（AA）FEX、ループバック、サブインターフェイス、トンネルイーサネッ

ト、およびスイッチ仮想インターフェイス（SVI）です。インターフェイス タイプを選択すると、それぞれのインターフェイス ID フィールドが表示されます。

- Nexusダッシュボード ファブリック コントローラ を通じてポート チャネルを作成する場合は、同じ速度のインターフェイスを追加します。さまざまな速度のインターフェイスから作成されたポート チャネルは起動しません。たとえば、2つの*10*ギガビット イーサネット ポートを持つポート チャネルが有効です。ただし、*10* ギガビット イーサネット *+ 25* ギガビット イーサネット ポートの組み合わせを持つポート チャネルは無効です。
- vPC ホストを追加するには、ファブリック トポロジで vPC スイッチを指定し、**[展開の保存（Save Deploy）]**オプションを使用して vPC およびピアリンク構成を展開する必要があります。vPC ペアの設定が展開されると、[vPC ペアの選択（Select a vPC pair）] ドロップダウン ボックスに表示されます。

  int_vpc_trunk_host ポリシーを使用して vPC を作成できます。
- サブインターフェイスを追加する場合は、[追加（Add）] ボタンをクリックする前に、インターフェイス テーブルからルーテッド インターフェイスを選択する必要があります。
- [インターフェイス（Interface）] ウィンドウでイーサネット インターフェイスを事前プロビジョニングできます。この事前プロビジョニング機能は、Easy、eBGP、および外部ファブリックでサポートされています。.

ステップ 4 **[デバイス タイプの選択（Select device type）]** フィールドで、デバイスを選択します。

デバイスは、ファブリックおよびインターフェイスタイプに基づいてリストされます。外部ファブリック デバイスは、ST FEX および AA FEX には表示されません。vPC またはアクティブからアクティブ FEX の場合は、vPC スイッチペアを選択します。

ステップ 5 選択したインターフェイスに基づいて、表示される各インターフェイスIDフィールド（**ポート チャネル ID**、**vPC ID**、**ループバック ID**、**トンネル ID**、**インターフェイス名**、**VLAN ID**、および**サブインターフェイス ID**）に ID 値を入力します。

この値は上書きできます。新しい値は、リソース マネージャ プールで使用可能な場合にのみ使用されます。それ以外の場合は、エラーになります。

ステップ 6 **[ポリシー（Policy）]** フィールドで、インターフェイスに適用するポリシーを選択します。

このフィールドには、インターフェイスのタイプに基づいてフィルタリングされた、*interface interface_edit_policy* のインターフェイス Python ポリシーのみが表示されます。

_upg インターフェイス ポリシーを作成しないでください。たとえば、**vpc_trunk_host_upg**、**port_channel_aa_fex_upg**、**port_channel_trunk_host_upg**、および **trunk_host_upg** オプションを使用してポリシーを作成することはできません。

（注） ポリシーは、**[タイプ（Type）]** ドロップダウン リストで選択したインターフェイス タイプと、**[デバイスの選択（Select a device）]** ドロップダウン リストで選択したデバイスに基づいてフィルタリングされます。

ステップ 7 **[ポリシー オプション（Policy Options）]** の必須フィールドに値を入力します。

フィールドは、選択したインターフェイス タイプによって異なります。

（注） Cisco Nexusダッシュボード ファブリック コントローラ Release 11.5(1) 以降では、vPC の作成時に Peer-1 の設定を Peer-2 にミラーリングできます。**[構成ミラーリングの有効化（Enable Config Mirroring）]** チェックボックスをオンにすると、[Peer-2] フィールドがグレー表示されます。[Peer-1] フィールドに入力した設定は、[Peer-2] フィールドにコピーされます。

ステップ 8 [保存（Save）] をクリックして、設定を保存します。

（注） インターフェイスに QoS ポリシーを適用するには、参照を使用してインターフェイスの自由形式を作成します。

保存された設定のみがデバイスにプッシュされます。インターフェイスの追加中は、最初の保存後にのみポリシー属性を変更できます。すでに使用されている ID を使用しようとすると、リソースが割り当てられないというエラーが発生します。

ステップ 9 （任意）**[プレビュー（Preview）]** オプションをクリックして、展開する構成をプレビューします。

ステップ 10 **[展開（Deploy）]** をクリックして、指定した論理インターフェイスを展開します。

新しく追加したインターフェイスが画面に表示されます。

ブレイクアウトと**ブレイクアウト解除**：**ブレイクアウト**と**ブレイクアウト解除**オプションを使用して、インターフェイスをブレイクアウトおよびブレイクアウト解除できます。

サブ会議

[ブレークアウト（Breakout）] アイコンの横にあるドロップダウン矢印をクリックして、使用可能なブレイクアウト オプションのリストを表示します。使用可能なオプションは、**10g-4x**、**25g-4x**、**50g-2x**、**50g-4x**、**100g-2x**、**100g-4x**、**200g-2x**、および **Unbreakout** です。必要なオプションを選択します。

インターフェイスの編集

Cisco Nexusダッシュボード ファブリック コントローラ Web UIからインターフェイスを編集するには、次の手順を実行します。

（注） **[インターフェイスの編集（Edit interface）]**では、ポリシーを変更したり、ポート チャネルまたは vPC からインターフェイスを追加または削除したりできます。

手順

ステップ 1 **[LAN] > [インターフェイス（Interfaces）] > [インターフェイス（Interfaces）]**の順に選択します。

[アクション（Actions）] メニューの [ブレイクアウト（breakout）] オプションを使用して、インターフェイスをブレークアウトおよびブレークアウト解除できます。

ステップ 2 インターフェイスまたは vPC を編集するには、インターフェイス チェックボックスをオンにします。

複数のインターフェイスを編集するには、対応するチェックボックスをオンにします。複数のポート チャネルおよび vPC を編集することはできません。異なるタイプのインターフェイスを同時に編集することはできません。

ステップ 3 インターフェイスを編集するには、**[アクション（Actions）]>[インターフェイスの編集（Edit interface）]** をクリックします。

[インターフェイスの編集（Edit interface）] ウィンドウに表示される変数は、テンプレートとそのポリシーに基づいています。適切なポリシーを選択します。ポリシーを保存し、同じものを展開します。このウィンドウには、インターフェイスの種類に基づいてフィルタリングされた、*interface_edit_policy* タグが付いたインターフェイス Python ポリシーのみが表示されます。

vPC のセットアップでは、2 つのスイッチは、編集ウィンドウに表示されるスイッチ名の順序になります。たとえば、スイッチ名が *LEAF1:LEAF2* と表示されている場合、Leaf1 はピア スイッチ 1、Leaf2 はピア スイッチ 2です。

スイッチへのオーバーレイ ネットワークの展開中に、ネットワークをトランク インターフェイスに関連付けることができます。トランク インターフェイスとネットワークの関連付けは、**[インターフェイス（Interfaces）]** タブに反映されます。このようなインターフェイスを更新できます。

[LAN] > [インターフェイス（Interfaces）] > [インターフェイス（Interfaces）] 画面から作成されていないインターフェイス ポリシーの場合、一部の設定を編集できますが、ポリシー自体は変更できません。編集できないポリシーとフィールドはグレー表示されます。

次に、編集できないポリシーの例を示します。

- ループバック インターフェイス ポリシー：int_fabric_loopback ポリシーは、ループバック インターフェイスを作成するために使用されます。ループバック IP アドレスと説明は編集できますが、int_fabric_loopback ポリシー インスタンスは編集できません。
- ファブリック アンダーレイ ネットワーク インターフェイス ポリシー（int_fabric_numなど）およびファブリック オーバーレイ ネットワーク インターフェイス（NVE）ポリシー。
- vPC に関連付けられたポート チャネルおよびメンバーポートを含む、ポート チャネルおよびポート チャネルのメンバー ポートに関連付けられたポリシー。

- ネットワークおよび VRF の作成時に作成された SVI。関連付けられた VLAN がインターフェイス リストに表示されます。

リンクに関連付けられたインターフェイスの編集

リンクには、ファブリック内リンクとファブリック間リンクの2種類があります。名前が示すように、ファブリック内リンクは同じ Easy ファブリック内のデバイス間に設定され、通常はスパイン リーフ接続に使用されます。ファブリック間リンクは、Easy ファブリックと、通常は他の外部または Easy ファブリック間に設定されます。外部 WAN や DC I接続に使用されます。ポリシーは、リンクの両端に適用される設定を効果的に示す各リンクに関連付けられます。つまり、リンク ポリシーは、リンクを形成する2つのインターフェイスに関連付けられた個々の子インターフェイス ポリシーの親になります。このシナリオでは、リンク ポリシーを編集して、説明、IPアドレス、インターフェイスごとの自由形式の設定などのインターフェイス ポリシー フィールドを編集する必要があります。次の手順は、リンクに関連付けられたインターフェイスを編集する方法を示しています。

手順

ステップ 1 **[LAN] > [インターフェイス（Interfaces）] > [インターフェイス（Interfaces）]**の順に選択します。

ステップ 2 リンクを選択し、**[アクション（Actions）] > [詳細（More）] > [インターフェイスの再検出（Rediscover Interface）]** の順にクリックします。

インターフェイスの削除

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からインターフェイスを削除するには、次の手順を実行します。

（注） このオプションを使用すると、論理ポート、ポート チャネル、および vPC のみを削除できます。オーバーレイまたはアンダーレイ ポリシーがアタッチされていない場合は、インターフェイスを削除できます。

ポート チャネルまたは vPC が削除されると、対応するメンバー ポートにデフォルトのポリシーが関連付けられます。デフォルト ポリシーは、`server.properties` ファイルで設定できます。

手順

ステップ 1 **[LAN] > [インターフェイス（Interfaces）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 インターフェイスを選択します。

ステップ 3 **[アクション（Actions）] > [詳細（More）] > [インターフェイスの削除（Delete Interface）]** の順にクリックします。

ファブリック アンダーレイで作成された論理インターフェイスは削除できません。

ステップ 4 **[Save（保存）]** をクリックします。

ステップ 5 **[展開（Deploy）]** をクリックして、インターフェイスを削除します。

インターフェイスのシャットダウンと起動

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からインターフェイスをシャットダウンして起動するには、次の手順を実行します。

手順

ステップ 1 **[LAN] > [インターフェイス（Interfaces）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 シャットダウンまたは起動するインターフェイスを選択します。

ステップ 3 **[シャットダウン（Shutdown）]**をクリックして、選択したインターフェイスを無効にします。たとえば、ネットワークからホストを分離したり、ネットワーク内でアクティブでないホストを分離したりできます。

変更を保存、プレビュー、および展開できる確認ウィンドウが表示されます。**[保存（Save）]** をクリックして、変更の展開をプレビューします。

ステップ 4 **[シャットダウンなし（No Shutdown）]** をクリックして、選択したインターフェイスを起動します。

変更を保存、プレビュー、および展開できる確認ウィンドウが表示されます。**[保存（Save）]** をクリックして、変更をプレビューまたは展開します。

インターフェイス構成の表示

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からインターフェイス構成コマンドを表示して実行するには、次の手順を実行します。

手順

ステップ 1 **[LAN] > [インターフェイス（Interfaces）] > [インターフェイス（Interfaces）]** の順に選択します。

設定を表示するインターフェイスを選択し、**[アクション（Actions）] > [詳細（More）] > [表示コマンド（Show commands）]** をクリックします。

ステップ 2 **[インターフェイス表示コマンド（Interface show commands）]** ウィンドウで、**[コマンド（Commands）]** ドロップダウン ボックスからアクションを選択し、**[実行（Execute）]** をクリックします。インターフェイス設定が画面の右側に表示されます。

Showコマンドの場合は、インターフェイスで対応する**show**テンプレート、またはポート チャネルや vPC などのインターフェイス サブタイプを**テンプレート**で定義する必要があります。

インターフェイスの再検出

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からインターフェイスを再検出するには、次の手順を実行します。

手順

ステップ 1 **[LAN] > [インターフェイス（Interfaces）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 再検出するインターフェイスを選択し、**[アクション（Actions）] > [詳細（More）] > [インターフェイスの再検出（Rediscover Interface）]** の順にクリックして、選択したインターフェイスを再検出します。たとえば、インターフェイスを編集または有効にした後、インターフェイスを再検出できます。

インターフェイス履歴の表示

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からインターフェイス履歴を表示するには、次の手順を実行します。

手順

ステップ 1 **[LAN] > [インターフェイス（Interfaces）] > [インターフェイス（Interfaces）]** を選択します。

ステップ 2 インターフェイスを選択し、**[アクション（Actions）]、[詳細（More）]、[Deployer 履歴（Deployer History）]** の順にクリックして、インターフェイスの設定履歴を表示します。

ステップ 3 **[ステータス（Status）]** をクリックして、その構成インスタンスに設定されている各コマンドを表示します。

インターフェイス構成の展開

Cisco Nexusダッシュボード ファブリック コントローラ Web UIからインターフェイス構成を展開するには、次の手順を実行します。

手順

ステップ 1 **[LAN] > [インターフェイス（Interfaces）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 展開するインターフェイスを選択し、**[アクション（Actions）] > [インターフェイスの展開（Deploy Interfaces）]** をクリックして、インターフェイスに保存されている設定を展開または再展開します。

（注） 複数のインターフェイスを選択し、保留中の設定を展開できます。

インターフェイス設定を展開すると、インターフェイス ステータス情報が更新されます。ただし、全体的なスイッチレベルの状態は保留状態（青色）になることがあります。インターフェイス、リンク、ポリシーテンプレートの更新、トップダウンなどのいずれかのモジュールからインテントが変更されると、スイッチ レベルの全体的な状態は保留状態になります。保留状態では、スイッチに保留中の設定またはスイッチ レベルの再計算がある場合があります。スイッチ レベルの再計算は、次の場合に発生します。

- スイッチに展開する
- 展開中
- 毎時同期中

外部ファブリック インターフェイスの作成

外部ファブリック デバイスのポート チャネル、vPC、サブインターフェイス、およびループバック インターフェイスを追加および編集できます。ストレート FEX およびアクティブ-アクティブ FEX 機能は追加できません。

ブレークアウト ポート機能は、外部ファブリックの Cisco Nexus 9000、3000、および 7000 シリーズ スイッチでのみサポートされます。

外部ファブリック デバイスにインターフェイスを追加すると、リソース マネージャはデバイスと同期しません。そのため、ID フィールドに入力された値（ポート チャネルID、vPC ID、ループバック ID など）がスイッチで事前に設定されていないことを確認します。

外部ファブリックでポート チャネルを設定する場合は、ポート チャネルが設定されるスイッチに **feature_lacp** ポリシーを追加して展開する必要があります。

外部ファブリックが **[ファブリック モニタ モードのみ（Fabric Monitor Mode Only）]** に設定されている場合は、そのスイッチに設定を展開できません。ファブリック トポロジ画面で **[保存して展開（Save & Deploy）]** をクリックすると、エラー メッセージが表示されます。ただし、次の設定（スイッチ アイコンを右クリックすると使用可能）が許可されます。

vPC ペアリング：vPC スイッチ ペアを指定できますが、これは参照用です。

ポリシーの表示/編集：ポリシーを追加できますが、スイッチに展開することはできません。

インターフェイスの管理：インターフェイスを追加する目的のみを作成できます。インターフェイスを展開、編集、または削除しようとすると、エラー メッセージが表示されます。

インターフェイスグループ

ファブリック レベルでホスト側のインターフェイスをグループ化できるインターフェイス グループを作成できます。具体的には、物理イーサネット インターフェイス、L2 ポート チャネル、および vPC のインターフェイス グループを作成できます。インターフェイス グループのインターフェイスに複数のオーバーレイ ネットワークを接続または接続解除できます。

ガイドライン

- インターフェイス グループは、**Easy_Fabric** テンプレートを使用するファブリックでのみサポートされます。
- インターフェイス グループは、ファブリックに固有です。たとえば、2 つのファブリック（Fab1 と Fabric 2）を考えます。Fab1 のインターフェイス グループ IG1 は、Fab 2 には適用されません。
- インターフェイス グループは、特定のタイプのインターフェイスのみを持つことができます。たとえば、物理イーサネット トランク インターフェイスの場合は IG1、L2 トランク ポート チャネルの場合は IG2、vPC ホスト トランク ポートの場合は IG3 など、3 つのタイプのインターフェイスをグループ化する場合は、3 つの個別のインターフェイス グループが必要です。
- インターフェイス グループは、事前プロビジョニングされたインターフェイスを使用して作成することもできます。
- インターフェイス グループは、リーフ ロールを持つスイッチに限定されます。これらは、Border、BGW、およびその他の関連バリアントなどの他のロールではサポートされません。
- インターフェイス グループの一部である L2 ポート チャネルおよび vPC の場合、インターフェイス グループに関連付けられているネットワークがない場合でも、それらはインターフェイス グループから関連付け解除されるまで削除できません。同様に、オーバーレイ ネットワークを持たないがIGの一部であるトランク ポートは、アクセス ポートに変換で

きません。つまり、インターフェイス グループの一部であるインターフェイスのポリシーは変更できません。ただし、ポリシーの特定のフィールドは編集できます。

- リーフ スイッチの L4～L7 サービス設定では、サービス接続に使用されるトランク ポートをインターフェイス グループの一部にすることはできません。
- イージー ファブリックのファブリック単位のバックアップを実行すると、そのファブリックで作成されたインターフェイス グループがある場合、関連するすべてのインターフェイス グループの状態がバックアップされます。
- イージー ファブリックにインターフェイス グループが含まれている場合、このファブリックは MSO にインポートできません。同様に、イージー ファブリックが MSO に追加されている場合は、イージー ファブリック内のスイッチに属するインターフェイスのインターフェイス グループを作成できません。
- **[インターフェイス グループ（Interface Group）]** ボタンは、管理者およびステージャ ユーザに対してのみ有効です。他のすべてのユーザの場合、このボタンは無効になります。
- **[インターフェイス グループ（Interface Group）]** ボタンは、次の状況では無効になります。
  - **[SCOPE]** ドロップダウン リストから **[データセンター（Data Center）]** を選択します。
  - スイッチのないファブリックを選択します。
  - vPC、ポート チャネル、およびイーサネット以外の他のインターフェイスを選択します。
  - インターフェイスに別の送信元からのポリシーがアタッチされている場合：
    - インターフェイスがポート チャネルまたは vPC のメンバーである場合。
    - ポート チャネルが vPC のメンバーである場合。
    - インターフェイスにアンダーレイまたはリンクからのポリシーがある場合。

（注） 異なるタイプのインターフェイスを選択すると、**[インターフェイス グループ（Interface Group）]** ボタンが有効になります。ただし、インターフェイス グループに対して異なるタイプのインターフェイスを作成または保存しようとすると、エラーが表示されます。

インターフェイス グループの作成

手順

ステップ 1 **[LAN] > [インターフェイス（Interfaces）] > [インターフェイス グループ（Interface Groups）]** の順に選択します。

ステップ 2 **[アクション（Actions）] > [新しいインターフェイス グループの作成（Create new interface group）]** をクリックします。

ステップ 3 [ファブリックの選択（Select Fabric）] ウィンドウで、ファブリックを選択し、**[選択（Select）]** をクリックします。

ステップ 4 [新しいインターフェイス 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 グループ名（Interface Group Name）]フィールドにインターフェイス グループ名を入力し、インターフェイス タイプを選択して、**[保存（Save）]**をクリックします。

インターフェイス グループ名の最大長は 64 文字です。

（注） インターフェイスは、1つのインターフェイス グループにのみ属することができます。

ステップ 5 [インターフェイス（Interfaces）] タブをクリックします。

ステップ 6 グループ化する必要があるインターフェイスを選択し、**[アクション（Actions）]> [インターフェイスグループに追加（Add to interface Group）]** をクリックします。

ステップ 7 **[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウで、**[インターフェイス グループの選択（Select Interface Group）]** フィールドにインターフェイス グループ名を入力してカスタム インターフェイス グループを作成し、**[カスタムの作成（Create custom）]** をクリックします。

すでにインターフェイス グループを作成している場合は、**[インターフェイス グループの選択（Select Interface Group）]** ドロップダウン リストから選択します。また、インターフェイスがすでにインターフェイス グループの一部である場合は、**[インターフェイス グループの選択（Select Interface Group）]** ドロップダウンリストから新しいグループを選択することで、そのインターフェイスを別のインターフェイス グループに移動できます。

インターフェイスグループは、[インターフェイス グループ（Interfaces Groups）] ウィンドウまたは [ファブリックの概要] の [インターフェイス（Interfaces）] ウィンドウから作成できます。

ステップ 8 **[Save（保存）]** をクリックします。

[インターフェイス（Interfaces）] ウィンドウの **[インターフェイス グループ（Interfaces Groups）]** 列にインターフェイス グループ名が表示されます。

インターフェイス グループからのインターフェイスの削除

手順

ステップ 1 **[LAN] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 インターフェイスグループから関連付けを解除するインターフェイスを選択し、**[アクション（Actions）]> [インターフェイスグループから削除（Remove from interface Group）]** をクリックします。

ステップ 3 **[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウで、**[インターフェイス グループの選択（Select Interface Group）]** ドロップダウンリストで何も選択されていないことを確認し、**[クリア（Clear）]** をクリックします。

関連付けられたすべてのインターフェイスをクリアするかどうかを確認するダイアログボックスが表示されます。**[はい（Yes）]** をクリックして続行します。これらのインターフェイスに接続されているネットワークがある場合、**[クリア（Clear）]** をクリックすると、それらのネットワークも切断されます。

インターフェイス グループへのネットワークの接続

手順

ステップ 1 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）]** を起動します。

ステップ 2 **[ネットワーク（Networks）]** タブで、インターフェイス グループに接続する必要があるネットワークを選択し、**[インターフェイス グループ（Interface Group）]** をクリックします。

（注）
- オーバーレイ ネットワークは、複数のインターフェイス グループに属することができます。
- VLAN ID を持つネットワークのみを選択できます。それ以外の場合は、適切なエラー メッセージが表示されます。

ステップ 3 **[インターフェイス グループ（Interface Groups）]** ウィンドウで、次の操作を実行できます。

- **[インターフェイス グループの選択（Select Interface Group）]** ドロップダウン リストから既存のインターフェイス グループを選択し、**[保存（Save）]** をクリックします。

  たとえば、3つのネットワークとインターフェイス グループ **test** を選択し、**[保存（Save）]** ボタンをクリックすると、次の操作がバックグラウンドで実行されます。

  1. 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 グループ **test** の一部であるインターフェイスを取得します。

2. Nexusダッシュボード ファブリック コントローラ は、3 つのネットワークがインターフェイス グループ **test** に追加されることを決定します。したがって、これらのネットワークは、インターフェイス グループ **test** の一部であるすべてのインターフェイスに自動接続されます。
3. インターフェイスごとに、Nexusダッシュボードファブリック コントローラ は、選択したネットワークごとに「**switchport trunk allowed vlan add xxxx**」コマンドを 3 回プッシュします。

   （注） Nexusダッシュボードファブリック コントローラ は、重複する構成インテントがないことを保証します。

[クリア（Clear）] ボタンをクリックすると、Nexusダッシュボード ファブリック コントローラ により「**switchport trunk allowed vlan remove xxx**」構成インテントがプッシュされます。

- **[インターフェイス グループの選択（Select Interface Group）]** フィールドにインターフェイス グループ名を入力してカスタム インターフェイス グループを作成し、**[カスタムの作成（Create custom）]** をクリックします。**[Save（保存）]** をクリックします。

  このオプションを選択する場合は、**[インターフェイス（Interfaces）]** ウィンドウでこのインターフェイス グループにインターフェイスを追加してください。その結果、Nexusダッシュボード ファブリック コントローラ は次の操作を実行します。

  1. インターフェイス グループに属していない既存のすべてのオーバーレイ ネットワークをこれらのインターフェイスから削除します。
  2. インターフェイス グループの一部であるが、まだこれらのインターフェイスに接続されていない新しいオーバーレイ ネットワークを追加します。

     インターフェイス グループへのインターフェイスの関連付けの詳細については、インターフェイス グループの作成 （395 ページ） を参照してください。

ステップ 4 **[続行（Continue）]** をクリックし、**[保存して展開（Save & Deploy）]** をクリックして、選択したネットワークをスイッチに展開します。

インターフェイス グループからのネットワークの接続解除

この手順では、[ネットワーク（Networks）] ウィンドウでインターフェイス グループからネットワークの接続を解除する方法を示します。また、**[インターフェイス（Interfaces）]** ウィンドウでインターフェイス グループからインターフェイスを削除すると、ネットワークの接続を解除できます。詳細については、「インターフェイス グループからのインターフェイスの削除」を参照してください。

手順

ステップ 1 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）]** を起動します。

ステップ 2 **[ネットワーク（Networks）]** タブで、インターフェイス グループに接続する必要があるネットワークを選択し、**[インターフェイス グループ（Interface Group）]** をクリックします。

ステップ 3 **[インターフェイス グループ（Interface Group）]** ウィンドウで、**[インターフェイス グループの選択（Select Interface Group）]** ドロップダウン リストからインターフェイスグループを選択し、**[クリア（Clear）]**をクリックしてネットワークの接続を解除します。

ステップ 4 （任意） **[LAN] > [インターフェイス（Interfaces）]** に移動します。

[オーバーレイ ネットワーク（Overlay Network）] 列の下に、対応するインターフェイスの未接続ネットワークが赤色で表示されます。ネットワークをクリックすると、取り消し線が引かれた設定が表示されます。

ステップ 5 **[ネットワーク（Network）]** 画面に移動します。[ファブリック アクション（Fabrics 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。

インターフェイス グループの削除

インターフェイス グループは、使用されていない場合は自動的に削除されます。インターフェイス グループにマッピングされたインターフェイスおよびネットワークがない場合、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 グループの暗黙的な削除を実行します。このチェックは、**[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウで **[クリア（Clear）]** ボタンをクリックするたびに実行されます。インターフェイスグループを明示的にクリーンアップする必要がある例外シナリオが存在する場合があります。

たとえば、インターフェイス グループ **storageIG** を作成し、それにインターフェイスを追加します。後で、インターフェイス マッピングを別のグループに変更します。したがって、インターフェイスを選択し、**[インターフェイス グループ（Interface Group）]** をクリックして **[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウを開きます。**diskIG** という名前の別のインターフェイス グループを選択します。現在、**storageIG** インターフェイス グループには、関連付けられているメンバー インターフェイスまたはネットワークがありません。この場合は、次の手順を実行します。

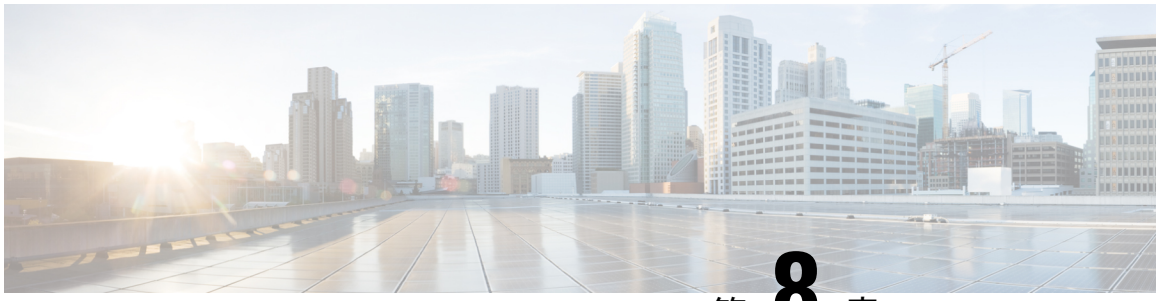
手順

ステップ 1 インターフェイスグループに属していないインターフェイスを選択します。

ステップ 2 インターフェイスを選択し、**[インターフェイス グループ（Interface Group）]** をクリックして **[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウを開きます。

ステップ 3 **[インターフェイス グループの選択（Select Interface Group）]**ドロップダウン リストから **StorageIG** インターフェイス グループを選択します。

ステップ 4 [Clear] をクリックします。



第 8 章

L4～L7 サービスの構成

Cisco Nexus Dashboard ファブリック コントローラでは、レイヤ 4～レイヤ 7（L4～L7）サービス デバイスをデータ センター ファブリックに挿入する機能が導入されました。これらの L4～L7 サービス デバイスにトラフィックを選択的にリダイレクトすることもできます。L4～L7 サービス ノードを追加し、L4～L7 サービス ノードと L4～L7 サービス リーフ スイッチの間にルート ピアリングを作成してから、これらの L4～L7 サービス ノードにトラフィックを選択的にリダイレクトできます。

（注） これは、Nexus Dashboard Fabric Controller、Release 12.0.1a のフィーチャのプレビューです。ラボセットアップでのみ、ベータ版としてマークされたこの機能を使用することをお勧めします。実稼働環境でこれらのフィーチャを使用しないでください。

NDFC リリース 12.0.2a 以降、この機能を本番環境で使用できます。

• L4 ～ L7 サービスか? （401 ページ）

L4 ～ L7 サービスか?

UI パス：**[LAN]** > **[サービス（Services）]**

または、**[LAN]** > **[ファブリック（Fabrics）]** > **[ファブリックの概要（Fabric Overview）]** > **[サービス（Services）]**からナビゲートできます。

Cisco は、データセンター ファブリックに L4～L7 サービス デバイスを挿入する機能を提供しており、これらのサービスデバイスにトラフィックを選択的にリダイレクトすることもできます。サービス ノードを追加し、サービス ノードとサービス スイッチの間にルート ピアリングを作成し、これらのサービス ノードにトラフィックを選択的にリダイレクトできます。

また、サービス リダイレクションのビデオも視聴できます。Cisco Nexusダッシュボード ファブリック コントローラが管理するデータセンターで VXLAN ファブリックを使用して L4～L7 サービスアプライアンスを編成する方法を示しています。このデモでは、プロビジョニング、サービスポリシーの定義、およびリダイレクトされたフローのモニタリングについて説明します。

サービスノード

外部ファブリックを作成し、サービス ノードの作成時にサービス ノードがその外部ファブリックに存在することを指定する必要があります。Nexusダッシュボードファブリック コントローラ は、サービス ノードを自動検出または検出しません。サービス ノード名、タイプ、およびフォーム ファクタも指定する必要があります。サービス ノードの名前は、ファブリック内で一意である必要があります。サービス ノードは、リーフ、ボーダー リーフ、ボーダー スパイン、またはボーダー スーパー スパインに接続されます。Nexusダッシュボード ファブリック コントローラ は、サービス スイッチの新しいスイッチ ロールを定義しません。

Nexusダッシュボードファブリック コントローラは、サービス ノードに接続されているスイッチを管理します。Nexusダッシュボード ファブリック コントローラ は、これらの接続されたスイッチのインターフェイスも管理します。サービス ノードが接続されているインターフェイスがトランク モードであり、どのインターフェイス グループにも属していないことを確認します。L4～L7 サービスは、そのモードを変更しません。接続されたスイッチが vPC ペアを形成している場合、接続されたスイッチの名前は両方のスイッチの組み合わせになります。

必要なサービス名をダブルクリックして、サービス ノードの詳細ウィンドウの以下のタブを表示します。

- 概要 （404 ページ）
- ルート ピアリング （404 ページ）
- サービス ポリシー （408 ページ）

MSD サポート

この機能は、マルチサイト ドメイン（MSD）をサポートします。サービス ノードの作成時に MSD メンバー ファブリックをアタッチされたファブリックとして選択し、サービス ノード（ファイアウォール、ロードバランサなど）を作成し、選択した MSD メンバー ファブリック内のスイッチにサービス ノードをアタッチし、ルート ピアリングとサービス ポリシーを定義し、選択した MSD メンバーファブリックの関連設定を展開します。サービスを構成する手順の詳細については、L4-L7 サービスの設定 （414 ページ） を参照してください。

RBAC サポート

L4～L7 サービスは、ロールベース アクセス コントロール（RBAC）とファブリック アクセス モードをサポートします。

admin、stager、および operator は、Nexusダッシュボード ファブリック コントローラ の事前定義済みロールです。次の表に、各ロールが実行できるさまざまな操作を示します。

サービスオペレーション	サービスノード	ルートピアリング	サービス ポリシー
作成/更新/削除/インポート	admin	admin、stager	admin、stager
リスト/エクスポート	admin、stager、operator	admin、stager、operator	admin、stager、operator

サービスオペレーション	サービスノード	ルートピアリング	サービス ポリシー
Attach/Detach	該当なし	admin、stager	admin、stager
Deploy	該当なし	admin（ファブリックがファブリック モニタまたは読み取り専用モードの場合はブロックされます）	admin（ファブリックがファブリック モニタまたは読み取り専用モードの場合はブロックされます）
プレビュー/展開履歴	該当なし	admin、stager、operator	admin、stager、operator

境界スイッチの WAN インターフェイスでの PBR サポート

トップダウン設定で定義されていない任意のネットワークを、サービス ポリシーの送信元または宛先ネットワークとして指定できます。これは、南北トラフィックのポリシー適用の合理化に役立ちます。Nexusダッシュボード ファブリック コントローラ UI には、VRF アソシエーションを持つすべてのボーダー スイッチ（スタンドアロンまたは vPC）のルーテッド レイヤ 3 インターフェイスがリストされます。その後、定義されたポリシーに関連付ける必要がある必要なインターフェイスを選択できます。境界スイッチには、境界リーフ、境界スパイン、境界スーパー スパイン、境界ゲートウェイが含まれます。複数のインターフェイス アソシエーションを設定できます。たとえば、1つの境界スイッチに対して複数のL3インターフェイス、サブインターフェイス、およびポートチャネルを選択できます。インターフェイスアソシエーション用に複数の境界スイッチを選択することもできます。詳細については、『NX-OS Unicast Routing Configuration Guide』を参照してください。

ポリシーの方向によっては、「任意」または任意のネットワークの境界スイッチとインターフェイスの関連付けが不要な場合があります。たとえば、転送ポリシーの場合、「任意」または任意の宛先ネットワークには、境界スイッチとインターフェイス入力またはルートマップの関連付けは必要ありません。リバース ポリシーの場合、境界スイッチとインターフェイスまたはルート マップの関連付けは、「任意」または任意の送信元ネットワークには必要ありません。

「任意」または任意のネットワークを含むポリシーが接続されると、ポリシー関連のCLIが生成され、境界スイッチの選択されたL3ルーテッド インターフェイスに関連付けられます。そのポリシーを展開すると、選択した境界スイッチにCLIがプッシュされます。展開履歴には対応するエントリが含まれ、VRFフィルタリングを使用してすばやくアクセスできます。サービス ポリシー統計情報の図には、境界スイッチの選択したL3ルーテッドインターフェイスに関連付けられたルート マップの PBR 統計情報が含まれます。

静的ルート

L4～L7サービスは、スタティック ルートで参照されているVRFがアタッチされているすべての VTEP（サービス リーフ スイッチを含む）にスタティック ルートをプッシュします。これにより、スタティック ルートによるサービス ノードのフェールオーバーが促進されます。

概要

[概要（Overview）] タブでは、選択したサービス ノードの **[概要（Summary）]**、**[ルート ピアリング（Route Peering）]**、**[サービス ポリシー（ Service Policy）]** トポロジを表示できます。

[更新（Refresh）] アイコンをクリックして、最新の詳細を表示します。

ルートピアリング

UI パス：**[LAN]** > **[サービス（Services）]** を選択し、必要なサービス名をダブルクリックして、詳細ウィンドウを表示します。**[ルート ピアリング（Route Peering）]** タブに移動します。

または、**[LAN]** > **[ファブリック（Fabrics）]** を選択し、ファブリックの詳細ビューをクリックし、**[サービス（Services）]** をクリックして、**[ルート ピアリング（Route Peering）]** タブを表示することもできます。

ルート ピアリングはサービス ネットワークを作成します。Nexus Dashboard ファブリック コントローラは、スタティック ルートと eBGP ベースのダイナミック ルート ピアリング オプションの両方をサポートします。サービス ネットワークを指定し、テナントのピアリング ポリシーを選択すると、Nexus ダッシュボード ファブリック コントローラは指定されたテナントの下にサービス ネットワークを自動的に作成します。このガイドでは、テナントと VRF という用語は同じ意味で使用されます。

サービス ネットワークは削除できません。サービス ネットワークの削除は、サービス ルート ピアリング削除プロセス中に自動的に処理されます。テナント/VRFごとに複数のルート ピアリングを定義できます。

ルート ピアリングを作成するには、ルート ピアリングの作成（416 ページ）を参照してください。

次の表で、[ルート ピアリング（Route Peering）] 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。

フィールド	説明
サービス ネットワーク 1	
ピアリング名	サービスのピアリング名を指定します **ピアリング名**をダブルクリックすると、詳細ウィンドウが表示されます。詳細については、ルート ピアリングの詳細（407 ページ）を参照してください。
デプロイ	展開のタイプを指定します。展開は次のいずれかになります。 • テナント内ファイアウォール • テナント間ファイアウォール • ワンアーム ロードバランサ

フィールド	説明
ピアリング オプション	選択したピアリング オプションを指定します。
ステータス	Specifies the status of service
添付ファイルの状態	サービスがアタッチされているか、デタッチされているかの状態を指定します
VRF	サービス ノードに接続されている VRF の名前を指定します
[ネットワーク名（Network Name）]	サービス ノードに関連付けられているネットワークの名前を指定します。
Gateway IP	サービス ノードのゲートウェイの IP アドレスを指定します。
サービス ネットワーク 2	
VRF	サービスにアタッチされている VRF の名前を指定します
[ネットワーク名（Network Name）]	サービス ノードに関連付けられているネットワークの名前を指定します。
Gateway IP	ゲートウェイ IP アドレスを指定します。
ネクストホップIP	サービス ノードに関連付けられたホップ IP アドレスを指定します
リバースネクストホップ IP	サービス ノードに関連付けられたリバース ネクスト ホップ IP アドレスを指定します
ネクストホップ IPv6	サービス ノードに関連付けられたネクスト ホップ IPv6 アドレスを指定します
リバースネクストホップ IPv6	サービス ノードに関連付けられたリバース ネクスト ホップ IPv6 アドレスを指定します。
最終更新	サービス ノードの最終変更日時を指定します。

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。**[ルート ピアリング（Route Peering）]** ウィンドウに表示されるものです。

アクション項目	説明
追加（Add）	[追加（Add）] を選択します。**[ルート ピアリングの作成（Create Route Peering）]**ウィンドウが表示されます。 必要なパラメータを指定して、**[保存（Save）]** をクリックします。

アクション項目	説明
編集	必要なピアリングを選択し、[編集] をクリックします。**[ルート ピアリングの編集（Edit Route Peering）]**ウィンドウが表示されます。 トグルを使用して、ルート ピアリングをアタッチまたはデタッチします。サービス ポリシーがアタッチまたは有効化されると、対応するポリシーが VRF（テナント）、送信元、および宛先ネットワークに適用されます。 必要なパラメータを指定し、**[保存（Save）]** をクリックします。
添付	特定のルート ピアリングをスイッチにアタッチするには、必要なピアリングを選択して、**[アタッチ（Attach）]** をクリックします。 （注） ルート ピアリングの一括アタッチ、デタッチ、プレビュー、および展開がサポートされています。最大 10 のルート ピアリングのみに制限されています。
切断	特定のルート ピアリングをスイッチからデタッチするには、必要なピアリングを選択して、**[デタッチ（Detach）]** をクリックします。
プレビュー	プレビューを表示するには、必要なピアリングを選択して**[プレビュー（Preview）]** をクリックします。 **[ルート ピアリングのプレビュー（Preview Route Peering）]** ウィンドウが表示されます。 特定のスイッチ、ネットワーク、または VRF のルート ピアリングを表示するには、それぞれのドロップダウン リストから特定のスイッチ、ネットワーク、または VRF を選択します。[閉じる（Close）] をクリックして、ウィンドウを閉じます。
展開	ルート ピアリングを展開するには、必要なピアリングを選択し、**[展開（Deploy）]** をクリックします。 展開の確認のためのポップアップ ウィンドウが表示されます。[展開（Deploy）] をクリックします。
インポート	ルート ピアリング情報を Excel ファイルとしてインポートするには、[インポート]をクリックします。**[ルート ピアリングのインポート（Route Peering Import）]**ウィンドウが表示されます。 **[参照（Browse）]** をクリックして適切なファイルを選択し、**[インポート（Import）]** をクリックしてルート ピアリングに関する情報をインポートします。

アクション項目	説明
エクスポート	ルート ピアリング情報をExcelファイルとしてエクスポートするには、**[エクスポート（Export）]** をクリックします。**[ルート ピアリングのエクスポート（Route Peering Export）]**ウィンドウが表示されます。 **[エクスポート（Export）]** をクリックして、選択したルート ピアリングに関する情報をエクスポートします。
削除（Delete）	ルート ピアリングを削除するには、適切なルート ピアリングを選択し、**[削除（Delete）]** をクリックします。

ルート ピアリングの詳細

ピアリングの詳細ウィンドウを表示するには、**[サービス（Services）]**に移動し、必要なサービスの**[名前（Name）]**をダブルクリックします。ピアリングの詳細ウィンドウが表示されます。このウィンドウでは、以下のタブを表示できます。

- 概要
- ステータスの詳細
- ルートピアリング
- サービス ポリシー

概要

[概要（Overivew）] タブには、**[ルート ピアリングの概要（Route Peering Summary）]** と、内部及び外部ネットワークの詳細、**[サービス ポリシー（Service Policies）]**、および **[サービス ノード（Service Node）]** がカードとして表示されます。

ステータスの詳細

このタブは、展開された構成のピークを提供します。**i** アイコン（各行の **[ステータスの詳細（Status Details）]** フィールドの横）にカーソルを合わせると、詳細が表示されます。

サービス ポリシー

サービス ポリシー （408 ページ） を参照してください。

展開履歴の表示

このタブには、ルートピアリングに関係するスイッチとネットワークの展開履歴が表示されます。このタブには、ネットワークの名前、VRF、スイッチ、ステータス、ステータス メッセージ、ステータスの詳細、実行時間などの情報が表示されます。

サービス ポリシー

任意または任意のネットワークでサービス ポリシーを定義し、境界スイッチの L3 ルーテッド インターフェイスに関連付けることができます。詳細については、「境界スイッチの WAN インターフェイスでの PBR サポート」を参照してください。L4～L7 サービスは、ルート ピアリング中に定義されたサービス ネットワーク以外の VRF またはネットワークを作成しません。作成されたネットワーク間でサービス ポリシーを定義する場合、送信元と宛先のネットワークは、サブネット、個々の IP アドレス、またはファブリックの詳細画面の **[サービス（Services）]** タブで定義されたネットワークにすることができます。**[LAN] > [ファブリック（Fabric）]** を選択し、[ファブリック（Fabric）] の 詳細ビューをクリックして、[サービス（Services）] タブを表示します。テナント内ファイアウォール、1 アームおよび 2 アームのロード バランサの場合、Nexus ダッシュボード ファブリック コントローラ の L4～L7 サービスはサービスの挿入にポリシーベース ルーティング（PBR）を使用します。テナント間ファイアウォールにはサービス ポリシーがありません。必要なのは、サービス ノードを作成し、テナント間ファイアウォールのピアリングをルーティングすることだけです。

送信元および宛先ネットワークはサービス ポリシーの展開とは関係なく接続または展開できるため、テナント/VRF 関連のサービス ポリシー設定は、サービス ノードに接続されたスイッチにのみ接続またはプッシュされ、送信元および宛先ネットワークは更新されます。サービス ポリシー関連の構成を使用します。生成された設定をプレビューして確認できます。デフォルトでは、サービス ポリシーは定義されていますが、有効またはアタッチされていません。アクティブ化するには、サービス ポリシーを有効にするか、アタッチする必要があります。

送信元および宛先ネットワークが接続されている場合は、送信元および宛先ネットワークに関連するサービス構成が自動処理され、ネットワークがすでに接続または展開されている場合は自動更新されます。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 5 分ごとに統計情報を収集し、集計および分析のためにデータベースに保存します。デフォルトでは、統計情報は最大 7 日間保存されます。

サービスの挿入は、作成されるフローでのみ有効です。既存のフローには影響ありません。有効なサービス ポリシーがそのネットワークに関連付けられている場合、ネットワークの削除は許可されません。

L4～L7 サービス統合は、Easy ファブリック ポリシーを適用した上で構築されます。**[LAN] > [ファブリック（Fabrics）]** を選択し、VXLAN EVPN ファブリックを作成し、事前定義されたファブリック ポリシーを使用して Cisco Nexus 9000 シリーズ スイッチをファブリックにインポートします。

サービス ポリシーの作成については、サービスポリシーの作成（423 ページ） を参照してください。

次の表で、[ルート ピアリング（Route Peering）] 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。

フィールド	説明
ポリシー名	サービスのポリシー名を指定します。 **[ポリシー名（Policy Name）]**をダブルクリックすると、詳細ウィンドウが表示されます。詳細については、サービス ポリシーセクションを参照してください。
ルートピアリング	ルート ピアリング名を指定します。
ステータス	Specifies the status of service
添付ファイルの状態	サービスがアタッチされているか、デタッチされているかの状態を指定します
Source VRF	サービス ノードに接続されている VRF の名前を指定します
送信元ネットワーク	Specifies the name of source network
宛先VRF	サービス ノードに接続されている宛先 VRF の名前を指定します
宛先ネットワーク（Destination Network）	Specifies the name of destination network
ネクストホップIP	サービス ノードに関連付けられたホップ IP アドレスを指定します
リバースネクストホップ IP	サービス ノードに関連付けられたリバース ネクスト ホップ IP アドレスを指定します
ネクストホップ IPv6	サービス ノードに関連付けられたネクスト ホップ IPv6 アドレスを指定します
リバースネクストホップ IPv6	サービス ノードに関連付けられたリバース ネクストホップ IPv6 アドレスを指定します。
リバース有効	リバース ネクスト ホップを有効にするかどうかを指定します。
ルートマップアクション	オプションはpermitまたはdenyです。[許可（permit）]を選択すると、一致したトラフィックはネクストホップオプションと定義されたポリシーに基づいてリダイレクトされます。[拒否（deny）]を選択すると、トラフィックはルーティングテーブルルールに基づいてルーティングされます。

フィールド	説明
ネクストホップオプション	Specify an option for the next-hop. オプションは、none、drop-on-fail、およびdropです。noneを選択すると、一致したトラフィックは定義されたPBRルールに基づいてリダイレクトされます。drop-on-failを選択すると、指定したネクストホップが到達不能な場合、一致したトラフィックはドロップされます。ドロップを選択すると、一致したトラフィックがドロップされます。
最終更新	サービス ポリシーが最後に更新された時刻を表示します。

The following table describes the action items, in the **Actions** drop-down list, that appears in the **Route Peering** window.

アクション項目	説明
追加（Add）	[追加（Add）] を選択します。The **Create Service Policy** window appears. Specify the required parameters and click **Save**.
編集	必要なサービスポリシーを選択し、[編集]をクリックします。The **Edit Service Policy** window appears. トグルを使用して、サービスポリシーをアタッチまたはデタッチします。サービスポリシーがアタッチまたは有効化されると、対応するポリシーがVRF（テナント）、送信元、および宛先ネットワークに適用されます。 必要なパラメータを指定し、**[保存（Save）]** をクリックします。
添付	特定のサービスポリシーをスイッチにアタッチするには、必要なポリシーを選択して [アタッチ] をクリックします。 （注） ルート ピアリングの一括アタッチ、デタッチ、プレビュー、および展開がサポートされており、最大 10 のサービス ポリシーのみに制限されています。
切断	特定のサービス ポリシーをスイッチから切り離すには、必要なサービス ポリシーを選択し、[切り離し] をクリックします。
プレビュー	プレビューを表示するには、必要なピアリングを選択して [プレビュー] をクリックします。 [サービス ポリシーのプレビュー] ウィンドウが表示されます。 特定のスイッチ、ネットワーク、またはVRFのサービスポリシーを表示するには、それぞれのドロップダウンリストから特定のスイッチ、ネットワーク、または VRF を選択します。[閉じる（Close）] をクリックして、ウィンドウを閉じます。

アクション項目	説明
展開	サービス ポリシーを展開するには、必要なサービス ポリシーを選択し、[展開] をクリックします。 A pop-up window appears for confirmation to deploy. [展開（Deploy）] をクリックします。
インポート	サービス ポリシー情報を Excel ファイルとしてインポートするには、[インポート] をクリックします。The **Service Policy Import** window appears. [参照] をクリックして適切なファイルを選択し、[インポート] をクリックしてサービス ポリシーに関する情報をインポートします。
エクスポート	ルート サービス ポリシー情報を Excel ファイルとしてエクスポートするには、**[エクスポート（Export）]** をクリックします。**[サービス ポリシーのエクスポート（Service Policy Export）]** ウィンドウが表示されます。 **[エクスポート（Export）]** をクリックして、選択したサービス ポリシーに関する情報をエクスポートします。
削除（Delete）	サービス ポリシーを削除するには、適切なサービス ポリシーを選択し、**[削除（Delete）]** をクリックします。

サービス ポリシーの詳細

サービス ポリシー ウィンドウを表示するには、**[サービス（Services）]** に移動し、必要なサービスの**[名前（Name）]** をダブルクリックします。サービス ポリシーの詳細ウィンドウが表示されます。このウィンドウでは、以下のタブを表示できます。

- 概要
- ステータスの詳細
- ルートピアリング
- サービス ポリシー

概要

[概要（Overivew）] タブには、内部および外部ネットワークの **[ポリシーの概要（Policy Summary）]**、**[サービス ノード（Service Node）]**、および**[ルート ピアリング（Route Peering）]** が、カードとして表示されます。

ステータスの詳細

このタブには、選択したサービス ポリシーに関連付けられた **[リソース タイプ（Resource Type）]**、**[ファブリック名（Fabric Name）]**、**[リソース名（Resource Name）]** の詳細が表示されます。

統計情報

このタブには、構成されたサービス ポリシーに関する統計情報が表示されます。**[時間範囲（Time Range）]** ドロップダウン ボックスから、統計を表示する時間範囲を選択します。ウィンドウに表示されているカレンダーから日付と時刻を選択するには、ウィンドウの右下隅にある**時間の選択**をクリックします。過去 15 分、1 時間、6 時間、1 日、1 週間、1 か月の統計を表示することもできます。必要な時間範囲を選択し、**[適用（Apply）]** をクリックします。**[スイッチ（Switch）]** ドロップダウン リストから、統計を表示するスイッチを選択します。選択したスイッチの指定した時間範囲での統計が表示されます。

関連するすべてのスイッチの特定のポリシーの統計をリセットするには、**[統計のクリア（Clear Stats）]** をクリックします。複数のポリシーが同じルート マップを共有している場合、他のポリシーの統計も影響を受けます。

展開履歴の表示

このタブには、サービス ポリシーに関係するスイッチおよびネットワークの展開履歴が表示されます。このタブには、ネットワーク名、VRF、スイッチ名、ステータス、ステータス メッセージ、ステータスの詳細、実行時間などの情報が表示されます。

L4～L7 サービスの注意事項と制限事項

- Nexus Dashboard ファブリック コントローラの L4～L7 サービスは、ファイアウォール、ロード バランサ、仮想ネットワーク機能などのサービス ノードを管理またはプロビジョニングしません。
- L4～L7 サービス機能は、**Easy_Fabric** テンプレートを使用する VXLAN BGP EVPN ファブリックでのみサポートされます。
- この機能で定義されるサービス ポリシーは、ポリシーベース ルーティング（PBR）を利用します。PBR 関連の設定、制約などについては、Nexus 9000 Series NX-OS Unicast Routing Configuration Guide を参照してください。
- この機能は、Cisco Nexus 9300-EX および 9300-FX プラットフォーム スイッチを、リーフ、ボーダー リーフ、ボーダー 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 スイッチとして動作するようにサポートします。
- L3 ネットワーク用のテナント内およびテナント間ファイアウォール、およびワンアーム仮想ネットワーク機能およびツーアーム展開のロードバランサを含む設定がサポートされています。

- 既存の Nexus ダッシュボード ファブリック コントローラ トポロジ ビューは、サービス ノードが接続されているスイッチに関連付けられたリダイレクトされたフローを表示します。特定のリダイレクトされたフローを見つけるためにも利用されます。
- L4～L7 サービス REST API は、Nexus ダッシュボード ファブリック コントローラにより パッケージ化された REST API ドキュメントからアクセスできます。詳細については、『Cisco Nexus Dashboard Fabric Controller REST API Reference Guide』を参照してください。
- L4～L7 サービスは、リアルタイムの対話のために Kafka 通知を生成します。
- ロード シェアリングはサポートされていません。
- この機能は、必要に応じてサービスネットワークを作成、更新、削除します。サービス ネットワークは、**[LAN] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** ウィンドウから作成または削除することはできません。

サービス デバイスのタイプ

Cisco Nexus Dashboard Fabric Controller の L4～L7 サービスは、すべてのベンダーのサービス ノード接続をサポートします。データセンターに導入される一般的なサービス ノード タイプは、ファイアウォール、ロード バランサ、およびその他のレイヤ 4 ーレイヤ 7 製品です。

サポートされているファイアウォール ベンダーの例は、Cisco Systems、Palo Alto Networks、Fortinet、Check Point Software Technologies などです。

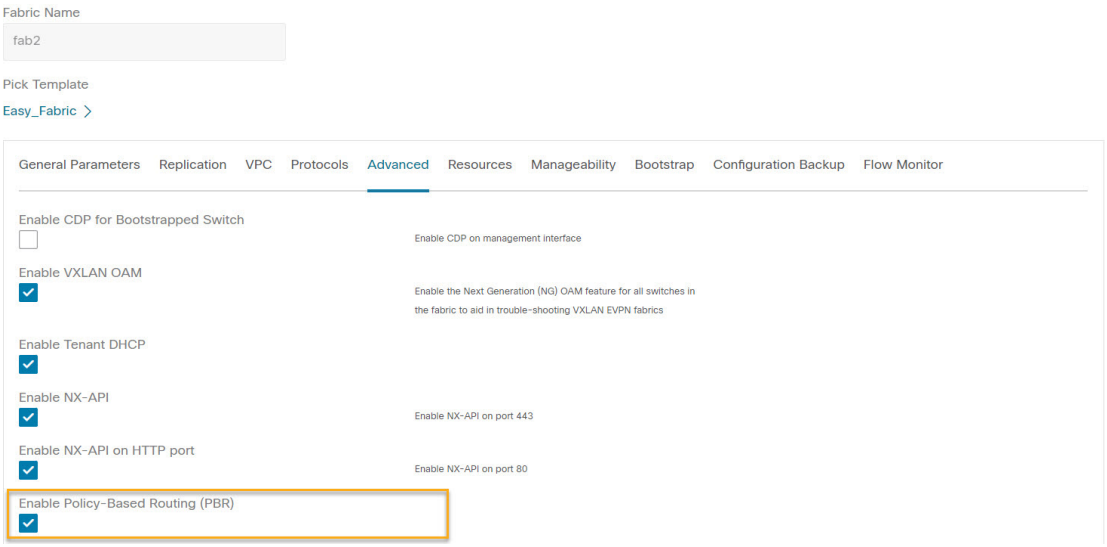
サポートされているロードバランサ ベンダーの例は、F5 ネットワーク、Citrix システム、A10 ネットワークなどです。

これらの例のリストは例として使用するものであり、すべてを網羅するものではありません。L4～L7 サービス接続は汎用であり、すべてのベンダー サービス ノードに適用されます。

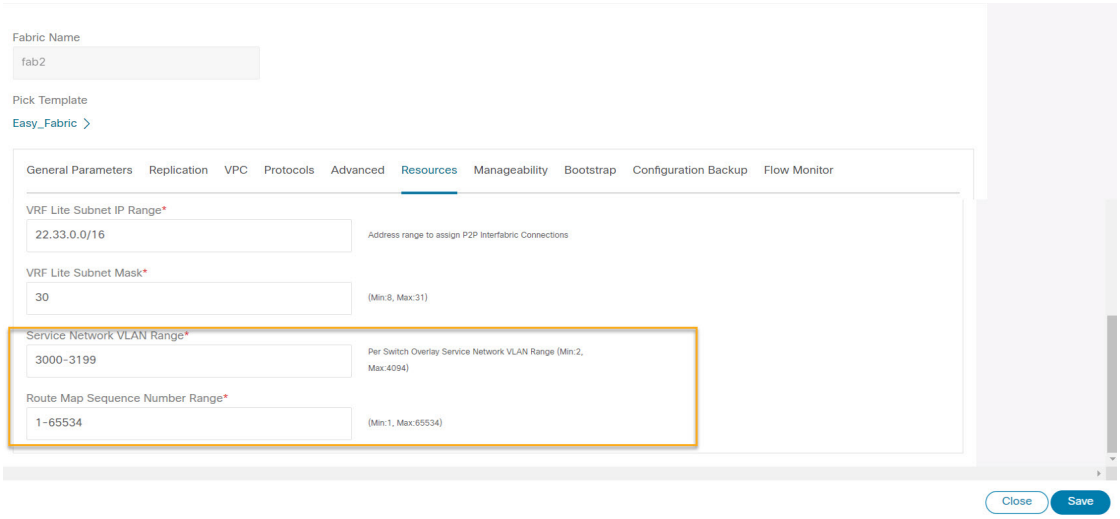
L4～L7 サービスのファブリック設定の構成

L4～L7サービス機能を有効にするには、特定のファブリック設定を構成する必要があります。これらの設定を行うには、**[LAN] > [ファブリック（Fabrics）]** を選択し、**[アクション（Actions）] > [ファブリックの作成（Create Fabric）]** をクリックします。

[ファブリックの作成（Create Fabric）] ウィンドウが表示されます。ファブリック名を入力し、テンプレートを選択します。[詳細設定（Advanced）] をクリックします。**[ポリシーベース ルーティング (PBR) の有効化 (Enable Policy-Based Routing (PBR))]** チェックボックスをオンにして、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します。



[リソース（Resources）] 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）]** フィールドで VLAN 範囲を指定します。これは、スイッチ オーバーレイ サービス ネットワーク単位での VLAN 範囲です。最小許容値は 2、最大許容値は 4094 です。また、**[ルート マップ シーケンス番号の範囲（Route Map Sequence Number Range）]** フィールドの値を指定します。最小許容値は 1、最大許容値は 65534 です。**[保存（Save）]** をクリックして、更新された構成を保存します。



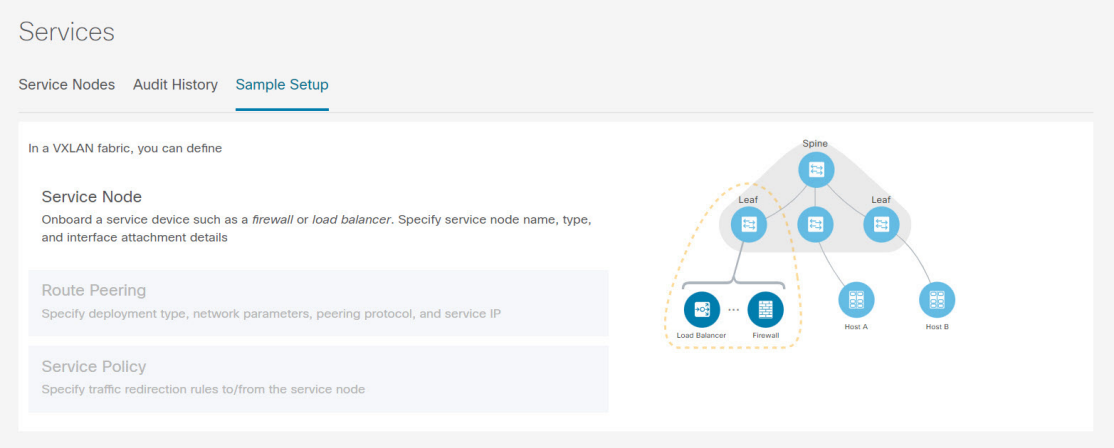
L4-L7 サービスの設定

Cisco Nexus Dashboard Fabric Controller の Web UI で L4～L7 サービスまたは Elastic Service を起動するには、**[LAN] > [サービス（Services）]** を選択します。

以下のいずれかのパスを使用して、**[サービス（Services）]** タブに移動することもできます。

[LAN] > [ファブリック（Fabrics）] > [ファブリックの概要（Fabric Overview）] > [サービス（Services）]

[LAN] > [スイッチ（Switches）] > [スイッチの概要（Switches Overview）] > [サービス（Services）]

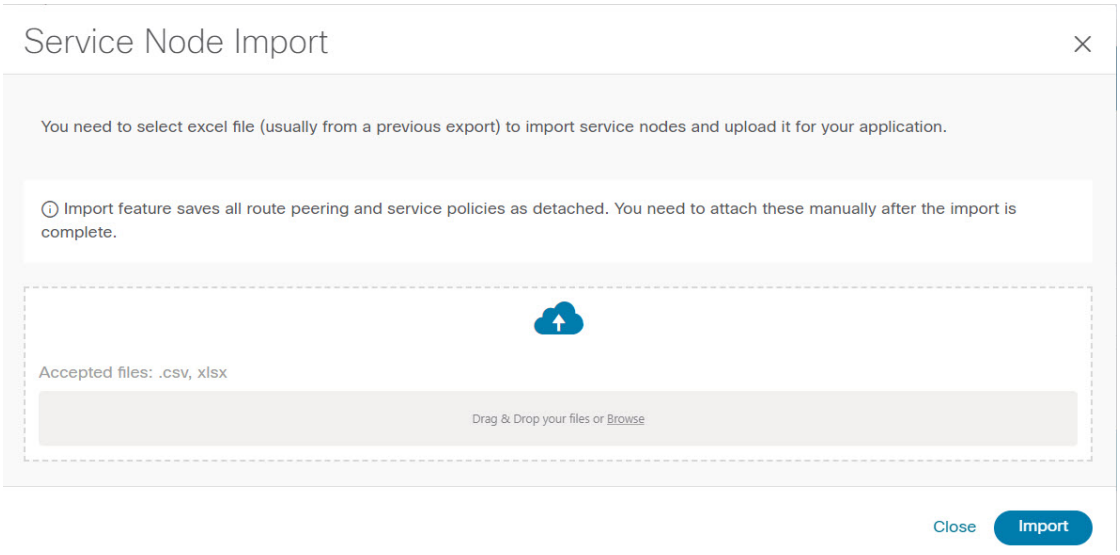


サービス構成のプロセスは、次の手順で構成されています。

サービス ノードの追加

以下のいずれかのパスを使用して、**[サービス ノード（Service Node）]** タブに移動できます。

[LAN] > [サービス（Services）]



サービス ノードを作成するには、**[アクション（Actions）] > [追加（Add）] > [サービス ノード（Service Nodes）]**の順にクリックします。**[新しいサービス ノードの作成（Create New Service Nodes）]** ウィンドウが表示されます。

[新しいサービス ノードの作成（Create New Service Node）] ウィンドウには、**[新しいサービス ノードの作成（Create New Service Node）]**、**[ルート ピアリングの作成（Create Route**

Peering）]、および **[サービス ポリシーの作成（Create Service Policy）]** の 3 つのステップがあります。

[新しいサービス ノードの作成 (Create New Service Node)] ウィンドウには、**[サービス ノードの作成 (Create Service Node)]** と **[スイッチのアタッチメント (Switch Attachment)]** の 2 つのセクションがあり、その後に **[テンプレートのリンク (Link Template)]** ドロップダウン リストがあります。このドロップダウンリストからは、指定され、アタッチされたインターフェイス タイプに基づき、[service_link_trunk]、[service_link_port_channel_trunk]、および [service_link_vpc] を選択できます。

[新しいサービス ノードの作成 (Create New Service Node)] ウィンドウのフィールドは次のとおりです。アスタリスク付きのフィールドの記入が必須です。

新しいサービス ノードの作成

[サービス ノード名 (Service Node Name)]：サービス ノードのノード名を入力します。名前には、英数字、アンダースコア、またはダッシュ文字を使用できます。

[サービス ノードのタイプ (Service Node Type)]：[ファイアウォール (Firewall)]、[ロード バランサ (Load Balancer)]、または [仮想ネットワークの機能 (Virtual Networking Function)] を選択します。

[フォーム ファクタ (Form Factor)]：[物理 (Physical)] または [仮想 (Virtual)] を選択します。

[外部ファブリック (External Fabric)]：外部ファブリックを指定します。

[サービス ノード インターフェイス (Service Node Interface)]：サービス ノード インターフェイスを指定します。

[アタッチされたファブリック (Attached Fabric)]：リストからファブリックを選択します。

[アタッチされたスイッチ（Attached Switch）]：リストからスイッチまたはスイッチ ペアを選択します。

[アタッチされたスイッチ インターフェイス (Attached Switch Interface)]：リストからインターフェイスを選択します。**[アタッチされたリーフ スイッチ（Attached Leaf Switch）]** リストから vPC ペアを選択すると、vPC チャネルが **[アタッチされたスイッチ インターフェイス（Attached Switch Interface）]** リストに表示されます。それ以外の場合、トランク モードのポートチャネルおよびインターフェイスは、**[アタッチされたリーフ スイッチ インターフェイス (Attached Leaf Switch Interface)]** リストに表示されます。

[リンク テンプレート (Link Template)]：[service_link_trunk]、[service_link_port_channel_trunk]、または [service_link_vpc] テンプレートを選択します。テンプレート フィールドについての詳細は、テンプレート （Templates） （425 ページ）を参照してください。

使用するテンプレートに応じて、フォームが表示されます。フォームのすべての必須フィールドを更新し、**[保存 (Save)]** をクリックします。

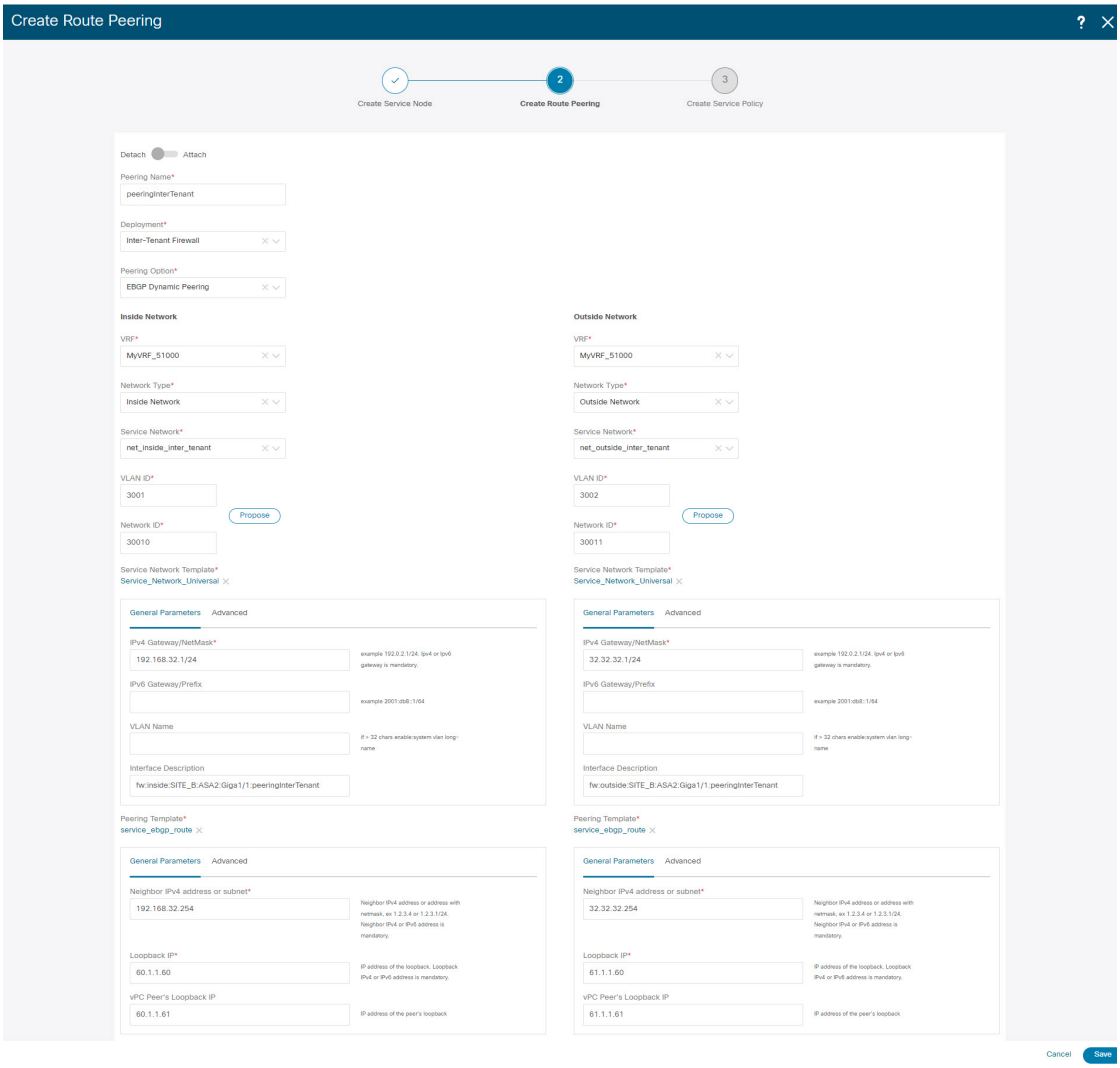
ルート ピアリングの作成

以下のいずれかのパスを使用して、**[ルート ピアリング（Route Peering）]** タブに移動できます。

[LAN] > [サービス（Services）]

[ルート ピアリングの作成（Create Route Peering）] ウィンドウに表示されるフィールドは、**[新しいサービス ノードの作成（Create New Service Node）]** ウィンドウで選択した L4～L7 サービスのタイプによって異なります。選択したタイプ（ファイアウォールまたはロード バランサ）に応じて、展開のタイプは、テナント内ファイアウォール、テナント間ファイアウォール、ワンアーム ロード バランサ、およびツーアーム ロード バランサです。

（注） 詳細画面の**[ネットワーク（Networks）]** タブでのサービス ネットワークの削除は許可されていません。これは、**[LAN] > [ファブリック（Fabrics）]** パスを選択し、**[起動（Launch）]** アイコンをクリックして、**[ネットワーク（Network）]** ウィンドウで表示されるものです。



内部ネットワーク

[VRF]：VRF を指定します。

[ネットワーク タイプ（Network Type）]：[内部ネットワーク（Inside Network）]を選択します。

[サービス ネットワーク（Service Network）]：サービスネットワークの名前を指定します。

[VLAN ID]：VLAN ID を指定します。有効な ID の範囲は 2 ～ 3967 です。定義済みの L4～L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、[提案（Propose）] をクリックします。

[サービス ネットワーク テンプレート]：ドロップダウンリストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、テンプレート（Templates） （425 ページ）を参照してください。

外部ネットワーク

[VRF]：VRF を指定します。

[ネットワーク タイプ（Network Type）]：[外部ネットワーク（Outside Network）] を選択します。

[サービス ネットワーク（Service Network）]：L4～L7 サービス ネットワークの名前を指定します。

[VLAN ID]：VLAN ID を指定します。有効な ID の範囲は 2 ～ 3967 です。定義済みの L4～L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、[提案（Propose）] をクリックします。

[サービス ネットワーク テンプレート]：ドロップダウンリストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、テンプレート（Templates） （425 ページ）を参照してください。

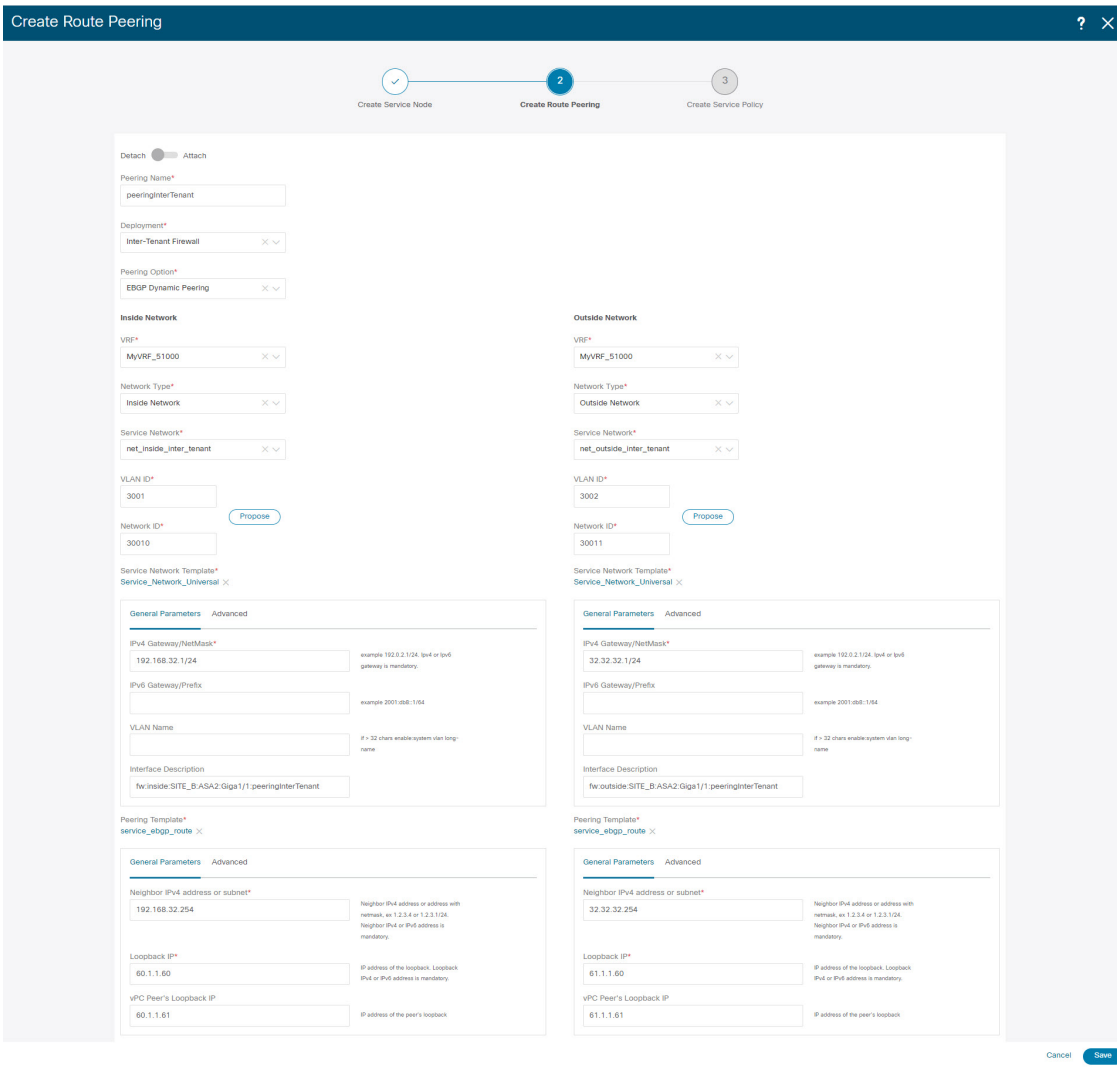
ネクスト ホップ セクション

[ネクスト ホップ IP アドレス（Next Hop IP Address）]：ネクストホップ IP アドレスを指定します。これは、トラフィック リダイレクションに使用されるサービス ノードの IP/VIP です。

[リバース トラフィックのネクスト ホップ IP アドレス（Next Hop IP Address for Reverse Traffic）]：リバース トラフィックのネクスト ホップ IP アドレスを指定します。これは、トラフィック リダイレクションに使用されるサービス ノードの IP/VIP です。

例：テナント間ファイアウォールの展開

ピアリング オプション：**静的ピアリング、内部ネットワーク ピアリング テンプレート**：**service_static_route、外部ネットワーク ピアリング テンプレート**：**service_static_route**



テナント間ファイアウォールを展開するための[ルートピアリングの作成（Create Route Peering）]ウィンドウのフィールドは次のとおりです。アスタリスク付きのフィールドの記入が必須です。

[ピアリング名（Peering Name）]：ピアリングの名前を指定します。名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。

[展開（Deployment）]：[テナント間ファイアウォール（Inter-Tenant Firewall）]を選択します。

[ピアリング オプション（Peering Option）]：[静的ピアリング（Static Peering）]または[eBGP動的ピアリング（eBGP Dynamic Peering）]を選択します。

内部ネットワーク

[VRF]：ドロップダウンリストから[VRF]を選択します。

[ネットワーク タイプ（Network Type）]：[内部ネットワーク（Inside Network）]を選択します。

[サービス ネットワーク（Service Network）]：L4～L7 サービス ネットワーク名を指定します。

[VLAN ID]：VLAN ID を指定します。有効な ID の範囲は 2 ー 3967 です。定義済みの L4～L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、**[提案（Propose）]** をクリックします。

[ネットワーク ID（Network ID）]：ネットワーク ID を指定します。有効な ID の範囲：

[サービス ネットワーク テンプレート]：ドロップダウンリストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、テンプレート（Templates） （425 ページ）を参照してください。

[ピアリング テンプレート（Peering Template）]：ドロップダウンリストから [service_static_route] または [service_ebgp_route] を選択します。テンプレート フィールドについての詳細は、テンプレート （Templates） （425 ページ）を参照してください。

外部ネットワーク

[VRF]：ドロップダウンリストから [VRF] を選択します。

[ネットワーク タイプ（Network Type）]：[外部ネットワーク（Outside Network）] を選択します。

[サービス ネットワーク（Service Network）]：L4～L7 サービス ネットワーク名を指定します。

[VLAN ID]：VLAN ID を指定します。有効な ID の範囲は 2 ー 3967 です。定義済みの L4～L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、**[提案（Propose）]** をクリックします。

[サービス ネットワーク テンプレート]：ドロップダウンリストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、テンプレート （Templates） （425 ページ）を参照してください。

[ピアリング テンプレート（Peering Template）]：ドロップダウンリストから [service_static_route] または [service_ebgp_route] を選択します。テンプレート フィールドについての詳細は、テンプレート （Templates） （425 ページ）を参照してください。

例：ワンアーム モードのロード バランサ

ワンアーム ファイアウォールを展開するための **[ルート ピアリングの作成（Create Route Peering）]** ウィンドウのフィールドは次のとおりです。アスタリスク付きのフィールドの記入が必須です。

[ピアリング名（Peering Name）]：ピアリングの名前を指定します。名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。

[展開（Deployment）]：[ワンアーム ファイアウォール（One-Arm F）] を選択します。

[ピアリング オプション（Peering Option）]：[静的ピアリング（Static Peering）] または [eBGP 動的ピアリング（eBGP Dynamic Peering）] を選択します。

内部ネットワーク

[VRF]：ドロップダウンリストから [VRF] を選択します。

[ネットワーク タイプ（Network Type）]：[ファースト モード（First Mode）] を選択します。

[サービス ネットワーク（Service Network）]：L4～L7 サービス ネットワーク名を指定します。

[VLAN ID]：VLAN ID を指定します。有効な ID の範囲は 2 ー 3967 です。定義済みの L4～L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、**[提案（Propose）]** をクリックします。

[サービス ネットワーク テンプレート]：ドロップダウンリストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、テンプレート（Templates） （425 ページ）を参照してください。

[ピアリング テンプレート（Peering Template）]：ドロップダウンリストから [service_static_route] または [service_ebgp_route] を選択します。テンプレート フィールドについての詳細は、テンプレート （Templates） （425 ページ）を参照してください。

[リバース トラフィックのネクスト ホップ IP アドレス（Next Hop IP Address for Reverse Traffic）]：リバース トラフィックのネクスト ホップ IP アドレスを指定します。

例：ツーアーム モードのロード バランサ

ツーアーム モード ロード バランサを展開するための [ルート ピアリングの作成（Create Route Peering）] ウィンドウのフィールドは、次のとおりです。アスタリスク付きのフィールドの記入が必須です。

[ピアリング名（Peering Name）]：ピアリングの名前を指定します。名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。

[展開（Deployment）]：[ツーアーム モード（Two-Arm Mode）] を選択します。

[ピアリング オプション（Peering Option）]：[静的ピアリング（Static Peering）] または [eBGP 動的ピアリング（eBGP Dynamic Peering）] を選択します。

ファースト アーム

[VRF]：ドロップダウンリストから [VRF] を選択します。

[ネットワーク タイプ（Network Type）]：[ファースト アーム（First Arm）] を選択します。

[サービス ネットワーク（Service Network）]：L4～L7 サービス ネットワーク名を指定します。

[VLAN ID]：VLAN ID を指定します。有効な ID の範囲は 2 ー 3967 です。定義済みの L4～L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、**[提案（Propose）]** をクリックします。

[サービス ネットワーク テンプレート]：ドロップダウンリストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、テンプレート（Templates） （425 ページ）を参照してください。

[ピアリング テンプレート（Peering Template）]：ドロップダウンリストから [service_static_route] または [service_ebgp_route] を選択します。テンプレート フィールドについての詳細は、テンプレート （Templates） （425 ページ）を参照してください。

セカンド アーム

[VRF]：ドロップダウンリストから [VRF] を選択します。

[ネットワーク タイプ（Network Type）]：[セカンド アーム（Second Second）] を選択します。

[サービス ネットワーク（Service Network）]：L4～L7 サービス ネットワーク名を指定します。

[VLAN ID]：VLAN ID を指定します。有効な ID の範囲は 2 ー 3967 です。定義済みの L4～L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、**[提案（Propose）]** をクリックします。

[サービス ネットワーク テンプレート]：ドロップダウンリストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、テンプレート （Templates） （425 ページ）を参照してください。

ネクスト ホップ セクション

[リバース トラフィックのネクスト ホップ IP アドレス（Next Hop IP Address for Reverse Traffic）]：リバース トラフィックのネクスト ホップ IP アドレスを指定します。

[保存（Save）] をクリックします。**[ポリシーの作成（Create Policy）]** ウィンドウが開きます。

例：ワンアーム仮想ネットワーク機能

ワンアーム モード仮想ネットワーク機能を導入するための [ルート ピアリングの作成（Create Route Peering）] ウィンドウのフィールドは、次のとおりです。アスタリスク付きのフィールドの記入が必須です。

[ピアリング名（Peering Name）]：ピアリングの名前を指定します。名前にはアルファベット、数字、アンダースコア、または文字を含めることができます。

[展開（Deployment）]：[ワンアーム モード（One-Arm Mode）] を選択します。

[ピアリング オプション（Peering Option）]：[静的ピアリング（Static Peering）] または [eBGP 動的ピアリング（eBGP Dynamic Peering）] を選択します。

ワンアーム

[VRF]：ドロップダウンリストから [VRF] を選択します。

[ネットワーク タイプ（Network Type）]：[ワンアーム（One Arm）] を選択します。

[サービス ネットワーク（Service Network）]：L4～L7 サービス ネットワーク名を指定します。

[VLAN ID]：VLAN ID を指定します。有効な ID の範囲は 2 ー 3967 です。定義済みの L4～L7 サービス ネットワーク VLAN 範囲プールから値を取得するには、[提案（Propose）] をクリックします。

[サービス ネットワーク テンプレート]：ドロップダウンリストから[Service_Network_Universal]テンプレートを選択します。テンプレートフィールドについての詳細は、「テンプレート」を参照してください。

[IPv4 ゲートウェイ/ネットマスク（IPv4 Gateway/Netmask）]：IPv4 ゲートウェイとネットマスクを指定します。

[ピアリング テンプレート（Peering Template）]：ドロップダウンリストから[service_static_route]または[service_ebgp_route]を選択します。テンプレートフィールドについての詳細は、「テンプレート」を参照してください。

[リバース トラフィックのネクスト ホップ IP アドレス（Next Hop IP Address for Reverse Traffic）]：リバース トラフィックのネクスト ホップ IP アドレスを指定します。

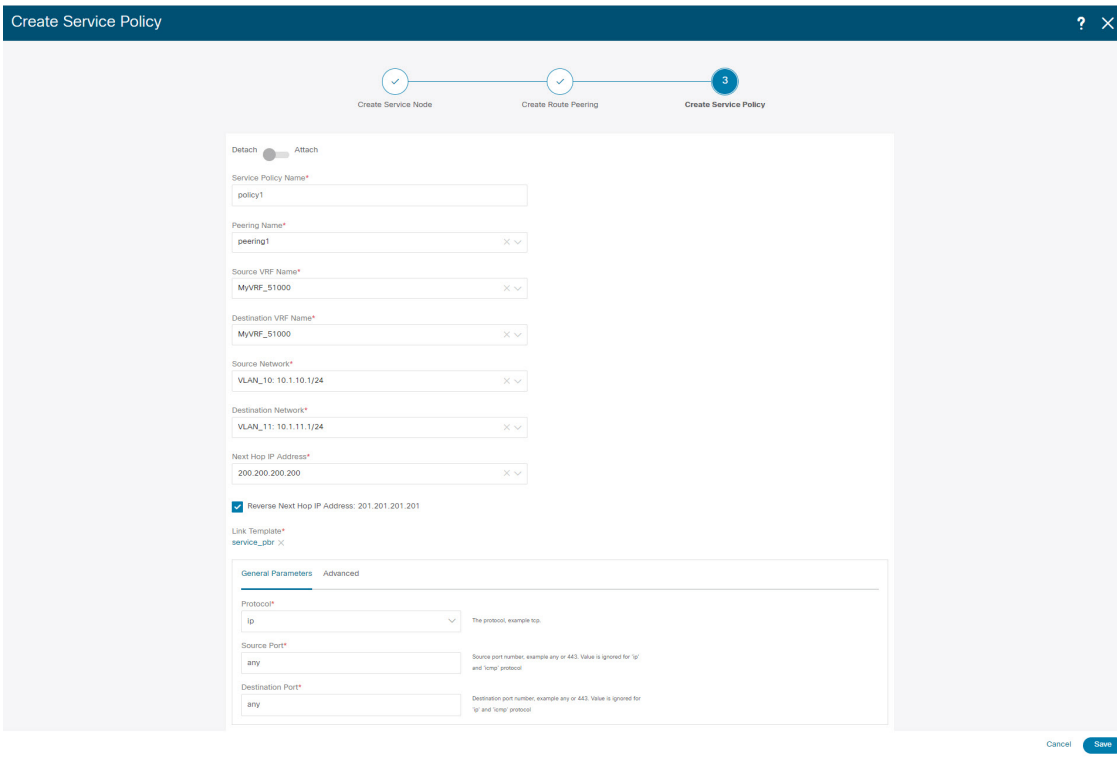
[保存（Save）]をクリックします。**[ポリシーの作成（Create Policy）]**ウィンドウが開きます。

サービスポリシーの作成

以下のいずれかのパスを使用して、**[サービス ポリシー（Service Policy）]**タブに移動します。

[LAN] > **[サービス（Services）]**

[サービス ポリシーの作成（Create Service Policy）]ウィンドウが次のように表示されます。



[サービス ポリシーの作成（Create Service Policy）]ウィンドウのフィールドは次のとおりです。アスタリスク付きのフィールドの記入が必須です。

[サービス ポリシー名（Service Policy Name）]：ポリシーの名前を指定します。

[ピアリング名（Peering Name）]：ドロップダウン リストからルート ピアリングの名前を選択します。

[送信元 VRF 名（Source VRF Name）]：ドロップダウン リストから送信元 VRF を選択します。

[宛先 VRF 名（Destination VRF Name）]：ドロップダウン リストから宛先 VR Fを選択します。

[送信元ネットワーク（Source Network）]：ドロップダウン リストから IP アドレスを選択します。

[宛先ネットワーク （Destination Network）]：ドロップダウン リストからネットワークを選択するか、任意のネットワークとサブネット情報を入力します。宛先ネットワークについても必要な情報は同じです。

[ネクスト ホップ IP アドレス（Next Hop IP Address）]：ネクストホップ IP アドレスが表示されます。

[リバース ネクスト ホップ IP アドレス（Reverse Next Hop IP Address）]：リバース ネクスト ホップ IP アドレスが表示されます。デフォルトでは、チェックボックスはオンになっています。

[リンク テンプレート（Link Template）]:ドロップダウン リストからテンプレートを選択します。テンプレート フィールドについての詳細は、テンプレート （Templates） （425 ページ）を参照してください。

一般的なパラメータ

[プロトコル（Protocol）]：ドロップダウン リストからプロトコルを選択します。オプションは、icmp、ip、tcp、および udp です。

[送信元ポート（Source Port）]: 送信元ポート番号を指定します。ip プロトコルが選択されている場合、この値は無視されます。

[宛先ポート（Destination Port）]：宛先ポート番号を指定します。ip プロトコルが選択されている場合、この値は無視されます。

[詳細設定（Advanced）]タブのオプションを使用すると、一致したトラフィックのリダイレクトをカスタマイズできます。たとえば、一致したトラフィックを PBR を使用してリダイレクトすること、一致したトラフィックにファイアウォールをバイパスさせてルーティング テーブル ルールを適用すること、一致したトラフィックをドロップすることなどを指定できます。優先順位付けのためにルート マップの一致シーケンス番号を上書きすることができます。ACL 名をカスタマイズすることもできますが、指定する ACL 名が一意であり、同じ名前が別の ACL に使用されていないことを確認してください。ルートマップの一致シーケンス番号または ACL 名を指定しない場合、指定されたリソース プールからシーケンス番号が自動的に入力され、ACL 名は 5 タプルに基づいて自動生成されます。**[詳細（Advanced）]** タブのフィールドの詳細については、テンプレート （Templates） （425 ページ） を参照してください。

[Save（保存）] をクリックします。サービス ポリシーが作成されます。

（注） サービスが使用するトップダウン プロビジョニングのサービス ネットワークを削除することはできません。サービス ポリシーで使用されている通常のネットワークを削除することもできません。

テンプレート（Templates）

サービスノードリンクテンプレート

service_link_trunk

[一般パラメータ（General Parameters）] タブ

[MTU]：インターフェイスの MTU 値を指定します。デフォルトでは、ジャンボに設定されています。

[速度（SPEED）]：インターフェイスの速度を指定します。デフォルトでは、これは[自動（Auto）]に設定されています。必要に応じて、サポートされている別の速度に変更できます。

Trunk Allowed Vlans： 'none'、 'all'、またはVLAN範囲を指定します。デフォルトでは、何も指定されていません。

[Enable BPDU Guard]：ドロップダウンリストからオプションを指定します。使用可能なオプションは、true、false、またはnoです。デフォルトでは、noが指定されています。

Enable Port Type Fast：このオプションをオンにすると、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。デフォルトでは有効になっています。

インターフェイスの有効化：このチェックボックスをオフにすると、インターフェイスが無効になります。デフォルトでは、インターフェイスはイネーブルになっています。

[詳細設定（Advanced）] タブ

[送信元インターフェイスの説明（Source Interface Description）]：送信元インターフェイスの説明を入力します。

Destination Interface Description：宛先インターフェイスの説明を入力します。

Source Interface Freeform Config：ソースインターフェイスの追加CLIを入力します。

Destination Interface Freeform Config：宛先インターフェイスの追加CLIを入力します。

service_link_port_channel_trunk

[ポート チャネル モード（Port Channel Mode）]：ドロップダウン リストからポート チャネル ポリシーのモードを選択します。デフォルトでは、activeが指定されています。

[Enable BPDU Guard]：ドロップダウンリストからオプションを指定します。使用可能なオプションは、true、false、またはnoです。

[MTU]：インターフェイスの MTU 値を指定します。デフォルトでは、ジャンボに設定されています。

Trunk Allowed Vlans： 'none'、 'all'、またはVLAN範囲を指定します。デフォルトでは、何も指定されていません。

Port Channel Description：ポートチャネルの説明を入力します。

自由形式の設定：必要な自由形式の設定CLIを指定します。

Enable Port Type Fast：このオプションをオンにすると、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。デフォルトでは有効になっています。

ポートチャネルを有効にする：ポートチャネルを有効にするには、このオプションをオンにします。デフォルトでは有効になっています。

service_link_vpc

このテンプレートには指定可能なパラメータがありません。

ルートピアリングサービスネットワークテンプレート

Service_Network_Universal

[一般パラメータ（General Parameters）] タブ

IPv4ゲートウェイ/ネットマスク：サービスネットワークのゲートウェイIPアドレスとマスクを指定します。

IPv6 Gateway / Prefix：サービスネットワークのゲートウェイIPv6アドレスとプレフィックスを指定します。

Vlan Name：VLANの名前を指定します。

[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。

[詳細設定（Advanced）] タブ

[ルーティングタグ（Routing Tag）]：ルーティングタグを指定します。有効値の範囲は、0 ～ 4294967295 です。

ルートピアリングテンプレート

service_static_route

[スタティックルート（Static Routes）]フィールドにスタティックルートを入力します。回線ごとに1つのスタティックルートを入力できます。

service_ebgp_route

[一般パラメータ（General Parameters）] タブ

[ネイバー IPv4（Neighbor IPv4）]：ネイバーの IPv4 アドレスを指定します。

Loopback IP：ループバックのIPアドレスを指定します。

[詳細設定（Advanced）] タブ

Neighbor IPv6：ネイバーのIPv6アドレスを指定します。

Loopback IPv6：ループバックのIPv6アドレスを指定します。

Route-Map TAG：インターフェイスIDに関連付けられているルートマップタグを指定します。

[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。

ローカルASN：システムASNを上書きするローカルASNを指定します。

[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有効にします。

インターフェイスの有効化：インターフェイスを無効にするには、このオプションをクリアします。デフォルトでは、インターフェイスはイネーブルになっています。

サービスポリシーテンプレート

service_pbr

[一般パラメータ（General Parameters）] タブ

[プロトコル（Protocol）]：ドロップダウン リストからプロトコルを選択します。オプションは、icmp、ip、tcp、および udp です。

[送信元ポート（Source port）]: 送信元ポート番号を指定します。ipプロトコルが選択されている場合、この値は無視されます。

[宛先ポート（Destination port）]：宛先ポート番号を指定します。ip プロトコルが選択されている場合、この値は無視されます。

[詳細設定（Advanced）] タブ

[ルート マップ アクション（Route Map Action）]：ドロップダウン リストからアクションを選択します。オプションはpermitまたはdenyです。[許可（permit）]を選択すると、一致したトラフィックはネクストホップオプションと定義されたポリシーに基づいてリダイレクトされます。[拒否（deny）]を選択すると、トラフィックはルーティングテーブルルールに基づいてルーティングされます。

[Next Hop Option]：ネクストホップのオプションを指定します。オプションは、none、drop-on-fail、およびdropです。noneを選択すると、一致したトラフィックは定義されたPBRルールに基づいてリダイレクトされます。drop-on-failを選択すると、指定したネクストホップが到達不能な場合、一致したトラフィックはドロップされます。ドロップを選択すると、一致したトラフィックがドロップされます。

ACL Name：生成されたアクセスコントロールリスト（ACL）の名前を指定します。指定しない場合、これは自動生成されます。

反転トラフィックのACL名：反転トラフィック用に生成されるACLの名前を指定します。指定しない場合、これは自動生成されます。

Route map match number：ルートマップの一致番号を指定します。有効な値の範囲は 1 ～ 65535 です。指定しない場合、ルートマップの一致シーケンス番号が事前定義されたリソースプールから取得されます。この番号は、ACLの名前に関連付けられます。

リバーストラフィックのルートマップ一致番号：リバーストラフィックのルートマップ一致番号を指定します。有効な値の範囲は 1 ～ 65535 です。指定しない場合、ルートマップの一致シーケンス番号が事前定義されたリソースプールから取得されます。この番号は、リバーストラフィック用に生成されたACLの名前に関連付けられます。

また、特定の要件に基づいてテンプレートをカスタマイズすることもできます。

サービス ノードの削除

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からサービス ノードを削除するには、以下の手順を実行します。

手順

テーブルからサービスノードを選択し、**[アクション (Actions)] > [削除 (Delete)]** をクリックします。

（注） 削除する必要があるサービス ノードにルート ピアリングまたはサービス ポリシーが関連付けられていないことを確認します。サービス ノードに関連付けられているサービス ポリシーまたはルート ピアリングがある場合、サービス ノードを削除する前にサービス ノードに関連付けられているルート ピアリングまたはサービス ポリシーを削除する必要があることを示す警告が出され、削除がブロックされます。

サービス ノードの編集

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からサービス ノードを編集するには、次の手順を実行します。

手順

ステップ 1 テーブルからサービスノードを選択し、**[アクション（Actions）] > [編集（Edit）]** をクリックします。

ステップ 2 **[サービス ノードの編集（Edit Service Node）]** ウィンドウが表示されます。

必要な変更を行って、[保存（Save）] をクリックします。

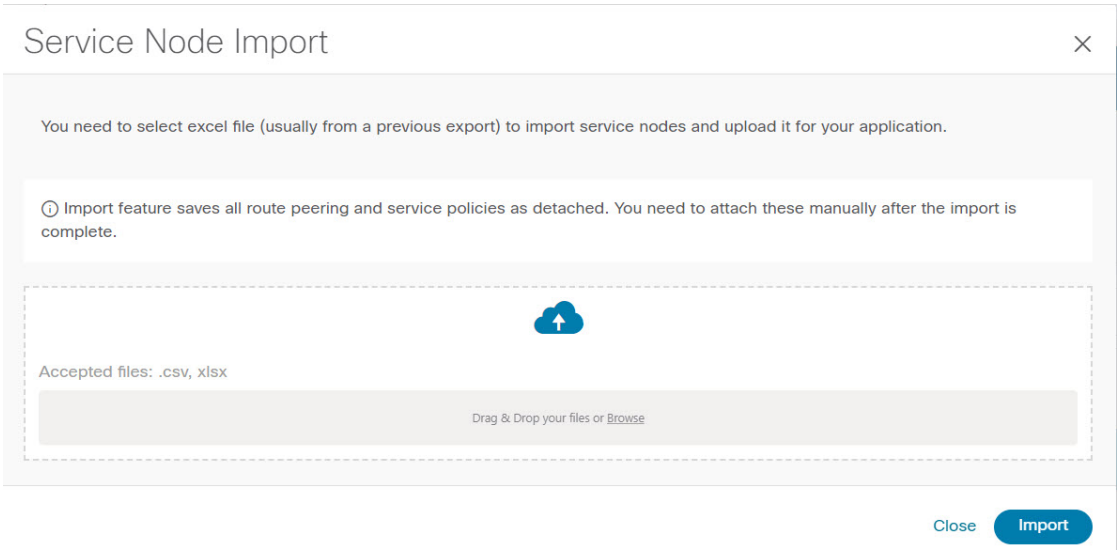
サービスノードの更新

[サービスノード（Service Nodes）] ウィンドウに表示される L4～L7 サービスノードのリストを更新するには、**[更新（Refresh）]** アイコン をクリックします。

サービス ノードのインポート

サービス ノードを Excel ファイルからインポートするには、**[アクション（Actions）] > [インポート（Import）]** をクリックします（**[サービス ノード（Service Nodes）]** ウィンドウ）。**[サービス ノードのインポート（Servie Node Import）]** ウィンドウが表示されます。

[ブラウザ（Browser）] をクリックするか、ファイルとドラッグアンドドロップし、**[インポート（Import）]** ボタン（**[サービス ノードのインポート（Service Node Import）]** ウィンドウ）をクリックして、サービス ノードに関する情報をインポートします。



また、**[アクション（Actions）] > [インポート（Import）]** をクリックして、サービス ノードに関するデータを Excel ファイルからインポートして、サービス ノードレベルのデータを復元することもできます。

L4～L7 サービス ノードのエクスポート

L4～L7 サービス ノードのレベルでデータをバックアップするには、**[アクション（Actions）] > [エクスポート（Export）]** オプションをクリックして、L4～L7 サービス ノードに関するデータを Excel ファイルにエクスポートします。すべてのサービス ノード、それぞれのルート ピアリング、および L4～L7 サービス ポリシーに関するデータがエクスポートされます。

特定の L4～L7 サービスノードのデータをエクスポートするには、ノードを選択し、**[アクション（Actions）] > [エクスポート（Export）]** をクリックします。

サービス ノードを Excel ファイルとしてエクスポートするには、テーブルから L4～L7 サービス ノードを選択し、**[アクション（Actions）] > [エクスポート（Export）]** をクリックします。**[サービス ノードのエクスポート（Service Node Export）]** ウィンドウで **[エクスポート（Export）]** をクリックして、L4～L7 サービス ノードに関する情報をエクスポートします。

監査履歴の表示

選択した L4～L7 サービス ポリシーまたはルート ピアリングに関連するスイッチおよびネットワークの監査履歴を表示するには、**[監査履歴（Audit History）]** タブ（**[サービス（Services）]** ウィンドウ）をクリックします。

[監査履歴（Audit History）] ウィンドウの [監査ログ（Audit Logs）] テーブルには、実行されたすべてのアクションに関する情報が表示されます。監査ログは、次のアクションが実行されたときに生成されます。

- L4～L7 サービス ノード、ルート ピアリング、および L4～L7 サービス ポリシーの作成
- L4～L7 サービス ノード、ルート ピアリング、および L4～L7 サービス ポリシーの削除
- L4～L7 サービス ノード、ルート ピアリング、および L4～L7 サービス ポリシーの更新
- ルート ピアリングの接続と切断、および L4～L7 サービス ポリシー
- ルート ピアリングと L4～L7 サービス ポリシーの展開

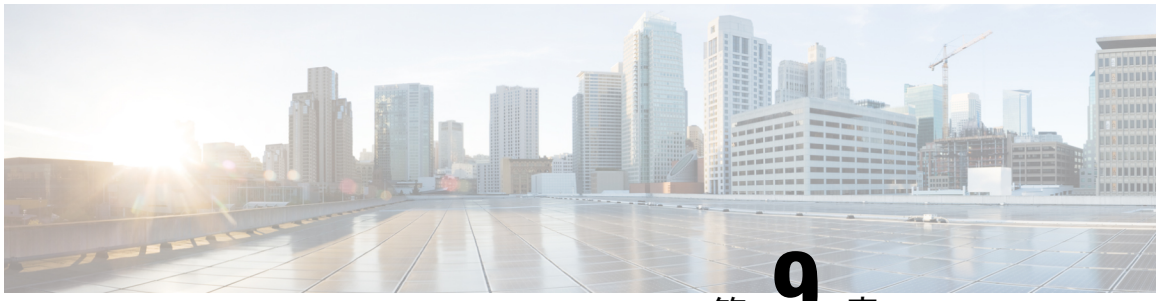
この監査ログは、アクションを実行したユーザの名前、ユーザのロール、実行されたアクション、アクションが実行されたエンティティ、アクションの詳細、ステータス、およびアクションが実行されました。

ユーザ名、ユーザ ロール、実行されたアクション、エンティティ、詳細、ステータス、実行時間などの情報が表示されます。監査ログを削除するには、**[アクション（Actions）] > [監査履歴の消去（Purge Audit History）]** をクリックし、**[消去（Purge）] > [確認（Confirm）]** をクリックします。

古い監査レポートを削除するには、**[アクション（Action）] > [変更履歴の消去（Purge Audit History）]** をクリックし、最大保持日を指定して、削除を確認します。監査ログエントリを削除できるのは管理者ロールを持つユーザーのみであることに注意してください。

第 II 部

仮想的な管理



第 9 章

仮想インフラストラクチャ マネージャ

仮想インフラストラクチャ マネージャ

UI パス：**[仮想管理（Virtual Management）]>[仮想インフラストラクチャ マネージャ（Virtual Infrastructure Manager）]**

（注） Cisco Nexus Dashboard ファブリックコントローラの仮想マシンのネットワーク可視化機能が有効になっていることを確認します。

1. **[設定（Settings）]>[機能管理（Feature Management）]** を選択し、次のチェックボックスをオンにします。
   - Kubernetes ビジュアライザ
   - VMM ビジュアライザ
   - OpenStack ビジュアライザ
2. [Apply] をクリックします。

次の表では、[仮想インフラストラクチャ マネージャ（Virtual Infrastructure Manager）] 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。

フィールド	説明
[サーバ（Server）]	サーバー IP アドレスを指定します。

フィールド	説明
タイプ	次のいずれかのインスタンスのタイプを指定します。 • vCenter • Kubernetesクラスタ • OpenStack クラスタ
管理対象（Managed）	管理対象または管理対象外のクラスタのステータスを指定します。
ステータス	追加されたクラスタの状態を指定します。
ユーザー（User）	クラスタを作成したユーザーを指定します。
最終更新時刻	クラスタの最終更新時刻を指定します。

（注） **[更新（Refresh）]**アイコンをクリックして、仮想インフラストラクチャ マネージャ テーブルを更新します。

次の表では、[アクション（Actions）] メニューのドロップダウン リストで、[仮想インフラストラクチャ マネージャ（Virtual Infrastracture Manager）] 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
インスタンスの追加	**[アクション（Actions）]** ドロップダウンリストから **[インスタンスの追加（Add Instance）]** を選択します。詳細については、「インスタンスの追加」を参照してください。 （注） ルート上で同じ IP アドレスを設定していることを確認します。「ルート IP アドレスの設定」を参照してください。
インスタンスの編集	編集するインスタンスを選択します。**[アクション（Actions）]** ドロップダウンリストから **[インスタンスの編集（Edit Instance）]** 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。**[キャンセル（Cancel）]** をクリックして、変更を破棄します。
インスタンスの削除	削除する1つ以上の必要なインスタンスを選択します。**[アクション（Actions）]** ドロップダウンリストから、**[削除（Delete）]** を選択します。[確認（Confirm）] をクリックしてインスタンスを削除します。**[キャンセル（Cancel）]** をクリックしてこの削除を破棄します。

アクション項目	説明
インスタンスの再検出	再検出する1つ以上の必要なインスタンスを選択します。**[アクション（Actions）]** ドロップダウンリストから、**[インスタンスの再検出（Rediscover Instance(s)）]** を選択します。確認メッセージが表示されます。

詳細については、次を参照してください。

Cisco UCS B シリーズ ブレードサーバーのサポート

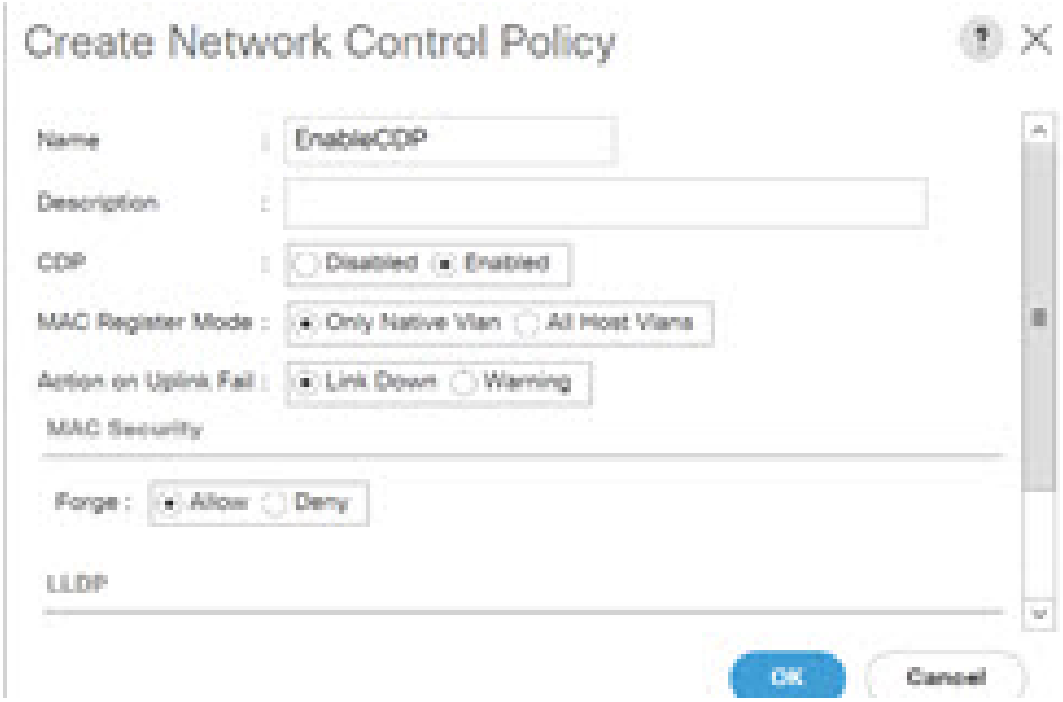
NDFC は、ファブリックインターコネクトの背後にある UCS タイプ B （シャーシ UCS）で実行されているホストをサポートします。この機能を使用するには、Cisco UCSM で vNIC の CDP を有効にする必要があります。

（注） デフォルトでは、CDP は Cisco UCSM で無効になっています。

参考のために、VMM-A と VMM-B の 2 つの VMM について考えてみましょう。Cisco UCS UCS B シリーズ ブレードサーバーの検出後、トポロジに青色の VMM-A と VMM-B がファブリック インターコネクト ノードであることが表示されます。トポロジの例を下図に示します。

UCSM で CDP を有効にするには、次の手順を使用して新しいネットワーク制御ポリシーを作成する必要があります。

1. USCM で、**[LAN]** を選択し、ポリシーを展開します。
2. **[ネットワーク制御ポリシー（Network Control Policies）]** を右クリックして、新しいポリシーを作成します。
3. [名前（Name）] フィールド、にポリシーの名前を **EnableCDP** と入力します。
4. CDP の**有効な**オプションを選択します。



5. **[OK]** をクリックしてポリシーを作成します。

新しいポリシーを ESX NIC に適用するには、次の手順を実行します。

- 更新された vNIC テンプレートを使用している場合は、ESXi vNIC の各 vNIC テンプレートを選択し、[ネットワーク制御ポリシー] ドロップダウンリストから EnableCDP ポリシーを適用します。
- vNIC テンプレートを使用していない場合は、更新されたサービス プロファイル テンプレートを使用します。各サービス プロファイル テンプレートに EnableCDP ポリシーを適用します。
- 1 回限りのサービスプロファイルを使用している場合（つまり、各サーバーが独自のサービスプロファイルを使用している場合）、すべてのサービスプロファイルに移動し、すべての vNIC で EnableCDP ポリシーを有効にする必要があります。

Cisco UCSM の詳細については、『Cisco UCSM ネットワーク管理ガイド』を参照してください。

ルート IP アドレスの設定

IP アドレスを vCenter に追加する前に、Cisco Nexus ダッシュボードで同じ IP アドレスを設定する必要があります。

Cisco Nexus ダッシュボードでルートを設定するには、次の手順を実行します。

手順

ステップ 1 **[インフラストラクチャ（Infrastructure）]** > **[クラスタ設定（Cluster Configuration）]** を選択します。

ステップ 2 **[全般（General）]** タブの **[ルート（Routes）]** カードで、**[編集（Edit）]** アイコンをクリックします。

[ルート（Routes）] ウィンドウが表示されます。

ステップ 3 IP アドレスを設定するには、**[管理ネットワーク ルートの追加（Add Management Network Routes）]** をクリックし、必要な IP アドレスを入力して、**[チェック（check）]** アイコンをクリックします。

ステップ 4 [保存（Save）] をクリックします。

ルート設定は、次の 2 つのシナリオによって管理されます。

1. アプリケーションサーバーである vCenter の場合、通常は管理ネットワーク経由で到達可能です。
2. vCenter によって管理される ESXi サーバーと、K8s インスタンスや OpenStack インスタンスをホストするベアメタルサーバーは、ファブリックネットワークに直接接続されます。したがって、それらはデータネットワークを介して到達可能です。

vCenter の可視化の追加

[仮想的な管理（Virtual Management）] > **[仮想インフラストラクチャ マネージャ（Virtual Infrastructure Manager）]** に表示される **[アクション（Actions）]** メニューのドロップダウンリストで、さまざまなアクションを実行できます。

手順

ステップ 1 **[アクション（Actions）]** **[インスタンスの追加（Add Instance）]** を選択します。

[インスタンスの追加（Add Instance）] ウィンドウが表示されます。

ステップ 2 [タイプの選択（Select Type）]ドロップダウン リストから **[vCenter]** を選択します。

必要な IP アドレスまたはドメイン名とパスワードをそれぞれのフィールドに入力します。

ステップ 3 [Add] をクリックします。

追加された vCenter クラスタは、**[仮想インフラストラクチャ マネージャ（Virtual Infrastructure Manager）]** ウィンドウで表示できます。

ステップ 4 インスタンスを編集するには、必要な vCenter を選択して、**[アクション（Actions）]>[インスタンスの編集（Edit Instance）]** を選択して、**[保存（Save）]** をクリックします。

選択済みの vCenter クラスタのパスワードをアップデートし、ステータスを「管理対象」または「管理対象外」に変更できます。

（注） 管理対象外ステータスの vCenter クラスタの場合、ダッシュボードでトポロジと vCenter クラスタの詳細を表示できません。

ステップ 5 1 つ以上の vCenter クラスタを削除するには、必要な vCenter を選択し、**[アクション（Actions）] > [インスタンスの削除（Delete Instance(s)）]** を選択して、**[変更の確認（Confirm changes）]** をクリックします。

（注） クラスタを削除すると、すべてのデータが削除されます。クラスタは、トポロジビューからも削除されます。

ステップ 6 1 つ以上の vCenter クラスタを再検出するには、必要な vCenter を選択して、**[アクション（Actions）] > [インスタンスの再検出（Rediscover Instance(s)）]** を選択します。

確認メッセージが表示されます。

Kubernetesクラスタ

（注） Cisco Nexusダッシュボード ファブリック コントローラ の K8s クラスタのネットワーク可視化機能が有効になっていることを確認します。

[設定（Settings）] > [機能管理（Feature Management）]を選択し、**[Kubernetes ビジュアライザ（Kubernetes Visualizer）]** チェックボックスを選択して、**[適用（Apply）]** をクリックします。

追加された Kubernetes Visualizer の詳細をダッシュボードで表示できます。[ダッシュボード（Dashboard）] > [Kubernetes ポッド（Kubernetes Pods）] に移動します >

NDFC で LLDP を有効にするには、**[設定（Settings）] > [サーバー（Server）] > [設定（Settings）] > [検出（Discovery）]**を選択します。**[LLDP を使用したネイバーリンクディスカバリを有効または無効にします（enable / disable neighbor link discovery using LLDP）]** チェックボックスを選択します。

（注） LLDP は、ベアメタル Kubernetes クラスタにのみ適用されます。

- クラスタノードが接続されているすべてのファブリックスイッチで LLDP 機能が有効になっていることを確認します。（スイッチはスパインまたはリーフスイッチの場合があります）。
- Kubernetes クラスタで、すべてのベアメタルノードで LLDP および SNMP サービスが有効になっていることを確認します。
- Cisco UCS が Intel NIC を使用している場合、FW-LLDP が原因で LLDP ネイバーシップの確立に失敗します。

  回避策：Intel® イーサネットコントローラ（800 および 700 シリーズなど）に基づく選択されたデバイスでは、ファームウェアで実行される LLDP エージェントを無効にします。LLDP を無効にするには、次のコマンドを使用します。

  echo 'lldp stop' > /sys/kernel/debug/i40e/<bus.dev.fn>/command

  特定のインターフェイスの bus.dev.fn を見つけるには、次のコマンドを実行し、インターフェイスに関連付けられた ID を選択します。ID は、以下のサンプル出力で強調表示されています。

```
[ucs1-lnx1]# dmesg | grep enp6s0 [ 12.609679] IPv6: ADDRCONF(NETDEV_UP): enp6s0:
link is not ready [ 12.612287] enic 0000:06:00.0 enp6s0: Link UP [ 12.612646] IPv6:
ADDRCONF(NETDEV_UP): enp6s0: link is not ready [ 12.612665] IPv6:
ADDRCONF(NETDEV_CHANGE): enp6s0: link becomes ready[ucs1-lnx1]#
```

（注） LLDP機能は、ベアメタルクラスタノードが接続されているファブリックスイッチで有効になっています。また、ボーダーゲートウェイスイッチに接続することもできます。

クラスタが検出された後にKubernetesクラスタが接続されているファブリックが検出された場合、トポロジを正しく表示するためにクラスタを再検出する必要があります。

LLDP の設定後にベアメタルベースの Kubernetes クラスタが検出された場合、トポロジを正しく表示するためにベアメタルクラスタを再検出する必要があります。

特定のインターフェイスの bus.dev.fn を見つけるには、次のコマンドを実行し、インターフェイスに関連付けられた ID を選択します。ID は、以下のサンプル出力で強調表示されています。

（注） VM ベースの Kubernetes クラスタを検出または視覚化する場合、最初に、検出される Kubernetes クラスタをホストする VM を管理している vCenter クラスタをオンボードする必要があります。これがないと、Kubernetes クラスタの検出が失敗します。

ルート IP アドレスの設定

Kubernetes クラスタに IP アドレスを追加する前に、Cisco Nexus Dashboard で同じ IP アドレスを設定する必要があります。

Cisco Nexus ダッシュボードでルートを設定するには、次の手順を実行します。

手順

ステップ 1 **[インフラストラクチャ（Infrastructure）]** > **[クラスタ設定（Cluster Configuration）]** を選択します。

ステップ 2 **[全般（General）]** タブの **[ルート（Routes）]** カードで、**[編集（Edit）]** アイコンをクリックします。

[ルート（Routes）] ウィンドウが表示されます。

ステップ 3 IP アドレスを設定するには、**[管理ネットワーク ルートの追加（Add Management Network Routes）]** をクリックし、必要な IP アドレスを入力して、**[チェック（check）]** アイコンをクリックします。

ステップ 4 [保存（Save）] をクリックします。

Kubernetes クラスタの追加

[仮想的な管理（Virtual Management）] > **[仮想インフラストラクチャ マネージャ（Virtual Infrastructure Manager）]**に表示される **[アクション（Actions）]** メニューのドロップダウンリストで、さまざまなアクションを実行できます。

（注） ルート上で同じ IP アドレスを設定していることを確認します。「ルート IP アドレスの設定」を参照してください。

手順

ステップ 1 **[アクション（Actions）]** > **[インスタンスの追加（Add Instance）]**を選択します。

[インスタンスの追加（Add Instance）] ウィンドウが表示されます。

ステップ 2 [タイプの選択（Select Type）] ドロップダウンリストから [Kubernetes クラスタ] を選択します。

ステップ 3 適切なフィールドに **[クラスタ IP アドレス（Cluster IP address）]**、**[ユーザー名（Username）]** を入力します。

ステップ 4 **[CSR の取得（Fetch CSR）]** をクリックして、Kubernetes ビジュアライザ アプリケーションから証明書署名要求（CSR）を取得します。

（注） このオプションは、有効なクラスタ IP アドレスとユーザー名を入力するまで無効になっています。

SSL 証明書を取得していない場合にのみ、**[CSR の取得（Fetch CSR）]** を使用してください。有効な証明書がすでにある場合は、CSR を取得する必要はありません。

[CSR のダウンロード（Download CSR）] をクリックします。証明書の詳細は、ディレクトリ内の **<username>.csr** に保存されます。CSR の内容をファイル **kubereader.csr** に貼り付けます。ここで、kubereader は、Kubernetes に接続する API クライアントのユーザー名です。

CSR ファイル名は命名規則 <<*username*> > に従う必要があります。

（注） 証明書は Kubernetes クラスタで生成されるため、証明書を生成するには Kubernetes 管理者権限が必要です。

付属文書 （445 ページ） を参照して証明書 **genk8clientcert.sh** を生成します。

ステップ 5 Kubernetes クラスタコントローラノードにログインします。

証明書を生成するには、管理者権限が必要です。

ステップ 6 genk8clientcert.sh と kubereader.csr を NDFC サーバーの場所から Kubernetes クラスタコントローラノードにコピーします。

「vnc カットアンドペースト」操作を実行して、すべての文字が正しくコピーされるようにします。

ステップ 7 **genk8sclientcert.sh** スクリプトを使用して、ユーザー名の CSR を生成します。

(k8s-root)# **./genk8sclientcert.sh kubereader 10.x.x.x** ここで、

- kubereader は、Kubernetes に接続する API クライアントのユーザー名です。（手順 3 で定義）。
- 10.x.x.x は NDFC サーバーの IP アドレスです。

同じ場所に 2 つの新しい証明書が生成されます。

- k8s_cluster_ca.crt
- *username_dcnm-IP.crt*

  例：kubereader_10.xxxcrt （ここで、kubereader はユーザー名で、10.x.x.x は NDFC IP アドレスです）

```
dcnm(root)# cat k8s_cluster_ca.crt
```

ステップ 8 cat コマンドを使用して、これら 2 つのファイルから証明書を抽出します。

```
dcnm(root)# cat kubereader_10.x.x.x.crt
dcnm(root)# cat k8s_cluster_ca.crt
```

Cisco NDFC に Kubernetes クラスタを追加するユーザーに、これらの 2 つの証明書を提供します。

ステップ 9 kubereader_10.x.x.x.crt の内容を **[クライアント証明書（Client Certificate）]**フィールドにコピーします。

（注） 「vnc カットアンドペースト」操作を実行して、すべての文字が正しくコピーされるようにします。

ステップ 10 k8s_cluster_ca.crt の内容を **[クライアント証明書（Client Certificate）]** クライアント証明書フィールドにコピーします。

（注） 「vnc カットアンドペースト」操作を実行して、すべての文字が正しくコピーされるようにします。

ステップ 11 [Add] をクリックします。

追加された Kubernetes クラスタは、**[仮想インフラストラクチャ マネージャ（Virtual Infrastructure Manager）]** ウィンドウで表示できます。

（注） ダッシュボードとトポロジウィンドウで、追加された Kubernetes クラスタの詳細を表示できます。**[ダッシュボード（Dashboard）]** > **[Kubernetes ポッド（Kubernetes Pods）]**に移動します。

ステップ 12 Kubernetes クラスタを編集するには、必要なクラスタを選択し、**[アクション（Actions）]** > **[インスタンスの編集（Edit Instance）]**を選択し、[編集（Edit）] をクリックして値を適切に変更します。クラスタとクライアントの証明書を更新できます。Kubernetes クラスタの管理ステー

タスを更新することもできます。管理ステータスの更新を選択した場合、証明書は必要ありません。

（注） 非管理ステータスのkubernetesクラスタの場合、ダッシュボードでトポロジとKubernetesクラスタの詳細を表示できません。

ステップ 13 **[保存（Save）]** をクリックして変更内容を保存するか、または **[キャンセル（Cancel）]** をクリックして変更内容を取り消します。

ステップ 14 1 つ以上の Kubernetes クラスタを削除するには、必要なクラスタを選択し、**[アクション（Actions）] > [インスタンスの削除（Delete Instance(s)）]**の順に選択してクラスタを削除します。

（注） クラスタを削除すると、すべてのデータが削除されます。クラスタは、トポロジビューからも削除されます。

ステップ 15 **[確認（Confirm）]** をクリックしてクラスタを削除します。

ステップ 16 1 つ以上の Kubernetes クラスタを再検出するには、必要な Kubernetes クラスタを選択し、**[アクション（Actions）] > [インスタンスの再検出（Rediscover Instance(s)）]**の順に選択します。

確認メッセージが表示されます。

OpenStack クラスタ

（注） これは、「Nexus ダッシュボード ファブリック コントローラ、リリース 12.0.2a」のプレビュー機能です。ラボセットアップでのみ、ベータ版としてマークされたこの機能を使用することをお勧めします。実稼働環境でこれらのフィーチャを使用しないでください。

（注）

- Cisco Nexus ダッシュ―ボード ファブリック コントローラの Openstack クラスタのネットワーク可視化機能が有効になっていることを確認します。**[設定（Settings）] > [機能管理（Feature Management）]** を選択し、**[Openstack ビジュアライザ（Openstack Visualizer）]** チェックボックスをオンにして、**[適用（Apply）]** をクリックします。
- openstack クラスタを追加するには、vCenter クラスタまたは Kubernetes クラスタ機能を有効にする必要があります。

- NDFC で LLDP を有効にするには、[Web UI] を選択し、**[設定（Settings ）] > [サーバー設定（Server Settings）] > [検出（Discovery）]** を選択します。**[LLDP を使用したネイバーリ**

ンクディスカバリを有効または無効にします（enable / disable neighbor link discovery using LLDP）] チェックボックスを選択します。

- OpenStack クラスタで、すべてのベアメタルノードで LLDP サービスが有効になっていることを確認します。LLDP機能は、ベアメタルクラスタノードが接続されているファブリックスイッチで有効になっています。また、ボーダーゲートウェイスイッチに接続することもできます。
- Intel® イーサネットコントローラに基づく、選択されたデバイス（例：800 および 700 シリーズ）については、ファームウェアで実行される Link Layer Discovery Protocol（LLDP）エージェントを無効にします。同じことを行うには、次のコマンドを使用します。

```
# echo 'lldp stop'>/sys/kernel/debug/i40e/bus.dev.fn/command
```

- 特定のインターフェイスの *bus.dev.fn* を見つけるには、次のコマンドを実行し、インターフェイスに関連付けられた ID を選択します。ID は、以下の出力で強調表示されています。

```
# dmesg | grep eth0
[ 8.269557] enic 0000:6a:00.0 eno5: renamed from eth0
[ 8.436639] i40e 0000:18:00.0 eth0: NIC Link is Up, 40 Gbps Full Duplex, Flow Control:
 None
[ 10.968240] i40e 0000:18:00.0 ens1f0: renamed from eth0
[ 11.498491] ixgbe 0000:01:00.1 eno2: renamed from eth0
```

ルート IP アドレスの設定

Openstack ビジュアライザに IP アドレスを追加する前に、Cisco Nexus ダッシュボードで同じ IP アドレスを設定する必要があります。

Cisco Nexus ダッシュボードでルートを設定するには、次の手順を実行します。

手順

ステップ 1 **[インフラストラクチャ（Infrastructure）]** > **[クラスタ設定（Cluster Configuration）]** を選択します。

ステップ 2 **[全般（General）]** タブの **[ルート（Routes）]** カードで、**[編集（Edit）]** アイコンをクリックします。

[ルート（Routes）] ウィンドウが表示されます。

ステップ 3 IP アドレスを設定するには、**[管理ネットワーク ルートの追加（Add Management Network Routes）]** をクリックし、必要な IP アドレスを入力して、**[チェック（check）]** アイコンをクリックします。

ステップ 4 [保存（Save）] をクリックします。

OpenStack クラスタでの AMQP エンドポイントの設定

- RabbitMQ 通知（oslo.messaging）バス設定は、OpenStack クラスタで完了する必要があります。

  OpenStack Nova サービスで以下の設定変更を行います。パラメータ値を次のように置き換えます。Nova 構成ファイルは次のパスにあります。

  `/etc/nova/nova.conf`

```
[notifications]
notify_on_state_change=vm_and_task_state
default_level=INFO
notification_format=both

[oslo_messaging_notifications]
driver = messagingv2
transport_url=rabbit://guest:guest@X.X.X.X:5672/
topics=notifications
retry=-1
```

（注）

- **transport_url** は、ポート 5672 に IP X.X.X.X を持つサーバーでホストされている RabbitMQ エンドポイントのアドレスです。適切なサーバーの IP アドレスに置き換えます。
- **guest:guest** は、エンドポイントに接続するためのユーザー名とパスワードです。

  また、モニタリング アプリケーション クライアントがポートに接続して通知データを読み取れるように、適切な「iptables」ルールを設定してポート 5672 を開きます。

- OpenStack プラグインは、OpenStack クラスタからリアルタイムの変更通知を受信して処理し、トポロジの説明情報を更新します。リアルタイムの変更通知は、VM の状態の変更（VM の追加、削除、または更新など）およびネットワークの状態の変更（VM と仮想スイッチ間のリンクのシャットダウンなど）に関連しています。
- クラスタノードの電源を入れると、トポロジビューに反映されます。対応するノードがクラスタビューに追加されます。同様に、クラスタノードの電源を切ると、トポロジビューに反映されます。対応するノードがクラスタビューから削除されます。
- OpenStack クラスタ内のノード（コントローラ、コンピューティング、またはストレージ）の追加または削除は、トポロジクラスタビューの NDFC に自動的に反映されます。

付属文書

証明書が正常に生成されると、次のメッセージが表示されます。

```
#!/usr/bin/bash
###############################################################
# Title: Script to provision the client CSR and generat the #
#        the client SSL certificate.                          #
###############################################################

# Create CSR resource template.
function create_csr_resource() {
    K8SUSER=$1
    DCNM=$2
    FILE=${K8SUSER}_${DCNM}_csr_res.yaml
    echo "
apiVersion: certificates.k8s.io/v1
kind: CertificateSigningRequest
metadata:
  name: ${K8SUSER}_${DCNM}csr
spec:
  groups:
  - system:authenticated
  request: ${BASE64_CSR}
  signerName: kubernetes.io/kube-apiserver-client
  usages:
  - digital signature
  - key encipherment
  - client auth" > $FILE
}

# Create CLUSTER ROLE resource template
function create_cluster_role() {
    K8SUSER=$1
    DCNM=$2
    FILE=${K8SUSER}_${DCNM}_cluster_role_res.yaml
    echo "
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: clustrole_${K8SUSER}_${DCNM}
rules:
- apiGroups: [\"\"]
  resources: ["nodes", "namespaces", "pods", "services"]
  verbs: ["get", "list", "watch"]" > $FILE
}

# Create CLUSTER ROLE BINDING template
function create_cluster_role_binding() {
    K8SUSER=$1
    DCNM=$2
    FILE=${K8SUSER}_${DCNM}_cluster_rolebinding_res.yaml
    echo "
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: clustrolebind_${K8SUSER}_${DCNM}
roleRef:
  kind: ClusterRole
  name: clustrole_${K8SUSER}_${DCNM}
  apiGroup: rbac.authorization.k8s.io
subjects:
- kind: User
  name: ${K8SUSER}
  apiGroup: rbac.authorization.k8s.io" > $FILE
}

function valid_ip() {
```

```
    local  ip=$1
    local  stat=1

    if [[ $ip =~ ^[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}$ ]]; then
        OIFS=$IFS
        IFS='.'
        ip=($ip)
        IFS=$OIFS
        [[ ${ip[0]} -le 255 && ${ip[1]} -le 255 \
            && ${ip[2]} -le 255 && ${ip[3]} -le 255 ]]
        stat=$?
    fi
    return $stat
}

# Start of the script
if [ "$#" -ne 2 ]; then
    echo "Please provide the username and IP of the DCNM"
    echo
    exit 1
else

    # Check if user have required K8s privileges
    LINUX_USER=$(whoami)
    K8S_CONF_PATH=""
    echo
    echo "Hello ${LINUX_USER}! I am going to help you generate K8s cluster CA and K8s
client certificate."

    if [ ${LINUX_USER} == "root" ] ; then
        # You are root
        if [ ! -d "/root/.kube" ] ; then
            echo
            echo "Directory /root/.kube does not exists."
            echo "User ${LINUX_USER} does not have required K8s privileges"
            echo "Please make sure you are logged into K8s cluster's master node"
            echo
            exit 1
        else
            K8S_CONF_PATH=/${LINUX_USER}/.kube/config
        fi
    else
        # You are not root
        if [ ! -d "/home/${LINUX_USER}/.kube" ] ; then
            echo
            echo "Directory /home/${LINUX_USER}/.kube does not exists."
            echo "User ${LINUX_USER} does not have required K8s privileges"
            echo "Please make sure you are logged into K8s cluster's master node"
            echo
            exit 1
        else
            K8S_CONF_PATH=/home/${LINUX_USER}/.kube/config
        fi
    fi

    # Check if K8s config file exist
    if [ ! -f ${K8S_CONF_PATH} ]; then
        echo
        echo "${K8S_CONF_PATH} file does not exist"
        echo "K8s CA certificate can not be exported"
        echo "Please make sure you are logged into K8s cluster's master node"
        echo
        exit 1
    fi
```

```
K8SUSER=$1
DCNM=$2
K8S_CA_CRT="k8s_cluster_ca.crt"

# Validate the IP address
if valid_ip $DCNM; then
    echo -e
else
    echo "${2} is not a valid IP address"
    echo
    exit 1
fi

# Validate the CSR file format
if [ ${K8SUSER: -4} == ".csr" ]; then
    K8SUSER=${K8SUSER%.csr}
fi

if [ ! -f "./${K8SUSER}.csr" ]; then
    echo
    echo "./${K8SUSER}.csr does not exist"
    echo "CSR file is required for creation of client certificate"
    echo
    exit 1
fi

echo "Generating certificate for ${K8SUSER} for DCNM ${DCNM}"
echo

# Encoding the .csr file in base64
export BASE64_CSR=$(cat ./${K8SUSER}.csr | tr -d '\n')

# Create the CSR resource in K8s cluster
create_csr_resource $K8SUSER $DCNM

# Delete if the CSR resource already exist. We need a fresh one.
kubectl delete csr ${K8SUSER}_${DCNM}csr &> /dev/null
status=$?
if test $status -eq 0
then
    echo "./${K8SUSER}_${DCNM}csr CSR resource already exist, removing it"
else
    echo "./${K8SUSER}_${DCNM}csr CSR resource does not exist, creating it"
fi

# Create the CertificateSigninRequest resource
kubectl apply -f ${K8SUSER}_${DCNM}_csr_res.yaml

# Check the status of the newly created CSR
kubectl get csr

# Approve this CSR
echo "Approving the CSR"
kubectl certificate approve ${K8SUSER}_${DCNM}csr

# Check the status of the newly created CSR
kubectl get csr

# Create role resource definition
kubectl delete clusterrole clustrole_${K8SUSER}_${DCNM} &> /dev/null
create_cluster_role $K8SUSER $DCNM
kubectl apply -f ${K8SUSER}_${DCNM}_cluster_role_res.yaml
```

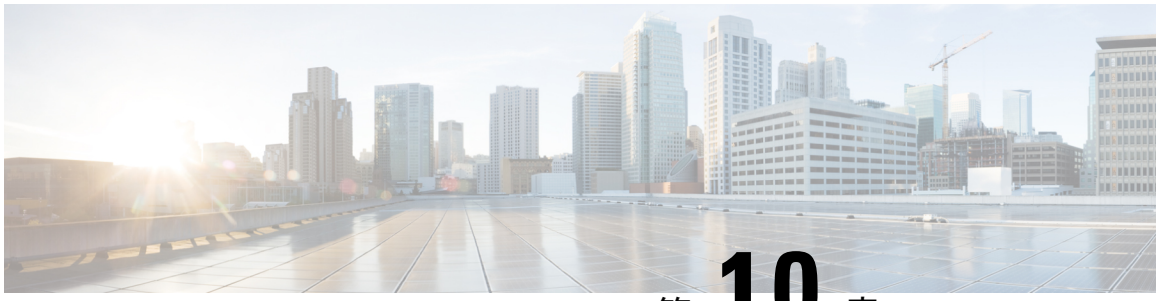
```
    # Create role binding definition
    kubectl delete clusterrolebinding clustrolebind_${K8SUSER}_${DCNM} &> /dev/null
    create_cluster_role_binding $K8SUSER $DCNM
    kubectl apply -f ${K8SUSER}_${DCNM}_cluster_rolebinding_res.yaml

    # Extract the client certificate
    echo "Extracting the user SSL certificate"
    kubectl get csr ${K8SUSER}_${DCNM}csr -o jsonpath='{.status.certificate}' >
${K8SUSER}_${DCNM}.crt
    echo "" >> ${K8SUSER}_${DCNM}.crt

    # Export the K8s cluster CA cert
    if [ -f ${K8S_CONF_PATH} ]; then
        echo "Exporting K8s CA certificate"
       cat ${K8S_CONF_PATH} | grep certificate-authority-data | awk -F ' ' '{print $2}'
 > ${K8S_CA_CRT}
    fi
    echo
    echo "----------------------------------------------------------------"
    echo "Notes: "
    echo "1. The K8s CA certificate is copied into ${K8S_CA_CRT} file."
    echo "      This to be copied into \"Cluster CA\" field."
    echo "2. The client certificate is copied into ${K8SUSER}_${DCNM}.crt file."
    echo "      This to be copied into \"Client Certificate\" field."
    echo "----------------------------------------------------------------"
    echo
fi
```

第 III 部

設定



第 10 章

[サーバ設定（Server Settings）]

サーバ設定

デフォルト値として入力されるパラメータを設定できます。

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 Nexusダッシュボード ファブリック コントローラ サーバのパラメータを設定するには、次の手順を実行します。

1. **[設定（Settings）] > [サーバ設定（Server Settings）]** を選択します。

   サーバ設定はさまざまなタブに分類され、

2. 要件に基づいて設定を変更します。

3. **[保存（Save）]** をクリックして設定を適用します。

Admin 下での LAN デバイス管理の接続性

この設定は、Nexus ダッシュボード ファブリック コントローラに必要な POD の永続的な IP の使用を決定します。ユーザーが初めてファブリック コントローラ ペルソナを選択すると、永続的な IP が Nexus ダッシュボードに割り当てられているかどうかを確認するための事前チェックが行われます。永続的な IP が割り当てられていない場合、オペレーターはエラーを表示します。ユーザーは、Nexus Dashboard 管理ネットワークまたは Nexus Dashboard データネットワークのいずれかで永続的な IP を提供できます。この選択に基づいて、ユーザーは、NDFC アプリケーションページのサーバー設定の下にある LAN デバイス管理の接続性の下でオプションを指定する必要があります。デフォルトでは、[管理] が選択されていますが、ユーザーが Nexus ダッシュボードデータ ネットワークで永続的な IP を提供する場合、ユーザーはオプションとして [データ] を選択する必要があります。

（注） LAN デバイス管理の接続を管理から DATA に、またはその逆に変更した場合。一部のデバイスでは、「SSH Unreachable」エラーのクリティカル アラートが短時間発生し、最終的に復元される場合があります。

SMTP 下の SMTP ホスト

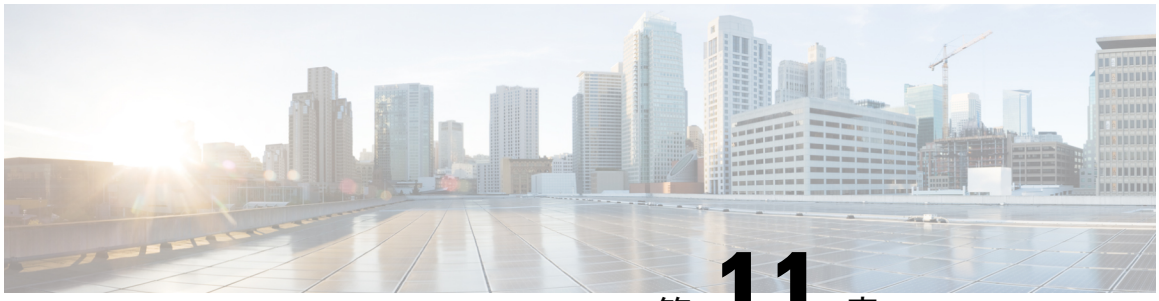
この設定は、プログラム可能なレポートとアラームの EMAIL アウトオブバンド通知として使用されます。NDFC 12.0.1a リリース以降、ユーザーは電子メール通知で NDFC アラームとレポートを受信できるようになりました。SMTP ホストアドレスは、Nexus ダッシュボード管理インターフェイスを介して到達可能である必要があります。Nexus ダッシュボード管理インターフェイスと SMTP ホストが異なる IP サブネットの一部である場合、ユーザーは Nexus ダッシュボードクラスタ構成で静的ルートエントリを作成する必要があります。

LAN ファブリックの下のすべてのファブリックで展開を無効にする

この設定により、NDFCインスタンスで定義されているすべてのファブリックの展開が無効になります。ユーザーは、ファブリックレベルごとに展開を有効にすることはできません。たとえば、ユーザーが 3 つのファブリックを持っている場合、構成の観点から 3 つのファブリックすべてが無効になります。ユーザーは、必要に応じてさまざまな構成のステージングを続けることができます。後で、ユーザーは、このサーバー設定のチェックを外すことにより、展開アクションを有効にすることができます。

PM 下の LAN スイッチの温度を収集する

この設定により、スイッチの温度の詳細を収集し、それを [ファブリックの概要] と [メトリック] セクションに表示することができます。デフォルトでは、温度データは収集されません。この設定を有効にすると、ユーザーはファブリックスイッチの温度情報も表示できます。



第 11 章

Feature Manager

Feature Manager

Cisco DCNM リリース 11.x では、DCNM のインストール時にインストール モードを選択する必要があります。リリース 12.0.1a 以降、Cisco Nexusダッシュボード ファブリック コントローラ では Nexus Dashboard にサービスをインストールできます。Nexusダッシュボード ファブリック コントローラ UI を起動すると、[機能管理（Feature Management）] ページに 3 つの異なるインストールモードが表示されます。

Nexusダッシュボード ファブリック コントローラ 12では、機能セットを動的に有効にし、アプリケーションを拡張できます。**[設定（Settings）] > [機能管理（Feature Management）]** の順に選択して、インストーラ タイプを選択し、選択した展開でいくつかの機能を有効または無効にします。

Cisco Nexus Dashboard から Nexusダッシュボード ファブリック コントローラ を初めて起動すると、[機能管理（Feature Management）]画面が表示されます。機能セットを選択する前に、バックアップと復元の操作のみを実行できます。

[機能管理（Feature Management）] ページで、次のインストール モードのいずれかを選択できます。

- ファブリック検出
- ファブリック コントローラ
- SAN コントローラ

機能セットを選択した後、Nexus Dashboard から Cisco Nexusダッシュボード ファブリック コントローラ を起動すると、次のログインから Dashboard ページが開きます。

フィーチャ セットの選択

Cisco Nexusダッシュボード ファブリック コントローラ 12を初めて起動すると、どのフィーチャ セットも有効になりません。この状態で、バックアップと復元を実行して、DCNM 11.5(x)

データをNexusダッシュボードファブリック コントローラ12に復元できます。Nexusダッシュボード ファブリック コントローラはバックアップ ファイルからデータを読み取り、それに応じてインストーラ タイプを選択します。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からフィーチャ セットを展開するには、次の手順を実行します。

手順

ステップ 1 **[設定（Settings）] > [機能管理（Feature Management）]** を選択します。

ステップ 2 ペルソナを選択して、デフォルトの機能セットを表示します。

Cisco NDFC ペルソナで使用できる機能については、「各ペルソナの機能 （456 ページ）」を参照してください。

ステップ 3 次の表で、機能セットで使用可能な機能名に対してチェックボックスをオンにします。

ステップ 4 [Apply] をクリックします。

フィーチャ セットが展開されます。選択したアプリケーションが有効になります。フィーチャ セットがインストールされていることを示すメッセージが表示されます。有効にするには更新する必要があります。

ステップ 5 ブラウザを更新して、選択したフィーチャセットとアプリケーションでNexusダッシュボード ファブリック コントローラ を展開します。

左側のペインには、展開されたフィーチャ セットで特にサポートされている機能が表示されます。

各ペルソナの機能

次の表に、Cisco NDFC リリース 12.1.1e で使用可能な機能に関する情報を示します。

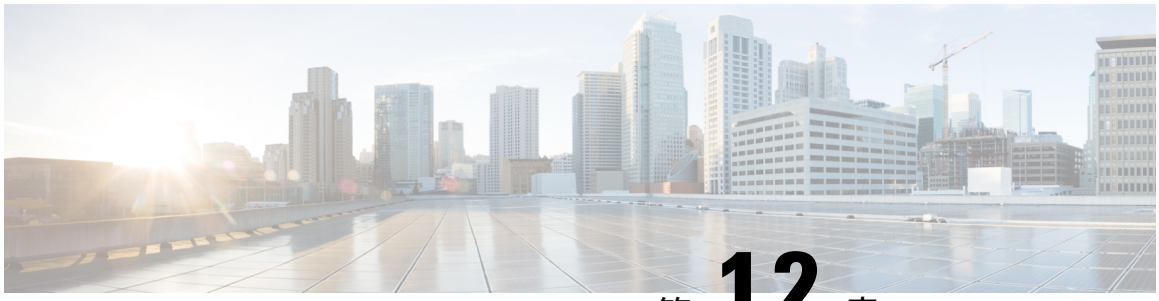
機能セット全体での変更

Nexusダッシュボード ファブリック コントローラ 12では、ある機能セットから別の機能セットに切り替えることができます。**[設定（Settings）] > [機能管理（Feature Management）]** を選択します。次の表で、目的の機能セットとアプリケーションを選択します。[保存して続行（Save and Continue）] をクリックします。ブラウザを更新して、新しい機能セットとアプリケーションでシスコ Nexusダッシュボード ファブリック コントローラ の使用を開始します。

特定の展開でサポートされる機能/アプリケーションがいくつかあります。機能セットを変更すると、これらの機能の一部は新しい展開でサポートされません。次の表に、機能セットを変更できる前提条件と基準の詳細を示します。

表 *39 :* 展開間でサポートされるスイッチング

送信元/宛先	ファブリック検出	ファブリック コントローラ	SAN コントローラ
ファブリック検出	-	ファブリック検出の展開では、モニタモードファブリックのみがサポートされます。機能セットを変更すると、ファブリック コントローラ導入でファブリックを使用できます。	サポート対象外
ファブリック コントローラ	ファブリックセットを変更する前に、既存のファブリックを削除する必要があります。	Easy Fabric から IPFM ファブリック アプリケーションに変更する場合は、既存のファブリックを削除する必要があります。	サポート対象外
SAN コントローラ	サポート対象外	サポート対象外	-



第 12 章

クレデンシャル管理

LAN クレデンシャル管理

デバイス設定の変更中、Cisco Nexusダッシュボード ファブリック コントローラ はユーザーから提供されたデバイスのログイン情報を使用します。ただし、LAN スイッチのログイン情報が指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 により **[設定（Settings）] > [LAN ログイン情報（LAN Credentials Management）]** ページを開いて LAN ログイン情報を設定するように求められます。

Cisco Nexusダッシュボード ファブリック コントローラ は、次の 2 つのログイン情報のセットを使用して LAN デバイスに接続します。

- **ディスカバリ ログイン情報**：Cisco Nexusダッシュボード ファブリック コントローラ は、デバイスのディスカバリおよび定期的なポーリング中にこれらのログイン情報を使用します。

  NDFC は、SSH および SNMPv3 でディスカバリ クレデンシャルを使用して、スイッチからハードウェアまたはソフトウェアインベントリを検出しました。したがって、これらはディスカバリ クレデンシャルと呼ばれます。スイッチごとに 1 つのインベントリを検出できます。これらは読み取り専用であり、スイッチ上で設定を変更することはできません。

- **構成変更ログイン情報**：ユーザーがデバイス構成を変更する機能を使用しようとすると、Cisco Nexusダッシュボード ファブリック コントローラ はこれらのログイン情報を使用します。

LAN クレデンシャル：LAN クレデンシャルで書き込みオプションを使用して、スイッチの設定を変更できます。1 つのスイッチで、ユーザーごとに 1 つのログイン情報が許可されます。ユーザーロールは、SSH 接続を介してスイッチに設定をプッシュするための書き込みオプションを使用するために NDFC にアクセスする必要があります。

NX-OS スイッチで作成されたユーザーロールの場合、SNMPv3 ユーザーは同じパスワードで作成されます。SSH および SNMPv3 のログイン情報がログイン情報の検出に一致することを確認します。SNMP 認証が失敗した場合、ログイン情報の検出はエラーメッセージの表示を停

止します。SNMP 認証は成功したが SSH 認証が失敗した場合、ログイン情報は続行されますが、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。

NX-OS スイッチで作成されたユーザーロールが AAA 認証を使用する場合、SNMPv3 ユーザーは作成されません。コントローラは、この AAA 認証を使用して NDFC 内のスイッチを検出またはインポートすることにより、ローカル SNMPv3 ユーザーがスイッチ上に作成されていないことを検出します。したがって、スイッチ上で exec コマンドを実行して、スイッチ上に同じパスワードを持つ SNMPv3 ユーザーを作成します。作成された SNMPv3 ユーザーロールは一時的なものです。ユーザーロールが期限切れになると、NDFC からのスイッチの継続的な検出により、SNMPv3 ユーザーが作成されます。

LAN ログイン情報管理では、構成変更ログイン情報を指定できます。LAN スイッチの設定を変更する前に、スイッチの LAN クレデンシャルを入力する必要があります。ログイン情報を提供しない場合、構成変更アクションは拒否されます。

これらの機能は、LAN ログイン情報機能からデバイス書き込みログイン情報を取得します。

- アップグレード（ISSU）
- メンテナンス モード（GIR）
- パッチ（SMU）
- テンプレートの展開
- POAP-Write erase reload、Rollback
- インターフェイスの作成/削除/設定
- VLAN の作成/削除/設定
- VPC ウィザード

デバイスが最初に検出されたかどうかに関係なく、構成変更のログイン情報を指定する必要があります。これは 1 回限りの操作です。ログイン情報が設定されると、ログイン情報は構成変更操作に使用されます。

Default Credentials

デフォルトのログイン情報は、ユーザーがアクセスできるすべてのデバイスに接続するために使用されます。次の [デバイス（Devices）] で各デバイスのログイン情報を指定することで、デフォルトのログイン情報を上書きできます。

Cisco Nexusダッシュボード ファブリック コントローラ は、まず、デバイスの個々のスイッチログイン情報を使用しようとします。[デバイス（Devices）] のログイン情報（ユーザー名/パスワード）列が空の場合、デフォルトのログイン情報が使用されます。

スイッチテーブル

デバイス テーブルには、ユーザーがアクセスできるすべての LAN スイッチがリストされます。デフォルトのログイン情報を上書きするスイッチログイン情報を個別に指定できます。ほとんどの場合、デフォルトのログイン情報のみを入力する必要があります。

[Nexusダッシュボードファブリック コントローラデバイスのLANログイン情報（LAN Credentials for the Devices）] テーブルには、次のフィールドがあります。

フィールド	説明
[デバイス名（Device Name）]	スイッチの名前が表示されます。
IP アドレス	スイッチの IP アドレスを指定します。
ログイン情報	デフォルトまたはスイッチ固有のカスタムクレデンシャルを使用するかどうかを指定します。
Username	Nexusダッシュボード ファブリック コントローラ がログインに使用するユーザー名を指定します。
ファブリック	スイッチが属するファブリックを表示します。

次の表では、**[アクション（Actions）]** メニューのドロップダウンリストで、**[LAN クレデンシャル管理（SAN Credentials Management）]**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
編集	デバイス名を選択し、**[編集（Edit）]** をクリックして、ユーザー名とパスワードを指定します。ローカルまたはカスタムの特定のログイン情報を編集できます
クリア	デバイス名を選択し、**[クリア（Clear）]** をクリックします。 確認ウィンドウが表示されたら、**[はい（Yes）]** をクリックして、NDFC サーバーからスイッチのログイン情報を消去します。
検証	デバイス名を選択し、**[検証（Validate）]** をクリックします。 操作が成功したか失敗したかを示す確認メッセージが表示されます。

ロボットのログイン情報

デフォルトのログイン情報を指定すると、ロボット機能を有効にできます。これにより、ロボットフラグが有効になります。

ロボットのロールは、DCNMの以前のロールに似ています。ロボットのユーザーロールは、スイッチとデバイスのアカウンティングに役立ちます。一般ユーザーアカウントを使用して、NDFC で行われたすべての変更を追跡できます。NDFC で、アウトオブバンド変更と呼ばれるデバイスの変更に影響を与える、ユーザーロールが変更された場合。これらの変更は、一般ユーザーアカウントによる変更としてデバイスに記録されます。したがって、アウトオブバン

ド変更とデバイスで行われた変更を追跡して区別できます。この一般ユーザーアカウントは、デバイスに記録された変更に対するロボットユーザーロールと呼ばれます。

たとえば、NDFC の network-admin を持つユーザーロールは、スイッチの設定をプッシュするためにLANデバイスのログイン情報を入力するアクセス権を持っています。このユーザーロールは、LAN クレデンシャルの作成中にロボットフラグをチェックできます。

LANクレデンシャルに指定されたユーザー名は、デバイスに記録された変更に表示されます。NDFC の LAN クレデンシャルのユーザー名がコントローラとして変更され、ロボットフラグをチェックすると、デバイスのクレデンシャルがデフォルトからロボットに変更されます。このユーザーロールは、NDFCのスイッチの設定をプッシュします。これらの変更は、ユーザーロールの network-admin によって行われた変更としてファブリック展開の履歴タブに記録されますが、スイッチのアカウントログオンはコントローラとして表示されます。したがって、適切なユーザーロールの詳細が NDFC とデバイスに記録されます。

NDFCでは、ロボットのユーザーロールは、すべてのファブリックとデバイスの管理者ロールと見なされます。デフォルトまたはログイン情報がファブリックに設定されていない場合、ロボットのユーザーロールを使用できます（異なるデバイスに設定されている場合）。書き込みアクセス権を持つ他のユーザーロールがNDFCにログインする場合、ロボットのユーザーロールが設定されているため、このユーザーロールはログイン情報を更新するように求められません。ログイン情報は、個々のスイッチ、ロボット、デフォルトのログイン情報の順に設定されます

LANクレデンシャル管理のホームページでは、顧客のログイン情報が設定されていない限り、デバイス設定を変更する際に、デフォルトのログイン情報またはロボットのログイン情報を選択できます。

ログイン情報を設定するには、次の手順を実行します。

1. 必要な **[デバイス名（Device 名）]** を選択し、**[設定（set）]** をクリックします。

   [ログイン情報の設定（Set Credentials）] ウィンドウが表示されます。

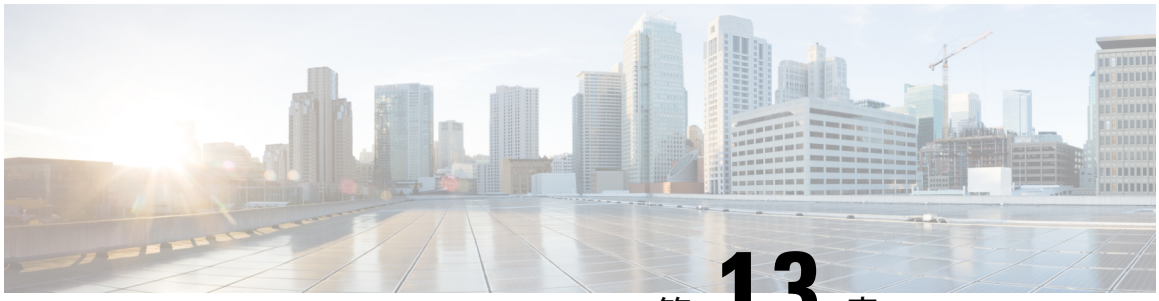
2. 適切な詳細を入力します。**[ロボット（Robot）]** チェックボックスをオンにして、ロボットのログイン情報を設定します。

   適切なロールを選択して、デバイスクレデンシャルを追加せずに設定をデバイスにプッシュできます。

必要な **[デバイス名（Device Name）]** を選択し、**[クリア（Clear）]** をクリックします。確認メッセージが表示されたら、**[はい（Yes）]**をクリックしてデフォルトのデバイスクレデンシャルをクリアします。

第 IV 部

操作



第 13 章

イベント分析

ここでは、次の内容について説明します。

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。

発行されたアラーム

UI パス：**[操作（Operations）] > [イベント分析（Event Analytics）] > [アラーム（Alarms）]** の順に選択します。

新しいアラーム ポリシーを作成した後、**[発生したアラーム（Alarms Raised）]** タブに移動し、**[更新（Refresh）]** アイコンをクリックして、作成したアラームを表示します。

必要な **[重大度（Severity）]** 列をクリックすると、スライドイン ペインが表示され、ポリシーの重大度の詳細と説明が示されます。

次の表では、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アラーム（Alarms）] > [発生したアラーム（Alarms Raised）]** 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
重大度	アラームの重大度を指定します

フィールド	説明
送信元	送信元の名前を指定します。
名前	アラームの名前を指定します。
カテゴリ	アラームのカテゴリを指定します。
作成時刻	アラームが作成された時刻を指定します。
ポリシー	アラームのポリシーを指定します。
Message	メッセージを表示します。
Ack User	アラームを確認したユーザのユーザ名。

次の表では、**[発行されたアラーム（Alarms Raised）]**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
確認応答あり	1つまたは複数のアラームを選択し、**確認**を選択します。アラームをブックマークし、**[確認済み（Acknowledged）]**の列にAck User名を追加できます。
未確認	1 つまたは複数のアラームを選択し、**未確認**を選択して、ブックマークされたアラームを削除します。 （注） 確認済みアラームのみを未確認にすることができます。
クリア	アラームを選択し、**消去**を選択して、アラームポリシーを手動で消去します。 消去されたアラームは、**[消去されたアラーム（Alarm Cleared）]**タブに移動します。
アラームの削除	アラームを選択し、**削除**を選択してアラームを削除します。

（注） リンクダウンイベントの場合、SNMP トラップの受信者に外部の可視 IP アドレスを設定し、SNMP トラップを NDFC に送信するようにスイッチを構成する必要があります。それ以外の場合、ポート状態の変更は、5分ごとのポーリングによってのみ実行できます。

クリアされたアラーム

UI パス：**操作 > イベント分析 > アラーム > クリアされたアラーム**

[クリアされたアラーム（Alarms Cleared）]タブには、**[発行されたアラーム（Alarms Raised）]**タブでクリアされたアラームのリストがあります。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、クリア時（オプション）、クリア元、ポリシー、メッセージなどの情報が表示されます。最大 90 日間、クリアされたアラームの詳細を表示できます。

1 つ以上のアラームを選択し、**[アクション（Actions）] > [削除（Delete）]** をクリックしてそれらを削除できます。

次の表では、**[発行されたアラーム（Alarms Raised）]** 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
重大度	アラームの重大度を指定します
送信元	送信元アラーム IP アドレスを指定します。
名前	アラームの名前を指定します。
カテゴリ	アラームのカテゴリを指定します。
作成時刻	アラームが作成された時刻を指定します。
クリアされた時間	アラームがクリアされた時刻を指定します。
クリアしたユーザ	アラームをクリアしたユーザを指定します。
ポリシー	アラームのポリシーを指定します。
Message	アラームの CPU 使用率およびその他の詳細を指定します。
Ack User	確認応答されたユーザ ロール名を指定します。

次の表では、**[発行されたアラーム（Alarms Raised）]** 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
アラームの削除	アラームを選択し、**[削除（Delete）]** を選択して、クリアされたアラームを削除します。

アラーム ポリシーの監視と追加

Nexus Dashboard ファブリック コントローラ でアラームを有効にし、**[操作（Operations）] > [イベント分析（Analytics）]>[アラーム（Alarms）]**に移動し、垂直タブの **[アラーム ポリシー（Alarm Policies）]** をクリックします。[外部アラームの有効化] チェック ボックスが選択されていることを確認します。これを有効にするには、Nexus Dashboard ファブリック コントローラ を再起動する必要があります。

Nexus Dashboard ファブリック コントローラ の登録済みSNMPリスナーにアラームを転送できます。Cisco Nexus Dashboard ファブリック コントローラ Web UIから、**[設定（Settings）] > [サーバ設定（Server Settings）] > [アラーム（Alarms）]** を選択し、**[外部アラームの有効化（Enable external alarms）]** 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。これを有効にするには、Nexus Dashboard ファブリック コントローラ を再起動する必要があります。

Nexus Dashboard ファブリック コントローラ の登録済みSNMPリスナーにアラームを転送できます。Cisco Nexus Dashboard ファブリック コントローラ Web UIから、**[設定（Settings）] > [サーバ設定（Server Settings）] > [アラーム（Alarms）]** を選択し、alarm.trap.listener.address フィールドに外部ポートアドレスを入力し、[**変更の適用（Apply Changes）]**をクリックして、SAN コントローラを再起動します。

（注） **[アラーム ポリシーの作成（Alarm Policy creation）]** ダイアログ ウィンドウで **[転送（Forwarding）]**チェックボックスをオンにして、外部SNMP リスナーへのアラームの転送を有効にします。

次の表では、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アラーム（Alarms）] > [アラーム ポリシー（Alarms Policies）]** 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
名前	アラーム ポリシーの名前を指定します
説明	アラーム ポリシーの名前を指定します
ステータス	アラーム ポリシーのステータスを指定します。 • アクティブ • 非アクティブ
ポリシータイプ	ポリシーのタイプを指定します。 • デバイスのヘルス ポリシー • インターフェイスのヘルス ポリシー • syslog アラームポリシー
Devices	アラーム ポリシーを適用するデバイスを指定します。
インターフェイス	インターフェイスを指定します。
詳細	ポリシーの詳細を指定します。

次の表では、**[操作（Actions）]** メニュー ドロップダウン リストのアクション項目について説明します。この項目は、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アラーム（Alarms）] > [アラーム ポリシー（Alarms Policies）]** に表示されます。

アクション項目	説明
新しいアラーム ポリシーの作成	新しいアラーム ポリシーを作成することを選択します。「新しいアラーム ポリシーの作成」の項を参照してください。
編集	アラーム ポリシーを編集するには、ポリシーを選択し、**[編集（Edit）]**を選択します。

アクション項目	説明
削除	アラーム ポリシーを削除するには、ポリシーを選択し、**[削除（Delete）]** を選択します。
アクティブ化（Activate）	アラーム ポリシーをアクティブ化して適用するには、ポリシーを選択し、**[アクティブ化（Activate）]**を選択します。
非アクティブ化	アラーム ポリシーを無効にして非アクティブにするには、ポリシーを選択し、**[非アクティブ化（Deactivate）]** を選択します。
インポート	.csv ファイルからアラーム ポリシーを一括でインポートする場合に選択します。
エクスポート	アラーム ポリシーを .csv ファイルから一括でエクスポートする場合に選択します。

次のアラーム ポリシーを追加できます。

- **デバイス ヘルス ポリシー**：デバイス ヘルス ポリシーを使用すると、デバイス ICMP 到達不能、デバイス SNMP 到達不能、またはデバイス SSH 到達不能の場合にアラームを作成できます。また、これらのポリシーを使用すると、シャーシの温度、CPU、およびメモリの使用状況をモニタできます。
- **インターフェイス ヘルス ポリシー**：インターフェイス ヘルス ポリシーを使用すると、インターフェイスのアップまたはダウン、パケット廃棄、エラー、帯域幅の詳細をモニタできます。デフォルトでは、すべてのインターフェイスがモニタリングのために選択されています。
- **Syslog アラーム ポリシー**：Syslog アラーム ポリシーは、Syslog メッセージ形式のペアを定義します。 1 つはアラームを発生させ、もう 1 つはアラームをクリアします。

新しいアラーム ポリシーの作成

次のアラーム ポリシーを追加できます。

- デバイスのヘルス ポリシー
- インターフェイスのヘルス ポリシー
- syslog アラームポリシー

デバイスのヘルス ポリシー

デバイスヘルスポリシーを使用すると、デバイス ICMP 到達不能、デバイス SNMP 到達不能、またはデバイス SSH 到達不能の場合にアラームを作成できます。また、これらのポリシーを使用すると、シャーシの温度、CPU、およびメモリの使用状況をモニタできます。

ポリシーを作成するデバイスを選択します。ポリシー名、説明、CPU使用率パラメータ、メモリ使用率パラメータ、環境温度パラメータ、デバイスの可用性、およびデバイス機能を指定します。**[デバイス機能（Device Features）]** で、BFD、BGP、および HSRP プロトコルを選択で

きます。これらのチェックボックスをオンにすると、**BFD**-ciscoBfdSessDown、ciscoBfdSessUp、**BFD**-bgpEstablishedNotification、bgpBackwardTransNotification、cbgpPeer2BackwardTransition（）、cbgpPeer2EstablishedNotification、および **HSRP**-cHsrpStateChange のアラームがトリガーされます。トラップ OID 定義の詳細については、「https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do」を参照してください。

インターフェイスのヘルス ポリシー

インターフェイス ヘルス ポリシーを使用すると、インターフェイスのアップまたはダウン、パケット廃棄、エラー、帯域幅の詳細をモニタできます。デフォルトでは、すべてのインターフェイスがモニタリングのために選択されています。

ポリシーを作成するデバイスを選択し、次のパラメータを指定します。

- ポリシー名：このポリシーの名前を指定します。一意の名前を指定する必要があります。
- 説明：このポリシーの簡単な説明を指定します。
- 転送：Cisco Nexus Dashboardファブリックコントローラ SANコントローラの登録済みSNMP リスナーにアラームを転送できます。 Web UI から、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。

（注） [アラーム ポリシーの作成（Alarm Policy creation）] ダイアログ ウィンドウで **[転送（Forwarding）]** チェックボックスをオンにして、外部 SNMP リスナーへのアラームの転送を有効にします。

- 電子メール：アラームが作成、クリア、または重大度が変更されたときに、アラームイベントの電子メールを受信者に転送できます。Cisco Nexus Dashboard ファブリック コントローラ Web UI から、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。SMTPパラメータを設定し、**[保存（Save）]** をクリックして、Cisco Nexus Dashboard ファブリック コントローラSAN コントローラ を再起動します。
- リンクステート：リンクステートオプションを選択して、インターフェイスリンクのアップまたはダウンを確認します。リンクダウンの場合、アラームを発生させることができ、リンクアップでアラームをクリアできます。
- 帯域幅（イン/アウト）：
- インバウンドエラー
- アウトバウンドエラー
- インバウンド破棄
- アウトバウンド破棄

Syslog アラーム

Syslog アラーム ポリシーは、Syslog メッセージ形式のペアを定義します。 1 つはアラームを発生させ、もう 1 つはアラームをクリアします。

ポリシーを作成するデバイスを選択し、次のパラメータを指定します。

- デバイス：このポリシーの範囲を定義します。このポリシーを適用する個々のデバイスまたはすべてのデバイスを選択します。
- ポリシー名：このポリシーの名前を指定します。一意の名前を指定する必要があります。
- 説明：このポリシーの簡単な説明を指定します。
- 転送：Cisco Nexus Dashboardファブリックコントローラ SANコントローラの登録済みSNMP リスナーにアラームを転送できます。 Web UI から、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。

（注） [アラーム ポリシーの作成（Alarm Policy creation）] ダイアログ ウィンドウで **[転送（Forwarding）]** チェックボックスをオンにして、外部 SNMP リスナーへのアラームの転送を有効にします。

- 電子メール：アラームが作成、クリア、または重大度が変更されたときに、アラームイベントの電子メールを受信者に転送できます。Cisco Nexus Dashboard ファブリック コントローラ Web UI から、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。SMTPパラメータを設定し、**[保存（Save）]** をクリックして、Cisco Nexus Dashboard ファブリック コントローラSAN コントローラ を再起動します。
- 重大度：この syslog アラーム ポリシーの重大度レベルを定義します。選択肢は、Critical、Major、Minor、および Warning です。
- 識別子：発生およびクリア メッセージの識別子部分を指定します。
- Raise Regex：syslog 発生メッセージの形式を定義します。構文は次のとおりです。
  Facility-Severity-Type：メッセージ
- Clear Regex：syslog クリア メッセージの形式を定義します。構文は次のとおりです。
  Facility-Severity-Type：メッセージ

正規表現の定義は単純な式ですが、完全な正規表現ではありません。テキストの可変領域は、$(LABEL) 構文を使用して示されます。各ラベルは、1 つ以上の文字に対応する正規表現キャプチャ グループ（.+）を表します。2 つのメッセージを関連付けるために、raise メッセージと clear メッセージの両方にある可変テキストが使用されます。識別子は、両方のメッセージに表示される 1 つ以上のラベルのシーケンスです。識別子は、ckear syslog メッセージをアラームを発生させた syslog メッセージと照合するために使用されます。テキストがメッセージの 1 つだけに表示される場合は、ラベルを付けて識別子から除外できます。

例：「値」が「ID1-ID2」のポリシー

```
"syslogRaise": "SVC-5-DOWN: $(ID1) module $(ID2) is down $(REASON)"
"syslogClear": "SVC-5-UP: $(ID1) module $(ID2) is up."
```

この例では、ID1 および ID2 ラベルをアラームとして検出するための識別子としてマークできます。この識別子は、対応する syslog メッセージで見つかります。ラベル「REASON」は昇格ですが、クリアメッセージにはありません。このラベルは、アラームをクリアする syslog メッセージに影響しないため、識別子から除外できます。

表 *40* : 例 *1*

識別子	ID1-ID2
正規表現を上げる	ETHPORT-5-IF_ADMIN_UP：インターフェイス Ethernet15/1 で admin が起動されています。
正規表現のクリア	ETHPORT-5-IF_DOWN_NONE：インターフェイス Ethernet15/1 がダウンしています（トランシーバ欠落）

上記の例では、正規表現は端末モニタに表示される syslog メッセージの一部です。

表 *41* : 例 *2*

Identifier	ID1-ID2
正規表現を上げる	ETH_PORT_CHANNEL-5-PORT_DOWN：$（ID1）：$（ID2）がダウンしています
Clear Regex	ETH_PORT_CHANNEL-5-PORT_UP：$（ID1）：$（ID2）が起動しています

表 *42* : 例 *3* :

Identifier	ID1-ID2
正規表現を上げる	ETHPORT-5-IF_SFP_WARNING：Interface $（ID1）、High Rx Power Warning
Clear Regex	ETHPORT-5-IF_SFP_WARNING：Interface $（ID1）、High Rx Power Warning clear

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 （474 ページ）を参照してください。

イベントのセットアップ

Cisco Nexusダッシュボード ファブリック コントローラ Web UI を使用してイベントを設定するには、次の手順を実行します。

手順

ステップ 1 **[操作（Operations）] > [イベント分析（Event Analytics）] > [イベントのセットアップ（Event Setup）]** の順に選択します。**[アクション（Actions）]** ドロップダウン メニューから、**[イベントのセットアップ（Event Setup）]** を選択します。

ステップ 2 [レシーバ（Receiver）] タブで、次の手順を実行します。

a) この機能を有効にするには、トグル ボタンを使用します。

b) **[Syslog メッセージを DB にコピー（Copy Syslog Messages to DB）]**を選択し、**[適用（Apply）]** をクリックして syslog メッセージをデータベースにコピーします。このオプションを選択しない場合、イベントは Web クライアントのイベント ページに表示されません。2 番目のテーブルの列には、次の情報が表示されます。

- トラップを送信するスイッチ
- syslog を送信するスイッチ
- syslog アカウンティングを送信するスイッチ
- 遅延トラップを送信するスイッチ

c) [送信元（Sources）] タブのテーブルには、関連付けられているファブリックとスイッチが表示されます。また、トラップと syslog に関する情報も表示されます。

ステップ 3 Cisco Nexusダッシュボード ファブリック コントローラ Web UI からシステムメッセージの通知転送を追加および削除するには、次の手順を実行します。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI は、電子メールまたは SNMPv1 トラップを介してファブリック イベントを転送します。一部の SMTP サーバでは、Nexusダッシュボード ファブリック コントローラ から SMTP サーバに送信される電子メールに認証パラメータを追加する必要があります。Nexusダッシュボード ファブリック コントローラ により認証を必要とする任意の SMTP サーバに送信される電子メールに認証パラメータを追加できます。この機能は、**[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** タブで有効にします。

a) **[設定（Settings）] > [サーバ設定（Server Settings）] > [イベント（Events）]** を選択します。イベント転送を有効にするには、**[イベント転送を有効にする（Enable Event forwarding）]** チェックボックスをオンにします。イベントの転送範囲、レシーバの電子メールアドレス、イベントの重大度、およびイベントのタイプが表示されます。説明の [正規表現（Regex）] フィールドは、転送送信元がイベント フォワーダの追加時に転送元が Syslog として選択されている場合にのみ適用されます。

b) **SMTP サーバ**の詳細と**送信元**電子メールアドレスを指定します。**スヌーズ**および**イベントカウント** フィルタを設定します。

c) **[Save（保存）]** をクリックします。

d) **[操作（Operations）] > [イベント分析（Event Analytics）]** の順に選択します。[操作（Actions）] ドロップダウン リストから **[ルールの追加（Add Tags）]** を選択します。

e) [転送メソッド（Forwarding Method）] で、**[電子メール]** または **[トラップ（Trap）]** を選択します。

[トラップ（Trap）] を選択した場合は、ダイアログボックスに **[アドレス（Address）** と **[ポート（Port）]** フィールドが追加されます。

f) **電子メール**転送メソッドを選択する場合は、[電子メールアドレス（Email Address）]フィールドに IP アドレスを入力します。**トラップ**メソッドを選択する場合は、[アドレス（Address）] フィールドにトラップ レシーバの IP アドレスを入力し、ポート番号を指定します。

[アドレス（Address）] フィールドに IPv4 または IPv6 アドレスまたは DNS サーバ名を入力できます。

g) **[ファブリック（Fabric）]** フィールドで、通知するすべてのグループまたは特定のファブリックを選択します。SAN インストーラの場合は、**[VSAN 範囲（VSAN Scope）]** を選択します。**[すべて（All）]** または **[リスト（List）]** オプションを選択できます。リストを選択した場合は、通知用の VSAN のリストを指定します。

h) [送信元] フィールドで、Nexusダッシュボード ファブリック コントローラ または **[Syslog]** 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 を選択すると、次のようになります。
  1. **[タイプ（Type）]** ドロップダウン リストから、イベント タイプを選択します。
  2. **[ストレージ ポートのみ（Storage Ports Only）]** チェックボックスをオンにして、ストレージ ポートのみを選択します。
  3. **[最低重大度（Minimum Severity）]** ドロップダウン リストで、受信するメッセージの重大度を選択します。
  4. **[追加（Add）]** をクリックして、通知を追加します。

- [Syslog] を選択した場合：
  1. **[ファシリティ（Facility）]** リストから、syslog のファシリティを選択します。
  2. syslog **タイプ**を指定します。

3. **[説明の正規表現（Description Regex）]** フィールドで、イベントの説明と一致する説明を指定します。
4. **[最低重大度（Minimum Severity）]** ドロップダウン リストで、受信するメッセージの重大度を選択します。
5. **[追加（Add）]** をクリックして、通知を追加します。

（注） [最低重大度（Minimum Severity）] オプションは、[イベント タイプ（Event Type）] が **[すべて（All）]** に設定されている場合のみ使用できます。

Cisco Nexusダッシュボード ファブリック コントローラが送信するトラップは、重大度タイプに対応しています。重大度タイプとともにテキストによる説明も提供されます。

```
trap type(s) = 40990 (emergency)
40991 (alert)
40992 (critical)
40993 (error)
40994 (warning)
40995 (notice)
40996 (info)
40997 (debug)
textDescriptionOid = 1, 3, 6, 1, 4, 1, 9, 9, 40999, 1, 1, 3, 0
```

i) [ルールの追加（Add Rule）] をクリックします。

ステップ 4 Cisco Nexusダッシュボード ファブリック コントローラ Web UI からイベント抑制にルールを追加するには、次の手順を実行します。

Cisco Nexusダッシュボード ファブリック コントローラ では、ユーザ指定のサプレッサ ルールに基づいて、指定されたイベントを抑制することができます。このようなイベントは、Cisco Nexusダッシュボード ファブリック コントローラ Web UIおよびSAN クライアントには表示されません。イベントはNexusダッシュボード ファブリック コントローラ データベースに保持されず、電子メールまたはSNMP トラップを介して転送されません。

テーブルからサプレッサ ルールを表示、追加、変更、および削除できます。既存のイベント テーブルからサプレッサ ルールを作成できます。テンプレートとして特定のイベントを選択し、ルール ダイアログウィンドウを呼び出します。イベントの詳細は、イベント テーブルで選択したイベントから、ルール作成ダイアログ ウィンドウの入力フィールドに自動的に移植されます。

（注） 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 EMC Call Home イベントを抑制することはできません。

a) ルールの**名前**を指定します。
b) イベント送信元に基づくルールに必要な **[範囲（Scope）]** を選択します。

[範囲（Scope）] ドロップダウン リストには、LAN グループとポート グループが個別に表示されます。**[SAN/LAN]**、**[ポート グループ（Port Groups）]**、または **[任意（Any）]** を選択できます。SAN および LAN の場合は、ファブリックまたはグループまたはスイッチ レベルでイベントの範囲を選択します。ポート グループ スコープのグループのみを選択で

きます。範囲として **[任意（Any）]** を選択すると、サプレッサ ルールがグローバルに適用されます。

c) **ファシリティ**名を入力するか、SAN/LAN スイッチイベント ファシリティ リストから選択します。

ファシリティを指定しない場合は、ワイルドカードが適用されます。

d) ドロップダウン リストから **[イベント タイプ（Event Type）]** を選択します。

イベント タイプを指定しない場合は、ワイルドカードが適用されます。

e) **[説明の照合（Description Matching）]** フィールドで、一致する文字列または正規表現を指定します。

ルール照合エンジンは、Java パターン クラスでサポートされている正規表現を使用して、イベントの説明テキストとの一致を検索します。

f) **[アクティブ範囲（Active Between）]** ボックスをオンにして、イベントが抑制される有効な時間範囲を選択します。

デフォルトでは、時間範囲は有効になっていません。つまり、ルールは常にアクティブです。

（注） 一般に、アカウンティング イベントを抑制しないでください。アカウンティング イベントの抑制ルールは、アカウンティング イベントが Nexusダッシュボード ファブリック コントローラ またはソフトウェアのスイッチのアクションによって生成される特定のまれな状況でのみ作成できます。たとえば、Nexusダッシュボード ファブリック コントローラと管理対象スイッチ間のパスワード同期中に、多数の「sync-snmp-password」AAA syslog イベントが自動的に生成されます。アカウンティング イベントを抑制するには、[サプレッサ（Suppressor）] テーブルに移動し、[イベント サプレッサ ルールの追加（Add Event Suppressor Rule）] ダイアログ ウィンドウを呼び出します。

g) [ルールの追加（Add Rule）] をクリックします。

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。

フィールド	説明
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。

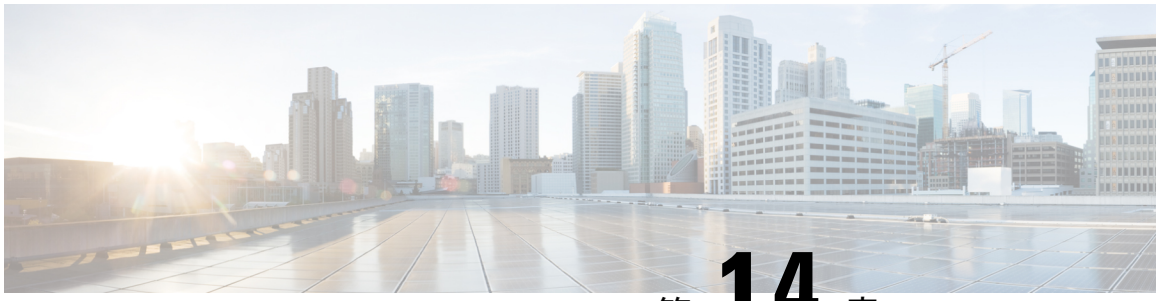
次の表では、**[操作（Actions）]**ドロップダウンリストのアクション項目について説明します。これらの項目は、**[操作（Operations）] > [イベント分析（Event Analytics）] > [アカウンティング（Accounting）]** に表示されます。

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。

リモートクラスタ

このタブには、セットアップの各クラスタ内のクラスタとファブリックの数が表示されます。

クラスタ名をクリックして概要情報を表示します。起動アイコンをクリックして、クラスタの詳細な概要を表示できます。



第 14 章

イメージ管理

イメージ管理

デバイスを最新のソフトウェアバージョンに手動でアップグレードすると、時間がかかり、エラーが発生しやすくなります。迅速で信頼性の高いソフトウェアアップグレードを実現するために、イメージ管理はアップグレードの計画、スケジューリング、ダウンロード、およびモニタリングに関連する手順を自動化します。イメージ管理は、Cisco Nexus スイッチでのみサポートされます。

（注） アップグレードする前に、Cisco Nexus 9000 シリーズ スイッチおよび Cisco Nexus 3000 シリーズ スイッチの POAP ブート モードが無効になっていることを確認します。POAP を無効にするには、スイッチ コンソールで [no boot poap enable] コマンドを実行します。ただし、アップグレード後に有効にすることができます。

[イメージ管理（Image Management）] ウィンドウには次のタブがあり、[アクション（Actions）] 列にリストされている操作を実行できます。

タブ	アクション
概要	イメージのステージング イメージの検証 イメージのアップグレード モードの変更 ポリシーの変更 コンプライアンスの再計算 レポートの実行
製品イメージ	イメージのアップロード
イメージ ポリシー	イメージ ポリシーの作成 削除
履歴	履歴 （492 ページ）

ユーザ ロールが **network-admin** または **device-upg-admin** であり、次の操作を実行するためにNexusダッシュボード ファブリック コントローラをフリーズしていないことを確認します。

- イメージをアップロードまたは削除します。
- イメージのインストール、削除、またはイメージのインストールを終了します。
- パッケージおよびパッチをインストールまたはアンインストールします。
- パッケージおよびパッチをアクティブ化または非アクティブ化します。
- イメージ管理ポリシーを追加または削除します（network-admin ユーザ ロールにのみ適用）。
- 管理ポリシーを表示します。

ユーザ ロールが network-admin、network-stager、network-operator、または device-upg-admin の場合は、任意のイメージインストールまたはデバイスアップグレードタスクを表示できます。Nexusダッシュボード ファブリック コントローラがフリーズ モードの場合は、それらを表示することもできます。

スイッチ イメージをアップグレードするプロセスを次に示します。

1. Nexusダッシュボード ファブリック コントローラへのスイッチを検出します。
2. イメージをアップロードします。
3. イメージ ポリシーを作成します。
4. イメージ ポリシーをスイッチに適用します。

5. スイッチでイメージをステージングします。
6. （任意）スイッチが中断のないアップグレードをサポートしているかどうかを検証します。
7. 適切にスイッチをアップグレードします。

概要

[概要（Overview）] ウィンドウには、シスコ 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すべてのスイッチが表示されます。スイッチの現在のバージョン、スイッチに接続されているポリシー、ステータス、およびその他のイメージ関連情報などの情報を表示できます。エントリをフィルタリングおよびソートできます。

Nexusダッシュボード ファブリック コントローラ UI ナビゲーション

- **[オペレーション（Operations）] > [イメージ管理（Image Management）] > [概要（Overview）]** を選択します。[アクション（Actions）] をクリックして、さまざまな操作を実行します。

実行するアクションに基づいて、[理由（Reason）] 列の値が更新されます。

[概要（Overview）] ウィンドウで以下のアクションを実行できます。

イメージのステージング

イメージ ポリシーをスイッチに適用した後、イメージをステージングします。イメージをステージングすると、ファイルがブートフラッシュにコピーされます。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からイメージをステージングするには、次の手順を実行します。

始める前に

- デバイスでイメージをステージングする前に、選択したデバイスにポリシーをアタッチする必要があります。
- ファブリックコントローラでサポートされるNX-OSイメージの最小バージョンは7.0(3)I7(9)です。

  上記のバージョンより前の NX-OS バージョンを実行している Nexus 9000 または Nexus 3000 スイッチでイメージをステージングするには、**Use KSTACK to SCP on N9K, N3K** 値を Falseに設定する必要があります。Web UI で、**[設定（Settings）] > [サーバー設定（Server Settings）] > [SSH]** タブを選択します。**[N9K、N3K で SCP に KSTACK を使用する（Use KSTACK to SCP on N9K, N3K）]** チェック ボックスをオフにします。サポートされているイメージバージョンをステージングする場合は、このチェックボックスをオンにします。

手順

ステップ 1 **[オペレーション（Operations）] > [イメージ管理（Image Management）] > [概要（Overview）]** を選択します。

ステップ 2 チェックボックスをオンにしてスイッチを選択します。

（注） 複数のスイッチを選択してイメージをステージングできます。

ステップ 3 **[アクション（Actions）]** をクリックし、**[イメージのステージング（Stage Image）]** を選択します。

[インストールするイメージの選択（Select Images to Install）] ウィンドウが表示されます。

このウィンドウでは、スイッチで使用可能な容量と必要な容量を確認できます。

ステップ 4 （任意）[ステージングするファイル（Files For Staging）] 列の下のハイパーリンクをクリックして、ブートフラッシュにコピーされるファイルを表示します。

ステップ 5 **[ステージ（Stage）]** をクリックします。

[イメージ管理（Image Management）] ウィンドウの [概要（Overview）] タブに戻ります。

ステップ 6 （任意）[ステージングするイメージ（Image Staged ）] 列でステータスを確認できます。

ステップ 7 （任意）ログを表示するには、[理由（Reason）] 列の下のハイパーリンクをクリックします。

イメージの検証

スイッチをアップグレードする前に、中断のないアップグレードがサポートされているかどうかを検証できます。Cisco Nexusダッシュボード ファブリック コントローラWeb UI からイメージを検証するには、次の手順を実行します。

手順

ステップ 1 **[オペレーション（Operations）] > [イメージ管理（Image Management）] > [概要（Overview）]** を選択します。

ステップ 2 チェックボックスをオンにしてスイッチを選択します。

（注） 複数のスイッチを選択してイメージをステージングできます。

ステップ 3 **[アクション（Actions）]** をクリックして **[検証（Validate）]** を選択します。

[検証（Validate）] ダイアログボックスが表示されます。

ステップ 4 破損のないアップグレード チェックボックスで [確認（Confirm）] にチェックします。

ステップ 5 [**Validate**] をクリックします。

[イメージ管理（Image Management）] ウィンドウの [概要（Overview）] タブに戻ります。

ステップ 6 （任意） [検証済み（Validated）] 列でステータスを確認できます。

ステップ 7 （任意） ログを表示するには、[理由（Reason）] 列の下のハイパーリンクをクリックします。

イメージのアップグレード

スイッチをアップグレードまたはアンインストールできます。アップグレード グループ オプションを使用すると、複数のスイッチでイメージのアップグレードを瞬時にトリガーできます。このオプションは、アップグレード/ダウングレードオプションで選択できます。

（注） 最大 12 個のスイッチを一度にアップグレードすることをお勧めします。12 個を超えるスイッチを選択した場合、アップグレードは順番に実行されます。

NX-OS スイッチのアップグレード オプション

- 中断：中断を伴うアップグレードの場合は、このオプションを選択します。
- [非中断を許可（Allow Non-disruptive）]：中断のないアップグレードを許可する場合に選択します。**[非中断を許可（Allow Non Disruptive）]** オプションを選択し、スイッチが非中断アップグレードをサポートしていない場合、中断アップグレードが実行されます。**[強制中断なし（Force Non Disruptive）]** を選択し、選択したスイッチが中断なしアップグレードをサポートしていない場合、スイッチの選択を確認するよう求める警告メッセージが表示されます。スイッチを選択または削除するには、チェックボックスを使用します。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からスイッチ イメージをアップグレードするには、次の手順を実行します。

手順

ステップ 1 **[オペレーション（Operations）] > [イメージ管理（Image Management）] > [概要（Overview）]** を選択します。

ステップ 2 チェックボックスをオンにしてスイッチを選択します。

ステップ 3 **[アクション（Actions）]** をクリックし、**[アップグレード（Upgrade）]** を選択します。

[アップグレード/アンインストール（Upgrade / Uninstall）] ウィンドウが表示されます。

ステップ 4 チェックボックスをオンにして、アップグレードのタイプを選択します。

有効なオプションは、NXOS、EPLD、およびパッケージ（RPM / SMU）です。

ステップ 5 NXOS、EPLD、またはパッケージを選択します。

a) アップグレードする方法に基づいて、ドロップダウン リストからアップグレード オプションを選択します。

b) （任意） [BIOS 適用（BIOS Force）] チェックボックスをオンにします。

すべてのデバイスの検証ステータスを表示できます。

c) **[ゴールデン（Golden）]**チェックボックスをオンにして、ゴールデンアップグレードを実行します。

d) **[モジュール番号（Module Number）]** フィールドにモジュール番号を入力します。

このフィールドの下にモジュールのステータスが表示されます。

（注）
- **[パッケージ（Packages）]**を選択すると、パッケージの詳細も表示できます。
- **[アンインストール（Uninstall）]** オプション ボタンを選択して、パッケージをアンインストールできます。

ステップ 6 [アップグレード（Upgrade）] をクリックします。

（注） 複数のスイッチをアップグレードする場合、アップグレード ステータスの更新には 30 ー 40 分かかります。

モードの変更

デバイスのモードを変更できます。Cisco Nexusダッシュボード ファブリック コントローラ Web UI からデバイスのモードを変更するには、次の手順を実行します。

手順

ステップ 1 **[オペレーション（Operations）] > [イメージ管理（Image Management）] > [概要（Overview）]** を選択します。

ステップ 2 チェックボックスをオンにして、モードを変更するスイッチを選択します。

（注） 複数のスイッチを選択できます。

ステップ 3 **[アクション（Actions）]** > **[モードの変更（Change Mode）** をクリックします。

[モードの変更（Change Mode）] ダイアログボックスが表示されます。

ステップ 4 ドロップダウン リストからモードを選択します。

有効なオプションは **[標準（Normal）]** と **[メンテナンス（Maintenance）]** です。

ステップ 5 **[保存して続Save and Deploy Now]** または **[Save and Deploy Later]** をクリックします。

[Image Management]ウィンドウの[Overview]タブに戻ります。

ポリシーの変更

スイッチにアタッチしたイメージ ポリシーは更新できます。複数のスイッチのイメージ ポリシーを同時に変更することができます。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からスイッチにアタッチされたイメージ ポリシーをアタッチまたは変更するには、次の手順を実行します。

手順

ステップ 1 **[オペレーション（Operations）] > [イメージ管理（Image Management）] > [概要（Overview）]** を選択します。

ステップ 2 チェックボックスをオンにしてスイッチを選択します。

ステップ 3 **[アクション (Actions)]** をクリックし、**[ポリシーの適用 (Apply Policy)]** を選択します。

[ポリシーの適用（Apply Policy）] ダイアログボックスが表示されます。

ステップ 4 ポリシーをアタッチまたはアタッチ解除するには、必要なチェックボックスを選択します。

ステップ 5 ドロップダウンリストからポリシーを選択します。

ステップ 6 必要に応じて **[アタッチ（Attach）]** または **(アタッチ解除（Detach）]** を選択します。

ステップ 7 （任意）変更を表示するには、[理由（Reason）] 列の下のハイパーリンクをクリックします。

ステップ 8 （任意）[ステータス（Status）] 列の下のハイパーリンクをクリックして、現在のイメージのバージョンと予期されるイメージのバージョンを表示します。

スイッチが **Out-Of-Sync** ステータスの場合は、予期されるイメージのバージョンを表示し、それに応じてスイッチをアップグレードします。

コンプライアンスの再計算

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からスイッチの設定コンプライアンスを再計算するには、次の手順を実行します。

手順

ステップ 1 **[オペレーション（Operations）] > [イメージ管理（Image Management）] > [概要（Overview）]** を選択します。

ステップ 2 チェックボックスをオンにしてスイッチを選択します。

ステップ 3 **[アクション（Actions）]** をクリックし、**[コンプライアンスの再計算（Recalculate Compliance）]** を選択します。

ステップ 4 変更を表示するには、[理由（Reason）] 列の下のハイパーリンクをクリックします。

レポートの実行

[レポート（Reports）] [レポート定義（Report Definitions）] を選択します。

再度生成する必要があるレポートの横にあるチェックボックスをオンにします。**[アクション（Actions）]** ドロップダウン リストから **[レポートの再実行（Re-run Report）]** を選択して、レポート ジョブを再度実行します。レポート ジョブが再実行されたことを示すポップアップ ウィンドウが表示されます。

[レポートの再実行（Re-run Report）] を使用すれば、スケジュールされた実行時間の前にレポートを生成できます。**オンデマンド ジョブ**の場合は、**[レポートの再実行（Re-run Report）]** をクリックしてレポートを生成します。

製品イメージ

このタブで、イメージとプラットフォームの詳細を表示できます。デバイスにイメージをアップロードまたは削除できます。

次の表で、[操作（Operations）]>[イメージ管理（Image Management）]>[イメージ（Images）] 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
プラットフォーム	プラットフォームの名前を指定します。イメージ、RPM、または SMU は、次のように分類されます。 • N9K/N3k • N6K • N7K • N77K • N5K • その他 • サード パーティ N9K プラットフォームと N3K プラットフォームのイメージは同じです。 アップロードされたイメージが既存のプラットフォームのいずれにもマッピングされていない場合、プラットフォームは [その他（Other）] になります。 プラットフォームは RPM の [サードパーティ（Third Party）] になります。
ビット	イメージのビットを指定します。

フィールド	説明
イメージ名	アップロードしたイメージ、RPM、または SMU のファイル名を指定します。
イメージのタイプ	イメージ、EPLD、RPM、または SMU のファイルタイプを指定します。
イメージ サブ タイプ	イメージ、EPLD、RPM、または SMU のファイルタイプを指定します。 ファイルタイプ EPLD は [epld] です。イメージのファイル タイプは、[nxos]、[system] または [kickstart] です。RPM のファイルタイプは [feature] で、SMU のファイル タイプは [patch] です。
NXOS バージョン	Cisco スイッチのみの NXOS イメージ バージョンを指定します。
イメージ バージョン	Cisco 以外のデバイスを含むすべてのデバイスのイメージ バージョンを指定します。
サイズ（バイト）	イメージ、RPM、または SMU ファイルのサイズをバイト単位で指定します。
Checksum	イメージのチェックサムを指定します。チェックサムは、イメージ、RPM、または SMU のファイルに破損がないかどうかをチェックします。Cisco の Web サイトからダウンロードしたファイルと [イメージのアップロード（Image Upload）] ウィンドウでアップロードしたファイルのチェックサム値が同じかどうかを確認することで、信頼性を検証できます。

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、[操作（Operations）] >[イメージ管理（Image Management）]>[イメージ（Images）]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
更新	イメージ テーブルを更新します。
アップロード	クリックして新しいイメージをアップロードします。この説明については、イメージのアップロード（488 ページ） を参照してください。

アクション項目	説明
削除	イメージをリポジトリから削除できます。 イメージを選択して、[アクション（Actions）]、[削除（Delete）] を選択します。確認ウィンドウが表示されます。[はい（Yes）] をクリックして、イメージを削除します。 （注） イメージを削除する前に、イメージにアタッチされているポリシーがどのスイッチにもアタッチされていないことを確認してください。

イメージのアップロード

32 ビットおよび 64 ビットのイメージをアップロードできます。Cisco Nexusダッシュボード ファブリック コントローラ Web UI からサーバにさまざまなタイプのイメージをアップロードするには、次の手順を実行します。

（注） デバイスは、POAP またはイメージのアップグレード中にこれらのイメージを使用します。すべてのイメージ、RPM、および SMU が **[イメージ ポリシー（Image Policies）]** ウィンドウで使用されます。

イメージをアップロードするには、ユーザ ロールが **network-admin** または **device-upg-admin** である必要があります。**network-stager** ユーザ ロールでは、この操作を実行できません。

手順

ステップ 1 **[操作（Operations）]**、**[イメージ管理（Image Management）]**、**[イメージ（Images）]** の順に選択します。

ステップ 2 **[アクション（Actions）]** をクリックし、**[アップロード（Upload）]** を選択します。

[アップロード イメージ（Upload Image）] ダイアログ ボックスが表示されます。

ステップ 3 **[ファイルの選択（Choose file）]** をクリックして、デバイスのローカル リポジトリからファイルを選択します。

ステップ 4 ファイルを選択し、**[OK]** をクリックします。

ZIP または TAR ファイルもアップロードできます。シスコ Nexusダッシュボード ファブリック コントローラ はイメージ ファイルを処理して検証し、それに応じて既存のプラットフォームで分類します。**N9K/N3K**、**N6K**、**N7K**、**N77K**、または **N5K** プラットフォームに該当しない場合、イメージファイルは **サードパーティ**または**その他**のプラットフォームに分類されます。**サードパーティ** プラットフォームは、RPM にのみ適用されます。

ステップ 5 [OK] をクリックします。

EPLD イメージ、RPM、および SMU は、/var/lib/dcnm/upload/<platform_name> のリポジトリにアップロードされます。

（注） EPLD ファイルのみがアップロードされている場合、EPLD イメージの [リリース（Release）] ドロップウンリストが空であるため、ポリシーを作成できません。

すべての NX-OS、キックスタートおよびシステム イメージは、/var/lib/dcnm/images and/var/lib/dcnm/upload/<platform_name> のパスのリポジトリにアップロードされます。

ファイル サイズとネットワーク帯域幅によっては、アップロードに時間がかかります。

（注） すべての Cisco Nexus シリーズ スイッチのイメージをアップロードできます。

Cisco Nexus 9000 シリーズ スイッチの EPLD イメージのみをアップロードできます。

ネットワークの速度が遅い場合は、Cisco Nexusダッシュボード ファブリック コントローラ の待機時間を 1 時間に増やして、イメージのアップロードを完了します。Cisco Nexusダッシュボード ファブリック コントローラ Web UI からの待機時間を増やすには、次の手順を実行します。

a) **[設定（Settings）] > [サーバ設定（Server Settings）]** を選択します。
b) **csrf.refresh.time** プロパティを検索し、値を **60** に設定します。

値は分単位です。

c) [Apply Changes] をクリックします。
d) Nexusダッシュボード ファブリック コントローラ サーバを再起動します。

イメージ ポリシー

イメージ管理ポリシーには、RPM または SMU とともに NX-OS イメージの目的の情報が含まれます。ポリシーは特定のプラットフォームに属することができます。スイッチに適用されたポリシーに基づいて、Cisco Nexusダッシュボードファブリック コントローラ では必要な NXOS と RPM または SMU がスイッチに存在するかどうかが確認されます。スイッチ上のポリシーとイメージの間に不一致があると、ファブリック警告が生成されます。

次の表では、**[アクション（Actions）]** メニューのドロップダウンリストで、**[操作（Operations）] > [イメージ管理（Image Management）] > [イメージポリシー（Images Policies）]** 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
作成（Create）	イメージに適用できるポリシーを作成できます。イメージ ポリシーの作成 （490 ページ）を参照してください。

アクション項目	説明
Delete	ポリシーを削除できます。 ポリシーを選択して、**[アクション（Actions）]**、**[削除（Delete）]**を選択します。確認ウィンドウが表示されます。**[確認（Confirm）]**をクリックして**ポリシー**を削除します。 （注） デバイスにアタッチされているポリシーを削除しようとすると、エラーメッセージが表示されます。
編集	ポリシーを編集できます。

イメージ ポリシーの作成

Cisco Web UI からイメージ ポリシーを作成するには、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

（注） MDS プラットフォームおよびSAN展開のポリシーを作成する際に、一部のフィールドがグレー表示されます。

始める前に

イメージポリシーを作成する前に、[イメージ（Images）] タブでイメージをアップロードします。イメージのアップロードの詳細については、を参照してください。イメージのアップロード （488 ページ）

手順

ステップ 1 **[操作（Operations）] > [イメージ管理（Image Management）] > [イメージ ポリシー（Image Policies）]** の順に選択します。

ステップ 2 **[アクション（Actions）] > [作成（Create）]** をクリックします。

[イメージ管理ポリシーの作成（Create Image Management Policy）] ダイアログボックスが表示されます。

ステップ 3 必要なフィールドに情報を入力します。

[イメージ管理ポリシーの作成（Create Image Management Policy）] ダイアログボックスに次のフィールドが表示されます。

フィールド	アクション
ポリシー名	ポリシー名を入力します。

フィールド	アクション
プラットフォーム	プラットフォーム ドロップダウンリストからプラットフォームを選択します。オプションは、[イメージ（Images）] ウィンドウでアップロードしたイメージに基づいて入力されます。[リリース（Release）] ドロップダウンリストのオプションは、選択したプラットフォームに基づいて自動的に入力されます。
リリース	[リリース（Release）] ドロップダウンリストから NX-OS バージョンを選択します。 64 ビット イメージのリリース バージョンでは、イメージ名に 64 ビットが付加されます。 （注） EPLD ファイルのみがアップロードされている場合、EPLD イメージの [リリース（Release）] ドロップウンリストが空であるため、ポリシーを作成できません。
パッケージ名	（任意）パッケージを選択します。特定のプラットフォーム（バージョンに依存しない）にアップロードされたすべてのパッケージを表示するには、[パッケージ（Packages）] を選択してから、[すべてのパッケージを表示（View All Packages）] チェックボックスをオンにします。
[ポリシーの説明（Policy Description）]	（任意）ポリシーの説明を入力します。
EPLD	（任意）ポリシーが EPLD イメージ用の場合は、[EPLD] チェックボックスをオンにします。
EPLD を選択します	（任意）EPLD イメージを選択します。
RPM の無効化	（任意）パッケージをアンインストールするには、このチェックボックスをオンにします。
アンインストールする RPM	（任意）アンインストールするパッケージをカンマで区切って入力します。[RPM 無効化（RPM Disable）] チェックボックスをオンにした場合にのみ、パッケージ名を入力できます。

ステップ 4 **[Save（保存）]** をクリックします。

次のタスク

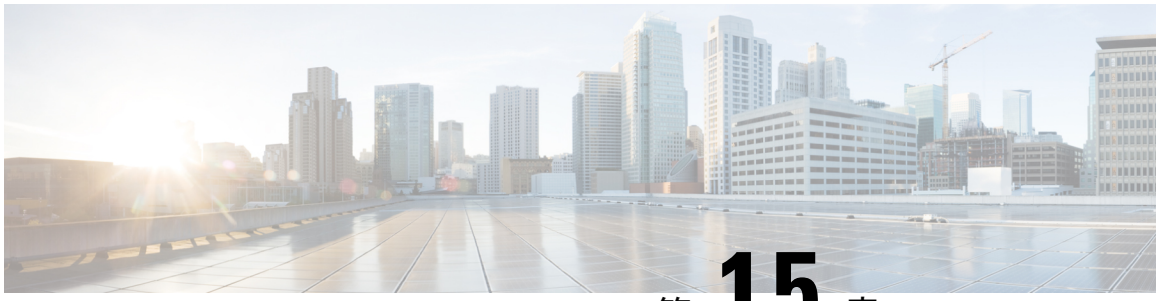
デバイスにポリシーをアタッチします。詳細については、ポリシーの変更（485 ページ）セクションを参照してください。

履歴

すべてのイメージ管理操作の履歴は、**[操作（Operations）] [イメージ管理（Image Management）] [履歴（History）]** タブで確認できます。

次の表では、この画面のフィールドについて説明します。

フィールド	説明
ID	ID 番号を指定します。
デバイス名（Device Name）	デバイス名を指定します。
バージョン	デバイスのイメージ バージョンを指定します。
ポリシー名	イメージにアタッチされるポリシー名を指定します。
ステータス	操作が成功したか失敗したかを表示します。
理由	操作の失敗の理由を示します。
操作タイプ	実行した操作のタイプを指定します。
Fabric Name（ファブリック名）	ファブリックの名前を指定します。
作成者	操作を実行したユーザー名を指定します。
タイムスタンプ	操作が実行された時刻を指定します。



第 15 章

プログラム可能レポート

[プログラム可能レポート（Programmable Reports）] アプリケーションでは、Python 2.7 スクリプトを使用してレポートを生成できます。レポート ジョブは、レポートを生成するために実行されます。各レポート ジョブは複数のレポートを生成できます。特定のデバイスまたはファブリックに対して実行するレポートをスケジュールできます。これらのレポートは、デバイスに関する詳細情報を取得するために分析されます。

[REPORT] テンプレート タイプは、[プログラム可能レポート（Programmable Reports）] 機能をサポートするために使用されます。このテンプレートには、[UPGRADE] と [GENERIC] の 2 つのテンプレート サブタイプがあります。REPORT テンプレートについて詳細は、レポート テンプレート（550 ページ）を参照してください。レポート生成を簡素化するために Python SDK が提供されています。この SDK はNexusダッシュボード ファブリック コントローラにバンドルされています。

（注） Jython テンプレートは 100k バイトの最大ファイル サイズをサポートします。いずれかのレポート テンプレートがこのサイズを超えると、Jython の実行が失敗する可能性があります。

Nexusダッシュボード ファブリック コントローラUI ナビゲーション

Cisco Nexusダッシュボード ファブリック コントローラ Web UI でプログラム可能なレポートを起動するには、[オペレーション（Operations）] [プログラム可能レポート（Programmable Reports）] を選択します。 >

[レポート（Reports） ウィンドウが表示されます。このウィンドウには、[レポート定義（Report Definitions）] タブと [レポート（Reports）] タブがあります。[レポートの作成（Create Report）] をクリックすると、両方のタブからレポートを作成できます。レポート ジョブの作成については、「レポート ジョブの作成」を参照してください。[更新（Refresh）] アイコンをクリックしてウィンドウを更新します。

（注） Cisco DCNM 11.5(x) から 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 にアップグレードした場合、レポート ジョブおよび SAN ユーザー定義レポートは移行されません。手動で再度作成する必要があります。

この章は、次の項で構成されています。

レポートの作成

[操作（Operations）] > **[プログラマブル レポート（Programmable Reports）]**を選択します。[Create Report] をクリックします。**[レポートの作成（Create Report）]** ウィザードが表示されます。

レポート ジョブを作成するには、次の手順を実行します。

手順

ステップ 1 **[レポート名（Report Name）]** フィールドにレポート ジョブの名前を入力します。

ステップ 2 **[Select Template（テンプレートの選択）]** をクリックします。

ステップ 3 ドロップダウン リストからレポート テンプレートを選択し、**[選択（Select）]** をクリックします。

選択したテンプレートに基づいて、画面に表示されるフィールドに必要な値を入力します。

ステップ 4 **[次へ（Next）]** をクリックして、**[ソースと繰り返し（Source & Recurrence）]** のステップに進みます。

ステップ 5 レポート ジョブを実行する頻度を選択します。

次の表に、使用可能なオプションとそれらの説明を示します。

使用可能な方法	説明
現在	レポートは直ちに生成されます
毎日	レポートは、開始日と終了日の間の指定された時刻に毎日生成されます。
毎週	レポートは、開始日と終了日の間に指定された時刻に週に1回生成されます。
毎月	レポートは、開始日と終了日の間に指定された時刻に月に1回生成されます。

使用可能な方法	説明
Periodic	レポートは、指定された開始日と終了日の間の期間に定期的に生成されます。レポート間の時間間隔は、分単位または時間単位で指定できます。

（注） 定期的な NVE VNI カウンタ レポートを作成する場合は、レポート生成の間隔を 60 分以上に設定する必要があります。間隔が 60 分未満の場合は、エラーメッセージが表示されます。

ステップ 6 レポートを電子メールで送信する場合は、**[電子メールレポート先（Email Report To）]** フィールドに電子メールの ID またはメーラーの ID を入力します。

[設定（Settings）] [サーバ設定（Server Settings）] [SMTP] タブで SMTP を設定する必要があります。データ サービスの IP アドレスがプライベート サブネットにある場合は、SMTP サーバーのスタティック管理ルートを Cisco Nexus Dashboard クラスタ設定に追加する必要があります。

ステップ 7 **[デバイスの選択 (Select device(s))]**、**[ファブリックの選択 (Select fabric(s))]**、または **[VSAN の選択 (Select VSAN(s))]** エリアでデバイス、ファブリック、または VSAN を選択します。

（注） 選択したテンプレートに基づいて、デバイス、ファブリック、または VSAN が読み込まれます。

ステップ 8 **[Save（保存）]** をクリックします。

新しいレポートが作成され、**[レポート（Reports）]** タブに表示されます。

レポート テンプレート

各レポート テンプレートには、いくつかのデータが関連付けられています。Nexusダッシュボード ファブリック コントローラ で有効にした機能に応じて、使用可能なレポート テンプレートの一部は次のとおりです。

- Inventory_Report
- Performance_Report
- Switch_Performance_Report
- fabric_cloudsec_oper_status
- fabric_macsec_oper_status
- fabric_nve_vni_counter
- fabric_resources
- sfp_report

- switch_inventory

上記のテンプレートに加えて、作成した他のテンプレートもここに表示されます。デフォルトテンプレートとカスタマイズされたテンプレートの作成の詳細については、「テンプレートライブラリ」を参照してください。テンプレートは、関連するタグに基づいてリストされます。

Inventory_Report、**Performance_Report**、 **Switch_Performance_Report** は、パフォーマンス管理レポートに使用されます。

レポート定義

[レポート定義（Report Definitions）] タブには、ユーザが作成したレポート ジョブが表示されます。

このタブで次の情報を表示できます。

フィールド	説明
タイトル（Title）	レポート ジョブのタイトルを指定します。
テンプレート	テンプレート名を指定します。
範囲	レポートの範囲を指定します。
スコープタイプ	デバイスまたはファブリックのレポートを生成するかどうかを指定します。
ステータス	レポートのステータスを指定します。ステータス メッセージは次のとおりです。 • 正常：レポートが正常に生成されました。 • スケジュール済み：レポート生成スケジュールが設定されています。 • 実行中：レポート ジョブが実行中です。 • 失敗：1つ以上の選択されたスイッチ/ファブリックでレポートの実行に失敗したか、レポート ジョブの実行中に問題が発生しました。 • 不明：ジョブの状態を特定できませんでした。
スケジュール	レポートの実行をスケジュールする時刻を指定します。
前回の実行時間（Last Run Time）	レポートが最後に生成された時刻を指定します。

フィールド	説明
ユーザ	レポート生成を開始したユーザを指定します。
繰り返し	レポートが生成される頻度を指定します。
内部	レポートがユーザによって生成されるか、ユーザまたは Nexusダッシュボード ファブリック コントローラ によって生成されるかを指定します。レポートがユーザによって生成された場合、値は **false** です。

このタブで次のアクションを実行できます。

（注） 内部レポート定義に対してこれらのアクションを実行することはできません。

アクション	説明
編集	レポートを編集できます。 （注） レポート名とテンプレートは変更できません。
レポートの再実行	レポートを再実行できます。再実行オプションを使用して、スケジュールされた実行時間の前にレポートを生成できます。
履歴	レポート ジョブ履歴を表示できます。 **[ジョブ履歴（Job History）]** ウィンドウが表示されます。レポート ジョブごとに複数のエントリを表示できます。 （注） 表示される定義の数は、**[設定（Settings）] > [サーバ設定（Server Settings）] > [レポート（Reports）]** タブの次の設定によって定義されます。これらの値に基づいて、レポートと履歴が消去されます。 • レポート定義全体の履歴の最大数 • レポート定義あたりの最大レポート数
削除	レポート ジョブを削除できます。

レポート

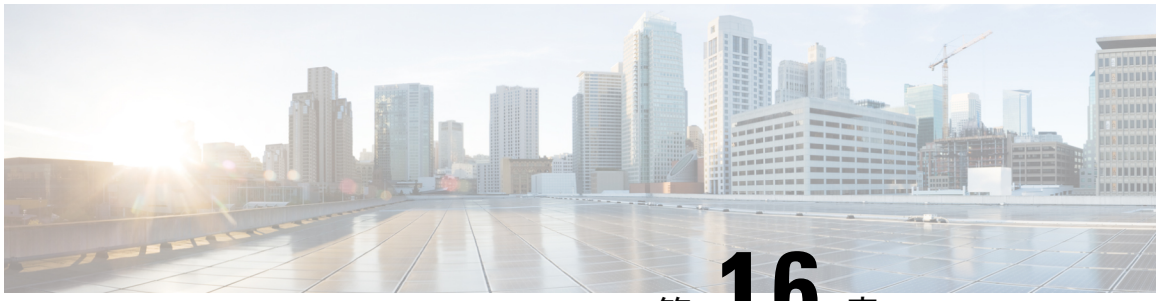
[レポート（Reports）] タブには、ユーザが実行したレポートが表示されます。

このタブで次の情報を表示できます。

フィールド	説明
タイトル（Title）	レポートのタイトルを指定します。 • レポートのタイトルを1回クリックすると、サマリー パネルにスライドが表示されます。 • レポートのタイトルをダブルクリックすると、[詳細とコマンド（Details and Commands）] ウィンドウが開きます。
テンプレート	テンプレート名を指定します。
範囲	レポートの範囲を指定します。
スコープタイプ	デバイスまたはファブリックのレポートを生成するかどうかを指定します。
ステータス	レポートのステータスを指定します。ステータス メッセージは次のとおりです。 • 完了 • 成功 • 実行中 • FAILED • 警告 • スケジュール済み • 不明ファイル
ユーザ	レポート生成を開始したユーザを指定します。
繰り返し	レポートが生成される頻度を指定します。
作成時刻	レポートをいつ作成するかを指定します。
内部	レポートがユーザによって作成されたかどうかを指定します。Nexusダッシュボード ファブリック コントローラレポートがユーザによって作成された場合、値は false です。

このタブで次のアクションを実行できます。

アクション	説明
削除	レポートを削除できます。 （注）　内部レポートは削除できません。
比較（2 レポート）	2つのレポートを並べて比較できます。レポートの詳細は、論理的にセクションにグループ化されます。 コマンドは、デバイスでコマンドを実行するために使用されるテンプレートと API に基づいて表示されます。たとえば、[switch_inventory] テンプレートでは、show version、show inventory、および show license usage コマンドを実行して情報を取得します。コマンドは、show_and_store API を使用してデバイスでコマンドを実行する場合にのみ表示されることに注意してください。
ダウンロード	レポートをダウンロードできます。ダウンロードするレポートを複数選択することはできません。



第 16 章

ライセンス管理

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、次のものからサポートが削除されます。

- 評価ライセンスの状態はサポートされていません。
- サーバ ライセンスファイルはサポートされていません。

  Cisco Smart Software Manager（CSSM）で既存のサーバーライセンスファイルをスマートライセンスに変換する必要があります。詳細については、『Cisco Smart Software Manager』を参照してください。

この章は次のトピックで構成されています。

概要

[操作（Operations）] > **[ライセンス管理（License Management）]** > **[概要（Overview）]**を選択して、既存の Cisco Nexusダッシュボード ファブリック コントローラ のライセンスを表示できます。次のタブでライセンスを表示して割り当てることができます。

- **NDFC**
- **スマート**
- **スイッチ ライセンス ファイル**

（注） デフォルトでは、**[概要（Overview）]** タブが表示されます。

[概要（Overview）] タブには、NDFC、Switch、および Smart の 3 つのカードがあります。これらのカードには、購入するライセンスの総数と期限切れになるライセンスの総数が表示されます。

スマート ライセンシングを有効にするには、**[スマート ライセンシングの設定（Setup Smart Licensing）]** をクリックします。スマート ライセンシングの詳細については、「スマートライセンス」の項を参照してください。

NDFC サーバ ライセンス

NDFC タブでは、各スイッチの NDFC ライセンスのステータスを確認できます。これらのライセンスは、デバイス、スマートライセンス、または名誉ライセンスまたはライセンスのないデバイスでプロビジョニングできます。

1 つまたは複数のスイッチを選択し、**[アクション（Actions）]**、>**[割り当て（Assign）]**または **[すべて割り当て（Assign All）]** をクリックします。

ライセンスをデバイスに割り当てると、NDFC ライセンスサービスは、デバイスの可用性、スマートライセンスのステータス、およびその他の要因に基づいて、使用可能なライセンスを割り当てます。

サーバ ベースのスマート ライセンスは、Cisco MDS スイッチ、Nexus 9000、3000 7000、および 5000 シリーズのスイッチでサポートされます。

ローカル ディレクトリからライセンスを追加するには、次の手順を実行します。

1. [ライセンスの追加（Add license）] をクリックします。

   [ライセンス ファイルの追加（Add License File）] ウィンドウが表示されます。

2. **[ライセンス ファイルの選択（Select License File）]** をクリックし、ローカルディレクトリから適切なファイルを選択します。

3. **[アップロード（Upload）]** をクリックし、**[更新（Refresh）]** アイコンをクリックしてテーブルを更新し、アップロードされたライセンス ファイルを表示します。

   ライセンスファイル名、ライセンスのタイプ、および有効期限の詳細がインポートされたライセンスファイルから抽出され、テーブルに表示されます。

次の表に、**ライセンス管理** > **NDFC** に表示されるフィールドを示します。

フィールド	説明
スイッチ名	スイッチの名前が示されます。

フィールド	説明
License Type	次のいずれかの、スイッチのライセンス ステータスが示されます。 • スイッチ • スマート • スイッチ スマート
ステータス	次のいずれかの、スイッチのライセンス ステータスが示されます。 • 永続 • Unlicensed • スマート • Expired • N/A • 無効
期限日（Expiration Date）	ライセンスの有効期限を指定します。
WWN/シャーシ ID	World Wide Name またはシャーシ ID を表示します。
モデル	デバイスのモデルが示されます。DS-C9124 や N5K-C5020P-BF など。
ファブリック	ファブリックの名前を指定します。

ライセンスを追加するには

次の表では、**[アクション（Actions）]** メニューのドロップダウン リストで、**[ライセンス管理]** > **[NDFC]**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
割り当て	スイッチを選択し、**[アクション（Actions）]** ドロップダウンリストから **[割り当て（Assign）]** を選択します。 確認メッセージが表示されます。
割り当て解除	スイッチを選択し、**[アクション（Actions）]** ドロップダウンリストから **[割り当て解除（UnAssign）]** を選択します。 確認メッセージが表示されます。

アクション項目	説明
すべて割り当て	• テーブル内のすべてのスイッチにライセンスを割り当てるには、[Actions]ドロップダウンリストから[Assign All]を選択します。 確認メッセージが表示されます。 • 表を更新するには、**OK** をクリックします。
すべて割り当て解除	• テーブル内のすべてのスイッチにライセンスを割り当て解除するには、**[アクション（Actions）]** ドロップダウンリストから **[すべて割り当て解除（UnAssign All）]** を選択します。 確認メッセージが表示されます。 • 表を更新するには、**OK** をクリックします。

スマートライセンス

Cisco Nexusダッシュボード ファブリック コントローラ では、スマートライセンスを設定することができ、スマートライセンス機能を使用してデバイスレベルでライセンスを管理し、必要に応じてライセンスを更新できます。

スマートライセンシングの概要

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンス モデルです。また、これは安全です。ユーザーがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- **管理の統合**：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供します。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（https://software.cisco.com/software/csws/ws/platform/home）。

シスコライセンスの詳細な概要については、https://www.cisco.com/c/en/us/buy/licensing/licensing-guide.html を参照してください。

スマートなライセンス管理

Cisco NDFC リリース 12.0.2 から、スマートライセンスポリシーが導入されました。このポリシーはライセンスマイクロサービスで実行され、CSSM を使用して NDFC の高度な機能のライセンスを管理する機能を提供します。このリリースから、スマートライセンスの OnPrem またはオフラインモードを登録できます。

インターネット アクセスを使用して NDFC にスマート ライセンスを直接登録すると、Cisco Nexus Dashboard は、ホスト名の代わりに IP アドレスを使用してスマート ライセンスにアクセスし、エラーを表示します。

https://smartreceiver.cisco.com の IP アドレスのサブネットが、Cisco Nexus Dashboard のルーティング IP アドレスに追加されていることを確認します。

IP アドレスを追加するには、Cisco Nexus ダッシュボード Web UI で、**[管理コンソール（Admin Console）]** の **[インフラストラクチャ（Infrastructure）]** > **[クラスタ構成（Cluster Configuration）]** > **[ルート（Routes）]**領域に移動します。編集アイコンをクリックし、**[管理ネットワーク ルート（Management Network Routes）]** の IP アドレスを追加します。**[保存（Save）]** をクリックして確認します。

[Smart] ページには、次のカードが表示されます。

- **スマートライセンシングの有効化**

  トグル スイッチを使用して、スマート ライセンシングを有効にします。有効にすると、スマートライセンスは、**信頼の確立**または**オフラインモード**の 2 つの方法で割り当てることができます。

- **信頼ステータス**

  [信頼を確立する（Establish Trust）] をクリックして信頼を確立します。**トランスポートゲートウェイ - CSLU を備えたオンプレミス**を使用し、CSSM を介して Cisco のライセンスサーバーと直接接続するか、**プロキシ - 中間 HTTP または HTTPS プロキシ経由のプロキシ**を経由して接続するかの 2 つのオプションを表示することができます。

  [Smart Licenseの信頼の確立]ウィンドウで、スマートライセンスエージェントとの信頼を確立するときに使用する転送タイプを選択します。

  - シスコ ライセンシング サーバと直接通信するには、**[デフォルト（Default）]**を選択します。
  - **[トランスポートゲートウェイ - CSLU を備えたオンプレミス（Transport Gateway - OnPrem with CSLU）]** を選択し、適切な URL を入力します。

    ライセンスを有効にするために信頼トークンは必要ありません。CSSM とオンプレミス CSLU の間で信頼が確立されます。NDFC およびオンプレミス CSLU から、ローカル接続であることが予想されるため、信頼は一定です。

  - プロキシサーバーを使用して転送するには、**[プロキシ - 中間 HTTP または HTTPS プロキシ経由のプロキシ（Proxy - Proxy via intermediate HTTP or HTTPS proxy）]** を選択します。プロキシ サーバ経由でアクセスするための URL とポートの詳細を入力します。詳細については、CSSM との信頼を確立するためにポリシーを使用したスマート ライセンシング （509 ページ）を参照してください。

デフォルトの転送を使用する場合は、CSSM から取得した登録トークンを入力します。

（注） スマート ライセンシングを登録したら、既存のスイッチにライセンスを手動で割り当てる必要があります。登録後に検出されたすべてのスイッチについて、スマート ライセンシングが自動的にスイッチに割り当てられます。

- **オフライン モード**

  オフラインモードでは、NDFC インスタンスと CSSM の間で代替的にデータを共有できます。エアギャップまたは切断された環境で動作している場合、オフラインモードを使用すると、状態をエクスポートして CSSM にアップロードし、応答を NDFC にインポートして戻すことができます。

  ライセンスデータをエクスポートし、CSSM からの応答をインポートするには、以下の手順に従ってください。

  1. **[信頼ステータス（Trust Status）]** で **[オフラインモードに切り替える（Switch to Offline mode）]** をクリックして、オフラインモードを有効にします。
  2. 1 つまたは複数のライセンスが割り当てられているオフラインモードで、**[ライセンスデータのエクスポート（Export License Data）]** をクリックします。
  3. https://software.cisco.com/software/csws/ws/platform/home で、スマートライセンスセクションに移動し、**[レポート（Reports）]** タブをクリックして、後続の使用状況データファイルタブを選択します。NDFC からの使用状況レポートをアップロードし、数分後に応答をダウンロードして NDFC にインポートできます。
  4. **[ライセンスデータのインポート（Import License Data）]** をクリックし、CSSM 確認応答ファイルを NDFC にアップロードします。

- **ライセンスステータス**

  NDFC のライセンスのステータスを指定します。スマート ライセンシングが有効になっていない場合、値は **UNCONFIGURED** です。登録せずにスマート ライセンシングを有効にすると、値は **NO LICENSES IN USE** に設定されます。値は、ライセンスを登録して割り当てると、**IN USE** または **NOT IN USE** に設定されます。**[ライセンス認証の詳細（License Authorization Details）]** ポップアップ ウィンドウで、最後のアクション、最後の認証試行、次の認証試行、および認証の有効期限を表示するには、ライセンス ステータスをクリックします。

  ポリシーの詳細 をクリックして、スマートライセンスポリシーの詳細を表示します。最初の 90 日間のデフォルトのスマートライセンスポリシーと、そのレポートから 365 日以内の現在利用可能なレポートを表示できます。

（注） 最初の登録から 30 日後にレポートを表示できます。

Resync

NDFC ライセンスの総数が CSSM ライセンスカウントと同じでない場合は、**[再同期（Resync）]** をクリックしてライセンスカウントを更新します。

再同期により、スイッチインベントリ内の NDFC ライセンスのローカル監査が実行され、レポート用にスマートライセンス数が更新されます。

CSSM はスマートライセンスへの従来のライセンスの変換を可能にします。手順については、「https://www.cisco.com/c/dam/en/us/products/se/2020/8/Collateral/brownfield-conversion-qrg.pdf.

ポリシーを使用してスマート ライセンシングからスマート ライセンシングに移行するには、Cisco Nexus Dashboard ファブリック コントローラを起動します。Web UI で、**[オペレーション (Operations)] > [ライセンス管理 (License Management)] > [スマート (Smart)]** タブの順に選択します。SLP を使用して CCSM との信頼を確立します。手順については、「CSSM との信頼を確立するためにポリシーを使用したスマート ライセンシング （509 ページ）.

次の表で、「**スイッチ ライセンス**」の項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
名前	ライセンス名を指定します。
数	使用するライセンスの数を指定します。
ステータス	使用されているライセンスのステータスを指定します。有効な値は、**IN USE** および **NOT IN USE** です。
説明	ライセンスのタイプと詳細を指定します。

ライセンスレポートをアップロードまたはダウンロードするには、https://software.cisco.com/ に移動し、**[スマート ソフトウェア ライセンシング（Smart Software Licensing）] > [Reports（レポート）]** に移動します。**[使用状況データ ファイル（Usage Data Files）]** タブで、**[使用状況データのアップロード（Upload Usage Data）]** をクリックして、NDFC から使用状況レポートをアップロードします。レポートをアップロードしてから数分後、**[確認応答（Acknowledgment）]** 列の **[ダウンロード（Upload Usage Data）]** をクリックして、NDFC に戻されてインポートされた応答をダウンロードします。

スイッチ ライセンス

スイッチがスマートライセンスで事前設定されている場合、Nexusダッシュボードファブリック コントローラ はスイッチのスマート ライセンスを検証して割り当てます。Nexusダッシュボード ファブリック コントローラ Cisco UI を使用してスイッチにライセンスを割り当てるには、**[操作（Operations）] > [ライセンス管理（License Management）] > [スマート（Smart）]** を選択します。 スマートライセンスを有効にするには、**[スマートライセンスの有効化（Enable Smart Licensing）]** をクリックします。

スイッチ ベースのスマート ライセンスは、MDSスイッチ、Nexus 9000、および 3000 シリーズのスイッチでサポートされます。

（注） 管理対象モードのスイッチの場合は、スイッチのスマートライセンスを Nexusダッシュボード ファブリック コントローラ を介して割り当てる必要があります。

スイッチのスマート ライセンスを有効にするには、Nexusダッシュボード ファブリック コントローラ の手順を実行します。

- 自由形式の CLI 設定を使用して、スイッチでスマート ライセンス機能を有効にします。
- スイッチで feature license smart または license smart enable コマンドを使用して、スマート ライセンシングを構成します。
- license smart register id token コマンドを使用して、デバイスのトークンをスマート アカウントにプッシュします。トークンをプッシュするには、Nexusダッシュボード ファブリック コントローラ で **EXEC** オプションを使用します。

表を更新するには、**更新** アイコンをクリックします。

次の表に、**ライセンス管理** > **スイッチ** に表示されるフィールドを示します。

フィールド	説明
スイッチ	スイッチの名前が示されます。
機能	スイッチの機能を表示します。
ステータス	スイッチが使用中かどうかのステータスを表示します。 • 未使用 • 使用中 • 非準拠
タイプ	次のいずれかの、スイッチのライセンス ステータスが示されます。 • 一時的 • 永続 • スマート • カウンター 永続 • Unlicensed • カウント
Warnings	有効期限など、ライセンスに関する警告を指定します。
グループ	ファブリック名または LAN 名を指定します。

CSSM との信頼を確立するためにポリシーを使用したスマート ライセンシング

Cisco Nexus Dashboard ファブリック コントローラのポリシーを使用してスマートライセンシングを使用して CSSM との信頼を確立するには、次の手順を実行します。

始める前に

- Cisco Nexus Dashboard と CSSM の間にネットワーク到達可能性があることを確認します。ネットワーク到達可能性を設定するには、**Cisco Nexus Dashboard Web UI** を起動します。**[管理コンソール（Admin Console）]** で、**[インフラストラクチャ（Infrastructure）] > [クラスタ構成（Cluster Configuration）] > [全般（General）]** タブの順に選択します。**[ルート（Routes）]** 領域で、編集アイコンをクリックし、データ ネットワーク ルートの IP アドレスを追加します。**[保存（Save）]** をクリックして確認します。
- CSSM からトークンを取得していることを確認します。

手順

ステップ 1 **[操作（Operations）] > [ライセンス管理（License Management）] > [Smart]** タブの順に選択します。

ステップ 2 スマート ライセンシングを有効にするには、**[スマート ライセンシングの有効化（Enable Smart Licensing）]** をクリックします。

ステップ 3 **[信頼ステータス（Trust Status）]** カードで、**[信頼の確立（Establish Trust）]** をクリックします。

[スマート ライセンスの信頼の確立（Stablish Trust for Smart License）] ウィンドウが表示されます。

ステップ 4 スマート ライセンス エージェントを登録するには、**[トランスポート（Transport）]** オプションを選択します。

次のオプションがあります。

- **デフォルト**：**NDFC はシスコのライセンシング サーバーと直接通信します**

  このオプションは、次の URL を使用します。https://smartreceiver.cisco.com/licservice/license

- **トランスポートゲートウェイ**：**CSLU オプションを備えたオンプレミス**

  CSLU トランスポート URL を入力します。

  （注） CSLU トランスポート URL を使用するには、製品にライセンススマート URL を設定する必要があります。

- **プロキシ**：**中間 HTTP または HTTPS プロキシ経由のプロキシ**

  このオプションを選択する場合は、URL とポートを入力します。

ステップ 5 **[トークン（Token）]** フィールドに、CSSM から取得したトークンを貼り付けて、スマート ライセンスの信頼を確立します。

ステップ 6 **[信頼の確立（Establish Trust）]** をクリックします。

確認メッセージが表示されます。

ステータスが UNTRUSTED から TRUSTED に変わります。スイッチ ライセンスの名前、数、およびステータスが表示されます。

[TRUSTED] をクリックして詳細を表示します。スイッチの詳細は、[ライセンス割り当て（License Assignments）] タブの [スイッチ/VDC（Switches/VDCs）] セクションで更新されます。スマート ライセンス オプションを使用してライセンスが付与されたスイッチのライセンス タイプとライセンス状態は Smart です。

ステップ 7 **[NDFC]** タブをクリックします。

ステップ 8 [アクション（Actions）] ドロップダウン リストから、**[すべての割り当て（Assign All）]** を選択します。

サーバー ライセンスの **[ステータス (Status)]** に **[コンプライアンス内 (InCompliance)]** が表示されます。

ステータスが **[コンプライアンス外 (OutofComplaince)]** になっている場合は、CSSM ポータルにアクセスして必要なライセンスを取得します。

これ以外のすべてのステータスについては、シスコテクニカルアシスタンスセンター（TAC）にお問い合わせください。

スイッチ ライセンス ファイル

Cisco Nexusダッシュボード ファブリック コントローラ では、1 つのインスタンスで複数のライセンスをアップロードできます。Nexusダッシュボード ファブリック コントローラ はライセンスファイルを解析し、スイッチのシリアル番号を抽出します。検出されたファブリックにライセンスファイルのシリアル番号をマッピングして、各スイッチにライセンスをインストールします。ライセンス ファイルがブート フラッシュに移動され、インストールされます。

次の表では、このタブのフィールドについて説明します。

フィールド	説明
スイッチ	スイッチ名を指定します。
IPのスイッチ	スイッチの IP アドレスを指定します。
ライセンスファイル	ライセンス ファイルのタイプを指定します。
ステータス	ライセンスのステータスを指定します。
Result Message	ライセンスの詳細を指定します。

フィールド	説明
最終アップロード時刻	サーバにアップロードされた日時を指定します。
機能	ライセンス機能を指定します。

スイッチ ライセンス ファイルの追加

Cisco Nexusダッシュボード ファブリック コントローラ Web Client UI でスイッチにライセンスを一括インストールするには、次の手順を実行します。

手順

ステップ 1 **[操作（Operations）]** > **[ライセンス管理（License Management）]** > **[スイッチ ライセンス ファイル（Switch License Files）]** を選択します。

[スイッチ ライセンス ファイル（Switch License File）] ウィンドウが表示されます。

ステップ 2 [スイッチ ライセンス ファイル（Switch License File）] タブで、**[ライセンスの追加（Add License）]** をクリックして適切なライセンス ファイルをアップロードします。

[ライセンス ファイルの追加（Add License File）] ウィンドウが表示されます。

ステップ 3 [ライセンスファイルの追加]で、[ライセンスファイルの選択]をクリックします。

ローカル ディレクトリにある適切なライセンス ファイルに移動して選択します。

ステップ 4 [アップロード（Upload）] をクリックします。

ライセンス ファイルが Nexusダッシュボード ファブリック コントローラ にアップロードされています。次の情報がライセンス ファイルから抽出されます。

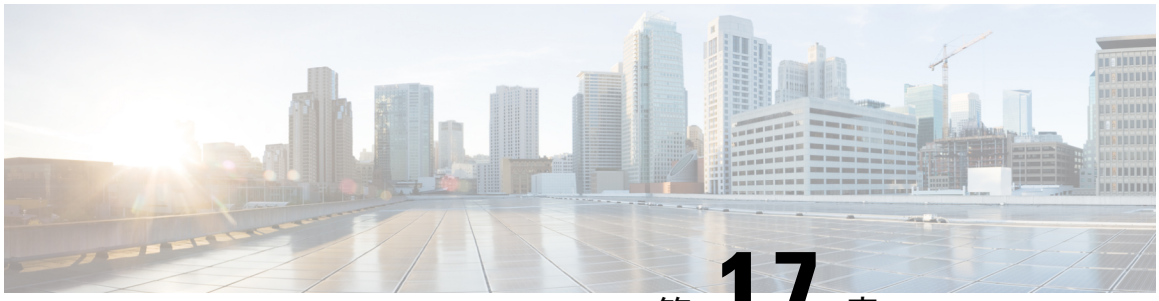
- スイッチ IP：このライセンスが割り当てられているスイッチの IP アドレス。
- ライセンス ファイル：ライセンス ファイルのファイル名
- 機能リスト：ライセンス ファイルでサポートされている機能のリスト

ステップ 5 アップロードし、それぞれのスイッチにインストールするライセンスのセットを選択します。ライセンス ファイルは、単一の特定のスイッチに適用されます。

ステップ 6 **[アクション（Actions）]** > **[インストール（Install）]** をクリックして、ライセンスをインストールします。

選択したライセンスがアップロードされ、それぞれのスイッチにインストールされます。問題やエラーを含むステータスメッセージは、ファイルが完了するたびに更新されます。

ステップ 7 ライセンスがそれぞれのデバイスと一致し、インストールされると、**[ステータス（Status）]** 列にステータスが表示されます。



第 17 章

テンプレート （Templates）

テンプレート （Templates）

UI ナビゲーション

- **[オペレーション（Operations）] > [テンプレート（Templates）]** を選択します。

Cisco Nexusダッシュボード ファブリック コントローラ Web クライアントを使用して、異なる Cisco Nexus、IOS-XE、IOS-XR、および Cisco MDS プラットフォームで設定されているテンプレートを追加、編集、または削除できます。Cisco Nexusダッシュボード ファブリック コントローラ Web クライアントで設定されているテンプレートごとに、次のパラメータが表示されます。テンプレートは JavaScript をサポートします。テンプレートの JavaScript 関数を使用して、テンプレートの構文で算術演算と文字列操作を実行できます。

Table 43: テンプレート テーブルのフィールドと説明

フィールド	説明
名前	テンプレート名を指定します。
サポートされるプラットフォーム	テンプレートがサポートするプラットフォームを指定します。
タイプ	テンプレート タイプを指定します。
サブタイプ	テンプレート サブ タイプを指定します。
変更日	テンプレート変更の日時を指定します。
タグ（Tags）	テンプレートがファブリックまたはデバイスにタグ付けされているかどうかを指定します。
説明	テンプレートの説明を指定します。
参照カウント	テンプレートが使用される回数を指定します。

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。

Note エラーのあるテンプレートは、[テンプレート（Templates）] ウィンドウに表示されません。エラーがあるテンプレートはインポートできません。このようなテンプレートをインポートするには、エラーを修正してインポートします。

次の表では、**[テンプレート（Templates）]** 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。

Table 44: テンプレートのアクションと説明

Actions	説明
新しいテンプレートの作成	新しいテンプレートを作成できるようにします。詳細については、新規テンプレートの作成, on page 516を参照してください。
テンプレートのプロパティの編集	テンプレートのプロパティを編集できるようにします。一度に編集できるテンプレートは1つだけです。詳細については、テンプレートの編集 , on page 517を参照してください。
テンプレートの内容の編集	テンプレートの内容を編集できるようにします。一度に編集できるテンプレートは 1 つだけです。詳細については、テンプレートの編集 , on page 517を参照してください。
テンプレートの複数	選択したテンプレートを別の名前で複製できるようにします。必要に応じて、テンプレートを編集できます。一度に複製できるテンプレートは 1 つだけです。 テンプレートを複製するには、複製するテンプレートの横にあるチェックボックスをオンにし、**[テンプレートの複製（Duplicate template）]** を選択します。**[テンプレートの複製（Duplicate template）]** ウィンドウが表示されます。複製されるテンプレートの名前を指定します。複製されたテンプレートの詳細については、テンプレートの編集 , on page 517を参照してください。

Actions	説明
テンプレートの削除	テンプレートを削除できるようにします。1つのインスタンスで複数のテンプレートを削除できます。 ユーザ定義テンプレートを削除できます。ただし、事前定義されたテンプレートは削除できません。 テンプレートを削除するには、削除するテンプレートの横にあるチェックボックスをオンにし、**[テンプレートの削除（Delete template）]** を選択します。警告メッセージが表示されます。テンプレートを削除する場合は、**[確認（Confirm）]** をクリックします。削除しない場合は、**[キャンセル（Cancel）]** をクリックします。テンプレートが使用中であるか、出荷テンプレートである場合は、削除できず、エラー メッセージが表示されます。 **Note** 複数のテンプレートを選択して、同じインスタンスで削除します。 テンプレートを完全に削除するには、ローカル ディレクトリ `Cisco Systems\dcn\ndfc\data\templates\` にあるテンプレートを削除します。
インポート	ローカル ディレクトリからテンプレートを 1 つずつインポートできます。詳細については、テンプレートのインポート, on page 519を参照してください。
Zip としてインポート	`.zip` 形式でバンドルされた複数のテンプレートを含む `.zip` ファイルをインポートできます ZIP ファイル内のすべてのテンプレートが抽出され、個々のテンプレートとしてテーブルにリストされます。 詳細については、「テンプレートのインポート, on page 519」を参照してください。。

Actions	説明
エクスポート	ローカル ディレクトリの場所にテンプレート設定をエクスポートできます。一度にエクスポートできるテンプレートは 1 つだけです。 テンプレートをエクスポートするには、テンプレートの横にあるチェックボックスを使用して選択し、**[エクスポート（Export）]** を選択します。テンプレート 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。テンプレート 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。

network-operator ロールを持つテンプレートのみを表示できます。このロールでテンプレートを作成、編集、または保存することはできません。ただし、**network-stager** ロールを使用してテンプレートを作成または編集できます。

この項の内容は、次のとおりです。

新規テンプレートの作成

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

- **[オペレーション（Operations）]** > **[テンプレート（Templates）]** を選択します。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からユーザ定義のテンプレートを作成し、ジョブをスケジュールするには、次の手順を実行します。

Procedure

ステップ 1 **[テンプレート（Templates）]** ウィンドウで、**[アクション（Actions）]** ドロップダウン リストから **[新規テンプレートの作成（Create new template）]** を選択します。

[テンプレートの作成（Create Template）] ウィンドウが表示されます。

ステップ 2 ウィンドウの **[テンプレート プロパティ（Template Properties）]** ページで、テンプレート名、説明、タグを指定し、新しいテンプレートのサポート対象プラットフォームを選択します。次に、ドロップダウン リストからテンプレート タイプとサブテンプレート タイプを選択します。ドロップダウン リストからテンプレートのコンテンツ タイプを選択します。

Note 基本テンプレートは CLI テンプレートです。

ステップ 3 **[次へ（Next）]** をクリックしてテンプレートの編集を続行するか、**[キャンセル（Cancel）]** をクリックして変更を破棄します。

編集したテンプレートのプロパティは、**[テンプレートの編集（Edit Template）]** ウィンドウの **[テンプレート コンテンツ（Template Content）]** ページに表示されます。構成テンプレートの構造については、「テンプレートの構造」の項を参照してください。

ステップ 4 **[検証（Validate）]** をクリックして、テンプレートの構文を検証します。

Note 警告のみがある場合は、テンプレートの保存を続行できます。ただし、エラーが発生した場合は、続行する前にテンプレートを編集してエラーを修正する必要があります。[開始行（Start Line）] 列の下の行番号をクリックして、テンプレートの内容でエラーを見つけます。テンプレート名がないテンプレートを検証すると、エラーが発生します。

ステップ 5 **[ヘルプ（Help）]** をクリックして、右側の **[エディタ（Help）]** ペインを開きます。

このウィンドウには、テンプレートの作成に使用された形式、変数、コンテンツ、およびデータ型に関する詳細情報が表示されます。**[エディタのヘルプ（Editor Help）]** ペインを閉じます。

ステップ 6 リンクが表示されたら、**エラー**および**警告**をクリックします。エラーまたは警告がない場合、リンクは使用できません。エラーまたは警告が表示されている場合にリンクをクリックすると、右側に**[エラーおよび警告（Errors & Warnings）]** ペインが表示され、エラーと警告が表示されます。**[エラーおよび警告（Errors & Warnings）]** ペインを閉じます。

ステップ 7 テンプレート コンテンツを作成するには、必要なテーマ、キー バインディング、およびフォント サイズをドロップダウン リストから選択します。

ステップ 8 **[完了（Finish）]** をクリックしてテンプレートの編集を完了し、**[キャンセル（Cancel）]** をクリックして変更を破棄し、**[前へ（Previous）]** をクリックして **[テンプレート プロパティ（Template Properties）]** ページに移動します。

テンプレートが作成されたことを示すメッセージのページが表示されます。このページには、テンプレート名、タイプ、サブタイプ、およびプラットフォームも表示されます。**[別のテンプレートの作成（Create another template）]** をクリックしてもう 1 つのテンプレートを作成するか、**[Edit <template name> template]** をクリックして編集したばかりのテンプレートを編集します。

ステップ 9 **[テンプレートの編集（Edit Template）]** ウィンドウを閉じるか、**[テンプレート ライブラリに戻る（Back to template library）]** をクリックして**[テンプレート（Templates）]** ウィンドウに戻ります。

テンプレートの編集

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

- **[オペレーション（Operations）]** > **[テンプレート（Templates）]** を選択します。

ユーザ定義のテンプレートを編集できます。ただし、定義済みのテンプレートおよびすでに公開されているテンプレートは編集できません。

[テンプレートの編集（Edit Template）] ウィンドウを使用して、最初にテンプレートのプロパティを編集し、次にテンプレートの内容を編集します。さらに、**[テンプレート プロパティの編集（Edit Template Properties）]** アクションを使用してテンプレート プロパティのみを編集するか、**[テンプレート コンテンツの編集（Edit template content）]** アクションを使用してテンプレート コンテンツのみを編集できます。つまり、あるインスタンスでテンプレートのプロパティを編集してから、別のインスタンスでテンプレートの内容を編集できます。このウィンドウを使用して、テンプレートのプロパティとコンテンツを表示することもできます。

テンプレートのプロパティを編集し、テンプレートの内容を編集するには、次の手順を実行します。

Procedure

ステップ 1 **[テンプレート（Templates）]** ウィンドウで、テンプレートを選択します。**[アクション（Actions）]** ドロップダウン リストから、**[テンプレート プロパティの編集（Edit Template Properties）]** を選択します。

[テンプレートの編集（Edit Template）] ウィンドウが表示されます。

ステップ 2 ウィンドウの **[テンプレート プロパティ（Template Properties）]** ページに、テンプレートの名前、その説明、サポートされるプラットフォーム、タグ、およびコンテンツ タイプが表示されます。テンプレートの説明とタグを編集できます。サポートされているプラットフォームを編集するには、選択したチェックボックスをオフにして他のスイッチを選択します。次に、ドロップダウン リストからテンプレート タイプとサブテンプレート タイプを選択します。

ステップ 3 **[次へ（Next）]** をクリックしてテンプレートの編集を続行するか、**[キャンセル（Cancel）]** をクリックして変更を破棄します。

編集したテンプレートのプロパティは、**[テンプレートの編集（Edit Template）]** ウィンドウの **[テンプレート コンテンツ（Template Content）]** ページに表示されます。

ステップ 4 **[検証（Validate）]** をクリックして、テンプレートの構文を検証します。

Note 警告のみがある場合は、テンプレートの保存を続行できます。ただし、エラーが発生した場合は、続行する前にテンプレートを編集してエラーを修正する必要があります。[開始行（Start Line）] 列の下の行番号をクリックして、テンプレートの内容でエラーを見つけます。テンプレート名がないテンプレートを検証すると、エラーが発生します。

ステップ 5 **[ヘルプ（Help）]** をクリックして、右側の **[エディタ（Help）]** ペインを開きます。

このウィンドウには、テンプレートの作成に使用された形式、変数、コンテンツ、およびデータ型に関する詳細情報が表示されます。**[エディタのヘルプ（Editor Help）]** ペインを閉じます。

ステップ 6 リンクが表示されたら、**エラー**および**警告**をクリックします。エラーまたは警告がない場合、リンクは使用できません。エラーまたは警告が表示されている場合にリンクをクリックすると、右側に**[エラーおよび警告（Errors & Warnings）]** ペインが表示され、エラーと警告が表示されます。**[エラーおよび警告（Errors & Warnings）]** ペインを閉じます。

ステップ 7 テンプレート コンテンツを作成するには、必要なテーマ、キー バインディング、およびフォント サイズをドロップダウン リストから選択します。

ステップ 8 **[完了（Finish）]** をクリックしてテンプレートの編集を完了し、**[キャンセル（Cancel）]** をクリックして変更を破棄し、**[前へ（Previous）]** をクリックして **[テンプレート プロパティ（Template Properties）]** ページに移動します。

テンプレートが保存されたことを示すメッセージが表示されたページが表示されます。このページには、テンプレート名、タイプ、サブタイプ、およびプラットフォームも表示されます。**[別のテンプレートの作成（Create another template）]** をクリックしてもう 1 つのテンプレートを作成するか、**[Edit <template name> template]** をクリックして編集したばかりのテンプレートを編集します。

ステップ 9 **[テンプレートの編集（Edit Template）]** ウィンドウを閉じるか、**[テンプレート ライブラリに戻る（Back to template library）]** をクリックして**[テンプレート（Templates）]** ウィンドウに戻ります。

テンプレートのインポート

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

- **[オペレーション（Operations）]** > **[テンプレート（Templates）]** を選択します。

zip 形式のテンプレートをインポートする場合も、同じ手順に従います。

Note テンプレート内の「\n」は、インポートおよび編集されると改行文字と見なされますが、ZIP ファイルとしてインポートされると正常に機能します。

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からテンプレートをインポートするには、次の手順を実行します。

Procedure

ステップ 1 **[テンプレート（Templates）]** ウィンドウで、**[アクション（Actions）]** ドロップダウンリストから **[テンプレートのインポート（Import template）]** を選択します。

[テンプレートのインポート（Import Template）] ウィンドウが表示されます。

ステップ 2 コンピュータに保存されているテンプレートを参照して選択します。

ステップ 3 **[OK]** をクリックしてテンプレートをインポートするか、**[キャンセル（Cancel）]** をクリックしてテンプレートを破棄します。

Note 圧縮されたテンプレート ファイルをインポートすると、成功またはエラー メッセージが表示されます。**[OK]** をクリックします。

ステップ 4 必要に応じて、テンプレート パラメータとコンテンツを編集できます。詳細については、テンプレートの編集 , on page 517を参照してください。

Note 圧縮されたテンプレート ファイルをインポートすると、**[テンプレートの編集（Edit Template）]** ウィンドウが表示されないことがあります。ただし、必要に応じて **[テンプレートの編集（Edit Template）]** アクションを使用して、テンプレート パラメータとコンテンツを編集できます。

ステップ 5 テンプレートのプロパティまたはコンテンツを編集しない場合は、**[次へ（Next）]**、**[完了（Finish）]**、**[テンプレート ライブラリに戻る（Back to template library）]**の順にクリックして、**[テンプレート（Templates）]** ウィンドウに戻ります。

テンプレート構造

構成テンプレートの内容は、主に4つの部分で構成されます。テンプレートのコンテンツの編集については、**[テンプレート コンテンツ（Template Content）]** の横にある **[ヘルプ（Help）]** アイコンをクリックします。

この項の内容は、次のとおりです。

テンプレートの形式

ここでは、テンプレートの基本情報について説明します。次の表に、使用可能なフィールドの詳細を示します。

プロパティ名	説明	有効な値	任意かどうか
名前（name）	テンプレートの名前	テキスト	いいえ
説明	テンプレートに関する簡単な説明	テキスト（Text）	はい
userDefined	ユーザがテンプレートを作成したかどうかを示します。ユーザが作成した場合、値は「true」です。	「true」または「false」	はい

プロパティ名	説明	有効な値	任意かどうか
supportedPlatforms	この設定テンプレートをサポートするデバイスプラットフォームのリスト。すべてのプラットフォームをサポートするには、[All] を指定します。	N1K、N3K、N3500、N4K、N5K、N5500、N5600、N6K、N7K、N9K、MDS、VDC、N9K-9000v、IOS-XE、IOS-XR、その他、すべての Nexus スイッチのリストがカンマで区切られています。	いいえ

プロパティ名	説明	有効な値	任意かどうか
templateType	使用するテンプレートのタイプを指定します。	• CLI • POAP **Note** POAP オプションは、Cisco Nexus ダッシュボード ファブリック コントローラ LAN ファブリックの展開には適用されません。 • ポリシー • SHOW • プロファイル • ファブリック • [抽象（ABSTRACT）] • レポート	はい

プロパティ名	説明	有効な値	任意かどうか
templateSubType	テンプレートに関連付けられたサブタイプを指定します。		

プロパティ名	説明	有効な値	任意かどうか
		• CLI • なし • POAP • なし • VXLAN • FABRICPATH • VLAN • PMN **Note** POAP オプションは、Cisco Nexus ダッシュボード ファブリック コントローラ LAN ファブリックの展開には適用されません。 • ポリシー • VLAN • interface-vlan • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORTCHANNEL	

プロパティ名	説明	有効な値	任意かどうか
		• INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VPC • INTERFACE_PORTCHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • SHOW • VLAN • interface-vlan • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORTCHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VPC • INTERFACE_PORTCHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE	

プロパティ名	説明	有効な値	任意かどうか
		• プロファイル • VXLAN • ファブリック • 該当なし • [抽象（ABSTRACT）] • VLAN • interface-vlan • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORT_CHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VPC • INTERFACE_SAN_PORT_CHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • レポート • アップグレード • GENERIC	

プロパティ名	説明	有効な値	任意かどうか
contentType			はい

プロパティ名	説明	有効な値	任意かどうか
		• CLI • TEMPLATE_CLI • POAP • TEMPLATE_CLI **Note** POAP オプションは、Cisco Nexus ダッシュボードファブリックコントローラ LAN ファブリックの展開には適用されません。 • ポリシー • TEMPLATE_CLI • PYTHON • SHOW • TEMPLATE_CLI • プロファイル • TEMPLATE_CLI • PYTHON • ファブリック • PYTHON	

プロパティ名	説明	有効な値	任意かどうか
		• [抽象（ABSTRACT）] • TEMPLATE_CLI • PYTHON • レポート • PYTHON	
実装（Implement）	抽象テンプレートを実装するために使用されます。	テキスト（Text）	はい
依存関係	スイッチの特定の機能を選択するために使用されます。	テキスト（Text）	はい
公開	テンプレートを読み取り専用としてマークし、変更を回避するために使用されます。	「true」または「false」	はい

テンプレート変数

このセクションには、テンプレートに使用されるパラメータの宣言された変数、データ型、デフォルト値、および有効な値の条件が含まれます。これらの宣言された変数は、動的コマンド生成プロセス中にテンプレート コンテンツ セクションの値の置換に使用されます。また、これらの変数は、意思決定およびテンプレート コンテンツ セクションの反復ブロックで使用されます。変数には事前定義されたデータ型があります。変数に関する説明を追加することもできます。次の表に、使用可能なデータ型の構文と使用方法を示します。

変数の型	有効値	反復可能?
boolean	true|false	いいえ
enum	`Example: running-config, startup-config`	いいえ
浮動	浮動小数点形式	いいえ
floatRange	`Example: 10.1,50.01`	はい
整数型（Integer）	任意の数値	いいえ

変数の型	有効値	反復可能?
integerRange	「-」で区切られた連続する番号 「,」で区切られた個別の番号 Example: 1-10,15,18,20	はい
インターフェイス	形式：<if type><slot>[/<sub slot>]/<port> Example: eth1/1, fa10/1/2 etc.	いいえ
interfaceRange	Example: eth10/1/20-25, eth11/1-5	はい
IPアドレス	IPv4 または IPv6 アドレス	いいえ
ipAddressList	IPv4、IPv6、または両方のタイプのアドレスの組み合わせのリストを作成できます。 Example 1: 172.22.31.97, 172.22.31.99, 172.22.31.105, 172.22.31.109 Example 2: 2001:0db8:85a3:0000:0000:8a2e:0370:7334, 2001:0db8:85a3:0000:0000:8a2e:0370:7335, 2001:0db8:85a3:1230:0000:8a2f:0370:7334 Example 3: 172.22.31.97, 172.22.31.99, 2001:0db8:85a3:0000:0000:8a2e:0370:7334, 172.22.31.254	はい
ipAddressWithoutPrefix	Example: 192.168.1.1 または Example: 1:2:3:4:5:6:7:8	いいえ
ipV4Address	IPv4 アドレス	いいえ
ipV4AddressWithSubnet	Example: 192.168.1.1/24	いいえ
ipV6Address	[IPv6 アドレス（IPv6 address）]	いいえ

変数の型	有効値	反復可能?
ipV6AddressWithPrefix	Example: 1:2:3:4:5:6:7:8 22	いいえ
ipV6AddressWithSubnet	IPv6アドレスとサブネット	いいえ
ISISNetAddress	Example: 49.0001.00a0.c96b.c490.00	いいえ
long	Example: 100	いいえ
MAC アドレス	14 または 17 文字長の MAC アドレス形式	いいえ

string	変数の説明などに使用される自由テキスト
	
	Example:
	string scheduledTime
	{
	regularExpr=^([01]\d|2[0-3]):([0-5]\d)$;
	}
		いいえ

string[]	Example: {a,b,c,str1,str2}	はい

構造体	単一の変数にバンドルされているパラメータのセット。
	
	struct <structure name declaration > {
	<parameter type> <parameter 1>;
	<parameter type> <parameter 2>;
	…..
	} [<structure_inst1>] [, <structure_inst2>] [, <structure_array_inst3 []>];
	
	struct interface_detail {
	string inf_name;
	string inf_description;
	ipAddress inf_host;
	enum duplex {
	validValues = auto, full, half;
	};
	}myInterface, myInterfaceArray[];
		いいえ
		Note 構造体変数が配列として宣言されている場合、変数は反復型です。

変数の型	有効値	反復可能?
wwn （Cisco Nexusダッシュボード ファブリック コントローラ Web クライアントでのみ使用可能）	Example: 20:01:00:08:02:11:05:03	いいえ

可変メタ プロパティ

テンプレート変数セクションで定義されている各変数には、一連のメタ プロパティがあります。メタ プロパティは、主に変数に定義されている検証ルールです。

次の表に、使用可能な変数タイプに適用されるさまざまなメタ プロパティを示します。

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
boolean	ブール値。 Example: true	はい											
enum			はい										
浮動	符号付き実数。 Example: 75.56, -8.5	はい	はい	はい	はい	はい							
floatRange	符号付き実数の範囲 Example: 50.5 - 54.75	はい	はい	はい	はい	はい							

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
integer	符号付き実数 Example: 50, -75	はい	はい		はい	はい							
integerRange	符号付き実数の範囲 Example: 50-65	はい	はい		はい	はい							
インターフェイス	インターフェイス/ポートを指定します Example: Ethernet 5/10	はい	はい				はい	はい	はい	はい			
interfaceRange		はい	はい				はい	はい	はい	はい			
IPアドレス	IPv4 または IPv6 形式の IP アドレス	はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
pAdtsLi		はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
	IPv4、IPv6、または両方のタイプのアドレスの組み合わせのリストを作成できます。 Example 1: 10.22.31.97, 10.22.31.99, 10.22.31.105, 10.22.31.109 Example 2: [redacted], [redacted], [redacted] Example 3: 10.22.31.97, 10.22.31.99, [redacted], 10.22.31.254 **Note** リス												

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
		ト内のアドレスは、ハイフンではなくカンマで区切ります。											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
[illegible]	IPv4 または IPv6 アドレス（プレフィックス/サブネットは不要）。												
[illegible]	IPv4 アドレス	はい											
[illegible]	IPv4 アドレスとサブネット	はい											
[illegible]	[IPv6 アドレス（IPv6 addrs）]	はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
[illegible]	プレフィックス付き IPv6 アドレス	はい											
[illegible]	IPv6 アドレスとサブネット	はい											
[illegible]	Example: [illegible]												
long	Example: 100	はい			はい	はい							
MAC アドレス	MAC アドレス												
string	リテラル文字列 Example for string Regular expression: string [illegible] { [illegible] }	はい									はい	はい	はい

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
string[]	カンマ（,）で区切られた文字列リテラル Example: {string1, string2}	はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
構造体	単一の変数にバンドルされているパラメータのセット。 struct <structure name> <declaration> { <parameter type> <parameter 1>; <parameter type> <parameter 2>; ….. } [structvar1] [, <structvar2> [, <structvarN> []>];												
wwn	WWN アドレス												

例：メタ プロパティの使用

```
##template variables

integer VLAN_ID {
min = 100;
max= 200;
};

string USER_NAME {
defaultValue = admin123;
minLength = 5;
};

struct interface_a{
 string inf_name;
 string inf_description;
 ipAddress inf_host;
 enum duplex {
  validValues = auto, full, half;
 };
}myInterface;

##
```

可変注釈

注釈を使用して変数をマーキングする変数プロパティを設定できます。

Note 可変注釈は、POAP でのみ使用できます。ただし、注釈はテンプレートタイプ「CLI」には影響しません。

テンプレート変数セクションでは、次の注釈を使用できます。

注釈キー	有効な値	説明
AutoPopulate	テキスト（Text）	あるフィールドから別のフィールドに値をコピーします。
DataDepend	テキスト	
説明	[テキスト（Text）]	ウィンドウに表示されるフィールドの説明
DisplayName	テキスト（Text） **Note** スペースがある場合は、テキストを引用符で囲みます。	ウィンドウに表示されるフィールドの表示名

注釈キー	有効な値	説明
列挙体	Text1、Text2、Text3 など	選択するテキストまたは数値をリストします
IsAlphaNumeric	「true」または「false」	文字列には、英数字を使用します。
IsAsn	「true」または「false」	
IsDestinationDevice	「true」または「false」	
IsDestinationFabric	「true」または「false」	
IsDestinationInterface	「true」または「false」	
IsDestinationSwitchName	「true」または「false」	
IsDeviceID	「true」または「false」	
IsDot1qId	「true」または「false」	
IsFEXID	「true」または「false」	
IsGateway	「true」または「false」	IPアドレスがゲートウェイかどうかを検証します。
IsInternal	「true」または「false」	フィールドを内部にし、ウィンドウに表示しません。 **Note** この注釈は、ipAddress変数にのみ使用します。
IsManagementIP	「true」または「false」 **Note** この注釈は、変数「ipAddress」に対してのみマークする必要があります。	

注釈キー	有効な値	説明
is_mandatory	「true」または「false」	値をフィールドに強制的に渡す必要があるかどうかを検証します
IsMTU	「true」または「false」	
IsMultiCastGroupAddress	「true」または「false」	
IsMultiLineString	「true」または「false」	文字列フィールドを複数行の文字列テキスト領域に変換します
IsMultiplicity	「true」または「false」	
IsPassword	「true」または「false」	
IsPositive	「true」または「false」	値が正であるかどうかを確認します。
IsReplicationMode	「true」または「false」	
IsShow	「true」または「false」	ウィンドウのフィールドを表示または非表示にします
IsSiteId	「true」または「false」	
IsSourceDevice	「true」または「false」	
IsSourceFabric	「true」または「false」	
IsSourceInterface	「true」または「false」	
IsSourceSwitchName	「true」または「false」	
IsSwitchName	「true」または「false」	
IsRMID	「true」または「false」	
IsVPCDomainID	「true」または「false」	
IsVPCID	「true」または「false」	
IsVPCPeerLinkPort	「true」または「false」	
IsVPCPeerLinkPortChannel	「true」または「false」	

注釈キー	有効な値	説明
IsVPCPortChannel	「true」または「false」	
[パスワード（Password）]	テキスト（Text）	パスワードフィールドを検証します
PeerOneFEXID	「true」または「false」	
PeerTwoFEXID	「true」または「false」	
PeerOnePCID	「true」または「false」	
PeerTwoPCID	「true」または「false」	
PrimaryAssociation		
ReadOnly	「true」または「false」	フィールドを読み取り専用にします
ReadOnlyOnEdit	「true」または「false」	
SecondaryAssociation	テキスト（Text）	
セクション		
UsePool	「true」または「false」	
UseDNSReverseLookup		
ユーザ名	テキスト（Text）	ウィンドウにユーザ名フィールドを表示します。
警告	テキスト（Text）	Description 注釈をオーバーライドするテキストを提供します。

例：**AutoPopulate** 注釈

```
##template variables
string BGP_AS;
 @(AutoPopulate="BGP_AS")
  string SITE_ID;
##
```

例：**DisplayName**注釈

```
##template variables
@(DisplayName="Host Name", Description = "Description of the host")
String hostname;
@(DisplayName="Host Address", Description = " test description" IsManagementIP=true)
```

```
ipAddress hostAddress;
##
```

例：IsMandatory注釈

```
##template variables
@(IsMandatory="ipv6!=null")
ipV4Address ipv4;
@(IsMandatory="ipv4!=null")
ipV6Address ipv6;
##
```

例：IsMultiLineString注釈

```
##template variables
@(IsMultiLineString=true)
string EXTRA_CONF_SPINE;
##
```

IsShow注釈

```
##template variables
boolean isVlan;
@(IsShow="isVlan==true")
integer vlanNo;
##

##template variables
boolean enableScheduledBackup;
@(IsShow="enableScheduledBackup==true",Description="Server time")
string scheduledTime;
##
The condition "enableScheduledBackup==true" evaluates to true/false

##template variables
@(Enum="Manual,Back2BackOnly,ToExternalOnly,Both")
string VRF_LITE_AUTOCONFIG;
@(IsShow="VRF_LITE_AUTOCONFIG!=Manual",  Description="Target Mask")
integer DCI_SUBNET_TARGET_MASK
##
The condition "VRF_LITE_AUTOCONFIG!=Manual" matches string comparison to evaluate to
true or false
```

例：警告の注釈

```
##template variables
@(Warning="This is a warning msg")
  string SITE_ID;
##
```

テンプレートの内容

この項には、テンプレートで使用する構成コマンドと、すべてのパラメータが含まれています。これらのコマンドには、テンプレート変数セクションで宣言された変数を含めることができます。コマンド生成プロセス中に、変数の値がテンプレートの内容に適切に置き換えられます。

Note 使用するコマンドは、任意のデバイスのグローバル構成コマンド モードで入力するのと同じように指定する必要があります。コマンドを指定するときは、コマンド モードを考慮する必要があります。

テンプレートの内容は、変数の使用によって決まります。

- スカラ変数：反復に使用できない値の範囲または配列を取得しません（変数タイプテーブルでは、iterate-ableが「No」としてマークされています）。スカラ変数はテンプレートの内容内で定義する必要があります。

```
Syntax: $$<variable name>$$
Example: $$USER_NAME$$
```

- 反復変数：ブロックの反復に使用されます。これらのループ変数は、次に示すように、繰り返しブロック内でアクセスする必要があります。

```
Syntax:@<loop variable>
Example:
foreach val in $$INTEGER_RANGE_VALUE$$ {
@val
}
```

- スカラー構造体変数：構造体メンバー変数は、テンプレートの内容からアクセスできます。

```
Syntax: $$<structure instance name>.<member variable name>$$
Example: $$myInterface.inf_name$$
```

- 配列構造変数：構造体のメンバー変数は、テンプレートの内容からアクセスできます。

```
Syntax: $$<structure instance name>.<member variable name>$$
Example: $$myInterface.inf_name$$
```

テンプレート変数に加えて、次のステートメントを使用して、条件付きコマンドと反復コマンドの生成を使用できます。

- if-else if-else ステートメント：その中の変数に割り当てられた値に基づいて、設定コマンドのセットの包含/除外を論理的に決定します。

```
Syntax: if(<operand 1>  <logical operator>  <operand 2>){
command1 ..
command2..
..
}
else  if (<operand 3> <logical operator> <operand 4> )
{
Command3 ..
Command4..
..
}
else
{
```

```
Command5 ..
Command6..
..
}
Example: if-else if-else statement
if($$USER_NAME$$ == 'admin'){
Interface2/10
no shut
}
else {
Interface2/10
shut
}
```

- foreach ステートメント：コマンドのブロックを反復するために使用されます。反復は、割り当てられたループ変数値に基づいて実行されます。

```
Syntax:
foreach <loop index variable> in $$<loop variable>$$ {
@<loop index variable> ..
}
Example: foreach Statement
foreach ports in $$MY_INF_RANGE$${
interface @ports
no shut
}
```

- オプションパラメータ：デフォルトでは、すべてのパラメータが必須です。パラメータをオプションにするには、パラメータに注釈を付ける必要があります。

変数セクションには、次のコマンドを含めることができます。

- **@(IsMandatory=false)**
- **Integer frequency;**

  テンプレートの内容の項では、「if」条件チェックを使用せずに、パラメータに値を割り当てることで、コマンドを除外または含めることができます。オプションのコマンドは、次のように構成できます。

- **probe icmp [frequency frequency-value] [timeout seconds] [retry-count retry-count-value]**

高度な機能

次に、テンプレートの構成に使用できる高度な機能を示します。

- 割り当て操作

  構成テンプレートは、テンプレートコンテンツセクション内の変数値の割り当てをサポートします。変数の宣言されたデータ型の値が検証されます。不一致がある場合、値は割り当てられません。

  割り当て操作は、次のガイドラインに従って使用できます。

  - 左側の演算子は、テンプレートパラメータまたは for ループパラメータのいずれかである必要があります。

- 正しい値の演算子は、テンプレート パラメータ、ループ パラメータ、引用符で囲まれたリテラル文字列値、または単純な文字列値のいずれかの値です。

ステートメントがこれらのガイドラインに従っていない場合、またはこの形式に適合しない場合は、割り当て操作とは見なされません。これは、他の通常の行と同様に、コマンド生成時に置き換えられます。

```
Example: Template with assignment operation
##template properties
name =vlan creation;
userDefined= true;
supportedPlatforms = All;
templateType = CLI;
published = false;
##
##template variables
integerRange vlan_range;
@(internal=true)
integer vlanName;
##
##template content
foreach vlanID in $$vlan_range$${
vlan @vlanID
$$vlanName$$=@vlanID
name myvlan$$vlanName$$
}
##
```

- Evaluate メソッド

  設定テンプレートは、Java ランタイムが提供する Java スクリプト環境を使用して、算術演算（ADD、SUBTRACT など）、文字列操作などを実行します。

  テンプレート リポジトリ パスで JavaScript ファイルを見つけます。このファイルには、算術文字列関数の主要なセットが含まれています。カスタム JavaScript メソッドを追加することもできます。

  これらのメソッドは、次の形式の設定テンプレート コンテンツ セクションから呼び出すことができます。

```
Example1:
$$somevar$$ = evalscript(add, "100", $$anothervar$$)
```

  また、次のようなif条件の内部で *evalscript* を呼び出すことができます。

```
if($$range$$ > evalscript(sum, $$vlan_id$$,  -10)){
do something...
}
```

  Java スクリプト ファイルのバックエンドにあるメソッドを呼び出すことができます。

- 動的な決定

  構成テンプレートは、特殊な内部変数LAST_CMD_RESPONSEを提供します。この変数には、コマンド実行中のデバイスからの最後のコマンド応答が格納されます。これは、デバ

イスの状態に基づいてコマンドを提供するための動的な決定を行うために、構成テンプレートのコンテンツで使用できます。

Note ifブロックの後には、空の場合もある新しい行でelseブロックを続ける必要があります。

VLANがデバイス上に存在しない場合のVLANの作成例。

```
Example: Create VLAN
##template content
show vlan id $$vlan_id$$
if($$LAST_CMD_RESPONSE$$ contains "not found"){
vlan $$vlan_id$$
}
else{
}
##
```

この特別な暗黙的変数は、「IF」ブロックでのみ使用できます。

- テンプレート参照

すべての変数を定義した基本テンプレートを作成できます。この基本テンプレートは、複数のテンプレートにインポートできます。基本テンプレートの内容は、拡張テンプレートの適切な場所に置き換えられます。インポートしたテンプレートパラメータと内容は、拡張テンプレート内でアクセスできます。

```
Example: Template Referencing
Base template:
##template properties
 name =a vlan base;
 userDefined= true;
 supportedPlatforms = All;
 templateType = CLI;
 published = false;
 timestamp = 2015-07-14 16:07:52;
 imports = ;
##
##template variables
 integer vlan_id;
##
##template content
 vlan $$vlan_id$$
##

Derived Template:
##template properties
 name =a vlan extended;
 userDefined= true;
 supportedPlatforms = All;
 templateType = CLI;
 published = false;
 timestamp = 2015-07-14 16:07:52;
 imports = a vlan base,template2;
##
##template variables
 interface vlanInterface;
##
##template content
```

```
 <substitute a vlan base>
 interface $$vlanInterface$$
 <substitute a vlan base>
##
```

拡張テンプレートを起動すると、基本テンプレートのパラメータ入力も取得されます。また、置換された内容は、完全な CLI コマンドの生成に使用されます。

レポート テンプレート

REPORT テンプレートのテンプレート タイプは python で、2 つのサブタイプ（UPGRADE と GENERIC）があります。

アップグレード

UPGRADEテンプレートは、ISSU前後のシナリオに使用されます。これらのテンプレートは、ISSU ウィザードに表示されます。

ISSU 前後の処理の詳細については、Nexusダッシュボード ファブリック コントローラ にパッケージ化されているデフォルトのアップグレードテンプレートを参照してください。デフォルトのアップグレード テンプレートは issu_vpc_check です。

GENERIC

GENERIC テンプレートは、リソース、スイッチ インベントリ、SFP、NVE VNI カウンタに関する情報の収集など、一般的なレポート シナリオに使用されます。このテンプレートを使用して、トラブルシューティング レポートを生成することもできます。

リソース レポート

このレポートには、特定のファブリックのリソース使用状況に関する情報が表示されます。

[サマリ（Summary）]セクションには、すべてのリソース プールと現在の使用率が表示されます。より多くの列を表示するには、ウィンドウの下部にある水平スクロール バーを使用します。

POOL NAME：プールの名前を指定します。

POOL RANGE：プールの IP アドレス範囲を指定します。

SUBNET MASK：サブネット マスクを指定します。

MAX ENTRIES：プールから割り当て可能な最大エントリ数を示します。

USAGE INSIDE RANGE：プール範囲内に割り当てられている現在のエントリ数を指定します。

USAGE OUTSIDE RANGE：プール範囲外に設定されている現在のエントリ数を指定します。

USAGE PERCENTAGE：これは、(範囲内での使用数/最大エントリ数) *100 という式を使用して計算されます。

[詳細の表示（View Details）]をクリックして、各リソースプールに割り当てられた、または設定されたリソースのビューを表示します。たとえば、SUBNET の詳細セクションには、サブネット内で割り当てられたリソースに関する情報が含まれます。

スイッチ インベントリ レポート

このレポートは、スイッチ インベントリに関する概要を提供します。

[詳細の表示（View Details）] をクリックして、モジュールとライセンスに関する詳細情報を表示します。

SFPレポート

このレポートは、ファブリックおよびデバイス レベルでの SFP の使用率に関する情報を提供します。

（注） スイッチインベントリおよび SFP レポートは、Cisco Nexus デバイスでのみサポートされます。

トラブルシューティング レポート

これらのレポートは、トラブルシューティングのシナリオに役立つように生成されます。現在、定義済みのトラブルシューティング レポートは **NVE VNI** カウンタ レポートのみです。**NVE VNI カウンタ** レポートの生成では、ネットワーク トラフィックに基づいて上位ヒットの VNI を特定するための定期的なチェックが実行されます。大規模なセットアップでは、レポートの生成頻度を 60 分以上に制限することをお勧めします。

NVE VNI カウンタ レポート

このレポートは、ファブリック内の各 VNI の **show nve vni counters** コマンド出力を収集します。

最も古いレポートと最新のレポートを比較すると、**[サマリ（Summary）]** セクションには上位 10 件のヒット VNI が表示されます。上位ヒット VNI は、次のカテゴリに表示されます。

- ユニキャスト トラフィック用の L2 または L3 VNI
- マルチキャスト トラフィック用の L2 または L3 VNI
- ユニキャスト トラフィック用の L2 のみの VNI
- マルチキャスト トラフィック用の L2 のみの VNI
- ユニキャスト トラフィック用の L3 のみの VNI
- マルチキャスト トラフィック用の L3 のみの VNI

最も古いレポートは、現在のレポート タスクで保存された最初のレポートを参照します。現在のレポートと比較する必要がある最初のレポートとして特定のレポートを選択する場合は、選択したレポートが最初で最も古いレポートになるように、選択したレポートよりも古いすべてのレポートを削除します。

たとえば、昨日の午前 8 時、午後 4 時、および午後 11 時に 3 つのレポートが実行されたとします。今日のレポートの最初の最も古いレポートとして午後 11 時にレポートを使用する場合は、昨日の午前 8 時と午後 4 時に実行されました。

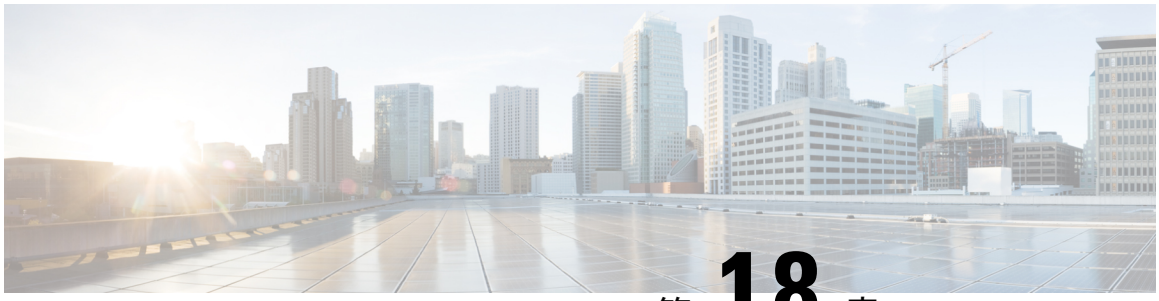
定期レポートの場合、最も古いレポートは、期間の開始時刻に実行される最初のレポートです。日次および週次レポートの場合、現在のレポートが以前に生成されたレポートと比較されます。

[サマリ（Summary）] セクションには、送信された合計バイト数と VNI に関する情報を含むカラムごとのレポートが表示されます。より多くの列を表示するには、ウィンドウの下部にある水平スクロール バーを使用します。

（注） NVE VNI カウンタ レポートの **[サマリ（Summary）]** セクションでは、スイッチのリロード後またはスイッチのカウンタのクリア後にレポートが生成された場合、[合計送信バイト数（TOTAL TX BYTES）] 列に負の数が表示されます。番号は、後続のレポートで正しく表示されます。回避策として、スイッチをリロードするか、カウンタをクリアする前に、古いレポートをすべて削除するか、新しいジョブを作成することを推奨します。

詳細については、**[詳細の表示（View Details）]** をクリックしてください。このセクションでは、スイッチごとに NVE VNI とカウンタを示します。

レポートの表示方法の詳細については、「プログラム可能なレポート」の章を参照してください。



第 18 章

テクニカル サポート

テクニカル サポートのログ収集を開始すると、すべてのデータ ストアのクエリが試行されます。システムの現在の状態のスナップショットを作成します。ログの収集が完了すると、通知が表示されます。ログはいつでもダウンロードできます。

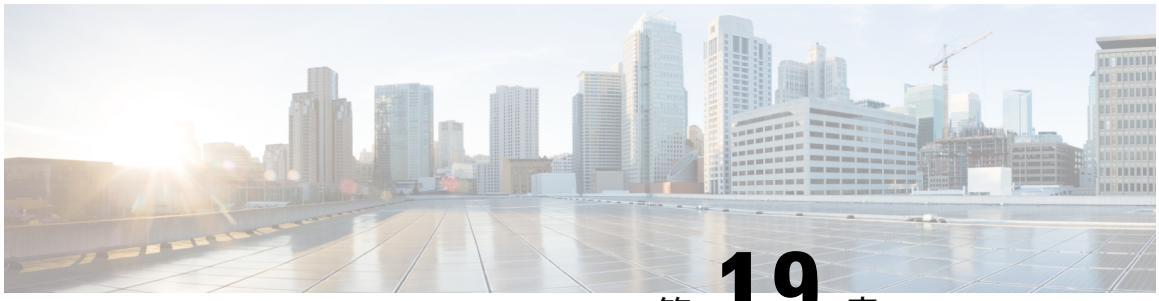
ログ収集

Cisco Nexusダッシュボード ファブリック コントローラ では、トラブルシューティング用のログを収集してダウンロードできます。

[データ収集の開始（Begin data collection）] をクリックして、トラブルシューティングのためにログを収集します。

[ログ収集の再開（Restart log collection）] をクリックして、ログの収集を開始します。この操作により、サーバ上の既存のテクニカル サポート ログが削除されます。収集が完了したら、トラブルシューティングのためにログをダウンロードできます。

[ログのダウンロード（Download log）]をクリックして、ローカル ディレクトリにログをダウンロードします。ログは `.zip` 拡張子でダウンロードされます。



第 19 章

バックアップと復元

いつでも手動でバックアップできます。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するようにスケジューラを設定することもできます。

次のいずれかの形式を使用してバックアップおよび復元できます。

- **設定のみ**：設定のみのバックアップの方が小さくなります。これにはインテント、依存データ、検出情報、ログイン情報、およびポリシーが含まれています。このバックアップからの復元には、機能するファブリック、スイッチの検出、予期される設定、およびその他の設定が含まれています。
- **完全**：フルバックアップは大規模です。これには、現在のデータ、履歴データ、アラーム、ホスト情報、および設定のみのバックアップのすべてが含まれます。このバックアップからの復元には、機能的な履歴レポート、メトリックグラフ、およびすべての基本機能があります。

構成のみのバックアップまたは完全バックアップを復元できます。

バックアップを復元するときは、設定のみの復元または完全な復元を選択できます。設定のみの復元では、設定（インテント、検出情報、ログイン情報、ポリシー）のみが復元され、設定のみのバックアップと完全バックアップの両方を使用して実行できます。完全な復元は、設定と、現在および過去のデータ、チャートなどを復元し、完全バックアップのみを使用して実行できます。

（注） 新規インストール後、バックアップデータを復元する前に、最低 20 分間待機してください。新しくインストールしたセットアップでバックアップをすぐに復元すると、一部のアプリケーションが動作しない場合があります。

アップグレード後の機能の互換性

次の表に、NDFC、リリース 12.1.1e へのアップグレード後に DCNM 11.5(x) バックアップから復元される機能に関連する警告を示します。

（注） 11.5(x) には、リリース 11.5(1)、11.5(2)、 のみが含まれます。11.5(4) から 12.1.1e へのアップグレードはサポートされていません。

DCNM 11.5(x) の機能	アップグレードのサポート
vCenter による VMM の可視性	サポート対象
設定されたプレビュー フィーチャー	サポート対象外
IPv6 で検出されたスイッチ	サポート対象外
DCNM トラッカー	サポート対象外
ファブリックのバックアップ	未サポート
レポート定義とレポート	未サポート
スイッチのイメージとイメージ管理ポリシー	サポート対象外
イメージ/イメージ管理データの切り替え	11.5(x) から 12.1.1e に引き継がれない
アラーム ポリシーの設定	11.5(x) から 12.1.1e に引き継がれない
パフォーマンス管理データ	アップグレード後、最大 90 日間の CPU/メモリ/インターフェイス統計情報が復元されます。

このセクションの内容は次のとおりです。

スケジューラ

スケジューラの目的は、システムを復元する必要がある場合にシステムのバックアップを取ることです。リモートロケーションにバックアップ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 からアプリケーションおよび設定データのバックアップをスケジュールするには、次の手順を実行します。

始める前に

スケジュールされたバックアップジョブがない場合は、**[スケジュールが設定されていません（No Schedule set）]** が表示されます。

手順

ステップ 1　**[スケジュール設定なし（No Schedule set）]** をクリックします。

[Scheduler（スケジューラ）] ウィンドウが表示されます。

ステップ 2　**[スケジュールされたバックアップの有効化（Enable Scheduled backups）]** チェックボックスをオンにします。

ステップ 3　**[種類（Type）]** で、復元する形式を選択します。

- **[構成のみ（Config only）]** または **[完全（Full）]** を選択します。

ステップ 4　**[SCP サーバ（SCP Server）]** フィールドに、SCP サーバの IP アドレスを入力します。

ステップ 5　**[ファイル パス（File Path）]** フィールドに、バックアップ ファイルを保存するディレクトリの絶対パスを入力します。

ステップ 6　バックアップディレクトリに**ユーザー名**と**パスワード**を入力します。

ステップ 7　バックアップ ファイルに対する**暗号キー**を入力します。

バックアップから復元するには、暗号化キーが必要です。暗号化キーは、機密情報を含むバックアップファイルの一部を暗号化するために使用されます。

ステップ 8　**[日単位で実行（Run on days）]** フィールドで、チェックボックスをオンにして、1 日以上のバックアップジョブをスケジュールします。

ステップ 9　**[開始時刻（Start at）]** フィールドで、タイムピッカーを使用して特定の時刻にバックアップをスケジュールします。

タイムピッカーは 12 時間制です。

ステップ 10　**[バックアップのスケジュール（Schedule backup）]** をクリックして、スケジュールに従ってバックアップジョブを実行します。

Restore（復元）

（注）　新規インストール後、バックアップデータを復元する前に、最低 20 分間待機してください。新しくインストールしたセットアップでバックアップをすぐに復元すると、一部のアプリケーションが動作しない場合があります。

ガイドライン

機能が有効になっていない、新しくインストールされた Nexusダッシュボード ファブリック コントローラ でのみ復元を実行できます。

L2 HA から L3 HA に移行する場合は、[外部サービス IP 構成を無視する（Ignore External Service IP Configuration）] チェックボックスをオンにして、バックアップ内の永続的な IP が無視され、復元中に新しい IP が選択されるようにします。残りのデータは復元されます。

（注） 災害復旧時に NDFC を使用した場合、バックアップが作成されたのと同じバージョンでのみ復元できます。

Cisco Nexusダッシュボード ファブリック コントローラ Web UIからアプリケーションおよび構成データを復元するには、次の手順を実行します。

手順

ステップ 1 [復元（Restore）] をクリックします。

[今すぐ復元（Restore now）] ウィンドウが表示されます。

ステップ 2 **[種類（Type）]** で、復元する形式を選択します。

- **[構成のみ（Config only）]** または **[完全（Full）]** を選択します。

ステップ 3 バックアップ ファイルを保存した適切な宛先を選択します。

- ファイルがローカル ディレクトリに保存されている場合は、**[ファイルのアップロード（Upload File）]** を選択します。
  1. バックアップ ファイルが保存されるディレクトリ
  2. バックアップファイルを **[今すぐ復元（Restore now）]** ウィンドウにドラッグアンドドロップします。

     または

     [Browse] をクリックします。バックアップ ファイルが保存されるディレクトリに移動します。バックアップ ファイルを選択して、[開く（Open）] をクリックします。
  3. バックアップ ファイルに対する**暗号キー**を入力します。

     （注） バックアップを復元するには、暗号化キーが必要です。暗号化キーは、機密情報を含むバックアップファイルの一部を暗号化するために使用されます。

- バックアップ ファイルがリモート ディレクトリに保存されている場合は、**[SCP からインポート（Import from SCP）]** を選択します。
  1. **[SCP サーバ（SCP Server）]** フィールドに、SCP サーバの IP アドレスを入力します。
  2. **[ファイル パス（File Path）]** フィールドに、バックアップ ファイルへの相対ファイル パスを入力します。
  3. **ユーザ名**と**パスワード**を該当するフィールドに入力します。

4. **[暗号キー（Encryption Key）]** フィールドにバックアップ ファイルに対する暗号キーを入力します。

（注） バックアップを復元するには、暗号化キーが必要です。暗号化キーは、機密情報を含むバックアップファイルの一部を暗号化するために使用されます。

ステップ 4 （オプション）**[外部サービスの IP 設定を無視する（Ignore External Service IP Configuration）]** チェックボックスをオンにします。

[外部サービスの IP 設定を無視する（Ignore External Service IP Configuration）] チェック ボックスがオンになっている場合、外部サービスの IP 設定は無視されます。この選択により、システムでバックアップを作成し、それを別の管理サブネットやデータサブネットを持つ別のシステムに復元することができます。

このオプションは、Cisco DCNM 11.5(x) から Cisco NDFC へのアップグレード中には影響しません。

ステップ 5 [復元（Restore）] をクリックします。

バックアップ ファイルが [バックアップと復元（Backup & Restore）] ウィンドウの表に表示されます。復元に必要な時間は、バックアップ ファイルのデータによって異なります。

今すぐバックアップ

Cisco Nexusダッシュボード ファブリック コントローラ Web UI からアプリケーションおよび設定データのバックアップを取得するには、次の手順を実行します。

手順

ステップ 1 **[今すぐバックアップ（Backup Now）]** をクリックします。

ステップ 2 **[種類（Type）]** で、復元する形式を選択します。

- **[構成のみ（Config only）]** または **[完全（Full）]** を選択します。

ステップ 3 バックアップ ファイルを保存する適切な**宛先**を選択します。

- ローカル ディレクトリにバックアップを保存するには、**[ローカル ダウンロード（Local Download）]** を選択します。

1. バックアップ ファイルに対する**暗号キー**を入力します。

（注） バックアップを復元するには、暗号化キーが必要です。暗号化キーは、機密情報を含むバックアップファイルの一部を暗号化するために使用されます。

2. [バックアップ（Backup）] をクリックします。

バックアップが完了すると、**[バックアップと復元（Backup & Restore）]**画面からバックアップ ファイルをダウンロードできます。

3. [アクション（Actions）] 列で、[ダウンロード（Download）] アイコンをクリックして、バックアップをローカル ディレクトリに保存できます。

   バックアップを削除するには、**[削除（Delete）]** アイコンをクリックします。

   （注） 割り当てられたディスク容量が限られているため、**[ローカルダウンロード（Local Download）]**オプションで取得したバックアップはできるだけ早く削除する必要があります。

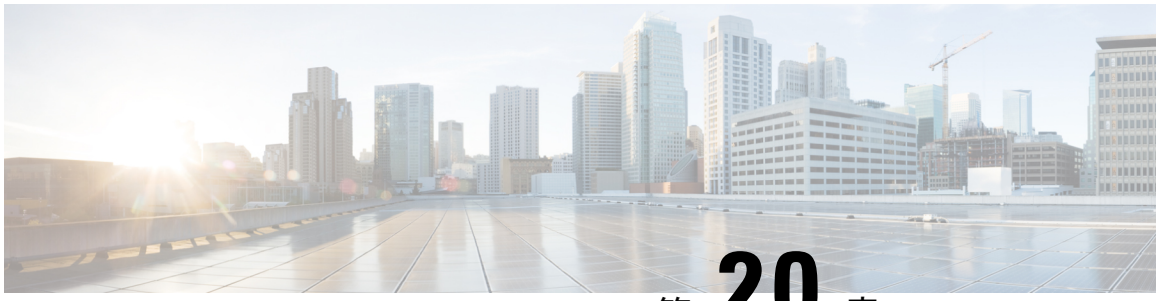
- **[SCP へのエクスポート（Export to SCP）]**を選択して、バックアップ ファイルをリモート ディレクトリに保存します。

  1. **[SCP サーバ（SCP Server）]** フィールドに、SCP サーバの IP アドレスを入力します。
  2. **[ファイル パス（File Path）]** フィールドに、バックアップ ファイルへの相対ファイル パスを入力します。
  3. **ユーザ名**と**パスワード**を該当するフィールドに入力します。
  4. **[暗号キー（Encryption Key）]** フィールドにバックアップ ファイルに対する暗号キーを入力します。

     （注） バックアップを復元するには、暗号化キーが必要です。暗号化キーは、機密情報を含むバックアップファイルの一部を暗号化するために使用されます。

  5. [バックアップ（Backup）] をクリックします。

     バックアップが完了すると、バックアップ ファイルがリモート ディレクトリに保存されます。



第 20 章

NXAPI 証明書

Cisco NX-OS スイッチを NX-API HTTPS モードで機能させるには、SSL 証明書が必要です。SSL 証明書を生成し、CA によってそれに署名することができます。証明書は、スイッチ コンソールで CLI コマンドを使用して手動でインストールすること、または Cisco Nexusダッシュボード ファブリック コントローラ を使用してスイッチにインストールすることができます。

Cisco Nexusダッシュボード ファブリック コントローラ では、NX-API 証明書を Nexusダッシュボード ファブリック コントローラ にアップロードするための Web UI フレームワークを提供しています。後で、Nexusダッシュボード ファブリック コントローラ によって管理されるスイッチに証明書をインストールできます。

（注） この機能は、Cisco NXOS バージョン 9.2(3) 以降で動作するスイッチでサポートされます。

• 証明書の生成と管理 （561 ページ）

証明書の生成と管理

データセンター管理者は、スイッチごとに ASCII（base64）エンコードの証明書を生成します。この証明書は、次の 2 つのファイルで構成されます。

- 秘密キーを含む `.key` ファイル
- 証明書を含む `.crt/.cer/.pem` ファイル

Cisco Nexusダッシュボード ファブリック コントローラ は、組み込みキー ファイル、つまり `.crt/.cer/.pem` ファイルを含む単一の証明書ファイルもサポートします。これには、`.key` ファイルの内容も含めることができます。

Nexusダッシュボード ファブリック コントローラ は、バイナリ エンコードされた証明書はサポートしていません。つまり、`.der` 拡張子の証明書はサポートされません。キー ファイルは、暗号化用のパスワードで保護できます。Cisco Nexusダッシュボード ファブリック コントローラは暗号化を義務付けていません。ただし、これは Nexusダッシュボード ファブリック

コントローラ に保存されるため、キーファイルを暗号化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 は AES 暗号化をサポートしています。

CA 署名付き証明書または自己署名証明書のいずれかを選択することができます。Cisco Nexusダッシュボード ファブリック コントローラ は署名を義務付けていません。ただし、セキュリティ ガイドラインでは、CA 署名付き証明書を使用することを推奨しています。

複数のスイッチ用に複数の証明書を生成して、Nexusダッシュボードファブリック コントローラにアップロードすることができます。証明書に適したスイッチを選択できるように、証明書に適切な名前を付けてください。

1 つの証明書と対応するキーファイルをアップロードすることも、複数の証明書とキーファイルを一括アップロードすることもできます。アップロードが完了したら、スイッチにインストールする前に、アップロード リストを確認することができます。組み込みキー ファイルを含む証明書ファイルがアップロードされた場合、Nexusダッシュボード ファブリック コントローラ は自動的にキーを取得します。

証明書とキーファイルは同じファイル名である必要があります。たとえば、証明書ファイル名が `mycert.pem` の場合、キーファイル名は `mycert.key` である必要があります。証明書とキー ペアのファイル名が同じでない場合、Nexusダッシュボード ファブリック コントローラはスイッチに証明書をインストールできません。

Cisco Nexusダッシュボード ファブリック コントローラ では、スイッチに証明書を一括インストールできます。一括インストールでは同じパスワードが使用されるため、すべての暗号化キーは同じパスワードで暗号化する必要があります。キーのパスワードが異なる場合、証明書を一括モードでインストールすることはできません。一括モードインストールでは、暗号化されたキー証明書と暗号化されていないキー証明書を一緒にインストールできますが、すべての暗号化キーは同じパスワードを持つ必要があります。

スイッチに新しい証明書をインストールすると、既存の証明書が新しい証明書に置き換えられます。

同じ証明書を複数のスイッチにインストールすることができます。ただし、一括アップロード機能は使用できません。

（注） Nexusダッシュボード ファブリック コントローラ は、提供される証明書またはオプションが有効であることを要求しません。この規則に従うかどうかは、ユーザーとスイッチの要件次第です。たとえば、スイッチ 1 のための証明書が生成されても、それがスイッチ 2 にインストールされた場合、Nexusダッシュボード ファブリック コントローラ は証明書の適用を強制しません。スイッチは、証明書のパラメータに基づいて証明書を受け入れるか、拒否するかを選択できます。

Cisco Nexusダッシュボード ファブリック コントローラ による NX-API 証明書の検証

リリース 12.0.1a 以降、Cisco Nexusダッシュボード ファブリック コントローラ はスイッチによって提供される NX-API 証明書を検証する機能をサポートしています。Cisco Nexusダッシュボード ファブリック コントローラ が行う NX-API リクエストには SSL 接続が必要です。ス

イッチはSSLサーバーのように動作し、SSLネゴシエーションの一部としてサーバー証明書を提供します。対応する CA 証明書が提供されている場合、Cisco Nexusダッシュボード ファブリック コントローラ はそれを確認できます。

（注） デフォルトでは、NX-API 証明書の検証は有効にされていません。これは、データセンター内のすべてのスイッチにCA署名付き証明書がインストールされている必要があり、Cisco Nexusダッシュボード ファブリック コントローラ には対応するすべての CA 証明書が供給されるためです。

Cisco Nexusダッシュボード ファブリック コントローラ の NX-API 証明書管理には、同じ対象を管理するためのスイッチ証明書とCA 証明書という 2 つの機能があります。

スイッチ証明書

証明書のアップロード

証明書を Nexusダッシュボード ファブリック コントローラ にアップロードするには、次の手順を実行します。

1. **[証明書のアップロード (Upload Certificate)]** をクリックして、適切な証明書ファイルをアップロードします。
2. ローカルディレクトリを参照し、Nexusダッシュボードファブリック コントローラにアップロードする必要がある証明書キーペアを選択します。

   拡張子が `.cer/.crt/.pem` および `.key` の証明書を個別に選択できます。

   Cisco Nexusダッシュボード ファブリック コントローラ では、埋め込みキーファイルを含む単一の証明書ファイルをアップロードすることもできます。キーファイルはアップロード後に自動的に取得されます。
3. **[アップロード (Upload)]** をクリックし、選択したファイルを Nexusダッシュボード ファブリック コントローラ にアップロードします。

   ファイルのアップロードに成功すると、そのことを知らせるメッセージが表示されます。アップロードされた証明書がテーブルに一覧表示されます。

   テーブルには、ステータスが UPLOADED と表示されます。証明書がキーファイルなしでアップロードされた場合、ステータスは KEY_MISSING と表示されます。

スイッチの割り当てと証明書のインストール

Cisco Nexusダッシュボード ファブリック コントローラ Web UIを使用してスイッチに証明書をインストールするには、次の手順を実行します。

1. 1 つまたは複数の証明書のチェックボックスをオンにします。

2. **[アクション (Actions)]** ドロップダウンリストから、**[スイッチの割り当てとインストール (Assign Switch & Install)]** を選択します。
3. **[NX API 証明書クレデンシャル (NX API Certificate Credentials)]** フィールドに、証明書の生成時にキーを暗号化するために使用したパスワードを入力します。

   [パスワード (Password)] フィールドは必須ですが、キーがパスワードを使用して暗号化されていない場合は、任意のランダムな文字列を入力できます（たとえばtest、installなど）。暗号化されていないファイルの場合、パスワードは使用されませんが、一括モードであるため、ランダムな文字列を入力する必要があります。

（注） 1回の一括インストールで、暗号化されていないキーと暗号化されたキーおよび証明書をインストールできます。ただし、暗号化キーに使用するキーパスワードを指定する必要があります。

4. 証明書ごとに、**[割り当て (Assign)]** の矢印をクリックし、証明書に関連付けるスイッチを選択します。
5. **[証明書のインストール (Install Certificates)]** をクリックして、それぞれのスイッチにすべての証明書をインストールします。

証明書のリンク解除と削除

証明書をスイッチにインストールすると、Nexusダッシュボードファブリック コントローラはNexusダッシュボードファブリック コントローラから証明書をアンインストールできません。ただし、スイッチにはいつでも新しい証明書をインストールできます。スイッチにインストールされていない証明書は削除できます。スイッチにインストールされている証明書を削除するには、スイッチから証明書のリンクを解除してから、Nexusダッシュボードファブリック コントローラから削除する必要があります。

（注） スイッチから証明書のリンクを解除しても、スイッチの証明書は削除されません。証明書はまだスイッチに存在します。Cisco 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の証明書を削除できません。

Nexusダッシュボード ファブリック コントローラ リポジトリから証明書を削除するには、次の手順を実行します。

1. 削除する必要がある証明書を選択します。
2. **[アクション (Actions)]** ドロップダウン リストから、**[リンク解除 (Unlink)]** を選択します

   確認メッセージが表示されます。
3. **[OK]** をクリックして、選択した証明書をスイッチからリンク解除します。

ステータス カラムには [UPLOADED] と表示されます。[Switch] カラムには [NOT_INSTALLED] と表示されます。

4. [Switch] から、現在リンク解除されている証明書を選択します。
5. **[アクション (Actions)]** ドロップダウン リストから、**[削除 (Delete)]** を選択します。

   証明書は Nexusダッシュボード ファブリック コントローラ から削除されます。

CA 証明書

証明書のアップロード

証明書を Nexusダッシュボード ファブリック コントローラ にアップロードするには、次の手順を実行します。

1. **[証明書のアップロード (Upload Certificate)]** をクリックして、適切なライセンス ファイルをアップロードします。
2. ローカルディレクトリを参照し、Nexusダッシュボードファブリック コントローラにアップロードする証明書とキーのペアを選択します。

   ファイル拡張子が `.cer/.crt/.pem` ファイル拡張子をもつ証明書を個別に選択できます。

（注） CA証明書は公開証明書であり、キーは含まれません。また、この操作にはキーは必要ありません。これは、スイッチが提供するNX-API証明書を確認するためにCisco Nexusダッシュボード ファブリック コントローラ が必要とする証明書です。つまり、CA 証明書はCisco Nexusダッシュボードファブリック コントローラ によってのみ使用され、スイッチにインストールされることはありません。

3. **[アップロード (Upload)]** をクリックし、選択したファイルを Nexusダッシュボード ファブリック コントローラ にアップロードします。

   ファイルのアップロードに成功すると、そのことを知らせるメッセージが表示されます。アップロードされた証明書がテーブルに一覧表示されます。

スイッチの割り当てと証明書のインストール

これらのCA 証明書は Cisco Nexusダッシュボード ファブリック コントローラ によってのみ使用され、スイッチにインストールされることはありません。

証明書のリンク解除と削除

CA 証明書はスイッチにインストールされないため、リンク解除する必要はありません。

CA 証明書は、特定の CA に新しい証明書を持ち込む必要があるため、削除できます。

[アクション (Actions)] ドロップダウン リストから、**[削除 (Delete)]** を選択します。証明書はNexusダッシュボード ファブリック コントローラ から削除されます。

NX-API 証明書検証の有効化

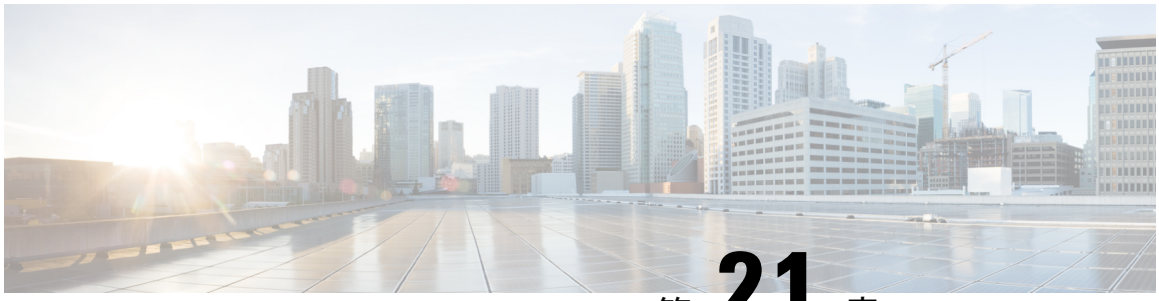
NX-API 証明書の検証は、[CA 証明書] ページのトグル ボタンを使用して有効にできます。ただし、これは、Cisco Nexusダッシュボード ファブリック コントローラ が管理するすべてのスイッチに CA 署名付き証明書がインストールされ、対応する CA ルート証明書（1つ以上）がCisco Nexusダッシュボード ファブリック コントローラ にアップロードされた後にのみ行う必要があります。これを有効にすると、Cisco Nexusダッシュボード ファブリック コントローラSSLクライアントはスイッチによって提供される証明書の検証を開始します。検証に失敗すると、NX-API コールも失敗します。

（注）

- NX-API 証明書の検証は、スイッチごとに適用できません。 all または none のいずれかです。したがって、すべてのスイッチに対応する CA 署名付き証明書がインストールされている場合にのみ、検証を有効にすることが重要です。
- また、すべての CA 証明書が Cisco Nexusダッシュボード ファブリック コントローラにインストールされている必要があります。
- 検証の問題が原因で特定のスイッチで NX-API コールが失敗した場合は、トグル ボタンを使用して適用を無効にできます。すべての結果は、以前の状態に戻ります。
- 上記の点から、メンテナンス期間中に適用を有効にする必要があります。

第 V 部

サービスの統合



第 21 章

エンドポイント ロケータ

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。

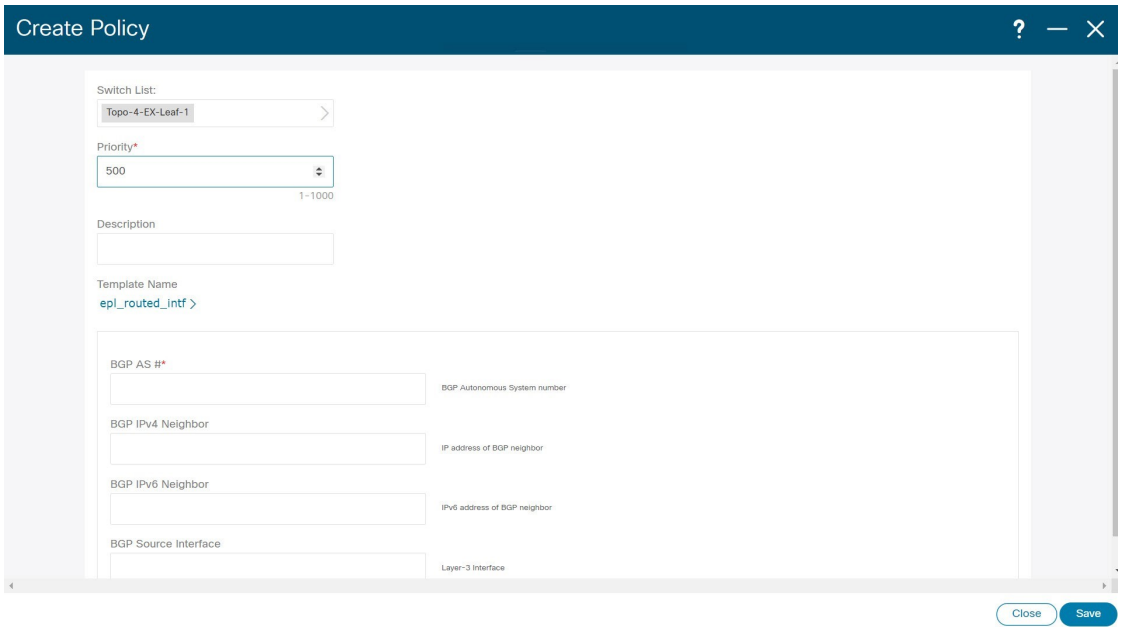
- 管理
- データ

（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。

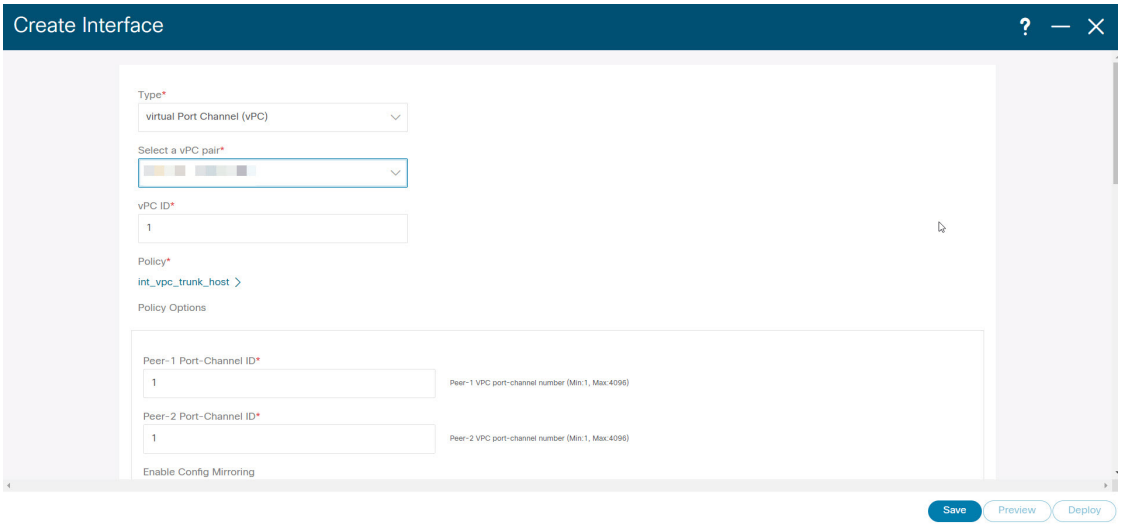
Note Nexusダッシュボード ファブリック コントローラ 上のデータ ネットワーク インターフェイスのセットアップは、ファブリック内のデバイスへのインバンド接続を必要とするアプリケーションの前提条件です。これには EPL とネットワーク インサイトのリソース（NIR）が含まれます。

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。

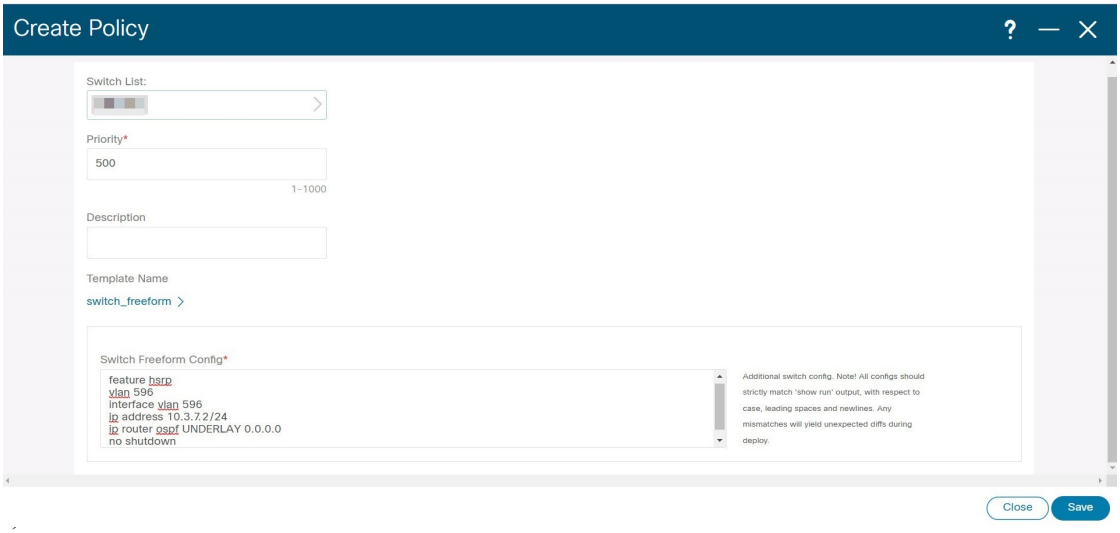


ただし、冗長性を確保するために、がインストールされているサーバをデュアルホームまたはデュアル接続にすることをお勧めします。Nexusダッシュボード ファブリック コントローラ OVA導入では、ポートチャネルを介してサーバをスイッチに接続できます。Nexusダッシュボー

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。

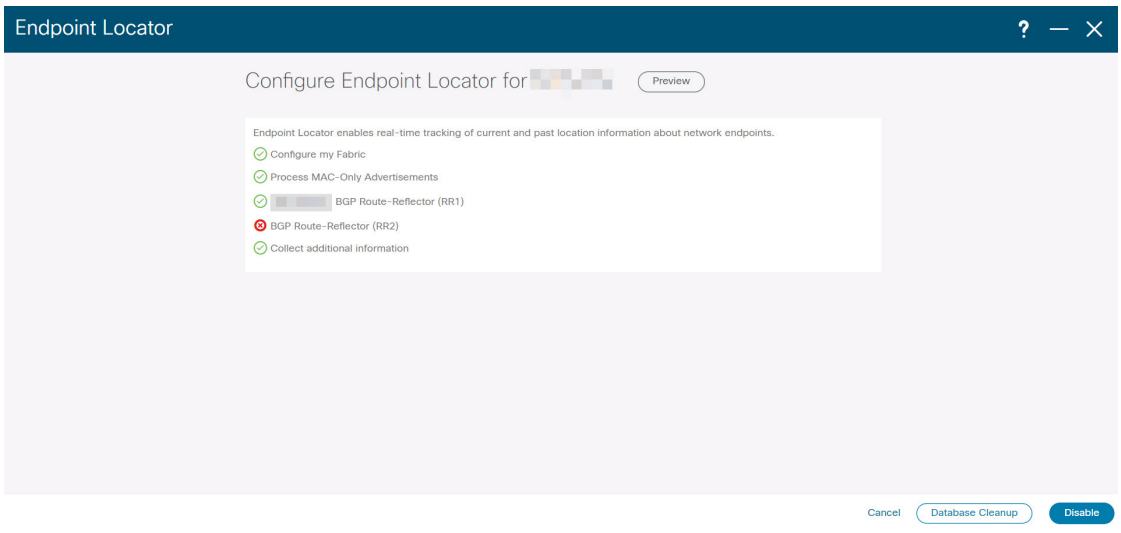
物理または仮想とファブリック間のインバンド接続を確立した後、BGPピアリングを確立できます。Nexusダッシュボード ファブリック コントローラ

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 330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。

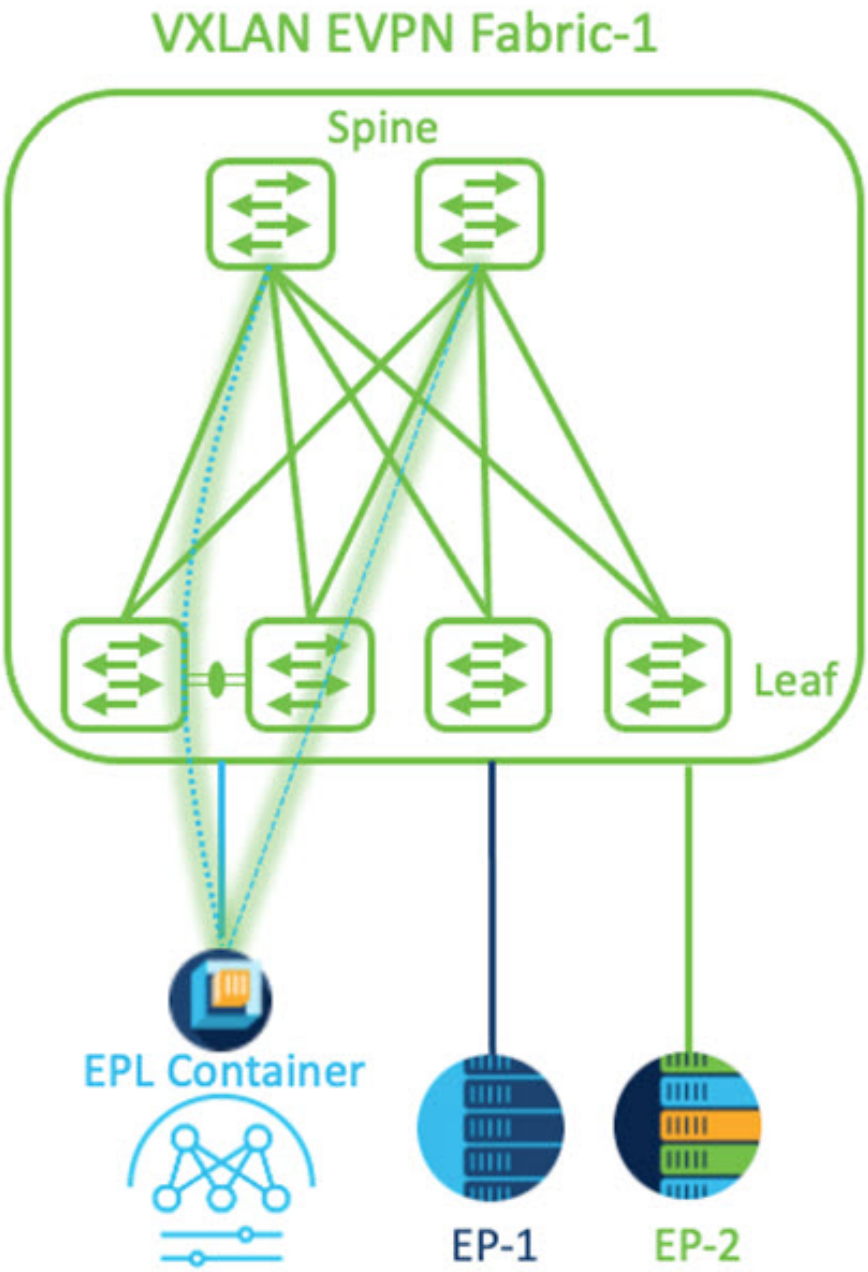
ステップ 2 [Delete]をクリックして続行するか、[Cancel]をクリックして中止します。

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

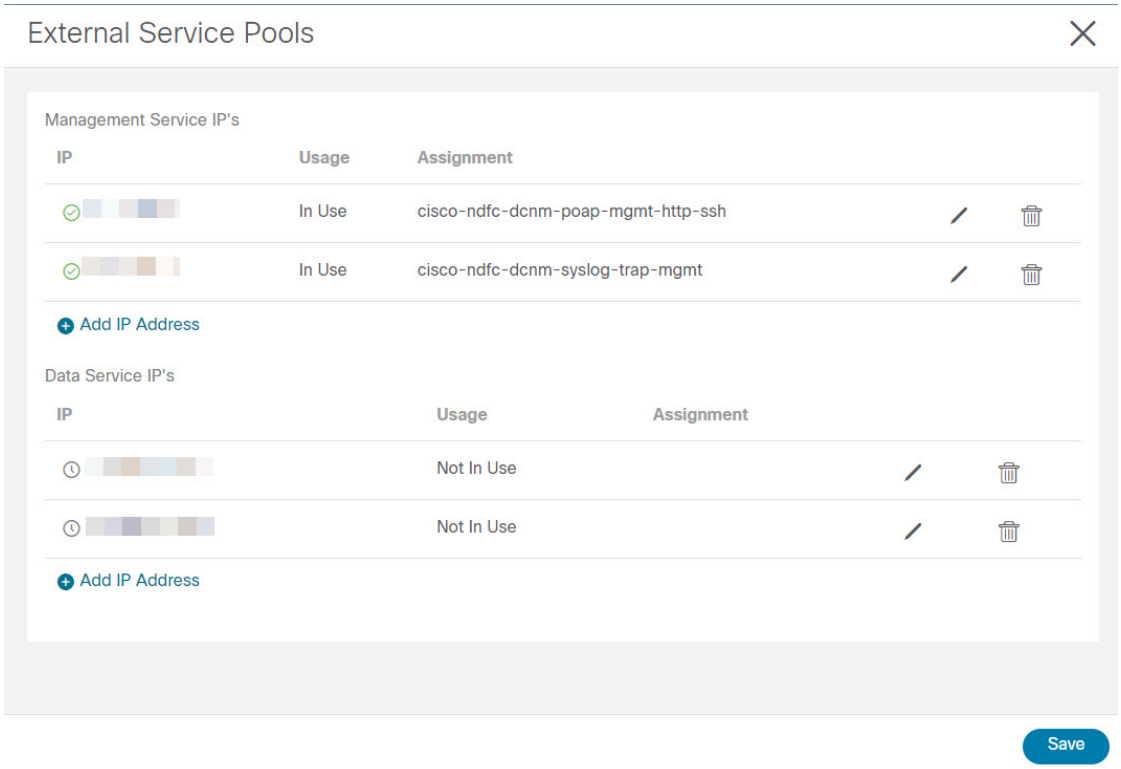
ステップ 1 Cisco Nexus Dashboard で永続 IP アドレスを構成する必要があります。Nexus Dashboard で、**[管理コンソール（Admin Console）]**>**[インフラストラクチャ（Infrastructure）]**>**[クラスタ構成（Cluster Configuration）]**を選択します。

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。

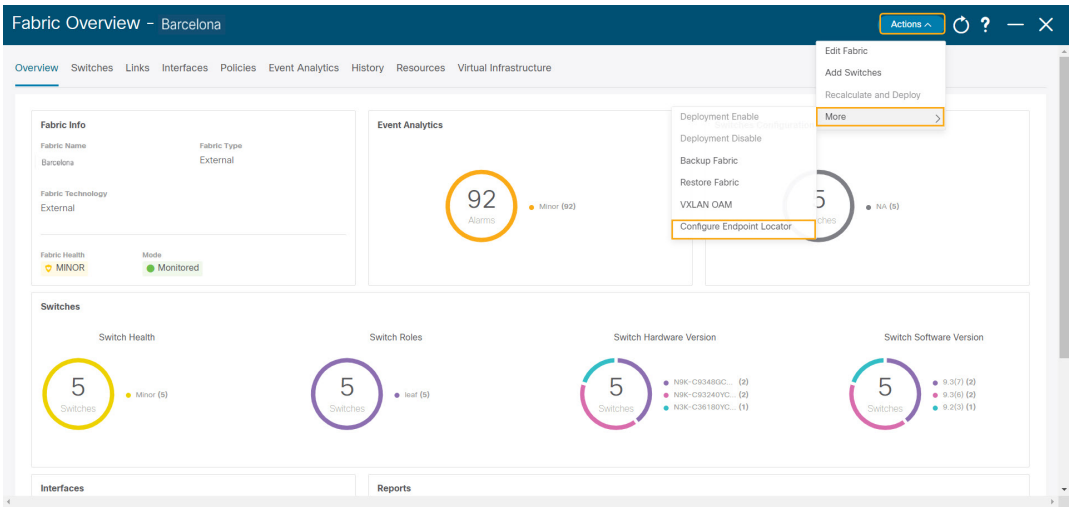
```
[rescue-user@ndfc-12-parth ~]$ ping 192.168.100.254 -c 2
PING 192.168.100.254 (192.168.100.254) 56(84) bytes of data.
64 bytes from 192.168.100.254: icmp_seq=1 ttl=255 time=1.95 ms
64 bytes from 192.168.100.254: icmp_seq=2 ttl=255 time=2.09 ms

--- 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。

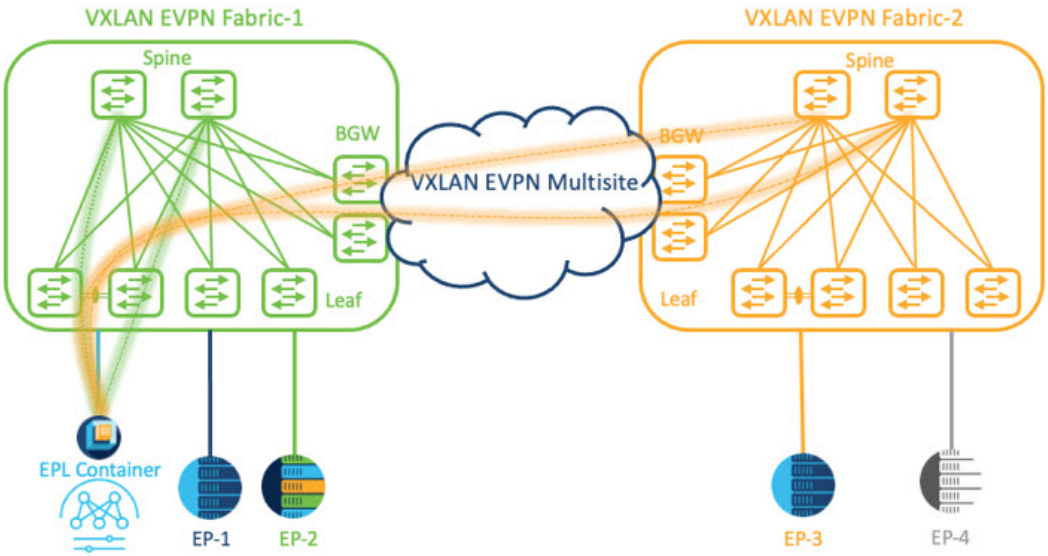
適切な選択を行い、さまざまな入力を確認したら、**[構成の保存（Save Config）]**をクリックして、EPL を有効にします。EPL の有効化中にエラーが発生した場合は、有効化プロセスが中止され、適切なエラーメッセージが表示されます。それ以外の場合、EPLは正常に有効化されます。EPL が有効になると、永続 IP が使用されます。

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。

（注） これは、Nexus Dashboard Fabric Controller、Release 12.0.1a のフィーチャのプレビューです。ラボセットアップでのみ、ベータ版としてマークされたこの機能を使用することをお勧めします。実稼働環境でこれらのフィーチャを使用しないでください。

エンドポイント ロケータの削除

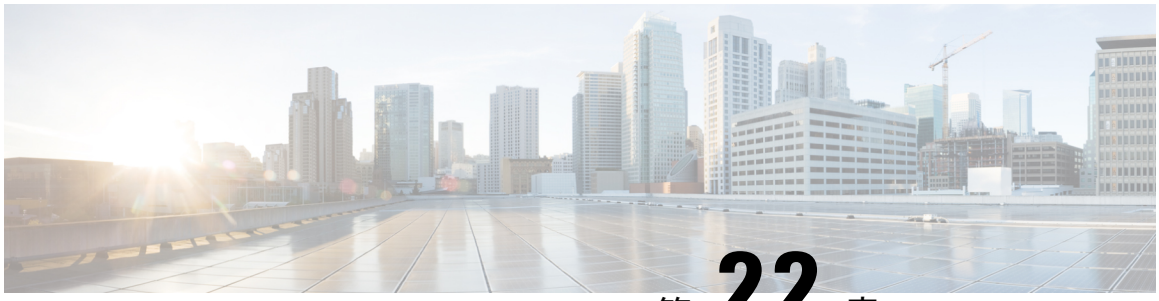
Cisco Nexusダッシュボード ファブリック コントローラ Web UI からエンドポイント ロケータを無効にするには、次の手順を実行します。

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。

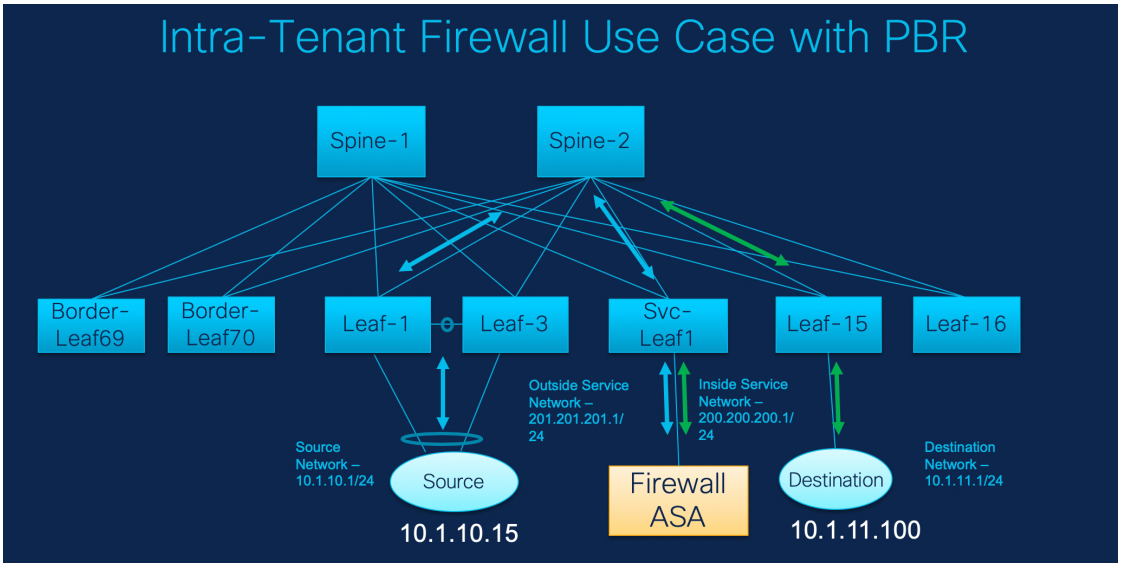


第 22 章

L4～L7 サービスのユースケース

ユースケース：ポリシーベースのルーティングを使用したテナント内ファイアウォール

トポロジの詳細については、以下の図を参照してください。



このトポロジでは、Leaf1 と Leaf3 は vPC ペアであり、**Source**（10.1.10.15）に **Source Network**（10.1.10.1/24）で接続されています。サービス リーフは仮想 **Firewall ASA** に接続され、リーフ 15 は **Destination**（10.1.11.100）に接続されます。このユース ケースでは、送信元ネットワークは「クライアント」を指し、宛先は「サーバー」を指します。

Source から **Destination** へ横断するトラフィックはすべて外部サービス ネットワークに送られる必要があり、ファイアウォールはトラフィックを許可または拒否する機能を実行します。その後、このトラフィックは内部サービス ネットワークにルーティングされ、宛先ネットワークに送信されます。トポロジはステートフルであるため、宛先から送信元に戻ってくるトラフィックは同じパスをたどります。

次に、NDFC でサービス リダイレクトを実行する方法を見てみましょう。

Note

- この使用例では、**Site_A** VXLAN ファブリックをプロビジョニングする方法については説明していません。このトピックの詳細については、『Cisco Nexus Dashboard Fabric Controller for LAN Configuration Guide』を参照してください。
- このユースケースは、サービス ノード（ファイアウォールまたはロード バランサ）の構成には対応していません。

以下のいずれかのパスを使用して、[サービス（Services）] タブに移動します。

[LAN] > [サービス（Services）]

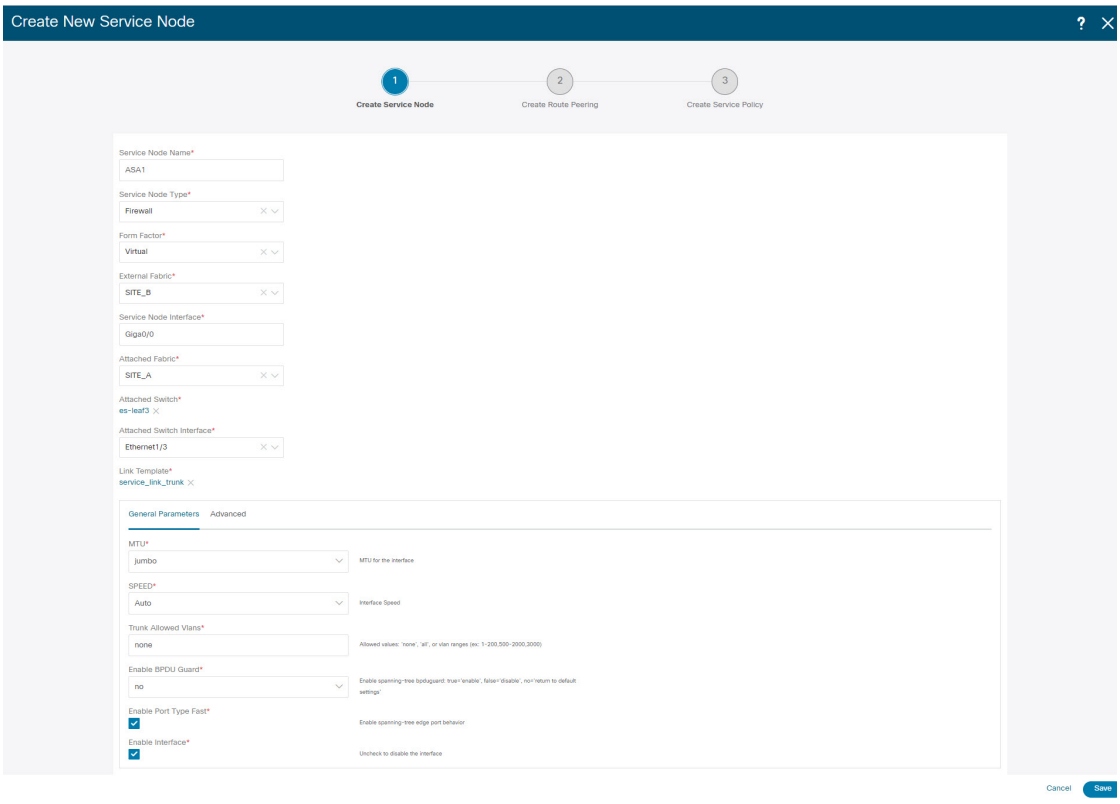
[LAN] > [ファブリック（Fabrics）] > [ファブリックの概要（Fabric Overview）] > [サービス（Services）]

[LAN] > [スイッチ（Switches）] > [スイッチの概要（Switches Overview）] > [サービス（Services）]

1. サービス ノードの作成

Procedure

ステップ 1 **[LAN] > [ファブリック（Fabrics）] > [ファブリックの概要（Fabric Overview）] > [サービス（Services）]** へ移動します。



ステップ 2 **[サービス（Service）]** タブで、**[アクション（Actions）]** > **[追加（Add）]**を選択します。

ステップ 3 サービス ノード名を入力し、**[ファイアウォール（Firewall）]** を **[タイプ（Type）]** ドロップダウン ボックスで指定します。

[サービス ノード名（Service Node Name）] は一意である必要があります。

ステップ 4 **[フォーム ファクター（Form Factor）]** ドロップダウン リストから、**[仮想（Virtual）]** を選択します。

ステップ 5 ドロップダウン リストから **[外部ファブリック（External Fabric）]** を選択し、サービス ノード（たとえば、ASA ファイアウォール）が配置されている外部ファブリックを選択します。

Note サービス ノードが外部ファブリックに属する必要があることを確認します。これは、サービス ノードを作成する際の前提条件です。

ステップ 6 サービス リーフに接続するサービスノードのインターフェイス名を入力します。

ステップ 7 サービス リーフである接続されたスイッチと、サービス リーフ上の対応するインターフェイスを選択します。

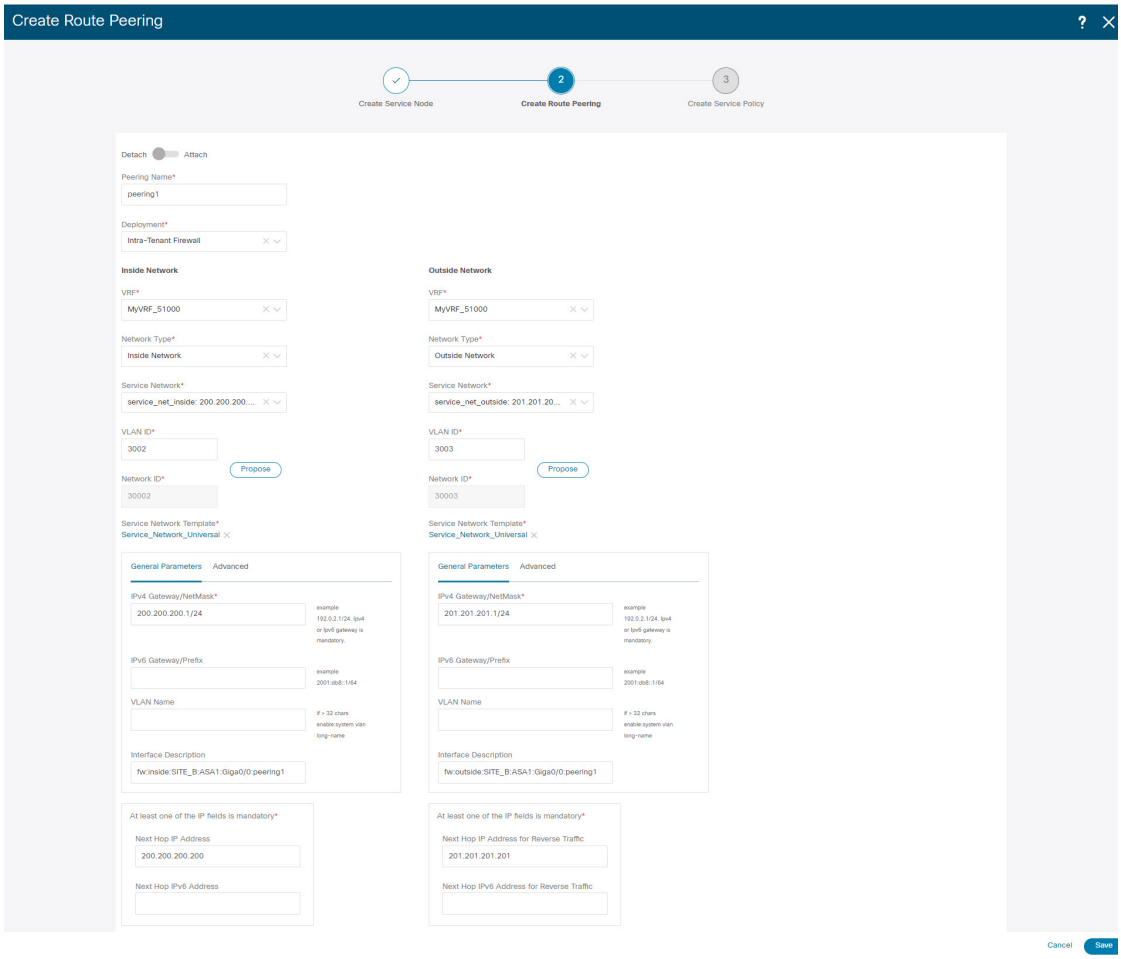
ステップ 8 **service_link_trunk** テンプレートを選択します。NDFC は、トランク、ポート チャネル、および vPC リンク テンプレートをサポートします。**[リンク テンプレート（Link Template）]** ドロップダウン リストで使用可能なリンク テンプレートは、選択した **[接続スイッチ インターフェイス （Attached Switch Interface）]** のタイプに基づいてフィルタリングされます。

ステップ 9 必要に応じて、**[一般パラメータ（General Parameters）]** と **[詳細（Advanced）]** パラメータを指定します。一部のパラメータには、デフォルト値が事前に入力されています。

ステップ 10 **[保存（Save）]** をクリックして、作成したサービス ノードを保存します。

2. ルート ピアリングの作成

サービス リーフとサービス ノード間のピアリングを構成しましょう。



Procedure

ステップ 1 ピアリング名を入力し、**[テナント内ファイアウォール（Intra-Tenant Firewall）]** を **[展開（Deployment）]** ドロップダウン リストから選択します。

ステップ 2 **[内部ネットワーク（Inside Network）]** で、**[VRF]** ドロップダウン リストから存在する VRF を選択し、**[内部ネットワーク（Inside Network）]** を **[ネットワーク タイプ（Network Type）]** で選択します。

[サービス ネットワーク（Service Network）] の名前を入力し、**[Vlan ID]** を指定します。**[提案（Propose）]** をクリックして、NDFC が次に使用可能な VLAN ID をファブリック設定で指定

されたサービス ネットワーク VLAN ID の範囲からフェッチできるようにすることもできます。デフォルトの**[サービス ネットワーク テンプレート（Service Network Template）]** は **Service_Network_Universal** です。

[一般パラメータ（General Parameters）] タブで、サービス ネットワークのゲートウェイ アドレスを指定します。**[ネクストホップ IP アドレス（Next Hop IP Address）]** を指定します。このネクスト ホップ アドレスは、「内部サービス ネットワーク」サブネット内にある必要があります。**[詳細設定（Advanced）]** タブの、デフォルトの **[ルーティング タグ（Routing Tag）]** 値は 12345 です。

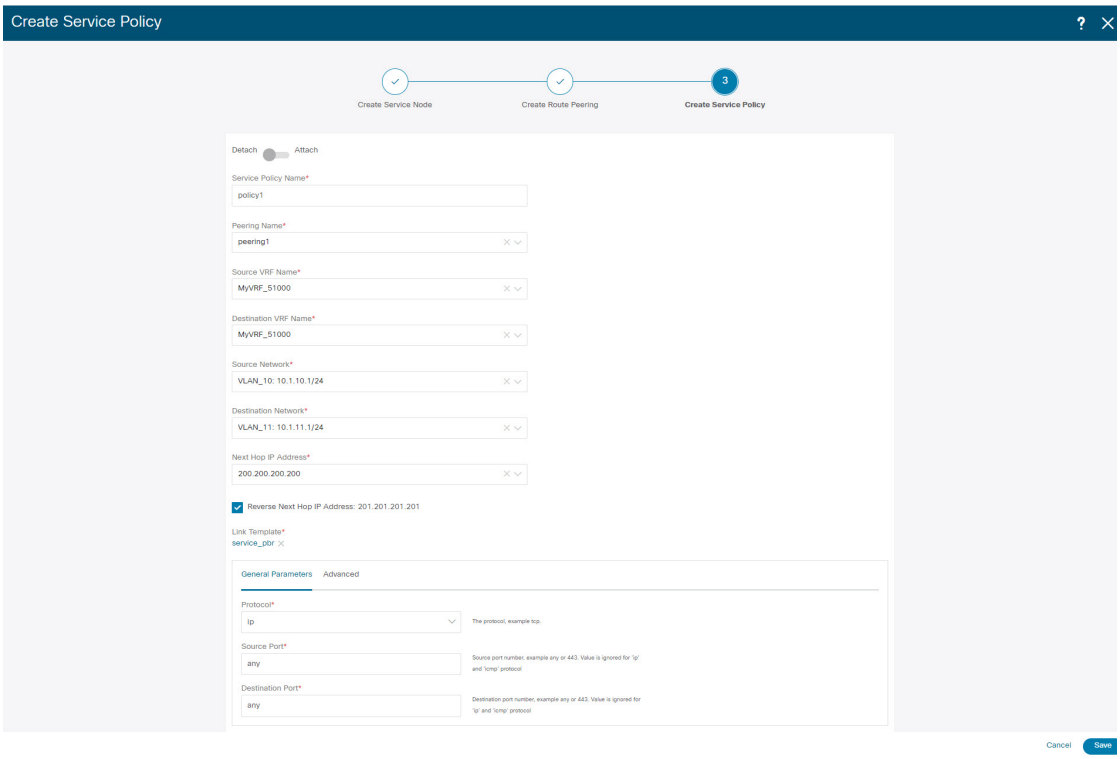
ステップ 3 **[外部ネットワーク（Outside Network）]** で必要なパラメータを指定し、**[リバース トラフィックのネクスト ホップ IP アドレス（Next Hop IP Address for Reverse Traffic）]** を指定します。リバース トラフィックのこのネクスト ホップ アドレスは、「外部サービス ネットワーク」サブネット内にある必要があります。

ステップ 4 **[保存（Save）]** をクリックして、作成したルート ピアリングを保存します。

3. サービスポリシーの作成

Procedure

ステップ 1 ポリシーの名前を指定し、**[ピアリング名（Peering Name）]** ドロップダウン リストからルート ピアリングを選択します。



ステップ 2 **[送信元 VRF 名（Source VRF Name）]** および **[宛先 VRF 名（Destination VRF Name）]** ドロップダウン リストから、送信元および宛先 VRF を選択します。テナント内ファイアウォール展開の送信元と宛先の VRF は同じである必要があります。

ステップ 3 **[送信元ネットワーク（Source Network）]** および **[宛先ネットワーク（Destination Network）]** ドロップダウン リストから、送信元ネットワークと宛先ネットワークを選択するか、**[ファブリックの概要（Fabric Overview）]**>**[サービス（Services）]**ウィンドウで定義されたネットワーク サブネット内にある送信元ネットワークまたは宛先ネットワークを指定します。

ステップ 4 ネクスト ホップおよびリバース ネクスト ホップのフィールドは、ルート ピアリングの作成中に入力された値に基づいて入力されます。**[リバース ネクスト ホップ IP アドレス（Reverse Next Hop IP Address）]** フィールドの横にあるチェック ボックスをオンにして、リバース トラフィックに対するポリシーの適用を有効にします。

ステップ 5 ポリシー テンプレートの **[一般パラメータ（General Parameters）]** タブで、**[ip]** を **[プロトコル（Protocol）]** ドロップダウン リストから選択します。また、**[任意（any）]** を **[送信元ポート（Source Port）]** および **[宛先ポート（Destination Port）]** フィールドで指定します。

Note **ip** および **icmp** プロトコルの場合、**任意**の送信元ポートと宛先ポートが ACL 生成に使用されます。別のプロトコルを選択して、対応する送信元ポートと宛先ポートを指定することもできます。NDFCは、既知のポート番号をスイッチで必要な形式に一致するように変換します。たとえば、ポート 80 を「www」に変換できます。

ステップ 6 **[詳細設定（Advanced）]** タブでは、**許可**が**[ルート マップ アクション（Route Map Action）]** のデフォルト、**なし**が**[ネクスト ホップ オプション（Next Hop Option）]** のデフォルトになっています。必要に応じて、これらの値を変更し、ACL 名とルート マップの一致シーケンス番

号をカスタマイズできます。詳細については、『レイヤ4～レイヤ7サービス構成ガイド』のテンプレート （Templates）, on page 425 を参照してください。

ステップ7 **[保存（Save）]** をクリックして、作成したサービス ポリシーを保存します。

これで、リダイレクトのフローを実行して指定する手順は完了です。

5. サービス ポリシーの展開

1. **[サービス（Services）]** タブの **[サービス ポリシー（Service Policy）]** ウィンドウで、必要なピアリングを選択します。
2. **[アクション（Actions）]** > **[展開（Deploy）]** を選択します。

   [サービス ポリシーの展開（Deploy Service Policy）] ウィンドウが表示されます
3. **[展開（Deploy）]** をクリックして展開を確認します。

4. ルート ピアリングを展開する

1. **[サービス（Services）]** タブの **[ルート ピアリング（Route Peering）]** ウィンドウで、必要なピアリングを選択します。
2. **[アクション（Actions）]** > **[展開（Deploy）]** を選択します。

   [ルート ピアリングの展開（Deploy Route Peering）]ウィンドウが表示されます。
3. **[展開（Deploy）]** をクリックして展開を確認します。

6. 統計情報を表示する

それぞれのリダイレクト ポリシーが展開されたので、対応するトラフィックはファイアウォールにリダイレクトされます。

このシナリオを NDFC で視覚化するには、サービス ポリシーをクリックします。スライドイン ペインが表示されます。

指定した時間範囲のポリシーの累積統計を表示できます。

次の統計が表示されます。

- 送信元スイッチでの転送トラフィック
- 宛先スイッチでのリバース トラフィック
- サービス スイッチの双方向のトラフィック

7. Fabric Builder でのトラフィック フローの表示

外部ファブリックのサービス ノードはサービス リーフにアタッチされ、この外部ファブリックは NDFC トポロジで雲のアイコンとして表示されます。

Procedure

ステップ 1 サービス リーフをクリックすると、スライドイン ペインが表示されます。**[さらにフローを表示（Show more flows）]** をクリックします。リダイレクトされるフローを確認できます。

ステップ 2 **[詳細（Details）]**（**[サービス フロー（Service Flows）]** ウィンドウ）をクリックして、アタッチメントの詳細を表示します。

8.[トポロジ（Topology）]ウィンドウでの宛先へリダイレクトされたフローの視覚化

Procedure

ステップ 1 **[トポロジ（Topology）]** をクリックし、リーフをクリックして、宛先にリダイレクトされたフローを視覚化します。

ステップ 2 ドロップダウンリストから**[リダイレクトされたフロー（Redirected Flows）]**を選択します。

ステップ 3 ドロップダウンリストからポリシーを選択するか、検索フィールドにポリシー名、送信元ネットワーク、および宛先ネットワークを入力して検索を開始します。検索フィールドへの入力を始めると、自動的に補完されます。

送信元ネットワークと宛先ネットワークがアタッチされていて、フローがリダイレクトされているスイッチが、強調表示されます。

ステップ 4 サービス ノードは、トポロジ ウィンドウのリーフ スイッチに点線で接続されているように表示されます。点線にカーソルを合わせると、インターフェイスの詳細が表示されます。

送信元からのトラフィックは、ファイアウォールが構成されているサービス リーフを横断します。

ファイアウォール ルールに基づいて、トラフィックは宛先であるリーフ 15 に到達することが許可されます。

ユースケース：eBGP ピアリングを使用したテナント間ファイアウォール

トポロジの詳細については、以下の図を参照してください。

このトポロジでは、es-leaf1 と es-leaf2 が vPC ボーダー リーフ スイッチです。

次に、NDFC でサービス リダイレクトを実行する方法を見てみましょう。

このユースケースは、次の手順で構成されます。

Note

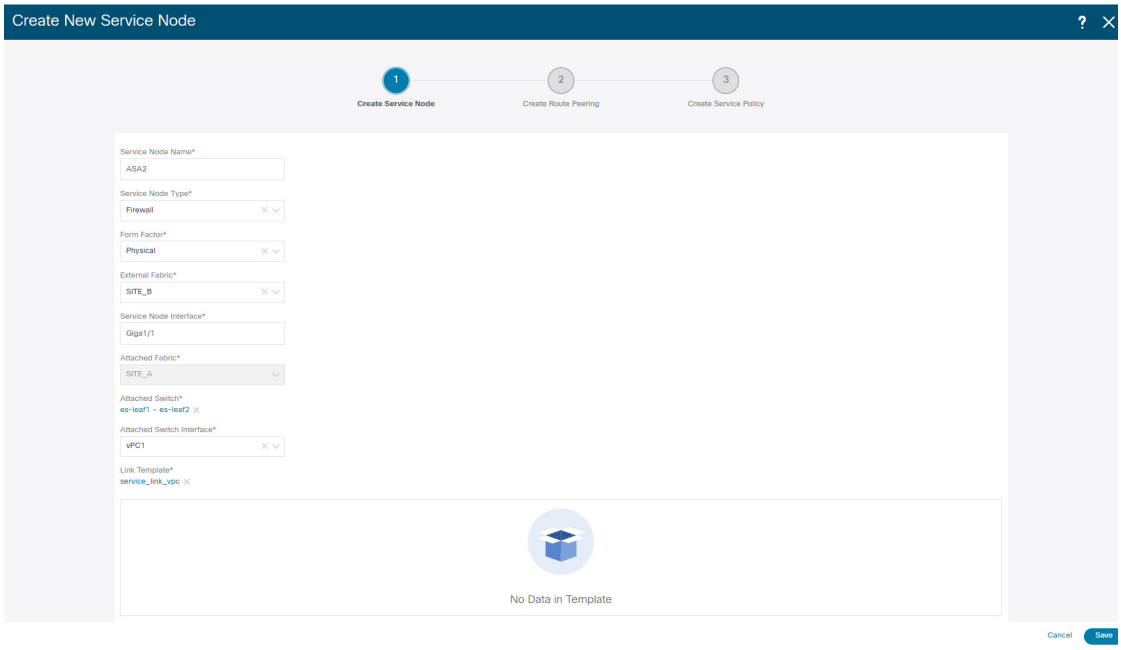
- 一部の手順は、テナント内ファイアウォールの展開のユース ケースで示されている手順に似ているため、そのユース ケースの手順への参照リンクが追加されています。
- サービス ポリシーは、テナント間ファイアウォールの展開には適用されません。

1. サービス ノードの作成

Procedure

ステップ 1 **[LAN]** > **[ファブリック（Fabrics）]** > **[ファブリックの概要（Fabric Overview）]** > **[サービス（Services）]** へ移動します。

ステップ 2 **[サービス（Service）]** タブで、**[アクション（Actions）]** > **[追加（Add）]**を選択します。



ステップ 3 サービス ノード名を入力し、[タイプ（Type）] ドロップダウン ボックスで**[ファイアウォール（Firewall）]** を指定します。**[サービス ノード名（Service Node Name）]** は一意である必要があります。

ステップ 4 **[フォーム ファクター（Form Factor）]** ドロップダウン リストから、**[仮想（Virtual）]** を選択します。

ステップ 5 **[外部ファブリック（External Fabric）]** ドロップダウン リストから、サービス ノード（たとえば、ASA ファイアウォール）が配置されている外部ファブリックを選択します。サービス ノードは外部ファブリックに属している必要があることに注意してください。これは、サービス ノードを作成する際の前提条件です。

ステップ 6 サービス リーフに接続するサービスノードのインターフェイス名を入力します。

ステップ 7 サービス リーフである接続されたスイッチと、サービス リーフ上の対応するインターフェイスを選択します。

ステップ 8 **service_link_trunk** テンプレートを選択します。NDFC は、トランク、ポート チャネル、および vPC リンク テンプレートをサポートします。**[リンク テンプレート（Link Template）]** ドロップダウン リストで使用可能なリンク テンプレートは、選択した **[接続スイッチ インターフェイス （Attached Switch Interface）]** のタイプに基づいてフィルタリングされます。

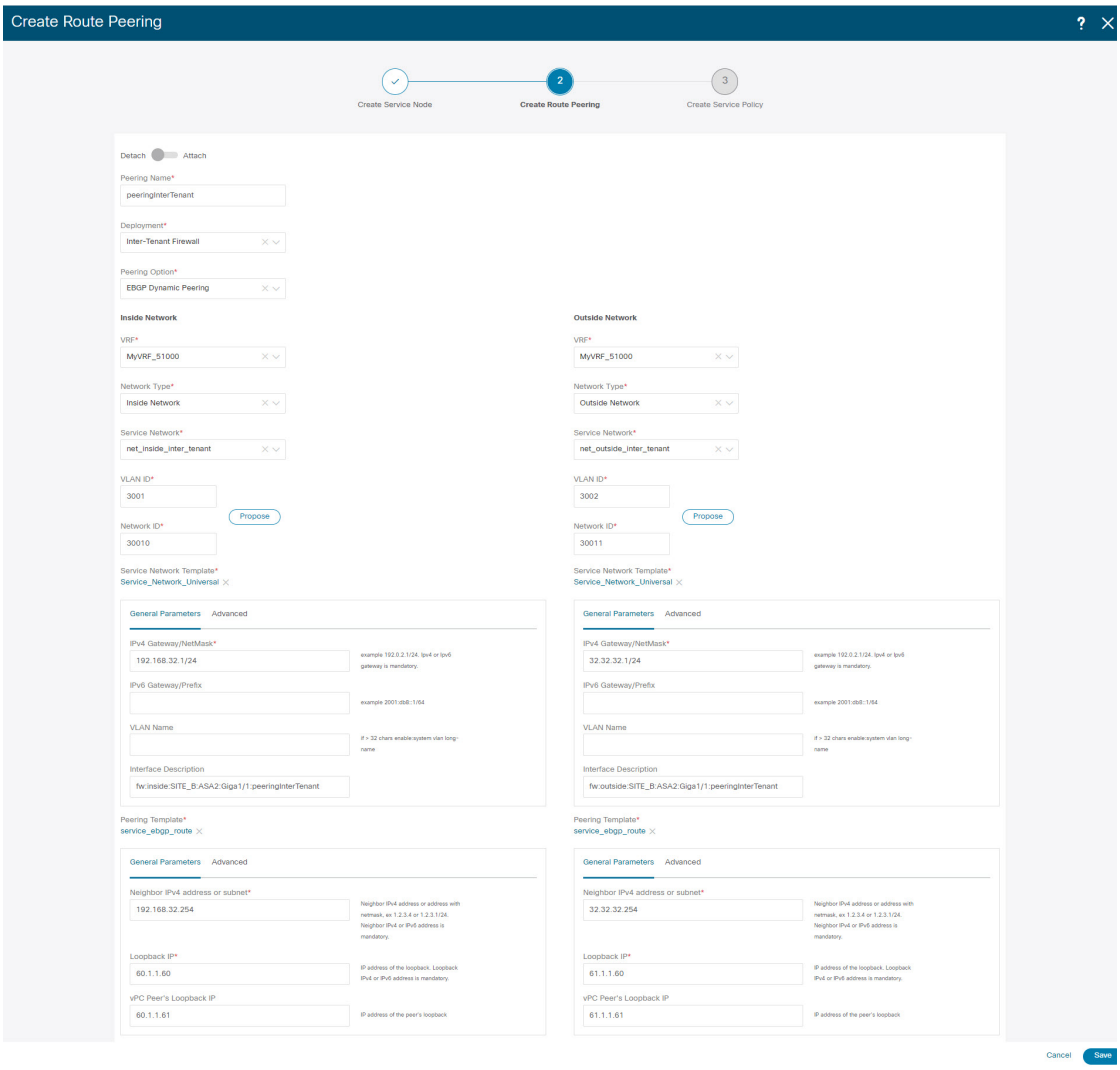
ステップ 9 必要に応じて、**[一般パラメータ（General Parameters）]** と **[詳細（Advanced）]** を指定します。一部のパラメータには、デフォルト値が事前に入力されています。

ステップ 10 **[保存（Save）]** をクリックして、作成したサービス ノードを保存します。

Note その他のサンプル スクリーンショットについては、ポリシー ベースのルーティング ユース ケースでのテナント内ファイアウォールの 1. サービス ノードの作成, on page 590 セクションを参照してください。

2. ルート ピアリングの作成

サービス リーフとサービス ノード間のピアリングを構成しましょう。



Procedure

ステップ 1 ピアリング名を入力し、**[テナント間ファイアウォール（Inter-Tenant Firewall）]** を **[展開（Deployment）]** ドロップダウン リストから選択します。**[ピアリング オプション（Peering Option）]** ドロップダウン リストから、**[eBGP ダイナミック ピアリング（eBGP Dynamic Peering）]** を選択します。

ステップ 2 **[内部ネットワーク（Inside Network）]** を **[VRF]** ドロップダウン リストで選択し、存在する VRF を選択し、**[内部ネットワーク（Inside Network）]** を**[ネットワーク タイプ（Network Type）]** で選択します。

[サービス ネットワーク（Service Network）] の名前を入力し、**[Vlan ID]** を指定します。**[提案（Propose）]** をクリックして、NDFC が次に使用可能な VLAN ID をファブリック設定で指定されたサービス ネットワーク VLAN ID の範囲からフェッチできるようにすることができます。デフォルトの**サービス ネットワーク テンプレート**は **Service_Network_Universal** です。

[一般パラメータ（General Parameters）] タブで、サービス ネットワークのゲートウェイ アドレスを指定します。**[ネクストホップ IP アドレス（Next Hop IP Address）]** を指定します。このネクスト ホップ アドレスは、「内部サービス ネットワーク」サブネット内にある必要があります。**[詳細設定（Advanced）]** タブの、デフォルトの **[ルーティング タグ（Routing Tag）]** 値は 12345 です。

ステップ 3 eBGP ダイナミック ピアリングのデフォルトのピアリング テンプレートは、**service_ebgp_route** です。

[一般パラメータ（General Parameters）] タブで、**[ネイバー IPv4（Neighbor IPv4）]** アドレス、**[ループバック IP（Loopback IP）]** アドレス、および **[vPC ピアのループバック IP（vPC Peer's Loopback IP）]** アドレスを指定します。ボーダー スイッチは vPC ペアです。

ステップ 4 **[詳細設定（Advanced）]** タブで、**[ローカル ASN（Local ASN）]** を指定し、**[ホスト ルートのアドバタイズ（Advertise Host Routes）]** チェックボックスをオンにします。このローカル ASN 値は、スイッチのシステム ASN を上書きするために使用され、ルーティング ループを回避するために必要です。

[ホスト ルートのアドバタイズ（Advertise Host Routes）] チェック ボックスがオンになっている場合、/32 および /128 ルートが表示されます。このチェックボックスが選択されていない場合、プレフィックス ルートが表示されます。

デフォルトでは、**[インターフェイスの有効化（Enable Interface）]** チェックボックスがオンになっています。

ステップ 5 **[外部ネットワーク（Outside Network）]** で必要なパラメータを指定し、**[リバース トラフィックのネクスト ホップ IP アドレス（Next Hop IP Address for Reverse Traffic）]** を指定します。リバース トラフィックのこのネクスト ホップ アドレスは、「外部サービス ネットワーク」サブネット内にある必要があります。

ステップ 6 eBGP ダイナミック ピアリングのデフォルトのピアリング テンプレートは、**service_ebgp_route** です。

[一般パラメータ（General Parameters）] タブで、**[ネイバー IPv4（Neighbor IPv4）]** アドレス、**[ループバック IP（Loopback IP）]** アドレス、および **[vPC ピアのループバック IP（vPC Peer's Loopback IP）]** アドレスを指定します。リーフ スイッチは vPC ペアです。

ステップ 7 **[詳細設定（Advanced）]** タブで、**[ローカル ASN（Local ASN）]** を指定し、**[ホスト ルートのアドバタイズ（Advertise Host Routes）]** チェックボックスをオンにします。このローカル ASN 値は、スイッチのシステム ASN を上書きするために使用され、ルーティング ループを回避するために必要です。

[ホスト ルートのアドバタイズ（Advertise Host Routes）] チェック ボックスがオンになっている場合、/32 および /128 ルートがアドバタイズされます。このチェックボックスが選択されていない場合、プレフィックス ルートがアドバタイズされます。

デフォルトでは、**[インターフェイスの有効化（Enable Interface）]** チェックボックスがオンになっています。

ステップ 8 **[保存（Save）]** をクリックして、作成したルート ピアリングを保存します。

3. ルート ピアリングを展開する

テナント内ファイアウォール展開のユースケースの 4. ルート ピアリングを展開する, on page 595 を参照してください。**InterTenantFW** が **[展開（Deployment）]** の下に表示されていることを確認します。

このユースケースの vPC ボーダー リーフの BGP 設定を以下に示します。

```
router bgp 12345
 router-id 10.2.0.1
 address-family l2vpn evpn
  advertise-pip
 neighbor 10.2.0.4
  remote-as 12345
  update-source loopback0
  address-family l2vpn evpn
   send-community
    send-community extended
 vrf myvrf_50001
  address-family ipv4 unicast
   advertise l2vpn evpn
   redistribute direct route-map fabric-rmap-redist-subnet
   maximum-paths ibgp 2
  address-family ipv6 unicast
   advertise l2vpn evpn
   redistribute direct route-map fabric-rmap-redist-subnet
   maximum-paths ibgp 2
  neighbor 192.168.32.254
   remote-as 9876
  local-as 65501 no-prepend replace-as // Note: This configuration corresponds to the
Local ASN template parameter value of the service_ebgp_route template of the inside
network with VRF myvrf_50001. The no-prepend replace-as keyword is generated along with
 the local-as command.
  update-source loopback2
  ebgp-multihop 5
  address-family ipv4 unicast
   send-community
   send-community extended
   route-map extcon-rmap-filter-allow-host out
vrf myvrf_50002
 address-family ipv4 unicast
  advertise l2vpn evpn
  redistribute direct route-map fabric-rmap-redist-subnet
  maximum-paths ibgp 2
 address-family ipv6 unicast
  advertise l2vpn evpn
  redistribute direct route-map fabric-rmap-redist-subnet
  maximum-paths ibgp 2
 neighbor 32.32.32.254
  remote-as 9876
  local-as 65502 no-prepend replace-as // Note: This configuration corresponds to the
Local ASN template parameter value of the service_ebgp_route template of the outside
network with VRF myvrf_50002. The no-prepend replace-as keyword is generated along with
 the local-as command.
  update-source loopback3
  ebgp-multihop 5
  address-family ipv4 unicast
   send-community
   send-community extended
   route-map extcon-rmap-filter-allow-host out
```

このユースケースの vPC スイッチ es-leaf1 のループバック インターフェイス設定を以下に示します。構成のループバック インターフェイスは、**service_ebgp_route** テンプレートの「ループバック IP」パラメータに対応します。**[ループバック IP（Loopback IP）]** パラメータ値（**service_ebgp_route** テンプレートで指定されたもの）を使用して、2 つの個別の VRF インスタンスの各 vPC スイッチに 2 つのループバック インターフェイスが自動的に作成されます。

```
interface loopback2
 vrf member myvrf_50001
 ip address 60.1.1.60/32 tag 12345
interface loopback3
 vrf member myvrf_50002
 ip address 61.1.1.60/32 tag 12345
```

vPC ピア スイッチ es-leaf2 のループバック インターフェイス設定：

```
interface loopback2
 vrf member myvrf_50001
 ip address 60.1.1.61/32 tag 12345
interface loopback3
 vrf member myvrf_50002
 ip address 61.1.1.61/32 tag 12345
```

ユースケース: ワンアーム ロード バランサ

トポロジの詳細については、以下の図を参照してください。

このトポロジでは、es-leaf1 と es-leaf2 が vPC リーフです。

次に、NDFC でサービス リダイレクトを実行する方法を見てみましょう。

以下のいずれかのパスを使用して、**[サービス（Services）]** タブに移動できます。

[LAN] > **[サービス（Services）]**

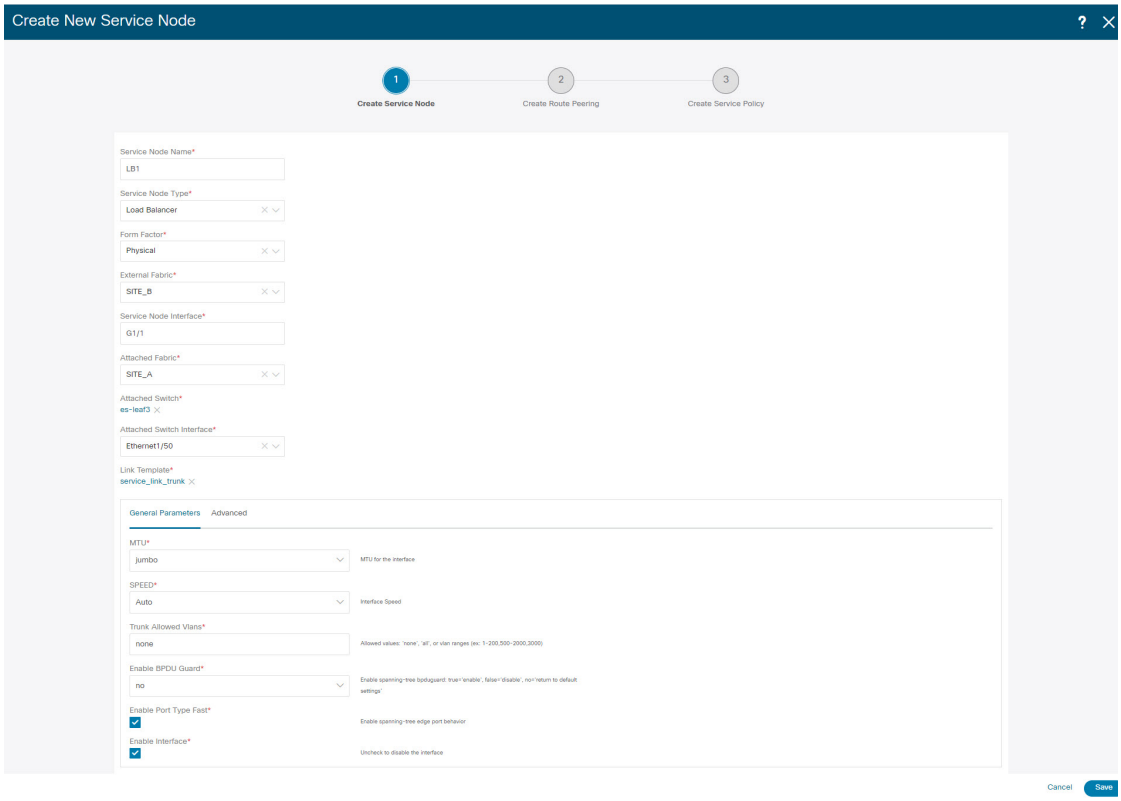
このユースケースは、次の手順で構成されます。

Note 一部の手順は、テナント内ファイアウォール展開のユースケースで示されている手順に似ているため、そのユースケースの手順に提供されているリンクを参照してください。

1. サービス ノードの作成

Procedure

ステップ 1 **[LAN]** > **[ファブリック（Fabrics）]** > **[ファブリックの概要（Fabric Overview）]** > **[サービス（Services）]** へ移動します。



ステップ 2 **[追加（Add）]** アイコン（**[サービス ノード（Service Nodes）]** ウィンドウ）をクリックします。

ステップ 3 ノード名を入力し、**[ロード バランサ（Load Balancer）]** を指定します（**[タイプ（Type）]** ドロップダウン ボックス）。**[サービス ノード名（Service Node Name）]** は一意である必要があります。

ステップ 4 **[フォーム ファクター（Form Factor）]** ドロップダウン リストから、**[仮想（Virtual）]** を選択します。

ステップ 5 **[スイッチの接続（Switch Attachment）]** セクションで、**[外部ファブリック（External Fabric）]** ドロップダウン リストから、サービス ノード（たとえば、ASA ファイアウォール）が配置されている外部ファブリックを選択します。サービス ノードは外部ファブリックに属している必要があることに注意してください。これは、サービス ノードを作成する際の前提条件です。

ステップ 6 サービス リーフに接続するサービスノードのインターフェイス名を入力します。

ステップ 7 サービス リーフである接続されたスイッチと、サービス リーフ上の対応するインターフェイスを選択します。

ステップ 8 **service_link_trunk** テンプレートを選択します。NDFC は、トランク、ポート チャネル、および vPC リンク テンプレートをサポートします。**[リンク テンプレート（Link Template）]** ドロップダウン リストで使用可能なリンク テンプレートは、選択した **[接続スイッチ インターフェイス （Attached Switch Interface）]** のタイプに基づいてフィルタリングされます。

ステップ 9 必要に応じて、**[一般パラメータ（General Parameters）]** と **[詳細（Advanced）]** パラメータを指定します。一部のパラメータには、デフォルト値が事前に入力されています。

ステップ 10 **[保存（Save）]** をクリックして、作成したサービス ノードを保存します。

Note その他のサンプル スクリーンショットについては、ポリシー ベース ルーティング使用例の、テナント内ファイアウォールの 1. サービス ノードの作成, on page 590 を参照してください。

2. ルート ピアリングの作成

サービス リーフとサービス ノード間のピアリングを構成しましょう。このユースケースでは、静的ルート ピアリングを設定します。

Procedure

ステップ 1 ピアリング名を入力し、**[ワンアーム モード（One-Arm Mode）]** を選択します（**[展開（Deployment）]** ドロップダウン リスト）。また、**[ピアリング オプション（Peering Option）]** ドロップダウン リストから、**[静的ピアリング（Static Peering）]** を選択します。

ステップ 2 **[最初のアーム（First Arm）]** で、必要な値を指定します。**[VRF]** ドロップダウン リストから存在する VRF を選択し、**[最初のアーム（First Arm）]** を **[ネットワーク タイプ（Network Type）]** から選択します。

ステップ 3 **[サービス ネットワーク（Service Network）]** の名前を入力し、**[Vlan ID]** を指定します。**[提案（Propose）]** をクリックして、NDFC がファブリック設定で指定されたサービス ネットワーク VLAN ID の範囲から次に使用可能な VLAN ID をフェッチできるようにします。デフォルトの **[サービス ネットワーク テンプレート（Service Network Template）]** は **Service_Network_Universal** です。

[一般パラメータ（General Parameters）] タブで、サービス ネットワークのゲートウェイ アドレスを指定します。**[ネクストホップ IP アドレス（Next Hop IP Address）]** を指定します。このネクスト ホップ アドレスは、最初のアームのサブネット内にある必要があります。**[詳細設定（Advanced）]** タブの、デフォルトの **[ルーティング タグ（Routing Tag）]** 値は 12345 です。

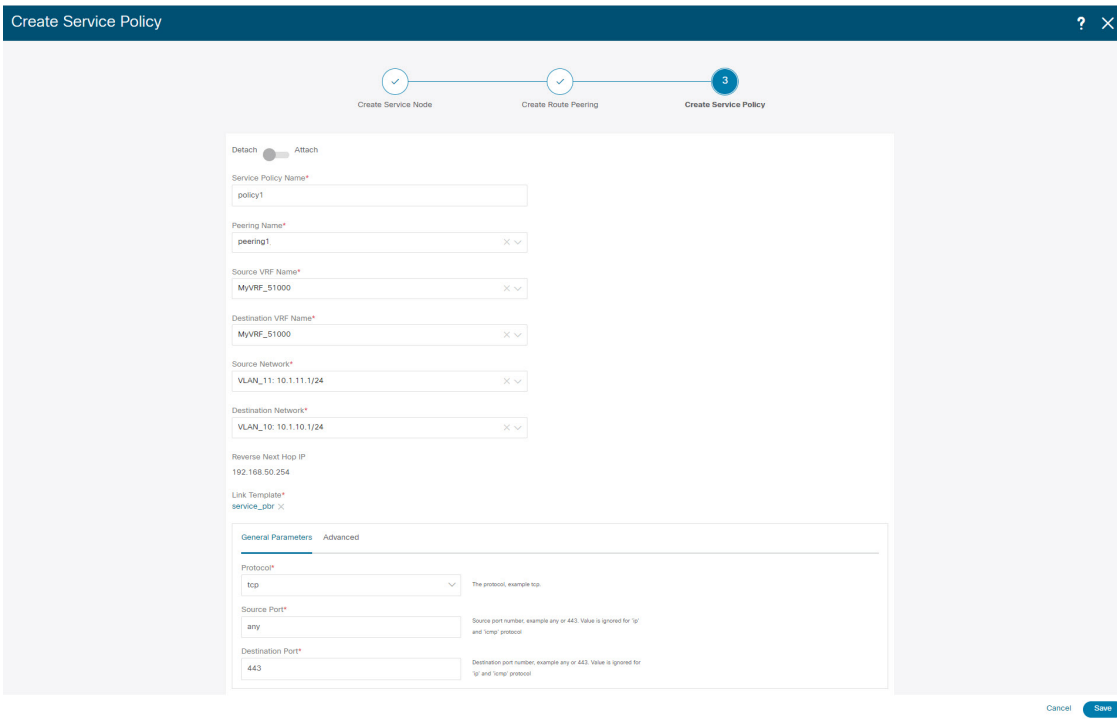
ステップ 4 デフォルトの **[ピアリング テンプレート（Peering Template）]** は **service_static_route** です。必要に応じて、**[静的ルート（Static Routes）]** フィールドにルートを追加します。

ステップ 5 リバース トラフィックの**[ネクスト ホップ IP アドレス（Next Hop IP Address）]** を指定します。

ステップ 6 **[保存（Save）]** をクリックして、作成したルート ピアリングを保存します。

3. サービスポリシーの作成

テナント内ファイアウォール展開のユースケースの 3. サービスポリシーの作成, on page 593 を参照してください。



4. ルート ピアリングを展開する

テナント内ファイアウォール展開のユースケースについての 4. ルート ピアリングを展開する, on page 595 を参照してください。**[OneArmADC]** が **[展開（Deployment）]** の下に表示されていることに注意してください。

5. サービス ポリシーの展開

テナント内ファイアウォール展開のユースケースについての 5. サービス ポリシーの展開, on page 595 を参照してください。ただし、このロード バランサのユース ケースには 2 台のサーバーがあるため、サーバー ネットワークごとに 2 つのサービス ポリシーを定義する必要があります。

6. 統計情報を表示する

テナント内ファイアウォール展開のユースケースの 6. 統計情報を表示する, on page 595 を参照してください。

7. Fabric Builder でのトラフィック フローの表示

テナント内ファイアウォール展開のユースケースの 7. Fabric Builder でのトラフィック フローの表示, on page 596 を参照してください。

8.[トポロジ（Topology）]ウィンドウでの宛先へリダイレクトされたフローの視覚化

テナント内ファイアウォール展開のユースケースの8.[トポロジ（Topology）]ウィンドウでの宛先へリダイレクトされたフローの視覚化, on page 596を参照してください。

サービス リーフの VRF 構成は以下のとおりです。

```
interface Vlan2000
 vrf member myvrf_50001
 ip policy route-map rm_myvrf_50001

interface Vlan2306
 vrf member myvrf_50001
vrf context myvrf_50001
vni 50001
 ip route 55.55.55.55/32 192.168.50.254 // Note: This is the static route
 rd auto
 address-family ipv4 unicast
  route-target both auto
  route-target both auto evpn
 address-family ipv6 unicast
  route-target both auto
  route-target both auto evpn
router bgp 12345
 vrf myvrf_50001
  address-family ipv4 unicast
   advertise l2vpn evpn
   redistribute direct route-map fabric-rmap-redist-subnet
   redistribute static route-map fabric-rmap-redist-static
   maximum-paths ibgp 2
  address-family ipv6 unicast
   advertise l2vpn evpn
   redistribute direct route-map fabric-rmap-redist-subnet
   redistribute static route-map fabric-rmap-redist-static
   maximum-paths ibgp 2
```

第 VI 部

VXLAN BGP EVPN ファブリックの Easy プロビジョニング

第 23 章

グリーンフィールド VXLAN BGP EVPN ファブリックの管理

この章では、グリーンフィールド VXLAN BGP EVPN ファブリックを管理する方法について説明します。

VXLAN BGP EVPN ファブリックのプロビジョニング

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

VXLAN BGP EVPN ファブリックの作成と展開については、VXLAN BGP EVPN ファブリックのプロビジョニング （49 ページ）を参照してください。

新規 VXLAN BGP EVPN ファブリックの作成

新しい VXLAN BGP EVPN ファブリックを作成するには、新規 VXLAN BGP EVPN ファブリックの作成, on page 612を参照してください。

IPv6 アンダーレイを使用した VXLAN ファブリックの作成

この手順では、IPv6 アンダーレイを使用して VXLAN BGP EVPN ファブリックを作成する方法を示します。IPv6 アンダーレイを使用して VXLAN ファブリックを作成するためのフィールドのみが記載されています。残りのフィールドについては、新しい VXLAN BGP EVPN ファブリックの作成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。

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。

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

- [ファブリック名（Fabric Name）]：ファブリックの名前を入力します。
- **[ファブリック テンプレート（Fabric Template）]**：このドロップダウンリストから、**Easy_Fabric** ファブリック テンプレートを選択します。

ステップ 3 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。2 バイトの BGP ASN または 4 バイトの BGP ASN のいずれかを入力できます。

[IPv6 アンダーレイの有効化（Enable IPv6 Underlay）]：**[IPv6 アンダーレイの有効化（Enable IPv6 Underlay）]** チェックボックスをオンにします。

[IPv6 リンク ローカル アドレスを有効にする （Enable IPv6 Link-Local Address）]：**[IPv6 リンク ローカル アドレスを有効にする （Enable IPv6 Link-Local Address）]** チェック ボックスをオンにして、リーフスパイン インターフェイスとスパイン ボーダー インターフェイス間のファブリックでリンク ローカル アドレスを使用します。このチェックボックスをオンにすると、**[アンダーレイ サブネット IPv6 マスク（Underlay Subnet IPv6 Mask ）]**フィールドは編集できなくなります。デフォルトでは、**[IPv6 リンク ローカル アドレスを有効にする （Enable IPv6 Link-Local Address）]** フィールドが有効になっています。

IPv6 アンダーレイは、**p2p** ネットワークのみをサポートします。したがって、**[ファブリック インターフェイスの番号付け（Fabric Interface Numbering）]** ドロップダウン リスト フィールドは無効になっています。

[アンダーレイ サブネット IPv6 マスク（Underlay Subnet IPv6 Mask）]：ファブリック インターフェイスの IPv6 アドレスのサブネットマスクを指定します。

[アンダーレイ ルーティング プロトコル （Underlay Routing Protocol）]：ファブリックで使用される IGP で、VXLANv6 の場合、OSPFv3 または IS-IS です。

ステップ 4 **[レプリケーション（Replication）]** タブの下のすべてのフィールドは無効になっています。

IPv6 アンダーレイは、入力レプリケーション モードのみをサポートします。

ステップ 5 **[VPC]** タブをクリックします。

[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、PKA のために使用される、アンダーレイ ルーティング ループバック（IPv6 アドレスを持つ）を選択します。どちらのオプションも IPv6 アンダーレイでサポートされています。

ステップ 6 **[プロトコル（Protocols）]** タブをクリックします。

[アンダーレイ エニーキャスト ループバック ID（Underlay Anycast Loopback Id）]：IPv6 アンダーレイのアンダーレイ エニーキャスト ループバック ID を指定します。IPv6 アドレスはセカンダリとして設定できないため、追加のループバック インターフェイスが各 vPC デバイスに割り当てられます。その IPv6 アドレスが VIP として使用されます。

ステップ 7 [リソース（Resources）] タブをクリックします。

[手動アンダーレイ IP アドレス割り当て （Manual Underlay IP Address Allocation）]：**[手動アンダーレイ IP アドレス割り当て （Manual Underlay IP Address Allocation）]** をオンにして、手動でアンダーレイ IP アドレスを割り当てます。動的アンダーレイ IP アドレス フィールドは無効になっています。

[アンダーレイ ルーティング ループバック IPv6 範囲（Underlay Routing Loopback IPv6 Range）]：プロトコル ピアリングのループバック IPv6 アドレスを指定します。

[アンダーレイ VTEP ループバック IPv6 範囲（Underlay VTEP Loopback IPv6 Range）]：VTEP のループバック IPv6 アドレスを指定します。

[アンダーレイ サブネット IPv6 範囲（Underlay Subnet IPv6 Range）]：番号付きおよびピアリンク SVI の IP を割り当てる IPv6 アドレス範囲を指定します。このフィールドを編集するには、**[IPv6 リンクローカル アドレスの有効化（Enable IPv6 Link-Local Address）]** チェックボックスをオフにする必要があります（[全般パラメータ（**General Parameters**）] タブ ）。

[IPv6 アンダーレイの BGP ルーター ID 範囲（BGP Router ID Range for IPv6 Underlay）]：BGP ルーター ID を割り当てるアドレス範囲を指定します。ルーターに使用される IPv4 アドレッシングは、BGP およびアンダーレイ ルーティング プロトコル用です。

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

[ブートストラップを有効にする（Enable Bootstrap）]：**[ブートストラップを有効にする（Enable Bootstrap）]** チェックボックスをオンにします。

[ローカル DHCP サーバーを有効にする（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、**[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。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。

[DHCP バージョン（DHCP Version）]：ドロップダウンリストから DHCPv4 を選択する必要があります。

残りのタブとフィールドについては、新しい VXLAN BGP EVPN ファブリックの作成を参照してください。

What to do next

ファブリックへのスイッチの追加

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。

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 （93 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 *45 : 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 *46 : 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 （218 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 (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。

[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。

[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 （175 ページ） を参照してください。

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 *47 : 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。

フィールド	説明
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 *48 : 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 （215 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 （93 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 （393 ページ） 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 *49 :* 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 （231 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 *50* : 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（215 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 *51* : 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 *52*：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。

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。「ファブリックへのスイッチの追加, on page 334」を参照してください。

eBGP EVPN を使用した VXLAN EVPN の展開

この手順では、eBGP ベースのアンダーレイを使用して eBGP VXLAN EVPN を作成し、ファブリック アンダーレイとオーバーレイ eBGP ポリシーを展開する方法について説明します。eBGP EVPN では IPv6 アンダーレイはサポートされていません。

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

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

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

   フィールドについて説明します。

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

   [ファブリックのテンプレート（Fabric Template）]：**Easy_Fabric_eBGP** ファブリック テンプレートを選択するには、これをクリックします。[選択（Select）]をクリックします。スタンドアロン ファブリックを作成するためのファブリック設定が表示されます。
3. 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。

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

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

   [マルチ AS（Multi-AS）] ファブリック：リーフ/ボーダーごとに固有の AS 番号。

   [同層 AS（Same-Tier-AS）]：ファブリック - リーフは 1 つの AS を共有し、ボーダーは 1 つの AS を共有します。

   マルチ AS と **同層 AS** の両方で、ファブリック内のすべてのスパインは 1 つの一意の AS 番号を共有します。

   リーフとボーダーは、同じ AS を持つことも、異なる AS を持つこともできます。

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

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

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

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

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

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

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

Note NX-OS ソフトウェア イメージ バージョン 9.3.6 以降をサポートします。

4. **[EVPN]** をクリックします。このタブのほとんどのフィールドは自動入力されます。該当するフィールドは次のとおりです。

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

   このオプションを選択すると、ルーテッド ファブリックを VXLAN 対応のファブリックに変換できます。ファブリックで VXLAN が有効になっている場合、オーバーレイ ネットワークまたは VRF を作成して展開できます。ネットワークまたは VRF を作成して展開する手順は、Easy_Fabric の場合と同じです。詳細については、*Creating and Deploying Networks and VRFs*（*Cisco NDFC Fabric Controller Configuration Guide*）を参照してください。

   ルーテッド ファブリック：ルーテッド ファブリック（VXLAN カプセル化のない IP ファブリック）を作成するには、**[EVPN VXLAN オーバーレイを有効にする（Enable EVPN VXLAN Overlay）]** チェック ボックスをオフにする必要があります。ルーテッド ファブリックでは、ネットワークを作成して展開できます。詳細については、「ルーテッド ファブリックのネットワークの概要, on page 776」を参照してください。

   eBGP ルーテッドまたは eBGP VXLAN ファブリックを作成する場合、ファブリックは eBGP をコントロール プレーンとして使用して、ファブリック内接続を構築します。スパイン スイッチとリーフ スイッチ間のリンクは、上側で eBGP ピアリングが構築されたポイント ツー ポイント（p2p）番号付き IP アドレスで自動構成されます。

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

   Routed_Network_Universal テンプレートは、ルーテッド ファブリックにのみ適用されることに注意してください。ルーテッド ファブリックを EVPN VXLAN ファブリックに変換する場合は、ネットワーク テンプレートとネットワーク拡張テンプレートを、EVPN VXLAN に定義されているものに設定します：**Default_Network_Universal** と

Default_Network_Universal です。EVPN VXLAN ファブリック用にカスタマイズされたテンプレートがある場合は、それを使用することも選択できます。

Note

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

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

[VXLAN OAM を有効にする（Enable VXLAN OAM）]：既存のスイッチの VXLAN OAM機能を有効にします。この設定はデフォルトでイネーブルになっています。VXLAN OAM 機能を無効にするにはチェックボックスをクリアします。

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

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

[テナント DHCP を有効にする（Enable Tenant DHCP）]：テナント DHCP サポートを有効にします。

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

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

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

[テナント ルーテッド マルチキャストを有効にする（Enable Tenant Routed Multicast）]：ファブリック オーバーレイ マルチキャスト プロトコルとしてテナント ルーテッド マルチキャスト（TRM）を有効にするには、**[テナント ルーテッド マルチキャストを有効にする（Enable Tenant Routed Multicast）]** チェックボックスをオンにします。

[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]：テナント ルーテッドマルチキャスト トラフィックのマルチキャスト アドレスが入力されます。デフォルトでは、このアドレスは [マルチキャスト グループ サブネット] フィールドで指定されたIPプレフィックスから取得されます。いずれかのフィールドをアップデート

する場合、**[マルチキャスト グループ サブネット（Multicast Group Subnet）]** で指定した IP プレフィックスから選択された TRM アドレスであることを確認してください。

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

[RP モード（RP mode）]：ASM（エニーソース マルチキャスト（ASM）の場合）または BiDir（双方向 PIM（BIDIR-PIM）の場合）の、サポート対象の 2 つのマルチキャスト モードからいずれかを選択します。[ASM] を選択すると、[BiDir] 関連のフィールドは有効になりません。[BiDir] を選択すると、[BiDir] 関連フィールドが有効になります。

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

[アンダーレイ RP ループバック ID（Underlay RP Loopback ID）]：ファブリック アンダーレイでのマルチキャスト プロトコル ピアリングの目的で、ランデブーポイント（RP）に使用されるループバック ID です。デフォルトは 254 です。

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

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

次のループバック ID オプションは、RP カウントが 4 の場合にのみ適用されます（[bidir] が選択されている場合）。

- **[アンダーレイ セカンド バックアップ RP ループバック ID（Underlay Second Backup RP Loopback ID）]**：ファブリック アンダーレイでマルチキャスト プロトコル ピアリングを目的としてファントム RP に使用される、第二のバックアップ ループバック ID です。
- **[アンダーレイ サード バックアップ RP ループバック ID（Underlay Third Backup RP Loopback ID）]**：ファブリック アンダーレイでマルチキャスト プロトコル ピアリングを目的としてファントム RP に使用される、第三のバックアップ ループバック ID です。

[VRF テンプレート（VRF Template）] および **[VRF 拡張テンプレート（VRF Extension Template）]**：VRF を作成するための VRF テンプレートと、他のファブリックで VRF 拡張を有効にするための VRF 拡張テンプレートを指定します。

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

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

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

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

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

[VRF Lite の展開（VRF Lite Deployment）]：ファブリック間接続を拡張するための VRF Lite 方式を指定します。[手動（Manual）] オプションのみがサポートされています。

5. **[vPC]** をクリックします。このタブのフィールドは次のとおりです。

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

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

   [vPC ピア キープアライブ オプション（vPC Peer Keep Alive option）]：管理またはループバック オプションを選択します。管理ポートおよび管理 VRF に割り当てられた IP アドレスを使用する場合は、[管理（management）] を選択します。ループバック インターフェイス（および非管理 VRF）に割り当てられた IP アドレスを使用する場合は、ループバックを選択します。IPv6 アドレスを使用する場合は、ループバック ID を使用する必要があります。

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

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

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

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

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

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

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

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）]：すべてのスパインで同じにする必要がある QoS ポリシー名を指定します。

6. **[プロトコル（Protocols）]**をクリックします。このタブのフィールドは次のとおりです。

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

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

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

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

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

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

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

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

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

[BFD の有効化（Enable BFD）]：**[BFD の有効化（Enable BFD）]** チェックボックスは、ファブリック内のすべてのスイッチで**機能 bfd** を有効にする場合にオンにします。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。

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

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

```
feature bfd
```

Note BFD が有効になっている NDFC では、次の構成がすべての P2P ファブリック インターフェイスにプッシュされます。

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

BFD機能の互換性については、それぞれのプラットフォームのマニュアルを参照してください。サポートされているソフトウェアイメージについては、*Compatibility Matrix for Cisco*を参照してください。

[BGP 向け BFD を有効にする（Enable BFD for BGP）]：**[BGP 向け BFD を有効にする（Enable BFD for BGP）]** チェックボックスをオンにして、BGP ネイバーの BFD を有効にします。このオプションは、デフォルトで無効です。

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

[BFD 認証キー ID（BFD Authentication Key ID）]：インターフェイス認証の BFD 認証キー ID を指定します。

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

BFD 認証パラメータを取得する方法については、『*Cisco NDFC LAN Fabric Configuration Guide*』の「*Retrieving the Encrypted BFD Authentication Key*」を参照してください。

7. [詳細設定（Advanced）] 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。

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

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

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

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

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

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

[ブートストラップスイッチの CDP を有効にする（Enable CDP for Bootstrapped Switch）]：**[ブートストラップスイッチの CDP を有効にする（Enable CDP for Bootstrapped Switch）]** チェックボックスをオンにして、ブートストラップスイッチの CDP を有効にします。

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

[HTTP での NX-API の有効化（Enable NX-API on HTTP）]：HTTP での NX-API の有効化を指定します。HTTP を使用するには、**[HTTP での NX-API の有効化（Enable NX-API on HTTP）]** チェックボックスと **[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 を使用するようになります。

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

[厳密な構成コンプライアンスの有効化（Enable Strict Config Compliance）]：このチェックボックスをオンにして、厳密な構成コンプライアンス機能を有効にします。

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

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

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

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

[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。

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

[デフォルト キューイング ポリシーの有効化（Enable Default Queuing Policies）]：**[デフォルト キューイング ポリシーの有効化（Enable Default Queuing Policies）]** チェックボックスをオンにして、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 NDFC Web UI から、**[操作（Operations）]** > **[テンプレート（Templates）]**の順に選択します。ポリシー ファイル名でキューイング ポリシーを検索します（例：[queuing_policy_default_8q_cloudscale]）。ファイルを選択し、**[テンプレートの変更/表示（Modify/View template）]** アイコンをクリックしてポリシーを編集します。

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

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

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

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

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

[スパインの自由形式の構成（Spine Freeform Config）]：スパイン、ボーダー スパイン、ボーダー ゲートウェイ スパイン、およびスーパー スパインのロールを持つスイッチに追加する CLI です。

[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 です。

8. **管理能力（Manageability）** タブをクリックします。このタブのフィールドは次のとおりです。

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

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

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

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

   [Syslog サーバー 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 サーバーのシビラティ（重大度）（Syslog Server Severity）]：syslog サーバーごとに、1 つの syslog シビラティ（重大度）値のカンマ区切りリストを指定します。最小値は 0 で、最大値は 7 です。高い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 をカンマ区切りリストで指定します。

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

   ファブリック設定で AAA 構成が指定されている場合は、**switch_freeform** PTI で、ソースが **UNDERLAY_AAA**、説明が **AAA Configurations** であるものが作成されます。

9. **[ブートストラップ（Bootstrap）]** タブをクリックします。このタブのフィールドは次のとおりです。

   [ブートストラップを有効にする（Enable Bootstrap）]：**[ブートストラップを有効にする（Enable Bootstrap）]** チェックボックスをオンにして、ブートストラップ機能を有効にします。

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

   - 外部 DHCP サーバ（External DHCP Server）：[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）] および [スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）] フィールドに外部 DHCP サーバに関する情報を入力します。

- ローカル DHCPサーバー（Local DHCP Server）：**[ローカル DHCP サーバー（Local DHCP Server）]**チェックボックスをオンにして、残りの必須フィールドに詳細を入力します。

[ローカル DHCP サーバーを有効にする（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、**[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。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、NDFC は自動 IP アドレス割り当てにリモートまたは外部の DHCP サーバーを使用します。

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

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

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

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

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

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

[AAA 構成を有効にする（Enable AAA Config）]：**[AAA 構成を有効にする（Enable AAA Config）]**チェックボックスをオンにして、デバイスの起動時に**[管理性（Manageability）]**タブからの AAA 構成が含められるようにします。

[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、AAA またはリモート認証関連の構成を使用している場合は、このフィールドにこれらの構成を追加してインテントを保存する必要があります。デバイスが起動すると、[Bootstrap Freeform Config]フィールドで定義されたインテントが含まれます。

NX-OSスイッチの実行コンフィギュレーションに示されているように、running-configを正しいインデントで自由形式の設定フィールドにコピーアンドペーストします。freeform config は running config と一致する必要があります。詳細については、スイッチでのフリーフォーム構成エラーの解決を参照してください。ファブリック スイッチでのフリーフォーム構成の有効化に記されています。

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

スコープの形式は次の順で定義する必要があります。

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

例：10.6.0.2、10.6.0.9、16.0.0.1、24

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

    [毎時ファブリック バックアップ（Hourly Fabric Backup）]：**[毎時ファブリック バックアップ（Hourly Fabric Backup）]**チェックボックスをオンにして、ファブリック構成とインテントの 1 時間ごとの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った場合、NDFC はバックアップを取ります。

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

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

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

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

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

Note 1 時間ごと、およびスケジュールされたバックアップ プロセスは、次の定期的な構成コンプライアンス アクティビティ中にのみ発生し、最大 1 時間の遅延が発生する可能性があります。即時バックアップをトリガーするには、次の手順を実行します。

a. **[LAN]** > **[トポロジ（Topology）]**を選択します。

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

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

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

関連情報を入力して更新したら、**[保存（Save）]** をクリックします。

11. **[フロー モニター（Flow Monitor）]** 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）]：**[Netflow を有効にする（Enable Netflow）]** 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。

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

netflow がファブリック レベルで有効になっていない場合、インターフェイス、ネットワーク、または vrf レベルで netflow を有効にすると、エラー メッセージが生成されます。Cisco NDFC の Netflow サポートについては、Netflow サポート, on page 175 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。このタブ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）]** をクリックして、1 つ以上の Netflow レコードを追加します。この画面のフィールドは次のとおりです。

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

12. [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 アンダーレイを備えた VXLAN ファブリック：ポインタ

- ブラウンフィールド移行は、eBGP ファブリックではサポートされていません。
- リーフスイッチの AS 番号は、作成後に再計算と展開（Recalculate & Deploy）操作を実行した後は変更できません。変更が必要になった場合は、**leaf_bgp_asn** ポリシーを削除し、再計算と展開（Recalculate & Deploy）操作を実行して、この AS に関連する BGP 構成を削除する必要があります。次に、新しい AS 番号を使用して、leaf_bgp_asn ポリシーを追加できます。
- Multi-AS モードと Same-Tier-AS モードを切り替える場合は、モードを変更する前に、手動で追加されたすべての BGP ポリシー（リーフ スイッチの Leaf_bgp_asn および ebgp オーバーレイ ポリシーを含む）を削除し、**再計算と展開（Recalculate & Deploy）**操作を実行します。
- デバイスに ebgp オーバーレイ ポリシーが存在する場合、リーフ スイッチの leaf_bgp_asn ポリシーを変更または削除することはできません。最初に ebgp オーバーレイ ポリシーを削除してから、leaf_bgp_asn ポリシーを削除する必要があります。
- サポートされているロールは、リーフ、スパイン、ボーダーのみです。リーフ、スパイン、およびボーダー以外のロールは、VXLAN BGP ファブリックではサポートされていません。
- ボーダーデバイスでは、VRF-Lite は手動モードでサポートされます。VXLAN マルチサイトは、VXLAN BGP ファブリックではサポートされていません。
- TRM はサポートされています。

ファブリック アンダーレイ eBGP ポリシーの展開

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

Same-Tier-AS モードを使用している場合、すべてのリーフが同じ BGP ASN を共有するため、**leaf_bgp_asn** ポリシーを一度にすべてのリーフに展開できます。

必要なスイッチにポリシーを追加するには、ポリシーの追加（377 ページ）およびポリシーの表示と編集（375 ページ）を参照してください。

ファブリック オーバーレイ eBGP ポリシーの展開

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

スパイン スイッチ オーバーレイ ポリシーの展開

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

この画面のフィールドは次のとおりです。

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

[リーフ BGP ASN（Leaf BGP ASN）]：リーフ スイッチの BGP AS 番号。

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

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

[BGP 認証を有効にする（Enable BGP Authentication）]：**[BGP 認証を有効にする（Enable BGP Authentication）]** チェックボックスをオンにして BGP 認証を有効にします。

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

リーフ スイッチ オーバーレイ ポリシーの展開

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

この画面のフィールドは次のとおりです。

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

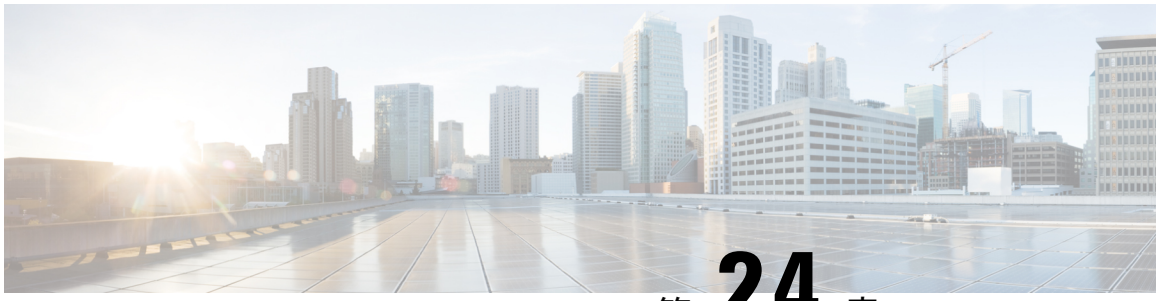
[BGP アップデート送信元インターフェイス（BGP Update-Source Interface）]：BGP アップデートの送信元インターフェイスです。このフィールドでは loopback0、つまり、アンダーレイ ルーティングのループバック インターフェイスを使用できます。

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

[BGP 認証を有効にする（Enable BGP Authentication）]：**[BGP 認証を有効にする（Enable BGP Authentication）]** チェックボックスをオンにして BGP 認証を有効にします。

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

[アクション（Actions）] > **[再計算と展開（Recalculate & Deploy）]** をクリックします。**[構成の展開（Deploy Configuration）]** ウィンドウで構成の展開が完了したら、**[閉じる（Close）]** をクリックします。または、**[ポリシーの表示/編集（View/Edit Policy）]** オプションを使用し、**[構成のプッシュ（Push Configuration）]** をクリックして構成を展開します。



第 24 章

ブラウンフィールド VXLAN BGP EVPN ファブリックの管理

概要

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

通常、ファブリックは手動の CLI 構成またはカスタム自動化スクリプトによって作成および管理されます。これで、Nexusダッシュボード ファブリック コントローラ でファブリックの管理を開始できるようになりました。移行後、ファブリック アンダーレイとオーバーレイ ネットワークは NDFC によって管理されます。

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

前提条件

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

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

注意事項と制約事項

- すべてのスイッチをNDFCファブリックに追加して、ファブリック全体に対してブラウンフィールド インポートを完了する必要があります。
- **[ファブリックの作成（Create Fabric）]** ウィンドウで、**[詳細設定（Advanced）]** > **[オーバーレイ モード（Overlay Mode）]**ファブリック設定で、オーバーレイの移行方法を決定します。デフォルトの config-profile が設定されている場合、VRF およびネットワーク オーバーレイ構成プロファイルは、移行プロセスの一部としてスイッチに展開されます。さらに、重複するオーバーレイ CLI 構成の一部を削除するための diffs 機能があります。これらはネットワークに影響を与えません。
- **CLI が設定されている場合、[オーバーレイ モード（Overlay Mode）]** ドロップダウン リストからの VRF およびネットワーク オーバーレイの構成は、整合性の違いに対応するための変更をまったく、またはほとんど行うことなく、そのままスイッチに残されます。
- NDFC のブラウンフィールド インポートは、簡素化された NX-OS VXLAN EVPN 構成 CLI をサポートします。詳細については、Cisco Nexus 9000 シリーズ NX-OS VXLAN 構成ガイド、リリース 10.2(x) を参照してください。
- 次の機能はサポートされていません。
  - スーパー スパイン ロール
  - ToR
  - eBGP アンダーレイ
  - レイヤ 3 ポートチャネル
  - vPC ファブリック ピアリング
- 移行前に、スイッチ構成のバックアップを取り、保存します。
- 移行が完了するまで、スイッチの構成を変更してはなりません（このドキュメントで指示されている場合を除く）。変更すると、重大なネットワークの問題が発生する可能性があります。
- Cisco Nexusダッシュボード ファブリック コントローラ への移行は、Cisco Nexus 9000 スイッチでのみサポートされています。
- ボーダー スパインとボーダー ゲートウェイ スパインのロールは、ブラウンフィールド移行でサポートされています。
- まず、設定を更新する際のガイドラインについての注意を述べます。次に、各 VXLAN ファブリック設定タブについて説明します。

- 一部の値（BGP AS 番号、OSPF など）は、既存のファブリックへの基準ポイントと見なされるので、入力する値は既存のファブリックの値と一致させる必要があります。
- 一部のフィールド（IPアドレス範囲、VXLAN ID範囲など）の場合、自動入力または設定で入力された値は、将来の割り当てにのみ使用されます。移行中は、既存のファブリック値が優先されます。
- 一部のフィールドは、既存のファブリックに存在しない可能性のある新しい機能（advertise-pip など）に関連しています。必要に応じて有効または無効にします。
- ファブリックの移行が完了した後で、必要に応じて設定を更新できます。

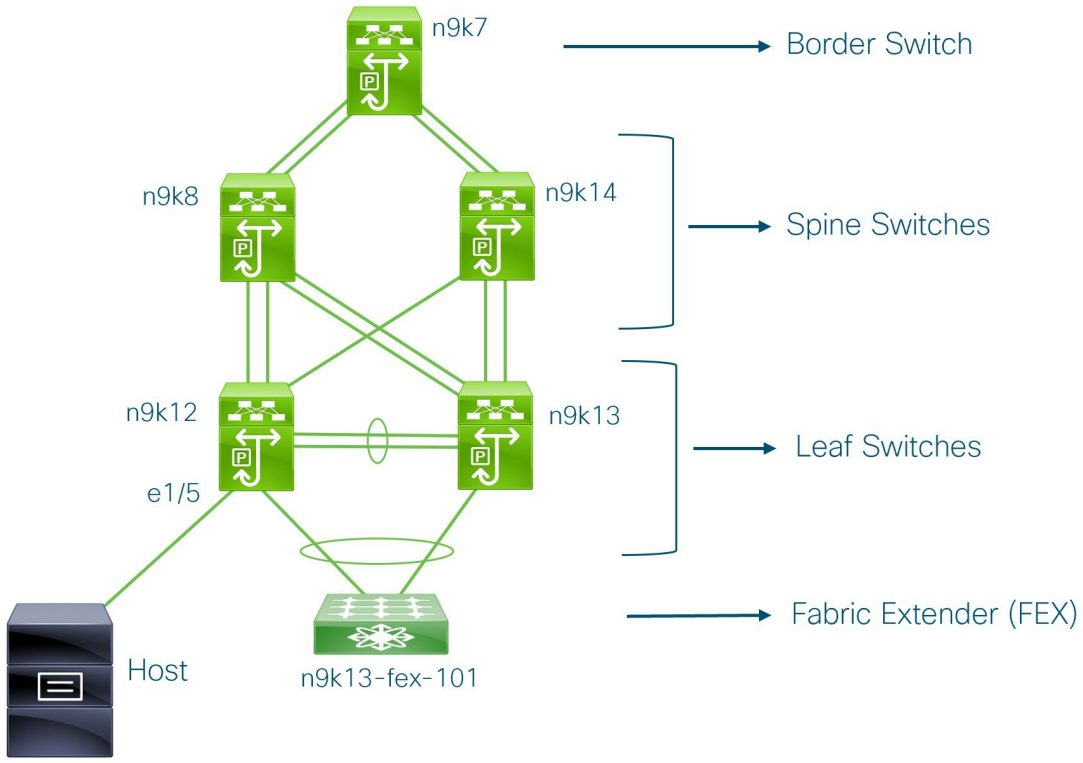
ファブリック トポロジの概要

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

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

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

既存のファブリックの移行を開始する前に、そのトポロジを見てみましょう。



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

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

NDFC ブラウンフィールド展開タスク

ブラウンフィールド移行には、次のタスクが含まれます。

1. 既存の VXLAN BGP EVPN ファブリックの確認 （661 ページ）
2. 新規 VXLAN BGP EVPN ファブリックの作成 （53 ページ）
3. スイッチの追加と VXLAN ファブリック管理の NDFC への移行 （686 ページ）

既存の VXLAN BGP EVPN ファブリックの確認

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

Procedure

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

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

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

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

ステップ 2 vPC の整合性と障害を確認します。

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

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

ステップ 3 **n9k-12** スイッチの EVPN ネイバーを確認します。

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

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

スパイン スイッチに対応する 2 つのネイバーがあることがわかります。

ASN が 65000 であることに注意してください。

ステップ 4 VRF 情報を確認します。

```
n9k12# show run vrf internet

!Command: show running-config vrf Internet
```

```
!Running configuration last done at: Fri Aug  9 01:38:02 2019
!Time: Fri Aug  9 02:48:03 2019

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

interface Vlan347
  vrf member Internet

interface Vlan349
  vrf member Internet

interface Vlan3962
  vrf member Internet

interface Ethernet1/25
  vrf member Internet

interface Ethernet1/26
  vrf member Internet
vrf context Internet
  description Internet
  vni 16777210
  ip route 204.90.141.0/24 204.90.140.129 name LC-Networks
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
router ospf 300
  vrf Internet
    router-id 204.90.140.3
    redistribute direct route-map allow
    redistribute static route-map static-to-ospf
router bgp 65000
  vrf Internet
    address-family ipv4 unicast
      advertise l2vpn evpn
```

VRF **インターネット**は、このスイッチで構成されています。

n9k-12 スイッチに接続されているホストは、VRF **インターネット**の一部です。

この VRF に関連付けられた VLAN を表示できます。

具体的には、ホストは **Vlan349** の一部です。

ステップ 5 レイヤ 3 インターフェイス情報を確認します。

```
n9k12# show run interface vlan349

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

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

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

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

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

```
n9k12# show run interface ethernet1/5

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

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

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

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

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

```
host# ping 204.90.140.134 count unlimited interval 1
PING 204.90.140.134 (204.90.140.134): 56 data bytes
64 bytes from 204.90.140.134: icmp_seq=0 ttl=254 time=1.078 ms
64 bytes from 204.90.140.134: icmp_seq=1 ttl=254 time=1.129 ms
64 bytes from 204.90.140.134: icmp_seq=2 ttl=254 time=1.151 ms
64 bytes from 204.90.140.134: icmp_seq=3 ttl=254 time=1.162 ms
64 bytes from 204.90.140.134: icmp_seq=4 ttl=254 time=1.84 ms
64 bytes from 204.90.140.134: icmp_seq=5 ttl=254 time=1.258 ms
64 bytes from 204.90.140.134: icmp_seq=6 ttl=254 time=1.273 ms
64 bytes from 204.90.140.134: icmp_seq=7 ttl=254 time=1.143 ms
```

既存のブラウンフィールド ファブリックを Nexusダッシュボード ファブリック コントローラに移行する間、ping コマンドをバックグラウンドで実行させます。

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 75 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 , on page 699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 75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 75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 93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 88

[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, on page 731 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 114

[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 108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。

[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。

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 108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 175 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。

スイッチの追加と VXLAN ファブリック管理の NDFC への移行

スイッチを検出して、新しく作成したファブリックに追加しましょう。

Procedure

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

[スイッチ（Switches）] タブをクリックします。

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

[スイッチの追加（Add Switches）] ウィンドウが表示されます。

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

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

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

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

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

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

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

ステップ 5 ファブリックにインポートする必要があるスイッチの横にあるチェックボックスをオンにして、**[ファブリックにインポート（Import into fabric）]** をクリックします。

1 回の試行で同時に複数のスイッチを検出することをお勧めします。スイッチは適切にケーブル接続しNDFCサーバーに接続する必要があり、スイッチのステータスは管理可能である必要があります。

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

ステップ 6 [ファブリックにインポート（Import into fabric）] をクリックします。

スイッチ検出プロセスが開始されます。**[進行状況（Progress）]** 列には、選択したすべてのスイッチの進行状況が表示されます。完了時には、スイッチごとに **[完了（done）]** と表示されます。

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

エラー メッセージが表示された場合は、画面を閉じます。[ファブリック トポロジ (fabric topology)] 画面が表示されます。エラー メッセージは、画面の右上に表示されます。エラーを解決し、**[スイッチの追加（Add Switches）]**（**[アクション（Actions）]** パネル）をクリックして、インポート プロセスを再度開始します。

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

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

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

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

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

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

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

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

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

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

Note スイッチで L3 キープアライブが構成されている場合は、vPC ペアリングを手動で作成する必要があります。それ以外の場合、vPC 構成はスイッチから自動的に取得されます。

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

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

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

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

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

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

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

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

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

Note

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

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

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

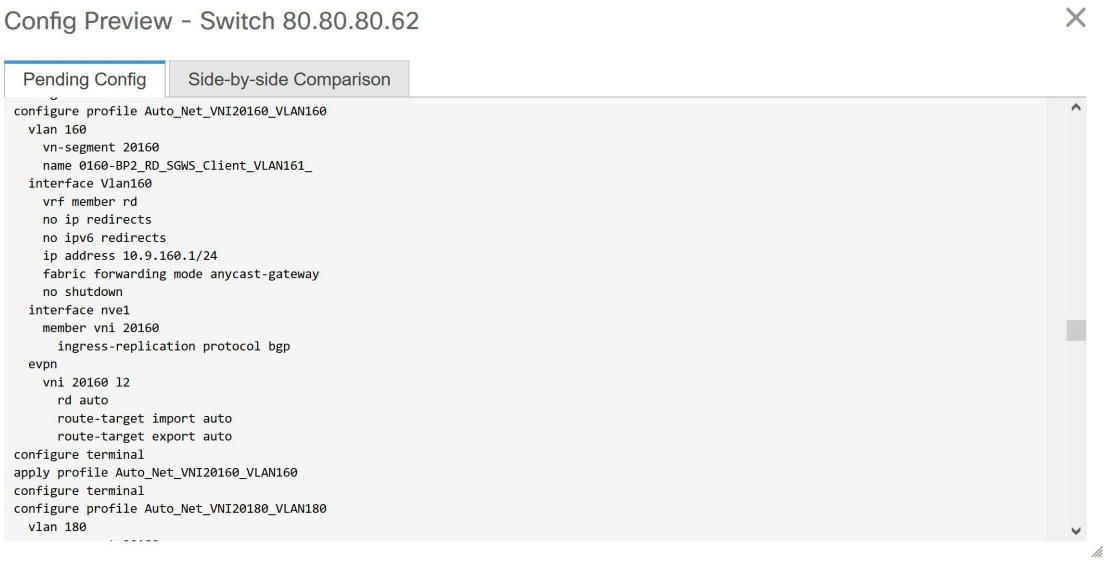
[並べて表示（Side-by-Side）] タブには、実行構成と予想される構成が並べて表示されます。

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

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

Note

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



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

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

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

ステップ 12 構成を確認したら、**[構成プレビュー スイッチ（Config Preview Switch）]** ウィンドウを閉じます。

ステップ 13 **[構成の展開（Deploy Config）]** をクリックして、構成をスイッチに展開します。

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

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

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

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

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

詳細については、ファブリックの概要, on page 194を参照してください。

ブラウンフィールド移行の構成プロファイルのサポート

Cisco NDFC は、構成プロファイルでプロビジョニングされる VXLAN オーバーレイを使用した、ファブリックのブラウンフィールド インポートをサポートしています。このインポート プロセスは、構成プロファイルに基づいてオーバーレイ構成のインテントを再作成します。アンダーレイの移行は、通常のブラウンフィールド移行で実行されます。

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

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

以下は、構成プロファイルのサポートに関するガイドラインです。

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

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

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

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

Procedure

ステップ 1 ブラウンフィールド移行によって追加された RP 用に作成された **base_pim_bidir_11_1** ポリシーを確認します。各 **ip pim rp-address** *RP_IP* **group-list** *MULTICAST_GROUP* **bidir** コマンドで使用される RP IP およびマルチキャスト グループを確認します。

ステップ 2 各 **base_pim_bidir_11_1** ポリシーを新しいリーフまたはスパインの **[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウから追加し、各 **base_pim_bidir_11_1** ポリシーの構成をプッシュします。

ボーダー ゲートウェイ スイッチを使用した MSD ファブリックの移行

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

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

    [両方を自動デプロイ（Auto Deploy Both）] チェックボックスをオフ（**[リソース（Resources）]** タブ）。
  - MSD_Fabric ファブリック

    [マルチサイト アンダーレイ IFC 自動展開フラグ（Multi-Site Underlay IFC Auto Deployment Flag）] チェックボックスをオフ（**[DCI]** タブ）。
- アンダーレイ マルチサイト ピアリング：サイト間のアンダーレイ拡張の eBGP ピアリングおよび対応するルーテッド インターフェイスは、**switch_freeform** および **routed_inerfaces**、オプションで **interface_freeform** 構成でキャプチャされます。この構成

には、マルチサイトのすべてのグローバル構成が含まれます。EVPN マルチサイトのループバックも、適切なインターフェイス テンプレートを介してキャプチャされます。

- オーバーレイ マルチサイト ピアリング：eBGP ピアリングは、**switch_freeform** の一部としてキャプチャされます。唯一の関連する構成が**ルータ bgp** の下にあるためです。
- ネットワークまたは VRF を含むオーバーレイ：対応するインテントは、**extension_type = MULTISITE** のボーダー ゲートウェイのプロファイルでキャプチャされます。

1. 必要なファブリック設定を使用して、Easy_Fabric および External_Fabric ファブリックを含むすべての必要なファブリックを作成します。上記のように [Auto VRF-Lite] 関連オプションを無効にします。詳細については、*VXLAN EVPN* ファブリックの作成および外部ファブリックセクションを参照してください。
2. すべてのスイッチを必要なすべてのファブリックにインポートし、それに応じてロールを設定します。
3. 各ファブリックで**[再計算して展開（Recalculate and Deploy）]** をクリックし、ブラウンフィールド移行プロセスが「展開」フェーズに到達することを確認します。ここでは、**[構成の展開（Deploy Configuration）]** をクリックしないでください。
4. ガイドラインに示すように、必要なファブリック設定で **MSD_Fabric** ファブリックを作成し、**[自動マルチサイト IFC（Auto MultiSite IFC）]** 関連オプションを無効にします。詳細については、『*Cisco DCNM LAN* ファブリック構成ガイド』の「*MSD* ファブリックの作成」を参照してください。
5. すべてのメンバーファブリックを MSD に移動します。この手順が正常に完了するまで、先に進まないでください。詳細については、『*Cisco DCNM LAN* ファブリック構成ガイド』の「*MSD-Parent-Fabric* での *Member1* ファブリックの移動」を参照してください。

（注） 各 Easy ファブリックのオーバーレイ ネットワークと VRF の定義は、対称である必要があります。それらが MSD に正常に追加されるためです。不一致が見つかった場合、エラーが報告されます。これらは、ファブリックのオーバーレイ情報を更新して MSD に追加することで修正する必要があります。

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

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

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

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

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

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

   この手順は、ファブリックで TRM が有効になっている場合に実行する必要があります。TRM が有効になっていない場合でも、各ネットワーク エントリを編集して保存する必要があります。
10. MSD ファブリックで **[再計算と展開（Recalculate and Deploy）]** をクリックしますが、**[構成の展開（Deploy Configuration）]** はクリックしないでください。
11. 各メンバー ファブリックに移動し、**[再計算と展開（Recalculate and Deploy）]** をクリックしてから、**[構成の展開（Deploy Configuration）]** をクリックします。

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

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

（注） MSD ファブリックを移行する前に、子ファブリックが MSD に追加されていることを確認してください。

1. MSD 子ファブリックをクリックし、**[ファブリック（Fabrics）]** > **[インターフェイス（Interfaces）]** に移動して、BGW を表示します。アンダーレイ IFC に使用する適切なレイヤ 3 ポート チャネルを選択します。
2. **[ポリシー（Policy）]** 列で、ドロップダウン リストから **int_port_channel_trunk_host_11_1** を選択します。関連付けられたポート チャネル インターフェイス メンバーを入力し、**[保存（Save）]** をクリックします。
3. MSD ファブリックの**表形式ビュー**に移動します。レイヤ 3 ポート リンクを編集し、マルチサイト アンダーレイ IFC リンク テンプレートを選択し、送信元と宛先の IP アドレスを入力します。これらの IP アドレスは、スイッチの既存の構成値と同じです。
4. 上記の手順 7 から 11 までの手順を実行します。

第 25 章

VXLANv6 ファブリックの構成

この章では、IPv6アンダーレイを使用してVXLANファブリックを構成する方法について説明します。

概要

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

次のガイドラインは、IPv6 アンダーレイに適用されます。

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

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

- VXLANv6 では、スパインでサポートされるプラットフォームは、すべての Nexus 9000 シリーズおよび Nexus 3000 シリーズ プラットフォームです。
- IPv6 ファブリックでサポートされるオーバーレイ ルーティング プロトコルは BGP EVPN です。
- 物理マルチシャーシ EtherChannel トランク（MCT）機能を備えた vPC は、NDFC の IPv6 アンダーレイ ネットワークでサポートされています。vPC ピア キープアライブは、IPv4

または IPv6 アドレスを使用したループバックまたは管理インターフェイスで設定できます。

- VXLANv6 ファブリックではブラウンフィールド移行がサポートされています。IPv6 アドレスを使用した L3 vPC キープアライブは、ブラウンフィールド移行ではサポートされないことに注意してください。この vPC 構成は、移行後に削除されます。ただし、IPv4 アドレスを使用した L3 vPC キープアライブはサポートされています。
- DHCPv6 は、IPv6 アンダーレイ ネットワークでサポートされています。
- 次の機能は、VXLAN IPv6 アンダーレイではサポートされていません。
  - マルチキャスト アンダーレイ
  - テナント ルーテッド マルチキャスト（TRM）
  - ISIS、OSPF、および BGP 認証
  - VXLAN マルチサイト
  - デュアル スタック アンダーレイ
  - vPC ファブリック ピアリング
  - DCI SR-MPLS または MPLS-LDP ハンドオフ
  - BFD
  - スーパー スパイン スイッチ ロール
  - NGOAM

IPv6 アンダーレイを使用した VXLAN ファブリックの作成

この手順では、IPv6 アンダーレイを使用して VXLAN BGP EVPN ファブリックを作成する方法を示します。IPv6 アンダーレイを使用して VXLAN ファブリックを作成するためのフィールドのみが記載されています。残りのフィールドについては、新しい VXLAN BGP EVPN ファブリックの作成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。

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。

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

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

- **[ファブリック テンプレート（Fabric Template）]**：このドロップダウンリストから、**Easy_Fabric** ファブリック テンプレートを選択します。

ステップ 3 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。2 バイトの BGP ASN または 4 バイトの BGP ASN のいずれかを入力できます。

[IPv6 アンダーレイの有効化（Enable IPv6 Underlay）]：**[IPv6 アンダーレイの有効化（Enable IPv6 Underlay）]** チェックボックスをオンにします。

[IPv6 リンク ローカル アドレスを有効にする（Enable IPv6 Link-Local Address）]：**[IPv6 リンク ローカル アドレスを有効にする（Enable IPv6 Link-Local Address）]** チェック ボックスをオンにして、リーフスパイン インターフェイスとスパイン ボーダー インターフェイス間のファブリックでリンク ローカル アドレスを使用します。このチェックボックスをオンにすると、**[アンダーレイ サブネット IPv6 マスク（Underlay Subnet IPv6 Mask ）]**フィールドは編集できなくなります。デフォルトでは、**[IPv6 リンク ローカル アドレスを有効にする（Enable IPv6 Link-Local Address）]** フィールドが有効になっています。

IPv6 アンダーレイは、**p2p** ネットワークのみをサポートします。したがって、**[ファブリック インターフェイスの番号付け（Fabric Interface Numbering）]** ドロップダウン リスト フィールドは無効になっています。

[アンダーレイ サブネット IPv6 マスク（Underlay Subnet IPv6 Mask）]：ファブリック インターフェイスの IPv6 アドレスのサブネットマスクを指定します。

[アンダーレイ ルーティング プロトコル（Underlay Routing Protocol）]：ファブリックで使用される IGP で、VXLANv6 の場合、OSPFv3 または IS-IS です。

ステップ 4 **[レプリケーション（Replication）]** タブの下のすべてのフィールドは無効になっています。

IPv6 アンダーレイは、入力レプリケーション モードのみをサポートします。

ステップ 5 **[VPC]** タブをクリックします。

[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、PKA のために使用される、アンダーレイ ルーティング ループバック（IPv6 アドレスを持つ）を選択します。どちらのオプションも IPv6 アンダーレイでサポートされています。

ステップ 6 **[プロトコル（Protocols）]** タブをクリックします。

[アンダーレイ エニーキャスト ループバック ID（Underlay Anycast Loopback Id）]：IPv6 アンダーレイのアンダーレイ エニーキャスト ループバック ID を指定します。IPv6 アドレスはセカンダリとして設定できないため、追加のループバック インターフェイスが各 vPC デバイスに割り当てられます。その IPv6 アドレスが VIP として使用されます。

ステップ 7 [リソース（Resources）] タブをクリックします。

[手動アンダーレイ IP アドレス割り当て（Manual Underlay IP Address Allocation）]：**[手動アンダーレイ IP アドレス割り当て（Manual Underlay IP Address Allocation）]** をオンにして、手動でアンダーレイ IP アドレスを割り当てます。動的アンダーレイ IP アドレス フィールドは無効になっています。

[アンダーレイ ルーティング ループバック IPv6 範囲（Underlay Routing Loopback IPv6 Range）]：プロトコル ピアリングのループバック IPv6 アドレスを指定します。

[アンダーレイ VTEP ループバック IPv6 範囲（Underlay VTEP Loopback IPv6 Range）]：VTEP のループバック IPv6 アドレスを指定します。

[アンダーレイ サブネット IPv6 範囲（Underlay Subnet IPv6 Range）]：番号付きおよびピアリンク SVI の IP を割り当てる IPv6 アドレス範囲を指定します。このフィールドを編集するには、**[IPv6 リンクローカル アドレスの有効化（Enable IPv6 Link-Local Address）]** チェックボックスをオフにする必要があります（[全般パラメータ（**General Parameters**）] タブ）。

[IPv6 アンダーレイの BGP ルーター ID 範囲（BGP Router ID Range for IPv6 Underlay）]：BGP ルーター ID を割り当てるアドレス範囲を指定します。ルーターに使用される IPv4 アドレッシングは、BGP およびアンダーレイ ルーティング プロトコル用です。

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

[ブートストラップを有効にする（Enable Bootstrap）]：**[ブートストラップを有効にする（Enable Bootstrap）]** チェックボックスをオンにします。

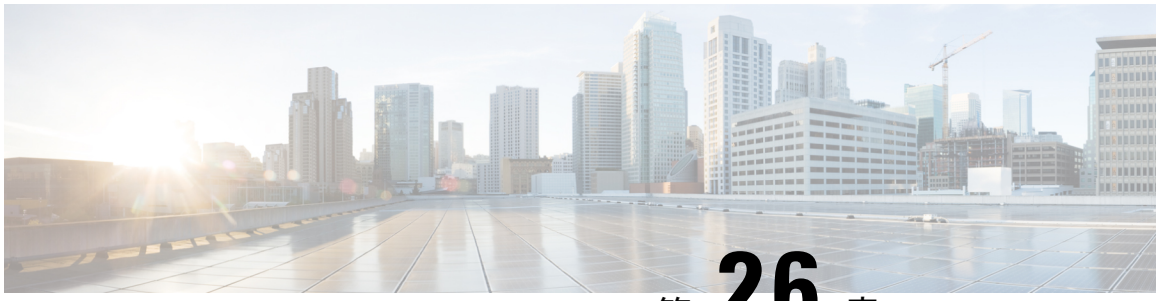
[ローカル DHCP サーバーを有効にする（Enable Local DHCP Server）]：ローカル DHCP サーバーを介した自動 IP アドレス割り当ての有効化を開始するには、**[ローカル DHCP サーバーを有効にする（Enable Local DHCP Server）]** チェックボックスをオンにします。このチェックボックスをオンにすると、**[DHCP スコープ開始アドレス（DHCP Scope Start Address）]** および **[DHCP スコープ終了アドレス（DHCP Scope End Address）]** フィールドが編集可能になります。

[DHCP バージョン（DHCP Version）]：ドロップダウンリストから DHCPv4 を選択する必要があります。

残りのタブとフィールドについては、新しい VXLAN BGP EVPN ファブリックの作成を参照してください。

What to do next

ファブリックへのスイッチの追加



第 26 章

VXLAN BGP EVPN ファブリックのマルチサイト ドメイン

VXLAN BGP EVPN ファブリックのマルチサイト ドメイン

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

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

MSD ファブリックのトポロジ ビューには、すべてのメンバー ファブリックと、それらが互いにどのように接続されているかが、1 つのビューとして表示されます。各メンバー ファブリックの展開画面に個別にアクセスして展開する代わりに、単一のトポロジ展開画面から、メンバー ファブリックにオーバーレイ ネットワーク（および VRF）を展開できます。

Note

- Cisco NDFC の VXLAN OAM 機能は、単一のファブリックまたはサイトでのみサポートされます。
- BGW vPC のペアリングを解除した後、メンバー ファブリックで**構成の再計算**と**構成の展開**を実行し、続いて MSD ファブリックの**構成の再計算**と**構成の展開**を実行します。

ファブリック固有の用語：

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

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

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

ファブリックとスイッチのインスタンス変数

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

ファブリック インスタンスの値は、[VRFs and Networks] ウィンドウからのファブリック コンテキストでのみ編集または更新できます。適切な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**を表示し、**[ネットワーク（Networks）]**または**[VRF]**タブを選択します。ファブリック インスタンス変数の例には、BGP ASN、ネットワークごとのマルチキャスト グループ

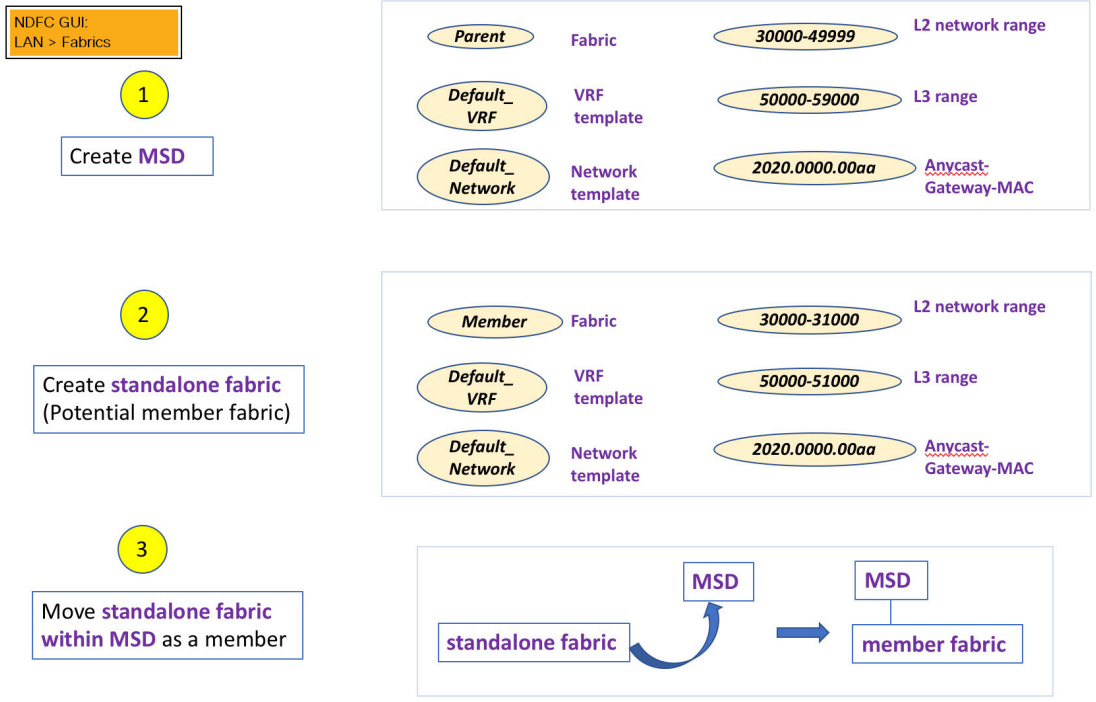
またはVRF などがあります。マルチキャスト グループ アドレスの編集方法については、MSD ファブリックでのネットワークの作成, on page 711を参照してください。

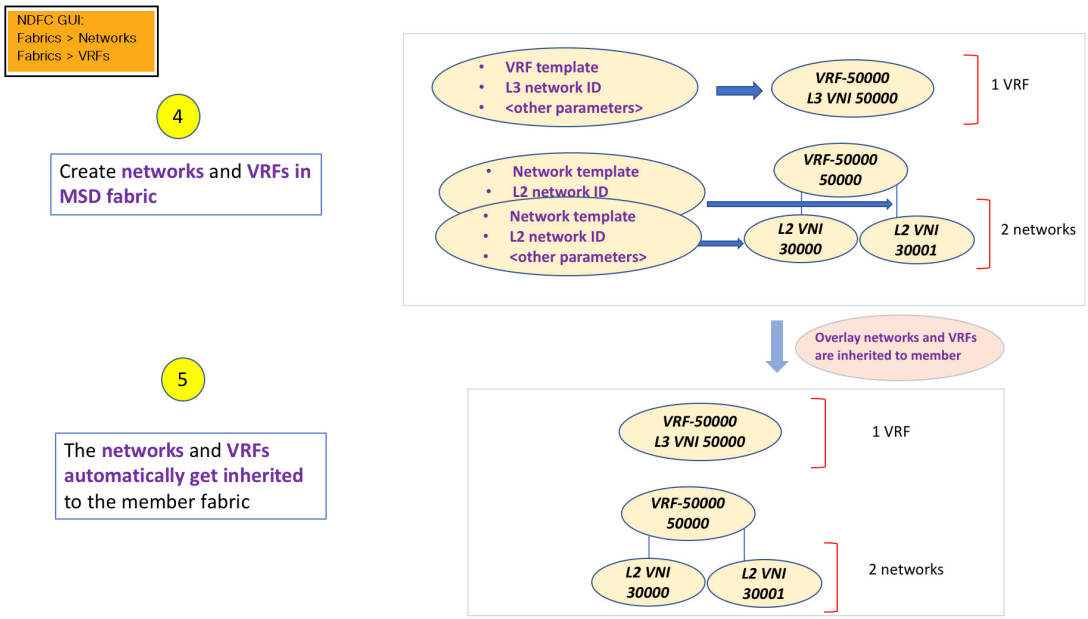
スイッチインスタンスの値は、スイッチにネットワークを展開するときに編集できます。例としては、*VLAN ID* があります。

MSD およびメンバー ファブリックのプロセス フロー

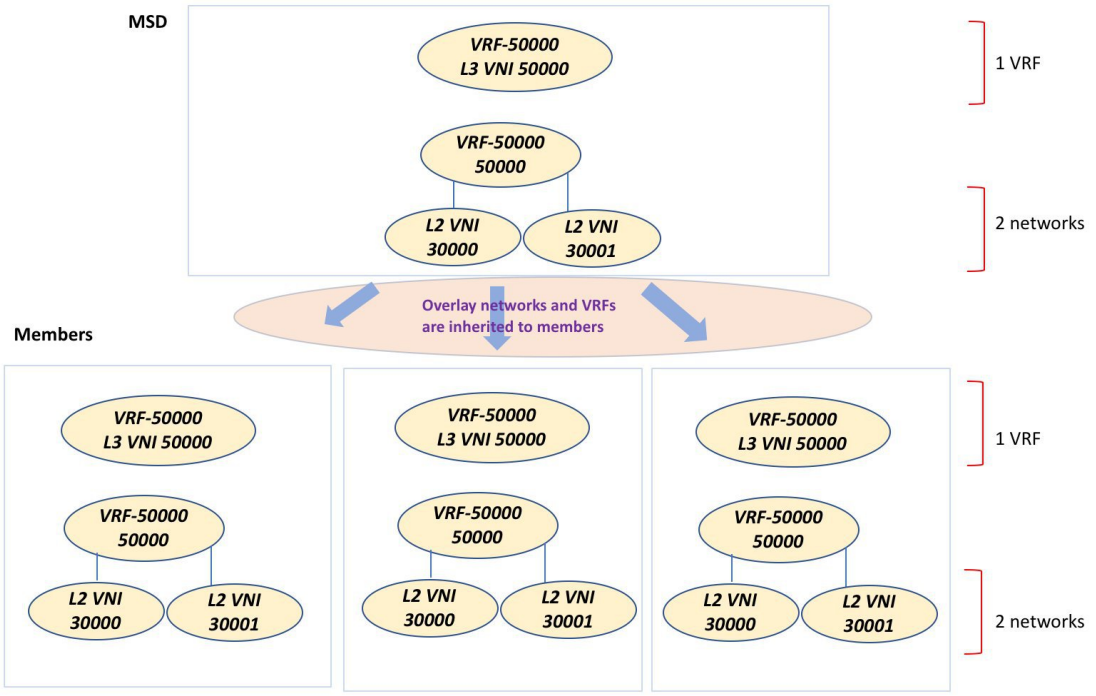
MSDには複数のサイトがあります（したがって、MSDの下に複数のメンバー ファブリックがあります）。MSD用にVRFとネットワークが作成され、メンバー ファブリックに継承されます。たとえば、VRF-50000（およびID 50000のL3ネットワーク）と、ID 30000および30001のL2ネットワークが、MSDに対して一度に作成されます。

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

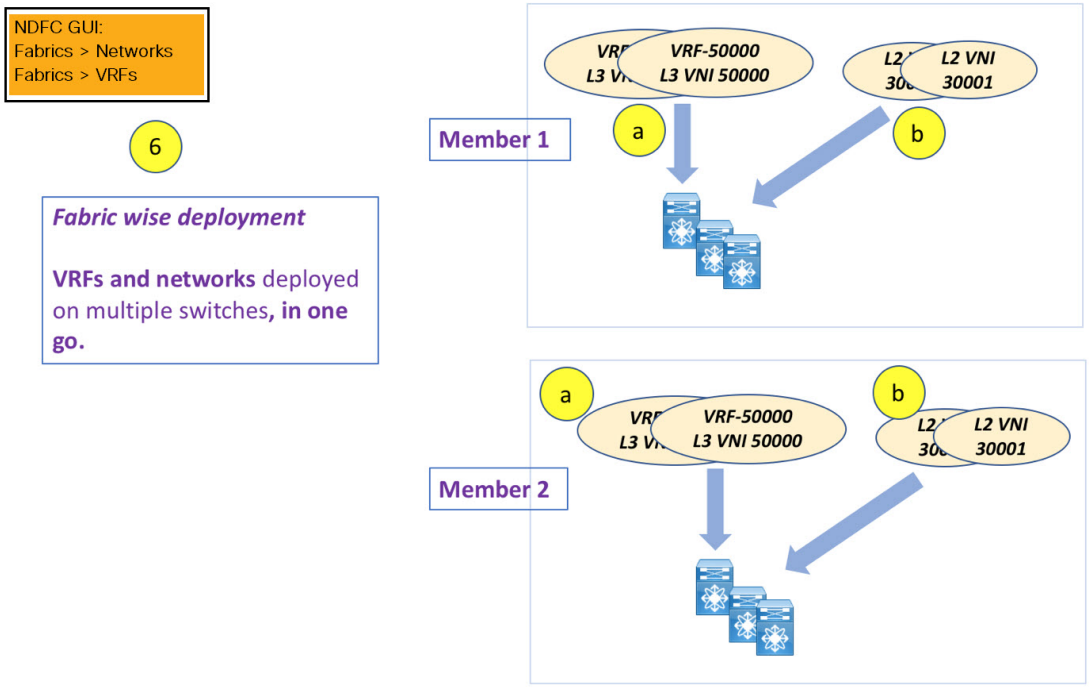




サンプル フローでは、MSD から 1 つのメンバーへの継承について説明しました。MSD には複数のサイトがあります（したがって、MSD の下に複数のメンバー ファブリックがあります）。MSD から複数のメンバーへのサンプル フロー：



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



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

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

ドキュメントの今後のセクションでは、以下について説明します。

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

MSDファブリックの作成とメンバーファブリックの関連付け

このプロセスは、次の 2 つのステップで説明されます。

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

MSD ファブリックの作成

1. **[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、**MSD_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。

4. **[一般パラメータ（General Parameters）]** タブでは、すべてのフィールドにデータが自動入力されます。フィールドは、レイヤ 2 およびレイヤ 3 VXLAN セグメント識別子の範囲、デフォルトのネットワークおよび VRF テンプレート、およびエニーキャスト ゲートウェイの MAC アドレスで構成されます。必要に応じて、以下のフィールドを更新します。

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

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

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

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

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

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

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

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

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

5. [**DCI**] タブをクリックします。

   該当するフィールドは次のとおりです。

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

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

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

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

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

   [マルチサイト（Multi-Site CloudSec）]：ボーダー ゲートウェイで CloudSec 構成を有効にします。このフィールドを有効にすると、CloudSec の残りの 3 つのフィールドが編集可能になります。詳細については、マルチサイト展開での CloudSec のサポート （713 ページ）を参照してください。

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

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

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

6. [リソース（Resources）] タブをクリックします。

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

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

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

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

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

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

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

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

8. [保存（Save）] をクリックします。

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

   新しい MSD が作成されると、新しく作成された MSD ファブリック インスタンスが [ファブリック（Fabrics）] テーブルに表示されます。

   MSD ファブリックは、*[Multi-Fabric Domain]* として **[ファブリック タイプ（Fabric Type）]** フィールドに表示されます。メンバー ファブリック名がブランチとして含まれています。メンバー ファブリックが作成されていない場合は、スタンドアロン ファブリックとして表示されます。

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

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

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

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

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

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

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

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

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

その他の指針：

- メンバー ファブリックにはサイト ID が設定されている必要があり、サイト ID はメンバー間で一意である必要があります。
- BGP AS 番号は、メンバー ファブリックに対して一意である必要があります。
- loopback0 のアンダーレイ サブネット範囲は一意である必要があります。
- loopback1 のアンダーレイ サブネット範囲は一意である必要があります。

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

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

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

1. MSD ファブリック名をダブルクリックして **[ファブリックの概要（Fabric Overview）]** 画面を表示します。
2. **[子ファブリック（Child Fabrics）]** で、**[アクション（Actions）] > [ファブリックを MSD に移動（Move Fabric into MSD）]** をクリックします。

   [ファブリックの概要（Fabric Overview）] > [アクション（Action）] > [子ファブリックの追加（Add Child Fabrics）] をクリックして、メンバー ファブリックを MSD に追加することもできます。

   MSD の一部ではない子ファブリックのリストが表示されます。他の MSD コンテナ ファブリックのメンバー ファブリックは、ここには表示されません。
3. *Member1* ファブリックを MSD ファブリックに関連付けるため、**Member1** ファブリックを選択して **[選択（Select）]** をクリックします。
4. ファブリックを選択し、**[選択（Select）]** をクリックします。

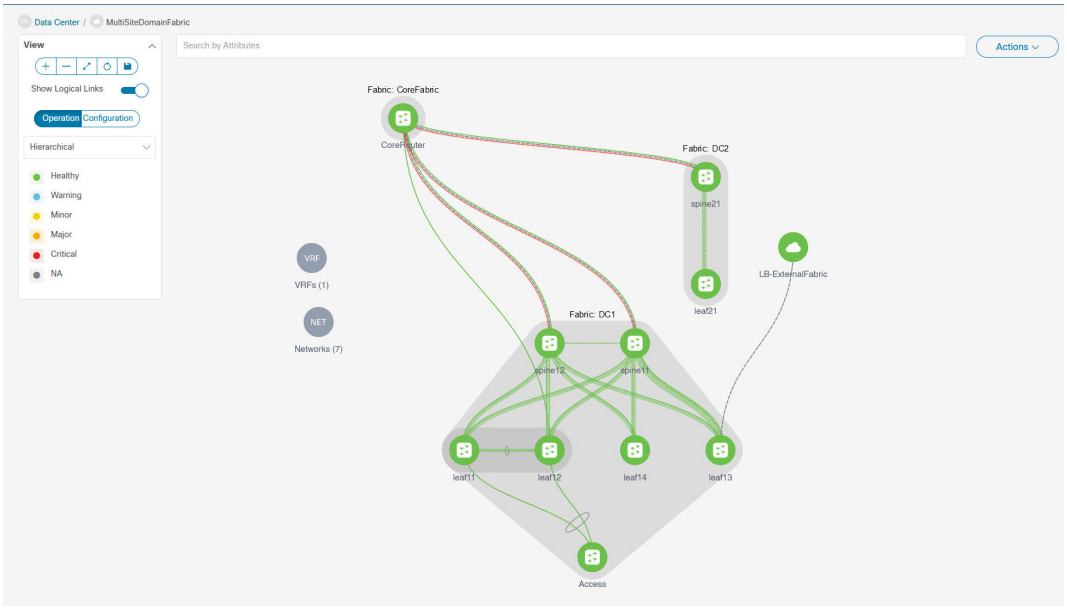
   Member1 が MSD ファブリックに追加され、ファブリック リスト テーブルの **[子ファブリック（Child Fabrics）]** に表示されることがわかります。

MSD ファブリックのトポロジ ビューの指針

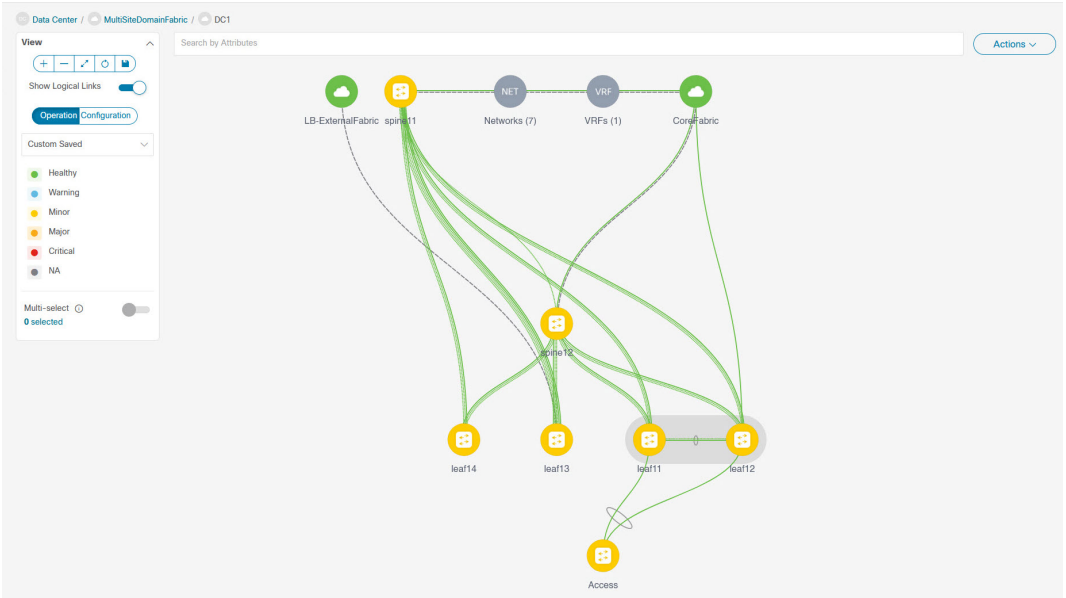
[トポロジ（Topology）] タブには、構成された MSD ファブリックとその子ファブリックが表示されます。

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

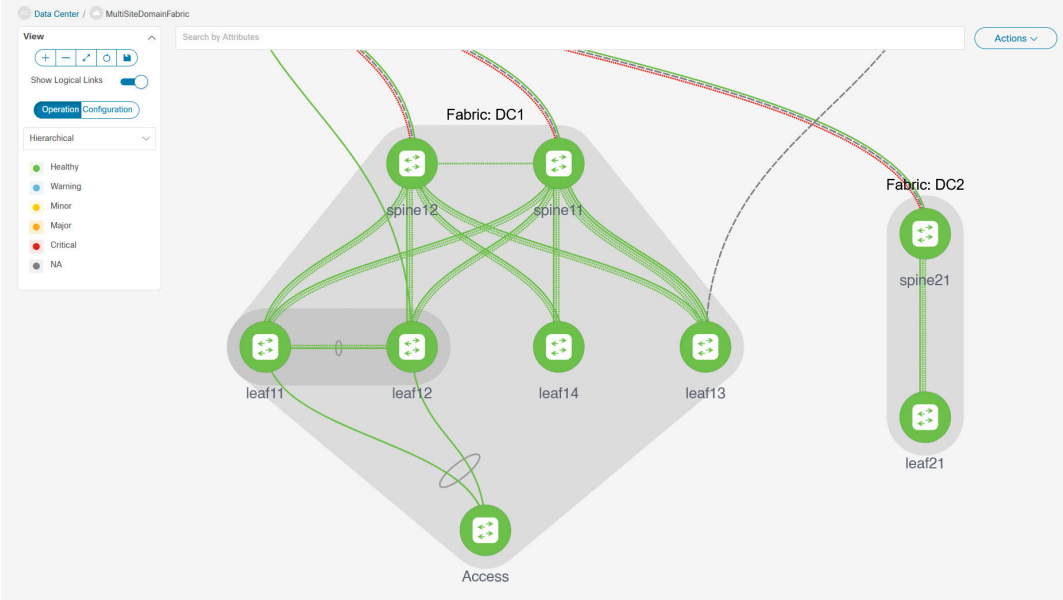
  メンバー ファブリックをダブルクリックして、さらに要素を表示します。



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



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



リンクの追加と編集

リンクを追加するには、**[アクション（Actions）] > [その他（More）] > [リンクを追加（Add Link）]**を選択します。リンクを編集するには、**[アクション（Actions）] > [その他（More）] > [リンクを編集（Edit Link）]**を選択します。

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

MSD ファブリックでのネットワークと VRF の作成と展開

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

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

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

ファブリックごとの展開ビューに加えて、MSD の展開ビューが導入されました。このビューでは、MSD 内のすべてのメンバー ファブリックのオーバーレイ ネットワークを一度に表示

し、プロビジョニングできます。ただし、ファブリックごとにネットワークと VRF の構成を個別に適用して保存する必要があります。

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

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

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

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

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

MSD ファブリックでのネットワークの作成

いくつかのガイドラインと指針：

- MSD ファブリック レベルで **[ボーダーで L3 ゲートウェイを有効にする（Enable L3 Gateway on Border）]** チェックボックスをオンにして、NDFC サービスをアップグレードしようとすると、アップグレード中に MSD ファブリック レベルから自動的に削除されます。
- MSD ファブリック ネットワークでは、**ネットワーク プロファイル**を一部だけ（**[一般（General）]** タブと **[詳細（Advanced）]** タブで）編集することができます。
- MSD には複数のファブリックを含めることができます。これらのファブリックは、マルチキャストまたは入力レプリケーションを介して BUM トラフィックを転送します。すべてのファブリックが BUM トラフィックにマルチキャストを使用する場合でも、これらのファブリック内のマルチキャスト グループは同じである必要はありません。
- MSD でネットワークを作成すると、すべてのメンバー ファブリックに継承されます。ただし、マルチキャスト グループ アドレスは、ファブリック インスタンス ごとの変数です。マルチキャスト グループ アドレスを編集するには、メンバー ファブリックに移動してネットワークを編集する必要があります。**[マルチキャスト グループ アドレス（Multicast**

Group Address）] フィールドの詳細については、スタンドアロン ファブリックのネットワークの作成を参照してください。

- ネットワークを削除できるのは MSD ファブリックからだけであり、メンバー ファブリックからは削除できません。削除する前には、それぞれのファブリック デバイスでネットワークを展開解除する必要があります。
- MSD ファブリックからネットワークを削除すると、そのネットワークはメンバー ファブリックからも自動的に削除されます。

スタンドアロン ファブリックのネットワークの作成を参照してください。

MSD ファブリックでの VRF の作成

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

VRF の作成を参照してください。

MSD およびメンバー ファブリックでのネットワークと VRF の削除

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

1. 削除する前に、それぞれのファブリック デバイスでネットワークを展開解除します。
2. MSD ファブリックからネットワークを削除します。
3. 削除する前に、それぞれのファブリック デバイスで VRF を展開解除します。
4. MSD ファブリックから VRF を削除します。複数の VRF インスタンスを一度に削除することもできます。

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

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

既存のネットワークと VRF を持つスタンドアロン ファブリックをメンバーとして MSD ファブリックに移動する場合は、共通のネットワーク（つまり、L2 VNI と L3 VNI 情報）、エニーキャスト ゲートウェイ MAC、VRF とネットワーク テンプレートがファブリックと MSD 全体で同じであることを確認してください。NDFC は、スタンドアロンファブリック（ネットワー

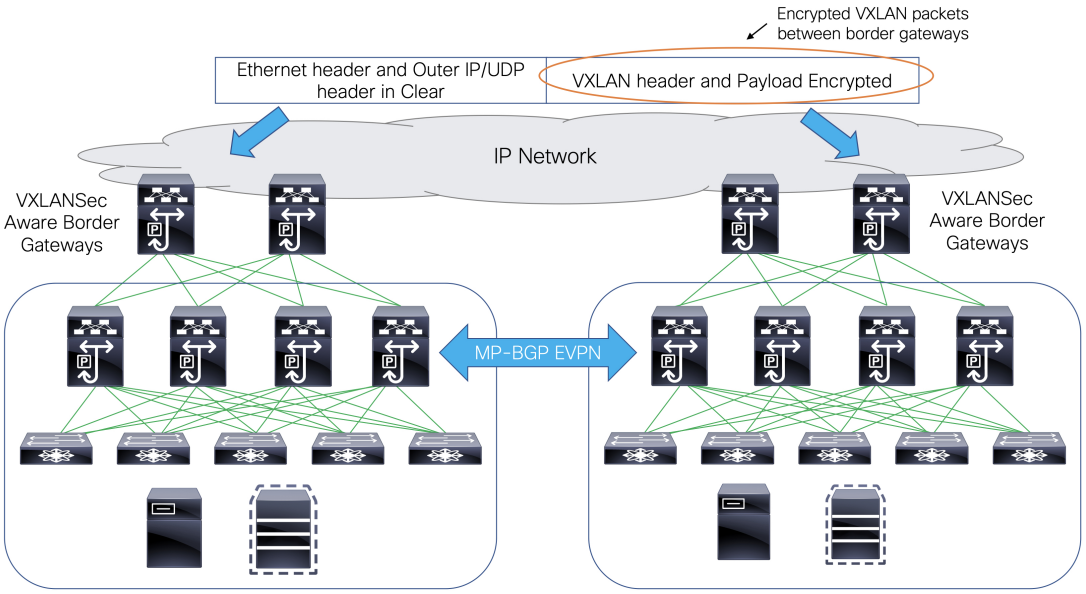
クおよび VRF 情報）を MSD ファブリックの（ネットワークおよび VRF 情報）に対して検証して、エントリの競合を回避します。エントリの競合の例は、2 つの一般的なネットワーク名が異なるネットワーク ID を持っている場合です。検証後、競合がなければ、スタンドアロン ファブリックはメンバー ファブリックとして MSD ファブリックに移動されます。詳細:

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

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

マルチサイト展開での CloudSec のサポート

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



CloudSec 機能は、Cisco NX-OS リリース 9.3(5) 以降を搭載した Cisco Nexus 9000 シリーズ FX2 プラットフォームでサポートされています。FX2 プラットフォームであり、Cisco NX-OS リ

リース 9.3(5) 以降を実行するボーダー ゲートウェイ、ボーダー ゲートウェイ スパイン、およびボーダー ゲートウェイ スーパースパインは、CloudSec 対応スイッチと呼ばれます。

CloudSec は、MSD ファブリックの作成中に有効にすることができます。

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

MSD で CloudSec を有効にする

NDFC Web UI で、**[LAN] > [ファブリック（Fabircs）]** を選択します。**[ファブリックの作成（Create Fabric）]** をクリックして新しい MSD ファブリックを作成するか、**[ファブリックの編集（Edit Fabric）]** をクリックして既存の MSD ファブリックを編集することができます。

[DCI] タブで、CloudSec 構成の詳細を指定できます。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NDFC の CloudSec 機能を使用すると、MSD 内のすべてのゲートウェイが同じキーチェーン（および 1 つのキー文字列のみ）を持ち、ポリシーを持つようにすることができます。NDFC に 1 つのキー チェーン文字列を指定して、キー チェーン ポリシーを形成することができます。NDFC は、すべてのデフォルト値を使用して encryption-policy を形成します。NDFC は、同じキー チェーン ポリシー、同じ暗号化ポリシー、および暗号化ピア ポリシーを各 CloudSec 対応ゲートウェイにプッシュします。各ゲートウェイには、CloudSec 対応で、同じキーチェーンと同じキー ポリシーを使用する encryption-peer ポリシーが、リモート ゲートウェイごとに 1 つあります。

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

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

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

```
feature tunnel-encryption
evpn multisite border-gateway 600
  dci-advertise-pip
tunnel-encryption must-secure-policy
tunnel-encryption policy CloudSec_Policy1
```

```
tunnel-encryption source-interface loopback20
key chain CloudSec_Key_Chain1 tunnel-encryption
  key 1000
    key-octet-string 7 075e731f1a5c4f524f43595f507f7d737062677147524054594070b0b0701585440

    cryptographic-algorithm AES_128_CMA
tunnel-encryption peer-ip 192.168.0.6
  keychain CloudSec_Key_Chain1 policy CloudSec_Policy1
```

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

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

詳細については、ファブリック スイッチでのフリーフォーム設定の有効化を参照してください。

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

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

CloudSec の動作状態の表示

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

手順

ステップ 1 MSD ファブリックを選択します。

ファブリック トポロジ ウィンドウが表示されます。

ステップ 2 **[アクション（Actions）]** > **[詳細ビュー（Detailed View）]**を選択します。

ステップ 3 **[リンク（Link）]** タブをクリックし、左側の **[CloudSec 操作ビュー（CloudSec Operational View）]** タブを選択します。

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

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

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

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

CloudSec セッションのトラブルシューティング

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

手順

ステップ 1 NDFC Web UI で、**[操作（Operations）] [プログラマブル レポート（Programmable Reports）]** を選択します。

ステップ 2 [Create Report] をクリックします。

ステップ 3 **[レポート名（Report Name）]** フィールドにレポート ジョブの一意な名前を入力します。

ステップ 4 **[テンプレートの選択（Select Template）]** ドロップダウン リストから、**fabric_cloudsec_oper_status** を選択します。

ステップ 5 **[次へ（Next）]** をクリックして、**[ソースと繰り返し（Source & Recurrence）]** タブを表示します。

ステップ 6 **[繰り返し（Recurrence）]** フィールドで、レポート ジョブを実行する頻度を選択します。

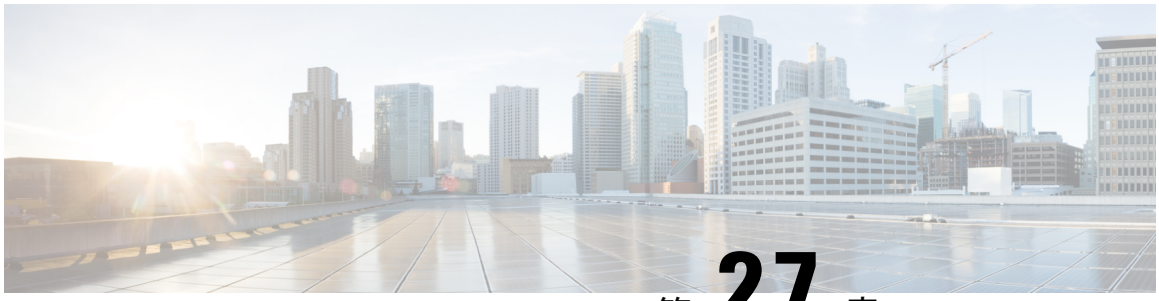
ステップ 7 レポートを電子メールで送信する場合は、**[電子メールレポート先（Email Report To）]** フィールドに電子メールの ID またはメーラーの ID を入力します。

[設定（Settings）] [サーバ設定（Server Settings）] [SMTP] タブで SMTP を設定する必要があります。データ サービスの IP アドレスがプライベート サブネットにある場合は、SMTP サーバーのスタティック管理ルートを Cisco Nexus Dashboard クラスタ設定に追加する必要があります。

ステップ 8 **[ファブリックの選択（Select fabric(s)）]** テーブルで、レポート ジョブを実行する MSD ファブリックを選択します。

ステップ 9 [保存（Save）] をクリックします。

レポート ジョブは、構成された間隔で実行されます。



第 27 章

ToRスイッチの設定と外部ファブリックへのネットワークの展開

この章では、Top-of-Rack（ToR）スイッチを構成し、NDFC にネットワークを展開する方法について説明します。

概要

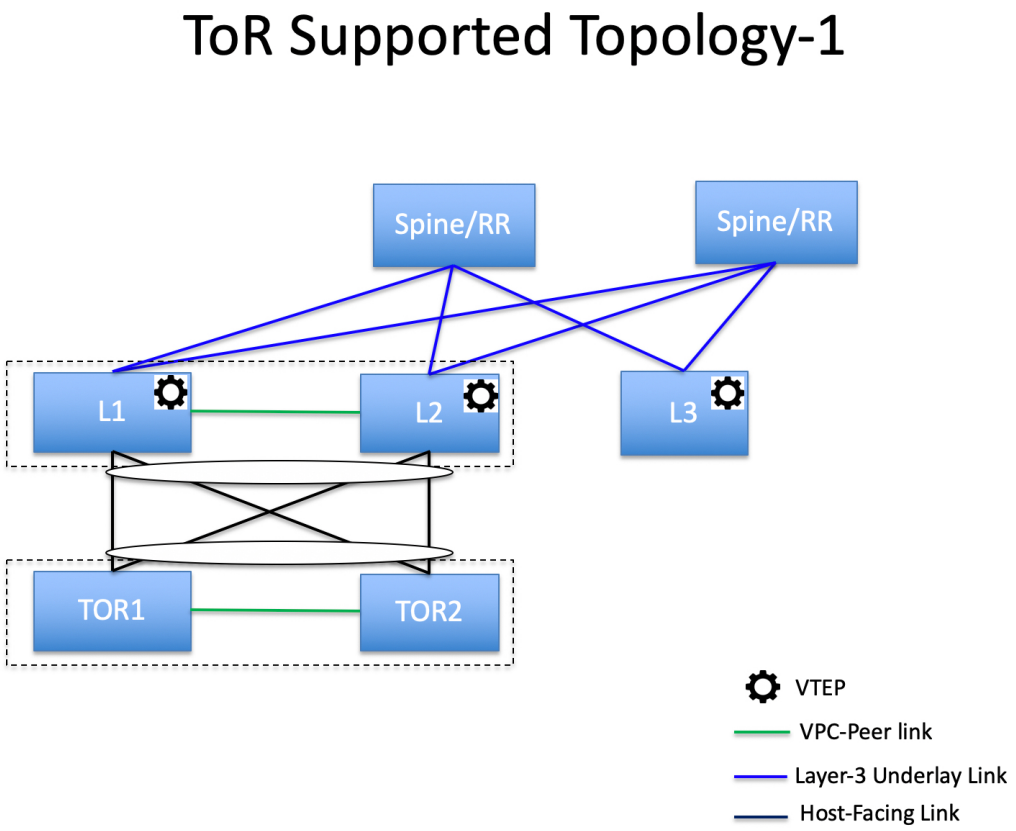
NDFC は、Top-of-Rack（ToR）スイッチをサポートしています。外部ファブリックにレイヤ 2 ToR スイッチを追加でき、それらを Easy ファブリックのリーフ スイッチに接続できます。通常、リーフ デバイスと ToR デバイスはバックツーバック vPC 接続で接続されます。詳細については、「ToR スイッチでサポートされるトポロジ」を参照してください。

ToR スイッチでサポートされるトポロジ

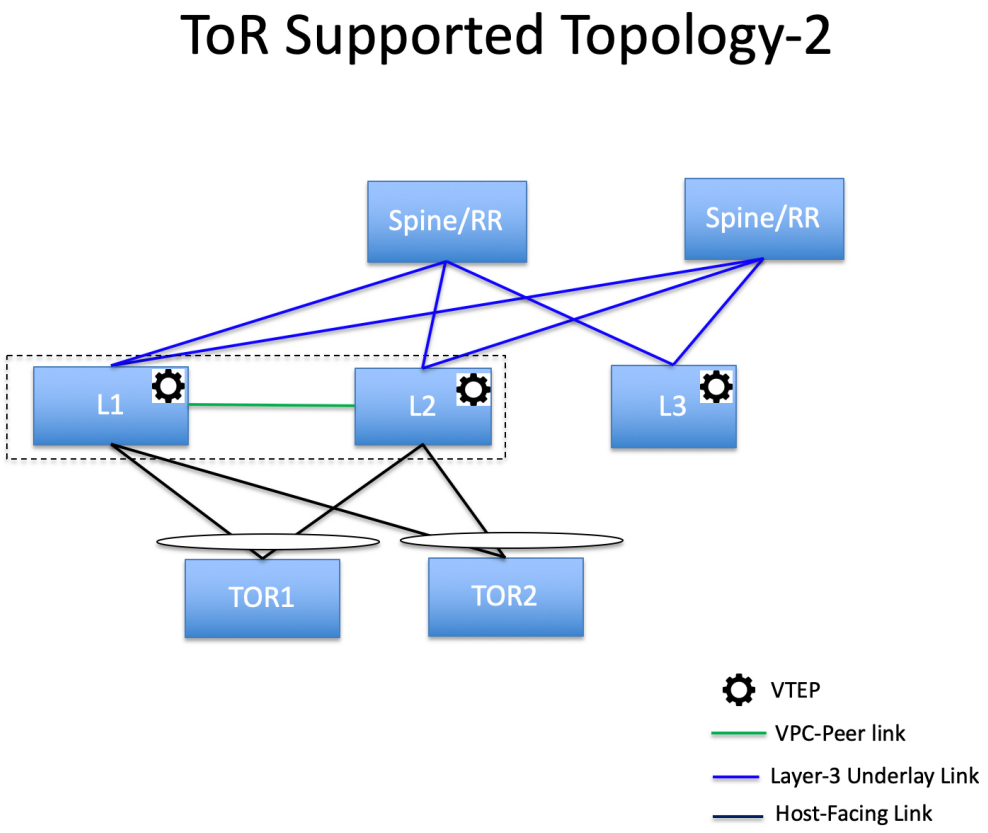
NDFC では、ToR スイッチを使用した次のトポロジがサポートされています。

Note Cisco Nexus 7000 シリーズ スイッチは、Cisco NDFC の **ToR** スイッチ ロールをサポートしていません。

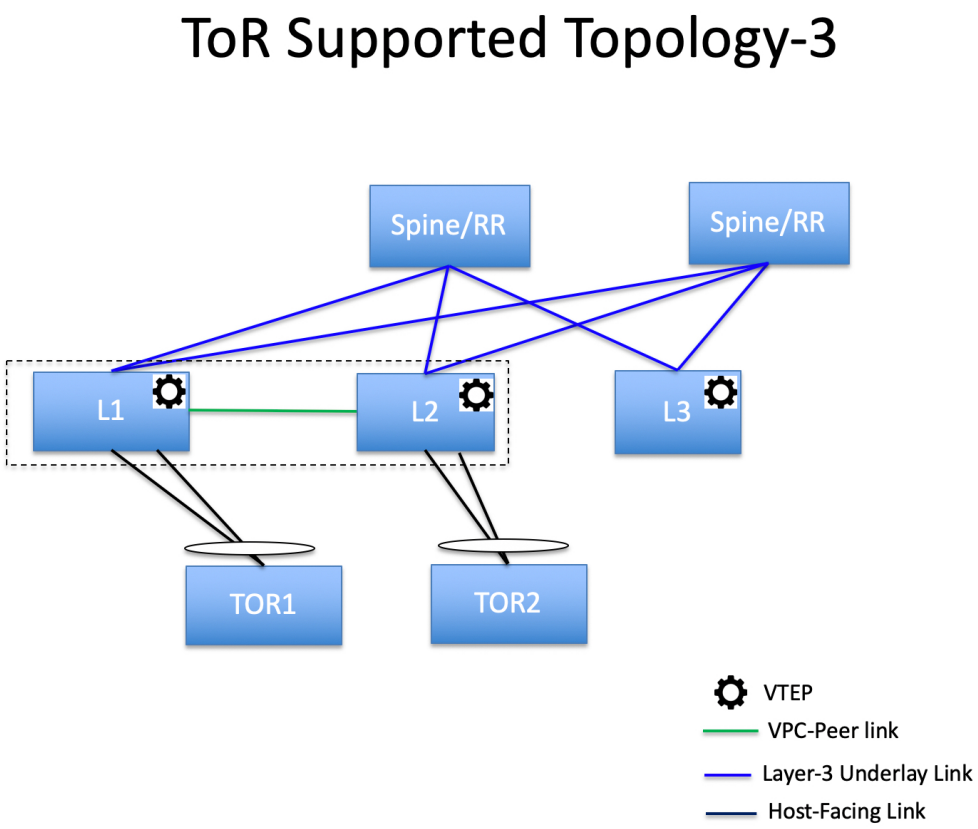
- リーフ スイッチへのバックツーバック vPC 接続を持つ ToR スイッチ。



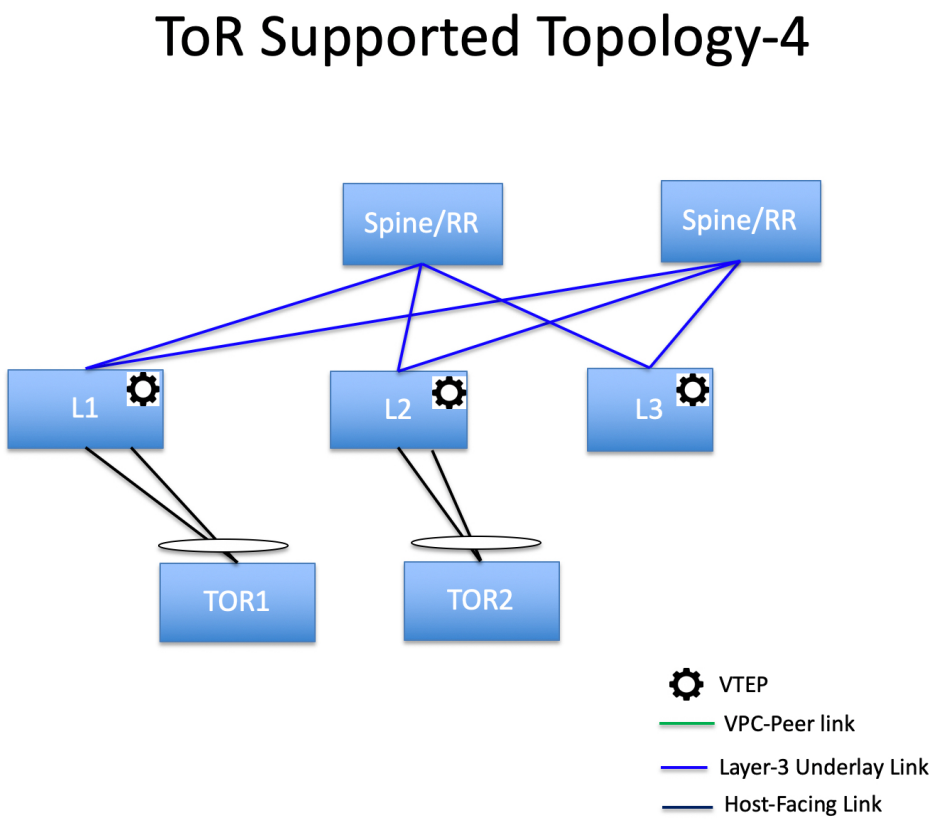
- ポート チャネルが両方のリーフ スイッチに接続されている ToR スイッチ。L1 スイッチと L2 スイッチは vPC ペアとして接続されます。



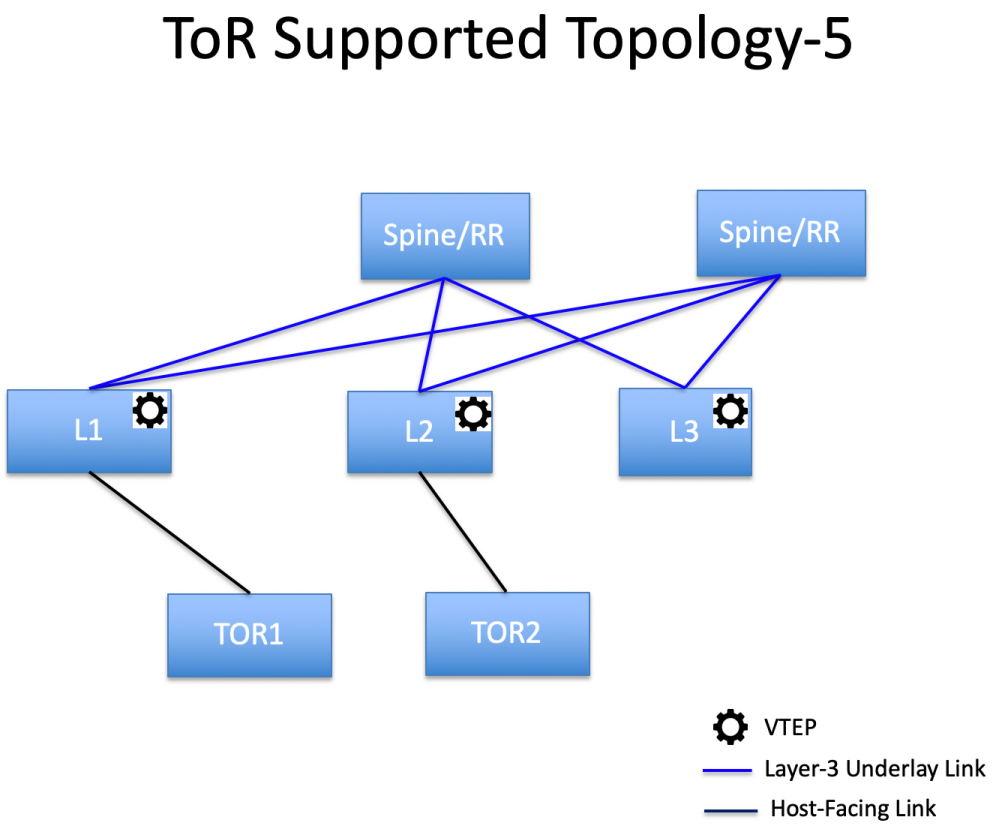
- ポート チャネルがリーフ スイッチに直接接続されている ToR スイッチ。L1 スイッチと L2 スイッチは vPC ペアとして接続されます。



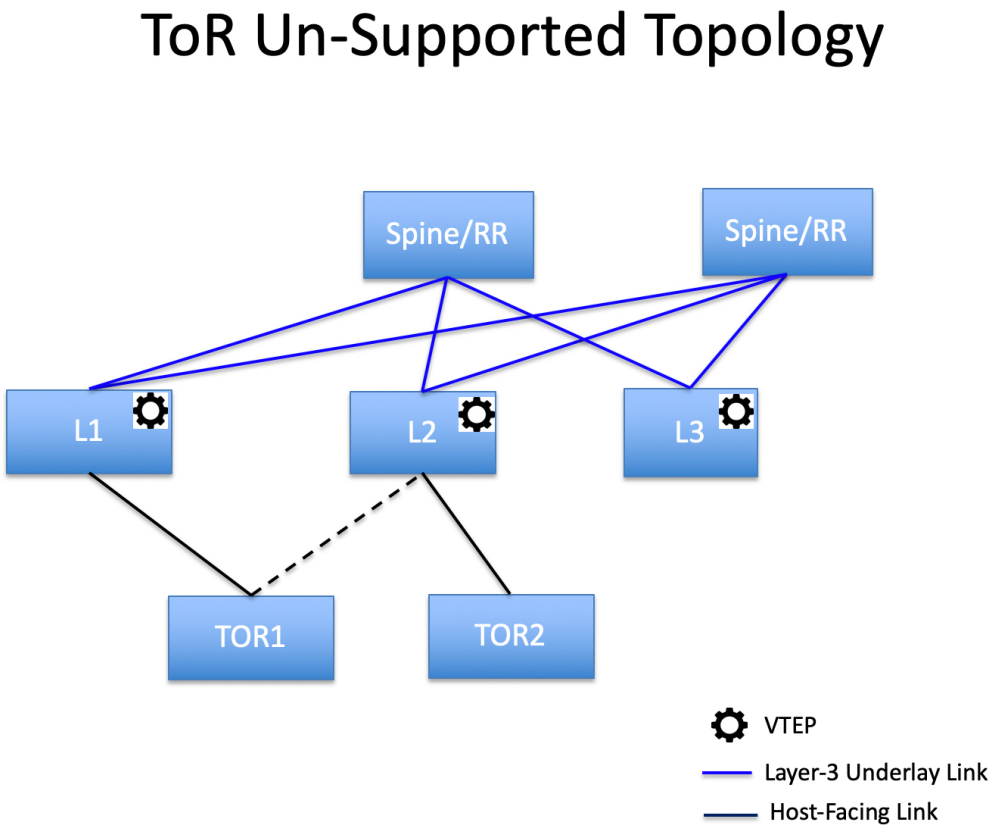
- ポート チャネルがリーフ スイッチに直接接続されている ToR スイッチ。 vPC ペアは、リーフ スイッチまたは ToR スイッチ用に構成されていません。



- リーフ スイッチに直接接続されている ToR スイッチ。 vPC ペアは、リーフ スイッチまたは ToR スイッチ用に構成されていません。



ToR スイッチを使用した次のトポロジは、NDFC ではサポートされていません。



ToR スイッチの構成

開始する前に、Easy ファブリックがあることを確認するか、新しいファブリックを作成して展開してください。詳細については、新規 VXLAN BGP EVPN ファブリックの作成, on page 53を参照してください。

Note NDFC は、ToR スイッチの trunk_host ポリシーをサポートします。ToR に、リーフに接続されたインターフェイスにアタッチされた vPC、ポート チャネル、またはトランク ホスト ポリシーがあることを確認します。これらのポリシーは、外部ファブリックの ToR スイッチを Easy ファブリックのリーフ スイッチに接続するために使用されます。

Procedure

ステップ 1 外部ファブリックを作成し、2 つの ToR スイッチを追加します。詳細については、外部ファブリックの作成, on page 129を参照してください。

ToR スイッチの数は 2 つよりもさらに多くすることができます。この手順は、ToR トポロジ-1 に示すように ToR スイッチを構成する方法を示しています。ここで ToR スイッチは vPC を使用して接続されています。以下は、ToR スイッチを接続するためのさまざまなシナリオです。

- ToR スイッチで vPC が構成されておらず、これらの ToR スイッチのアップリンクが vPC リーフ スイッチに接続されている場合は、ToR に面したインターフェイスに vPC ポリシーを適用する必要があります。
- ToR スイッチがポート チャネルを使用してリーフに接続されている場合は、リーフ スイッチに接続されている ToR インターフェイスにポート チャネル ポリシーを適用する必要があります。
- ToR スイッチがスタンドアロンとしてリーフ スイッチに接続されている場合、トランク ポリシーを TOR インターフェイスに適用する必要があります。

Note
- 外部ファブリックを作成するときは、**[ファブリック モニタ モード（Fabric Monitor Mode）]** チェック ボックスがオンになっていないことを確認してください。
- 2 つの ToR スイッチが接続されていて、同じスイッチ ロールを持っている必要があります。

ToR スイッチを追加したら、ToR スイッチのロールが ToR として選択されていることを確認します。

ステップ 2 ToR スイッチの 1 つを選択し、**[アクション（Actions）]** > **[vPC ペアリング（vPC Pairing）]** をクリックします。

2 番目の ToR スイッチを vPC ピアとして選択します。

ステップ 3 [vPC ペア テンプレート（vPC Pair Template）] で、両方の ToR スイッチ間の vPC 接続に関連するすべての詳細を入力します。フィールドの詳細とその説明については、vPC セットアップの作成, on page 150 を参照してください。

Note この例はトポロジ 1 の ToR 設定を示しているため、手順 2 および 3 が必要です。トポロジ 2、3、4、および 5 の場合、手順 2 と 3 は必要ありません。

ステップ 4 **[スイッチの概要（Switch Overview）]** ウィンドウで、**[アクション（Actions）]** > **[再計算して展開（Recalculate and Deploy）]** の順にクリックします。

ステップ 5 **[構成の展開（Config Deployment）]** ウィンドウで構成が完了したら、**[閉じる（Close）]** をクリックします。

ステップ 6 MSD ファブリックを作成します。

MSD ファブリックの作成中に、[全般（General）] タブで、**[ToR 自動展開フラグ（ToR Auto-deploy Flag）]** チェック ボックスをオンにします。これにより、MSD ファブリックで **[再計算と展開（Recalculate and Deploy）]** をクリックしたときに、Easy ファブリックのネットワークと VRF を外部ファブリックの ToR スイッチに自動展開できます。詳細については、ToR スイッチへのネットワークの展開, on page 727を参照してください。

残りのタブとフィールドについては、*MSD* ファブリックの作成を参照してください。

ステップ 7 MSD ファブリックを開きます。**[子ファブリック（Child Fabrics）]** に移動し、**[アクション（Actions）]** をクリックしてファブリックを MSD に移動します。ToR が接続されている Easy ファブリックを選択し、**[追加（Add）]** をクリックします。

同様に、ToR スイッチを含む外部ファブリックを MSD ファブリックに移動します。

ステップ 8 リーフ スイッチを含む Easy ファブリックを開きます。

ステップ 9 リーフ スイッチと ToR スイッチの間にバックツーバック vPC を作成する必要があります。

ステップ 10 **[LAN]** > **[インターフェイス（Interfaces）]** > **[アクション（Actions）]** > **[インターフェイス（Interface）]**に移動します。

vPC を選択し、関連するすべての詳細を入力して、**[保存（Save）]** をクリックします。

このウィンドウのフィールドの詳細については、インターフェイスの追加, on page 385 を参照してください。

すべての情報を保存したら、**[展開（Deploy）]** をクリックします。

同様に、ステップ 9 および 10 に従って、ToR スイッチ上にも vPC を作成します。

ToR スイッチへのネットワークの展開

外部ファブリックの ToR スイッチにネットワークを展開するには、MSD を介して Easy ファブリックのスイッチにネットワークを展開する必要があります。これらのスイッチはToR スイッチに接続する必要があります。

Procedure

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

ステップ 2 **[ネットワーク（Networks）]** ウィンドウで、展開するネットワークを選択するか、新しいネットワークを作成します。ネットワークの作成については、スタンドアロンファブリック向けのネットワークの作成, on page 231 を参照してください。

ステップ 3 **[ネットワーク（Network）]** を **[ネットワーク アタッチメント（Network Attachment）]** ウィンドウから選択します。**[アクション（Actions）]** をクリックし、[編集（Edit）] を選択します。ネットワークをアタッチし、適切なインターフェイス/ポート チャネルを選択して、**[保存（Save）]** をクリックします。これらのポート チャネルは、リーフ スイッチを ToR スイッチに接続します。ネットワークはこれらのポート チャネルに展開されます。

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 and Deploy）]**をクリックします。

これで、VLAN がリーフ スイッチに展開されました。

ステップ 5 MSD ファブリックに移動します。

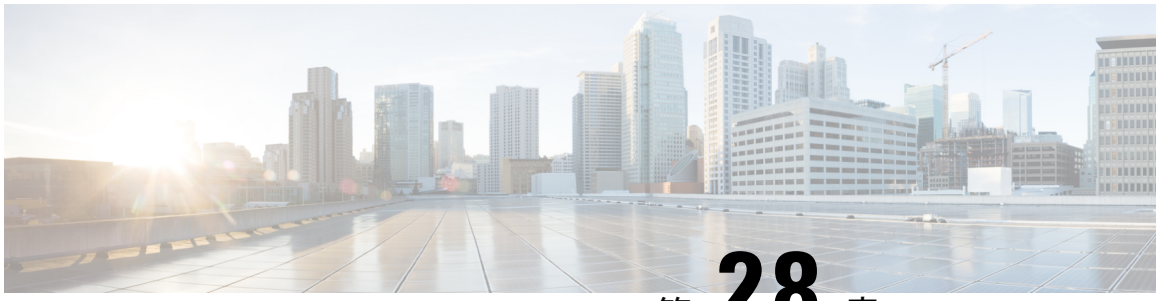
ステップ 6 **[ファブリックの概要（Fabric Overview）]** ウィンドウで、**[アクション（Actions）]** > **[再計算と展開（Recalculate and Deploy）]**をクリックします。

Easyファブリックのリーフスイッチで作成および展開されたネットワークは、外部ファブリックの ToR スイッチにも展開されます。この手順により、手順 4 でリーフ スイッチに展開された ToR スイッチに同じ VLAN を構成できます。

Note フリーフォーム構成を使用してToRスイッチでVLANを手動で作成した場合、VLANは変更されません。

第 VII 部

VXLAN BGP EVPN ファブリックの外部/WAN レイヤ 3 接続



第 28 章

MPLS SR および LDP ハンドオフ

この章では、MPLS ハンドオフ機能を構成する方法について説明します。

VXLAN EVPN から SR-MPLS および MPLS LDP への相互接続の概要

Nexusダッシュボード ファブリック コントローラ（NDFC）は、次のハンドオフ機能をサポートしています。

- VXLAN から SR-MPLS
- VXLAN から MPLS LDP

これらの機能は、**Easy_Fabric** テンプレートを使用して、VXLAN ファブリックのボーダー デバイス、つまりボーダー リーフ、ボーダー スパイン、およびボーダー スーパー スパインで提供されます。デバイスは Cisco NX-OS リリース 9.3(1) 以降を実行している必要があることに注意してください。これらの DCI ハンドオフ アプローチは、外部ファブリックに追加のプロバイダー エッジ（PE）デバイスを必要としないワンボックス DCI ソリューションです。

Note スイッチが Cisco NX-OS リリース 7.0(3)I7(X) を実行している場合、MPLS ハンドオフ機能を有効にすると、スイッチがリロードされたときに、NVE 関連の構成プロファイル CLI が削除されます。

NDFC DCI MPLS ハンドオフ機能では、ボーダー デバイスを外部ファブリックに接続するためのアンダーレイ ルーティング プロトコルは ISIS または OSPF であり、オーバーレイ プロトコルは eBGP です。VXLAN ファブリックと、SR-MPLS または MPLS LDP を実行している外部ファブリックとの間の NS トラフィックがサポートされています。ただし、SR-MPLS または MPLS LDP 経由で 2 つのデータセンター VXLAN ファブリックを接続するために NDFC を使用できます。

サポートされるプラットフォームと構成

次の表は、サポート対象のプラットフォームに関する情報を示しています。

機能	サポートされるプラットフォーム
VXLAN から SR-MPLS	Cisco Nexus 9300-FX2/FX3/GX、N9K-X96136YC-R、および Cisco Nexus 3600 R シリーズ スイッチ
VXLAN から MPLS LDP	N9K-X96136YC-R および Cisco Nexus 3600 R シリーズ スイッチ

次の機能はスイッチでサポートされていないため、サポートされていません。

- MPLS LDP と SR-MPLS 相互接続の共存
- vPC

VXLAN から SR-MPLS へのハンドオフ機能は、次の設定で構成されます。

- 基本の SR-MPLS 機能構成。
- DCI ハンドオフ デバイスと、アンダーレイ接続のための外部ファブリック内のデバイス間のアンダーレイ構成。NDFC は、アンダーレイ接続のルーティング プロトコルとして ISIS または OSPF をサポートします。
- DCI ハンドオフ デバイスと、外部ファブリック内のコア ルータまたはエッジ ルータ、または別のファブリック内の別のボーダーデバイスとの間のオーバーレイ構成。接続は eBGP を介して確立されます。
- VRF プロファイル

VXLAN から MPLS LDP へのハンドオフ機能は、次の設定で構成されます。

- 基本の MPLS LDP 機能構成。
- DCI ハンドオフ デバイスと、アンダーレイ接続のための外部ファブリック内のデバイス間のアンダーレイ構成。NDFC は、アンダーレイ接続のルーティング プロトコルとして ISIS または OSPF をサポートします。
- DCI ハンドオフ デバイスと、外部ファブリック内のコア ルータまたはエッジ ルータ、または別のファブリック内の別のボーダーデバイスとの間のオーバーレイ構成。接続は eBGP を介して確立されます。

- VRF プロファイル

MPLS ハンドオフのためのファブリック間接続

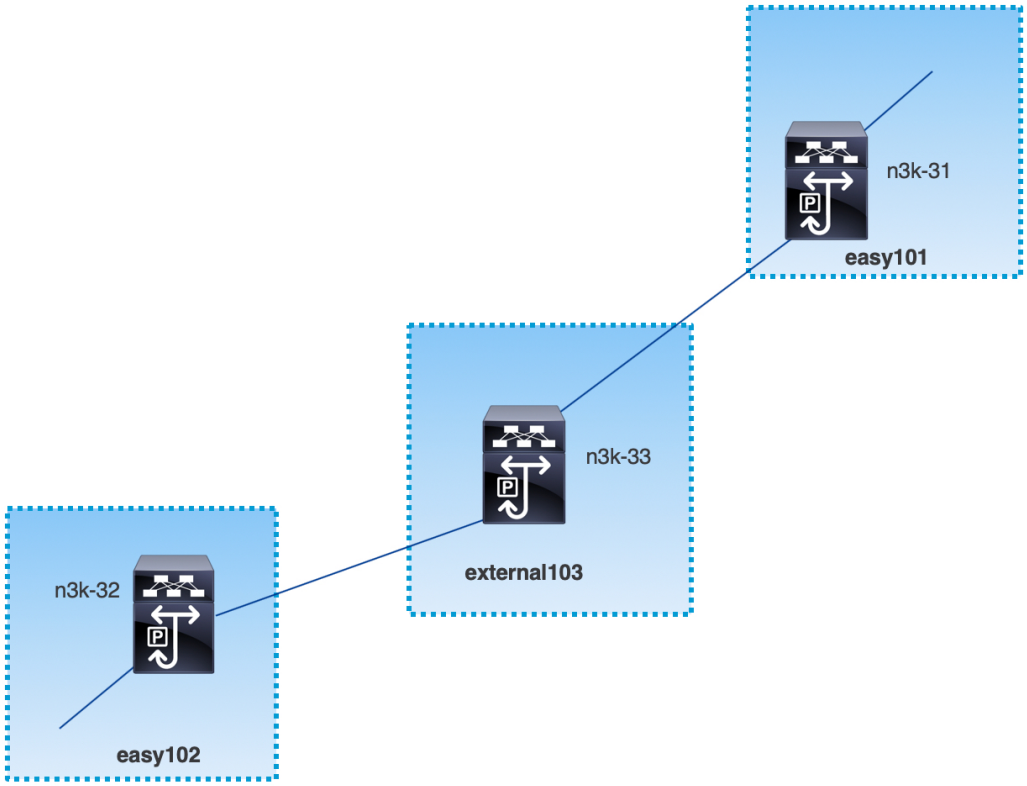
次の 2 つのファブリック間接続リンクが導入されています。

- アンダーレイ構成用の **VXLAN_MPLS_UNDERLAY**：このリンクは、ボーダーと外部デバイス（または MPLS または SR-MPLS の P ルータ）の間の各物理リンクまたはレイヤ 3 ポート チャネルに対応します。複数のリンクが 1 つ以上の外部デバイスに接続できるため、ボーダー デバイスは複数のファブリック間接続リンクを持つことができます。
- eBGP オーバーレイ設定用の **VXLAN_MPLS_OVERLAY**：このリンクは、DCI ハンドオフ デバイスと、外部ファブリックのコアまたはエッジルータ、または別のファブリックの別のボーダー デバイスとの間の仮想リンクに対応します。このファブリック間接続リンクは、イメージとプラットフォームの要件を満たすボーダーデバイスでのみ作成できます。ボーダー デバイスは、複数のコア ルータまたはエッジ ルータと通信できるため、このタイプの IFC リンクを複数持つことができます。

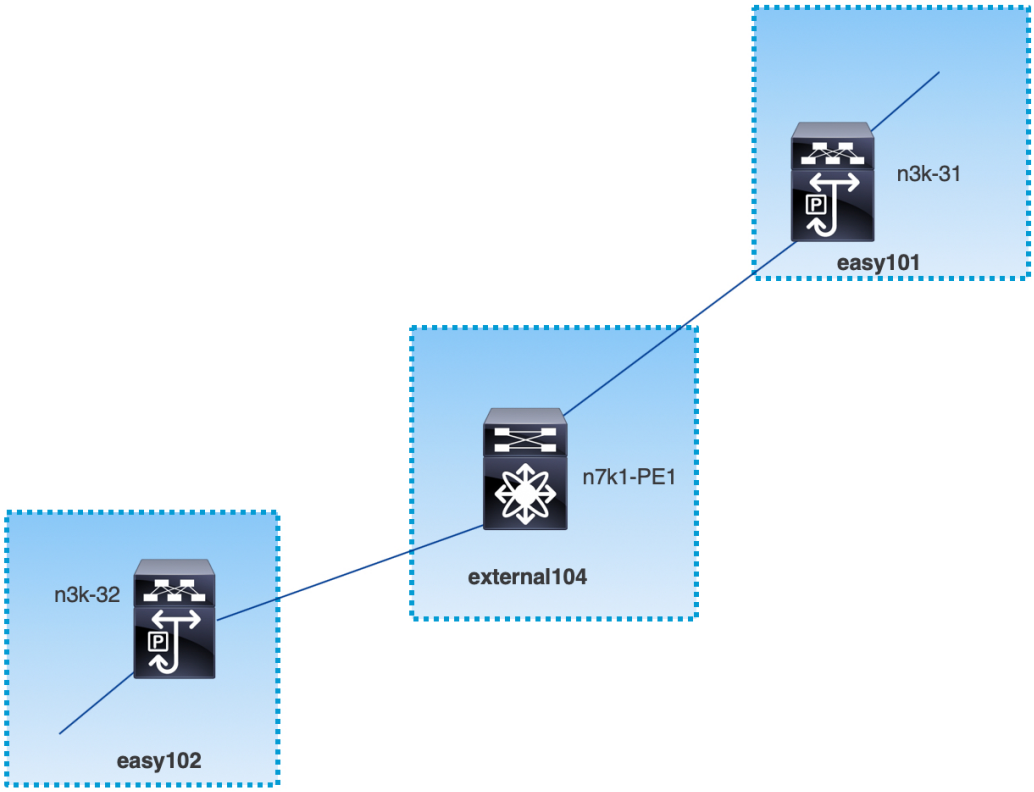
これらのファブリック間接続は、NDFC Web UI または REST API を使用して手動で作成できます。これらのファブリック間接続の自動作成はサポートされていないことに注意してください。

VXLAN MPLS トポロジ

MPLS-SR トポロジ



MPLS-LDP トポロジ



このトポロジは、Easy ファブリックのボーダー デバイスと、外部ファブリックのコアまたはエッジ ルータのみを示しています。

- **Easy_Fabric** テンプレートを使用しているファブリックは次のとおりです。
  - **easy101**
  - **easy102**
- **External_Fabric** テンプレートを使用しているファブリックは次のとおりです。
  - **external103**
  - **external104**
- 外部ファブリック **external103** は、MPLS SR プロトコルを実行しています。
- 外部ファブリック **external104** は、MPLS LDP プロトコルを実行しています。
- **n3k-31** および **n3k-32** は、VXLAN から MPLS へのハンドオフを実行するボーダー デバイスです。
- **n7k-PE1** は MPLS LDP のみをサポートします。
- **n3k-33** は SR-MPLS をサポートします。

VXLAN MPLS ハンドオフの構成タスク

MPLS ハンドオフ機能の構成には、次のタスクが含まれます。

1. MPLS ハンドオフを有効にするためのファブリック設定の編集。
2. ファブリック間のアンダーレイ ファブリック間接続リンクの作成。

   ファブリック間接続リンク設定で、MPLS SR または LDP のどちらを使用しているかを指定します。
3. ファブリック間のオーバーレイ ファブリック間接続リンクの作成。
4. VXLAN から MPLS への相互接続のための VRF の展開。

MPLS ハンドオフのファブリック設定の編集

このセクションでは、Easyファブリックと外部ファブリックのファブリック設定を編集して、MPLS ハンドオフ機能を有効にする方法を示します。

Easy ファブリック設定の編集

Procedure

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

ステップ 2 **[アクション（Actions）]** ドロップダウン リストから、**[ファブリックの編集（Edit Fabric）]** を選択して、ファブリックを編集します。

ステップ 3 [Advanced] タブをクリックします。

[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。

注：ブラウンフィールドインポートの場合は、**[MPLS ハンドオフを有効にする（Enable MPLS Handoff）]** 機能を選択します。IFC 構成のほとんどは、**switch_freeform** にキャプチャされます。

[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。

ステップ 4 [リソース（Resources）] タブをクリックします。

[アンダーレイ MPLS ループバック IP 範囲（Underlay MPLS Loopback IP Range）]：アンダーレイ MPLS 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。

ステップ 5 **[保存（Save）]** をクリックして、ファブリック内の各ボーダー デバイスに MPLS 機能を設定します。

ステップ 6 **[アクション（Actions）]** ドロップダウンリストから、**[再計算と導入（Recalculate and Deploy）]** を選択します。

残りのフィールドの詳細については、新しい VXLAN BGP EVPN ファブリックの作成を参照してください。

外部ファブリック設定の編集

Procedure

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

ステップ 2 **[アクション（Actions）]** ドロップダウンリストから、**[ファブリックの編集（Edit Fabric）]** を選択して、ファブリックを編集します。

ステップ 3 (Optional) **[一般パラメータ（General Parameters）]** タブで、**[ファブリック モニター モード（Fabric Monitor Mode）]** チェックボックスをオフにします。

ステップ 4 [Advanced] タブをクリックします。

[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。

[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。

ステップ 5 [リソース（Resources）] タブをクリックします。

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

IP 範囲は一意である必要がある点に注意してください。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 6 **[保存（Save）]** をクリックして、ファブリック内の各エッジルータまたはコアルータで MPLS 機能を構成します。

ステップ 7 **[アクション（Actions）]** ドロップダウンリストから、**[再計算と導入（Recalculate and Deploy）]** を選択します。

残りのフィールドの詳細については、外部ファブリックの作成を参照してください。

アンダーレイ ファブリック間接続の作成

この手順は、アンダーレイ ファブリック間接続リンクを作成する方法を示しています。

Procedure

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

ステップ 2 MPLS へのアンダーレイ ファブリック間接続を作成する VXLAN ファブリックを選択します。

ステップ 3 **[ファブリックの概要（Fabric Overview）]** ウィンドウで、**[リンク（Links）]** タブをクリックします。

ステップ 4 ファブリックに対してすでに検出されている既存のリンクを確認します。

この例では、**easy101** から **external103** へのリンクがすでに検出されています。

ステップ 5 検出された既存のリンクを選択し、**[アクション（Actions）]** > **[編集（Edit）]**をクリックします。

リンクが見つからない場合は、**[アクション（Actions）]**>**[作成（Create）]**をクリックし、ファブリック間リンクを追加するためのすべての詳細を指定します。

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、必要な情報をすべて入力します。

[リンク タイプ（Link Type）] : [ファブリック間（inter-fabric）] を選択します。

[リンク サブタイプ（Link Sub-Type）] : ドロップダウン リストから [VXLAN_MPLS_Underlay] を選択します。

[リンク テンプレート（Link Template）] : ドロップダウン リストから [ext_vxlan_mpls_underlay_setup] を選択します。

[一般パラメータ（General Parameters）] タブで、すべての詳細を指定します。

[IP アドレス/マスク（IP Address/Mask）] : 送信元インターフェイスのマスク付き IP アドレスを指定します。

[ネイバー IP（Neighbor IP）] : 宛先インターフェイスの IP アドレスを指定します。

[MPLS ファブリック （MPLS Fabric）] : 外部ファブリックが SR または LDP を実行しているかどうかを指定します。

Note MPLS SR と LDP は、単一のデバイス上で共存できません。

[送信元 SR インデックス（Source SR Index）] : 送信元ボーダーの一意の SID インデックスを指定します。**[LDP]** を **[MPLS ファブリック（MPLS Fabric）]** フィールドで選択した場合、このフィールドは無効になります。

[宛先 SR インデックス（Destination SR Index）]：宛先ボーダーの一意の SID インデックスを指定します。[LDP] を **[MPLS ファブリック（MPLS Fabric）]** フィールドで選択した場合、このフィールドは無効になります。

[SR グローバル ブロック範囲 （SR Global Block Range）]：SR グローバル ブロック範囲を指定します。ファブリック全体で同じグローバルブロック範囲が必要です。デフォルトの範囲は 16000～23999 です。[LDP] を **[MPLS ファブリック（MPLS Fabric）]** フィールドで選択した場合、このフィールドは無効になります。

[DCI ルーティング プロトコル（DCI Routing Protocol）]：DCI MPLS アンダーレイ リンクで使用されるルーティング プロトコルを指定します。**is-is** または **ospf** のいずれかを選択できます。

[OSPF エリア ID（OSPF Area ID）]：ルーティング プロトコルとして OSPF を選択した場合は、OSPF エリア ID を指定します。

[DCI ルーティング タグ（DCI Routing Tag）]：DCI ルーティング プロトコルに使用される DCI ルーティング タグを指定します。

ステップ 7 [保存（Save）] 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。

ステップ 9 **[構成の展開（Deploy Configuration）]** ウィンドウで、**[構成の展開（Deploy Config）]** をクリックします。

ステップ 10 **[LAN ファブリック（LAN Fabrics）]** ウィンドウから宛先ファブリックに移動し、**[再計算と展開（Recalculate & Deploy）]** を実行します。つまり、ステップ 9 と 10 を実行します。

オーバーレイ ファブリック間接続の作成

この手順では、アンダーレイ ファブリック間接続を作成した後で、オーバーレイ ファブリック間接続を作成する方法を示します。オーバーレイ接続は eBGP を使用するため、オーバーレイ ファブリック間接続は MPLS SR と LDP で同じです。

Procedure

ステップ 1 **[リンク（Links）]** タブで、**[アクション（Actions）]** > **[作成（Create）]** をクリックします。

ステップ 2 **[リンク管理 - リンクの作成（Link Management - Create Link）]** ウィンドウで、すべての詳細を入力します。

[リンク タイプ（Link Type）]：**[ファブリック間（Inter-Fabric）]** を選択します。

[リンクのサブ タイプ（ Link-Sub Type）]：ドロップダウン リストから **VXLAN_MPLS_OVERLAY** を選択します。

[リンク テンプレート（Link Template）]：ドロップダウン リストから **ext_vxlan_mpls_overlay_setup** を選択します。

[送信元ファブリック（Source Fabric）]：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ます。

[宛先ファブリック（Destination Fabric）]：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（Source Device）] と **[送信元インターフェイス（Source Interface）]**：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。ループバック インターフェイスの IP アドレスは、オーバーレイ eBGP ピアリングに使用されます。

[宛先デバイス（Destination Device）] と **[宛先インターフェイス（Destination Interface）]**：送信元デバイスに接続する宛先デバイスとループバック インターフェイスを選択します。

[一般パラメータ] タブで、すべての詳細を指定します。

[BGP ローカル ASN（BGP Local ASN）]：このフィールドには、送信元デバイスの AS 番号が自動入力されます。

[BGP ネイバー IP（BGP Neighbor IP）]：このフィールドには、eBGP ピアリングの宛先デバイスのループバック インターフェイスの IP アドレスを入力します。

[BGP ネイバー ASN（BGP 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 [保存（Save）] をクリックします。

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。

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

ステップ 6 **[LAN ファブリック（LAN Fabrics）]** ウィンドウから宛先ファブリックに移動し、**[再計算と展開（Recalculate & Deploy）]** を実行します。つまり、ステップ 4 と 5 を実行します。

Note スイッチに MPLS オーバーレイ IFC リンクが 1 つしかない場合、MPLS オーバーレイ リンクのいずれかの端に VRF がアタッチされていない場合にのみ、それを削除できます。

VRF の導入

この手順は、VXLAN から MPLS への相互接続に VRF を展開する方法を示しています。

Note 4 バイトの ASN を使用し、自動ルート ターゲットが構成されている場合、自動的に生成されるルート ターゲットは 23456:VNI です。2 つの異なるファブリックの 2 つの異なる VRF に同じ VNI 値がある場合、自動ルート ターゲットにより、2 つの VRF のルート ターゲットは同じになり、値 23456 は常に一定です。VXLAN MPLS ハンドオフを介して接続された 2 つのファブリックの場合、これにより、意図しないルート交換が発生する可能性があります。したがって、セキュリティ上の理由から自動ルート ターゲットを無効にする場合は、ネットワーク テンプレートとネットワーク拡張テンプレートをカスタマイズすることで無効にすることができます。

Procedure

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。 >

ステップ 2 **[VRF]** タブで、**[アクション（Actions）]** > **[作成（Create）]** をクリックして、VRF を作成します。詳細については、スタンドアロン ファブリックの VRF の作成を参照してください。

ステップ 3 新しく追加された VRF を選択し、**[続行（Continue）]** をクリックします。

ステップ 4 **[VRF 展開（VRF Deployment）]** ウィンドウで、ファブリックのトポロジを確認できます。ボーダー デバイスを選択して、MPLS LDP IFC リンクが作成されるボーダー デバイスに VRF をアタッチします。

この例では、**n3k-31** は **easy101** ファブリックのボーダー デバイスです。

ステップ 5 **[VRF 拡張アタッチメント（VRF Extension Attachment）]** ウィンドウで、VRF を選択し、[CLI フリーフォーム（CLI Freeform）] 列の下にある **[フリーフォーム構成（Freeform config）]** ボタンをクリックします。

ステップ 6 次のフリーフォーム構成を VRF に手動で追加します。

```
vrf context $$VRF_NAME$$
  address-family ipv4 unicast
    route-target import $$REMOTE_PE_RT$$
  address-family ipv6 unicast
    route-target import $$REMOTE_PE_RT$$
```

フリーフォーム構成では、*REMOTE_PE_RT* は、ネイバーが NDFC によって管理される Easy Fabric のボーダー デバイスである場合、**ASN:VNI** 形式のネイバーの BGP ASN および VNI 番号を参照します。

ステップ 7 **[構成の保存（Save Config）]** をクリックします。

ステップ 8 (Optional) ボーダー デバイスのループバック ID とループバック IPv4 アドレスと IPv6 アドレスを入力します。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 (Optional) **[プレビュー（Preview）]** アイコン（**[VRF 展開（VRF Deployment）]** ウィンドウ）をクリックして、展開される構成をプレビューします。

ステップ 11 [展開（Deploy）] をクリックします。

ネイバーが NDFC によって管理される Easy ファブリックのボーダー デバイスである場合は、宛先ファブリックでステップ 3 からステップ 11 までの同じタスクを実行します。

ルーティング プロトコルと MPLS 設定の変更

この手順では、デバイスのルーティング プロトコルを IS-IS から OSPF に変更する方法、またはアンダーレイ IFC を MPLS SR から LDP に変更する方法を示します。

Note MPLS SR と LDP はデバイス上で共存できず、同じデバイスで MPLS ハンドオフに IS-IS と OSPF の両方を使用することはサポートされていません。

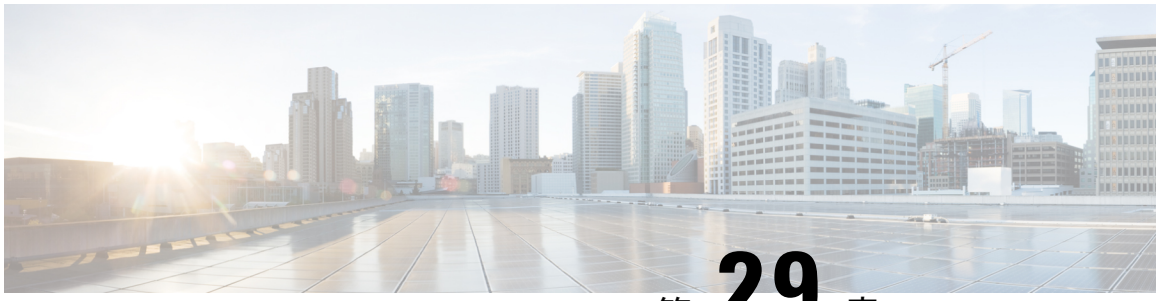
Procedure

ステップ 1 DCI ルーティング プロトコルまたは MPLS ファブリックの変更が必要な場合には、デバイスから、すべての MPLS アンダーレイおよびオーバーレイ IFC を削除します。

ステップ 2 IFC の削除に関係する各ファブリックについて、**[再計算と展開（Recalculate & Deploy）]** をクリックします。

この手順により、すべてのグローバル MPLS SR/LDP 構成と、以前に作成された MPLS ループバック インターフェイスが削除されます。

ステップ 3 優先される DCI ルーティング プロトコルと MPLS 設定を使用して、新しい IFC を作成します。詳細については、アンダーレイ ファブリック間接続の作成 , on page 738を参照してください。



第 29 章

VRF Lite

VRF Lite

データ センター ファブリックの一部であるワークロードが WAN またはバックボーン サービスを介して外部ファブリックと通信する可能性がある場合、データ センターからの外部接続は主要な要件です。North-South トラフィック フローのレイヤ 3 を有効にするには、データセンターの境界デバイスと外部ファブリック エッジ ルータ間で仮想ルーティングおよび転送インスタンス（VRF）Lite ピアリングを使用します。

仮想拡張ローカルエリア ネットワーク（VXLAN）イーサネット仮想プライベート ネットワーク（EVPN）ファブリックでは、境界ルータまたは境界ゲートウェイ ルータにすることが可能です。次のデバイスで VRF Lite を有効にできます。

- 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
- ボーダースーパースパイン

前提条件とガイドライン

- VRF Lite には、Cisco Nexus 9000 シリーズと、Cisco Nexus オペレーティング システム（NX-OS）リリース 7.0(3)I6(2) 以降が必要です。
- VXLAN BGP EVPN データセンター ファブリック アーキテクチャおよび NDFC を介した VXLAN オーバーレイ プロビジョニングに関する知識。
- さまざまなリーフおよびスパインデバイスのアンダーレイおよびオーバーレイ構成、NDFC を介した外部ファブリック構成、および関連する外部ファブリック デバイス構成（エッジ ルータなど）を含む、完全に構成された VXLAN BGP EVPN ファブリック。
  - VXLAN BGP EVPN ファブリック（および North-South トラフィック フローの外部レイヤ 3 ドメインへの接続）は、手動または NDFC を使用して構成できます。

    このドキュメントでは、NDFC を介してファブリックをエッジルータ（ファブリックの外部、外部ファブリックに向かって）に接続するプロセスについて説明します。したがって、NDFC を介して VXLAN BGP EVPN および外部ファブリックを構成および展開する方法を知っている必要があります。
  - VRF Lite は、物理イーサネット インターフェイスまたはレイヤ 3 ポート チャネルで有効にできます。VRF が拡張される各 VRF Lite リンクの VRF 拡張時に NDFC で作成される物理インターフェイスまたはレイヤ 3 ポート チャネル インターフェイス上のサブインターフェイス。
- VRF Lite IFC を削除するには、IFC で有効になっているすべての VRF 拡張を削除します。それ以外の場合は、エラー メッセージが報告されます。VRF Lite アタッチメントを削除した後、ファブリックを再計算して展開し、保留中のレイヤ 3 拡張設定をすべて削除します。これにより、デバイス上の VRF ごとのサブインターフェイスおよび VRF ごとの外部ボーダー ゲートウェイ プロトコルの設定が削除されます。
- VXLAN VRF を作成するときは、以下の 3 つのフィールドを確認してください。
  - **[ホスト ルートのアドバタイズ（Advertise Host Routes）]**：デフォルトでは、VRF Lite ピアリング セッションの場合、非ホスト（/32 または /128）プレフィックスのみがアドバタイズされます。ホスト ルート（/32 または /128）を有効にして、境界デバイスからエッジ/WAN ルータにアドバタイズする必要がある場合は、**[ホスト ルートのアドバタイズ（Advertise Host Routes）]** チェック ボックスをオンにします。ルート マップはアウトバウンドフィルタリングを行います。デフォルトでは、このチェックボックスは無効になっています。
  - **[デフォルト ルートのアドバタイズ（Advertise Default Route）]**：このフィールドは、VRF でネットワーク ステートメント 0/0 を有効にするかどうかを制御します。これにより、BGP で 0/0 ルートがアドバタイズされます。このフィールドは、デフォルトで有効になっています。このチェック ボックスをオンにすると、0/0 ルートがファブリック内で EVPN ルート タイプ 5 を介してリーフにアドバタイズされ、そこでリーフからボーダー デバイスに向かうデフォルト ルートが提供されます。

- **[スタティック 0/0 ルートの構成（Config Static 0/0 Route）]**：このフィールドは、エッジ/WAN ルータへのスタティック 0/0 ルートをボーダー デバイスの VRF で設定する必要があるかどうかを制御します。このフィールドは、デフォルトで有効になっています。WAN/エッジ ルータが、VRF Lite ピアリングを介してファブリック内のボーダー デバイスへのデフォルト ルートをアドバタイズしている場合、このフィールドを無効にする必要があります。

  さらに、**[デフォルト ルートのアドバタイズ（Advertise Default Route）]** フィールドを無効にする必要があります。外部ボーダー ゲートウェイ プロトコルを介してアドバタイズされる 0/0 ルートは、追加の構成を必要とせずに、EVPN を介してリーフに送信します。外部のファブリック外ピアリング提供のための eBGP を使用した、ファブリック内のクリーンな iBGP EVPN 分離が必要です。デフォルトでは、このチェック ボックスはオンになっています。

サンプル シナリオ

次のセクションでは、VRF Lite を設定するためのさまざまな使用例について説明します。

- 自動 VRF Lite（IFC）設定
- Cisco Nexus 9000 ベースのボーダーと Cisco Nexus 9000 ベースのエッジ ルータ間の VRF Lite
- Cisco Nexus 9000 ベースのボーダーとシスコ以外のデバイス間の VRF Lite
- Cisco Nexus 9000 ベースのボーダーと非 Nexus デバイス間の VRF Lite

  これは、管理モードでの Cisco ASR 9000 ベースのエッジ ルータの一般的な使用例です。

自動 VRF Lite（IFC）設定

ガイドライン

- 自動 IFC は、Cisco Nexus デバイスでのみサポートされています。
- Cisco ASR 1000 シリーズルータおよび Cisco Catalyst 9000 シリーズスイッチはエッジルータとして構成できます。

  構成するには、VRF Lite IFC をセットアップし、Easy ファブリックでボーダー デバイスとして接続します。
- Cisco ASR 9000 シリーズ ルータは管理対象モードのエッジ ルータとして設定できます。
- 外部ファブリックのデバイスが Nexus 以外の場合は、IFC を手動で作成する必要があります。

- エッジ ルータに接続するインターフェイスでユーザー ポリシーが有効になっていないことを確認します。ポリシーが存在する場合、インターフェイスは構成されません。
- 自動構成は、次の場合にサポートされています。
  - VXLAN ファブリックの**ボーダー** ロールと、接続された外部ファブリック デバイスの**エッジ ルータ** ロール
  - VXLAN ファブリックの**ボーダー ゲートウェイ** ロールと、接続された外部ファブリック デバイスの**エッジ ルータ** ロール
  - **ボーダー** ロールから直接別の**ボーダー** ロールへ

Note 自動構成は、2 つのボーダー ゲートウェイ（BGW）間では提供されません。

他のロール間で VRF Lite が必要な場合は、NDFC Web UI を使用して手動で展開する必要があります。

- 外部ファブリックに設定を展開するには、外部ファブリック設定にある **[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する必要があります。外部ファブリックが **[ファブリック モニタ モードのみ（Fabric Monitor Mode Only）]** に設定されている場合は、そのスイッチには構成を展開できません。

Easy ファブリック設定

VRF Lite を展開するモードは 4 つあります。デフォルトでは、VRF Lite 展開は手動に設定されています。以下のさまざまなモードで、要件に基づいて設定を変更できます。

- **[手動（Manual）]**：送信元デバイスと宛先デバイス間で VRF Lite IFC を手動で展開します。
- **[外部のみ（To External Only）]**：外部ファブリックの**エッジ ルータ** ロールを持つデバイスに接続されている VXLAN ファブリックの境界リーフデバイスの各物理インターフェイスで VRF Lite IFC を設定します。
- **[バックツーバックのみ（Back-to-Back Only）]**：異なる VXLAN ファブリックの直接接続された境界リーフ デバイス インターフェイス間に VRF Lite IFC を設定します。
- **[バックツーバックと外部（Back2Back&ToExternal）]**：このオプションを使用して、モード **[外部のみ（To External Only）]** および **[バックツーバックのみ（Back-to-Back Only）]** の IFC を構成します。

Note NDFC リソース処理の場合、VRF Lite モードは **[手動（Manual）]** に設定されますが、データ センター相互接続（DCI）サブネットが必要になります。

[手動（Manual）] モードは、ファブリック設定のデフォルト モードです。デフォルト モードを他のモードに変更するには、ファブリック設定の **[編集（Edit）]** をクリックします。**[リソース（Resource）]** タブで、VRF Lite 展開フィールドを上記の自動設定モードのいずれかに変更します。この例では、**[外部のみ（To External Only）]** チェック ボックスがオンになっています。

[自動展開両方（Auto Deploy Both）]：このチェックボックスは、対称 VRF Lite 展開に適用されます。このチェックボックスをオンにすると、自動作成された IFC の **[自動展開フラグ（Auto Deploy Flag）]** 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オンまたはオフにできます。選択した値が優先されます。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）]：VRF Lite IFC 展開の IP アドレスは、この範囲から選択されます。デフォルト値は 10.33.0.0/16 です。重複の可能性を避けるために、各ファブリックに独自の一意の範囲があり、アンダーレイ範囲とは区別されていることを確認してください。これらのアドレスは、リソース マネージャで予約されています。

[VRF Lite サブネット マスク（VRF Lite Subnet Mask）]：デフォルトでは、/30 に設定されています。これは、ポイント ツー ポイント（P2P）リンクのベスト プラクティスです。

Cisco Nexus 9000 ベースのボーダーと Cisco Nexus 9000 ベースのエッジ ルータ間の VRF Lite

DC-Vxlan VXLAN EVPN ファブリックは WAN-Vxlan クラウドに接続されています。次のトポロジでは、WAN-Vxlan が表示されています。

Easy ファブリックにはボーダー リーフのロールがあり、WAN-Vxlan クラウドにはエッジ ルータのロールを持つデバイスがあります。NDFC は、CDP/LLDP リンク ディスカバリを使用してトポロジの物理的および論理的な表現を示します。

この例では、DC-Vxlan ボーダー リーフと WAN-Vxlan エッジ ルータ間の VRF Lite 接続を有効にできます。

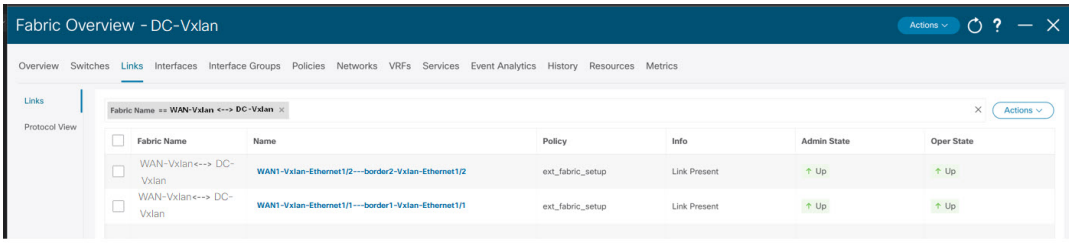
VRF Lite 構成では、ポイントツーポイント（P2P）接続を介して、ファブリックのボーダー インターフェイスとエッジ ルータのインターフェイスの間で外部ボーダー ゲートウェイ プロトコル（EBGP）ピアリングを有効にする必要があります。

ボーダーの物理インターフェイスは次のとおりです。

- **eth1/1**（**border1-Vxlan** 上）、**eth1/1**（**WAN1-Vxlan** 上）に向かうもの。
- **eth1/2**（**border2-Vxlan** 上）、**eth1/2**（**WAN1-Vxlan** 上）に向かう。

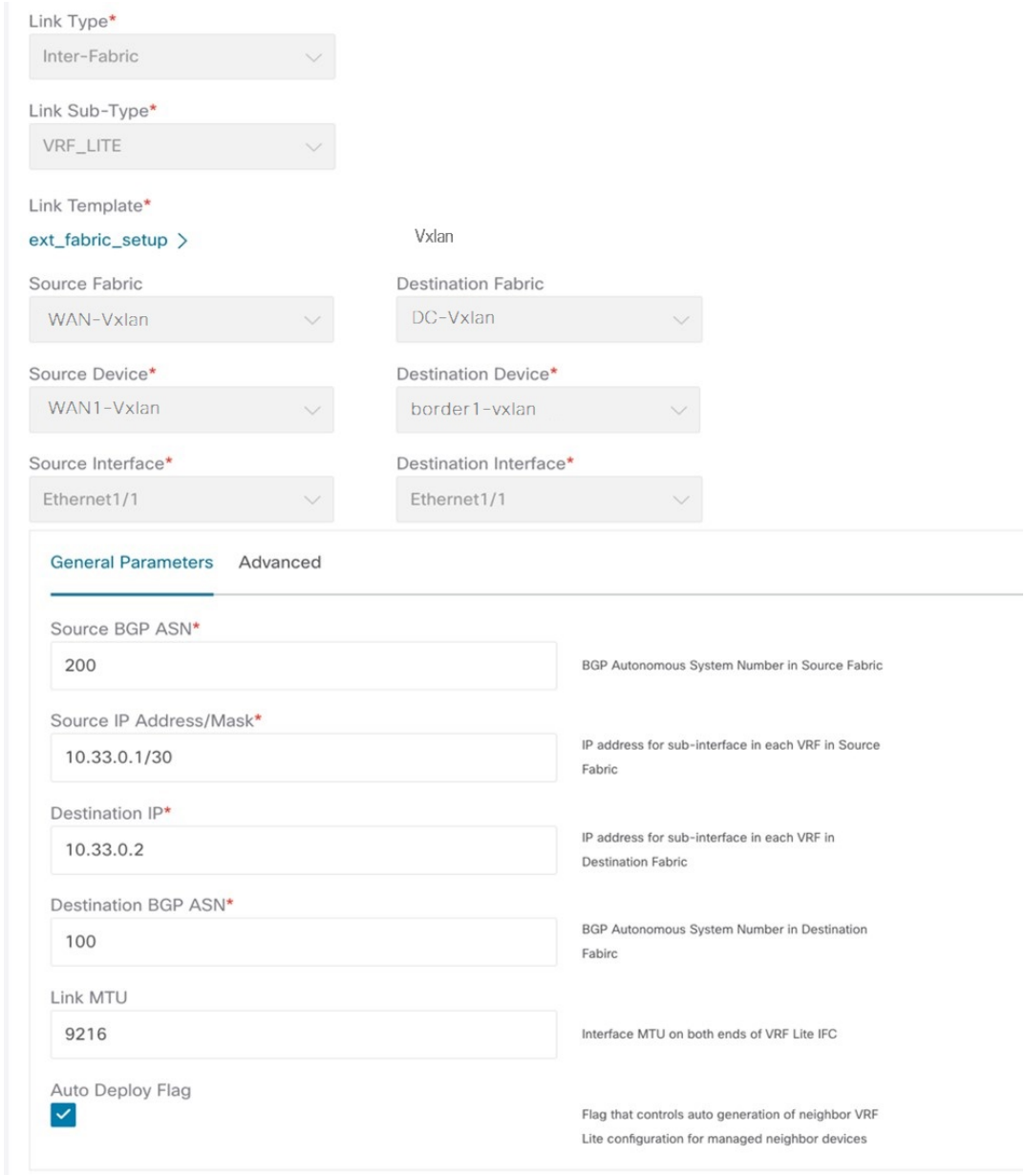
1. ボーダーとエッジ ルータ間のリンクを確認します。**[LAN]** > **[ファブリック（Fabrics）]**に移動し、**[DC-Vxlan]** ファブリックをダブルクリックします。

   [ファブリックの概要（Fabric Overview）] ウィンドウで、**[リンク（Links）]** タブをクリックします。NDFC によって検出されたリンクが表示され、**ext_fabric_setup** ポリシーが自動的に割り当てられます。



2. VRF Lite 設定を確認するには、ファブリック名を選択し、**[アクション（Actions）]** > **[編集（Edit）]**を選択します。

   適切な **[リンク（Links）]** をクリックし、**[アクション（Actions）]** > **[編集（Edit）]**を選択します。



[リンク タイプ（Link Type）]：NDFC 内の 2 つの異なるファブリック間のファブリック間リンクを指定します。

[リンク サブタイプ（Link Sub-Type）]：リンクのサブタイプを指定します。デフォルトでは、**VRF_LITE** オプションが表示されます。

[リンク テンプレート（Link Template）]：リンクのテンプレートを指定します。VRF Lite IFC のデフォルト テンプレートとして、**ext_fabric_setup** が表示されます。テンプレートは、送信元インターフェイスと宛先インターフェイスをレイヤ 3 インターフェイスとして有効にし、**no shutdown** コマンドを計算して、それらの MTU を 9216 に設定します。

送信元と宛先のファブリック、デバイス、およびインターフェイスは、CDP/LLDP ディスカバリに基づき、NDFC によって自動検出され、選択されます。

[一般パラメータ（General Parameters）] タブの、このタブのフィールドは次のとおりです。

[送信元 BGP ASN（Source BGP ASN）]：選択した送信元ファブリックの BGP ASN。

[送信元 IP アドレス/マスク（Source IP Address/Mask）]：IFC の送信元インターフェイスである **Ethernet1/1** サブインターフェイスの VRF Lite サブネット プールのリソース マネージャ プールから、NDFC により自動的に割り当てられた IP プール。この IFC を介して拡張される各 VRF に対してサブインターフェイスが作成され、一意の 802.1Q ID が割り当てられます。ここで入力された IP アドレス/マスクは、BGP ネイバー IP フィールド （以下で説明）とともに、VRF 拡張で作成され、上書きできるサブインターフェイスのデフォルト値として使用されます。

たとえば、802.1Q ID の 2 は VRF CORP トラフィックのサブインターフェイス Eth 1/1.2 に関連付けられ、802.1Q ID の 3 は Eth 1/1.3 および VRF ENG に関連付けられます。

IP プレフィックスは、NDFC リソース マネージャで予約されます。トポロジで作成する IFC ごとに一意の IP アドレス プレフィックスを使用するようにしてください。

[宛先 IP（Destination IP）]：VRF Lite サブネット プールのリソース マネージャ プールから NDFC により自動的に割り当てられた IP プールです。これは、デバイスの BGP ネイバー IP です。

IFC の異なる VRF からのファブリック間トラフィックの例としては、同じ送信元 IP アドレス（10.33.0.1/30）と宛先 IP アドレス（10.33.0.2）のものがあります。

[宛先 BGP ASN（Destination BGP ASN）]：選択した宛先ファブリックの BGP ASN です。

リンク MTU（Link MTU）：デフォルトは 9216 です。

[自動展開フラグ（Auto Deploy Flag）]：ファブリック設定に基づいて選択されたデフォルトの自動設定です。このノブは、ネイバー管理対象デバイスのネイバー VRF を自動設定します。たとえば、WAN-Vxlan 外部ファブリック内のエッジ ルータに VRF を自動的に作成します。

[詳細設定（Advanced）] タブが **[リンク プロファイル（Link Profile）]** セクションに追加されます。このタブのフィールドは次のとおりです。

- **[送信元インターフェイスの説明（Source Interface Description）]**
- **[宛先インターフェイスの説明（Destination Interface Description）]**
- **[送信元インターフェイスのフリーフォーム構成（Source Interface Freeform Config）]**
- **[宛先インターフェイスのフリーフォーム構成（Destination Interface Freeform Config）]**

[保存（Save）] をクリックして、設定を保存します。

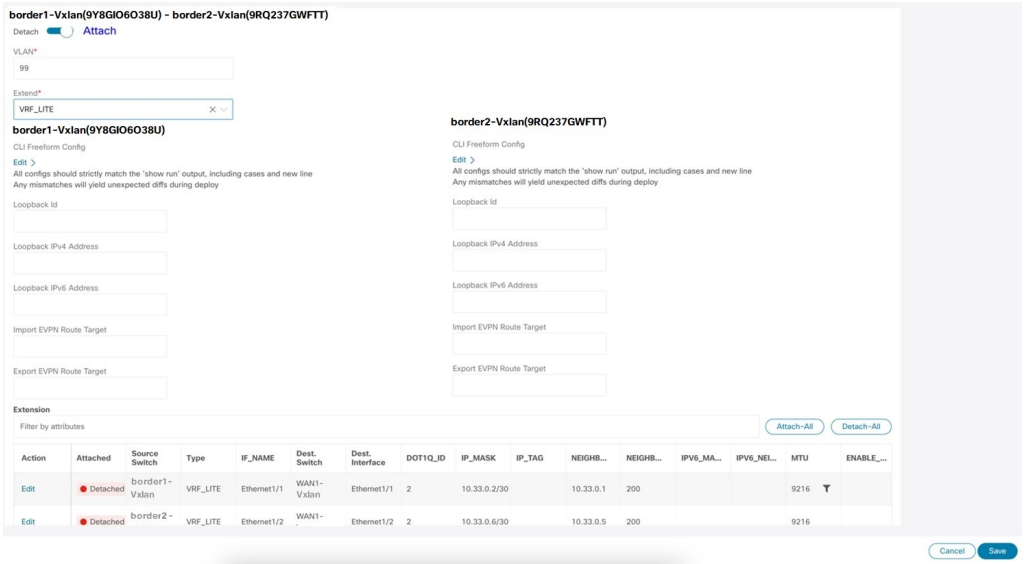
3. ボーダー デバイスで VRF および VRF Lite 拡張をアタッチするには、次の手順を実行します。

a. **[VRF（VRFs）]** > **[VRF アタッチメント（VRF Attachments）]** タブをクリックします。

b. **[VRF 名（VRF Name）]** を選択し、**[アクション（Actions）]** > **[編集（Edit）]**をクリックします。

   [編集（Edit）] ウィンドウが表示されます。

c. 以下に示すように、**[拡張（Extension）]** フィールドの詳細を編集できます。



- ノブを **[アタッチ（Attach）]** に切り替えます。
- **[拡張（Extend）]** で、ドロップダウン リストから **[VRF_LITE]** を選択します。
- **[拡張（Extension）]** カードで、一度に 1 つのスイッチを選択し、**[編集（Edit）]** をクリックして、**PEER_VRF_NAME** の詳細を入力します。これにより、ネイバー デバイスに VRF が自動展開されます。

VRF Lite 連続シナリオを拡張する場合、VRF はピア ファブリック内にあり、VRF 名は同じである必要があります。VRF がピア ファブリック内にない場合に、VRF Lite を拡張しようとすると、問題を示すエラー メッセージが生成されます。

Easy ファブリックと外部ファブリックの間で VRF Lite を拡張する場合、VRF 名は、送信元ファブリックの名前と同じにすることも、デフォルト名、または別の VRF 名と同じにすることもできます。**PEER_VRF_NAME** フィールドに必要な VRF 名を入力します。サブインターフェイスの子 PTI、外部ファブリックで作成される VRF および BGP ピアリングには、そこに入力される送信元の値があるため、ポリシーを編集または削除することはできません。

他のリンクについては、上記の手順に従ってください。

[編集（Edit）] ウィンドウで、**[すべてアタッチ（Attach-all）]** をクリックして、ボーダー デバイスに必要な VRF 拡張をアタッチし、**[保存（Save）]** をクリックします。

4. VXLAN EVPN Easy ファブリックで構成を再計算して展開するには、次の手順を実行します。

   [ファブリック（Fabric）] ウィンドウで、適切な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）]** ウィンドウに移動します。**[アクション（Actions）]** > **[再計算と展開（Recalculate & Deploy）]**をクリックします。

   同様に、操作を実行し、必要な **[VRF 名（VRF Name）]** を **[VRF アタッチメント（VRF attachments）]** タブで選択し、**[アクション（Actions）]** > **[展開（Deploy）]** をクリックして、ボーダー デバイスで VRF および VRF Lite の構成を開始することもできます。

5. VXLAN EVPN Easy ファブリックを再計算して展開するには：

   [ファブリック（Fabric）] 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。

   同様に、VRF アタッチメントを選択して編集し、**[展開（Deploy）]** をクリックできます。VRF および VRF Lite 構成をボーダー デバイスにプッシュします。

6. 外部ファブリックで構成を再計算して展開するには、外部ファブリックを選択し、上記の手順に従います。

Cisco Nexus 9000 ベースのボーダーと Cisco 以外のデバイス間の VRF Lite

この例では、DC-Vxlan ボーダー リーフと外部ファブリック内のシスコ以外のデバイスとの間で VRF Lite 接続を有効にする手順を示しています。

Cisco は、外部ファブリックにデバイスをインポートする代わりに、デバイスのメタ定義を使用することを推奨しています。これにより、Easy ファブリック内の Cisco Nexus 9000 管理ボーダーデバイスを VRF Lite 構成により拡張できます。NDFC は宛先の Cisco 以外のデバイスを管理しません。宛先デバイス上で関連する VRF Lite 設定を設定する必要があります。

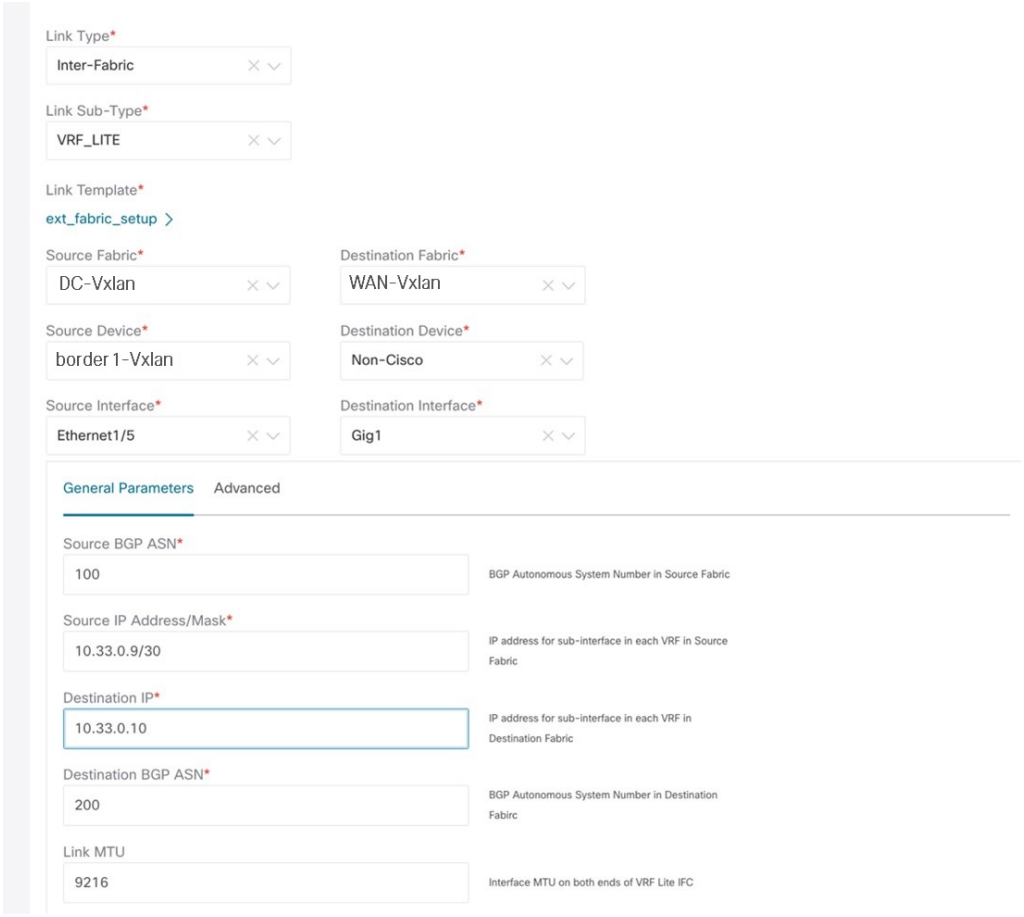
1. ボーダー ルータとエッジ ルータの間に新しい IFC リンクを作成します。

   a. **[ファブリック（Fabrics）]** ウィンドウで、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。

   b. **[リンク（Links）]** タブに移動します。**[リンク（Links）]** タブで、**[アクション（Actions）]** > **[新しいリンクの作成（Create New link）]**をクリックします。

      [新しいリンクの作成（Create New link）] ウィンドウが表示されます。



c. ウィンドウに次の必須パラメータを入力します。

- **[リンク タイプ（Link Type）]**：ファブリック間リンクを選択します。これは、NDFC 内の 2 つの異なるファブリック間の IFC です。
- **[リンク サブタイプ（Link Sub-Type）]**：デフォルトでは、**VRF_LITE** オプションが表示されます。
- [**リンク テンプレート（Link Template）]**：VRF Lite IFC のデフォルト テンプレートである **ext_fabric_setup** が表示されます。このテンプレートは、送信元インターフェイスと宛先インターフェイスをレイヤ 3 インターフェイスとして有効にし、**no shutdown** コマンドを設定して、それらの MTU を 9216 に設定します。
- **[送信元ファブリック（Source Fabric）]**：送信元ファブリックを選択します。これは、Cisco Nexus 9000 ベースのボーダー デバイスが存在する Easy ファブリックです。
- **[宛先ファブリック（Destination Fabric）]**：任意の外部またはクラシック LAN ファブリックを選択します。モニター モードにもなります。
- **[送信元デバイス（Source Device）]**：送信元デバイスを選択します。これは Cisco Nexus 9000 ベースのボーダー デバイスです。

- **[宛先デバイス（Destination Device）]**：これで、「メタデバイス定義」を作成できます。任意の名前を入力して、[作成（Create）] をクリックします。たとえば、「non-cisco」です。
- **[送信元インターフェイス（Source Interface）]**：Cisco 以外のデバイスが接続されているボーダー デバイス上のインターフェイスを選択します。
- **[宛先インターフェイス（Destination Interface）]**：これで、「メタデバイス インターフェイス」を作成できます。任意のインターフェイス名を入力して、[作成（Create）] をクリックします。たとえば、「gig1」、「tengig1/10」、「eth1/1」は有効なインターフェイス名です。

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

- **[送信元 BGP ASN（Source BGP ASN）]**：選択した送信元ファブリックの BGP ASN。
- **[送信元 IP アドレス/マスク（Source IP Address/Mask）]**：IFC の送信元インターフェイスである **Ethernet1/5** サブインターフェイスの IP アドレスとマスクを提供します。この IFC を介して拡張される VRF ごとにサブインターフェイスが作成され、一意の 802.1Q ID が割り当てられます。ここで入力された IP アドレス/マスク、および VRF 拡張で作成される BGP ネイバーの IP フィールド（以下で説明）は、サブインターフェイスのデフォルト値として使用されるもので、上書きできます。

  たとえば、802.1Q ID 2 は VRF CORP トラフィックのサブインターフェイス Eth 1/5.2 に関連付けられ、802.1Q ID 3 は Eth 1/5.3 および VRF ENG に関連付けられます。以下も同様です。

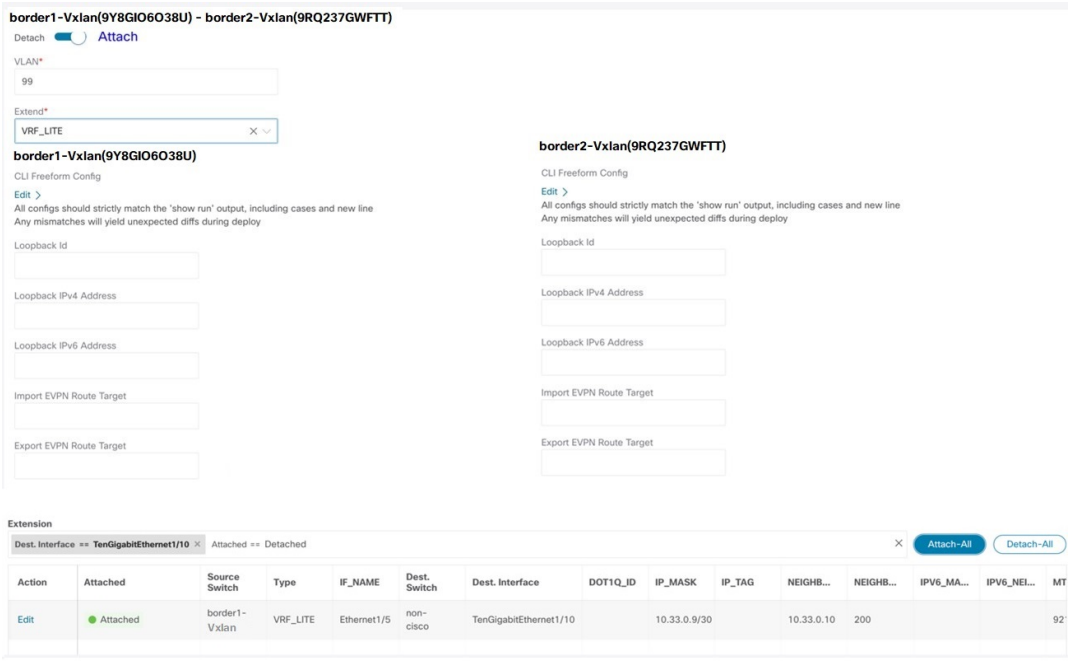
  IP プレフィックスは、NDFC リソース マネージャーで予約されます。トポロジで作成する IFC ごとに一意の IP アドレス プレフィックスを使用するようにしてください。
- **[宛先 IP（Destination IP）]**：VRF Lite サブネット プールのリソース マネージャー プールから NDFC により自動的に割り当てられた IP プールです。これは、デバイス上の BGP ネイバー IP です。

  例として、同じ送信元 IP アドレス（10.33.0.1/30）と宛先 IP アドレス（10.33.0.2）を持つ IFC の異なる VRF からのファブリック間トラフィックがあります。
- **[宛先 BGP ASN（Destination BGP ASN）]**：選択した宛先ファブリックの BGP ASN です。
- **リンク MTU（Link MTU）**：デフォルトは 9216 です。
- **[自動展開フラグ（Auto Deploy Flag）]**：宛先デバイスが Nexus 以外、Cisco 以外であるため、適用されません。

[詳細設定（Advanced）] タブには、適切な詳細を入力します。タブには以下のフィールドがあります。

- **[送信元インターフェイスの説明（Source Interface Description）]**
- **[宛先インターフェイスの説明（Destination Interface Description）]**
- **[送信元インターフェイスのフリーフォーム構成（Source Interface Freeform Config）]**
- **[宛先インターフェイスのフリーフォーム構成（Destination Interface Freeform Config）]**

2. **[保存（Save）]** をクリックして、記載されているパラメータを使用して新しいリンクを作成します。
3. ボーダー デバイスに VRF および VRF Lite 拡張をアタッチするには、**[DC-Vxlan]** 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）]** ウィンドウで、**[VRF]** > **[VRF アタッチメント（VRF Attachments）]**に移動し、次の図に示すように詳細を編集します。



[すべてアタッチ（Attach-all）] をクリックして、ボーダー デバイスに必要な VRF 拡張をアタッチし、**[保存（Save）]** をクリックします。

4. VXLAN EVPN Easy ファブリックで構成を再計算して展開するには、**[ファブリック（Fabric）]** ウィンドウで適切なファブリックをクリックします。

[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）]**をクリックするか、**[VRF]**>**[VRF アタッチメント（VRF attachments）]** に移動し、VRF アタッチメントを選択して編集し、**[展開（Deploy）]** をク

リックします。これにより、ボーダー デバイスで VRF および VRF Lite 構成が開始されます。

Cisco Nexus 9000 ベースのボーダーと非 Nexus デバイス間の VRF Lite

この例では、DC-Vxlan ボーダー リーフと外部ファブリック内の非 Nexus デバイス間の VRF Lite 接続を有効にできます。

Cisco NDFC リリース 12.0.1a より前は、ASR 9000 はモニター モードの外部ファブリックに対してのみサポートされていました。リリース 12.0.1a から、ASR 9000 は、エッジ ルータのロールを持つ管理モードでサポートされます。

サポートされているプラットフォームは次のとおりです。

- ASR 9000
- NCS 5500
- ASR 8000

外部ファブリックの IOS-XR スイッチでは、外部ファブリックで構成された Cisco Nexus スイッチと同様に、構成コンプライアンスが有効になります。NDFC は展開の最後に構成をプッシュします。

（注） VXLAN BGP EVPN ボーダー デバイスがアクティブであることを確認します。

手順

ステップ 1 **[LAN]** > **[ファブリック（Fabrics）]**に移動して、外部ファブリックを作成します。3

ステップ 2 **[ファブリックの作成（Create Fabric）]** ウィンドウで、適切な ASN 番号を入力し、**[モニター モード（Monitor Mode）]** をオフにし、**[保存（Save）]** をクリックします。

ステップ 3 [スイッチ] ウィンドウに移動し、[アクション]、[スイッチの追加] の順にクリックします。 >

（注） ディスカバリ用の SNMP 設定を使用して、IOS-XR デバイスに NDFC への IP アドレス到達可能性があることを確認します。

外部ファブリックに 非 Nexus デバイスを追加する方法については、非 Nexus デバイスを外部ファブリックに追加する （142 ページ） を参照してください。

ステップ 4 **[スイッチの追加（Add Switches）]** ウィンドウで、**[検出（Discover）]** チェックボックスをオンにし、**[IOS-XR]** を **[デバイス タイプ（Device Type）]** フィールドのドロップダウン リストから選択します。

ステップ 5 ルータが検出されると、**[検出結果（Discovery Results）]** フィールドにスイッチ名が表示されます。

ステップ 6 検出されたルータを選択し、ファブリックに追加します。ステータス列で **[検出ステータス（Discovery Status ）]** が **[OK]** と表示されていることを確認します。エッジ ルータのロールがサポートされます。

検出が成功すると、**[リンク（Links）]** タブでデバイス間のリンクを表示できます。

ステップ 7 Cisco Nexus 9000 ボーダー リーフを使用して外部ファブリックの VRF Lite IFC を作成するには、リンクを選択し、**[アクション（Actions）]** > **[編集（Edit）]**をクリックします。

ステップ 8 **[リンクの編集（Edit Link）]** ウィンドウで、IFC 作成に必要な詳細を入力します。一部のフィールドのみ自動入力されます。

（注） 非 NX-OS デバイスの自動化の場合、展開フラグは適用されません。

ステップ 9 VXLAN ボーダー デバイスで VRF Lite 設定を拡張するには、**[VRF]** > **[VRF アタッチメント（VRF Attachment）]**タブに移動し、VRF 名を選択し、**[アクション（Actions）]**>**[編集（Edit）]** をクリックして、VRF Lite として拡張します。

ステップ 10 VXLAN ボーダー デバイスに構成を展開します。

ステップ 11 [ファブリック（Fabrics）] ウィンドウに移動し、外部ファブリックにルータがあることを確認し、**[VRF Lite BGP ポリシーに適用（Apply to VRF Lite BGP policies）]** をクリックします。

ステップ 12 **[ポリシー（Policies）]** タブに移動し、ポリシー **ios_xr_base_bgp** を追加し、必要な詳細を入力して **[保存（Save）]** をクリックします。

ステップ 13 別のポリシー **ios_xr_Ext_VRF_Lite_Jython** を追加し、必要な詳細を入力して **[保存（Save）]** をクリックします。

ステップ 14 IOS-XR ルータに構成を展開します。

付録

Nexus 9000 ボーダー デバイスの構成

テンプレート ext_base_border_vrflite_11_1 によって生成された Border-Vxlan（ベース ボーダー構成）

```
switch configure terminal
switch(config)#
ip prefix-list default-route seq 5 permit 0.0.0.0/0 le 1
ip prefix-list host-route seq 5 permit 0.0.0.0/0 eq 32
route-map extcon-rmap-filter deny 10
    match ip address prefix-list default-route
route-map extcon-rmap-filter deny 20
    match ip address prefix-list host-route
route-map extcon-rmap-filter permit 1000
route-map extcon-rmap-filter-allow-host deny 10
    match ip address prefix-list default-route
route-map extcon-rmap-filter-allow-host permit 1000
```

```
ipv6 prefix-list default-route-v6 seq 5 permit 0::/0
ipv6 prefix-list host-route-v6 seq 5 permit 0::/0 eq 128
route-map extcon-rmap-filter-v6 deny 10
    match ipv6 address prefix-list default-route-v6
route-map extcon-rmap-filter-v6 deny 20
    match ip address prefix-list host-route-v6
route-map extcon-rmap-filter-v6 permit 1000
route-map extcon-rmap-filter-v6-allow-host deny 10
    match ipv6 address prefix-list default-route-v6
route-map extcon-rmap-filter-v6-allow-host permit 1000
```

Border-Vxlan VRF Lite 拡張構成

```
switch configure terminal
vrf context CORP
  ip route 0.0.0.0/0 2.2.2.2
exit
router bgp 100
  vrf CORP
    address-family ipv4 unicast
      network 0.0.0.0/0
      exit
    neighbor 2.2.2.2
      remote-as 200
      address-family ipv4 unicast
        send-community both
        route-map extcon-rmap-filter out
configure terminal
interface ethernet1/1.2
  encapsulation dot1q 2
  mtu 9216
  vrf member CORP
  ip address 2.2.2.22/24
  no shutdown
configure terminal
```

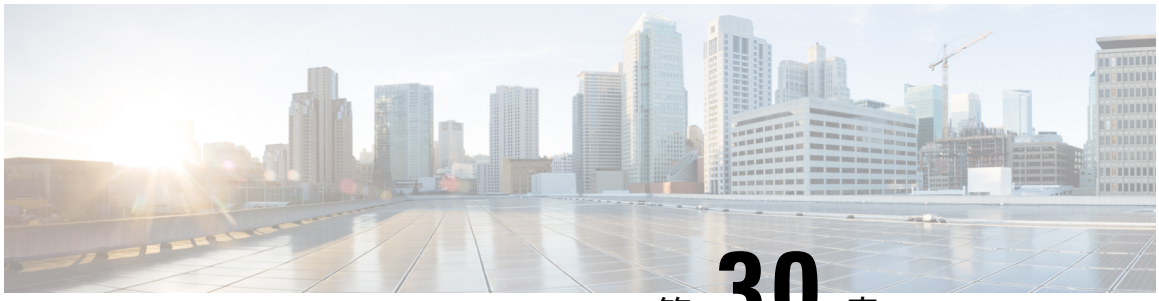
WAN-Vxlan（外部ファブリック エッジ ルーター）VRF Lite 拡張構成

```
switch configure terminal
vrf context CORP
  address-family ipv4 unicast
exit
router bgp 200
  vrf CORP
    address-family ipv4 unicast
    neighbor 10.33.0.2
      remote-as 100
      address-family ipv4 unicast
        send-community both
        exit
      exit
    neighbor 10.33.0.6
      remote-as 100
      address-family ipv4 unicast
        send-community both
configure terminal
interface ethernet1/1.2
  mtu 9216
  vrf member CORP
  encapsulation dot1q 2
  ip address 10.33.0.1/30
```

```
  no shutdown
interface ethernet1/2.2
  vrf member CORP
  mtu 9216
  encapsulation dot1q 2
  ip address 10.33.0.5/30
  no shutdown
configure terminal
```

第 VIII 部

MSDC 展開の Easy プロビジョニング



第 30 章

eBGP ルーテッド ファブリックの管理

BGP ベースのルーテッド ファブリックの管理

この章では、選択したルーティング プロトコルとして eBGP を使用して、典型的なスパイン リーフ ベースのルーテッド ファブリックを構成する方法について説明します。これは、大規模なスケーラブル データ センター（MSDC）ネットワークに推奨される展開の選択肢です。Same-Tier-AS オプションと Multi-AS オプションの両方がサポートされています。ルーテッド ファブリックには、リーフ間のレイヤ 2 ストレッチまたはサブネット ストレッチはありません。つまり、ネットワークはリーフのペアまたはラックに配置され、リーフは直接接続されたサーバー ワークロードのデフォルト ゲートウェイをホストします。ラック全体のサブネット アドバタイズメントは、スパインを介して eBGP 経由で通信されるため、ルーテッド ファブリック内での Any-to-Any の到達可能性が実現されます。ルーテッド ファブリックは、IPv4 または IPv6 ベースにすることができます。IPv6 ルーテッド ファブリックは IPv6 を使用して、ファブリック内接続とルート アドバタイズメントを構築します。IPv6 ルーテッド ファブリックは、ファブリック内リンクにリンク ローカル アドレスを割り当て、RFC 5549 をサポートして、IPv6 ネクスト ホップを使用した IPv4 ルート アドバタイジングを可能にします。スイッチ ロール リーフ、スパイン、ボーダー、スーパー スパイン、およびボーダー スーパー スパインがサポートされています。

eBGP ベースのファブリックの作成

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

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

   フィールドについて説明します。

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

[ファブリックのテンプレート（Fabric Template）]：**Easy_Fabric_eBGP** ファブリック テンプレートを選択するには、これをクリックします。スタンドアロン ファブリックを作成するためのファブリック設定が表示されます。[選択（Select）] をクリックします。

3. 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。

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

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

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

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

   Same-Tier-AS ファブリックでは、スパイン スイッチには一意の BGP AS 番号があり、リーフ スイッチには一意の AS 番号があり、ボーダーは 1 つの AS を共有します。同じ役割を持つリーフ スイッチまたはボーダー スイッチは、異なる AS を持つことはできません。

   リーフとボーダーは、同じ AS を持つことも、異なる AS を持つこともできます。

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

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

5. **[EVPN]** をクリックします。[EVPN VXLAN オーバーレイを有効にする（Enable EVPN VXLAN Overlay）] オプションを明示的に無効にする必要があります。このチェックボックスはデフォルトで有効になっていることに注意してください。このオプションは、顧客が eBGP アンダーレイ/オーバーレイ ベースの VXLAN EVPN ファブリックを構築することを望むユースケースでのみ有効にします。

   [ルーテッド ファブリック（Routed Fabric）]：ルーテッド ファブリックでは、スパイン リーフ ネットワーク間の IP 到達可能性が確立されると、選択したファースト ホップ ルーティング プロトコル （FHRP）として HSRP または VRRP を使用し、リーフ上にネットワークを簡単に作成して展開することができます。

   eBGP ルーテッド ファブリックを作成すると、ファブリックは eBGP をコントロール プレーンとして使用して、ファブリック内接続を構築します。スパイン スイッチとリーフ スイッチ間のリンクは、eBGP ピアリングがその上に構築される、ポイント ツー ポイント（p2p）番号付き IP アドレスで自動構成されます。

   Routed_Network_Universal テンプレートは、ルーテッド ファブリックにのみ適用されることに注意してください。

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

Note

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

6. **[vPC]** をクリックします。このタブのフィールドは次のとおりです。

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

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

   [vPC ピア キープアライブ オプション（vPC Peer Keep Alive option）]：管理またはループバック オプションを選択します。管理ポートおよび管理 VRF に割り当てられた IP アドレスを使用する場合は、[管理（management）] を選択します。ループバック インターフェイス（および非管理 VRF）に割り当てられた IP アドレスを使用する場合は、ループバックを選択します。IPv6 アドレスを使用する場合は、ループバック ID を使用する必要があります。

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

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

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

   [vPC IPv6 ND 同期（vPC IPv6 ND Synchronize）]：vPC スイッチ間の IPv6 ネイバー探索同期を有効にします。チェック ボックスはデフォルトでオンになっています。この機能を無効にするには、チェック ボックスをオフにします。

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

   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 ペアで同じ 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 ペアで同じ vPC ドメイン ID を有効にする（Enable the same vPC Domain Id for all vPC Pairs）]** チェックボックスをオンにします。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）]**をクリックします。このタブのフィールドは次のとおりです。

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

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

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

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

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

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

[BFD の有効化（Enable BFD）]：**[BFD の有効化（Enable BFD）]**チェックボックスは、ファブリック内のすべてのスイッチで**機能 bfd** を有効にする場合にオンにします。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。

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

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

```
feature bfd
```

Note BFD が有効になっている NDFC では、次の構成がすべての P2P ファブリック インターフェイスにプッシュされます。

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

BFD機能の互換性については、それぞれのプラットフォームのマニュアルを参照してください。サポートされているソフトウェアイメージについては、*Compatibility Matrix for Cisco*を参照してください。

[BGP 向け BFD を有効にする（Enable BFD for BGP）]：**[BGP 向け BFD を有効にする（Enable BFD for BGP）]** チェックボックスをオンにして、BGP ネイバーの BFD を有効にします。このオプションは、デフォルトで無効です。

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

[BFD 認証キー ID（BFD Authentication Key ID）]：インターフェイス認証の BFD 認証キー ID を指定します。

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

BFD認証パラメータを取得する方法については、『*Cisco NDFC* ファブリック コントローラ構成ガイド』の「暗号化された *BFD* 認証キーの取得」を参照してください。

8. [詳細設定（Advanced）] 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。

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

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

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

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

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

[ブートストラップスイッチの CDP を有効にする（Enable CDP for Bootstrapped Switch）]：**[ブートストラップスイッチの CDP を有効にする（Enable CDP for Bootstrapped Switch）]** チェックボックスをオンにして、ブートストラップスイッチの CDP を有効にします。

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

[HTTP での NX-API の有効化（Enable NX-API on HTTP）]：HTTP での NX-API の有効化を指定します。HTTP を使用するには、**[HTTP での NX-API の有効化（Enable NX-API on HTTP）]** チェックボックスと **[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 を使用するようになります。

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

[厳密な構成コンプライアンスの有効化（Enable Strict Config Compliance）]：**[厳密な構成コンプライアンスの有効化（Enable Strict Config Compliance）]** チェックボックスをオンにして、この機能を有効にします。

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

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

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

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

[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。

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

[デフォルト キューイング ポリシーの有効化（Enable Default Queuing Policies）]：**[デフォルト キューイング ポリシーの有効化（Enable Default Queuing Policies）]** チェックボックスをオンにして、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 NDFC Web UI から、**[操作（Operations）]** > **[テンプレート（Templates）]**の順に選択します。ポリシー ファイル名でキューイング ポリシーを検索します（例：[queuing_policy_default_8q_cloudscale]）。ファイルを選択し、**[テンプレートの変更/表示（Modify/View template）]** アイコンをクリックしてポリシーを編集します。

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

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

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

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

[MACsec の有効化（Enable MACsec）]：ファブリックの MACsec を有効にします。詳細については、Easy ファブリックおよび eBGP ファブリックでの MACsec サポート, on page 113を参照してください。

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

[スパインの自由形式の構成（Spine Freeform Config）]：スパイン、ボーダー スパイン、ボーダー ゲートウェイ スパイン、およびスーパー スパインのロールを持つスイッチに追加する CLI です。

[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 です。

9. **[管理性（Manageability）]** をクリックします。このタブのフィールドは次のとおりです。

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

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

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

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

   [Syslog サーバー 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 サーバーのシビラティ（重大度）（Syslog Server Severity）]：syslog サーバーごとに、1 つの syslog シビラティ（重大度）値のカンマ区切りリストを指定します。最小値は 0 で、最大値は 7 です。高い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 自由形式の構成（AAA Freeform Config）]：AAA 自由形式の構成を指定します。

   ファブリック設定で AAA 構成が指定されている場合は、**switch_freeform** PTI で、ソースが **UNDERLAY_AAA**、説明が **AAA Configurations** であるものが作成されます。

10. **[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。

    [ブートストラップを有効にする（Enable Bootstrap）]：**[ブートストラップを有効にする（Enable Bootstrap）]** チェックボックスをオンにして、ブートストラップ機能を有効にします。

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

    - 外部 DHCP サーバ（External DHCP Server）：[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）] および [スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）] フィールドに外部 DHCP サーバに関する情報を入力します。

- ローカル DHCPサーバー（Local DHCP Server）：**[ローカル DHCP サーバー（Local DHCP Server）]**チェックボックスをオンにして、残りの必須フィールドに詳細を入力します。

[ローカル DHCP サーバーを有効にする（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、**[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。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、NDFC は自動 IP アドレス割り当てにリモートまたは外部の DHCP サーバーを使用します。

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

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

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

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

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

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

[AAA 構成を有効にする（Enable AAA Config）]：**[AAA 構成を有効にする（Enable AAA Config）]**チェックボックスをオンにして、デバイスの起動時に**[管理性（Manageability）]**タブからの AAA 構成が含められるようにします。

[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、AAA またはリモート認証関連の構成を使用している場合は、このフィールドにこれらの構成を追加してインテントを保存する必要があります。デバイスが起動すると、[Bootstrap Freeform Config]フィールドで定義されたインテントが含まれます。

NX-OSスイッチの実行コンフィギュレーションに示されているように、running-configを正しいインデントで自由形式の設定フィールドにコピーアンドペーストします。freeform config は running config と一致する必要があります。詳細については、スイッチでのフリーフォーム構成エラーの解決を参照してください。ファブリック スイッチでのフリーフォーム構成の有効化に記されています。

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

スコープの形式は次の順で定義する必要があります。

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

例：10.6.0.2、10.6.0.9、16.0.0.1、24

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

    [毎時ファブリック バックアップ（Hourly Fabric Backup）]：**[毎時ファブリック バックアップ（Hourly Fabric Backup）]**チェックボックスをオンにして、ファブリック構成とインテントの 1 時間ごとの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った場合、NDFC はバックアップを取ります。

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

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

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

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

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

Note 1 時間ごと、およびスケジュールされたバックアップ プロセスは、次の定期的な構成コンプライアンス アクティビティ中にのみ発生し、最大 1 時間の遅延が発生する可能性があります。即時バックアップをトリガーするには、次の手順を実行します。

a. **[LAN]** > **[トポロジ（Topology）]**を選択します。

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

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

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

関連情報を入力して更新したら、**[保存（Save）]** をクリックします。

12. **[フロー モニタ（Flow Monitor）]** 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）]：**[Netflow を有効にする（Enable Netflow）]** 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。

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

netflow がファブリック レベルで有効になっていない場合、インターフェイス、ネットワーク、または vrf レベルで netflow を有効にすると、エラー メッセージが生成されます。Cisco NDFC の Netflow サポートについては、Netflow サポート, on page 175 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。このタブ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）]** をクリックして、1 つ以上の Netflow レコードを追加します。この画面のフィールドは次のとおりです。

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

13. [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。

特筆すべき点

- ブラウンフィールド移行は、eBGP ファブリックではサポートされていません。
- リーフスイッチの AS 番号は、作成後に**再計算と展開（Recalculate & Deploy）**操作を実行した後は変更できません。変更が必要になった場合は、**leaf_bgp_asn** ポリシーを削除し、**再計算と展開（Recalculate & Deploy）**操作を実行して、この AS に関連する BGP 構成を削除する必要があります。次に、新しい AS 番号を使用して、leaf_bgp_asn ポリシーを追加できます。
- Multi-AS モードと Same-Tier-AS モードを切り替える場合は、モードを変更する前に、手動で追加されたすべての BGP ポリシー（リーフ スイッチの Leaf_bgp_asn および ebgp オーバーレイ ポリシーを含む）を削除し、**再計算と展開（Recalculate & Deploy）**操作を実行します。
- サポートされているロールは、リーフ、スパイン、スーパー スパイン、ボーダー リーフ、およびボーダー スーパー スパインです。
- ボーダーおよびスーパー スパイン ボーダー デバイスでは、VRF-Lite が手動モードでサポートされます

ファブリックへのスイッチの追加

各ファブリックのスイッチは一意であるため、各スイッチは 1 つのファブリックにのみ追加できます。ファブリックへのスイッチの追加, on page 334 を参照してください。

ファブリック アンダーレイ eBGP ポリシーの展開

NDFC では、**Easy_Fabric_eBGP** テンプレートを持つファブリックが作成されます。1 つのスパイン スイッチと 3 つのリーフ スイッチがインポートされます。

ファブリックには次の 2 種類があります。

- **マルチ AS モード ファブリックの作成**：マルチ AS モード ファブリックでは、スパイン スイッチには共通の BGP AS 番号があり、各リーフ スイッチには一意の BGP AS 番号があ

ります。Same-Tier-AS から Multi-AS モードへのファブリック変換にも同じ手順を使用します。

- **Same-Tier-AS モード ファブリックの作成**：Same-Tier-AS モード ファブリックの作成については、別の手順が説明されています。Multi-AS から Same-Tier-AS モードへのファブリック変換にも同じ手順を使用します。

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

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

必要なスイッチにポリシーを追加するには、ポリシーの追加 （377 ページ）およびポリシーの表示と編集 （375 ページ）を参照してください。

eBGP ベースのファブリックでのネットワークの展開

ルーテッド ファブリックのネットワークの概要

NDFC を使用して、ルーテッド ファブリックのトップダウン ネットワーク構成を作成できます。ルーテッド ファブリックは、1 つの VRF で実行されます。これがデフォルトの VRF です。ルーテッド ファブリックでは、VRF の手動作成は無効になっていることに注意してください。ファブリックは IPv4 ファブリックであるため、ネットワーク内の IPv6 アドレスはサポートされていません。ルーテッドファブリックでは、レイヤ 2 のみのネットワークでない限り、ネットワークは 1 つのデバイスまたは vPC デバイスのペアにのみアタッチできます。

Note ルーテッド ファブリック ネットワークの構成は、config-profile の下に置かれません。

eBGP ファブリックがルーテッド ファブリック（EVPN が無効）として構成されている場合、ファブリック レベルで、ホスト トラフィックのファースト ホップ冗長性プロトコル（FHRP）として HSRP または VRRP のいずれかを選択できます。HSRP がデフォルト値です。

vPC ペアの場合、NDFC はファブリック設定に基づいてネットワーク レベルで HSRP または VRRP 設定を生成します。HSRP を選択した場合、各ネットワークは 1 つの HSRP グループと HSRP VIP アドレスを持つように構成されます。デフォルトでは、すべてのネットワークは NDFC によって割り当てられた同じ HSRP グループ番号を共有しますが、これはネットワークごとに上書きできます。VRRP サポートは HSRP に似ています。

ガイドライン

- HSRP 認証または VRRP 認証はサポートされていません。認証を使用する場合は、ネットワークの自由形式構成に適切なコマンドを入力できます。
- vPC ピア ゲートウェイを使用すると、一部のサードパーティ デバイスが HSRP 仮想 MAC を無視し、ARP 学習に ARP パケット送信元 MAC を使用している場合に、ピア リンクの使用を最小限に抑えることができます。ルーテッド ファブリック モードでは、NDFC は VPC デバイスの vPC ピア ゲートウェイ コマンドを生成します。
- eBGP ファブリックで、ネットワークと VRF が存在する場合、ルーテッド ファブリック タイプと EVPN ファブリック タイプの間、または HSRP と VRRP の間で変更することはできません。ファブリック タイプまたは FHRP を変更する場合には、これらのネットワークと VRF を展開解除して削除する必要があります。詳細については、スタンドアロン ファブリックのネットワークの展開解除およびスタンドアロン ファブリックの *VRF* の展開解除を参照してください。
- ファブリックが以前にルーテッドファブリック モードで実行されていた場合、FHRP プロトコルやネットワーク VLAN 範囲などのデフォルトのファブリック値は、ルーテッドファブリックに対して内部的に設定されます。異なる値を構成する場合は、ファブリック設定を編集する必要があります。ネットワーク構成を展開する前に、FHRP プロトコル ファブリック設定を更新し、**[再計算して展開（Recalculate & Deploy）]** をクリックする必要があります。

ルーテッド ファブリックでのネットワークの作成と展開

この手順は、ルーテッド ファブリックでネットワークを作成して展開する方法を示しています。

Before you begin

ルーテッド ファブリックを作成し、必要なリーフおよびスパイン ポリシーを展開します。

Procedure

ステップ 1 次のナビゲーションパスのいずれかを選択します。

- **[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）]** 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。

ステップ 2 **[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。

[ネットワークの作成（Create Networks）] ウィンドウが表示されます。このウィンドウのフィールドは次のとおりです。

[ネットワーク名（Network Name）]：ネットワークの名前を指定します。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）]：（オプション）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。FHRP 構成は、レイヤ 2 のみのネットワークでは生成されません。

Note L3 ネットワーク テンプレートがスタンドアロン デバイスにアタッチされている場合、FHRP 構成は生成されません。

[ネットワーク テンプレート（Network Template）]：**Routed_Network_Universal** テンプレートを選択します。

VLAN ID：（オプション）ネットワークの対応するテナント VLAN ID を指定します。

[ネットワーク プロファイル（Network Profile）] セクションには、[一般パラメータ（General Parameters）] タブと [詳細（Advanced）] タブがあります。

[一般パラメータ（General Parameters）] タブで、必要な詳細を指定します。

[アクティブ時のインターフェイス IPv4 アドレス（Intf IPv4 addr on active）]：vPC ペアのアクティブ デバイスの IPv4 インターフェイス アドレスを指定します。このフィールドは、デバイスの vPC ペア用にネットワークを作成して展開する場合にのみ適用されます。

[スタンバイ時のインターフェイス IPv4 アドレス（Intf IPv4 addr on standby）]：vPC ペアのスタンバイ/バックアップ デバイスの IPv4 インターフェイス アドレスを指定します。このフィールドは、デバイスの vPC ペア用にネットワークを作成して展開する場合にのみ適用されます。

[IPv4 ゲートウェイ/ネットマスク（IPv4 Gateway/NetMask）]：IPv4 ゲートウェイ アドレスとサブネットを指定します。

[アクティブ時のインターフェイス IPv6 アドレス（Interface IPv6 addr on active）]: vPC ペアのアクティブ デバイスの IPv6 インターフェイス アドレスを指定します。このフィールドは、デバイスの vPC ペア用にネットワークを作成して展開する場合にのみ適用されます。

[スタンバイ時のインターフェイス IPv6 アドレス（Interface IPv6 addr on standby）]：vPC ペアのスタンバイ/バックアップ デバイスの IPv6 インターフェイス アドレスを指定します。このフィールドは、デバイスの vPC ペア用にネットワークを作成して展開する場合にのみ適用されます。

[IPv6 リンク ローカル アドレス（IPv6 Link Local address）]：IPv6 リンク ローカル アドレスを指定します。このフィールドは、デバイスの vPC ペア用のネットワークを作成、展開しており、VRRP が FHRP プロトコルとして選択されている場合にのみ適用されます。

Note IPv4 ゲートウェイ アドレスとインターフェイス アドレスは同じサブネットになければなりません。

[一般パラメータ（General Parameters）] タブの次のフィールドはオプションです。

[Vlan 名（Vlan Name）]：VLAN 名を指定します。

[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。

[スタンバイ インターフェイスの説明（Standby Intf Description）]：vPC ペアのスタンバイ インターフェイスの説明を指定します。

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

[ルーティング タグ（Routing Tag）]：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ているルーティング タグを指定します。

[詳細（Advanced）] タブ：このタブは、デバイスの vPC ペア用にネットワークを作成、展開している場合にのみ適用されます。

[ファースト ホップ冗長性プロトコル（First Hop Redundancy Protocol）]：ファブリック設定で選択された FHRP を指定する読み取り専用フィールド。

[アクティブ/マスター スイッチの優先度（Active/master Switch Priority）]：アクティブまたはマスター デバイスの優先度を指定します。

[スタンバイ/バックアップ スイッチの優先度（Standby/backup Switch Priority）]：スタンバイまたはバックアップ デバイスの優先度を指定します。デフォルト値は 100 です。展開前にネットワーク構成をプレビューしても、このデフォルト値は表示されないことに注意してください。

[プリエンプトを有効にする（Enable Preempt）]：スタンバイ/バックアップ デバイスがアクティブ デバイスをプリエンプトできるかどうかを指定します。

[HSRP/VRRP グループ（HSRP/VRRP Group）]：HSRP または VRRP グループ番号を指定します。デフォルトでは、HSRP グループ番号は 1 です。

[仮想 MAC アドレス（Virtual MAC Address）]：オプション。仮想 MAC アドレスを指定します。デフォルトでは、VMAC は HSRP グループ番号（0000.0c9f.f000 + グループ番号）に基づいて内部的に生成されます。仮想 MAC アドレスは、ファブリック設定で **hsrp** が選択されている場合にのみ適用されます。

[HSRP バージョン（HSRP Version）]：HSRP バージョンを指定します。デフォルト値は 1 です。**[HSRP バージョン（HSRP Version）]** フィールドは、HSRP にのみ適用されます。

ステップ 3 [ネットワークの作成（Create Network）] をクリックします。詳細については、ネットワーク, on page 226を参照してください。

ステップ 4 **[ネットワーク アタッチメント（Network Attachment）]** ウィンドウで、vPC ペアに対し、デバイスにアクティブ状態を割り当てます。

アクティブ デバイスの場合は **[isActive]** チェックボックスをオンにし、スタンバイ デバイスの場合は **[isActive]** チェックボックスをオフにします。

[保存（Save）] をクリックします。

Note ルーテッドファブリックで、展開されたネットワークを編集し、変更を加えずに保存すると、ネットワークのステータスが **[保留中（Pending）]** に変わります。同様に、展開されたネットワークに対して **[ネットワーク アタッチメント（Network Attachment）]** ウィンドウを開き、変更せずに保存すると、ネットワークのステータスが **[保留中（Pending）]** に変わります。このような場合は、**[プレビュー（Preview）]** アイコンをクリックして構成をプレビューします。このアクションにより、ネットワーク ステータスが **展開済み（Deployed）** に戻ります。

ステップ 5 （オプション）**[プレビュー（Preview）]** アイコンをクリックして、デバイスに展開された構成をプレビューします。

[構成のプレビュー（Preview Configuration）] ウィンドウが表示されます。

ステップ 6 [展開（Deploy）] をクリックします。

[ファブリックの概要（Fabric Overview）] ウィンドウに移動し、**[展開（Deploy）]** ボタンをクリックして、ネットワークを展開することもできます。

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

ファブリック間リンクを使用して、ルート ファブリックをエッジ ルータに接続できます。このリンクは、物理インターフェイスで IP アドレスを構成し、デフォルトの vrf でエッジ ルーターとの eBGP ピアリングを確立します。BGP 構成には、リーフ スイッチへのデフォルト ルートのアドバタイズが含まれます。

Note 外部ファブリック設定の **[ファブリック モニター モード（Fabric Monitor Mode）]** チェックボックスはオフにすることができます。**[ファブリック モニター モード（Fabric Monitor Mode）]** チェックボックスをオフにすると、NDFC が設定を外部ファブリックに展開できるようになります。詳細については、外部ファブリックの作成, on page 129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。ルーティングされた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 **[リンク（Links）]** タブで、**[アクション（Actions）] > [作成（Create）]** をクリックします。

[リンク管理 - リンクの作成（Link Management-Create Link）] ウィンドウが表示されます。

[リンク タイプ（Link Type）] : **[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ボーダー スイッチを介するファブリック間接続を作成します。

[リンク サブタイプ（Link Sub-Type）]：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 **[ROUTED_FABRIC]** プロファイルを選択します。

[リンク テンプレート（Link Template）]：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設定されます。ルーテッドファブリックの場合、**ext_routed_fabric** テンプレートが読み込まれます。

[送信元ファブリック（Source Fabric）]：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ます。

[宛先ファブリック（Destination Fabric）]：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（Source Device）] と **[送信元インターフェイス（Source Interface）]**：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 インターフェイスまたはポート チャネル インターフェイスを選択します。ボーダーのロールを持つデバイスのみを選択できます。

[宛先デバイス（Destination Device）] と **[宛先インターフェイス（Destination Interface）]**：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 インターフェイスまたはポート チャネル 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き、Cisco 検出プロトコル情報（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。

[一般パラメータ（General Parameters）] タブには、次のフィールドが含まれています。

[送信元 BGP ASN（Source BGP ASN）]：このフィールドには、**leaf_bgp_asn** ポリシーを作成して適用した場合、リーフの AS 番号が自動入力されます。

[送信元 IPv4 アドレス/マスク（Source IPv4 Address/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。

[宛先 IPv4（Destination IPv4）]：このフィールドに宛先インターフェイスの IPv4 アドレスを入力します

[宛先 BGP ASN（Destination BGP 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。

[送信元 IPv6 アドレス/マスク（Source IPv6 Address/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。

[宛先 IPv6（Destination IPv6）]：このフィールドに宛先インターフェイスの IPv6 アドレスを入力します

[BGP の最大パス（BGP Maximum Paths）]：サポートされる最大の BGP パスを指定します。

[リンク MTU（Link MTU）]：このフィールドにインターフェイス MTU を入力します。

[デフォルト ルート構成を無効にする（Disable Default Route Config）]：**[デフォルト ルート構成を無効にする（Disable Default Route Config）]** チェック ボックスをオンにします。

[詳細設定（Advanced）] タブには、次のオプションのフィールドが含まれています。

[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。**保存して展開**すると、この説明が実行構成に反映されます。

[送信元インターフェイス フリーフォーム CLI（Source Interface Freeform CLIs）] および **[宛先インターフェイス フリーフォーム CLI（Destination Interface Freeform CLIs）]**：送信元と宛先インターフェイスに固有のフリーフォーム構成を入力します。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 , on page 108を参照してください。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 外部ファブリックのエッジ ルータに接続しているデバイスをダブルクリックし、**[アクション（Actions）] > [再計算と展開（Recalculate & Deploy）]** をクリックします。

ステップ 5 **[構成の展開（Deploy Configuration）]** ウィンドウで構成の展開が完了したら、**[閉じる（Close）]** をクリックします。

ステップ 6 **[LAN ファブリック（LAN Fabric）]** ウィンドウで外部ファブリックに移動し、ファブリックをダブルクリックします。

ステップ 7 **[リンク（Links）]** タブをクリックして、外部ファブリックのすべてのリンクを表示します。

作成されたファブリック間リンクが表示されます。

Note 外部ファブリックが監視モードでない場合、ファブリック間リンクが作成されます。

ステップ 8 **[LAN ファブリック（LAN Fabric）]** ウィンドウに移動します。

ステップ 9 ルーテッド ファブリックに接続している外部ファブリックをダブルクリックし、**[アクション（Actions）] > [再計算と展開（Recalculate & Deploy）]** をクリックします。

ステップ 10 **[構成の展開（Deploy Configuration）]** ウィンドウで構成の展開が完了したら、**[閉じる（Close）]** 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。