Cisco DCNM LAN ファブリックの 構成ガイド、リリース 11.5(x)

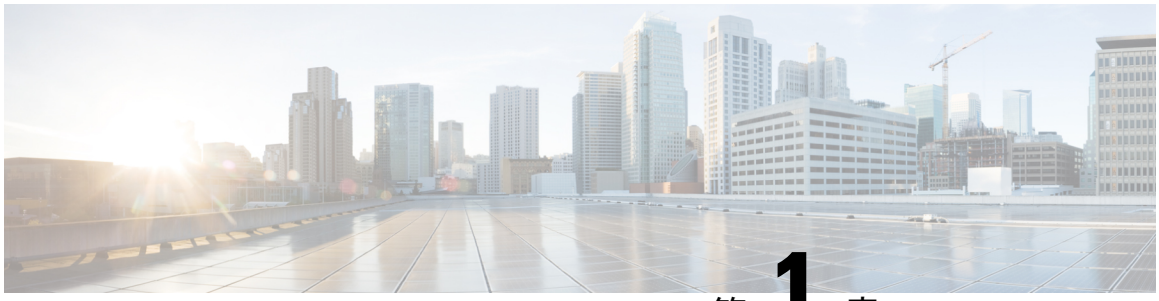
初版：2020 年 12 月 22 日

最終更新：2022 年 3 月 4 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。

目 次



第 1 章

[概要（Overview）]

Cisco Data Center Network Manager

Cisco Data Center Network Manager（Cisco DCNM）は、Cisco Nexus 5000、6000、7000、および 9000 シリーズ スイッチと Cisco MDS 9000 シリーズ スイッチのインフラストラクチャを自動化します。Cisco DCNM では、制御、自動化、モニタリング、視覚化、トラブルシューティングなどのすぐに使用できる機能を提供しながら、複数のデバイスを管理できます。

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

Cisco DCNM を LAN ファブリック モードで展開している場合、デバイス コネクタの構成は必須です。インストール時にデバイス コネクタを構成しなかった場合は、ログインするたびにデバイス コネクタを構成するように求めるメッセージが表示されます。**[次回から表示しない（Do not show again）]** にチェックを入れると、メッセージは表示されません。ただし、**[アラーム（Alarms）]** アイコンの下にアラーム通知が追加されます。

Cisco DCNM ホームページの左側にはナビゲーション ペインがあり、中央のペインにはいくつかの Cisco DCNM 機能へのショートカットがあります。

このガイドでは、Cisco DCNM ローカル エリア ネットワーク（LAN） ファブリック 展開の UI 機能に関する包括的な情報を提供します。

上部ペインには、次の UI 要素が表示されます。

- **[アラートと通知（Alerts and Notifications）]**：Cisco DCNM の上部ペインにある **[ヘルプ（Help）]** アイコンの横にある**[アラートと通知（Alerts and Notifications）]**アイコンをクリックすると、アラートとイベント通知を表示できます。
- **[ヘルプ（Help）]**：文脈依存オンライン ヘルプを起動します。
- **[アラーム（Alarms）]**：**[アラーム（Alarms）]**アイコンは、アラームがある場合、またはCisco DCNM 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。
  - **[DCNM の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（Alarms）]** アイコンが点滅し、メッセージが表示されます。
  - **[デバイス コネクタの切断（Device Connector Disconnected）]**：インストール中にデバイス コネクタが構成されていない場合、このアラームは、デバイス コネクタがIntersight に接続されていないことを示しているように見えます。**[管理（Administration）] > [デバイス コネクタ（Device Connector）]** を選択して、デバイス コネクタを構成し、アラームを削除します。
  - **[DCNM の高可用性 (HA) 状態（High Availability (HA) State of DCNM）]**：ネイティブ HA セットアップが同期されていない場合。**[アラーム（Alarms）]** アイコンが点滅している場合は、ノードの 1 つまたは両方が停止しているか、障害が発生しているか、準備ができていない可能性があります。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 DCNM 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。それぞれのアラームをクリックして、**[Web UI] > [アプリケーション（Applications）] > [カタログ（Catalog）]** のアプリケーションに移動します。
  - **[コンピューティング ノードが切断されました（Compute Node disconnected）]**：1 つ以上のコンピューティング ノードがダウンすると、アラーム メッセージが表示されます。
- [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。
- **[歯車（Gear）]**アイコン：歯車アイコンをクリックして、次のオプションを含むドロップダウン リストを表示します。
  - **[選択したユーザーとしてログイン（Logged in as）]**：現在ログインしているユーザーのユーザー ロールを表示します。
  - **[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 （network administrator）]ユーザの場合、他のユーザーのパスワードを変更できます。

- **[詳細（About）]**：バージョン、インストールタイプ、およびWeb UIが動作してからの時間を表示します。
- **[REST API ツール（REST API Tool）]**：すべての操作で呼び出された API を調べることができます。API 検査についてもっと詳しい情報を得るには*[REST API ツール（REST API Tool）]* セクションを表示します。
- **[ログアウト（Logout）]**：Web UI を終了し、ログイン画面に戻ります。

Cisco DCNM の詳細については、次を参照してください：

https://www.cisco.com/c/en/us/support/cloud-systems-management/data-center-network-manager-11/model.html.

REST API ツール

Cisco DCNM Web UI で実行される検出、ファブリック管理、モニタリングなどの操作では、アクセスされた情報をフェッチしてコミットするために HTTP 呼び出しを行います。REST API ツールを使用すると、API 呼び出しの構造を表示して API 呼び出しを調べることができます。このツールは、対応する CURL リクエストも提供し、迅速なプロトタイプの作成と API のテストを支援します。

[REST API ツール（REST API Tool）] ダイアログ ボックスには、次のフィールドがあります。

***Table 1: REST API* ツール ダイアログ ボックスのフィールドと説明**

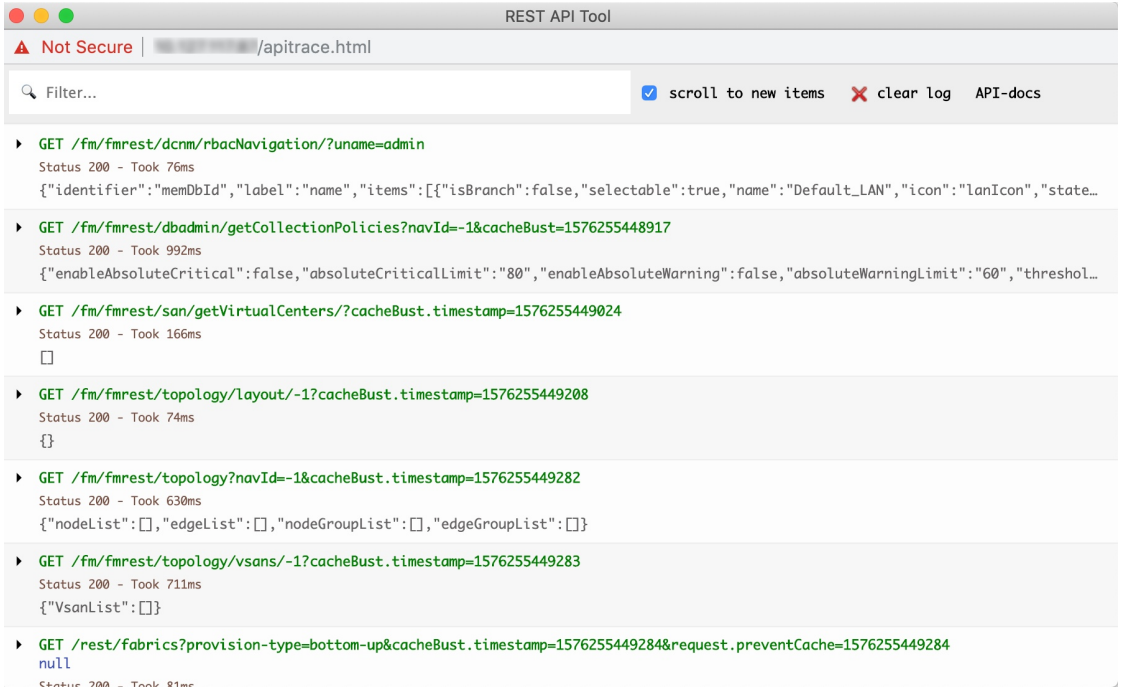
フィールド	説明
フィルタ	任意のキーワードを入力してログを検索します。
新しいアイテムにスクロール	Web UI で操作を実行した後、**[REST API ツール（REST API Tool）]** ダイアログ ボックスに戻ったときに、新しいエントリにスクロールするには、このチェック ボックスをオンにします。 このチェックボックスは、デフォルトでオンになっています。
clear log	**[ログのクリア（clear log）]** をクリックして、ダイアログ ボックスのログをクリアします。

フィールド	説明
API ドキュメント	API-docs をクリックして、Web UI で Cisco DCNM REST API ドキュメントを表示します。このオプションをクリックすると、次の URL に移動します。https://*DCNM-IP*/api-docs

Cisco DCNM Web UI で実行するすべてのアクションは、API インスペクタ ツールに表示されます。次の情報は、すべての操作で呼び出される API に表示されます。

- HTTPメソッド
- URI
- ペイロード
- HTTP ステータス コード
- 操作にかかる時間

次の画像は、**[REST API ツール（REST API Tool）]** ダイアログ ボックスにログがどのように表示されるかを示しています。

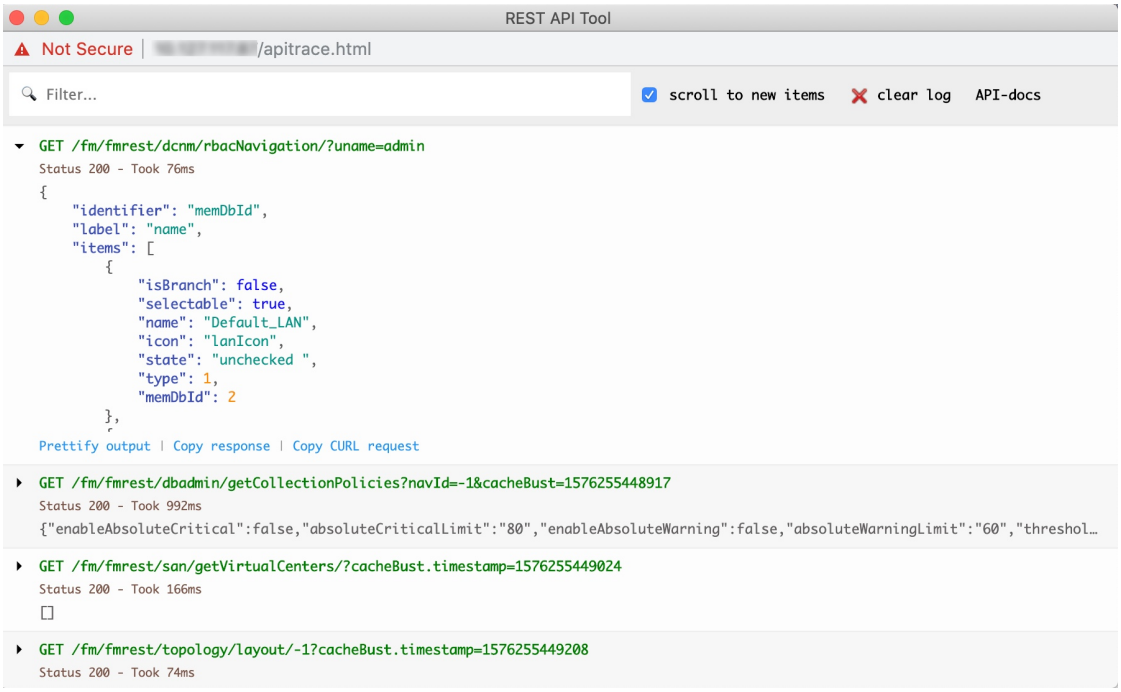


各 REST メソッドを展開または折りたたむには、URI をクリックします。REST メソッドを展開した後、次のアクションを実行できます。

- **出力を整形する**：このオプションをクリックして、応答コードをより見やすいように配置します。そうしないと、1行で表示されます。応答をスクロールして、完全に表示します。

- **応答をコピー**：このオプションをクリックして、応答コードをクリップボードにコピーします。
- **CURL リクエストをコピー**：このオプションをクリックして、CURL リクエストをクリップボードにコピーします。

```
curl -k -XGET --header 'Dcnm-Token: <DCNM_TOKEN>' --header 'Content-Type:
application/x-www-form-urlencoded'
https://<ip-address>/fm/fmrest/dcnm/rbacNavigation/?uname=admin
```



[REST API ツール（REST API Tool）] ダイアログ ボックスは、Cisco DCNM Web UI が更新されるたびに更新されます。

Cisco DCNM Web UI から API インスペクタを使用するには、次の手順を実行します。

Procedure

ステップ 1 上部ペインの**歯車**アイコンをクリックします。

ステップ 2 ドロップダウン リストから **[REST API ツール（REST API Tool）]** を選択します。

Cisco DCNM Web UI で操作を実行する前は、**[REST API ツール（REST API Tool）]** ダイアログ ボックスが表示されており、ログは空です。

ステップ 3 **[REST API ツール（REST API Tool）]** ダイアログ ボックスを最小化します。

Note ダイアログボックスを開いたままにすることもできますが、閉じないようにすることもできます。

ステップ 4 Cisco DCNM Web UI で操作を実行します。

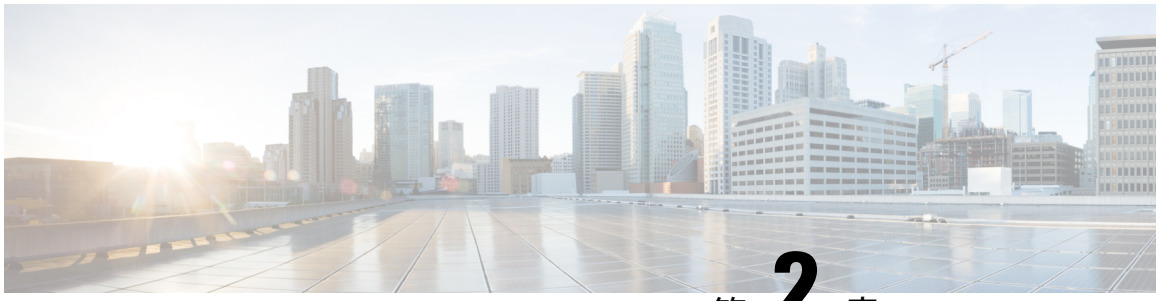
Note オプションの表示、追加、削除など、Cisco DCNM Web UI で任意の操作を実行できます。

ステップ 5 **[REST API ツール（REST API Tool）]** ダイアログ ボックスに戻ります。

ログには、実行した操作に応じてフェッチされた REST API が入力されます。

Note 操作を実行する前に **[REST API ツール（REST API Tool）]** ダイアログ ボックスを最小化するのではなく閉じてしまうと、ログがクリアされます。

REST API ツールを使用して実行できる操作の一部のデモについては、Cisco DCNM ビデオでの REST API ツールの使用を参照してください。



第 2 章

新機能と変更情報

この章は、次の内容で構成されています。

Cisco DCNM リリース 11.5(3) の新しい情報と変更された情報

次の表は、この最新リリースに関するマニュアルでの主な変更点の概要を示したものです。ただし、このリリースに関するガイドの変更点や新機能の中には、一部、この表に記載されていないものもあります。

表 *2 : Cisco DCNM* リリース *11.5(3)* の新しい動作と変更された動作

機能	説明	参照先
ThousandEyes Enterprise Agent	モニタ対象のネットワーク内でユーザーが特定のウェブサイトにアクセスするとき、ThousandEyes Enterprise Agent はネットワークとアプリケーション レイヤのパフォーマンス データを収集します。テストの実行、ネットワークパスと接続の詳細なアスペクトのチェック、ネットワーク ルーティングのステータス チェック、インテント、実行構成などの変更のモニタを行うために、データは使用されます。	• ThousandEyes Enterprise Agent （518 ページ） • ThousandEyes Enterprise エージェント アクションの実行

Cisco DCNM リリース 11.5(1) の新しい情報と変更された情報

次の表は、この最新リリースに関するマニュアルでの主な変更点の概要を示したものです。ただし、このリリースに関するガイドの変更点や新機能の中には、一部、この表に記載されていないものもあります。

表 *3 : Cisco DCNM* リリース *11.5(1)* の新しい動作および変更された動作

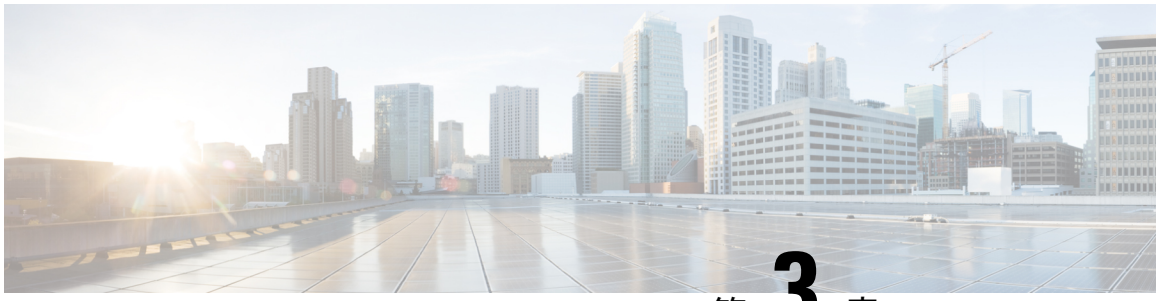
機能	説明	参照先
単一スイッチ構成の復元	Cisco DCNM Web UI から外部ファブリックおよび LAN クラシック ファブリックの Cisco Nexus スイッチの構成を復元できます。スイッチ レベルで復元する情報は、ファブリック レベルのバックアップから抽出されます。スイッチ レベルの復元では、ファブリック レベルのインテントおよびファブリック設定を使用して適用されたその他の構成は復元されません。スイッチ レベルのインテントのみが復元されます。	スイッチの復元 （383 ページ）
EPLD ゴールデン アップグレード	Cisco DCNM リリース 11.5(1) 以降、DCNM は EPLD ゴールデン アップグレードもサポートします。EPLDアップグレードを実行するときに、Nexus 9000 シリーズ スイッチのゴールデン リージョンまたはプライマリ リージョンを選択するオプションがあります。**[イベント（Events）]** ウィンドウで EPLD ゴールデン アップグレード通知を表示できます。Cisco DCNM Web UI のホームページから、**[モニタ（Monitor）] > [スイッチ（Switch）] > [イベント（Events）]** を選択します。	EPLD インストール （504 ページ）

PTP モニタリング アプリケーション	高精度時間プロトコル（PTP）はネットワークに分散したノードの時刻同期プロトコルです。ローカルエリア ネットワークでは、サブマイクロ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。DCNM では、PTP モニタリングをアプリケーションとしてインストールできます。以前はメディア コントローラの展開にインストールできたこの PTP モニタリング アプリケーションを、プレビュー機能として LAN ファブリックの展開にインストールできるようになりました。この機能を実稼働環境で展開することは推奨されていません。	PTP Monitoring （722 ページ）
ブラウンフィールド展開のための簡素化された CLI 構成のサポート	DCNM 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。	ガイドラインと制約事項 （831 ページ）
CloudSec の操作表示	MSD ファブリックで CloudSec が有効になっている場合、**DCNM の [CloudSec 操作表示（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。	CloudSec の動作状態の表示 （209 ページ）
アウトオブバンド スイッチインターフェイス構成と DCNM の同期	**[host_port_resync]** ポリシーを使用して、アウトオブバンドスイッチインターフェイス レベルの構成を（CLI 経由で）Cisco DCNM と同期させ、その後管理することができます。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。	アウトオブバンド スイッチインターフェイス構成と DCNM の同期 （226 ページ）
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 を構成するには、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。これは、Cisco DCNM リリース 11.5(1) のプレビュー機能です。	Easy ファブリックおよび eBGP ファブリックでの MACsec サポート （231 ページ）

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。	インターフェイス グループ （324 ページ）
L4 ～ 7 サービス拡張	DCNM リリース 11.5(1) では、次の拡張機能が導入されています。 • 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。 • レイヤ 4 ～ レイヤ 7 サービスは、静的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）に静的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。 • ワンアーム仮想ネットワーク機能がサポートされています。 • レイヤ 4 ～ レイヤ 7 サービス REST API は、DCNM パッケージの REST API ドキュメントを介してアクセスできます。 • ルート ピアリングの一括アタッチ、デタッチ、プレビュー、および展開と、サービス ポリシーがサポートされていますが、最大 10 のルート ピアリングまたは 10 のサービス ポリシーまでに制限されています。 • **[監査履歴（Audit History）]** 機能は、サービス ノード、ルート ピアリング、およびサービス ポリシーに加えられた変更のログを表示します。	レイヤ 4 ～ レイヤ 7 サービス （1013 ページ）

OpenStack ワークロードの可視性	OpenStack クラスタをモニタするのに役立つ OpenStack プラグイン アプリケーションが DCNM によって提供されます。物理ネットワーク接続と仮想化されたワークロードに関する可視性を得て、データセンターのコンテキスト内で VM ネットワーキング固有の問題をデバッグできます。これは、Cisco DCNM リリース 11.5(1) のプレビュー機能です。	• OpenStack ビジュアライザ （436 ページ） • OpenStack ワークロードの可視性（53 ページ）
ファブリックのボーダーでの L3 ゲートウェイのサポート	Cisco DCNM リリース 11.5(1) 以降、**[ボーダーで L3 ゲートウェイを有効にする（Enable L3 Gateway on Border）]** フィールドは、MSD ネットワーク設定の一部として使用できません。ボーダー スイッチのレイヤ 3 ゲートウェイをファブリック レベルで有効にすることができます。	VXLAN BGP EVPN ファブリックのマルチサイト ドメイン （174 ページ）
定期レポート生成の頻度	• 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。 • レポートの生成中に generateReport メソッドが呼び出されます。レポートにはレポート導入ロジックが含まれます。このメソッドは、任意のコンテキスト オブジェクトを受け入れます。	• レポート ジョブの作成 （728 ページ） • テンプレート機能のレポート （478 ページ）
デバイスの事前プロビジョニング	Cisco DCNM リリース 11.5(1) 以降、事前プロビジョニングされたデバイスへの構成サポートが拡張されました。	デバイスの事前プロビジョニング
拡張されたロールベースのアクセス制御	新しいユーザー ロール、**[device-upg-admin]**、および **[access-admin]** が追加されています。 • **[device-upg-admin]** ロールを持つユーザーは、**[イメージ管理（Image Management）]** ウィンドウでのみ操作を実行できます。 • **[access-admin]** ロールを持つユーザーは、すべてのファブリックの **[インターフェイス マネージャ（Interface Manager）]** ウィンドウでのみ操作を実行できます。	• Cisco DCNM の拡張された役割別のアクセス制御 • インターフェイス

スイッチスマートライセンス	Cisco DCNM リリース 11.5(1) 以降、新しいライセンスタイプがスイッチに追加されました。	スイッチ スマート ライセンス
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	Cisco DCNM では、ブラウンフィールド展開でのみ、外部および LAN クラシック ファブリックのインバンド接続のスイッチをインポートまたは検出できます。ファブリック設定を構成または編集しながら、ファブリックごとにインバンド管理を有効にします。POAP を使用してインバンド接続のスイッチをインポートまたは検出することはできません。	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 （223 ページ）
外部ファブリックまたは LAN クラシック ファブリック向け高精度時間プロトコル（PTP）	リリース 11.5(1) から、**[External_Fabric_11_1]** または **[LAN_Classic]** テンプレートのファブリック設定で、[高精度時間プロトコル（PTP）を有効化（Enable Precision Time Protocol（PTP）] チェックボックスをオンにして、ファブリック全体で PTP を有効にします。	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） （224 ページ）
GUI から DNS、NTP サーバーを編集する機能	Cisco DCNM では、Web UI からいくつかのネットワーク パラメータを変更できます。これらを変更すると、以前に構成されたパラメータが上書きされます。	ネットワーク基本設定（577 ページ）



第 3 章

ダッシュボード

この章は次のトピックで構成されています。

ダッシュボード

[ダッシュボード（Dashboard）]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エリア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。ローカル エリア ネットワーク（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範囲のコンテキストで情報を表示する[6 つ（six）] のダイナミック ダッシュレットで構成されます。ウィンドウの右上隅で範囲を調整して、管理対象ドメインに固有のフォーカスされた情報を表示できます。データ センターの範囲の一部である特定のトポロジまたはトポロジの設定の詳細を提供します。

Cisco Data Center Network Manager (DCNM) Web インターフェイスで使用できるさまざまな範囲は次のとおりです。

- **データセンター**
- **Default_SAN**
- **Default_LAN**
- 各 SAN ファブリック
- 作成するカスタム 範囲

左のメニュー バーから **[ダッシュボード（Dashboard）]** を選択します。**[ダッシュボード（Dashboard）]** ウィンドウには、次のデフォルト ダッシュレットが表示されます。

[ダッシュボード（Dashboard）] 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。

- Data Center
- インベントリ（スイッチ）

- インベントリ（モジュール）
- 上位 CPU
- 上位の ISL/トランク
- リンク トラフィック
- アラーム
- イベント
- サーバステータス（Server Status）
- 監査ログ

[ダッシュレット（Dashlets）] ドロップダウン リストから、さらにダッシュレットを選択して、 ダッシュボードに追加できます。

パネルを追加、削除、ドラッグして並べ替えることができます。

ダッシュレット

デフォルトでは、使用可能なダッシュレットのサブセットがダッシュボードのに自動的に表示されます。ダッシュボードに自動的に表示されないダッシュレットを追加するには、Cisco DCNM Web UI から、次の手順を実行します。

Procedure

ステップ 1 **[ダッシュボード（Dashboard）]** を選択します。

ステップ 2 **[ダッシュレット（Dashlets）]** ドロップダウン リストから、ダッシュボードに追加するダッシュレットを選択します。

[ダッシュレット（Dashlets）] ドロップダウン リストで、選択したダッシュレットの前にアイコンが表示されます。

次の表に、**[ダッシュボード（Dashboard）]** ウィンドウに追加できるダッシュレットを示します。

ダッシュレット	説明
Events	シビラティ（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。このダッシュレットで、**[確認済みイベントの表示（Show Acknowledged Events）]** リンクをクリックして、**[モニタ（Monitor）] > [スイッチ（Switch）] > [イベント（Events）]** に移動します。

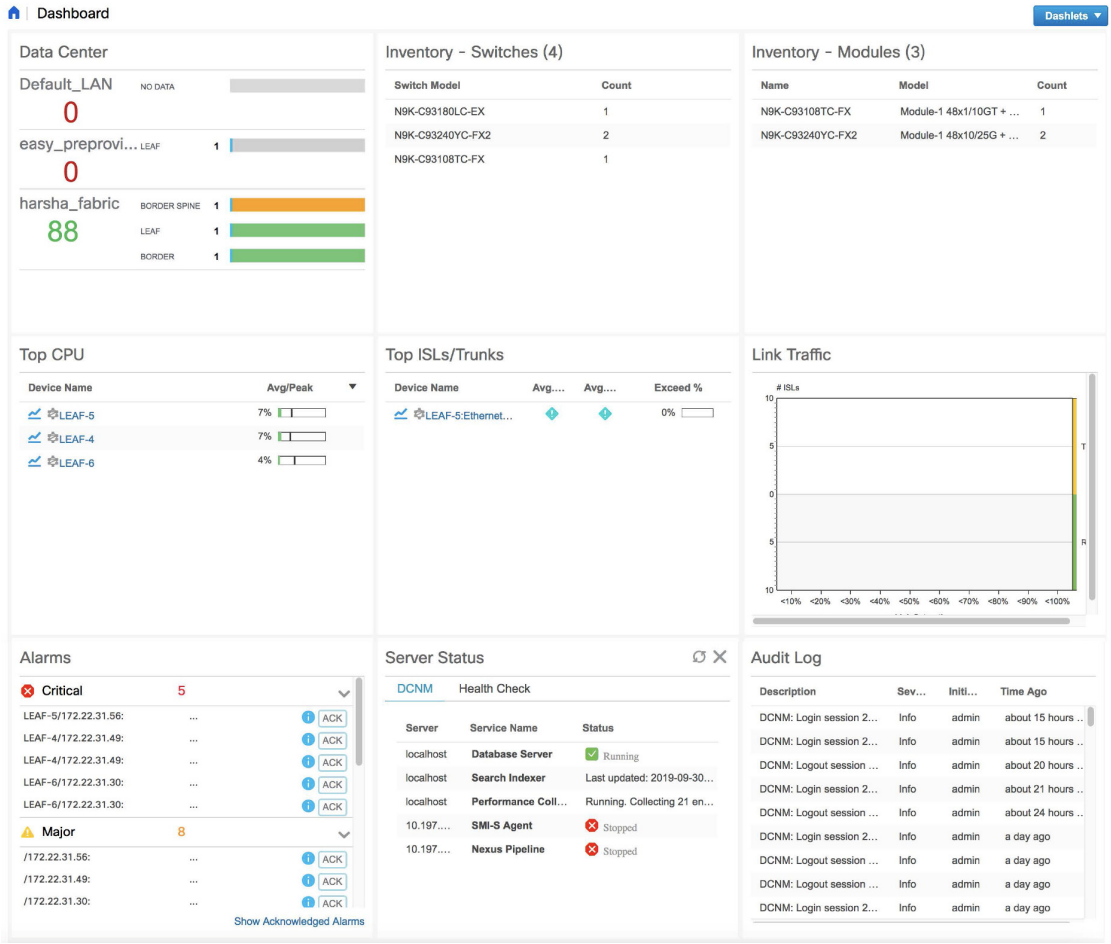
ダッシュレット	説明
アラーム	**重大、メジャー、マイナー**および**警告**の重大度のアラームを表示します。このダッシュレットで、**[確認済みアラームの表示（Show Acknowledged Alarms）]** リンクをクリックして、**[モニタ（Monitor）] > [アラーム（Alarms）] > [表示（View）]** ウィンドウに移動します。特定のアラームの詳細については、青い **[i]** アイコンにマウス カーソルを合わせます。特定のアラームを確認するには、**[ACK]** をクリックします。
リンク トラフィック	データセンターで送受信するための Inter-Switch Link（ISL）およびサチュレーション リンクの図を表示します。
Data Center	現在の範囲内の各スイッチ グループのアクセス、スパインおよびリーフ デバイスの数、および一般的な正常性スコアを表示します。デバイスは、スイッチ グループ内のタイプ別に集約されます。
監査ログ	Cisco DCNM のアカウンティング ログ テーブルを表示します。
ネットワーク マップ	Role Based Access Control（RBAC）範囲で表示される設定済みのスイッチ グループを世界地図に表示します。範囲セレクタを使用すると、表示されるスイッチ グループのセットが制限されます。[デタッチ（detach）] オプションをクリックすると、マップが新しいタブで開き、構成できます。 • [ネットワーク マップ（network map）] ダイアログ ボックスには、サマリ ダッシュボード ビューとは異なるプロパティがあります。 • ノードをクリックしてドラッグすると、マップ内でノードを移動できます。マップは新しい位置を保存します。 • ノードをダブルクリックすると、特定のスイッチ グループに関するサマリ インベントリ情報を含むスライダーをトリガできます。

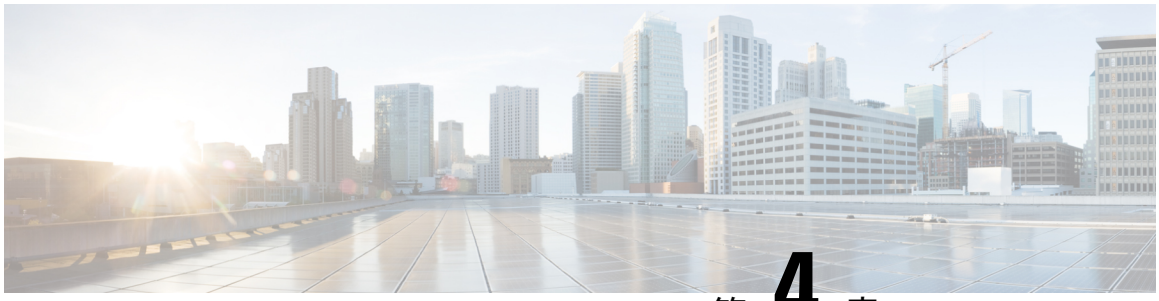
ダッシュレット	説明
	• 選択した画像をネットワーク マップの背景としてアップロードできます。 **Note** 現在のウィンドウサイズである推奨サイズの画像ファイルをアップロードするように求められます。リセットは、ネットワークマップをデフォルトの状態に戻し、ノードの位置をリセットし、カスタム画像をクリアします。
サーバステータス（Server Status）	DCNMおよびフェデレーションサーバーのステータス、およびコンポーネントの正常性チェック ステータスを表示します。 次のサービス、サーバー、およびステータスの詳細が **[DCNM]** タブに表示されます。 • データベース サーバ • 検索インジケータ • パフォーマンスコレクタ • NTPD サーバー • DHCP サーバー • SNMP トラップ • [Syslogサーバ（Syslog Server）] **[正常性チェック（Health Check）]** タブには、次のコンポーネントのステータスと詳細が表示されます。 • AMQP サーバー • DHCP サーバー • TFTP サーバ • EPLS • EPLC
上位の ISL/トランク	パフォーマンスの上位 10 個の ISL、トランクポート、またはその両方のパフォーマンスデータを表示します。各エントリには、現在の平均の受信と送信の割合が表示され、各トラン

ダッシュレット	説明
	クが現在設定されているしきい値を超えて費やした時間の割合を示すグラフが表示されます。
上位の SAN エンド ポート（SAN のみ）	パフォーマンスが高い上位 10 位までの SAN ホストおよびストレージポートのパフォーマンスデータを表示します。各エントリには、現在の受信と送信の割合が表示され、各トランクが現在設定されているしきい値を超えて費やした時間の割合を示すグラフが表示されます。 **Note** このダッシュレットは SAN 専用です。
上位 CPU	過去 24 時間に検出されたスイッチの CPU 使用率を表示し、赤いバーにその 24 時間の最高水準点を表示します。
上位パラメータ	スイッチのモジュール温度センサの詳細を表示します。 **Note** このダッシュレットは LAN 専用です。
ヘルス（Health）	過去 24 時間の問題の概要とイベントの要約を表示する 2 つの列を含む正常性の概要を表示します。 スイッチ、ISL、ホスト、またはストレージ（0 以外）に関する警告の横にあるカウントをクリックして、そのファブリックの対応するインベントリを表示します。 イベントの重大度レベル（緊急、アラート、クリティカル、エラー、警告、通知、情報、またはデバッグ）の横にあるカウントをクリックして、対応するイベントの概要と説明を表示します。 リリース 11.4(1) 以降、Cisco DCNM を HA モードで展開している場合、正常性ダッシュレットに HA セットアップのステータスが表示されます。HA 状態とともに、アクティブ、スタンバイ HA ノード、および VIP の IP アドレスも表示されます。

ダッシュレット	説明
エラー	選択されたインターフェイスのエラー パケットを表示します。この情報は、**[モニタ（Monitor）] > [LAN/イーサネット（LAN / Ethernet）]** ページの **[エラー（Errors）] > [In-Peak]** および **[エラー（Errors）] > [Out-Peak]** 列から取得されます。
破棄	選択したインターフェイスで破棄された上位のエラーパケットを表示します。 **Note** 破棄ダッシュレットは LAN 専用です。
インベントリ（ポート）	ポートインベントリに関する要約情報を表示します。
インベントリ（モジュール）	モジュールが検出されたスイッチ、モデル名、カウントを表示します。
インベントリ（ISL）	ISL のカテゴリや数など、ISL インベントリの概要情報を表示します。
インベントリ（論理）	論理リンクのカテゴリや数など、論理インベントリの概要情報を表示します。
インベントリ（スイッチ）	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。
インベントリ（ポート容量）	階層、使用可能なポートの数と割合、残りの日数など、ポート容量インベントリの概要情報を表示します。

Note ダッシュボードページでデフォルトのダッシュレットを復元するには、**[ダッシュレット（Dashlet）]** ドロップダウン リストの **[デフォルト セット（Default Set）]** リンクをクリックします。


Dashboard
Dashlets
Data Center
Default_LAN
NO DATA
0
easy_preprovi...
LEAF
1
0
harsha_fabric
BORDER SPINE
1
88
LEAF
1
BORDER
1
Inventory - Switches (4)
Switch Model
Count
N9K-C93180LC-EX
1
N9K-C93240YC-FX2
2
N9K-C93108TC-FX
1
Inventory - Modules (3)
Name
Model
Count
N9K-C93108TC-FX
Module-1 48x1/10GT + ...
1
N9K-C93240YC-FX2
Module-1 48x10/25G + ...
2
Top CPU
Device Name
Avg/Peak
LEAF-5
7%
LEAF-4
7%
LEAF-6
4%
Top ISLs/Trunks
Device Name
Avg....
Avg....
Exceed %
LEAF-5:Ethernet...
0%
Link Traffic
ISLs
10
5
0
5
10
<10%
<20%
<30%
<40%
<50%
<60%
<70%
<80%
<90%
<100%
Alarms
Critical
5
LEAF-5/172.22.31.56:
LEAF-4/172.22.31.49:
LEAF-4/172.22.31.49:
LEAF-6/172.22.31.30:
LEAF-6/172.22.31.30:
ACK
Major
8
/172.22.31.56:
/172.22.31.49:
/172.22.31.30:
Show Acknowledged Alarms
Server Status
DCNM
Health Check
Server
Service Name
Status
localhost
Database Server
Running
localhost
Search Indexer
Last updated: 2019-09-30...
localhost
Performance Coll...
Running. Collecting 21 en...
10.197....
SMI-S Agent
Stopped
10.197....
Nexus Pipeline
Stopped
Audit Log
Description
Sev...
Initi...
Time Ago
DCNM: Login session 2...
Info
admin
about 15 hours ..
DCNM: Login session 2...
Info
admin
about 15 hours ..
DCNM: Logout session ...
Info
admin
about 20 hours ..
DCNM: Login session 2...
Info
admin
about 21 hours ..
DCNM: Logout session ...
Info
admin
about 24 hours ..
DCNM: Login session 2...
Info
admin
a day ago
DCNM: Logout session ...
Info
admin
a day ago
DCNM: Logout session ...
Info
admin
a day ago
DCNM: Login session 2...
Info
admin
a day ago



第 4 章

トポロジ

トポロジ

[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ホバーさせます。また、リンクのノードまたは線をクリックします。ウィンドウの右側からスライドインペインが表示されます。このペインには、スイッチまたはリンクに関する詳細情報が表示されます。

Note 複数のタブを同時に開いたり、並べて機能させたりして、比較やトラブルシューティングをすることができます。

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。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。
- 黄：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。
- 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。

Note

- **[トポロジ（Topology）]** ウィンドウでは、FEX の正常性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。

  同様に、**[ファブリックビルダー（Fabric Builder）]** トポロジウィンドウにはFEXの設定同期ステータスがなく、**n/a** と表示されます)。

- 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。ポートの移動は、**[トポロジ（Topology）]** ウィンドウでは更新されません。更新されたポートが DCNM に表示されるようにスイッチを再検出する必要があります。

- 黒: エレメントがダウンしていることを示します。

Cisco DCNM リリース 11.4(1) 以降、スイッチがメンテナンス モードの場合、スイッチの横に**メンテナンス モード バッジ**が表示されます。スイッチが移行モードの場合、スイッチの横に**移行モード**のバッジが表示されます。

スコープ

範囲に基づいてトポロジを検索できます。**[範囲（SCOPE）]** ドロップダウン リストから使用可能なデフォルトの範囲は、**[DEFAULT_LAN]**

[DEFAULT_LAN] では、次の検索オプションを使用できます。

- 高速検索
- ホスト名（vCenter）
- ホスト IP
- ホスト MAC
- マルチキャスト グループ

- VXLAN 識別子（VNI）
- VLAN
- FabricPath
- VXLAN OAM

検索

ノード数が多いと、目的のスイッチやリンクを見つけるのがすぐに難しくなります。検索を実行すると、スイッチやリンクをすばやく見つけることができます。VM トラッカーと汎用セットアップを検索することもできます。検索機能により、ホストが接続されているリーフを確認できます。

次の検索が利用できます。

Note デフォルトでは、クイック検索が選択されています。

高速検索

[クイック検索（Quick Search）] では、名前、IP アドレス、モデル、シリアル番号、スイッチのロールでデバイスを検索できます。**[検索（Search）]** フィールドに検索パラメータを入力すると、トポロジ内で対応するスイッチが強調表示されます。複数のノードおよびリンクの検索を実行するには、複数のキーワードをコンマで区切ります（例：ABCD12345、N7K、sw-dc4-12345, core、172.23.45.67）。Cisco DCNM はワイルドカード検索もサポートしています。シリアル番号またはスイッチ名の一部がわかっている場合は、ABCD*、sw*12345、core などのように、アスタリスクを付けてこれらの部分的な用語で検索を構築できます。

[クイック検索（Quick Search）] には、タイプ（IP アドレスまたは名前）に基づいて OpenStack 技術情報を検索するオプションが用意されています。ホスト IP で検索でき、対応するホストが強調表示されます。**OpenStack** ドロップダウン リストから IP アドレスに基づいて特定の OpenStack クラスタを選択し、その中で検索することもできます。

検索の範囲をパラメータに制限するには、パラメータ名の後にスペースを入力し、パラメータを検索フィールドに入力します（例：name=sw*12345、serialNumber=ABCD12345 など）。

ホスト名（確認ポップアップで、[はい（Yes）]をクリックしてテンプレートを削除します。）

ホスト名検索では、vCenter を使用してホストを検索できます。

ポッド名（コンテナ）

ポッドリストをクリックして選択したクラスタで実行されているすべてのポッドに関する詳細を表示できます。クラスタの選択が [すべて（All）] の場合、トポロジ内のすべてのクラスタ

で実行されているすべてのポッドが表示されます。今後の分析のため、ポッド リスト データをエクスポートすることもできます。

VM 名（OpenStack）

検索欄から **[VM 名（OpenStack）]**を選択し、VM 名を入力します。VM からファブリック スイッチへのパスが強調表示されます。この検索オプションでは、**[表示（Show）]** パネルの OpenStackで **[すべて（All）]** を選択しておく必要があります。それ以外の場合、この検索オプションは無効になります。

ホスト IP

ホストの IP アドレスを使用してトポロジを検索できます。**[ホスト IP（Host IP）]** は、範囲内のスイッチを検索して、**[検索（Search）]**フィールドに入力した IP アドレスに一致するホストを見つけます。**[ホスト IP（Host IP）]** 検索は IPv4 アドレスをサポートします。検索ドロップダウン リストから **[ホスト IP（Host IP）]** を選択し、ホストの MAC アドレスを使用してトポロジを検索します。**[検索（Search）]** フィールドにホストの IP アドレスを入力し、**Enter** キーを押します。**[詳細（Details）]**をクリックして、対応するホストの詳細を表示します。

ホスト MAC

ホストの MAC アドレスを使用してトポロジを検索できます。**[ホスト MAC（Host MAC）]** は、範囲内のスイッチを検索して、**[検索（Search）]**フィールドに入力した MAC アドレスに一致するホストを見つけます。検索ドロップダウン リストから **[ホスト MAC（Host MAC）]** を選択し、ホストの MAC アドレスを使用してトポロジを検索します。検索フィールドにホストの MAC アドレスを入力し、**Enter** キーを押します。**[詳細（Details）]**をクリックして、対応するホストの詳細を表示します。

マルチキャスト グループ

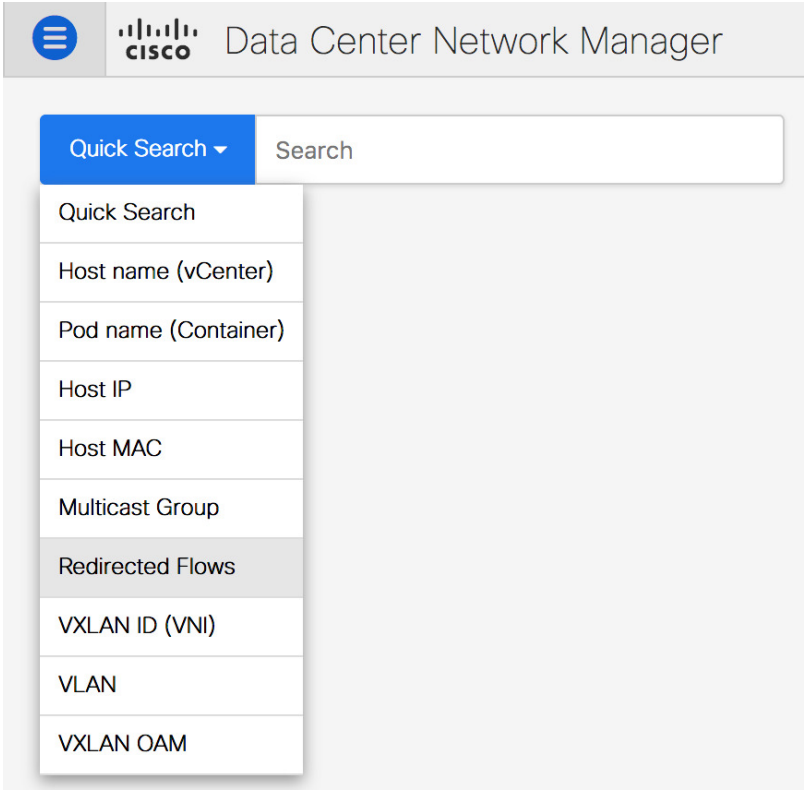
[マルチキャスト グループ（Multicast Group）]の検索は、VXLAN コンテキスト、VXLAN トンネル エンドポイント、または VTEP スイッチに限定され、このマルチキャスト アドレスに関連付けられた VXLAN ID（VNI）を取得します。

ドロップダウン リストから**[マルチキャスト グループ（Multicast Group）]**検索を選択し、検索フィールドにマルチキャスト アドレスを入力して、**Enter** キーを押します。検索フィールドの横にある **[詳細（Details）]** リンクをクリックして、詳細な マルチキャスト アドレス テーブルを取得します。テーブルには、検索されたマルチキャスト アドレスが設定されているスイッチと、関連付けられた VNI、VNI ステータス、およびマッピングされた VLAN が表示されます。

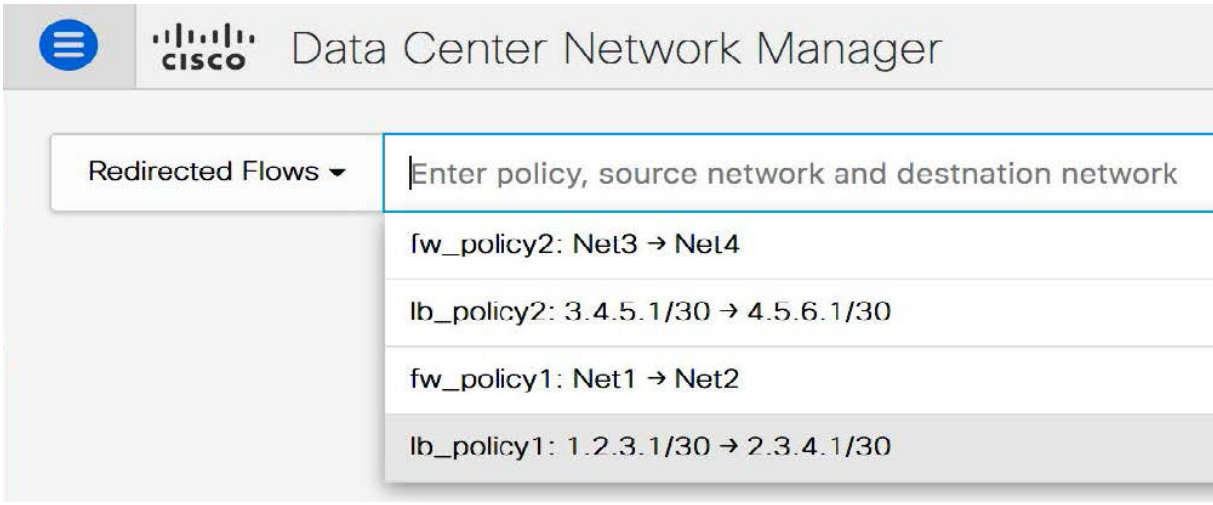
ハイライト表示されているスイッチにカーソルをホバーさせると、実行した検索の詳細を表示することもできます。

リダイレクト フロー

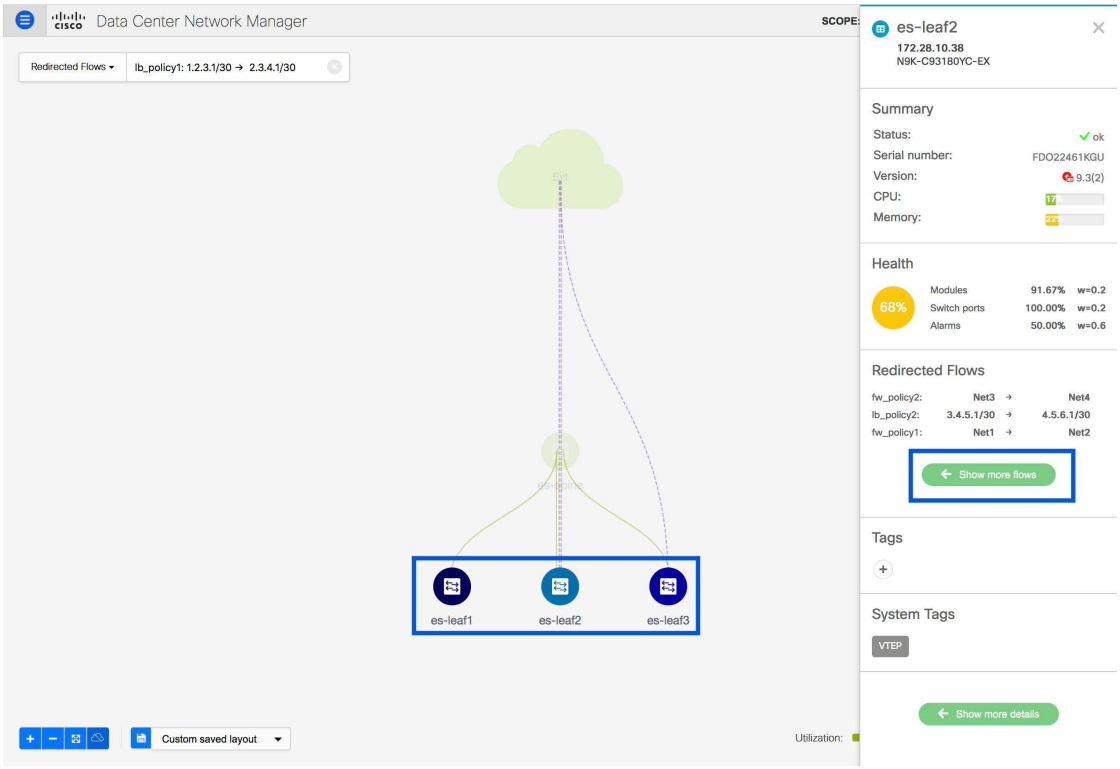
ファブリックへのサービス ノードの物理的な接続が定義されたら、**[トポロジ（Topology）]** ウィンドウの **[クイック検索（Quick Search）]** ドロップダウン リストから **[リダイレクトされたフロー（Redirected Flow）]** を選択します。



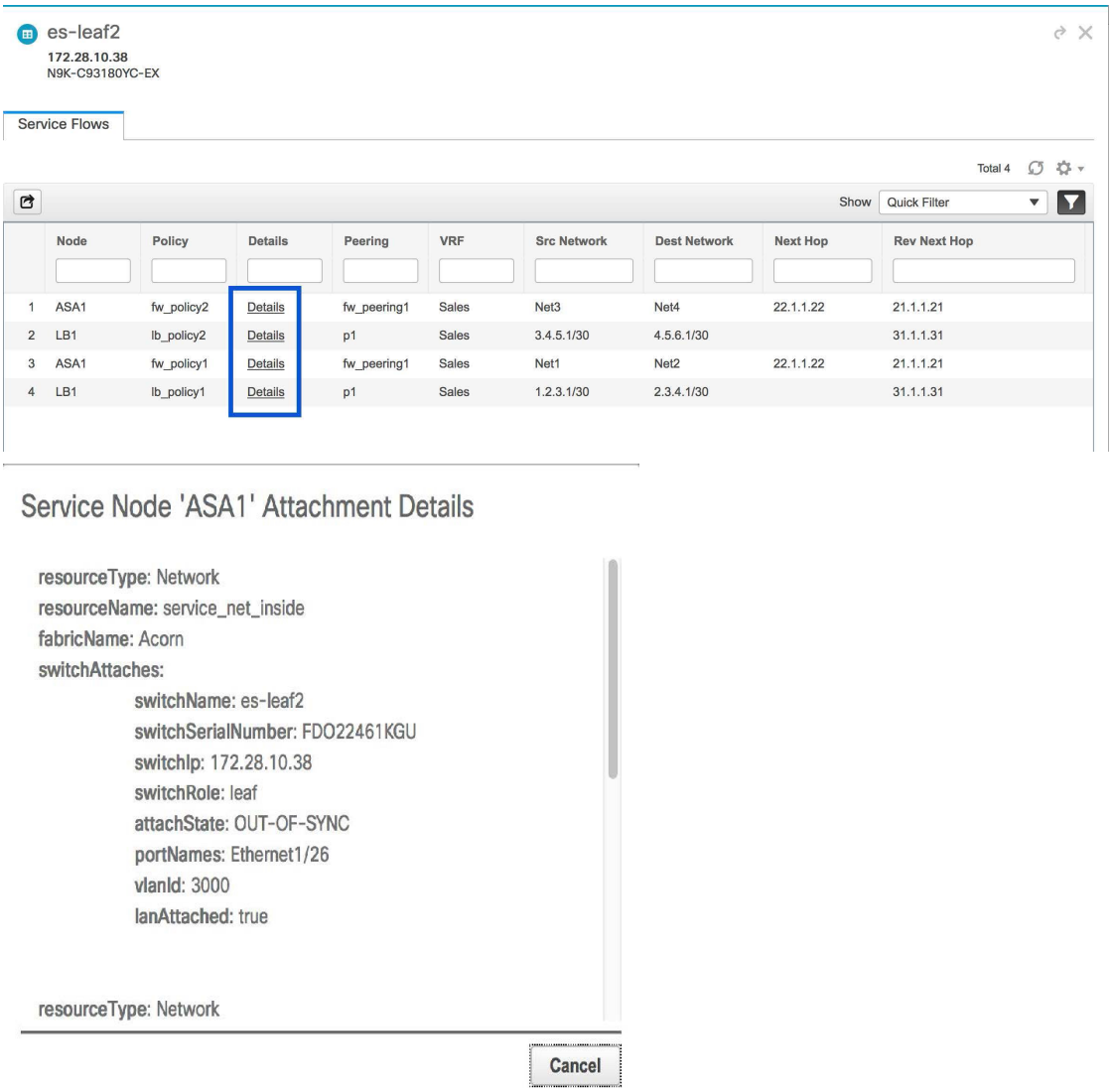
ドロップダウン リストからポリシーを選択するか、検索フィールドにポリシー名、送信元ネットワーク、および宛先ネットワークを入力して検索を開始することができます。検索フィールドへの入力を始めると、自動的に補完されます。



検索フィールドへの入力に基づいて、トポロジ ウィンドウでスイッチが強調表示されます。送信元ネットワークと宛先ネットワークが接続され、フローがリダイレクトされたスイッチは、トポロジ ウィンドウで強調表示されます。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。スイッチをクリックして、そのスイッチで開始、リダイレクト、または終了したリダイレクト フローを表示します。**[他のフローを表示（Show more flows）]** をクリックして、リダイレクトされたすべてのフローに関する情報を含む **[サービス フロー（Service Flows）]** ウィンドウを表示します。



[詳細（Details）]（**[サービス フロー（Service Flows）]** ウィンドウ）をクリックして、付属ファイルの詳細を表示します。



VXLAN 識別子（VNI）

VXLAN 識別子または VNI 検索では、VNI でトポロジを検索できます。ドロップダウン リストから **[VXLAN 識別子（VNI）VXLAN ID (VNI)]** 検索フィールドに [VNI] と入力し、**[入力（Enter）]** を押します。検索フィールドの横にある **[詳細（Details）]** リンクをクリックして、詳細な VNI テーブルを表示します。テーブルには、VNI が構成されているスイッチが、関連付けられたマルチキャスト アドレス、VNI ステータス、およびマッピングされた VLAN とともに表示されます。

VLAN

指定された VLAN 識別子 で検索します。VLAN 検索では、スイッチまたはリンクに構成されている VLAN を検索できます。STP が有効になっている場合、STP プロトコルに関連する情報とリンクの STP 情報が提供されます。

VXLAN OAM

VXLAN EVPN ベースのファブリック トポロジ内のフローの到達可能性や実際のパスなどの詳細を追跡するには、**[検索（Search）]** ドロップダウン リストから **[VXLAN OAM]** オプションを選択するか、**[検索（Search）]** フィールドに **VXLAN OAM** と入力します。**[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。DCNM 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、接続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。

- **[送信元スイッチ（Source IP）]** フィールドに、送信元ホストの IP アドレスを入力します。
- **[接続先スイッチ（Destination IP）]** フィールドに、接続先ホストの IP 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。
- （オプション）**[送信元ポート（Source Port）]** 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。
- （オプション）**[接続先ポート（Destination Port）]** フィールドで、接続先ポート番号を選択するか、その値を入力します。

- （オプション）**[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。
- **[送信元と接続先のIP（および該当する場合はMAC）の交換/スワップ（Interchange/Swap Source and Destination IPs (and MACs if applicable)）]** アイコンをクリックして、送信元と接続先のIPアドレスを交換します。この交換により、ホストのIPアドレスまたはMACアドレスを再入力することなく、リバース パスをすばやくトレースできます。
- **[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。

次の追加フィールドに値を入力します。

パネルを表示

次のオプションに基づいてトポロジを表示することを選択できます。

- **自動更新**：このチェック ボックスをオンにすると、トポロジが自動的に更新されます。
- **スイッチの健全性**：このチェックボックスをオンにして、スイッチの健全性ステータスを表示します。
- **FEX**：このチェックボックスをオンにして、ファブリック エクステンダを表示します。

  Cisco NX-OS リリース 11.4(1) 以降、このチェックボックスをオフにすると、FEX デバイスは **Fabric Builder** トポロジ ウィンドウでも非表示になります。**Fabric Builder** で FEX を表示するには、このチェックボックスをオンにする必要があります。このオプションはすべてのファブリックに適用でき、セッションごとに保存されるか、DCNMからログアウトするまで保存されます。ログアウトしてDCNMにログインすると、FEXオプションはデフォルトにリセットされます。つまり、デフォルトで有効になります。詳細については、新規 VXLAN BGP EVPN ファブリックの作成, on page 64を参照してください。

Note FEX機能は、LANデバイスでのみ使用できます。したがって、このチェックボックスをオンにすると、FEXをサポートするCisco Nexusスイッチのみが表示されます。

Note FEXは、Cisco Nexus 1000Vデバイスでもサポートされていません。したがって、**[FEX]** チェックボックスをオンにしても、そのようなデバイスはトポロジに表示されません。

- **リンク**：このチェックボックスを選択し、トポロジのリンクを表示します。次のオプションを使用できます。
  - **エラーのみ**：エラーのあるリンクのみを表示するには、このラジオボタンをクリックします。
  - **すべて**：このラジオボタンをクリックして、トポロジ内のすべてのリンクを表示します。
  - **VPC のみ**：vPC ピア リンクと vPC のみを表示するには、このチェックボックスをオンにします。
  - **帯域幅**：リンクによって消費される帯域幅に基づいて色分けを表示するには、このチェック ボックスをオンにします。
- **OTV**：このチェック ボックスをオンにすると、オーバーレイ トランスポート仮想化（OTV）トポロジがクラウド アイコンと OTV エッジ デバイスからの点線で表示されます。クラウドとリンクにカーソルを合わせると、コントロール グループ、拡張 VLAN などの OTV トポロジに関連する情報が表示されます。フィルタ フィールドの下に OTV 検索フィールドが表示されます。OTV 検索フィールドを使用して、**オーバーレイ ID** と**拡張 VLAN ID** に基づいて表示されている OTV トポロジを検索します。**オーバーレイ ID** と**拡張 VLAN ID** に基づいて検索された仮想リンクは、緑色でマークされます。

  [OTV] チェックボックスをオンにすると、**[詳細（Details）]**リンクが表示されます。リンクをクリックすると、OTV トポロジデータが表示されます。**[オーバーレイ ネットワーク（Overlay Network）]**列は、特定のトポロジがマルチキャスト ベースかユニキャスト ベースかを示します。**[エッジ デバイス（Edge Device）]** 列には、特定の OTV トポロジのエッジ スイッチが表示されます。他の列には、対応するオーバーレイ インターフェイス、拡張 VLAN、参加インターフェイス、およびデータ グループ情報が表示されます。
- **UI 制御**：チェック ボックスをオンにして、**[トポロジ（Topology）]** ウィンドウのさまざまな制御を表示または非表示にします。
- **コンピューティング**：チェックボックスをオンにして、**[トポロジ（Topology）]** ウィンドウでのコンピューティングの可視性を有効にします。
- **更新**：このパネルの右上隅にある **[更新（Refresh）]** アイコンをクリックして、トポロジの更新を実行することもできます。

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。

- **[階層（Hierarchical）]** および **[階層左右（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、DCNM は 16 のスイッチごとにリーフ層を分割します。

- **[ランダム（Random）]**: ノードはウィンドウ上に[ランダム（randomly）]に配置されます。DCNM は、推測を行い、近接するノードをインテリジェントに配置しようとします。
- **[円形（Circular）]** および **[同心円状（Tiered-Circular）]** : ノードを円形または同心円状に描画します。
- **[カスタム保存レイアウト（Custom saved layout）]** : 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、DCNM により最後に保存したレイアウト位置に基づいてノードが描画されます。

レイアウトを選択する前に、DCNM 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、DCNM それを使用します。カスタム レイアウトが適用されていない場合は、DCNM 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。

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。

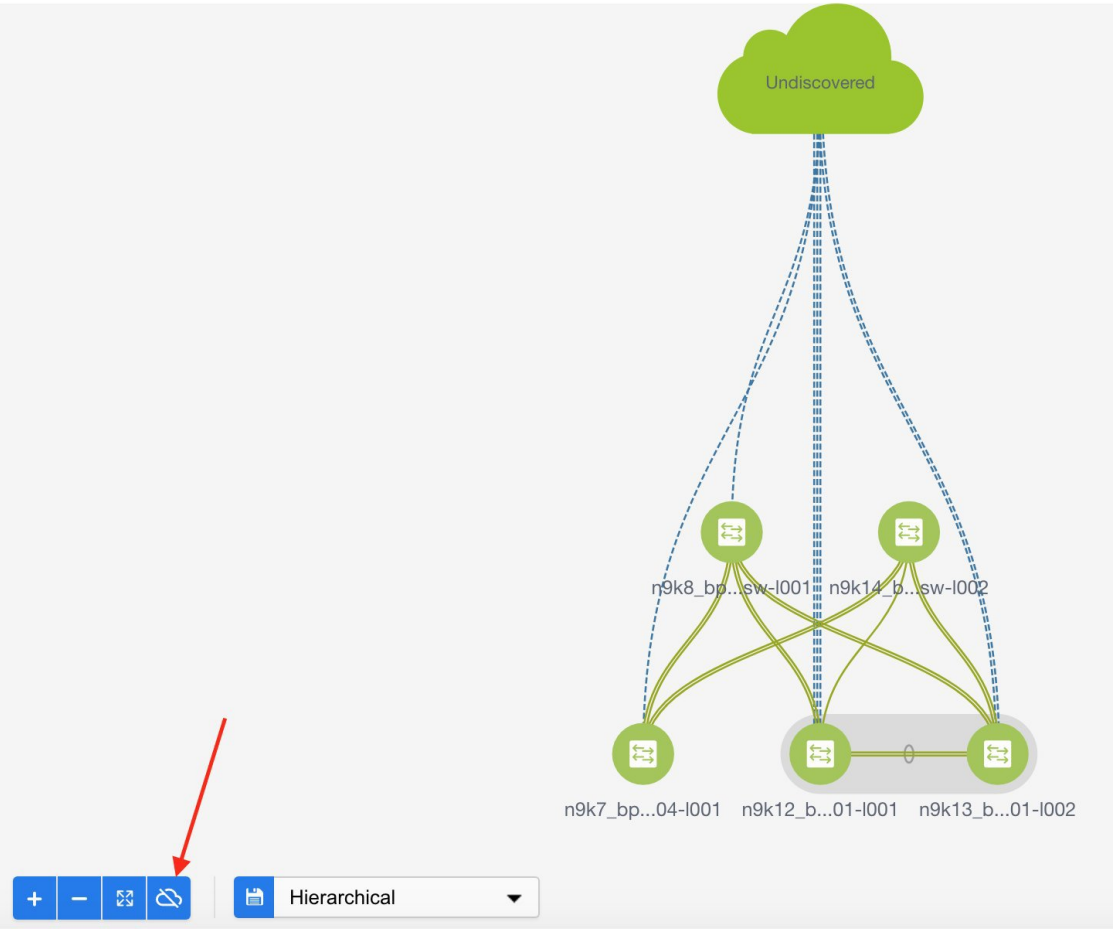
スイッチをドラッグするには、トポロジの空白領域をクリックしてカーソルを移動します。

VXLAN（スタンドアロン、MSD、およびMSD メンバー）ファブリックおよび外部ファブリックでは、非 DCNM 管理対象スイッチへの検出されたリンクまたは接続（CDP 経由）は、**[未検出（Undiscovered）]** というラベルの付いたクラウドで表されます。

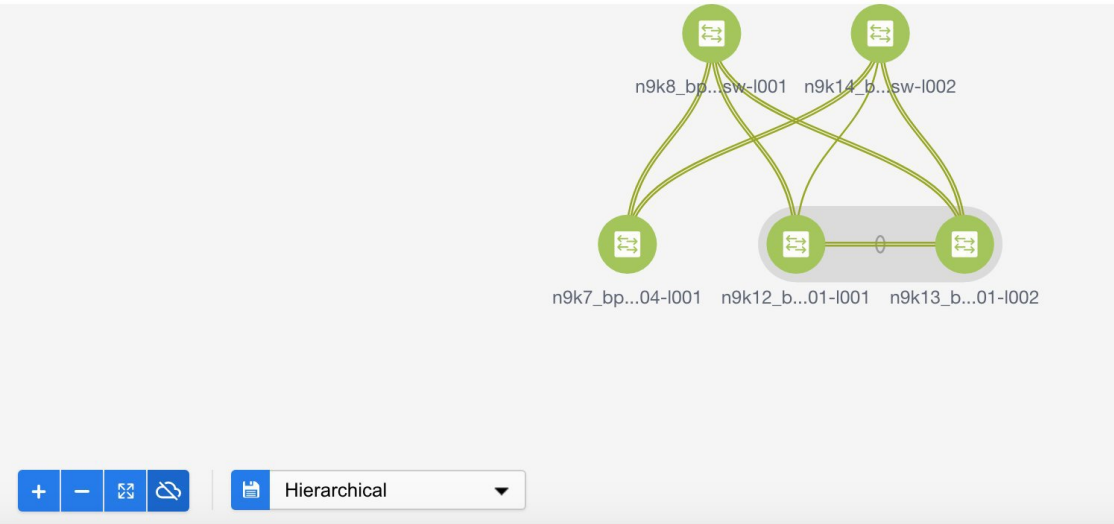
未検出のクラウド ディスプレイ

[トポロジ（Topology）] 画面では、画像の上部に**[未検出（Undiscovered）]**のクラウドが表示されます。

Note 未検出のクラウドはデフォルトで非表示になっています。画面左下のクラウドアイコンをクリックすると、未検出のクラウドを表示できます。



もう一度クリックすると、**[未検出（Undiscovered）]**のクラウドが表示されなくなります。**[未検出（Undiscovered）]**のクラウドとそのファブリック デバイスへのリンクが表示されていないことがわかります。



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

スイッチ スライドアウト パネル

構成したスイッチ名、IP アドレス、スイッチ モデルとステーテス、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要約情報をスイッチをクリックすることで表示することができます。

ビーコン

このボタンは、**beacon** コマンドをサポートするスイッチに表示されます。ビーコンが開始されると、ボタンにカウントダウンが表示されます。デフォルトでは、ビーコンは 60 秒後に停止しますが、**[ビーコンの停止（Stop Beacon）]** をクリックしてすぐに停止できます。

Note デフォルト時間は、`server.properties` ファイルで構成できます。**beacon.turnOff.time** を検索します。ミリ秒単位の時間。この機能を有効にするには、サーバの再起動が必要です。

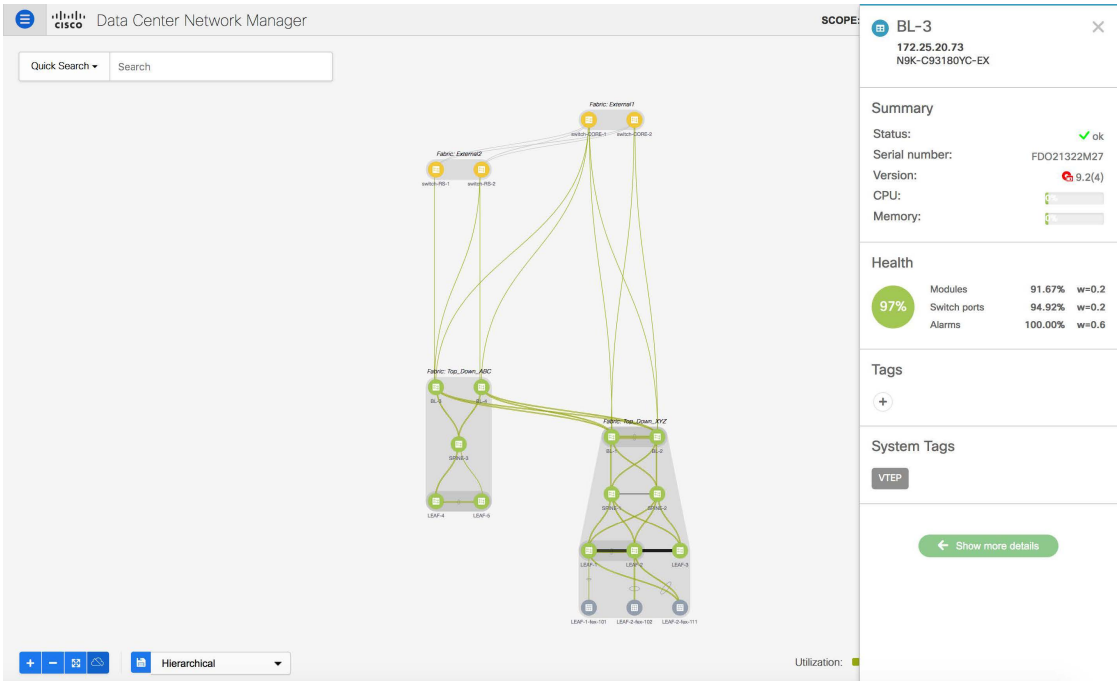
タギング

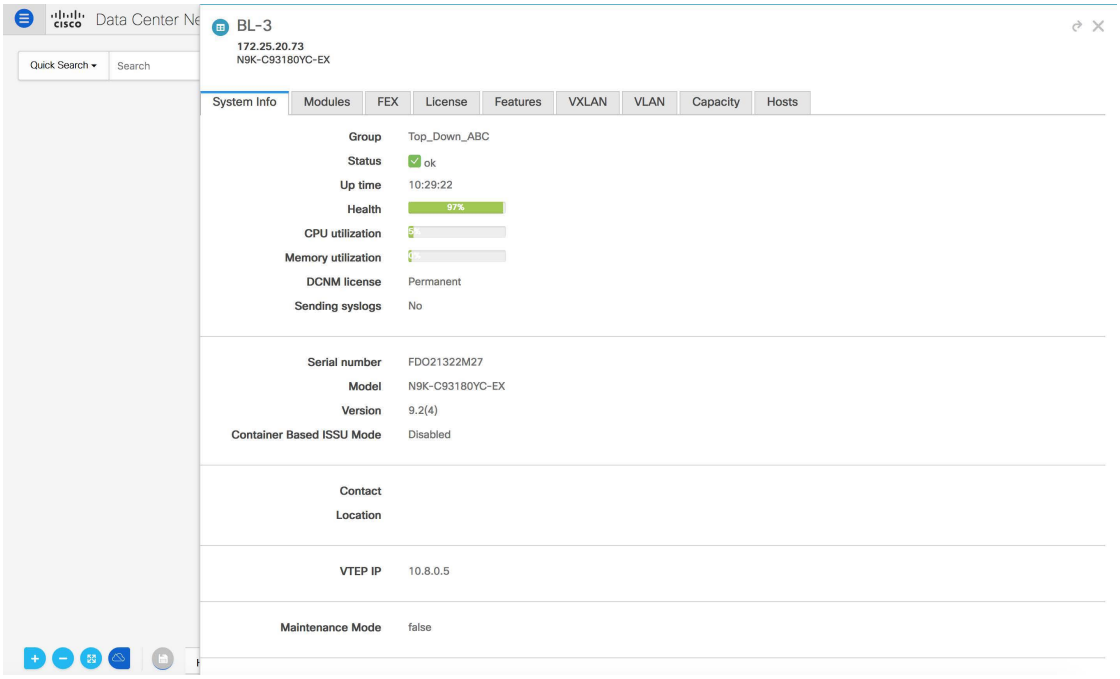
タグ付けは、スイッチを整理するための強力かつ簡単な方法です。タグは、*[建物 6（building 6）]*、*[フロア 2（floor 2）]*、*[ラック 7（rack 7）]*、*[問題スイッチ（problem switch）]*、*[ジャスティン デバッグ（Justin debugging）]* など、事実上任意の文字列にすることができます。

検索機能を使用して、タグに基づいて検索を実行します。

詳細の表示

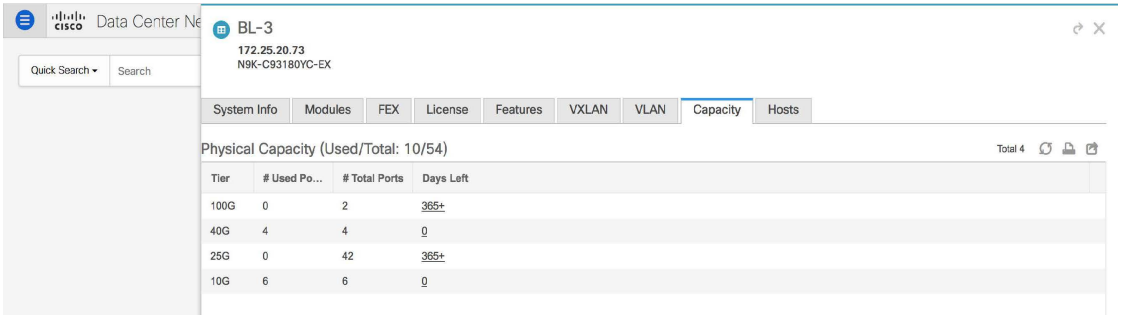
[詳細を表示（Show more details）] をクリックして、**[システム情報、モジュール、FEX、ライセンス、機能、VXLAN、VLAN、容量（System Info, Modules, FEX, License, Features, VXLAN, VLAN, Capacity）]**、および **[ホスト（Host）]** のタブの下に詳細情報を表示します。





Cisco DCNM リリース 11.4(1) 以降、400G 層も **[キャパシティ（Capacity）]** タブの **[物理キャパシティ（Physical Capacity）]** テーブルに追加されています。ただし、**[キャパシティ（Capacity）]**

タブの **[物理キャパシティ（Physical Capacity）]** テーブルには、スイッチに存在する物理ポートに関する情報のみが表示されます。たとえば、スイッチに 400G の物理ポートがない場合、400G 層は、 **[物理キャパシティ（Physical Capacity）]** テーブルに表示されません。



リンク スライドアウト パネル

リンクをクリックして、ステータスと、リンクを説明するポートまたはスイッチを表示できます。

24 時間トラフィック

この機能を使用するには、**パフォーマンス モニタリング**を**オン**にする必要があります。**[パフォーマンス監視（Performance Monitoring）]** が **[オン（ON）]** になると、トラフィック情報が収集され、集約情報がグラフ トラフィックの使用状況とともに表示されます。

vCenter コンピューティングの可視化

仮想化環境では、あらゆる種類のトラブルシューティングは、仮想マシンのネットワーク接続ポイントを識別することから始まります。これは、サーバ、仮想スイッチ、ポートグループ、VLAN、関連するネットワーク スイッチ、および物理ポートの迅速な決定が重要であることを意味します。これには、複数のツール（コンピューティング オーケストレータ、コンピューティング マネージャ、ネットワーク マネージャ、ネットワーク コントローラなど）への参照に加えて、サーバーとネットワーク管理者との間の複数のタッチポイントと対話が必要です。

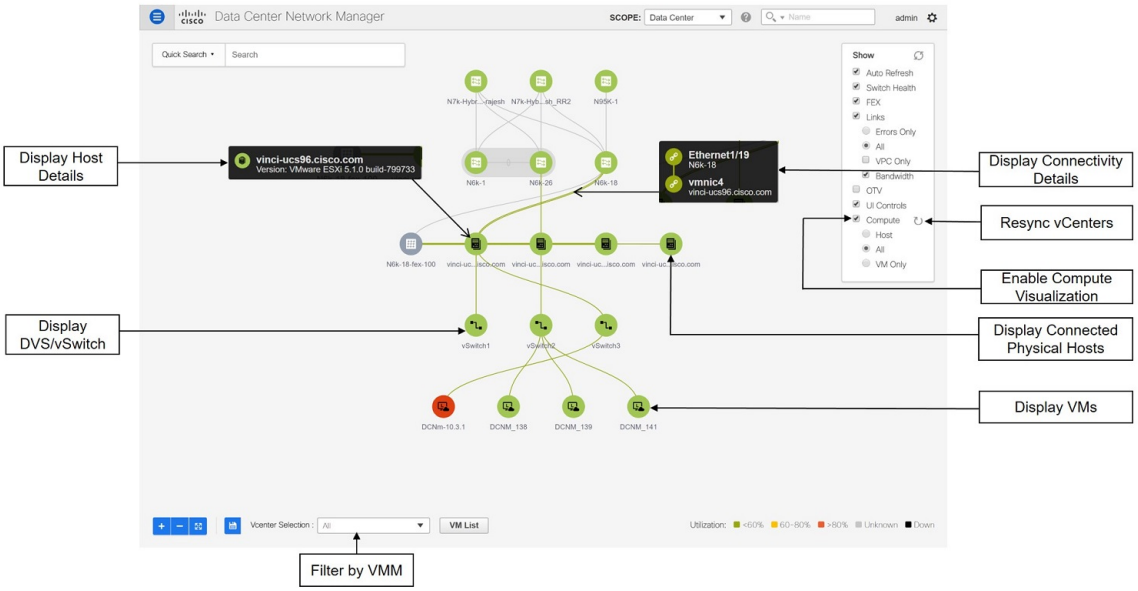
これにより、vCenter で管理されるホストとそのリーフ スイッチ接続を**[トポロジ（Topology）]** ウィンドウで可視化できます。可視化オプションには、接続された物理ホストのみ、VM のみ、またはその両方の表示が含まれます。両方を選択すると、仮想スイッチを含むリーフ スイッチから VM までのトポロジが表示されます。VM 検索オプションは、VM のパスを強調表示します。ホストまたは接続されたアップリンクにカーソルを置くと、そのエンティティに関連する重要な情報が表示されます。最大 4 つの vCenter がサポートされます。

VMM は、ボーダー スパインに接続するコンピューティングをサポートします。ボーダー スパイン は、Cisco DCNM 11.1(1) の Easy Fabric によって管理される新しいスイッチ ロールです。

Note

- vCenter コンピューティングの可視化機能は、vCenter が管理するコンピューティングの LAN クラシック インストールと Easy Fabrics のインストールの両方でサポートされます。
- vCenter は表示名で使用される特殊文字をエスケープしないため、VM 名に特殊文字を使用することは推奨されません。詳細については、https://vss-wiki.eis.utoronto.ca/display/VSSPublic/Virtual+Machine+Naming を参照してください。
- Cisco DCNM は、シスコ以外のブレード サーバをサポートしていません。

***Figure 1: vCenter* コンピューティングの可視化**

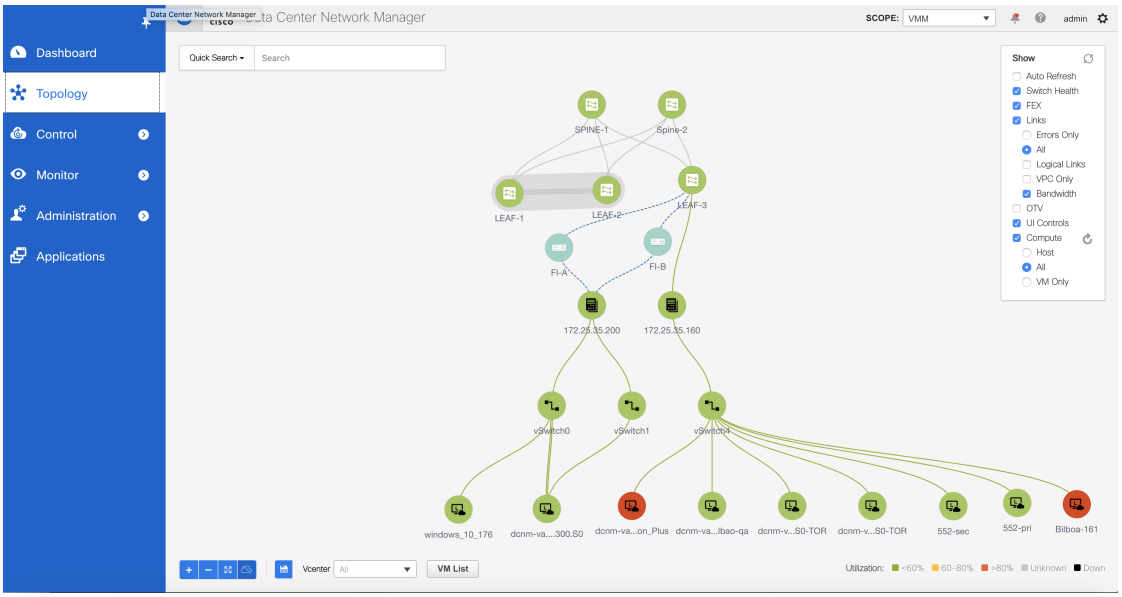


Cisco UCS B シリーズ ブレードサーバーのサポート

Cisco DCNM 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。

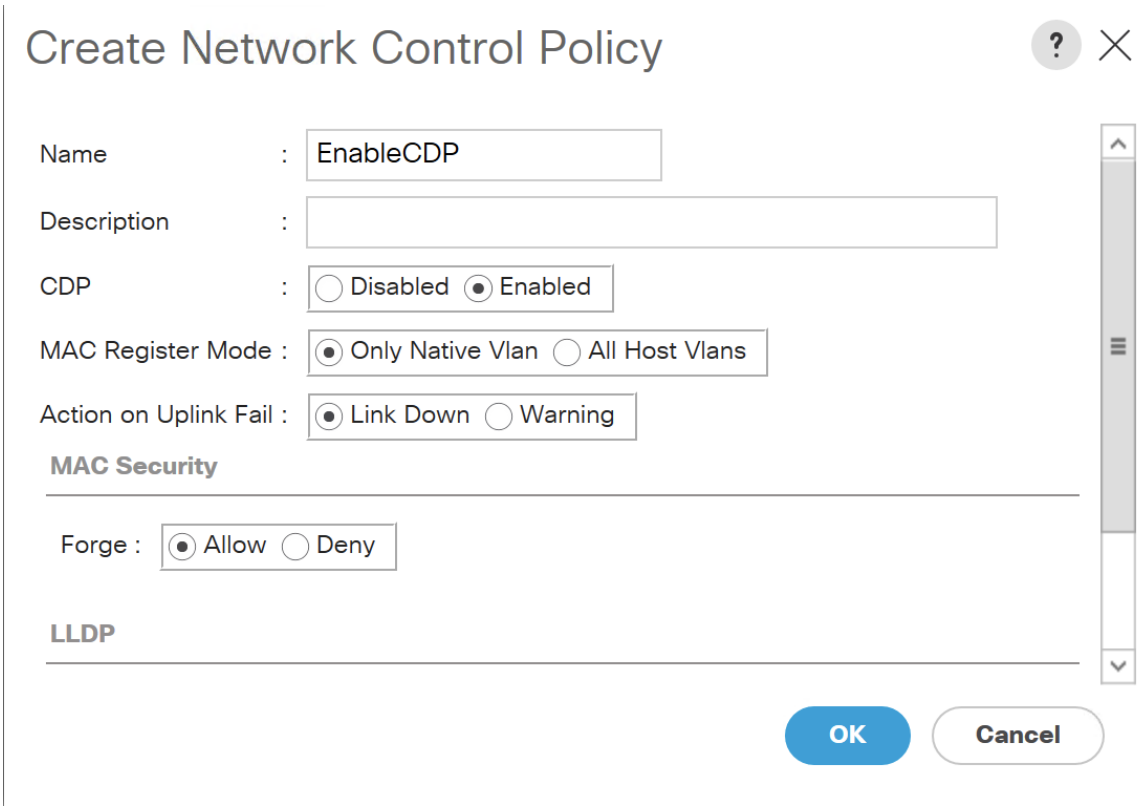
Note デフォルトでは、CDP は Cisco UCSM で無効になっています。

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。

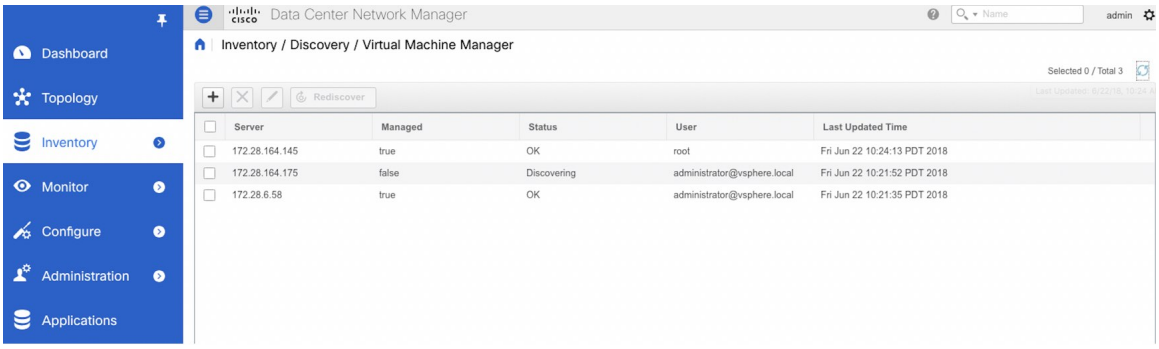
vCenter コンピューティングの視覚化の有効化

Cisco DCNM Web UI から vCenter Compute Visualization 機能を有効にするには、次の手順を実行します。

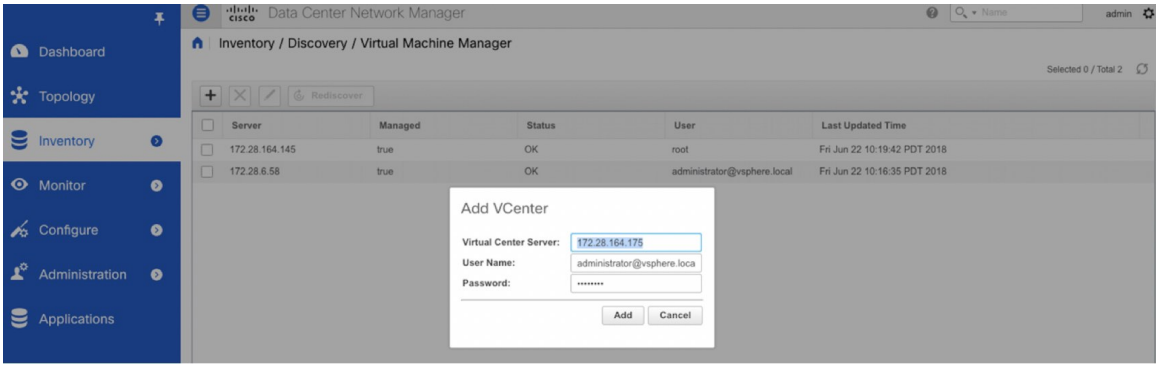
Procedure

ステップ 1 **[制御（Control）] > [管理（Management）] > [仮想マシン マネージャ（Virtual Machine Manager）]** を選択します。

コントロール（ Virtual Machine Manger Control）] > [管理（Management）] > [仮想マシン マネージャ（Virtual Machine Manager）] ウィンドウが表示されます。

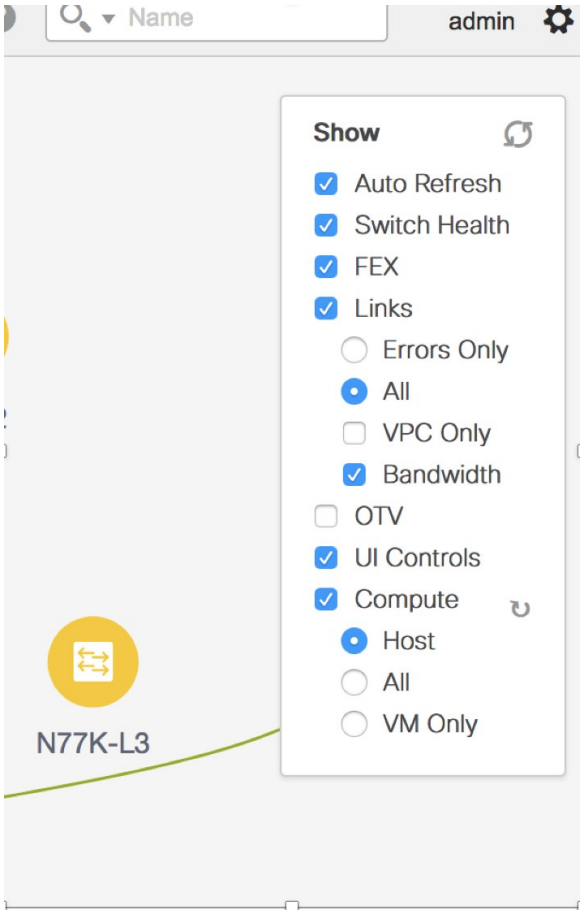


ステップ 2 **+** アイコンをクリックして、新しい **VMware vSphere vCenter** を追加します。



ステップ 3 サーバの IP アドレス、ユーザー名、およびパスワードを vCenter に入力します。 vCenter バージョン 5.5 以降が必要です。

最初の検出後、vCenterから受信した情報は適切に編成され、メインの**[トポロジ（Topology）]** ウィンドウに表示されます。**[表示（Show）]** ペインに **[コンピュート（Compute）]** というラベルの付いた追加のメニュー項目が表示されます。



Note vCenter を追加すると、イメージのアップロードが進行中であるため、コンピューティングの視覚化が完了しない状況に陥る可能性があります。**[トポロジ（Topology）]** ウィンドウに、次のメッセージが 10 分以上表示されます。

「コンピューティング視覚化データのフェッチが進行中です - しばらくお待ちください。」

[アプリケーション（Applications）] ウィンドウに移動し、VMM アプリケーションが実行されていないことを確認します。アプリケーションアイコンの左上隅にある緑色またはオレンジ色のドットで示される実行中の場合、問題は別のシナリオが原因です。それ以外の場合は、vCenter を削除し、約 15 分待ってから再度追加します。アプリケーションのステータスを確認し、DCNM タスクを続行します。

vCenter コンピューティングの視覚化の使用

Cisco DCNM Web UI から vCenter Compute Visualization 機能を使用にするには、次の手順を実行します。

Procedure

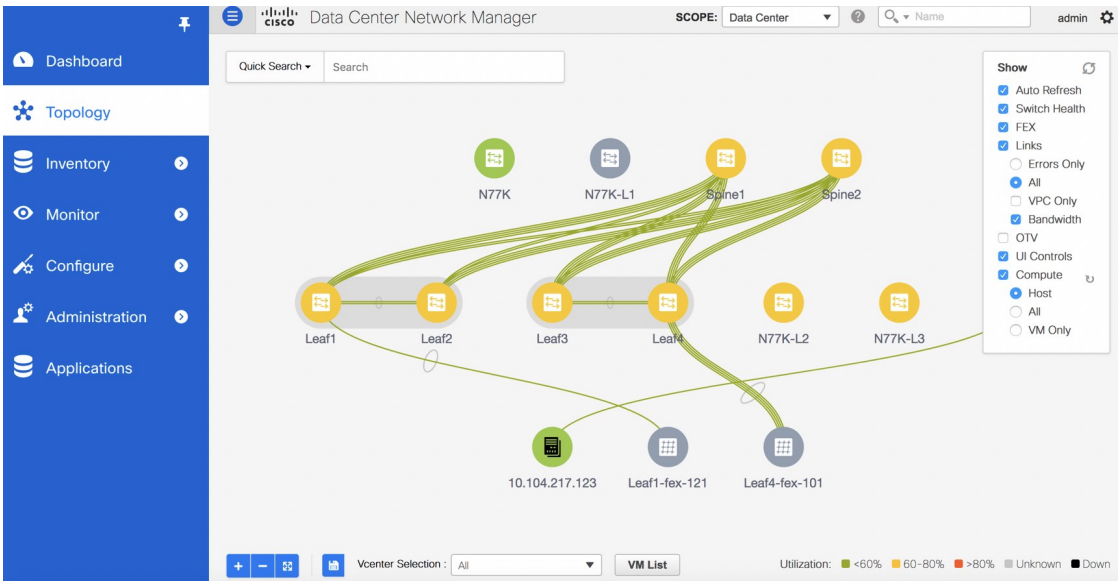
ステップ 1 **[トポロジ（Topology）]** を選択します。

ステップ 2 **[表示（Show）]** リストで **[コンピューティング（Compute）]** を選択して、コンピューティングの可視性を有効にします。

デフォルトでは、**[ホスト（Host）]**チェックボックスはオンになっています。これは、トポロジがネットワーク スイッチに接続されている VMWare vSphere ESXi ホスト（サーバー）を示していることを意味します。

コンピューティング可視化機能では、次のオプションを使用できます。

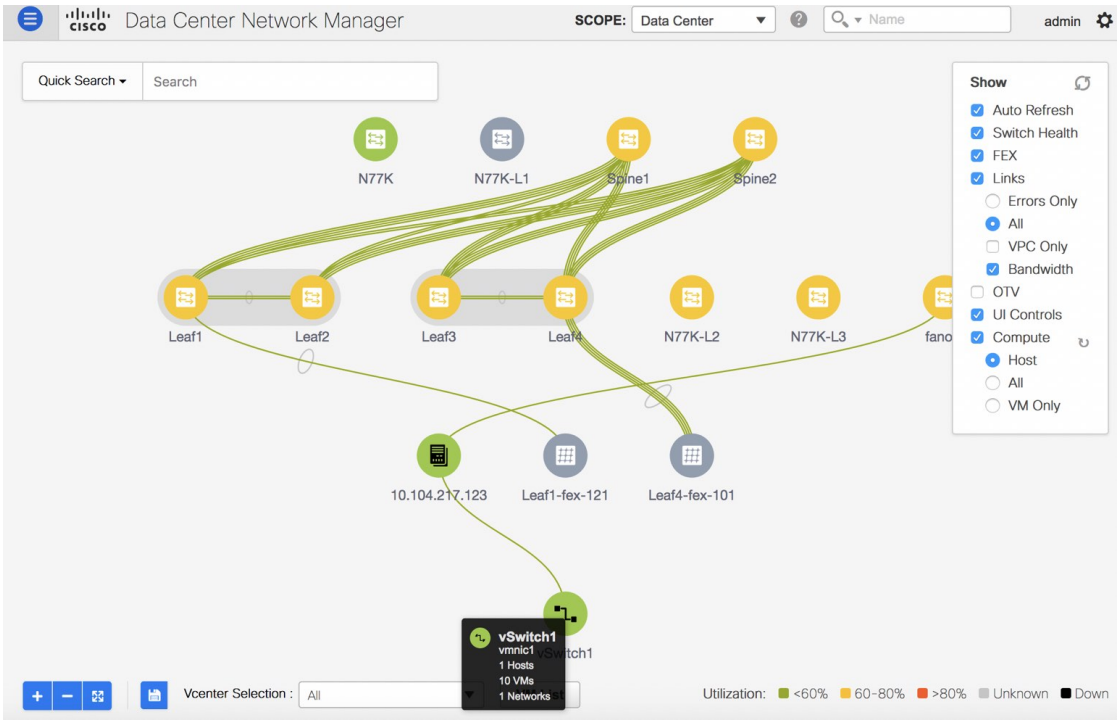
- **ホスト**
- [すべて（All）]
- **[VMのみ（VM Only）]**



[全て（All）]モードでは、ノードを拡張するのに役立つ二重矢印が表示されます。このノードをダブルクリックすると、非表示の子ノードがすべて表示されます。

ステップ 3 特定の ESXi ホストをクリックして、追加情報を表示します。

次の図に表示されている展開されたトポロジは、特定の ESXi ホストで構成されている仮想スイッチ（vSwitch と分散仮想スイッチの両方）を示しています。



ステップ 4 **[ホスト（Host）]** サブオプションから **[全て（All）]** サブオプションに変更すると、すべてのコンピューティング 技術情報が拡張されます。

[全て（All）] を選択すると、トポロジの一部であるすべてのホスト、仮想スイッチ、および仮想マシンの展開ビューが表示されます。VM の電源がオフの場合は、赤色で表示されます。それ以外の場合は、緑色で表示されます。

Note コンピューティングの視覚化が有効になっていない場合、vCenter 検索は使用できません。また、この検索は、**[全て（All）]** オプションを選択した場合にのみ使用できます。

ステップ 5 利用可能な大量の情報を参照する代わりに、特定の VM に注目します。

左上の**[検索（Search）]**フィールドにホスト名（vCenter）を入力します。文字の入力を開始すると、トポロジは一致するオブジェクトで瞬時に更新されます。

Note コンピューティング ノードを表示しているときに、**[FEX]** チェックボックスを選択していることを確認してください。そうしなければ、ホストまたはFEX の後ろのVMはぶら下がります。

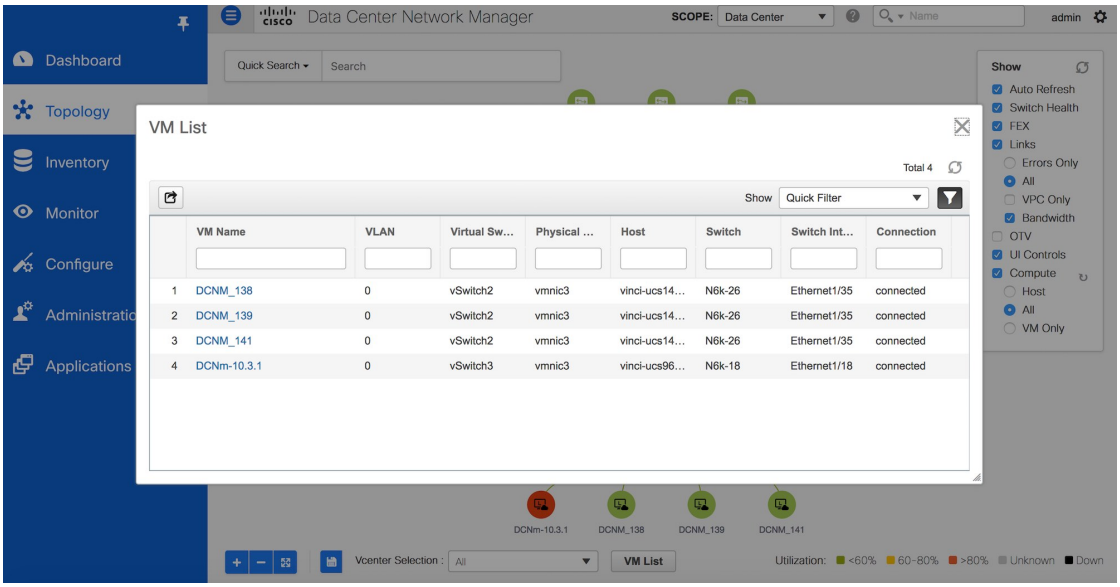
仮想マシン リストの使用

[仮想マシン リスト（Virtual Machine List）]では、仮想マシンの完全なリストを表示できます。

Procedure

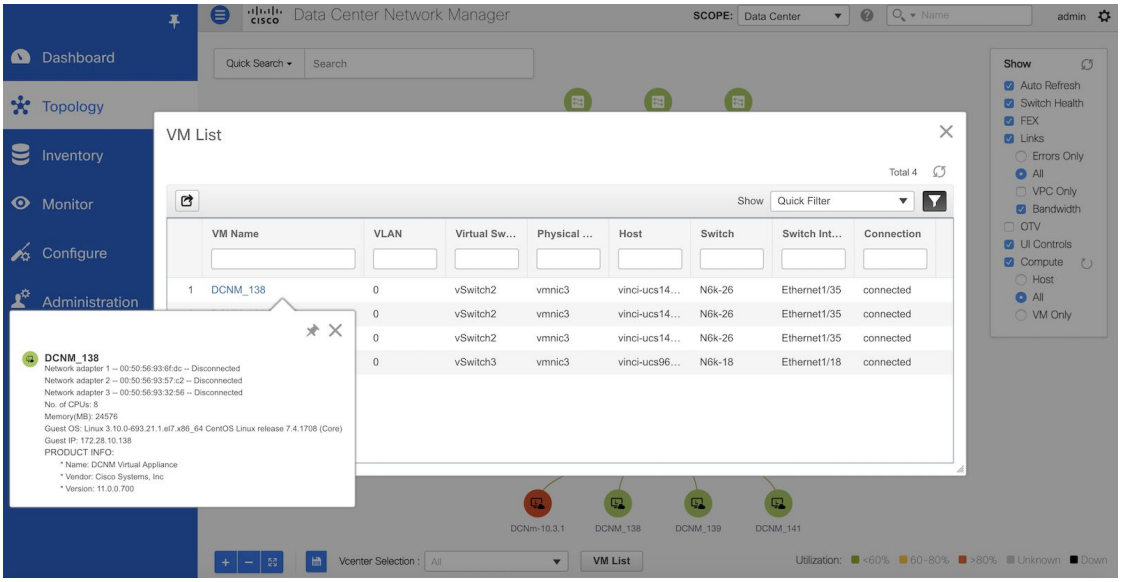
ステップ 1 **[トポロジ（Topology）]** を選択します。

ステップ 2 **[VM リスト（VM List）]**をクリックします。



[エクスポート（Export）] をクリックし、仮想マシンのリストを .csv ファイルにエクスポートします。

VM の名前をクリックして、その仮想マシンに関する追加情報を表示します。



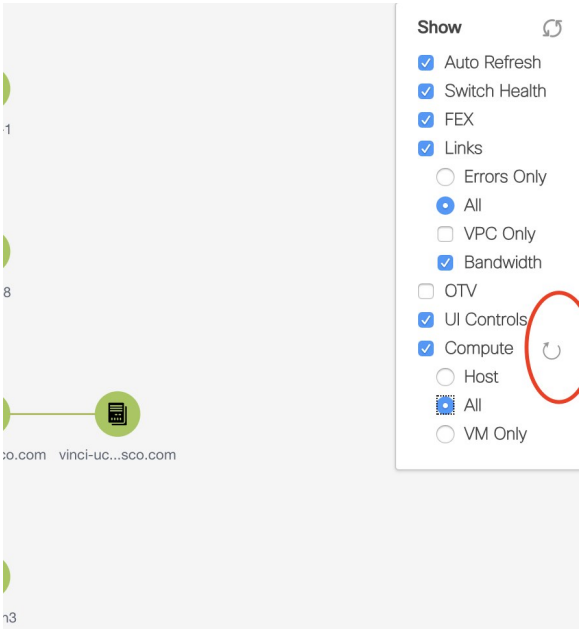
Note VM リストを.CSV ファイルにエクスポートすると、.CSV ファイルが正しく表示される場合があります。ただし、.CSV ファイルを Microsoft Excel にインポートすると、再フォーマットされる可能性があります。たとえば、VLAN 列 1-1024 が 2019 年 1 月 1 日の日付に再フォーマットされる可能性があります。したがって、.CSV ファイルをインポートするときに、列が Microsoft Excel で正しくフォーマットされていることを確認してください。

仮想マシンの再同期

Procedure

ステップ 1 **[トポロジ（Topology）]** を選択します。

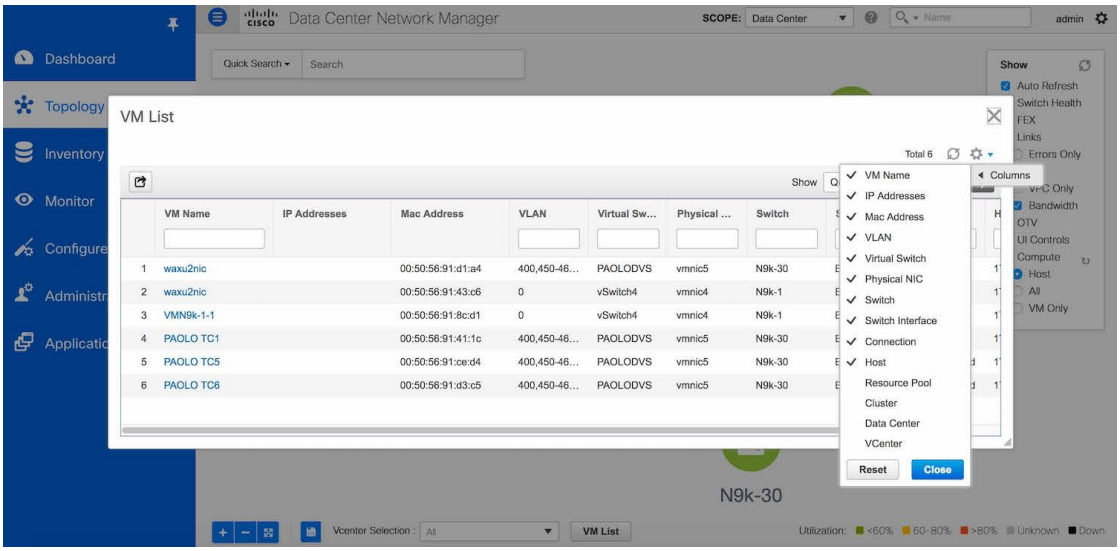
ステップ 2 **[コンピューティング（Compute）]** の横にある **[vCenter の再同期（Resync vCenters）]** アイコンをクリックします。



仮想マシン リストでの列の選択

Procedure

ステップ 1 **[VM リスト（VM List）]** ウィンドウで、歯車アイコンのドロップダウンリストの下にある **[列（Columns）]** をクリックします。

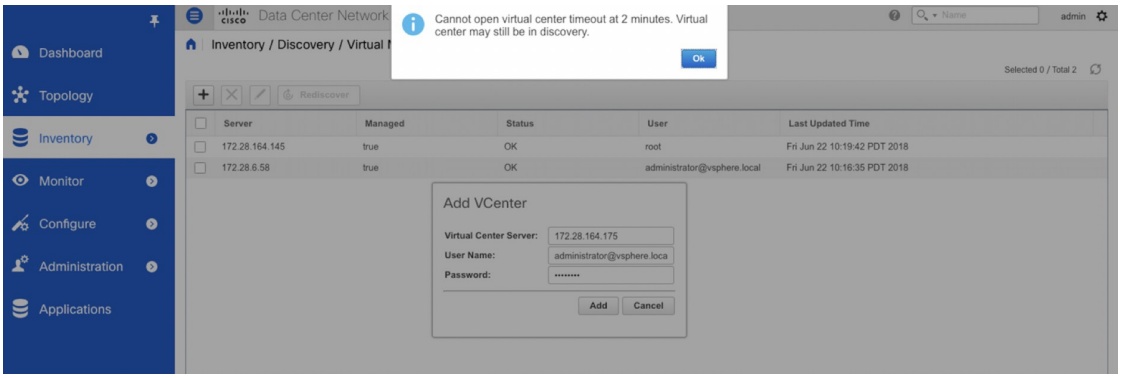


ステップ 2 VM リストテーブルで表示する列を選択します。追加の列を選択した場合は、**[vCenter の再同期（Resync vCenters）]** アイコンをクリックして更新し、新しい列を表示します。

vCenter との定期的な再同期はバックエンドで行われます。再同期タイマー値を設定するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択します。**[#GENERAL] > [DATA SOURCES VMWARE]** セクションで、**[vmm.resync.timer]** フィールドにタイマー値を指定します。デフォルト値は 60（60 分）で、この値は増減できます。60 分未満の値を入力すると、この機能は無効になります。

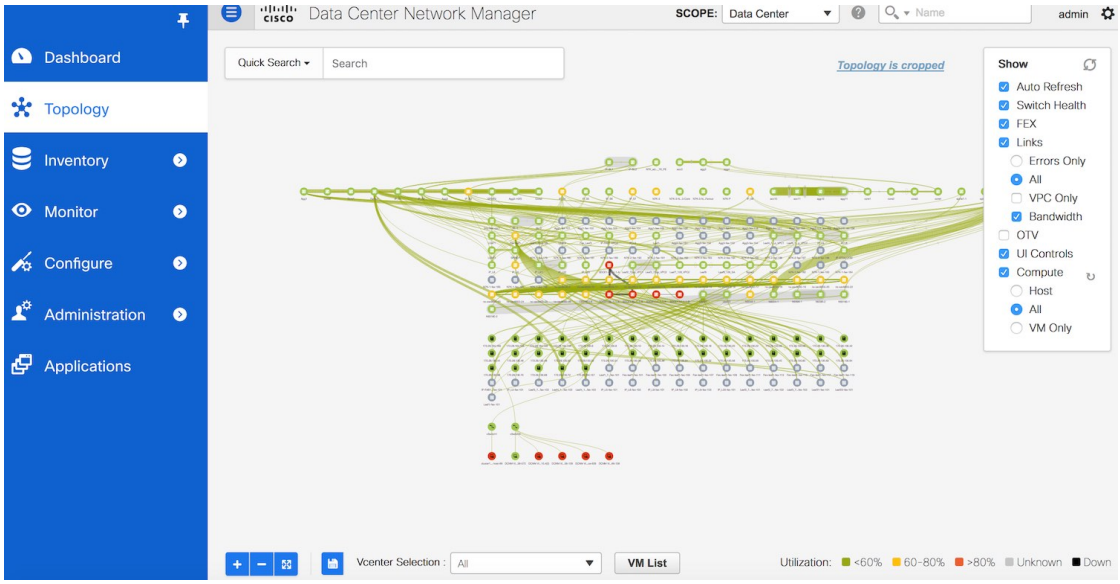
vCenter コンピューティング仮想化のトラブルシューティング

vCenter がタイムアウトすると、次のエラー ウィンドウが表示されます。このエラーは、vCenter の検出の進行中に発生することがあります。



スケール モードでのトポロジの表示

次のウィンドウは、トポロジで約 200 台のデバイスが使用可能になった後に **[トポロジ（Topology）]** ウィンドウがどのように表示されるかを示しています。トポロジ グラフは、拡張に合わせて縮小されていることに注意してください。



コンテナ オーケストレータ

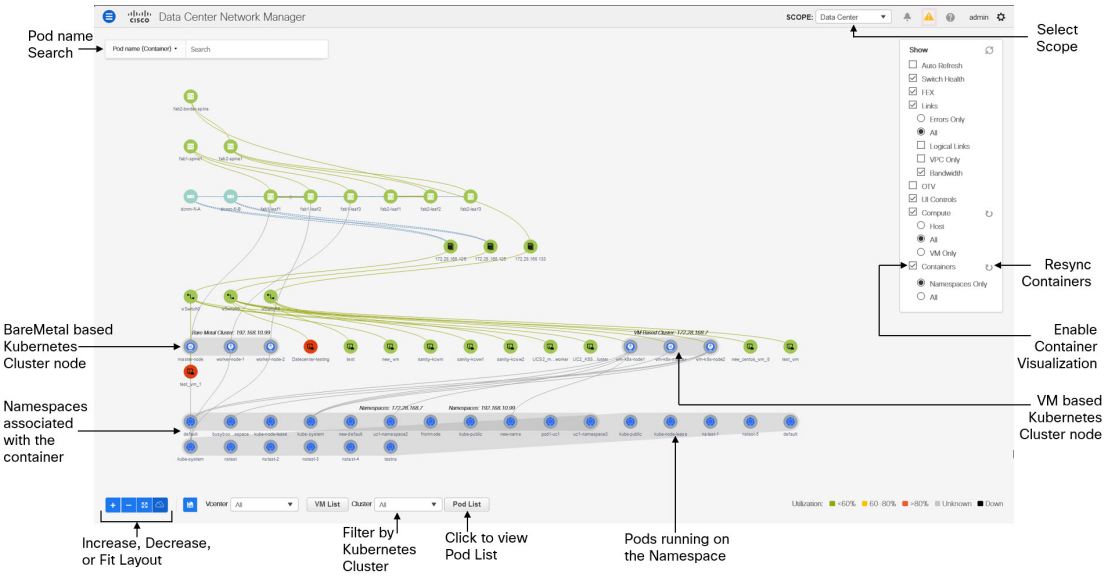
リリース 11.3(1) 以降、Cisco DCNM ではコンテナ オーケストレータを構成できます。この機能により、Kubernetes クラスタを Cisco DCNM のコンテナ オーケストレータとして視覚化できます。

コンテナ オーケストレータの視覚化機能を有効にする前に、Cisco DCNM で VMM が正常に構成されていることを確認してください。ただし、ベアメタル ベース Kubernetes クラスタには VMM は必要ありません。

コンテナの視覚化は、最初の Kubernetes クラスタがコンテナ オーケストレータに追加された後にのみ開始されます。Kubernetes から受信した情報は適切に編成され、メインの [トポロジ（Topology）] ウィンドウに表示されます。[表示（Show）] ペインに、**[コンテナ（Containers）]** というラベルの付いた追加のメニュー項目が表示されます。

いつでも、**[トポロジTopology（）]** 内の任意のコンポーネントをクリックして、選択したコンポーネントとファブリック間のすべてのネットワーク パスを表示します。

次の画像は、Cisco DCNM でのコンテナ オーケストレータの視覚化のさまざまな機能をすべて詳しく示しています。



次の重要なオプションに基づいて、コンテナ オーケストレータの視覚化を表示できます。

- **更新**：このアイコンをクリックして、トポロジ データを更新します。
- **自動更新**：このチェックボックスを選択すると、トポロジが自動的に更新されます。
- **スイッチの健全性**：このチェックボックスを選択して、スイッチの健全性ステータスを表示します。
- **リンク**：トポロジ内のリンクを表示するには、このチェック ボックスをオンにします。次のオプションを使用できます。
  - **エラーのみ**：エラーのあるリンクのみを表示するには、このラジオボタンをクリックします。
  - **すべて**：このラジオボタンをクリックして、トポロジ内のすべてのリンクを表示します。
  - **VPC のみ**：vPC ピア リンクと vPC のみを表示するには、このチェックボックスをオンにします。
  - **帯域幅**：リンクによって消費される帯域幅に基づいて色分けを表示するには、このチェック ボックスをオンにします。
- **UI 制御**：このチェック ボックスをオンにすると、[トポロジ（Topology）] ウィンドウにさまざまなコントロールがすべて表示されます。
- **コンピューティング**：チェックボックスをオンにして、VCenter Compute Visualization を有効にします。
  - **[ホスト（Host）]** を選択して、コンピューティング ホストを表示します。

- **[すべて（All）]** を選択して、すべてのコンピュータ ノードを表示します。
- VM のみを表示するには、**[VM のみ（VM Only）]** を選択します。

[表示（Show）]パネルの[コンピューティング（Compute）]の横にある **[再同期（Resync）]** アイコンをクリックして、トポロジを再同期するには、再同期します。

- **コンテナ**：チェックボックスをオンにすると、コンテナが表示されます。
  - デフォルトでは、**[名前スペース（Namespaces only）]** が選択されており、Kubernetes クラスタ内の名前空間のみが表示されます。
  - 名前スペースに関連付けられた名前空間とポッドの両方を表示するには、**[すべて（All）]** を選択します。
- **再同期**：[表示（Show）]パネルの[コンテナ（Containers）]の横にある **[再同期（Resync）]** アイコンをクリックして、トポロジを再同期することもできます。

  コンピューティングの再同期が完了した後、コンテナを再同期する前に数分間待つことをお勧めします。

Container Orchestrator の可視化での UI コントロールの使用

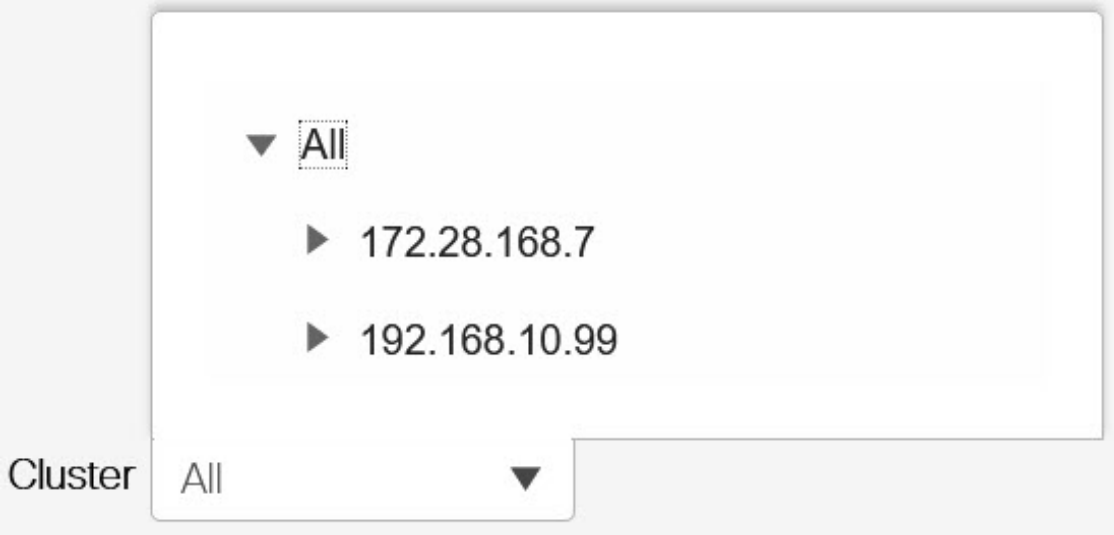
表示パネルでコンテナーを有効にすると、クラスタ ノードが名前空間の関連付けと共に表示されます。VM ベースの クーベネティス クラスタの場合、コンピューティングの選択 (ホスト、VM のみ、またはすべて) に基づいて、トポロジにクーベネティス クラスタと関連する名前空間が表示されます。ベアメタル ベースのクーベネティス クラスタの場合、コンピューティングの選択は必要ありません。

 アイコンはクーベネティス ノードを示しています。クーベネティスのインストール タイプと IP アドレスがクーベネティス クラスタに表示されます。  アイコンは Kubernetes クラスタの名前スペースを示し、  アイコンは名前スペースに関連付けられたポッドを示します。

Kubernetes クラスタには、2 つのタイプがあります。

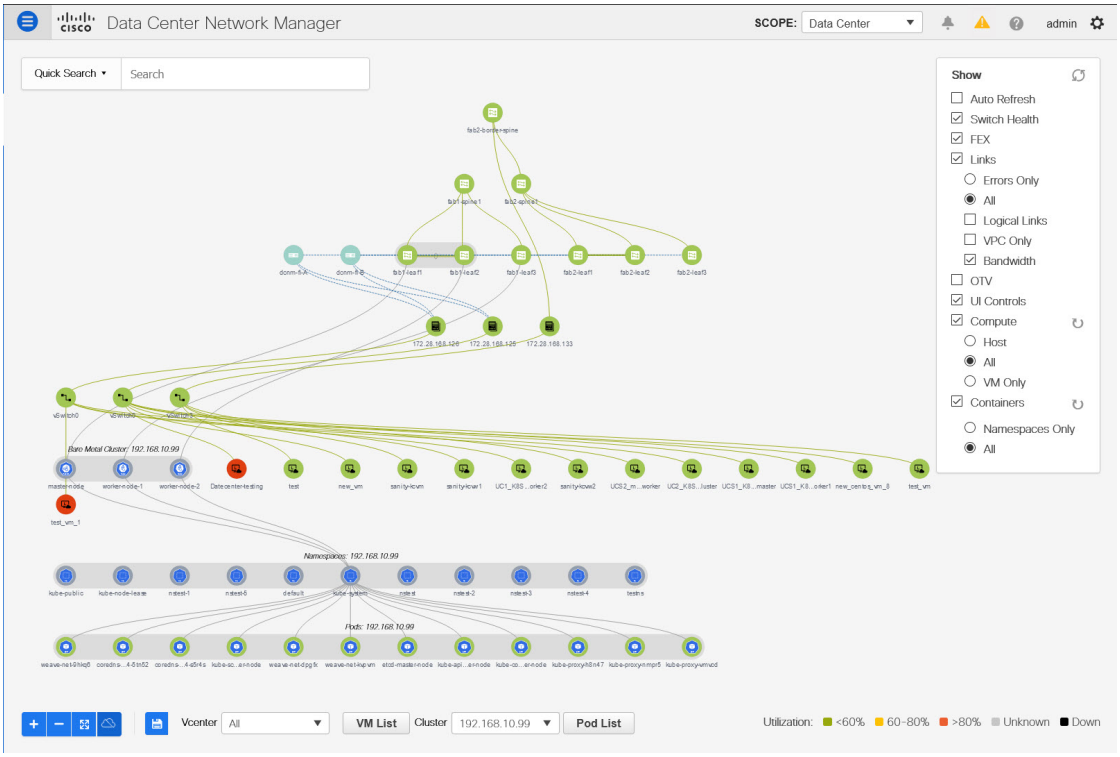
- VM ベースの クーベネティス クラスタは、VCenter 上でホストされます。
- スイッチに直接接続されているベアメタルにインストールされた クーベネティス。

[UI 制御（UI Controls）] の [クラスタの選択（Cluster Selection）] ドロップダウン リストから、1 つのクラスタを選択して、そのクラスタのコンテナの視覚化を表示できます。



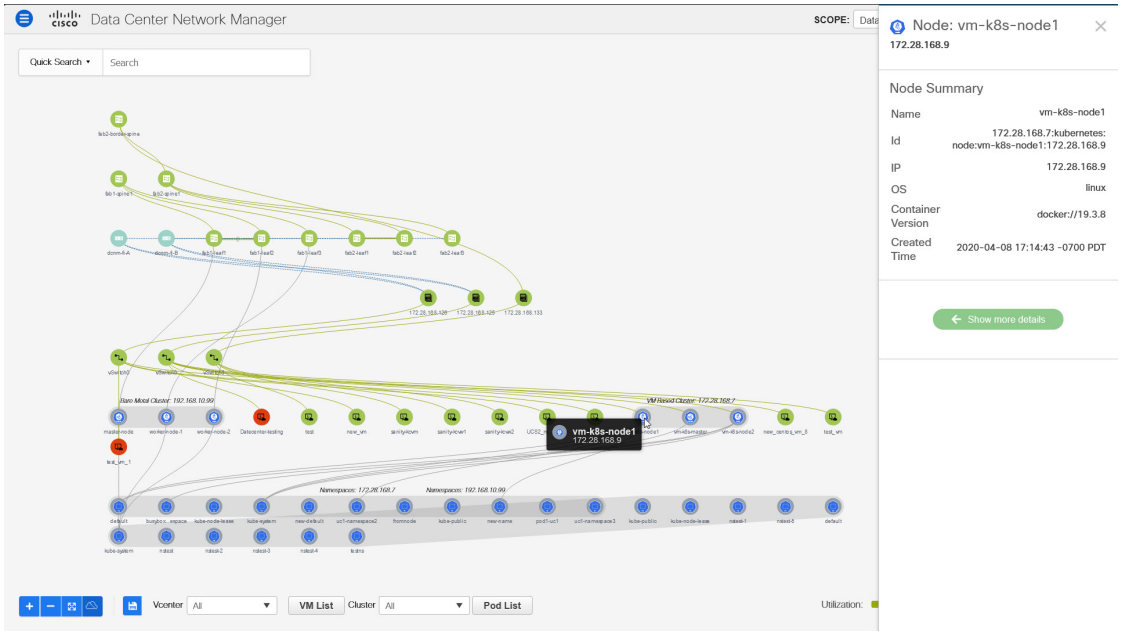
トポロジには、選択したクラスタのコンテナの可視化のみが表示されるようになりました。他の クーベネティス クラスタ アイコンが VM アイコンに変わることに注意してください。

（注） コンピューティング ノードを表示しているときに、[FEX] チェックボックスを選択していることを確認してください。そうしなければ、ホストまたはFEXの後ろのVMはぶら下がります。



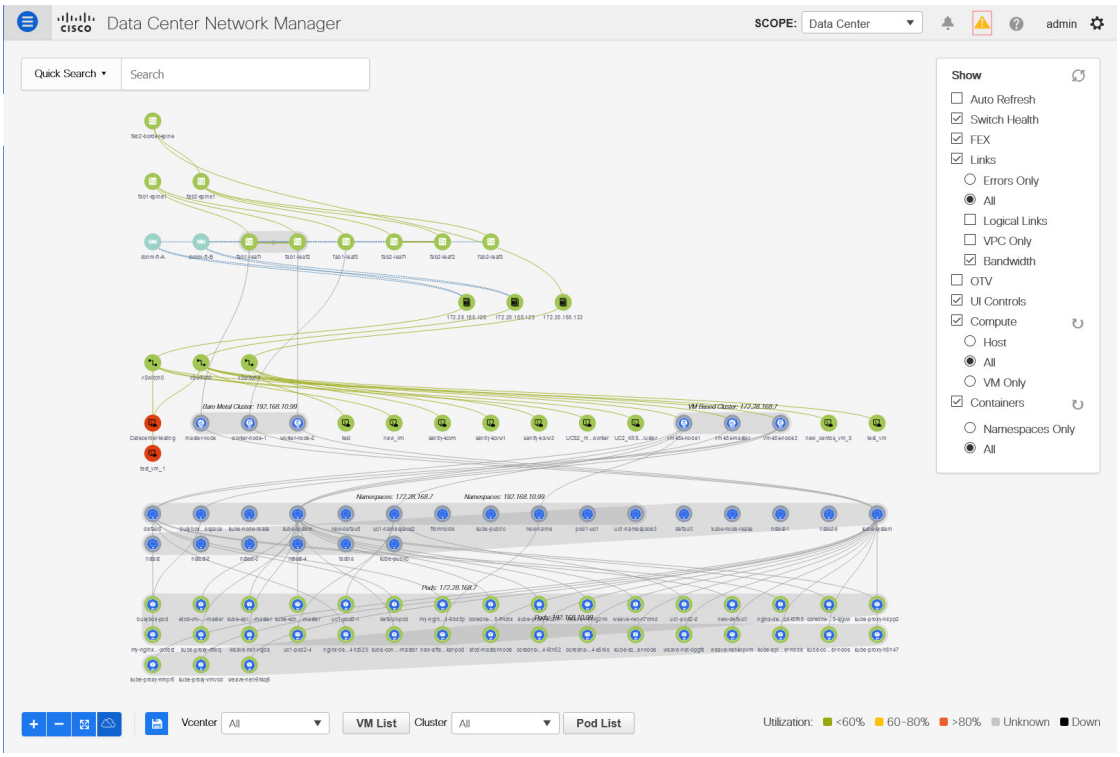
ノードをダブルクリックして、ノードに関する詳細を表示します。ノードの概要を示すサイドパネルが表示されます。**[詳細を表示（Show More Details）]** をクリックして、選択したノードのメタデータ、仕様、およびステータス情報を表示します。

メタデータ タブは、Show More Details ノードまたはポッド名で構成されます。仕様タブには、ノードまたはポッドの望ましいデザイン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。



名前スペースをダブルクリックして、そこで実行されているポッドを表示します。名前スペースを再度ダブルクリックして、名前スペースに関連付けられたポッドを折りたたみます。

表示パネルのコンテナで **[すべて（All）]** を選択して、すべての名前スペースで実行されているすべてのポッドを表示します。200 を超えるポッドがある場合、レンダリングの遅延を避けるために、トポロジのトリミングされた新しいビューが、クラスタごとに 5 つの名前スペース、名前スペースごとに 5 つのポッドで表示されます。トポロジが切り取られたことを示すインジケータが表示されます。完全なトポロジの詳細を表示するには、ポッドリストを表示する必要があります。今後の分析のため、ポッド リスト データをエクスポートすることもできます。



ポッドをダブルクリックして、ポッドに関する詳細を表示します。ポッドの概要を示すサイドパネルが表示されます。**[詳細を表示（Show More Details）]** をクリックして、接続された名前スペース専用の選択したポッドのメタデータ、仕様、およびステータス情報を表示します。

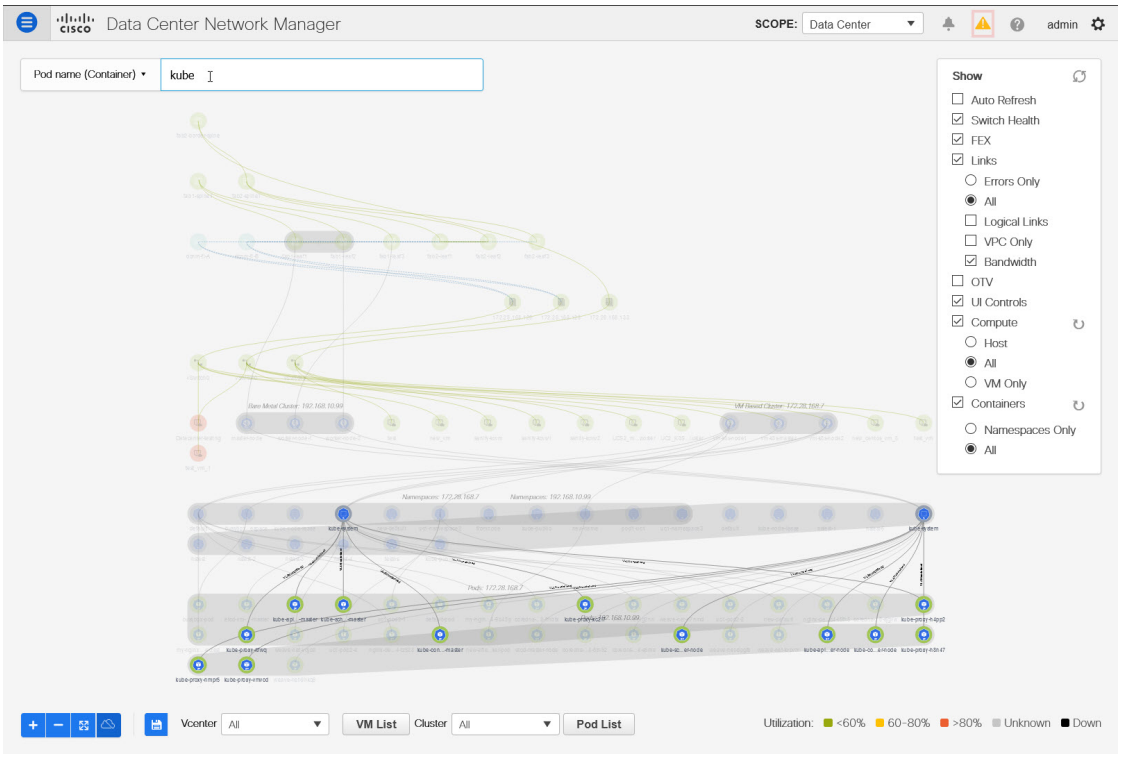
（注） コンテナ ノードを表示しているときに、**FEX** チェックボックスを選択していることを確認してください。そうしなければ、ホストまたはFEX の後ろのVMはぶら下がります。

ポッドリストをクリックして選択したクラスタで実行されているすべてのポッドに関する詳細を表示できます。クラスタの選択が [すべて（All）] の場合、トポロジ内のすべてのクラスタで実行されているすべてのポッドが表示されます。今後の分析のため、ポッド リスト データをエクスポートすることもできます。

ポッド名 (コンテナ) トポロジ検索01-11-2022 21:46

トポロジ検索を使用してポッドを見つけることができます。トポロジ**[検索（Search）]** ドロップダウン リストから、**[ポッド名（コンテナ）（Pod name (Container)）]** 検索タイプを選択します。[検索（Search）] フィールドに、ポッド名を入力します。接続先のポッドと名前スペースがトポロジで強調表示されます。

（注） ポッドの正確な名前を入力しない限り、ポッド検索は部分的です。検索文字列で始まるすべてのポッドが強調表示されます。



OpenStack ワークロードの可視性

通常、データセンターの展開は、ベアメタルサーバやVMなどのさまざまな種類のワークロードで構成されます。あらゆるトラブルシューティングは、ワークロードが存在する複数のサーバの場所から始まり、そのワークロードにサービスを提供しているコンピューティング、ストレージ、およびネットワーク 技術情報へと調査が続きます。

Cisco DCNM リリース 11.5(1) から、OpenStack クラスタを監視するのに役立つ OpenStack プラグインが DCNM によって提供されます。物理ネットワーク接続と仮想化されたワークロードに関する可視性を得て、データセンターのコンテキスト内でVMネットワーキング固有の問題をデバッグできます。

ガイドライン

- DCNM アプリケーション カタログから OpenStack アプリケーションを開始または停止することはできません。OpenStack アプリケーションは、最初の OpenStack クラスタの追加後に起動します。DCNM OpenStack インベントリから最後の OpenStack クラスタ インスタンスを削除すると、OpenStack アプリケーションが停止します。OpenStack クラスタ インスタンスを途中で削除しても、OpenStack プラグイン アプリケーションの実行には影響しません。
- OpenStack アプリケーションの自動再同期機能に基づいて、設定された間隔でクラスタから情報を取得します。

OpenStack トポロジ拡張

- 100 を超える OpenStack VM がある場合、ホストごとに 5 つの VM のみが表示され、残りは切り捨てられてメッセージが表示されます。メッセージには、ホストと VM の合計数が表示されます。
- OpenStack プラグインは、最大 4 つの OpenStack クラスタをモニタできます。
- OpenStack プラグインは、4 つのクラスタ全体で最大 1000 個の VM、つまりクラスタあたり 250 個の VM をモニタできます。

OpenStack の通知およびトリガ

- 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 DCNM に自動的に反映されます。

OpenStack ビジュアライザを使用

始める前に

DCNM に OpenStack クラスタを追加してください。詳細については、OpenStack ビジュアライザ （436 ページ）を参照してください。

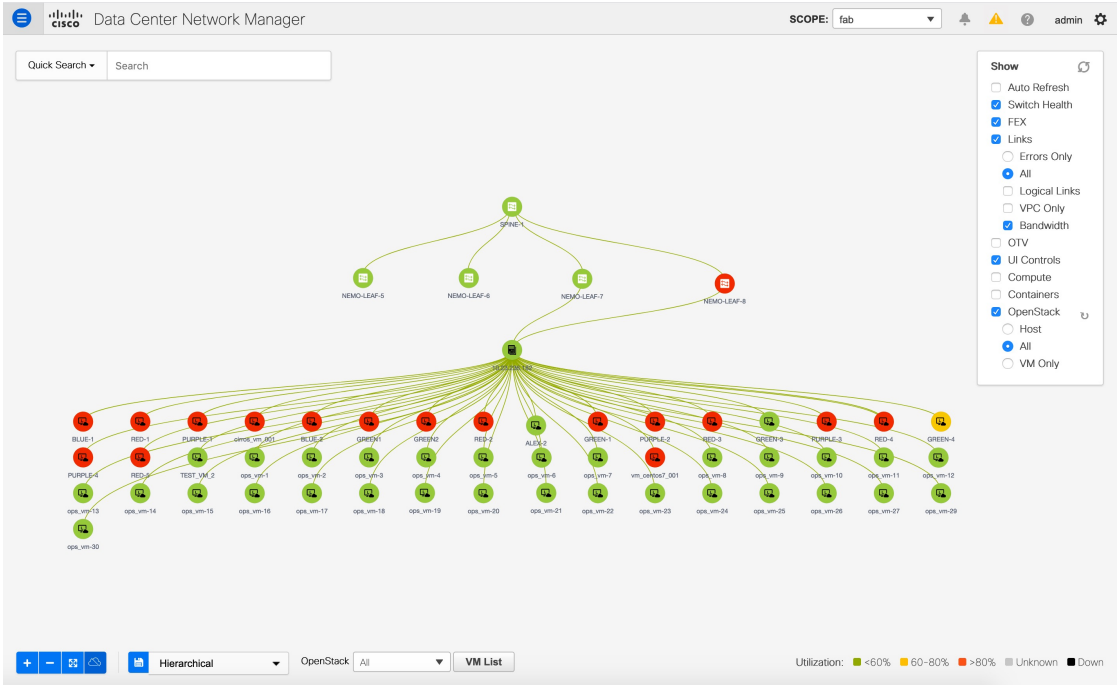
手順

ステップ 1 **[トポロジ（Topology）]** に移動します。

ステップ 2 **[表示（Show）]** パネルで、**[OpenStack]** チェックボックスを選択して、クラスタ内の VM を表示せずに、ファブリックに接続している OpenStack クラスタ ノードのみを表示します。これはホストのみのビューです。ノードは、クラスタに従ってグループ化されて表示されます。OpenStack では、次のオプションを使用できます。

- **[ホスト（Host）]** を選択して、OpenStack クラスタ ホストのみを表示します。
- **[すべて（All）]** を選択して、すべての OpenStack クラスタ ノードと、クラスタ ノードでホストされている VM インスタンスを表示します。
- **[VM のみ（VM Only）]** を選択して、OpenStack VM インスタンスのみを表示します。

OpenStack の横にある**再同期**アイコンをクリックして、すべてのクラスタを再同期します。このアイコンは、再同期操作が完了するまで無効になっています。



各 VM ノードの色分けは、その状態に対応しています。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。
- 黄色：要素が一時停止および中断されていることを示します。
- 赤：要素が停止またはシャットダウンされていることを示します。

ステップ 3 **[OpenStack]** ドロップダウン リストから **[すべて（All）]** を選択して、存在するすべての OpenStack クラスタからすべての OpenStack クラスタ ノードを表示します。

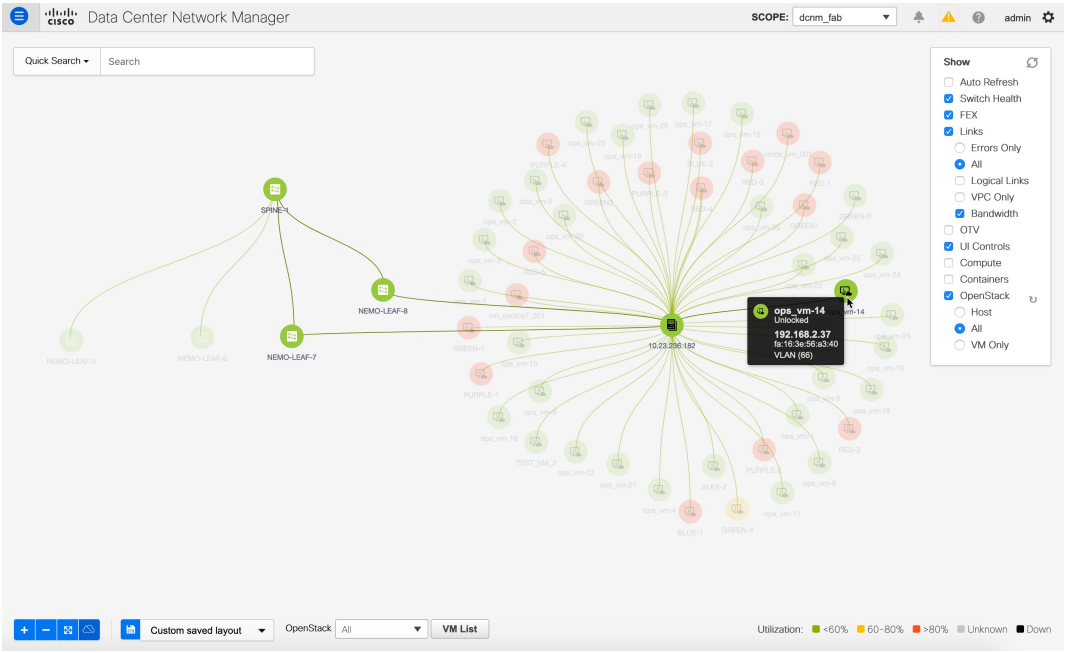
このドロップダウン リストから特定の OpenStack クラスタの IP アドレスを選択して、選択した OpenStack クラスタからすべての OpenStack クラスタ ノードを表示します。単一のクラスタは、そのノードの灰色のグループで識別されることに注意してください。

ステップ 4 **[範囲（SCOPE）]** ドロップダウン リストから、ファブリックを選択します。このアクションにより、選択したファブリックに接続されている場合、OpenStack クラスタが表示されます。

ステップ 5 トポロジにカーソルを合わせると、特定の OpenStack リソースの詳細を示すツールチップ情報ポップアップが表示されます。このアクションは、2 つの技術情報を接続するエッジにも適用できます。次の詳細情報が表示されます。

- OpenStack クラスタ ホストのツールチップ情報には、ホスト IP とバージョンが含まれています。
- OpenStack VM のツールチップ情報には、VM 名、VM ステータス: Locked/Unlocked、VM IP、MAC、および VLAN が表示されます。

- ホストと VM 間のリンクにカーソルをホバーさせると、ホストと VM の IP アドレス、MAC アドレスの詳細などの情報を取得できます。
- 技術情報をクリックしたままにすると、それに接続しているすべてのエッジが表示されます。



VM を OpenStack クラスタで表示する

手順

ステップ 1 VM をダブルクリックして、名前、IP、MAC、メモリ、セグメント タイプ、ロックされているかどうか、電源、状態、vCPU 情報などの要約された OpenStack VM データを表示します。**[詳細を表示（Show more details）]** をクリックして、VM の動作状態、仕様、メタ データなどの情報を表示します。

（注） VM は、ホストに接続する 2 つのインターフェイスを持つことができます。この場合、VM は、2 つの異なる IP アドレスを持つホスト上の 2 つの異なるネットワークに接続しています。

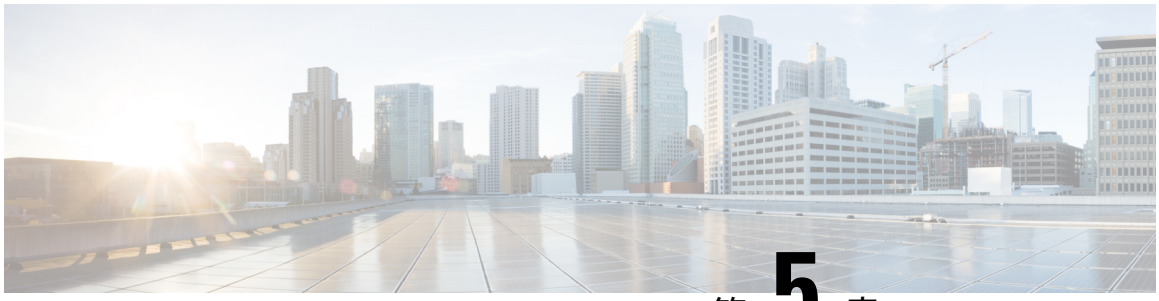
ステップ 2 **[VM リスト（VM List）]** をクリックして、クラスタ トポロジの表形式のビューを表示します。

[VM リスト（OpenStack）（VM List(OpenStack)）] ウィンドウには、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 に接続されているホスト名
- 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
- VLAN セグメント タイプ
- VM の電源状態とステータス
- 割り当て済みメモリと vCPU

各列の下にある検索フィールドを使用して、VM を検索およびフィルタリングできます。.CSV ファイルにこのデータを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。



第 5 章

Control

この章は次のトピックで構成されています。

ファブリック

このマニュアルでは、次の用語を使用しています。

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

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

ここでは、次の内容について説明します。

VXLAN BGP EVPN ファブリックのプロビジョニング

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

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

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

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

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

ファブリックの作成、編集、および削除：

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

新しいスイッチでのデバイス検出とプロビジョニングの起動設定：

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

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

アンダーレイのプロビジョニング：

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

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

オーバーレイ ネットワークのプロビジョニング

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

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

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

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

VXLAN BGP EVPN ファブリック プロビジョニングのガイドライン

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

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

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

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

  スイッチのアイコンを右クリックして、**[構成の展開（Deploy Config）]** オプションを選択すれば、スイッチごとの構成を展開できます。このオプションは、スイッチのローカル操作です。つまり、スイッチの予想される構成またはインテントが現在の実行構成に対して評価され、構成のコンプライアンス チェックが実行されて、スイッチが **In-Sync** または **Out-of-Sync** ステータスを取得します。スイッチが同期していない場合、ユーザには、その特定のスイッチで実行されているすべての設定のプレビューが提供されます。これらの設定は、それぞれのスイッチに対してユーザが定義した意図とは異なります。
- 永続的な設定の差分は、コマンドライン**system nve infra-vlan** *int* **force**で確認できます。永続的な差分は、スイッチにフリーフォームの設定を介してこのコマンドを展開すると、発生します。スイッチは展開時に **force** キーワードを必要としますが、DCNM 内でスイッチ

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

DCNM のインテントには次の行が含まれます：

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

実行設定には次の行が含まれいます：

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

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

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

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

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

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

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

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

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

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

  元の **tcam** コマンドが上書きされていることがわかります。

新規 VXLAN BGP EVPN ファブリックの作成

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

この手順には、IPv4 アンダーレイの説明が含まれています。IPv6 アンダーレイについては、Easy Fabric の IPv6 アンダーレイ サポート, on page 134 を参照してください。

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

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

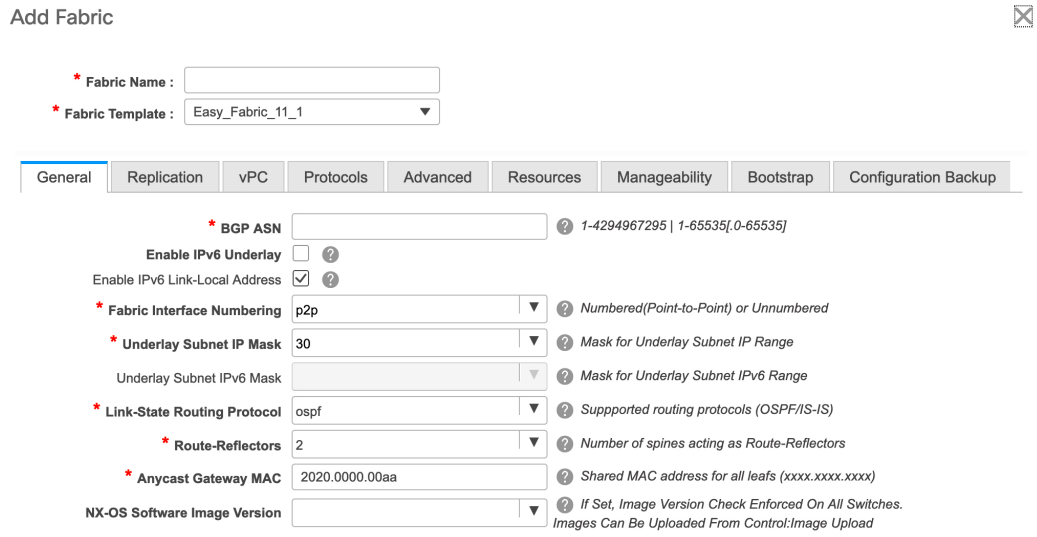
   スタンドアロンまたはメンバーファブリックには、Switch_Fabric（タイプフィールド）、AS 番号（ASN フィールド）、および複製モード（複製モード フィールド）が含まれます。

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

   フィールドについて説明します。

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

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



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

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

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

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

   [IPv6 アンダーレイの有効化（Enable IPv6 Underlay）]：IPv6 アンダーレイ機能を有効にします。詳細については、Easy Fabric の IPv6 アンダーレイ サポート, on page 134を参照してください。

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

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

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

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

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

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

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

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

   a. ドロップダウンボックスの値を 2 に変更します。

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

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

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

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

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

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

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

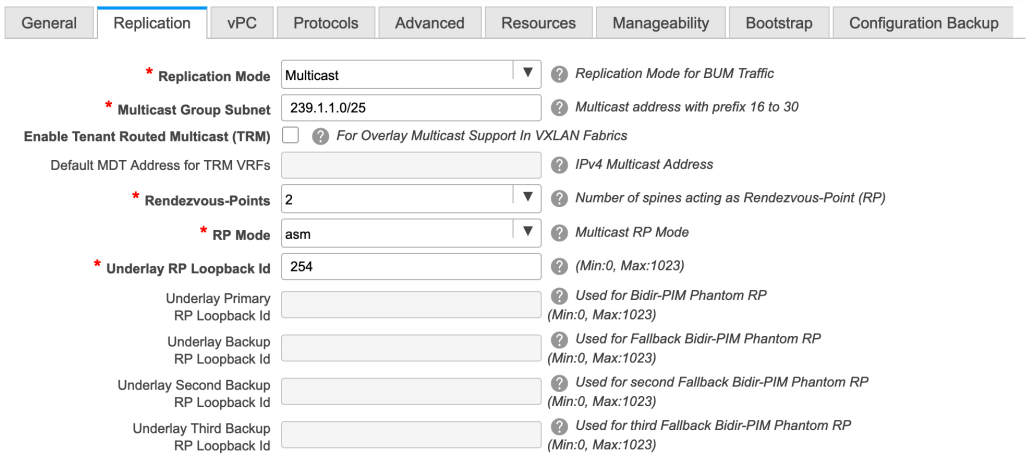
[エニーキャスト ゲートウェイ MAC（Anycast Gateway MAC）]：エニーキャスト ゲートウェイ MAC アドレスを指定します。

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

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

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

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



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

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

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

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

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

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

詳細については、テナント ルーテッド マルチキャストの概要, on page 234を参照してください。

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

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

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

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

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

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

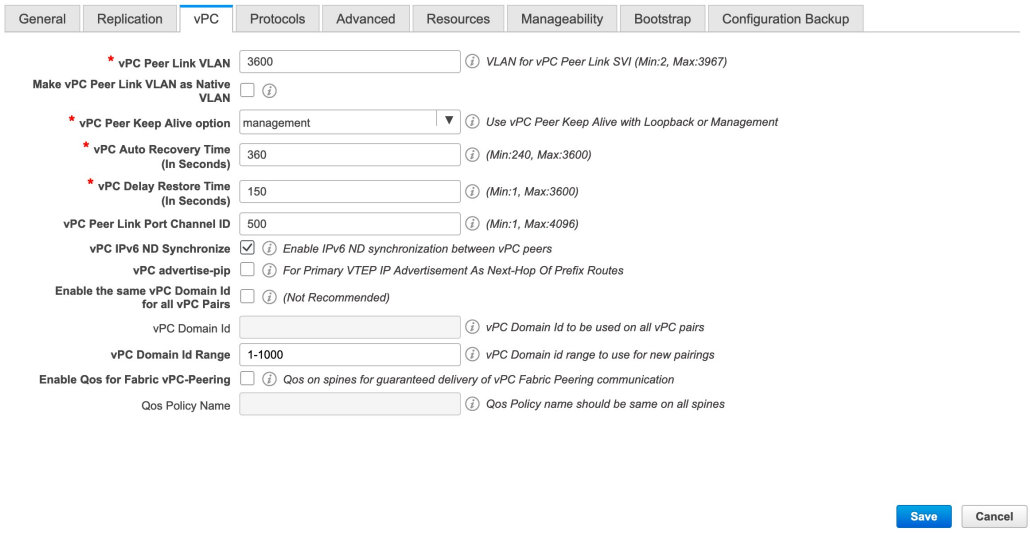
次の 2 つのフィールドは、レプリケーションのマルチキャスト モードとして [BIDIR-PIM] を選択した場合に有効になります。

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

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

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

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



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

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

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

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

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

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

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

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

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

特定の vPC でアドバタイズ PIP 機能をイネーブルにすることもできます。詳細については、vPC で PIP をアドバタイズする, on page 286を参照してください。

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

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

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

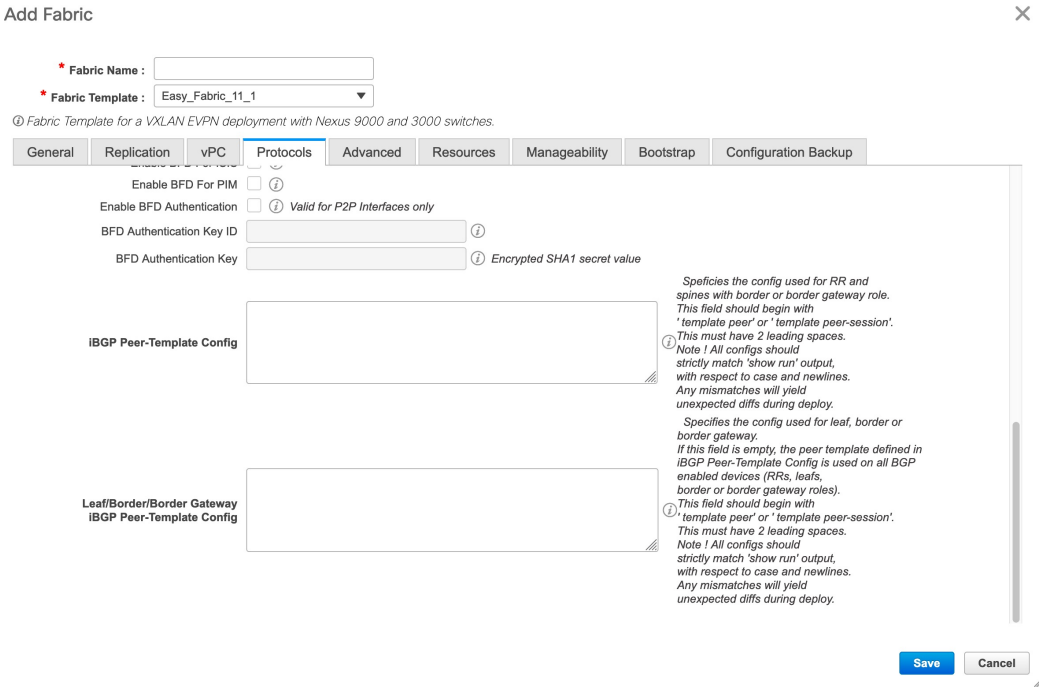
[vPC ドメイン ID の範囲（vPC Domain Id Range）]：新しいペアリングに使用する vPC ドメイン ID の範囲を指定します。

[ファブリック vPC ピアリングの QoS を有効にする（Enable QoS for Fabric vPC-Peering）]：スパインの QoS を有効にして、vPC ファブリック ピアリング通信の配信を保証します。詳細については、ファブリック vPC ピアリングの QoS, on page 277を参照してください。

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```
feature bfd
```

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

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

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

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

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

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

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

BFD グローバル ポリシーの例を次に示します。

```
router ospf <ospf tag>
   bfd

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

ip pim bfd

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

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

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

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

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

BFD 認証パラメータを取得する方法については、暗号化された BFD 認証キーの取得, on page 300 を参照してください。

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

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

構成例では、パスワード 3 の後に 3DES パスワードが表示されます。

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

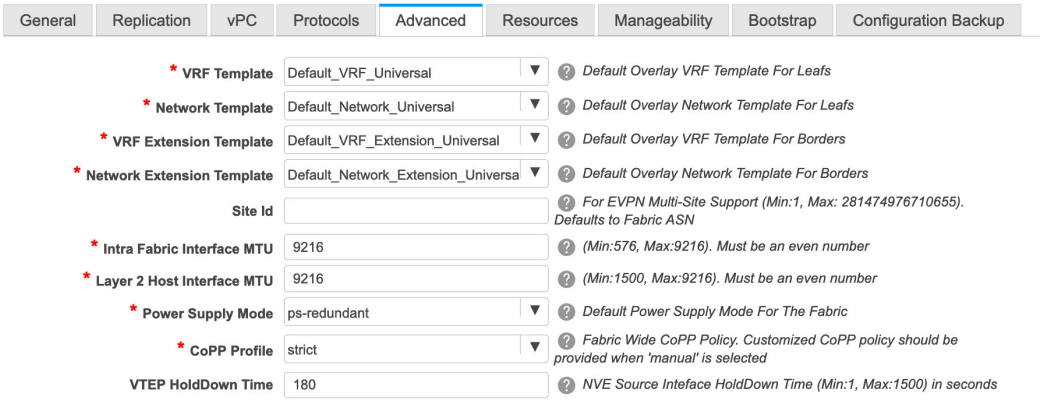
Cisco DCNM リリース 11.3(1) までは、リーフまたはボーダー ロール デバイスの iBGP 定義の iBGP ピア テンプレートと BGP RR は同じでした。DCNM リリース 11.4(1) 以降、次のフィールドを使用してさまざまな構成を指定できます。

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

  10.4(2) で作成された構成プロファイルベースのオーバーレイ

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[精密時間プロトコル（PTP）の有効化（Enable Precision Time Protocol（PTP））]：ファブリック全体で PTP を有効にします。このチェックボックスをオンにすると、PTP がグローバルに有効になり、コアに面するインターフェイスで有効になります。また、**[PTP 送信元ループバック ID（PTP Source Loopback Id）]** および **[PTP ドメイン ID（PTP Domain Id）]** フィールドが編集可能になります。詳細については、Easy ファブリック向け高精度時間プロトコル, on page 119を参照してください。

[PTP 送信元ループバック ID（PTP Source Loopback Id）]：すべての PTP パケットの送信元 IP アドレスとして使用されるループバック インターフェイス ID ループバックを指定します。有効な値の範囲は 0 ～ 1023 です。PTP ループバック ID を RP、ファントム RP、NVE、または MPLS ループバック ID と同じにすることはできません。そうでない場合は、エラーが生成されます。PTP ループバック ID は、DCNM から BGP ループバックまたは作成元のユーザー定義ループバックと同じにすることができます。

保存して展開中に PTP ループバック ID が見つからない場合は、次のエラーが生成されます。

PTP 送信元 IP に使用するループバック インターフェイスが見つかりません。PTP 機能を有効にするには、すべてのデバイスでPTPループバック インターフェイスを作成します。

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

[MPLS ハンドオフの有効化（Enable MPLS Handoff）]：MPLS ハンドオフ機能を有効にするには、このチェックボックスをオンにします。詳細については、「VXLAN BGP EVPN ファブリックでの境界プロビジョニングの使用例：MPLS SR および LDP ハンドオフ」の章を参照してください。

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

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

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

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

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

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

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

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

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

[MACsec の有効化（Enable MACsec）]：ファブリックの MACsec を有効にします。詳細については、Easy ファブリックおよび eBGP ファブリックでの MACsec サポート, on page 231を参照してください。

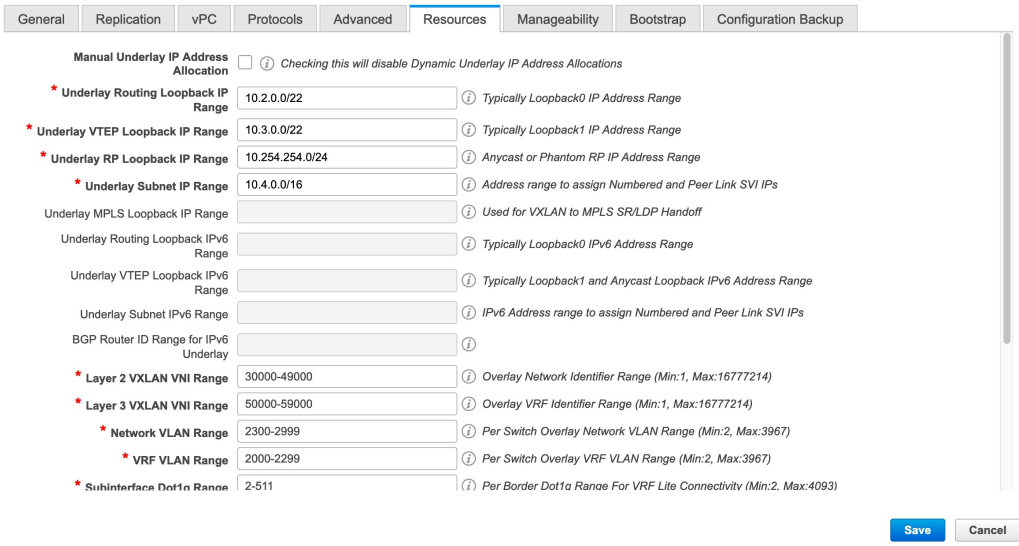
[自由形式の CLI（Freeform CLIs）]：ファブリック レベルの自由形式の CLI は、ファブリックの作成または編集中に追加できます。ファブリック全体のスイッチに適用できます。インデントなしで、実行コンフィギュレーションに表示されている設定を追加する必要があります。VLAN、SVI、インターフェイス構成などのスイッチ レベルの自由形式の構成は、スイッチでのみ追加する必要があります。詳細については、「ファブリック スイッチでのフリーフォーム設定の有効化」を参照してください。

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

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

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

8. [リソース（Resources）] タブをクリックします。



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

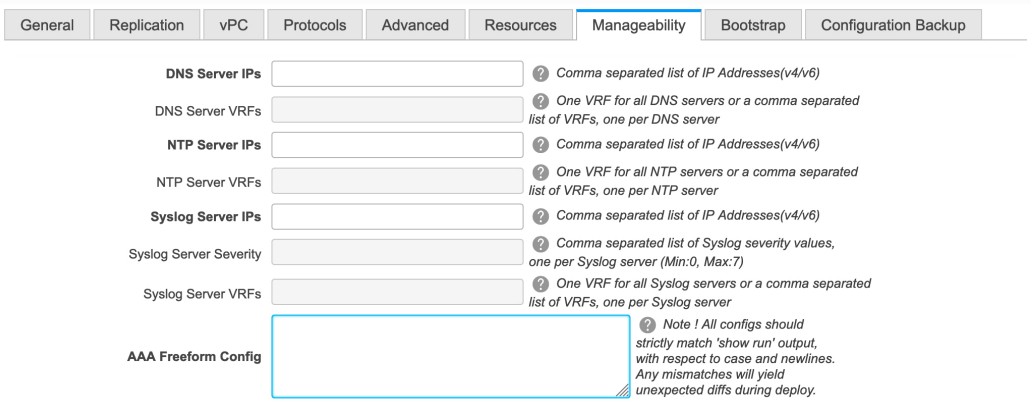
a. L2 範囲を更新し、[保存（Save）] をクリックします。

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

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

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

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



このタブのフィールドは次のとおりです。

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

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

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

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

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

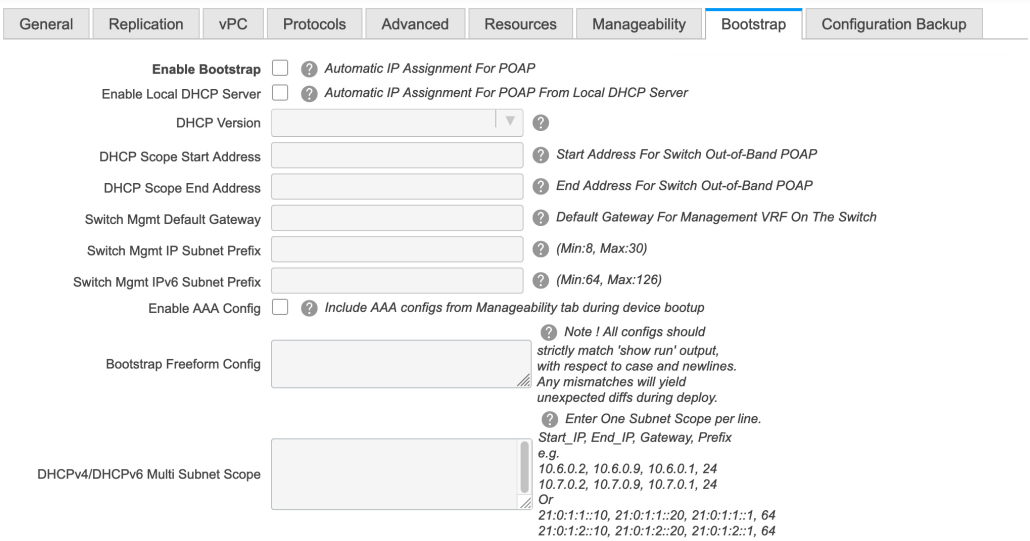
[Syslog サーバのシビラティ（重大度）（Syslog Server Severity）]：syslog サーバごとに 1 つの syslog シビラティ（重大度）値のカンマ区切りリストを指定します。最小値は 0 で、最大値は 7 です。高いシビラティ（重大度）を指定するには、大きい数値を入力します。

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

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

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

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



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

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

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

ローカル DHCP サーバーの有効化（Enable Local DHCP Server）：ローカル DHCP サーバーを介した自動 IP アドレス割り当ての有効化を開始するには、このチェックボックス

をオンにします。このチェックボックスをオンにすると、**[DHCP スコープ開始アドレス（DHCP Scope Start Address）]** および **[DHCP スコープ終了アドレス（DHCP Scope End Address）]** フィールドが編集可能になります。

このチェックボックスをオンにしない場合、DCNM は自動 IP アドレス割り当てにリモートまたは外部DHCPサーバを使用します。

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

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

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

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

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

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

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

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

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

running-config をコピーして **[フリーフォームの設定（freeform config）]** フィールドに、NX-OS スイッチの実行設定に示されているように、正しいインデントでコピーアンドペーストします。freeform config は running config と一致する必要があります。詳細については、スイッチのフリーフォーム設定エラーの解決, on page 411を参照してください。

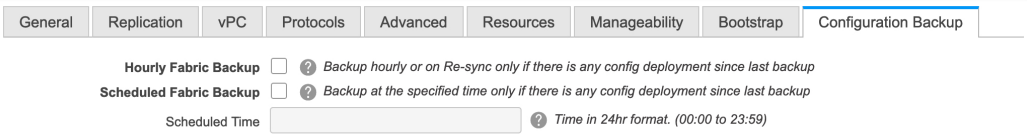
[DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）]：1行に1つのサブネット スコープを入力して、フィールドを指定します。**[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）]** チェックボックスをオンにした後で、このフィールドは編集可能になります。

スコープの形式は次の順で定義する必要があります。

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

例：10.6.0.2、10.6.0.9、16.0.0.1、24

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



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

時間単位のバックアップは、その時間の最初の 10 分間にトリガーされます。

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

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

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

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

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

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

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

Note 即時バックアップをトリガーするには、次の手順を実行します。

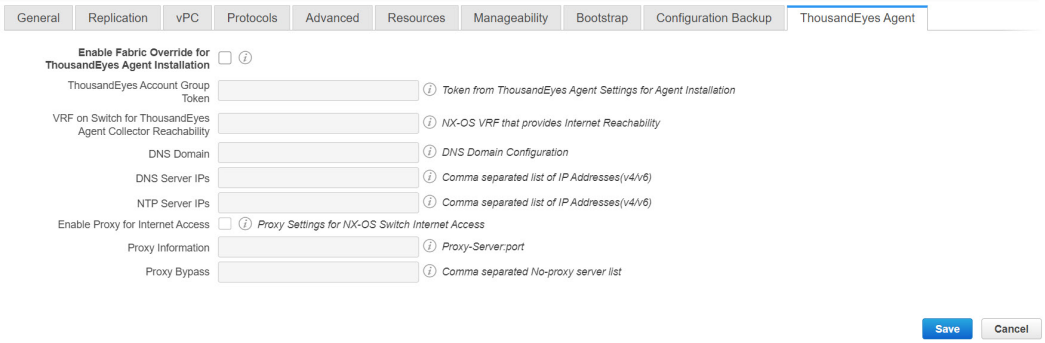
a. **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。[Fabric Builder] 画面が表示されます。

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

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

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

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



このタブのフィールドは次のとおりです。

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

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

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

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

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

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

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

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

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

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

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

ファブリックへのスイッチの追加

各ファブリックのスイッチは一意であるため、各スイッチは1つのファブリックにのみ追加できます。

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

さらに、スイッチとインターフェイスを事前プロビジョニングできます。詳細については、デバイスの事前プロビジョニング , on page 104およびイーサネット インターフェイスの事前プロビジョニング, on page 109を参照してください。

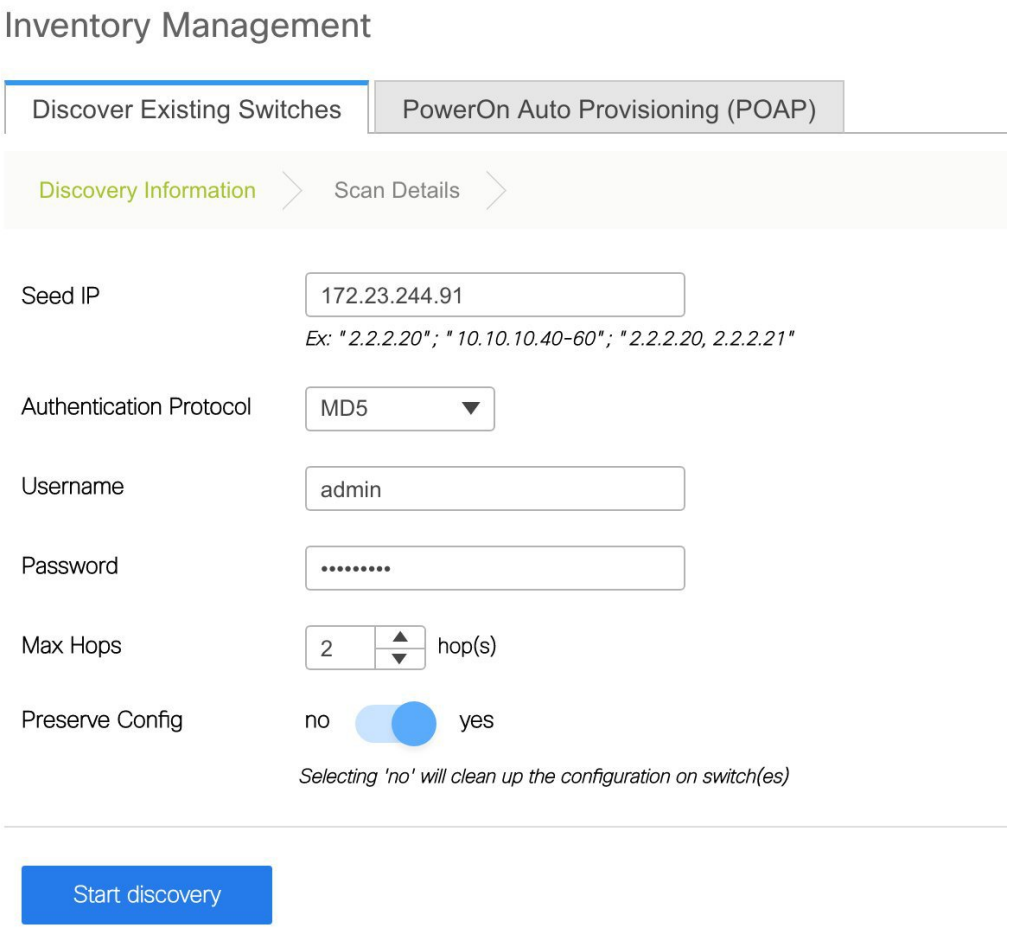
Note DCNM でピリオド文字（.）を含むホスト名を持つスイッチが検出されると、ドメイン名として扱われ、切り捨てられます。ピリオド文字（.）の前のテキストのみがホスト名と見なされます。次に例を示します。

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

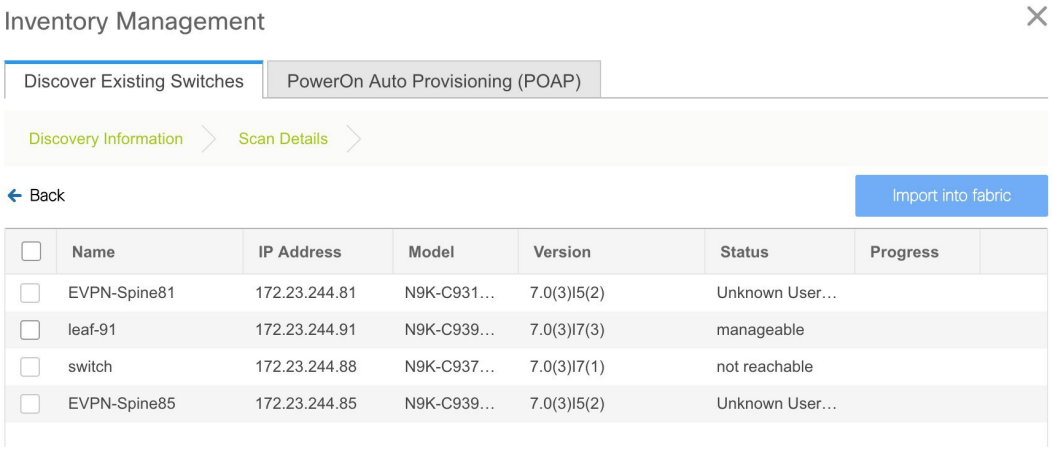
既存のスイッチの検出

1. **[スイッチの追加（Add Switches）]**をクリックした後、**[既存のスイッチの検出（Discover Existing Switches）]**タブを使用して、1つ以上の既存のスイッチをファブリックに追加します。この場合、既知のクレデンシャルと事前プロビジョニングされたIPアドレスを持つスイッチがファブリックに追加されます。スイッチの IP アドレス（シード IP）、管理者名、ユーザー名、およびパスワード（**[ユーザー名（Username）]**フィールドと**[パスワード（Password）]**フィールド）は、ユーザーによる入力として提供されます。**[構成の保持（Preserve Config）]**ノブは、デフォルトで**[yes]**に設定されています。これは、ファブリックへのデバイスのブラウンフィールドインポートに対してユーザが選択するオプションです。デバイス構成がインポートプロセスの一部としてクリーンアップされるグリーンフィールドインポートの場合、ユーザーは**[構成の保持（Preserve Config）]**ノブを**[no]**に設定する必要があります。

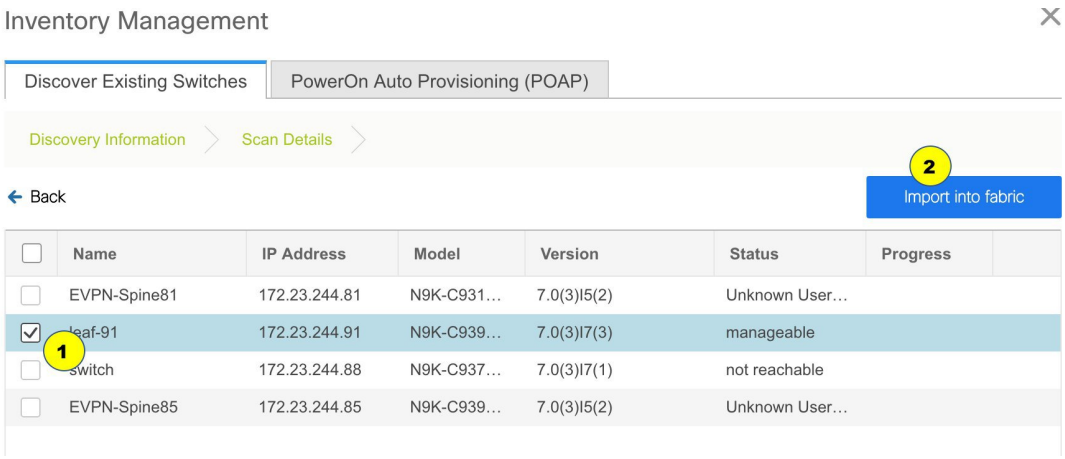
Note Easy_Fabric_eBGP は、ファブリックへのデバイスのブラウンフィールドインポートをサポートしていません。



2. [検出の開始（Start discovery）] をクリックします。**[スキャン詳細（Scan Details）]** ウィンドウが間もなく表示されます。**[最大ホップ（Max Hops）]** フィールドに 2 が入力されているため（デフォルト）、指定された IP アドレス（リーフ 91）を持つスイッチとそのスイッチからの 2 つのホップが **[スキャン詳細（Scan Details）]** の結果に入力されます。



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



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

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

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

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

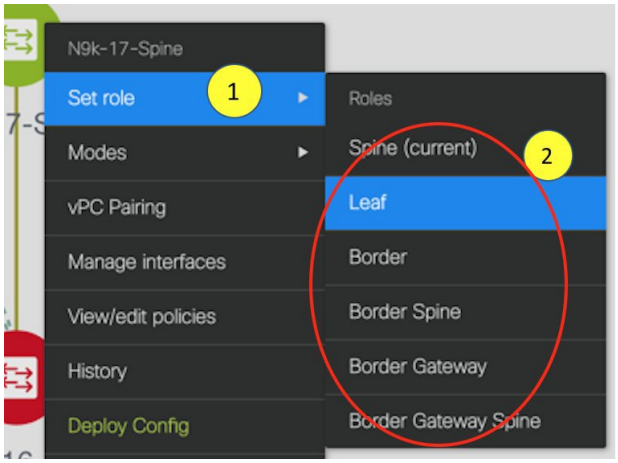
DCNM がすべてのスイッチを検出し、[進行状況（Progress）] 列にすべてのスイッチの **[done]** が表示されたら、画面を閉じます。*[*スタンドアロン ファブリック トポロジ（Standalone fabric topology）] 画面が再び表示されます。追加されたスイッチのスイッチアイコンが表示されます。

Note スイッチの検出中に次のエラーが発生することがあります。

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

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

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



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

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

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

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

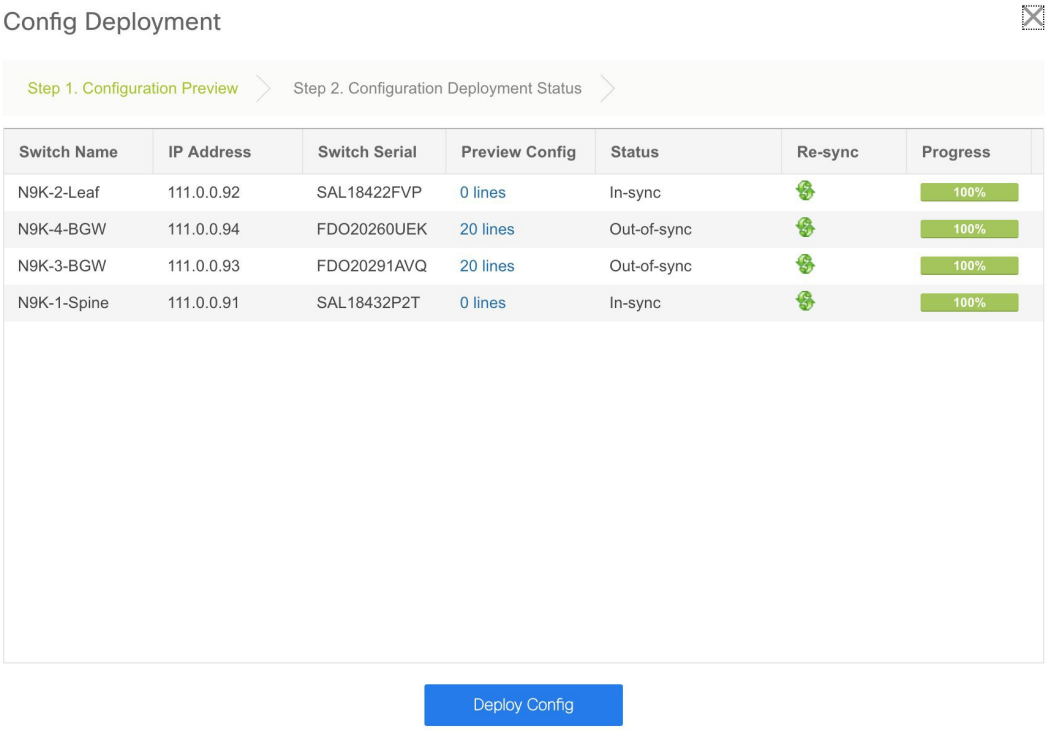
6. 画面の右上にある **[保存と展開（Save & Deploy）]** をクリックします。

テンプレートとインターフェイスの設定は、スイッチのアンダーレイ ネットワーク構成を形成します。また、ファブリック構成の一部として入力されたフリーフォーム CLI（[詳細（Advanced）]タブで入力されたリーフおよびスパイン スイッチのフリー フォーム設定）も展開されます。自由形式構成の詳細については、「ファブリック スイッチでのフリーフォーム設定の有効化」を参照してください。

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

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

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



ステータスが非同期の場合は、デバイスの DCNM との構成に不整合があることを示しています。

[再同期（Re-sync）] 列のスイッチごとに [再同期（Re-sync）] ボタンが表示されます。大規模なアウトオブバンド変更がある場合、または設定変更が DCNM に正しく登録されていない場合に、このオプションを使用して DCNM 状態を再同期します。再同期操作は、スイッチに対して完全な CC 実行を実行し、「show run」および「show run all」コマンドをスイッチから再収集します。再同期プロセスを開始すると、進行状況メッセージが画面に表示されます。再同期中に、実行構成がスイッチから取得されます。スイッチの Out-of-Sync/In-Sync ステータスは、DCNM で定義されたインテントに基づいて再計算されます。

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

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

[Side-by-sideComparison] タブには、現在の構成と予想される構成が一緒に表示されます。

DCNM 11 では、複数行のバナー motd 構成がサポートされています。マルチライン バナー motd 構成は、**switch_freeform** を使用するスイッチごと、またはリーフ/スパイン自由形式構成を使用するファブリックごとのいずれかで、自由形式の構成ポリシーを使用して Cisco DCNM で構成できます。複数行のバナー motd が構成された後、ファブリック トポロジ画面（の右上）で **[保存と展開（Save & Deploy）]** オプションを実行して、ポリシーを展開します。そうしないと、ポリシーがスイッチに適切に展開されない可能性があります。**バナー**ポリシーは、単一行のバナー設定のみを設定します。また、自由形式の設定/ポリシー

に関連するバナーは1つだけ作成できます。バナー motd を構成するための複数のポリシーはサポートされていません。

7. 画面 を閉じます。

   構成展開の画面で、画面下部の [構成の展開（Deploy Config）] をクリックして、保留中の構成をスイッチに展開開始します。[ステータス（Status）] カラムには、「FAILED」または「SUCCESS」の状態が表示されます。FAILED ステータスの場合は、問題の解決に失敗した理由を調査します。

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

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

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

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

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

Cisco NX-OS リリース 11.4(1) 以降、**[トポロジ（Topology）]** ウィンドウの **[FEX]** チェックボックスをオフにすると、FEX デバイスは **[ファブリック ビルダ（Fabric Builder）]** トポロジ ウィンドウでも非表示になります。**Fabric Builder** で FEX を表示するには、このチェックボックスをオンにする必要があります。このオプションはすべてのファブリックに適用でき、セッションごとに保存されるか、DCNMからログアウトするまで保存されます。ログアウトしてDCNMにログインすると、FEXオプションはデフォルトにリセットされます。つまり、デフォルトで有効になります。詳細については、パネルを表示, on page 29を参照してください。

[構成の展開（Deploy Config）] オプションの使用例は、スイッチ レベルの自由形式の設定です。詳細については、「ファブリック スイッチでのフリーフォーム設定の有効化」を参照してください。

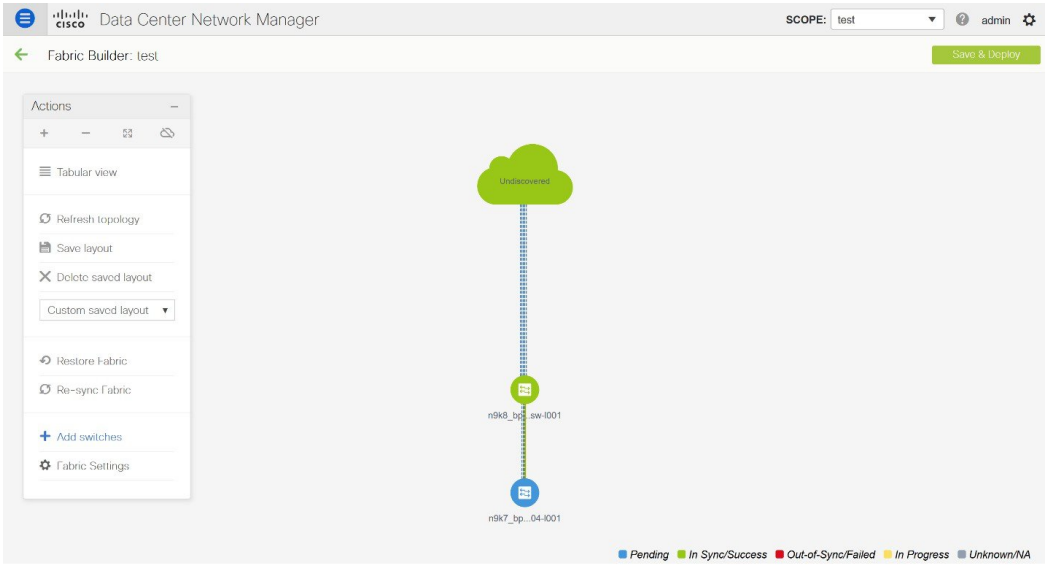
新しいスイッチの検出

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

2. デバイスと DCNM の間に IP 到達可能性がある限り、デバイスからの DHCP 要求は DCNM に転送されます。ゼロデイ デバイスを簡単に起動するには、前述のように、**ファブリック設定**でブート ストラップ オプションを有効にする必要があります。

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

4. DCNM GUI で、ファブリックに移動します（**[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** をクリックし、ファブリックをクリックします）。ファブリック トポロジが表示されます。



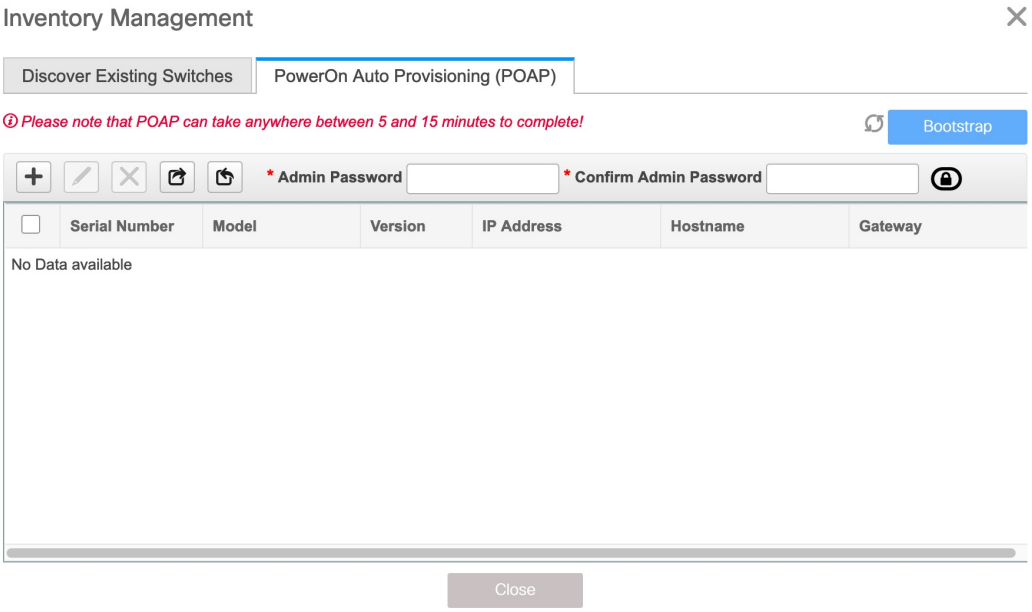
ファブリック トポロジ ウィンドウに移動し、**[アクション（Actions）]** パネルから **[スイッチの追加（Add switches）]** オプションをクリックします。[インベントリ管理（Inventory Management）] ウィンドウが表示されます。

5. **[POAP]** タブをクリックします。

前述のように、DCNM はデバイスからシリアル番号、モデル番号、およびバージョンを取得し、それらを [インベントリ管理（Inventory Management）] ウィンドウに表示します。また、IP アドレス、ホスト名、およびパスワードを追加するオプションが使用可能になります。スイッチ情報が取得されない場合は、ウィンドウを更新します。

Note

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



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

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

リリース 11.2(1) 以降、デバイスを事前にプロビジョニングできます。デバイスの事前プロビジョニングについては、デバイスの事前プロビジョニング , on page 104 を参照してください。

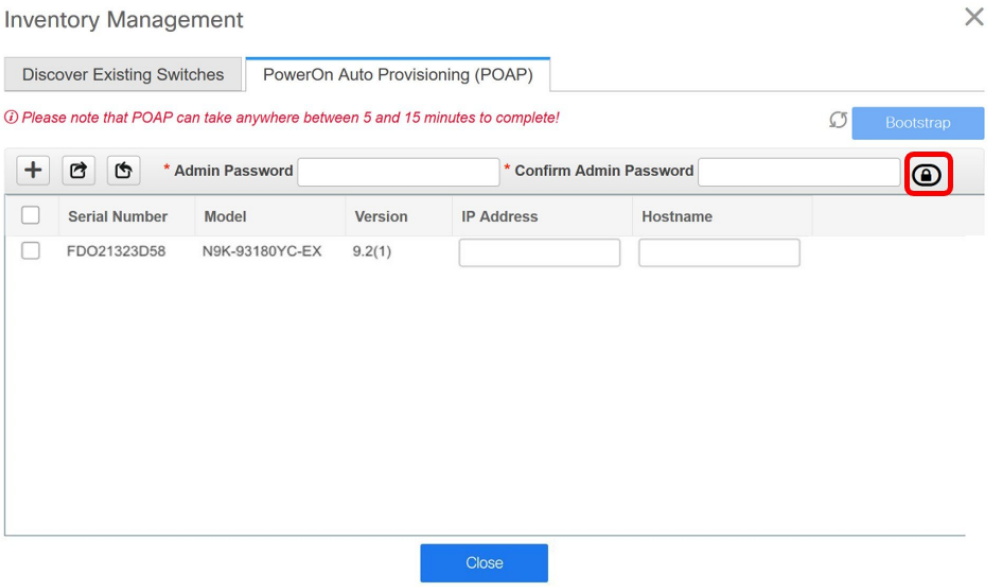
6. **[管理者パスワード（Admin Password）]** フィールドと **[管理者パスワードの確認（Confirm Admin Password）]** フィールドに、新しいパスワードを入力します。

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

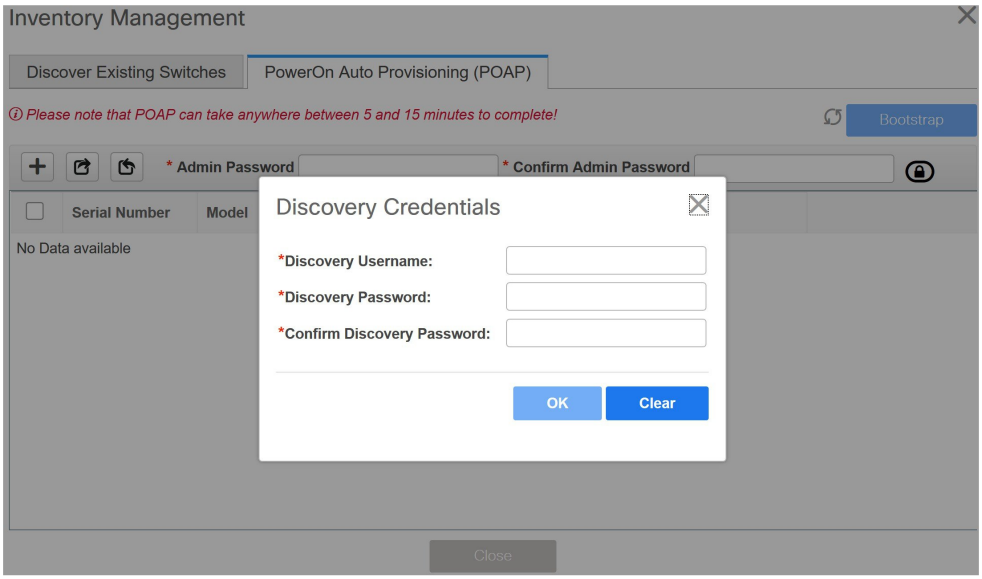
Note 管理者クレデンシャルを使用してスイッチを検出しない場合は、代わりに AAA 認証（RADIUS または TACACS クレデンシャル）を使用できます。

7. （任意）スイッチの検出に検出クレデンシャルを使用します。

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



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



[OK] をクリックして、ディスカバリ クレデンシャルを保存します。

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

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

DCNM は管理IPアドレスおよびその他のクレデンシャルをスイッチにプロビジョニングします。この単純化された POAP プロセスでは、すべてのポートが開かれます。

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

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

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

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

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

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

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

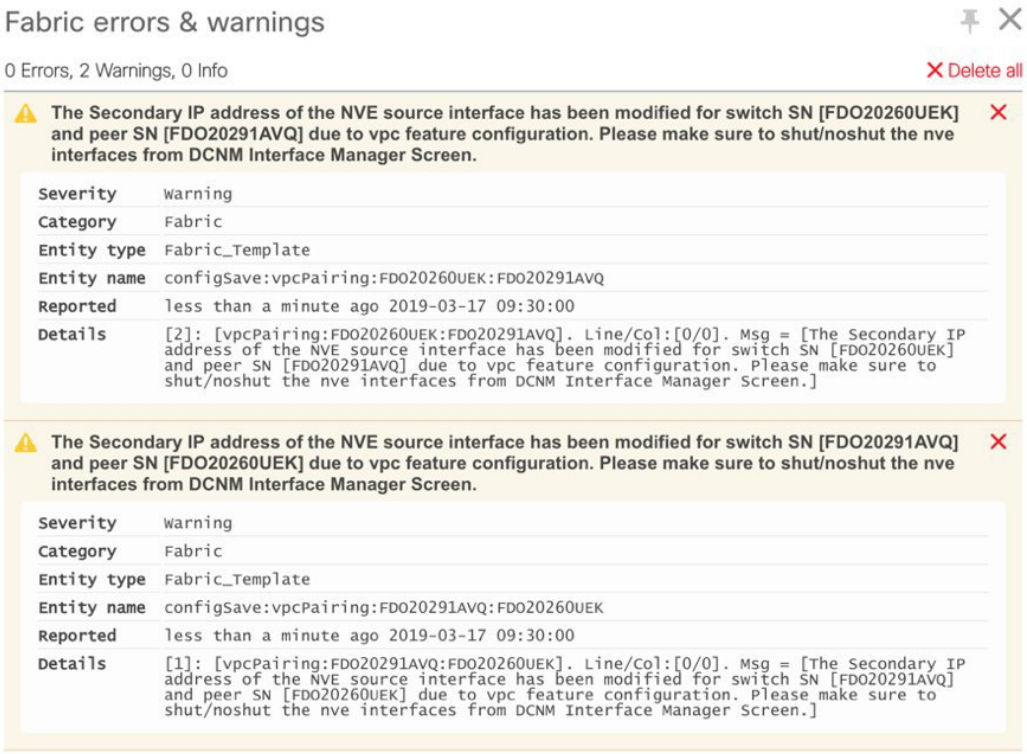
14. スイッチとリンクが DCNM で検出されます。設定は、さまざまなポリシー（ファブリック、トポロジ、スイッチ生成ポリシーなど）に基づいて構築されます。スイッチイメージ（およびその他の必要な）設定がスイッチで有効になっている。

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

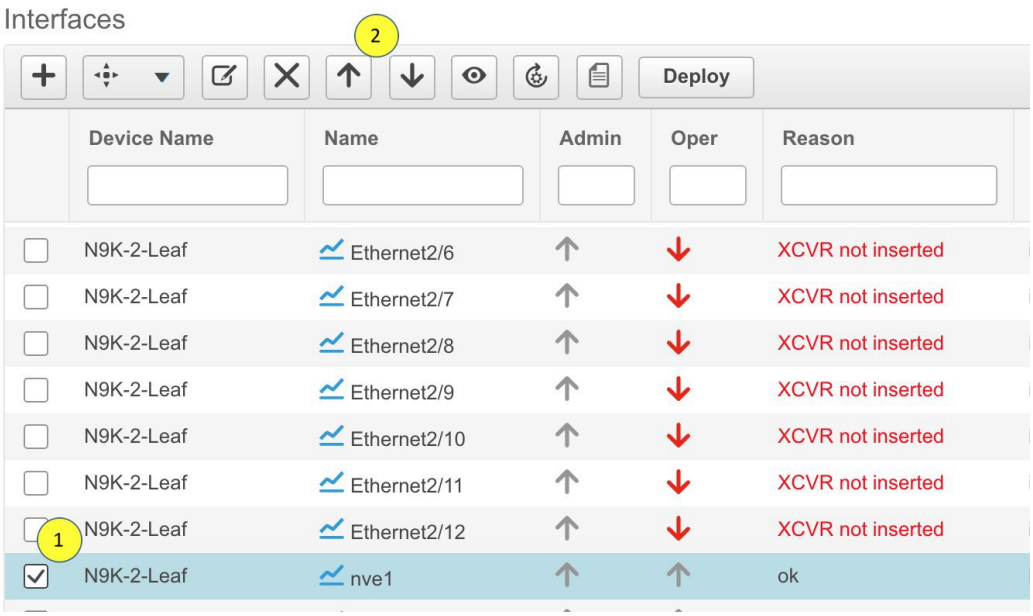
    - vPC ペアリング。
    - ブレークアウト インターフェイス。
    - ポートチャネル、およびポートへのメンバーの追加。

    vPCのペアリング/ペアリング解除または advertise-pip オプションを有効または無効にするか、マルチサイト構成を更新する場合は、**[保存と展開（Save & Deploy）]** 操作を使用する必要があります。操作の終了時に、nve インターフェイスで **shutdown** または **no**

shutdown コマンドを設定するように求めるエラーが表示されます。vPC 設定を有効にした場合のエラー スクリーンショットのサンプル：



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



スイッチを右クリックすると、さまざまなオプションを表示できます。

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

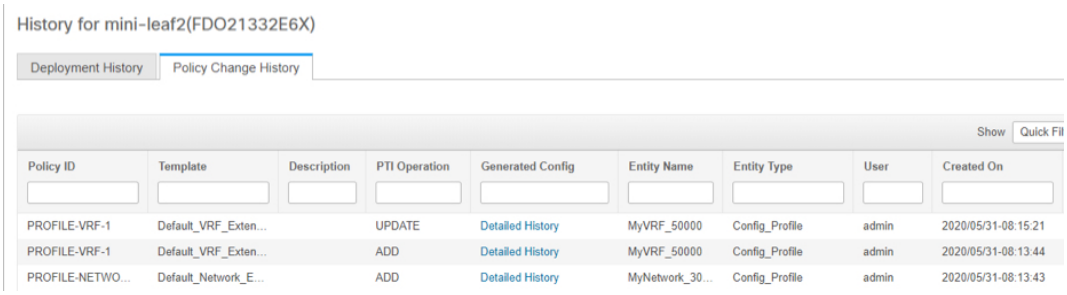
Note

- スイッチのロールの変更は、**[保存と展開（Save & Deploy）]** を実行する前にのみ許可されます。
- DCNM 11.1(1) 以降、スイッチのロールは、スイッチ上にオーバーレイがない場合に変更できますが、スイッチ操作, on page 244 で指定された許可されたスイッチ ロール変更のリストに従ってのみ変更できます。

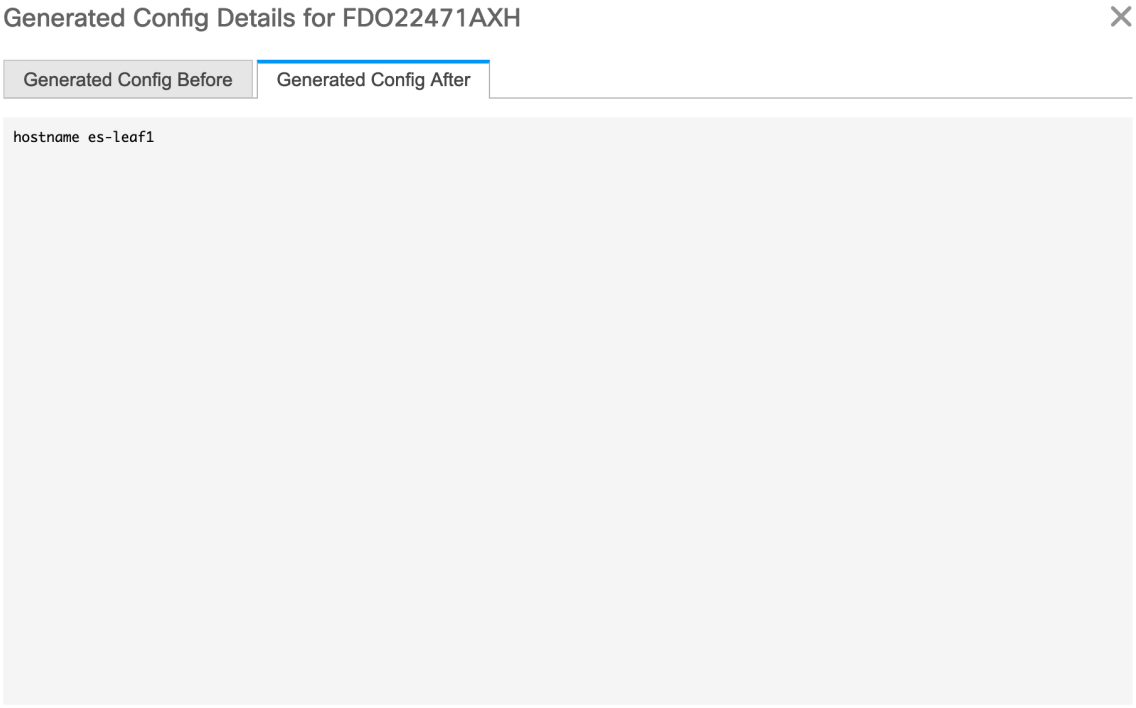
- **モード**：メンテナンス モードとアクティブ/操作モード。
- **vPC** ペアリング：vPC のスイッチを選択し、そのピアを選択します。

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

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



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



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

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

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

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

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

- vPC、ループバック インターフェイス、サブインターフェイス設定などのインターフェイス構成をプロビジョニングします。[「インターフェイス」を参照してください]。
- ネットワークを作成し、スイッチに展開します。[「ネットワークおよび VRF の作成と展開 」を参照してください]。

DCNM 11 での事前プロビジョニングのサポート

Cisco DCNM は、事前のデバイス構成のプロビジョニングをサポートしています。これは特に、デバイスが調達されたものの、まだお客様に配送されていない、または受領されていないシナリオに当てはまります。発注書には通常、デバイスのシリアル番号、デバイスモデルなどに関する情報が含まれており、これらの情報を使用して、デバイスをネットワークに接続する前に DCNM でデバイス構成を準備できます。Easy ファブリックと外部/Classic_LAN ファブリックの両方で、Cisco NX-OS デバイスの事前プロビジョニングがサポートされています。

デバイスの事前プロビジョニング

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

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

- 事前プロビジョニングされたデバイスは、DCNM で次の構成をサポートします。
  - 基本管理
  - vPC ペアリング
  - ファブリック内リンク

- イーサネット ポート
- ポートチャネル
- vPC
- ST FEX
- AA FEX
- ループバック
- オーバーレイ ネットワーク設定

- 事前プロビジョニングされたデバイスは、DCNM で次の構成をサポートしません。
  - ファブリック間リンク
  - Sub-interface
  - インターフェイス ブレークアウト構成

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

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

  [データ（Data）] フィールドの値の例を次に示します。
  - {"modulesModel": ["N9K-C93180LC-EX"], "gateway": "10.1.1.1/24"}

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

Procedure

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

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

ステップ 2 ファブリック ボックス内をクリックします。

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

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

ステップ 4 **[POAP]** タブをクリックします。

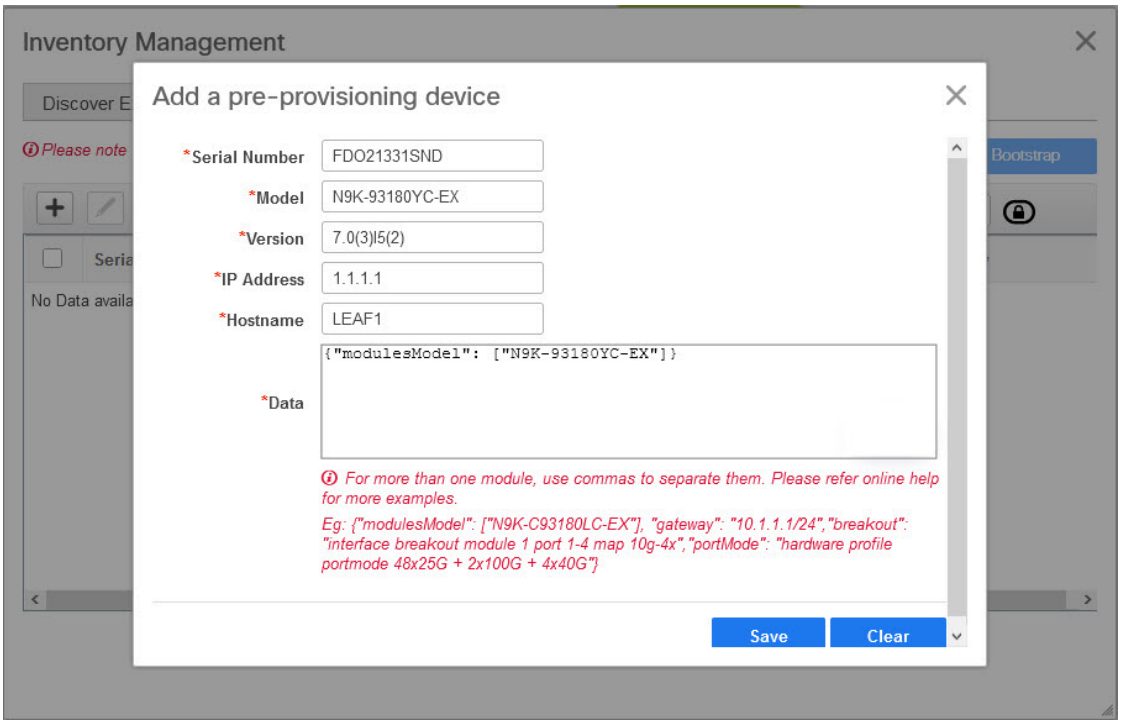
ステップ 5 **[POAP]** タブで、次の手順を実行します。

a. 画面左上の [+] をクリックします。

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

b. スクリーンショットに示されているように、デバイスの詳細を入力します。

c. [保存（Save）] をクリックします。



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

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

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

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

ウィンドウの左上には、スイッチ情報を含む .csv ファイルをエクスポートおよびインポートするための **[エクスポート（Export）]** および **[インポート（Import）]** アイコンがあります。

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

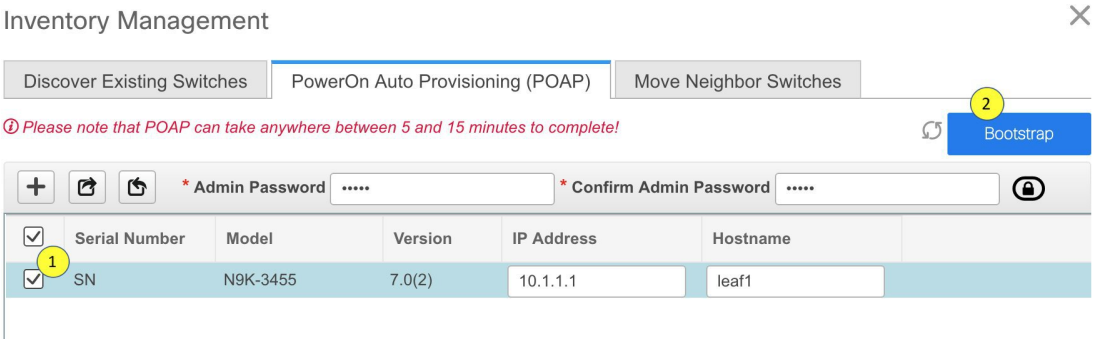
すべての必須フィールド（シリアル番号、モデル、バージョン、IpAddress、ホスト名、およびデータ フィールド [JSON オブジェクト]）を使用して、.csv ファイルに新しいデバイスの情報を追加します。

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

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

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

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



Leaf1 デバイスがファブリック トポロジに表示されます。

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

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

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

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

次のいずれかのテンプレートを使用して、リンク内ポリシーを作成します。

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

[保存して展開（Save & Deploy）] をクリックします。

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

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

詳細については、返品許可（RMA）, on page 304を参照してください。

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

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

イーサネット インターフェイスの事前プロビジョニング

DCNM リリース 11.4(1) 以降、**[インターフェイス（Interface）]** ウィンドウでイーサネット インターフェイスを事前プロビジョニングできます。この事前プロビジョニング機能は、Easy、外部、およびeBGP ファブリックでサポートされています。DCNM で検出される前に、事前にプロビジョニングされたデバイスにのみ、イーサネット インターフェイスを追加できます。

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

始める前に

ファブリックに事前にプロビジョニングされたデバイスがあることを確認してください。詳細については、デバイスの事前プロビジョニング （104 ページ）を参照してください。

手順

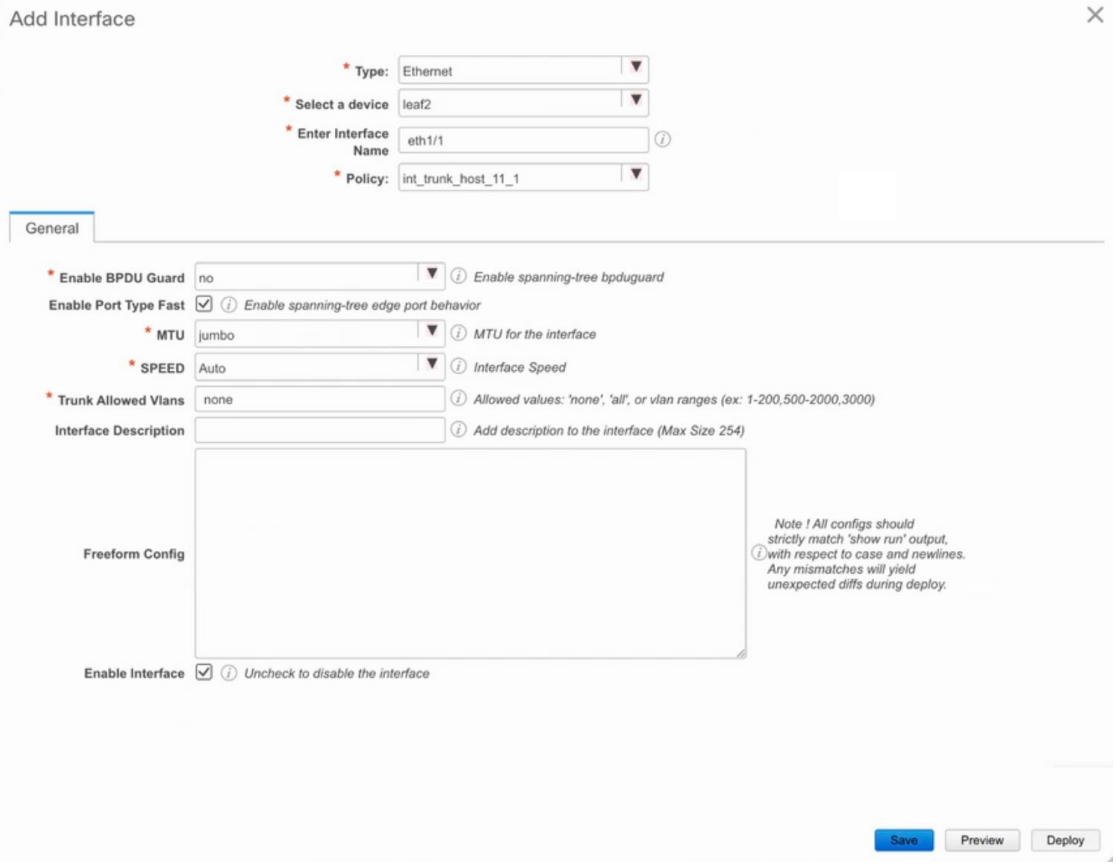
ステップ 1 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウから事前にプロビジョニングされたデバイスを含むファブリックに移動します。

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

[制御（Control）] > [ファブリック（Fabrics）] > [インターフェイス（Interfaces）] を選択して、[インターフェイス（Interfaces）] ウィンドウに移動することもできます。[範囲（Scope）] ドロップダウンリストから、事前にプロビジョニングされたデバイスを含むファブリックを選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 **[インターフェイスの追加（Add Interface）]** ウィンドウで、必要なすべての詳細を入力します。



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

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

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

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

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

詳細については、インターフェイスの追加 （316 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 **[プレビュー（Preview）]** をクリックして、追加後にスイッチに展開される予定の構成を確認します。

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

vPC ペアの事前プロビジョニング

始める前に

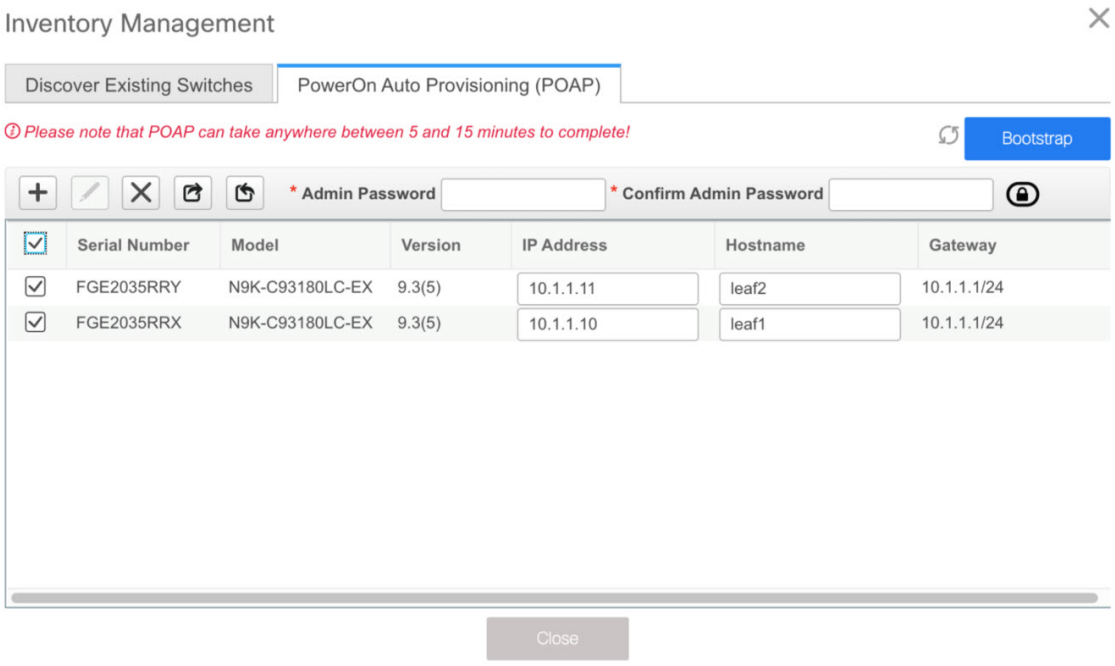
[ファブリックの設定（Fabric Settings）] で**[ブートストラップ（Bootstrap）]**が有効になっていることを確認します。

手順

ステップ 1 両方のデバイスをファブリックにインポートします。

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

次の例は、事前にプロビジョニングされ、既存のファブリックに追加された 2 台の Cisco Nexus 9000 シリーズ デバイスを表示するイメージを示します。[アクション（Action）] パネルで **[スイッチの追加（Add Switches）]** を選択します。**[インベントリ管理（Inventory Management）]** 画面で、**[パワーオン自動プロビジョニング（PowerOn Auto Provisioning、POAP）]** をクリックします。



デバイスは、ファブリック内に灰色の/未検出デバイスとして表示されます。

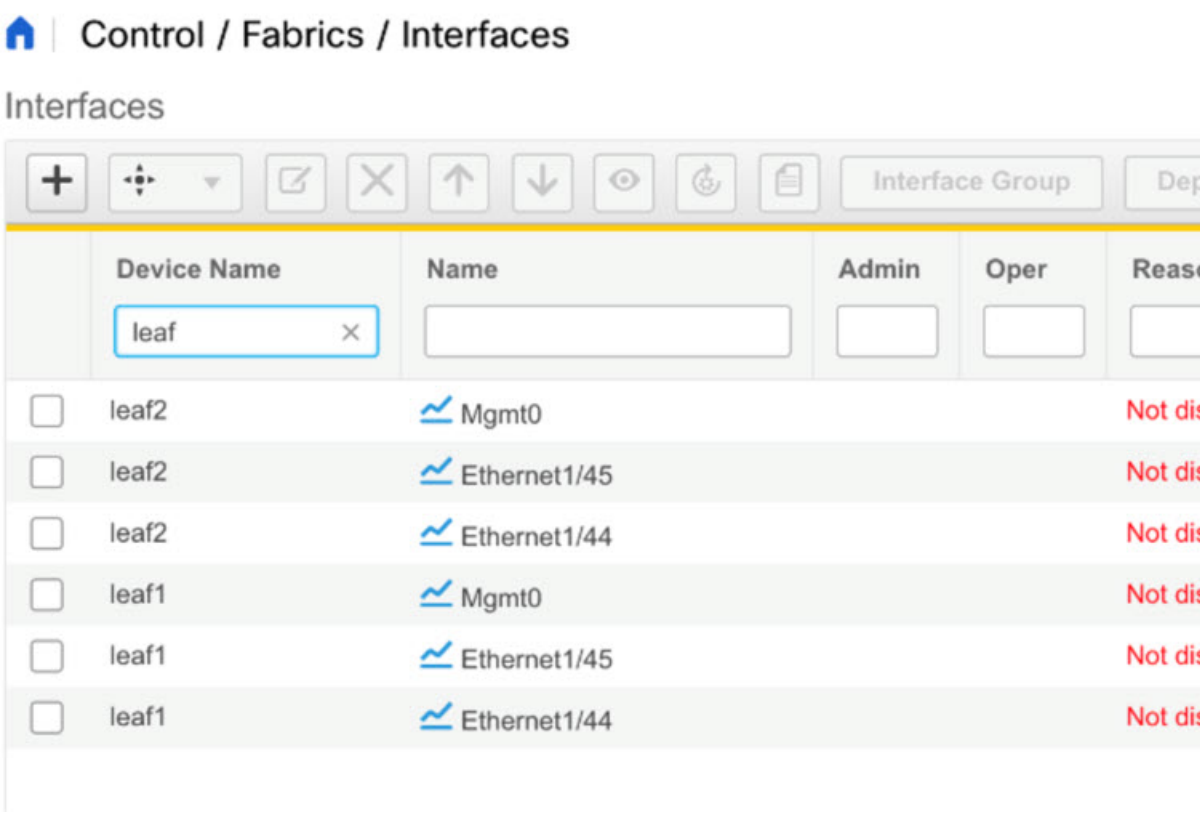
ステップ 2 右クリックして、他の到達可能なデバイスと同様に、これらのデバイスの適切な役割を選択します。

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

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

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

手順については、「**イーサネット インターフェイスの事前プロビジョニング**」を参照してください。



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

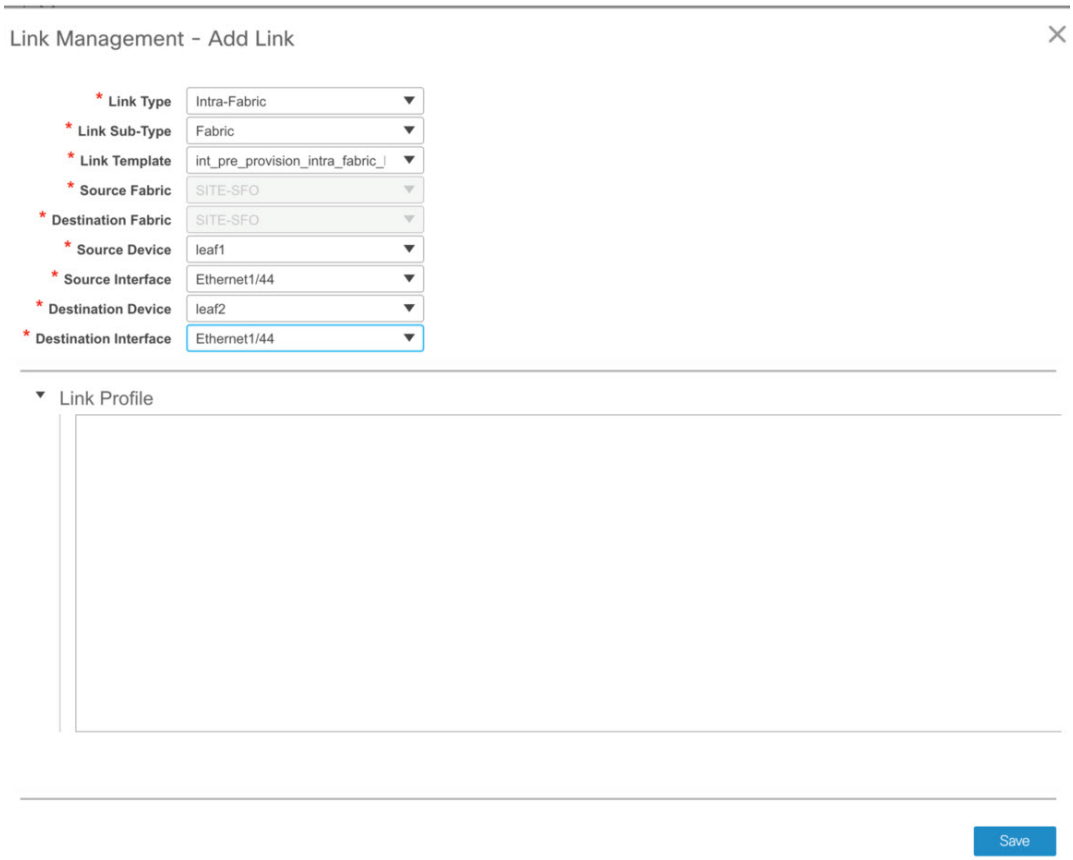
ファブリック ビルダ表示で、**[追加（Add）]** リンクを右クリックするか、ファブリック ビルダの表形式ビューの [リンク] タブで **[追加（+）（Add(+)）]** アイコンをクリックします。

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

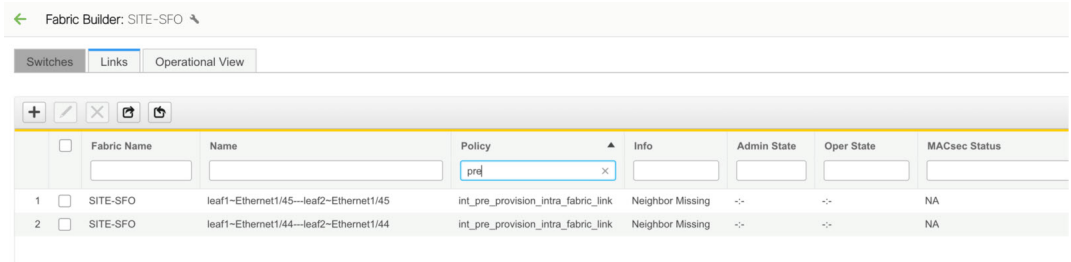
リンク テンプレートとして **int_pre_provision_intra_fabric_link** を選択していることを確認してください。送信元インターフェイスと宛先インターフェイスのフィールド名は、前の

手順で事前にプロビジョニングされたイーサネットインターフェイスと一致している必要があります。

事前にプロビジョニングされたリンク作成の例を次のイメージに示します。



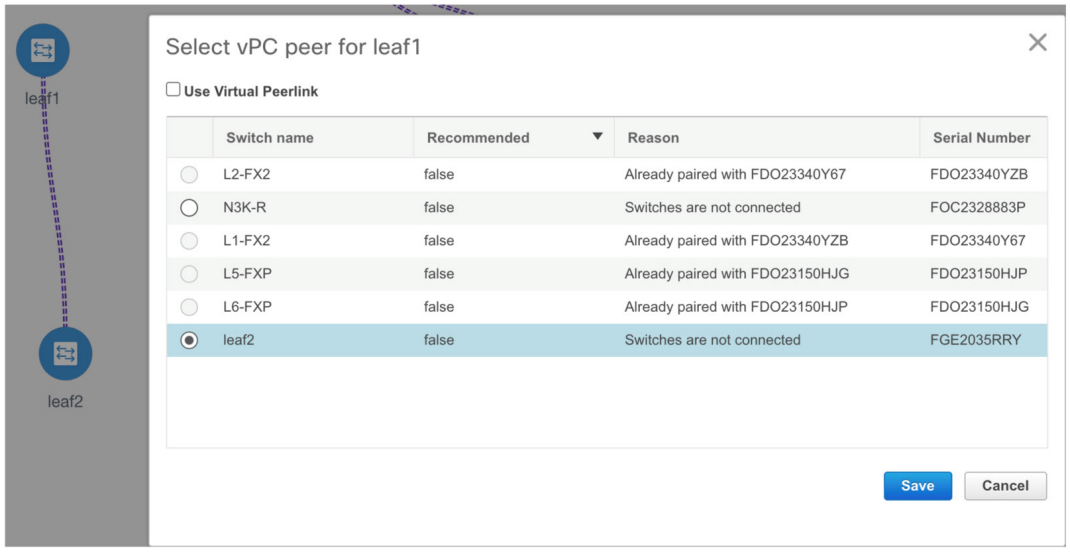
リンクが作成されると、次のイメージに示すように、[ファブリック ビルダ（Fabric builder）] の下の [リンク（Links）] タブにリスト表示されます。



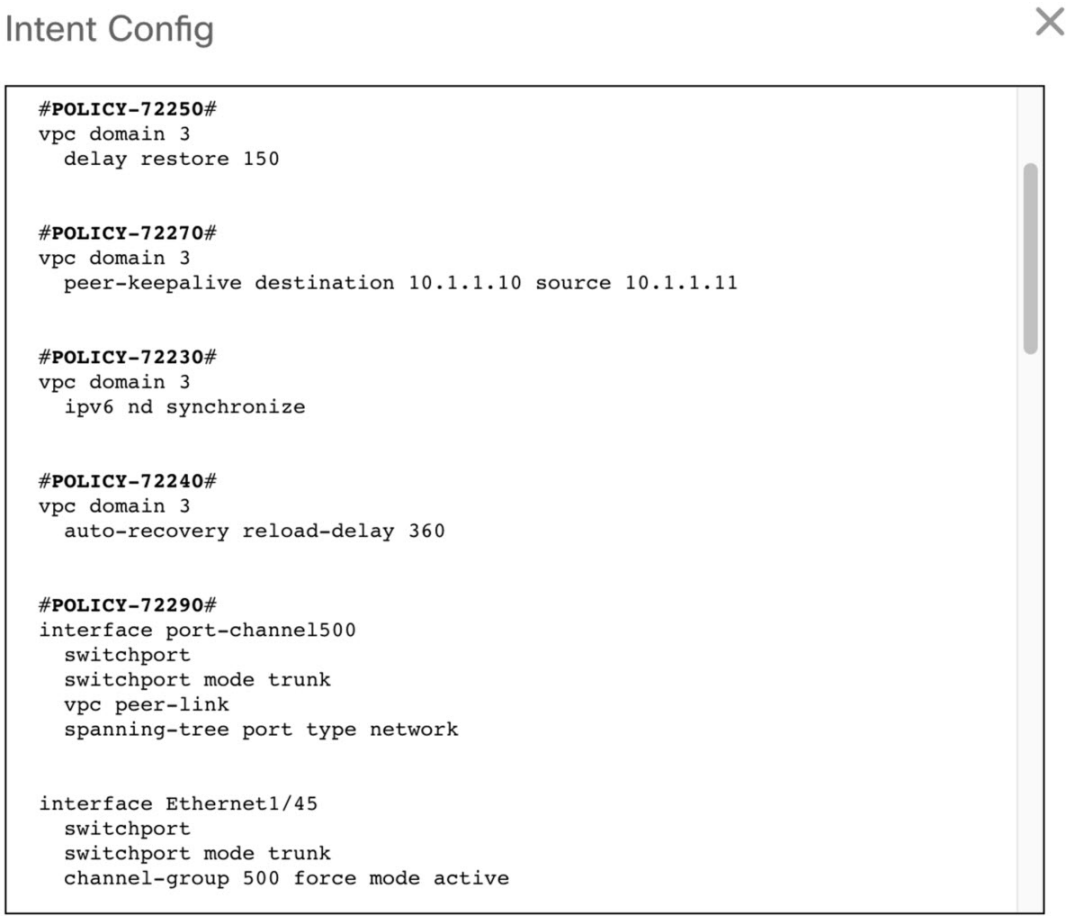
c) [ファブリック トポロジ（Fabric topology）] で、スイッチを右クリックし、ドロップダウンリストから [vPC ペアリング（vPC Pairing）] を選択します。

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

d) **[保存と展開（Save & Deploy）]** をクリックして、事前にプロビジョニングされたデバイスに必要な目的の vPC ペアリング構成を生成します。



完了すると、デバイスは正しくペアリングされ、デバイスの vPC ペアリング インテントが生成されます。ポリシーは、次の図に示すように生成されます。



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

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

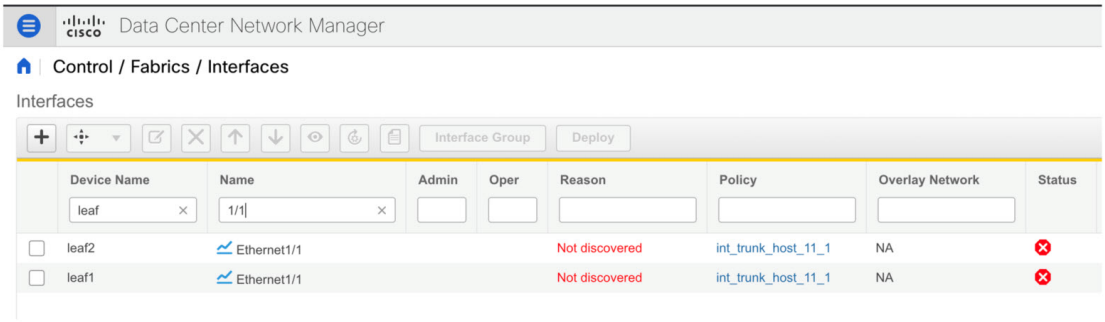
vPC ホスト インターフェイスの事前プロビジョニング

手順

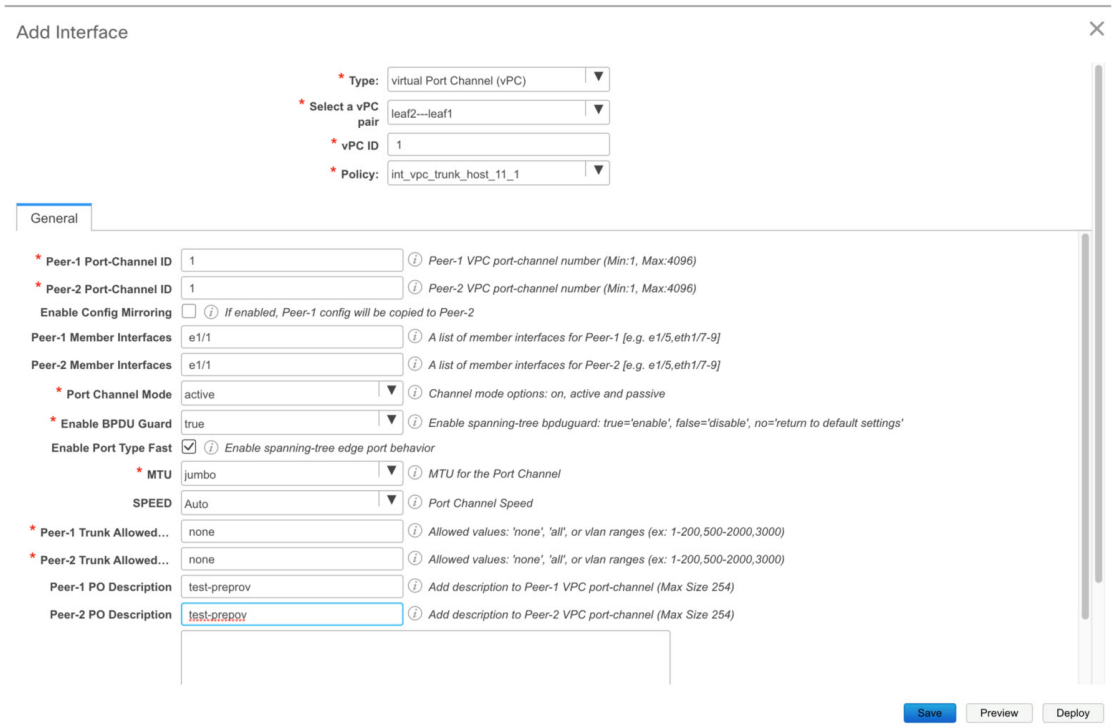
ステップ 1 事前プロビジョニングされたデバイスに物理イーサネットインターフェイスを作成します。通常の vPC ペアまたはスイッチと同様の vPC ホスト インターフェイスを追加します。

手順については、イーサネット インターフェイスの事前プロビジョニング （109 ページ）を参照してください。

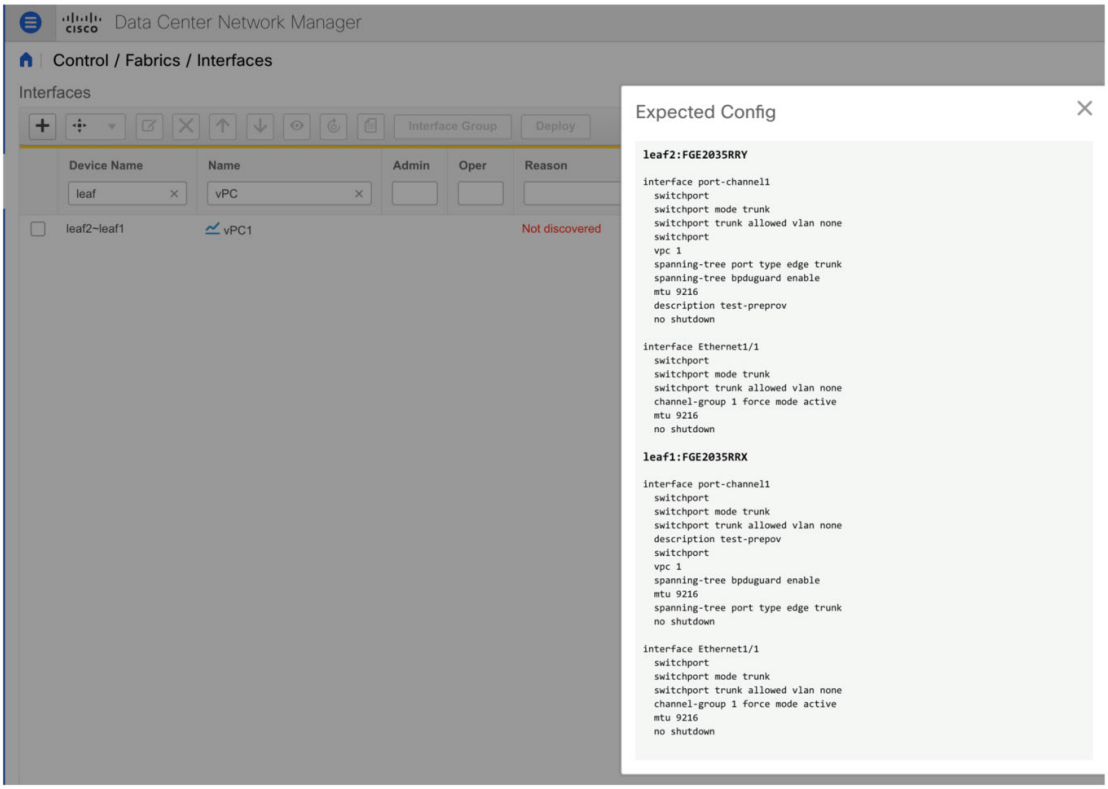
たとえば、leaf1-leaf2 は、事前プロビジョニングされた vPC デバイス ペアを表します。ただし、イーサネット インターフェイス 1/1 は、leaf1 と leaf2 の両方のデバイスで事前プロビジョニングされているものとします。



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



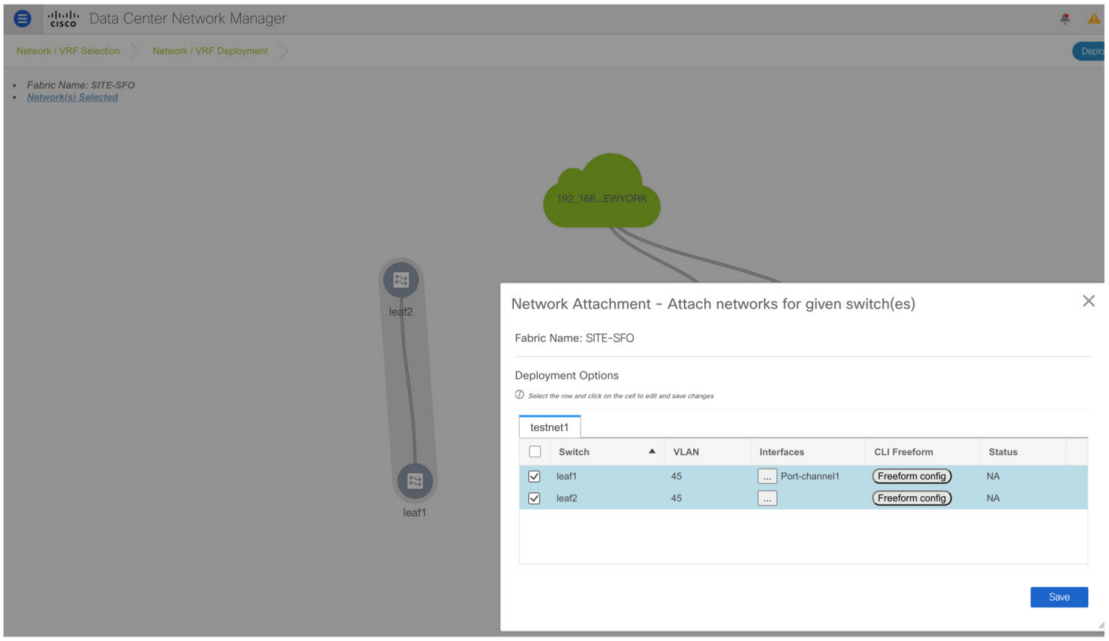
[プレビュー（Preview）] アクションと **[展開（Deploy）]** アクションは、どちらもデバイスが存在する必要があるため、結果を生成しません。vPC ホストインターフェイスが作成され、次のイメージで示すように、ステータスが **[未検出（Not discovered）]** と表示されます。



事前にプロビジョニングされたデバイスへのオーバーレイのアタッチ

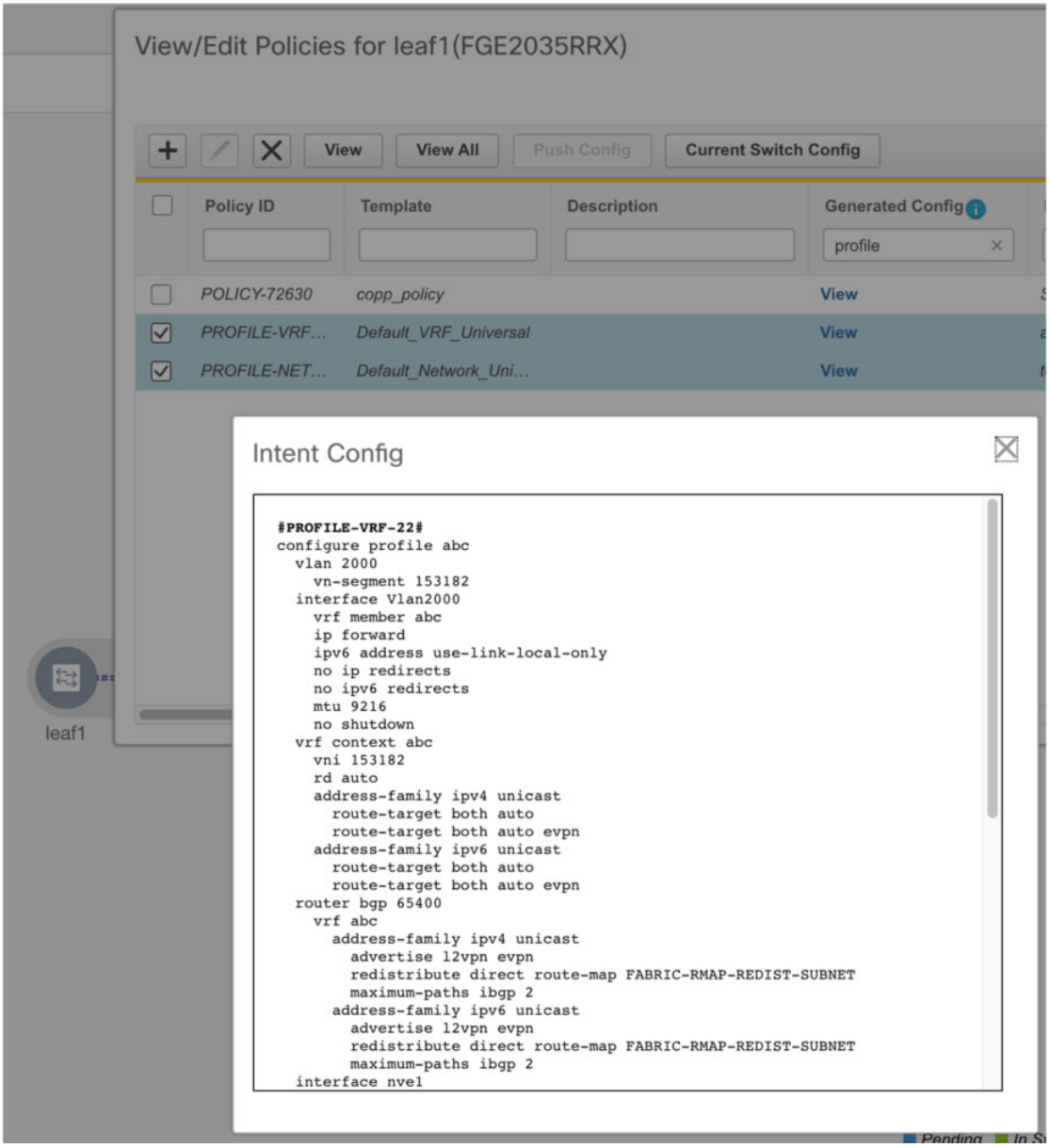
オーバーレイ VRF とネットワークは、他の検出されたデバイスと同様に、事前にプロビジョニングされたデバイスにアタッチできます。

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



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

次のイメージに示すように、**[ファブリック ビルダ（Fabric Builder）] > [ポリシーの表示/編集（View/Edit Policies）]** で、オーバーレイ ネットワーク/VRF アタッチメント情報を含む、事前にプロビジョニングされたデバイス用に生成されたインテント全体を表示できます。



Easy ファブリック向け高精度時間プロトコル

Easy_Fabric_11_1 テンプレートのファブリック設定で、**[高精度時間プロトコル（PTP）を有効化（Enable Precision Time Protocol（PTP）]** チェックボックスをオンにして、ファブリック全体でPTPを有効にします。このチェックボックスを選択すると、PTPはグローバルで、およびコア向きのインターフェイスで有効化されます。また、**[PTP ループバック ID（PTP Loopback Id）]** および **[PTP ドメイン ID（PTP Domain Id）]** フィールドは編集可能です。

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

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

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

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

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

PTP の構成例を次に示します。

```
feature ptp

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

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

interface Ethernet1/59 -> Core facing interface
  ptp

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

次のガイドラインは PTP で適用可能です。

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

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

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

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

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

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

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

DCNM のスーパー スパイン ロールのサポート

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

DCNM リリース 11.3(1) 以降では、スーパー スパインを使用した追加のインターコネクトのオプションがあります。スーパー スパインを介してインターコネクトされた同じ Easy ファブリック内に複数のスパイン リーフ POD を持つことができ、同じ IGP ドメインがスーパー スパインを含むすべての POD にまたがって拡張されます。このような展開では、BGP RR と RP（該当する場合）がスーパー スパイン レイヤでプロビジョニングされます。スパイン レイヤは、リーフとスーパー スパイン間の疑似相互接続になります。VTEP にボーダー機能がある場合は、オプションでスーパー スパインでホストできます。

DCNM では、次のスーパー スパインのロールがサポートされています。

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

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

DCNM のスーパー スパイン スイッチのロールの特徴は次のとおりです。

- **[Easy_Fabric_11_1]** テンプレートでのみサポートされています。
- スパインとボーダーにのみ接続できます。有効な接続は次のとおりです。
  - スパインからスーパー スパインへ
  - スパインからボーダー スーパー スパインおよびボーダー GW スーパー スパインへ

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

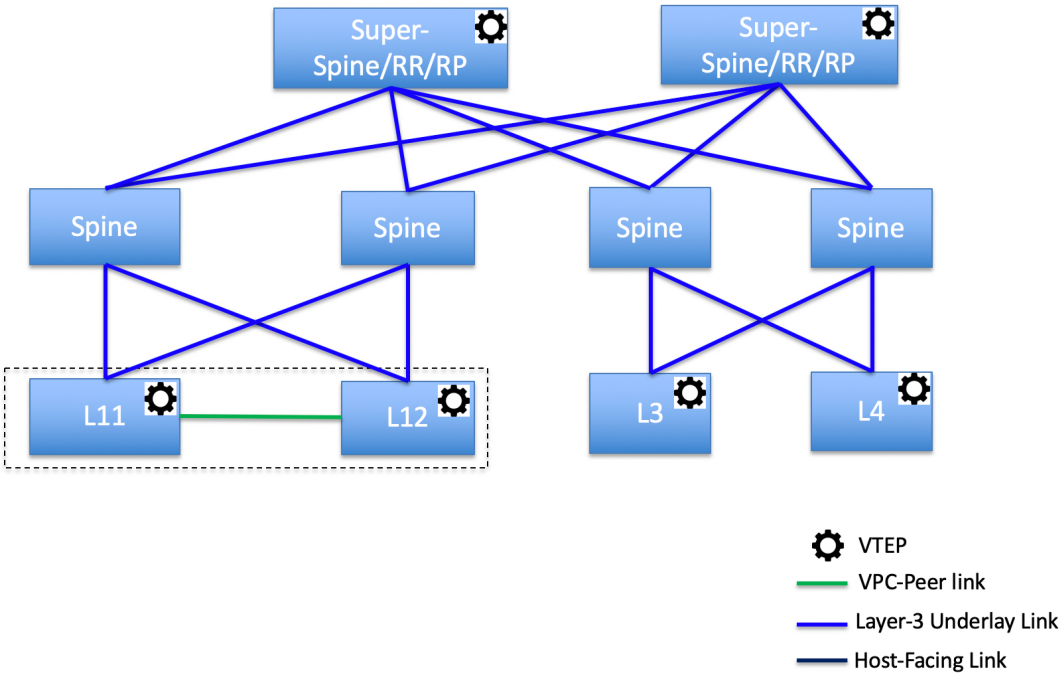
- RR または RP は、ファブリックに存在する場合、常にスーパー スパイン上で構成される必要があります。スーパー スパインでサポートされる RR および RP の数は 4 です。
- ボーダー スーパー スパインおよびボーダー GW スーパー スパインのロールは、ファブリック間接続でサポートされます。
- スーパー スパインでは vPC 構成はサポートされていません。
- スーパー スパインは IPv6 アンダーレイ構成をサポートしていません。
- スイッチにスーパースパイン ロールがある場合、スイッチのブラウンフィールドインポート中に、次のエラーが表示されます。

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

スーパー スパイン スイッチでサポートされるトポロジ

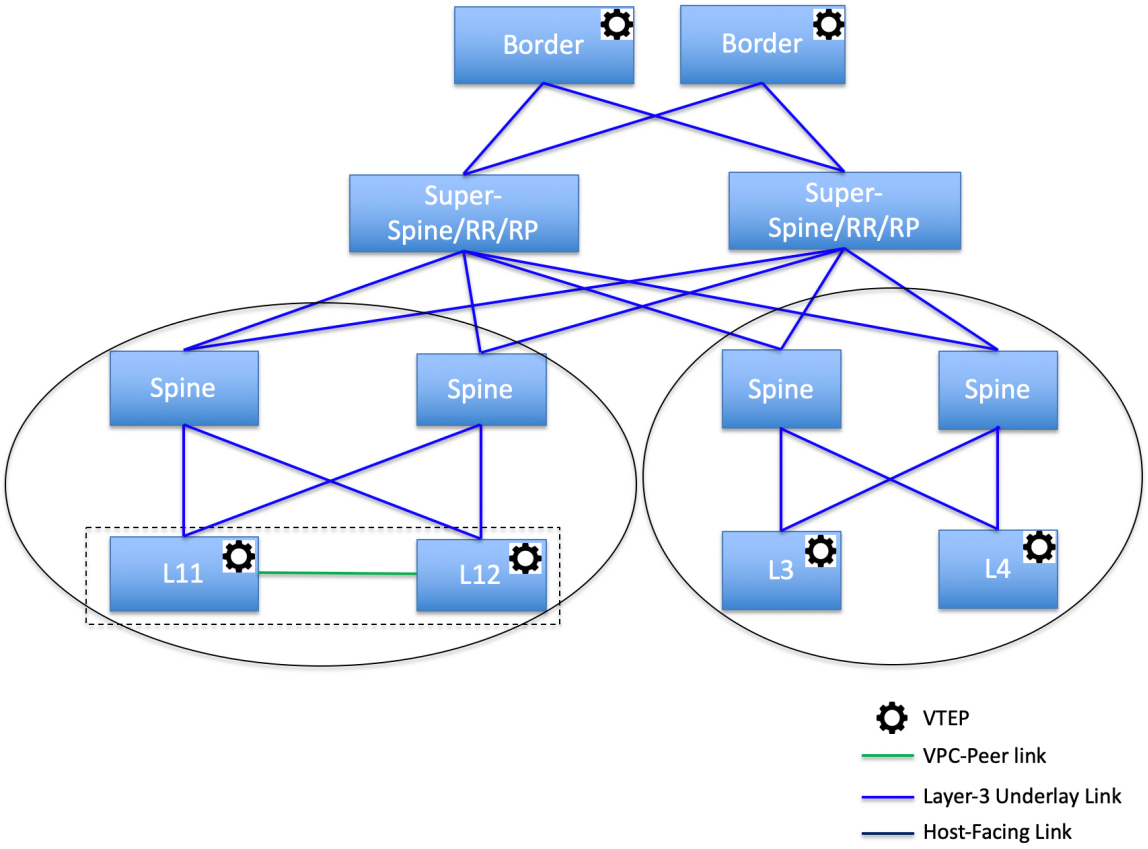
DCNM は、スーパー スパイン スイッチで次のトポロジをサポートします。

トポロジ 1：スパイン リーフ トポロジのスーパー スパイン スイッチ



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

トポロジ 2：ボーダーに接続されたスーパー スパイン スイッチ



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

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

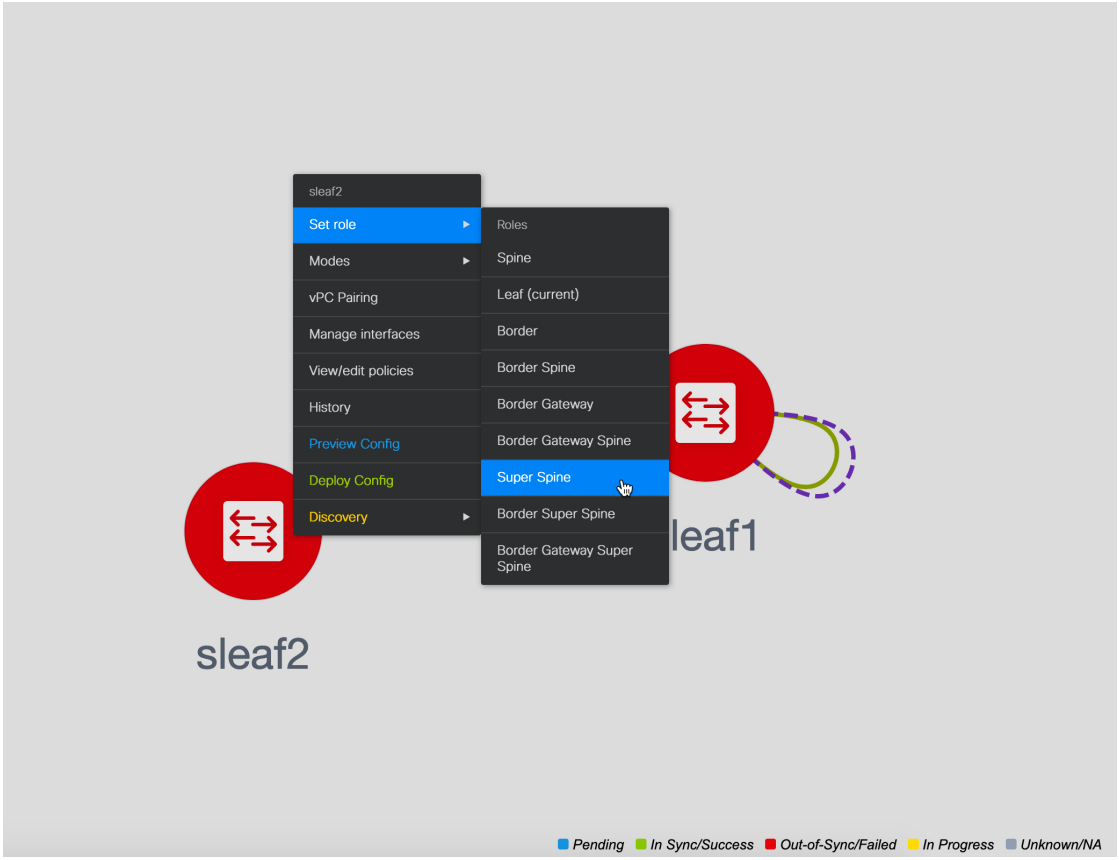
Procedure

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

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

詳細については、ファブリックへのスイッチの追加, on page 90を参照してください。

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



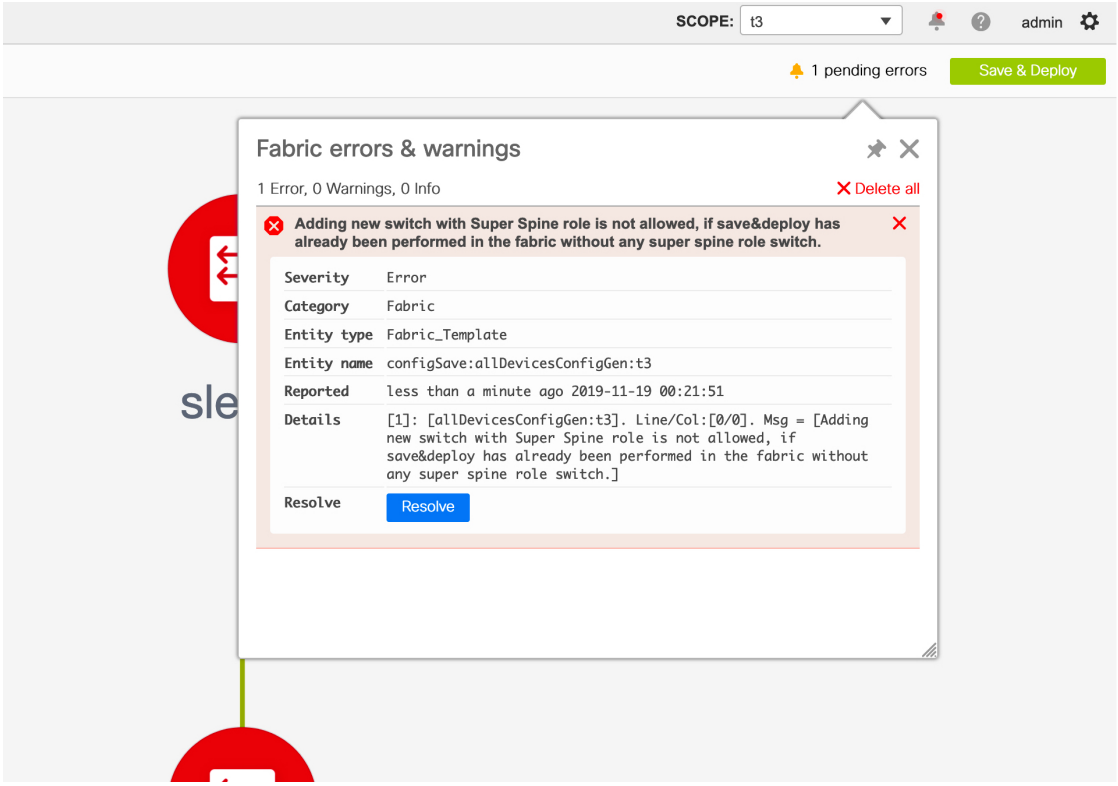
Note **[スーパー スパイン（Super Spine）]** ロールがファブリックに存在する場合、ファブリック内の他の可能なスパイン ロールは、ボーダー スーパー スパインまたはボーダー ゲートウェイ スーパー スパインです。ボーダー スパインまたはボーダー ゲートウェイ スパイン ロール (これらのスイッチ ロールにはスーパーが存在しない) が使用されている場合、[保存してデプロイ] をクリックした後にエラーが生成されます。ボーダー スパインとボーダーゲートウェイ スパインのロールが既存のファブリックにすでに存在する場合は、それらのスイッチを削除して、正しいボーダー スーパー スパイン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

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

次のエラーが表示されます。

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

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



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

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

デバイスでの TCAM 構成の変更

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

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

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

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

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

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

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

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

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

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

ルート リフレクタおよびランデブー ポイントとしてのスイッチの事前選択

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

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

手順

ステップ 1 スイッチが正常にインポートされました。

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

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

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

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

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

vPC L3 ピア キープアライブ リンクの追加

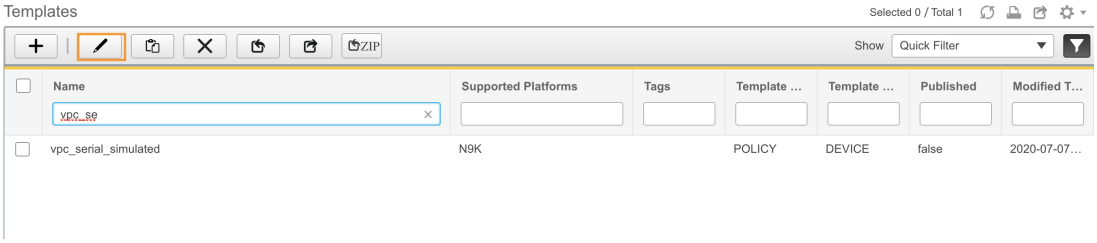
この手順は、vPC L3 ピア キープアライブ リンクを追加する方法を示しています。

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

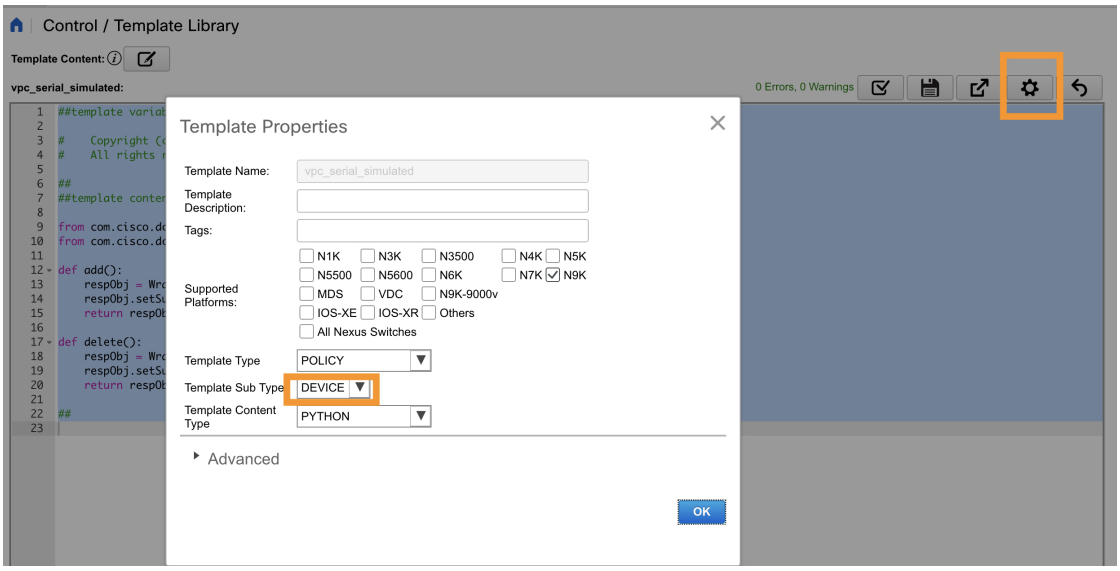
手順

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

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



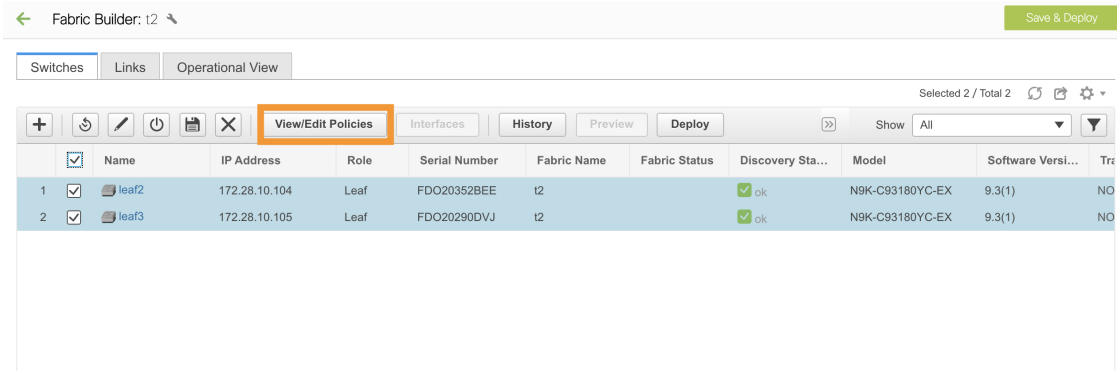
ステップ 3 テンプレート プロパティを編集し、**[テンプレート サブ タイプ（Template Sub Type）]** を **[デバイス（Device）]** に設定して、このポリシーが **[ポリシーの表示/編集（View/Edit Policies）]** に表示されるようにします。



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

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

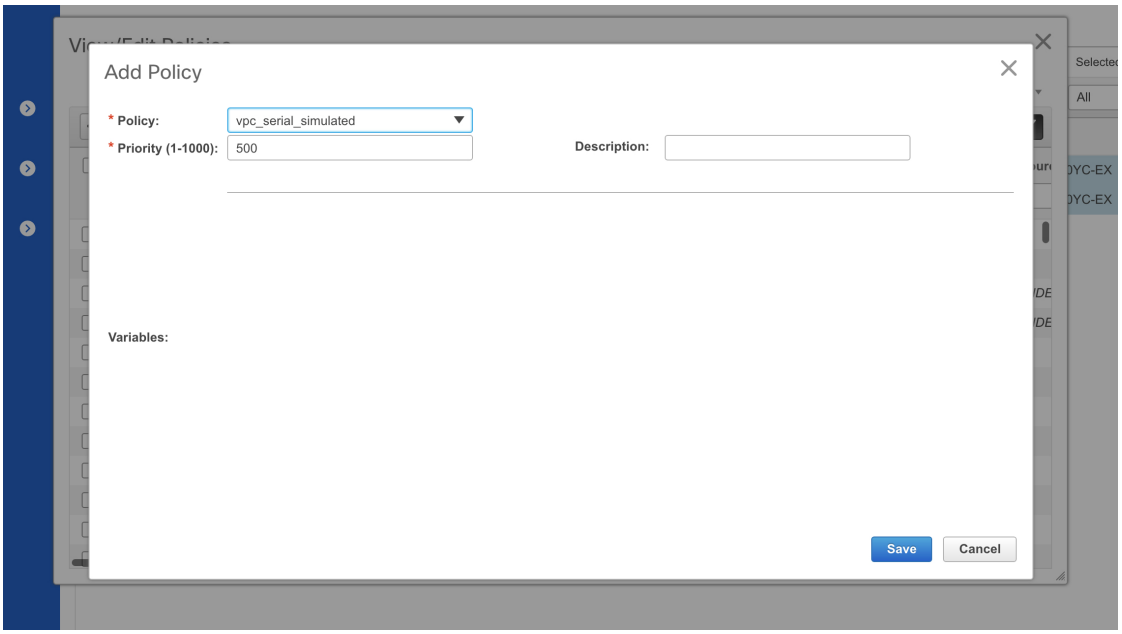
トポロジ内のスイッチを個別に右クリックして、**[ポリシーの表示/編集（View/Edit Policies）]** を選択することもできます。



ステップ 6 **[+]** をクリックしてポリシーを追加します。

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

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

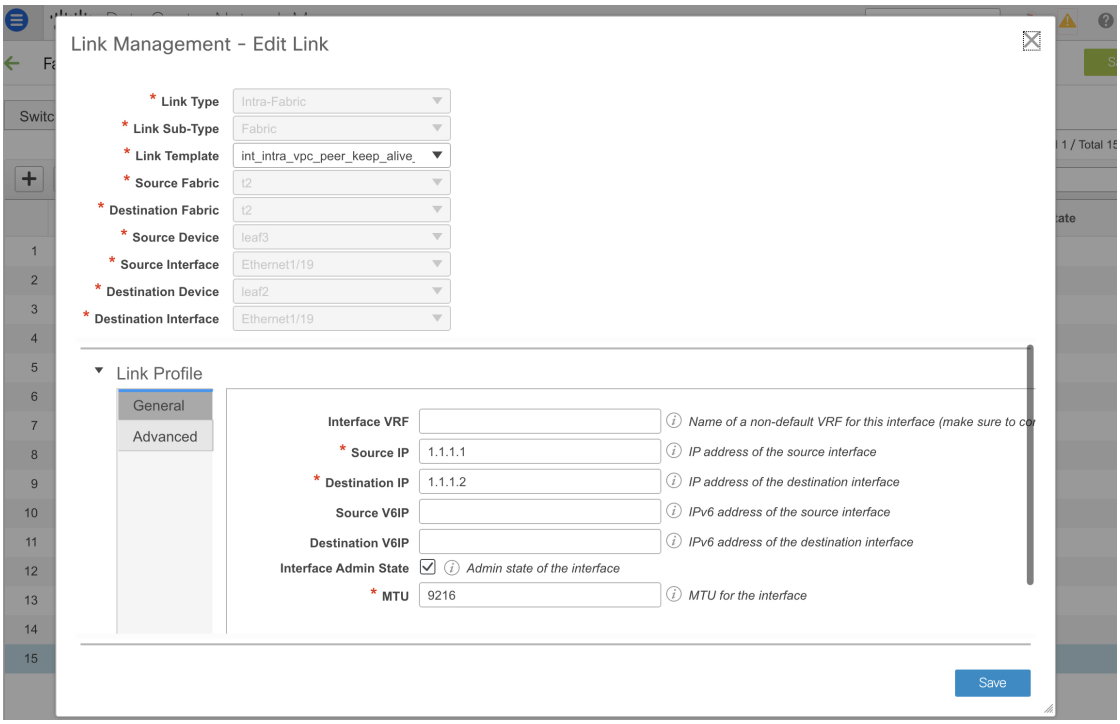


ステップ 8 **[表形式ビュー（Tabular View）]** に戻り、**[リンク（Links）]** タブをクリックします。

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

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

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

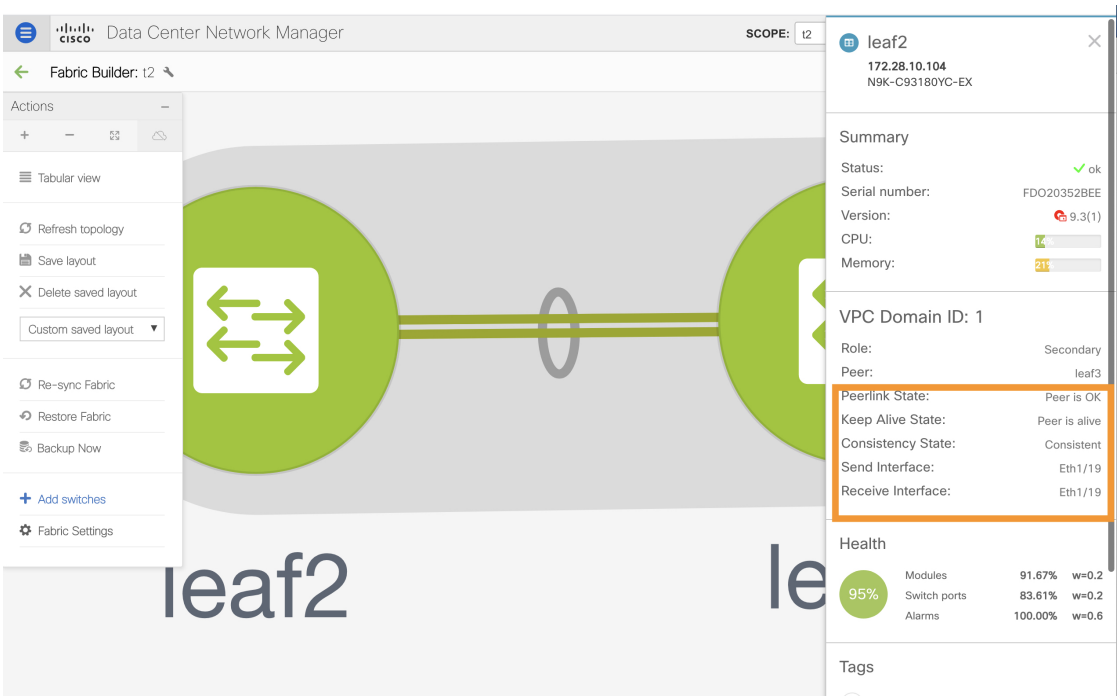


ステップ 11 **[保存と展開（Save & Deploy）]** をクリックし、いずれかのスイッチの **[構成のプレビュー（Preview Config）]** をクリックします。

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

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

トポロジに移動し、vPC ペア スイッチをクリックして詳細を表示します。

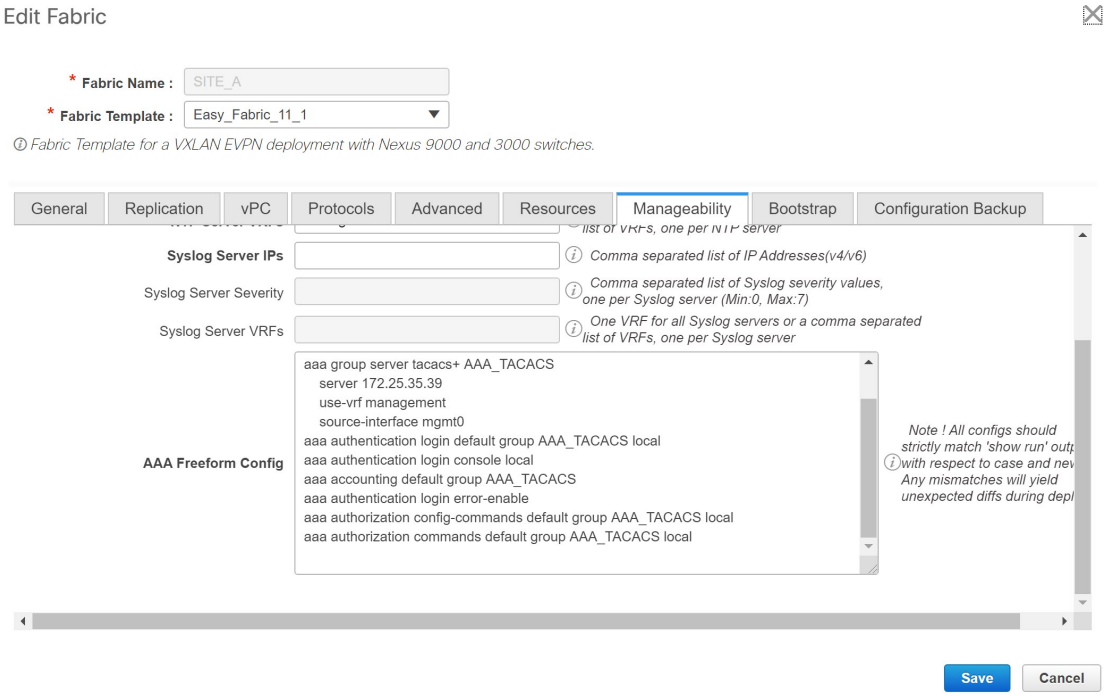


ファブリック内スイッチ向けのローカル認証を AAA 認証へ変更する

手順

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

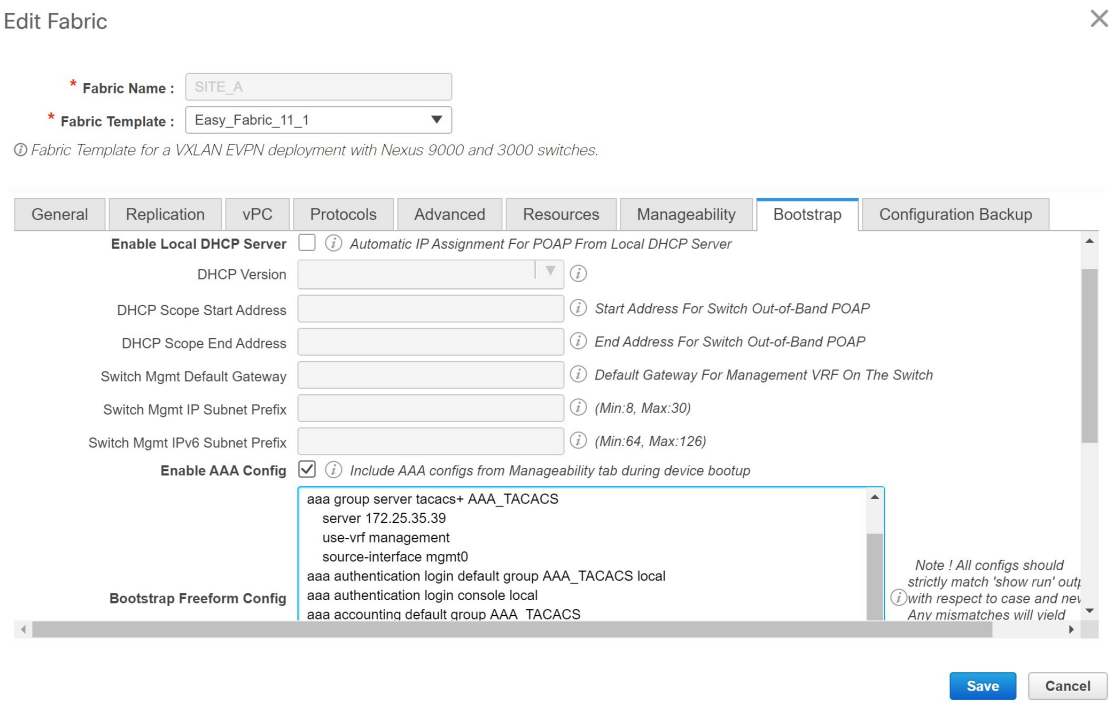
ステップ 2 ファブリックの **[編集（Edit）]** アイコンをクリックし、**[管理性（Manageability）]** タブの **[AAA 自由形式構成（AAA Freeform Config）]** フィールドに AAA 認証コマンドを追加します。



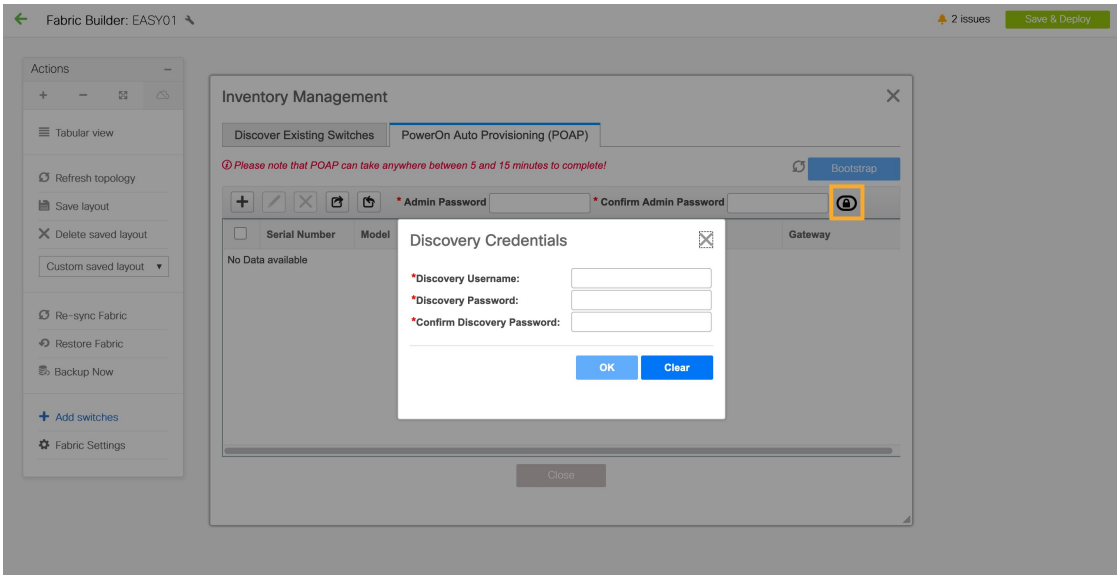
ステップ 3 **[ファブリック ビルダ（Fabric Builder）]** トポロジ ウィンドウで、**[スイッチの追加（Add Switches）]** をクリックします。このウィンドウの AAA ログイン情報を使用して、スイッチを DCNM に追加します。

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

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



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



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

Easy Fabric の IPv6 アンダーレイ サポート

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

ブラウンフィールド展開：VXLAN ファブリック管理から DCNMへの移行

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

eBGP アンダーレイを使用したファブリックの構成

Easy_Fabric_eBGP ファブリック テンプレートを使用して、eBGP アンダーレイを使用するファブリックを作成できます。詳細については、「BGP ベースのルーテッド ファブリックの管理, on page 1127」および「グリーンフィールド VXLAN BGP EVPN ファブリックの管理, on page 761」を参照してください。

外部ファブリックの作成

DCNM 11.1(1) リリースで、外部ファブリックにスイッチを追加できます。汎用ポインタ：

- 外部ファブリックは、モニタ専用または管理モードのファブリックです。DCNMは、Cisco IOS-XR ファミリ デバイスのモニタ モードのみをサポートします。
- 外部ファブリックのスイッチをインポート、削除、および削除できます。
- ファブリック間接続（IFC）の場合、外部ファブリックの宛先スイッチとしてCisco 9000、7000、および5600シリーズスイッチを選択できます。
- 存在しないスイッチを宛先スイッチとして使用できます。
- 外部ファブリックをサポートするテンプレートは、External_Fabricです。
- 外部ファブリックがMSDファブリックメンバーである場合、MSDトポロジ画面には、外部ファブリックとそのデバイス、およびメンバーファブリックとそのデバイスが表示されます。

  外部ファブリック トポロジ画面から表示すると、非 DCNM 管理対象スイッチへの接続はすべて、**[未検出（Undiscovered）]** というラベルの付いたクラウド アイコンで表されます。
- マルチサイトまたはVRF-lite IFCを設定するには、VXLANファブリック内の境界デバイスのリンクを手動で設定するか、または自動的にDeploy Border Gateway MethodまたはVRF

Lite IFC Deploy Methodを使用します。ボーダーデバイスのリンクを手動で設定する場合は、コアルータロールを使用してマルチゲートウェイeBGPアンダーレイをボーダーゲートウェイデバイスからコアルータに設定し、エッジルータロールを使用してVRF-Lite Interを設定することを推奨します。 -ボーダーデバイスからエッジデバイスへのファブリック接続（IFC）。

- Cisco Nexus 7000シリーズスイッチとCisco NX-OSリリース6.2（24a）をLANクラシックまたは外部ファブリックで使用している場合は、ファブリック設定でAAA IP認証を有効にしてください。
- 外部ファブリックでは、次の非Nexusデバイスを検出できます。
  - IOS-XEファミリ デバイス：Cisco CSR 1000v、Cisco IOS XE ジブラルタ 16.10.x、Cisco ASR 1000 シリーズ ルータ、および Cisco Catalyst 9000 シリーズ スイッチ
  - IOS-XRファミリデバイス：ASR 9000シリーズルータ、IOS XRリリース6.5.2およびCisco NCS 5500シリーズルータ、IOS XRリリース6.5.3
  - Arista 4.2（任意のモデル）
- 外部ファブリックに追加する前に、Cisco CSR 1000vを除くすべてのNexus以外のデバイスを設定します。
- Cisco DCNM リリース 11.4(1) 以降、非 Nexus デバイスをボーダーとして構成できます。外部ファブリックの非Nexusデバイスと簡易ファブリックのCisco Nexusデバイス間でIFCを作成できます。これらのデバイスでサポートされるインターフェイスは次のとおりです。
  - ルート化済み
  - サブインターフェイス
  - ループバック
- Cisco DCNM リリース 11.4(1) 以降、Cisco ASR 1000 シリーズ ルータおよび Cisco Catalyst 9000 シリーズ スイッチをエッジルータとして構成し、VRF-lite IFC を設定し、簡単なファブリックを使用してボーダー デバイスとして接続できます。
- VDCをリロードする前に、ファブリックで管理VDCを検出します。それ以外の場合、リロード操作は行われません。
- Cisco CSR 1000vを使用して、シスコデータセンターをパブリッククラウドに接続できます。使用例については、「Cisco Data Centerとパブリッククラウドの接続」の章を参照してください。
- 外部ファブリックでswitch_userポリシーを追加し、ユーザ名とパスワードを指定する場合、パスワードはshow runコマンドで表示される暗号化された文字列である必要があります。

  次に例を示します。

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

この場合、入力したパスワードは5 $ 5 $ I4sapkBh $ S7B7UcPH / iVTihLKH5sgldBeS3O2X1StQsvv3cmbYd1です。

- Cisco Network Insights for Resources（NIR）リリース2.1以降、およびフローテレメトリの場合、feature lldpコマンドは必須設定の1つです。

  シスコは、Easy Fabric 展開、つまり eBGP ルーテッド ファブリックまたは VXLAN EVPN ファブリックの場合にのみ、**lldp** 機能をスイッチにプッシュします。

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

  - モニタモードまたは管理モードの外部ファブリック
  - モニタモードまたは管理モードの LAN クラシック ファブリック（DCNM 11.4(1) 以降で該当）

ファブリック ビルダからの外部ファブリックの作成

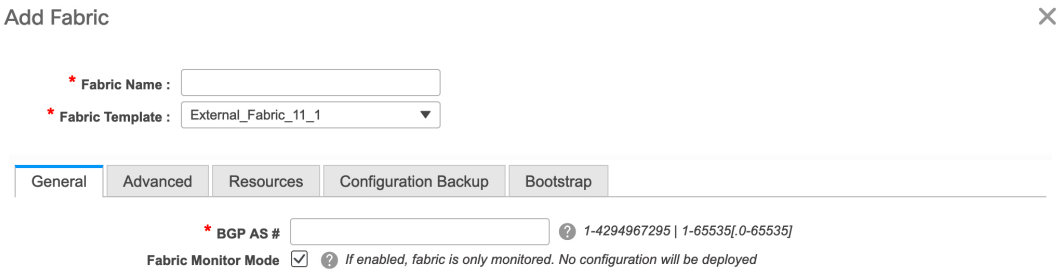
次の手順に従って、ファブリック ビルダから外部ファブリックを作成します。

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

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

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

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



[BGP AS #]：BGP AS番号を入力します。

[ファブリック モニタ モード（Fabric Monitor Mode）]：DCNM でファブリックを管理する場合は、このチェックボックスをオフにします。モニタ専用の外部ファブリックを有効にする場合には、チェックボックスをオンのままにします。DCNM は、Cisco IOS-XR ファミリ デバイスのモニタ モードのみをサポートします。

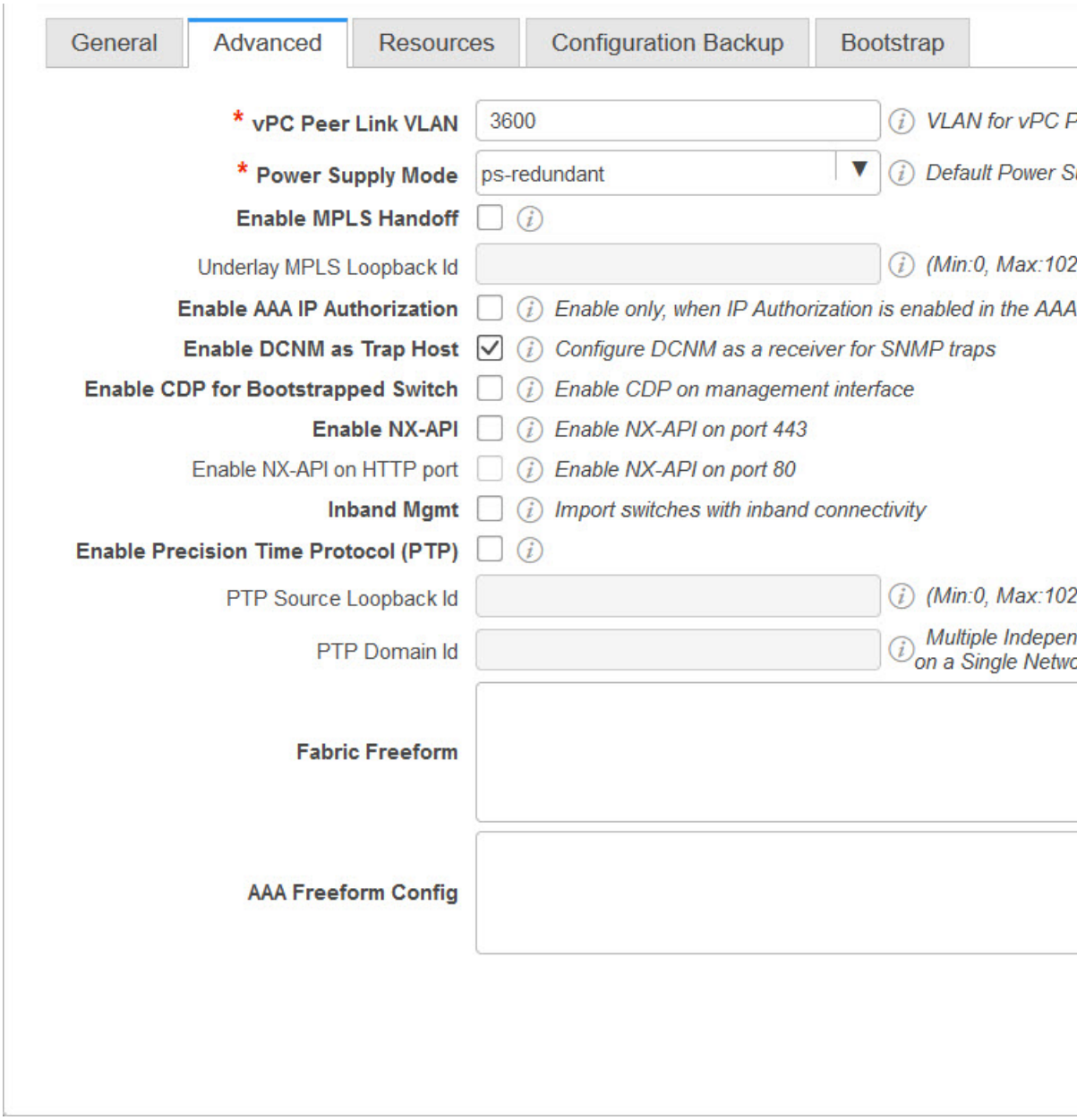
VXLANファブリックからこの外部ファブリックへのファブリック間接続を作成すると、BGP AS番号が外部またはネイバーファブリックAS番号として参照されます。

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

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

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

4. [詳細（Advanced）]タブのフィールドに値を入力します。



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

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

[MPLS ハンドオフの有効化（Enable MPLS Handoff）]：MPLS ハンドオフ機能を有効にするには、このチェックボックスをオンにします。詳細については、「VXLAN BGP EVPN ファブリックでの境界プロビジョニングの使用例：MPLS SR および LDP ハンドオフ」の章を参照してください。

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

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

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

[ブートストラップ スイッチの CDP を有効にする（Enable CDP for Bootstrapped Switch）]：チェックボックスをオンにして、ブートストラップ スイッチの CDP を有効にします。

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

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

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

[インバンド管理（Inband Mgmt）]：外部およびクラシック LAN ファブリックの場合、このノブを使用すると DCNM は、インバンド接続（スイッチ ループバック、ルーテッド、または SVI インターフェイス経由で到達可能）でのスイッチのインポートおよび管理が可能になり、またアウトオブバンド接続（つまり、スイッチ mgmt0 インターフェイス経由で到達可能）でのスイッチの管理が可能になります。唯一の要件は、インバンド管理型スイッチの場合、eth2（別名インバンド インターフェイス）を介して DCNM からスイッチ IP に到達可能であることです。この目的のために、DCNM で静的ルートが必要になる場合があります。これは、[管理（Administration）] > [カスタマイズ（Customization）] > [ネットワーク設定（Network Preferences）]オプションで構成できます。インバンド管理を有効にした後、検出中に、インバンド管理を使用してインポートするすべてのスイッチの IP を指定し、最大ホップ数を 0 に設定します。DCNM は、インバンド管理されたスイッチ IP が eth2 インターフェイスを介して到達可能であるかを検証する事前チェックを行います。事前チェックをパスすると、DCNM はインターフェイスが属する VRF に加えて、指定された検出 IP を持つそのスイッチ上のインターフェイスを検出し、学習します。スイッチのインポート/検出のプロセスの一部として、この情報は DCNM に入力される目的の基準設定にキャプチャされます。詳細については、外部ファブリックおよびLAN クラシック ファブリックでのインバンド管理, on page 223を参照してください。

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

[精密時間プロトコル（PTP）の有効化（Enable Precision Time Protocol（PTP））]：ファブリック全体で PTP を有効にします。このチェックボックスをオンにすると、PTP がグローバルに有効になり、コアに面するインターフェイスで有効になります。また、[PTP 送信元ループバック ID（PTP Source Loopback Id）] および [PTP ドメイン ID（PTP Domain Id）] フィールドが編集可能になります。詳細については、外部ファブリックおよび LAN クラシック ファブリック向け高精度時間プロトコル（PTP）, on page 224を参照してください。

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

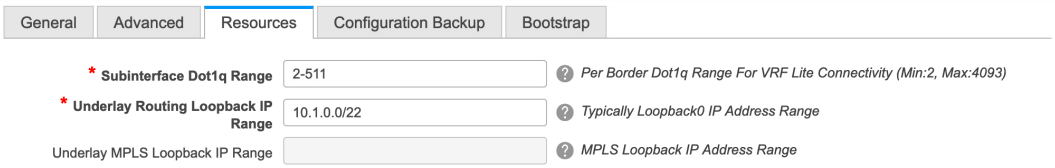
[PTP ドメイン ID（PTP Domain Id）]：単一のネットワーク上の PTP ドメイン ID を指定します。有効な値の範囲は 0 ～ 127 です。

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

- NX-OS
- IOS-XE
- IOS-XR
- その他

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

5. 次に示すように、[リソース（Resources）]タブに入力します。



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

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

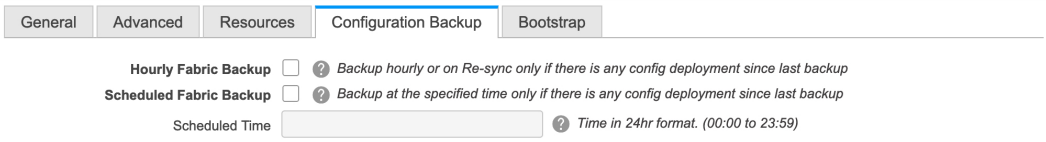
[アンダーレイ MPLS ループバック IP 範囲（Underlay MPLS Loopback IP Range）]：アンダーレイ MPLS SR または LDP ループバック IP アドレス範囲を指定します。

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

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

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

6. 次に示すように、[Configuration Backup]タブに入力します。



このタブのフィールドは次のとおりです。

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

新しいファブリック設定とインテントの1時間ごとのバックアップを有効にできます。前の時間に構成のプッシュがある場合、DCNM はバックアップを取得します。外部ファブリックの場合、VXLAN ファブリックと比較して、スイッチの構成全体が DCNM のインテントに変換されません。したがって、外部ファブリックでは、インテントと実行コンフィギュレーションの両方がバックアップされます。

インテントとは、DCNM に保存されているが、まだスイッチにプロビジョニングされていない構成を指します。

時間単位のバックアップは、その時間の最初の 10 分間にトリガーされます。

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

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

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

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

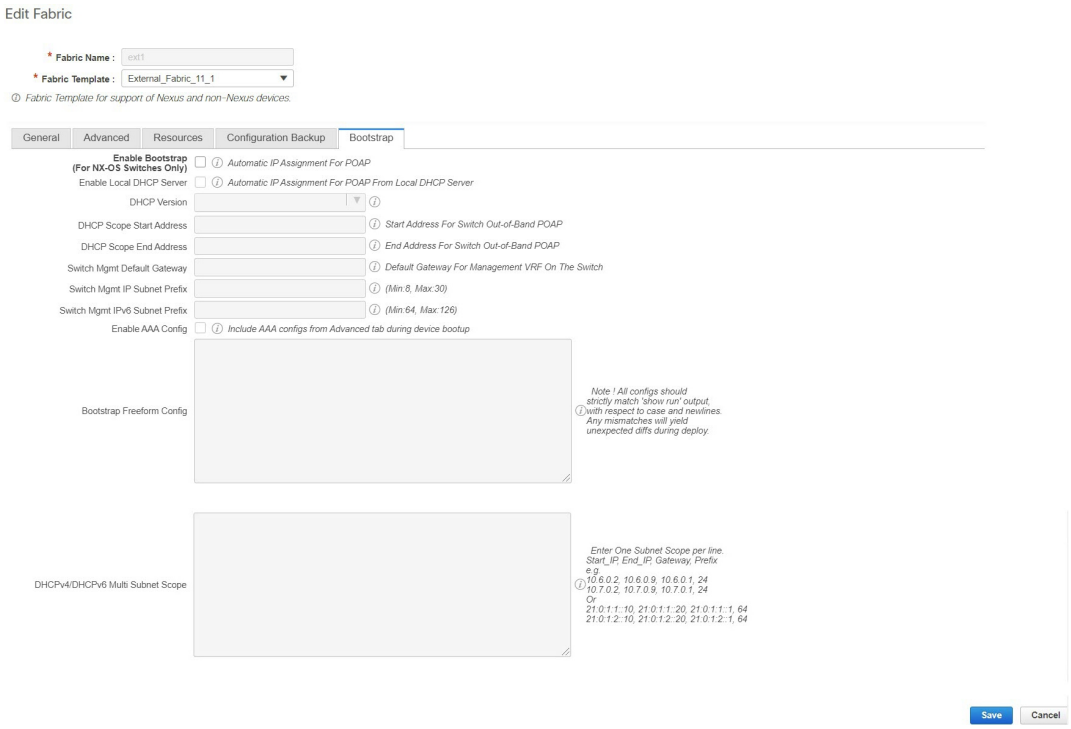
スケジュールされたバックアップは、指定した時刻に最大 2 分の遅延でトリガーされます。スケジュールされたバックアップは、構成の展開ステータスに関係なくトリガーされます。

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

毎時バックアップとスケジュール済みバックアップのポインタ：

- バックアップには、実行構成と DCNM によってプッシュされたインテントが含まれます。構成コンプライアンスは、実行構成が DCNM 構成と同じになるようにします。外部ファブリックでは、一部の構成のみがインテントの一部であり、残りの構成は DCNM によってトラックされないことに注意してください。したがって、バックアップの一部として、スイッチからの DCNM インテントと実行構成の両方がキャプチャされます。

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



[ブートストラップの有効化（Enable Bootstrap）]：このチェックボックスを選択し、ブートストラップ機能を有効にします。ブートストラップをイネーブルにした後、次のいずれかの方法を使用して、DHCP サーバで IP アドレスの自動割り当てをイネーブルにできます。

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

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

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

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

このチェックボックスをオンにしない場合、DCNM は自動 IP アドレス割り当てにリモートまたは外部DHCPサーバを使用します。

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

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

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

DHCP スコープおよび管理デフォルト ゲートウェイ *IP* アドレスの仕様（*DHCP scope and management default gateway IP address specification*）：管理デフォルト ゲートウェイ IP アド

レスを 10.0.1.1 に、サブネット マスクを 24 に指定した場合、DHCP スコープが指定したサブネット、10.0.1.2 ～ 10.0.1.254 の範囲内であることを確認してください。

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

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

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

NX-OSスイッチの実行コンフィギュレーションに示されているように、running-configを正しいインデントで自由形式の設定フィールドにコピーアンドペーストします。freeform config は running config と一致する必要があります。詳細については、スイッチのフリーフォーム設定エラーの解決, on page 411を参照してください。

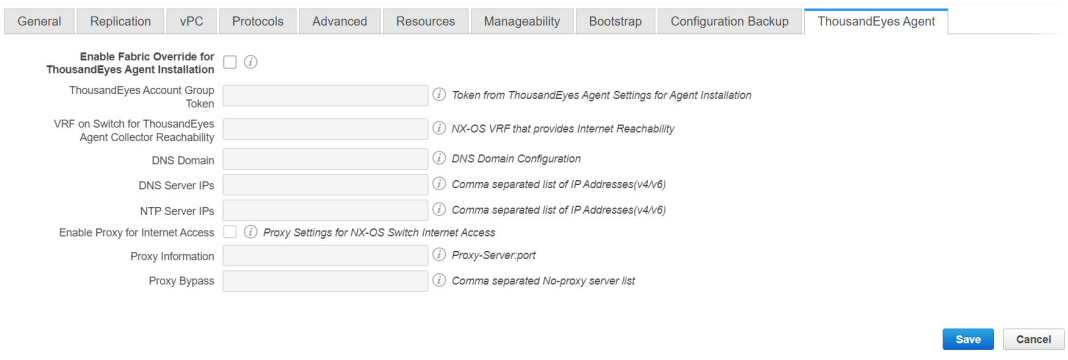
[DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）]：1 行に 1 つのサブネット スコープを入力して、フィールドを指定します。**[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）]**チェックボックスをオンにした後で、このフィールドは編集可能になります。

スコープの形式は次の順で定義する必要があります。

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

例：10.6.0.2、10.6.0.9、16.0.0.1、24

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



このタブのフィールドは次のとおりです。

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

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

9. **[Save（保存）]** をクリックします。

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

外部ファブリックを作成したら、スイッチを追加します。

外部ファブリックへのスイッチの追加

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

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

2. スイッチの IP アドレス（シード IP）を入力します。
3. **[デバイス タイプ（Device Type）]** ドロップダウン リストからデバイス タイプを選択します。

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

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

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

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

   Cisco CSR 1000v を除くすべての Nexus 以外のデバイスの設定コンプライアンスは無効です。
4. スイッチ管理者ユーザ名およびパスワードを入力します。
5. 画面の下部にある [検出の開始（Start discovery）] をクリックします。[スキャン詳細（Scan Details）] セクションが間もなく表示されます。[最大ホップ（Max Hops）] フィールドに 2 が入力されているため、指定された IP アドレスを持つスイッチとその 2 ホップのスイッチが入力されます。
6. 該当するスイッチの横にあるチェックボックスをオンにし、[ファブリックにインポート（Import into fabric）] をクリックします。

   複数のスイッチを同時に検出できます。スイッチは適切にケーブル接続し DCNM サーバーに接続する必要があり、スイッチのステータスは管理可能である必要があります。

   スイッチ検出プロセスが開始されます。[進行状況（Progress）] 列には、進行状況が表示されます。DCNM がスイッチを検出すると、画面が閉じ、ファブリック画面が再び表示されます。ファブリック画面の中央にスイッチ アイコンが表示されます。
7. 最新のトポロジ ビューを表示するには、[トポロジの更新（Refresh topology）] をクリックします。
8. 外部ファブリック スイッチの設定：外部ファブリック スイッチの設定は、VXLAN ファブリック スイッチの設定とは異なります。スイッチアイコンを右クリックして、スイッチ オプションを設定または更新します。

   次のオプションがあります。

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

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

モード：アクティブ/動作モード。

vPC ペアリング：vPC のスイッチを選択し、そのピアを選択します。

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

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

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

[履歴（History）]：スイッチごとの導入履歴を表示します。

[構成のプレビュー（Preview Config）]：保留中の構成と、実行中の構成と予想される構成の比較を表示します。

[展開設定（Deploy Config）]：スイッチ設定ごとに展開します。

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

9. 画面の右上にある [保存と展開（Save & Deploy）] をクリックします。テンプレートとインターフェイスの設定は、スイッチの設定を形成します。

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

10. 画面の下部にある [構成の展開（Deploy Config）] をクリックして、保留中の構成をスイッチに展開します。

11. 展開が完了したら、画面を閉じます。

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

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

MSDファブリックの下での外部ファブリックの移動

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

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

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

   右上の[Scope]ドロップダウンボックスで、MSDファブリックの下に外部ファブリックが表示されていることがわかります。
5. 画面の左上にある [←] をクリックして、ファブリック ビルダ画面に移動します。MSD ファブリック ボックスの [メンバー ファブリック（Member Fabrics）] フィールドに、外部ファブリックが表示されます。

MSDファブリックトポロジでの外部ファブリックの説明

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

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

外部ファブリック スイッチの操作

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

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

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

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

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

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

外部ファブリック リンク

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

外部ファブリックのリンクを削除するには、次の手順を実行します。

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

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

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

   リンクは削除されます。

ネイバー スイッチを外部ファブリックに移動

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

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

新しいスイッチの検出

新しいスイッチを検出するには、次の手順を実行します。

Procedure

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

Cisco NX-OS を起動し、スイッチのクレデンシャルを設定します。

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

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

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

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

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

[ファブリックの編集（Edit Fabric）] 画面が表示されます。

ステップ 5 **[ブートストラップ（Bootstrap）]** タブをクリックし、DHCP 情報を更新します。

ステップ 6 [ファブリックの編集（Edit Fabric）] 画面の右下の **[保存（Save）]** をクリックして、設定を保存します。

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

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

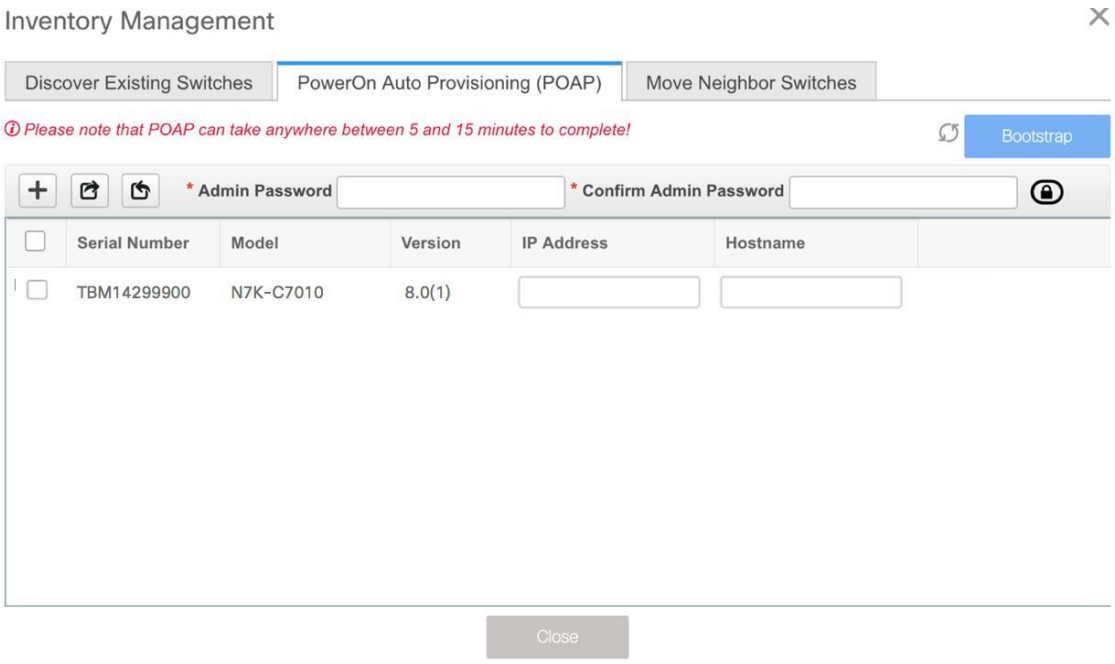
ステップ 8 ファブリック トポロジ画面で、画面の左側にある [アクション（Actions）] パネルから、**[スイッチの追加（Add switches）]** をクリックします。

インベントリ管理画面が表示されます。

ステップ 9 **[POAP]** タブをクリックします。

前の手順では、reload コマンドをスイッチで実行していました。スイッチが再起動してリブートすると、DCNM はスイッチからシリアル番号、モデル番号、およびバージョンを取得し、[インベントリ管理（Inventory Management）] 画面に表示します。また、管理 IP アドレス、ホスト名、およびパスワードを追加するオプションが使用可能になります。スイッチ情報が取得されない場合は、画面の右上にある [更新（Refresh）] アイコンを使用して画面を更新します。

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



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

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

リリース 11.2(1) 以降、事前にプロビジョニングデバイスが可能です。デバイスの事前プロビジョニングについては、デバイスの事前プロビジョニング , on page 104 を参照してください。

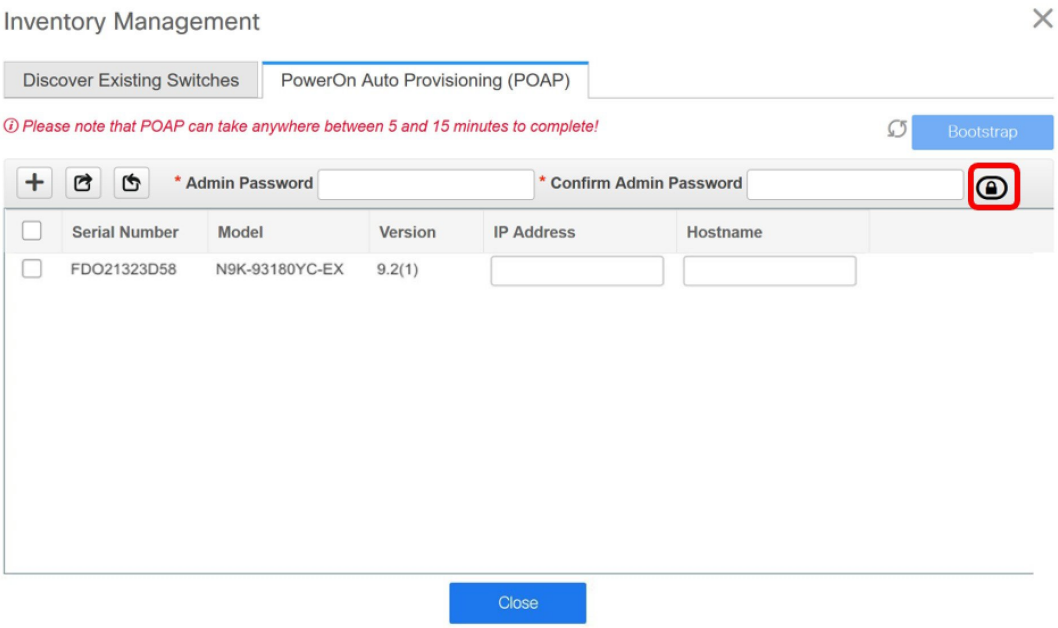
ステップ 10 **[管理者パスワード（Admin Password）]** フィールドと **[管理者パスワードの確認（Confirm Admin Password）]** フィールドに、新しいパスワードを入力します。

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

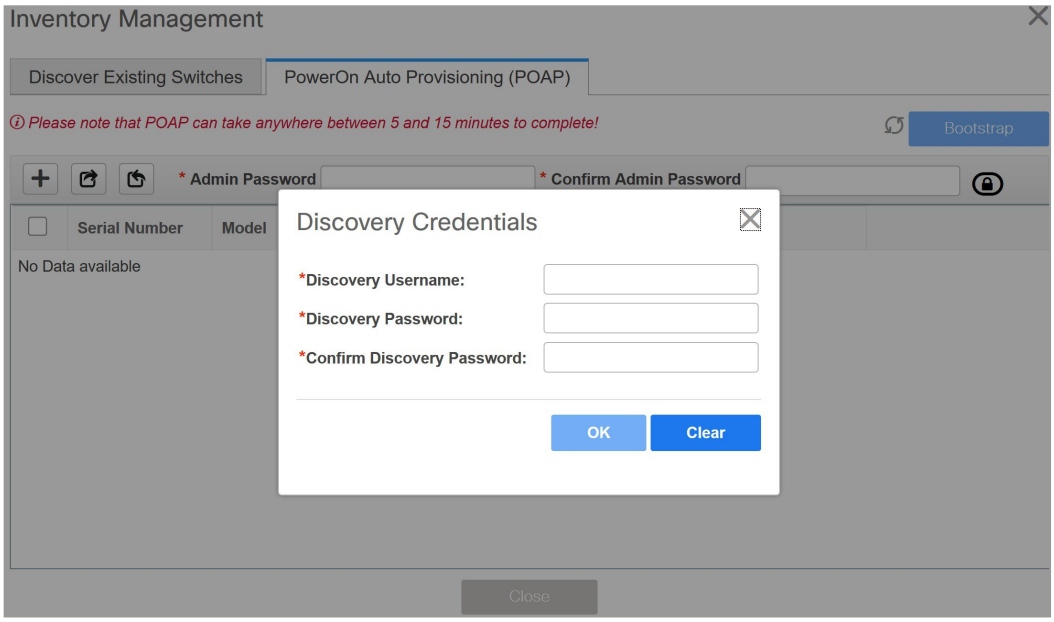
Note 管理者クレデンシャルを使用してスイッチを検出しない場合は、代わりに AAA 認証（RADIUS または TACACS クレデンシャル）を使用できます。

ステップ 11 (Optional) スイッチの検出に検出クレデンシャルを使用します。

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



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



[OK] をクリックして、ディスカバリ クレデンシャルを保存します。

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

Note

- 使用できるディスカバリクレデンシャルは、AAA認証ベースのクレデンシャル（RADIUS または TACACS）です。
- 検出クレデンシャルは、デバイス設定のコマンドに変換されません。このクレデンシャルは、主にスイッチを検出するリモート ユーザー（または管理ユーザー以外）を指定するために使用されます。デバイス設定の一部としてコマンドを追加する場合は、ファブリック設定の **[ブートストラップ（Bootstrap）]** タブにある **[ブートストラップ フリーフォーム設定（Bootstrap Freeform Config）]** フィールドにコマンドを追加します。また、**[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウからそれぞれのポリシーを追加できます。

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

DCNM は管理IPアドレスおよびその他のクレデンシャルをスイッチにプロビジョニングします。この単純化された POAP プロセスでは、すべてのポートが開かれます。

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

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

追加されたスイッチが POAP を完了すると、ファブリック ビルダー トポロジ画面に、追加されたスイッチと物理接続が表示されます。

ステップ 15 スイッチをモニタし、POAP 完了を確認します。

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

Note
- スイッチと DCNM の間に同期の問題がある場合、スイッチ アイコンが赤色で表示され、ファブリックが同期していないことを示します。ファブリックの変更が原因で同期が外れた場合は、変更を展開する必要があります。このプロセスは、「既存スイッチの検出」の項で説明したものと同じです。
- 検出クレデンシャルは、デバイス設定のコマンドに変換されません。このクレデンシャルは、主にスイッチを検出するリモートユーザー（または管理ユーザー以外）を指定するために使用されます。デバイス設定の一部としてコマンドを追加する場合は、ファブリック設定の **[ブートストラップ（Bootstrap）]** タブにある **[ブートストラップ フリーフォーム設定（Bootstrap Freeform Config）]** フィールドにコマンドを追加します。また、**[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウからそれぞれのポリシーを追加できます。

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

ステップ 17 保留中の設定が展開されると、すべてのスイッチの **[進捗（Progress）]** 列に 100％ と表示されます。

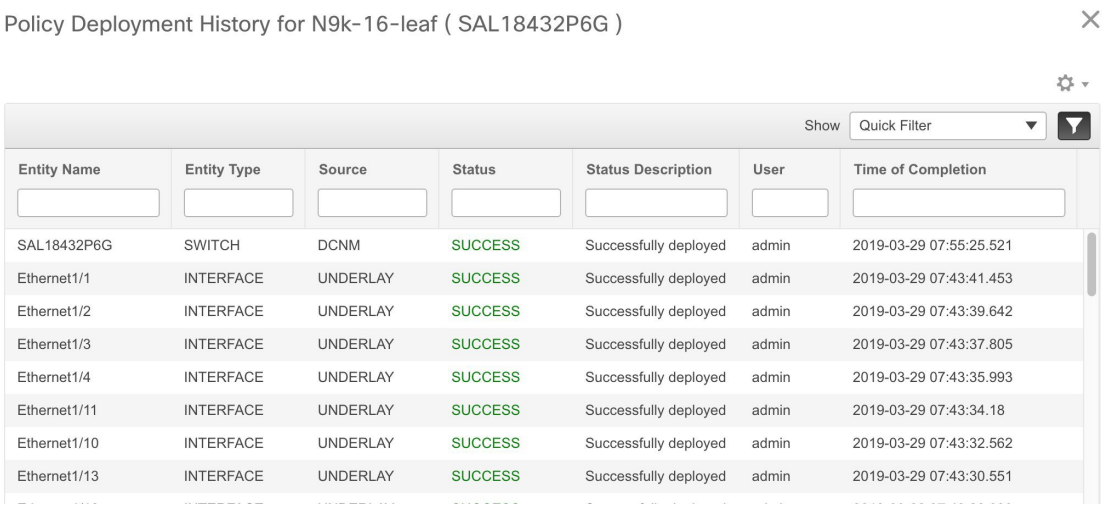
ステップ 18 **[閉じる（Close）]** をクリックして、ファブリック ビルダ トポロジに戻ります。

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

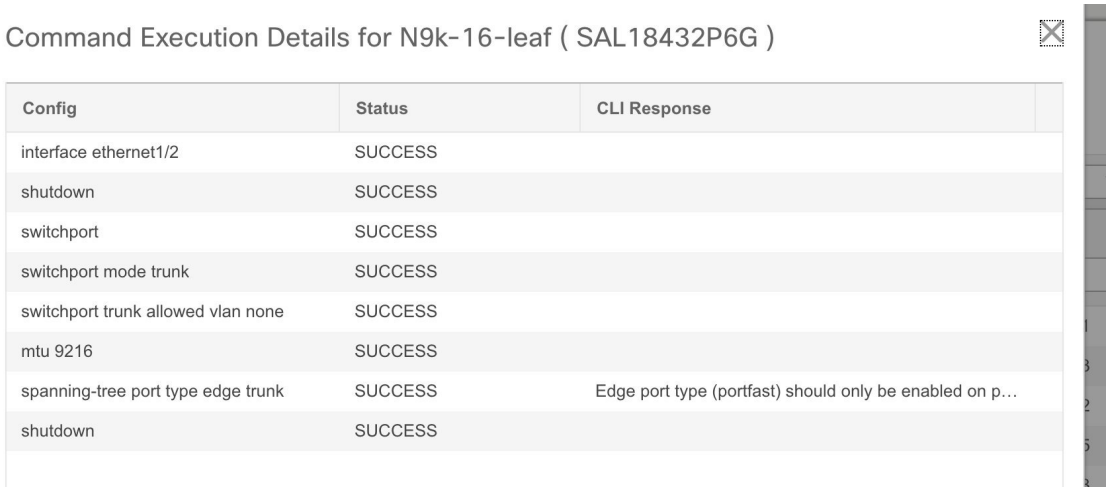
すべてのスイッチは、機能していることを示す緑色でなければなりません。

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

ステップ 20 展開された設定を表示するには、右クリックして [履歴（History）] を選択します。



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



ステップ 21 DCNM UIでは、検出されたスイッチはファブリック トポロジで確認できます。

このステップまでで、POAP の基本設定は完了です。すべてのインターフェイスがトランクポートに設定されます。追加構成を行うには、**[制御（Control）] > [インターフェイス（Interfaces）]** オプションを使用してインターフェイスを設定する必要があります。以下が含まれますが、これらに限定されません。

- vPC ペアリング。
- ブレークアウト インターフェイス

  ブレークアウトインターフェイスのサポートは、9000 シリーズスイッチで使用できます。
- ポート チャネル、およびポートへのメンバーの追加。

Note スイッチ（新規または既存）を検出した後は、いつでも、POAP プロセスを使用してスイッチの設定を再度プロビジョニングできます。このプロセスにより、既存の設定が削除され、新しい設定がプロビジョニングされます。また、POAP を呼び出さずに設定を段階的に展開することもできます。

非 Nexus デバイスを外部ファブリックに追加

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

デフォルトでは、Cisco Nexus スイッチのみが SNMP 検出をサポートします。したがって、すべての非 Nexus デバイスを外部ファブリックに追加する前に設定してください。非 Nexus デバイスの設定には、SNMP ビュー、グループ、およびユーザーの設定が含まれます。詳細については、「*Nexus*以外のデバイスの検出の設定」セクションを参照してください。

Cisco CSR 1000v は SSH を使用して検出されます。Cisco CSR 1000v は、SNMP がセキュリティ上の理由でブロックされているクラウドでもインストールできるため、SNMP のサポートは必要ありません。外部ファブリックに Cisco CSR 1000v、Cisco IOS XE Gibraltar 16.10.xを追加する使用例については、「*Cisco Data Center*とパブリッククラウドの接続」の章を参照してください。

ただし、Cisco DCNM がアクセスできるのは、システム名、シリアル番号、モデル、バージョン、インターフェイス、稼働時間などの基本的なデバイス情報に限られます。ホストが CDP または LLDP の一部である場合、Cisco DCNM は非 Nexus デバイスを検出しません。

ファブリックトポロジウィンドウで非Nexusデバイスを右クリックすると多くのオプションが表示されますが、非Nexus デバイスに適用されない設定は空白で表示されます。ASR 9000 シリーズ ルータおよび Arista スイッチのインターフェイスは追加または編集できません。

Cisco DCNM、リリース 11.4(1) 以降、Cisco Catalyst 9000 シリーズスイッチや Cisco ASR 1000 シリーズ ルータなどの IOS-XE デバイスは外部ファブリックに追加できます。

検出用非 Nexus デバイスの構成

Cisco DCNM で非 Nexus デバイスを検出する前に、スイッチ コンソールで構成します。

検出用の *IOS-XE* デバイスの設定

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

手順

ステップ 1 スイッチ コンソールで次の SSH コマンドを実行します。

```
switch (config)# hostname <hostname>
switch (config)# ip domain name <domain_name>
switch (config)# crypto key generate rsa
switch (config)# ip ssh time-out 90
switch (config)# ip ssh version 2
```

```
switch (config)# line vty 1 4
switch (config-line)# transport input ssh
switch (config)# aaa authentication login default local
switch (config)# aaa authorization exec default local none
switch (config)# username admin privilege secret <password>
switch (config)# aaa new-model
switch (config)# session-id-common
```

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

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

ステップ 3 スイッチ コンソールで次の SNMP コマンドを実行します。

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

検出用 *Arista* デバイスの構成

次のコマンドを使用して、特権 EXEC モードを有効化します。

```
switch> enable
switch#

switch# show running confiruation | grep aaa        /* to view the authorization*/
aaa authorization exec default local
```

Arista デバイスを構成するには、スイッチ コンソールで次のコマンドを実行します。

```
switch# configure terminal
switch (config)# username dcnm privilege 15 role network-admin secret cisco123
snmp-server view view_name SNMPv2 included
snmp-server view view_name SNMPv3 included
snmp-server view view_name default included
snmp-server view view_name entity included
snmp-server view view_name if included
snmp-server view view_name iso included
snmp-server view view_name lldp included
snmp-server view view_name system included
snmp-server view sys-view default included
snmp-server view sys-view ifmib included
snmp-server view sys-view system included
snmp-server community private ro
snmp-server community public ro
snmp-server group group_name v3 auth read view_name
snmp-server user username group_name v3 auth md5 password priv aes password
```

（注） SNMP パスワードはユーザ名のパスワードと同じにする必要があります。

[show run] コマンドを実行して設定を確認し、[show snmp view] コマンドを実行して SNMP ビューの出力を表示できます。

Show Run コマンド

```
switch (config)# snmp-server engineID local f5717f444ca824448b00
snmp-server view view_name SNMPv2 included
snmp-server view view_name SNMPv3 included
snmp-server view view_name default included
snmp-server view view_name entity included
snmp-server view view_name if included
snmp-server view view_name iso included
snmp-server view view_name lldp included
snmp-server view view_name system included
snmp-server view sys-view default included
snmp-server view sys-view ifmib included
snmp-server view sys-view system included
snmp-server community private ro
snmp-server community public ro
snmp-server group group_name v3 auth read view_name
snmp-server user user_name group_name v3 localized f5717f444ca824448b00 auth md5
be2eca3fc858b62b2128a963a2b49373 priv aes be2eca3fc858b62b2128a963a2b49373
!
spanning-tree mode mstp
!
service unsupported-transceiver labs f5047577
!
aaa authorization exec default local
!
no aaa root
!
username admin role network-admin secret sha512
$6$5ZKs/7.k2UxrWDg0$FOkdVQsBTnOquW/9AYx36YUBSPNLFdeuPIse9XgyHSdEOYXtPyT/0sMUYYdkMffuIjgn/d9rx/Do71XSbygSn/
username cvpadmin role network-admin secret sha512
$6$fLGFj/PUcuJT436i$Sj5G5c4y9cYjI/BZswjjmZW0J4npGrGqIyG3ZFk/ULza47Kz.d31q13jXA7iHM677gwqQbFSH2/3oQEaHRq08.
username dcnm privilege 15 role network-admin secret sha512
$6$M48PNrCdg2EITEdG$iiB880nvFQQlrWoZwOMzdt5EfkuCIraNqtEMRS0TJUhNKCQnJN.VDLFsLAmP7kQBo.C3ct4/.n.2eRlcP6hij/
```

Show SNMP View コマンド

```
configure terminal# show snmp view
view_name SNMPv2 - included
view_name SNMPv3 - included
view_name default - included
view_name entity - included
view_name if - included
view_name iso - included
view_name lldp - included
view_name system - included
sys-view default - included
sys-view ifmib - included
sys-view system - included
leaf3-7050sx#show snmp user

User name : user_name
Security model : v3
Engine ID : f5717f444ca824448b00
Authentication : MD5
Privacy : AES-128
Group : group_name
```

検出用 *Cisco IOS-XR* デバイスの構成

IOS-XR デバイスを構成するには、スイッチ コンソールで次のコマンドを実行します。

```
switch# configure terminal
switch (config)# snmp-server view view_name cisco included
snmp-server view view_name mib-2 included
snmp-server group group_name v3 auth read view_name write view_name
snmp-server user user_name group_name v3 auth md5 password priv des56 password SystemOwner
```

（注） SNMP パスワードはユーザ名のパスワードと同じにする必要があります。

構成を確認するには、show run コマンドを実行します。

Cisco IOS-XR デバイスの構成と確認

```
RP/0/RSP0/CPU0:ios(config)#snmp-server view view_name cisco included
RP/0/RSP0/CPU0:ios(config)#snmp-server view view_name mib-2 included
RP/0/RSP0/CPU0:ios(config)#snmp-server group group_name v3 auth read view_name write
view_name
RP/0/RSP0/CPU0:ios(config)#snmp-server user user_name group_name v3 auth md5 password
priv des56 password SystemOwner
RP/0/RSP0/CPU0:ios(config)#commit Day MMM DD HH:MM:SS Timezone
RP/0/RSP0/CPU0:ios(config)#
RP/0/RSP0/CPU0:ios(config)#show run snmp-server Day MMM DD HH:MM:SS Timezone snmp-server
 user user_name group1 v3 auth md5 encrypted 10400B0F3A4640585851 priv des56 encrypted
000A11103B0A59555B74 SystemOwner
snmp-server view view_name cisco included
snmp-server view view_name mib-2 included
snmp-server group group_name v3 auth read view_name write view_name
```

外部ファブリックで非 Nexus デバイスの検出

ファブリック トポロジ ウィンドウで外部ファブリックに非 Nexus デバイスを追加するには、次の手順を実行します。

始める前に

外部ファブリックに追加する前に、非Nexusのデバイスの設定がプッシュされていることを確認します。モニタ モードでは、ファブリックの設定をプッシュできません。

手順

ステップ 1 [アクション（Actions）] ペインで [スイッチの追加（Add switches）] をクリックします。

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

ステップ 2 [既存スイッチの検出（Discover Existing Switches）] タブの次のフィールドに値を入力します。

フィールド	説明
シードIP	スイッチの IP アドレスを入力します。 IP アドレスの範囲を入力することにより、複数のスイッチをインポートできます。たとえば、10.10.10.40 ～ 60 スイッチは適切にケーブル接続しDCNMサーバーに接続する必要があり、スイッチのステータスは管理可能である必要があります。
デバイス タイプ	• Cisco CSR 1000v、Cisco ASR 1000 シリーズ ルータ、または Cisco Catalyst 9000 シリーズ スイッチを追加するには、ドロップダウンリストから [IOS XE] を選択します。 • Cisco NCS 5500 シリーズ ルータ、IOS XR リリース 6.5.3 を追加するには、ドロップダウンリストから **[IOS XR]** を選択します。 • シスコ以外のデバイス（Arista スイッチなど）を追加するには、ドロップダウンリストから [その他（Other）] を選択します。
ユーザ名	ユーザ名を入力します。
[パスワード（Password）]	パスワードを入力します。

（注） すでに検出されているデバイスを検出しようとすると、エラーメッセージが表示されます。

パスワードが設定されていない場合は、[LAN クレデンシャル（LAN Credentials）] ウィンドウでデバイスのパスワードを設定します。Cisco DCNM Web UI から **[LAN ログイン情報（LAN Credentials）]** ウィンドウに移動するには、**[管理（Administration）] > [LAN ログイン情報（LAN Credentials）]** を選択します。

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

[詳細のスキャン（Scan Details）] セクションが表示され、スイッチの詳細が入力されます。

ステップ 4 インポートするスイッチに隣接するチェックボックスをオンにします。

ステップ 5 [ファブリックにインポート（Import into fabric）] をクリックします。

スイッチ検出プロセスが開始されます。**[進行状況（Progress）]** 列には、進行状況が表示されます。

デバイスの検出には時間がかかります。検出の進行状況が [100%] または [完了（done）] になった後、デバイスの検出に関するポップアップ メッセージが右下に表示されます。次に例を示します。[<ip-address> 検出用に追加されました。（<ip-address> added for discovery.）]

ステップ 6 [閉じる（Close）] をクリックします。

ファブリック トポロジ ウィンドウにスイッチが表示されます。

ステップ 7 （任意） 最新のトポロジ ビューを表示するには、**[トポロジの更新（Refresh topology）]** をクリックします。

ステップ 8 （任意） **[アクション（Actions）]** ペインで **[表形式ビュー（Tabular view）]** をクリックします。

スイッチとリンクのウィンドウが表示され、スキャンの詳細を確認できます。検出が進行中の場合、検出ステータスは赤色の [検出中（discovering）] でありその横に警告アイコンが表示されます。

ステップ 9 （任意） デバイスの詳細を表示します。

デバイスの検出後：

- 検出ステータスが緑色の [OK] に変わり、横のチェックボックスがオンになります。
- [ファブリック ステータス（Fabric Status）] 列のデバイスの値が [同期中（In-Sync）] に変わります。

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

次のタスク

適切なロールを設定します。デバイスを右クリックし、[ロールの設定（Set role）] を選択します。

デバイスの事前プロビジョニング

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

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

- 事前プロビジョニングされたデバイスは、DCNM で次の構成をサポートします。
  - 基本管理
  - vPC ペアリング

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

- 事前プロビジョニングされたデバイスは、DCNM で次の構成をサポートしません。
  - ファブリック間リンク
  - Sub-interface
  - インターフェイス ブレークアウト構成

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

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

  [データ（Data）] フィールドの値の例を次に示します。
  - {"modulesModel": ["N9K-C93180LC-EX"], "gateway": "10.1.1.1/24"}

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

Procedure

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

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

ステップ 2 ファブリック ボックス内をクリックします。

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

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

ステップ 4 **[POAP]** タブをクリックします。

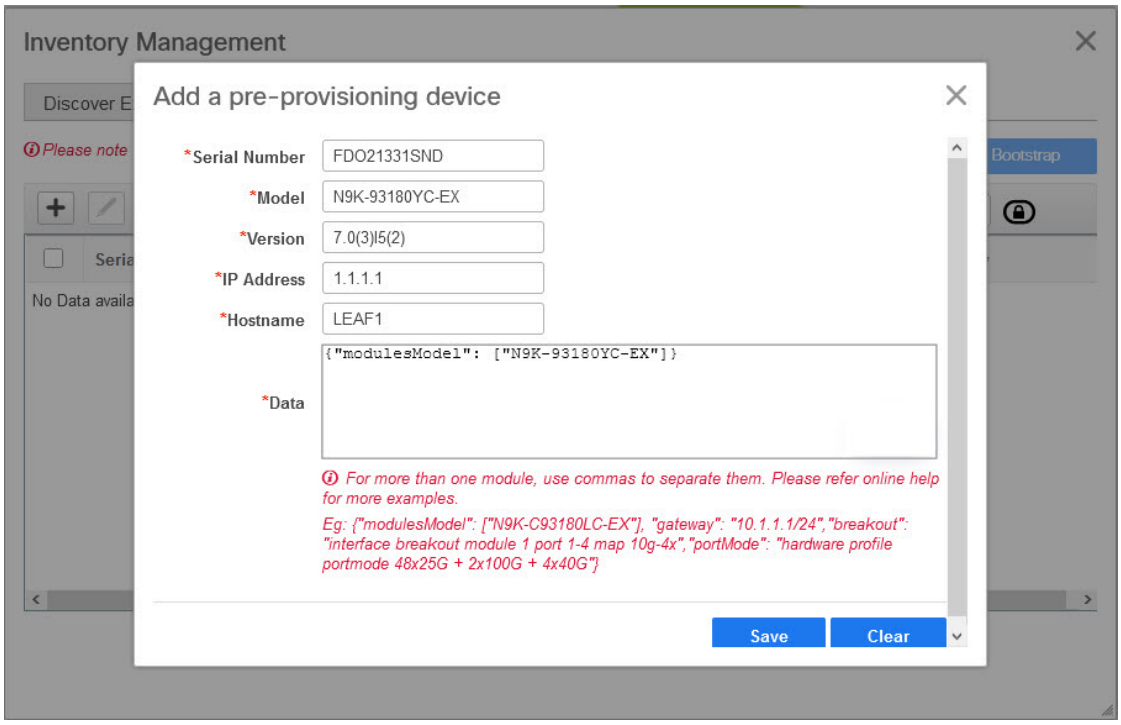
ステップ 5 **[POAP]** タブで、次の手順を実行します。

a. 画面左上の [+] をクリックします。

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

b. スクリーンショットに示されているように、デバイスの詳細を入力します。

c. [保存（Save）] をクリックします。



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

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

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

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

ウィンドウの左上には、スイッチ情報を含む .csv ファイルをエクスポートおよびインポートするための **[エクスポート（Export）]** および **[インポート（Import）]** アイコンがあります。

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

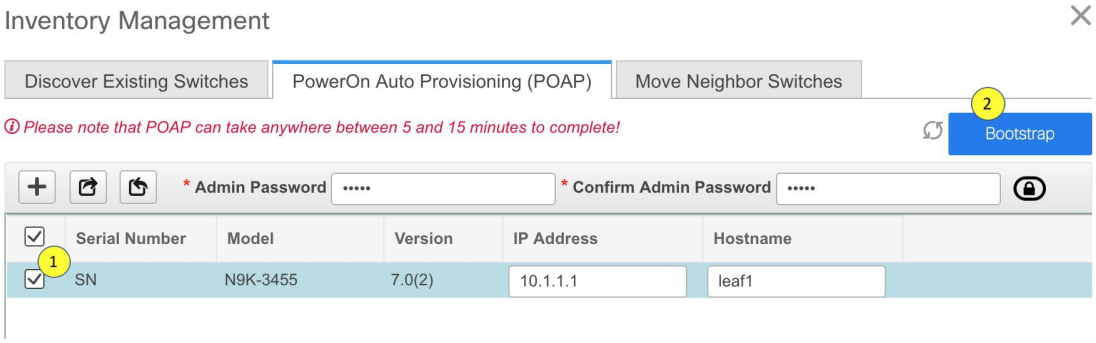
すべての必須フィールド（シリアル番号、モデル、バージョン、IpAddress、ホスト名、およびデータ フィールド [JSON オブジェクト]）を使用して、.csv ファイルに新しいデバイスの情報を追加します。

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

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

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

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



Leaf1 デバイスがファブリック トポロジに表示されます。

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

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

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

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

次のいずれかのテンプレートを使用して、リンク内ポリシーを作成します。

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

[保存して展開（Save & Deploy）] をクリックします。

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

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

詳細については、返品許可（RMA）, on page 304を参照してください。

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

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

イーサネット インターフェイスの事前プロビジョニング

DCNM リリース 11.4(1) 以降、**[インターフェイス（Interface）]** ウィンドウでイーサネット インターフェイスを事前プロビジョニングできます。この事前プロビジョニング機能は、Easy、外部、およびeBGPファブリックでサポートされています。DCNMで検出される前に、事前にプロビジョニングされたデバイスにのみ、イーサネット インターフェイスを追加できます。

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

始める前に

ファブリックに事前にプロビジョニングされたデバイスがあることを確認してください。詳細については、デバイスの事前プロビジョニング （104 ページ）を参照してください。

手順

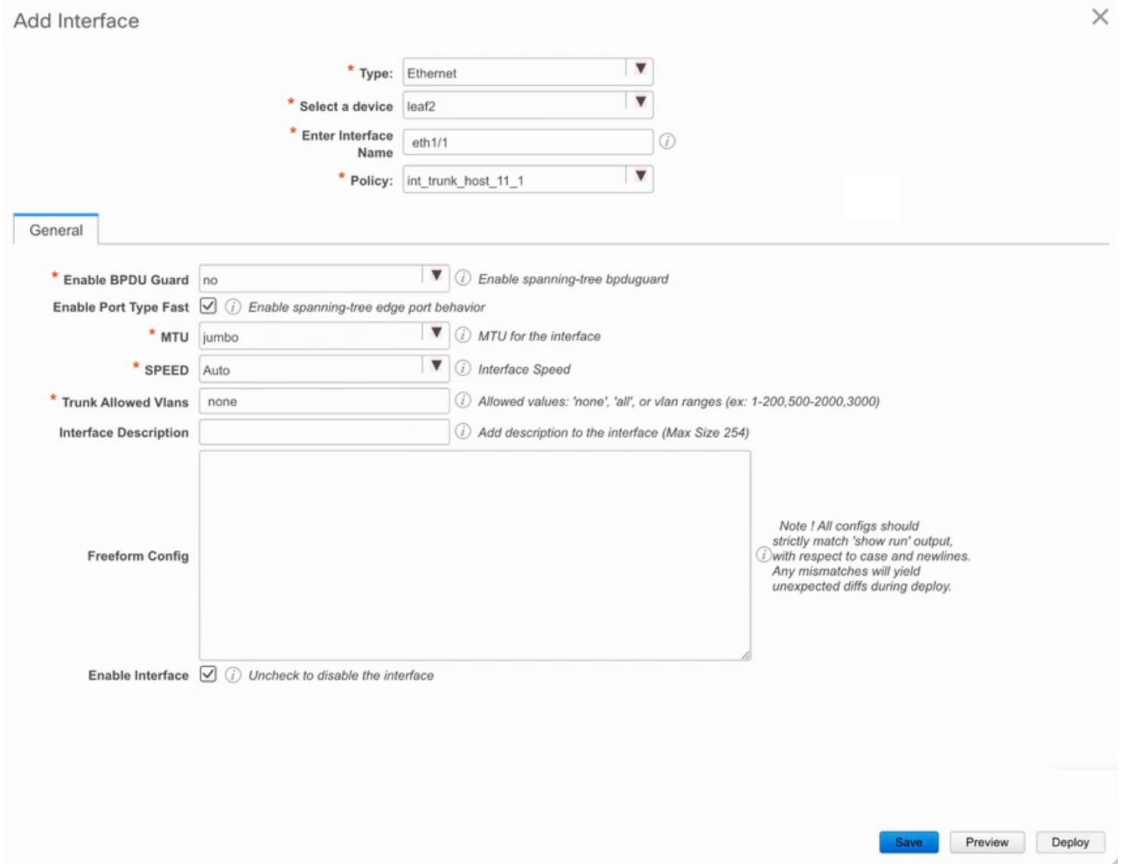
ステップ 1 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウから事前にプロビジョニングされたデバイスを含むファブリックに移動します。

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

[制御（Control）] > [ファブリック（Fabrics）] > [インターフェイス（Interfaces）] を選択して、[インターフェイス（Interfaces）] ウィンドウに移動することもできます。[範囲（Scope）] ドロップダウンリストから、事前にプロビジョニングされたデバイスを含むファブリックを選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 **[インターフェイスの追加（Add Interface）]** ウィンドウで、必要なすべての詳細を入力します。



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

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

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

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

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

詳細については、インターフェイスの追加 （316 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 **[プレビュー（Preview）]** をクリックして、追加後にスイッチに展開される予定の構成を確認します。

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

vPC セットアップの作成

外部ファブリック内のスイッチのペアに対してvPCセットアップを作成できます。スイッチの役割が同じで、相互に接続されていることを確認します。

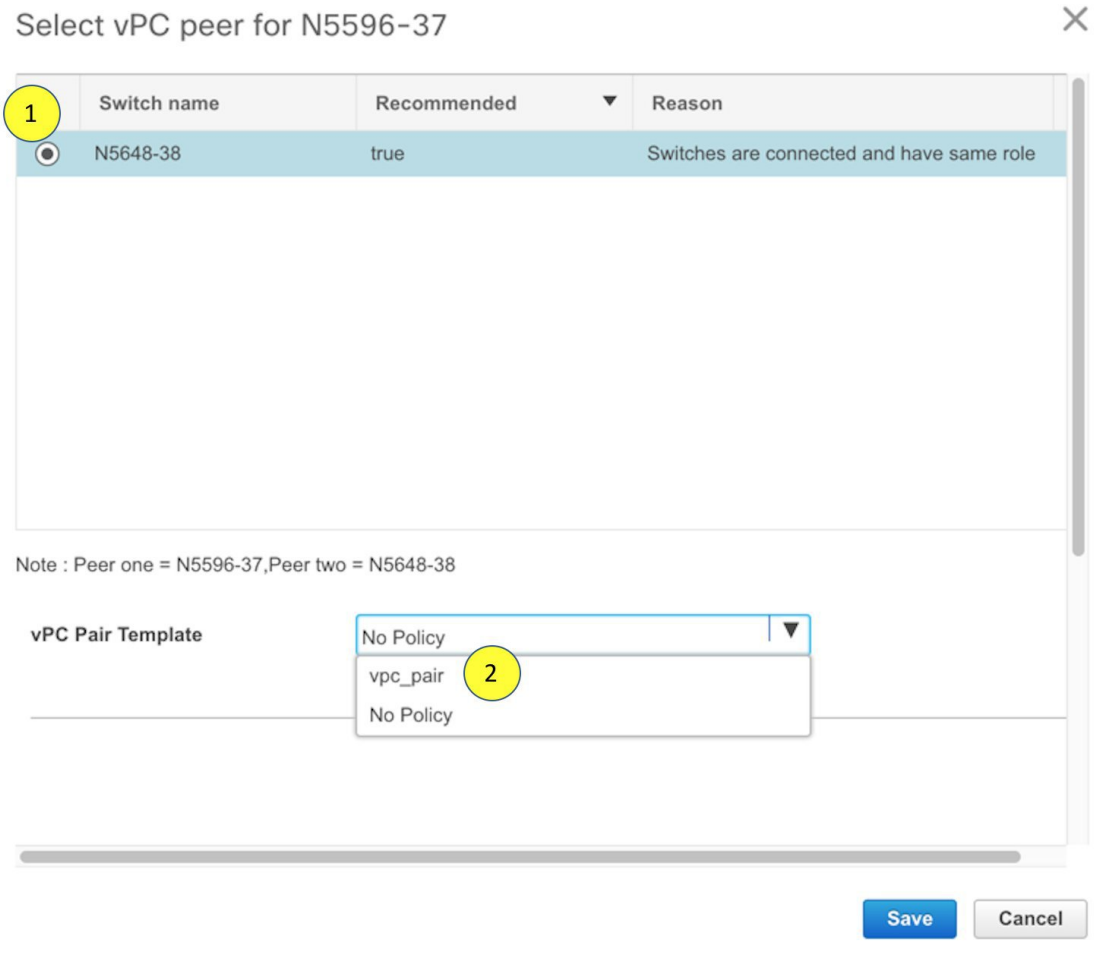
Procedure

ステップ 1 2つの指定された**vPC スイッチ**のいずれかを右クリックし、**[vPC ペアリング]** を選択します。

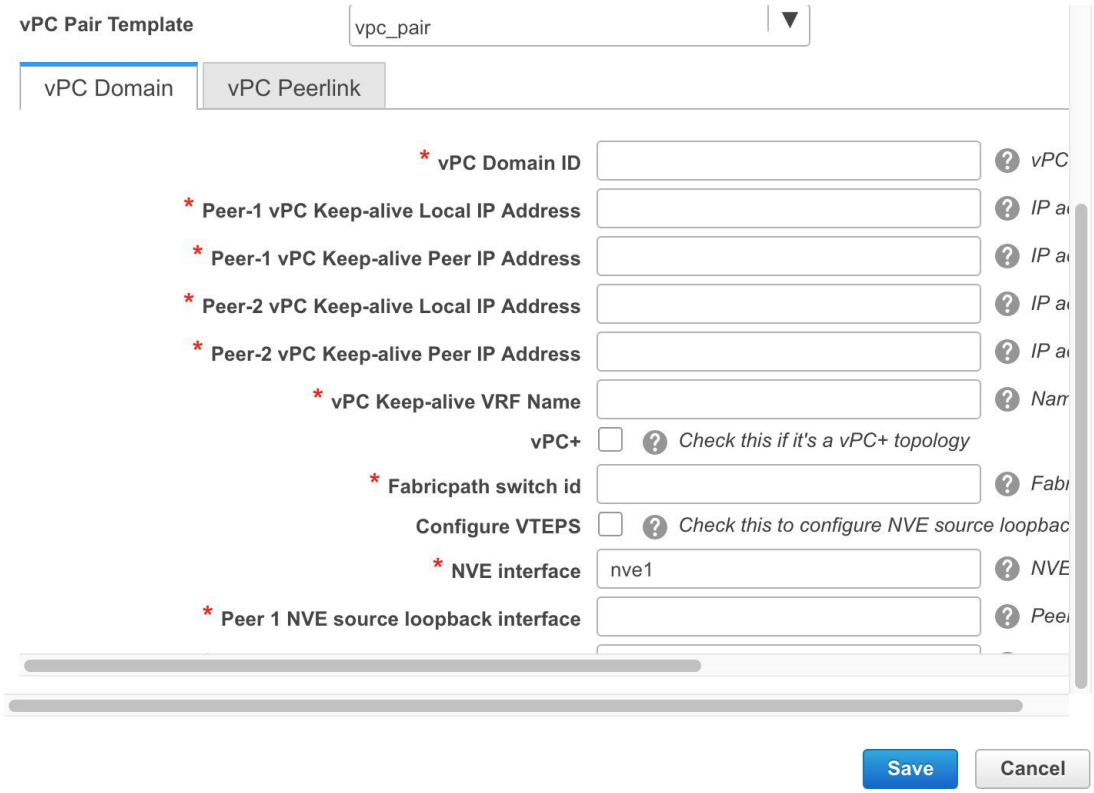
[vPC ピアの選択（Select vPC peer）] ダイアログボックスが表示されます。潜在的なピア スイッチのリストが含まれます。vPC ピア スイッチの**[推奨（Recommended）]**列が **[true]**に更新されていることを確認します。

Note または、**[アクション（Actions）]** ペインから**表形式ビュー**に移動することもできます。**[スイッチ（Switches）]** タブでスイッチを選択し、**[vPC Pairing（vPC ペアリング）]**をクリックしてvPCペアを作成、編集、またはペアリング解除します。ただし、このオプションは、Cisco Nexus スイッチを選択した場合にのみ使用できます。

ステップ 2 vPCピアスイッチの横にあるオプションボタンをクリックし、**[vPC ペア テンプレート（vPC Pair Template）]** ドロップダウンリストから **vpc_pair** を選択します。ここには、**VPC_PAIR** テンプレートサブタイプのテンプレートのみが表示されます。



[vPC ドメイン（vPC Domain）] タブと **[vPC ピアリンク（vPC Peerlink）]** タブが表示されます。vPC設定を作成するには、タブのフィールドに入力する必要があります。各フィールドの説明は、右端に表示されます。



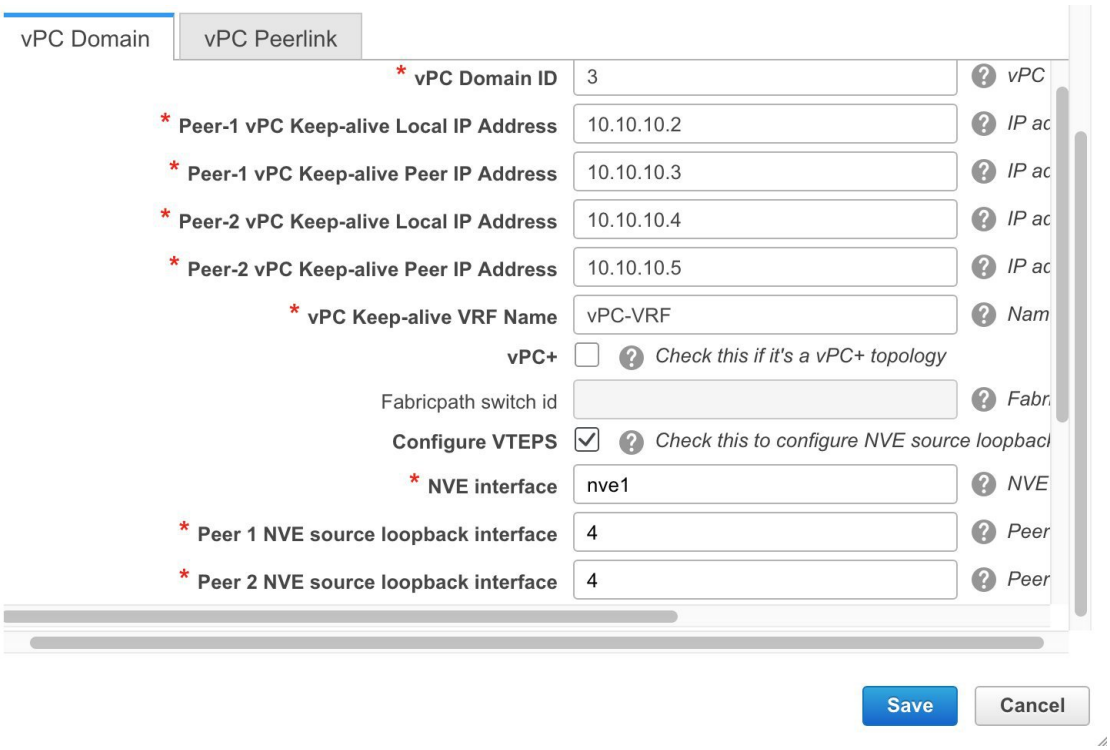
[vPC ドメイン（vPC Domain）] タブ：vPC ドメインの詳細を入力します。

[vPC+]：スイッチが FabricPath vPC+ セットアップの一部である場合は、このチェックボックスをオンにして **[FabricPath スイッチ ID]** フィールドに入力します。

[VTEP の構成（Configure VTEPs）]：2 つの vPC ピア VTEP の送信元ループバック IP アドレスと、NVE 設定のループバック インターフェイス セカンダリ IP アドレスを入力します。

[NVE インターフェイス（NVE interface）]：NVE インターフェイスを入力します。 vPC ペアリングでは、送信元ループバック インターフェイスのみが設定されます。追加構成には、自由形式のインターフェイス マネージャを使用します。

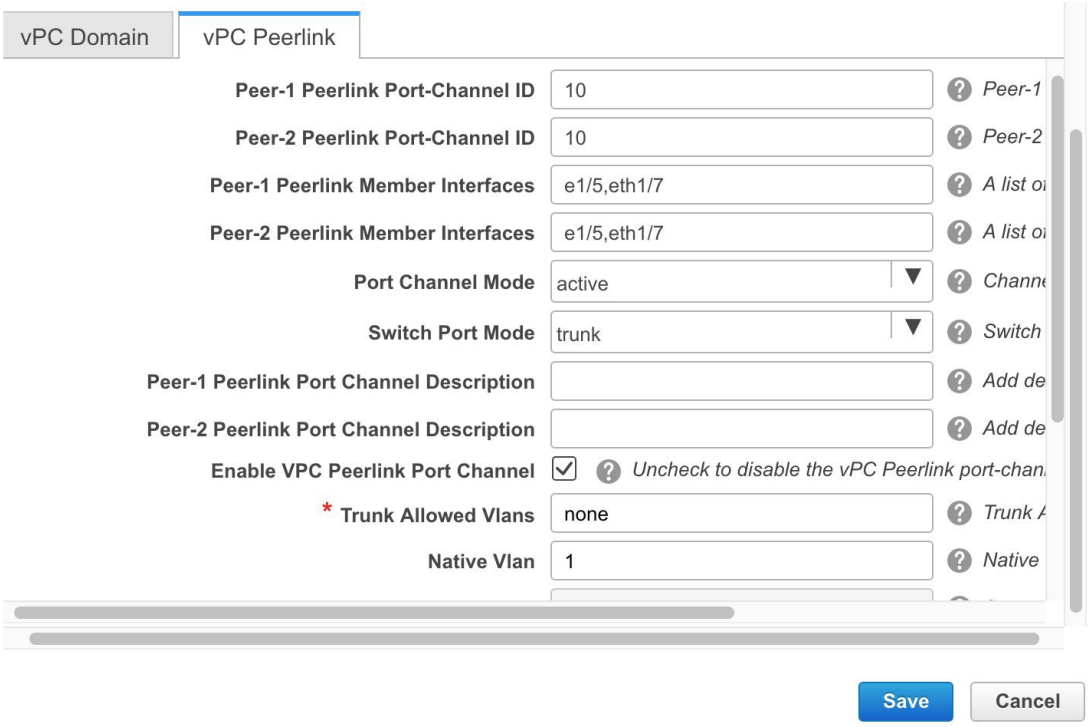
[NVE ループバック構成（NVE loopback configuration）]：IP アドレスをマスクで入力します。vPC ペアリングは、ループバック インターフェイスのプライマリおよびセカンダリ IP アドレスのみを構成します。追加構成には、自由形式のインターフェイスマネージャを使用します。



[vPC ピアリンク（vPC Peerlink）]タブ：vPCピアリンクの詳細を入力します。

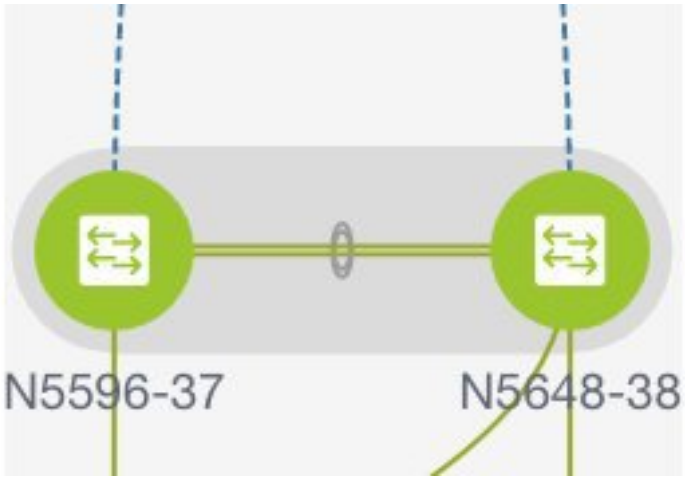
[スイッチポート モード（Switch Port Mode）]：**trunk** または **access** または **fabricpath** を選択します。

トランクを選択すると、対応するフィールド（**[トランク許可 VLAN（Trunk Allowed VLANs）]** および**[ネイティブ VLAN（Native VLAN）]**）が有効になります。**access** を選択すると、**[VLAN にアクセス（Access VLAN）]**フィールドが有効になります。**fabricpath** を選択すると、トランクおよびアクセスポート関連のフィールドは無効になります。



ステップ 3 **[Save（保存）]** をクリックします。

[ファブリック トポロジ（fabric topology）] ウィンドウが表示されます。**vPC セットアップ**が作成されます。



vPC セットアップの詳細を更新するには、次の手順を実行します。

a. vPC スイッチを右クリックし、[vPC ペアリング] を選択します。

[vPC ピア（vPC peer）] ダイアログボックスが表示されます。

b. 必要に応じて、次のフィールドを更新します。

フィールドを更新すると、**[ペアリング解除（Unpair）]** アイコンが **[保存（Save）]** に変わります。

c. **[保存（Save）]** をクリックして更新を完了します。

vPC セットアップの展開解除

Procedure

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

vPC ピア画面が表示されます。

ステップ 2 画面の右下にある **[ペアリング解除（Unpair）]** をクリックします。

vPC ペアが削除され、ファブリック トポロジ ウィンドウが表示されます。

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

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

ステップ 4 (Optional) **[構成のプレビュー（Preview Config）]**列の値をクリックします。

[構成プレビュー] ダイアログボックスで保留中の設定を表示します。vPC 機能、vPC ドメイン、vPC ピアリンク、vPC ピアリンク メンバー ポート、ループバックセカンダリ IP、およびホスト vPC のペアリングを解除すると、スイッチの次の設定の詳細が削除されます。ただし、ホスト vPC とポート チャネルは削除されません。必要に応じて、**[インターフェイス（Interfaces）]** ウィンドウからこれらのポート チャネルを削除します。

Note 同期していない場合は、ファブリックを再同期します。

ペアリングを解除すると、次の機能の PTI のみが削除されますが、**[保存と展開（Save & Deploy）]** の間に構成がクリアされません。NVE 構成、LACP 機能、FabricPath 機能、nv オーバーレイ機能、ループバック プライマリ ID です。ホスト vPC の場合、ポート チャネルとそのメンバー ポートはクリアされません。必要に応じて、**[インターフェイス（Interfaces）]** ウィンドウからこれらのポート チャネルを削除できます。ペアリングを解除した後でも、スイッチでこれらの機能を引き続き使用できます。

fabricpath から VXLAN に移行する場合は、VXLAN 設定を展開する前にデバイスの設定をクリアする必要があります。

VXLAN BGP EVPN ファブリックのマルチサイト ドメイン

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

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

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

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

Note

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

ファブリック固有の用語：

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

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

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

ファブリックとスイッチのインスタンス変数

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

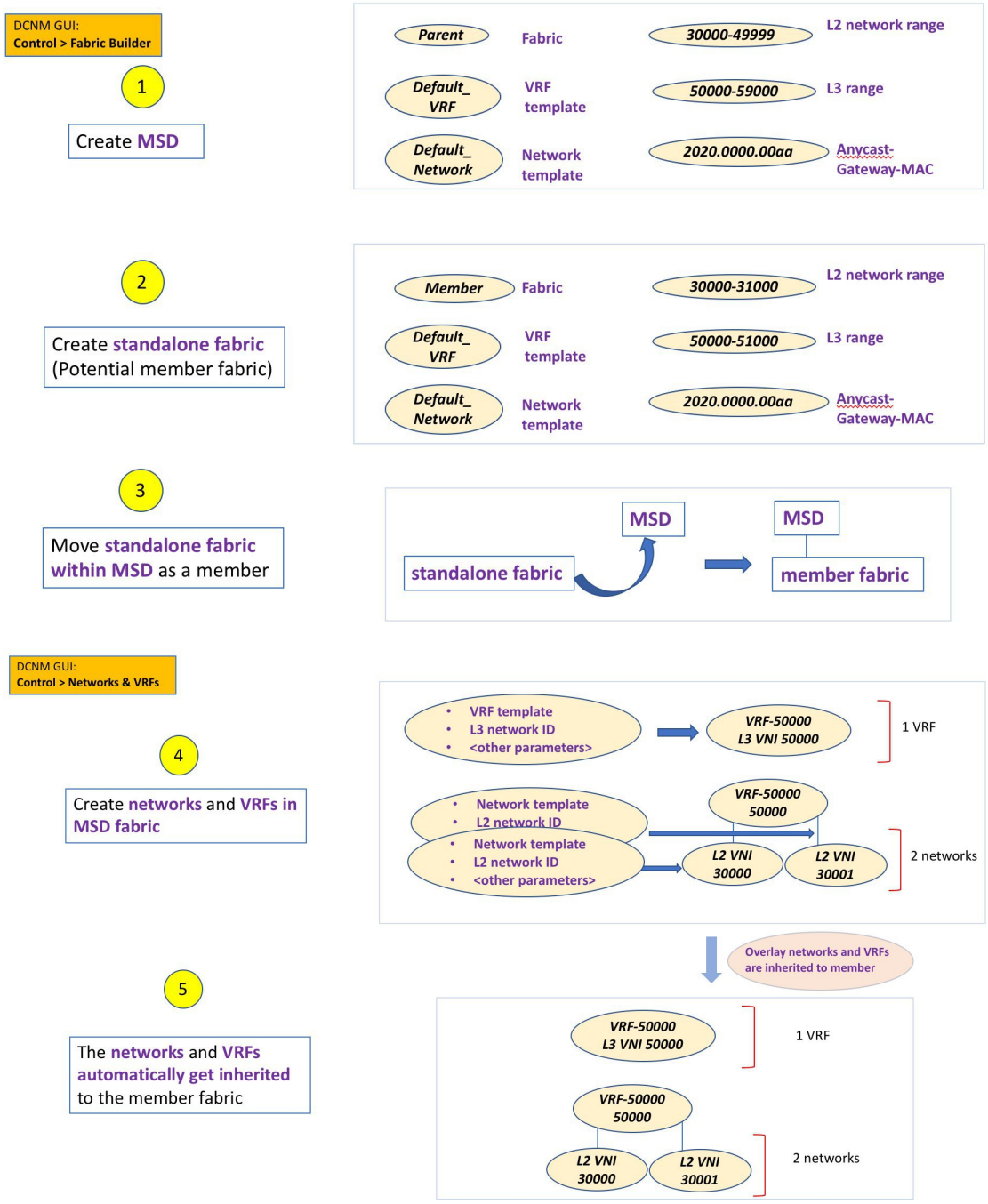
ファブリック インスタンスの値は、[VRFs and Networks] ウィンドウからのファブリック コンテキストでのみ編集または更新できます。ファブリック インスタンスの値を編集するには、**[範囲（SCOPE）]** ドロップダウンリストで適切なファブリックを選択する必要があります。ファブリック インスタンス変数の例には、BGP ASN、ネットワークごとのマルチキャスト グループまたは VRF などがあります。マルチキャスト グループ アドレスの編集方法については、メンバー ファブリックでのネットワークの編集, on page 198を参照してください。

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

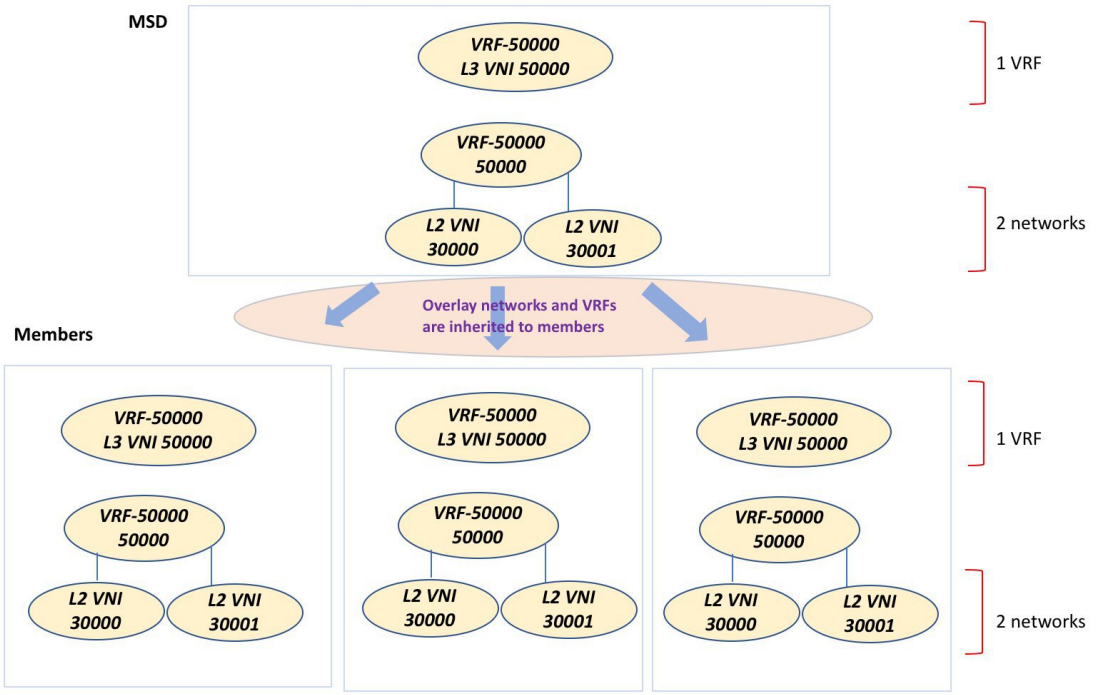
MSD およびメンバー ファブリックのプロセス フロー

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

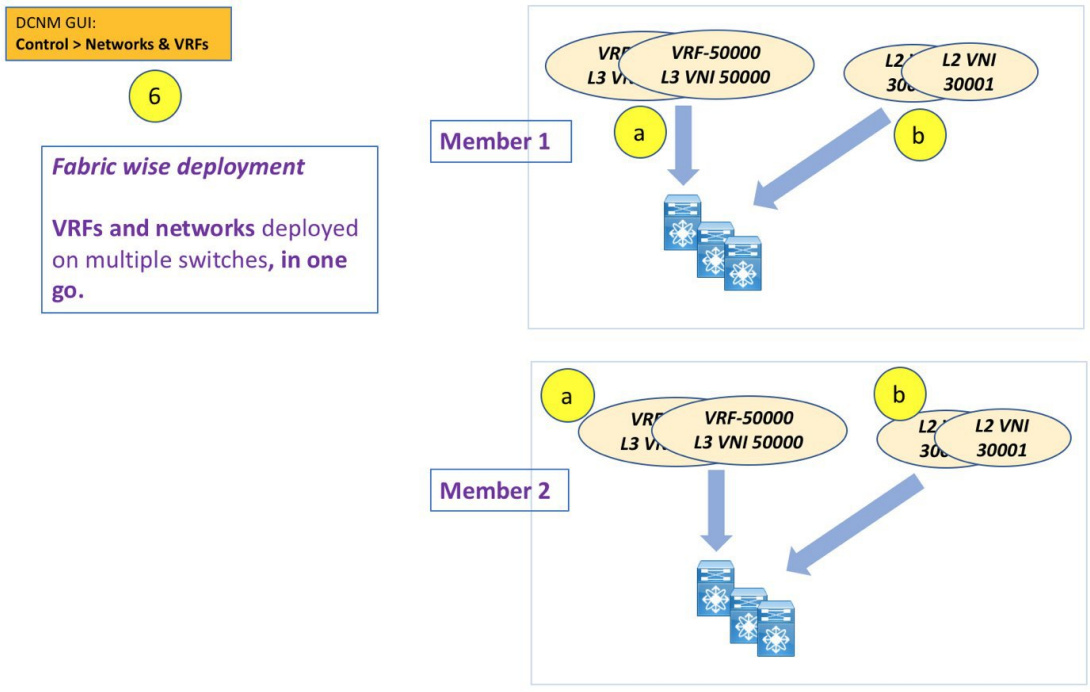
MSD とメンバー ファブリックの作成、および MSD からメンバー ファブリックへの継承プロセスの概要フロー チャート：



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



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



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

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

ドキュメントの今後のセクションでは、以下について説明します。

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

MSD ファブリックの作成とメンバー ファブリックの関連付け

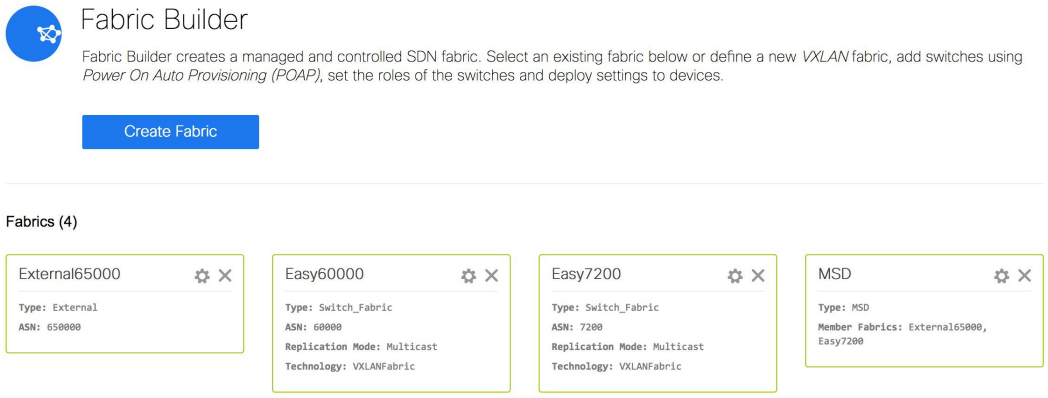
このプロセスは、次の 2 つのステップで説明されます。

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

MSD ファブリックの作成

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

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

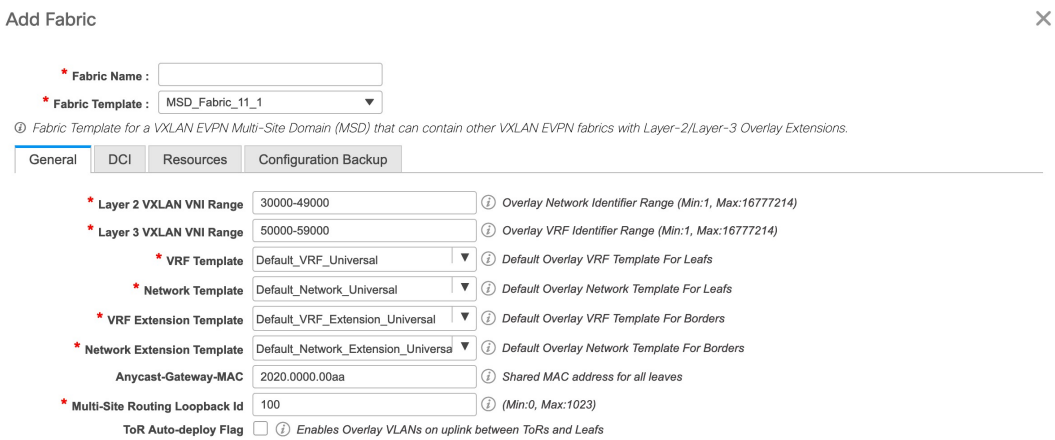


スタンドアロンまたはメンバー ファブリックには、*Switch_Fabric*（**タイプ** フィールド）、AS 番号（**ASN** フィールド）、および複製モード（**複製モード** フィールドのマルチキャストまたは複製の入力）が含まれます。MSD ファブリックはコンテナであり、デバイスまたはネットワーク トラフィックは関連付けられていないため、これらのフィールドはありません。

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

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

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



画面のフィールドについて説明します。

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

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

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

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

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

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

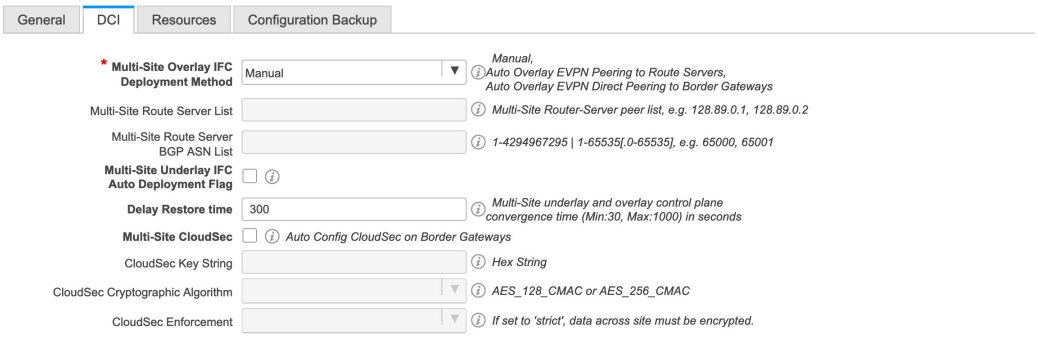
[ネットワーク拡張テンプレート（Network Extension Template）]：デフォルトのネットワーク拡張テンプレート。

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

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

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

3. **[DCI]** タブをクリックします。



該当するフィールドは次のとおりです。

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

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

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

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

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

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

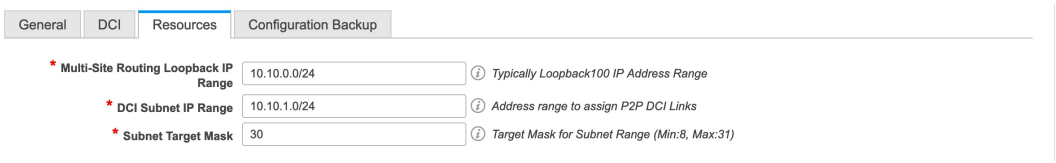
[マルチサイト（Multi-Site CloudSec）]：ボーダー ゲートウェイで CloudSec 構成を有効にします。このフィールドを有効にすると、CloudSec の残りの 3 つのフィールドが編集可能になります。詳細については、マルチサイト展開での CloudSec のサポート, on page 205を参照してください。

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

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

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

4. [リソース（Resources）] タブをクリックします。

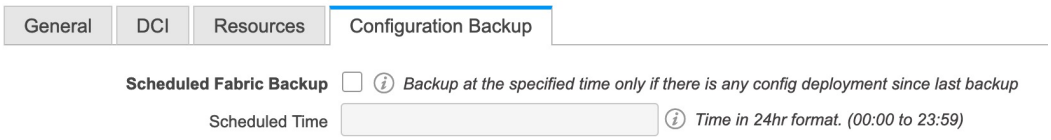


[マルチサイト ルーティング ループバック IP 範囲（MultiSite Routing Loopback IP Range）]：EVPN マルチサイト機能に使用されるマルチサイト ループバック IP アドレス範囲を指定します。

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

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

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



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

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

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

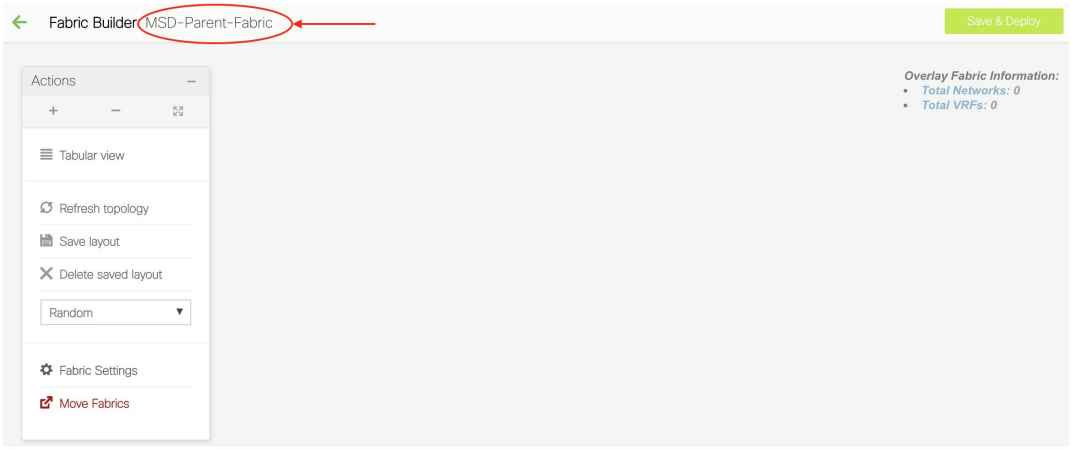
[保存（Save）]をクリックすると、バックアップ プロセスが開始されます。

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

6. [保存（Save）] をクリックします。

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

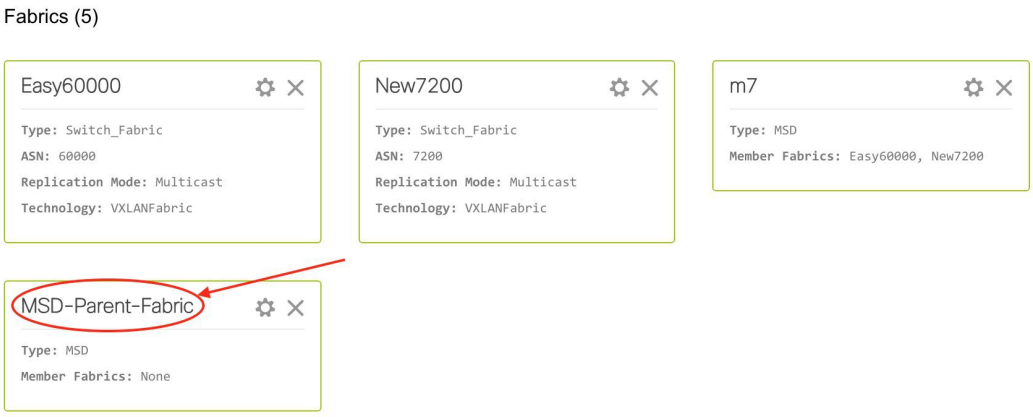
Note Cisco DCNM リリース 11.4(1) 以降、MSD ファブリック設定を更新すると、MSD に関連するロールを持つスイッチだけが更新されます。



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

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

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



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

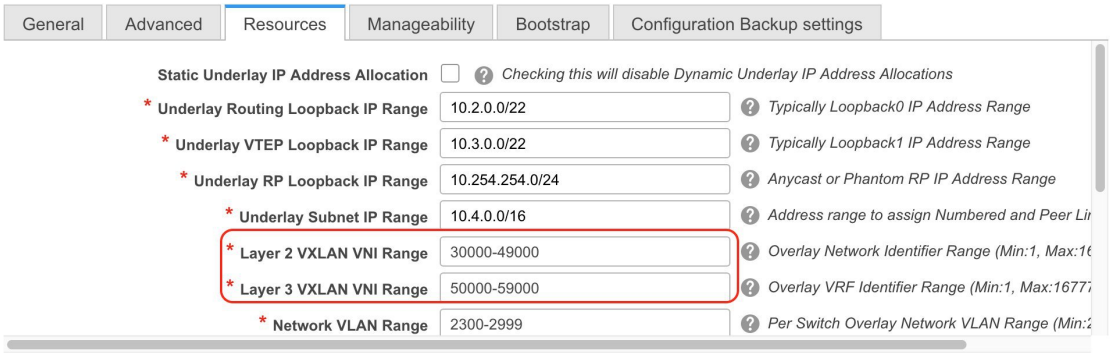
1. MSD ファブリックを作成します。
2. **新しいスタンドアロン ファブリックを作成し、メンバー ファブリックとして MSD ファブリックの下に移動します。**

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

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

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

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



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

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

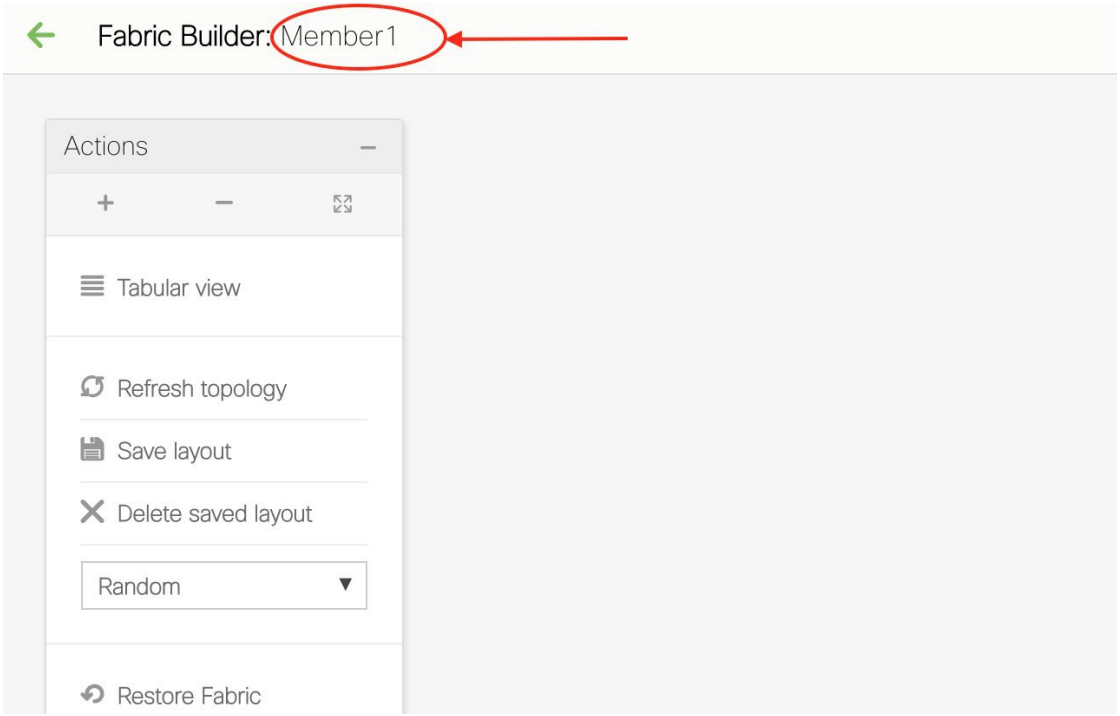
[エニーキャスト ゲートウェイ MAC（Anycast Gateway MAC）]、**[ネットワーク テンプレート（Network Template）]**、および**[VRF テンプレート（VRF Template）]**フィールドの値がMSDファブリックと同じであることを確認します。それ以外の場合、MSDへのメンバーファブリックの移動は失敗します。

その他の指針：

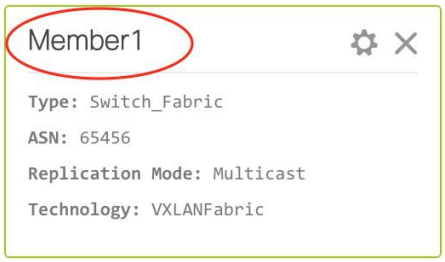
- [エニーキャスト ゲートウェイ MAC（Anycast Gateway MAC）]、[ネットワーク テンプレート（Network Template）]、および[VRF テンプレート（VRF Template）]フィールドの値がMSDファブリックと同じであることを確認します。それ以外の場合、MSDへのメンバーファブリックの移動は失敗します。
- メンバーファブリックにはサイトIDが設定されている必要があり、サイトIDはメンバー間で一意である必要があります。
- BGP AS番号は、メンバー ファブリックに対して一意である必要があります。
- loopback0のアンダーレイ サブネット範囲は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

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

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



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



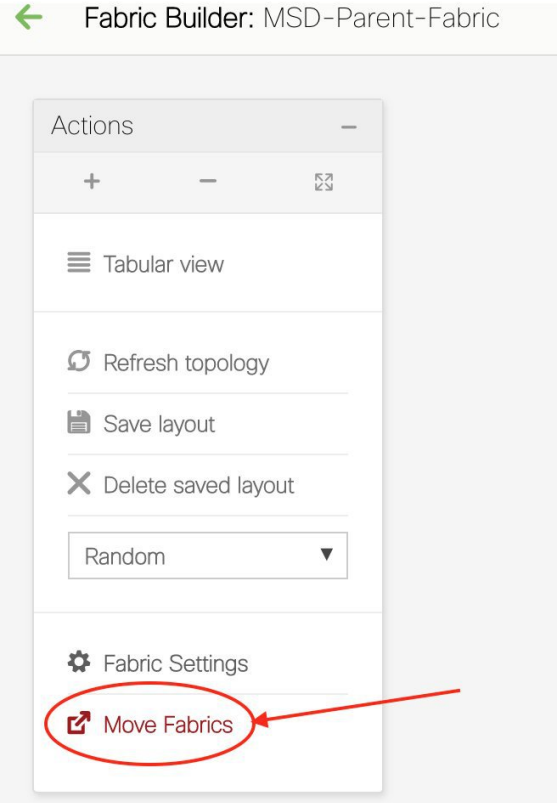
MSD-Parent-Fabric の下での Member1 ファブリックの移動

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

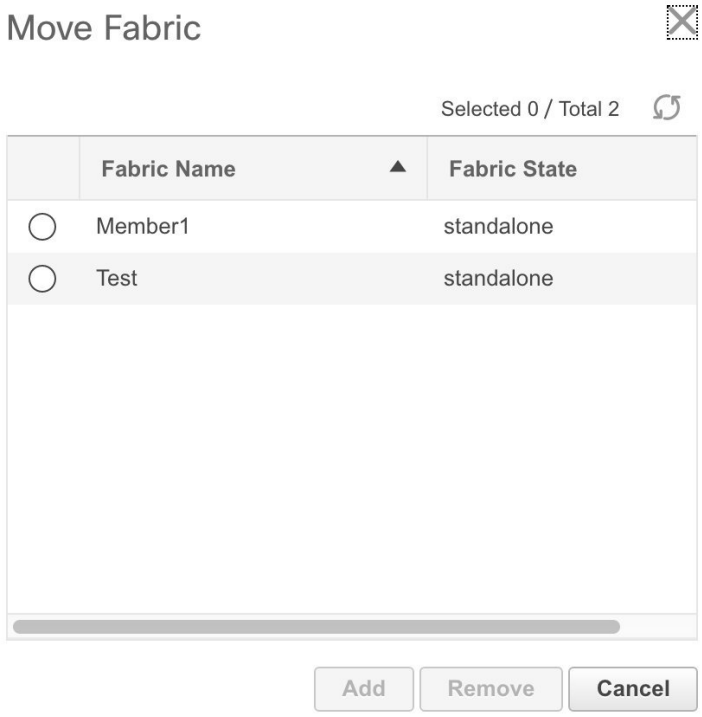
ファブリック ビルダ ページを表示している場合は、**MSD-Parent-Fabric** ボックス内をクリックして、MSD-Parent-Fabric ページに移動します。

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

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



[ファブリックの移動（Move Fabric）] 画面が表示されます。ファブリックのリストが含まれています。

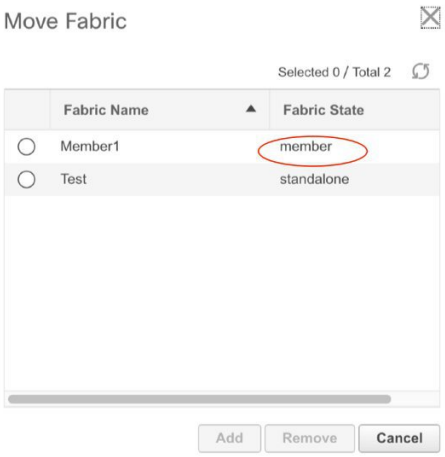


他の MSD コンテナ ファブリックのメンバー ファブリックは、ここには表示されません。

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

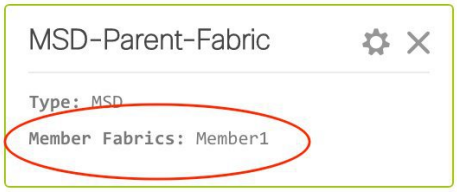
2. *Member1* ファブリックを MSD ファブリックに関連付けるため、**[Member1]** ラジオ ボタンを選択します。**[追加（Add）]** ボタンが有効になります。
3. [追加（Add）] をクリックします。

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



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

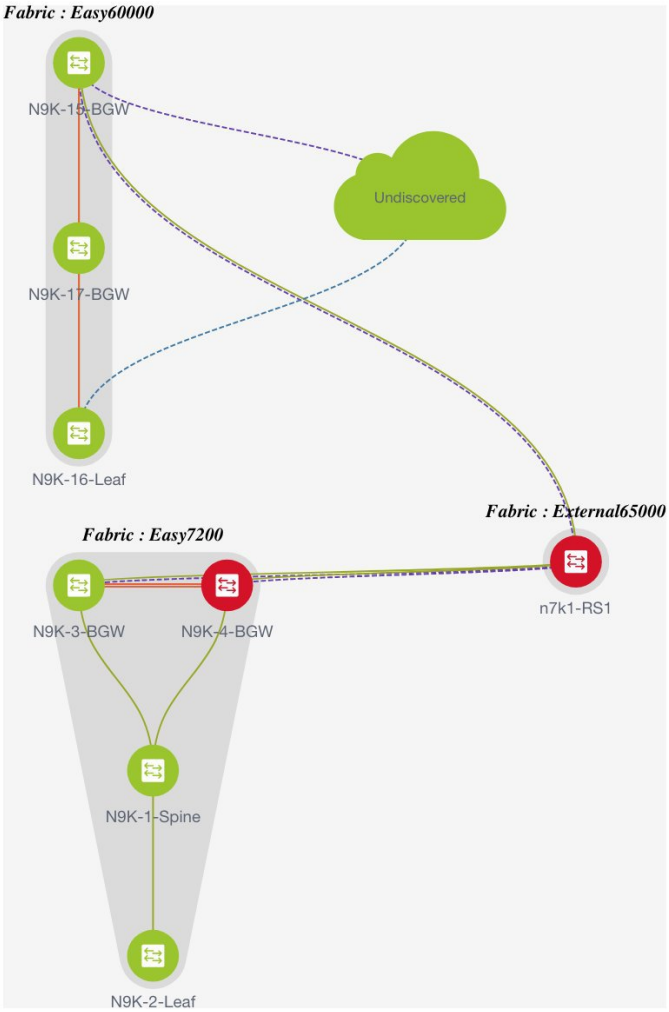
   Member1 が MSD ファブリックに追加され、**[メンバー ファブリック（Member Fabrics）]** フィールドに表示されることがわかります。



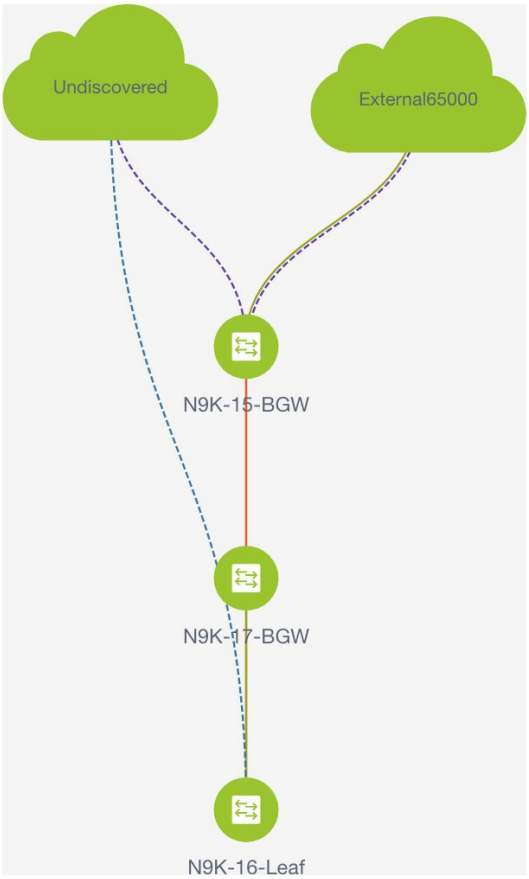
MSD ファブリックのトポロジ ビューのポインタ

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

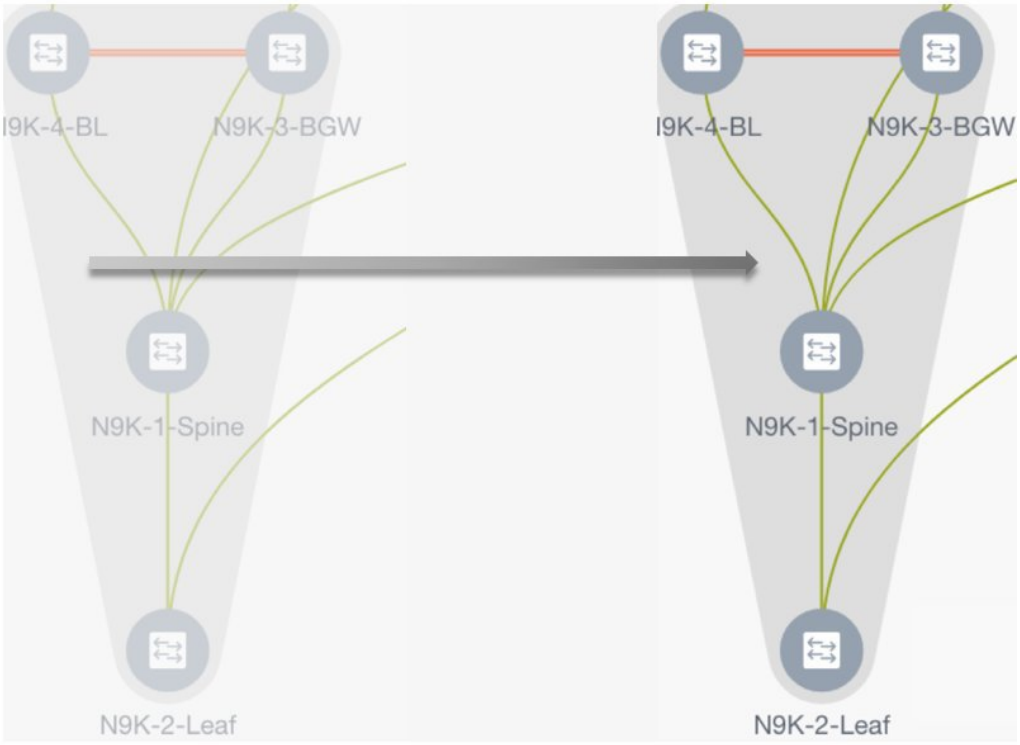
  ファブリック内リンクとマルチサイト（アンダーレイとオーバーレイ）、およびリモート ファブリックへの VRF Lite リンクを含むすべてのリンクが表示されます。



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



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



リンクの追加と編集

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

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

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

MSD ファブリックでのネットワークと VRF の作成と展開

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

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

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

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

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

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

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

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

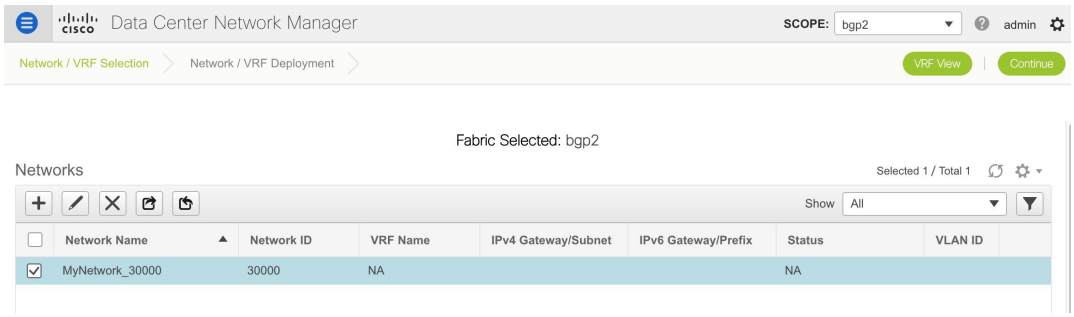
1. MSD ファブリックにネットワークと VRF を作成します。
2. メンバー ファブリックのデバイスにネットワークと VRF を展開します。1 回に付き 1 つのファブリックを展開します。

MSD ファブリックでのネットワークの作成

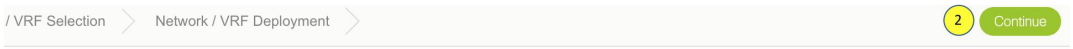
1. **[制御（Control）] > [ネットワーク（Networks）]**（**[ファブリック（Fabrics）]** サブメニューの下）をクリックします。

   [ネットワーク（Networks）] 画面が表示されます。

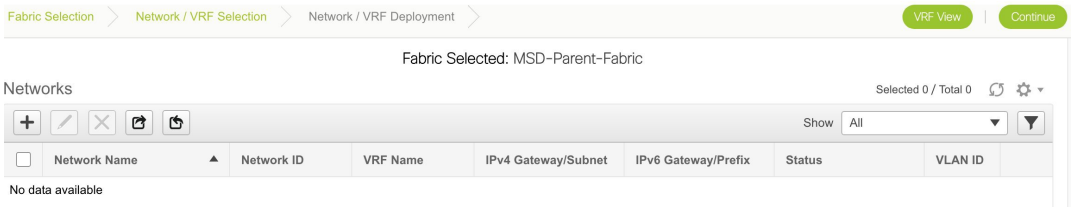
2. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[ネットワーク（Networks）]** 画面が更新され、選択したファブリックのネットワークが一覧表示されます。



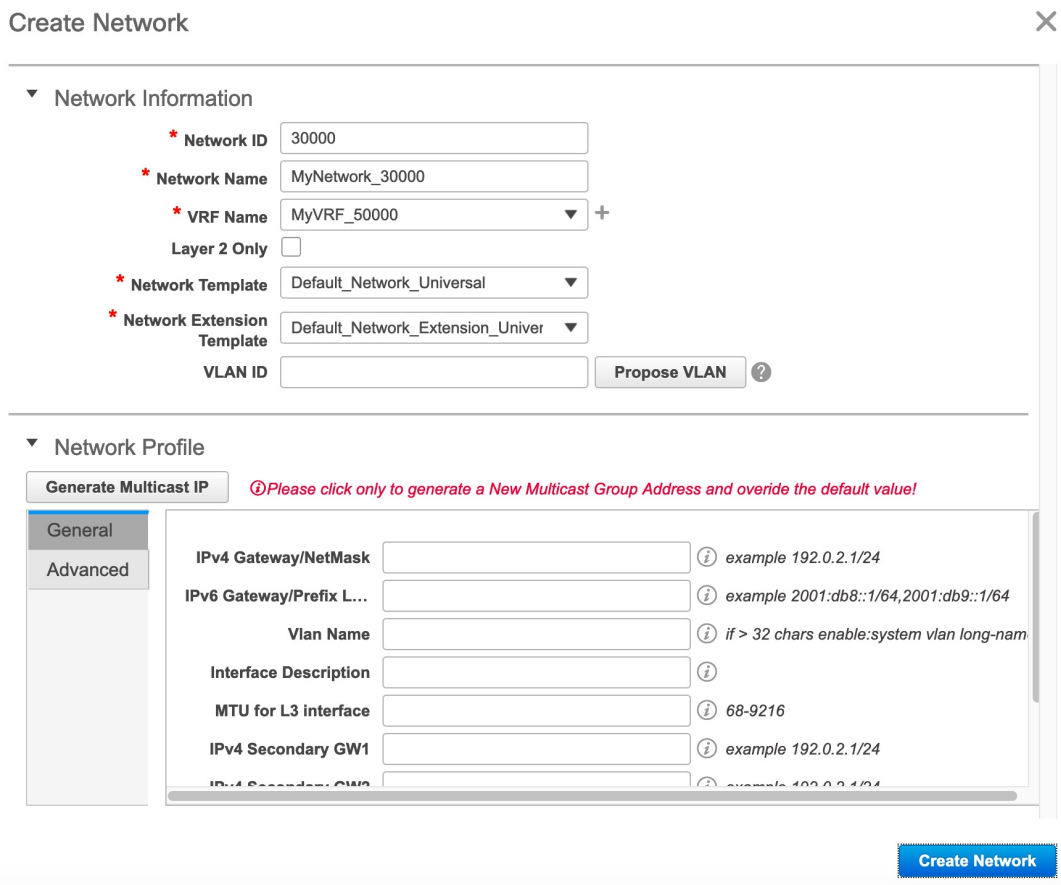
3. リストから *MSD-Parent-Fabric* を選択し、画面の右上にある **[続行（Continue）]** をクリックします。



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



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



この画面のフィールドは次のとおりです。

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

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

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

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

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

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

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

VLAN ID：ネットワークの対応するテナントVLAN IDを指定します。

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

[General] タブ

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

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

[Vlan 名（Vlan Name）]：VLAN 名を入力します。

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

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

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

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

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

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

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

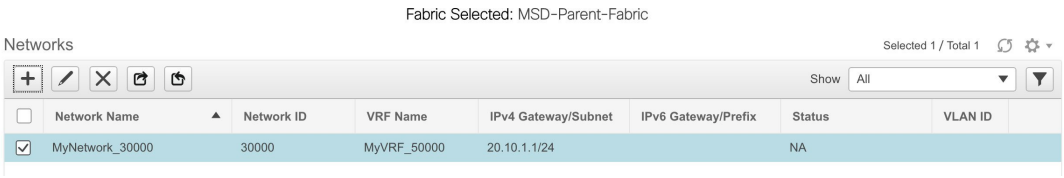
  詳細については、テナント ルーテッド マルチキャストの概要, on page 234を参照してください。
- L2 VNI ルート ターゲットの両方が有効：すべての L2 仮想ネットワークのルート ターゲットの自動インポートとエクスポートを有効にするには、このチェックボックスをオンにします。

Note Cisco DCNM リリース 11.5(1) 以降、**[ボーダーで L3 ゲートウェイを有効にする（Enable L3 Gateway on Border）]** フィールドは、MSD ネットワーク設定の一部として使用できません。ボーダー スイッチのレイヤ 3 ゲートウェイをファブリック レベルで有効にすることができます。詳細については、スタンドアロン ファブリック向けのネットワークの作成, on page 333を参照してください。

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

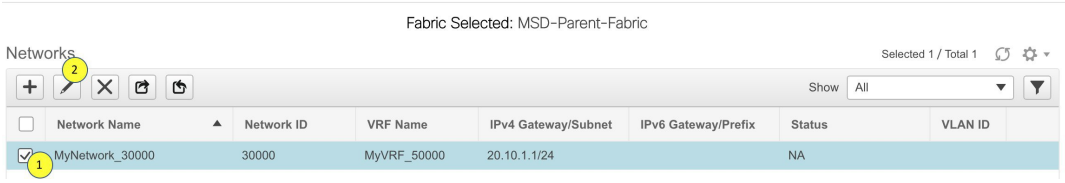
- [ネットワークの作成（Create Network）] 画面のサンプル：

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

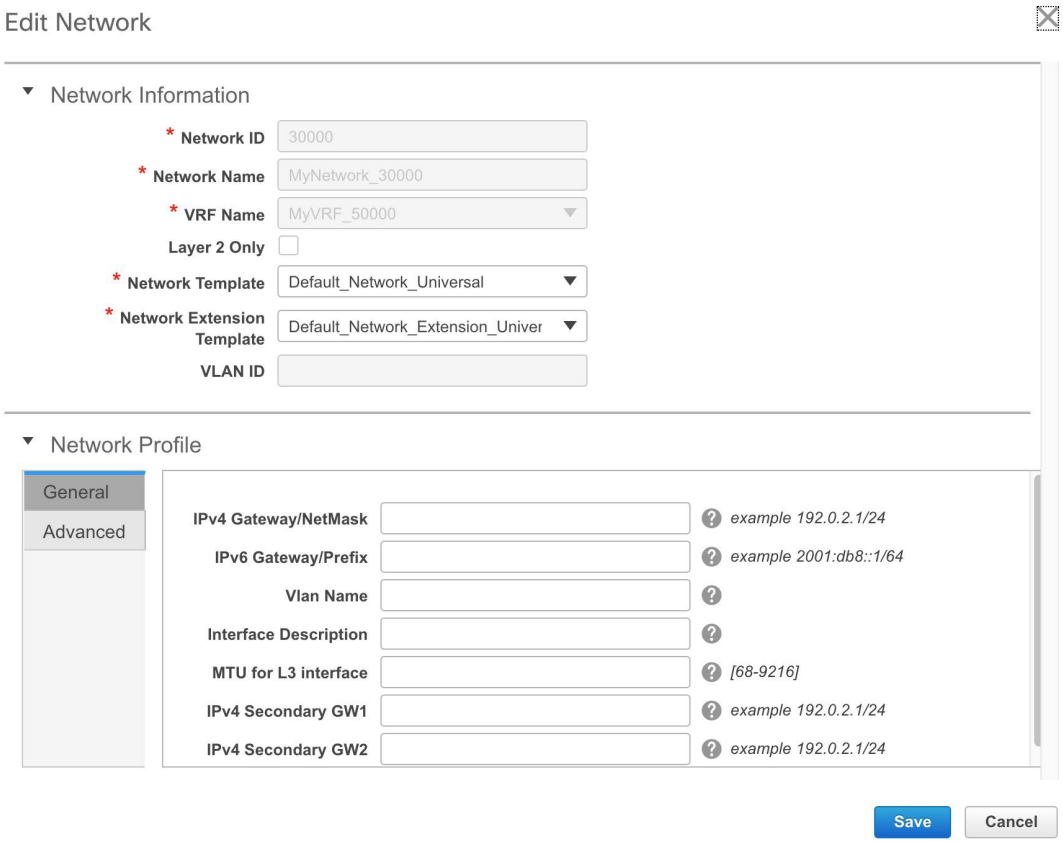


MSD ファブリックでのネットワークの編集

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



[ネットワークの編集（Edit Network）] 画面が表示されます。



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

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

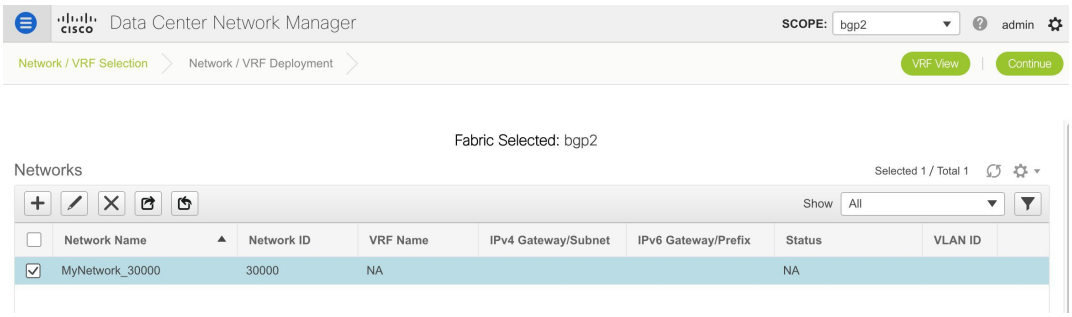
MSD-Parent-Fabric から Member1 へのネットワーク継承

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

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

   [ネットワーク（Networks）] 画面が表示されます。

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

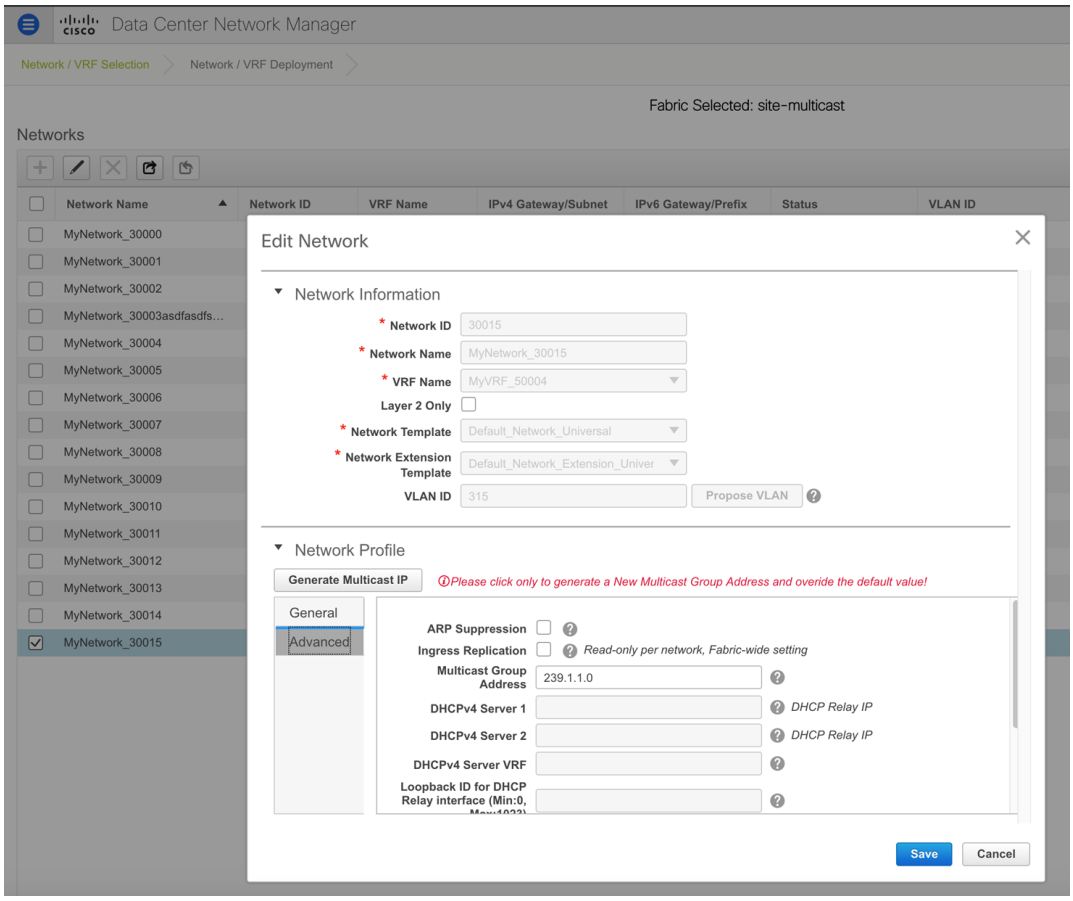


メンバー ファブリックでのネットワークの編集

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

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

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



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

MSD およびメンバー ファブリックでのネットワークの削除

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

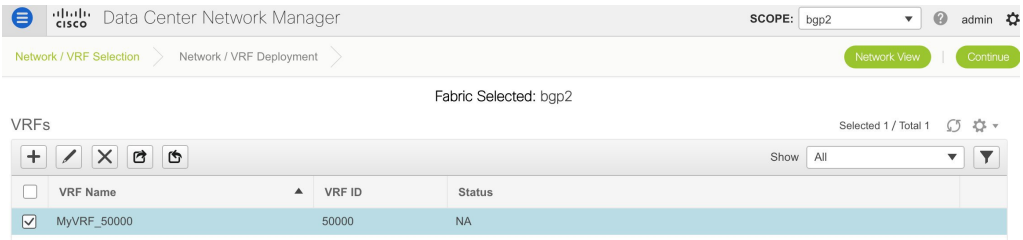
1. 削除する前に、それぞれのファブリック デバイスでネットワークを展開解除します。
2. MSD ファブリックからネットワークを削除します。ネットワークを削除するには、[ネットワーク（Networks）] 画面の左上にある削除（**[X]**）オプションを使用します。複数のネットワークを一度に削除することもできます。

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

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

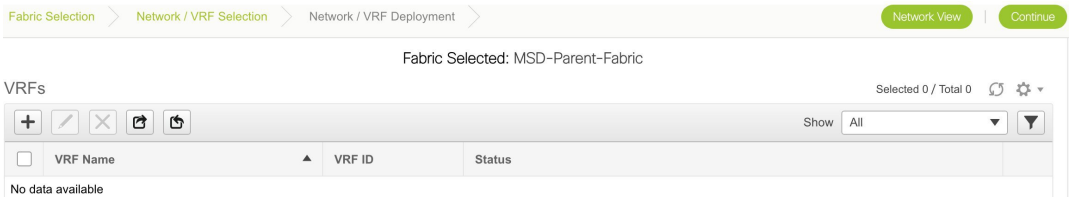
MSD ファブリックでの VRF の作成

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



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

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



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

   この画面のフィールドは次のとおりです。

   VRF ID と **VRF 名**：VRF の ID と名前です。

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

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

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

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

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

4. **[詳細（Advanced）]** タブ

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

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

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

   [TRM の有効（TRM Enable）]：TRM を有効にするには、このチェックボックスをオンにします。

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

   詳細については、テナント ルーテッド マルチキャストの概要, on page 234を参照してください。

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

   RP アドレス：RP の IP アドレスを指定します。

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

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

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

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

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

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

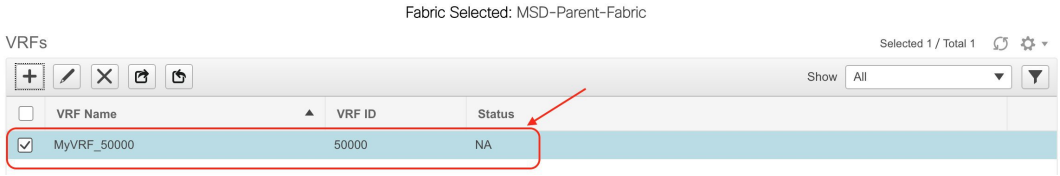
[デフォルト ルートのアドバタイズ（Advertise Default Route）]：このチェックボックスを選択して、ファブリック内のデフォルト ルートのアドバタイズを制御します。

サンプル スクリーンショット：

[Advanced] タブ：

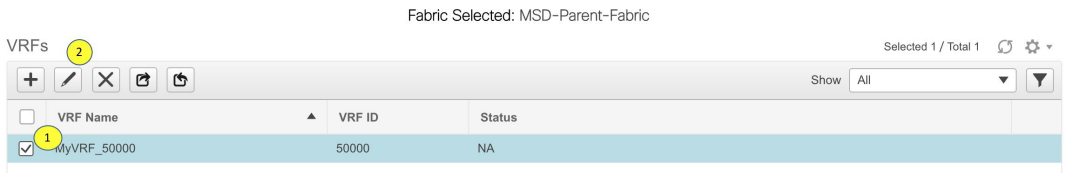
5. **[VRF の作成（Create VRF）]** をクリックします。

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

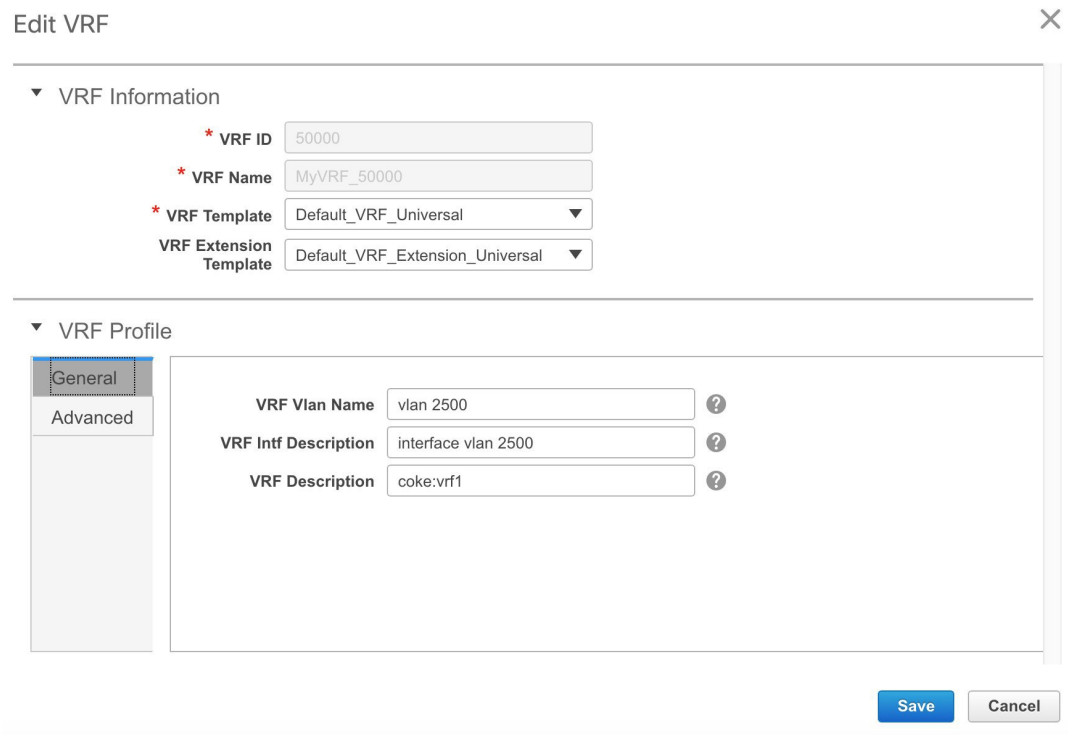


MSD ファブリックでの VRF の編集

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



   [VRF の編集（Edit VRF）] 画面が表示されます。



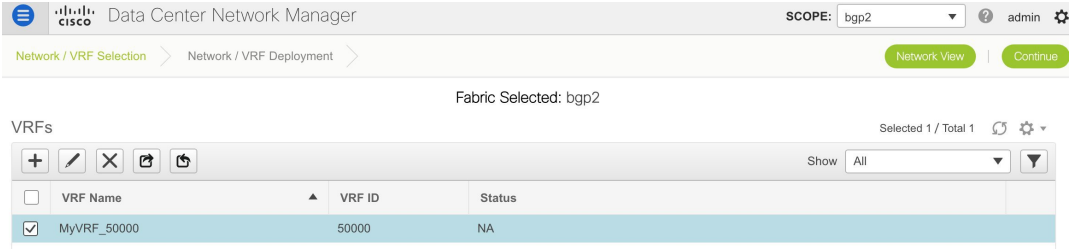
[VRF プロファイル（VRF Profile）] の部分（**[全般（General）]** タブと **[詳細（Advanced）]** タブ）を編集することができます。

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

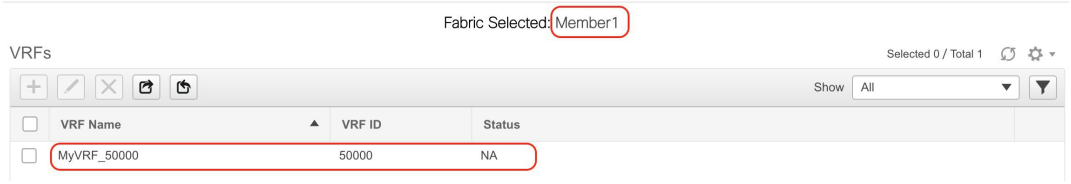
MSD-Parent-Fabric から Member1 への VRF 継承

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

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



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



MSD およびメンバー ファブリックでの VRF の削除

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

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

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

メンバー ファブリックでの VRF の編集

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

メンバー ファブリックでの VRF の削除

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

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

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

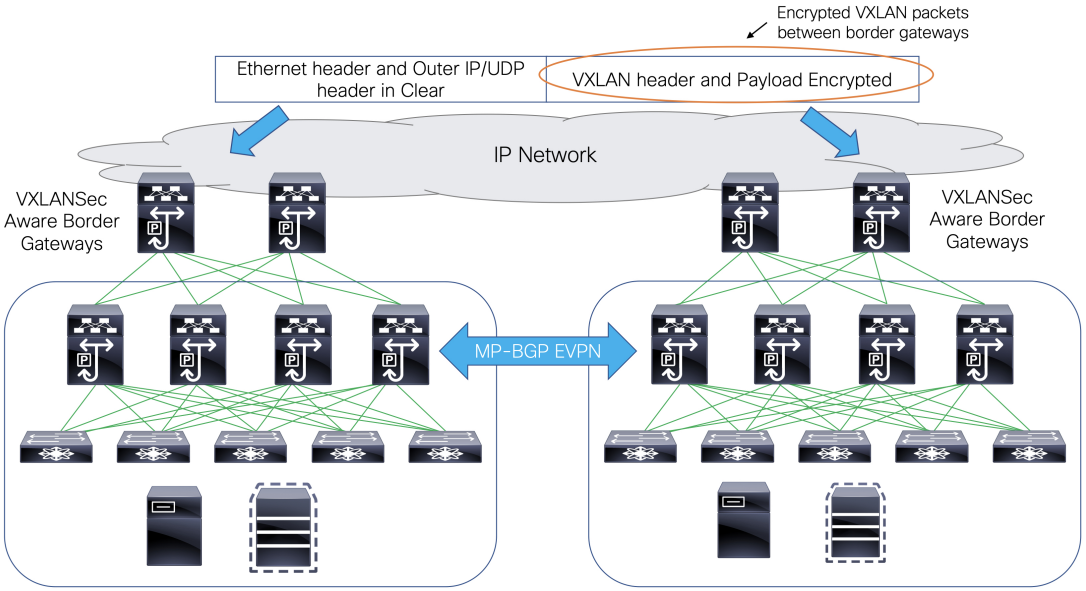
メンバー ファブリックでのネットワークと VRF の展開と展開解除

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

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

マルチサイト展開での CloudSec のサポート

CloudSec 機能は、異なるファブリック内のボーダー ゲートウェイ デバイス間の送信元から宛先へのパケット暗号化をサポートすることにより、マルチサイト展開で安全なデータセンター相互接続を可能にします。



CloudSec 機能は、Cisco NX-OS リリース 9.3(5) 以降を搭載した Cisco Nexus 9000 シリーズ FX2 プラットフォームでサポートされています。FX2 プラットフォームであり、Cisco NX-OS リリース 9.3(5) 以降を実行するボーダー ゲートウェイ、ボーダー ゲートウェイ スパイン、およびボーダー ゲートウェイ スーパースパインは、CloudSec 対応スイッチと呼ばれます。

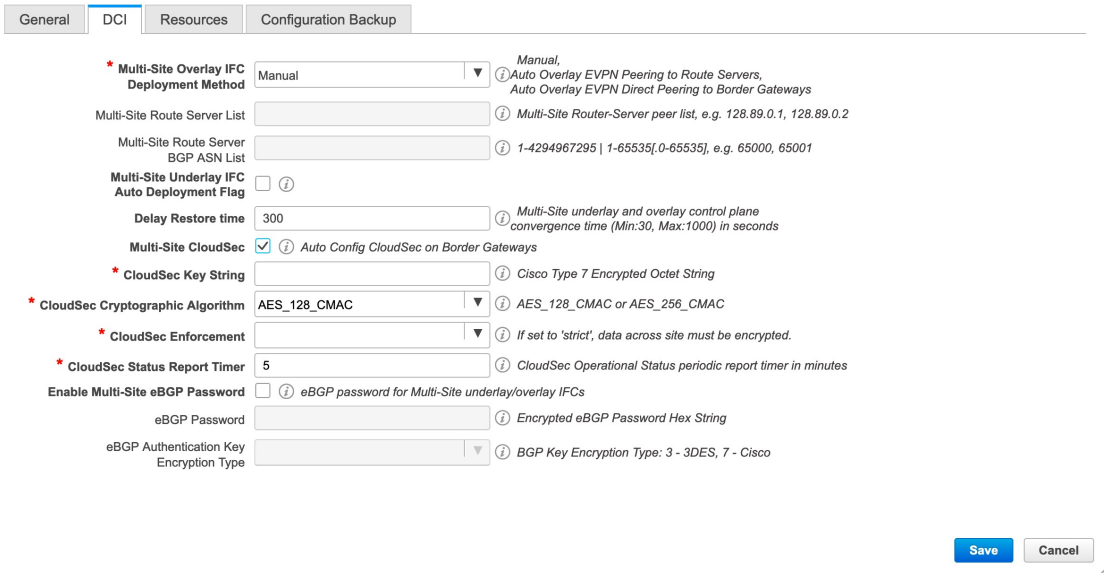
Cisco DCNM リリース 11.4(1) には、MSD ファブリックで CloudSec を有効にするオプションが用意されています。

（注） CloudSec セッションは、2 つの異なるサイトのボーダー ゲートウェイ（BGW）間の DCI を介したポイントツーポイントです。サイト間のすべての通信は、VIP の代わりにマルチサイト PIP を使用します。CloudSec を有効にするには、VIP から PIP に切り替える必要があります。これにより、サイト間のデータ フローのトラフィックが中断される可能性があります。したがって、CloudSec の有効または無効の切り替えは、メンテナンス ウィンドウ中に行うことをお勧めします。

CloudSec 機能を構成する方法を示すビデオを見ることもできます。「ビデオ：Cisco DCNM での CloudSec の構成」を参照してください。

MSD で CloudSec を有効にする

[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）] に移動します。**[ファブリックの作成（Create Fabric）]** をクリックして新しい MSD ファブリックを作成するか、**[ファブリックの編集（Edit Fabric）]** をクリックして既存の MSD ファブリックを編集することができます。



[DCI] タブで、CloudSec 構成の詳細を指定できます。

[マルチサイト（Multi-Site CloudSec）]：ボーダー ゲートウェイで CloudSec 構成を有効にします。このフィールドを有効にすると、CloudSec の残りのフィールドが編集可能になります。

[マルチサイト（Multi-Site CloudSec）]：ボーダー ゲートウェイで CloudSec 構成を有効にします。このフィールドを有効にすると、CloudSec の残りの 3 つのフィールドが編集可能になります。

Cloudsec が MSD レベルで有効になっている場合、DCNM は、すべての Cloudsec 対応ゲートウェイのアップリンクで、**dci-advertise-pip**（**evpn multisite border-gateway**の下） と 、**tunnel-encryption** も有効にします。

[保存と展開（Save & Deploy）] をクリックすると、ボーダーゲートウェイ スイッチの **[構成のプレビュー（Preview Config）]** ウィンドウでこれらの構成を確認できます。

[注（Note）]：ボーダーゲートウェイに vPC がある場合、または TRM が有効になっている場合、つまり、マルチサイト オーバーレイ IFC で TRM が有効になっている場合、CloudSec はサポートされません。このシナリオで CloudSec が有効になっている場合、適切な警告またはエラー メッセージが生成されます。

[CloudSec キー文字列（CloudSec Key String）]：16 進キー文字列を指定します。**AES_128_CMAC** を選択した場合は 66 文字の 16 進文字列を入力し、**AES_256_CMAC** を選択した場合は 130 文字の 16 進文字列を入力します。

[CloudSec 暗号化アルゴリズム（CloudSec Cryptographic Algorithm）]：**AES_128_CMAC** または **AES_256_CMAC** を選択します。

[CloudSec 強制（CloudSec Enforcement）]：CloudSec を厳密に強制するか、緩和するかを指定します。

[厳密（strict）]：MSD のファブリック内のすべてのボーダー ゲートウェイに CloudSec 構成を展開します。CloudSec をサポートしていないボーダー ゲートウェイがある場合、エラー メッセージが生成され、構成はどのスイッチにもプッシュされません。

[厳密（strict）] が選択されている場合、**tunnel-encryption must-secure** CLI が MSD 内の CloudSec 対応ゲートウェイにプッシュされます。

[緩和（loose）]：MSD のファブリック内のすべてのボーダー ゲートウェイに CloudSec 構成を展開します。CloudSec をサポートしていないボーダー ゲートウェイがある場合は、警告メッセージが生成されます。この場合、CloudSec 構成は、CloudSec をサポートするスイッチにのみ展開されます。**[緩和（loose）]** が選択されていて、**tunnel-encryption must-secure** CLI が存在する場合は削除されます。

（注） CloudSec をサポートするボーダー ゲートウェイを備えた MSD には、少なくとも 2 つのファブリックが必要です。CloudSec 対応デバイスを備えたファブリックが 1 つしかない場合は、次のエラー メッセージが生成されます。

CloudSec には、CloudSec をサポートできるサイトが少なくとも 2 つ必要です（CloudSec needs to have at least 2 sites that can support CloudSec）。

このエラーを解消するには、CloudSec をサポートするか、CloudSec を無効にできるサイトが少なくとも 2 つあるという条件を満たす必要があります。

[CloudSec ステータス レポート タイマー（CloudSec Status Report Timer）]：CloudSec 動作ステータス定期レポート タイマーを分単位で指定します。この値は、DCNM がスイッチから CloudSec ステータス データをポーリングする頻度を指定します。デフォルト値は 5 分で、範囲は 5 ～ 60 分です。

DCNM の CloudSec 機能を使用すると、MSD 内のすべてのゲートウェイが同じキーチェーン（および1つのキー文字列のみ）を持ち、ポリシーを持つようにすることができます。DCNM に1つのキーチェーン文字列を指定して、キーチェーン ポリシーを形成することができます。

DCNM は、すべてのデフォルト値を使用して encryption-policy を形成します。DCNM は、同じキー チェーン ポリシー、同じ暗号化ポリシー、および暗号化ピア ポリシーを各 CloudSec 対応ゲートウェイにプッシュします。各ゲートウェイには、CloudSec 対応で、同じキーチェーンと同じキー ポリシーを使用する encryption-peer ポリシーが、リモート ゲートウェイごとに 1 つあります。

MSD ファブリック全体に同じキーを使用したくない場合、またはすべてのサイトのサブセットでのみ CloudSec を有効にしたい場合は、**switch_freeform** を使用して、CloudSec 構成をスイッチに手動でプッシュできます。

switch_freeform のすべての CloudSec 構成をキャプチャします。

たとえば、次の設定は **switch_freeform** ポリシーに含まれています。

```
feature tunnel-encryption
evpn multisite border-gateway 600
  dci-advertise-pip
tunnel-encryption must-secure-policy
tunnel-encryption policy CloudSec_Policy1
tunnel-encryption source-interface loopback20
key chain CloudSec_Key_Chain1 tunnel-encryption
  key 1000
    key-octet-string 7 075e731f1a5c4f524f43595f507f7d737062677147524054590 70b0b0701585440
 cryptographic-algorithm AES_128_CMA
tunnel-encryption peer-ip 192.168.0.6
  keychain CloudSec_Key_Chain1 policy CloudSec_Policy1
```

次のような構成を生成するアップリンク インターフェイス ポリシーのフリーフォーム構成に **tunnel-encryption** を追加します。

```
interface ethernet1/13
  no switchport
  ip address 192.168.1.14/24 tag 54321
  evpn multisite dci-tracking
  tunnel-encryption
  mtu 9216
  no shutdown
```

詳細については、ファブリック スイッチでのフリーフォーム設定の有効化 （408ページ）を参照してください。

CloudSec 設定がスイッチに追加または削除されると、DCI アップリンクがフラップし、マルチサイト BGP セッション フラッピングがトリガーされます。既存のクロス サイト トラフィックがあるマルチサイトの場合、この移行中にトラフィックの中断が発生します。したがって、メンテナンス期間中に移行を行うことをお勧めします。

CloudSec 構成の MSD ファブリックを DCNM に移行する場合、Cloudsec 関連の構成は、**[switch_freeform]** およびインターフェイス自由形式構成でキャプチャされます。MSD ファブリック設定で Multi-Site Cloudsec をオンにする必要はありません。さらにファブリックを追加し、既存のものとキーを含む同じ CloudSec ポリシーを共有する CloudSec トンネルを確立する場合は、MSD ファブリック設定で CloudSec 構成を有効にすることができます。MSD ファブリック設定の CloudSec パラメータは、スイッチの既存の CloudSec 設定と一致する必要があります。CloudSec 構成は既にフリーフォーム構成に取り込まれており、MSD で CloudSec を有効にすると構成インテントも生成されます。したがって、二重のインテントが生じます。たとえば、MSD 設定で CloudSec キーを変更する場合、DCNM は **switch_freeform** の構成を変更しな

いため、CloudSec 自由形式構成を削除する必要があります。そうしないと、MSD ファブリック設定のキーがフリーフォーム構成のキーと競合します。

CloudSec の動作状態の表示

Cisco DCNM 11.5(1) 以降では、MSD ファブリックで CloudSec が有効になっている場合、**[CloudSec 操作ビュー（CloudSec Operational View）]** を使用して CloudSec セッションの操作ステータスを確認できます。

手順

ステップ 1 MSD ファブリックを選択します。

ファブリック トポロジ ウィンドウが表示されます。

ステップ 2 **[アクション（Actions）]** ペインで **[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 **[CloudSec 操作ビュー（CloudSec Operational View）]** タブを選択します。

ステップ 4 CloudSec が無効になっている場合、**[CloudSec 操作ビュー（CloudSec Operational View）]** タブは表示されません。

[操作ビュー（Operational View）] タブには、次のフィールドと説明があります。

フィールド	説明
Fabric Name（ファブリック名）	CloudSec セッションを持つファブリックを指定します。
セッション	CloudSec セッションに関係するファブリックとボーダー ゲートウェイ スイッチを指定します。
リンク ステータス	CloudSec セッションのステータスを指定します。この状態は次のいずれかになります。 • Up：スイッチ間で CloudSec セッションが正常に確立されています。 • Down：CloudSec セッションは動作していません。
稼働時間	CloudSec セッションの稼働時間を指定します。具体的には、最後の Rx および Tx セッションがフラップしてからの稼働時間であり、2 つのセッションのうち小さい方の値が表示されます。
動作理由	CloudSec セッション状態のダウン理由を指定します。

これらすべての列が並べ替え可能です。

（注） ファブリックで CloudSec が有効になった後、セッションが作成され、次のステータス ポーリングが発生するまでは、動作ステータスを使用できない場合があります。

CloudSec セッションのトラブルシューティング

CloudSec セッションが停止している場合は、プログラマブル レポートを使用してその詳細を確認できます。

手順

ステップ 1 **[アプリケーション（Applications）] > [プログラマブル レポート（Programmable report）]** に移動します。

ステップ 2 **[レポートの作成（Create Report）]** アイコンをクリックします。

ステップ 3 レポート名を指定し、レポートジョブを実行するMSDファブリックを選択して、**[次へ（Next）]** をクリックします。

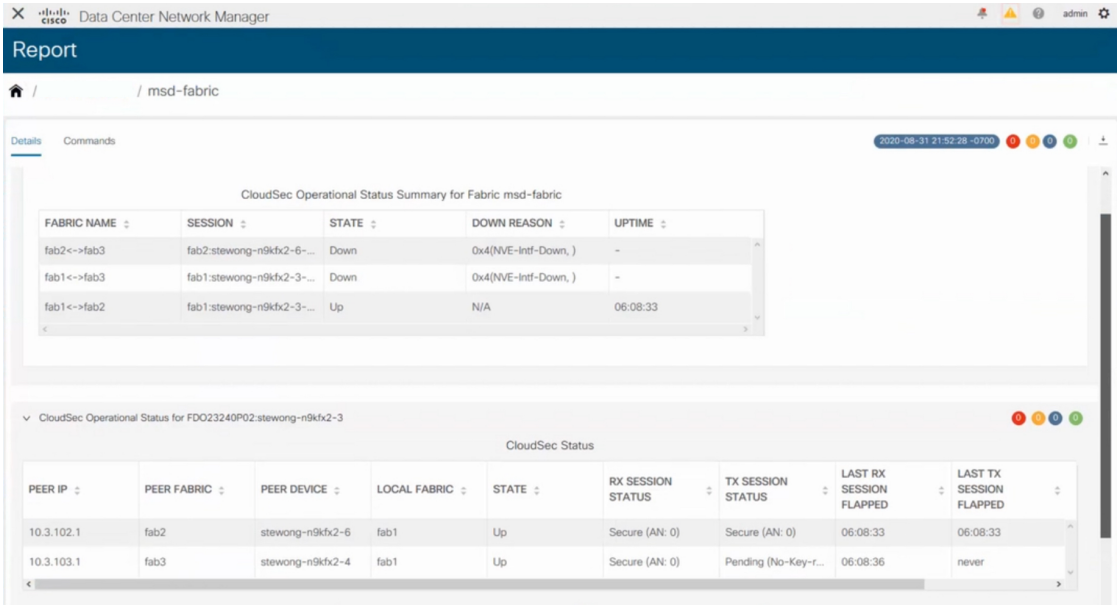
ステップ 4 **[テンプレート（Template）]** ドロップダウン リストから、**fabric_cloudsec_oper_status** を選択して **[ジョブの作成（Create Job）]** をクリックします。

レポートが正常に生成されると、ステータスは成功を示す緑色のチェックマークに変わります。

ステップ 5 [レポート（report）] をクリックして表示します。このレポートは、**CloudSec 操作ビュー（CloudSec Operation View）]** タブに似ています。

ステップ 6 CloudSecセッション ステータスの詳細を表示するには、**[詳細の表示（View Details）]** をクリックします。

ステップ 7 セッションの動作ステータスをクリックして、各ピア ファブリックおよびデバイスのCloudSecセッションに関する詳細情報を表示します。



MSD からのファブリックの削除

MSD ファブリックからファブリックを削除するには、次の手順を実行します。

Before you begin

削除するファブリックのボーダー スイッチに VRF が展開されていないことを確認してください。詳細については、メンバー ファブリックでのネットワークと VRF の展開と展開解除, on page 205を参照してください。

Note Cisco DCNM リリース 11.4(1) 以降、MSD から個々のファブリックを削除した後、アンダーレイおよびオーバーレイ IFC が削除されます。IFC が拡張されている場合、ファブリックの削除を禁止するエラーが報告されます。

Procedure

ステップ 1 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウで、MSD ファブリックをクリックします。

ステップ 2 **[アクション（Actions）]** メニューで **[ファブリックの移動（Move Fabric）]** をクリックします。

ステップ 3 **[ファブリックの移動（Move Fabric）]** ウィンドウで、削除するファブリックのそれぞれのラジオ ボタンを選択し、**[削除（Remove）]** をクリックします。

ファブリックの削除通知ウィンドウで、**[閉じる（Close）]** をクリックします。

ステップ 4 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウで MSD の **[保存と展開（Save & Deploy）]** をクリックします。

ステップ 5 **[構成の展開（Config Deployment）]** ウィンドウで **[展開構成（Deploy Config）]** をクリックします。

[閉じる（Close）] をクリックします。

ステップ 6 MSD から削除したファブリックに移動し、**[保存と展開（Save & Deploy）]** をクリックします。

ステップ 7 **[構成の展開（Config Deployment）]** ウィンドウで **[展開構成（Deploy Config）]** をクリックします。

[閉じる（Close）] をクリックします。

スタンドアロン ファブリック（既存のネットワークと VRF を使用）を MSD ファブリックに移動する

既存のネットワークと VRF を持つスタンドアロン ファブリックをメンバーとして MSD ファブリックに移動する場合は、共通のネットワーク（つまり、L2 VNI と L3 VNI 情報）、エニー

キャスト ゲートウェイ MAC、VRF とネットワーク テンプレートがファブリックと MSD 全体で同じであることを確認してください。DCNMは、スタンドアロンファブリック（ネットワークおよび VRF 情報）を MSD ファブリックの（ネットワークおよび VRF 情報）に対して検証して、エントリの重複を回避します。エントリの重複の例は、2 つの一般的なネットワーク名が異なるネットワーク ID を持っている場合です。競合があるかの検証後、スタンドアロンファブリックはメンバー ファブリックとして MSD ファブリックに移動されます。詳細：

- MSD ファブリックは、MSD ファブリックに存在しないスタンドアロン ファブリックのネットワークと VRF を継承します。それから、これらのネットワークと VRF は、メンバー ファブリックに継承されます。
- 新しく作成されたメンバー ファブリックは、MSD ファブリックのネットワークと VRF（新しく作成されたメンバー ファブリックには存在しないもの）を継承します。
- スタンドアロン ファブリックと MSD ファブリックの間に競合がある場合、検証によって、エラー メッセージが表示されます。更新後、メンバー ファブリックを MSD ファブリックに移動すると、移動は成功します。ページの上部に移動が成功したことを示すメッセージが表示されます。

メンバー ファブリックをスタンドアロン ステータスに戻すと、ネットワークと VRF はそのまま残りますが、独立したファブリックのように、MSD ファブリックの範囲外で関連したままになります。

LAN クラシック テンプレートを使用したスイッチ管理

Cisco DCNM リリース 11.4(1) 以降、**[LAN_Classic]** および **[Fabric_Group]** テンプレートを使用して、以前 DCNM クラシック LAN 展開で管理していたスイッチを管理できます。

[LAN_Classic] ファブリック テンプレートは、Cisco Nexus スイッチを管理するための汎用ファブリック テンプレートです。

ガイドラインと制約事項

- **[LAN_Classic]** ファブリック テンプレートを使用するファブリックは、**[External_Fabric_11_1]** ファブリック テンプレートを使用するように変更してから、関連するすべての機能を使用することができます。これはサポートされている唯一のファブリック テンプレートの変換であり、元に戻すことはできません。
- **[LAN_Classic]** ファブリックは、MSD ファブリックのメンバーとして追加できます。
- **[LAN_Classic]** ファブリックでは、Cisco Nexus スイッチのみがサポートされています。
- **[ToR]** ロールを持つスイッチがファブリック内にある場合、TOR Auto-Deploy 機能は **[LAN_Classic]** メンバー ファブリックでサポートされます。詳細については「*ToR* スイッチの構成とネットワークの展開」を参照してください。
- Cisco Nexus 7000シリーズスイッチとCisco NX-OSリリース6.2（24a）をLANクラシックまたは外部ファブリックで使用している場合は、ファブリック設定でAAA IP認証を有効にしてください。

- **[LAN_Classic]** テンプレートの次の機能は、**[External_Fabric_11_1]** テンプレートと同じサポートを提供します。

  サポートされる機能は次のとおりです。

  - 設定コンプライアンス
  - ファブリックのバックアップまたは復元
  - ネットワーク インサイト
  - パフォーマンス モニタリング
  - VMM
  - トポロジ ビュー
  - Kubernetes の可視化
  - RBAC

  詳細については、機能固有のセクションを参照してください。

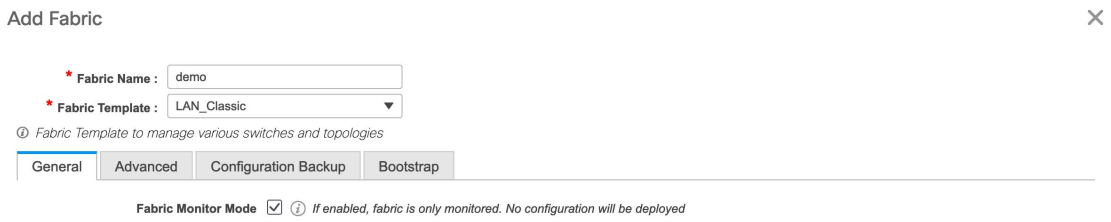
LAN クラシック ファブリックの作成

手順

ステップ 1 **[制御（Control）]** > **[ファブリック（Fabrics）]** > **[ファブリック ビルダ（Fabric Builder）]** に移動します。

ステップ 2 [ファブリックの作成（Create Fabric）] をクリックします。

ステップ 3 ファブリック名を入力し、**[ファブリック テンプレート（Fabric Template）]** ドロップダウンリストから **[LAN_Classic]** を選択します。



ステップ 4 デフォルトでは **[全般（General）]** タブが表示されます。このタブのフィールドは次のとおりです。

[ファブリック モニタ モード（Fabric Monitor Mode）]：DCNM がファブリックを管理する場合は、このチェックボックスをオフにします。ファブリックのモニタリングのみを有効にする場合は、チェックボックスをオンのままにします。この状態では、スイッチに構成を展開できません。

ファブリックで検出する前に、デバイスの構成をプッシュする必要があります。モニタ モードでは構成をプッシュできません。

ステップ 5 [Advanced] タブをクリックします。このタブのフィールドは次のとおりです。

[vPC ピア リンク VLAN（vPC Peer Link VLAN）]：vPC ピア リンク VLAN ID は自動入力されます。正しい値を反映させてフィールドをアップデートします。

電源モード（Power Supply Mode）：適切な電源モードを選択します。

[MPLS ハンドオフの有効化（Enable MPLS Handoff）]：MPLS ハンドオフ機能を有効にするには、このチェックボックスをオンにします。詳細については、「VXLAN BGP EVPN ファブリックでの境界プロビジョニングの使用例：MPLS SR および LDP ハンドオフ」の章を参照してください。

[アンダーレイ MPLS ループバック ID（Underlay MPLS Loopback Id）]：アンダーレイ MPLS ループバック ID を指定します。デフォルト値は 101 です。

[AAA IP 認証の有効化（Enable AAA IP Authorization）]：AAA サーバで IP 認証が有効になっている場合に、AAA IP 認証を有効にします。

[トラップホストとして有効にする（Enable as Trap Host）]：トラップホストとして有効にする場合は、このチェックボックスをオンにします。

[ブートストラップ スイッチの CDP の有効化（Enable CDP for Bootstrapped Switch）]：管理インターフェイスで CDP を有効にします。

[NX-API の有効化（Enable NX-API）]：NX-API の有効化を指定します。このチェックボックスは、デフォルトでオフになっています。

[ポートの HTTP で NX-API を有効化する（Enable on NX-API on HTTP）]：HTTP 上の NX-API の有効化を指定します。このチェックボックスは、デフォルトでオフになっています。HTTP を使用するには、[NX-API の有効化（Enable NX-API）] チェックボックスをオンにします。このチェックボックスをオフにすると、レイヤ 4 ～ レイヤ 7 サービス（L4 ー L7 サービス）、VXLAN OAM など、NX-API を使用し、Cisco DCNM がサポートするアプリケーションは、HTTP ではなく HTTPS の使用を開始します。

（注） [NX-API の有効化（Enable NX-API）] チェックボックスと [HTTP での NX-API の有効化（Enable NX-API on HTTP）] チェックボックスをオンにすると、アプリケーションは HTTP を使用します。

[インバンド管理（Inband Mgmt）]：外部およびクラシック LAN ファブリックの場合、このノブを使用すると DCNM は、インバンド接続（スイッチ ループバック、ルーテッド、または SVI インターフェイス経由で到達可能）でのスイッチのインポートおよび管理が可能になり、またアウトオブバンド接続（つまり、スイッチ mgmt0 インターフェイス経由で到達可能）でのスイッチの管理が可能になります。唯一の要件は、インバンド管理型スイッチの場合、eth2（別名インバンドインターフェイス）を介して DCNM からスイッチ IP に到達可能であることです。この目的のために、DCNM で静的ルートが必要になる場合があります。これは、[管理（Administration）] > [カスタマイズ（Customization）] > [ネットワーク設定（Network Preferences）]オプションで構成できます。インバンド管理を有効にした後、検出中に、インバンド管理を使用してインポートするすべてのスイッチの IP を指定し、最大ホップ数を 0 に設

定します。DCNM は、インバンド管理されたスイッチ IP が eth2 インターフェイスを介して到達可能であるかを検証する事前チェックを行います。事前チェックをパスすると、DCNM はインターフェイスが属する VRF に加えて、指定された検出 IP を持つそのスイッチ上のインターフェイスを検出し、学習します。スイッチのインポート/検出のプロセスの一部として、この情報は DCNM に入力される目的の基準設定にキャプチャされます。詳細については、外部ファブリックおよび LAN クラシック ファブリックでのインバンド管理 （223 ページ）を参照してください。

（注） ブートストラップまたは POAP は、アウトオブバンド接続、つまりスイッチ mgmt0 を介して到達可能なスイッチでのみサポートされます。DCNM 上のさまざまな POAP サービスは通常、eth1 またはアウトオブバンド インターフェイスにバインドされます。DCNM eth0/eth1 インターフェイスが同じ IP サブネットに存在するシナリオでは、POAP サービスは両方のインターフェイスにバインドされます。

[精密時間プロトコル（PTP）の有効化（Enable Precision Time Protocol（PTP））]：ファブリック全体で PTP を有効にします。このチェックボックスをオンにすると、PTP がグローバルに有効になり、コアに面するインターフェイスで有効になります。また、[PTP 送信元ループバック ID（PTP Source Loopback Id）] および [PTP ドメイン ID（PTP Domain Id）] フィールドが編集可能になります。詳細については、外部ファブリックおよび LAN クラシック ファブリック向け高精度時間プロトコル（PTP） （224 ページ）を参照してください。

[ファブリック自由形式（Fabric Freeform）]：この自由形式フィールドを使用して、外部ファブリックで検出されたすべてのデバイスに構成をグローバルに適用できます。

[AAA 自由形式の構成（AAA Freeform Config）]：AAA 自由形式の構成を指定します。

ステップ 6 [リソース（Resources）] タブをクリックします。このタブのフィールドは次のとおりです。

[サブインターフェイス Dot1q 範囲（Subinterface Dot1q Range）]：サブインターフェイス 802.1Q 範囲とアンダーレイ ルーティング ループバック IP アドレス範囲が自動入力されます。

[アンダーレイ ルーティング ループバック IP 範囲（Underlay Routing Loopback IP Range）]：プロトコル ピアリングのループバック IP アドレスを指定します。

[アンダーレイ MPLS ループバック IP 範囲（Underlay MPLS Loopback IP Range）]：アンダーレイ MPLS SR または LDP ループバック IP アドレス範囲を指定します。

IP 範囲は一意である必要があります。つまり、他のファブリックの IP 範囲と重複しないようにする必要があります。

ステップ 7 [設定（Configuration）] タブをクリックします。このタブのフィールドは次のとおりです。

[毎時ファブリック バックアップ（Hourly Fabric Backup）]：ファブリック構成とインテントの毎時バックアップを有効にします。

[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]：毎日のバックアップを有効にします。

[スケジュール済みの時間（Scheduled Time）]：スケジュールされたバックアップ時間を 24 時間形式で指定します。[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）] チェックボックスをオンにすると、このフィールドが有効になります。

（注） 毎時またはスケジュールされたバックアップは、次の CC の毎時実行後にのみ実行されます。バックアップは、スケジュールされた時間が経過した後にのみ実行され、その時間が経過した後に CC が実行されるたびに実行されます。

バックアップと復元のプロセスは、外部ファブリックのプロセスに似ています。外部ファブリックのバックアップおよび復元に関する詳細については、ファブリックのバックアップと復元 （371 ページ） を参照してください。

ステップ 8 **[ブートストラップ（Bootstrap）]** タブをクリックします。このタブのフィールドは次のとおりです。

ブートストラップの有効化（NX-OS スイッチのみ）（Enable Bootstrap）（For NX-OS Switches Only） ：Cisco Nexus スイッチのみに対してブートストラップ機能を有効にするにはこのチェックボックスをオンにします。

ブートストラップをイネーブルにした後、次のいずれかの方法を使用して、DHCP サーバで IP アドレスの自動割り当てをイネーブルにできます。

- [外部 DHCP サーバー（External DHCP Server）] : **スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]** および **[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** フィールドの外部 DHCP サーバーについての情報を入力します。
- [ローカル DHCP サーバー（Local DHCP Server）] : **[ローカル DHCP サーバー（Local DHCP Server）]** チェックボックスを有効にして、残りの必須フィールドに詳細を入力します。

ローカル DHCP サーバーの有効化（Enable Local DHCP Server） ：ローカル DHCP サーバーを介した自動 IP アドレス割り当ての有効化を開始するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、残りのすべてのフィールドが編集可能になります。

[DHCP バージョン（DHCP Version）] : このドロップダウンリストから [DHCPv4] または [DHCPv6] を選択します。DHCPv4 を選択すると、**[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]** フィールドが無効になります。DHCPv6 を選択すると、**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** は無効になります。

（注） Cisco DCNM IPv6 POAP は、Cisco Nexus 7000 シリーズ スイッチではサポートされていません。Cisco Nexus 9000 および 3000 シリーズ スイッチは、スイッチが L2 隣接（eth1 またはアウトオブバンド サブネットは /64 が必須）、またはスイッチがいくつかの IPv6 /64 サブネット内に存在する L3 隣接である場合にのみ、IPv6 POAP をサポートします。/64 以外のサブネット プレフィックスはサポートされません。

このチェックボックスをオンにしない場合、DCNM は自動 IP アドレス割り当てにリモートまたは外部 DHCP サーバーを使用します。

[DHCP スコープ開始アドレス（DHCP Scope Start Address）] および [DHCP スコープ終了アドレス（DHCP Scope End Address）] : スイッチのアウトオブバンド POAP に使用される IP アドレス範囲の最初と最後の IP アドレスを指定します。

[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]：スイッチの管理 VRF のデフォルト ゲートウェイを指定します。

スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）：スイッチの Mgmt0 インターフェイスのプレフィックスを指定します。プレフィックスは 8 ～ 30 の間である必要があります。

DHCP スコープおよび管理デフォルト ゲートウェイ *IP* アドレスの仕様（*DHCP scope and management default gateway IP address specification*）：管理デフォルト ゲートウェイ IP アドレスを 10.0.1.1 に、サブネットマスクを 24 に指定した場合、DHCP スコープが指定したサブネット、10.0.1.2 ～ 10.0.1.254 の範囲内であることを確認してください。

[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]：スイッチの Mgmt0 インターフェイスの IPv6 プレフィックスを指定します。プレフィックスは 112 ー 126 の範囲で指定する必要があります。このフィールドは DHCP の IPv6 が有効な場合に編集できます。

[AAA 構成の有効化（Enable AAA Config）]：AAA 構成を有効にします。これには、デバイスの起動時に **[詳細（Advanced）]** タブからの AAA 構成が含まれます。

ブートストラップ自由形式の構成（Bootstrap Freeform Config）：（任意）必要に応じて追加のコマンドを入力します。たとえば、AAAまたはリモート認証関連の構成を使用している場合は、このフィールドにこれらの構成を追加してインテントを保存します。デバイスが起動すると、[Bootstrap Freeform Config]フィールドで定義されたインテントが含まれます。

running-config をコピーして **[自由形式の構成（freeform config）]** フィールドに正しいインデントでペーストします。NX-OS スイッチの実行構成に表示されているように正しく行ってください。freeform config は running config と一致する必要があります。詳細については、「スイッチでの自由形式の構成エラーの解決」を参照してください。

[DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）]：1 行に 1 つのサブネット スコープを入力して、フィールドを指定します。**[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）]** チェックボックスをオンにした後で、このフィールドは編集可能になります。

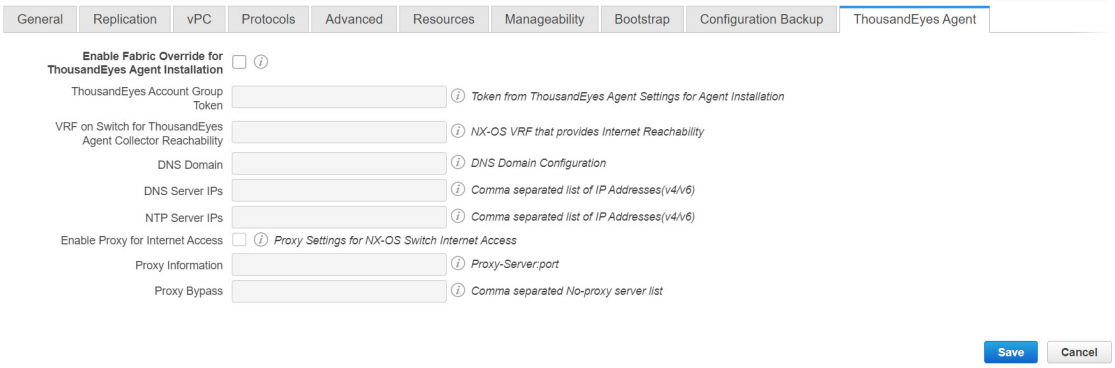
スコープの形式は次の順で定義する必要があります。

[DHCP スコープ開始アドレス、DHCP スコープ終了アドレス、スイッチ管理デフォルト ゲートウェイ、スイッチ管理サブネット プレフィックス（DHCP Scope Start Address, DHCP Scope End Address, Switch Management Default Gateway, Switch Management Subnet Prefix）]

例：10.6.0.2、10.6.0.9、16.0.0.1、24

外部ファブリックが作成されると、外部ファブリック トポロジ ページが表示されます。

ステップ 9 **[ThousandEyes Agent]** タブをクリックします。この機能は、Cisco DCNM リリース 11.5（3）でのみサポートされています。詳細については、「Cisco DCNM での ThousandEyes Enterprise Agent のグローバル設定の構成」を参照してください。



このタブのフィールドは次のとおりです。

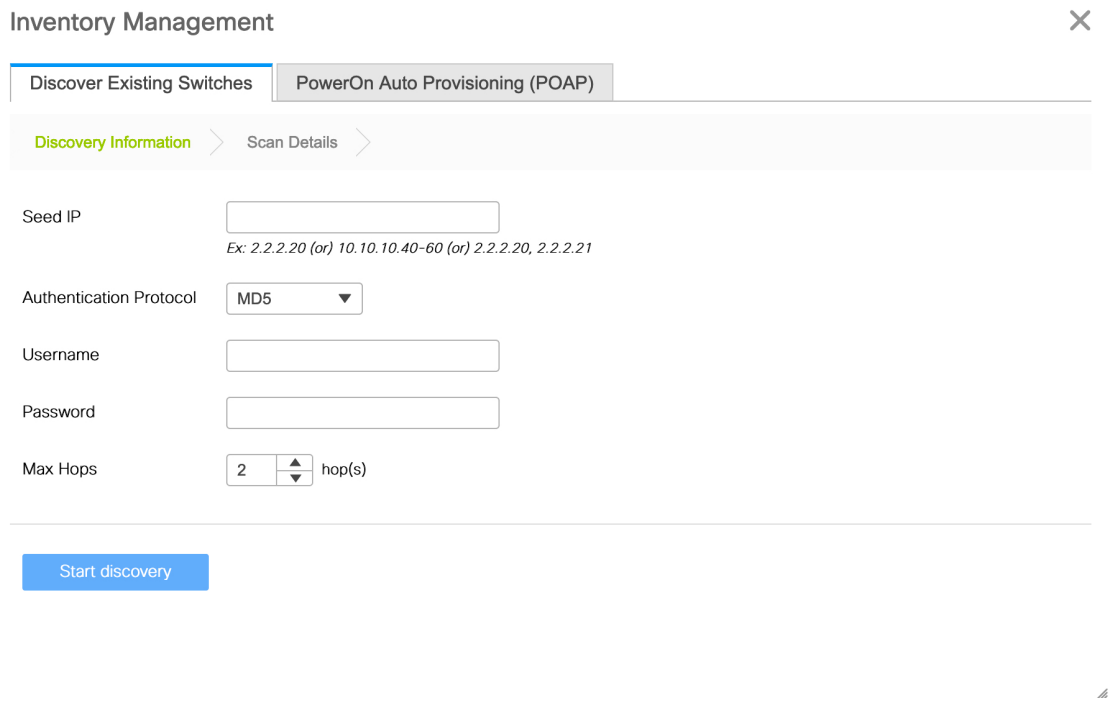
（注） ThousandEyes Agent のファブリック設定はグローバル設定を上書きし、そのファブリック内のスイッチにインストールされているすべての ThousandEyes エージェントに同じ構成を適用します。

- **[ThousandEyes Agent インストールのファブリック オーバーライドを有効にする（Enable Fabric Override for ThousandEyes Agent Installation）]**：チェック ボックスを選択して、ファブリックで ThousandEyes Enterprise Agent を有効にします。
- **[ThousandEyes アカウント グループ トークン（ThousandEyes Account Group Token）]**：インストール用の ThousandEyes Enterprise Agent アカウント グループ トークンを指定します。
- **[ThousandEyes Agent コレクタ到達可能性のスイッチ上の VRF（VRF on Switch for ThousandEyes Agent Collector Reachability）]**：インターネットの到達可能性を提供する VRF データを指定します。
- **[ドメイン ネーム システム（DNS） ドメイン（DNS Domain）]**：スイッチのドメイン ネーム システム（DNS） ドメイン構成を指定します。
- **[ドメイン ネーム システム（DNS） サーバ IP（DNS Server IPs）]**： ドメイン ネーム システム（DNS） サーバの IP アドレス（v4/v6）のカンマ区切りリストを指定します。DNS サーバには、最大 3 つの IP アドレスを入力できます。
- **[NTP サーバ IP（NTP Server IPs）]**： Network Time Protocol (NTP) サーバの IP アドレス（v4/v6）のコンマ区切りリストを指定します。NTP サーバには、最大 3 つの IP アドレスを入力できます。
- **[プロキシを有効にする（Enable Proxy）]**：チェックボックスをオンにして、NX-OS スイッチのインターネット アクセスのプロキシ設定を選択します。
- **[プロキシ情報（Proxy Information）]**：プロキシ サーバのポート情報を指定します。
- **[プロキシ バイパス（Proxy Bypass）]**：プロキシをバイパスするサーバ リストを指定します。

LAN クラシック ファブリックへのスイッチの追加

手順

ステップ 1 スイッチの **[追加（Add）]** をクリックします。**[インベントリ管理（Inventory Management）]** ウィンドウが表示されます。



[表形式ビュー（Tabular View）] > **[スイッチ（Switches）]** > **[+]** をクリックして、スイッチを追加することもできます。

ステップ 2 スイッチの IP アドレス（**[シード IP（Seed IP）]**）を入力します。

ステップ 3 スイッチ管理者ユーザ名およびパスワードを入力します。

ステップ 4 画面の下部にある **[検出の開始（Start discovery）]** をクリックします。**[スキャン詳細（Scan Details）]** セクションが間もなく表示されます。**[最大ホップ（Max Hops）]** フィールドに 2 が入力されているため、指定された IP アドレスを持つスイッチとその 2 ホップのスイッチが入力されます。

ステップ 5 該当するスイッチの横にあるチェックボックスをオンにし、**[ファブリックにインポート（Import into fabric）]** をクリックします。

複数のスイッチを同時に検出できます。スイッチは適切にケーブル接続し DCNM サーバーに接続する必要があり、スイッチのステータスは管理可能である必要があります。

スイッチ検出プロセスが開始されます。[進行状況（Progress）] 列には、進行状況が表示されます。DCNM がスイッチを検出すると、画面が閉じ、ファブリック画面が再び表示されます。ファブリック画面の中央にスイッチ アイコンが表示されます。

ステップ 6 最新のトポロジ表示を表示するには、トポロジの **[更新（Refresh）]** をクリックします。

詳細については、以下を参照してください。

- 既存のスイッチの検出 （90 ページ）
- 新しいスイッチの検出 （97 ページ）

ファブリック グループの作成とメンバー ファブリックの関連付け

この手順は、**[Fabric_Group]** を作成し、**[LAN_Classic]** ファブリックを追加する方法を示しています。**[Fabric_Group]** テンプレートは、視覚化のために **[LAN_Classic]** ファブリックをグループ化するために使用されます。

次の機能は **[Fabric_Group]** ではサポートされていません。

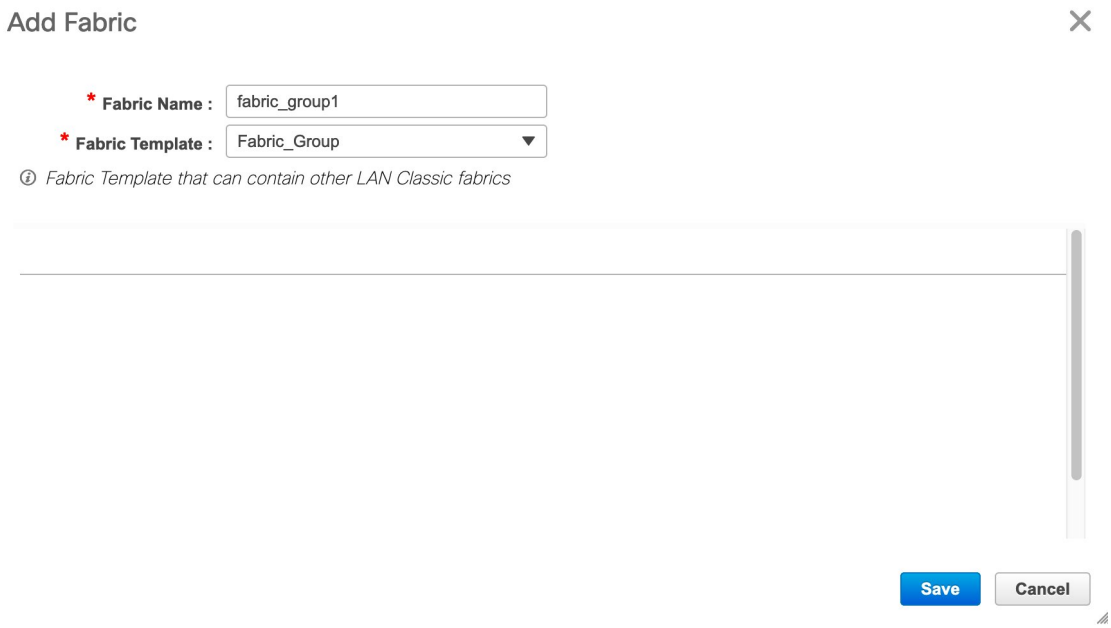
- ファブリックのバックアップと復元
- VXLAN オーバーレイまたは IFC 展開
- ファブリック テンプレートを他のファブリック テンプレートから、または他のファブリック テンプレートに変更する
- **[Fabric_Group]** は構成を管理しないため、**[保存と展開（Save & Deploy）]** をクリックするとエラーが報告されます。

手順

ステップ 1 **[制御（Control）]** > **[ファブリック（Fabrics）]** > **[ファブリック ビルダ（Fabric Builder）]** に移動します。

ステップ 2 [ファブリックの作成（Create Fabric）] をクリックします。

ステップ 3 ファブリック名を入力し、**[ファブリック テンプレート（Fabric Template）]** ドロップダウンリストから **[Fabric_Group]** を選択します。



ステップ 4 [保存（Save）] をクリックします。

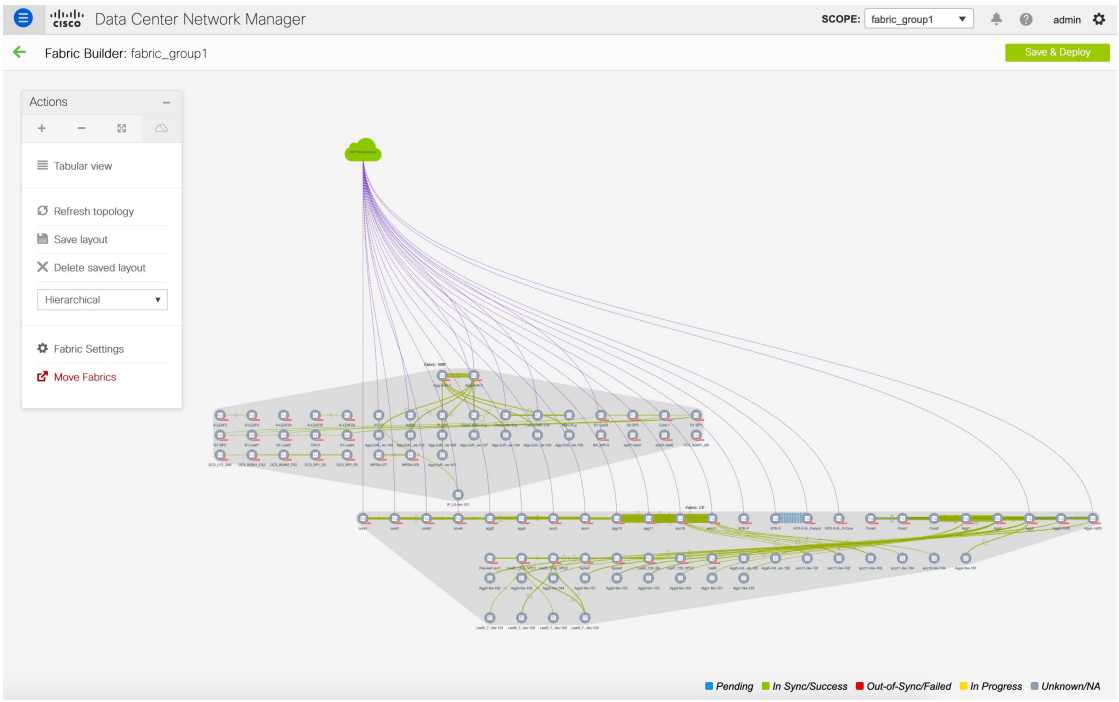
ステップ 5 **[アクション（Actions）]** パネルで、**[ファブリックの移動（Move Fabrics）]** をクリックします。

ステップ 6 **[ファブリックの移動（Move Fabric）]** ウィンドウで **[LAN_Classic]** ファブリックを選択します。

（注） ファブリック グループ内の **[LAN_Classic]** ファブリックのみを選択して追加できます。

ステップ 7 [追加（Add）] をクリックします。

同様に、メンバー ファブリックを選択して **[削除（Remove）]** をクリックすることで、メンバー ファブリックを削除できます。



LAN クラシック ファブリック テンプレートのファブリック内接続のサポート

[LAN_Classic] ファブリックは、次の条件で VRF-Lite、Multi-Site、および MPLS IFC をサポートします。

- DCI/VRF-Lite および Multi-Site IFC の接続先として **[LAN_Classic]** ファブリックがサポートされていますが、必要な情報を提供することで手動でのみ作成できます。**[Easy_Fabric_11_1]** および **[MSD_Fabric_11_1]** ファブリックで自動展開オプションが有効になっている場合でも、これらは自動的に作成されません。
- 存在しない（メタ）スイッチを **[LAN_Classic]** ファブリックに追加することはできません。メタ スイッチは、DCNM が検出できないスイッチまたはデバイスのプレースホルダです。
- 「エッジ ルータ」および「コア ルータ」スイッチ ロールの基本 BGP 構成は、自動生成されません。これらは、**[switch_freeform]** ポリシーまたはその他の適切な手段を使用して構成します。
- ファブリック設定で MPLS ハンドオフが有効になっている場合、MPLS 基本構成は、「エッジ ルータ」および「コア ルータ」スイッチ ロールに対して自動生成されます。

外部ファブリックおよびLANクラシックファブリックでのインバンド管理

リリース 11.5(1) 以降 Cisco DCNM では、ブラウンフィールド展開でのみ、外部および LAN クラシック ファブリックのインバンド接続のスイッチをインポートまたは検出できます。ファブリック設定を構成または編集しながら、ファブリックごとにインバンド管理を有効にします。POAP を使用してインバンド接続のスイッチをインポートまたは検出することはできません。

設定後、ファブリックはインバンド管理の VRF に基づいてスイッチの検出を試みます。ファブリック テンプレートは、シード IP を使用してインバンド スイッチのVRFを決定します。同じシード IP に複数の VRF がある場合、シードインターフェイスのインテントは学習されません。インテント/設定を手動で作成する必要があります。

ファブリック設定を構成/編集した後、保存して展開する必要があります。インバンド管理対象スイッチをファブリックにインポートした後は、インバンド管理設定を変更できません。このチェックボックスをオフにすると、次のエラー メッセージが生成されます。

```
Inband IP <<IP Address>> cannot be used to import the switch,
please enable Inband Mgmt in fabric settings and retry.
```

スイッチをファブリックにインポートしたら、インターフェイスを管理してインテントを作成する必要があります。スイッチをインポートするインターフェイスのインテントを作成します。インターフェイス コンフィギュレーションを編集/更新します。このインバンド管理スイッチのインターフェイス IP を変更しようとすると、エラー メッセージが生成されます。

```
Interface <<interface_name>> is used as seed or next-hop egress interface
for switch import in inband mode.
IP/Netmask Length/VRF changes are not allowed for this interface.
```

インターフェイスの管理中に、インバンド管理を使用してインポートされたスイッチでは、スイッチのシード IP を変更できません。次のエラーが生成されます。

```
<<switch-name>>: Mgmt0 IP Address (<ip-address>) cannot be changed,
when is it used as seed IP to discover the switch.
```

ネクストホップ インターフェイスのポリシーを作成します。サードパーティ製デバイスから DCNM へのルートには、ECMP ルートと呼ばれる複数のインターフェイスが含まれる場合があります。ネクストホップインターフェイスを検索し、スイッチのインテントを作成します。インターフェイス IP および VRF の変更は許可されません。

インバンド管理が有効になっている場合、イメージ管理中に、ISSU、EPLD、RPM、および SMU インストール フローで、スイッチ上のイメージをコピーするために eth2 IP アドレスが使用されます。

ファブリック内のインバンド接続を使用してスイッチをインポートし、後でファブリック設定でインバンド管理を無効にすると、次のエラー メッセージが生成されます。

```
The fabric <<fabric name>> was updated with below message:
Fabric Settings cannot be changed for Inband Mgmt, when switches are already imported
using inband Ip. Please remove the existing switches imported using Inband Ip from the
fabric,
then change the Fabric Setttings.
```

ただし、同じファブリックに、インバンド接続とアウトオブバンド接続の両方を使用してインポートされたスイッチを含めることができます。

外部ファブリックおよびLANクラシック ファブリック向け高精度時間プロトコル（PTP）

リリース 11.5(1) から、**[External_Fabric_11_1]** または **[LAN_Classic]** テンプレートのファブリック設定で、**[高精度時間プロトコル（PTP）を有効化（Enable Precision Time Protocol（PTP））]** チェックボックスをオンにして、ファブリック全体で PTP を有効にします。このチェックボックスを選択すると、PTP はグローバルで、およびコア向きのインターフェイスで有効化されます。また、**[PTP ループバック ID（PTP Loopback Id）]** および **[PTP ドメイン ID（PTP Domain Id）]** フィールドは編集可能です。

PTP 機能は、NX-OS バージョン 7.0(3)I7(1) 以降の Cisco Nexus 9000 シリーズ クラウド スケール スイッチでサポートされます。ファブリック内にクラウドスケール以外のデバイスがあり、PTP が有効になっていない場合は、警告が表示されます。クラウドスケールデバイスの例としては、Cisco Nexus 93180YC-EX、Cisco Nexus 93180YC-FX、Cisco Nexus 93240YC-FX2、および Cisco Nexus 93360YC-FX2 スイッチがあります。詳細については、https://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html#~products を参照してください。

Note PTP グローバル設定は、Cisco Nexus 3000 シリーズ スイッチでサポートされます。ただし、PTP および ttag の設定はサポートされていません。

詳細については、『*Cisco Nexus 9000* シリーズ *NX-OS* システム管理構成ガイド』の「*PTP* の構成」の章、および『*Cisco DCNM* ユーザーガイド（「リソース アプリケーション向け *Cisco Network Insights*」』を参照してください。

外部および LAN クラシック ファブリック展開の場合、PTP をグローバルに有効にし、コア側のインターフェイスで PTP を有効にする必要があります。インターフェイスは、VM や Linux ベースのマシンのような外部 PTP サーバに対して構成できます。したがって、インターフェイスを編集して、グランドマスター クロックと接続する必要があります。PTP および TTAG 構成を外部および LAN クラシック ファブリックで動作させるには、**host_port_resync** ポリシーを使用して DCNM にスイッチ構成を同期する必要があります。詳細については、アウトオブバンド スイッチ インターフェイス構成と DCNM の同期, on page 226を参照してください。

グランドマスター クロックは Easy ファブリックの外部で構成する必要があり、IP 到達可能です。グランドマスター クロックへのインターフェイスは、[interface freeform config] を使用して PTP で有効にする必要があります。

[保存して展開（Save & Deploy）] をクリックすると、すべてのコア側インターフェイスが PTP 構成で自動的に有効になります。このアクションにより、すべてのデバイスがグランドマスター クロックに確実に PTP 同期されます。さらに、ホスト、ファイアウォール、サービス ノード、またはその他のルータに接続されている境界デバイスやリーフ上のインターフェイスなど、コア側でないインターフェイスについては、ttag 関連の CLI を追加する必要があります。ttag は、VXLAN EVPN ファブリックに入るすべてのトラフィックに追加され、トラフィックがこのファブリックを出るときに ttag を削除する必要があります。

次に、PTP の構成例を示します。`feature ptp`

```
feature ptp

ptp source 100.100.100.10 -> IP address of the loopback interface (loopback0)
that is already created, or user-created loopback interface in the fabric settings

ptp domain 1 -> PTP domain ID specified in fabric settings

interface Ethernet1/59 -> Core facing interface
  ptp

interface Ethernet1/50 -> Host facing interface
  ttag
  ttag-strip
```

次のガイドラインはPTPで適用可能です。

- ファブリック内のすべてのスイッチにCisco NX-OSリリース7.0(3)I7(1)以降のバージョンが搭載されている場合、ファブリックでPTP機能をイネーブルにできます。それ以外の場合、次のエラー メッセージが表示されます。

  ```
  PTP feature can be enabled in the fabric, when all the switches have
  NX-OS Release 7.0(3)I7(1) or higher version. Please upgrade switches to
  NX-OS Release 7.0(3)I7(1) or higher version to enable PTP in this fabric.
  ```

- NIRのハードウェア テレメトリ サポートでは、PTP構成が前提条件です。
- PTP構成を含む既存のファブリックに非クラウド スケール デバイスを追加すると、次の警告が表示されます。

  ```
  TTAG is enabled fabric wide, when all devices are cloud-scale switches
  so it cannot be enabled for newly added non cloud-scale device(s).
  ```

- ファブリックにクラウドスケール デバイスと非クラウドスケール デバイスの両方が含まれている場合、PTPを有効にしようとすると、次の警告が表示されます。

  ```
  TTAG is enabled fabric wide when all devices are cloud-scale switches
  and is not enabled due to non cloud-scale device(s).
  ```

- ホスト構成の同期がすべてのデバイスで実行されると、すべてのデバイスに対してTTAG構成が生成されます。新しく追加されたすべてのデバイスでホスト構成の同期が実行されない場合、新しく追加されたデバイスのTtag構成は生成されません。

  構成が同期されていない場合は、次の警告が表示されます。

  ```
  TTAG on interfaces with PTP feature can only be configured for cloud-scale devices.
  It will not be enabled on any newly added switches due to the presence of non
  cloud-scale devices.
  ```

- PTPおよびTTAG構成は、ホスト インターフェイスに展開されます。
- PTPおよびTTAG構成は、同じファブリック内のスイッチ間でサポートされます（ファブリック内リンク）。PTPはファブリック間リンク用に作成され、ttagは他のファブリック（スイッチ）がDCNMによって管理されていない場合に作成されます。ファブリック間リンクは、両方のファブリックがDCNMによって管理されている場合、PTPまたはttag構成をサポートしません。
- TTAG設定は、ブレークアウト後にデフォルトで設定されます。リンクが検出され、ブレークアウト後に接続されたら、[保存および展開（Save & Deploy）]を実行して、ポート

のタイプ（ホスト、ファブリック内リンク、またはファブリック間リンク）に基づいて正しい構成を生成します。

アウトオブバンド スイッチ インターフェイス構成と DCNM の同期

DCNM リリース 11.5(1) 以降、DCNM の外部で（CLI を介して）作成されたすべてのインターフェイス レベルの構成を DCNM に同期し、DCNM から管理できます。また、vPC ペア構成は自動的に検出され、ペアリングされます。これは、External_Fabric_11_1 および LAN_Classic ファブリックにのみ適用されます。vPC ペアリングは **vpc_pair** ポリシーで実行されます。

（注） DCNM がスイッチを管理している場合は、すべての構成変更が DCNM から開始されることを確認し、スイッチで直接変更を行わないようにします。

インターフェイス構成が DCNM インテントに同期されると、スイッチ構成が参照と見なされます。つまり、同期アップの終了時に、スイッチに存在する内容が DCNM インテントに反映されます。再同期操作の前にそれらのインターフェイスに展開されていないインテントが DCNM にある場合、それらは失われます。

ガイドライン

- Easy_Fabric_11_1、External_Fabric_11_1、および LAN_Classic テンプレートを使用するファブリックでサポートされます。
- Cisco Nexus スイッチでのみサポートされます。
- 再同期前にファブリック アンダーレイ関連ポリシーが関連付けられていないインターフェイスでサポートされます。たとえば、IFC インターフェイスとファブリック内リンクは再同期の対象になりません。
- 再同期の前に関連付けられているカスタム ポリシー（Cisco DCNM に付属していないポリシー テンプレート）がないインターフェイスでサポートされます。
- 再同期前に Cisco DCNM の機能やアプリケーションによってインテントが排他的に所有されていないインターフェイスでサポートされます。
- インターフェイス グループが関連付けられていないスイッチでサポートされます。
- インターフェイスモード（スイッチポートからルーテッド、トランクからアクセスなど）の変更は、そのインターフェイスに接続されたオーバーレイではサポートされません。

同期アップ機能は、次のインターフェイス モードおよびポリシーでサポートされます。

インターフェイス モード	ポリシー

トランク（スタンドアロン、po、および vPC PO）	• int_trunk_host_11_1 • int_port_channel_trunk_host_11_1 • int_vpc_trunk_host_11_1
アクセス（スタンドアロン、po、および vPC PO）	• int_access_host_11_1 • int_port_channel_access_host_11_1 • int_vpc_access_host_11_1
dot1q-tunnel	• int_dot1q_tunnel_host_11_1 • int_port_channel_dot1q_tunnel_host_11_1 • int_vpc_ dot1q_tunnel_host_11_1
ルーテッド	int_routed_host_11_1
loopback	int_freeform
sub-interface	int_subif_11_1
FEX (ST, AA)	• int_port_channel_fex_11_1 • int_port_channel_aa_fex_11_1
ブレイクアウト	interface_breakout
nve	int_freeform（External_Fabric_11_1/LAN_Classic のみ）
SVI	int_freeform（External_Fabric_11_1/LAN_Classic のみ）
mgmt0	int_mgmt_11_1

Easyファブリックでは、インターフェイスの再同期によって、インターフェイス上のアクセス VLAN または許可された VLAN に基づいて、ネットワーク オーバーレイ接続が自動的に更新されます。

再同期操作が完了すると、スイッチ インターフェイスのインテントを通常の DCNM 手順で管理できます。

スイッチ インターフェイス構成と DCNM の同期

始める前に

- インターフェイスの再同期を試みる前に、ファブリックのバックアップを作成することをお勧めします。
- **[External_Fabric_11_1]** および **[LAN_Classic]** ファブリックで vPC ペアリングが正しく機能するには、両方のスイッチがファブリック内にあり、機能している必要があります。

- スイッチが **[同期（In-Sync）]** しており、スイッチ モードが**[移行モード（Migration-mode）]** または **[メンテナンス モード（Maintenance-mode）]** でないことを確認します。

手順

ステップ 1 DCNM で、**[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** に移動し、ファブリックをクリックします。

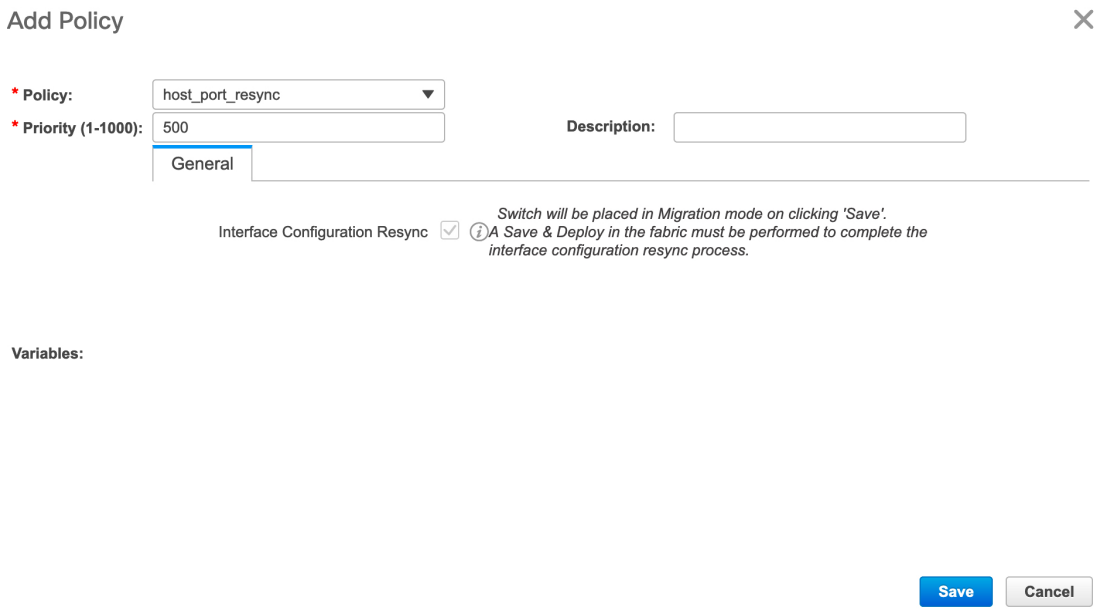
ステップ 2 スイッチがファブリックに存在し、vPC ペアリングが完了していることを確認します。これらは **[トポロジ（Topology）]** 表示に示されています。**[アクション（Actions）]** パネルで **[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 **[表形式ビュー（Tabular view）]** から、インターフェイス インテントの再同期が必要な 1 つ以上のスイッチを選択して、**[ポリシー（Policies）]** をクリックします。

（注）
- スイッチのペアが **no_policy** または **vpc_pair** のいずれかを使用してすでにペアリングされている場合は、ペアの一方のスイッチのみを選択します。
- スイッチのペアがまだペアリングされていない場合は、両方のスイッチを選択します。

ステップ 4 **[ポリシー（Policies）]** ウィンドウで、**[ポリシーの追加（Add Policy）]** アイコンをクリックします。

ステップ 5 **[ポリシーの追加（Add Policy）]** ウィンドウで、**[host_port_resync]** を **[ポリシー（Policy）]** ドロップダウンリストから選択します。[保存（Save）] をクリックします。



ステップ 6 スイッチの **[モード（Mode）]** 列をチェックして、それらが **[移行（Migration）]** を報告していることを確認します。vPC ペアの場合、両方のスイッチが **Migration-mode** になります。

- この手順の後、**[トポロジ（Topoplogy）]** ビューのスイッチは **Migration-mode** になります。
- いずれかのスイッチを移行モードにしただけでも、vPC ペアの両方のスイッチが移行モードになります。
- スイッチが意図せずに再同期モードになった場合は、**[host_port_resync]** ポリシー インスタンスを識別して **[ポリシー（Policies）]** ウィンドウから削除することで、通常モードに戻すことができます。

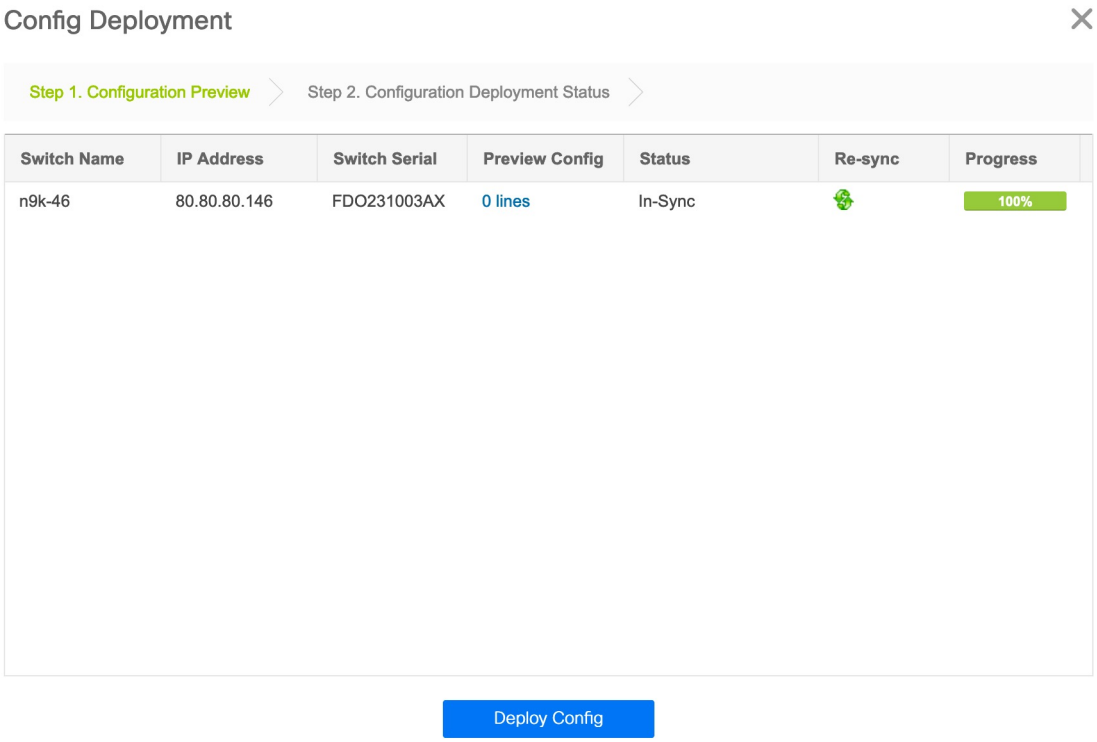
ステップ 7 構成の変更を DCNM に同期する準備ができたら、**[表形式ビュー（Tabular view）]** に移動して必要なスイッチを選択し、**[スイッチの再検出（Rediscover switch）]** をクリックして、DCNM が新しいインターフェイスやその他の変更を認識していることを確認します。

ステップ 8 **[保存と展開（Save & Deploy）]** をクリックして、再同期プロセスを開始します。

（注） このプロセスは、スイッチ構成のサイズと関連するスイッチの数によっては、完了するまでに時間がかかる場合があります。

ステップ 9 再同期操作中にエラーが検出されなかった場合は、**[構成展開（Config Deployment）]** ウィンドウが表示されます。インターフェイス インテントは DCNM で更新されます。

（注） External_Fabric_11_1 または LAN_Classic ファブリックが **[監視モード（Monitored Mode）]** の場合、ファブリックが読み取り専用モードであることを示すエラー メッセージが表示されます。このエラー メッセージは、再同期プロセスが失敗したことを意味するものではないため、無視してかまいません。



[構成展開（Config Deployment）] ウィンドウを閉じると、スイッチが自動的に **[移行モード（Migration-mode）]** を終えたことが観察できます。ペアになっていなかった、または **no_policy** を使用してペアになっていた vPC ペアのスイッチは、ペアとして表示され、**vpc_pair** ポリシーに関連付けられます。

（注） スイッチ用に作成された **host_port_resync** ポリシーは、再同期プロセスが正常に完了すると自動的に削除されます。

次のタスク

次の制限は、スイッチ インターフェイス構成を DCNM に同期した後に適用されます。

- ポートチャネル メンバーシップ（ポリシーが存在する場合）はサポートされていません。
- オーバーレイがアタッチされているインターフェイスのモードの変更（トランクからアクセスなど）はサポートされていません。
- **インターフェイス グループ**に属するインターフェイスの再同期はサポートされていません。
- **External_Fabric_11_1** および **LAN_Classic** テンプレートの vPC ペアリングは、**vpc_pair** ポリシーで更新する必要があります。

- オーバーレイがアタッチされているインターフェイスのモードの変更はサポートされていません。
- **Easy_Fabric** ファブリックでは、VXLAN オーバーレイ インターフェイスのアタッチは、許可された VLAN に基づいて自動的に実行されます。

Easy ファブリックおよび eBGP ファブリックでの MACsec サポート

Cisco DCNM リリース 11.5（1）からMACsec は、ファブリック内リンクの Easy Fabric および eBGP ファブリックでサポートされます。MACsec を設定するには、ファブリックおよび必要な各ファブリック内リンクで MACsec を有効にする必要があります。CloudSec とは異なり、MACsec の自動設定はサポートされていません。

MACsec は、Cisco NX-OS リリース 7.0(3)I7(8) および 9.3(5) 以降のスイッチでサポートされます。

（注） MACsec のサポートは、Cisco DCNM リリース 11.5(1) のプレビュー機能です。

ガイドライン

- リンクの物理インターフェイスで MACsec を設定できない場合は、**[保存（Save）]** をクリックするとエラーが表示されます。次の理由により、デバイスおよびリンクで MACsec を設定できません。
  - NX-OS の最小バージョンが満たされていません。
  - インターフェイスは MACsec に対応していません。
- ファブリック設定の MACsec グローバル パラメータは、いつでも変更できます。
- MACsec と CloudSec は BGW デバイス上で共存できます。
- MACsec はボーダー リーフではサポートされていません。
- MACsec が有効になっているリンクの MACsec ステータスが **[リンク（Links）]** ウィンドウに表示されます。
- MACsec が設定されたデバイスのブラウンフィールド移行は、スイッチおよびインターフェイスの自由形式の設定を使用してサポートされます。

  サポートされているプラットフォームとリリースを含むMACsec設定の詳細については、『Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイド』の「*MACsec* の設定」の章を参照してください。

次のセクションでは、 DCNM で MACsec を有効または無効にする方法を示します：

MACsec の有効化

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** に移動します。

ステップ 2 既存の Easy または eBGP ファブリックで **[ファブリックの作成（Create Fabric）]** をクリックして新しいファブリックを作成するか、**[ファブリックの編集（Edit Fabric）]** をクリックします。

ステップ 3 **[アドバンスト（Advanced）]** タブをクリックし、MACsec の詳細を指定します。

[MACsec の有効化（Enable MACsec）]：ファブリックの MACsec を有効にするには、このチェックボックスをオンにします。

[MACsec プライマリ キー文字列（MACsec Primary Key String）]：プライマリ MACsec セッションの確立に使用される Cisco Type 7 暗号化オクテット文字列を指定します。AES_256_CMAC の場合、キー文字列の長さは 130、AES_128_CMAC の場合、キー文字列の長さは 66 である必要があります。これらの値が正しく指定されていない場合、ファブリックの保存時にエラーが表示されます。

（注） デフォルトのキー ライフタイムは無期限です。

[MACsec プライマリ暗号化アルゴリズム（MACsec Primary Cryptographic Algorithm）]：プライマリ キー文字列に使用する暗号化アルゴリズムを選択します。**AES_128_CMAC** または **AES_256_CMAC** です。デフォルト値は **AES_128_CMAC** です。

プライマリ セッションが失敗した場合にバックアップ セッションを開始するように、デバイスのフォールバック キーを設定できます。

[MACsec フォールバック キー文字列（MACsec Fallback Key String）]：フォールバック MACsec セッションの確立に使用される Cisco Type 7 暗号化オクテット文字列を指定します。AES_256_CMAC の場合、キー文字列の長さは 130、AES_128_CMAC の場合、キー文字列の長さは 66 である必要があります。これらの値が正しく指定されていない場合、ファブリックの保存時にエラーが表示されます。

[MACsec フォールバック暗号化アルゴリズム（MACsec Fallback Cryptographic Algorithm）]：フォールバック キー文字列に使用する暗号化アルゴリズムを選択します。AES_128_CMAC または AES_256_CMAC です。デフォルト値は AES_128_CMAC です。

[MACsec 暗号スイート（MACsec Cipher Suite）]：MACsec ポリシーの次の MACsec 暗号スイートのいずれかを選択します。

- GCM-AES-128
- GCM-AES-256
- GCM-AES-XPN-128
- GCM-AES-XPN-256

デフォルト値は **GCM-AES-XPN-256** です。

（注） ファブリックの展開が完了した後、MACsec 設定はスイッチに展開されません。スイッチに MACsec 設定を展開するには、ファブリック内リンクで MACsec を有効にする必要があります。

[MACsec ステータス レポート タイマー（MACsec Status Report Timer）]：MACsec 動作ステータス定期レポート タイマーを分単位で指定します。

ステップ 4 ファブリックをクリックし、**[アクション（Actions）]** パネルで **[表形式ビュー（Tabular View）]** をクリックしてから、**[リンク（Links）]** をクリックします。

ステップ 5 MACsec を有効にするファブリック内リンクを選択し、**[リンクのアップデート（Update Link）]** をクリックします。

ステップ 6 **[リンク管理 - リンクの編集（Link Management – Edit Link）]** ウィンドウで、**[リンク プロファイル（Link Profile）]** セクションの **[アドバンスト（Advanced）]** をクリックし、**[MACsec の有効化（Enable MACsec）]** チェックボックスをオンにします。

MACsec がファブリック内リンクで有効になっているが、ファブリック設定では有効になっていない場合、**[保存（Save）]** をクリックするとエラーが表示されます。

MACsec がリンクで設定されると、次の設定が生成されます。

- MACsec を有効にする最初のリンクである場合は、MACsec グローバル ポリシーを作成します。
- リンクの MACsec インターフェイス ポリシーを作成します。

ステップ 7 **[保存（Save）]** をクリックし、**[保存と展開（Save & Deploy）]** をクリックして、MACsec 構成を展開します。

MACsec の無効化

ファブリック内リンクで MACsec を無効にするには、**[リンク管理 – リンクの編集（Link Management – Edit Link）]** ウィンドウに移動し、**[MACsec の有効化（Enable MACsec）]** チェックボックスをオフにして、**[保存（Save）]** をクリックし、**[保存と展開（Save & Deploy）]** をクリックします。このアクションは、次を実行します。

- リンクから MACsec インターフェイスポリシーを削除します。
- これが MACsec が有効になっている最後のリンクである場合、MACsec グローバル ポリシーもデバイスから削除されます。

リンクで MACsec を無効にした後でのみ、**[ファブリックの設定（Fabric Settings）]** に移動し、**[MACsec の有効化（Enable MACsec）]** チェックボックス（**[詳細（Advanced）]** タブ）をオフにして、ファブリックで MACsec を無効にすることができます。MACsec が有効になっているファブリック内にファブリック内リンクがある場合、**[保存と展開（Save & Deploy）]** をクリックするとエラーが表示されます。

テナント ルーテッド マルチキャストの概要

テナント ルーテッド マルチキャスト（TRM）は、BGP ベースの EVPN コントロール プレーンを使用する VXLAN ファブリック内でのマルチキャスト転送を有効にします。TRM は、ローカルまたは VTEP 間で同じサブネット内または異なるサブネット内の送信元と受信側の間にマルチテナント対応のマルチキャスト転送を実装します。

TRM を有効にすると、アンダーレイでのマルチキャスト転送が活用され、VXLAN でカプセル化されたルーテッド マルチキャスト トラフィックが複製されます。デフォルト マルチキャスト配信ツリー（デフォルト MDT）は、VRF ごとに構築されます。これは、レイヤ 2 仮想ネットワーク インスタンス（VNI）のブロードキャストおよび不明ユニキャスト トラフィック、およびレイヤ 2 マルチキャスト複製グループの既存のマルチキャスト グループに追加されます。オーバーレイ内の個々のマルチキャスト グループ アドレスは、複製および転送のためにそれぞれのアンダーレイ マルチキャスト アドレスにマッピングされます。BGP ベースのアプローチを使用する利点は、TRM を備えた BGP EVPN VXLAN ファブリックが、すべてのエッジ デバイスまたは VTEP に RP が存在する完全な分散型オーバーレイ ランデブー ポイント（RP）として動作できることです。

マルチキャスト対応のデータセンターファブリックは、通常、マルチキャストネットワーク全体の一部です。マルチキャスト送信元、受信側、およびマルチキャスト ランデブー ポイントはデータセンター内に存在する可能性がありますが、キャンパス内にある場合や WAN 経由で外部から到達可能である場合もあります。TRM を使用すると、既存のマルチキャスト ネットワークをシームレスに統合できます。ファブリック外部のマルチキャスト ランデブー ポイントを活用できます。さらに、TRM では、レイヤ 3 物理インターフェイスまたはサブインターフェイスを使用したテナント対応外部接続が可能です。

詳細については、次のトピックを参照してください。

- テナント ルーテッド マルチキャストに関する注意事項と制限事項
- レイヤ 3 テナント ルーテッド マルチキャストの注意事項と制約事項
- レイヤ 2/レイヤ 3 テナント ルーテッド マルチキャスト（混合モード）の注意事項と制約事項

VXLAN EVPN マルチサイトのテナント ルーテッド マルチキャストの概要

マルチサイトを使用したテナント ルーテッド マルチキャストは、マルチサイト経由で接続された複数の VXLAN EVPN ファブリック間でのマルチキャスト転送を可能にします。

次の 2 つのユース ケースがサポートされています。

- ユース ケース 1：TRM は、さまざまなサイトの送信元と受信者に、レイヤ 2 およびレイヤ 3 マルチキャスト サービスを提供します。
- ユース ケース 2：TRM 機能を VXLAN ファブリックからファブリック外部の送信元受信者に拡張します。

TRM Multi-Site は、BGP ベースの TRM ソリューションを拡張したもので、複数の VTEP を持つ複数の TRM サイトが相互に接続して、最も効率的な方法でサイト間でマルチキャスト サー

ビスを提供できるようにします。各TRMサイトは独立して動作しており、各サイトのボーダーゲートウェイは各サイトをつなぐことができます。サイトごとに複数のボーダーゲートウェイを設定できます。特定のサイトで、BGWはEVPNおよびMVPNルートを交換するために、他のサイトのルートサーバまたはBGWとピアリングします。BGWで、BGPはローカルVRF/L3VNI/L2VNIにルートをインポートし、ルートが学習された場所に応じて、それらのインポートされたルートをファブリックまたはWANにアドバタイズします。

VXLAN EVPN マルチサイト オペレーションのテナント ルーテッド マルチキャスト

VXLAN EVPN マルチサイトでの TRM の操作は次のとおりです。

- 各サイトはエニーキャスト VTEP BGW で表されます。BGW 間での DF の選択により、パケットの重複がなくなります。
- ボーダーゲートウェイ間のトラフィックは、入力複製メカニズムを使用します。トラフィックは VXLAN ヘッダーとともにカプセル化され、その後に IP ヘッダーが続きます。
- 各サイトは、パケットのコピーを 1 つだけ受信します。
- サイト間のマルチキャスト送信元および受信者情報は、TRM が設定されたボーダー ゲートウェイ上の BGP プロトコルによって伝播されます。
- 各サイトの BGW はマルチキャスト パケットを受信し、ローカル サイトに送信する前にパケットを再カプセル化します。

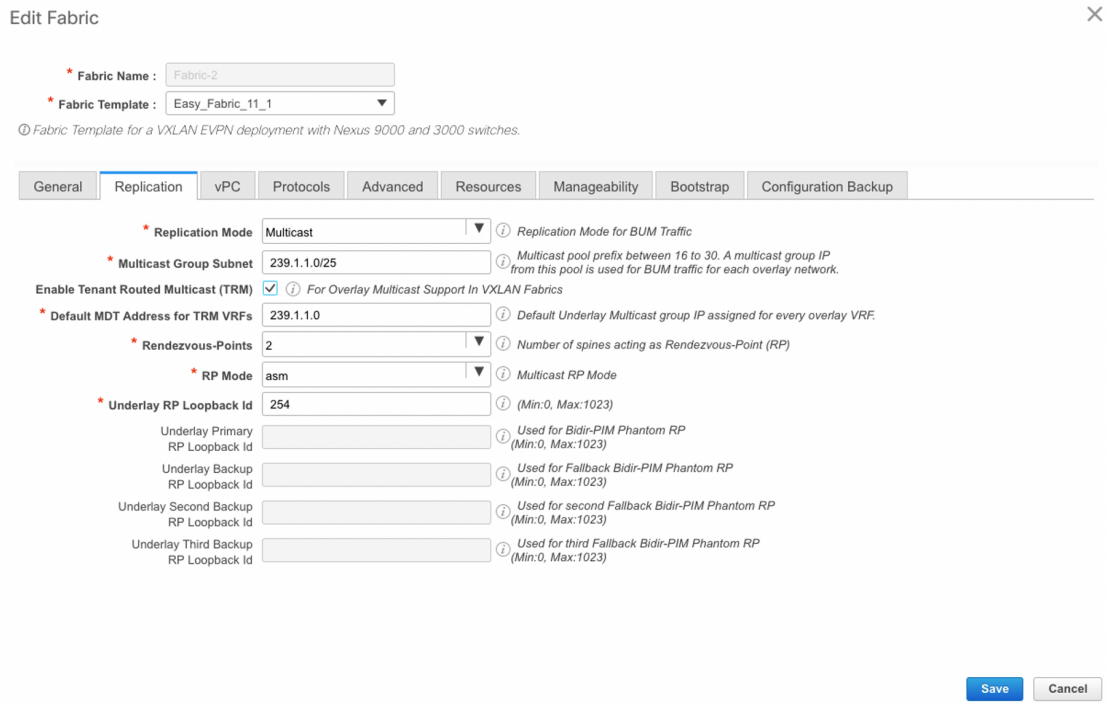
VXLAN EVPNマルチサイトでのTRMのガイドラインと制限事項については、「テナント ルーテッド マルチキャストの設定」を参照してください。

Cisco DCNM を使用したシングル サイト向け TRM の構成

この項では、VXLAN EVPN ファブリックが Cisco DCNM を使用してすでにプロビジョニングされていることを前提としています。

Procedure

ステップ 1 選択した Easy ファブリックの TRM を有効にします。ファブリック テンプレートが **[Easy_Fabric_11_1]** の場合は、[ファブリック（Fabric）]設定をクリックし、**[複製（Replication）]** タブに移動して、**[テナント ルーテッド マルチキャスト（TRM）の有効化（Enable Tenant Routed Multicast (TRM)）]** フィールドをオンにします。さらに、デフォルトの MDT マルチキャスト グループ フィールドには、デフォルト値が自動入力されます。



[テナント ルーテッド マルチキャスト（TRM）の有効化（Enable Tenant Routed Multicast（TRM））]：VXLAN BGP EVPN ファブリックで EVPN/MVPN を介してオーバーレイ マルチキャスト トラフィックをサポートできるようにするテナント ルーテッド マルチキャスト（TRM）を有効にするには、このチェックボックスをオンにします。

[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]：テナント ルーテッド マルチキャスト トラフィックのマルチキャスト アドレスが入力されます。デフォルトでは、このアドレスは [マルチキャスト グループ サブネット] フィールドで指定された IP プレフィックスから取得されます。いずれかのフィールドをアップデートする場合、**[マルチキャスト グループ サブネット（Multicast Group Subnet）]** で指定した IP プレフィックスから選択された TRM アドレスであることを確認してください。

[保存（Save）] をクリックして、ファブリックの設定を保存します。この時点で、すべてのスイッチは保留状態になるため、「青色」になります。**[保存して展開（Save and Deploy）]** をクリックして、以下を有効にします。

- 機能 ngmvpn の有効化（Enable feature ngmvpn）：BGP ピアリング向け次世代マルチキャスト VPN（ngMVPN）コントロール パネルを有効にします。
- IP マルチキャスト マルチパス s-g-hash next-hop-based の構成（Configure ip multicast multipath s-g-hash next-hop-based）：VRF で有効化された TRM 向けマルチパス ハーシング アルゴリズムです。
- IP IGMP スヌーピング VXLAN の構成（Configure ip igmp snooping vxlan）：VXLAN VLAN の IGMP スヌーピングを有効化します。
- IP マルチキャスト overlay-spt-only の構成（Configure ip multicast Overlay-spt-only）：すべての MPVN 対応 Cisco Nexus 9000 スイッチで MVPN ルートタイプ 5 を有効にします。

- MVPN BGP AFI ピアリングの設定と確立（Configure and Establish MVPN BGP AFI Peering）：これは、BGP RR とリーフ間のピアリングに必要です。

Easy_Fabric_eBGP ファブリック テンプレートを使用して作成された VXLAN EVPN ファブリックの場合は、[EVPN] タブに **[テナント ルーテッド マルチキャスト（TRM）の有効化（Enable Tenant Routed Multicast（TRM））]** フィールドと **[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]** フィールドが表示されます。

ステップ 2 VRF の TRM を有効にします。

[制御（Control）] > [VRF] に移動し、選択した VRF を編集します。**[詳細（Advanced）]** タブに移動し、次の TRM 設定を編集します。

TRM の有効化：TRM を有効にするためにチェックボックスを選択します。TRM を有効化する場合、RP アドレスおよびアンダーレイ マルチキャスト アドレスを入力する必要があります。

RP が外部：ファブリックに対して RP が外部である場合、このチェックボックスを有効にします。このフィールドのチェックがオフの場合、RP はすべての VTEP に分散されます。

Note RP が外部の場合、適切なオプションを選択します。RP が外部の場合、RP ループバック ID がグレー化されます。

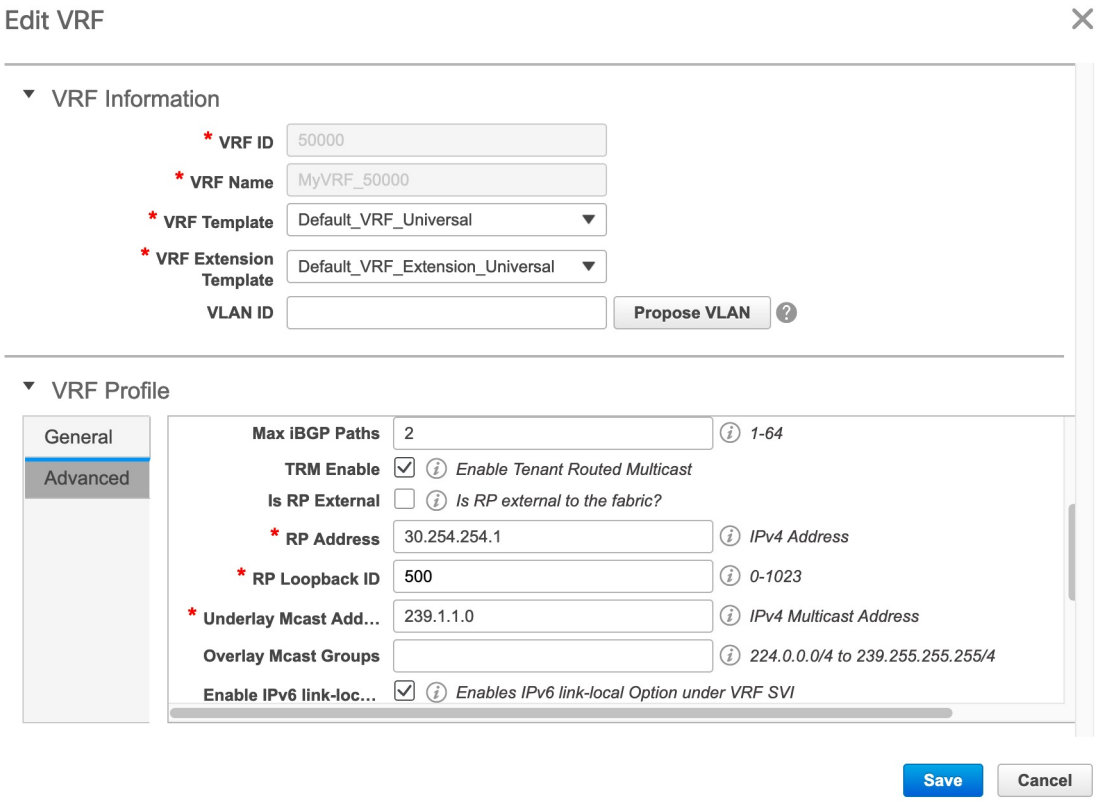
RP アドレス：RP の IP アドレスを指定します。

RP ループバック ID：**RP が外部** が有効化されていない場合、RP のループバック ID を指定します。

[アンダーレイ マルチキャスト アドレス（Underlay Multicast Address）]：VRF に関連付けられたマルチキャストアドレスを指定します。マルチキャストアドレスは、ファブリック アンダーレイでマルチキャスト トラフィックを転送するために使用します。

Note ファブリック設定画面の **[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]** フィールドのマルチキャスト アドレスは、このフィールドに自動的に入力されます。ユーザーはこの VRF に別のマルチキャスト グループ アドレスを使用する必要がある場合は、このフィールドを上書きできます。

[オーバーレイ マルチキャスト グループ（Overlay Multicast Groups）]：指定した RP のマルチキャスト グループ サブネットを指定します。値は「ip pim rp-address」コマンドのグループ範囲です。フィールドが空の場合、デフォルトで 224.0.0.0/24 が使用されます。



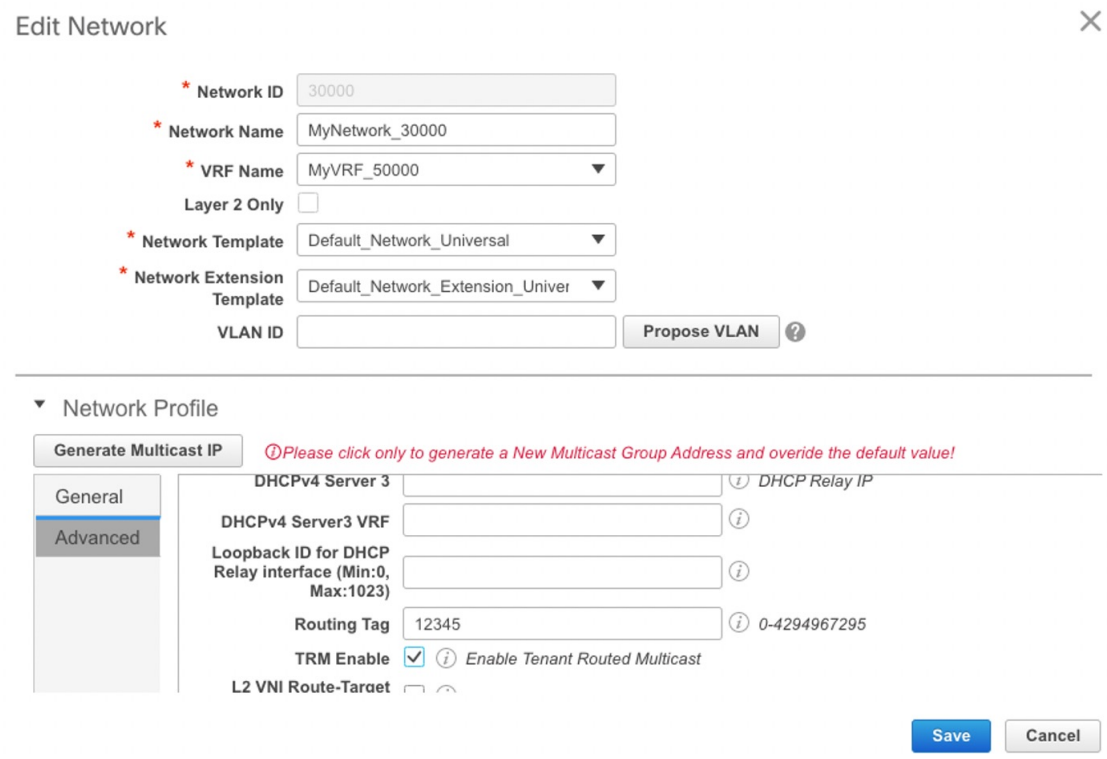
[Save] をクリックして設定を保存します。スイッチは保留状態に入り、青色になります。これらの設定で次のことが有効化されます。

- L3VNI SVI で PIM を有効にします。
- MVPN AFI のルートターゲットのインポートおよびエクスポート。
- VRF 向け RP およびその他のマルチキャスト構成。
- 分散 RP の上記の RP アドレスと RP ループバック ID を使用するループバック インターフェイス。

ステップ 3 ネットワークの TRM を有効にします。

[制御（Control）]>[ネットワーク（Networks）] に移動します。選択したネットワークを編集し、[詳細（Advanced）] タブに移動します。次の TRM 設定を編集します。

[TRM が有効（TRM enable）]：TRM を有効にするには、このチェックボックスをオンにします。



[Save] をクリックして設定を保存します。スイッチは保留状態、つまり青色になります。TRM 設定により、次のことが可能になります。

- L2VNI SVI で PIM を有効にします。
- PIM ポリシーを **なし（none）** で作成して、VLAN 内の PIM ルータとの PIM ネイバーシップを回避します。**なし（none）** キーワードは、すべての ipv4 アドレスを拒否するように設定されたルートマップで、エニーキャスト IP を使用した PIM ネイバーシップ ポリシーの確立を回避します。

Cisco DCNM を使用したマルチサイト向け TRM の構成

このセクションでは、マルチサイト ドメイン（MSD）がすでに Cisco DCNM によって展開されており、TRM を有効にする必要があることを前提としています。

Procedure

ステップ 1 BGW で TRM を有効にします。

[制御（Control）] > [VRF] に移動します。[スコープ（Scope）] で正しい DC ファブリックが選択されていることを確認し、VRF を編集します。[Advanced] タブまで移動します。TRM 設定の編集すべての DC ファブリックとその VRF に対してこのプロセスを繰り返します。

TRM の有効化：TRM を有効にするためにチェックボックスを選択します。TRM を有効化する場合、RP アドレスおよびアンダーレイ マルチキャスト アドレスを入力する必要があります。

RP が外部：ファブリックに対して RP が外部である場合、このチェックボックスを有効にします。このフィールドのチェックがオフの場合、RP はすべての VTEP に分散されます。

Note RP が外部の場合、適切なオプションを選択します。RP が外部の場合、RP ループバック ID がグレー化されます。

RP アドレス：RP の IP アドレスを指定します。

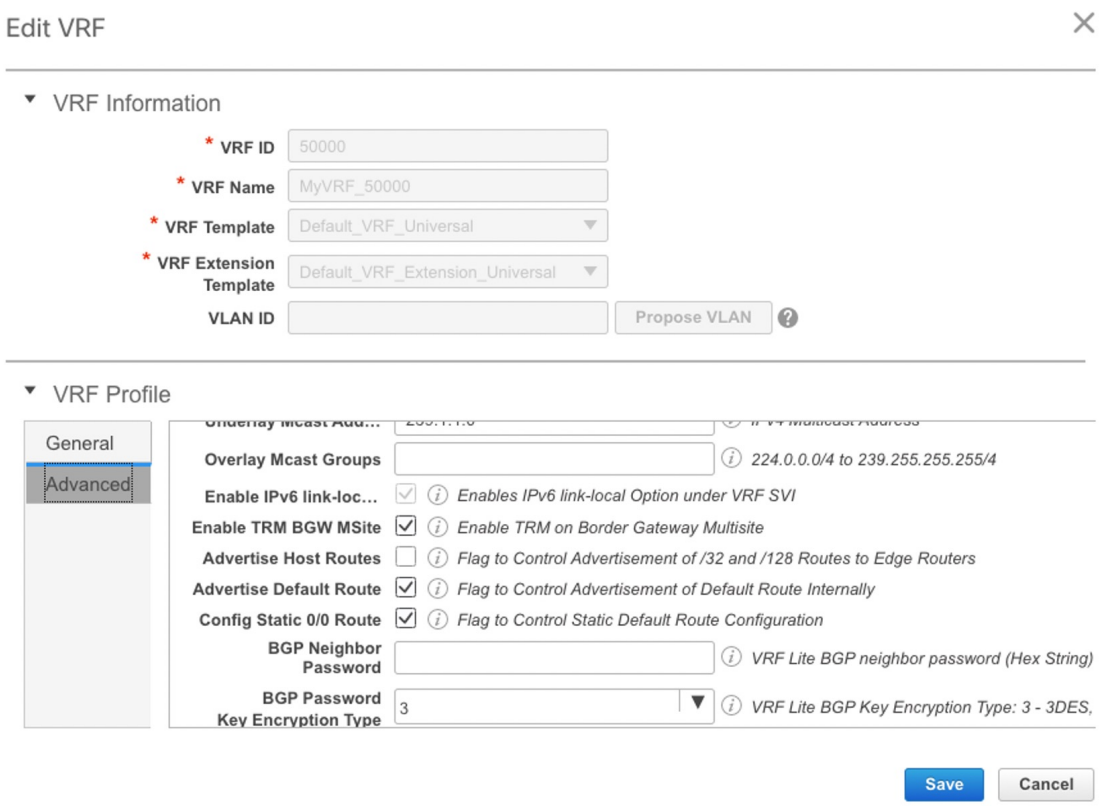
RP ループバック ID：**RP が外部** が有効化されていない場合、RP のループバック ID を指定します。

[アンダーレイ マルチキャスト アドレス（Underlay Multicast Address）]：VRF に関連付けられたマルチキャストアドレスを指定します。マルチキャストアドレスは、ファブリック アンダーレイでマルチキャスト トラフィックを転送するために使用します。

Note ファブリック設定画面の **[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]** フィールドのマルチキャスト アドレスは、このフィールドに自動的に入力されます。ユーザはこの VRF に別のマルチキャスト グループ アドレスを使用する必要がある場合は、このフィールドを上書きできます。

[オーバーレイ マルチキャスト グループ（Overlay Multicast Groups）]：指定した RP のマルチキャスト グループ サブネットを指定します。値は「ip pim rp-address」コマンドのグループ範囲です。フィールドが空の場合、デフォルトで 224.0.0.0/24 が使用されます。

[TRM BGW MSite の有効化（Enable TRM BGW MSite）]：境界ゲートウェイ マルチサイトで TRM を有効にするには、このチェックボックスをオンにします。

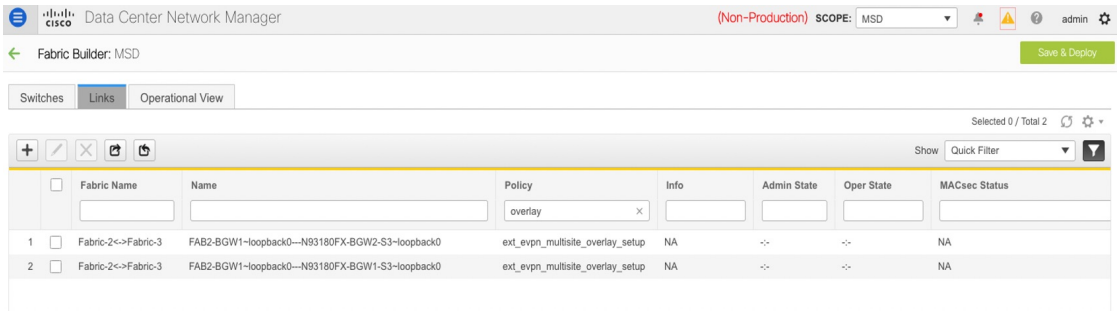


[保存（Save）] をクリックして、設定を保存します。スイッチは保留状態に入り、青色になります。これらの設定で次のことが有効化されます。

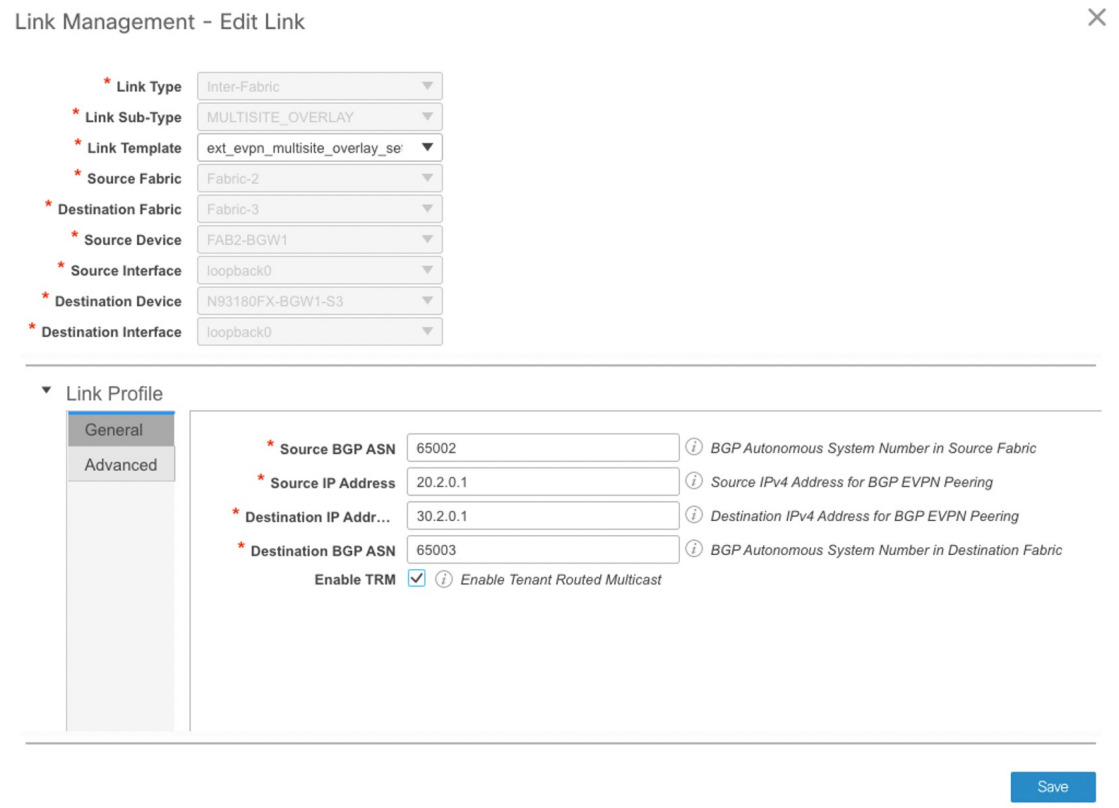
- 機能 ngmvpn の有効化：BGP ピアリング向け次世代マルチキャスト VPN（ngMVPN）コントロール パネルを有効にします。
- L3VNI SVIでPIMをイネーブルにします。
- L3VNI マルチキャスト アドレスを構成します。
- MVPN AFI のルートターゲットのインポートおよびエクスポート。
- VRF 向け RP およびその他のマルチキャスト構成。
- 分散 RP のループバック インターフェイス。
- レイヤ 2 VNI を拡張するためのマルチサイト BUM 入力レプリケーション方式を有効化します。

ステップ 2 BGW 間の MVPN AFI を確立します。

[制御（Control）] > [ファブリック（Fabrics）] に移動します。MSD ファブリックを選択します。**[表形式ビュー（Tabular view）]** をクリックし、**[リンク（Links）]** をクリックします。ポリシー：[オーバーレイ（Overlays）] でフィルタします。



[TRM の有効化（Enable TRM）] チェックボックスをオンにして、各オーバーレイ ピアリングを選択および編集し、TRM を有効にします。



[Save] をクリックして設定を保存します。スイッチは保留状態、つまり青色になります。TRM 設定により、BGW 間、または BGW とルート サーバ間の MVPN ピアリングが有効になります。

SSH キー RSA ハンドリング

ブートストラップのシナリオ

スイッチの実行構成にキー長変数値が 1024 以外の **ssh key rsa** コマンドがある場合、ブートストラップ中に **ssh key rsa** *key-length* **force** コマンドを必要な値（1024 以外の任意の値）を使用してブートストラップ自由形式構成に追加する必要があります。

グリーンフィールドとブラウンフィールドのシナリオ

ssh key rsa *key-length* **force** コマンドを使用して、キー長変数を 1024 以外の値に変更します。

ただし、Cisco Nexus 9000 リリース 9.3(1) および 9.3(2) では、ASCII 再生プロセス中にデバイスが起動しているときに、**ssh key rsa** *key-length* **force** コマンドが失敗します。詳細については、CSCvs40704 を参照してください。

インテントとスイッチの両方の実行構成に同じコマンドがある場合、構成は同期していると見なされます。たとえば、**ssh key rsa 2048** コマンドがインテントと実行構成の両方に存在する場合、ステータスは同期中と見なされます。ただし、アウトオブバンドの変更として **ssh key rsa 2040** コマンドがスイッチにプッシュされたシナリオを検討してください。インテントのキー長値は 2048 ですが、デバイスのキー長値は 2040 です。このような場合、スイッチは非同期としてマークされます。

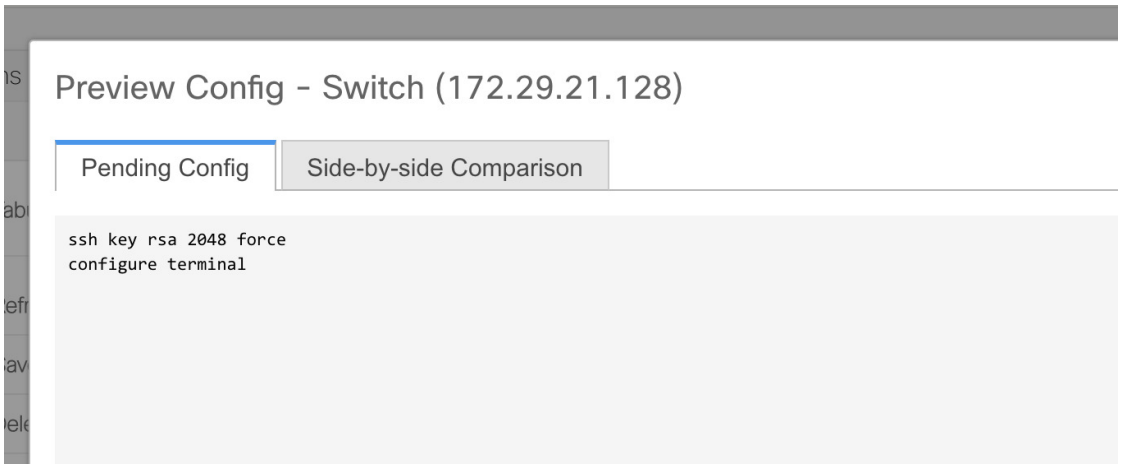
[保留中構成（Pending Config）] タブに表示される差分（厳格構成コンプライアンス モードと非厳格構成コンプライアンス モードの両方）は、**ssh key rsa** コマンドに変更を加える前に **feature ssh** コマンドを使用して SSH 機能を無効にする必要があるため、DCNM からスイッチに展開できません。これにより、DCNM への接続が切断されます。このようなシナリオでは、差分がないようにインテントを変更することで差分を解決できます。

厳格構成コンプライアンス モードの場合：

- **[ファブリック ビルダ（Fabric Builder）]** ウィンドウの **[表形式ビュー（Tabular View）]** で **[ポリシーの表示/編集（View/Edit Policies）]** をクリックして、**ssh key rsa 2048 force** コマンドを持つポリシー テンプレート インスタンス（PTI）を削除します。

- **[ポリシーの表示/編集（View/Edit Policies）]** をクリックして、**ssh key rsa 2040 force** コマンドで新しい PTI を作成します。

厳格構成コンプライアンス モードなしの場合：



- **[ファブリック ビルダ（Fabric Builder）]** ウィンドウの **[表形式ビュー（Tabular View）]** で **[ポリシーの表示/編集（View/Edit Policies）]** をクリックして、**ssh key rsa 2048 force** コマンドを持つ PTI を削除します。

- デバイスからのアウトオブバンドの変更に一致する目的で、**ssh key rsa 2040 force** コマンドを使用して switch_freeform PTI を作成します。

スイッチ操作

さまざまなオプションを表示するには、スイッチを右クリックします。

[ロールの設定（Set Role）]：スイッチにロールを割り当てます。次のロールのいずれかをスイッチに割り当てることができます。

- スパイン
- リーフ（デフォルト ロール）
- 境界
- ボーダースパイン
- ボーダーゲートウェイ
- アクセス
- 集約

- エッジ ルータ
- コア ルータ
- スーパースパイン
- ボーダースーパースパイン
- ボーダー ゲートウェイ スパイン
- ToR

または、**[アクション（Actions）]**ペインから**表形式ビュー**に移動することもできます。同じデバイス タイプの 1 つ以上のデバイスを選択し、**[ロールの設定（Set Role）]** をクリックしてデバイスのロールを設定します。デバイス タイプは次のとおりです。

- NX-OS
- IOS XE
- IOS XR
- その他

Note ロールを設定する前に、スイッチをメンテナンス モードからアクティブ モードまたは動作モードに移動したことを確認します。

[保存と展開（Save & Deploy）] を実行する前にのみ、スイッチのロールを変更できます。

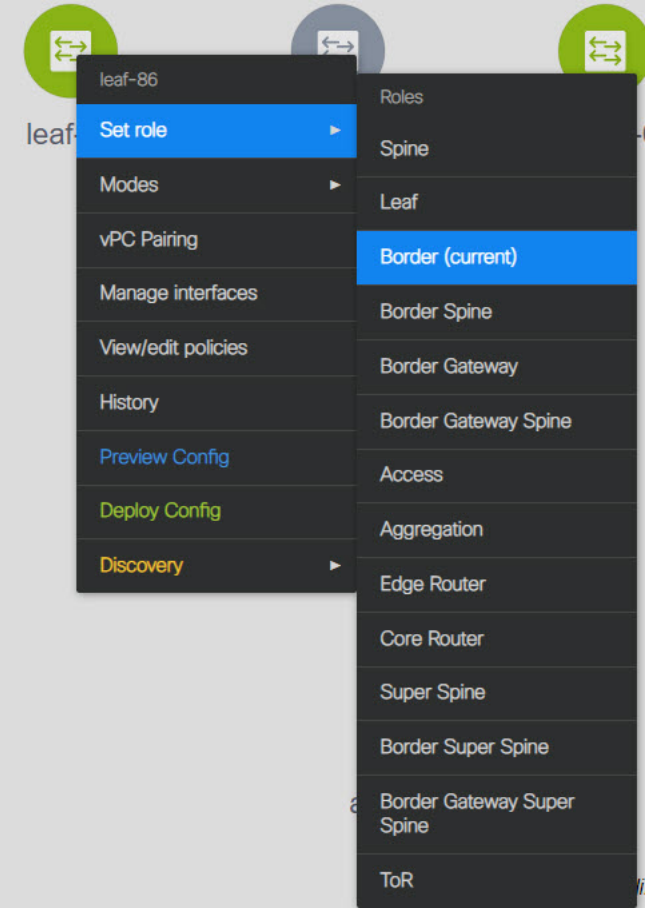
非 Nexus デバイスには、次のいずれかのロールを割り当てることができます。

- スパイン
- リーフ
- アクセス（このロールは、Cisco ASR 1000 シリーズ ルータおよび Cisco Catalyst 9000 シリーズ スイッチでのみ使用できます)。
- エッジ ルータ（VRF-Lite にはこのロールを使用します）。
- コア ルータ
- スーパースパイン
- 設定のプレビュー
- ToR（このロールは、Cisco Catalyst 9000 シリーズ スイッチでのみ使用できます）。

DCNM 11.1(1) リリースから、スイッチにオーバーレイがない場合、スイッチのロールを既存のロールから必要なロールにシフトできます。**[保存して展開（Save and Deploy）]** をクリックして、更新後の構成を生成します。スイッチ ロールには、次のシフトが許可されています。

- リーフからボーダー

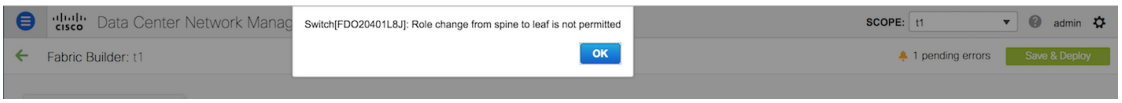
- ボーダーからリーフ
- リーフからボーダーゲートウェイ
- ボーダーゲートウェイからリーフ
- ボーダーからボーダーゲートウェイ
- ボーダーゲートウェイからボーダー
- スパインからボーダー スパイン
- ボーダー スパインからスパイン
- スパインからボーダーゲートウェイ スパイン
- ボーダーゲートウェイ スパインからスパイン
- ボーダー スパインからボーダーゲートウェイ スパイン
- ボーダーゲートウェイ スパインからボーダー スパイン



スイッチ ロールをリーフ ロールからスパイン ロールに、スパイン ロールからリーフ ロールに変更することはできません。

上記の Easy ファブリックで許可されているスイッチ ロールの変更に従ってスイッチ ロールが変更されていない場合、**[保存して展開（Save and Deploy）]** をクリックした後に次のエラーが表示されます。

```
Switch[<serial-number>]: Role change from <switch-role> to <switch-role> is not permitted.
```



その後、スイッチ ロールを以前に設定されたロールに変更するか、新しいロールを設定して、ファブリックを構成できます。

[保存して展開（Save and Deploy）] をクリックする前にポリシー テンプレート インスタンスを作成しておらず、オーバーレイがない場合は、スイッチのロールを他の必要なロールに変更できます。

vPC ペアの一部である vPC スイッチのスイッチ ロールを変更すると、**[保存して展開（Save and Deploy）]** をクリックすると次のエラーが表示されます。

```
Switches role should be the same for VPC pairing. peer1 <serial-number>: [<switch-role>],
 peer2 <serial-number>: [<switch-role>]
```

このシナリオを回避するには、vPC ペアの両方のスイッチのスイッチ ロールを同じロールに変更します。

DCNM での EXEC モード コマンドの実行

初めてログインしたときに、Cisco NX-OS ソフトウェアでは EXEC モードが開始されます。EXEC モードで使用可能なコマンドには、デバイスの状態および構成情報を表示する show コマンド、clear コマンド、ユーザがデバイス コンフィギュレーションに保存しない処理を実行するその他のコマンドがあります。

次の手順は、DCNM でEXECコマンドを実行する方法を示しています。

手順

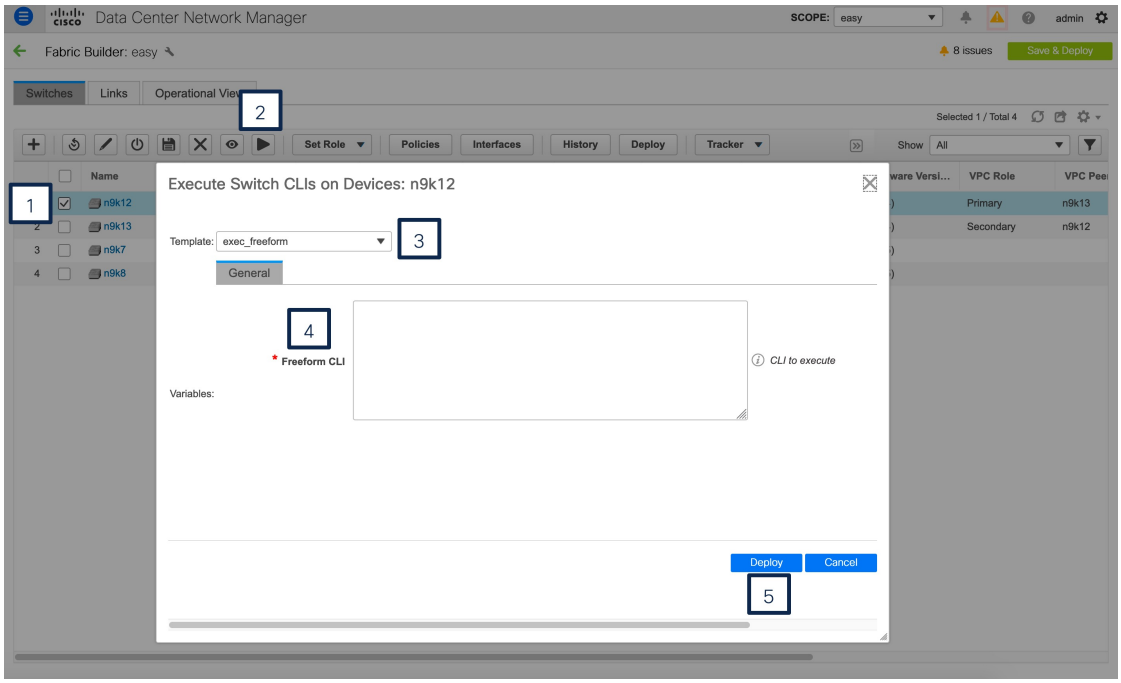
ステップ 1 DCNM から、**[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** の順に移動します。

ステップ 2 ファブリックをクリックし、**[アクション（Actions）]** メニューで **[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 1 つまたは複数のスイッチを選択し、**[再生（Play）]** ボタン（コマンド実行）をクリックします。

ステップ 4 **[テンプレート（Template）]** ドロップダウンリストから、**[exec_freeform]** を選択します。

ステップ 5 コマンドを **[自由形式 CLI（Freeform CLI）]** フィールドに入力します。



ステップ 6 **[展開（Deploy）]** をクリックして、EXEC コマンドを実行します。

ステップ 7 **[CLI 実行ステータス（CLI Execution Status）]** ウィンドウで、展開のステータスを確認できます。**[コマンド（Command）]** 列の **[詳細なステータス（Detailed Status）]**をクリックして詳細を表示します。

ステップ 8 **[コマンド実行の詳細（Command Execution Details）]** ウィンドウで、**[CLI 応答（CLI Response）]** 列の情報をクリックして、出力または応答を表示します。

ファブリック マルチ スイッチ操作

ファブリック トポロジ ウィンドウの **[アクション（Actions）]** ペインから **[表形式ビュー（Tabular View）]** をクリックします。表形式ビューには、次のタブがあります。

- 表形式ビュー：スイッチ
- 表形式ビュー：リンク
- 表形式ビュー：操作ビュー

表形式ビュー：スイッチ

このタブでスイッチ操作を管理できます。各行はファブリック内のスイッチを表し、シリアル番号を含むスイッチの詳細が表示されます。

このタブから実行できるアクションの一部は、ファブリック トポロジ ウィンドウでスイッチを右クリックしたときにも使用できます。ただし、**[スイッチ（Switches）]** タブでは、ポリシーの展開など、複数のスイッチの設定を同時にプロビジョニングできます。

[スイッチ（Switches）] タブには、ファブリックで検出されたすべてのスイッチに関する次の情報が表示されます。

- 名前：スイッチ名を指定します。
- IP アドレス：スイッチの IP アドレスを指定します。
- ロール：スイッチのロールを指定します。
- シリアル番号：スイッチのシリアル番号を入力します。
- ファブリック名：スイッチが検出されたファブリックの名前を指定します。
- ファブリック ステータス：スイッチが検出されたファブリックのステータスを指定します。
- 検出ステータス：スイッチの検出ステータスを指定します。
- モデル：スイッチ モデルを指定します。
- ソフトウェア バージョン：スイッチのソフトウェア バージョンを指定します。
- ThousandEyes ステータス：ThousandEyes Enterprise Agent のステータスを指定します。
- 最終更新日：スイッチが最後に更新された日時を示します。
- モード：スイッチの現在のモードを指定します。
- VPC ロール：スイッチの vPC ロールを指定します。
- VPC ピア：スイッチの vPC ピアを指定します。

[スイッチ（Switches）] タブには、次のアイコンとボタンがあります。

- スイッチの追加：このアイコンをクリックして、ファブリックに既存または新規のスイッチを検出します。**[インベントリ管理（Inventory Management）]** ダイアログボックスが表示されます。

  このオプションは、ファブリック トポロジ ウィンドウでも使用できます。[アクション（Actions）] ペインで [スイッチの追加（Add switches）] をクリックします。

  詳細については、次の項を参照してください。

  - ファブリックへのスイッチの追加：簡易ファブリックへのスイッチの追加について説明します。
  - 新しいスイッチの検出：外部ファブリックへの Cisco Nexus スイッチの追加に関する情報を提供します。
  - 非 Nexus デバイスを外部ファブリックに追加：外部ファブリックへの非 Nexus スイッチの追加に関する情報を提供します。

- スイッチの再検出：スイッチ検出プロセスを DCNM afresh により開始します。
- ディスカバリ クレデンシャルの更新：認証プロトコル、ユーザ名、パスワードなどのデバイス クレデンシャルを更新します。
- 構成の保存とリロード：構成を保存して、スイッチをリロードします。

Note このオプションは、ファブリックがフリーズモードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。

- コピー実行からスタートアップ構成：Cisco DCNM、リリース 11.4(1) 以降、1 つ以上のスイッチに対して、オンデマンドのコピー実行コンフィギュレーションからスタートアップ構成への動作を実行できます。

Note このオプションは、ファブリックがフリーズモードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。

- スイッチの削除：ファブリックからスイッチを削除します。

Note このオプションは、ファブリックがフリーズモードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。

- プレビュー：保留中の設定と、実行中の設定と予想される設定の並べた比較をプレビューできます。
- ポリシーの：ポリシーを追加、更新、および削除します。ポリシーはテンプレート ライブラリでテンプレートのテンプレート インスタンスです。ポリシーを作成したら、 ウィンドウで使用できる **[展開（Deploy）]** オプションを使用してスイッチに展開します。複数のポリシーを選択して表示できます。

Note 複数のスイッチを選択してポリシー インスタンスを展開する場合、選択したすべてのスイッチに展開されます。

- **[ThousandEyes Agent]**：スイッチで ThousandEyes Enterprise Agent を起動、停止、インストール、またはアンインストールできます。単一または複数のスイッチを選択し、**[ThousandEyes エージェント（ThousandEyes Agent）]** ドロップダウンリストから必要な操作を選択します。

Note ThousandEyes Enterprise Agent アクションを実行するために複数のスイッチを選択する場合は、選択したスイッチのステータスが同じであることを確認してください。

- インターフェイスの：スイッチ インターフェイスに構成を展開します。
- 履歴：このボタンを使用して、展開履歴とポリシー変更履歴を表示します。1 つ以上のスイッチを選択し、**[履歴（History）]** をクリックします。

  [ポリシー変更履歴（Policy Change History）]タブには、追加、更新、削除などの変更を行ったユーザとともにポリシーの履歴が一覧表示されます。

  ポリシーの **[ポリシー変更履歴（Policy Change History）]** タブで、**[生成された構成（Generated Config）]** 列の **[詳細な履歴（Detailed History）]** をクリックして、前後の生成された構成を表示します。

  次の表に、ポリシーテンプレートインスタンス（PTI）の前後に生成される構成の概要を示します。

PTI の操作	前に生成された構成	生成後の構成
追加	Empty	構成が含まれています
更新	変更前の構成が含まれています	変更後の構成が含まれています
マーク - 削除	削除する構成が含まれます	色を変更して削除する構成が含まれます
削除	構成が含まれています	Empty

Note ポリシーまたはプロファイルテンプレートが適用されると、テンプレートのアプリケーションごとにインスタンスが作成されます。このインスタンスは、ポリシー テンプレート インスタンスまたは PTI と呼ばれます。

- 展開：スイッチ構成を展開します。Cisco DCNM リリース 11.3(1) 以降では、**[展開（Deploy）]** ボタンを使用して複数のデバイスの構成を展開できます。

Note

- このオプションは、ファブリックがフリーズ モードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。
- MSD ファブリックでは、Border Gateway、Border Gateway Spine、Border Gateway Super-Spine、または外部ファブリック スイッチにのみ構成を展開できます。

- ロールの設定：同じデバイスタイプの 1 つ以上のデバイスを選択し、**[ロールの設定（Set Role）]** をクリックしてデバイスのロールを設定します。デバイス タイプは次のとおりです。
  - NX-OS
  - IOS XE
  - IOS XR
  - その他

  ロールを設定する前に、スイッチをメンテナンス モードからアクティブ モードまたは動作モードに移動したことを確認します。ロールの設定の詳細については、スイッチ操作の項を参照してください。
- vPC ペアリング：スイッチを選択し、**[vPC ペアリング（vPC Pairing）]** をクリックして vPC ペアを作成、編集、またはペアリング解除します。ただし、このオプションは、Cisco Nexus スイッチを選択した場合にのみ使用できます。詳細については、次の項を参照してください。
  - vPC セットアップの作成：外部ファブリックで vPC ペアを作成する方法について説明します。
  - vPC ファブリック ピアリング：簡単なファブリックで vPC ペアを作成する方法について説明します。

表形式ビュー：リンク

異なるファブリックの境界スイッチ間（ファブリック間）、または同じファブリック内のスイッチ間（ファブリック内）にリンクを追加できます。DCNM による管理対象のスイッチに対してのみ、ファブリック間接続（IFC）を作成できます。

物理的に接続する前にスイッチ間のリンクを定義する必要があるシナリオがあります。リンクは、ファブリック間リンクまたはファブリック内リンクです。そうすることで、リンクを追加する意図を表現して表すことができます。インテントのあるリンクは、実際に機能するリンクに変換されるまで、異なる色で表示されます。リンクを物理的に接続すると、接続済みとして表示されます。

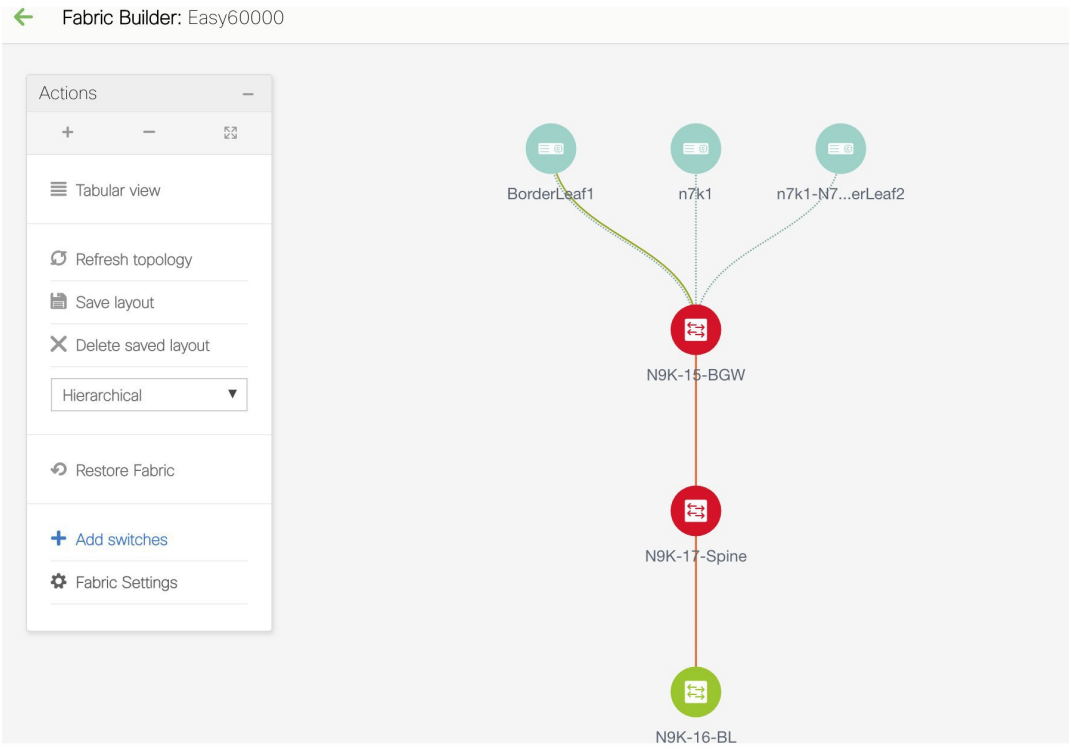
管理リンクは、ファブリックトポロジでは赤色のリンクとして表示される場合があります。このようなリンクを削除するには、リンクを右クリックし、**[リンクの削除（Delete Link）]** をクリックします。

Cisco DCNM リリース 11.1(1) 以降で、ボーダー スイッチのスイッチ ロールに、ボーダー スパイン ロールとボーダーゲートウェイ スパイン ロールが追加されます。

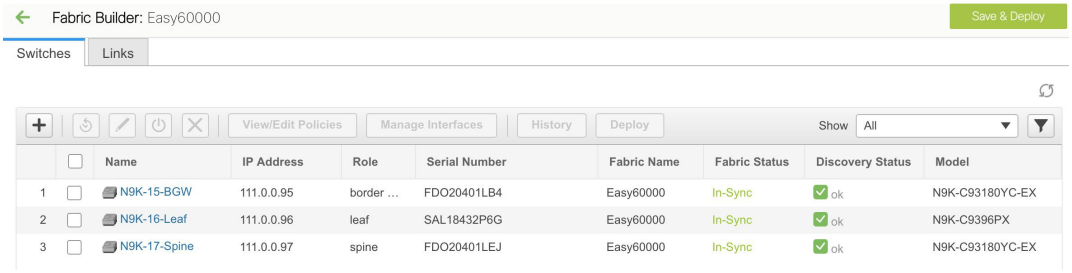
事前プロビジョニングされたデバイスを宛先デバイスとして選択することで、既存のデバイスと事前プロビジョニングされたデバイス間のリンクを作成できます。

ファブリック間リンクの作成

1. [制御（Control）] > [ファブリック ビルダ（Fabric Builder）] をクリックして、ファブリック ビルダ画面に移動します。
2. ファブリックを表す長方形のボックス内をクリックします。[ファブリック トポロジ(fabric topology)] 画面が表示されます。
3. ウィンドウの左側に表示される [アクション（Actions）] パネルの [表形式ビュー（Tabular view）] をクリックします。

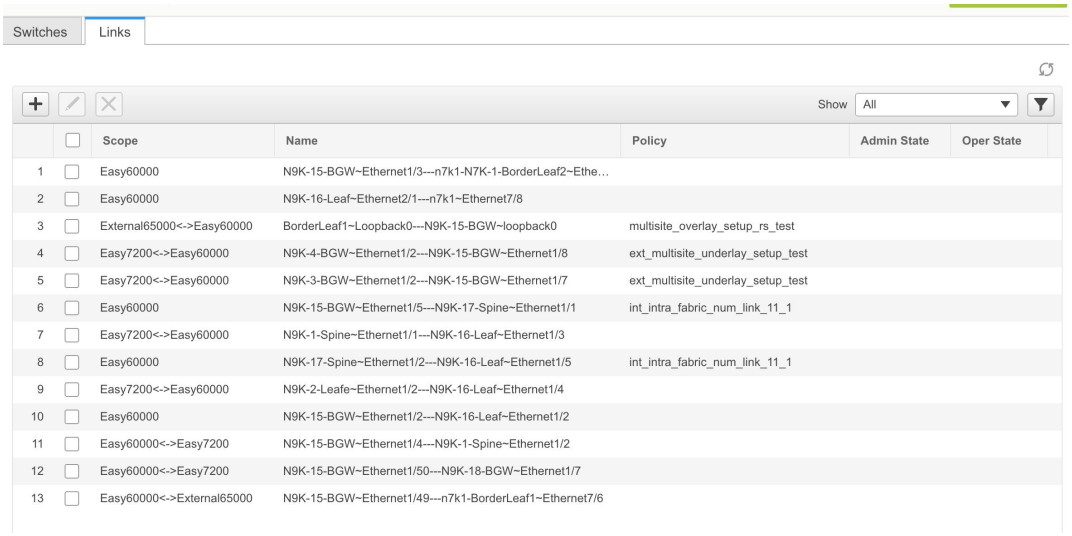


[スイッチ（Switches）] タブと [リンク（Links）] タブのあるウィンドウが表示されます。ファブリック スイッチとリンクをテーブルにリストします。



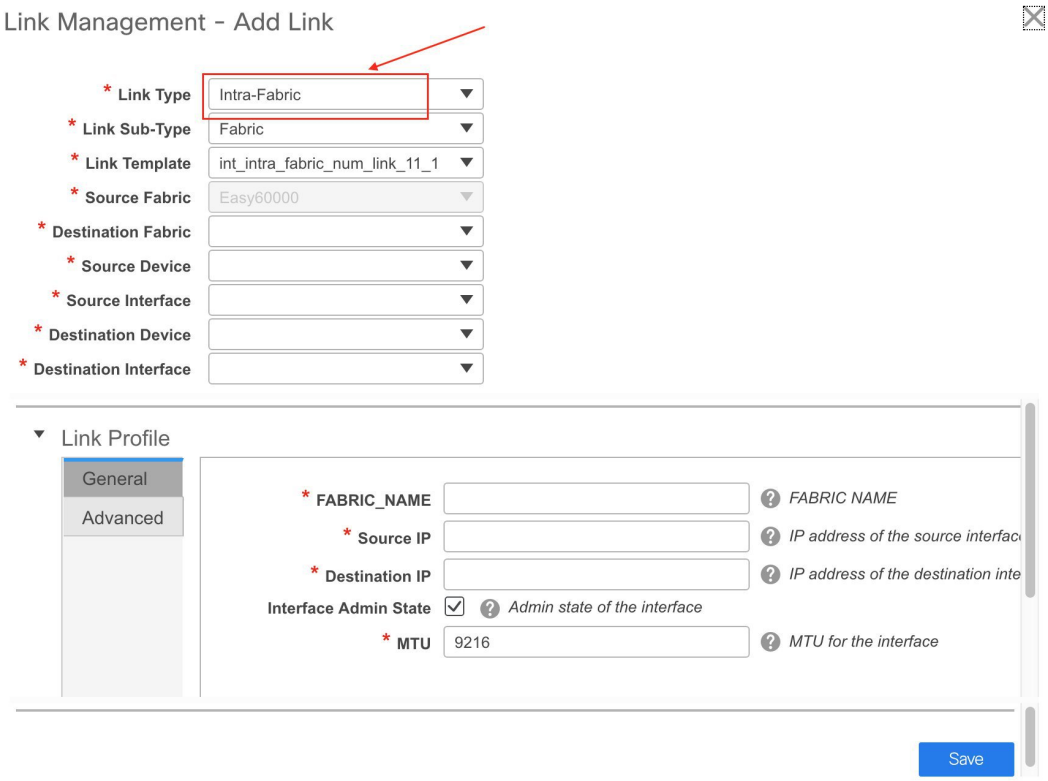
4. [リンク（Links）] タブをクリックします。リンクのリストを確認できます。

   まだリンクを作成していない場合、リストは空です。



5. 画面の左上にある [追加（+）（Add (+)）] ボタンをクリックしてリンクを追加します。

   [リンクの追加（Add Link）] 画面が表示されます。デフォルトでは、リンク タイプとして [ファブリック内（Intra-Fabric）] オプションが選択されています。



該当するフィールドは次のとおりです。

リンク タイプ：ファブリック内の2つのスイッチ間にリンクを作成するには、[ファブリック内（Intra-Fabric）] を選択します。

リンク サブタイプ：このフィールドは、これがファブリック内のリンクであることを示す「ファブリック」に入力されます。

リンク テンプレート：次のリンク テンプレートのいずれかを選択できます。

- int_intra_fabric_num_link_11_1：リンクが IP アドレスが割り当てられた 2 つのイーサネット インターフェイス間にある場合は、int_intra_fabric_num_link_11_1 を選択します。
- int_intra_fabric_unnum_link_11_1：リンクが 2 つの IP アンナンバード インターフェイス間にある場合は、int_intra_fabric_unnum_link_11_1 を選択します。
- int_intra_vpc_peer_keep_alive_link_11_1：リンクが vPC ピア キープアライブ リンクの場合は、int_intra_vpc_peer_keep_alive_link_11_1 を選択します。
- int_pre_provision_intra_fabric_link：リンクが2つの事前プロビジョニングされたデバイス間にある場合は、int_pre_provision_intra_fabric_link を選択します。**[保存と展開（Save & Deploy）]** をクリックすると、アンダーレイ サブネット IP プールから IP アドレスが選択されます。

これに対応して、[リンク プロファイル（Link Profile）] セクションのフィールドが更新されます。

送信元ファブリック：送信元ファブリックが既知であるため、このフィールドにファブリック名が入力されます。

宛先ファブリック：宛先ファブリックを選択します。ファブリック内リンクの場合、送信元と宛先のファブリックは同じです。

送信元デバイスと送信元インターフェイス：送信元デバイスと送信元インターフェイスを選択します。

宛先デバイスと宛先インターフェイス：宛先デバイスと宛先インターフェイスを選択します。

Note 既存のデバイスと事前プロビジョニングされたデバイスの間にリンクを作成する場合は、事前プロビジョニングされたデバイスを宛先デバイスとして選択します。

[リンク プロファイル（Link Profile）]セクションの **[全般（General）]** タブ

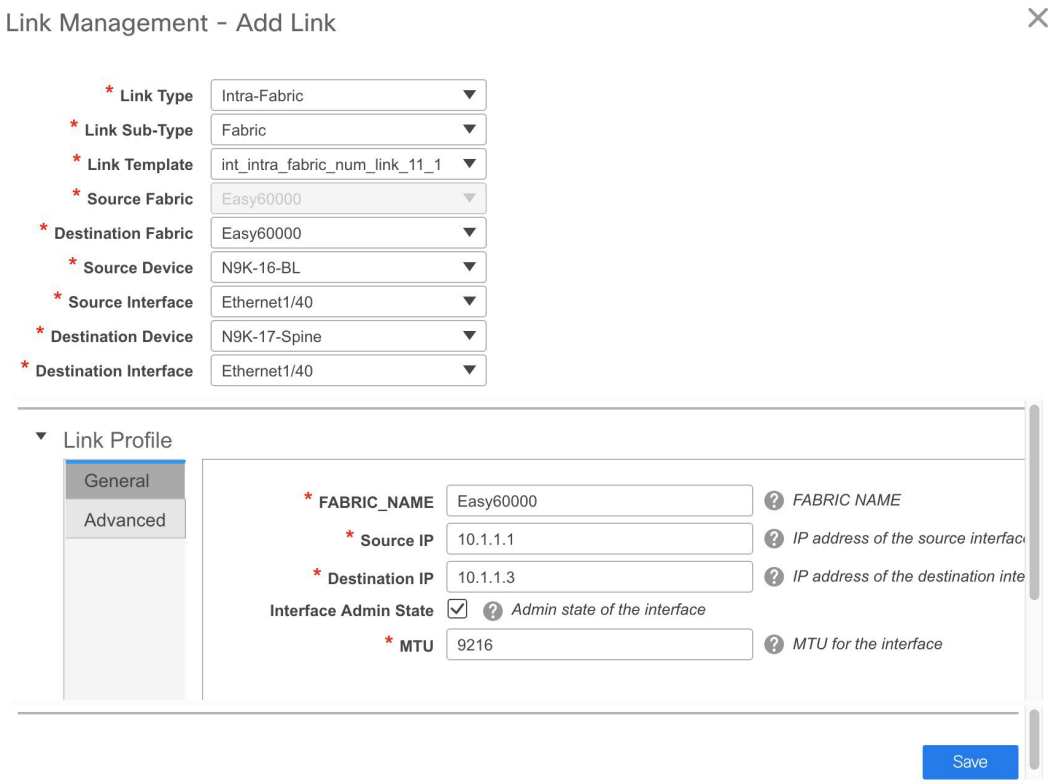
インターフェイス VRF：このインターフェイスのデフォルト以外の VRF の名前。

送信元 IP および宛先 IP：送信元と宛先インターフェイスの送信元 IP および宛先 IP アドレスをそれぞれ指定します。

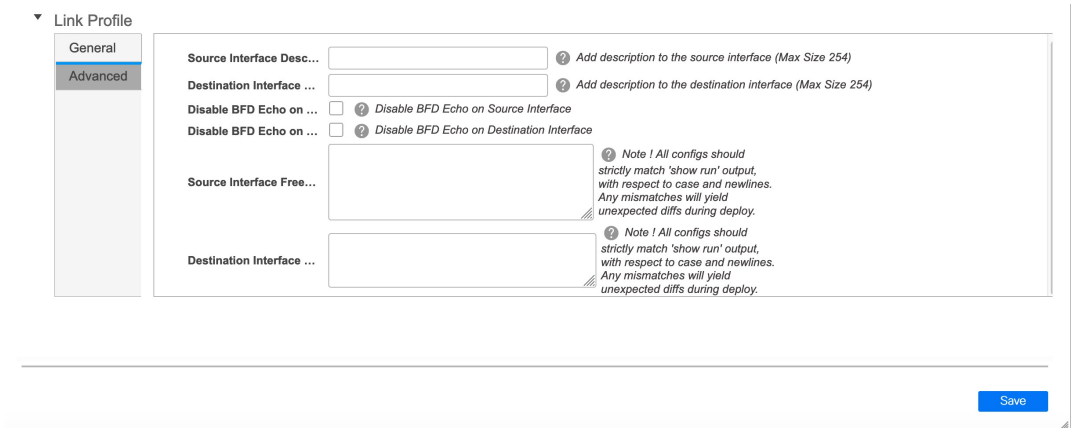
Note **[int_pre_provision_intra_fabric_link]** テンプレートを選択すると、[送信元 IP] フィールドと [接続先 IP] フィールドは表示されません。

インターフェイスの管理状態（Interface Admin State）：このチェックボックスをオンまたはオフにして、インターフェイスの管理状態を有効または無効にします。

MTU：2 つのインターフェイスの最大伝送単位（MTU）を指定します。



[詳細（Advanced）] タブ



[送信元インターフェイスの説明（Source Interface Description）] および [宛先インターフェイスの説明（Destination Interface Description）] : 後で使用するためのリンクについて説明します。たとえば、リンクがリーフ スイッチとルート リフレクタ デバイスの間にある場合は、これらのフィールドに情報を入力できます（リーフ スイッチからRR1へのリンク、およびRR1からリーフ スイッチへのリンク）。この説明は設定に変換されますが、スイッチにはプッシュされません。**[保存と展開（Save & Deploy）]** の後、実行構成に反映されます。

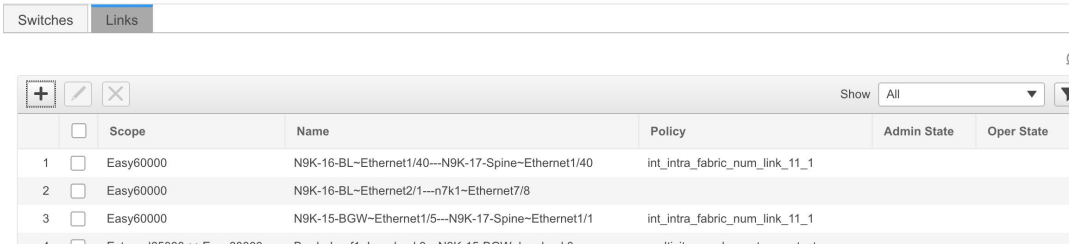
[送信元インターフェイスの BFD エコーの無効化（Disable BFD Echo on Source Interface）] および **[宛先インターフェイスの BFD エコーの無効化（Disable BFD Echo on Destination Interface）]**：送信元および宛先インターフェイスでBFDエコーパケットを無効にします。

BFD エコー フィールドは、ファブリック設定で BFD を有効にした場合にのみ適用されることに注意してください。

送信元インターフェイス フリーフォーム CLI および宛先インターフェイス フリーフォーム CLI（Source Interface Freeform CLIs and Destination Interface Freeform CLIs）：送信元と宛先インターフェイスに特別なフリーフォーム構成を入力してください。スイッチの実行構成に表示されている設定を、インデントなしで追加する必要があります。詳細な説明と例については、「ファブリック スイッチでの自由形式構成」セクションを参照してください。

6. 画面の下部にある [保存（Save）] をクリックします。

   リンク タブに新しいリンクが表示されます。



7. **[保存と展開（Save & Deploy）]** をクリックして、リンク構成をスイッチに展開します。

   [構成展開（Config Deployment）] 画面が表示されます。スイッチの構成ステータスが表示されます。[構成のプレビュー（Preview Config）]列のそれぞれのリンクをクリックして、保留中の構成を表示することもできます。[構成のプレビュー（Preview Config）]列のリンクをクリックすると、[構成プレビュー（Config Preview）] ウィンドウが表示されます。スイッチの保留中の設定が一覧表示されます。[並べて表示（Side-by-Side）] タブには、実行構成と予想される構成が並べて表示されます。

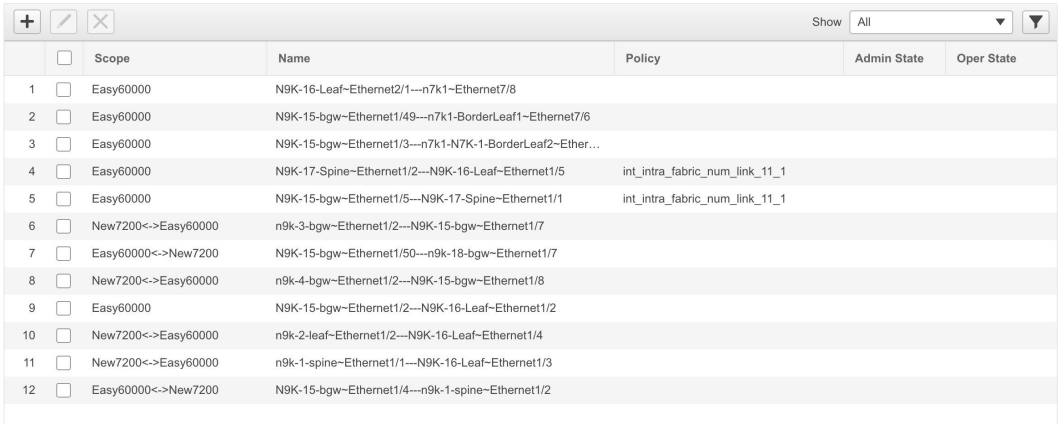
8. プレビュー画面を閉じて、[構成の展開（Deploy Config）] をクリックします。保留中の構成が展開されます。

9. すべての行で進行状況が 100% であることを確認したら、画面の下部にある [閉じる（Close）] をクリックします。[リンク（Links）] 画面が再び表示されます。

   画面の左上にある [<-] をクリックして、ファブリック トポロジに移動します。 ファブリック トポロジでは、2 つのデバイス間のリンクが表示されます。

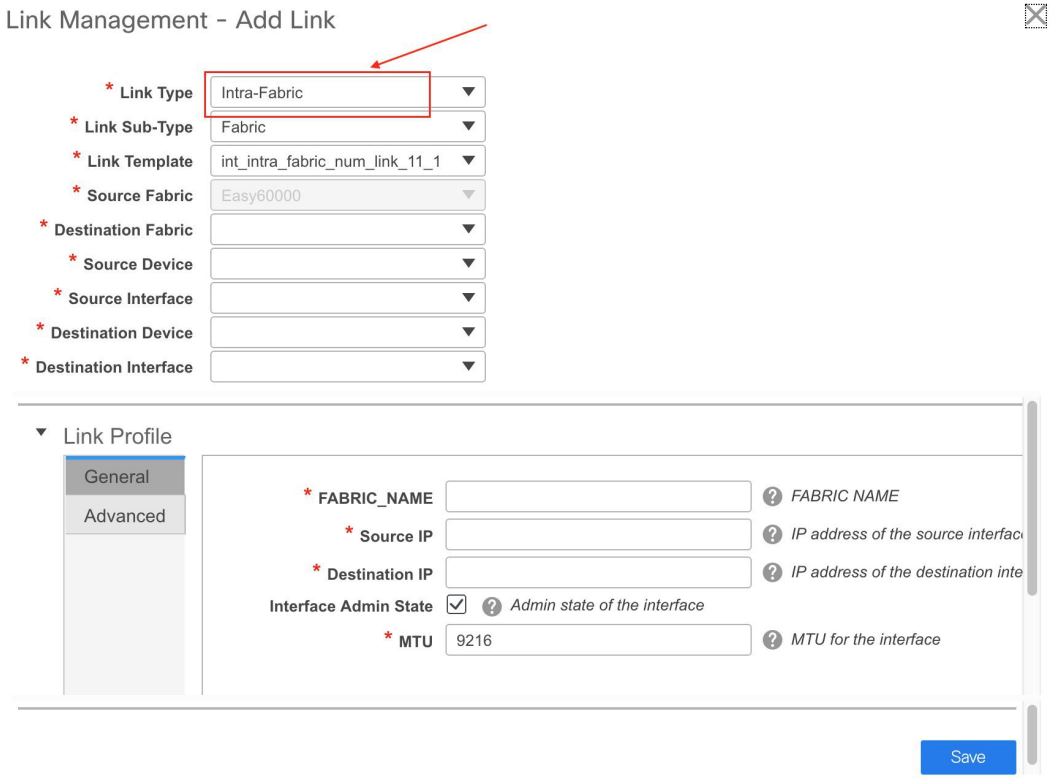
ファブリック内リンクの作成

1. [スイッチ | リンク（Switches | Links）] ページの [リンク（Links）] タブをクリックします。以前に作成されたリンクのリストが表示されます。リンクには、ファブリック内リンク（ファブリック内のスイッチ間）、およびファブリック間リンク（BGW 間、または異なるファブリックのボーダー リーフスイッチ/スパイン スイッチ間）が含まれます。

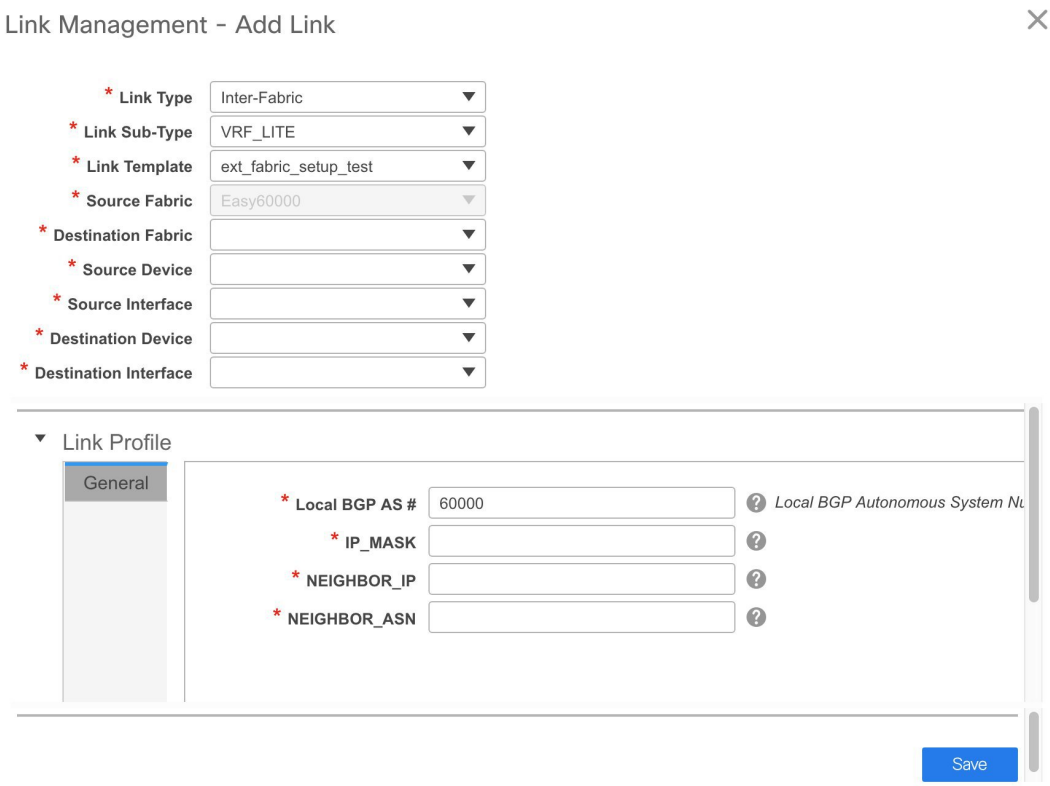


2. 画面の左上にある [追加（+）（Add (+)）] ボタンをクリックしてリンクを追加します。[リンクの追加（Add Link）] 画面が表示されます。

   デフォルトでは、リンク タイプとして [ファブリック内（Intra-Fabric）] オプションが選択されています。



3. IFC を作成しているため、[Link Type] ドロップダウン ボックスから [ファブリック間（Inter-Fabric）] を選択します。画面がそれに応じて変化します。



ファブリック間リンク作成のフィールドについて説明します。

リンク タイプ：ファブリック間（Inter-Fabric） を選択して、2 つのファブリック間の境界スイッチを介したファブリック間接続を作成します。

リンク サブタイプ：このフィールドは IFC タイプを入力します。ドロップダウン リストから **[VRF_LITE]**、**[MULTISITE_UNDERLAY]**、または **[MULTISITE_OVERLAY]** を選択します。

マルチサイト オプションについては、マルチサイトの使用例で説明します。

VXLAN MPLS 相互接続の詳細については、「*VXLAN BGP EVPN* ファブリック *-MPLS SR* および *LDP* ハンドオフの境界プロビジョニングの使用例」の章を参照してください。

ルーテッドファブリックの相互接続については、「*eBGP* アンダーレイを使用したファブリックの構成（*Configuring a Fabric with eBGP Underlay*）」の章の「ルーテッド ファブリックと外部ファブリック間のファブリック間リンクの作成（*Creating Inter-Fabric Links between a Routed Fabric and an External Fabric*）」の項を参照してください。

リンク テンプレート：リンク テンプレートが入力されます。

テンプレートには、選択内容に基づいて、対応するパッケージ済みのデフォルト テンプレートが自動的に入力されます。

Note ユーザ定義テンプレートを追加、編集、削除できます。詳細については、「制御」の章の「テンプレート ライブラリ」のセクションを参照してください。

[送信元ファブリック]：このフィールドには、送信元ファブリック名が事前に入力されています。

[宛先ファブリック]：このドロップダウンボックスから宛先ファブリックを選択します。

[送信元デバイスと宛先インターフェイス]：宛先デバイスに接続する送信元デバイスとイーサネット インターフェイスを選択します。

[宛先デバイスと宛先インターフェイス]：送信元デバイスに接続する宛先デバイスとイーサネット インターフェイスを選択します。

送信元デバイスと送信元インターフェイスの選択に基づいて、Cisco Discovery Protocol 情報（使用可能な場合）に基づいて宛先情報が自動入力されます。宛先外部デバイスが宛先ファブリックの一部であることを確認するために、追加の検証が実行されます。

[リンク プロファイル] セクションの **[全般]** タブ。

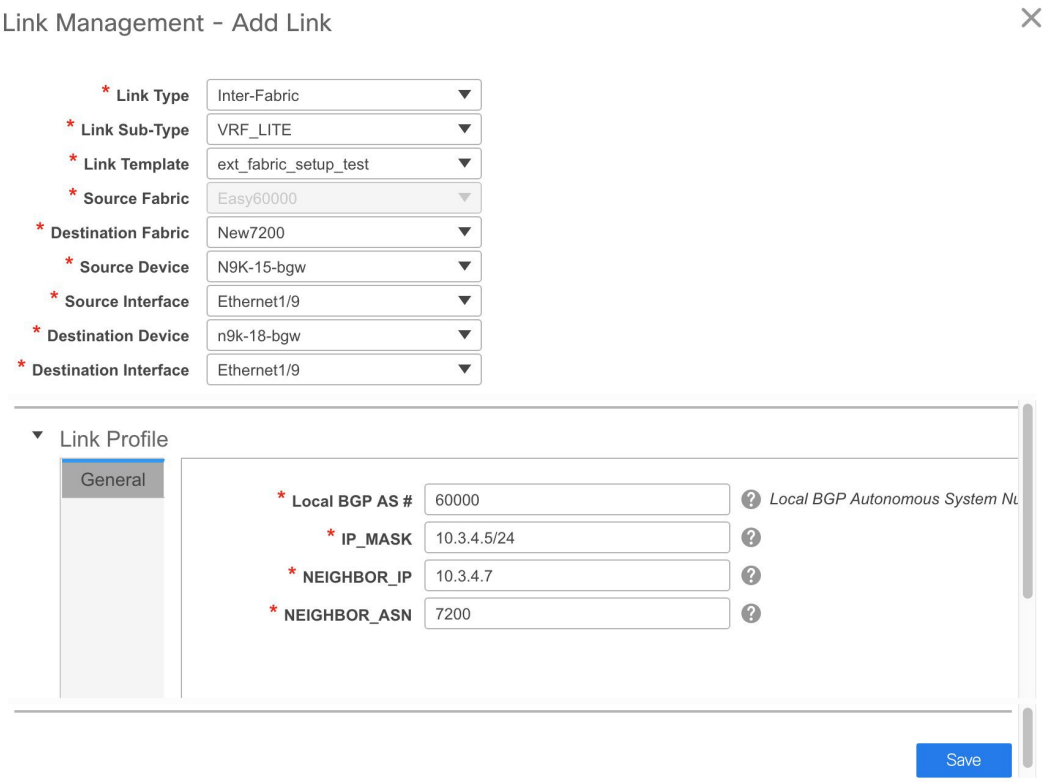
ローカル BGP AS # ：このフィールドには、送信元ファブリックの AS 番号が自動入力されます。

IP_MASK：宛先デバイスに接続する送信元インターフェイスの IP アドレスをこのフィールドに入力します。

NEIGHBOR_IP：宛先インターフェイスの IP アドレスをこのフィールドに入力します。

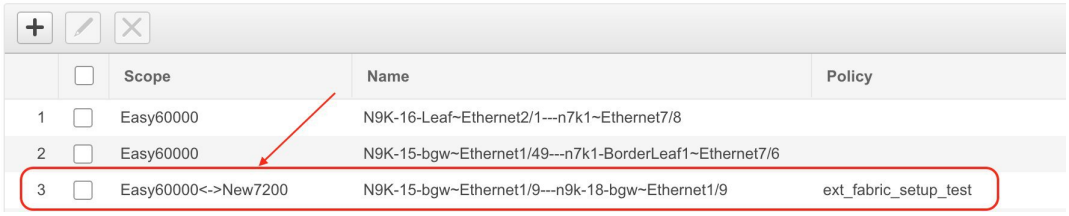
NEIGHBOR_ASN：このフィールドには、宛先デバイスの AS 番号が自動入力されます。

[リンクの追加（Add Link）] 画面に入力すると、次のようになります。



4. 画面の下部にある [保存（Save）] をクリックします。

   [スイッチ | リンク（Switches | Links）] 画面が再び表示されます。IFC が作成され、リンクのリストに表示されていることがわかります。



5. [保存と展開（Save & Deploy）] をクリックして、リンク構成をスイッチに展開します。

   [構成展開 (Config Deployment)] 画面が表示されます。スイッチの構成ステータスが表示されます。[構成のプレビュー（Preview Config）]列のそれぞれのリンクをクリックして、保留中の構成を表示することもできます。[構成のプレビュー（Preview Config）]列のリンクをクリックすると、[構成プレビュー（Config Preview）] ウィンドウが表示されます。スイッチの保留中の設定が一覧表示されます。[並べて表示（Side-by-Side）] タブには、実行構成と予想される構成が並べて表示されます。

6. プレビュー画面を閉じて、[構成の展開（Deploy Config）] をクリックします。保留中の構成が展開されます。

7. すべての行で進行状況が 100％ であることを確認したら、画面の下部にある [閉じる（Close）] をクリックします。[リンク（Links）] 画面が再び表示されます。
8. 画面の左上にある [<-] をクリックして、ファブリック トポロジに移動します。ファブリック トポロジでは、2 つのデバイス間のリンクが表示されます。

   2 つのファブリックが MSD のメンバー ファブリックである場合は、MSD トポロジにもリンクが表示されます。

ToExternalOnly メソッドまたは MSD ファブリック経由のマルチサイト機能を使用して VRF Lite 機能を有効にすると、（VXLAN ファブリック）ボーダー/BGW デバイスと接続された（外部ファブリック）エッジ ルータ/コア デバイス間で IFC が自動的に作成されます。ER/コア/ボーダー/BGW デバイスを削除すると、DCNM でそのスイッチとの間で対応する IFC（リンク PTI）が削除されます。その後、DCNM は次の保存および展開操作で、残りのデバイスから対応する IFC 構成（存在する場合）を削除します。また、IFC およびオーバーレイ拡張を備えたデバイスをそれらの IFC から削除する場合は、それらの IFC に対応するすべてのオーバーレイ拡張を展開して、スイッチを削除できるようにする必要があります。

VRF 拡張を展開解除するには、[制御（Control）] > [ネットワークと VRF（Networks & VRFs）] をクリックして、VXLAN ファブリックと拡張 VRF を選択し、VRF 展開画面で VRF を展開解除します。

IFC を削除するには、[制御（Control）] > [ファブリック ビルダ（Fabric Builder）] をクリックし、ファブリック トポロジ画面に移動し、[表形式ビュー（Tabular view）] をクリックして、[リンク（Links）] タブから IFC を削除します。

ファブリック スイッチ名が一意であることを確認します。同じ名前のスイッチに VRF 拡張を導入すると、設定が誤ってしまいます。

新しいファブリックが作成され、DCNM でファブリックスイッチが検出され、これらのスイッチでアンダーレイ ネットワークがプロビジョニングされ、DCNM とスイッチ間の構成が同期されます。その他のタスクは、次のとおりです。

- vPC、ループバック インターフェイス、サブインターフェイス設定などのインターフェイス構成をプロビジョニングします。インターフェイスを参照してください。
- オーバーレイ ネットワークと VRF を作成し、スイッチに展開します。「ネットワークおよび VRF の作成と展開」を参照してください。

リンクのエクスポート

1. **[制御（Control）]> > [ファブリック ビルダ（Fabric Builder）]** の順に選択し、1 つのファブリックを選択します。

   ファブリック トポロジ ウィンドウが表示されます。
2. **[アクション（Actions）]** パネルで **[表形式ビュー（Tabular view）]** をクリックします。

   [スイッチ（Switches）] タブと **[リンク（Links）]** タブのあるウィンドウが表示されます。
3. **[リンク（Links）]** タブをクリックします。

リンクのリストを確認できます。まだリンクを作成していない場合、リストは空です。

4. **[リンクのエクスポート（Export Links）]** アイコンをクリックしてリンクを CSV ファイルにエクスポートします。

   リンクの次の詳細がエクスポートされます。リンクテンプレート、送信元ファブリック、宛先ファブリック、送信元デバイス、宛先デバイス、送信元スイッチ名、宛先スイッチ名、送信元インターフェイス、宛先インターフェイス、および nvPairs。nvPairs フィールドは JSON オブジェクトで構成されます。

リンクのインポート

リンクの詳細を含む CSV ファイルをインポートして、ファブリックに新しいリンクを追加できます。CSV ファイルには、リンクテンプレート、送信元ファブリック、宛先ファブリック、送信元デバイス、宛先デバイス、送信元スイッチ名、宛先スイッチ名、送信元インターフェイス、宛先インターフェイス、および nvPairs の詳細が含まれている必要があります。

Note

- 既存のリンクは更新できません。
- **[リンクのインポート（Import Links）]** アイコンは、外部ファブリックでは無効です。

1. **[制御（Control）]**> > **[ファブリック ビルダ（Fabric Builder）]** の順に選択し、1 つのファブリックを選択します。

   ファブリック トポロジ ウィンドウが表示されます。

2. **[アクション（Actions）]** パネルで **[表形式ビュー（Tabular view）]** をクリックします。

   [スイッチ（Switches）] タブと **[リンク（Links）]** タブのあるウィンドウが表示されます。

3. **[リンク（Links）]** タブをクリックします。

   リンクのリストを確認できます。まだリンクを作成していない場合、リストは空です。

4. **[リンクのインポート（Import Links）]** アイコンをクリックします。

   ファイル サーバ ディレクトリが開きます。

5. ディレクトリを参照し、インポートする CSV ファイルを選択します。

6. [開く（Open）] をクリックします。

   確認の画面が表示されます。

7. **[はい（Yes）]** をクリックして、選択したファイルをインポートします。

ファブリック リンクの詳細の表示

ファブリック ビルダのトポロジ表示で、アンダーレイを展開するリンク間の IP サブネット、MTU、速度の不一致などのファブリック リンクに関する情報を表示できます。Cisco DCNM Web クライアントからリンクの詳細を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** の順に選択し、1 つのファブリックを選択します。

ファブリックのトポロジ表示が表示されます。

ステップ 2 いずれかのリンクをダブルクリックします。

詳細ウィンドウが表示されます。このリンクを使用して接続されているデバイス、サマリ、およびデータトラフィックを表示できます。

ステップ 3 **[さらに詳細を表示（Show more details）]** をクリックします。

リンクで接続されている 2 つのデバイスの比較表が表示されます。これには、デバイスの次のパラメータが含まれます。デバイス名、名前、管理ステータス、動作ステータス、理由、ポリシー、オーバーレイ ネットワーク、ステータス、PC、vPC ID、速度、MTU、モード、VLAN、IP またはプレフィックス、VRF、ネイバー、および説明。

Note
- ハイパーリンクのあるデバイス名をクリックすると、ファブリック リンクのトラフィックの詳細を表示できます。または、詳細ウィンドウでこれらのトラフィックの詳細を表示できます。詳細については、「ファブリック リンクのトラフィックの詳細の表示」セクションを参照してください。
- ハイパーリンクのあるポリシーをクリックすると、ファブリック リンクの予想される構成を表示できます。

ステップ 4 **[戻る（Back）]** アイコンをクリックして、詳細ウィンドウに戻ります。

Note **[閉じる（Close）]** アイコンをクリックして、詳細ウィンドウを終了できます。

ファブリック リンクのトラフィック詳細の表示

ファブリック リンクの詳細ウィンドウで、トラフィックの詳細を表示する方法を選択できます。期間、形式に基づいてトラフィックの詳細を表示し、この情報をエクスポートできます。

[期間（Duration）] ドロップダウンリストでは、次のリンクのデータ トラフィックを表示することができます。

- 24 時間
- 週

- 月
- 年

表示：**[表示（Show）]** をクリックし、ドロップダウン リストから **[チャート（Chart）]**、**[表（Table）]**、または **[チャートと表（Chart and Table）]** を選択して、トラフィックの詳細を表示する方法を表示します。ブラウザ ウィンドウを拡大して、**[チャートと表形式（Chart and Table）]** フォーマットで詳細を表示します。

[チャート（Chart）] を選択した場合、トラフィック チャートにカーソルを合わせると、Y 軸に沿って、対応する時間の Rx 値と Tx 値が X 軸に沿って表示されます。時間範囲セレクターのスライダを動かすことで、X 軸の持続時間の値を変更できます。Rx および Tx チェック ボックスをオンまたはオフにして、Y 軸の値を選択できます。

（注） 期間として**週**、**月**、または**年**を選択すると、Y 軸に沿ってピーク受信およびピーク送信の値を表示することもできます。

[表（Table）] を選択して、交通情報を表形式で表示します。

[チャート タイプとチャートのオプション（Chart Type and Chart Options）]：**[チャート タイプ（Chart Type）]** ドロップダウン リストから **[エリア チャート（Area Chart）]** または **[ライン チャート（Line Chart）]** を選択します。

次のチャート オプションを選択できます。

- **塗りつぶしのパターンを表示**
- **データマーカーを表示**
- **Y軸(対数目盛)**

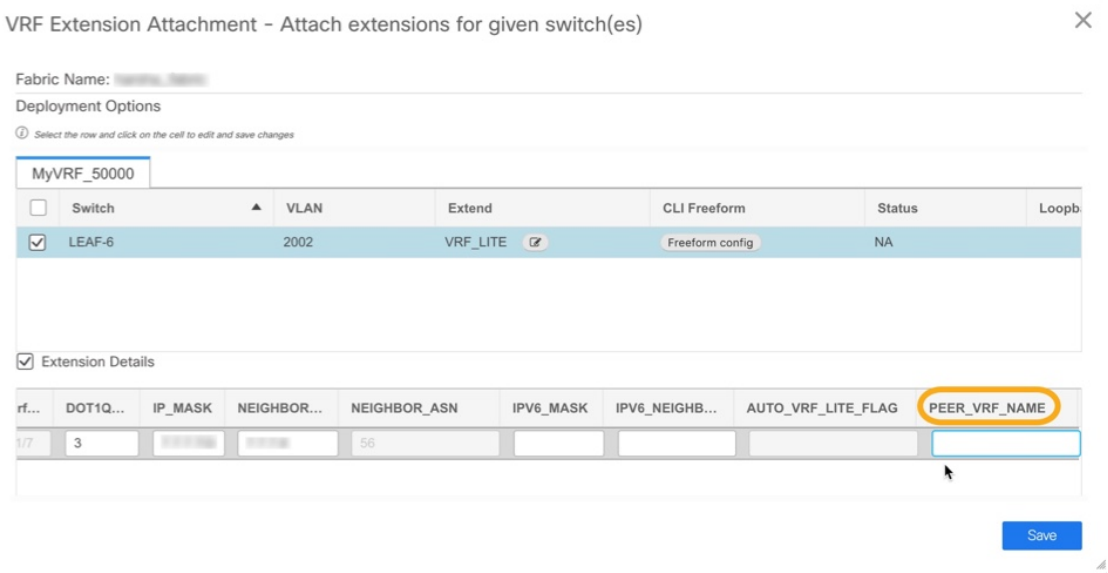
アクション：**[アクション（Actions）]** ドロップダウン リストから適切なオプションを選択して、トラフィック情報をエクスポートまたは印刷します。

シンメトリック自動 VRF Lite

- **[リンク管理（Link Management）]** ダイアログボックスの **[自動展開フラグ（Auto Deploy Flag）]** チェックボックスをオンにします。このチェックボックスをオンにすると、管理対象デバイスのリンクの両端で、VRF lite 展開が有効になります。
- バックツーバック シナリオで VRF lite を拡張する場合、VRF はピア ファブリックにすでに存在している必要があり、VRF 名は同じである必要があります。VRF がピア ファブリック内にない場合に、VRF Lite を拡張しようとすると、エラー メッセージが表示されます。
- Easy ファブリックと外部ファブリックの間で VRF Lite を拡張する場合、VRF 名は、送信元ファブリック、デフォルト、または別の VRF 名と同じにすることができます。ただし、サブインターフェイスの子 PTI および外部ファブリックでの VRF の作成またはピアリン

グには送信元があります。したがって、**[ポリシーの表示/編集（View/Edit policies）]**ウィンドウからポリシーを編集または削除することはできません。

- DCNM アップグレードを実行し、ポリシーが IFC にアタッチされていないことに気付いた場合は、ポリシーと VRF を編集して、それらを再度アタッチします。
- IPv6 アドレスの他に、IP マスク、IPv4 アドレス、ネイバー IP アドレスも入力して、対称 VRF lite を使用してトップダウンから VRF を展開します。
- 両方のファブリックに構成を展開します。



- VXLAN ファブリックの **[リンク（Link）]** タブで IFC を編集または削除できます。自動構成 IFC に関する追加の考慮事項は、次回の保存および展開時に IFC が再生成されないようにするために、モードを手動モードに戻すか、関連するデバイスでのみ構成を保存することです。
- バックツーバック シナリオでは、ファブリックの 1 つで VRF lite IFC を削除すると、VRF lite はピア ファブリックからも削除されます。
- Easy ファブリックと外部ファブリックの間の VRF ライトを削除する場合は、トップダウン方式を使用して Easy ファブリック内の拡張を削除します。拡張は外部ファブリックから自動的に削除されます。
- 両方のファブリックに構成を展開します。

VRF Lite でのユースケースについては、「*VXLAN BGP EVPN* ファブリックでのボーダー プロビジョニングのユースケース：*VRF Lite*」の章を参照してください。

レイヤ 3 ポートチャネル

Cisco DCNM リリース 11.3(1) 以降、レイヤ 3 ポートチャネルは外部リンクおよびインターフェイスでサポートされます。**[インターフェイス（Interfaces）]** ウィンドウでは、ポートチャネルおよび対応するレイヤ 3 ポートチャネル インターフェイス テンプレートを選択できます。このテンプレートを使用すると、レイヤ3インターフェイス関連のすべての構成を指定する機能など、レイヤ 3 ポートチャネルに関連するさまざまなオプションを構成できます。レイヤ 3 ポートチャネルは、Easy ファブリックと外部ファブリックでのみサポートされます。

VRF_LITE を使用した外部接続も、レイヤ 3 ポートチャネルを使用してサポートされます。物理ルーテッドインターフェイスおよびレイヤ3ポートチャネルインターフェイスの場合、MTU を設定できます。

Cisco DCNM でレイヤ 3 ポートチャネルを使用して対称 VRF Lite を拡張する方法を示すビデオも視聴できます。「レイヤ 3 ポートチャネルを使用した対称 VRF Lite の拡張」ビデオを参照してください。

インターフェイス上にレイヤ 3 ポートチャネルを構成する

Cisco DCNM Web UI からインターフェイス上にレイヤ 3 ポートチャネル を構成するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）]** > **[ファブリック（Fabrics）]** > **[インターフェイス（Interfaces）]** の順に選択します。

[インターフェイス（Interfaces）] ウィンドウが表示されます。

ステップ 2 [インターフェイスの追加（Add Interface）] をクリックします。

[Add Interface] ダイアログボックスが表示されます。

ステップ 3 **[ポートチャネル（Port Channel）]** のタイプとデバイスを選択します。

port-channel ID が自動入力されます。

ステップ 4 **[int_l3_port_channel]** ポリシーを選択します。

それに伴い **[全般（General）]** エリアにあるフィールドが変更されます。

ステップ 5 フィールドに値を入力し、**[保存（Save）]** をクリックします。

保存された設定のみがデバイスにプッシュされます。インターフェイスの追加中は、最初の保存後にのみポリシー属性を変更できます。既に使用している ID を使用しようとすると **Resource could not be allocated** エラーが表示されます。

ステップ 6 (Optional) **[プレビュー（Preview）]** オプションをクリックして、展開する構成をプレビューします。

ステップ 7 **[展開（Deploy）]** をクリックして、指定した論理インターフェイスを展開します。

新しく追加したインターフェイスが画面に表示されます。左上にあるブレークアウトオプションを使用してインターフェイスのブレークアウト、およびブレークアウト解除ができます。

IOS XE デバイス向けのインターフェイス上にレイヤ 3 ポートチャネルを構成する

IOS XE デバイス向けのインターフェイス上にレイヤ 3 ポートチャネル を構成するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [インターフェイス（Interfaces）]** の順に選択します。

[インターフェイス（Interfaces）] ウィンドウが表示されます。

ステップ 2 [インターフェイスの追加（Add Interface）] をクリックします。

[Add Interface] ダイアログボックスが表示されます。

ステップ 3 **[ポートチャネル（Port Channel）]** のタイプとデバイスを選択します。

port-channel ID が自動入力されます。

ステップ 4 **[ios_xe_int_l3_port_channel]** ポリシーを選択します。

それに伴い **[全般（General）]** エリアにあるフィールドが変更されます。

ステップ 5 フィールドに値を入力し、**[保存（Save）]** をクリックします。

保存された設定のみがデバイスにプッシュされます。インターフェイスの追加中は、最初の保存後にのみポリシー属性を変更できます。既に使用しているIDを使用しようとすると **Resource could not be allocated** エラーが表示されます。

（注） Cisco Catalyst 9000 シリーズ スイッチのポートチャネル ID の範囲は 1 ～ 128 で、Cisco ASR 1000 シリーズ ルータの範囲は 1 ～ 64 です。

ステップ 6 （任意） **[プレビュー（Preview）]** オプションをクリックして、展開する構成をプレビューします。

ステップ 7 **[展開（Deploy）]** をクリックして、指定した論理インターフェイスを展開します。

新しく追加したインターフェイスが画面に表示されます。

非 Nexus デバイスの物理インターフェイスへのポリシーの展開

Cisco DCNM リリース 11.4(1) からの非 Nexus デバイスをサポートするためのポリシーがさらに追加されました。非Nexusデバイスを外部ファブリックにインポートすると、ポートの数に基

づいてデフォルトでいくつかの物理インターフェイスが作成されます。ポリシーは、管理ポートに対してのみ作成されます。Cisco Catalyst 9000 シリーズ スイッチの場合、管理ポートは GigabitEthernet0/0 であり、Cisco ASR 1000 シリーズルータの場合、管理ポートは GigabitEthernet0 です。

次の表に、さまざまな 非 Nexus デバイスに追加されたポリシーを示します。

デバイス	ポリシー
Cisco CSR 1000v シリーズ ルータ	ギガビットイーサネット
Cisco IOS-XE デバイス	• GigabitEthernet_mgmt • ios_xe_int_access_host • ios_xe_int_freeform • ios_xe_int_routed_host • ios_xe_int_trunk_host （注） GigabitEthernet0/0 である管理ポートにのみ GigabitEthernet_mgmt ポリシーを使用します。

Cisco DCNM Web UI の **[インターフェイス（Interfaces）]** ウィンドウで物理インターフェイスにポリシーを展開するには、次の手順を実行します。

始める前に

非 Nexus デバイスを外部ファブリックにインポートして検出します。ファブリックがモニタモードになっていないことを確認してください。

手順

ステップ 1 ポリシーを展開するインターフェイスのチェックボックスをオンにします。

ステップ 2 **[構成の編集（Edit Configuration）]** アイコンをクリックします。

ステップ 3 ドロップダウンリストから **[ポリシー（Policy）]** を選択します。

有効なオプションは次のとおりです。

- **ギガビットイーサネット**
- **GigabitEthernet_mgmt**
- **ios_xe_int_access_host**
- **ios_xe_int_freeform**
- **ios_xe_int_routed_host**
- **ios_xe_int_trunk_host**

（注）
- 選択したオプションに基づいて、**[全般（General）]** エリアの下のフィールドは異なります。
- **ios_xe_int_routed_host** ポリシーを選択した場合は、VRF が帯域外で手動で構成されているか、**[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウで **ios_xe_switch_freeform** ポリシーを使用していることを確認してください。
- DCNM は NVE または BDI インターフェイスをサポートしていません。ただし、それらを手動またはアウトオブバンドですでに作成している場合は、**ios_xe_int_freeform** ポリシーを使用して構成を定義します。

ステップ 4 すべての必須フィールドに値を入力します。

（注） デバイスに基づいて速度を選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 **[プレビュー（Preview）]** をクリックし、保留中の構成をプレビューします。

ステップ 7 **[展開（Deploy）]** をクリックして、インターフェイスのポリシーを展開します。

サブインターフェイス上にレイヤ 3 ポートチャネルを構成する

Cisco DCNM Web UI からインターフェイス上にレイヤ 3 ポートチャネル を構成するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）]** > **[ファブリック（Fabrics）]** > **[インターフェイス（Interfaces）]** の順に選択します。

[インターフェイス（Interfaces）] ウィンドウが表示されます。

ステップ 2 レイヤ 3 ポートチャネル インターフェイスを選択します。

ステップ 3 [インターフェイスの追加（Add Interface）] をクリックします。

[Add Interface] ダイアログボックスが表示されます。

ステップ 4 **[サブインターフェイス（Subinterface）]** タイプを選択します。

サブインターフェイス ID とポリシーが自動入力され、**[全般（General）]** エリアのフィールドがそれに応じて変更されます。

ステップ 5 フィールドに値を入力し、**[保存（Save）]** をクリックします。

保存された設定のみがデバイスにプッシュされます。

ステップ 6 (Optional) **[プレビュー（Preview）]** オプションをクリックして、展開する構成をプレビューします。

ステップ 7 **[展開（Deploy）]** をクリックして、指定した論理インターフェイスを展開します。

確認ウィンドウが表示され、新しく追加されたサブインターフェイスがリストに表示されます。

ファブリック間接続のためのレイヤ 3 ポートチャネルの構成

[ファブリック ビルダ（Fabric Builder）] ウィンドウからレイヤ 3 ポートチャネル リンクを構成するには、次の手順を実行します。

Before you begin

インターフェイスにレイヤ 3 ポートチャネルが作成されていることを確認します。

Procedure

ステップ 1 VRF-Lite を拡張する Easy ファブリックまたは外部ファブリックを選択します。

ファブリック トポロジ ウィンドウが表示されます。

ステップ 2 **[アクション（Actions）]** ペインで **[表形式ビュー（Tabular view）]** をクリックします。

このファブリックのすべてのコンポーネントは、ステータスとその他の詳細とともにさまざまなタブに表示されます。

ステップ 3 **[リンク（Links）]** タブを選択します。

ステップ 4 **[リンクの追加（Add Link）]** アイコンをクリックします。

[リンクの追加（Add Link）] ダイアログボックスが表示されます。

ステップ 5 **[Inter-Fabric]** リンク タイプを選択します。

ステップ 6 **[VRF_LITE]** リンク サブタイプを選択します。

ステップ 7 **[テンプレートのリンク（Link Template）]** ドロップダウンリストから [テンプレートのリンク（link template）] を選択します。

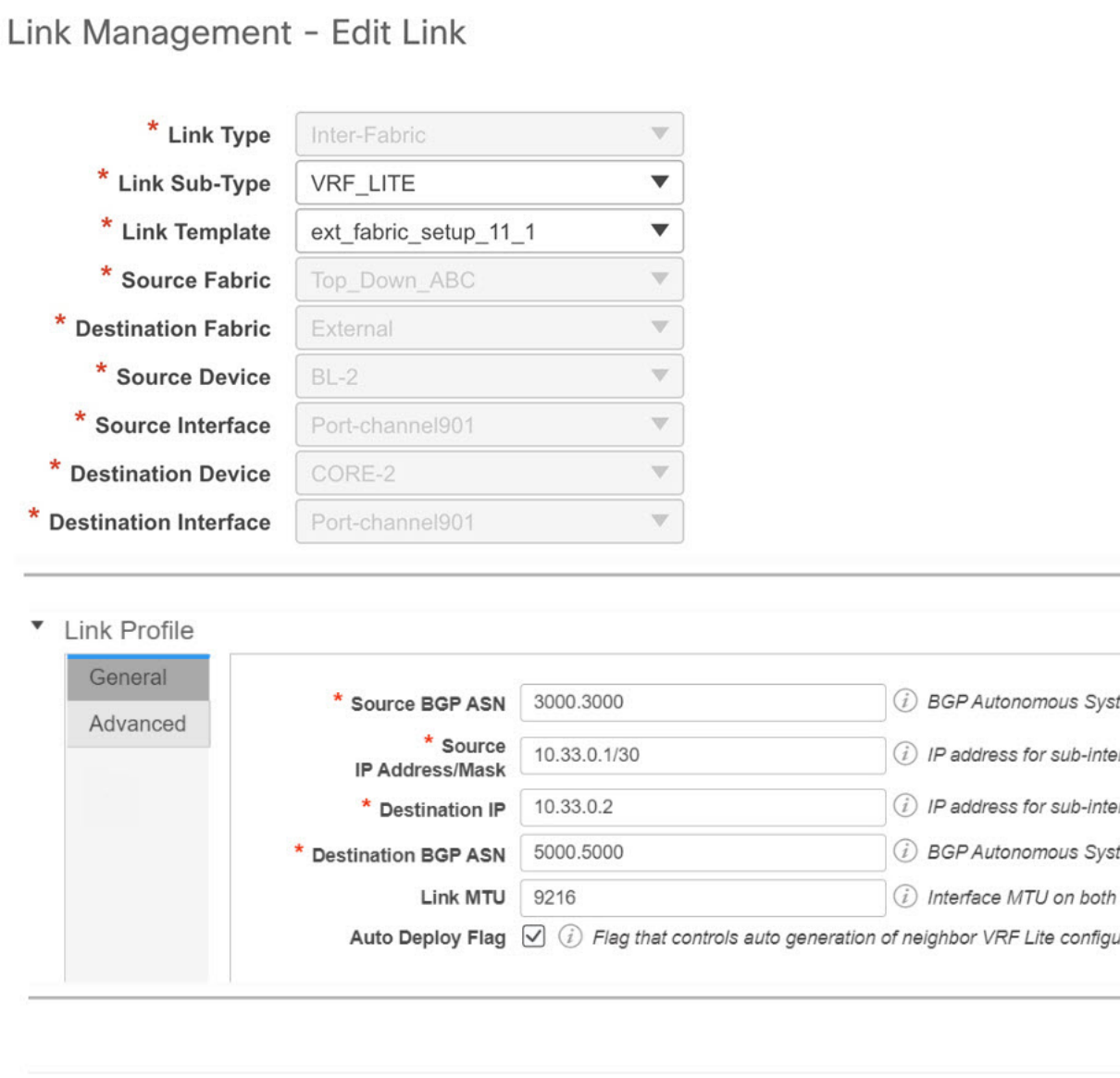
有効な値は、**[ext_fabric_setup_11_1]** および **[service_link_trunk]** です。

ステップ 8 それに応じて、他のすべてのフィールドに詳細を入力します。

ステップ 9 必要に応じて、**[リンク プロファイル（Link Profile）]** エリアのフィールドに詳細を入力します。

MTU を設定できます。**[Ext_VRF_Lite_Jython]** 自動展開テンプレートは、ファブリック内のデバイスの VRF-Lite 構成に使用されます。

ステップ 10 [保存（Save）] をクリックします。



What to do next

トップダウン フローを使用してレイヤ 3 ポートチャネルで VRF Lite IFC を作成した後、VRF Lite を使用して VRF を拡張すると、レイヤ 3 ポートチャネルにサブインターフェイスが作成されます。VRF が拡張された後でも、レイヤ 3 ポートチャネル リンクを編集できます。ただし、レイヤ 3 ポートチャネルは、ファブリック内リンクではサポートされていません。

表形式ビュー：操作ビュー

Cisco DCNM 11.3(1) から、ファブリックの運用サポートが提供されます。この機能は、次の情報を提供します。

- ファブリックの稼働状況
- アラームとイベント通知

[操作表示（Operational View）] タブで操作ステータス情報を表示できます。Cisco DCNM の上部ペインにある **[ヘルプ（Help）]** アイコンの横にある **[アラートと通知（Alerts and Notifications）]** アイコンをクリックすると、アラートとイベント通知を表示できます。

動作ステータスの表示

[ファブリック ビルダ（Fabric Builder）] ウィンドウからファブリックの動作ステータスを表示するには、次の手順を実行します。

手順

ステップ 1 ファブリックを選択します。
ファブリック トポロジ ウィンドウが表示されます。

ステップ 2 **[アクション（Actions）]** ペインで **[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 **[操作表示（Operational View）]** タブを選択します。

[操作表示（Operational View）] タブには、次のフィールドと説明があります。

フィールド	説明
Fabric Name（ファブリック名）	リンクのあるファブリックを指定します。
Name	リンクの名前を指定します。
Is Present	リンクが存在するかどうかを指定します。有効な値は **true** と **false** です。

フィールド	説明
リンクステータス	論理的リンクのステータスを指定します。論理リンクは、次のいずれかの状態になります。 • **[確立済み（Established）]**：リンクが **[確立済み（Established）]** 状態の場合、ピアは更新メッセージを送信して、BGP ピアにアドバタイズされた各ルートに関する情報を交換します。エラーが発生し、状態が **[Idle]** に変わると、通知が送信されます。**[確立（Established）]** 状態にできるのは、BGP ルーティング プロトコルを使用するリンクのみです。 • **[Idle]**：ピア間でエラーが発生した場合、BGP プロトコルを使用するリンクは [アイドル（Idle）] 状態になります。 • **[UP]**：ピア間でリンクが正常に確立されると、ISIS プロトコルを使用するリンクは **[UP]** 状態になります。 • **[FULL]**：ピア間でリンクが正常に確立されると、OSPF プロトコルを使用するリンクは **[FULL]** 状態になります。 • **[peer-alive]**：vPC ピア スイッチのバイタリティをモニタするピア キープアライブ リンクとしてリンクを指定します。
リンクタイプ	論理リンクのタイプを指定します。リンクは次のタイプにすることができます。 • **BGP** • **ISIS** • **OSPF** • **[VPC_KEEPALIVE]**
稼働時間	リンク タイプの稼働時間を指定します。

これらすべての列が並べ替え可能です。

論理リンクの表示

[トポロジ（Topology）] ウィンドウに論理リンクが表示されます。Cisco DCNM Web UI から論理リンクを表示するには、次の手順を実行します。

手順

ステップ 1 **[トポロジ（Topology）]** を選択します。

[トポロジ（Topology）] ウィンドウが表示されます。

ステップ 2 [表示（Show）] ペインの **[論理リンク（Logical Links）]** チェック ボックスをオンにします。

デバイス間の論理リンクは青色で表示されます。

（注） リンクの色は、状態に基づいて変化します。

ステップ 3 （任意） リンクにカーソルを合わせると、リンク タイプが表示されます。

アラートとイベント通知の表示

アラートおよびイベント通知には、正常性スコア、トポロジ ノード表示、アラーム ビュー、アラーム ポリシー、および通知サービスが含まれます。イベントは、ネットワーク、デバイス、またはCisco DCNMに影響を与えるアクションです。アラートは、イベントの一部としてトリガーされて表示される通知です。

ToR スイッチのサポート

Cisco DCNM 11.3(1)以降、トップオブラック（ToR）スイッチのサポートがDCNMに追加されました。外部ファブリックにレイヤ 2 ToR スイッチを追加でき、それらを Easy ファブリックのリーフ スイッチに接続できます。詳細については「*ToR* スイッチの構成とネットワークの展開」を参照してください。

vPC ファブリック ピアリング

2 台のスイッチの仮想ピア リンクを作成するか、既存の物理ピア リンクを仮想ピア リンクに変更できます。Cisco DCNM リリース 11.2(1) で vPC ファブリック ピアリングをサポートするのは、グリーンフィールド展開だけです+ ただし、グリーンフィールド展開とブラウンフィールド展開の両方で、Cisco DCNM リリース 11.3(1) の vPC ファブリック ピアリングがサポートされます。この機能は、**Easy_Fabric_11_1** および **Easy_Fabric_eBGP** ファブリック テンプレートに適用されます。

（注） **Easy_Fabric_eBGP** ファブリックは、ブラウンフィールドインポートをサポートしていません。

ガイドラインと制約事項

次に、vPC ファブリック ピアリングの注意事項と制限事項を示します。

- vPC ファブリック ピアリングは、Cisco DCNM リリース 11.2(1) および Cisco NX-OS リリース 9.2(3) からサポートされています。

- Cisco Nexus N9K-C9332C スイッチ、Cisco Nexus N9K-C9364C スイッチ、Cisco Nexus N9K-C9348GC-FXP スイッチ、および FX で終わる Cisco Nexus 9000 シリーズ スイッチ、FX2 だけが vPC ファブリック ピアリングをサポートします。
- Cisco DCNM リリース 11.4(1) 以降、Cisco Nexus N9K-C93180YC-FX3S および N9K-C93108TC-FX3P プラットフォーム スイッチは vPC ファブリック ピアリングをサポートします。
- Cisco Nexus 9300-EX 、および 9300-FX/FXP/FX2/FX3 プラットフォーム スイッチは、vPC ファブリック ピアリングをサポートします。Cisco Nexus 9200 および 9500 プラットフォーム スイッチは、vPC ファブリック ピアリングをサポートしていません。
- 他の Cisco Nexus 9000 シリーズ スイッチを使用している場合、**[保存して展開（Save & Deploy）]** 中に警告が表示されます。これらのスイッチは将来のリリースでサポートされるため、警告が表示されます。
- **[仮想ピアリンクを使用（Use Virtual Peerlink）]** オプションを使用して、vPC ファブリック ピアリングをサポートしていないスイッチをペアリングしようとすると、ファブリックの展開時に警告が表示されます。
- オーバーレイの有無にかかわらず、物理ピア リンクを仮想ピア リンクに、またはその逆に変換することができます。
- ボーダー ゲートウェイのリーフ ロールを持つスイッチは、vPC ファブリック ピアリングをサポートしていません。
- vPC ファブリック ピアリングは、Cisco Nexus 9000 シリーズ モジュラ シャーシおよび FEX ではサポートされていません。これらのいずれかをペアリングしようとすると、**[保存して展開中（Save & Deploy）]** にエラーが表示されます。
- ブラウンフィールド展開とグリーンフィールド展開は、Cisco DCNM リリース 11.3(1) の vPC ファブリック ピアリングをサポートします。
- ただし、物理ピア リンクを使用して接続されているスイッチをインポートし、**[保存して展開（Save & Deploy）]** 後に物理ピア リンクを仮想ピア リンクに変換することはできます。機能の設定中に TCAM リージョンを更新するには、構成端末で **hardware access-list tcam ingress-flow redirect** *512* コマンドを使用します。

ファブリック vPC ピアリングの QoS

Cisco DCNM リリース 11.4(1) 以降、**Easy_Fabric_11_1** ファブリック設定で、vPC ファブリック ピアリング通信の配信を保証するためにスパインで QoS を有効にできます。さらに、QoS ポリシー名を指定できます。

グリーンフィールド展開については、次のガイドラインに注意してください。

- QoS が有効で、ファブリックが新しく作成された場合：
  - スパインまたはスーパー スパイン ネイバーが仮想 vPC である場合に、スーパー スパインが存在しているなら、スーパー スパインからリーフまたはボーダーからスパインなどの無効なリンクからのネイバーが優先されないようにします。

- Cisco Nexus 9000 シリーズ スイッチ モデルに基づいて、**switch_freeform** ポリシー テンプレートを使用して、推奨されるグローバル QoS 構成を作成します。
- スパインから正しいネイバーへのファブリック リンクで QoS を有効にします。

- QoS ポリシー名が編集されている場合は、ポリシー名の変更がすべての場所（グローバルとリンクなど）に適用されることを確認してください。
- QoS が無効になっている場合は、QoS ファブリック vPC ピアリングに関連するすべての設定を削除します。
- 変更がない場合は、既存の PTI を尊重します。

グリーンフィールド展開の詳細については、「新しい *VXLAN BGP EVPN* ファブリックの作成」セクションを参照してください。

ブラウンフィールド展開については、次のガイドラインに注意してください。

ブラウンフィールドのシナリオ 1：

- QoS が有効で、ポリシー名が指定されている場合：

（注） QoS は、グローバル QoS およびネイバー リンク サービス ポリシーのポリシー名が、すべてのファブリック vPC ピアリング接続スパインで同じ場合にのみ有効にする必要があります。

  - ポリシー名に基づいてスイッチから QoS 構成をキャプチャし、ポリシー名に基づいて説明されていない構成からそれをフィルタリングし、構成を PTI 説明付きの **switch_freeform** に入れます。
  - ファブリック インターフェイスのサービス ポリシー構成も作成します。
  - グリーンフィールド構成は、ブラウンフィールド構成を尊重する必要があります。

- QoS ポリシー名が編集されている場合は、既存のポリシーとブラウンフィールドの追加構成も削除し、推奨される構成でグリーンフィールド フローに従います。
- QoS が無効になっている場合は、QoS ファブリック vPC ピアリングに関連するすべての設定を削除します。

（注） 生じ得る、またはエラーのために不一致が生じたユーザー構成のクロスチェックは行われず、ユーザーには差分が表示される場合があります。

ブラウンフィールドのシナリオ 2：

- QoSが有効になっていて、ポリシー名が指定されていない場合、QoS設定は、アカウントの対象となっていない、スイッチの自由形式設定の一部です。
- ブラウンフィールドの **[保存して展開（Save & Deploy）]** 後にファブリック設定から QoS が有効になっている場合、QoS構成が重複し、ファブリック vPC ピアリング構成がすでに存在する場合は相違が表示されます。

ブラウンフィールド展開の詳細については、「新しい *VXLAN BGP EVPN* ファブリックの作成」セクションを参照してください。

フィールドと説明+

スイッチの vPC ペアリング ウィンドウを表示するには、ファブリック トポロジ ウィンドウでスイッチを右クリックし、**[vPC ペアリング（vPC Pairing）]** を選択します。スイッチの vPC ペアリング ウィンドウには、次のフィールドがあります。

フィールド	説明
仮想ピアリンクを使用	スイッチ間の仮想ピア リンクを有効または無効にすることができます。
スイッチ名	ファブリック内のすべてのピア スイッチを指定します。 （注） ピア スイッチをペアリングしていない場合は、ファブリック内のすべてのスイッチを表示できます。ピア スイッチをペアリングすると、vPC ペアリング ウィンドウにはピア スイッチだけが表示されます。
推奨	ピア スイッチを選択したスイッチとペアリングできるかどうかを指定します。有効な値は **true** と **false** です。推奨されるピア スイッチは **true** に設定されます。
理由	選択したスイッチとピア スイッチ間の vPC ペアリングが可能または不可能な理由を指定します。
シリアル番号（Serial Number）	スイッチのシリアル番号を指定します。

[vPC ペアリング（vPC Pairing）] オプションを使用して、次のことを実行できます。

仮想ピア リンクの作成

Cisco DCNM Web UI で仮想ピア リンクを作成するには、次の手順を実行します。

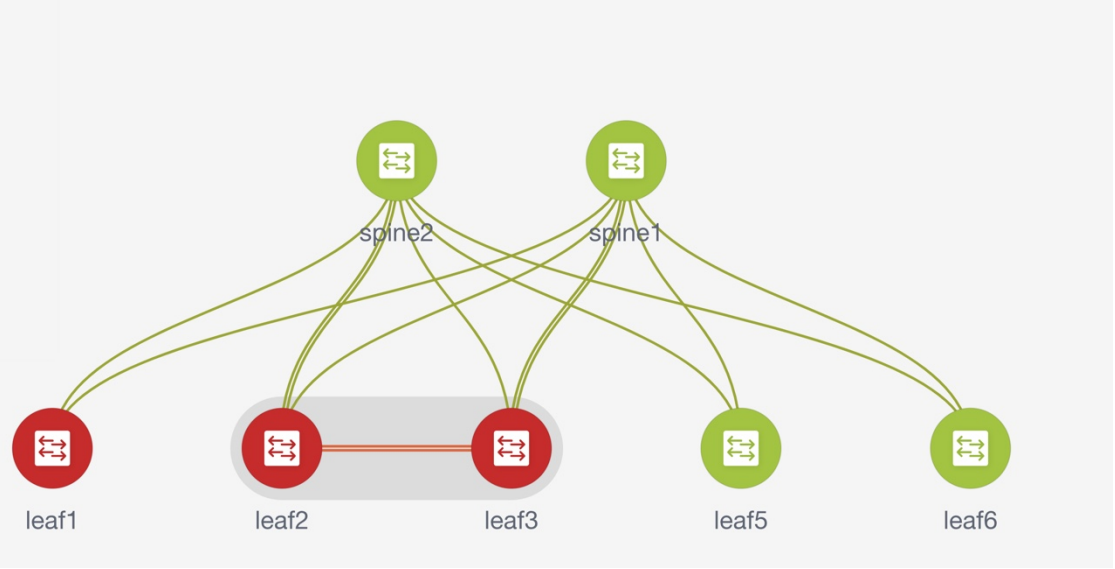
Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

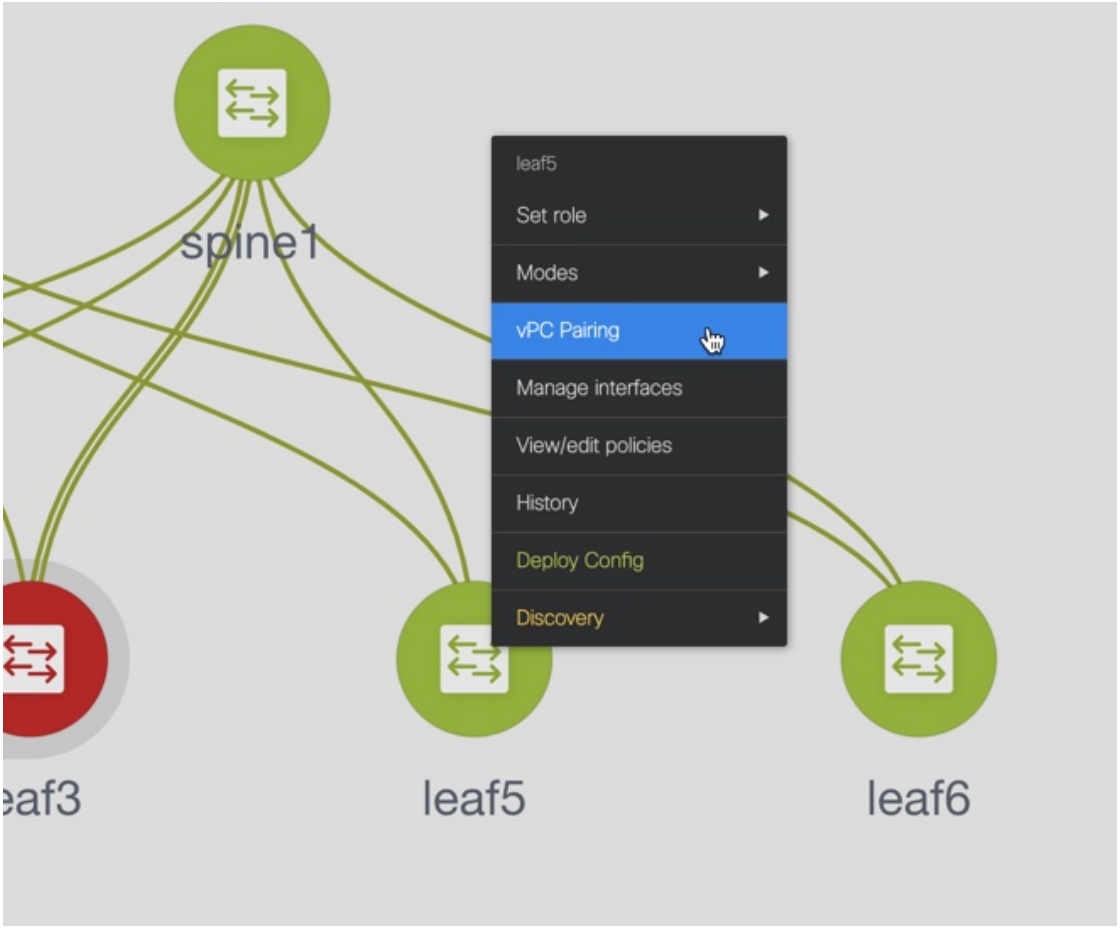
ステップ 2 **Easy_Fabric_11_1** または **Easy_Fabric_eBGP** ファブリック テンプレートを使用してファブリックを選択します。

ファブリック トポロジ ウィンドウが表示されます。



ステップ 3 ドロップダウン リストから **[vPC ペアリング（vPC Pairing）]** を選択します。

ピア選択のためのウィンドウが表示されます。



Note または、**[アクション（Actions）]** ペインから**表形式ビュー**に移動することもできます。**[スイッチ（Switches）]** タブでスイッチを選択し、**[vPC Pairing（vPC ペアリング）]**をクリックしてvPCペアを作成、編集、またはペアリング解除します。ただし、このオプションは、Cisco Nexus スイッチを選択した場合にのみ使用できます。

ボーダー ゲートウェイ リーフ ロールを持つスイッチを選択すると、次のエラーが表示されます。

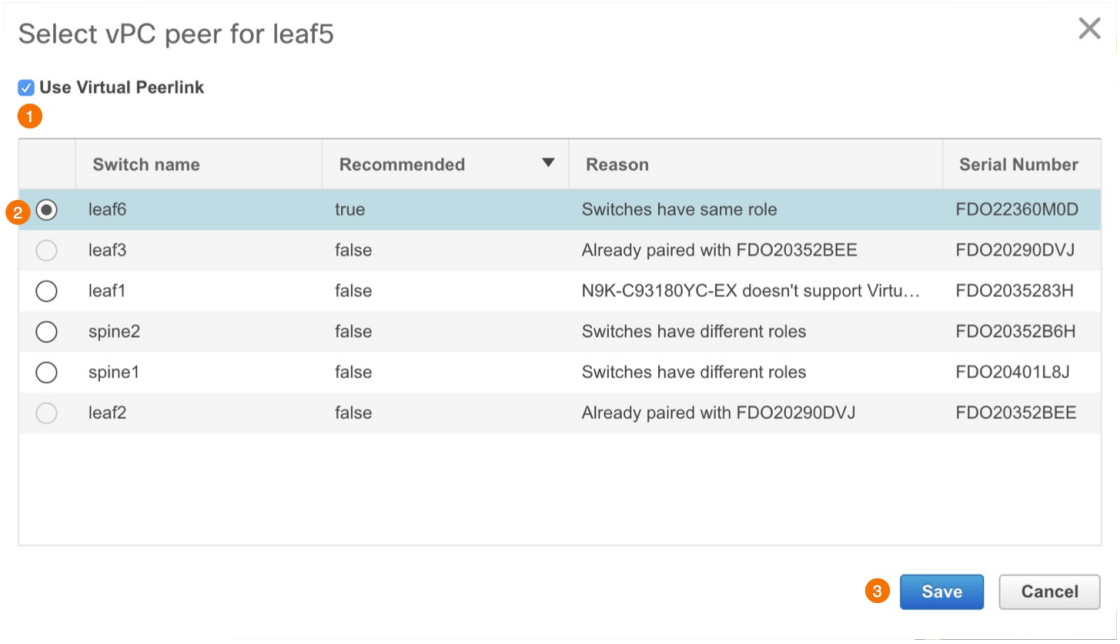
`<switch-name> にはネットワーク/VRF がアタッチされています（<switch-name> has a Network/VRF attached）。vPC ペアリング/ペアリング解除の前にネットワーク/VRF をデタッチしてください（Please detach the Network/VRF before vPC Pairing/Unpairing）。`

ステップ 4 **[仮想ピアリンクを使用（Use Virtual Peerlink）]** チェック ボックスをオンにします。

ステップ 5 ピア スイッチを選択し、**[推奨（Recommended）]** 列をチェックして、ペアリングが可能かどうかを確認します。

値が **true** の場合、ペアリングが可能です。推奨が **false** の場合でも、スイッチをペアリングすることは可能です。ただし、**[保存と展開（Save & Deploy）]** 中に警告またはエラーが発生します。

ステップ 6 [保存（Save）] をクリックします。



ステップ 7 **[ファブリック トポロジ（Fabric Topology）]** ウィンドウで、**[保存と展開（Save & Deploy）]** をクリックします。

[構成展開（Config Deployment）] ウィンドウが表示されます。

ステップ 8 **[構成のプレビュー（Preview Config）]** 列のスイッチに関連するフィールドをクリックします。

そのスイッチの **[構成のプレビュー（Config Preview）]** ウィンドウが表示されます。

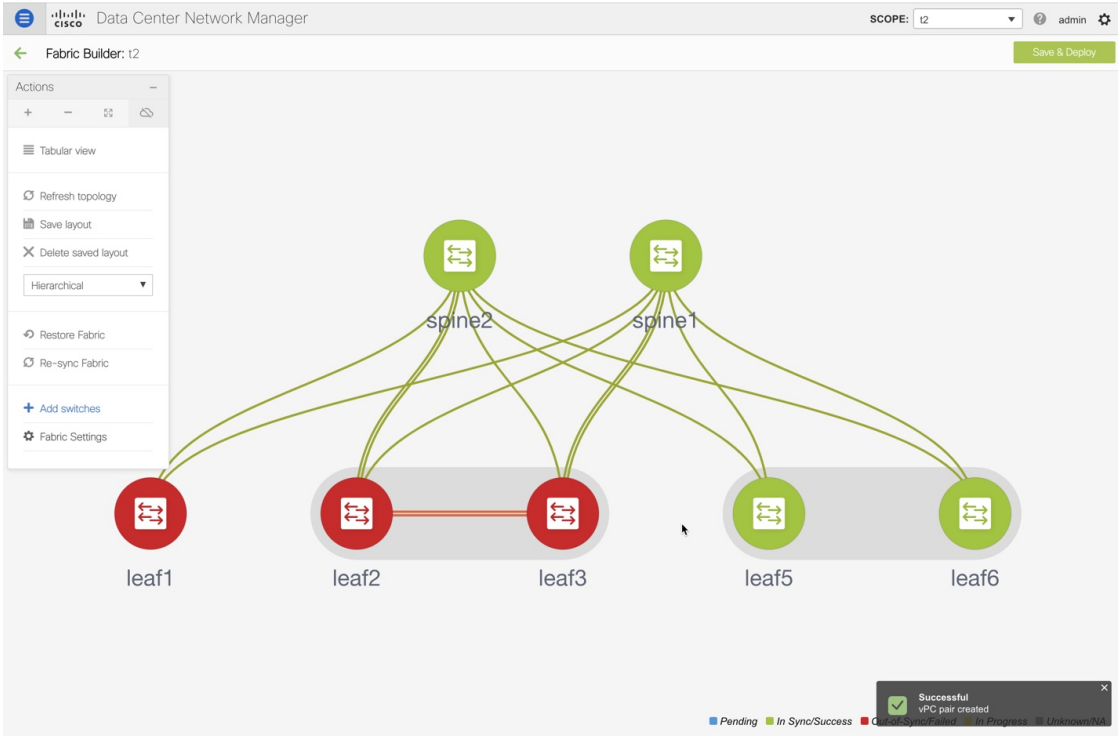
ステップ 9 vPC リンクの詳細が、保留中の構成と、元の構成を横に並べて表示されます。

ステップ 10 ウィンドウを閉じます。

ステップ 11 **[保存と展開（Save & Deploy）]** アイコンの横にある保留中のエラーアイコンをクリックして、エラーと警告を表示します（存在する場合）。

TCAM に関連する警告が表示された場合は、**[解決（Resolve）]** アイコンをクリックします。スイッチのリロード確認用のダイアログボックスが表示されます。[OK] をクリックします。ファブリック トポロジ ウィンドウの **[表形式ビュー（Tabular view）]** からスイッチをリロードすることもできます。

vPC ファブリック ピアリングを介して接続されているスイッチは、灰色の雲で囲まれています。



物理ピア リンクから仮想ピア リンクへの変換

Cisco NDFC Web UI で物理ピア リンクを仮想ピア リンクに変換するには、次の手順を実行します。

Before you begin

- スイッチのメンテナンス ウィンドウ中に、物理ピア リンクから仮想ピア リンクへの変換を計画します。
- スイッチが vPC ファブリック ピアリングをサポートしていることを確認します。以下のスイッチのみが vPC ファブリック ピアリングをサポートします。
  - Cisco Nexus N9K-C9332C スイッチ、Cisco Nexus N9K-C9364C スイッチ、および Cisco Nexus N9K-C9348GC-FXP スイッチ。
  - FX、FX2、および FX2-Z で終わる Cisco Nexus 9000 シリーズ スイッチ。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 **Easy_Fabric_11_1** または **Easy_Fabric_eBGP** ファブリック テンプレートを使用してファブリックを選択します。

ステップ 3 物理ピア リンクを使用して接続されているスイッチを右クリックし、ドロップダウンリストから **[vPC ペアリング（vPC Pairing）]** を選択します。

ピア選択のためのウィンドウが表示されます。

Note または、**[アクション（Actions）]** ペインから**表形式ビュー**に移動することもできます。**[スイッチ（Switches）]** タブでスイッチを選択し、**[vPC Pairing（vPC ペアリング）]**をクリックしてvPCペアを作成、編集、またはペアリング解除します。ただし、このオプションは、Cisco Nexus スイッチを選択した場合にのみ使用できます。

ボーダー ゲートウェイ リーフ ロールを持つスイッチを選択すると、次のエラーが表示されます。

`<switch-name> にはネットワーク/VRF がアタッチされています（<switch-name> has a Network/VRF attached）。vPC ペアリング/ペアリング解除の前にネットワーク/VRF をデタッチしてください（Please detach the Network/VRF before vPC Pairing/Unpairing）。`

ステップ 4 **[推奨（Recommended）]** 列をチェックして、ペアリングが可能かどうかを確認します。

値が **true** の場合、ペアリングが可能です。推奨が **false** の場合でも、スイッチをペアリングすることは可能です。ただし、**[保存と展開（Save & Deploy）]** 中に警告またはエラーが発生します。

ステップ 5 **[仮想ピアリンクを使用（Use Virtual Peerlink）]** チェック ボックスをオンにします。

[ペア解除（Unpair）] アイコンが **[保存（Save）]** に変わります。

ステップ 6 [保存（Save）] をクリックします。

Note **[保存（Save）]** をクリックすると、展開しなくても、スイッチ間の物理 vPC ピア リンクが自動的に削除されます。

ステップ 7 **[ファブリック トポロジ（Fabric Topology）]** ウィンドウで、**[保存と展開（Save & Deploy）]** をクリックします。

[構成展開（Config Deployment）] ウィンドウが表示されます。

ステップ 8 **[構成のプレビュー（Preview Config）]** 列のスイッチに関連するフィールドをクリックします。

そのスイッチの **[構成のプレビュー（Config Preview）]** ウィンドウが表示されます。

ステップ 9 vPC リンクの詳細が、保留中の構成と、元の構成を横に並べて表示されます。

ステップ 10 ウィンドウを閉じます。

ステップ 11 **[保存と展開（Save & Deploy）]** アイコンの横にある保留中のエラーアイコンをクリックして、エラーと警告を表示します（存在する場合）。

TCAM に関連する警告が表示された場合は、**[解決（Resolve）]** アイコンをクリックします。スイッチのリロード確認用のダイアログボックスが表示されます。[OK] をクリックします。ファブリック トポロジ ウィンドウの **[表形式ビュー（Tabular view）]** からスイッチをリロードすることもできます。

ピア スイッチ間の物理ピア リンクが赤に変わります。このリンクを削除します。スイッチは仮想ピア リンクを介してのみ接続されるようになり、灰色の雲に囲まれて表示されます。

仮想ピア リンクから物理ピア リンクへの変換

Cisco DCNM Web UI で仮想ピア リンクを物理ピア リンクに変換するには、次の手順を実行します。

Before you begin

vPC ファブリック ピアリングを無効にする前に、物理ピア リンクを使用してスイッチを接続します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 **[Easy_Fabric_11_1]** または **[Easy_Fabric_eBGP]** ファブリック テンプレートを使用してファブリックを選択します。

ステップ 3 仮想ピア リンクを介して接続されているスイッチを右クリックし、ドロップダウンリストから **[vPC ペアリング（vPC Pairing）]** を選択します。

ピア選択のためのウィンドウが表示されます。

Note または、**[アクション（Actions）]** ペインから**表形式ビュー**に移動することもできます。**[スイッチ（Switches）]** タブでスイッチを選択し、**[vPC Pairing（vPC ペアリング）]**をクリックしてvPCペアを作成、編集、またはペアリング解除します。ただし、このオプションは、Cisco Nexus スイッチを選択した場合にのみ使用できます。

ステップ 4 **[仮想ピアリンクを使用（Use Virtual Peerlink）]** チェック ボックスをオフにします。

[ペア解除（Unpair）] アイコンが **[保存（Save）]** に変わります。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 **[ファブリック トポロジ（Fabric Topology）]** ウィンドウで、**[保存と展開（Save & Deploy）]** をクリックします。

[構成展開（Config Deployment）] ウィンドウが表示されます。

ステップ 7 **[構成のプレビュー（Preview Config）]**列のスイッチに関連するフィールドをクリックします。

そのスイッチの **[構成のプレビュー（Config Preview）]** ウィンドウが表示されます。

ステップ 8 vPC ピア リンクの詳細が、保留中の構成と、元の構成を横に並べて表示されます。

ステップ 9 ウィンドウを閉じます。

ステップ 10 **[保存と展開（Save & Deploy）]** アイコンの横にある保留中のエラーアイコンをクリックして、エラーと警告を表示します （存在する場合）。

TCAM に関連する警告が表示された場合は、**[解決（Resolve）]** アイコンをクリックします。スイッチのリロード確認用のダイアログボックスが表示されます。[OK] をクリックします。ファブリック トポロジ ウィンドウの **[表形式ビュー（Tabular view）]** からスイッチをリロードすることもできます。

灰色の雲で表される仮想ピア リンクが表示されなくなり、代わりにピア スイッチが物理ピア リンクを介して接続されます。

vPC で PIP をアドバタイズする

ファブリック設定では、**vPC advertise-pip** チェックボックスをオンにして、ファブリック内のすべての vPC で PIP アドバタイズ機能を有効にすることができます。Cisco DCNM リリース 11.4（1）以降、**vpc_advertise_pip_jython** ポリシーを使用して、ファブリック内の特定の vPC で PIP のアドバタイズ機能を有効にできます。

次のガイドラインに注意してください。

- Advertising-pip がグローバルに有効になっていない場合、または vPC ピアがファブリック ピアリングを使用していない場合にのみ、特定のピアで vpc_advertise_pip_jython ポリシーを作成できます。
- **vpc advertise-pip** を有効にしても、現在の動作には影響しません。
- ファブリックのアドバタイズ ピップを無効化しても、このポリシーには影響しません。
- スイッチのペアリングを解除すると、このポリシーが削除されます。
- このポリシーは、作成されたピア スイッチから手動で削除できます。

手順

ステップ 1 **[ファブリック ビルダー（Fabric Builder）]** ウィンドウでファブリックをクリックし、vPC のあるスイッチを右クリックして **[表示 / ポリシーを編集（View/Edit Policies）]** を選択します。

ステップ 2 **[追加（Add）]** をクリックして **vpc_advertise_pip_jython** ポリシー テンプレートを選択し、必須パラメータ データを入力します。

（注） このポリシーを 1 つの vPC ピアに追加すると、両方のピアで vpc アドバタイズのそれぞれのコマンドが作成されます。

ステップ 3 **[保存（Save）]** をクリックして、このポリシーを展開します。

ThousandEyes Enterprise Agent

モニタ対象のネットワーク内でユーザが特定のウェブサイトにアクセスするとき、ThousandEyes Enterprise Agent はネットワークとアプリケーション レイヤのパフォーマンス データを収集します。テストの実行、ネットワーク パスと接続の詳細なアスペクトのチェック、ネットワーク ルーティングのステータス チェック、インテント、実行構成などの変更のモニタを行うために、データは使用されます。

リリース 11.5(3) から、ThousandEyes Enterprise Agent は Cisco DCNM と統合されています。

ThousandEyes Enterprise Agent は、NX-OS バージョン 9.3(7) および 10.2(1) 以降のリリースを備えた Cisco Nexus 3000-R シリーズおよび Cisco Nexus 9000 クラウド スケール シリーズでサポートされています。

これは、次のファブリック テンプレートでサポートされています。

- Easy_Fabric_11_1
- Easy_Fabric_eBGP
- External_Fabric_11_1
- LAN_Classic

Cisco DCNM **[Web UI]** > **[制御（Control）]** > **[ThousandEyes]** > **[構成（Configure）]** を使用して、ThousandEyes Enterprise Agent のグローバル設定を構成できます。

このセクションの内容は次のとおりです。

TCAM および CoPP ポリシーの構成

スイッチに ThousandEyes Enterprise Agent 機能をインストールする前に、関連するポリシーを Cisco Nexus 3000-R シリーズおよび Cisco Nexus 9000 クラウド 拡張 シリーズ スイッチに追加してください。

Cisco DCNM Web UI からスイッチで TCAM および CoPP ポリシーを構成するには、次の手順を実行します。

Procedure

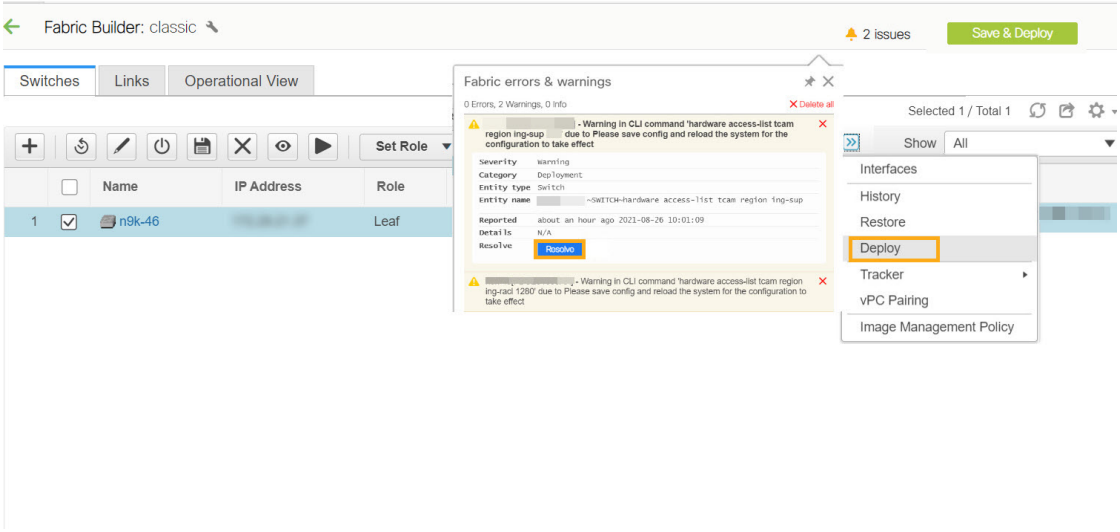
ステップ 1 DCNM Web UI から、**[制御（Control）]** > **[ファブリック ビルダー（Fabric Builder）]** を選択し、ファブリックを選択して、**[アクション（Actions）]** ウィンドウで **[Tabular View]** をクリックします。

[スイッチ（Switches）] タブが表示されます。

ステップ 2 **[スイッチ（Switches）]** タブで 1 つまたは複数のスイッチを選択し、**[ポリシー（Policies）]** ボタンをクリックします。

ステップ 3 **[追加（Add）]** アイコンをクリックします。

ステップ 4 Cisco Nexus 9000 EX、FX、および FX2 シリーズ スイッチの TCAM ポリシーを追加するには、次の手順を実行します。



- EX シリーズ スイッチには ThousandEyes_Agent_N9K_EX_tcam_config を、FX および FX2 シリーズ スイッチには ThousandEyes_Agent_N9K_FX_FEX2_tcam_config を選択します。
- **[優先度（Priority）]** フィールドに値 200 を入力し、**[保存（Save）]** をクリックします。
- **[スイッチ（Switches）]** タブで、ポリシーを追加するスイッチを選択します。**[展開する（Deploy）]** をクリックして、設定をスイッチに展開します。

Note スイッチに TCAM の変更を反映させるためにスイッチをリロードする必要があることを示す警告メッセージが表示されます。**[解決（Resolve）]**をクリックしてスイッチをリロードします。

ステップ 5 Easy_Fabric_11_1 および Easy_Fabric_eBGP テンプレートに CoPP ポリシーを追加するには、次の手順を実行します。

- DCNM Web UI から、**[Control（制御）]** > **[Fabric Builder（ファブリック ビルダー）]** > **[Fabric Settings（ファブリック設定）]** を選択し、**[Advanced（詳細設定）]** タブをクリックします。
- **[CoPP プロファイル（CoPP Profile）]** フィールドで手動を選択します。

ステップ 6 サポートされているすべてのスイッチとファブリック テンプレートにポリシーを展開するには、次の手順を実行します。

- 適切なスイッチを選択し、**[再生（Play）]** ボタンをクリックします。

  [デバイスでのスイッチ CLI の実行（Execute Switch CLIs on Devices）] ウィンドウが表示されます。

- [テンプレート（Template）] ドロップダウン リストから **ThousandEyes_Agent_Copy_CoPP** を選択し、[展開（Deploy）] をクリックします。
- **[スイッチ（Switches）]** タブで、適切なスイッチを選択します。**[ポリシー（New Policy）]** をクリックします。

[ポリシー（Policy）] ウィンドウが表示されます。

- **[追加（Add）]** アイコンをクリックします。
- [ポリシー（Priority）] ドロップダウン リストから **[ThousandEyes_Agent_CoPP]** を選択します。
- [優先度（Priority）] フィールドに値 210 を入力し、**[保存（Save）]** をクリックします。
- **[スイッチ（Switches）]** タブで、ポリシーを追加するスイッチを選択します。**[保存（Save）]** をクリックして、構成をスイッチに展開します。

ThousandEyes Enterprise エージェント アクションの実行

管理モードのファブリックに対してのみ、ThousandEyes Enterprise Agent アクションを実行できます。

Note ThousandEyes Enterprise Agent をスイッチにインストールする前に、TCAM および COPP ポリシーがスイッチに設定されていることを確認してください。

DCNM Web UI を使用して ThousandEyes Enterprise Agent を起動、停止、インストール、またはアンインストールするには、次の手順を実行します。

Procedure

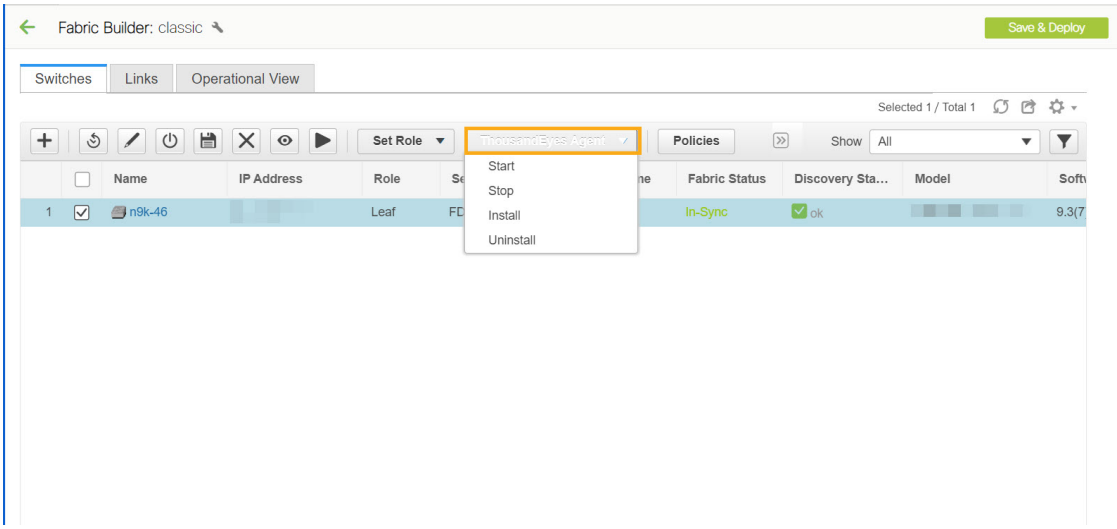
ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。長方形のボックスは、各ファブリックを表します。

ステップ 2 ファブリックを選択し、**[アクション（Actions）]** ウィンドウの **[表形式のビュー（Tabular View）]** をクリックします。

[スイッチ（Switches）] タブが表示されます。

ステップ 3 単一または複数のスイッチを選択し、**[ThousandEyes エージェント（ThousandEyes Agent）]** ドロップダウン リストから必要なアクションをクリックします。



次の操作を実行できます。

- **[インストール（Install）]** – ThousandEyes Enterprise Agent をインストールしますインストール後、[ThousandEyes Agent Status] 列に RUNNING と表示されます。
- **[開始（Start）]** – 以前に停止した、スイッチ上の ThousandEyes Enterprise Agent を開始します。

  Note スイッチでエージェントを開始する前に、ThousandEyes Enterprise Agent をインストールする必要があります。

- **[停止（Stop）]** – スイッチの ThousandEyes Enterprise Agent を停止します。
- **[アンインストール（Uninstall）]** – スイッチから ThousandEyes Enterprise Agent をアンインストールします。アクションを実行するとポップアップ ウィンドウが表示され、メッセージが表示されます - **ThousandEyes アクションが完了しました。ステータスを確認してください！**

  DCNM から ThousandEyes Enterprise Agent をアンインストールしても、ThousandEyes ポータルのアカウント グループ トークン番号はクリアされません。スイッチ上の既存の ThousandEyes Enterprise Agent アカウント グループ トークンを削除するには、ThousandEyes Enterprise Agent の削除セクションを参照してください。

ThousandEyes Enterprise Agent ステータス

ThousandEyes Enterprise Agent のステータス メッセージは次のとおりです。

- **[NOT_INSTALLED]**：ThousandEyes Enterprise Agent はスイッチにインストールされません。
- **[RUNNING]**：ThousandEyes Enterprise Agent はスイッチでアクティブです。
- **[STOPPED]**：ThousandEyes Enterprise Agent をスイッチで停止します。

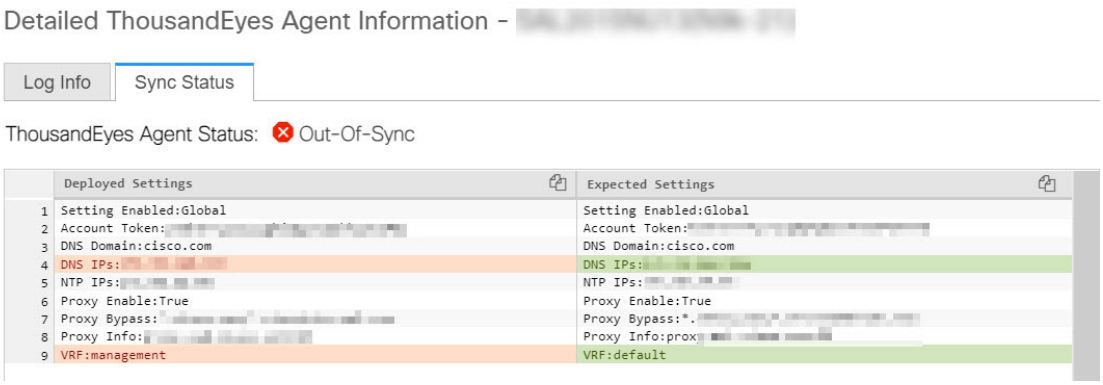
- **[UNSUPPORTED_VERSION]**：ThousandEyes Enterprise Agent は、スイッチの NX-OS バージョンではサポートされていません。
- **[UNSUPPORTED_PLATFORM]**：ThousandEyes Enterprise Agent は、選択したスイッチ プラットフォームでサポートされていません。
- **NA**：ThousandEyes Enterprise Agent グローバル設定は DCNM で構成されていません

1. **[ThousandEyes ステータス（ThousandEyes Status）]** をクリックして、ThousandEyes Enterprise Agent の情報を表示します。

   [ThousandEyes Agent の詳細情報（Detailed ThousandEyes Agent Information）] ページが表示されます。

   - **[ログ情報（Log Info）]** タブには、ランタイム エージェントのステータスまたはスイッチのエラー ログが表示されます。
   - **[同期ステータス（Sync Status）]** タブには、スイッチの展開された設定と予想される設定の詳細が表示されます。

ThousandEyes Enterprise Agent の構成がその時点での DCNM の有効な構成と異なる場合、DCNM は構成の不一致（**[In-Sync]**、**[Out-Of-Sync]**）を示します。構成が一致しない場合は、ThousandEyes Enterprise Agent をアンインストール、削除、およびインストールして、構成を同期させる必要があります。



ThousandEyes Enterprise Agent の削除

ThousandEyes Enterprise ポータルで既存の ThousandEyes Enterprise Agent エントリを削除するには、[古いエージェント エントリの削除（Removing Old Agent Entries）]セクションの手順を参照してください。

DCNM のスイッチから既存の ThousandEyes Enterprise Agent アカウント グループ トークンを削除するには、次の手順を実行します。

Procedure

ステップ 1 Cisco DCNM Web UI から、**[制御（Control）] > [Fabric Builder]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。長方形のボックスは、各ファブリックを表します。

ステップ 2 ファブリックを選択し、**[アクション（Actions）]** ウィンドウの **[表形式のビュー（Tabular View）]** をクリックします。

[スイッチ（Switches）] タブが表示されます。

ステップ 3 適切なスイッチを選択して ThousandEyes Enterprise Agent を削除し、**[再生（Play）]** ボタン（コマンドの実行）をクリックします。

[デバイスでのスイッチ CLI の実行（Execute Switch CLIs on Devices）] ウィンドウが表示されます。

ステップ 4 [テンプレート（Template）] ドロップダウン リストから **[ThousandEyes_Agent_Identity_Delete]** を選択し、**[展開（Deploy）]** をクリックします。

ポリシーの表示と編集

Cisco DCNM は、一連のスイッチをグループ化する機能を提供し、グループに一連のアンダーレイ構成をプッシュできます。このリリースでは、ポリシーテンプレートを作成し、選択した複数のスイッチに適用できます。

ポリシーを表示、追加、展開、または編集するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

ステップ 2 使用可能なファブリックを選択し、**[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 [スイッチ（switches）] タブで複数のスイッチを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** をクリックします。

Note **[ポリシーの表示/編集（View/Edit Policies）]**は、MSD ファブリックに対して有効になっていません。

ポリシーの表示

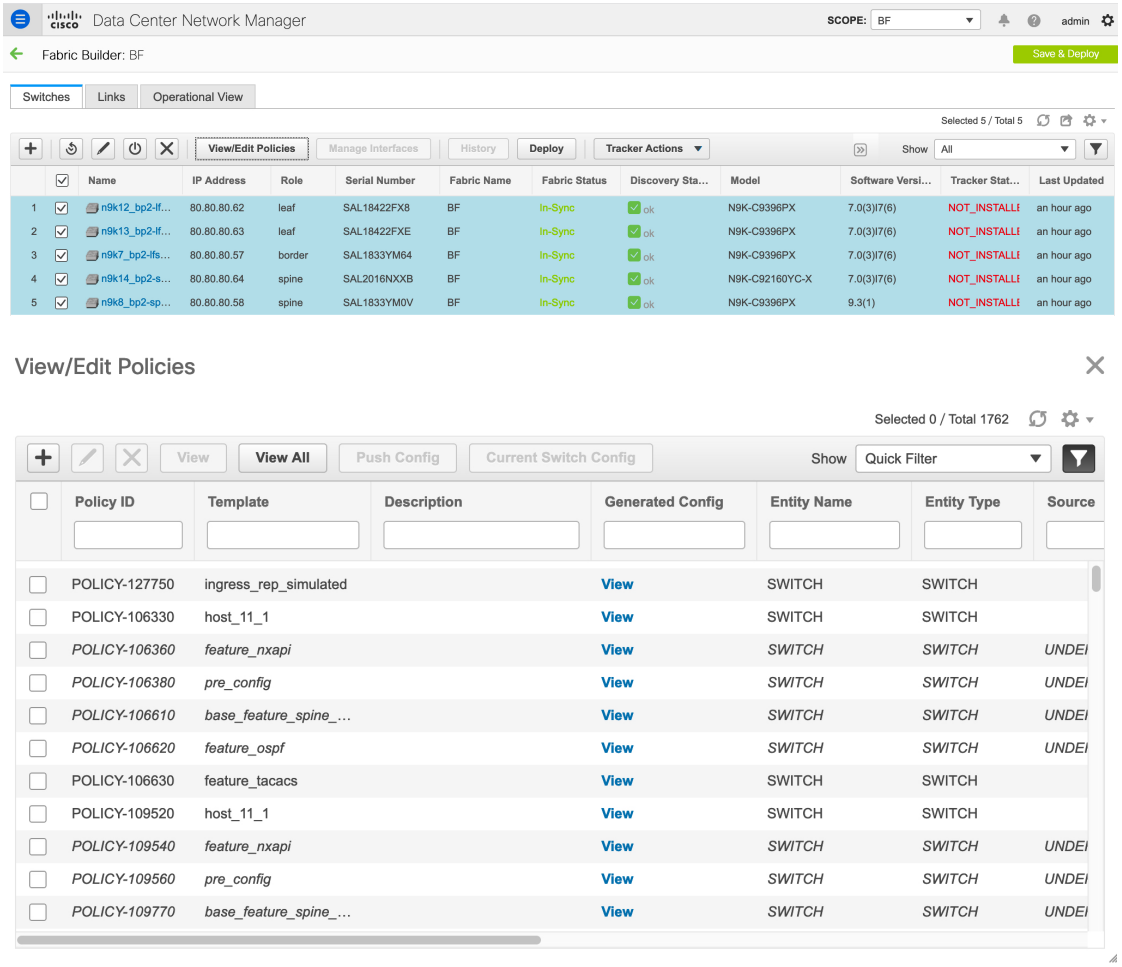
Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

ステップ 2 使用可能なファブリックを選択し、**[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 [スイッチ（switches）] タブで複数のスイッチを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** をクリックします。

ポリシーは、複数のスイッチのポリシー テーブルの表示または編集にリストされます。

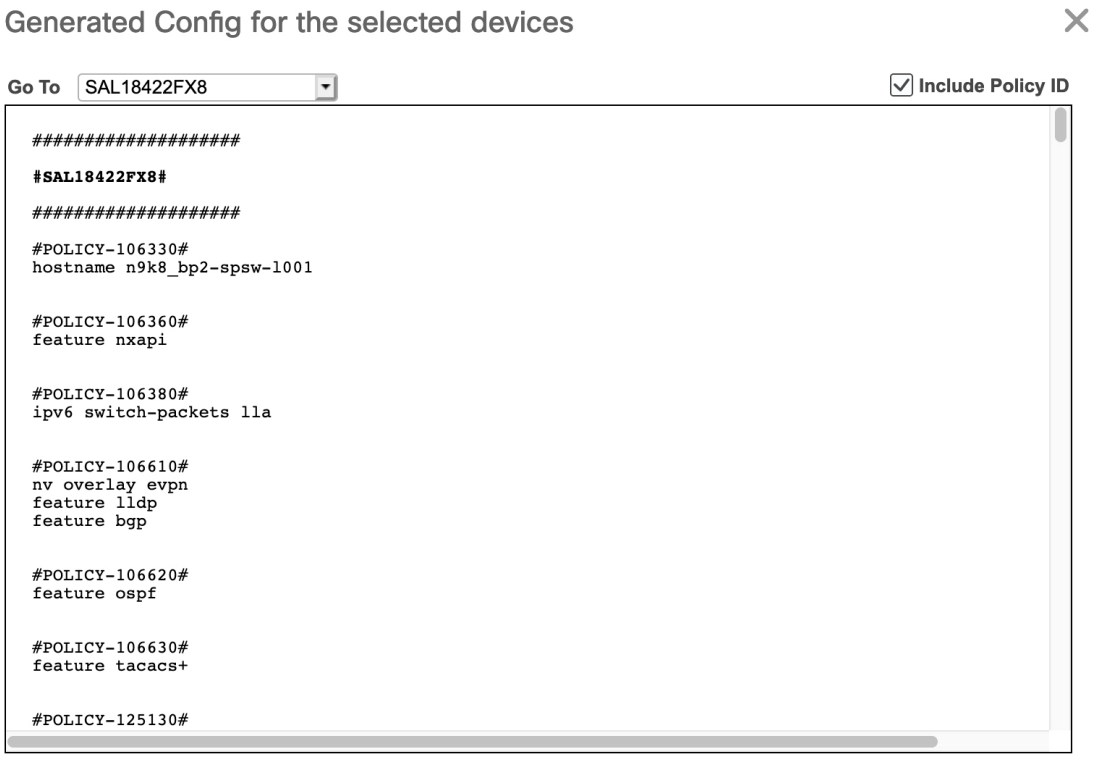


Note **[生成された構成（Generated Config）]** 列の下にある **[表示（View）]** ボタンにカーソルを合わせると、デバイスに対して生成された構成を表示できます。さらに、この列の下の検索フィールドに構成を入力して、ポリシーをフィルタリングできます。

ステップ 4 ポリシーを選択し、**[表示（View）]** ボタンをクリックしてその構成を表示します。

Note Python ポリシーは、ロジックを配置し、CLI ポリシーを制御するために使用されます。DCNM リリース 11.3(1) 以降、複数の CLI 子ポリシーが Python ポリシーごとに集約されます。

ステップ 5 **[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウで、**[すべてを表示（View All）]** をクリックして、ポリシーを使用してスイッチにプッシュされたすべての構成を表示します。



[移動先：（Go To:）] このドロップダウンリストからデバイスを選択して、その開始構成に移動します。

このオプションは、複数のデバイスのポリシーを表示する場合にのみ適用されます。

ポリシー ID を含める：（Include Policy ID:） すべてのポリシーのポリシー ID を表示するには、このチェックボックスをオンにします。デフォルトでは、このチェックボックスはオンです。

ポリシーの追加

Procedure

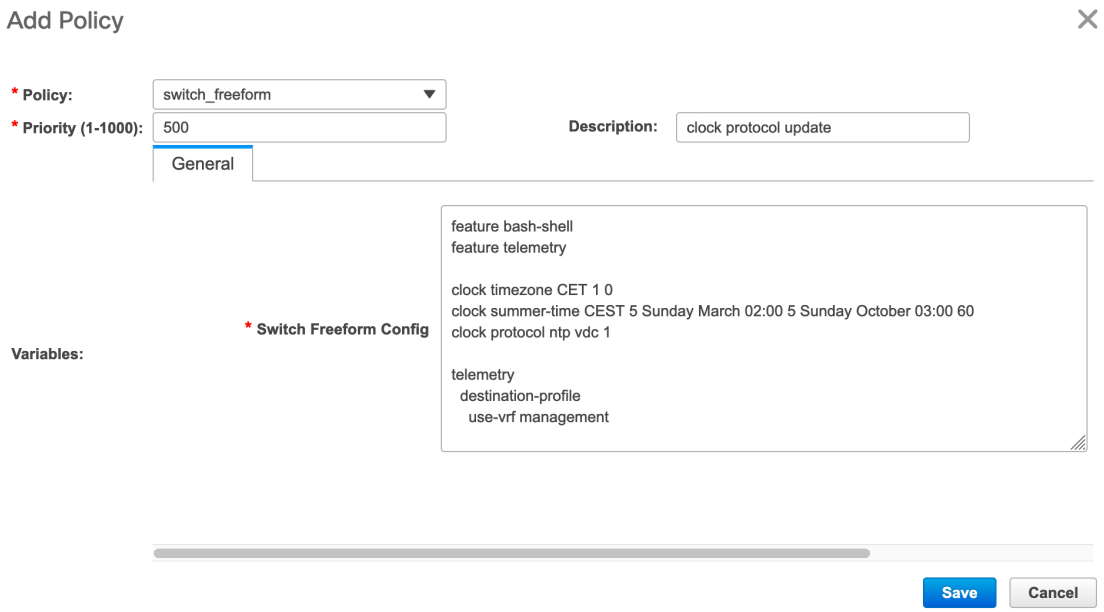
ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

ステップ 2 使用可能なファブリックを選択し、[表形式ビュー（Tabular view）] をクリックします。

ステップ 3 **[スイッチ（Switches）]** タブで 1 つまたは複数のスイッチを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** ボタンをクリックします。

ステップ 4 [追加（Add）] アイコンをクリックします。

ステップ 5 ポリシーテンプレートを選択し、必須パラメータ データを入力して、**[保存（Save）]** をクリックします。n 個のデバイスの選択に基づいて、各デバイスごとに PTI が追加されます。



[ポリシー（Policy]：このドロップダウンリストからポリシーを選択します。

[優先順位（Priority）]：ポリシーの優先順位を指定します。適用可能な値は 1 ～ 1000 です。デフォルト値は 500 です。**[優先順位（Priority）]** フィールドの数値が小さいほど、生成された構成およびPOAP スタートアップ構成の優先順位が高いことを意味します。たとえば、機能は 50、ルート マップは 100、vpc-domain は 200 です。

[説明（Description）]：（オプション）ポリシーの説明を指定します。このフィールドは、複数の自由形式ポリシーを差別化するために使用されます。**[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウに **[説明（Description）]** 列が追加され、説明に基づいてポリシーをフィルタリングまたは検索するために使用できます。

ポリシーの展開

Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

ステップ 2 使用可能なファブリックを選択し、[表形式ビュー（Tabular view）] をクリックします。

ステップ 3 [スイッチ（switches）] タブで複数のスイッチを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** ボタンをクリックします。

ステップ 4 複数のポリシーを選択し、> **[構成をプッシュ（Push Config）]** をクリックします。選択した PTI の構成がスイッチのグループにプッシュされます。

- 外部ファブリックがモニタ モードの場合、**[構成をプッシュ（Push Config）]** オプションは無効になっています。
- このオプションは、ファブリックが凍結モードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。

ポリシーの編集

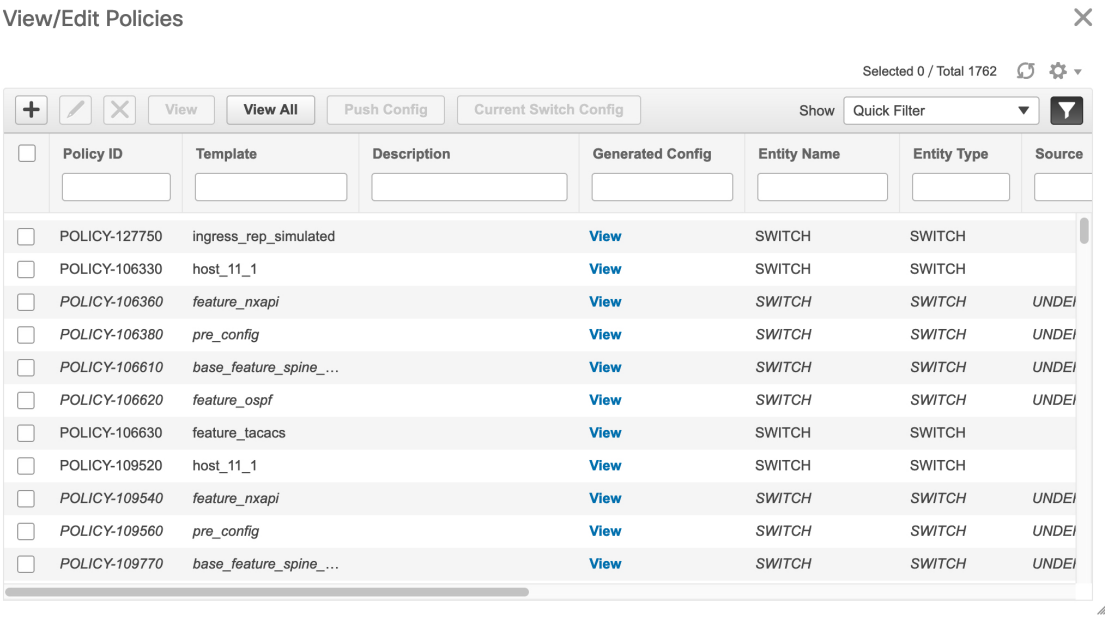
Note 複数のポリシーの編集はサポートされていません。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

ステップ 2 使用可能なファブリックを選択し、**[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 [スイッチ（switches）] タブで複数のスイッチを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** ボタンをクリックします。

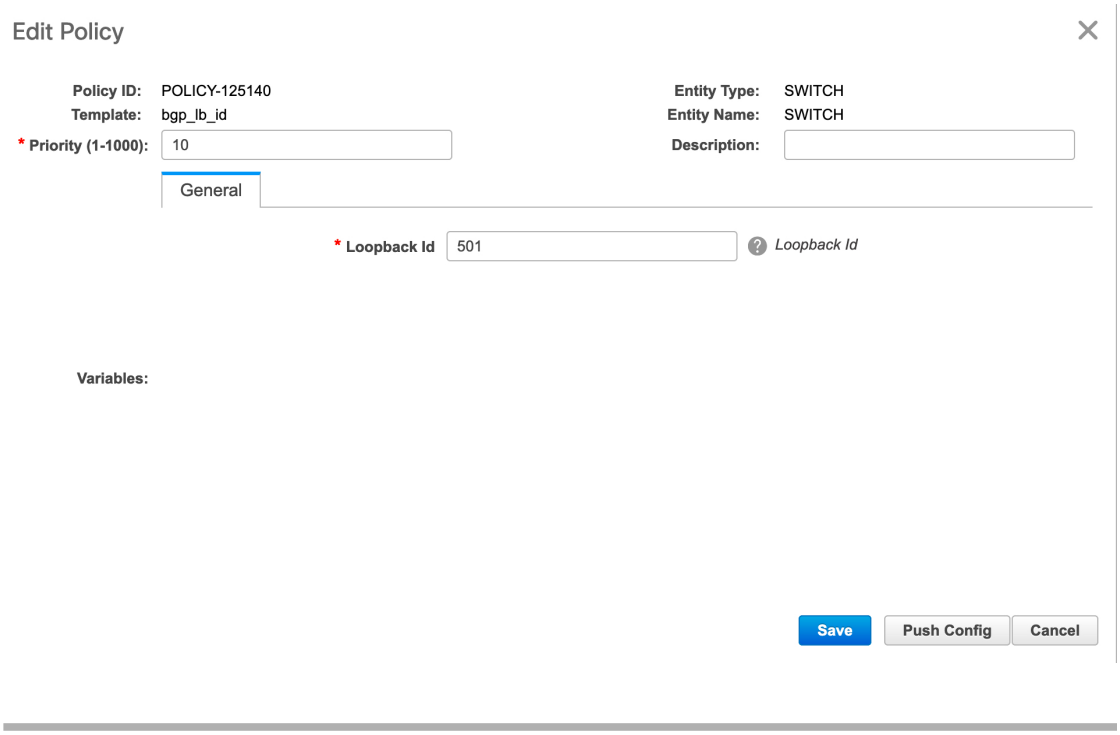


Note イタリック体のフォントのポリシーは編集できません。これらのポリシーの **[編集可能（Editable）]** 列と **[削除済みマーク（Mark Deleted）]** 列の値は **[false]** です。

ステップ 4 PTI を選択し、**[編集（Edit）]** をクリックして必要なデータを変更し、**[保存（Save）]** をクリックして PTI を保存します。

ステップ 5 PTI を選択し、**[編集（Edit）]** をクリックして必要なデータを変更し、>**[構成をプッシュ（Push Config）]** をクリックしてポリシー構成をデバイスにプッシュします。

Note
- このオプションは、ファブリックが凍結モードの場合、つまり、ファブリックで展開を無効にしている場合はグレー表示されます。
- Python ポリシーの構成をプッシュすると、Warning（注意）が表示されます。
- mark-deleted ポリシーを編集、削除、または構成をプッシュすると、Warning（注意）が表示されます。mark-deleted ポリシーは、**[削除済みマーク（Mark Deleted）]** 列で **[true]** に設定されています。**[削除済みマーク（Mark Deleted）]** ポリシーのスイッチの自由形式の子ポリシーが **[ポリシーの表示/編集（View/Edit Policies）]** ダイアログボックスに表示されます。**Python** の switch_freeform ポリシーのみを編集できます。**Template_CLI** switch_freeform_config ポリシーは編集できません。



現在のスイッチ構成

Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

ステップ 2 使用可能なファブリックを選択し、**[表形式ビュー（Tabular view）]** をクリックします。

ステップ 3 [スイッチ（switches）] タブで複数のスイッチを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** をクリックします。

ステップ 4 **[現在のスイッチ構成（Current Switch Config）]** をクリックします。

[実行構成（Running Config）] ダイアログ ボックスに現在のスイッチ構成が表示されます。

Note ユーザーロールがデフォルトでプロンプトの有効化にアクセスできない場合、**[現在のスイッチ構成（Current Switch Config）]** をクリックしても、Cisco CSR 1000v の実行構成は表示されません。

認証キーの取得

3DES 暗号化 OSPF 認証キーの取得

1. スイッチに SSH 接続します。
2. 未使用のスイッチインターフェイスで、次を有効にします。

```
config terminal
    feature ospf
    interface Ethernet1/1
       no switchport
       ip ospf message-digest-key 127 md5 ospfAuth
```

この例では、**ospfAuth** は暗号化されていないパスワードです。

（注） このステップ 2 は、新しいキーを設定する場合に必要です。

3. **show run interface Ethernet1/1** コマンドを入力してパスワードを取得します。

```
Switch # show run interface Ethernet1/1
   interface Ethernet1/1
     no switchport
     ip ospf message-digest key 127 md5 3 sd8478f4fsw4f4w34sd8478fsdfw
     no shutdown
```

md5 3 の後の文字のシーケンスは、暗号化されたパスワードです。

4. **[OSPF 認証キー（OSPF Authentication Key）]** フィールドの暗号化されたパスワードを更新します。

暗号化された IS-IS 認証キーの取得

キーを取得するには、スイッチにアクセスできる必要があります。

1. スイッチに SSH 接続します。
2. 一時キーチェーンを作成します。

```
config terminal
   key chain isis
   key 127
   key-string isisAuth
```

この例では、**isisAuth** はプレーンテキスト パスワードです。これは、CLI が受け入れられた後に Cisco タイプ 7 パスワードに変換されます。

3. **show run | section "key chain"** コマンドを入力してパスワードを取得します。

```
key chain isis
   key 127
       key-string 7 071b245f5a
```

key-string 7 の後の文字のシーケンスは、暗号化されたパスワードです。設定を保存します。

4. [OSPF 認証キー（OSPF Authentication Key）] フィールドの暗号化されたパスワードを更新します。
5. ステップ 2 で行った不要な設定を削除します。

3DES 暗号化 BGP 認証キーの取得

1. スイッチに SSH 接続し、存在しないネイバーの BGP 設定を有効にします。

（注） 存在しないネイバー設定は、パスワードを取得するための一時的な BGP ネイバー設定です。

```
router bgp
   neighbor 10.2.0.2 remote-as 65000
   password bgpAuth
```

この例では、**bgpAuth** は暗号化されていないパスワードです。

2. パスワードを取得するには、show run bgp コマンドを入力します。サンプル出力：

```
neighbor 10.2.0.2
   remote-as 65000
   password 3 sd8478fswerdfw3434fsw4f4w34sdsd8478fswerdfw3434fsw4f4w3
```

パスワード 3 の後の文字のシーケンスは、暗号化されたパスワードです。

3. **[BGP 認証キー（BGP Authentication Key）]** フィールドの暗号化されたパスワードを更新します。
4. BGP ネイバー設定を削除します。

暗号化された BFD 認証キーの取得

1. スイッチに SSH 接続します。
2. 未使用のスイッチインターフェイスで、次を有効にします。

```
switch# config terminal
switch(config)# int e1/1
switch(config-if)# bfd authentication keyed-SHA1 key-id 100 key cisco123
```

この例では、**cisco123** は暗号化されていないパスワードで、キー ID は **100** です。

（注） このステップ 2 は、新しいキーを設定する場合に必要です。

3. キーを取得するには、**show running-config interface** コマンドを入力します。

```
switch# show running-config interface Ethernet1/1

interface Ethernet1/1
description connected-to- switch-Ethernet1/1
no switchport
mtu 9216
bfd authentication Keyed-SHA1 key-id 100 hex-key 636973636F313233
no ip redirects
ip address 10.4.0.6/30
no ipv6 redirects
ip ospf network point-to-point
ip router ospf 100 area 0.0.0.0
no shutdown
```

BFD キー ID は **100** で、暗号化キーは **636973636F313233** です。

4. **[BFD 認証キー（BFD Authentication Key ID）]** フィールドと **[BFD 認証キー（BFD Authentication Key）]** フィールドのキー ID とキーを更新します。

カスタム メンテナンス モードのプロファイル ポリシー

DCNM を使用してスイッチをメンテナンス モードにすると、メンテナンス モード プロファイルでは、BGP および OSPF 分離 CLI の固定セットのみが構成されます。Cisco DCNM リリース 11.3(1) 以降では、メンテナンス モードおよび通常モード プロファイル用にカスタマイズされた構成で **[custom_maintenance_mode_profile]** PTI を作成し、PTI をスイッチに展開してから、スイッチをメンテナンス モードに移行できます。

カスタム メンテナンス モードのプロファイル ポリシーの作成と展開

Procedure

ステップ 1 **[制御（Control）]** > **[ファブリック ビルダ（Fabric Builder）]** を選択し、**[表形式ビュー（Tabular View）]** をクリックして、**[名前（Name）]** 列でスイッチを選択する、または、**[制御（Control）]** > **[ファブリック ビルダ（Fabric Builder）]** を選択してスイッチを右クリックします。

ステップ 2 **[ポリシーの表示/編集（View/Edit Policies）]** をクリックして、**[+]** をクリックして新しいポリシーを追加します。**[ポリシーの追加（Add Policy）]** ウィンドウが表示されます。

ステップ 3 **[ポリシー（Policy）]** ドロップダウンリストから **[custom_maintenance_mode_profile]** を選択します。

ステップ 4 **[メンテナンス モード プロファイル コンテンツ（Maintenance mode profile contents）]** に、必要な構成 CLI を入力します。

例：

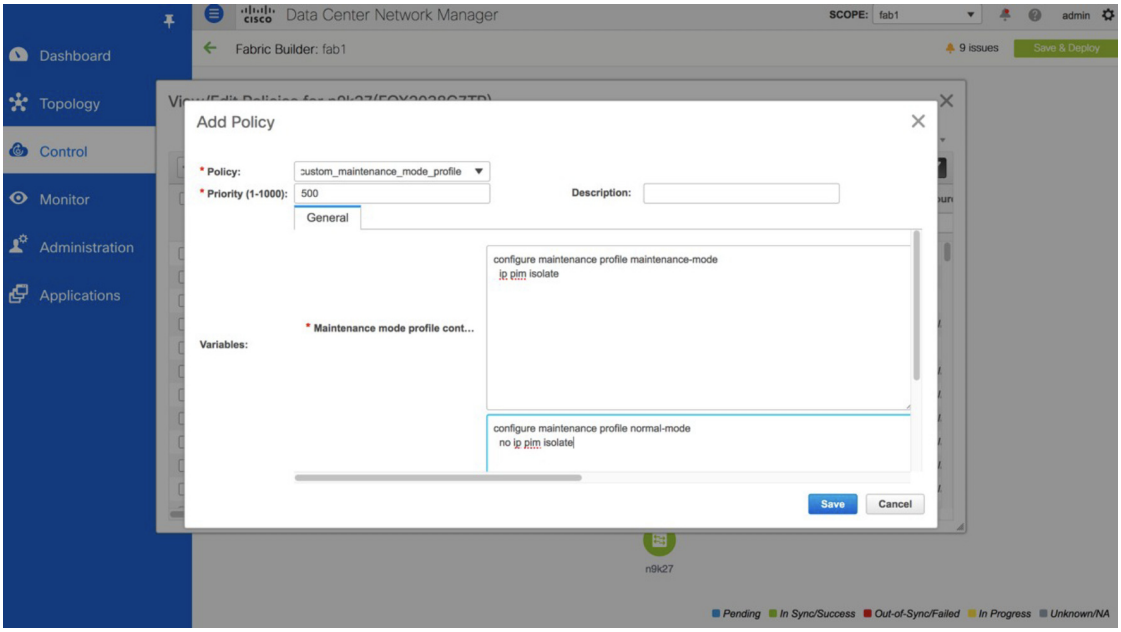
```
configure maintenance profile maintenance-mode
ip pim isolate
```

[通常モード プロファイル コンテンツ（Normal mode profile contents）] に、必要な構成 CLI を入力します。

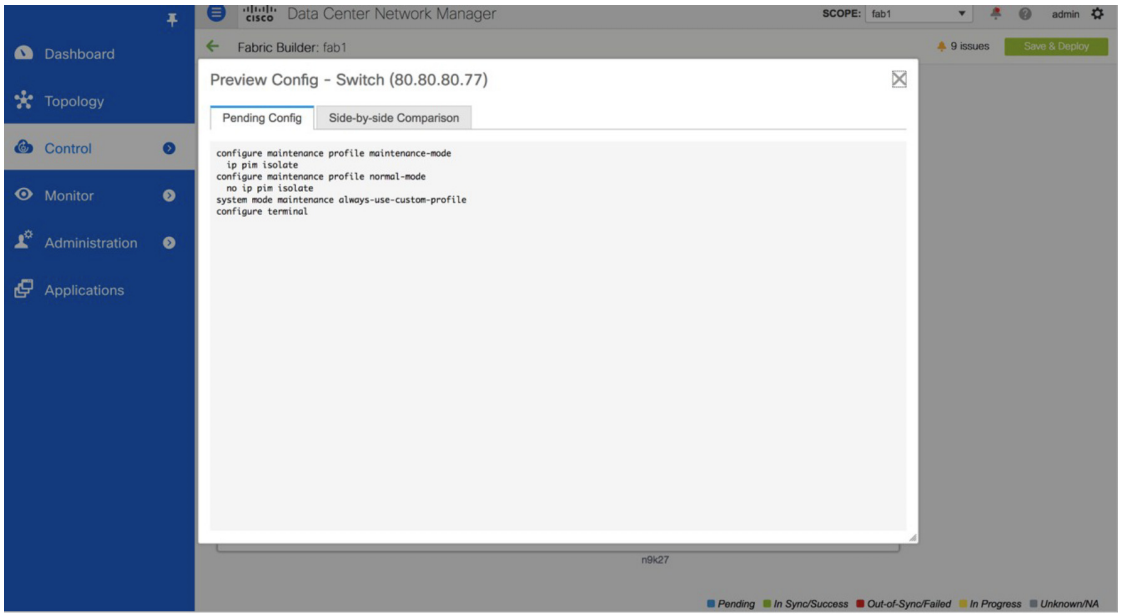
例：

```
configure maintenance profile normal-mode
no ip pim isolate
```

ステップ 5 [保存（Save）] をクリックします。



ステップ 6 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウでスイッチを右クリックし、**[構成の展開（Deploy Config）]** を選択します。**[保留中の構成（Pending Config）]** ウィンドウで構成を確認し、構成をスイッチに展開します。



ステップ 7 次に、スイッチを右クリックし、**[モード（Modes）] > [メンテナンス モード（Maintenance Mode）]** を選択して、スイッチをメンテナンス モードに移動します。

カスタム メンテナンス モード のプロファイル ポリシーの削除

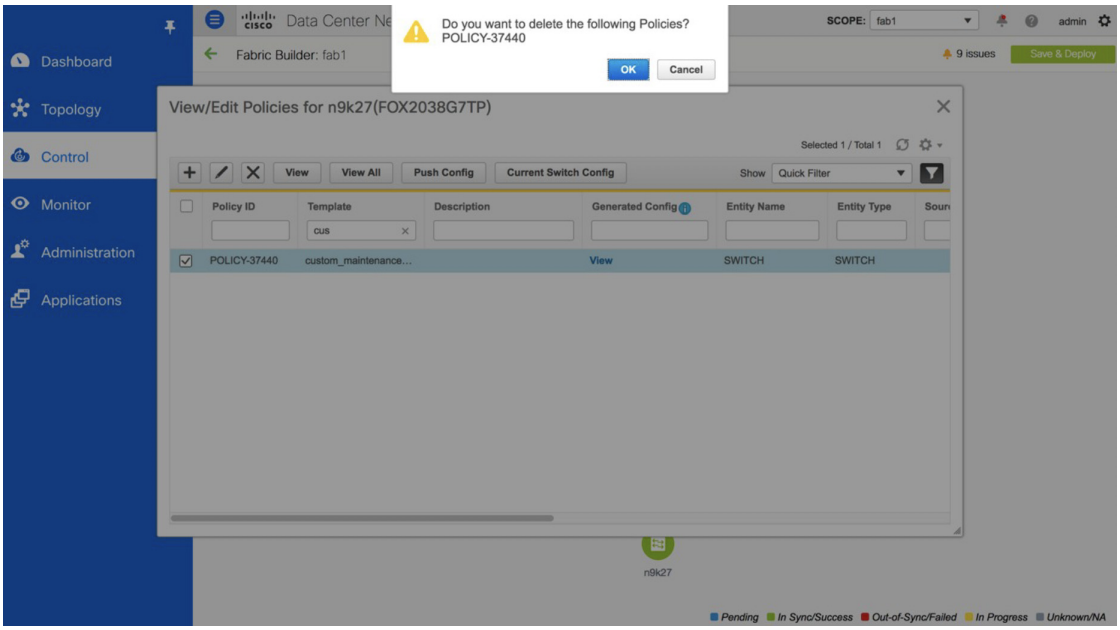
Procedure

ステップ 1 カスタム メンテナンス モード プロファイル ポリシーを削除する前に、スイッチをアクティブ/動作モードまたは通常モードに移行する必要があります。これを行うには、**[ファブリック ビルダ（Fabric Builder）]** ウィンドウでスイッチを右クリックし、**[モード（Modes）] > [アクティブ/（Active/）] > [動作モード（Operational Mode）]** の順に選択します。

ステップ 2 スイッチがアクティブ/動作モードまたは通常モードに移動した後、**[ファブリック ビルダ（Fabric Builder）]** ウィンドウで **[表形式ビュー（Tabular View）]** をクリックし、**[名前（Name）]** 列でスイッチを選択するか、**[ファブリック ビルダ（Fabric Builder）]** ウィンドウでスイッチを右クリックします。

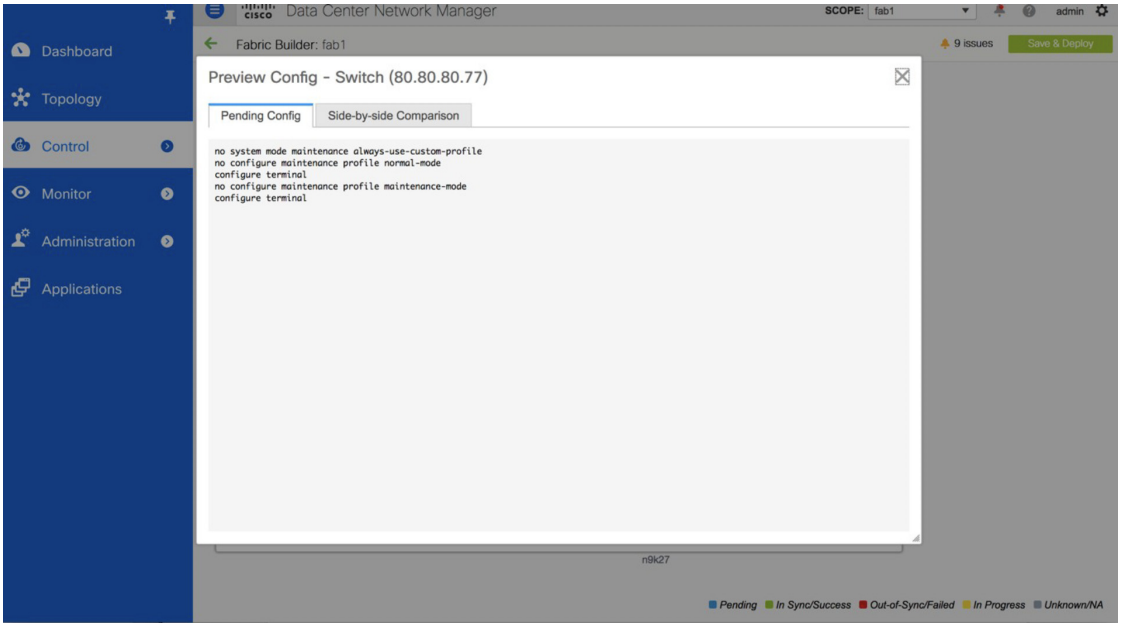
ステップ 3 **[ポリシーの表示/編集（View/Edit Policies）]** をクリックし、削除する必要がある **[custom_maintenance_mode_profile]** ポリシーを選択します。

ステップ 4 **[X]** をクリックしてポリシーを削除します。



ステップ 5 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウでスイッチを右クリックし、**[構成の展開（Deploy Config）]** を選択します。**[保留中の構成（Pending Config）]** ウィンドウで構成を確認し、構成をスイッチに展開します。

```
no system mode maintenance always-use-custom-profile
no configure maintenance profile normal-mode
no configure maintenance profile maintenance-mode
configure terminal
```



返品許可（RMA）

ここでは、Cisco DCNM Easy ファブリック モードを使用する場合に、ファブリック内の物理スイッチを交換する方法について説明します。

前提条件

- スイッチの交換時に、中断を最小限に抑えてファブリックが稼働していることを確認します。
- POAP RMA フローを使用するには、ファブリックをブートストラップ（POAP）用に設定します。
- 必要に応じて、保存と展開を複数回実行し、FEX が展開されているスイッチの RMA の FEX 構成をコピーします。

注意事項と制約事項

- スイッチを交換するには、ファブリックから古いスイッチを取り外し、ファブリック内の新しいスイッチを検出します。たとえば、Cisco Nexus 9300-EX スイッチを Cisco Nexus 9300-FX スイッチに交換する場合は、ファブリックから 9300-EX スイッチを取り外し、同じファブリック内の 9300-FX スイッチを検出します。
- Cisco Nexus 7000 シリーズ スイッチをアップグレードする前に GIR が有効になっている場合、DCNM は、DCNM RMA 手順の開始時に **system mode maintenance** コマンドをスイッチにプッシュします。このコマンドは、デフォルトのメンテナンス モード プロファイルに存在する設定をスイッチに適用します。Cisco Nexus 7000 シリーズ スイッチでのグレースフル挿入および取り外し（GIR）の実行の詳細については、「GIRの構成」を参照してください。

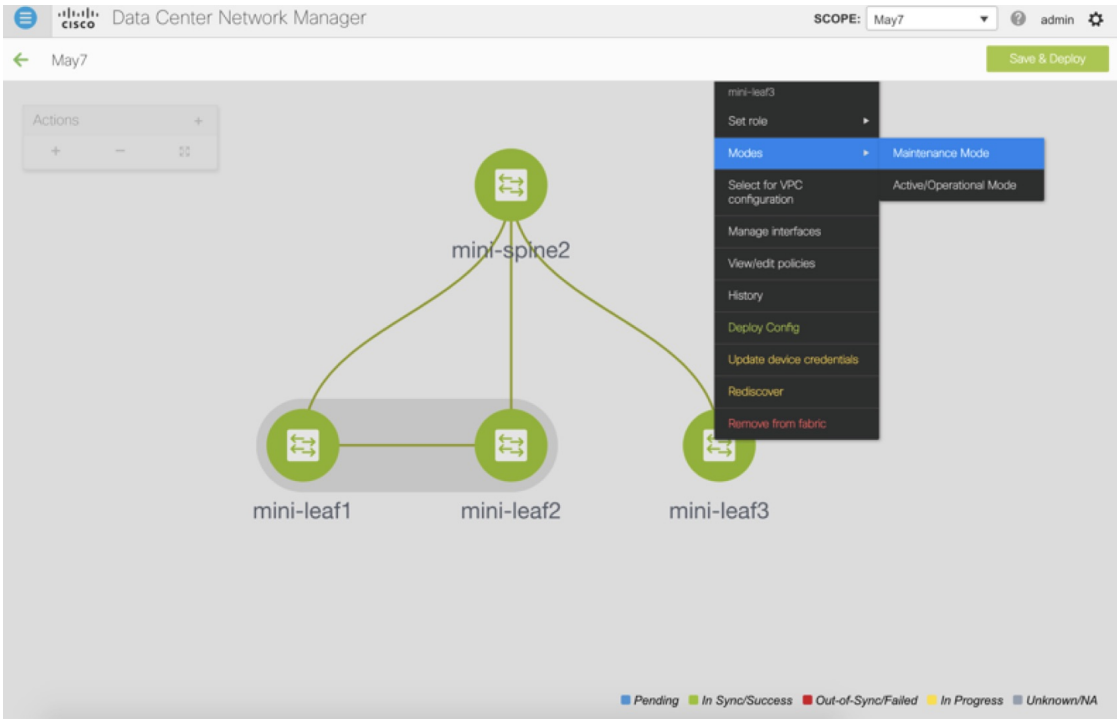
POAP RMA フロー

Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

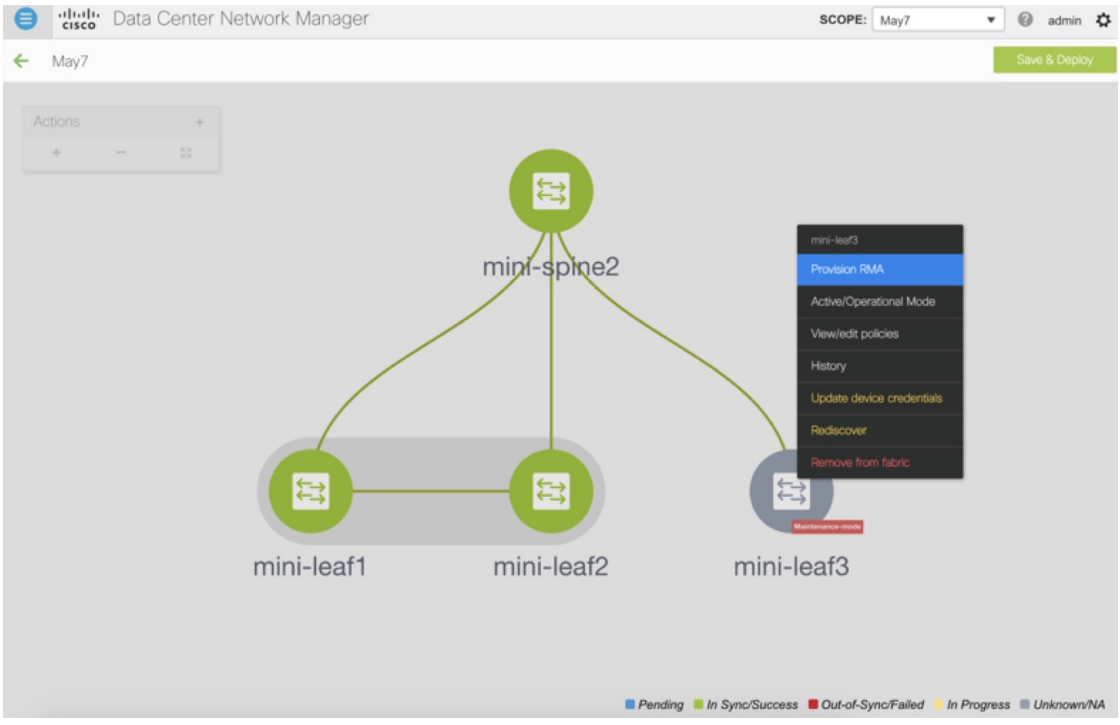
ステップ 2 RMA を実行するファブリックをクリックします。

ステップ 3 デバイスをメンテナンス モードにします。デバイスをメンテナンス モードに移行するには、デバイスで右クリックし、**[モード（Modes）] > [メンテナンス モード（Maintenance Mode）]** を選択します。

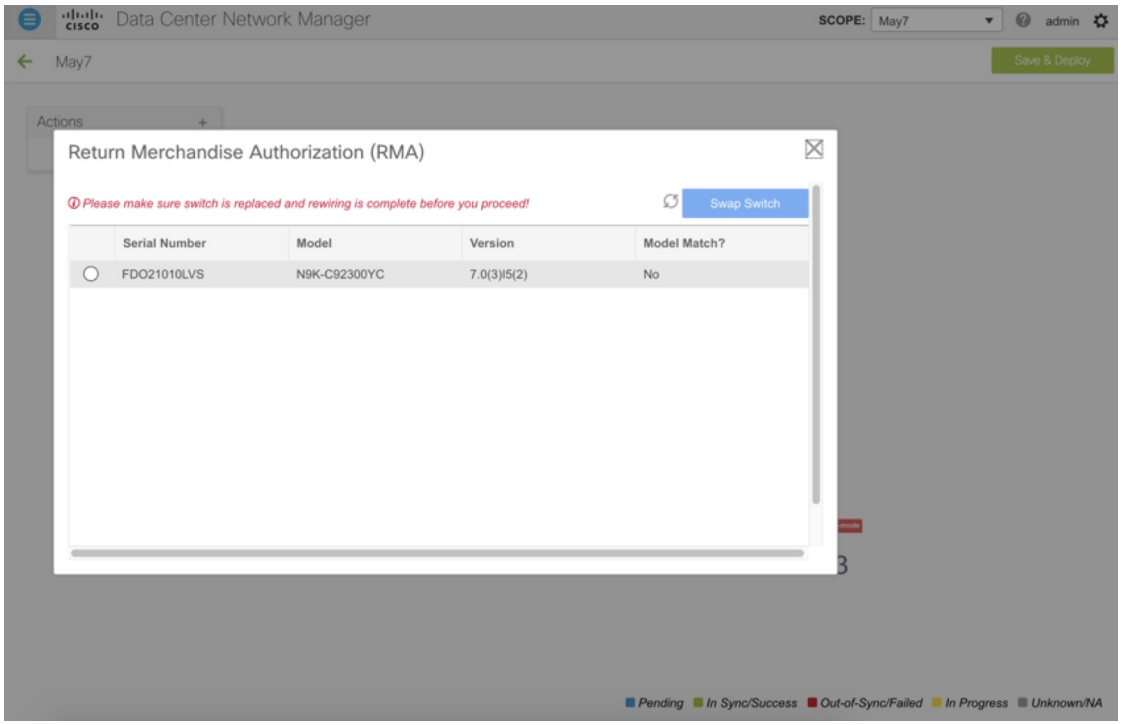


ステップ 4 ネットワークのデバイスを物理的に交換します。物理接続は、交換用スイッチの元のスイッチと同じ場所で行う必要があります。

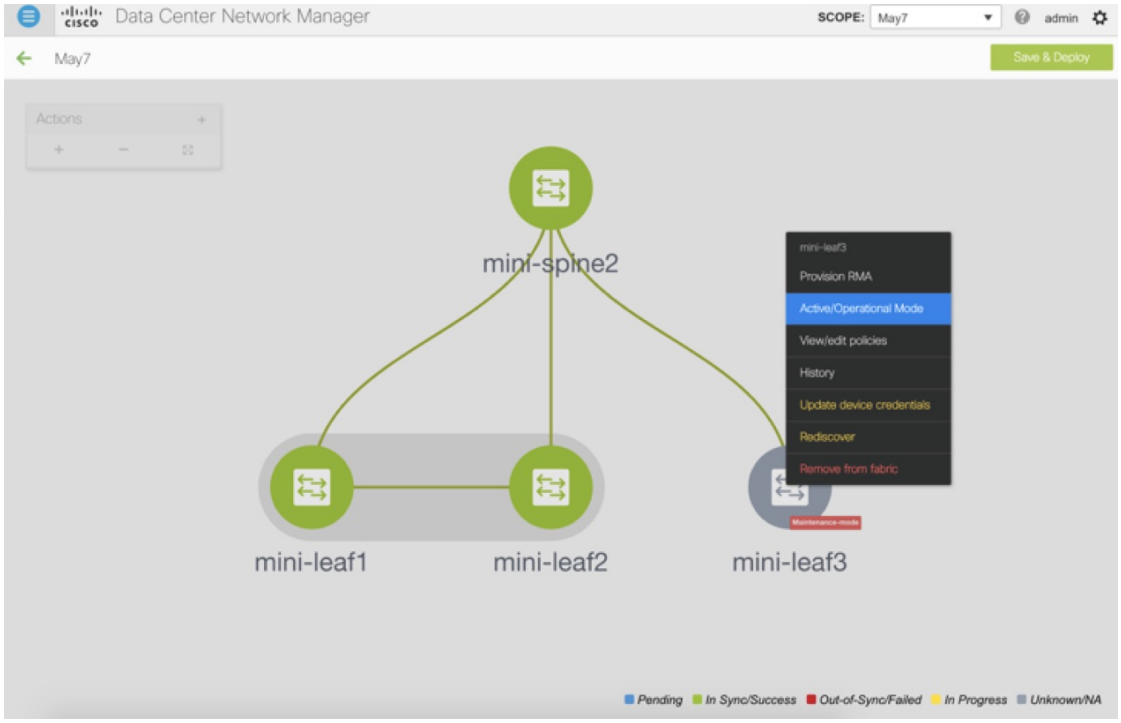
ステップ 5 RMA フローをプロビジョニングし、交換用デバイスを選択します。



ステップ 6 [RMA のプロビジョニング（Provision RMA）] UIには、電源がオンになってから 5ー10 分後に交換デバイスが表示されます。



ステップ 7 正しい交換用デバイスを選択し、**[スイッチの交換（Swap Switch）]** をクリックします。これにより、そのデバイスの完全な「予想される」構成で POAP が開始されます。合計 POAP 時間は、通常、約 10 ～ 15 分です。

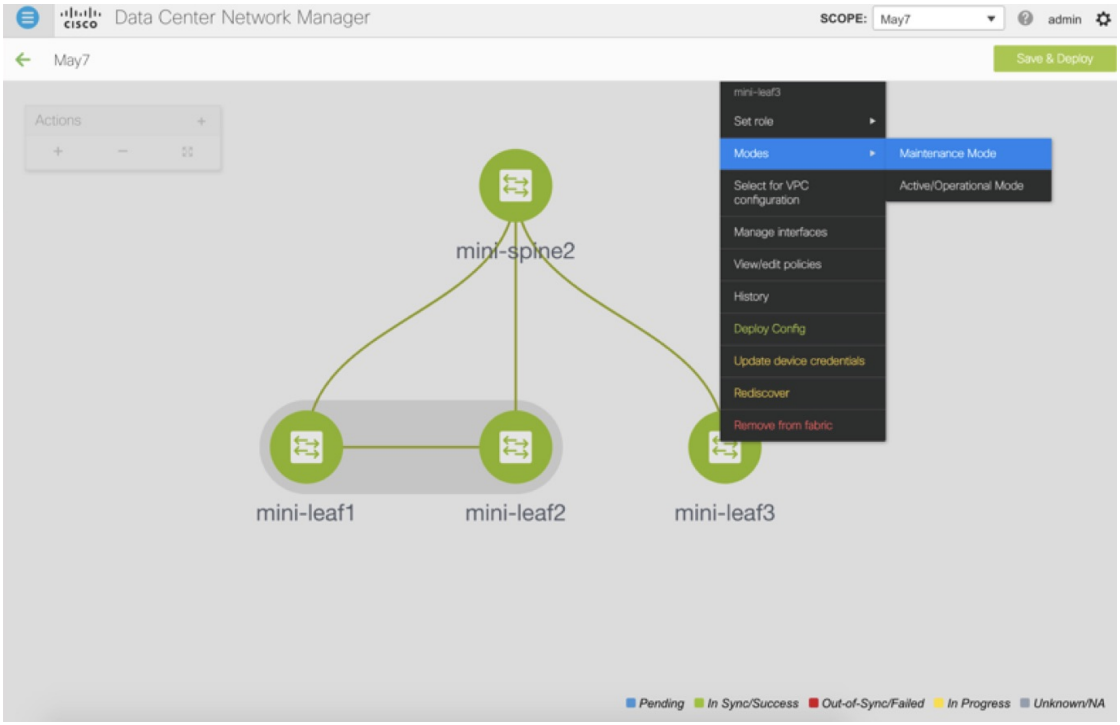


手動 RMA フロー

このフローは、最初の Cisco DCNM 11.0(1) リリースで *IPv6* のみ である場合など、「ブートストラップ」が不可能な（または望ましくない）場合に使用します。

Procedure

ステップ 1 デバイスをメンテナンス モード（オプション）にします。

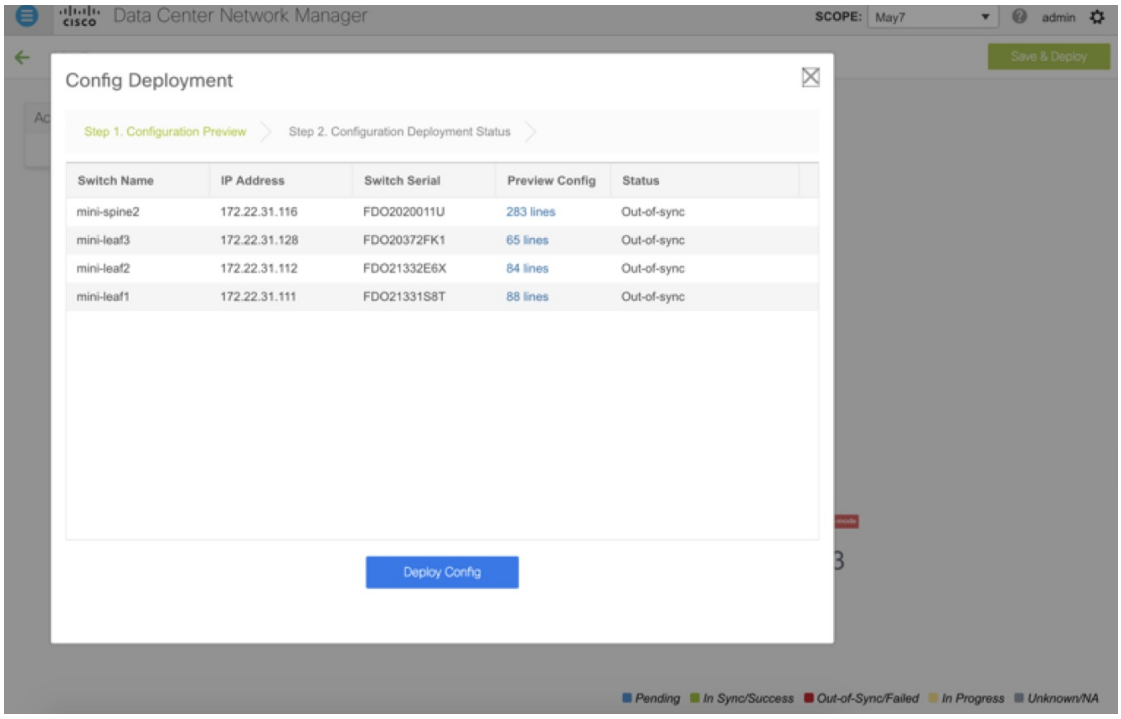


ステップ 2 ネットワーク内のデバイスを物理的に交換します。

ステップ 3 コンソールからログインし、管理 IP とクレデンシャルを設定します。

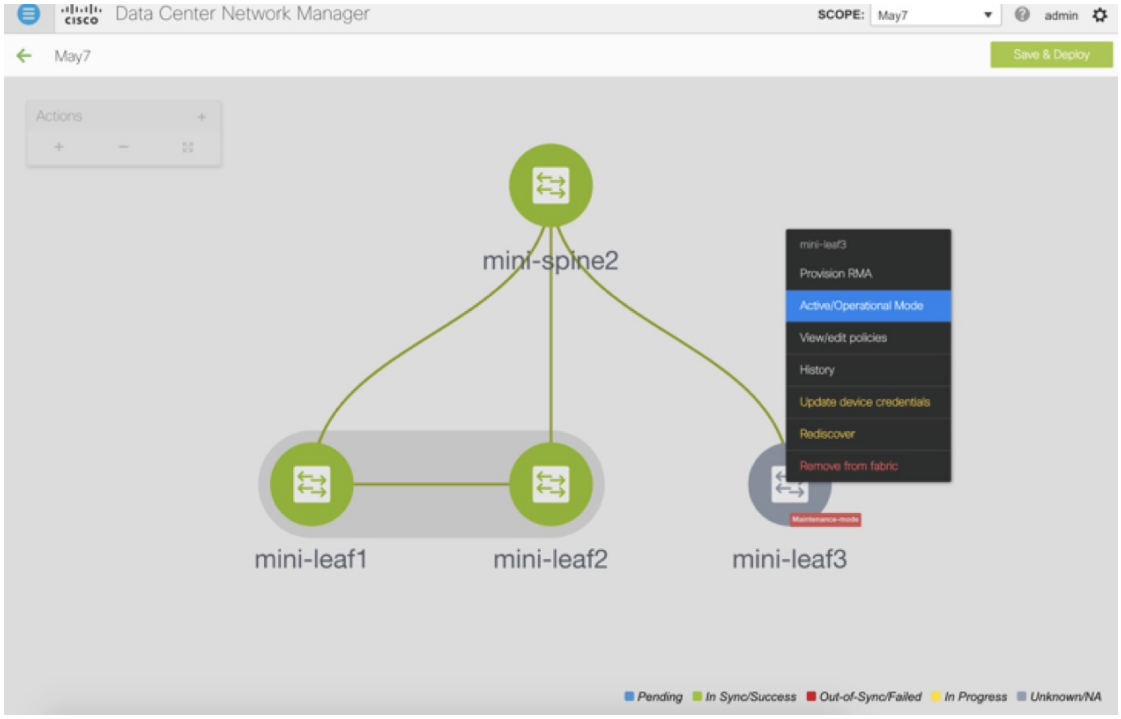
ステップ 4 Cisco DCNM は新しいデバイスを再検出します（または、**[検出（Discovery）] > [再検出（Rediscover）]** を手動で選択できます）。

ステップ 5 **[展開（Deploy）]** を使用して、必要な設定を展開します。



ステップ 6 設定によっては、ブレイクアウト ポートまたは FEX ポートが使用中の場合、設定を完全に復元するために再度展開する必要があります。

ステップ 7 展開が正常に完了し、デバイスが「同期中」になったら、デバイスを通常モードに戻す必要があります。



カスタム メンテナンス モード のプロファイル ポリシー

ローカル認証を持つユーザの RMA

Note このタスクは、非 POAP スイッチにのみ適用されます。

ローカル認証を持つユーザの RMA を実行するには、次の手順を使用します。

Procedure

ステップ 1 新しいスイッチがオンラインになったら、スイッチに SSH 接続し、「username」コマンドを使用してクリア テキスト パスワードでローカル ユーザ パスワードをリセットします。これは、SNMP パスワードを再同期するために必要であり、転送不可能な形式で構成ファイルに保存されます。

ステップ 2 RMA が完了するまで待ちます。

ステップ 3 スイッチの新しい SNMP MD5 キーを使用して、スイッチの Cisco DCNM switch_snmp_user ポリシーを更新します。

インターフェイス

[インターフェイス（Interfaces）] オプションは、スイッチで検出されたすべてのインターフェイス、仮想ポート チャネル（vPC）、およびデバイスに存在しない目的のインターフェイスを表示します。

次の機能を使用できます。

- ポート チャネル、vPC、 Straight-through FEX、Active-Active FEX、ループバック、およびサブインターフェイスを作成、展開、表示、編集、および削除します。

（注）

- 次の機能は、Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x)イメージを使用したスイッチのブラウンフィールド移行ではサポートされていません。
  - X9500 ラインカードを搭載した Cisco Nexus 9300 シリーズ スイッチおよびCisco Nexus 9500 シリーズ スイッチ以外のスイッチでの FEX
  - AA-FEX

  FEX のプラットフォーム サポートについては、プラットフォームと NX-OS のマニュアルを参照して、機能の互換性を確認してください。
- ファブリック内リンクやファブリック間リンクなどのファブリック リンクに関連付けられているインターフェイスを編集するには、リンクに関連付けられたインターフェイスの編集 （319 ページ） を参照してください。
- **flowcontrol** または **priority-flow-control** の設定は、HIF ポートまたはメンバーとしての HIF ポートではサポートされません。

- Cisco Cloud Services Router 1000v シリーズ（Cisco CSR 1000v シリーズ）のトンネル インターフェイスを作成します。
- ブレイクアウト ポートとアンブレイクアウト ポートを作成します。
- インターフェイスをシャットダウンして起動します。
- ポートを再検出し、インターフェイスの設定履歴を表示します。
- インターフェイスおよび vPC にホストポリシーを適用します。たとえば、int_trunk_host_11_1、int_access_host_11_1 などです。
- インターフェイスの情報（管理ステータス、動作ステータス、理由、ポリシー、速度、MTU、モード、VLAN、IP/プレフィックス、VRF、ポートチャネル、インターフェイスのネイバーなど）を表示します。

（注）

- **[ネイバー（Neighbor）]** 列には、検出された接続スイッチ、インテント リンク、および Virtual Machine Manager（VMM）接続の詳細が表示されます。対応するスイッチをクリックすると、その **[スイッチ（Switch）]** のダッシュボードに移動できます。ただし、インテント リンクと VMM リンクはハイパーリンクされておらず、対応する **[スイッチ（Switch）]** ダッシュボードに移動できません。
- [名前（Name）] 列のグラフ アイコンをクリックして、過去 24 時間のインターフェイス パフォーマンス チャートを表示します。ただし、オーバーレイ ネットワークに関連付けられている VLAN インターフェイスのパフォーマンス データは、このグラフには表示されないことに注意してください。

[ステータス（Status）] 列に、次のいずれかのステータスが表示されます。

- 青：保留中
- 緑：同期/成功
- 赤: 非同期/失敗
- 黄色：進行中
- グレー：不明/ NA

- インターフェイスがアウトオブバンドで作成された場合、このインターフェイスを削除するには、ファブリックの再同期を実行するか、構成コンプライアンスのポーリングを待機する必要があります。そうしないと、Config Compliance は正しい差分を生成しません。

ただし、ASR 9000 シリーズ ルータおよび Arista スイッチのインターフェイスを追加または編集することはできません。

特定のフィールド（[デバイス名（Device Name）]など）の情報をフィルタリングおよび表示できます。次の表で、このページに表示されるボタンを説明します。

（注）

- 適切な vPC ペア構成を含む、インターフェイス オプションから展開する前に、適切な構成がファブリック ビルダ オプションを介して展開されていることを確認します。ファブリックの展開の前にインターフェイスを追加または編集すると、デバイスで構成が失敗することがあります。
- ファブリック ビルダ トポロジ画面からインターフェイスを管理することもできます。スイッチを右クリックし、[インターフェイスの管理（Manage Interfaces）] オプションを選択します。スイッチごとにインターフェイスを管理できます。スイッチが vPC ペアの一部である場合、両方のピアからのインターフェイスがページに表示されます。
- インターフェイス マネージャから構成を展開する前に、vPCペアリングを含むアンダーレイをファブリックに展開します。

フィールド	説明
追加（Add）	ポートチャネル、vPC、Straight-through FEX、Active-Active FEX、ループバックおよびサブインターフェイスなどの論理インターフェイスを追加できます。
ブレークアウト、ブレークアウト解除	ブレークアウト状態のインターフェイスまたはブレークアウト解除インターフェイスを、ブレークアウトにできます。
編集	インターフェイスに関連付けられているポリシーを編集および変更できます。
削除	[インターフェイス（Interfaces）] 画面から作成された論理インターフェイスを削除できます。オーバーレイとアンダーレイからアタッチされたポリシーを持つインターフェイスは削除できません。
シャットダウンなし	インターフェイスを有効にできます（シャットダウンまたは管理起動なし）。
シャットダウン	インターフェイスをシャットダウンできます。
表示する	interface show コマンドを表示できます。show コマンドを使用するには、テンプレート ライブラリに show テンプレートが必要です。
再検出	選択したインターフェイスのコンプライアンス ステータスを再検出または再計算できます。

フィールド	説明
インターフェイス履歴	インターフェイス展開履歴の詳細を表示できます。
展開	保存したインターフェイス設定を展開または再展開できます。

Cisco DCNM リリース 11.4(1) 以降で、**[インターフェイス（Interfaces）]** ウィンドウでサポートされるさまざまなユーザーロールとこれらのロールの操作について、次の表で説明します。

操作	ユーザ ロール		
	network-admin	**network-operator**	**network-stager**
追加	保存、プレビュー、展開	ブロック	保存、プレビュー
サブ会議	サポート対象	ブロック済み	ブロック済み
ブレークアウト解除	サポート対象	ブロック済み	ブロック済み
編集	保存、プレビュー、展開	プレビュー	保存、プレビュー
削除	保存、プレビュー、展開	ブロック	保存、プレビュー
シャットダウン	保存、プレビュー、展開	ブロック	保存、プレビュー
シャットダウンなし	保存、プレビュー、展開	ブロック	保存、プレビュー
表示	サポート対象	サポート対象	サポート対象
再検出	サポート対象	サポート対象	サポート対象
展開	プレビュー、展開	ブロック済み	ブロック済み

次の表に、Cisco DCNM リリース 11.5(1) からの **[インターフェイス（Interfaces）]** ウィンドウのホスト側ポートでの新しいユーザーロール access-admin 操作のサポートを示します。

操作	ユーザ ロール
	Role: access-admin
追加	保存、プレビュー、展開
サブ会議	ブロック済み
ブレークアウト解除	ブロック済み

操作	ユーザ ロール
	Role: access-admin
編集	保存、プレビュー、展開 （注） Access-admin ユーザー ロールは、Easy ファブリックのファブリック間リンクやファブリック内リンクなどのリンク ポリシーに関連付けられたインターフェイスを編集できません。このユーザーロールは、LAN クラシック ファブリックのインターフェイスを編集できます。
削除	保存、プレビュー、展開
シャットダウン	保存、プレビュー、展開
シャットダウンなし	保存、プレビュー、展開
表示	サポート対象
再検出	サポート対象
展開	プレビュー、展開

Cisco DCNM リリース 11.4(1) 以降、DCNM で展開を無効にしたり、ネットワーク管理者としてファブリックをフリーズしたりできます。ただし、ファブリックをフリーズする場合、またはファブリックがモニタ モードの場合、すべてのアクションを実行することはできません。

次の表に、ファブリックをフリーズするとき、およびファブリックのモニタ モードを有効にするときに実行できるアクションを示します。

操作	DCNM モード	
	フリーズ モード	モニタ モード
追加	保存、プレビュー	ブロック
サブ会議	ブロック済み	ブロック済み
ブレークアウト解除	ブロック済み	ブロック済み
編集	保存、プレビュー	ブロック
削除	保存、プレビュー	ブロック
シャットダウン	保存、プレビュー	ブロック

操作	DCNM モード	
	フリーズ モード	モニタ モード
シャットダウンなし	保存、プレビュー	ブロック
表示	サポート対象	サポート対象
再検出	サポート対象	サポート対象
展開	ブロック済み	ブロック済み

関連付けられた操作のボタンは、それに応じてグレー表示されます。

構成プロファイルの一部である SVI で管理操作（shutdown/no shutdown）を実行すると、連続した**保存して展開**操作で **no interface vlan** コマンドが生成されます。

ポリシーのない SVI の場合、管理操作の実行時、つまり **Interface Manager** から shutdown /no shutdown コマンドがプッシュされると、**int_vlan_admin_state** ポリシーが SVI に関連付けられます。

たとえば、**switch_freeform** から SVI を作成して展開します。

```
interface vlan1234
  description test
  no shutdown
  no ip redirects
  no ipv6 redirects
```

インターフェイス マネージャから SVI をシャットダウンすると、**int_vlan_admin_state** ポリシーが SVI に関連付けられます。

保留中の差分は次のように表示されます。

```
interface Vlan1234
  shutdown
  no ip redirects
  no ipv6 redirects
  description test
  no shutdown
```

自由形式の設定から **no shutdown CLI** を削除します。

ユーザが SVI で管理操作を実行した場合、デバイスには実行構成のインターフェイスがあります。したがって、ネットワーク切断後の **interface vlan** は引き続き存在し、インターフェイスが検出されます。**Interface Manager** からインターフェイスを手動で削除する必要があります。

この項の内容は、次のとおりです。

インターフェイスの追加

Cisco DCNM Web UIからインターフェイスを追加するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

右上に **[範囲（Scope）]** オプションが表示されます。特定のファブリックのインターフェイスを表示する場合は、リストからファブリック ウィンドウを選択します。

ステップ 2 **[追加（Add）]** をクリックして、論理インターフェイスを追加します。

[インターフェイスの追加（Add Interface）] ウィンドウが表示されます。

ステップ 3 **[タイプ（Type）]** ドロップダウン リストで、インターフェイス タイプを選択します。

有効な値は、ポートチャネル、仮想ポートチャネル（vPC）、ストレート（ST）FEX、アクティブ-アクティブ（AA）FEX、ループバック、、トンネルイーサネット、およびスイッチ仮想インターフェイス（SVI） です。インターフェイス タイプを選択すると、それぞれのインターフェイス ID フィールドが表示されます。

- DCNMを通じてポートチャネルを作成する場合は、同じ速度のインターフェイスを追加します。さまざまな速度のインターフェイスから作成されたポート チャネルは起動しません。たとえば、2 つの *10* ギガビット イーサネット ポートを持つポート チャネルが有効です。ただし、*10* ギガビット イーサネット + *25* ギガビット イーサネット ポートの組み合わせを持つポート チャネルは無効です。
- vPC ホストを追加するには、ファブリック トポロジで（ファブリック ビルダを介して）vPC スイッチを指定し、**[保存して展開（Save and Deploy）]**オプションを使用して vPC およびピアリンク構成を展開する必要があります。vPC ペアの構成が展開されると、[vPC ペアの選択（Select a vPC pair）] ドロップダウンボックスに表示されます。

  int_vpc_trunk_host_11_1 ポリシーを使用して vPC を作成できます。
- サブインターフェイスを追加する場合は、[追加（Add）] ボタンをクリックする前に、インターフェイス テーブルからルーテッド インターフェイスを選択する必要があります。
- [インターフェイス（Interface）] ウィンドウでイーサネット インターフェイスを事前プロビジョニングできます。この事前プロビジョニング機能は、Easy、eBGP、および外部ファブリックでサポートされています。詳細については、イーサネットインターフェイスの事前プロビジョニング （109 ページ）を参照してください。

ステップ 4 **[デバイスの選択（Select a Device）]** フィールドで、デバイスを選択します。

デバイスは、ファブリックおよびインターフェイスタイプに基づいてリストされます。外部ファブリック デバイスは、ST FEX および AA FEX には表示されません。vPC またはアクティブからアクティブ FEX の場合は、vPC スイッチペアを選択します。

ステップ 5 選択したインターフェイスに基づいて、表示される各インターフェイス ID フィールド（**ポートチャネル ID**、**vPC ID**、**ループバック ID**、および **サブインターフェイス ID**）に ID 値を入力します。

この値は上書きできます。新しい値は、リソース マネージャ プールで使用可能な場合にのみ使用されます。それ以外の場合は、エラーになります。

ステップ 6 **[ポリシー（Policy）]** フィールドで、インターフェイスに適用するポリシーを選択します。

このフィールドには、インターフェイスのタイプに基づいてフィルタリングされた、*interface interface_edit_policy* のインターフェイス Python ポリシーのみが表示されます。

_upg インターフェイス ポリシーを作成しないでください。たとえば、**vpc_trunk_host_upg**、**port_channel_aa_fex_upg**、**port_channel_trunk_host_upg**、および **trunk_host_upg** オプションを使用してポリシーを作成することはできません。

（注） ポリシーは、**[タイプ（Type）]** ドロップダウンリストで選択したインターフェイス タイプと、**[デバイスの選択（Select a Device）]** ドロップダウンリストで選択したデバイスに基づいてフィルタリングされます。

ステップ 7 **[全般（General）]** タブの必須フィールドに値を入力します。

フィールドは、選択したインターフェイス タイプによって異なります。

（注） Cisco DCNM Release 11.5(1) 以降では、vPC の作成時に Peer-1 の構成を Peer-2 にミラーリングできます。**[構成ミラーリングの有効化（Enable Config Mirroring）]** チェックボックスをオンにすると、[Peer-2] フィールドがグレー表示されます。[Peer-1] フィールドに入力した設定は、[Peer-2] フィールドにコピーされます。

ステップ 8 [保存（Save）] をクリックして、設定を保存します。

（注） インターフェイスに QoS ポリシーを適用するには、参照を使用してインターフェイスの自由形式を作成します。

保存された設定のみがデバイスにプッシュされます。インターフェイスの追加中は、最初の保存後にのみポリシー属性を変更できます。すでに使用されている ID を使用しようとすると、リソースが割り当てられないというエラーが発生します。

ステップ 9 （任意）**[プレビュー（Preview）]** オプションをクリックして、展開する構成をプレビューします。

ステップ 10 **[展開（Deploy）]** をクリックして、指定した論理インターフェイスを展開します。

新しく追加したインターフェイスが画面に表示されます。

サブ会議

[ブレークアウト（Breakout）] アイコン  の横にあるドロップダウン矢印をクリックして、使用可能なブレイクアウト オプションのリストを表示します。使用可能なオプションは、

10g-4x、**25g-4x**、**50g-2x**、**50g-4x**、**100g-2x**、**100g-4x**、**200g-2x**、および**Unbreakout**です。必要なオプションを選択します。

インターフェイスの編集

Cisco DCNM Web UIからインターフェイスを編集するには、次の手順を実行します。

（注） **[インターフェイスの編集（Edit Interface）]**では、ポリシーを変更したり、ポートチャネルまたはvPCからインターフェイスを追加または削除したりできます。

手順

ステップ1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

画面の左上にあるブレークアウトオプションを使用してインターフェイスのブレークアウト、およびブレークアウト解除ができます。

ステップ2 インターフェイスまたはvPCを編集するには、インターフェイス チェックボックスをオンにします。

複数のインターフェイスを編集するには、対応するチェックボックスをオンにします。複数のポート チャネルおよびvPCを編集することはできません。異なるタイプのインターフェイスを同時に編集することはできません。

ステップ3 インターフェイスを編集するには、**[編集（Edit）]** をクリックします。

[構成の編集（Edit Configuration）]ウィンドウに表示される変数は、テンプレートとそのポリシーに基づいています。適切なポリシーを選択します。ポリシーをプレビューし、同じように保存して展開します。このウィンドウには、インターフェイスの種類に基づいてフィルタリングされた、*interface_edit_policy*タグが付いたインターフェイスPythonポリシーのみが表示されます。

vPCのセットアップでは、2つのスイッチは、編集ウィンドウに表示されるスイッチ名の順序になります。たとえば、スイッチ名が *LEAF1:LEAF2* と表示されている場合、Leaf1はピア スイッチ1、Leaf2はピア スイッチ2です。

スイッチへのオーバーレイ ネットワークの展開中に、ネットワークをトランク インターフェイスに関連付けることができます。トランクインターフェイスとネットワークの関連付けは、**[インターフェイス（Interfaces）]**画面に反映されます。このようなインターフェイスを更新できます。

[制御（Control）]>[インターフェイス（Interfaces）]画面から作成されていないインターフェイスポリシーの場合、一部の構成を編集できますが、ポリシー自体は変更できません。編集できないポリシーとフィールドはグレー表示されます。

次に、編集できないポリシーの例を示します。

- ループバック インターフェイス ポリシー：int_fabric_loopback_11_1 ポリシーは、ループバック インターフェイスを作成するために使用されます。ループバック IP アドレスと説明は編集できますが、int_fabric_loopback_11_1 ポリシーインスタンスは編集できません。
- ファブリック アンダーレイ ネットワーク インターフェイス ポリシー（int_fabric_num_11_1 など）およびファブリック オーバーレイ ネットワーク インターフェイス（NVE）ポリシー。
- vPC に関連付けられたポート チャネルおよびメンバーポートを含む、ポート チャネルおよびポート チャネルのメンバー ポートに関連付けられたポリシー。
- ネットワークおよび VRF の作成時に作成された SVI。関連付けられた VLAN がインターフェイス リストに表示されます。

リンクに関連付けられたインターフェイスの編集

リンクには、ファブリック内リンクとファブリック間リンクの2種類があります。名前が示すように、ファブリック内リンクは同じ Easy ファブリック内のデバイス間に設定され、通常はスパイン リーフ接続に使用されます。ファブリック間リンクは、Easy ファブリックと、通常は他の外部または Easy ファブリック間に設定されます。外部 WAN や DC I接続に使用されます。ポリシーは、リンクの両端に適用される設定を効果的に示す各リンクに関連付けられます。つまり、リンク ポリシーは、リンクを形成する2つのインターフェイスに関連付けられた個々の子インターフェイス ポリシーの親になります。このシナリオでは、リンク ポリシーを編集して、説明、IPアドレス、インターフェイスごとの自由形式の設定などのインターフェイス ポリシー フィールドを編集する必要があります。次の手順は、リンクに関連付けられたインターフェイスを編集する方法を示しています。

Procedure

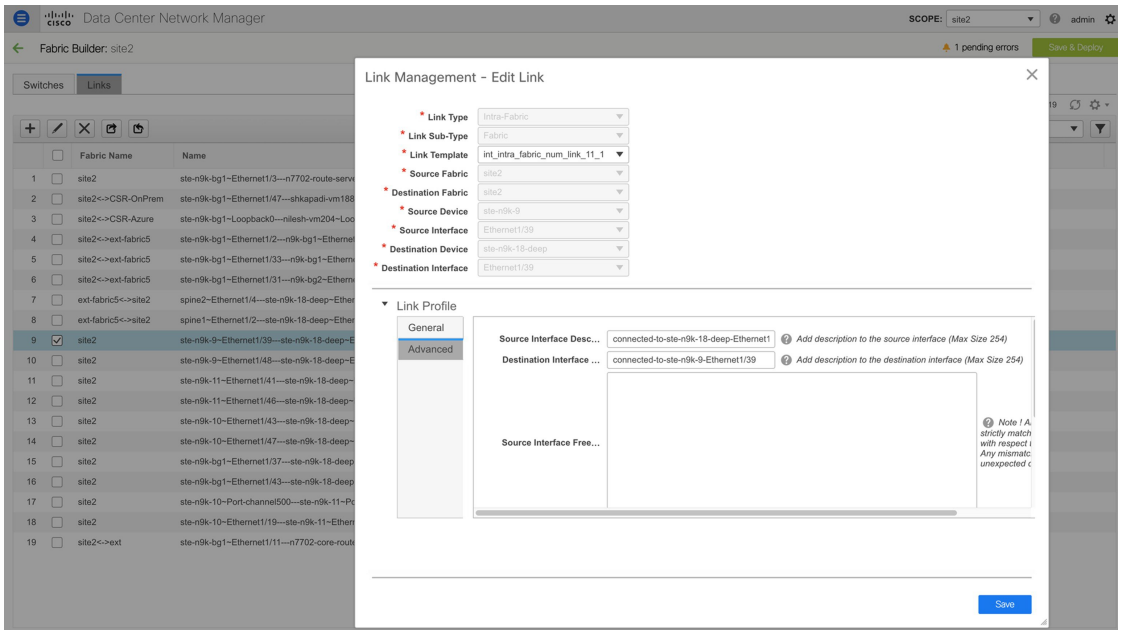
ステップ 1 **[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** を選択し、リンクを含むファブリックを選択します。

ステップ 2 **[アクション（Actions）]** パネルで **[表形式ビュー（Tabular view）]** をクリックします。

[スイッチ（Switches）] タブと **[リンク（Links）]** タブのあるウィンドウが表示されます。

ステップ 3 **[リンク（Links）]** タブをクリックします。

ステップ 4 編集するリンクを選択し、**[リンクの更新（Update Link）]** アイコンをクリックします。



要件に基づいてリンクを更新し、**[保存（Save）]** をクリックします。

インターフェイスの削除

Cisco DCNM Web UI からインターフェイスを削除するには、次の手順を実行します。

（注） このオプションを使用すると、論理ポート、ポート チャネル、および vPC のみを削除できます。オーバーレイまたはアンダーレイ ポリシーがアタッチされていない場合は、インターフェイスを削除できます。

ポート チャネルまたは vPC が削除されると、対応するメンバー ポートにデフォルトのポリシーが関連付けられます。デフォルト ポリシーは、`server.properties` ファイルで設定できます。

手順

ステップ 1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 インターフェイスを選択します。

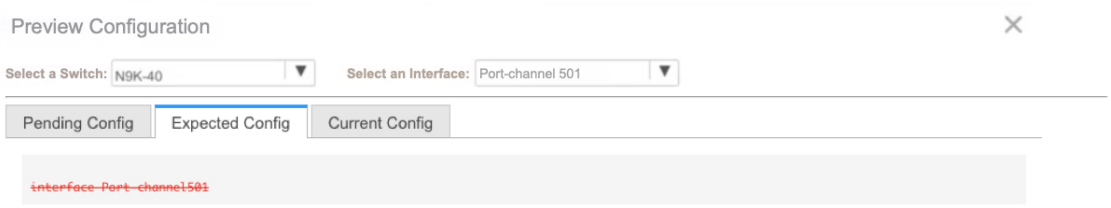
ステップ 3 [削除（Delete）] をクリックします。

ファブリック アンダーレイで作成された論理インターフェイスは削除できません。

ステップ 4 **[Save（保存）]** をクリックします。

ステップ 5 （任意）インターフェイスを削除する前に、**[プレビュー（Preview）]** をクリックしてすべての変更を表示します。

削除は、**[予期される構成（Expected Config）]** タブの下に取り消し線付きの赤色で強調表示されます。



ステップ 6 **[展開（Deploy）]** をクリックして、インターフェイスを削除します。

インターフェイスのシャットダウンと起動

Cisco DCNM Web UI からインターフェイスをシャットダウンして起動するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 シャットダウンまたは起動するインターフェイスを選択します。

ステップ 3 **[シャットダウン（Shutdown）]**をクリックして、選択したインターフェイスを無効にします。たとえば、ネットワークからホストを分離したり、ネットワーク内でアクティブでないホストを分離したりできます。

変更を保存、プレビュー、および展開できる確認ウィンドウが表示されます。**[保存（Save）]** をクリックして、変更の展開をプレビューします。

ステップ 4 **[シャットダウンなし（No Shutdown）]** をクリックして、選択したインターフェイスを起動します。

変更を保存、プレビュー、および展開できる確認ウィンドウが表示されます。**[保存（Save）]** をクリックして、変更をプレビューまたは展開します。

インターフェイス構成の表示

Cisco DCNM Web UI からインターフェイス構成コマンドを表示して実行するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

構成を表示するインターフェイスを選択します。

ステップ 2 **[インターフェイス表示コマンド（Interface Show Commands）]** ウィンドウで、**[表示（Show）]** ドロップダウンボックスからアクションを選択し、**[実行（Execute）]** をクリックします。インターフェイス構成が、画面の右側の **[出力（Output）]** セクションに表示されます。

Show コマンドの場合は、インターフェイスで対応する **show** テンプレート、またはポートチャネルや vPC などのインターフェイス サブタイプを **[テンプレート ライブラリ（Template Library）]** で定義する必要があります。

インターフェイスの再検出

Cisco DCNM Web UI からインターフェイスを再検出するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 再検出するインターフェイスを選択します。

ステップ 3 **[再検出（Rediscover）]** をクリックして、選択されたインターフェイスを再検出します。たとえば、インターフェイスを編集または有効にした後、インターフェイスを再検出できます。

インターフェイス履歴の表示

Cisco DCNM Web UI からインターフェイス履歴を表示するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 インターフェイスを選択します。

ステップ 3 **[インターフェイス履歴（Interface History）]** をクリックして、インターフェイスでの構成履歴を表示します。

ステップ 4 **[ステータス（Status）]** をクリックして、その構成インスタンスに設定されている各コマンドを表示します。

インターフェイス構成の展開

Cisco DCNM Web UIからインターフェイス構成を展開するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [インターフェイス（Interfaces）]** の順に選択します。

ステップ 2 展開するインターフェイスを選択します。

（注） 複数のインターフェイスを選択し、保留中の設定を展開できます。

ステップ 3 **[展開（Deploy）]** をクリックして、インターフェース用に保存されている構成を展開または再展開します。

インターフェイス設定を展開すると、インターフェイス ステータス情報が更新されます。ただし、全体的なスイッチレベルの状態は保留状態（青色）になることがあります。インターフェイス、リンク、ポリシーテンプレートの更新、トップダウンなどのいずれかのモジュールからインテントが変更されると、スイッチ レベルの全体的な状態は保留状態になります。保留状態では、スイッチに保留中の設定またはスイッチ レベルの再計算がある場合があります。スイッチ レベルの再計算は、次の場合に発生します。

- スイッチをプレビューまたは展開します
- 保存および展開中
- 毎時同期中

スイッチをプレビューまたは展開して、状態を確認し、保留状態の根本原因を理解します。ファブリック全体の再計算のために保存して展開します。

[展開（Deploy）] をクリックする前に **[プレビュー（Preview）]** をクリックし、構成をプレビューします。

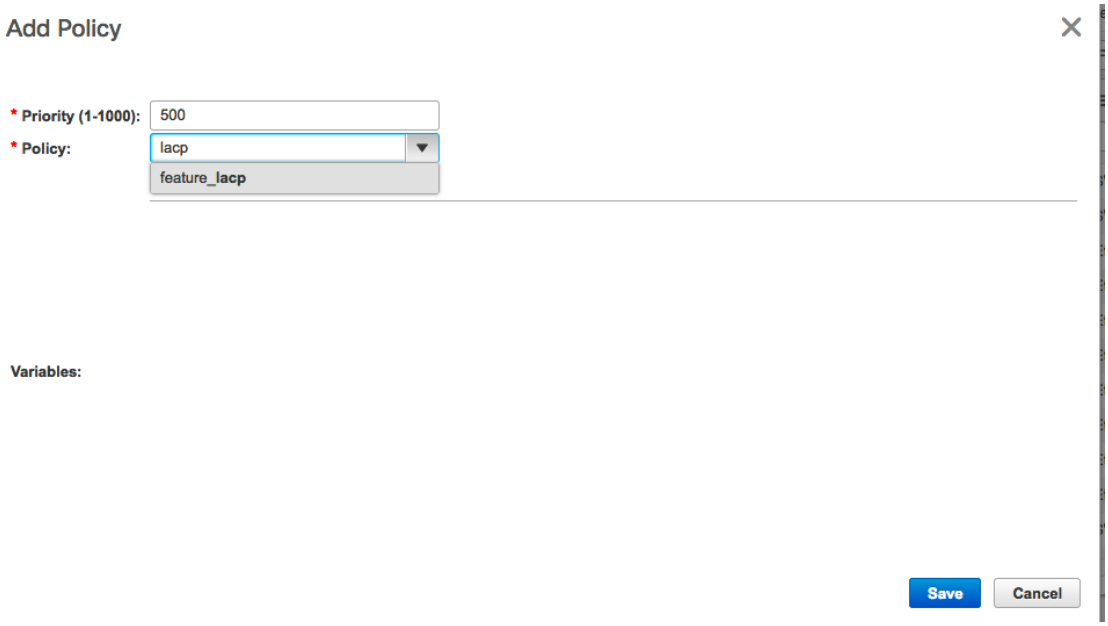
外部ファブリック インターフェイスの作成

外部ファブリック デバイスのポート チャネル、vPC、サブインターフェイス、およびループバック インターフェイスを追加および編集できます。ストレート FEX およびアクティブ-アクティブ FEX 機能は追加できません。

ブレークアウト ポート機能は、外部ファブリックの Cisco Nexus 9000、3000、および 7000 シリーズ スイッチでのみサポートされます。

外部ファブリック デバイスにインターフェイスを追加すると、リソース マネージャはデバイスと同期しません。そのため、ID フィールドに入力された値（ポート チャネルID、vPC ID、ループバック ID など）がスイッチで事前に設定されていないことを確認します。

外部ファブリックでポート チャネルを設定する場合は、ポート チャネルが設定されるスイッチに **feature_lacp** ポリシーを追加して展開する必要があります。



外部ファブリックが **[ファブリック モニタ モードのみ（Fabric Monitor Mode Only）]** に設定されている場合は、そのスイッチに設定を展開できません。ファブリック トポロジ画面で **[保存して展開（Save & Deploy）]** をクリックすると、エラー メッセージが表示されます。ただし、次の設定（スイッチ アイコンを右クリックすると使用可能）が許可されます。

vPC ペアリング：vPC スイッチ ペアを指定できますが、これは参照用です。

ポリシーの表示/編集：ポリシーを追加できますが、スイッチに展開することはできません。

インターフェイスの管理：インターフェイスを追加する目的のみを作成できます。インターフェイスを展開、編集、または削除しようとすると、エラー メッセージが表示されます。

インターフェイスグループ

Cisco DCNM リリース 11.5(1) 以降、ファブリック レベルでホスト側のインターフェイスをグループ化できるインターフェイス グループを作成できます。具体的には、物理イーサネット インターフェイス、L2 ポート チャネル、および vPC のインターフェイス グループを作成できます。インターフェイス グループのインターフェイスに複数のオーバーレイ ネットワークを接続または接続解除できます。

ガイドライン

- インターフェイス グループは、**Easy_Fabric_11_1** テンプレートを使用するファブリックでのみサポートされます。
- インターフェイス グループは、ファブリックに固有です。たとえば、2つのファブリック（Fab1 と Fabric 2）を考えます。Fab1 のインターフェイス グループ IG1 は、Fab 2 には適用されません。
- インターフェイス グループは、特定のタイプのインターフェイスのみを持つことができます。たとえば、物理イーサネット トランク インターフェイスの場合は IG1、L2 トランク ポート チャネルの場合は IG2、vPC ホスト トランク ポートの場合は IG3 など、3 つのタイプのインターフェイスをグループ化する場合は、3つの個別のインターフェイス グループが必要です。
- インターフェイス グループは、事前プロビジョニングされたインターフェイスを使用して作成することもできます。
- インターフェイス グループは、リーフ ロールを持つスイッチに限定されます。これらは、Border、BGW、およびその他の関連バリアントなどの他のロールではサポートされません。
- インターフェイス グループの一部である L2 ポート チャネルおよび vPC の場合、インターフェイス グループに関連付けられているネットワークがない場合でも、それらはインターフェイス グループから関連付け解除されるまで削除できません。同様に、オーバーレイ ネットワークを持たないがIGの一部であるトランク ポートは、アクセス ポートに変換できません。つまり、インターフェイス グループの一部であるインターフェイスのポリシーは変更できません。ただし、ポリシーの特定のフィールドは編集できます。
- リーフ スイッチの L4～L7 サービス設定では、サービス接続に使用されるトランク ポートをインターフェイス グループの一部にすることはできません。
- イージーファブリックのファブリック単位のバックアップを実行すると、そのファブリックで作成されたインターフェイス グループがある場合、関連するすべてのインターフェイス グループの状態がバックアップされます。
- イージーファブリックにインターフェイス グループが含まれている場合、このファブリックは MSO にインポートできません。同様に、イージー ファブリックが MSO に追加されている場合は、イージーファブリック内のスイッチに属するインターフェイスのインターフェイス グループを作成できません。
- **[インターフェイス グループ（Interface Group）]** ボタンは、管理者およびステージャ ユーザに対してのみ有効です。他のすべてのユーザの場合、このボタンは無効になります。
- **[インターフェイス グループ（Interface Group）]** ボタンは、次の状況では無効になります。
  - **[SCOPE]** ドロップダウン リストから **[データセンター（Data Center）]** を選択します。
  - スイッチのないファブリックを選択します。

- vPC、ポートチャネル、およびイーサネット以外の他のインターフェイスを選択します。
- インターフェイスに別の送信元からのポリシーがアタッチされている場合：
  - インターフェイスがポート チャネルまたは vPC のメンバーである場合。
  - ポート チャネルが vPC のメンバーである場合。
  - インターフェイスにアンダーレイまたはリンクからのポリシーがある場合。

（注） 異なるタイプのインターフェイスを選択すると、**[インターフェイス グループ（Interface Group）]** ボタンが有効になります。ただし、インターフェイス グループに対して異なるタイプのインターフェイスを作成または保存しようとすると、エラーが表示されます。

インターフェイス グループの作成

手順

ステップ 1 DCNM から、**[制御（Control）]>[ファブリック（Fabrics）]>[インターフェイス（Interfaces）]** に移動します。

ステップ 2 **[範囲（SCOPE）]** ドロップダウン リストから、ファブリックを選択します。

ステップ 3 グループ化する必要があるインターフェイスを選択し、**[インターフェイスグループ（Interface Group）]** をクリックします。

ステップ 4 4.**[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウで、**[インターフェイス グループの選択（Select Interface Group）]** フィールドにインターフェイス グループ名を入力してカスタム インターフェイス グループを作成し、**[カスタムの作成（Create custom）]** をクリックします。インターフェイス グループ名の最大長は 64 文字です。

すでにインターフェイス グループを作成している場合は、**[インターフェイス グループの選択（Select Interface Group）]** ドロップダウン リストから選択します。また、インターフェイスがすでにインターフェイス グループの一部である場合は、**[インターフェイス グループの選択（Select Interface Group）]** ドロップダウンリストから新しいグループを選択することで、そのインターフェイスを別のインターフェイス グループに移動できます。

（注） インターフェイスは、1つのインターフェイス グループにのみ属することができます。

インターフェイス グループは、**[インターフェイス （Interfaces）]** ウィンドウまたは **[ネットワーク（Networks）]** ウィンドウから作成できます。詳細については、インターフェイス グループへのネットワークの接続 （328 ページ）を参照してください。

ステップ 5 [保存（Save）] をクリックします。

[インターフェイス（Interfaces）] ウィンドウの **[インターフェイス グループ（Interfaces Groups）]** 列にインターフェイス グループ名が表示されます。

インターフェイス グループからのインターフェイスの削除

手順

ステップ 1 DCNM から、**[制御（Control）] > [ファブリック（Fabrics）] > [インターフェイス（Interfaces）]** に移動します。

ステップ 2 **[範囲（SCOPE）]** ドロップダウン リストから、ファブリックを選択します。

ステップ 3 インターフェイス グループから関連付けを解除するインターフェイスを選択し、**[インターフェイス グループ（Interface Group）]** をクリックします。

ステップ 4 **[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウで、**[インターフェイス グループの選択（Select Interface Group）]** ドロップダウンリストで何も選択されていないことを確認し、**[クリア（Clear）]** をクリックします。

関連付けられたすべてのインターフェイスをクリアするかどうかを確認するダイアログボックスが表示されます。**[はい（Yes）]** をクリックして続行します。これらのインターフェイスに接続されているネットワークがある場合、**[クリア（Clear）]** をクリックすると、それらのネットワークも切断されます。

インターフェイス グループへのネットワークの接続

手順

ステップ 1 DCNM から、**[制御（Control）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** に移動します。

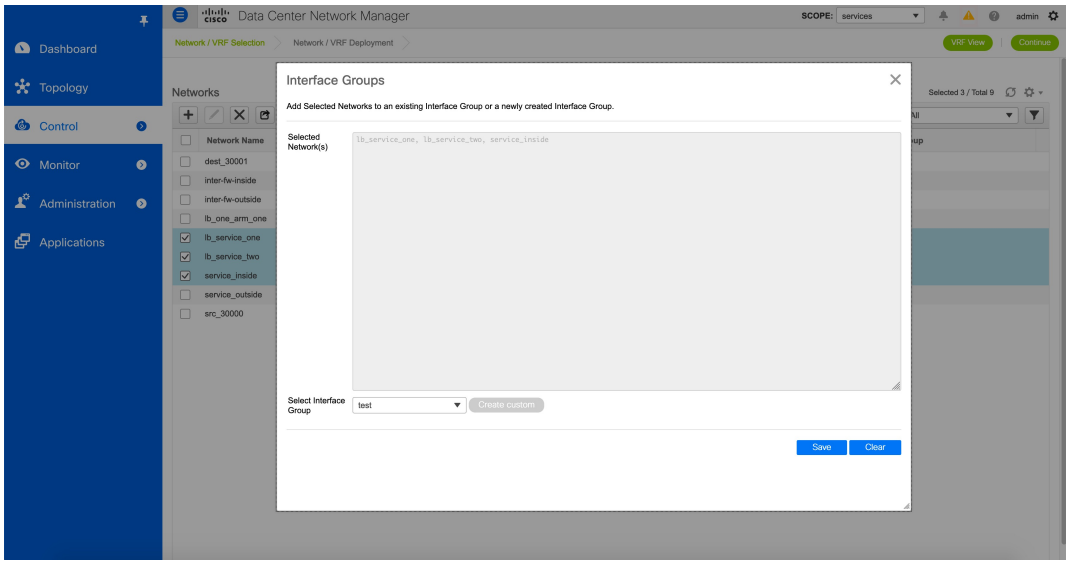
ステップ 2 **[範囲（SCOPE）]** ドロップダウン リストから、ファブリックを選択します。

ステップ 3 **[ネットワーク（Networks）]** ウィンドウで、インターフェイス グループに接続する必要があるネットワークを選択し、**[インターフェイス グループ（Interface Group）]** をクリックします。

（注）
- オーバーレイ ネットワークは、複数のインターフェイス グループに属することができます。
- VLAN ID を持つネットワークのみを選択できます。それ以外の場合は、適切なエラー メッセージが表示されます。

ステップ 4 **[インターフェイス グループ（Interface Groups）]** ウィンドウで、次の操作を実行できます。

- **[インターフェイス グループの選択（Select Interface Group）]** ドロップダウン リストから既存のインターフェイス グループを選択し、**[保存（Save）]** をクリックします。



たとえば、3つのネットワークとインターフェイス グループ **test** を選択し、**[保存（Save）]** ボタンをクリックすると、次の操作がバックグラウンドで実行されます。

1. DCNM は、インターフェイス グループ **[test]** の一部であるインターフェイスを取得します。
2. DCNM は、3 つのネットワークがインターフェイス グループ **[test]** に追加されることを決定します。したがって、これらのネットワークは、インターフェイス グループ **test** の一部であるすべてのインターフェイスに自動接続されます。
3. インターフェイスごとに、DCNM は 選択したネットワークごとに **[switchport trunk allowed vlan add xxxx]** コマンドを 3 回プッシュします。

   （注）　DCNM は、重複する構成インテントがないことを保証します。

[クリア（Clear）] ボタンをクリックすると、DCNM により **[switchport trunk allowed vlan remove xxx]** 構成インテントがプッシュされます。

- **[インターフェイス グループの選択（Select Interface Group）]** フィールドにインターフェイス グループ名を入力してカスタム インターフェイス グループを作成し、**[カスタムの作成（Create custom）]** をクリックします。**[Save（保存）]** をクリックします。

  このオプションを選択する場合は、**[インターフェイス（Interfaces）]** ウィンドウでこのインターフェイス グループにインターフェイスを追加してください。その結果、DCNM は次の操作を実行します。

  1. インターフェイス グループに属していない既存のすべてのオーバーレイ ネットワークをこれらのインターフェイスから削除します。
  2. インターフェイス グループの一部であるが、まだこれらのインターフェイスに接続されていない新しいオーバーレイ ネットワークを追加します。

インターフェイス グループへのインターフェイスの関連付けの詳細については、インターフェイス グループの作成 （326 ページ） を参照してください。

ステップ 5 **[続行（Continue）]** をクリックし、**[保存して展開（Save & Deploy）]** をクリックして、選択したネットワークをスイッチに展開します。

インターフェイス グループからのネットワークの接続解除

この手順では、[ネットワーク（Networks）] ウィンドウでインターフェイス グループからネットワークの接続を解除する方法を示します。また、**[インターフェイス（Interfaces）]** ウィンドウでインターフェイス グループからインターフェイスを削除すると、ネットワークの接続を解除できます。詳細については、「インターフェイス グループからのインターフェイスの削除」を参照してください。

手順

ステップ 1 1. DCNM から、**[制御（Control）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** に移動します。

ステップ 2 **[範囲（SCOPE）]** ドロップダウン リストから、ファブリックを選択します。

ステップ 3 **[ネットワーク（Networks）]** ウィンドウで、インターフェイス グループに接続解除する必要があるネットワークを選択し、**[インターフェイス グループ（Interface Group）]** をクリックします。

ステップ 4 **[インターフェイス グループ（Interface Group）]** ウィンドウで、**[インターフェイス グループの選択（Select Interface Group）]** ドロップダウン リストからインターフェイスグループを選択し、**[クリア（Clear）]** をクリックしてネットワークの接続を解除します。

ステップ 5 （任意） **[制御（Control）] > [ファブリック（Fabrics）] > [インターフェイス（Interfaces）]** に移動します。

[オーバーレイ ネットワーク（Overlay Network）] 列の下に、対応するインターフェイスの未接続ネットワークが赤色で表示されます。ネットワークをクリックすると、取り消し線が引かれた設定が表示されます。

ステップ 6 **[ファブリック ビルダ（Fabric Builder）]** または **[ネットワーク（Networks）]** ウィンドウに移動し、**[保存と展開（Save & Deploy）]** をクリックします。

インターフェイス グループの削除

インターフェイス グループは、使用されていないときに自動的に削除されます。インターフェイス グループにマッピングされたインターフェイスおよびネットワークがない場合、DCNM はインターフェイス グループの暗黙的な削除を実行します。このチェックは、**[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウで **[クリア（Clear）]** ボタンをクリッ

クするたびに実行されます。インターフェイスグループを明示的にクリーンアップする必要がある例外シナリオが存在する場合があります。

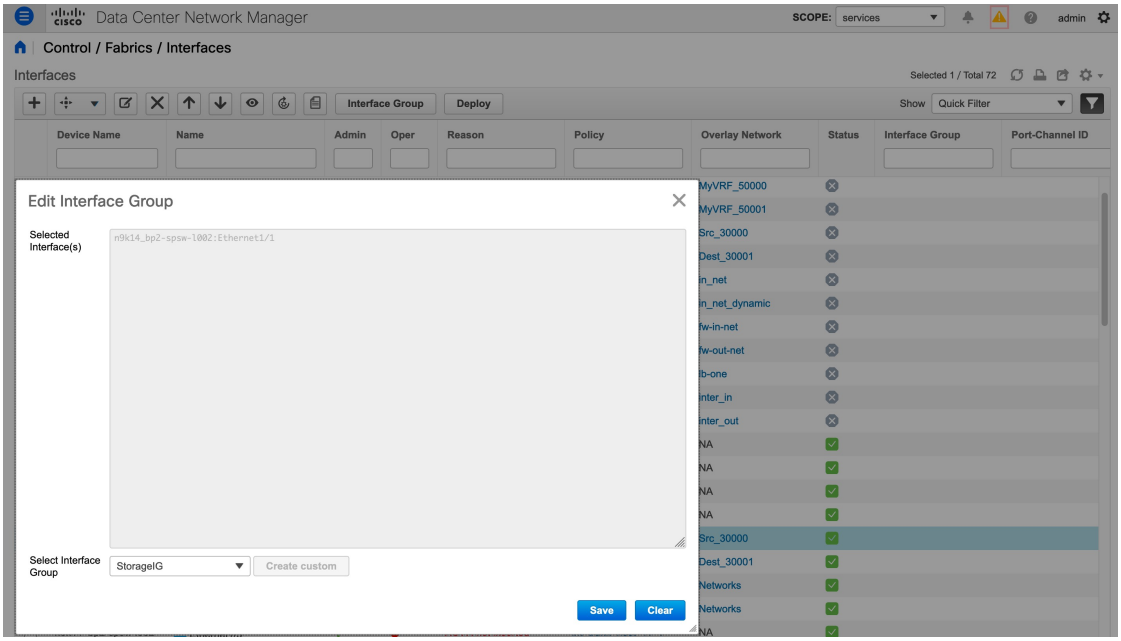
たとえば、インターフェイス グループ **storageIG** を作成し、それにインターフェイスを追加します。後で、インターフェイス マッピングを別のグループに変更します。したがって、インターフェイスを選択し、**[インターフェイス グループ（Interface Group）]** をクリックして **[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウを開きます。**diskIG** という名前の別のインターフェイス グループを選択します。現在、**storageIG** インターフェイス グループには、関連付けられているメンバー インターフェイスまたはネットワークがありません。この場合は、次の手順を実行します。

手順

ステップ 1 インターフェイスグループに属していないインターフェイスを選択します。

ステップ 2 インターフェイスを選択し、**[インターフェイス グループ（Interface Group）]** をクリックして **[インターフェイス グループの編集（Edit Interface Group）]** ウィンドウを開きます。

ステップ 3 **[インターフェイス グループの選択（Select Interface Group）]** ドロップダウン リストから **StorageIG** インターフェイス グループを選択します。



ステップ 4 [Clear] をクリックします。

ネットワークおよび VRF の作成と展開

オーバーレイ ネットワークと VRF プロビジョニングの手順は次のとおりです。

1. ファブリックにネットワークと VRF を作成します。

2. ファブリック スイッチでネットワークと VRF を展開します。

Note 展開の説明の後に、オーバーレイネットワークとVRFの展開解除と削除について説明します。最後に、外部ファブリックの作成と、VXLANから外部ファブリックへのファブリック拡張について説明します。

インターフェイス グループの作成とネットワークの接続については、インターフェイスグループ, on page 324 を参照してください。

次のオプションのいずれかを使用して、ネットワークおよびVRF ウィンドウに移動できます。

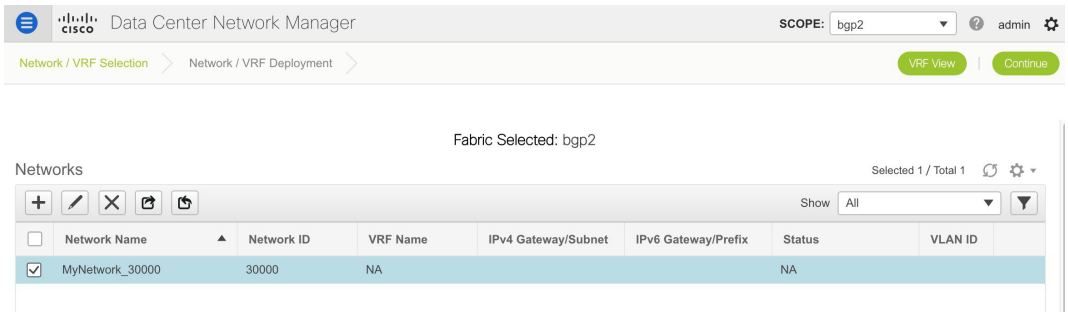
- ホームページから： Cisco DCNM Web UI のランディングページで **[ネットワークと VRF（Networks & VRFs）]** ボタンをクリックします。
- [制御（Control）] メニューから：Cisco DCNM Web UI のホームページから、**[制御（Control）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** を選択して、**[ネットワーク（Networks）]** ウィンドウに移動します。**[制御（Control）] > [ファブリック（Fabrics）] > [VRF]** を選択して、**[VRF]** ウィンドウに移動します。
- ファブリック トポロジ ウィンドウから：ファブリック トポロジ ウィンドウの任意の場所を右クリックします。**[オーバーレイ表示（Overlay View）] > [VRF 表示（VRF View）]** または **[オーバーレイ表示（Overlay View）] > [ネットワーク表示（Network View）]** を選択します。このオプションはスイッチ ファブリック、Easy ファブリック、および MSD ファブリックにのみ適用可能です。

[VRF 表示（VRF View）] または **[ネットワーク表示（Network View）]** ボタンをクリックすると、両方のウィンドウでネットワーク表示と VRF 表示を切り替えることができます。ネットワークまたは VRF ウィンドウを開いているとき、ネットワークまたは VRF を作成する前に、**[範囲（Scope）]** ドロップダウンリストから適切なファブリックを選択していることを確認してください。

ファブリックのネットワークと VRF の表示

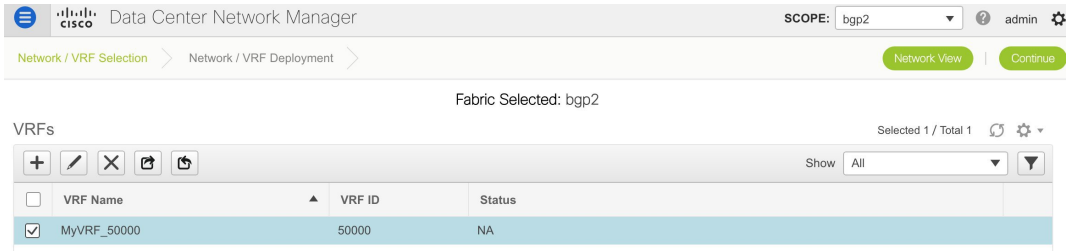
- メイン メニューから **[制御（Control）] > [ネットワーク（Networks）]** をクリックします。

  [ネットワーク（Networks）] 画面が表示されます。（画面の右上にある）[範囲（SCOPE）] ドロップダウンボックスには、DCNM インスタンスによって管理されるすべてのファブリックがアルファベット順に一覧表示されます。[範囲（SCOPE）]から正しいファブリックを選択できます。ファブリックを選択すると、**[ネットワーク（Networks）]** 画面が更新され、選択したファブリックのネットワークが一覧表示されます。



- メイン メニューから **[制御（Control）] > [VRF]** をクリックします。

  VRF 画面が表示されます。（画面の右上にある）SCOPE ドロップダウン ボックスには、DCNM インスタンスによって管理されるすべてのファブリックがアルファベット順に一覧表示されます。[範囲（SCOPE）] から正しいファブリックを選択できます。ファブリックを選択すると、**[VRF]** 画面が更新され、選択したファブリックの VRF が一覧表示されます。



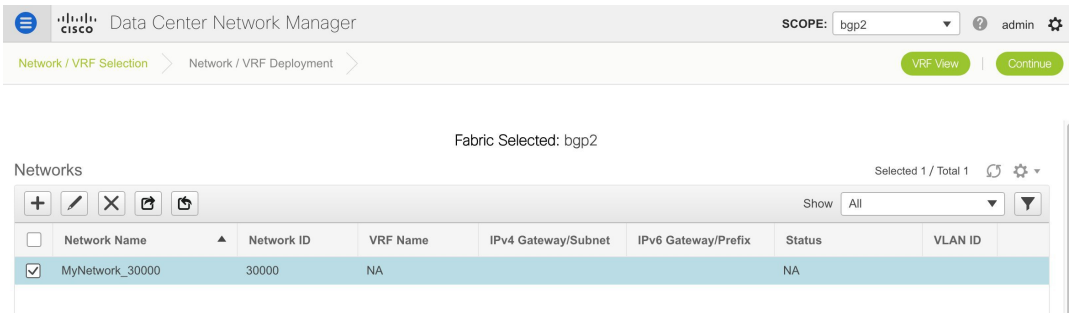
Note **[ネットワーク（Networks）]** または **[VRF]** ウィンドウは、Easy ファブリックまたは MSD ファブリックにのみ適用されます。

スタンドアロン ファブリック向けのネットワークの作成

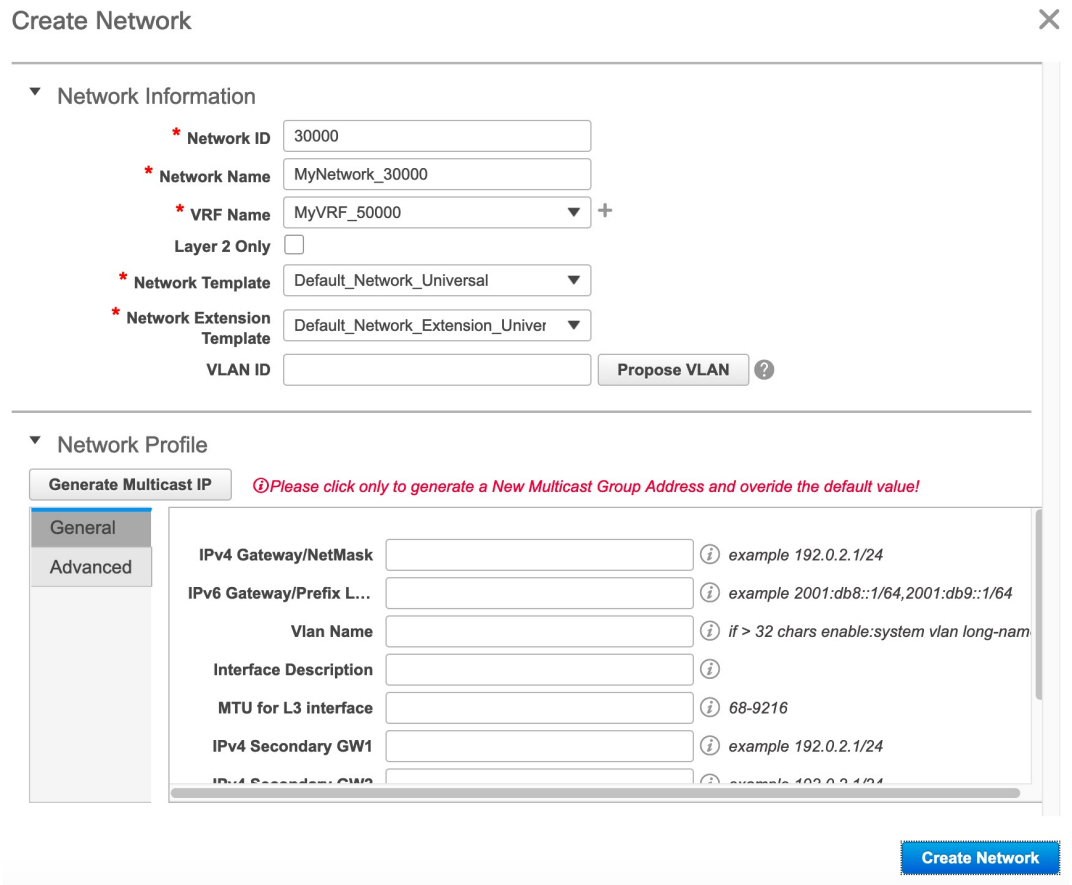
1. **[制御（Control）] > [ネットワーク（Networks）]**（**[ファブリック（Fabrics）]** サブメニューの下）をクリックします。

   [ネットワーク（Networks）] 画面が表示されます。

2. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[ネットワーク（Networks）]** 画面が更新され、選択したファブリックのネットワークが一覧表示されます。



3. 画面の左上部分（**[ネットワーク（Networks）]** の下）にある **[+]** ボタンをクリックして、ネットワークをファブリックに追加します。[ネットワークの作成（Create Network）]画面が表示されます。ほとんどのフィールドは自動入力されます。



この画面のフィールドは次のとおりです。

[ネットワーク ID（Network ID）] と **[ネットワーク名（Network Name）]**：ネットワークのレイヤ 2 VNI と名前を指定します。ネットワーク名には、アンダースコア（_）とハイフン（-）以外の空白や特殊文字は使用できません。対応するレイヤ 3 VNI（または VRF VNI）は、VRF の作成時に生成されます。

[VRF 名（VRF Name）]：仮想ルーティングおよび転送（VRF）を選択できます。

VRF が作成されていない場合、このフィールドは空白になります。新しい VRF を作成する場合は、**[+]** ボタンをクリックします。VRF名には、アンダースコア（_）、ハイフン（-）、およびコロン（:）以外の空白文字や特殊文字は使用できません。

[レイヤ 2 のみ（Layer 2 Only）]：ネットワークがレイヤ 2 のみであるかどうかを指定します。

[ネットワーク テンプレート (Network Template)]：ユニバーサル テンプレートが自動入力されます。これはリーフ スイッチにのみ適用されます。

[ネットワーク拡張テンプレート (Network Extension Template)]：ユニバーサル拡張テンプレートが自動入力されます。これにより、このネットワークを別のファブリックに拡張できます。メソッドは VRF Lite、Multi Site などです。このテンプレートは、境界リーフ スイッチおよび BGW に適用できます。

[VLAN ID]：ネットワークの対応するテナントVLAN IDを指定します。

VLAN ID のデフォルト範囲は 2 から 3967 です。DCNM リリース 11.5(2) 以降、デフォルト値 3967 以上の VLAN 範囲を使用できます。予約済み VLAN 範囲は異なる範囲で設定する必要があります。スイッチ コマンドで「**system vlan <vlan> reserve**」を入力します。スタートアップ構成で構成を保存し、新しい予約済み VLAN 範囲を反映させてスイッチをリロードします。

Cisco DCNM Web UI から、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** の順に選択し、**RM.TOP_DOWN_NETWORK_VLAN.MAX** および **RM.TOP_DOWN_VRF_VLAN.MAX** に値 4094 として入力し、**[変更の適用（Apply Changes）]** をクリックし DCNM を再起動します。DCNM が起動したら、3967 以上の VLAN 値を使用して VRF とネットワークを作成できます。

[ネットワーク プロファイル（Network Profile）] セクションには、*[全般（General）]* タブと *[詳細（Advanced）]* タブがあります。

[General] タブ

IPv4 ゲートウェイ/ネットマスク (IPv4 Gateway/NetMask)]：IPv4 アドレスとサブネットを指定します。

Note ネットワーク テンプレートの IPv4 ゲートウェイと IPv4 セカンダリ GW1 または GW2 フィールドに同じ IP アドレスを構成した場合、DCNM はエラーを表示しないので、この構成は保存できます。

ただし、このネットワーク設定がスイッチにプッシュされると、スイッチは設定を許可しないため、障害が発生します。

[IPv6ゲートウェイ/プレフィックス（IPv6 Gateway/Prefix）]：サブネットの IPv6 アドレスを指定します。

MyNetwork_30000 に属するサーバーおよび別の仮想ネットワークに属するサーバーからの L3 トラフィックを転送するためのエニーキャスト ゲートウェイ IP アドレスを指定しま

す。デフォルトでエニーキャスト ゲートウェイ IP アドレスは、ネットワークが存在するファブリックのすべてのスイッチの MyNetwork_30000 で同じです。

[Vlan 名（Vlan Name）]：VLAN 名を入力します。

[インターフェイスの説明 (Interface Description)]：インターフェイスの説明を指定します。このインターフェイスはスイッチの仮想インターフェイス（SVI）です。

[L3 インターフェイスの MTU（MTU for L3 interface）]：レイヤ 3 インターフェイスの MTU を入力します。

IPv4セカンダリGW1：追加のサブネットのゲートウェイIPアドレスを入力します。

IPv4セカンダリGW2：追加のサブネットのゲートウェイIPアドレスを入力します。

[詳細（Advanced）]タブ：オプションとして、**[詳細（Advanced）]**タブをクリックしてプロファイルの詳細設定を指定できます。

[ARP 抑制 (ARP Suppression)]：ARP 抑制機能を有効にするには、このチェックボックスをオンにします。

[入力レプリケーション（Ingress Replication）]：レプリケーション モードが入力レプリケーションの場合、チェックボックスはオンになります。

Note 入力レプリケーションは、[詳細（Advanced）]タブの読み取り専用オプションです。ファブリック設定を変更すると、このフィールドは更新されます。

[マルチキャスト グループ アドレス（Multicast Group Address）]：ネットワークのマルチキャスト IP アドレスが自動入力されます。

マルチキャストグループアドレスは、ファブリックインスタンスごとの変数です。サポートされるアンダーレイ マルチキャスト グループの数は 128 に限られます。すべてのネットワークがすべてのスイッチに展開されている場合は、L2 VNI またはネットワークごとに異なるマルチキャストグループを使用する必要はありません。したがって、ファブリック内のすべてのネットワークのマルチキャストグループは同じままです。新しいマルチキャスト グループ アドレスが必要な場合は、**[マルチキャスト IP の生成 (Generate Multicast IP)]**ボタンをクリックして生成できます。

DHCPv4サーバ1：最初のDHCPサーバのDHCPリレーIPアドレスを入力します。

DHCPv4サーバ2：次のDHCPサーバのDHCPリレーIPアドレスを入力します。

[DHCPv4 サーバー VRF（DHCPv4 Server VRF）]：DHCP サーバーの VRF ID を入力します。

Loopback ID for DHCP Relay interface（Min：0、Max：1023）：DHCPリレーインターフェイスのループバックIDを指定します。

[ルーティング タグ（Routing Tag）]：ルーティングタグは自動入力されます。このタグは、各ゲートウェイの IP アドレス プレフィックスに関連付けられます。

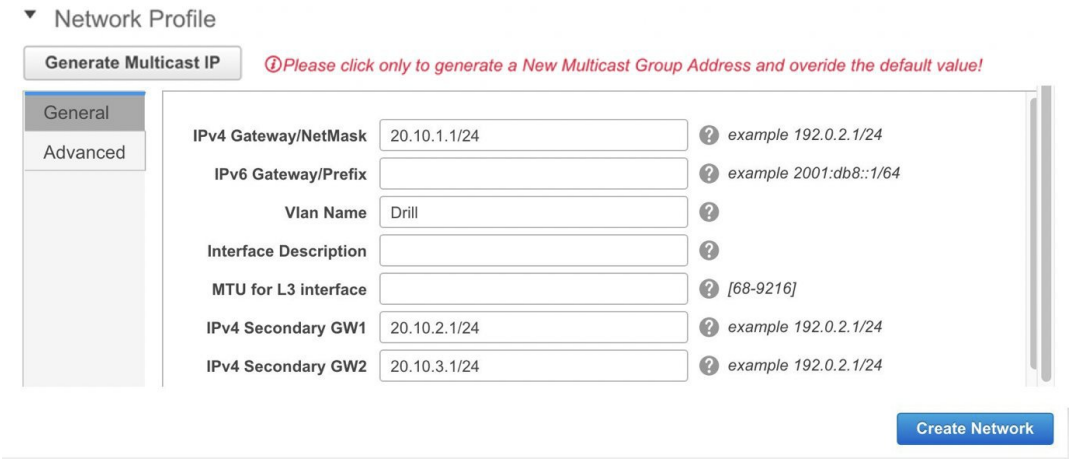
[TRM が有効（TRM enable）]：TRM を有効にするには、このチェックボックスをオンにします。

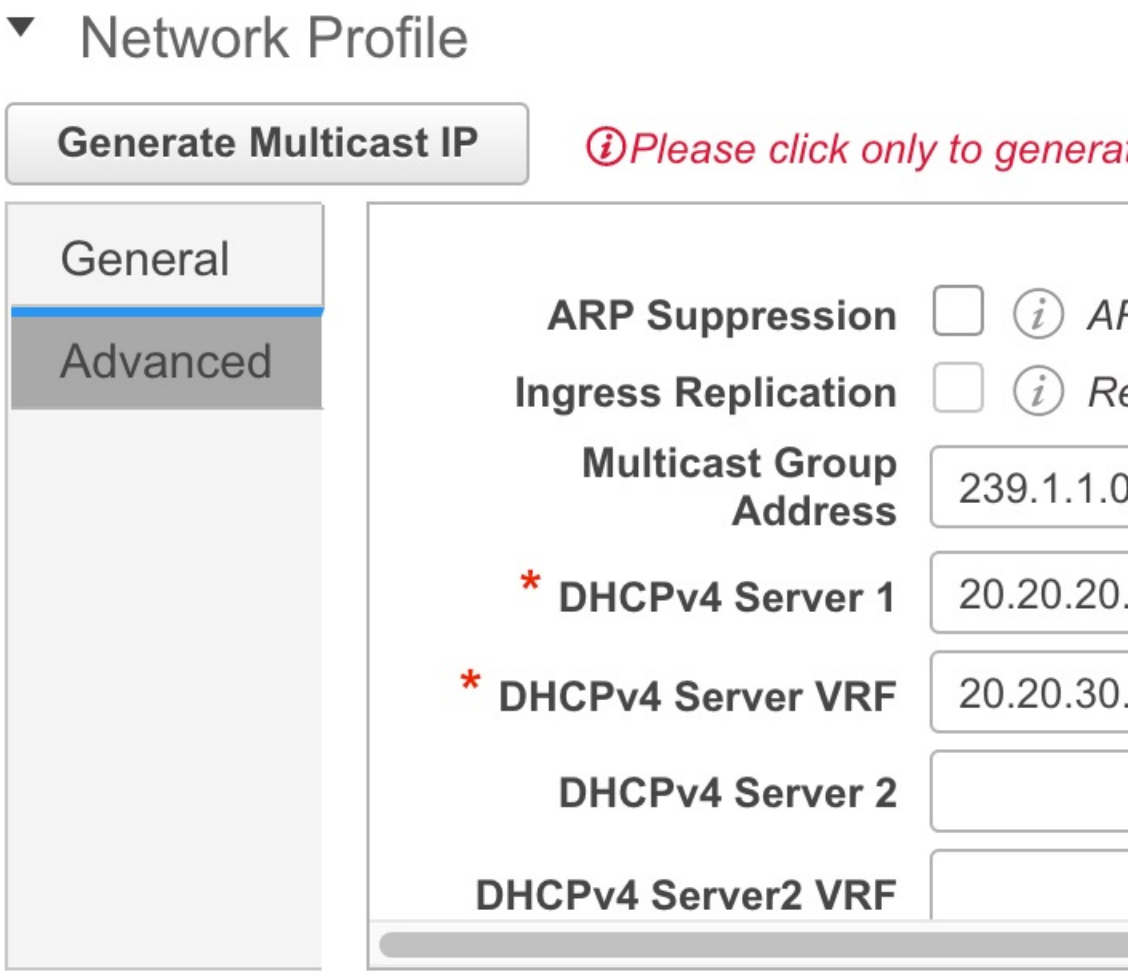
詳細については、テナント ルーテッド マルチキャストの概要, on page 234を参照してください。

[L2 VNI ルート ターゲットの両方が有効（L2 VNI Route Target Both Enable）]：すべての L2 仮想ネットワークのルート ターゲットの自動インポートとエクスポートを有効にするには、このチェックボックスをオンにします。

[境界でのL3ゲートウェイの有効化（Enable L3 Gateway on Border）]：チェックボックスをオンにすると、境界スイッチでレイヤ3ゲートウェイが有効になります。

[ネットワークの作成（Create Network）] 画面のサンプルを以下に示します。





4. [ネットワークの作成（Create Network）]をクリックします。画面の右下に、ネットワークが作成されたことを示すメッセージが表示されます。

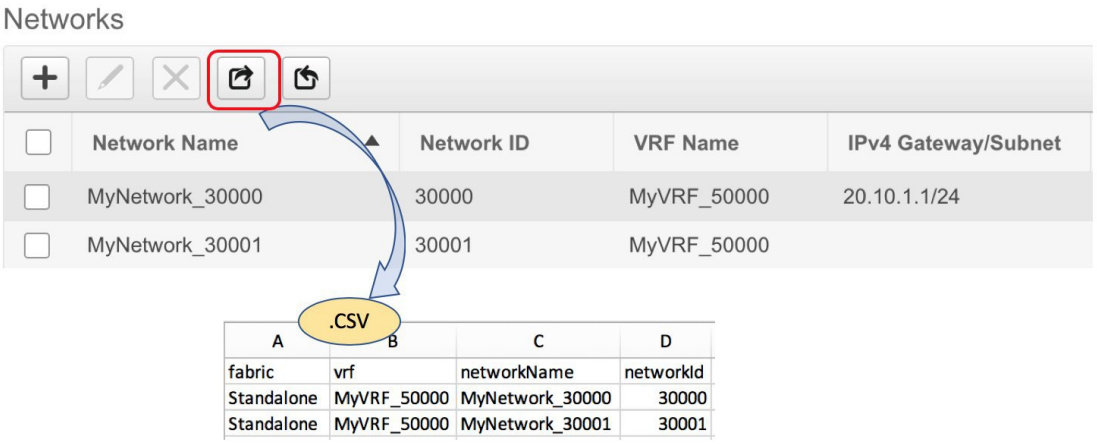
   新しいネットワークは、表示される **[ネットワーク (Networks)]** ページに表示されます。

ネットワークは作成されていますが、まだスイッチに展開されていないため、ステータスは *NA* です。これでネットワークは作成されました。必要であればさらにネットワークを作成し、ファブリック内のデバイスにネットワークを展開できます。

ネットワーク情報のエクスポートとインポート

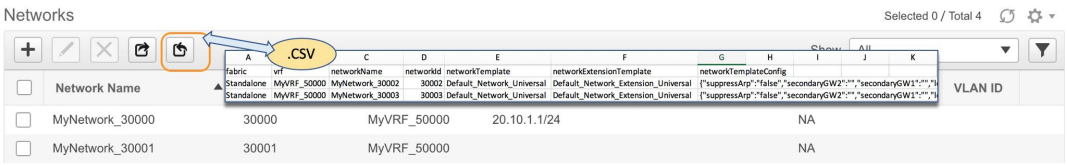
ネットワーク接続についての情報は、.CSV ファイルにエクスポートすることが可能です。エクスポートされたファイルには、所属するファブリック、関連付けられている VRF、ネットワークの作成に使用されたネットワーク テンプレート、およびネットワークの作成時に保存したその他のすべての設定の詳細が含まれます。

[ネットワーク（Networks）]画面で、[エクスポート（Export）]アイコンをクリックして、ネットワーク情報を .CSV ファイルとしてエクスポートします。



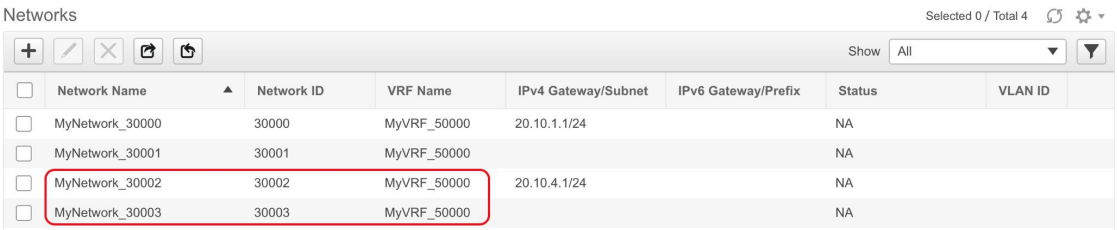
エクスポートされた .CSV ファイルは参照用に使用することや、新しいネットワークを作成するためのテンプレートとして使用することができます。ネットワークをインポートするには、次の手順を実行します。

1. .CSV ファイル内の新しいレコードをアップデートします。[networkTemplateConfig] フィールドに JSON オブジェクトが含まれていることを確認します。画面の右下にあるメッセージ部に、エラーメッセージと成功メッセージが表示されます。このスクリーンショットは、インポートされる 2 つの新しいネットワークを示しています。



2. [ネットワーク（Networks）]画面で、[インポート（Import）]アイコンをクリックし、.CSV ファイルを DCNM にインポートします。

インポートされたネットワークが[ネットワーク（Networks）]画面に表示されていることがわかります。



スタンドアロン ファブリック向けのネットワークの編集

Cisco DCNM Web UI からスタンドアロン ファブリック向けのネットワークを編集するには、以下の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ネットワーク（Networks）]** をクリックします。

[ネットワーク（Networks）] ウィンドウが表示されます。

ステップ 2 **[範囲（SCOPE）]** ドロップダウンリストから [ファブリック（Fabric）] を選択します。

[ネットワーク（Networks）] ウィンドウが更新され、ファブリック内のネットワークが一覧表示されます。

ステップ 3 ネットワークを選択します。

ステップ 4 [編集（Edit）] アイコンをクリックします。

[ネットワークの編集（Edit Network）] ウィンドウが表示されます。

ステップ 5 必要に応じて、**[ネットワーク プロファイル（Network Profile）]** エリアの **[全般（General）]** タブと **[詳細（Advanced）]** タブのフィールドを更新します。

Note ネットワーク名を編集できます。編集したネットワーク名は、**[ネットワーク（Networks）]** ウィンドウの **[ネットワーク名（Network Name）]** 列に表示されます。ネットワークの作成時に使用した元の名前が **[ディスプレイ名（Display Name）]** 列に表示されます。**[ネットワーク（Networks）]** ウィンドウの **[ディスプレイ名（Display Name）]** 列から元のネットワーク名を表示するには、**[設定（Settings）]** をクリックします。**[列（Columns）]** ドロップダウンリストを展開し、**[ディスプレイ名（Display Name）]** オプションを選択します。[閉じる（Close）] をクリックします。ネットワーク トポロジ表示で元のネットワーク名を表示することもできます。

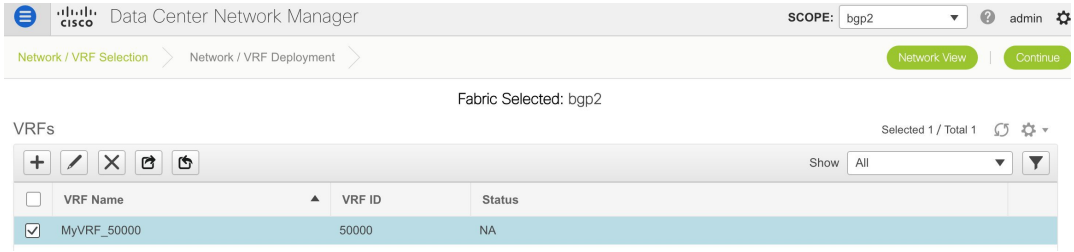
ステップ 6 ウィンドウの右下の **[保存（Save）]** ボタンをクリックして、アップデートを保存します。

スタンドアロン ファブリック向けの VRF の作成

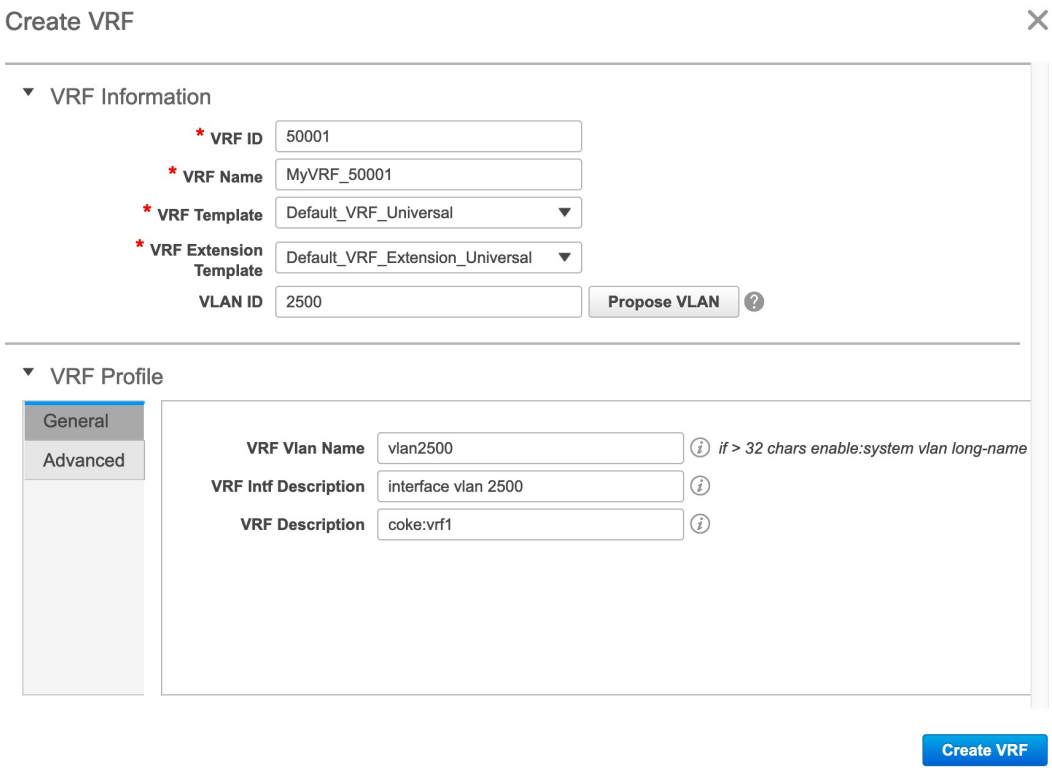
1. **[制御（Control）] > [VRF]（[ファブリック（Fabrics）]** サブメニューの下）をクリックします。

   [VRF] 画面が表示されます。

2. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[VRF]** 画面が更新され、選択したファブリックの VRF が一覧表示されます。



3. **[+]** ボタンをクリックして、スタンドアロン ファブリックに VRF を追加します。[VRF の作成 (Create VRF)] 画面が表示されます。ほとんどのフィールドは自動入力されます。



この画面のフィールドは次のとおりです。

[VRF ID] と **[VRF 名（VRF Name）]**：VRF の ID と名前です。

Note 使いやすいように、ネットワークの作成時に VRF 作成オプションも使用できます。

[VRF テンプレート（VRF Template）]：このテンプレートは VRF の作成に適用でき、リーフスイッチにのみ適用できます。

[VRF 拡張テンプレート（VRF Extension Template）]：テンプレートは、VRF を他のファブリックに拡張する場合に適用され、ボーダー デバイスに適用されます。

[VRF プロファイル（VRF Profile）] セクションのフィールドに入力します。

[全般（General）] タブ：VRF に関連付けられた VLAN の VLAN ID、対応するレイヤ 3 仮想インターフェイス、および VRF ID を入力します。

VLAN ID のデフォルト範囲は 2 から 3967 です。DCNM リリース 11.5(2) 以降、デフォルト値 3967 以上の VLAN 範囲を使用できます。予約済み VLAN 範囲は異なる範囲で設定する必要があります。スイッチ コマンドで「**system vlan <vlan> reserve**」を入力します。スタートアップ構成で構成を保存し、新しい予約済み VLAN 範囲を反映させてスイッチをリロードします。

Cisco DCNM Web UI から、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** の順に選択し、**[RM.TOP_DOWN_NETWORK_VLAN.MAX]** および **[RM.TOP_DOWN_VRF_VLAN.MAX]** に値 4094 として入力し、**[変更の適用（Apply Changes）]** をクリックし DCNM を再起動します。DCNM が起動したら、3967 以上の VLAN 値を使用して VRF とネットワークを作成できます。

[詳細（Advanced）] タブ：タブのフィールドは自動入力されます。

[VRF インターフェイス MTU（VRF Intf MTU）]：VRFインターフェイスMTUを指定します。

[ルーティング タグ（Routing Tag）]：VLAN が複数のサブネットに関連付けられている場合、このタグは各サブネットの IP プレフィックスに関連付けられます。このルーティング タグは、オーバーレイ ネットワークの作成にも関連付けられています。

[再配布直接ルート マップ（Redistribute Direct Route Map）]：VRF でルートを再配布するためのルート マップ名を指定します。

[最大 BGP パス（Max BGP Paths）] および **[最大 iBGP パス（Max iBGP Paths）**：最大 BGP および iBGP パスを指定します。

[TRM の有効（TRM Enable）]：TRM を有効にするには、このチェックボックスをオンにします。

TRM を有効にする場合は、RP アドレスとアンダーレイ マルチキャスト アドレスを入力する必要があります。

詳細については、テナント ルーテッド マルチキャストの概要, on page 234を参照してください。

[RP が外部（Is RP External）]：ファブリックに対して RP が外部である場合、このチェックボックスを有効にします。このフィールドのチェックがオフの場合、RP はすべての VTEP に分散されます。

RP アドレス：RP の IP アドレスを指定します。

RP ループバック ID：**RP が外部** が有効化されていない場合、RP のループバック ID を指定します。

[アンダーレイ マルチキャスト アドレス（Underlay Multicast Address）]：VRF に関連付けられたマルチキャスト アドレスを指定します。マルチキャスト アドレスは、ファブリック アンダーレイでマルチキャスト トラフィックを転送するために使用します。

Note ファブリック設定画面の **[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]** フィールドのマルチキャスト アドレスは、このフィールドに自動的に入力されます。この VRF に別のマルチキャスト グループ アドレスを使用する必要がある場合は、このフィールドを上書きできます。

[オーバーレイ マルチキャスト グループ（Overlay Multicast Groups）]：指定した RP のマルチキャスト グループ サブネットを指定します。値は「ip pim rp-address」コマンドのグループ範囲です。フィールドが空の場合、デフォルトで 224.0.0.0/24 が使用されます。

[IPv6 リンク ローカル オプションの有効化（Enable IPv6 link-local Option）]：このチェックボックスをオンにすると、VRF SVI で IPv6 リンク ローカル オプションが有効になります。このチェックボックスをオフにすると、IPv6 転送が有効になります。

[TRM BGW マルチサイトの有効化（Enable TRM BGW MSite）]：チェックボックスをオンにして、ボーダー ゲートウェイ マルチサイトで TRM を有効にします。

[ホスト ルートのアドバタイズ（Advertise Host Routes）]：エッジ ルータへの /32 および /128 ルートのアドバタイズメントを制御するには、このチェックボックスをオンにします。

[デフォルトルートのアドバタイズ（Advertise Default Route）]：このチェックボックスをオンにすると、デフォルトルートのアドバタイズメントが内部的に制御されます。

異なる VXLAN ファブリック内（両方のファブリックにサブネットが存在する）のエンドホスト間のサブネット間通信を許可するには、関連付けられている VRF の **デフォルト ルートのアドバタイズ**機能を無効にする（**[デフォルト ルートのアドバタイズ（Advertise Default Route）]** チェックボックスをオフにする）必要があります。これにより、両方のファブリックでホストの /32 ルートが表示されます。たとえば、ファブリック 1 のホスト 1（VNI 30000、VRF 50001）は、ホスト ルートが両方のファブリックに存在する場合にのみ、ファブリック 2 のホスト 2（VNI 30001、VRF 50001）にトラフィックを送信できます。サブネットが 1 つのファブリックにのみ存在する場合は、サブネット間通信にはデフォルト ルートだけで十分です。

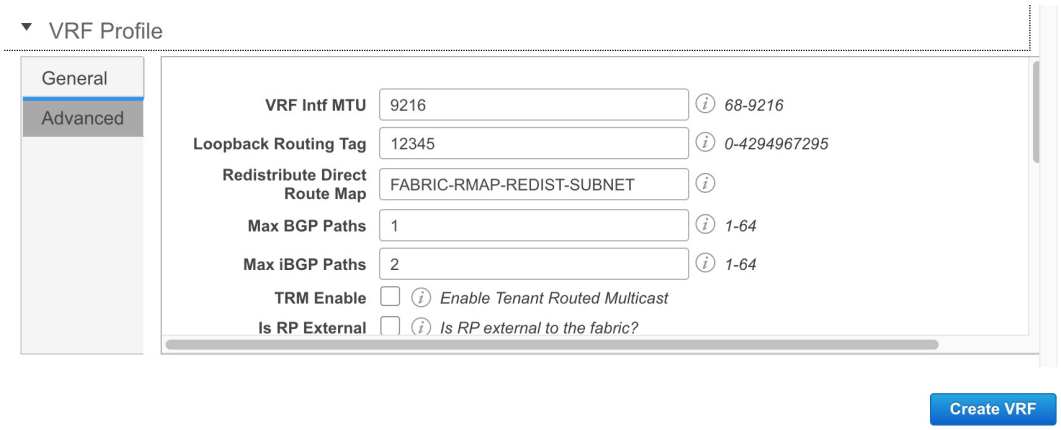
[静的 0/0 ルートの構成（Config Static 0/0 Route）]：静的デフォルトルートの構成を制御するには、このチェックボックスをオンにします。

[BGP ネイバーパスワード（BGP Neighbor Password）]：VRF Lite BGP のネイバー パスワードを指定します。

[BGP パスワード キー暗号化タイプ（BGP Password Key Encryption Type）]：このドロップダウン リストから暗号化タイプを選択します。

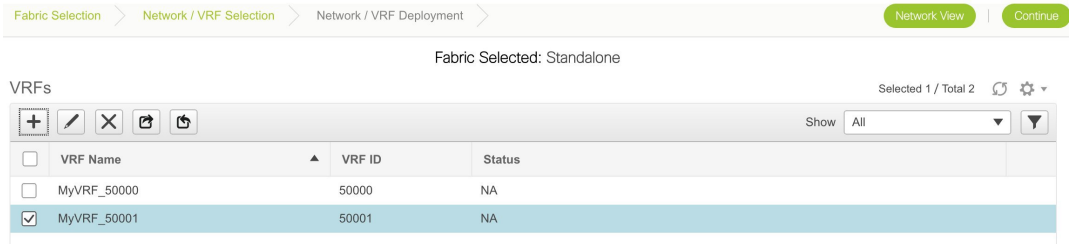
VRF の作成画面のサンプル スクリーンショット：

[Advanced] タブ：



4. **[VRF の作成（Create VRF）]** をクリックします。

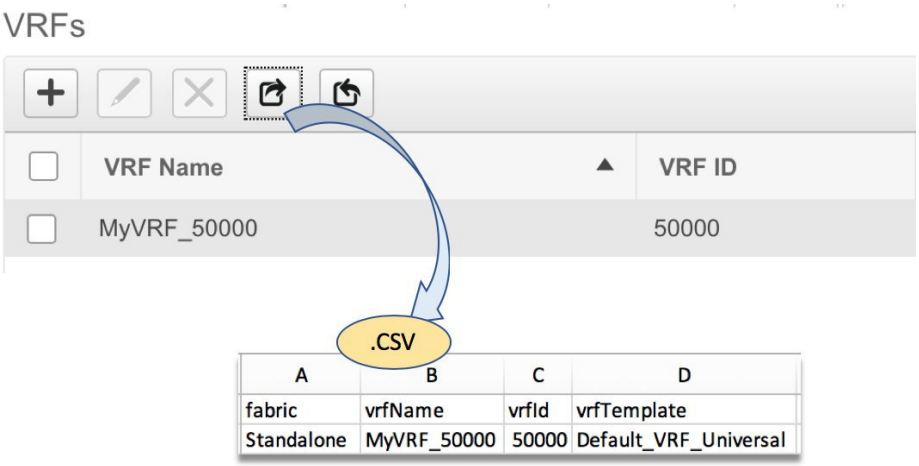
   MyVRF_50001 VRF が作成され、VRFs ページに表示されます。



[VRF 情報のエクスポートとインポート（Export and Import VRF Information）]

VRF 接続についての情報は、.CSV ファイルにエクスポートすることが可能です。エクスポートされたファイルには、含まれるファブリック、VRF 作成に使用されたテンプレート、および VRF の作成時に保存したその他のすべての構成の詳細を含む、各 VRF に関連する情報が格納されています。

[VRF] 画面で、[エクスポート（Export）] アイコンをクリックして、VRF 情報を .CSV ファイルとしてエクスポートします。



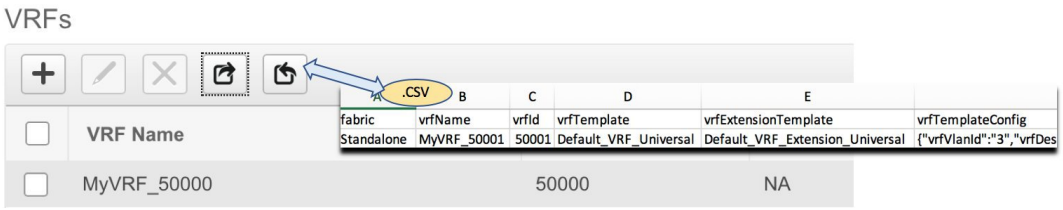
エクスポートされた .CSV ファイルは参照用に使用することや、新しい VRF を作成するためのテンプレートとして使用することができます。VRF をインポートするには、次の手順を実行します。

1. .CSV ファイル内の新しいレコードをアップデートします。**[vrfTemplateConfig]** フィールドに JSON オブジェクトが含まれていることを確認します。
2. [VRF] 画面で、**[インポート（Import）]** アイコンをクリックし、.CSV ファイルを DCNM にインポートします。

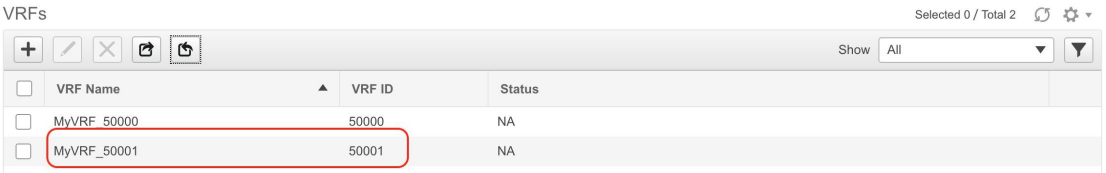
   画面の右下にあるメッセージ部に、エラーメッセージと成功メッセージが表示されます。このスクリーンショットは、インポートされる新しい VRF を示しています。

Note [VRF] ウィンドウの **[インポート（Import）]** オプションまたは DCNM API を使用して VRF を作成すると、次のエラーが表示される場合があります。「インスタンス名が指定されていません。」

このエラーは、タグ付けの問題が原因です。このエラーを削除するには、DCNM Web UI で VRF を編集してから展開します。

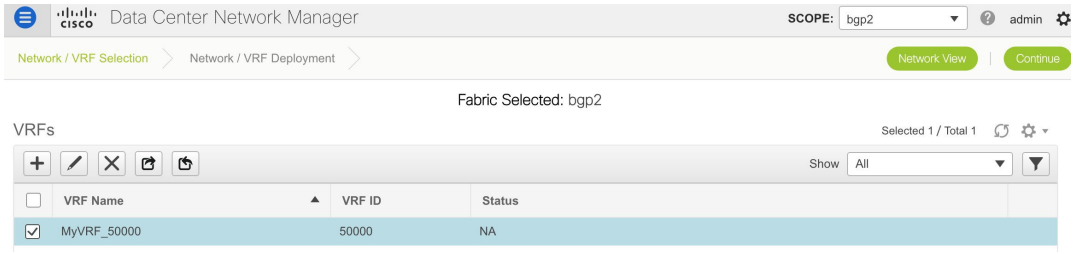


インポートされた VRF が [VRF] 画面に表示されていることがわかります。

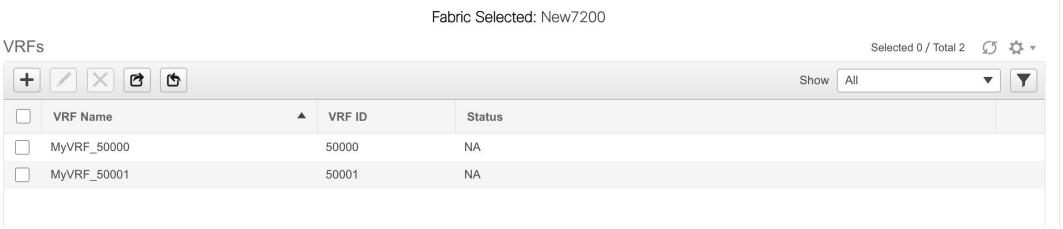


スタンドアロン ファブリック向けの VRF の編集

1. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[VRF（VRFs）]** 画面が更新され、選択したファブリックの VRF が一覧表示されます。



2. **[ファブリックの選択（Select a Fabric）]** ドロップダウンリストから *[スタンドアロン（Standalone）]* を選択し、画面の右上にある **[続行（Continue）]** をクリックします。[ネットワーク（Networks）] ページが表示されます。
3. 画面右上の **[VRF の表示（VRF View）]** をクリックします。VRF ページが表示されます。



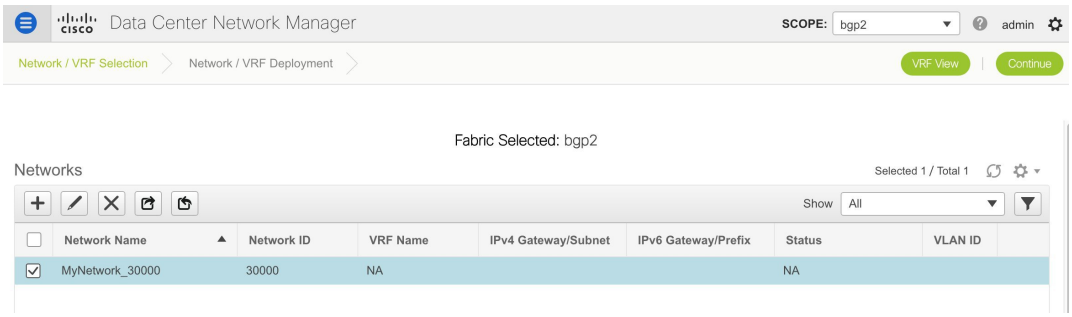
4. **[VRF]** を選択し、画面の左上にある **[編集（Edit）]** オプションをクリックします。**[VRF の編集（Edit VRF）]** 画面が表示されます。
5. 必要に応じて、**[VRF プロファイル（VRF Profile）]** セクションの **[全般（General）]** タブと **[詳細（Advanced）]** タブのフィールドを更新します。
6. 画面の右下の **[保存（Save）]** ボタンをクリックして、アップデートを保存します。

スタンドアロンおよび MSD ファブリック向けネットワークの展開

開始の前に：ファブリックのネットワークが作成されていることを確認します。

1. **[制御（Control）]>[ネットワーク（Networks）]**（**[ファブリック（Fabrics）]** サブメニューの下）をクリックします。

   [ネットワーク（Networks）] 画面が表示されます。
2. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[ネットワーク（Networks）]** 画面が更新され、選択したファブリックのネットワークが一覧表示されます。



3. 展開するネットワークを選択します。この場合、両方のネットワークの横にあるチェックボックスをオンにして、画面の右上にある **[続行（Continue）]** をクリックします。

   [ネットワークの展開（Network Deployment）] ページが表示されます。このページでは、スタンドアロン ファブリックのネットワーク トポロジを確認できます。

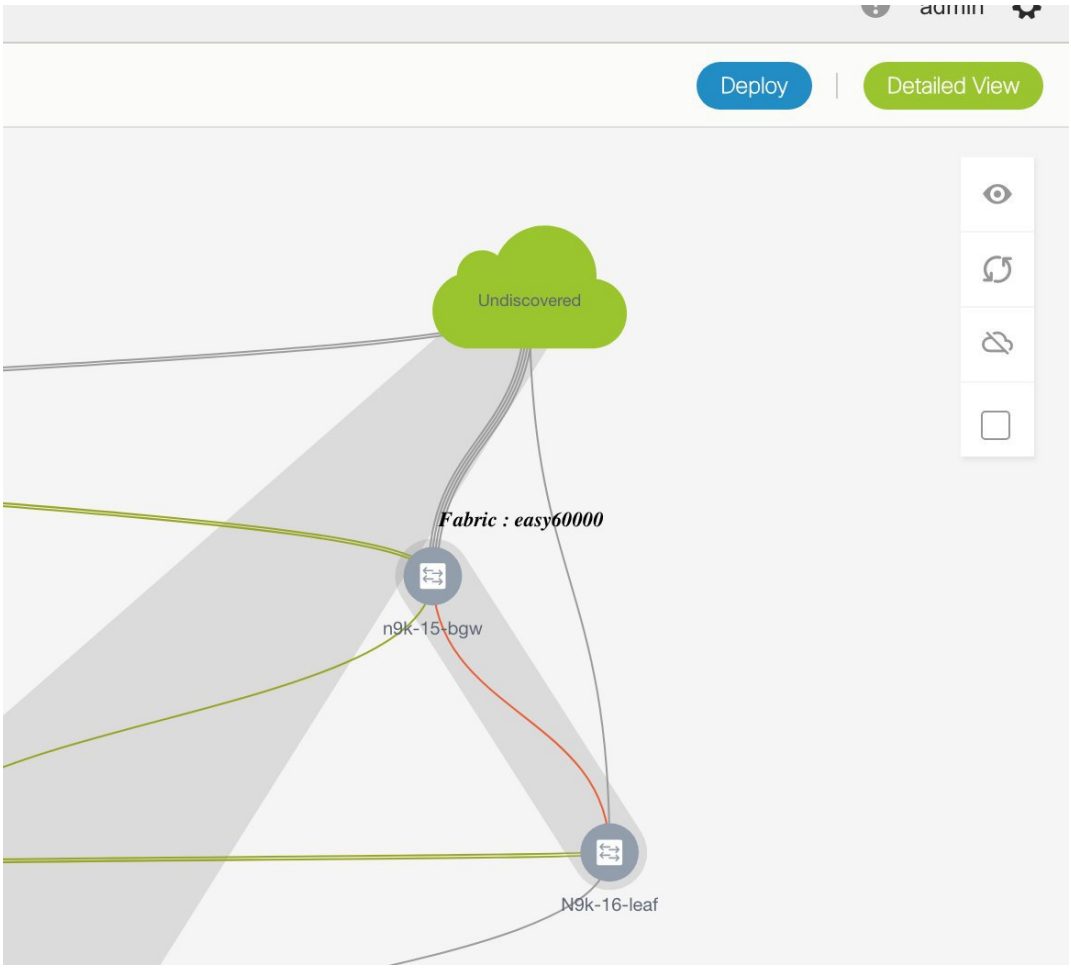
複数のスイッチにネットワークを同時に展開できます。選択したデバイスは、同じロール（リーフ、ボーダーゲートウェイなど）を持つ必要があります。

Note MSD ファブリックでは、すべてのメンバー ファブリックがこの画面から表示されます。

画面の右下に、展開のさまざまな段階を表すカラー コードが表示されます。それに応じてスイッチ アイコンの色が変わります。保留中 の状態は青色、プロビジョニングが進行中の場合の 進行中 は黄色、正常に展開された場合は緑色などです。 DCNM 11.3(1) 以降、保留状態は、保留中の展開または保留中の再計算があることを示します。スイッチをクリックし、**[プレビュー（Preview）]** または **[構成の展開（Deploy Config）]** オプションを使用して保留中の展開を確認するか、**[保存と展開（Save & Deploy）]** をクリックしてスイッチの状態を再計算できます。

オーバーレイ ネットワーク（/VRF）のプロビジョニング ステータスは、コンテキスト固有です。これは、プロビジョニング用に選択したネットワークとトポロジ内の関連するスイッチの組み合わせです。この例では、ネットワーク *MyNetwork_30000* および *MyNetwork_30001* が、このファブリック内のどのスイッチにもまだ展開されていないことを意味します。

[未検出のクラウド（Undiscovered cloud）] の表示：この画面に **[未検出（Undiscovered）]** クラウドを表示（または非表示）するには、画面の右上にある垂直パネルのクラウドアイコンをクリックします。アイコンをクリックすると、**[未検出（Undiscovered）]** クラウドと、選択したファブリック トポロジへのリンクは表示されません。**[未検出（Undiscovered）]** クラウドを表示するためにアイコンを再度クリックします。



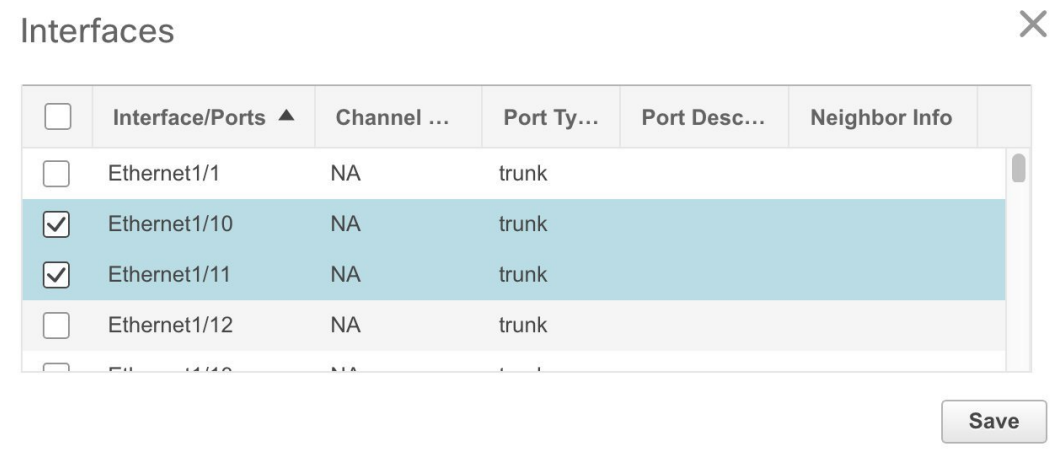
画面上でマウスの左ボタンをクリックし、希望する方向に移動することにより、画面上でトポロジを移動できます。カーソル ローラーを移動することで、スイッチ アイコンを比例して拡大または縮小できます。タッチパッドで対応する代替手段を使用することもできます。

4. **[インターフェイス（Interfaces）]** 列で **[...]** をクリックします。

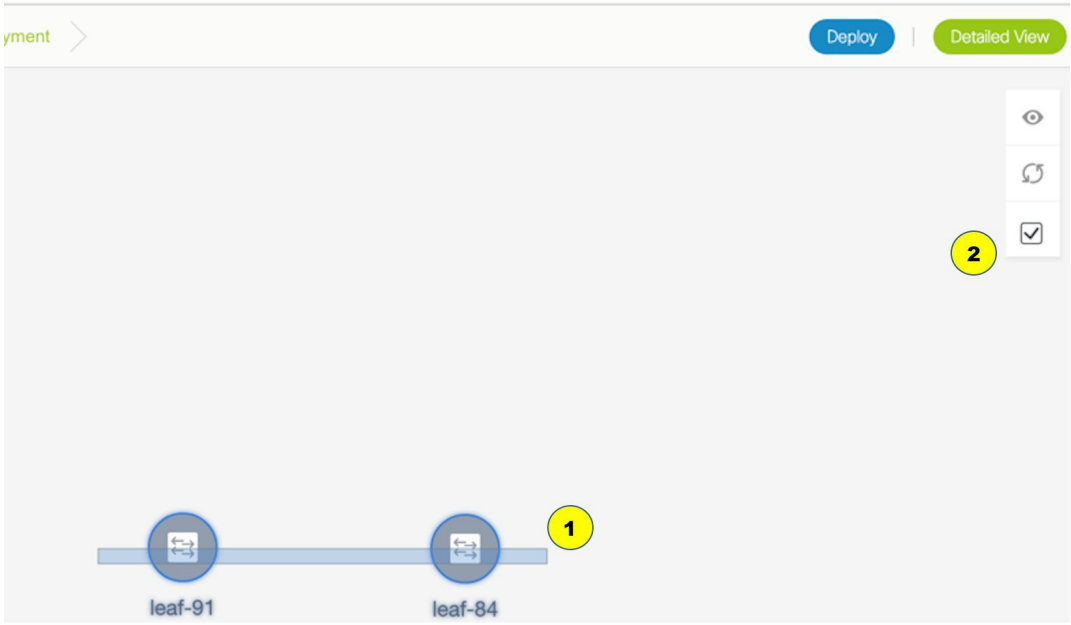
   [インターフェイス（Interfaces）] ボックスが開きます。インターフェイスまたはポートチャネルが一覧表示されます。インターフェイス/ポートチャネルを選択して、選択したネットワークに関連付けることができます。インターフェイスごとに、ポートタイプと説明、チャネル番号、および接続されたネイバーインターフェイスの詳細が表示されます。

   Cisco DCNM リリース 11.5(1) 以降、**[インターフェイス（Interfaces）]** ウィンドウには、インターフェイス グループの一部であるインターフェイスが表示されません。具体的には、トランク ポート、アクセス ポート、および dot1q トンネル ポートです。

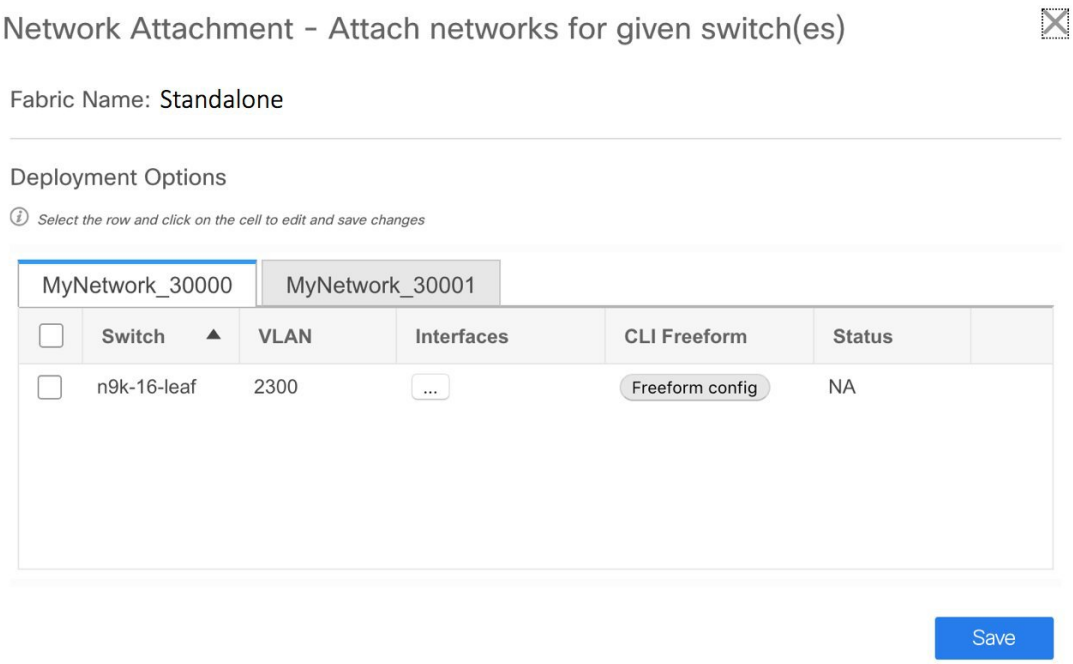
   スイッチへのネットワーク接続を実行しようとしたときに、インターフェイスがインターフェイス グループの一部である場合、適切なエラーが表示されます。



5. スイッチをダブルクリックして、スイッチにネットワークを展開します。複数のスイッチにネットワークを展開するには、画面の右上にあるパネルから [複数選択（Multi-Select）] をクリックし（トポロジが静的な状態に凍結します）、スイッチ間でカーソルをドラッグします。



すぐに [ネットワーク接続（Network Attachment）] ダイアログ ボックスが表示されます。



タブは、展開されている各ネットワークを表します（最初のネットワークがデフォルトで表示されます）。各ネットワーク タブに、スイッチが表示されます。各行はスイッチを表します。

[スイッチ（Switch）] 列の横にあるチェックボックスをクリックし、すべてのスイッチを選択します。ネットワークは、スイッチでプロビジョニングする準備ができています。

VLAN：必要に応じて VLAN ID を更新します。

VLAN ID を更新して、ネットワークの展開プロセスを完了しても、古い VLAN は自動的に削除されません。プロセスを完了するには、ファブリック トポロジ画面に移動し（**[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** をクリックし、対応するファブリック ボックス内をクリックして画面に移動します）、[保存して展開（Save and Deploy）] オプションを使用する必要があります。

特定のネットワークの VLAN ID を更新する場合、元の VLAN ID は接続されたトランク インターフェイスから自動的に削除されません。古いまたは元の VLAN ID を削除するには、ファブリック ビルダのファブリック内から **[保存して展開（Save and Deploy）]** + **[構成展開（Config Deploy）** 操作を実行する必要があります。このためには、ファブリック トポロジ画面に移動し（**[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** をクリックし、対応するファブリック ボックス内をクリックして画面に移動します）、**[保存して展開**（Save and Deploy）] 操作を実行する必要があります。構成コンプライアンスによって必要な構成が削除されていることを確認してから、**[構成の展開（Deploy Config）]** 操作を実行して構成を削除します。

インターフェイス：列の [...] をクリックして、選択したネットワークに関連付けられたインターフェイスを追加します。

VLAN からトランク ポートへのマッピング：選択したトランク ポートには、ポートで許可された VLAN として VLAN が含まれます。

VLAN から vPC ドメインへのマッピング：VLAN を vPC ドメインのポートチャネルに関連付ける場合は、インターフェイスのリストからポートチャネルを追加します。vPC ポートチャネルには、許可された VLAN として VLAN が含まれています。

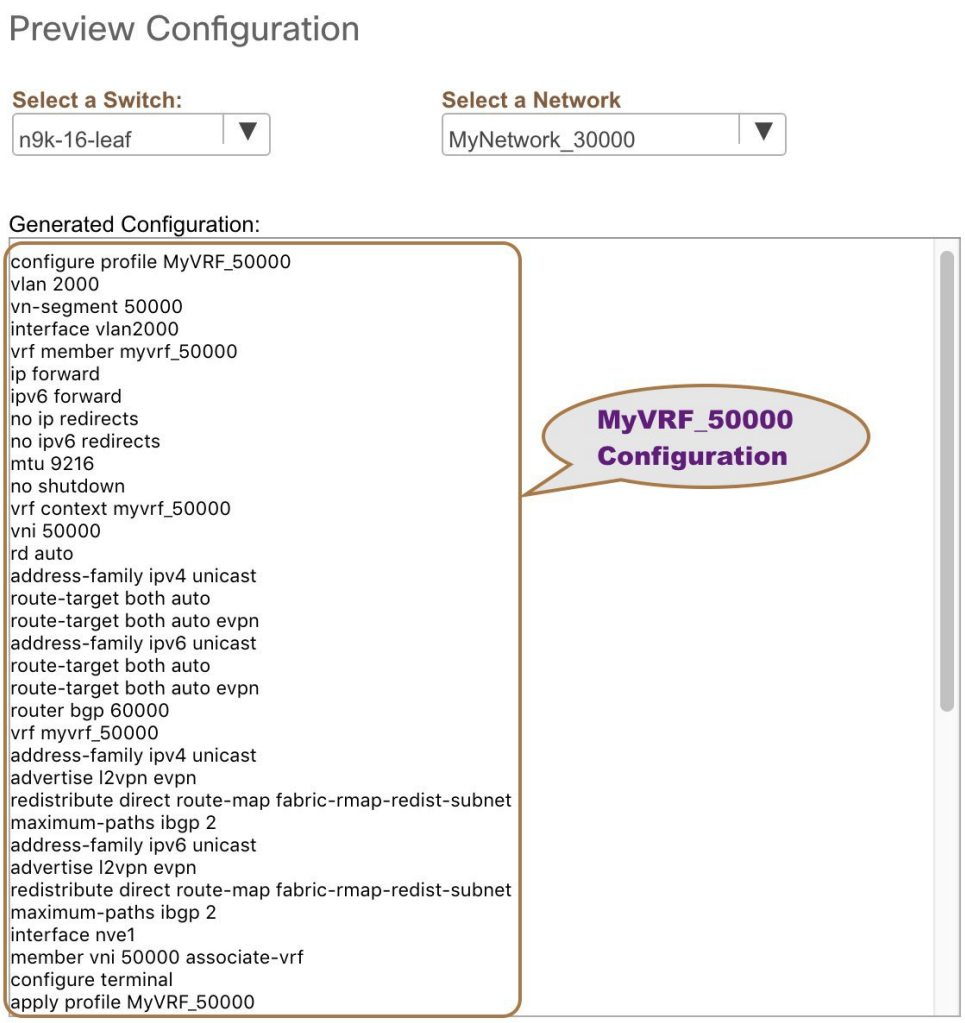
自由形式構成：[自由形式構成（Freeform config）]をクリックして、スイッチで追加の構成を有効にします。構成が保存されると、[自由形式構成（Freeform config）]ボタンが強調表示されます。

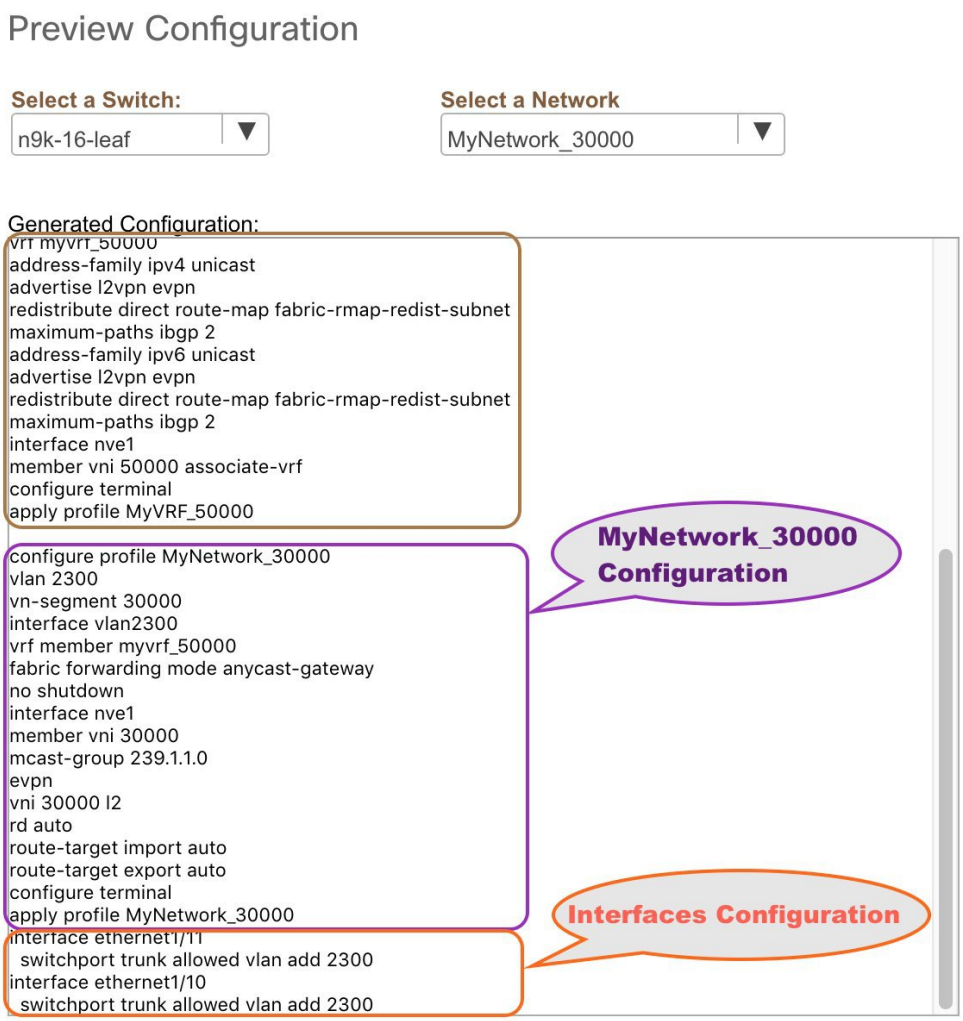
6. 他のネットワーク タブを選択し、同じ選択を行います。
7. **[保存（Save）]**（画面の右下部分）をクリックして、構成を保存します。

Note インターフェイスの追加と削除は、[スイッチの展開（Switches Deploy）]画面の**[インターフェイス（Interfaces）]**列に表示されます。インターフェイス関連の更新（トランク ポートの追加または削除など）はスイッチにプロビジョニングされますが、正しい構成はプレビュー画面に反映されません。トランクまたはアクセス ポートを追加または削除すると、プレビューには、そのネットワーク下のインターフェイスの構成の追加または削除が表示されます。

[トポロジ（Topology）] ウィンドウが再び表示されます。画面の右上にある垂直パネルの *[更新（Refresh）]* をクリックします。スイッチアイコンの青色は、展開が保留中であることを示します。 DCNM 11.3(1) 以降、保留状態は、保留中の展開または保留中の再計算があることを示します。スイッチをクリックし、**[プレビュー（Preview）]** または **[構成の展開（Deploy Config）]** オプションを使用して保留中の展開を確認するか、**[保存と展開（Save & Deploy）]** をクリックしてスイッチの状態を再計算できます。

8. *[プレビュー（Preview）]*（[複数選択（Multi-Select）] オプションの上にある目のアイコン）をクリックして、構成をプレビューします。*MyNetwork_30000* と *MyNetwork_30001* は VRF *50000* のネットワークであるため、構成には VRF 構成とそれに続くネットワーク構成が含まれます。


Preview Configuration
Select a Switch:
n9k-16-leaf
Select a Network
MyNetwork_30000
Generated Configuration:
configure profile MyVRF_50000
vlan 2000
vn-segment 50000
interface vlan2000
vrf member myvrf_50000
ip forward
ipv6 forward
no ip redirects
no ipv6 redirects
mtu 9216
no shutdown
vrf context myvrf_50000
vni 50000
rd auto
address-family ipv4 unicast
route-target both auto
route-target both auto evpn
address-family ipv6 unicast
route-target both auto
route-target both auto evpn
router bgp 60000
vrf myvrf_50000
address-family ipv4 unicast
advertise l2vpn evpn
redistribute direct route-map fabric-rmap-redist-subnet
maximum-paths ibgp 2
address-family ipv6 unicast
advertise l2vpn evpn
redistribute direct route-map fabric-rmap-redist-subnet
maximum-paths ibgp 2
interface nve1
member vni 50000 associate-vrf
configure terminal
apply profile MyVRF_50000
MyVRF_50000
Configuration

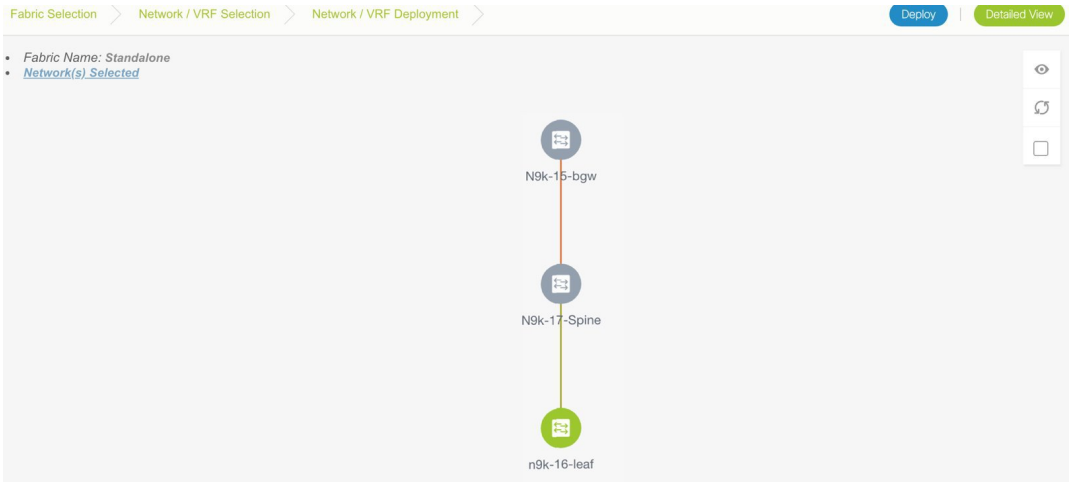


プレビュー画面では、画面上部の **[スイッチの選択（Select a switch）]** および **[ネットワークの選択（Select a network）]** ドロップダウンボックスから選択して、他のネットワーク構成を表示できます。

構成を確認したら、画面を閉じます。[トポロジ（Topology）] 画面が再び表示されます。

9. 画面の右上にある **[展開（Deploy）]** をクリックします。スイッチアイコンの色が黄色に変わり、画面の右下に展開が進行中であることを示すメッセージが表示されます。ネットワークの展開が完了すると、スイッチアイコンの色が緑に変わり、展開が成功したことを示します。

Note **[展開（Deploy）]** をクリックして、展開する必要のある構成差分がない場合は、**[展開保留中のスイッチなし（No switches PENDING for deployment）]** と示すポップアップ ウィンドウが表示されます。



Note スイッチのステータスは、選択したネットワークまたは次の階層の VRF の集約ステータスによって決定されます：**[保留中（Pending）]**、**[進行中（In Progress）]**、**[同期していない/失敗（Out-of-Sync/Failed）]**、**[同期中/成功（In Sync/Success）]**、**[不明/NA（Unknown/NA）]**。たとえば、いずれかのネットワークまたは VRF のステータスが **Out-of-Sync/Failed** で、他のネットワークまたは VRF が **[保留中（Pending）]** または **[進行中（In Progress）]** のステータスでない場合、スイッチのステータスは **[同期していない/失敗（Out-of-Sync/Failed）]** です。ステータスが不明の場合、デフォルトのステータスは **[不明/NA（Unknown/NA）]** です。

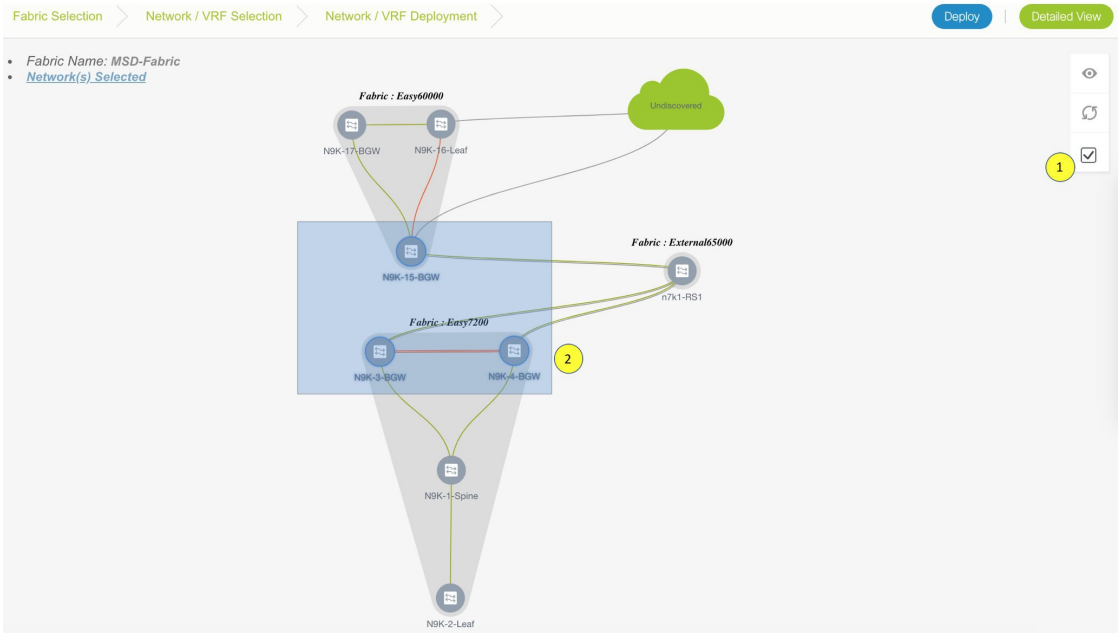
[ネットワーク（Network）] ページに移動して、すべてのネットワークの個々のステータスを表示します。

[MSD ファブリックのネットワーク展開（Network Deployment for an MSD Fabric）]

異なるメンバー ファブリック ボーダー デバイスに同じネットワークを展開しているシナリオを検討してください。1つのファブリックを選択し、そのボーダーデバイスにネットワークを展開してから、2 番目のファブリックを選択してネットワークを展開できます。

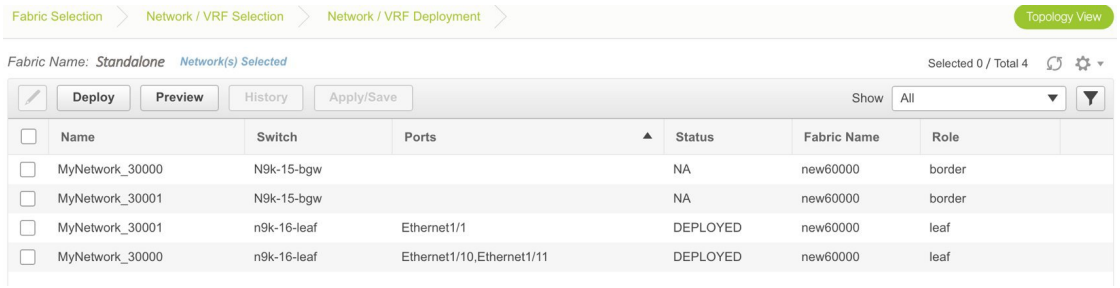
または、MSD ファブリックを選択し、すべてのメンバー ファブリック ボーダー デバイスの単一トポロジ表示からネットワークを展開できます。

これは、MSD ファブリックのトポロジ表示であり、2 つのメンバー ファブリック トポロジとそれらの接続が示されています。ファブリックの BGW にネットワークを一度に展開できます。



[詳細表示（Detailed view）]

[詳細表示（Detailed View）] オプションを使用して、ネットワークと VRF を展開することもできます。画面右上の **[詳細表示（Detailed View）]** をクリックします。[詳細表示（Detailed View）] ウィンドウが表示されます。これにより、表形式ビューでネットワークが一覧表示されます。



次のオプションがあります。

編集：ネットワークを選択し、画面の左上にある [編集（Edit）] アイコンをクリックします。

Note ネットワーク/スイッチ エントリを 1 つ選択して [編集（Edit）] をクリックすると、[ネットワーク接続（Network Attach）] ダイアログ ボックスが表示されます。[トポロジ表示（Topology View）] 画面と [詳細表示（Detailed View）] 画面の間で一貫性を維持するために、ネットワーク接続画面には、選択したネットワーク/スイッチ エントリだけでなく、すべてのネットワークが表示されます。

プレビュー：[プレビュー（Preview）] をクリックして、展開をする前に構成をプレビューします。プレビューできるのは保留中の構成のみであり、開始されていない構成や展開された構成はプレビューできません。

展開：[展開（Deploy）] をクリックして、ネットワークをスイッチにプロビジョニングします。

履歴：行を選択し、[履歴（History）] をクリックして、構成インスタンスとステータスを表示します。ネットワークおよび VRF に関する構成が表示されます。詳細については、任意のインスタンスの [ステータス（Status）] 列をクリックします。

テーブルのフィールドには、各行の構成インスタンス、関連するスイッチとファブリックの名前、スイッチのロール、トランク ポート（ある場合）、および展開ステータスが含まれています。

クイック アタッチ：ネットワークを選択し、**[クイック アタッチ（Quick Attach）]** をクリックします。 確認ウィンドウが表示されます。**[OK]** をクリックします。選択したスイッチにネットワークが接続されます。

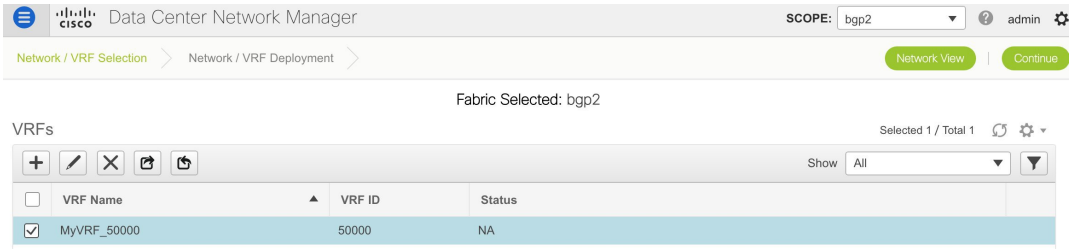
クイック アタッチ解除：ネットワークを選択し、**[クイック アタッチ解除（Quick Detach）]** をクリックします。 確認ウィンドウが表示されます。**[OK]** をクリックします。選択したスイッチからネットワークが切り離されます。

[詳細表示（Detailed View）] ページでは、ネットワーク プロファイルの構成履歴が表示されます。特定のトランク インターフェイスをそのネットワークに関連付けている場合、インターフェイス構成は別個の構成インスタンスとして表示されます。

Note 以前のリリース（DCNM 10.4[2] など）から DCNM 11.0(1) リリースにアップグレードすると、以前の DCNM リリースからのオーバーレイ ネットワークおよび VRF 展開履歴情報は保持されません。

スタンドアロンおよび MSD ファブリック向け VRF の展開

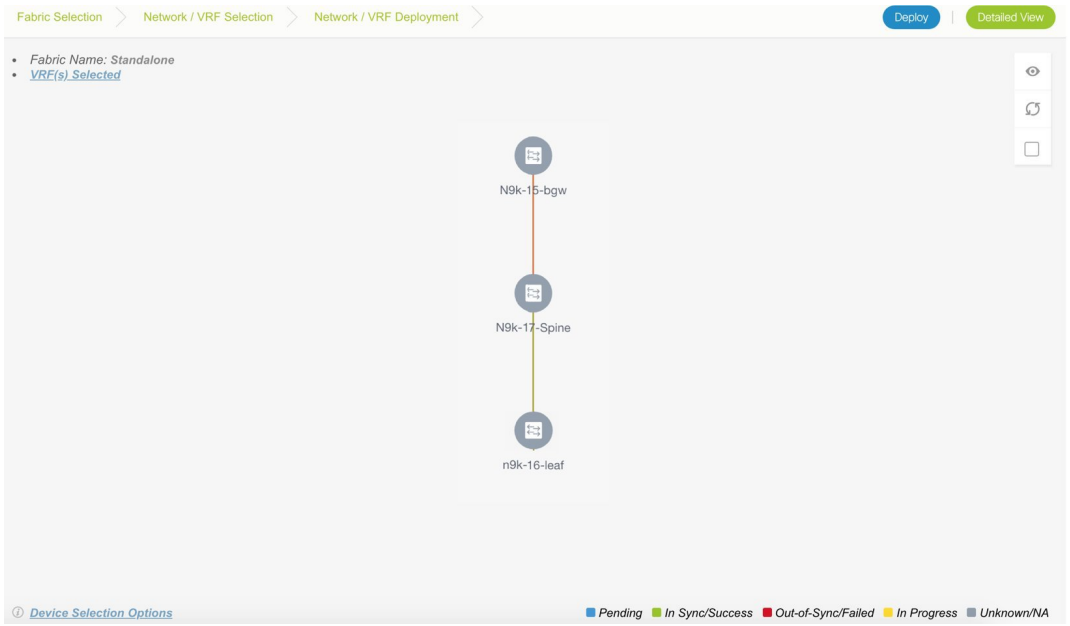
1. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[VRF（VRFs）]** 画面が更新され、選択したファブリックの VRF が一覧表示されます。



2. 展開する VRF の横にあるチェックボックスをオンにして、画面の右上にある [続行（Continue）] をクリックします。

[VRF 展開（VRF Deployment）] 画面が表示されます。このページでは、スタンドアロンファブリックのトポロジを確認できます。次の例は、リーフスイッチに VRF MyVRF_50000

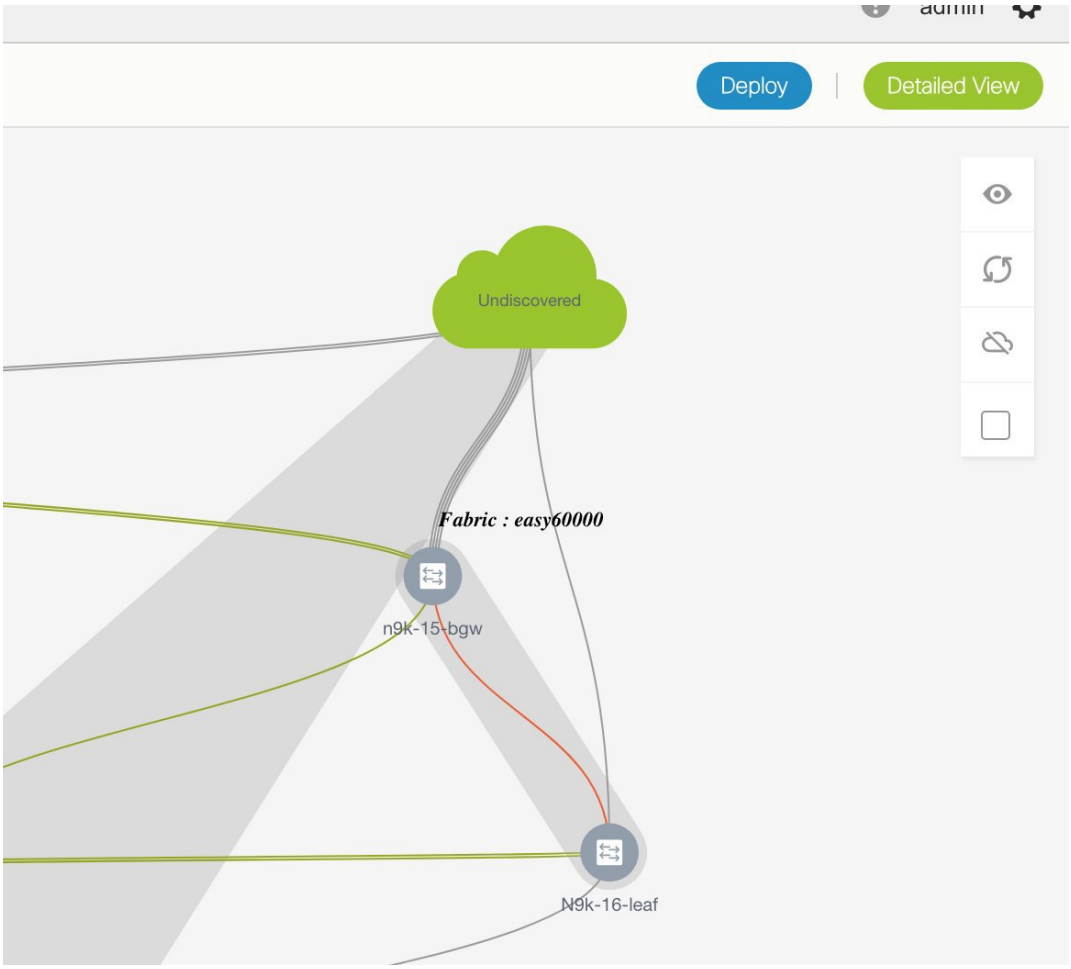
およびMyVRF_50001を展開する方法を示しています。複数のスイッチに同時にVRFを展開できますが、ロールは同じです（リーフ、ボーダーゲートウェイなど）。



画面の右下に、展開のさまざまな段階を表すカラーコードが表示されます。それに応じてスイッチ アイコンの色が変わります。保留中 の状態は青色、プロビジョニングが 進行中 の場合は黄色、失敗状態の場合は赤色、正常に展開された場合は緑色です。 DCNM 11.3(1) 以降、保留状態は、保留中の展開または保留中の再計算があることを示します。スイッチをクリックし、**[プレビュー（Preview）]** または **[構成の展開（Deploy Config）]** オプションを使用して保留中の展開を確認するか、**[保存と展開（Save & Deploy）]** をクリックしてスイッチの状態を再計算できます。

オーバーレイ ネットワーク（または VRF）のプロビジョニング ステータスは、コンテキスト固有です。これは、プロビジョニング用に選択した VRF とトポロジ内の関連するスイッチの組み合わせです。この例では、VRF がこのファブリックのどのスイッチにもまだ展開されていないことを意味します。

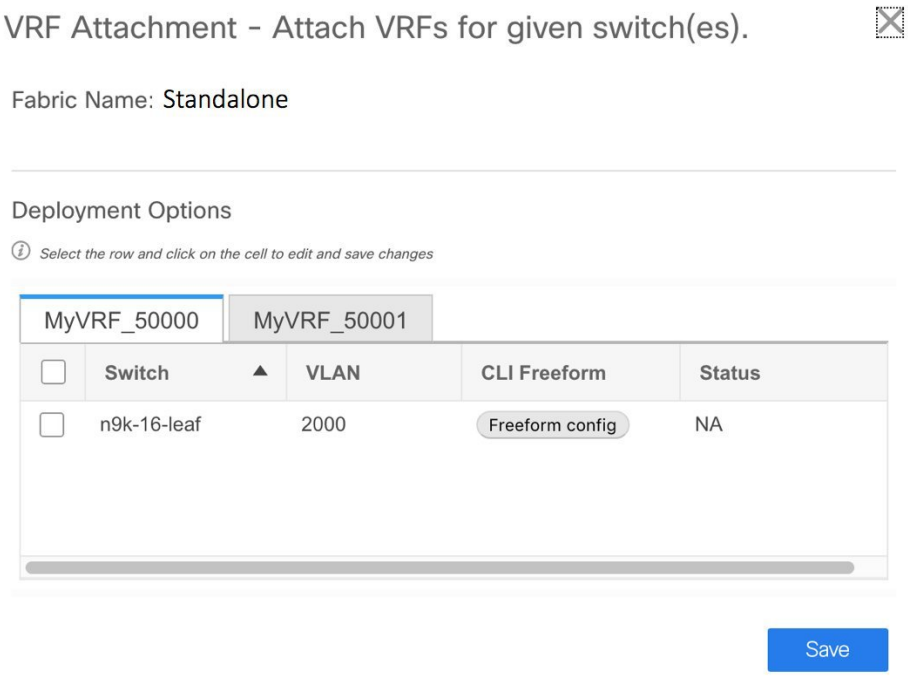
[未検出のクラウド（Undiscovered cloud）] の表示：この画面に **[未検出（Undiscovered）]** クラウドを表示（または非表示）するには、画面の右上にある垂直パネルのクラウドアイコンをクリックします。アイコンをクリックすると、**[未検出（Undiscovered）]** クラウドと、選択したファブリック トポロジへのリンクは表示されません。**[未検出（Undiscovered）]** クラウドを表示するためにアイコンを再度クリックします。



画面上でマウスの左ボタンをクリックし、希望する方向に移動することにより、画面上でトポロジを移動できます。カーソル ローラーを移動することで、スイッチ アイコンを比例して拡大または縮小できます。タッチパッドで対応する代替手段を使用することもできます。

3. スイッチをダブルクリックして、スイッチに VRF を展開します。[VRF アタッチメント（VRF Attachment）] 画面が表示されます。

Note 複数のスイッチに VRF を展開するには、画面の右上部分にあるパネルから [複数選択（Multi-Select）] オプションをクリックし（これにより、トポロジが静的な状態に凍結します）、スイッチ間でカーソルをドラッグします。



タブは、展開されている各 VRF を表します（最初に選択された VRF がデフォルトで表示されます）。各 VRF タブには、選択したスイッチが表示されます。各行はスイッチを表します。

VLAN ID：必要に応じて、VLAN 列内をクリックして VRF VLAN ID を更新します。

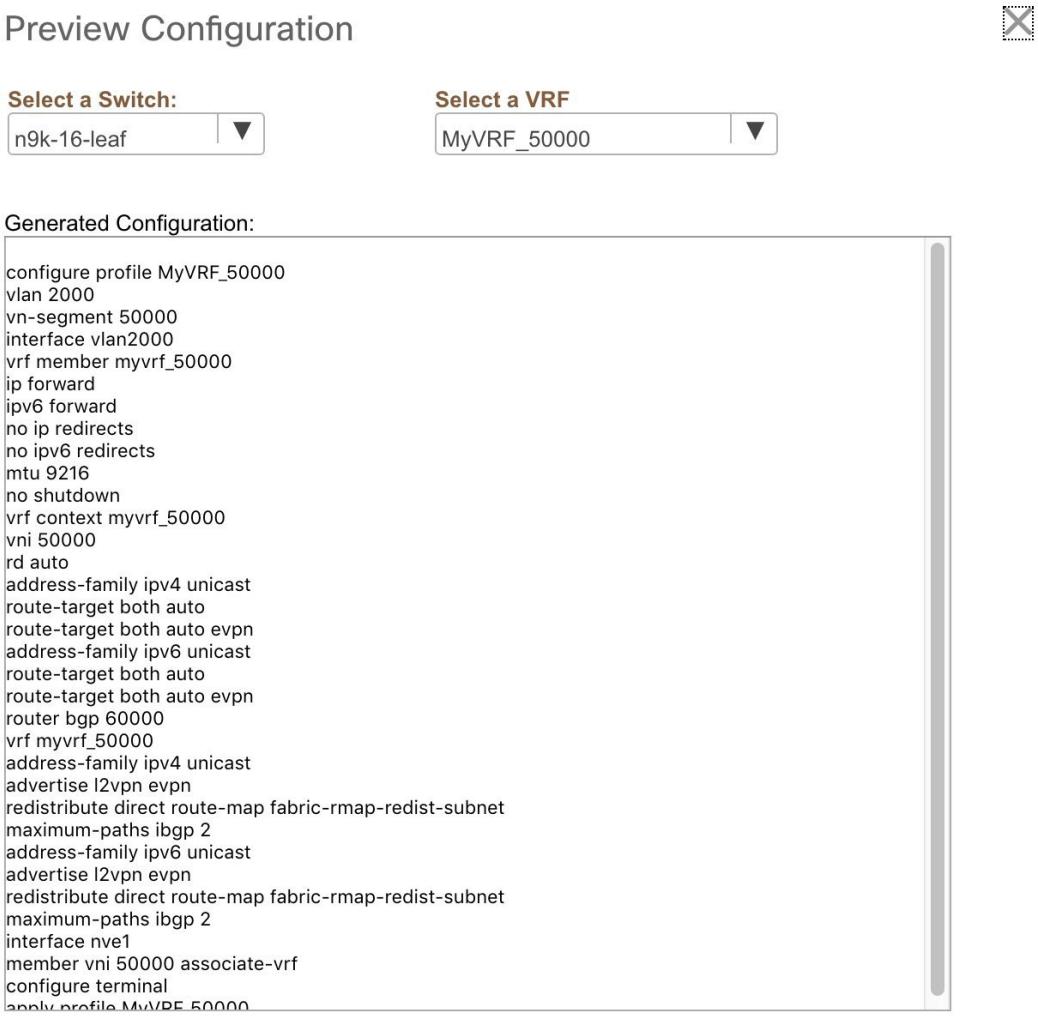
自由形式構成：[自由形式構成（Freeform config）] をクリックして、スイッチで追加の構成を有効にします。自由形式構成を保存すると、[自由形式構成（Freeform config）] ボタンが強調表示されます。

[スイッチ（Switch）] 列の横にあるチェックボックスをクリックし、すべてのスイッチを選択します。VRF MyVRF_50000 は、スイッチでプロビジョニングする準備ができています

4. 他の VRF タブを選択し、同じ選択を行います。
5. **[保存（Save）]**（画面の右下部分）をクリックして、VRF 構成を保存します。

   トポロジ画面が再び起動します。画面の右上にある垂直パネルの *[更新（Refresh）]* ボタンをクリックします。スイッチ アイコンの青色は、展開が保留中であることを示します。DCNM 11.3(1) 以降、保留状態は、保留中の展開または保留中の再計算があることを示します。スイッチをクリックし、**[プレビュー（Preview）]** または **[構成の展開（Deploy Config）]** オプションを使用して保留中の展開を確認するか、**[保存と展開（Save & Deploy）]** をクリックしてスイッチの状態を再計算できます。

   [プレビュー（Preview）] ボタン（*[複数選択（Multi-Select）]* オプションの上にある目のアイコン）をクリックして、構成をプレビューします。



構成を確認したら、画面を閉じます。*[*トポロジ表示（*Topology View*）*]* 画面が表示されます。

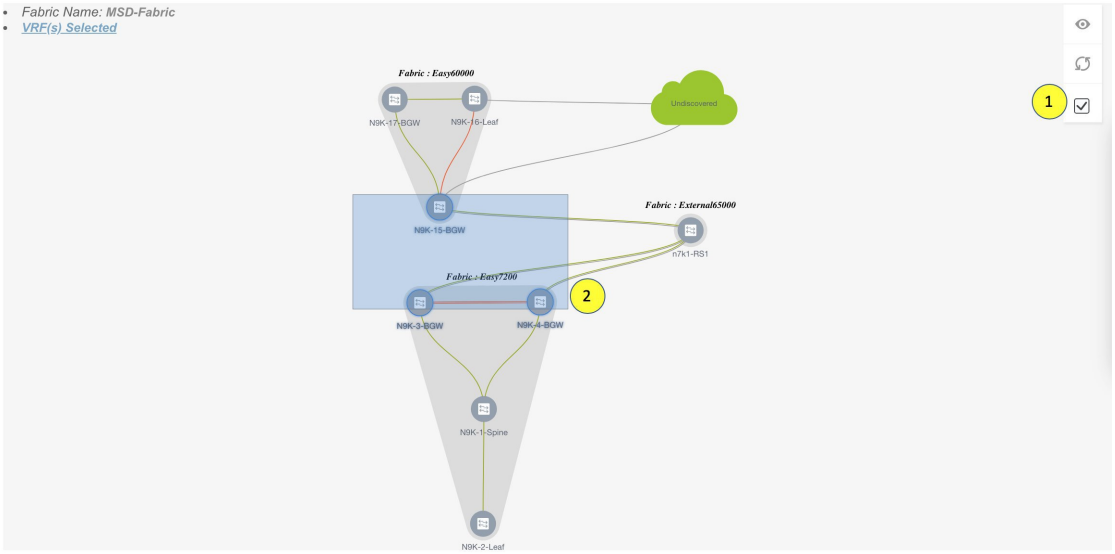
6. 画面右上の **[展開（Deploy）]** ボタンをクリックします。スイッチアイコンの色が黄色に変わり、画面の右下に展開が進行中であることを示すメッセージが表示されます。VRF の展開が完了すると、スイッチアイコンの色が緑に変わり、展開が成功したことを示します。

Note **[展開（Deploy）]** をクリックして、展開する必要のある構成差分がない場合は、**[展開保留中のスイッチなし（No switches PENDING for deployment）]** と示すポップアップ ウィンドウが表示されます。

[MSD ファブリックの VRF 展開（VRFs Deployment for an MSD Fabric）]

異なるメンバー ファブリック ボーダー デバイスに同じ VRF を展開しているシナリオを検討してください。1 つのファブリックを選択し、そのボーダー デバイスに VRF を展開してから、2 番目のファブリックを選択して VRF を展開できます。

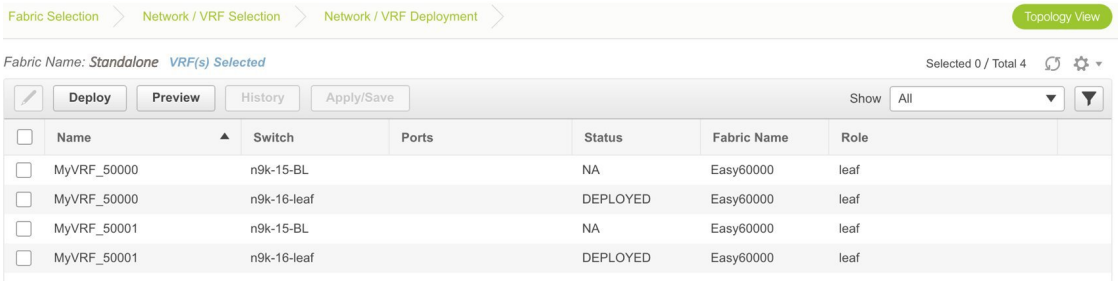
または、MSD ファブリックを選択し、すべてのメンバー ファブリック ボーダー デバイスの単一トポロジ表示から VRF を一度に展開できます。



詳細ビュー

[詳細表示（Detailed View）] ボタンを使用して、ネットワークと VRF を展開することもできます。

画面右上の **[詳細表示（Detailed View）]** をクリックします。[詳細表示（Detailed View）] 画面が表示されます。これにより、表形式ビューで VRF が一覧表示されます。



次のオプションがあります。

編集：VRF を選択し、画面の左上にある [編集（Edit）] アイコンをクリックします。

Note 1 つの VRF/スイッチ エントリを選択すると、VRF 接続画面が表示されます。[トポロジ表示（Topology View）] 画面と [詳細表示（Detailed View）] 画面の間で一貫性を維持するために、VRF 接続画面には、選択した VRF/スイッチエントリだけでなく、すべての VRF が表示されます。

プレビュー：[プレビュー（Preview）] をクリックして、展開をする前に構成をプレビューします。プレビューできるのは保留中の構成のみであり、開始されていない構成や展開された構成はプレビューできません。

展開：[展開（Deploy）] をクリックして、VRF をスイッチにプロビジョニングします。

履歴：行を選択し、[履歴（History）] をクリックして、構成インスタンスとステータスを表示します。ネットワークおよび VRF に関する構成が表示されます。詳細については、任意のインスタンスの [ステータス（Status）] 列をクリックします。

テーブルのフィールドには、各行の構成インスタンス、関連するスイッチとファブリックの名前、スイッチのロール、および展開ステータスが含まれています。

クイック アタッチ：VRF を選択し、**[クイック アタッチ（Quick Attach）]** をクリックします。確認ウィンドウが表示されます。**[OK]** をクリックします。選択したスイッチに VRF が接続されます。

クイック アタッチ解除：VRF を選択し、**[クイック アタッチ解除（Quick Detach）]** をクリックします。確認ウィンドウが表示されます。**[OK]** をクリックします。選択したスイッチから VRF が切り離されます。

Note 以前のリリース（DCNM 10.4[2] など）から DCNM 11.0(1) リリースにアップグレードすると、以前の DCNM リリースからのオーバーレイ ネットワークおよび VRF 展開履歴情報は保持されません。

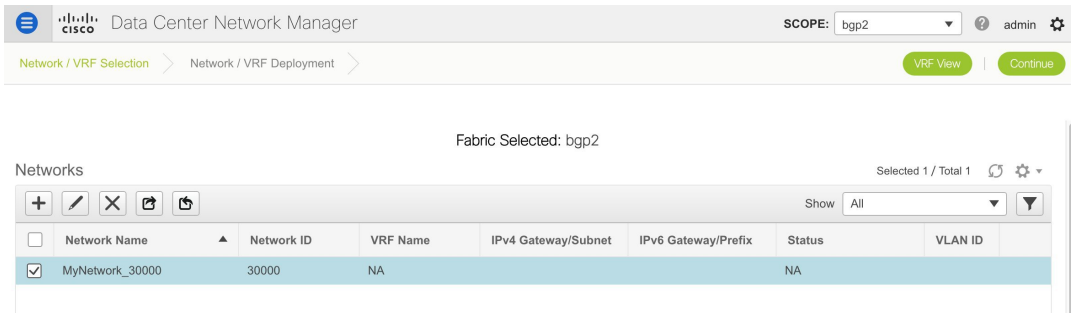
スタンドアロン ファブリック向けのネットワークの展開解除

展開画面から VRF とネットワークを展開解除できます。展開解除の DCNM 画面フローは、展開プロセス フローに似ています。展開画面（トポロジ表示）に移動して、ネットワークの展開を解除します。

1. **[制御（Control）]>[ネットワーク（Networks）]（[ファブリック（Fabrics）]** サブメニューの下）をクリックします。

   [ネットワーク（Networks）] 画面が表示されます。

2. [範囲（SCOPE）] から正しいファブリックを選択してください。ファブリックを選択すると、**[ネットワーク（Networks）]** 画面が更新され、選択したファブリックのネットワークが一覧表示されます。



3. 展開解除するネットワークを選択し、[続行（Continue）] をクリックします。トポロジ表示が表示されます。
4. 複数のスイッチからネットワークを展開解除する場合は、[複数選択（Multi-Select）] ボタンを選択し、同じロールを持つスイッチ間でカーソルをドラッグします。[ネットワーク接続（Network Attachment）] 画面が表示されます。

   （単一のスイッチの場合、スイッチをダブルクリックすると、[ネットワーク接続（Network Attachment）] 画面が表示されます）。

   （単一のスイッチの場合、スイッチをダブルクリックすると、[スイッチ展開（Switches Deploy）] 画面が表示されます）。
5. [ネットワーク接続（Network Attachment）] 画面で、展開されたネットワークの [ステータス（Status）] 列が [展開済み（DEPLOYED）] と表示されます。必要に応じて、スイッチの横にあるチェックボックスをオフにします。各タブはネットワークを表すため、すべてのタブでこれを繰り返します。
6. **[保存（Save）]**（画面の右下部分）をクリックして、ネットワークの展開解除を開始します。トポロジ表示 が再び表示されます。

Note または、**[詳細表示（Detailed View）]** ボタンをクリックして、ネットワークを展開解除することもできます。

7. 画面を更新し、必要に応じて構成をプレビューし、**[展開（Deploy）]** をクリックしてスイッチのネットワーク構成を削除します。スイッチアイコンが緑色に変わったら、展開解除が成功したことを示します。
8. [ネットワーク（Networks）] ページに移動して、ネットワークが展開されていないかどうかを確認します。

スタンドアロン ファブリック向けの VRF の展開解除

展開画面から VRF を展開解除できます。展開解除の DCNM 画面フローは、展開プロセス フローに似ています。

1. **[制御（Control）] > [ファブリック（Fabrics）] > [VRF]** を選択します。

2. **[範囲（SCOPE）]**から正しいファブリックを選択してください。ファブリックを選択すると、**[VRF]** 画面が更新され、選択したファブリックのネットワークが一覧表示されます。
3. 展開解除する VRF を選択し、**[続行（Continue）]** をクリックします。*[*トポロジ表示（*Topology View*）*]* ページが表示されます。
4. 複数のスイッチから VRF を展開解除する場合は、Multi-Select オプションを選択し、同じロールを持つスイッチ間でカーソルをドラッグします。[VRF アタッチメント（VRF Attachment）] 画面が表示されます。

   （単一のスイッチの場合、スイッチをダブルクリックすると、VRF 接続画面が表示されます）。
5. [スイッチの展開（Switches Deploy）] 画面で、展開された VRF の **[ステータス（Status）]** 列が [展開済み（DEPLOYED）] と表示されます。必要に応じて、スイッチの横にあるチェックボックスをオフにします。各タブは VRF を表すため、すべてのタブでこれを繰り返します。
6. **[保存（Save）]**（画面の右下部分）をクリックして、VRF の展開解除を開始します。トポロジ表示が再び表示されます。

Note または、**[詳細表示（Detailed View）]** ボタンをクリックして、VRF を展開解除することもできます。

7. 画面を更新し、必要に応じて構成をプレビューし、**[展開（Deploy）]**をクリックしてスイッチの VRF 構成を削除します。スイッチ アイコンが緑色に変わったら、展開解除が成功したことを示します。
8. [VRF] ページに移動して、ネットワークが展開されていないかどうかを確認します。

ネットワークおよび VRF の削除

MSD ファブリック内のネットワークおよび対応する VRF を削除するには、次の手順に従います。

1. ネットワークを展開解除します（まだ実行していない場合）。
2. ネットワークを削除します。
3. VRF を展開解除します（まだ実行していない場合）。
4. VRF を削除します。

複数の VLAN ID を単一の VNI に構成する

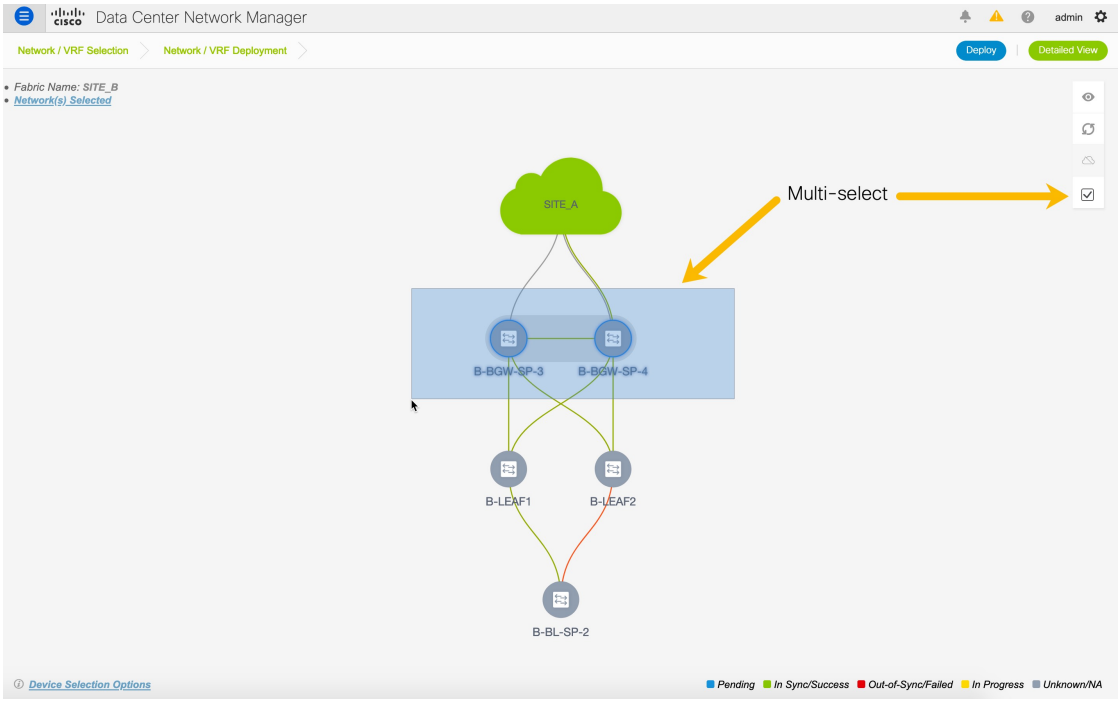
次の手順は、DCNM で複数の VLAN ID を単一の VNI にタグ付けする方法を示しています。

手順

ステップ 1 **[制御（Control）] > [ネットワーク（Networks）]** に移動します。

ステップ 2 **[範囲（SCOPE）]** ドロップダウンリストからファブリックを選択し、ネットワークを選択します。**[続行（Continue）]**をクリックします。

ステップ 3 **[複数選択（Multi-Select）]** チェックボックスをオンにして、VLAN ID で更新する必要があるスイッチの上にカーソルをドラッグします。



ステップ 4 **[ネットワーク接続（Network Attachment）]** ウィンドウで、スイッチの VLAN ID を編集し、**[保存（Save）]** をクリックします。

ステップ 5 構成を展開するには、**[展開（Deploy）]** をクリックします。

Cisco DCNM の拡張された役割別のアクセス制御

Cisco DCNM リリース 11.4（1）から、次のロールベース アクセス コントロール（RBAC）の変更を確認できます。

- **network-operator** ユーザー ロールの Cisco DCNM Web UI および API への読み取り専用アクセス
- **network-stager** と呼ばれる新しいユーザー ロール。
- **network-admin**ロールを持つユーザーとして、DCNM 内の特定のファブリックまたはすべてのファブリックの展開をフリーズします。

Cisco DCNM リリース 11.5（1））から、新しいユーザー ロール、**device-upg-admin**、および **access-admin** が追加されていることがわかります。

（注） 選択したユーザー ロールで実行できないアクションはグレー表示されます。

また、ネットワーク ステージャによって実行される操作の一部と、Cisco DCNM でファブリックを凍結する方法についてのビデオを見ることもできます。[拡張されたロールベース アクセス コントロール（RBAC）（Enhanced Role-based Access Control (RBAC)）]ビデオを参照してください。

Device-upg-admin ロール

[device-upg-admin] ロールを持つユーザーは、**[イメージ管理（Image Management）]** ウィンドウでのみ操作を実行できます。

詳細については、イメージ管理 （491 ページ）を参照してください。

Access-admin ロール

[access-admin] ロールを持つユーザーは、すべてのファブリックの **[インターフェイス マネージャ（Interface Manager）]** ウィンドウでのみ操作を実行できます。

access-admin は次のアクションを実行できます。

- レイヤ 2 ポート チャネル、および vPC を追加、編集、削除、展開します。
- ホスト vPC、およびイーサネット インターフェイスを編集します。
- 管理インターフェイスからの保存、プレビュー、および展開。
- LAN クラシック ファブリックのインターフェイスを編集します。

nve、管理、トンネル、サブインターフェイス、SVI、インターフェイス グループ、およびループバック インターフェイスを除く

ただし、access-admin ロールを持つユーザーは、次のアクションを実行できません。

- レイヤ 3 ポートチャネル、ST FEX、AA FEX、ループバック インターフェイス、nve インターフェイス、およびサブインターフェイスは編集できません。
- レイヤ 3、ST FEX、AA FEX のメンバー インターフェイスおよびポート チャネルは編集できません。
- Easy ファブリック用に、アンダーレイとリンクから関連付けられたポリシーを持つインターフェイスは編集できません。
- ピア リンク ポート チャネルを編集できません。
- 管理インターフェイスを編集できません。
- トンネルを編集できません。

（注） ファブリックまたは DCNM が deployment-freeze モードの場合、このロールのアイコンとボタンはグレー表示されます。

Network-Operator ロール

[network-operator] ロールを持つユーザーは、DCNM Web UI の次のメニューにアクセスできます。

- ダッシュボード
- トポロジ
- モニタ（Monitor）
- アプリケーション

Cisco DCNM リリース 11.4(1) 以降、このロールを持つユーザーは、**[制御（Control）]** メニューへの読み取り専用アクセスもできます。

ネットワーク オペレータは、ファブリック ビルダー、ファブリック設定、構成のプレビュー、ポリシー、およびテンプレートを表示できます。ただし、ネットワーク オペレータは次の操作を実行できません。

- ファブリック内のスイッチの予期される構成を変更できません。
- スイッチに構成を展開できません。
- ライセンス、追加ユーザの作成などの管理オプションにアクセスできません。

Network-Stager ロール

network-stager ロールを持つユーザーは、DCNM で構成を変更できます。network-admin ロールを持つユーザーは、これらの変更を後で展開できます。ネットワーク ステージャは、次のアクションを実行できます。

- インターフェイス構成を編集します。
- ポリシーを表示または編集します。
- インターフェイスを作成します。
- ファブリック設定を変更します。
- テンプレートを編集または作成します。

ただし、ネットワーク ステージャは次のアクションを実行できません。

- スイッチに設定を展開できません。
- DCNM Web UI または REST API から展開関連のアクションを実行できません。
- ライセンス、追加ユーザの作成などの管理オプションにアクセスできません。
- メンテナンス モードの切り替えはできません。
- 展開フリーズモードでファブリックを移動したり、展開モードから解放したりすることはできません。
- パッチをインストールします。
- スイッチをアップグレードできません。
- ファブリックを作成または削除できません。
- スイッチをインポートまたは削除できません。

ネットワーク オペレータとネットワーク ステージャの違いは、ネットワーク ステージャとして、既存のファブリックのインテントのみを定義できますが、それらの構成を展開できないことです。

[network-stager] ロールを持つユーザーがステージングした変更および編集を展開できるのは、ネットワーク管理者だけです。

ポリシー変更履歴の表示

異なるユーザーは、DCNM でスイッチの予期される構成を同時に変更できます。**[ポリシー変更履歴（Policy Change History）]** タブでこれらの段階的な変更履歴を表示できます。展開履歴は、DCNM からスイッチにプッシュまたは展開された変更をキャプチャします。

（注） 非 Nexus デバイスでは、展開履歴のみがサポートされます。

さまざまなユーザーによる変更を表示するには、次の手順を実行します。

手順

ステップ 1 **[network-admin]**、**[network-stager]**、または **[network-operator]** のユーザーロールで Cisco DCNM にログインします。

ステップ 2 ファブリック トポロジ ウィンドウに移動します。

ステップ 3 履歴を変更する対象のスイッチを右クリックします。

ステップ 4 **[履歴（History）]** を選択します。

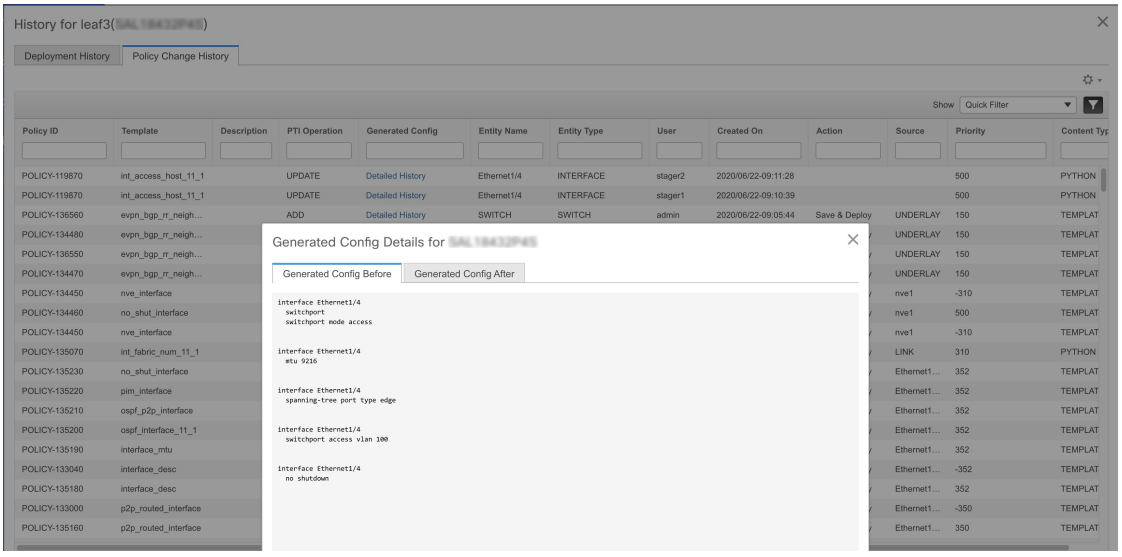
ステップ 5 **[ポリシー変更履歴（Policy Change History）]** タブをクリックします。

ステップ 6 **[生成された構成（Generated Config）]** 列で変更を加えたインターフェイスを検索します。

ステップ 7 **[PTI 操作（PTI Operation）]** 列には、さまざまなユーザーによって行われた変更の値 **[UPDATE]** が含まれます。

ステップ 8 **[ユーザー（User）]** 列まで水平にスクロールします。タイムスタンプ付きのユーザー名が表示されます。

構成可能なエンティティごとに、**[生成された構成（Generated Config）]** 列の下の詳細な履歴に、すべてのユーザーが行った構成変更の差分が表示されます。



Cisco DCNM でのファブリックの凍結

ネットワーク管理者は、LAN クラシック ファブリック、Easy ファブリック、および外部ファブリックの展開を無効にするか、凍結することができます。展開が凍結すると、DCNM からスイッチへの構成または書き込みアクセスが無効になります。ファブリックを凍結すると、スイッチをリロードしたり、メンテナンス モードに移行したり、メンテナンス モードを終了したり、ファブリック内でスイッチを追加または削除したりできなくなります。この機能は、メ

ンテナンス ウィンドウがスケジュールされていない限り、ネットワーク管理者が DCNM から物理ネットワークへの不注意な変更を無効にする完全な制御を提供します。

ファブリックの凍結

Cisco DCNM Web UI からのファブリックの展開を無効にするには、次の手順を実行します。

手順

ステップ 1 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウまたはファブリック トポロジ ウィンドウに移動します。

ステップ 2 スパナ（🔧）アイコンをクリックします。

スパナアイコンは、ファブリック トポロジウィンドウのファブリック名の横にあります。ファブリックのすべての展開を無効にするかどうかを尋ねる確認ウィンドウが表示されます。

ステップ 3 **[はい（Yes）]** をクリックします。

（注） ファブリックを凍結する前にスパナアイコンにカーソルを合わせると、ツールチップに **[展開有効化（Deployment Enabled）]** と表示されます。ファブリックを凍結した後にスパナアイコンにカーソルを合わせると、ツールチップに **[展開無効化（Deployment Disabled）]** と表示されます。

展開を無効にするか、ファブリックを凍結した後は、変更を保存、編集、またはプレビューすることはできますが、それらを展開することはできません。DCNM からこのファブリックへの展開関連のアクションはすべてグレー表示されます。

ファブリックのすべての展開を有効にするには、同じスパナ（⊗）アイコンをクリックして、ファブリックの凍結を解除します。

すべてのファブリックの凍結

ファブリックごとの展開凍結ノブに加えて、ネットワーク管理者は、DCNM 内のすべてのファブリックの展開を同時に凍結できます。

Cisco DCNM Web UI から DCNM セットアップですべてのファブリックを凍結するには、以下の手順を実行します。

手順

ステップ 1 **[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** を選択します。

ステップ 2 **[DEPLOYMENT_FREEZE]** フィールドを検索します。

ステップ 3 値を **[true]** に設定します。

デフォルト値は **false** です。

（注） DCNMを凍結すると、スイッチに変更を展開できません。ただし、network-adminロールやnetwork-stagerロールなどの適切なロールを持つユーザーは、適切なアクセス権を持ち、後の段階で展開するためにDCNMに変更を加えることができます。

ファブリックまたはDCNMを凍結したときに実行できないアクションはグレー表示されます。

ファブリックのバックアップと復元

このセクションでは、Cisco DCNM でのファブリックのバックアップと復元について説明します。

ファブリックのバックアップ

すべてのファブリック設定とインテントを自動または手動でバックアップできます。インテントである構成をCisco DCNMに保存できます。インテントは、スイッチにプッシュされる場合とされない場合があります。

DCNM は、次のファブリックをバックアップしません。

- モニタ専用モードの外部ファブリック：構成またはインテントを復元できないため、モニタ専用モードでの外部ファブリックのバックアップはサポートされていません。ただし、そのような外部ファブリックが MSD ファブリックのメンバー ファブリックである場合、バックアップは MSD ファブリック レベルで取得されます。

（注） Cisco DCNM リリース 11.4(1) 以降、モニタ専用モードで外部ファブリックのバックアップを取得できますが、復元することはできません。外部ファブリックがモニタ専用モードでない場合は、このバックアップを復元できます。

- Cisco DCNM リリース 11.4(1) より前のリリースの親 MSD ファブリック：MSD ファブリック内のメンバー ファブリックの構成とインテントのみを個別にバックアップできます。

（注） Cisco DCNM リリース 11.4(1) から、MSD ファブリックのバックアップを取得できます。親ファブリックからバックアップを開始すると、バックアッププロセスはメンバーファブリックにも適用されます。ただし、DCNM は、メンバー ファブリックと MSD ファブリックのすべてのバックアップ情報を 1 つのディレクトリにまとめて保存します。

Cisco DCNM リリース 11.4(1) 以降、バックアップは IFC に関連するインテントもキャプチャします。外部ファブリックをバックアップすると、チェックポイントがスイッチから DCNM にコピーされます。 バックアップ構成ファイルは、DCNM にある次のパスに保存されます：`/usr/local/cisco/dcm/dcnm/data/archive`

バックアップされた構成ファイルは、ファブリック名を持つ対応するディレクトリにあります。ファブリックの各バックアップは、手動または自動のどちらでバックアップされたかに関係なく、異なるバージョンとして扱われます。バックアップのすべてのバージョンは、対応するファブリック ディレクトリにあります。したがって、バックアップされたインテント構成ファイル、実行構成ファイル、および PTI は、次の場所にあります。`/usr/local/cisco/dcm/dcnm/data/archive/<fabric_name> /Version_x`、ここで `x` はバージョン番号です。有効な値は、1 から、**[archived.versions.limit]** フィールドで設定した制限までです。デフォルト値は 50 です。これは、50 個のバックアップのみがアーカイブされ、最も古いバックアップが削除されることを意味します。最小値は 10 です。10 未満の値を指定すると、10 に上書きされます。**[サーバーのプロパティ（Server Properties）]** ウィンドウで、アーカイブするバックアップファイルの数を設定できます。**[サーバーのプロパティ（Server Properties）]** ウィンドウで、**[ファブリックあたり保持されるアーカイブ ファイルの数：（# Number of archived files per fabric to be retained:）]** セクションを検索します。**[archived.versions.limit]** フィールドに値を入力します。

Cisco DCNM でMSD ファブリックをバックアップおよび復元する方法を示すビデオも視聴できます。「MSD ファブリックのバックアップと復元」のビデオを参照してください。

ファブリックの自動バックアップ

ファブリック構成およびインテントの毎時の自動バックアップ、またはスケジュール バックアップを有効にできます。自動バックアップには 2 つのタイプがあります。

バックアップには、ファブリック上の使用済みリソースに関するリソースマネージャの状態に加えて、インテントとファブリック設定に関連する情報が含まれます。DCNM は、構成のプッシュがある場合にのみバックアップします。DCNM は、最後の構成プッシュ後に手動バックアップをトリガーしなかった場合にのみ、自動バックアップをトリガーします。

自動バックアップには 2 つのタイプがあります。

- **[毎時のファブリック バックアップ（Hourly Fabric Backup）]**：毎時のバックアップを有効にすることができます。

（注） MSD ファブリックは、毎時バックアップをサポートしていません。

- **[スケジュール ファブリック バックアップ（Scheduled Fabric Backup）]**：定期的な間隔でファブリック バックアップをスケジュールできます。

（注） 外部ファブリックでは、DCNMは実行構成の変更もバックアップします。構成のプッシュは、展開後に行われます。変更を展開しなかった場合、インテントでそれらをバックアップすることはできません。

1時間ごと、およびスケジュールされたバックアップ プロセスは、次の定期的な構成コンプライアンス アクティビティ中にのみ発生し、最大 1 時間の遅延が発生する可能性があります。

ファブリックの毎時バックアップおよびスケジュール済みバックアップ

Cisco DCNM Web クライアントからファブリック構成およびインテントの自動バックアップを有効化するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

[ファブリック ビルダ（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 バックアップするファブリックの**[ファブリックの編集（Edit Fabric）]**アイコンをクリックします。

ステップ 3 [構成のバックアップ（Configuration Backup）] タブをクリックします。

ステップ 4 適切なチェックボックスをオンにして、バックアップの種類を選択します。

有効なオプションは、**[毎時のファブリック バックアップ（Hourly Fabric Backup）]** と **[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]** です。両方のバックアップを有効にする場合は、**[毎時のファブリック バックアップ（Hourly Fabric Backup）]** チェックボックスと**[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]** チェックボックスをオンにします。

（注） **[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]**チェックボックスをオンにする場合は、**[スケジュール時刻（Scheduled Time）]** フィールドでスケジュール済みのバックアップ時刻を指定します。`HH:MM` フォーマットで値を入力します。

ステップ 5 [保存（Save）] をクリックします。

[保存（Save）] をクリックすると、DCNM はバックアップ プロセスを開始します。

ファブリックの手動バックアップ

ファブリック構成およびインテントの手動バックアップを有効にできます。**[ファブリックの編集（Edit Fabric）]** ダイアログ ボックスの **[構成バックアップ（Configuration Backup）]** タブで選択した設定に関係なく、このオプションを使用してバックアップを開始できます。MSD

ファブリックのメンバー ファブリックのスタンドアロン バックアップを開始することはできません。

Cisco DCNM Web UI からファブリック構成およびインテントの手動バックアップを開始するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 すぐにバックアップするファブリックをクリックします。

ファブリック トポロジ ウィンドウが表示されます。

ステップ 3 [アクション（Actions）] ペインで [今すぐバックアップ（Backup Now）] をクリックします。

[今すぐバックアップ（Backup Now）] ダイアログが表示されます。

ステップ 4 **[タグ（Tag）]** フィールドにタグ名を入力します。

ステップ 5 [OK] をクリックします。

バックアップが正常にトリガーされたことを示す確認メッセージが表示されます。

（注） 確認メッセージは、バックアップが成功したかどうかではなく、バックアップがトリガーされたことのみを示しています。

ステップ 6 （任意） **[アクション（Actions）]** ペインで **[ファブリックの復元（Restore Fabric）]** をクリックして、手動バックアップが成功したかどうかを確認します。

手動バックアップは濃い青色で示されます。バックアップにカーソルを合わせると、名前に手順 *4* で言及したタグが付いており、手動バックアップであることを確認できます。

ゴールデン バックアップ

アーカイブの制限に達した後でも、削除しないバックアップにマークを付けることができます。これらのバックアップはゴールデン バックアップです。ファブリックのゴールデン バックアップは削除できません。ただし、Cisco DCNM は最大 10 のゴールデン バックアップのみをアーカイブします。ファブリックの復元中に、バックアップをゴールデン バックアップとしてマークできます。Cisco DCNM でゴールデンとしてバックアップをマークするには、Cisco DCNM Web UI から次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** の順に選択し、1 つのファブリックを選択します。

ステップ 2 **[アクション（Actions）]** メニューから **[ファブリックの復元（Restore Fabric）]** をクリックします。

[ファブリックの復元（Restore Fabric）] ウィンドウが表示されます。

ステップ 3 バックアップを選択する期間を選択します。

有効な値は、**1m**、**3m**、**6m**、**YTD**、**1y**および**All**です。グラフを拡大できます。デフォルトでは、**1m** のバックアップ情報（1 ヵ月）が表示されます。カスタムの日付範囲を選択することもできます。バックアップ情報には、次の情報が含まれます。

- バックアップ日
- デバイスの総数
- 同期しているデバイスの数
- 同期されていないデバイスの数

ステップ 4 バックアップをクリックして、ゴールデンとしてマークするバックアップを選択します。

自動または手動バックアップを選択できます。これらのバックアップは色分けされています。自動バックアップは青色で示されます。手動バックアップは濃い青色で示されます。ゴールデンバックアップはオレンジ色で示されます。自動バックアップの名前にはバージョンのみが含まれます。一方、手動バックアップには、手動バックアップを開始したときに指定したタグ名と、バックアップ名のバージョンがあります。バックアップにカーソルを合わせると、名前が表示されます。自動バックアップは、**[ファブリックの設定（Fabric Settings）]** ダイアログボックスの **[構成のバックアップ（Configuration Backup）]** タブから開始します。手動バックアップを開始するには、ファブリック トポロジ ウィンドウの **[アクション（Actions）]** ペインから **[今すぐバックアップ（Backup Now）]** をクリックします。

ステップ 5 バックアップをゴールデン バックアップとしてマークするには、**[バックアップをゴールデン バックアップとしてマーク（Mark backup as golden backup）]** チェックボックスにチェックを入れます。

確認用のダイアログボックスが表示されます。

ステップ 6 **[はい（Yes）]** をクリックします。

ステップ 7 「ファブリックの復元」の項に記載されている残りのファブリック復元手順を続行するか、ウィンドウを終了します。

バックアップの検証

ファブリックの復元プロセスを開始すると、DCNMはすべてのバックアップを検証します。検証には、次のチェックが含まれます。

- 復元する DCNM リリース：Cisco DCNM リリース 11.3(1) および Cisco DCNM リリース 11.4(1) からのみバックアップを復元できます。したがって、Cisco DCNM リリース 11.3(1) から Cisco DCNM リリース 11.4(1) にアップグレードする場合、アップグレード前にアーカイブしたバックアップを復元できます。
- メンバーファブリックの構成：DCNMは、MSDファブリックのメンバーファブリックの名前またはIDをチェックします。バックアップ後にそれらを変更すると、復元は続行されません。
- テンプレートの検証：DCNMは、バックアップのテンプレートが現在のバージョンのテンプレートと一致するかどうかを確認します。テンプレートを削除または名前を変更すると、復元を続行できません。
- ファブリックのデバイス構成：バックアップ後にスイッチのインベントリに変更があった場合、復元することはできません。

ファブリックの復元

このセクションでは、さまざまなタイプのファブリックの復元について説明します。Cisco DCNM はファブリック レベルで構成の復元をサポートします。復元する構成のバックアップを取ります。

Easy Fabric の復元

Cisco DCNM で Easy ファブリックを復元するには、Cisco DCNM Web UI から以下の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** の順に選択し、1 つのファブリックを選択します。

ステップ 2 **[アクション（Actions）]** メニューから **[ファブリックの復元（Restore Fabric）]** を選択します。

[ファブリックの復元（Restore Fabric）] ウィンドウが表示されます。

ステップ 3 構成を復元する時間を選択します。

有効な値は、**1m**、**3m**、**6m**、**YTD**、**1y** および **All** です。グラフを拡大できます。デフォルトでは、**1m** のバックアップ情報（1 ヵ月）が表示されます。カスタムの日付範囲を選択することもできます。バックアップ情報には、次の情報が含まれます。

- バックアップ日
- デバイスの総数

- 同期しているデバイスの数
- 同期されていないデバイスの数

ステップ 4 復元するバックアップを選択します。

自動または手動バックアップを選択できます。これらのバックアップは色分けされています。自動バックアップは青色で示されます。手動バックアップは濃い青色で示されます。ゴールデンバックアップはオレンジ色で示されます。自動バックアップの名前にはバージョンのみが含まれます。一方、手動バックアップには、手動バックアップを開始したときに指定したタグ名と、バックアップ名のバージョンがあります。バックアップにカーソルを合わせると、名前が表示されます。自動バックアップは、**[ファブリックの設定（Fabric Settings）]** ダイアログボックスの **[構成のバックアップ（Configuration Backup）]** タブから開始します。手動バックアップを開始するには、ファブリック トポロジ ウィンドウの **[アクション（Actions）]** ペインから **[今すぐバックアップ（Backup Now）]** をクリックします。

Note ファブリックが MSD ファブリックのメンバーであり、バックアップが MSD ファブリック レベルで取得された場合、そのバックアップはここに表示されません。MSD ファブリックの一部になる前に取得されたファブリックのスタンドアロンバックアップのみがここに表示されます。

ステップ 5 バックアップをゴールデン バックアップとしてマークするには、**[バックアップをゴールデンバックアップとしてマーク（Mark backup as golden backup）]** チェックボックスにチェックを入れます。

ステップ 6 > **[次へ（Next）]** をクリックして、同期しているデバイスの選択したバックアップ情報を表示します。

スイッチ名、スイッチのシリアル番号、IP アドレス、と差分構成の詳細が表示されます。

Note ファブリックにデバイスを追加または削除すると、バックアップは無効になります。有効なバックアップのみを復元できます。

ステップ 7 **[構成の取得（Get Config）]** をクリックして、構成の詳細をプレビューします。

[構成のプレビュー（Config Preview）] ウィンドウが表示されます。このウィンドウには 2 つのタブがあります。

- **バックアップ構成（Backup Config）**：このタブには、選択したデバイスのバックアップ設定が表示されます。
- **[現在の構成（Current Config）]**：このタブには、選択したデバイスの現在の構成が表示されます。

ステップ 8 **[バックアップのサマリを表示（View Backup Summary）]** ウィンドウに戻ります。

ステップ 9 **[インテントの復元（Restore Intent）]** をクリックして、復元の手順に進みます。

[ステータスの復元（Restore Status）] ウィンドウが表示されます。次のステータスを表示できます。

- **[バックアップの検証（Validating Backup）]**

- **[ファブリック インテントの復元（Restoring fabric intent）]**
- **[アンダーレイ インテントの復元（Restoring underlay intent）]**
- **[インターフェイス インテントの復元（Restoring interface intent）]**
- **[オーバーレイ インテントの復元（Restoring overlay intent）]**

アクションのステータスの有効な値は、**[進行中（In Progress）]**、**[保留中（Pending）]**、または **[失敗（Failed）]**です。

Note **[検証のバックアップ（Validating Backup）]** のステータスが **[失敗（Failed）]** の場合、他の復元アクションはこのウィンドウにリストされません。

ステップ 10 インテントが復元されたら、**[次へ（Next）]** をクリックします。

[構成のプレビュー（Configuration Preview）] ウィンドウが表示されます。このウィンドウでは、次の詳細を表示できます。

- スイッチ名
- [IP アドレス（IP Address）]
- スイッチのシリアル番号
- 構成のプレビュー
- Status
- 進歩

ステップ 11 復元された構成を展開するには、**[展開（Deploy）]** をクリックします。

[構成展開ステータス（Configuration Deployment Status）] ウィンドウが表示されます。スイッチ名、IP アドレス、ステータス、ステータスの説明、進行状況の詳細を表示できます。

ステップ 12 復元プロセスが完了したら、**[閉じる（Close）]** をクリックします。

外部ファブリックの復元

外部ファブリックを復元すると、バックアップされたチェックポイントが DCNM からスイッチにコピーされます。Cisco DCNM で外部ファブリックを復元するには、Cisco DCNM Web UI から以下の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** の順に選択し、1 つのファブリックを選択します。

ステップ 2 [アクション（Actions）] メニューから **[ファブリックの復元（Restore Fabric）]** を選択します。

[ファブリックの復元（Restore Fabric）] ウィンドウが表示されます。

ステップ 3 構成を復元する時間を選択します。

有効な値は、**1m**、**3m**、**6m**、**YTD**、**1y**および**All**です。グラフを拡大できます。デフォルトでは、**1m** のバックアップ情報（1 ヵ月）が表示されます。

バックアップバージョンを選択すると、それを表す垂直バーがグレーになり、対応する情報が画面下部に表示されます。収集する情報は次のとおりです。

- バックアップ日
- DCNM Version
- デバイスの総数
- 同期しているデバイスの数
- 同期されていないデバイスの数

垂直バーの下にある日付スライドを再配置するか、画面の右上にある **[開始（From）]** ボックスと **[終了（To）]** ボックスを使用して、カスタムの日付範囲を選択できます。

ステップ 4 復元するバックアップを選択します。

自動または手動バックアップを選択できます。これらのバックアップは色分けされています。自動バックアップは青色で示されます。手動バックアップは濃い青色で示されます。ゴールデンバックアップはオレンジ色で示されます。自動バックアップの名前にはバージョンのみが含まれます。一方、手動バックアップには、手動バックアップを開始したときに指定したタグ名と、バックアップ名のバージョンがあります。バックアップにカーソルを合わせると、名前が表示されます。自動バックアップは、**[ファブリックの設定（Fabric Settings）]** ダイアログボックスの **[構成のバックアップ（Configuration Backup）]** タブから開始します。手動バックアップを開始するには、ファブリック トポロジ ウィンドウの **[アクション（Actions）]** ペインから **[今すぐバックアップ（Backup Now）]** をクリックします。

Note ファブリックが MSD ファブリックのメンバーであり、MSD ファブリックのバックアップが取られた場合、そのバックアップはここに表示されません。MSDファブリックの一部になる前に取得されたファブリックのスタンドアロンバックアップのみがここに表示されます。

ステップ 5 (Optional) バックアップをゴールデン バックアップとしてマークするには、**[バックアップをゴールデン バックアップとしてマーク（Mark backup as golden backup）]** チェックボックスにチェックを入れます。

ステップ 6 > **[次へ（Next）]** をクリックして、同期しているデバイスの選択したバックアップ情報を表示します。

スイッチ名、スイッチのシリアル番号、IPアドレス、ステータス、復元のサポート（デバイスがチェックポイントロールバックをサポートしているかどうかを示します）、デバイスの構成の詳細、および VRF が表示されます。

Note プラットフォームでのチェックポイントロールバック機能のサポートについては、それぞれのプラットフォームのドキュメントを参照してください。

デフォルトでは、管理 VRF は、復元プロセス中のコピー操作に使用されるため、VRF 列に表示されます。コピー操作に別の VRF を使用する場合は、VRF 列を更新します。すべてのデバイスに同じ VRF を更新するには、画面の左下にある [すべてのデバイスに適用（Apply for all devices）] オプションを使用します。サンプル スクリーンショット：

Note ファブリックにデバイスを追加または削除した場合、現在の日付から過去の日付にファブリックを復元することはできません。

ステップ 7 **[構成の取得（Get Config）]** をクリックして、デバイスの構成の詳細をプレビューします。

[構成のプレビュー（Config Preview）] ウィンドウが表示されます。このウィンドウには 3 つのタブがあります。

- **バックアップ構成（Backup Config）**：このタブには、選択したデバイスのバックアップ設定が表示されます。
- **現在の構成（Current Config）**：このタブには、選択したデバイスの現在の実行構成が表示されます。
- **[並列比較（Side-by-side Comparison）]**：このタブには、スイッチの現在の実行構成と、バックアップ構成（または予想される構成）が表示されます。

ステップ 8 **[バックアップのサマリを表示（View Backup Summary）]** ウィンドウに戻ります。

ステップ 9 **[インテントの復元（Restore Intent）]** をクリックして、復元の手順に進みます。

[ステータスの復元（Restore Status）] ウィンドウが表示されます。次のステータスを表示できます。

- **[バックアップの検証（Validating Backup）]**
- **[ファブリック インテントの復元（Restoring fabric intent）]**
- **[アンダーレイ インテントの復元（Restoring underlay intent）]**
- **[インターフェイス インテントの復元（Restoring interface intent）]**
- **[オーバーレイ インテントの復元（Restoring overlay intent）]**
- **[インテント再生（Intent Regeneration）]**

アクションのステータスの有効な値は、**[進行中（In Progress）]**、**[保留中（Pending）]**、**[完了（Completed）]** または **[失敗（Failed）]**です。

Note **[検証のバックアップ（Validating Backup）]** のステータスが **[失敗（Failed）]** の場合、他の復元アクションはこのウィンドウにリストされません。

ステップ 10 復元プロセスが完了したら、**[閉じる（Close）]** をクリックします。

MSD ファブリックの復元

MSD ファブリックを復元すると、MSD ファブリックに関連するオーバーレイ情報が復元されてから、子ファブリックに関連する情報が復元されます。MSD ファブリックのインベントリ

に変更がある場合、バックアップは無効と見なされ、復元はブロックされます。メンバーファブリックの復元プロセスを開始することはできません。ファブリックが現在 MSD ファブリックのメンバー ファブリックであることを示すエラーが表示されます。メンバー ファブリックを MSD ファブリックから移動して、以前のスタンドアロン バックアップを復元します。MSD ファブリックの復元には、ファブリック インテント、アンダーレイまたはインターフェイス インテント、オーバーレイ インテント、およびインテント再生成の復元が含まれます。

Cisco DCNM でMSD ファブリックをバックアップおよび復元する方法を示すビデオも視聴できます。「MSD ファブリックのバックアップと復元」のビデオを参照してください。

Cisco DCNM で Easy ファブリックを復元するには、Cisco DCNM Web UI から以下の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

ステップ 2 MSD ファブリックを選択します。

ステップ 3 **[アクション（Actions）]** メニューから **[ファブリックの復元（Restore Fabric）]** をクリックします。

[ファブリックの復元（Restore Fabri）]ウィザードが表示され、**[バックアップの選択（Select Backup）]**手順に進みます。

（注） このオプションは、対応するファブリック トポロジ ウィンドウから、MSD ファブリックのメンバー ファブリックには使用できません。

ステップ 4 構成を復元する時間を選択します。

有効な値は、**1m**、**3m**、**6m**、**YTD**、**1y**および**All**です。グラフを拡大できます。デフォルトでは、**1m** のバックアップ情報（1 ヵ月）が表示されます。カスタムの日付範囲を選択することもできます。バックアップ情報には、次の情報が含まれます。

- バックアップ日
- デバイスの総数
- 同期しているデバイスの数
- 同期されていないデバイスの数

ステップ 5 復元するバックアップを選択します。

自動または手動バックアップを選択できます。これらのバックアップは色分けされています。自動バックアップは青色で示されます。手動バックアップは濃い青色で示されます。ゴールデンバックアップはオレンジ色で示されます。自動バックアップの名前にはバージョンのみが含まれます。一方、手動バックアップには、手動バックアップを開始したときに指定したタグ名と、バックアップ名のバージョンがあります。バックアップにカーソルを合わせると、名前が表示されます。自動バックアップは、**[ファブリックの設定（Fabric Settings）]**ダイアログボッ

クスの **[構成のバックアップ（Configuration Backup）]** タブから開始します。手動バックアップを開始するには、ファブリック トポロジ ウィンドウの **[アクション（Actions）]** ペインから **[今すぐバックアップ（Backup Now）]** をクリックします。

（注） メンバー ファブリックを MSD ファブリックにインポートする前に取ったスタンドアロン バックアップは、ここには表示されません。MSD バックアップのみがここに表示されます。

ステップ 6 復元したいバックアップをクリックします。

[バックアップ サマリ（Backup Summary）] エリアが表示されます。収集する情報は次のとおりです。

- バックアップ取得時間：バックアップを取った時点のタイムスタンプ
- DCNM バージョン：バックアップを取った時点の DCNM バージョン
- バックアップ バージョン：バックアップのバージョン（手動バックアップの場合はタグ名も含みます。）
- ファブリックの総数：MSD ファブリックにインポートされたメンバー ファブリックの総数を指定します。
- Easy ファブリックの総数：Easy ファブリックであるメンバー ファブリックの数を指定します。
- 外部ファブリックの総数：外部ファブリックであるメンバーファブリックの数を指定します。
- デバイスの総数：すべてのメンバー ファブリック内のスイッチの総数を指定します。
- 同期ステータス以外のデバイスの数：同期していないデバイスの数を指定します。
- 不明なステータスのデバイスの数：ステータスが不明のデバイスの数を指定します。
- メンバー ファブリック：メンバー ファブリックの名前を指定します。[ゴールデン バックアップとしてバックアップをマーク付け（Mark backup as golden backup）] チェックボックス：（オプション）バックアップをゴールデン バックアップとしてマーク付けするには、**[ゴールデン バックアップとしてバックアップをマーク付け（Mark backup as golden backup）]** チェック ボックスをオンにします。

（注） 同期ステータス以外（Out-of-Sync）または不明な（Unknown）ステータスのデバイスがある場合、復元プロセスはブロックされます。

ステップ 7 **[次へ（Next）]** をクリックして、**[プレビューの復元（Restore Preview）]** の手順に進みます。

[Easy ファブリック（Easy Fabric）] タブには、スイッチ名、ファブリック名、スイッチ シリアル、IPアドレス、およびメンバーEasyファブリックのデルタ構成に関する情報があります。**[Easy ファブリック（Easy Fabric）]** タブには、スイッチ名、ファブリック名、スイッチのシリアル、IPアドレス、スイッチのステータス、構成、およびメンバーの外部ファブリックで復元がサポートされているかどうかに関する情報が含まれています。

（注） デバイスがファブリックに追加または削除された場合、バックアップは無効です。有効なバックアップのみを復元できます。

ステップ 8 **[インテントの復元（Restore Intent）]** をクリックして、復元の**ステータスの復元**手順に進みます。

メンバー ファブリックの復元ステータスと説明が表示されます。メンバー ファブリック オプション ボタンをクリックして、そのファブリックのファブリック レベルの進行状況を表示します。進行状況は 5 秒ごとに自動的に更新されます。

ステップ 9 ステータスが成功したら、**[次へ（Next）]** をクリックします。

[構成のプレビュー（Configuration Preview）] ウィンドウが表示されます。このウィンドウでは、スイッチ名、IPアドレス、スイッチのシリアル番号、構成のプレビュー、ステータス、および進行状況の詳細を表示できます。

（注）
- **[次へ（Next）]** をクリックできるのは、ステータスが **[完了（Completed）]** の場合のみです。
- ファブリック設定が変更されているため、前の手順に戻ることはできません。
- 復元に失敗した場合、ファブリックは以前の構成にロール バックします。

ステップ 10 復元された構成を展開するには、**[展開（Deploy）]** をクリックします。

[構成展開ステータス（Configuration Deployment Status）] ウィンドウが表示されます。次の詳細情報を表示できます。

- スイッチ名
- [IP アドレス（IP Address）]
- Status
- ステータスの説明
- 進歩

ステップ 11 復元プロセスが完了したら、**[閉じる（Close）]** をクリックします。

スイッチの復元

Cisco DCNM リリース 11.5(1) 以降、Cisco DCNM Web UI から外部ファブリックおよび LAN クラシック ファブリックの Cisco Nexus スイッチを復元できます。スイッチ レベルで復元する情報は、ファブリック レベルのバックアップから抽出されます。スイッチ レベルの復元では、ファブリック レベルのインテントおよびファブリック設定を使用して適用されたその他の設定は復元されません。スイッチ レベルのインテントのみが復元されます。したがって、スイッチを復元すると、ファブリック レベルのインテントが復元されないため、同期がとれなくなる可能性があります。ファブリック レベルの復元を実行して、インテントも復元します。復元は一

度に 1 つしか実行できません。スイッチが検出されたファブリックが MSD ファブリックの一部である場合、スイッチを復元することはできません。

Cisco DCNM でスイッチを復元するには、Cisco DCNM Web UI から以下の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

ステップ 2 外部ファブリック、または LAN クラシック ファブリックを選択します。

ステップ 3 構成を復元する Cisco Nexus スイッチを右クリックします。

ステップ 4 **[構成の復元（Restore Config）]** オプションを選択します。

または、**[アクション（Actions）]** ペインの **[表形式ビュー（Tabular view）]** をクリックして、**[スイッチ（Switches）]** タブに移動することもできます。チェックボックスをオンにして Cisco Nexus スイッチを選択し、**[復元（Restore）]** をクリックします。

非 Nexus スイッチの場合、**[構成の復元（Restore Config）]** オプションは表示されず、**[復元（Restore）]** ボタンはグレー表示されます。

このオプションは、**[network-operator]** ロールでログインした場合、またはファブリックがモニタ モードまたは凍結モードの場合は表示されません。

[スイッチの復元（Restore Switch）] ウィザードが表示され、**[バックアップの選択（Select Backup）]** 手順に進みます。

ステップ 5 構成を復元する時間を選択します。

有効な値は、**1m**、**3m**、**6m**、**YTD**、**1y** および **All** です。グラフを拡大できます。デフォルトでは、**1m** のバックアップ情報（1 ヵ月）が表示されます。カスタムの日付範囲を選択することもできます。

ステップ 6 復元するバックアップを選択します。

自動、手動、またはゴールデンバックアップを選択できます。これらのバックアップは色分けされています。自動バックアップは青色で示されます。手動バックアップは濃い青色で示されます。ゴールデンバックアップはオレンジ色で示されます。自動バックアップの名前にはバージョンのみが含まれます。一方、手動バックアップには、手動バックアップを開始したときに指定したタグ名と、バックアップ名のバージョンがあります。バックアップにカーソルを合わせると、名前が表示されます。自動バックアップは、**[ファブリックの設定（Fabric Settings）]** ダイアログボックスの **[構成のバックアップ（Configuration Backup）]** タブから開始します。手動バックアップを開始するには、ファブリック トポロジ ウィンドウの **[アクション（Actions）]** ペインから **[今すぐバックアップ（Backup Now）]** をクリックします。

ステップ 7 復元するバックアップをクリックします。

[バックアップ サマリ（Backup Summary）] エリアが表示されます。収集する情報は次のとおりです。

- バックアップ取得時間：バックアップを取った時点のタイムスタンプ

- DCNM バージョン：バックアップを取った時点の DCNM バージョン
- バックアップバージョン：バックアップのバージョン（手動バックアップの場合はタグ名も含みます。）
- デバイスの総数：バックアップを取った時点のファブリック内のスイッチの総数を指定します。
- 同期ステータスのデバイスの数：同期しているデバイスの数を指定します。
- 同期ステータス以外のデバイスの数：同期していないデバイスの数を指定します。
- 不明なステータスのデバイスの数：ステータスが不明のデバイスの数を指定します。
- [ゴールデン バックアップとしてバックアップをマーク付け] チェックボックス：（オプション）バックアップをゴールデン バックアップとしてマーク付けするには、**[ゴールデン バックアップとしてバックアップをマーク付け（Mark backup as golden backup）]** チェック ボックスをオンにします。バックアップをゴールデン バックアップとしてマークすると、ファブリック レベルのバックアップもゴールデン バックアップとしてマークされます。

（注） この情報の大部分はファブリックレベルであり、スイッチレベルの復元の手順に直接影響する場合と影響しない場合があります。

ステップ 8 **[次へ（Next）]** をクリックして、**[プレビューの復元（Restore Preview）]** の手順に進みます。

スイッチ名、スイッチ シリアル、IP アドレス、ステータス、サポートされている復元、デルタ構成、および VRF の詳細に関する情報を表示できます。

ステップ 9 （任意）**[構成の取得（Get Config）]** をクリックして、デバイスの構成の詳細をプレビューします。

[構成のプレビュー（Config Preview）] ウィンドウが表示されます。このウィンドウには 3 つのタブがあります。

- **バックアップ構成（Backup Config）**：このタブには、選択したデバイスのバックアップ設定が表示されます。
- **現在の構成（Current Config）**：このタブには、選択したデバイスの現在の実行構成が表示されます。
- **並列比較**：このタブには、スイッチの現在の実行構成と、予想される構成が表示されます。

ステップ 10 **[復元（Restore）]** をクリックして、復元の **[ステータスの復元（Restore Status）]** 手順に進みます。

スイッチの復元ステータスと説明が表示されます。

ステップ 11 復元プロセスが完了したら、**[閉じる（Close）]** をクリックします。

（注）
- ファブリック設定が変更されているため、前の手順に戻ることはできません。
- 復元に失敗した場合、スイッチは以前の設定にロールバックします。

VXLAN BGP EVPN ファブリックの削除

[制御（Control）] > [ファブリック ビルダ (Fabric Builder)] を選択します。ファブリック ビルダページで、ファブリックを表す長方形のボックスの **[X]** をクリックします。ファブリックを削除する前に、次のことを確認してください。

- ファブリックデバイスは、ファブリック内またはファブリックからの移行、進行中のネットワークまたは VRF プロビジョニングなどの移行中でないようにしてください。移行が完了したら、ファブリックを削除します。
- まだファブリックに接続されているデバイスを削除します。最初に Cisco Nexus 9000 シリーズ以外のスイッチを削除してから、9000 シリーズ スイッチを削除します。

VXLAN BGP EVPN、外部ファブリック、MSD ファブリックの DCNM 11.5(1) アップグレードのポスト

DCNM リリース 11.5(1) にアップグレードした後は、次のガイドラインに注意してください。

- 以前の DCNM リリースからのアップグレードの一環として、ファブリックおよび関連するテンプレートは DCNM リリース 11.5(1) に引き継がれます。
- DCNM 11.3(1) 以降、以前の DCNM リリースのポリシーテンプレートの一部は廃止され、新しい DCNM リリースごとにアクティブに更新されます。これらのポリシー テンプレートは、使用中でないことが判明した場合、アップグレード後に自動的に削除されます。この削除により動作が影響を受けることはなく、DCNM テンプレート ライブラリで表示されるポリシーの数を削減することに役立ちます。
- **[ファブリック ビルダ（Fabric Builder）]** ウィンドウから各ファブリックに移動し、**[保存と展開（Save & Deploy）]** をクリックして変更を展開します。

  [保存と展開（Save & Deploy）] をクリック後、新規または予期しない保留中の構成が見つかった場合は、DCNM での構成コンプライアンス （387 ページ）を参照してください。

⚠

注意 この手順の一部として、いくつかの構成変更が想定されています。したがって、スケジュール済みのメンテナンス ウィンドウについてのみ、実行するようにしてください。

- リリース 11.2(1) からの DCNM アップグレード後、ファブリックにボーダーデバイス（ボーダー、ボーダースパイン、ボーダーゲートウェイなど）がある場合、次の相違点が表示されます。

```
route-map extcon-rmap-filter-v6 deny 20
  no match ip address prefix-list host-route-v6
route-map extcon-rmap-filter-v6 deny 20
  match ipv6 address prefix-list host-route-v6
```

  上記の構成は予期されるものであり、正しいルートマップ定義であることを意味します。この差分を展開することで、スイッチ構成を正常に行えます。アップグレードの前にファブリックがグリーンフィールドとして作成された場合、追加のアクションは必要ありません。デバイス上での誤ったルートマップ構成によってアップグレードが行われる前に、ファブリックがブラウンフィールドとして作成された場合、この構成は **switch_freeform** ポリシーでキャプチャされます。アップグレード後、展開の前に、自由形式ポリシーを編集して CLI **match ip address prefix-list host-route-v6** を削除する必要があります。

- Cisco DCNM 10.4(2) または 11.0(1) 以降では、マルチレベルのアップグレードの後、VRF テンプレートを **Default_VRF_Universal** または **Default_VRF_Extension_Universal** に変更して、**ipv6 address use-link-local-only** を有効にすることができます。

レベル 1 からレベル 2 へ ISIS 構成の変更

この手順は、VXLAN ファブリック展開で、スイッチの ISIS 構成をレベル 1 からレベル 2 に変更する方法を示しています。

1. **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。
2. **ファブリック ビルダ（Fabric Builder）** ウィンドウで、ファブリックをクリックします。
3. **[アクション（Actions）]** メニューで **[表形式ビュー（Tabular view）]** をクリックします。
4. **[テンプレート（Template）]** 検索フィールドですべての **base_isis** ポリシーを検索します。
5. すべての **base_isis** ポリシーを選択し、**[削除（Delete）]** アイコンをクリックしてポリシーを削除します。
6. [保存して展開（Save & Deploy）] をクリックします。

すべての **base_isis** ポリシーが削除されると、DCNM は移行されたブラウンフィールド ファブリックをグリーンフィールド ファブリックと見なし、スイッチに **base_isis_level2** ポリシーを作成します。

DCNM での構成コンプライアンス

特定のスイッチに定義されたインテント全体または予想される構成は、DCNM に保存されます。この構成を 1 つ以上のスイッチにプッシュする場合、構成コンプライアンス（CC）モジュールがトリガーされます。CC は、現在のインテント、現在の実行構成を取得し、現在の

実行構成から現在期待されている構成に移行するために必要な一連の構成を算出し、すべてが同期するようにします。

スイッチでソフトウェアまたはファームウェアのアップグレードを実行しても、スイッチの現在の実行構成は変更されません。アップグレード後、現在の実行構成が現在期待されている構成またはインテントを持っていないことを検出した場合、CC は非同期ステータスを報告します。構成の自動展開は行われません。展開される差分をプレビューしてから、1 つ以上のデバイスを同期状態に戻すことができます。

CC では、同期は常に DCNM からスイッチに対して行われます。逆方向の同期は行われません。そのため、Switchに対し、DCNM で定義されたインテントと競合するアウトオブバンドの変更を行うと、CC はこの差分をキャプチャし、デバイスが同期していないことを示します。保留中の差分は、アウトオブバンドで行われた構成を元に戻し、デバイスを同期状態に戻します。アウトオブバンド変更によるこのような競合がキャプチャされるのは、デフォルトで 60 分ごとに発生する定期的なCC実行時、またはファブリックごとまたはスイッチごとにRESYNC オプションをクリックしたときであることに注意してください。CC の REST API を使用して、スイッチ全体のアウトオブバンド変更をキャプチャすることもできます。詳細については、『*Cisco DCNM REST API* ガイド、リリース *11.2(1)* 』を参照してください。

Cisco DCNM リリース 11.2(1) 以降、展開される構成の使いやすさと読みやすさを向上させるために、DCNM の CC は以下のように拡張されました。

- DCNM でのすべての表示は、読みやすく理解しやすいものにされました。
- 繰り返される構成スニペットは表示されません。
- 保留中の構成には、正確に差分構成だけが表示されます。
- 並列比較による差分表示はより読みやすくなり、統合された検索またはコピー、および差分サマリー機能を備えています。

CC エンジンは、インテントをスイッチで実行中の構成と比較することで差分を計算し、インテントで定義されている構成がスイッチに存在することを確認します。インテントで定義されているコンポーネントまたは構成スニペットについて、CCエンジンは、必要に応じて、スイッチ構成をインテント構成と一致させる適切なコマンドを生成することにより、同じコンポーネントまたは構成スニペットがスイッチ上に存在することを保証します。

DCNMインテントが関連付けられていない、スイッチの最上位の構成コマンドでは、構成コンプライアンス（CC） のコンプライアンス チェックは行われません。ただし、以下のコマンドについては、DCNMインテントがない場合でも、CC はコンプライアンス チェックを実行し、削除を試みます。

- **configure profile**
- **apply profile**
- **interface vlan**
- **interface loopback**
- **interface Portchannel**
- サブインターフェイス、例えば **interface Ethernet** *X/Y.Z*

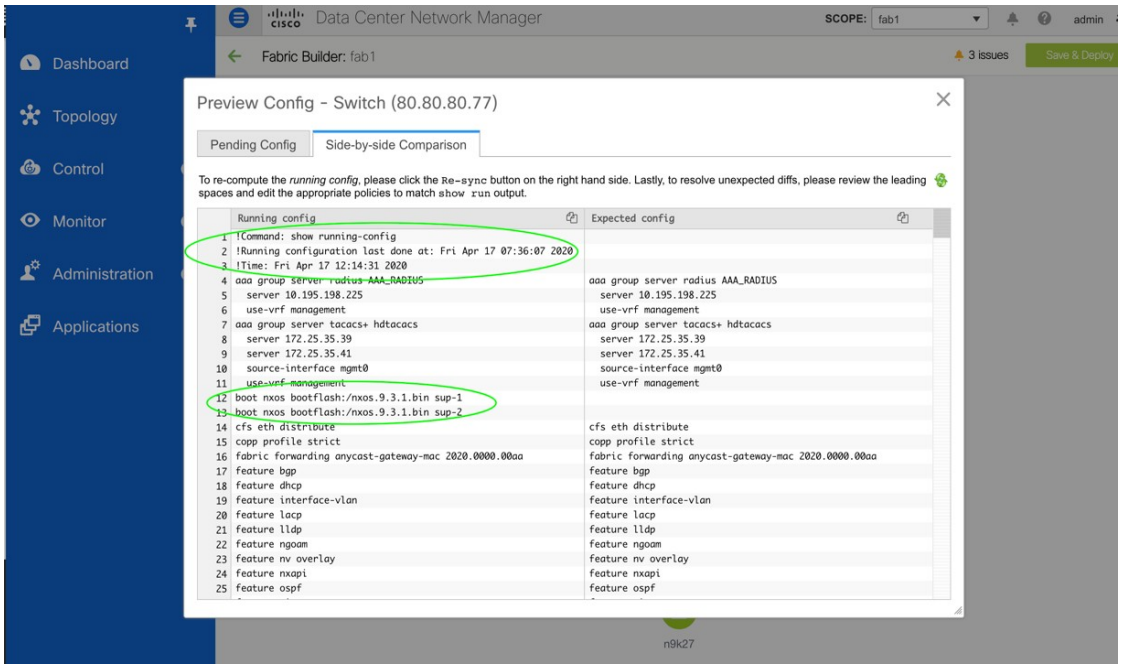
- **fex**
- **vlan** <*vlan-ids*>

CC は、*Easy_Fabric_11_1* および *Easy_Fabric_eBGP* ファブリック テンプレートが使用されている場合にのみ、コンプライアンスチェックを実行し、これらのコマンドの削除を試みます。*External_Fabric* テンプレートの場合、上記のコマンドも含めて、関連する DCNM インテントを持たないスイッチの最上位の構成コマンドでは、CC はコンプライアンス チェックを実行しません。

予期しない動作を避けるために、これらのコマンドをスイッチに展開する場合には、DCNM 自由形式構成テンプレートを使用して追加のインテントを作成することが推奨されています。

ここで、スイッチに存在する構成がインテントで定義された構成と関係していないシナリオを考えてみましょう。このような構成の例としては、インテントでキャプチャされていないがスイッチに存在する新しい機能、またはインテントでキャプチャされていない他の構成の特徴があります。構成コンプライアンスは、これらの構成の不一致を差分とは見なしません。このような場合、厳密な構成コンプライアンスは、インテントで定義されているすべての構成行がスイッチに存在する唯一の構成であることを保証します。ただし、厳密な CC チェックは、ブート文字列、rommon 構成、およびその他のデフォルト構成などの構成を無視します。このような場合、内部構成コンプライアンスエンジンは、これらの構成変更が差分として呼び出されないようにします。これらの差分は、**[保留中の構成（Pending Config）]** ウィンドウにも表示されません。ただし、並列比較差分ユーティリティは、2つをテキストファイルとして差分の比較を行います。diff の計算で使用される内部ロジックは利用しません。その結果、デフォルト構成の差分は、**並列比較（Side-by-side Comparison）**ウィンドウで赤で強調表示されます。

Cisco DCNM リリース 11.4(1) から、そのような差分は、**[並列比較（Side-by-side Comparison）]** ウィンドウで強調表示されません。**[実行中の構成（Running config）]** ウィンドウで強調表示される自動生成されたデフォルト構成は、**[期待される構成（Expected config）]** ウィンドウには表示されません。



[保留中の構成（Pending Config）] ウィンドウに表示される構成が **[並列比較（Side-by-side Comparison）]** ウィンドウでは赤で強調表示される場合があります。これは、その構成が **[実行中の構成（Running config）]** ウィンドウには表示されるものの、**[期待される構成（Expected config）]** ウィンドウには表示されない場合です。一方、**[保留中の構成（Pending Config）]** ウィンドウに表示される構成が **[並列比較（Side-by-side Comparison）]** ウィンドウでは緑で強調表示される場合もあります。これは、その構成が **[期待される構成（Expected config）]** ウィンドウには表示されるものの、**[実行中の構成（Running config）]** ウィンドウには表示されない場合です。**[保留中の構成（Pending Config）]** ウィンドウに構成が表示されない場合、**[並列比較（Side-by-side Comparison）]** ウィンドウに赤で構成が表示されることはありません。

すべての自由形式の構成は、スイッチの **show running configuration** の出力と厳密に一致する必要があり、構成からの逸脱は、**[保存と展開（Save & Deploy）]** の際に差分として表示されます。先頭のスペースによるインデントは守る必要があります。

通常、次の方法を使用して DCNM に構成スニペットを入力できます。

- ユーザー定義のプロファイルとテンプレート
- スイッチ、インターフェイス、オーバーレイ、および vPC フリーフォーム設定
- スイッチごとのネットワークおよび VRF フリーフォーム構成
- リーフ、スパイン、または iBGP 構成のファブリック設定

⚠

注意 設定形式は、対応するスイッチの **show running configuration** と同じである必要があります。そうなっておらず、構成の先頭のスペースが欠落していたり、正しくなかったりした場合、予期しない展開エラーが発生したり、保留中の構成が予測不能な状態になったりする可能性があります。予期しない差分または展開エラーが表示された場合は、ユーザー提供またはカスタムの構成スニペットに間違った値がないか確認してください。

予期しない保留中の構成が原因で DCNM に「非同期」ステータスが表示され、この構成が展開できないか、展開後も変化がない場合は、次の手順を実行して回復します。

1. **[保留中の構成（Pending Config）]** タブ（**[構成プレビュー（Pending Config）]** ウィンドウ）で強調表示されている構成の行を確認します。
2. **[並列比較（Side-by-side Comparison）]** タブで同じ行を確認します。このタブには、「intent」または「show run」、あるいはその両方の先頭スペースが異なっていて、差分になっていた場合、それが表示されます。先頭のスペースは、**[並列比較（Side-by-side Comparison）]** タブで強調表示されます。
3. 保留中の構成または非同期状態のスイッチが、「インテント」と「実行構成」の先頭のスペースが一致しない、識別可能な構成が原因である場合、インテント側のスペースが正しくないため、編集する必要があることを示しています。
4. カスタム ポリシーまたはユーザー定義ポリシーの不適切なスペースを編集するには、スイッチに移動して対応するポリシーを編集します。
    1. ポリシーのソースが **[アンダーレイ（UNDERLAY）]** の場合、ファブリック設定画面からこれを編集し、更新された構成を保存する必要があります。
    2. ソースが空白の場合は、そのスイッチの **[ポリシーの表示/編集（View/Edit policies）]** ウィンドウから編集できます。
    3. ポリシーのソースが **[オーバーレイ（OVERLAY）]** であるが、スイッチの自由形式構成から派生している場合。この場合、適切な **[オーバーレイ（OVERLAY）]** スイッチ自由形式構成に移動して更新します。
    4. ポリシーのソースが **[オーバーレイ（OVERLAY）]** またはカスタム テンプレートの場合は、次の手順を実行します。
        1. **[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** に移動し、**[template.in_use.check]** プロパティを **[false]** に設定します。これにより、プロファイルまたはテンプレートを編集できるようになります。
        2. **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** 編集ウィンドウから特定のプロファイルまたはテンプレートを編集し、更新されたプロファイル テンプレートを適切なスペースを設定して保存します。
        3. **[保存と展開（Save & Deploy）]** をクリックして、影響を受けるスイッチの差分を再計算します。

4. 構成が更新されたら、**[template.in_use.check]** プロパティを **[true]** に設定します。これは、特に **[保存と展開（Save & Deploy）]** 操作で、DCNM システムのパフォーマンスが低下するためです。

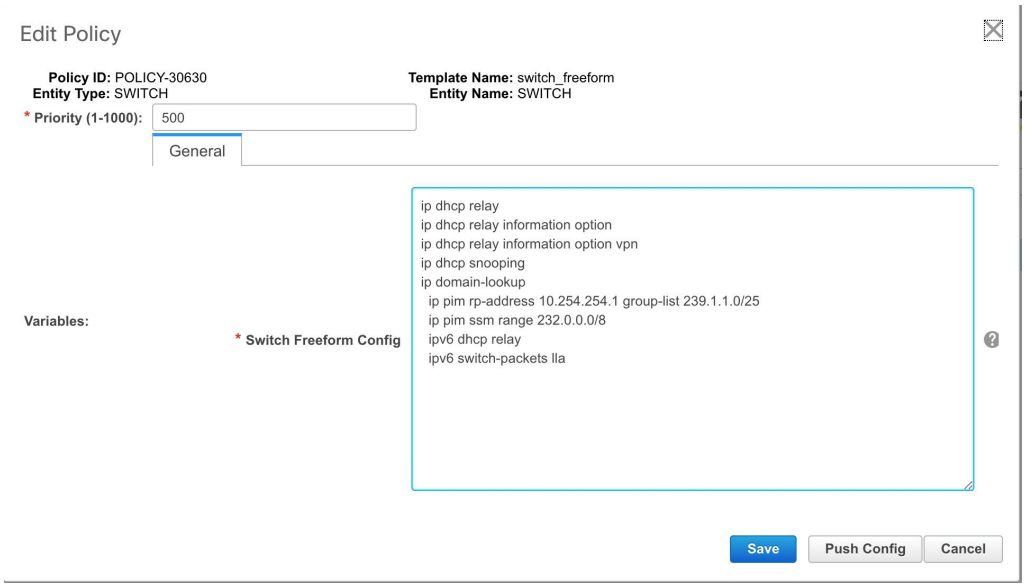
差分が解決されたことを確認するには、ポリシーを更新した後に**[保存と展開（Save & Deploy）]** をクリックして変更を検証します。

（注） DCNM は、特に複数のコマンド シーケンスの場合、コマンドの階層を意味するものであるため、先頭のスペースのみをチェックします。DCNM は、コマンド シーケンスの末尾のスペースをチェックしません。

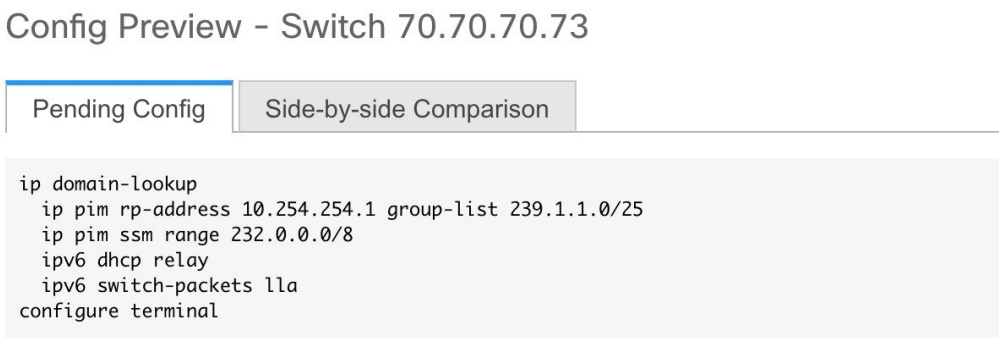
例 1: スイッチの自由形式ポリシーの構成コンプライアンス

スイッチの [自由形式構成（Freeform Config）] フィールドのスペースが正しくない例を考えてみましょう。

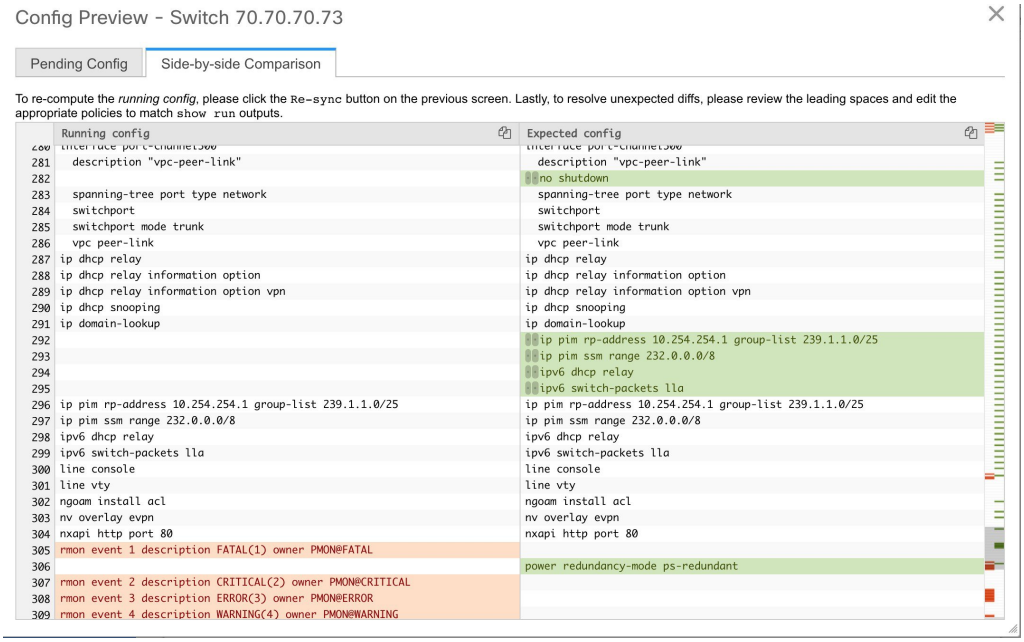
スイッチ自由形式ポリシーは、次のように作成されます。



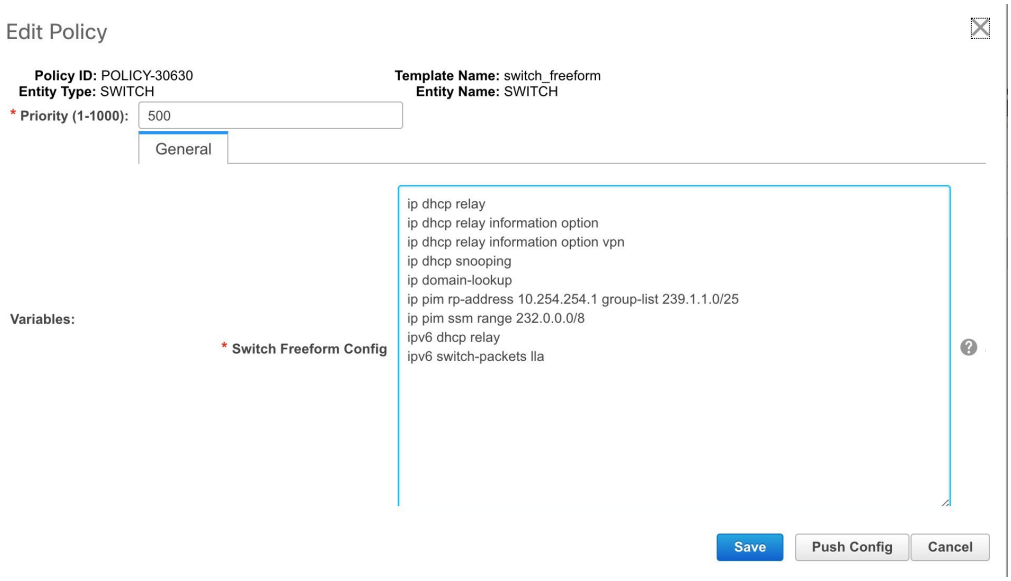
このポリシーがスイッチに正常に展開されると、DCNM は次のように永続的に差分をレポートします。



[並列比較（Side-by-side Comparison）] タブをクリックすると、差分の原因を確認できます。以下のように、**[ip pim rp-address]** 行の先頭には 2 文字のスペースがありますが、実行構成の先頭にはスペースがありません。

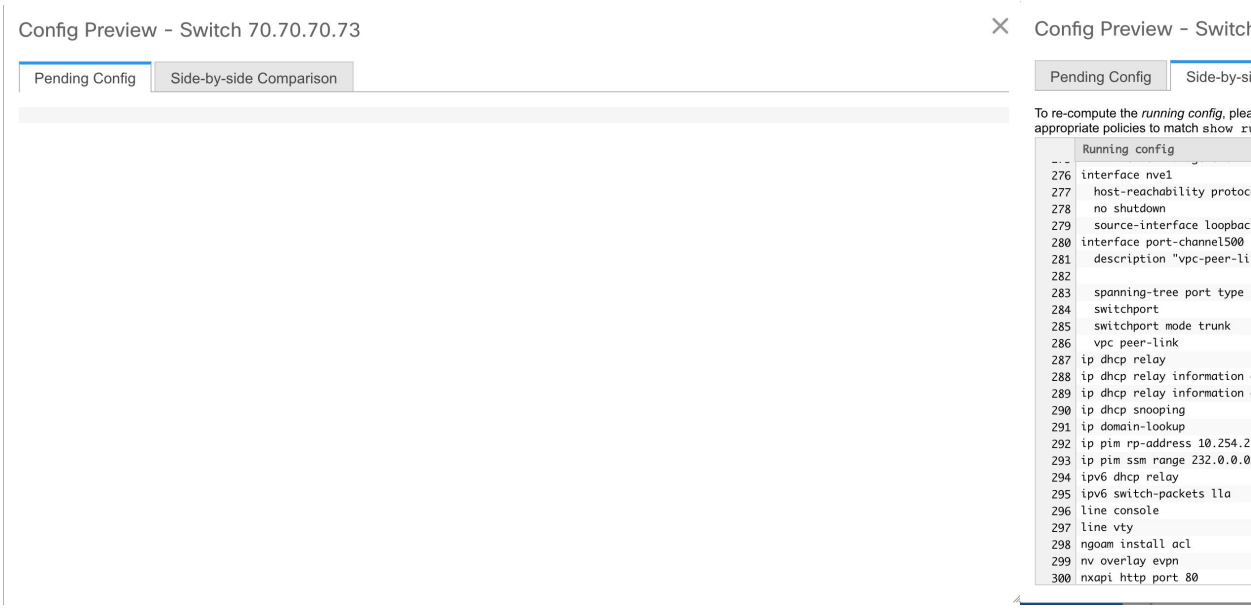


この相違を解決するには、対応するスイッチの自由形式ポリシーを編集して、スペースを合わせます。



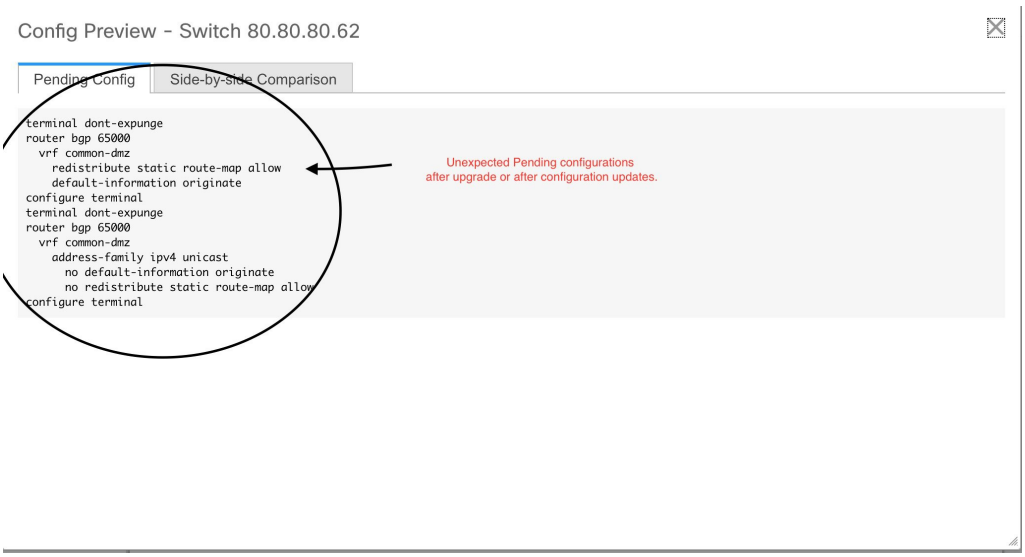
保存後、**[構成のプッシュ（Push Config）]** または **[保存と展開（Save & Deploy）]** オプションを使用して差分を再計算します。

以下に示すように、差分が解決されたことがわかります。**[並列比較（Side-by-side Comparison）]** タブで、先頭のスペースが更新されていることを確認します。

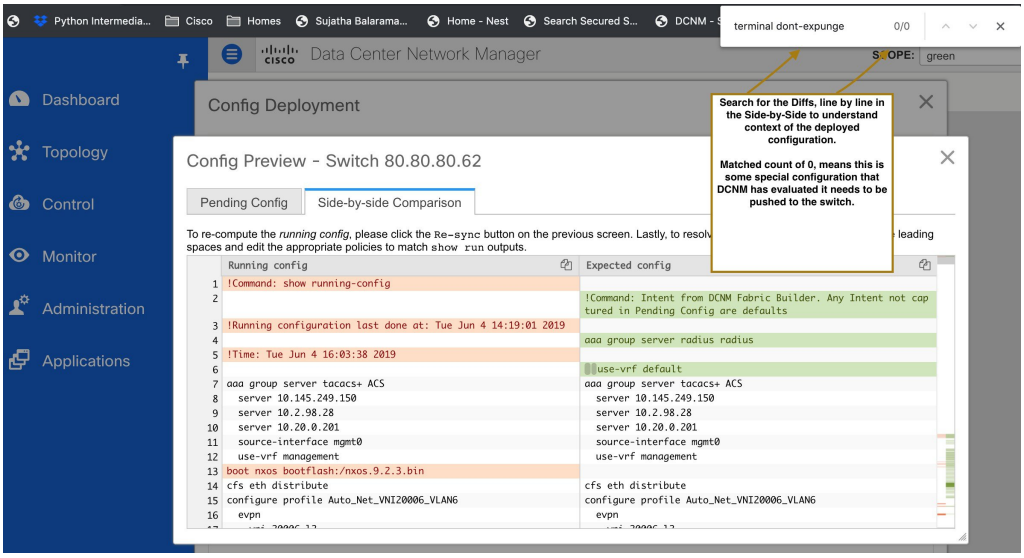


例 2：オーバーレイ構成での先頭スペース エラーの解決

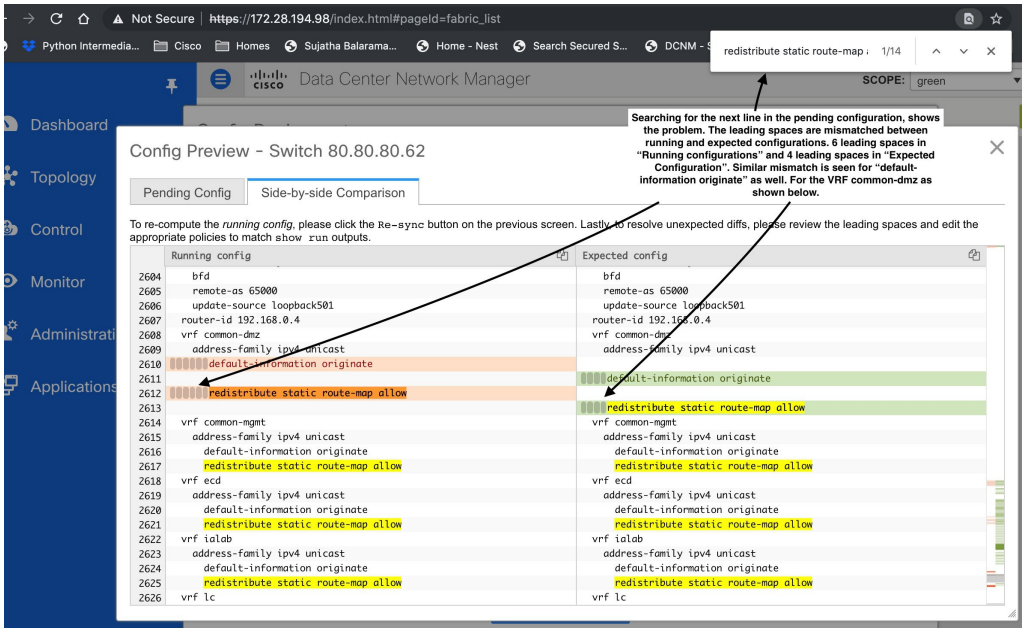
[保留中の構成（Pending Config）] タブに表示される先頭スペース エラーの例を考えてみましょう。



[並列比較（Side-by-side Comparison）] タブで、展開された構成のコンテキストを理解するために、行ごとの差分を検索します。

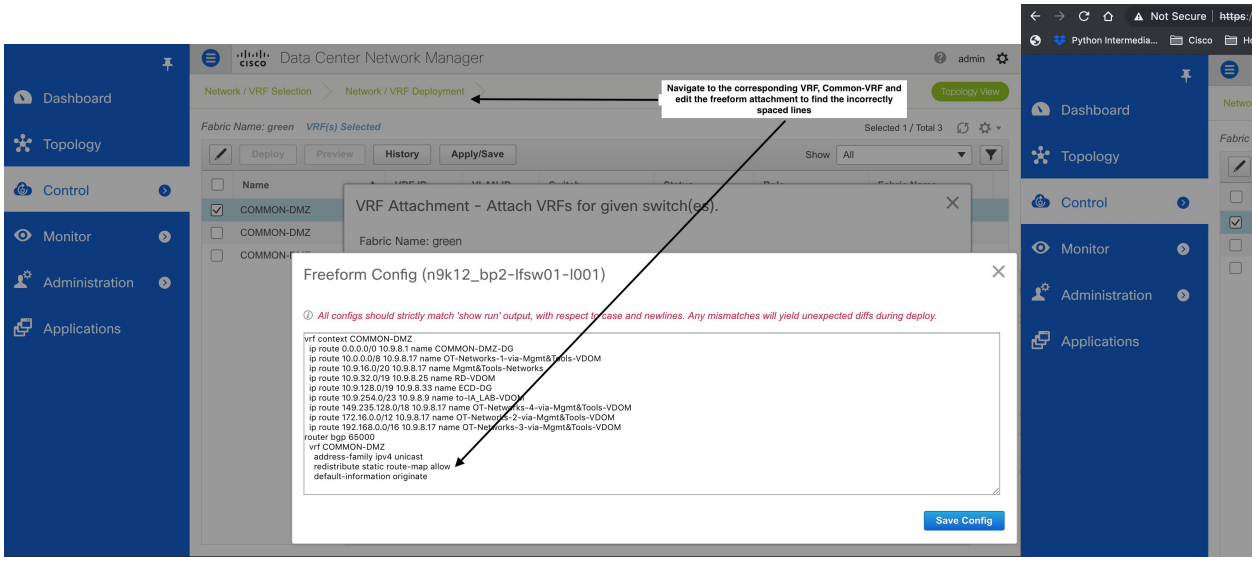


一致数が 0 の場合は、DCNM がスイッチにプッシュするために評価した特別な構成であることを意味します。



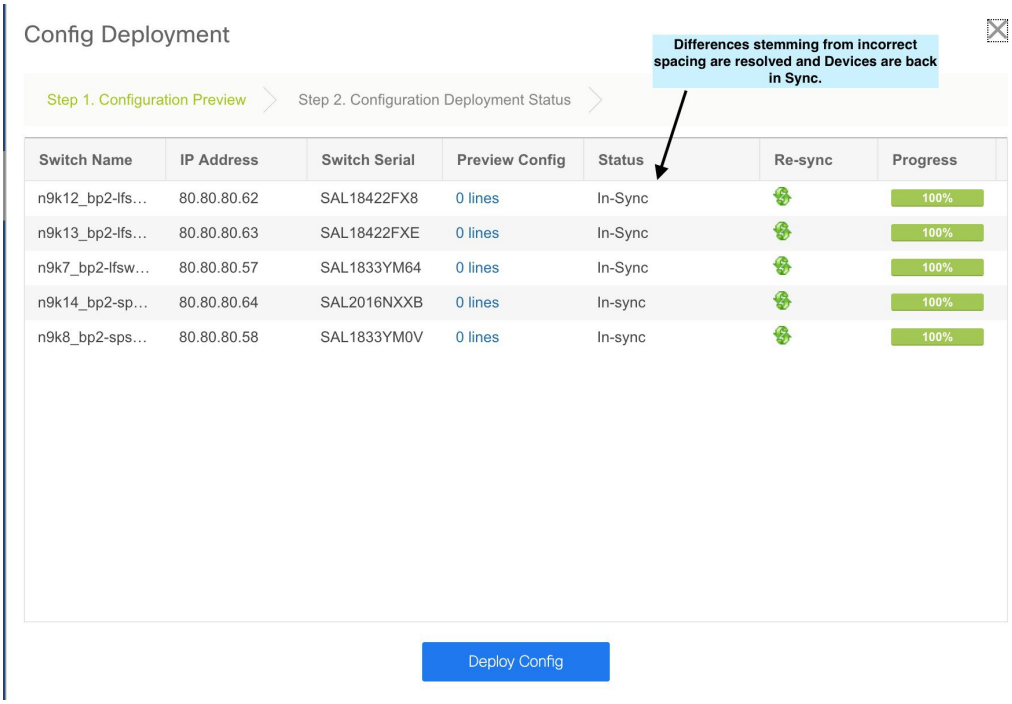
実行中の構成と期待される構成の間で、先頭のスペースが一致していないことがわかります。

それぞれの自由形式の構成に移動し、先頭のスペースを修正して、更新された構成を保存します。



ファブリックの **[ファブリック ビルダ（Fabric Builder）]** ウィンドウに移動し、**[保存と展開（Save & Deploy）]** をクリックします。

[構成展開（Config Deployment）] ウィンドウで、すべてのデバイスが同期していることがわかります。



外部ファブリックでのコンプライアンスの構成

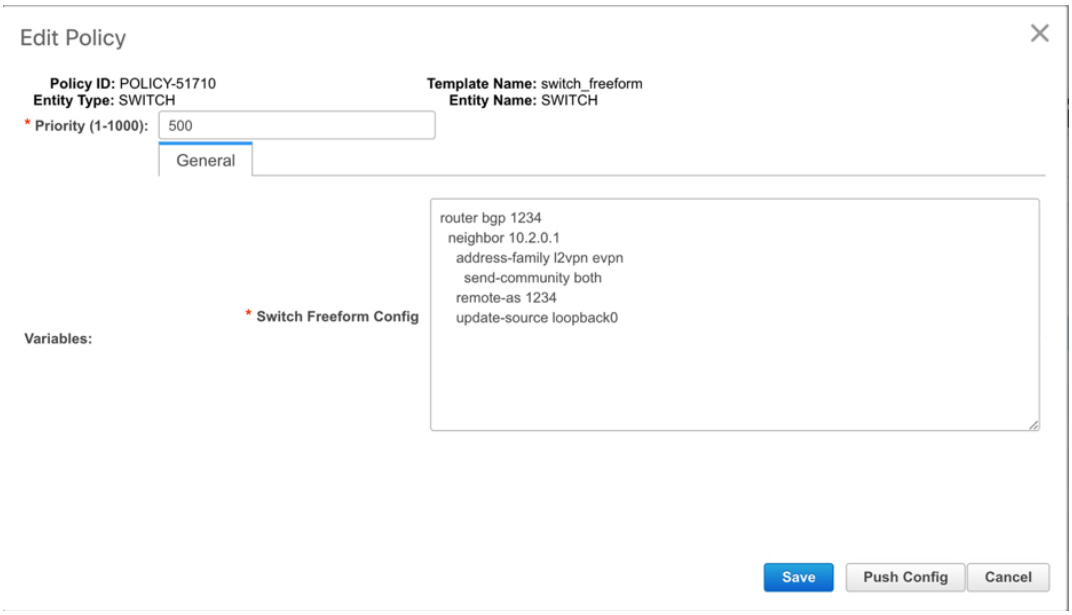
外部ファブリックを使用すると、Nexus スイッチをファブリックにインポートできます。展開のタイプに制限はありません。LAN クラシック、VXLAN、FabricPath、vPC、HSRP などを使用できます。スイッチが外部ファブリックにインポートされるとき、非中断となるようにスイッチの設定が保持されます。スイッチユーザ名やmgmt0インターフェイスなどの基本ポリシーのみが、スイッチのインポート後に作成されます。

外部ファブリックでは、DCNM で定義されているインテントに対して、構成コンプライアンス（CC）により、このインテントが対応するスイッチに存在することが保証されます。このインテントがスイッチに存在しない場合、CC は **OUT-OF-SYNC** ステータスを報告します。さらに、このインテントをスイッチにプッシュしてステータスを **IN-SYNC** に変更するために生成された保留中の構成があります。スイッチ上にあるが、DCNM で定義されたインテントではない追加の構成は、インテント内の構成との競合がない限り、CC によって無視されます。

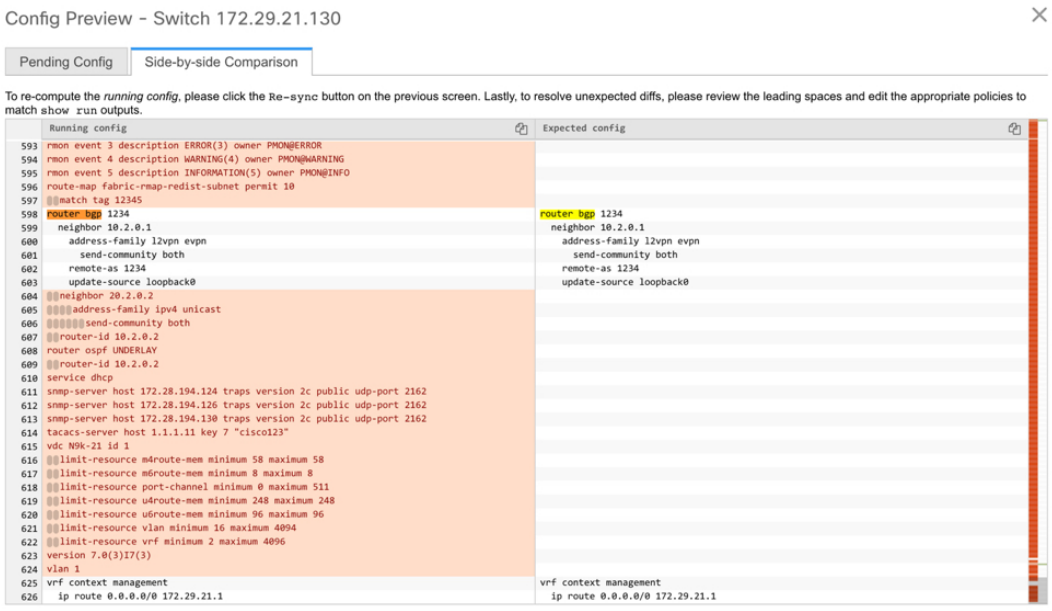
前述のように、ユーザー定義のインテントが DCNM に追加され、同じトップレベル コマンドの下にスイッチの追加構成がある場合、CC は DCNM で定義されたインテントがスイッチに存在することのみを確認します。DCNM 上のこのユーザー定義インテントがスイッチから削除する目的で全体として削除され、対応する構成がスイッチに存在する場合、CC はスイッチの **OUT-OF-SYNC** ステータスをレポートし、**保留中の構成** を作成してスイッチからその構成を削除します。この保留中の設定には、トップレベルのコマンドの削除が含まれています。このアクションにより、このトップレベルコマンドでスイッチで行われた他のアウトオブバンド設定も削除されます。この動作を上書きすることを選択した場合は、自由形式ポリシーを作成し、関連する最上位コマンドを自由形式ポリシーに追加することを推奨します。

この動作を例で見てみましょう。

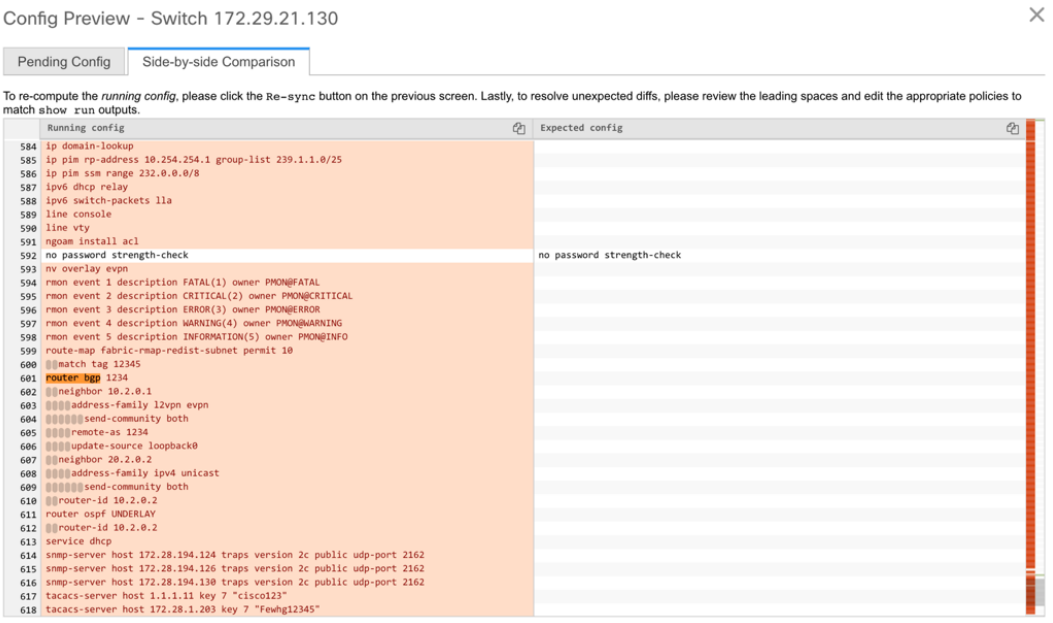
1. **switch_freeform** ポリシーはユーザーによって DCNM に定義され、スイッチに展開されています。

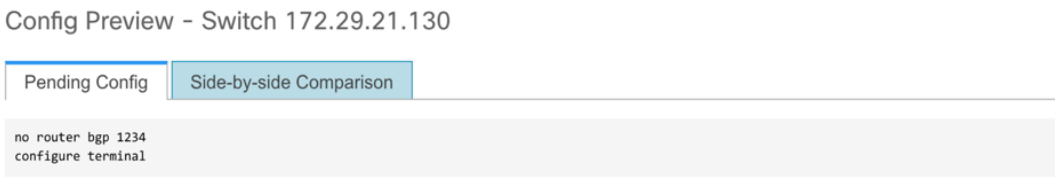


2. **実行構成** の **ルータ bgp** の下に、ユーザー定義 DCNM インテントの **予期される構成** に存在しない追加構成があります。DCNM でユーザー定義のインテントなしでスイッチに存在する追加の構成を削除する **保留中の構成** はありません。

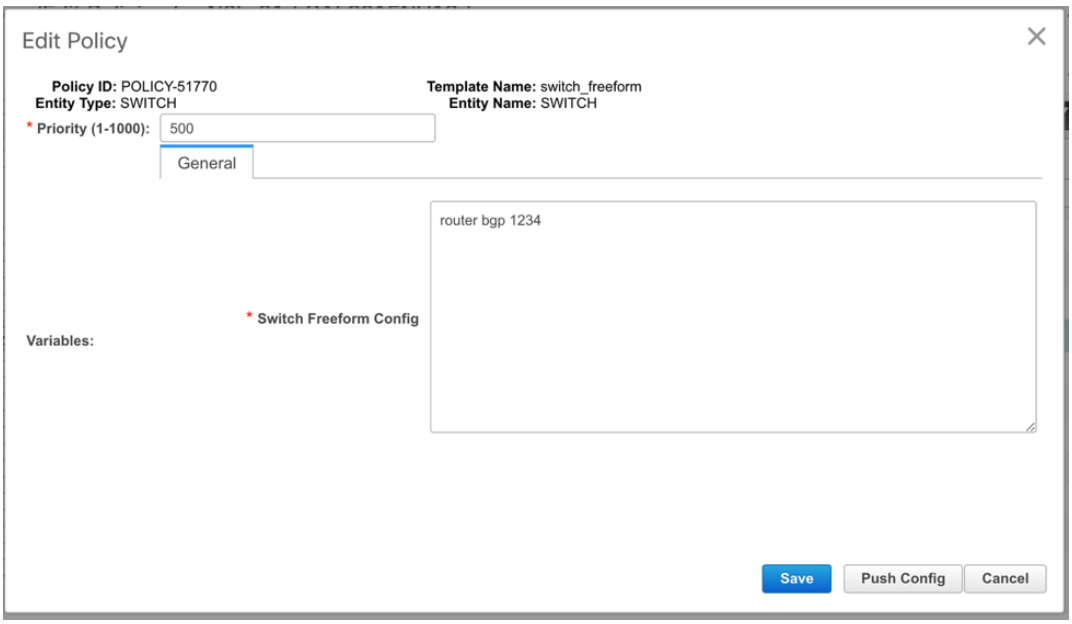


3. 手順 1 で作成された switch_freeform ポリシーを削除することで、DCNM によって以前にプッシュされたインテントが DCNM から削除された場合の **[保留中の構成（Pending Config）]** と **[サイドバイサイド比較（Side-by-side Comparison）]**。

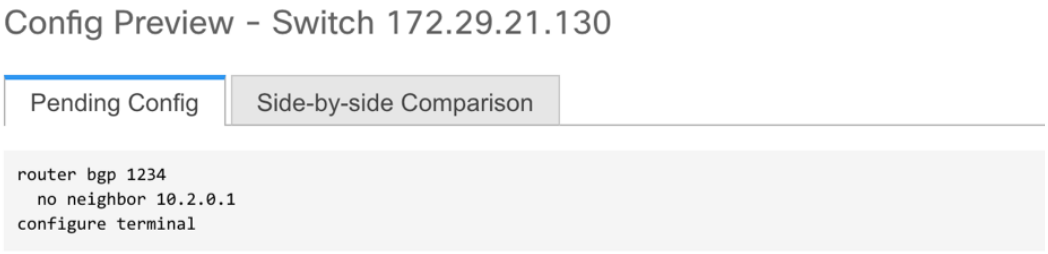


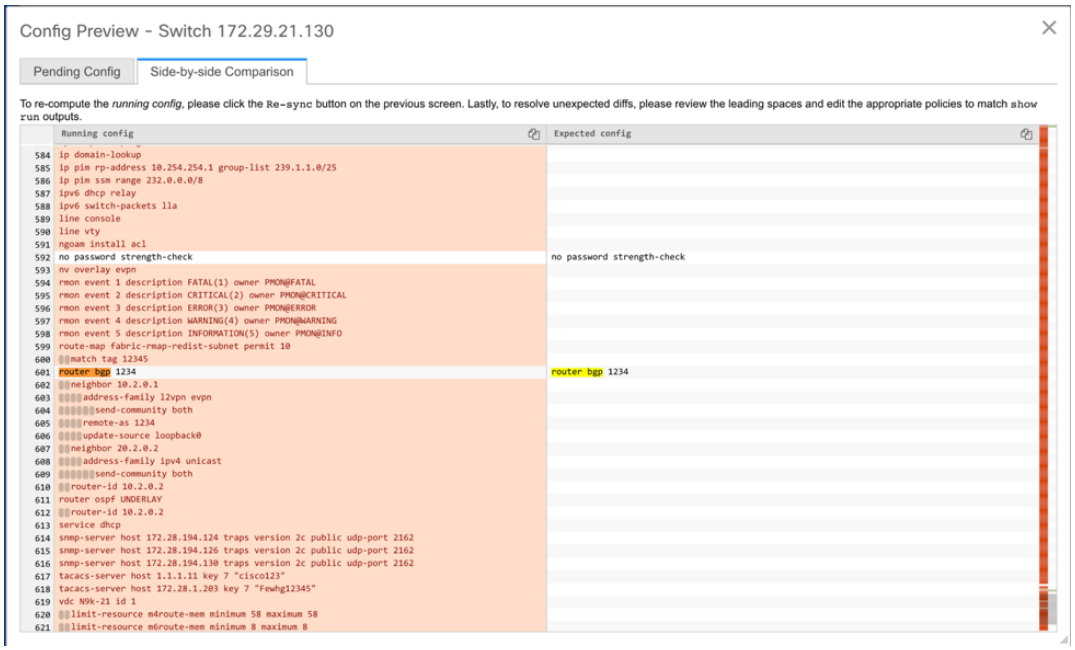


4. 最上位のrouter bgpコマンドを使用してswitch_freeformポリシーを作成する必要があります。これにより、CC は以前に DCNM からプッシュされた目的のサブ構成のみを削除するために必要な構成を生成できます。



5. 削除された構成は、以前に DCNM からプッシュされた構成のサブセットのみです。





外部ファブリックのスイッチのインターフェイスでは、DCNMはインターフェイス全体を管理するか、まったく管理しません。CC は次の方法でインターフェイスをチェックします。

- 任意のインターフェイスについて、ポリシーが定義され、関連付けられている場合、このインターフェイスは管理対象と見なされます。このインターフェイスに関連付けられているすべての設定は、関連付けられたインターフェイス ポリシーで定義する必要があります。これは、論理インターフェイスと物理インターフェイスの両方に適用されます。それ以外の場合、CC は、インターフェイスに行われたアウトオブバンド更新を削除して、ステータスを **[IN-SYNC]** に変更します。
- アウトオブバンドで作成されたインターフェイス（ポートチャネル、サブインターフェイス、SVI、ループバックなどの論理インターフェイスに適用）は、通常の検出プロセスの一部としてDCNMによって検出されます。ただし、これらのインターフェイスにはインテントがないため、CCはこれらのインターフェイスの**[OUT-OF-SYNC]**ステータスをレポートしません。
- どのインターフェイスでも、モニタポリシーはDCNMに常に関連付けられています。この場合、CC は **[IN-SYNC]** または **[OUT-OF-SYNC]** 構成コンプライアンスステータスをレポートするときに、インターフェイスの構成を無視します。

構成コンプライアンスで無視される特別な構成 CLI

次の構成 CLI は、構成コンプライアンス チェック中に無視されます。

- 「ユーザー名」とともに「パスワード」が含まれている CLI
- 「snmp-server user」で始まるすべての CLI

上記に一致する CLI は保留中の差分に表示されず、**[ファブリック ビルダ（Fabric Builder）]** ウィンドウで **[保存と展開（Save & Deploy）]** をクリックしても、そのような構成はスイッチにプッシュされません。これらの CLI は、**[並列比較（Side-by-side Comparison）]**ウィンドウにも表示されません。

このような構成 CLI を展開するには、次の手順を実行します。

1. **[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** を選択し、**[表形式ビュー（Tabular View）]** をクリックして、**[名前（Name）]** 列でスイッチを選択する、または、**[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** を選択してデバイスを右クリックします。
2. **[ポリシーの表示/編集（View/Edit Policies）]** をクリックして、**[+]** をクリックして新しいポリシーを追加します。**[ポリシーの追加（Add Policy）]** ウィンドウが表示されます。
3. **[switch_freeform]** テンプレートを使用して、必要な構成 CLI を含む PTI を追加し、**[保存（Save）]** をクリックします。
4. 作成したポリシーを選択し、**[構成をプッシュ（Push Config）]** をクリックして、構成をスイッチに展開します。

大文字と小文字を区別しないコマンドの差分の解決

デフォルトでは、インテントを比較する際に DCNM で生成されるすべての差分（予期される構成と実行構成の差分）では、大文字と小文字が区別されます。ただし、スイッチには大文字と小文字を区別しないコマンドも多くあるため、これらのコマンドで相違点が存在するとしてフラグを付けるのは適切でない場合があります。これらの外れ値は、**compliance_case_insensitive_clis.txt** テキスト ファイルにキャプチャされます。

既存の **compliance_case_insensitive_clis.txt** ファイルに含まれていない追加のコマンドは、大文字と小文字を区別するものとして扱うべきです。構成の保留が、DCNM が予期している構成と実行構成との間の大文字と小文字の違いによって生じたものである場合、次の方法で、大文字と小文字の違いを無視するように DCNM を構成できます。

1. DCNM ファイル システムで次のファイルを変更します。

   `/usr/local/cisco/dcm/dcnm/model-config/compliance_case_insensitive_clis.txt`

   compliance_case_insensitive_clis.txt ファイルのサンプル エントリが次のように表示されます。

```
[root@dcnm98 model-config]# pwd
/usr/local/cisco/dcm/dcnm/model-config
[root@dcnm98 model-config]# cat compliance_case_insensitive_clis.txt
"^(no |)interface\s+Port(.)"
"^(no |)interface\s+Loo(.)"
"^(no |)interface\s+Eth(.)"
"^update-source\s+Loo(.)"
"^vrf\s+"
"^hardware profile portmode\s+"
"^(.*)route-map\s+(.)"
"^(.*)neighbor-policy(.)"
"(no |)encapsulation\s+(.)"
"(.*)alert-group\s+(.)"
"^streetaddress\s+(.)"
"^transport email\s+(.)"
"(no |)action\s+(.)"
"(no|)\s+\d*\s+remark.*"
[root@dcnm98 model-config]#
```

展開中に新しいパターンが検出され、それらが構成の保留をトリガーしている場合、これらのパターンをこのファイルに追加します。パターンは、有効な正規表現パターンである必要があります。

これにより、DCNMは、比較の実行中に、記述された構成パターンを大文字と小文字を区別しないものとして扱うことができます。

2. ファブリックについて、**[保存と展開（Save & Deploy）]** をクリックして、更新された比較出力を表示します。

スイッチのインポート後の構成コンプライアンスの解決

Cisco DCNM にスイッチをインポートした後、管理インターフェイス（mgmt0）の説明フィールドに余分なスペースがあるため、スイッチの構成コンプライアンスが失敗することがあります。

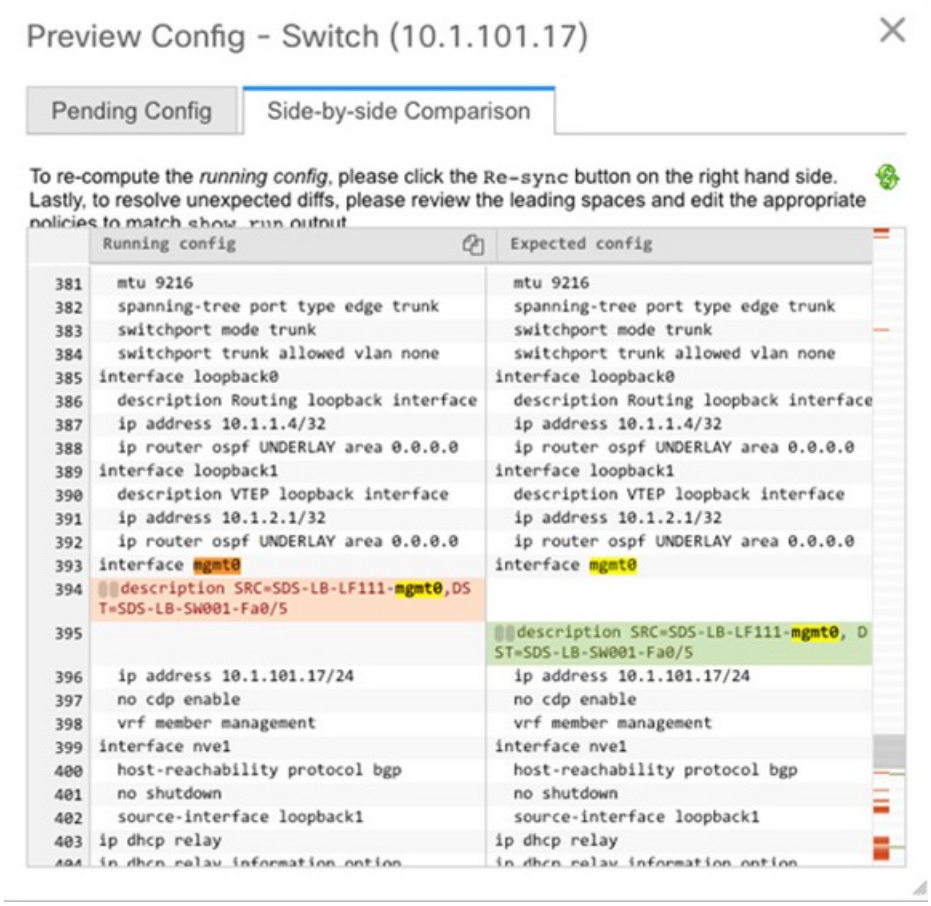
たとえば、スイッチをインポートする前に：

```
interface mgmt0
  description SRC=SDS-LB-LF111-mgmt0, DST=SDS-LB-SW001-Fa0/5
```

スイッチをインポートして構成プロファイルを作成したら、次の手順を実行します。

```
interface mgmt0
  description SRC=SDS-LB-LF111-mgmt0,DST=SDS-LB-SW001-Fa0/5
```

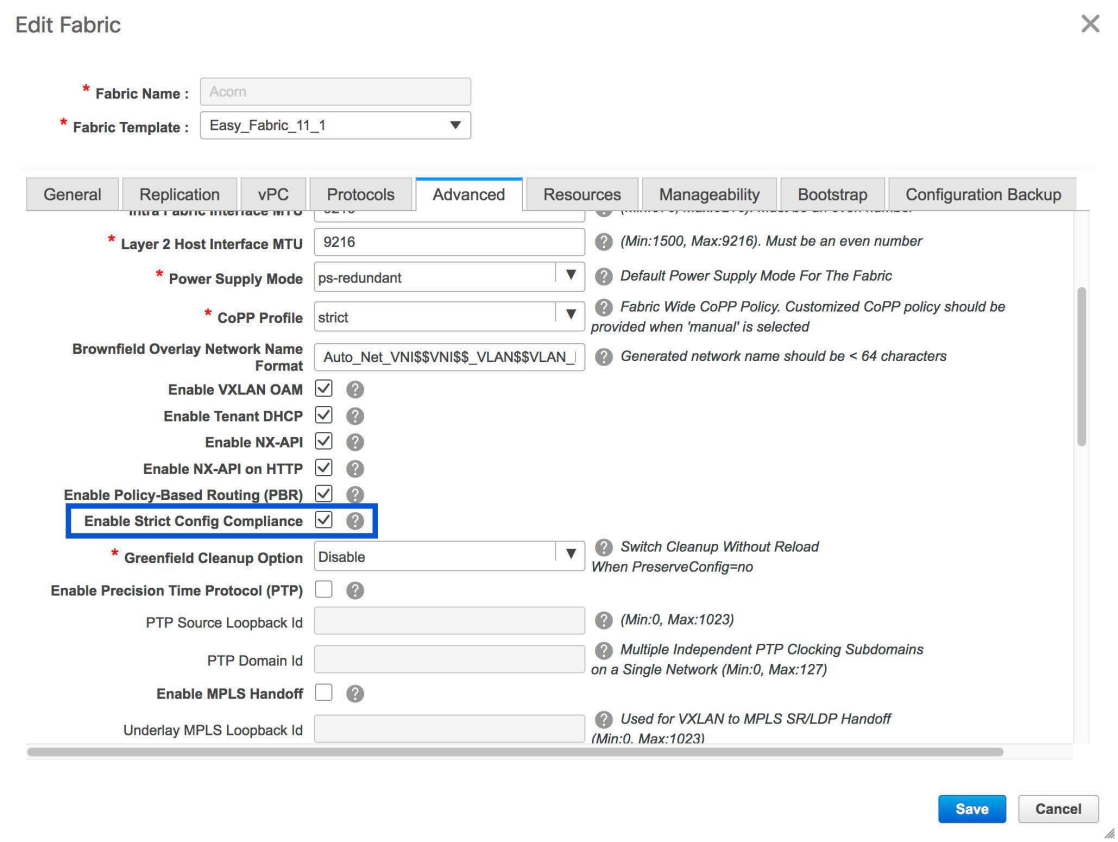
この例では、コンマ（,）の後のスペースが削除されています。



mgmt0インターフェイスを選択した後、インターフェイスマネージャに移動し、**[編集（Edit）]** アイコンをクリックします。説明の余分なスペースを削除してください。

厳密な構成コンプライアンス

Cisco DCNM リリース 11.3(1) から厳密な構成コンプライアンスは、スイッチ構成と関連するインテント間の相違をチェックし、スイッチに存在するが関連するインテントに存在しない構成の **no** コマンドを生成します。**[保存して展開（Save and Deploy）]** をクリックすると、関連付けられたインテントに存在しないスイッチ構成が削除されます。この機能を有効にするには、**[厳密な公正コンプライアンスを有効にする（Enable Strict Config Compliance）]** チェックボックスをオンにします。これは **[詳細設定（Advanced）]** タブ（**[ファブリックの追加（Add Fabric）]** または **[ファブリックの編集（Edit Fabric）]** ウィンドウ）にあります。デフォルトで、この機能は無効になっています。



厳密な構成コンプライアンス機能は、Easy Fabric テンプレート（Easy_Fabric_11_1 および Easy_Fabric_eBGP）でサポートされています。スイッチによって自動生成されるコマンド（vdc、rmon など）について差分が生成されないようにするために、CC はデフォルトのコマンドのリストを含むファイルを使用して、これらのコマンドに対して差分が生成されないようにします。このファイルは、**/usr/local/cisco/dcm/dcnm/model-config/strict_cc_exclude_clis.txt** にあります。

（注）

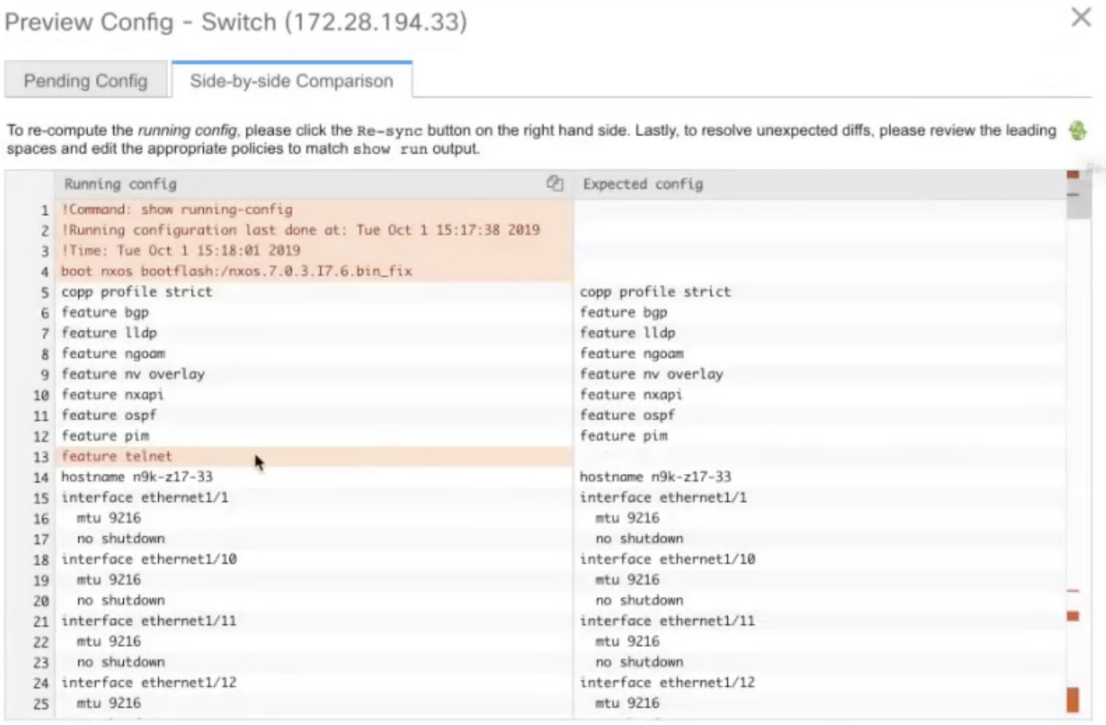
- 厳密な構成コンプライアンスを有効にした後に差分が生成された場合、**[ファブリック ビルダー（Fabric Builder）]** ウィンドウでスイッチアイコンが青色に変わります。

例：厳密な構成コンプライアンス

コマンドがスイッチで構成されているが、インテントに存在しない例を考えてみましょう。**feature telnet** このようなシナリオでは、CC チェックが実行された後、スイッチのステータスが**非同期**として表示されます。

次に、非同期スイッチの **[構成のプレビュー（Preview Config）]** をクリックします。厳密な構成コンプライアンス機能が有効になっているため、**[構成のプレビュー（Preview Config）]** ウィンドウの **[保留中の構成（Pending Config）]** の下に **feature telnet** コマンドの **no** 形式が表示されます。

[並べて比較（Side-by-Side Comparison）] タブには、実行構成と予想される構成の差が並べて表示されます。Cisco DCNM リリース 11.3(1)から**[再同期（Re-sync）]** ボタンは、構成のプレビューウィンドウの [並べて比較（Side-by-Side Comparison）] タブの右上隅にも表示されます。大規模なアウトオブバンド変更がある場合、または設定変更が DCNM に正しく登録されていない場合に、このオプションを使用して DCNM 状態を再同期します。



再同期操作は、スイッチに対して完全なCC実行を実行し、「show run」および「show run all」コマンドをスイッチから再収集します。再同期プロセスを開始すると、進行状況メッセージが画面に表示されます。再同期中に、実行構成がスイッチから取得されます。スイッチのOut-of-Sync/In-Syncステータスは、DCNMで定義されたインテントに基づいて再計算されます。

次に、**[構成のプレビュー（Preview Config）]**ウィンドウを閉じ、**[保存と展開（Save and Deploy）]**をクリックします。厳密な構成コンプライアンス機能により、**feature telnet** コマンドの **no** 形式をスイッチにプッシュすることによって、スイッチの実行構成がインテントから逸脱しないようにします。構成間の相違が強調表示されます。**feature telnet** コマンド以外の差分は、デフォルトのスイッチ構成およびブート構成であり、厳密なCCチェックでは無視されます。

Cisco DCNMリリース11.2(1)以前のリリースでは、[ファブリックのビルダー（Fabric Builder）]ウィンドウでスイッチを右クリックし、**[構成を展開（Deploy Config）]**を選択して**[構成展開（Config Deployment）]**ウィンドウを表示する必要がありました。次に、特定のスイッチの**[構成のプレビュー（Preview Config）]**をクリックして、そのスイッチの保留中の構成を表示する**[構成のプレビュー（Preview Config）]**ウィンドウを表示する必要がありました。これにより、ユーザは、プレビュー構成が誤ってスイッチに展開されていると考える可能性があります。Cisco DCNMリリース11.3(1)から**[ファブリックのビルダー（Fabric Builder）]**ウィンドウでスイッチを右クリックして**[構成のプレビュー（Preview Config）]**を選択すると、**[構成のプレビュー（Preview Config）]**ウィンドウが表示されます。このウィンドウには、意図に準拠した構成を実現するためにスイッチにプッシュする必要がある保留中の構成が表示されます。

カスタム自由形式構成を DCNM に追加して、DCNM での目的の構成とスイッチ構成を同一にすることができます。その後、スイッチは同期中ステータスになります。DCNM にカスタム自由形式構成の追加方法の詳細については、「ファブリック スイッチでのフリーフォーム設定の有効化」を参照してください。

ファブリック スイッチでのフリーフォーム設定の有効化

DCNM では、次の方法でフリーフォーム ポリシーを使用してカスタム設定を追加できます。

1. ファブリック全体
   - ファブリック内のすべてのリーフ、ボーダー リーフ スイッチ上で一度に。
   - すべてのスパインとボーダー スパイン スイッチで一度に。
2. 特定のスイッチ上で。

リーフ スイッチは、リーフ、境界、および境界ゲートウェイのロールによって識別され、スパイン スイッチは、スパイン、境界スパイン、および境界ゲートウェイ スパインのロールによって識別されます。

Note 自由形式の CLI は、ファブリックを作成するときでも、ファブリックがすでに作成されているときでも展開できます。次に、既存のファブリックでの例を示します。ただし、これは新しいファブリックを作成するときでも参考にすることができます。

リーフおよびスパイン スイッチ上でのファブリック全体のフリーフォーム CLI の導入

1. **[制御（Control）] > [Fabric Builder]**の順にクリックします。[Fabric Builder] 画面が表示されます。長方形のボックスが各ファブリックを表します。
2. 既存のファブリックにカスタム構成を追加するには、**[ファブリックの編集（Edit Fabric）]** アイコン（長方形のボックスの右上部分）をクリックします。**[ファブリックの編集 (Edit Fabric)]** 画面が表示されます。

   （ファブリックを初めて作成する場合は、**[ファブリックの作成 (Create Fabric)]** をクリックします）。
3. **[詳細設定 (Advanced)]** タブをクリックし、次のフィールドを更新します。

   [リーフのフリーフォーム構成 (Leaf Freeform Config)]：このフィールドでは、ファブリック内のすべてのリーフ、境界リーフ、および境界リーフ スイッチの構成を追加します。

   [スパインのフリーフォーム構成 (Spine Freeform Config)] - このフィールドでは、ファブリック内のすべてのスパイン、境界スパイン、および境界ゲートウェイ スパイン スイッチの構成を追加します。

Note 目的の設定を正しいインデントでコピー アンド ペーストします。Nexus スイッチでの実行コンフィギュレーションを参考にしてください。詳細については、スイッチのフリーフォーム設定エラーの解決, on page 411を参照してください。

4. [保存（Save）] をクリックします。[ファブリック トポロジ (fabric topology)] 画面が表示されます。
5. 画面の右上にある **[保存して展開 (Save & Deploy)]** をクリックして、構成を保存して展開します。

   構成の遵守機能により、これらの CLI で示された目的の設定がスイッチ上に確実に存在するようにします。仮にそれらが削除されるか、ミスマッチが生じた場合には、ミスマッチとしてフラグが付けられ、デバイスが同期外れであることが示されるようにします。

*[*不完全な構成の遵守 *(Incomplete Configuration Compliance)]*：一部の Cisco Nexus 9000 シリーズ スイッチでは、**[保存して展開 (Save & Deploy)]** オプションを使用して保留中のスイッチ構成を構成しても、意図した構成とスイッチ構成の間にミスマッチが生じる場合があります。問題を解決するには、影響を受けるスイッチに **switch_freeform** ポリシーを追加します（「特定のスイッチへのフリーフォーム *CLI* の展開」の項を参照）。たとえば、次の永続的な保留設定を考えてみます。

```
line vty
logout-warning 0
```

上記の設定をポリシーに追加し、更新を保存したら、トポロジ画面で **[保存して展開 (Save and Deploy)]** をクリックして展開プロセスを完了します。

スイッチを同期状態に戻すには、上記の構成を保存した **switch_freeform** ポリシーで追加し、スイッチに展開します。

特定のスイッチへのフリーフォーム CLIの導入

1. **[制御（Control）] > [Fabric Builder]**の順にクリックします。[Fabric Builder] 画面が表示されます。
2. ファブリックを表す長方形のボックスをクリックします。[ファブリック トポロジ（fabric topology）] 画面が表示されます。

Note 新しいファブリックにフリーフォームのCLIをプロビジョニングするには、ファブリックを作成し、そのファブリックにスイッチをインポートしてから、フリーフォームの CLI を展開する必要があります。

3. スイッチ アイコンを右クリックし、**[ポリシーの表示/編集（View/edit policies）]** オプションを選択します。

[ポリシーの表示/編集（View/edit policies）] 画面が表示されます。

4. **[+]** をクリックします。**[ポリシーの追加（Add Policy）]** 画面が表示されます。

   [プライオリティ (Priority)] フィールドで、優先順位はデフォルトで500に設定されます。展開時に上位に表示する必要がある CLI には、（低い番号を指定して）高い優先順位を選択できます。たとえば、機能を有効にするコマンドは、コマンドリストの前に表示されます。

5. **[ポリシー]** フィールドから、**switch_freeform** を選択します。

6. **[フリーフォーム CLI (Freeform Config CLI)]** ボックスで CLI を追加または更新します。

   目的の設定を正しいインデントでコピーアンドペーストします。Nexus スイッチでの実行コンフィギュレーションを参考にしてください。詳細については、スイッチのフリーフォーム設定エラーの解決, on page 411を参照してください。

7. [保存（Save）] をクリックします。

   ポリシーが保存されると、そのスイッチの目的の設定に追加されます。

8. ポリシー画面を閉じます。ファブリック トポロジが再び起動します。

9. スイッチを右クリックし、**[構成の展開（Deploy Config）]** をクリックします。

   [保存して展開（Save ＆Deploy）] オプションは、展開にも使用できます。ただし、**[保存して展開（Save ＆Deploy）]** オプションを使用すると、すべてのファブリック スイッチで意図した構成と実行構成のミスマッチが特定されます。

switch_freeform ポリシー構成：

- ポリシーでは複数のインスタンスを作成できます。
- vPCスイッチペアの場合は、両方のvPCスイッチで一貫した **switch_freeform** ポリシーを作成します。
- **switch_freeform** ポリシーを編集してスイッチに展開すると、（[プレビュー（Preview）] オプションの **[並べて表示（Side-by-side）]** タブで）変更内容を確認できます。

フリーフォーム CLI の設定例

コンソール ラインの設定

この例では、一部のファブリック全体のフリーフォーム設定（すべてのリーフ スイッチとスパイン スイッチ）、および個々のスイッチ設定を展開します。

ファブリック全体のセッション タイムアウトの設定：

```
line console
  exec-timeout 1
```

特定のスイッチのコンソール速度設定：

```
line console
  speed 115200
```

ACL の設定

ACL 設定は通常、ファブリック全体ではなく、特定のスイッチ（リーフ/スパイン スイッチ）で設定されます。スイッチで ACL をフリーフォーム CLIとして設定する場合は、シーケンス番号を含める必要があります。それ以外の場合は、意図した設定と実行での設定が一致しなくなります。シーケンス番号の設定例：

```
ip access-list ACL_VTY
  10 deny tcp 172.29.171.67/32 172.29.171.36/32
  20 permit ip any any
ip access-list vlan65-acl
  10 permit ip 69.1.1.201/32 65.1.1.11/32
  20 deny ip any any

interface Vlan65
  ip access-group vlan65-acl in
line vty
  access-class ACL_VTY in
```

switch_freeform ポリシーでシーケンス番号なしで ACL を構成した場合は、スイッチの実行構成に示されているようにシーケンス番号でポリシーを更新します。

ポリシーを更新して保存したら、デバイスを右クリックし、スイッチごとに**[設定の展開(Deploy Config)]** オプションを選択して設定を展開します。または、ファブリック トポロジ画面 (Fabric Builder 内) の **[保存して展開]** オプションを使用して、ファブリックが構成遵守をトリガーし、構成のミスマッチを解決するようにします。

スイッチのフリーフォーム設定エラーの解決

実行設定を、NX-OS スイッチの実行設定に示されているように、正しいインデントでフリーフォーム設定にコピーアンドペーストします。フリーフォームの設定は、実行設定とマッチしている必要があります。それ以外の場合、DCNM の構成遵守は、スイッチを非同期としてマークします。

スイッチのフリーフォーム設定の例を見てみましょう。

```
feature bash-shell
feature telemetry

clock timezone CET 1 0
# Daylight saving time is observed in Metropolitan France from the last Sunday in March
 (02:00 CET) to the last Sunday in October (03:00 CEST)
clock summer-time CEST 5 Sunday March 02:00 5 Sunday October 03:00 60
clock protocol ntp

telemetry
  destination-profile
    use-vrf management
```

夏時間に関する強調表示された行は、**show running config** コマンドの出力には表示されないコメントです。したがって、インテントが実行設定とマッチしないため、設定コンプライアンスはスイッチを非同期としてマークします。

クロック プロトコルのスイッチの実行設定を確認します。

```
spine1# show run all | grep "clock protocol"
clock protocol ntp vdc 1
```

フリーフォームの設定に **vdc 1** がないことがわかります。

この例では、実行設定をフリーフォーム設定にコピーアンドペーストします。

更新されたフリーフォーム設定を次に示します。

```
feature bash-shell
feature telemetry

clock timezone CET 1 0
clock summer-time CEST 5 Sunday March 02:00 5 Sunday October 03:00 60
clock protocol ntp vdc 1

telemetry
  destination-profile
    use-vrf management
```

実行設定をコピーアンドペーストして展開すると、スイッチは同期されます。**[保存して展開（Save & Deploy）]** をクリックすると、**[構成プレビュー(Config Preview)]** ウィンドウの **[並べて比較 (Side-by-Side Comparison)]** により、定義済みのインテントと実行中の構成の違いに関する情報を表示します。

VMM ワークロードの自動化

VMM ワークロードの自動化は、VMware 環境で生成されたワークロード用の Cisco の Nexus スイッチでのネットワーク構成の自動化に関するものです。これは、Cisco DCNM リリース 11.4(1) のプレビュー機能です。

この自動化を示すビデオを見ることもできます。「ビデオ：Cisco DCNM での VMM ワークロードの自動化」を参照してください。

vCenter でのネットワークオブジェクトの概要

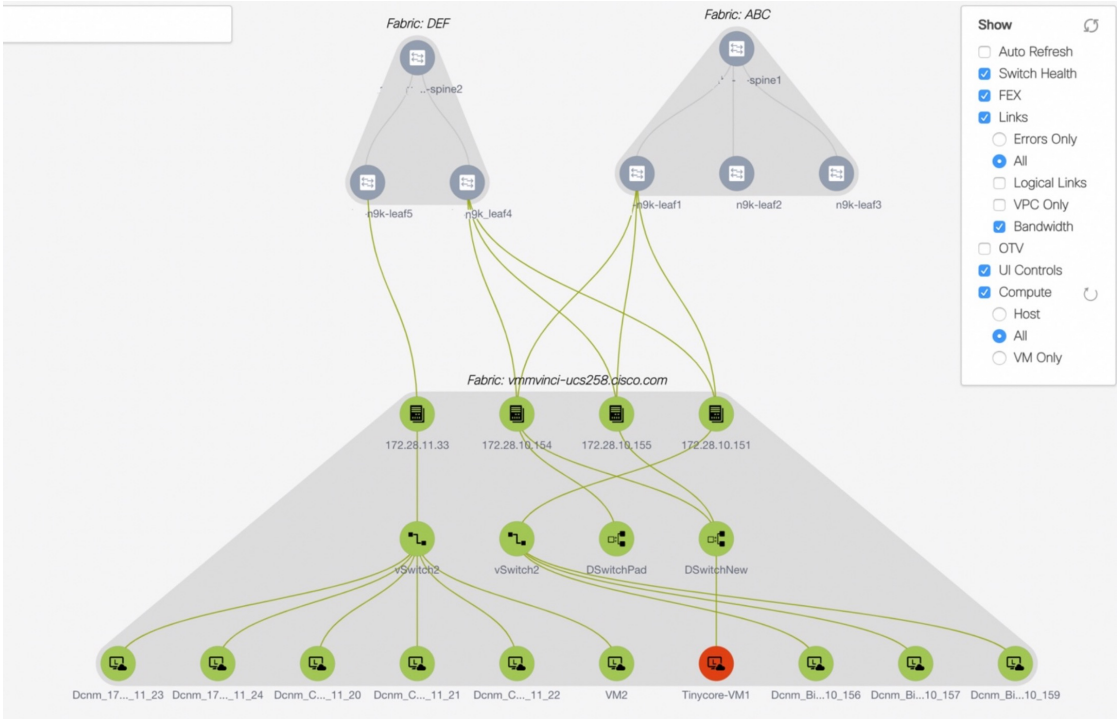
VMM ワークロードの自動化には、vCenter のネットワークオブジェクトを DCNM のネットワークオブジェクトにマッピングすることが含まれます。vCenter の次のネットワークオブジェクトが検討されます。

- 仮想スイッチ（VS）：通常の VS は、ソフトウェア ベースの切り替えを実行する ESXi ホストで実行されます。VS は複数のポート グループ（PG）を持つことができます。各 PG には、VLAN などのネットワークに接続するネットワークポート構成プロパティがあります。各 VS は、リーフスイッチに接続する複数のアップリンクポートを持つことができま

す。ESXi ホストで生成されたワークロードは、この VS で作成された PG に接続できます。

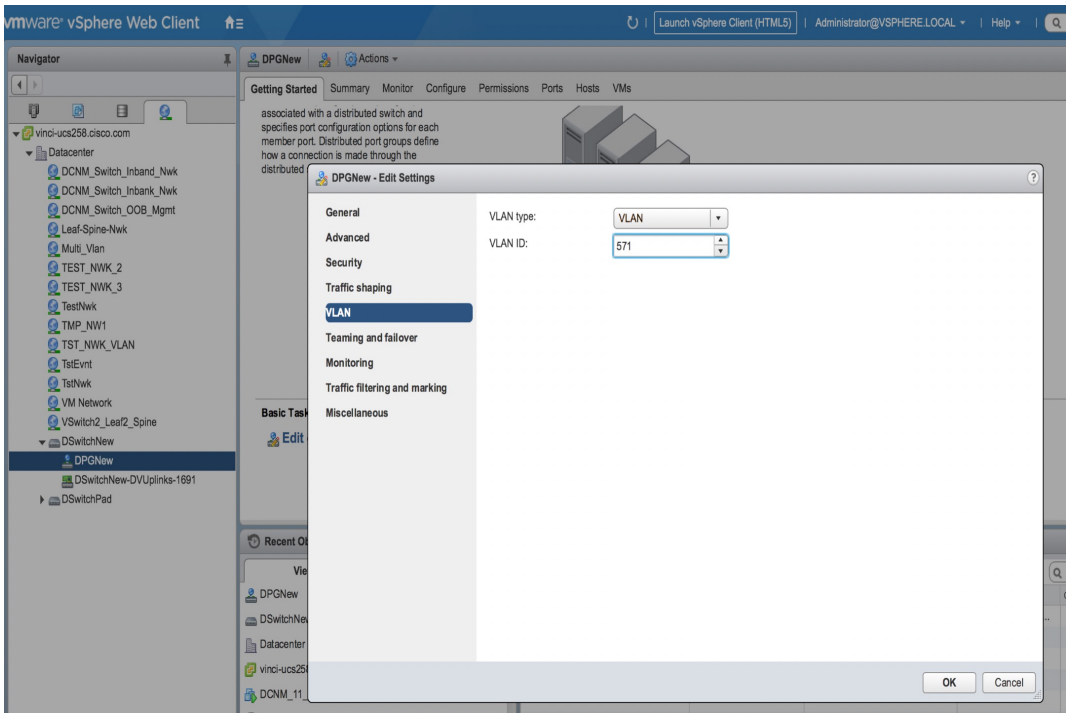
- 分散仮想スイッチ（DVS）：DVS は、複数の ESXi ホストにまたがる仮想スイッチです。通常の VS と同様に、DVS には分散ポート グループ（DPG）と呼ばれる複数のポート グループがあります。DPG には、VLAN など、ネットワークに接続するネットワークポート構成プロパティがあります。各 DVS は、リーフスイッチに接続できる複数のアップリンクポートを持つことができます。DVS のメンバーであるホストのいずれかで生成されたワークロードは、DPG に接続できます。このドキュメントおよび構成ファイルでは、DPG は分散仮想ポートグループ（DV-PG）とも呼ばれます。

DCNM の次のトポロジを考えてみましょう。

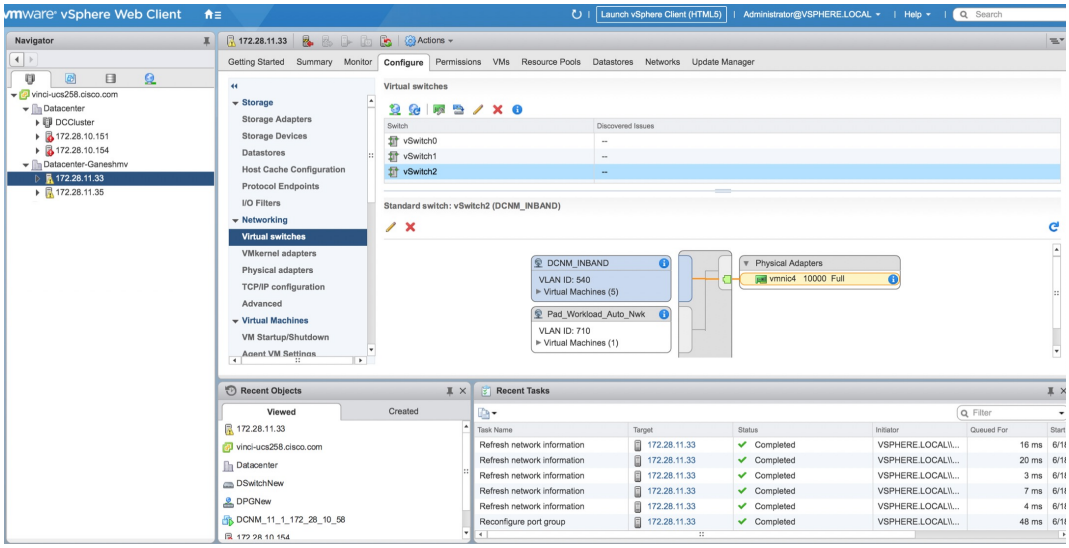


- セットアップには、IP アドレスを持つ 4 つのホストがあります。
  - 172.28.11.33
  - 172.28.10.154
  - 172.28.10.151
  - 172.28.10.155

- **DSwitchNew** という名前の DVS は、ホスト 172.28.10.154 と 172.289.10.155 にまたがって生成されます。この DVS には、図には示されていない **DPGNew** という名前の DPG があります。この DVS は、アップリンクポート <vmnic3, vmnic1> およびスイッチ インターフェイス <e1/25, e1/7> それぞれを介して、スイッチ n9k-leaf1 および n9k-leaf4 に接続します（図には示されていません）。571 の VLAN 値は、**DPG DPGNew** に関連付けられています。



- ホスト 172.28.11.33 には、vSwitch2 という名前の通常の vSwitch もあります。この VS には、DCNM_Inband という名前の PG があります。この VS は、アップリンクポート vmnic4 およびスイッチインターフェイス e1/23 を介してリーフスイッチ n9k-leaf5 に接続します。540 の VLAN 値は、PG **DCNM_Inband** に関連付けられています。



VMM ワークロード自動化の仕組み

ワークロードが生成されると、ネットワークまたはファブリックでのプロビジョニングが必要になります。vCenter で生成されたワークロードは、DPG または PG に関連付けられています。VMWare 内のこの DPG または PG は、対応する DCNM ネットワークにマッピングする必要が

あります。以前のトポロジの例として、ワークロードが PG **インバンド** を備えたホスト 172.28.11.33 で生成された場合、オーバーレイおよびアンダーレイ構成を含むネットワーク プロビジョニングは、関連するインターフェイス e1/23 を備えたリーフスイッチ n9k-leaf5 で発生する必要があります。

ネットワーク プロビジョニングを行うには、vCenter（DPG または PG）の各ネットワークオブジェクトを DCNM のネットワークオブジェクトにマッピングする必要があります。DCNM のネットワークオブジェクトには、次の特性があります。

- VRF Name
- VLAN ID
- IPv4/IPv6 サブネットおよびゲートウェイ情報
- セカンダリ IPv4/v6 およびゲートウェイ情報
- BGP-EVPN 構成

静的マッピングは、vCenter のネットワーク オブジェクトを DCNM のネットワーク オブジェクトにマッピングする構成ファイルで定義する必要があります。詳細については、VMM ワークロード自動化の構成ファイル （416 ページ）を参照してください。

構成ファイルにデータが入力されたら、ワークロード自動化モジュールを開始できます。このモジュールは、構成ファイル（conf.yml）で指定されたすべての vCenter をスキャンし、vCenter ごとに次の情報を収集します。

- すべてのデータセンターで構成されている DVS と DPG のリスト。
- すべてのデータセンターのすべてのホストで構成されている PG のリスト。
- 構成ファイルで指定されたすべての DPG または PG について、構成された VLAN と直接接続されたネイバー スイッチをそのインターフェイス情報と共に検索します。
- 構成ファイルで指定されている <DVS, DPG> または <Host, PG> はそれぞれ、DCNM で関連付けられたネットワークマッピングを取得します。

モジュールはすべての情報をマージし、DCNM API を呼び出して、前の手順のいずれかでネイバーとして検出されたすべてのスイッチのネットワークをプロビジョニングまたは修正します。

ネットワークまたはファブリックのプロビジョニングは、DCNM トップダウン プロビジョニングを使用し、次の手順で構成されます。

1. ネイバーとして検出された 1 つ以上のスイッチの関連インターフェースにネットワーク構成をアタッチします。このアタッチメントは、ワークロード自動化モジュールによって行われます。
2. 構成がアタッチされた後、スイッチにプッシュされた正確な CLI を確認できます。
3. 確認後、構成をスイッチに展開できます。この展開は、構成ファイルの設定に基づいてスクリプトで実行するか（デフォルトは **False**）、DCNM を介して実行できます。この手順の後、構成がスイッチに表示されます。

詳細については、https://pypi.org/project/vmm-workload-auto/ を参照してください。

VMM ワークロード自動化の構成ファイル

VMM ワークロードの自動化には、次の構成ファイルが使用されます。

- グローバル YML ファイル（conf.yml）：このファイルには、DCNM および vCenter のグローバル構成とアクセスまたは認証情報が含まれています。また、各 DCNM の CSV ファイルの場所は、このファイルで指定されます。詳細については、VMM ワークロード自動化の構成ファイル （416 ページ）を参照してください。
- CSV ファイル（sample.csv）：このファイルは、vCenter の <DVS, DVS-PG> または <Host, PG> DCNM を DCNM のネットワーク名にマッピングします。DCNM ごとに個別の CSV ファイルがあります。詳細については、vCenter および DCNM のネットワークのマッピング用 CSV ファイル （417 ページ）を参照してください。

DCNM および vCenter のマッピング用構成ファイル

構成ファイル（conf.yml）は、DCNM の IP アドレス、ユーザー名、およびパスワードを指定します。DCNM ごとに、IP アドレス、ユーザー名、パスワードなどの vCenter 情報のリストも指定されます。この conf.yml ファイルでは、複数の DCNM を指定できます。すべての DCNM インスタンスには、関連付けられた CSV ファイルがあります。マルチ DCNM の場合は、スクリプトが DCNM で実行されず、構成ファイルで指定されたすべての DCNM および vCenter に接続できるサーバーで実行される場合にのみ適用されます。

構成ファイルで指定する情報の階層は以下のとおりです。

```
Global config parameters
DCNM1
      DCNM1 config parameters including location of the CSV file
 vCenter1
  vCenter1 config parameters
  …
 vCenter2
              vCenter2 config parameters
  ….
DCNM2
       ….
  …
```

この構成ファイルの場所は、VMM ワークロード自動化スクリプトのインストール方法によって異なります。詳細については、VMM ワークロード自動化スクリプトのインストールを参照してください。このファイルには、サンプルエントリが含まれています。使用環境に合わせて変更してください。

構成ファイルには次のエントリがあります。

LogFile：ワークロード自動化モジュールがエラーとデバッグ情報を記録するために使用する絶対パスを含むログファイルの名前を指定します。ディレクトリにログファイルを作成するための書き込み権限があることを確認してください。たとえば、/tmp/workloadauto.log です。

ListenPort：ワークロード自動化モジュールが REST API をリッスンするために使用するポート（9590 など）を指定します。このポートが他のアプリケーションによって使用されていないことを確認してください。**sudo netstat -tulpn** コマンドを実行して同じことを確認できます。

AutoDeploy：ネットワークを接続した後、スクリプトがスイッチに構成を自動的に展開するかどうかを指定します。デフォルトでは、構成を確認して DCNM に展開できるように **False** に設定されています。

NwkMgr：DCNM 情報を含むトップレベル セクションを指定します。複数の DCNM インスタンスの場合は、適切な値でフィールドを繰り返します。例については、複数の DCNM を処理する conf_multiple_dcnm.yml ファイルを参照してください。

Ip：DCNM の IP アドレスを指定します（例：172.28.10.156）。

User：DCNM へのログインに使用するユーザー名を指定します（例：admin）。

Password：DCNM のパスワードを指定します。

CsvFile：この DCNM の CSV ファイルの場所の絶対パスを指定します。
（例：/etc/vmm_workload_auto/sample.csv）

ServerCntrlr：サーバー コントローラ、つまり vCenter/vSphere の情報を指定します。この DCNM に該当する複数の vCenter については、このセクションが繰り返されます。例については、DCNM の下に複数の vCenter が含まれている conf_multiple_vcenter.yml ファイルを参照してください。

Ip：vCenter の IP アドレスを指定します。

タイプ：サーバー コントローラのタイプを指定します。デフォルトは vCenter です。

ユーザー：vCenter へのログインに使用するユーザー名を指しますたとえば、administrator@vsphere.local とします。

パスワード：vCenter のパスワードを指します。

次の例は、conf.yml ファイルの内容を示しています。

```
LogFile: /tmp/workloadauto.log
ListenPort: 9590
AutoDeploy: false
NwkMgr:
- Ip: 172.28.10.151
  User: admin
  Password: C1sco_123
  CsvFile: /etc/sample.csv
  ServerCntrlr:
    - Ip: 172.28.10.194
      Type: vCenter
      User: administrator@vsphere.local
      Password: Cisc0!23
```

vCenter および DCNM の ネットワークのマッピング用 CSV ファイル

CSV ファイルには、vCenter のネットワーク オブジェクトから DCNM で作成されたネットワークへのマッピングが含まれています。このファイルには、次のエントリが CSV 形式で含まれています。つまり、コンマ区切りのエントリです。CSV ファイルを作成する理由は、vSphere

の PG（または DPG）と DCNM のネットワーク名との間のマッピングを指定するためです。1 対 1 のマッピングです。ただし、PG または DPG は単独では識別できない（一意ではない）ため、マッピングするには追加の DVS 名またはホスト名が必要です。

CSV ファイルは、次のフィールドを含みます。

vCenter：vCenter の IP アドレスを指定します

Dvs：DVS の名前を指定します。

Dvs_pg：DVS の DVS PG（DPG）を指定します。

ホスト（Host）：ホスト/サーバー（IP アドレス）を指定します。

Host_pg：ホストのポート グループを指定します。

ファブリック（Fabric）：DCNM のファブリックを指定します。

ネットワーク（Network）：DCNM ですでに作成されているネットワークの名前を指定します。

ネットワーク オブジェクトは、次のいずれかの一意のペアによって識別されます。<DVS, DVS_PG> または <Host, Host_PG>

次の例を考えて見ましょう。

vCenter Params					**DCNM Params**	
vCenter	**DVS**	**DVPortGroup/ネットワーク**	**ESXi ホスト**	**ポート グループ/ネットワーク**	**Fabric Name（ファブリック名）**	**ネットワーク名（Network Name）**
172.28.12.123	DVS1	DPG1			Fab1	ネットワーク 10
172.28.12.123	DVS1	DPG1			Fab2	ネットワーク 30
172.28.12.123			172.28.12.11	PG10	Fab1	ネットワーク 20
172.28.12.123			172.28.12.12	PG20	Fab1	ネットワーク 20

このテーブルには、vCenter 172.28.12.123 のマッピングがあります。次の 4 つのエントリがあります。

- 最初のエントリは、DVS1 の DPG1 について、DCNM のネットワークがファブリック「Fab1」の「Network10」であることを指定します。DVS のホストが複数のファブリックのスイッチに接続できる場合があります。各ファブリックのネットワーク名は異なる場合があるため、ファブリック名も必要です。表の例では、2番目のエントリにそのようなケースの 1 つを示しています。
- 2番目のエントリは同じものを指定します。<DVS1, DPG1>ペアは、ファブリック「Fab2」のネットワーク 30 にマッピングされています。
- 3 番目のエントリは、ホスト 172.28.12.11 の PG10 の場合、DCNM のネットワークがファブリック「Fab1」の「Network20」であることを指定します。

- 4 番目のエントリは、ホスト 172.28.12.11 の PG20 の場合、DCNM のネットワークがファブリック「Fab1」の「Network20」であることを指定します。

前の表に見られるように、ネットワーク オブジェクトは、次のいずれかの一意のペアによって識別されます。<DVS, DVS_PG> または <Host, Host PG> DVS、DVS_PG に指定された値がある場合、<Host, Host_PG> の値はブランクです。つまり、<DVS, DVS_PG> と <Host, Host_PG> は相互に排他的な値です。

上記の表を CSV 形式で指定すると、CSV ファイルでは以下のように表示されます。

```
172.28.12.123,DVS1,DPG1,,,Fab1,Network10
172.28.12.123,DVS1,DPG1,,,Fab2,Network30
172.28.12.123,,,172.28.12.11,PG10,Fab1,Network20
172.28.12.123,,,172.28.12.12,PG20,Fab1,Network20
```

より多くの例を考えてみましょう：

- **172.28.10.184,DSwitchPad,DSPad-PG2,,,DEF,MyNetwork_30000**

  CSV ファイルのこの行では、vCenter の IP アドレスを 172.28.10.184 として指定し、<DVS, DVS PG> 値はそれぞれ DSwitchPad、DSPad-PG2 です。DVS、DVS-PG の値が指定されているため、この例に示すように、Host、Host-PG の値はブランクです。ファブリック名は DEF で、DCNM のネットワークは MyNetwork_30000 です。

- **172.28.10.184,,,172.28.11.33,Pad_Workload_Auto_Nwk,DEF,MyNetwork_60000**

  この例では、<DVS, DVS-PG> はブランクで、値 <Host, Host_PG> は、それぞれ 172.28.11.33 および Pad_Workload_Auto_Nwk として指定されます。DCNM のファブリックは DEF で、DCNM のネットワーク名は MyNetwork_60000 です。

CSV ファイルの例は次のとおりです。

```
vCenter,Dvs,Dvs_pg,Host,Host_pg,Fabric,Network
172.28.10.184,DSwitchNew,DPGNew,,,DEF,MyNetwork_30000
172.28.10.184,DSwitchNew,DPGNew,,,ABC,MyNetwork_30000
172.28.10.184,,,172.28.11.33,Pad_Workload_Auto_Nwk,DEF,MyNetwork_60000
```

VMM ワークロード自動化モジュールのインストールと開始

PIP インストールまたはインストール スクリプトを使用して、VMM ワークロード自動化モジュールをインストールできます。

PIP インストールの使用

始める前に

このインストール方法は、**pip インストール** に精通しており、プロキシの設定方法や Python パッケージで競合が発生した場合の処理方法を知っているユーザー向けです。

手順

ステップ 1 このモジュールを仮想環境で実行するか、物理サーバーで実行するかを決定します。サーバーでこれを実行する場合は、pip インストールを実行するための書き込み権限があることを確認してください。

ステップ 2 http_proxy、https_proxy、および no_proxy を適切に設定します。

次に例を示します。

```
export http_proxy=http://proxy.esl.cisco.com:80
export https_proxy=https://proxy.esl.cisco.com:80
export no_proxy=127.0.0.1,172.28.10.0/24
```

この例では、no_proxy で指定されている 172.28.10.0 が DCNM の管理サブネットです。

ステップ 3 モジュールを https://pypi.org/ からダウンロードしてインストールします。

```
pip3 install vmm-workload-auto
```

同様に、次のコマンドを使用してモジュールをアンインストールできます。**pip3 uninstall vmm-workload-auto**

ステップ 4 デフォルトでは、**pip** コマンドでオプションを指定して上書きしない限り、インストールは次のディレクトリで行われます。

パッケージは以下にインストールされます。`/usr/local/lib/python3.7/site-packages/vmm_workload_auto-0.1.1.dist-info`

構成ファイルは `/usr/local/lib/python3.7/site-packages/etc/vmm_workload_auto` にインストールされます。

ソース コードは `/usr/local/lib/python3.7/site-packages/workload_auto` にあります。

ステップ 5 `/usr/local/lib/python3.7/site-packages/etc/vmm_workload_auto` の構成ファイルを編集します。

詳細については、DCNM と vCenter をマッピングするための構成ファイルを参照してください。

conf.yml ファイルに指定されている CSV ファイルのパスが正しいことを確認してください。

ステップ 6 VMM ワークロード自動化モジュールを開始します。

Python モジュールのエントリ ポイントは、`/usr/local/bin/vmm_workload_auto` です。

次のように実行できます。

```
/usr/local/bin/vmm_workload_auto
```

または

```
vmm_workload_auto
```

/usr/local/bin/ がすでに **$PATH** にある場合。

コマンドライン オプションとして構成ファイルを指定します。

```
/usr/local/bin/vmm_workload_auto
--config=/usr/local/lib/python3.7/site-packages/etc/vmm_workload_auto/conf.yml
```

インストール スクリプトの使用

インストール スクリプトの使用は、**pip install** を使用したくないユーザのための代替方法です。インストール スクリプトはインストールを実行し、Python モジュールを開始します。

手順

ステップ 1 https://pypi.org/project/vmm-workload-auto/ に移動し、 latest.tar.gz ファイルをダウンロードします。

ステップ 2 解凍します。次に例を示します。

```
tar -xvf vmm_workload_auto-0.1.0.tar.gz
```

ステップ 3 config/conf.yml と config/sample.csv を作業環境に合わせて変更します。

ステップ 4 セットアップ スクリプトを「source setup.sh」として実行します。

ステップ 5 インストール スクリプトは、最初に conf.yaml および .csv ファイルを編集するようにユーザに促します。次に、スクリプトは、ユーザにプロキシおよびその他の詳細を求めるプロンプトを表示します。すべてが完了すると、スクリプトは Python パッケージをインストールし、モジュールを自動的に開始します。

ステップ 6 スクリプトのインストールについては、https://pypi.org/project/vmm-workload-auto/ にある README ファイルのインストール セクションを参照してください。

インストール後

ワークロード自動化モジュールを実行したら、DCNM ネットワーク ウィンドウに移動して、ネットワーク接続が完了しているかどうかを確認します。構成ファイル（conf.yml）で **AutoDeploy** が **false** に設定されている場合は、構成を確認して展開します。

REST API を使用する追加の機能

ワークロード自動化モジュールは、次の REST API も提供します。

（注） REST API は、VMM ワークロード自動化モジュールの実行後に別のウィンドウで実行されます。REST API を実行する前に、自動化モジュールが実行されていることを確認してください。

- 更新：CSVファイルが変更された場合、更新操作を実行する必要があります。この操作により、ファイルが再読み取りされ、必要に応じて新しい構成が適用されます。更新APIは次のとおりです。

```
curl -XPOST http://127.0.0.1:{port}/workload_auto/refresh
```

- 再同期：DVS-PG、PG、VLAN、またはネイバースイッチに変更がある場合は、再同期操作が必要です。変更が見つかった場合、それに応じて構成が再適用されます。再同期APIは次のとおりです。

```
curl -XPOST http://127.0.0.1:{port}/workload_auto/resync
```

- クリーン：モジュールを使用して以前に実行されたネットワーク プロビジョニングをクリーンアップするには、クリーンアップ操作が必要です。クリーン API は次のとおりです。

```
curl -XPOST http://127.0.0.1:{port}/workload_auto/clean
```

vCenter のイベント

DCNM リリース 11.4(1) では、リアルタイム イベント処理はモジュールを使用して実行されません。さまざまな関連イベントと、このモジュールに対するその重要性は次のとおりです。

更新

更新 API により、モジュールは CSV ファイルを再度読み取り、ネットワーク構成を 1 つ以上の関連スイッチに適用できます。更新の操作は、次のイベントに対して実行する必要があります。

- PG の追加：この PG の DCNM で関連付けられたネットワークを指定するエントリを CSV ファイルに作成します。エントリが追加されたら、更新 REST API を呼び出します。
- DPG の追加：この DPG の DCNM で関連付けられたネットワークを指定するエントリを CSV ファイルに作成します。エントリが追加されたら、更新 REST API を呼び出します。

Resync

再同期 API により、モジュールはネットワーク オブジェクトとその関連プロパティを再度検出できます。この再同期操作の結果として、ネットワーク構成が新規または変更されたスイッチまたはインターフェイスに適用されます。次のイベントに対して再同期操作を実行します。

- DVS へのホストの追加
- DPG または PG の VLAN を変更します。
- トポロジの変更：以下のいずれかの情報が変更された場合は、Resync REST API を発行してトポロジを再検出し、REST API を適用します。
  - ネイバースイッチの変更：これは、接続されているリーフスイッチが新しいスイッチに置き換えられた場合、または別のスイッチに再配線された場合に発生する可能性があります。

- インターフェイスの変更：これは、スイッチ内の別のインターフェイスへの再配線が原因で発生する可能性があります。
- ホスト pNIC の変更。
- 追加の接続を追加：これは、次の場合に発生する可能性があります。
  - ホストの通常のインターフェイスは、ホストからスイッチに追加のインターフェイスを接続することにより、ポートチャネルになります。
  - vPC ペアを形成する別のスイッチに接続するホストの追加インターフェイス。

操作の必要はありません

次のイベントの場合、アクションを実行する必要はありません。

- スタンドアロン ホストを追加します。
- vSwitch を追加します。
- DVS を追加します。
- DVS を削除します。

マッピングの変更

CSV でのマッピング変更のさまざまなシナリオは次のとおりです。

- 新しいマッピングが追加された場合は、CSV ファイルにマッピングを追加した後に更新 API を実行します。
- vCenter ネットワークから DCNM ネットワークへのマッピングを変更する必要がある場合は、クリーンな REST API を実行し、CSV ファイルのマッピングを変更して、更新 REST API を実行します。
- 既存のマッピングを削除する必要がある場合は、クリーンな REST API を実行し、CSV ファイル内のマッピングを削除して、更新 API を実行します。

その他のイベント

カテゴリに属さないその他のイベントと操作は次のとおりです。

- DVS から削除されたホスト：ホストが DVS から削除された場合、関連するリーフスイッチと接続されたインターフェイスのネットワーク構成を削除する必要があります。これは、この DVS のすべての DPG に対して行う必要があります。DCNM に移動し、適切なネットワークを接続解除します。
- DPG または PG の削除：この DPG または PG に関連付けられているスペック ファイルで指定されたすべてのネットワーク マッピングについて、関連するスイッチおよびインターフェイスのネットワーク構成を削除します。DCNM に移動し、適切なネットワークを接続解除します。

- ポート ダウンまたはスイッチ ダウン：ポートまたはスイッチが永続的にオフラインになる場合は、構成をアウトオブバンドで削除する必要があります。スイッチにホストから到達できないが、まだDCNMによって管理されている場合は、DCNMに移動し、適切なネットワークを接続解除します。

管理

管理メニューには、次のサブメニューがあります。

リソース

Cisco DCNM では、リソースを管理できます。次の表で、このページに表示されるフィールドを説明します。

フィールド	説明
スコープタイプ	リソースが管理される範囲レベルを指定します。範囲タイプは、**[ファブリック（Fabric）]**、**[デバイス（Device）]**、**[DeviceInterface]**、**[DevicePair]**、**[ファブリック（Fabric）]**、および **[リンク（Link）]** です。
範囲	リソース使用範囲を指定します。有効な値は、スイッチのシリアル番号またはファブリック名です。シリアル番号を持つリソースは一意であり、スイッチのシリアル番号でのみ使用できます。
リソースの割り当て	リソースをデバイス、デバイス インターフェイス、またはファブリックで管理するかどうかを指定します。有効な値は、ID タイプ、サブネット、または IP アドレスです。
割り当て先	リソースが割り当てられるエンティティ名を指定します。
[リソース タイプ（Resource Type)]	リソース タイプを指定します。有効な値は、**TOP_DOWN_VRF_LAN**、**TOP_DOWN_NETWORK_VLAN**、**LOOPBACK_ID**、**VPC_ID** などです。
割り当てされましたか？	リソースが割り当てられているかどうかを指定します。リソースが特定のエンティティに永続的に割り当てられている場合、値は **True** に設定されます。リソースがエンティティに予約されており、永続的に割り当てられていない場合、値は **False** に設定されます。
割り当て日時	リソース割り当ての日時を指定します。

リソースの割り当て

Cisco DCNM Web UI からリソースを割り当てるには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 リソースを割り当てるファブリックで、**[ファブリックの編集（Edit Fabric）]** アイコンをクリックします。

[ファブリックの編集（Edit Fabric）] ダイアログボックスが表示されます。

（注） または、ファブリック トポロジ ウィンドウから **[ファブリックの編集（Edit Fabric）]** ダイアログボックスに移動できます。**[アクション（Actions）]** ペインで **[ファブリック設定（Fabric Settings）]** をクリックします。

ステップ 3 **[リソース（Resources）]** タブを選択します。

ステップ 4 **[手動アンダーレイ IP アドレスの割り当て（Manual Underlay IP Address Allocation）]** チェックボックスをオフにします。

このチェックボックスをオンにすると、**[リソース割り当て（Resource Allocation）]** ウィンドウを使用して、すべてのリソースに IP アドレスを手動で提供します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 **[制御（Control）] > [管理（Management）] > [リソース（Resources）]** を選択します。

[**リソースの割り当て（Resource Allocation**）] ウィンドウが表示されます。このウィンドウには、選択した範囲の下にあるすべてのリソースが一覧表示されます。

ステップ 7 **[リソースの割り当て（Allocate Resource）]** アイコンをクリックします。

[リソースの割り当て（Allocate Resource）] ダイアログボックスが表示されます。

ステップ 8 ドロップダウン リストからプール タイプ、プール名、およびスコープ タイプを適宜選択します。

プール タイプのオプションは、**[ID]**、**[IP]**、および **[SUBNET]** です。選択したプールタイプに基づいて、**[プール名（Pool Name）]** ドロップダウン リストの値が変更されます。

ステップ 9 **[シリアル番号（Serial Number）]** ドロップダウンリストから、シリアル番号を選択します。

このフィールドは、ファブリック範囲タイプを除くすべての範囲タイプに表示されます。

ステップ 10 **[エンティティ名（Entity Name）]** フィールドにエンティティ名を入力します。

組み込みヘルプには、さまざまなスコープ タイプの名前の例が示されています。

ステップ 11 **[リソース（Resource）]** フィールドに ID、IP アドレス、またはサブネットを入力します。ステップ *3* で選択したプール タイプに従う必要があります。

ステップ 12 **[保存（Save）]** をクリックしてリソースを割り当てます。

リソース割り当ての例

例 1：IP を loopback 0 と loopback 1 に割り当てる

```
#loopback 0 and 1
    L0_1: #BL-3
        pool_type: IP
        pool_name: LOOPBACK0_IP_POOL
        scope_type: Device Interface
        serial_number: BL-3(FDO2045073G)
        entity_name: FDO2045073G~loopback0
        resource : 10.7.0.1


    # L1_1: #BL-3
    #     pool_type: IP
    #     pool_name: LOOPBACK1_IP_POOL
    #     scope_type: Device Interface
    #     serial_number: BL-3(FDO2045073G)
    #     entity_name: FDO2045073G~loopback1
    #     resource : 10.8.0.3
```

例 2：サブネットの割り当て

```
#Link subnet
    Link0_1:
        pool_type: SUBNET
        pool_name: SUBNET
        scope_type: Link
        serial_number: F3-LEAF(FDO21440AS4)
        entity_name: FDO21440AS4~Ethernet1/1~FDO21510YPL~Ethernet1/3
        resource : 10.9.0.0/30
```

例 3：IP をインターフェイスに割り当てる

```
    #Interface IP
    INT1_1: #BL-3
        pool_type: IP
        pool_name: 10.9.0.8/30
        scope_type: Device Interface
        serial_number: BL-3(FDO2045073G)
        entity_name: FDO2045073G~Ethernet1/17
        resource : 10.9.0.9
```

例 4：エニーキャスト IP の割り当て

```
    #ANY CAST IP
    ANYCAST_IP:
        pool_type: IP
        pool_name: ANYCAST_RP_IP_POOL
        scope_type: Fabric
        entity_name: ANYCAST_RP
        resource : 10.253.253.1
```

例 5：ループバック ID の割り当て

```
#LOOPBACK ID
LID0_1: #BL-3
    pool_type: ID
    pool_name: LOOPBACK_ID
    scope_type: Device
    serial_number: BL-3(FDO2045073G)
    entity_name: loopback0
    resource : 0
```

リソースの解放

Cisco DCNM Web UI からリソースを解放するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [リソース（Resources）]** を選択します。

[**リソースの割り当て（Resource Allocation**）] ウィンドウが表示されます。このウィンドウには、選択した範囲の下にあるすべてのリソースが一覧表示されます。

ステップ 2 削除するリソースを選択します。

（注） 複数のリソースを選択すると、複数のリソースを同時に削除できます。

ステップ 3 **[リソースの解放（Release Resource(s)]** アイコンをクリックします。

確認用のダイアログボックスが表示されます。

ステップ 4 **[はい（Yes）]** をクリックして、リソースを解放します。

VMware サーバの追加、編集、再検出、削除

この項の内容は、次のとおりです。

VirtualCenter サーバを追加

Cisco DCNM から仮想センター サーバを追加できます。

Procedure

ステップ 1 **[制御（Control）] > [管理（Management）] > [仮想マシン マネージャ（Virtual Machine Manager）]** を選択します。

Cisco DCNM-LAN によって管理されている VMware Server（存在する場合）のリストがテーブルに表示されます。

ステップ 2 [追加（Add）] をクリックします。

[vCenter の追加（Add VCenter）] ウィンドウが表示されます。

ステップ 3 この VMware **[VirtualCenter サーバ（Virtual Center Server）]** の IP アドレスを入力します。

ステップ 4 この VMware Server の**[ユーザー名（User Name）]**と**[パスワード（Password）]**を入力します。

ステップ 5 **[Add（追加）]** をクリックすると、このVMware Server の管理が開始されます。

VMware サーバを削除

Cisco DCNM から VMware サーバを削除できます。

Procedure

ステップ 1 **[コントロール > マネジメント > 仮想マシン マネージャ（Control > Management > Virtual Machine Manager）]** を選択。

ステップ 2 VMware サーバのデータ収集を中止するために、削除したい VMware サーバの隣にあるチェック ボックスを選択して、**[削除（Delete）]** をクリックします。

VMware サーバの編集

Cisco DCNM Web クライアントから VMware サーバを編集できます。

Procedure

ステップ 1 **[コントロール > 管理 > 仮想マシン マネージャ（Control > Management > Virtual Machine Manager）]** を選択します。

ステップ 2 編集する VMware サーバーの隣のチェックボックスをオンにして、**[Edit（編集）]** VirtualCenter アイコンをクリックします。

[vCenter の編集（Edit VCenter）] ダイアログ ボックスが表示されます。

ステップ 3 **[ユーザー名（User Name）]** と **[パスワード（Password）]** を入力します。

ステップ 4 管理対象または管理対象外のステータスを選択します。

ステップ 5 [適用（Apply）] をクリックし、変更を保存します。

VMware サーバの再検出

Cisco DCNM から VMware サーバを再検出できます。

Procedure

ステップ 1 **[制御（Control）] > [管理（Management）] > [仮想マシン マネージャ（Virtual Machine Manager）]** を選択します。

ステップ 2 再検出する VMware の隣のチェックボックスを選択します。

ステップ 3 **[再検出（Rediscover）]** をクリックします。

「再検出操作が完了するまでお待ちください」という警告が記載されたダイアログボックスが表示されます。

ステップ 4 ダイアログ ボックスで [OK] をクリックします。

コンテナ オーケストレータ

Cisco DCNM Web UI で、**[制御（Control] > [管理（Management）] > [コンテナ オーケストレータ（Container Orchestrator）]** を選択します。コンテナ タイプを追加、削除、編集、および再検出できます。

Cisco DCNM を使用してコンテナ可視化を使用する方法を示すビデオも視聴できます。「ビデオ：Cisco DCNM でのコンテナ可視化の使用」を参照してください。

次の表に、[Container Orchestrator] ウィンドウのフィールドと説明が記載されています。

フィールド	説明
コンテナタイプ	オーケストレータのタイプを表示します。
クラスタIP	Kubernetes クラスタの IP アドレスを表示します。
クラスタ名	クラスタの名前を指定します。
管理対象（Managed）	クラスタが管理されていることを指定します。

フィールド	説明
Status	クラスタのステータスを表示します。 • **[証明書の期限切れ（Cert expired）]** は、証明書の期限が切れていることを意味します。正しい証明書を再度追加する必要があります。 • **[到達不能（Not reachable）]** は、DCNM が Kubernetes クラスタに到達できないことを意味します。 • **[Ok]** は、クラスタが正しく機能していることを意味します。 • **[検出中（Discovering）]** は、クラスタが検出中であることを意味します。 • **[空白（Blank）]**は、クラスタが管理されていないことを意味します。 （注） 注：ステータスが空の場合、クラスタが管理されていないことを意味します。
User	Kubernetes クラスタのロールを指定します
最終更新時刻	前回の変更からの経過時間を表示します。

次の表は、[コンテナ オーケストレータ（Container Orchestrator）] ウィンドウで実行できるアクションについて説明しています。

フィールド	説明
追加（Add）	**[追加（Add）]**アイコンをクリックして、新しいクラスタをコンテナ オーケストレーションに追加します。コンテナは 4 つまで追加できます。
削除	Kubernetes クラスタを選択し、**[削除（Delete）]** アイコンをクリックして削除します。
編集	Kubernetes クラスタを選択し、**[編集（Edit）]** アイコンをクリックしてクラスタの詳細を編集します。
再検出	Kubernetes クラスタを選択し、**[再検出（Rediscover）]** をクリックしてクラスタを更新します。

コンテナ オーケストレータでは、次のアクションを実行できます。

コンテナ オーケストレータの追加

Cisco DCNM Web UI からコンテナ オーケストレータを追加するには、次の手順を実行します。

始める前に

VM ベースの Kubernetes クラスタを追加するには、コンテナ オーケストレータの可視化機能を有効にする前に、Cisco DCNM で VMM が正常に構成されていることを確認してください。VM ベースの Kubernetes クラスタが実行されている VM をホストする VMM に vCenter を追加する必要があります。

ホスト名がすべてのクラスタ ノードで一意であることを確認してください。

ベアメタル ベースのクラスタには VMM は必要ありません。ベアメタル ベースのクラスタの場合、次を実行します。

- **[Web UI] > [管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバーのプロパティ（Server Properties）]** の順に選択してサーバー プロパティを編集し、DCNM で LLDP を有効にします。**[cdp.discover-lldp]** フィールドに **[true]** を入力して、LLDP を有効にします。
- ファブリックのすべてのリーフスイッチで LLDP 機能が有効化されていることを確認してください。
- Kubernetes クラスタで、すべてのベアメタルノードで LLDP および SNMP サービスが有効になっていることを確認します。
- Cisco UCS が Intel NIC を使用している場合、FW-LLDP が原因で LLDP ネイバーシップの確立に失敗します。

  回避策：Intel® イーサネットコントローラ（800 および 700 シリーズなど）に基づく選択されたデバイスでは、ファームウェアで実行される LLDP エージェントを無効にします。LLDP を無効にするには、次のコマンドを使用します。

  echo 'lldp stop' > /sys/kernel/debug/i40e/<bus.dev.fn>/command

  特定のインターフェイスの *bus.dev.fn* を見つけるには、次のコマンドを実行し、インターフェイスに関連付けられた ID を選択します。ID は、以下のサンプル出力で強調表示されています。

```
[ucs1-lnx1]# dmesg | grep enp6s0
[ 12.609679] IPv6: ADDRCONF(NETDEV_UP): enp6s0: link is not ready
[ 12.612287] enic 0000:06:00.0 enp6s0: Link UP
[ 12.612646] IPv6: ADDRCONF(NETDEV_UP): enp6s0: link is not ready
[ 12.612665] IPv6: ADDRCONF(NETDEV_CHANGE): enp6s0: link becomes ready
[ucs1-lnx1]#
```

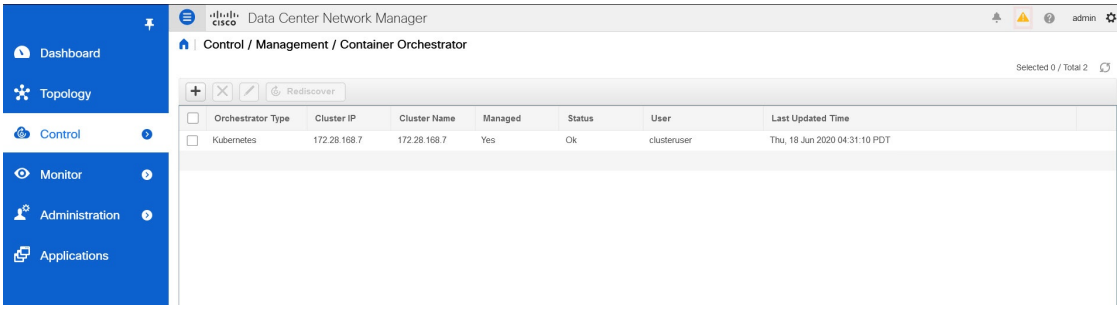
（注） LLDP 機能は、ベアメタルクラスタノードが接続されているファブリックスイッチで有効になっています。また、ボーダーゲートウェイスイッチに接続することもできます。

クラスタが検出された後にKubernetesクラスタが接続されているファブリックが検出された場合、トポロジを正しく表示するためにクラスタを再検出する必要があります。

LLDP の設定後にベアメタルベースの Kubernetes クラスタが検出された場合、トポロジを正しく表示するためにベアメタルクラスタを再検出する必要があります。

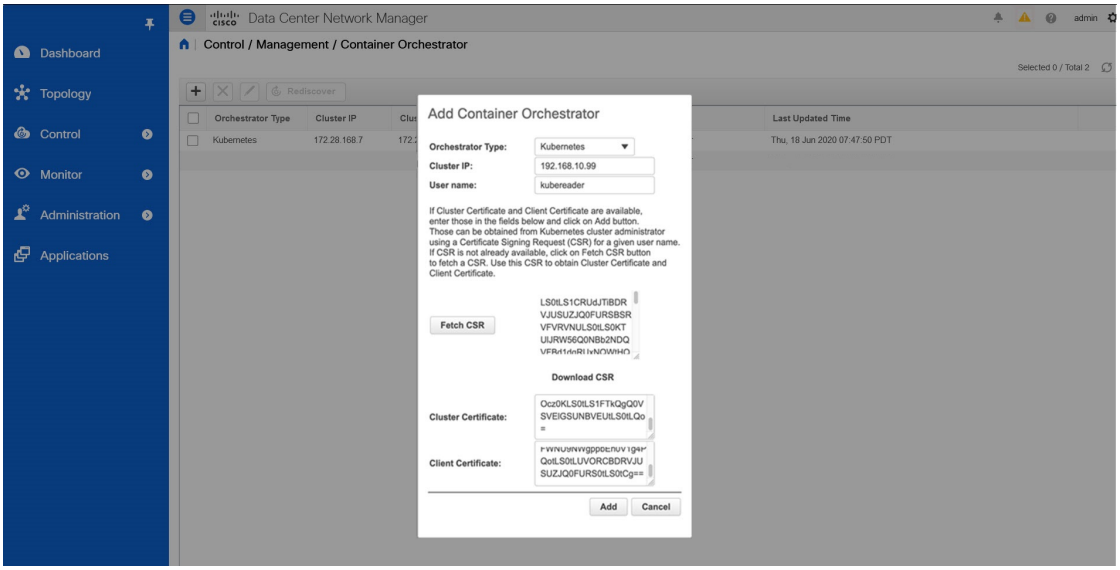
手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [コンテナ オーケストレータ（Container Orchestrator）]** の順に選択します。



ステップ 2 [追加（Add）] をクリックします。

[コンテナ オーケストレータの追加（Add Container Orchestrator）] が表示されます。



ステップ 3 **[オーケストレータ（Orchestrator）]** ドロップダウンリストから、**[Kubernetes]** を選択します。

ステップ 4 **[クラスター IP（Cluster IP）** フィールドに、Kubernetes クラスタのマスター ノードの IP アドレスを入力します。

ステップ 5 **[ユーザー名（User Name）]** フィールドに、Kubernetes に接続する API クライアントのユーザー名を入力します。

ステップ 6 **[CSR の取得（Fetch CSR）]** をクリックして、Kubernetes ビジュアライザ アプリケーションから証明書署名要求（CSR）を取得します。

（注） このオプションは、有効なクラスタ IP アドレスとユーザー名を入力するまで無効になっています。

SSL 証明書を取得していない場合にのみ、**[CSR の取得（Fetch CSR）]** を使用してください。有効な証明書がすでにある場合は、CSR を取得する必要はありません。

[CSR のダウンロード（Download CSR）] をクリックします。証明書の詳細は、ディレクトリ内の **<username>.csr** に保存されます。CSR の内容をファイル **[kubereader.csr]** に貼り付けます。ここで、*kubereader* は、Kubernetes に接続する API クライアントのユーザー名です。

CSR ファイル名は命名規則 <<*username*> > に従う必要があります。

（注） 証明書は Kubernetes クラスタで生成されるため、証明書を生成するには Kubernetes 管理者権限が必要です。

証明書 **[genk8clientcert.sh]** を生成するスクリプトは、DCNM サーバの `./root/packaged-files/scripts/genk8sclientcert.sh` の場所にあります。

ステップ 7 Kubernetes クラスタコントローラノードにログインします。

（注） 証明書を生成するには、管理者権限が必要です。

ステップ 8 `[genk8clientcert.sh]` と `[kubereader.csr]` を DCNM サーバーの場所から Kubernetes クラスタ コントローラ ノードにコピーします。

（注） 「vnc カットアンドペースト」操作を実行して、すべての文字が正しくコピーされるようにします。

ステップ 9 **genk8sclientcert.sh** スクリプトを使用して、ユーザー名の CSR を生成します。

```
(k8s-root)# ./genk8sclientcert.sh kubereader 10.x.x.x
```

値は次のとおりです。

- `kubereader` は、Kubernetes に接続する API クライアントのユーザー名です。（手順 ステップ 5 （432 ページ） で定義）。
- `10.x.x.x` は DCNM サーバーの IP アドレスです。

証明書が正常に生成されると、次のメッセージが表示されます。

```
------------------------------------------------------------
The K8s CA certificate is copied into k8s_cluster_ca.crt file.
    This to be copied into "Cluster CA" field.
The client certificate is copied into kubereader_10.x.x.x.crt file.
    This to be copied into "Client Certificate" field.
------------------------------------------------------------
```

同じ場所に 2 つの新しい証明書が生成されます。

- k8s_cluster_ca.crt
- *username_dcnm-IP*.crt

例：kubereader_10.x.x.x.crt （ここで、kubereader はユーザー名で、10.x.x.x は DCNM IP アドレスです）

ステップ 10 **cat** コマンドを使用して、これら 2 つのファイルから証明書を抽出します。

```
dcnm(root)# cat kubereader_10.x.x.x.crt
dcnm(root)# cat k8s_cluster_ca.crt
```

Cisco DCNM に Kubernetes クラスタを追加するユーザに、これらの 2 つの証明書を提供します。

ステップ 11 kubereader_10.x.x.x.crt の内容を **[クライアント証明書（Client Certificate）]** フィールドにコピーします。

（注） 「vnc カットアンドペースト」操作を実行して、すべての文字が正しくコピーされるようにします。

ステップ 12 k8s_cluster_ca.crt の内容を **[クラスタ証明書（Cluster Certificate）]** フィールドにコピーします。

（注） 「vnc カットアンドペースト」操作を実行して、すべての文字が正しくコピーされるようにします。

ステップ 13 **[追加（Add）]** をクリックして、コンテナ オーケストレータを追加します。

[キャンセル（Cancel）] をクリックして、コンテナ オーケストレータの追加を破棄します。

コンテナ オーケストレータの削除

Cisco DCNM Web UI からコンテナ オーケストレータを削除するには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [コンテナ オーケストレータ（Container Orchestrator）]** の順に選択します。

ステップ 2 削除する **[コンテナ オーケストレータ（Container Orchestrator）]** を選択します。

一度に複数のクラスタを選択できます。

[削除（Delete）] をクリックします。

（注） クラスタを削除すると、すべてのデータが削除されます。クラスタは、トポロジビューからも削除されます。

ステップ 3 確認メッセージで **[はい（Yes）]** をクリックして、コンテナ オーケストレータを削除します。

[いいえ（No）] をクリックして破棄します。

コンテナ オーケストレータの編集

Cisco DCNM Web UI からコンテナを編集するには、以下の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [コンテナ オーケストレータ（Container Orchestrator）]** の順に選択します。

ステップ 2 変更する**[コンテナ オーケストレータ（Container Orchestrator）]** を選択します。[編集（Edit）] をクリックします。

[コンテナ オーケストレータの編集（Edit Container Orchestrator）] ウィンドウが表示されます。

ステップ 3 値を適切に変更します。

クラスタとクライアントの証明書を更新できます。Kubernetes クラスタの管理ステータスを更新することもできます。管理ステータスの更新を選択した場合、証明書は必要ありません。

ステップ 4 [適用（Apply）] をクリックし、変更を保存します。

[キャンセル（Cancel）] をクリックして破棄します。

Kubernetes クラスタの再検出

Cisco DCNM Web UI からKubernetes クラスタを再検出するには、以下の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [コンテナ オーケストレータ（Container Orchestrator）]** の順に選択します。

ステップ 2 再検出する**[コンテナ オーケストレータ（Container Orchestrator）]** を選択します。

一度に複数のクラスタを選択できます。

[再検出（Rediscover）] をクリックします。

このアクションでは、コンテナ情報を更新するのに時間がかかる場合があります。

OpenStack ビジュアライザ

Cisco DCNM Web UI で、**[制御（Control）] > [管理（Management）] > [OpenStack ビジュアライザ（OpenStack Visualizer）]** を選択します。OpenStack クラスタを追加、削除、編集、および再検出できます。これはプレビュー機能であることに注意してください。

[トポロジ（Topology）] で OpenStack クラスタを表示する方法については、OpenStack ワークロードの可視性 （53 ページ） を参照してください。

次のテーブルでは、**[OpenStack ビジュアライザ（OpenStack Visualizer）]** ウィンドウのフィールドと説明を説明します。

フィールド	説明
クラスタ タイプ	クラスタのタイプを指定します。
クラスタIP	クラスタのコントローラのIPアドレスを指定します。
管理対象（Managed）	クラスタが管理対象か非管理対象かを指定します。
Status	クラスタのステータスを指定します。
ユーザ名	クラスタのユーザー名を指定します。
プロジェクト名	プロジェクト名を指定します。
[リージョン（Region）]	リージョンを指定します。
ユーザ ドメイン	ユーザー ドメインを指定します。
プロジェクト ドメイン	プロジェクト ドメインを指定します。
最終更新時刻	最後に更新された日時を示します。

次の表は、**[OpenStack ビジュアライザ（OpenStack Visualizer）]** ウィンドウで実行できるアクションについて説明しています。

フィールド	説明
追加（Add）	**[追加（Add）]** アイコンをクリックして、新しいOpenStackクラスタをコンテナオーケストレーションに追加します。
削除	OpenStack クラスタを選択し、**[削除（Delete）]** アイコンをクリックして削除します。
編集	OpenStack クラスタを選択し、**[編集（Edit）]** アイコンをクリックしてクラスタの詳細を編集します。
再検出	OpenStack クラスタを選択し、**[再検出（Rediscover）]** をクリックしてクラスタを更新します。

OpenStack クラスタの追加

このタスクは、OpenStack クラスタを追加する方法を示しています。

始める前に

- **[管理 (Administration)] > [DCNM サーバー (DCNM Server)] > [サーバー ステータス (Server Status)]** を選択します。**[cdp.discover-lldp]** プロパティが **[True]** に設定されていることを確認し、**[変更の適用（Apply Changes）]** をクリックします。

  OpenStack クラスタで、すべてのベアメタルノードで LLDP サービスが有効になっていることを確認します。LLDP機能は、ベアメタルクラスタノードが接続されているファブリックスイッチで有効になっています。また、ボーダーゲートウェイスイッチに接続することもできます。

- 再同期タイマーは、**[openstackviz.resync.timer]** プロパティを使用して変更できます。デフォルト値は 60 分です。この値を 60 分未満に設定できないことに注意してください。再同期機能は、OpenStack プラグインを再起動し、すべての OpenStack クラスタを再検出します。

- Intel® イーサネットコントローラに基づく、選択されたデバイス（例：800 および 700 シリーズ）については、ファームウェアで実行される Link Layer Discovery Protocol（LLDP）エージェントを無効にします。同じことを行うには、次のコマンドを使用します。

  ```
  # echo 'lldp stop' > /sys/kernel/debug/i40e/bus.dev.fn/command
  ```

  特定のインターフェイスの *bus.dev.fn* を見つけるには、次のコマンドを実行し、インターフェイスに関連付けられた ID を選択します。ID は、以下の出力で強調表示されています。

  ```
  # dmesg | grep eth0
  [ 8.269557] enic 0000:6a:00.0 eno5: renamed from eth0
  [ 8.436639] i40e 0000:18:00.0 eth0: NIC Link is Up, 40 Gbps Full Duplex, Flow Control:
   None
  [ 10.968240] i40e 0000:18:00.0 ens1f0: renamed from eth0
  [ 11.498491] ixgbe 0000:01:00.1 eno2: renamed from eth0
  ```

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [OpenStack ビジュアライザ（OpenStack Visualizer）]** の順に移動します。

ステップ 2 **[追加（Add）]** アイコンをクリックして、OpenStack クラスタを追加します。

- クラスタ情報（VM やホスト情報など）を取得するには、少なくとも読み取りアクセス許可が必要です。

- DCNM リリース 11.5(1) では、単一のプロジェクトとリージョンでのみクラスタを追加できます。

ステップ 3 **[OpenStack クラスタの追加（Add OpenStack Cluster）]** ウィンドウで、次の詳細情報を指定します。

- **[オーケストレータ タイプ（Orchestrator Type）]**：オーケストレータのタイプを指定します。デフォルトでは、このドロップダウンリストから OpenStack が選択されています。
- **[サーバー IP（Server IP）]**：OpenStack クラスタのコントローラの IP アドレスを指定します。
- **[ポート（Port）]**：ポート番号を指定します。
- **[バージョン（Version）]**：バージョンを指定します。
- **[ユーザー名（Username）]** および **[パスワード（Password）]**：OpenStack クラスタのユーザー名とパスワードを指定します。
- **[プロジェクト（Project）]**：プロジェクト名を指定します。
- **[リージョン（Region）]**：リージョンを指定します。デフォルトのリージョンは **[RegionOne]** です。
- **[ユーザ ドメイン（User Domain）]**：ユーザ ドメインを指定します。デフォルトのユーザ ドメインは **[default]** です。
- **[プロジェクト ドメイン（Project Domain）]**：プロジェクト ドメインを指定します。デフォルトのプロジェクト ドメインは **[default]** です。
- **[AMQP エンドポイント（AMQP Endpoint）]**：AMQP エンドポイントのアドレス詳細を含む multi-valued フィールドを、コロン（：）区切りで指定します。値はフォーマット：**[username:password:port]** で指定される必要があります。フィールドは次の情報で指定されます。
  - **[username]**：AMQP エンドポイントのユーザー名を指定します。
  - **[password]**：AMQP エンドポイントのパスワードを指定します。
  - **[port]**：AMQP エンドポイントのポート番号を指定します。

  このフィールドのデフォルト値は **[guest:guest:5672]** です。

ステップ 4 [追加（Add）] をクリックします。

検出後、ステータスは **[検出中（Discovering）]** から **[OK]** に変わります。OpenStack クラスタから受信した情報は適切に編成され、メインの **[トポロジ（Topology）]** ウィンドウに表示されます。**[表示（Show）]** ペインに **[OpenStack]** というラベルの付いた追加のメニュー項目が表示されます。

OpenStack クラスタの編集

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [OpenStack ビジュアライザ（OpenStack Visualizer）]** の順に移動します。

ステップ 2 変更する OpenStack クラスタを選択します。[編集（Edit）] をクリックします。

[OpenStack クラスタの編集（Edit OpenStack Cluster）] ウィンドウでは、次のフィールドを編集できます。

- **[ユーザー名（Username）]** および **[パスワード（Password）]**：OpenStack クラスタのユーザー名とパスワードを指定します。
- **[管理対象（Managed）]**：**[管理対象外（unmanaged）]** を選択して、OpenStack クラスタを管理対象外にできます。
- **[AMQP エンドポイント（AMQP Endpoint）**：AMQP エンドポイントのアドレス詳細を含む multi-valued フィールドを、コロン（：）区切りで指定します。値はフォーマット：**[username:password:port]** で指定される必要があります。フィールドは次の情報で指定されます。
  - **[username]**：AMQP エンドポイントのユーザー名を指定します。
  - **[password]**：AMQP エンドポイントのパスワードを指定します。
  - **[port]**：AMQP エンドポイントのポート番号を指定します。

  このフィールドのデフォルト値は **[guest:guest:5672]** です。

ステップ 3 [適用（Apply）] をクリックし、変更を保存します。

[キャンセル（Cancel）] をクリックして破棄します。

OpenStack クラスタの削除

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [OpenStack ビジュアライザ（OpenStack Visualizer）]** の順に移動します。

ステップ 2 変更する OpenStack クラスタを削除します。[削除（Delete）] をクリックします。

インベントリ ビューからクラスタを削除すると、OpenStack プラグインはクラスタからの変更通知のフェッチと受信を停止し、削除されたクラスタとの接続をシャットダウンして、すべてのソフトウェア リソースを解放します。

ステップ 3 確認メッセージで **[はい（Yes）]** をクリックして、OpenStack クラスタを削除します。

[いいえ（No）] をクリックして破棄します。

OpenStack クラスタの再検出

手順

ステップ 1 **[制御（Control）] > [管理（Management）] > [OpenStack ビジュアライザ（OpenStack Visualizer）]** の順に移動します。

ステップ 2 再検出する特定のクラスタまたはすべてのクラスタを選択します。**[再検出（Rediscover）]** をクリックします。

[テンプレート ライブラリ（Template Library）]

Cisco DCNM Web クライアントを使用して、異なる Cisco Nexus および Cisco MDS プラットフォームで設定されているテンプレートを追加、編集、または削除できます。Cisco DCNM Web クライアントのホームページから、**[制御（Control）] > [テンプレート ライブラリ（Template Library）] > [テンプレート（Templates）]** を選択します。Cisco DCNM Web クライアントで構成されているテンプレートごとに、次のパラメータが表示されます。テンプレートは JavaScript をサポートします。テンプレートの JavaScript 関数を使用して、テンプレートの構文で算術演算と文字列操作を実行できます。

次の表で、このページに表示されるフィールドを説明します。

Table 4: テンプレート操作

フィールド	説明
Add Template	新しいテンプレートを追加できます。
テンプレートの変更/表示	テンプレート定義を表示し、必要に応じて変更できます。
テンプレートに名前を付けて保存	選択したテンプレートを別の名前で保存できます。必要に応じて、テンプレートを編集できます。
テンプレートの削除（Delete Template）	テンプレートの削除を許可します
テンプレートのインポート	ローカル ディレクトリからテンプレートを 1 つずつインポートできます。

フィールド	説明
テンプレートのエクスポート	ローカル ディレクトリの場所にテンプレート設定をエクスポートできます。
テンプレート Zip ファイルのインポート	.zip 形式でバンドルされた複数のテンプレートを含む .zip ファイルをインポートできます ZIP ファイル内のすべてのテンプレートが抽出され、個々のテンプレートとしてテーブルにリストされます。

Note サーバーの再起動後にテンプレートのロード中に問題が発生した場合は、**[テンプレート Zip ファイルのインポート]** の横に通知が表示されます。通知をクリックして、**[テンプレートの読み込み中の問題]** ウィンドウにエラーを表示します。エラーのあるテンプレートは、**[テンプレート（Templates）]** ウィンドウに表示されません。このようなテンプレートをインポートするには、エラーを修正してインポートします。

Cisco DCNM Release 11.4(1) から **network-operator** ロールでのみテンプレートのみを表示できます。このロールでテンプレートを作成、編集、または保存することはできません。ただし、**network-stager** ロールを使用してテンプレートを作成または編集できます。

Table 5: テンプレートのプロパティ

フィールド	説明
テンプレート名（Template Name）	構成されたテンプレートの名前が表示されます。
[テンプレートの説明（Template Description）]	テンプレートの構成中に提供される説明を表示します。
タグ（Tags）	テンプレートに割り当てられたタグを表示し、タグに基づいてテンプレートをフィルタリングするのに役立ちます。
サポートされるプラットフォーム	テンプレートと互換性のあるサポートされている Cisco Nexus プラットフォームを表示します。テンプレートでサポートされているプラットフォームのチェック ボックスをオンにします。 **Note** 複数のプラットフォームを選択できます。
テンプレートのタイプ	テンプレートのタイプが表示されます。
テンプレート サブ タイプ	テンプレートに関連付けられたサブタイプを指定します。
テンプレートのコンテンツ タイプ	Jython または Template CLI のどちらであるかを指定します。

Table 6: 詳細テンプレートのプロパティ

フィールド	説明
実装	実装する抽象テンプレートを表示します。
依存関係	スイッチの特定の機能を指定します。
作成日：	テンプレートを公開するかどうかを指定します。
インポート	インポートのベース テンプレートを指定します。

さらに、メニュー バーから **[制御] > [テンプレート ライブラリ] > [テンプレート]** を選択し、次のこともできます。

- **[フィルタを表示]** をクリックして、ヘッダーに基づいたテンプレートをフィルタ処理します。
- **[印刷]** をクリックして、テンプレートのリストを印刷します。
- **[Excel にエクスポート]** をクリックして、テンプレートのリストを Microsoft Excel スプレッドシートにエクスポートします。

この項の内容は、次のとおりです。

テンプレート構造

構成テンプレートの内容は、主に4つの部分で構成されます。テンプレートのコンテンツの編集については、**[テンプレート コンテンツ（Template Content）]** の横にある **[ヘルプ（Help）]** アイコンをクリックします。

この項の内容は、次のとおりです。

テンプレートの形式

ここでは、テンプレートの基本情報について説明します。次の表に、使用可能なフィールドの詳細を示します。

プロパティ名	説明	有効な値	任意かどうか
名前（name）	テンプレートの名前	テキスト	いいえ
説明	テンプレートに関する簡単な説明	テキスト（Text）	はい

プロパティ名	説明	有効な値	任意かどうか
userDefined	ユーザがテンプレートを作成したかどうかを示します。ユーザが作成した場合、値は「true」です。	「true」または「false」	はい
supportedPlatforms	この設定テンプレートをサポートするデバイスプラットフォームのリスト。すべてのプラットフォームをサポートするには、[All]を指定します。	N1K、N3K、N3500、N4K、N5K、N5500、N5600、N6K、N7K、N9K、MDS、VDC、N9K-9000v、IOS-XE、IOS-XR、その他、すべてのNexusスイッチのリストがカンマで区切られています。	いいえ

プロパティ名	説明	有効な値	任意かどうか
templateType	使用するテンプレートのタイプを指定します。	• CLI • POAP **Note** POAP オプションは、Cisco DCNM ローカル エリア ネットワーク（LAN）ファブリックの展開には適用されません。 • ポリシー • SHOW • プロファイル • ファブリック • [抽象（ABSTRACT）] • レポート	はい

プロパティ名	説明	有効な値	任意かどうか
templateSubType	テンプレートに関連付けられたサブタイプを指定します。		

プロパティ名	説明	有効な値	任意かどうか
		• CLI • なし • POAP • なし • VXLAN • FABRICPATH • VLAN • PMN **Note** POAP オプションは、Cisco DCNM ローカル エリア ネットワーク（LAN）ファブリックの展開には適用されません。 • ポリシー • VLAN • interface-vlan • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORTCHANNEL • INTERFACE_FC • INTERFACE_MGMT	

プロパティ名	説明	有効な値	任意かどうか
		• INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VPC • INTERFACE_PORTCHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • SHOW • VLAN • interface-vlan • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORTCHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VPC • INTERFACE_PORTCHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • プロファイル • VXLAN	

プロパティ名	説明	有効な値	任意かどうか
		• ファブリック • 該当なし • [抽象（ABSTRACT）] • VLAN • interface-vlan • INTERFACE_VPC • INTERFACE_ETHERNET • INTERFACE_BD • INTERFACE_PORT_CHANNEL • INTERFACE_FC • INTERFACE_MGMT • INTERFACE_LOOPBACK • INTERFACE_NVE • INTERFACE_VFC • INTERFACE_SAN_PORT_CHANNEL • DEVICE • FEX • INTRA_FABRIC_LINK • INTER_FABRIC_LINK • INTERFACE • レポート • アップグレード • GENERIC	

プロパティ名	説明	有効な値	任意かどうか
contentType			はい

プロパティ名	説明	有効な値	任意かどうか
		• CLI • TEMPLATE_CLI • POAP • TEMPLATE_CLI **Note** POAP オプションは、Cisco DCNM ローカル エリア ネットワーク（LAN）ファブリックの展開には適用されません。 • ポリシー • TEMPLATE_CLI • PYTHON • SHOW • TEMPLATE_CLI • プロファイル • TEMPLATE_CLI • PYTHON • ファブリック • PYTHON • [抽象（ABSTRACT）]	

プロパティ名	説明	有効な値	任意かどうか
		• TEMPLATE_CLI • PYTHON • レポート • PYTHON	
実装（Implement）	抽象テンプレートを実装するために使用されます。	テキスト（Text）	はい
依存関係	スイッチの特定の機能を選択するために使用されます。	テキスト（Text）	はい
公開	テンプレートを読み取り専用としてマークし、変更を回避するために使用されます。	「true」または「false」	はい

テンプレート変数

このセクションには、テンプレートに使用されるパラメータの宣言された変数、データ型、デフォルト値、および有効な値の条件が含まれます。これらの宣言された変数は、動的コマンド生成プロセス中にテンプレート コンテンツ セクションの値の置換に使用されます。また、これらの変数は、意思決定およびテンプレート コンテンツ セクションの反復ブロックで使用されます。変数には事前定義されたデータ型があります。変数に関する説明を追加することもできます。次の表に、使用可能なデータ型の構文と使用方法を示します。

変数の型	有効値	反復可能?
boolean	true|false	いいえ
enum	`Example: running-config, startup-config`	いいえ
浮動	浮動小数点形式	いいえ
floatRange	`Example: 10.1,50.01`	はい
整数型（Integer）	任意の数値	いいえ

変数の型	有効値	反復可能?
integerRange	「-」で区切られた連続する番号 「,」で区切られた個別の番号 Example: 1-10,15,18,20	はい
インターフェイス	形式：<if type><slot>[/<sub slot>]/<port> Example: eth1/1, fa10/1/2 etc.	いいえ
interfaceRange	Example: eth10/1/20-25, eth11/1-5	はい
IPアドレス	IPv4 または IPv6 アドレス	いいえ
ipAddressList	IPv4、IPv6、または両方のタイプのアドレスの組み合わせのリストを作成できます。 Example 1: 172.22.31.97, 172.22.31.99, 172.22.31.105, 172.22.31.109 Example 2: 2001:0db8:85a3:0000:0000:8a2e:0370:7334, 2001:0db8:85a3:0000:0000:8a2e:0370:7335, 2001:0db8:85a3:1230:0000:8a2f:0370:7334 Example 3: 172.22.31.97, 172.22.31.99, 2001:0db8:85a3:0000:0000:8a2e:0370:7334, 172.22.31.254	はい
ipAddressWithoutPrefix	Example: 192.168.1.1 または Example: 1:2:3:4:5:6:7:8	いいえ
ipV4Address	IPv4 アドレス	いいえ
ipV4AddressWithSubnet	Example: 192.168.1.1/24	いいえ
ipV6Address	[IPv6 アドレス（IPv6 address）]	いいえ

変数の型	有効値	反復可能?
ipV6AddressWithPrefix	Example: 1:2:3:4:5:6:7:8 22	いいえ
ipV6AddressWithSubnet	IPv6アドレスとサブネット	いいえ
ISISNetAddress	Example: 49.0001.00a0.c96b.c490.00	いいえ
long	Example: 100	いいえ
MAC アドレス	14 または 17 文字長の MAC アドレス形式	いいえ

string	変数の説明などに使用される自由テキスト
	
	Example:
	string scheduledTime
	{
	regularExpr=^([01]\d|2[0-3]):([0-5]\d)$;
	}
		いいえ

string[]	Example: {a,b,c,str1,str2}	はい

構造体	単一の変数にバンドルされているパラメータのセット。
	
	struct <structure name declaration > {
	<parameter type> <parameter 1>;
	<parameter type> <parameter 2>;
	…..
	} [<structure_inst1>] [,
	<structure_inst2>] [,
	<structure_array_inst3 []>];
	
	struct interface_detail {
	string inf_name;
	string inf_description;
	ipAddress inf_host;
	enum duplex {
	validValues = auto, full, half;
	};
	}myInterface,
	myInterfaceArray[];
		いいえ
		Note 構造体変数が配列として宣言されている場合、変数は反復型です。

wwn （Cisco DCNM Web Client でのみ使用可能）	Example: 20:01:00:08:02:11:05:03	いいえ

可変メタ プロパティ

テンプレート変数セクションで定義されている各変数には、一連のメタ プロパティがあります。メタ プロパティは、主に変数に定義されている検証ルールです。

次の表に、使用可能な変数タイプに適用されるさまざまなメタ プロパティを示します。

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
boolean	ブール値。 Example: true	はい											
enum			はい										
浮動	符号付き実数。 Example: 75.56, -8.5	はい	はい	はい	はい	はい							
floatRange	符号付き実数の範囲 Example: 50.5 - 54.75	はい	はい	はい	はい	はい							
integer	符号付き実数 Example: 50, -75	はい	はい		はい	はい							

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
integerRange	符号付き実数の範囲 Example: 50-65	はい	はい		はい	はい							
インターフェイス	インターフェイス/ポートを指定します Example: Ethernet 5/10	はい	はい				はい	はい	はい	はい			
interfaceRange		はい	はい				はい	はい	はい	はい			
IPアドレス	IPv4 または IPv6 形式の IP アドレス	はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
pAdtsLi		はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
	IPv4、IPv6、または両方のタイプのアドレスの組み合わせのリストを作成できます。 Example 1: 172.23.97, 172.23.99, 172.23.105, 172.23.109 Example 2: [redacted], [redacted], [redacted] Example 3: 172.23.97, 172.23.99, [redacted], 172.23.254 **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
ipv4_ipv6_addr	IPv4 または IPv6 アドレス（プレフィックス/サブネットは不要）。												
ipv4_addr	IPv4 アドレス	はい											
ipv4_prefix	IPv4 アドレスとサブネット	はい											
ipv6_addr	[IPv6 アドレス（IPv6 addr）]	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 shell line { [illegible] }	はい									はい	はい	はい

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
string[]	カンマ（,）で区切られた文字列リテラル Example: {string1, string2}	はい											

変数の型	説明	可変メタ プロパティ											
		デフォルト値	有効な値	10 進数の長さ	最低	最大	最小スロット	最大スロット	最小ポート	最大ポート	最小長	最大長	正規表現
構造体	単一の変数にバンドルされているパラメータのセット。 struct <structure name> declaration > { <parameter type> <parameter 1>; <parameter type> <parameter 2>; ….. } [structvar1] [, structvar2] [, structvar3] []>];												
wwn	WWN アドレス												

例：メタ プロパティの使用

```
##template variables

integer VLAN_ID {
min = 100;
max= 200;
};

string USER_NAME {
defaultValue = admin123;
minLength = 5;
};

struct interface_a{
 string inf_name;
 string inf_description;
 ipAddress inf_host;
 enum duplex {
  validValues = auto, full, half;
 };
}myInterface;

##
```

可変注釈

注釈を使用して変数をマーキングする変数プロパティを設定できます。

Note 可変注釈は、POAP でのみ使用できます。ただし、注釈はテンプレートタイプ「CLI」には影響しません。

テンプレート変数セクションでは、次の注釈を使用できます。

注釈キー	有効な値	説明
AutoPopulate	テキスト（Text）	あるフィールドから別のフィールドに値をコピーします。
DataDepend	テキスト	
説明	[テキスト（Text）]	ウィンドウに表示されるフィールドの説明
DisplayName	テキスト（Text） **Note** スペースがある場合は、テキストを引用符で囲みます。	ウィンドウに表示されるフィールドの表示名

注釈キー	有効な値	説明
列挙体	Text1、Text2、Text3 など	選択するテキストまたは数値をリストします
IsAlphaNumeric	「true」または「false」	文字列には、英数字を使用します。
IsAsn	「true」または「false」	
IsDestinationDevice	「true」または「false」	
IsDestinationFabric	「true」または「false」	
IsDestinationInterface	「true」または「false」	
IsDestinationSwitchName	「true」または「false」	
IsDeviceID	「true」または「false」	
IsDot1qId	「true」または「false」	
IsFEXID	「true」または「false」	
IsGateway	「true」または「false」	IPアドレスがゲートウェイかどうかを検証します。
IsInternal	「true」または「false」	フィールドを内部にし、ウィンドウに表示しません。 **Note** この注釈は、ipAddress変数にのみ使用します。
IsManagementIP	「true」または「false」 **Note** この注釈は、変数「ipAddress」に対してのみマークする必要があります。	

注釈キー	有効な値	説明
is_mandatory	「true」または「false」	値をフィールドに強制的に渡す必要があるかどうかを検証します
IsMTU	「true」または「false」	
IsMultiCastGroupAddress	「true」または「false」	
IsMultiLineString	「true」または「false」	文字列フィールドを複数行の文字列テキスト領域に変換します
IsMultiplicity	「true」または「false」	
IsPassword	「true」または「false」	
IsPositive	「true」または「false」	値が正であるかどうかを確認します。
IsReplicationMode	「true」または「false」	
IsShow	「true」または「false」	ウィンドウのフィールドを表示または非表示にします
IsSiteId	「true」または「false」	
IsSourceDevice	「true」または「false」	
IsSourceFabric	「true」または「false」	
IsSourceInterface	「true」または「false」	
IsSourceSwitchName	「true」または「false」	
IsSwitchName	「true」または「false」	
IsRMID	「true」または「false」	
IsVPCDomainID	「true」または「false」	
IsVPCID	「true」または「false」	
IsVPCPeerLinkPort	「true」または「false」	
IsVPCPeerLinkPortChannel	「true」または「false」	

注釈キー	有効な値	説明
IsVPCPortChannel	「true」または「false」	
[パスワード（Password）]	テキスト（Text）	パスワードフィールドを検証します
PeerOneFEXID	「true」または「false」	
PeerTwoFEXID	「true」または「false」	
PeerOnePCID	「true」または「false」	
PeerTwoPCID	「true」または「false」	
PrimaryAssociation		
ReadOnly	「true」または「false」	フィールドを読み取り専用にします
ReadOnlyOnEdit	「true」または「false」	
SecondaryAssociation	テキスト（Text）	
セクション		
UsePool	「true」または「false」	
UseDNSReverseLookup		
ユーザ名	テキスト（Text）	ウィンドウにユーザ名フィールドを表示します。
警告	テキスト（Text）	Description 注釈をオーバーライドするテキストを提供します。

例：**AutoPopulate** 注釈

```
##template variables
string BGP_AS;
 @(AutoPopulate="BGP_AS")
  string SITE_ID;
##
```

例：**DisplayName**注釈

```
##template variables
@(DisplayName="Host Name", Description = "Description of the host")
String hostname;
@(DisplayName="Host Address", Description = " test description" IsManagementIP=true)
```

```
ipAddress hostAddress;
##
```

例：IsMandatory注釈

```
##template variables
@(IsMandatory="ipv6!=null")
ipV4Address ipv4;
@(IsMandatory="ipv4!=null")
ipV6Address ipv6;
##
```

例：IsMultiLineString注釈

```
##template variables
@(IsMultiLineString=true)
string EXTRA_CONF_SPINE;
##
```

IsShow注釈

```
##template variables
boolean isVlan;
@(IsShow="isVlan==true")
integer vlanNo;
##

##template variables
boolean enableScheduledBackup;
@(IsShow="enableScheduledBackup==true",Description="Server time")
string scheduledTime;
##
The condition "enableScheduledBackup==true" evaluates to true/false

##template variables
@(Enum="Manual,Back2BackOnly,ToExternalOnly,Both")
string VRF_LITE_AUTOCONFIG;
@(IsShow="VRF_LITE_AUTOCONFIG!=Manual",  Description="Target Mask")
integer DCI_SUBNET_TARGET_MASK
##
The condition "VRF_LITE_AUTOCONFIG!=Manual" matches string comparison to evaluate to
true or false
```

例：警告の注釈

```
##template variables
@(Warning="This is a warning msg")
  string SITE_ID;
##
```

テンプレートの内容

この項には、テンプレートで使用する構成コマンドと、すべてのパラメータが含まれています。これらのコマンドには、テンプレート変数セクションで宣言された変数を含めることができます。コマンド生成プロセス中に、変数の値がテンプレートの内容に適切に置き換えられます。

Note 使用するコマンドは、任意のデバイスのグローバル構成コマンド モードで入力するのと同じように指定する必要があります。コマンドを指定するときは、コマンド モードを考慮する必要があります。

テンプレートの内容は、変数の使用によって決まります。

- スカラ変数：反復に使用できない値の範囲または配列を取得しません（変数タイプテーブルでは、iterate-ableが「No」としてマークされています）。スカラ変数はテンプレートの内容内で定義する必要があります。

```
Syntax: $$<variable name>$$
Example: $$USER_NAME$$
```

- 反復変数：ブロックの反復に使用されます。これらのループ変数は、次に示すように、繰り返しブロック内でアクセスする必要があります。

```
Syntax:@<loop variable>
Example:
foreach val in $$INTEGER_RANGE_VALUE$$ {
@val
}
```

- スカラー構造体変数：構造体メンバー変数は、テンプレートの内容からアクセスできます。

```
Syntax: $$<structure instance name>.<member variable name>$$
Example: $$myInterface.inf_name$$
```

- 配列構造変数：構造体のメンバー変数は、テンプレートの内容からアクセスできます。

```
Syntax: $$<structure instance name>.<member variable name>$$
Example: $$myInterface.inf_name$$
```

テンプレート変数に加えて、次のステートメントを使用して、条件付きコマンドと反復コマンドの生成を使用できます。

- if-else if-else ステートメント：その中の変数に割り当てられた値に基づいて、設定コマンドのセットの包含/除外を論理的に決定します。

```
Syntax: if(<operand 1>  <logical operator>  <operand 2>){
command1 ..
command2..
..
}
else  if (<operand 3> <logical operator> <operand 4> )
{
Command3 ..
Command4..
..
}
else
{
```

```
Command5 ..
Command6..
..
}
Example: if-else if-else statement
if($$USER_NAME$$ == 'admin'){
Interface2/10
no shut
}
else {
Interface2/10
shut
}
```

- foreach ステートメント：コマンドのブロックを反復するために使用されます。反復は、割り当てられたループ変数値に基づいて実行されます。

```
Syntax:
foreach <loop index variable> in $$<loop variable>$$ {
@<loop index variable> ..
}
Example: foreach Statement
foreach ports in $$MY_INF_RANGE$${
interface @ports
no shut
}
```

- オプションパラメータ：デフォルトでは、すべてのパラメータが必須です。パラメータをオプションにするには、パラメータに注釈を付ける必要があります。

変数セクションには、次のコマンドを含めることができます。

- **@(IsMandatory=false)**
- **Integer frequency;**

  テンプレートの内容の項では、「if」条件チェックを使用せずに、パラメータに値を割り当てることで、コマンドを除外または含めることができます。オプションのコマンドは、次のように構成できます。

- **probe icmp [frequency frequency-value] [timeout seconds] [retry-count retry-count-value]**

テンプレート コンテンツ エディタ

テンプレート コンテンツ エディタには、次の機能があります。

- 構文の強調表示: エディタは、Python スクリプトのさまざまなタイプのステートメント、キーワードなどの構文を強調表示します。
- オートコンプリート: 入力を開始すると、エディタはテンプレートのデータ型、注釈、またはメタプロパティを提案します。
- 行に移動: スクロールする代わりに、テンプレート コンテンツ エディタで正確な行に移動できます。Mac の場合は **Command-L**、Windows の場合は **Ctrl-L** を押し、ポップアップ ウィンドウに移動先の行番号を入力します。

エディタで行数より大きい値を入力すると、エディタ ウィンドウの最後の行に移動します。

- テンプレートの検索と置換: Mac の場合は **Command-F**、Windows の場合は **Ctrl-F** を押し、**検索対象**フィールドに検索語を入力し、検索ウィンドウで検索のタイプを選択します。エディタで次の検索を実行できます。
  - **RegExp 検索**：エディタで正規表現検索を実行できます。
  - **CaseSensitive 検索** ：エディタで大文字と小文字を区別した検索を実行できます。
  - **単語全体の検索 : 単語全体の検索を実行して、エディタで正確な単語を見つけることができます。**たとえば、"play" という単語の通常の検索では、"display" などの単語の一部である結果が返されますが、単語全体の検索では、"play" という単語に完全に一致する場合にのみ結果が返されます。
  - **選択範囲で検索** : 選択したコンテンツで検索を実行できます。検索を絞り込みたいコンテンツを選択し、検索語を入力します。

  置換オプションを使用するには、検索ウィンドウで + アイコンを選択します。**[置換後の文字列（Replace with）]** フィールドに置換する単語を入力します。**[置換]** を選択すると、選択した単語を 1 回だけ置き換えることができます。選択した単語の出現箇所をすべて置換するには、**[すべて]** を選択します。
- コードの折りたたみ: エディタでコード ブロックを展開またはグループ化するには、行番号の横にある矢印をクリックします。
- その他の機能: エディタは、コード、閉じ括弧を自動的にインデントし、対応する括弧を強調表示します。

テンプレート エディタの設定

[テンプレート エディタの設定（Template Editor Settings）] をクリックすると、テンプレート エディタの次の機能を編集できます。

- **[テーマ（Theme）]** : ドロップダウン リストからエディタに必要なテーマを選択します。
- **KeyBinding**：エディタをカスタマイズするには、**KeyBinding** ドロップダウン リストからエディタ モードを選択します。 **Vim** と **Ace** モードがサポートされています。デフォルトは **Ace** です。
- **[フォント サイズ（Font Size）]** : エディタに必要なフォント サイズを選択します。

高度な機能

次に、テンプレートの構成に使用できる高度な機能を示します。

- 割り当て操作

構成テンプレートは、テンプレートコンテンツセクション内の変数値の割り当てをサポートします。変数の宣言されたデータ型の値が検証されます。不一致がある場合、値は割り当てられません。

割り当て操作は、次のガイドラインに従って使用できます。

- 左側の演算子は、テンプレートパラメータまたはforループパラメータのいずれかである必要があります。
- 正しい値の演算子は、テンプレートパラメータ、ループパラメータ、引用符で囲まれたリテラル文字列値、または単純な文字列値のいずれかの値です。

ステートメントがこれらのガイドラインに従っていない場合、またはこの形式に適合しない場合は、割り当て操作とは見なされません。これは、他の通常の行と同様に、コマンド生成時に置き換えられます。

```
Example: Template with assignment operation
##template properties
name =vlan creation;
userDefined= true;
supportedPlatforms = All;
templateType = CLI;
published = false;
##
##template variables
integerRange vlan_range;
@(internal=true)
integer vlanName;
##
##template content
foreach vlanID in $$vlan_range$${
vlan @vlanID
$$vlanName$$=@vlanID
name myvlan$$vlanName$$
}
##
```

- Evaluate メソッド

設定テンプレートは、Java ランタイムが提供する Java スクリプト環境を使用して、算術演算（ADD、SUBTRACT など）、文字列操作などを実行します。

テンプレートリポジトリパスでJavaScriptファイルを見つけます。このファイルには、算術文字列関数の主要なセットが含まれています。カスタム JavaScript メソッドを追加することもできます。

これらのメソッドは、次の形式の設定テンプレート コンテンツ セクションから呼び出すことができます。

```
Example1:
$$somevar$$ = evalscript(add, "100", $$anothervar$$)
```

また、次のようなif条件の内部で *evalscript* を呼び出すことができます。

```
if($$range$$ > evalscript(sum, $$vlan_id$$,  -10)){
```

```
do something...
}
```

Java スクリプト ファイルのバックエンドにあるメソッドを呼び出すことができます。

- 動的な決定

  構成テンプレートは、特殊な内部変数LAST_CMD_RESPONSEを提供します。この変数には、コマンド実行中のデバイスからの最後のコマンド応答が格納されます。これは、デバイスの状態に基づいてコマンドを提供するための動的な決定を行うために、構成テンプレートのコンテンツで使用できます。

Note ifブロックの後には、空の場合もある新しい行でelseブロックを続ける必要があります。

VLAN がデバイス上に存在しない場合の VLAN の作成例。

```
Example: Create VLAN
##template content
show vlan id $$vlan_id$$
if($$LAST_CMD_RESPONSE$$ contains "not found"){
vlan $$vlan_id$$
}
else{
}
##
```

この特別な暗黙的変数は、「IF」ブロックでのみ使用できます。

- テンプレート参照

  すべての変数を定義した基本テンプレートを作成できます。この基本テンプレートは、複数のテンプレートにインポートできます。基本テンプレートの内容は、拡張テンプレートの適切な場所に置き換えられます。インポートしたテンプレートパラメータと内容は、拡張テンプレート内でアクセスできます。

```
Example: Template Referencing
Base template:
##template properties
 name =a vlan base;
 userDefined= true;
 supportedPlatforms = All;
 templateType = CLI;
 published = false;
 timestamp = 2015-07-14 16:07:52;
 imports = ;
##
##template variables
 integer vlan_id;
##
##template content
 vlan $$vlan_id$$
##

Derived Template:
##template properties
 name =a vlan extended;
 userDefined= true;
```

```
 supportedPlatforms = All;
 templateType = CLI;
 published = false;
 timestamp = 2015-07-14 16:07:52;
 imports = a vlan base,template2;
##
##template variables
 interface vlanInterface;
##
##template content
 <substitute a vlan base>
 interface $$vlanInterface$$
 <substitute a vlan base>
##
```

拡張テンプレートを起動すると、基本テンプレートのパラメータ入力も取得されます。また、置換された内容は、完全な CLI コマンドの生成に使用されます。

レポート テンプレート

Cisco DCNM 11.3(1) リリース以降、新しいテンプレート タイプ、REPORT が追加されました。このテンプレートには、[UPGRADE] と [GENERIC] の 2 つのサブタイプがあります。テンプレートの種類は python です。

アップグレード

UPGRADE テンプレートは、ISSU 前後のシナリオに使用されます。これらのテンプレートは、ISSU ウィザードに表示されます。

ISSU 前後の処理の詳細については、DCNM にパッケージ化されているデフォルトのアップグレード テンプレートを参照してください。デフォルトのアップグレード テンプレートは issu_vpc_check です。

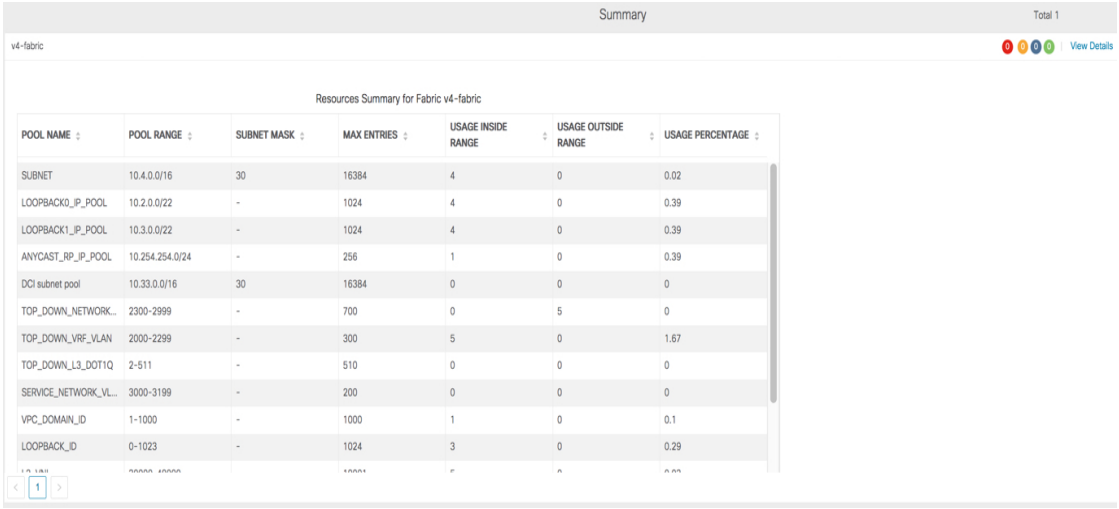
GENERIC

GENERIC テンプレートは、リソース、スイッチ インベントリ、SFP、NVE VNI カウンタに関する情報の収集など、一般的なレポート シナリオに使用されます。このテンプレートを使用して、トラブルシューティング レポートを生成することもできます。

リソース レポート

このレポートには、特定のファブリックのリソース使用状況に関する情報が表示されます。

[サマリ（Summary）]セクションには、すべてのリソース プールと現在の使用率が表示されます。より多くの列を表示するには、ウィンドウの下部にある水平スクロール バーを使用します。



POOL NAME：プールの名前を指定します。

POOL RANGE：プールの IP アドレス範囲を指定します。

SUBNET MASK：サブネット マスクを指定します。

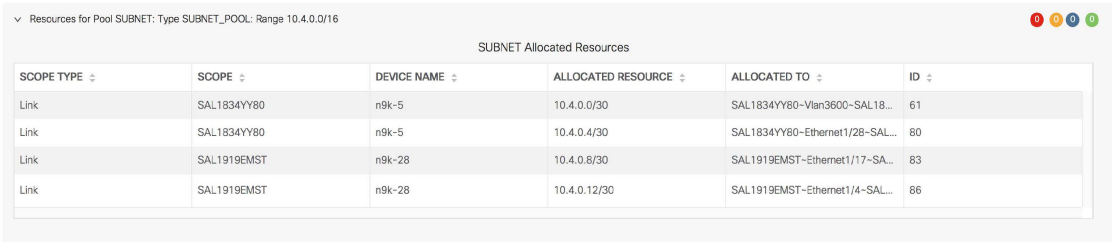
MAX ENTRIES：プールから割り当て可能な最大エントリ数を示します。

USAGE INSIDE RANGE：プール範囲内に割り当てられている現在のエントリ数を指定します。

USAGE OUTSIDE RANGE：プール範囲外に設定されている現在のエントリ数を指定します。

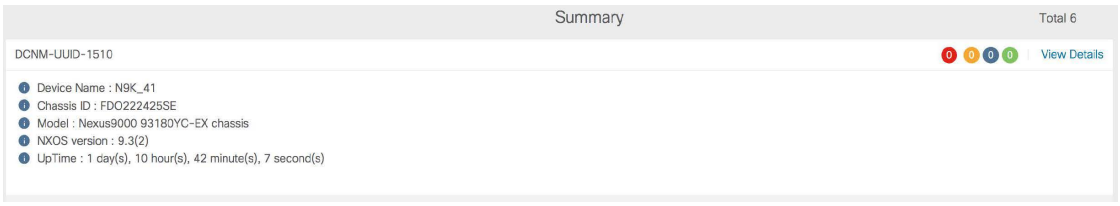
USAGE PERCENTAGE：これは、(範囲内での使用数/最大エントリ数) *100 という式を使用して計算されます。

[詳細の表示（View Details）]をクリックして、各リソースプールに割り当てられた、または設定されたリソースのビューを表示します。たとえば、SUBNET の詳細セクションには、サブネット内で割り当てられたリソースに関する情報が含まれます。

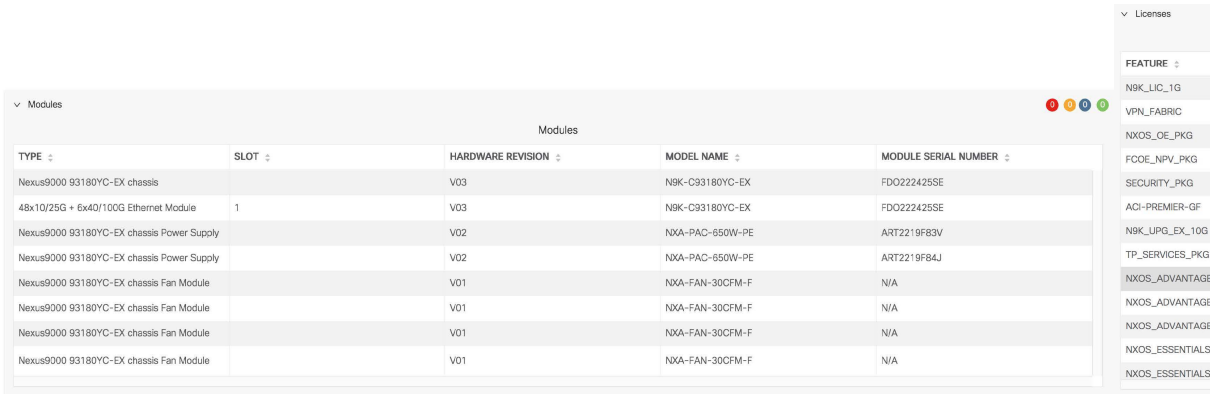


スイッチ インベントリ レポート

このレポートは、スイッチ インベントリに関する概要を提供します。

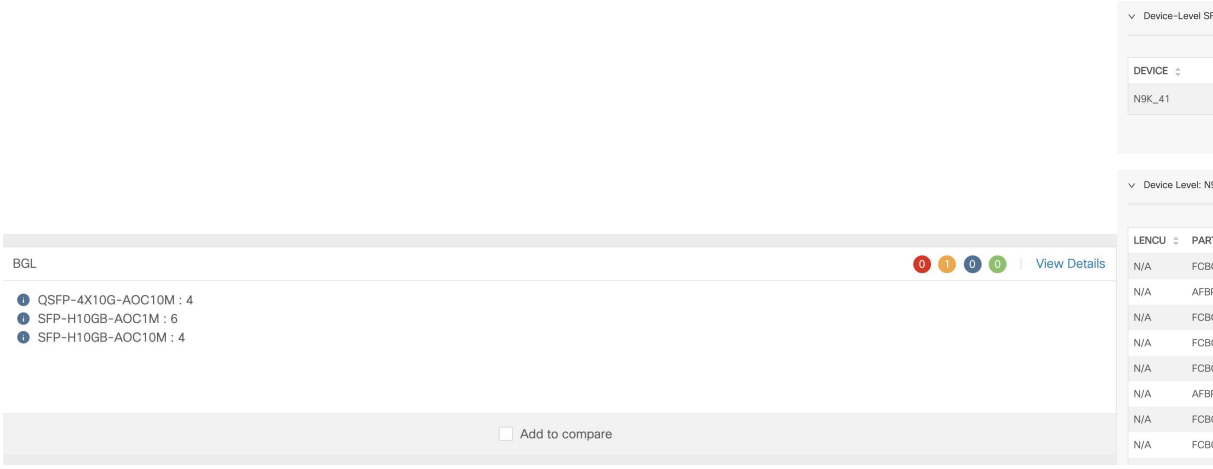


[詳細の表示（View Details）] をクリックして、モジュールとライセンスに関する詳細情報を表示します。



SFPレポート

このレポートは、ファブリックおよびデバイス レベルでの SFP の使用率に関する情報を提供します。



（注） スイッチインベントリおよび SFP レポートは、Cisco Nexus デバイスでのみサポートされます。

トラブルシューティング レポート

これらのレポートは、トラブルシューティングのシナリオに役立つように生成されます。現在、定義済みのトラブルシューティング レポートは **NVE VNI** カウンタ レポートのみです。**NVE VNI カウンタ** レポートの生成では、ネットワーク トラフィックに基づいて上位ヒットの VNI を特定するための定期的なチェックが実行されます。大規模なセットアップでは、レポートの生成頻度を 60 分以上に制限することをお勧めします。

NVE VNI カウンタ レポート

このレポートは、ファブリック内の各 VNI の **show nve vni counters** コマンド出力を収集します。

最も古いレポートと最新のレポートを比較すると、**[サマリ（Summary）]** セクションには上位 10 件のヒット VNI が表示されます。上位ヒット VNI は、次のカテゴリに表示されます。

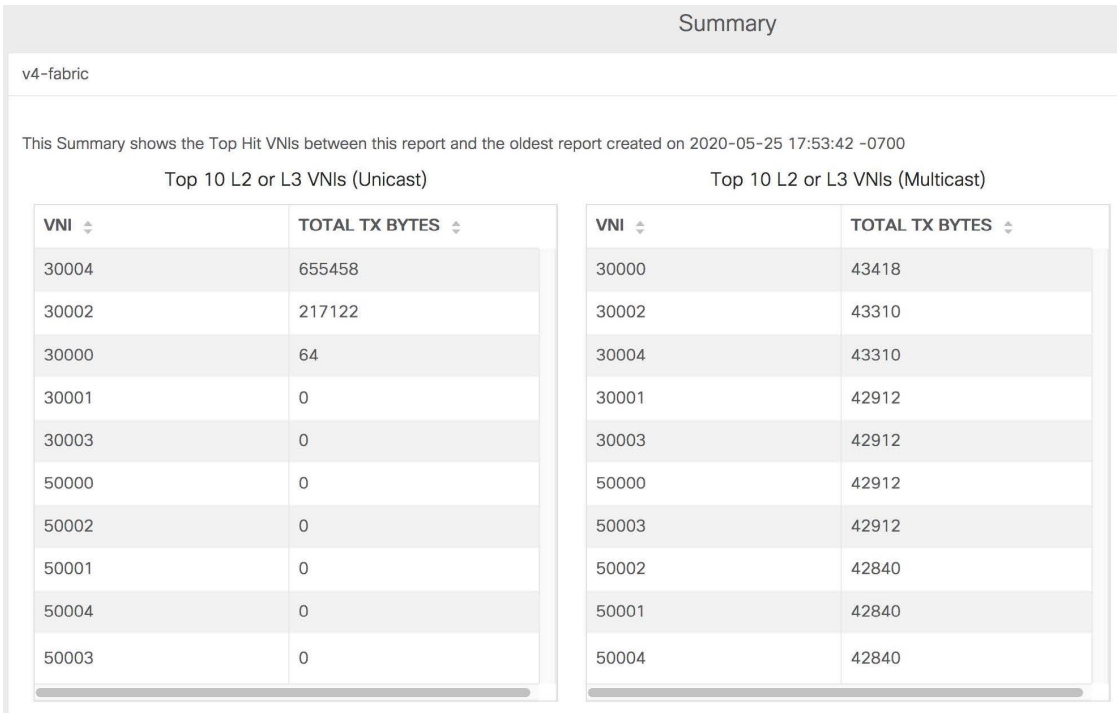
- ユニキャスト トラフィック用の L2 または L3 VNI
- マルチキャスト トラフィック用の L2 または L3 VNI
- ユニキャスト トラフィック用の L2 のみの VNI
- マルチキャスト トラフィック用の L2 のみの VNI
- ユニキャスト トラフィック用の L3 のみの VNI
- マルチキャスト トラフィック用の L3 のみの VNI

最も古いレポートは、現在のレポートタスクで保存された最初のレポートを参照します。現在のレポートと比較する必要がある最初のレポートとして特定のレポートを選択する場合は、選択したレポートが最初で最も古いレポートになるように、選択したレポートよりも古いすべてのレポートを削除します。

たとえば、昨日の午前 8 時、午後 4 時、および午後 11 時に 3 つのレポートが実行されたとします。今日のレポートの最初の最も古いレポートとして午後 11 時にレポートを使用する場合は、昨日の午前 8 時と午後 4 時に実行されました。

定期レポートの場合、最も古いレポートは、期間の開始時刻に実行される最初のレポートです。日次および週次レポートの場合、現在のレポートが以前に生成されたレポートと比較されます。

[サマリ（Summary）] セクションには、送信された合計バイト数と VNI に関する情報を含むカラムごとのレポートが表示されます。より多くの列を表示するには、ウィンドウの下部にある水平スクロール バーを使用します。


Summary

v4-fabric

This Summary shows the Top Hit VNIs between this report and the oldest report created on 2020-05-25 17:53:42 -0700

Top 10 L2 or L3 VNIs (Unicast)

VNI	TOTAL TX BYTES
30004	655458
30002	217122
30000	64
30001	0
30003	0
50000	0
50002	0
50001	0
50004	0
50003	0

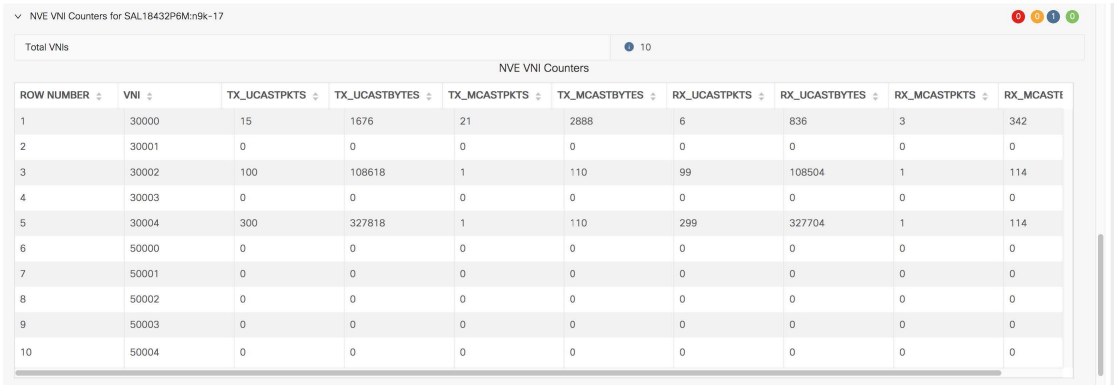
Top 10 L2 or L3 VNIs (Multicast)

VNI	TOTAL TX BYTES
30000	43418
30002	43310
30004	43310
30001	42912
30003	42912
50000	42912
50003	42912
50002	42840
50001	42840
50004	42840

VNI
30004
30002
30000
30001
30003

（注） NVE VNI カウンタ レポートの **[サマリ（Summary）]** セクションでは、スイッチのリロード後またはスイッチのカウンタのクリア後にレポートが生成された場合、[合計送信バイト数（TOTAL TX BYTES）] 列に負の数が表示されます。番号は、後続のレポートで正しく表示されます。回避策として、スイッチをリロードするか、カウンタをクリアする前に、古いレポートをすべて削除するか、新しいジョブを作成することを推奨します。

詳細については、**[詳細の表示（View Details）]** をクリックしてください。このセクションでは、スイッチごとに NVE VNI とカウンタを示します。


NVE VNI Counters for SAL18432P6M:n9k-17

Total VNIs 10

NVE VNI Counters

ROW NUMBER	VNI	TX_UCASTPKTS	TX_UCASTBYTES	TX_MCASTPKTS	TX_MCASTBYTES	RX_UCASTPKTS	RX_UCASTBYTES	RX_MCASTPKTS	RX_MCASTE
1	30000	15	1676	21	2888	6	836	3	342
2	30001	0	0	0	0	0	0	0	0
3	30002	100	108618	1	110	99	108504	1	114
4	30003	0	0	0	0	0	0	0	0
5	30004	300	327818	1	110	299	327704	1	114
6	50000	0	0	0	0	0	0	0	0
7	50001	0	0	0	0	0	0	0	0
8	50002	0	0	0	0	0	0	0	0
9	50003	0	0	0	0	0	0	0	0
10	50004	0	0	0	0	0	0	0	0

レポートの表示方法の詳細については、プログラム可能レポート（726ページ）を参照してください。

テンプレート機能のレポート

generateReport メソッド

レポートの生成中に generateReport メソッドが呼び出されます。レポートにはレポート導入ロジックが含まれます。このメソッドは、任意のコンテキスト オブジェクトを受け入れ、WrappersResp オブジェクトを返します。WrappersResp の詳細については、リンクを参照してください。

検証メソッド

検証メソッドはオプションです。テンプレートでこのメソッドが定義されている場合、プログラマブル レポート アプリケーションはこのメソッドを呼び出して、ジョブの作成中に事前検証チェックを実行します。このメソッドは、選択されたデバイスまたはファブリックの数に関係なく、ジョブが作成され、1 回だけ呼び出された場合にのみ呼び出されます。検証を通過すると、このメソッドは SuccessRetCode を持つ WrappersResp オブジェクトを返します。検証が失敗した場合、このメソッドはエラー リストとともに FailureRetCode を返します。

正常な検証と失敗した検証の例は次のとおりです。

*正常な検証

```
def validate(context):
    respObj = WrappersResp.getRespObj()

 ## Validation logic here

    respObj.setSuccessRetCode()
    return respObj
```

*失敗した検証

```
def validate(context):
    respObj = WrappersResp.getRespObj()

 ## Validation logic here

    respObj.setFailureRetCode()
    respObj.addErrorReport(template_name,error)
    return respObj
```

コンテキスト パラメータの内容に基づいて検証を実行することもできます。

コンテキスト パラメータ

コンテキスト パラメータは、次の属性で構成されます。

- ユーザー名：ジョブを作成したユーザーの名前
- ユーザーロール：ジョブを作成したユーザーのロール
- Job ID
- 再発：現在、1 回、毎日、毎週、毎月、オンデマンド、定期
- 期間：繰り返しが定期的な場合、期間には選択した頻度が表示されます。

ジョブ コンテキスト API の詳細については、「ジョブ コンテキスト情報」セクションを参照してください。

レポート Python ライブラリ

REPORT には次のコンポーネントがあります。

- 要約
  - キーと値
  - メッセージ - 推論
- 詳細/セクション
  - キーと値
  - JSON ドキュメント – カード
  - JSON ドキュメントの配列 – テーブル
- コマンド ログ

レポート JSON モデルを生成するための Python ライブラリが提供されています。これらの API を使用するには、次のインポート ステートメントをテンプレートに追加する必要があります。

```
from reportlib.preport import Report
```

レポート API

レポートの作成

「レポート」オブジェクトを作成するには、この API を使用します –

```
report = Report (“Report title”)
```

サマリの追加

各レポートには概要を含めることができます。これは python の辞書です。概要を追加するには、この API を使用します –

```
summary = report.add_summary ()
```

[概要へのコンテンツの追加（Adding Content to the Summary）]

概要にコンテンツを追加するには、次の API を使用します。

キーと値 -

```
summary [‘NXOS Version’] = ‘8.4(1)’
```

メッセージとインターフェイス -

```
summary.add_message (“Simple message”)
```

Note Cisco DCNM リリース 11.4(1) では、概要の値として JSON オブジェクトを追加することはサポートされていません。次の例はサポートされていません -

```
summary["info"] = {"key":"value","key-2":"value-2"}
```

[概要でテーブルの追加（Adding tables in Summary）]

概要にテーブルを追加するには、この API を使用します –

```
table = summary.add_table(title,_id)
```

title： テーブルのタイトル。

_id： テーブルの一意の識別子。

[テーブルへの行の追加（Adding rows to the table）]

テーブルに行を追加するには、この API を使用します –

```
table.append(value, _id)
```

値：JSON オブジェクトです。ネストされた JSON はサポートされません。

_id：行の一意の識別子です。

[セクションの追加（Adding a Section）]

セクションは、レポートコンテンツの論理グループです。セクションは、必要な情報を表示するためにユーザーが作成および構成します。セクションを追加するには、この API を使用します。

```
section = report.add_section ("Section title",_id)
```

_id：セクションの一意の識別子。

[セクションのキーと値へのコンテンツの追加（Adding Content to a Section Key and Values）]

セクションに単純なキーと値のペアを追加するには、この API を使用します。

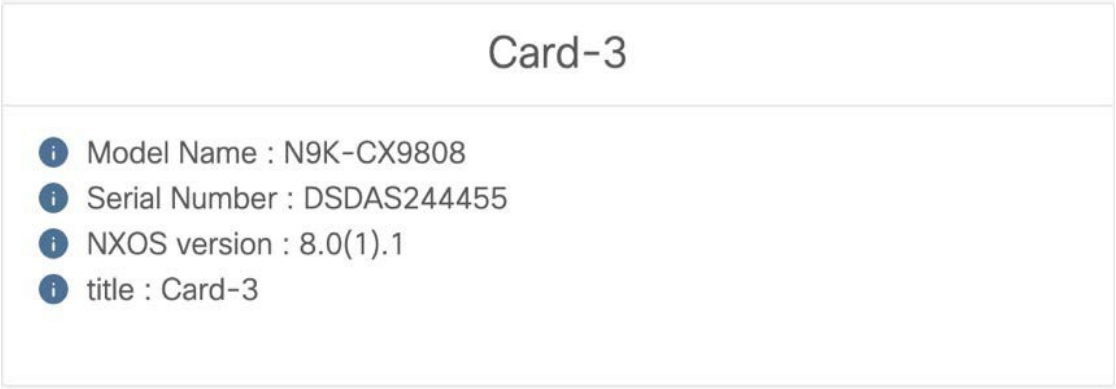
```
section['key'] = 'value'
```

[JSON ドキュメント – カード（JSON Document – Cards）]

JSON ドキュメントは、単純なキーと値のペアが追加されるのと同じ方法で追加できます。

Note ネストされた JSON は、Cisco DCNM リリース 11.4(1) ではサポートされていません。

カード ウィジェットとして表示される JSON ドキュメントの例を次に示します。



JSON ドキュメントの配列 – テーブル

テーブルを作成し、このテーブルに行を追加するには、この API を使用します。

```
section.append(key, dictionary, _id)
```

_id：テーブルの行を識別する一意の識別子。*_id* が重複すると、一意の id 違反エラーが発生します。

例：

```
section.append('Switch Details', {'name': 'N5K'},'DSDAS244455')
```

この API を使用したテーブルの作成には、次の制限があります。

- すべての JSON ドキュメントには、同じキー/列のセットが必要です。列の数または列名が異なると、テーブルが Web UI に表示されない場合があります。
- ネストされた JSON はサポートされません。

[Formatters]

Formatter は、ユーザー インターフェイスに表示される値の追加の書式設定を有効にします。たとえば、値を ERROR、SUCCESS、WARNING、および INFO としてマークできます。これらの値は色分けされ、Web UI に表示されます。エラーは赤、警告は黄色、情報は青、成功は緑で表示されます。

形式を構成するには、この API を使用します。

```
Formatter.add_marker(value,marker)
```

値：マーカーを追加する値

マーカー：Marker.ERROR、Marker.SUCCESS、Marker.WARNING、および Marker.INFO

例：

```
Formatter.add_marker (“NXOS version”,Marker.INFO)
```

グラフ

概要とセクションの両方にグラフを追加できます。

チャートを概要に追加するには、この API を使用します-

```
report = Report("title")
summary = report.add_summary()
summary.add_chart(ChartType, _id)
```

ChartType：ChartTypes.COLUMN_CHART、ChartTypes.PIE_CHART、および ChartTypes.LINE_CHART

_id：チャートの一意の ID

チャートをセクションに追加するには、この API を使用します。

```
report = Report("title")
section = report.add_section ("section_title",_id)
section.add_chart(ChartType, _id)
```

ChartType：ChartTypes.COLUMN_CHART、ChartTypes.PIE_CHART、および ChartTypes.LINE_CHART

_id：チャートの一意の ID

Note インポート セクションでクラスがインポートされていることを確認します。

円グラフ

円グラフで情報を表示するには、この API を使用します。

タイトルとサブタイトルを設定するには：

```
pie_chart.set_title("Chart title")
pie_chart.set_subtitle("Sub title")
```

値を追加するには：

```
pie_chart.add_value("key",value)
```

キー：文字列キー

値：数字の値

[列チャート（Column chart）]

縦棒グラフで情報を表示するには、この API を使用します。

タイトルとサブタイトルのタイトルを設定するには：

```
column_chart.set_title("Chart title")
column_chart.set_subtitle("Sub title")
```

X 軸と Y 軸のタイトルを設定するには

```
column_chart.set_xAxis_title("X-Axis title")
column_chart.set_yAxis_title("y-Axis title")
```

値を追加するには：

```
bar_chart.add_value("key",value,category)
```

キー：文字列キー

値：数字の値

カテゴリ：縦棒グラフは、データをカテゴリと呼ばれる論理グループに分割します。指定されたキーには、各カテゴリの値が必要です。たとえば、デバイス数がキーで、ファブリック名がカテゴリです。チャートには、各ファブリックのデバイス数が必要です。

折れ線グラフ

折れ線グラフで情報を表示するには、この API を使用します。

タイトルとサブタイトルのタイトルを設定するには：

```
line_chart.set_title("Chart title")
line_chart.set_subtitle("Sub title")
```

X 軸と Y 軸のタイトルを設定するには

```
line_chart.set_xAxis_title("X-Axis title")
line_chart.set_yAxis_title("y-Axis title")
```

値を追加するには：

```
line_chart.add_value("key",value,category)
```

キー：文字列キー

値：数字の値

カテゴリ：折れ線グラフは、データをカテゴリと呼ばれる論理グループに分割します。指定されたキーには、各カテゴリの値が必要です。たとえば、「デバイス数」がキーで、「ファブリック名」がカテゴリです。チャートには、ファブリックまたはカテゴリごとのデバイス数が必要です。

[デバイスでの CLI の実行（Running CLIs on a Device）]

デバイスでの CLI の実行を構成するには、この API を使用します。

```
from reportlib.preport import show
cli_responses = show(serial_number,*commands)
```

serial_number：コマンドを実行する必要があるデバイスのシリアル番号。VDC インスタンスの場合、シリアル番号は **[serial_number:vdc_name]** です。

**commands*：デバイスで実行されるコマンド。これらは可変引数です。

例：

- 単一のスイッチでコマンドを実行する：

```
cli_responses = show("FOX1816G0S9",'show version | xml', 'show inventory | xml', 'show
license usage | xml')
```

- 複数のスイッチでコマンドを実行する：

```
cli_responses = show( ["FOX1816G0S9","SSI15470HJ5"],'show version | xml', 'show
inventory | xml', 'show     license usage | xml')
```

[コマンドを表示して応答を保存（Show commands and store responses）]

show コマンドを構成し応答を保存するには、この API を使用します。

```
from reportlib.preport import show_and_store
cli_responses = show_and_store(report,serial_number,*commands)
```

report：以前に作成されたレポート オブジェクト。

serial_number：コマンドを実行するデバイスのシリアル番号。VDC の場合、シリアル番号は *serial_number:vdc_name* である必要があります。シリアル番号のリストを追加して、複数のデバイスで同じコマンド セットを実行できます。

commands：デバイスで実行するコマンド。これらは可変引数です。複数のコマンドを指定できます。

例：

- 単一のスイッチでコマンドを実行する：

```
cli_responses = show_and_store(report, "FOX1816G0S9", 'show version | xml', 'show
inventory | xml', 'show license usage | xml')
```

- 複数のスイッチでコマンドを実行する：

```
cli_responses = show_and_store(report, ["FOX1816G0S9","SSI15470HJ5"], 'show version
 | xml', 'show inventory | xml', 'show license usage | xml')
```

Note この API は、デバイスからの応答をレポートとともに elasticsearch に保存します。すべての応答を保存すると、使用可能なストレージ スペースが減少する可能性があるため、この API を使用するときは注意することをお勧めします。

[戻り値（Return value）]

上記の API は、応答のリストを返します。各応答は、次の構造を持つディクショナリです。

```
{
'status': 'success' | 'failed,
'response':<response from device>,
'command':<cli command>,
'serial_number': <device serial number>
}
```

複数のスイッチの場合、応答はスイッチごとに個別のエントリを持つ応答のリストです。

例：

```
[
{
'status': 'success',
'response':<response from device>,
'command':'show version',
'serial_number': 'FOX1816G0S9'
},
{
'status': 'success',
'response':<response from device>,
'command':'show version',
'serial_number': 'SSI15470HJ5'
}
]
```

[ジョブ コンテキスト情報（Job context information）]

アプリケーションからジョブをスケジュールしているときに繰り返しを表示するには、この API を使用します。

```
get_recurrence(context)
```

戻り値は、NOW、ONCE、DAILY、WEEKLY、MONTHLY、ONDEMAND、および PERIODIC です。

ジョブが定期的にスケジュールされ、特定の期間に関する情報を取得する必要がある場合は、この API を使用します。

```
period = get_period(context)
```

period.get_period()：期間を返します。

period. get_time_unit()：時間単位（HOURS、MINUTES）を返します。

[履歴レポートによる分析（Analysis with Historical Reports）]

[以前生成されたレポートを取得（Retrieve previously generated reports）]

過去に生成されたレポートを取得するには、*get_previous_reports()* メソッドを使用します。これは、現在のデータと履歴データに基づいて分析を実行するために使用できます。この API は、レポートが作成された時間の降順でレポートのリストを返します。

```
List of reports = get_previous_reports(context,entity,count)
```

コンテキスト：generateReport（コンテキスト）メソッドから入力として受け取ったオブジェクト

エンティティ：serial_number またはファブリック名

カウント：取得するレポートの数

[最も古いレポートを取得（Get oldest report）]

最も古いレポートを取得するには、この API を使用します。

```
oldest_report = get_oldest_report(context,entity)
```

コンテキスト：generateReport（コンテキスト）メソッドから入力として受け取ったオブジェクト

エンティティ：serial_number またはファブリック名

上記の両方の API は、情報を取得するために次の API を使用して Report オブジェクトを返します。

- 概要を取得する：*report.get_summary()*
- セクションの取得：*report.get_section(_id)*。*_id* は *[*セクションの追加（*Adding a Section*）*]* で説明したセクションの一意の識別子です。

[XML ユーティリティ（XML Utilities）]

XML ユーティリティは、xml.etree.elementtree（https://docs.python.org/2/library/xml.etree.elementtree.html）に基づいています。

[getxmltree]

指定されたタグの下にある XML ツリーを返すには、この API を使用します。

```
from reportlib.preport import getxmltree
xml_element_tree = getxmltree(xml_string,tag)
```

xml_string：デバイスからの XML 応答。

タグ：XML タグ。このタグの下の完全な XML は、ElementTree として返されます。

xml_element_tree：xml.etree.ElementTree オブジェクトを返す API

[getxmlrows]

CLI 応答に行が含まれている場合に行の配列を取得するには、この API を使用します。

```
from reportlib.preport import getxmlrows
rows = getxmlrows(xml_tree,tag_xpath)
```

xml_tree：xml.etree.ElementTree オブジェクト。

tag_xpath：XML レコードの xpath。
https://docs.python.org/2/library/xml.etree.elementtree.html#xpath-support を参照してください。

行：行の配列

[getnodevalue]

XML ノード値を読み取るには、この API を使用します。

```
from reportlib.preport import getnodevalue
value = getnodevalue(xml_tree,node_xpath)
```

xml_tree：**xml.etree.ElementTree** オブジェクト

node_xpath：XML レコードの xpath。
https://docs.python.org/2/library/xml.etree.elementtree.html#xpath-support を参照してください。

[ノードの存在を確認する（Check for existence of node）]

この API は、指定されたタグが XML ツリーに存在するかどうかに応じて、True または False を返します。

```
from reportlib.preport import
has_tag has_tag(xml_tree,tag)
```

xml_tree：**xml.etree.ElementTree** オブジェクト

[WrappersResp]

各レポートは**WrappersResp** タイプのオブジェクトを返す必要があります。これは、以下に示す API を使用して開始できます。これを com.cisco.dcbu.vinci.rest.services.jython import WrappersResp からインポートします。

```
respObj = WrappersResp.getRespObj()
```

WrapperResp のリターン コードは、レポートが正常に実行されたかどうかを示します。

- すべてのコマンドが実行され、必要な情報が抽出された場合、レポートは成功 API - *respObj.setSuccessRetCode()* を返します。
- コマンドの失敗などの例外が発生した場合、レポートは失敗 API - *respObj.setFailureRetCode()* を返します。

エラーコードを設定すると、レポートの実行に問題があり、レポートが生成されないことを示します。

エラーのあるレポートを返すには、Formatter を使用してエラーをマークし、*WrapperResp* を *Success* に設定します。詳細については、「*Formatters*」を参照してください。

発生する可能性のあるエラーについては、この API を使用してエラーの理由を指定できます。

```
respObj.addErrorReport(template_name,error_message)
```

作成したレポート オブジェクトは、次に示すように *WrappersResp* の値に設定する必要があります。

```
respObj.setValue(report)
```

ロガー

ロガーは、レポートテンプレートからのメッセージのログを有効にします。ロガーを使用して記録される情報は、「/usr/local/cisco/dcm/fm/logs/preport_jython.log」に記録されます。

```
Logger.info("message")
Logger.debug("message")
Logger.error("message")
Logger.trace("message")
Logger.warn("message")
```

テンプレートの追加

Cisco Web UI からユーザー定義のテンプレートを作成し、ジョブをスケジュールするには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択します。

[テンプレート プロパティ（Template Properties）] ウィンドウに、テンプレートの名前、その説明、サポートされるプラットフォーム、およびタグが表示されます。

ステップ 2 **[追加（Add）]** をクリックして新しいテンプレートを追加します。

[テンプレートのプロパティ（Properties）] ウィンドウが表示されます。

ステップ 3 [テンプレート名、詳細、タグとサポートされているプラットフォームを指定。（Specify a template name, description, tags, and supported platforms for the new template.）]

ステップ 4 テンプレートの**[テンプレート タイプ（Template Type）]**を指定します。

ステップ 5 テンプレートの**[テンプレート サブ タイプ（Template Sub Type）]**と**[テンプレート コンテンツ タイプ（Template Content Type）]**を選択します。

ステップ 6 **[詳細（Advanced）]** タブをクリックして、**[実装（Advanced）]**、**[依存関係（Dependencies）]**、**[公開（Published）]**、**[インポート（Imports）]**などの他のプロパティを編集します。**[発行済み（Published）]** を選択して、テンプレートを読み取り専用にします。公開されたテンプレートは編集できません。

ステップ 7 **[インポート（Imports）] > [テンプレート名（Template Name）]** リストから、テンプレートチェックボックスを選択します。

基本テンプレート コンテンツは、**[テンプレート コンテンツ（Template Content）]** ウィンドウに表示されます。ベース テンプレートには、テンプレート プロパティ、テンプレート変数、およびテンプレート コンテンツが表示されます。他のテンプレートにこのテンプレートをインポートすることができます。そして、基本テンプレートの内容は、拡張テンプレートの適切な場所に置き換えられます。拡張テンプレートを起動すると、基本テンプレートのパラメータ入力も取得されます。また、置換された内容は、完全な CLI コマンドの生成に使用されます。

Note 基本テンプレートは CLI テンプレートです。

ステップ 8 **[OK]** をクリックしてテンプレートのプロパティを保存するか、ウィンドウの右上隅にあるキャンセル アイコンをクリックして変更を元に戻します。

Note **[テンプレート プロパティ（Template Property）]** をクリックして、テンプレート プロパティを編集できます。

ステップ 9 **[テンプレート コンテンツ（Template Content）]** をクリックして、テンプレートの構文を編集します。構成テンプレートの構造については、「テンプレートの構造」の項を参照してください。

ステップ 10 **[テンプレート構文の検証]** をクリックして、テンプレート値を検証します。

エラーまたは警告メッセージが表示された場合は、エラーおよび警告フィールドをクリックして、**検証テーブル（Validation Table）**で検証の詳細を確認できます。

Note 警告のみがある場合は、テンプレートの保存を続行できます。ただし、エラーが発生した場合は、続行する前にテンプレートを編集してエラーを修正する必要があります。[開始行（Start Line）] 列の下の行番号をクリックして、テンプレートの内容でエラーを見つけます。テンプレート名がないテンプレートを検証すると、エラーが発生します。

ステップ 11 **[保存（Save）]** をクリックして、テンプレートを保存します。

ステップ 12 **[保存して閉じる（Save and Exit）]** をクリックし構成を保存して、構成テンプレート画面に戻ります。

テンプレートの変更

ユーザ定義のテンプレートを編集できます。ただし、定義済みのテンプレートおよびすでに公開されているテンプレートは編集できません。

Procedure

ステップ 1 **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** から、テンプレートを選択します。

ステップ 2 **[テンプレートの変更/表示（Modify/View template）]** をクリックします。

ステップ 3 テンプレートの説明とタグを編集します。

編集したテンプレートの内容が右側のペインに表示されます。

ステップ 4 **[インポート（Imports）] > [テンプレート名（Template Name）]** リストから、テンプレートチェックボックスを選択します。

基本テンプレート コンテンツは、**[テンプレート コンテンツ（Template Content）]** ウィンドウに表示されます。**[テンプレート コンテンツ（Template Content）]** ウィンドウで、要件に基づいてテンプレート コンテンツを編集できます。テンプレートのコンテンツの編集については、**[テンプレート コンテンツ（Template Content）]** ウィンドウの横にある [ヘルプ（Help）] アイコンをクリックします。

ステップ 5 テンプレートでサポートされているプラットフォームを編集します。

ステップ 6 **[テンプレートシンタックスの検証（Validate Template Syntax）]** をクリックして、テンプレート値を検証します。

ステップ 7 **[保存（Save）]** をクリックして、テンプレートを保存します。

ステップ 8 **[保存して閉じる（Save and Exit）]** をクリックし構成を保存して、構成テンプレート画面に戻ります。

テンプレートのコピー

Cisco DCNM Web UI からテンプレートをコピーするには、以下の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択して、テンプレートを選択します。

ステップ 2 **[テンプレートに名前を付けて保存（Save Template As）]** をクリックします。

ステップ 3 テンプレート名、説明、タグ、およびその他のパラメータを編集します。

編集したテンプレートのコンテンツが右側のペインに表示されます。

ステップ 4 **[インポート（Imports）] > [テンプレート名（Template Name）]** リストから、テンプレートチェックボックスを選択します。

基本テンプレート コンテンツは、**[テンプレート コンテンツ（Template Content）]** ウィンドウに表示されます。**[テンプレート コンテンツ（Template Content）]** ウィンドウで、要件に基づいてテンプレート コンテンツを編集できます。テンプレートのコンテンツの編集については、**[テンプレート コンテンツ（Template Content）]** ウィンドウの横にある [ヘルプ（Help）] アイコンをクリックします。

ステップ 5 テンプレートでサポートされているプラットフォームを編集します。

ステップ 6 **[テンプレートシンタックスの検証（Validate Template Syntax）]** をクリックして、テンプレート値を検証します。

ステップ 7 **[保存（Save）]** をクリックして、テンプレートを保存します。

ステップ 8 **[保存して閉じる（Save and Exit）]** をクリックし構成を保存して、構成テンプレート画面に戻ります。

テンプレートの削除

ユーザ定義テンプレートを削除できます。ただし、事前定義されたテンプレートは削除できません。Cisco DCNM リリース 11.0(1) 以降、複数のテンプレートを一度に削除できます。

Cisco DCNM Web UI からテンプレートを削除するには、以下の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択します。

ステップ 2 チェックボックスを使用してテンプレートを選択し、**[テンプレートの削除（Remove template）]** アイコンをクリックします。

テンプレートは警告メッセージなしで削除されます。

What to do next

DCNM Web UI のテンプレート リストからテンプレートが削除されます。DCNM サービスを再起動すると、削除されたテンプレートが **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** ページに表示されます。

テンプレートを永久的に削除するには、ローカル ディレクトリ `Cisco Systems\dcm\dcnm\data\templates\` に位置するテンプレートを削除します。

テンプレートのインポート

Cisco DCNM Web UI からテンプレートをインポートするには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択し、**[インポート テンプレート（Import Template）]** をクリックします。

ステップ 2 コンピュータに保存されているテンプレートを参照して選択します。

必要に応じて、テンプレートパラメータを編集できます。詳細については、テンプレートの変更, on page 488を参照してください。

Note テンプレート内の「\n」は、インポートおよび編集されると改行文字と見なされますが、ZIP ファイルとしてインポートされると正常に機能します。

ステップ 3 **[テンプレート構文の検証]** をクリックして、テンプレートを検証します。

ステップ 4 **[保存（Save）]** をクリックしてテンプレートを保存するか、**[保存して終了（Save and Exit）]** をクリックしてテンプレートを保存して終了します。

テンプレートのエクスポート

Cisco DCNM Web UI からテンプレートをエクスポートするには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択します。

ステップ 2 チェック ボックスを使用してテンプレートを選択し、**[テンプレートのエクスポート（Export Template）]** アイコンをクリックします。

ブラウザは、テンプレートを開くか、ディレクトリに保存するように要求します。

イメージ管理

デバイスを最新のソフトウェアバージョンに手動でアップグレードすると、時間がかかり、エラーが発生しやすくなります。迅速で信頼性の高いソフトウェアアップグレードを実現するために、イメージ管理はアップグレードの計画、スケジューリング、ダウンロード、およびモニタリングに関連する手順を自動化します。画像管理は、Cisco Nexus スイッチと でのみサポートされます。

（注） アップグレードする前に、Cisco Nexus 9000 シリーズ スイッチおよび Cisco Nexus 3000 シリーズ スイッチの POAP ブート モードが無効になっていることを確認します。POAP を無効にするには、スイッチ コンソールで [no boot poap enable] コマンドを実行します。ただし、アップグレード後に有効にすることができます。

[画像管理（Image Management）] メニューには、次のサブメニューとオプションが含まれています：

表 7: 画像管理メニュー

サブメニュー	オプション	操作	
イメージのアップロード	[スマート イメージ管理（Smart Image Management）]	イメージのアップロード	
		イメージの削除	
インストールとアップグレード	アップグレード履歴 ウィンドウ名：**ソフトウェア アップグレード タスク**	表示	
		削除	
		新規インストール	新しい ISSU インストール
			EPLD インストール
		インストールの終了	
	スイッチ レベルの履歴	デバイス アップグレード タスクを表示	
		スイッチ レベル履歴テーブルの更新	
パッケージ [SMU/RPM]	パッケージ	パッケージおよびパッチのインストール	
		パッケージおよびパッチのアンインストール	
		パッケージおよびパッチのアクティブ化	
		非アクティブ化	
画像管理ポリシー	画像管理ポリシー	画像管理ポリシーの追加	
		画像管理ポリシーの削除	

ユーザー ロールが **network-admin** または **device-upg-admin** であり、次の操作を実行するために DCNM をフリーズしていないことを確認します。

- イメージをアップロードまたは削除します。
- イメージのインストール、削除、またはイメージのインストールを終了します。
- パッケージおよびパッチをインストールまたはアンインストールします。
- パッケージおよびパッチをアクティブ化または非アクティブ化します。
- 画像管理ポリシーを追加または削除します（network-admin ユーザー ロールにのみ適用）。
- 管理ポリシーを表示します。

ユーザ ロールが network-admin、network-stager、network-operator、または device-upg-admin の場合は、任意のイメージインストールまたはデバイスアップグレードタスクを表示できます。DCNM がフリーズ モードの場合は、それらを表示することもできます。

[スマート イメージ管理（Smart Image Management）]

この機能により、POAP およびスイッチのアップグレード中に使用されるイメージをアップロードまたは削除できます。（This feature allows you to upload or delete images that are used during POAP and switch upgrade.） **[パッケージ（Packages）]** ウィンドウで、インストールに使用される RPM および SMU をアップロードまたは削除することもできます。 Cisco DCNM Web UI ホームページから **スマート イメージ管理（Image and Configuration Servers Smart Image Management）]** ウィンドウを表示するには、**コントロール（Repositories Control）] > [イメージ管理（Image Management）] > [イメージをアップロード（Image Upload）]** を選択します。

[**スマート イメージ管理**（Image and Configuration Servers Smart Image Management）] ウィンドウで、次の詳細を表示できます。

フィールド	説明
[プラットフォーム（Platform）]	プラットフォームの名前を指定します。イメージ、RPM、または SMU は、次のように分類されます。 • N9K/N3k • N6K • N7K • N77K • N5K • その他 • サード パーティ N9K プラットフォームと N3K プラットフォームのイメージは同じです。 アップロードされたイメージが既存のプラットフォームのいずれにもマッピングされていない場合、プラットフォームは [その他（Other）] になります。 プラットフォームは RPM の [サード パーティ（Third Party）] になります。
イメージ名	アップロードしたイメージ、RPM、または SMU のファイル名を指定します。
[イメージ タイプ（Image Type）]	イメージ、[EPLD、（EPLD,）]RPM、または SMU のファイル タイプを指定します。

フィールド	説明
[イメージのサブタイプ（Image Subtype）]	イメージ、EPLD、RPM、またはSMUのファイルタイプを指定します。 ファイルタイプ EPLD は [epld] です。イメージのファイル タイプは、[nxos]、[system] または [kickstart] です。RPM のファイルタイプは [feature] で、SMU のファイル タイプは [patch] です。
NXOS バージョン	Cisco スイッチのみの NXOS イメージ バージョンを指定します。
イメージ バージョン	Cisco 以外のデバイスを含むすべてのデバイスのイメージ バージョンを指定します。
サイズ（バイト）	イメージ、RPM、または SMU ファイルのサイズをバイト単位で指定します。
Checksum	イメージのチェックサムを指定します。チェックサムは、イメージ、RPM、または SMU のファイルに破損がないかどうかをチェックします。Cisco の Web サイトからダウンロードしたファイルと [イメージのアップロード（Image Upload）] ウィンドウでアップロードしたファイルのチェックサム値が同じかどうかを確認することで、信頼性を検証できます。

すべての列を並べ替えることができます。

イメージのアップロード

Cisco DCNM Web UI からサーバにさまざまなタイプの画像をアップロードするには、次の手順を実行します。

Note デバイスは、POAP またはイメージのアップグレード中にこれらのイメージを使用します。RPMとSMU は、**[パッケージ（Packages）]** ウィンドウで使用されます。すべての画像、RPM、およびSMU が **[画像管理ポリシー（Image Management Policies）]** ウィンドウで使用されます。

画像をアップロードするには、ユーザー ロールが **network-admin** または **device-upg-admin** である必要があります。**network-stager** ユーザ ロールでは、この操作を実行できません。

Procedure

ステップ 1 **[制御（Control）] > [画像管理（Image Management）] > [画像のアップロード（Image Upload）]** を選択します。

のスマート画像管理（Smart Image Management）] ウィンドウが表示されます。

ステップ 2 **[画像のアップロード（Image Upload）]** をクリックします。

[アップロードするファイルを選択（Select File to Upload）] ダイアログボックスが表示されます。

ステップ 3 **[ファイルの選択（Choose file）]** をクリックして、デバイスのローカル リポジトリからファイルを選択します。

ステップ 4 ファイルを選択し、**[アップロード（Upload）]**をクリックする。

ZIP ファイルもアップロードできます。シスコ DCNM は画像ファイルを処理して検証し、それに応じて既存のプラットフォームで分類します。**N9K/N3K**、**N6K**、**N7K**、**N77K**、または **N5K** プラットフォームに該当しない場合、イメージファイルは **サードパーティ**または**その他**のプラットフォームに分類されます。**サードパーティ** プラットフォームは、RPM にのみ適用されます。

ステップ 5 [OK] をクリックします。

[EPLD 画像、（EPLD images,）]RPM、および SMU はリポジトリにある次のパスにアップロードされます：**/var/lib/dcnm/upload/<platform_name>**

すべての NX-OS、キックスタートおよびシステム 画像はリポジトリにある次のパスにアップロードされます：**/var/lib/dcnm/images** と **/var/lib/dcnm/upload/<platform_name>**

ファイル サイズとネットワーク帯域幅によっては、アップロードに時間がかかります。

Note すべての Cisco Nexus シリーズ スイッチのイメージをアップロードできます。

Cisco Nexus 9000 シリーズ スイッチの EPLD イメージのみをアップロードできます。

ネットワークの速度が遅い場合は、Cisco DCNM の待機時間を 1 時間に増やして、画像のアップロードを完了します。Cisco DCNM Web UI からの待機時間を増やすには、次の手順を実行します。

a. **[管理者 (Administrator)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** を選択します。

b. **csrf.refresh.time** プロパティを検索し、値を **60** に設定します。

Note 値は分単位です。

c. [Apply Changes] をクリックします。

d. Cisco DCNM サーバを再起動します。

イメージの削除

Cisco DCNM Web UI から画像をリポジトリから削除するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [画像管理（Image Management）] > [画像のアップロード（Image Upload）]** を選択します。

のスマート画像管理（Smart Image Management）] ウィンドウが表示されます。

ステップ 2 リストから既存の画像を選択し、**[画像の削除（Delete Image）]** アイコンをクリックします。

確認ウィンドウが表示されます。

ステップ 3 [はい（Yes）] をクリックして、イメージを削除します。

[インストールとアップグレード（Install & Upgrade）]

[インストールおよびアップグレード（Install & Upgrade）] メニューには、次のサブメニューが含まれています。

アップグレード履歴

この機能により、In-Service Software Upgrade（ISSU）を使用して Cisco Nexus プラットフォーム スイッチをアップグレードできます。このアップグレード手順は、デバイス構成に基づいて、中断を伴う場合もあれば、中断しない場合もあります。アップグレードに必要なキックスタート、システム、または NX-OS イメージ SSIデバイス上のイメージ リポジトリまたはファイル システムから選択できます。リポジトリからイメージを選択するには、**[コントロール] > [イメージ管理] > [イメージ アップロード]** タブから同じイメージをアップロードする必要があります。

次の表では、**[制御] > [イメージ管理] > [アップグレード履歴]** に表示されるフィールドについて説明します。

フィールド	説明
タスク ID（Task Id）	タスクのシリアル番号を指定します。最新のタスクが上部に表示されます。 **Note** ネイティブ HA でフェールオーバーがトリガーされると、タスク ID シーケンス番号が 32 ずつ増加します。
タスクタイプ	タスクのタイプを指定します。 • 互換性 • アップグレード
[オーナー（Owner）]	Role-Based Authentication Control（RBAC）に基づいて、このタスクを開始した所有者を指定します。

フィールド	説明
デバイス	このタスク用に選択されたすべてのデバイスを表示します。
[ジョブ ステータス（Job Status）]	ジョブのステータスを指定します。 • 計画済み • In Progress（進行中） • Completed（完了） • 例外ありで完了 **Note** ジョブが 1 つまたは複数のデバイスで失敗した場合、ステータスフィールドには失敗を示す COMPLETED WITH EXCEPTION が表示されます。
作成時刻	タスクが作成された時間を指定します。
スケジュール	タスクの実行を指定する時刻を指定します。タスクを後で実行するようにスケジュールすることもできます。
完了時刻	タスクが完了した時間を指定します。
備考	タスクの実行中に所有者が追加したコメントを表示します。

Note Cisco DCNM の新規インストール後、このページにはエントリがありません。

次を実行します。

表示

Cisco DCNM Web UI からイメージ アップグレード履歴を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [画像管理（Image Management）] > [インストールおよびアップグレード（Install & Upgrade）] > [アップグレード履歴（Upgrade History）]**を選択し、タスク 識別子 チェックボックスを選択します。

一度に 1 つのタスクのみを選択します。

ステップ 2 [表示（View）] をクリックします。

[インストール タスクの詳細（Installation Task Details）] ウィンドウが表示されます。

ステップ 3 [設定（Settings）] をクリックします。**[列（Columns）]** メニューを展開し、表示する詳細を選択します。

このウィンドウには次の情報が表示されます。

- キックスタートとシステム イメージのローケーション
- 互換性チェック ステータス
- インストールステータス
- プレ ISSU レポート ステータスとポスト ISSU レポート ステータス
- 説明
- レポートサマリー
- バージョン チェック結果
- ログ

列は、表示することを選択したタスクに応じて変わります。EPLD タスクのスイッチ名、IP アドレス、プラットフォームの詳細、イメージ名、およびインストール ステータスを表示できます。レポート ステータスには、レポートの概要も含まれます。 レポートの概要には、ISSU 前の詳細レポートと ISSU 後のレポートへのハイパーリンクが含まれています。これらのハイパーリンクをクリックすると、レポートを表示するための新しいタブまたはウィンドウに移動します。レポート サマリーには、レポート テンプレートで定義したコマンドも含まれます。

ステップ 4 デバイスを選択します。

タスクの詳細ステータスが表示されます。完了したタスクについては、デバイスからの応答が表示されます。

アップグレード タスクが進行中の場合は、インストール プロセスのライブ ログが表示されます。

Note
- このウィンドウが表示されている場合、このテーブルは、進行中のジョブについて 30 秒ごとに自動更新されます。
- アップグレードされた EPLD 情報が表示されるまでに時間がかかります。スイッチが到達可能になるまで、5 分ごとにスイッチから DCNM に更新をフェッチするジョブがスケジュールされています。

削除

Cisco DCNM Web UI からタスクを削除するために、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [画像管理（Image Management）] > [インストールおよびアップグレード（Install & Upgrade）] > [アップグレード履歴（Upgrade History）]**を選択し、**[タスク 識別子（Task ID）]** チェックボックスを選択します。

ステップ 2 [削除（Delete）] をクリックします。

ステップ 3 **[OK]** をクリックして、ジョブの削除を確認します。

新規インストール

Cisco DCNM に ISSU および EPLD イメージをインストールできます。

新しい *ISSU* インストール

Cisco DCNM から検出されたデバイスをアップグレードするには、次の手順を実行します。

Before you begin

ISSU 前および ISSU 後のレポートが必要な場合は、**[テンプレート ライブラリ]** ウィンドウにレポート テンプレートを追加します。ISSU 前後の処理の詳細については、DCNM にパッケージ化されているデフォルトのアップグレード テンプレートを参照してください。デフォルトのアップグレード テンプレートは **issu_vpc_check** です。

Procedure

ステップ 1 **[制御（Control）]>[イメージ管理（Image Management）]>[インストールおよびアップグレード（Install & Upgrade）] > [アップグレード履歴（Upgrade History）]**を選択します。

ステップ 2 **[新しいインストール（New Installation）] > [ISSU]** を選択して、デバイス上のキックスタートおよびシステム イメージをインストールまたはアップグレードします。

デフォルトの VDC を持つデバイスが **[スイッチの選択（Select Switches）]** ウィンドウに表示されます。

Note フリーズモードまたはモニタリング モードのファブリックの一部であるスイッチは、ここにリストされていません。**[デバイス範囲（Device Scope）]** ドロップダウン メニューから、フリーズ モードまたはモニタ モードでファブリックを選択する場合、エラー メッセージが表示されます。

ステップ 3 スイッチ名の左側にあるチェック ボックスをオンにします。

複数のスイッチを選択して。

ステップ 4 [次へ（Next）] をクリックします。

[ISSU 前後のレポート（Pre-Post ISSU Reports）] ウィンドウが表示されます。

Note プレポストISSU レポートは、SANおよびメディア コントローラのインストールではサポートされていません。

ステップ 5 (Optional) **[ISSU 前後のレポートのスキップ（Skip Pre-Post ISSU Reports）]** チェックボックスをオンにして、スイッチの ISSU 前後のレポートをスキップし、ステップ *8* に進みます。

デフォルトでは、このチェックボックスはオフになっています。

ステップ 6 **[レポート テンプレートの選択]** ドロップダウン リストからレポート テンプレートを選択します。

[制御（Control）] > [テンプレート ライブラリ（Template Library）] ウィンドウにリストされている **UPGRADE** サブタイプを持つ **REPORT** テンプレート タイプのテンプレートのみが、**[レポート テンプレートの選択（Select Report Template）]** ドロップダウン リストに表示されます。

ステップ 7 ステップ *6* で選択したテンプレートに基づいて、**[全般]** タブの必須フィールドに入力します。

ステップ 8 [次へ（Next）] をクリックします。

[ソフトウェア イメージの指定（Specify Software Images）] ウィンドウが表示されます。このタブには、前の画面で選択したスイッチが表示されます。アップグレードするイメージも選択できます。

- **[自動ファイル選択]** チェック ボックスを使用すると、イメージ バージョン、およびアップグレードされたイメージを選択したデバイスに適用できるパスを指定できます。
- **[ファイル サーバーの選択]**を無効にし、デフォルトのサーバーが使用されます。
- **[イメージ バージョン]** フィールドで、**[イメージのアップロード]** ウィンドウに表示されるイメージのバージョンを指定します。
- **[パス]** フィールドは無効になり、デフォルトのイメージ パスが使用されます。

ステップ 9 **[キックスタート イメージ]** 列で **[イメージを選択]** をクリックします。

[ソフトウェア イメージ ブラウザ（Software Image Browser）] ダイアログボックスが表示されます。

Note
- Cisco Nexus 9000 シリーズ スイッチでは、Cisco NX-OS オペレーティング システムをロードするためにシステム イメージのみが必要です。したがって、これらのデバイスのキックスタート イメージを選択するオプションは無効になっています。
- **[ソフトウェア イメージ ブラウザ]** ダイアログ ボックスの表示に問題がある場合は、ブラウザのフォント サイズを小さくして再試行してください。

ステップ 10 **[システム イメージ]** 列で **[イメージの選択]** をクリックします。

[ソフトウェア イメージ ブラウザ（Software Image Browser）] ダイアログボックスが表示されます。

ステップ 11 **[ソフトウェア イメージ ブラウザ（Software Image Browser）]** ダイアログボックスで、**[ファイル サーバー（File Server）]** または **[スイッチ ファイル システム（Switch File System）]** からイメージを選択できます。

ファイル サーバーを選択した場合：

a) **[ファイル サーバーの選択]** リストから、イメージが保存されている Default_SCP_Repository のファイル サーバーを選択します。

b) **[画像の選択]** リストから、適切な画像を選択します。同じプラットフォームの他のすべての選択したデバイスに同じイメージを使用するには、チェック ボックスをオンにします。

例：プラットフォーム タイプ N9K-C93180YC-EX および N9K-C93108TC-EX の場合、ロジックはプラットフォーム（N9K）とサブプラットフォームの 3 つの文字（C93）に一致します。すべてのプラットフォーム スイッチで同じロジックが使用されます。

Note **ファイル サーバー**を選択すると、BIN 拡張子を持つファイルのみが一覧表示されます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバーを再起動します。デフォルトでは **true** に設定されています。

Note **[イメージのアップロード（Image Upload）]** ウィンドウに存在するイメージファイルのみが選択できます。他のパスにあるイメージは選択できません。

c) [VRF の選択（**Select Vrf**）] ドロップダウン リストから VRF を選択します。

Note このフィールドは、Cisco MDS スイッチには表示されません。

この VRF は、他の選択されたデバイスに対してデフォルトで選択されています。デフォルト値は **[management]** です。

d) [OK] をクリックします。

このイメージは、同じプラットフォーム タイプの他のすべての選択されたデバイスに対して選択されます。

[ファイル システムの切り替え] を選択した場合：

a) **[イメージの選択（Select Image）]** リストから、デバイスのフラッシュ メモリにある適切なイメージを選択します。

Note **スイッチ ファイル システム（Switch File System）]** を選択すると、BIN 拡張子を持つファイルのみが一覧表示されます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバーを再起動します。デフォルトでは **true** に設定されています。

b) **[OK]** をクリックしキックスタート イメージを選択するか、**[キャンセル（Cancel）]** をクリックして **[ソフトウェア イメージの指定（Specify Software Images）]** ダイアログ ボックスに戻ります。

ステップ 12 **[Vrf]** 列では、仮想ルーティングおよびフォワーディング（VRF）の名前を示します。

ステップ 13 **[使用可能なスペース（Available Space）]**列で、スイッチの**プライマリ スーパーバイザ**モジュールと**セカンダリ スーパーバイザ** モジュールに使用可能なスペースを指定します。

[使用可能なスペース] 列には、スイッチで使用可能なメモリが MB で表示されます (1 MB 未満の場合は、KB として表示およびマークされます。

ブートフラッシュ ブラウザでは、スイッチ ブートフラッシュにあるすべてのファイルとディレクトリのファイル名、サイズ、最新の変更日を表示します。ファイルを削除するには、ファイルを選択して **[削除]** をクリックし、スイッチの空き容量を増やします。

ステップ 14 **[選択されたファイルのサイズ]**列には、サーバーから選択されたイメージのサイズが表示されます。

選択したイメージの合計サイズがスイッチの使用可能なスペースより大きい場合、ファイルサイズは赤でマークされます。スイッチにイメージをコピーしてインストールするためのスペースを増やすことをお勧めします。

ステップ 15 スイッチをドラッグ アンド ドロップして、アップグレード タスク シーケンスを並べ替えます。

ステップ 16 (Optional) デバイス上の Cisco NX-OS ソフトウェア バージョンと、選択したアップグレードされたイメージとの互換性をチェックする場合は、**[バージョンの互換性をスキップ（Skip Version Compatibility）]** チェックボックスをオフにします。

ステップ 17 すべてのラインカードを同時にアップグレードするには、**[パラレル ライン カードのアップグレードの選択（Select Parallel Line Card upgrade）]** を選択します。

パラレル ライン カードのアップグレードは、Cisco MDS デバイスには適用されません。

ステップ 18 **[アップグレード オプション]** 列の **[オプション]** をクリックして、アップグレードのタイプを選択します。

[アップグレードオプション] ウィンドウに2つのアップグレードオプションが表示されます。**アップグレード オプション 1** のドロップダウン リストには、次のオプションがあります。

- **中断**
- **Bios force**
- **無停止を許可**
- **無停止を強制**

中断は、Cisco Nexus 9000 シリーズ スイッチのデフォルト値です。アップグレード オプションは、他のスイッチには**適用されません**。

[アップグレード オプション1] の下で **[無停止を許可（Allow Non Disruptive）]** を選択し、スイッチが無停止アップグレードをサポートしていない場合、中断アップグレードが実行されます。

アップグレード オプション 1 で **[無停止を強制（Force non-disruptive）]** を選択すると、互換性チェックが無停止アップグレードに必須であるため、**[バージョン互換性の確認（Skip Version Compatibility）]** チェック ボックスがオフになります。選択したスイッチが無停止アップグ

レードをサポートしていない場合、スイッチの選択を確認するよう求める警告メッセージが表示されます。スイッチを選択または削除するには、チェックボックスを使用します。

[アップグレード オプション 2] のドロップダウン リストには、**[アップグレード オプション 1]** で **[無停止を許可]** または **[無停止を強制]** を選択すると、次のオプションがあります。

- **北米**
- **バイオスフォース**

アップグレード オプション 1 で **Disruptive** または **Bios-force** を選択すると、**アップグレード オプション 2** では **アップグレード オプション 2** は無効になります。

選択したすべてのデバイスに選択したオプションを使用するには、**[他のすべての選択したデバイスにこのオプションを使用する]** チェック ボックスをオンにして、**[OK]** をクリックします。

Note
- アップグレード オプションは、Cisco Nexus 3000 シリーズおよび 9000 シリーズ スイッチにのみ適用されます。
- アップグレードに **[無停止を許可]** オプションを選択しても、無停止アップグレードが保証されるわけではありません。互換性チェックを実行して、デバイスが無停止アップグレードをサポートしていることを確認します。

ステップ 19 [次へ（Next）] をクリックします。

[バージョンの互換性をスキップ] を選択しなかった場合、Cisco DCNM は互換性チェックを実行します。

チェックが完了するまで待つか、**[後でインストールを終了]** をクリックするかを選択できます。

インストール ウィザードが閉じられ、互換性タスクが **[制御] > [イメージ管理] > [インストールとアップグレード] > [アップグレード履歴タスク]** で作成されます。

イメージの互換性のチェックにかかる時間は、構成とデバイスの負荷によって異なります。

互換性検証 ステータス列には、検証のステータスが表示されます。

[バージョン互換性をスキップ（Skip Version Compatibility）] を選択してバージョン互換性チェックをスキップすると、Cisco DCNM はデバイスの名前だけを表示します。**[現在のアクション]** 列には **[完了]** と表示され、**互換性検証]** 列には **[スキップされました]** と表示されます。

ISSU 前レポート ステータス（Pre-ISSU Report Status）] 列は、ISSU 前レポートが生成されたかどうかを示します。**[互換性ステータス]** 列で、互換性ログとレポートの概要を表示できます。レポート サマリーのハイパーリンクをクリックして、ISSU 前チェックの詳細レポートを表示します。

Note インターネットの帯域幅によっては、ステータスが Web UI に反映されるまでに時間がかかる場合があります。

スイッチの選択を確認し、それに応じてアップグレードするスイッチをオンまたはオフにすることができます。

ステップ 20 **[後でインストールを終了]** をクリックして、後でアップグレードを実行します。

ステップ 21 [次へ（Next）] をクリックします。

ステップ 22 デバイスのアップグレード前に実行構成をスタートアップ構成に保存するには、このチェックボックスをオンにします。

ステップ 23 アップグレードプロセスは、すぐに実行するか、後で実行するようにスケジュールできます。

a. デバイスを今すぐアップグレードするには、**[今すぐ展開（Deploy Now）]** を選択します。

b. **[展開時間の選択（Choose time to Deploy）]** を選択し、後でアップグレードを実行するための時刻を MMM/DD/YYYY HH:MM:SS 形式で指定します。

時刻はサーバーに相対的です。選択した展開時刻が過去の場合、ジョブはすぐに実行されます。

ステップ 24 アップグレード対象として選択したデバイスとラインカードに基づいて、実行モードを選択できます。

a. **[順次]** を選択して、選択した順序でデバイスをアップグレードします。

Note デバイスをメンテナンス モードにすると、このオプションは無効になります。

b. **[同時]** を選択して、すべてのデバイスを同時にアップグレードします。

ステップ 25 **[終了（Finish）]** をクリックし、アップグレード プロセスを開始します。

インストール ウィザードが閉じ、**[制御] > [イメージ管理] > [インストールとアップグレード] > [アップグレード履歴]** ページにアップグレードするタスクが作成されます。

What to do next

スイッチで ISSU を完了したら、スイッチが再起動し、SNMP エージェントが安定するまで 20 分間待機します。DCNM は、Cisco DCNM Web UI にスイッチの新しいバージョンを表示するために、投票サイクルを検出します。

EPLD インストール

Cisco DCNM は、Cisco Nexus 9000 シリーズ スイッチでの 2 種類の EPLD 画像のインストールまたはアップグレードをサポートしています。

- EPLD 画像からすべてのモジュールをアップグレードします。
- EPLD 画像から特定のモジュールのみをアップグレードします。

リポジトリから画像を選択するには、**[制御（Control）] > [画像管理（Image Management）] > [画像のアップロード（Image Upload）]** からアップロードします。

Cisco DCNM で EPLD 画像をインストールまたはアップグレードするには、次の手順を実行します。

手順

ステップ 1 **[制御（Control）] > [画像管理（Image Management）] > [インストールとアップグレード（Install & Upgrade）] > [アップグレード履歴（Upgrade History）]** を選択します。

ステップ 2 **[新規インストール（New Installation）] > [EPLD]** を選択します。

[スイッチの選択（Select Switches）] ウィンドウに Cisco Nexus 9000 シリーズ スイッチが表示されます。

（注） フリーズモードまたは監視モードのファブリックの一部であるスイッチは、ここにリストされていません。**[デバイス範囲（Device Scope）]** ドロップダウン メニューから、フリーズモードまたはモニタ モードでファブリックを選択する場合、エラー メッセージが表示されます。

ステップ 3 スイッチ名の左側にあるチェックボックスをチェックします。

複数のデバイスを選択できます。

ステップ 4 [次へ（Next）] をクリックします。

[EPLD 画像の指定（Specify EPLD Images）] ウィンドウが表示されます。このタブには、前の画面で選択したスイッチが表示され、アップグレードする EPLD 画像を選択できます。

ステップ 5 **[EPLD 画像（Select Image）]** 列で **[画像の選択（EPLD image）]** をクリックします。

[EPLD 画像ブラウザ（EPLD Image Browser）] ダイアログ ボックスが表示されます。

ステップ 6 ファイル サーバまたはスイッチ ファイル システムから EPLD 画像 ファイルを選択します。

[ファイル サーバ（File Server）] を選択した場合：

a) **[画像の選択（Select Image）]** リストから適切な画像を選択します。

（注）
- **[ファイル サーバ（File Server）]** を選択すると、IMG 拡張子を持つファイルのみがリストされます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバーを再起動します。デフォルトでは **true** に設定されています。
- **[イメージのアップロード（Image Upload）]** ウィンドウに存在するイメージ ファイルのみが選択できます。他のパスにある画像は選択できません。

b) **[OK]** をクリックして EPLD 画像を選択するか、**[キャンセル（Cancel）]** をクリックして、**[ソフトウェア画像の指定（Specify Software Images）]** ウィンドウに戻ります。

[ファイル システムの切り替え] を選択した場合：

a) **[イメージの選択（Select Image）]** リストから、デバイスのフラッシュ メモリにある適切なイメージを選択します。

（注） **[ファイル システムの切り替え（Switch File System）]** を選択すると、IMG 拡張子を持つファイルのみが一覧表示されます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバーを再起動します。デフォルトでは **true** に設定されています。

b) **[OK]** をクリックし EPLD 画像を選択するか、**[キャンセル（Cancel）]** をクリックして **[ソフトウェア画像の指定（Specify Software Images）]** ダイアログ ボックスに戻ります。

ステップ 7 [VRF の選択（Select Vrf）] ドロップダウン リストから VRF を選択します。

有効な値は、管理、デフォルト、およびキープアライブです。

ステップ 8 （任意） 選択した他のすべてのデバイスに VRF を使用するには、**[その他すべての選択されたデバイスにこの VRF を使用する（Use this Vrf for other all selected devices）]** チェックボックスをオンにします。

ステップ 9 （任意） 選択した他のすべてのデバイスにこの画像を使用するには、**[同じプラットフォーム タイプのその他すべての選択されたデバイスにこの画像を使用するUse this image for other all selected devices of same platform type]** チェックボックスをオンにします。

ステップ 10 **[Vrf]** 列では、仮想ルーティングおよびフォワーディング（VRF）の名前を示します。

ステップ 11 **[使用可能なスペース（Available Space）]** 列で、スイッチの**プライマリ スーパーバイザ** モジュールと**セカンダリ スーパーバイザ** モジュールに使用可能なスペースを指定します。

[使用可能なスペース（Available Space）] 列には、スイッチで使用可能なメモリが MB 単位で表示されます（1 MB 未満の場合は、KB として表示およびマークされます）。

ブートフラッシュ ブラウザでは、スイッチ ブートフラッシュにあるすべてのファイルとディレクトリのファイル名、サイズ、最新の変更日を表示します。ファイルを削除するには、ファイルを選択して **[削除]** をクリックし、スイッチの空き容量を増やします。

ステップ 12 選択した画像の合計サイズが、**[選択されたファイルのサイズ（Selected Files Size）]** 列のスイッチで使用可能なスペースより大きいかどうかを確認します。

[選択されたファイルのサイズ（Selected Files Size）] 列には、サーバから選択した画像のサイズが表示されます。

選択したイメージの合計サイズがスイッチの使用可能なスペースより大きい場合、ファイル サイズは赤でマークされます。スイッチにイメージをコピーしてインストールするためのスペースを増やすことをお勧めします。

（注） 返されるはずのバージョンが返されない場合、EPLDのアップグレードは失敗します。

ステップ 13 スイッチをドラッグアンドドロップして、アップグレード タスクの順序を並び替えます。

ステップ 14 **[モジュール オプション（Module Options）]** 列のハイパーリンクをクリックして、対応するスイッチのモジュールを選択して EPLD モジュールをアップグレードします。

[モジュール オプション（Module Options）] ダイアログ ボックスが表示されます。デフォルト値は **[すべて（All）]** で、選択したスイッチのすべての EPLD モジュールをインストールまたはアップグレードします。

ステップ 15 モジュールを選択します。

ステップ 16 [OK] をクリックします。

ステップ 17 **[FPGA リージョン（FPGA Region）]** 列の下のハイパーリンクをクリックして、FPGA リージョンを選択します。

有効なオプションは、**[プライマリ（Primary）]** および **[ゴールデン（Golden）]** です。

ゴールデン アップグレードを選択した場合は、BIOS が更新され、すべての前提条件が満たされていることを確認してください。詳細については、「*Cisco Nexus 9000* シリーズ *FPGA/EPLD* アップグレード リリース ノート」を参照してください。

ステップ 18 **[終了（Finish）]** をクリックし、アップグレード プロセスを開始します。

インストール ウィザードが閉じ、アップグレードするタスクが **[制御（Control）] > [画像管理（Image Management）] > [インストールおよびアップグレード（Install & Upgrade）] > [アップグレード履歴（Upgrade History）]** ウィンドウで作成されます。EPLD アップグレード タスクは、タスク タイプによって識別できます。

次のタスク

スイッチのアップグレードが完了したら、スイッチが再起動し、SNMP エージェントが安定するまで 20 分間待機します。Cisco DCNM は、Cisco DCNM Web UI の **[スイッチ レベル履歴（Switch Level History）]** ウィンドウにスイッチの新しいバージョンを表示するために、ポーリング サイクルを検出します。

[イベント（Events）] ウィンドウで EPLD ゴールデン アップグレード通知を表示できます。Cisco DCNM Web UI のホームページから、**[モニタ（Monitor）] > [スイッチ（Switch）] > [イベント（Events）]** を選択します。

インストールの終了

[互換性チェック（Compatibility Check）] ページで完了したタスクのインストールを完了することを選択できます。次のタスクを実行して、デバイスのアップグレードプロセスを完了します。

Procedure

ステップ 1 **[制御（Control）] > [イメージ管理（Image Management）] > [インストールとアップグレード（Install & Upgrade）] > [アップグレード履歴（Upgrade History）]** を選択し、互換性チェックが完了したタスクを選択します。

一度に 1 つのタスクのみを選択します。

ステップ 2 **[インストールの終了（Finish Installation）]** をクリックします。

[ソフトウェア インストール ウィザード（Software Installation Wizard）] が表示されます。

ステップ 3 スイッチの選択を確認し、それに応じてアップグレードするスイッチをオンまたはオフにすることができます。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 デバイスのアップグレード前に実行構成をスタートアップ構成に保存するには、このチェックボックスをオンにします。

ステップ 6 チェックボックスをオンにして、アップグレードの前にデバイスをメンテナンス モードにします。このオプションは、メンテナンス モードをサポートするデバイスに対してのみ有効です。

ステップ 7 アップグレードプロセスは、すぐに実行するか、後で実行するようにスケジュールできます。

a. デバイスを今すぐアップグレードするには、**[今すぐ展開（Deploy Now）]** を選択します。

b. **[展開時間の選択（Choose time to Deploy）]** を選択し、後でアップグレードを実行するための時刻を MM/DD/YYYY HH:MM:SS 形式で指定します。

ステップ 8 アップグレード対象として選択したデバイスとライン カードに基づいて、実行モードを選択できます。

a. **[順次（Sequential）]** を選択して、選択された順序でデバイスをアップグレードします。

Note デバイスをメンテナンス モードにすると、このオプションは無効になります。

b. **[同時（Concurrent）]** を選択して、すべてのデバイスを同時にアップグレードします。

ステップ 9 **[終了（Finish）]** をクリックして、アップグレード プロセスを完了します。

スイッチ レベルの履歴

アップグレードプロセスの履歴をスイッチ レベルで表示できます。スイッチの現在のバージョンとその他の詳細を表示できます。

次の表では、**[制御（Control）] > [画像管理（Image Management）] > [インストールとアップグレード（Install & Upgrade）] > [スイッチ レベル履歴（Switch Level History）]** に表示されるフィールドについて説明します。

フィールド	説明
スイッチ名	スイッチの名前を指定します
IP アドレス	スイッチの IP アドレスを指定します
プラットフォーム	Cisco Nexus スイッチ プラットフォームを指定します

フィールド	説明
現在のバージョン	スイッチ ソフトウェアの現在のバージョンを指定します。

スイッチ名の横にあるラジオボタンをクリックしてスイッチを選択し、そのアップグレード履歴を表示します。**[表示（View）]** をクリックして、選択したスイッチのアップグレード タスク履歴を表示します。

次の表では、**[制御（Control）] > [画像管理（Image Management）] > [インストールとアップグレード（Install & Upgrade）] > [スイッチ レベル履歴（Switch Level History）] > [デバイス アップグレード タスクの表示（View Device Upgrade Tasks）]** に表示されるフィールドについて説明します。

フィールド	説明
オーナー（Owner）	アップグレードを開始した所有者を指定します。
[ジョブ ステータス（Job Status）]	ジョブのステータスを指定します。 • 計画済み • In Progress（進行中） • Completed（完了）
キックスタート画像	スイッチのアップグレードに使用するキックスタート イメージを指定します。
システムのイメージ（System Image）	スイッチのアップグレードに使用するシステム画像を指定します。
完了時刻	アップグレードが正常に完了した日時を指定します。
ステータスの説明	ジョブのインストールログ情報を指定します。

パッケージ

画像管理は、必要なパッケージとパッチのインストールまたはアンインストールにも役立ちます。スイッチにインストールされているすべての RPM パッケージと SMU パッチが **[パッケージ [SMU/RPM]（Package [SMU/RPM]）]** ウィンドウに表示されます。パッケージまたはパッチに対して次のアクションを実行できるようになりました。

- インストール
- アンインストール
- 有効化

• 非アクティブ化

この操作を実行するには、管理者権限が必要です。次のテーブルは、**[制御（Control）] > [画像管理（Image Management）] > [パッケージ [SMU/RPM]（Package [SMU/RPM]）] > [インストール履歴（Installation History）]**に現れるフィールドを説明します。

フィールド	説明
Switch Name	ファイルがインストールされているスイッチの名前を指定します。
シリアル番号（Serial Number）	スイッチのシリアル番号を指定します。
IP Address	デバイスの IP アドレスを指定します。
リリース	スイッチのリリース OS バージョンを指定します。
Name	ファイルの名前を指定します。
バージョン	ファイルのバージョンを指定します。
[タイプ（Type）]	ファイルが基本パッケージ、非基本パッケージ、またはパッチのいずれであるかを指定します。
ステータス	パッケージまたはパッチがアクティブ化されているかどうかを指定します。有効な値は**[アクティブ（active）]**と**[非アクティブ（inactive）]**です。

[パッケージ（Package）] ウィンドウで次のタスクを実行することができます。

パッケージおよびパッチのインストール

Cisco DCNM Web UI からパッケージまたはパッチをインストールするには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [画像管理（Image Management）] > [パッケージ [SMU/RPM]（Package [SMU/RPM]）]** を選択し、**[インストール]** アイコンをクリックします。

[デバイスの選択（Select Devices）] ウィンドウが表示されます。

Note フリーズモードまたは監視モードのファブリックの一部であるスイッチは、ここにリストされていません。**[デバイス範囲（Device Scope）]** ドロップダウンメニューから、フリーズモードまたはモニタモードでファブリックを選択する場合、エラーメッセージが表示されます。

スイッチが移行モードの場合、チェック ボックスは無効になります。

ステップ 2 スイッチ名の左側にあるチェックボックスを選択します。

複数のスイッチを選択できます。

ステップ 3 [次へ（Next）] をクリックします。

ステップ 4 **[パッケージ / パッチ（Packages/Patches）]** 列の **[パッケージの選択（Select Packages）]**

[パッケージ/パッチ ブラウザ（Packages/Patches Browser）] ダイアログ ボックスが表示されます。

ステップ 5 **[ファイル サーバ（File Server）]** または **[スイッチ ファイル システム（Switch File System）]** からファイルを選択します。

ファイル サーバを選択した場合:

a) **[画像の選択（Select Image）]** リストから、デバイスにインストールする必要がある適切なパッケージまたはパッチを選択します。

特定のプラットフォーム用にアップロードされたパッケージまたはパッチは、このファイルセレクターにリストされます。インストールするファイルを複数選択できますが、インストールでスイッチのリロードが必要な場合は、パッチまたはパッケージを 1 つだけ選択してください。

同じプラットフォームの他のすべての選択されたデバイスに同じパッケージを使用するには、チェックボックスをオンにします。

このパッケージまたはパッチ画像は、他の選択されたデバイスに対してデフォルトで選択されています。

b) **[OK]** をクリックしてパッチ画像を選択します。

c) ドロップダウン リストから VRF を選択します。

この VRF は、選択した他のすべてのデバイスに使用できます。

この VRF は、他の選択されたデバイスに対してデフォルトで選択されています。

[ファイル システムの切り替え（Switch File System）] を選択した場合：

a) **[画像の選択（Select Image）]** リストから、デバイスのフラッシュ メモリにある適切なファイル画像を選択します。

デバイスにインストールするファイルを複数選択できますが、インストールでデバイスのリロードが必要な場合は、パッチまたはパッケージを 1 つだけ選択してください。**[ファイル システムの切り替え（Switch File System）]** を選択すると、RPM または SMU 拡張子を持つファイルのみがリストされます。他のファイルを表示するには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** を選択し、**[FILE_SELECTION_FILTER]** を **[false]** に設定して、サーバーを再起動します。デフォルトでは **true** に設定されています。

b) [**OK**] をクリックします。

ステップ 6 [Finish] をクリックします。

[パッケージ（Packages）] ウィンドウで、スイッチにインストールされているパッケージのリストを表示できます。

Note パッケージをインストールすると、それもアクティブ化されます。

パッケージおよびパッチのアンインストール

アンインストールプロセスでは、選択したパッケージまたはパッチが非アクティブ化され、その後削除されます。非ベースRPMパッケージとSMUパッチのみを削除できます。ベースRPMパッケージをアンインストールすると、非アクティブ化されるだけです。ベースRPMパッケージは削除できません。アンインストールでデバイスの再ロードが必要な場合は、パッチまたはパッケージを1つだけ選択します。

Cisco DCNM Web UIからデバイスのパッケージまたはパッチをアンインストールするには、次の手順を実行します。

Procedure

ステップ1 **[制御（Control ）] > [画像管理（Image Management）] > [パッケージ [SMU/RPM]（Package [SMU/RPM]）]** を選択します。

ステップ2 パッケージまたはパッチを選択し、**[アンインストール（Uninstall）** アイコンをクリックします。

確認ウィンドウが表示されます。

ステップ3 [OK] をクリックします。

一度に複数のパッケージまたはパッチをアンインストールできますが、選択したすべてのパッケージまたはパッチのステータスは同じである必要があります。

パッケージおよびパッチのアクティブ化

非アクティブなパッケージまたはパッチをアクティブ化できます。Cisco DCNM Web UIからパッケージまたはパッチをアクティブ化にするには、次の手順を実行します。

Procedure

ステップ1 **[[制御（Control ）] > [画像管理（Image Management）] > [パッケージ [SMU/RPM]（Package [SMU/RPM]）]** を選択します。

ステップ2 非アクティブなパッケージまたはパッチを選択し、**[アクティブ化（Activate）]** アイコンをクリックします。

確認用のダイアログボックスが表示されます。

ステップ3 [OK] をクリックします。

[インストール タスクの詳細（Installation Task Details）] ダイアログ ボックスが表示されます。**[ステータス（Status）]** 列の下のハイパーリンクをクリックして、インストール ステータスの詳細を表示できます。

非アクティブ化

アクティブなパッケージまたはパッチを非アクティブ化できます。Cisco DCNM Web UI からパッケージまたはパッチを非アクティブ化にするには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control ）] > [画像管理（Image Management）] > [パッケージ [SMU/RPM]（Package [SMU/RPM]）]** を選択します。

ステップ 2 1 つ以上のアクティブなパッケージまたはパッチを選択し、**[非アクティブ化（Deactivate）]** アイコンをクリックします。

確認用のダイアログボックスが表示されます。

ステップ 3 **[OK]**をクリックします。

画像管理ポリシー

イメージ管理ポリシーには、RPM または SMU とともに NX-OS イメージの目的の情報が含まれます。ポリシーは、特定のプラットフォームに属することも、さまざまなタイプのプラットフォームに対して包括的に属することもあります。包括タイプのポリシーには、1 つ以上のプラットフォームのポリシーを含めることができます。スイッチのプラットフォームに関係なく、包括的なイメージ管理ポリシーをスイッチのグループに関連付けることができます。包括タイプのポリシーでは、プラットフォームごとに1つのプラットフォーム ポリシーのみを選択できます。スイッチに適用されたポリシーに基づいて、Cisco DCNM では必要な NXOS と RPM または SMU がスイッチに存在するかどうかが確認されます。スイッチ上のポリシーとイメージの間に不一致があると、ファブリック警告が生成されます。

次のテーブルに **[ポリシー（Policies）]** ウィンドウのフィールドと詳細があります。

フィールド	説明
ポリシー名（Policy Name）	ポリシー名を指定します。
ポリシータイプ	ポリシー タイプが **[プラットフォーム（PLATFORM）]** か **[Cisco Umbrella（UMBRELLA）]** かを指定します。
リリース	プラットフォーム ポリシーのプラットフォーム リリースを指定します。包括的なポリシーの場合、フィールドは空です。

フィールド	説明
[ポリシー/パッケージ名（Policy / Package Name）]	パッチまたは、パッケージ名を指定します。プラットフォーム ポリシーにはパッケージ名が表示され、Cisco 包括ポリシーには関連するプラットフォーム ポリシーが表示されます。
プラットフォーム	プラットフォーム ポリシーのプラットフォームを指定します。
[ポリシーの説明（Policy Description）]	ユーザー定義のポリシーの説明を指定します。

[ポリシー（Policies）] ウィンドウで次のタスクを実行することができます。

画像管理ポリシーの追加

Cisco DCNM Web UI から画像管理ポリシーを追加するには、次の手順を実行します。

Before you begin

画像ポリシーを作成する前に、**[画像のアップロード（Images Upload）]** タブで画像をアップロードします。画像のアップロードに関しては、「イメージのアップロード, on page 494」セクションを参照してください。

Procedure

ステップ 1 **[制御（Control）]** > **[画像管理（Image Management）]** > **[画像管理ポリシー（Image Management Policies）]** の順に選択します。

[ポリシー（Policies）] ウィンドウが表示されます。

ステップ 2 [追加（Add）] アイコンをクリックします。

[イメージ管理ポリシーの作成（Create Image Management Policy）] ダイアログボックスが表示されます。

ステップ 3 ポリシー タイプの選択

有効な値は**プラットフォーム**と**包括的** です。

ステップ 4 a) **プラットフォーム** ポリシータイプを選択すると、**[画像管理ポリシーの作成（Create Image Management Policy）]** ダイアログ ボックスに次のフィールドが表示されます。

フィールド	アクション
ポリシー名（Policy Name）	ポリシー名を入力します。

フィールド	アクション
プラットフォーム	プラットフォーム ドロップダウンリストからプラットフォームを選択します。オプションは、**[画像のアップロード（Image Upload）]** ウィンドウでアップロードした画像に基づいて入力されます。[リリース（Release）] ドロップダウンリストのオプションは、選択したプラットフォームに基づいて自動的に入力されます。
リリース	[リリース（Release）] ドロップダウンリストから NX-OS バージョンを選択します。**[パッケージ名（Package Name）]** のオプションは、選択したリリースに基づいて自動的に入力されます。
パッケージ名	（オプション）パッケージを選択します。
[ポリシーの説明（Policy Description）]	（任意）ポリシーの説明を入力します。

b) **包括的な**ポリシー タイプを選択すると、**[画像管理ポリシーの作成（Create Image Management Policy）]** ダイアログ ボックスに次のフィールドが表示されます。

フィールド	アクション
ポリシー名	ポリシー名を入力します。
プラットフォーム ポリシー	この包括的なポリシーの下にあるプラットフォーム ポリシーを選択します。プラットフォームごとに 1 つのポリシーのみを選択します。
[ポリシーの説明（Policy Description）]	（任意）ポリシーの説明を入力します。

ステップ 5 [OK] をクリックします。

確認ウィンドウが表示されます。

What to do next

デバイスにポリシーをアタッチします。詳細については、デバイスへのイメージ管理ポリシーのアタッチ, on page 515セクションを参照してください。

デバイスへのイメージ管理ポリシーのアタッチ

Cisco DCNM Web UI から画像管理ポリシーをアタッチするには、次の手順を実行します。

Before you begin

[画像管理ポリシー（Image Management Policies）] ウィンドウで、ポリシーをアタッチするスイッチ プラットフォームの画像管理ポリシーを作成します。詳細については、画像管理ポリシーの追加, on page 514を参照してください。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 ファブリックを選択します。

ファブリック トポロジ ウィンドウが表示されます。

ステップ 3 **[アクション（Actions）]** ペインで **[表形式ビュー（Tabular view）]** をクリックします。

ステップ 4 **[スイッチ（Switches）]** タブで、画像管理ポリシーをアタッチするスイッチを選択します。

ステップ 5 **[画像管理ポリシー（Image Management Policies）]** アイコンをクリックします。

[ポリシーをデバイスにアタッチする（Attach Policy to Device）] ダイアログ ボックスが表示されます。このダイアログ ボックスには、選択したスイッチの IP アドレス、スイッチ名、シリアル番号、およびポリシー名が表示されます。

ステップ 6 イメージ管理ポリシーを適用するスイッチを選択します。

ステップ 7 [追加（Add）] アイコンをクリックします。

選択したプラットフォームに対してポリシーが作成されていない場合は、警告が表示されます。

ステップ 8 **[ポリシーの選択（Selec Policy）]** ドロップダウン リストからポリシーを選択します。

[画像管理ポリシー（Image Management Policies）] ウィンドウにリストされている、選択したスイッチと互換性のあるすべてのプラットフォーム ポリシーと包括的なポリシーが、ドロップダウン リストに表示されます。選択したポリシーに、選択したスイッチのプラットフォームに関連する情報が含まれていることを確認してください。デフォルト以外の VDC にはポリシーを適用しないでください。

ステップ 9 [OK] をクリックします。

[ポリシーをデバイスにアタッチする（Attach Policy to Device）] ダイアログ ボックスで、スイッチのポリシー名が更新されます。

ステップ 10 (Optional) ファブリック トポロジ ウィンドウに移動します。

ステップ 11 (Optional) **[アクション（Actions）]** ペインで **[ファブリックの再同期（Re-sync Fabric）]** をクリックします。

または、スケジュールされた CC チェックを待って、目的の NX-OS 画像、RPM、または SMU がスイッチにインストールされているかどうかを確認できます。

ステップ 12 (Optional) 保留中のエラーを確認し、**[解決（Resolve）]** をクリックして解決します。

スイッチからポリシーを削除するには、上記の手順に従って*[ステップ 6（Step 6）]* まで実行し、**[ステップ 7（Step 7）]** で *[*削除（*Delete*）*]* アイコンをクリックします。

画像管理ポリシーの削除

Cisco DCNM Web UI から画像管理ポリシーを削除するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [画像管理（Image Management）] > [画像管理ポリシー（Image Management Policies）]** の順に選択します。

[ポリシー（Policies）] ウィンドウが表示されます。

ステップ 2 **削除**アイコンをクリックします。

確認用のダイアログボックスが表示されます。

Note
- 包括的なポリシーで使用されているプラットフォーム ポリシーは削除できません。このようなプラットフォーム ポリシーを削除する前に、包括的なポリシーを削除してください。
- 使用中のポリシーは削除できません。削除する前にデバイスからポリシーを切断します。

ステップ 3 **[OK]**をクリックします。

エンドポイント ロケータ

エンドポイントロケータ（EPL）機能により、データセンター内のエンドポイントをリアルタイムで追跡できます。追跡には、エンドポイントのネットワーク ライフ履歴のトレースと、エンドポイントの追加、削除、移動などに関連する傾向へのインサイトの取得が含まれます。

エンドポイント ロケータに関する情報は、単一のランディング ページまたはダッシュボードに表示されます。ダッシュボードには、すべてのアクティブなエンドポイントに関するデータがほぼリアルタイムで（30秒ごとに更新されて）1つのペインに表示されます。このランディング ページに表示されるデータは、**[範囲（Scope）]** ドロップダウン リストで選択した範囲によって異なります。

- エンドポイント ロケータ
- エンドポイント ロケータの監視 （691 ページ）

ThousandEyes Enterprise Agent

ThousandEyes は Network Intelligence SaaS プラットフォームであり、これによりユーザはグローバルの監視ポイントを使用して、DNS 解決、ブラウザの応答特性、ネットワーク パスと接続の詳細なアスペクト、ネットワーク ルーティングのステータス、VoIP ストリーミング接続の品質を監視するための様々なテストを実行することができます。

モニタ対象のネットワーク内でユーザが特定のウェブサイトにアクセスするとき、ThousandEyes Enterprise Agent はネットワークとアプリケーション レイヤのパフォーマンス データを収集します。テストの実行、ネットワーク パスと接続の詳細なアスペクトのチェック、ネットワーク ルーティングのステータス チェック、インテント、実行構成などの変更のモニタを行うために、データは使用されます。

Cisco DCNM リリース 11.5(3) 以降、ThousandEyes Enterprise Agent は Cisco DCNM と統合されています。

Cisco DCNM **[Web UI]** > **[制御（Control）]** > **[ThousandEyes]** > **[構成（Configure）]** を使用して、ThousandEyes Enterprise Agent のグローバル設定を構成できます。

Cisco DCNM での ThousandEyes Enterprise Agent のグローバル設定の構成

DCNM のスイッチで ThousandEyes Enterprise Agent アクションを実行するには、最初に Cisco DCNM で ThousandEyes Enterprise Agent のグローバル設定を構成する必要があります。

ThousandEyes ポータルからアカウント グループ トークンを取得したことを確認します。

管理者の資格情報を使用して ThousandEyes ポータルにログインします。**[Cloud & Enterprise Agents]** > **[エージェント設定（Agent Settings）]** に移動し、関連するエージェント名を選択して **[新規 Enterprise Agent の追加（Add New Enterprise Agent）]** をクリックし、**[アカウント グループ トークン（Account Group Token）]** フィールドからトークンをコピーします。

ThousandEyes Enterprise Agent は、DCNM のすべてのファブリックでサポートされています。グローバル設定ですべてのファブリックに対して ThousandEyes Enterprise Agent を構成し、新しいファブリックを作成するときに個々のファブリックに対しても構成できます。個々のファブリックを構成すると、グローバル設定が上書きされ、選択したファブリックに適用されます。選択したファブリックに ThousandEyes Enterprise Agent を構成する前に、グローバル設定が構成されていることを確認してください。

Procedure

ステップ 1 **[制御（Control）]** > **[ThousandEyes]** > **[構成（Configure）]** を選択します。

[ThousandEyes 構成（ThousandEyes Configuration）] ウィンドウが表示されます。

ステップ 2 **[ThousandEyes エージェントのインストールを有効にする（Enable ThousandEyes Agent Installation）]** チェック ボックスをオンにして、すべてのフィールドを有効にします。

ステップ 3 次のフィールドには適切なデータを入力します。

- **ThousandEyes アカウント グループ トークン**：インストール用の ThousandEyes Enterprise Agent アカウント グループ トークンを入力します。**[ThousandEyes エージェント設定（ThousandEyes Agent Settings）]** をクリックして、ThousandEyes ポータルにログインします。
- **ThousandEyes Agent Collector Reachability のスイッチ上の VRF**：インターネットの到達可能性を提供する VRF データを入力します。
- **DNS ドメイン**：スイッチの DNS ドメイン構成を入力します。
- **DNS サーバ IP**： Domain Name System（DNS）サーバの IP アドレス（v4/v6）のコンマ区切りリストを入力します。DNS サーバには、最大 3 つの IP アドレスを入力できます。
- **NTP サーバ IP**： Network Time Protocol (NTP) サーバの IP アドレス（v4/v6）のコンマ区切りリストを入力します。NTP サーバには、最大 3 つの IP アドレスを入力できます。
- **プロキシを有効にする**：チェックボックスをオンにして、NX-OS スイッチのインターネット アクセスのプロキシ設定を有効にします。
- **プロキシ情報**：プロキシ サーバのポート情報を入力します。
- **プロキシ バイパス**：プロキシをバイパスするサーバ リストを入力します。

ステップ 4 [保存（Save）] をクリックします。

ThousandEyes Enterprise Agent をインストールする前に、サポートされているスイッチのポリシーを追加するには、「TCAM および CoPP ポリシーの構成」セクションの手順を参照してください。

スイッチで ThousandEyes Enterprise エージェントの操作を実行するには、「ThousandEyes Enterprise エージェント アクションの実行」セクションの手順を参照してください。

レイヤ 4 ～ レイヤ 7 サービス

Cisco DCNM リリース 11.3(1) は、レイヤ 4～レイヤ 7 （L4～L7）サービス デバイスをデータセンター ファブリックに挿入する機能を展開し、これらのサービス デバイスにトラフィックを選択的にリダイレクトすることもできます。サービス ノードを追加し、サービス ノードとサービス リーフ スイッチの間にルート ピアリングを作成し、これらのサービス ノードにトラフィックを選択的にリダイレクトできます。

Cisco Web UI で、**[制御（Control）] > [サービス（Services）]** を選択します。サービス ノードの構成については、レイヤ 4 ～ レイヤ 7 サービス, on page 1013 を参照してください。

クロス サイト スクリプティング（XSS）脅威および緩和

クロスサイト スクリプティング（XSS）攻撃は、インジェクションの一種です。悪意のあるスクリプトが、安全で信頼されている Web サイトに投入されます。XSS 攻撃は、攻撃者が Web アプリケーションを使用して悪意のあるコードを送信すると発生します。悪意のあるコードは、ブラウザ スクリプトの形式で別のエンドユーザーに送信されます。

攻撃者はXSSを使用して、疑いを持たないユーザーに悪意のあるスクリプトを送信できます。ブラウザは、スクリプトが信頼されるべきではないことを認識できず、スクリプトを実行します。ブラウザはスクリプトが信頼できる送信元からのものであると考えるため、悪意のあるスクリプトは、ブラウザが保持し、そのサイトで使用されるCookie、セッショントークン、またはその他の機密情報にアクセスできます。

XSS 攻撃は、DCNM へのアクセスが確立されたときに発生します。システムにアクセスし、悪意のある文字列をデータとして DCNM に投入できる承認が与えられたことにより、このブラウザ上の疑いを持たないユーザーによって読み取り可能となりました。そのため、悪意のあるコードが実行されます。 OWASP XSS チートシート は、XSS を引き起こす可能性のある特殊文字の完全なリストを提供します。

クロスサイトスクリプト（XSS）の脅威、およびポリシーフィールドでの特殊文字の取り扱い

さまざまなポリシーフィールドでは、従来、特殊文字を含む文字列を含む値が使用されてきました。

例

```
Port mode = “40G+10G”
Shared secret = <A password having many special characters>
Description = “NYC & SFO, >100G”
```

（注） 「説明」など、一部のフィールドには特殊文字が含まれていない場合があります。「ポート モード」や「共有秘密」などの他のフィールドには、NXOS CLI コマンド形式に関連付けられているか、システムのインターワーキングに必要なため、特殊文字が必要です。

DCNM 11.5(1) での処理

DCNM リリース 11.5(1) は、OWASP ガイドラインに基づいて特殊文字のポリシー関連フィールド コンテンツをサニタイズ（無害化）し、クロス サイト スクリプティング（XSS）攻撃を回避します。ポリシー テンプレート変数の値は、XSS 文字の特別なセットについてスキャンされ、エラーとして報告されます。一部の特殊文字はポリシーで必要になるため、NXOS 要件に従って、DCNM リリース 11.5(2) は特殊文字を許可するメカニズムを提供します。

次の図は、典型的なエラー メッセージを示しています。

DCNM 11.5(2) での処理

Cisco DCNM リリース 11.5(2) には、サニタイズ動作を制御するサーバー プロパティ **ef.sanitize.state** が用意されています。次のキーワードは、機能を説明します。

- **Strict**—OWASP ガイドラインに従って、XSS 脅威文字のコンテンツをサニタイズします。

  これは、例外がないことを意味します。**@ & + \ + % = < >** などの特殊文字はすべて、XSS エラーの原因になります。

- **Default** — 削減された文字セットのコンテンツをサニタイズします。

  使用可能な文字は次のとおりです。**@ % & \ + ‘ = .**

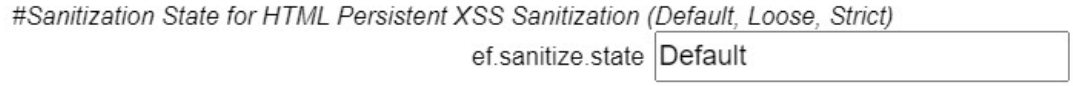
  ただし、これにより、**$** または **< >** のプレフィックス付きの許可された文字がサニタイズされます。

  例：**$@** または **<>@** は許可されていません。ただし、**@** は使用できます。

- **Loose** — サニタイズを完全に無効にします。

Cisco DCNM Web UI でサーバー プロパティをアップデートするには、**[管理（Administration）]** > **[サーバー プロパティ（Server Properties]** を選択します。

このサーバー プロパティのデフォルト値は **Default** です。



Strict モードは、XSS の脆弱なデータが Cisco DCNM に保存されるのを防ぐため、XSS に対する効率的な防御を提供します。ただし、従来のテンプレートが使用されている実用的な理由や、特殊文字の使用が義務付けられている NXOS CLI コマンドの場合は、次のメカニズムのいずれかを使用します。

- 特殊文字を許可するには、次の手順を使用してプロパティ値を **Loose** に設定します。ただし、これにより XSS の脅威が増加します。この場合、次の点に注意してください。
  - データセンター VPN 内など、安全なマシンを使用して DCNM にアクセスできます。これにより、悪意のあるユーザが DCNM に簡単に到達することがなくなります。

- これらの操作には管理者権限が必要なため、**admin** ロールを持つユーザはパスワードのセキュアな管理に取り組みます。

- **[テンプレート コンテンツ（Template Content）]**に XSS の安全でないコンテンツを直接含むカスタム ポリシー テンプレートを作成し、これらのポリシーをスイッチに展開します。

例

以下の CLI を GUI **switch_freeform** ポリシーに追加すると、XSS 脅威緩和の実施により、ポリシーを保存するとエラーが発生します。

```
ip as-path access-list ORIGIN-ACL seq 10 permit "^$"
```

XSS 脅威を軽減するには、次のいずれかを実行します。

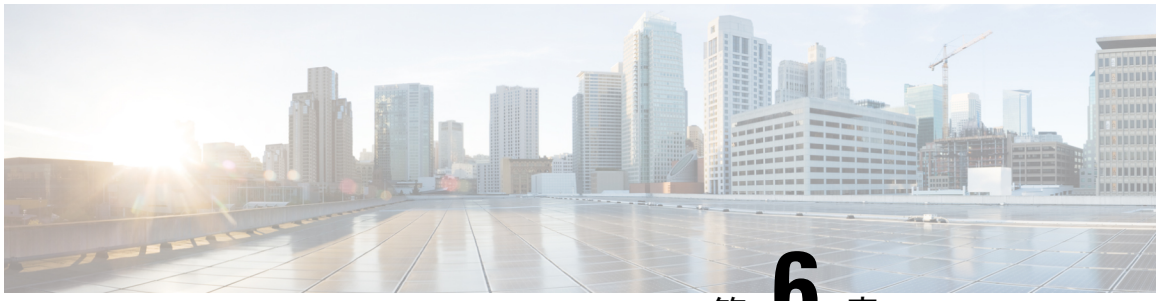
- カスタム テンプレートを作成します。手順については、「テンプレートの追加 （487 ページ）.

  次の例は、サンプルのカスタム テンプレートを示しています。

```
##template properties
name =ip_as_path;
description = IP AS Path Custom Template;
tags = ;
userDefined = true;
supportedPlatforms = All;
templateType = POLICY;
templateSubType = DEVICE;
contentType = TEMPLATE_CLI;
implements = ;
dependencies = ;
published = false;
imports = ;
##
##template variables
##

##template content
ip as-path access-list ORIGIN-ACL seq 10 permit "^$"
##
```

- [ポリシーの表示/編集（View/Edit Policies）] から、スイッチにこのテンプレートを使用してポリシーを追加します。

- 新しいポリシーをスイッチに展開します。



第 6 章

モニター

この章は次のトピックで構成されています。

インベントリ

この章は次のトピックで構成されています。

スイッチのインベントリ情報の表示

Cisco DCNM Web UI のスイッチ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 **[モニタ（Monitor）] > [インベントリ（Inventory）] > [スイッチ（Switches）]** を選択します。

[スイッチ（Switches）] ウィンドウが選択した [範囲（Scope）] のすべてのスイッチのリストとともに表示されます。

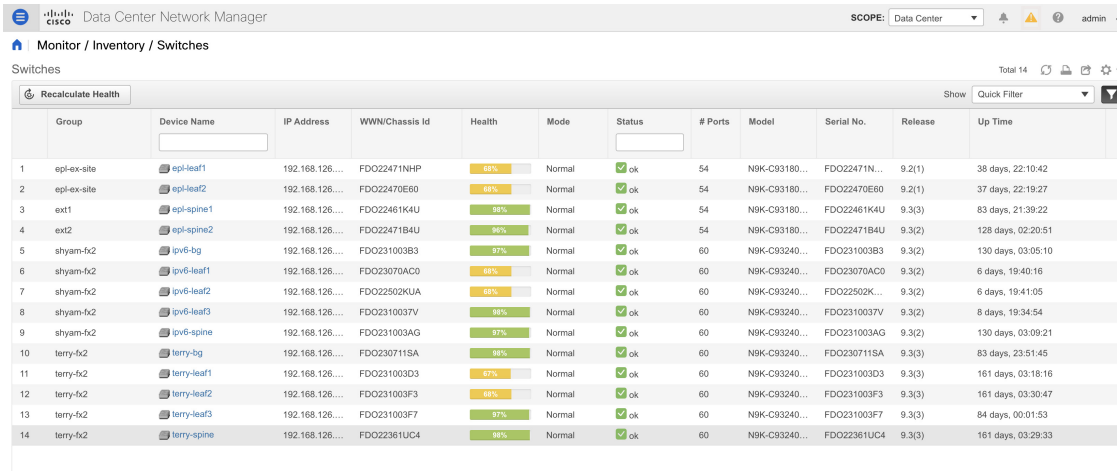
ステップ 2 次の情報が表示されます。

- **[グループ（Group）]** 列には、スイッチが属するスイッチ グループが表示されます。
- **[デバイス名（Device Name）]** 列でスイッチを選択して、スイッチ ダッシュボードを表示します。
- **[IP アドレス]** 列にはスイッチの IP アドレスを表示します。
- **[WWN/シャーシ ID（WWN/Chassis ID）]** には、ワールドワイド名（WWN）がある場合、またはシャーシ ID が表示されます。

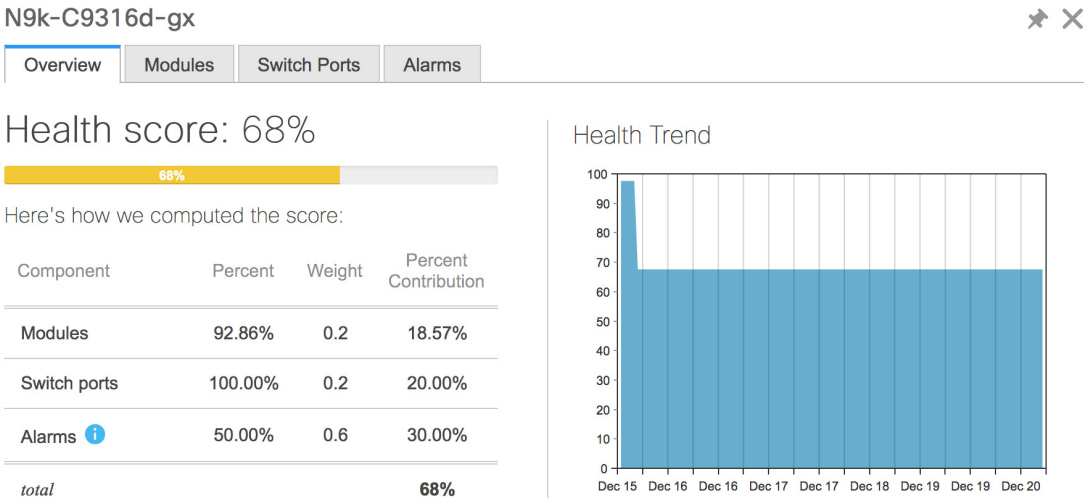
- **[ヘルス（Health）]** には、スイッチの正常性の状況が表示されます。

  Note Cisco DCNM 上のすべてのスイッチの最新のヘルス データを更新して再計算するには、スイッチ テーブルの上にある **[ヘルスの再計算（Recalculate Health）]** ボタンをクリックします。

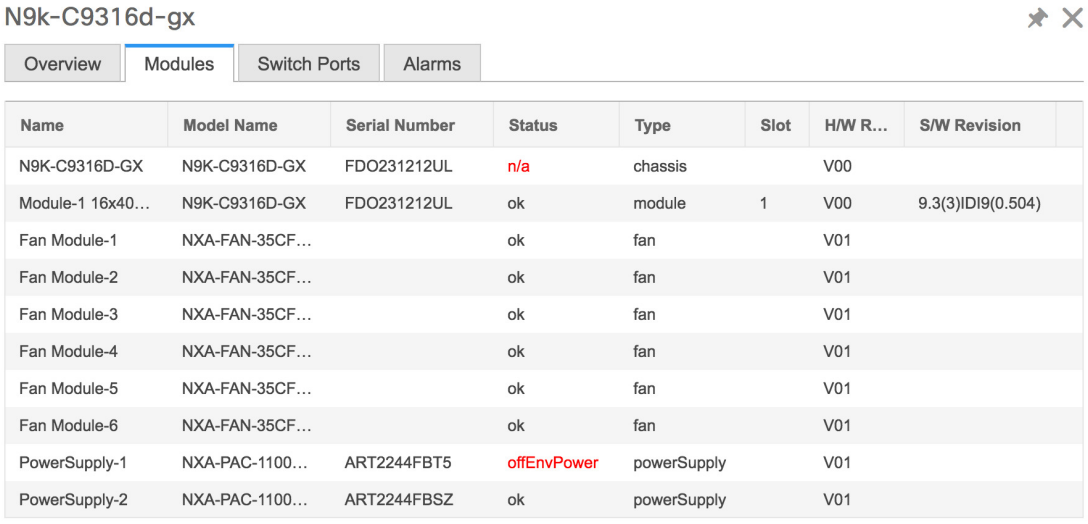
- **[モード]**列には、スイッチの現在のモードを指定します。スイッチは、**通常**、**メンテナンス**、または**移行**モードにすることができます。
- **[ステータス（Status）]** 列には、スイッチのステータスが表示されます。
- **[# ポート（#Ports）]** 列には、ポートの数が表示されます。
- **[モデル（Model）]** 列には、スイッチのモデル名が表示されます。
- **[シリアル番号（Serial No.）]** 列には、スイッチのシリアル番号を表示します。
- **[リリース（Release）]** 列には、スイッチのバージョンが表示されます。
- **[稼働時間（Up Time）]**列には、スイッチがアクティブになっている時間が表示されます。



ステップ 3 **[ヘルス（Health）]** をクリックして、デバイスの [正常性スコア（Health）] ウィンドウにアクセスします。[ヘルス スコア（Health score）] ウィンドウには、ヘルス スコアの計算とヘルス トレンドが含まれています。[概要（Overview）] タブには、全体的なヘルス スコアが表示されます。ヘルス スコアの計算時には、すべてのモジュール、スイッチ ポート、およびアラームが考慮されます。特定の日付の詳細情報については、[ヘルス トレンド（Health Trend ）] の下のグラフにカーソルを合わせます。[アラーム（Health score）] の横にある情報アイコンにカーソルを合わせると、生成された重大、メジャー、マイナー、および警告のアラームの数が表示されます。

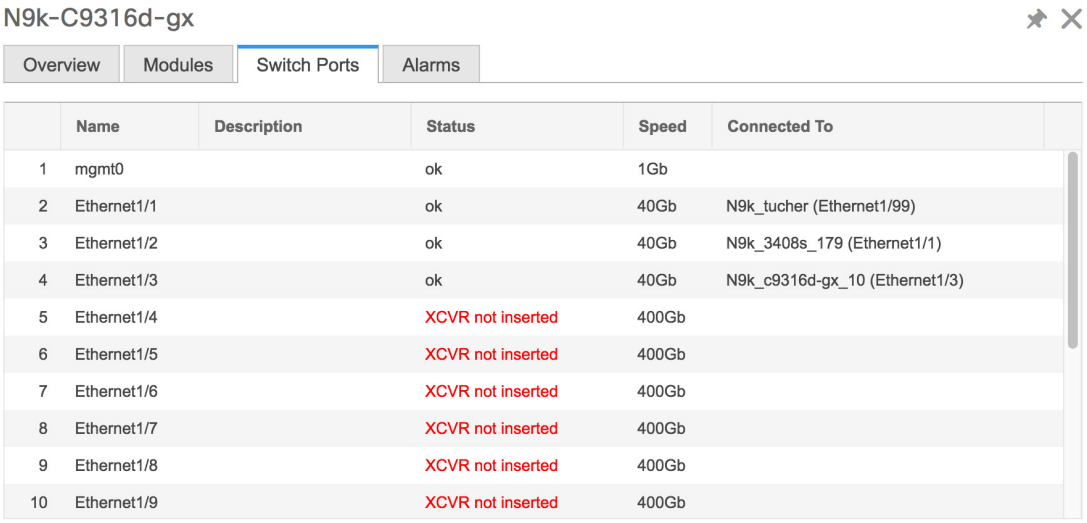


[モジュール]タブをクリックして、デバイスのさまざまなモジュールに関する情報を表示します。このタブには、名前、モデル名、シリアル番号、ステータス、タイプ、スロット、ハードウェア リビジョン、ソフトウェア リビジョンなどの情報が表示されます。

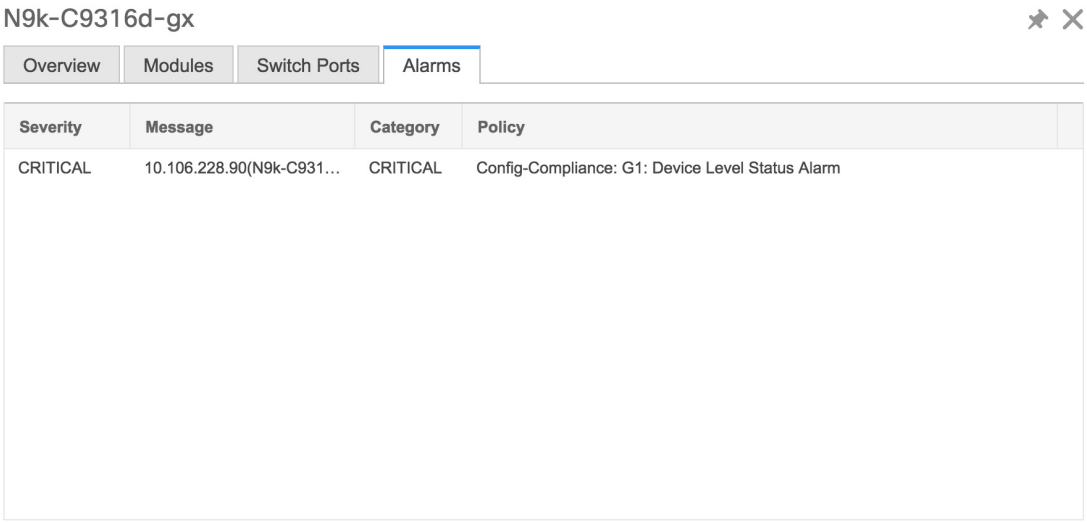


Name	Model Name	Serial Number	Status	Type	Slot	H/W R...	S/W Revision
N9K-C9316D-GX	N9K-C9316D-GX	FDO231212UL	n/a	chassis		V00	
Module-1 16x40...	N9K-C9316D-GX	FDO231212UL	ok	module	1	V00	9.3(3)IDI9(0.504)
Fan Module-1	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-2	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-3	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-4	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-5	NXA-FAN-35CF...		ok	fan		V01	
Fan Module-6	NXA-FAN-35CF...		ok	fan		V01	
PowerSupply-1	NXA-PAC-1100...	ART2244FBT5	offEnvPower	powerSupply		V01	
PowerSupply-2	NXA-PAC-1100...	ART2244FBSZ	ok	powerSupply		V01	

[スイッチ ポート] タブをクリックして、デバイス ポートに関する情報を表示します。このタブには、名前、説明、ステータス、速度、ポートが接続されているデバイスなどの情報が表示されます。



[アラーム]タブをクリックして、生成されたアラームに関する情報を表示します。このタブには、アラームの重大度、メッセージ、カテゴリ、およびアラームが生成されたためにアクティブ化されたポリシーなどの情報が表示されます。



[ヘルス]列では、スイッチのヘルスは、次のパラメーターに基づいてキャパシティマネージャーによって計算されます。

- モジュールの合計数
- 警告の影響を受けたモジュールの総数
- スイッチ ポートの合計数
- 警告の影響を受けたスイッチ ポートの総数

- シビラティがクリティカルのアラームの総数
- シビラティが警告のアラームの総数
- 重大度の重大なアラームの総数
- 重大度が小さいアラームの総数

ステップ 4 **[ヘルス]** 列の値は、以下に基づいて計算されます。

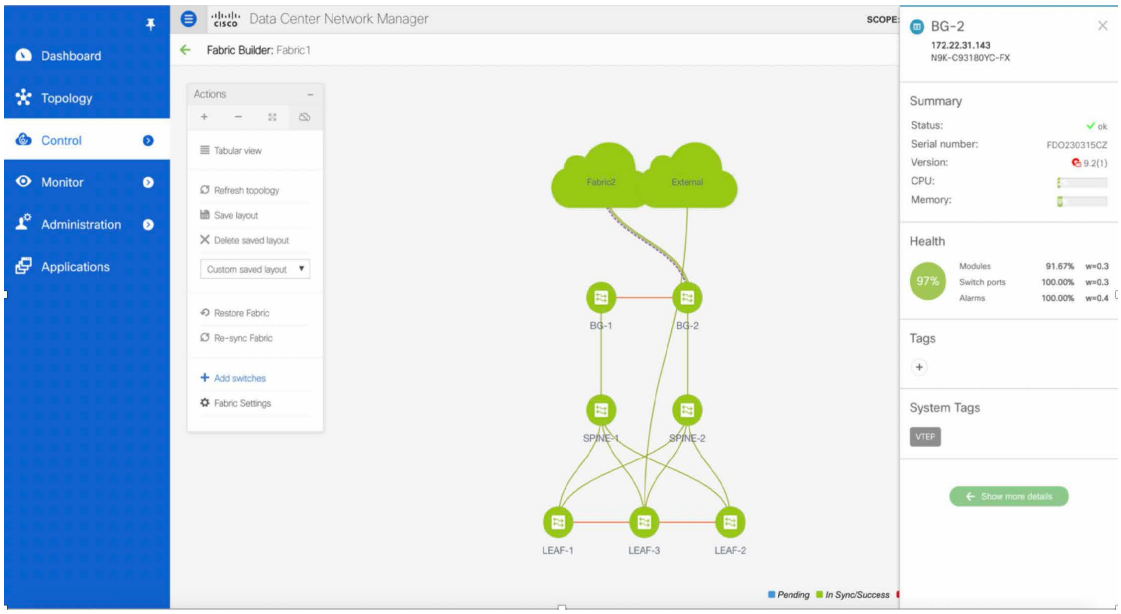
- 警告の影響を受けるモジュールの割合（正常性全体の 20% に寄与）。
- 警告の影響を受けるポートの割合（正常性全体の 20% に影響します）。
- アラームのパーセンテージ（正常性全体の 60% に影響します）。このパーセンテージの最大値を占めるのはクリティカル アラームで、次にメジャー アラーム、マイナー アラーム、および警告アラームが続きます。

共通インターフェイス クラス com.cisco.dcbu.sm.common.rif.HealthCalculatorRif を実装して、独自の正常性計算式を持つこともできます。

デフォルトの Java クラスは health.calculator=com.cisco.dcbu.sm.common.util.HealthCalculatorAlarms として定義されています。

- Capacity Manager は、ライセンス スイッチのヘルスのみを計算します。正常性カラムに値が表示されない場合は、スイッチにライセンスがないか、キャパシティ マネージャの毎日のサイクルを実行できていません。
- スイッチにライセンスがない場合は、[DCNM License] 列で [Unlicensed] をクリックします。[管理] > [ライセンス] ウィンドウが表示され、ユーザーにライセンスを割り当てることができます。
- キャパシティ マネージャは、DCNM サーバが起動してから 2 時間後に実行されます。したがって、DCNM 開始時刻の 2 時間後にデバイスを検出した場合、正常性はこの DCNM 開始時刻の 24 時間後に計算されます。

Cisco DCNM 11.3(1) リリース以降では、**[トポロジ（Topology）]** ウィンドウでスイッチをクリックするか、**[制御（Control）]>[ファブリック（Fabrics）]>[ファブリック ビルダー（Fabric Builder）]** を選択し、ファブリックを選択してから**ファブリック ビルダー** ウィンドウのスイッチをクリックすることにより、スイッチの概要とともにスイッチの状態に関する情報を表示できます。



システム情報の表示

スイッチのダッシュボードには、選択したスイッチの詳細が表示されます。

Procedure

ステップ 1 Cisco DCNM ホームページから、**[モニタ（Monitor）]>[インベントリ（Inventory）]>[スイッチ（Switches）]** を選択します。

Cisco DCNM Web UI によって検出されたすべてのスイッチのインベントリが表示されます。

ステップ 2 **[デバイス名（Device Name）]** 列のスイッチをクリックします。

そのスイッチに対応する **[スイッチ（Switch）]** ダッシュボードが、次の情報とともに表示されます。

ステップ 3 **[システム情報（System Info）]** タブをクリックします。このタブには、グループ名、ヘルス、モジュール、システムが稼働している時間、シリアル番号、バージョン番号、連絡先、場所、DCNM ライセンス、ステータス、システム ログ送信ステータス、CPU とメモリの使用率、VTEP IP などの詳細なシステム情報が表示されます。アドレスが表示されます。**[正常性]** をクリックして、正常性スコアの計算と正常性トレンドを含む[正常性スコア]画面にアクセスします。 ポップアップには、概要、モジュール、スイッチ ポート、イベント タブが含まれています。

- （オプション）**SSH** をクリックして、Secure Shell（SSH）を介してスイッチにアクセスします。

- （オプション）**[Show Commands]** をクリックして、デバイスの show コマンドを表示します。Device Show Commands ページでは、コマンドを表示して実行できます。

ホスト

スイッチのホストの詳細を表示できます。

[ホスト（Hosts）] タブを表示するには、**[モニタ（Monitor）] > [インベントリ（Inventory）] > [スイッチ（Switches）]** を選択し、**[Device Name（デバイス名）]** 列でスイッチ名をクリックして、**[Hosts（ホスト）]** タブに移動します。

次の表に、表示されたフィールドの説明を示します。

表 *8*：ホスト タブ

フィールド	説明
VRF	スイッチの VRF 詳細を表示します。
ホスト IP	スイッチのホスト IP アドレスを表示します。
ホストのMACアドレス	スイッチのホスト MAC アドレスを表示します。
VLAN	スイッチに構成された VLAN を表示します。
ポート	
L2 VNI	スイッチに構成されているレイヤ 2 VXLAN ネットワーク識別子（L2 VNI）を表示します。
L3 VNI	スイッチに設定されているレイヤ 3 VXLAN ネットワーク識別子（L3 VNI）を表示します。

容量（Capacity）

スイッチの物理容量を表示できます。

[キャパシティ（Capacity）] タブには、スイッチに存在する物理ポートに関する情報が表示されます。

[キャパシティ（Capacity）] タブを表示するには、**[モニタ（Monitor）] > [インベントリ（Inventory）] > [スイッチ（Switches）]** を選択し、**[デバイス名（Device Name）]** 列でスイッチ名をクリックして、**[キャパシティ（Capacity）]** タブに移動します。

次の表に、表示されたフィールドの説明を示します。

表 *9*: 容量タブ

フィールド	説明
階層	スイッチで使用可能な物理ポートを表示します。
使用済みポート	スイッチの使用ポート数を表示します。
合計ポート数	スイッチのポート数を表示します。
残り日数	残りの合計日数を表示します。

機能

スイッチで有効になっている機能を表示できます。

[機能（Features）] タブを表示するには、**[モニタ（Monitor）] > [インベントリ（Inventory）] > [スイッチ（Switches）]** を選択し、**[デバイス名（Device Name）]** 列のスイッチ名をクリックし、**[機能（Features）]** タブに移動します。

VXLAN

VXLAN タブで、VXLAN とその詳細を表示できます。

VXLAN を表示するには、**[モニタ（Monitor)] > [インベントリ（Inventory）] > [表示（View）] > [スイッチ（Switches）]** を選択し、**[デバイス名（Device Name）]** 列でスイッチ名をクリックします。

次の表に、表示されたフィールドの説明を示します。

表 *10* : *VXLAN* タブ

フィールド	説明
VNI	スイッチに設定されているレイヤ 2 (ネットワーク) またはレイヤ 3 (VRF) VXLAN VNI を表示します。
マルチキャスト アドレス。	該当する場合、レイヤ 2 VNI に関連付けられているマルチキャストアドレスを表示します。
VNI ステータス	VNI のステータスを表示します。
モード	VNIモードを表示します。コントロールプレーンまたはデータ プレーン。
タイプ	VXLAN VNI がネットワーク (レイヤー 2) または VRF (レイヤー 3) に関連付けられているかどうかを表示します。

フィールド	説明
VRF	レイヤ 3 VNI の場合、VXLAN VNI に関連付けられている VRF 名を表示します。
マッピングされた VLAN	VNI にマッピングされている VLAN またはブリッジ ドメインを表示します。

VLAN

[VLAN] タブで、VLAN とその詳細を表示できます。

VLAN を表示するには、**[モニタ（Monitor)] > [インベントリ（Inventory）] > [表示（View）] > [スイッチ（Switches）]** を選択し、**[デバイス名（Device Name）]** 列でスイッチ名をクリックします。

次のテーブルでは、表示されるフィールドについて説明します。

表 11 : [VLAN] タブ

フィールド	説明
VLAN	スイッチに構成した VLAN を表示します。
Name	VLAN の名前を表示します。
タイプ	ネットワークに関連付けられている VLAN が表示されます。
ポリシー	関連付けられたポリシーの名前を表示します。ポリシーが関連付けられていない場合、デフォルトでは未定義です。
モード	VLAN モードを表示します。
Status	VLAN のステータスを表示します。
ポート	VLAN がスイッチに物理的に接続されているポート番号を指定します。

スイッチ モジュール

[モジュール（Modules）] タブで、スイッチ モジュールとその詳細を表示できます。

To view the **[モジュール（Modules）]** タブを表示するには、**[モニタ（Monitor）] > [インベントリ（Inventory）] > [スイッチ（Switches）]** を選択し、**[デバイス名（Device Name）]** 列のスイッチ名をクリックし、**[モジュール（Modules）]** タブに移動します。

次の表に、表示されたフィールドの説明を示します。

表 *12 :* モジュール タブ

フィールド	説明
名前	モジュールの名前を指定します。
ModelName	モジュールのモデル名を指定します。
SerialNum	モジュールのシリアル番号を指定します。
タイプ	モジュール タイプを指定します。有効な値は、**[シャーシ（chassis）]**、**[モジュール（module）]**、**[ファン（fan）]**、および **powerSupply** です。
OperStatus	モジュールの操作ステータスを指定します。
スロット	モジュールのスロット番号を指定します。
H/W 改定	NX-OS ハードウェア バージョンを指定します。
S/W 改訂	NX-OS ソフトウェア バージョンを指定します。
AssetID	モジュールのアセット ID を指定します。
IO FPGA	IO フィールド プログラマブル ゲート アレイ (FPGA) バージョンを指定します。
MI FPGA	MI フィールド プログラマブル ゲート アレイ（FPGA）のバージョンを指定します。

FEX

ファブリック エクステンダ機能を使用すると、Cisco Nexus 2000 シリーズ ファブリック エクステンダと、それが接続されている Cisco NX-OS スイッチとの関連付けを管理できます。ファブリックエクステンダは、物理イーサネットインターフェイスまたはポートチャネルを介してスイッチに接続されます。ファブリックエクステンダは、デフォルトでは、シャーシ ID を割り当てるか、接続するインターフェイスに関連付けるまで、スイッチに接続できません。ファブリック エクステンダのホスト インターフェイス ポートをルーテッド ポートまたはレイヤ 3 ポートとして構成できます。ただし、このルーテッド インターフェイスにルーティング プロトコルを関連付けることはできません。

（注） FEX 機能は LAN デバイスでのみ使用できます。したがって、Cisco DCNM **[インベントリ スイッチ（Inventory Switches）]**に FEX が表示されます。FEX は、Cisco Nexus 1000V デバイスでもサポートされていません。

（注） FEX 接続の 4x10G ブレークアウトは、Cisco Nexus 9500 スイッチではサポートされていません。

（注） ファブリックエクステンダは、いくつか個別の物理イーサネット インターフェイスまたは最大 1 つのポートチャネル インターフェイスを通して、スイッチに接続可能です。

このセクションでは、Cisco DCNM を介して Cisco Nexus スイッチで Fabric Extender（FEX; ファブリックエクステンダ）を管理する方法について説明します。

Cisco DCNM **[インベントリ（Inventory）] > [スイッチ（Switches）]** から FEX を作成および管理できます。

（注） [FEX] タブは、LAN デバイスを選択した場合にのみ表示されます。

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 *13 : FEX*動作

フィールド	説明
表示する	選択した FEX ID のさまざまな構成の詳細を表示できます。ドロップダウンリストから以下を選択できます。 • show_diagnostic • show_fex • show_fex_detail • show_fex_fabric • show_fex_inventory • show_fex_module それぞれの show コマンドの変数は、[変数（Variables）] エリアに表示されます。変数を確認し、**[実行（Execute）]** をクリックします。出力は **[出力（Output）]** エリアに表示されます。 FEX の表示テンプレートを作成できます。テンプレート タイプとして [SHOW] を選択し、サブ タイプとして [FEX] を選択します。

表 *14 : FEX* フィールドと説明

フィールド	説明
FEX ID	Cisco NX-OS デバイスに接続されているファブリックエクステンダを一意に識別します。
FEX の説明	ファブリックエクステンダ用に構成された説明。

フィールド	説明
FEX バージョン	スイッチに関連付けられている FEX のバージョンを指定します。
ピン接続	一度にアクティブである、ファブリックエクステンダの最大ピン接続アップリンク数を表す整数値です。
州	Cisco Nexus スイッチに関連付けられた FEX のステータスを指定します。
モデル	FEX のモデルを指定します。
通番	構成されたシリアル番号を指定します。 （注） この構成済みシリアル番号とファブリックエクステンダの実際のシリアル番号が同じでない場合、ファブリックエクステンダはアクティブになりません。
ポート チャネル	FEXがスイッチに物理的に接続されているポートチャネル番号を指定します。
イーサネット	FEX が接続されている物理インターフェイスを指します。
vPC ID	FEX 用に構成された vPC ID を指定します。

VDC

このセクションでは、Cisco DCNM を介して Cisco Nexus 7000 スイッチで仮想デバイス コンテキスト (VDC) を管理する方法について説明します。

ネットワーク管理者（network-admin）ロールに指定されたユーザーは、仮想デバイスコンテキスト（VDC）を作成できます。VDC リソーステンプレートは、VDC が使用可能な物理デバイスの量を制限します。Cisco NX-OS ソフトウェアはデフォルトのリソーステンプレートを提供します。また、ユーザはリソース テンプレートを作成できます。

Cisco DCNMで **[インベントリ（Inventory）] > [スイッチ（Switches）] > [VDC]** から VDC を作成および管理できます。Cisco DCNM は Cisco Nexus 7000 シリーズでのみ DCNM をサポートするため、アクティブな Cisco Nexus 7000 スイッチをクリックします。VDC の作成後は、インターフェイスの割り当て、VDC リソース制限、およびハイアベイラビリティ（HA）ポリシーを変更できます。

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。

表 *15 : VDC* オペレーション

フィールド	説明
追加（Add）	クリックして新しい vDC を追加します。

フィールド	説明
編集	アクティブな VDC ラジオ ボタンを選択し、[編集（Edit）] をクリックして VDC 構成を編集します。
削除	VDC を削除できます。アクティブな VDC ラジオ ボタンを選択し、[削除（Delete）] をクリックして、デバイスに関連付けられた VDC を削除します。
再開	中断された VDC を再開できます。
一時停止	アクティブなデフォルト以外の VDC を停止できます。 VDC を停止する前に、VDC の実行構成をスタートアップ構成に保存します。保存しなかった場合、実行コンフィギュレーションに対する変更が失われます。 （注） デフォルト VDC は停止できません。 **注意** VDC を停止すると、その VDC 上のすべてのトラフィックが中断されます。
再検出	デフォルト以外の VDC を停止状態から再開できます。VDC は、スタートアップ構成に保存された設定内容で再開します。
表示する	選択した VDC に割り当てられているインターフェイスとリソースを表示できます。 [インターフェイス（Interface）] タブでは、VDC に関連付けられている各インターフェイスのモード、管理ステータス、および動作ステータスを表示できます。 [リソース（Resource）] タブでは、リソースの割り当てとこれらのリソースの現在の使用状況を表示できます。

表 *16 : VRF* テーブルのフィールドと説明

フィールド	説明
名前	VDC の一意の名前を表示します。
タイプ	VDC のタイプを指定します。VDC には次の 2 つのタイプがあります。 • イーサネット • ストレージ
Status	VDC のステータスを指定します。

フィールド	説明
リソース制限モジュールタイプ	割り当てられたリソース制限とモジュール タイプを表示します。

フィールド	説明
HA-Policy • スーパーバイザ 1 台 • デュアル スーパーバイザ	

フィールド	説明
	回復不可能なVDC障害が発生した場合にCisco NX-OS ソフトウェアによって実行される処理を指定します。 HA ポリシーは、VDC の作成時に、シングル スーパーバイザ モジュールおよびデュアル スーパーバイザ モジュール構成に対して指定できます。HAポリシーのオプションは次のとおりです。 **シングル スーパーバイザ モジュール構成**： • 停止（Bringdown）：VDC を障害状態に移行します。障害状態から復旧するには、物理デバイスをリロードする必要があります。 • リロード（Reload）：スーパーバイザ モジュールをリロードします。 • 再起動（Restart）：VDC プロセスとインターフェイスをいったん削除し、スタートアップ コンフィギュレーションを使用して再起動します。 **デュアル スーパーバイザ モジュール構成**： • 停止（Bringdown）：VDC を障害状態に移行します。障害状態から復旧するには、物理デバイスをリロードする必要があります。 • 再起動（Restart）：VDC プロセスとインターフェイスをいったん削除し、スタートアップ コンフィギュレーションを使用して再起動します。 • スイッチオーバー（Switchover）：スーパーバイザ モジュールのスイッチオーバーを開始します。 作成した、デフォルト以外のVDCに対するデフォルトのHAポリシーは、シングルスーパーバイザ モジュール構成の場合は再起動、デュアル スーパーバイザ モジュール構成の場合はスイッチオーバーです。デフォルトVDCに対するデフォルトの HA ポリシーは、シングル スーパーバイザモジュール構成の場合はリロー

フィールド	説明
	ド、デュアル スーパーバイザ モジュール構成の場合はスイッチオーバーです。
Mac アドレス	デフォルト VDC には管理 MAC アドレスを指定します。
管理インターフェイス • IP Address Prefix • Status	VDC 管理インターフェイスの IP アドレスを指定します。ステータスは、インターフェイスがアップかダウンかを示します。
SSH	SSH ステータスを指定します。

（注） 初期構成後にネイバー デバイスの VDC ホスト名を変更しても、古い VDC ホスト名へのリンクは新しいホスト名に自動的に置き換えられません。回避策として、古い VDC ホスト名へのリンクを手動で削除することをお勧めします。

この章は、次の項で構成されています。

VDC の追加

Cisco DCNM Web UI から VDC を追加するには、次の手順を実行します。

始める前に

network-admin ロールを持つユーザ名を使用する物理デバイスが検出されたことを確認します。

VDC の帯域外管理を使用するには、管理インターフェイス（mgmt 0）用に IPv4 または IPv6 アドレスを取得します。

ストレージ VDC を作成して FCoE を実行します。ストレージ VDC をデフォルト VDC にすることはできません。デバイスには 1 つのストレージ VDC を保有できます。

手順

ステップ 1 **[インベントリ（Inventory）] > [スイッチ（Switches）] > [VDC]** を選択します。

VDC ウィンドウが表示されます。

ステップ 2 **[追加（Add）]** アイコンをクリックします。

ステップ 3 ドロップダウン リストから、VDC タイプを選択します。

VDC は 2 つのモードで構成できます。

- イーサネット VDC の構成

- ストレージ VDC の構成

デフォルトの VDC タイプは Ethernet です。

ステップ 4 [OK] をクリックします。

イーサネット VDC の構成

Cisco DCNM Web UI からイーサネット モードの VDC を構成するには、次の手順を実行します。

手順

ステップ 1 [一般パラメータ（General Parameter）] タブで、VDC **名**、**単一スーパーバイザ HA ポリシー**、**デュアル スーパーバイザ HA ポリシー**、および**リソース制限 - モジュール タイプ**を指定します。

ステップ 2 割り当てインターフェイス タブでVDC に割り当てられるネットワーク インターフェイス（専用インターフェイスのメンバーシップ）を選択します。

[次へ（Next）] をクリックします。

ステップ 3 [リソースの割り当て（Allocate Resource）] タブで、VDC のリソース制限を指定します。

ラジオ ボタンを選択し、**[既存のテンプレートからテンプレートを選択（Select a Template from existing Templates）]** または **[新しいリソース テンプレートを作成（Create a New Resource Template）]** を選択します。VDC リソース テンプレートは、VDC で使用可能な最小および最大リソースを指定します。VDC の作成時に VDC リソース テンプレートを指定しない場合は、Cisco NX-OS ソフトウェアはデフォルトのテンプレートである vdc-default を使用します。

- 既存のテンプレートからテンプレートを選択を選択した場合、**[テンプレート名（Template Name）]** ドロップダウン リストから、**[なし（None）]**、**[global-default]**、または **[vdc-default]** を選択できます。

  テンプレート リソースの制限については、以下で詳しく説明します。

表 *17:* テンプレート リソースの制限

Resource	最小	最大
グローバル デフォルト VDC テンプレート リソースの制限		
エニーキャスト同梱		
IPv6 マルチキャスト ルート メモリ	8	8 ルート メモリの単位はメガバイトです。

Resource	最小	最大
IPv4 マルチキャスト ルート メモリ	48	48
IPv6 ユニキャスト ルート メモリ	32	32
IPv4 ユニキャスト ルート メモリ		
VDC デフォルト テンプレートのリソース制限		
モニタ セッション延長		
モニタ セッション mx の例外		
SRC INBAND のモニタ		
ポート チャネル		
DST ERSPAN のモニタ		
SPAN セッション		
VLAN		
エニーキャスト同梱		
IPv6 マルチキャスト ルート メモリ		
IPv4 マルチキャスト ルート メモリ		
IPv6 ユニキャスト ルート メモリ		
IPv4 ユニキャスト ルート メモリ		
VRF		

- **[新しいリソース テンプレートを作成（Create New Resource Template）]** を選択した場合は、一意のテンプレート名を入力します。[リソース制限（Resource Limits）] エリアで、技術情報の必要に応じて、最小制限と最大制限を入力します。

[Cisco DCNM Web Client] > [Inventory] > [Switches] > [VDC] を使用して、単一の VDC の個々のリソース制限を編集できます。

[次へ（Next）] をクリックします。

ステップ 4 [認証（Authenticate）] タブでは、管理者にパスワードの設定を許可し、AAA サーバ グループを使用してユーザーを認証することもできます。

[管理ユーザー（Admin User）] 領域で：

- 必要に応じて、**[パスワード強度チェックを有効にする（Enable Password Strength Check）]** チェックボックスをオンにします。
- **[Password（パスワード）]** フィールドに管理ユーザー パスワードを入力します。
- **[Confirm Password（パスワードを確認）]** フィールドに管理ユーザー パスワードを再度入力します。
- **[有効期限日（Expiry Date）]** フィールドで下矢印キーをクリックし、有効期限日ダイアログボックスで管理ユーザの有効期限を選択します。**[期限切れにしない（Never）]** ラジオボタンを選択して、パスワードを期限切れにしないようにすることもできます。

AAA サーバ グループ エリア内：

- **[グループ名（Group Name）]** フィールドに AAA サーバ グループ名を入力します。
- **[サーバ（Servers）]** フィールドに、ホスト サーバの IPv4 または IPv6 のアドレスまたは名前を 1 つまたは複数（カンマで区切る）入力します。
- **[タイプ（Type）]** フィールドで、ドロップダウン リストから サーバ グループのタイプを選択します。

[次へ（Next）] をクリックします。

ステップ 5 マネジメント Ip タブ内で IPv4 または IPv6 のアドレス情報を入力します。

[次へ（Next）] をクリックします。

ステップ 6 [概要（Summary）] タブ内で VDC 構成を確認します。

パラメータを編集するには、**[前へ（Previous）]** をクリックします。

[展開（Deploy）] をクリックして、デバイスに VDC を設定します。

ステップ 7 [展開（Deploy）] タブに、VDC 展開のステータスが表示されます。

確認メッセージが表示されます。**[詳細情報（Know More）]** をクリックして、VDC を展開するために実行されるコマンドを表示します。

[完了（Finish）] をクリックして VDC 構成ウィザードを閉じ、デバイスに構成されている VDC のリストを表示するために戻ります。

ストレージ VDC の構成

Cisco DCNM Web UI からストレージ モードの VDC を構成するには、次の手順を実行します。

始める前に

デバイスで FCoE を実行する際には、個別のストレージ VDC を作成します。ストレージ VDC にできるのは、VDC のいずれか 1 つだけです。デフォルト VDC をストレージ VDC として設定することはできません。

イーサネット トラフィックとファイバ チャネル トラフィックの両方を伝送する共有インターフェイスを設定できます。この特定のケースでは、同じインターフェイスが複数の VDC に属します。共有インターフェイスはイーサネット VDC とストレージ VDC の両方に割り当てられます。

手順

ステップ 1 一般パラメータ タブで VDCの **[名前（Name）]** 、 **[シングル スーパーバイザ HA ポリシー（Single supervisor HA-policy）]** 、 **[デュアル スーパーバイザ HA ポリシー（Dual supervisor HA-policy）]** と **[技術情報リミットモジュール タイプ（Resouce Limit - Module Type）]**を指定します。

ステップ 2 [FCoE Vlan の割り当て] タブで、ドロップダウン リストから使用可能な**イーサネット Vdc** を選択します。

既存のイーサネット VLAN 範囲が表示されます。使用可能なイーサネット VDC を選択しない場合は、**[なし]** を選択します。

ストレージ VDC には、指定のインターフェイスと指定の FCoE VLAN を割り当てます。

[次へ（Next）] をクリックします。

ステップ 3 [インターフェイスの割り当て] タブで、専用インターフェイスと共有インターフェイスを FCoE VDC に追加します。

（注） 専用インターフェイスは FCoE トラフィックだけを伝送し、共有インターフェイスはイーサネット トラフィックと FCoE トラフィックの両方を伝送します。

イーサネット トラフィックとファイバ チャネル トラフィックの両方を伝送する共有インターフェイスを設定できます。この特定のケースでは、同じインターフェイスが複数の VDC に属します。FCoE VLAN および共有インターフェイスは、同じイーサネット VDC から割り当てることができます。

[次へ（Next）] をクリックします。

ステップ 4 [認証（Authenticate）] タブでは、管理者にパスワードの設定を許可し、AAA サーバ グループを使用してユーザーを認証することもできます。

[管理ユーザー（Admin User）] 領域で：

- 必要に応じて、**[パスワード強度チェックを有効にする（Enable Password Strength Check）]** チェックボックスをオンにします。
- **[Password（パスワード）]** フィールドに管理ユーザー パスワードを入力します。

- **[Confirm Password（パスワードを確認）]** フィールドに管理ユーザーパスワードを再度入力します。
- **[有効期限日（Expiry Date）]** フィールドで下矢印キーをクリックし、有効期限日ダイアログボックスで管理ユーザの有効期限を選択します。**[期限切れにしない（Never）]** ラジオボタンを選択して、パスワードを期限切れにしないようにすることもできます。

AAA サーバ グループ エリア内：

- **[グループ名（Group Name）]** フィールドに AAA サーバ グループ名を入力します。
- **[サーバ（Servers）]** フィールドに、ホスト サーバの IPv4 または IPv6 のアドレスまたは名前を 1 つまたは複数（カンマで区切る）入力します。
- **[タイプ（Type）]** フィールドで、ドロップダウン リストから サーバ グループのタイプを選択します。

[次へ（Next）] をクリックします。

ステップ 5 マネジメント Ip タブ内で IPv4 または IPv6 のアドレス情報を入力します。

[次へ（Next）] をクリックします。

ステップ 6 [概要（Summary）] タブ内で VDC 構成を確認します。

パラメータを編集するには、**[前へ（Previous）]** をクリックします。

[展開（Deploy）] をクリックして、デバイスに VDC を設定します。

ステップ 7 [展開（Deploy）] タブに、VDC 展開のステータスが表示されます。

確認メッセージが表示されます。**[詳細情報（Know More）]** をクリックして、VDC を展開するために実行されるコマンドを表示します。

[完了（Finish）] をクリックして VDC 構成ウィザードを閉じ、デバイスに構成されている VDC のリストを表示するために戻ります。

VDC の編集

Cisco DCNM Web UI から VDC を編集するには、次の手順を実行します。

手順

ステップ 1 **[インベントリ（Inventory）] > [スイッチ（Switches）] > [VDC]** を選択します。

VDC ウィンドウが表示されます。

ステップ 2 編集する必要がある VDC ラジオ ボタンを選択します。VDC の **[編集（Edit）]** アイコンをクリックします。

ステップ 3 必要に応じてパラメータを変更します。

ステップ 4 概要タブで構成の概要を確認したら、新しい構成で VDC を**[展開（Deploy）]** をクリックします。

モジュールのインベントリ情報の表示

Cisco DCNM Web UI の 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 **[インベントリ（Inventory）] > [表示（View）] > [モジュール（Modules）]**の順に選択します。

[モジュール（Modules）] ウィンドウに、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。

ステップ 2 次の情報が表示されます。

- **[グループ（Group）]** 列には、モジュールのグループ名が表示されます。
- **[スイッチ（Switch）]** 列には、モジュールが検出される時にスイッチ名が表示されます。
- **[名前（Name）]** にはモジュール名が表示されます。
- **[ModelName]** にモデル名が表示されます。
- **[SerialNum]** 列には、シリアル番号が表示されます。
- **[2nd SerialNum（2 番目の SerialNum ）]** 列には、 2 番目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。
- **[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（Hardware 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。
- **[OperStatus]** 列には、デバイスの動作状態が表示されます。
- **[IO FPGA]** 列には、IO フィールド プログラマブル ゲート 配列（FPGA）バージョンが表示されます。
- **[MI FPGA]** 列には、MI フィールド プログラマブル ゲート 配列（FPGA）のバージョンが表示されます。

ライセンスのインベントリ情報の表示

Cisco DCNM Web UI のライセンス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 **[インベントリ] > [表示] > [ライセンス]** の順に選択します。

選択した範囲に基づいて **[ライセンス（Licenses）]** ウィンドウが表示されます。

ステップ 2 次の情報が表示されます。

- **[グループ（Group）]** 列には、スイッチのグループ名が表示されます。
- **[スイッチ（Switch）]** 列には、機能が有効になっているスイッチ名が表示されます「
- **[機能（Feature）]** には、インストールされている機能が表示されます。
- **[ステータス（Status）]**は、ライセンスの使用ステータスを表示します。
- **[タイプ（Type）]** 列には、ライセンスのタイプが表示されます。
- **[警告（Warnings）]** 列には警告メッセージが表示されます。

スイッチのモニタリング

[スイッチ（Switch）] メニューには次のサブメニューが含まれます。

スイッチ CPU 情報の表示

スイッチ CPU 情報を Cisco DCNM Web UI から表示するには、次の操作を行なってください。

Procedure

ステップ 1 **[モニタ（Monitor）] > [スイッチ（Switch）] > [CPU]** を選択します。

[CPU] ウィンドウが表示されます。このウィンドウには、その範囲内のスイッチの CPU 情報が表示されます。

ステップ 2 ドロップダウンを使用して、の過去 10 分、過去 1 時間、前日、先週、先月、および昨年で表示するようにフィルタできます。

ステップ 3 **[スイッチ（Switch）]** 列でスイッチ名をクリックして、スイッチ ダッシュボードを表示します。

ステップ 4 **[スイッチ（Switch）]** 列のグラフ アイコンをクリックして、CPU 使用率を表示します。

また、チャートのタイムラインを の過去 10 分、過去 1 時間、前日、先週、先月、および昨年に変更することもできます。表示するグラフの種類とグラフのオプションも選択できます。

スイッチのメモリ情報の表示

スイッチ メモリ 情報を Cisco DCNM Web UI から表示するには、次の操作を行なってください。

Procedure

ステップ 1 **[モニタ（Monitor）] > [スイッチ（Switch）] > [メモリ（Memory）]** を選択します。

メモリ パネルが表示されます。このパネルには、その範囲内のスイッチの メモリ 情報が表示されます。

ステップ 2 ドロップダウンを使用して、の過去 10 分、過去 1 時間、前日、先週、先月、および昨年で表示するようにフィルタ処理ができます。

ステップ 3 **[スイッチ（Switch）]**列のグラフアイコンをクリックして、スイッチのメモリ使用量のグラフを表示します。

ステップ 4 **[スイッチ（Switch）]** 列でスイッチ名をクリックして、スイッチ ダッシュボードを表示します。

ステップ 5 ドロップダウンを使用して、さまざまなタイム ラインでチャートを表示できます。チャートアイコンを使用して、さまざまなビューでメモリ使用チャートを表示します。

スイッチ トラフィックとエラー情報の表示

スイッチ トラフィックとエラー 情報を Cisco DCNM Web UI から表示するには、次の操作を行なってください。

Procedure

ステップ 1 **[モニタ（Monitor）] > [スイッチ（Switch）] > [Traffic（トラフィック）]** を選択します。

[スイッチ トラフィック（Switch Traffic）] パネルが表示されます。このパネルには、過去 24 時間のそのデバイスのトラフィックが表示されます。

ステップ 2 ドロップダウンを使用して、24 時間、週、月、および年でビューをフィルタ処理します。

ステップ 3 スプレッドシートにデータをエクスポートするには、右上の隅の **[エクスポート（Export）]** 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。

ステップ 5 スイッチ名をクリックして、スイッチ ダッシュボード セクションを表示します。

スイッチ温度の表示

Cisco DCNM には、スイッチのセンサー温度を表示できるモジュール温度センサー モニタリング機能が含まれています。センサー リストをフィルタ処理する間隔を選択できます。デフォルトの間隔は **[最終日（Last Day）]** です。履歴温度データを持つセンサーのみがリストに表示されます。過去 10 分間、過去 1 時間、最終日、先週、および先月から選択できます。

Note **[構成（Configure）] > [資格情報管理（Credentials Management）] > [ローカル エリア ネットワーク資格情報（LAN Credentials）]** 画面で LAN の資格情報を設定して、スイッチから温度モニタリング データを取得する必要はありません。

スイッチ 温度情報を Cisco DCNM Web UI から表示するには、次の操作を行なってください。

Procedure

ステップ 1 **[モニタ（Monitor）] > [スイッチ（Switch）] > [温度（Temperature）]** を選択します。

[スイッチ温度（Switch Temperature）] ウィンドウには、次の列が表示されます。

- **[範囲（Scope）]**: センサーは、ファブリックの一部であるスイッチに属しています。属しているファブリックが範囲として表示されます。Cisco DCNM の上部にある範囲 セレクタを使用すると、センサー リストはその範囲によってフィルタ処理されます。
- **[スイッチ（Switch）]** : センサーが属するスイッチの名前。
- **[IP Address（ IP アドレス ）]** : スイッチの IP アドレス。
- **[温度モジュール（Temperature Module）]** : センサー モジュールの名前。
- **[平均 / 範囲（Avg/Range）]** : 最初の数値は、表の上部で指定された間隔での平均温度です。2 番目の数値セットは、その間隔における温度の範囲です。
- **[ピーク（Peak）]** : インターバルにおける最高温度

ステップ 2 このリストの各行には、クリックできるチャート アイコンがあります。
センサーの履歴データを示すチャートが表示されます。このチャートの間隔も 24 時間、1 週間あるいは1 か月の間で変更できます。

温度監視の有効化

LAN 収集画面から LAN スイッチの温度モニタリング機能を有効にできます。また、[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]

画面でいくつかのプロパティを設定することで、SAN スイッチの温度モニタリング機能を有効にすることができます。

LAN スイッチの温度モニタリングの有効化

1. **[管理（Administration）] > [パフォーマンス セットアップ（Performance Setup）] > [ローカル エリア ネットワーク（LAN） コレクション（LAN Collections）]** をメニュー バーから選択します。
2. **[温度センサー（Temperature Sensor）]** チェック ボックスを選択します。
3. 性能データを収集したい LAN スイッチの種類を選択します。
4. [Apply] をクリックして、設定を保存します

アカウンティング情報の表示

アカウンティング情報を Cisco DCNM Web UI から表示するには、次の操作を行なってください。

Procedure

ステップ 1 **[モニタ（Monitor）] > [スイッチ（Switch）] > [アカウンティング（Accounting）]**の順に選択します。

アカウンティング情報とともにファブリック名またはグループ名が表示されます。

ステップ 2 アカウンティング情報を **[送信元（Source）]** 、 **[ユーザー名（Username）]** 、**[時間（Time）]** と **[詳細（Description）]** で検索するためにフィルタ アイコンの横にある **[高度フィルタ（Advanced Filter）]** を選択ます。 または **[クイック フィルタ（Quick Filter）]** カラムの元で検索するために選択します。

ステップ 3 行を選択して **[削除（Delete）]** アイコンをクリックすることによってリストのアカウンティング情報を削除することもできます。

ステップ 4 **[印刷（Print）]**アイコンを使用してアカウンティングの詳細を印刷し、**[エクスポート（Export）]** アイコンを使用してデータを Microsoft Excel スプレッドシートにエクスポートできます。

イベント情報の表示

Cisco DCNM Web UI からイベントと syslog を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）] > [スイッチ（Switch）] > [Events（イベント）]** を選択します。

ファブリック、スイッチ名、およびイベントの詳細が表示されます。

[数（Count）] 列には、**[最後に見た（Last Seen）]** および **[最初に見た（First Seen）]** 列に示されているように、期間中に同じイベントが発生した回数が表示されます。

[スイッチ（Switch）] 列のスイッチ名をクリックして、スイッチ ダッシュボードを表示します。

ステップ 2 テーブルでイベントを選択し、**[抑制の追加（Add Suppressor）]** アイコンをクリックして、イベント抑制ルールを追加するショートカットを開きます。

ステップ 3 テーブルから1つ以上のイベントを選択し、**[確認（Acknowledge）]** アイコンをクリックして、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の横の **Ack** 列に表示されます。

ステップ 4 ファブリックを選択し、**[未確認（Unacknowledge）]** アイコンをクリックして、ファブリックの確認をキャンセルします。

ステップ 5 アカウンティング情報を **[送信元（Source）]** 、 **[ユーザー名（Username）]** 、**[時間（Time）]** と **[詳細（Description）]** で検索するためにフィルタ アイコンの横にある **[高度フィルタ（Advanced Filter）]** を選択します。 または **[クイック フィルタ（Quick Filter）]** カラムの元で検索するために選択します。

ステップ 6 ファブリックを選択し、**[削除（Delete）]** アイコンを使用して、リストからファブリックおよびイベント情報を削除します。

ステップ 7 イベント情報を印刷するには **[印刷（Print）]** アイコンをクリックします。

ステップ 8 **[Excel にエクスポート（Export to Excel）]** アイコンをクリックして、データをエクスポートします。

LAN のモニタリング

LAN メニューには次のサブメニューが含まれます。

イーサネットに関するパフォーマンス情報のモニタリング

Cisco DCNM Web UI からイーサネットのパフォーマンス情報を監視するには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）]** > **[ローカル エリア ネットワーク（LAN）]** > **[イーサネット（Ethernet）]** を選択します。

[イーサネット（Ethernet）] ウィンドウが表示されます。

ステップ 2 ドロップダウンを使用して、の過去 10 分、過去 1 時間、前日、先週、先月、および昨年で表示するようにフィルタできます。

他にもいくつかの方法で情報を表示できます。これらの基本的な手順以外に、次の手順を実行することもできます。

- **[名前（Name）]**カラムからイーサネットポート名を選択すると、過去24時間にそのイーサネットポートを通過したトラフィックを示すグラフが表示されます。時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。
- スプレッドシートにデータをエクスポートするには、右上の隅の**[エクスポート（Export）]** アイコンをクリックしてから **[保存（Save）]** をクリックします。
- チャートアイコンを使用して、さまざまなビューでトラフィックチャートを表示します。アイコンを使用して、データを **[追加（Append）]**、**[予測（Predict）]**、および **[データの補間はしないでください（Do not interpolate data）]**することもできます。

  Note **[データの補間はしないでください（Do not interpolate data）]** オプションを使用するために**[サーバー プロパティ（Server Properties）]** ウィンドウ の中にある **pmchart.doInterpolate** プロパティを false に設定します。

- Rx/Tx の計算については、以下の Rx/Tx 計算を参照してください。

  Note ファブリックの変換は、10 ビット = 1 バイトで、LAN トラフィックの場合変換が 8 ビット = 1 バイトです。

  - 平均 Rx/Tx % = 平均 Rx/Tx を速度で割った値 * 100
  - ピーク Rx/Tx % = ピーク Rx/Tx を速度で割った値 * 100

Note パフォーマンス テーブルにデータが含まれていない場合は、パフォーマンス データ収集をオンにするため、しきい値セクションを参照してください。

Note トラフィックの表示単位をバイトからビットに変更するには、Cisco DCNM Web UI から、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** を選択し、**pm.showTrafficUnitAsbit** プロパティに true として値を入力し、**[変更を適用（Apply Changes）]** をクリックします。

ISL トラフィックとエラーのモニタリング

Cisco DCNM Web UI から ISL トラフィックとエラーをモニタするには、次の手順を実行します。

Procedure

ステップ 1 **[モニタ（Monitor）] > [LAN] > [リンク（Link）]** を選択します。

[ISL トラフィックとエラー（ISL Traffic and Errors）] ウィンドウが表示されます。このパネルには、その範囲内のエンドデバイスの ISL 情報が表示されます。範囲メニューを使用して、表示される範囲を縮小または拡大できます。

ステップ 2 ドロップダウンを使用して、の過去 10 分、過去 1 時間、前日、先週、先月、および昨年で表示するようにフィルタできます。

Note データ グリッドの **NaN**（非数）は、データが利用できないことを意味します。

他にもいくつかの方法で情報を表示できます。これらの基本的な手順以外に、次の手順を実行して ISL の詳細情報を表示することもできます。

- このグラフの時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。
- 期間を指定して詳細情報を表示するには、スライダコントロールをドラッグして、表示する期間を指定します。
- チャートアイコンを使用して、さまざまなビューでトラフィックチャートを表示します。アイコンを使用して、データを **[追加（Append）]**、**[予測（Predict）]**、および **[データの補間はしないでください（Do not interpolate data）]**することもできます。

  Note **[データの補間はしないでください（Do not interpolate data）]** オプションを使用するために**[サーバ プロパティ（Server Properties）]** ウィンドウ の中にある **pmchart.doInterpolate** プロパティを false に設定します。

- データをスプレッドシートにエクスポートするには、**[チャート（Chart）]** メニューのドロップダウン リストから **[エクスポート（Export）]** を選択し、**[保存（Save）]** をクリックします。
- Rx/Tx の計算については、以下の Rx/Tx 計算を参照してください。

  Note ファブリックの変換は、10 ビット = 1 バイトで、LAN トラフィックの場合変換が 8 ビット = 1 バイトです。

  - 平均 Rx/Tx % = 平均 Rx/Tx を速度で割った値 * 100
  - ピーク Rx/Tx % = ピーク Rx/Tx を速度で割った値 * 100

Note パフォーマンステーブルにデータが含まれていない場合は、パフォーマンス設定のしきい値セクションを参照してパフォーマンスをオンにします。

vPC のモニタリング

仮想ポート チャネル（vPC）は、シングル ポート チャンネルとして違うデバイスに物理的に接続されたリンクを表示することを有効化します。vPC は、ノード間の複数の並列パスを可能にし、トラフィックのロードバランシングを可能にすることによって、冗長性を作り、2 分割帯域幅を増やす拡張された形式のポートチャネルです。トラフィックは、2 つの単一デバイス

vPC エンドポイント間で分散されます。vPC 構成に矛盾がある場合、vPC は正しく機能しません。

Note **[vPC パフォーマンス（vPC Performance）]**で vPC を表示するには、プライマリ デバイスとセカンダリ デバイスの両方をユーザーに指定する必要があります。いずれかのスイッチが指定されていない場合は、vPC 情報が再生されます。

Cisco DCNM **[Web クライアント（Web Client）] > [モニタ（Monitor）] > [vPC]** は、一貫性のある vPC のみを表示します。一貫性のある vPC と一貫性のない vPC の両方が表示されます。

Cisco DCNM **[Web UI] > [構成（Configure）] > [展開（Deploy）] > [vPC ピア（vPC Peer）]** および **[Web クライアント（Web Client）] > [構成（Configure）] > [展開（Deploy）] > [vPC]** を使用して、矛盾する vPC を特定し、各 vPC の矛盾を解決できます。

Table 18: vPC パフォーマンス, on page 553 は、データ グリッド表示に次の vPC 構成の詳細を表示します。

***Table 18: vPC* パフォーマンス**

列	説明
検索ボックス	任意の文字列を入力して、それぞれの列のエントリをフィルタ処理します。
vPC ID	vPC 識別子の構成済みデバイスを表示します。
ドメイン ID	vPC ピア スイッチのドメイン 識別子 を表示します。
[マルチ シャーシ vPC エンドポイント（Multi Chassis vPC EndPoints）]	vPC ドメインの下の各 vPC 識別子 のマルチシャーシ vPC エンドポイントを表示します。
[プライマリ vPC ピア - デバイス名（Primary vPC Peer - Device Name）]	vPC プライマリ デバイス名を表示します。
[プライマリ vPC ピア - プライマリ vPC インターフェイス（Primary vPC Peer - Primary vPC Interface）]	プライマリ vPC インターフェイスを表示します。
[プライマリ vPC ピア - キャパシティ（Primary vPC Peer - Capacity）]	プライマリ vPC ピアのキャパシティを表示します。
プライマリ vPC ピア - 平均受信/秒	プライマリ vPC ピアの平均受信速度を表示します。
プライマリ vPC ピア - 平均送信/秒	プライマリ vPC ピアの平均送信速度を表示します。

列	説明
[プライマリ vPC ピア - ピーク使用率（Primary vPC Peer - Peak Util%）]	プライマリ vPC ピアのピーク使用率を表示します。
[セカンダリ vPC ピア - デバイス名（econdary vPC Peer - Device Name）]	vPC セカンダリ デバイス名を表示します。
[セカンダリ vPC インターフェイス（Secondary vPC Interface）]	セカンダリ vPC インターフェイスを表示します
[セカンダリ vPC ピア - キャパシティ（Secondary vPC Peer - Capacity）]	セカンダリ vPC ピアのキャパシティを表示します。
セカンダリ vPC ピア - 平均。受信/秒	セカンダリ vPC ピアの平均受信速度を表示します。
セカンダリ vPC ピア - 平均。送信/秒	セカンダリ vPC ピアの平均送信速度を表示します。
[セカンダリ vPC ピア - ピーク使用率（Secondary vPC Peer - Peak Util%）]	セカンダリ vPC ピアのピーク使用率を表示します。

この機能は次のように使用できます。

vPC パフォーマンスのモニタリング

一貫性のある仮想ポート チャネル(vPC)間の関係を表示できます。すべてのメンバー インターフェイスの統計と、ポート チャネル レベルでの統計の集約を表示できます。

Note このタブには、一貫性のある vPC のみが表示されます。

Cisco DCNM Web UI から VPC パフォーマンス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 **[モニタ（Monitor）] > [LAN] > [vPC]** を選択します。

vPC パフォーマンス統計が表示されます。すべての vPC の集約された統計が表形式で表示されます。

ステップ 2 **[vPC ID]** をクリックします。

vPC トポロジ、**[vPC の詳細（vPC Details）]**、**[ピア リンクの詳細（Peer-link Details）]**、および **[ピア リンクのステータス（Peer-link Status）]** が表示されます。

vPC の **[vPC 整合性（vPC Consistency）]**、**[ピア リンク整合性（Peer-link Consistency）]**、および **[vPC Type2 整合性（vPC Type2 Consistency）]** が表示されます。

- **[vPC の詳細（vPC Details）]** タブをクリックすると、プライマリとセカンダリの両方の vPC デバイスの vPC **[基本設定（Basic Setting）]** と **[レイヤ 2 設定（Layer 2 Settings）]** のパラメータの詳細を表示できます。
- **[ピア リンクの詳細（Peer-link Details）]** タブをクリックして、プライマリとセカンダリの両方の vPC デバイスのピア リンク **[vPC グローバル設定（vPC Global Setting）]** および **[STP グローバル設定（STP Global Settings）]** のパラメータの詳細を表示します。
- **[ピア リンクのステータス（Peer-link Status）]** タブをクリックすると、**[vPC の整合性（vPC Consistency）]** が表示され、**[ピア リンクの整合性（Peer-Link Consistency）]** ステータスが表示されます。プライマリとセカンダリの両方の vPC デバイスの **[ロール ステータス（Role Status）]** と **[vPC ピア キープアライブ ステータス（vPC Peer keep-alive Status）]** のパラメータの詳細も表示されます。

ステップ 3 **[プライマリ vPC ピア（Primary vPC peer）]** または **[セカンダリ vPC ピア（Secondary vPC peer）]** 列の **[デバイス名（Device Name）]** の前にあるピア リンク アイコンをクリックして、そのメンバー インターフェイスを表示します。

ステップ 4 対応するインターフェイスの **[チャートの表示（Show Chart）]** アイコンをクリックして、履歴統計を表示します。

トラフィック分散統計は、vPC ウィンドウの下部に表示されます。デフォルトでは、Cisco DCNM Web クライアントは 24 時間の履歴統計を表示します。

他にもいくつかの方法で情報を表示できます。これらの基本的な手順以外に、次の手順を実行してフローの詳細情報を表示することもできます。

- 時間範囲を変更するには、右上の隅のドロップダウン リストから時間範囲を選択します。
- 期間を指定して詳細情報を表示するには、スライダコントロールをドラッグして、表示する期間を指定します。
- チャートアイコンを使用して、さまざまなビューでトラフィックチャートを表示します。
- アイコンを使用して、データを **[追加（Append）]**、**[予測（Predict）]**、および **[データの補間はしないでください（Do not interpolate data）]**することもできます。

  Note **[データの補間はしないでください（Do not interpolate data）]** オプションを使用するために**[サーバー プロパティ（Server Properties）]** ウィンドウ の中にある **pmchart.doInterpolate** プロパティを false に設定します。

- vPC Utilization データを印刷するには、右上隅にある **[印刷（Print）]** アイコンをクリックします。[vPC 使用率（vPC Utilization）] ページが表示されます。
- スプレッドシートにデータをエクスポートするには、右上の隅の**[エクスポート（Export）]** アイコンをクリックしてから **[保存（Save）]** をクリックします。

Note パフォーマンス テーブルにデータが含まれていない場合は、パフォーマンス データ収集をオンにするため、しきい値セクションを参照してください。

エンドポイント ロケータ

エンドポイントロケータ（EPL）機能により、データセンター内のエンドポイントをリアルタイムで追跡できます。追跡には、エンドポイントのネットワーク ライフ履歴のトレースと、エンドポイントの追加、削除、移動などに関連する傾向へのインサイトの取得が含まれます。

エンドポイント ロケータに関する情報は、単一のランディング ページまたはダッシュボードに表示されます。ダッシュボードには、すべてのアクティブなエンドポイントに関するデータがほぼリアルタイムで（30秒ごとに更新されて）1つのペインに表示されます。このランディング ページに表示されるデータは、**[範囲（Scope）]** ドロップダウン リストで選択した範囲によって異なります。

- エンドポイント ロケータ
- エンドポイント ロケータの監視 （691 ページ）

アラーム

アラーム メニューには次のサブメニューが含まれます。

アラームとイベントの表示

アラーム、クリアされたアラーム、およびイベントを表示できます。

Procedure

ステップ 1 **[モニタ（Monitor）] > [アラーム（Alarms）] > [表示（View）]** を選択します。

ステップ 2 次のいずれかのタブを選択します。

- **[Alarms（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。
- **[クリアされたアラーム（Cleared Alarms）]**：このタブには、クリア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）、シビラティ（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。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。
- **[Events（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**、**確認済みユーザー**、**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。

アラーム ポリシーの監視と追加

Note

- アラーム ポリシーは、コンピューティング ノードに保存されます。したがって、DCNM のバックアップを取得することに加えて、各コンピューティング ノードで **appmgr backup** コマンドを実行します。

アラームを DCNM の登録済み SNMP リスナーに転送できます。Cisco DCNM Web UI から、**[Administration（管理）] > [DCNM Server（DCNM サーバー）] > [Server Properties（サーバーのプロパティ）]** 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、**[Apply Changes（変更の適用）]** をクリックして、DCNM サービスを再起動します。

Note **[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。

次のアラーム ポリシーを追加できます。

- **[デバイスの正常性（Device Health）]**：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。
- **[インターフェイス正常性ポリシー（Interface Health）]**：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（Syslog Alarm）]**：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。

Procedure

ステップ 1 **[モニター（Monitor）] > [アラーム（Alarms）] > [アラームポリシー（Alarm Policies）]**を選択します。

ステップ 2 **[アラームを有効にする（Enable Alarms）]** チェック ボックスをオンにして、アラーム ポリシーを有効にします。

ステップ 3 **[追加（Add）]** ドロップダウンリストから、次のいずれかのログイン情報を選択します。

- デバイス正常性ポリシー：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。詳細なトラップ OID 定義については、https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en を参照してください。
- インターフェイス正常性ポリシー：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、リンクステート、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、インバウンド廃棄、およびアウトバウンド廃棄を指定します。
- Syslogアラーム ポリシー：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。
  - 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。シンタックスは次のとおりです。**Facility-Severity-Type: Message**
  - Clear Regex：syslog クリア メッセージの形式を定義します。シンタックスは次のとおりです。**Facility-Severity-Type: Message**

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。

Table 19: 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。

Table 20: 例 2

識別子	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

Table 21: 例 3

識別子	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

ステップ 4 **[OK]**をクリックしてポリシーを追加します。

端末モニターとコンソールの syslog メッセージ

次の例は、syslog メッセージが端末モニタとコンソールにどのように表示されるかを示しています。正規表現は、syslog メッセージの % 記号の後の部分と一致します。

```
leaf-9516# terminal monitor
leaf-9516# conf t
leaf-9516(config)# int e15/1-32
leaf-9516(config-if-range)# no shut
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/1 is admin up .
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_DOWN_NONE: Interface
Ethernet15/1 is down (Transceiver Absent)
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/2 is admin up .
2019 Aug 2 04:41:27 leaf-9516 %ETHPORT-5-IF_DOWN_NONE: Interface
Ethernet15/2 is down (Transceiver Absent)
2019 Aug 2 04:41:28 leaf-9516 %ETHPORT-5-IF_ADMIN_UP: Interface
Ethernet15/3 is admin up .
```

コンソールの syslog メッセージは、%$ 記号で囲まれた追加のポート情報を除いて、端末モニタに表示されるものと同様の形式です。ただし、正規表現は、syslog メッセージの最後の % 記号の後の部分と一致します。

```
SR-leaf1# 2019 Aug 26 23:55:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-
PFM_ALERT: FAN_BAD: fan6
2019 Aug 26 23:56:15 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:18 SR-leaf1 %$ VDC-1 %$ %ASCII-CFG-2-CONF_CONTROL:
System ready
2019 Aug 26 23:56:25 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:35 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:39 SR-leaf1 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:
Successfully activated virtual service 'guestshell+'
2019 Aug 26 23:56:39 SR-leaf1 %$ VDC-1 %$ %VMAN-2-GUESTSHELL_ENABLED:
The guest shell has been enabled. The command 'guestshell' may be used
to access it, 'guestshell destroy' to remove it.
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-2-FAN_REMOVED: Fan
module 5 (Serial number ) Fan5(sys_fan5) removed
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
System will shutdown in 2 minutes 0 seconds due to fan policy
__pfm_fanabsent_any_singlefan.
2019 Aug 26 23:56:45 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:56:54 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
System will shutdown in 1 minutes 40 seconds due to fan policy
__pfm_fanabsent_any_singlefan.
2019 Aug 26 23:56:54 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
2019 Aug 26 23:57:03 SR-leaf1 %$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK:
Fan module 5 (Fan5(sys_fan5) fan) ok
2019 Aug 26 23:57:03 SR-leaf1 %$ VDC-1 %$ %PLATFORM-1-PFM_ALERT:
FAN_BAD: fan6
```

アクティブなポリシー

新しいアラーム ポリシーを作成したら、それらをアクティブにします。

Procedure

ステップ 1 **[モニター（Monitor）] > [アラーム（Alarms）] > [アラーム ポリシー（Alarm Policies）]**を選択します。

ステップ 2 アクティブ化するポリシーを選択し、**[アクティブ化（Activate）]** ボタンをクリックします。

ポリシーの非アクティブ化

アクティブなアラーム ポリシーを非アクティブ化できます。

Procedure

ステップ 1 **[モニター（Monitor）] > [アラーム（Alarms）] > [ポリシー（Policies）]**を選択します。

ステップ 2 非アクティブ化するポリシーを選択し、**[非アクティブ化（Deactivate）]** ボタンをクリックします。

ポリシーのインポート

インポート機能を使用してアラーム ポリシーを作成できます。

Procedure

ステップ 1 **[モニター] > [アラーム] > [ポリシー]** を選択し、**[インポート]** ボタンをクリックします。

ステップ 2 コンピュータに保存されているポリシー ファイルを参照して選択します。

ポリシーはテキスト形式でのみインポートできます。

ポリシーのエクスポート

アラーム ポリシーをテキスト ファイルにエクスポートできます。

Procedure

ステップ 1 メニュー バーから **[モニター（Monitor）] > [アラーム（Alarms）] > [ポリシー（Policies）]** を選択します。

ステップ 2 [エクスポート]ボタンをクリックし、エクスポートしたファイルを保存するコンピューター上の場所を選択します。

ポリシーの編集

Procedure

ステップ 1 メニュー バーから**[モニター（Monitor）] > [アラーム（Alarms）] > [ポリシー（Policies）]**を選択します。

ステップ 2 編集するポリシーを選択します。

ステップ 3 **[編集（Edit）]** ボタンをクリックして変更を加えます。

ステップ 4 [OK] ボタンをクリックします。

ポリシーの削除

Procedure

ステップ 1 メニュー バーから**[モニター（Monitor）] > [アラーム（Alarms）] > [ポリシー（Policies）]**を選択します。

ステップ 2 削除するポリシーを選択します。

ステップ 3 **[削除（Delete）]** ボタンをクリックします。ポリシーが削除されます。

外部アラームの有効化

次のいずれかの方法を使用して、外部アラームを有効にできます。

- Cisco DCNM Web UI を使用します。
  1. **[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** Cisco DCNM Web UI を選択します。
  2. **alarm.enable.external** プロパティを見つけます。
  3. フィールドに値として **true** を入力します。
- REST API の使用
  1. DCNM セットアップから API ドキュメントの URL に移動します: https://<*DCNM-ip*>/api-docs
  2. **[アラーム（Alarms）]** セクションに移動します。

3. **[POST] > [rest/alarms/enabledisableextalarm]** をクリックします。
4. **[値（Value）]** ドロップダウン リストから、**[body（本体）]** パラメータ値として **[true]** を選択します。
5. **[試してみる!（Try it out!）]** をクリックします。

- CLI の使用

1. SSH を使用してDCNM サーバにログインします。
2. server.properties ファイルで、**alarm.enable.external** プロパティを **true** に設定します。

   ファイルパスは `/usr/local/cisco/dcm/fm/config/server.properties` です。

構成コンプライアンス アラーム

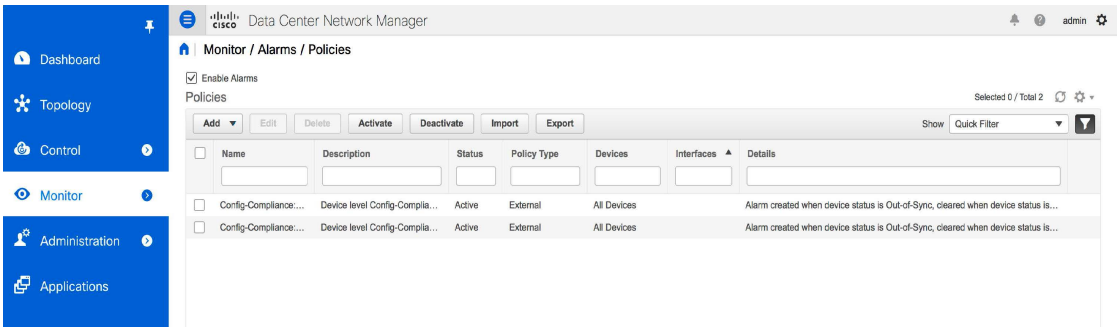
Cisco DCNM リリース 11.3(1) 以降、外部カテゴリの下のアラーム ポリシーとアラームは、DCNM で実行されているアプリケーションによって作成されます。これらの外部アラーム ポリシーはアプリケーションによって作成され、DCNM Web UI を介して作成または追加することはできません。

Config-Compliance(CC) は、DCNM で実行されるコア アプリケーションです。CC は、外部アラーム カテゴリの下にアラームを登録および作成します。

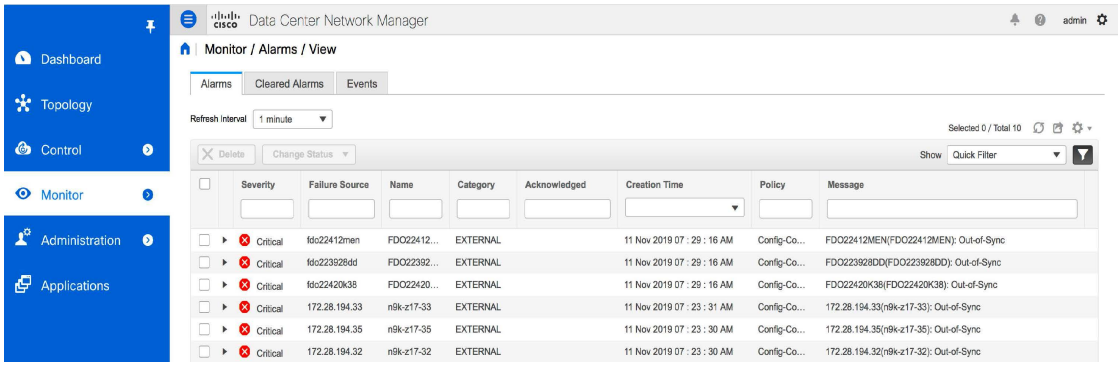
Config-Compliance : アラーム ポリシー

この外部アラーム カテゴリ ポリシーは、ファブリックの作成時にアクティブ化され、そのファブリック内のすべてのデバイスで有効になります。ポリシーの重大度レベルは重大です。ファブリック内のいずれかのデバイスが In-Sync から Out-of-Sync に移動し、**[アラームを有効化（Enable Alarms）]** チェックボックスが選択されている場合、重大な重大度のアラームが生成されます。

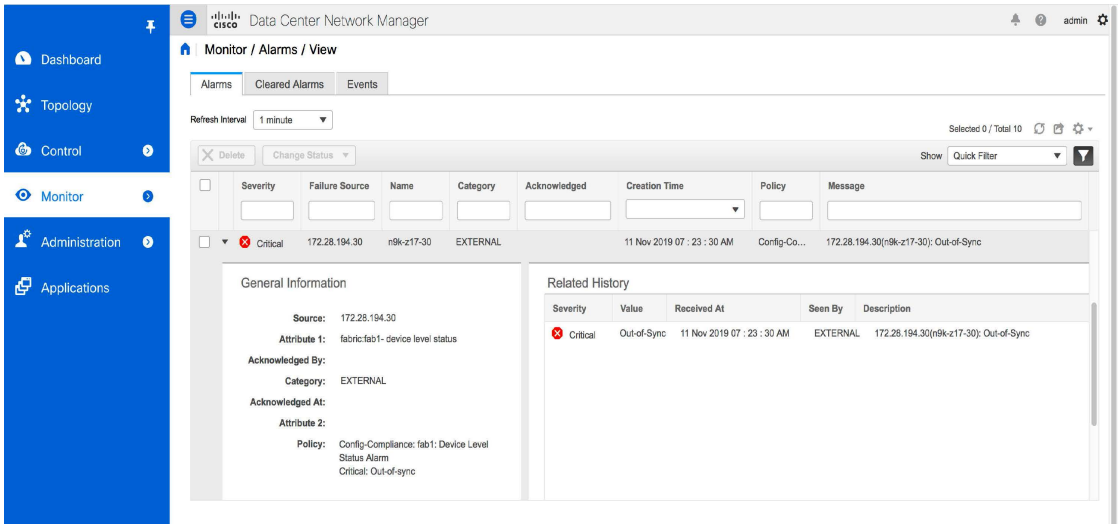
[モニタ（Monitor）] > [アラーム（Alarms）] > [ポリシー（Policies）] を選択して、デフォルトのアラーム ポリシーを表示します。このアラームポリシーは、Web UI では編集できません。**[アクティブ化（Activate）]** または **[非アクティブ化（Disactivate）]** をクリックして、選択したポリシーをアクティブ化または非アクティブ化します。



DCNM Web UI を使用してアラーム ポリシーが非アクティブ化された場合、そのポリシーに対して作成またはクリアされたアラームは、**[モニタ（Monitor）]>[アラーム（Alarm）]>[表示（View）]**タブに表示されません。ポリシーを削除するには、ポリシーの横にあるチェックボックスをオンにして、**[削除（Delete）]**をクリックします。ただし、DCNM Web UI からはポリシーを削除しないことをお勧めします。ポリシーが削除された場合、CC は、次回の定期実行時、またはデバイス レベルまたはそのファブリックの下のファブリック レベルで再同期がトリガーされたときに、ポリシーを再生成します。



アラームの詳細な情報を表示するには**[重大（Critical）]**の横にある矢印アイコンをクリックします。

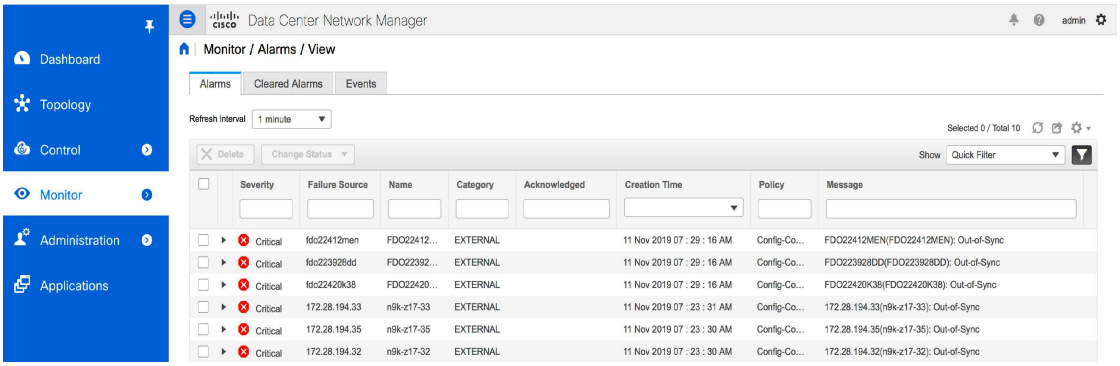


Out-of-Sync ステータスは、DCNM でデバイスに定義されたインテントとデバイスで実行中の構成との間に違いがあることを示します。In-Sync ステータスは、DCNM でデバイスに定義されたインテントが実行構成と一致し、CC が構成間に違いを検出しなかったことを示します。差分の計算の詳細については、「*DCNM* での構成の準拠」を参照してください。

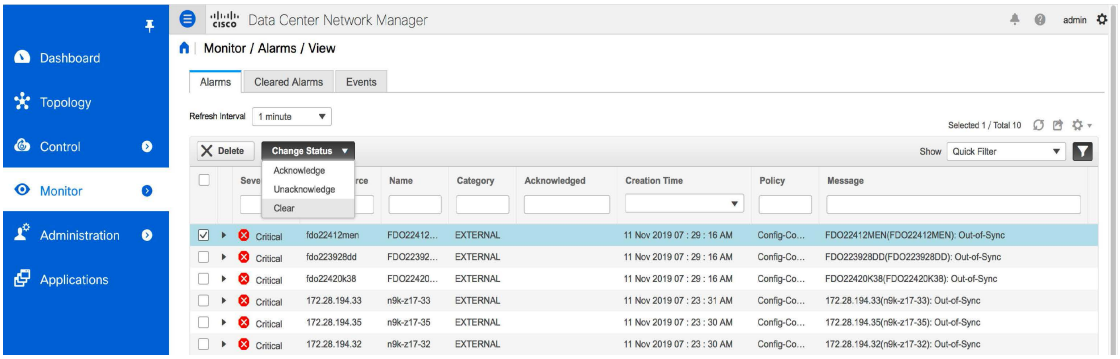
ファブリックが削除されると、アラームポリシーとそのファブリック内のデバイスのすべてのアクティブアラームが削除されます。

Config-Compliance：アクティブ アラーム

CC がファブリックで実行されていて、そのファブリック内のデバイスが Out-of-Sync ステータスに移行するシナリオを検討してください。これにより、重大な重大度アラームが生成されます。**[モニタ（Monitor）] > [アラーム（Alarm）] > [表示（View）]** を選択して、アラームを表示します。これらのアラームは、デバイスが Out-of-Sync から In-Sync に移行するまでアクティブです。



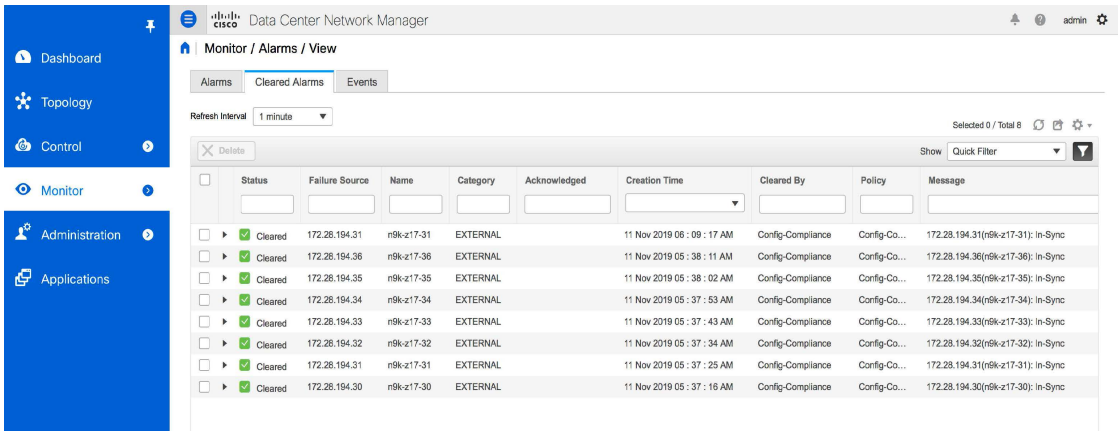
アクティブなアラームをクリアするには、アラームの横にあるチェックボックスを選択し、**[ステータスを変更（Change Status）]**をクリックして**[クリア（Clear）]** を選択します。同じデバイスが再び Out-of-Sync ステータスに移行すると、アクティブなアラームが再作成されます。



アクティブなアラームを削除するには、アラームの横にあるチェックボックスを選択し、**[削除（Delete）]** をクリックします。同じデバイスが再び Out-of-Sync ステータスに移行すると、アクティブなアラームが再作成されます。

Config-Compliance：クリアされたアラーム

Out-of-Sync ステータスにあるデバイスが In-Sync ステータスに移行すると、現用系アラームがクリアされます。クリアされたアラームを表示するには **[モニタ（Monitor）]>[アラーム（Alarms）]>[表示（View）]>[クリアされたアラーム（Cleared Alarms）]**を選択します。クリアされたアラームは、全体的なデバイス 正常性スコアには影響しません



クリアされたアラームのリストからクリアされたアラームを削除するには、**[モニタ（Monitor）] > [アラーム（Alarms）] > [表示（View）] > [クリアされたアラーム（Cleared Alarms）]** を選択し、アラームの横にあるチェックボックスを選択し、**[削除（Delete）]** をクリックします。これにより、選択したクリア済みアラームがリストから削除されます。

スイッチが Out-of-Sync から In-Sync に移動すると、アラームはクリアされます。構成コンプライアンス アラームは、デバイスの全体的な正常性スコアにも影響します。

アラームとポリシーの詳細については、「アラーム」を参照してください。

エンドポイント ロケータ アラーム

Cisco DCNM リリース 11.4(1) よりアラームは、エンドポイントロケータ（EPL）によって外部アラーム カテゴリに登録および作成されます。

エンドポイント ロケータ：アラーム ポリシー

EPL 外部アラームカテゴリポリシーは、ファブリックで EPL が有効になっているときにアクティブになります。アラームは、重複する IP アドレス、重複する MAC アドレス、VRF に表示されるエンドポイント、VRF から消えるエンドポイント、ファブリック内で移動するエンドポイント、ルートリフレクタ接続の喪失、ルートリフレクタ接続の復元などの問題に対して発生します。問題に応じて、アラームポリシーの重大度レベルは CRITICAL または MINOR になります。

アラームは、次のイベントに対して発生し、CRITICAL に分類されます。

- ルートリフレクタの切断
- 重複する IP アドレスの検出
- 重複する MAC アドレスの検出

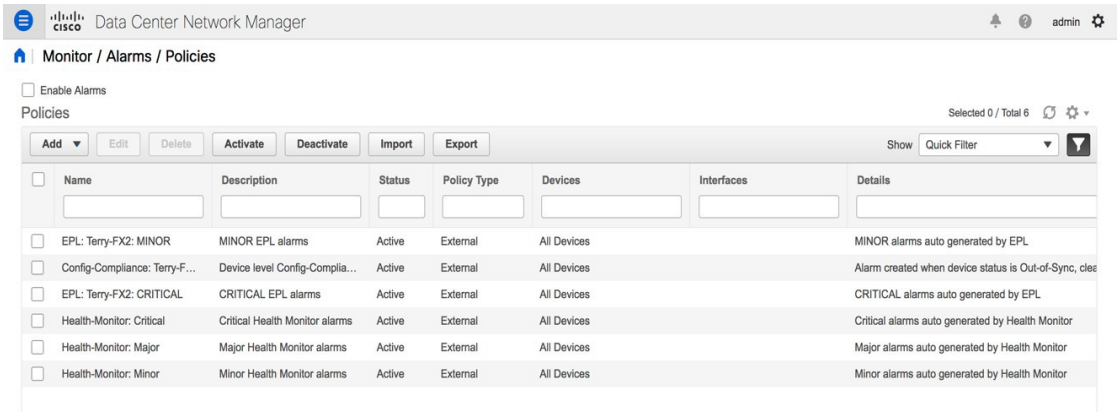
次のイベントの場合、アラームが発生し、MINOR として分類されます。

- エンドポイントの移動
- ファブリック内の新しい VRF の表示

- ファブリック内のエンドポイントの数が 0 になる
- VRF のエンドポイントの数が 0 になる
- スイッチからのすべてのエンドポイントの消失
- ルートリフレクタ（RR）の接続

状態が修正されると、CRITICAL アラームは自動的にクリアされます。たとえば、DCNM と RR 間の接続が失われると、CRITICAL アラームが生成されます。このアラームは、DCNM と RR 間の接続が回復すると自動的にクリアされます。その他の MINOR アラームは、アラームが生成されてから 30 分が経過すると自動的にクリアされます。

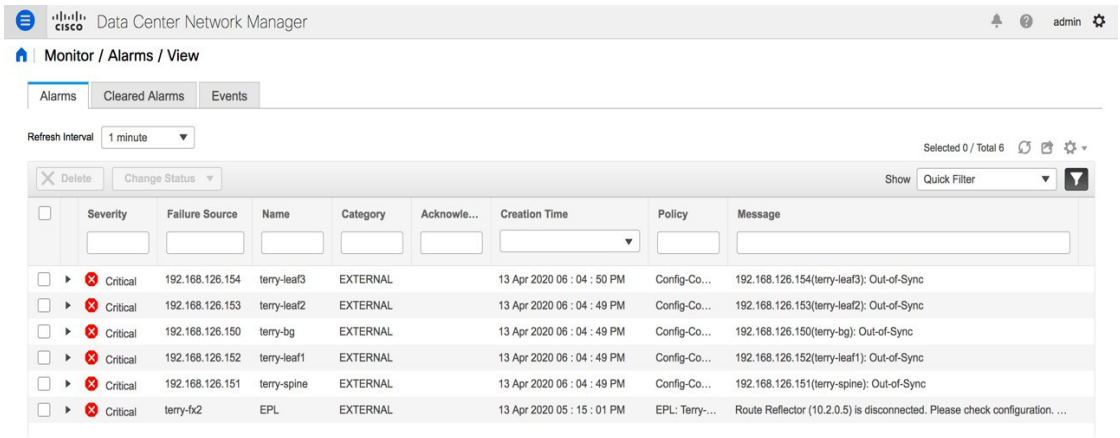
[モニタ（Monitor）] > [アラーム（Alarm）] > [ポリシー（Policies）] を選択して、EPL アラームポリシーを表示します。これらのアラームポリシーは、Web UI では編集できません。**[アクティブ化（Activate）]** または **[非アクティブ化（Disactivate）]** をクリックして、選択したポリシーをアクティブ化または非アクティブ化します。



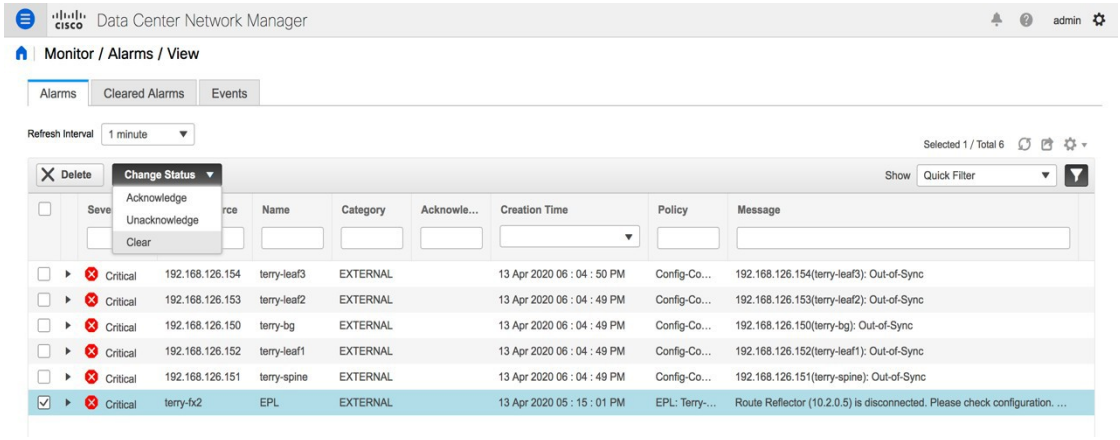
DCNM Web UI を使用してアラーム ポリシーが非アクティブ化された場合、そのポリシーに対して作成またはクリアされたアラームは、**[モニタ（Monitor）] > [アラーム（Alarm）] > [表示（View）]** タブに表示されません。ポリシーを削除するには、ポリシーの横にあるチェックボックスをオンにして、**[削除（Delete）]** をクリックします。ただし、DCNM Web UI からはポリシーを削除しないことをお勧めします。ファブリックが削除されると、アラームポリシーとそのファブリック内のデバイスのすべてのアクティブアラームが削除されます。

エンドポイントロケータ：アクティブアラーム

[モニタ（Monitor）] > [アラーム（Alarm）] > [表示（View）] を選択して、アクティブなアラームを表示します。



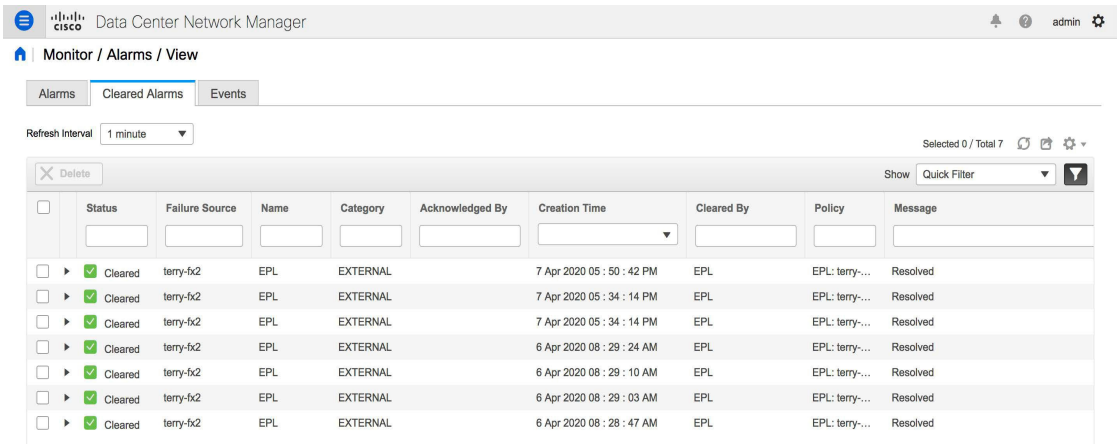
アクティブなアラームをクリアするには、アラームの横にあるチェックボックスを選択し、**[ステータスを変更（Change Status）]**をクリックして **[クリア（Clear）]** を選択します。



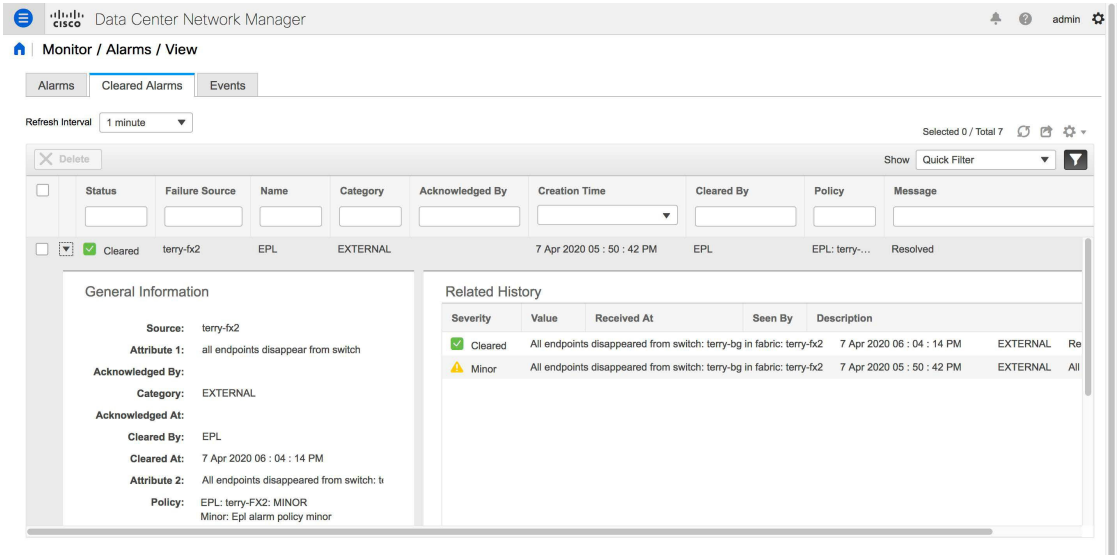
アクティブなアラームを削除するには、アラームの横にあるチェックボックスを選択し、**[削除（Delete）]** をクリックします。

エンドポイントロケータ：クリアされたアラーム

クリアされたアラームを表示するには **[モニタ（Monitor）]>[アラーム（Alarms）]>[表示（View）]>[クリアされたアラーム（Cleared Alarms）]**を選択します。



必須のアラームの詳細な情報を表示するには矢印アイコン ▶ をクリックします。



クリアされたアラームのリストからクリアされたアラームを削除するには、アラームの横にあるチェックボックスを選択し、**[削除（Delete）]** をクリックします。

アラームとポリシーの詳細については、「アラーム」を参照してください。

ヘルス モニタ アラーム

Cisco DCNM リリース 11.4(1) 以降、アラームはヘルス モニタによって外部アラーム カテゴリに登録および作成されます。

ヘルス モニタ：アラーム ポリシー

ヘルス モニタの外部アラーム カテゴリ ポリシーは、ファブリック内のすべてのデバイスで自動的にアクティブ化および有効化されます。このアラーム ポリシーの重大度は、マイナー、メジャー、または重大です。

アラームは、次のイベントに対して発生し、CRITICAL に分類されます。

- Elasticsearch （ES）クラスタのステータスが赤：重大（クラスタ/HA モードの場合のみ）
- CPU/メモリ/ディスク使用率/ES JVM ヒープ使用率 >= 90%

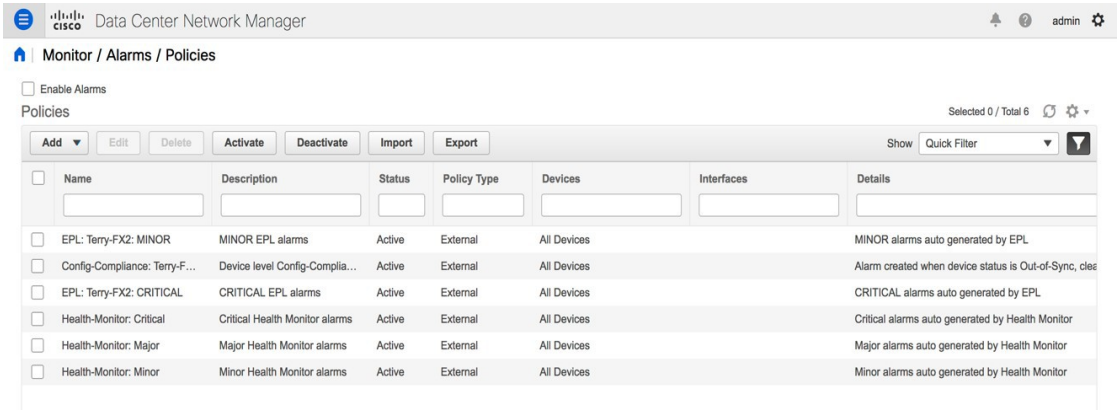
次のイベントの場合、アラームが発生し、メジャーとして分類されます。

- ES クラスタ ステータスが黄色（クラスタ/HA モードの場合のみ）
- ES に未割り当てのシャードがある（クラスタ/HA モードのみ）
- CPU/メモリ/ディスク使用率/ES JVM ヒープ使用率 >= 80% および <90%

次のイベントの場合、アラームが発生し、MINOR として分類されます。

- CPU/メモリ/ディスク使用率/ES JVM ヒープ使用率 >= 65% および <80%
- Kafka: アクティブなリーダーのないパーティションの数 > 0
- Kafka: 適格なパーティション リーダーが見つかりません。不明確なリーダー > 0

[モニタ（Monitor）] > [アラーム（Alarms）] > [ポリシー（Policies）] を選択して、ヘルス モニタのアラーム ポリシーを表示します。これらのアラームポリシーは、Web UI では編集できません。**[アクティブ化（Activate）]** または **[非アクティブ化（Disactivate）]** をクリックして、選択したポリシーをアクティブ化または非アクティブ化します。



GUI を使用してアラームポリシーが非アクティブ化された場合、そのポリシーに対して作成またはクリアされたアラームは、**[モニタ（Monitor）] > [アラーム（Alarm）] > [表示（View）]** タブに表示されません。ポリシーを削除するには、ポリシーの横にあるチェックボックスをオンにして、**[削除（Delete）]** をクリックします。ただし、GUI からはポリシーを削除しないことをお勧めします。ファブリックが削除されると、アラームポリシーとそのファブリック内のデバイスのすべてのアクティブアラームが削除されます。

ヘルス モニタ：アクティブ アラーム

[モニタ（Monitor）] > [アラーム（Alarm）] > [表示（View）] を選択して、アクティブなアラームを表示します。

アクティブなアラームをクリアするには、アラームの横にあるチェックボックスを選択し、**[ステータスを変更（Change Status）]**をクリックして **[クリア（Clear）]** を選択します。

アクティブなアラームを削除するには、アラームの横にあるチェックボックスを選択し、**[削除（Delete）]** をクリックします。

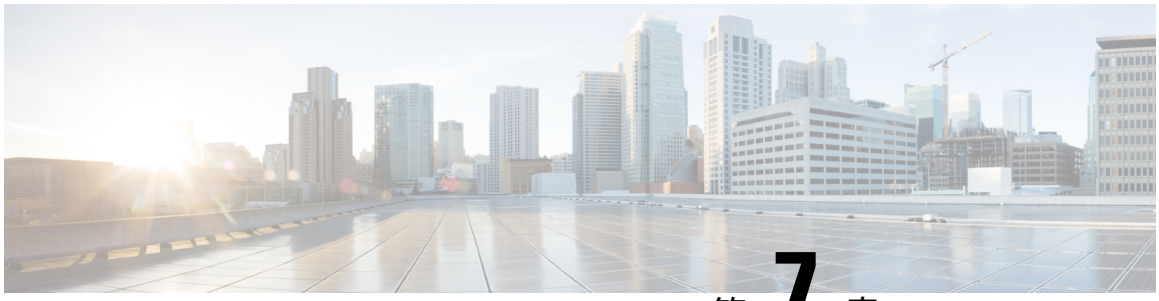
ヘルス モニタ：クリアされたアラーム

クリアされたアラームを表示するには **[モニタ（Monitor）]>[アラーム（Alarms）]>[表示（View）]>[クリアされたアラーム（Cleared Alarms）]**を選択します。

必須のアラームの詳細な情報を表示するには矢印アイコン ▶ をクリックします。

クリアされたアラームのリストからクリアされたアラームを削除するには、アラームの横にあるチェックボックスを選択し、**[削除（Delete）]** をクリックします。

アラームとポリシーの詳細については、「アラーム」を参照してください。



第 7 章

管理

この章は次のトピックで構成されています。

DCNM サーバ

DCNM メニューには次のサブメニューが含まれます。

サービスの開始、再開、停止

デフォルトでは DCNM とそのスイッチ間の ICMP 接続は、パフォーマンス管理中に接続を検証します。ICMP を無効にすると、パフォーマンス管理データはスイッチから取得されません。このパラメータは、**サーバー プロパティ**で構成できます。Cisco DCNM Web UI から ICMP 接続チェックを無効にするには、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバ プロパティ（Server Properties）]** を選択し、`skip.checkPingAndManageable` パラメータの値を `[true]` に設定します。

Performance Manager データベース（PM DB）の古いエントリをクリーンアップし、サービスを開始、再起動、または停止するには、Cisco DCNM Web UI から、次の手順を実行します。

Procedure

ステップ 1 **[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** を選択します。

サーバーの詳細を表示する **[ステータス（Status）]** ウィンドウが表示されます。

ステップ 2 **[アクション]** 列で、実行するアクションをクリックします。次の操作を実行できます。

- サービスを起動または再起動します。
- サービスを停止します。
- 古い PM DB エントリをクリーンアップします。
- Elasticsearch DB スキーマを再初期化します。

ステップ 3 **[ステータス（Status）]** 列でステータスを表示します。

What to do next

[ステータス（Status）] 列で最新のステータスを確認します。

Cisco DCNM リリース 11.4(1) から、次のサービスのステータスも表示できます。

Note 次のサービスは、OVA/ISO 展開でのみ利用できます。

- NTPD サーバー：DCNM OVA で実行されている NTPD サービス、IP アドレス、およびサービスがバインドされているポート。
- DHCP サーバー：DCNM OVA で実行されている DHCP サービス、IP アドレス、およびサービスがバインドされているポート。
- SNMP トラップ
- syslog レシーバ

これらのサービスの DCNM サーバーは次のとおりです。

サービス名	DCNM サーバー
NTPD サーバー	0.0.0.0:123
DHCP サーバー	0.0.0.0:67
SNMP トラップ	0.0.0.0:2162
[Syslogサーバ（Syslog Server）]	0.0.0.0:514

コマンド テーブルの使用

コマンド テーブルには、サーバー ステータスとサーバー管理ユーティリティ スクリプトに関する情報を提供する新しいダイアログ ボックスを起動するコマンドへのリンクが含まれています。これらのコマンドは、サーバー CLI で直接実行できます。

- **ifconfig**：このリンクをクリックして、Cisco DCNM サーバで使用されるインターフェイス パラメータ、IP アドレス、およびネットマスクに関する情報を表示します。

- **appmgr status all**：このリンクをクリックして、現在実行されているさまざまなサービスのステータスをチェックする DCNM サーバー管理ユーティリティ スクリプトを表示します。
- **appmgr show vmware-info**：このリンクをクリックして、仮想マシンの CPU とメモリに関する情報を表示します。
- **時計**：このリンクをクリックして、時間、ゾーン情報などのサーバークロックの詳細に関する情報を表示します。

Note コマンド セクションは、OVA または ISO のインストールにのみ適用されます。

カスタマイズ（Customization）

Cisco DCNM リリース 11.3(1) 以降、Web UI ログイン ページで背景画像とメッセージを変更できます。この機能は、同時に多数のインスタンスを実行している場合に、DCNMインスタンスを区別するのに役立ちます。ログイン ページで企業ブランドの背景を使用することもできます。[デフォルトに戻す（Restore Defaults）] をクリックして、カスタマイズを元のデフォルト値にリセットします。

カスタムを削除してデフォルト値に復元するには、**[デフォルトの復元（Restore defaults）]** をクリックします。

ログイン画像

この機能では、 Cisco DCNM Web UI のログイン ページの背景画像を変更できます。DCNM のインスタンスが多数ある場合、これは、背景画像に基づいて正しい DCNM インスタンスを識別するのに役立ちます。

Cisco DCNM Web UI ログイン ページのデフォルトの背景画像を編集するには、次の手順を実行します。

1. **[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [カスタマイズ（DCNM Server）]** を選択します。
2. ログイン画像領域で、**[追加（+）（Add (+)）]** アイコンをクリックします。

   ローカル ディレクトリからアップロードする必要がある画像を参照します。背景画像には、JPEG、GIF、PNG、IVL、および SVG のファイル形式を使用できます。
3. 画像を選択し、**[開く（Open）]** をクリックします。

   ステータス メッセージが右下隅に表示されます。

```
ログイン画像アップロード成功
```

（注） 読み込み時間を短縮するには、拡大縮小された画像をアップロードすることをお勧めします。

アップロードされた画像が選択され、背景画像として適用されます。

4. 既存の画像をログイン画像として選択するには、画像を選択し、右下隅にメッセージが表示されるまで待ちます。
5. デフォルトのログイン画像に戻すには、**[デフォルトに戻す（Restore Defaults）]**をクリックします。

本日のメッセージ（MOTD）

この機能を使用すると、Cisco DCNM Web UI ログイン ページにメッセージを追加できます。構成された頻度でローテーションするメッセージのリストを表示できます。この機能を使用すると、ログイン ページで重要なメッセージをユーザーに伝えることができます。

Cisco DCNM Web UI ログイン ページでその日のメッセージを追加または編集するには、次の手順を実行します。

1. **[管理（Administration）] > [DCNM サーバ] > [カスタマイズ（Customization）]** を選択します。
2. **[本日のメッセージ（MOTD）]**フィールドに、ログインページに表示する必要があるメッセージを入力します。
3. [保存（Save）] をクリックします。

オーバーレイ展開のデフォルト ファブリック

リリース 11.4(1) 以降、Cisco DCNM カスタマイズでは、有効なファブリックの 1 つをデフォルトとして選択できます。この機能は、Cisco DCNM LAN ファブリック展開でのみ使用できます。

Cisco DCNM Web UI ですべてのオーバーレイ展開のデフォルト ファブリックを設定するには、次の手順を実行します。

（注） デフォルトファブリックの構成を使用できるのは、**ネットワーク管理者**ロールを持つユーザーのみです。

1. **[管理（Administration）] > [DCNM サーバー] > [カスタマイズ（Customization）]** を選択します。
2. **[オーバーレイ展開のデフォルト ファブリック（Default Fabric for Overlay Deployments）]** ドロップダウン リストで、すべてのオーバーレイ展開のデフォルトとして設定するファブリックの設定を選択します。

3. **[保存]** をクリックして、ファブリックをデフォルトとして設定します。

   デフォルトファブリックが正常に更新されたことを確認するメモがウィンドウの右下に表示されます。

4. デフォルトのファブリックを削除するには、ドロップダウンリストから **--select as オプション**を選択し、**[保存（Save）]** をクリックします。

ネットワーク基本設定

リリース 11.5（1）より前の **appmgr update network-properties** コマンドでは、ネットワークプロパティを変更できます。リリース 11.5（1）以降、Cisco DCNM では、Web UI からいくつかのネットワーク パラメータを変更できます。これらを変更すると、以前に構成されたパラメータが上書きされます。

[Cisco DCNM **Web UI] > [管理（Admin）] > [DCNMサーバ（DCNM Server）] > [カスタム化（Customization）] > [ネットワーク基本設定（Network Preferences）]** を選択して、DNS、NTP、および eth1/eth2 インターフェイスを変更します。

DNS

ドメイン ネーム システム（DNS）フィールドに、ドメイン ネーム システム（DNS）の IP アドレスを入力します。IPv6 アドレスを使用して DNS サーバを設定することもできます。複数のドメイン ネーム システム（DNS）サーバを構成できます。IP アドレス間の差別化要因としてコンマ (,) を使用します。

Note Network Insights アプリケーションを使用している場合は、DNS サーバが有効で到達可能であることを確認します。

NTP

[NTP サーバー (NTP Server)] フィールドに、NTP サーバーの IP アドレスを入力します。値は IP または IPv6 アドレスか RFC 1123 に準拠した名前である必要があります。

ルート

インバンド (eth2)

[インバンド ネットワーク (In-Band Network)] 領域で、インバンド ネットワークの IPv4 アドレスおよびゲートウェイ IPv4 アドレスを入力します。DCNM が IPv6 ネットワーク上にある場合は、 IPv6 アドレス と ゲートウェイ IPv6 アドレス の関連する IPv6 アドレスを入力することで、ネットワークを構成します。

Note Nexus ダッシュボード サーバが DCNM 11.5(1) からサイトを追加する場合、データ ネットワーク経由で DCNM サーバに到達する必要があります。DCNM データ ネットワーク接続は、DCNM サーバの eth2 インターフェイスを介して定義されます。 DCNM のインバンド接続インターフェイスとも呼ばれます。Nexus ダッシュボードのデータ ネットワーク接続を使用した DCNM の eth2 接続が複数のサブネットにまたがっている場合、つまり、それらがレイヤ 3 ルートで接続されている場合、ND にサイトを追加する前に DCNM にルートを追加する必要があります。ダッシュレットのインバンド (eth2) 入力を介して ND データ ネットワークへのルートを入力します。

インバンド ネットワークにより、前面パネルのポートを介してデバイスへ到達可能になります。

[帯域外 (eth1)（Out-of-Band (eth1)）]

アウトオブバンド ネットワーク エリアで、IPv4 アドレスと ゲートウェイ IPv4 アドレスを入力します。DCNMがIPv6ネットワーク上にある場合は、IPv6アドレスとゲートウェイIPv6アドレスに関連するIPv6アドレスを入力して、ネットワークを設定します。

アウトオブバンド管理では、デバイス管理ポート (通常 mgmt0) への接続を提供します。

ログ情報の表示

Performance Manager、、SME サーバー、Web レポート、Web サーバー、および Web サービスのログを表示できます。しかし、これらのプロセスには、ログ ファイルの情報を表示できる GUI はありません。エラーを調べる場合は、表示できるようにこれらのファイルを保存してください。

リリース 11.2(1) 以降、DCNM OVA および DCNM ISO のインストールでは、.log 拡張子を持つすべてのログ ファイルもリストされます。

Note フェデレーション内のリモート サーバからログを表示することはできません。

Cisco DCNM Web UI からログを表示するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [ログ（Logs）]** を選択します。

左列にログのツリーベース リストが表示されます。ツリーの下には、フェデレーション内のすべてのサーバのノードがあります。ログ ファイルは、対応するサーバ ノードの下にあります。

ステップ 2 ツリーの各ノードの下にあるログ ファイルをクリックして、右側に表示します。

ステップ 3 各サーバのツリー ノードをダブルクリックして、そのサーバからログ ファイルを含む ZIP ファイルをダウンロードします。

ステップ 4 (Optional) **[テクニカル サポートの生成（Generate Techsupport）]** をクリックして、テクニカル サポートに必要なファイルを生成およびダウンロードします。

このファイルには、ログ ファイルに加えて詳細情報が含まれています。

Note OVA および ISO の展開では TAR.GZ ファイルがダウンロードされ、他のすべての展開では ZIP ファイルがダウンロードされます。 CLI で **appmgr tech_support** コマンドを使用して、techsupport ファイルを生成できます。

ステップ 5 (Optional) ログを印刷するには、右上隅の **[印刷（Print）]** アイコンをクリックします。

サーバ プロパティ

DCNM サーバで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。

バックアップ構成ファイルは、次のパスに保存されます：`/usr/local/cisco/dcm/dcnm/data/archive`

保持できるアーカイブ ファイルの数は **[デバイスあたり保持できる# アーカイブ ファイルの数：（# Number of archived files per device to be retained:）]** フィールドで設定されています。Cisco DCNM LAN ファブリックのインストールでは、バックアップはデバイスごとではなく、ファブリックごとに取得されます。バックアップ ファイルの数がフィールドに入力された値を超えると、バックアップの最初のバージョンが削除され、最新バージョンに対応します。たとえば、フィールドに入力された値が **50** の場合、ファブリックの 51 番目のバージョンがバックアップされると、最初のバックアップ ファイルが削除されます。

Cisco DCNM Web UI から DCNM 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。

Procedure

ステップ 1 **[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** を選択します。

ステップ 2 **[変更を適用（Apply Changes）]** をクリックしてサーバ設定を保存します。

モジュラ デバイスのサポート

大きな変更をあまり必要としない新しいハードウェアをサポートするために、次の DCNM リリースを待たずにパッチを配布できます。**[モジュラ デバイス サポート（Modular Device Support）]**は、DCNM パッチ リリースの配布と適用に役立ちます。認証された DCNM 管理者は、パッチを本番環境のセットアップに適用できます。パッチ リリースは、次のシナリオに適用されます。

- シャーシやライン カードなどの新しいハードウェアをサポート

- 最新の NX-OS バージョンをサポート
- 重要な修正をパッチとしてサポート

Cisco DCNM Web UI からパッチの詳細を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [モジュラ デバイス サポート（Modular Device Support）]** を選択します。

ウィンドウの左側に **[DCNM サーバ（DCNM Servers）]** 列が表示され、右側に **[文殊ら デバイス サポート上布（Modular Device support information）]** ウィンドウが表示されます。

ステップ 2 **[DCNM サーバ（DCNM Servers）]**を展開して、すべての DCNM サーバを表示します。

これには、**[モジュラ デバイス サポート情報（Modular Device support information）]** テーブルのバージョン番号、対応するプラットフォーム、サポートされるシャーシ、サポートされる NX-OS バージョン、PID サポート、バックアップ ディレクトリ、および最後のパッチ展開時間とともに、インストールされたパッチのリストが含まれます。

What to do next

パッチを適用してロールバックする方法の詳細については、http://www.cisco.com/go/dcnm を参照してください。

ネイティブ HA

Before you begin

Note フェデレーションのスイッチオーバーまたはフェイルオーバーの後は、毎回ブラウザのキャッシュと Cookie をクリアするようにしてください。

Procedure

ステップ 1 デフォルトでは、DCNM は組み込みデータベース エンジン PostgreSQL にバンドルされています。ネイティブ DCNM HA は、**アクティブ/ウォーム スタンバイ**として実行されている 2 つの DCNM によって実現され、組み込みデータベースはリアルタイムで同期されます。アクティブ DCNM がダウンすると、スタンバイは同じデータベースデータを引き継ぎ、操作を再開します。スタンバイ ホスト データベースの停止シナリオは、この手順の後に文書化されます。

ステップ 2 メニュー バーから、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [ネイティブ HA（Native HA）]** を選択します。

ネイティブ HA ウィンドウが表示されます。

ステップ 3 **[フェールオーバ（Failover）]**ボタンをクリックしてから**[OK]**をクリックすると、スタンバイ ホストへの DCNM の手動フェールオーバを許可できます。

- または、Linux コンソールからこのアクションを開始することもできます。

  a. DCNM アクティブ ホストに SSH で接続します。

  b. 「/usr/share/heartbeat/hb_standby」と入力します。

ステップ 4 **[強制同期（Force Sync）]** をクリックし、**[OK]** をクリックすると、データベースとディスク ファイルをスタンバイ ホストに手動で同期することができます。

ステップ 5 **[テスト（Test）]** をクリックしてから **[OK]** をクリックすると、HA セットアップをテストまたは検証できます。

What to do next

このサブセクションでは、いくつかのHAトラブルシューティング シナリオについて説明します。

スタンバイ ホスト データベースがダウンしています：通常、DCNMデータベース（PostgreSQL）はアクティブ ホストとスタンバイ ホストでアップしていますDCNM 10.1 以前のバージョンでは、データベース同期の失敗によりスタンバイ データベースがダウンする場合があります。

- 「ps -ef | grep post」と入力します。複数の postgres プロセスが実行されていることがわかります。そうでない場合は、データベースがダウンしていることを示しています。
- データベース同期の開始時に作成されたバックアップ ファイルからデータベース データを復元します。ディレクトリを「/usr/local/cisco/dcm/db」に変更します
- ファイル replication/ pgsql-standby-backup.tgz の存在を確認します。ファイルが存在する場合は、データベース データ ファイルを復元します。

```
rm -rf    data/*
tar -zxf    replication/ pgsql-standby-backup.tgz    data
/etc/init.d/postgresql-9.4 start
ps -ef | grep post
```

アクティブな DCNM ホストは、2 つのデータベースを同期します。

TFTP サーバはアクティブ ホストの eth1 VIP アドレスにバインドされていません : TFTP サーバはアクティブ ホスト (スタンバイ ホストではなく) で実行する必要があり、eth1 VIP アドレスにバインドする必要があります。一部のセットアップでは、TFTP 設定ファイルによるとバインドアドレスが VIP アドレスではないため、スイッチが TFTP を使用しようとしたときに問題が発生する可能性があります。

- 「grep bind /etc/xinetd.d/tftp」と入力して、TFTP 設定ファイルに正しいバインド アドレスがあるかどうかを確認します。表示された IP アドレスが eth1 VIP アドレスでない場合は、バインド アドレスを VIP アドレスに変更します。新しいスタンバイ ホストに対してこの手順を繰り返します。バインド アドレスを VIP アドレスに更新します。
- アクティブ ホストで " " /etc/init.d/xinetd restart" と入力して、TFTP を再起動します。

Note TFTP サーバーは、「appmgr start/stop ha-apps」コマンドで開始または停止できます。

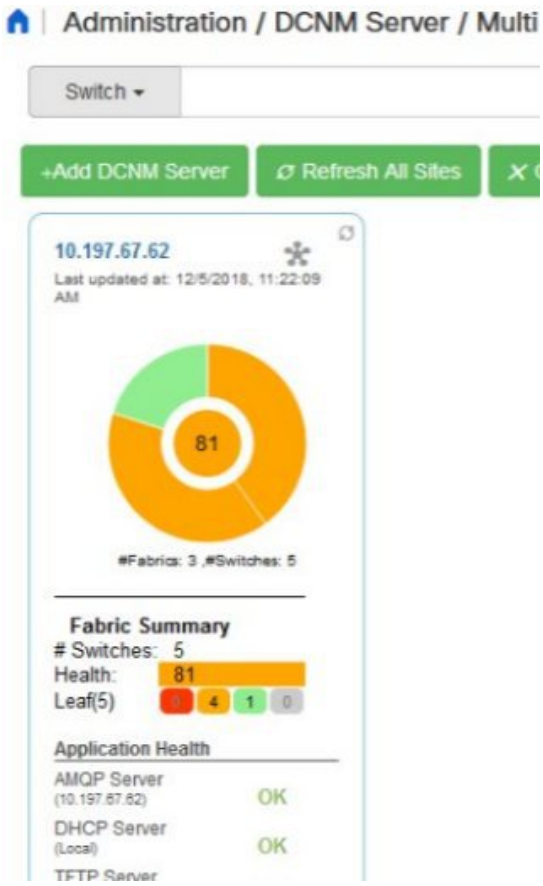
マルチ サイト マネージャ

Multi Site Manager を使用すると、DCNM サーバ アプリケーションの状態を表示し、ローカル サイトとリモート サイトのスイッチのスイッチ情報を取得できます。リモート DCNM サーバのスイッチ情報にアクセスするには、そのサーバを Multi Site Manager に登録する必要があります。リモート DCNM サーバにアクセスし、スイッチ情報を検索する手順について説明します。

リモート DCNM サーバ情報の追加

この手順により、現在ログオンしている DCNM サーバからリモート サイトの DCNM サーバにアクセスできます。リモート サイトが現在の DCNM サーバにアクセスするには、リモート サイトでの登録が必要です。

1. **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [Multi Site Manager]**を選択します。Multi Site Manager 画面が表示されます。



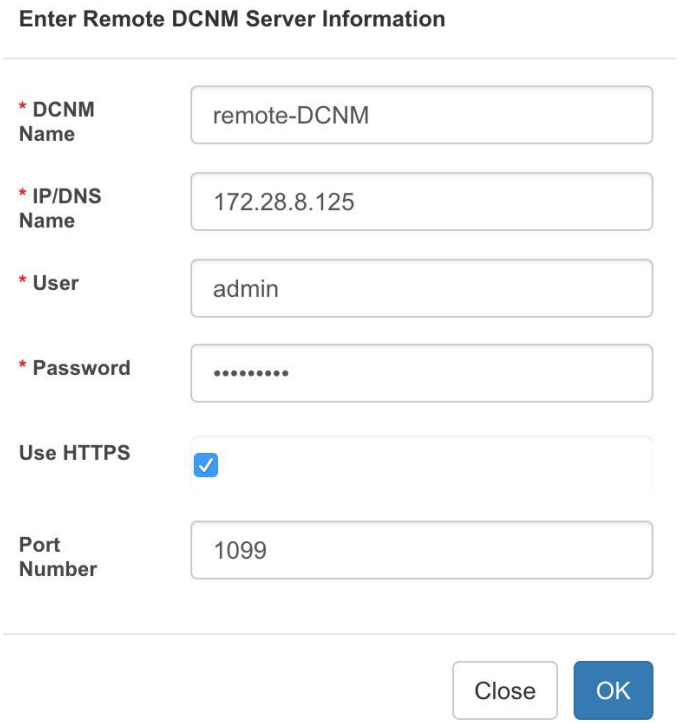
現在ログオンしている DCNM アプリケーションのヘルス ステータスが画面に表示されます。

Note **アプリケーション ヘルス**機能は、DCNM ISO/OVA インストール タイプでのみ使用でき、Windows/RHEL インストール タイプでは使用できません。

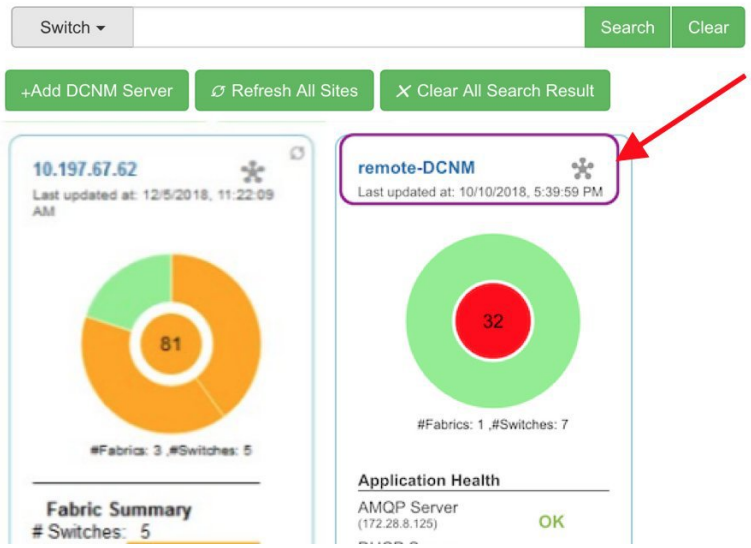
2. **[+ DCNM サーバの追加（+Add DCNM Server）]** をクリックします。**[リモート DCNM サーバ情報の入力（Enter Remote DCNM Server Information）]** 画面が表示されます。

   リモート DCNM サーバ名、その IP アドレスまたは URL、リモート DCNM サーバのユーザ クレデンシャル、およびオプションでポート番号を入力します。

Note **[HTTPS を使用（Use HTTPS）]** チェック ボックスを無効にしないでください。無効にすると、DCNM にアクセスできなくなります。



3. [OK] をクリックします。検証後、リモート DCNM サーバが画面のローカル DCNM サーバの隣に表示されます。



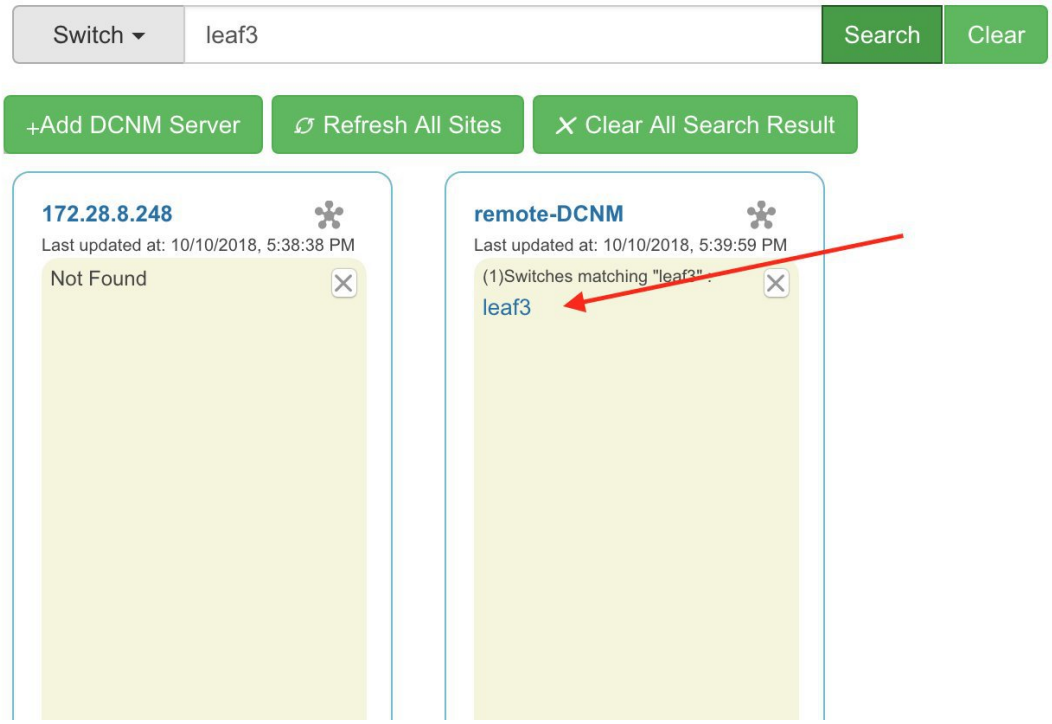
[すべてのサイトを更新（Refresh All Sites）] をクリックして、更新された情報を表示できます。

スイッチ情報の取得

1. **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [Multi Site Manager]**を選択します。Multi Site Manager 画面が表示されます。
2. 画面上部の検索ボックスから、次のいずれかのパラメータに基づいてスイッチを検索します。
   - VM 情報（**[VM IP]** および **[VM 名（VM Name）]**フィールド）：接続された VM の IP アドレスまたは名前。
   - スイッチ情報（**[スイッチ（Switch）]**および**[MAC]**フィールド）：スイッチの名前または MAC アドレス。
   - スイッチ上に存在するセグメント（**[セグメント ID（Segment ID）]** フィールド）。

   一致する場合、スイッチ名は適切なローカルまたはリモート DCNM サーバの図の検索ボックスの下にハイパーリンクとして表示されます。

   この例では、スイッチ **leaf3** は、DCNM サーバによって管理されるリモート サイトで使用できます。**Leaf3** へのリンクは、**リモート DCNM** パネルで使用できます。



3. **Leaf3** をクリックして、隣接するブラウザタブに詳細なスイッチ情報を表示します。

   いつでも、**[トポロジ ビューの開始（Launch Topology View）]** アイコンをクリックして、ファブリックのトポロジを表示できます。

デバイス コネクタ

デバイスコネクタは、クラウドベース管理プラットフォームであるCisco Intersightの機能を実現する組み込み管理コントローラです。

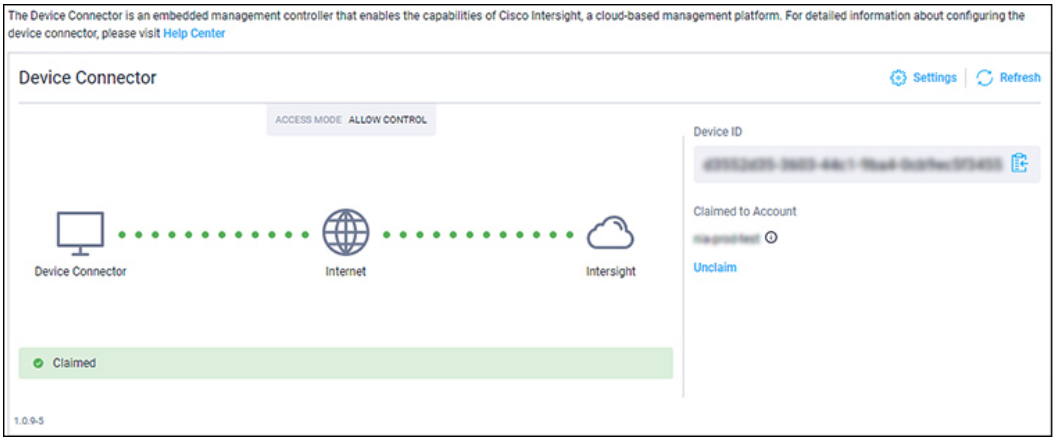
Networks Insights アプリケーションは、Cisco DCNM プラットフォームの管理コントローラに組み込まれているデバイス コネクタを介して Cisco Intersight クラウド ポータルに接続されます。Cisco Intersight は、Network Insights アプリケーションを介してデバイスを管理およびモニタするのに役立つ仮想アプライアンスです。デバイス コネクタは、接続されている DCNM に対して、セキュリティで保護されたインターネット接続を使用して情報を送信し、Cisco Intersight ポータルから制御命令を受信できる安全な方法を提供します。

デバイス コネクタの構成

Cisco DCNM Web UI からデバイス コネクタを構成するには、次の手順を実行します。

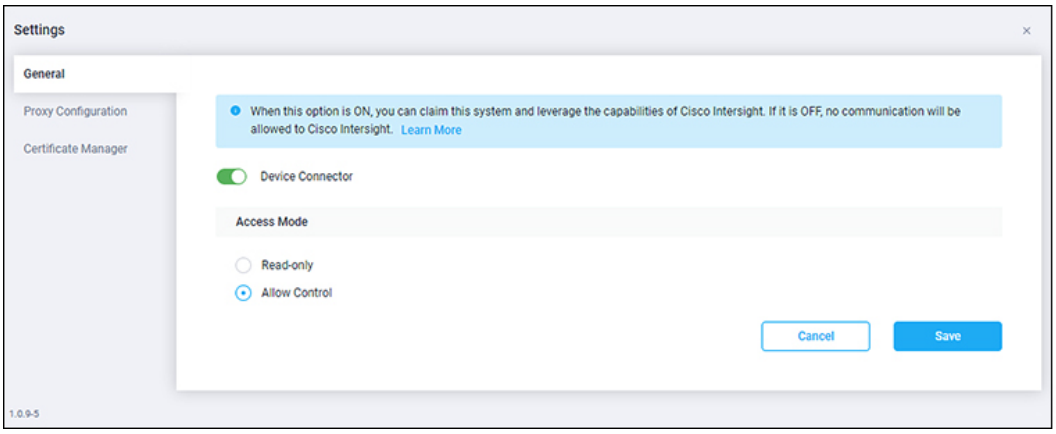
1. **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [デバイス コネクタ（Device Connector）]** を選択します。

   [デバイス コネクタ（Device Connector）] 作業ウィンドウが表示されます。



2. [設定（Settings）] をクリックします。

   [設定 - 全般（Settings - General）] ウィンドウが表示されます。



- **デバイス コネクタ（スイッチ）**

  これは、Cisco Intersight とのデバイス コネクタ通信のメイン スイッチです。スイッチがオンの場合（緑色のハイライト）、デバイス コネクタはシステムを要求し、Cisco Intersight の機能を活用します。スイッチがオフの場合（灰色の強調表示）、Cisco DCNM と Cisco Intersight の間で通信を行うことができません。

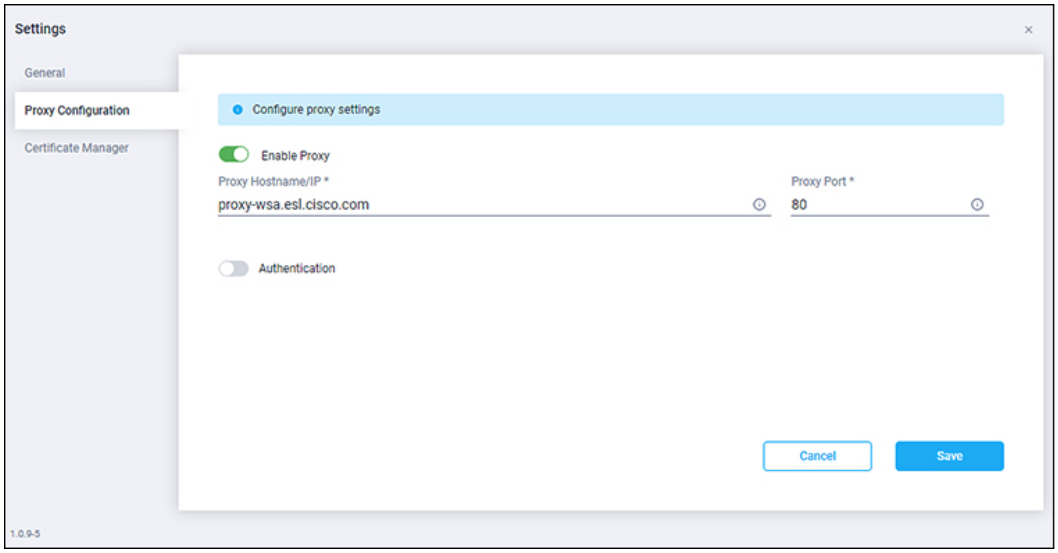
- **アクセス モード**

  - **[読み取り専用（Read-only）]**：このオプションは、Intersight からこのデバイスに変更が加えられないことを保証します。たとえば、ファームウェアのアップグレードやプロファイルの展開などのアクションは読み取り専用モードでは許可されません。ただし、アクションは特定のシステムで使用可能な機能によって異なります。

  - **[制御を許可（Allow Control）]**：このオプション（デフォルトで選択）を使用すると、Cisco Intersight で使用可能な機能に基づいて、クラウドからすべての読み取り/書き込み操作を実行します。

3. [デバイス コネクタ（Device Connector）] をオン（緑のハイライト）に設定し、**[制御を許可（Allow Control）]** を選択します。
4. **[プロキシ構成（Proxy Configuration）]** をクリックします。

   [設定 - プロキシ構成（Settings - Proxy Configuration）] ウィンドウが表示されます。



- **プロキシを有効にする（スイッチ）**

  [HTTPS プロキシ（HTTPS Proxy）] を有効にしてプロキシを構成します。

（注） Network Insights にはプロキシ設定が必要です。

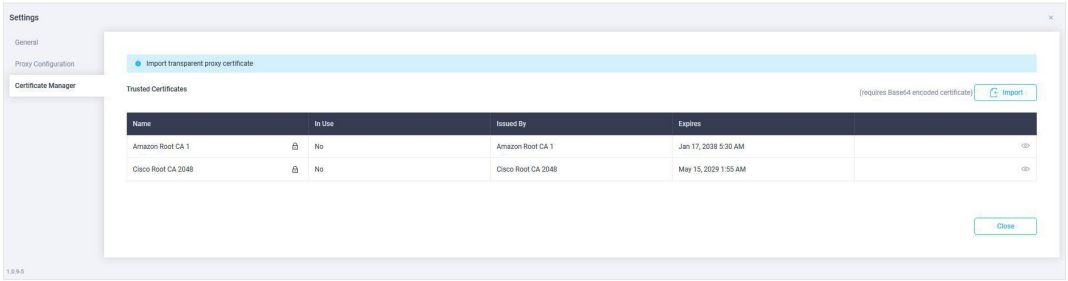
- **プロキシ ホスト名/IP* およびプロキシ ポート***：プロキシ ホスト名または IP アドレス、およびプロキシ ポート番号を入力します。
- **認証（スイッチ）**

  認証を通じてプロキシアクセスを有効にします。スイッチがオンの場合（緑色のハイライト）、プロキシ サーバへの認証が必要です。スイッチがオフ（灰色のハイライト）の場合、認証は必要ありません。

  ユーザー名*とパスワード：認証用のユーザー名とパスワードを入力します。

  デバイス コネクタには必須のログイン クレデンシャルのフォーマットはないので、入力したクレデンシャルがそのまま構成済み HTTP プロキシ サーバに渡されます。ドメイン名でユーザー名を限定する必要があるかどうかは、HTTP プロキシ サーバーの構成によって異なります。

5. プロキシを有効にし（緑色のハイライト）、ホスト名とポート番号を入力します。
6. （オプション）プロキシ認証が必要な場合は、それを有効にして（緑色のハイライト）、ユーザー名とパスワードを入力します。
7. [保存（Save）] をクリックします。
8. **[証明書マネージャ（Certificate Manager）]** をクリックします。



信頼できる証明書がテーブルに表示されます。

信頼できる証明書の一覧が表示されます。有効な信頼できる証明書をインポートできます。

- **[インポート（Import）]**

  ディレクトリを参照し、CA 署名付き証明書を選択してインポートします。

（注） インポートされた証明書が ***.pem（base64 エンコード）** 形式である必要があります。

- 次の情報と証明書のリストを表示することができます。
  - **[名前 (Name)]**—CA 証明書の共通名。

- **[使用中（In Use）] -** トラストストアで証明書を正常にリモート サーバの確認に使用されたかどうか。
- **[Issued By]**: 証明書の発行認証局。
- **[Expires]**—証明書の有効期限。

（注） バンドルされた証明書は削除できません。

スイッチの NX API 証明書管理

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。スイッチ コンソールで CLI コマンドを使用して、証明書を手動でインストールできます。

リリース 11.4(1) から、Cisco DCNM では、NX-API 証明書を DCNM 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、DCNM 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。

この機能は、Cisco DCNM OVA/ISO 展開でのみサポートされます。

（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。

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 DCNM 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 ファイルのコンテンツも含めることができます。

DCNM 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 DCNM は暗号化を義務付けていません。ただし、これは DCNM 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。DCNM は AES 暗号化をサポートします。

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 DCNM 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、DCNM 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、DCNM 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、DCNM はスイッチに証明書をインストールできません。

Cisco DCNM 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） DCNM 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、DCNM 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 **DCNM Web UI] > [管理（Administration）] > [DCNM サーバ（DCNM Server）] > [NX API 証明書（NX API Certificates）]** に、次のテーブルが表示されます。

- **[証明書インストール ステータス（Certificate Installation Status）]** テーブル：スイッチに最後にインストールされた証明書のステータスを表示します。また、証明書が以前に更新された時刻も表示されます。
- **[DCNM にアップロードされた証明書（Certificates Uploaded to DCNM）] テーブル**：DCNM およびスイッチ アソシエーションにアップロードされた証明書を表示します。

  ただし、証明書とスイッチの関連付けを確認するには、証明書のインストール ステータスの表を参照してください。アップロードテーブルは、DCNM に証明書をアップロードし、スイッチにインストールするためだけのものです。

また、スイッチ NX-API SSL 証明書管理機能の使用方法を示すビデオを見ることもできます。ビデオ：NX-API SSL 証明書管理の切り替えを参照してください。

DCNM での証明書のアップロード

Cisco DCNM Client Web UIを使用して証明書を DCNM にアップロードするには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [NX API 証明書（NX API Certificates）]** を選択します。

ステップ 2 適切なライセンス ファイルをアップロードするには **[DCNM にアップロードされた証明書（Certificates Uploaded to DCNM）]** エリア内にある **[証明書をアップロード（Upload Certificates）]** をクリックします。

ステップ 3 ローカル ディレクトリを参照し、DCNM 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 DCNM 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。

ステップ 4 **[開く (Open)]** をクリックし、選択したファイルを DCNM 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は、**[DCNMにアップロードされた証明書（Certificates Uploaded to DCNM）]** エリアに表示されます。

[証明書のインストール ステータス（Certificate Installation Status）] エリアに、ステータスが **UPLOADED** である証明書が表示されます。

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。

スイッチでの証明書のインストール

Cisco DCNM 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。

手順

ステップ 1 **[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [NX API 証明書（NX API Certificates）]** を選択します。

ステップ 2 **[証明書のインストール ステータス（Certificate Installation Status）]** 領域で、証明書ごとに **[スイッチ（Switch）]** 列をクリックします。

ステップ 3 ドロップダウン リストから、証明書に関連付けるスイッチを選択します。

[保存（Save）] をクリックします。

ステップ 4 インストールする必要がある証明書を選択し、**[スイッチに証明書をインストール（Install Certificates on Switch）]** をクリックします。

複数の証明書を選択して、一括インストールを実行できます。

ステップ 5 **[一括証明書インストール（Bulk Certificate Install）]** ウィンドウで、証明書を DCNM にアップロードします。次の操作を行ってください。

一括インストール機能を使用して、同じインスタンスに最大 20 の証明書をインストールできます。

a) 証明書を DCNM にアップロードするためのファイル転送プロトコルを選択します。

証明書をアップロードするために、SCP または SFTP プロトコルを選択できます。

b) VRF 構成をサポートする証明書の VRF チェックボックスをオンにします。

スイッチが DCNM に到達するために使用する VRF 名を入力します。一般に、DCNM にはスイッチの管理 VRF を介して到達しますが、DCNM に到達するために使用されるスイッチで構成されている任意の VRF に到達できます。

c) NX-API 証明書資格情報に、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。

証明書とともにアップロードされたキーが暗号化されていない場合は、このフィールドを空のままにします。

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ることに注意てください。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。

d) [インストール（Install）] をクリックします。

証明書が特定のスイッチに正常にインストールされたかどうかを確認する通知メッセージが表示されます。

証明書のインストール ステータス エリアで、証明書のステータスに「**インストール済み**」が表示されるようになりました。

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、DCNM は DCNM 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、DCNM 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 DCNM はスイッチの証明書を削除できません。

Cisco DCNM Web UI を使用してDCNM レポジトリから証明書を削除するには、以下の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [NX API 証明書（NX API Certificates）]** を選択します。

ステップ 2 **[証明書のインストール ステータス（Certificate Installation Status）]** 領域で、削除する必要がある証明書を選択します。

ステップ 3 **[クリア（Clear）]** 認証書をクリックします。

確認メッセージが表示されます。

ステップ 4 **[OK]** をクリックして、選択した証明書をクリアします。

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。

ステップ 5 証明書を選択し、**[証明書のクリア（Clear Certificates）]** をクリックします。

証明書が [証明書のインストール ステータス（Certificate Installation Status）] テーブルから削除されます。

ステップ 6 DCNMエリアにアップロードされている証明書で、スイッチから現在、リンク解除されている証明書を選択します。

[証明書を削除（Delete Certificates）]をクリックします。

証明書は DCNM から削除されます。

NX API 証明書管理のトラブルシューティング

証明書のインストール中にエラーが発生することがあります。次のセクションでは、スイッチの NX-API 証明書管理のトラブルシューティングについて説明します。

COPY_INSTALL_ERROR

問題文 : エラー メッセージ COPY_INSTALL_ERROR

理由 Cisco DCNM がスイッチに到達できません。

解決策 :

- スイッチが Cisco DCNM から到達可能かどうかを確認します。SSH ログインを実行し、スイッチに ping を実行して確認できます。
- スイッチは、その管理インターフェイスを介して DCNM に接続します。スイッチ コンソールから DCNM に ping できるかどうかを確認します。スイッチが VRF を必要とする場合、正しい vrf が提供されている場合。
- 証明書の秘密鍵が暗号化されている場合は、正しいパスワードを指定してください。
- 正しいキー ファイルが証明書とともにアップロードされていることを確認します。証明書ファイルとキー ファイルが同じファイル名であることを確認します。

CERT_KEY_NOT_FOUND

問題文：Error message CERT_KEY_NOT_FOUND

理由：証明書（.cer、.crt、.pem）のアップロード中にキー ファイルがアップロードされませんでした。

解決策：

- 証明書（.cer、.crt、または.pem）ファイルとそれに対応する .key ファイルのファイル名が同じであることを確認します。

  例：証明書ファイル名が mycert.crt の場合、キー ファイルも mycert.key である必要があります。

- DCNM はキー ファイルを証明書ファイル名で識別します。したがって、キー ファイルは同じファイル名にする必要があります。
- 証明書とキー ファイルを同じファイル名でアップロードし、証明書をインストールします。

DCNM のバックアップ

Cisco DCNM リリース 11.5（1） から、Cisco DCNM Web UI からスケジュールされた DCNM バックアップをトリガーできます。Web UI からバックアップをトリガすると、**appmgr backup** コマンドが実行されます。**[バックアップ（Backup）]** ウィンドウの **[サーバ バックアップ ジョブ（Server Backup Jobs）]** タブに、次の情報が表示されます。

Table 22: サーバ バックアップ ジョブ タブ

パラメータ	説明
ノード	バックアップがアクティブかスタンバイかを指定します。スタンドアロン ノードの場合、ローカルパスとして表示されます。 **Note** HA クラスタの場合、1 つのアクティブ ノードと 1 つのスタンバイ ノードが作成されます。ただし、HA クラスタにはアクティブ ノードのみを選択できます。
スケジュール	スケジュールされたバックアップがいつトリガーされるかを指定します。
ローカルパス	バックアップが保存されるローカル パスを指定します。
リモート宛先	バックアップが保存されるユーザー名、ホストIP、およびリモート宛先を指定します。バックアップをリモートの場所に保存しない場合は空です。 **Note** バックアップのコピーもローカルパスに保存されます。
ログパス	ログエントリが保存されるパスを指定します。この情報を使用して、問題をトラブルシューティングできます。
保存されたバックアップ	バックアップのバージョン数を指定します。デフォルト値は 5 です。

[バックアップ（Backup）] ウィンドウで次のアクションを実行できます。

バックアップの作成

Cisco DCNM ウェブ UI からバックアップを作成するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]> [DCNM サーバ（DCNM Server）]> [バックアップ（Backup）]** を選択します。

[サーバ バックアップスケジュール（Server Backup Schedules）] 領域の下で全ての情報を持っている**[バックアップ（Backup）]** ウィンドウが表示されます。

ステップ 2 [追加（Add）] をクリックします。

[バックアップ スケジュールを作成（Create Backup Schedule）] ダイアログ ボックスが表示されます。

ステップ 3 **[スケジュール（schedule）]** 領域の **[開始時刻（Start At）]** ドロップダウン リストを使用して時間を選択します。

ステップ 4 バックアップの周波数を次から選択します。

有効なオプションは次のとおりです。

- **[毎日（Daily）]** : 毎日バックアップをトリガする場合は、このラジオ ボタンを選択します。
- **[毎週（Weekly）]** : 週に 1 回バックアップをトリガする場合は、このラジオ ボタンを選択します。このラジオ ボタンを選択すると、曜日を選択するオプションが表示されます。

ステップ 5 保存するバックアップの数を、**[宛先（Destination）]** エリアの下の **[保存されたバックアップの最大数（Max # of Saved Backups）]** フィールドに入力します。

最大 10 個のバックアップを保存でき、デフォルト値は 5 です。

ステップ 6 （任意） リモートの場所にバックアップを保存するには、**[リモートの宛先（Remote Destination）]** チェックボックスをオンにします。

[リモート処理接続先（Remote Destination）] チェックボックスをオンにすると、次のフィールドが使用可能になります。

フィールド	説明
User	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） DCNM とリモート ホスト間のキーレス構成を有効にしている場合は、パスワードを入力する必要はありません。
ホスト IP	DCNM に接続されているホストの IP アドレスを入力します。
パス	バックアップを保存するリモート処理の接続先パスを入力します。

（注）
- バックアップ ファイルは巨大で、サイズはギガバイトです。
- バックアップのコピーは常にローカルの接続先にも保存されます。

ステップ 7 [作成（Create）] をクリックします。

CLI を使用して **appmgr backup** コマンドを実行しても、**[バックアップ（Backup）]** ウィンドウにデータが入力されます。また、**appmgr backup schedule show** コマンドを使用して、CLI で Web UI からスケジュールしたバックアップを表示することもできます。

バックアップの変更

Cisco DCNM Web UI からバックアップを変更するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]> [DCNM サーバ（DCNM Server）]> [バックアップ（Backup）]** を選択します。

[サーバ バックアップスケジュール（Server Backup Schedules）] 領域の下で全ての情報を持っている**[バックアップ（Backup）]** ウィンドウが表示されます。

ステップ 2 [変更（Modify）] をクリックします。

[バックアップ スケジュールの変更（Modify Backup Schedule）] ダイアログ ボックスが表示されます。

ステップ 3 必要な変更を加えます。

ステップ 4 [変更（Modify）] をクリックします。

バックアップを削除

Cisco DCNM ウェブ UI からバックアップを削除するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]> [DCNM サーバ（DCNM Server）]> [バックアップ（Backup）]** を選択します。

[サーバ バックアップスケジュール（Server Backup Schedules）] 領域の下で全ての情報を持っている**[バックアップ（Backup）]** ウィンドウが表示されます。

ステップ 2 [削除（Delete）] をクリックします。

確認用のダイアログボックスが表示されます。

ステップ 3 **[はい（Yes）]** をクリックします。

（注） CLI で **appmgr backup schedule none** コマンドを実行すると、バックアップが削除されます。**[バックアップ（Backup）]** ウィンドウを更新すると、バックアップが削除されたかどうかを確認できます。

ジョブ実行の詳細

[バックアップ（Backup）] ウィンドウの **[ジョブ実行の詳細（Job Execution Details）]** タブに、次の情報が表示されます。

Table 23: サーバのバックアップ スケジュール エリア

パラメータ	説明
ノード	ノードがアクティブかスタンバイかを指定します。スタンドアロン ノードの場合、ローカル ノードとして表示されます。
ファイルのバックアップ	バックアップが保存されるパスを指定します。
Start Time	バックアップ プロセスが開始された時刻を指定します。
終了時刻	バックアップ プロセスが終了した時刻を指定します。
ログ ファイル	ログエントリが保存されるパスを指定します。この情報を使用して、問題をトラブルシューティングできます。
Status	バックアップが成功したか失敗したかを指定します。
エラーメッセージ	バックアップ中に表示されたエラー メッセージがあれば、それを指定します。

ライセンスの管理

[ライセンス付与の管理 (Manage Licensing)] メニューには、次のサブメニューがあります。

ライセンスの管理

[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] を選択すると、既存の Cisco DCNM 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。

- ライセンスの割り当て
- スマート ライセンス
- サーバ ライセンス ファイル

Note デフォルトでは、**[ライセンスの割り当て（License Assignments）]** タブが表示されます。

次の表に、SAN および LAN のライセンス情報を示します。

フィールド	説明
License	SANまたはローカルエリアネットワーク（LAN）を指定します。
無料/合計サーバベースのライセンス	ライセンスの総数のうち、購入する無料ライセンスの数を指定します。新規インストールのライセンスの総数は 50 です。ただし、インライン アップグレードの場合、ライセンスの合計数は 500 のままになります。
ライセンスなし/合計（スイッチ/VDC）	スイッチまたはVDCの総数のうち、ライセンスのないスイッチまたは VDC の数を指定します。
購入する必要があります	購入するライセンス数を指定します。

このセクションは、次のトピックで構成されています。

ライセンスの割り当て

次の表に、すべてのスイッチまたは VDC のライセンス割り当ての詳細を示します。

フィールド	説明
グループ	グループがファブリックか LAN かを表示します。
スイッチ名	スイッチの名前が示されます。
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。

フィールド	説明
ライセンスの状態	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 • 評価用 • Unlicensed • N/A • Expired • 無効 • スマート
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。 • DCNM サーバー • スイッチ • スマート • オナー • スイッチ スマート
期限日 （Expiration Date）	ライセンスの有効期限日が表示されます。 **Note** **[有効期限日（Expiration Date）]** 列の下のテキストは、7日で期限切れになるライセンスの場合は赤で表示されます。
ライセンスの割り当て	行を選択し、ツールバーでこのオプションをクリックしてライセンスを割り当てます。
ライセンスの割り当てを解除	ライセンスの割り当てを解除するには、行を選択し、ツールバーのこのオプションをクリックします。
すべて割り当て	ツールバーのこのオプションをクリックして表を更新し、テーブル内のすべてのアイテムにライセンスを割り当てます。
すべて割り当て解除	ツールバーのこのオプションをクリックしてテーブルを更新し、すべてのライセンスの割り当てを解除します。

Note ライセンスの割り当てまたは割り当て解除を行うには、ネットワーク管理者権限が必要です。

ファブリックが最初に検出されたときに、スイッチに有効なスイッチベースのライセンスがない場合、ライセンスはファイルライセンスプールからファブリックに自動的に割り当てられ、プール内にライセンスが残っていない状態になります。既存のファブリックがあり、新しいスイッチがファブリックに追加された場合、ファイル ライセンス プールで使用可能なライセンスがあり、まだスイッチベースのライセンスがない場合は、新しいスイッチにライセンスが割り当てられます。

スマート ライセンスを登録した後、永久ライセンスを持たないスイッチの **[ライセンスの割り当て]** をクリックすると、スマート ライセンスがスイッチに割り当てられます。割り当てられるライセンスの優先順位は、次の順序です。

1. **永続**
2. **スマート**
3. **評価用**

POAP を介してスイッチにライセンスを割り当てるには、『DCNM ライセンス ガイド』を参照してください。

スマート ライセンスを無効にすると、スマート ライセンスされたスイッチのライセンスの割り当てが解除されます。

評価ライセンスは、スマートライセンスをサポートしていないスイッチに割り当てられます。ライセンス状態は **Eval** で、ライセンス タイプは **DCNM-Server** です。スマート ライセンスをサポートするスイッチのリストを表示するには、『*Cisco DCNM* ライセンス ガイド、リリース *11.x*』を参照してください。

オナー ライセンス モード

リリース 11.3(1) から、Cisco DCNM 評価ライセンスの有効期間が 30 日から 60 日に延長されました。つまり、60日後です。すべてのライセンスには、有効期限が付いています。ライセンスの有効期限が切れると、Cisco DCNM では、ライセンスされたすべての機能を使用できるようになります。スイッチが再度ライセンスを付与されるか、ライセンスを手動で削除するまで、スイッチはオナーモードのままになります。

ライセンス オナー モードのスイッチがある場合、DCNM にログオンした後にエラー メッセージが表示されます。

```
**************************************
*Your licenses are out of compliance.
Your inventory contains switches that are unlicensed for DCNM Operation*

**************************************
```

[管理（Administration）] > [ライセンシングの管理（Manage Licensing）] > [DCNM] に移動し、**[スイッチ/VDC（Switches/VDCs）]** テーブルでスイッチを選択し、**[ライセンスの割当（Assign License）]** をクリックしてライセンスを更新します。

ガイドライン

- ライセンスが割り当てられていないスイッチは、ライセンスがないと見なされます。ライセンスのないスイッチは、ライセンスが必要な DCNM 機能を使用できません。

- スイッチに期限切れの EVAL ライセンスがある場合、EVAL から オナー モードに変更され、ライセンス機能は引き続き動作します。
- 期限切れの EVAL ライセンスをスイッチに割り当てることはできません。
- スイッチベースのオナー ライセンスを持つスイッチは、サーバーベースのライセンスで上書きすることはできません。
- 検出されたスイッチにライセンスが割り当てられていて、有効なライセンスが利用できない場合、有効期限付きの優先ベースのライセンスがスイッチに割り当てられます。

名誉モード ライセンスのナグ イベント

オナー モードのすべてのライセンスについて、7 日ごとにイベントが生成されますnag イベントは、ユーザーに「DCNM-SAN ファイル ライセンスはオナー モードです。このスイッチに新しいライセンスを割り当てる/購入する必要があります」と通知します。または、「DCNM-LAN ファイル ライセンスはオナー モードです。このスイッチに新しいライセンスを割り当てる/購入する必要があります。」

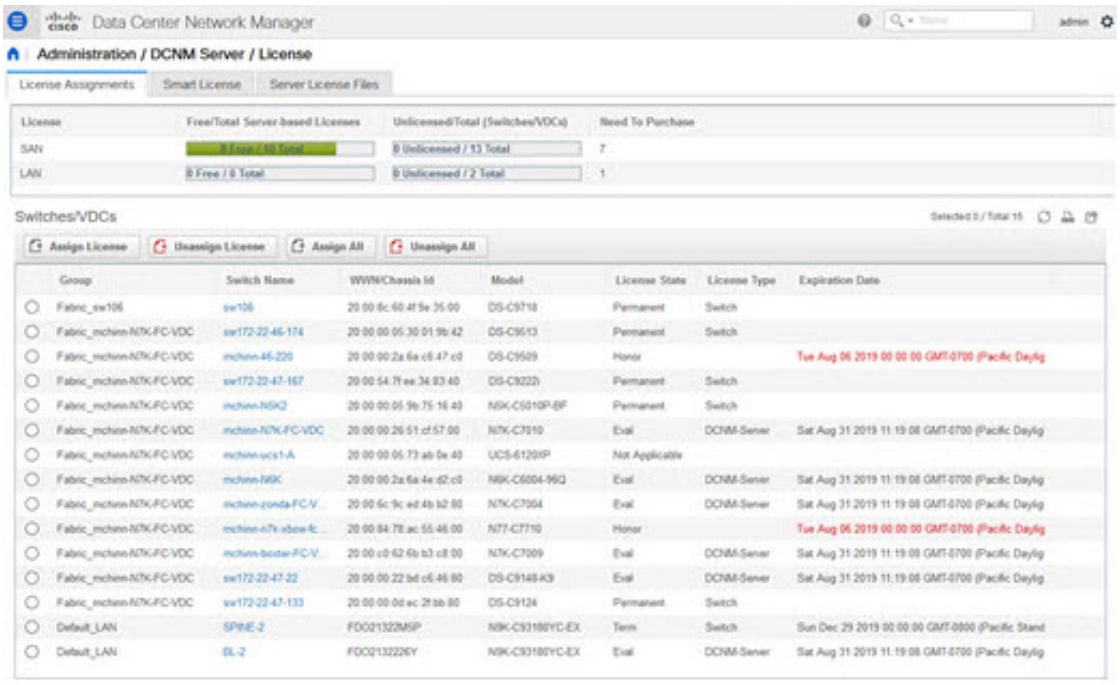
Cisco DCNM にログオンすると、追加のポップアップ通知が表示され、「DCNM-SAN ファイル ライセンスはオナー モードです。このスイッチに新しいライセンスを割り当てる/購入する必要があります」という通知が表示されます。

サーバーベースのオナー ライセンスのサポート

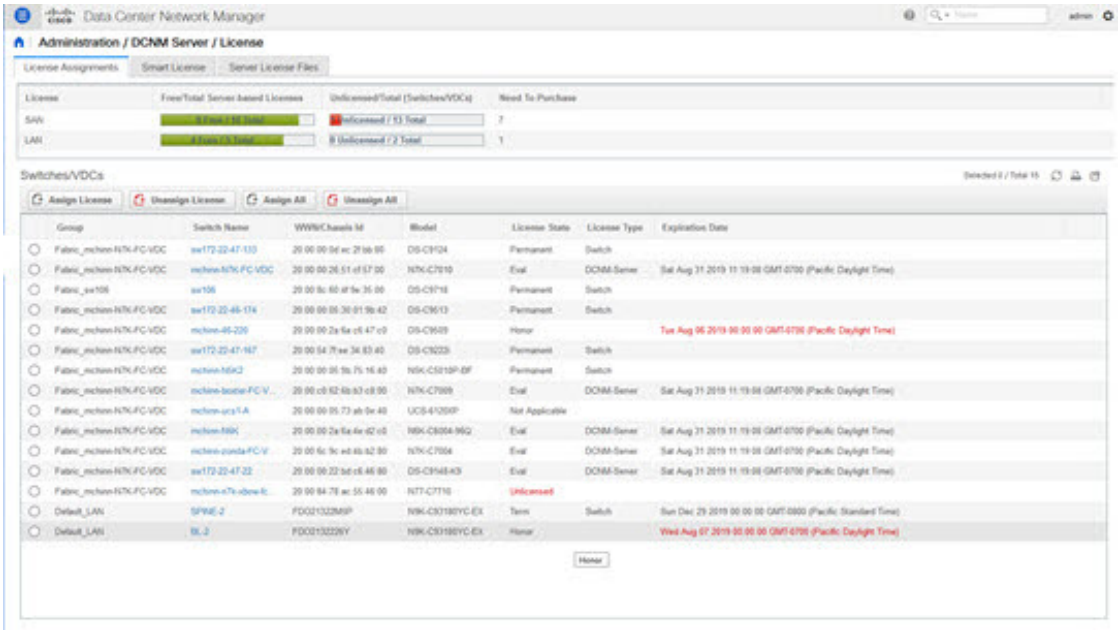
DCNM **Web UI > [管理] > [ライセンスの管理] > [DCNM]** で、**[ライセンスの状態]** 列に [名誉] が表示され、**[有効期限日]** 列に、ライセンスが期限切れになって**オナー** モードに変更された日時が表示されます。

スイッチは、再起動後もオナー モードのままになります。ライセンスをオナーモードから変更するには、ライセンスの割り当てを手動で解除するか、新しい有効なライセンスをスイッチに割り当てる必要があります。

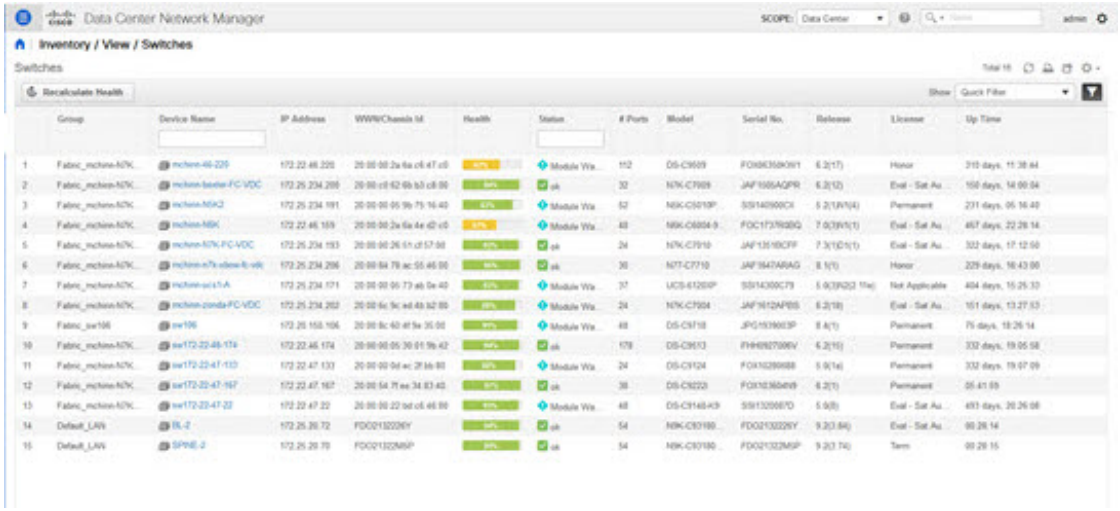
次の図は、オナー モードの SAN スイッチのライセンス ページを示しています。



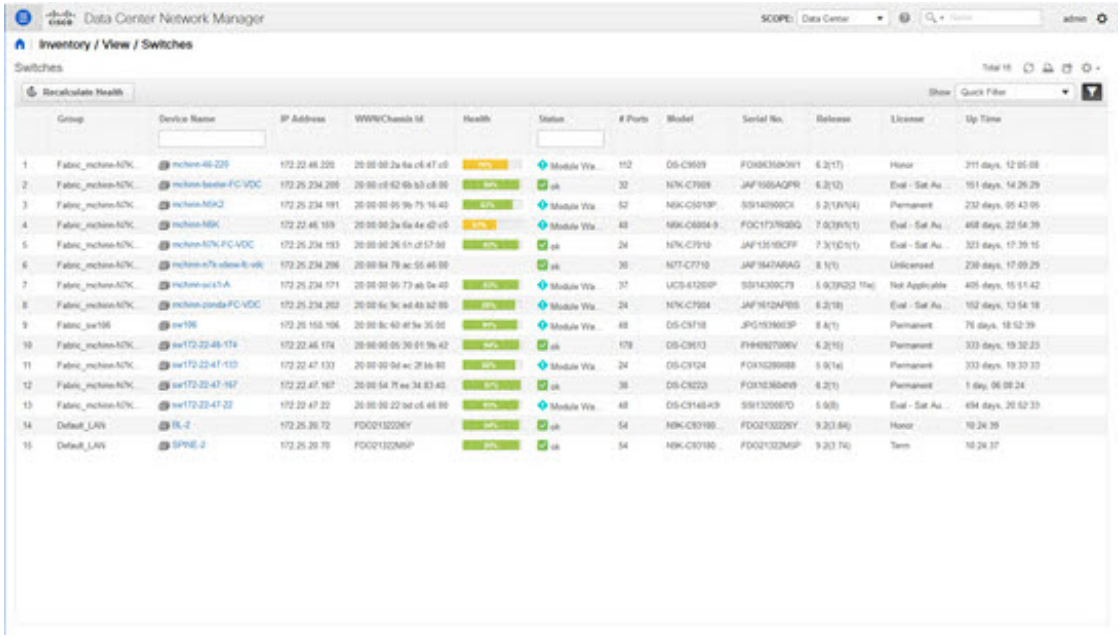
次の図は、オナー モードの LAN スイッチのライセンス ページを示しています。



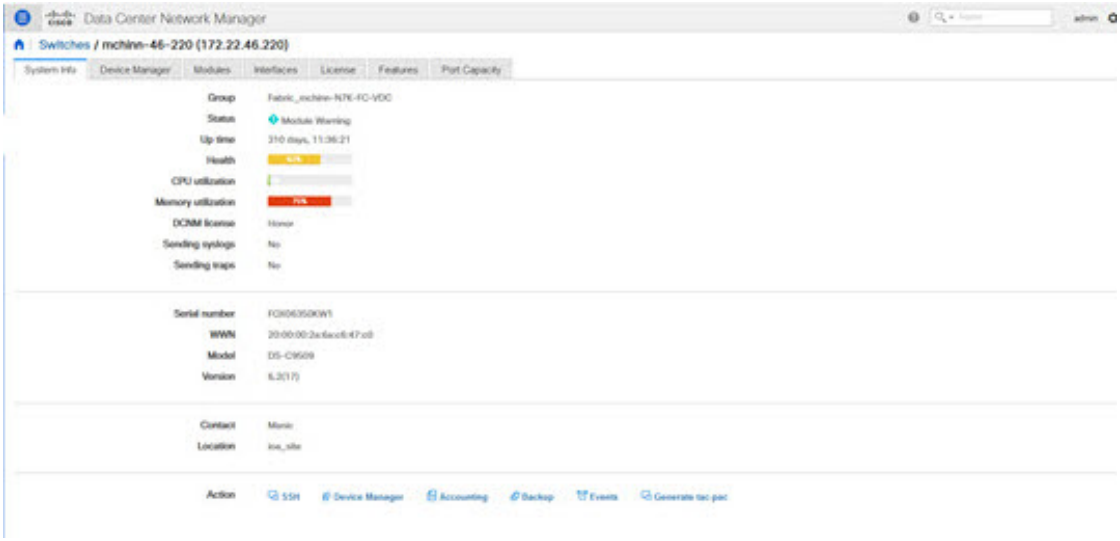
次の図は、ライセンスと期間のオナー モードを表示するスイッチ テーブルを示しています。



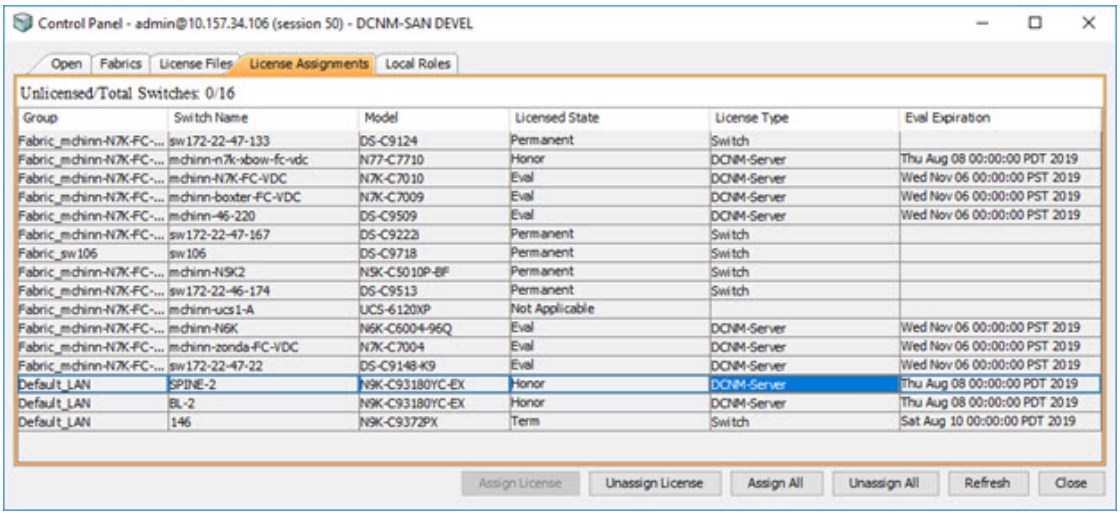
次の画像は、オナー モード ライセンスの LAN スイッチを備えたスイッチ ダッシュボードを示しています。



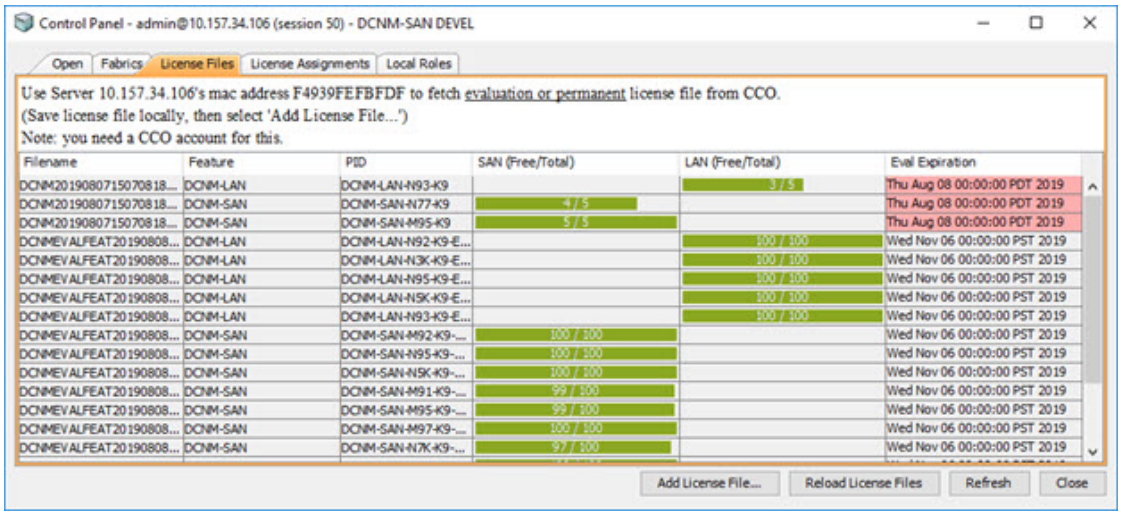
次の図は、オナー モード ライセンスの SAN スイッチを備えたスイッチ ダッシュボードを示しています。



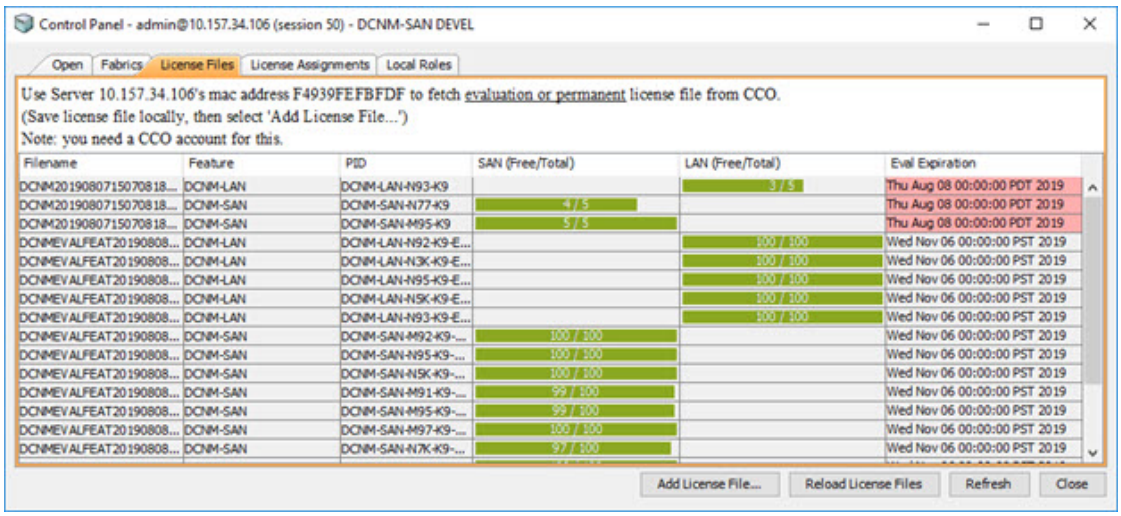
次の図は、SAN クライアント ライセンスの使用許諾契約タブを示しています。



次の図は、**SAN クライアント ライセンス** ファイル タブを示しています。



（注） スイッチベースのオナー ライセンスは、サーバーベースのライセンス ファイルで上書きできません。



スマート ライセンス

Cisco DCNM リリース 11.1(1) からスマート ライセンシング機能を使用して、デバイス レベルでライセンスを管理し、必要に応じて更新します。Cisco DCNM Web UI から、**管理 （Smart License Administration）] > [ライセンス管理（Manage Licensing）] > [DCNM] > [スマート ライセンス（Smart License）]** を選択します。Cisco スマート ライセンスの簡単な紹介、メニューバー、および**[スイッチ ライセンス（Switch Licenses）]**エリアが表示されます。

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。

概要で、**[ここをクリック（Click Here）]** をクリックして、スマート ソフトウェア ライセンスに関する情報を表示します。

メニュー バーには次のアイコンがあります。

- **[登録状況（Registration Status）]**: クリックするとポップアップ ウィンドウに現在の登録の詳細が表示されます。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 **DEREGISTERED** に設定されます。登録後、値は **REGISTERED** に設定されます。登録ステータスをクリックして、最後のアクション、アカウントの詳細、およびその他の登録の詳細を **[登録の詳細（Registration Details）]** ポップアップ ウィンドウに表示します。
- **[ライセンスのステータス（License Status）]**: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、**AUTHORIZED** または **OUT-OF-COMPLIANCE** 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。
- **[制御（Control）]**: スマート ライセンスの有効化または無効化、トークンの登録、認証の更新を行うことができます。

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。

フィールド	説明
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、**[認証済み（Authorized）]** と **[コンプライアンス違反（Out of Compliance）]** です。
説明	ライセンスのタイプと詳細を指定します。
最終更新日	スイッチ ライセンスが最後に更新されたときのタイムスタンプを指定します。
プリント	スイッチ ライセンスの詳細を印刷できます。
エクスポート	ライセンスの詳細をエクスポートできます。

Cisco Smart Software Manager でアカウントから製品ライセンスを削除した後、スマート ライセンスを無効にして、再度登録します。

スマート ライセンスの有効化

Cisco DCNM Web UI からスマート ライセンスを有効にするには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] > [スマート ライセンス（Smart License）]** を選択します。

ステップ 2 **[制御（Control）]** をクリックし、ドロップダウン リストで **[有効化（Enable）]** を選択して、スマート ライセンスを有効にします。

確認ウィンドウが表示されます。

ステップ 3 **[はい（Yes）]** をクリックします。

DCNM インスタンスを登録する手順が表示されます。

登録ステータスが **[未構成（UNCONFIGURED）]** から **[登録抹消（DEREGISTERED）]** に変わり、ライセンス ステータスが **[未構成（UNCONFIGURED）]** から **[使用されているライセンスはありません（No Licenses in Use）]** に変わります。

Cisco DCNM インスタンスの登録

Before you begin

Cisco Smart Software Manager のトークンを作成します。

Procedure

ステップ 1 **[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] > [スマートライセンス（Smart License）]** を選択します。

ステップ 2 **[制御（Control）]** をクリックし、ドロップダウンリストで **[登録（Register）]** を選択します。

[登録（Register）] ウィンドウが表示されます。

ステップ 3 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://tools.cisco.com/its/service/oddce/services/DDCEService

- **トランスポート ゲートウェイ（Transport Gateway） - ゲートウェイまたはサテライト経由のプロキシ**

  このオプションを選択する場合は、URL を入力します。

- **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 4 **[トークン（Token）]** フィールドに登録トークンを入力します。

ステップ 5 ライセンスを登録するために、**[送信（Submit）]** をクリックします。

登録ステータスが **[登録抹消（DEREGISTERED）]** から **[登録済み（REGISTERED）]** 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。

[登録ステータス：登録済み（Registration Status: REGISTERED）] をクリックして、登録されたトークンの詳細を表示します。

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。

What to do next

登録後に発生した通信エラーのトラブルシューティングを行います。

通信エラーのトラブルシューティング

登録中の通信エラーを解決するには、次の手順を実行します。

Procedure

ステップ 1 DCNM サービスを停止します。

ステップ 2 次のパスからサーバ プロパティ ファイルを開きます：/usr/local/cisco/dcm/fm/conf/server.properties

Note Windows のサーバ プロパティ ファイルは、次の場所にあります：C:/Program Files/Cisco/dcm/fm/conf/server.properties

ステップ 3 サーバ プロパティ ファイルに次のプロパティを含めます：

```
#cisco.smart.license.production=false #smartlicense.url.transport=https://
CiscoSatellite_Server_IP /Transportgateway/services/DeviceRequestHandler
```

ステップ 4 次のシンタックスで、/etc/hosts ファイルのホスト データベースにある Cisco サテライトの詳細を更新します：*Satellite_Server_IP* CiscoSatellite

ステップ 5 DCNM サービスを開始します。

認証を更新

登録済みの場合にのみ、承認を手動で更新できます。自動再承認は定期的に行われます。**[ライセンス ステータス（License Status）]** をクリックして、次回の自動再承認に関する詳細を表示します。Cisco DCNM Web UI から承認を更新するには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] > [スマート ライセンス（Smart License）]** を選択します。

ステップ 2 **[制御（Control）]** をクリックし、ドロップダウン リストで **[承認の更新（Renew Authorization）]** を選択して、ライセンス承認を更新します。

更新がある場合は、更新を取得する要求が Cisco Smart Software Manager に送信されます。更新後、**[スマート ライセンス（Smart Licenses）]** ウィンドウが更新されます。

スマート ソフトウェア ライセンスの無効化

Cisco DCNM Web UI からスマート ライセンスを無効にするには、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] > [スマート ライセンス（Smart License）]** を選択します。

ステップ 2 **[制御（Control）]** を選択し、**[無効化（Disable）]** を選択して、スマート ライセンスを無効にします。

確認ウィンドウが表示されます。

ステップ 3 **[はい（Yes）]** をクリックします。

このトークンを使用するスイッチのライセンス ステータスは、**[ライセンスの割り当て（License Assignments）]** タブで、**[ライセンスなし（Unlicensed）]** に変わります。このトークンは、Cisco Smart Software Manager の **[製品インスタンス（Product Instances）]** タブの下のリストから削除されます。

スマート ライセンスが利用できず、スマート ライセンスを無効にした場合は、**[ライセンスの割り当て（License Assignments）]** タブからライセンスを手動で解放します。

スイッチ スマート ライセンス

スマート ライセンスでスイッチが事前構成されている場合、DCNM がスイッチ スマート ライセンスを検証し割り当てます。Cisco DCNM UI を使用してスイッチにライセンスを割り当てるには、**[管理（Administration）]>[ライセンスの管理（Manage Licensing）]>[ライセンスの割り当て（Assign License）]** または **[すべて割り当て（Assign All）]** を選択します。

（注） 管理モードのスイッチについては、スイッチ スマート ライセンスは DCNM を通して割り当てる必要があります。

（注） Cisco NX-OS リリース 9.3(6) 以降、スイッチ スマート ライセンスがサポートされます。

DCNM でスイッチ スマート ライセンスを有効にするには：

- 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、スイッチのスマート ライセンスを構成します。
- license smart register **idtoken** 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。DCNM の **[EXEC]** オプションを使用して、トークンをプッシュします。詳細については、[DCNM での EXEC モード コマンドの実行（Running EXEC Mode Commands in DCNM）]を参照してください。

ライセンスのないスイッチの場合、ライセンスは次の優先度に基づいて割り当てられます。

1. DCNM スマート ライセンス
2. DCNM サーバ ライセンス
3. DCNM 評価ライセンス

サーバ ライセンス ファイル

Cisco DCNM Web UI から、**[管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [DCNM] > [サーバ ライセンス ファイル（Server License Files）]** を選択します。次のテーブルには Cisco DCNM

フィールド	説明
ファイル名	ライセンス ファイル名を指定します。
機能	ライセンス機能を指定します。
PID	製品 ID を指定します。
LAN (空き/合計)	LAN の無料ライセンス数と合計ライセンス数を表示します。
期限日 （Expiration Date）	ライセンスの有効期限日が表示されます。 **Note** **[有効期限日（Expiration Date）]** フィールドのテキストで、7 日間で期限切れになるライセンスについては赤い色になっています。

Cisco DCNM ライセンスの追加

Cisco DCNM から Cisco DCNM ライセンスを追加するには、以下の手順を実行します。

Before you begin

次の手順を実行するには、ネットワーク管理者権限が必要です。

Procedure

ステップ 1 ライセンス ウィザードを開始するには **[管理（Administration）]> [ライセンスの管理（Manage Licensing）] > [DCNM]** を選択します。

ステップ 2 **[サーバ ライセンス ファイル（Server License Files）]** タブを選択します。

有効な Cisco DCNM-LAN ライセンス ファイルは表示されています。

ライセンスをロードするときは、セキュリティ エージェントが無効になっていることを確認してください。

ステップ 3 シスコから送付されたライセンス パック ファイルをローカル システムのディレクトリにダウンロードします。

ステップ 4 **[ライセンス ファイルの追加（Add License File）]** をクリックし、ローカル マシンに保存したライセンス パック ファイルを選択します。

ファイルはサーバ マシンにアップロードされ、サーバ ライセンス ディレクトリに保存されてから、サーバにロードされます。

Note .licファイルのコンテンツを編集しないようにしてください。編集すると、Cisco DCNMソフトウェアでは、そのライセンスファイルに関連付けられたすべての機能が無視されます。このファイルの内容に署名して、内容が変更されないようにする必要があります。ライセンス ファイルを間違って複数回コピー、名前変更、または挿入した場合、重複ファイルは無視されますが、元のファイルはカウントされます。

スイッチの機能：一括インストール

リリース 11.3(1) 以降、Cisco DCNM 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。DCNM 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解析します。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。

Cisco DCNM 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。

1. **[管理 (Administration)] > [ライセンス付与の管理 (Manage Licensing)] > [スイッチ機能（Switch features）]** を選択します。
2. スイッチ ライセンス エリアで、**[ライセンス ファイルのアップロード（Upload License files）]** 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。

   一括でスイッチ ライセンスをインストール ウィンドウが表示されます。
3. ライセンスを選択で、**[ライセンスファイルの選択（Select License File file(s）]**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。

   [開く（Open）] をクリックします。
4. DCNMサーバからスイッチにライセンスファイルをコピーするためのファイル転送プロトコルを選択します。
   - ライセンス ファイルをアップロードするには、**TFTP**、**SCP**、または **SFTP** プロトコルのいずれかを選択します。

（注） すべてのプラットフォームですべてのプロトコルがサポートされているわけではありません。TFTPは、Win/RHEL DCNM SAN インストールでのみサポートされます。ただし、SFTP/SCP はすべてのインストール タイプでサポートされています。

5. **VRF** 構成をサポートするライセンスの VRF チェックボックスをオンにします。

定義済みルートの 1 つの VRF 名を入力します。

6. **[スイッチでファイルを上書きする（Overwrite file on Switch）]** チェックボックスをオンにして、アップロードされた新しいライセンス ファイルでライセンス ファイルを上書きします。

（注） overwrite コマンドは、ブート フラッシュ内の既存のファイルに新しいファイルをコピーします。以前のライセンスがすでにインストールされている場合、それはインストールを上書きしません。

7. DCNM サーバ ログイン情報で、DCNM サーバのルート ユーザー名とパスワードを入力します。

   DCNM にアクセスするための認証ログイン情報を入力します。DCNM Linux 展開の場合、これはユーザー名です。OVA\ISO 展開の場合、**sysadmin** ユーザーの資格情報を使用します。

8. [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 DCNM 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

9. 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。

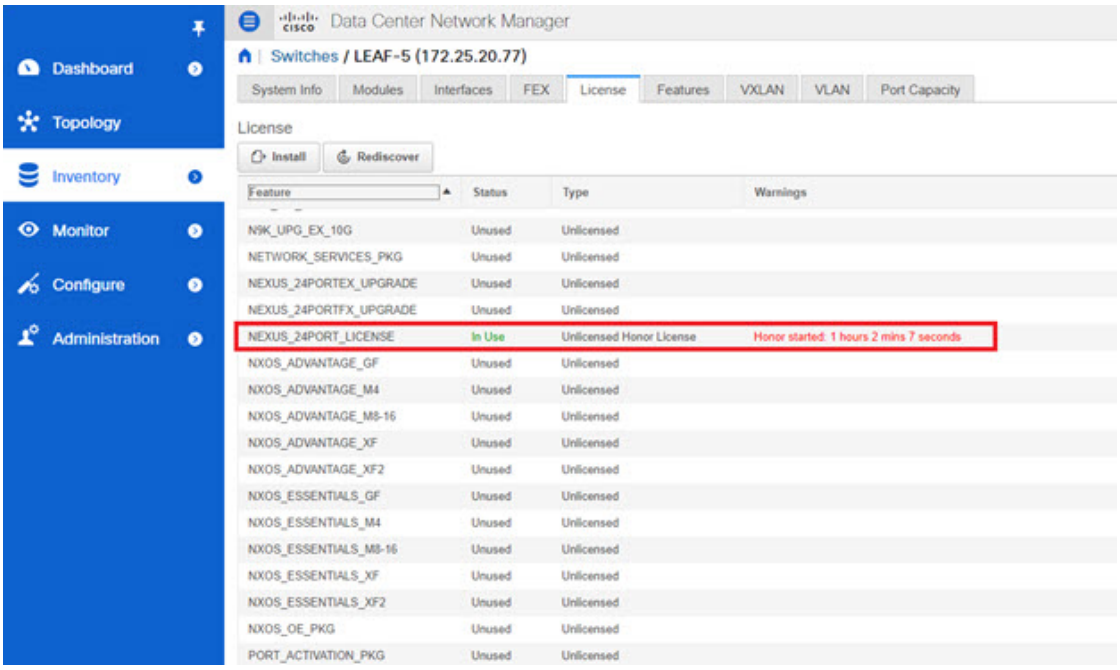
10. **[ライセンスのインストール（Install Licenses）]** をクリックします。

    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。

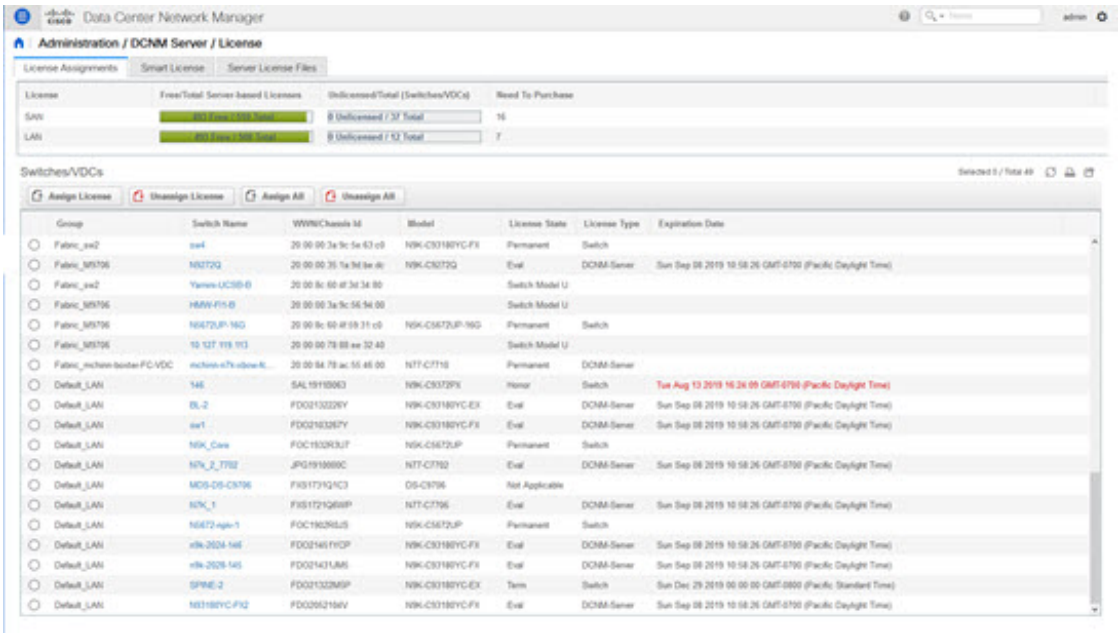
11. ライセンスがそれぞれのデバイスと一致し、インストールされると、**[ライセンスのステータス（License Status）]** テーブルにステータスが表示されます。

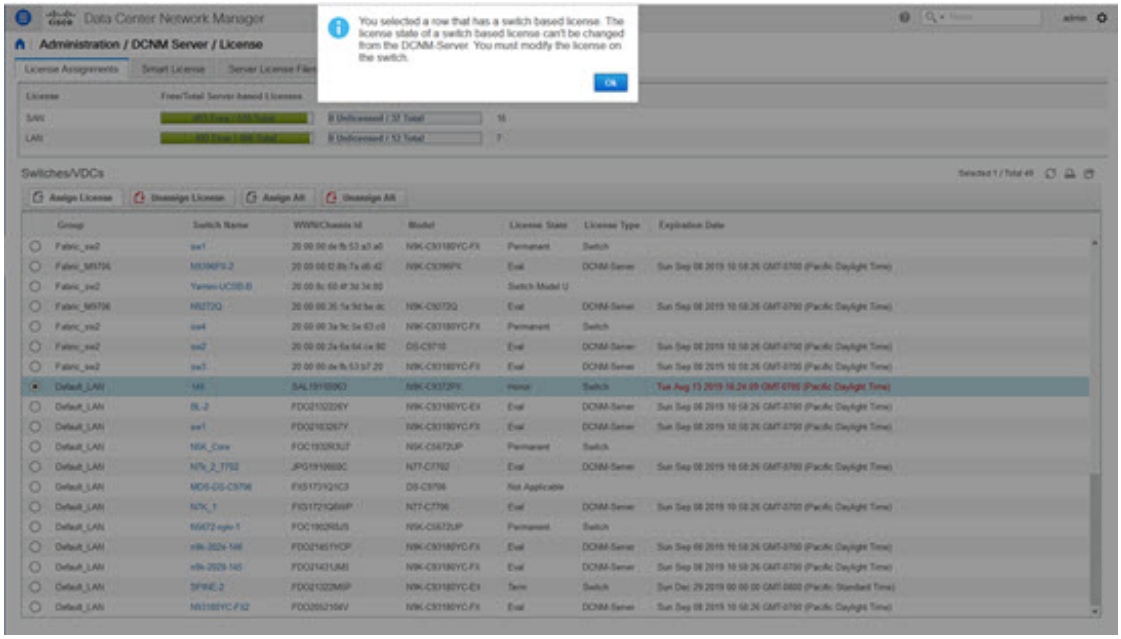
スイッチベースの名誉ライセンスのサポート

[DCNM **Web UI]** > **[インベントリ（Inventory）]** > **[スイッチ（Switch）]** > **[ライセンス（License）]** で、**[タイプ（Type）]** 列に「Unlicensed Honor License」と表示され、**[警告（Warnings）]** 列に **[Honor started: …]** と表示され、ライセンスが名誉モードに変更されてからの経過時間が表示されます。



（注） スイッチベースのオナー ライセンスは、サーバーベースのライセンス ファイルで上書きできません。

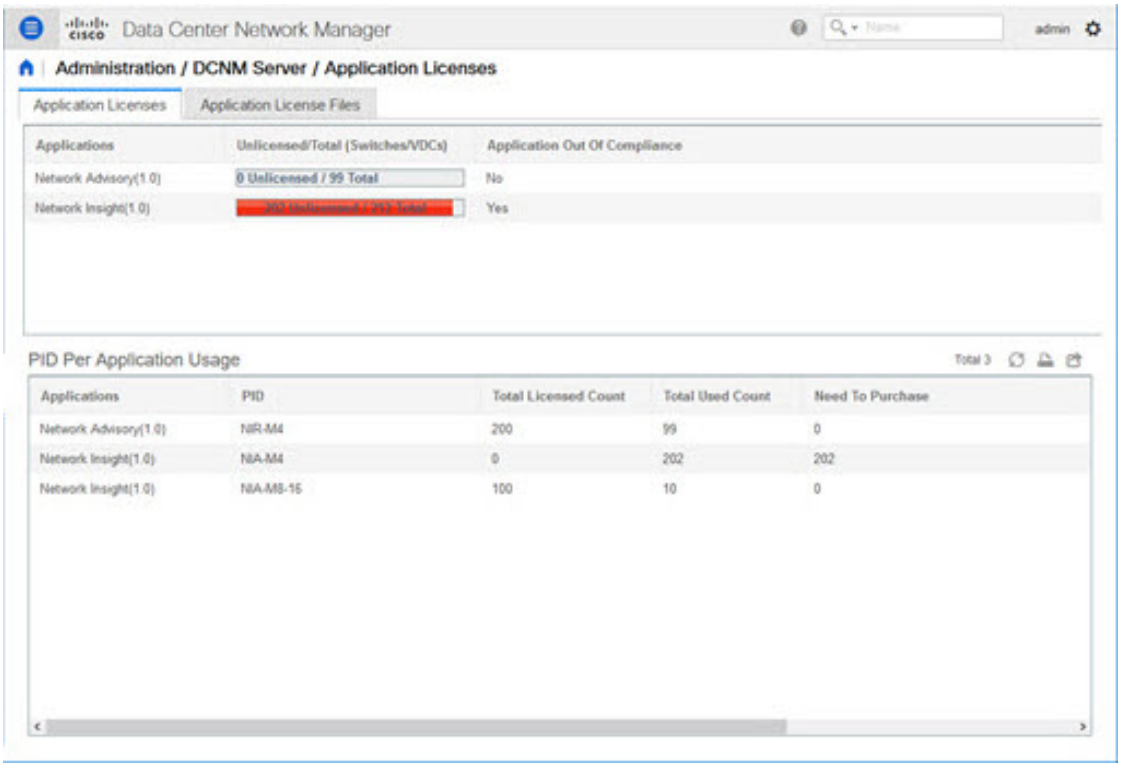




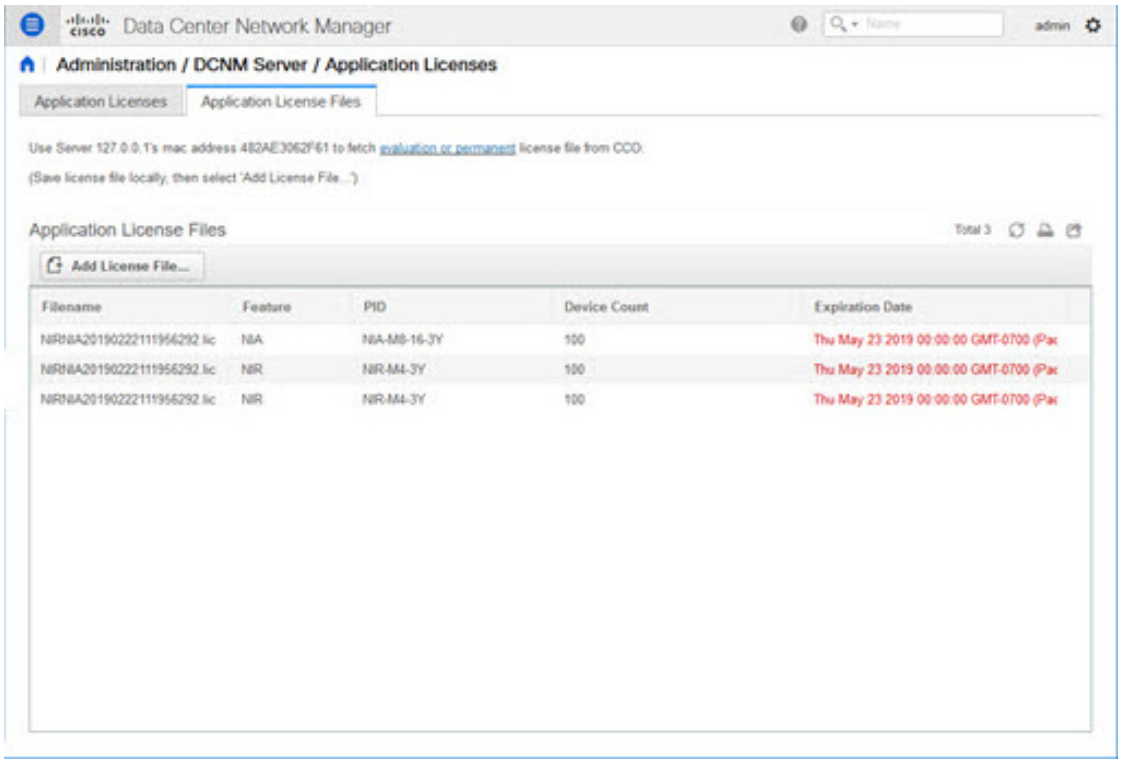
アプリケーション ライセンス

リリース 11.3(1) 以降、Cisco DCNM でアプリケーションのライセンスを管理できます。**[Web UI] > [管理（Administration）] > [ライセンスの管理（Manage Licensing）] > [アプリケーション（Applications）]** を選択して、アプリケーション ライセンスを表示します。

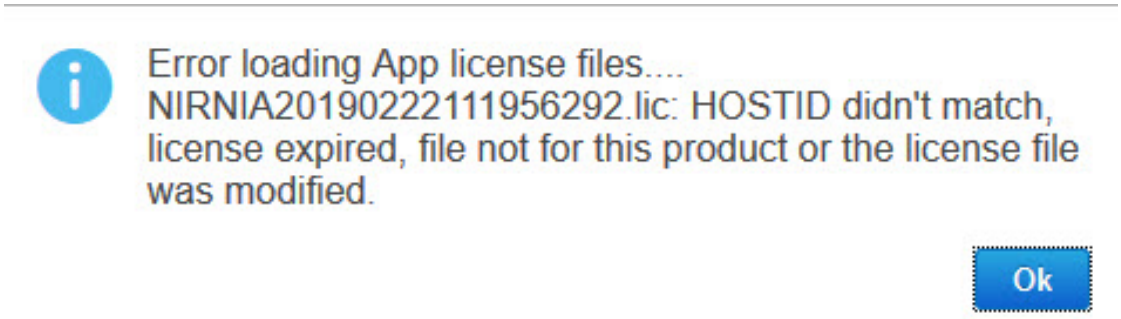
[アプリケーション ライセンス（Application Licenses）] タブには、ライセンスのないスイッチ/合計スイッチの概要、およびコンプライアンスに違反しているかどうかを示す DCNM アプリケーションが表示されます。[アプリケーション使用状況ごとの PID（PID Per Application Usage）] テーブルには、アプリケーション フレームワークからサーバに指定された PID ごとの実際のカウントが表示されます。アプリケーションごとに購入する必要がある PID もリストされています。



[アプリケーション ライセンス ファイル（Application License Files）] タブでは、アプリケーションのライセンス ファイルを追加できます。[ライセンス ファイルの追加（Add license file）] をクリックして、ローカル ディレクトリからライセンス ファイルを追加します。ライセンスのファイル名、アプリケーション名、PID、デバイス数および有効期限日の詳細は、インポートされたライセンス ファイルから抽出されます。ライセンスが永続的でない場合、または評価または期限付きである場合は、有効期限も表示されます。



次の画像は、アプリケーション ライセンス ファイルをアップロードする際のサンプル エラー メッセージを示しています。



ユーザー管理

（注） DCNM にログインするたびに、DCNM サーバーは AAA 認証のために ISE サーバーから情報を取得します。最初のログイン後、ISE サーバは再度認証されません。

ユーザー管理メニューには、次のサブメニューがあります。

リモート AAA

Cisco DCNM Web UI からリモート AAA を構成するには、次の手順を実行します。

Procedure

ステップ 1 **[管理] > [管理ユーザー] > [リモート AAA プロパティ]** を選択します。

AAA プロパティ構成ウィンドウが表示されます。

ステップ 2 ラジオ ボタンを使用して、次の認証モードのいずれかを選択します。

- ローカル：このモードでは、認証はローカル サーバで認証されます。
- RADIUS：このモードでは、認証は指定された RADIUS サーバに対して認証を行います。
- TACACS+：このモードでは、認証は指定された TACACS サーバに対して認証を行います。
- スイッチ：このモードでは、認証は指定されたスイッチに対して認証を行います。
- LDAP：このモードでは、認証は指定された LDAP サーバに対して認証されます。

ステップ 3 [適用（Apply）] をクリックします。

ローカル

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **[ローカル（Local）]** を選択します。

ステップ 2 **[適用（Apply）]** をクリックし、認証モードを確認します。

RADIUS

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **Radius** を選択します。

Note DCNM AAA または Radius 認証を使用する場合、秘密鍵の先頭にハッシュ (#) 記号を指定しないでください。そうしないと、DCNM は # を暗号化されたものとして使用しようとし、失敗します。

ステップ 2 プライマリ サーバの詳細を指定し、**[テスト（Test）]** をクリックしてサーバをテストします。

ステップ 3 （オプション）セカンダリおよびターシャリ サーバーの詳細を指定し、**[テスト（Test）]** をクリックしてサーバをテストします。

ステップ 4 **[適用（Apply）]** をクリックし、認証モードを確認します。

TACACS+

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **TACACS+** を選択します。

Note DCNM AAA または Radius 認証を使用する場合、秘密鍵の先頭にハッシュ (#) 記号を指定しないでください。そうしないと、DCNM は # を暗号化されたものとして使用しようとし、失敗します。

ステップ 2 プライマリ サーバの詳細を指定し、**[テスト（Test）]** をクリックしてサーバをテストします。

ステップ 3 （オプション）セカンダリおよびターシャリ サーバーの詳細を指定し、**[テスト（Test）]** をクリックしてサーバをテストします。

Note IPv6 トランスポートの場合、フェールオーバの状況中にアドレスの順序が変更されるため、AAA 認証の物理アドレスと VIP アドレスを入力します。

ステップ 4 **[適用（Apply）]** をクリックし、認証モードを確認します。

スイッチ

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **[スイッチ（Switch）]** を選択します。

DCNM は、IPv6 管理インターフェイスを備えた LAN スイッチもサポートします。

ステップ 2 プライマリ スイッチ名を指定し、**[適用（Apply）]** をクリックして認証モードを確認します。

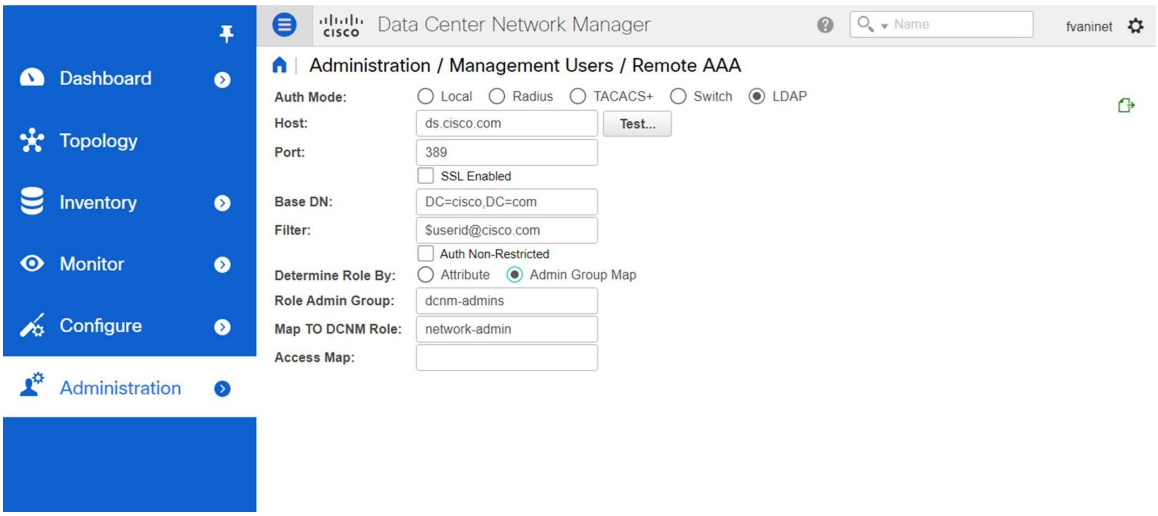
ステップ 3 (Optional) セカンダリおよびターシャリ スイッチの名前を指定します。

ステップ 4 **[適用（Apply）]** をクリックし、認証モードを確認します。

LDAP

Procedure

ステップ 1 ラジオ ボタンを使用して、認証モードとして **[LDAP]** を選択します。



ステップ 2 **[ホスト（Host）]** フィールドを展開し、IPv4 アドレスまたは IPv6 アドレスを入力します。

ドメイン ネーム システム（DNS）サービスが有効になっている場合は、LDAP サーバの DNS アドレス（ホスト名）を入力できます。

ステップ 3 [ポート（Port）] フィールドに、ポート番号を入力します。

非 SSL の場合は 389 を入力します。 SSL には 636 を入力します。デフォルトでは、ポートは非 SSL 用に構成されています。

ステップ 4 AAA サーバで SSL が有効になっている場合は、**[SSL を有効にする（SSL Enabled）]** チェック ボックスをオンにします。

Note LDAP over SSL を使用するには、ポートフィールドに **636** と入力し、**[SSL を有効にする（SSL Enabled）]** チェック ボックスをオンにする必要があります。

これで、LDAP クライアントに SSL セッションを確立させてからバインドまたは検索の要求を送信することにより、転送されたデータの完全性と機密保持を保証します。

Note Cisco DCNM は、TLS を使用して LDAP サーバとのセキュアな接続を確立します。Cisco DCNM は、すべてのバージョンの TLS をサポートします。ただし、TLS の特定のバージョンは LDAP サーバによって決定されます。

たとえば、LDAP サーバがデフォルトで TLSv1.2 をサポートしている場合、DCNM は TLSv1.2 を使用して接続します。

ステップ 5 **[ベース DN（Base DN）]** フィールドに基本ドメイン名を入力します。

LDAP サーバはこのドメインを検索します。ベース DN は、DAP サーバで **dsquery.exe user -name**<*display_name*> コマンドを使用することで見つけることができます。

次に例を示します。

```
ldapserver# dsquery.exe users -name "John Smith"

CN=john smith,CN=Users,DC=cisco,DC=com
```

ベース DN は DC=cisco,DC=com です。

Note ベース DN 内の要素を正しい順序で入力していることを確認してください。これは、アクティブ ディレクトリ を照会するときのアプリケーションのナビゲーションを指定します。

ステップ 6 **[フィルタ処理（Filter）]** フィールドで、フィルタ処理 パラメータを指定します。

これらの値は、検索クエリをアクティブディレクトリに送信するために使用されます。LDAP 検索フィルタ文字列は最大 128 文字に制限されています。

次に例を示します。

- $userid@cisco.com

  これは、ユーザー プリンシパル名と一致します。

- CN=$userid、OU=従業員、OU=Cisco ユーザー

  これは、正確なユーザー DN と一致します。

ステップ 7 ロールを決定するオプションを選択します。**[属性（Attribute）]** または **[管理グループ マップ（Admin Group Map）]** のいずれかを選択します。

- **[管理グループ マップ（Admin Group Map）]**：このモードでは、DCNM はベース DN とフィルタ処理に基づいて、LDAP サーバにユーザーをクエリします。ユーザーがいずれかのユーザー グループに属している場合、DCNM ロールはそのユーザー グループにマッピングされます。
- **[属性（Attribute）]**：このモードでは、DCNM はユーザー属性をクエリします。属性を選択できます。**[属性（Attribute）]** を選択すると、**[ロール管理者グループ（Role Admin Group）]** フィールドが **[ロール属性（Role Attributes）]** に変わります。

ステップ 8 前の手順での選択に基づいて、**[ロール属性（Roles Attributes）]** または **[ロール管理者グループ（Role Admin Group）]** フィールドに値を入力します。

- **[管理グループ マップ（Admin Group Map）]** を選択した場合は、**[ロール管理グループ（Role Admin Group）]** フィールドに管理グループの名前を入力します。
- **[属性（Attribute）]** を選択した場合は、**[属性（Attribute）]** フィールドに適切な属性を入力します。

ステップ 9 **[DCNM ロールにマッピング（Map to DCNM Role）]** フィールドに、ユーザーにマッピングされる DCNM ロールの名前を入力します。

一般に、**network-admin** または **network-operator** が最も一般的なロールです。

次に例を示します。

```
Role Admin Group: dcnm-admins
Map to DCNM Role: network-admin
```

この例では、Active Directory ユーザー グループ **dcnm-admins** を **network-admin** ロールにマップします。

複数の Active Directory ユーザー グループを複数のロールにマッピングするには、次のフォーマットを使用します：

```
Role Admin Group:
Map To DCNM Role: dcnm-admins:network-admin;dcnm-operators:network-operator
```

[ロール管理グループ（Role Admin Group）] は空白で、**[DCNM ロールにマッピング（Map To DCNM Role）]** にはセミコロンで区切られた 2 つのエントリが含まれていることに注意してください。

ステップ 10 **[アクセス マップ（Access Map）]** フィールドに、ユーザーにマップするロール ベースのアクセスコントロール（RBAC）デバイス グループを入力します。

ステップ 11 **[テスト（Test）]** をクリックし、構成を確認します。[テスト AAA サーバ（Test AAA Server）] ウィンドウが表示されます。

ステップ 12 [テスト AAA サーバ（Test AAA Server）] ウィンドウに有効な**ユーザー名**と**パスワード**を入力します。

構成が正しい場合、次のメッセージが表示されます。

```
Authentication succeeded.
The cisco-av-pair should return 'role=network-admin' if this user needs to
see the DCNM Admin pages. 'SME' roles will allow SME page access. All other
roles - even if defined on the switches - will be treated
as network operator.
```

このメッセージは、[ロール管理グループ（Role Admin Group）] または [属性（Atribute）] モードに関係なく表示されます。これは、Cisco DCNM がクエリを Active Directory、グループ、およびロールにすることができ、を正しく構成できることを意味します。

テストが失敗すると、LDAP 認証に失敗したというメッセージが表示されます。

Warning テストが成功しない限り、構成を保存しないでください。間違った構成を保存すると、DCNM にアクセスできません。

ステップ 13 **[変更の適用（Apply Changes）]** アイコン（画面の右上隅にあります）をクリックして、構成を保存します。

ステップ 14 DCNM SAN サービスを再起動します。

- Windows の場合 – システムで、**[コンピュータの管理（Computer Management）] > [サービスとアプリケーション（Computer Management）] > [サービス（Services）]** に移動します。DCNM アプリケーションを見つけて右クリックします。**[停止（Stop）]** を選択します。1 分後、DCNM アプリケーションを右クリックし、**[開始（Start）]** を選択して DCNM SAN サービスを再起動します。

- Linux の場合 – **/etc/init.d/FMServer.restart** に移動し、リターン キーを押して DCNM SAN サービスを再起動します。

ローカル ユーザーを管理

管理者ユーザーとして、Cisco DCNM Web UI を使用して新しいユーザーを作成し、ロールを割り当て、そのユーザーに 1 つ以上のグループまたは範囲を関連付けることができます。

DCNM リリース 11.5(1) から、新しいユーザー ロール **device-upg-admin** が追加され、画像管理ウィンドウでのみ操作を実行します。

この項の内容は、次のとおりです。

ローカルユーザーの追加

Procedure

ステップ 1 メニュー バーから**[管理（Administration）] > [管理ユーザー（Management Users）] > [ローカル（Local）]**を選択します。**[ローカル ユーザー]** ページが表示されます。

ステップ 2 [ユーザの追加（Add User）] をクリックします。

[ユーザーを追加（Add User）] ダイアログボックスを表示します。

ステップ 3 **[ユーザー名（User name）]** フィールドにユーザー名を入力します。

Note ユーザー名は大文字と小文字が区別されますが、ユーザー名ゲストは予約済みの名前であり、大文字と小文字は区別されません。guest ユーザにできるのは、レポートの表示だけです。guest ユーザは guest パスワードを変更できず、DCNM Web クライアントの Admin オプションにもアクセスできません。

ステップ 4 **[ロール（Role）]** ドロップダウン リストからユーザーのロールを選択します。

ステップ 5 [Password] フィールドにパスワードを入力します。

Note SPACE 以外の全ての特殊文字はパスワードで許可されています。

ステップ 6 **[Confirm Password（パスワードの確認）]** フィールドで、パスワードを再入力します。

ステップ 7 **[Add（追加）]** をクリックすると、そのユーザーがデータベースに追加されます。

ステップ 8 ユーザーの追加を続行する場合は、ステップ 2 ～ 7 を繰り返します。

ローカル ユーザの削除

Cisco DCNM Web UI からローカル ユーザーを削除するために、次の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [ローカル（Local）]** を選択します。

[ローカル ユーザー（Local Users）] ページが表示されます。

ステップ 2 **[ローカル ユーザー（Local Users）]** テーブルから 1 人以上のユーザーを選択し、**[ユーザーの削除（Delete User）]** ボタンをクリックします。

ステップ 3 警告ウィンドウで **[はい（Yes）]** をクリックして、ローカル ユーザーを削除します。**[いいえ（No）]** をクリックし、削除をキャンセルします。

ユーザの編集

Cisco DCNM Web UI からユーザーを編集するには、以下の手順を実行します。

Procedure

ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [ローカル（Local）]** を選択します。

ステップ 2 チェックボックスを使用してユーザーを選択し、**[ユーザーの編集（Edit User）]**アイコンをクリックします。

ステップ 3 **[ユーザーの編集（Edit User）]** ウィンドウでは、デフォルトで**[ユーザー名（Username）]**と**[ロール（Role）]**が示されます。**[パスワード（Password）]** の指定と **[パスワードの確認（Confirm Password）]** をします。

ステップ 4 [適用（Apply）] をクリックし、変更を保存します。

ユーザ アクセス

ローカルユーザーがアクセスできる特定のグループまたはファブリックを選択できます。これにより、ローカルユーザーは、アクセスが許可されていない特定のグループまたはファブリックにアクセスできなくなります。これを行うには、次の手順を実行します。

Procedure

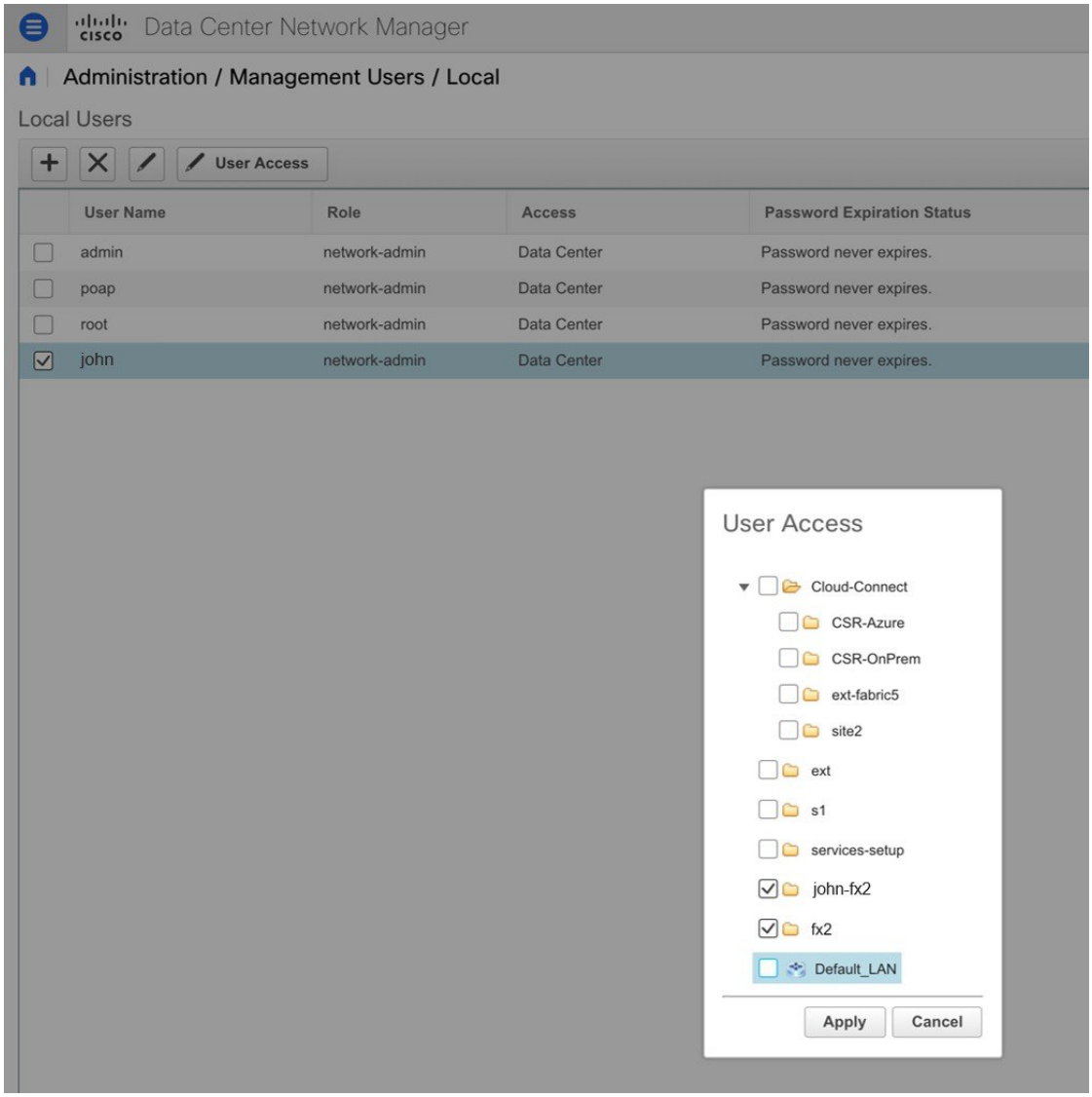
ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [ローカル（Local）]** を選択します。

[ローカル ユーザー（Local Users）] ウィンドウが表示されます。

ステップ 2 **[ローカル ユーザー（Local Users）]** テーブルから一人のユーザーを選択します。**[ユーザー アクセス（User Access）]** をクリックします。

[ユーザー アクセス（User Access）]選択ウィンドウが表示されます。

ステップ 3 ユーザーがアクセスできる特定のグループまたはファブリックを選択し、**[適用（Apply）]** をクリックします。



Note **[ネットワーク管理者（network-admin）]**ロールを持つユーザーにデータ センター全体へのアクセス権がない場合、**[ユーザー アクセス（User Access）]** ボタンはグレー表示され、**[アクセス（Access）]** 列の値は**[データ センター（Data Center）]**ではありません。その場合、データセンター全体にアクセスできる新しい**[ネットワーク管理者（network-admin）]**ロールのユーザーを作成するには、*addUser.sh/bat* スクリプトを使用します。

クライアントを管理する

Cisco DCNM を使用して、DCNM クライアント サーバを切断できます。

Procedure

ステップ 1 **[管理（Administration）] > [管理ユーザー（Management Users）] > [クライアント（Clients）]** を選択します。

DCNM サーバのリストが表示されます。

ステップ 2 チェックボックスを使用して DCNM サーバを選択し、**[クライアントの切断（Disconnect Client）]** をクリックして DCNM サーバを切断します。

Note 現在のクライアント セッションを切断することはできません。

パフォーマンスのセットアップ

パフォーマンスのセットアップ メニューには次のサブメニューが含まれます。

パフォーマンス セットアップ LAN 収集

Performance Manager を使用してファブリックを管理する場合は、ファブリック上でフローおよび収集の初期セットを設定する必要があります。Cisco DCNM を使用してパフォーマンス収集を追加または、削除することができます。スイッチの収集を作成する前に、スイッチにライセンスを付与し、**継続的な管理対象**状態に維持します。

Note Performance Manager データを収集するには、スイッチと DCNM サーバ間で ICMP ping を有効にする必要があります。**pm.skip.checkPingAndManageable** サーバ プロパティを true に設定してから、DCNM を再起動します。[Web **UI**]、**[管理（Administration）]**、**[DCNM サーバー（DCNM Server）]**、**[サーバーのプロパティ（Server Properties）]** の順に選択して、サーバ プロパティを設定します。

収集を追加する手順は、次のとおりです。

Procedure

ステップ 1 **[管理（Administration）] > [パフォーマンス セットアップ（Performance Setup）] > [LAN コレクション（LAN Collections）]** を選択します。

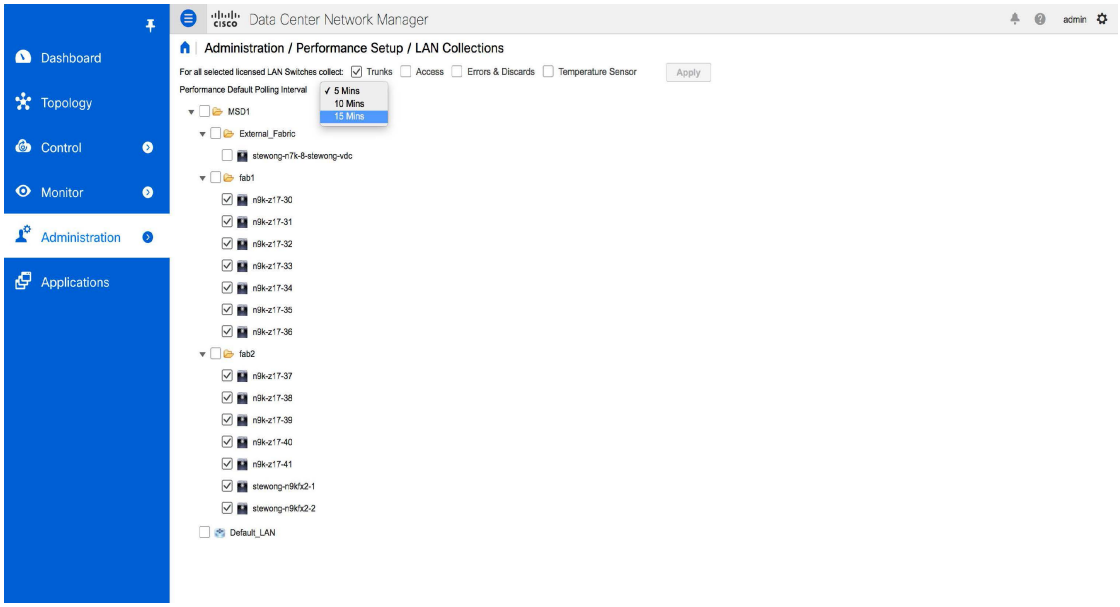
ステップ 2 ライセンスを取得したすべての LAN スイッチについて、チェック ボックスを使用して、**トランク**、**アクセス**、**エラーと破棄**、および**温度センサー**のパフォーマンスデータ収集を有効にします。

ステップ 3 ドロップダウン リストから **[パフォーマンス デフォルト投票間隔（Performance Default Polling Interval）]** の値を選択します。有効な値は、**5 分**、**10 分**、および **15 分**です。デフォルト値は **5 分**です。

ステップ 4 パフォーマンス データを収集する LAN スイッチのタイプを選択するためのチェックボックスをオンにします。

ステップ 5 [Apply] をクリックして、設定を保存します

ステップ 6 確認ダイアログボックスで、**[はい（Yes）]** をクリックして Performance Manager を再起動します。新しい設定を有効にするには、Performance Manager を再起動する必要があります。



イベントのセットアップ

イベントのセットアップ メニューには次のサブメニューが含まれます。

イベント登録の表示

Syslog の送信、**トラップの送信**、および**トラップの遅延**を有効にするには、DCNM Web UI で次を構成する必要があります。

- **Syslog の送信**を有効にするには：**[物理的属性（Physical Attributes）]** > **[イベント（Events）]** > **[Syslog]** > **[サーバ（Servers）]** を選択します。**[行の作成（Create Row）]** をクリックし、必要な詳細を入力して、**[作成（Create）]** をクリックします。

- **送信トラップ**の有効化：**[物理属性（Physical Attributes）] > [イベント（Events）] > [SNMP トラップ（SNMP Traps）] > [送信先（Destination）]** を選択します。**[行の作成（Create Row）]** をクリックし、必要な詳細を入力して、**[作成（Create）]** をクリックします。
- **遅延トラップ**の有効化：**[物理属性（Physical Attributes）] > [イベント（Events）] > [SNMP トラップ（SNMP Traps）] > [遅延トラップ（Delayed Traps）]** を選択します。**[機能の有効化（Feature Enable）]** 列で、チェック ボックスを使用してスイッチの遅延トラップを有効にし、遅延を分単位で指定します。

Procedure

ステップ 1 **[管理（Administration）] > [イベント セットアップ（Event Setup）] > [登録（Registration）]** を選択します。

SNMP および Syslog レシーバと統計情報が表示されます。

ステップ 2 **[Syslog レシーバを有効にする（Enable Syslog Receiver）]** チェックボックスをオンにして **[適用（Apply）]** をクリックすると、サーバ プロパティで Syslog レシーバが無効になっている場合に有効になります。

イベント登録または syslog のプロパティを構成するには、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** を選択し、画面の指示に従います。

ステップ 3 **[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

通知の転送

Cisco DCNM Web UI を使用して、システム メッセージの通知転送の追加および削除を実行できます。

この項の内容は、次のとおりです。

通知転送の追加

Cisco DCNM 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 サーバーでは、DCNM から SMTP サーバー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。Cisco DCNM リリース 11.4(1) 以降、DCNM により認証を必要とする任意の SMTP サーバー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。この機能を構成するには、**[管理] > [DCNM サーバー] > [サーバー プロパティ]** ウィンドウで **[SMTP] > [認証]** プロパティを設定します。**server.smtp.authenticate** フィールドに **true** を入力し、**server.smtp.username** フィールドに必要なユーザー名を入力し、**server.smtp.password** フィールドに必要なパスワードを入力します。

Cisco DCNM 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。

Note テスト転送は、ライセンスされたファブリックに対してのみ機能します。

Procedure

ステップ 1 **[管理（Administration）] > [イベント設定（Event Setup）] > [転送（Forwarding）]** を選択します。

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。

ステップ 2 イベント転送を有効にするには、**[有効にする（Enable）]** チェックボックスをオンにします。

ステップ 3 **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。

ステップ 4 **[適用（Apply）]** をクリックして、設定を保存します。

ステップ 5 **[イベント カウント フィルタ（Event Count Filter）]** で、イベント カウントのフィルタをイベント フォワーダーに追加します。

イベント カウントがイベント カウント フィルタで指定された制限を超えると、転送はイベントの転送を停止します。このフィールドでは、カウント制限を指定できます。イベントを転送する前に、Cisco DCNM はその発生がカウント制限を超えていないかどうかを確認します。その場合、イベントは転送されません。

ステップ 6 **[スヌーズ（Snooze）]** チェックボックスを選択して、**[開始（Start）]** 日付と時刻、**[終了（End）]** 日付と時刻を指定します。[Apply] をクリックして、設定を保存します

ステップ 7 **[イベント フォワーダー ルール（Event Forwarder Rules）]** テーブルで、**[+]** アイコンをクリックしてイベント フォワーダー ルールを追加します。

[イベント フォワーダー ルールの追加] ダイアログ ボックスが表示されます。

ステップ 8 **[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 **[ポート]** フィールドが追加されます。

ステップ 9 **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の受信者の 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 サーバー名を入力できます。

ステップ 10 **転送範囲（Forwarding Scope）** では、通知の**[ファブリック/ ローカル エリア ネットワーク（LAN）（Fabric/LAN）]** または**ポート グループ**を選択します。

ステップ 11 **[送信元（Source）]** フィールドで、**[DCNM]** または **[Syslog]** を選択します。

DCNM を選択すると、次のようになります。

a) **[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。
b) **[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。
c) **[最低重大度（Minimum Severity）]** ドロップダウン リストから、受信するメッセージのシビラティ レベルを選択します。
d) **[追加（Add）]** をクリックして、通知を追加します。

[Syslog]を選択しと、次のようになります。

a) **[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。
b) syslog **タイプ**を指定します。
c) **[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。
d) **[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。
e) **[追加（Add）]** をクリックして、通知を追加します。

Note **[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 DCNM 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
```

通知の転送を削除する

通知の転送を削除できます。

Procedure

ステップ 1 **[管理（Administration）] > [イベント設定（Event Setup）] > [転送（Forwarding）]** を選択します。

ステップ 2 削除する通知の前のチェックボックスを選択し、**[削除（Delete）]** をクリックします。

イベント抑制

Cisco DCNM では、ユーザー指定のサプレッサ 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 DCNM Web UIには表示されません。イベントは DCNM 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。

Note Cisco DCNM Web UI から EMC Call Home イベントを抑制することはできません。

このセクションの内容は次のとおりです。

イベント抑制ルールの追加

Cisco DCNM 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。

Procedure

ステップ 1 **[管理（Administration）] > [イベント セットアップ（Event Setup）] > [抑制（Suppression）]** を選択します。

[抑制（Suppression）] ウィンドウが表示されます。

ステップ 2 **[イベント抑制（Event Suppressors）]** テーブルの上にある **[追加（Add）]** アイコンをクリックします。

[イベント抑制ルールの追加（Add Event Suppressor Rule）] ウィンドウが表示されます。

ステップ 3 **[イベント抑制ルールの追加（Add Event Suppressor Rule）]** ウィンドウで、ルールに **Name** を指定します。

ステップ 4 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。**[ローカル エリア ネットワーク（LAN）、ポート グループ（LAN, Port Groups）]** または **[任意（Any）]** を選択できます。**ローカル エリア ネットワーク（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（Port Group）]** 範囲のグループのみ選択できます。範囲として **[任意（Any）]** を選択する場合、抑制ルールはグローバルに適用されます。

ステップ 5 **Facility** 名を入力するか、**LAN Switch Event Facility** 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。

ステップ 6 ドロップダウン リストから、[イベント**Type**（Event）] 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。

ステップ 7 **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。

ステップ 8 **[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。

Note 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 DCNM 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、DCNM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、**[抑制（Suppressor）]** テーブルに移動し、**[イベント抑制ルールの追加（Add Event Suppressor Rule）]** ダイアログ ウィンドウを呼び出します。

Note **[モニタ（Monitor）] > [スイッチ（Switch）] > [イベント（Events）]** を選択して、既知のイベントの抑制ルールを作成します。アカウンティングイベントの抑制ルールを作成する際にショートカットはありません。

イベント抑制ルールを削除

Cisco DCNM Web UI からイベント抑制ルールを削除するには、次の手順を実行します。

Procedure

ステップ 1 **[管理 > イベントをセットアップ > 抑制（Administration > Event Setup > Suppression）]** を選択します。

ステップ 2 リストからルールを選択し、**[Delete（削除）]**アイコンをクリックします。

ステップ 3 確認のために [はい（Yes）] をクリックします。

イベント抑制ルールの変更

イベント抑制ルールを変更するには、次のタスクを実行します。

Procedure

ステップ 1 **[管理（Administration）] > [イベント セットアップ（Event Setup）] > [抑制（Suppression）]** を選択します。

ステップ 2 リストからルールを選択し、**[編集（Edit）]** をクリックします。

[施設（Facility）]、**[タイプ（Type）]**、**[説明一致（Description Matching）]**文字列、および**[有効な時間範囲（Valid time range）]**を編集できます。

ステップ 3 **[適用（Apply）]** をクリックして、変更内容を保存します。

クレデンシャル管理

ユーザー 資格情報管理メニューには、次のサブメニューがあります：

LAN 資格情報

デバイス構成の変更中、Cisco DCNM はユーザーから提供されたデバイスの資格情報を使用します。ただし、LAN スイッチ資格情報がプロビジョニングされない場合、Cisco DCNM では **[管理（Administration）] > [資格情報管理（Credentials Management）] > [LAN 資格情報（LAN Credentials）]** ページを開き、LAN 資格情報を構成するようにプロンプトが表示されます。

Cisco DCNM は、次の 2 つの資格情報のセットを使用して LAN デバイスに接続します。

- **ディスカバリ資格情報**：Cisco DCNM は、デバイスの検出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。
- **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 DCNM はこれらのログイン情報を使用します。

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 スイッチの構成を変更する前に、スイッチの構成変更 SSH ログイン情報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。資格情報が設定されると、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。[スイッチ（Switch）] テーブルのデバイスそれぞれに資格情報を指定して、デフォルトの資格情報を上書きできます。

Note **[パスワード（Password）]**、**[パスワードの確認（Confirm Password）]** フィールドに適切な資格情報を入力して **[保存（Save）]** をクリックした後、**[パスワードの確認（Confirm Password）]** フィールドが空白です。空白の **[パスワードの確認（Confirm Password）]** フィールドは、パスワードが正常に保存されたことを意味します。

Cisco DCNM はまず、[スイッチ（Switch）] テーブルの個別のスイッチ資格情報を使用しようとします。[スイッチ（Switch）] テーブルの資格情報（ユーザー名/パスワード）列が空白の場合、デフォルトの資格情報が使用されます。

スイッチテーブル

[スイッチ（Switch）] テーブルは、ユーザーがアクセスしたすべての LAN スイッチをリストにします。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。

この画面で次の操作を実行できます。

- ログイン情報の編集, on page 636

- 資格情報の検証, on page 636
- スイッチ資格情報のクリア, on page 636
- リモート アクセスによる認証情報管理, on page 637

[DCNM ユーザーの LAN 資格情報（LAN Credentials for the DCNM User）] 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
スイッチ	LAN スイッチ名を表示します。
IP アドレス	スイッチの IP アドレスを指定します。
[ユーザ名（User Name）]	スイッチ DCNM ユーザーのユーザー名を指定します。
パスワード	SSH パスワードの暗号化形式を表示します。
グループ	スイッチが属するグループを表示します。

ログイン情報の編集

次のタスクを実行して、資格情報を編集します。

1. Cisco DCNM ホームページから、**[管理（Administration）] > [資格情報管理（Credentials Management）] > [LAN 資格情報（LAN Credentials）]** を選択し、クレデンシャルを編集する必要がある **[スイッチ（Switch）]** チェックボックスをオンにします。
2. [Edit] アイコンをクリックします。
3. スイッチに **[ユーザー名（User Name）]** および **[パスワード（Password）]** を指定します。

資格情報の検証

資格情報を検証するには、次のタスクを実行します。

1. **[管理（Administration）] > [資格情報管理（Credentials Management）] > [LAN 資格情報（LAN Credentials）]** から、資格情報を検証する必要がある **[スイッチ（Switch）]** チェックボックスを選択します。
2. **[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。

スイッチ資格情報のクリア

次のタスクを実行して、スイッチ資格情報をクリアします。

1. **[管理（Administration）] > [資格情報管理（Credentials Management）] > [LAN 資格情報（LAN Credentials）]**から、資格情報をクリアする必要がある **[スイッチ（Switch）]** チェックボックスをオンにします。
2. [Clear] をクリックします。
3. **[はい（Yes）]** をクリックして、DCNM サーバからスイッチ資格情報をクリアします。

リモート アクセスによる認証情報管理

DCNM では、次のようなさまざまなモードでユーザを認証できます。

- ローカル ユーザー：このモードでは、Cisco DCNM Web UI を使用して、新しいユーザーを作成し、ロールを割り当て、そのユーザーに 1 つ以上のファブリックまたはグループへのアクセスを提供できます。
- リモート ユーザー：このモードでは、DCNM にログインできます。DCNM サーバーは、AAA 認証のために、リモート認証サーバー（Cisco Identity Services Engine（ISE）など）から情報を取得します。シスコは、リモート認証用に TACACS+、RADIUS、および LDAP オプションをサポートしています。詳細については、リモート AAA を参照してください。

リモート認証用に DCNM を構成すると、AAA サーバーは認証と認可の両方を処理します。DCNM は、認証を確認するために入力されたユーザー ログインとパスワードを AAA サーバーに転送します。認証後、AAA サーバーは **cisco-avpair** 属性を介してユーザーに割り当てられた適切な権限/ロールを返します。この属性には、特定のユーザーがアクセスできるファブリックのリストを含めることができます。DCNM LAN 展開でサポートされるロールは次のとおりです。

- network-admin
- network-operator
- network-stager
- access-admin
- device-upg-admin

各ロールは、特定のカテゴリのリソースに対する読み取りおよびオプションの書き込み権限を許可します。DCNM ロールの詳細については、『Cisco DCNM の拡張された役割別のアクセス制御』を参照してください。

デバイス検出ログイン情報と LAN ログイン情報はどちらもデバイスへの書き込みアクセス権を提供しますが、書き込み操作は LAN ログイン情報でのみ実行されるため、両者は異なります。デバイス検出ログイン情報は各デバイスに関連付けられ、デバイスを DCNM にインポートするときに 1 回だけ入力されます。DCNM は、デバイスへの SSH アクセスと SNMPv3 アクセスを組み合わせて使用する定期的な再検出に、これらのログイン情報を使用します。ただし、LAN ログイン情報は、ユーザーごとにすべてのユーザーに対して構成されます。適切なロールを持つユーザーが DCNM にアクセスできる場合、そのユーザーは LAN ログイン情報を入力してデバイスへの書き込みアクセスを取得できます。書き込み操作では、LAN ログイン

情報を使用してデバイスにアクセスします。これにより、すべてのユーザーが DCNM で行った変更と、その結果としてデバイスに加えられた変更の適切な監査証跡が得られます。

TACACS+ や RADIUS などのリモート認証方式を使用して DCNM を構成する場合、ユーザーは次のように LAN ログイン情報を構成できます。

- 通常の AAA リモート認証
- AAA リモート認証パススルー メカニズム
- DCNM サービス アカウントを使用した AAA リモート認証

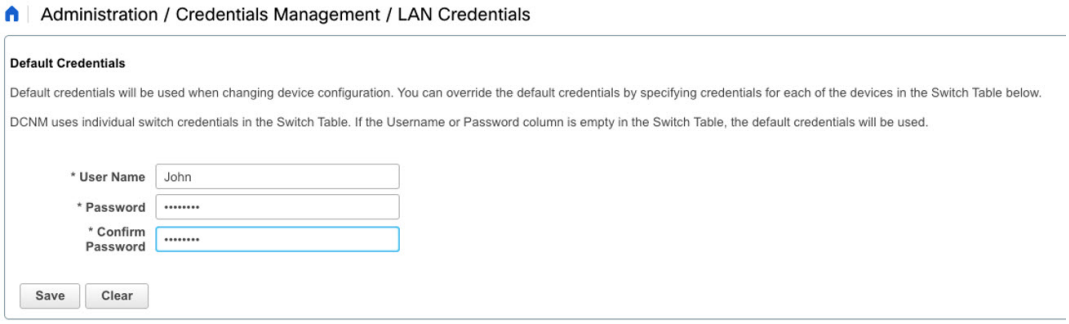
通常の AAA リモート認証

認証後、適切なロールを持つユーザーが初めて DCNM にログインすると、DCNM はユーザーに LAN ログイン情報の入力を求めます。前述のように、DCNM はこれらのログイン情報を使用して、デバイスへの書き込みアクセスを提供します。すべてのユーザーは、このプロセスに従う必要があります。社内のビジネス ポリシーにより、ユーザーは 3 ～ 6 か月ごとにパスワードを変更する必要があるとします。次に、すべてのユーザーは、DCNM **[LAN ログイン情報（LAN Credentials）]** ウィンドウでデバイスにアクセスするためのパスワードを更新する必要があります。また、AAA サーバーでパスワードを更新する必要があります。

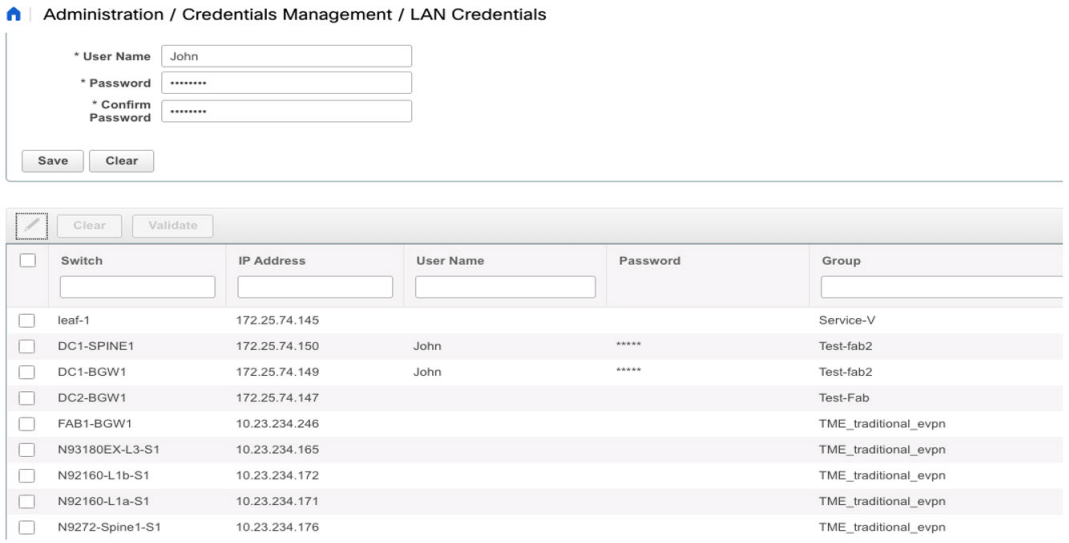
たとえば、ISE サーバーで認証を行う John という名前のユーザーについて考えてみましょう。

1. John は、自分のユーザー ログイン情報を使用して DCNM にログインします。
2. ISE サーバーは John のユーザー ログイン情報を認証し、DCNM は彼の LAN スイッチ ログイン情報を入力するためのメッセージを表示します。DCNM はこれらのログイン情報を使用して、デバイスでさまざまな構成と書き込み操作を実行します。

3. John は、LAN スイッチのログイン情報を入力します。DCNM は、すべてのデバイスで John によってトリガーされるすべての書き込み操作に LAN スイッチ ログイン情報を使用します。ただし、ジョンは、デバイスごとのアクセス ベースで LAN スイッチのログイン情報を入力することを選択することもできます。このデバイスごとのアクセス オプションは、デフォルトのログイン情報を入力することによって提供されるアクセスを上書きします。



Johnが再びDCNMにログインすると、DCNMはLANスイッチログイン情報をすでにキャプチャしているため、LANスイッチログイン情報を入力するためのメッセージを表示しません。Johnは、同じログイン情報を使用して、DCNMおよびアクセス可能なデバイスにログインします。



4. ここで、数か月後に企業のITポリシーが変更されたとします。次に、JohnはリモートAAAサーバーで自分のパスワードを更新する必要があります。また、ステップ3を実行して、DCNMがLANスイッチログイン情報を更新できるようにする必要があります。

したがって、このモードではJohnが更新されたパスワードを使用してDCNM Web GUIにログインすると、DCNMはLANログイン情報を入力するためのメッセージを表示しません。ただし、JohnはLANログイン情報のパスワードを更新する必要があります。DCNMが新しく更新されたパスワードを継承し、デバイスで書き込み操作を実行できるようになるため、パスワードを更新する必要があります。

AAA リモート認証パススルー メカニズム

このモードでは、ユーザーがユーザー名とパスワードを入力してDCNMにログインすると、DCNMはそのユーザーログイン情報をそのユーザーのLANスイッチログイン情報設定のデフォルトログイン情報に自動的にコピーします。その結果、ユーザーが初めてログインしたときに、DCNMはLANスイッチログイン情報を入力するためのメッセージを表示しません。

1. SSH を使用して、sysadmin ユーザーとして DCNM にログインします。
2. **su** コマンドを使用して、/root/ ディレクトリにログインします。
3. /usr/local/cisco/dcm/fm/conf/server.properties ファイルに移動します。
4. 次のサーバー プロパティをファイルに追加し、変更を保存します。

   dcnm.lanSwitch.sameUserAccount=true

```
[root@dcnm sysadmin]# cat /usr/local/cisco/dcm/fm/conf/server.properties | grep dcnm.lan
dcnm.lanSwitch.sameUserAccount=true
[root@dcnm sysadmin]#
```

5. **service FMServer restart** コマンドを使用して DCNM を再起動します。
6. ここで、John は DCNM にログインします。
7. 認証に成功すると、DCNM は LAN スイッチ ログイン情報を更新するためのメッセージを表示しません。これは、この情報が LAN スイッチ ログイン情報に自動的にコピーされるためです。
8. 数か月後、企業の IT ポリシーが変更されたことを考慮してください。このモードでは、John はリモート AAA サーバーでパスワードを更新する必要があります。その後、John が DCNM にログインすると、DCNM は更新されたログイン情報をユーザー John に関連付けられたデフォルトの LAN ログイン情報に自動的にコピーします。

DCNM サービス アカウントを使用した AAA リモート認証

多くの場合、顧客は、共通のサービス アカウントを使用して DCNM コントローラから行われたすべての変更を追跡することを好みます。次の例では、ユーザーが DCNM コントローラを使用して変更を行い、デバイスに変更を加えています。これらの変更は、共通のサービスアカウントに対してデバイス上で監査ログに記録されます。したがって、コントローラによってトリガされた変更を、ユーザーがデバイス上で直接行った他の変更（アウトオブバンド変更とも呼ばれます）と区別することができます。アウトオブバンドの変更は、ユーザーアカウントから行われたデバイス アカウンティング ログに表示されます。

たとえば、リモート AAA サーバーに**ロボット**という名前のサービス アカウントを作成します。対応するログイン情報を使用して、ロボット ユーザーは DCNM にログインできます。ロボット ユーザーは、デフォルトの LAN ログイン情報を入力して、デバイスへの書き込みアクセス権を持つことができます。DCNM network-admin は、すべてのユーザーのデフォルトの LAN ログイン情報を自動的に設定し、ロボットに関連付けられたデフォルトの LAN ログイン情報を継承するサーバー プロパティを有効にします。

したがって、ユーザーが DCNM にログインして設定を変更すると、DCNM はロボットの LAN ログイン情報を使用して変更をデバイスにプッシュします。DCNM 展開履歴ログは、変更をトリガーしたユーザーを追跡し、DCNM からスイッチに展開された対応する変更を、ユーザーロボットの監査ログに表示します。

DCNM でサービス アカウントを設定するには、次の手順を実行します。

1. SSH を使用して、sysadmin ユーザーとして DCNM にログインします。

2. /root/ directory（**su** コマンドを使用）にログインします。
3. /usr/local/cisco/dcm/fm/conf/server.properties ファイルに移動します。
4. 次のサーバー プロパティをファイルに追加し、変更を保存します。

   service.account=robot

（注） AAA パススルー アカウントまたはサービス アカウントのいずれかを有効にできます。

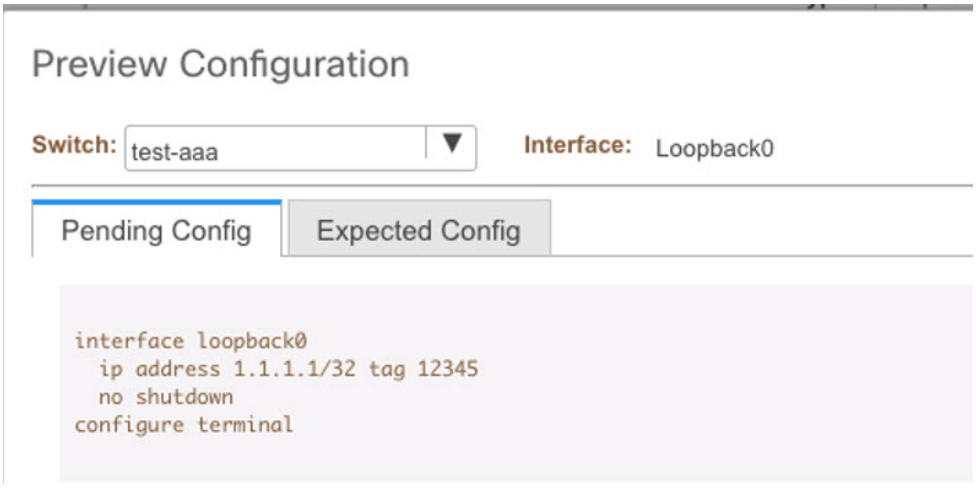
```
[root@dcnm sysadmin]# cat /usr/local/cisco/dcm/fm/conf/server.properties | grep robot
service.account=robot
[root@dcnm sysadmin]#
```

5. **service FMServer restart** コマンドを使用して DCNM を再起動します。
6. ここで、John は DCNM にログインします。
7. 認証に成功した後、DCNM は LAN スイッチ ログイン情報を更新するためのメッセージを表示しません。ただし、John が **[LAN ログイン情報（LAN Credentials）]** ページに移動すると、DCNM は、サービス アカウントが DCNM で有効になっているため、すべての LAN ログイン情報がサービスアカウントから継承されることを示すメッセージを表示します。

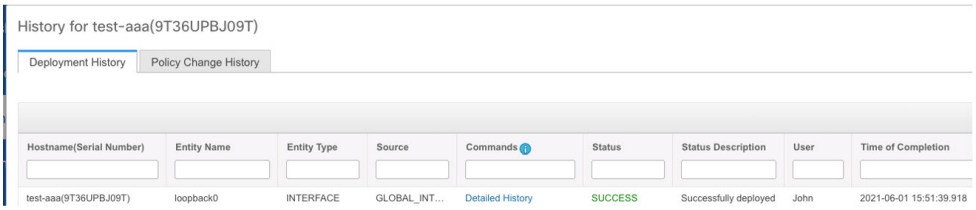
サービス アカウント構成監査

次のワークフローの例では、DCNM サービスアカウント機能の使用中に構成の監査を検証できます。ただし、サービス アカウントのアクティブ化手順を完了している必要があります。

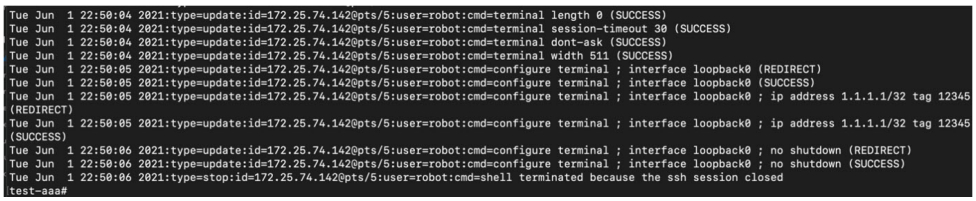
1. John は、デバイスでテスト ループバックを作成します。



2. John は、DCNM を使用して構成を展開します。
3. DCNM 展開の履歴により、John が最近の構成変更を行ったことを確認できます。

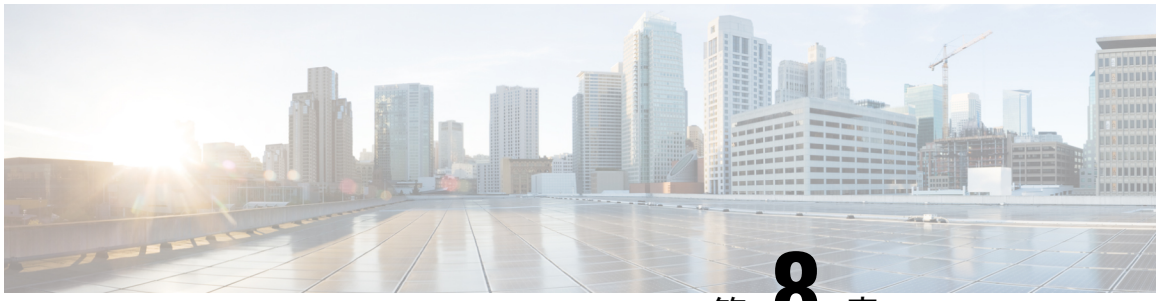


4. デバイスのアカウンティング ログは、DCNM サービス アカウント（つまり、この例ではロボット）が NX-OS デバイスの変更をトリガしたことを示しています。



第 部

アプリケーション



第 8 章

アプリケーション フレームワーク

Cisco Data Center Network Manager（DCNM）は、アプリケーション フレームワークを使用してさまざまなプラグインとマイクロサービスをホストし、Cisco DCNM の操作と関連機能をサポートします。

アプリケーション フレームワークは、次の機能を提供します。

- ネットワークの規模が大きくなるにつれて、より多くのシステム リソースを必要とするアプリケーションをホストするためのインフラストラクチャ。
- アプリケーションの独立したアプリケーション開発、展開、管理のライフサイクル。

Cisco DCNM アプリケーション フレームワークは、クラスタ モードと非クラスタ モードの 2 つのモードをサポートしています。クラスタ モードでは、コンピューティング ノードは一緒にクラスタ化されますが、後者では DCNM サーバ ノード、つまりアクティブ/スタンバイのみが存在します。Network Insights などのほとんどのアプリケーションでは、DCNM アプリケーション フレームワークを使用してアップロードおよび展開する前に、クラスタ化されたセットアップを準備する必要があります。

クラスタ解除モードの Cisco DCNM

Cisco DCNM リリース 11.0(1) 以降、非クラスタ化モードは、スタンドアロンおよびネイティブ HA 環境の両方でのデフォルトの展開モードです。このモードでは、Cisco DCNM は内部サービスの一部をコンテナとしても実行します。

- エンドポイント ロケータは、Cisco DCNM リリース 11.1(1) からコンテナ アプリケーションとして実行されています。
- 構成コンプライアンス サービスは、Cisco DCNM リリース 11.0(1) からのコンテナ アプリケーションです。
- Virtual Machine Manager（VMM）は、Cisco DCNM リリース 11.0(1) からのコンテナ アプリケーションでもあります。

Cisco DCNM は、一部の コンテナ アプリケーションの実行にスタンバイ ノードのリソースを利用します。Cisco DCNM のアクティブノードとスタンバイ ノードは連携して動作し、DCNM とそのアプリケーションの全体的な機能と展開にリソースを拡張します。ただし、一部の高度なアプリケーションを実行したり、システムを拡張して Cisco AppCenter を介して配信されるアプリケーションをさらに導入したりするには、リソースが限られています。たとえば、Cisco AppCenter からダウンロードした Network Insights アプリケーションを、実稼働用に非クラスタ モードで展開することはできません。

アプリケーションをインストールして展開するには、アプリケーションのインストールと展開（660 ページ） を参照してください。

Cisco DCNM およびコンピューティング ノードのすべてのインターフェイスの IP アドレス構成に関するベスト プラクティスと推奨される展開については、展開タイプの『*Cisco DCNM* インストール ガイド』にある「*Cisco DCNM* およびコンピューティングを展開する場合のベスト プラクティス」を参照してください。

クラスタ モードの Cisco DCNM

デフォルトでは、Cisco DCNM 展開で有効になっていない場合、クラスタ モード。Cisco DCNM サーバーを展開した後、クラスタ モードを有効にします。クラスタ モードでは、より多くのコンピューティング ノードを備えた Cisco DCNM サーバは、より多くのアプリケーションを展開するときにリソースを拡張するアーキテクチャを提供します。

コンピューティング ノードは、大規模なファブリックにサービスを提供するためにリソースを大量に消費するサービスを実行するスケールアウト アプリケーション ホスティング ノードです。コンピューティング ノードを追加すると、コンテナであるすべてのサービスがこれらのノードでのみ実行されます。これには、Config Compliance、Endpoint Locator、および Virtual Machine Manager が含まれます。これらの機能の Elasticsearch 時系列データベースは、クラスタ モードのコンピューティング ノードで実行されます。DCNM サーバーは、コンテナ化されたアプリケーションを実行しません。非クラスタ化モードで動作するすべてのアプリケーションは、クラスタ化モードでも動作します。

『*Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment*』の「*Installing Cisco DCNM Compute Node*」を参照してください。

（注） クラスタ モードは、メディア コントローラ展開の Cisco DCNM ではサポートされていません。

Cisco DCNM リリース 11.1(1) 以降、ネイティブ HA セットアップでは、エンドポイント ロケータ、仮想マシン マネージャを備えた 80 個のスイッチの非クラスタ モードで構成コンプライアンスが検証されます。80 スイッチを超えるネットワークで、特定の Cisco DCNM インスタンスにこれらの機能がある場合（最大認定規模は 256 スイッチ）、クラスタ モードを有効にすることをお勧めします。

ネイティブ HA セットアップでは、Endpoint Locator、Virtual Machine Manager、構成コンプライアンスを備えた 80 個のスイッチが非クラスター化モードで検証されます。特定の Cisco DCNM インスタンスでこれらの機能を備えた 80 個のスイッチを超えるネットワークの場合（Cisco DCNM 11.3(1) リリース以降、最大認定スケールは 350 個のスイッチ）、クラスタ化モードを有効にすることをお勧めします。

Cisco DCNM のコア機能はネイティブ HA ノードでのみ実行されますが、80 スイッチを超えるコンピューティング ノードを追加すると、Cisco DCNM および関連サービスのスケールアウト モデルが構築されます。

リリース 11.2(1) から、コンピューティング クラスタのネットワーク管理に IPv6 アドレスを構成できます。ただし、DCNM はコンテナの IPv6 アドレスをサポートしていないため、IPv4 アドレスのみを使用して DCNM に接続する必要があります。

Cisco DCNM およびコンピューティング ノードのすべてのインターフェイスの IP アドレス構成に関するベスト プラクティスと推奨される展開については、展開タイプの『*Cisco DCNM* インストール ガイド』にある「*Cisco DCNM* およびコンピューティングを展開する場合のベスト プラクティス」を参照してください。

Cisco DCNM クラスタ モードの要件

（注） Cisco DCNM をネイティブ HA モードでインストールすることをお勧めします。

ネットワーク インサイトなしの Cisco DCNM LAN ファブリック展開（NI）

（注） *Network Insights*（*NI*）を使用した Cisco DCNM LAN 展開のサイジング情報については、Network Insights ユーザー ガイドを参照してください。

LAN ファブリック展開を管理するために、Cisco DCNM 11.5(1) の検証済みのスケール制限を表示するには、*Cisco DCNM* の検証済みのスケール制限 を参照してください。

表 *24* : 最大 *80* 個のスイッチ

ノード	CPU 展開モード	CPU	メモリー	ストレージ	ネットワーク
DCNM	OVA/ISO	16 vCPU	32G	500G HDD	3xNIC

ノード	CPU 展開モード	CPU	メモリー	ストレージ	ネットワーク
コンピューティング	該当なし	—	—	—	—

表 *25 : 81–350* スイッチ

ノード	CPU 展開モード	CPU	メモリー	ストレージ	ネットワーク
DCNM	OVA/ISO	16 vCPU	32G	500G HDD	3xNIC
コンピューティング	OVA/ISO	16 vCPU	64G	500G HDD	3xNIC

サブネット要件

一般的に、Cisco DCNM サーバの Eth0 は管理に使用され、Eth1 はスイッチ管理と Cisco DCNM アウトオブバンドと接続するために使用され、eth2 は Cisco DCNM のインバンド フロント パネル接続に使用されます。同じ概念がコンピューティング ノードにも拡張されます。クラスタ モードの一部のサービスには、他の要件があります。一部のサービスは、スイッチは Cisco DCNM に到達する必要があります。たとえば、リフレクターをエンドポイント ロケーターに接続したり、ストリーミング テレメトリをアプリケーションのテレメトリ レシーバー サービスに切り替えたりするには、DCNM に到達するためのスイッチが必要です。この IP アドレスは、すべての障害シナリオでスティッキーのままである必要があります。この目的のために、アウトオブバンドとインバンドの両方のサブネットのクラスタ設定時に、IP プールを Cisco DCNM に提供する必要があります。

テレメトリ NTP の要件

テレメトリが正しく機能するためには、Cisco Nexus 9000 スイッチと Cisco DCNM が同期された時刻である必要があります。Cisco DCNM テレメトリ マネージャは、イネーブル化の一部として必要な NTP 設定を行います。スイッチで NTP サーバ設定を手動で変更する使用例がある場合は、DCNM とスイッチが常に時刻同期されていることを確認します。

Cisco DCNM コンピューティングのインストール

（注） ネイティブ HA インストールでは、DCNM がクラスタ モードに変換される前に、HA ステータスが **OK** であることを確認してください。

Cisco DCNM コンピューティングは、通常の Cisco DCNM イメージの ISO または OVA を使用してインストールできます。ISO を使用してベア メタルに直接展開することも、OVA を使用して VM に展開することもできます。DCNM Web インストーラを使用して Cisco DCNM を展

開した後、Cisco DCNM コンピューティング ノードのインストール モードとして **[コンピューティング（Compute）]** を選択します。コンピューティング VM では、DCNM プロセスまたは postgres データベースは見つかりません。アプリケーションのプロビジョニングと監視に必要な最小限のサービス セットを実行します。

『*Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment, Release 11.5(1)*』の「Installing Cisco DCNM Compute Node」を参照してください。

OVA インストールのネットワーク ポリシー

コンピューティング OVA のインストールごとに、ホストの対応する vSwitch に次のネットワーク ポリシーが適用されていることを確認します。

- vCenter にログオンします。
- コンピューティング OVA が実行されているホストをクリックします。
- **[構成（Configuration）] > [ネットワーキング（Networking）]** をクリックします。
- eth1 および eth2 に対応するポート グループを右クリックし、**[設定の編集（Edit Settings）]** を選択します。

  [VM ネットワーク - 設定の編集（VM Network - Edit Settings）] が表示されます。
- [セキュリティ設定] の **[無差別モード（Promiscuous）]** で、**[承諾（Accepted）]** を選択します。
- DVS ポート グループがコンピューティング VM に接続されている場合は、**[vCenter] > [ネットワーキング（Networking）] > [ポート グループ（Port-Group）]** でこれらの設定を構成します。通常の vSwitch ポート グループが使用されている場合は、Compute の各ホストの **[構成（Configuration）] > [ネットワーキング（Networking）] > [ポート グループ（port-group）]** でこれらの設定を構成します。

図 *2 : vSwitch* ポート グループのセキュリティ設定

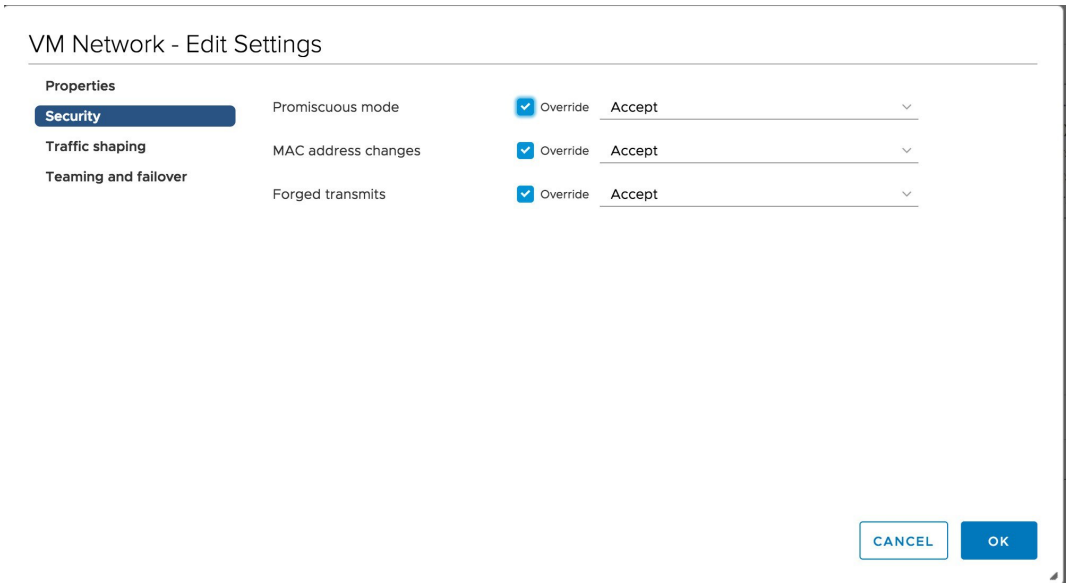
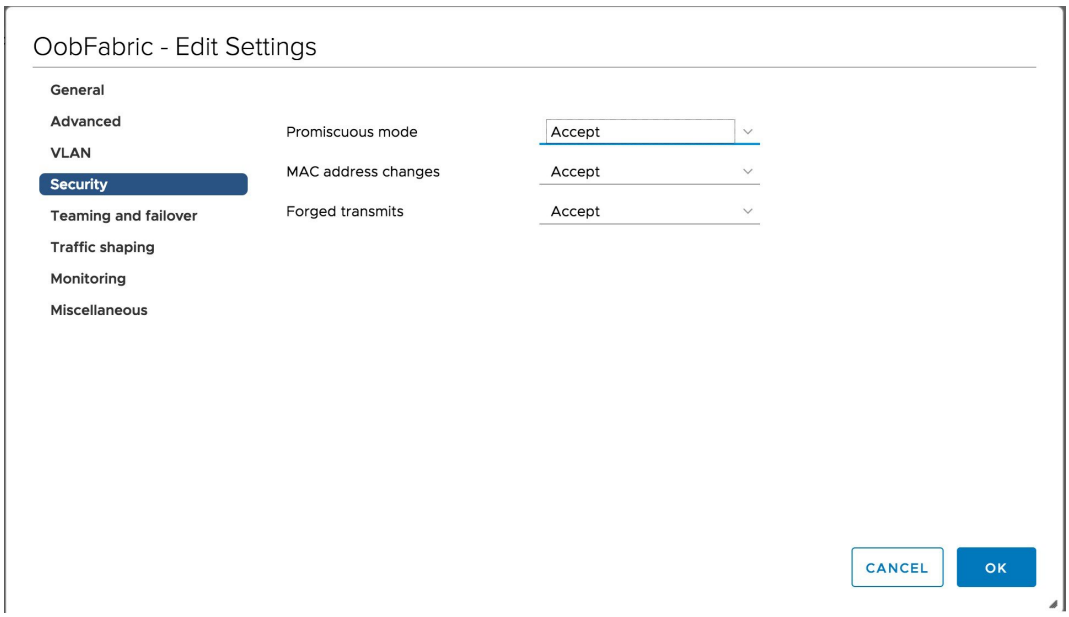


図 *3 : DVSwitch* ポート グループのセキュリティ設定



（注） コンピューティング OVA が実行されているすべてのホストで、この手順を必ず繰り返してください。

コンピューティング クラスタの有効化

（注） アプリケーションをインストールする前に、コンピューティング クラスタが有効になっていることを確認します。AppCenter を介してインストールされた NIR および NIA アプリケーションは、アプリケーションのインストール後にコンピューティング クラスタを有効にすると機能しません。

（注） 構成が完了するまで、サービスは停止します。構成の進行中に、セッションがアクティブであることを確認してください。

（注） Cisco DCNM のインストール中にクラスタ モードを有効にする場合は、クラスタを有効にする必要はありません。コンピューティング ノードは、Cisco DCNM **[Web UI] > [アプリケーション（Applications）] > [コンピューティング（Compute）]** にあります。コンピューティング （665 ページ） に移動してクラスタを形成します。

インストールする間にクラスタされたモードを有効にしなかった場合は、次のコマンドを使用して、コンピューティング クラスタを有効にします。

appmgr afw config-cluster
[--ewpool<*InterApp-Subnet*>*]***--oobpool***<*OutOfBand-Subnet*>***--ibpool***<*Inband-Subnet*>***--computeip***<*compute-ip*>

それぞれの説明は次のとおりです。

- **ewpool**：east-west プールのサブネットを指定します。サービス間接続用。

  展開タイプに合わせて Cisco DCNM のインストール中にアプリケーション間サブネットが指定されている場合、このフィールドはオプションです。これらのアドレスは、コンピューティング間で直接使用されたり、別のノードと通信したりすることはありません。これらは、コンテナが相互に通信するために使用されます。このサブネットは最小 /24（256 アドレス）、最大 /20（4096 アドレス）である必要があります。

  Cisco DCNM 展開のインストール中にアプリ間サブネットが指定されている場合、このフィールドはオプションです。

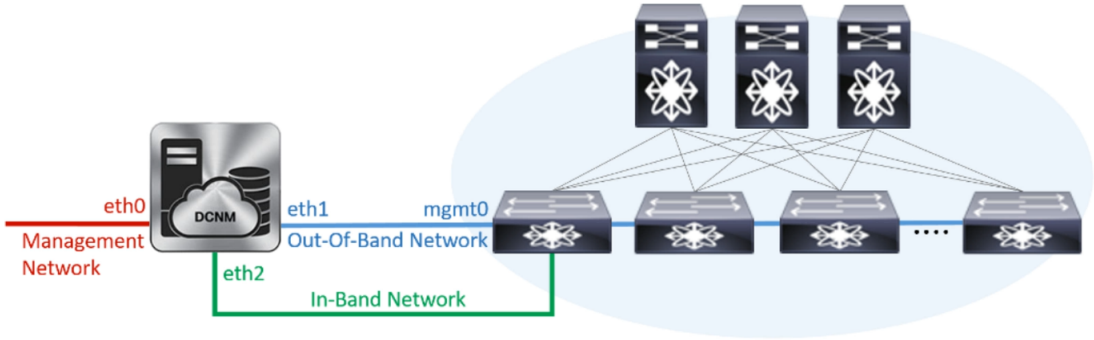
- **oobpool**：アウトオブバンドプールを指定します。 eth1 サブネットから使用可能な IP アドレスのより小さいプレフィックス。例：eth1 サブネットがインストール中に 10.1.1.0/24 に設定された場合、10.1.1.240/28 を使用します。

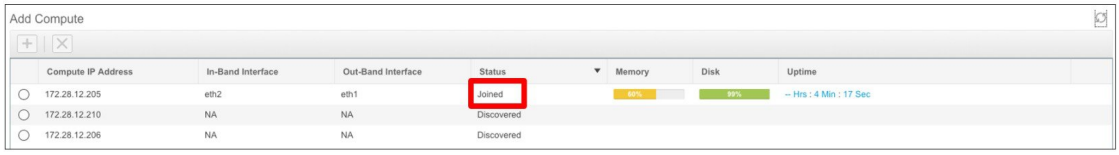
  このサブネットは、最小で /28 (16 アドレス) および最大で /24 (256 アドレス) である必要があります。また、east-west プール以上にしないでください。このサブネットは、スイッチとの通信のためコンテナに割り当てられます。

- **ibpool**：インバンド プールを指定します。使用可能な IP アドレス eth2 サブネットのより小さいプレフィックス。例：eth2 サブネットがインストール中に 11.1.1.0/24 に設定された場合、11.1.1.240/28 を使用します。

  このサブネットは、最小で /28 (16 アドレス) および最大で /24 (256 アドレス) である必要があります。また、east-west プール以上にしないでください。このサブネットは、スイッチとの通信のためコンテナに割り当てられます。

- **computeip**：クラスタに追加された最初のコンピューティング ノードの dcnm-mgmt ネットワーク（eth0）インターフェイス IP アドレスを指定します。このコンピューティングは、このコマンド プロセスの一部としてクラスタに追加され、アプリケーション データを DCNM サーバからコンピューティングに移行するために使用されます。





他の 2 つのコンピューティングは自動的に検出され、Cisco DCNM **[Web UI] > [アプリケーション（Applications）] > [コンピューティング（Compute）]** に表示されます。

インバンドまたはアウトオブバンドプールは、必要に応じてスイッチに接続するためにサービスによって使用されます。これらのプールからの IP アドレスは、構成に使用できる必要があります。

（注） コンピューティングをクラスタ モードに追加するには、クラスタ モードへのコンピューティングの追加 （654 ページ） を参照します。

アプリケーション ネットワーク プールの管理

eth1 または eth2 インターフェイス サブネットを変更する場合は、対応する oob プールとインバンド プールを変更して、新しい構成に一致させる必要があります。Network Insights および

エンドポイント ロケータ アプリケーションは、アウトオブバンドおよびインバンド プールからの IP アドレスを使用します。

コンピューティング クラスタで実行されているサービスに割り当てられている IP アドレスを変更するには、次のコマンドを使用します。

（注） インバンドまたはアウトオブバンド プールは、アプリケーションが Cisco Nexus スイッチに接続するために使用します。したがって、これらのプールからの IP アドレスは、使用可能で空いている必要があります。

appmgr afw config-pool [--ewpool *<InterApp-Subnet>]* **--oobpool** *<OutOfBand-Subnet>* **--ibpool** *<Inband-Subnet>***--compute***<compute-IP>*

それぞれの説明は次のとおりです。

- **ewpool**：イースト ウエスト プールのサブネットを指定します。サービス間接続用。

  ネットワーク マスクの範囲は 20 から 24 です。これらのアドレスは、コンピューティング間で直接使用されたり、別のノードと通信したりすることはありません。これらは、コンテナが相互に通信するために使用されます。

- **oobpool**：アウトオブバンド プールを指定します。 eth1 サブネットからの利用可能な IP アドレスのより小さいプレフィックス。

  ネットワーク マスクの範囲は 24 ～ 28 です。

- **ibpool**：インバンド プールを指定します。 eth2 サブネットからの利用可能な IP アドレスのより小さなプレフィックス。

  ネットワーク マスクの範囲は 24 ～ 28 です。

- **ipv6oobpool**：アウトオブバンド IPv6 プールを指定します。 eth1 サブネットからの利用可能な IPv6 アドレスのより小さいプレフィックス。

  IPv6 が有効になっている場合、これらのアドレスは帯域内サブネットと帯域外サブネットの両方で必要です。

  ネットワーク マスクの範囲は 112 ～ 124 です。

- **ipv6ibpool**：インバンド IPv6 プールを指定します。 eth2 サブネットからの利用可能な IPv6 アドレスのより小さいプレフィックス。

  IPv6 が有効になっている場合、これらのアドレスは帯域内サブネットと帯域外サブネットの両方で必要です。

  ネットワーク マスクの範囲は 112 ～ 124 です。

クラスタ モードへのコンピューティングの追加

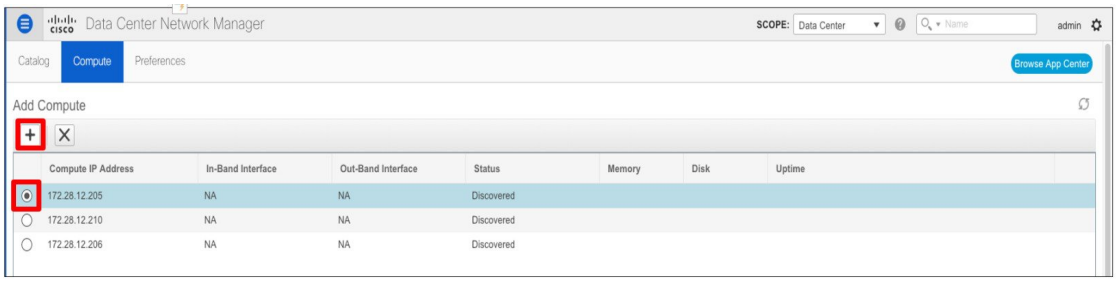
Cisco DCNM Web UI からクラスタ モードにコンピューティングを追加するには、次の手順を実行します。

手順

ステップ 1 **[アプリケーション（Applications）] > [コンピューティング（Compute）]** を選択します。

[コンピューティング（Compute）] タブには、Cisco DCNM で有効になっているコンピューティングが表示されます。

ステップ 2 **[検出済み（Discovered）]** ステータスのコンピューティング ノードを選択します。**[コンピューティングの追加（Add Compute）]** (+) アイコンをクリックします。

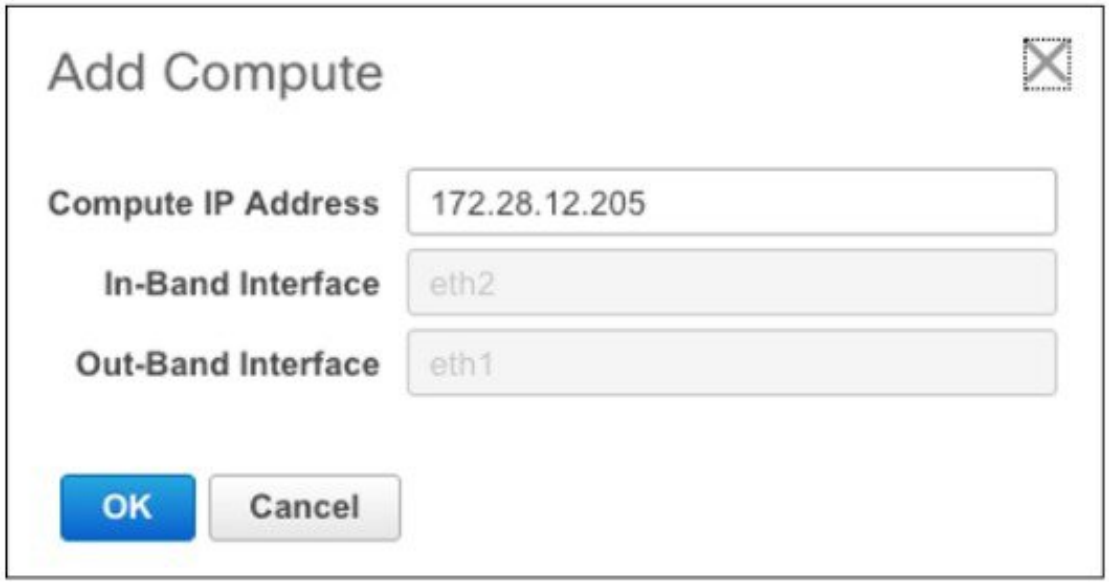


- [コンピューティング（Compute）] を使用している間、Cisco DCNM GUI にノードが [参加済み（Joined）] と表示されていることを確認します。
- [オフライン（Offline）] は接続の問題を示しているため、オフライン コンピューティングで実行されているアプリケーションはありません。
- [失敗（Failed）] は、コンピューティング ノードがクラスタに参加できなかったことを示します。
- ヘルスは、コンピューティング ノードの空きメモリとディスクの量を示します。[ヘルスモニタ] アプリケーションは、より詳細な統計情報を提供します。
- Cisco DCNM 3 ノードクラスタは、単一ノード障害に対してのみ回復力があります。
- インラインアップグレード中またはその後、およびすべてのコンピューティングが結合済みに変更された後で Performance Manager が停止した場合、Performance Manager を再起動する必要があります。

[コンピューティング（Compute）] ウィンドウでは、コンピューティングの正常性をモニタリングできます。正常性は本質的に、コンピューティングで残されたメモリの大きさを示し、これは有効化されたアプリケーションに基づいています。コンピューティングが DCNM サーバと適切に通信していない場合、コンピューティングのステータスはオフラインとして表示され、オフライン コンピューティングでは実行されているアプリケーションはありません。

ステップ 3 **[コンピューティングの追加（Add Compute）]** ダイアログ ボックスで、**[コンピューティング IP アドレス（Compute IP Address）]**、**[帯域内インターフェイス（In-Band Interface）]**、および**[帯域外インターフェイス（Out-Band Interface）]** 値を確認してください。

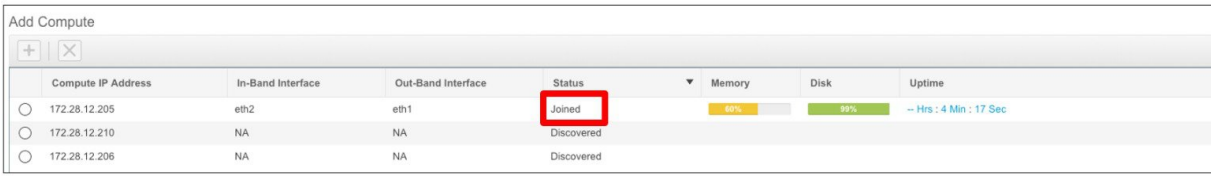
（注） 各コンピューティング ノードのインターフェイス値は、**appmgr afw config-cluster** コマンドを使用して設定されます。



ステップ 4 [OK] をクリックします。

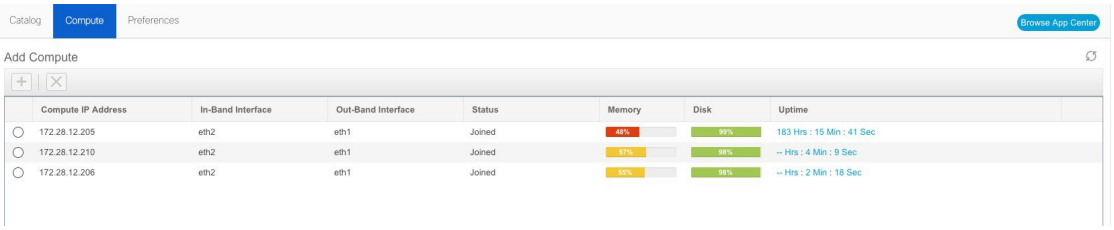
そのコンピューティング IP のステータスを **[結合（Joining）]** に変更します。

コンピューティング IP ステータスが **[結合済み（Joined）]** として表示されるまで待ちます。



ステップ 5 残りのコンピューティング ノードを追加するために、上記の手順を繰り返します。

すべてのコンピューティングが **[結合済み（Joined）]** として表示されます。



（注） VMware プラットフォームの仮想マシンとしてコンピューティングをインストールするときに、eth1 と eth2 に関連付けられた vSwitch または DV スイッチ グループは、eth1 および eth2 以外の Mac アドレスと関連付けられたパケットに対して転送することを許可しなければなりません。

コンピューティング ノードの移行

VM からサービス エンジンにコンピューティング ノードを移行する

Cisco DCNM Web クライアントを使用して Cisco DCNM コンピュート ノードを VM から Applications Services Engine に移行するには、次の手順を実行します。

始める前に

- Cisco DCNM Web クライアントが機能していることを確認します。
- [Cisco DCNM **Web Client**] > **[アプリケーション（Applications）]** > **[コンピューティング（Compute）]** で、すべてのコンピューティング ノードが **結合**状態になっている必要があります。

手順

ステップ 1 **[アプリケーション（Applications）]** > **[コンピューティング（Compute）]** を選択します。

たとえば、3 つのコンピューティング ノードを **compute1** 、 **compute2** 、 **compute3** と示します。

ステップ 2 vCenter サーバ アプリケーションを開き、vCenter ユーザー クレデンシャルを使用して vCenter サーバに接続します。

ステップ 3 **[ホーム（Home）]** > **[インベントリ（Inventory）]** > **[ホストおよびクラスタ（Hosts and Clusters）]** に移動し、DCNM コンピューティング ノードが展開されている VM を特定します。

ステップ 4 **compute1** については、インストール中に提供された構成とセットアップの詳細を書き留めます。

ステップ 5 **compute1** をオフにします。VM を右クリックし、**[電源オフ（Power off）]** を選択します。

[Web UI] > [アプリケーション（Applications）] > [コンピューティング（Compute）] で、**compute1** のステータスが**オフライン**と表示されます。

ステップ 6 コンピューティング ノード VM の構成の詳細を使用して、コンピューティング ノードを Cisco Applications Services Engine にインストールします。

マニュアルについては、「*Cisco ASE* で *DCNM* コンピューティング ノードをインストールする」を参照してください。

ステップ 7 Web UI を起動し、**[アプリケーション（Applications）] > [コンピューティング（Compute）]** を選択します。

新しく追加されたコンピューティングは、自動的にクラスタに参加します。**compute1** のステータスが **Offline → Joining → Joined** に変わります。

ステップ 8 ステップ ステップ 4 （656 ページ） ～ ステップ 7 （657 ページ） を、**compute2** および **compute3** コンピューティング ノードで繰り返します。

完了後、**[Web UI] > [アプリケーション（Applications）] > [コンピューティング（Compute）]** のすべてのコンピューティング ノードが**結合**状態になります。

すべてのコンピューティング ノードは、Cisco Applications Services Engine で正常にホストされています。

サービス エンジンから VM にコンピューティング ノードを移行する18-10-2022 13:39

Cisco DCNM Web クライアントを使用して、アプリケーション サービス エンジンから VM に Cisco DCNM コンピューティング ノードを移行するには、次の手順を実行します。

始める前に

- Cisco DCNM Web クライアントが機能していることを確認します。
- [Cisco DCNM **Web Client**] > **[アプリケーション（Applications）] > [コンピューティング（Compute）]** で、すべてのコンピューティング ノードが **結合**状態になっている必要があります。

手順

ステップ 1 **[アプリケーション（Applications）] > [コンピューティング（Compute）]** を選択します。

たとえば、3 つのコンピューティング ノードを **compute1** 、 **compute2** 、 **compute3** と示します。

ステップ 2 Cisco Applications Server コンソールで、**compute1** について、インストール中に提供された構成とセットアップの詳細を書き留めます。

ステップ 3 アプリケーション サービス エンジンの電源をオフにして、**compute1** をオフにします。

[Cisco DCNM **Web UI**] > **[アプリケーション（Applications）]** > **[コンピューティング（Compute）]** で、**compute1** のステータスが**オフライン**と表示されます。

ステップ 4 アプリケーション サービス エンジンのコンピューティング ノードの構成の詳細を使用して、VM にコンピューティング ノードをインストールします。

詳細は、「ISO 仮想アプライアンスで DCNM をインストールする」を参照してください。

ステップ 5 Web UI を起動し、**[アプリケーション（Applications）]** > **[コンピューティング（Compute）]** を選択します。

新しく追加されたコンピューティングは、自動的にクラスタに参加します。**compute1** のステータスが **Offline → Joining → Joined** に変わります。

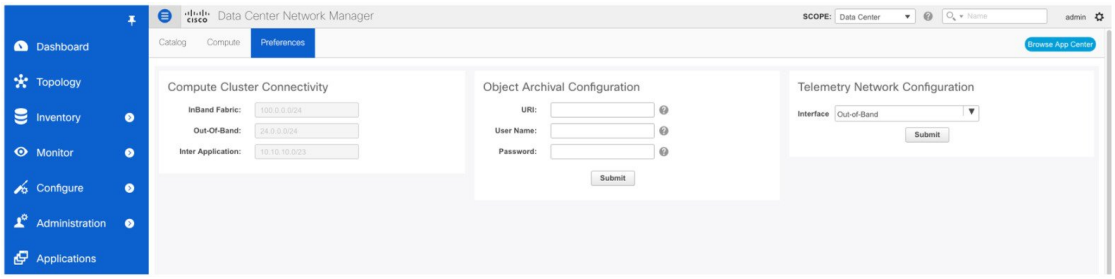
ステップ 6 **compute2** および **compute3** コンピューティング ノードで手順 3 から 5 を繰り返します。

完了後、**[Web UI]** > **[アプリケーション（Applications）]** > **[コンピューティング（Compute）]** のすべてのコンピューティング ノードが**結合**状態になります。

すべてのコンピューティング ノードが VM で正常にホストされています。

初期設定

このタブは、アプリケーションインスタンスが配置されるクラスタ モードに関連しています。このタブでは、クラスタ接続を計算し、[Cluster Connectivity] 基本設定を行うことができます。



コンピューティング クラスタ接続

フィールドには、クラスタ ノードの接続インターフェイスの設定に使用される IP アドレスが表示されます。インバンドファブリック、アウトオブバンドファブリック、およびアプリケーション間 の IP アドレスが表示されます。

オブジェクト アーカイブの設定

NIA アプリケーションは、ファブリック内のすべてのスイッチのテクニカル サポート ログを収集し、データに基づいてアドバイザリを決定します。ログは、さらに分析またはトラブルシューティングするために Cisco DCNM サーバに保存されます。期限が切れる前にこれらのログをダウンロードする必要がある場合、または DCNM サーバにスペースを作成する必要がある場合は、ログをリモート サーバに移動できます。

[URI] フィールドに、アーカイブ フォルダーへの相対パスを host[:port]/[path to archive] の形式で入力します。**[ユーザー名（Username）]**および**[パスワード（Password）]** フィールドに、ユーザー名とパスワードを入力します。**[送信（Submit）]**をクリックして、リモート データベースを設定します。

テレメトリおよび NTP 要件

Network Insights Resource（NIR）アプリケーションの場合、NIR 内で実行されている UTR マイクロサービスは、アウトオブバンド（Eth1）またはインバンド（Eth2）インターフェイスを介してスイッチからテレメトリ トラフィックを受信します。デフォルトでは、テレメトリは構成され、アウトオブバンド インターフェイス経由でストリーミングされます。[インバンド インターフェイス（In-Band interface）] に変更することもできます。

Cisco Network Insights for Resources（NIR）リリース2.1以降、およびフローテレメトリの場合、feature lldpコマンドは必須設定の1つです。

シスコは、Easy Fabric 展開、つまり eBGP ルーテッド ファブリックまたは VXLAN EVPN ファブリックの場合にのみ、**lldp** 機能をスイッチにプッシュします。したがって、NIRユーザは、次のシナリオですべてのスイッチで機能lldpを有効にする必要があります。

- モニタモードまたは管理モードの外部ファブリック
- モニタモードまたは管理モードの LAN クラシック ファブリック（DCNM 11.4(1) 以降で該当）

アウトオブバンド（OOB）ネットワークを使用したテレメトリ

デフォルトでは、テレメトリ データは、スイッチの管理インターフェイスを介して Cisco DCNM OOB ネットワーク eth1 インターフェイスにストリーミングされます。これは、Cisco DCNM LAN ファブリック展開のすべてのファブリック、または Cisco DCNM クラシック LAN 展開のスイッチ グループのグローバル構成です。テレメトリが NIR アプリケーションによって有効になった後、Cisco DCNM のテレメトリ マネージャは、DCNM OOB ド IP アドレスを NTP サーバ IP アドレスとして使用して、必要な NTP サーバ構成をスイッチにプッシュします。次の例は、**show run ntp** コマンドの出力例です。

```
switch# show run ntp

!Command: show running-config ntp
!Running configuration last done at: Thu Jun 27 18:03:07 2019
!Time: Thu Jun 27 20:32:18 2019

version 7.0(3)I7(6) Bios:version 07.65
ntp server 192.168.126.117 prefer use-vrf management
```

（注） OOB からインバンドに変更しようとすると、エラー「**アプリはこのネットワークで実行されています。」最初に無効にしてから再試行してください。**」が表示されます。。Network Insights がこのネットワークを使用するように構成されている場合は、すべてのファブリックの構成を無効にしてから再試行してください。

アプリケーションのインストールと展開

次のセクションは、Cisco DCNM Web UI からアプリケーションをダウンロード、追加、開始、停止、および削除する方法を説明します。

App Store からのアプリのダウンロード

Cisco DCNM Web UI から新しいアプリケーションをダウンロードするために、次の手順を実行してください。

1. **アプリケーション** を選択します。

   デフォルトで **[カタログ（Catalog）]** タブが表示されます。

2. ウィンドウの右上隅の **[App Center の参照]** をクリックします。

   Cisco ACI App Center で、必要なアプリケーションを検索し、ダウンロード アイコンをクリックします。

3. ローカル ディレクトリにアプリケーション実行ファイルを保存します。

DCNM に新しいアプリケーションを追加します。

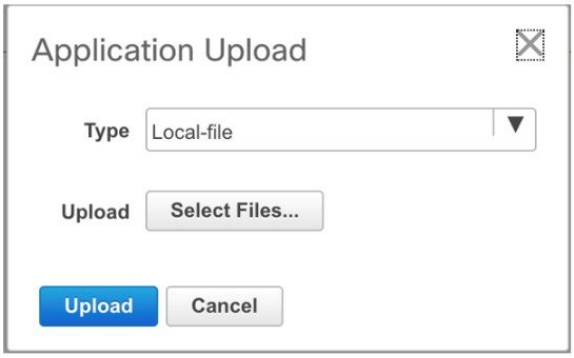
Cisco DCNM Web UI から新しいアプリケーションを追加するために、次の手順に従ってください。

1. **アプリケーション** を選択します。

   デフォルトで **[カタログ（Catalog）]** タブが表示されます。

2. **[アプリケーションの追加 (+)（Add Application (+)）]** アイコンをクリックします。

[アプリケーションのアップロード（Application Upload）] ウィンドウで、[タイプ] ドロップダウン フィールドから、アプリケーションをアップロードするために次の 1 つを選択します。



[タイプ] ドロップダウン リストから次のうちの 1 つを選択します。

- ファイルがローカル ディレクトリで見つかった場合、**Local-file** を選択します。

  [アップロード（Upload）] フィールドで、**[ファイルの選択（Select files）]** をクリックします。アプリケーション ファイルを保存したディレクトリに移動します。

  アプリケーション ファイルを選択し、**[開く（Open）]** をクリックします。

  [Upload] をクリックします。

- アプリケーションがリモート サーバにある場合、**セキュアなコピー**を選択してください。

（注） リモート サーバはセキュアなコピー（SCP）を扱えることを確認してください。

URI フィールドにアプリケーション ファイルへのパスを指定します。パスは `{host-ip}:{filepath}` の形式でなければなりません。

[ユーザー名（Username）] フィールドに、URI にアクセスするためにユーザー名を入力します。

[パスワード（Password）] フィールドに、URI にアクセスするための適切なパスワードを入力します。

[Upload] をクリックします。

アプリケーションを正常にアップロードすると、[カタログ（Catalog）] ウィンドウに表示されます。

左上隅の緑のアイコンは、アプリケーションが正常に起動し、操作可能であることを示します。アプリケーションに緑のアイコンがない場合は、アプリケーションが実行中でないことを示します。アプリケーションをクリックして、起動します。

（注） アプリケーションをインストールする前に、クラスタのコンピューティングが有効になっていることを確認します。クラスタのコンピューティングがアプリケーションの起動後に構成された場合、いくつかのアプリケーションが動作しないことがあります。

アプリケーション アイコンの左下のギア アイコンをクリックして、アプリケーションの仕様を表示します。[情報] タブは実行中のコンテナ情報を表示します。[仕様] タブは構成を表示します。

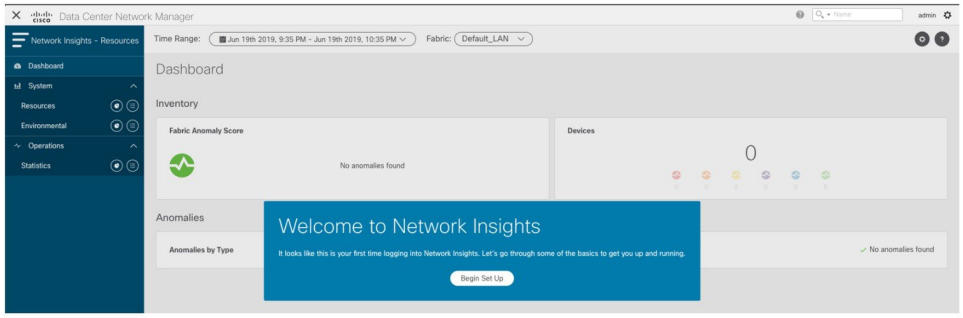
アプリケーションの開始

アプリケーションを Cisco DCNM サーバにインストールしたら、アプリケーションを展開する必要があります。アプリケーションをクリックして、展開を開始します。Cisco DCNM は、アプリケーションに必要なバックエンドのすべてのサービスを開始します。

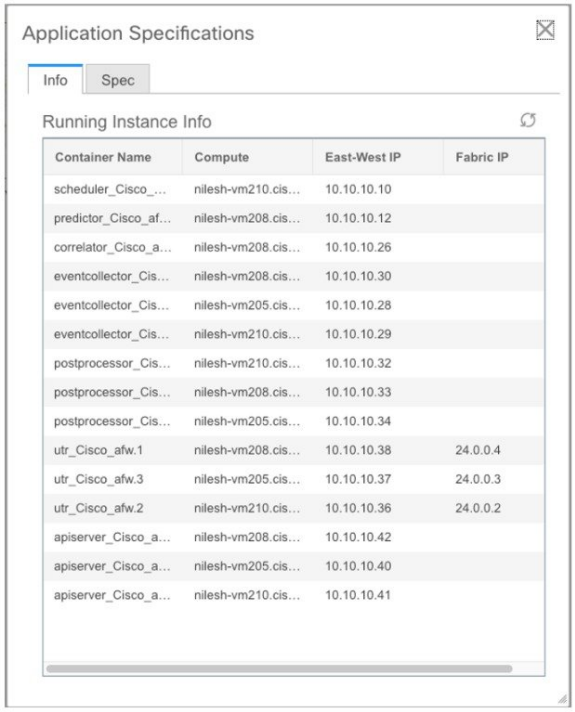
左上隅の緑のアイコンは、アプリケーションが正常に起動し、操作可能であることを示します。

Kafka インフラストラクチャ サービスを利用するアプリケーションでは、アプリケーションの開始時に 3 つのアクティブに結合されたコンピューティング ノードを必要とします。たとえば、NIR と NIA アプリケーションです。アプリケーションにユーザー インタフェイスがある場合、アプリケーションが正常に起動された後で、UI がアプリケーションによりサービスされたインデックス ページに導きます。

アプリケーションにユーザーインタフェイスがある場合、アプリケーションが正常に起動された後で、UI がアプリケーションによりサービスされたインデックス ページに導きます。



実行中のサービスを確認するには、**Applications > Catalog** に戻ります。アプリケーション アイコンの左下のギアアイコンをクリックして、アプリケーションの仕様を表示します。[情報] タブは実行中のコンテナ情報を表示し、[仕様] タブは下図で示されるとおり構成を表示します。



クラスタからコンピューティングを削除する方法やアプリケーションの停止または削除方法については、アプリケーション フレームワーク ユーザー インターフェイス （664 ページ） を参照してください。

アプリケーションの停止および削除

Cisco DCNM Web UI のカタログからアプリケーションを削除するには、次の手順に従ってください。

1. **アプリケーション** を選択します。

   デフォルトで、**[カタログ（Catalog）]** タブが表示され、すべてのインストールされたアプリケーションが示されます。

2. アプリケーションを停止するには、右下隅の赤いアイコンをクリックします。

3. **[ボリュームのワイプ]** チェックボックスをオンにして、そのアプリケーションに関連するすべてのデータを消去します。

4. **[停止]** をクリックして、アプリケーションの Cisco DCNM.wa から のデータストリーミングを停止します。

   アプリケーションが正常に停止すると、緑のアイコンが消えます。

5. アプリケーションを停止した後で、**[ゴミ箱]** アイコンからカタログのアプリケーションを削除します。

アプリケーション フレームワーク ユーザー インターフェイス

アプリケーション フレームワーク機能を使用するために、Cisco DCNM ホームページの左ウィンドウで、**[アプリケーション]** をクリックします。

[アプリケーション] ウィンドウに次のタブが表示されます。

- **Catalog**—このタブは Cisco DCNM で使用されるアプリケーションをリストします。Cisco DCNM 内でさまざまな機能を実行するこれらのアプリケーション。詳細については、*Catalog* を参照してください。
- **Compute**—のタブは既存のコンピューティング ノードを表示します。タブは、ホスティング インフラストラクチャの一部であるノードを示します。アップタイムは、それらがインフラストラクチャの一部であった時間を示します。高可用性（HA）設定では、アクティブとスタンバイ ノードが結合されているものとして表示されます。詳細については、コンピューティング （665 ページ）を参照してください。

（注） クラスタモードでは、Cisco DCNM サーバは [コンピューティング（Compute）] タブに表示されません。

- **[設定（Preferences）]**：このタブは、アプリケーション インスタンスが配置される展開のクラスタ モードに関連しています。このタブでは、クラスタ接続をコンピューティングし、[クラスタ接続（Cluster Connectivity）] 基本設定を行うことができます。詳細については、初期設定 （658 ページ）を参照してください。

Cisco DCNM は次のアプリケーションを使用します。

- Compliance：このアプリケーションは、Easy Fabric インストール用のファブリックの構築に役立ちます。Compliance アプリケーションは、ファブリックあたり 1 つのインスタンスとして実行されます。ファブリックの作成時に有効になります。同様に、ファブリックが削除されるときに無効になります。
- DCNM Kibana (1.0)：Kibana は、可視化機能を提供する、Elasticsearch 用のオープンソース データ可視化プラグインです。Cisco DCNM は、メディア コントローラ、Endpoint Locator のために Kibana アプリケーションを使用します。
- vmmplugin: Virtual Machine Manager (VMM) プラグインは、Cisco DCNM にロードされているファブリックまたはスイッチ グループに接続するすべてのコンピューティングと仮想マシンの情報を保存します。VMM は、コンピューティング リポジトリ情報を収集し、VM、VSwitches/DVS、ホストをトポロジ ビューに表示します。
- Endpoint Locator：Endpoint Locator（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、IP アドレスと MAC アドレスを持つものです。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。

カタログ

カタログを使用すると、Cisco DCNM でインストールまたは有効にしたすべてのアプリケーションを表示できます。Cisco DCNM をインストールすると、ほとんどのアプリケーションはインストールされず、デフォルトで動作します。

Cisco DCNM 展開に基づいて、次のアプリケーションが表示されます。

- Health Monitor (2.1)
- PTP Monitoring (1.1)
- Kibana (2.0)
- Programmable report (1.1.0)
- Elastic Service (1.1)
- Compliance (4.0.0)
- Debug Tools (2.1)
- IPAM Integrator (1.0)
- Endpoint Locator (2.1)
- Kubernetes Visualizer (1.1)
- vmmplugin (4.1)

Note デフォルトで起動されたアプリケーション、または DCNM にインストールされたインフラストラクチャ サービスを使用するアプリケーションは、デフォルトで動作します。

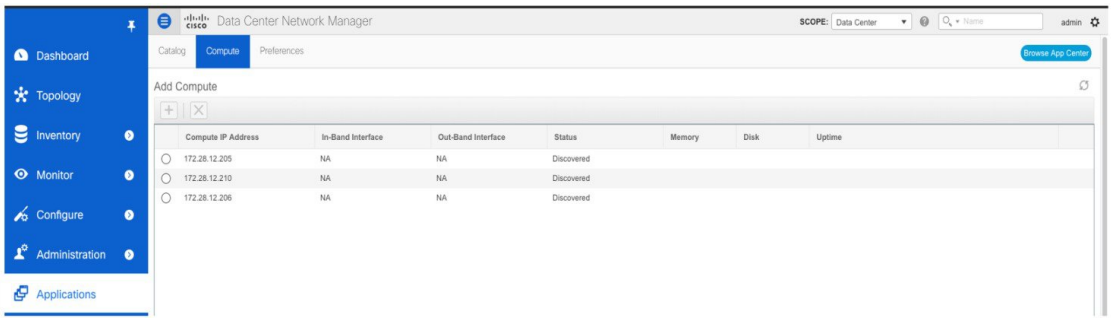
Web UI を介して App Center から追加のアプリケーションをインストールできます。

Cisco DCNM Web UI からのアプリケーションのダウンロード、追加、起動、停止、および削除の手順については、アプリケーションのインストールと展開, on page 660 を参照してください。

コンピューティング

このタブは既存のコンピューティング ノードを表示します。タブは、ホスティング インフラストラクチャの一部であるノードを示します。アップタイムは、それらがインフラストラクチャの一部であった時間を示します。高可用性（HA）設定では、アクティブとスタンバイ ノー

ドが結合されているものとして表示されます。クラスタモードでは、コンピューティングノードのステータスで、ノードが結合されているか、発見されたかを示します。



（注） コンピューティング ノードの NTP サーバが DCNM サーバ（アクティブとスタンバイ）とコンピューティングのための NTP サーバと同期されていない場合、クラスタを構成することはできません。

証明書はタイムスタンプ付きで生成されます。異なる NTP サーバを使用してコンピューティング ノードを構成する場合、タイムスタンプの不一致により証明書の検証が許可されなくなります。したがって、NTP サーバの不一致にもかかわらず、コンピューティング クラスタが構成される場合、アプリケーションは適切に機能しなくなります。

（注） クラスタ モードで、Cisco DCNM サーバは [コンピューティング（Compute）] タブの下に表示されません。

下表は**[アプリケーション（Applications）]>[コンピューティング（Compute）]**に表示されるフィールドを説明します。

表 *26 : [*コンピューティング（*Compute***）*]* タブのフィールドと説明**

フィールド	説明
コンピューティング IP アドレス	コンピューティング ノードの IP アドレスを指定します。
インバンド インターフェイス	インバンド管理インターフェイスを指定します。
アウトバウンド インターフェイス	アウトバウンド管理インターフェイスを指定します。

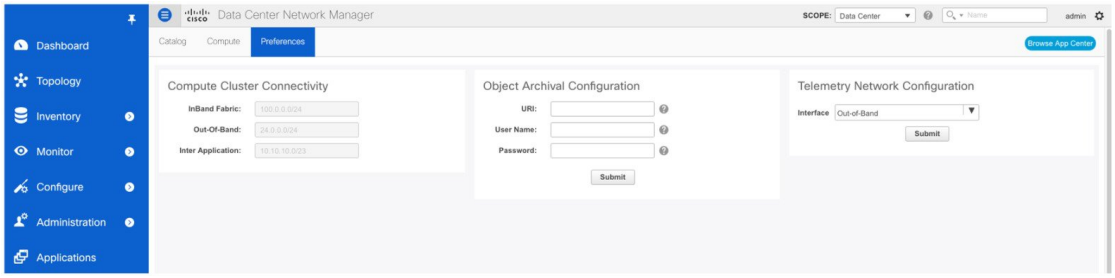
フィールド	説明
ステータス	コンピューティング ノードのステータスを指定します。 • 参加 • Discovered • Failed • Offline
メモリ	ノードごとに消費されるメモリを指定します。
ディスク	コンピューティング ノードで消費されるディスク スペースを指定します。
Uptime	コンピューティング ノードのアップタイムの時間を指定します。

コンピューティング ノードを正しいパラメータでインストールすると、[ステータス（Status）] 列に **[結合済み（Joined）]** と表示されます。しかし、他の 2 つのコンピューティングが [発見済み（Discovered）] として表示されます。Cisco DCNM Web UI からクラスタ モードにコンピューティングを追加するには、クラスタ モードへのコンピューティングの追加 （654 ページ） を参照してください。

クラスタ接続の基本設定を構成または変更するには、初期設定 （658 ページ） を参照してください。

初期設定

このタブは、アプリケーション インスタンスが配置されるクラスタ モードに関連しています。このタブでは、クラスタ接続を計算し、[Cluster Connectivity] 基本設定を行うことができます。



コンピューティング クラスタ接続

フィールドには、クラスタ ノードの接続インターフェイスの設定に使用される IP アドレスが表示されます。インバンドファブリック、アウトオブバンドファブリック、およびアプリケーション間 の IP アドレスが表示されます。

オブジェクト アーカイブの設定

NIA アプリケーションは、ファブリック内のすべてのスイッチのテクニカル サポート ログを収集し、データに基づいてアドバイザリを決定します。ログは、さらに分析またはトラブルシューティングするためにCisco DCNM サーバに保存されます。期限が切れる前にこれらのログをダウンロードする必要がある場合、またはDCNM サーバにスペースを作成する必要がある場合は、ログをリモート サーバに移動できます。

[URI] フィールドに、アーカイブ フォルダーへの相対パスを `host[:port]/[path to archive]` の形式で入力します。**[ユーザー名（Username）]** および **[パスワード（Password）]** フィールドに、ユーザー名とパスワードを入力します。**[送信（Submit）]** をクリックして、リモート データベースを設定します。

障害シナリオ

DCNM OVA のインストールで最小限の冗長性構成を確保するための推奨設定は、

- server1 の DCNM アクティブ ノード（アクティブ）およびコンピューティング ノード 1。
- server2 の DCNM スタンバイ ノードおよびコンピューティング ノード 2。
- server3 のコンピューティング ノード 3。

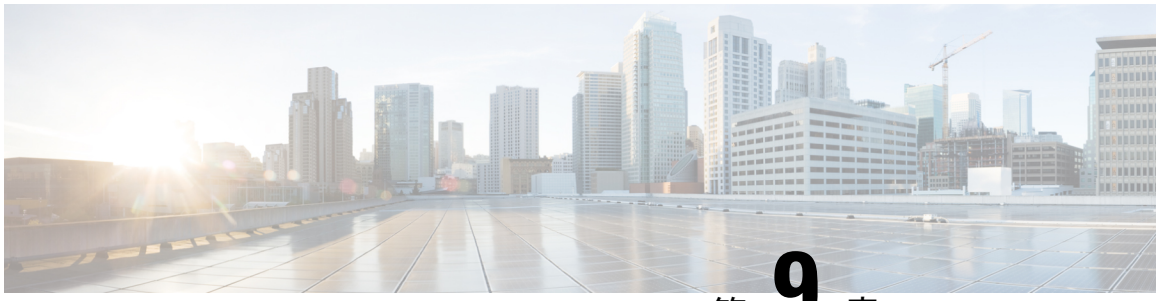
DCNM アクティブ ノードがダウンすると、スタンバイ ノードがコア機能の実行の全責任を負います。

コンピューティング ノードがダウンしても、アプリケーションは機能が制限されて機能し続ける可能性があります。この状況が長期間続くと、アプリケーションのパフォーマンスと信頼性に影響します。複数のノードがダウンすると、アプリケーションの機能に影響し、ほとんどのアプリケーションが機能しなくなります。

常に3つのコンピューティングノードを維持する必要があります。コンピューティング ノードがダウンした場合は、サービスが期待どおりに機能するように、できるだけ早く問題を修正してください。

コンピューティング ノードの障害復旧

障害によりコンピューティング ノードが失われ、回復不能になった場合は、同じパラメータを使用して別のコンピューティング ノードをインストールする必要があります。これは基本的に、データが失われたコンピューティングの再起動として表示され、クラスタに自動的に結合しようとします。クラスタに結合した後、すべてのデータはほかの2つのコンピューティング ノードから同期されます。



第 9 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）（(IPv4 and\or IPv6)）] と MAC アドレスをもつ任意のものです。Cisco DCNM リリース 11.3(1) から、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。

重要

- EPLは、VXLAN BGP EVPN ファブリック展開で DCNM 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。Cisco DCNM リリース 11.3(1) 以降、EPL は MAC のみのエンドポイントを表示することもできます。EPL の構成時に **[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、通常は DCNM 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、DCNM から RR への IP 到達可能性が必要です。これは、DCNM eth2 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 サーバー（or Route Servers）]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。リリース 11.2(1) から、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、DCNM 11.2) において適切な BGP 構成でスパインまたは RR を自動的に構成するオプションで有効にできます。
- Cisco DCNM リリース 11.3(1) 以降、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。これは、クラスタ モードでのみサポートされます。
- Cisco DCNM リリース 11.3(1) 以降、EPL はマルチサイト ドメイン（MSD）でサポートされます。
- Cisco DCNM リリース 11.3(1) 以降、IPv6 アンダーレイがサポートされます。
- ハイ アベイラビリティのサポート
- 最大 180 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。
- サポートされるスケール：ファブリックあたり 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 100K を超えてはなりません。

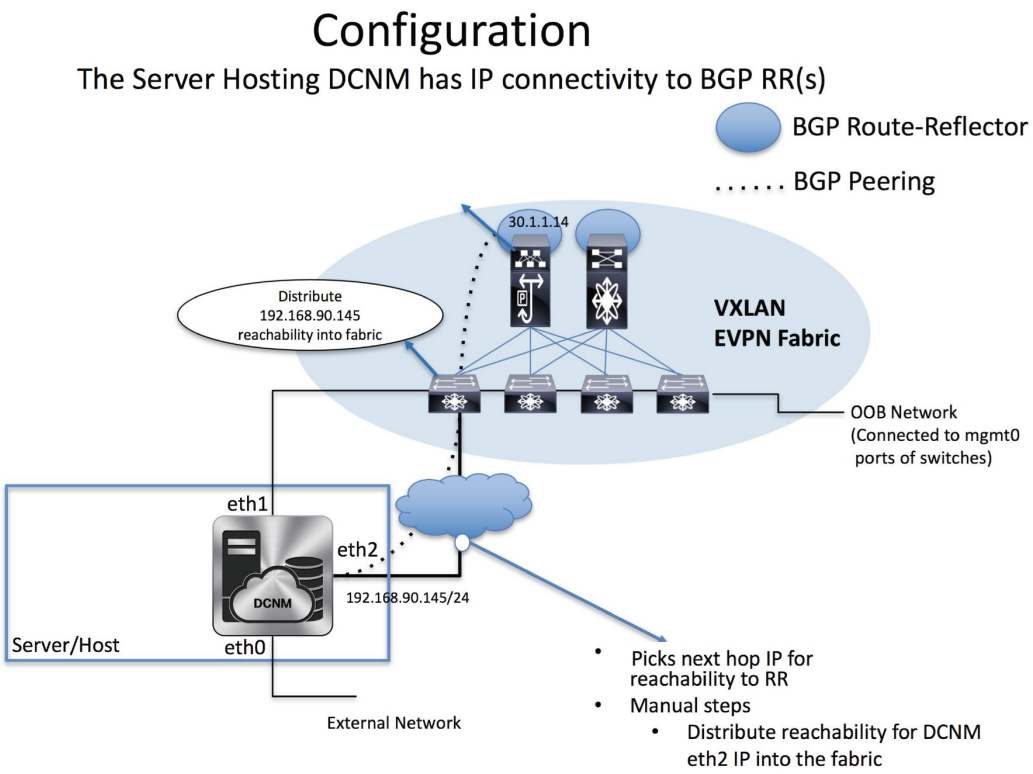
  Cisco DCNM リリース 11.4(1) から、すべてのファブリックのエンドポイントの合計数が 100K を超えると、アラームが生成され、ウィンドウの右上にある **[アラーム（Alarms）]** アイコンの下にリストされます。このアイコンは、新しいアラームが生成されるたびに点滅し始めます。

EPL の詳細については、次の項を参照してください。

エンドポイント ロケータの構成

DCNM OVA または ISO インストールには、次の 3 つのインターフェイスが付属しています。

- 外部アクセス用のeth0インターフェイス
- ファブリック管理用のeth1インターフェイス（アウトオブバンドまたはOOB）
- インバンドネットワーク接続用のeth2インターフェイス



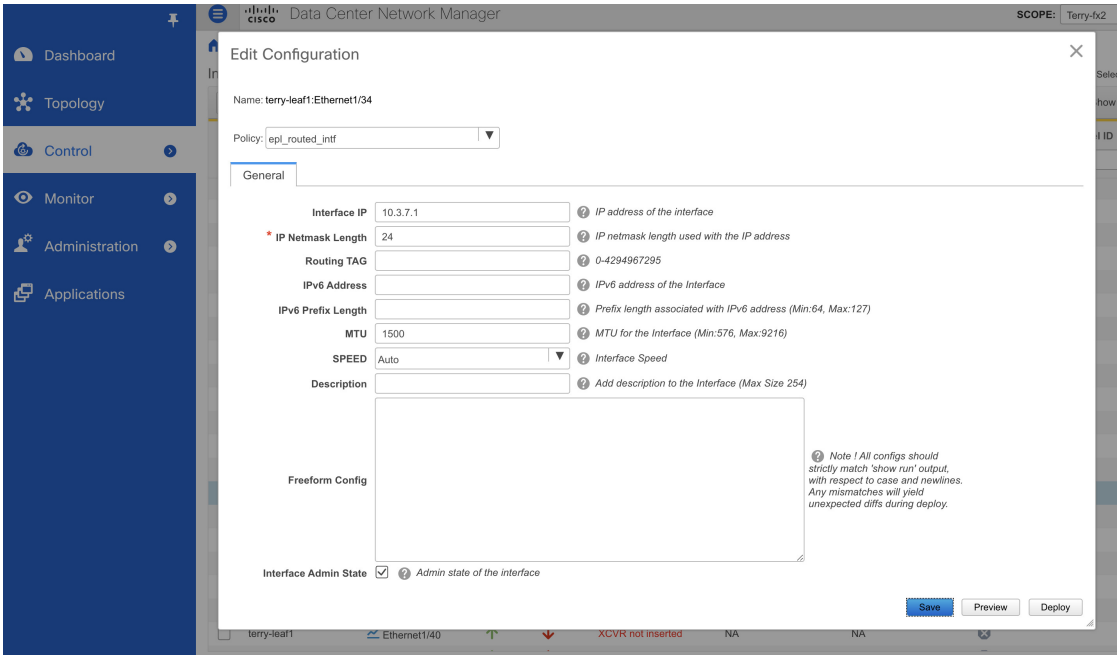
eth1インターフェイスは、レイヤ2またはレイヤ3隣接のmgmt0インターフェイスを介してデバイスに到達可能性を提供します。これにより、DCNM は POAP を含むこれらのデバイスを管理およびモニタできます。EPL では、DCNM とルートリフレクタの間で BGP ピアリングが必要です。Nexus デバイスの BGP プロセスは通常、デフォルト VRF で実行されるため、DCNM からファブリックへのインバンド IP 接続が必要です。この目的で、コマンドを使用してeth2インターフェイスを設定できます。**appmgr setup inbandappmgr update network-properties** オプションで、Cisco DCNM のインストール時に eth2 インターフェイスを構成できます。

すでに構成されているインバンドネットワーク（eth2インターフェイス）を変更する必要がある場合は、 コマンドを実行して、**appmgr setup inbandappmgr update network-properties** コマンドを再度実行します。**appmgr setup inbandappmgr update network-properties** コマンドを実行するには、「DCNM インストール後のネットワーク プロパティの編集」を参照してください。

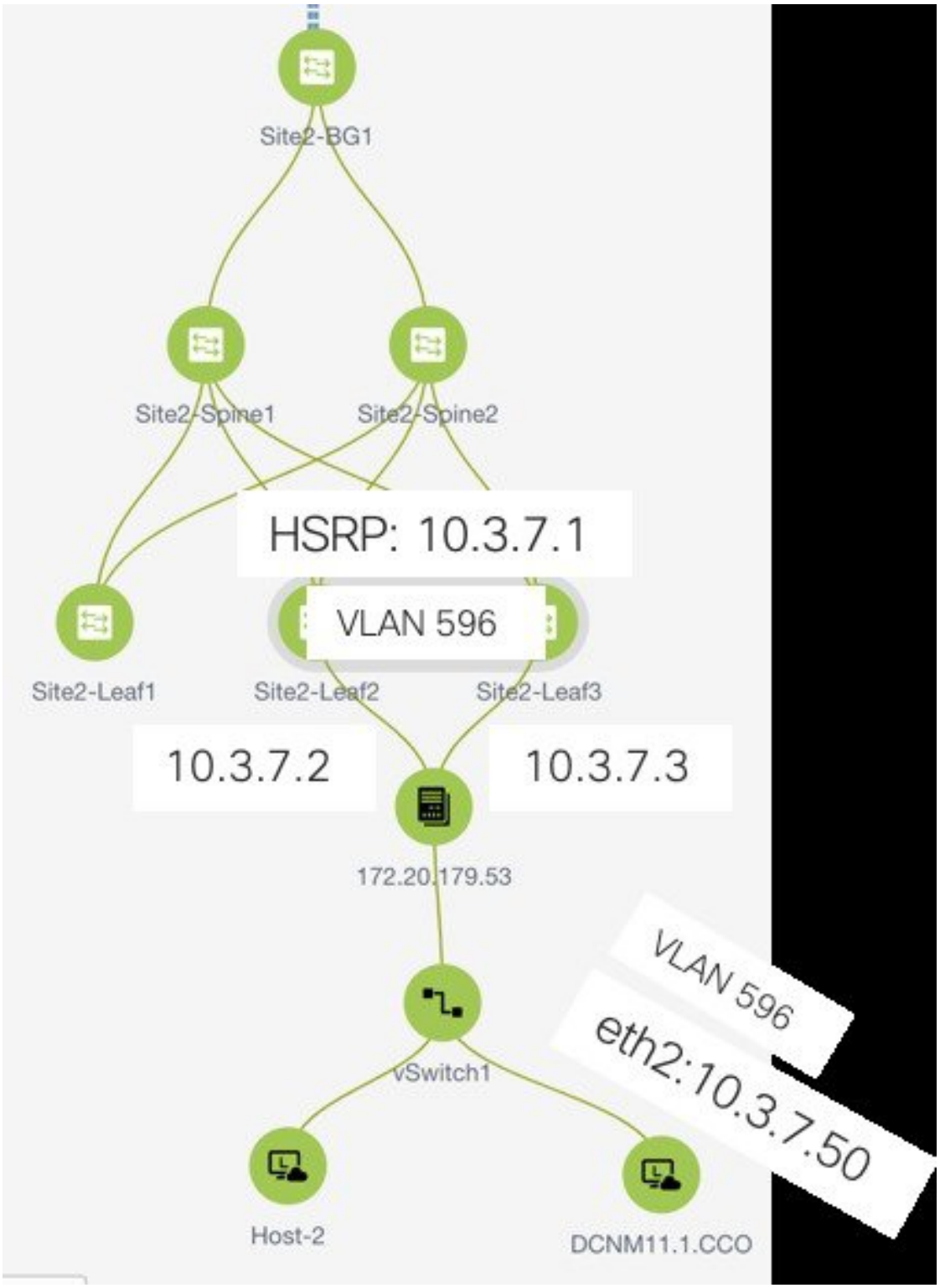
Note DCNM 上の eth2 インターフェイスの設定は、ファブリック内のデバイスへのインバンド接続を必要とするアプリケーションの前提条件です。これには EPL とネットワーク インサイトのリソース（NIR）が含まれます。

Note スタンドアロンモードで EPL を構成するには、単一のネイバーを EPL に追加する必要があります。DCNM eth2 IP アドレスは EPL IP です。

ファブリック側では、スタンドアロン DCNM 展開の場合、DCNM eth2 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る場合、そのインターフェイスは **[epl_routed_intf]** テンプレートを使用して構成できます。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。

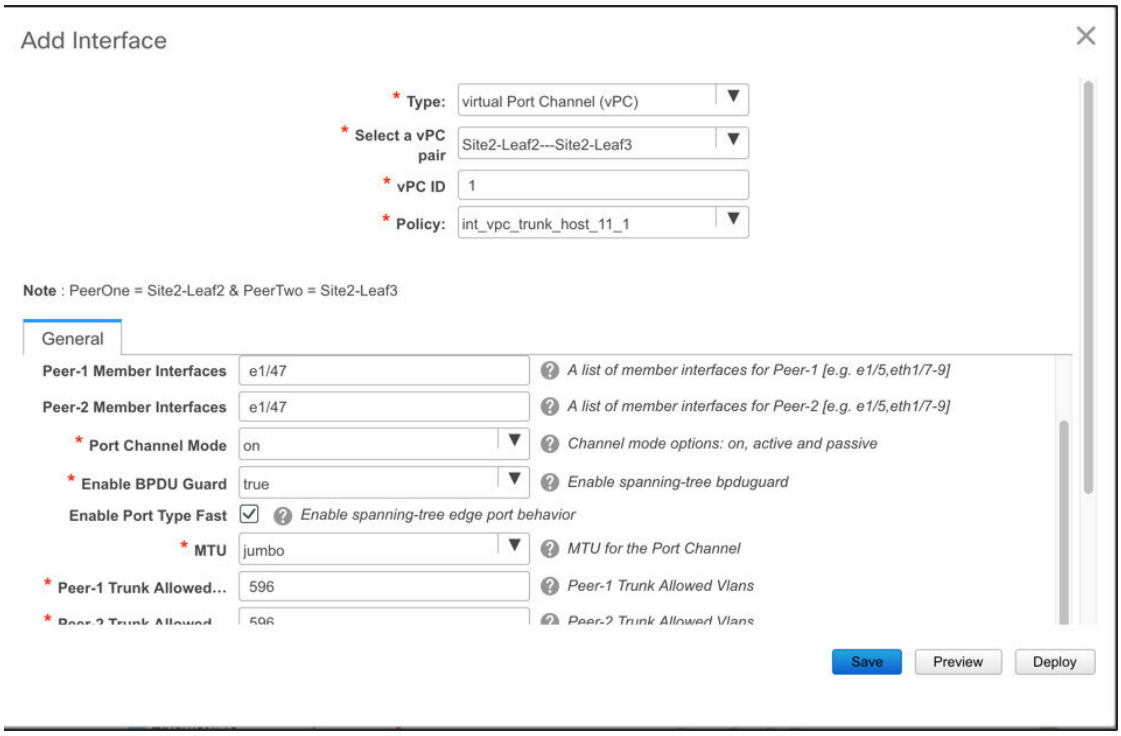


ただし、冗長性を確保するために、DCNMがインストールされているサーバーをデュアルホームまたはデュアル接続にすることをお勧めします。OVA DCNM 展開では、ポートチャネルを介してサーバーをスイッチに接続できます。これにより、リンクレベルの冗長性が提供されます。ネットワーク側のノードレベルの冗長性を確保するために、サーバをリーフスイッチのvPCペアに接続することもできます。このシナリオでは、HSRP VIP が DCNM 上の eth2 インターフェイスのデフォルトゲートウェイとして機能するようにスイッチを構成する必要があります。次の図に、シナリオの設定例を示します。

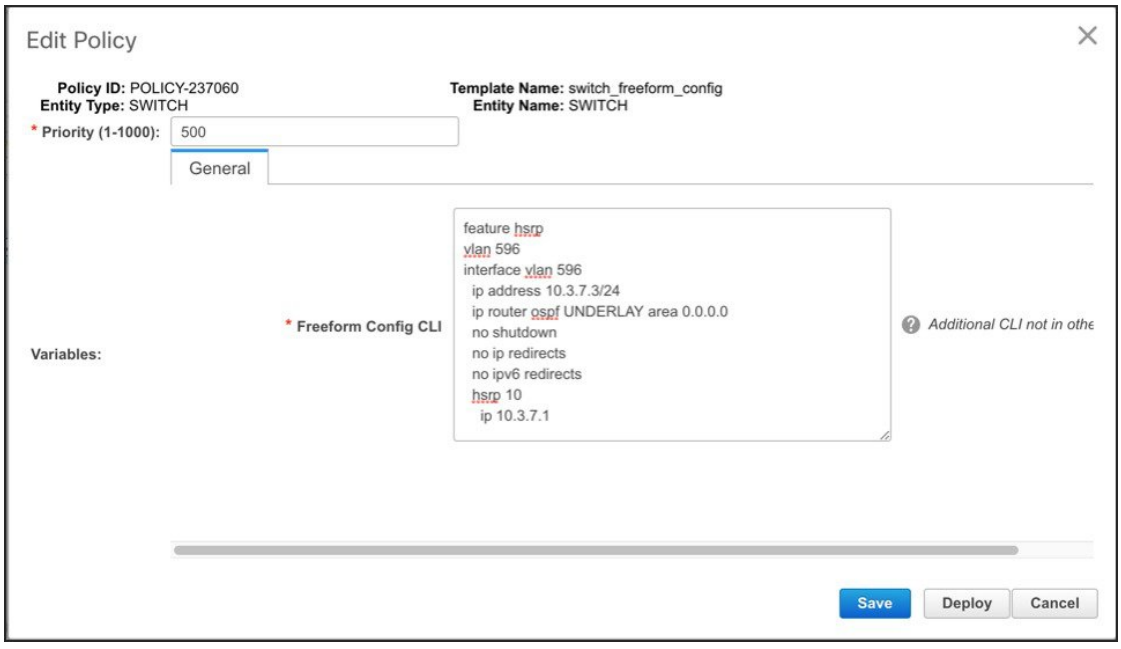


この例では、DCNM VM を搭載したサーバーは、それぞれ Site2-Leaf2 および Site2-Leaf3 という名前のスイッチの vPC ペアにデュアル接続されています。IPサブネット10.3.7.0/24に関連付

けられたVLAN 596は、インバンド接続に使用されます。次の図に示すように、インターフェイスvpc trunkホストポリシーを使用して、vPCホストポートをサーバに向けて設定できます。



Site2-Leaf2のHSRP設定では、次の図に示すようにswitch_freeformポリシーを使用できます。



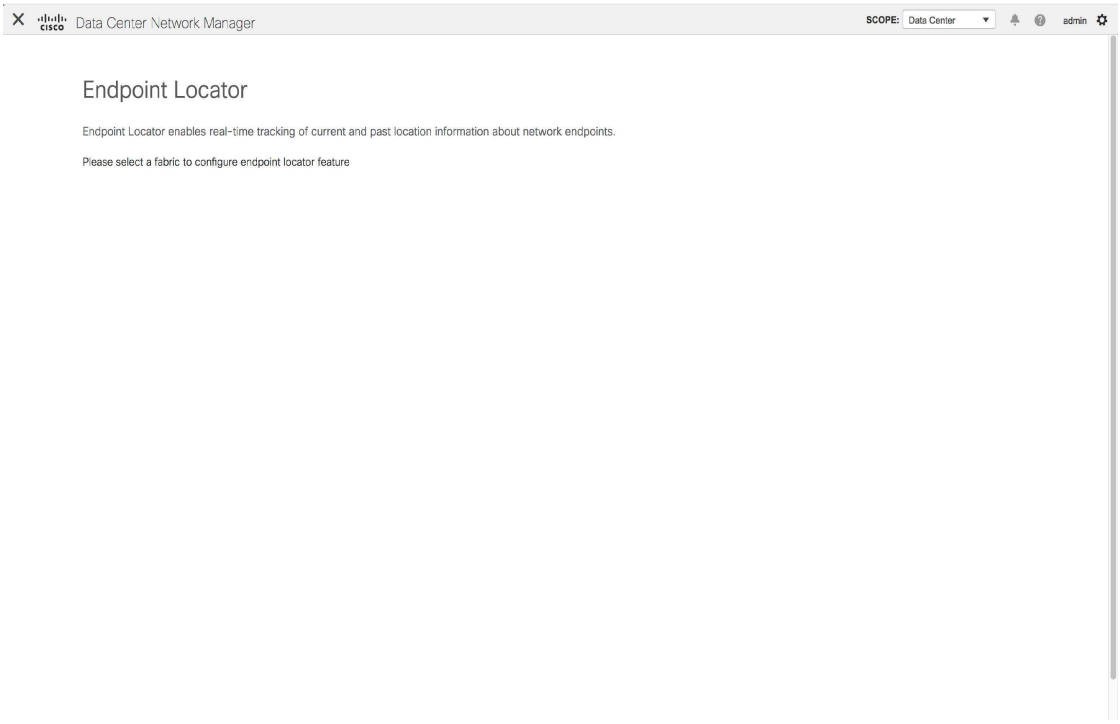
SVI 596にIPアドレス10.3.7.2/24を使用しながら、Site2-Leaf3に同様の設定を展開できます。これにより、デフォルトゲートウェイが 10.3.7.1 に設定された eth2 インターフェイスを介して DCNM からファブリックへのインバンド接続が確立されます。

物理または仮想 DCNM 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。

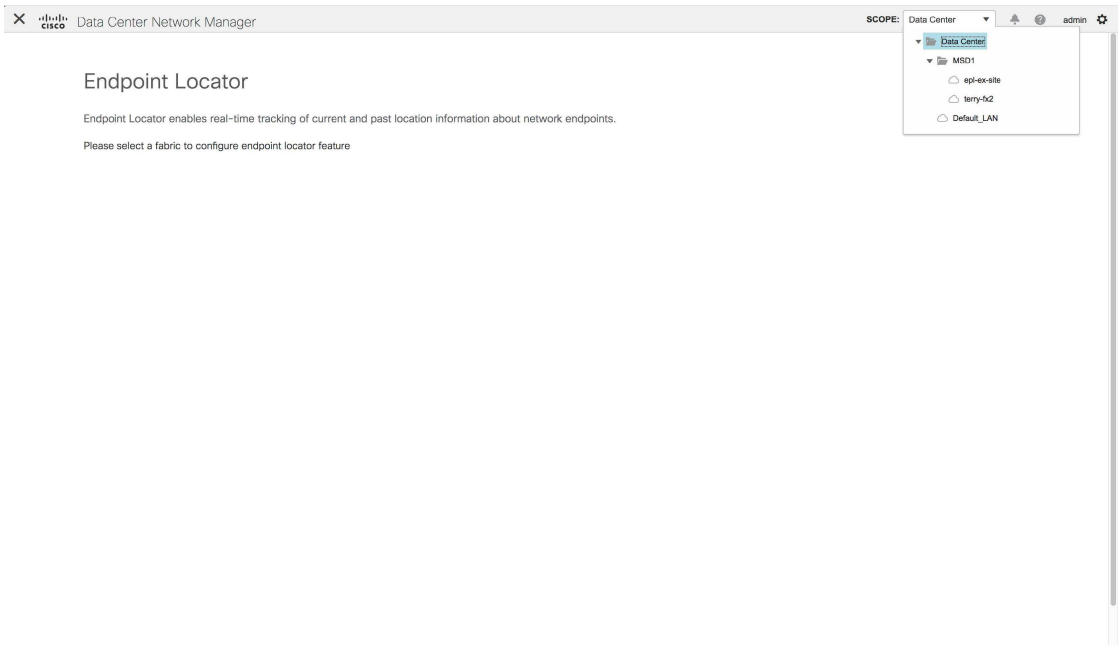
EPL の構成時に、ルート リフレクタ（RR）は BGP ピアとして DCNM を受け入れるように構成されます。同じ構成中に、DCNM は、eth2 ゲートウェイを介してスパイン/RR の BGP ループバック IP にルートを追加することによっても構成されます。

Note Cisco DCNM 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 をクエリします。

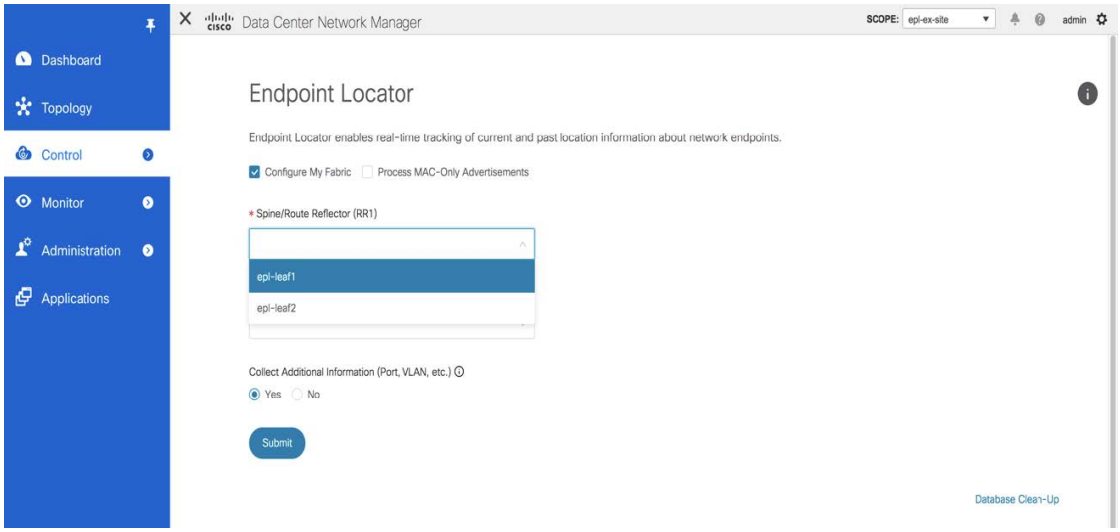
Cisco Web UI からエンドポイント ロケータを構成するには、**[制御（Control）] > [エンドポイント ロケータ（Endpoint Locator）] > [構成（Configure）]** の順に選択します。**[エンドポイント ロケータ（Endpoint Locator）]** ウィンドウが表示されます。



エンドポイントのアクティビティを追跡するためにエンドポイント ロケータ機能を有効にする必要があるファブリックを**[範囲（Scope）]** ドロップダウンリストから選択します。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。Cisco DCNM は RR とピアリングします。



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。DCNMによってモニタ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、それらは DCNMによって構成されていないファブリックであるため、このオプションはグレー表示されます。

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、[Process MAC-Only Advertisements]オプションを選択します。

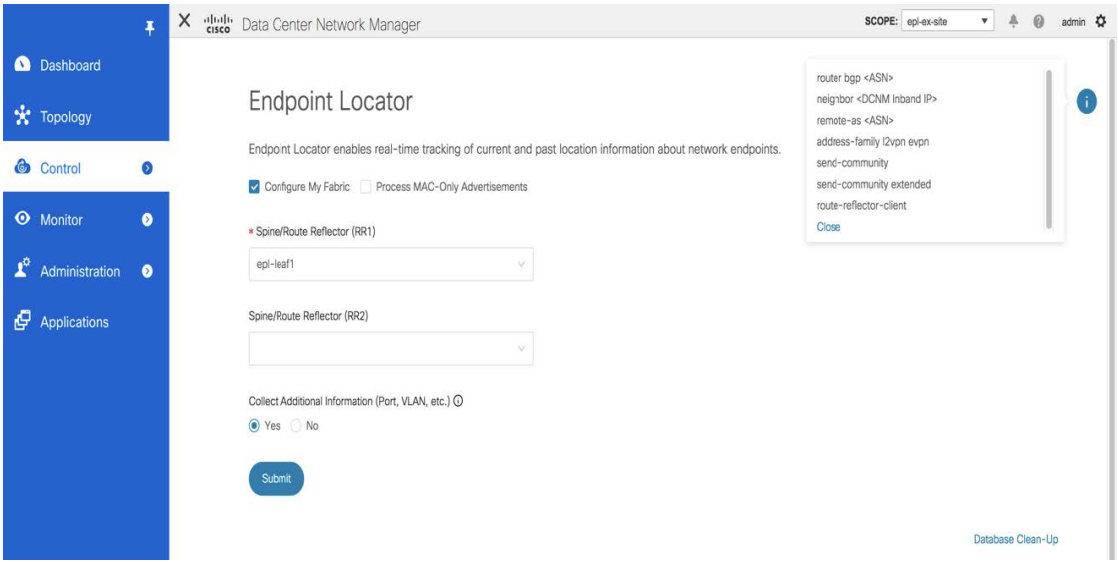
Note [Process Mac-Only Advertisements]チェックボックスをオンまたはオフにしてEPLをファブリックで有効にし、後でこの選択を切り替える場合は、まずEPLを無効にしてから、[データベースのクリーンアップ（Database Clean-up）]をクリックしてエンドポイントデータを削除してから、EPLを再度有効にします。必要な[Macのみのアドバタイズメントの処理（Process Mac-Only Advertisements）]設定を使用します。

[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。

Cisco DCNM を使用して EPL を構成する方法を示すビデオも視聴できます。「エンドポイントロケータの構成」を参照してください。

Cisco DCNM リリース 11.4(1) 以降、**[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構成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。



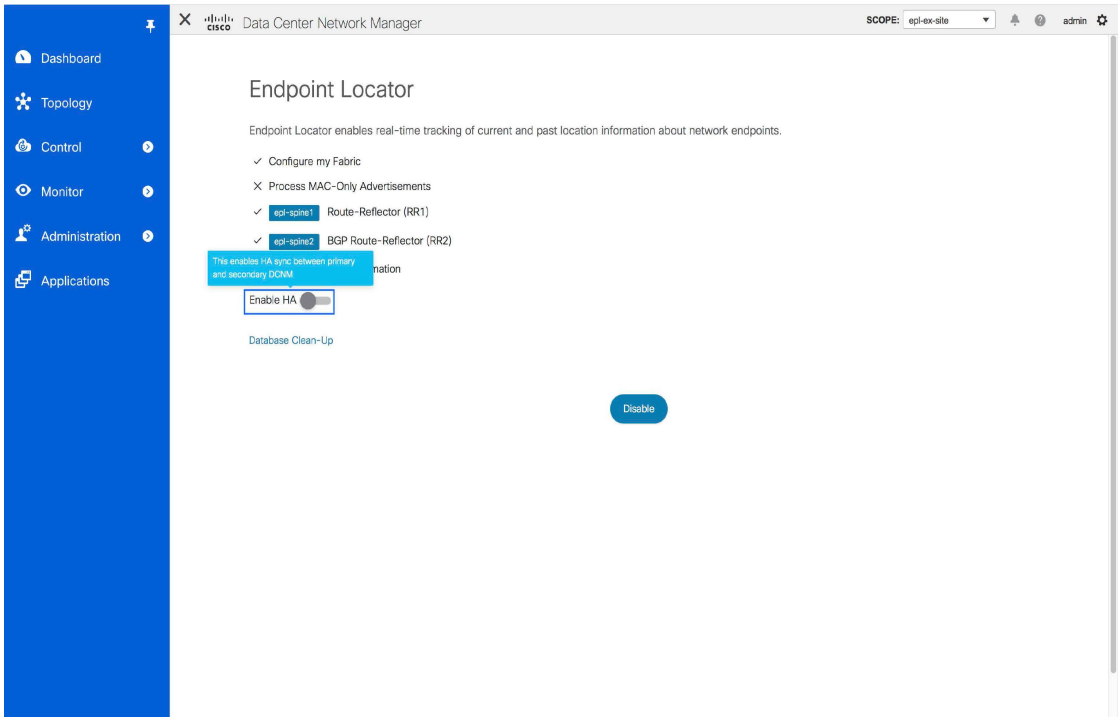
適切な選択を行い、さまざまな入力を確認したら、[送信（Submit）]をクリックしてEPLを有効にします。EPLの有効化中にエラーが発生した場合は、有効化プロセスが中止され、適切なエラーメッセージが表示されます。それ以外の場合、EPLは正常に有効化されます。

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。DCNM は、選択された RR に接続し、ASN を決定します。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、DCNM 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。ネイティブ HA DCNM 展開では、プライマリおよびセカンダリの両方の DCNM eth2 インターフェイス IP が BGP ネイバーとして追加されますが、いずれか一方のみがアクティブになります。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 ロケータのモニタリング」を参照してください。

高可用性の有効化

非 HA モードの展開で EPL が DCNM で有効になり、その後 DCNM が HA モードに移行するシナリオを考えます。このようなシナリオでは、[Enable HA] トグルが[Endpoint Locator]ウィンドウに表示されます。**[HA の有効化（Enable HA）]** ノブを切り替えて、プライマリとセカンダリ DCNM 間の高可用性同期を有効にします。



Cisco DCNM Web UIから高可用性同期を有効にするには、次の手順を実行します。

Procedure

ステップ 1 **[Control] > [エンドポイント ロケータ（Endpoint Locator）] > [構成（Configure）]** を選択します。

ステップ 2 [Enable HA]ボタンを切り替えます。

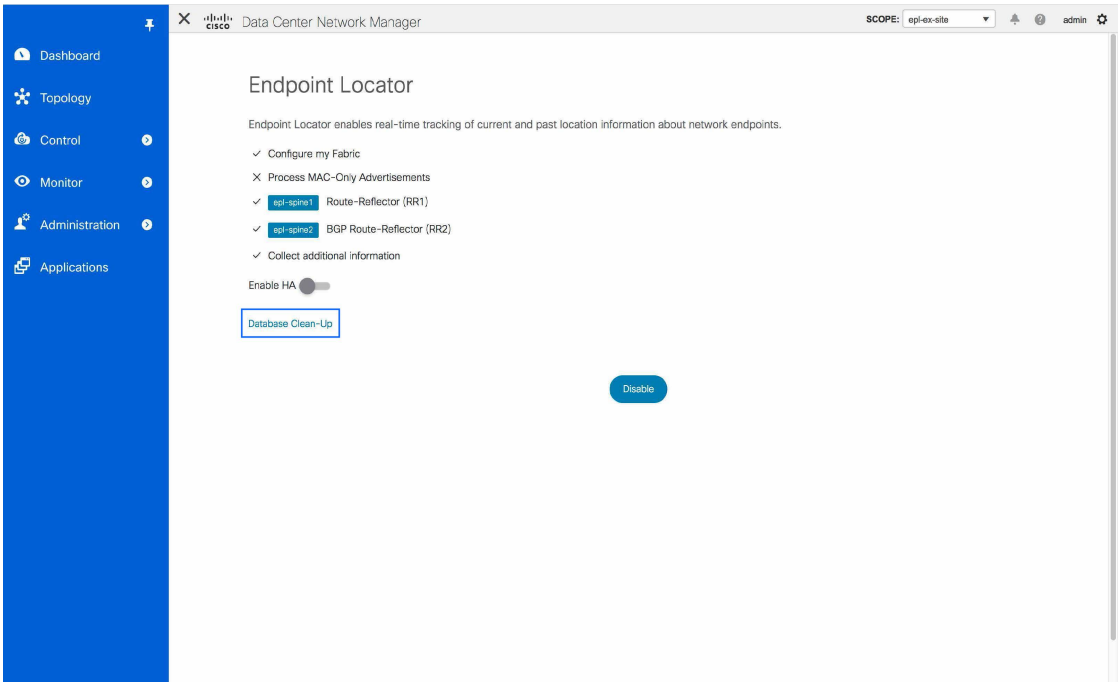
エンドポイントデータベースのフラッシュ

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。Cisco DCNM リリース 11.4(1) 以降、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 DCNM 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。

Procedure

ステップ 1 **[制御（Control）] > [エンドポイント ロケータ（Endpoint Locator）] > [構成（Configure）]** を選択し、**[データベース クリーンアップ（Database Clean-Up）]** をクリックします。



データベースに保存されているすべてのエンドポイント情報がフラッシュされることを示すメッセージとともに警告が表示されます。

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。

DCNM 高可用性モードでのエンドポイント ロケータの構成

Note ネイティブ HA モードで EPL を設定するには、2 つのネイバーを EPL に追加する必要があります。DCNM プライマリ eth2 および DCNM セカンダリ eth2 アドレスである EPL IP。

実稼働展開の場合は、DCNM ノードのネイティブ HA ペアが推奨されています。DCNM アクティブ ノードとスタンバイ ノードはレイヤ 2 隣接である必要があるため、それぞれの eth2 インターフェイスは同じ IP サブネットまたは VLAN の一部である必要があります。さらに、両方の DCNM ノードに同じ eth2 ゲートウェイを構成する必要があります。推奨オプションは、DCNM アクティブ ノードとスタンバイ ノードを Nexus スイッチの vPC ペア（リーフの場合もあります）に接続し、単一リンク障害、単一デバイス障害、または単一 DCNM ノード障害が発生した場合に十分なフォールトトレランスを確保することです。

次の例は、Cisco DCNM ネイティブ HA アプライアンスに対する **appmgr update network-properties** コマンドの出力例を示しています。この例では、1.1.1.2 はプライマリ eth2 インターフェイス IP アドレス、1.1.1.3 はスタンバイ eth2 インターフェイス IP アドレス、1.1.1.1 はデフォルト ゲートウェイ、1.1.1.4 はインバンドの仮想 IP（VIP）です。

Cisco DCNM プライマリ アプライアンスで、次のようにします。

```
appmgr update network-properties session start
appmgr update network-properties set ipv4 eth2 1.1.1.2 255.255.255.0 1.1.1.1
appmgr update network-properties set ipv4 peer2 1.1.1.3
appmgr update network-properties set ipv4 vip2 1.1.1.4 255.255.255.0
appmgr update network-properties session apply
appmgr update ssh-peer-trust
```

Cisco DCNM セカンダリ アプライアンスで、次のようにします。

```
appmgr update network-properties session start
appmgr update network-properties set ipv4 eth2 1.1.1.3 255.255.255.0 1.1.1.1
appmgr update network-properties set ipv4 peer2 1.1.1.2
appmgr update network-properties set ipv4 vip2 1.1.1.4 255.255.255.0
appmgr update network-properties session apply
appmgr update ssh-peer-trust
```

プライマリ ノードとセカンダリ ノードの両方からファブリックへのインバンド接続が確立された後、Cisco DCNM Web UI からエンドポイント ロケータを DCNM HAモードで構成するには、次の手順を実行します。

Procedure

ステップ 1 **[Control] > [エンドポイント ロケータ（Endpoint Locator）] > [構成（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、ファブリック設定の詳細が表示されます。

ステップ 2 DCNM HAモードでエンドポイント ロケータを構成するには、**[範囲（SCOPE）]** ドロップダウンリストからファブリックを選択します。

ステップ 3 ドロップダウン リストからルート リフレクタ（RR）を選択します。

ステップ 4 **[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。[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。

ステップ 5 **[送信（Submit）]** をクリックします。`

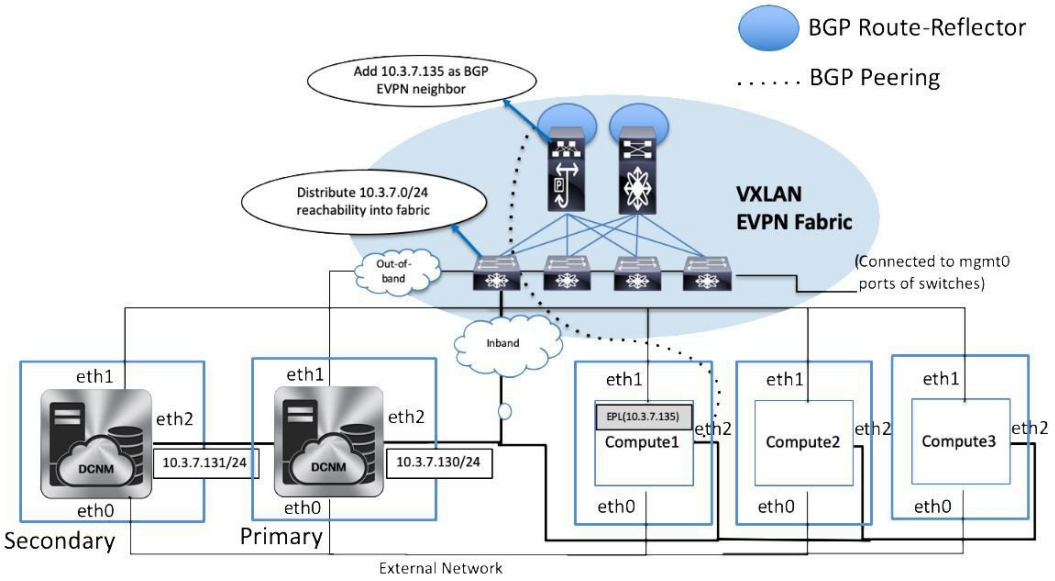
What to do next

エンドポイント ロケータを HA モードで設定すると、エンドポイント ロケータ ダッシュボードでエンドポイントアクティビティやエンドポイント履歴などの詳細を表示できます。これらの詳細を表示するには、**[監視（Monitor）] > [エンドポイント ロケータ（Endpoint Locator）] > [検出（Explore）]** の順に移動します。

DCNM クラスタ モードでのエンドポイント ロケータの構成

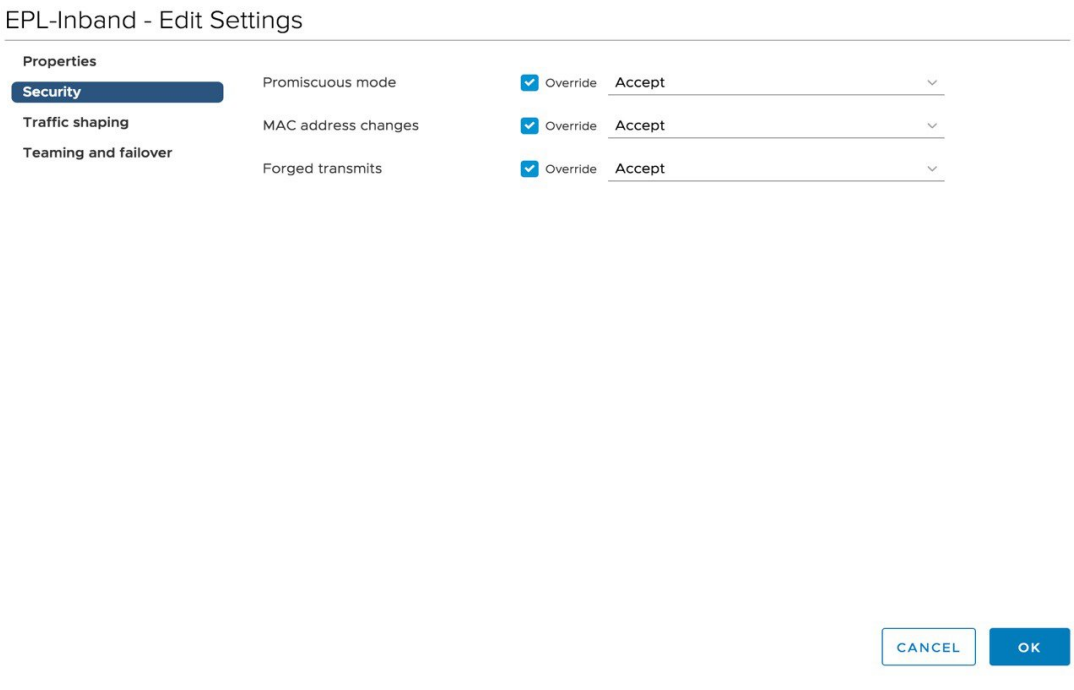
（注） クラスタ モードで EPL を設定するには、単一のネイバーを EPL に追加する必要があります。DCNM EPL コンテナのインバンド IP アドレスは EPL の IP です。

DCNM クラスタ モードの展開では、DCNM ノードに加えて、追加の 3 つのコンピューティングノードが展開内に存在するようになります。クラスタ モードでのアプリケーションの展開については、「クラスタ モードの *Cisco DCNM*」を参照してください。



DCNM クラスタ モードでは、EPL を含むすべてのアプリケーションがコンピューティング ノードで実行されます。DCNM アプリケーション フレームワークは、コンピューティング ノードで実行されるすべてのアプリケーションの完全な耐用周期の管理を行います。EPL インスタンスは、コンピューティング ノードに割り当てられたインバンド プールから割り当てられた独自の IP アドレスを持つコンテナとして実行されます。この IP アドレスは、eth2 またはインバンド インターフェイスに割り当てられたものと同じ IP サブネットにあります。EPL 機能を有効にすると、EPL インスタンスはこの IP アドレスを使用してスパイン/RR と BGP ピアリングを形成します。EPL インスタンスをホストしているコンピューティング ノードがダウンすると、残りの 2 つのコンピューティング ノードのいずれかで EPL インスタンスが自動的に再生成されます。EPL インスタンスに関連付けられているすべての IP アドレスおよびその他のプロパティは保持されます。

コンピューティング ノードのレイヤ 2 隣接関係（アジャセンシー）要件により、コンピューティング ノードの eth2 インターフェイスは DCNM ノードと同じ IP サブネットの一部である必要があります。この場合もやはり、同じ vPC ペアのスイッチにコンピューティング ノードを接続することが、推奨される導入オプションです。以下に示すように、クラスタ モード DCNM の OVA 設定では、eth2 インターフェイスに対応するポート グループで無差別モードが有効になっていることを確認してください。



DCNM クラスタ モードの EPL 機能の有効化は、非クラスタ モードの有効化と同じです。主な違いは、スパイン/RR では、EPL インスタンスに割り当てられた IP アドレスを指す単一の BGP ネイバーシップだけが必要なことです。非クラスタモードでの DCNM ネイティブ HA 導入では、すべてのスパイン/RR に常に 2 つの構成済み BGP ネイバーがあります。1 つは DCNM プライマリ eth2 インターフェイスを指し、もう 1 つは DCNM セカンダリ eth2 インターフェイスを指します。ただし、アクティブになるネイバーは常に 1 つだけです。

外部ファブリックのエンドポイント ロケータの構成

DCNM リリース 11.2(1) 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。DCNM からモニタ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。

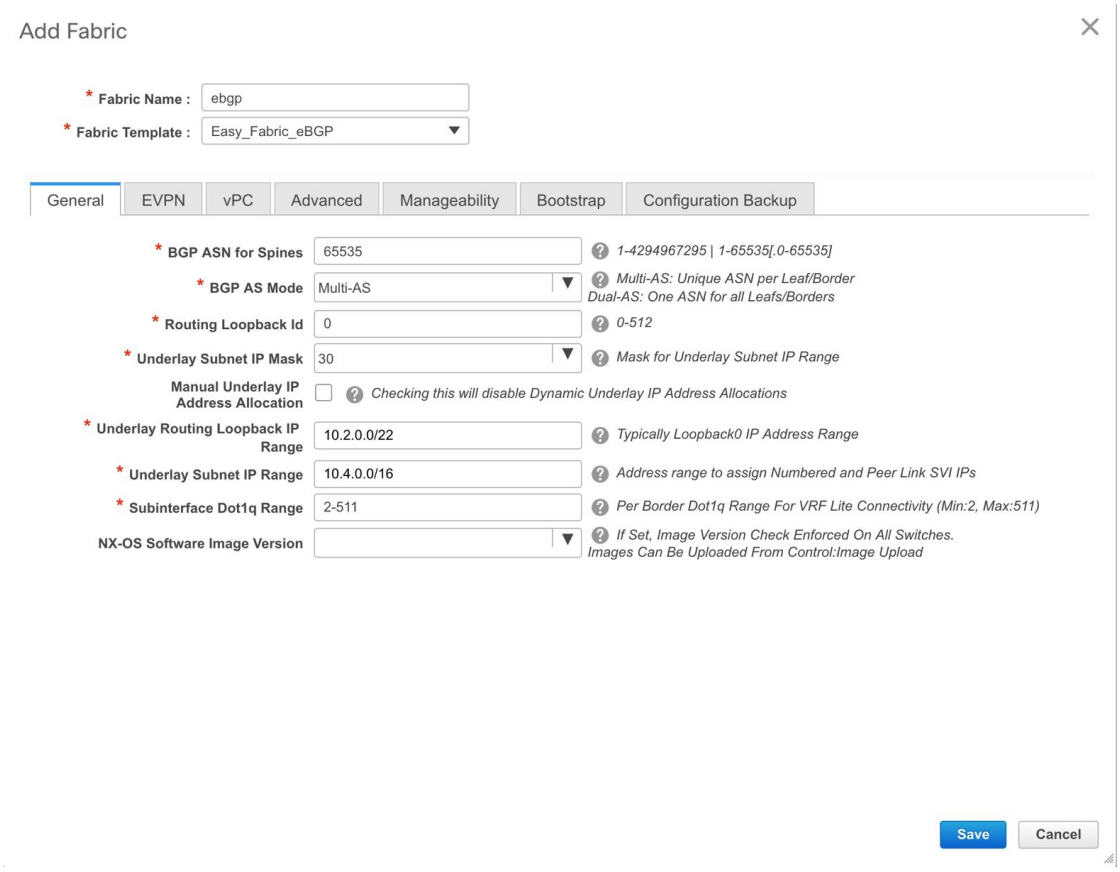
eBGP EVPN ファブリックのエンドポイント ロケータの構成

Cisco DCNM リリース 11.2(1) 以降、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 DCNM Web UIから eBGP EVPN ファブリックの EPL を構成するには、次の手順を実行します。

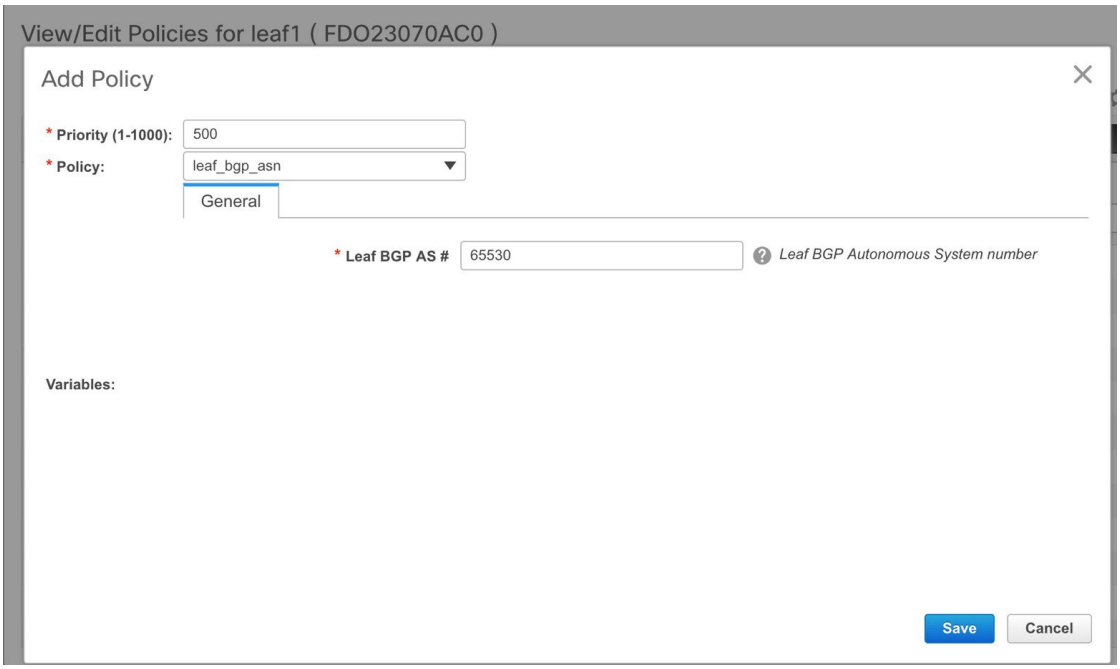
Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** 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。



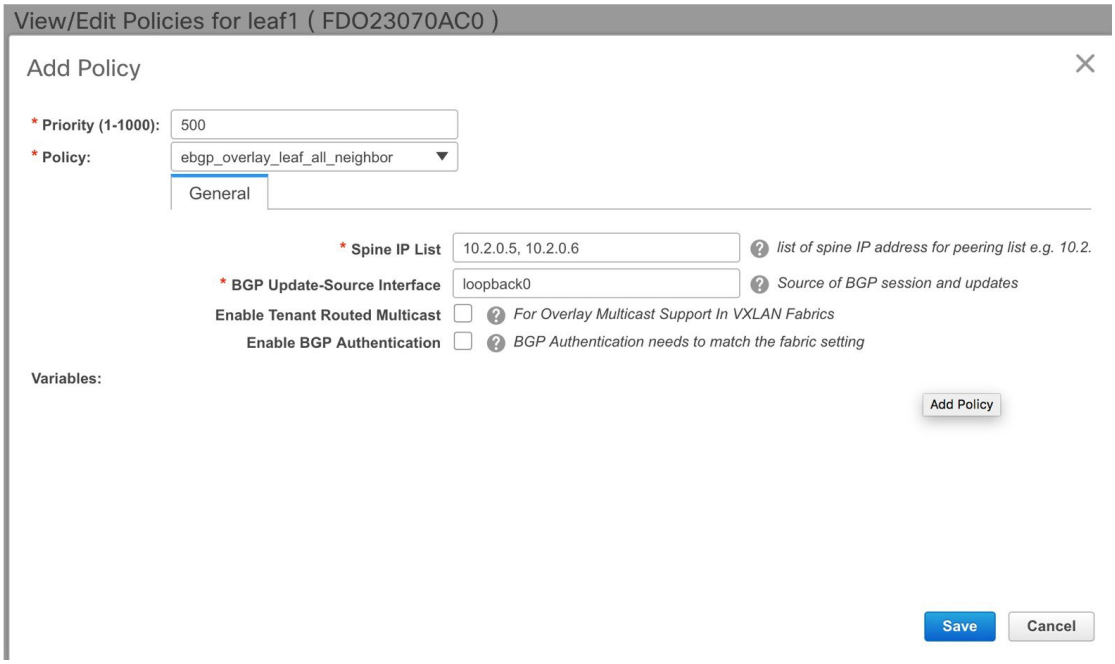
ステップ 2 すべてのリーフで一意の ASN を設定するには、**leaf_bgp_asn** ポリシーを使用します。



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。

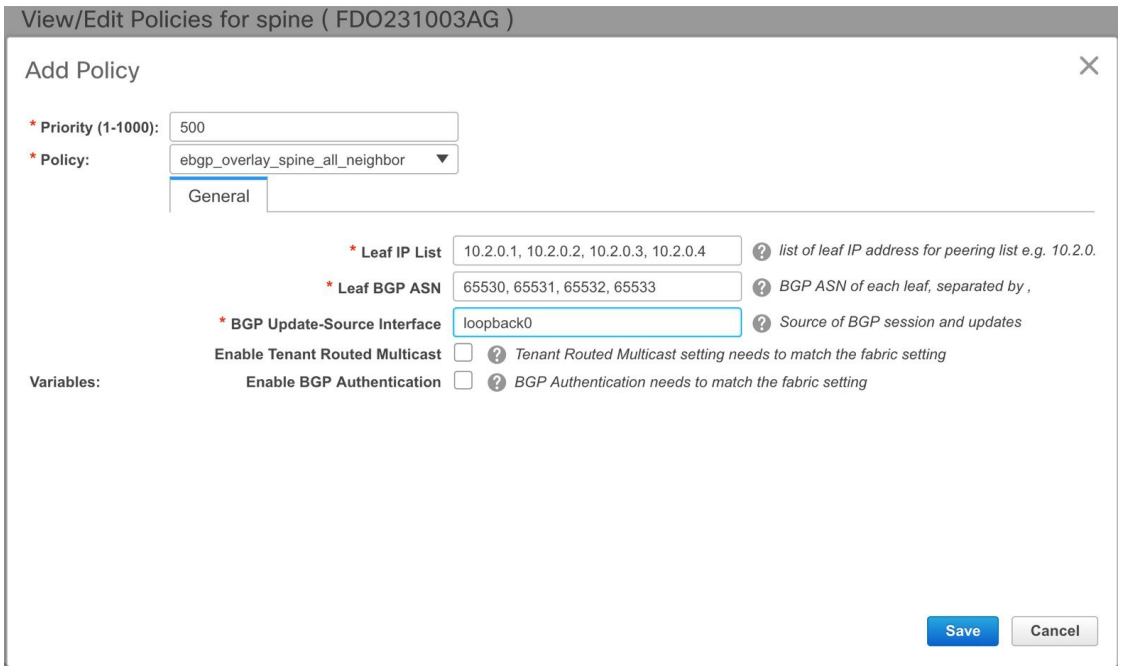


ステップ 4 **ebgp_overlay_spine_all_neighbor** ポリシーを各スパインに追加します。

[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 ロケータの削除

Cisco DCNM 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。

手順

ステップ 1 **[Control] > [エンドポイント ロケータ（Endpoint Locator）] > [構成（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。

エンドポイント ロケータのトラブルシューティング

エンドポイントロケータ機能の有効化に失敗する理由は複数あります。通常、適切なデバイスが選択され、使用する IP アドレスが正しく指定されている場合は、DCNM から BGP RR への接続が存在しないため、機能を有効にできません。これは、基本的な IP 接続が使用可能であることを確認するための健全性チェックです。次の図は、EPL 機能を有効にしようとしたときに発生したエラーシナリオの例を示しています。

EPL 機能が有効または無効になったときに発生した内容の詳細を示すログは、/usr/local/cisco/dcm/fm/logs/epl.log にある、epl.log ファイルに記載されています。次の例は、ファブリックの EPL 設定の進行状況を示す epl.log のスナップショットです。

```
2019.12.05 12:18:23  INFO  [epl] Found DCNM Active Inband IP: 192.168.94.55/24
2019.12.05 12:18:23  INFO  [epl] Running script: [sudo, /sbin/appmgr, setup, inband-route,
 --host, 11.2.0.4]
2019.12.05 12:18:23  INFO  [epl] Getting EPL configure progress for fabric 4
2019.12.05 12:18:23  INFO  [epl] EPL Progress 2
2019.12.05 12:18:23  INFO  [epl] [sudo, /sbin/appmgr, setup, inband-route, --host,
11.2.0.4] command executed, any errors? No
2019.12.05 12:18:23  INFO  [epl] Received response:
2019.12.05 12:18:23  INFO  [epl] Validating host route input
2019.12.05 12:18:23  INFO  [epl] Done configuring host route
2019.12.05 12:18:23  INFO  [epl] Done.
2019.12.05 12:18:23  INFO  [epl] Running script: [sudo, /sbin/appmgr, setup, inband-route,
 --host, 11.2.0.5]
2019.12.05 12:18:23  INFO  [epl] [sudo, /sbin/appmgr, setup, inband-route, --host,
11.2.0.5] command executed, any errors? No
2019.12.05 12:18:23  INFO  [epl] Received response:
2019.12.05 12:18:23  INFO  [epl] Validating host route input
2019.12.05 12:18:23  INFO  [epl] Done configuring host route
2019.12.05 12:18:23  INFO  [epl] Done.
2019.12.05 12:18:23  INFO  [epl] Running command: sudo /sbin/appmgr show inband
2019.12.05 12:18:24  INFO  [epl] Received response: Physical IP=192.168.94.55/24
Inband GW=192.168.94.1
No IPv6 Inband GW found

2019.12.05 12:18:26  INFO  [epl] Call:
http://localhost:35000/afw/apps?imagetag=cisco:epl:2.0&fabricid=epl-ex-site, Received
response:
[illegible]
2019.12.05 12:18:26  INFO  [epl] Epl started on AFW
```

EPL が正常に有効化されると、エンドポイント情報に関連付けられているすべてのデバッグ、エラー、および情報ログが、関連するファブリックのディレクトリの下の /var/afw/applogs/ に保存されます。たとえば、**[test]** ファブリックで EPL が有効になっている場合、ログは /var/afw/applogs/epl_cisco_test_afw_log /epl/ に置かれ、ファイル名 afw_bgp.log.1 で始まります。ネットワークの規模とエンドポイントイベントの数に応じて、ファイルサイズが増加します。したがって、`afw_bgp.log` の最大数とサイズには制限があります。ファイル サイズは最大 100 MB、10 ファイルまで保存されます。

Note EPL は Docker コンテナ内のこのディレクトリにシンボリック リンクを作成するので、ネイティブにアクセスすると破損しているように見えます。

EPL は、BGP アップデートを使用してエンドポイント情報を取得します。これが機能するためには、エンドポイントを持つすべてのスイッチのスイッチ ループバックまたは VTEP インターフェイスの IP アドレスを DCNM で検出する必要があります。検証するには、Cisco DCNM の **[Web UI] > [ダッシュボード（Dashboard）] > [スイッチ（Switch）] > [インターフェイス（Interfaces）]** タブに移動し、対応するレイヤ 3 インターフェイス（通常はループバック）に関連付けられている IP アドレスとプレフィックスが正しく表示されるかどうかを確認します。

Cisco DCNM クラスタの導入で、EPL が BGP ピアリングを確立できず、アクティブな DCNM はスパインのループバック IP アドレスに ping を送信できるものの、EPL コンテナはできない場合、Cisco DCNM およびそのコンピューティング ノードの eth2 ポート グループで無差別（Promiscuous）モードが **[受容（Accept）]** に設定されていないことを意味します。この設定を変更すると、コンテナはスパインにを ping を送信でき、EPL は BGP を確立します。

大規模なセットアップでは、スイッチからこの情報を取得するために 30 秒（Cisco DCNM で設定されたデフォルトタイマー）以上かかる場合があります。この場合、`ssh.read-wait-timeout` プロパティ（**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]**）をデフォルトの 30000 から、60000 以上の値に変更する必要があります。

大規模なセットアップでは、ダッシュボードに表示されるエンドポイントデータがいくらか不正確になることがあります。エンドポイント数が多い場合、パフォーマンスの精度は最大で約 1% 低下します。ダッシュボードが予想と大きく異なる場合は、DCNM にパッケージ化されている検証スクリプトを使用して有効性を確認できます。root として、/root/packaged-files/scripts/ にある epl-rt-2.py スクリプトを実行します。このスクリプトを実行するには、RR/スパインの IP と、関連するユーザー名とパスワードが必要です。/root/packaged-files/scripts /ディレクトリは読み取り専用であるため、スクリプトはそのディレクトリの外部で実行する必要があります。たとえば、IP 10.2.0.5、ユーザ名 admin、パスワード cisco123 を使用してスパインのスクリプトを実行するには、作業ディレクトリを /root/ にして、**/root/packaged-files/scripts/epl-rt-2.py -s 10.2.0.5 -u admin -p cisco123** を実行します。EPL ダッシュボードに予想された数値が表示されず、epl-rt-2.py スクリプトの出力がダッシュボードと大きく異なる場合は、テクニカル サポートにお問い合わせください。

クラスタ モードでは、BGP はスパイン/RR と DCNM の間で確立されません。eth2 DCNM インターフェイスに対応するポート グループの **[無差別モード（Promiscuous mode）]** 設定が **[受容（Accept）]** に設定されていることを確認します。接続がまだ確立されていない場合は、次の手順を実行して、DCNM の BGP クライアントとスパイン/RR 間の接続を確認します。

1. アクティブな DCNM でシェルを開いて、次のコマンドを実行します。
   a. *docker service ls*

      * EPL サービスの ID をメモします

   b. *docker service ps $ID*

*[ノード（NODE）] フィールドをメモします、

c. *afw compute list -b*

*以前の ホスト名（HostName）（ノード）に一致する HostIp をメモします。これは、EPL サービスが現在実行されているコンピューティング ノードです。

2. 手順 1-c でメモしたコンピューティング ノードでシェルを開き、次のコマンドを実行します。

a. *docker container ls*

*EPL のコンテナ ID をメモします複数の EPL コンテナがある場合は、コンテナ名を確認して、どのコンテナがどのファブリックに対応しているかを確認します。命名スキームは epl_cisco_ $ FabricName_afw*です。

b. *docker container inspect $CONTAINER_ID*

*SandboxKeyの値をメモします

c. *nsenter --net=$SandboxKey*

このコマンドにより、EPL コンテナのネットワーク名前空間に入ります。これで、ifconfig、ip、ping などのネットワーク コマンドは、シェルで exit コマンドを発行するまで、コンテナ内から実行されているかのように動作します。

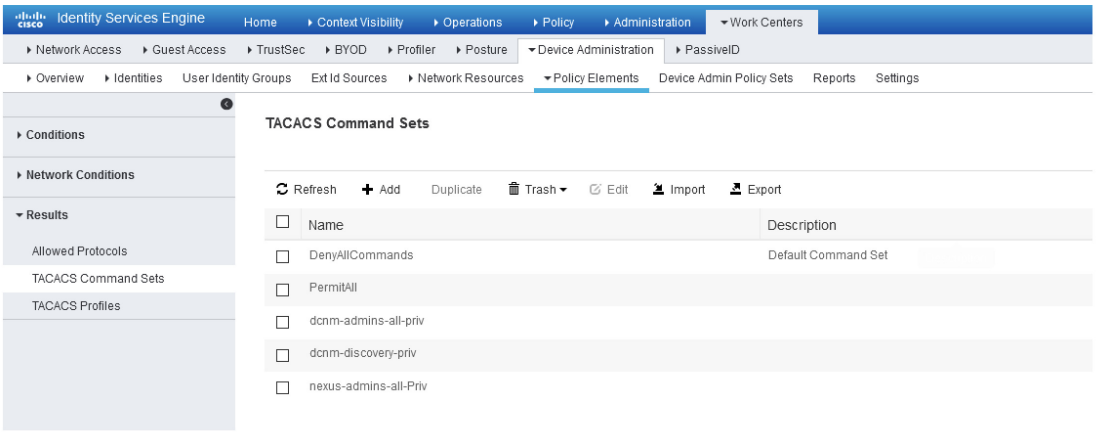
3. スパイン/RR に ping を送信してみます。DCNM クラスタに構成されているインバンド IP プールが、スイッチ ループバック IP と競合しないことを確認します。

ISE ポリシーが設定された EPL

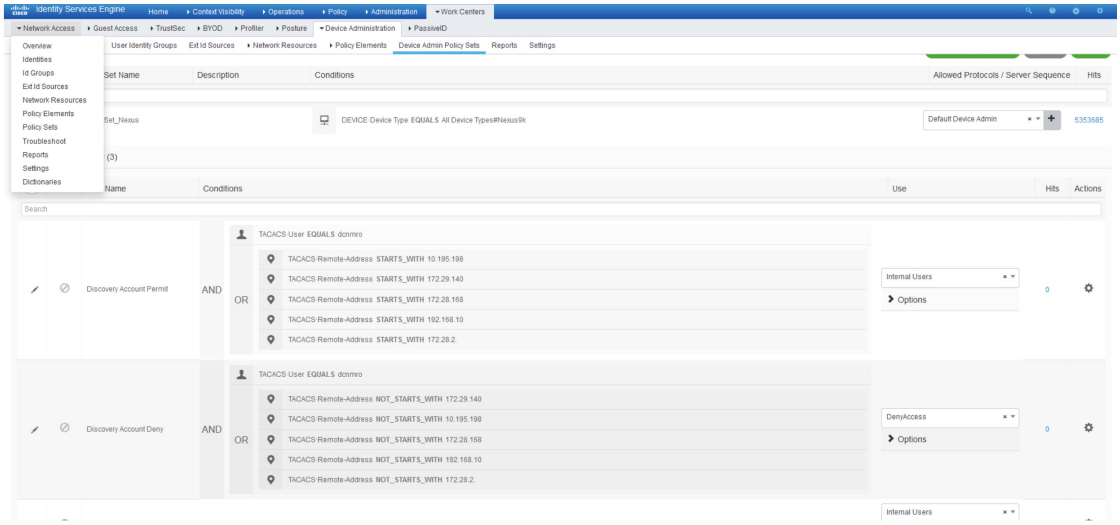
Cisco NX-OS リリース 9.3(4) 以前のリリースを実行しているスイッチで、AAA 構成が設定されているシナリオを考えます。AAA スイッチの構成例を次に示します。

```
feature tacacs+
tacacs-server host ISE_ACS_IP_ADDDRESS 5 key 7 "Fewhg12345"
aaa group server tacacs+ AAA_TACACS
       server ISE_ACS_IP_ADDDRESS
       use-vrf management
       source-interface mgmt0
aaa authentication login default group AAA_TACACS local
aaa authentication login console local
aaa authorization config-commands default group AAA_TACACS local
aaa authorization commands default group AAA_TACACS local
aaa accounting default group AAA_TACACS
aaa authentication login error-enable
```

guestshell、**run guestshell**、**show** といったコマンドにより設定された ISE サーバーは、ISE 内で作成された検出アカウントまたはポリシーにアクセスすることが許可されます。許可されるコマンドは、**[TACACS コマンド セット（TACACS Command Sets）]** ウィンドウで設定します。このウィンドウは、ISE の **[ポリシー エレメント（Policy Elements）]** タブの下にあります。



DCNM の eth0 IP およびファブリック デバイスのサブネットも許可されます。これは、**[デバイス管理ポリシー セット（Device Admin Policy Sets）]** ウィンドウで設定します。このウィンドウは、**[デバイス管理（Device Administration）]** タブの下にあります。



これで、DCNM は、エンドポイント ロケータ機能に必要なすべての **show** コマンドを実行するために検出アカウントを使用するように構成されます。ただし、スイッチ NXAPI の問題により、リクエスタ IP がリモート AAA 認証要求に入力されていないため、AAA 検証が失敗します。**show** コマンドは IP アドレスから発行されたものとは見なされないため、コマンドはブロックされ、EPL ダッシュボードに必要なエンドポイント情報が表示されなくなります。

回避策として、AAA ルールを緩和し、「ブランク」の送信者からの要求を許可することを推奨します。「空白」の送信者からの要求を許可するには、**[ステータス（Status）]** 列の下にある ⊘ アイコンをクリックします（**[アカウント検出許可（Discovery Account Permit）]** と **[アカウント検出拒否（Discovery Account Deny）]** の両方で、**[デバイス管理ポリシー セット（Device Admin Policy Sets）]** ウィンドウにあります）。**[無効（Disabled）]** を選択して **[保存（Save）]** をクリックします。

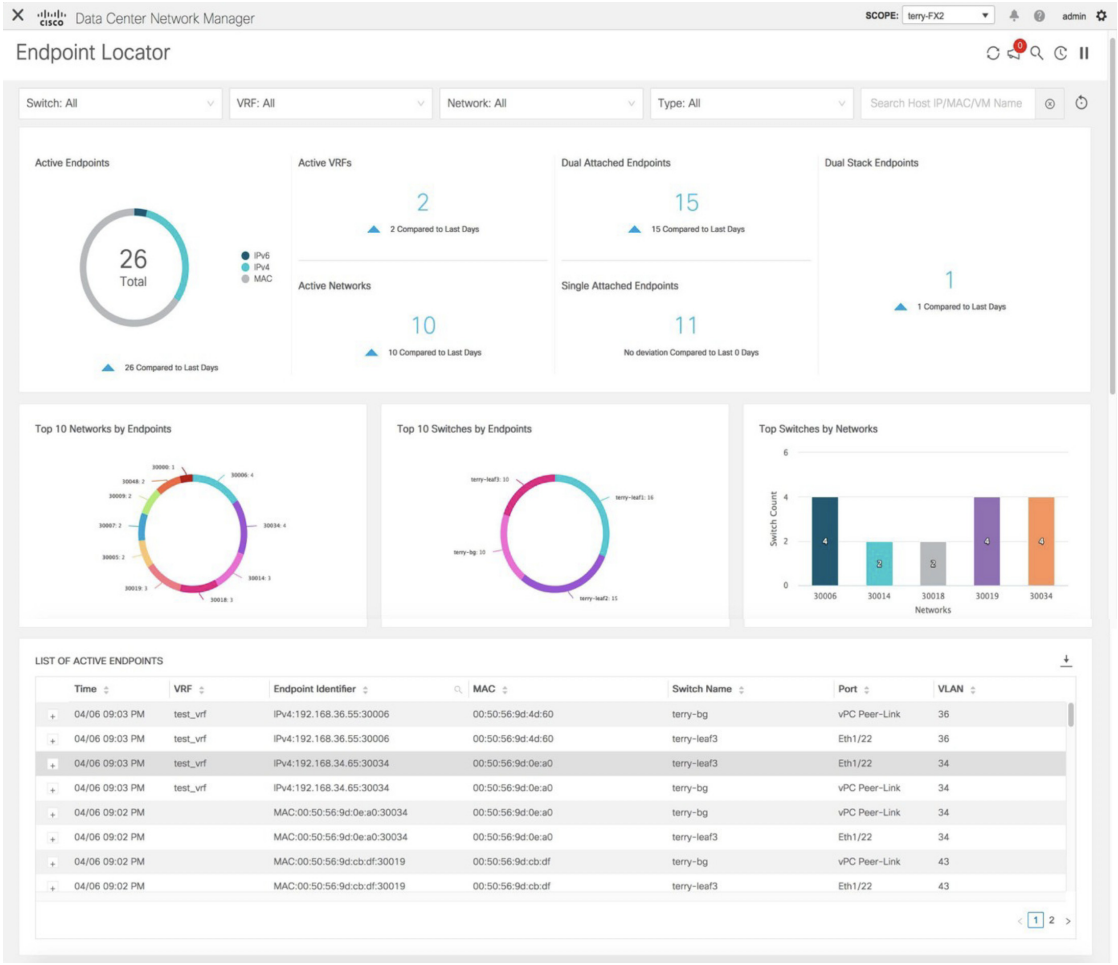
また、この問題は、Cisco NXOS リリース 9.3(5) 以降のリリースを実行しているスイッチでは発生しません。

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。DCNM範囲階層はファブリックから始まります。ファブリックは、マルチサイト ドメイン（MSD）にグループ化できます。MSDのグループはデータセンターを構成します。エンドポイント ロケータ ダッシュボードに表示されるデータは、選択した範囲に基づいて集約されます。このダッシュボードから、[エンドポイント履歴（Endpoint History）]、[エンドポイント検索（Endpoint Search）]、および [エンドポイント寿命（Endpoint Life）] にアクセスできます。

エンドポイント ロケータ ダッシュボード

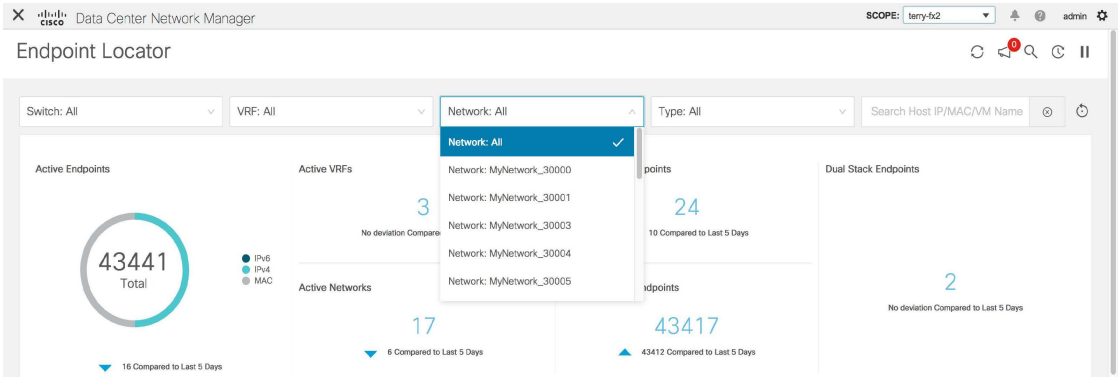
Cisco DCNM Web UIからエンドポイント ロケータの詳細を確認するには、**[モニタ（Monitor）] > [エンドポイント ロケータ（Endpoint Locator）] > [調査（Explore）]** を選択します。**エンドポイント ロケータ** ダッシュボードが表示されます。



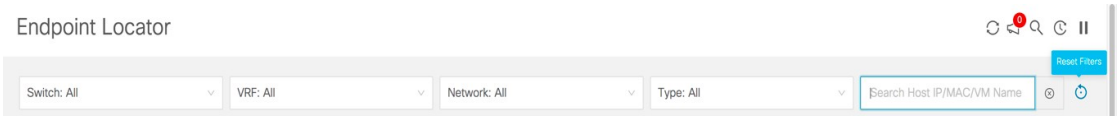
（注） Cisco DCNMリリース 11.3(1) からの規模の拡大により、システムがエンドポイント データを収集してダッシュボードに表示するまでに時間がかかる場合があります。また、エンドポイントの一括追加または削除では、EPL ダッシュボードに表示されるエンドポイント情報が最新のエンドポイントデータを更新して表示するまでに数分かかります。

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。Cisco DCNM リリース 11.3(1) 以降では、フィルタ属性としてエンドポイントの MAC タイプを選択できます。Cisco DCNM リリース 11.4(1) 以降、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もできます。

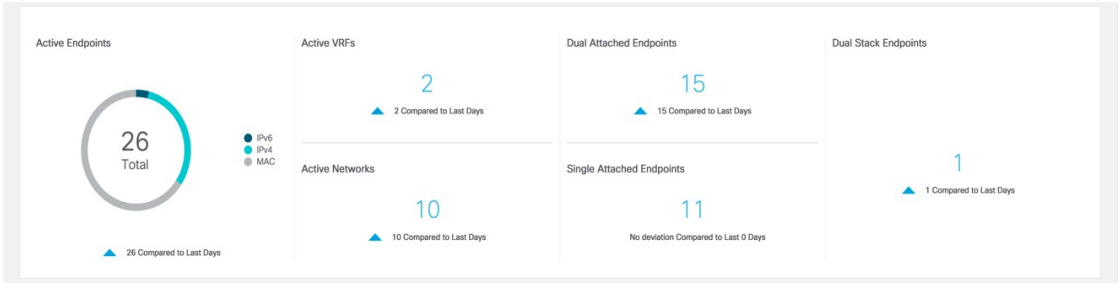
（注） ドロップダウン リストから使用可能なオプションを使用するか、**[ホスト IP/MAC/VM 名の検索（Search Host IP/MAC/VM Name）]** フィールドを使用して、検索を開始できます。ドロップダウン リストと検索フィールドの組み合わせを使用して検索を開始することはできません。



[フィルタのリセット（Reset Filters）] アイコンをクリックすると、フィルタをデフォルトのオプションにリセットできます。



ウィンドウの [上部（Top）] 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、デュアル接続エンドポイント、デュアル接続エンドポイントの数が表示されます。Cisco DCNM リリース 11.3(1) 以降、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。

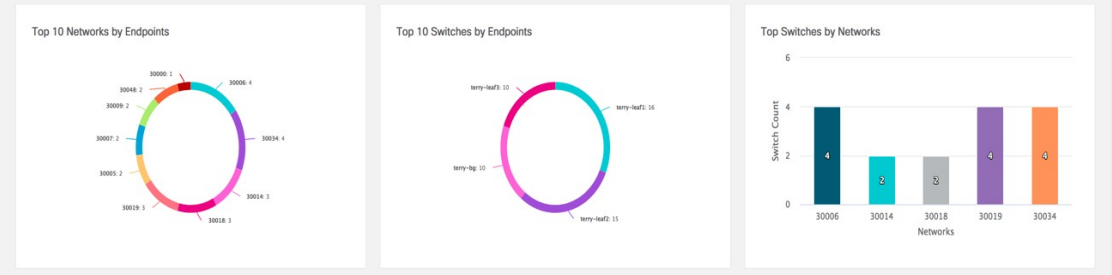


データの履歴分析が実行され、前の日に偏差が発生したかどうかを示す文が各タイルの下部に表示されます。

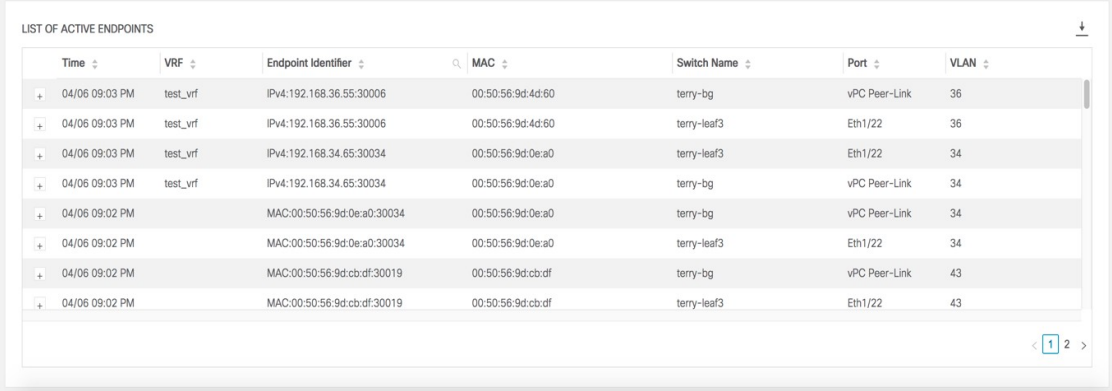
[エンドポイント履歴（Endpoint History）] ウィンドウに移動するには、EPL ダッシュボードの上部ペインで任意のタイルをクリックします。

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。

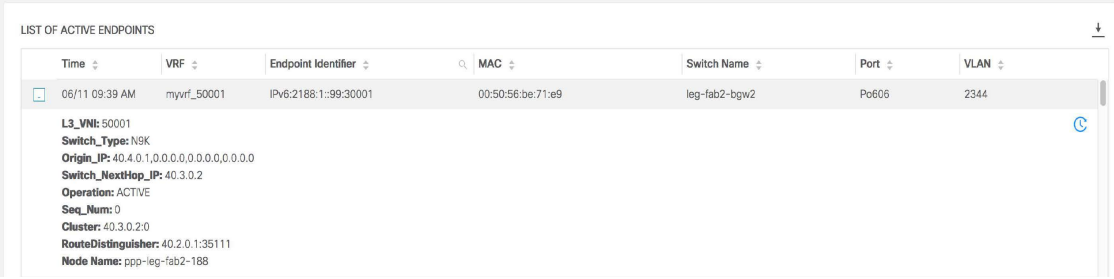
- **エンドポイント別の上位 10 個のネットワーク**：エンドポイントの数が最も多い上位 10 個のネットワークを示す円グラフが表示されます。円グラフにカーソルを合わせると、詳細情報が表示されます。必要なセクションをクリックして、IPv4、IPv6、および MAC アドレスの数を表示します。
- **エンドポイント別の上位 10 個のスイッチ**：最も多くのエンドポイントに接続されている上位 10 個のスイッチを示す円グラフが表示されます。円グラフにカーソルを合わせると、詳細情報が表示されます。必要なセクションをクリックして、IPv4、IPv6、および MAC アドレスの数を表示します。
- **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。



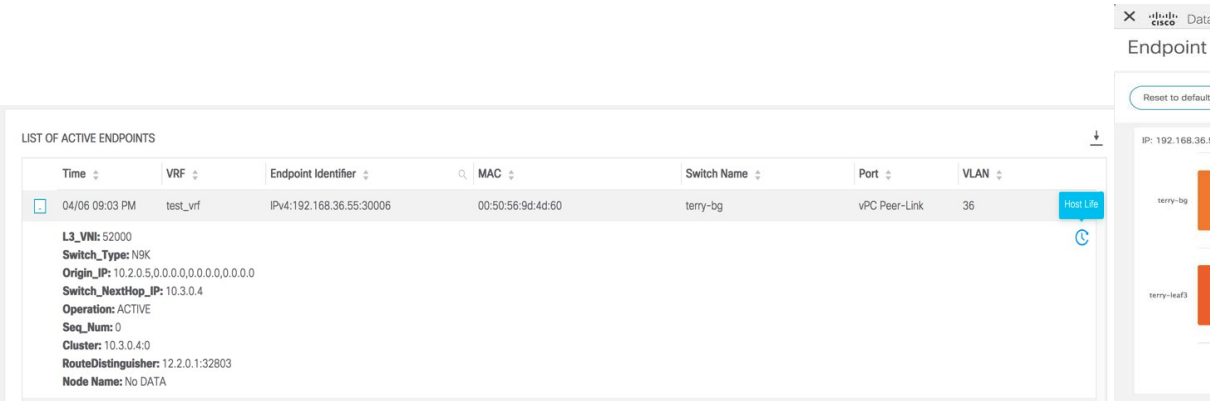
ウィンドウの「下部ペイン」には、アクティブなエンドポイントのリストが表示されます。



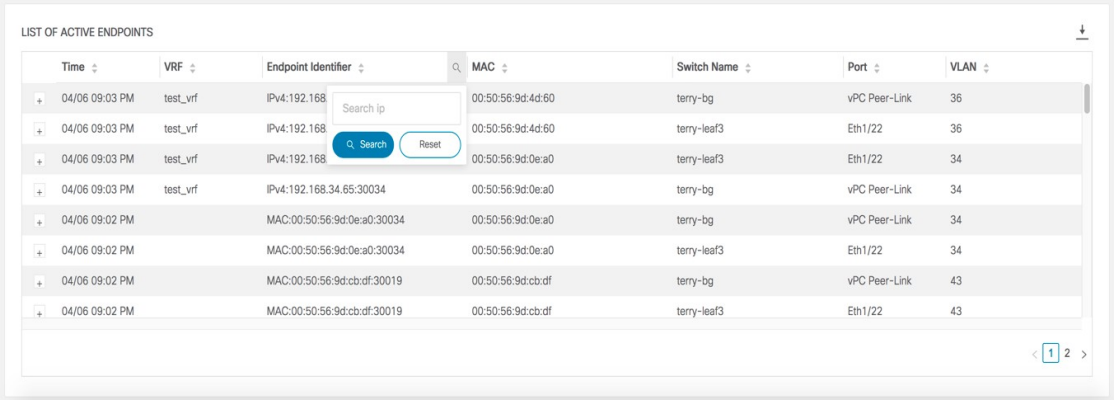
特定のエンドポイントの詳細情報を表示するには、**[+]** をクリックします。仮想マシンが設定されている場合は、VM の名前が **[ノード名（Node Name）]** フィールドに表示されます。VM の名前が EPL ダッシュボードに反映されるまでに最大 15 分かかることに注意してください。それまでは、EPL ダッシュボードの **[ノード名（Node Name）]** フィールドに**[データなし（No DATA）]** と表示されます。



[ホスト寿命（Host Life）] アイコンをクリックして、そのエンドポイントの **[エンドポイント寿命（Endpoint Life）]** ウィンドウを表示します。



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。



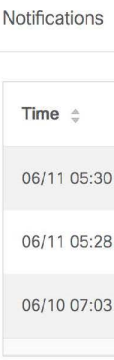
特定のシナリオでは、データポイントデータベースが同期せず、エンドポイントの数などの情報が、次のようなネットワークの問題により正しく表示されないことがあります。

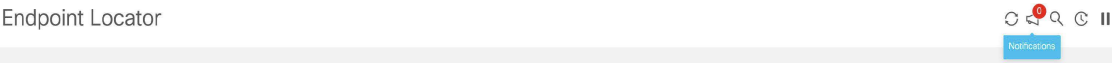
- エンドポイントが同じスイッチの下でポート間を移動し、ポート情報を更新するのに時間がかかる。
- 孤立したエンドポイントが 2 番目の VPC スイッチに接続され、孤立したエンドポイントではなくなりました。
- NX-API は最初は有効になっておらず、後で有効になります。

- 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。

このような場合、**[再同期（Resync）]** アイコンをクリックすると、現在 RR にあるデータにダッシュボードが同期されます。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。

[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。



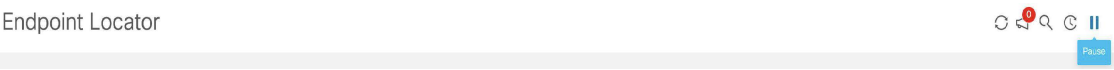


通知が生成された時刻、通知の説明、シビラティ（重大度）、ノードの名前などの情報が表示されます。

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、DCNM が BGP を介して RR に接続できることを示します（DCNM 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。ダウンロードアイコンをクリックすると、通知のリストを CSV ファイルの形式でダウンロードできます。

Cisco DCNM リリース 11.4(1) 以降、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。エンドポイントアラームの詳細については、「エンドポイント ロケータ アラーム」を参照してください。

[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。



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、EPL ダッシュボードの右上にある**[再同期（Resync）]** アイコンをクリックします。

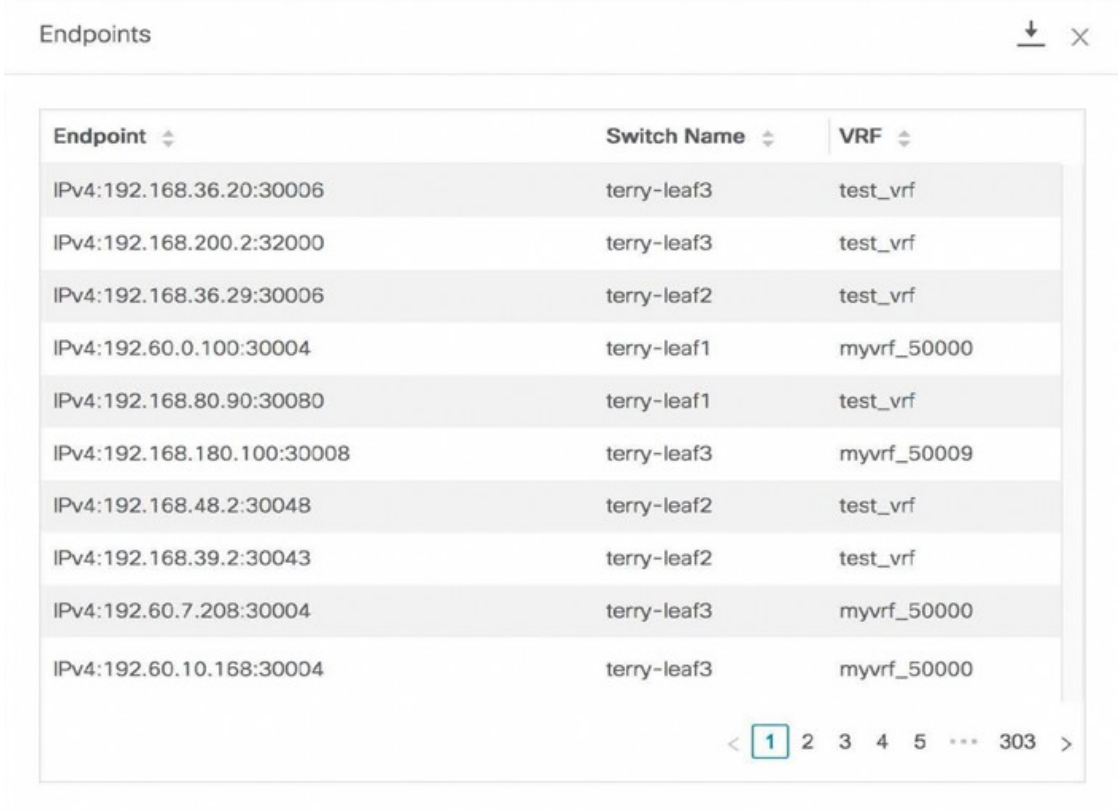
エンドポイント履歴

[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 180 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、**[アクティブ（IPv4）（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**[アクティブ（IPv4）（active（IPv4））]**

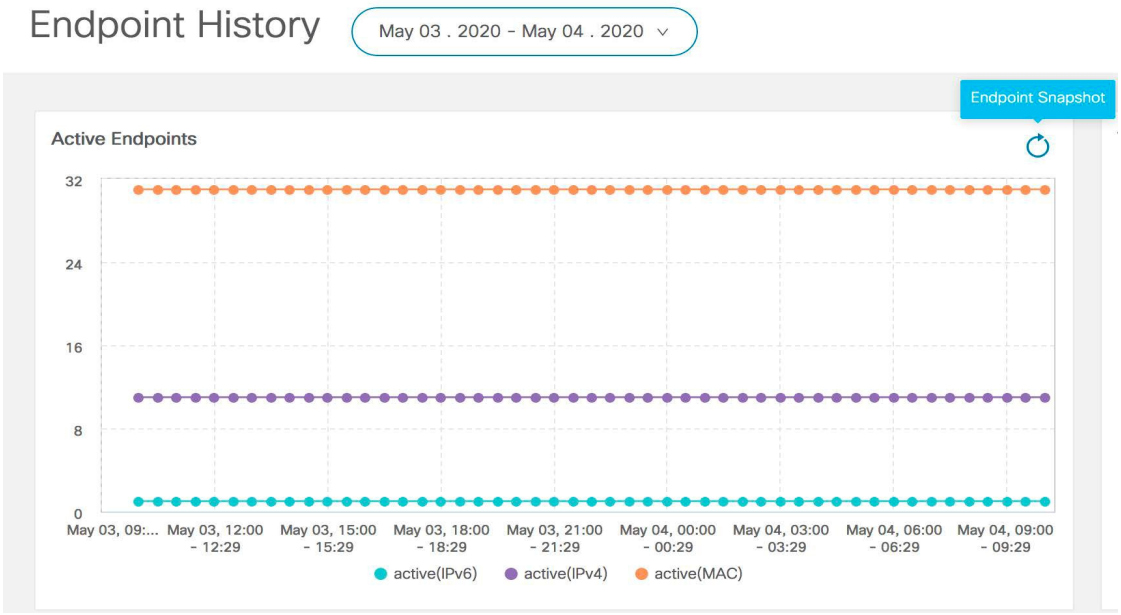
以外のすべての色分けされたポイントをクリックします。このようなシナリオでは、アクティブな IPv4 エンドポイントのみがグラフに表示されます。また、グラフの下部にある色分けされたポイントにカーソルを合わせると、特定の要件のグラフが表示されます。たとえば、**[アクティブ（IPv4）（active（IPv4））]** にカーソルを合わせると、アクティブな IPv4 エンドポイントのみがグラフに表示されます。

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。**[エンドポイント（Endpoints）]** ウィンドウの右上にあるダウンロードアイコンをクリックして、データをCSVファイルとしてダウンロードします。

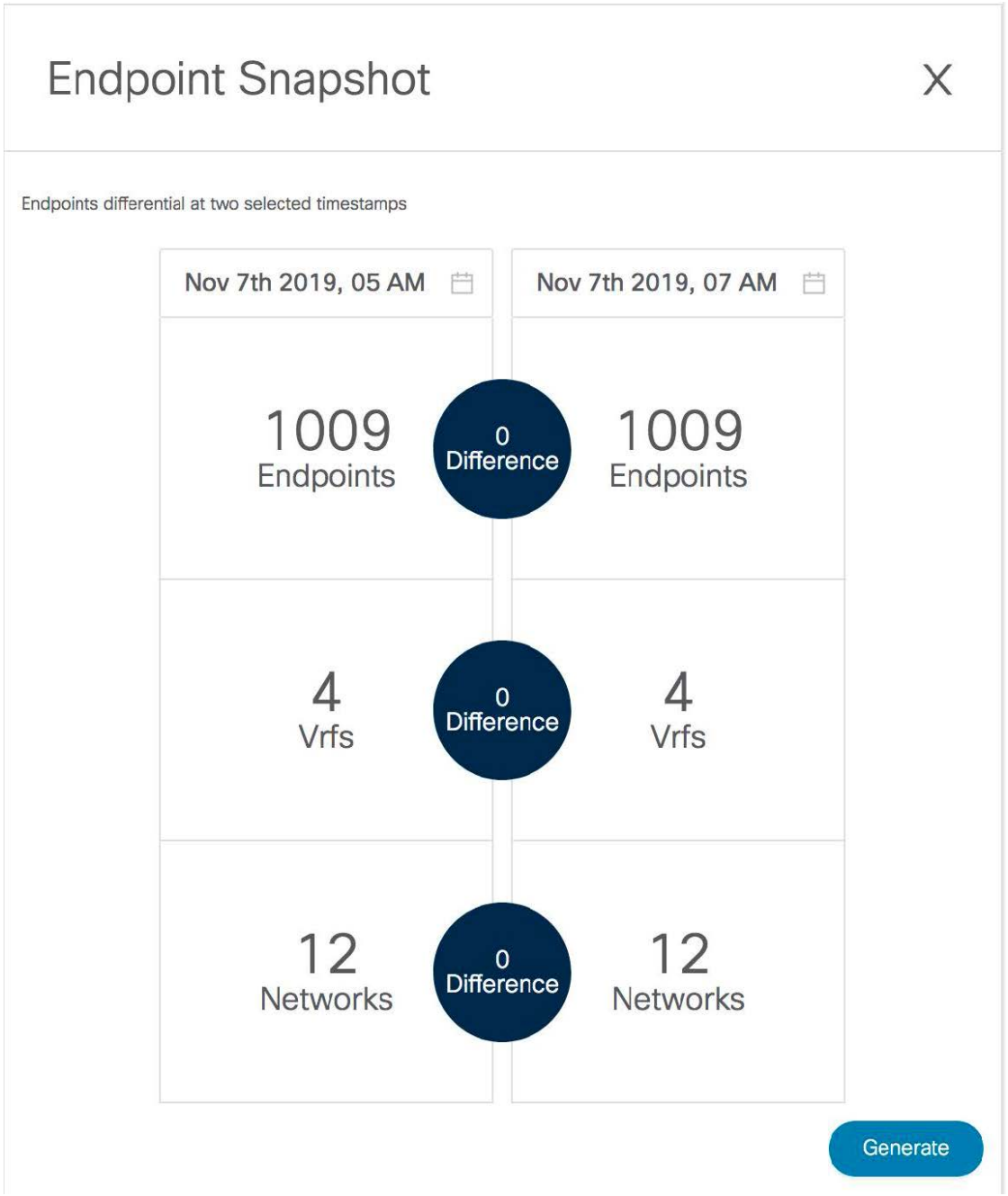


エンドポイント スナップショット

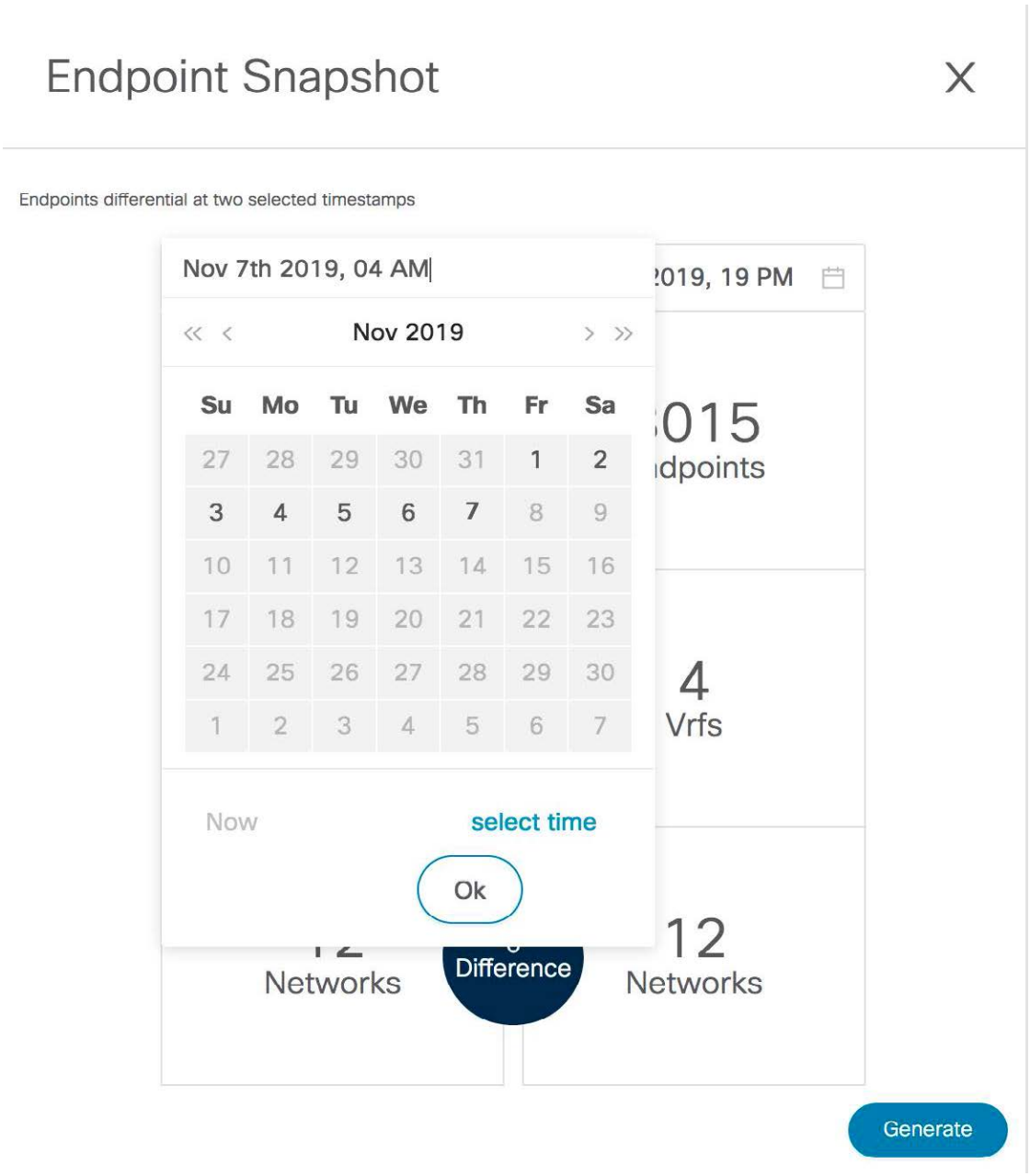
Cisco DCNM リリース 11.3(1) から、特定の 2 つの時点でエンドポイント データを比較できます。**[エンドポイント スナップショット（Endpoint Snapshot）]** ウィンドウを表示するには、**[エンドポイント履歴（Endpoint History）]** ウィンドウの **[アクティブなエンドポイント（Active Endpoints）]**グラフの右上にある **[エンドポイント スナップショット（Endpoint Snapshot）]** アイコンをクリックします。



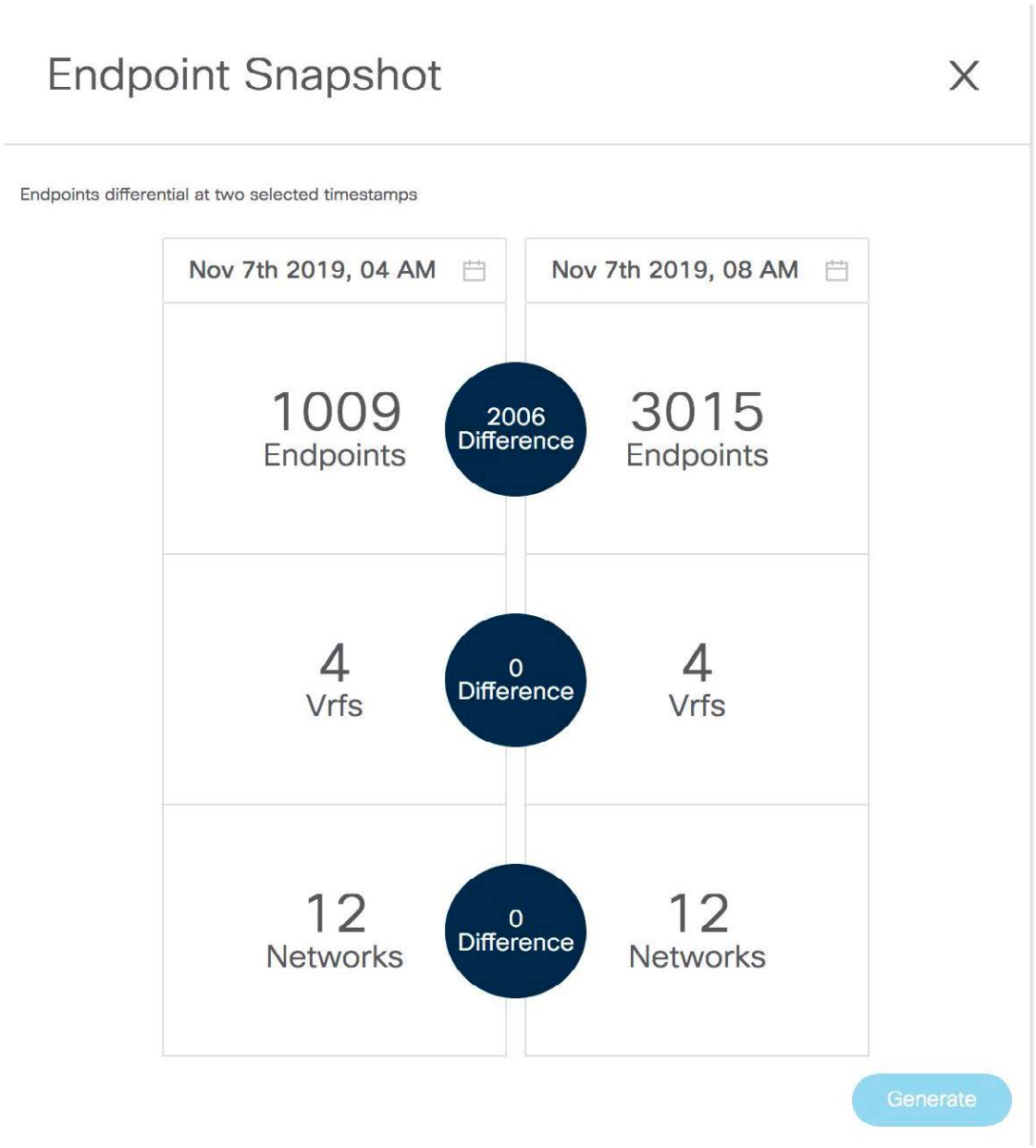
デフォルトでは、過去1時間のエンドポイント スナップショット比較データが表示されます。



特定の時点のエンドポイント スナップショットを比較するには、2 つの時点（T1 と T2）を選択し、**[生成（Generate）]** をクリックします。



選択した時点のエンドポイント、VRF、およびネットワークの比較が表示されます。エンドポイント、VRF、またはネットワークに関する詳細情報をダウンロードするには、各タイルをクリックします。**[相違（Difference）]** アイコンをクリックして、指定した時間間隔のデータの相違に関する詳細をダウンロードします。スナップショットは最大3ヵ月間保存され、その後破棄されます。

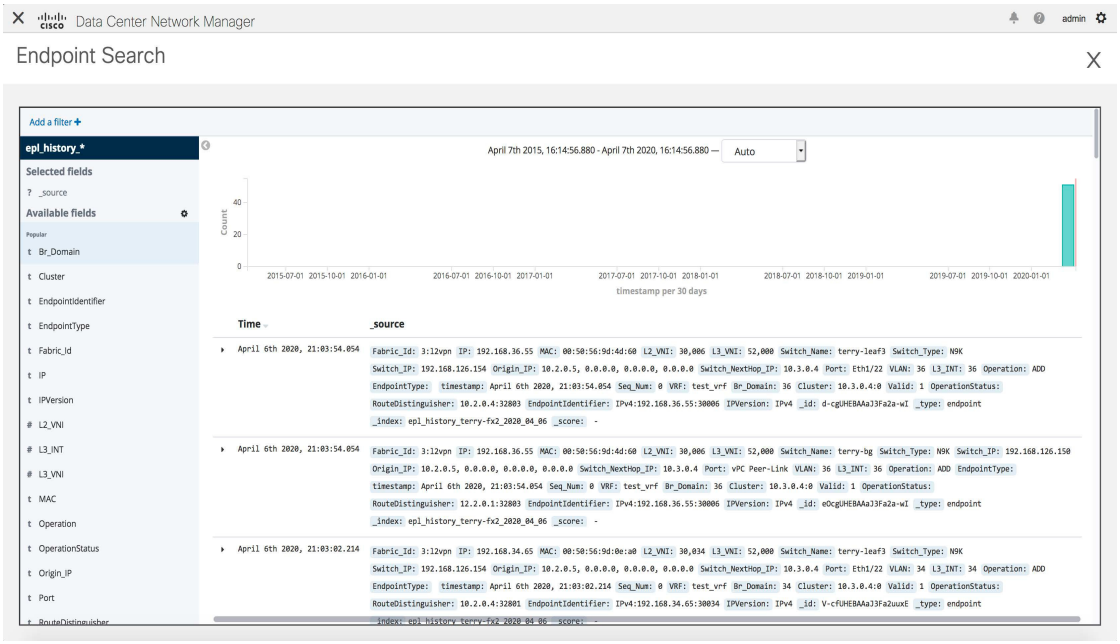


エンドポイント検索

エンドポイント ロケータ ランディング ページの右上にある **[エンドポイント検索（Endpoint Search）]** アイコンをクリックして、日付範囲で指定された期間のエンドポイント イベントを表示するリアルタイム プロットを表示します。

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。

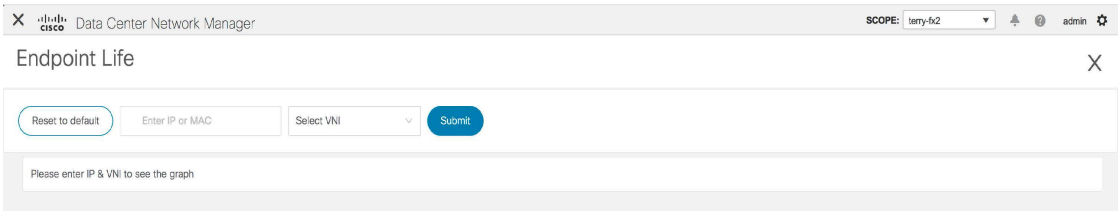


エンドポイントの寿命

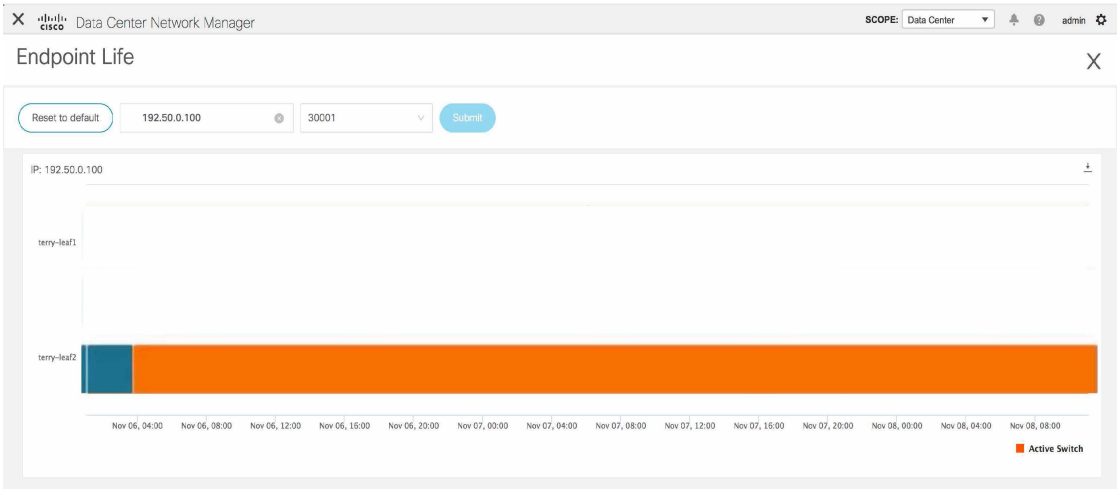
[エンドポイント ロケーター（Endpoint Locator）] ランディング ページの右上にある **[エンドポイント寿命（Endpoint Life）]** アイコンをクリックして、ファブリック内に存在する特定のエンドポイントのタイムラインを表示します。

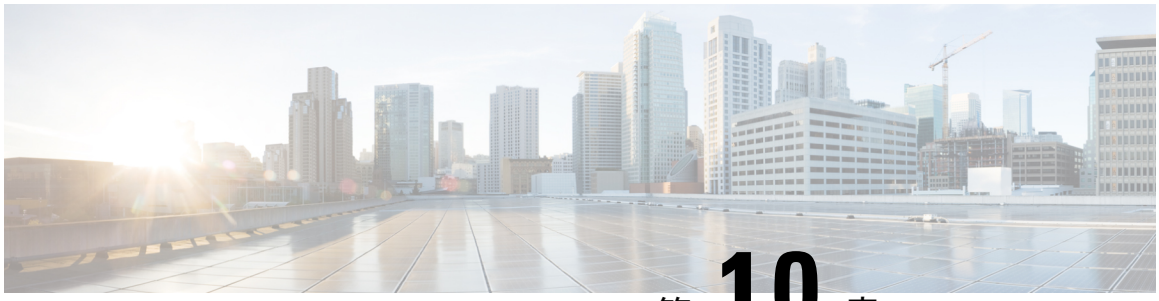
エンドポイントの IP または MAC アドレスと VXLAN ネットワーク識別子（VNI）を指定して、エンドポイントが存在していたスイッチのリストを、関連する開始日と終了日を含めて表示します。**[送信（Submit）]** をクリックします。`

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 10 章

IPAM インテグレータ

カタログ

カタログを使用すると、Cisco DCNM でインストールまたは有効にしたすべてのアプリケーションを表示できます。Cisco DCNM をインストールすると、ほとんどのアプリケーションはインストールされず、デフォルトで動作します。

Cisco DCNM 展開に基づいて、次のアプリケーションが表示されます。

- Health Monitor (2.1)
- PTP Monitoring (1.1)
- Kibana (2.0)
- Programmable report (1.1.0)
- Elastic Service (1.1)
- Compliance (4.0.0)
- Debug Tools (2.1)
- IPAM Integrator (1.0)
- Endpoint Locator (2.1)
- Kubernetes Visualizer (1.1)
- vmmplugin (4.1)

Note デフォルトで起動されたアプリケーション、または DCNM にインストールされたインフラストラクチャ サービスを使用するアプリケーションは、デフォルトで動作します。

Web UI を介して App Center から追加のアプリケーションをインストールできます。

Cisco DCNM Web UI からのアプリケーションのダウンロード、追加、起動、停止、および削除の手順については、アプリケーションのインストールと展開, on page 660 を参照してください。

IPAM インテグレータ

Cisco DCNM リリース 11.4(1) 以降、IPAM インテグレータ アプリケーションを使用して、IPAM サーバの IP 割り当てと、DCNM で定義された関連ネットワークを表示できます。DCNM 11.4(1) では、IPAM と Infoblox が統合されています。

DCNM 11.4(1) の IPAM インテグレータ アプリケーションは、IPAM および DCNM サーバへの読み取り専用アクセスを許可します。現在、IPv4 オーバーレイ DHCP がサポートされています。読み取り専用アクセス モードでは、IPAM レコードが取得され、Easy Fabric および eBGP VXLAN ファブリックの DCNM ネットワークにマッピングされます。DCNM と IPAM サーバ間でオンデマンドでレコードを同期することも選択できます。API アクセス許可と、IPAM の少なくとも IPv4 ネットワーク読み取りアクセス許可を持つ Infoblox ユーザーは、取得した Infoblox レコードを表示できます。

IPAM インテグレータ アプリケーションは、IPAM サーバと DCNM の両方に存在する一致したサブネットに加えて、競合するネットマスクを持つサブネットを確認のためにリストにします。

また、IPAM インテグレータ アプリケーションを使用して、IPAM サーバの IP 割り当てと DCNM で定義された関連ネットワークを表示する方法に関するビデオを見ることもできます。ビデオ：Cisco DCNM での IPAM インテグレータの使用を参照してください。

IPAM インテグレータへのアクセス

この手順は、IPAM インテグレータ アプリケーションにアクセスする方法を示しています。

手順

ステップ 1 **[アプリケーション（Applications）] > [カタログ（Catalog）]** に移動します。

ステップ 2 IPAM インテグレータ アプリケーション アイコンをクリックして、アプリケーションにアクセスします。アプリケーションがまだ開始されていない場合、このアクションは、GUI にアクセスする前にアプリケーションを開始します。

ステップ 3 **[アクセス認証（Access Authentication）]** ウィンドウで、必要なアクセスの詳細を入力します。

（注） Infoblox サーバまたは Infoblox グリッド マネージャのアクセスの詳細を提供できます。

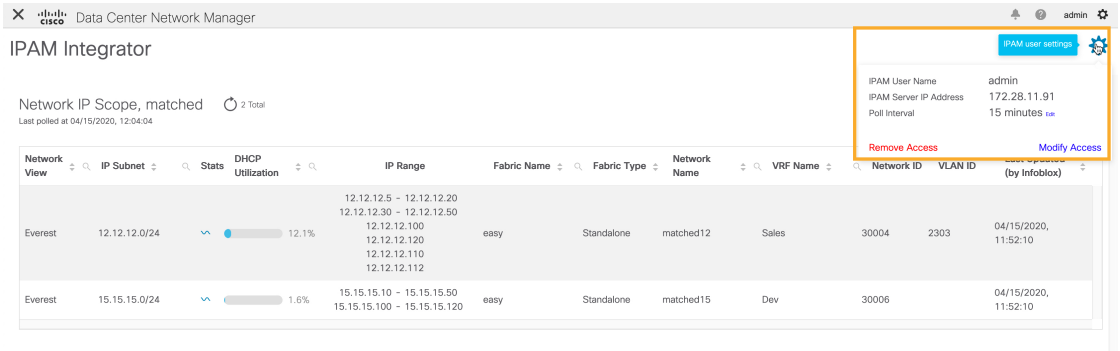
- **IPAM ユーザー名** – IPAM サーバのユーザー名を指定します。Infoblox ユーザーは、アプリケーションが API を介して Infoblox サーバからデータを取得するための API アクセス許可を付与されている必要があります。
- **パスワード** – ユーザー名に対応する IPAM サーバのパスワードを指定します。
- **IPAM サーバの IP アドレス** – IPAM サーバの IP アドレスを指定します。

- **ポーリング間隔（分）**– Cisco DCNM および IPAM サーバからデータを取得する頻度を決定する時間を分単位で指定します。デフォルト値は 15 分です。ポーリング値の範囲は 2 ～ 60 分です。

ステップ 4 [作成（Create）] をクリックします。

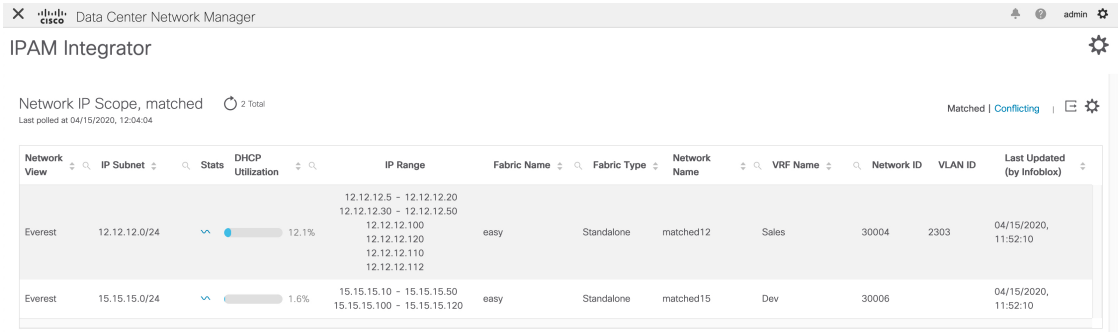
ステップ 5 IPAM にアクセスした後、**[設定（Settings）]** アイコンを使用してアクセスの詳細を削除または変更できます。**[編集（Edit）]** を使用して、ポーリング間隔を編集することもできます。

（注） **admin** ロールを持つ DCNM ユーザーのみが、アクセス設定を追加、更新、および削除できます。また、API アクセス許可と、少なくとも IPAM アクセス許可の IPv4 ネットワーク読み取りアクセスが付与されている Infoblox ユーザーのみが、取得した Infoblox ネットワーク レコードを表示できます。



ネットワーク IP スコープの表示

[ネットワーク IP 範囲（Network IP Scope）] は、IPAM インテグレータ アプリケーションにアクセスした後のランディング ページです。



次の表では、IPAM サーバから取得されるフィールドについて説明します。

フィールド	説明
ネットワーク ビュー	Infoblox サーバ上に独自のネットワークと共有ネットワークを持つ単一のルーティング ドメインであるネットワーク ビューを指定します。

IPサブネット	IPAM サーバで定義されている IP サブネットを指定します。サブネットまたはサブネットワークは、より大きなネットワークのセグメント化された部分です。より具体的には、サブネットは、IP ネットワークを複数のより小さなネットワーク セグメントに分割した論理パーティションです。
Stats	**[統計（Stats）]** 列の下のアイコンをクリックして、IP サブネットの使用率に関する統計を表示します。詳細については、サブネット使用状況の統計の表示 （709 ページ）を参照してください。
DHCP 使用率	リースされている IP アドレスに関して、ネットワークの使用率を指定します。 パーセンテージ値にカーソルを合わせると、割り当てられた IP の数とその詳細が表示されます。 Infoblox サーバでは、DHCP 使用率の計算に時間がかかります。IPAM 使用率は Infoblox サーバー上で約 15 分ごとに計算されます。その後、最新の値が IPAM インテグレータ アプリに反映されます。
IP範囲	ネットワークの IP 範囲を指定します。範囲にカーソルを合わせると、有効な DHCP 範囲、予約済み DHCP 範囲、およびネットワークの固定アドレスが表示されます。

次の表では、DCNM から取得される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。
ファブリックタイプ	ファブリックのタイプを指定します。マルチサイト展開（MSD）、スタンドアロンの簡易ファブリック、eBGP VXLAN ファブリックのいずれかです。
ネットワーク名（Network Name）	ネットワークの名前を指定します。
VRF Name	VRF の名前を指定します。
ネットワーク ID（Network ID）	ネットワーク ID を指定します。
VLAN ID	VLAN ID を指定します。
最終更新日（Last Updated）（Infoblox による）	データが Infoblox によって最後に更新された日時を指定します。 （注） 前回のポーリングの日時は、**[ネットワーク IP 範囲（Network IP Scope）]** タイトルの下に表示されます。

.csv ファイルにデータを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。

各フィールドでは、矢印アイコンをクリックして値をソートし、**[検索（search）]** アイコンをクリックし値を入力して検索できます。

フィールドの上にある **[設定（Settings）]** アイコンをクリックして、表示するフィールドを削除または追加します。

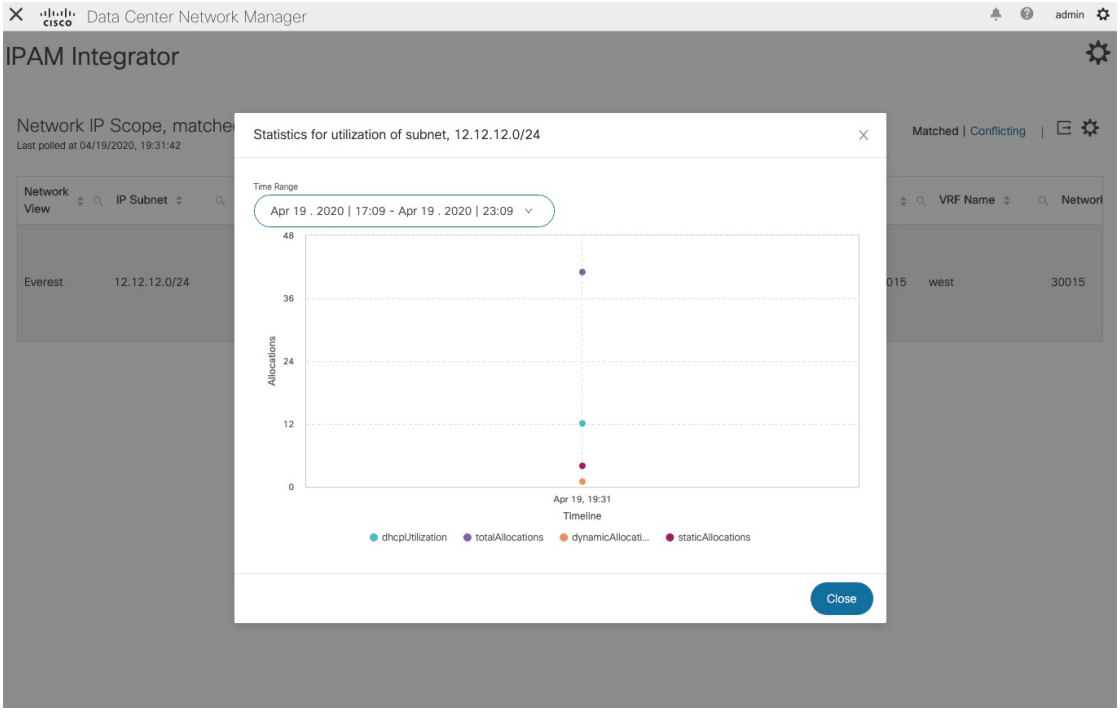
データのポーリングは、次の基準に基づいています。

- ユーザーが **[アクセス認証（Access Authentication）]** ウィンドウで最初に構成したポーリング間隔の値。Cisco DCNM および IPAM からデータを取得する頻度を指定します。
- ユーザーは、**[更新（Refresh）]** アイコンをクリックして、DCNM および IPAM サーバから瞬時にデータを受信できます。
- DCNM Web UI は 2 分ごとに自動的に更新され、DCNM および Infoblox サーバから取得したデータを表示します。

  たとえば、ポーリング間隔が 15 分で、ユーザーがこの 15 分の期間中にデータを（オンデマンドで） 更新しなかった場合、DCNM Web UI には、15 分まで 2 分の更新ごとに同じポーリング データが表示されます。15 分後、新しいデータが DCNM および IPAM からポーリングされ、データベースに保存されます。この新しいデータは結局、最初から 16 分後に DCNM によってフェッチされます。

サブネット使用状況の統計の表示

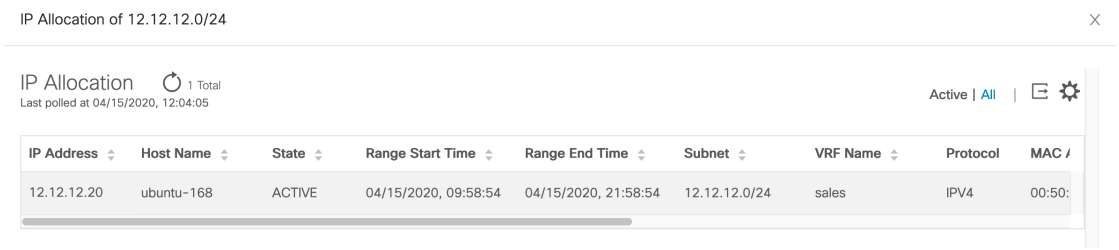
[統計（Stats）] 列の下のアイコンをクリックして、一定期間の IP サブネットの使用率に関する統計を表示します。



[時間範囲（Time Range）] ドロップダウン リストから、統計を表示する時間を選択します。これらの統計には、DHCP 使用率、合計割り当て、動的割り当て、静的割り当てなどのサブネットの使用率が含まれます。

ホストの IP 割り当ての表示

[IP 範囲（IP Range）] 列の下の IP 範囲の値をクリックして、各ホストの IP 割り当てを表示します。



[IP 割り当て（IP Allocation）] ウィンドウの各ホストについて、以下のフィールドが表示されます。これらのフィールドのデータは、IPAM サーバーから取得されます。

- IP アドレス
- ホスト名
- ホストの状態（アクティブまたはフリー）
- 開始時間と終了時間の範囲
- Subnet
- VRF Name
- プロトコル バージョン
- MAC アドレス
- IP アドレスやサーバー名などの DHCP サーバー情報
- ホストが最後にリクエストした

各フィールドでは、矢印アイコンをクリックして値をソートし、**[検索（search）]** アイコンをクリックし値を入力して検索できます。

デフォルトでは、アクティブなホストのみに関する情報が表示されます。**[すべて（All）]** の値をクリックして、IPAM サーバーから取得したすべてのホストに関する情報を表示します。.csv ファイルにデータを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。

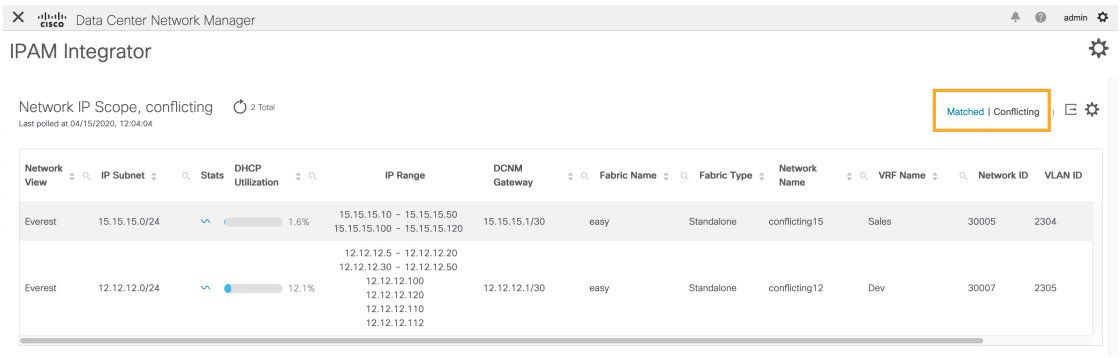
最近解放されたホストは、**[すべて（All）]** タブに「FREE」と表示されます。もともとフリーのホストは FREE として表示されません。このタブには、最近解放されたホストのみが表示されます。

右側の **[設定（Settings）]**（歯車）アイコンをクリックして、表示するフィールドを削除または追加します。

競合するネットワークの表示

IPAM インテグレータは、IPAM サーバと DCNM で定義されている競合するネットワークを検出します。この情報を表示するには、**[ネットワーク IP 範囲（Network IP Scope）]** ウィンドウで **[競合（Conflicting）]** をクリックします。

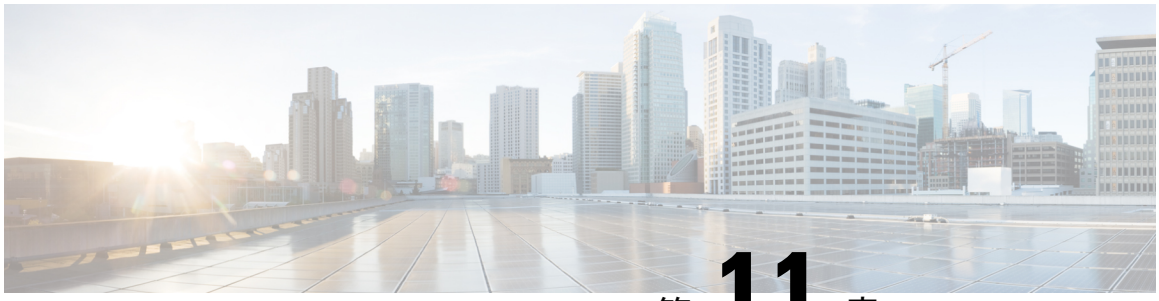
たとえば、あるネットワークが別のネットワークのサブセットである場合、ネットワークの競合する IP アドレスは、**[競合（Conflicting）]** の下に表示されます。



データは、**一致した**データが表示される方法と同様に表示されます。**[IP 範囲（IP Range）]** 列の下の IP 範囲の値をクリックして、各ホストの IP 割り当てを表示できます。

この表には、IPAM サーバからのサブネット情報に加えて、競合する IP 範囲の DCNM ゲートウェイもリストされていることに注意してください。

各フィールドでは、矢印アイコンをクリックして値をソートし、**[検索（search）]** アイコンをクリックし値を入力して検索できます。



第 11 章

ヘルスモニター

カタログ

カタログを使用すると、Cisco DCNM でインストールまたは有効にしたすべてのアプリケーションを表示できます。Cisco DCNM をインストールすると、ほとんどのアプリケーションはインストールされず、デフォルトで動作します。

Cisco DCNM 展開に基づいて、次のアプリケーションが表示されます。

- Health Monitor (2.1)
- PTP Monitoring (1.1)
- Kibana (2.0)
- Programmable report (1.1.0)
- Elastic Service (1.1)
- Compliance (4.0.0)
- Debug Tools (2.1)
- IPAM Integrator (1.0)
- Endpoint Locator (2.1)
- Kubernetes Visualizer (1.1)
- vmmplugin (4.1)

Note デフォルトで起動されたアプリケーション、または DCNM にインストールされたインフラストラクチャ サービスを使用するアプリケーションは、デフォルトで動作します。

Web UI を介して App Center から追加のアプリケーションをインストールできます。

Cisco DCNM Web UI からのアプリケーションのダウンロード、追加、起動、停止、および削除の手順については、アプリケーションのインストールと展開, on page 660 を参照してください。

ヘルス モニタ

ヘルス モニタは、インフラストラクチャの健全性とステータスを監視するのに役立ちます。ヘルス モニタ アプリケーションを使用して、アラート、サービス使用率、およびコンピューティング使用率を監視できます。11.2(1) をインストールまたはアップグレードすると、デフォルトで エルス モニタ アプリケーションがインストールされ、動作可能になります。

ヘルス モニタ アプリを起動するには、Cisco DCNM Web UI で、**[アプリケーション（Applications）]** を選択します。[カタログ（Catalog）] タブで、 **ヘルス モニタ**をクリックしてアプリケーションを起動します。

Note ヘルス モニタ アプリケーションは、デフォルトで Cisco DCNM クラスタ モードでインストールされます。

ヘルス モニタ アプリは、サービス、コンピューティング、および DCNM サーバの次のメトリックを広く監視し、アラートを生成します。

- CPU 使用率
- メモリ使用率
- ネットワーク I/O（eth0）
- ディスク I/O（Disk I/O）

ヘルス モニタ アプリケーションを使用して、以下を監視できます。

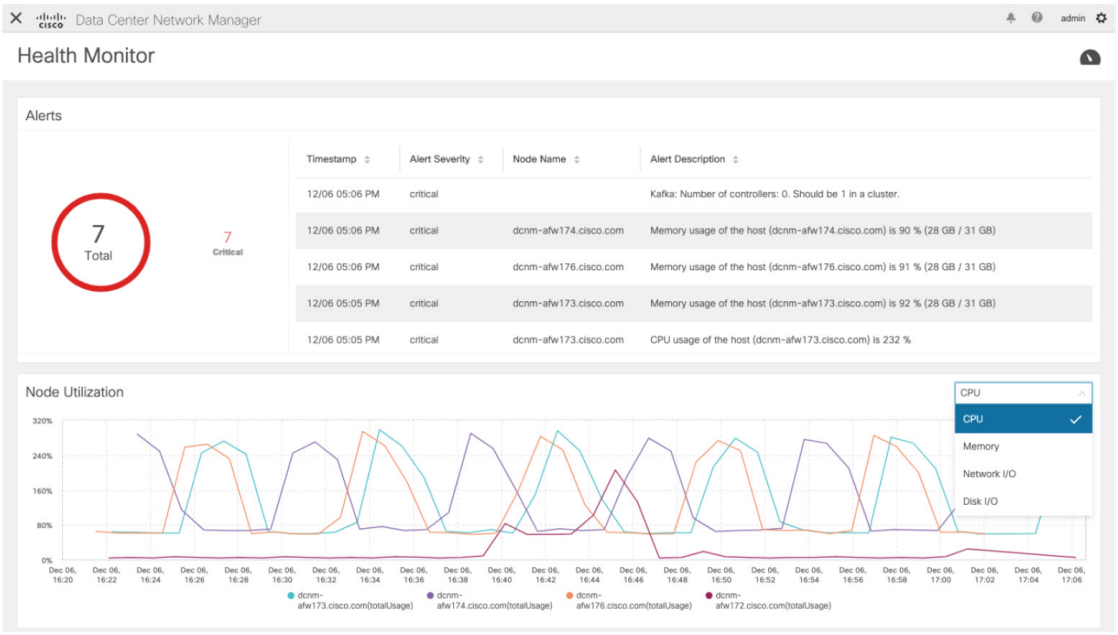
アラート

[アラート（Alarts）] ウィンドウには、指定した日時以降に発生したアラートの数に関する情報が表示されます。アラートは、次のカテゴリに基づいて、グラフィカル ビューとリスト ビューで表示できます。

グラフィカル ビューでは、カテゴリは次のとおりです。

- **[重大度（Severity）]** は、重大/メジャー/マイナー/情報に基づいてアラートを表示します。
- **[タイプ（Type）]** には、クラスター タイプに基づいてアラートが表示されます。
- **[コンピューティング（Compute）]** は、コンピューティング ノードごとのアラートを表示します。
- **[サービス（Service）]** は、Cisco DCNM で実行されているすべてのサービスのアラートを表示します。

[更新（Refresh）] アイコンをクリックしてアラートを更新します。リスト表示アイコンをクリックして、アラートをリスト形式で表示します。



リスト ビューでは、アラートが次のカテゴリの表形式で表示されます。

- **[タイムスタンプ（Timestamp）]** は、アラートがトリガされた時刻を表示します。形式は MM/DD HH:MM AM/PM です。
- **[アラートの重大度（Alert Severity）]** には、アラートの重大度が表示されます。
- **[アラート タイプ（Alert Type）]** には、クラスタのアラート タイプが表示されます。
- **[ノード名（Node Name）]** には、アラートがトリガーされるノード名が表示されます。
- **[アラートの説明（Alert Description）]** には、アラートの概要が表示されます。

右または左のナビゲーション矢印をクリックして、次または前のページに移動します。

ページに表示するアイテムの数を設定することもできます。**[ページごとのオブジェクト（Objects Per Page）]** ドロップダウンリストで適切な番号を選択します。

[グラフィカル表示（Graphical representation）] アイコンをクリックして、グラフィカル ビューに移動します。**[データのダウンロード（Download Data）]** アイコンをクリックして、トラブルシューティングの目的でアラート情報をダウンロードします。

ヘルス モニタは、次のメトリクスのアラートを生成します。

- CPU 使用率 >= 65 %
- メモリ使用率 >= 65 %
- ディスク使用率 >= 65 %
- Elasticsearch クラスタのステータス：赤/黄

- Elasticsearch の未割り当てのシャード > 0
- 使用されている Elasticsearch JVM ヒープ >= 65 %
- リーダーのない Kafka パーティション：コントローラのオフライン パーティション数 > 0
- Kafka コントローラ数：コントローラのアクティブなコントローラ数 != 1
- Kafka パーティション リーダー：コントローラの不明確なリーダー選挙カウント > 0

サービス使用率

このウィンドウで、Cisco DCNM で実行されているすべてのサービスをモニタできます。時間範囲とサービスに基づいて、グラフィック ビューにサービスの CPU とメモリの使用率が表示されます。右上隅の **[コンピューティングの使用率（Compute Utilization）]** アイコンをクリックして、CPU 使用率のグラフィカル ビューを起動します。

[時間範囲（Time Range）] ドロップダウン リストから、使用率を表示する時間範囲を選択します。特定の時間間隔を選択し、時間間隔中のメトリクスを表示できます。必要な時間と日付間隔を選択するために日付と時間を表示しているフィールドをクリックします。カレンダーの日付をクリックし、範囲を設定することもできます。**[適用（Apply）]** をクリックし、時間範囲を確認します。

[サービス（Services）] ドロップダウン リストからサービスを選択して、そのサービスの使用率を表示します。このリストには、Cisco DCNM で現在実行されているすべてのサービスが含まれています。

[時間範囲（Time Range）] を選択し、**[サービス（Service）]**、**[CPU 使用率（Cpu Utilization）]**、および **[メモリ使用率（Memory Utilization）]** グラフを表示します。特定の時間の CPU とメモリ使用率の詳細については、個別のグラフの特定のポイントにカーソルを置いて表示することもできます。

メモリ使用率のグラフィカルビューは、実際のメモリ消費量（RAM）をギガバイト（GB）単位で示します。

右上隅の **[X]** アイコンをクリックし、[サービス使用率（Service Utilization）] ウィンドウを閉じて、[アラート（Service Utilization）] ウィンドウに戻ります。

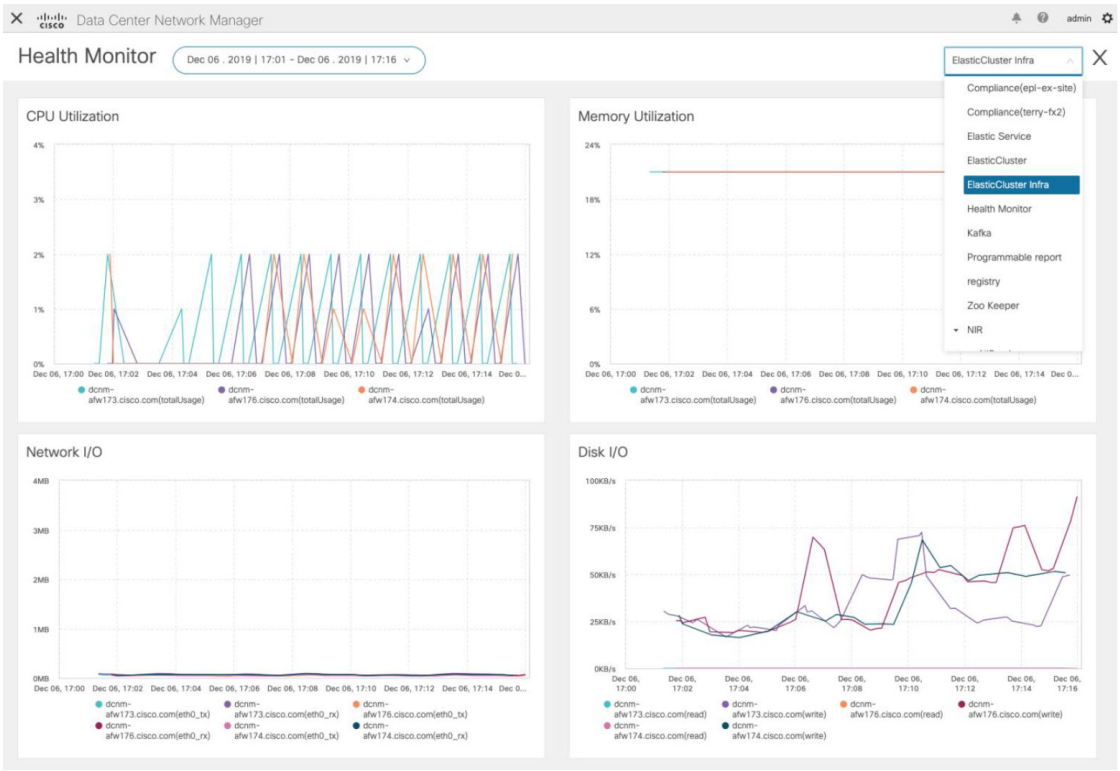
サービス使用率におけるヘルス モニタのガイドラインと制限事項

- Kafka、ElasticSearch、FMserver など、CPU 制限のないアプリケーションの CPU 使用率は、グラフで 100% の使用率を示す場合があります。100% の使用率は、このアプリケーションが 1 つ以上のコアを使用するためです。
- アプリケーションの CPU 使用率に関して、次のアラートがトリガされます。
  - マイナー アラート：200 ～ 400 %

    メジャー アラート：400 ～ 600%

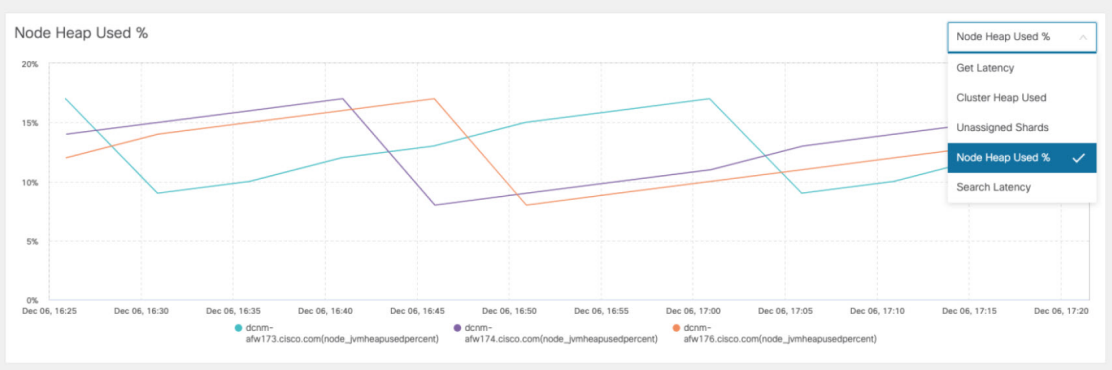
    重大： > 600%

- Kafka コントローラ カウントの一時的なメッセージが、重大なアラートとして表示されることがあります。更新後 2 分以内にアラートがクリアされた場合は、アラートを無視できます。
- **[ディスク I/O（Disk I/O）]** および **[メモリ使用率（Memory Utilization）]** のメトリックは、Kafka および Elastic Service では使用できません。
- **[ネットワーク I/O（Network I/O）]** メトリックは、**[DCNM: FMServer]** および **[DCNM: Postgres]** では使用できません。
- メトリクスは自動的に更新されません。ドロップダウンリストのオプションを使用して異なるウィンドウ間を移動し、メトリクスを更新します。さらに、時間範囲を変更して、選択した期間のメトリクスを更新することもできます。
- 同じ機能のアラートが重複している可能性があります。



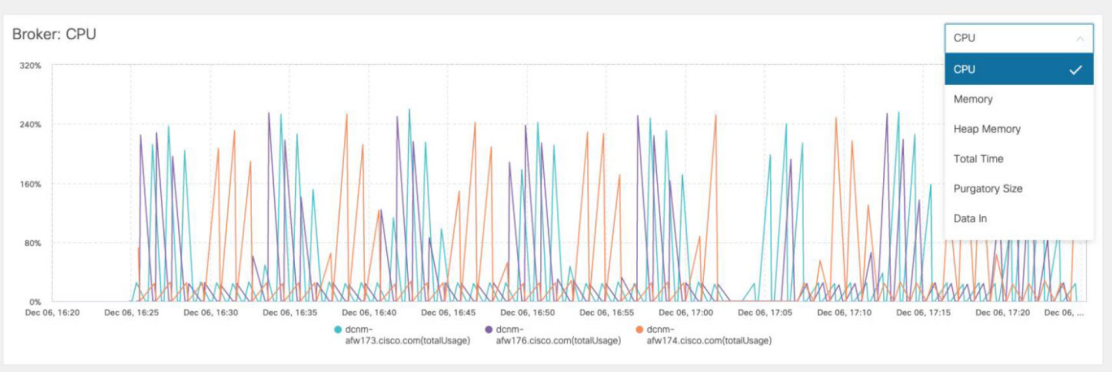
エラスティック クラスタについて、次の追加のメトリクスが収集されます。

- 取得待ち時間：ID で 1 つのレコードを取得するための待ち時間
- 使用されているクラスタ ヒープ：クラスタによって使用されるヒープ メモリ
- 未割り当てのシャード：未割り当てのシャードの数
- ノード ヒープ使用率：ノードによって使用されたヒープ メモリのパーセンテージ
- 検索レイテンシー：レコードのコレクションを取得するためのレイテンシー



Kafka ブローカーについて、次の追加のメトリックが収集されます。

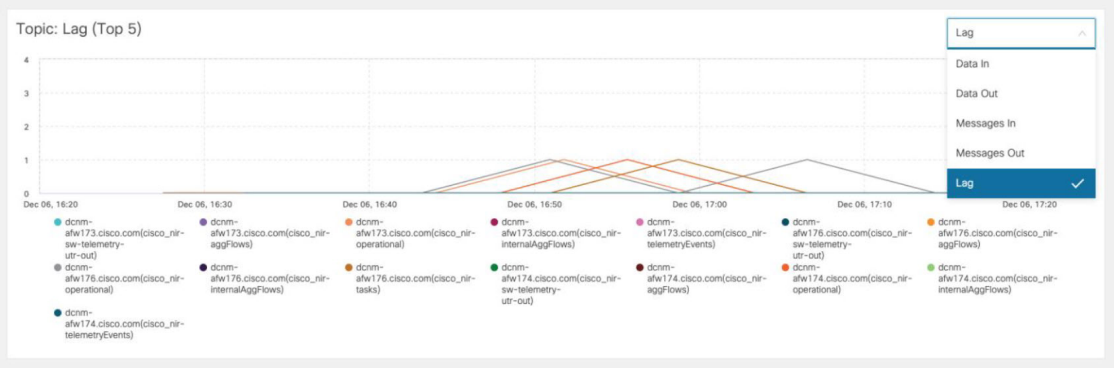
- CPU：ブローカーの CPU 使用率
- メモリ：ブローカーのメモリ使用率
- ヒープ メモリ：ブローカーが使用するヒープ メモリ
- 合計時間：ネットワーク生産、ネットワーク フェッチ フォロワー、ネットワーク フェッチ消費時間
- パーガトリー サイズ：サーバー フェッチ パーガトリー サイズ、サーバー プロデュース パーガトリー サイズのブローカー
- データ入力：ブローカーのバイト入力
- データ出力：ブローカーのバイト出力
- メッセージの受信：ブローカーが受信したメッセージ
- フェッチ要求：ブローカーの合計フェッチ要求
- ISR：ブローカーの同期レプリカの拡張と縮小



上位 5 つの Kafka トピックについて、次の追加のメトリックが収集されます。

- データ入力：トピックのバイト入力
- データ出力：トピックのバイト出力

- メッセージの受信：トピックのメッセージ受信数
- メッセージ の送信：トピックのメッセージ送信数
- ラグ：トピックごとのラグ



コンピューティング使用率

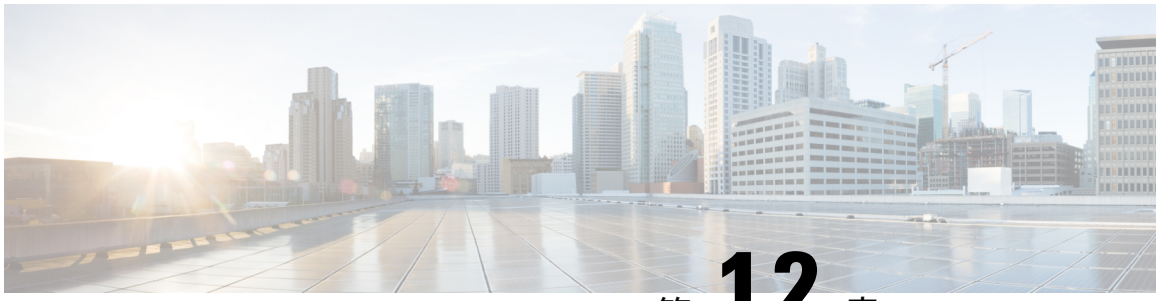
Cisco DCNM とともにインストールされたすべてのコンピューティングを監視できます。時間範囲とサービスに基づき、グラフィッカル ビューではサービスの CPU とメモリ使用率を表示します。右上隅の **[コンピューティングの使用率（Compute Utilization）]** アイコンをクリックして、CPU 使用率のグラフィカル ビューを起動します。

[時間範囲（Time Range）] ドロップダウン リストから、使用率を表示する時間範囲を選択します。特定の時間間隔を選択し、時間間隔中のメトリクスを表示できます。必要な時間と日付間隔を選択するために日付と時間を表示しているフィールドをクリックします。カレンダーの日付をクリックし、範囲を設定することもできます。**[適用（Apply）]** をクリックし、時間範囲を確認します。

[時間範囲（Time Range）] を選択し、**[サービス（Service）]**、**[CPU 使用率（Cpu Utilization）]**、および **[メモリ使用率（Memory Utilization）]** グラフを表示します。特定の時間の CPU とメモリ使用率の詳細については、個別のグラフの特定のポイントにカーソルを置いて表示することもできます。

メモリ使用率のグラフィカルビューは、実際のメモリ消費量（RAM）をギガバイト（GB）単位で示します。

右上隅の **[X]** アイコンをクリックし、[サービス使用率（Service Utilization）] ウィンドウを閉じて、[アラート（Service Utilization）] ウィンドウに戻ります。



第 12 章

PTP Monitoring

カタログ

カタログを使用すると、Cisco DCNM でインストールまたは有効にしたすべてのアプリケーションを表示できます。Cisco DCNM をインストールすると、ほとんどのアプリケーションはインストールされず、デフォルトで動作します。

Cisco DCNM 展開に基づいて、次のアプリケーションが表示されます。

- Health Monitor (2.1)
- PTP Monitoring (1.1)
- Kibana (2.0)
- Programmable report (1.1.0)
- Elastic Service (1.1)
- Compliance (4.0.0)
- Debug Tools (2.1)
- IPAM Integrator (1.0)
- Endpoint Locator (2.1)
- Kubernetes Visualizer (1.1)
- vmmplugin (4.1)

Note デフォルトで起動されたアプリケーション、または DCNM にインストールされたインフラストラクチャ サービスを使用するアプリケーションは、デフォルトで動作します。

Web UI を介して App Center から追加のアプリケーションをインストールできます。

Cisco DCNM Web UI からのアプリケーションのダウンロード、追加、起動、停止、および削除の手順については、アプリケーションのインストールと展開, on page 660 を参照してください。

PTP Monitoring

このセクションでは、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。

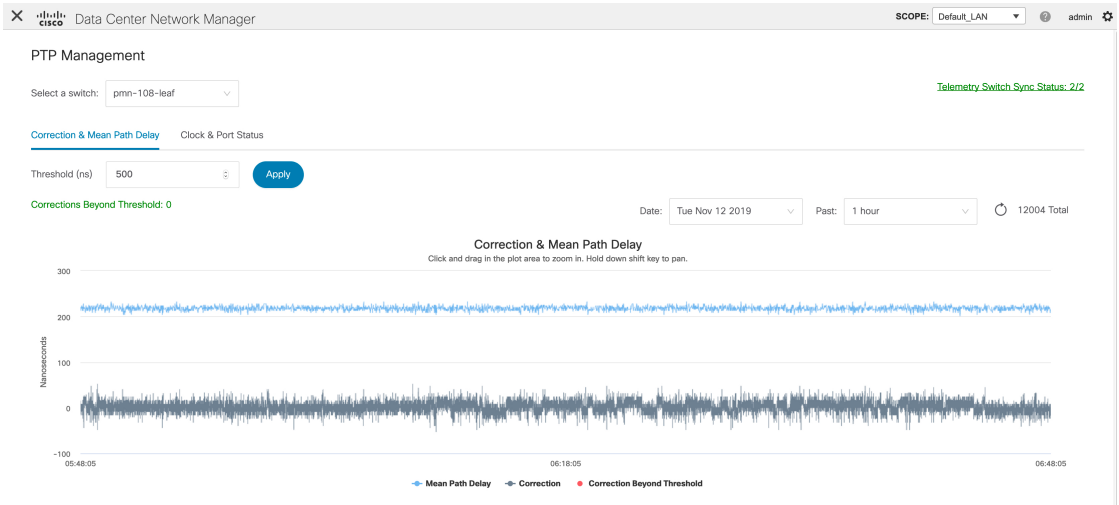
DCNM では、PTP モニタリングをアプリケーションとしてインストールできます。DCNM Web UI から、**[アプリケーション（Applications）]** に移動し、**[PTP モニタリング（PTP Monitoring）]** をクリックします。このアプリケーションは、IPFM モードでのみ動作します。

[PTP 管理（PTP Management）] ウィンドウで、**[スイッチの選択（Select a switch）]** ドロップダウンリストから選択したスイッチに基づき、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）**

Note **[範囲（SCOPE）]** ドロップダウンリストから選択したスイッチ グループの PTP 関連情報が表示されます。



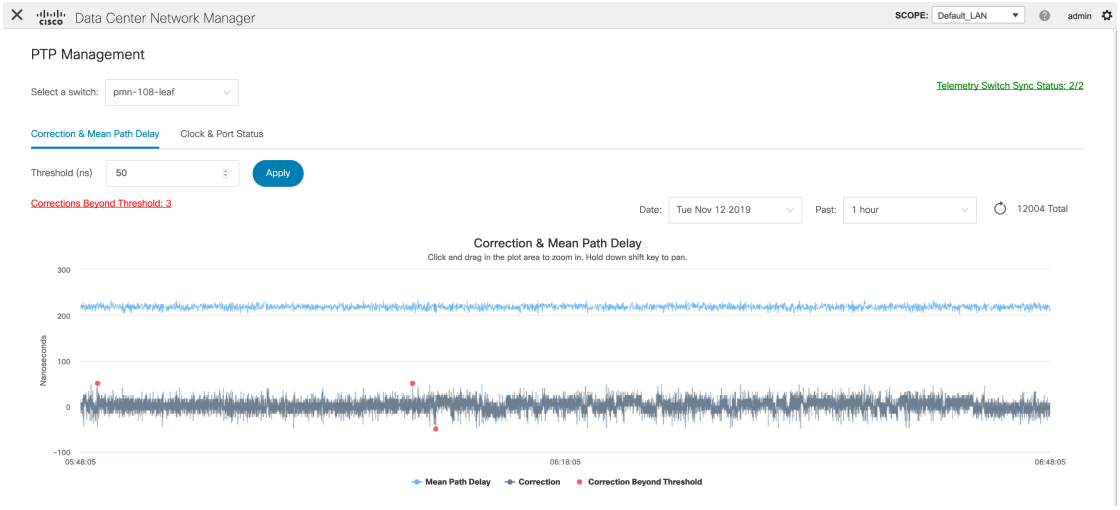
修正と平均パス遅延

[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 DCNM 設定で永続的であり、PTP 修正しきい値の AMQP 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）] ドロップダウンリストから、適切な日付を選択してデータを表示できます。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、**[管理（Administration）] > [DCNM サーバー（DCNM Server）] > [サーバー プロパティ（Server Properties）]** に移動し、**pmn.elasticsearch.history.days** プロパティの値を更新します。

[過去（Past）] ドロップダウンリストから、データを表示する期間を選択することもできます。**[過去（Past）]** ドロップダウンリストの値は、1、6、12、および 24 時間です。

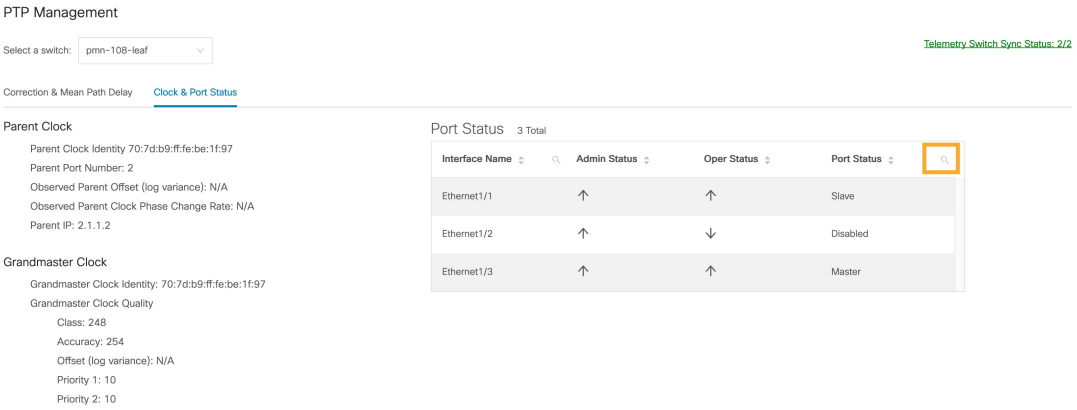


グラフの凡例をクリックすると、統計情報の表示/非表示を切り替えることができます。

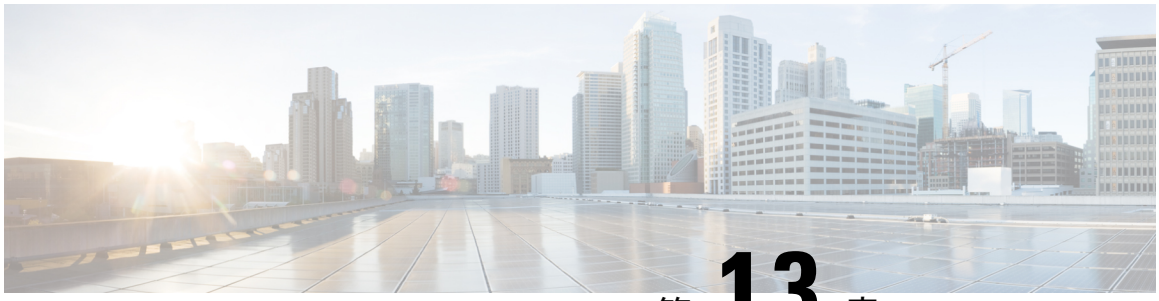
修正がある場合は、**[しきい値を超えて修正（Corrections Beyond Threshold）]** リンクをクリックして、表形式で修正を表示できます。

クロックとポートのステータス

[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、ポートとピア ポートのステータスが表示されます。**[検索（Search）]** アイコンをクリックしてポート ステータスを入力し、**[検索（Search）]** をクリックしてポート ステータスをフィルタリングします。



第 13 章

プログラム可能レポート

カタログ

カタログを使用すると、Cisco DCNM でインストールまたは有効にしたすべてのアプリケーションを表示できます。Cisco DCNM をインストールすると、ほとんどのアプリケーションはインストールされず、デフォルトで動作します。

Cisco DCNM 展開に基づいて、次のアプリケーションが表示されます。

- Health Monitor (2.1)
- PTP Monitoring (1.1)
- Kibana (2.0)
- Programmable report (1.1.0)
- Elastic Service (1.1)
- Compliance (4.0.0)
- Debug Tools (2.1)
- IPAM Integrator (1.0)
- Endpoint Locator (2.1)
- Kubernetes Visualizer (1.1)
- vmmplugin (4.1)

Note デフォルトで起動されたアプリケーション、または DCNM にインストールされたインフラストラクチャ サービスを使用するアプリケーションは、デフォルトで動作します。

Web UI を介して App Center から追加のアプリケーションをインストールできます。

Cisco DCNM Web UI からのアプリケーションのダウンロード、追加、起動、停止、および削除の手順については、アプリケーションのインストールと展開, on page 660 を参照してください。

プログラム可能レポート

プログラム可能レポート 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。

レポート テンプレート タイプは、プログラム可能なレポート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、[アップグレード（UPGRADE）] と [汎用（GENERIC）] の 2 つのテンプレート サブタイプがあります。レポート テンプレートの詳細は、「レポート テンプレート」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 DCNM にバンドルされており、レポートを生成するための API を提供します。API の詳細については、「レポート Python ライブラリ」を参照してください。

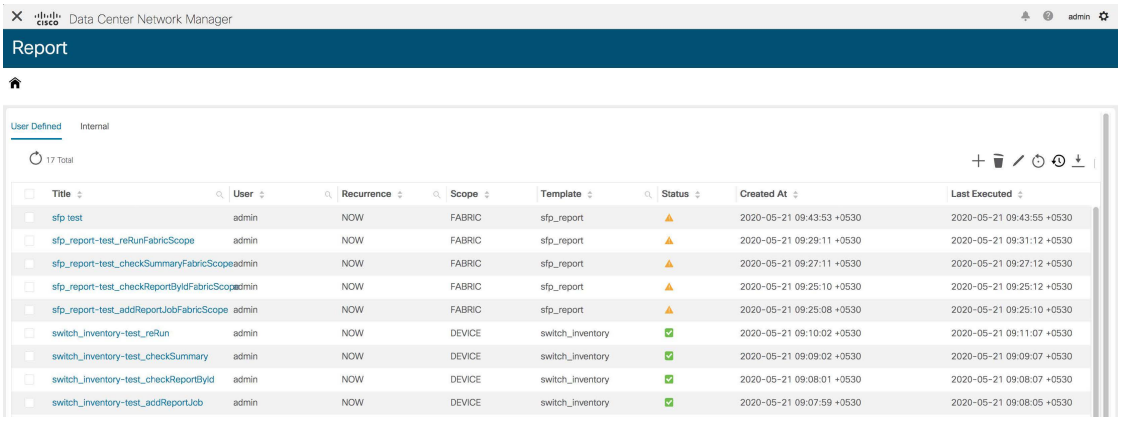
RBAC サポート

- 管理者またはネットワーク オペレータは、レポートを作成できます。
- ネットワーク オペレータは、他の管理者やオペレータによって作成されたレポートを表示できます。
- ネットワーク オペレータは、管理者や他のネットワーク オペレータによって作成されたレポートを削除/編集/再実行することはできません。
- 管理者は、レポートを作成したユーザーに関係なく、レポートを表示および削除できます。
- ファブリックとデバイスの関連付けにより、管理者はネットワーク オペレータを含む他のユーザーが作成したレポートを編集できません。

（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。

プログラム可能レポート アプリを起動するには、Cisco DCNM Web UI で、**[アプリケーション（Applications）]** を選択します。**[カタログ（Catalog）]** タブで、**[プログラム可能レポート（Programmable report）]** をクリックしてアプリケーションを起動します。[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、**[ユーザー定義（User Defined）]** と **[内部（Internal）]** の 2 つのタブがあります。**[ユーザー定義（User Defined）]** タブでは、ユーザーによって作成されるレポートジョブが表示されます。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。レポートジョブの作成（728 ページ） どのウィンドウでも、画面の左上にある **[ホーム（Home）]** アイコンをクリックして、この**[レポート**

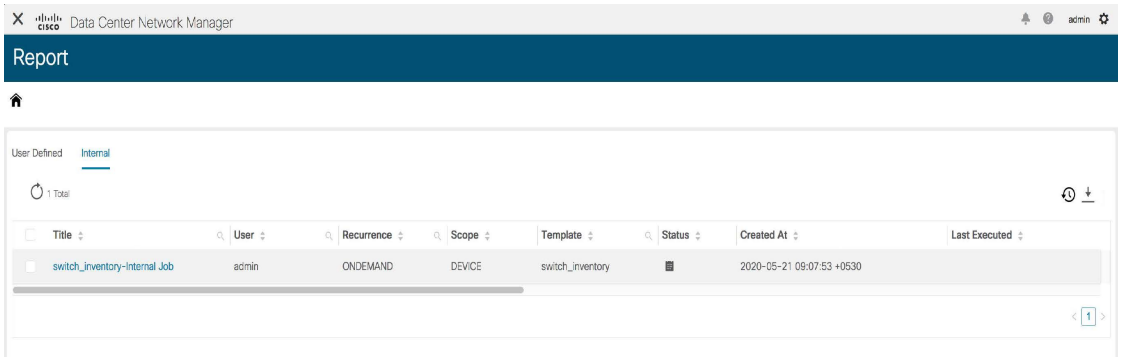
（**Report**）] ウィンドウに戻ります。このタブに表示されるジョブは、レポート ジョブ情報の作成、削除、編集、再実行、履歴の表示、ダウンロードなどのすべての操作がサポートされています。



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。
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。
範囲	レポートの範囲を指定します。レポートはデバイスまたはファブリックに生成可能です。
テンプレート	テンプレート名を指定します。
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 メッセージが以下の通りです。 *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。17-10-2022 11:19 *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。
作成時刻	アラームが作成された時刻を指定します。
最終実行	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
開始日	レポート生成を開始する予定の日付を指定します。
終了日	レポート生成の終了予定日を指定します。

[内部（Internal）] タブには、DCNM によって作成されたレポート ジョブが表示されます。たとえば、[ISSU] ウィザードによって作成された Pre-ISSU レポート ジョブと Post-ISSU レポート ジョブは内部ジョブと見なされます。ただし、このタブではレポート ジョブの情報とレポート ジョブの履歴のみを表示できます。このレポートに依存する DCNM 機能の動作に影響を与える可能性があるため、このタブに表示されているレポート ジョブを削除することはできません。



また、Cisco DCNM でプログラム可能レポート アプリケーションを使用する方法を示すビデオを見ることもできます。「プログラム可能レポート」を参照してください。

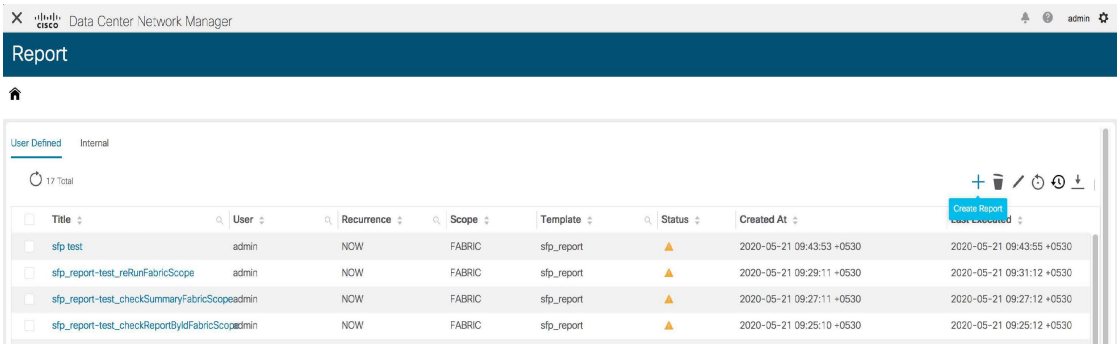
レポート ジョブの作成

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

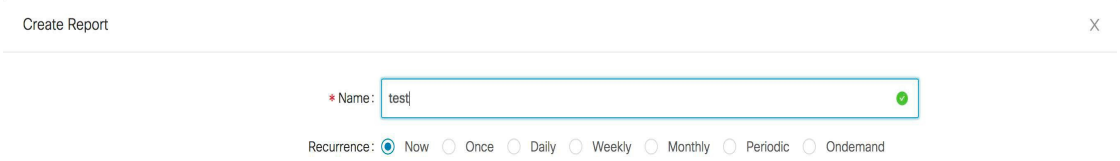
ステップ 1 **[レポートの作成（Create Report）]** アイコンをクリックします。

[レポートの作成（Create Report）] ウィンドウが表示されます。



ステップ 2 **[名前（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 3 [繰り返し（Recurrence）] の横にある必要なボタンを選択して、レポート ジョブを実行する頻度を指定します。このユース ケースでは、**[今すぐ（Now）]** を選択します。



繰り返しオプションは次のとおりです。

*今すぐ：レポートは直ちに生成されます

*1 回：レポートは指定された時間に 1 回生成されます。

*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。

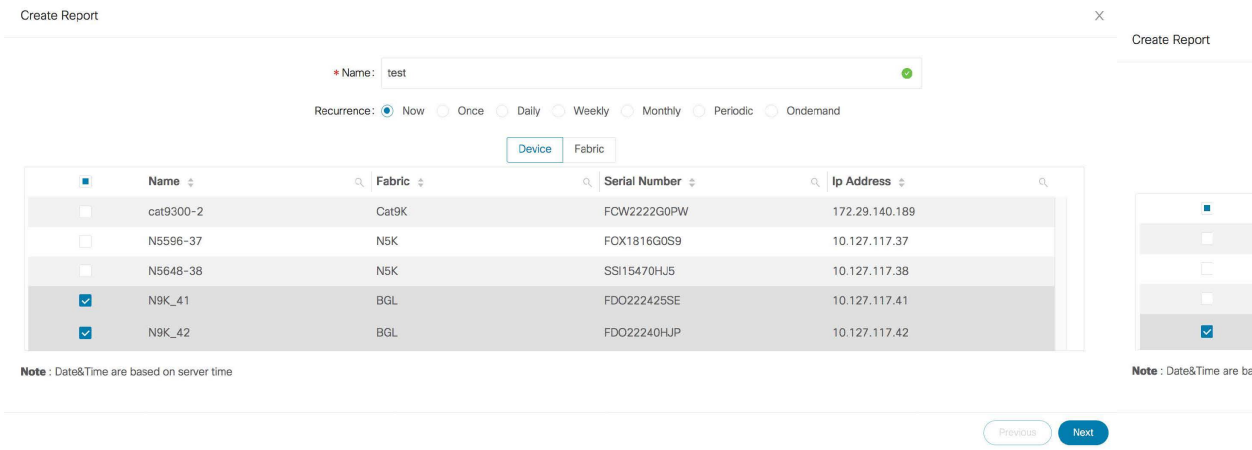
*定期的：レポートは、指定された開始日と終了日の間の期間に定期的に生成されます。レポートの間隔は、分または時間で指定できます。

（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。

*オンデマンド：レポートはオンデマンドで生成されます。このレポートは、[レポート（Report）] ウィンドウの **[再実行（Rerun）]** アイコンをクリックすることによってのみ生成できます。

（注） **開始日時**と**終了日時**は 24 時間制で表示されます。

ステップ 4 レポートを生成するためにレポート ジョブを実行するデバイスまたはファブリックを指定します。



ステップ 5 [次へ（Next）] をクリックします。**[レポートの作成（Create Report）]** ウィンドウにある **[テンプレート（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。各レポート テンプレートには、デバイスまたはファブリック タグが関連付けられています。

次の事前定義されたテンプレートを使用できます。

デバイス範囲

*switch_inventory

ファブリック範囲

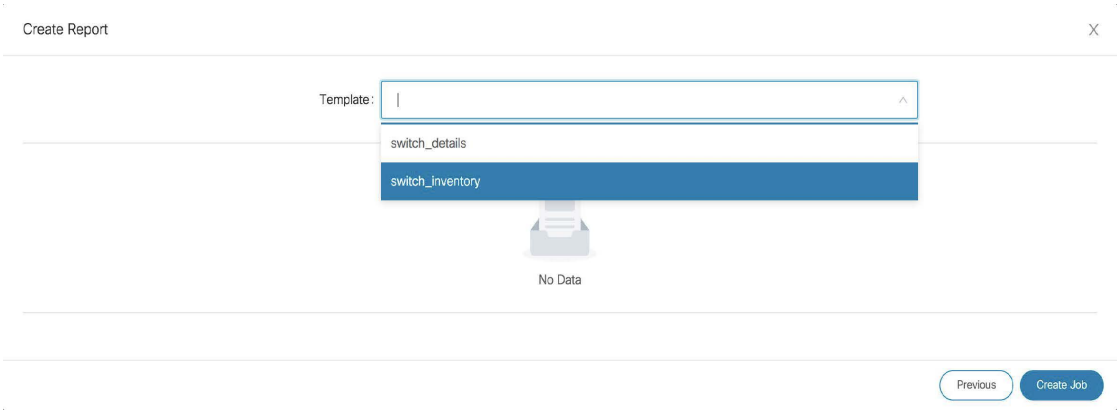
*fabric_nve_vni_counter

*fabric_resources

*sfp_report

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（Template Library）]」を参照してください。

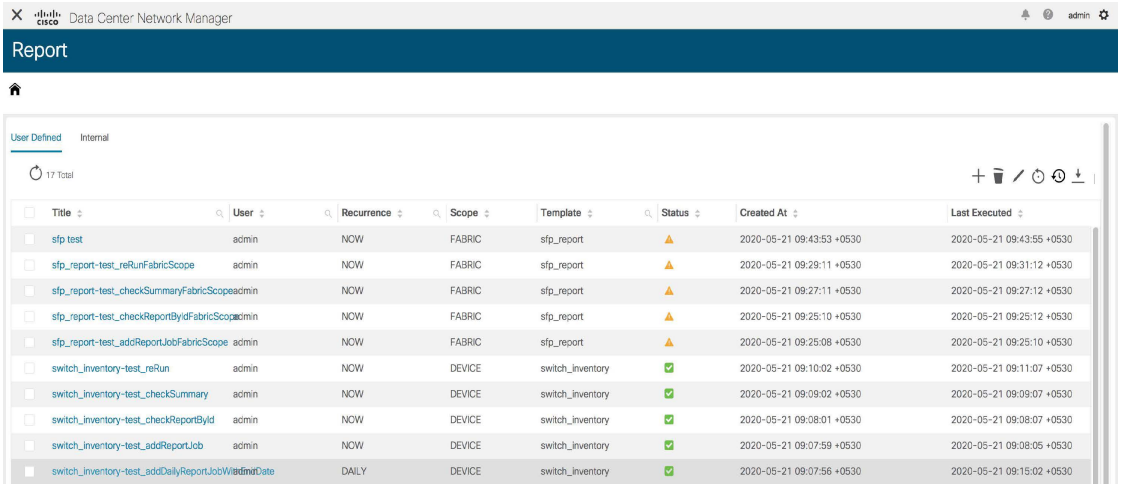
テンプレートは、関連するタグに基づいてリストされます。**[デバイス（Device）]** 範囲を選択すると、デバイス タグを持つテンプレートがドロップダウン リストに表示されます。**[ファブリック（Fabric）]** 範囲を選択すると、ファブリック タグが付いたテンプレートがドロップダウン リストに表示されます。



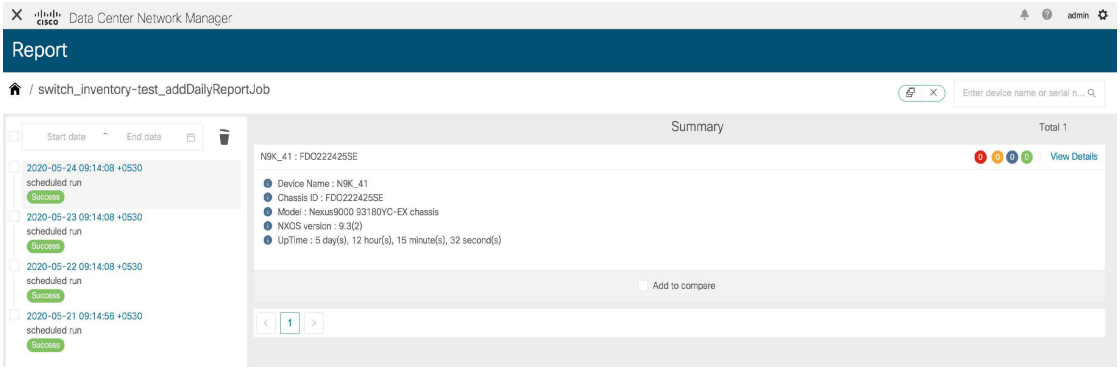
ステップ 6 **[ジョブの作成（Create Job）]** をクリックします。ジョブ レポートが正常に作成されたことを示すポップアップが表示されます。新しく作成したジョブ レポートがリストに表示されない場合は、**[更新（Refresh）]** アイコンをクリックします。新しいレポートの[ステータス（Status）]列にカーソルを合わせると、ステータスは **[実行中（Running）]** になり、レポートが現在生成されていることを示します。レポートが正常に生成されると、ステータスは**成功**を示す緑色のチェックマークに変わります。

レポート ジョブの表示

表示されたレポート ジョブのリストからレポート タイトルをクリックして、必要な情報を表示します。



[レポート（Reports）] ウィンドウが表示されます。このウィンドウに色分けされて表示されるエラー、警告、情報、および成功メッセージの数は、レポートの詳細によって異なります。エラーは赤、警告は黄色、情報は青、成功は緑で表示されます。概要は、これらの数値の生成には考慮されません。

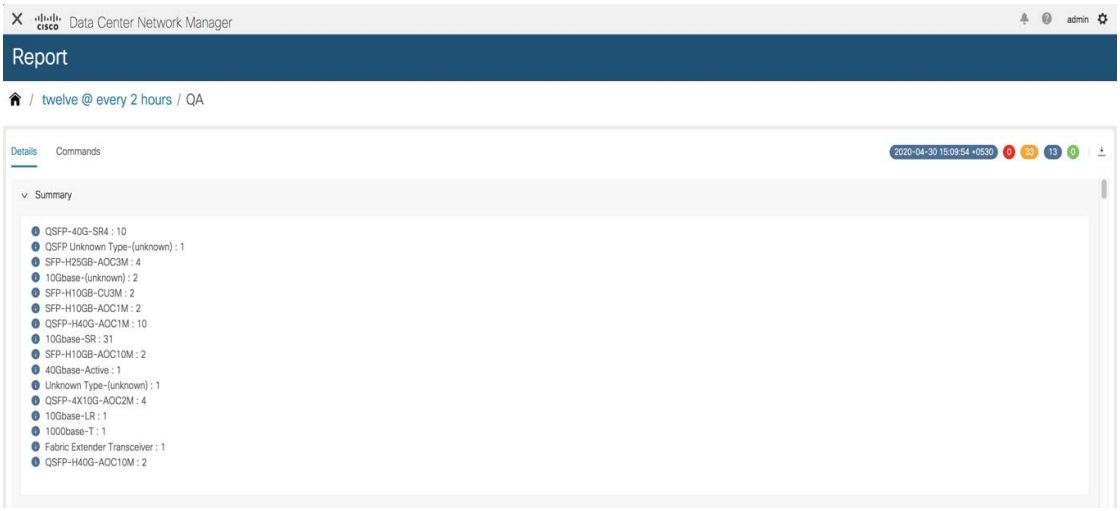


レポートは、複数のデバイスに対して生成できます。ウィンドウの左側には、レポートが生成された時刻を示すタイムラインも表示されます。このタイムラインの項目をクリックすると、その時点で生成されたレポートを表示できます。**[開始日（Start date）]**と**[終了日（End date）]**を選択して、特定の時間枠で生成されたレポートを表示することもできます。

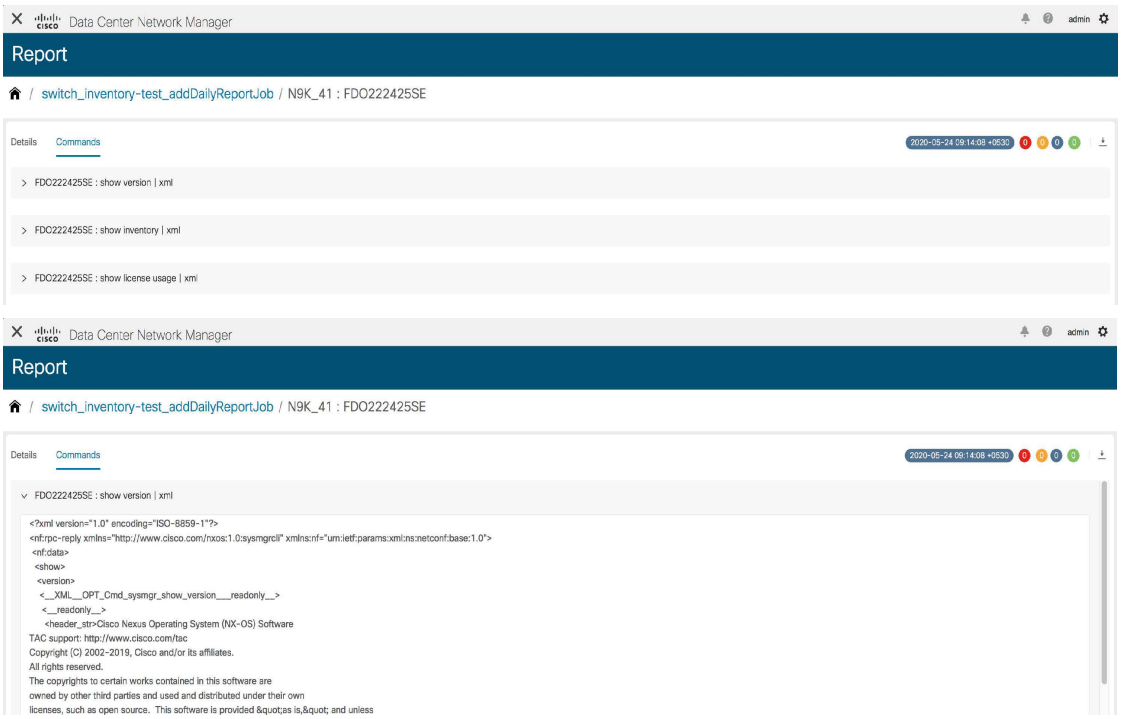
[詳細を表示（View Details）]をクリックすると、詳細な情報が表示されます。

[詳細（Details）]タブには、レポートテンプレートのタイプに基づいて、他の関連情報とともにレポートの概要が表示されます。

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。各セクションは、折りたたみ可能なウィジェットで個別に表示されます。レポートで生成されたエラー、警告、情報、および成功メッセージの数は色分けされ、ウィンドウの右上に表示されます。

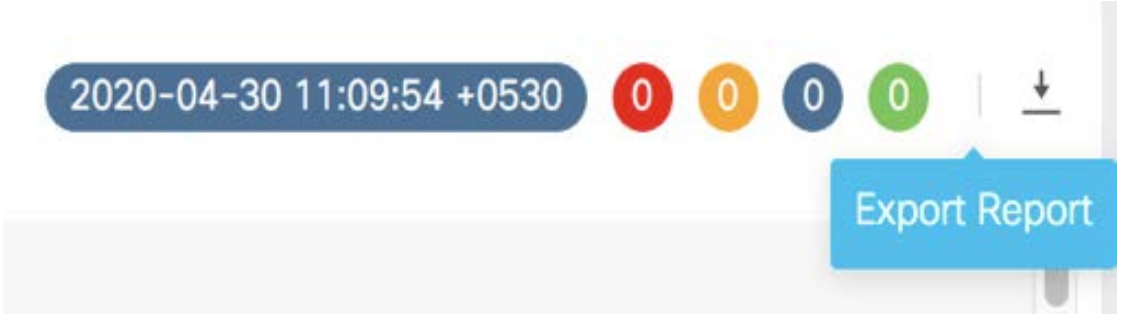


[コマンド（Commands）]タブをクリックして、レポートを生成するために実行されたコマンドを表示します。コマンドは、デバイスでコマンドを実行するために使用されるテンプレートと API に基づいて表示されます。たとえば、[switch_inventory] テンプレートでは、**show version**、**show inventory**、および **show license usage** コマンドを実行して情報を取得します。コマンドは、**show_and_store** API を使用してデバイスでコマンドを実行する場合にのみ表示されることに注意してください。

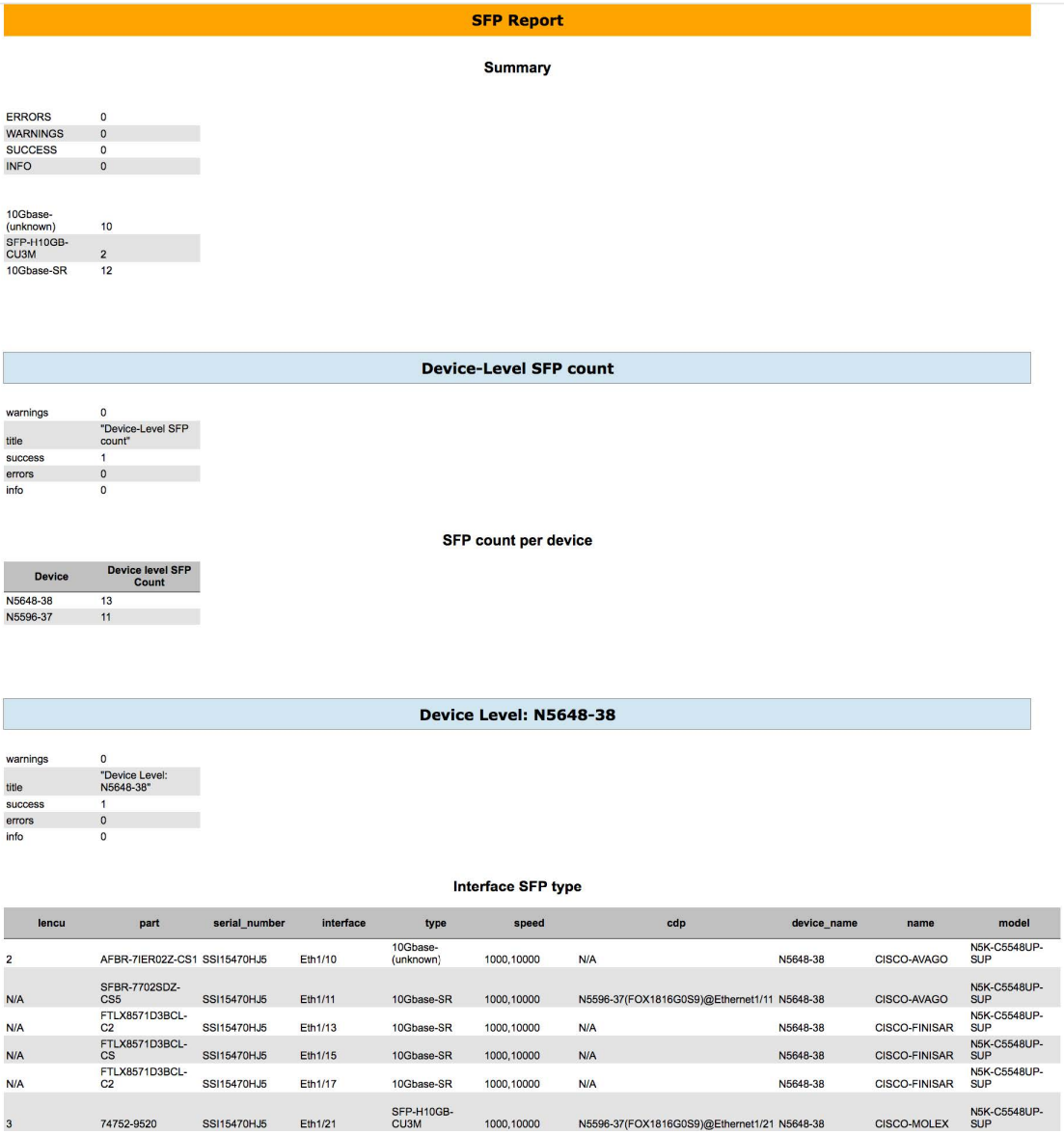


レポート情報のダウンロード

レポート情報をダウンロードするには、[詳細（Details）] タブの **[レポートのエクスポート（Export Report）]** アイコンをクリックします。出力とともにコマンドをダウンロードするには、**[コマンド（Commands）]** タブの **[レポートのエクスポート（Export Report）]** アイコンをクリックします。



レポートに関する詳細情報が別のウィンドウに表示されます。



SFP Report

Summary

ERRORS	0
WARNINGS	0
SUCCESS	0
INFO	0

10Gbase-(unknown)	10
SFP-H10GB-CU3M	2
10Gbase-SR	12

Device-Level SFP count

warnings	0
title	"Device-Level SFP count"
success	1
errors	0
info	0

SFP count per device

Device	Device level SFP Count
N5648-38	13
N5596-37	11

Device Level: N5648-38

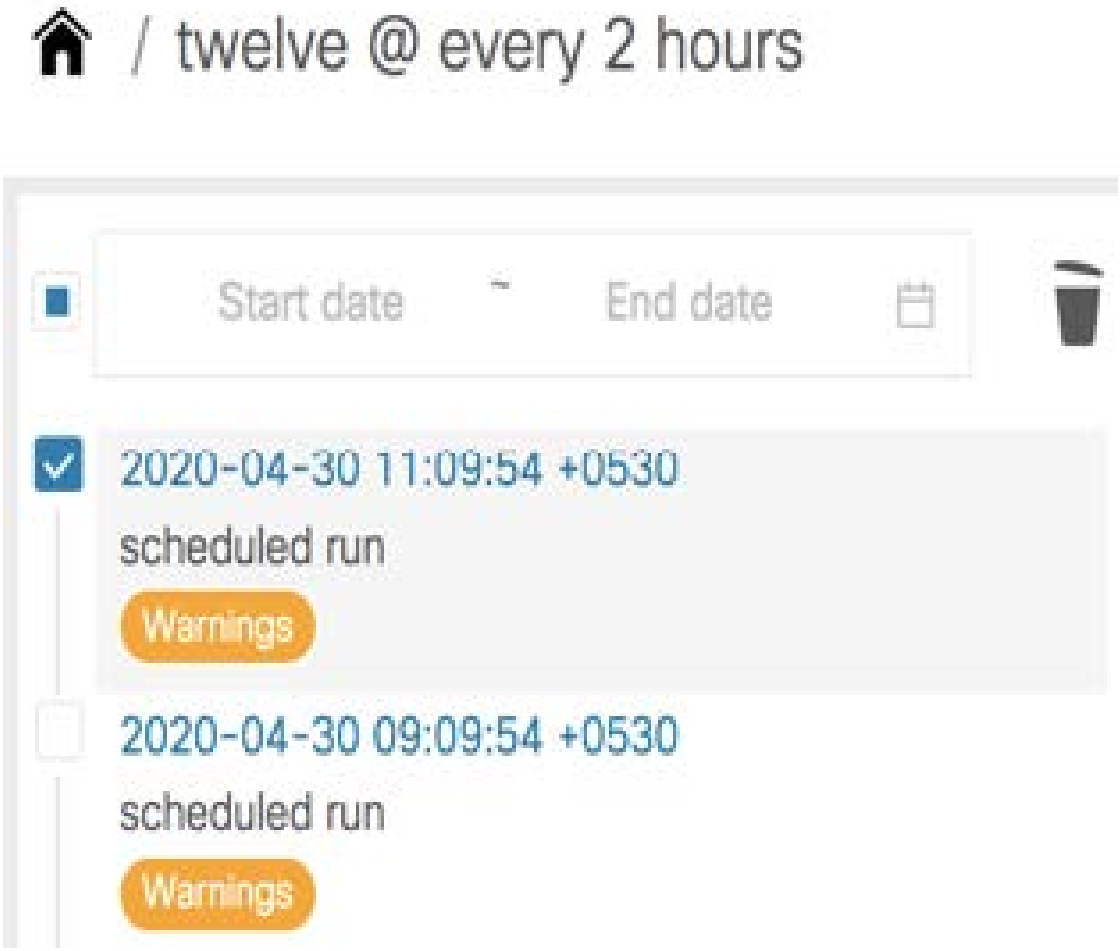
warnings	0
title	"Device Level: N5648-38"
success	1
errors	0
info	0

Interface SFP type

lencu	part	serial_number	interface	type	speed	cdp	device_name	name	model
2	AFBR-7IER02Z-CS1	SSI15470HJ5	Eth1/10	10Gbase-(unknown)	1000,10000	N/A	N5648-38	CISCO-AVAGO	N5K-C5548UP-SUP
N/A	SFBR-7702SDZ-CS5	SSI15470HJ5	Eth1/11	10Gbase-SR	1000,10000	N5596-37(FOX1816G0S9)@Ethernet1/11	N5648-38	CISCO-AVAGO	N5K-C5548UP-SUP
N/A	FTLX8571D3BCL-C2	SSI15470HJ5	Eth1/13	10Gbase-SR	1000,10000	N/A	N5648-38	CISCO-FINISAR	N5K-C5548UP-SUP
N/A	FTLX8571D3BCL-CS	SSI15470HJ5	Eth1/15	10Gbase-SR	1000,10000	N/A	N5648-38	CISCO-FINISAR	N5K-C5548UP-SUP
N/A	FTLX8571D3BCL-C2	SSI15470HJ5	Eth1/17	10Gbase-SR	1000,10000	N/A	N5648-38	CISCO-FINISAR	N5K-C5548UP-SUP
3	74752-9520	SSI15470HJ5	Eth1/21	SFP-H10GB-CU3M	1000,10000	N5596-37(FOX1816G0S9)@Ethernet1/21	N5648-38	CISCO-MOLEX	N5K-C5548UP-SUP

レポートの削除

レポートを削除するには、削除する必要があるレポート タイムラインでレポートを選択し、**[削除（Delete）]** アイコンをクリックします。



レポートの削除の確認を求めるポップアップ ウィンドウが表示されます。**[**はい（**Yes**）**]** をクリックし、レポートを削除します。

レポートの比較

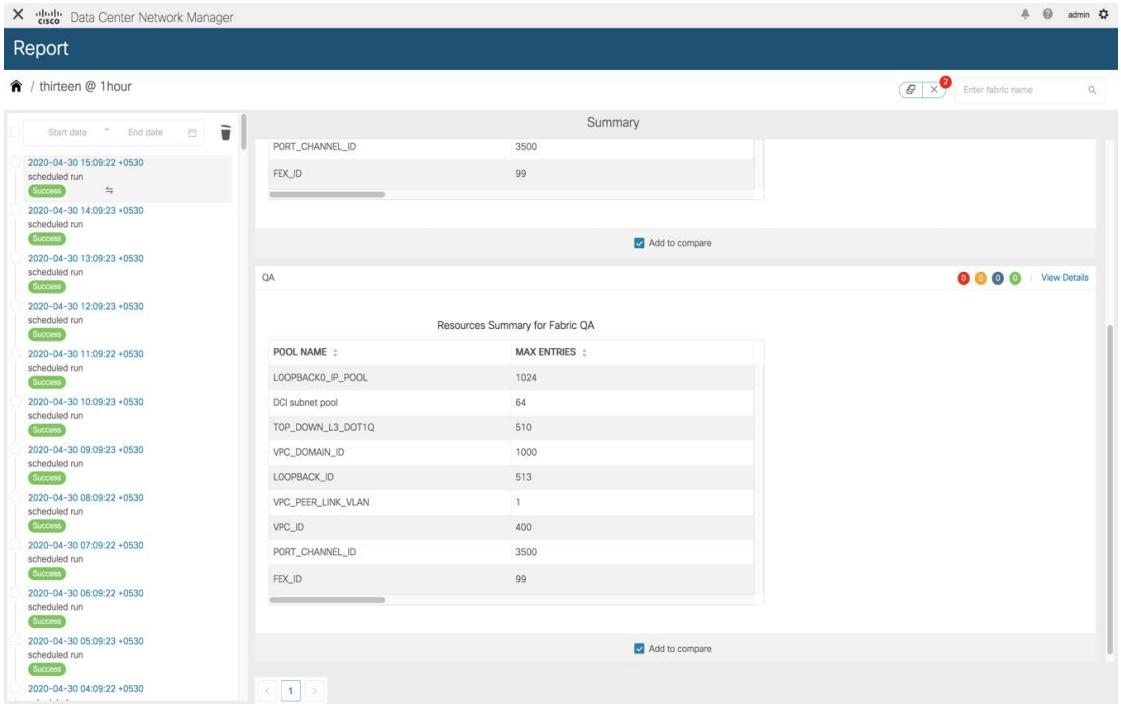
同じレポート ジョブから生成された 2 つのレポートを比較できます。

レポートを比較するには、次の手順を実行します。

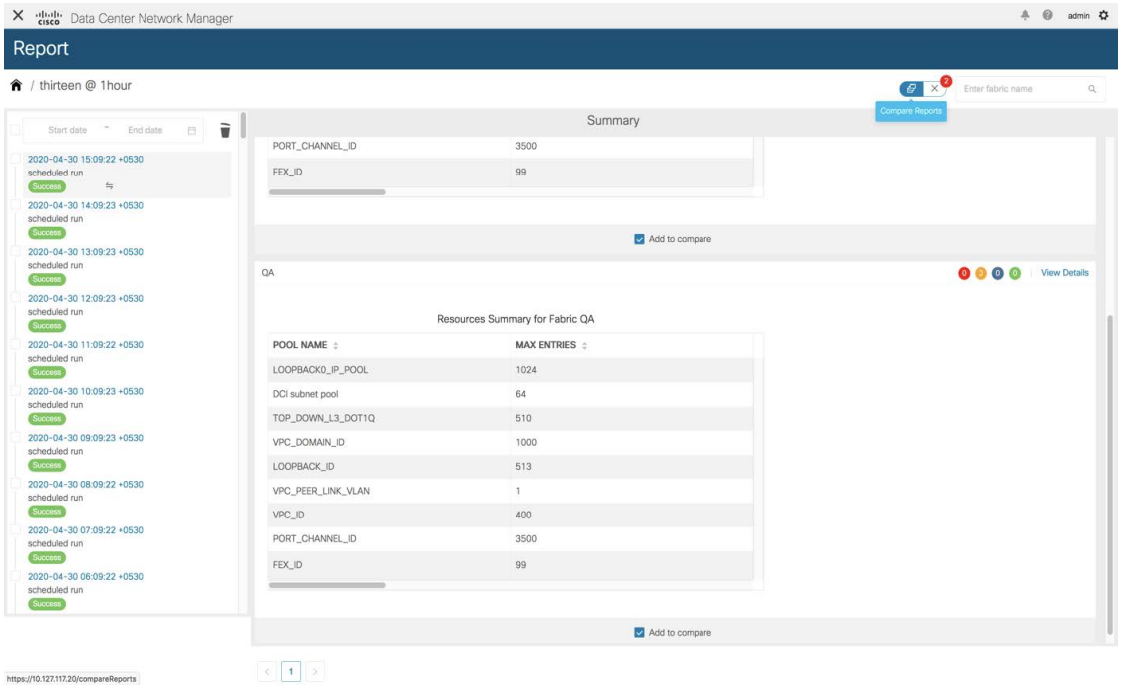
手順

ステップ 1 **[**レポート（**Report**）**]** ウィンドウで **[**比較するために追加（**Add to compare**）**]** チェックボックスを選択します。比較対象として選択されたレポートの数は、ウィンドウの右上の **X** の横にあ

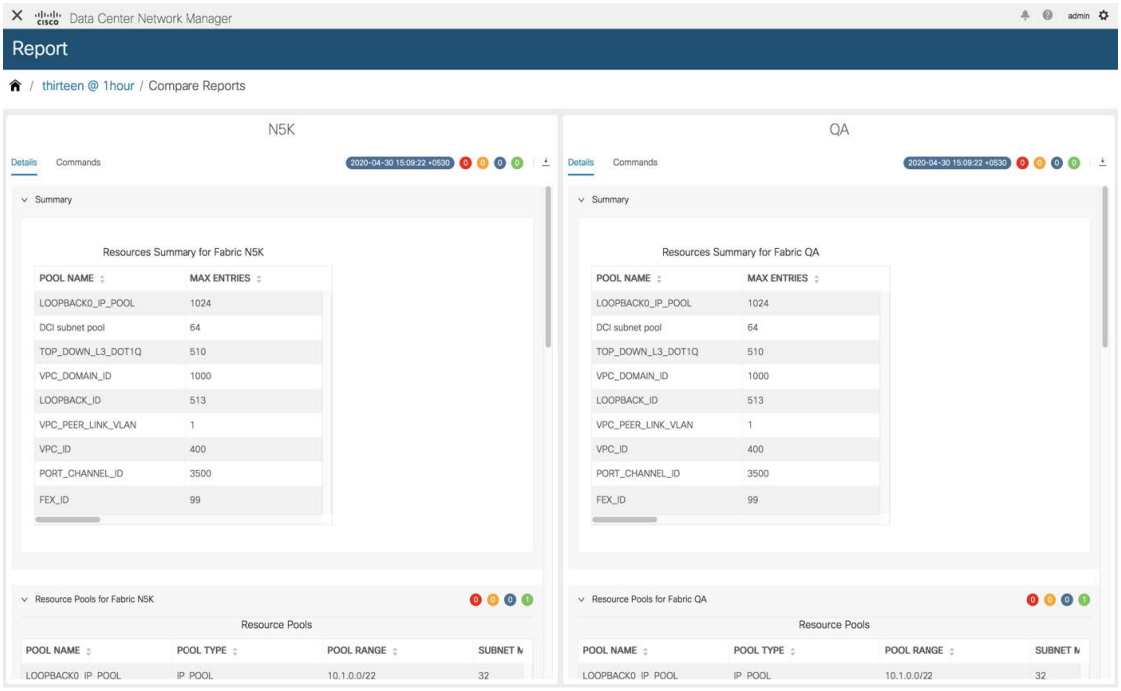
る赤い数字のアイコンで示されます。



ステップ 2 ウィンドウの右上にある **[レポートの比較（Compare Reports）]** アイコンをクリックします。

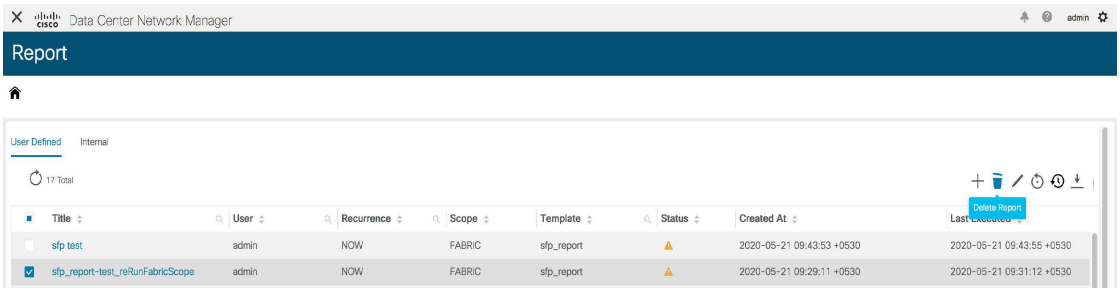


ステップ 3 **[レポートの比較（Compare Reports）]** ウィンドウが並べて比較されて表示されます。



レポート ジョブの削除

レポートジョブを削除するには、削除する必要があるレポートジョブの横にあるチェックボックスを選択し、**[レポートの削除（Delete Report）]** アイコンをクリックします。



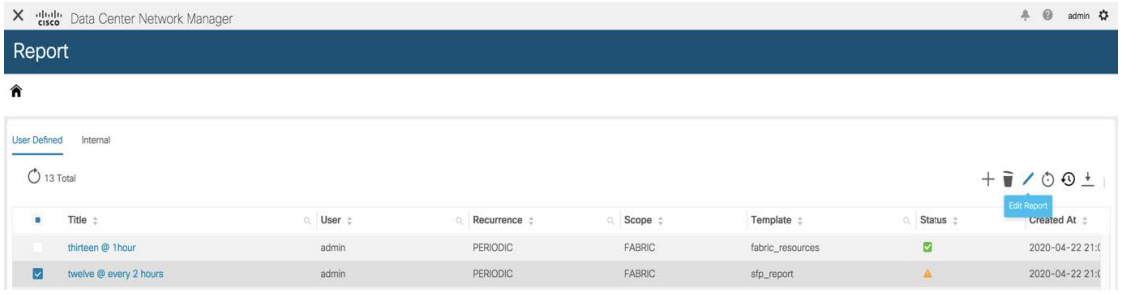
レポート ジョブを削除すると、そのレポート ジョブによって生成されたすべてのレポートも削除されます。

レポート ジョブの編集

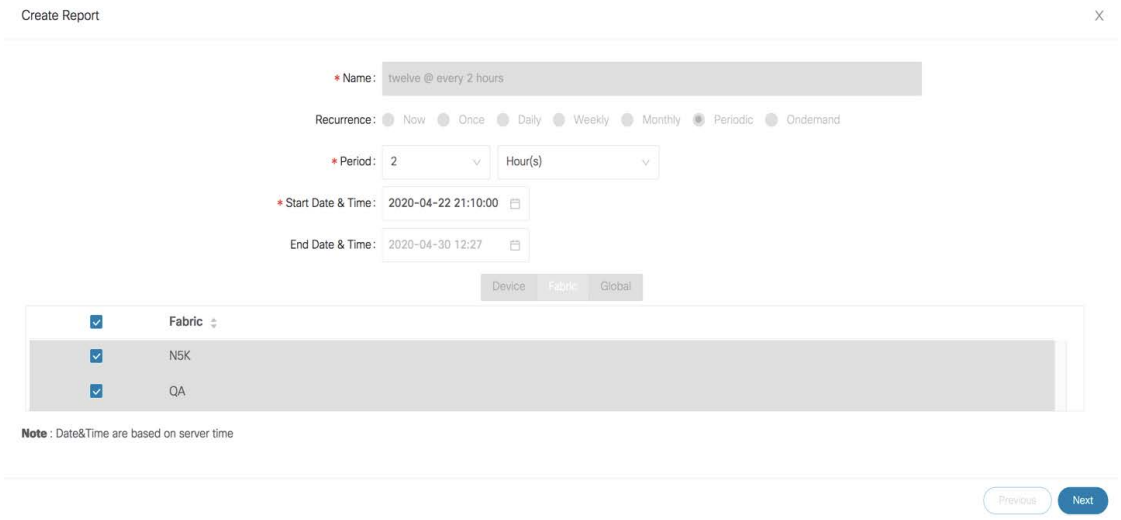
レポート ジョブを編集するには、次の手順を実行します。

手順

ステップ 1 編集したレポートの隣にあるチェックボックスを選択し、**[レポートの編集（Edit Report）]** アイコンをクリックします。同時に編集できるのは1つのジョブのみであることに注意してください。



ステップ 2 **[レポートの作成（Create Report）]** ウィンドウが表示されます。開始日時、終了日時、期間、選択したデバイスまたはファブリックを編集できます。必要なパラメータを編集したら、**[次へ（Next）]** をクリックします。

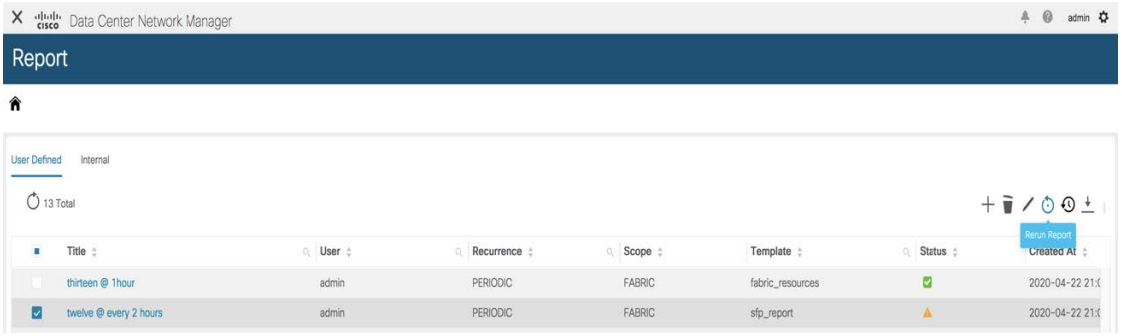


ステップ 3 **[ジョブの更新（Update Job）]** をクリックします。

レポート ジョブが更新されたことを示すポップアップ ウィンドウが正常に表示されます。

レポート ジョブの再実行

[レポート（Report）] ウィンドウで、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選択し、**[レポートの再実行（Rerun Report）]** アイコンをクリックしてレポート 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 ウィンドウが正常に表示されます。

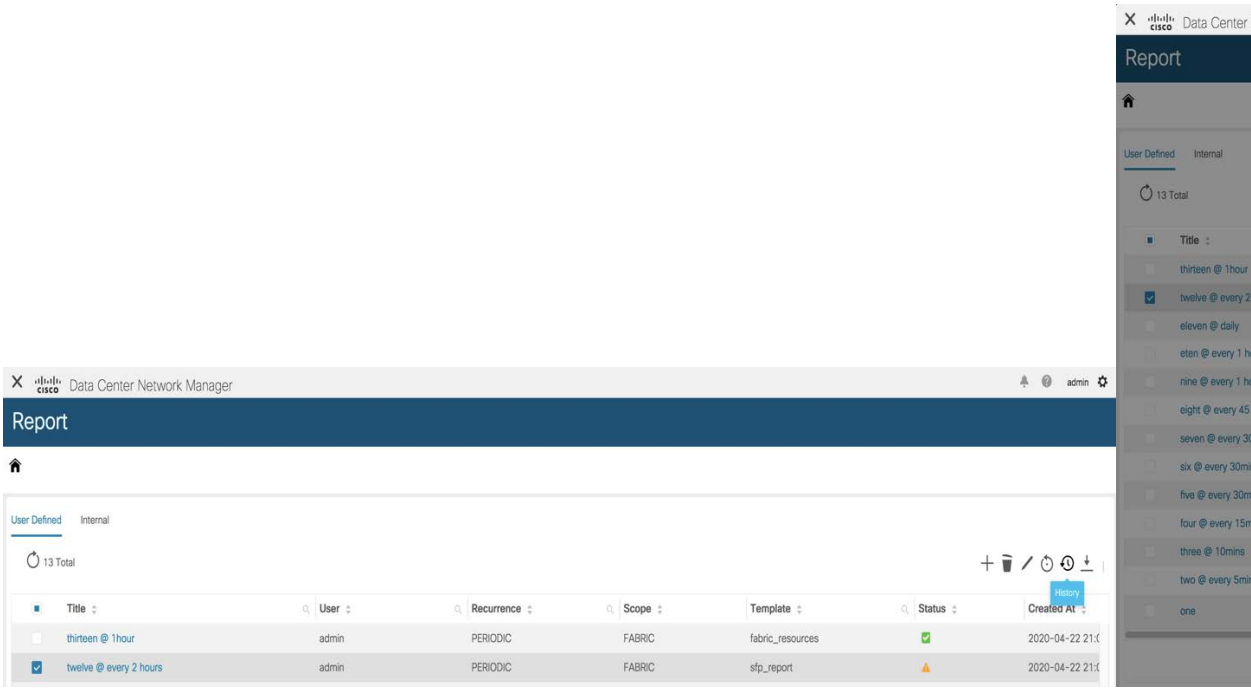


再実行オプションを使用して、スケジュールされた実行時間の前にレポートを生成できます。**[オンデマンド（Ondemand）]** ジョブの場合、**[レポートの再実行（Rerun Report）]** アイコンをクリックし、レポートを生成する必要があります。

レポート ジョブ履歴の表示

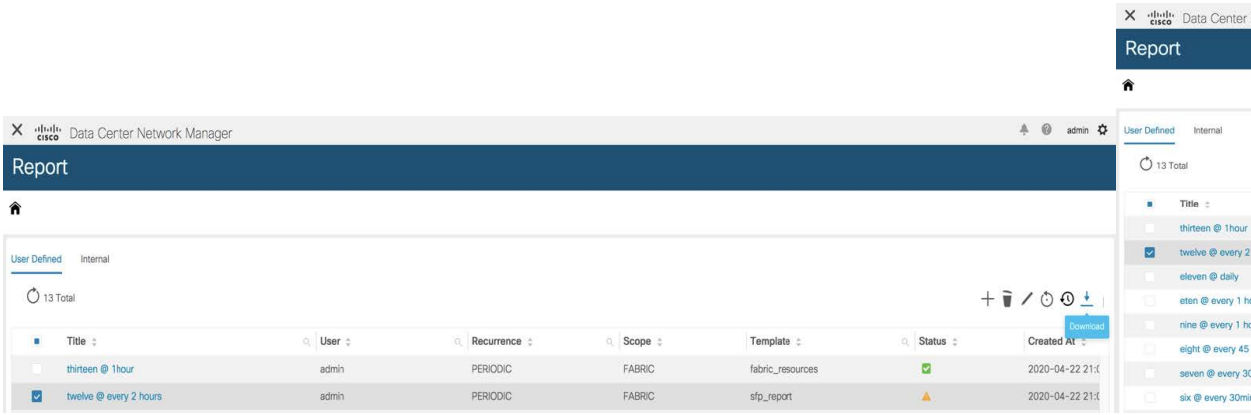
レポート ジョブの履歴を表示するには、履歴を表示する必要があるレポート ジョブの横にあるチェックボックスを選択し、**[履歴（History）]**アイコンをクリックします。**[ジョブ履歴（Job History）]** ウィンドウが表示されます。レポート ジョブごとに最新の 100 エントリを表示でき

ます。



レポート ジョブ情報のダウンロード

レポートジョブ情報を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）]** アイコンをクリックし、CSV ファイルのダウンロード先の場所を選択して、**[OK]** をクリックします。レポート ジョブに関する情報を含む CSV ファイルがダウンロードされます。



レポートの消去

レポートを消去すると、新しいレポート用のスペースが作成されます。レポートジョブごとに異なる繰り返し間隔を設定できるため、レポート ジョブごとに個別のレポート インデックスが作成されます。したがって、特定の期間に生成されるレポートの数は、レポート ジョブによって異なる場合があります。個別のレポートインデックスは、レポートを簡単に削除するのに役立ちます。各レポート インデックスには、100MB の最大サイズ制限と 500 の最大レポー

ト数があります。制限を超えると、古いレポートが削除され、新しいレポート用のスペースが確保されます。

どの時点でも、最大しきい値の 70% のみが保持されます。たとえば、レポート インデックスの最大サイズが 100MB であるシナリオを考えてみます。パージ時には、平均で最大 70MB のスペースを使用するレポートのみが保持されます。これにより、生成される新しいレポート用のスペースが提供されます。最大レポート数 500 のしきい値も 70% です。

- 制限としきい値のパーセンテージ値を変更するには、次の REST API を使用します。

  URL：*appcenter/Cisco/preport/integrated/admin/reportconfig*

  メソッド：POST

  1 つ以上のしきい値属性と値を構成できます。

```
{
<threshold attributes>: <value>
}
```

  <threshold attributes> は以下に示されています。

  MAX_REPORT_SIZE：レポート インデックスの最大サイズ（KB）

  MAX_USAGE_PERCENTAGE：保持する「MAX_REPORT_SIZE」の最大割合

  MAX_NUMBER_OF_REPORTS：レポートの最大数

  MAX_NUMBER_OF_REPORTS_PERCENTAGE：レポートの最大パーセンテージ

  保持する「MAX_NUMBER_OF_REPORTS」

  MAX_HISTORY_SIZE：KB 単位の履歴の最大サイズ

  MAX_HISTORY_PERCENTAGE：「MAX_HISTORY_SIZE」の最大保持率

  MAX_NUMBER_OF_HISTORY：保持する履歴レポートの最大数

  MAX_NUMBER_OF_HISTORY_PERCENTAGE：履歴の最大パーセンテージ

  保持する「MAX_NUMBER_OF_HISTORY」

  <*value*> 属性に整数を入力します。

- *現在構成されている制限を取得するには、次の API を使用します。

  URL：*appcenter/Cisco/preport/integrated/admin/reportconfig*

  メソッド：GET

- 現在の使用状況の統計を取得するには、次の API を使用します。

  URL：*appcenter/Cisco/preport/integrated /admin/index/stats*

  メソッド：GET

- レポートは、1 日 1 回午前 12 時にパージされます。パージを開始することもできます。パージを開始するには、次を使用します。

  REST API

URL：*appcenter/Cisco/preport/integrated/admin/purge/report*

メソッド：POST

- レポートの実行履歴は、すべてのジョブの単一のインデックスに保存され、偶数時間にパージされます。レポート実行履歴の最大インデックス制限は 1000 で、許可される最大サイズは 500MB です。これらの制限を変更するには、次の REST API を使用します。

  URL：*appcenter/Cisco/preport/integrated/admin/reportconfig*

  メソッド：POST

- レポート実行履歴の消去を開始するには、次の REST API を使用します。

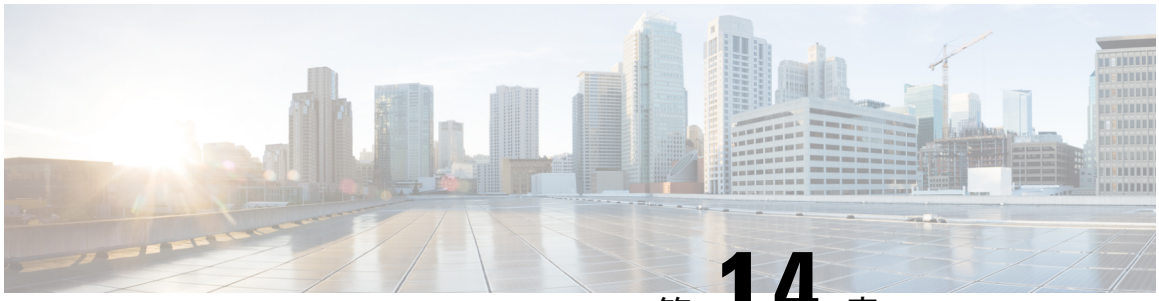
  URL： *appcenter/Cisco/preport/integrated/admin/purge/history*

  メソッド：POST

- レポートとレポート実行履歴の両方のパージを開始するには、次の REST API を使用します。

  URL：*appcenter/Cisco/preport/integrated/admin/purge*

  メソッド：POST



第 14 章

[ServiceNow 統合（ServiceNow Integration）]

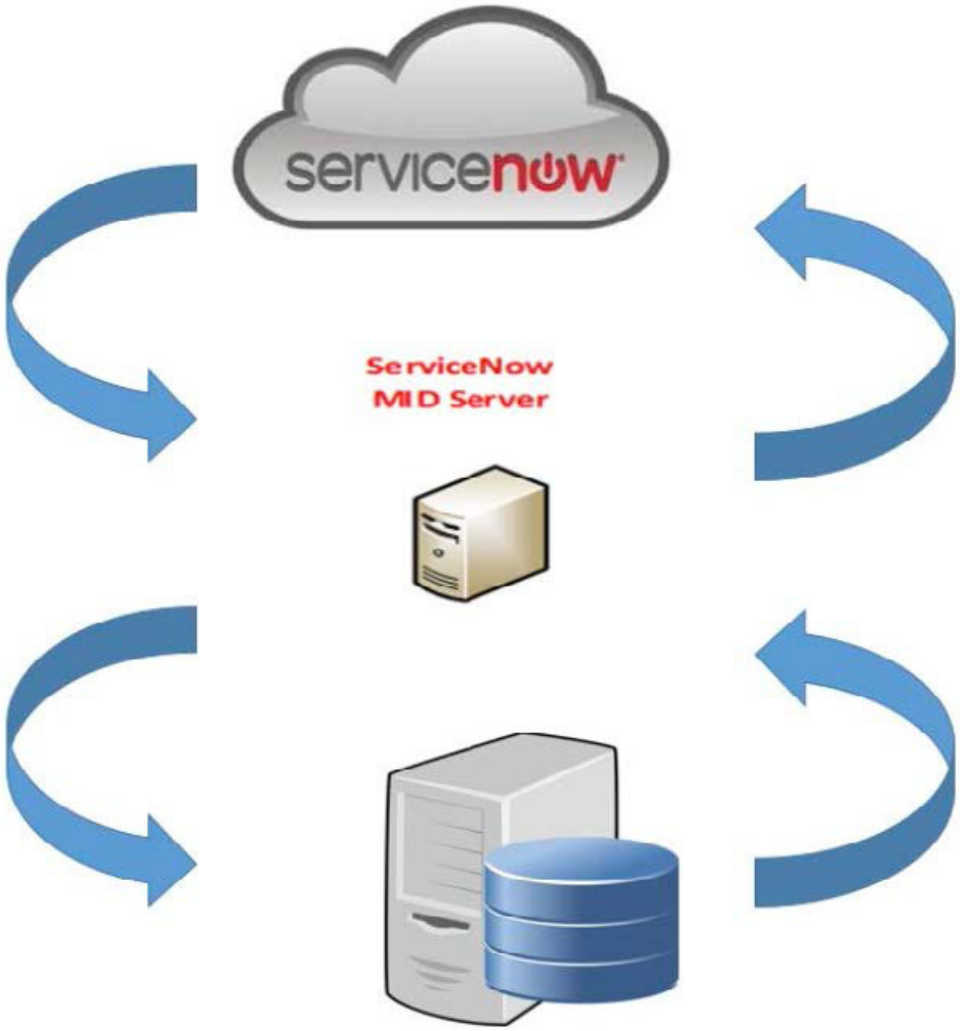
DCNM と ServiceNowの統合

ServiceNow では、IT サービス管理（ITSM）および IT 運用管理（ITOM）のアプリケーションを提供します。4 つの主要なモジュールがあります：インベントリ検出、インシデント管理、イベント管理、変更管理ワークフローです。Cisco DCNM リリース 11.3(1) 以降、Cisco DCNM と ServiceNow の統合を提供します。これにより、エンドユーザーの IT データを ServiceNow プラットフォームと統合できます。統合により、構成データが入力された ServiceNow カスタム テーブルのデフォルト セットが提供されます。

この機能を利用するには、ServiceNow カスタマー インスタンスに DCNM アプリケーションをインストールし、DCNM ミッドサーバの詳細を提供します。スイッチの詳細、ポートの詳細、アラームに関する情報またはデータは、ServiceNow 構成管理データベース（CMDB）テーブルに取得されます。デフォルトでは、データは 15 分ごとに取得され、表示されます。

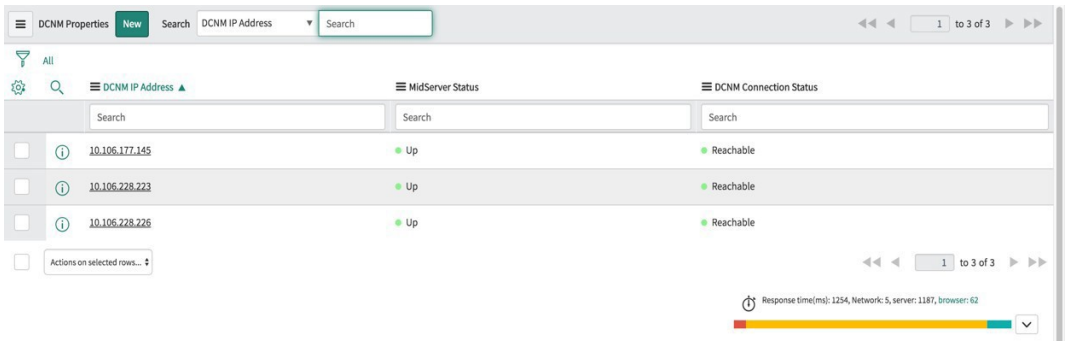
スイッチおよび各スイッチのポートに関する詳細は、DCNMインベントリから収集されます。アラームは、DCNMをポーリングすることによって収集されます。次に、アラームはフィルタリングされ、CPU、MEMORY、POWER、LINKSTATE、EXTERNAL、ICMP、SNMP、SSH などのタイプに基づいて分類されます。その後、アラームはイベントテーブルに保存されます。これらのイベントは、CPU、MEMORY、SNMP、および SSH カテゴリのインシデントを生成するために使用されます。各アラームのソース、説明、重大度、およびカテゴリが保存されます。ただし、アラームが DCNM に存在しなくなると、アラームに対して発生したインシデントは DCNM ServiceNow アプリケーションで更新またはクリアされません。アラームのポーリングが初めて開始されると、過去 7 日間に発生したアラームが DCNM から取り込まれます。

ServiceNow 上の DCNM アプリケーションは、スケジュールされたスクリプトを実行し、中間サーバに接続します。中間サーバは DCNM に接続してデータを取得します。DCNM は、要求されたデータを中間サーバに送信します。中間サーバは、そのデータを ServiceNow 上の DCNM アプリケーションに渡します。ServiceNow の DCNM インスタンスのテーブルには、この取得したデータが読み込まれます。



ServiceNow との DCNM 統合の注意事項と制限事項

- ServiceNow Cisco DCNM アプリケーション バージョン 1.0 では、1 つの MID サーバーに関する詳細のみを **[Cisco DCNM] > [プロパティ]** テーブルに追加できます。Cisco DCNM アプリケーション バージョン 1.1 以降、複数の MID サーバーを **[Cisco DCNM] > [プロパティ]** テーブルに追加できます。これは、複数の DCNM セットアップから同時にデータを取得できることを意味します。ServiceNow GUI では、各 DCNM からのデータは DCNM IP アドレスによって区別されます。

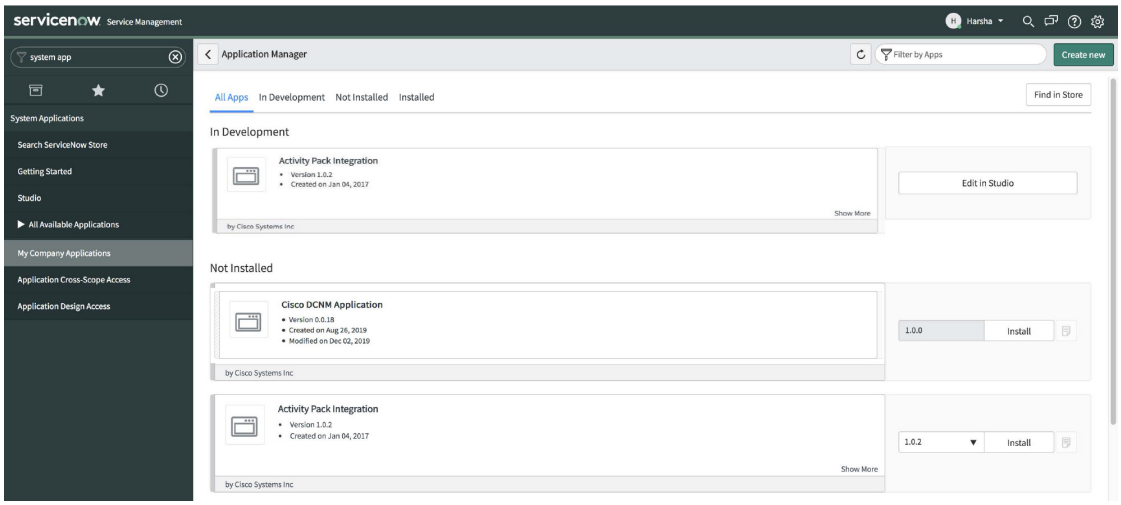


- データを取得するためにスケジュールされたスクリプトは、**[Cisco DCNM] > [プロパティ]** テーブルにサーバー レコードを挿入した後にのみ実行されます。
- **[Cisco DCNM] > [プロパティ]** テーブルの中間サーバーの IP アドレスとクレデンシャルが変更された場合、以前の中間サーバーを使用してインポートされたデータは、アプリケーション範囲テーブルから削除されます。ただし、ServiceNow CMDB（グローバル範囲）にインポートされたデータは残り、削除されません。
- ServiceNow データベースで最適なパフォーマンスを確保するために、各エントリはスイッチ データベース ID および IP アドレスと照合され、エントリが重複しないようにします。
- **[Cisco DCNM] > [プロパティ]** テーブルに新しいサーバーが追加された場合は、cmdb_ci_ip_switch テーブルのエントリを手動で削除する必要があります。

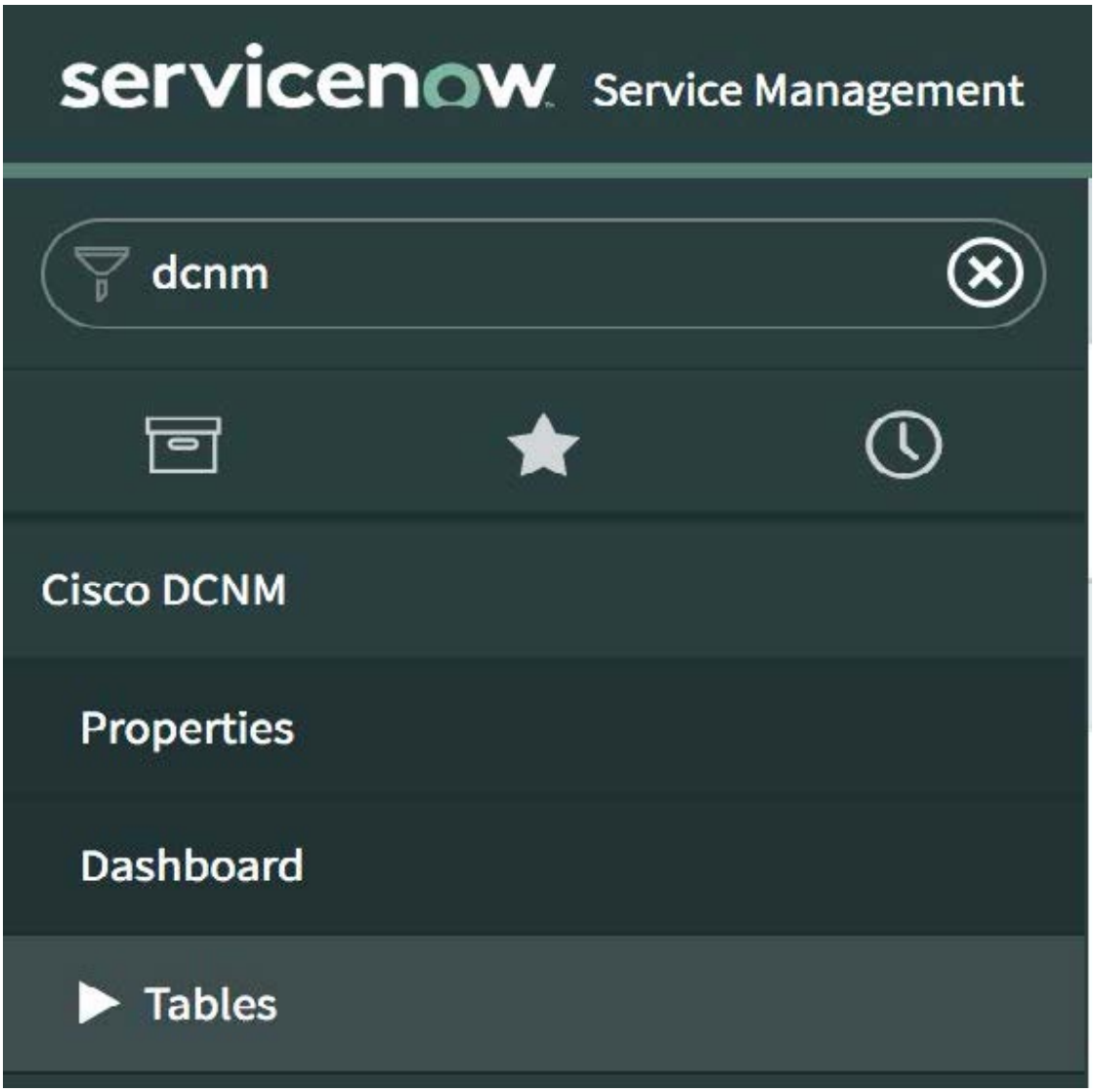
ServiceNow での Cisco DCNM アプリケーションのインストールと構成

Procedure

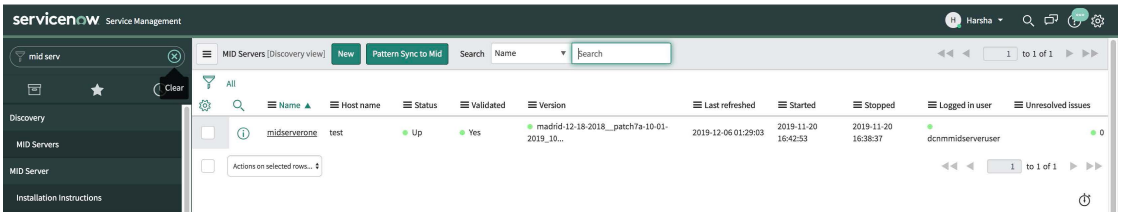
ステップ 1 https://dcnm1.service-now.com にログインします。**[システム アプリケーション（System Applications）] > [アプリケーション（Applications）]** を選択します。**[すべてのアプリケーション（All Apps）]** タブから **Cisco DCNM アプリケーション**をインストールします。



ステップ 2 インストールが完了したら、Cisco DCNM の [プロパティ（Properties）] タブと [ダッシュボード（Dashboard）] タブがアプリケーションに表示されていることを確認します。

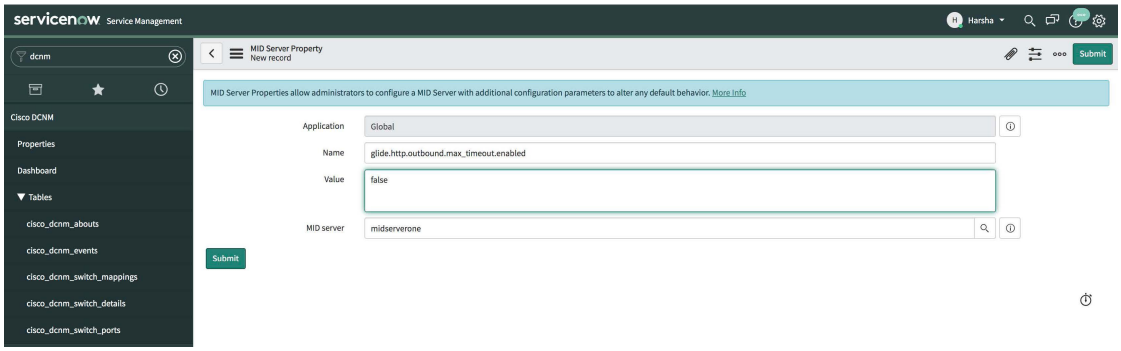


ステップ 3 **[MID サーバー（MID Servers）]** を選択し、DCNM 統合に使用される MID サーバーをクリックします。

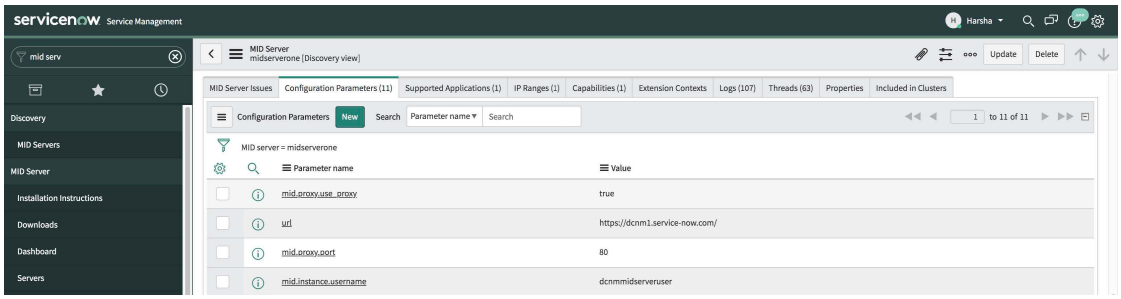


ステップ 4 下にスクロールして、**[プロパティ（Properties）]** タブをクリックします。**[新規]** をクリックし、**[MID サーバー プロパティの新規レコード（MID Server Property New record）]** ウィンドウで以下に示すプロパティを追加します。[送信（Submit）] をクリックします。

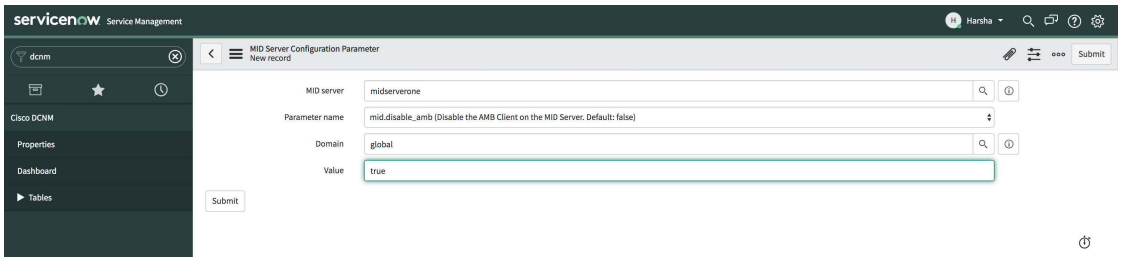
名前	タイプ	値
glide.http.outbound.max_timeout.enabled	True/false	いいえ（False）



ステップ 5　次に、**[構成パラメータ]** タブを選択します。

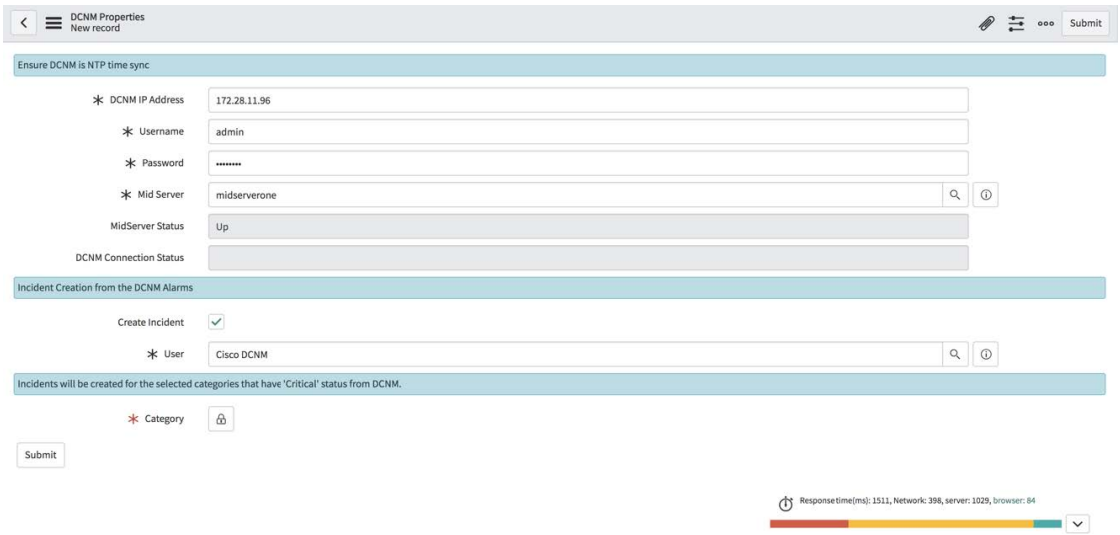


ステップ 6　**[構成パラメータ（Configuration Parameters）]** タブで、**[新規（New）]** をクリックします。フィールドに必要な詳細情報を入力します。



ステップ 7　**[送信（Submit）]** をクリックして MID サーバーを設定します。

ステップ 8　**[Cisco DCNM] > [プロパティ（Properties）]** を選択します。**[新規サーバ（New Server）]** をクリックします。必須パラメータを入力します。



DCNM IP アドレス：DCNM の IP アドレス。

ユーザー名：DCNM へのログインに使用するユーザー名を入力します。

パスワード：DCNM へのログインに使用するパスワードを入力します。

Note アクセス権は、DCNM 管理者のみに提供する必要があります。

MID サーバー：使用する MID サーバーの名前を指定します。名前は、入力時に自動的に入力されます。このフィールドの横にある検索アイコンをクリックして、[MID サーバー（MID Servers）] ウィンドウを表示することもできます。その後、表示されるリストから MID サーバーを選択できます。

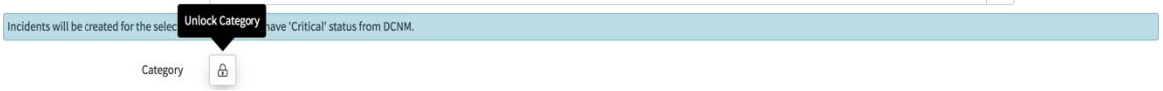
MidServer ステータス：MID サーバーが起動しているか、停止しているかを示します。

DCNM 接続ステータス：提供された DCNM IP アドレスにデータを取得できるかどうかを示します。このステータス フィールドは、必要な情報を入力した後に **[送信（Submit）]** をクリックすると入力されます。 DCNM との通信が成功した場合は **[到達可能（Reachable）]** が表示され、接続が失敗した場合は **[到達不能（Unreachable）]** と表示されます。

インシデントの作成：アラームイベントに対してインシデントを自動的に発生させる必要がある場合は、このチェックボックスを選択します。

ユーザ：新しいユーザを作成し、このフィールドにユーザ名を追加します。作成されたインシデントの [発信者（Caller）] フィールドには、このユーザ名が入力されます。このフィールドは、入力時に自動入力されます。このフィールドの横にある検索アイコンをクリックして、[ユーザ（Users）] ウィンドウを表示することもできます。表示されたリストからユーザを選択できます。

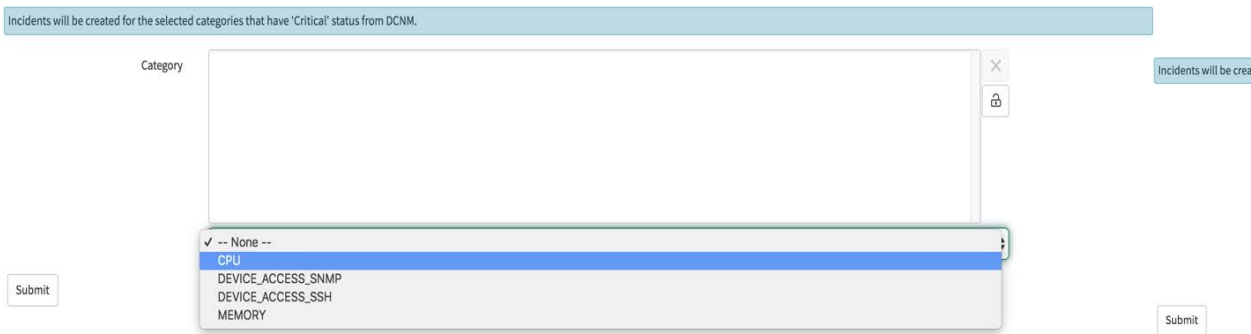
カテゴリ：ロックアイコン をクリックして、特定のカテゴリのみのインシデントを自動的に作成します。



[カテゴリ（Category）] ウィンドウの下にあるドロップダウンリストから、インシデントを作成する必要がある必要なカテゴリを選択します。インシデントの作成に使用できるカテゴリは、CPU、DEVICE_ACCESS_SNMP、DEVICE_ACCESS_SSH、および MEMORY です。詳細については、次の表を参照してください。

Table 27: イベントおよびインシデント

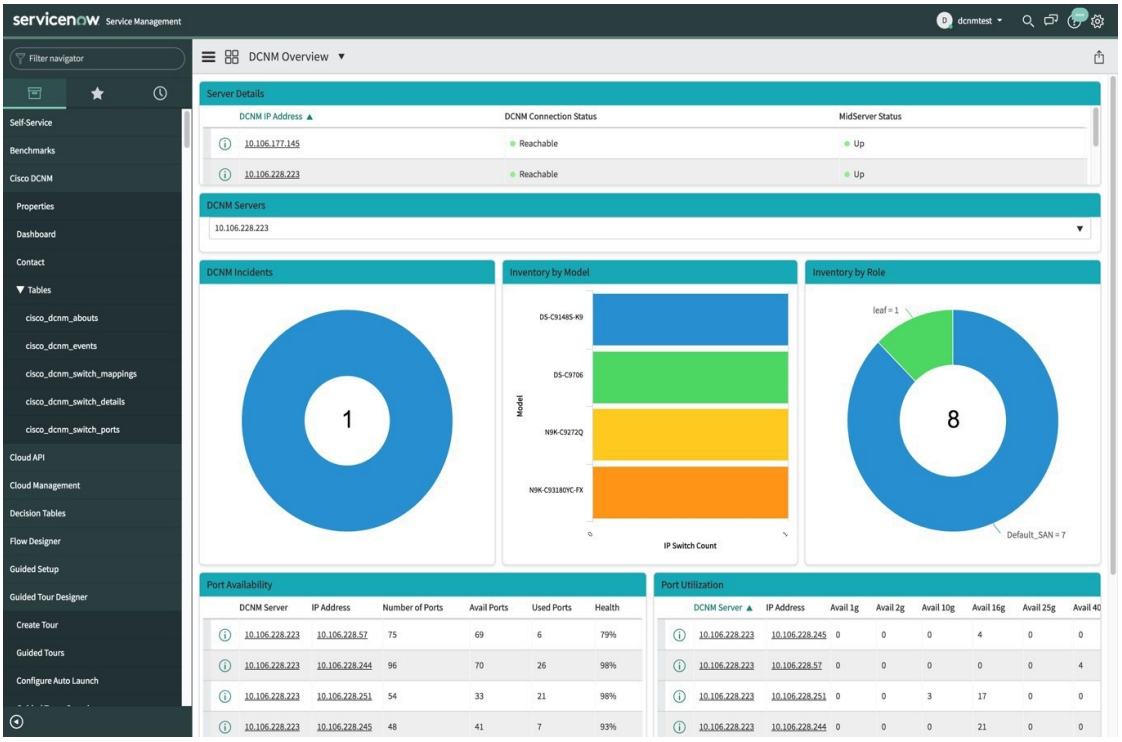
Category	ServiceNow でのデータ収集	発生したインシデント	インシデントルール	ServiceNow インシデントの詳細
CPU	はい	はい	DCNM アラーム重大度＝「クリティカル」	優先順位＝2 緊急性＝2 影響度＝2
メモリー	はい	はい	DCNM アラーム重大度＝「クリティカル」	優先順位＝2 緊急性＝2 影響度＝2
電源	はい	いいえ	該当なし	該当なし
リンクステート	はい	いいえ	該当なし	該当なし
ICMP	はい	いいえ	該当なし	該当なし
SNMP	はい	はい	DCNM アラーム重大度＝「クリティカル」	優先順位＝2 緊急性＝2 影響度＝2
SSH	はい	はい	DCNM アラーム重大度＝「クリティカル」	優先順位＝2 緊急性＝2 影響度＝2



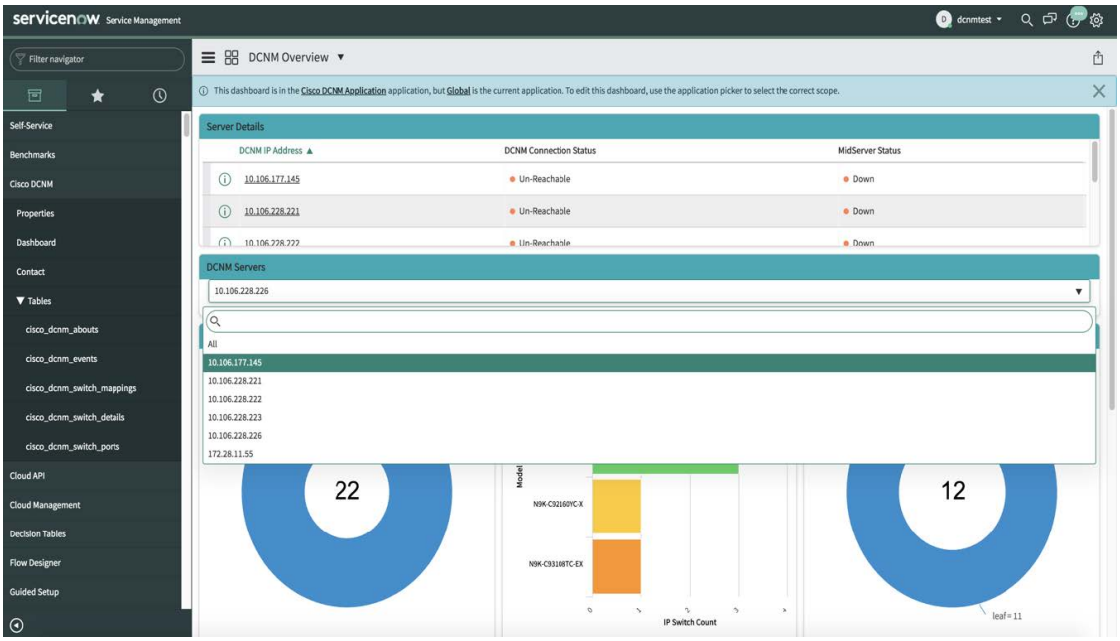
ここで、**[Submit（送信）]** をクリックします。

ダッシュボードの表示

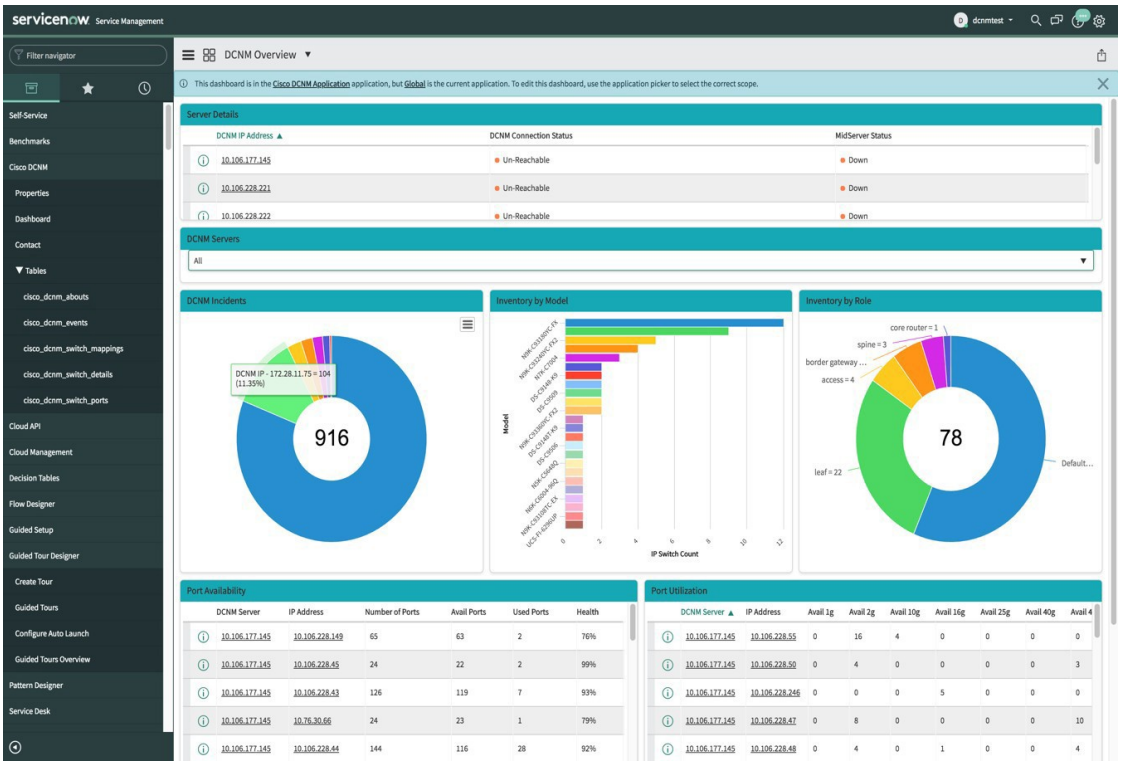
[Cisco DCNM] > [Dashboard（ダッシュボード）] を選択して、ダッシュボードを表示します。**DCNM IP アドレス**、**DCNM 接続ステータス**、および**MidServer ステータス**がダッシュボードの上部に表示されます。



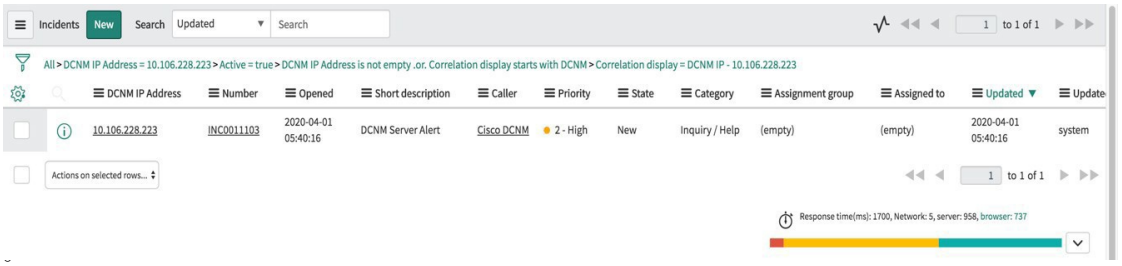
[DCNM サーバー] セクションには、データが取得および表示される DCNM サーバの IP アドレスが表示されます。ドロップダウン リストをクリックして、要件に応じて他の DCNM サーバを選択します。



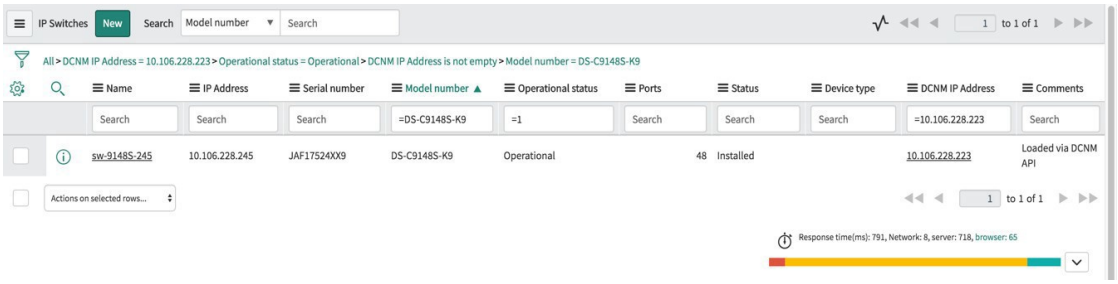
[すべて（All）] をクリックして、ドロップダウン リストに表示されているすべての DCNM サーバーからデータを取得して表示します。**[すべて]** オプションを選択すると、DCNM インシデント ドーナツに表示されるインシデントの数が色分けされ、さまざまな DCNM サーバーの IP アドレスに基づいて表示されます。[モデル別インベントリ（Inventory by Model）] ドーナツおよび [ロール別インベントリ（Inventory by Role）] ドーナツには、すべての DCNM サーバーからのデータも表示されます。ポートの可用性とポート使用率のドーナツには、各 IP アドレスが属する DCNM サーバーとともにデータが表示されます。



DCNM インシデント - これには、DCNM から取得したアラームに基づいて発生したインシデントの数が表示されます。インシデントの詳細については、ドーナツをクリックしてくださ

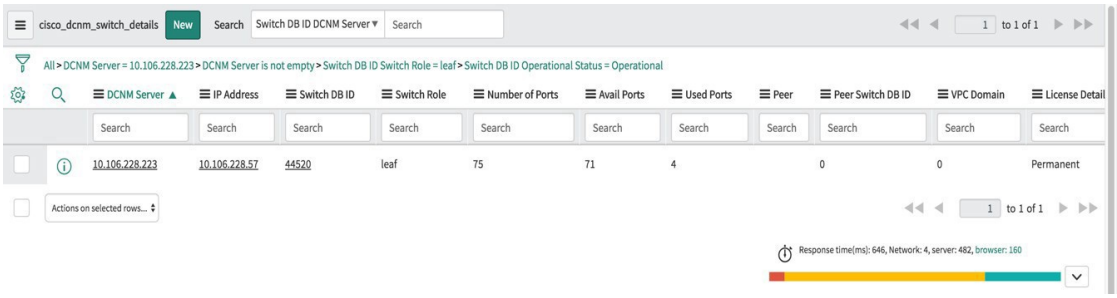


モデル別インベントリ - DCNM に存在するスイッチの数とタイプを表示します。各バンドはデバイス モデルを表します。詳細については、バンドをクリックしてください。

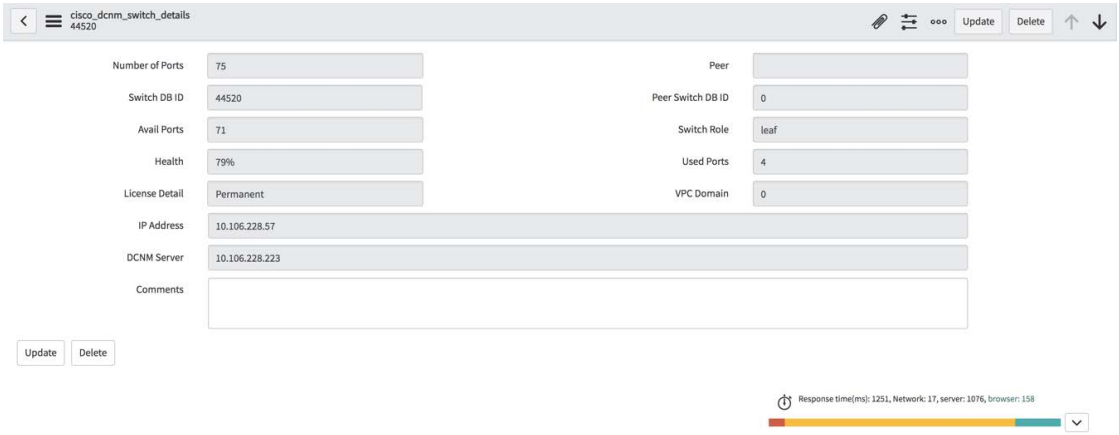


ロール別インベントリ - DCNM に存在するスイッチ ロールの数とタイプが表示されます。必要なセクションをクリックして、操作可能な役割の数を表示し、その絵図をクリックしてロールに関する詳細を表示します。

（注） [ロール別インベントリ] ドーナツに表示される数は、スイッチが DCNM から削除されても変わりません。削除されたスイッチは Non Operational として表示され、ドーナツに表示される番号に変更はありません。

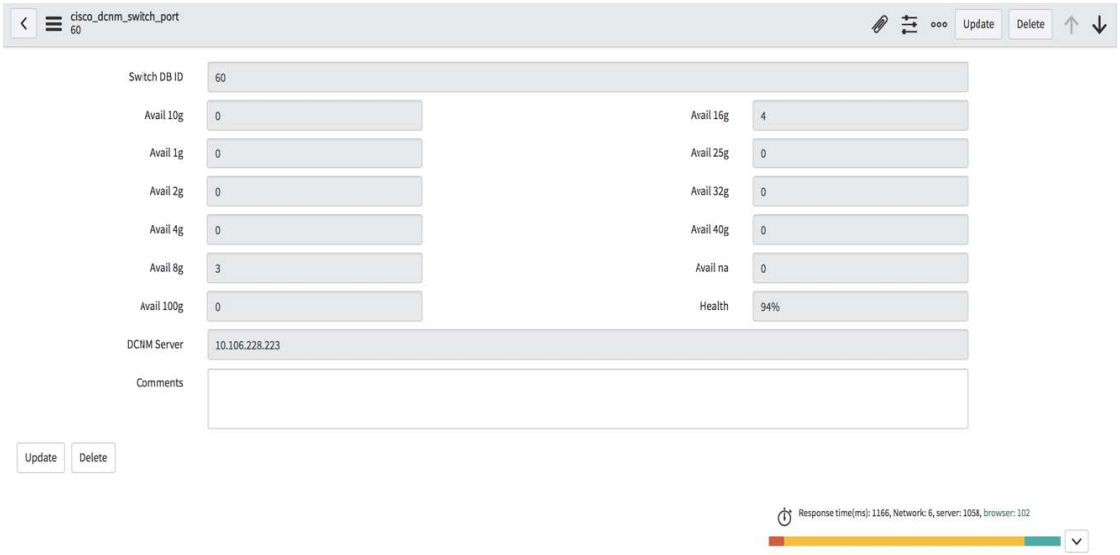


ポートの可用性 - ポートの可用性に関する情報が表示されます。ポートの総数、使用可能なポート、使用されているポート、およびスイッチのヘルスとともに、DCNM サーバーと IP アドレスが表示されます。IP アドレスをクリックすると、詳細が表示されます。



ポート使用率 - これは、各 IP アドレスに基づいたポート使用率に関する情報を表示します。1G、2G、4G、8G、10G、16G、25G、32G、40G、100Gのポート数が表示されます。IPアドレ

スをクリックすると、詳細が表示されます。



お問い合わせ

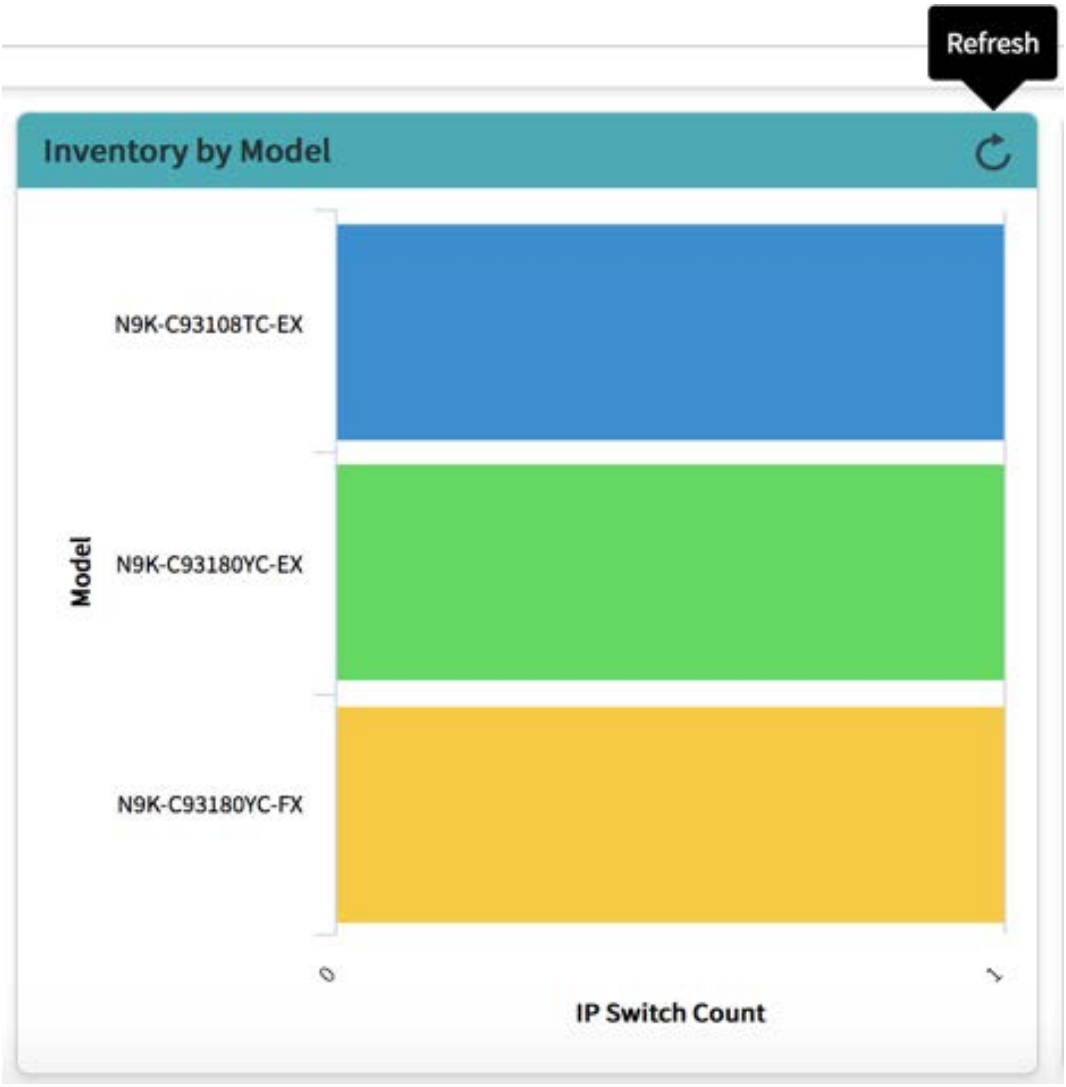
[Cisco DCNM] > [連絡先（Contact）] を選択して、問い合わせについてシスコ システムズに連絡するために使用できる電子メール アドレスと電話番号を表示します。

ServiceNow との DCNM 統合のトラブルシューティング

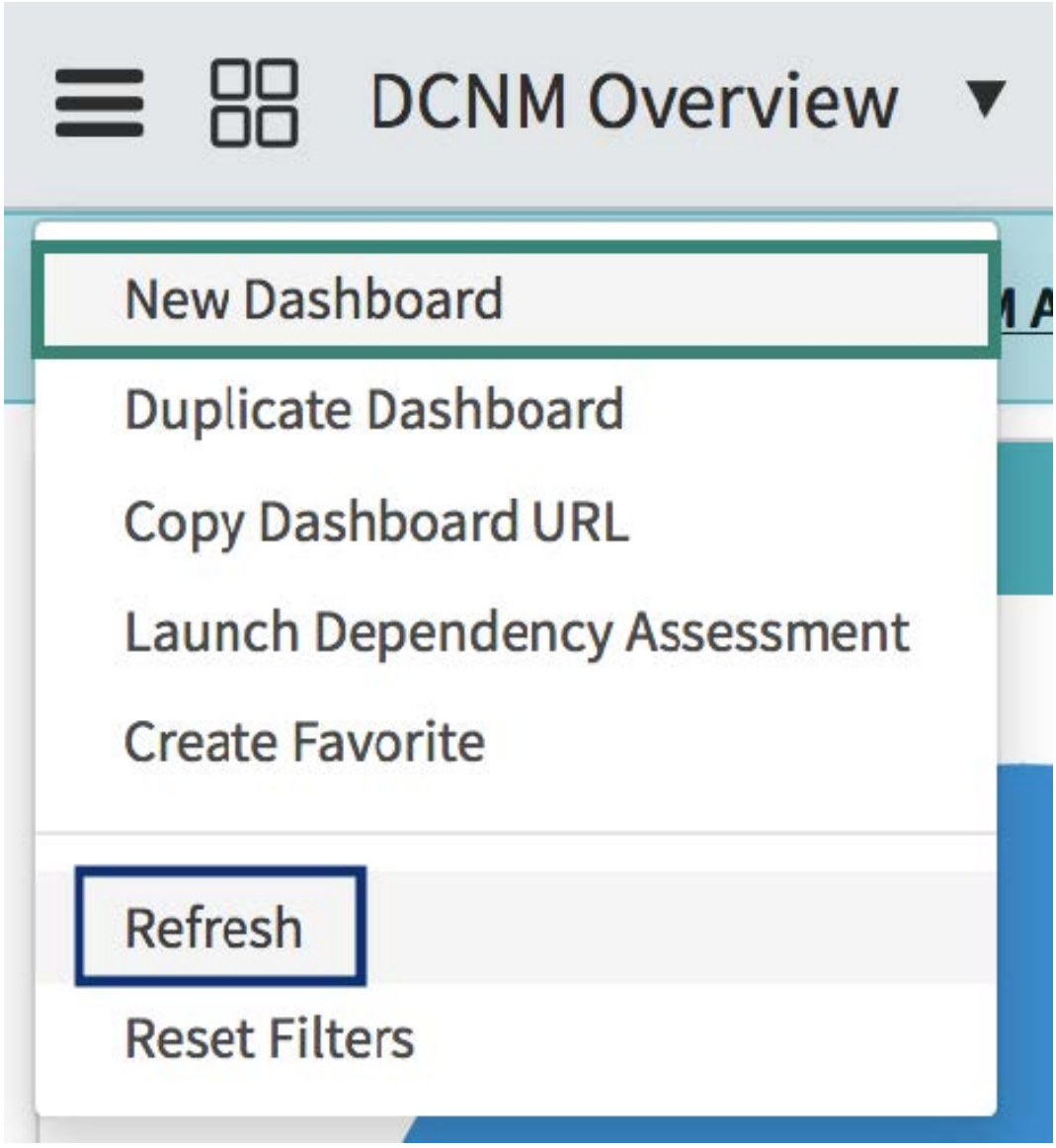
ServiceNow テーブルでデータが取得されていない場合：

- MID サーバが起動しているか、停止しているかを確認します。
- 送信元「x_caci_cisco_dcnm」でシステム ログの情報エントリを確認します。
- Cisco DCNM プロパティに追加された資格情報を確認します。
- 選択した DCNM サーバの ServiceNow ダッシュボードにデータが表示されていて、別の DCNM サーバのデータを表示するシナリオを考えてみましょう。このようなシナリオでは、キャッシュの更新の遅延のため、ServiceNow ダッシュボードが他の DCNM サーバからデータを読み込むのに時間がかかることがあります。データを手動で更新するには、タ

イルの上にカーソルを合わせるときに個々のタイルの右上隅に表示される**[更新（Refresh）]**アイコンをクリックします。



[ダッシュボード コントロール（Dashboard Controls）]アイコン をクリックし、**[更新（Refresh）]**をクリックしてレポートを正しく読み込むことで、ダッシュボード全体を更新することもできます。



ServiceNow との DCNM アプリケーション統合の詳細については、ここをクリックしてください。

第 II 部

VXLAN BGP EVPN ファブリックの Easy プロビジョニング

第 15 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

DCNM 11 では、Nexus 9000 および 3000 シリーズ スイッチでの VXLAN BGP EVPN 構成の統合アンダーレイおよびオーバーレイ プロビジョニングのための拡張「Easy」ファブリック ワークフローを導入しています。ファブリックの設定は、強力で柔軟でカスタマイズ可能なテンプレートベースのフレームワークによって実現されます。最小限のユーザー入力に基づいて、シスコ推奨のベストプラクティス設定により、ファブリック全体を短時間で立ち上げることができます。[ファブリック設定（Fabric Settings）]で公開されている一連のパラメータにより、ユーザーはファブリックを好みのアンダーレイ プロビジョニング オプションに合わせて調整できます。

ファブリック内の境界デバイスは通常、適切なエッジ/コア/WAN ルータとのピアリングを介して外部接続を提供します。これらのエッジ/コア ルータは、DCNM によって管理またはモニタできます。これらのデバイスは、外部ファブリックと呼ばれる特別なファブリックに配置されます。同じ DCNM コントローラが、複数の VXLAN BGP EVPN ファブリックを管理できると同時に、マルチサイト ドメイン（MSD）ファブリックと呼ばれる特別な構造を使用して、これらのファブリック間のレイヤ 2 およびレイヤ 3 DCI アンダーレイおよびオーバーレイ構成を簡単にプロビジョニングし、管理できます。

このドキュメントでは、「スイッチ」と「デバイス」という用語は同じ意味で使用されていることにご注意ください。

VXLAN BGP EVPN ファブリックを作成および展開するための DCNM GUI の機能は次のとおりです。

[制御（Control）] > [ファブリック ビルダ（Fabric Builder）] メニューオプション（**[ファブリック（Fabrics）]** サブメニューの下）。

ファブリックの作成、編集、および削除：

- 新しい VXLAN、MSD、および外部 VXLAN ファブリックを作成します。
- ファブリック間の接続を含む、VXLANおよびMSDファブリック トポロジを表示します。
- ファブリック設定を更新します。
- 更新された変更を保存し、展開します。
- ファブリックを削除します（デバイスが削除された場合）。

新しいスイッチでのデバイス検出とプロビジョニングの起動設定：

- ファブリックにスイッチ インスタンスを追加します。
- POAP設定を使用して、新しいスイッチに起動設定とIPアドレスをプロビジョニングします。
- スイッチ ポリシーを更新し、更新された変更を保存し、展開します。
- ファブリック内およびファブリック間リンク（ファブリック間接続（IFC）とも呼ばれる）を作成します。

[制御（Control）] > [インターフェイス（Interfaces）] メニューオプション（**[ファブリック（Fabrics）]** サブメニューの下）。

アンダーレイのプロビジョニング：

- ポートチャネル、vPC スイッチ ペア、ストレート スルー FEX（ST-FEX）、アクティブ-アクティブ FEX（AA-FEX）、ループバック、サブインターフェイスなどを作成、展開、表示、編集、削除します。
- ブレイクアウト ポートとアンブレイクアウト ポートを作成します。
- インターフェイスをシャットダウンして起動します。
- ポートを再検出し、インターフェイスの設定履歴を表示します。

[制御（Control）] > [ネットワーク（Networks）] および **[制御（Control）] > [VRF]** メニューオプション（**[ファブリック（Fabrics）]** サブメニューの下）。

オーバーレイ ネットワークのプロビジョニング

- （ファブリックの作成で指定された範囲から）新しいオーバーレイ ネットワークと VRF を作成します。
- ファブリックのスイッチでオーバーレイ ネットワークとVRFをプロビジョニングします。

- スイッチからネットワークと VRF を展開解除します。
- DCNM でファブリックからプロビジョニングを削除します。

[制御（Control）] > [サービス（Serviecs）] メニューオプション（**[ファブリック（Fabrics）]** サブメニューの下）。

L4 ～ 7 サービス アプライアンスを接続できるサービス リーフの設定のプロビジョニング。詳細については、「*L4 ～ L7*サービスの基本的なワークフロー」を参照してください。

この章では、単一の VXLAN BGP EVPN ファブリックの設定プロビジョニングについて主に説明します。MSD ファブリックを使用した複数のファブリックでのレイヤ 2/レイヤ 3 DCI の EVPN Multi-Site プロビジョニングについては、別の章で説明します。DCNM からオーバーレイ ネットワークおよび VRF を簡単にプロビジョニングできる方法の展開の詳細については、「ネットワークおよび VRF の作成と展開 」で説明されています。

VXLAN BGP EVPN ファブリック プロビジョニングのガイドライン

- スイッチを DCNM に正しくインポートするには、検出/インポート用に指定されたユーザーに次の権限が必要です。
  - スイッチへの SSH アクセス
  - SNMPv3 クエリを実行する権限
  - show run、show interfaces などを含む **show** コマンドを実行する権限
- スイッチ検出ユーザーには、スイッチの設定を変更する権限は必要ありません。主に読み取りアクセスに使用されます。
- 無効なコマンドが DCNM によってデバイスに展開された場合、たとえば、ファブリック設定の無効なエントリが原因で無効なキーチェーンを持つコマンドが生じた場合には、この問題を示すエラーが生成されます。このエラーは、無効なファブリック エントリを修正した後もクリアされません。エラーをクリアするには、無効なコマンドを手動でクリーンアップまたは削除する必要があります。

  コマンドの実行に関連するファブリック エラーは、失敗したのと同じコマンドが後続の展開で成功した場合にのみ、自動的にクリアされることに注意してください。
- LAN クレデンシャルは、デバイスへの書き込みアクセスを実行する必要があるすべてのユーザーに設定する必要があります。LAN ログイン情報は、デバイスごと、ユーザーごとに DCNM に設定する必要があります。ユーザーがデバイスを Easy ファブリックにインポートし、そのデバイスに LAN ログイン情報が設定されていない場合、DCNM はこのデバイスを移行モードに移動します。ユーザーがそのデバイスに適切な LAN ログイン情報を設定し、その後で [保存と展開（Save & Deploy）] を選択すると、デバイス インポート プロセスが再トリガーされます。
- **[保存と展開（Save & Deploy）]** ボタンをクリックすると、ファブリック全体のインテントの再生成と、ファブリック内のすべてのスイッチの設定コンプライアンス チェックがトリガーされます。このボタンは以下の場合に必須ですが、それらに限定されません。

- スイッチまたはリンクが追加された、またはトポロジが変更されたとき
- ファブリック全体で共有する必要があるファブリック設定が変更されたとき
- スイッチが取り外された、または削除されたとき
- 新しい vPC のペアリングまたはペアリングの解除が実行されたとき
- デバイスのロールが変更されたとき

[保存と展開（Save & Deploy）] をクリックすると、ファブリックの変更が評価され、ファブリック全体の構成が生成されます。生成された構成をプレビューし、ファブリック レベルで展開できます。そのため、ファブリックのサイズによっては、**[保存と展開（Save & Deploy）]** に時間がかかることがあります。

スイッチのアイコンを右クリックして、**[構成の展開（Deploy Config）]** オプションを選択すれば、スイッチごとの構成を展開できます。このオプションは、スイッチのローカル操作です。つまり、スイッチの予想される構成またはインテントが現在の実行構成に対して評価され、構成のコンプライアンス チェックが実行されて、スイッチが **In-Sync** または **Out-of-Sync** ステータスを取得します。スイッチが同期していない場合、ユーザには、その特定のスイッチで実行されているすべての設定のプレビューが提供されます。これらの設定は、それぞれのスイッチに対してユーザが定義した意図とは異なります。

- 永続的な設定の差分は、コマンドライン**system nve infra-vlan** *int* **force**で確認できます。永続的な差分は、スイッチにフリーフォームの設定を介してこのコマンドを展開すると、発生します。スイッチは展開時に **force** キーワードを必要としますが、DCNM 内でスイッチから取得された実行構成では **force** キーワードは表示されません。したがって、**system nve infra-vlan** *int* **force** コマンドは常に diff として表示されます。

  DCNM のインテントには次の行が含まれます：

  ```
  system nve infra-vlan int force
  ```

  実行設定には次の行が含まれいます：

  ```
  system nve infra-vlan int
  ```

  永続的な差分を修正する回避策として、最初の展開後にフリーフォームの設定を編集して **force** キーワードを削除し、 **system nve infra-vlan** *int* になるようにします。

  force キーワードは最初の展開に必要ですが、展開が成功した後では削除する必要があります。**[比較（Side-by-side）]** タブ（**[設定のプレビュー（Config Preview）]** ウィンドウ）を使用して、差分を確認できます。

  永続的な差分は、スイッチの消去書き込みおよびリロードの後にも表示されます。**force** キーワードを含めるように DCNM のインテントを更新し、最初の展開後に **force** キーワードを削除する必要があります。

- スイッチに、**hardware access-list tcam region arp-ether 256** コマンドが含まれている場合、このコマンドは、**double-wide** キーワードなしでは非推奨になり、次の警告が表示されます。

警告：「double-wide」なしで arp-ether 領域を設定すると、非 vxlan パケットのドロップが発生する可能性があります。（WARNING: Configuring the arp-ether region without "double-wide" is deprecated and can result in silent non-vxlan packet drops.）arp-ether リージョンの TCAM スペースを分割する場合は、「double-wide」キーワードを使用します。

元の **hardware access-list tcam region arp-ether 256** コマンドは DCNM のポリシーと一致しないため、この構成は **switch_freeform** ポリシーでキャプチャされます。**hardware access-list tcam region arp-ether 256 double-wide** コマンドがスイッチにプッシュされると、元の **tcam** コマンド（**double-wide** キーワードを含まないもの）は削除されます。

hardware access-list tcam region arp-ether 256 コマンドを **switch_freeform** ポリシーから手動で削除する必要があります。それ以外の場合、設定コンプライアンスには永続的な差分が表示されます。

スイッチでの **hardware access-list** コマンドの例を次に示します。

```
switch(config)# show run | inc arp-ether
switch(config)# hardware access-list tcam region arp-ether 256
Warning: Please save config and reload the system for the configuration to take
effect
switch(config)# show run | inc arp-ether
hardware access-list tcam region arp-ether 256
switch(config)#
switch(config)# hardware access-list tcam region arp-ether 256 double-wide
Warning: Please save config and reload the system for the configuration to take
effect
switch(config)# show run | inc arp-ether
hardware access-list tcam region arp-ether 256 double-wide
```

元の **tcam** コマンドが上書きされていることがわかります。

新規 VXLAN BGP EVPN ファブリックの作成

この手順では、新しい VXLAN BGP EVPN ファブリックを作成する方法を示します。

この手順には、IPv4 アンダーレイの説明が含まれています。IPv6 アンダーレイについては、Easy Fabric の IPv6 アンダーレイ サポート, on page 134 を参照してください。

1. **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

   [ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。初めてログインしたときには、**[ファブリック（Fabrics）]** セクションにはまだエントリはありません。ファブリックを作成すると、**[ファブリック ビルダ（Fabric Builder）]** ウィンドウに表示されます。長方形のボックスが各ファブリックを表します。

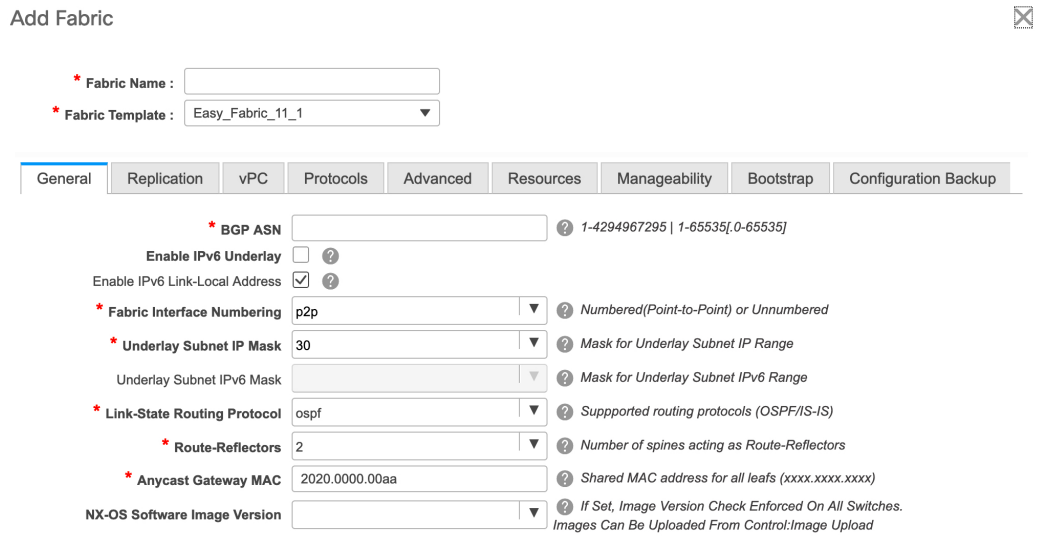
   スタンドアロンまたはメンバーファブリックには、Switch_Fabric（タイプフィールド）、AS 番号（ASN フィールド）、および複製モード（複製モード フィールド）が含まれます。

2. **[ファブリックの作成（Create Fabric）]** をクリックすると、**[ファブリックの追加（Add Fabric）]** 画面が表示されます。

フィールドについて説明します。

[ファブリック名（Fabric Name）]：ファブリックの名前を入力します。

[ファブリック テンプレート（Fabric Template）]：ドロップダウンメニューから、**[Easy_Fabric_11_1]** ファブリック テンプレートを選択します。スタンドアロン ファブリックを作成するためのファブリック設定が表示されます。



画面のタブとそのフィールドについては、以降のポイントで説明します。オーバーレイおよびアンダーレイ ネットワーク パラメータは、これらのタブに含まれています。

Note MSD ファブリックの潜在的なメンバー ファブリックとしてスタンドアロン ファブリックを作成する場合（EVPN マルチサイト テクノロジーを介して接続されるファブリックのオーバーレイ ネットワークのプロビジョニングに使用）、メンバー ファブリックの作成前に、トピック「VXLAN BGP EVPN ファブリックのマルチサイト ドメイン」を参照してください。

3. デフォルトでは **[全般（General）]** タブが表示されます。このタブのフィールドは次のとおりです。

[BGP ASN]：ファブリックが関連付けられている BGP AS 番号を入力します。

[IPv6 アンダーレイの有効化（Enable IPv6 Underlay）]：IPv6 アンダーレイ機能を有効にします。詳細については、Easy Fabric の IPv6 アンダーレイ サポート, on page 134を参照してください。

[IPv6 リンクローカル アドレスの有効化（Enable IPv6 Link-Local Address）]：IPv6 リンクローカル アドレスを有効にします。

[ファブリック インターフェイスの番号付け（Fabric Interface Numbering）]：ポイントツーポイント（[p2p]）またはアンナンバード ネットワークのどちらを使用するかを指定します。

[アンダーレイ サブネット IP マスク（Underlay Subnet IP Mask）]：ファブリック インターフェイスの IP アドレスのサブネットマスクを指定します。

[アンダーレイ ルーティング プロトコル（Underlay Routing Protocol）]：ファブリック、OSPF、または IS-IS で使用される IGP。

[ルートリフレクタ（RR）（Route-Reflectors（RRs））]：BGP トラフィックを転送するためのルート リフレクタとして使用されるスパイン スイッチの数。ドロップダウン リスト ボックスで [なし（None）] を選択します。デフォルト値は 2 です。

スパイン デバイスを RR として展開するには、DCNM はスパイン デバイスをシリアル番号に基づいてソートし、2つまたは4つのスパインデバイスをRRとして指定します。スパイン デバイスを追加しても、既存の RR 設定は変更されません。

カウントの増加：ルート リフレクタを任意の時点で 2 から 4 に増やすことができます。設定は、RR として指定された他の 2 つのスパイン デバイスで自動的に生成されます。

カウントの削減：4 つのルート リフレクタを 2 つに減らす場合は、不要なルート リフレクタ デバイスをファブリックから削除します。カウントを 4 から 2 に減らすには、次の手順に従います。

a. ドロップダウンボックスの値を 2 に変更します。

b. ルート リフレクタとして指定するスパイン スイッチを特定します。

ルート リフレクタの場合、**[rr_state]** ポリシーのインスタンスがスパイン スイッチに適用されます。ポリシーがスイッチに適用されているかどうかを確認するには、スイッチを右クリックし、[ポリシーの表示/編集（View/edit policies）] を選択します。[ポリシーの表示/編集（View/Edit Policies）] 画面の [テンプレート（Template）] フィールドで [rr_state] を検索します。画面に表示されます。

c. ファブリックから不要なスパインデバイスを削除します（スパイン スイッチアイコンを右クリックし、[検出（Discovery）] > [ファブリックから削除（Remove from fabric）] の順に選択します）。

既存の RR デバイスを削除すると、次に使用可能なスパイン スイッチが交換 RR として選択されます。

d. ファブリック トポロジ ウィンドウで **[保存と展開（Save & Deploy）]** をクリックします。

最初の [保存と展開（Save & Deploy）] 操作を実行する前に、RR と RP を事前に選択できます。詳細については、「ルート リフレクタおよびランデブー ポイントとしてのスイッチの事前選択」を参照してください。

[エニーキャスト ゲートウェイ MAC（Anycast Gateway MAC）]：エニーキャスト ゲートウェイ MAC アドレスを指定します。

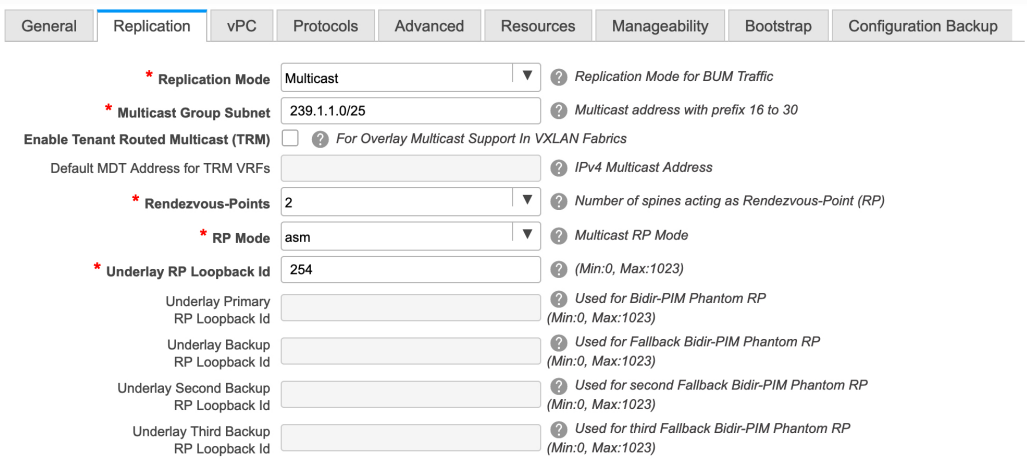
[NX-OS ソフトウェア イメージ バージョン（NX-OS Software Image Version）]：リストからイメージを選択します。

イメージアップロードオプションを使用して Cisco NX-OS ソフトウェアイメージをアップロードすると、アップロードされたイメージがこのフィールドにリストされます。イ

メージを選択してファブリック設定を保存すると、システムはファブリック内のすべてのスイッチに選択したバージョンがあることを確認します。一部のデバイスでイメージが実行されない場合、指定されたイメージへのインサービス ソフトウェア アップグレード（ISSU）を実行するように警告するプロンプトが表示されます。警告には、[解決（Resolve）]ボタンも付いています。これにより、[ファブリック設定（Fabric Settings）]で指定された指定の NX-OS イメージへのデバイス アップグレード/ダウングレードに対して不一致のスイッチが自動的に選択されたイメージ管理画面が表示されます。すべてのデバイスが指定されたイメージを実行するまで、展開プロセスは完了しません。

ファブリック スイッチに複数のタイプのソフトウェア イメージを展開する場合は、イメージを指定しないでください。イメージが指定されている場合は削除します。

4. **[レプリケーション（Replication）]** タブをクリックします。ほとんどのフィールドは自動生成されます。必要に応じてフィールドを更新できます。



[レプリケーション モード（Replication Mode）]：BUM（ブロードキャスト、不明なユニキャスト、マルチキャスト）トラフィックのファブリックで使用されるレプリケーションのモードです。選択肢は[レプリケーションの入力（Ingress Replication）]または[マルチキャスト（Multicast）]です。[レプリケーションの入力（Ingress replication）]を選択すると、マルチキャスト関連のフィールドは無効になります。

ファブリックのオーバーレイ プロファイルが存在しない場合は、ファブリック設定をあるモードから別のモードに変更できます。

[マルチキャスト グループ サブネット（Multicast Group Subnet）]：マルチキャスト通信に使用される IP アドレス プレフィックスです。オーバーレイ ネットワークごとに、このグループから一意の IP アドレスが割り当てられます。

DCNM 11.1(1) リリースでは、現在のモードのポリシー テンプレート インスタンスが作成されている場合、レプリケーション モードの変更は許可されません。たとえば、マルチキャスト関連のポリシーを作成して展開する場合、モードを入力に変更することはできません。

[テナント ルーテッド マルチキャスト（TRM）の有効化（Enable Tenant Routed Multicast（TRM））]：VXLAN BGP EVPN ファブリックで EVPN/MVPN を介してオーバーレイ

マルチキャスト トラフィックをサポートできるようにするテナント ルーテッド マルチキャスト（TRM）を有効にするには、このチェックボックスをオンにします。

[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]：テナント ルーテッド マルチキャスト トラフィックのマルチキャスト アドレスが入力されます。デフォルトでは、このアドレスは [マルチキャスト グループ サブネット] フィールドで指定された IP プレフィックスから取得されます。いずれかのフィールドをアップデートする場合、**[マルチキャスト グループ サブネット（Multicast Group Subnet）]** で指定した IP プレフィックスから選択された TRM アドレスであることを確認してください。

詳細については、テナント ルーテッド マルチキャストの概要, on page 234を参照してください。

[ランデブーポイント（Rendezvous-Points）]：ランデブーポイントとして機能するスパイン スイッチの数を入力します。

[RP モード（RP mode）]：ASM（エニーソース マルチキャスト（ASM）の場合）または BiDir（双方向 PIM（BIDIR-PIM）の場合）の 2 つのサポート対象のマルチキャスト モードから選択します。

[ASM] を選択すると、[BiDir] 関連のフィールドは有効になりません。[BiDir] を選択すると、[BiDir] 関連フィールドが有効になります。

Note BIDIR-PIM は、Cisco のクラウド スケール ファミリ プラットフォーム 9300-EX および 9300-FX/FX2、およびソフトウェア リリース 9.2(1) 以降でサポートされています。

ファブリック オーバーレイの新しい VRF を作成すると、このアドレスが [アドバンス（Advanced）] タブの [アンダーレイ マルチキャスト アドレス（Underlay Multicast Address）] フィールドに入力されます。

[アンダーレイ RP ループバック ID（Underlay RP Loopback ID）]：ファブリック アンダーレイでのマルチキャスト プロトコル ピアリングの目的で、ランデブーポイント（RP）に使用されるループバック ID です。

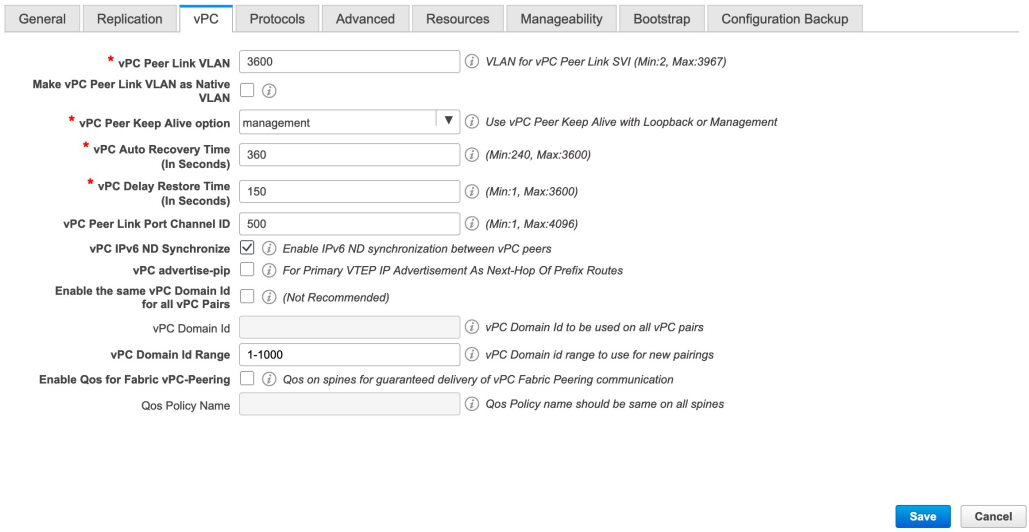
次の 2 つのフィールドは、レプリケーションのマルチキャスト モードとして [BIDIR-PIM] を選択した場合に有効になります。

[アンダーレイ プライマリ RP ループバック ID（Underlay Primary RP Loopback ID）]：ファブリック アンダーレイでマルチキャスト プロトコル ピアリングのためにファントム RP に使用されるプライマリ ループバック ID です。

[アンダーレイ バックアップ RP ループバック ID（Underlay Backup RP Loopback ID）]：ファブリック アンダーレイでマルチキャスト プロトコル ピアリングを目的として、ファントム RP に使用されるセカンダリ ループバック ID です。

[アンダーレイ セカンド バックアップ RP ループバック ID（Underlay Second Backup RP Loopback Id）] および [アンダーレイ サード バックアップ RP ループバック ID（Underlay Third Backup RP Loopback Id）]：2 番目と 3 番目のフォールバック Bidir-PIM ファントム RP に使用されます。

5. **[vPC]** タブをクリックします。ほとんどのフィールドは自動生成されます。必要に応じてフィールドを更新できます。



[vPC ピア リンク VLAN（vPC Peer Link VLAN）]：vPC ピア リンク SVI に使用される VLAN です。

[vPC ピア リンク VLAN をネイティブ VLAN とする（Make vPC Peer Link VLAN as Native VLAN）]：vPC ピア リンク VLAN をネイティブ VLAN として有効にします。

[vPC ピア キープアライブ オプション（vPC Peer Keep Alive option）]：管理またはループバック オプションを選択します。管理ポートおよび管理 VRF に割り当てられた IP アドレスを使用する場合は、[管理（management）] を選択します。ループバック インターフェイス（および非管理 VRF）に割り当てられた IP アドレスを使用する場合は、ループバックを選択します。

IPv6 アドレスを使用する場合は、ループバック ID を使用する必要があります。

[vPC 自動回復時間（vPC Auto Recovery Time）]：vPC 自動回復タイムアウト時間を秒単位で指定します。

[vPC 遅延復元時間（vPC Delay Restore Time）]：vPC 遅延復元期間を秒単位で指定します。

[vPC ピア リンク ポートチャネル ID（vPC Peer Link Port Channel ID）：vPC ピア リンクのポートチャネル ID を指定します。デフォルトでは、このフィールドの値は 500 です。

[vPC IPv6 ND 同期（vPC IPv6 ND Synchronize）]：vPC スイッチ間の IPv6 ネイバー探索同期を有効にします。デフォルトでチェックボックスはオンになっています。機能を無効にするにはチェックボックスをクリアします。

[vPC advertise-pip]：アドバタイズ PIP 機能を有効にします。

特定の vPC でアドバタイズ PIP 機能をイネーブルにすることもできます。詳細については、vPC で PIP をアドバタイズする, on page 286を参照してください。

[すべての vPC ペアに同じ vPC ドメイン ID を有効にする（Enable the same vPC Domain Id for all vPC Pairs）]：すべての vPC ペアに同じ vPC ドメイン ID を有効にします。このフィールドを選択すると、[vPC ドメイン ID（vPC Domain Id）] フィールドが編集可能になります。

[vPC ドメイン ID（vPC Domain Id）]：すべての vPC ペアで使用される vPC ドメイン ID を指定します。

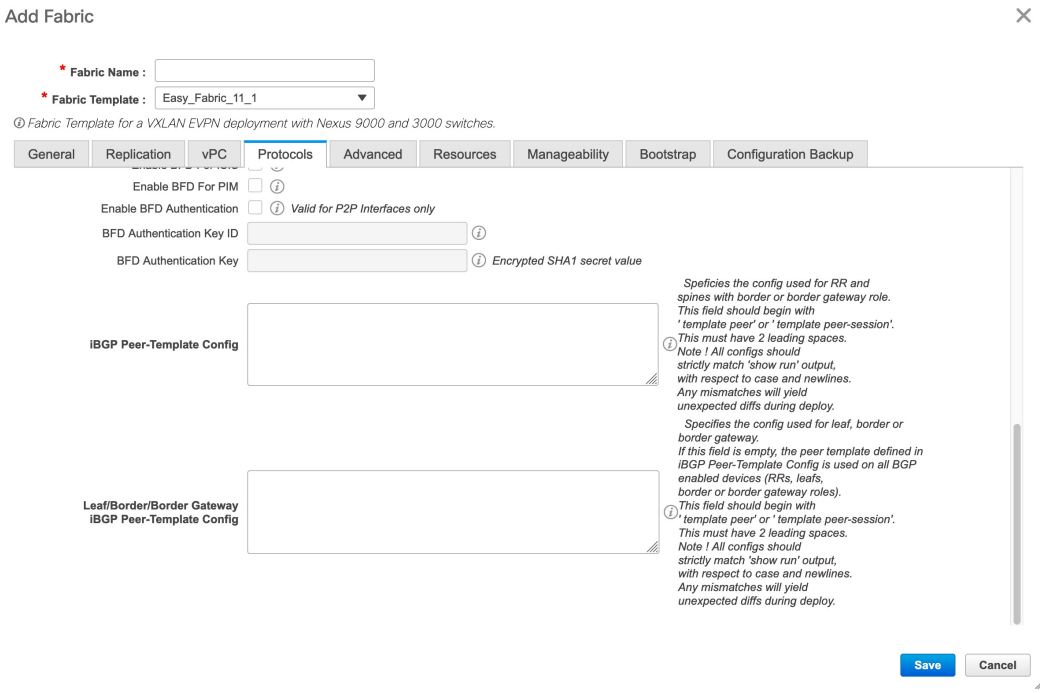
[vPC ドメイン ID の範囲（vPC Domain Id Range）]：新しいペアリングに使用する vPC ドメイン ID の範囲を指定します。

[ファブリック vPC ピアリングの QoS を有効にする（Enable QoS for Fabric vPC-Peering）]：スパインの QoS を有効にして、vPC ファブリック ピアリング通信の配信を保証します。詳細については、ファブリック vPC ピアリングの QoS, on page 277を参照してください。

Note ファブリック設定の vPC ファブリック ピアリングとキューイング ポリシーの QoS オプションは相互に排他的です。

[QoS ポリシー名（QoS Policy Name）]：すべてのファブリック vPC ピアリング スパインで同じにする必要がある QoS ポリシー名を指定します。デフォルト名は [spine_qos_for_fabric_vpc_peering] です。

6. **[プロトコル（Protocols）]** タブをクリックします。ほとんどのフィールドは自動生成されます。必要に応じてフィールドを更新できます。



[アンダーレイ ルーティング ループバック ID（Underlay Routing Loopback Id）]：通常は loopback0 がファブリック アンダーレイ IGP ピアリングに使用されるため、ループバック インターフェイス ID は 0 に設定されます。

[アンダーレイ VTEP ループバック ID（Underlay VTEP Loopback Id）]：loopback1 は VTEP ピアリングの目的で使用されるため、ループバック インターフェイス ID は 1 に設定されます。

[アンダーレイ ルーティング プロトコル タグ（Underlay Routing Protocol Tag）]：ネットワークのタイプを定義するタグです。

[OSPF エリア ID（OSPF Area ID）]：OSPF エリア ID です（OSPF がファブリック内で IGP として使用されている場合）。

Note OSPF または IS-IS 認証フィールドは、[全般（**General**）] タブの**[アンダーレイ ルーティング プロトコル（Underlay Routing Protocol）]** フィールドでの選択に基づいて有効になります。

[OSPF 認証の有効化（Enable OSPF Authentication）]：OSPF 認証を有効にするには、このチェックボックスをオンにします。無効にするにはチェックボックスをオフにします。このフィールドを有効にすると、OSPF 認証キー ID フィールドおよび OSPF 認証キー フィールドが有効になります。

[OSPF 認証キー ID（OSPF Authentication Key ID）]：キー ID が入力されます。

[OSPF 認証キー（OSPF Authentication Key）]：OSPF 認証キーは、スイッチからの 3DES キーである必要があります。

Note プレーン テキスト パスワードはサポートされていません。スイッチにログインし、暗号化キーを取得して、このフィールドに入力します。詳細については、「認証キーの取得」の項を参照してください。

[IS-IS レベル（IS-IS Level）]：このドロップダウンリストから IS-IS レベルを選択します。

[IS-IS 認証の有効化（Enable IS-IS Authentication）]：IS-IS 認証を有効にするにはチェックボックスをオンにします。無効にするにはチェックボックスをオフにします。このフィールドを有効にすると、IS-IS 認証フィールドが有効になります。

[IS-IS 認証キーチェーン名（IS-IS Authentication Keychain Name）]：CiscoisisAuth などのキーチェーン名を入力します。

[IS-IS 認証キー ID（IS-IS Authentication Key ID）：キー ID が入力されます。

[IS-IS 認証キー（IS-IS Authentication Key）]：Cisco Type 7 暗号化キーを入力します。

Note プレーン テキスト パスワードはサポートされていません。スイッチにログインし、暗号化キーを取得して、このフィールドに入力します。詳細については、「認証キーの取得」の項を参照してください。

[BGP 認証の有効化（Enable BGP Authentication）]：BGP 認証を有効にするにはチェックボックスをオンにします。無効にするにはチェックボックスをオフにします。このフィールドを有効にすると、[BGP 認証キー暗号化タイプ（BGP Authentication Key Encryption Type）] および [BGP 認証キー（BGP Authentication Key）] フィールドが有効になります。

Note このフィールドを使用して BGP 認証を有効にする場合は、[iBGP Peer-Template Config] フィールドを空白のままにして、設定が重複しないようにします。

[BGP 認証キー暗号化タイプ（BGP Authentication Key Encryption Type）]：3DES 暗号化タイプの場合は 3、Cisco 暗号化タイプの場合は 7 を選択します。

[BGP 認証キー（BGP Authentication Key）]：暗号化タイプに基づいて暗号化キーを入力します。

Note プレイン テキスト パスワードはサポートされていません。スイッチにログインし、暗号化されたキーを取得して、[BGP 認証キー（BGP Authentication Key）] フィールドに入力します。詳細については、「認証キーの取得」の項を参照してください。

[PIM hello 認証の有効化（Enable PIM Hello Authentication）]：PIM hello認証を有効にします。

[PIM Hello 認証キー（PIM Hello Authentication Key）]：PIM hello 認証キーを指定します。

[BFD の有効化（Enable BFD）]：ファブリック内のすべてのスイッチで機能 [bfd] を有効にするには、このチェックボックスをオンにします。この機能は、IPv4 アンダーレイでのみ有効で、範囲はファブリック内にあります。

Cisco DCNM リリース 11.3(1) 以降、ファブリック内の BFD はネイティブにサポートされます。ファブリック設定では、BFD機能はデフォルトで無効になっています。有効にすると、デフォルト設定のアンダーレイ プロトコルに対して BFD が有効になります。カスタムの必須BFD構成は、スイッチごとの自由形式またはインターフェイスごとの自由形式ポリシーを使用して展開する必要があります。

[BFD の有効化（Enable BFD）] チェックボックスをオンにすると、次の構成がプッシュされます。

```
feature bfd
```

Note BFD が有効になっている DCNM リリース 11.2(1) から DCNM リリース 11.3(1) にアップグレードすると、次の設定がすべての P2P ファブリック インターフェイスにプッシュされます。

```
no ip redirects
no ipv6 redirects
```

BFD機能の互換性については、それぞれのプラットフォームのマニュアルを参照してください。サポートされているソフトウェア画像については、「*Cisco DCNM* の互換性マトリクス」を参照してください。

[iBGP 向け BFD の有効化（Enable BFD for iBGP）]：iBGP ネイバーの BFD を有効にするには、このチェックボックスをオンにします。このオプションは、デフォルトで無効です。

[OSPF 向け BFD の有効化（Enable BFD for OSPF）]：このチェックボックスをオンにすると、OSPF アンダーレイ インスタンスの BFD が有効になります。このオプションはデフォルトで無効になっており、リンクステートプロトコルがISISの場合はグレー表示されます。

[ISIS 向け BFD の有効化（Enable BFD for ISIS）]：このチェックボックスをオンにして、ISIS アンダーレイ インスタンスの BFD を有効にします。このオプションはデフォルトで無効になっており、リンク ステート プロトコルが OSPF の場合はグレー表示されます。

[PIM 向け BFD の有効化（Enable BFD for PIM）]：PIM の BFD を有効にするには、このチェックボックスをオンにします。このオプションはデフォルトで無効になっており、レプリケーション モードが [入力（Ingress）] の場合はグレー表示されます。

BFD グローバル ポリシーの例を次に示します。

```
router ospf <ospf tag>
   bfd

router isis <isis tag>
  address-family ipv4 unicast
    bfd

ip pim bfd

router bgp <bgp asn>
  neighbor <neighbor ip>
    bfd
```

[BGP 認証の有効化（Enable BGP Authentication）]：BGP 認証を有効にするにはチェックボックスをオンにします。このフィールドを有効にすると、[BFD 認証キー ID（BFD Authentication Key ID）] フィールドと [BFD 認証キー（BFD Authentication Key）] フィールドが編集可能になります。

Note [全般（General）] タブの [ファブリック インターフェイスの番号付け（Fabric Interface Numbering）] フィールドが [番号付けなし（unnumbered）] に設定されている場合、BFD 認証はサポートされません。BFD 認証フィールドは自動的にグレー表示されます。BFD 認証は、P2P インターフェイスに対してのみ有効です。

[BFD 認証キー ID（BFD Authentication Key ID）]：インターフェイス認証の BFD 認証キー ID を指定します。デフォルト値は 100 です。

[BFD 認証キー（BFD Authentication Key）]：BFD 認証キーを指定します。

BFD 認証パラメータを取得する方法については、暗号化された BFD 認証キーの取得, on page 300 を参照してください。

[iBGP ピアテンプレート構成（iBGP Peer-Template Config）] ：リーフ スイッチに iBGP ピア テンプレート構成を追加して、リーフ スイッチとルート リフレクタの間に iBGP セッションを確立します。

BGP テンプレートを使用する場合は、テンプレート内に認証構成を追加し、[BGP 認証の有効化（Enable BGP Authentication）] チェックボックスをオフにして、構成が重複しないようにします。

構成例では、パスワード 3 の後に 3DES パスワードが表示されます。

```
router bgp 65000
    password 3 sd8478fswerdfw3434fsw4f4w34sdsd8478fswerdfw3434fsw4f4w
```

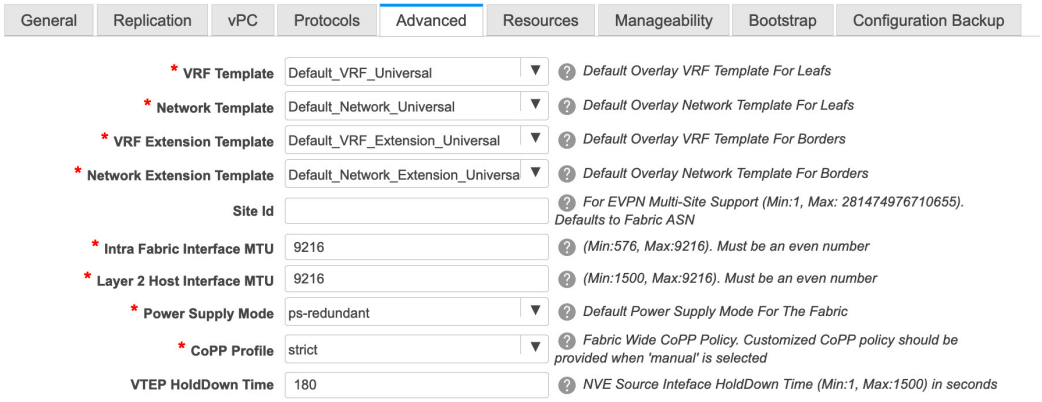
Cisco DCNM リリース 11.3(1) までは、リーフまたはボーダー ロール デバイスの iBGP 定義の iBGP ピア テンプレートと BGP RR は同じでした。DCNM リリース 11.4(1) 以降、次のフィールドを使用してさまざまな構成を指定できます。

- [iBGP ピアテンプレート構成（iBGP Peer-Template Config）]：境界ロールを持つ RR およびスパインに使用される構成を指定します。

- [リーフ/境界/境界ゲートウェイ iBGP ピアテンプレート構成（Leaf/Border/Border Gateway iBGP Peer-Template Config）]：リーフ、境界、または境界ゲートウェイに使用される構成を指定します。このフィールドが空の場合、[iBGP ピアテンプレート構成（iBGP Peer-Template Config）] で定義されたピア テンプレートがすべての BGP 対応デバイス（RR、リーフ、境界、または境界ゲートウェイ ロール）で使用されます。

ブラウンフィールド移行では、スパインとリーフが異なるピアテンプレート名を使用する場合、[iBGP ピアテンプレート構成（iBGP Peer-Template Config）] フィールドと [リーフ/境界/境界ゲートウェイ iBGP ピアテンプレート構成（Leaf/Border/Border Gateway iBGP Peer-Template Config）] フィールドの両方をスイッチ構成に従って設定する必要があります。スパインとリーフが同じピア テンプレート名とコンテンツを使用する場合（「route-reflector-client」CLIを除く）、ファブリック設定の [iBGP ピアテンプレート構成（iBGP Peer-Template Config）] フィールドのみを設定する必要があります。iBGP ピアテンプレートのファブリック設定が既存のスイッチ構成と一致しない場合、エラー メッセージが生成され、移行は続行されません。

7. [Advanced] タブをクリックします。ほとんどのフィールドは自動生成されます。必要に応じてフィールドを更新できます。



VRFテンプレートおよびVRF拡張テンプレート：VRFを作成するためのVRFテンプレートと、他のファブリックへのVRF拡張を有効にするためのVRF拡張テンプレートを指定します。

[ネットワーク テンプレート（Network Template）] と [ネットワーク拡張テンプレート（Network Extension Template）]：ネットワークを作成するためのネットワーク テンプレートと、他のファブリックにネットワークを拡張するためのネットワーク拡張テンプレートを指定します。

[サイト ID（Site ID）]：このファブリックを MSD 内で移動する場合の ID です。メンバー ファブリックが MSD の一部であるためには、サイト ID が必須です。MSD の各メンバー ファブリックには、一意のサイト ID があります。

[イントラ ファブリック インターフェイス MTU（Intra Fabric Interface MTU）]：ファブリック内インターフェイスの MTU を指定します。この値は偶数にする必要があります。

[レイヤ 2 ホスト インターフェイス MTU（Layer 2 Host Interface MTU）]：レイヤ 2 ホスト インターフェイスの MTU を指定します。この値は偶数にする必要があります。

電源モード（Power Supply Mode）：適切な電源モードを選択します。

[CoPP プロファイル（CoPP Profile）]：ファブリックの適切なコントロールプレーン ポリシング（CoPP）プロファイルポリシーを選択します。デフォルトでは、strict オプションが入力されます。

[VTEP HoldDown 時間（VTEP HoldDown Time）]：NVE 送信元インターフェイスのホールドダウン時間を指定します。

[ブラウンフィールド オーバーレイ ネットワーク名の形式（Brownfield Overlay Network Name Format）]：ブラウンフィールドのインポートまたは移行時にオーバーレイ ネットワーク名を作成するために使用する形式を入力します。ネットワーク名は、アンダースコア（_）およびハイフン（-）を除く特殊文字または空のスペースが含まれないようにしてください。ブラウンフィールドの移行が開始されたら、ネットワーク名を変更しないでください。ネットワーク名の命名規則については、「スタンドアロンファブリックのネットワークの作成」の項を参照してください。構文は**[<string> | $$VLAN_ID$$] $$VNI$$ [<string>| $$VLAN_ID$$]**です。デフォルト値は **[Auto_Net_VNI$$VNI$$_VLAN$$VLAN_ID$$]** です。ネットワークを作成すると、指定した構文に従って名前が生成されます。次の表で構文内の変数について説明します。

変数	説明
$$VNI$$	スイッチ構成で検出されたネットワーク VNI ID を指定します。これは、一意のネットワーク名を作成するために必要な必須キーワードです。
$$VLAN_ID$$	ネットワークに関連付けられた VLAN ID を指定します。 VLAN ID はスイッチに固有であるため、DCNM はネットワークが検出されたスイッチの 1 つから VLAN ID をランダムに選択し、名前に使用します。 VLAN ID が VNI のファブリック全体で一貫していない限り、これを使用しないことを推奨します。
<string>	この変数はオプションであり、ネットワーク名のガイドラインを満たす任意の数の英数字を入力できます。

オーバーレイ ネットワーク名の例：Site_VNI12345_VLAN1234

Note グリーンフィールド展開では、このフィールドを無視します。ブラウンフィールド オーバーレイ ネットワーク名の形式は、次のブラウンフィールド インポートに適用されます。

- CLI ベースのオーバーレイ
- 構成プロファイルが Cisco DCNM リリースで作成された構成プロファイルベースのオーバーレイ

  10.4(2) で作成された構成プロファイルベースのオーバーレイ

[ブートストラップ スイッチの CDP の有効化（Enable CDP for Bootstrapped Switch）]：ブートストラップ スイッチの管理（mgmt0）インターフェイスでCDP を有効にします。デフォルトでは、ブートストラップ スイッチの場合、mgmt0 インターフェイスで CDP は無効にされています。

[VXLAN OAM の有効化（Enable VXLAN OAM）]：ファブリック内のデバイスのVXLAM OAM機能を有効にします。この設定はデフォルトでイネーブルになっています。VXLAN OAM 機能を無効にするにはチェックボックスをクリアします。

ファブリック内の特定のスイッチで VXLAN OAM 機能を有効にし、他のスイッチで無効にする場合は、自由形式構成を使用して、ファブリック設定でOAM を有効にし、OAM を無効にすることができます。

Note Cisco DCNM の VXLAN OAM 機能は、単一のファブリックまたはサイトでのみサポートされます。

[テナント DHCP の有効化（Enable Tenant DHCP）]：機能 dhcp および関連する構成をファブリック内のすべてのスイッチでグローバルに有効にするには、このチェックボックスをオンにします。これは、テナント VRF の一部であるオーバーレイ ネットワークの DHCP をサポートするための前提条件です。

Note オーバーレイ プロファイルでDHCP 関連のパラメータを有効にする前に、**[テナント DHCP の有効化（Enable Tenant DHCP）]** が有効であることを確認します。

[NX-API の有効化（Enable NX-API）]：HTTPS での NX-API の有効化を指定します。このチェックボックスは、デフォルトでオンになっています。

[ポートの HTTP で NX-API を有効化する（Enable on NX-API on HTTP）]：HTTP 上の NX-API の有効化を指定します。HTTP を使用するには、[NX-API の有効化（Enable NX-API）] チェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。このチェックボックスをオフにすると、エンドポイント ロケータ（EPL）、レイヤ 4 ～ レイヤ 7 サービス（L4ーL7 サービス）、VXLAN OAM など、NX-API

を使用し、Cisco DCNM がサポートするアプリケーションは、HTTP ではなく HTTPS の使用を開始します。

Note [NX-API の有効化（Enable NX-API）] チェックボックスと [HTTP での NX-API の有効化（Enable NX-API on HTTP）] チェックボックスをオンにすると、アプリケーションは HTTP を使用します。

[ポリシーベース ルーティング（PBR）の有効化（Enable Policy-Based Routing（PBR））]：指定したポリシーに基づいてパケットのルーティングを有効にするにはこのチェックボックスを選択します。Cisco NX-OS リリース 7.0(3)I7(1) 以降では、この機能は Nexus 9000 クラウド スケール（Tahoe）ASIC を搭載した Cisco Nexus 9000 シリーズ スイッチで動作します。この機能は、レイヤ 4 ～ レイヤ 7 サービス ワークフローとともに使用されます。レイヤ 4 ～ レイヤ 7 サービスの詳細については、「レイヤ 4 ～ レイヤ 7 サービス」の章を参照してください。

[厳密な構成コンプライアンスの有効化（Enable Strict Config Compliance）]：このチェックボックスをオンにして、厳密な構成コンプライアンス機能を有効にします。デフォルトで、この機能は無効になっています。詳細については、「厳密な構成コンプライアンス」を参照してください。

[AAA IP 認証の有効化（Enable AAA IP Authorization）]：IP 認証がリモート認証サーバーで有効になっている場合に、AAA IP 認証を有効にします。これは、スイッチにアクセスできる IP アドレスを顧客が厳密に制御できるシナリオで DCNM をサポートするために必要です。

[NDFC をトラップ ホストとして有効化（Enable NDFC as Trap Host）]：DCNM を SNMP トラップの接続先として有効にするには、このチェックボックスをオンにします。通常、ネイティブ HA DCNM の展開では、スイッチの eth1 VIP IP アドレスが SNMP トラップ接続先として構成されます。デフォルトでは、このチェックボックスは有効になっています。

[グリーンフィールド クリーンアップ オプション（Greenfield Cleanup Option）]：Preserve-Config=No で DCNM にインポートされたスイッチのスイッチ クリーンアップ オプションを有効にします。このオプションは、通常、スイッチのクリーンアップ時間を短縮するために、Cisco Nexus 9000v スイッチを使用するファブリック環境でのみ推奨されます。グリーンフィールド導入の推奨オプションは、ブートストラップを使用するか、または再起動によるクリーンアップです。つまり、このオプションはオフにする必要があります。

[精密時間プロトコル（PTP）の有効化（Enable Precision Time Protocol（PTP））]：ファブリック全体で PTP を有効にします。このチェックボックスをオンにすると、PTP がグローバルに有効になり、コアに面するインターフェイスで有効になります。また、**[PTP 送信元ループバック ID（PTP Source Loopback Id）]** および **[PTP ドメイン ID（PTP Domain Id）]** フィールドが編集可能になります。詳細については、Easy ファブリック向け高精度時間プロトコル, on page 119を参照してください。

[PTP 送信元ループバック ID（PTP Source Loopback Id）]：すべての PTP パケットの送信元 IP アドレスとして使用されるループバック インターフェイス ID ループバックを指定します。有効な値の範囲は 0 ～ 1023 です。PTP ループバック ID を RP、ファントム RP、NVE、または MPLS ループバック ID と同じにすることはできません。そうでない場合は、エラーが生成されます。PTP ループバック ID は、DCNM から BGP ループバックまたは作成元のユーザー定義ループバックと同じにすることができます。

保存して展開中に PTP ループバック ID が見つからない場合は、次のエラーが生成されます。

PTP 送信元 IP に使用するループバック インターフェイスが見つかりません。PTP 機能を有効にするには、すべてのデバイスでPTPループバックインターフェイスを作成します。

[PTP ドメイン ID（PTP Domain Id）]：単一のネットワーク上の PTP ドメイン ID を指定します。有効な値の範囲は 0 ～ 127 です。

[MPLS ハンドオフの有効化（Enable MPLS Handoff）]：MPLS ハンドオフ機能を有効にするには、このチェックボックスをオンにします。詳細については、「VXLAN BGP EVPN ファブリックでの境界プロビジョニングの使用例：MPLS SR および LDP ハンドオフ」の章を参照してください。

[アンダーレイ MPLS ループバック ID（Underlay MPLS Loopback Id）]：アンダーレイ MPLS ループバック ID を指定します。デフォルト値は 101 です。

[TCAM 割り当ての有効化（Enable TCAM Allocation）]：TCAM コマンドは、有効にすると VXLAN および vPC ファブリック ピアリングに対して自動的に生成されます。

[デフォルト キューイング ポリシーの有効化（Enable Default Queuing Policies）]：このファブリック内のすべてのスイッチにQoSポリシーを適用するには、このチェックボックスをオンにします。すべてのスイッチに適用したQoSポリシーを削除するには、このチェックボックスをオフにし、すべての設定を更新してポリシーへの参照を削除し、保存して展開します。Cisco DCNM リリース 11.3(1) 以降、さまざまな Cisco Nexus 9000 シリーズスイッチに使用できる定義済みのQoS設定が含まれています。このチェックボックスをオンにすると、適切な QoS 設定がファブリック内のスイッチにプッシュされます。システム キューイングは、設定がスイッチに展開されると更新されます。インターフェイスごと自由形式ブロックに必要な設定を追加することにより、必要に応じて、定義されたキューイング ポリシーを使用してインターフェイス マーキングを実行できます。

Cisco DCNM リリース 11.4(1) 以降、ポリシー テンプレートの QoS 5 の DSCP マッピングが 40 から 46 に変更されました。11.4(1) にアップグレードされた DCNM 11.3(1) 展開の場合、展開する必要がある差分が表示されます。

テンプレート エディタでポリシー ファイルを開いて、実際のキューイング ポリシーを確認します。Cisco DCNM Web UI から、**[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択します。ポリシー ファイル名でキューイング ポリシーを検索します（例：[queuing_policy_default_8q_cloudscale]）。ファイルを選択し、**[テンプレートの変更/表示（Modify/View template）]** アイコンをクリックしてポリシーを編集します。

プラットフォーム特有の詳細については、『*Cisco Nexus 9000 Series NX-OS Quality of Service* コンフィグレーション ガイド』を参照してください。

[N9K クラウド スケール プラットフォームのキューイング ポリシー（N9K Cloud Scale Platform Queuing Policy）]：ファブリック内の EX、FX、および FX2 で終わるすべての Cisco Nexus 9200 シリーズスイッチおよび Cisco Nexus 9000 シリーズスイッチに適用するキューイング ポリシーをドロップダウン リストから選択します。有効な値は [queuing_policy_default_4q_cloudscale] および [queuing_policy_default_8q_cloudscale] です。FEX には [queuing_policy_default_4q_cloudscale] ポリシーを使用します。FEX がオフラインの場合にのみ、[queuing_policy_default_4q_cloudscale] ポリシーから [queuing_policy_default_8q_cloudscale] ポリシーに変更できます。

[N9K R シリーズ プラットフォーム キューイング ポリシー（N9K R-Series Platform Queuing Policy）]：ドロップダウンリストから、ファブリック内の R で終わるすべての Cisco Nexus スイッチに適用するキューイング ポリシーを選択します。有効な値は [queuing_policy_default_r_series] です。

[その他の N9K プラットフォーム キューイング ポリシー（Other N9K Platform Queuing Policy）]：ドロップダウンリストからキューイング ポリシーを選択し、ファブリック内にある、上記 2 つのオプションで説明したスイッチ以外の他のすべてのスイッチに適用します。有効な値は [queuing_policy_default_other] です。

[MACsec の有効化（Enable MACsec）]：ファブリックの MACsec を有効にします。詳細については、Easy ファブリックおよび eBGP ファブリックでの MACsec サポート, on page 231を参照してください。

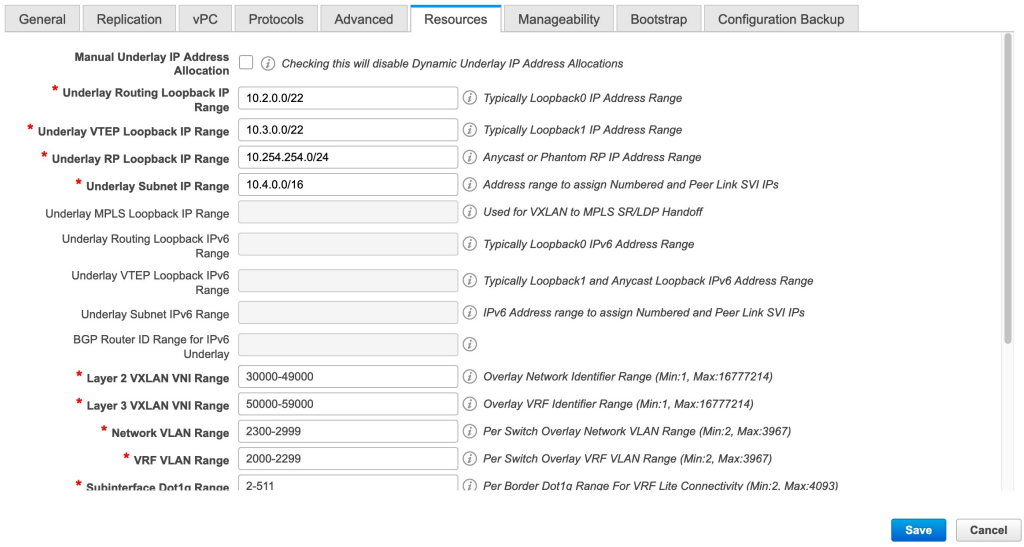
[自由形式の CLI（Freeform CLIs）]：ファブリック レベルの自由形式の CLI は、ファブリックの作成または編集中に追加できます。ファブリック全体のスイッチに適用できます。インデントなしで、実行コンフィギュレーションに表示されている設定を追加する必要があります。VLAN、SVI、インターフェイス構成などのスイッチ レベルの自由形式の構成は、スイッチでのみ追加する必要があります。詳細については、「ファブリック スイッチでのフリーフォーム設定の有効化」を参照してください。

[リーフの自由形式の構成（Leaf Freeform Config）]：リーフ、ボーダー、およびボーダーゲートウェイのロールを持つスイッチに追加する CLI です。

[スパインの自由形式の設定（Spine Freeform Config）]：スパイン、ボーダー スパイン、ボーダーゲートウェイ スパイン、および スーパー スパインのロールを持つスイッチに追加する必要がある CLI を追加します。

[ファブリック内リンクの追加設定（Intra-fabric Links Additional Config）]：ファブリック内リンクに追加する CLI を追加します。

8. [リソース（Resources）] タブをクリックします。



[手動アンダーレイ IP アドレスの割り当て（Manual Underlay IP Address Allocation）]：VXLAN ファブリック管理を移行する場合は、このチェックボックスをオンにしないでください。

- デフォルトでは、DCNM は定義されたプールから動的にアンダーレイ IP アドレス リソース（ループバック、ファブリック インターフェイスなど）を割り当てます。このチェックボックスをオンにすると、割り当て方式が静的に切り替わり、動的 IP アドレス範囲フィールドの一部が無効になります。
- 静的割り当ての場合、REST API を使用してアンダーレイ IP アドレス リソースをリソース マネージャ（RM）に入力する必要があります。

  詳細については、『Cisco REST API 参照ガイド、リリース 11.2(2)』を参照してください。スイッチをファブリックに追加した後、REST APIを呼び出してから [保存して展開（Save & Deploy）] オプションを使用する必要があります。
- マルチキャスト レプリケーションに BIDIR-PIM 機能が選択されている場合、[アンダーレイ RP ループバック IP 範囲（Underlay RP Loopback IP Range）] フィールドは有効のままになります。
- 静的割り当てから動的割り当てに変更しても、現在の IP リソースの使用情況は維持されます。それ以後の IP アドレス割り当て要求のみが動的プールから取得されます。

[アンダーレイ ルーティング ループバック IP 範囲（Underlay Routing Loopback IP Range）]：プロトコル ピアリングのループバック IP アドレスを指定します。

[アンダーレイ VTEP ループバック IP 範囲（Underlay VTEP Loopback IP Range）]：VTEP のループバック IP アドレスを指定します。

[アンダーレイ RP ループバック IP 範囲（Underlay RP Loopback IP Range）]：エニーキャストまたはファントム RP の IP アドレス範囲を指定します。

[アンダーレイ サブネット IP 範囲（Underlay Subnet IP Range）]：インターフェイス間のアンダーレイ P2P ルーティング トラフィックの IP アドレスです。

[アンダーレイ MPLS ループバック IP 範囲（Underlay MPLS Loopback IP Range）]：アンダーレイ MPLS ループバック IP アドレス範囲を指定します。

Easy A の境界と Easy B の間の eBGP では、アンダーレイ ルーティング ループバックとアンダーレイ MPLS ループバック IP 範囲は一意の範囲である必要があります。他のファブリックの IP 範囲と重複しないようにしてください。重複すると、VPNv4 ピアリングが起動しません。

[レイヤ 2 VXLAN VNI 範囲（Layer 2 VXLAN VNI Range）] および [レイヤ 3 VXLAN VNI 範囲（Layer 3 VXLAN VNI Range）]：ファブリックの VXLAN VNI ID を指定します。

[ネットワーク VLAN 範囲（Network VLAN Range）] および **[VRF VLAN 範囲（VRF VLAN Range）]**：レイヤ 3 VRF およびオーバーレイ ネットワークの VLAN 範囲です。

[サブインターフェイス Dot1q 範囲（Subinterface Dot1q Range）]：L3 サブインターフェイスを使用する場合のサブインターフェイスの範囲を指定します。

[VRF Lite の展開（VRF Lite Deployment）]：ファブリック間接続を拡張するための VRF Lite 方式を指定します。

[VRF Lite サブネット IP 範囲（VRF Lite Subnet IP Range）] フィールドは、VRF LITE IFC が自動作成されるときに VRF LITE に使用される IP アドレス用に予約されたリソースを指定します。Back2BackOnly、ToExternalOnly、または Back2Back & ToExternal を選択すると、VRF LITE IFC が自動作成されます。

[自動展開両方（Auto Deploy Both）]：このチェックボックスは、対称 VRF Lite 展開に適用されます。このチェックボックスをオンにすると、自動作成された IFC の自動展開フラグが true に設定され、対称 VRF Lite 構成がオンになります。

このチェックボックスは、[VRF Lite 展開（VRF Lite Deployment）] フィールドが [手動（Manual）] に設定されていない場合に選択または選択解除できます。この場合、ユーザは自動作成された IFC の [自動展開（auto-deploy）] フィールドを明示的にオフにし、ユーザ入力には常に優先順位が与えられます。このフラグは、新しい自動作成 IFC にのみ影響し、既存の IFC には影響しません。

[VRF Lite サブネット IP 範囲（VRF Lite Subnet IP Range）] および [VRF Lite サブネットマスク（VRF Lite Subnet Mask）]：これらのフィールドには、DCI サブネットの詳細が入力されます。必要に応じて、次のフィールドを更新します。

画面に表示される値は自動的に生成されます。IP アドレス範囲、VXLAN レイヤ 2/レイヤ 3 ネットワーク ID 範囲、または VRF/ネットワーク VLAN 範囲を更新する場合は、次のことを確認します。

Note 値の範囲を更新する場合は、他の範囲と重複しないようにしてください。一度に更新できる値の範囲は 1 つだけです。複数の値の範囲を更新する場合は、別のインスタンスで実行します。たとえば、L2 と L3 の範囲を更新する場合は、次の手順を実行する必要があります。

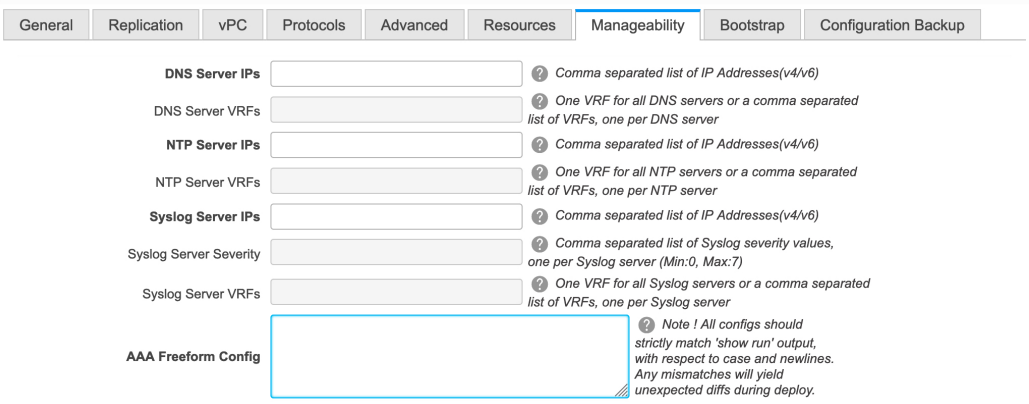
a. L2 範囲を更新し、[保存（Save）] をクリックします。

b. [ファブリックの編集（Edit Fabric）] オプションをもう一度クリックし、L3 範囲を更新して [保存（Save）] をクリックします。

[サービス ネットワーク VLAN 範囲（Service Network VLAN Range）]：[サービス ネットワーク VLAN 範囲（Service Network VLAN Range）] フィールドで VLAN 範囲を指定します。これはスイッチごとのオーバーレイ サービス ネットワーク VLAN 範囲です。最小許容値は 2 で、最大許容値は 3967 です。

[ルート マップ シーケンス番号範囲（Route Map Sequence Number Range）]：ルートマップのシーケンス番号の範囲を指定します。最小許容値は 1 で、最大許容値は 65534 です。

9. **管理能力（Manageability）** タブをクリックします。



このタブのフィールドは次のとおりです。

[DNS サーバ IP（DNS Server IPs）]：ドメイン ネーム システム（DNS) サーバの IP アドレス（v4/v6）のカンマ区切りリストを指定します。

[DNS サーバ VRF（DNS Server VRFs）]：すべての DNS サーバに 1 つの VRF を指定するか、DNS サーバごとに 1 つの VRF を、カンマ区切りリストで指定します。

[NTP サーバ IP（NTP Server IPs）]：NTP サーバの IP アドレス（v4/v6）のカンマ区切りリストを指定します。

[NTP サーバ VRF（NTP Server VRFs）]：すべての NTP サーバに 1 つの VRF を指定するか、NTP サーバごとに 1 つの VRF を、カンマ区切りリストで指定します。

[Syslog サーバ IP（Syslog Server IPs）]：syslog サーバの IP アドレスのカンマ区切りリスト（v4/v6）を指定します（使用する場合）。

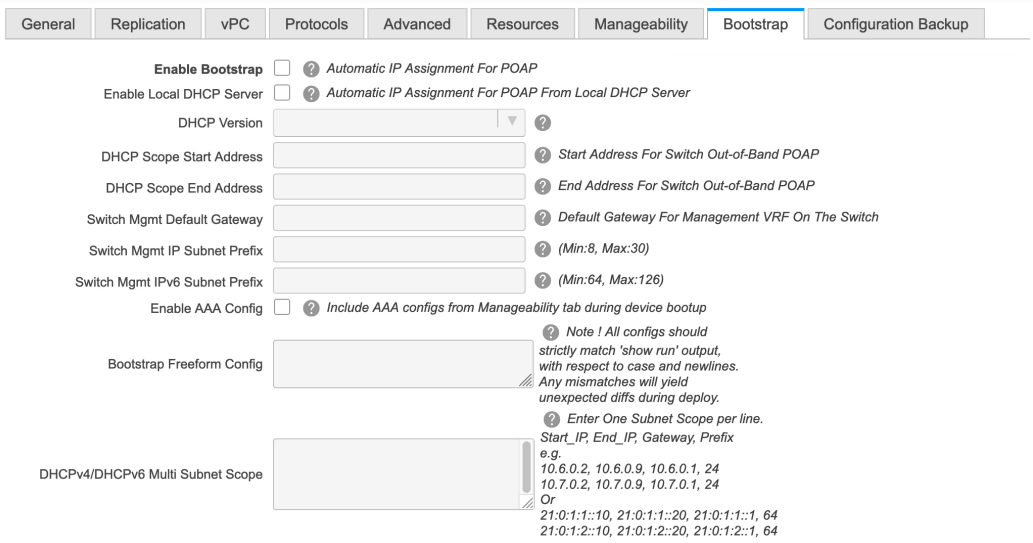
[Syslog サーバのシビラティ（重大度）（Syslog Server Severity）]：syslog サーバごとに 1 つの syslog シビラティ（重大度）値のカンマ区切りリストを指定します。最小値は 0 で、最大値は 7 です。高いシビラティ（重大度）を指定するには、大きい数値を入力します。

[Syslog サーバ VRF（Syslog Server VRFs）]：すべての syslog サーバに 1 つの VRF を指定するか、syslog サーバごとに 1 つの VRF を指定します。

[AAA 自由形式の構成（AAA Freeform Config）：AAA 自由形式の構成を指定します。

ファブリック設定で AAA 構成が指定されている場合は、ソースが [UNDERLAY_AAA]、説明が [AAA 構成（AAA Configurations）] の [switch_freeform PTI] が作成されます。

10. **[ブートストラップ（Bootstrap）]** タブをクリックします。



[ブートストラップの有効化（Enable Bootstrap）]：このチェックボックスを選択し、ブートストラップ機能を有効にします。ブートストラップを使用すると、新しいデバイスを day-0 段階で簡単にインポートし、既存のファブリックに組み込むことができます。ブートストラップは NX-OS POAP 機能を活用します。

ブートストラップをイネーブルにした後、次のいずれかの方法を使用して、DHCP サーバで IP アドレスの自動割り当てをイネーブルにできます。

- 外部 DHCP サーバ（External DHCP Server）：**[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]**および**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** 外部 DHCP サーバに関する情報を入力します。
- ローカル DHCPサーバ（Local DHCP Server）：[ローカル DHCP サーバ（Local DHCP Server）] チェックボックスをオンにして、残りの必須フィールドに詳細を入力します。

ローカル DHCP サーバーの有効化（Enable Local DHCP Server）：ローカル DHCP サーバーを介した自動 IP アドレス割り当ての有効化を開始するには、このチェックボックス

をオンにします。このチェックボックスをオンにすると、**[DHCP スコープ開始アドレス（DHCP Scope Start Address）]** および **[DHCP スコープ終了アドレス（DHCP Scope End Address）]** フィールドが編集可能になります。

このチェックボックスをオンにしない場合、DCNM は自動 IP アドレス割り当てにリモートまたは外部DHCPサーバを使用します。

[DHCP バージョン（DHCP Version）]：このドロップダウンリストから [DHCPv4] または [DHCPv6] を選択します。DHCPv4 を選択すると、**[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]** フィールドが無効になります。DHCPv6 を選択すると、**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** は無効になります。

Note Cisco Nexus 9000 および 3000 シリーズ スイッチは、スイッチがレイヤ 2 隣接（eth1 またはアウトオブバンド サブネットが /64 である必要がある）、または一部の IPv6 /64 サブネットにある L3 隣接である場合にのみ、IPv6 POAP をサポートします。/64 以外のサブネット プレフィックスはサポートされません。

[DHCP スコープ開始アドレス（DHCP Scope Start Address）] および [DHCP スコープ終了アドレス（DHCP Scope End Address）]：スイッチのアウトオブバンド POAP に使用される IP アドレス範囲の最初と最後の IP アドレスを指定します。

[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]：スイッチの管理 VRF のデフォルト ゲートウェイを指定します。

[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]：スイッチの Mgmt0 インターフェイスのプレフィックスを指定します。プレフィックスは 8 ～ 30 の間である必要があります。

DHCP スコープおよび管理デフォルト ゲートウェイ *IP* アドレスの仕様（*DHCP scope and management default gateway IP address specification*）：管理デフォルト ゲートウェイ IP アドレスを 10.0.1.1 に、サブネット マスクを 24 に指定した場合、DHCP スコープが指定したサブネット、10.0.1.2 ～ 10.0.1.254 の範囲内であることを確認してください。

[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]：スイッチの Mgmt0 インターフェイスの IPv6 プレフィックスを指定します。プレフィックスは 112 ー 126 の範囲で指定する必要があります。このフィールドは DHCP の IPv6 が有効な場合に編集できます。

[AAA 構成の有効化（Enable AAA Config）]：ブートストラップ後のデバイス起動構成の一部として [管理可能性（Manageability）] タブから AAA 構成を含めます。

[ブートストラップ フリーフォームの構成（Bootstrap Freeform Config）]：（オプション）必要に応じて追加のコマンドを入力します。たとえば、デバイスにプッシュするいくつかの追加の設定が必要であり、ポストデバイスブートストラップが使用可能である場合、このフィールドでキャプチャして要求のとおりに保存することが可能です。デバイスの起動後、**[ブートストラップ自由形式の構成（Bootstrap Freeform Config）** フィールドで定義された構成を含めることができます。

running-config をコピーして **[フリーフォームの設定（freeform config）]** フィールドに、NX-OS スイッチの実行設定に示されているように、正しいインデントでコピーアンドペーストします。freeform config は running config と一致する必要があります。詳細については、スイッチのフリーフォーム設定エラーの解決, on page 411を参照してください。

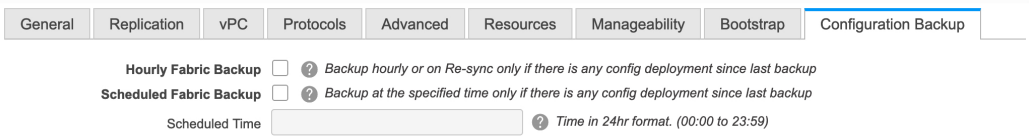
[DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）]：1行に1つのサブネット スコープを入力して、フィールドを指定します。**[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）]** チェックボックスをオンにした後で、このフィールドは編集可能になります。

スコープの形式は次の順で定義する必要があります。

[DHCP スコープ開始アドレス、DHCP スコープ終了アドレス、スイッチ管理デフォルト ゲートウェイ、スイッチ管理サブネット プレフィックス（DHCP Scope Start Address, DHCP Scope End Address, Switch Management Default Gateway, Switch Management Subnet Prefix）]

例：10.6.0.2、10.6.0.9、16.0.0.1、24

11. [構成のバックアップ（Configuration Backup）] タブをクリックします。このタブのフィールドは次のとおりです。



[毎時ファブリック バックアップ（Hourly Fabric Backup）]：ファブリック構成とインテントの毎時バックアップを有効にします。

時間単位のバックアップは、その時間の最初の 10 分間にトリガーされます。

[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]：毎日のバックアップを有効にします。このバックアップは、構成のコンプライアンスによって追跡されないファブリック デバイスの実行構成の変更を追跡します。

[スケジュール済みの時間（Scheduled Time）]：スケジュールされたバックアップ時間を 24 時間形式で指定します。[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）] チェックボックスをオンにすると、このフィールドが有効になります。

両方のチェックボックスをオンにして、両方のバックアップ プロセスを有効にします。

[保存（Save）]をクリックすると、バックアップ プロセスが開始されます。

スケジュールされたバックアップは、指定した時刻に最大 2 分の遅延でトリガーされます。スケジュールされたバックアップは、構成の展開ステータスに関係なくトリガーされます。

バックアップ構成ファイルは、DCNM にある次のパスに保存されます：`/usr/local/cisco/dcm/dcnm/data/archive`

保持できるアーカイブファイルの数は、[サーバ プロパティ（Server Properties）] ウィンドウの [保持するデバイスあたりのアーカイブ ファイル数（# Number of archived files per device to be retained:）] フィールドで設定します。

Note 即時バックアップをトリガーするには、次の手順を実行します。

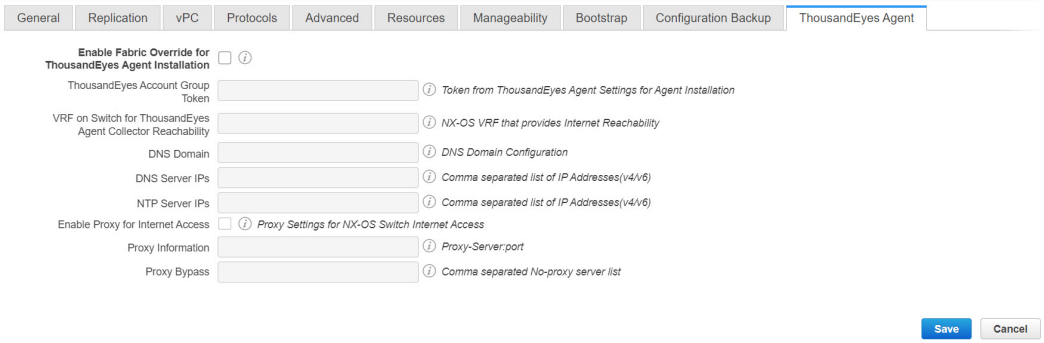
a. **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。[Fabric Builder] 画面が表示されます。

b. 特定のファブリック ボックス内をクリックします。[ファブリック トポロジ (fabric topology)] 画面が表示されます。

c. 画面左側の [アクション（Actions）] ペインで、[ファブリックの再同期（Re-Sync Fabric）] をクリックします。

ファブリック トポロジ ウィンドウでファブリック バックアップを開始することもできます。[アクション（Actions）] ペインで [今すぐバックアップ（Backup Now）] をクリックします。

12. **[ThousandEyes Agent]** タブをクリックします。この機能は、Cisco DCNM リリース 11.5（3）でのみサポートされています。詳細については、「Cisco DCNM での ThousandEyes Enterprise Agent のグローバル設定の構成」を参照してください。



このタブのフィールドは次のとおりです。

Note ThousandEyes Agent のファブリック設定はグローバル設定を上書きし、そのファブリック内のスイッチにインストールされているすべての ThousandEyes エージェントに同じ構成を適用します。

- **[ThousandEyes Agent インストールのファブリック オーバーライドを有効にする（Enable Fabric Override for ThousandEyes Agent Installation）]**：チェック ボックスを選択して、ファブリックで ThousandEyes Enterprise Agent を有効にします。

- **[ThousandEyes アカウント グループ トークン（ThousandEyes Account Group Token）]** : インストール用の ThousandEyes Enterprise Agent アカウント グループ トークンを指定します。
- **[ThousandEyes Agent コレクタ到達可能性のスイッチ上の VRF（VRF on Switch for ThousandEyes Agent Collector Reachability）]** : インターネットの到達可能性を提供する VRF データを指定します。
- **[ドメイン ネーム システム（DNS） ドメイン（DNS Domain）]** : スイッチのドメイン ネーム システム（DNS） ドメイン構成を指定します。
- **[ドメイン ネーム システム（DNS） サーバ IP（DNS Server IPs）]** : ドメイン ネーム システム（DNS） サーバの IP アドレス（v4/v6）のカンマ区切りリストを指定します。DNS サーバには、最大 3 つの IP アドレスを入力できます。
- **[NTP サーバ IP（NTP Server IPs）]** : Network Time Protocol (NTP) サーバの IP アドレス（v4/v6）のコンマ区切りリストを指定します。NTP サーバには、最大 3 つの IP アドレスを入力できます。
- **[プロキシを有効にする（Enable Proxy）]** : チェックボックスをオンにして、NX-OS スイッチのインターネット アクセスのプロキシ設定を選択します。
- **[プロキシ情報（Proxy Information）]** : プロキシ サーバのポート情報を指定します。
- **[プロキシ バイパス（Proxy Bypass）]** : プロキシをバイパスするサーバ リストを指定します。

13. 関連情報を入力して更新したら、**[保存（Save）]** をクリックします。画面の右下に、ファブリックが作成されたことを示すメモが短時間表示されます。ファブリックが作成されると、ファブリックのページが表示されます。画面左上に生地名が表示されます。

(同時に、新しく作成されたファブリック インスタンスが **[ファブリック ビルダ（Fabric Builder）]** 画面に表示されます。**[ファブリック ビルダ（Fabric Builder）]** 画面に移動するには、**[アクション（Actions）]** ペインの上にある左矢印（**[←]**）ボタン [画面の左側] をクリックします。

[アクション（Actions）] ペインでは、さまざまな機能を実行できます。それらの 1 つは、ファブリックにスイッチを追加する **[スイッチの追加（Add switches）]** オプションです。ファブリックを作成したら、ファブリック デバイスを追加する必要があります。オプションについて説明します：

- **[表形式の表示（Tabular View）]** : デフォルトでスイッチはトポロジ表示として映されます。このオプションを使用して、表形式のビューでスイッチを表示します。
- **[トポロジの更新（Refresh topology）]** : トポロジを更新できます。
- **[レイアウトの保存（Save Layout）]** : トポロジのカスタム 表示を保存します。トポロジに特定のビューを作成し、使いやすいように保存できます。
- **[保存されたレイアウトの削除（Delete saved layout）]** : トポロジのカスタム 表示を削除します。

- **[トポロジ表示（Topology views）]**：保存されたレイアウトの表示オプションは、階層型、ランダム、およびカスタムから選択できます。
  - **[階層型（Hierarchical）]**：トポロジのアーキテクチャ表示を表示。CLOS トポロジの構成方法に関するノードを示すさまざまなスイッチロールを定義できます。
  - **[ランダム（Random）]**：ノードはウィンドウ上にランダムに配置されます。DCNMは、推測を行い、近接するノードをインテリジェントに配置しようとします。
  - **[カスタム保存レイアウト（Custom saved layout）]**：ノードを好きなようにドラッグできます。好きな位置に配置したら、レイアウトの保存をクリックして位置を記憶することができます。次回トポロジにアクセスすると、DCNMにより最後に保存したレイアウト位置に基づいてノードが描画されます。
- **[ファブリックの復元（Restore Fabric）]**：ファブリックを以前の DCNM 構成状態に復元できます（1 か月前、2 か月前など）。詳細については、「ファブリックの復元」セクションを参照します。
- **[今すぐバックアップ（Backup Now）]**：**[今すぐバックアップ（Backup Now）]** をクリックして、ファブリックバックアップを手動で開始できます。タグの名前を入力して、**[OK]** をクリックします。**[ファブリック設定（Fabric Settings）]** ダイアログボックスの **[構成バックアップ（Configuration Backup）]** タブで選択した設定に関係なく、このオプションを使用してバックアップを開始できます。
- **[ファブリックの再同期Resync Fabric（Resync Fabric）]**：大規模なアウトオブバンド変更がある場合、または構成変更が DCNM に正しく登録されていない場合に、このオプションを使用して DCNM 状態を再同期します。再同期操作は、ファブリックスイッチに対して完全な CC 実行を実行し、「show run」および「show run all」コマンドをスイッチから再収集します。再同期プロセスを開始すると、進行状況メッセージがウィンドウに表示されます。再同期中に、実行構成がスイッチから取得されます。次に、スイッチの Out-of-Sync/In-Sync ステータスは、DCNM で定義された意図または予想される構成と、スイッチから取得された現在実行中の構成に基づいて再計算されます。
- **[スイッチを追加（Add Switches）]**：ファブリックにスイッチ インスタンスを追加しすることを許可します。
- **[ファブリック設定（Fabric Settings）]**：ファブリック設定を表示または編集できます。
- **[クラウド（Cloud）]**アイコン：**[クラウド（Cloud）]**アイコンをクリックして、**[未検出（Undiscovered）]** のクラウドを表示（または非表示に）します。

  アイコンをクリックすると、未検出のクラウドと、選択したファブリックトポロジへのリンクは表示されません。

  [未検出（Undiscovered）] クラウドを表示するために**[クラウド（Cloud）]**アイコンをまたクリックします。

[範囲（SCOPE）]：右上の[範囲（SCOPE）]ドロップダウンボックスを使用して、ファブリックを切り替えることができます。現在のファブリックは、強調表示されます。MSD とそのメンバーファブリックが明確に表示され、メンバーファブリックはMSDファブリックの下にくぼんで表示されます。

ファブリックへのスイッチの追加

各ファブリックのスイッチは一意であるため、各スイッチは1つのファブリックにのみ追加できます。

[アクション（Actions）]パネルから**[スイッチの追加（Add Switches）]**オプションをクリックして、DCNMで作成されたファブリックにスイッチを追加します。**[インベントリ管理（Inventory Management）]**画面が表示されます。画面には2つのタブがあり、1つは既存のスイッチを検出するためのもので、もう1つは新しいスイッチを検出するためのものです。両方のオプションについて説明します。

さらに、スイッチとインターフェイスを事前プロビジョニングできます。詳細については、デバイスの事前プロビジョニング , on page 104およびイーサネット インターフェイスの事前プロビジョニング, on page 109を参照してください。

Note DCNM でピリオド文字（.）を含むホスト名を持つスイッチが検出されると、ドメイン名として扱われ、切り捨てられます。ピリオド文字（.）の前のテキストのみがホスト名と見なされます。次に例を示します。

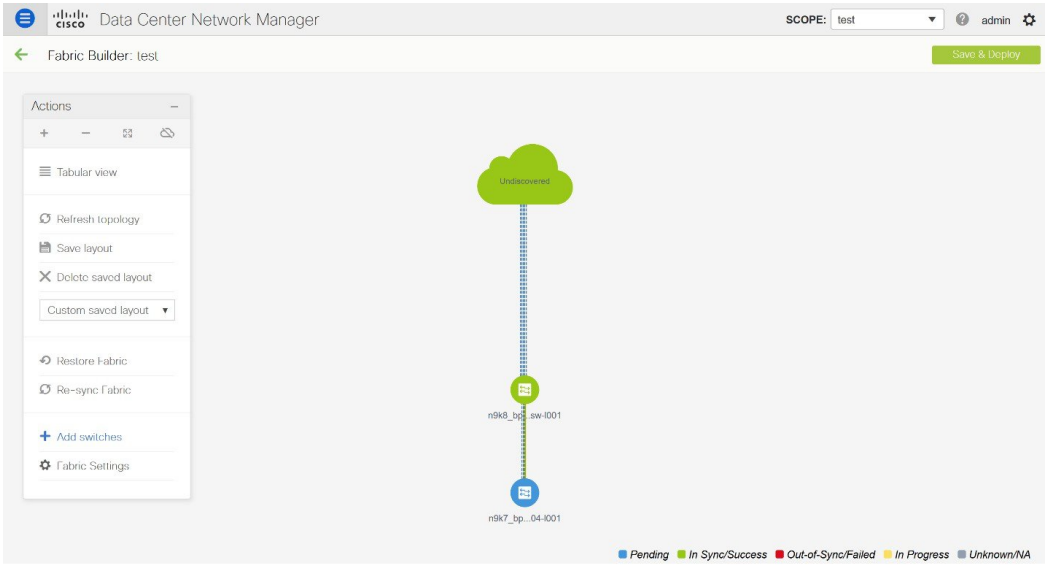
- ホスト名が **[leaf.it.vxlan.bgp.org1-XYZ]** の場合、DCNM で **[leaf]** のみが表示されます。
- ホスト名が **[leaf-itvxlan.bgp.org1-XYZ]** の場合、DCNM で **[leafit-vxlan]** のみが表示されます。

新しいスイッチの検出

1. 新しい Cisco NX-OS デバイスの電源がオンになると、通常、そのデバイスにはスタートアップ構成も構成ステートもありません。その結果、NX-OS で電源が投入され、初期化後に POAP ループに入ります。デバイスは、mgmt0 インターフェイスを含むアップ状態のすべてのインターフェイスで DHCP 要求の送信を開始します。
2. デバイスとDCNMの間にIP到達可能性がある限り、デバイスからのDHCP要求はDCNMに転送されます。ゼロデイデバイスを簡単に起動するには、前述のように、**ファブリック設定**でブート ストラップ オプションを有効にする必要があります。
3. ファブリックに対してブートストラップが有効になっている場合、デバイスからのDHCP要求は DCNM によって処理されます。DCNM によってデバイスに割り当てられた一時

IP アドレスは、デバイス モデル、デバイス NX-OS バージョンなどを含むスイッチに関する基本情報を学習するために使用されます。

4. DCNM GUI で、ファブリックに移動します（**[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** をクリックし、ファブリックをクリックします）。ファブリック トポロジが表示されます。



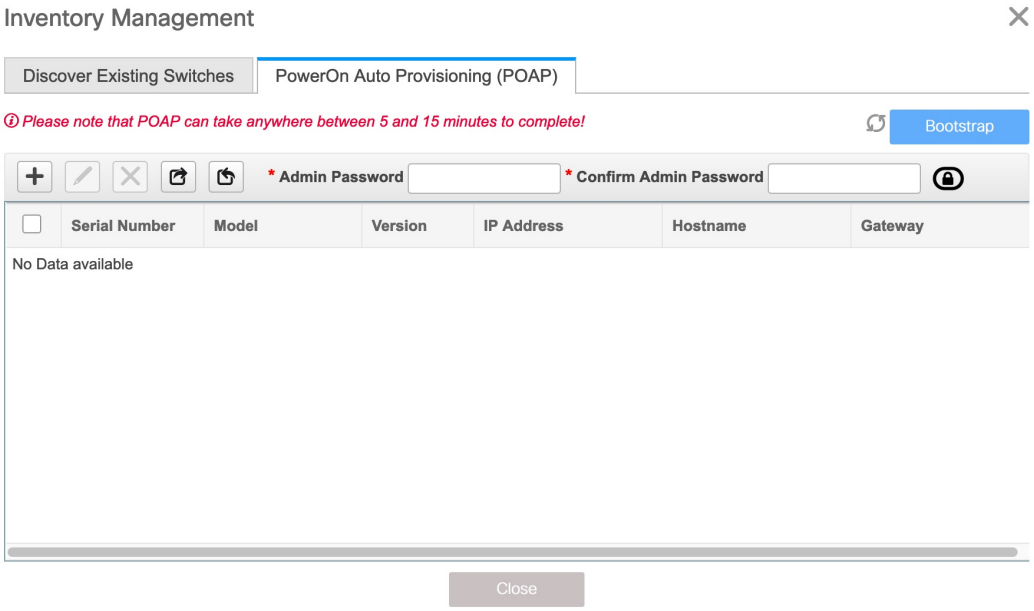
ファブリック トポロジ ウィンドウに移動し、**[アクション（Actions）]** パネルから **[スイッチの追加（Add switches）]** オプションをクリックします。[インベントリ管理（Inventory Management）] ウィンドウが表示されます。

5. **[POAP]** タブをクリックします。

前述のように、DCNM はデバイスからシリアル番号、モデル番号、およびバージョンを取得し、それらを [インベントリ管理（Inventory Management）] ウィンドウに表示します。また、IP アドレス、ホスト名、およびパスワードを追加するオプションが使用可能になります。スイッチ情報が取得されない場合は、ウィンドウを更新します。

Note

- ウィンドウの左上には、スイッチ情報を含む .csv ファイルをエクスポートおよびインポートするためのエクスポートおよびインポートオプションがあります。インポート オプションを使用してデバイスを事前プロビジョニングすることもできます。



スイッチの横にあるチェックボックスを選択し、スイッチのクレデンシャル（IP アドレスとホスト名）を入力します。

デバイスの IP アドレスに基づいて、**[IP アドレス（IP Address）]** フィールドに IPv4 または IPv6 アドレスを追加できます。

リリース 11.2(1) 以降、デバイスを事前にプロビジョニングできます。デバイスの事前プロビジョニングについては、デバイスの事前プロビジョニング , on page 104 を参照してください。

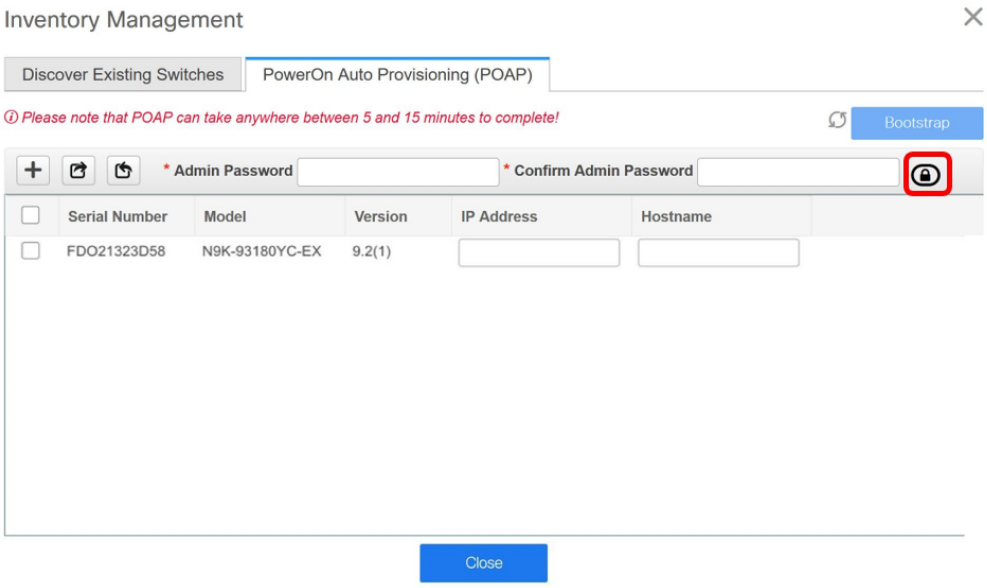
6. **[管理者パスワード（Admin Password）]** フィールドと **[管理者パスワードの確認（Confirm Admin Password）]** フィールドに、新しいパスワードを入力します。

   この管理者パスワードは、POAP ウィンドウに表示されるすべてのスイッチに適用されます。

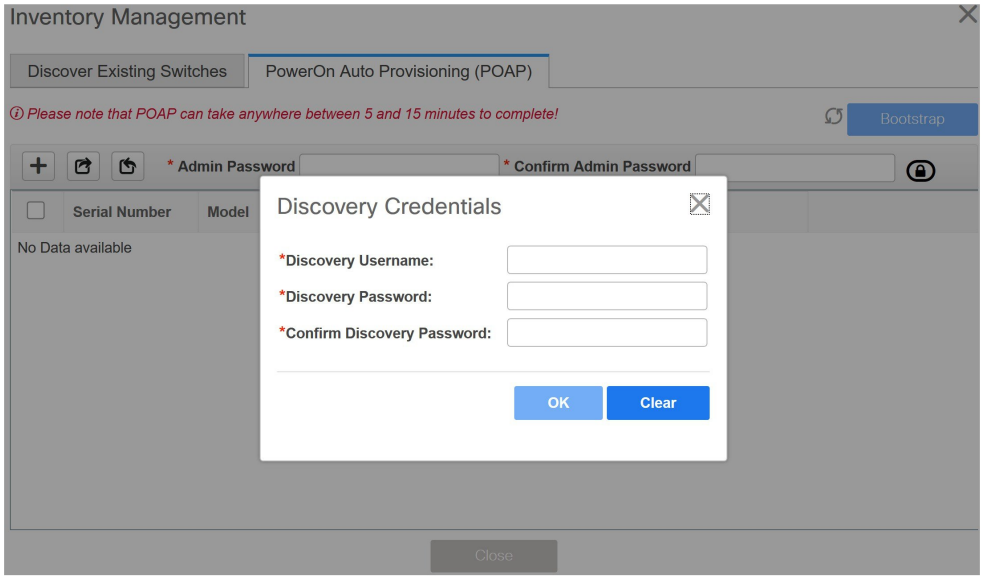
Note 管理者クレデンシャルを使用してスイッチを検出しない場合は、代わりに AAA 認証（RADIUS または TACACS クレデンシャル）を使用できます。

7. （任意）スイッチの検出に検出クレデンシャルを使用します。

   a. **[ディスカバリ クレデンシャルの追加（Add Discovery Credentials）]** アイコンをクリックして、スイッチのディスカバリ クレデンシャルを入力します。



b. **[ディスカバリ クレデンシャル（Discovery Credentials）]** ウィンドウで、ディスカバリ ユーザ名やパスワードなどのディスカバリ クレデンシャルを入力します。



[OK] をクリックして、ディスカバリ クレデンシャルを保存します。

検出クレデンシャルが指定されていない場合は、DCNM は管理者ユーザとパスワードを使用してスイッチを検出します。

8. 画面右上の **[ブートストラップ（Bootstrap）]** をクリックします。

DCNM は管理IPアドレスおよびその他のクレデンシャルをスイッチにプロビジョニングします。この単純化された POAP プロセスでは、すべてのポートが開かれます。

9. 最新情報を入手するには、**[トポロジの更新（Refresh Topology）]** ボタンをクリックします。追加されたスイッチは、POAP サイクルを実行します。スイッチをモニタし、POAP 完了を確認します。

10. 追加されたスイッチが POAP を完了すると、ファブリック ビルダ トポロジページが追加されたスイッチで更新され、検出された物理接続が示されます。スイッチに適切なロールを設定し、ファブリック レベルで [保存と展開（Save & Deploy）] 操作を実行します。ファブリック設定、スイッチロール、トポロジなどが Fabric Builder によって評価され、スイッチの適切な意図された設定が保存操作の一部として生成されます。保留中の設定は、新しいスイッチをインテントと同期させるために新しいスイッチに導入する必要がある設定のリストを提供します。

Note ファブリックで変更が発生して Out-of-Sync が発生した場合は、変更を展開する必要があります。このプロセスは、「既存スイッチの検出」の項で説明したものと同じです。

ファブリックの作成時に、**[管理性（Manageability）]** タブに AAA サーバ情報を入力した場合は、各スイッチの AAA サーバパスワードを更新する必要があります。そうでない場合、スイッチの検出は失敗します。

11. 保留中の設定が展開されると、すべてのスイッチの **[進捗（Progress）]** 列に 100% と表示されます。

12. **[閉じる（Close）]** をクリックして、ファブリック ビルダ トポロジに戻ります。

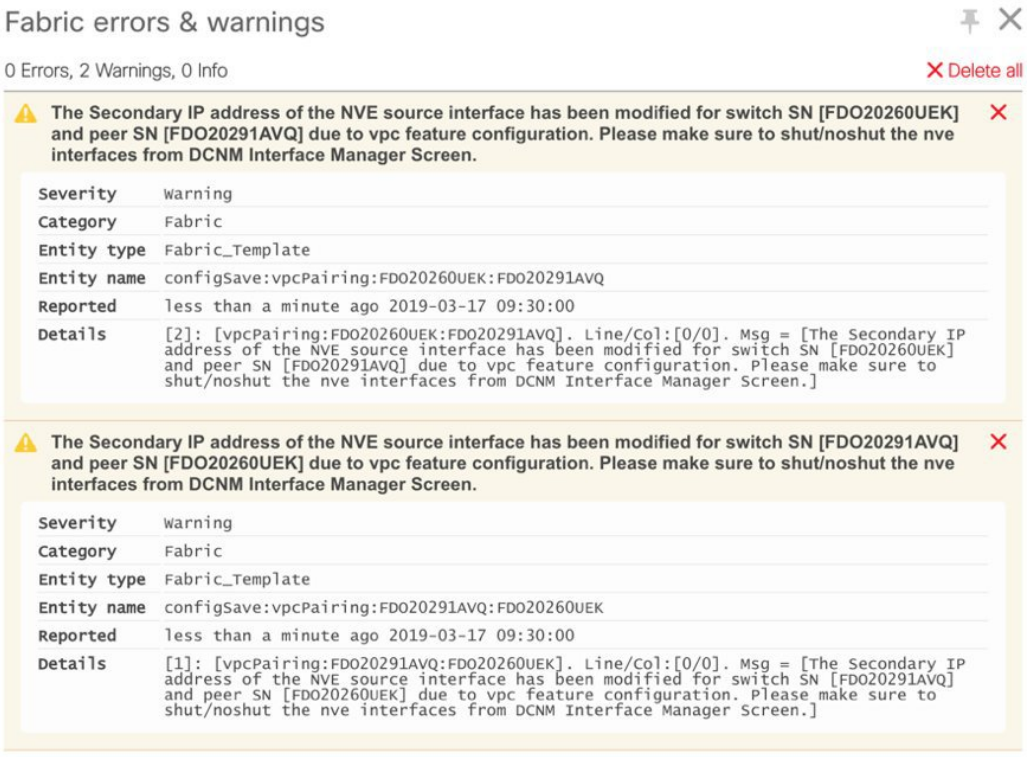
13. **[トポロジの更新（Refresh Topology）]** をクリックして、更新を表示します。すべてのスイッチは、機能していることを示す緑色でなければなりません。

14. スイッチとリンクが DCNM で検出されます。設定は、さまざまなポリシー（ファブリック、トポロジ、スイッチ生成ポリシーなど）に基づいて構築されます。スイッチイメージ（およびその他の必要な）設定がスイッチで有効になっている。

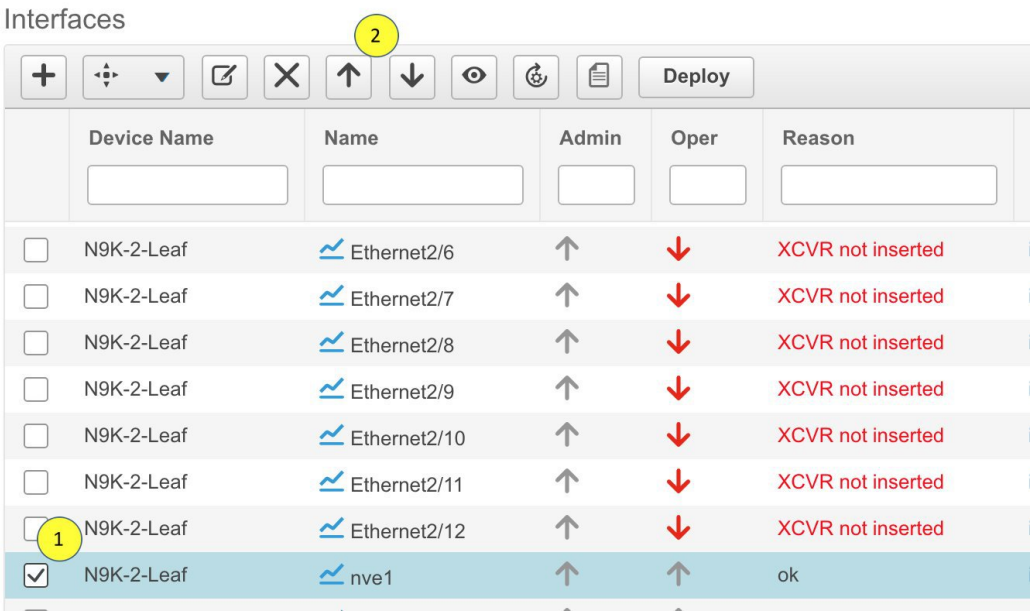
15. DCNM GUIでは、検出されたスイッチは スタンドアロン ファブリック トポロジで確認できます。このステップまでで、POAP は基本設定で完了します。追加構成を行うには、**[制御（Control）] > [インターフェイス（Interfaces）]** オプションを使用してインターフェイスを設定する必要があります。以下が含まれますが、これらに限定されません。

    - vPC ペアリング。
    - ブレークアウト インターフェイス。
    - ポートチャネル、およびポートへのメンバーの追加。

    vPCのペアリング/ペアリング解除または advertise-pip オプションを有効または無効にするか、マルチサイト構成を更新する場合は、**[保存と展開（Save & Deploy）]** 操作を使用する必要があります。操作の終了時に、nve インターフェイスで **shutdown** または **no shutdown** コマンドを設定するように求めるエラーが表示されます。vPC 設定を有効にした場合のエラー スクリーンショットのサンプル：



解決するには、[制御（Control）]>[インターフェイス（Interfaces）]画面に移動し、nve インターフェイスでシャットダウン操作を展開してから、No Shutdown 構成を実行します。これを次の図に示します。上矢印は No Shutdown 操作に対応し、下矢印はShutdown 操作に対応します。



スイッチを右クリックすると、さまざまなオプションを表示できます。

- **ロールの設定**：スイッチにロールを割り当てます（スパイン、ボーダーゲートウェイなど）。

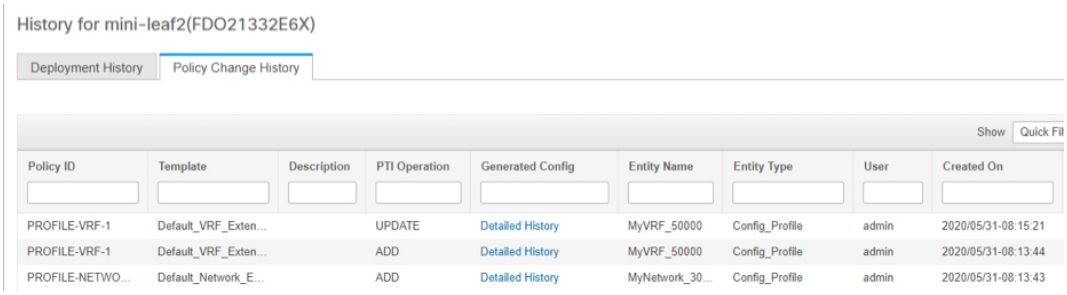
Note

- スイッチのロールの変更は、**[保存と展開（Save & Deploy）]** を実行する前にのみ許可されます。
- DCNM 11.1(1) 以降、スイッチのロールは、スイッチ上にオーバーレイがない場合に変更できますが、スイッチ操作, on page 244 で指定された許可されたスイッチ ロール変更のリストに従ってのみ変更できます。

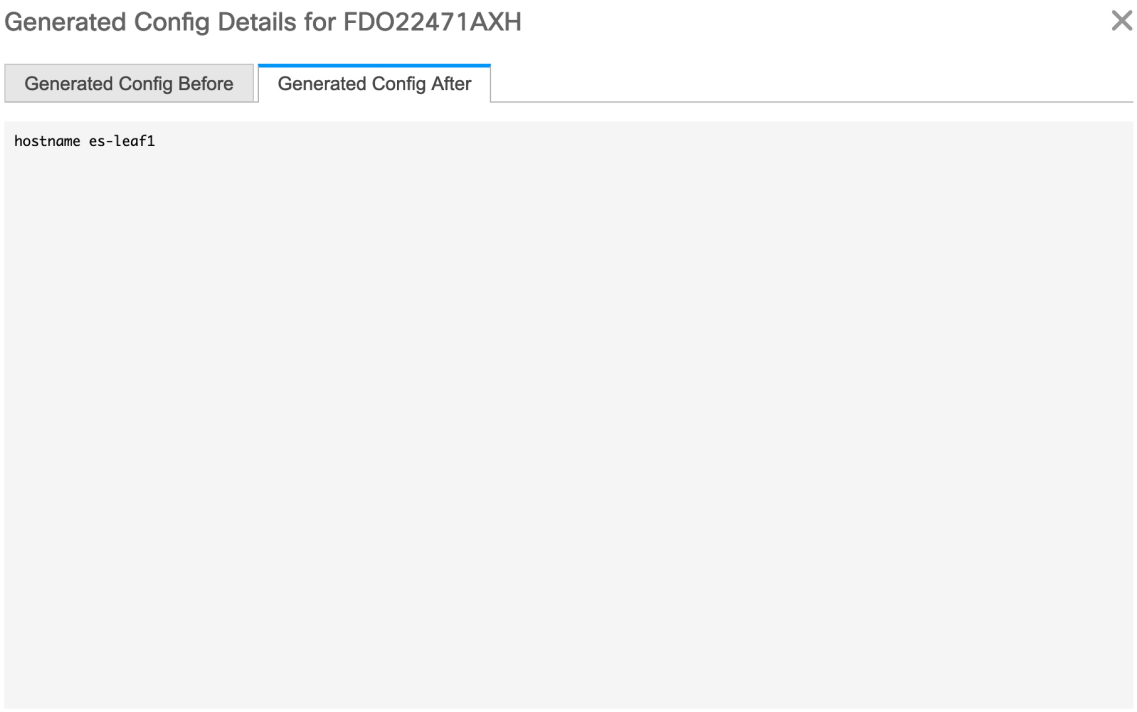
- **モード**：メンテナンス モードとアクティブ/操作モード。
- **vPC** ペアリング：vPC のスイッチを選択し、そのピアを選択します。

  vPCペアの仮想リンクを作成するか、既存の物理リンクをvPCペアの仮想リンクに変更できます。
- **インターフェイスの管理**：スイッチ インターフェイスに構成を展開します。
- **ポリシーの表示/編集**：スイッチ ポリシーを参照し、必要に応じて編集します。
- **履歴**：スイッチの展開およびポリシーの変更履歴を表示します。

  [ポリシー変更履歴（Policy Change History）]タブには、追加、更新、削除などの変更を行ったユーザとともにポリシーの履歴が一覧表示されます。



ポリシーの **[ポリシー変更履歴（Policy Change History）]** タブで、**[生成された構成（Generated Config）]** 列の **[詳細な履歴（Detailed History）]** をクリックして、前後の生成された構成を表示します。



次の表に、ポリシーテンプレートインスタンス（PTI）の前後に生成される構成の概要を示します。

PTI の操作	前に生成された構成	生成後の構成
追加	Empty	構成が含まれています
更新	変更前の構成が含まれています	変更後の構成が含まれています
マーク - 削除	削除する設定が含まれます。	色を変更して削除する構成が含まれます。
削除	構成が含まれています	Empty

Note ポリシーまたはプロファイルテンプレートが適用されると、テンプレートのアプリケーションごとにインスタンスが作成されます。これは、ポリシー テンプレート インスタンスまたは PTI と呼ばれます。

- **[構成のプレビュー（Preview Config）]**：保留中の構成と、実行中の構成と予想される構成の比較を表示します。
- **展開構成** - スイッチ構成ごとに展開します。

- 検出：このオプションを使用して、スイッチのクレデンシャルを更新し、スイッチをリロードし、スイッチを再検出し、ファブリックからスイッチを削除できます。

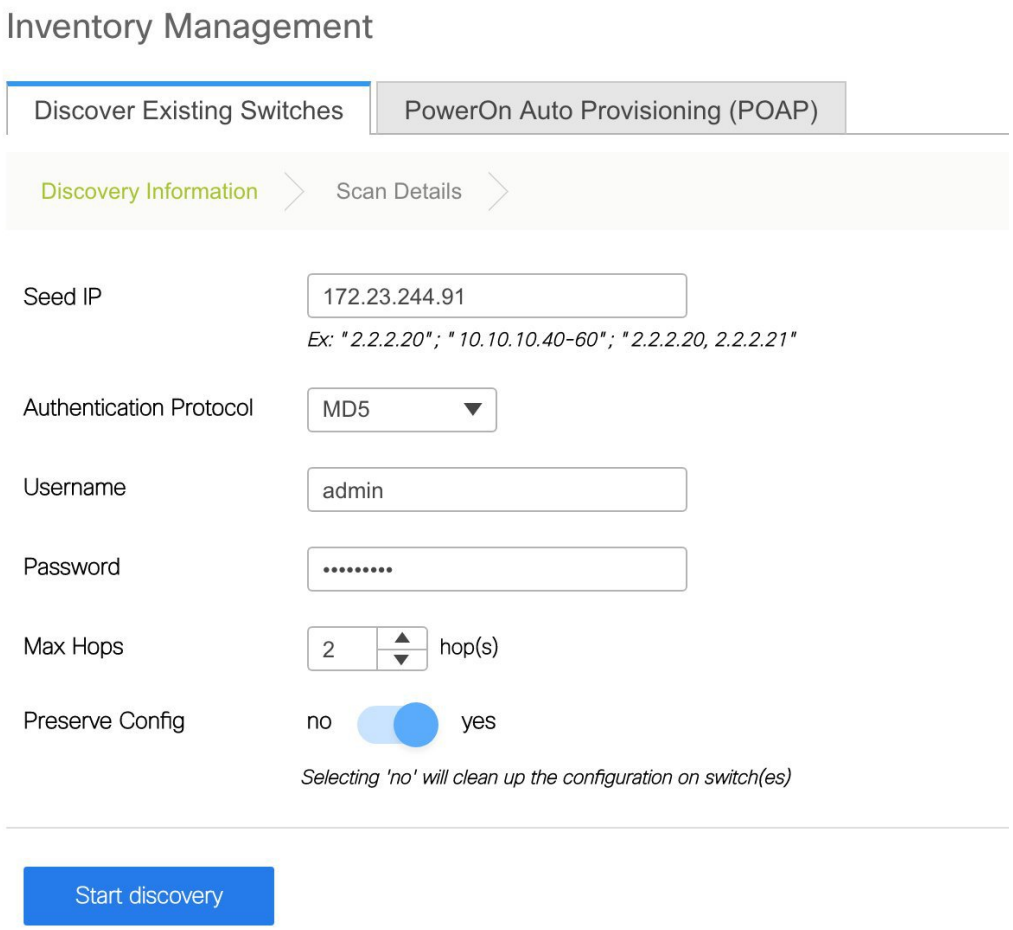
新しいファブリックが作成され、ファブリック構成スイッチが DCNM で検出され、アンダーレイ構成がそれらのスイッチでプロビジョニングされ、DCNM との間の構成が同期されます。その他のタスクは、次のとおりです。

- vPC、ループバック インターフェイス、サブインターフェイス設定などのインターフェイス構成をプロビジョニングします。[「インターフェイス」を参照してください]。
- ネットワークを作成し、スイッチに展開します。[「ネットワークおよび VRF の作成と展開 」を参照してください]。

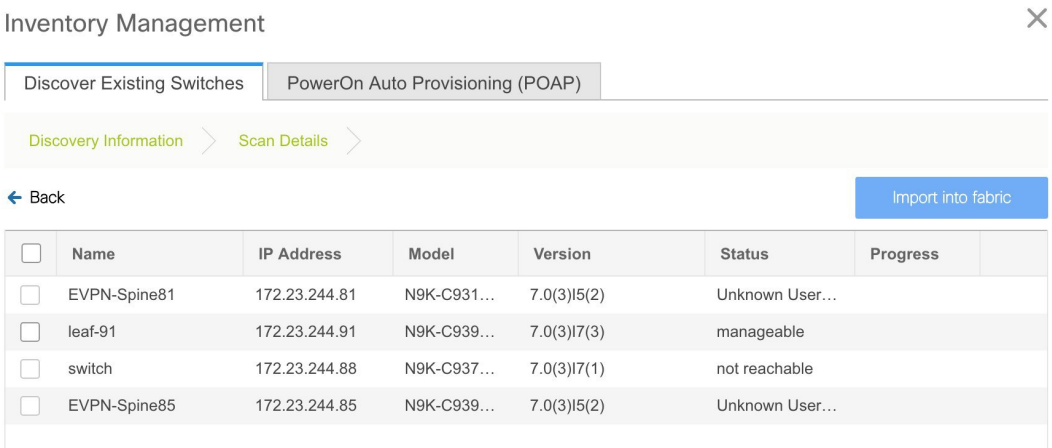
既存のスイッチの検出

1. **[スイッチの追加（Add Switches）]** をクリックした後、**[既存のスイッチの検出（Discover Existing Switches）]** タブを使用して、1 つ以上の既存のスイッチをファブリックに追加します。この場合、既知のクレデンシャルと事前プロビジョニングされた IP アドレスを持つスイッチがファブリックに追加されます。スイッチの IP アドレス（シード IP）、管理者名、ユーザー名、およびパスワード（**[ユーザー名（Username）]** フィールドと **[パスワード（Password）]** フィールド）は、ユーザーによる入力として提供されます。**[構成の保持（Preserve Config）]** ノブは、デフォルトで **[yes]** に設定されています。これは、ファブリックへのデバイスのブラウンフィールドインポートに対してユーザが選択するオプションです。デバイス構成がインポートプロセスの一部としてクリーンアップされるグリーンフィールド インポートの場合、ユーザーは **[構成の保持（Preserve Config）]** ノブを **[no]** に設定する必要があります。

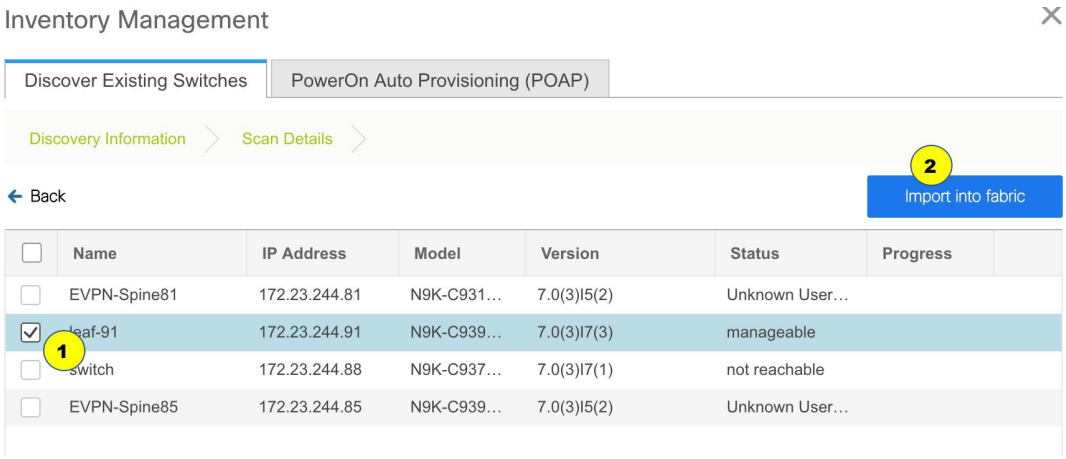
Note Easy_Fabric_eBGP は、ファブリックへのデバイスのブラウンフィールドインポートをサポートしていません。



2. [検出の開始（Start discovery）] をクリックします。**[スキャン詳細（Scan Details）]** ウィンドウが間もなく表示されます。**[最大ホップ（Max Hops）]** フィールドに 2 が入力されているため（デフォルト）、指定された IP アドレス（リーフ 91）を持つスイッチとそのスイッチからの 2 つのホップが **[スキャン詳細（Scan Details）]** の結果に入力されます。



3. DCNM がスイッチに対して正常なシャロー検出を実行できた場合、ステータスに **[管理性（Manageable）]** と表示されます。適切なスイッチの横にあるチェックボックスをオンにして、**[ファブリックにインポート（Import into fabric）]** をクリックします。



この例では 1 つのスイッチの検出について説明しますが、複数のスイッチを同時に検出できます。

スイッチ検出プロセスが開始されます。**[進行状況（Progress）]** 列には、選択したすべてのスイッチの進行状況が表示されます。完了時に各スイッチの**完了**を表示します。

Note 選択したすべてのスイッチがインポートされるか、エラーメッセージが表示されるまで、画面を閉じないでください（また、スイッチを再度追加してください）。

エラー メッセージが表示された場合は、画面を閉じます。[ファブリック トポロジ(fabric topology)] 画面が表示されます。エラーメッセージは、画面の右上に表示されます。必要に応じてエラーを解決し、[アクション（Actions）] パネルの **[スイッチの追加（Add Switches）]** をクリックしてインポート プロセスを再度開始します。

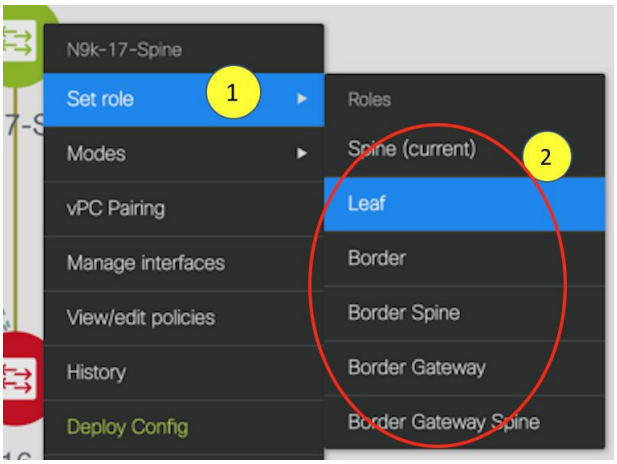
DCNM がすべてのスイッチを検出し、[進行状況（Progress）] 列にすべてのスイッチの **[done]** が表示されたら、画面を閉じます。*[*スタンドアロン ファブリック トポロジ（Standalone fabric topology）] 画面が再び表示されます。追加されたスイッチのスイッチアイコンが表示されます。

Note スイッチの検出中に次のエラーが発生することがあります。

4. 最新のトポロジ ビューを表示するには、**[トポロジの更新（Refresh topology）]** をクリックします。

すべてのスイッチが追加され、ロールが割り当てられると、ファブリック トポロジにはスイッチとスイッチ間の接続が含まれます。

5. デバイスを検出したら、各デバイスに適切なロールを割り当てます。このためには、デバイスをクリックし、**[ロールの設定]** オプションを使用して適切なロールを設定します。代わりに、表形式のビューを使用して、一度に複数のデバイスに同じロールを割り当てることもできます。



表示用に階層レイアウトを選択すると（[アクション（Actions）] パネルで）、トポロジはロールの割り当てに従って自動的に配置され、リーフ デバイスが下部に、スパイン デバイスが上部に接続され、境界デバイスが上部に配置されます。

vPC スイッチ ロールの割り当て：スイッチのペアを vPC スイッチ ペアとして指定するには、スイッチを右クリックし、スイッチのリストから vPC ピア スイッチを選択します。

AAA サーバ パスワード：（**[管理性（Manageability）]** タブで）AAA サーバ情報を入力した場合は、各スイッチで AAA サーバ パスワードを更新する必要があります。そうでない場合、スイッチの検出は失敗します。

Cisco DCNM を使用して新しい vPC ペアが正常に作成および展開されると、コマンドがスイッチに存在する場合でも、**no ip redirects** CLI のいずれかのピアが同期しなくなることがあります。この非同期は、実行構成で CLI を表示するためのスイッチの遅延が原因で発生

し、構成のコンプライアンスに相違が生じます。**[構成の展開（Config Deployment）]** ウィンドウでスイッチを再同期して、差分を解決します。

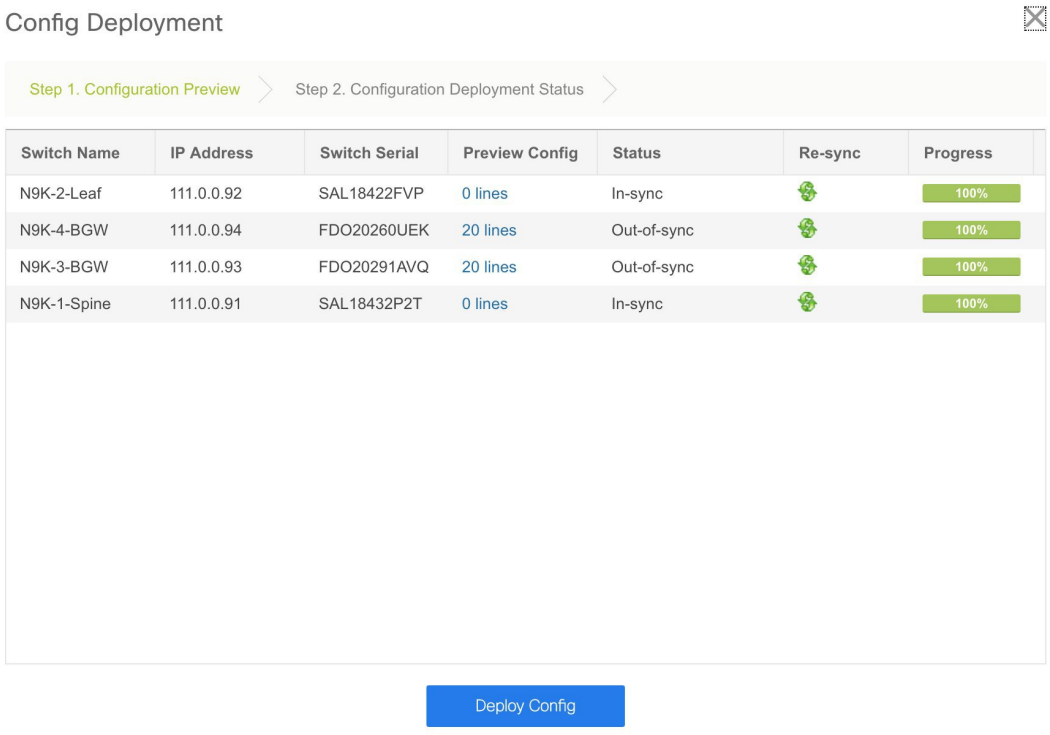
6. 画面の右上にある **[保存と展開（Save & Deploy）]** をクリックします。

テンプレートとインターフェイスの設定は、スイッチのアンダーレイ ネットワーク構成を形成します。また、ファブリック構成の一部として入力されたフリーフォーム CLI（[詳細（Advanced）]タブで入力されたリーフおよびスパイン スイッチのフリー フォーム設定）も展開されます。自由形式構成の詳細については、「ファブリック スイッチでのフリーフォーム設定の有効化」を参照してください。

構成のコンプライアンス：プロビジョニングされた構成とスイッチの構成が一致しない場合、**[ステータス（Status）]** 列に非同期が表示されます。たとえば、CLI を使用してスイッチの機能を手動で有効にすると、設定が一致しなくなります。

Cisco DCNM からファブリックにプロビジョニングされた構成が正確であることを確認したり、逸脱（アウトオブバンド変更など）を検出したりするために、DCNM の構成コンプライアンス エンジンは、必要な修復構成を報告し、提供します。

[保存と展開（Save & Deploy）] をクリックすると、**[構成の展開（Config Deployment）]** ウィンドウが表示されます。



ステータスが非同期の場合は、デバイスの DCNM との構成に不整合があることを示しています。

[再同期（Re-sync）] 列のスイッチごとに [再同期（Re-sync）] ボタンが表示されます。大規模なアウトオブバンド変更がある場合、または設定変更が DCNM に正しく登録されていない場合に、このオプションを使用して DCNM 状態を再同期します。再同期操作は、

スイッチに対して完全な CC 実行を実行し、「show run」および「show run all」コマンドをスイッチから再収集します。再同期プロセスを開始すると、進行状況メッセージが画面に表示されます。再同期中に、実行構成がスイッチから取得されます。スイッチの Out-of-Sync/In-Sync ステータスは、DCNM で定義されたインテントに基づいて再計算されます。

[構成のプレビュー（Preview Config）] 列エントリ（特定の行数で更新）をクリックします。[構成のプレビュー (Config Preview)] 画面が表示されます。

[保留中の構成（PendingConfig）] タブには、正常な展開の保留中の構成が表示されます。

[Side-by-sideComparison] タブには、現在の構成と予想される構成が一緒に表示されます。

DCNM 11 では、複数行のバナー motd 構成がサポートされています。マルチライン バナー motd 構成は、**switch_freeform** を使用するスイッチごと、またはリーフ/スパイン自由形式構成を使用するファブリックごとのいずれかで、自由形式の構成ポリシーを使用して Cisco DCNM で構成できます。複数行のバナー motd が構成された後、ファブリック トポロジ画面（の右上）で **[保存と展開（Save & Deploy）]** オプションを実行して、ポリシーを展開します。そうしないと、ポリシーがスイッチに適切に展開されない可能性があります。**バナー**ポリシーは、単一行のバナー設定のみを設定します。また、自由形式の設定/ポリシーに関連するバナーは1つだけ作成できます。バナー motd を構成するための複数のポリシーはサポートされていません。

7. 画面 を閉じます。

   構成展開の画面で、画面下部の [構成の展開（Deploy Config）] をクリックして、保留中の構成をスイッチに展開開始します。[ステータス（Status）] カラムには、「FAILED」または「SUCCESS」の状態が表示されます。FAILED ステータスの場合は、問題の解決に失敗した理由を調査します。

   構成が正常にプロビジョニングされた後（すべてのスイッチで 100% の進捗が表示された場合）、画面を閉じます。

   ファブリック トポロジが表示されます。構成が成功すると、スイッチのアイコンが緑色に変わります。

   スイッチ アイコンが赤色の場合、スイッチと DCNM の構成が同期していないことを示します。スイッチで展開が保留中の場合、スイッチは青色で表示されます。保留状態は、保留中の展開または保留中の再計算があることを示します。スイッチをクリックし、**[プレビュー（Preview）]** または **[構成の展開（Deploy Config）]** オプションを使用して保留中の展開を確認するか、**[保存と展開（Save & Deploy）]** をクリックしてスイッチの状態を再計算できます。

Note CLI の実行で警告またはエラーが発生した場合は、**[Fabric Builder]** ウィンドウに通知が表示されます。自動解決可能な警告またはエラーには、**[解決（Resolve）]** オプションがあります。

スイッチのリロードまたはRMA操作の後にリーフスイッチが起動すると、DCNMは、スイッチとそれに接続されているFEXデバイスの構成をプロビジョニングします。DCNMがFEX（ホストインターフェイス）構成をプロビジョニングした後にFEX接続が起動し、構成が一致しない場合があります。不一致を解決するには、ファブリック トポロジ画面で**[保存と展開（Save & Deploy）]**を再度クリックします。

Cisco NX-OS リリース 11.4(1) 以降、**[トポロジ（Topology）]**ウィンドウの**[FEX]**チェックボックスをオフにすると、FEXデバイスは**[ファブリック ビルダ（Fabric Builder）]**トポロジウィンドウでも非表示になります。**Fabric Builder**でFEXを表示するには、このチェックボックスをオンにする必要があります。このオプションはすべてのファブリックに適用でき、セッションごとに保存されるか、DCNMからログアウトするまで保存されます。ログアウトしてDCNMにログインすると、FEXオプションはデフォルトにリセットされます。つまり、デフォルトで有効になります。詳細については、パネルを表示, on page 29を参照してください。

[構成の展開（Deploy Config）]オプションの使用例は、スイッチ レベルの自由形式の設定です。詳細については、「ファブリック スイッチでのフリーフォーム設定の有効化」を参照してください。

eBGP EVPN を使用した VXLAN EVPN の展開

eBGP ベースのアンダーレイを使用した eBGP の新しい VXLAN EVPN の作成

1. **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]**を選択します。

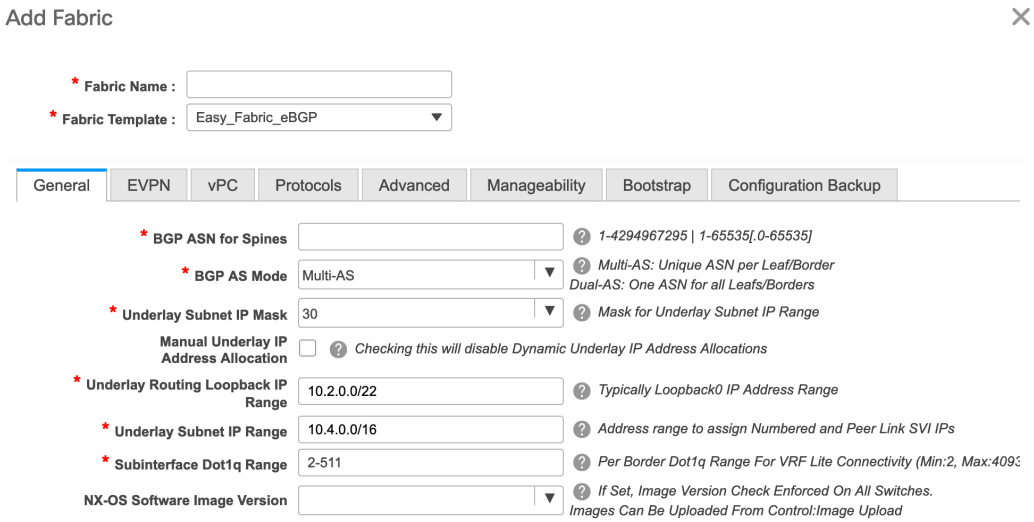
   [ファブリック ビルダ（Fabric Builder）]画面が表示されます。初めてログインしたときには、**[ファブリック（Fabrics）]**セクションにはまだエントリはありません。ファブリックを作成すると、**[ファブリック ビルダ（Fabric Builder）]**画面に表示されます。長方形のボックスが各ファブリックを表します。

2. [ファブリックの作成（Create Fabric）]をクリックします。**[ファブリックの追加（Add Fabric）]**画面が表示されます。

   フィールドについて説明します。

   [ファブリック名（Fabric Name）]：ファブリックの名前を入力します。

   [ファブリック テンプレート（Fabric Template）]：ドロップダウンメニューから、**[Easy_Fabric_eBGP]**ファブリックテンプレートを選択します。スタンドアロンルーテッドファブリックを作成するためのファブリック設定が表示されます。



3. デフォルトでは **[全般（General）]** タブが表示されます。このタブのフィールドは次のとおりです。

   [スパインの BGP ASN（BGP ASN for Spines）]：ファブリックのスパイン スイッチの BGP AS 番号を入力します。

   [BGP AS モード（BGP AS Mode）]：**[Multi-AS]** または **[Dual-AS]** を選択します。

   Multi-AS ファブリックでは、スパイン スイッチには一意の BGP AS 番号があり、各リーフ スイッチには一意の AS 番号があります。2 つのリーフ スイッチが vPC スイッチ ペアを形成している場合、それらは同じ AS 番号を持ちます。

   [Dual-AS] ファブリックでは、スパイン スイッチには一意の BGP AS 番号があり、リーフスイッチには一意の AS 番号があります。

   ファブリックは、スパイン スイッチの AS 番号によって識別されます。

   [アンダーレイ サブネット IP マスク（Underlay Subnet IP Mask）]：ファブリック インターフェイスの IP アドレスのサブネットマスクを指定します。

   [手動アンダーレイ IP アドレス割り当て（Manual Underlay IP Address Allocation）]：[動的アンダーレイ IP アドレス割り当て（Dynamic Underlay IP Address Allocation）] を無効にするには、このチェックボックスをオンにします。

   [アンダーレイ ルーティング ループバック IP 範囲（Underlay Routing Loopback IP Range）]：プロトコル ピアリングのループバック IP アドレスを指定します。

   [アンダーレイ サブネット IP 範囲（Underlay Subnet IP Range）]：インターフェイス間のアンダーレイ P2P ルーティング トラフィックの IP アドレスです。

   [サブインターフェイス Dot1q 範囲（Subinterface Dot1q Range）]：L3 サブインターフェイスを使用する場合のサブインターフェイスの範囲を指定します。

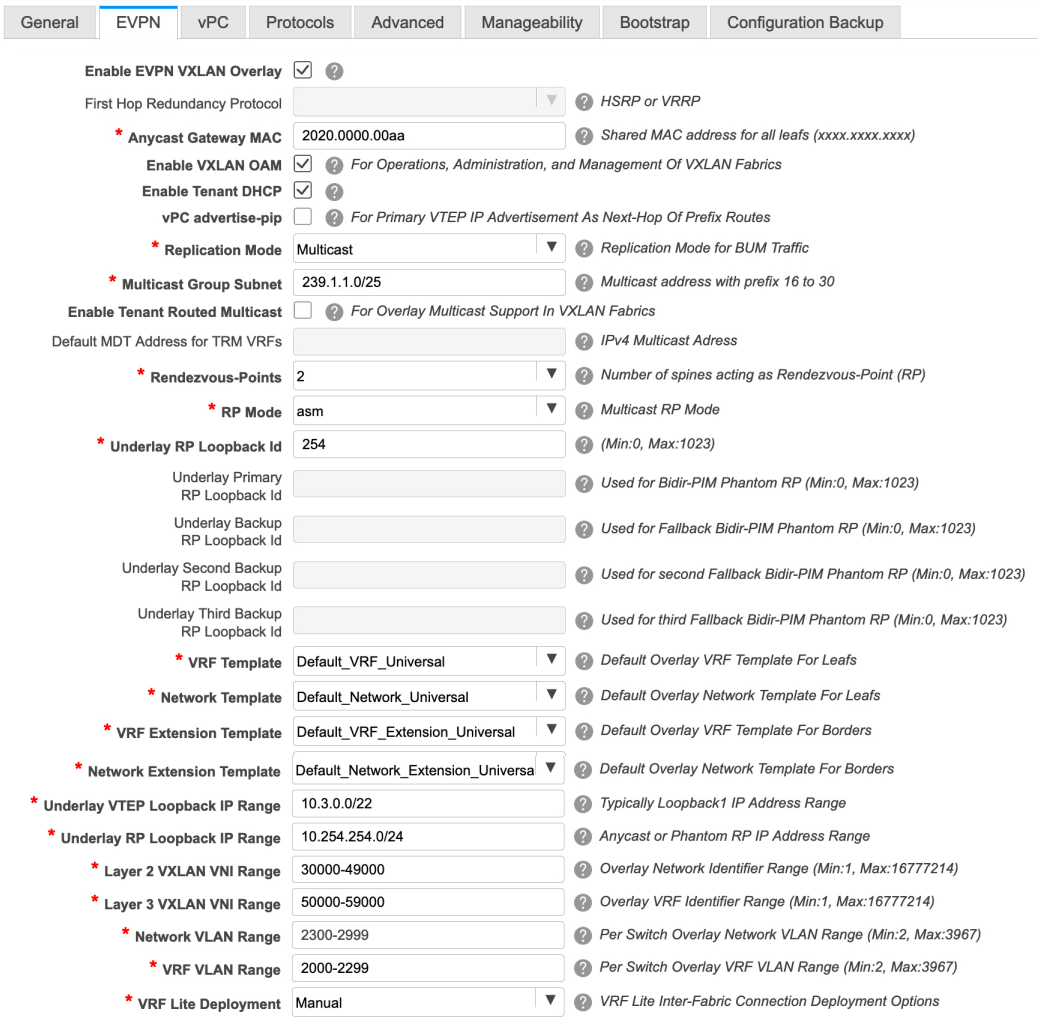
   [NX-OSソフトウェア イメージ バージョン（NX-OS Software Image Version）]：ドロップダウンリストからイメージを選択します。

イメージアップロードオプションを使用してCisco NX-OS ソフトウェアイメージをアップロードすると、アップロードされたイメージがこのフィールドにリストされます。イメージを選択すると、システムはスイッチに選択したバージョンがあるかどうかを確認します。選択されていない場合、エラー メッセージが表示されます。[解決（Resolve）] をクリックすることで、エラーを解決できます。イメージ管理画面が表示され、ISSU オプションを処理できます。その代わりに、リリース ナンバーを削除した後で保存することも可能です。

このフィールドでイメージを指定する場合、ファブリックのすべてのスイッチはそのイメージを実行する必要があります。一部のデバイスでイメージが実行されない場合、指定されたイメージへのインサービス ソフトウェア アップグレード（ISSU）を実行するように警告するプロンプトが表示されます。すべてのデバイスが指定されたイメージを実行するまで、展開プロセスは完了しません。

ファブリック スイッチに複数のタイプのソフトウェア イメージを展開する場合は、イメージを指定しないでください。イメージが指定されている場合は削除します。

4. **[EVPN]** をクリックします。このタブのほとんどのフィールドは自動入力されます。該当するフィールドは次のとおりです。



[EVPN VXLAN オーバーレイを有効にする（Enable EVPN VXLAN Overlay）]：ファブリックの VXLAN オーバーレイ プロビジョニングを有効にします。

このオプションを選択すると、ルーテッドファブリックを VXLAN 対応のファブリックに変換できます。ファブリックで VXLAN が有効になっている場合、オーバーレイ ネットワークまたは VRF を作成して展開できます。ネットワークまたは VRF を作成して展開する手順は、Easy_Fabric_11_1 の場合と同じです。詳細については、『*Cisco DCNM LAN* ファブリックの構成ガイド』の「ネットワークおよび *VRF* の作成と展開」章を参照してください。

[ルーテッド ファブリック（Routed Fabric）]：ルーテッド ファブリック（VXLAN カプセル化のない IP ファブリック）を作成するためには、EVPN VXLAN オーバーレイ フィールドの有効化を無効にする必要があります。ルーテッドファブリックでは、ネットワークを作成して展開できます。詳細については、ルーテッドファブリックのネットワークの概要, on page 1157を参照してください。

eBGP ルーテッドまたは eBGP VXLAN ファブリックを作成する場合、ファブリックは eBGP をコントロール プレーンとして使用して、ファブリック内接続を構築します。ス

パイン スイッチとリーフ スイッチ間のリンクは、上側で eBGP ピアリングが構築されたポイント ツー ポイント（p2p）番号付き IP アドレスで自動構成されます。

ファブリック内にネットワークまたはVRFが作成されている場合、**[EVPN VXLAN オーバーレイを有効にする（Enable EVPN VXLAN Overlay）]** チェック ボックスを選択して、VXLAN EVPN モードとルーテッド ファブリック モードを切り替えることはできません。ファブリック設定を変更するには、これらのネットワークまたはVRFを削除する必要があります。

Routed_Network_Universal テンプレートは、ルーテッド ファブリックにのみ適用されることに注意してください。ルーテッド ファブリックを EVPN VXLAN ファブリックに変換する場合は、ネットワーク テンプレートとネットワーク拡張テンプレートを、EVPN VXLAN に定義されているものに設定します：**Default_Network_Universal** と **Default_Network_Universal** です。EVPN VXLAN ファブリック用にカスタマイズされたテンプレートがある場合は、それを使用することも選択できます。

[ファースト ホップ冗長性プロトコル（First Hop Redundancy Protocol）]：FHRP プロトコルを指定します。**hsrp** または **vrrp** のいずれかを選択します。このフィールドは、ルーテッド ファブリックにのみ適用されます。

Note

- ネットワークの作成後に、このファブリック設定を変更することはできません。変更する場合は、すべてのネットワークを削除してから、FHRP設定を変更する必要があります。
- [EVPN] タブ セクションの残りのフィールドは、EVPN VXLAN オーバーレイを有効にする場合にのみ適用されます。

[エニーキャスト ゲートウェイ MAC（Anycast Gateway MAC）]：リーフ スイッチのエニーキャスト ゲートウェイ MAC アドレスを指定します。

[VXLAN OAM を有効にする（Enable VXLAN OAM）]：既存のスイッチの VXLAN OAM機能を有効にします。この設定はデフォルトでイネーブルになっています。VXLAN OAM 機能を無効にするにはチェックボックスをクリアします。

ファブリック内の特定のスイッチで VXLAN OAM 機能を有効にし、他のスイッチで無効にする場合は、ファブリック設定でOAMを無効にしておいて、自由形式構成でOAMを有効にすることができます。

Note Cisco DCNM の VXLAN OAM 機能は、単一のファブリックまたはサイトでのみサポートされます。

[テナント DHCP を有効にする（Enable Tenant DHCP）]：テナント DHCP サポートを有効にします。

[vPC advertise-pip]：アドバタイズ PIP 機能を有効にするには、[vPC advertise-pip] チェックボックスをオンにします。

[レプリケーション モード（Replication Mode）]：ファブリック、入力レプリケーション、またはマルチキャストで使用されるレプリケーションのモードです。

[マルチキャスト グループ サブネット（Multicast Group Subnet）]：マルチキャスト通信に使用される IP アドレス プレフィックスです。オーバーレイ ネットワークごとに、このグループから一意の IP アドレスが割り当てられます。

[テナント ルーテッド マルチキャストを有効にする（Enable Tenant Routed Multicast）]：ファブリック オーバーレイ マルチキャスト プロトコルとしてテナント ルーテッド マルチキャスト（TRM）を有効にするには、チェックボックスをオンにします。

[TRM VRF のデフォルト MDT アドレス（Default MDT Address for TRM VRFs）]：テナント ルーテッドマルチキャスト トラフィックのマルチキャストアドレスが入力されます。デフォルトでは、このアドレスは [マルチキャスト グループ サブネット] フィールドで指定された IP プレフィックスから取得されます。いずれかのフィールドをアップデートする場合、**[マルチキャスト グループ サブネット（Multicast Group Subnet）]** で指定した IP プレフィックスから選択された TRM アドレスであることを確認してください。

[ランデブーポイント（Rendezvous-Points）]：ランデブーポイントとして機能するスパイン スイッチの台数を入力します。

[RP モード（RP mode）]：ASM（エニーソース マルチキャスト（ASM）の場合）または BiDir（双方向 PIM（BIDIR-PIM）の場合）の、サポート対象の 2 つのマルチキャスト モードからいずれかを選択します。[ASM] を選択すると、[BiDir] 関連のフィールドは有効になりません。[BiDir] を選択すると、[BiDir] 関連フィールドが有効になります。

Note BIDIR-PIM は、Cisco のクラウド スケール ファミリ プラットフォーム 9300-EX および 9300-FX/FX2、およびソフトウェア リリース 9.2(1) 以降でサポートされています。

[アンダーレイ RP ループバック ID（Underlay RP Loopback ID）]：ファブリック アンダーレイでのマルチキャスト プロトコル ピアリングの目的で、ランデブーポイント（RP）に使用されるループバック ID です。デフォルトは 254 です。

[双方向（bidir）]を選択すると、以下のフィールドが有効になります。RP カウントに応じて、2 つまたは 4 つのファントム RP ループバック ID フィールドが有効になります。

- **[アンダーレイ プライマリ RP ループバック ID（Underlay Primary RP Loopback ID）]**：ファブリック アンダーレイでマルチキャスト プロトコル ピアリングのためにファントム RP に使用されるプライマリ ループバック ID です。
- **[アンダーレイ バックアップ RP ループバック ID（Underlay Backup RP Loopback ID）]**：ファブリック アンダーレイでマルチキャスト プロトコル ピアリングを目的として、ファントム RP に使用されるセカンダリ（つまりバックアップ）ループバック ID です。

次のループバック ID オプションは、RP カウントが 4 の場合にのみ適用されます。

- **[アンダーレイ セカンド バックアップ RP ループバック ID（Underlay Second Backup RP Loopback ID）]**：ファブリック アンダーレイでマルチキャスト プロトコル ピア

リングを目的としてファントム RP に使用される、第二のバックアップ ループバック ID です。

- **[アンダーレイ サード バックアップ RP ループバック ID（Underlay Third Backup RP Loopback ID）]**：ファブリック アンダーレイでマルチキャスト プロトコル ピア リングを目的としてファントム RP に使用される、第三のバックアップ ループバック ID です。

[VRF テンプレート（VRF Template）] および **[VRF 拡張テンプレート（VRF Extension Template）]**：VRF を作成するための VRF テンプレートと、他のファブリックで VRF 拡張を有効にするための VRF 拡張テンプレートを指定します。

[ネットワーク テンプレート（Network Template）] と **[ネットワーク拡張テンプレート（Network Extension Template）]**：ネットワークを作成するためのネットワーク テンプレートと、他のファブリックにネットワークを拡張するためのネットワーク拡張テンプレートを指定します。

[アンダーレイ VTEP ループバック IP 範囲（Underlay VTEP Loopback IP Range）]：VTEP のループバック IP アドレス範囲を指定します。

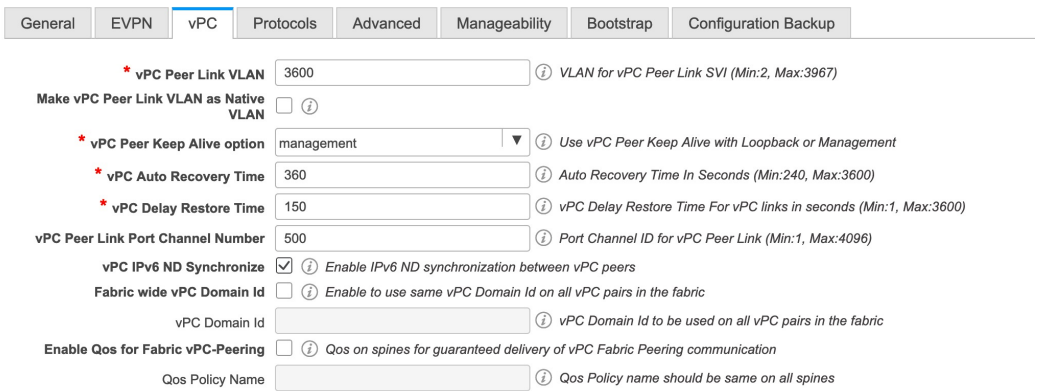
[アンダーレイ RP ループバック IP 範囲（Underlay RP Loopback IP Range）]：エニーキャストまたはファントム RP の IP アドレス範囲を指定します。

[レイヤ 2 VXLAN VNI 範囲（Layer 2 VXLAN VNI Range）] および **[レイヤ 3 VXLAN VNI 範囲（Layer 3 VXLAN VNI Range）]**：ファブリックの VXLAN VNI ID を指定します。

[ネットワーク VLAN 範囲（Network VLAN Range）] および **[VRF VLAN 範囲（VRF VLAN Range）]**：レイヤ 3 VRF およびオーバーレイ ネットワークの VLAN 範囲です。

[VRF Lite の展開（VRF Lite Deployment）]：ファブリック間接続を拡張するための VRF Lite 方式を指定します。[手動（Manual）] オプションのみがサポートされています。

5. **[vPC]** をクリックします。このタブのフィールドは次のとおりです。



[vPC ピア リンク VLAN（vPC Peer Link VLAN）]：vPC ピア リンク SVI に使用される VLAN です。

[vPC ピア リンク VLAN をネイティブ VLAN とする（Make vPC Peer Link VLAN as Native VLAN）]：vPC ピア リンク VLAN をネイティブ VLAN として有効にします。

[vPC ピア キープアライブ オプション（vPC Peer Keep Alive option）]：管理またはループバック オプションを選択します。管理ポートおよび管理 VRF に割り当てられた IP アドレスを使用する場合は、[管理（management）] を選択します。ループバック インターフェイス（および非管理 VRF）に割り当てられた IP アドレスを使用する場合は、ループバックを選択します。IPv6 アドレスを使用する場合は、ループバック ID を使用する必要があります。

[vPC 自動回復時間（vPC Auto Recovery Time）]：vPC 自動回復タイムアウト時間を秒単位で指定します。

[vPC 遅延復元時間（vPC Delay Restore Time）]：vPC 遅延復元時間を秒単位で指定します。

[vPC ピア リンク ポートチャネル番号（vPC Peer Link Port Channel Number）]：vPC ピア リンクのポートチャネル ID を指定します。デフォルトでは、このフィールドの値は 500 です。

[vPC IPv6 ND 同期（vPC IPv6 ND Synchronize）]：vPC スイッチ間の IPv6 ネイバー探索同期を有効にします。デフォルトでチェックボックスはオンになっています。機能を無効にするにはチェックボックスをクリアします。

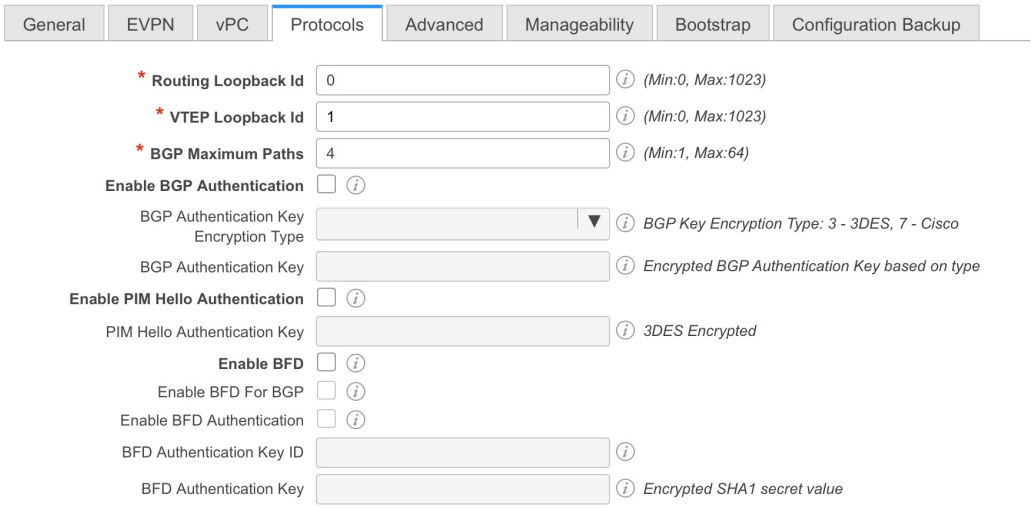
[ファブリック全体の vPC ドメイン ID（Fabric wide vPC Domain Id）]：ファブリック内のすべての vPC ペアで同じ vPC ドメイン ID の使用を有効にします。このフィールドを選択すると、[vPC ドメイン ID（vPC Domain Id）] フィールドが編集可能になります。

[vPCドメインID（vPC Domain Id）]：すべての vPC ペアで使用される vPC ドメイン ID を指定します。

[ファブリック vPC ピアリングの QoS を有効にする（Enable QoS for Fabric vPC-Peering）]：スパインの QoS を有効にして、vPC ファブリック ピアリング通信の配信を保証します。

[QoS ポリシー名（QoS Policy Name）]：すべてのスパインで同じにする必要がある QoS ポリシー名を指定します。

6. **[プロトコル（Protocols）]** タブをクリックします。このタブのフィールドは次のとおりです。



[ルーティング ループバック ID（Routing Loopback Id）]：ループバック インターフェイス ID は、デフォルトで 0 として設定されます。BGP ルータ ID として使用されます。

[VTEP ループバック ID（VTEP Loopback Id）]：loopback1 は通常 VTEP ピアリングの目的で使用されるため、ループバック インターフェイス ID は 1 に設定されます。

[BGP 最大パス（BGP Maximum Paths）]：BGP 最大パスを指定します。

[BGP 認証の有効化（Enable BGP Authentication）]：BGP 認証を有効にするにはチェックボックスをオンにします。無効にするにはチェックボックスをオフにします。このフィールドを有効にすると、[BGP 認証キー暗号化タイプ（BGP Authentication Key Encryption Type）] および [BGP 認証キー（BGP Authentication Key）] フィールドが有効になります。

[BGP 認証キー暗号化タイプ（BGP Authentication Key Encryption Type）]：3DES 暗号化タイプの場合は 3、Cisco 暗号化タイプの場合は 7 を選択します。

[BGP 認証キー（BGP Authentication Key）]：暗号化タイプに基づいて暗号化キーを入力します。

Note プレーン テキスト パスワードはサポートされていません。スイッチにログインし、暗号化されたキーを取得して、[BGP 認証キー（BGP Authentication Key）] フィールドに入力します。詳細については、「認証キーの取得」の項を参照してください。

[PIM Hello 認証の有効化（Enable PIM Hello Authentication）]：PIM hello 認証を有効にします。

[PIM Hello 認証キー（PIM Hello Authentication Key）]：PIM hello 認証キーを指定します。

[BFD の有効化（Enable BFD）]：ファブリック内のすべてのスイッチで機能 [bfd] を有効にするには、このチェックボックスをオンにします。この機能は、IPv4 アンダーレイでのみ有効で、範囲はファブリック内にあります。

Cisco DCNM リリース 11.3(1) 以降、ファブリック内の BFD はネイティブにサポートされます。ファブリック設定では、BFD機能はデフォルトで無効になっています。有効にすると、デフォルト設定のアンダーレイ プロトコルに対して BFD が有効になります。カスタムの必須BFD構成は、スイッチごとの自由形式またはインターフェイスごとの自由形式ポリシーを使用して展開する必要があります。

[BFD の有効化（Enable BFD）] チェックボックスをオンにすると、次の構成がプッシュされます。

```
feature bfd
```

Note BFD が有効になっている DCNM リリース 11.2(1) から DCNM リリース 11.3(1) にアップグレードすると、次の構成がすべての P2P ファブリック インターフェイスにプッシュされます。

```
no ip redirects
no ipv6 redirects
```

BFD機能の互換性については、それぞれのプラットフォームのマニュアルを参照してください。サポートされているソフトウェア画像については、「*Cisco DCNM* の互換性マトリクス」を参照してください。

[BGP 向け BFD の有効化（Enable BFD for BGP）]：BGP ネイバーの BFD を有効にするには、このチェックボックスをオンにします。このオプションは、デフォルトで無効です。

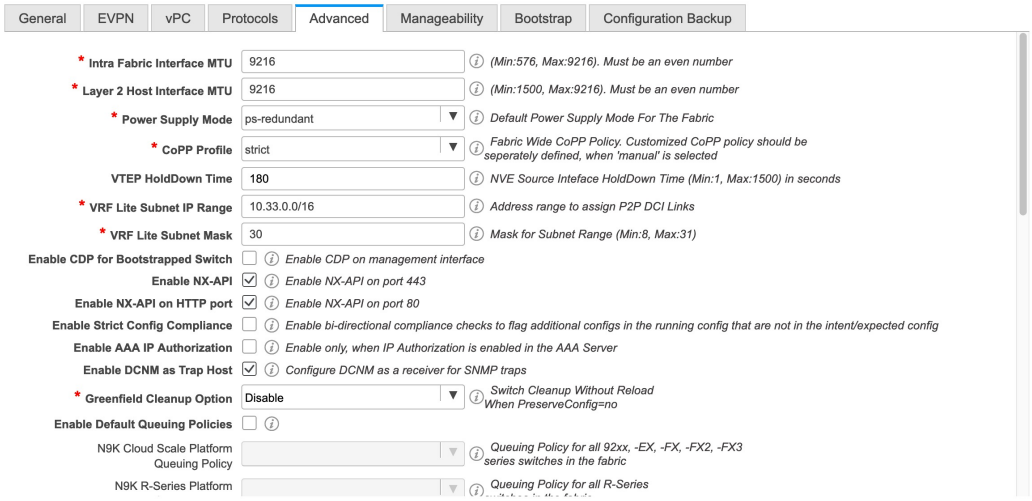
[BGP 認証の有効化（Enable BGP Authentication）]：BGP 認証を有効にするにはチェックボックスをオンにします。このフィールドを有効にすると、[BFD 認証キー ID（BFD Authentication Key ID）] フィールドと [BFD 認証キー（BFD Authentication Key）] フィールドが編集可能になります。

[BFD 認証キー ID（BFD Authentication Key ID）]：インターフェイス認証の BFD 認証キー ID を指定します。

[BFD 認証キー（BFD Authentication Key）]：BFD 認証キーを指定します。

BFD 認証パラメータを取得する方法については、『*Cisco DCNM LAN* ファブリック構成ガイド』の「暗号化された *BFD* 認証キーの取得」を参照してください。

7. [Advanced] タブをクリックします。このタブのフィールドは次のとおりです。



[イントラ ファブリック インターフェイス MTU（Intra Fabric Interface MTU）]：ファブリック内インターフェイスの MTU を指定します。この値は偶数にする必要があります。

[レイヤ 2 ホスト インターフェイス MTU（Layer 2 Host Interface MTU）]：レイヤ 2 ホスト インターフェイスの MTU を指定します。この値は偶数にする必要があります。

電源モード（Power Supply Mode）：適切な電源モードを選択します。

[CoPP プロファイル（CoPP Profile）]：ファブリックの適切なコントロールプレーン ポリシング（CoPP）プロファイルポリシーを選択します。デフォルトでは、strict オプションが入力されます。

[VTEP HoldDown 時間（VTEP HoldDown Time）]：NVE 送信元インターフェイスのホールドダウン時間を指定します。

[VRF Lite サブネット IP 範囲（VRF Lite Subnet IP Range）] および [VRF Lite サブネット マスク（VRF Lite Subnet Mask）]：これらのフィールドには、DCI サブネットの詳細が入力されます。必要に応じて、次のフィールドを更新します。

[ブートストラップ スイッチの CDP を有効にする（Enable CDP for Bootstrapped Switch）]：チェックボックスをオンにして、ブートストラップ スイッチの CDP を有効にします。

[NX-API の有効化（Enable NX-API）]：HTTPS での NX-API の有効化を指定します。このチェックボックスは、デフォルトでオンになっています。

[HTTP での NX-API の有効化（Enable NX-API on HTTP）]：HTTP での NX-API の有効化を指定します。HTTP を使用するには、[NX-API の有効化（Enable NX-API）] チェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。このチェックボックスをオフにすると、エンドポイント ロケータ（EPL）、レイヤ 4～レイヤ 7 サービス（L4ーL7 サービス）、VXLAN OAM など、NX-API を使用し、Cisco DCNM がサポートするアプリケーションは、HTTP ではなく HTTPS の使用を開始します。

Note [NX-API の有効化（Enable NX-API）] チェックボックスと [HTTP での NX-API の有効化（Enable NX-API on HTTP）] チェックボックスをオンにすると、アプリケーションは HTTP を使用します。

[厳密な構成コンプライアンスの有効化（Enable Strict Config Compliance）]：このチェックボックスをオンにして、厳密な構成コンプライアンス機能を有効にします。

厳密な構成コンプライアンスについては、*Enhanced Monitoring and Monitoring Fabrics Guide*を参照してください。

Note ファブリックで厳密な構成コンプライアンスが有効になっている場合、Cisco DCN M のリソースで Network Insights を展開することはできません。

[AAA IP 認証の有効化（Enable AAA IP Authorization）]：AAA サーバーで IP 認証が有効になっている場合に、AAA IP 認証を有効にします。

[トラップホストとして有効にする（Enable as Trap Host）]：トラップホストとして有効にする場合は、このチェックボックスをオンにします。

[グリーンフィールド クリーンアップ オプション（Greenfield Cleanup Option）]：スイッチをリロードせずにスイッチのグリーンフィールドクリーンアップ オプションを有効にします。このオプションは、通常、Cisco Nexus 9000v スイッチを使用するデータセンター環境でのみ推奨されます。

[デフォルト キューイング ポリシーの有効化（Enable Default Queuing Policies）]：このファブリック内のすべてのスイッチに QoS ポリシーを適用するには、このチェックボックスをオンにします。すべてのスイッチに適用した QoS ポリシーを削除するには、このチェックボックスをオフにし、すべての設定を更新してポリシーへの参照を削除し、保存して展開します。Cisco DCNM リリース 11.3(1) 以降、さまざまな Cisco Nexus 9000 シリーズスイッチに使用できる定義済みの QoS 設定が含まれています。このチェックボックスをオンにすると、適切な QoS 設定がファブリック内のスイッチにプッシュされます。システム キューイングは、設定がスイッチに展開されると更新されます。インターフェイスごと自由形式ブロックに必要な設定を追加することにより、必要に応じて、定義されたキューイング ポリシーを使用してインターフェイス マーキングを実行できます。

テンプレート エディタでポリシー ファイルを開いて、実際のキューイング ポリシーを確認します。Cisco DCNM Web UI から、**[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択します。ポリシー ファイル名でキューイング ポリシーを検索します（例：[queuing_policy_default_8q_cloudscale]）。ファイルを選択し、**[テンプレートの変更/表示（Modify/View template）]** アイコンをクリックしてポリシーを編集します。

プラットフォーム特有の詳細については、『*Cisco Nexus 9000 Series NX-OS Quality of Service* コンフィグレーション ガイド』を参照してください。

[N9K クラウド スケール プラットフォームのキューイング ポリシー（N9K Cloud Scale Platform Queuing Policy）]：ファブリック内の EX、FX、および FX2 で終わるすべての Cisco Nexus 9200 シリーズスイッチおよび Cisco Nexus 9000 シリーズスイッチに適用するキューイング ポリシーをドロップダウン リストから選択します。有効な値は [queuing_policy_default_4q_cloudscale] および [queuing_policy_default_8q_cloudscale] です。FEX には [queuing_policy_default_4q_cloudscale] ポリシーを使用します。FEX がオフラインの場合にのみ、[queuing_policy_default_4q_cloudscale] ポリシーから [queuing_policy_default_8q_cloudscale] ポリシーに変更できます。

[N9K R シリーズ プラットフォーム キューイング ポリシー（N9K R-Series Platform Queuing Policy）]：ドロップダウンリストから、ファブリック内の R で終わるすべての Cisco Nexus スイッチに適用するキューイング ポリシーを選択します。有効な値は [queuing_policy_default_r_series] です。

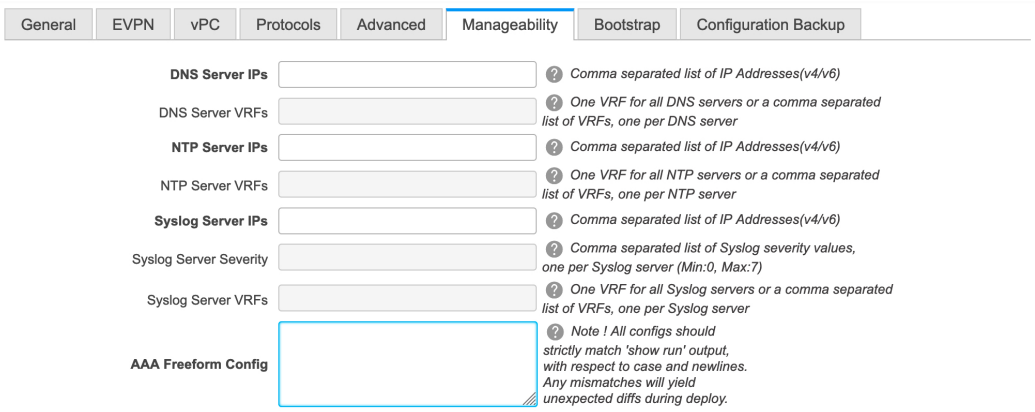
[その他の N9K プラットフォーム キューイング ポリシー（Other N9K Platform Queuing Policy）]：ドロップダウンリストからキューイング ポリシーを選択し、ファブリック内にある、上記 2 つのオプションで説明したスイッチ以外の他のすべてのスイッチに適用します。有効な値は [queuing_policy_default_other] です。

[リーフの自由形式の構成（Leaf Freeform Config）]：リーフ、ボーダー、およびボーダー ゲートウェイのロールを持つスイッチに追加する CLI です。

[スパインの自由形式の構成（Spine Freeform Config）]：スパイン、ボーダー スパイン、およびボーダーゲートウェイ スパインのロールを持つスイッチに追加する必要がある CLI を追加します。

[ファブリック内リンクの追加設定（Intra-fabric Links Additional Config）]：ファブリック内リンクに追加する CLI を追加します。

8. **管理能力（Manageability）** タブをクリックします。



このタブのフィールドは次のとおりです。

[DNS サーバー IP（DNS Server IPs）]：DNS サーバーの IP アドレス（v4/v6）のカンマ区切りリストを指定します。

[DNS サーバー VRF（DNS Server VRFs）]：すべての DNS サーバーに 1 つの VRF を指定するか、DNS サーバーごとに 1 つの VRF を、カンマ区切りリストで指定します。

[NTP サーバー IP（NTP Server IPs）]：NTP サーバーの IP アドレス（v4/v6）のカンマ区切りリストを指定します。

[NTP サーバー VRF（NTP Server VRFs）]：すべての NTP サーバーに 1 つの VRF を指定するか、NTP サーバーごとに 1 つの VRF を、カンマ区切りリストで指定します。

[Syslog サーバ IP（Syslog Server IPs）]：syslog サーバの IP アドレスのカンマ区切りリスト（v4/v6）を指定します（使用する場合）。

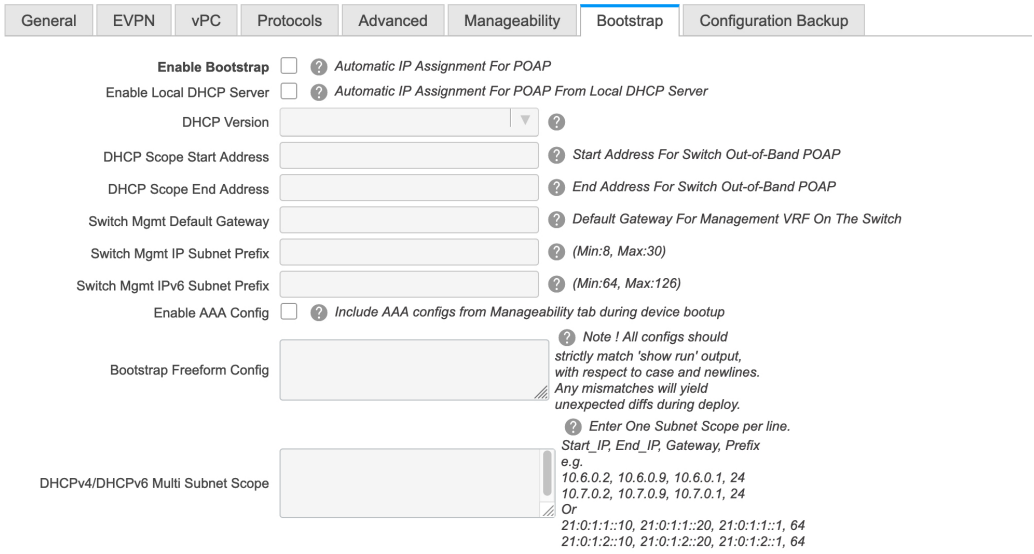
[Syslog サーバのシビラティ（重大度）（Syslog Server Severity）]：syslog サーバごとに 1 つの syslog シビラティ（重大度）値のカンマ区切りリストを指定します。最小値は 0 で、最大値は 7 です。高いシビラティ（重大度）を指定するには、大きい数値を入力します。

[Syslog サーバ VRF（Syslog Server VRFs）]：すべての syslog サーバに 1 つの VRF を指定するか、syslog サーバごとに 1 つの VRF を指定します。

[AAA 自由形式の構成（AAA Freeform Config）]：AAA 自由形式の構成を指定します。

ファブリック設定で AAA 構成が指定されている場合は、**switch_freeform** PTI で、ソースが **UNDERLAY_AAA**、説明が **AAA Configurations** であるものが作成されます。

9. **[ブートストラップ（Bootstrap）]** タブをクリックします。



[ブートストラップの有効化（Enable Bootstrap）]：このチェックボックスを選択し、ブートストラップ機能を有効にします。

ブートストラップをイネーブルにした後、次のいずれかの方法を使用して、DHCP サーバで IP アドレスの自動割り当てをイネーブルにできます。

- 外部 DHCP サーバ（External DHCP Server）：**[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]**および**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** 外部 DHCP サーバに関する情報を入力します。

- [ローカル DHCP サーバー（Local DHCP Server）]：**[ローカル DHCP サーバー（Local DHCP Server）]** チェックボックスを有効にして、残りの必須フィールドに詳細を入力します。

ローカル DHCP サーバーの有効化（Enable Local DHCP Server）：ローカル DHCP サーバーを介した自動 IP アドレス割り当ての有効化を開始するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、**[DHCP スコープ開始アドレス（DHCP Scope Start Address）]** および **[DHCP スコープ終了アドレス（DHCP Scope End Address）]** フィールドが編集可能になります。

このチェックボックスをオンにしない場合、DCNM は自動 IP アドレス割り当てにリモートまたは外部DHCPサーバを使用します。

[DHCP バージョン（DHCP Version）]：このドロップダウンリストから [DHCPv4] または [DHCPv6] を選択します。DHCPv4 を選択すると、**[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]** フィールドが無効になります。DHCPv6 を選択すると、**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** は無効になります。

Note Cisco DCNM IPv6 POAP は、Cisco Nexus 7000 シリーズ スイッチではサポートされていません。Cisco Nexus 9000 および 3000 シリーズ スイッチは、スイッチが L2 隣接（eth1 またはアウトオブバンド サブネットは /64 が必須）、またはスイッチがいくつかの IPv6 /64 サブネット内に存在する L3 隣接である場合にのみ、IPv6 POAP をサポートします。/64 以外のサブネット プレフィックスはサポートされません。

[DHCP スコープ開始アドレス（DHCP Scope Start Address）] および [DHCP スコープ終了アドレス（DHCP Scope End Address）]：スイッチのアウトオブバンド POAP に使用される IP アドレス範囲の最初と最後の IP アドレスを指定します。

[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]：スイッチの管理 VRF のデフォルト ゲートウェイを指定します。

[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]：スイッチの Mgmt0 インターフェイスのプレフィックスを指定します。プレフィックスは 8 ～ 30 の間である必要があります。

DHCP スコープおよび管理デフォルト ゲートウェイ *IP* アドレスの仕様（*DHCP scope and management default gateway IP address specification*）：管理デフォルト ゲートウェイ IP アドレスを 10.0.1.1 に、サブネット マスクを 24 に指定した場合、DHCP スコープが指定したサブネット、10.0.1.2 ～ 10.0.1.254 の範囲内であることを確認してください。

[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]：スイッチの Mgmt0 インターフェイスの IPv6 プレフィックスを指定します。プレフィックスは 112 ー 126 の範囲で指定する必要があります。このフィールドは DHCP の IPv6 が有効な場合に編集できます。

[AAA 構成を有効化（Enable AAA Config）]：デバイスの起動時に [管理性（Manageability）] タブから AAA 構成を含めるには、このチェックボックスをオンにします。

[ブートストラップ自由形式の構成（Bootstrap Freeform Config）]：（オプション）必要に応じて追加のコマンドを入力します。たとえば、AAA またはリモート認証関連の構成を使用している場合は、このフィールドにこれらの構成を追加してインテントを保存する必要があります。デバイスが起動すると、[Bootstrap Freeform Config]フィールドで定義されたインテントが含まれます。

NX-OSスイッチの実行コンフィギュレーションに示されているように、running-configを正しいインデントで自由形式の設定フィールドにコピーアンドペーストします。freeform config は running config と一致する必要があります。詳細については、スイッチでのフリーフォーム構成エラーの解決を参照してください。ファブリック スイッチでのフリーフォーム構成の有効化に記されています。

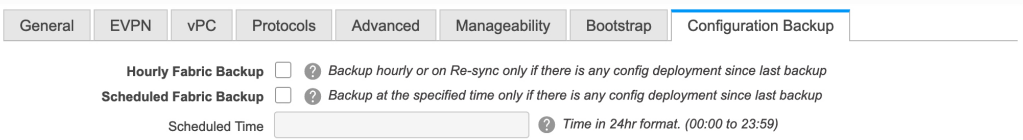
[DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）]：1行に1つのサブネット スコープを入力して、フィールドを指定します。**[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）]** チェックボックスをオンにした後で、このフィールドは編集可能になります。

スコープの形式は次の順で定義する必要があります。

[DHCP スコープ開始アドレス、DHCP スコープ終了アドレス、スイッチ管理デフォルト ゲートウェイ、スイッチ管理サブネット プレフィックス（DHCP Scope Start Address, DHCP Scope End Address, Switch Management Default Gateway, Switch Management Subnet Prefix）]

例：10.6.0.2、10.6.0.9、16.0.0.1、24

10. **[構成のバックアップ（Configuration Backup）]** タブをクリックします。このタブのフィールドは次のとおりです。



[毎時ファブリック バックアップ（Hourly Fabric Backup）]：ファブリック構成とインテントの毎時バックアップを有効にします。

新しいファブリック設定とインテントの1時間ごとのバックアップを有効にできます。前の時間に構成のプッシュがある場合、DCNM はバックアップを取得します。

インテントとは、DCNM に保存されているが、まだスイッチにプロビジョニングされていない構成を指します。

[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]：毎日のバックアップを有効にします。このバックアップは、構成のコンプライアンスによって追跡されないファブリック デバイスの実行構成の変更を追跡します。

[スケジュール済みの時間（Scheduled Time）]：スケジュールされたバックアップ時間を 24 時間形式で指定します。[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]チェックボックスをオンにすると、このフィールドが有効になります。

両方のチェックボックスをオンにして、両方のバックアップ プロセスを有効にします。

[保存（Save）]をクリックすると、バックアップ プロセスが開始されます。

Note 1 時間ごと、およびスケジュールされたバックアップ プロセスは、次の定期的な構成コンプライアンス アクティビティ中にのみ発生し、最大 1 時間の遅延が発生する可能性があります。即時バックアップをトリガーするには、次の手順を実行します。

a. **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。[Fabric Builder] 画面が表示されます。

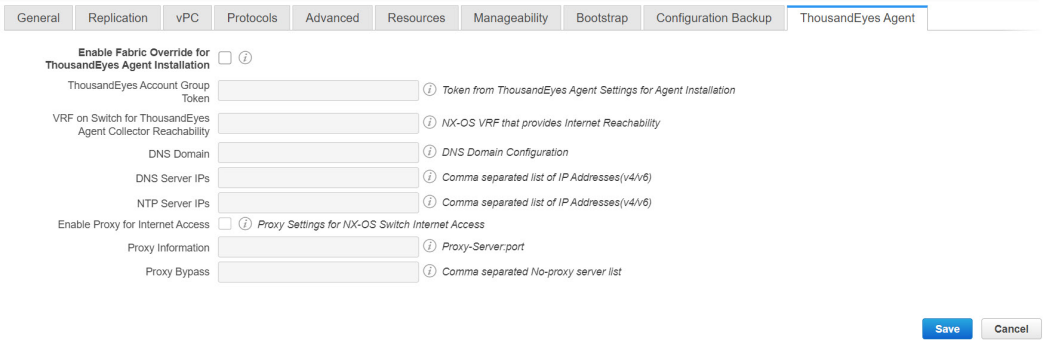
b. 特定のファブリック ボックス内をクリックします。[ファブリック トポロジ (fabric topology)] 画面が表示されます。

c. 画面左側の **[アクション（Actions）]** パネルで、**[ファブリックの再同期（Re-Sync Fabric）]** をクリックします。

ファブリック トポロジ ウィンドウでファブリック バックアップを開始することもできます。[アクション（Actions）]ペインで[今すぐバックアップ（Backup Now）]をクリックします。

関連情報を入力して更新したら、**[保存（Save）]** をクリックします。

11. **[ThousandEyes Agent]** タブをクリックします。この機能は、Cisco DCNM リリース 11.5（3）でのみサポートされています。詳細については、「Cisco DCNM での ThousandEyes Enterprise Agent のグローバル設定の構成」を参照してください。



このタブのフィールドは次のとおりです。

Note ThousandEyes Agent のファブリック設定はグローバル設定を上書きし、そのファブリック内のスイッチにインストールされているすべての ThousandEyes エージェントに同じ構成を適用します。

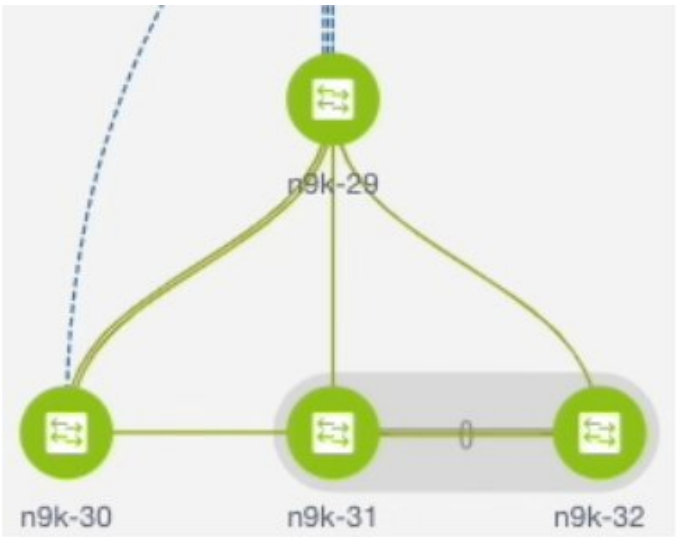
- **[ThousandEyes Agent インストールのファブリック オーバーライドを有効にする（Enable Fabric Override for ThousandEyes Agent Installation）]** : チェック ボックスを選択して、ファブリックで ThousandEyes Enterprise Agent を有効にします。
- **[ThousandEyes アカウント グループ トークン（ThousandEyes Account Group Token）]** : インストール用の ThousandEyes Enterprise Agent トークン ID を指定します。
- **[ThousandEyes Agent コレクタ到達可能性のスイッチ上の VRF（VRF on Switch for ThousandEyes Agent Collector Reachability）]** : インターネットの到達可能性を提供する VRF データを指定します。
- **[ドメイン ネーム システム（DNS） ドメイン（DNS Domain）]** : スイッチのドメイン ネーム システム（DNS） ドメイン構成を指定します。
- **[ドメイン ネーム システム（DNS） サーバ IP（DNS Server IPs）]** : ドメイン ネーム システム（DNS） サーバの IP アドレス（v4/v6）のカンマ区切りリストを指定します。DNS サーバには、最大 3 つの IP アドレスを入力できます。
- **[NTP サーバ IP（NTP Server IPs）]** : Network Time Protocol (NTP) サーバの IP アドレス（v4/v6）のコンマ区切りリストを指定します。NTP サーバには、最大 3 つの IP アドレスを入力できます。
- **[プロキシを有効にする（Enable Proxy）]** : チェックボックスをオンにして、NX-OS スイッチのインターネット アクセスのプロキシ設定を選択します。
- **[プロキシ情報（Proxy Information）]**: プロキシ サーバのポート情報を指定します。
- **[プロキシ バイパス（Proxy Bypass）]** : プロキシをバイパスするサーバー リストを指定します。

eBGP アンダーレイを備えた VXLAN ファブリック：ポインタ

- すべてのリーフスイッチには共通の AS 番号があるため、リーフ オーバーレイ ポリシーとアンダーレイ ポリシーを一度にすべてのリーフスイッチに展開します。
- ブラウンフィールド移行は、eBGP ファブリックではサポートされていません。
- リーフスイッチの AS 番号は、作成後に再計算と展開（Recalculate & Deploy）操作を実行した後は変更できません。変更が必要になった場合は、**leaf_bgp_asn** ポリシーを削除し、再計算と展開（Recalculate & Deploy）操作を実行して、この AS に関連する BGP 構成を削除する必要があります。次に、新しい AS 番号を使用して、leaf_bgp_asn ポリシーを追加できます。

- Multi-AS モードと Dual-AS モードを切り替える場合は、モードを変更する前に、手動で追加されたすべての BGP ポリシー（リーフスイッチの Leaf_bgp_asn および ebgp オーバーレイ ポリシーを含む）を削除し、**[保存と展開（Save & Deploy）]** 操作を実行します。
- デバイスに ebgp オーバーレイ ポリシーが存在する場合、リーフスイッチの leaf_bsp_asn ポリシーを変更または削除することはできません。最初に ebgp オーバーレイ ポリシーを削除してから、leaf_bgp_asn ポリシーを削除する必要があります。
- サポートされているロールは、リーフ、スパイン、ボーダー リーフです。
- ボーダー デバイスでは、VRF-Lite は手動モードでサポートされます。外部接続のマルチサイト サポートはありません。
- TRM はサポートされています。
- 機能ファブリックのリーフスイッチとスパイン スイッチにポリシーを適用する必要があります。
- VXLAN 対応ファブリックの場合、Easy Fabric と同じ方法でオーバーレイ ネットワークと VRF を作成して展開できます。詳細については、『*Cisco DCNM LAN* ファブリックの構成ガイド』の「ネットワークおよび *VRF* の作成と展開」章を参照してください。

ファブリック アンダーレイ eBGP ポリシーの展開



トポロジは、eBGP アンダーレイが有効化された VXLAN ファブリックを表示します。DCNM では、**[Easy_Fabric_eBGP]** テンプレートを持つファブリックが作成されます。1 つのスパイン スイッチ（n9k-29）と 3 つのリーフスイッチ（n9k-30、および vPC スイッチ ペア：n9k-31 と n9k-32）がインポートされています。

ファブリックには次の 2 種類があります。

- **マルチ AS モード ファブリックの作成**：マルチ AS モード ファブリックでは、スパイン スイッチには共通の BGP AS 番号があり、各リーフ スイッチには一意の BGP AS 番号があります。Dual-AS から Multi-AS モードへのファブリック変換にも同じ手順を使用します。
- **[Dual-AS モード ファブリックの作成（Creating a Dual-AS mode fabric）]**：Dual-AS モードファブリックの作成については、別の手順が説明されています。Multi-AS から Dual-AS モードへのファブリック変換にも同じ手順を使用します。

  Dual-AS ファブリックでは、すべてのスパイン スイッチには共通の BGP AS 番号があり、すべてのリーフスイッチには共通の BGP AS 番号があります（スパイン スイッチの BGP AS 番号とは異なります）。次のセクションで説明するように、ポリシーを展開する必要があります。

ファブリック アンダーレイ eBGP ポリシーを展開するには、各リーフ スイッチに **leaf_bgp_asn** ポリシーを手動で追加して、スイッチで使用される BGP AS 番号を指定する必要があります。後ほど **[保存と展開（Save & Deploy）]** 操作を実施すると、リーフスイッチとスパイン スイッチ間の物理インターフェイス上に eBGP ピアリングが生成され、アンダーレイの到達可能性情報が交換されます。

1. 画面左側の **[表形式ビュー（Tabular View）]** をクリックします。**Switches | Links** 画面が表示されます。
2. リーフスイッチ（たとえば、n9k-30 チェックボックス）を選択し、**[ポリシーの表示/編集（View/Edit Policies）]** をクリックします。[ポリシーの表示/編集（View/edit policies）] 画面が表示されます。

（注） Dual-AS モードで eBGP ファブリックを作成する場合（または Multi-AS モードから Dual-AS モードに変更する場合）、すべてのリーフスイッチを選択します。これは、共通の BGP AS 番号があるためです。

3. [追加（Add）] をクリックします。**[ポリシーの追加（Add Policy）]** 画面が表示されます。
4. [ポリシー（Policy）] ドロップダウンボックスから、**leaf_bgp_asn** を選択し、**[BGP AS #]** フィールドに BGP AS 番号を入力します。
5. [保存（Save）] をクリックします。
6. vPC スイッチに対してこの手順を繰り返します。vPC スイッチ ペアの場合は、両方のスイッチを選択し、**leaf_bgp_asn** ポリシーを適用します。

（注） 前の手順で説明したように、Dual-AS モードでファブリックを作成（または Dual-AS モードに変換）し、それらすべてに BGP AS 番号を割り当てている場合、この手順は必要ありません。

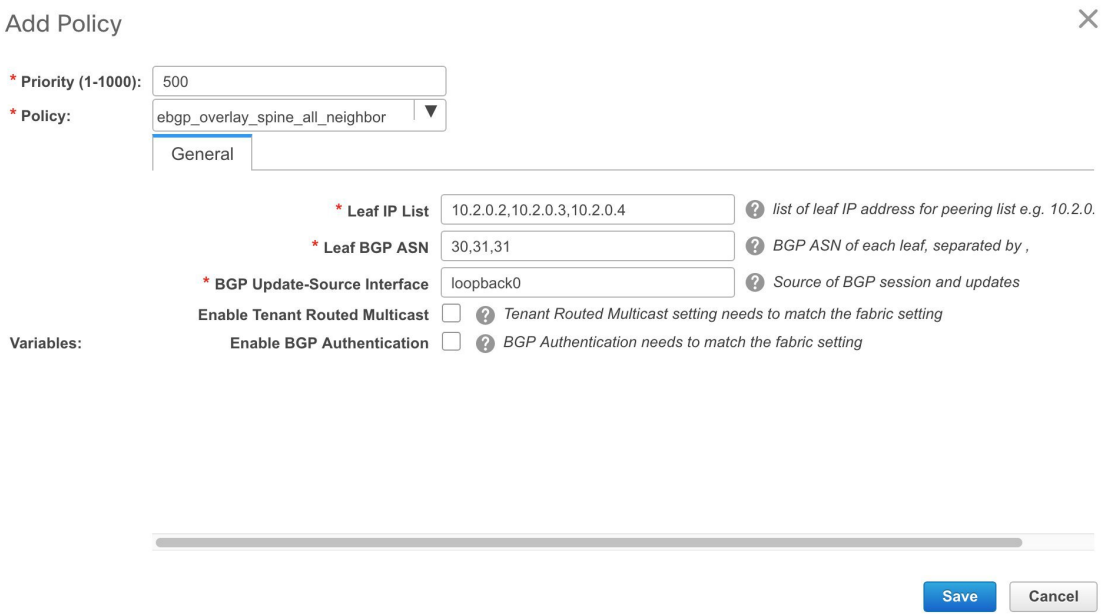
7. **[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウを閉じます
8. トポロジ画面で、画面の右上にある **[保存と展開（Save & Deploy）]** をクリックします。
9. **構成展開** ウィザードに従って構成を展開します。

ファブリック オーバーレイ eBGP ポリシーの展開

オーバーレイ ピアリングの eBGP オーバーレイ ポリシーは手動で追加する必要があります。DCNM は、リーフおよびスパイン スイッチに手動で追加して EVPN オーバーレイ ピアリングを形成できる eBGP リーフおよびスパイン オーバーレイ ピアリング ポリシー テンプレートを提供します。

スパイン スイッチ オーバーレイ ポリシーの展開

ebgp_overlay_spine_all_neighbor ポリシーをスパイン スイッチ n9k-29 に追加します。このポリシーは、すべてのスパイン スイッチで同じフィールド値を共有するため、一度にすべてのスパイン スイッチに展開できます。



この画面のフィールドは次のとおりです。

[リーフ IP リスト（Leaf IP List）]：リーフ スイッチ ルーティング ループバック インターフェイスの IP アドレス。

10.2.0.2 は、リーフスイッチ n9k-30 のループバック 0 ピアリング IP アドレスです。10.2.0.3 および 10.2.0.4 は、vPC スイッチ ペア n9k-31 および n9k-32 の IP アドレスです。

[リーフ BGP ASN（Leaf BGP ASN）]：リーフ スイッチの BGP AS 番号。vPC スイッチの AS 番号は同じ 31 であることに注意してください。

（注） デュアル AS モードでファブリックを作成する場合（またはデュアル AS モードに変換する場合）、すべてのリーフスイッチが属する共通の BGP AS 番号でこのフィールドを更新する必要があります。

[BGP アップデート送信元インターフェイス（BGP Update-Source Interface）]：BGP アップデートの送信元インターフェイスです。このフィールドでは loopback0、つまり、アンダーレイ ルーティングのループバック インターフェイスを使用できます。

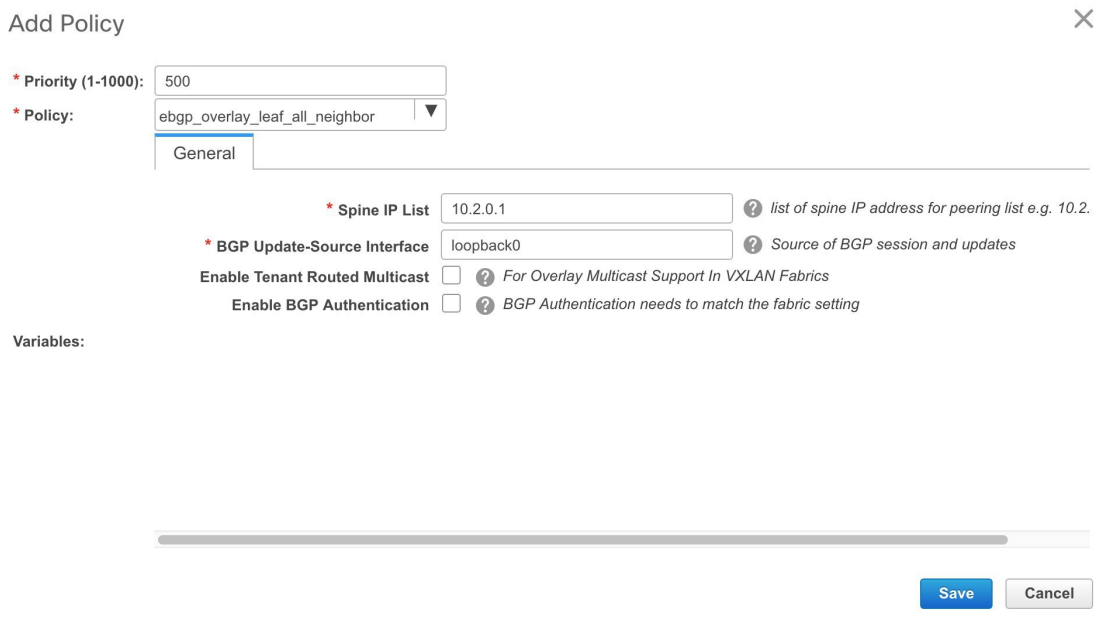
[テナント ルーテッド マルチキャストを有効にする（Enable Tenant Routed Multicast）]：チェックボックスをオンにして、オーバーレイ マルチキャスト トラフィックを処理するための TRM を有効にします。TRM の有効化は、ファブリック設定と一致する必要があります。

[BGP 認証の有効化（Enable BGP Authentication）]：BGP 認証を有効にするにはチェックボックスをオンにします。

BGP 認証は、ファブリック設定と一致する必要があります。BGP 認証の詳細については、「認証キーの取得」セクションを参照してください。

リーフ スイッチ オーバーレイ ポリシーの展開

すべてのリーフ スイッチに **ebgp_overlay_leaf_all_neighbor** ポリシーを追加して、スパイン スイッチへの eBGP オーバーレイ ピアリングを確立します。このポリシーは、すべてのリーフ スイッチで同じフィールド値を共有するため、一度にすべてのリーフ スイッチに展開できます。



この画面のフィールドは次のとおりです。

[スパイン IP リスト（Spine IP List）]：スパイン スイッチ ルーティング ループバック インターフェイスの IP アドレス。

10.2.0.1 は、スパイン スイッチ n9k-29 のループバック 0 ピアリング IP アドレスです。

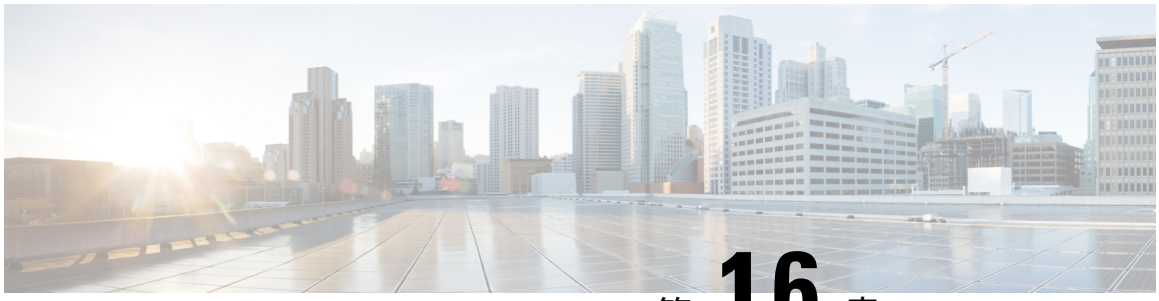
[BGP アップデート送信元インターフェイス（BGP Update-Source Interface）]：BGP アップデートの送信元インターフェイスです。このフィールドでは loopback0、つまり、アンダーレイ ルーティングのループバック インターフェイスを使用できます。

[テナント ルーテッド マルチキャストを有効にする（Enable Tenant Routed Multicast）]：チェックボックスをオンにして、オーバーレイ マルチキャスト トラフィックを処理するための TRM を有効にします。TRM の有効化は、ファブリック設定と一致する必要があります。

[BGP 認証の有効化（Enable BGP Authentication）]：BGP 認証を有効にするにはチェックボックスをオンにします。

BGP 認証は、ファブリック設定と一致する必要があります。BGP 認証の詳細については、「認証キーの取得」セクションを参照してください。

画面の右上にある **[保存と展開（Save & Deploy）]** をクリックして、構成展開ウィザードごとに構成を展開します。または、**[ポリシーの表示/編集（View/Edit Policy）]** オプションを使用し、**[構成のプッシュ（Push Config）]** をクリックして構成を展開します。



第 16 章

ブラウンフィールド VXLAN BGP EVPN ファブリックの管理

この章では、ブラウンフィールド ファブリックを Cisco DCNM に移行する方法について説明します。

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 DCNM 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構成の DCNM 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、DCNM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DCNM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

- DCNM サポート対象の NX-OS ソフトウェア バージョン詳細については、Cisco DCNM 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。
- サポートされているアンダーレイは、Cisco.com で入手可能な VXLAN ファブリック用の DCNM 10.2(1) POAP テンプレートのベストプラクティス（dcnm_ip_vxlan_fabric_templates.10.2.1.ST.1.zip）に基づいています。
- 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デーレイ ランデブー ポイント ループバック ID。
- BGP 構成では、「router-id」を使用します。これはルーティング ループバック インターフェイスの IP アドレスです。
- iBGP ピア テンプレートが構成されている場合は、リーフ スイッチとルート リフレクタで構成する必要があります。リーフ リフレクタとルート リフレクタの間で使用する必要があるテンプレート名は同じにするべきです。
- BGP ルート リフレクタおよびマルチキャスト ランデブー ポイント（該当する場合）機能が、スパイン スイッチに実装されていること。リーフ スイッチはこの機能をサポートしていません。
- VXLAN BGP EVPN ファブリックの概念と、DCNM の観点から見たファブリックの機能に関する知識があること。
- ファブリック スイッチ ノードの動作は安定していて機能しており、すべてのファブリック リンクがアップ状態であること。
- vPC スイッチとピア リンクは、移行前にアップ状態になっていること。構成の更新が進行中でないこと、保留中の変更がないことを確認してください。
- IP アドレスとログイン情報を使用して、ファブリック内のスイッチのインベントリ リストを作成します。DCNM 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 DCNM 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 DCNM 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。

ガイドラインと制約事項

- ファブリック インターフェイスは、番号付きまたは番号なしにすることができます。
- 他の各種インターフェイス タイプがサポートされています。
- Cisco DCNM リリース 11.5(1) 以降、DCNM で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 9.3(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。
  - eBGP アンダーレイ
  - レイヤ 3 ポートチャネル
- 移行前に、スイッチ構成のバックアップを取り、保存します。
- 移行が完了するまで、スイッチの構成を変更してはなりません（このドキュメントで指示されている場合を除く）。変更すると、重大なネットワークの問題が発生する可能性があります。
- Cisco DCNM 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。
- スイッチでのマルチライン バナーの構成は、switch_freeform 構成内にキャプチャされた他の構成と共に（存在する場合）、switch_freeform 構成内で保持されます。
- DCNM リリース 11.2(1) 以降、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。
- IS-IS Level-1 および Level-2 のファブリックはブラウンフィールド移行でサポートされています。
- Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x) イメージを使用したスイッチは、ブラウンフィールド移行をサポートしています。機能の互換性については、それぞれのプラッ

トフォームのマニュアルを参照してください。サポートされているソフトウェア画像については、「*Cisco DCNM* の互換性マトリクス」を参照してください。

次の注意事項および制限事項に注意してください。

- ネットワークまたは VRF の VLAN 名は、少なくとも 1 つの非スパイン スイッチに Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x) の画像がある場合、オーバーレイ プロファイル内にキャプチャされません。VLAN名は、オーバーレイ ネットワークまたは VRF に関連付けられた自由形式の構成にキャプチャされます。VLAN 名は自由形式の構成をアップデートすることにより、変更できます。詳細については、「*Cisco NX-OS* リリース *7.0(3)I4(8b)* および *7.0(4)I4(x)* のイメージに沿って、スイッチで *VLAN* 名を変更する」を参照してください。
- 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 スイッチの TCAM CLI での構成遵守の違い詳細については、「*Cisco NX-OS* リリース *7.0(3)I4(8b)* および *7.0(4)I4(x)* の画像に沿って、スイッチでの構成遵守エラーを解決する」
- オーバーレイ プロファイルのリフレッシュ機能は、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。

- Cisco Nexus 9500 シリーズ スイッチは、Cisco NX-OS リリース 7.0.3.I7(3) またはそれ以降で、ボーダー スパイン、BGW スパイン、またはリーフ ロールを搭載した VTEP としてサポートされます。
- Cisco DCNM リリース 11.1(1) でのブラウンフィールド移行の間、オーバーレイ構成プロファイルはスイッチに展開され、すべてのオーバーレイ関連の構成はそれぞれ対応するネットワークまたは VRF 自由形式構成でキャプチャされます。移行後、スイッチには元の構成 CLI と構成プロファイルがあります。

  Cisco DCNM リリース 11.2(1) 以降、ブラウンフィールド移行の間、オーバーレイ構成プロファイルはスイッチに展開され、元の構成 CLI は削除されます。ブラウンフィールド移行のスイッチに次の Cisco NX-OS イメージがある場合、移行後のスイッチには構成プロファイルと他の余計な構成（構成プロファイルの一部ではないもの）のみが存在します。

  - Cisco NX-OS リリース 7.0(3)I7(6) またはそれ以降
  - Cisco NX-OS リリース 9.2(3) またはそれ以降

  スイッチがこれらの要件に一致しない場合、ブラウンフィールド移行の動作は Cisco DCNM リリース 11.1(1) で説明されているのと同様になります。
- 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。

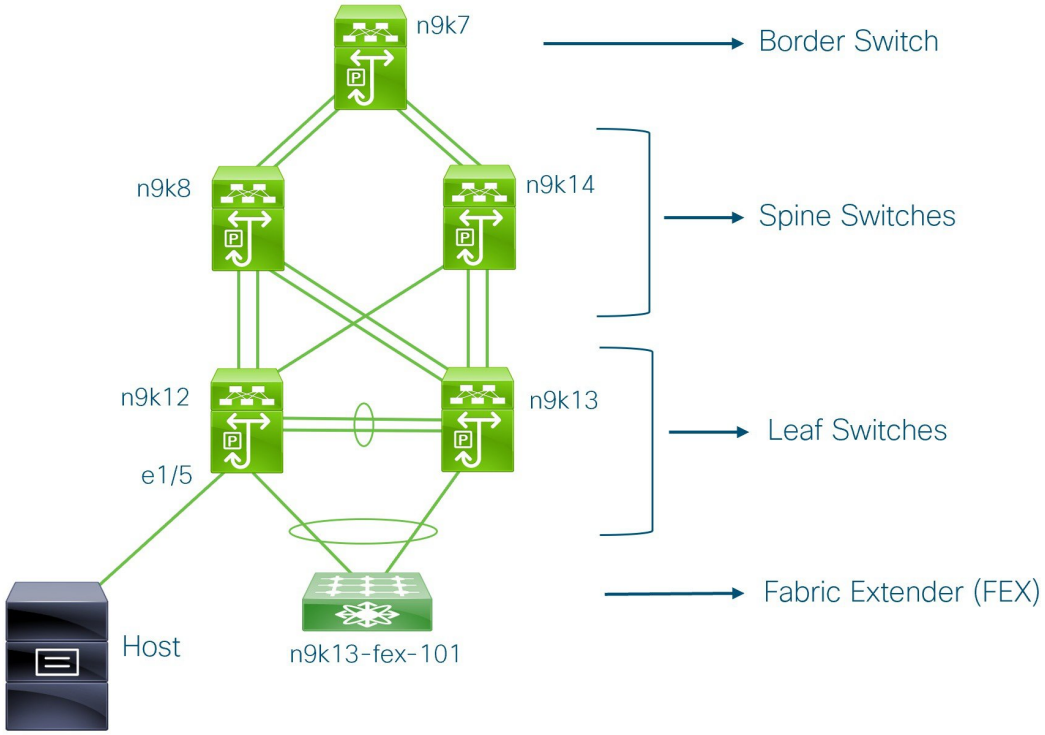
ファブリック トポロジの概要

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 NX-OS（リリース 7.0(3)I7(6)）
- 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、「*Cisco DCNM* の互換性マトリックス」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。

DCNM 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 （834 ページ）
2. #unique_500
3. #unique_501
4. VXLAN BGP EVPN ファブリックのインポートの確認 （867 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 DCNM 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。

VXLAN BGP EVPN ファブリックの作成

この手順では、DCNM で VXLAN BGP EVPN ファブリックを作成する方法を示します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

[ファブリック ビルダ（Fabric Builder）] 画面が表示されます。初めてログインしたときには、**[ファブリック（Fabrics）]** セクションにはまだエントリはありません。ファブリックを作成す

ると、**[ファブリック ビルダ（Fabric Builder）]** 画面に表示されます。長方形のボックスが各ファブリックを表します。

スタンドアロンまたはメンバー ファブリックには、Switch_Fabric（タイプ フィールド）、AS 番号（ASN フィールド）、および複製モード（複製モード フィールド）が含まれます。

ステップ 2 [ファブリックの作成（Create Fabric）] をクリックします。**[ファブリックの追加（Add Fabric）]** ウィンドウが表示されます。

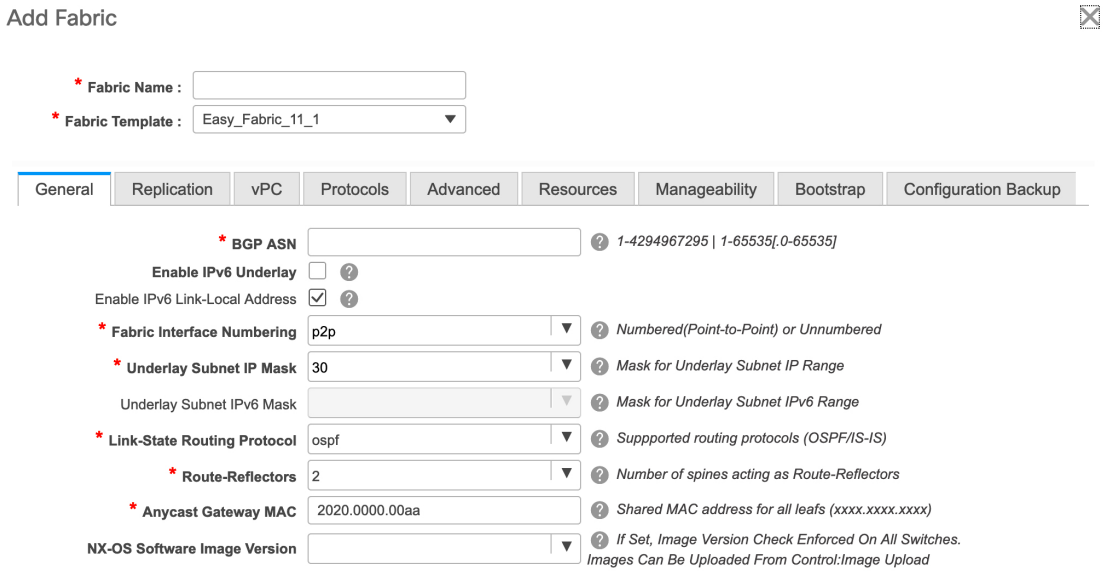
[ファブリック テンプレート（Fabric Template）]：ドロップダウン メニューから、**Easy_Fabric_11_1** ファブリック テンプレートを選択します。スタンドアロン ファブリックを作成するためのファブリック設定が表示されます。

[ファブリック名（Fabric Name）]：ファブリックの名前を入力します。

画面のタブとそのフィールドについては、以降のポイントで説明します。オーバーレイおよびアンダーレイ ネットワーク パラメータは、これらのタブに含まれています。

Note MSD ファブリックの潜在的なメンバー ファブリックとしてスタンドアロン ファブリックを作成する場合（EVPN マルチサイト テクノロジーを介して接続されるファブリックのオーバーレイ ネットワークのプロビジョニングに使用）、メンバー ファブリックの作成前に、トピック「VXLAN BGP EVPN ファブリックのマルチサイト ドメイン」を参照してください。

ステップ 3 デフォルトでは **[全般（General）]** タブが表示されます。このタブのフィールドは次のとおりです。



[BGP ASN]：ファブリックが関連付けられている BGP AS 番号を入力します。

[IPv6 アンダーレイの有効化（Enable IPv6 Underlay）]：このチェックボックスを選択して、IPv6 アンダーレイ機能を有効にします。

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。

IPv6 アンダーレイの詳細については、*VXLANv6* ファブリックの構成を参照してください。

[ファブリック インターフェイスの番号付け（Fabric Interface Numbering）]：既存のセットアップで、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）]：既存のセットアップでファブリック アンダーレイ IP アドレス サブネットに使用するサブネット マスクを指定します。

[ルートリフレクタ（Route-Reflectors）]：ルートリフレクタのカウントは移行後にのみ適用可能です。既存のルート リフレクタの構成は、DCNM セットアップへのインポート時に優先されます。

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 デバイスをルート リフレクタとして展開するには、DCNM はスパイン デバイスをシリアル番号に基づいてソートし、2 つまたは 4 つのスパイン デバイスをルート リフレクタとして指定します。スパイン デバイスを追加しても、既存のルート リフレクタ構成は変更されません。

カウントの増加：ルート リフレクタを任意の時点で 2 から 4 に増やすことができます。構成は、ルート リフレクタとして指定された他の 2 つのスパイン デバイスで自動的に生成されます。

カウントの削減

4 つのルート リフレクタを 2 つに減らす場合に、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する必要があります。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）。

既存のルート リフレクタ デバイスを削除する場合、次に使用可能なスパイン スイッチを置き換えるルート リフレクタとして選択します。

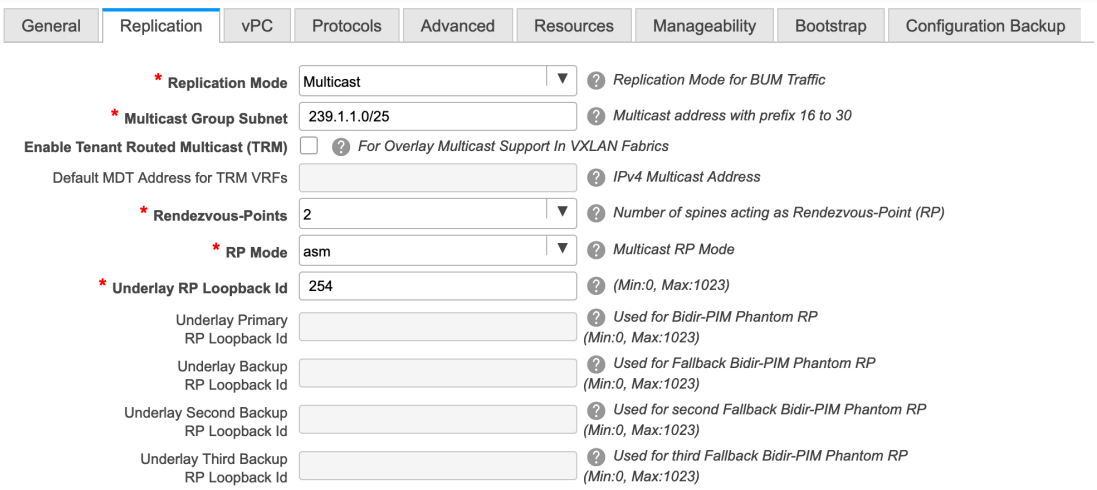
d. [ファブリック トポロジ（Fabric Topology）] スクリーンの右上にある [保存して展開（Save and Deploy）] をクリックします。

最初の [保存と展開（Save & Deploy）] 操作を実行する前に、RR と RP を事前に選択できます。詳細については、「ルート リフレクタおよびランデブー ポイントとしてのスイッチの事前選択」を参照してください。。

Anycast Gateway MAC：既存のファブリックの Anycast ゲートウェイ MAC アドレスを入力します。

NX-OS ソフトウェア イメージ バージョン：このフィールドは空欄のままにします。この post-transition は必要に応じてアップデートできます。

ステップ 4 **[レプリケーション（Replication）]** タブをクリックします。ほとんどのフィールドは自動生成されます。



[レプリケーション モード（Replication Mode）]：既存のファブリック、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。

[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 レプリケーション フィールドは無効になります。

[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の IP アドレスプレフィックスは移行後の割り当てに使用されます。既存のファブリックで使用される IP アドレスプレフィックスは以降の間、優先されます。

オーバーレイ ネットワークごとに、このグループから一意の IP アドレスが割り当てられます。

[テナント ルーテッド マルチキャストを有効にする（Enable Tenant Routed Multicast）]：ファブリック オーバーレイ マルチキャスト プロトコルとしてテナント ルーテッド マルチキャスト（TRM）を有効にするには、チェックボックスをオンにします。

TRM を有効化する場合、TRM のマルチキャストアドレスを入力する必要があります。すべての TRM 固有のテナント構成は、テナント ネットワークおよび VRF プロファイルにリンクされたスイッチ自由形式ポリシーでキャプチャされます。

TRM 機能は、Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x) イメージを持つスイッチでサポートされていないことに注意してください。

[TRM VRF のデフォルト MDT アドレス（Default MDT address for TRM VRFs）]：TRM VRF のデフォルトのマルチキャスト配布ツリー（MDT）IPv4 アドレスを入力します。

[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**（Any-Source Multicast）または **bidir**（双方向 PIM）モードを選択してください。

[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。

asm RP モードは最大 4 つの RP をサポートします。

bidir モードは最大 2 つの RP をサポートします。BIDIR 構成により 2 つ以上の RP が使用されていることを示す場合、エラー メッセージが表示されます。

ブラウンフィールド移行の後、移行済みファブリックでサポートされるのは 2 つの RP のみです。RP カウントを 4 に変更後、**[保存と展開（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。

RP をファブリックから削減または削除した場合、この RP は他のスパインに置き換えることができません。Easy Fabric は削除されたスイッチの構成内容を保持しないためです。Easy Fabric は固有のスキームを使用して Bidir に RP 構成を生成します。そのため、生成された Bidir 構成は、ブラウンフィールドがインポートされた構成では動作しません。ブラウンフィールド移行後、RP カウントを変更、または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 機能を手動で構成する必要があります。手動による構成が必要な場合、**[保存と展開（Save & Deploy）]** をクリックした後で、警告メッセージが表示されます詳細については、「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」を参照してください。

また、ブラウンフィールドがインポート済みの bidir 構成を変更して、**ファブリック ビルダ** によって生成された構成を使用できます。詳細については、「ブラウンフィールドでインポートされた *BIDIR* 構成の変更」を参照してください。

[アンダーレイ RP ループバック ID（Underlay RP Loopback ID）]：ループバック ID は既存セットアップのループバック ID と一致する必要があります。これは、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。

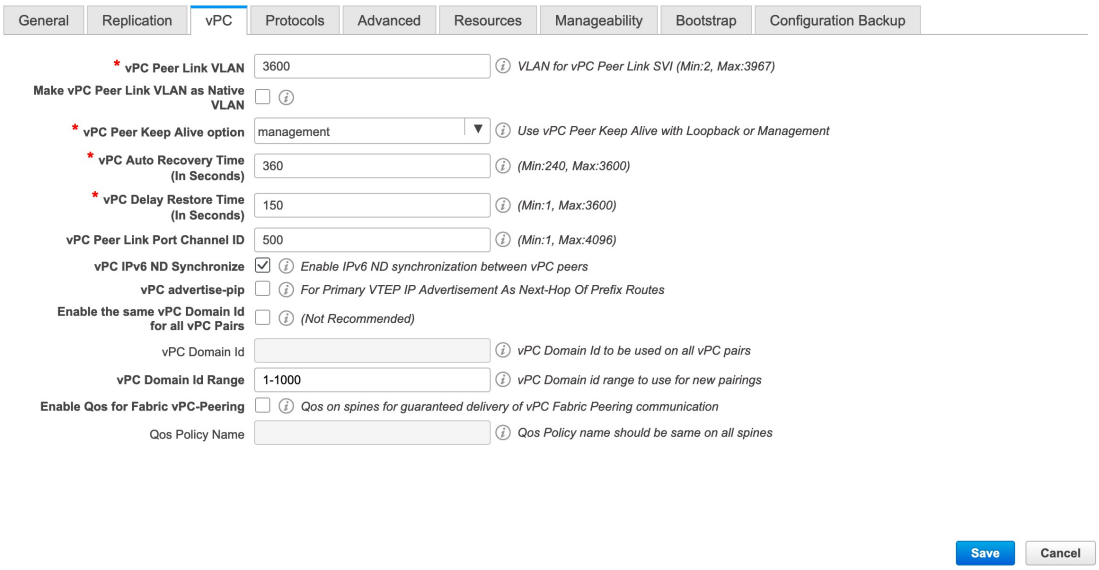
[アンダーレイ バックアップ RP ループバック ID（Underlay Backup RP Loopback ID）]：ファブリック アンダーレイでマルチキャスト プロトコル ピアリングを目的として、ファントム RP に使用されるセカンダリ ループバック ID です。

Rendezvous-Points が 4 に設定されている場合、次の 2 つのフィールドは有効化されています。ただし、ファブリックはブラウンフィールド移行の RP は 2 つのみ持つことができます。

[アンダーレイ セカンド バックアップ RP ループバック ID（Underlay Second Backup RP Loopback ID）]：ファブリック アンダーレイでマルチキャスト プロトコル ピアリングを目的としてファントム RP に使用される、第二のフォールバック 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、第三のフォールバック ループバック ID です。

ステップ 5 **[vPC]** タブをクリックします。ほとんどのフィールドは自動生成されます。



[vPC ピア リンク VLAN（vPC Peer Link VLAN）]：既存のファブリックでの vPC ピア リンク SVI に使用する VLAN ID を入力します。

[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）]：既存のファブリックで使用するため、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。

管理インターフェイスで IPv6 アドレスのみを使用する場合、ループバック オプションを使用する必要があります。

移行の間、スイッチ構成は vPC タブの次のフィールドでチェックされません。異なる場合、スイッチ構成はアップデートされます。

[vPC 自動回復時間（vPC Auto Recovery Time）]：必要に応じて、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）]：必要に応じて、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。既存の設定に基づいて値を変更します。

[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。必要に応じて、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。

Advertise PIP 機能は、Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x) イメージを持つスイッチでサポートされていないことに注意してください。

[すべての vPC ペアに同じ vPC ドメイン ID を有効にする（Enable the same vPC Domain Id for all vPC Pairs）]：すべての vPC ペアに同じ vPC ドメイン ID を有効にします。このフィールドを選択すると、[vPC ドメイン ID（vPC Domain Id）] フィールドが編集可能になります。

[vPCドメインID（vPC Domain Id）]：すべての vPC ペアで使用される vPC ドメイン ID を指定します。

[vPC ドメイン ID の範囲（vPC Domain Id Range）]：新しいペアリングに使用する vPC ドメイン ID の範囲を指定します。

[ファブリック vPC ピアリングの QoS を有効にする（Enable QoS for Fabric vPC-Peering）]：スパインの QoS を有効にして、vPC ファブリック ピアリング通信の配信を保証します。詳細については、ファブリック vPC ピアリングの QoS, on page 277を参照してください。

Note ファブリック設定の vPC ファブリック ピアリングとキューイング ポリシーの QoS オプションは相互に排他的です。

[QoS ポリシー名（QoS Policy Name）]：すべてのファブリック vPC ピアリング スパインで同じにする必要がある QoS ポリシー名を指定します。デフォルト名は [spine_qos_for_fabric_vpc_peering] です。

ステップ 6 **[プロトコル（Protocols）]** タブをクリックします。ほとんどのフィールドは自動生成されます。必要に応じてフィールドを更新できます。

[アンダーレイ ルーティング ループバック ID（Underlay Routing Loopback Id）]：通常は loopback0 がファブリック アンダーレイ IGP ピアリングに使用されるため、ループバック インターフェイス ID は 0 に設定されます。これは、スイッチ上の既存の構成と一致する必要があります。これは、すべてのスイッチに全体で同様です。

[アンダーレイ VTEP ループバック ID（Underlay 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。これは、スイッチ上の既存の構成と一致する必要があります。VTEP が存在する場合にすべてのスイッチに全体で同様です。

[リンクステート ルーティング プロトコル タグ（Link-State Routing Protocol Tag）]：既存のファブリックのルーティング プロトコル タグをこのフィールドに入力し、ネットワークのタイプを定義します。

[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、既存のファブリックの OSPF エリア ID です。

Note OSPF または IS-IS 認証フィールドは、**[全般（General）]** タブの**[リンクステート ルーティング プロトコル（Link-State 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（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）]：OSPF 認証キー ID を入力します。

[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、OSPF 認証の詳細を取得します。

使用中のスイッチで **show run ospf** コマンドを使用することで OSPF 認証の詳細を取得することができます。

```
# show run ospf | grep message-digest-key
ip ospf message-digest-key 127 md5 3 c7c83ec78f38f32f3d477519630faf7b
```

この例では、OSPF 認証キー ID は **127** で、認証キーは **c7c83ec78f38f32f3d477519630faf7b** です。

新しいキーを構成して取得する方法については、「認証キーの取得」を参照してください。

[IS-IS レベル（IS-IS Level）]：このドロップダウン リストから IS-IS レベルを選択します。

[IS-IS 認証の有効化（Enable IS-IS Authentication）]：IS-IS 認証を有効にするにはチェックボックスをオンにします。無効にするにはチェックボックスをオフにします。このフィールドを有効にすると、IS-IS 認証フィールドが有効になります。

[IS-IS 認証キーチェーン名（IS-IS Authentication Keychain Name）]：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）]：IS-IS 認証キー ID を入力します。

[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、IS-IS 認証の詳細を取得します。

使用中のスイッチで **show run | section "key chain"** コマンドを使用することで IS-IS 認証の詳細を取得することができます。

```
# show run | section "key chain"
key chain CiscoIsisAuth
  key 127
      key-string 7 075e731f
```

この例では、キーチェーン名は **CiscoIsisAuth**、キー ID は **127**、およびタイプ 7 認証キーは **075e731f** です。

[BGP 認証の有効化（Enable BGP Authentication）]：BGP 認証を有効にするにはチェックボックスをオンにします。無効にするにはチェックボックスをオフにします。このフィールドを有効にすると、**[BGP 認証キー暗号化タイプ（BGP Authentication Key Encryption Type）]** および **[BGP 認証キー（BGP Authentication Key）]** フィールドが有効になります。

[BGP 認証キー暗号化タイプ（BGP Authentication Key Encryption Type）]：3DES 暗号化タイプの場合は 3、Cisco 暗号化タイプの場合は 7 を選択します。

[BGP 認証キー（BGP Authentication Key）]：暗号化タイプに基づいて暗号化キーを入力します。

Note プレーン テキスト パスワードはサポートされていません。スイッチにログインし、BGP 認証の詳細を取得します。

使用中のスイッチで **show run bgp** コマンドを使用することで BGP 認証の詳細を取得することができます。

```
# show run bgp
neighbor 10.2.0.2
remote-as 65000
password 3 sd8478fswerdfw3434fsw4f4w34sdsd8478fswerdfw3434fsw4f4w3
```

この例では、暗号化タイプ **3** の後に、BGP 認証キーが表示されます。

[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 機能の有効化（Enable BFD feature）]：BFD 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。

この機能はデフォルトで無効に設定されています。

BFD 機能の設定がスイッチ構成と一致するようにしてください。スイッチ構成に **feature bfd** が含まれる場合でも、BFD機能がファブリック設定で有効化されていない場合、ブラウンフィー

ルド移行の後で構成遵守は diff を生成して BFD 機能を削除します。つまり、**no feature bfd** は移行後に生成されます。

Cisco DCNM リリース 11.3(1) 以降、ファブリック内の BFD はネイティブにサポートされます。ファブリック設定では、BFD機能はデフォルトで無効になっています。有効にすると、デフォルト設定のアンダーレイ プロトコルに対して BFD が有効になります。カスタムの必須 BFD 構成は、スイッチごとの自由形式またはインターフェイスごとの自由形式ポリシーを使用して展開する必要があります。

[BFD の有効化（Enable BFD）] チェックボックスをオンにすると、次の構成がプッシュされます。

```
feature bfd
```

BFD機能の互換性については、それぞれのプラットフォームのマニュアルを参照してください。サポートされているソフトウェア画像については、「*Cisco DCNM* の互換性マトリクス」を参照してください。

[iBGP 向け BFD の有効化（Enable BFD for iBGP）]：iBGP ネイバーの BFD を有効にするには、このチェックボックスをオンにします。このオプションは、デフォルトで無効です。

[OSPF 向け BFD の有効化（Enable BFD for OSPF）]：このチェックボックスをオンにすると、OSPF アンダーレイ インスタンスの BFD が有効になります。このオプションはデフォルトで無効になっており、リンクステートプロトコルがISISの場合はグレー表示されます。

[ISIS 向け BFD の有効化（Enable BFD for ISIS）]：このチェックボックスをオンにして、ISIS アンダーレイ インスタンスの BFD を有効にします。このオプションはデフォルトで無効になっており、リンク ステート プロトコルが OSPF の場合はグレー表示されます。

[PIM 向け BFD の有効化（Enable BFD for PIM）]：PIM の BFD を有効にするには、このチェックボックスをオンにします。このオプションはデフォルトで無効になっており、レプリケーション モードが [入力（Ingress）] の場合はグレー表示されます。

BFD グローバル ポリシーの例を次に示します。

```
router ospf <ospf tag>
   bfd

router isis <isis tag>
  address-family ipv4 unicast
    bfd

ip pim bfd

router bgp <bgp asn>
  neighbor <neighbor ip>
    bfd
```

[BGP 認証の有効化（Enable BGP Authentication）]：BGP 認証を有効にするにはチェックボックスをオンにします。このフィールドを有効にすると、[BFD 認証キー ID（BFD Authentication Key ID）] フィールドと [BFD 認証キー（BFD Authentication Key）] フィールドが編集可能になります。

Note

- [全般（General）] タブの [ファブリック インターフェイスの番号付け（Fabric Interface Numbering）] フィールドが [番号付けなし（unnumbered）] に設定されている場合、BFD 認証はサポートされません。BFD 認証フィールドは自動的にグレー表示されます。BFD認証は、P2Pインターフェイスに対してのみ有効です。
- BFD が有効になっている DCNM リリース 11.2(1) から DCNM リリース 11.3(1) にアップグレードすると、次の構成がスイッチにプッシュされます。

```
no ip redirects
no ipv6 redirects
```

[BFD 認証キー ID（BFD Authentication Key ID）]：インターフェイス認証の BFD 認証キー ID を指定します。デフォルト値は 100 です。

[BFD 認証キー（BFD Authentication Key）]：BFD 認証キーを指定します。

BFD 認証パラメータを取得する方法については、「認証キーの取得」を参照してください。

[iBGP ピアテンプレート構成（iBGP Peer-Template Config）]：リーフスイッチおよびルートリフレクタに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。スイッチ構成に基づいてこのフィールドを設定します。このフィールドがブランクの場合、iBGP ピア テンプレートが使用されていないことを意味します。iBGP ピア テンプレートが使用されている場合、スイッチで定義されているピア テンプレート定義を入力してください。BGP で構成されているデバイスのピア テンプレート名は、ここで定義されているものと同一にする必要があります。

Note iBGPピアテンプレートを使用する場合、このテンプレート構成フィールドのBGP認証構成を含めるようにしてください。さらに、BGP構成の重複を避けるために、[BGP認証を有効化する（Enable BGP Authentication）] チェックボックスのチェックを外してください。

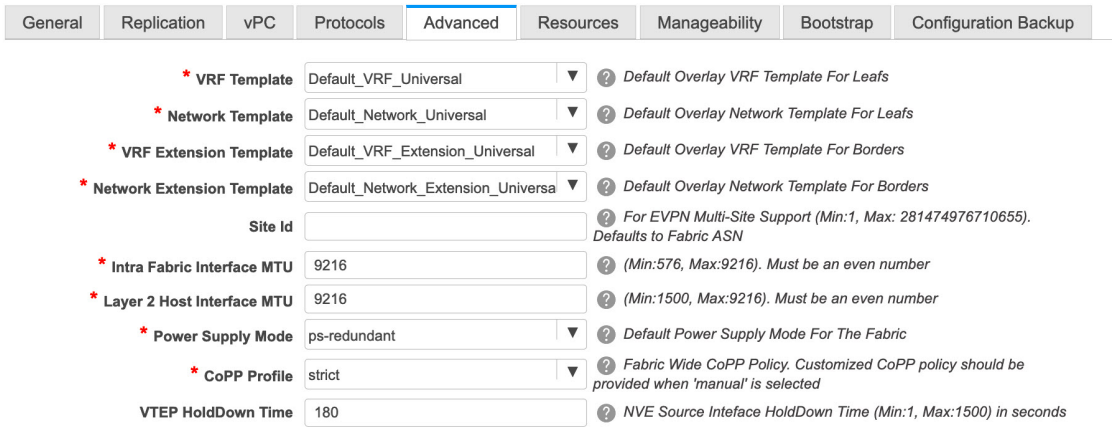
Cisco DCNM リリース 11.3(1) までは、リーフまたはボーダー ロール デバイスの iBGP 定義の iBGP ピア テンプレートと BGP RR は同じでした。DCNM リリース 11.4(1) 以降、次のフィールドを使用してさまざまな構成を指定できます。

- [iBGP ピアテンプレート構成（iBGP Peer-Template Config）]：境界ロールを持つ RR およびスパインに使用される構成を指定します。
- [リーフ/境界/境界ゲートウェイ iBGP ピアテンプレート構成（Leaf/Border/Border Gateway iBGP Peer-Template Config）]：リーフ、境界、または境界ゲートウェイに使用される構成を指定します。このフィールドが空の場合、[iBGP ピアテンプレート構成（iBGP Peer-Template Config）] で定義されたピア テンプレートがすべての BGP 対応デバイス（RR、リーフ、境界、または境界ゲートウェイ ロール）で使用されます。

ブラウン フィールド移行では、スパインとリーフが異なるピア テンプレート名を使用する場合、**[iBGP ピアテンプレート構成（iBGP Peer-Template Config）]** フィールドと **[リーフ/ボーダー/ボーダーゲートウェイ 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。

ステップ 7 [Advanced] タブをクリックします。ほとんどのフィールドは自動生成されます。



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。

移行中はテンプレートの変更をしないでください。ユニバーサルテンプレートのみ、オーバーレイ移行でサポートされています。

[サイト ID（Site ID）]：このファブリックを MSD 内で移動する場合の ID です。このフィールド post-migration をアップデートすることができます。

[イントラ ファブリック インターフェイス MTU（Intra Fabric Interface MTU）]：ファブリック内インターフェイスの MTU を指定します。この値は偶数にする必要があります。

[レイヤ 2 ホスト インターフェイス MTU（Layer 2 Host Interface MTU）]：レイヤ 2 ホスト インターフェイスの MTU を指定します。この値は偶数にする必要があります。

電源モード（Power Supply Mode）：適切な電源モードを選択します。

[CoPP プロファイル（CoPP Profile）]：既存のファブリックのコントロール プレーン ポリシング（CoPP）プロファイル ポリシーを選択します。デフォルトでは、strict オプションが入力されます。

[VTEP HoldDown 時間（VTEP HoldDown Time）]：NVE 送信元インターフェイスのホールドダウン時間を指定します。

[ブラウンフィールド オーバーレイ ネットワーク名の形式（Brownfield Overlay Network Name Format）]：ブラウンフィールドのインポートまたは移行時にオーバーレイ ネットワーク名を作成するために使用する形式を入力します。ネットワーク名は、アンダースコア（_）および

ハイフン（-）を除く特殊文字または空のスペースが含まれないようにしてください。ブラウンフィールドの移行が開始されたら、ネットワーク名を変更しないでください。ネットワーク名の命名規則については、「スタンドアロンファブリックのネットワークの作成」の項を参照してください。構文は**[<string> | $$VLAN_ID$$] $$VNI$$ [<string>| $$VLAN_ID$$]**です。デフォルト値は **[Auto_Net_VNI$$VNI$$_VLAN$$VLAN_ID$$]** です。ネットワークを作成すると、指定した構文に従って名前が生成されます。次の表で構文内の変数について説明します。

変数	説明
$$VNI$$	スイッチ構成で検出されたネットワーク VNI ID を指定します。これは、一意のネットワーク名を作成するために必要な必須キーワードです。
$$VLAN_ID$$	ネットワークに関連付けられた VLAN ID を指定します。 VLAN ID はスイッチに固有であるため、DCNM はネットワークが検出されたスイッチの 1 つから VLAN ID をランダムに選択し、名前に使用します。 VLAN ID が VNI のファブリック全体で一貫していない限り、これを使用しないことを推奨します。
<string>	この変数はオプションであり、ネットワーク名のガイドラインを満たす任意の数の英数字を入力できます。

オーバーレイ ネットワーク名の例：Site_VNI12345_VLAN1234

Note グリーンフィールド展開では、このフィールドを無視します。ブラウンフィールド オーバーレイ ネットワーク名の形式は、次のブラウンフィールド インポートに適用されます。

- CLI ベースのオーバーレイ
- 構成プロファイルが Cisco DCNM リリースで作成された構成プロファイルベースのオーバーレイ

  10.4(2) で作成された構成プロファイルベースのオーバーレイ

[VXLAN OAM を有効にする（Enable VXLAN OAM）]：既存のスイッチの VXLAM OAM 機能を有効にします。

この設定はデフォルトでイネーブルになっています。VXLAN OAM 機能を無効にするにはチェックボックスをクリアします。

ファブリック内の特定のスイッチで VXLAN OAM 機能を有効にし、他のスイッチで無効にする場合は、自由形式構成を使用して、ファブリック設定で OAM を有効にし、OAM を無効にすることができます。

Note Cisco DCNM の VXLAN OAM 機能は、単一のファブリックまたはサイトでのみサポートされます。

NGOAM 機能は、Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x) イメージを持つスイッチでサポートされていないことに注意してください。

[テナント DHCP を有効にする（Enable Tenant DHCP）]：チェックボックスを選択して、テナント DHCP サポートを有効にします。

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）]：NX-API の有効化を指定します。

[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。

[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。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」を参照してください。

[厳密な構成コンプライアンスの有効化（Enable Strict Config Compliance）]：このチェックボックスをオンにして、厳密な構成コンプライアンス機能を有効にします。デフォルトで、この機能は無効になっています。詳細については、「厳格な構成コンプライアンス」を参照してください。

Note ファブリックで厳密な構成コンプライアンスが有効になっている場合、Cisco DCN M のリソースで Network Insights を展開することはできません。

[AAA IP 認証の有効化（Enable AAA IP Authorization）]：AAA サーバで 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。

[グリーンフィールド クリーンアップ オプション（Greenfield Cleanup Option）]：グリーンフィールド スイッチのスイッチ クリーンアップ オプションを有効または無効にします。新しいスイッチが追加されたときに、これは適用可能な post-migration です。

[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、『*Cisco DCNM LAN* ファブリック構成ガイド』の「*Easy* ファブリックの精密時間プロトコル」を参照してください。

[PTP 送信元ループバック ID（PTP Source Loopback Id）]：すべての PTP パケットの送信元 IP アドレスとして使用されるループバック インターフェイス ID ループバックを指定します。有効な値の範囲は 0 ～ 1023 です。PTP ループバック ID を RP、ファントム RP、NVE、または

MPLS ループバック ID と同じにすることはできません。そうでない場合は、エラーが生成されます。PTP ループバック ID は、DCNM から BGP ループバックまたは作成元のユーザー定義ループバックと同じにすることができます。

保存して展開中に PTP ループバック ID が見つからない場合は、次のエラーが生成されます。

PTP 送信元 IP に使用するループバック インターフェイスが見つかりません。PTP機能を有効にするには、すべてのデバイスでPTPループバックインターフェイスを作成してください。

[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。

[MPLS ハンドオフの有効化（Enable MPLS Handoff）]：MPLS ハンドオフ機能を有効にするには、このチェックボックスをオンにします。詳細については、「*VXLAN BGP EVPN* ファブリックでのボーダー プロビジョニングの使用例：*MPLS SR* および *LDP* ハンドオフ」を参照してください。

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）]** 機能を選択する必要があります。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。

[TCAM 割り当ての有効化（Enable TCAM Allocation）]：TCAM コマンドは、有効にすると VXLAN および vPC ファブリック ピアリングに対して自動的に生成されます。

[デフォルト キューイング ポリシーの有効化（Enable Default Queuing Policies）]：このファブリック内のすべてのスイッチに QoS ポリシーを適用するには、このチェックボックスをオンにします。すべてのスイッチに適用した QoS ポリシーを削除するには、このチェックボックスをオフにし、すべての設定を更新してポリシーへの参照を削除し、保存して展開します。Cisco DCNM リリース 11.3(1) 以降、さまざまな Cisco Nexus 9000 シリーズ スイッチに使用できる定義済みの QoS 設定が含まれています。このチェックボックスをオンにすると、適切な QoS 設定がファブリック内のスイッチにプッシュされます。システム キューイングは、設定がスイッチに展開されると更新されます。インターフェイスごと自由形式ブロックに必要な設定を追加することにより、必要に応じて、定義されたキューイング ポリシーを使用してインターフェイス マーキングを実行できます。

テンプレート エディタでポリシー ファイルを開いて、実際のキューイング ポリシーを確認します。Cisco DCNM Web UI から、**[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択します。ポリシー ファイル名でキューイング ポリシーを検索します（例：[queuing_policy_default_8q_cloudscale]）。ファイルを選択し、**[テンプレートの変更/表示（Modify/View template）]** アイコンをクリックしてポリシーを編集します。

プラットフォーム特有の詳細については、『*Cisco Nexus 9000 Series NX-OS Quality of Service* コンフィグレーション ガイド』を参照してください。

[N9K クラウド スケール プラットフォームのキューイング ポリシー（N9K Cloud Scale Platform Queuing Policy）]：ファブリック内の EX、FX、および FX2 で終わるすべての Cisco Nexus 9200 シリーズスイッチおよび Cisco Nexus 9000 シリーズスイッチに適用するキューイング ポリシーをドロップダウン リストから選択します。有効な値は [queuing_policy_default_4q_cloudscale] お

よび [queuing_policy_default_8q_cloudscale] です。FEX には [queuing_policy_default_4q_cloudscale] ポリシーを使用します。FEX がオフラインの場合にのみ、[queuing_policy_default_4q_cloudscale] ポリシーから [queuing_policy_default_8q_cloudscale] ポリシーに変更できます。

[N9K R シリーズ プラットフォーム キューイング ポリシー（N9K R-Series Platform Queuing Policy）]：ドロップダウンリストから、ファブリック内の R で終わるすべての Cisco Nexus スイッチに適用するキューイング ポリシーを選択します。有効な値は [queuing_policy_default_r_series] です。

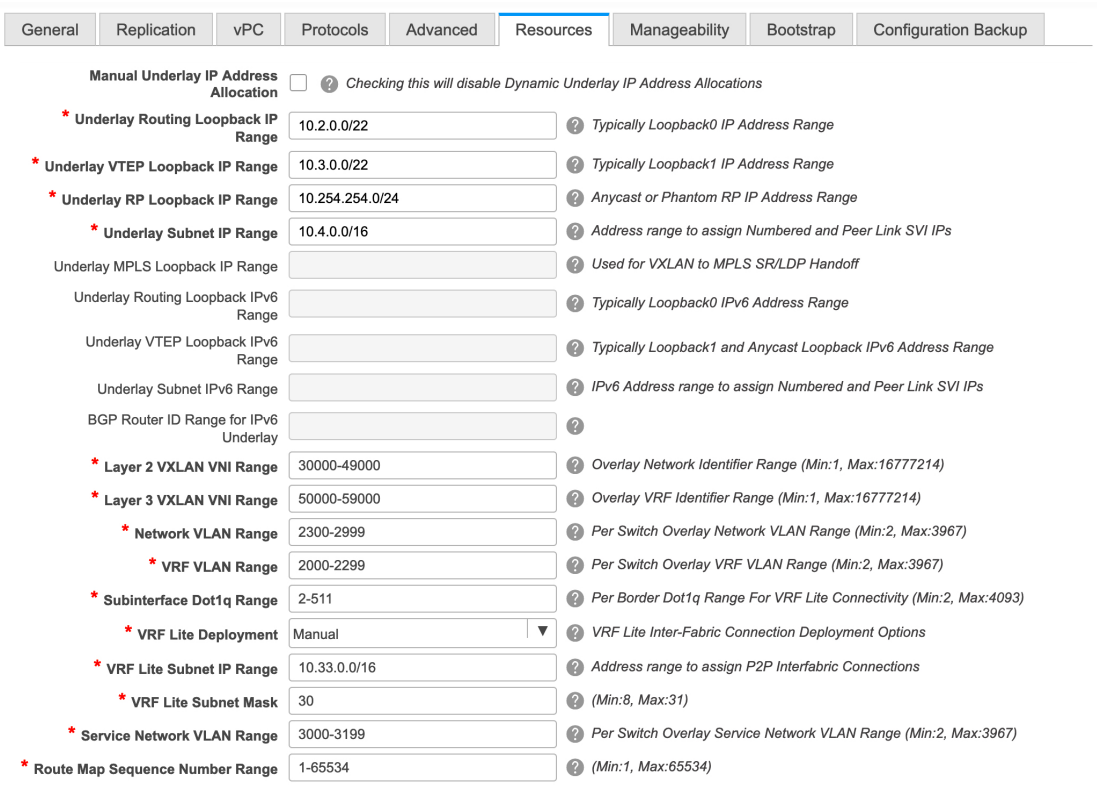
[その他の N9K プラットフォーム キューイング ポリシー（Other N9K Platform Queuing Policy）]：ドロップダウンリストからキューイング ポリシーを選択し、ファブリック内にある、上記2つのオプションで説明したスイッチ以外の他のすべてのスイッチに適用します。有効な値は [queuing_policy_default_other] です。

[MACsec の有効化（Enable MACsec）]：ファブリックの MACsec を有効にします。詳細については、Easy ファブリックおよび eBGP ファブリックでの MACsec サポート, on page 231を参照してください。

[リーフ自由形式構成（Leaf Freeform Config）]および**[スパイン自由形式構成（Spine Freeform Config）]**：ファブリックの移行が完了後必要に応じて、このフィールドに入力ができます。

[Intra-fabric リンクの追加構成（Intra-fabric Links Additional Config）]：ファブリックの移行が完了後必要に応じて、このフィールドに入力ができます。

ステップ 8 [リソース（Resources）] タブをクリックします。



[手動アンダーレイ IP アドレスの割り当て（Manual Underlay IP Address Allocation）]：VXLAN ファブリック管理を移行する場合は、このチェックボックスをオンにしないでください。

範囲を確認し、それらが既存のファブリックと整合していることを確認してください。移行は、ファブリック上にある既存のリソースに優先されます。範囲の設定は移行後の割り当てに適用します。

[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 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。

[レイヤ 2 VXLAN VNI 範囲（Layer 2 VXLAN VNI Range）] および [レイヤ 3 VXLAN VNI 範囲（Layer 3 VXLAN VNI Range）]：ファブリックの VXLAN VNI ID を指定します。

[ネットワーク VLAN 範囲（Network VLAN Range）] および **[VRF VLAN 範囲（VRF VLAN Range）]**：レイヤ 3 VRF およびオーバーレイ ネットワークの VLAN 範囲です。

[サブインターフェイス Dot1q 範囲（Subinterface Dot1q Range）]：L3 サブインターフェイスを使用する場合のサブインターフェイスの範囲を指定します。

[VRF Lite の展開（VRF Lite Deployment）]：ファブリック間接続を拡張するための VRF Lite 方式を指定します。

[VRF Lite サブネット IP 範囲（VRF Lite Subnet IP Range）] フィールドは、VRF LITE IFC が自動作成されるときに VRF LITE に使用される IP アドレス用に予約されたリソースを指定します。Back2BackOnly、ToExternalOnly、または Back2Back & ToExternal を選択すると、VRF LITE IFC が自動作成されます。

[自動展開両方（Auto Deploy Both）]：このチェックボックスは、対称 VRF Lite 展開に適用されます。このチェックボックスをオンにすると、自動作成された IFC の自動展開フラグが true に設定され、対称 VRF Lite 構成がオンになります。

このチェックボックスは、[VRF Lite 展開（VRF Lite Deployment）] フィールドが [手動（Manual）] に設定されていない場合に選択または選択解除できます。この場合、ユーザは自動作成された IFC の [自動展開（auto-deploy）] フィールドを明示的にオフにし、ユーザ入力には常に優先順位が与えられます。このフラグは、新しい自動作成 IFC にのみ影響し、既存の IFC には影響しません。

[VRF Lite サブネット IP 範囲（VRF Lite Subnet IP Range）] および [VRF Lite サブネット マスク（VRF Lite Subnet Mask）]：これらのフィールドには、DCI サブネットの詳細が入力されます。必要に応じて、次のフィールドを更新します。

画面に表示される値は自動的に生成されます。IP アドレス範囲、VXLAN レイヤ 2/レイヤ 3 ネットワーク ID 範囲、または VRF/ネットワーク VLAN 範囲を更新する場合は、次のことを確認します。

Note 値の範囲を更新する場合は、他の範囲と重複しないようにしてください。一度に更新できる値の範囲は1つだけです。複数の値の範囲を更新する場合は、別のインスタンスで実行します。たとえば、L2 と L3 の範囲を更新する場合は、次の手順を実行する必要があります。

a. L2 範囲を更新し、[保存（Save）] をクリックします。

b. [ファブリックの編集（Edit Fabric）] オプションをもう一度クリックし、L3 範囲を更新して [保存（Save）] をクリックします。

[サービス ネットワーク VLAN 範囲（Service Network VLAN Range）] : [サービス ネットワーク VLAN 範囲（Service Network VLAN Range）] フィールドで VLAN 範囲を指定します。これはスイッチごとのオーバーレイ サービス ネットワーク VLAN 範囲です。最小許容値は 2 で、最大許容値は 3967 です。

[ルート マップ シーケンス番号範囲（Route Map Sequence Number Range）] : ルートマップのシーケンス番号の範囲を指定します。最小許容値は 1、最大許容値は 65534 です。

残りのタブはアップデートは必要ありません。ただし、これらの目的は記載されています。

ステップ 9 **管理能力（Manageability）** タブをクリックします。

DNS、NTP、AAA、または syslog サーバーの IP アドレス、VRF、およびスイッチ構成に一致するその他の該当する情報を入力します。これらの機能を持つサーバーが2つ以上ある場合、**[詳細（Advanced）]** タブの **[リーフ自由形式構成（Leaf Freeform Config）]** および **[スパイン自由形式構成（Spine Freeform Config）]** フィールドに追加のサーバーの構成を追加します。

Note ファブリック設定で AAA 構成が指定されていない場合は、**switch_freeform** PTI で、ソースが **UNDERLAY_AAA**、説明が **DCNM Extra AAA Configurations** であるものが作成されます。

ステップ 10 **[ブートストラップ（Bootstrap）]** タブをクリックします。新しいスイッチがファブリックに追加されたとき、移行後のこのタブのフィールドをアップデートします。

ステップ 11 [構成のバックアップ（Configuration Backup）] タブをクリックします。このタブのフィールドを空白のままにします。移行後にアップデートすることができます。

ステップ 12 関連情報を入力して更新したら、**[保存（Save）]** をクリックします。画面の右下に、ファブリックが作成されたことを示すメモが短時間表示されます。ファブリックが作成されると、ファブリックのページが表示されます。画面左上にファブリック名が表示されます。

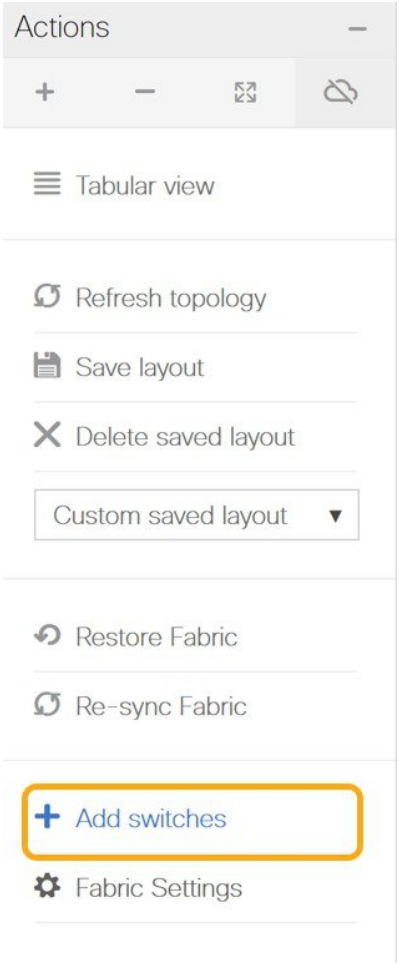
画面左側にある **[操作（Actions）]** パネルでは、さまざまな機能を実行できます。それらの 1 つは、ファブリックにスイッチを追加する **[スイッチの追加（Add switches）]** オプションです。ファブリックを作成したら、ファブリックデバイスを追加する必要があります。このプロセスは、次で説明されます。

スイッチの追加と VXLAN ファブリック管理の DCNM への移行

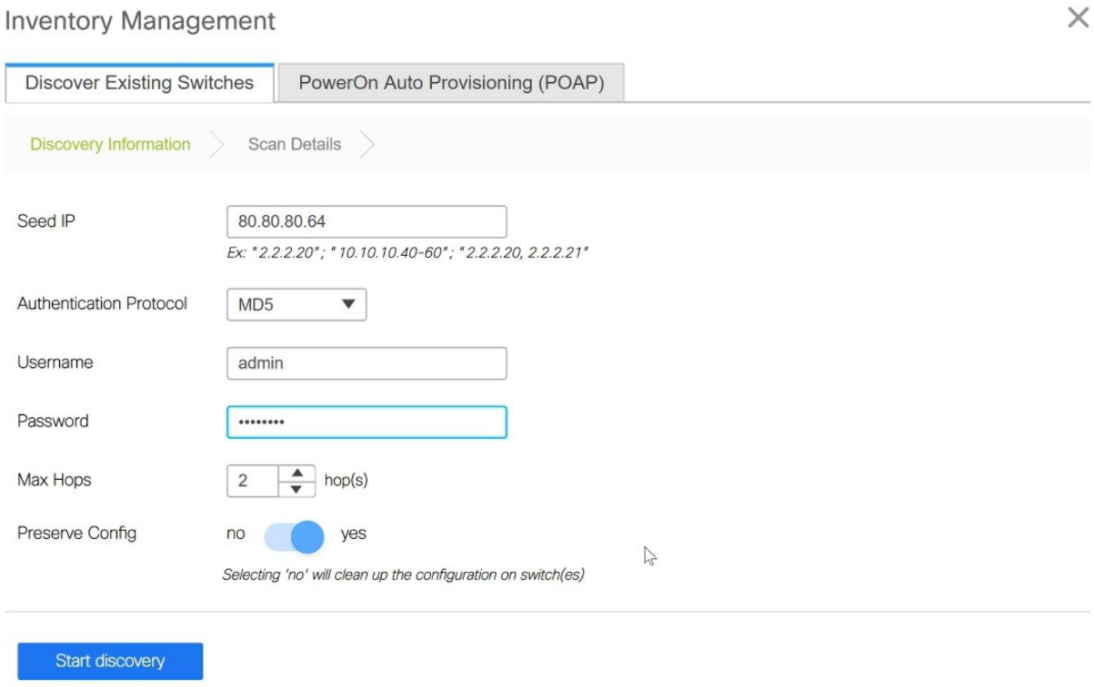
スイッチを検出して、新しく作成したファブリックに追加しましょう。

Procedure

ステップ 1 **[アクション（Actions）]** メニューで **[スイッチの追加（Add Switches）]** をクリックします。



ステップ 2 **[既存のスイッチの検出（Discover Existing Switches）]** タブで、**[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。

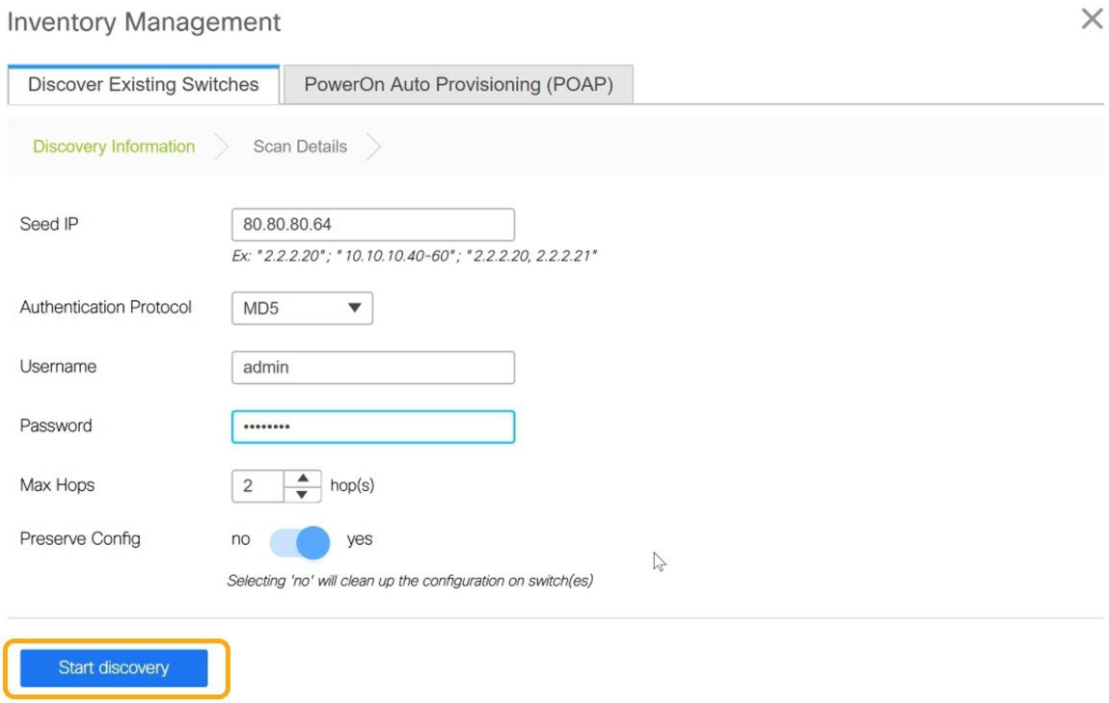
[構成の保持（Preserve Config）] トグル ボタンが **yes** に設定されていることを確認します。

[はい（Yes）] 設定により、スイッチの現在の構成が保持されることを意味します。

重要：[構成の保持（Preserve Config）] フィールドが **yes** に設定されたままになっていることを確認してください。**no** を選択すると、構成が大幅に失われ、ファブリックが中断する可能性があります。

[POAP] タブは、新しいスイッチをファブリックに追加するためにのみ使用されます。このタブは、既存のファブリックを DCNM に移行した後でのみ使用してください。

ステップ 3 [検出の開始（Start discovery）] をクリックします。

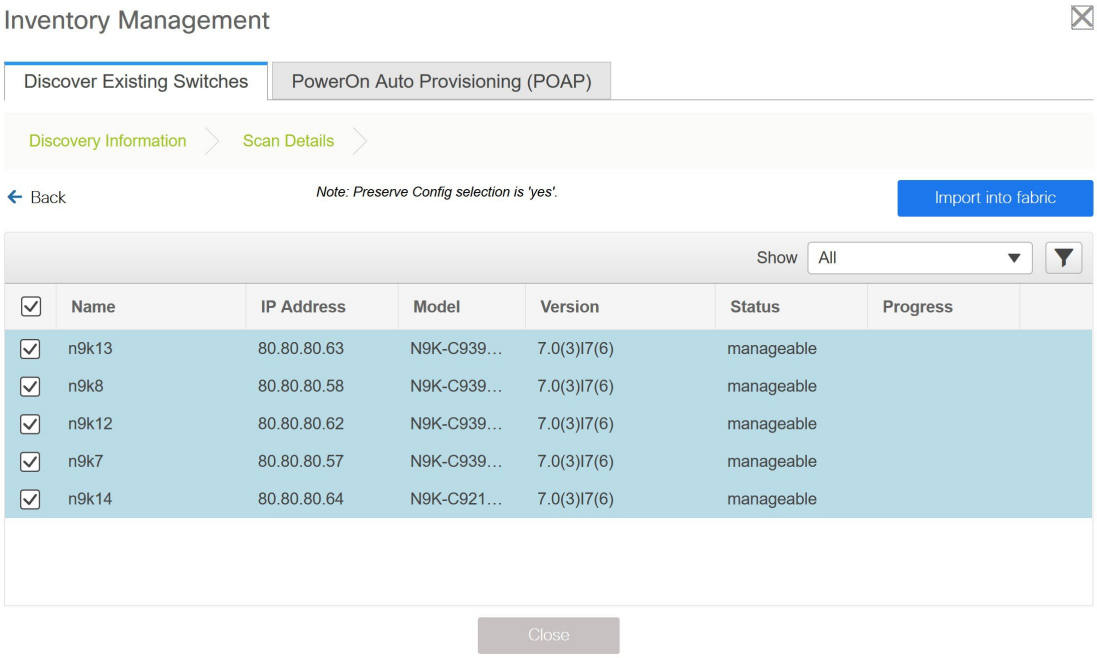


指定された IP アドレスを持つスイッチと、そこから最大 2 ホップ離れたスイッチ（最大ホップ数の設定による）が、[スキャンの詳細（Scan Details）] セクションに表示されます。

ステップ 4 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。スイッチはケーブル接続し DCNM サーバーに接続する必要があり、スイッチのステータスは管理可能である必要があります。

スイッチを複数回インポートする場合は、ファブリックに変更を加える前、つまり **[保存と展開（Save & Deploy）]** をクリックする前に、すべてのスイッチをファブリックに追加する必要があります。



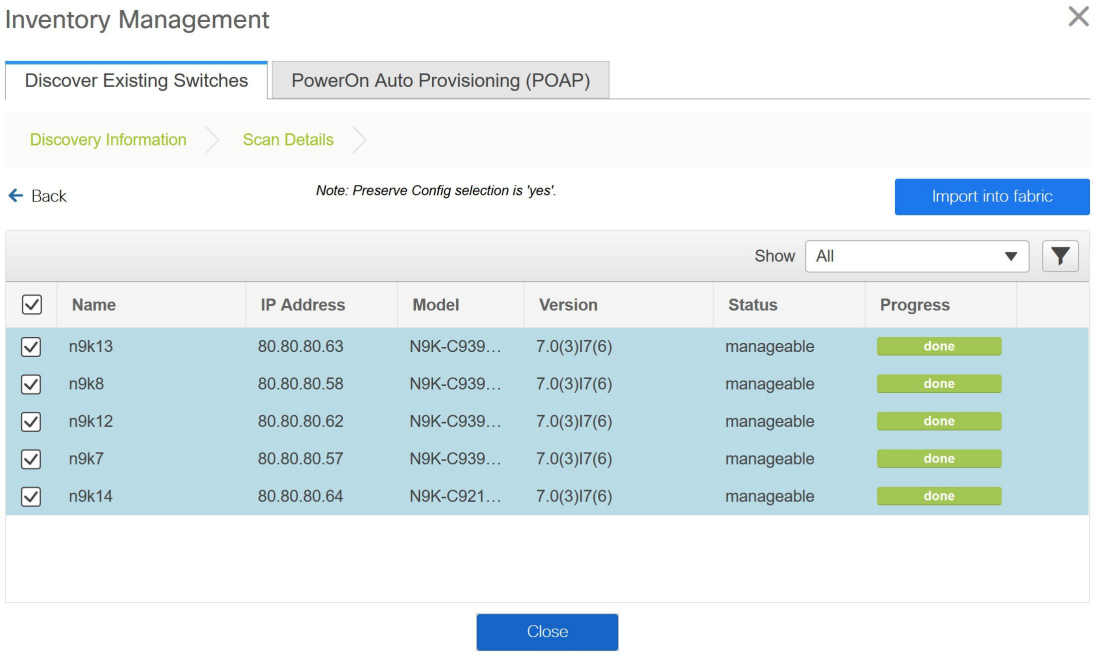
ステップ 5 [ファブリックにインポート（Import into fabric）] をクリックします。

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、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。

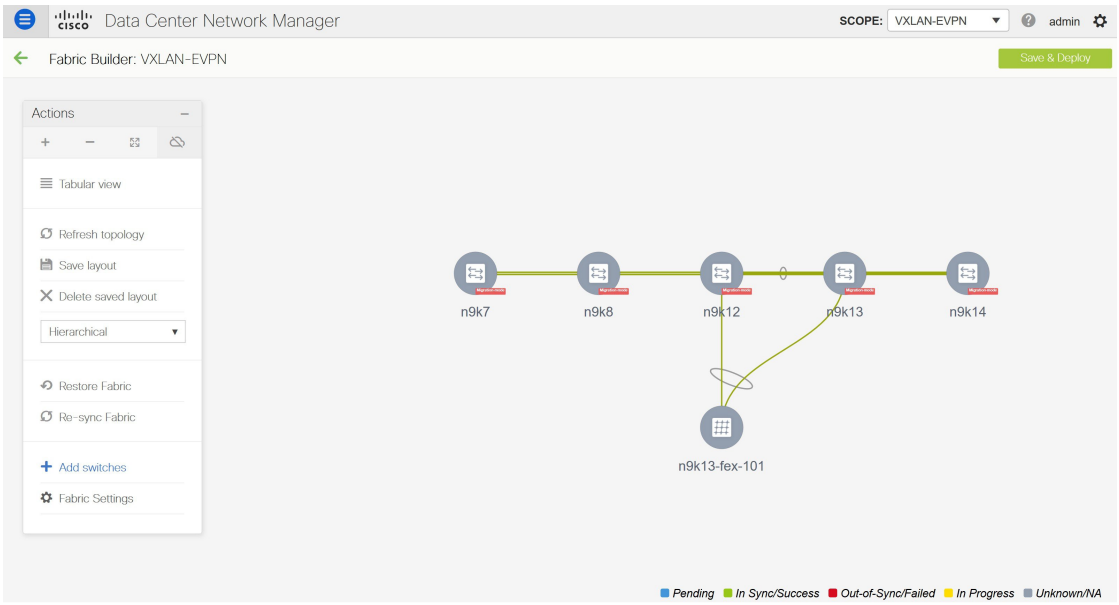
ステップ 6 インポートが成功すると、進行状況バーにすべてのスイッチの **[完了（Done）]** が表示されます。[閉じる（Close）] をクリックします。



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 c 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 7 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**[ファブリック ビルダ（Fabric Builder）]** 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。



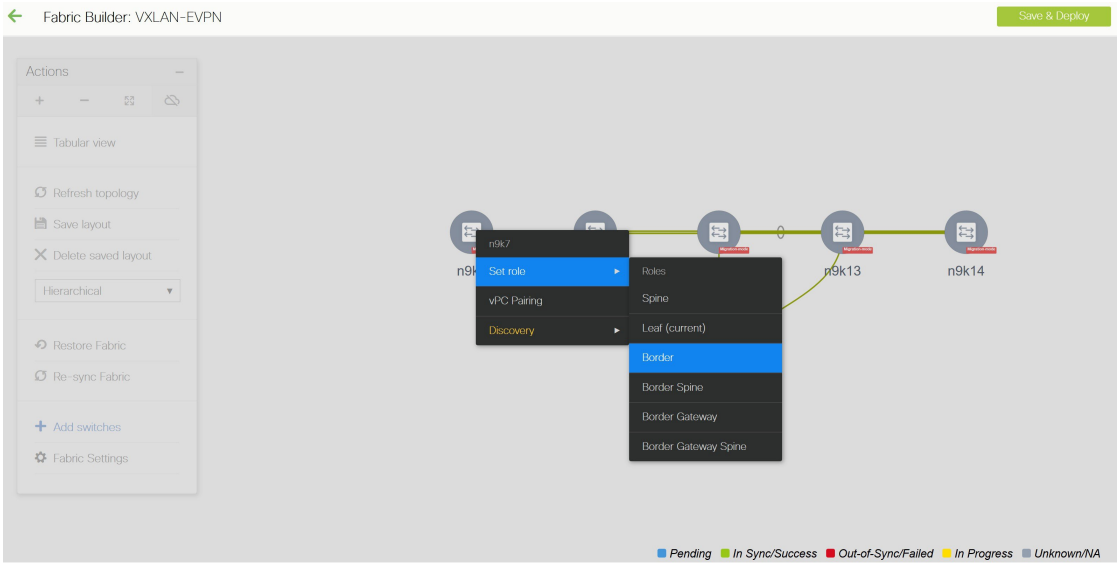
いくつかのスイッチでスイッチ ディスカバリ プロセスが失敗し、ディスカバリ エラー メッセージが表示されることがあります。それでも、そのようなスイッチは引き続きファブリック トポロジに表示されます。このようなスイッチをファブリックから削除し（スイッチアイコンを右クリックし、**[検出（Discovery）] > [ファブリックから削除（Remove from fabric）]** をクリックします）、再度インポートする必要があります。

既存のファブリック内のすべてのスイッチが DCNM 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。

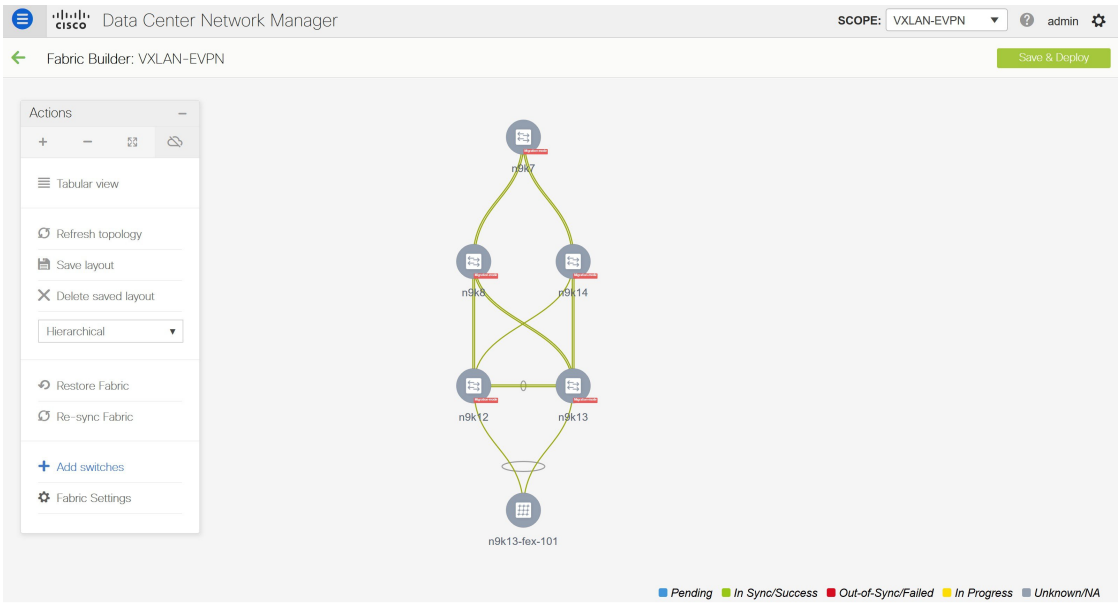
Note Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x) イメージのスイッチでサポートされるロールは、ボーダー リーフ、ボーダー スパイン、リーフ、およびスパインです。

ステップ 8 **[n9k-7]** スイッチを右クリックし、**[ロールの設定（Set Role）]** を選択して、**[ロール（Roles）]** ドロップダウンリストから **[ボーダー（Border）]** を選択します。



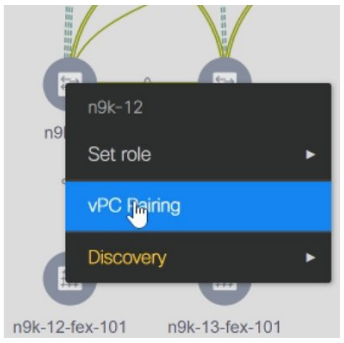
同様に、**スパイン** ロールを **n9k-14** および **n9k-8** スパイン スイッチで設定します。

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。詳細については、vPC L3 ピア キープアライブ リンクの追加, on page 127を参照してください。



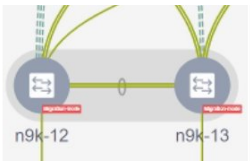
vPC ペアリング：vPC ペアリングは、レイヤ 3 vPC ピア キープ アライブが使用されているスイッチに対して行う必要があります。vPC ピア キープ アライブが管理オプションによって確立されると、vPC 構成はスイッチから自動的に取得されます。このペアリングは、移行が完了した後にのみ GUI に反映されます。

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。これで 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 9 [保存して展開（Save & Deploy）] をクリックします。

[保存と展開（Save & Deploy）] をクリックすると、DCNM はスイッチ構成を取得し、現在実行中の構成から現在予想される構成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、DCNM で維持されます。

[ファブリック構成を保存する（Saving Fabric Configuration）] メッセージがすぐに表示されます。これは、オーバーレイおよびアンダーレイ ネットワークの移行、およびDCNMへのスイッチおよびポートチャネル設定の移行が開始されたことを示しています。

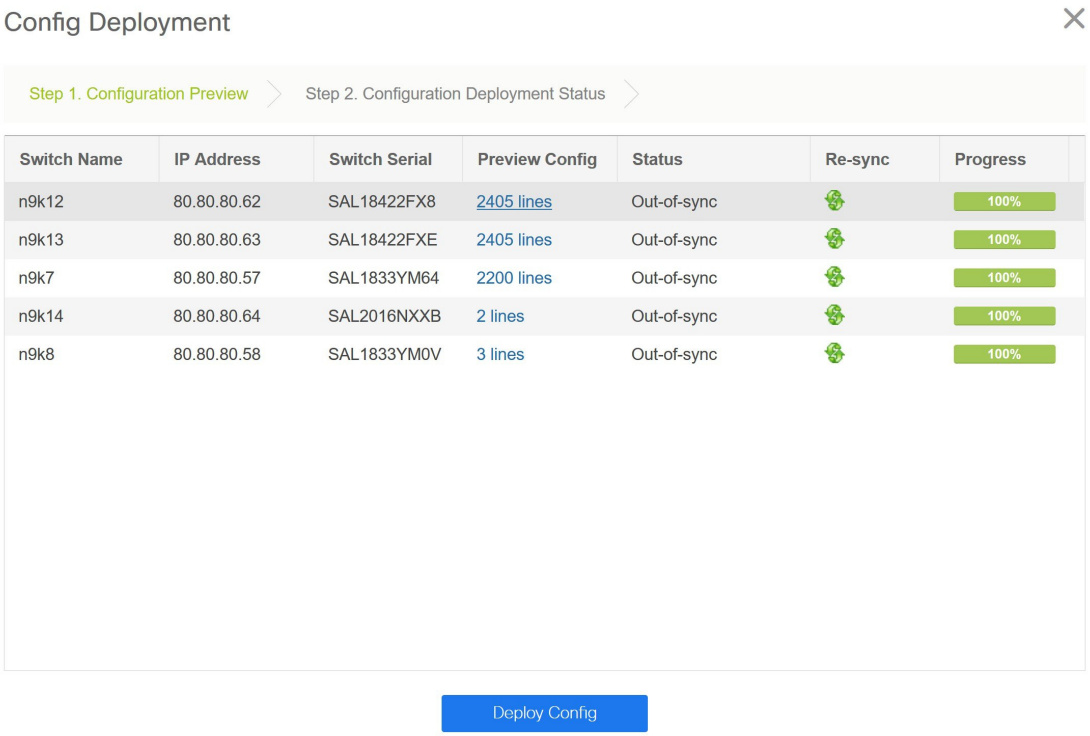
構成の不一致がある場合は、エラー メッセージが表示されます。必要に応じてファブリック設定またはスイッチ構成の変更を更新し、[保存して展開（Save and Deploy）] を再度クリックします。

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（Configuration Deployment）] 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。詳細については、「制御」の章を参照してください。
- 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、エラーがレポートされなくなるまで **[保存と展開（Save & 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 10 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 Config）] 列のエントリをクリックします。[構成のプレビュー (Config Preview)] 画面が表示されます。スイッチの保留中の設定が一覧表示されます。

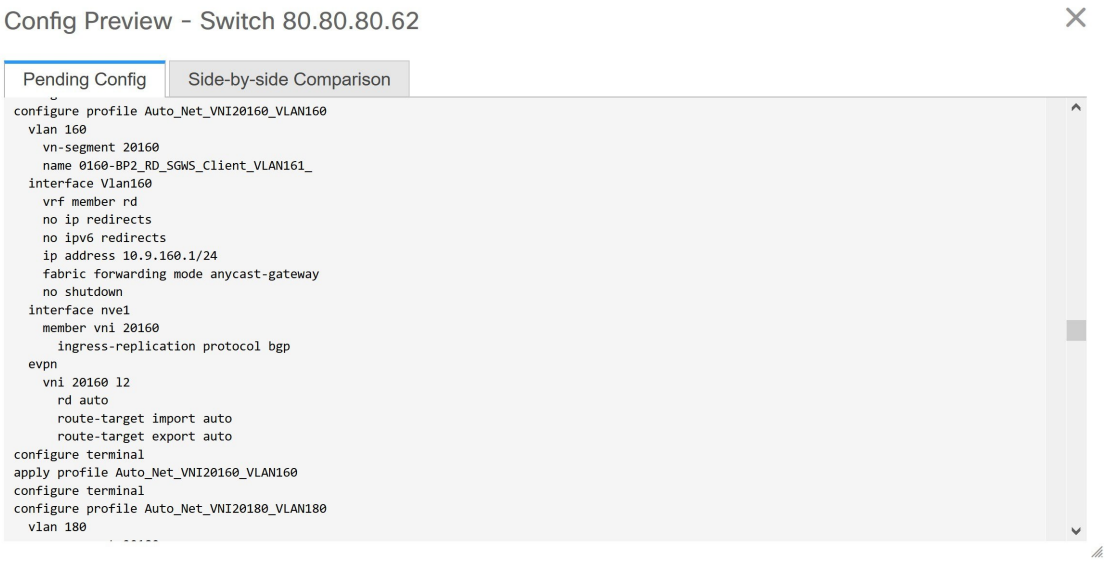
[並べて表示（Side-by-Side）] タブには、実行構成と予想される構成が並べて表示されます。

[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。

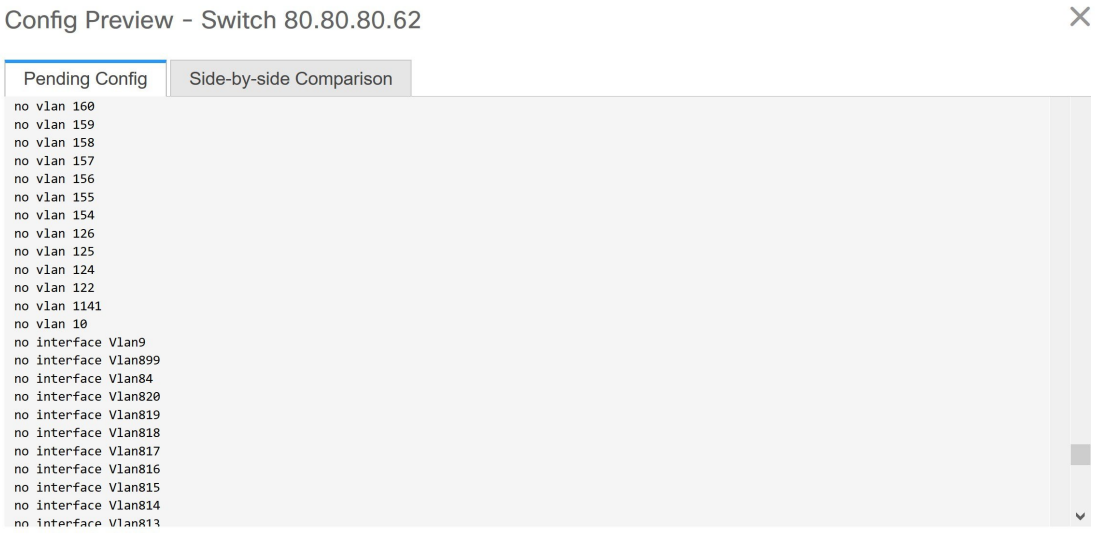
[保留中の構成（Pending Config）] タブには、スイッチに展開される多くの構成行が表示される場合があります。通常、ブラウンフィールドインポートが成功すると、これらの行が、オーバーレイ ネットワーク構成のためにスイッチにプッシュされた構成プロファイルに対応するこ

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。

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 DCNM 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。



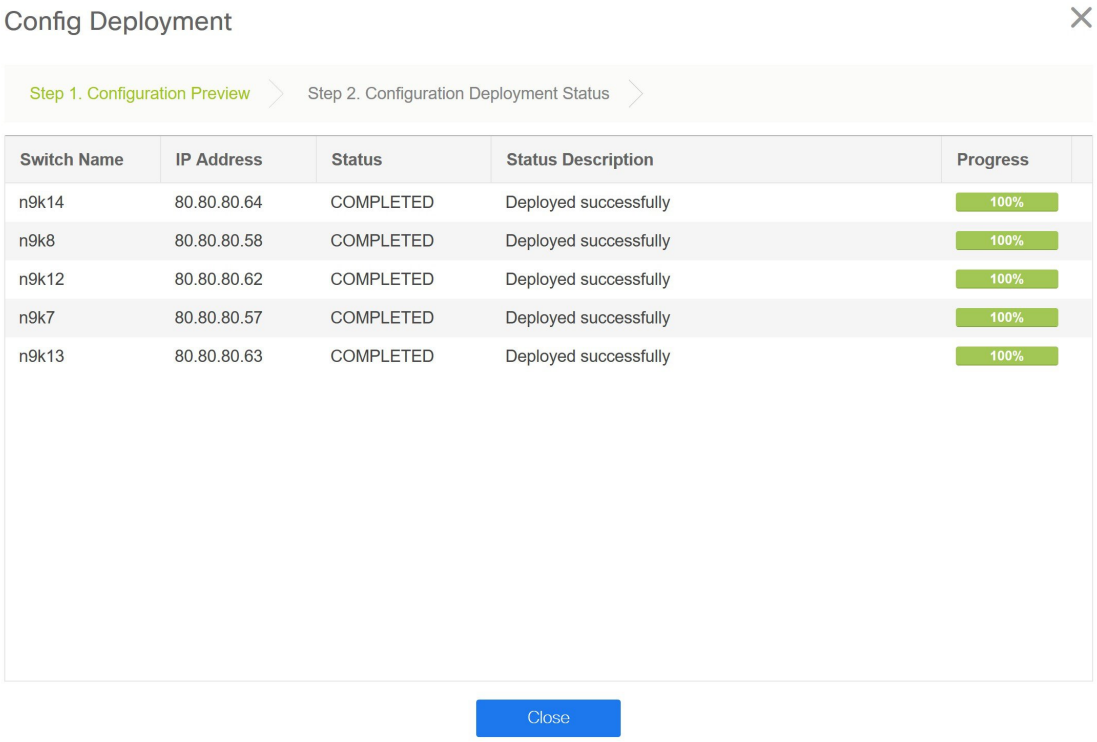
インポート プロセスの一環として、構成プロファイルが適用された後、元の CLI ベースの基準構成はスイッチから削除されます。これらは、差分の最後に表示される「no」CLI です。スイッチの VXLAN 構成は、構成プロファイルに保持されます。次の画像では、構成が削除されることがわかります。具体的には、**no vlan 160** が削除されます。



[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 11 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 12 **[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。

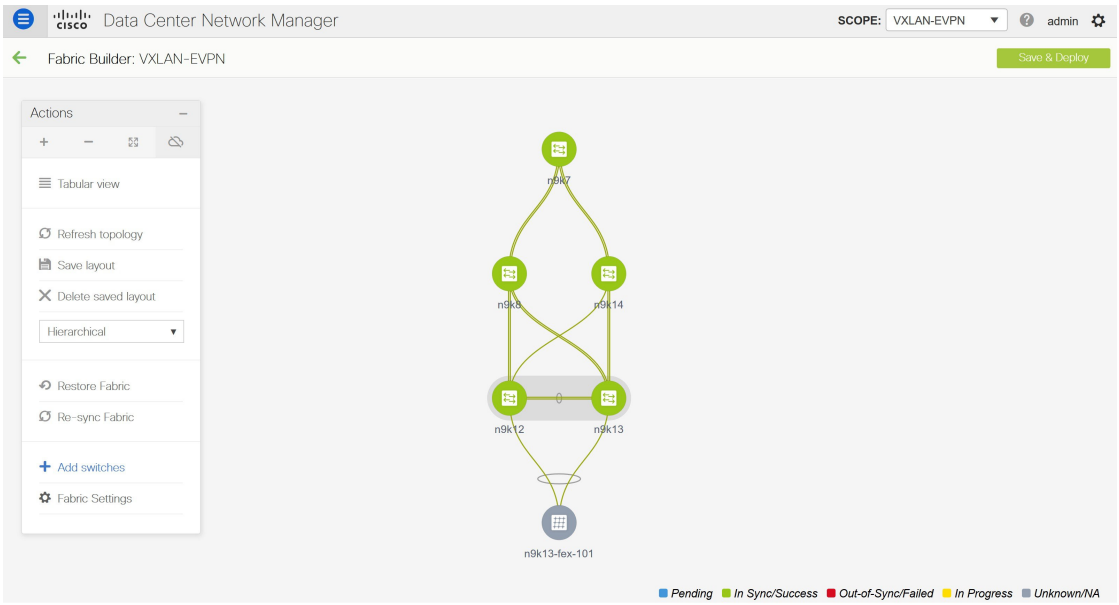


[ステータス（Status）] 列に **[失敗（FAILED）]** と表示された場合は、失敗の理由を調査して問題に対応してください。

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。

DCNM 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 DCNM への移行後：VXLAN ファブリック管理から DCNM 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。

ファブリックのオプション

- **[表形式の表示（Tabular View）]**：デフォルトでスイッチはトポロジ表示として映されます。このオプションを使用して、表形式のビューでスイッチを表示します。
- **[トポロジの更新（Refresh topology）]**：トポロジを更新できます。
- **[レイアウトの保存（Save Layout）]**：トポロジのカスタム表示を保存します。トポロジに特定のビューを作成し、使いやすいように保存できます。
- **[保存されたレイアウトの削除（Delete saved layout）]**：トポロジのカスタム表示を削除します。
- **[トポロジ表示（Topology views）]**：保存されたレイアウトの表示オプションは、階層型、ランダム、およびカスタムから選択できます。
  - **[階層型（Hierarchical）]**：トポロジのアーキテクチャ表示を表示。CLOS トポロジの構成方法に関するノードを示すさまざまなスイッチ ロールを定義できます。
  - **[ランダム（Random）]**：ノードは画面上にランダムに配置されます。 DCNM は、推測を行い、近接するノードをインテリジェントに配置しようとします。
  - **[カスタム保存レイアウト（Custom saved layout）]**：ノードを好きなようにドラッグできます。好きな位置に配置したら、レイアウトの保存をクリックして位置を記憶することができます。次回トポロジにアクセスすると、DCNMにより最後に保存したレイアウト位置に基づいてノードが描画されます。

- **[ファブリックの復元（Restore Fabric）]**：ファブリックを以前の DCNM 構成状態に復元できます（1か月前、2か月前など）。詳細については、「ファブリックの復元」セクションを参照します。
- **[今すぐバックアップ（Backup Now）]**：**[今すぐバックアップ（Backup Now）]** をクリックして、ファブリック バックアップを手動で開始できます。タグの名前を入力して、**[OK]** をクリックします。**[ファブリック設定（Fabric Settings）]** ダイアログ ボックスの **[構成バックアップ（Configuration Backup）]** タブで選択した設定に関係なく、このオプションを使用してバックアップを開始できます。
- **[ファブリックの再同期Resync Fabric（Resync Fabric）]**：大規模なアウトオブバンド変更がある場合、または構成変更が DCNM に正しく登録されていない場合に、このオプションを使用して DCNM 状態を再同期します。再同期操作は、ファブリックスイッチに対して完全な CC 実行を実行し、「show run」および「show run all」コマンドをスイッチから再収集します。再同期プロセスを開始すると、進行状況メッセージが画面に表示されます。再同期中に、実行構成がスイッチから取得されます。スイッチの Out-of-Sync/In-Sync ステータスは、DCNM で定義されたインテントに基づいて再計算されます。
- **[スイッチを追加（Add Switches）]**：ファブリックにスイッチ インスタンスを追加しすることを許可します。
- **[ファブリック設定（Fabric Settings）]**：ファブリック設定を表示または編集できます。

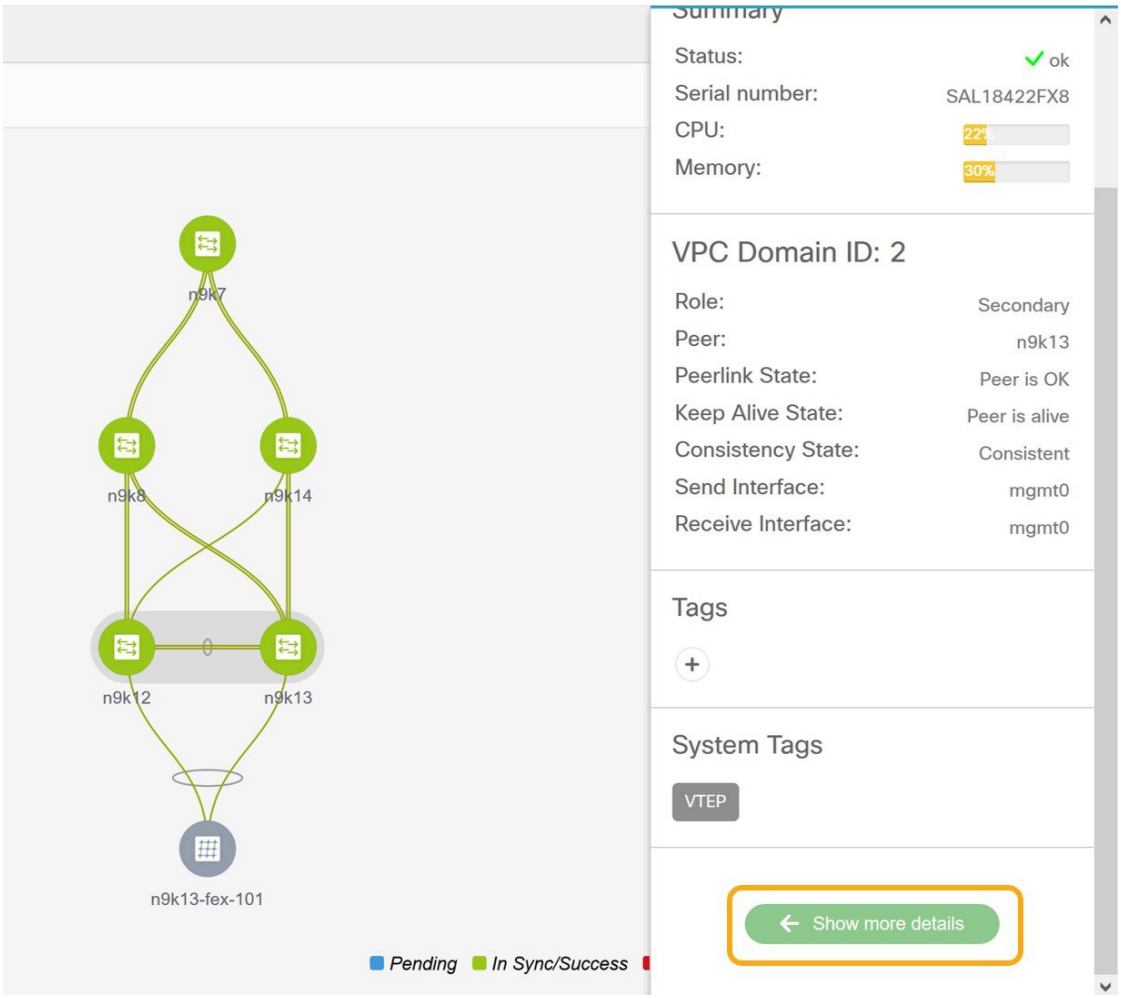
VXLAN BGP EVPN ファブリックのインポートの確認

ブラウンフィールドの移行が成功したかどうかを確認しましょう。

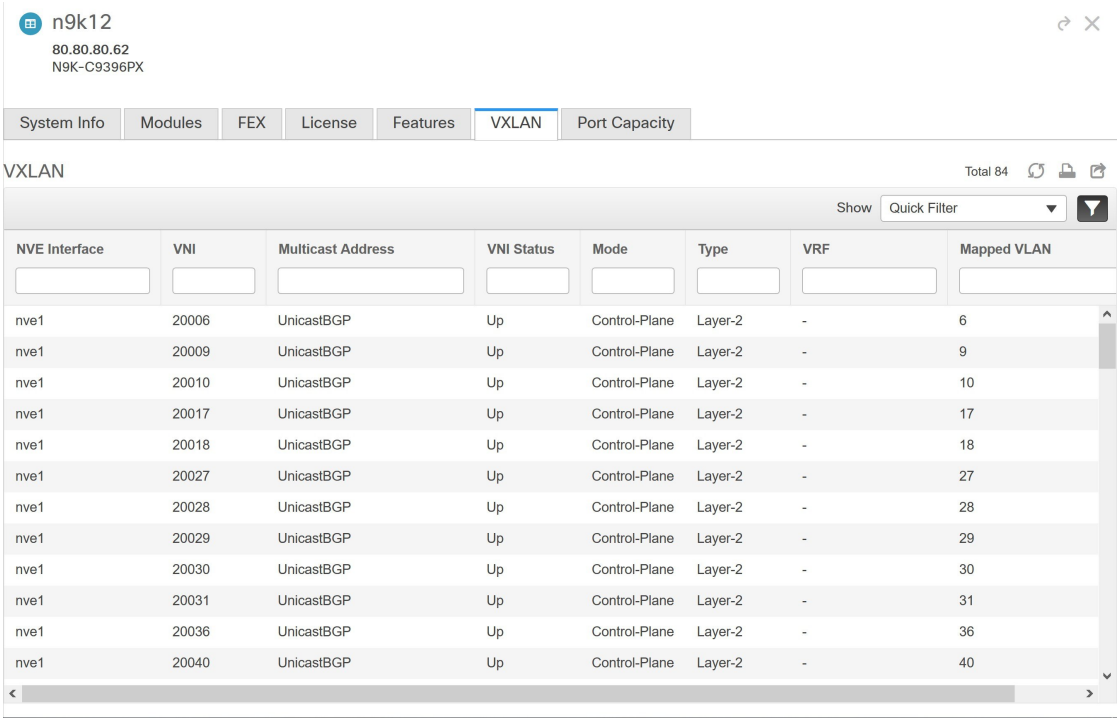
スイッチ上の VXLAN およびコマンドの確認

Procedure

ステップ 1 このファブリックのVXLANを確認するには、スイッチをダブルクリックし、スイッチペインで **[詳細を表示（Show more details）]** をクリックします。



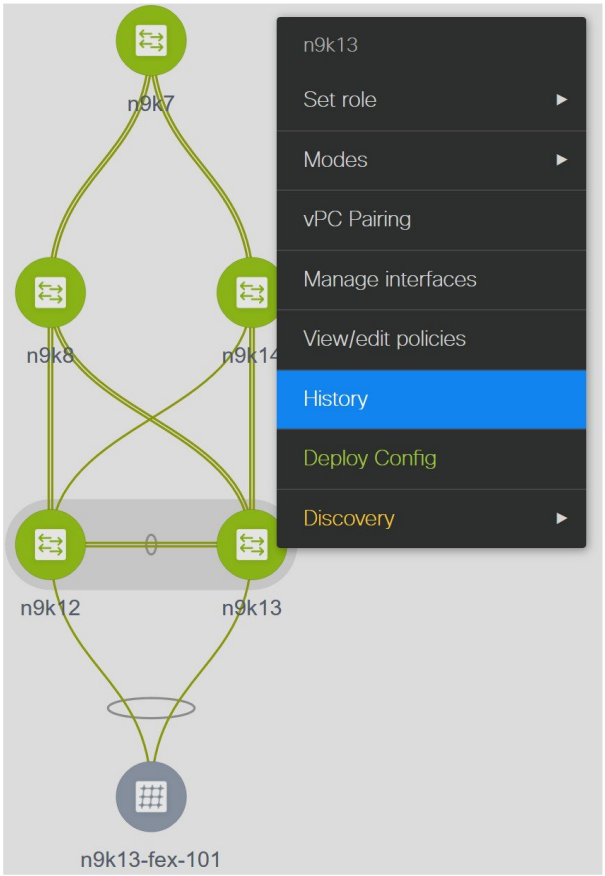
ステップ 2 **[VXLAN（VXLAN）]** タブをクリックします。



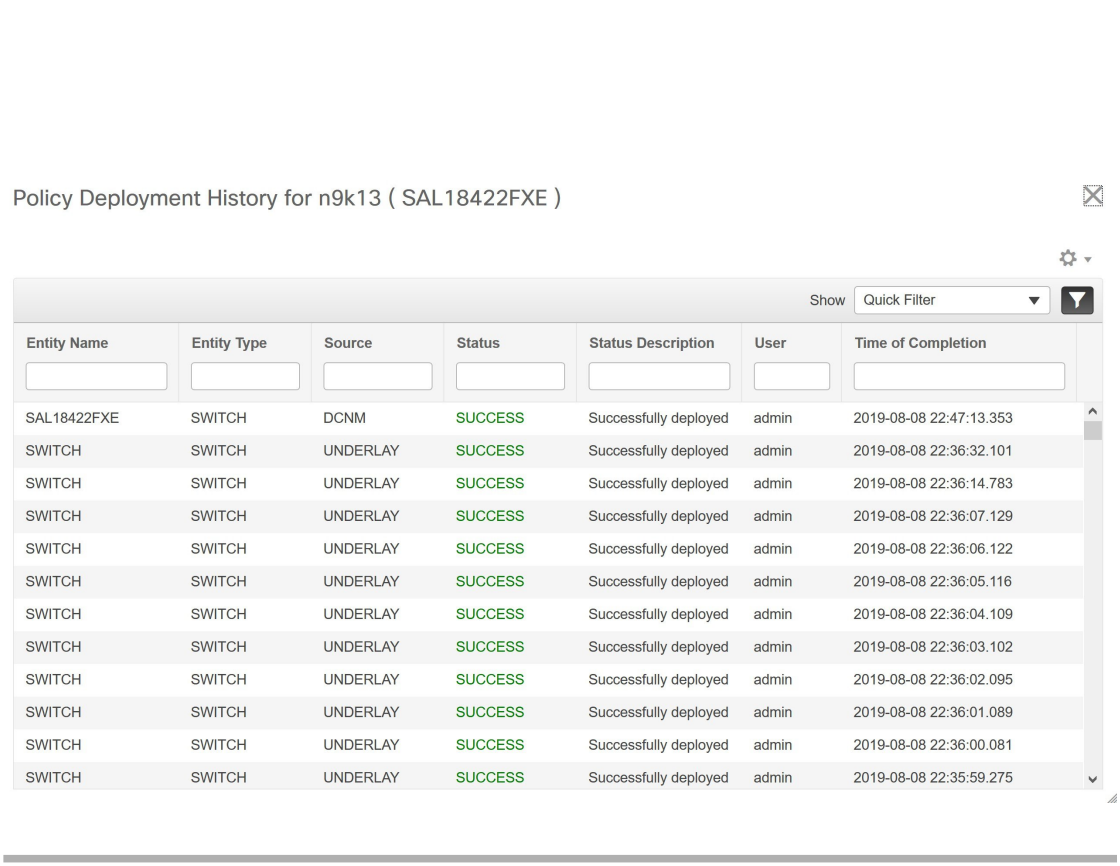
すべての VXLAN が正常に移行されたことがわかります。

Note このウィンドウのさまざまなタブをクリックして、残りの情報を確認できます。

ステップ 3 スイッチを右クリックし、**[履歴（History）]** を選択して、DCNM によってプッシュされたコマンドを確認します。

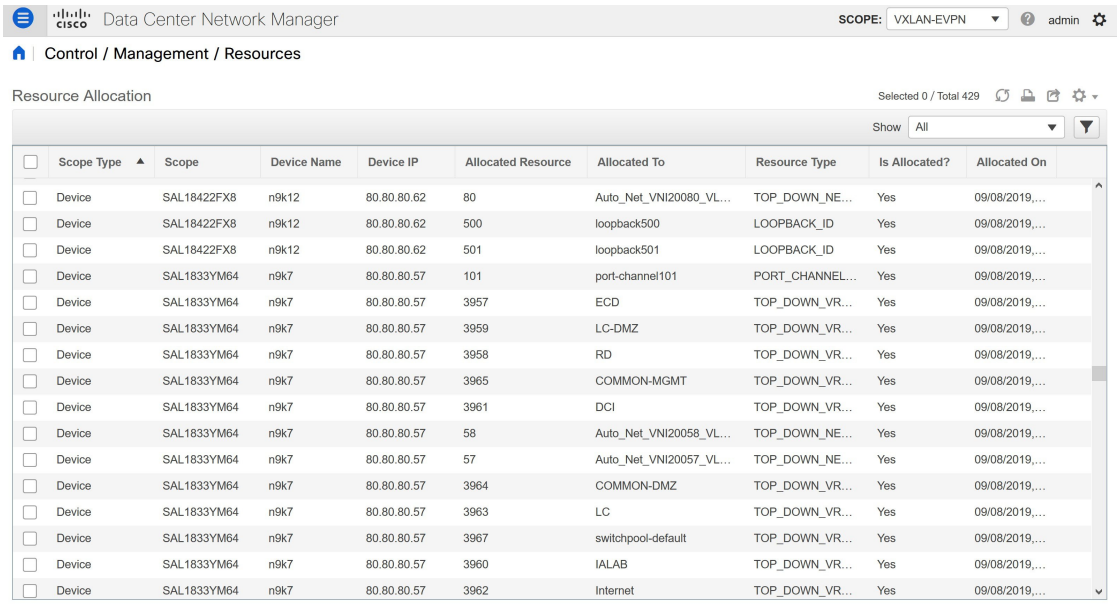


ステップ 4 **[ステータス（Status）]**列の下の**[成功（Success）]**ハイパーリンクをクリックして、DCNM によってプッシュされたコマンドを表示します。



リソースの確認

DCNMにはファブリックで使用されているすべてのリソースを追跡する、リソースマネージャがあります。左側のメニューで **[制御（Control）] > [管理（Management）] > [リソース（Resources）]** に移動します。



VLAN ID、ポートチャネル ID、ポイント ツー ポイント IP アドレス、ループバック ID など、VXLAN EVPN ファブリックで使用されているリソースがこのウィンドウに表示されます。

ネットワークの確認

Procedure

ステップ 1 メニューから、**[制御（Control）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** を選択します。

ステップ 2 **[範囲（Scope）]** ドロップダウンリストから **[VXLAN-EVPN]** を選択します。

このウィンドウに表示されるすべてのネットワークは、ブラウンフィールド移行の一環として DCNM によって学習され、入力されたものです。

ステップ 3 **[表示（Show）]** ドロップダウンリストから **[クイック フィルタ（Quick Filter）]** を選択し、VLAN ID フィールドに **[349]** を入力します。

このネットワークは VLAN ID 349 に関連付けられており、エニーキャスト IP 204.90.140.134 で構成されています。

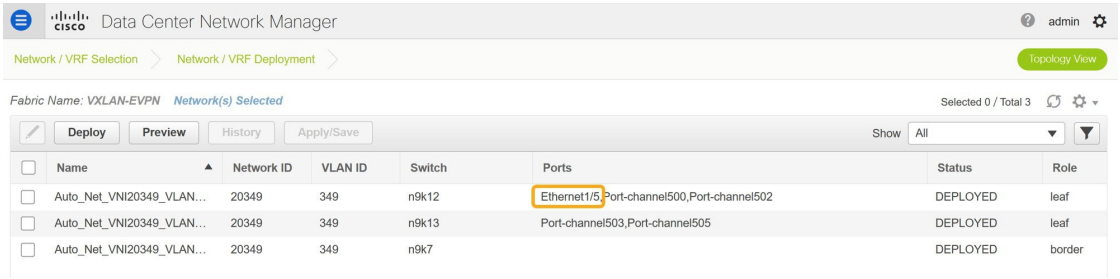
このネットワークが展開されていることがわかります。

このネットワークを選択し、**[続行（Continue）]** をクリックします。

ステップ 4 **[詳細表示（Detailed View）]** をクリックします。

このネットワークは、リーフスイッチとボーダー スイッチに展開されています。

イーサネット 1/5 は、リーフスイッチのポートの 1 つであることに注意してください。

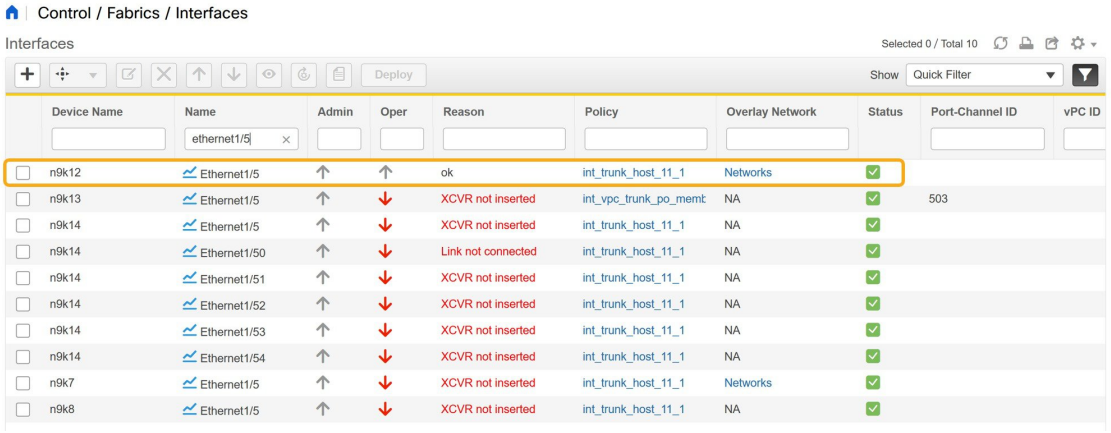


このインターフェイスに関連付けられたオーバーレイ ネットワークを確認しましょう。

ステップ 5 メニューで、**[制御（Control）]>[ファブリック（Fabrics）]>[インターフェイス（Interfaces）]** をクリックします。

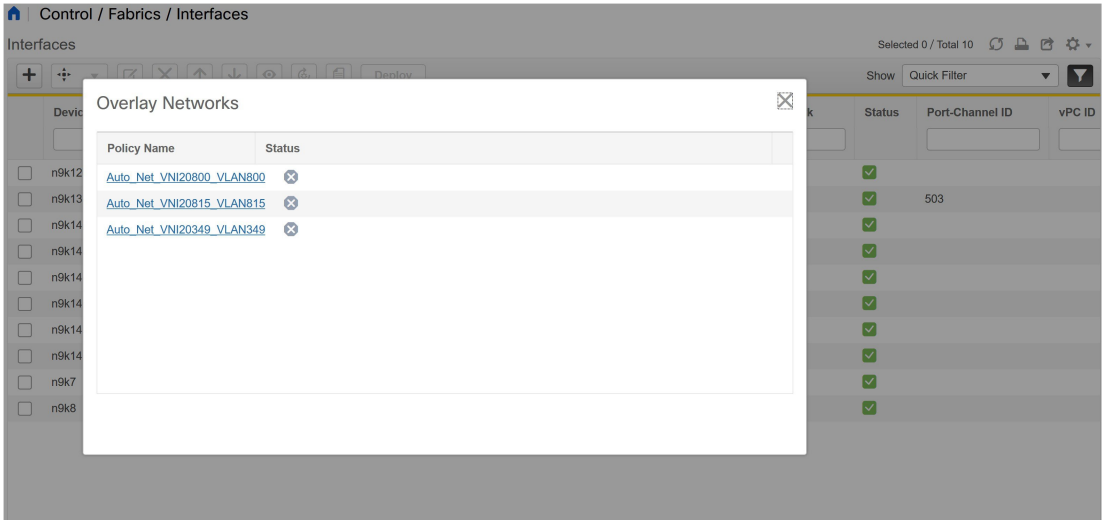
ポートチャネル、vPC、およびmgmt0インターフェイスを含む、インポートされたすべてのインターフェイスが **[インターフェイス（Interfaces）]** ウィンドウに表示されます。

ステップ 6 [名前（Name）] フィールドに、**[Ethernet1/5]** と入力します。



このインターフェイスは、**n9k-12 switch** を介してホストに接続されます。

ステップ 7 **[オーバーレイ ネットワーク（Overlay Networks）]** 列で、n9k-12 スイッチとイーサネット 1/5 インターフェイスに対応する **[ネットワーク（Networks）]** をクリックします。

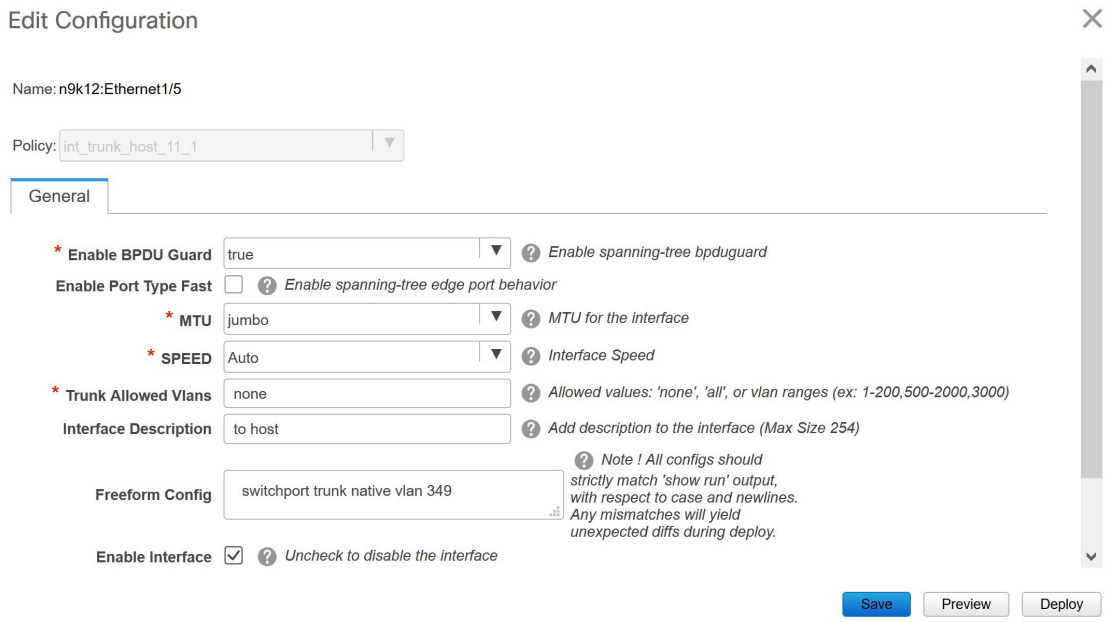


これらは、イーサネット 1/5 インターフェイスに接続されているネットワークです。

VLAN 349 もその 1 つです。

このネットワークをクリックして、望む構成を表示できます。

ステップ 8 **[Ethernet1/5]** インターフェイスに対応する **[n9k-12]** スイッチを選択し、**[編集（Edit）]** アイコンをクリックします。



BPDUガード設定やインターフェイスの説明など、このインターフェイスのすべての設定が正常にインポートされていることがわかります。

ホストに戻りましょう。

ping コマンドはまだ実行中です。

ステップ 9 **ping** コマンドを終了します。

```
64 bytes from 204.90.140.134: icmp_seq=4100 ttl=254 time=1.188 ms
64 bytes from 204.90.140.134: icmp_seq=4101 ttl=254 time=1.122 ms
64 bytes from 204.90.140.134: icmp_seq=4102 ttl=254 time=1.224 ms
64 bytes from 204.90.140.134: icmp_seq=4103 ttl=254 time=1.09 ms
64 bytes from 204.90.140.134: icmp_seq=4104 ttl=254 time=1.054 ms
64 bytes from 204.90.140.134: icmp_seq=4105 ttl=254 time=1.079 ms
64 bytes from 204.90.140.134: icmp_seq=4106 ttl=254 time=1.172 ms
64 bytes from 204.90.140.134: icmp_seq=4107 ttl=254 time=1.226 ms
--- 204.90.140.134 ping statistics ---
4108 packets transmitted, 4108 packets received, 0.00% packet loss
round-trip min/avg/max = 1.003/1.264/3.412 ms
```

移行中に 4108 個のパケットが送受信され、パケット損失は 0 % であることがわかります。

ブラウンフィールド ファブリックが DCNM に正常に移行されました。

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 DCNM リリース 11.3(1) は、構成プロファイルでプロビジョニングされる XLAN 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。

構成プロファイルのサポートが有用となるのは次のケースです。

- アップグレードが不可能な場合に、ファブリックを古いバージョンの DCNM から新しいバージョンの DCNM に移動します。通常、最新の DCNM 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。
- 単一の大規模なファブリック展開を小規模な展開に分割します。新しいファブリックを作成し、大規模なファブリック展開からスイッチを削除して、新しいファブリックにインポートします。

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_11_1** 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。**ユニバーサル** 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、**[保存と展開（Save & Deploy）]** をクリックした後、**並行比較** 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。

ボトムアップ VXLAN ファブリックを DCNM に移行する

この手順は、ボトムアップ VXLAN ファブリックを DCNM に移行する方法を示しています。

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。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 DCNM を使用して管理することができます。

ボトムアップ VXLAN 移行のガイドラインと制限、および前提条件は、ブラウンフィールド移行と同じです。詳細については、「ブラウンフィールド展開：VXLAN ファブリック管理から DCNMへの移行」を参照してください。

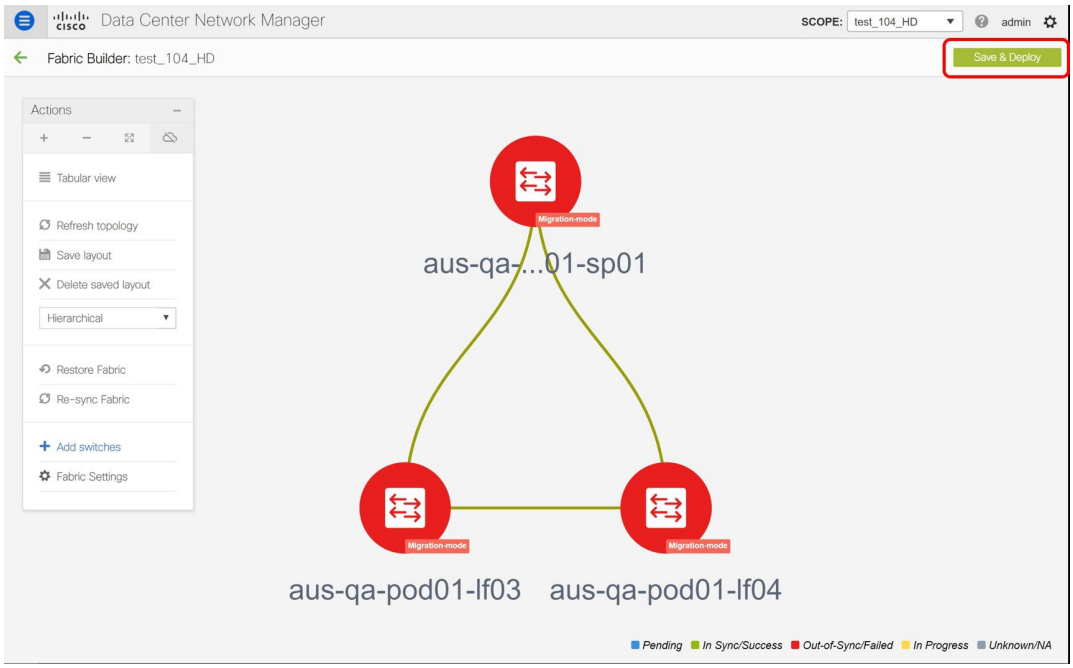
1. VXLAN BGP EVPN ファブリックを作成します。

   詳細については、「ブラウンフィールド展開： DCNM への VXLAN ファブリック管理の移行」の「新しい *VXLAN BGP EVPN* ファブリックの作成」セクションを参照してください。

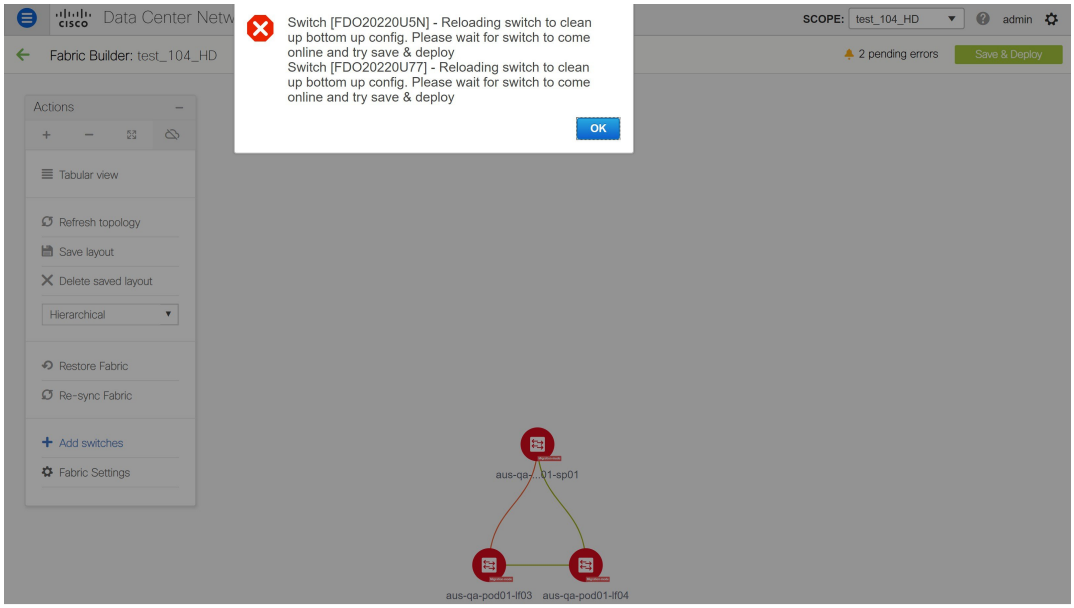
2. ファブリックにスイッチ インスタンスを追加します。

   詳細については、「ブラウンフィールド展開：VXLAN ファブリック管理から DCNM への移行」の「スイッチ インスタンスの追加と *VXLAN* ファブリック管理の移行」セクションのステップ 1 からステップ 5 に従ってください。

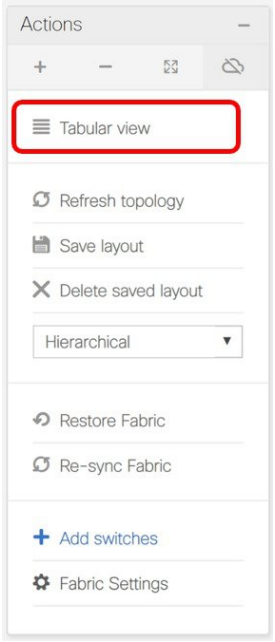
3. **[保存と展開（Save & Deploy）]** をクリックして、スイッチと DCNM の間で構成を同期します。



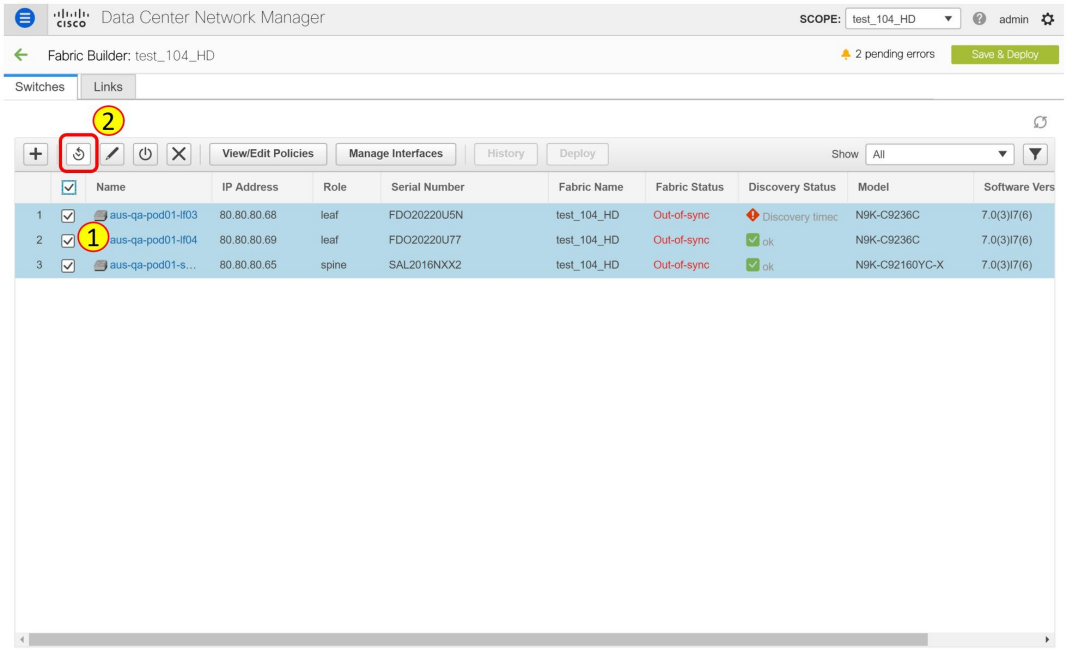
追加されたスイッチにボトムアップ構成が含まれている場合、次のエラーが表示されます。「ボトムアップ構成をクリーンアップするためにスイッチを再ロードしています。」スイッチがオンラインになるまで待ってから、**[保存と展開（Save & Deploy）]** を試行してください。



4. スイッチがリロード操作を完了するまで待ちます。**[アクション（Actions）]** メニューの **[表形式ビュー（Tabular view）]** をクリックして、スイッチのステータスを表示します。



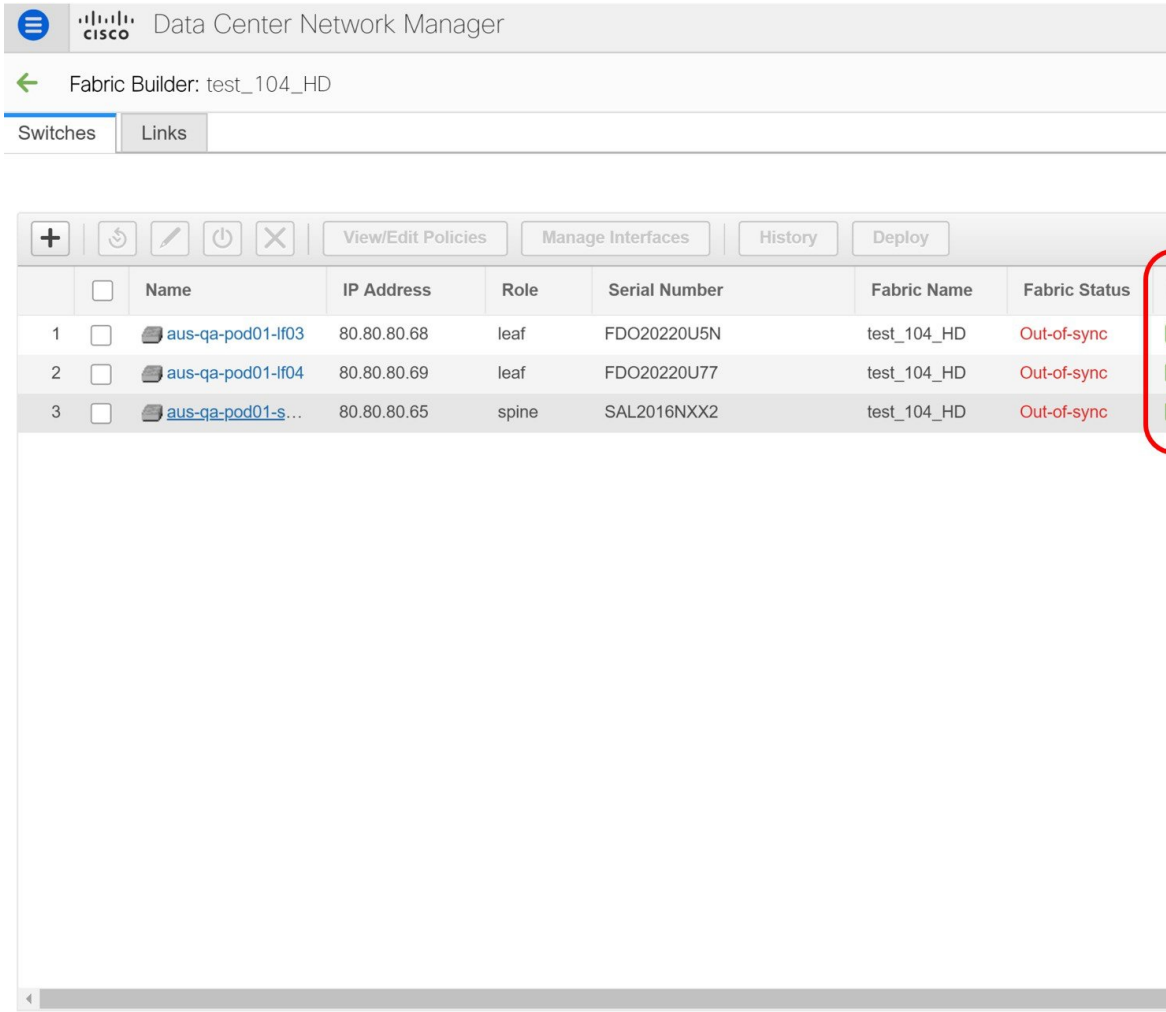
5. （オプション）リロードされたスイッチの再検出は 5 分ごとに発生します。スイッチを手動で再検出する場合は、スイッチを選択して **[スイッチの再検出（Rediscover switch）]** アイコンをクリックします。



Note **[更新（Refresh）]** アイコンをクリックして **ファブリック ビルダ（Fabric Builder）** ウィンドウを更新し、更新されたスイッチの検出ステータスを確認します。

6. リロードおよび再検出操作が完了したら、スイッチの**[検出ステータス（Discovery Status）]**を確認します。すべてのスイッチのステータスが**正常**であることを確認します。

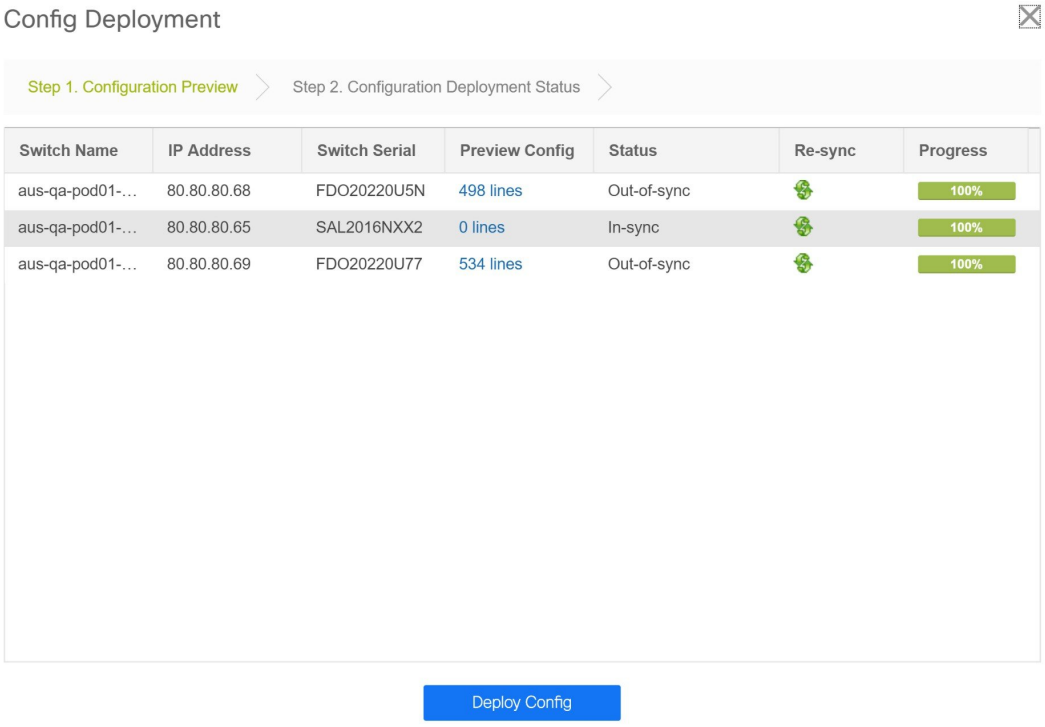
Note スイッチが [到達不能（Unreachable）] 検出ステータスの場合、スイッチの最後の使用可能な情報が他の列に保持されます。



7. **[保存と展開（Save & Deploy）]** を再度クリックして、スイッチと DCNM の間で構成を同期します。

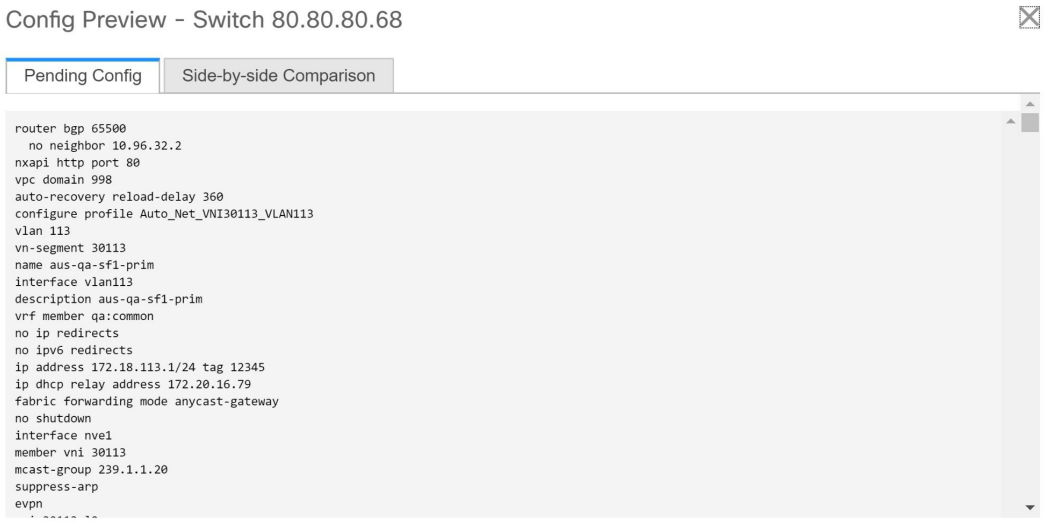
[ファブリック構成を保存する（Saving Fabric Configuration）] メッセージがすぐに表示されます。これは、オーバーレイおよびアンダーレイ ネットワークの移行、および DCNM へのスイッチおよびポートチャネル設定の移行が開始されたことを示しています。

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（Config Deployment）]** ウィンドウが表示されます。



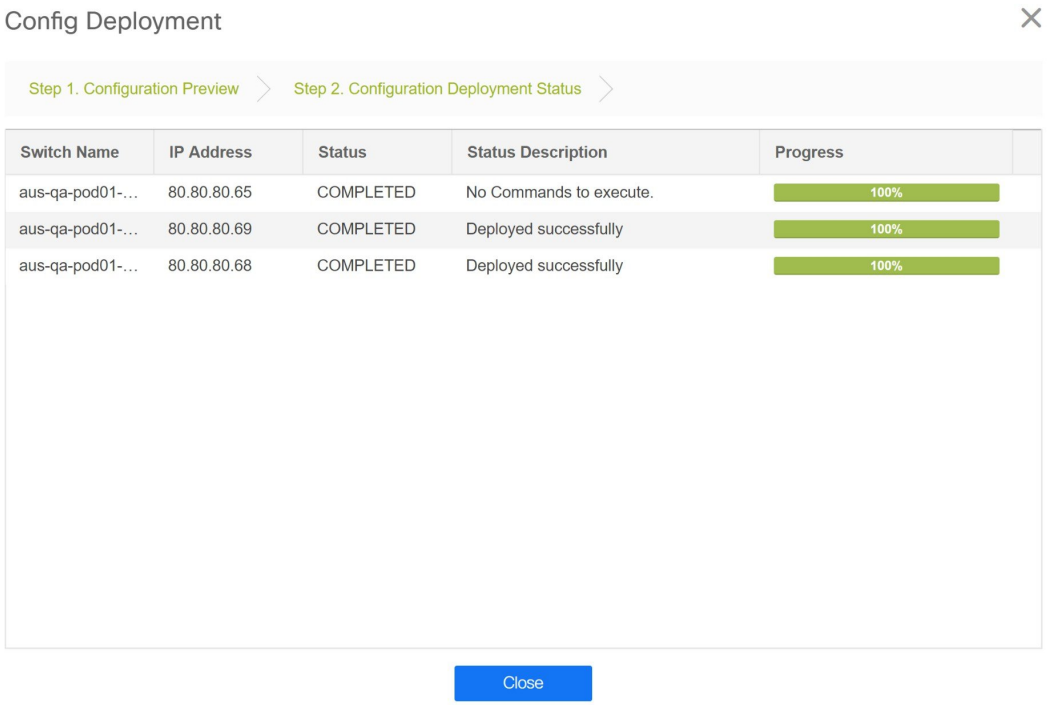
[構成のプレビュー（Preview Config）]列が、特定の行数を示すエントリで更新されます。

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 Config）]** 列のエントリをクリックします。**[構成プレビュー（Config Preview）]** ウィンドウが表示されます。このウィンドウには、スイッチの保留中の構成が一覧表示されます。**[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。



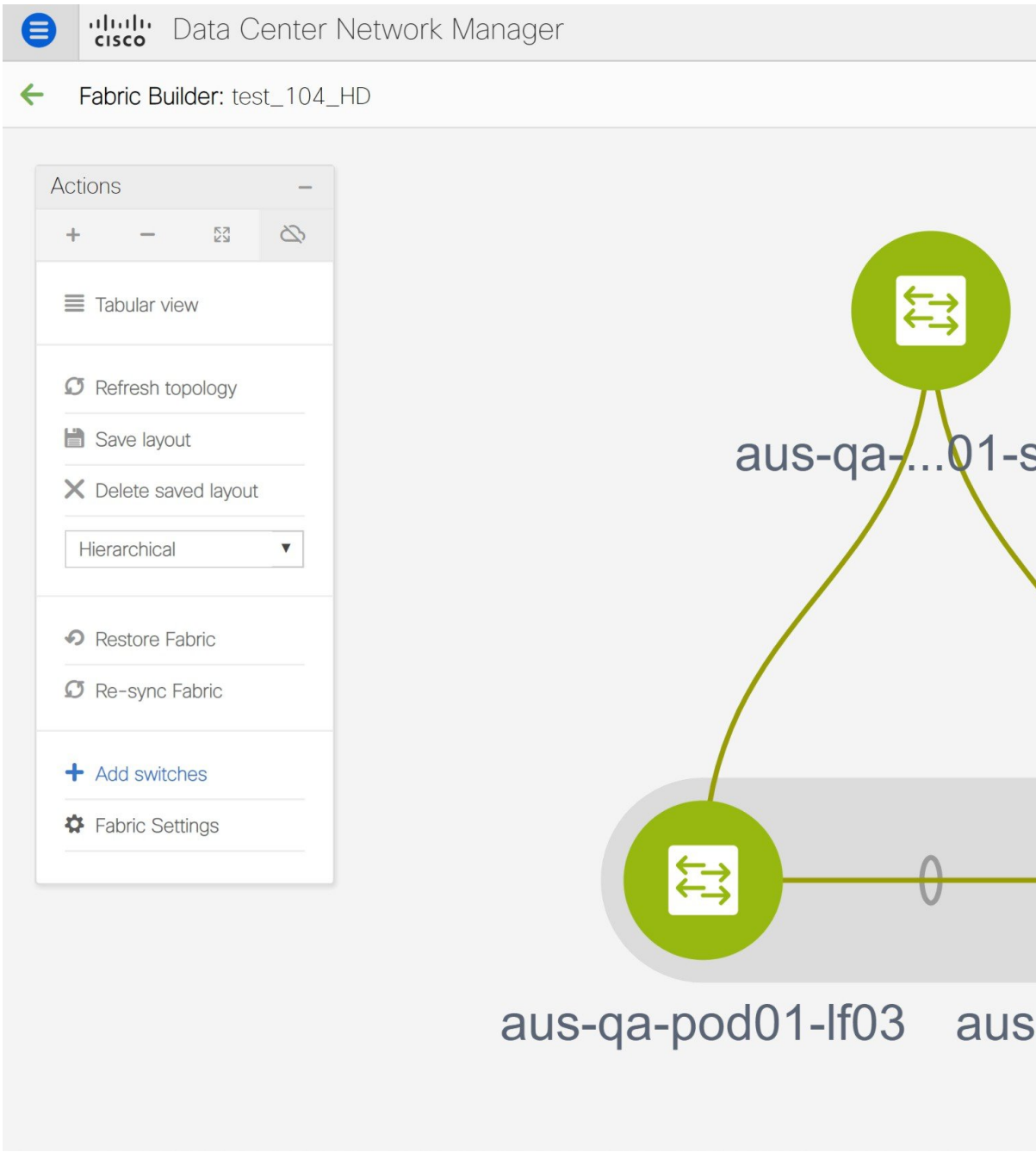
[構成プレビュー（Config Preview）] ウィンドウを閉じます。

8. **[構成の展開（Config Deployment）]** ウィンドウの下部にある **[構成の展開（Deploy Config）]** をクリックして、保留中の構成をスイッチに展開します。**[ステータス（Status）]** 列には、完了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。



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、**[構成の展開（Config Deployment）]** ウィンドウを閉じます。

ファブリック トポロジ ウィンドウでは、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、構成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。

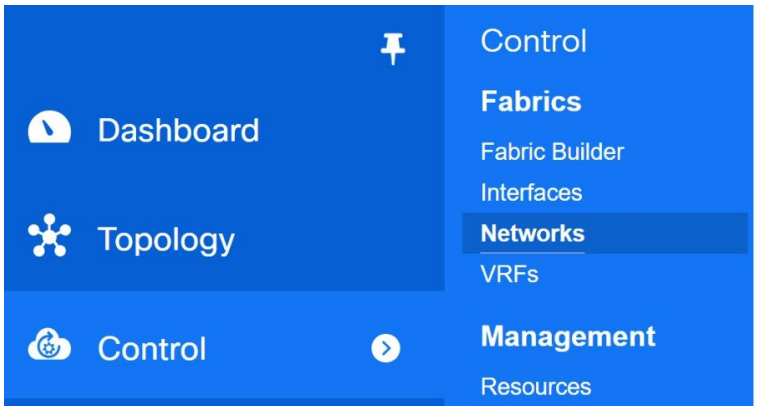


これで、ボトムアップ VXLAN ファブリックから DCNM への移行プロセスは完了です。

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。

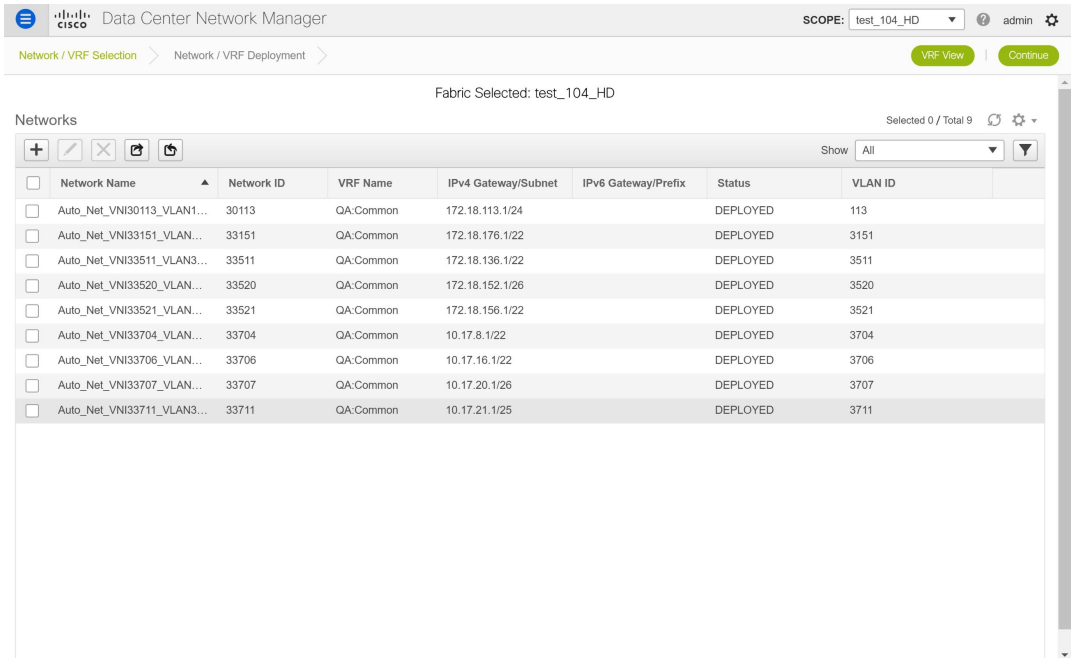
次の手順に従って、移行したネットワークを確認することもできます。

1. **[制御（Control）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** を選択します。



2. **[ネットワーク（Networks）]** ウィンドウの **[範囲（SCOPE）]** ドロップダウンリストからファブリックを選択します。

3. ボトムアップ VXLAN ファブリックから移行されたネットワークとその展開ステータスを確認します。



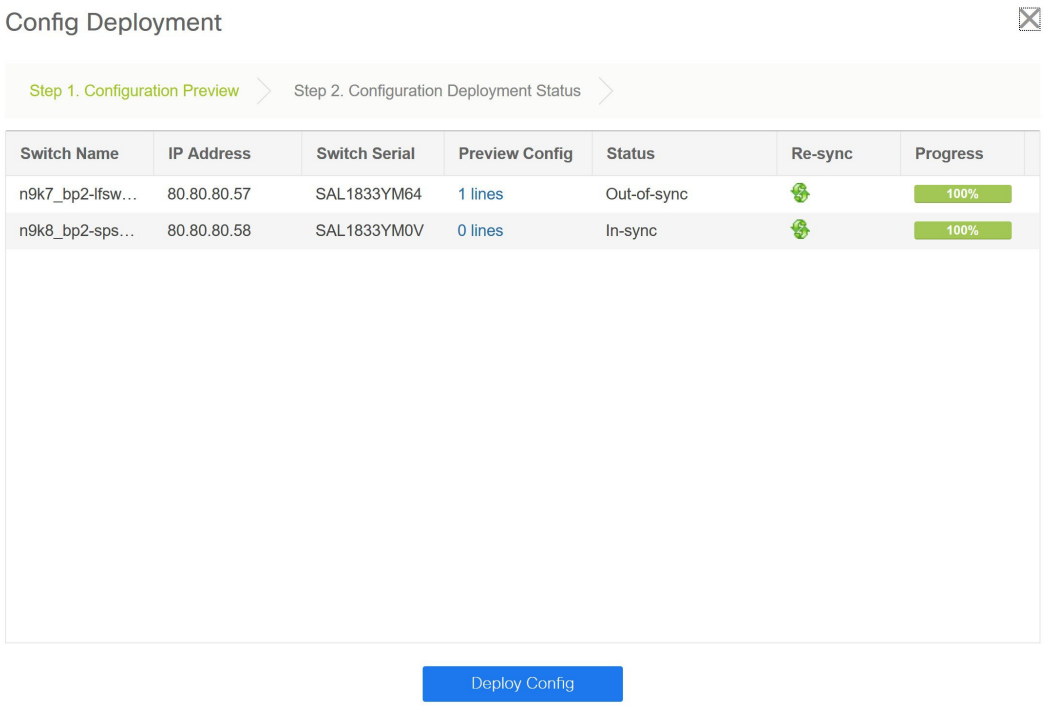
Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x) のイメージに沿って、スイッチでの構成コンプライアンス エラーを解決する

Cisco Nexus 9300 シリーズ スイッチおよび Cisco Nexus 9500 シリーズ スイッチと Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x) イメージを備えた X9500 ラインカードをブラウンフィールド展開した後、構成コンプライアンスの違いが表示されます。構成コンプライアンス エラーを解決するには、これらのスイッチから **tcam_pre_config_vxlan** ポリシーを削除する必要があります。

ブラウンフィールド展開後のスイッチでの構成コンプライアンス エラーの解決

次の手順は、ブラウンフィールド展開後にスイッチから **tcam_pre_config_vxlan** ポリシーを削除する方法を示しています。

1. **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。
2. **[ファブリック ビルダ（Fabric Builder）]** ウィンドウで、X9500 ラインカードを備えた Cisco Nexus 9300 シリーズ スイッチまたは Cisco Nexus 9500 シリーズ スイッチを含むブラウンフィールド ファブリックをクリックします。
3. （オプション）**[保存と展開（Save & Deploy）]** をクリックして、構成コンプライアンス エラーを表示します。

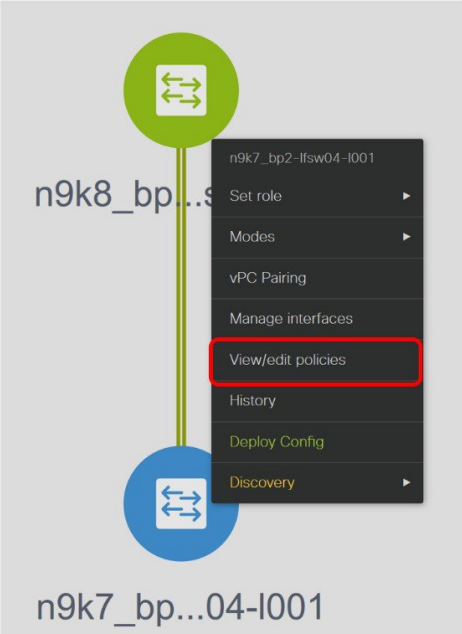


4. （オプション）**[構成のプレビュー（Preview Config）]** 列の下にある **1 行**が表示されているエントリをクリックします。

   [構成のプレビュー（Config Preview）] ウィンドウの **[保留中の構成（Pending Config）]** タブに TCAM コマンドが表示されます。

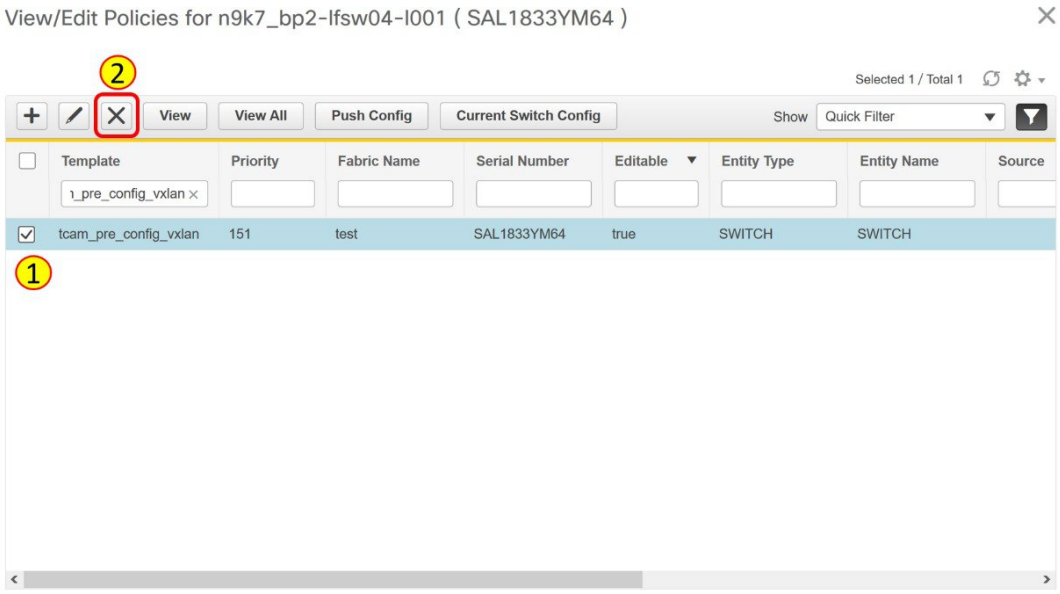
   [構成プレビュー（Config Preview）] ウィンドウを閉じます。

5. スイッチを右クリックし、**[ポリシーの表示/編集（View/Edit Policies）]** をクリックします。



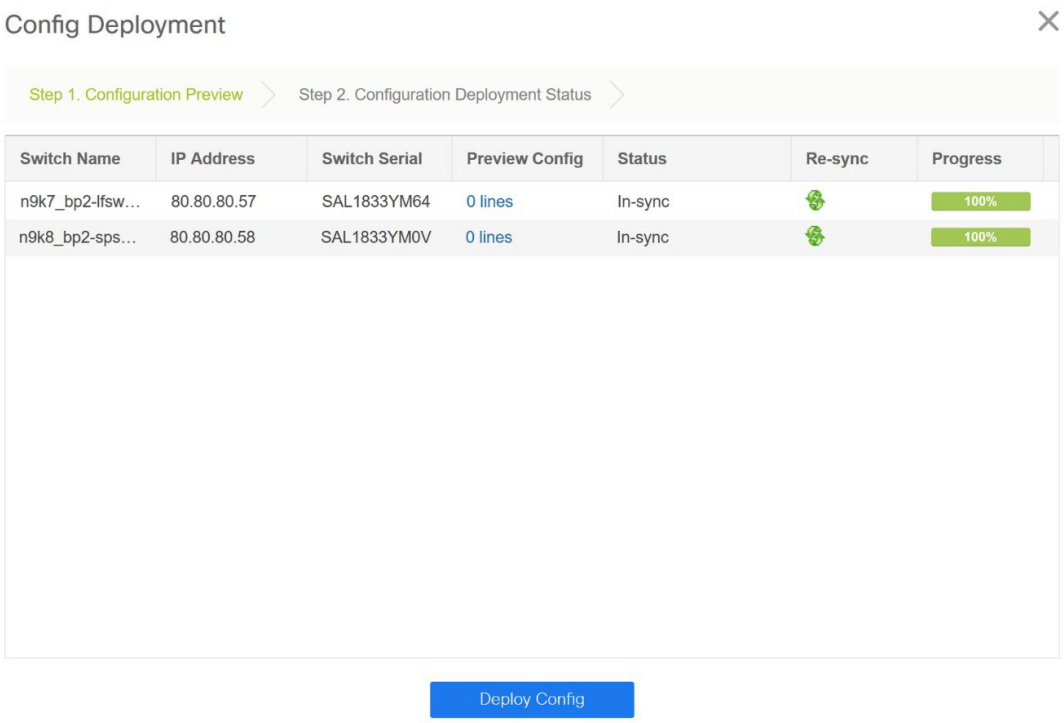
6. **[テンプレート（Template）]**検索フィールドで **tcam_pre_config_vxlan** ポリシーを検索します。

7. **tcam_pre_config_vxlan** ポリシーを選択し、**[削除（Delete）]** アイコンをクリックしてポリシーを削除します。



[ポリシーの表示/編集（View/Edit Policies）] ウィンドウを閉じます

8. （オプション）**[保存と展開（Save & Deploy）]** をクリックして、保留中の構成があるかどうかを確認します。

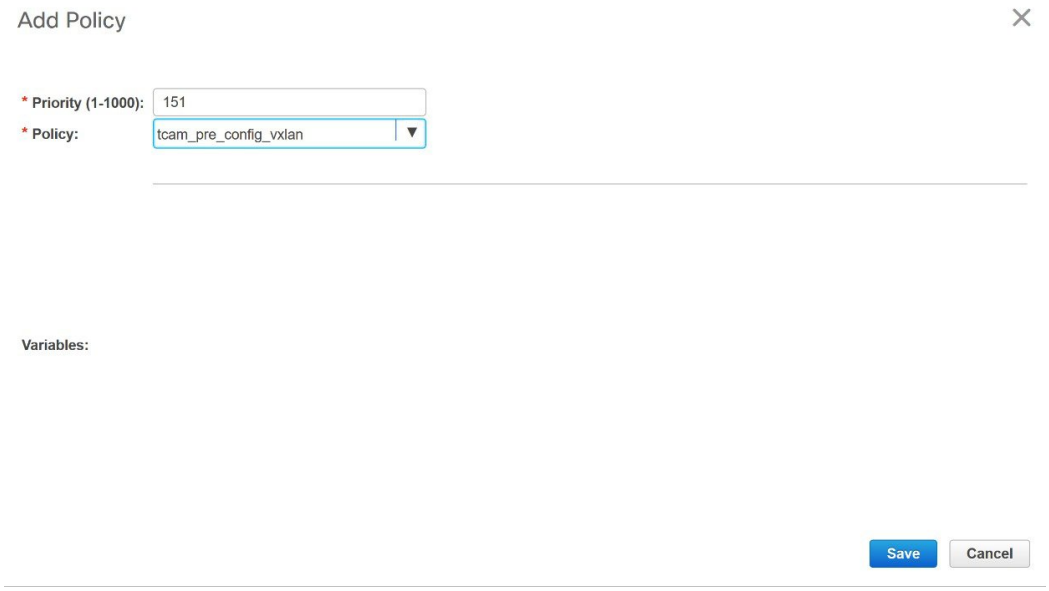


RMA のスイッチでの構成コンプライアンス エラーの解決、および書き込み消去およびリロード操作

Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x) イメージを搭載した Cisco Nexus 9300 シリーズ スイッチおよび X9500 ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチで RMA または書き込み消去およびリロード操作を実行する前に、次の手順を実行します。

1. **[制御（Control）]>[ファブリック（Fabrics）]>[ファブリック ビルダ（Fabric Builder）]** を選択します。
2. 指定されたスイッチと Cisco イメージを含むブラウンフィールド ファブリックをクリックします。
3. スイッチを右クリックし、**[ポリシーの表示/編集（View/Edit Policies）]** をクリックします。
4. [追加（Add）] アイコンをクリックします。

5. 優先順位（1-1000）フィールドに 151 を入力し、**[ポリシー（Policy）]** ドロップダウンリストから **tcam_pre_config_vxlan** を選択します。



6. [保存（Save）] をクリックします。
7. RMA または書き込み消去およびリロード操作を完了します。

   スイッチがオンラインになると、Out-of-Sync になります。
8. スイッチを右クリックし、**[ポリシーの表示/編集（View/Edit Policies）]** をクリックします。
9. **[テンプレート（Template）]**検索フィールドで **tcam_pre_config_vxlan** ポリシーを検索します。
10. **tcam_pre_config_vxlan** ポリシーを選択し、**[削除（Delete）]** アイコンをクリックしてポリシーを削除します。

[ポリシーの表示/編集（View/Edit Policies）] ウィンドウを閉じます

Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x) のイメージに沿って、スイッチで VLAN 名を変更する

ブラウンフィールド移行後、ネットワークまたは VRF の VLAN 名は、少なくとも 1 つの非スパイン スイッチに Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x) のイメージがある場合、オーバーレイ プロファイル内にキャプチャされません。

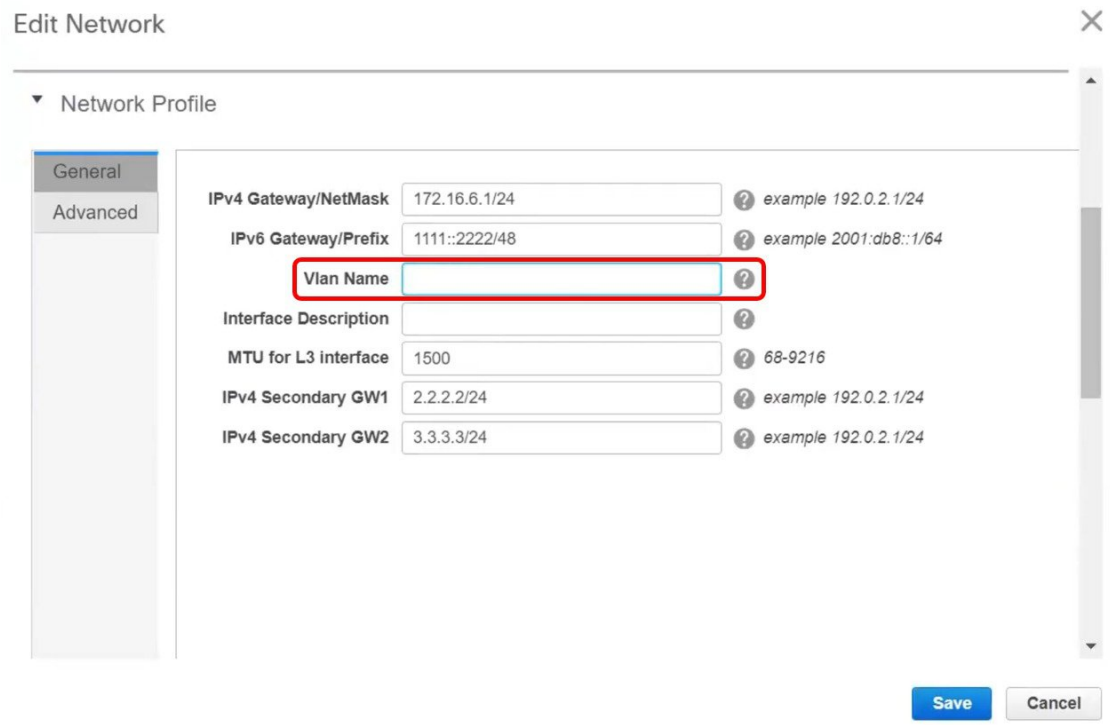
この手順は、VLAN 名を確認して変更する方法を示しています。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** を選択します。

ステップ 2 **[範囲（SCOPE）]** ドロップダウンリストから、Cisco NX-OS Release 7.0(3)I4(8b) および 7.0(4)I4(x) イメージの非スパイン スイッチを含むファブリックを選択します。

ステップ 3 **[ネットワーク（Networks）]** ウィンドウでネットワークのチェックボックスを選択し、**[ネットワークの編集（Edit Network）]** アイコンをクリックします。



[ネットワークの編集（Edit Network）] ウィンドウでは、DCNM がオーバーレイ プロファイルでこの情報をキャプチャしていないため、**[VLAN 名（Vlan Name）]** フィールドは空です。代

わりに、VLAN 名は、オーバーレイ ネットワークまたは VRF に関連付けられた自由形式の構成にキャプチャされます。

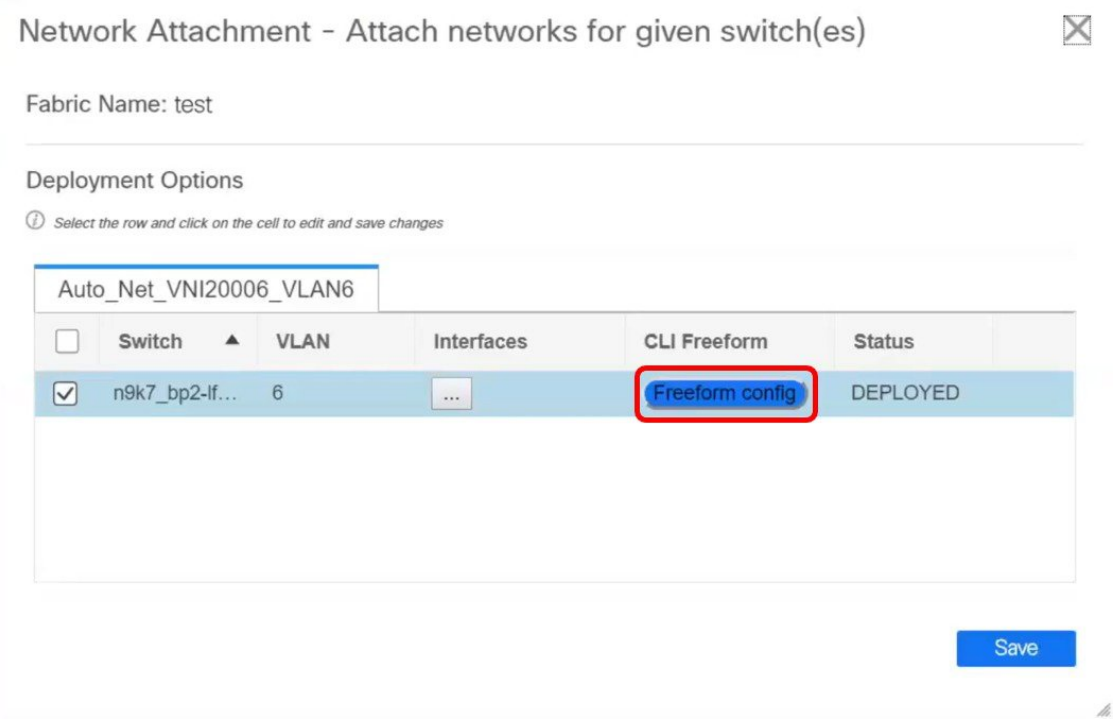
Note ブラウンフィールド移行前に VLAN に名前がなかった場合は、**[ネットワークの編集（Edit Network）]** ウィンドウの **[VLAN 名（Vlan Name）]** フィールドに名前を追加できます。

[ネットワークの編集（Edit Network）] ウィンドウを閉じます。

ステップ 4 **[ネットワーク（Networks）]** ウィンドウで **[続行（Continue）]** をクリックします。

ステップ 5 **[トポロジ表示（Topology View）]** ウィンドウでスイッチをダブルクリックします。

ステップ 6 スイッチの **[ネットワーク アタッチメント（Network Attachment）]** ウィンドウで、**[CLI 自由形式（CLI Freeform）]** 列の下にある **[自由形式構成（Freeform config）]** ボタンをクリックします。

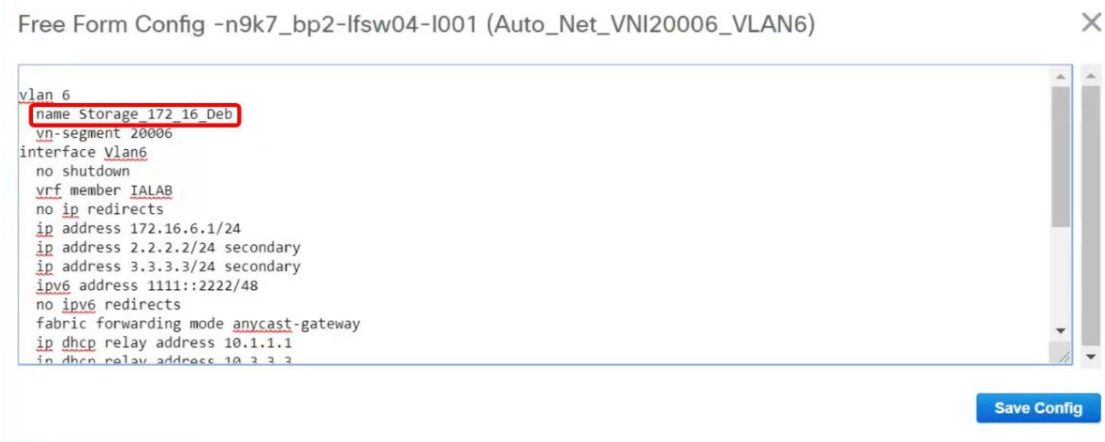


ステップ 7 **[自由形式構成（Free Form Config）]** ウィンドウで VLAN 名を確認します。

ステップ 8 **[自由形式構成（Free Form Config）]** ウィンドウで VLAN 名を変更し、**[構成の保存（Save Config）]** をクリックします。

次に例を示します。

```
vlan 6
  name Storage_172_16_Deb
  vn-segment 20006
interface Vlan6
.
.
.
```



ステップ 9 **[ネットワーク アタッチメント（Network Attachment）]** ウィンドウで **[保存（Save）]** をクリックします。

ステップ 10 **[ネットワーク（Networks）]** ウィンドウで **[展開（Deploy）]** をクリックします。

選択したネットワークの変更された VLAN 名がスイッチに展開されます。

ブラウンフィールドでインポートされた BIDIR 構成の変更

この手順は、**ファブリック ビルダ**によって生成された構成を使用するようにブラウンフィールドでインポートされた BIDIR 構成を変更する方法を示しています。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** を選択します。

ステップ 2 ブラウンフィールド ファブリックをクリックします。

ステップ 3 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウの **[アクション（Actions）]** パネルの下にある **[表形式ビュー（Tabular View）]** をクリックします。

ステップ 4 すべてのデバイスを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** アイコンをクリックします。

ステップ 5 **[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウで、すべてのデバイスの次のポリシーを削除します。

- **base_pim_bidir_11_1**
- ファブリックに 1 つの RP がある場合は、**rp_lb_id** ポリシーを削除します。

  ファブリックに 2 つの RP がある場合は、**phantom_rp_lb_id1** および **phantom_rp_lb_id2** ポリシーを削除します。

ステップ 6 **[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウを閉じます

ステップ 7 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウの **[インターフェイスの管理（Manage Interfaces）]** ボタンをクリックします。

ステップ 8 **[インターフェイス（Interfaces）]** ウィンドウですべての RP ループバック インターフェイスを削除し、このウィンドウを閉じます。

ステップ 9 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウで **[保存と展開（Save & Deploy）]** をクリックします。

このアクションにより、デバイスのファブリック設定に基づいて、BIDIR 関連の構成の新しいセットが生成されます。

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。

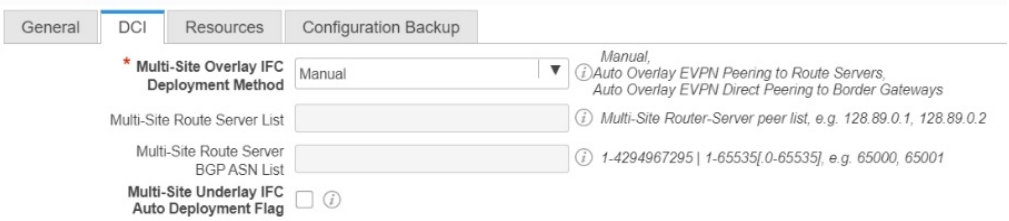
ステップ 2 各 **base_pim_bidir_11_1** ポリシーを新しいリーフまたはスパインの **[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウから追加し、各 **base_pim_bidir_11_1** ポリシーの構成をプッシュします。

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_11_1 ファブリック

  - MSD_Fabric_11_1 ファブリック

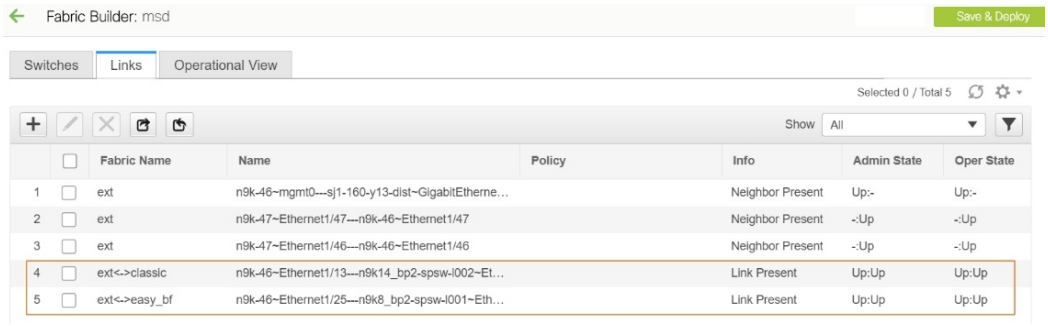


- アンダーレイ マルチサイト ピアリング：サイト間のアンダーレイ拡張の eBGP ピアリングおよび対応するルーテッド インターフェイスは、**switch_freeform** および **routed_inerfaces**、オプションで **interface_freeform** 構成でキャプチャされます。この構成には、マルチサイトのすべてのグローバル構成が含まれます。EVPN マルチサイトのループバックも、適切なインターフェイス テンプレートを介してキャプチャされます。
- オーバーレイ マルチサイト ピアリング：eBGP ピアリングは、**switch_freeform** の一部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_11_1 および External_Fabric_11_1 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 **[保存と展開（Save & 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 **[構成の展開（Deploy Config）]** をクリックしないでください。
4. 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_11_1** 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。**[表形式ビュー（Tabular View）]** に移動し、IFC リンクを編集します。



以下は、[IFC 編集リンク（IFC Edit Link）] ウィンドウの例です。

（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 [送信元/宛先インターフェイス（Source/Destination interface）] フリーフォーム フィールドに追加する必要があります。

詳細については、マルチサイト オーバーレイ *IFC* の構成を参照してください。

7. 展開された構成の IP アドレスと設定に一致するように、すべてのマルチサイト オーバーレイ IFC を作成します。IFC リンクを追加する必要があります。詳細については、マルチサイト オーバーレイ *IFC* の構成を参照してください。
8. VRF-Lite IFC もある場合は、それらも作成します。

（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 **[保存と展開（Save & Deploy）]** をクリックしますが、**[構成の展開（Deploy Config）]** 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、**[保存と展開（Save & Deploy）]** をクリックしてから、**[構成の展開（Deploy Config）]** 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 DCNM 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 17 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 DCNM リリース 11.3(1) から、IPv6 のみのアンダーレイで Easy fabric を作成できます。IPv6 アンダーレイは、**Easy_Fabric_11_1** テンプレートでのみサポートされています。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、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、DCNM 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 **[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]** に移動します。

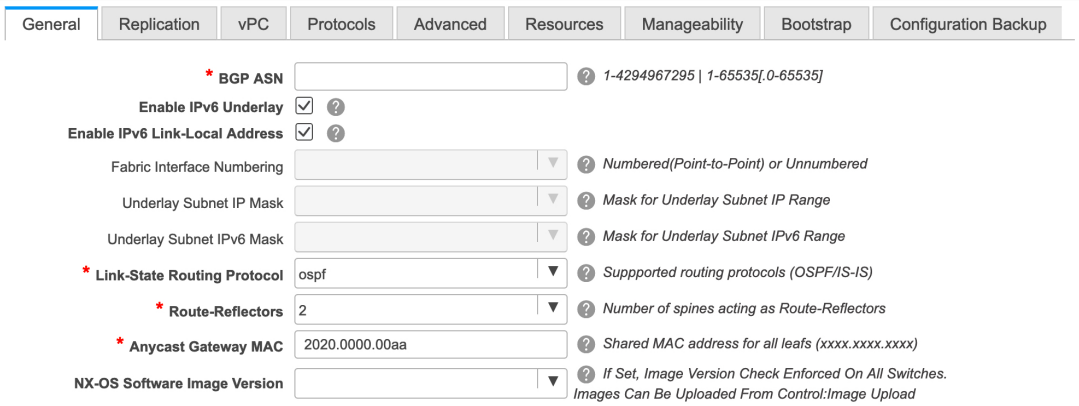
ステップ 2 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウで、**[ファブリックの作成（Create Fabric）]** をクリックします。

[ファブリックの追加（Add Fabric）] 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_11_1]** ファブリック テンプレートを選択します。

ステップ 3 **[全般（General）]** タブで関連する値を入力します。



[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）]：このチェックボックスを選択して、IPv6 アンダーレイ機能を有効にします。

[リンク ローカル アドレスを有効にする （Enable Link-Local Address）]：このチェック 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、**[リンク ローカル アドレスを有効にする （Enable 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。

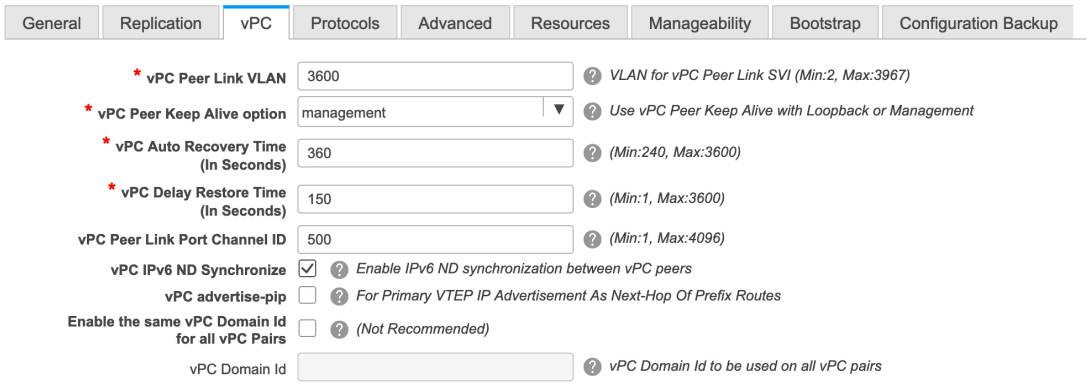
[リンクステート ルーティング プロトコル （Link-State Routing Protocol）]：ファブリックで使用される IGP で、VXLANv6 の場合、OSPFv3 または IS-IS です。

ステップ 4 [レプリケーション（Replication）] タブをクリックします。

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。

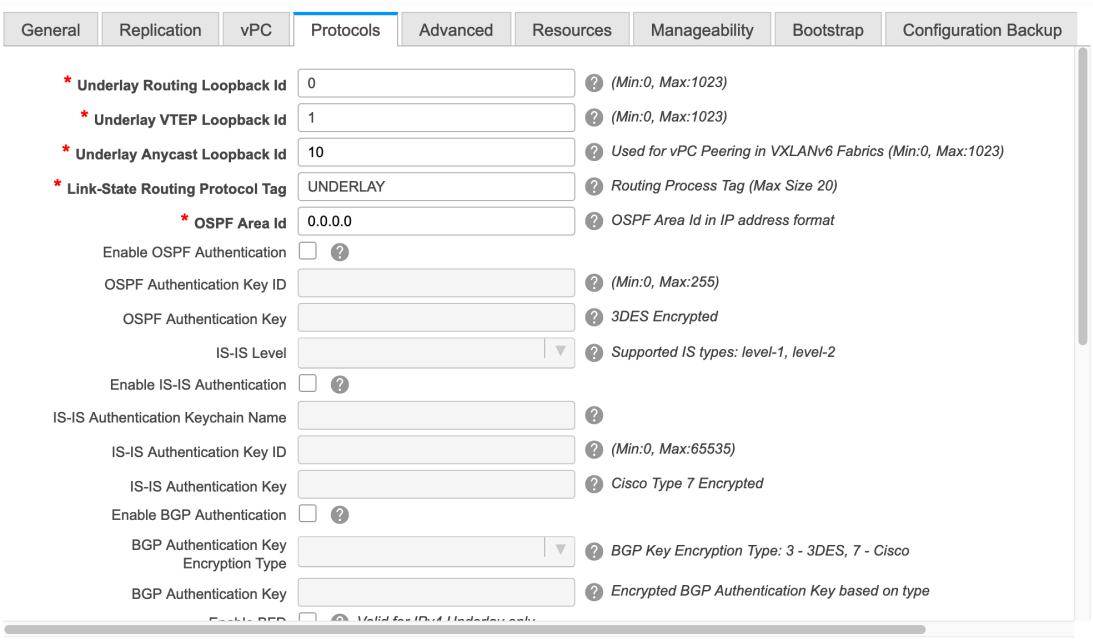
このタブの下のすべてのフィールドは無効になっています。

ステップ 5 **[vPC]** タブをクリックします。



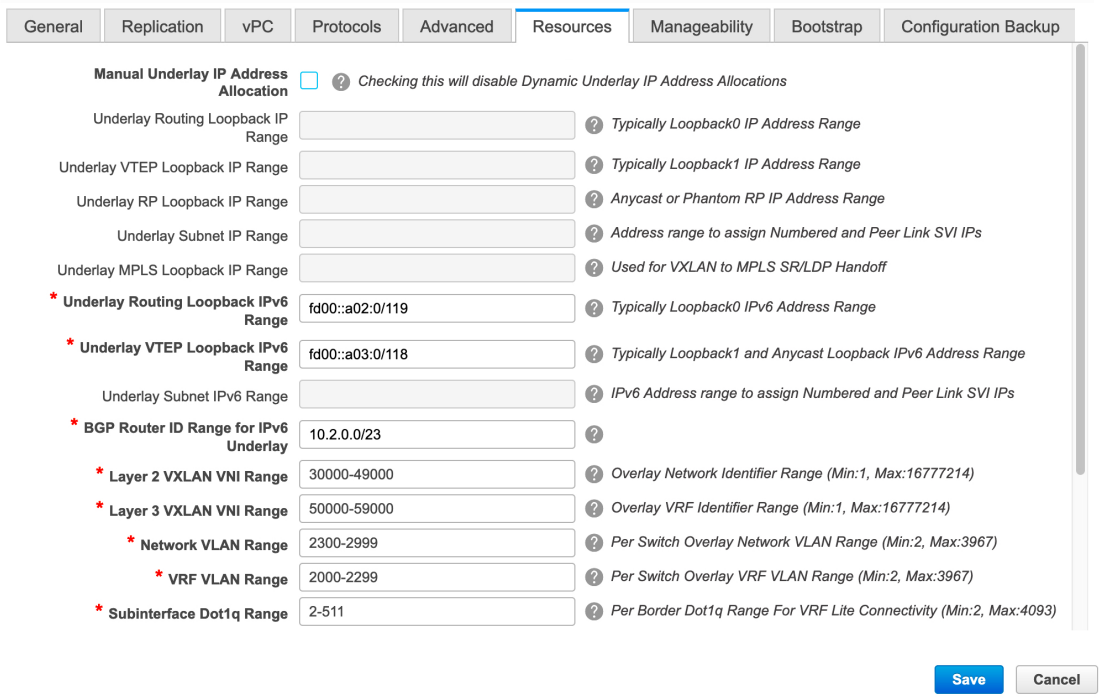
[vPC ピア キープアライブ オプション（vPC Peer Keep Alive option）]：管理またはループバック オプションを選択します。管理ポートおよび管理 VRF に割り当てられた IP アドレスを使用する場合は、[管理（management）] を選択します。ループバック インターフェイス（および非管理 VRF）に割り当てられた IP アドレスを使用する場合は、ループバックを選択します。どちらのオプションも IPv6 アンダーレイでサポートされています。

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）]：このチェックボックスをオンにして、アンダーレイ IP アドレスを手動で割り当てます。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。

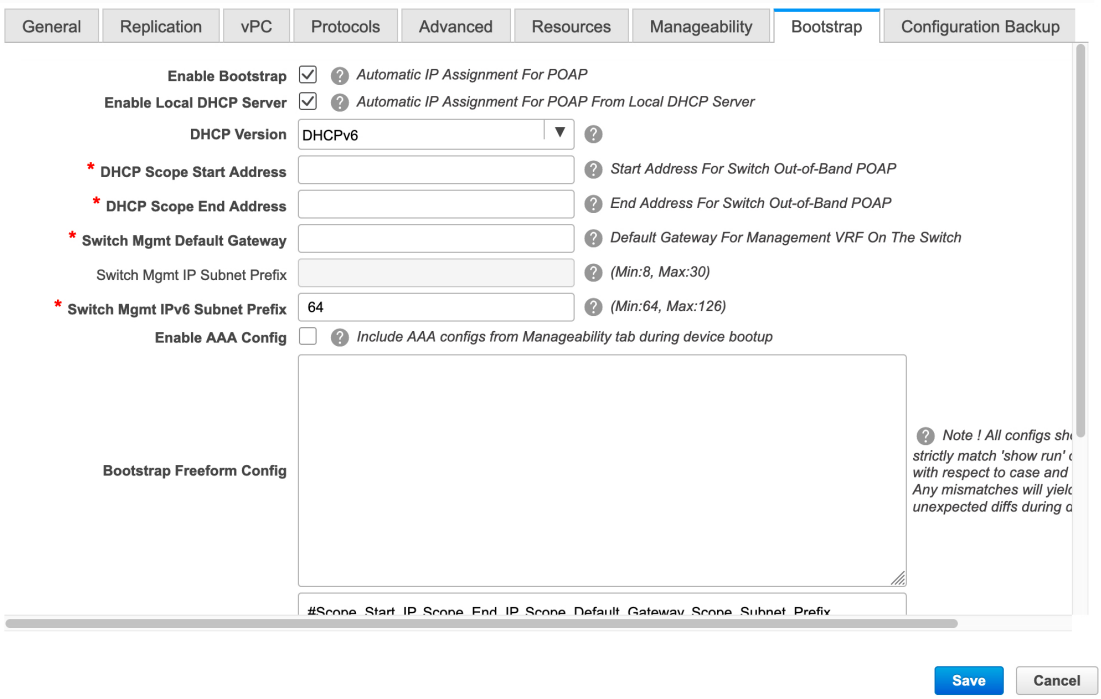
[アンダーレイ ルーティング ループバック IPv6 範囲（Underlay Routing Loopback IPv6 Range）]：プロトコル ピアリングのループバック IPv6 アドレスを指定します。

[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 IP アドレスを指定します。エニーキャストの IPv6 アドレスは、この範囲から割り当てられます。

[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、[全般（**General**）] タブの **[リンクローカル アドレスの有効化（Enable Link-Local Address）]** チェックボックスをオフにする必要があります。

[アンダーレイ BGP ルータ ID 範囲（Underlay BGP Router ID Range）]：BGP ルータ ID を割り当てるアドレス範囲を指定します。

ステップ 8 **[ブートストラップ（Bootstrap）]** タブをクリックします。



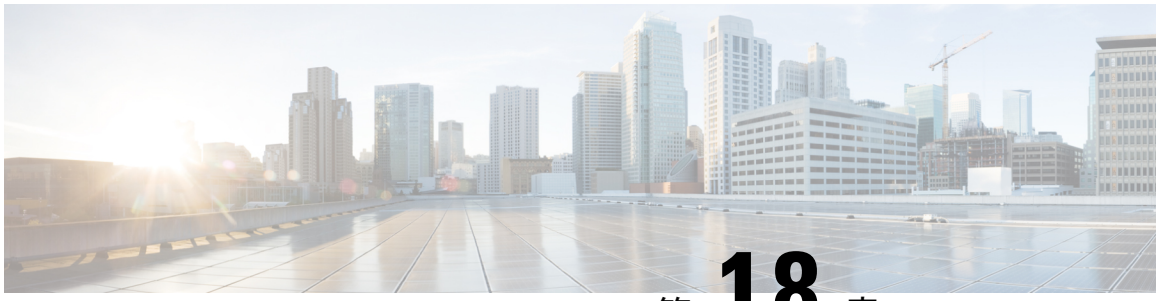
[DHCP バージョン（DHCP Version）]：このドロップダウンリストから [DHCPv4] または [DHCPv6] を選択します。DHCPv4 を選択すると、**[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]** フィールドが無効になります。DHCPv6 を選択すると、**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** は無効になります。

[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 の間で設定可能です。このフィールドは DHCP の IPv6 が有効な場合に編集できます。

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 18 章

VXLAN VTEP にアタッチされた ToR スイッチの自動プロビジョニング

この章では、Top-of-Rack（ToR）スイッチを構成し、DCNM 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

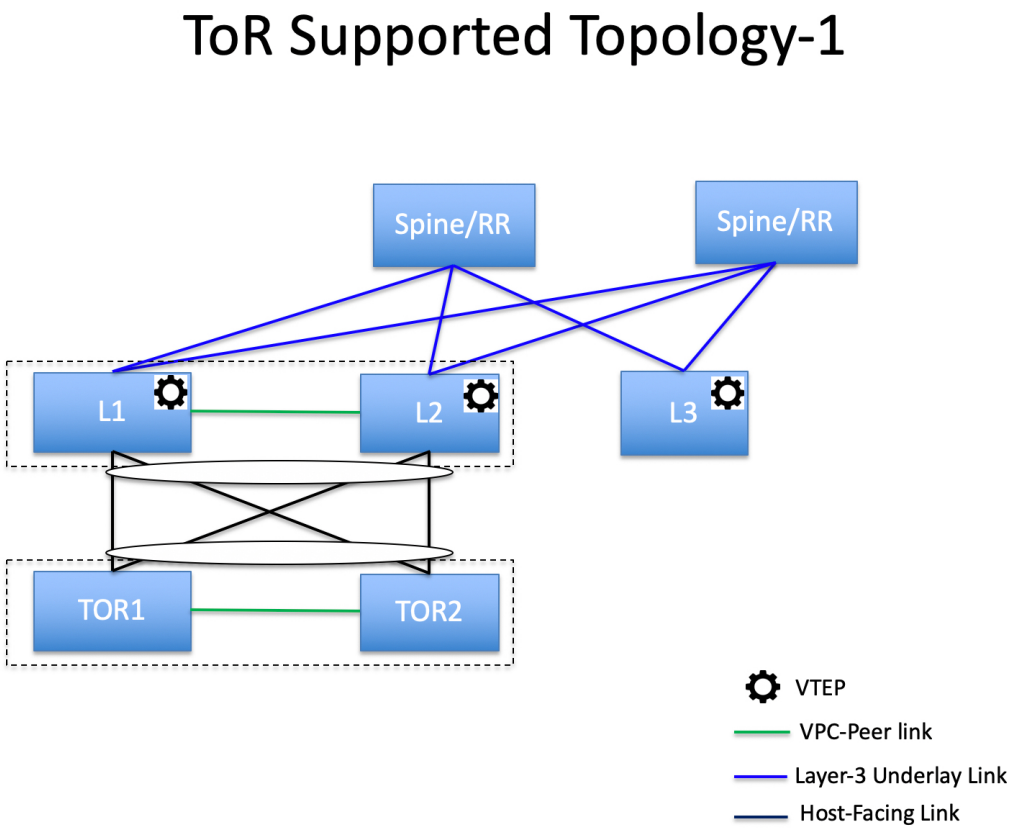
Cisco DCNM 11.3(1) 以降、トップオブラック（ToR）スイッチのサポートが Cisco DCNM に追加されました。外部ファブリックにレイヤ 2 ToR スイッチを追加でき、それらを Easy ファブリックのリーフ スイッチに接続できます。通常、リーフ デバイスと ToR デバイスはバックツーバック vPC 接続で接続されます。詳細については、「ToR スイッチでサポートされるトポロジ」を参照してください。

また、ToR スイッチを構成し、Cisco DCNM を使用してこれらのスイッチにネットワークを展開する方法を示すビデオを見ることもできます。「ToR スイッチの構成」を参照してください。

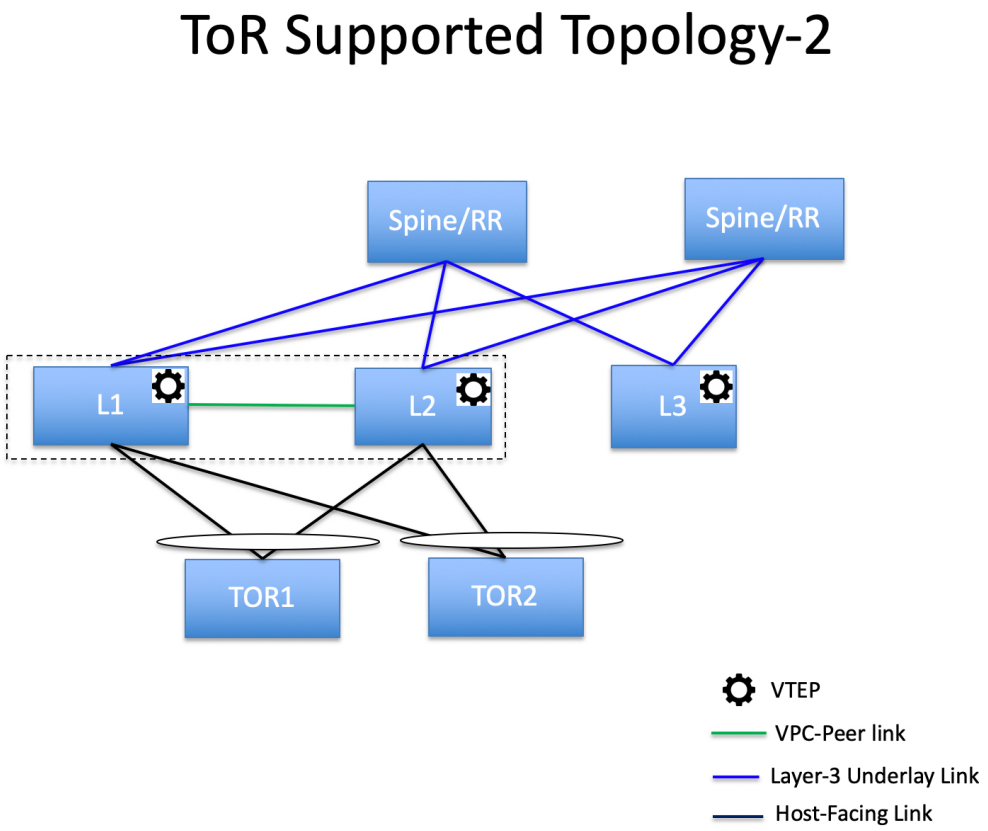
ToR スイッチでサポートされるトポロジ

DCNM 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。

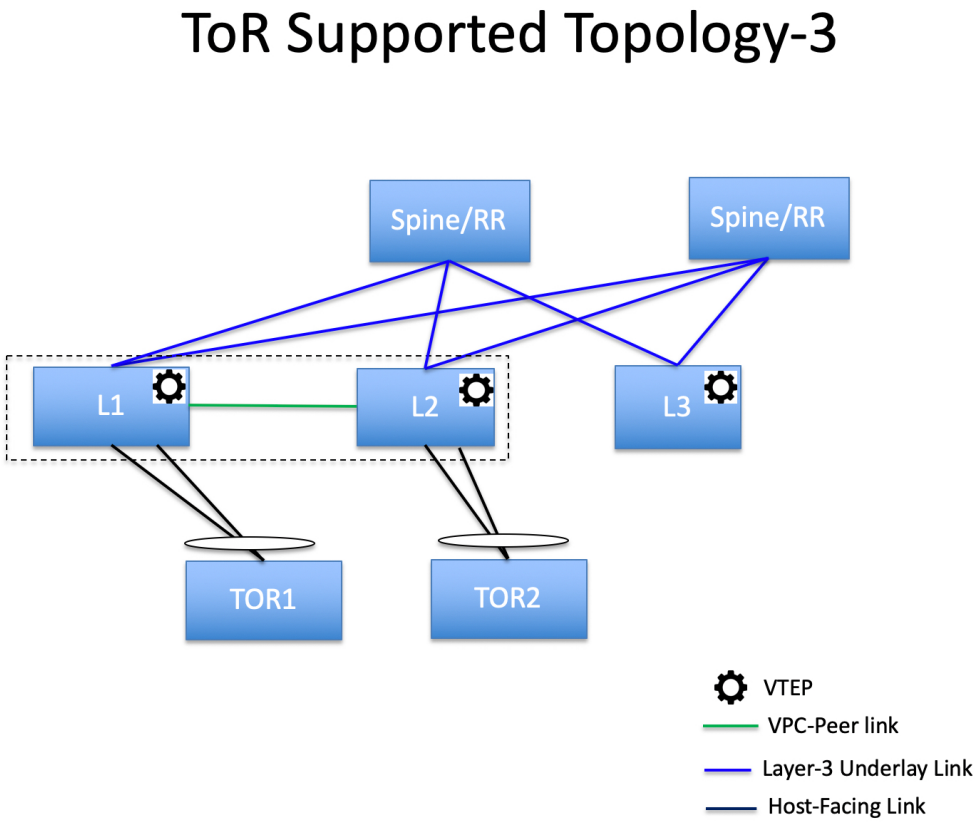
- リーフ スイッチへのバックツーバック vPC 接続を持つ ToR スイッチ。



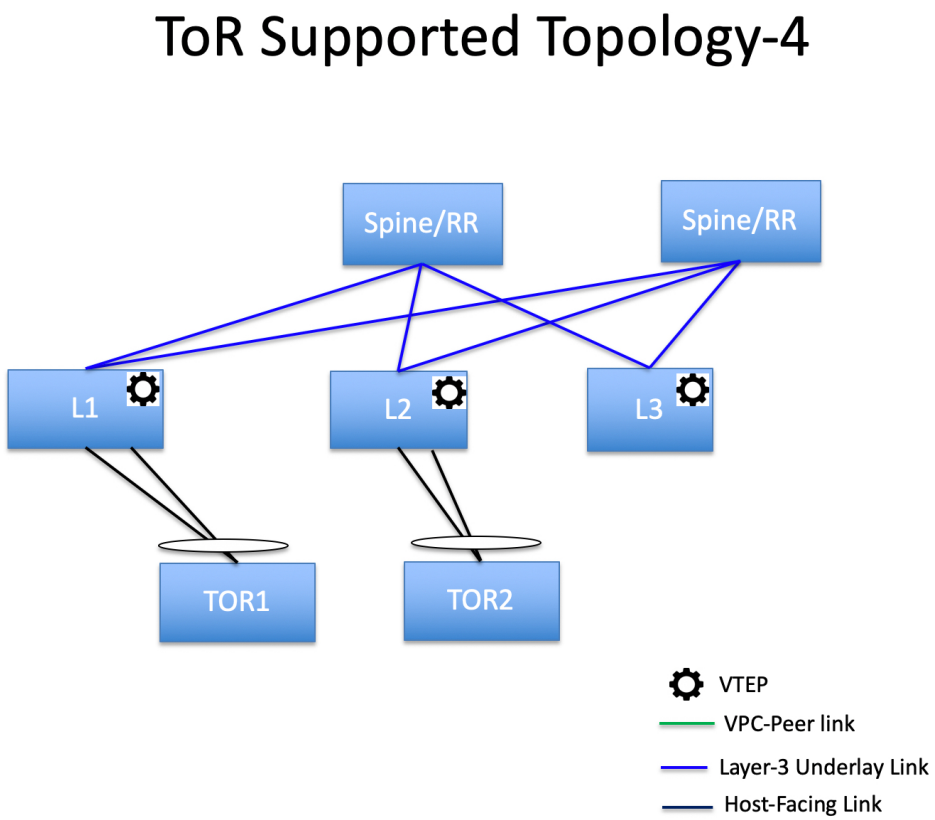
- ポート チャネルが両方のリーフ スイッチに接続されている ToR スイッチ。L1 スイッチと L2 スイッチは vPC ペアとして接続されます。



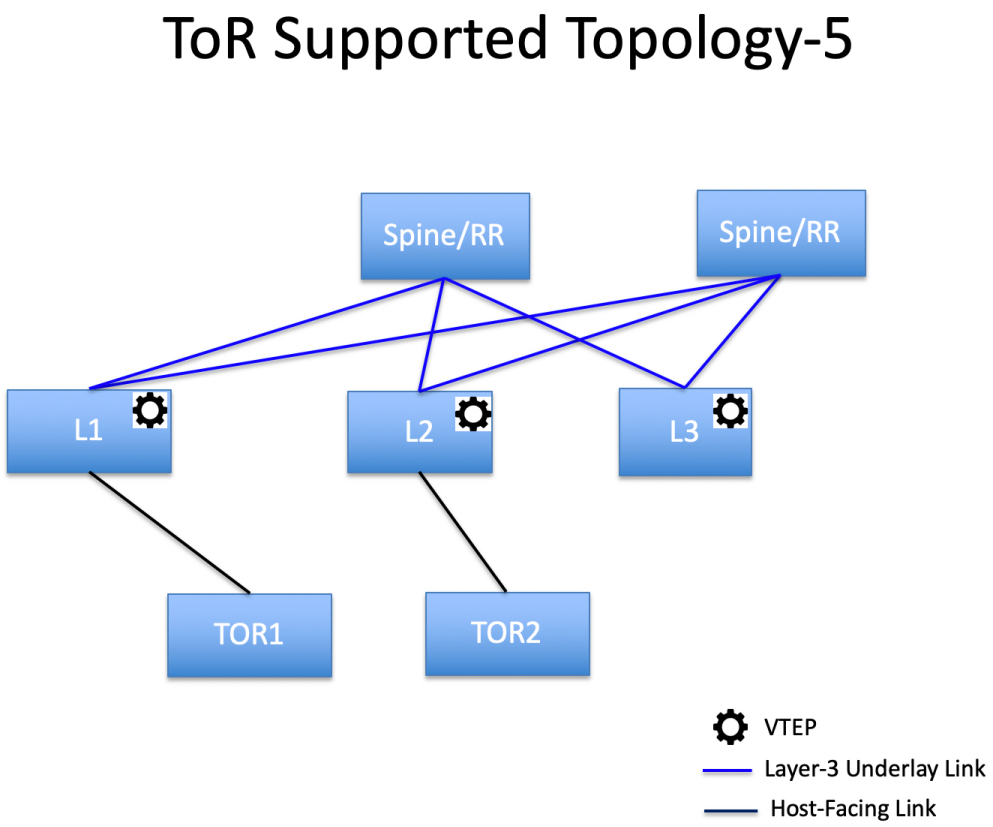
- ポート チャネルがリーフ スイッチに直接接続されている ToR スイッチ。L1 スイッチと L2 スイッチは vPC ペアとして接続されます。



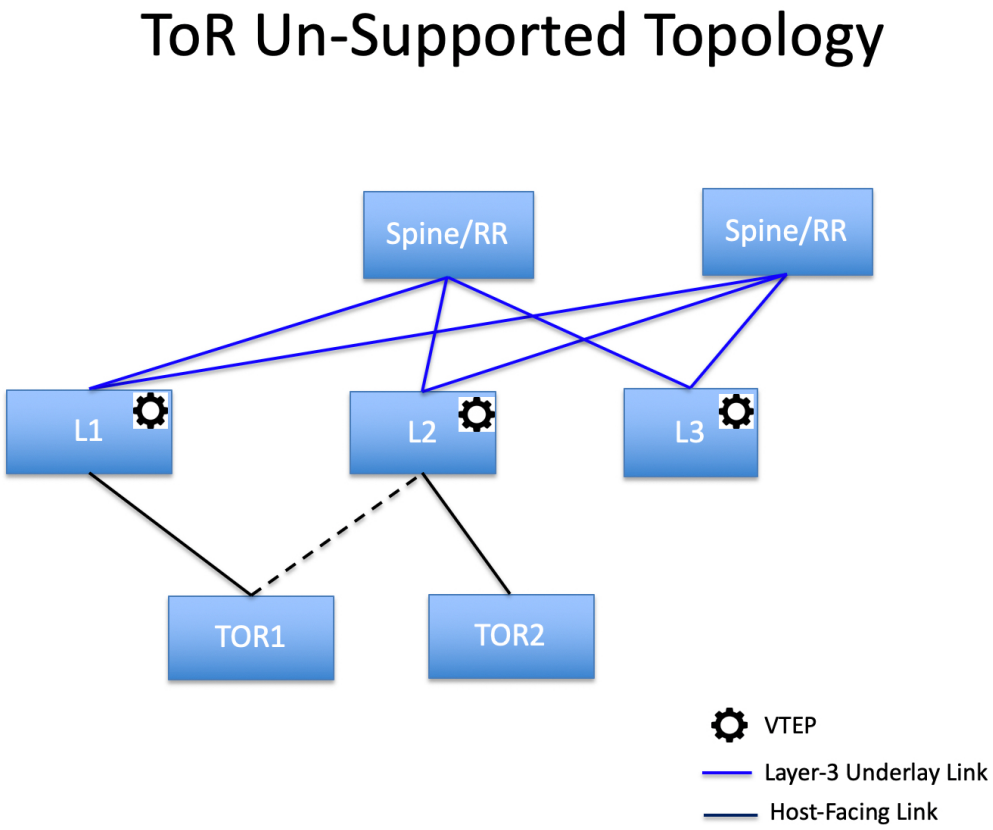
- ポート チャネルがリーフ スイッチに直接接続されている ToR スイッチ。 vPC ペアは、リーフ スイッチまたは ToR スイッチ用に構成されていません。



- 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、DCNM 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、『*Cisco DCNM LAN* ファブリック構成ガイド』の「新規 *VXLAN BGP EVPN* ファブリックの作成」を参照してください。

Note DCNM は、ToR スイッチの trunk_host ポリシーをサポートします。ToR に vPC ポリシー、ポートチャネル、およびトランク ホストがあることを確認してください。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、『*Cisco DCNM LAN* ファブリック構成ガイド』の「外部ファブリックの作成」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** 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。

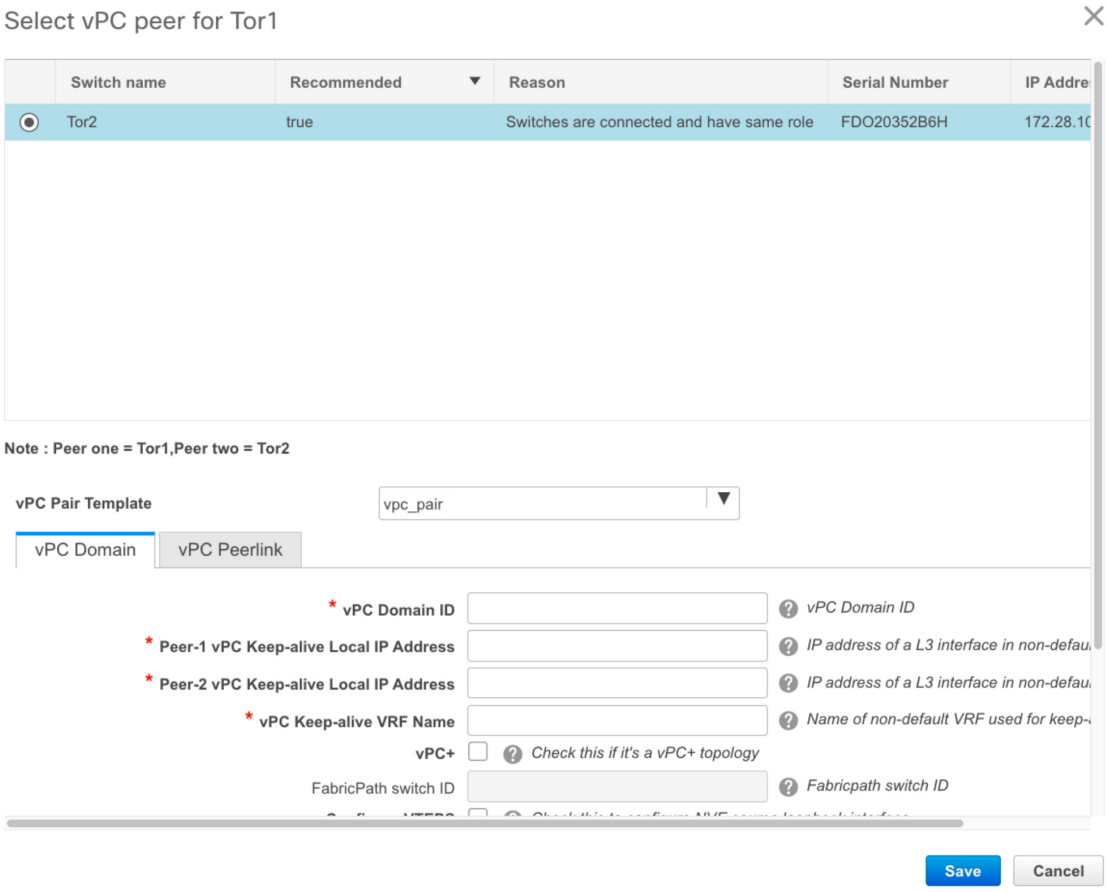
ToR スイッチを追加したら、ToR スイッチのロールが ToR として選択されていることを確認します。

ステップ 2 ToR スイッチを右クリックし、**[vPC ペアリング（vPC Pairing）]** を選択します。

2 番目の ToR スイッチを vPC ピアとして選択します。

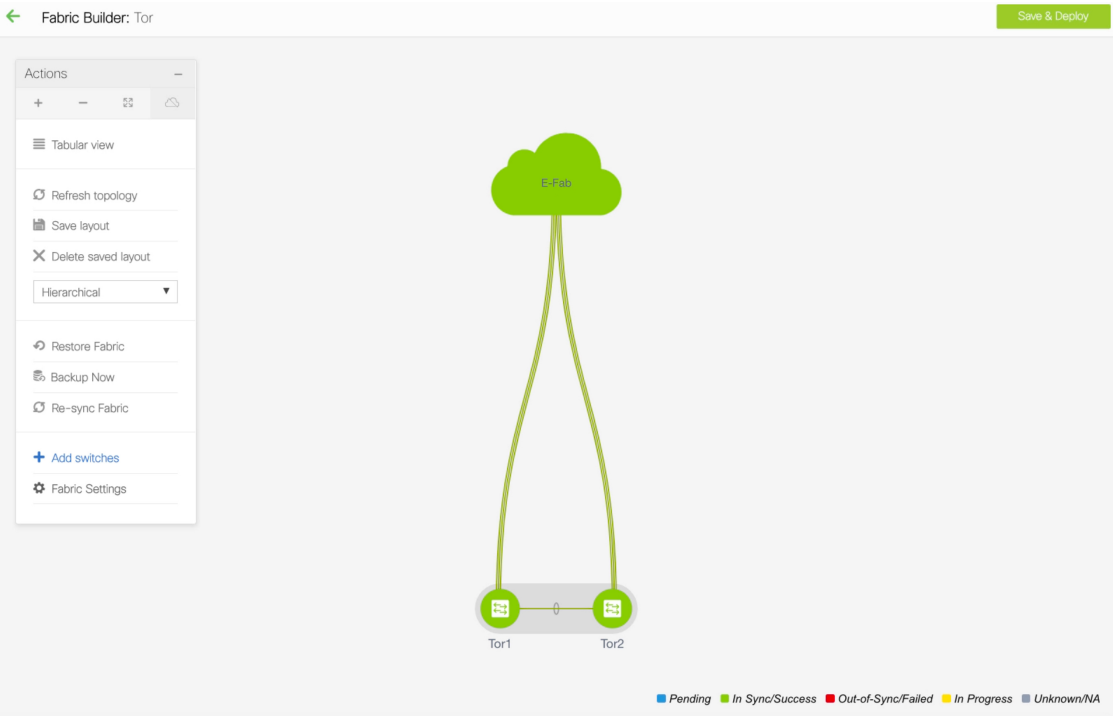
ステップ 3 [vPC ペア テンプレート（vPC Pair Template）] で、両方の ToR スイッチ間の vPC 接続に関連するすべての詳細を入力します。フィールドとその説明の詳細については、『*Cisco DCNM LAN* ファブリック構成ガイド』の「外部ファブリックでの *vPC* セットアップの作成」を参照してください。

Note この例はトポロジ 1 の ToR 構成を示しているため、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　**[保存と展開（Save & Deploy）]** をクリックし、**[構成の展開（Deploy Config）]** をクリックします。

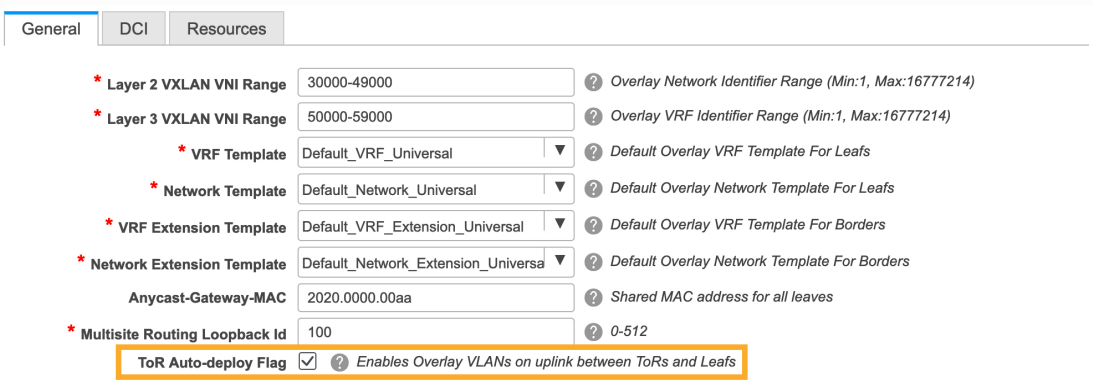
ステップ 5　**[構成展開（Config Deployment）]** ウィンドウの進行状況バーに 100% が表示されたら、**[閉じる（Close）]** をクリックします。



ステップ 6 MSD ファブリックを作成します。

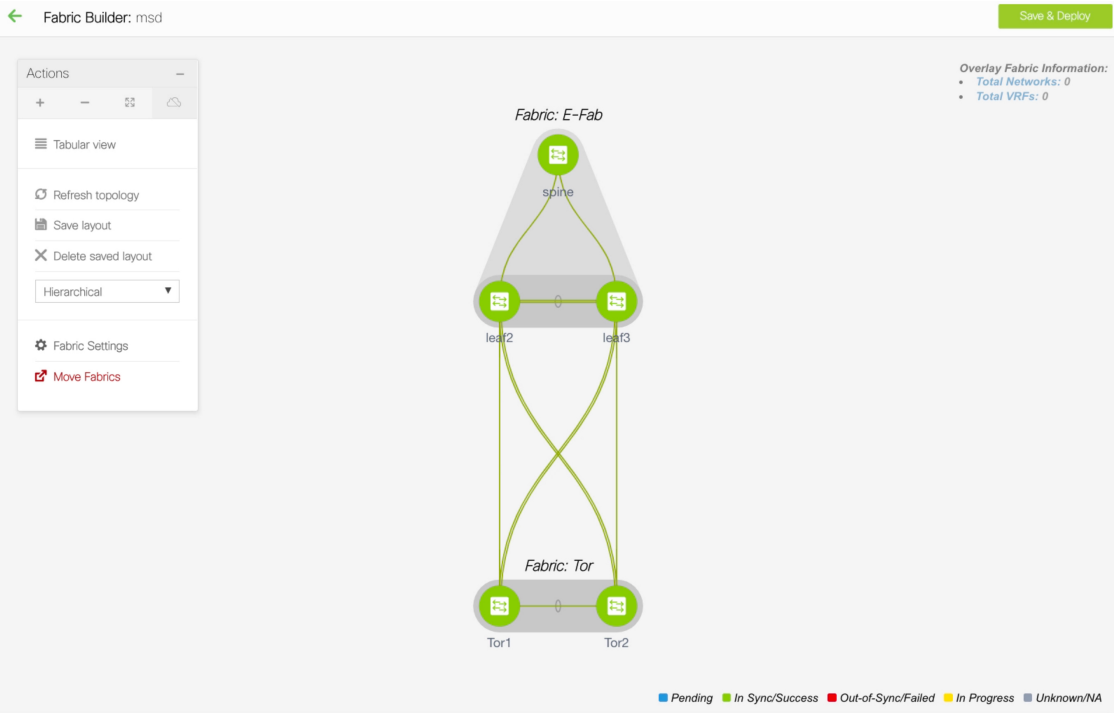
MSD ファブリックの作成中に、[全般（General）] タブで、[ToR 自動展開フラグ（ToR Auto-deploy Flag）] チェック ボックスをオンにします。これにより、MSD ファブリックで [保存と展開（Save & Deploy）] をクリックしたときに、Easy ファブリックのネットワークと VRF を外部ファブリックの ToR スイッチに自動展開できます。詳細については、「ToR スイッチでのネットワークの展開」を参照してください。

残りのタブとフィールドの詳細については、『*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。



ステップ 7 **[アクション（Action）]** パネルで **[ファブリックの移動（Move Fabric）]** をクリックします。**[ファブリックの移動（Move Fabric）]** ウィンドウで、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。

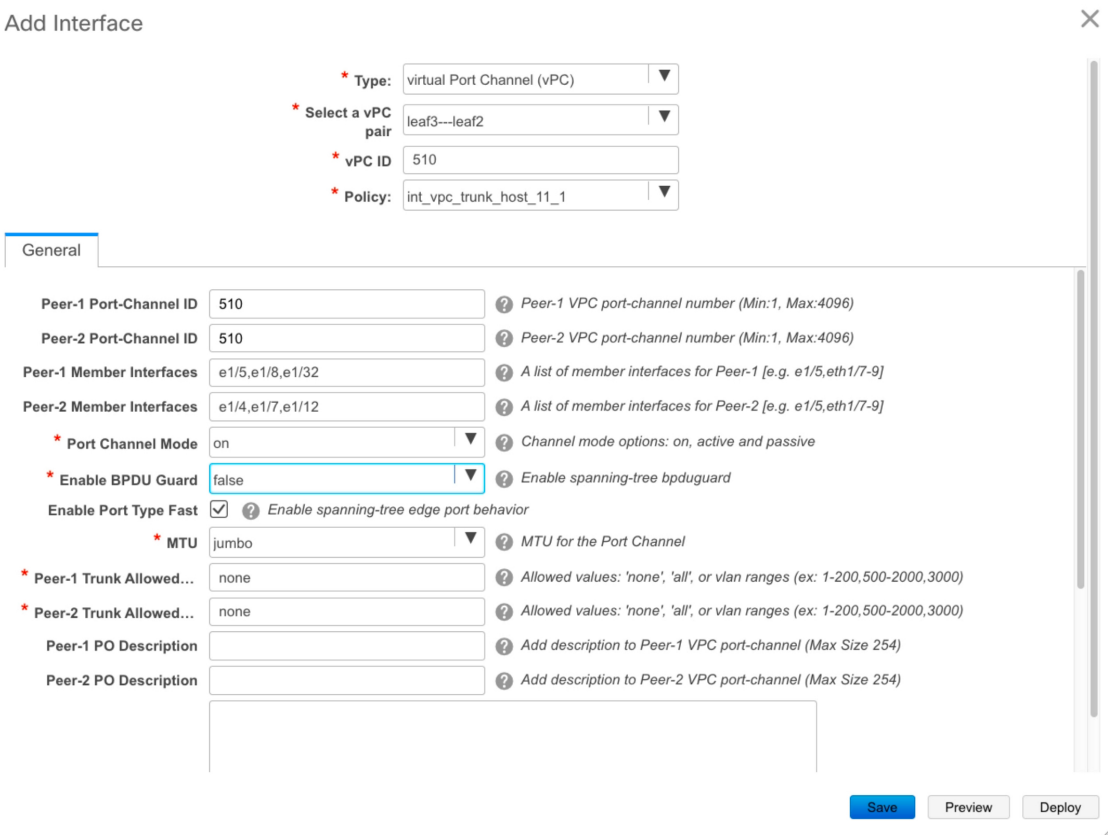


ステップ 8 **[戻る（Back）]** アイコンをクリックして、リーフスイッチを含む Easy ファブリックをクリックします。

ステップ 9 リーフスイッチと ToR スイッチの間に vPC を作成する必要があります。リーフスイッチを右クリックし、**[インターフェイスの管理（Manage Interfaces）]** を選択します。

ステップ 10 **[インターフェイスの管理（Manage Interfaces）]** ウィンドウで、**[追加（Add）]** アイコンをクリックして vPC を作成します。

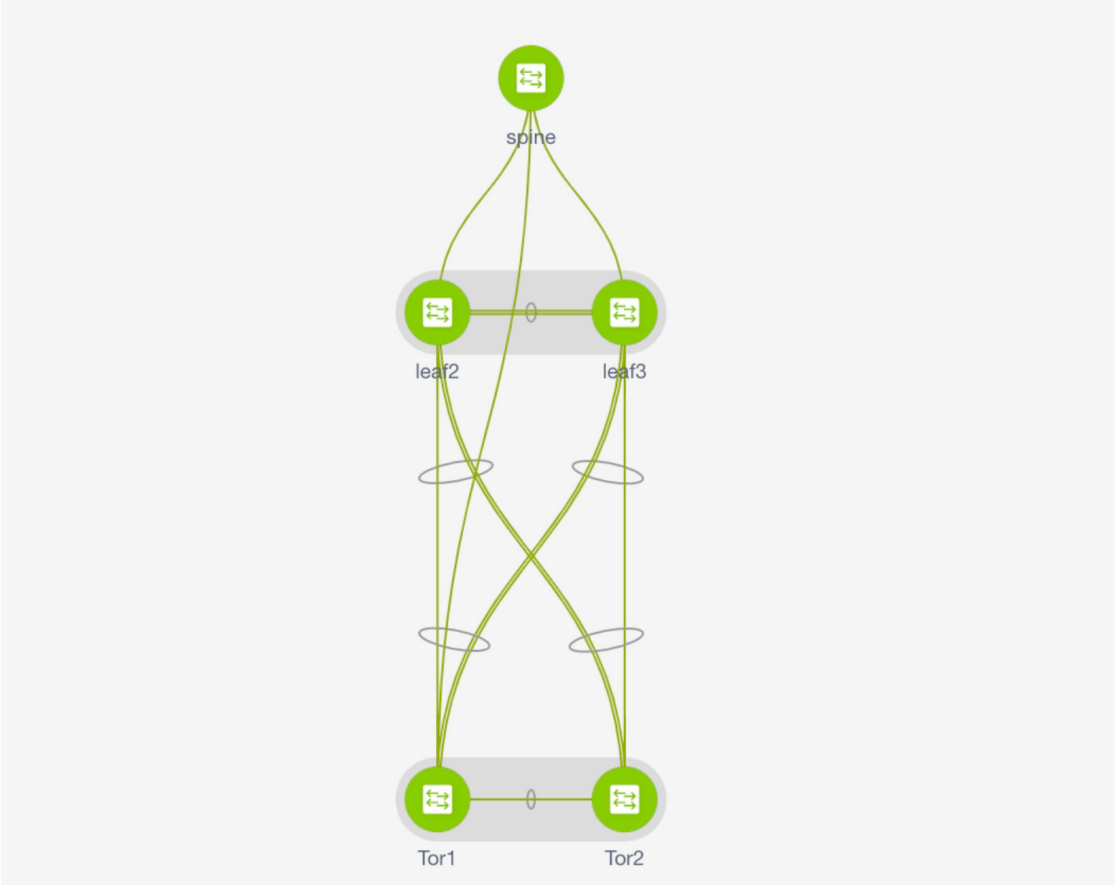
[インターフェイスの追加（Add Interface）] ウィンドウに関連するすべての詳細を入力し、**[保存（Save）]** をクリックします。



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」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、手順 9 および 10 に従って、ToR スイッチにも 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

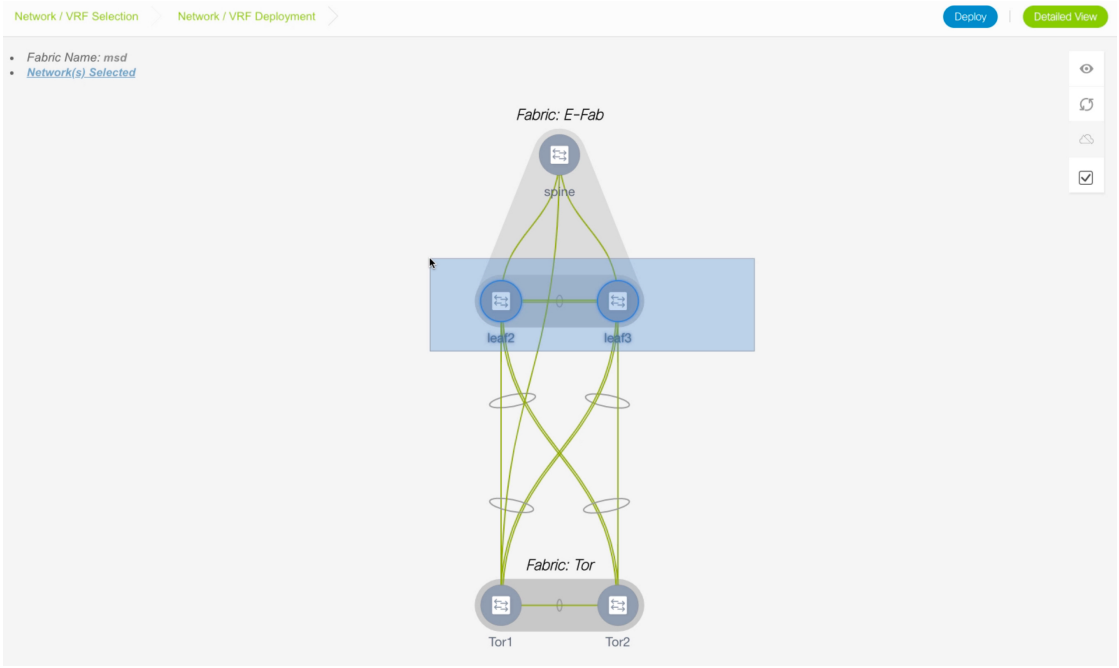
ステップ 1 **[制御（Control）] > [ネットワーク（Networks）]** に移動します。

ステップ 2 **[ネットワーク（Networks）]** ウィンドウの **[範囲（SCOPE）]** ドロップダウンリストから MSD ファブリックを選択します。

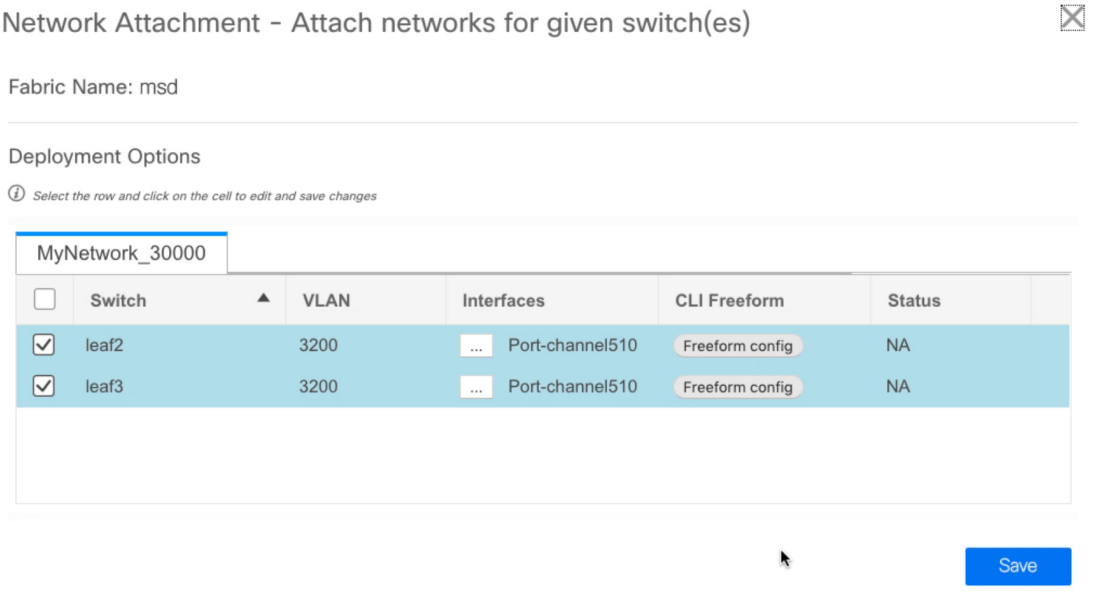
ステップ 3 展開するネットワークを選択するか、新しいネットワークを作成します。ネットワークの作成については、『*Cisco DCNM LAN* ファブリックの構成ガイド』の「スタンドアロン ファブリック向けのネットワーク作成」を参照してください。

[続行（Continue）]をクリックします。

ステップ 4 **[ネットワークの展開（Network Deployment）]** ウィンドウで、**[Multi-select]** チェック ボックスをオンにして、カーソルを Easy Fabric のリーフスイッチの上にドラッグします。



ステップ 5 **[ネットワーク アタッチメント（Network Attachment）]** ウィンドウで、**[インターフェイス（Interfaces）]** 列の **[...]** をクリックします。



[インターフェイス（Interfaces）] ウィンドウには、インターフェイスまたはポートチャネルが一覧表示されます。インターフェイス/ポートチャネルを選択して、選択したネットワークに関連付けることができます。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。

[保存（Save）] をクリックしてこのウィンドウを閉じます。

ステップ 6 **[展開（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 7 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** に移動します。

ステップ 8 MSD ファブリックをクリックし、**[保存と展開（Save & 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 6 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 III 部

VXLAN BGP EVPN ファブリックの外部/WAN レイヤ 3 接続

第 19 章

VXLAN BGP EVPN ファブリックでの VRF Lite

データセンターからの外部接続は、主要な要件です。Virtual Extensible Local Area Network（VXLAN）ボーダーゲートウェイ プロトコル（BGP）イーサネット VPN（EVPN）ベースのデータセンターファブリックは、ファブリック内のさまざまなデバイス間で IP-MAC 到達可能性の情報を配布することにより、East-West 接続を提供します。EVPN マルチサイト機能はサイト間接続を提供しますが、VRF Lite 機能はファブリックを外部レイヤ 3 ドメインに接続するために使用されます。通常、仮想ルーティングおよび転送インスタンス（VRF）によって表されるテナントは、ボーダーと呼ばれる特別なノードを介して外部接続を調達できます。このようにして、1 つのデータセンターファブリック内のテナント ワークロードは、他のファブリック内の同じ VRF 内のホストへのレイヤ 3 接続を持つことができます。この章では、VRF Lite の使用例での Cisco® Data Center Network Manager（DCNM）による Nexus 9000 ベースのボーダーデバイスの LAN ファブリック プロビジョニングについて説明します。この使用例は、VRF を外部ファブリックに拡張する方法を示しています。DCNM では、構成パラメータが次のように拡張されています。

構成メソッド：自動構成および DCNM GUI を使用して VRF Lite を構成できます。

サポートされている接続先デバイス：VRF を VXLAN ファブリックから Cisco Nexus および Nexus 以外のデバイスに拡張できます。接続されたシスコ以外のデバイスもトポロジで表すことができます。

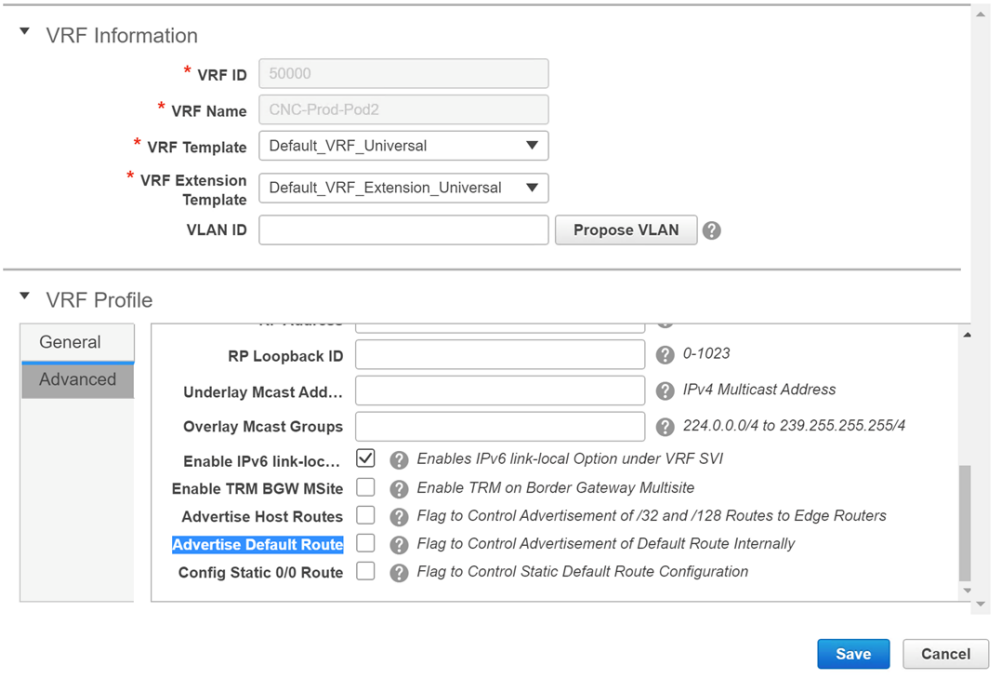
前提条件とガイドライン

前提条件

- VRF Lite 機能は、Cisco Nexus 9000 シリーズ 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 DCNM を介したトップダウン ベースの LAN ファブリック プロビジョニングに精通していること。
- 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、DCNM 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 DCNM を使用して構成できます。このドキュメントでは、DCNM 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、DCNM 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。詳細については、『Cisco DCNM LAN ファブリックの構成ガイド、リリース 11.2(1)』の**「制御」**の章を参照してください。
- 指定されたボーダー デバイスのロールが、ボーダー、ボーダー スパイン、ボーダー ゲートウェイ、またはボーダーゲートウェイ スパイン（マルチサイト機能と VRF Lite 機能が共存するスイッチ）であることを確認します。確認するには、スイッチを右クリックし、**[ロールの設定（Set role）]** をクリックします。スイッチの現在のロールに（**current**）が追加されていることがわかります。ロールがボーダーデバイスに不適切な場合は、適切なロールを設定します。
- 外部ファブリックの作成外部接続のために VLXAN ファブリック ボーダー デバイスを Nexus 7000 シリーズ スイッチ（または他の Nexus デバイス）に接続する場合、Nexus 7000 シリーズ スイッチを外部ファブリックに追加し、そのロールを **エッジ ルータ** に設定します。DCNM では、スイッチを外部ファブリックにインポートし、選択した構成を更新できます。詳細については、「制御」の章の「外部ファブリックの作成」セクションを参照してください。
- 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。Steps:

  1. ファブリックの **VRF** 画面に移動し、[VRF] を選択します。
  2. 画面の左上にある **[編集（Edit）]** オプションをクリックします。

3. **VRF の編集** 画面で、[VRF プロファイル（VRF Profile）] セクションの **[詳細（Advanced）]** をクリックします。
4. **[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して、**[保存（Save）]** をクリックします。



次のオプションは、ボーダー デバイスで VRF Lite 接続が有効になっている場合にのみ適用されます。デフォルトでは、シスコのベスト プラクティスに従って、DCNM は VRF Lite、オプション A ピアリングのサブインターフェイス上で eBGP を使用します。つまり、VRF Lite ファブリック間接続（IFC）ごとに、ボーダー デバイスから edge/WAN ルータまで、IPv4/IPv6 を介してそれぞれ確立された、VRF ごと、ピアごとの eBGP ピアリング セッションがあります。この VRF Lite ピアリングに該当するように、3 つのフィールドがあります。

- **[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。ただし、ホスト ルート（/32 または /128）を有効にして、ボーダー デバイスから edge/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 ボックスをオンにできます。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 ボックスを有効にすると、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。

- **[静的 0/0 ルートの構成（Config Static 0/0 Route）]**：このフィールドは、edge/WAN ルータへの静的 0/0 ルートをボーダーデバイスの VRF で構成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/edge 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）] フィールドも無効にする必要があります。これは、eBGP を介してアドバタイズされた 0/0 ルートが、追加の構成を必要とせずに EVPN を介してリーフに送信されるためです。この動作を行うためには、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。

リストされているオプションはすべてファブリック フィールドごとであることに注意してください。したがって、MSD を使用したマルチサイト展開では、これらのフィールドをメンバーごとのファブリック レベルで制御できます。

5. VRF Lite を介して接続された VXLAN ファブリックのボーダー デバイスに展開されたすべての VRF について、この手順に従います。

Note 新しい VRF を作成する場合は、**[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してください。

Note VRF Lite 機能の説明については、『Cisco Programmable Fabric with VXLAN BGP EVPN Configuration Guide』を参照してください。

ガイドライン

VRF-Lite IFC が作成される DCNM リリース 10.4(2) 設定では、必要なデフォルトのプレフィックス リストまたはルート マップ構成がスイッチに追加されます。この DCNM リリース 10.4(2) セットアップがいずれかの DCNM 11.x リリースにアップグレードされると、VRF-Lite 関連の RPM 構成が switch_freeform ポリシーの一部として保存される場合があります。

次のルート マップ構成は、この switch_freeform の一部です。

```
route-map EXTCON-RMAP-FILTER-V6 deny 20
match ip address prefix-list host-route-v6
```

このセットアップが DCNM リリース 11.x から 11.3(1) にアップグレードされると、ルート マップ構成は次の構成で修正されます。

```
route-map EXTCON-RMAP-FILTER-V6 deny 20
match ipv6 address prefix-list host-route-v6
```

RPM 構成は DCNM 11.x に switch_freeform として保存されるため、switch_freeformpolicy の ip prefix-list match config を手動で削除して、スイッチで ipv6 match config が成功するようにする必要があります。

サンプル シナリオ

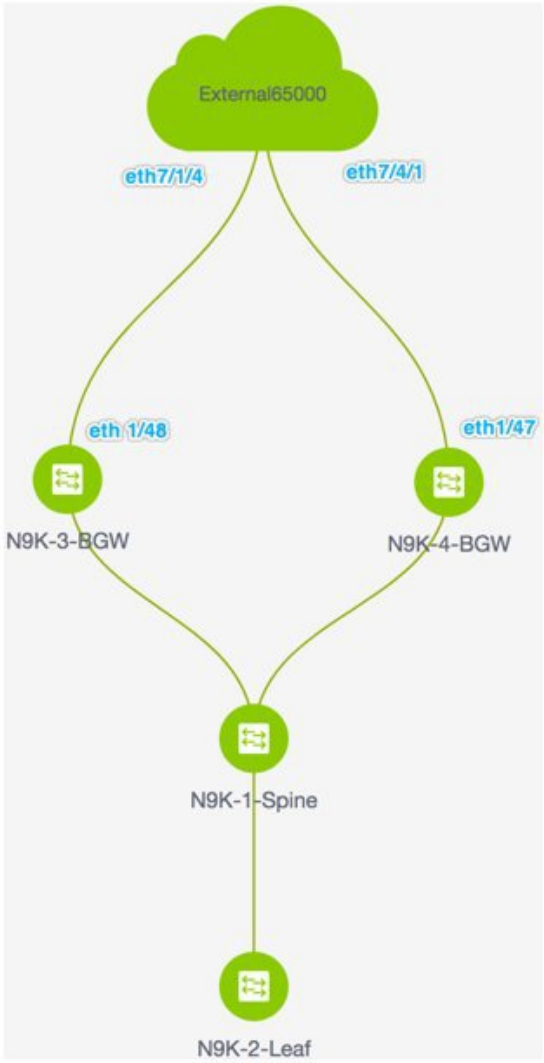
このドキュメントで説明されているシナリオ：

- DCNM GUI を介した VRF Lite – BGW デバイスから Nexus 7000 シリーズ エッジ ルータへ。
- DCNM GUI を介した VRF Lite – BGW デバイスから非 Nexus デバイスへ。
- 自動 VRF Lite（IFC）構成

Note

- サンプル シナリオは、ボーダーゲートウェイ ロールを使用して示されていますが、ボーダーノードにも同様に適用できます。
- ボーダーまたはボーダーゲートウェイのロールに適用されるものはすべて、ボーダースパインおよびボーダーゲートウェイ スパインのロールにも適用されます。

DCNM GUI を介した VRF Lite – BGW デバイスから Nexus 7000 シリーズ エッジ ルータへ



- トポロジには、外部ファブリック **External65000**（クラウドアイコン）に接続された VXLAN BGP EVPN ファブリック **Easy7200** が表示されます。VXLAN ファブリックの BGW は、外部ファブリックのエッジ ルータ **n7k1-Edge1**（画像には表示されていません）に接続されています。
- BGW は、ファブリック ドメインから外部レイヤ 3 ドメインへの明確な制御およびデータプレーンの分離を可能にするとともに、ファブリック間トラフィックのポリシー適用ポイントを可能にする特別なデバイスです。VXLAN ファブリックのネットワーク構成は、DCNM を介してプロビジョニングされます。ファブリック内のリーフスイッチに接続され

たホストからの外部レイヤ 3 到達可能性については、ボーダー デバイスを適切な VRF 構成でプロビジョニングする必要があります。ファブリック内の複数のボーダーデバイスにより、障害が発生した場合の冗長性と効果的な負荷分散が保証されます。このドキュメントでは、VXLAN ファブリックと外部ファブリックの間でレイヤ 3 North-South トラフィックを有効にする方法を示します。

- VRF Lite 構成の前に、特定の VRF に関連付けられたエンド ホストは、ファブリック内でのみトラフィックを相互に送信できます。VRF Lite 構成後、エンドホストは VXLAN ファブリックの外部にトラフィックを送信し、他の（VXLAN またはクラシック LAN）ファブリックに向けて送信できます。

VRF Lite 機能の有効化

この例では、Easy7200 と External65000 間の接続を有効にします。ステップ：

ステップ 1：**N9K-3-BGW および N9K-4-BGW の物理インターフェイスに IFC プロトタイプを展開します。**

ステップ 2：BGW **N9K-3-BGW** および **N9K-4-BGW** で個々の VRF 拡張を展開します。

ステップ 3：エッジ ルータ **n7k1-Edge1** に VRF 拡張を展開します。

3 番目のステップは、**Easy7200** と **External65000** 間の構成を完了します。

ステップ 1：N9K-3-BGW および N9K-4-BGW の物理インターフェイスに IFC プロトタイプを展開する

VRF Lite 構成では、ポイントツーポイント接続を介して、ファブリックの BGW 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 eBGP ピアリングを有効にする必要があります。BGW の物理インターフェイスは次のとおりです。

- **N9K-3-BGW** の **eth 1/48**、**n7k1-Edge1** の **eth 7/1/4** に向けられたもの。
- **N9K-4-BGW** の **eth 1/47**、**n7k1-Edge1** の **eth 7/4/1** に向けられたもの。

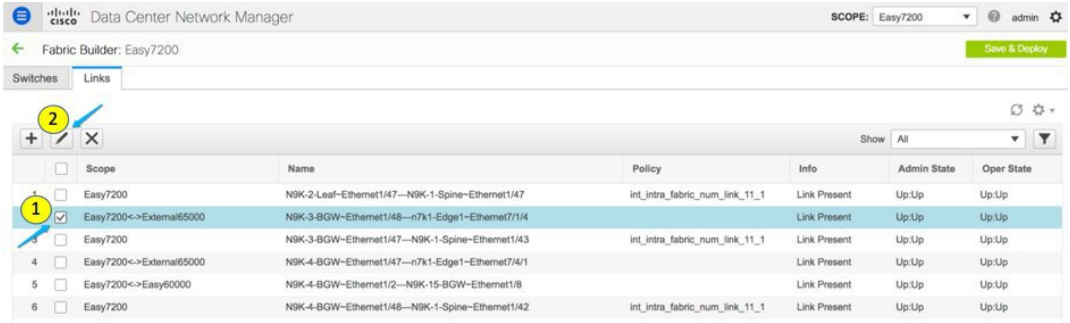
Note また、ボーダー/ボーダーゲートウェイが相互に直接接続されているバックツーバック トポロジで VRF Lite を有効にすることもできます。 VRF Lite は、物理イーサネット インターフェイスまたはレイヤ 3 ポートチャネルで有効にできます。物理インターフェイスまたはレイヤ 3 ポートチャネル インターフェイス上のサブインターフェイスは、VRF が拡張される各 VRF Lite リンクの VRF 拡張時に DCNM によって作成されます。

1. **[制御（Control）] > [Fabric Builder]**の順にクリックします。[Fabric Builder] 画面が表示されます。
2. **Easy7200** ボックスをクリックします。ファブリック トポロジが起動します。
3. **[表形式ビュー（Tabular view）]** をクリックします。**スイッチ | リンク** 画面が表示されます。

[リンク（Links）] タブには、ファブリック リンクが一覧表示されます。各行は、**Easy7200** 内の 2 つのデバイス間のリンク、または **Easy7200** 内のデバイスから外部ファブリックへのリンクを表します。

Note ファブリック間リンクは、2 つのイーサネット インターフェイス間の物理接続または仮想接続（2 つのループバック インターフェイス間のファブリック オーバーレイなど）です。デバイス間に物理接続を追加すると、デフォルトで新しいリンクが **[リンク（Links）]** タブに表示されます。

4. [リンク（link）] チェックボックス（**N9K-3-BGW** の **eth 1/48** 間の接続、**n7k1-Edge1** の **eth 7/1/4** への接続を表します）を選択し、画面の左上部分にある [編集（Edit）] アイコンをクリックします。



該当するフィールドは次のとおりです。

[範囲（Scope）]：送信元と接続先のファブリックが表示されます。ファブリック内リンクの場合、送信元インターフェイスと接続先インターフェイスが同じファブリックの一部であるため、1 つのファブリック名 (**Easy7200**) のみが表示されます。ファブリック間のリンクは、**Easy7200 <->External65000** として表示されます。

[名前（Name）]：名前は次の構文で形成されます。

*[*送信元デバイス ~ 送信元インターフェイス **---** 接続先デバイス ~ 接続先インターフェイス

したがって、エントリは **N9K-4-BGW ~ Ethernet1/47 --- n7k1-Edge1 ~ Ethernet7/4/1** です。

[ポリシー（Policy）]：VRF Lite の作成に使用されるポリシー、ext_fabric_setup_11_1 が表示されます。

[情報（Info）]：リンクのステータスを表示します（リンクあり、ネイバーあり、ネイバーが欠落、など）。

[管理ステート（Admin State）]：リンクの管理状態を表示します（アップ、ダウン、など）。

[運用ステート（Oper State）]：リンクの運用状態を表示します（アップ、ダウン、など）。

[リンク管理：リンクの編集（Link Management – Edit Link）] が表示されます。

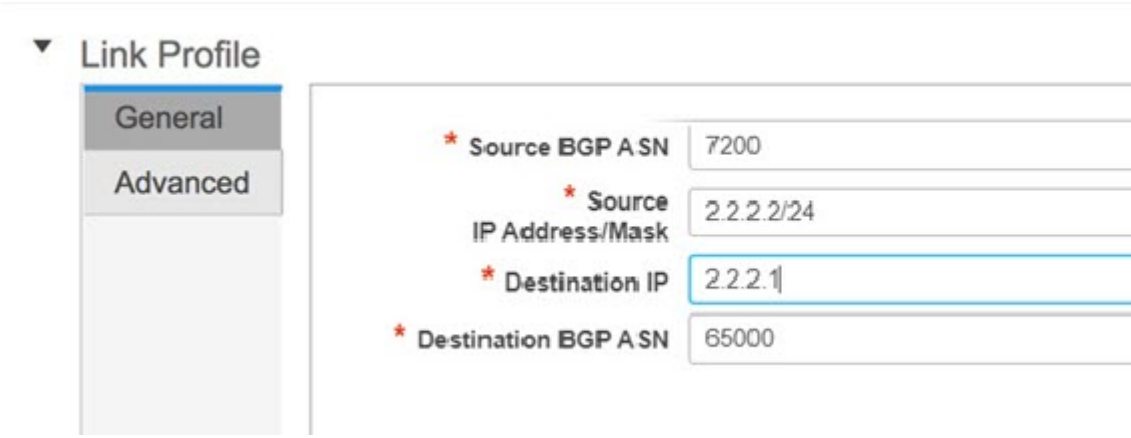
いくつかのフィールドについて説明します。

[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_11_1** 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。

ext_fabric_setup_11_1 テンプレートを編集するか、カスタム構成で新しいテンプレートを作成できます。

[全般（General）] タブには、**Easy7200** と **External65000** の BGP AS 番号が表示されます。説明のように他のフィールドに入力します。



IP アドレス/マスク：IP アドレスプレフィックスを入力して、IFC の送信元インターフェイスである**イーサネット 1/48** サブ インターフェイスに IP アドレスを割り当てます。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 2 は VRF 50000 トラフィックのサブインターフェイス Eth 1/48.2 に関連付けられ、802.1Q ID 3 は Eth 1/48.3 および VRF 50001に関連付けられます。以下も同様です。

（VRF 拡張の展開については、後続のセクションで説明します）。

IP プレフィックスは、DCNM 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。

BGP ネイバー IP：**N9K-3_BGW** 側で、この IFC に展開された各 VRF 拡張の eBGP ネイバーの IP アドレスを入力します。

IFC の VRF からのファブリック間トラフィックは、同じ送信元 IP アドレス（**2.2.2.2/24**）と宛先 IP アドレス（**2.2.2.1**）を持ちます。

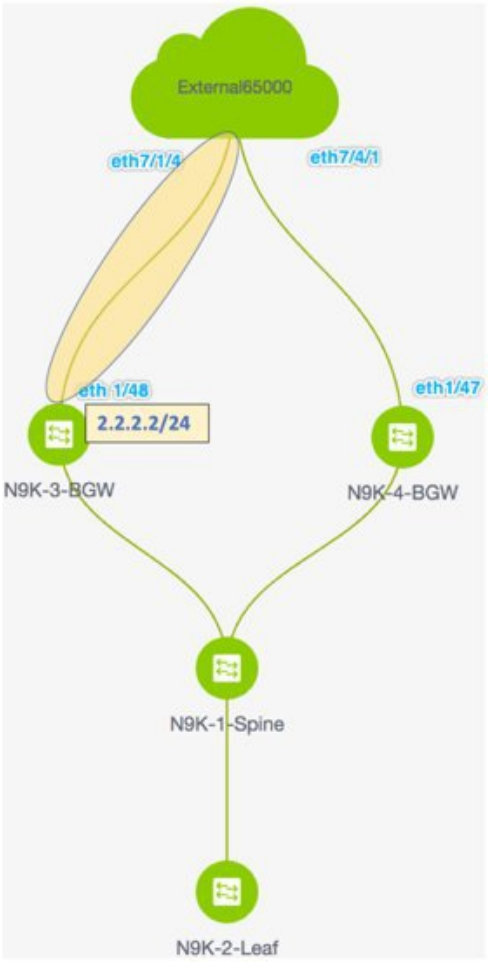
[詳細（Advanced）] タブが **[リンク プロファイル（Link Profile）]** セクションに追加されます。

このタブには、次のフィールドがあります。

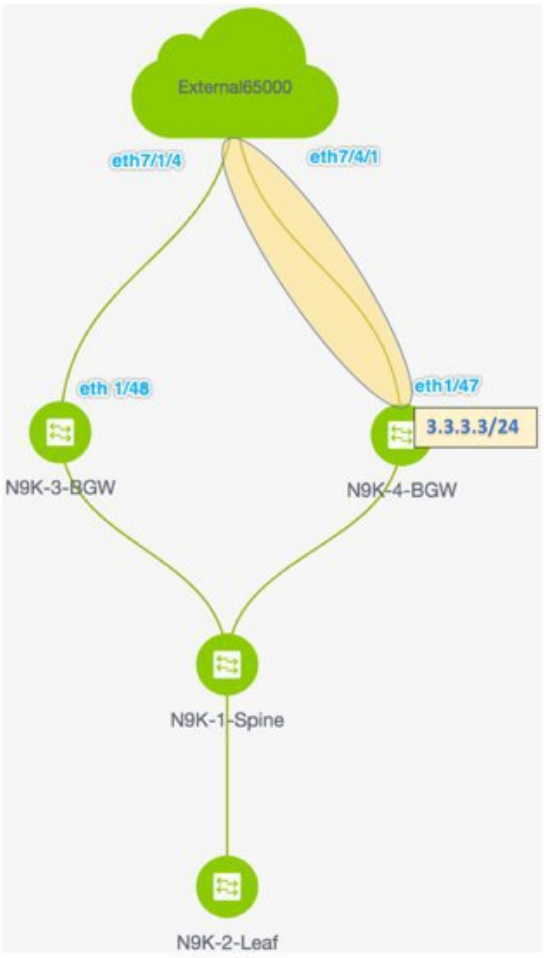
- **[送信元インターフェイスの説明（Source Interface Description）]**
- **[接続先インターフェイスの説明（Destination Interface Description）]**
- **[送信元インターフェイスのフリーフォーム構成（Source Interface Freeform Config）]**
- **[宛先インターフェイスのフリーフォーム構成（Destination Interface Freeform Config）]**

5. 画面の下部にある **[保存（Save）]** をクリックします。

   スイッチ|リンク 画面が再び表示されます。IFC エントリが、IFC の作成に使用された VRF Lite ポリシーテンプレート **ext_fabric_setup_11_1** で更新されていることがわかります。トポロジの表現を以下に示します。

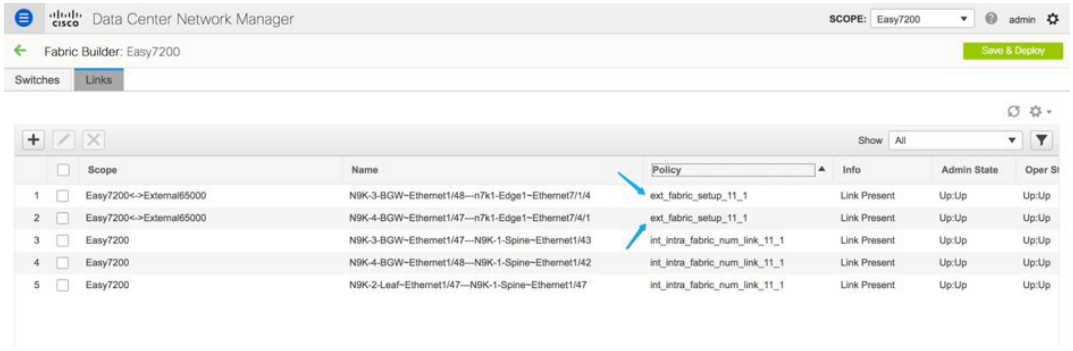


6. 同様に、**N9K-4-BGW** の **eth 1/47** から **n7k1-Edge1** の **eth 7/4/1** に向かう IFC を作成します。**[リンク（Links）]** 画面にエントリが表示されます。トポロジの表現を以下に示します。



7. 画面の右上にある **[保存して展開（Save and Deploy）]** をクリックします。

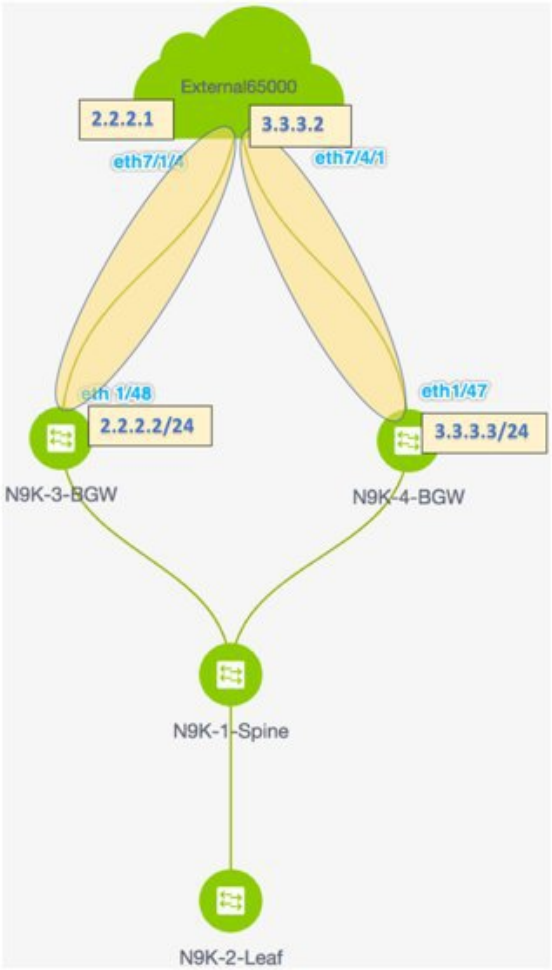
   [保存して展開（Save and Deploy）] を実行した後の **[リンク（Links）]** タブは次のようになります。IFC が展開されるリンクには、**[ポリシー（Policy）]** 列で構成済みの関連するポリシーがあります。



8. 画面の右上にある **[範囲（Scope）]** ドロップダウンリストへ移動し、**External65000** を選択します。外部ファブリック **[リンク（Links）]** 画面が表示されます。ここでは、**Easy7200** から **External65000** へ作成された 2 つの IFC が表示されていることが確認できます。

Note VXLAN ファブリックで IFC を作成するか、その設定を編集すると、接続された外部ファブリックに対応するエントリが自動的に作成されます。

9. **[保存して展開（Save and Deploy）]** をクリックして、IFC の作成を **External65000** に保存します。



基本設定：VRF Lite が機能するには、VRF に適用される適切なルート マップとポリシーをボーダー デバイス **N9K-3-BGW** および **N9K-4-BGW** に展開する必要があります。基本構成を手動で有効にする必要はありません。これらは、デフォルトのテンプレート **ext_base_border_vrflite_11_1** を介して自動的に展開されます。

ボーダー リーフまたはボーダー スパイン ロールを持つデバイスの場合、基本構成は、**[保存および展開（Save and Deploy）]操作]**（ファブリック トポロジ画面で **[ファブリック ビ**

ルダ（**Fabric Builder**）**]** 画面 > [ファブリック ボックス（Fabric Box）] で利用可能）をファブリックで初めて実行したときに展開されます。

ボーダーゲートウェイまたはボーダーゲートウェイ スパイン ロールの場合、基本構成は、デバイスに最初の VRF Lite IFC を展開するときに展開されます。

展開する前に、特定のニーズに合わせて **ext_base_border_vrflite_11_1** テンプレートを変更する必要があります。または、そのポリシーを削除し、テンプレートを変更してから、テンプレートを再度展開する必要があります。構成は、**[付録（Appendix）]** セクションに記載されています。

VRF Lite 構成シナリオの最初の手順である、ボーダー デバイスとエッジ ルータでの IFC の作成は完了です。次に、VRF 拡張がスイッチに展開されます。

ステップ 1： **N9K-3-BGW** および **N9K-4-BGW** の物理インターフェイスに IFC プロトタイプを展開します。

ステップ 2：**BGW N9K-3-BGW および N9K-4-BGW で個々の VRF 拡張を展開します。**

ステップ 3：エッジ ルータ **n7k1-Edge1** に VRF 拡張を展開します。

3 番目のステップは、**Easy7200** と **External65000** 間の構成を完了します。

ステップ 2：**BGW N9K-3-BGW および N9K-4-BGW で個々の VRF 拡張を展開します。**

IFC 作成プロセス中に、基本構成が作成され、**N9K-3-BGW** および **N9K-4-BGW** でファブリック間トラフィックを転送するインターフェイス用に IP アドレスが予約されます。この手順では、VRF および VRF 拡張構成がインターフェイスに展開されます。

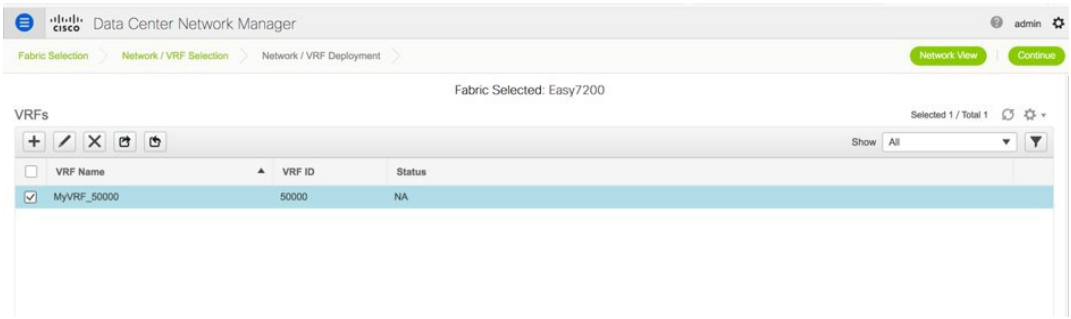
ファブリックを超えて VRF を拡張するには、VRF が作成され、ボーダー デバイスを除く関連するファブリック デバイスに展開されている必要があります。

この手順は次のとおりです。

1. **[制御（Control）] > [ネットワークと VRF（Networks and VRFs）]** をクリックします。**[ネットワークと VRF（Networks & VRFs）]** 画面が表示されます。
2. **[続行（Continue）]**をクリックします。**[ファブリックの選択（Select a Fabric）]** 画面が表示されます。
3. **Easy7200** を選択し、画面右上の **[続行（Continue）]** をクリックします。

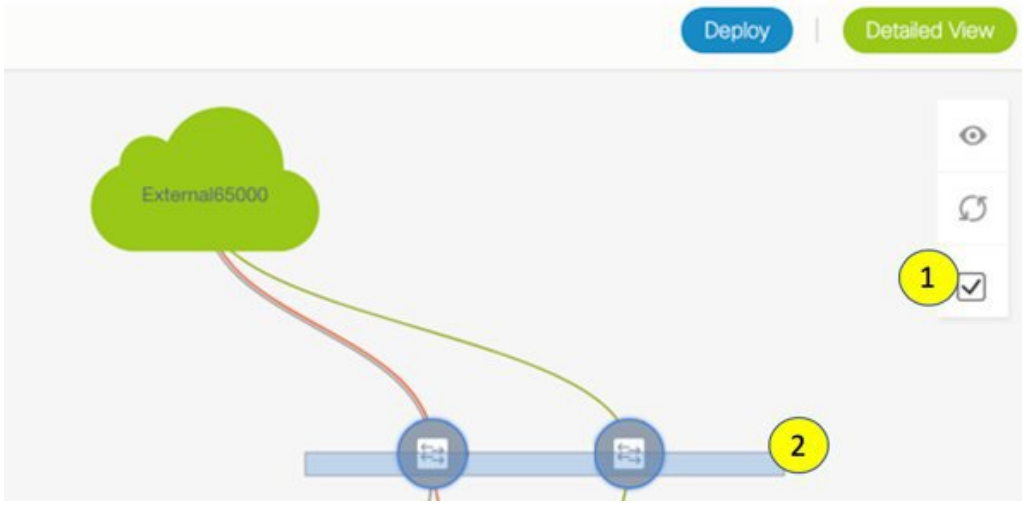
[ネットワーク（Networks）] 画面が表示されます。

4. 画面右上の **[VRF]** をクリックします。**[VRF]** 画面が表示されます。
5. 展開する VRF（この場合は **MyVRF_5000**）を選択し、画面の右上にある **[続行（Continue）]** をクリックします。

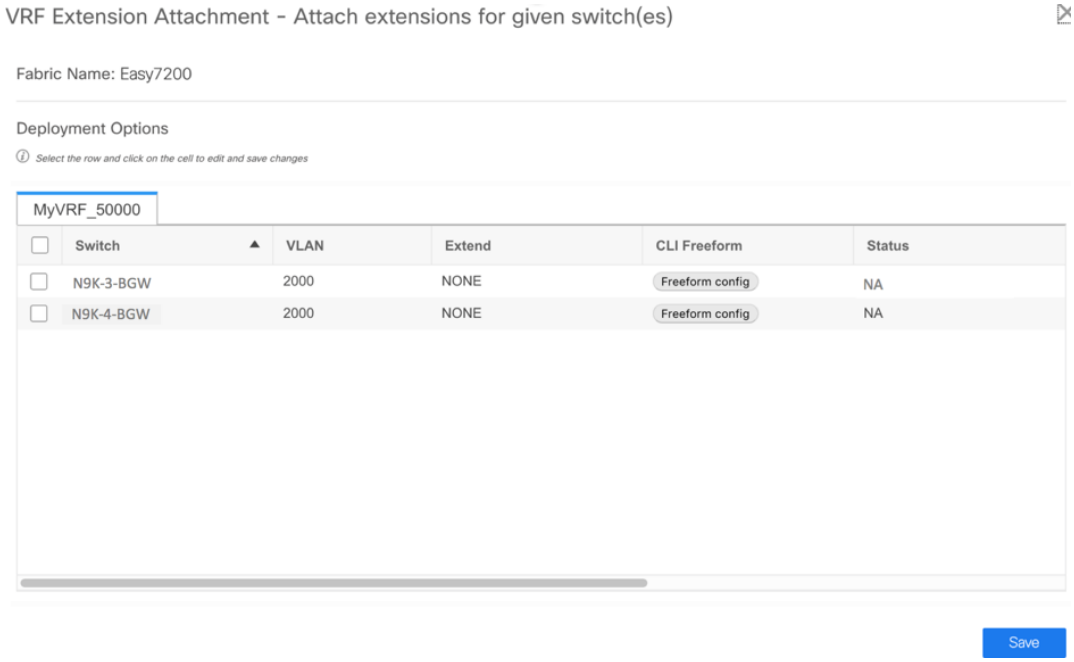


Easy7200 ファブリック トポロジが起動します。

6. 画面の右上にある **[複数選択（Multi-Select）]** チェックボックスを選択し、VRF および VRF 拡張構成を展開する BGW 全体にカーソルをドラッグします。



[VRF 拡張アタッチメント（VRF Extension Attachment）] 画面が表示されます。各行はスイッチを表し、各タブは VRF を表します。説明に従って各タブの設定を更新します。



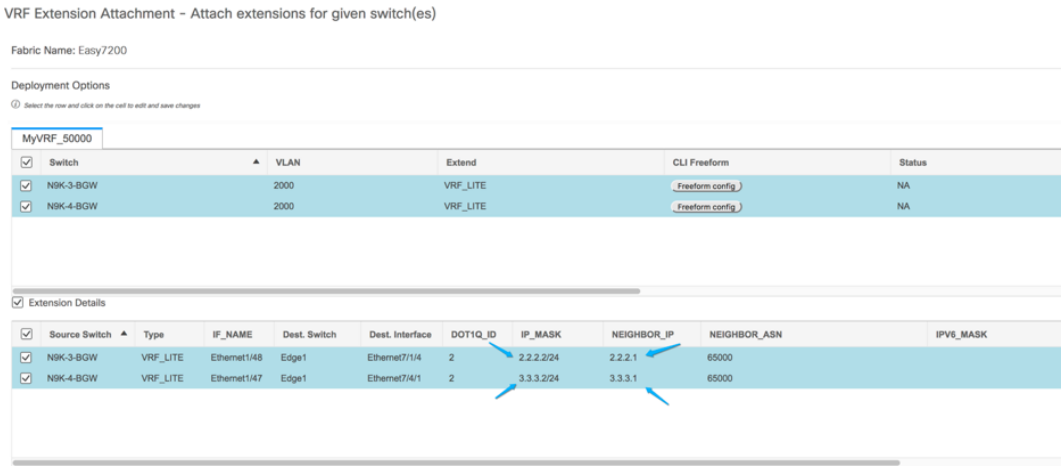
[拡張（Extend）] 列で、**[なし（NONE）]** をクリックし、ドロップダウンボックスから **[VRF_LITE]** オプションを選択します。これを 2 列目も行います。

両方の行のチェックボックスをオンにします。

画面の下部に **[拡張機能の詳細（Extension Details）]** セクションが表示されます。選択したスイッチで作成された IFC が表示されます。各行は IFC を表します。

両方の行の IFC チェックボックスをオンにします。

IFC を選択すると、画面は次のようになります。



DCNM は、DOT1Q_IP、IP_MASK、および NEIGHBOR_IP フィールドの値を使用して、上記の VRF-LITE リンクごとに 1 つのサブインターフェイスを作成します。各 VRF LITE 拡張の IP_MASK および NEIGHBOR_IP フィールドには、VRF LITE リンク作成で入力された **IP アドレス/マスク** および **BGP ネイバー IP** 値が入力されます。IP_MASK および NEIGHBOR_IP フィールドは、DOT1Q_ID フィールドとともに上書きできます。サブインターフェイスを介した IPv6 eBGP セッションが必要な場合は、オプションで IPV6_MASK および NEIGHBOR_IPV6 フィールドを入力できます。

画面の下部にある **[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。

7. 画面の右上にある **[プレビュー（Preview）]** オプションをクリックして、VRF および VRF 拡張構成をプレビューします。

8. 画面の右上にある **[展開（Deploy）]** をクリックします。

   画面の右下に、展開のさまざまな段階を表すカラー コードが表示されます。それに応じて、スイッチアイコンの色が変わります（保留中の状態は青色、プロビジョニングが進行中の場合は黄色、失敗状態の場合は赤色、正常に展開された場合は緑色です）。

   スイッチ アイコンが緑色に変わったら、VRF が正常に展開されたことを意味します。

VRF Lite 構成シナリオの 2 番目のステップである、ボーダー デバイスへの VRF 拡張の展開は完了です。次に、VRF 拡張がエッジ ルータ **n7k1-Edge1** に展開されます。

ステップ 1： **N9K-3-BGW** および **N9K-4-BGW** の物理インターフェイスに IFC プロトタイプを展開します。

ステップ 2：BGW **N9K-3-BGW** および **N9K-4-BGW** で個々の VRF 拡張を展開します。

ステップ 3：エッジ ルータ **n7k1-Edge1** に VRF 拡張を展開します。

3 番目のステップは、**Easy7200** と **External65000** 間の構成を完了します。

ステップ 3：エッジ ルータ **n7k1-Edge1** に VRF 拡張を展開します。

エッジ ルータで VRF を拡張するには、次のフィールドに注意してください。ボーダー デバイスの VRF 拡張は、インターフェイスごとに行われます。

- **[IP_MASK]**：これはエッジ ルータ エンドのネイバー アドレスになり、マスクはエッジ ルータのローカル マスクになります。これは、前の手順で作成した IFC プロトタイプから派生したものです。
- **[Easy Fabric ASN]**：これは、エッジ ルータ側からのネイバー ASN になります。これは、前の手順で作成した IFC プロトタイプから派生したものです。
- **[Dot1Q タグ（Dot1Q tag）]**：これはエッジ ルータでも同じです。これは、VRF 拡張テーブルから取得されます。
- **[ネイバー ASN（Neighbor ASN）]**：これはエッジルータのローカル ASN になります。IFC プロトタイプ
- **[ネイバー IP（Neighbor IP）]**：これはエッジ ルータのサブインターフェイスのローカル IP になります。IFC プロトタイプ
- **[宛て先ポート（Destination port）]**：拡張機能が展開されるエッジ ルーターのローカル ポートになります。

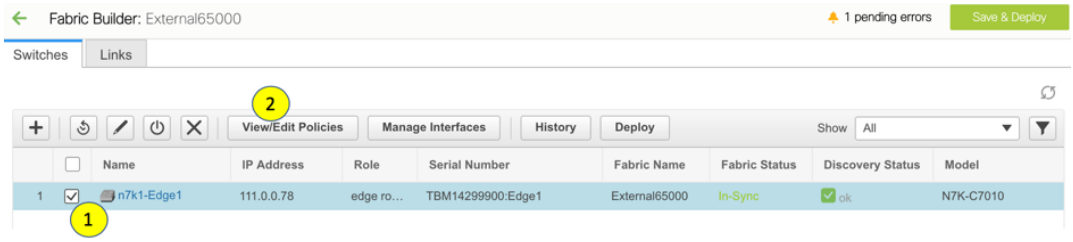
BGW **N9K-3-BGW** および **N9K-4-BGW** から **MyVRF_50000** の VRF 拡張を展開しました。ここで、**n7k1-Edge1** のリンクのもう一方の端に VRF 拡張を展開する必要があります。DCNM では、これに使用される CLI テンプレートは **External_VRF_Lite_eBGP** です。

エッジ ルータでの eBGP 構成

1. **[External65000]** ファブリック トポロジ画面で、**[表形式ビュー（Tabular view）]** をクリックします。

   Switches | Links 画面が表示されます。

2. スイッチのチェックボックスを選択し、**[ポリシーの表示/編集（View/Edit Policies）]** ボタンをクリックします。



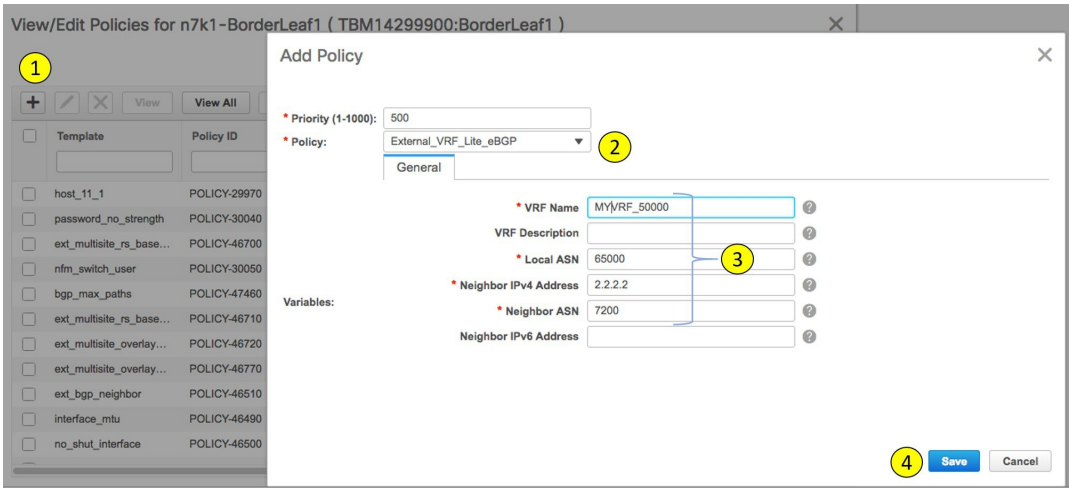
   [ポリシーの表示/編集（View/edit policies）] 画面が表示されます。

3. 画面の左上部分にある **[+]** をクリックしてポリシーを追加し、イメージに示すように **[ポリシーの追加（Add Policy）]** 画面に入力します。

   [ポリシー（Policy）] フィールドでは、ユーザー定義のテンプレートも使用できます。

Note この VRF 拡張のポリシー ID に注意してください。ポリシーを削除して拡張機能を削除する場合に便利です（該当する場合）。

これにより、エッジ ルータから **N9K-3-BGW** へのポリシーが定義されます。



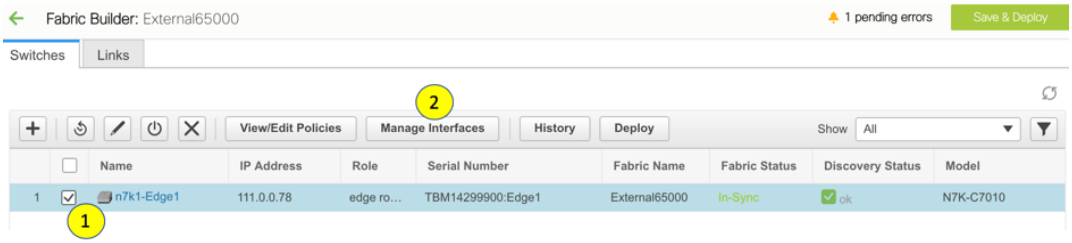
4. 前の手順に従って、**N9K-4-BGW** に対する VRF 拡張のポリシーを作成します。2 番目の拡張機能の **ネイバー IPv4 アドレス** フィールドは、3.3.3.3 で更新されます。

エッジ ルータのサブ インターフェイス ポリシー

1. **[External65000]** ファブリック トポロジ画面で、**[表形式ビュー（Tabular view）]** をクリックします。

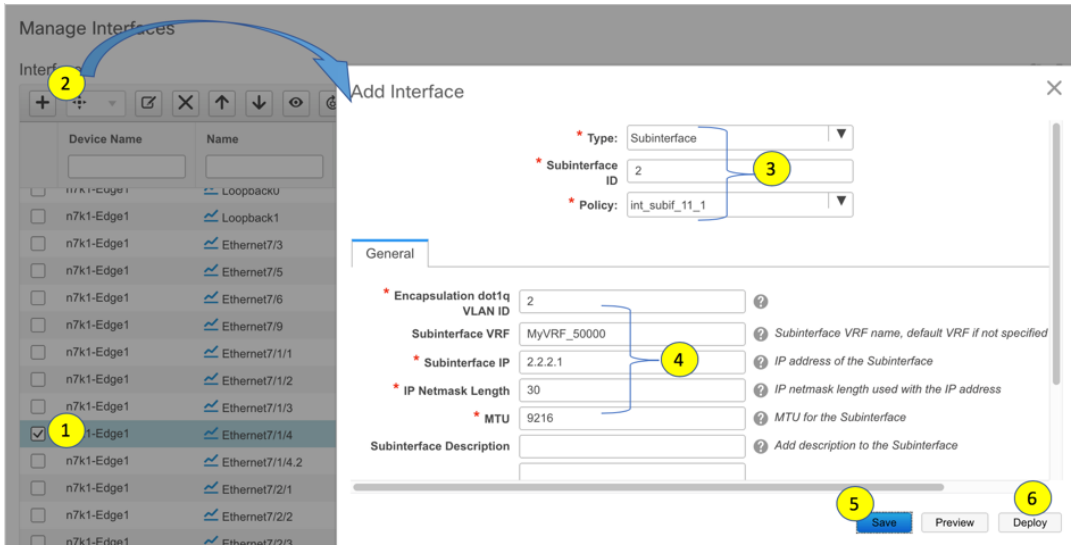
   スイッチ | リンク 画面が表示されます。

2. スイッチのチェックボックスを選択し、**[インターフェイスの管理（Manage Interfaces）]** ボタンをクリックします。



   [インターフェイスの管理（Manage Interfaces）] 画面が表示されます。

3. 画像に示すように、ボーダー デバイス（この場合は **Eth7/1/4**）に接続されているインターフェイスを選択し、画面の左上部分にある **[+]** をクリックします。次に、ボーダー デバイスの対応する IFC および VRF 拡張機能から **[インターフェイスの追加（Add Interface）]** 画面に入力します。



この例は、Cisco Nexus 7000 シリーズ スイッチのブレークアウト ポートを示しています。このブレークアウトは、DCNM ブレークアウト ポリシーを使用して実行する必要があります（テンプレート名は**breakout_interface** です）。これを行わないと、サブインターフェイスの削除は DCNM によってブロックされます。

4. **[保存（Save）]** をクリックして設定を保存し、**[展開（Deploy）]** をクリックして設定をスイッチに展開します。
5. 前の手順の説明に従って、**N9K-4-BGW** への VRF 拡張用に別のサブインターフェイス ポリシーを作成します。2 番目の拡張の **[サブインターフェイス IP（Subinterface IP）]** フィールドは、3.3.3.1 で更新されます。

VRF Lite 構成シナリオの 3 番目のステップである、エッジ ルータ **N7k1-Edge1** での VRF 拡張の展開は完了です。このステップで、**Easy7200** と **External65000** 間の構成が完了します。

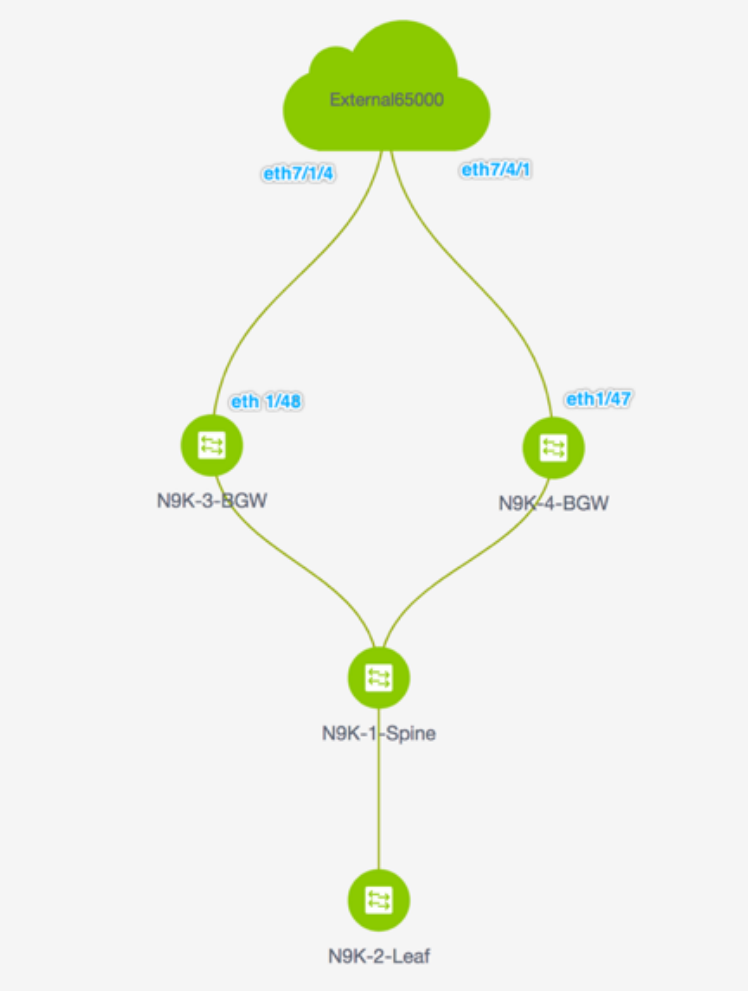
DCNM GUI を介した VRF Lite：BGW デバイスから非 Nexus デバイス

この場合、非 Nexus デバイスは、**Easy7200** ファブリックの BGW **N9K-3-BGW** に接続された ASR 9000 シリーズ ルータ、**ASR9K-1-Edge** です。ルータは DCNM 経由でインポートされず、CDP または LLDP 経由で検出されません。非 Nexus デバイスを表すには、外部ファブリックを作成する必要があります。外部ファブリックの作成方法については、**外部ファブリックの作成** のトピックを参照してください。この例では、外部ファブリック **External65000** が作成されます。

デバイスと接続は、**ASR9K-1-Edge** と **N9K-3-BGW** 間の IFC 作成後に DCNM トポロジに表示されます。

Note 接続されたシスコ以外のデバイスもトポロジで表すことができます。

トポロジ：



この手順は次のとおりです。

手順 1：**ASR9K-1-Edge** に接続する **N9K-3-BGW** 物理インターフェイスに **IFC** プロトタイプを展開します。

手順 2：**N9K-3-BGW** で個々の **VRF** 拡張を展開します。

この手順で、**Easy7200** と非 Nexus デバイス間の構成が完了します。

手順 1：**ASR9K-1-Edge** に接続する **N9K-3-BGW** 物理インターフェイスに **IFC** プロトタイプを展開します。

VRF Lite 構成では、ポイントツーポイント リンクを介して、ファブリックの BGW インターフェイスと **ASR9K-1-Edge** インターフェイス間の eBGP ピアリングを有効にする必要があります。

1. **[制御（Control）] > [Fabric Builder]**の順にクリックします。**ファブリック ビルダ** 画面が表示されます。
2. **Easy7200** ファブリックを表す長方形のボックスをクリックします。[ファブリック トポロジ (fabric topology)] 画面が表示されます。
3. **[表形式ビュー（Tabular view）]** をクリックします。**スイッチ | リンク** 画面が表示されます。

   [リンク（Links）] タブには、ファブリック リンクが一覧表示されます。各行は、**Easy7200** 内の 2 つのデバイス間のリンク、または **Easy7200** 内のデバイスから外部ファブリックへのリンクを表します。
4. **[+]** をクリックして新しいリンクを追加します。**リンク管理**：**リンクを追加** 画面が表示されます。

記載されているようにフィールドを入力または選択します。

リンク タイプ：**[ファブリック間（Inter-Fabric）]** を選択します。

リンク サブタイプ：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：デフォルトでは、**ext_fabric_setup_11_1** テンプレートが設定されています。

Note ユーザ定義テンプレートを追加、編集、削除できます。詳細については、「**制御**」の章の「**テンプレート ライブラリ**」のセクションを参照してください。

送信元ファブリック：**Easy7200** がデフォルトで選択されています。

接続先ファブリック：**[External65000]** 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**：ASR デバイスに接続する BGW とインターフェイスを選択します。

接続先デバイス と **接続先インターフェイス**：接続先デバイスと接続先インターフェイスはドロップダウンボックスに表示されません。デバイスの識別に役立つ文字列をここに入力します。この名前は、**ファブリック ビルダ**画面の外部ファブリック トポロジ画面に表示されます。

[リンク プロファイル] セクションの [全般] タブ。

BGP ローカル ASN：このフィールドには、送信元ファブリック Easy7200 の AS 番号が自動入力されます。

IP アドレス/マスク：VRF 拡張サブインターフェイスで使用される IP アドレスとマスクを入力します。

BGP ネイバー IP：VRF 拡張のローカルインターフェイスアドレスとして [外部（External）] ボックスで使用される IP アドレスを入力します。

BGP ネイバー ASN：このフィールドでは、外部ファブリックとして選択したため、外部ファブリック External65000 の AS 番号が自動入力されます。

[リンクの追加（Add Link）] 画面に入力すると、次のようになります。

5. 画面の下部にある **[保存（Save）]** をクリックします。

   スイッチ | リンク 画面が再び表示されます。IFC エントリがアップデートされることを確認できます。

6. 画面の右上にある **[保存して展開（Save and Deploy）]** をクリックします。

IFC が展開されるリンクには、**ポリシー** 列で構成済みの関連するポリシー（**ext_fabric_setup_11_1**）があります。

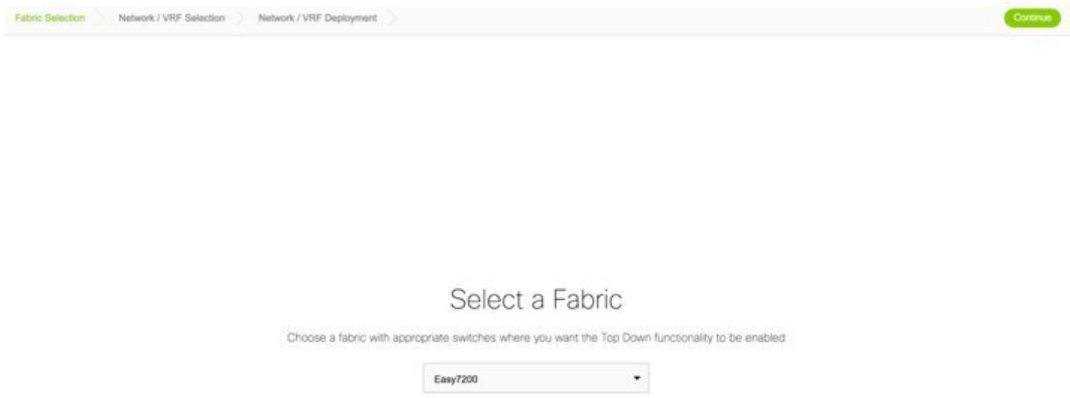
7. 画面の右上にある **[範囲（Scope）]** ドロップダウンリストへ移動し、**External65000** を選択します。外部ファブリック **[リンク（Links）]** 画面が表示されます。ここでは、IFC が **Easy7200** から ASR デバイスへ作成されたことを確認できます。
8. [保存して展開（Save and Deploy）] をクリックします。

BGW から非 Nexus デバイスへの VRF Lite 構成シナリオの最初の手順は完了です。次に、VRF 拡張が ASR デバイスに向けて BGW に展開されます。

手順 2：N9K-3-BGW で個々の VRF 拡張を展開します。

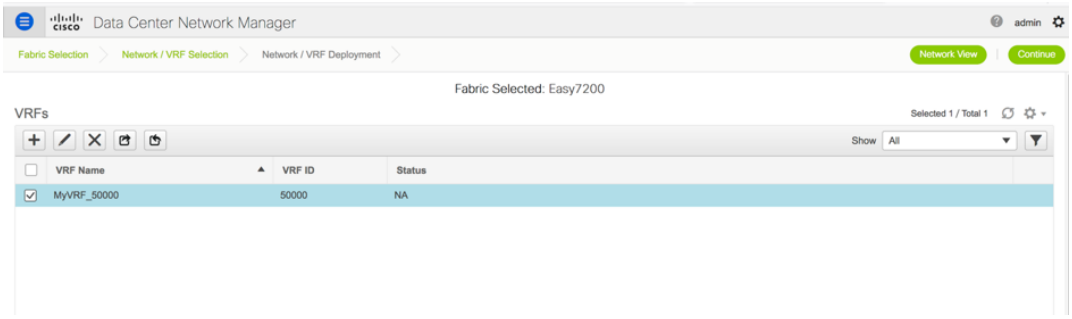
ファブリックを超えて VRF を拡張するには、VRF が作成され、ボーダー デバイスを除く関連するファブリック デバイスに展開されている必要があります。

1. **[制御（Control）] > [ネットワークと VRF（Networks and VRFs）]** をクリックします。**[ネットワークと VRF（Networks & VRFs）]** 画面が表示されます。
2. **[続行（Continue）]**をクリックします。**[ファブリックの選択（Select a Fabric）]** 画面が表示されます。
3. **Easy7200** を選択し、画面右上の **[続行（Continue）]** をクリックします。



[ネットワーク（Networks）] 画面が表示されます。

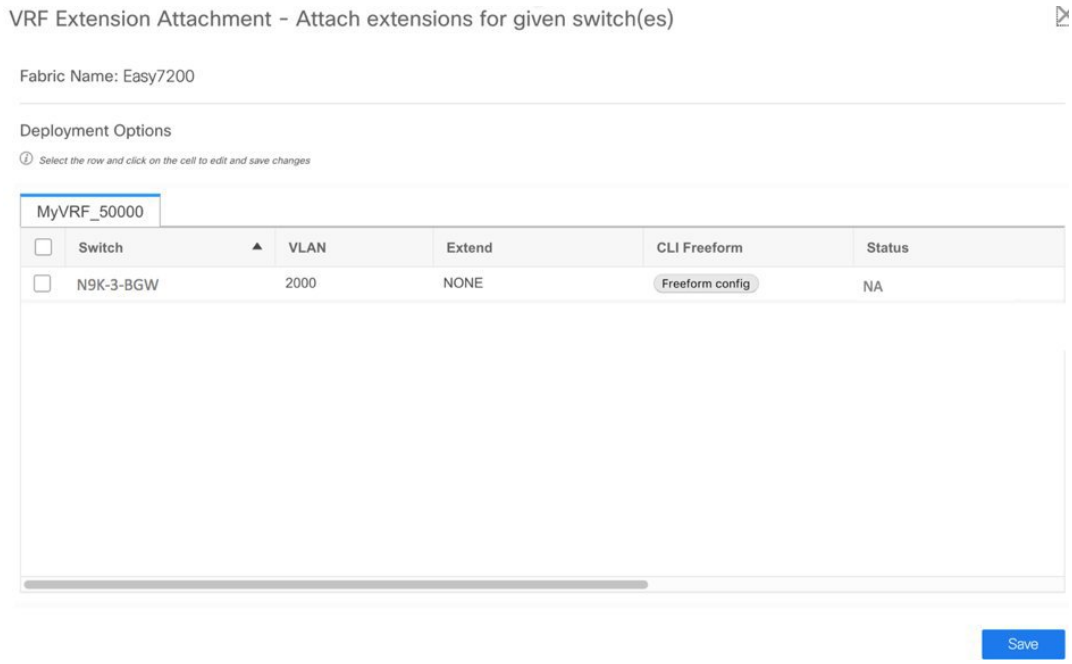
4. 画面右上の **[VRFs]** をクリックします。**[VRF]** 画面が表示されます。
5. 展開する VRF（この場合は **MyVRF_5000**）を選択し、画面の右上にある **[続行（Continue）]** をクリックします。



Easy7200 ファブリック トポロジが起動します。

6. VRF および VRF 拡張構成を展開する **N9K-3-BGW** アイコンをダブルクリックします。

[VRF 拡張アタッチメント（VRF Extension Attachment）] 画面が表示されます。各行はスイッチを表し、各タブは VRF を表します。この例では、1 つの VRF だけが拡張されています。

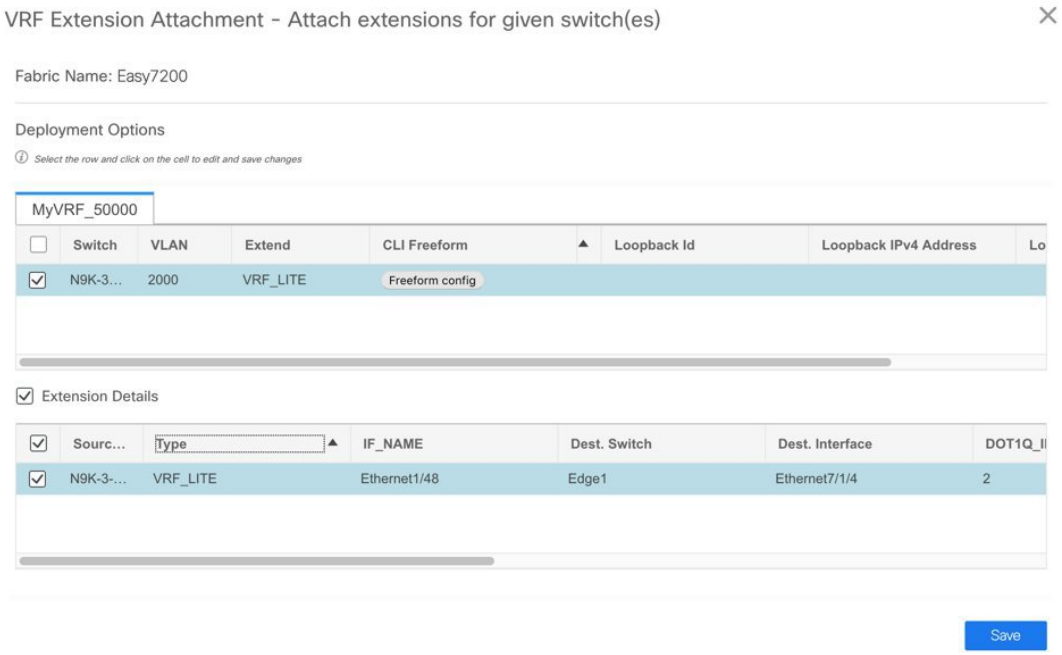


[拡張（Extend）] 列で、**[NONE]** をクリックします。ドロップダウンボックスが表示されます。**VRF_LITE** オプションを選択し、行の外側をクリックします。

スイッチの横にあるチェックボックスを選択します。

画面の下部に **[拡張機能の詳細（Extension Details）]** セクションが表示されます。選択したスイッチで作成された IFC が表示されます。各行は IFC を表します。

[IFC] チェックボックスをオンにします。IFC を選択すると、画面は次のようになります。



画面の下部にある **[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。

7. 画面の右上にある **[プレビュー（Preview）]** オプションをクリックして、VRF および VRF 拡張構成をプレビューします。

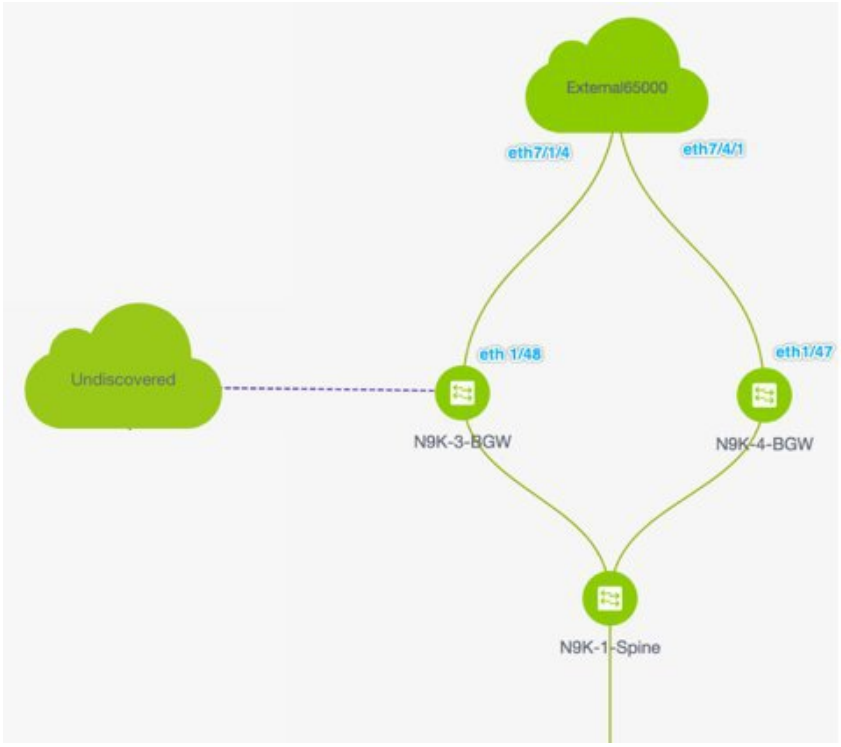
8. 画面の右上にある **[展開（Deploy）]** をクリックします。

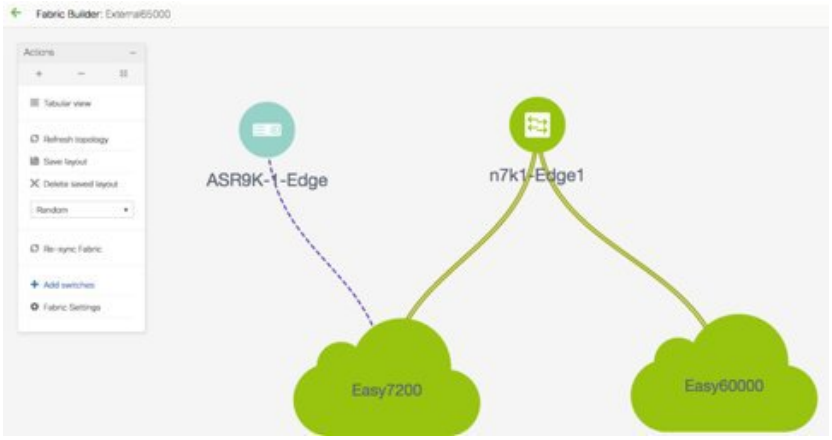
   画面の右下に、展開のさまざまな段階を表すカラー コードが表示されます。それに応じて、スイッチアイコンの色が変わります（保留中の状態は青色、プロビジョニングが進行中の場合は黄色、失敗状態の場合は赤色、正常に展開された場合は緑色、など）。

   スイッチ アイコンが緑色に変わったら、VRF が正常に展開されたことを意味します。

VRF Lite 構成シナリオの 2 番目のステップである、非 Nexus ASR デバイスに向けたボーダー デバイスでの VRF 拡張の展開は完了です。

デバイスと接続は、**Easy7200** および **External65000** ファブリックに表示されます。

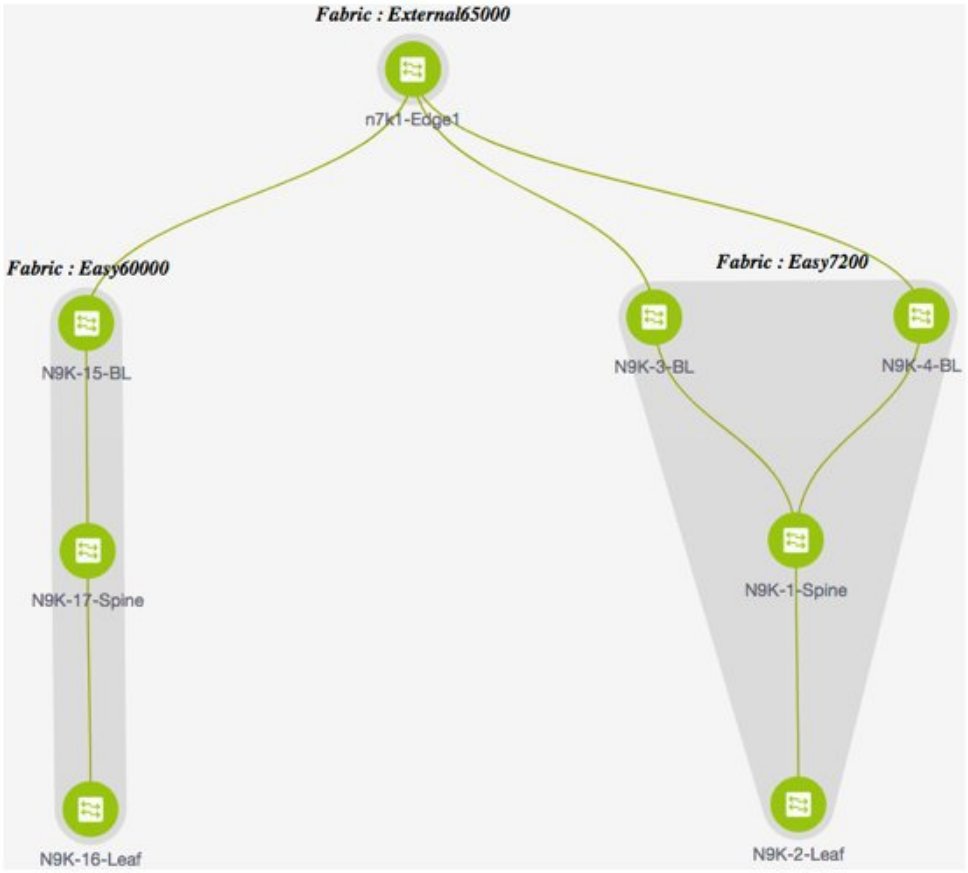




自動 VRF Lite（IFC）設定

[リソース（Resources）] タブの **[VRF Lite 展開（VRF Lite Deployment）]** フィールドのファブリック設定を **[手動（Manual）]** から任意の自動構成の設定に変更することにより、VRF Lite 自動構成を有効にすることができます。

Note **[ファブリック ビルダ（Fabric Builder）]** 内のファブリック トポロジ画面では、個々のファブリックと接続されている外部ファブリックのみを表示できます。



- トポロジには、VXLAN BGP EVPN ファブリック **Easy60000**（左側）と **Easy7200**（右側）、および外部ファブリック **External65000**（上部）が表示されます。1 つの VXLAN ファブリックのボーダー リーフは、外部ファブリックのエッジルータ **n7k1-Edge1** を介して他のボーダー リーフに接続されます。
- ボーダー リーフは、ファブリックから外部レイヤ 3 ドメインへの明確な制御およびデータプレーンの分離を可能にするとともに、ファブリック間トラフィックのポリシー適用ポイントを可能にする特別なデバイスです。ファブリック内の複数のボーダー デバイスにより、障害が発生した場合の冗長性と効果的な負荷分散が保証されます。このドキュメントでは、VXLAN ファブリックと外部ファブリックの間でレイヤ 3 North-South トラフィックを有効にする方法を示します。
- VRF Lite 構成の前に、特定の VRF に関連付けられたエンド ホストは、ファブリック内でのみトラフィックを相互に送信できます。VRF Lite 構成後、エンド ホストはファブリック間でトラフィックを送信できます。
- VXLAN ファブリックのネットワーク構成は、DCNM を介してプロビジョニングされます。

  VRF Lite IFC 自動設定に使用されるテンプレートは **ext_fabric_setup_11_1** です。**ext_fabric_setup_11_1** テンプレートを編集するか、カスタム構成で新しいテンプレートを作成できます。

自動 VRF Lite 作成ルール

- 自動 IFC は、Cisco Nexus デバイス向けにのみサポートされています。
- Cisco DCNM リリース 11.4(1) 以降、Cisco ASR 1000 シリーズ ルータおよび Cisco Catalyst 9000 シリーズ スイッチをエッジルータとして構成し、VRF-lite IFC を設定し、簡単なファブリックを使用してボーダー デバイスとして接続できます。
- 外部ファブリックのデバイスが Nexus 以外の場合は、IFC は手動で作成される必要があります。
- 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。
- 自動設定は、次の場合に提供されます。
  - 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

  自動設定は 2 つの BGW 間では提供されないことに注意してください。

  他のロール間で VRF Lite が必要な場合は、DCNM GUI を使用して手動で導入する必要があります。
- 外部ファブリックに構成を展開するには、**External65000** ファブリックの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）]** チェックボックスがオフになっていることを確認してください。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。

VRF Lite IFC の作成には 4 つのモードがあります。

1. **[手動（Manual）]**：前のセクションで示したように、GUI を使用して VRF Lite IFC を展開します。
2. **[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 ファブリックのボーダー リーフ（スパイン）デバイスの各物理インターフェイスで、VRF Lite IFC を構成します。
3. **[バック間のみ（Back to Back Only）]**：異なる VXLAN ファブリックの直接接続されたボーダー リーフ（スパイン）デバイス インターフェイス間に、VRF Lite IFC を構成します。
4. **[Back2Back&ToExternal]**：このオプションを使用して、**[外部のみ（To External Only）]** および **[バック間のみ（Back to Back Only）]** モードの IFC を構成します。

Note VRF Lite モードが **[手動（Manual）]** の場合でも、DCI サブネットが必要です。これは、DCNM リソースの処理に役立ちます。

ファブリック設定のデフォルトモードは、[手動（Manual）]モードです。モードを他のモードに変更するには、ファブリック設定を編集します。[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のいずれかのモードに変更します。この例では、ToExternalOnly オプションが選択されています。

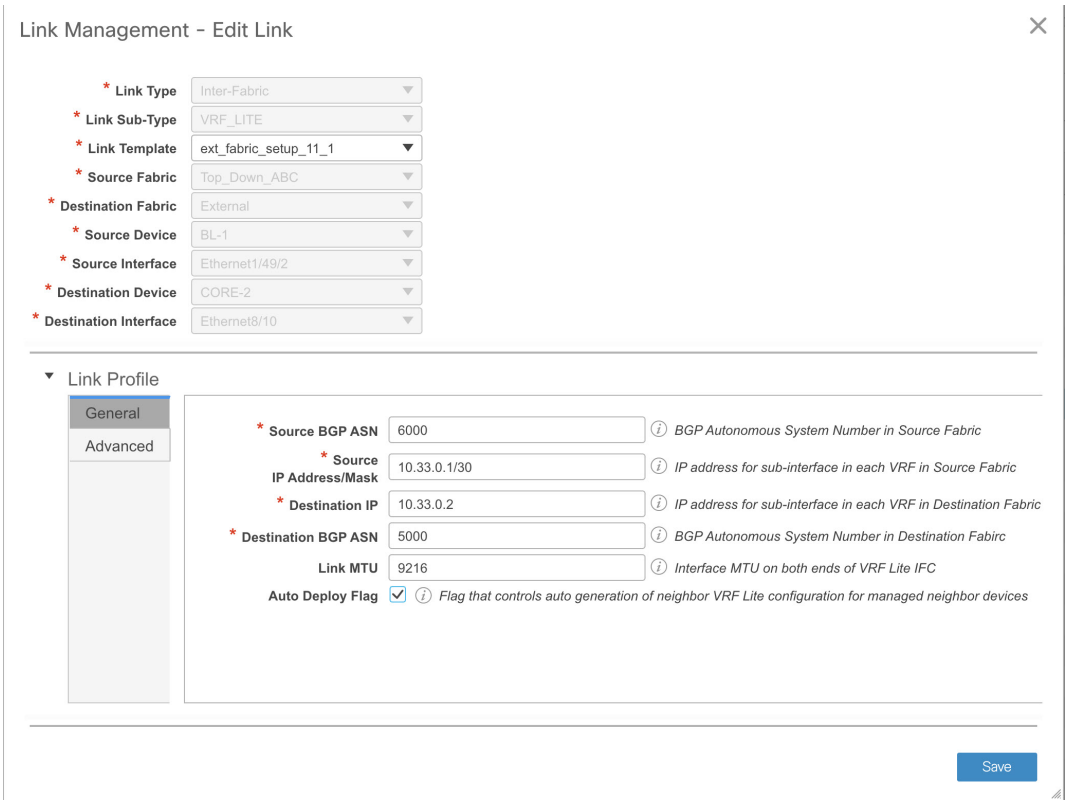
[両方を自動展開（Auto Deploy Both）] : このチェックボックスは、対称 VRF Lite 展開に適用されます。このチェックボックスをオンにすると、自動作成された IFC の **[自動展開フラグ（Auto Deploy Flag）]** が true に設定され、対称 VRF Lite 構成がオンになります。このチェックボックスは、**[VRF Lite 展開（VRF Lite Deployment）]** フィールドが **[手動（Manual）]** に設定されていない場合に選択または選択解除できます。選択した値が優先されます。このフラグは、新しい自動作成 IFC にのみ影響し、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。ベストプラクティスは、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することです。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。

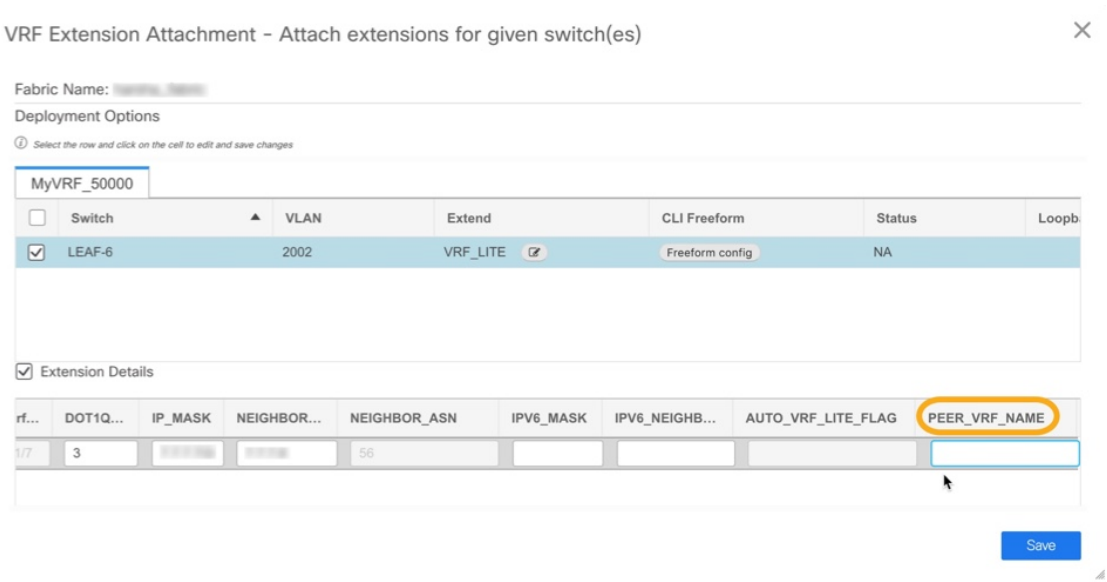
[VRF Lite サブネット マスク（VRF Lite Subnet Mask）] : デフォルトでは、/30 に設定されています。これは、P2P リンクの場合のベスト プラクティスです。

同様に、Easy60000 ファブリックの設定も更新します。

- **[リンク管理（Link Management）]** ダイアログボックスの **[自動展開フラグ（Auto Deploy Flag）]** チェックボックスをオンにします。このチェックボックスをオンにすると、管理対象デバイスのリンクの両端で、VRF Lite サブインターフェイスおよび BGP ピアリング構成を含む VRF lite 展開が有効になります。



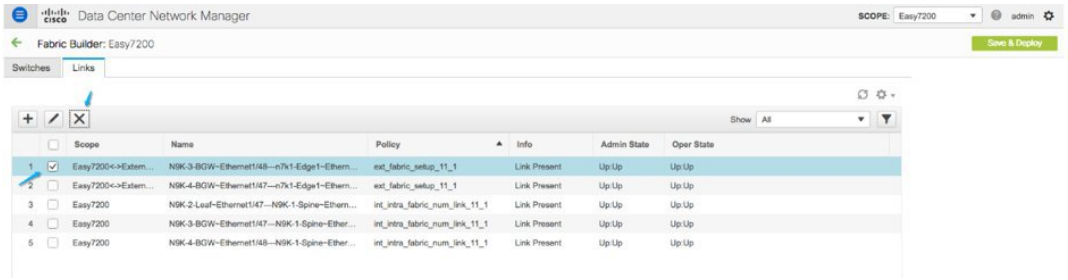
- 連続シナリオで VRF Lite を拡張する場合、VRF はピア ファブリック内にあり、VRF 名は同じである必要があります。VRF がピア ファブリック内にない場合に、VRF Lite を拡張しようとすると、エラー メッセージが表示されます。
- Easy ファブリックと外部ファブリックの間で VRF Lite を拡張する場合、VRF 名は、送信元ファブリック、デフォルト、または別の VRF 名と同じにすることができます。**PEER_VRF_NAME** フィールドに、外部ファブリックで使用される VRF 名を入力します。サブインターフェイスの子 PTI、外部ファブリックの VRF 作成、および BGP ピアリングには、空でない送信元があります。したがって、**[ポリシーの表示/編集（View/Edit policies）]** ウィンドウからポリシーを編集または削除することはできません。
- 両方のファブリックに構成を展開します。外部ファブリックで **[保存と展開（Save & Deploy）]** を実行して、構成を展開します。簡単なファブリック構成は、トップダウン VRF ページまたは **ファブリック ビルダ（Fabric Builder）]** ウィンドウから展開できます。



VRF Lite IFC の削除

IFC を削除する前に、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。

1. ファブリックの [リンク（Links）] タブに移動します。
2. VRF Lite ポリシーが構成されているリンクを選択し、削除ボタンをクリックします。



3. [OK] をクリックして、削除を確認します。
4. ファブリックで [保存して展開（Save and Deploy）] オプションを実行して、VRF Lite ポリシーをリセットします。

外部ファブリックに展開された VRF 拡張の削除

これは 2 つの部分からなるプロセスです。

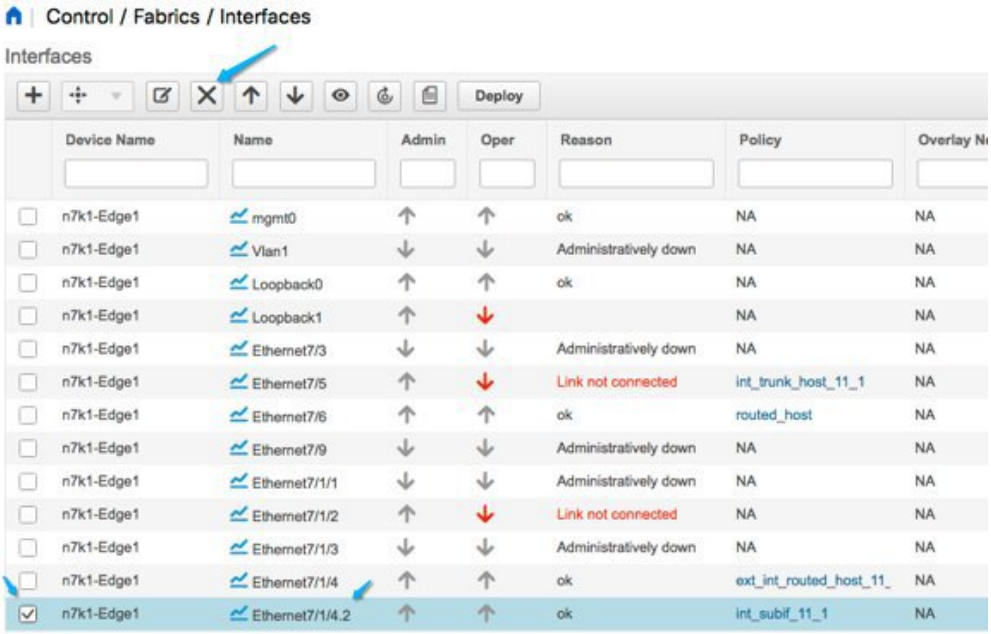
1. インターフェース TAB を使用して作成されたサブインターフェースを削除します。

Note VRF 拡張が Nexus 以外のデバイスに対するものである場合は、この手順をスキップしてください。

2. eBGP 外部接続用に作成されたポリシーを削除します。

サブインターフェイスを削除しています

以下に示すように、[制御（Control）] > [インターフェース（Interfaces）] ページに移動し、削除するサブインターフェースを選択して、[削除（Delete）] ボタンをクリックします。

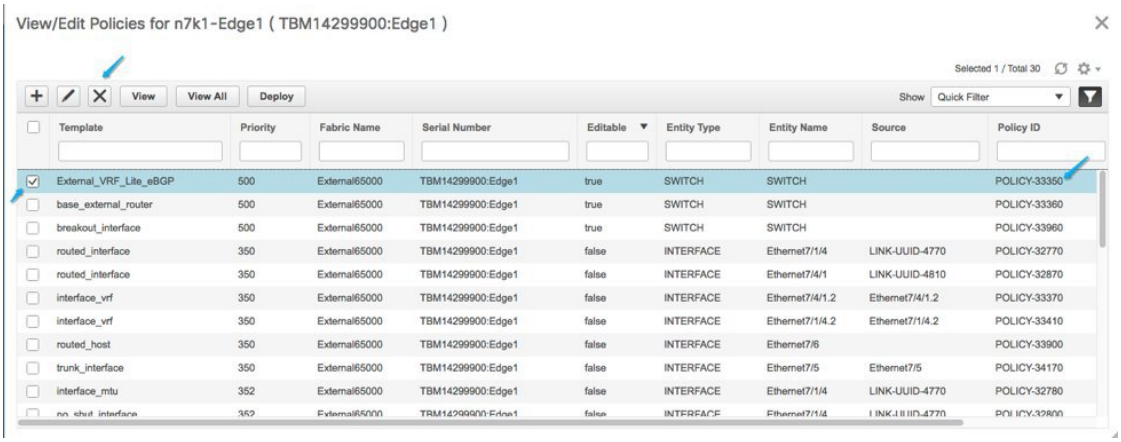


eBGP ポリシーの削除

ファブリック ビルダ ページに移動し、関連する外部ファブリック（この例ではExternal65000）を選択します。デバイスを選択し、2 番目のマウス ボタンを使用して [ポリシーの表示/編集（view edit policy）] を選択します。

eBGP ポリシー作成で使用されるポリシー ID の行を選択します。以下に示すように [X] をクリックしてポリシーを削除します。

保存して外部ファブリックに展開して、ポリシーの変更を展開します。



自動 VRF Lite 作成によって作成された IFC の削除

IFC の編集と削除は、VXLAN ファブリックの [リンク（Link）] タブから行います。自動構成 IFC に関する追加の考慮事項は、次回の保存および展開時に IFC が再生成されないようにするために、モードを手動モードに戻すか、関連するデバイスでのみ構成を保存することです。

- 連続したシナリオでは、ファブリックの 1 つで VRF lite IFC を削除すると、VRF lite はピア ファブリックからも削除されます。
- Easy ファブリックと外部ファブリックの間の VRF ライトを削除する場合は、トップダウン方式を使用して Easy ファブリック内の拡張を削除します。拡張は外部ファブリックから自動的に削除されます。
- 両方のファブリックに構成を展開します。

その他の参考資料

マニュアルのタイトルおよびリンク	マニュアルの説明
VXLAN BGP EVPN を使用した Cisco プログラマブル ファブリックの構成ガイド	このドキュメントでは、VRF Lite を使用した外部接続について説明します。

付録

N9K-3-BGW の構成

テンプレート ext_base_border_vrflite_11_1 によって生成された N9K-3-BGW（ベース ボーダー構成）

Note *switch(config)#* は、グローバル構成モードを示します。このモードにアクセスするには、スイッチで次のように入力します。switch# **configure terminal**

```
(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
```

N9K-3-BGW VRF 拡張構成

```
(config) #
configure profile MyVRF_50000
    vlan 2000
        vn-segment 50000
    interface vlan2000
        vrf member myvrf_50000
           ip forward
           ipv6 forward
           no ip redirects
           no ipv6 redirects
           mtu 9216
           no shutdown

(config) #

vrf context myvrf_50000
    vni 50000
    rd auto
    address-family ipv4 unicast
        route-target both auto
        route-target both auto evpn

   ip route 0.0.0.0/0 2.2.2.1
   address-family ipv6 unicast
         route-target both auto
         route-target both auto evpn

router bgp 7200
    vrf myvrf_50000
        address-family ipv4 unicast
            advertise l2vpn evpn
```

```
            redistribute direct route-map fabric-rmap-redist-subnet
            maximum-paths ibgp 2
            network 0.0.0.0/0
        address-family ipv6 unicast
            advertise l2vpn evpn
            redistribute direct route-map fabric-rmap-redist-subnet
            maximum-paths ibgp 2
        neighbor 2.2.2.1 remote-as 65000
            address-family ipv4 unicast
                send-community both
                route-map extcon-rmap-filter out

(config) #

interface ethernet1/48.2
    encapsulation dot1q 2
    vrf member myvrf_50000
    ip address 2.2.2.2/24
    no shutdown
interface nve1
    member vni 50000 associate-vrf
configure terminal
    apply profile MyVRF_50000
```

第 20 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

Cisco DCNM リリース 11.3(1) 以降、次のハンドオフ機能がサポートされています。

- VXLAN から SR-MPLS
- VXLAN から MPLS LDP

これらの機能は、**Easy_Fabric_11_1** 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。

DCNM 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 DCNM 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、Jerico+ ベースの Nexus 9000 R シリーズ、および Nexus 3600 R シリーズ スイッチ
VXLAN から MPLS LDP	Jericho+ ベースの Cisco Nexus 9000 R シリーズおよび 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。DCNM 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 MPLS LDP 機能設定。
- 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。DCNM 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

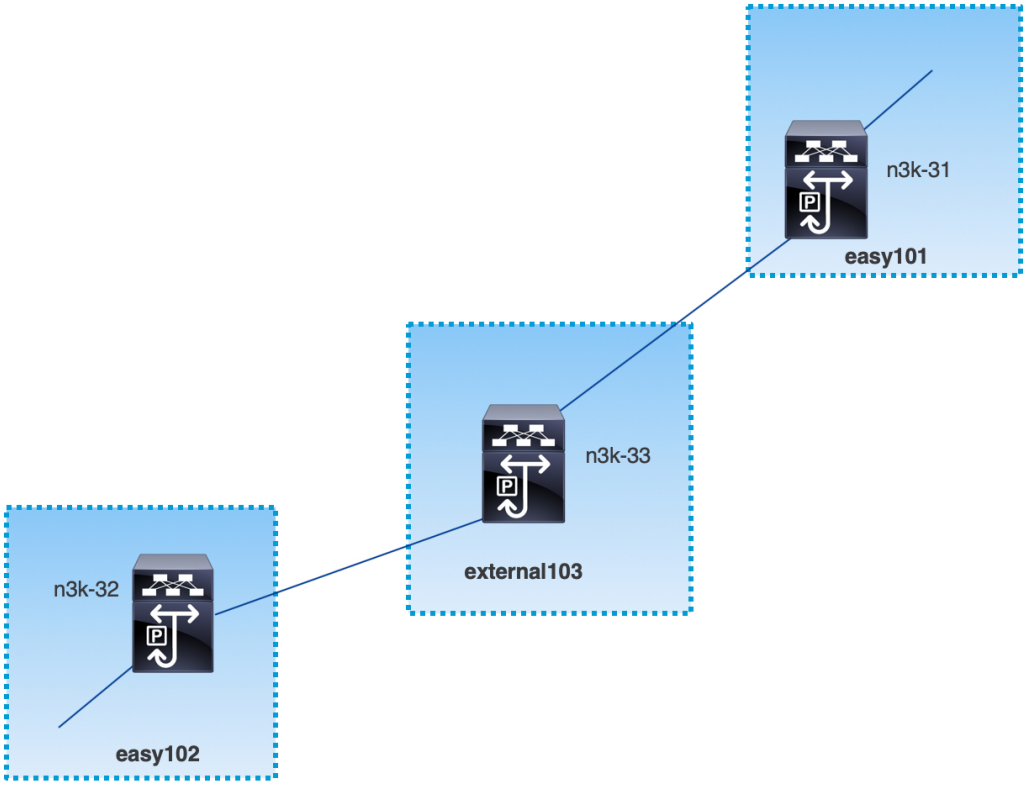
次の 2 つのファブリック間接続リンクが導入されています。

- 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。

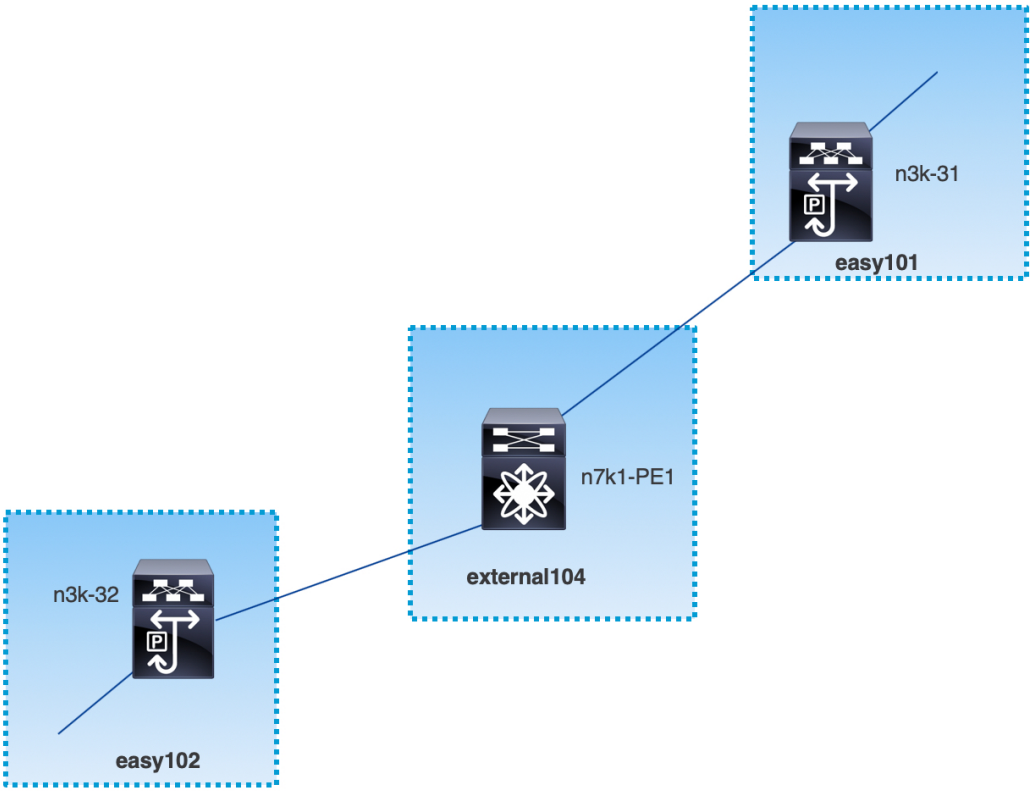
これらのファブリック間接続は、DCNM Web UI または REST API を使用して手動で作成できます。これらのファブリック間接続の自動作成はサポートされていないことに注意してください。

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_11_1** 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_11_1** 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。

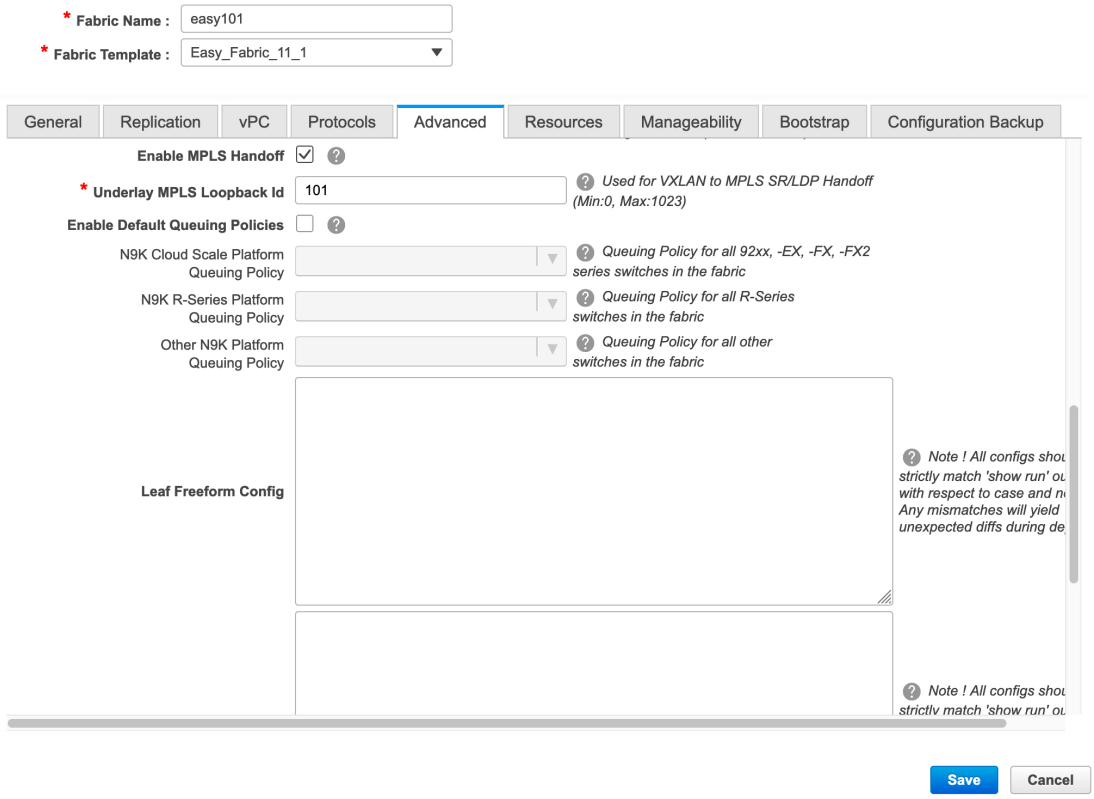
Easy ファブリック設定の編集

Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** に移動します。

ステップ 2 **[ファブリックの編集（Edit Fabric）]** アイコンをクリックして、ファブリック設定を編集します。

ステップ 3 [Advanced] タブをクリックします。

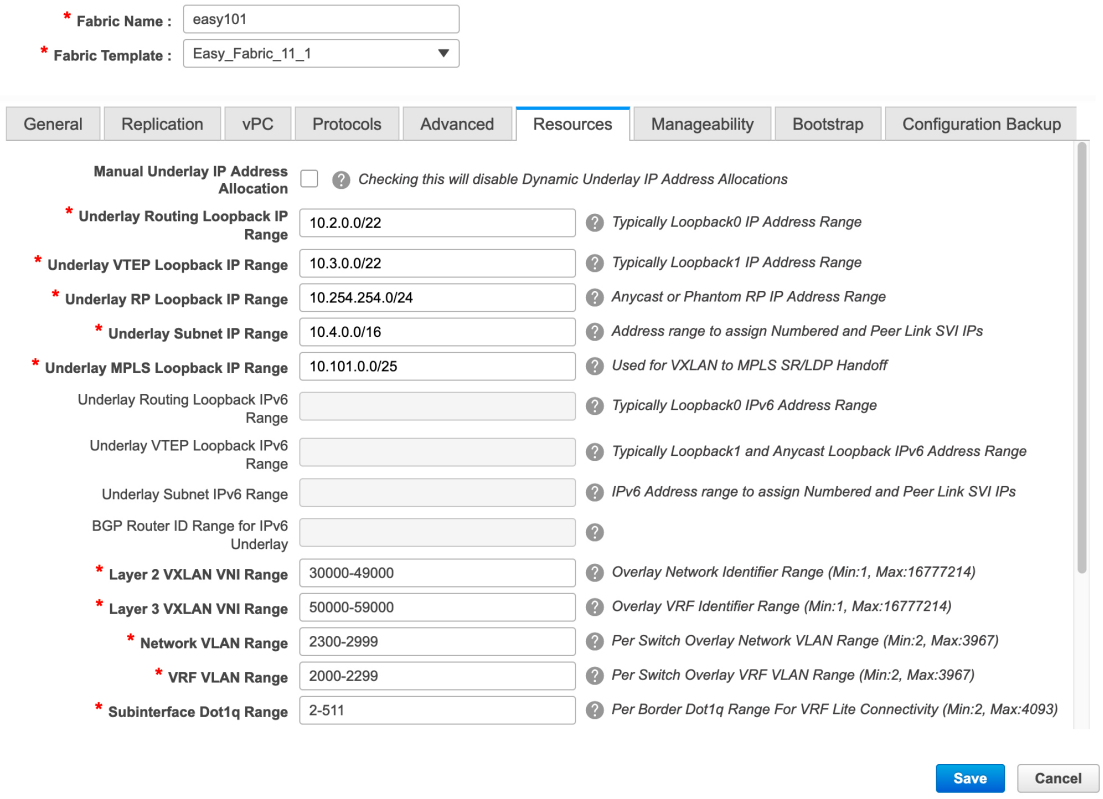


[MPLS ハンドオフの有効化（Enable MPLS Handoff）]：MPLS ハンドオフ機能を有効にするには、このチェックボックスをオンにします。

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 **[保存と展開（Save & Deploy）]** 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。

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

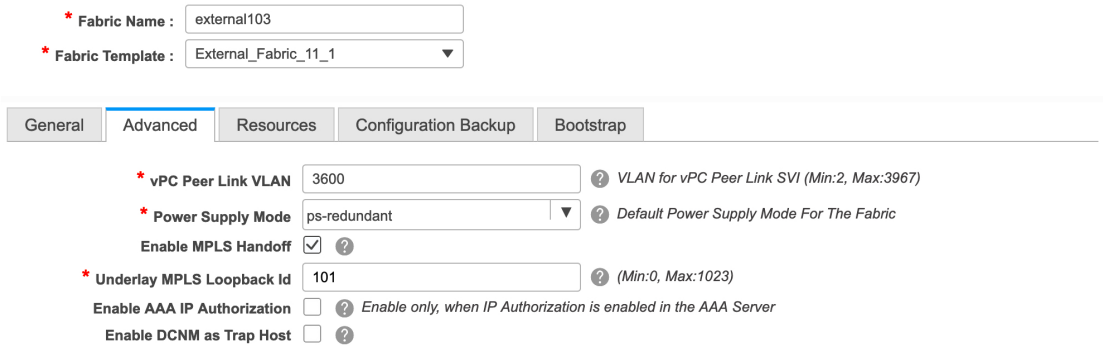
Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** に移動します。

ステップ 2 **[ファブリックの編集（Edit Fabric）]** アイコンをクリックして、ファブリック設定を編集します。

ステップ 3 (Optional) **[全般（General）]** タブで、**[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。

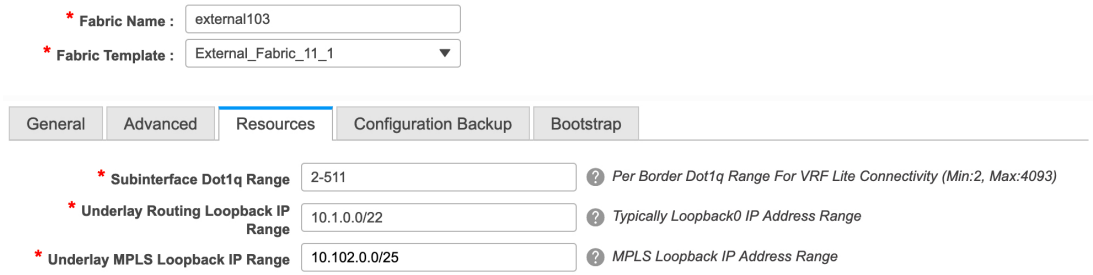
ステップ 4 [Advanced] タブをクリックします。



[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 **[保存と展開（Save & Deploy）]** 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。

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 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

ステップ 2 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。

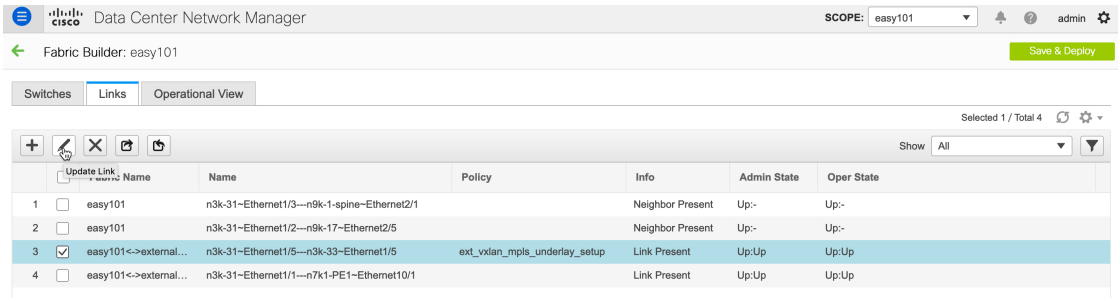
ステップ 3 ウィンドウの左上に表示される **[アクション（Actions）]** パネルの **[表形式ビュー（Tabular view）]** をクリックします。

ステップ 4 **[リンク（Links）]** タブをクリックします。

ステップ 5 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 6 検出された既存のリンクを選択し、**[リンクの更新（Update Link）]** アイコンをクリックします。



リンクが見つからない場合は、**[リンクの追加（Add Link）]** アイコンをクリックし、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 7 **[リンク管理：リンクの編集（Link Management - Edit Link）]** ウィンドウで、**[リンク タイプ（Link Type）]** は **[ファブリック間（Inter-Fabric）]** である必要があります。**[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、**[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。

ステップ 8 **[リンク プロファイル（Link Profile）]** で、**[全般（General）]** タブに必要なすべての情報を入力します。

ファブリック間リンクの MPLS-SR 構成例

ファブリック間リンクの MPLS-LDP 構成例

[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）]：接続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。

[接続先 SR インデックス（Destination SR Index）]：接続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 9 [保存（Save）] をクリックします。

ステップ 10 **[保存と展開（Save & Deploy）]** をクリックして、更新後の構成を展開します。

ステップ 11 **[構成展開（Config Deployment）]** 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 12 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウから接続先ファブリックに移動し、**[保存と展開（Save & Deploy）]** を実行します。つまり、手順 10 と 11 を実行します。

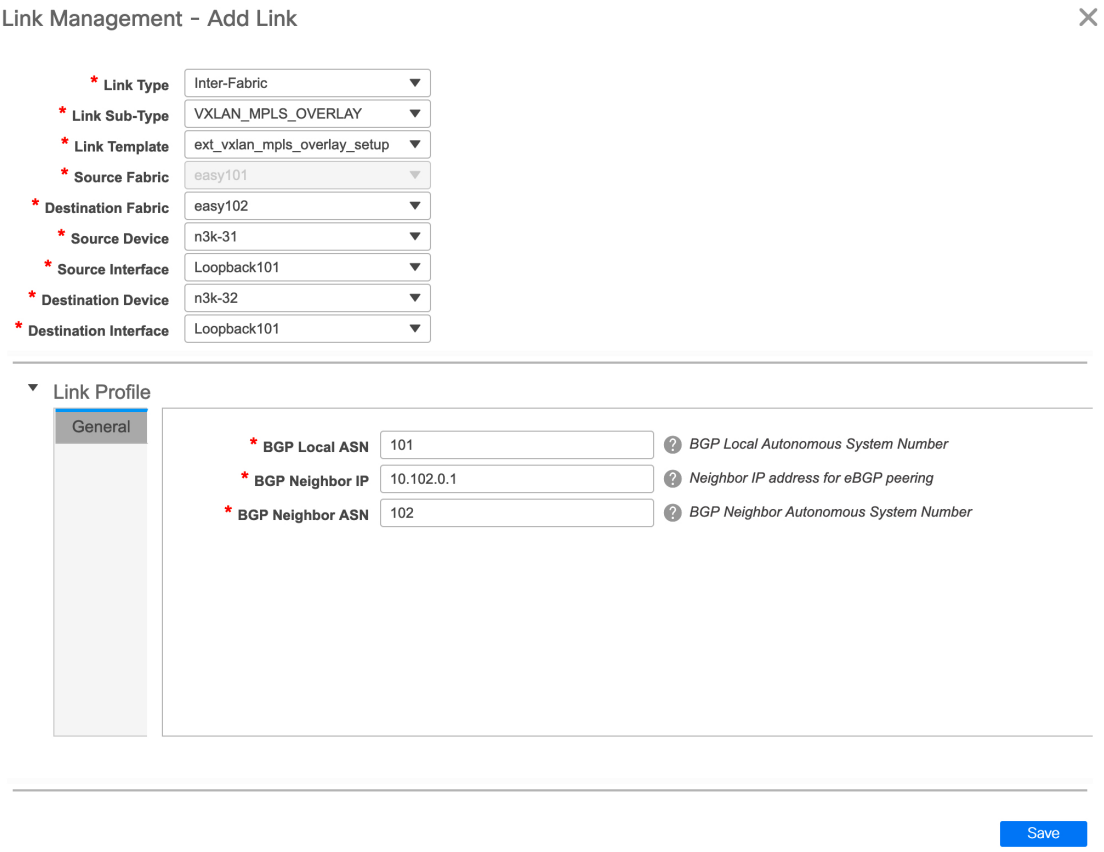
オーバーレイ ファブリック間接続の作成

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 **[リンクの追加（Add Link）]** アイコンをクリックします。

ステップ 2 **[リンク管理 - リンクの追加（Link Management - Add 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。

[接続先ファブリック（Destination Fabric）]：このドロップダウンボックスから接続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。

[リンク プロファイル（Link Profile）] セクションの **[全般（General）]** タブ。

[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 **[保存と展開（Save & Deploy）]** をクリックして、更新後の構成を展開します。

ステップ 5 **[構成展開（Config Deployment）]** 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 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウから接続先ファブリックに移動し、**[保存と展開（Save & Deploy）]** を実行します。つまり、手順 4 と 5 を実行します。

Note 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、MPLS オーバーレイ IFC リンクを削除できます。

VRF の展開

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。

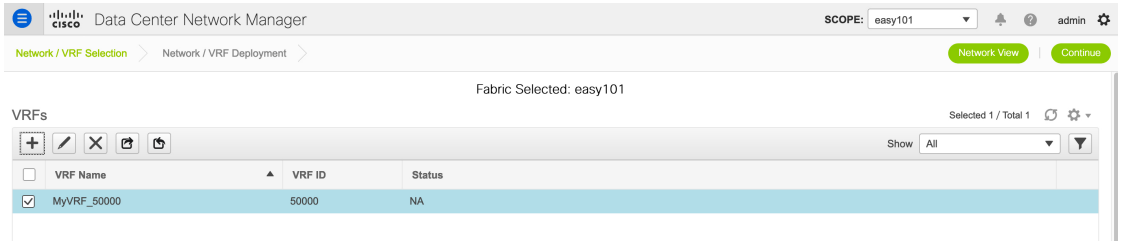
Note 4 バイトの ASN を使用し、自動ルート ターゲットが構成されている場合、自動的に生成されるルート ターゲットは 23456:VNI です。2 つの異なるファブリックの 2 つの異なる VRF に同じ VNI 値がある場合、自動ルート ターゲットにより、2 つの VRF のルート ターゲットは同じになり、値 23456 は常に一定です。VXLAN MPLS ハンドオフを介して接続された 2 つのファブリックの場合、これにより、意図しないルート交換が発生する可能性があります。したがって、セキュリティ上の理由から自動ルート ターゲットを無効にする場合は、ネットワーク テンプレートとネッ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 **[制御（Control）] > [ファブリック（Fabrics）] > [VRF]** に移動します。

ステップ 2 **[VRF]** ウィンドウで、**[追加（Add）]** アイコンをクリックして 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。

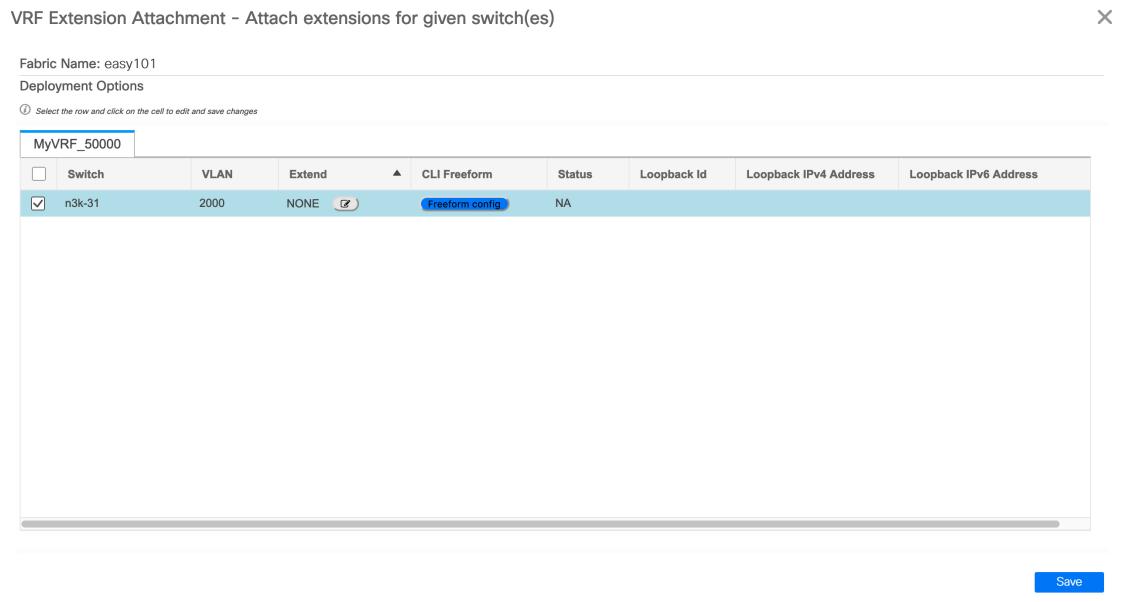
ステップ 3 新しく追加された VRF を選択し、**[続行（Continue）]** をクリックします。



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。

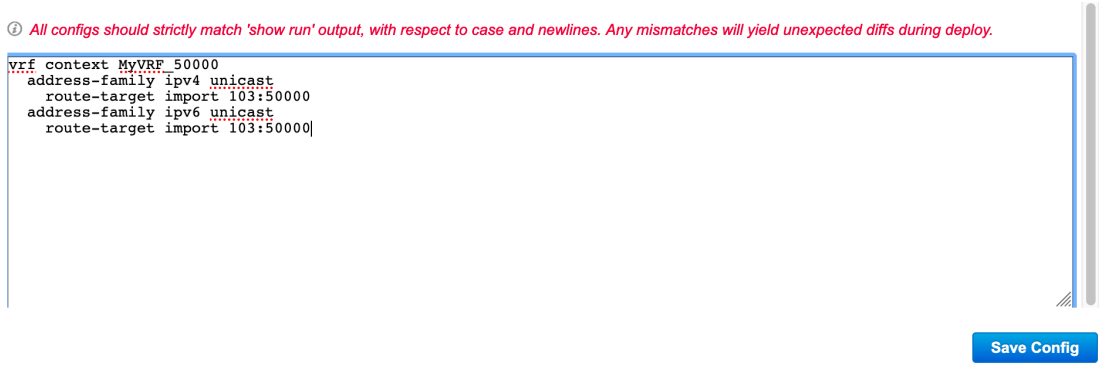
ステップ 5 **[VRF 拡張アタッチメント（VRF Extension Attachment）]** ウィンドウで、VRF を選択し、[CLI フリーフォーム（CLI Freeform）] 列の下にある **[フリーフォーム構成（Freeform config）]** ボタンをクリックします。



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 $$REMOTE_PE_RT$$
```

自由形式構成では、*REMOTE_PE_RT* は、ネイバーが DCNM 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、**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 DCNM 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、接続先ファブリックで手順 3 から手順 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。

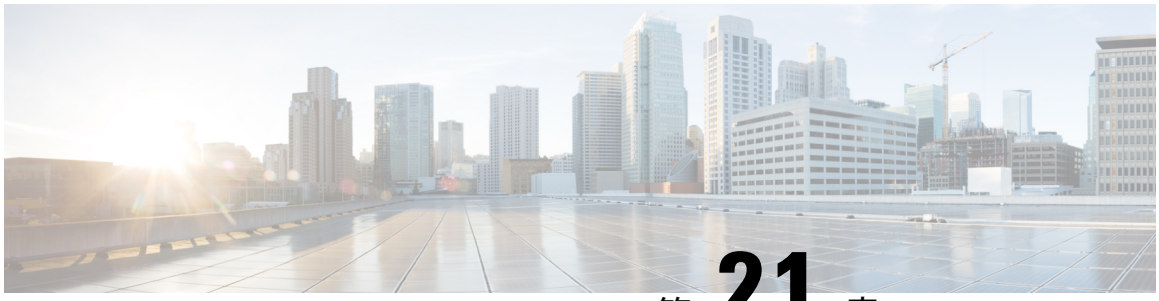
ステップ 2 IFC の削除に関係する各ファブリックについて、**[保存と展開（Save & Deploy）]** をクリックします。

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 967を参照してください。

第 IV 部

VXLAN EVPN マルチサイトを持つレイヤ 2/レイヤ 3 DCI



第 21 章

：マルチサイト ドメインを使用したマルチサイト自動プロビジョニング ボーダー ゲートウェイ

この章では、EVPN マルチサイト機能を使用した LAN ファブリック ボーダー プロビジョニングについて説明します。

VXLAN BGP EVPN ファブリックでのボーダー プロビジョニングの使用例：マルチサイト

このセクションでは、EVPN マルチサイト機能を使用して、DCNM を介して 2 つの仮想拡張ローカル エリア ネットワーク（VXLAN）ボーダーゲートウェイ プロトコル（BGP）イーサネット VPN（EVPN）ファブリックを接続する方法について説明します。EVPN マルチサイト構成は、2つのファブリックのボーダーゲートウェイ（BGW）に適用されます。また、マルチサイト ドメイン（MSD）の 2 つのメンバー ファブリックを接続することもできます。

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 コンテナであることが、DCNM 11.0(1) リリースで導入されました。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。MSD の詳細については、「制御」の章の「VXLAN BGP EVPN ファブリックのマルチサイト ドメイン」セクションを参照してください。

EVPN マルチサイト機能の詳細については、『VXLAN BGP EVPN マルチサイトの設計と展開』に関するドキュメントを参照してください。

構成メソッド：自動構成および DCNM GUI を使用して、メンバー ファブリック間にアンダーレイおよびオーバーレイのファブリック間接続（IFC）を作成できます。

vPC 構成は、Cisco DCNM リリース 11.1(1) の**ボーダーゲートウェイ**のロールを持つ BGW でサポートされます。

サポートされている接続先デバイス：VXLAN ファブリックを Cisco Nexus および Nexus 以外のデバイスに接続できます。接続されたシスコ以外のデバイスもトポロジで表すことができます。

前提条件

- EVPN マルチサイト機能には、Cisco Nexus 9000 シリーズ NX-OS リリース 7.0(3)I7(1) 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 DCNM を介した構成に精通していること。
- MSD ファブリックのメンバー ファブリックを接続する場合は、MSD ファブリックに精通していること。
- EVPN マルチサイト機能、DCNM 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 デバイスの構成（ルート サーバーなど）を使用して接続する準備が整った、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（およびその相互接続）は、手動または DCNM を使用して構成できます。このドキュメントでは、DCNM を介してファブリックを接続するプロセスについて説明します。したがって、DCNM を介して VXLAN BGP EVPN ファブリックの構成と展開方法、および外部ファブリックの作成方法を知っている必要があります。詳細については、「**制御**」の章の「VXLAN BGP EVPN ファブリック プロビジョニング」セクションを参照してください。
- BGW で EVPN マルチサイト機能を有効にするときは、以前のオーバーレイ展開がないことを確認してください。既存のオーバーレイ プロファイルを削除してから、DCNM を介してマルチサイト拡張機能のプロビジョニングを開始します。
- メンバー ファブリックと外部ファブリックで、次に MSD ファブリックで、**[保存と展開（Save & Deploy）]** 操作を実行します。

Note **[保存と展開（Save & Deploy）]** ボタンは、ファブリック トポロジ画面の右上部分に表示されます（**[ファブリック ビルダ（Fabric Builder）]** ウィンドウからアクセス可能で、ファブリックをクリックします）。

- 指定されたBGWのロールが**ボーダー ゲートウェイ**（またはスパイン スイッチの**ボーダー ゲートウェイ スパイン**）であることを確認します。確認するには、BGW を右クリックし、**[ロールの設定（Set role）]** をクリックします。スイッチの現在のロールに（**current**）が追加されていることがわかります。
- ファブリック全体で一貫性を確保するには、次のことを確認してください。

Note これらのチェックは、MSDファブリックがMSDファブリックの下に移動されたときに、MSD のメンバー ファブリックに対して実行されます。

  - ファブリック全体のアンダーレイ IPアドレス、ループバック 0アドレス、およびループバック 1アドレス サブネットは一意である必要があります。重複を避けるために、各ファブリックに一意の IP アドレス プールがあることを確認してください。
  - 各ファブリックには、一意のサイト ID と BGP AS 番号が関連付けられて構成されている必要があります。
  - すべてのファブリックは、同じエニーキャスト ゲートウェイ MACアドレスを持つ必要があります。
  - 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。各ファブリックのファブリック インスタンス値（たとえば、マルチキャスト グループ サブネット アドレス）と、各スイッチのスイッチ インスタンス値（たとえば、VLAN ID）を指定する必要があります。

Note

ケース 1：ネットワークの作成中にVLANが指定されている場合、すべてのスイッチについて、ネットワークをスイッチに接続すると、VLANには、ネットワークの作成中に指定されたのと同じ VLAN が自動的に入力されます。ネットワーク リスト画面には、すべてのスイッチに適用されるネットワーク レベルの VLAN が表示されます（同じである必要があります）。もう1つ注意すべきことは、ネットワークの作成中に VLAN を指定した場合でも、スイッチごとに上書きできるということです。

ケース 2：ネットワークの作成中にVLANが指定されていない場合、すべてのスイッチについて、ネットワークをスイッチに接続すると、スイッチごとの VLAN プールから次の空き VLAN が自動入力されます。これは、スイッチごとにVLANが異なる可能性があることを意味します。ユーザは自動入力された VLAN をいつでも上書きでき、DCNM はそれを優先します。この場合、VNI 10000 は、leaf1 で VLAN 10 を使用し、leaf2 で VLAN 11 を使用する可能性があります。したがって、ネットワーク リストでは、この場合、VLAN は表示されません。

DCNM は、リソース マネージャでスイッチごとに VLAN を常に追跡します。これは、上記の2つのケースのいずれにも当てはまります。

制限事項

- **ボーダーゲートウェイ スパイン** ロールでは、vPC 構成はサポートされていません。
- Cisco DCNM の VXLAN OAM 機能は、単一のファブリックまたはサイトでのみサポートされます。
- FEXは、vPCまたはエニーキャストを使用するボーダーゲートウェイまたはボーダー リーフではサポートされていません。

MSD ファブリックでの保存と展開操作

[保存と展開（Save & Deploy）] を実行すると、次の操作が実行されます。

- **[重複する IP アドレスのチェック（Duplicate IP address check）]**：MSD ファブリックは、BGW に重複する IP アドレスがあるかどうかをチェックします。その場合は、エラー メッセージが表示されます。

BGW の BGP ピアリング ループバック IP アドレスを変更します。

IP アドレスの重複の問題が解決されたら、MSD ファブリックで **[保存と展開（Save & Deploy）]** 操作を再度実行します。

- **[BGW 基本構成（BGW base configuration）]**：MSD ファブリックで初めて保存および展開を実行する場合（現在、展開する IFC またはオーバーレイがないと仮定）、適切な基本構成が BGW に展開されます。それらを以下に示します。

設定	説明
`evpn multisite border-gateway 7200` `  delay-restore time 300`	7200 はメンバー ファブリック Easy7200 のサイト ID です。 BGP ASN 値は、サイト ID フィールドに自動入力するために使用されます。この値は上書きできます。BGP ASN 値を変更しても、サイト ID は最初の BGP ASN 値に設定されたままです。

設定	説明
`interface nve1` `multisite border-gateway interface loopback100`	ループバック インターフェース 100 は、MSD ファブリック設定で設定された構成です。ループバック ID を選択して **保存して展開** を実行すると、ループバック ID を変更することはできません。 MSD ファブリックで BGW のロールを変更するには、次の手順を実行します。 **1.** Easy ファブリックでは、BGW のロールをリーフまたはボーダーに変更します。 **2.** 変更を保存して展開します。 これにより、スイッチからループバック 100 が削除されます。 **3.** ロールを BGW に戻し、保存して展開します。 **4.** MSD ファブリックで、ループバック ID 設定を目的の値に変更し、保存して展開します。
`interface ethernet1/47` `  evpn multisite fabric-tracking`	**evpn multisite fabric-tracking** コマンドは、スパイン ロールを持つスイッチに接続されているボーダーゲートウェイ上のすべてのポートで構成されます。 ボーダーゲートウェイ スパイン ロールの場合、リーフスイッチに面するすべてのポートにこのコマンドが構成されています。

`interface loopback100`
`  ip address 10.10.0.1/32 tag 54321`
`  ip router ospf UNDERLAY area 0.0.0.0`
`  ip pim sparse-mode`
`  no shutdown`
	マルチサイト ループバック インターフェイス。これは、すべてのボーダーゲートウェイ（スパイン）で構成されます。
	同じファブリック内のすべての BGW は、同じ IP アドレスを取得します。各ファブリックは、独自の一意の IP アドレスを取得します。
	最初に BGW のロールを変更しない限り、このアドレスまたは ID を変更することはできません。

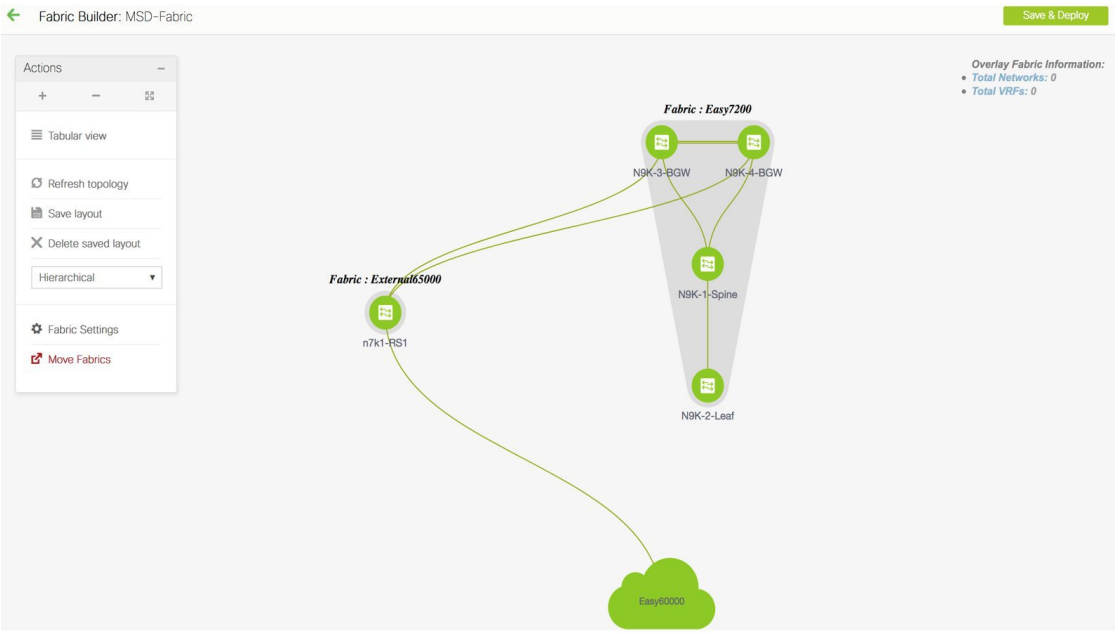
設定	説明
`route-map rmap-redist-direct permit 10` `  match tag 54321`	これは、BGP ピアリング ループバック IP アドレス（通常は loopback0）、VTEP プライマリ（vPC の場合はループバック セカンダリ IP アドレス）、通常は loopback1、およびマルチサイト ループバック IP アドレスをマルチサイト eBGP アンダーレイ セッションに再配布する構成です。

- MSD ファブリックで **保存と展開** 操作を実行すると、MSD のメンバー ファブリック内のすべての BGW（または BGW スパイン）デバイスで動作します。

EVPN マルチサイト固有の前提条件を完了したら、EVPN マルチサイト構成を開始します。サンプル シナリオについて説明します。

EVPN マルチサイト構成

EVPN マルチサイト機能は、シナリオ例を通じて説明されています。2 つの VXLAN BGP EVPN ファブリック、**[Easy60000]** と **[Easy7200]**、および外部ファブリック、**[External65000]** を検討してください。3 つのファブリックは、MSD ファブリック **[MSD-Fabric]** のメンバー ファブリックであり、一意の AS 番号によって識別されます。Easy60000 と Easy7200 は、（各ファブリックにある）External65000 のルート サーバーに接続されています。このドキュメントでは、ルート サーバーを介して、Easy60000 と Easy7200 のホスト間でエンドツーエンドのレイヤ 3 およびレイヤ 2 トラフィックを有効にする方法を示します。



ネットワークおよび VRF 構成を含む VXLAN BGP EVPN ファブリック内構成は、DCNM ソフトウェア、11.1(1) リリースを介してスイッチにプロビジョニングされます。ただし、ファブリック間のサーバー トラフィックは、次の構成を介してのみ可能です。

- マルチサイト機能のようなデータセンターインターコネクト（DCI）機能は、両方のファブリック（Easy7200 の N9K-3-BGW および N9K-4-BGW、Easy60000 の BGW）の BGW で構成されます。構成の一部として、ファブリックの BGW が外部ファブリック External65000 のルート サーバー N7k1-RS1 に接続されるため、適切な eBGP ピアリング構成が BGW で有効になります。
- 現在、オーバーレイ ネットワークと VRF は、非 BGW リーフおよびスパイン スイッチで有効になっています。ファブリックのトラフィックが BGW を超えるには、ネットワークと VRF をすべての BGW にも展開する必要があります。

  簡単に言えば、EVPN マルチサイト機能の構成は、BGW 基本構成（保存および展開操作中に有効化）、3 つの BGW からルート サーバー N7k1-RS1 への eBGP アンダーレイおよびオーバーレイ ピアリングのセットアップで構成されます。アンダーレイとオーバーレイの両方のピアリングは、DCNM リリース 11.1(1) を介して eBGP 上で確立されます。

DCNM GUI または自動構成を使用して、ファブリック間にマルチサイト ファブリック間接続（IFC）を作成できます。まず、アンダーレイ IFC の作成について説明し、次にオーバーレイ IFC の作成について説明します。

マルチサイト アンダーレイ IFC の構成：DCNM GUI

エンド ツーエンドの構成は、これらの 2 つの高レベルの手順に分割できます。

ステップ 1：**Easy7200 の BGW での EVPN マルチサイト構成**

ステップ 2：Easy60000 の BGW での EVPN マルチサイト構成

Note ファブリック間リンクは、2つのイーサネットインターフェイス間の物理接続（アンダーレイ接続）または仮想接続（2つのループバックインターフェイス間のファブリック オーバーレイ接続）です。デバイス間に物理接続を追加すると、デフォルトで新しいリンクが [リンク（Links）] タブに表示されます。

ステップ 1：**Easy7200 の BGW での EVPN マルチサイト構成**

Easy7200から外部ファブリックへのマルチサイト接続の場合、N9K-3-BGWおよびN9K-4-BGWは、外部ファブリックのルート サーバー N7k1-RS1 に接続されます。手順は以下のとおりです。

Easy7200 と External65000 間のアンダーレイ IFC の展開

- N9K-3-BGW から N7k1-RS1 へのアンダーレイ IFC の展開。
- N9K-4-BGW から N7k1-RS1 へのアンダーレイ IFC の展開。

N9K-3-BGW から N7k1-RS1 へのアンダーレイ IFC の展開

Multi-Site DCNM GUI 構成オプションの場合、MSD ファブリックの設定（**[DCI]** タブ）の **[ボーダーゲートウェイ メソッドの展開（Deploy Border Gateway Method）]** フィールドが **[手動（Manual）]** に設定されています。

1. **[リンク（Links）]** タブに移動し、N9K-3-BGW を N7k1-RS1 に接続する物理リンクを選択します。
2. 下の図に示すリンク編集アイコンをクリックして、ポップアップを表示します。
3. MS アンダーレイ IFC サブタイプを選択し、必須フィールドに入力します。

Note DCNM が最大パス値を選択できるようにするには、**[BGP 最大パス（BGP Maximum Paths）]** フィールドに値 1 を入力します。2 ～ 64 の値を入力して、最大パス値を決定します。

4. MSD に保存して展開すると、構成が N9K-3-BGW および N7k1-RS1 に展開されます。

   同様の手順を使用して、[リンク（Links）] タブで作成済みの IFC を編集できます。
5. 同様に、N9K-4-BGW から N7k1-RS1 へのアンダーレイ IFC を作成します。

これで、次のステップ 1 が完了します。

ステップ 1：Easy7200 の BGW での EVPN マルチサイト構成

ステップ 2：Easy60000 の BGW での EVPN マルチサイト構成

次に、Easy60000 の BGW で構成を有効にします。

ステップ 2：**Easy60000 の BGW での EVPN マルチサイト構成**

Easy6000 ファブリックと外部ファブリック間のマルチサイト接続の場合、EVPN マルチサイト構成は、外部ファブリックのルート サーバー（N7k1-RS1）に接続されている Easy60000 の BGW インターフェイスで有効になっています。Easy7200 と External65000 間の接続は、説明ごとの手順に従ってください。

マルチサイト アンダーレイ IFC の構成：自動構成

アンダーレイ IFC は、デバイスのインターフェイス間の物理リンクです。

- Easy7200 から外部ファブリックへのアンダーレイ接続の場合、N9K-3-BGW および N9K-4-BGW は、外部ファブリックのルート サーバー N7k1-RS1 に接続されます。
- Easy60000 から外部ファブリックへのアンダーレイ接続の場合、その BGW はルート サーバー N7k1-RS1 に接続されます。

自動構成によるマルチサイト アンダーレイ IFC の展開

DCNM によって生成されるアンダーレイは、デフォルトの IPv4 ユニキャスト ルーティング テーブル内の eBGP セッションであり、マルチサイト コントロールプレーンとデータプレーンが正しく機能するために必要な 3 つのループバック アドレスを配布します。

マルチサイト自動構成オプションの場合、アンダーレイ IFC は MSD ファブリックによって自動的に展開されます。

マルチサイト アンダーレイ IFC の作成には、次のルールが適用されます。

1. **[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、マルチサイト アンダーレイ自動構成を有効にします。自動構成を無効にするには、チェックボックスをオフにします。このチェックボックスは、デフォルトでオフになっています。
2. IFC は、物理的に接続されているさまざまなメンバー ファブリックの BGW 間のすべての物理接続に展開されます。
3. IFC は、BGW と、MSD ファブリックのメンバーである外部ファブリックにインポートされたコア ルータのロールを持つルータとの間のすべての物理接続に展開されます。

   接続で IFC が自動生成されないようにする場合は、リンクを閉じて、保存して展開操作を実行し、不要な IFC を削除します。また、インターフェイスに既存のポリシーまたは事前構成された IP アドレスがないことを確認してください。それ以外の場合は、手動モードを使用します。
4. アンダーレイの展開に使用される IP アドレスは、MSD ファブリックの DCI サブネット IP 範囲フィールド（DCI タブ）の IP アドレス範囲から取得されます。

オーバーレイ IFC と同様に、マルチサイト アンダーレイ IFC は、MSD、外部およびメンバー ファブリックを介して表示できます。また、アンダーレイ IFC は、VXLAN または MSD ファブリックを介して編集および削除できます。

非 Nexus Device に対するマルチサイト アンダーレイ IFC の構成：DCNM GUI

このケースでは、非 Nexus デバイスは DCNM にインポートされず、または Cisco Discovery Protocol または Link Layer Discovery Protocol（LLDP）を介して検出されません。たとえば、Cisco ASR 9000 シリーズのルータ、または非 Cisco デバイスでも同様です。

手順は、**マルチサイト アンダーレイ IFC の構成**：**DCNM GUI** タスクと同様です。

1. **[ファブリック ビルダ（Fabric Builder）]** ウィンドウで、**[Easy7200]** ファブリックを選択します。

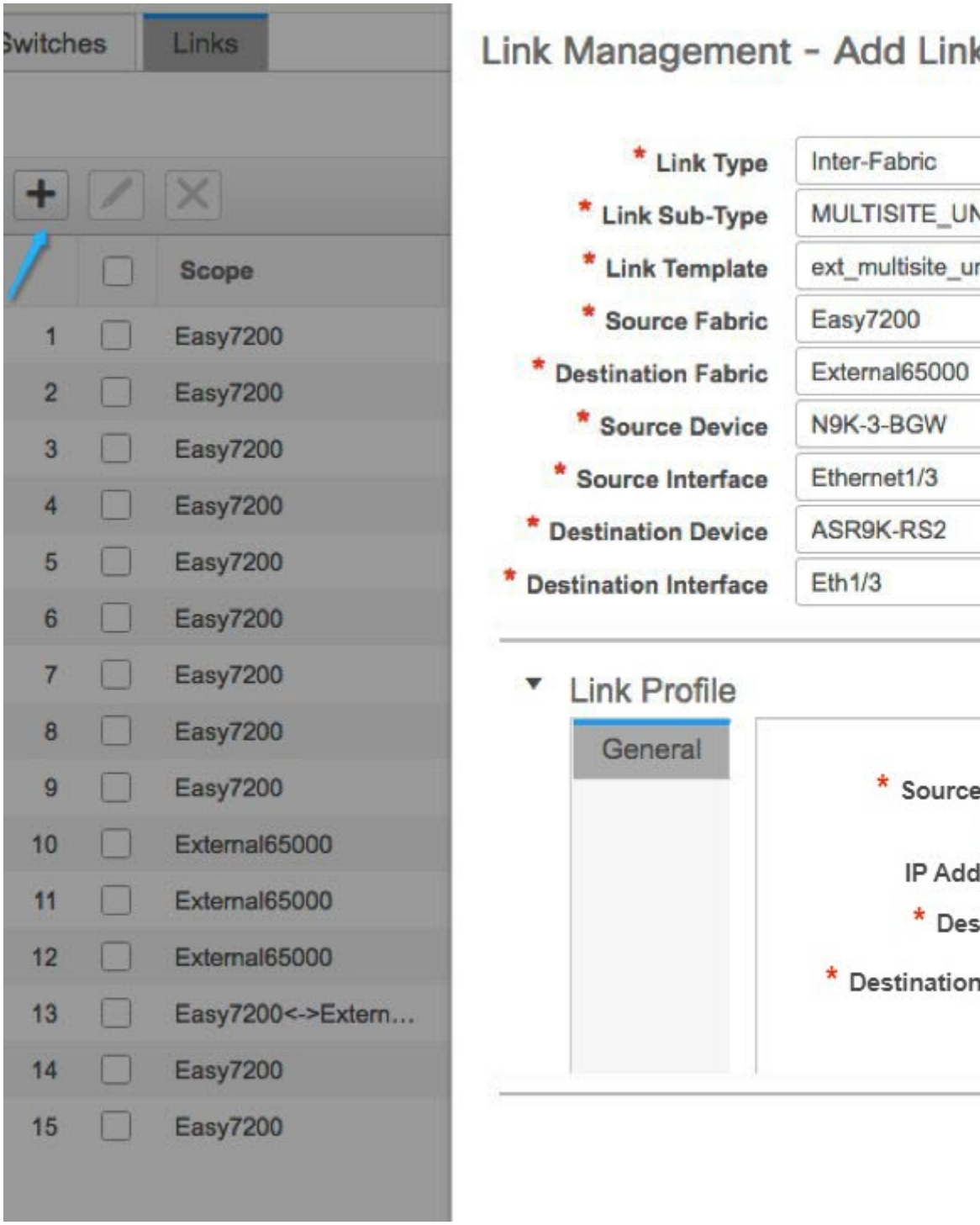
   [Easy7200] トポロジ ウィンドウが表示されます。
2. 左側の **[アクション（Actions）]** パネルで、**[表形式ビュー（Tabular view）]** をクリックします。

   [スイッチ | リンク（Switches | Links）] ウィンドウが表示されます。

3. **[リンク（Links）]** タブをクリックし、**[+]** をクリックします。

   [リンクの追加（Add Link）] ウィンドウが表示されます。

4. フィールドに情報を入力します。



リンク タイプ：**[ファブリック間（Inter-Fabric）]** を選択します。

リンク サブタイプ：**MULTISITE_UNDERLAY** を選択します。

リンク テンプレート：デフォルトでは、**ext_multisite_underlay_setup_11_1** テンプレートが設定されています。

送信元ファブリック：IFC が **Easy7200** から ASR デバイスに作成されるため、**Easy7200** がデフォルトで選択されます。

接続先ファブリック：外部ファブリックを選択します。このケースでは、**External65000** が選択されています。

送信元デバイスと**送信元インターフェイス**：ASR デバイスに接続するボーダーデバイスとインターフェイスを選択します。

接続先デバイス：デバイスを識別する任意の文字列を入力します。IFC を初めて作成するとき、接続先デバイス **ASR9K-RS2** はドロップダウンリストに表示されません。**ASR9K-RS2** への IFC を作成し、外部ファブリック **External65000** に関連付けると、**ASR9K-RS2** が **[接続先デバイス（Destination Device）]** フィールドに表示されるデバイスのリストに表示されます。

また、最初の IFC 作成後、**ASR9K-RS2** が Fabric Builder 内の **External65000** 外部ファブリック トポロジに表示されます。

接続先インターフェース：インターフェースを識別する任意の文字列を入力します。

接続先インターフェイスの名前を毎回手動で入力する必要があります。

[リンク プロファイル（Link Profile）] セクションの **[全般（General）]** タブ。

送信元 BGP ASN（Source BGP ASN：このフィールドには、送信元ファブリック **Easy7200** の AS 番号が自動入力されます。

送信元 IP アドレス/マスク：マルチサイト アンダーレイ IFC のローカル インターフェイスとして使用される IP アドレスとマスクを入力します。

接続先 IP：eBGP ネイバーとして使用される **ASR9K-RS2** インターフェイスの IP アドレスを入力します。

接続先 BGP ASN：このフィールドでは、外部ファブリック **External65000** の AS 番号が自動入力されます。これは、外部ファブリックとして選択されているためです。

5. ウィンドウの右下にある **[保存（Save）]** をクリックします。

   [スイッチ | リンク（Switches | Links）] ウィンドウが再び表示されます。IFC エントリがアップデートされることを確認できます。

6. ウィンドウの右上にある **[保存して展開（Save and Deploy）]** をクリックします。

   IFC が展開されるリンクには、**ポリシー** 列で構成済みの関連するポリシーがあります。

7. ウィンドウの右上にある **[範囲（Scope）]** ドロップダウンリストへ移動し、**External65000** を選択します。外部ファブリック **[リンク（Links）]** ウィンドウが表示されます。ここでは、IFC が **Easy7200** から ASR デバイスへ作成されたことを確認できます。

マルチサイト オーバーレイ IFC の構成

オーバーレイ IFC はデバイスの loopback0 インターフェイス間のリンクです。

Easy7200 および Easy60000 でのオーバーレイ IFC の展開は、次の手順で構成されます。

- N9K-3-BGW から N7k1-RS1 へのオーバーレイ IFC の展開。
- N9K-4-BGW から N7k1-RS1 へのオーバーレイ IFC の展開。
- Easy60000 の BGW から N7k1-RS1 へのオーバーレイ IFC の展開。

Easy7200 と External65000 間のオーバーレイ IFC の展開

- N9K-3-BGW から N7k1-RS1 へのオーバーレイ IFC の展開。
- N9K-4-BGW から N7k1-RS1 へのオーバーレイ IFC の展開。

N9K-3-BGW から N7k1-RS1 へのオーバーレイ IFC の展開。

1. [制御（Control）]>[Fabric Builder]の順にクリックします。[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。
2. MSD ファブリック、**[MSD-Fabric]** を選択します。ファブリック トポロジが起動します。
3. [表形式ビュー（Tabular view）] をクリックします。[スイッチ | リンク（Switches | Links）] 画面が表示されます。
4. [リンク（Links）] タブをクリックします。MSD ファブリック内のリンクが一覧表示されます。各行は、Easy7200 または Easy60000 内のファブリック内リンクを表すか、External65000 を含むメンバー ファブリックのボーダーデバイス間のリンクを表します。
5. 画面の左上にある [リンクを追加（Add Link）] アイコンをクリックします。

   [リンク管理：リンクを追加（Link Management – Add Link）] が表示されます。

   いくつかのフィールドについて説明します。

   リンク タイプ – Inter-Fabric は自動入力されます。

   リンク サブタイプ：MULTISITE_UNDERLAY を選択します。

   リンク テンプレート – オーバーレイを作成するためのデフォルトのテンプレートが表示されます。

   テンプレートを編集するか、カスタム構成で新しいテンプレートを作成できます。

   [全般（General）] タブには、Easy7200 と External65000 の BGP AS 番号が表示されます。説明のように他のフィールドに入力します。BGP AS 番号は、ファブリック値に基づいて導出されます。

6. 画面の下部にある [保存（Save）] をクリックします。

   [スイッチ | リンク（Switches | Links）] 画面が再び表示されます。IFC エントリがアップデートされることを確認できます。

7. 画面の右上にある [保存と展開（Save & Deploy）] をクリックします。

8. ウィンドウの右上にある **[範囲（Scope）]** ドロップダウンリストへ移動し、External65000 を選択します。外部ファブリック [リンク（Links）] 画面が表示されます。Easy7200 から External65000 に作成された 2 つの IFC がここに表示されていることがわかります。

Note VXLAN ファブリックで IFC を作成するか、その設定を編集すると、接続された外部ファブリックに対応するエントリが自動的に作成されます。

9. [保存して展開（Save and Deploy）] をクリックして、IFC の作成を External65000 に保存します。

10. 同様に、N9K-4-BGW から N7k1-RS1 へのオーバーレイ IFC を作成します。

    N9K-3-BGW および N9K-4-BGW から N7k1-RS1 へのオーバーレイ IFC が展開された後、ファブリック オーバーレイ トラフィックは Easy7200 と External65000 の間を流れることができます。

11. 同様に、Easy60000 ファブリックの BGW から N7k1-RS1 にオーバーレイ IFC を展開します。

マルチサイト オーバーレイ IFC の構成：自動構成

オーバーレイ IFC はデバイスの loopback0 インターフェイス間のリンクです。Easy7200 および Easy60000 ファブリックから External65000 のルート サーバー N7k1-RS1 へのオーバーレイ接続の場合、BGW デバイスと N7k1-RS1 の loopback0 インターフェイスの間でリンクが有効になります。

Easy7200 および Easy60000 でのオーバーレイ IFC の展開

- N9K-3-BGW から N7k1-RS1 へのオーバーレイ IFC の展開。
- N9K-4-BGW から N7k1-RS1 へのオーバーレイ IFC の展開。
- Easy60000 の BGW から N7k1-RS1 へのオーバーレイ IFC の展開。

自動構成によるマルチサイト オーバーレイ IFC の展開

次のオプションのいずれかを使用して、マルチサイト オーバーレイを自動的に構成できます。

1. ルート サーバーに：BGW はルート サーバーへのオーバーレイを形成します。このオプションは、例で説明されています。

2. Direct to BGW：ファブリック内のすべての BGW から他のメンバー ファブリック内のすべての BGW へのマルチサイト オーバーレイ IFC のフル メッシュです。

上記のオプションのいずれかを選択するには、MSD ファブリックの設定に移動し、[DCI] タブを選択して、[ボーダーゲートウェイ メソッドの展開（Deploy Border Gateway Method）] フィールドを [Route_Server に（Centralized to Route_Server）]（この例の場合など）または [Direct to BGW] に設定します。デフォルトでは、[手動（Manual）] オプションが選択されています。

BGW ノードでのネットワークと VRF の展開に必要な IFC は、MSD ファブリック テンプレートを介して自動構成できます。有効にする設定は、MSD ファブリック テンプレートにあります。

[ボーダーゲートウェイの展開メソッド（Deploy Border Gateway Method）] フィールドのデフォルト モードは **[手動（Manual）]** です。これは、MSD ファブリックのリンク タブを介して IFC を作成する必要があることを意味します。自動構成のために、Route_Server に、または、Direct to BGW モードに変更する必要があります。

自動構成で作成された IFC は、MSD またはメンバー ファブリック（外部ファブリックを除く）のリンク タブからのみ編集または削除できます。IFC が存在するか、物理リンクまたは論理リンクにユーザ定義ポリシーがある限り、自動構成は IFC 構成に影響しません。

上記の画像の [ボーダーゲートウェイの展開メソッド（Deploy Border Gateway Method）] フィールドで [Route_Server に（Centralized to Route_Server）] が選択されていることがわかります。

ルートサーバーに

これは、すべてのメンバー ファブリック内のすべての BGW デバイスが、MSD ファブリックのメンバーである 1 つ以上の外部ファブリック内の 1 つ以上のルート サーバーへのマルチサイト オーバーレイ BGP 接続を作成することを意味します。

このトポロジでは、1 つのルート サーバー n7k1-RS1 があり、その BGP ピアリング アドレス（1.1.1.1）がルート サーバー リストに表示されます。このピアリング アドレスは、アウトオブバンドで構成することも、DCNM の [インターフェイスの作成（create interface）] タブで構成することもできます。N7k1-RS1 を DCNM（この例では外部ファブリック内）にインポートし、保存して展開オプションを実行する前にピアリング アドレスを構成する必要があります。

ルート サーバー ピアリング IP アドレス リストはいつでも編集できますが、構成済みのマルチサイト オーバーレイは [リンク] タブからのみ削除できます。

各ルート サーバーの BGP AS 番号は、MSD ファブリック設定で指定する必要があります。ルート サーバーの AS 番号は、外部ファブリックのファブリック AS 番号とは異なる場合があることに注意してください。

非 Nexus デバイスに対するマルチサイト オーバーレイ IFC の構成：DCNM GUI

このケースでは、非 Nexus デバイスは DCNM にインポートされず、または Cisco Discovery Protocol または Link Layer Discovery Protocol（LLDP）を介して検出されません。たとえば、Cisco ASR 9000 シリーズのルータ、または非 Cisco デバイスでも同様です。

手順は、**マルチサイト オーバーレイ IFC の構成**：**DCNM GUI** タスクと同様です。

1. **[ファブリック ビルダ（Fabric Builder）]** ウィンドウで、**[Easy7200]** ファブリックを選択します。

   [Easy7200] トポロジ ウィンドウが表示されます。

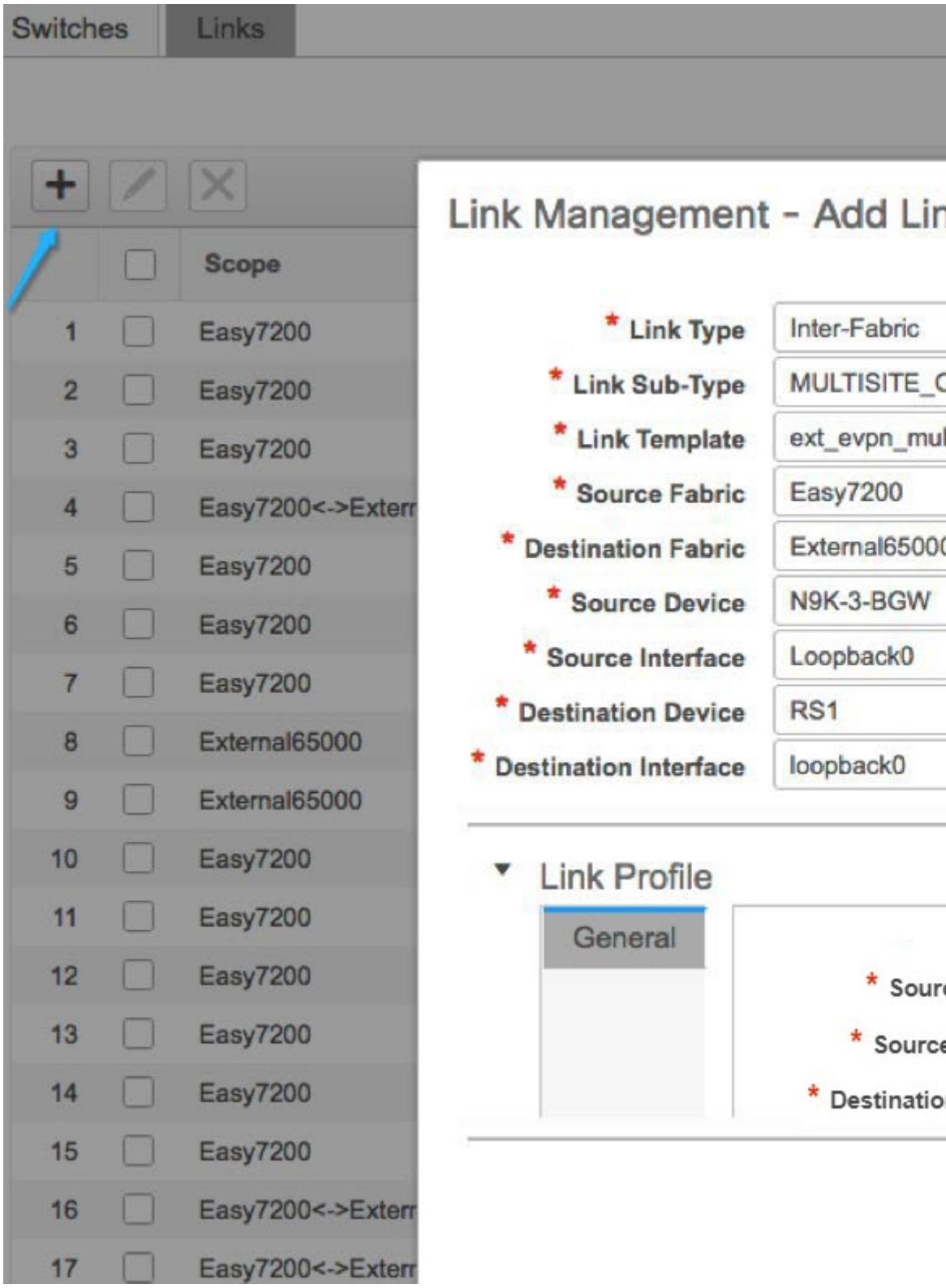
2. **[アクション（Actions）]** パネルで、**[表形式ビュー（Tabular view）]** をクリックします。

   [スイッチ | リンク（Switches | Links）] ウィンドウが表示されます。

3. **[リンク（Links）]** タブをクリックし、**[+]** をクリックします。

   [リンクの追加（Add Link）] 画面が表示されます。

4. フィールドに情報を入力します。



リンク タイプ：**[**ファブリック間（**Inter-Fabric**）**]** を選択します。

リンク サブタイプ：**MULTISITE_UNDERLAY** を選択します。

リンク テンプレート：デフォルトでは、**ext_evpn_multisite_overlay_setup** テンプレートが設定されています。

送信元ファブリック：IFC が **Easy7200** から ASR デバイスに作成されるため、**Easy7200** がデフォルトで選択されます。

接続先ファブリック：外部ファブリックを選択します。このケースでは、**External65000** が選択されています。

[送信元デバイス（Source Device）] と **[送信元インターフェイス（Source Interface）]**：ボーダー デバイスと、オーバーレイの送信元インターフェイスである loopback0 インターフェイスを選択します。

接続先デバイス：デバイスを識別する任意の文字列を入力します。IFC を初めて作成するとき、接続先デバイス **ASR9K-RS1** はドロップダウンリストに表示されません。**ASR9K-RS1** への IFC を作成し、外部ファブリック **External65000** に関連付けると、**ASR9K-RS1** が **[接続先デバイス（Destination Device）]** フィールドに表示されるデバイスのリストに表示されます。

また、最初の IFC 作成後、**ASR9K-RS1** がファブリック ビルダ内の **External65000** トポロジ画面に表示されます。

接続先インターフェース：インターフェースを識別する任意の文字列を入力します。

接続先インターフェイスの名前を毎回手動で入力する必要があります。

[リンク プロファイル（Link Profile）] セクションの **[全般（General）]** タブ。

送信元 BGP ASN（Source BGP ASN：このフィールドには、送信元ファブリック **Easy7200** の AS 番号が自動入力されます。

送信元 IP アドレス/マスク：マルチサイト オーバーレイ IFC の loopback0 インターフェイスの IP アドレスを入力します。

接続先 IP：このマルチサイト オーバーレイ IFC に使用される **ASR9K-RS1** 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。

接続先 BGP ASN：このフィールドでは、外部ファブリック **External65000** の AS 番号が自動入力されます。これは、外部ファブリックとして選択されているためです。

5. 画面の下部にある **[保存（Save）]** をクリックします。

   [スイッチ | リンク（Switches | Links）] 画面が再び表示されます。IFC エントリがアップデートされることを確認できます。

6. 画面の右上にある **[保存して展開（Save and Deploy）]** をクリックします。

   IFC が展開されるリンクには、**ポリシー** 列で構成済みの関連するポリシーがあります。

7. ウィンドウの右上にある **[範囲（Scope）]** ドロップダウンリストへ移動し、**External65000** を選択します。外部ファブリック **[リンク（Links）]** 画面が表示されます。ここにオーバーレイ IFC が表示されていることがわかります。

ルート サーバー N7k1-RS1 でのオーバーレイおよびアンダーレイ ピアリング構成

IFC の作成中に MSD ファブリックで [保存して展開（Save and Deploy）] 操作を実行すると、VXLAN ファブリックの BGW へのルータ サーバー N7k1-RS1 でピアリング構成が有効になります。

マルチサイト オーバーレイの表示、編集、および削除

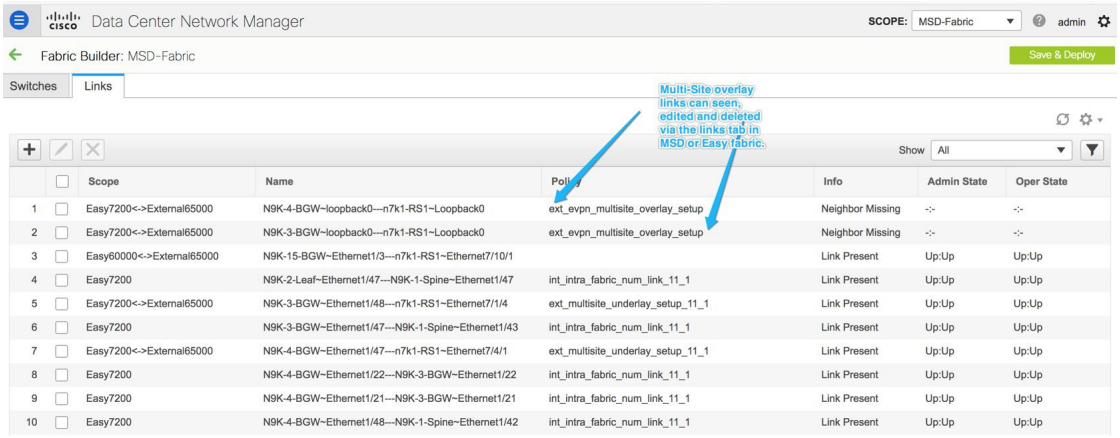
オーバーレイ IFC は、次に示すように、MSD およびメンバー ファブリックのリンク タブで表示できます。

IFC は、メンバー ファブリックまたは MSD ファブリックで編集および削除できます。

マルチサイト オーバーレイ IFC は、MSD ファブリックのリンク タブで作成することもできます。

IFC が削除されたら、外部および VXLAN ファブリック（または MSD ファブリック）で [保存と展開（Save & Deploy）] 操作を実行して、スイッチの IFC を展開解除し、DCNM からインテントを削除する必要があります。

Note 特定の IFC が DCNM から完全に削除されるまで、自動構成は MSD ファブリックでの [保存と展開（Save & Deploy）] 操作でその IFC を再生成しません。



マルチサイト IFC の削除

1. [リンク（Links）] タブに移動し、削除する IFC を選択して、次に示すように [削除（Delete）] アイコンをクリックします。

2. MSD ファブリックで [保存と展開（Save & Deploy）] を実行して、削除を完了します。

Note MSD ファブリック設定で IFC の自動構成が有効になっている場合、保存して展開を実行すると、IFC インテントが再生成される場合があります。

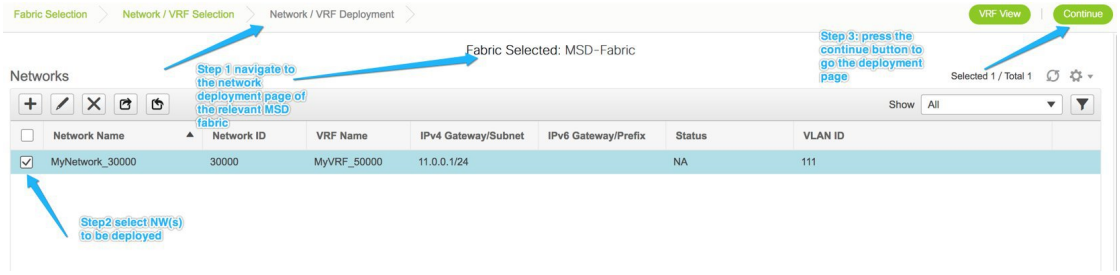
すべてまたは多数の IFC を削除する場合は、一時的に BGW 展開モードを手動設定に変更してから、保存と展開を実行します。

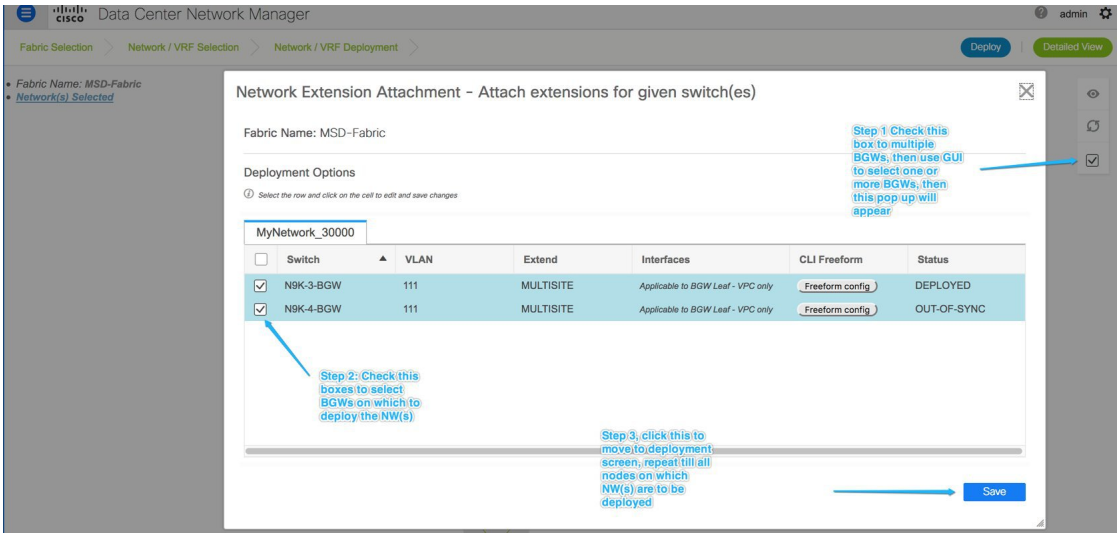
- 非 Nexus スイッチでの IFC の削除：非 Nexus スイッチで最後の IFC を削除すると、そのスイッチはトポロジから削除されます。Cisco DCNM リリース 11.2(1) 以降、非 Nexus スイッチおよび物理スイッチなどのネイバー スイッチを **[表形式ビュー（Tabular view）]** ウィンドウまたはファブリック トポロジ ウィンドウから削除するには、スイッチを右クリックし、ドロップダウンメニューで **[検出（Discovery）] > [ファブリックから削除（Remove from fabric）]** を選択します。
- MSD ファブリックからのファブリックの削除：MSD ファブリックからファブリックを削除する前に、そのファブリック内のすべての BGW からすべてのマルチサイト オーバーレイを削除します。そうしないと、ファブリックを取り除くことができません。次の保存および Easy ファブリックへの展開の後、MSD で構成された IFC、マルチサイト ループバック アドレスなどのすべてのマルチサイト構成が BGW から削除されます。
- デバイス ロールの変更：デバイス ロールをボーダーからボーダーゲートウェイに変更できますが、ボーダーゲートウェイからボーダーへのロールの変更は、デバイスにマルチサイト IFC またはオーバーレイが展開されていない場合にのみ許可されます。

MSD ファブリックでのネットワークと VRF の作成と展開

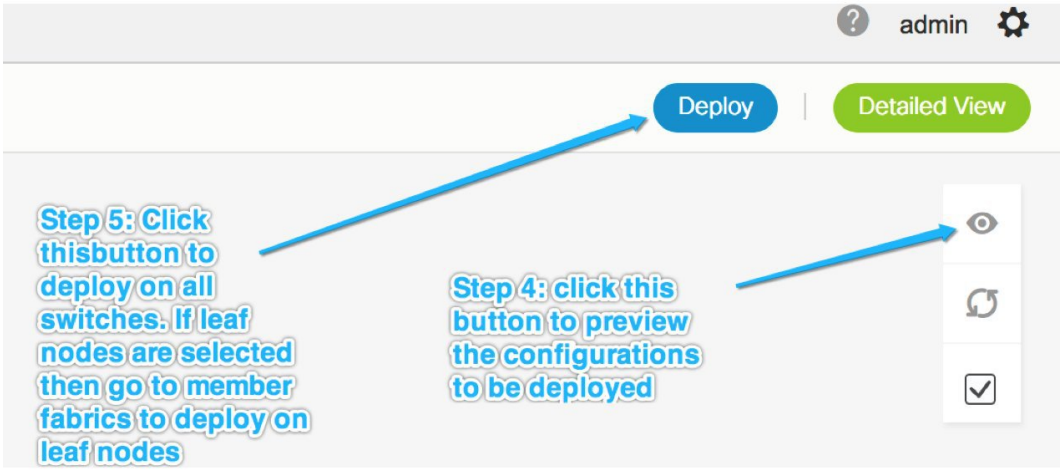
ネットワークと VRF は、[ネットワークと VRF（Networks and VRF）] ページの MSD コンテキストから作成できます。これらは、その MSD のすべてのメンバー ファブリックの BGW ノードに展開できます。

次のスクリーンショットは、ネットワークを選択して展開する方法を示しています。MSD ファブリック コンテキストから、ネットワークまたは VRF 展開用に任意のデバイスを選択できます。ただし、ネットワークまたは VRF は、ネットワーク展開画面の MSD コンテキストから BGW にのみ展開できます。リーフ展開は、ファブリック コンテキストまたはファブリック ビルダ コンテキストから実行できます。


Fabric Selection
Network / VRF Selection
Network / VRF Deployment
VRF View
Continue
Networks
Fabric Selected: MSD-Fabric
Step 1 navigate to the network deployment page of the relevant MSD fabric
Step 3: press the continue button to go the deployment page
Selected 1 / Total 1
Show All
Network Name
Network ID
VRF Name
IPv4 Gateway/Subnet
IPv6 Gateway/Prefix
Status
VLAN ID
MyNetwork_30000
30000
MyVRF_50000
11.0.0.1/24
NA
111
Step2 select NW(s) to be deployed


Data Center Network Manager
admin
Fabric Selection
Network / VRF Selection
Network / VRF Deployment
Deploy
Detailed View
Fabric Name: MSD-Fabric
Network(s) Selected
Network Extension Attachment - Attach extensions for given switch(es)
Fabric Name: MSD-Fabric
Deployment Options
Select the row and click on the cell to edit and save changes
MyNetwork_30000
Switch
VLAN
Extend
Interfaces
CLI Freeform
Status
N9K-3-BGW
111
MULTISITE
Applicable to BGW Leaf - VPC only
Freeform config
DEPLOYED
N9K-4-BGW
111
MULTISITE
Applicable to BGW Leaf - VPC only
Freeform config
OUT-OF-SYNC
Step 1 Check this box to multiple BGWs, then use GUI to select one or more BGWs, then this pop up will appear
Step 2: Check this boxes to select BGWs on which to deploy the NW(s)
Step 3, click this to move to deployment screen, repeat till all nodes on which NW(s) are to be deployed
Save


Deploy
Detailed View
Undiscovered



BGW でのレイヤ 3 ゲートウェイを使用したネットワークの展開

次の操作を行ってください。

Note SVI を展開するインターフェイスの選択は、vPC BGW セットアップでのみ使用できます。これはデバイスの制限であり、DCNM の制限ではありません。

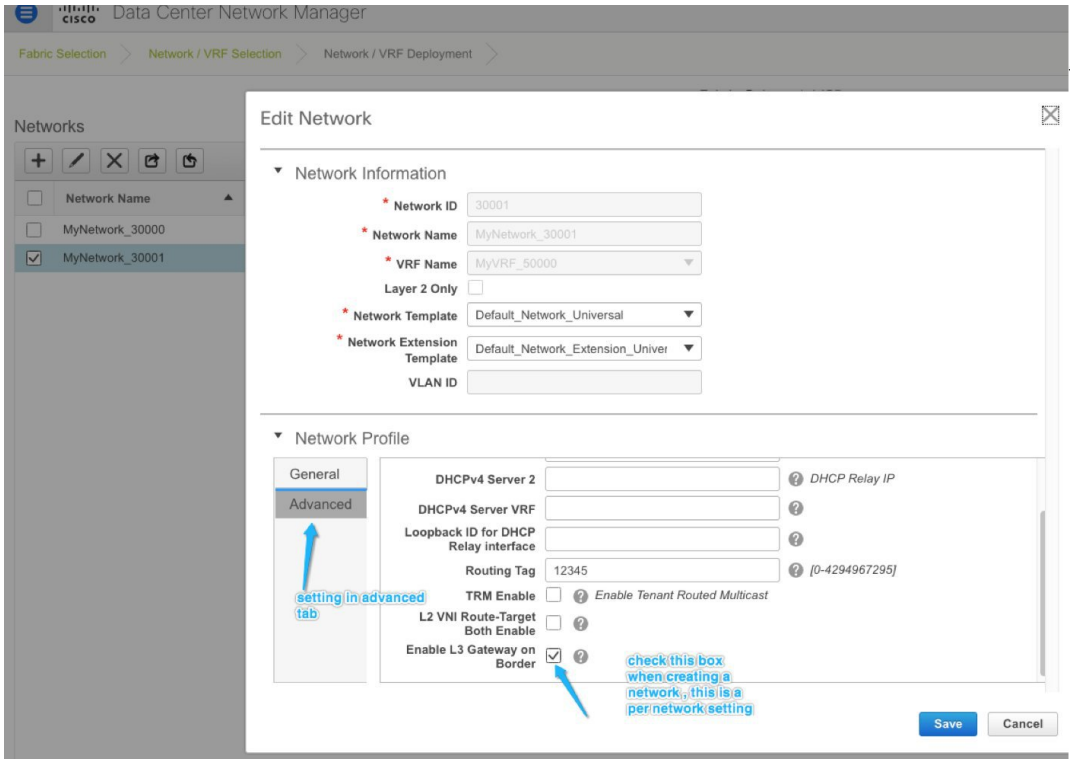
1. ボーダーデバイス（ボーダー、ボーダースパイン、ボーダーゲートウェイ、ボーダーゲートウェイ スパイン）にレイヤ 3 ゲートウェイを備えたネットワークを展開するには、次の手順を実行します。

   ネットワークを作成するときは、次の図に示すように、**[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ます。これはネットワーク全体の設定であるため、このネットワークがボーダーデバイスに展開されるたびに、レイヤ 3 ゲートウェイが展開されることに注意してください。これがボーダーのサブセットのみで必要な場合は、カスタム テンプレートが必要です。

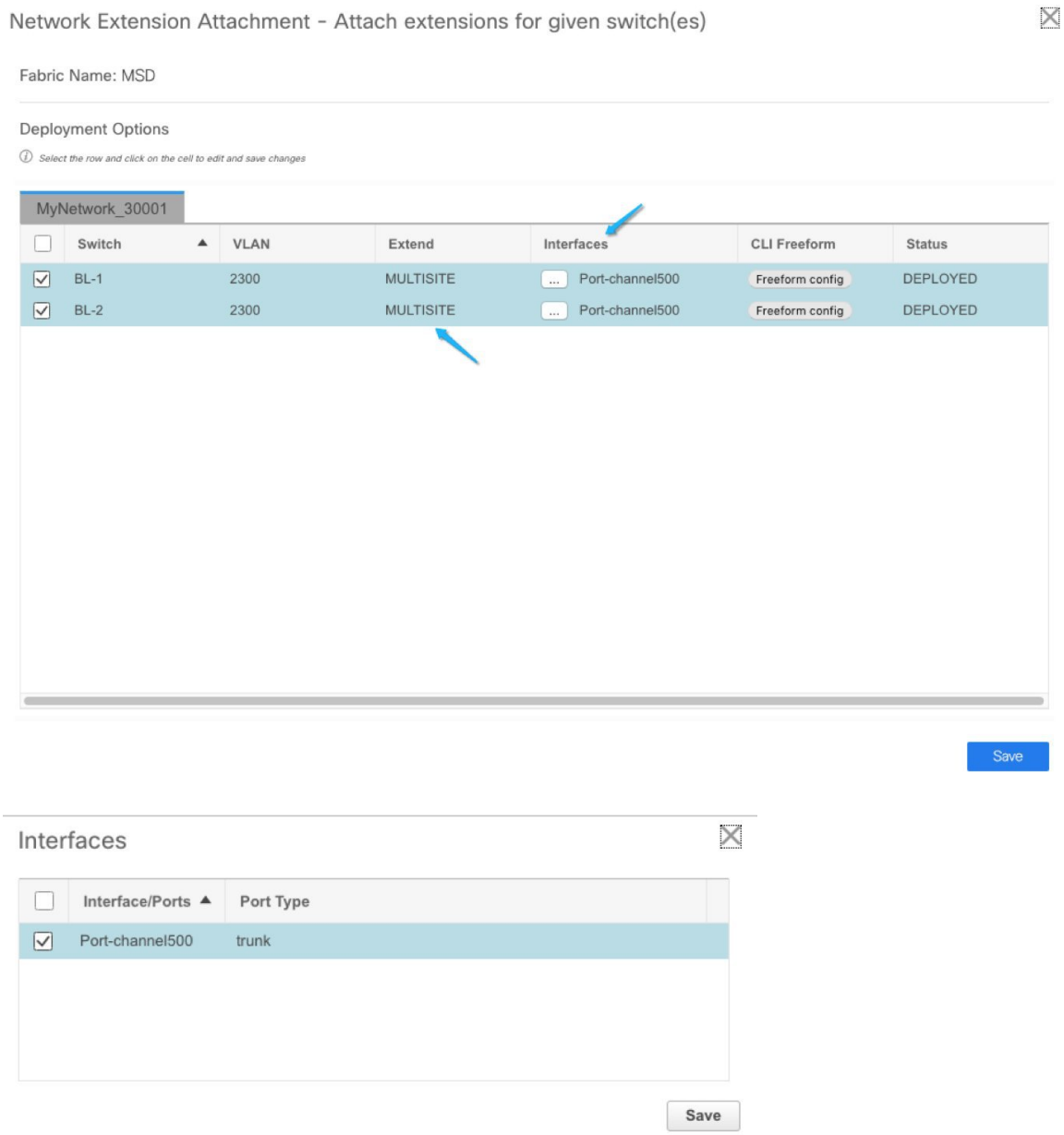
   ボーダーデバイスにネットワークを展開する場合、vPC BGW の場合は **[インターフェイス（Interface）]** 列でインターフェイスを選択します。

   リーフスイッチと同様に、候補ポートには **int_trunk_host_policy_11_1** が必要です。そうしないと、インターフェイス リストに含まれません。

   インターフェイス ポリシーは、**[制御（Control）] > [インターフェイス（Interfaces）]** タブで変更できます。



2. BGW の vPC ペアにネットワークを展開する場合は、[インターフェイス（Interfaces）] 列でインターフェイスを選択します。vPC ポートチャネルインターフェイスだけが候補のインターフェイスです。



レガシー サイト BGW（vPC-BGWs）の展開

非 VXLAN BGP EVPN（レガシー）と VXLAN BGP EVPN ファブリックを統合する推奨される方法は、VPC BGW のペアを使用することです。このメソッドについて詳細は、「vPC ボーダーゲートウェイを使用した VXLAN EVPN マルチサイトでの次世代 DCI ホワイトペーパー」を参照してください。

vPC BGW メソッドは、DCNM リリース 11.1(1) で推奨される Pseudo-Border Gateway メソッドに置き換わるものです。

このセクションでは、DCNM で実行できるホワイトペーパーのタスクについて、トポロジ例を使用して説明します。

前提条件

- レガシーネットワークはすでにメソッドでセットアップされています。このドキュメントの範囲から外れるためです。
- ファブリックの作成とマルチサイトのユースケースに精通していること。

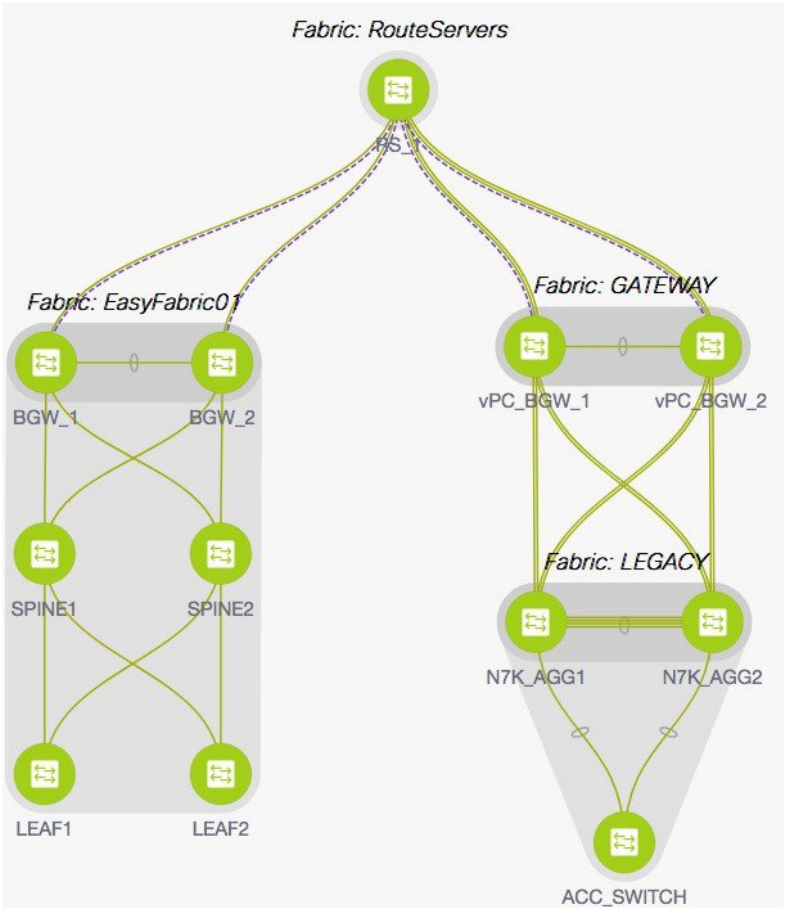
作業の概要

このセクションでは、次の情報について説明します。

1. DCNM を使用して作成されるファブリック：
    1. vPC ボーダーゲートウェイを備えた VXLAN ファブリック。
    2. VXLAN の Easy ファブリック。
    3. ルートサーバーの外部ファブリック。Direct to BGW トポロジを使用している場合、このファブリックはオプションであることに注意してください。
    4. レガシー デバイスをモニタするための外部ファブリック。
    5. すべてのファブリックのコンテナとしての MSD ファブリック。
2. vPC BGW からレガシー サイトへの vPC 接続。レガシーから BGW への vPC はアウトオブバンドで実行されることが期待されます。
3. マルチサイト アンダーレイ eBGP ファブリック間接続（IFC）の作成。
4. マルチサイト オーバーレイ eBGP IFC の作成。

トポロジの概要

トポロジの例を見てみましょう。



このトポロジには、次の 5 つのファブリックが含まれています。

1. **ゲートウェイ**

   このファブリックは、vPC ボーダーゲートウェイ用に作成されます。

   このファブリックは、スパイン ノードのない Easy ファブリックであり、次の特性を持つ通常の Easy ファブリックとして設定されています。

   - **[レプリケーション（Replication）]** タブで、**[レプリケーション モード（Replication Mode）]** が **[入力（Ingress）]** に設定されています。
   - vPC ボーダーゲートウェイのロールは BGW として設定されています。
   - IFC の作成方法は、ユーザーの好みに応じて手動または自動構成に設定されます。
   - ゲートウェイ ファブリックには、レガシー ファブリックに対する vPC インターフェイス構成があります。
   - MSDのメンバー ファブリック。

- 保存および展開操作は、EasyファブリックおよびMSDファブリックで実行されます。

2. **レガシー**

   このファブリックは、レガシー ネットワーク用に作成されています。ファブリック タイプは外部であり、モニタ モードで保持できます。外部ファブリックの手順に示すように、完全に構成されたデバイスはこのファブリックにインポートされます。

3. **EasyFabric01**

   これは、完全に機能する VXLAN ファブリックを表します。このファブリックのボーダー ゲートウェイ スイッチは、トポロジに従って、IFC を介してルート サーバーに接続されるか、レガシー ファブリックの BGW に直接接続されます。マルチサイトのユースケースに示されているように、両方のモデルがサポートされています。

4. **RouteServers**

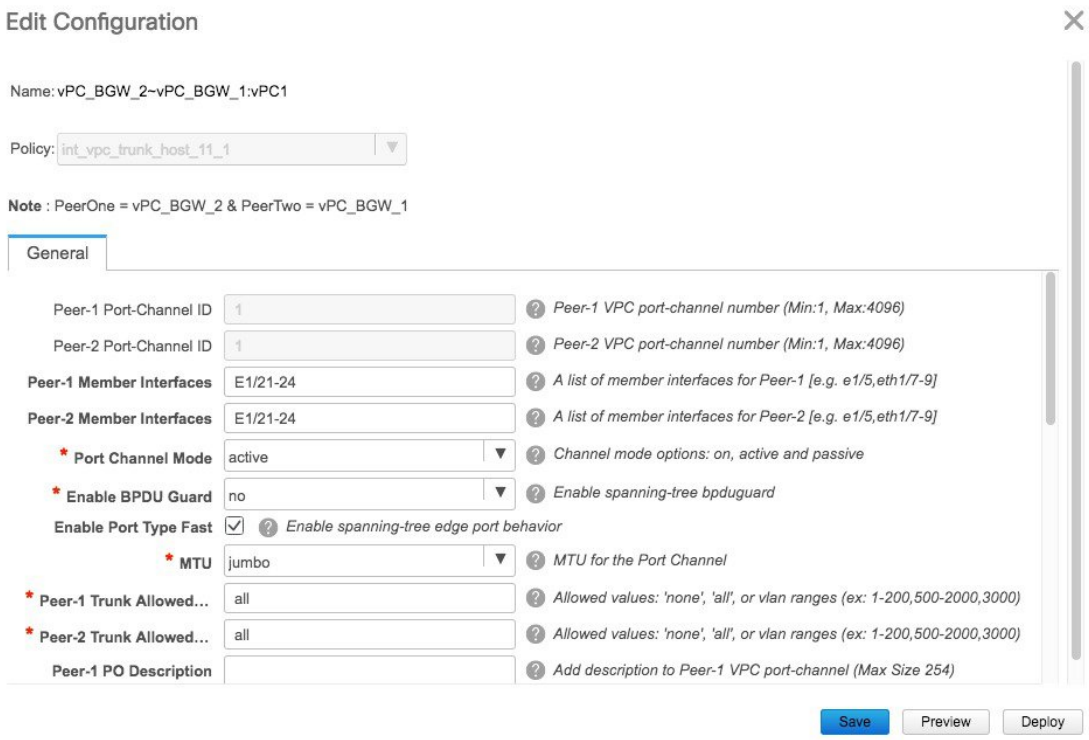
   このトポロジでは、ルート サーバーへの集中トポロジが使用されます。通常、冗長性の理由から、複数のルート サーバーが存在します。このファブリックは、マルチサイトのユース ケースに示されているように、タイプが外部です。

5. **MSD**

   MSD ファブリックは、メンバー ファブリックのベース マルチサイトを構成するために作成されます。上記の 4 つのファブリックはすべて、BGW ベースの MSD ファブリックにインポートされます。必要に応じて、すべてのアンダーレイおよびオーバーレイ IFC の自動構成を有効にすることができます。

vPC ボーダーゲートウェイからレガシー ネットワークへの vPC の構成

[GATEWAY] ファブリックの **[インターフェイスの管理（Manage Interfaces）]** ウィンドウで、**[追加（Add）]**（+）アイコンをクリックし、次の図に示すようにフィールドに情報を入力します。**[ポリシー（Policy）]** ドロップダウンリストから vPC ポリシーを選択し、トポロジのフィールドに入力します。



すべての情報を入力したら、**[プレビュー（Preview）]** をクリックして展開された構成をプレビューし、**[展開（Deploy）]** をクリックします。

マルチサイト アンダーレイ eBGP IFC の作成

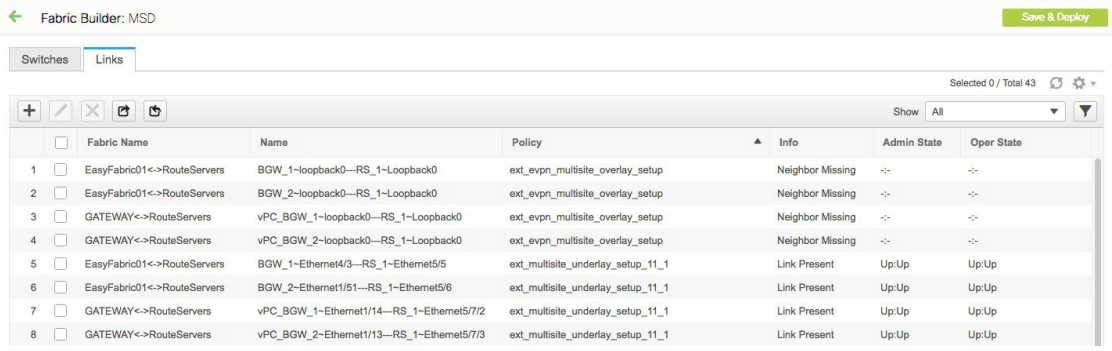
マルチサイト アンダーレイ構成は、マルチサイトのユースケースに示されている MSD と同じです。GUI または自動構成ベースのメソッドを選択して、トポロジに従って、コア ルータまたは他のファブリックの BGW に直接 IFC を作成します。

このトポロジでは、vPC ボーダーゲートウェイがルート サーバー（RS1）に物理的に接続され、1 つの MS アンダーレイ IFC が各 BGW（GATEWAY および EasyFabric01 内）から RS1 に構成されます。両方のメソッドについては、マルチサイトのユースケースで詳しく説明しています。

マルチサイト オーバーレイ IFC の構成

マルチサイト オーバーレイ IFC は、vPC BGW 間で、集中型ルート サーバーまたは **[EasyFabric01]** の各 BGW へのダイレクトのいずれかに作成する必要があります。トポロジの例では、各 BGW から RS1 への 1 つのオーバーレイ IFC があります。

このトポロジの IFC の概要を次の図に示します。



その他の参考資料

マニュアルのタイトルおよびリンク	マニュアルの説明
VXLAN EVPN マルチサイト設計および導入ホワイトペーパー	このマニュアルでは、マルチサイトの設計と展開について詳しく説明します。
VXLAN EVPN マルチサイトの構成	このマニュアルでは、マルチサイト ソリューションの手動構成について説明します。

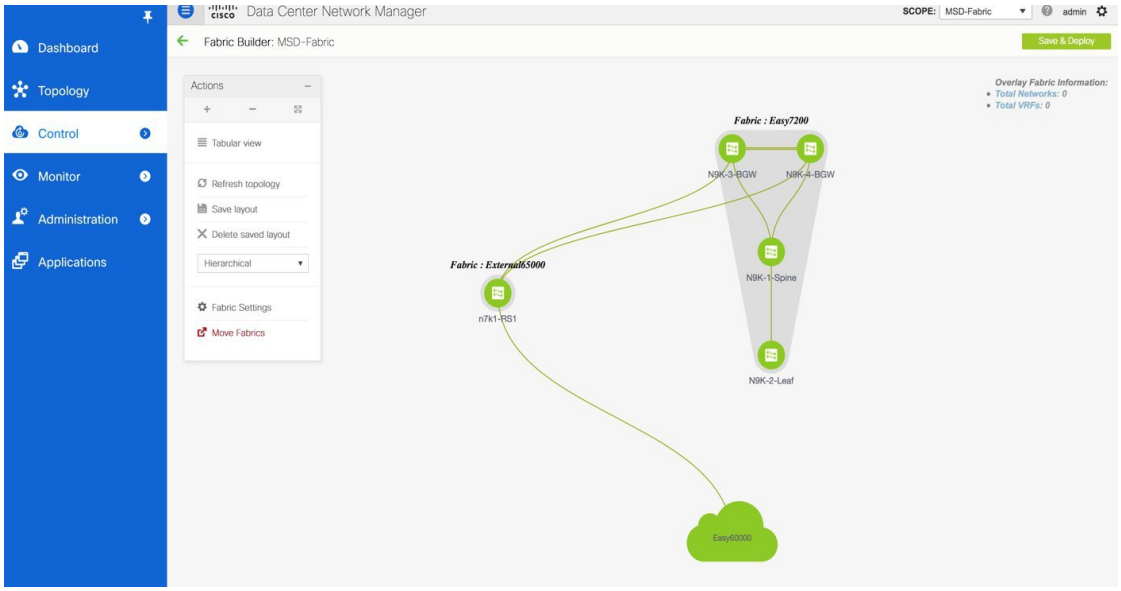
付録

マルチサイト ファブリックの基本構成：ボックス トポロジ

Easy7200 ファブリックでは、N9K-3-BGW と N9K-4-BGW は 2 つの物理インターフェイスを介して相互に接続されており、BGW は vPC ペアを形成しません。このようなトポロジは、ボックス トポロジと呼ばれます。IBGP セッションは、各物理接続で構成されます。1 つは Eth1/21 インターフェイス間で、もう 1 つは Eth1/22 インターフェイス間です。

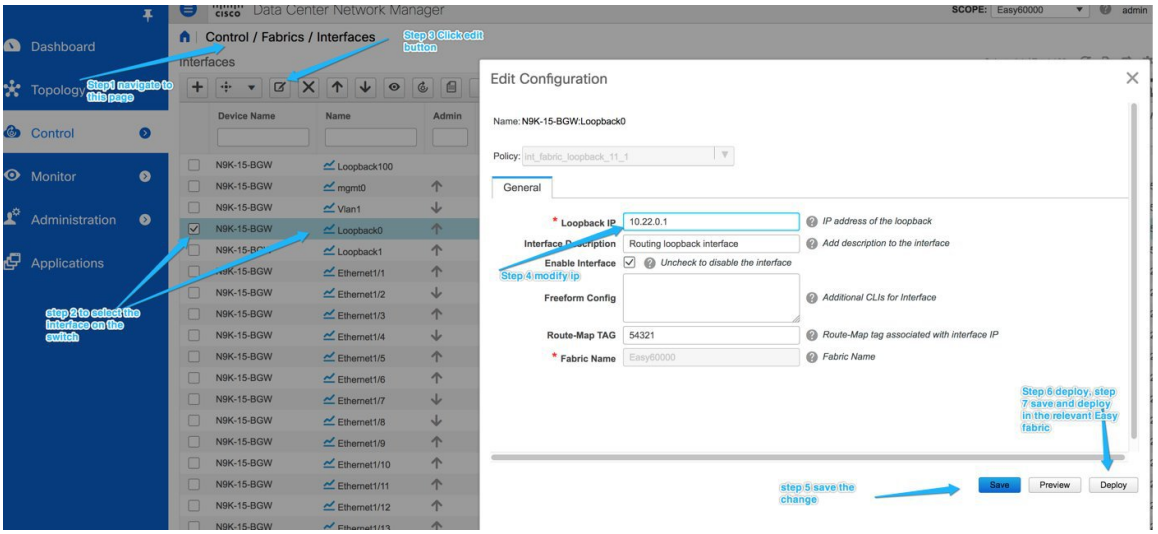
Easy7200 ファブリックのボックス トポロジの IBGP 構成

ファブリックに番号付きインターフェイスがある場合、次の構成が各ノードで生成されます。ファブリック インターフェイスが番号付けされていない場合、IBGP セッションは loopback0 アドレスを介して形成されます。



N9K-BGW-3	N9K-BGW-4
router bgp 7200 neighbor 10.4.0.17 remote-as 7200 update-source ethernet1/22 address-family ipv4 unicast next-hop-self	router bgp 7200 neighbor 10.4.0.18 remote-as 7200 update-source Ethernet1/22 address-family ipv4 unicast next-hop-self
router bgp 7200 neighbor 10.4.0.13 remote-as 7200 update-source ethernet1/21 address-family ipv4 unicast next-hop-self	router bgp 7200 neighbor 10.4.0.14 remote-as 7200 update-source Ethernet1/21 address-family ipv4 unicast next-hop-self
interface ethernet1/22 evpn multisite dci-tracking no switchport ip address 10.4.0.18/30 description connected-to-N9K-4-BGW--Ethernet1/22	interface Ethernet1/22 evpn multisite dci-tracking no switchport ip address 10.4.0.17/30 description connected-to-N9K-3-BGW-Ethernet1/22
interface ethernet1/21 evpn multisite dci-tracking no switchport ip address 10.4.0.14/30 description connected-to-N9K-4-BGW-Ethernet1/21	interface Ethernet1/21 evpn multisite dci-tracking no switchport ip address 10.4.0.13/30 description connected-to-N9K-3-BGW-Ethernet1/21

loopback0 ポリシーを変更して IP アドレスを変更する



ルート サーバー構成

ルート サーバーのオーバーレイおよび基本構成は、外部ファブリックがモニタ モードでない場合にのみ展開されます。

Note 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。詳細については、「制御」の章の「外部ファブリックの作成」トピックを参照してください。

ルート サーバーの基本構成：これらはルート サーバーに 1 回だけ展開され、対応するポリシーを介して編集または削除できます。ルータ サーバーのオーバーレイおよび基本構成は、外部ファブリックがモニタ モードでない場合にのみ展開されます。

設定	説明
`route-map unchanged permit 10` `  set ip next-hop unchanged`	–

`router bgp 65000`
`  address-family ipv4 unicast`
`  network /32`
	BGW が RS に到達する方法を認識できるように、RS1 の BGP ピアリング アドレスを eBGP アンダーレイ セッションに再配布するネットワーク コマンド。
	オペレータがルート サーバー ピアリング アドレスを BGW に配布するために別の方法を使用している場合、これは必要ありません。

設定	説明

interface ethernet1/22
  evpn multisite dci-tracking
  no switchport
  ip address 10.4.0.18/30
  description
connected-to-N9K-4-BGW--Ethernet1/22
	interface Ethernet1/22
	  evpn multisite dci-tracking
	  no switchport
	  ip address 10.4.0.17/30
	  description
	connected-to-N9K-3-BGW-Ethernet1/22

template peer OVERLAY-PEERING
    update-source loopback0
    ebgp-multihop 5
    address-family l2vpn evpn
      route-map unchanged out
      address-family l2vpn evpn
         retain route-target all
         send-community
         send-community extended
	外部ファブリックのノブは、send community がここに示されている形式で送信されるか、send-community both として送信されるかを制御します。
	このフォームによって永続的な CC の違いが生じる場合は、以下の「送信コミュニティの両方の属性の展開」セクションに示すように、外部ファブリックのデバイスでポリシーを編集します。

マルチサイト オーバーレイ IFC 構成

参照トポロジでは、Easy7200 ファブリックに 2 つの BGW があります。各 BGW は、ルートサーバーとの BGP オーバーレイ接続を形成します。

BGW	ルーティング サーバ

router bgp 7200
   neighbor
     remote-as 65000
     update-source loopback0
     ebgp-multihop 5
     peer-type fabric-external
     address-family l2vpn evpn
       send-community
       send-community extended
       rewrite-evpn-rt-asn
	router bgp 65000
	  neighbor 10.2.0.1
	   remote-as 7200
	   inherit peer OVERLAY-PEERING
	   address-family l2vpn evpn
	     rewrite-evpn-rt-asn
	router bgp 65000
	   neighbor 10.2.0.2
	   remote-as 7200
	   inherit peer OVERLAY-PEERING
	   address-family l2vpn evpn
	     rewrite-evpn-rt-asn

BGW とルート サーバーで生成された構成については、以下を参照してください。

マルチサイト アンダーレイ IFC 構成：すぐに使用できるプロファイル

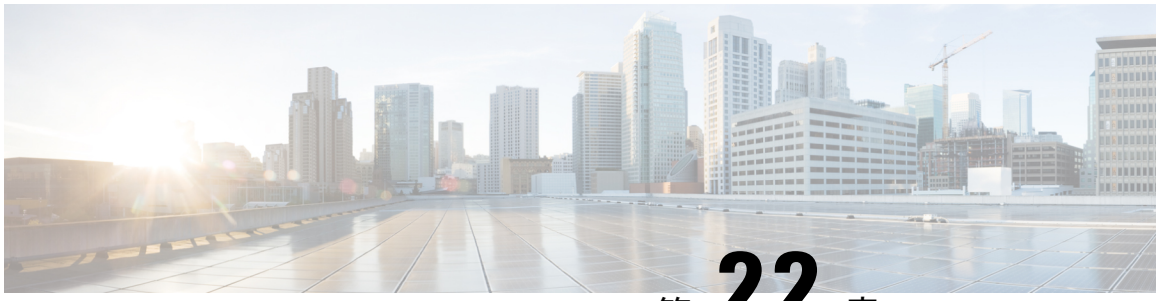
次の表は、すぐに使用できるプロファイルを使用して DCNM によって展開されたマルチサイト IFC 構成を示しています。IFC が 2 つの VXLAN ファブリックの間にある場合、両側に以下に示す BGW 構成があります。

BGW 構成	コア ルータ構成
router bgp 7200 neighbor 10.10.1.6 remote-as 65000 update-source ethernet1/47 address-family ipv4 unicast next-hop-self	router bgp 65000 neighbor 10.10.1.5 remote-as 7200 update-source ethernet7/4/1 address-family ipv4 unicast next-hop-self
interface ethernet1/47 mtu 9216 no shutdown no switchport ip address 10.10.1.5/30 tag 54321 evpn multisite dci-tracking	interface ethernet7/4/1 mtu 9216 no shutdown no switchport ip address 10.10.1.6/30 tag 54321

IP アドレスに付加されたタグ 54321 は、正しく機能するために必要ではなく、後続のリリースで削除されます。良性です。

第 V 部

L4 レイヤ7サービスのネットワーク プロビジョニング



第 22 章

L4-L7 サービスの基本的なワークフロー

レイヤ 4 ～ レイヤ 7 サービス

Cisco DCNM リリース 11.3(1) は、レイヤ 4～レイヤ 7 （L4～L7）サービス デバイスをデータセンター ファブリックに挿入する機能を展開し、これらのサービス デバイスにトラフィックを選択的にリダイレクトすることもできます。サービス ノードを追加し、サービス ノードとサービス リーフ スイッチの間にルート ピアリングを作成し、これらのサービス ノードにトラフィックを選択的にリダイレクトできます。

また、Cisco DCNM 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すビデオも視聴できます。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。詳細については、「ビデオ：Cisco DCNM のサービス リダイレクション」を参照してください。

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。DCNM 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。Cisco DCNM リリース 11.4(1) 以降、サービス ノードは vPC ボーダーゲートウェイにも接続できます。DCNM は、サービス リーフの新しいスイッチ ロールを定義しません。

DCNM 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。DCNM 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。

ルートピアリング

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。DCNM は、静的ルートと 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、DCNM 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。ルート ピアリングを選択し、**[サービス ノード（Service Nodes）]** ウィンドウで **[展開（Deploy）]** をクリックすると、L4-L7 サービスは、対応するサービス ネットワークと VRF 構成を、サービス ノードに接続されているリーフに展開します。**[プレビュー（Preview）]** をクリックして、ピアリングとサービス ネットワーク構成の両方を確認します。

自動的に作成されたサービス ネットワークは、**[制御（Control）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** ウィンドウにも表示されます。**[ネットワーク（Networks）]** ウィンドウで、対応する構成パラメータを表示および編集できます。ただし、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。

サービス ポリシー

DCNM 11.5(1) 以降、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、ボーダー 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 [制御（Control）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）] ウィンドウで定義されたネットワークにすることができます。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、DCNM 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、DCNM は 5 分ごとに統計を収集し、集計および分析のために ElasticSearch に保存します。**[サービス ノード（Service Nodes）]** ウィンドウの **[サービス ポリシー（Service Policy）]** タブにある **[Stats]** の下のグラフ線をクリックして、時間ベースの履歴統計を表示します。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。ファブリック ビルダを使用して 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。

MSD サポート

Cisco DCNM リリース 11.4(1) 以降、この機能はマルチサイト ドメイン（MSD）をサポートします。DCNM ファブリック スコープ セレクタから MSD メンバー ファブリックを選択し、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 ノードを接続し、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構成を展開します。レイヤ 4 ～ レイヤ 7 サービスを構成する手順の詳細については、レイヤ 4 ～ レイヤ 7 サービスの構成（1021 ページ） を参照してください。

RBAC サポート

Cisco DCNM リリース 11.4(1) 以降、レイヤ 4 ～ レイヤ 7 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、DCNM 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。

L4-L7 サービス操作	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
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

（注） 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、管理者はルートピアリングまたはサービス ポリシーを展開できません。また、サービス ノードが存在する外部ファブリックがファブリック モニタモードの場合、サービス ノードを削除するアイコンは表示されません。ファブリック モニタ モードからファブリックを削除して、サービス ノードを削除するアイコンを表示します。このアイコンは、admin ロールのアクセス権を持つユーザーにのみ表示されます。

レイヤ 4 ～ レイヤ 7 [サービス（Service）]ウィンドウは、ログインしているユーザーロールに基づいて表示され、ユーザが実行できるアクションを反映します。admin、stager、および operator ロールの[サービス ノード（Service Nodes）]ウィンドウのスクリーンショットの例を以下に示します。

図 *4:* 管理者のロール

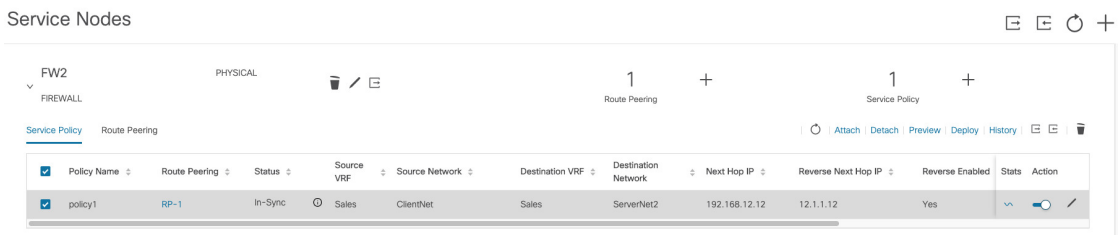


図 *5:* ステージャーのロール

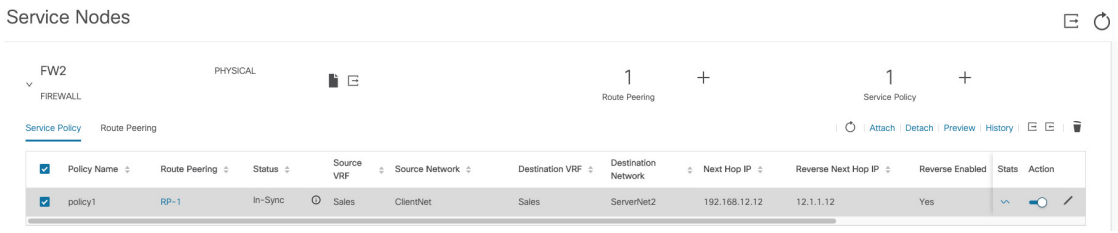
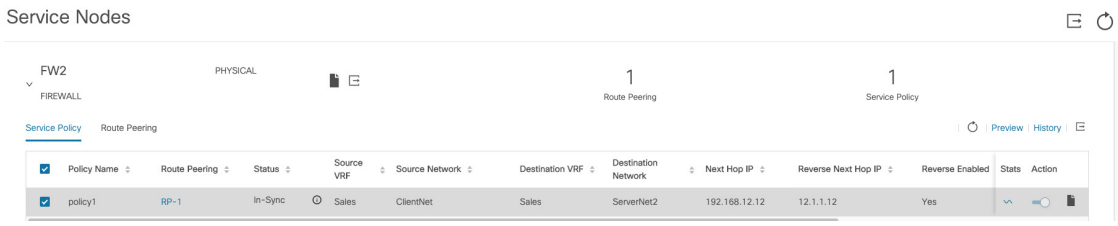


図 *6:* オペレーターのロール



境界スイッチの WAN インターフェイスでの PBR サポート

Cisco DCNM リリース 11.4(1) 以前のリリースでは、サービス ポリシーの作成中に「任意の」送信元または接続先ネットワークを指定する自由形式の構成テンプレートを使用して、サービス ポリシーを特定のスイッチ インターフェイスに手動で関連付ける必要があります。Cisco DCNM リリース 11.5(1) 以降、トップダウン構成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接続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。DCNM 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。PBR はレイヤ 3 ポート チャネル サブインターフェイスではサポートされないため、DCNM はレイヤ 3 ポート チャネルのサブインターフェイスを除外します。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

Cisco DCNM リリース 11.4(1) 以前のリリースでは、静的ルート ピアリングが使用されている場合、静的ルートはサービス リーフスイッチにのみ展開されます。Cisco DCNM リリース 11.5(1) 以降、レイヤ 4 ～ レイヤ 7 サービスは、静的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）に静的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。

レイヤ 4 ～ レイヤ 7 サービスの注意事項と制限事項

- DCNM の L4 ～ L7 サービスは、ファイアウォールやロードバランサなどのサービス ノードの管理またはプロビジョニングを行いません。
- L4 ～ L7 サービス機能は、**Easy_Fabric_11_1** 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 DCNM 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。
- Cisco DCNM リリース 11.5(1) 以降、仮想ネットワーク機能がサポートされています。
- Cisco DCNM リリース 11.5(1) 以降、レイヤ 4 ～ レイヤ 7 サービス REST API は、DCNM パッケージの REST API ドキュメントを介してアクセスできます。詳細については、『Cisco DCNM REST API 参照ガイド、リリース 11.5(1) 』を参照してください。
- 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、**[制御（Control）] > [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。

レイヤ 4 ～ レイヤ 7 サービス デバイスのタイプ

シスコ DCNM の L4 ～ L7 サービスは、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。

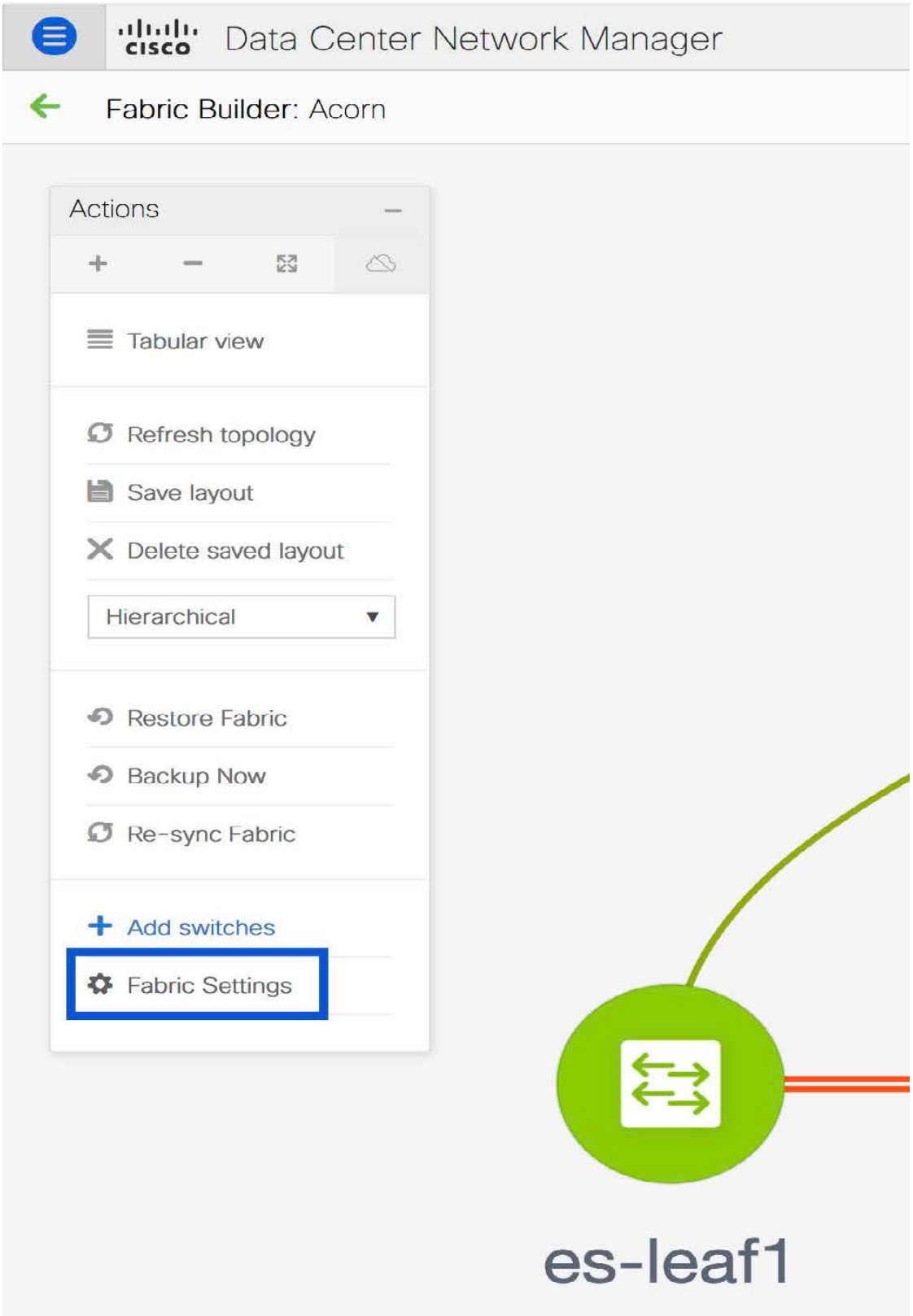
サポートされているファイアウォール ベンダーの例は、Cisco Systems、Palo Alto Networks、Fortinet、Check Point Software Technologies などです。

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。

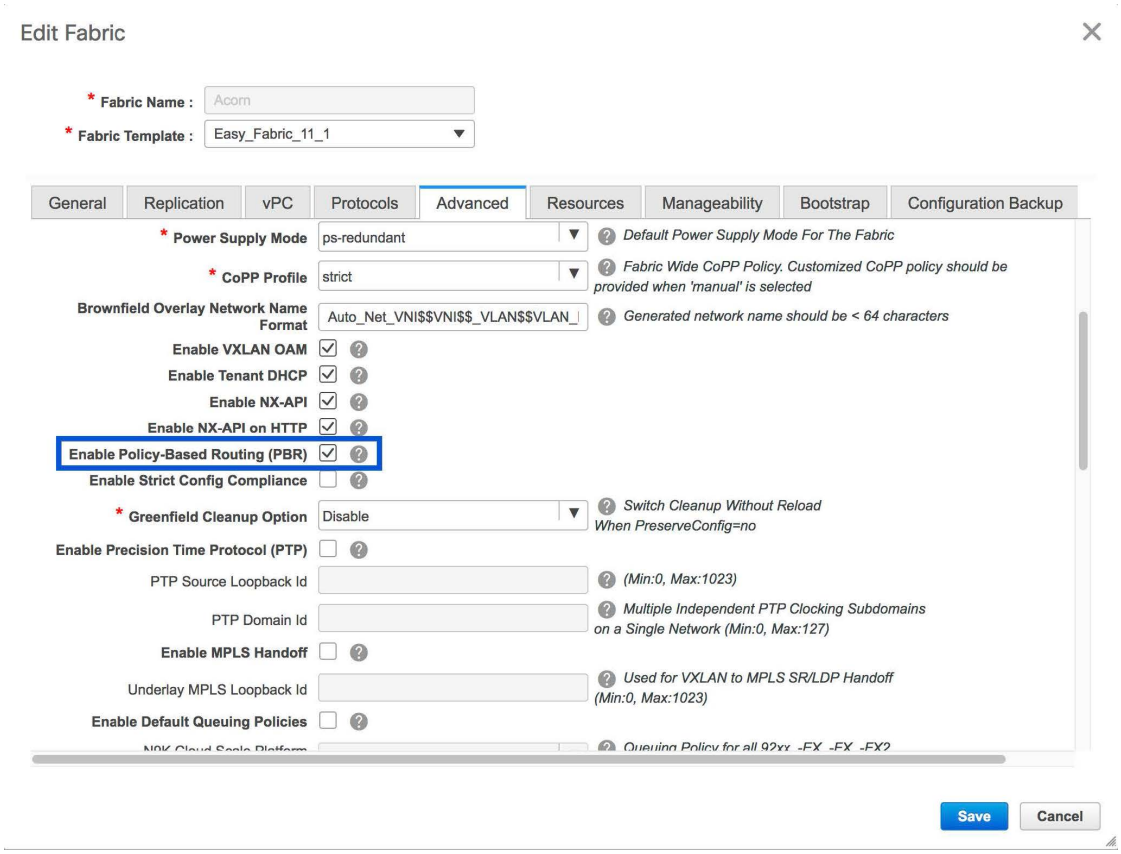
これらの例のリストは例として使用するものであり、すべてを網羅するものではありません。L4～L7 サービス接続は汎用であり、すべてのベンダー サービス ノードに適用されます。

L4 ～ L7 サービスのファブリック設定の構成

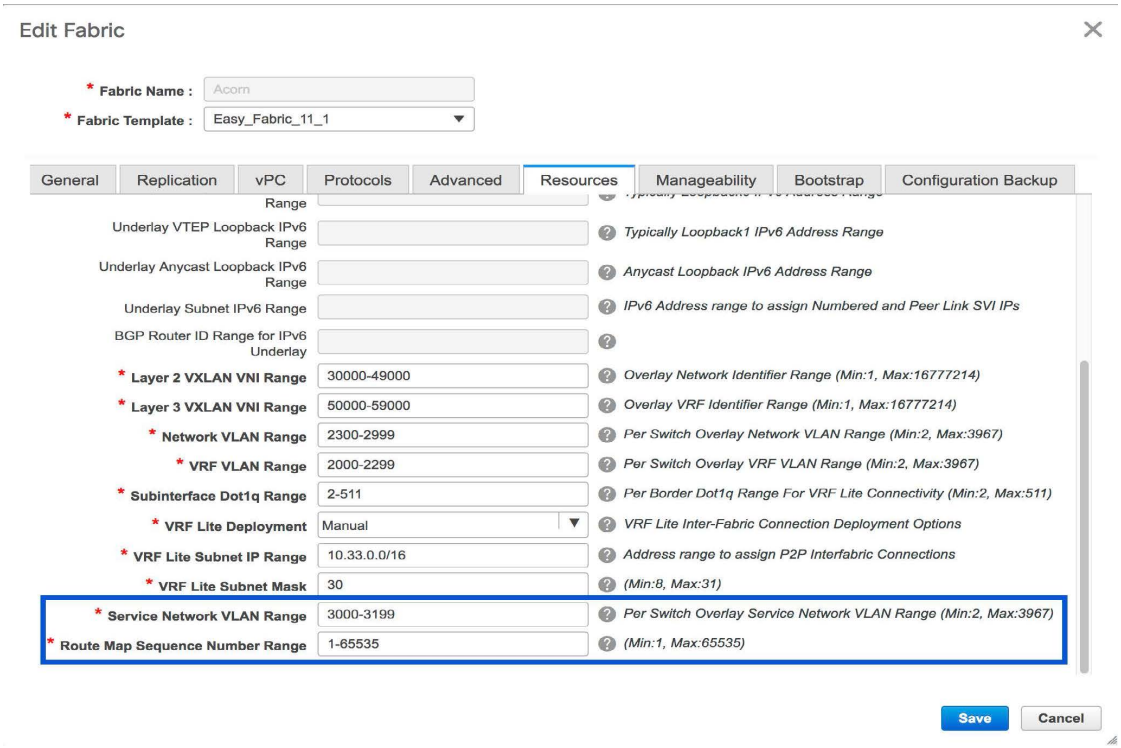
L4～L7 サービス機能を有効にするには、特定のファブリック設定を構成する必要があります。これらの設定を構成するには、**[ファブリック ビルダ（Fabric Builder）]** ウィンドウの **[アクション（Actions）]** の下にある **[ファブリックの設定（Fabric Settings）]** をクリックします。


Data Center Network Manager
Fabric Builder: Acorn
Actions
Tabular view
Refresh topology
Save layout
Delete saved layout
Hierarchical
Restore Fabric
Backup Now
Re-sync Fabric
Add switches
Fabric Settings
es-leaf1

[ファブリックの編集（Edit Fabric）] ウィンドウが表示されます。[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。



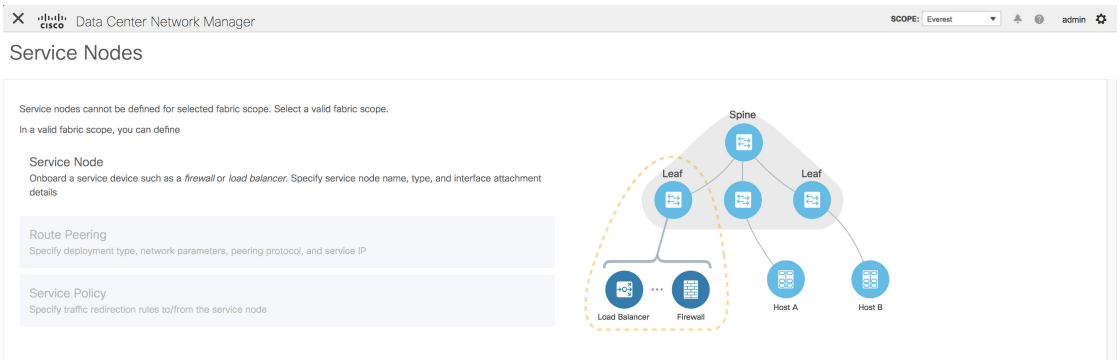
次に、**[リソース（Resources）]** をクリックします。**[サービス ネットワーク VLAN 範囲（Service Network VLAN Range）]** フィールドで VLAN 範囲を指定します。これは、スイッチ オーバーレイ サービス ネットワーク単位での VLAN 範囲です。最小許容値は 2 で、最大許容値は 3967 です。また、**[ルート マップ シーケンス番号の範囲（Route Map Sequence Number Range）]** フィールドの値を指定します。最小許容値は1、最大許容値は65535 です。**[保存して展開（Save and Deploy）]** をクリックして、更新後の構成を展開します。



レイヤ 4 ～ レイヤ 7 サービスの構成

Cisco DCNM Web UI で レイヤ 4 ～ レイヤ 7 サービス、または Elastic Service を起動するには、**[制御（Control）] > [ファブリック（Fabrics）] > [サービス（Services）]** を選択します。

[サービス ノード（Service Nodes）] ウィンドウが表示されます。有効なスイッチ ファブリックを選択して、そのファブリック内のサービス ノード、ルート ピアリング、およびサービス ポリシーを表示または定義します。

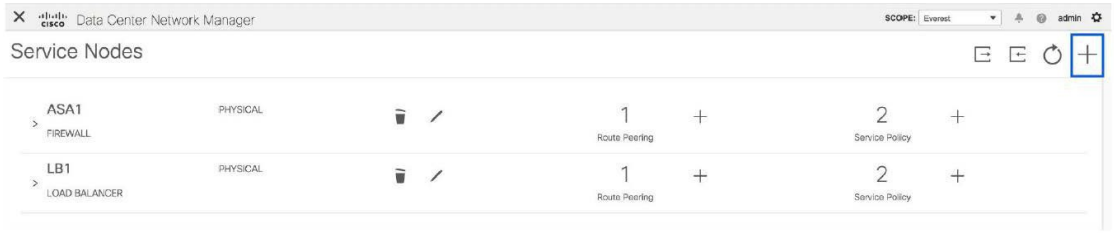


（注） Cisco DCNM リリース 11.5(1) 以降、過去 15 分間に更新されたサービス ノード、ルート ピアリング、およびサービス ポリシーが強調表示されます。

レイヤ 4 ～ レイヤ 7 サービスの構成手順は、次の手順で構成されます。

サービス ノードの作成

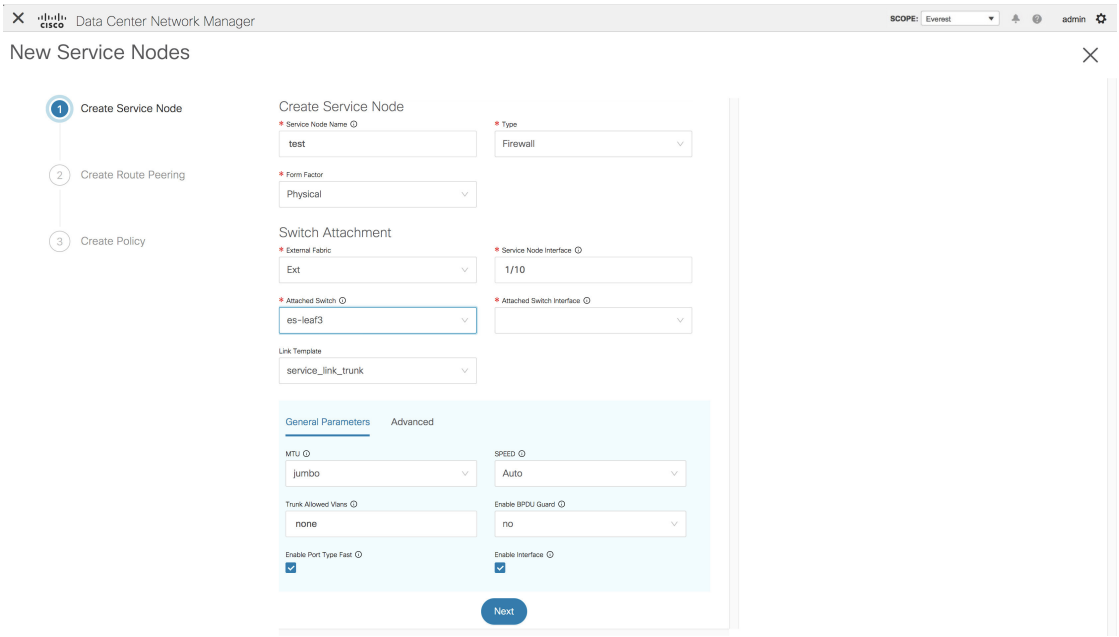
サービス ノードを作成するには、**[サービスノード（Service Nodes）]** ウィンドウの右上にある **[+]** をクリックして、**[新しいサービスノード（New Service Node）]** ウィンドウを表示します。



[新しいサービス ノード（New Service Node）] ウィンドウには、**[サービス ノードの作成（Create 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 つの手順があります。

[サービス ノードの作成（Create Service Node）] ウィンドウには、[サービス ノードの作成（Create Service Nod）] 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 [service_link_trunk]、[service_link_port_channel_trunk]、および [service_link_vpc] を選択できます。

図 *7:* 例：リンク テンプレート *- service_link_trunk*



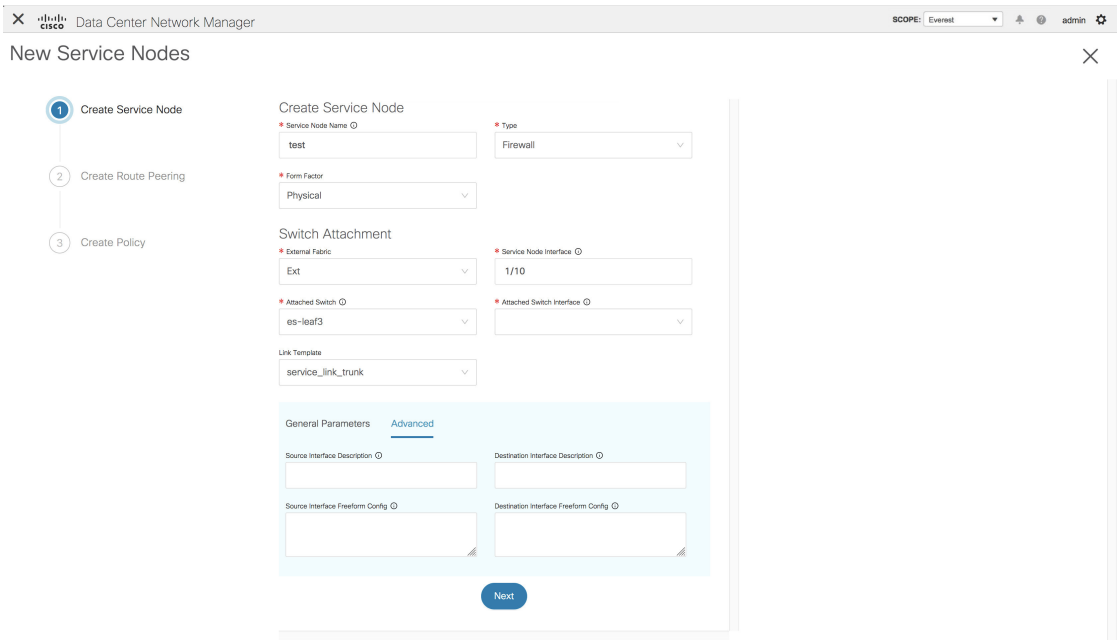


図 *8 :*例：リンク テンプレート - *service_link_port_channel_trunk*

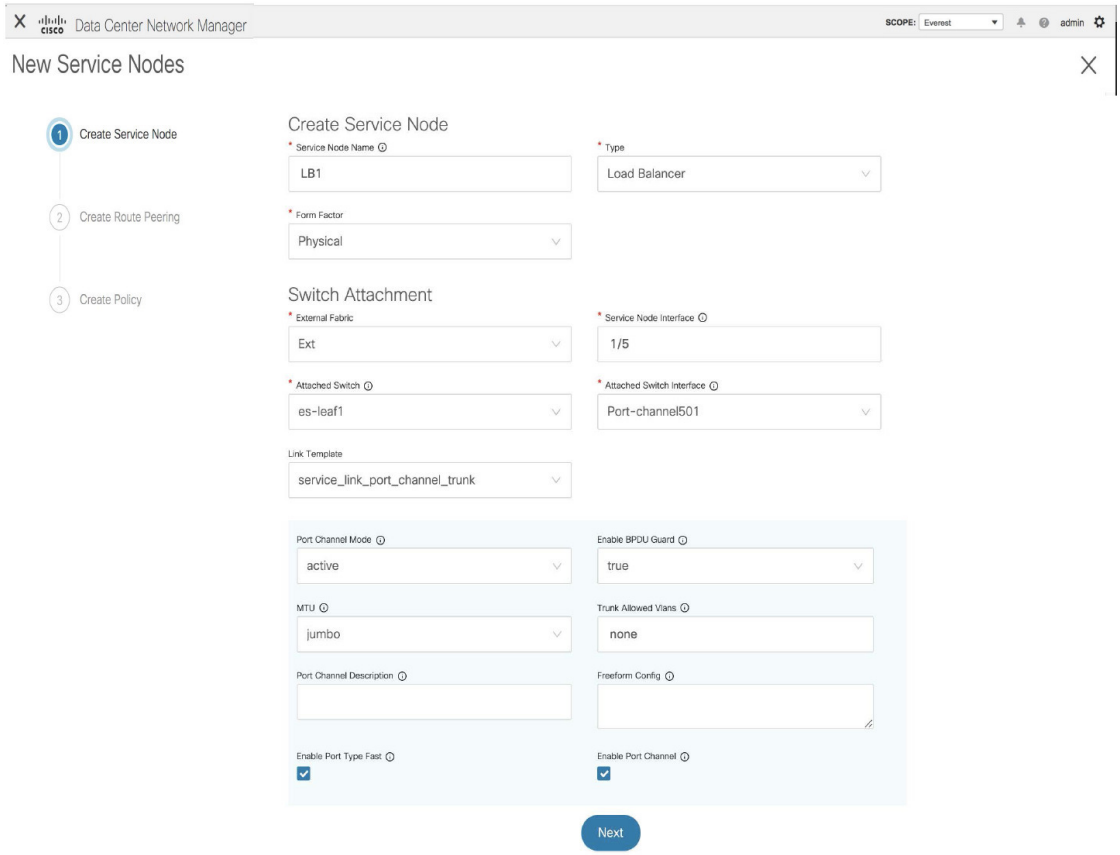


図 *9*：例：リンク テンプレート - *service_link_vpc*

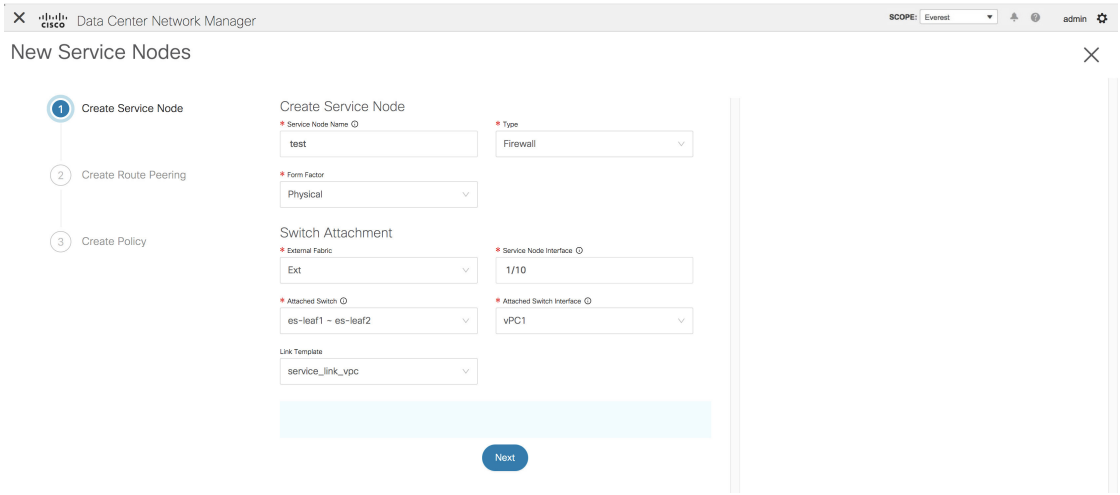
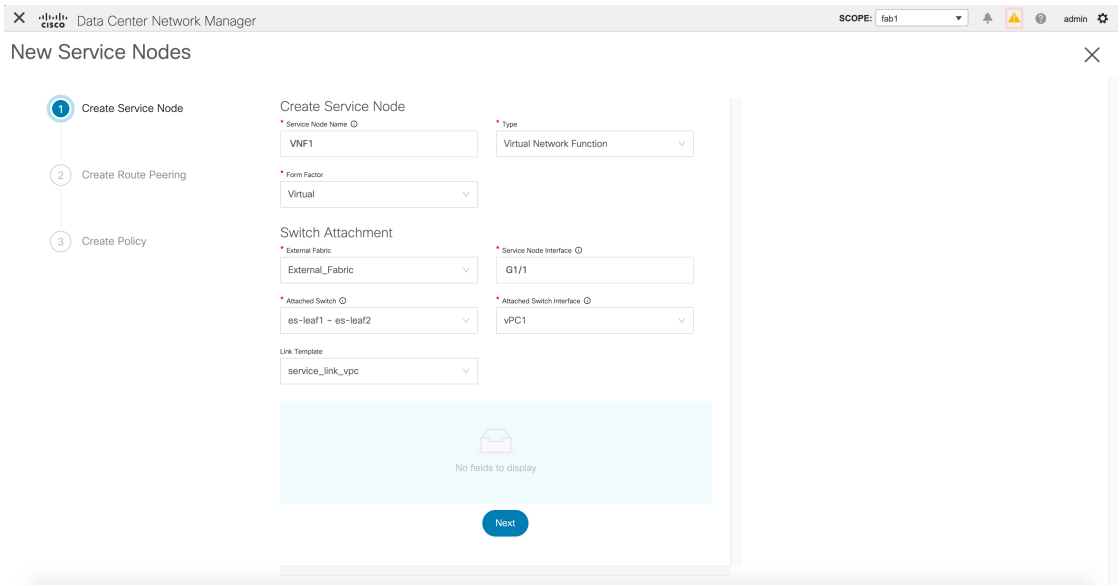


図 *10*：例：タイプ - 仮想ネットワーク機能

（注） DCNM リリース 11.5(1) 以降、仮想ネットワーク機能がサポートされています。



[サービス ノードの作成（Create 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。このウィンドウのフィールドの詳細については、**[i]** アイコンにカーソルを合わせてください。

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。

[タイプ（Type）]：ファイアウォールまたはロードバランサを選択します。

[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。

スイッチ アタッチメント

[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。

[アタッチされたスイッチ（Attached Switch）]：ドロップダウンリストからスイッチを選択します。

[アタッチされたスイッチ インターフェイス（Attached Switch Interface）]：ドロップダウン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）]** ドロップダウンリストから vPC ペアを選択すると、vPC チャネルが **[アタッチされたリーフスイッチ インターフェイス（Attached Leaf Switch Interface）]** ドロップダウン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）]** ドロップダウン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）」を参照してください。

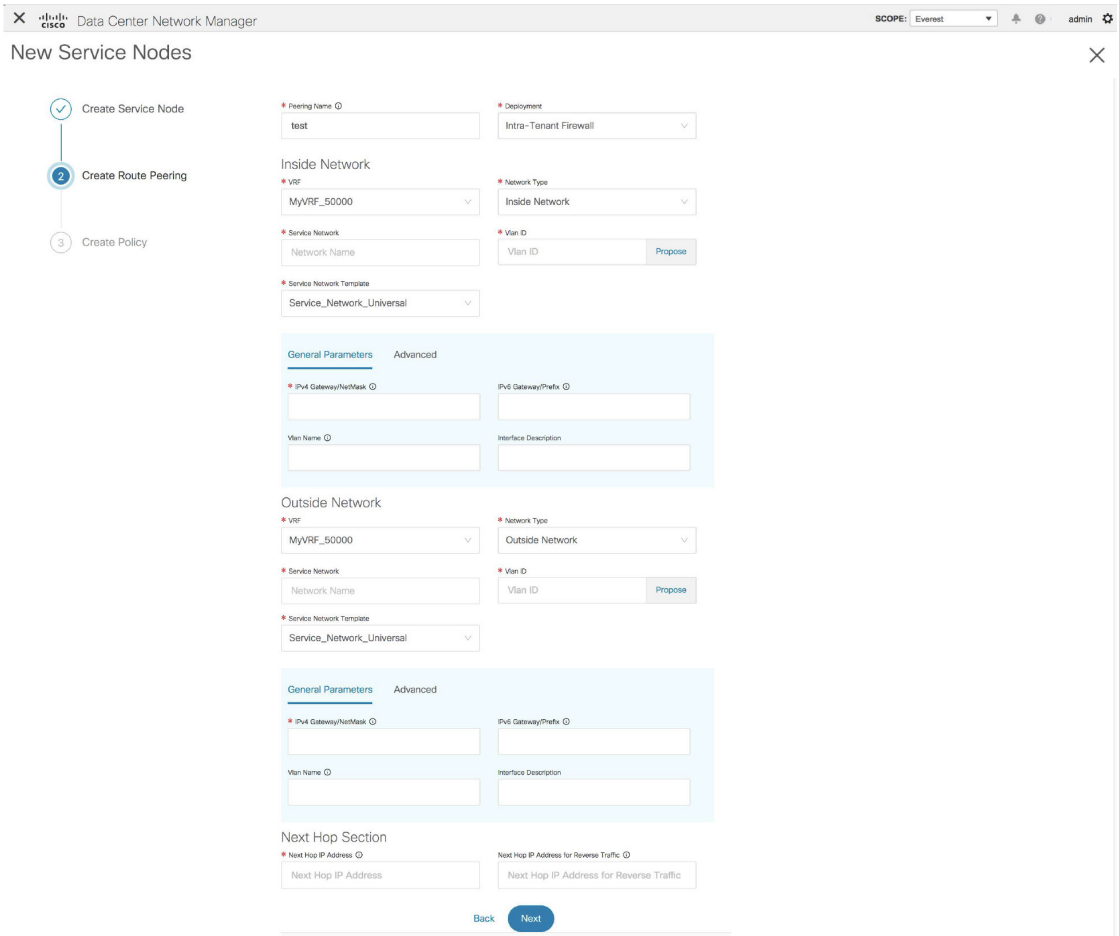
[**次へ（Next）**] をクリックします。新しいサービス ノードが正常に作成されたことを示すポップアップ ウィンドウが表示され、**[ルート ピアリングの作成（Create Route Peering）]** ウィンドウが表示されます。

ルート ピアリングの作成

[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、**[サービス ノードの作成（Create Service Node）]** ウィンドウで選択した展開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） **[制御（Control）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** ウィンドウでは、サービス ネットワークの削除は許可されていません。

例：テナント内ファイアウォールの展開



テナント内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。このウィンドウのフィールドの詳細については、**[i]** アイコンにカーソルを合わせてください。

[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）]：[テナント内ファイアウォール（Inter-Tenant Firewall）] を選択します。

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 ー 3967 です。定義済みのサービス 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（Service Network Template）]：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）」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）]：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 ー 3967 です。定義済みのサービス 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（Service Network Template）]：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）」を参照してください。

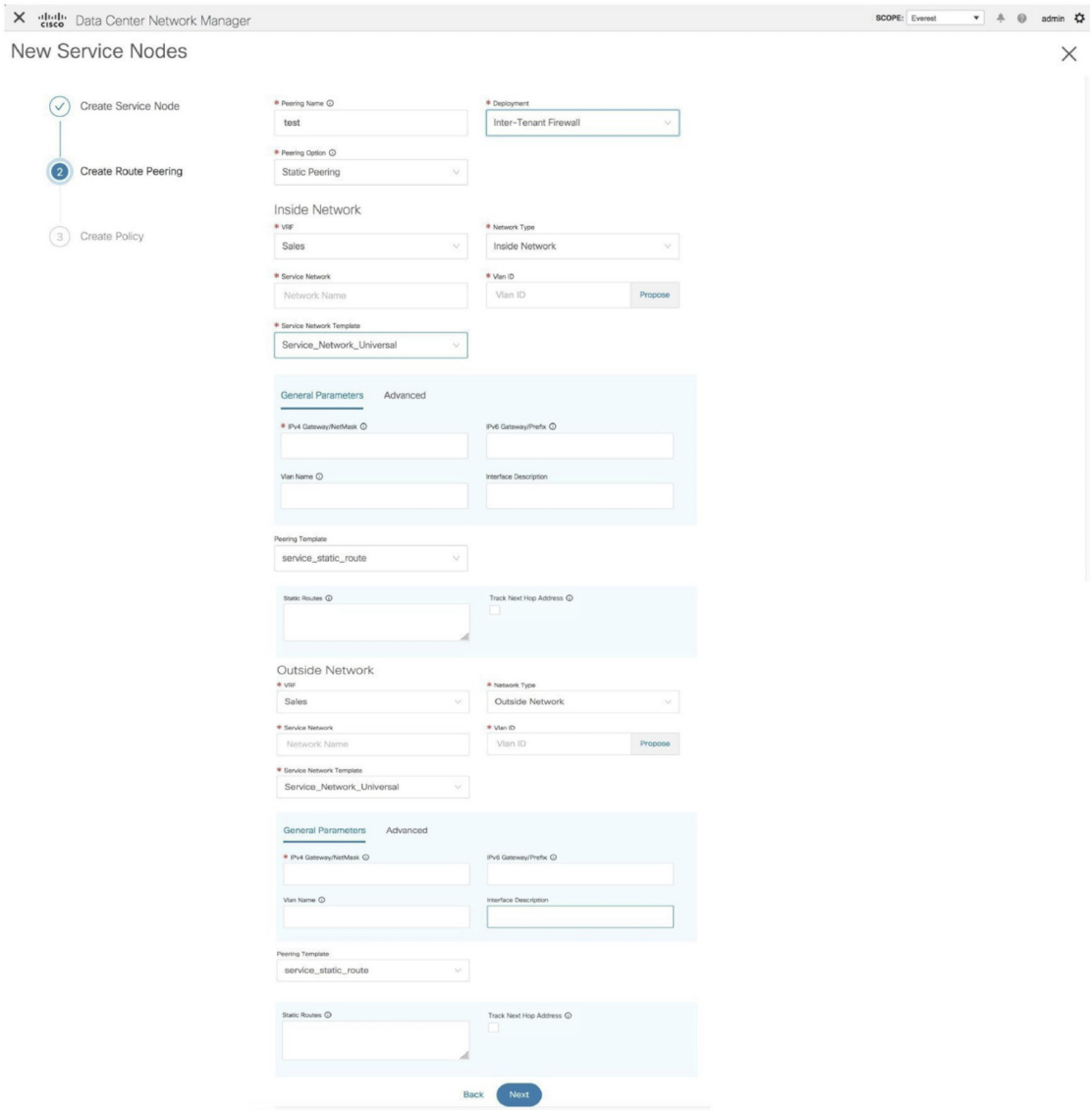
ネクスト ホップ セクション

[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）]：ドロップダウンリストから [サービス ネットワーク名（service network name）] を選択します。

[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（Service Network Template）]：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）」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）」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。

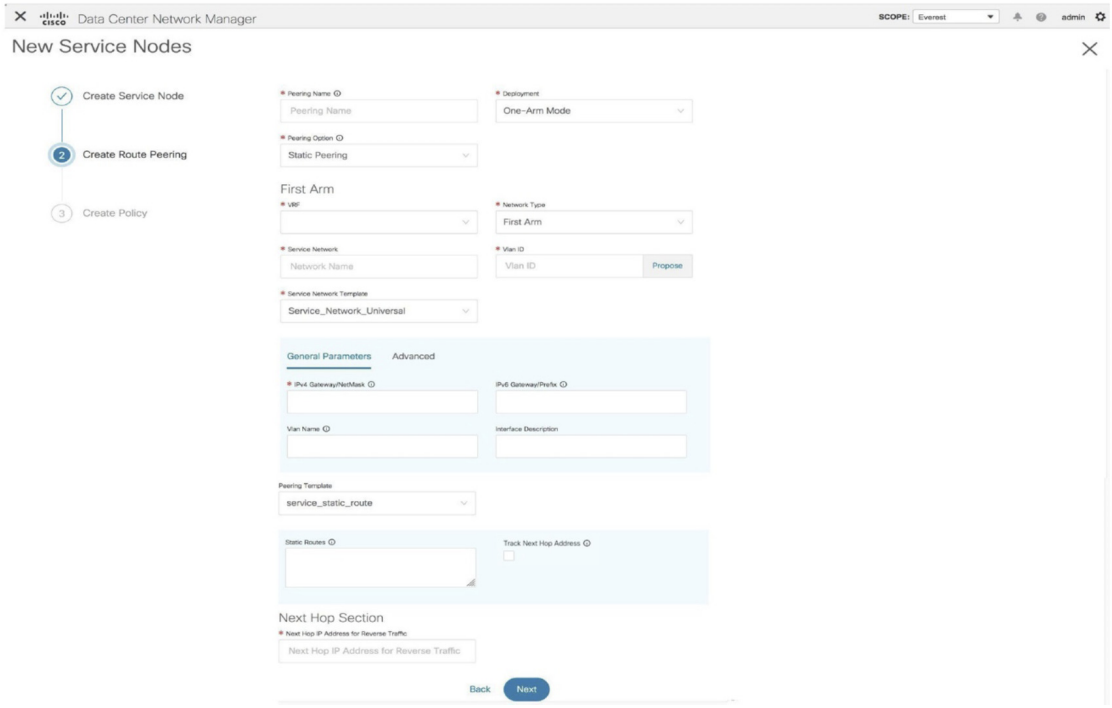
[サービス ネットワーク（Service Network）]：ドロップダウンリストから [サービス ネットワーク名（service network name）] を選択します。

[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（Service Network Template）]：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）」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）」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 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）]：[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。

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）]：ドロップダウンリストから [サービス ネットワーク名（service network name）] を選択します。

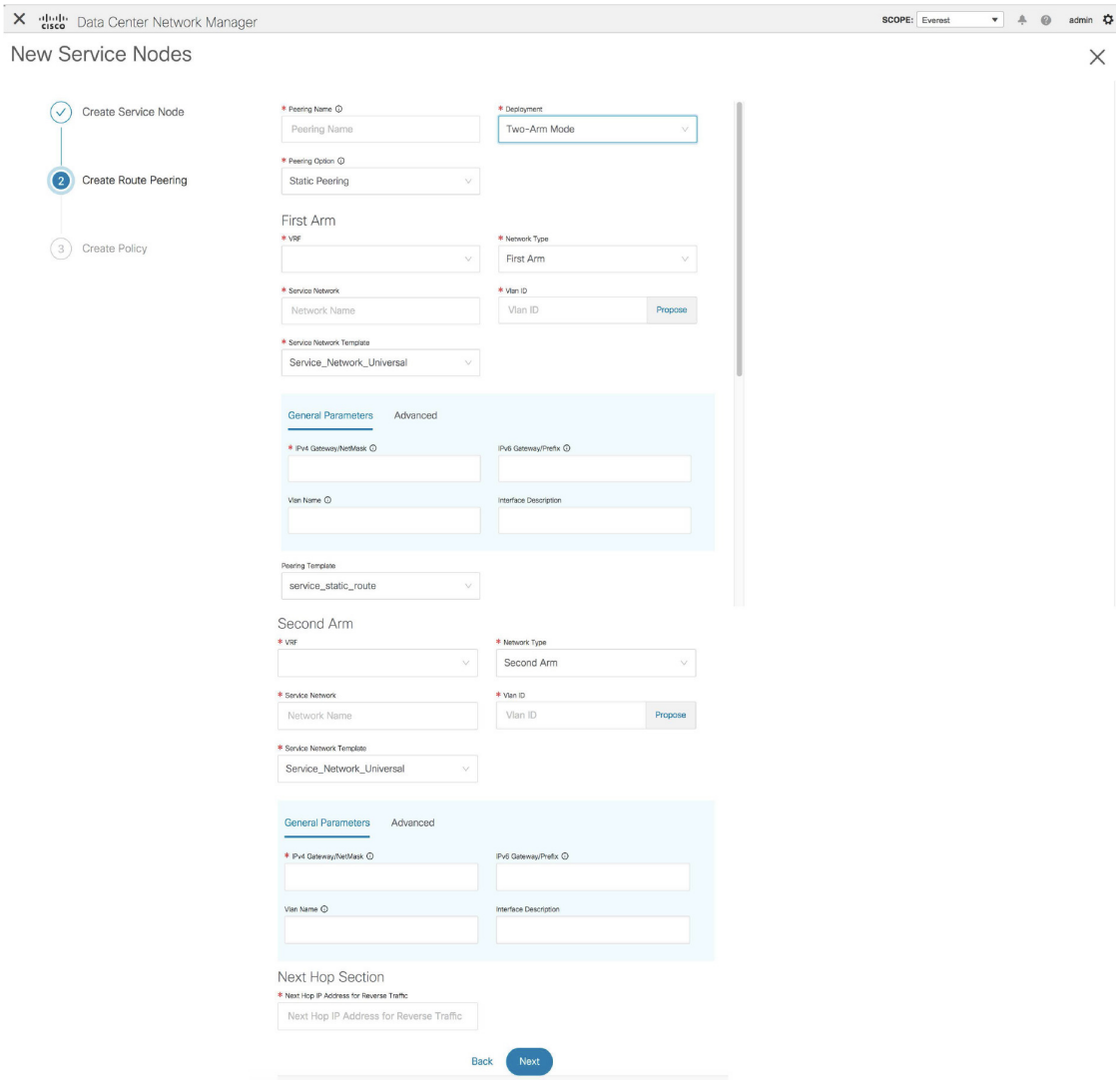
[VLAN ID]：VLAN ID を指定します。有効な ID の範囲は 2 ー 3967 です。定義済みのサービス ネットワーク VLAN 範囲プールから値を取得するには、[提案（Propose）] をクリックします。

[サービス ネットワーク テンプレート（Service Network Template）]：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）」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）」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）]：ドロップダウンリストから [サービス ネットワーク名（service network name）] を選択します。

[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（Service Network Template）]：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）」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）」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 Arm）] 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 ー 3967 です。定義済みのサービス 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。

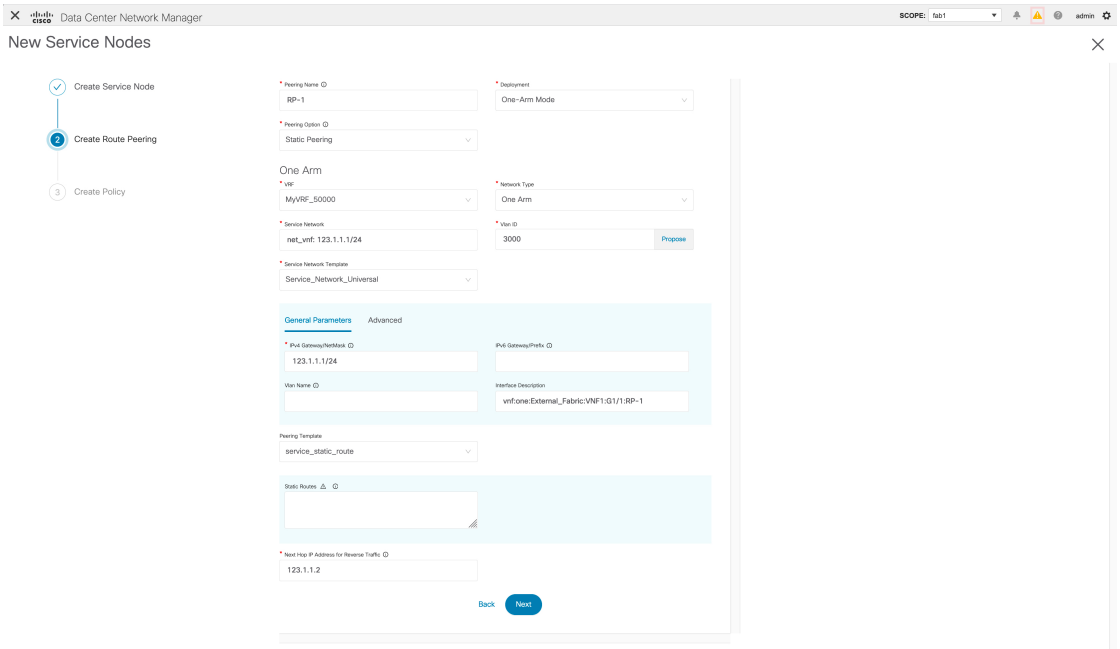
[サービス ネットワーク テンプレート]：ドロップダウンリストから [Service_Network_Universal] テンプレートを選択します。テンプレート フィールドについての詳細は、「テンプレート （Templates）」を参照してください。

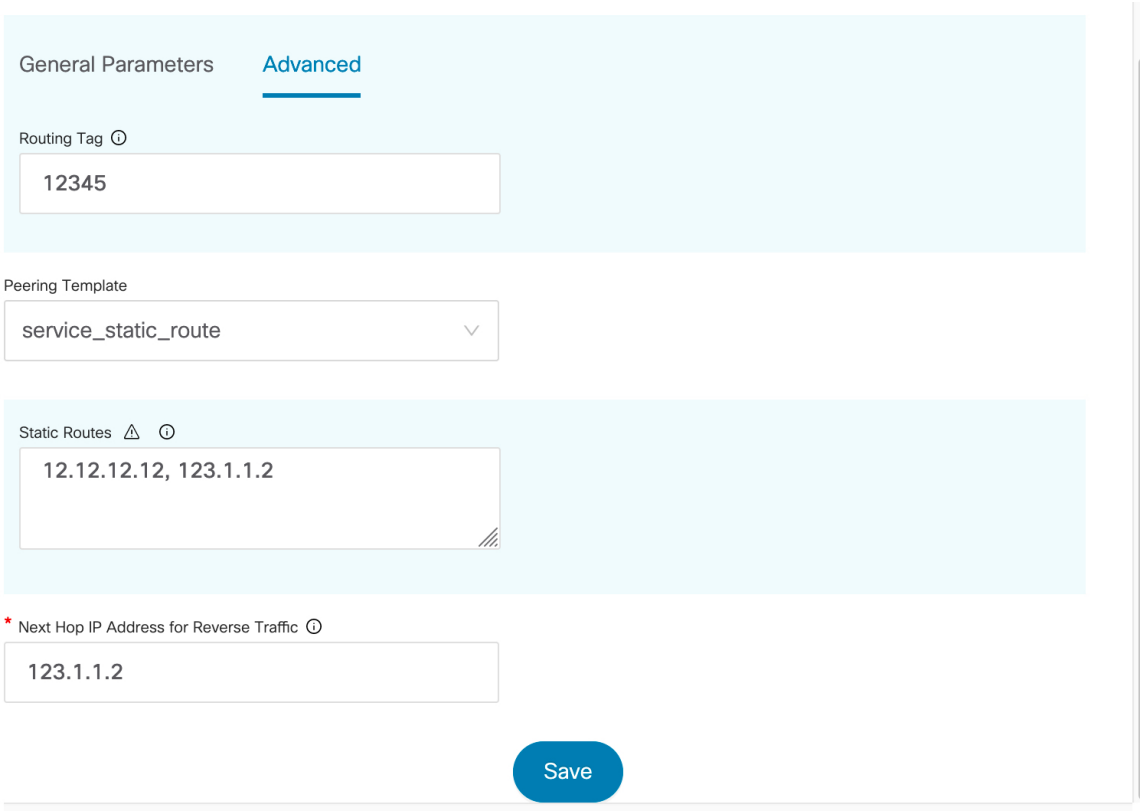
ネクスト ホップ セクション

[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。

[次へ（Next）] 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）]：ドロップダウンリストから [サービス ネットワーク名（service network name）] を選択します。

[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（Service Network Template）]：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。

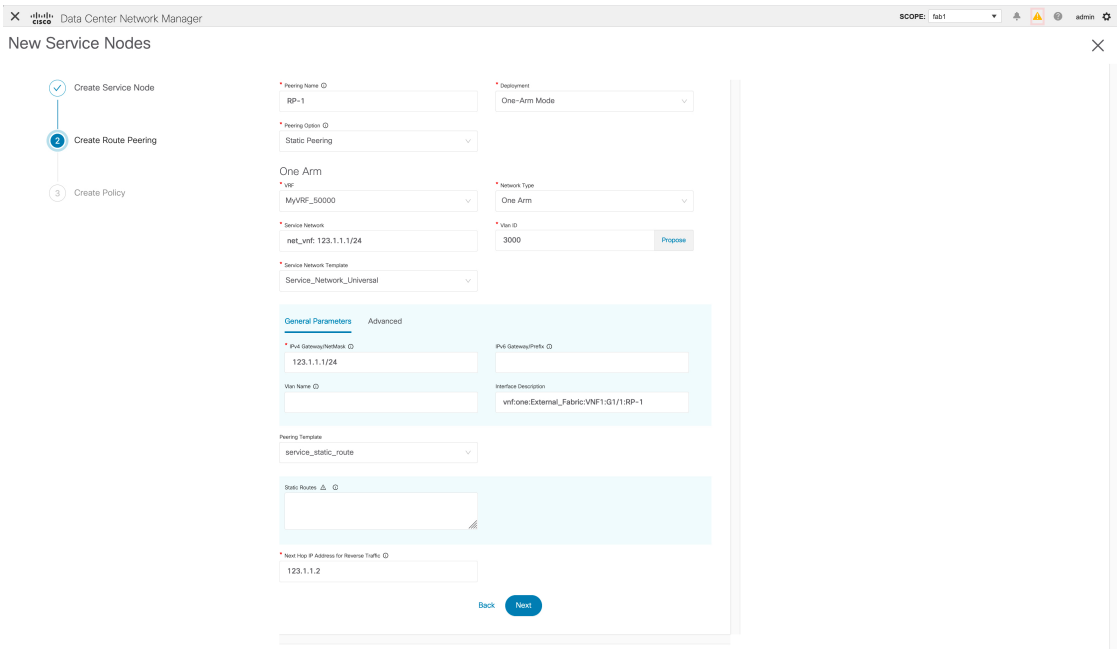
[ピアリング テンプレート（Peering Template）]：ドロップダウンリストから [service_static_route] または [service_ebgp_route] を選択します。テンプレート フィールドについての詳細は、「テンプレート」を参照してください。

[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。

[次へ（Next）] 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

[ポリシーの作成（Create Policy）] ウィンドウが次のように表示されます。



[ポリシーの作成（Create 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。

[ポリシー名（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ピアリング オプションを選択します。

[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。

[接続先 VRF 名（Destination VRF Name）]：ドロップダウンリストから接続先 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。

[接続先ネットワーク（Destination Network）]：ドロップダウンリストから IP アドレスを選択します。

[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。

[ポリシー テンプレート名（Polocy Template Name）]: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）」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。

[宛て先ポート（Destination Port）] : 宛て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。

Cisco DCNM リリース 11.4(1) 以降、**[詳細（Advanced）]** タブが導入されました。この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、Cisco DCNM リリース 11.3(1) に記載されているように、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）」を参照してください。

[作成（Create）] 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、100Mb、1Gb、10GB、25Gb、40Gb、または 100Gb に変更できます。

[トランク許可済み VLAN（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。

[BPDU ガードの有効化（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。

[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。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（Enable Interface）]：インターフェイスを無効化するには、チェックボックスをオフにします。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。

[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。

[接続先インターフェイスの説明（Destination Interface Description）]：接続先インターフェイスの説明を入力します。

[送信元インターフェイスの自由形式構成（Source Interface Freeform Config）]：送信元インターフェイスの追加 CLI を入力します。

[接続先インターフェイスの自由形式構成（Destination Interface Freeform Config）]：接続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。

[BPDU ガードの有効化（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。

[トランク許可済み VLAN（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。

[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。

[自由形式の構成（Freeform Config）]：必要な自由形式の構成 CLI を指定します。

[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。デフォルトでは有効になっています。

[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。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（IPv4 Gateway/Netmask）]：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 ゲートウェイ/プレフィックス（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 名（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。

[ループバック IP（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

[ネイバー IPv6（Neighbor IPv6）]：ネイバーの IPv6 アドレスを指定します。

[ループバック IPv6（Loopback IPv6）]：ループバックの IPv6 アドレスを指定します。

[ルートマップ タグ（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（Local 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化するには、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有効化（Enable Interface）]：インターフェイスを無効化するには、チェックボックスをオフにします。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。

[宛て先ポート（Destination Port）]：宛て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。

[ネクスト ホップ オプション（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 名（ACL Name）]：生成されたアクセス制御リスト（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。

[リバース トラフィックの ACL 名（ACL Name for reversed traffic）]：リバース 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。

[ルートマップ一致番号（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（Route map match number for reversed traffic）]：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。

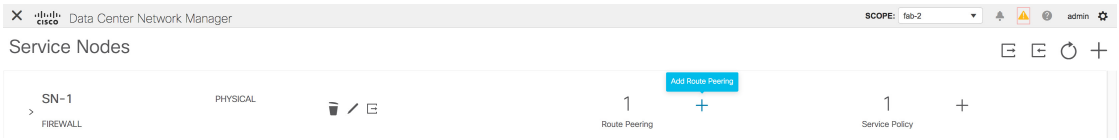
また、特定の要件に基づいてテンプレートをカスタマイズすることもできます。テンプレートについての詳細は、「[テンプレート ライブラリ（Template Library）]」を参照してください。

ルート ピアリングの追加

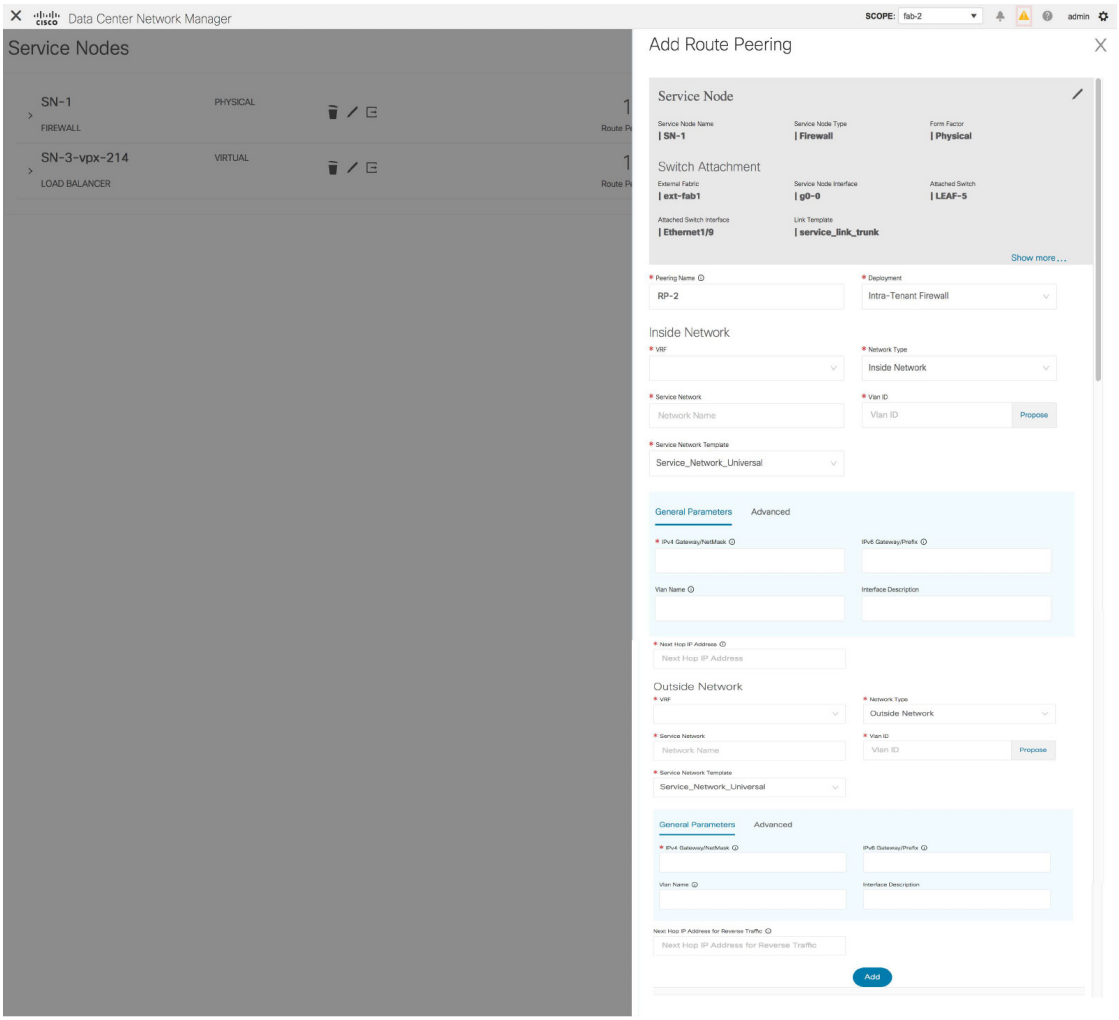
Cisco DCNM Web UI からルート ピアリングを追加するために、次の手順を実行します。

Procedure

ステップ 1 **[サービス ノード（Service Nodes）]** ウィンドウで、**[ルート ピアリングの追加（Add Route Peering）]** アイコンをクリックします。



ステップ 2 **[ルート ピアリングの追加（Add Route Peering）]** ウィンドウが表示されます。



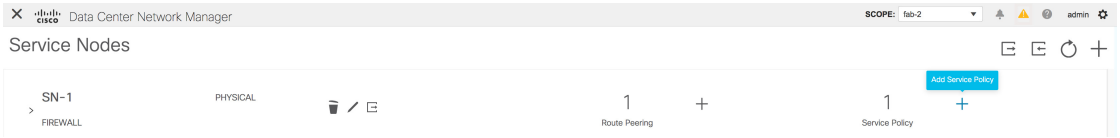
必要なパラメータを指定し、**[追加（Add）]** をクリックします。特定のフィールドの詳細については、**[i]** アイコンにカーソルをホバーして（合わせて）ください。

サービス ポリシーの追加

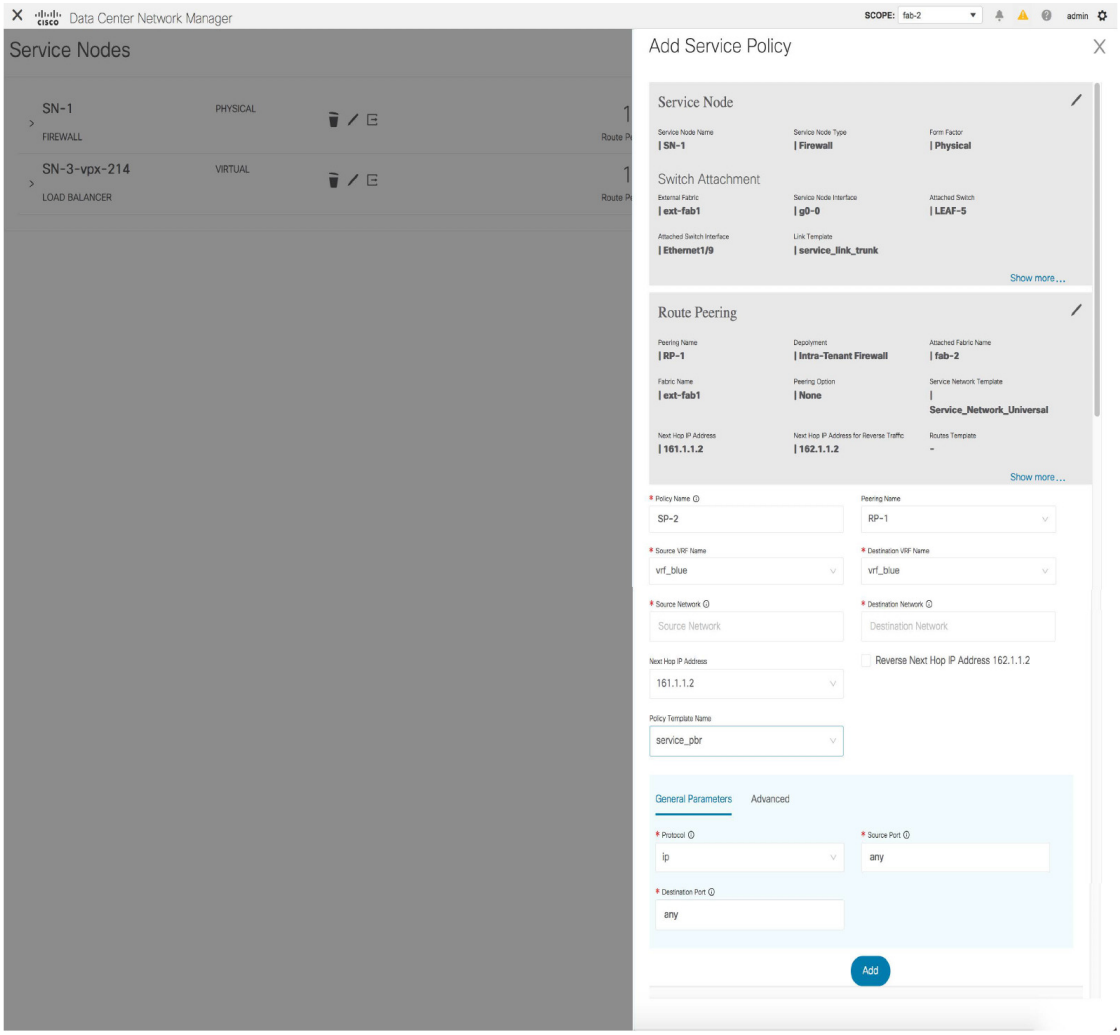
Cisco DCNW Web UI からサービス ポリシーを追加するには、次の手順を実行します。

Procedure

ステップ 1 **[サービス ノード（Service Nodes）]** ウィンドウで **[サービス ポリシーの追加（Add Service Policy）]** アイコンをクリックします。



ステップ 2 **[サービス ポリシーの追加（Add Service Policy）]** ウィンドウが表示されます。



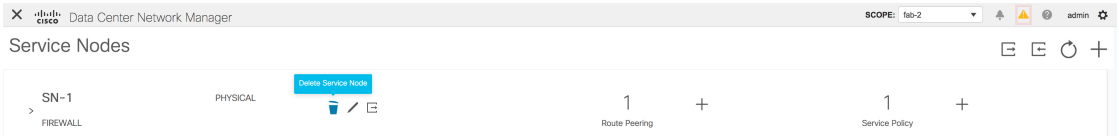
必要なパラメータを指定し、**[追加（Add）]** をクリックします。特定のフィールドの詳細については、**[i]** アイコンにカーソルをホバーして（合わせて）ください。

サービス ノードの削除

Cisco DCNW Web UI からサービス ノードを削除するには、次の手順を実行します。

Procedure

ステップ 1 **[サービス ノード（Service Nodes）]** ウィンドウで **[サービス ノードの削除（Delete Service Node）]** アイコンをクリックします。



ステップ 2 ノードを削除する必要があるかどうかを確認するポップアップ ウィンドウが表示されます。[削除（Delete）] をクリックします。

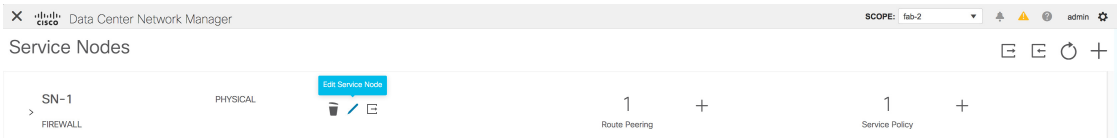
Note 削除する必要があるサービス ノードにルート ピアリングまたはサービス ポリシーが関連付けられていないことを確認します。サービス ノードに関連付けられているサービス ポリシーまたはルート ピアリングがある場合、サービス ノードを削除する前にサービス ノードに関連付けられているルート ピアリングまたはサービス ポリシーを削除する必要があることを示す警告が出され、削除がブロックされます。

サービス ノードの編集

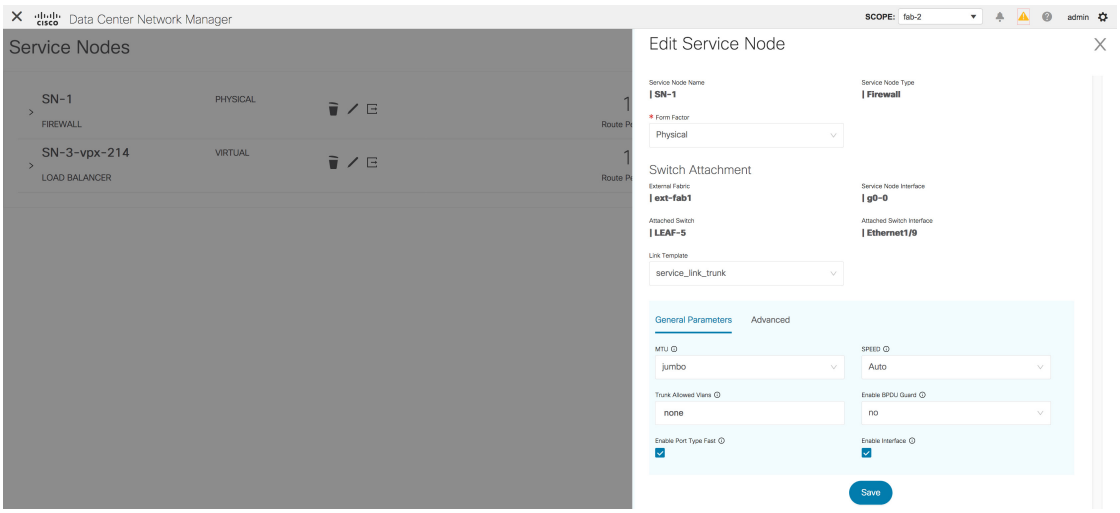
Cisco DCNW Web UI からサービス ノードを編集するには、次の手順を実行します。

Procedure

ステップ 1 **[サービス ノード（Service Nodes）]** ウィンドウで **[サービス ノードの編集（Edit Service Node）]** アイコンをクリックします。



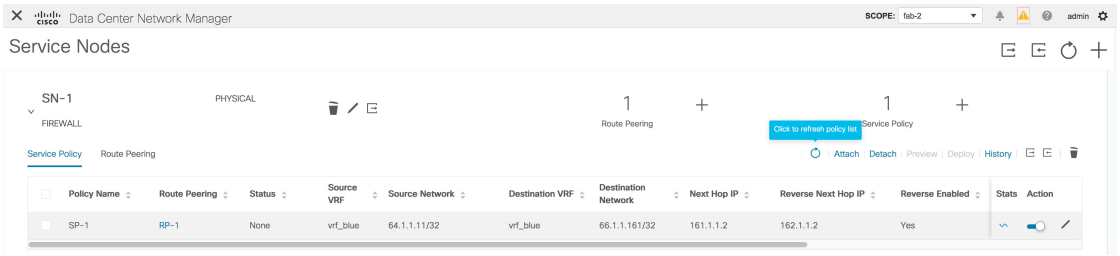
ステップ 2 **[サービス ノードの編集（Edit Service Node）]** ウィンドウが表示されます。



必要な変更を行って、[保存（Save）] をクリックします。

サービス ポリシーおよびルート ピアリング リストの更新

[サービス ノード（Service Nodes）] ウィンドウに表示されるサービス ポリシーまたはルート ピアリングのリストを更新するには、**[サービス ポリシー（Service Policy）]** タブまたは **[ルート ピアリング（Route Peering）]** タブに表示される **[更新（Refresh）]** アイコン をクリックします。



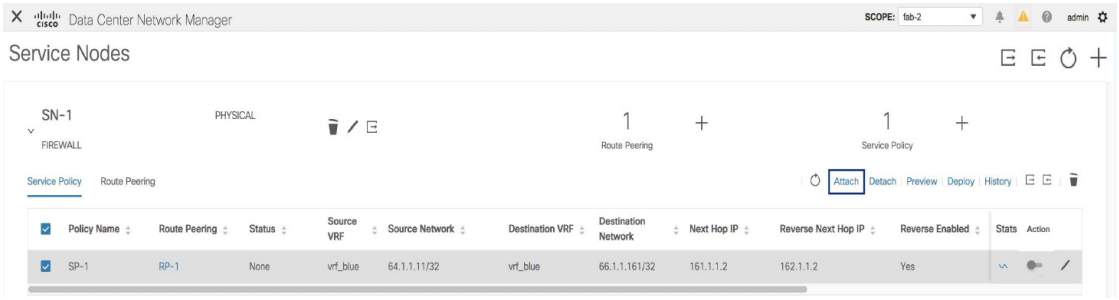
特定のサービス ポリシーまたはルート ピアリングの更新

Cisco DCNM リリース 11.5(1) から、特定のサービス ポリシーまたはルート ピアリングを更新するには、**[アクション（Action）]** 列の下に表示される **[更新（Refresh）]** アイコンをクリックします。

サービス ポリシーまたはルート ピアリングのアタッチ

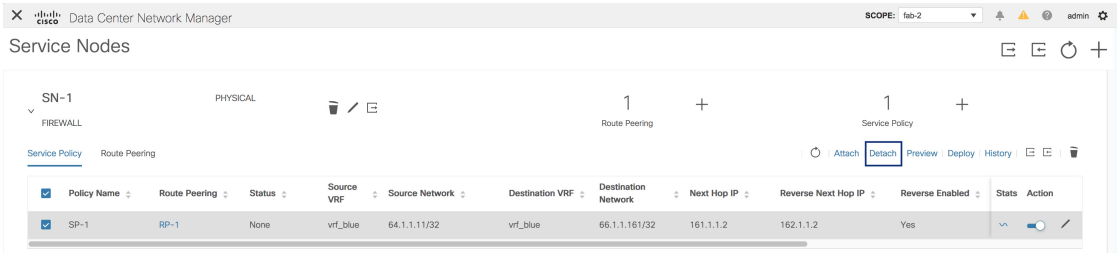
特定のサービス ポリシーまたはルート ピアリングをスイッチからアタッチするには、必要なサービス ポリシーまたはルート ピアリングの横にあるチェックボックスを選択し、**[アタッチ（Attach）]** をクリックします。

（注） Cisco DCNM リリース 11.5(1) 以降、ルート ピアリングの一括アタッチ、デタッチ、プレビュー、および展開と、サービス ポリシーがサポートされていますが、最大 10 のルート ピアリングまたは 10 のサービス ポリシーまでに制限されています。



サービス ポリシーまたはルート ピアリングの解除

特定のサービス ポリシーまたはルート ピアリングをスイッチから切り離すには、必要なサービスポリシーまたはルートピアリングの横にあるチェックボックスを選択し、**[解除（Detach）]** をクリックします。

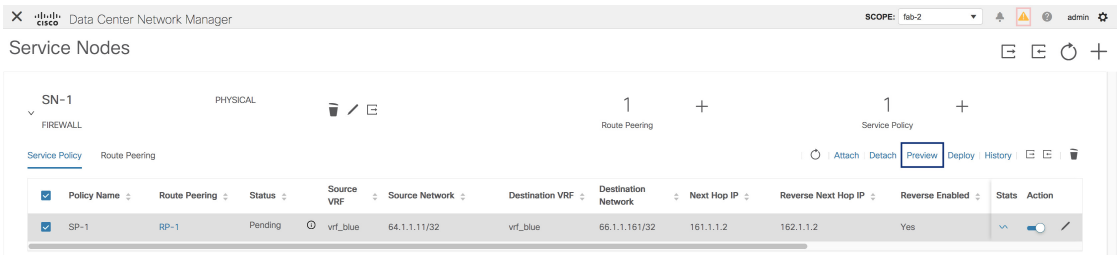


サービス ポリシーまたはルート ピアリングのプレビュー

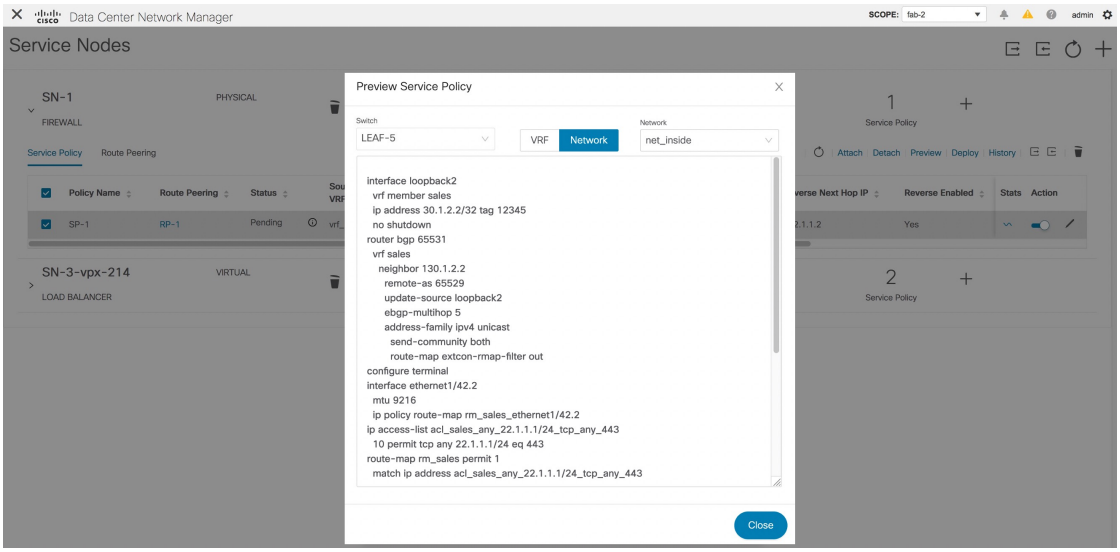
Cisco DCNM Web UI からサービス ポリシーまたはルート ピアリングのプレビューを表示するには、次の手順を実行します。

Procedure

ステップ 1 サービス ポリシーまたはルート ピアリングのチェックボックスを選択し、**[サービス ノード（Service Nodes）]** ウィンドウで **[プレビュー（Preview）]** をクリックします。



[サービス ポリシーのプレビュー（Preview Service Policy）] または **[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。



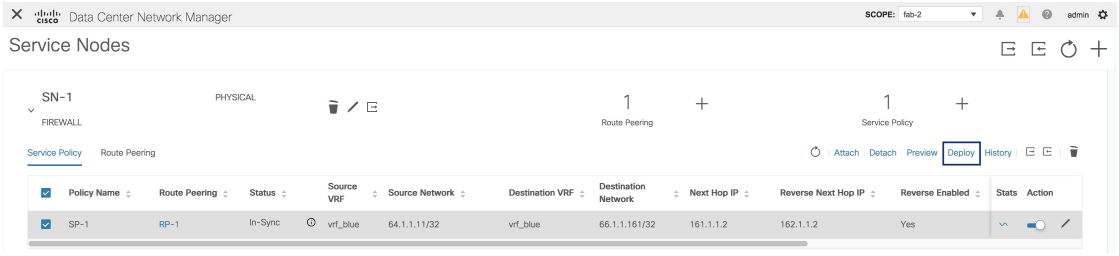
ステップ 2 特定のスイッチ、ネットワーク、または VRF のサービス ポリシーまたはルート ピアリングを表示するには、それぞれのドロップダウンリストから特定のスイッチ、ネットワーク、または VRF を選択します。[閉じる] をクリックして、ウィンドウを閉じます。

サービス ポリシーまたはルート ピアリングの展開

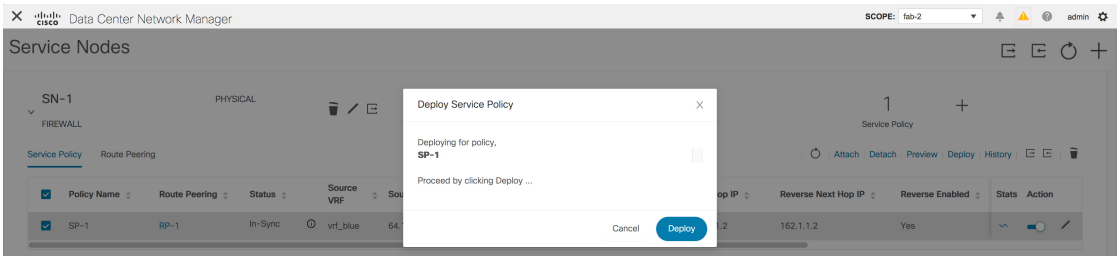
Cisco DCNM Web UI からサービス ポリシーまたはルート ピアリングを展開するには、次の手順を実行します。

Procedure

ステップ 1 サービス ポリシーまたはルート ピアリングのチェックボックスを選択し、**[サービス ノード（Service Nodes）]** ウィンドウで **[展開（Deploy）]** をクリックします。



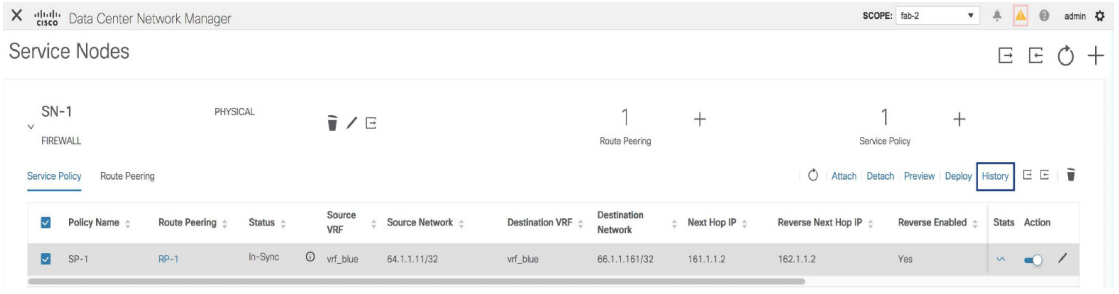
展開の確認を求めるポップアップ ウィンドウが表示されます。



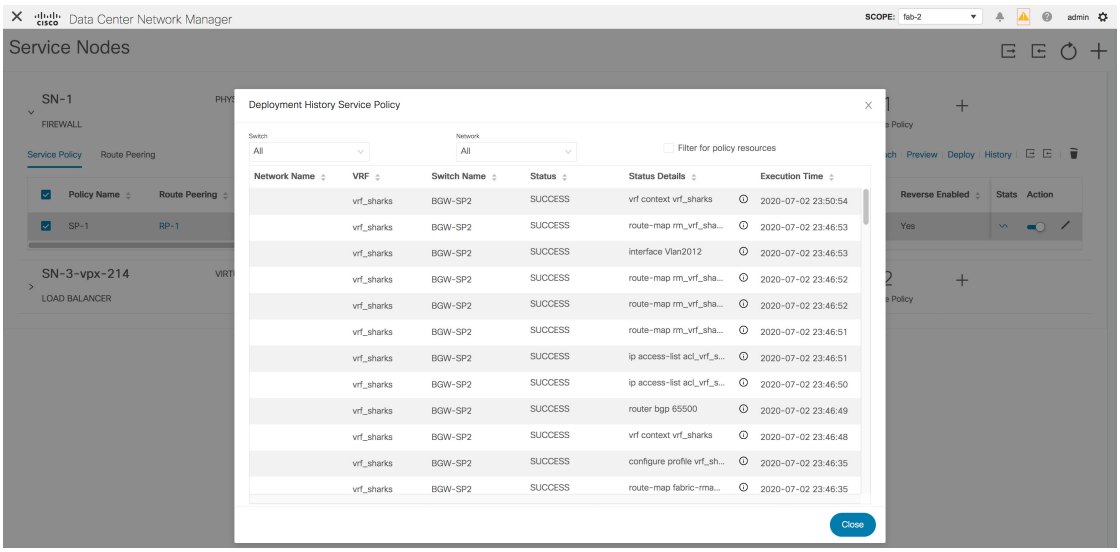
ステップ 2 [展開（Deploy）] をクリックします。

展開履歴の表示

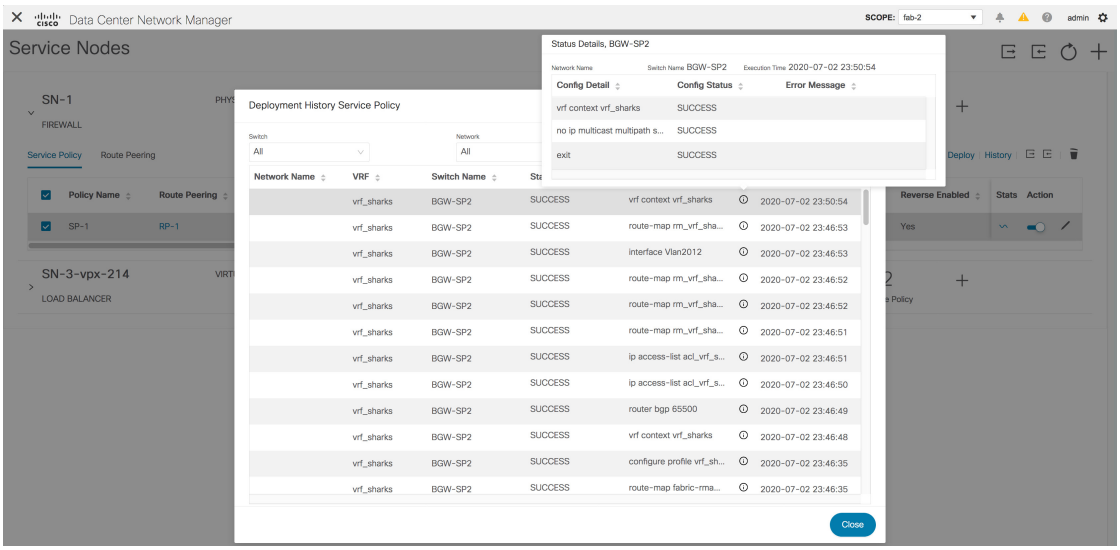
選択したサービス ポリシーまたはルート ピアリングに関連するスイッチおよびネットワークの展開履歴を表示するには、**[サービス ポリシー（Service Policy）]** タブまたは **[ルート ピアリング（Route Peering）]** タブの **[履歴（History）]** をクリックします。**[サービス ポリシーの展開履歴（Deployment History Service Policy）]** または **[ルート ピアリングの展開履歴（Deployment History Route Peering）]** ウィンドウが表示されます。



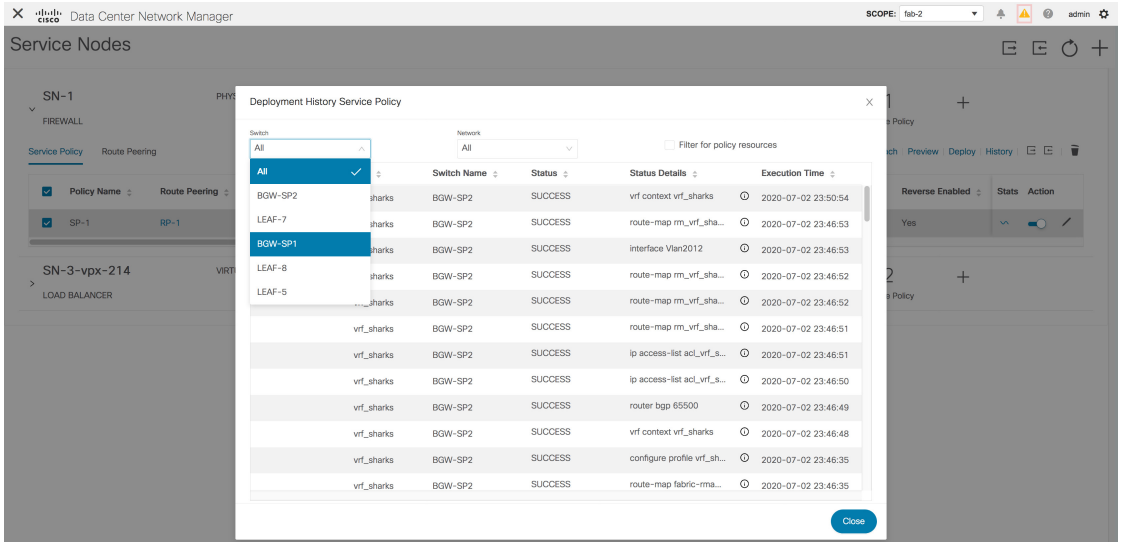
ネットワークの名前、VRF、スイッチ、ステータス、ステータスの詳細、実行時間などの情報が表示されます。



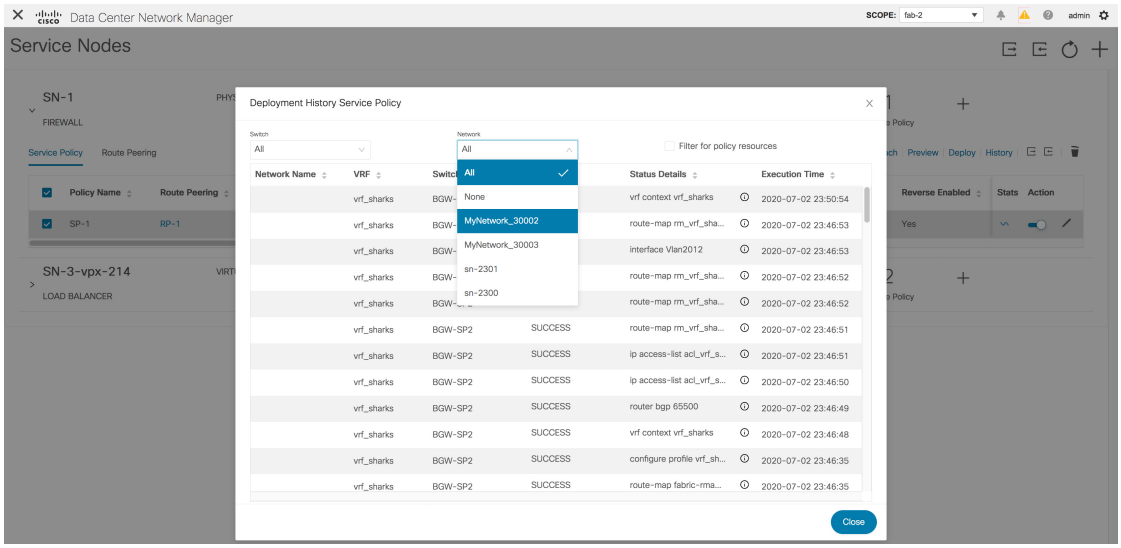
CLIのリストの最初の行は、**[ステータスの詳細（Status Details）]**列に表示されます。これは、展開された構成のピークを表示します。**i**アイコン（各行の**[ステータスの詳細（Status Details）]**フィールドの横）にカーソルを合わせると、詳細が表示されます。



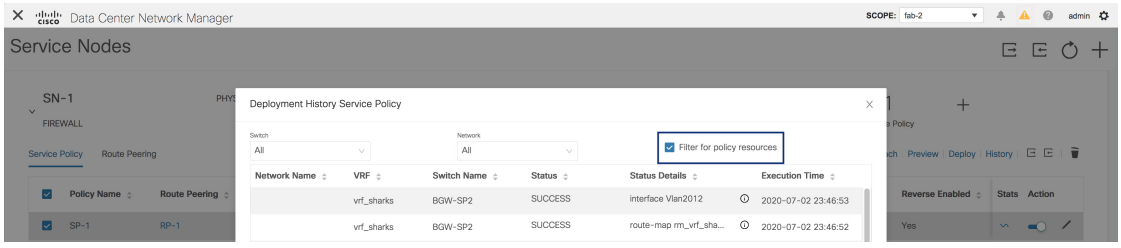
[スイッチ（Switch）]ドロップダウン リストからスイッチを選択して、選択したスイッチの情報を表示します。



[ネットワーク（Network）] ドロップダウン リストからネットワークを選択して、選択したネットワークの情報を表示します。

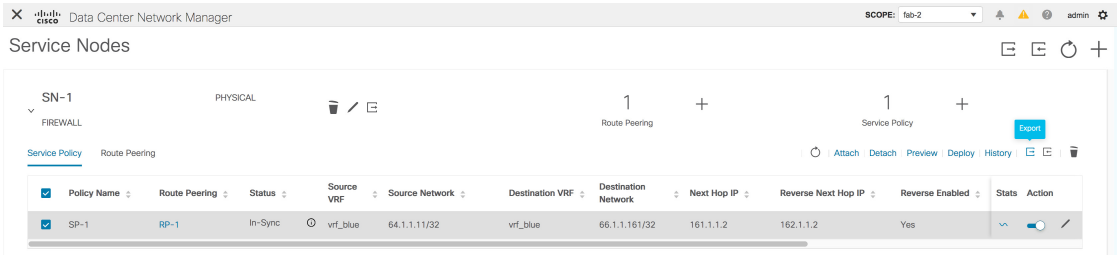


[ポリシー リソースのフィルタ（Filter for policy resources）] チェックボックスを選択して、ACL、ルートマップ、関連するCLIなどのポリシー関連の展開のみを表示します。このチェックボックスは、**[サービス ポリシーの展開履歴（Deployment History Service Policy）]** ウィンドウでのみ使用できます。



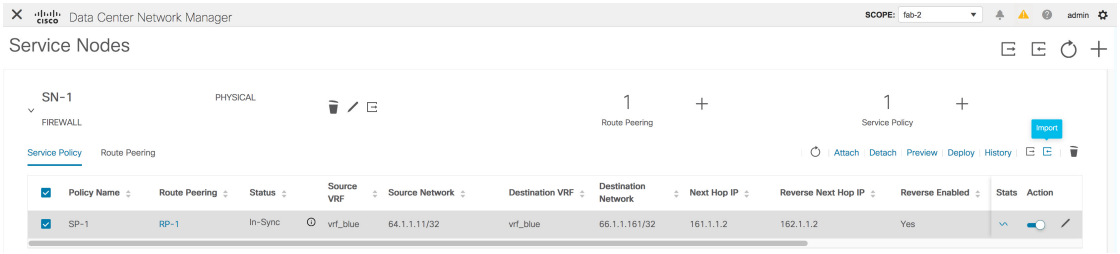
サービス ポリシーまたはルート ピアリング テーブルのエクスポート

サービス ポリシーまたはルート 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、**[サービス ノード（Service Nodes）]** ウィンドウで **[エクスポート（Export）]** アイコンをクリックします。**[サービス ポリシー（Service Policy）]** タブの **[エクスポート（Export）]** アイコンをクリックして、サービス ポリシーに関する情報をエクスポートします。**[ルート ピアリング（Route Peering）]** タブの **[エクスポート（Export）]** アイコンをクリックして、ルート ピアリングに関する情報をエクスポートします。



サービス ポリシーまたはルート ピアリング テーブルのインポート

サービス ポリシーまたはルート 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、**[サービス ノード（Service Nodes）]** ウィンドウで **[インポート（Import）]** アイコンをクリックします。**[サービス ポリシー（Service Policy）]** タブの **[インポート（Import）]** アイコンをクリックして、サービス ポリシーに関する情報をエクスポートします。**[ルート ピアリング（Route Peering）]** タブの **[インポート（Import）]** アイコンをクリックして、ルート ピアリングに関する情報をエクスポートします。

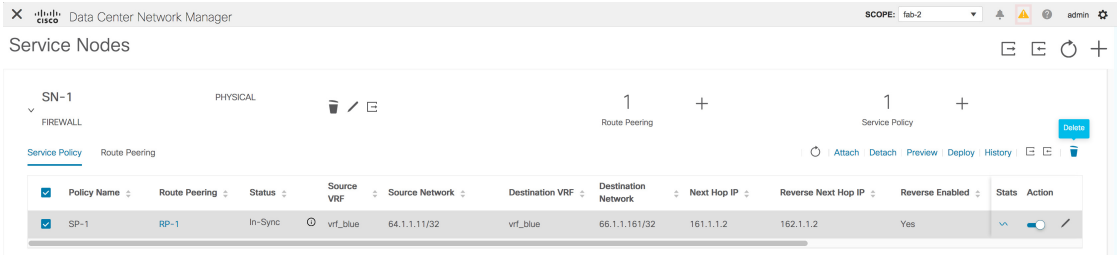


サービス ポリシーの削除

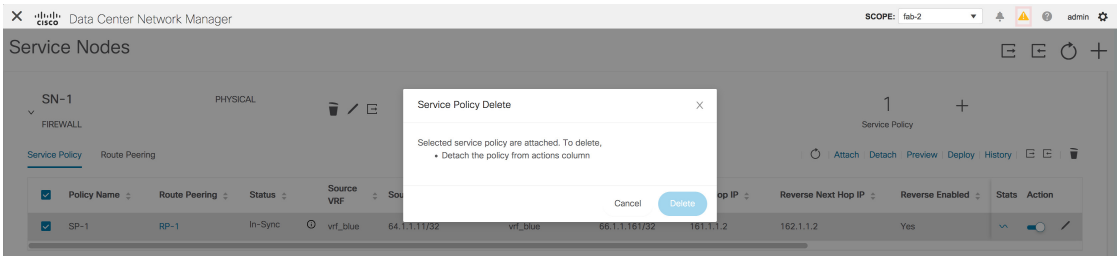
Cisco DCNW Web UI からサービス ポリシーを削除するには、次の手順を実行します。

Procedure

ステップ 1 ポリシーの名前の横にあるチェックボックスをクリックして削除する必要があるサービス ポリシーを選択し、**[サービス ノード（Service Nodes）]** ウィンドウの **[削除（Delete）]** アイコンをクリックします。



ステップ 2 削除の確認を求めるポップアップ ウィンドウが表示されます。[削除（Delete）] をクリックします。削除する必要があるサービス ポリシーがアタッチされている場合、ポップアップ ウィンドウは、**[アクション（Action）]** 列のトグルを使用してサービス ポリシーをアタッチ解除し、削除する前に変更を展開（ポリシーの削除）する必要があることを示します。

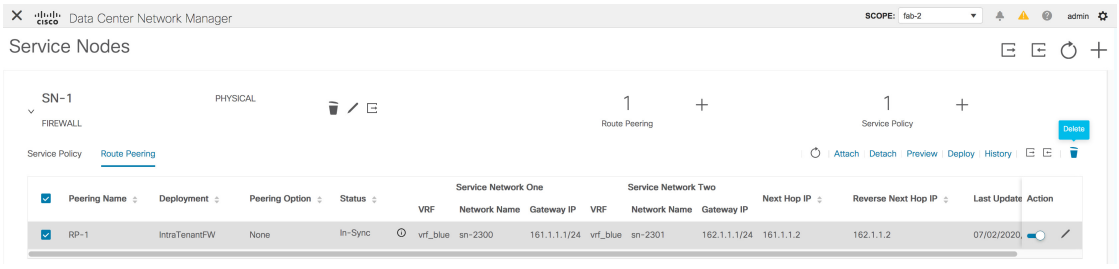


ルート ピアリングの削除

Cisco DCNM Web UI からルート ピアリングを削除するために、次の手順を実行します。

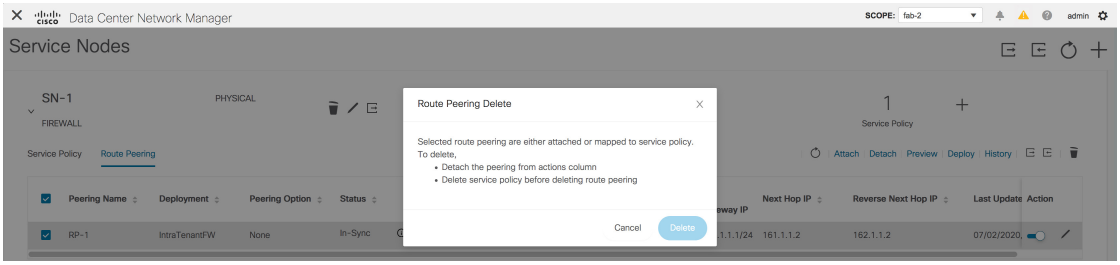
Procedure

ステップ 1 ルート ピアリングの名前の横にあるチェックボックスをクリックして削除する必要があるルート ピアリングを選択し、**[サービス ノード（Service Nodes）]** ウィンドウの **[削除（Delete）]** アイコンをクリックします。



ステップ 2 削除の確認を求めるポップアップ ウィンドウが表示されます。[削除（Delete）] をクリックします。削除する必要があるルート ピアリングがアタッチされている場合、またはルート ピアリングに関連付けられたサービス ポリシーがアクティブな場合、ポップアップ ウィンドウは、**[アクション（Action）]** 列のトグルを使用してピアリングをデタッチする必要があることを示

し、変更を展開し（ポリシーを削除）、ルート ピアリングを削除する前に、ルート ピアリングに関連付けられたサービス ポリシーを削除します。



サービス ポリシー情報の表示

[サービス ノード（Service Nodes）] ウィンドウの **[サービス ポリシー（Service Policy）]** タブには、構成済みのサービス ポリシーに関する情報が表示されます。

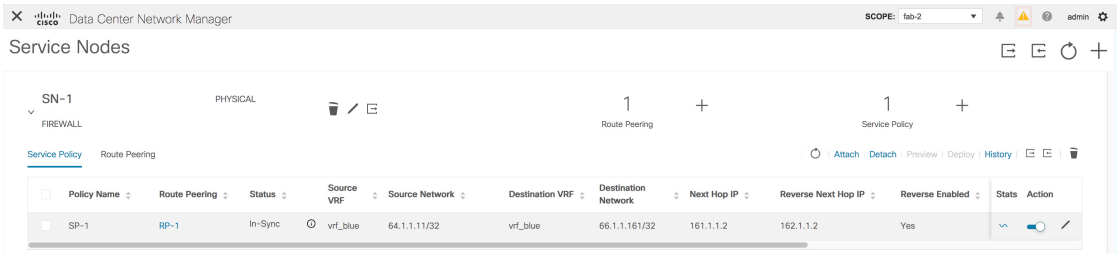
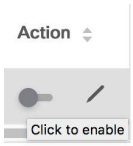
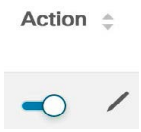


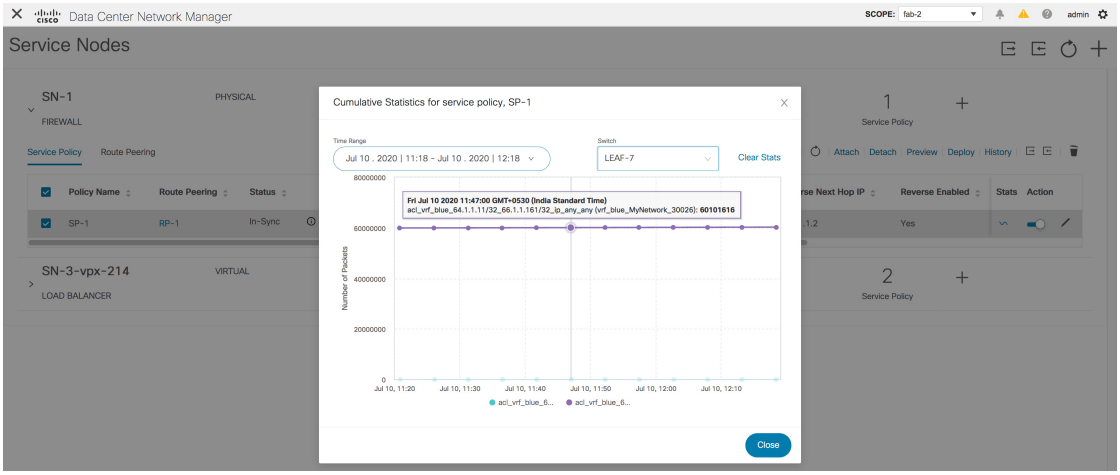
表 *28 :* サービス ポリシー テーブル フィールドおよび説明

フィールド	説明
ポリシー名	ポリシーの名前を表示します。
ルートピアリング	ピアリング構成に指定されたルート ピアリング名を表示します。指定したピアリング名をクリックすると、ルートのピアリング情報が表示されます。
Status	サービスポリシーのステータスを表示します。
Source VRF	仮想ルーティングおよび転送（VRF）送信元を表示します。
送信元ネットワーク	送信元ネットワークを表示します。
宛先VRF	接続先 VRF を表示します。
宛先ネットワーク（Destination Network）	接続先ネットワークを表示します。
ネクストホップIP	ネクストホップ IP アドレスを表示します。

フィールド	説明
Reverse Next Hop IP	リバース ネクストホップ IP アドレスを表示します。
Reverse Enabled	リバース ネクストホップを有効にするかどうかを表示します。
ルートマップアクション	指定されたルートマップアクションを表示します。
Next Hop Option	指定されたネクストホップ オプションを表示します。
最終更新日	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。
Stats	グラフ行をクリックして、指定した時間範囲のポリシーの累積統計を表示します。詳細については、統計を参照してください。
アクション	トグルを使用して、サービス ポリシーを有効/アタッチ、または無効/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。  サービス ポリシーがアタッチまたは有効化されると、トグルが青色に変わります。  **[編集（Edit）]**アイコンをクリックして、サービス ポリシーを編集します。 

Stats

[サービス ノード（Service Nodes）] ウィンドウの **[サービス ポリシー（Service Policy）]** タブには、構成済みのサービス 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。Cisco DCNM リリース 11.4(1) 以降では、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。



ルート ピアリング情報の表示

[サービス ノード（Service Nodes）] ウィンドウで、**[ルート ピアリング（Route Peering）]** をクリックします。**[ルート ピアリング（Route Peering）]** タブには、ルート ピアリング情報が表示されます。

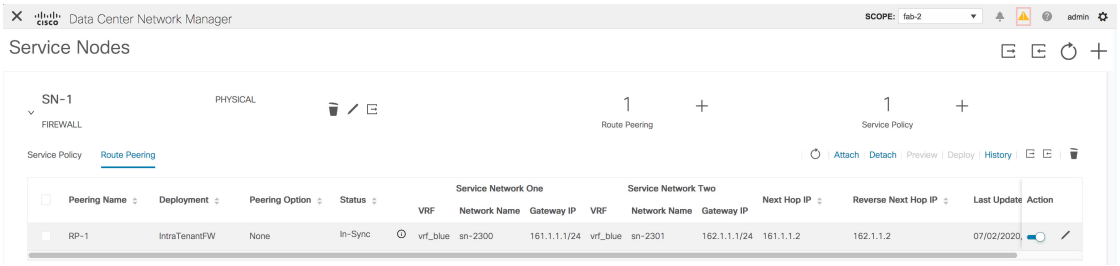
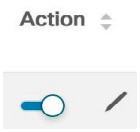
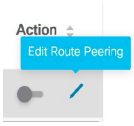


表 *29* : ルート ピアリング テーブルのフィールドと説明

フィールド	説明
Peering Name	定義されたピアリング名を表示します。

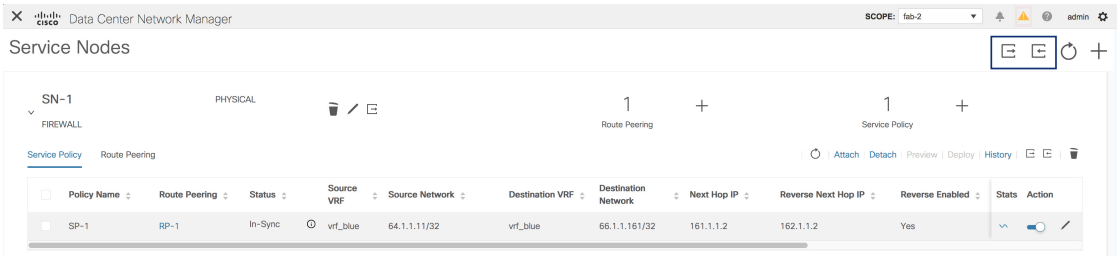
フィールド	説明
導入	展開の表示：One-Arm モードまたは Two-Arm モード。
ピアリング オプション	ピアリング オプションの表示：静的または eBGP ダイナミック ピアリング。
Status	ルートピアリングのステータスを表示します。
サービス ネットワーク VRF	サービスネットワークのVRFを表示します。
サービスネットワーク名	サービスネットワークの名前が表示されます。
サービス ネットワーク ゲートウェイ IP	サービス ネットワーク VRF のゲートウェイ IP を表示します。
ネクストホップIP	ネクストホップ IP アドレスを表示します。
Reverse Next Hop IP	リバースネクストホップIPアドレスを表示します。
最終更新日	ルート ピアリングが最後に更新された時刻を表示します。

フィールド	説明
アクション	トグルを使用して、ルート ピアリングを有効/アタッチ、または無効/デタッチします。ルート ピアリングを有効にすると、そのルート ピアリングで定義されたサービス ネットワークがサービス リーフに接続されます。  ルート ピアリングが接続されているか、有効になっている場合、トグルは青色に変わります。  **[編集（Edit）]**アイコンをクリックしてルート ピアリングを編集します。 

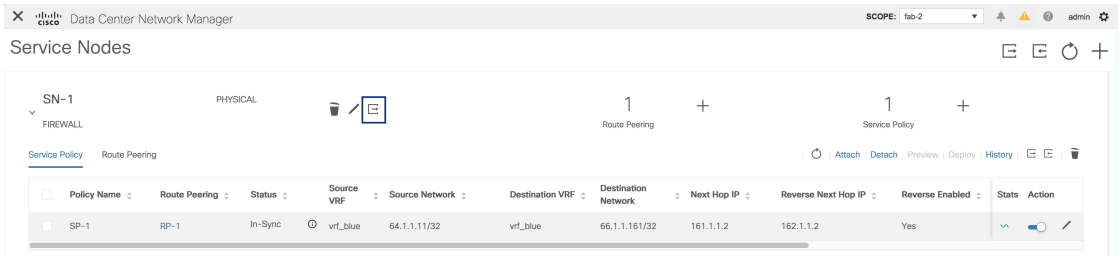
サービス ノードのバックアップと復元

サービス ノード レベルでデータをバックアップするには、**[エクスポート（Export）]** アイコン 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。

また、**[インポート（Import）]** アイコン 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。



[サービス ノードの編集（Edit Service Node）] アイコンの横にある **[エクスポート（Export）]** アイコン をクリックして、特定のサービス ノードのデータをエクスポートすることもできます。



ファブリックのバックアップと復元

Easy ファブリックと親 MSD ファブリックのバックアップ中に、サービス ノード接続、ルート ピアリング、およびサービス ポリシー構成（構成された ACL やルート マップなど）が、ファブリック、VRF、およびテナント ネットワーク インテントの一部として保存されます。ただし、サービス ノード、ルート ピアリング、サービス ポリシーの定義は保存されません。**[制御（Control）] > [サービス（Services）]** ウィンドウのサービス ノード レベルで **[エクスポート（Export）]** アイコンをクリックして、サービス データをバックアップすることが推奨されています。Easy ファブリックと親 MSD ファブリックの復元中に、サービス データは、**[制御（Control）] > [サービス（Services）]** ウィンドウからサービス ノード レベルで **[インポート（Import）]** アイコンをクリックすることで復元できます。サービス ノード接続、ルート ピアリング、およびサービス ポリシー構成は、関連付けられたファブリック、VRF、およびテナント ネットワーク インテントとともに復元されます。

既存環境の移行

ブラウンフィールド移行中に、ネットワークと VRF に関連付けられた ACL やルート マップなどの L4-L7 サービス構成は、テナント ネットワークと VRF プロファイルにリンクされたスイッチの自由形式ポリシーでキャプチャされます。ブラウンフィールド移行の結果として、サービス ノード、ルート ピアリング、またはサービス ポリシーは自動生成されません。新しいサービス ポリシーを同じテナント ネットワークまたは VRF に適用する場合は、キャプチャされた自由形式の構成を削除すると、構成のコンプライアンスによって、後で展開できる必要な CLI が生成されます。

監査履歴

Cisco DCNM リリース 11.5(1) から、[サービス ノード（Service Nodes）] ウィンドウの [監査（Audit）] アイコンをクリックして、[監査履歴（Audit History）] ウィンドウを表示します。

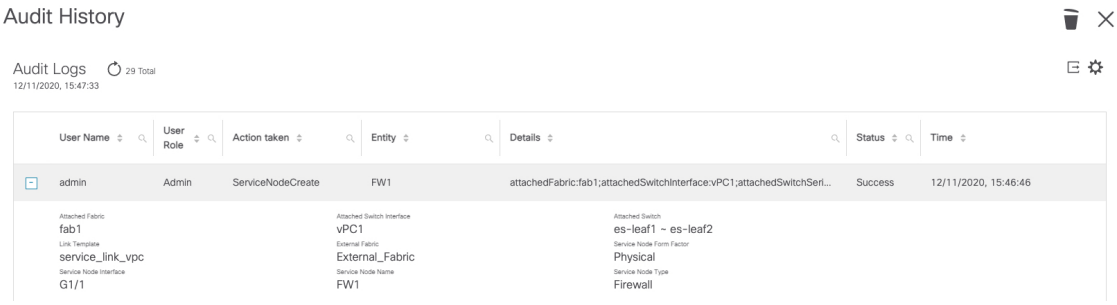
[監査履歴（Audit History）] ウィンドウの [監査ログ（Audit Logs）] テーブルには、実行されたすべてのアクションに関する情報が表示されます。監査ログは、次のアクションが実行されたときに生成されます。

- サービス ノード、ルート ピアリング、およびサービス ポリシーの作成
- サービス ノード、ルート ピアリング、およびサービス ポリシーの削除
- サービス ノード、ルート ピアリング、およびサービス ポリシーの更新
- ルート ピアリングの接続と切断、およびサービス ポリシー
- ルート ピアリングおよびサービス 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。

各列で検索を実行するには、必要な列の検索アイコンをクリックし、検索文字列を入力します。

各行の詳細を表示するには、ユーザ名の横にある [+] アイコンをクリックします。

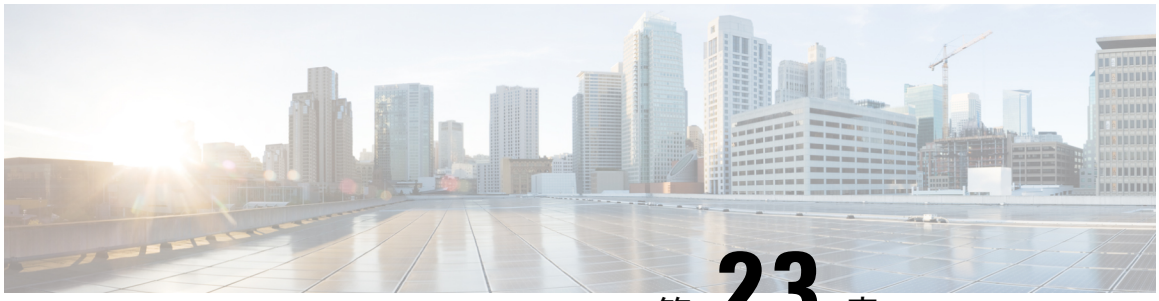


このウィンドウのデータを Excel ファイルにエクスポートするには、[エクスポート（Export）] アイコンをクリックします。

監査ログテーブルのフィールドを選択的に非表示または表示するには、[エクスポート（export）] アイコンの隣にある歯車アイコンをクリックして、監査ログ テーブルに表示する必要があるフィールドを選択します。

古い監査レポートを削除するには、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。

最新の監査ログを表示するには、[監査ログ（Audit Logs）] テーブルの上にある [更新（Refresh）] アイコンをクリックします。

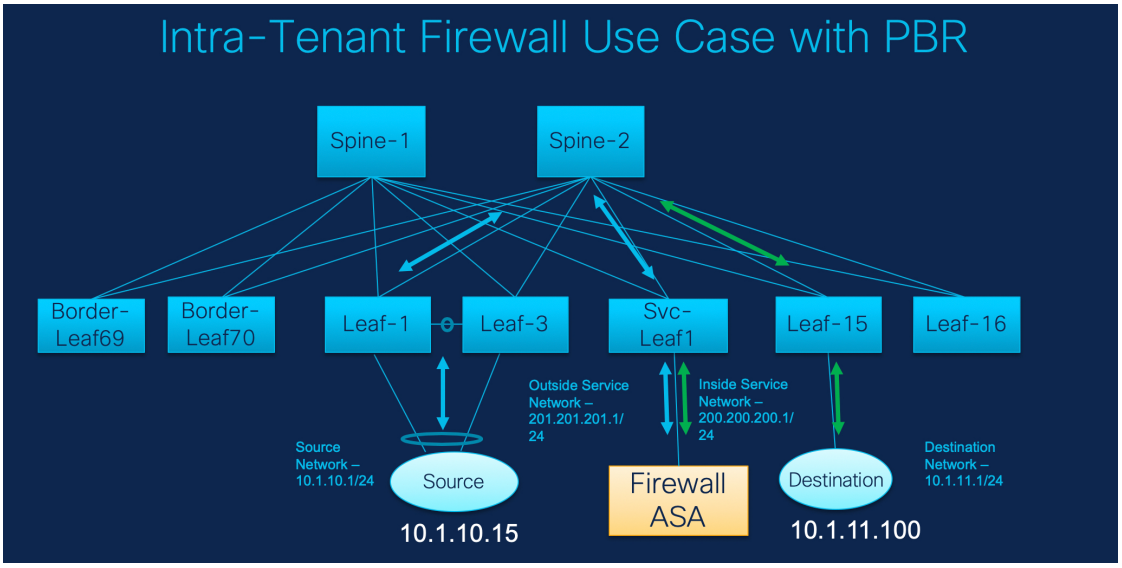


第 23 章

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、DCNM 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 LAN ファブリックの構成ガイド』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。

[制御（Control）] > [ファブリック（Fabrics）] > [サービス（Services）] の順に選択します。

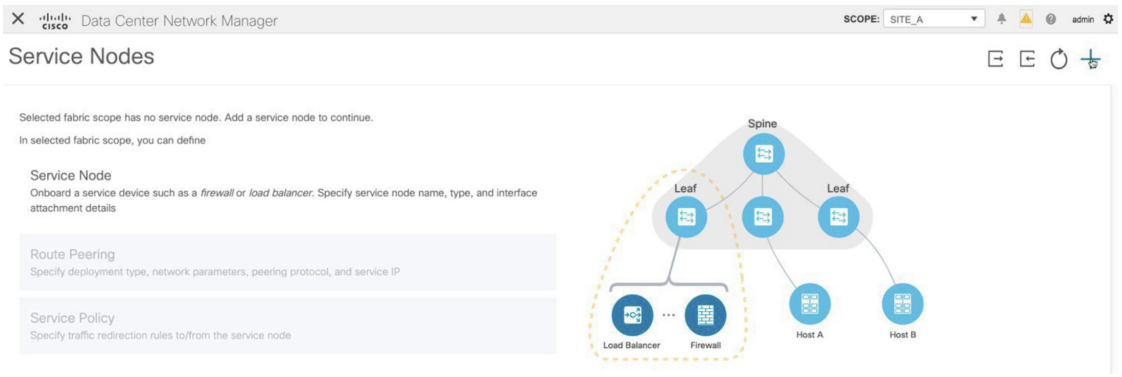
このユースケースは、次の手順で構成されます。

1. サービス ノードの作成

Procedure

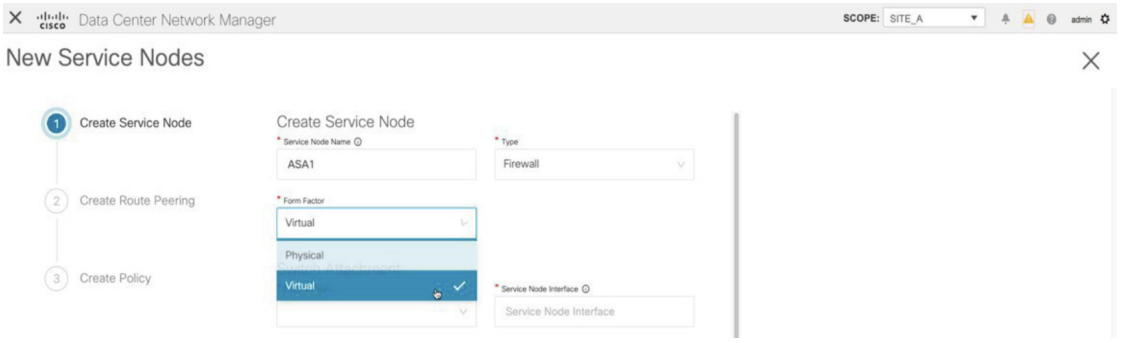
ステップ 1 **[範囲（Scope）]** ドロップダウンリストから、**Site_A** を選択します。

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。



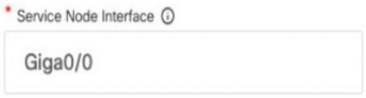
ステップ 3 ノード名を入力し、**[ファイアウォール（Firewall）]** を指定します（**[タイプ（Type）]** ドロップダウン ボックス）。**[サービス ノード名（Service Node Name）]** は一意である必要があります。

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。

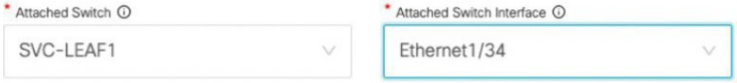


ステップ 5 **[スイッチの接続（Switch Attachment）]** セクションで、**[外部ファブリック（External Fabric）]** ドロップダウン リストから、サービス ノード（たとえば、ASA ファイアウォール）が配置されている外部ファブリックを選択します。サービス ノードは外部ファブリックに属している必要があることに注意してください。これは、サービス ノードを作成する際の前提条件です。

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。

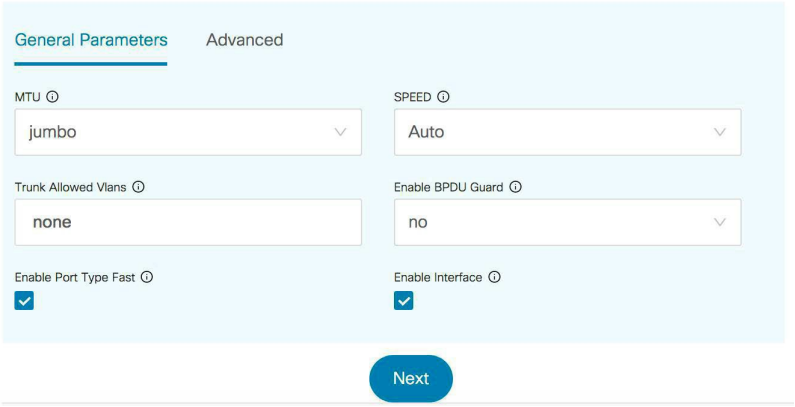


ステップ 7 サービス リーフである接続されたスイッチと、サービス リーフ上の対応するインターフェイスを選択します。



ステップ 8 **service_link_trunk** テンプレートを選択します。DCNM 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。



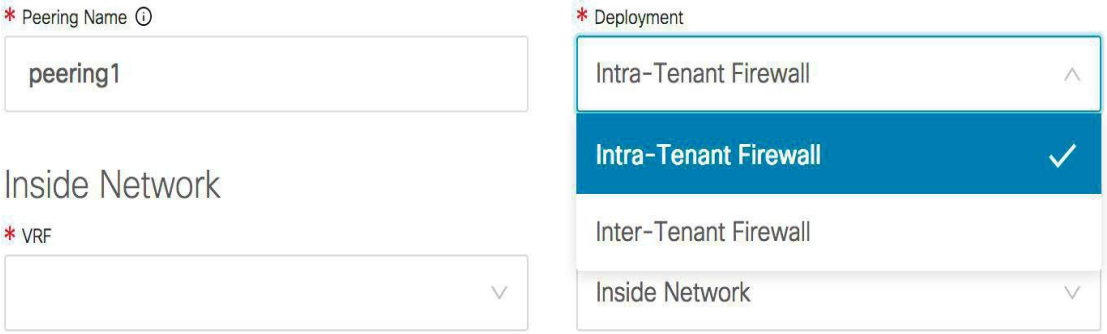
ステップ 10 **[次へ（Next）]** をクリックして、作成したサービス ノードを保存します。

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

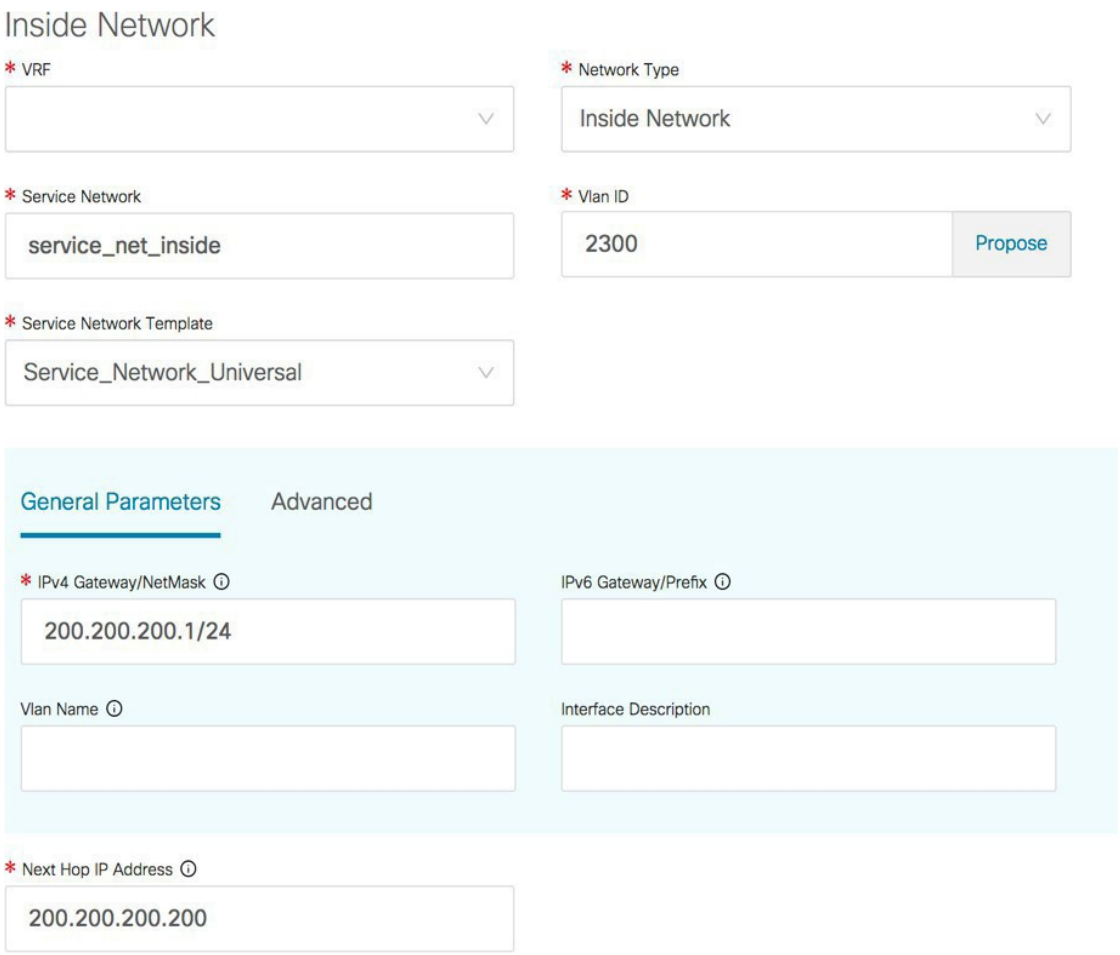
ステップ 1 ピアリング名を入力し、**[テナント内ファイアウォール（Intra-Tenant Firewall）]** を **[展開（Deployment）]** ドロップダウン リストから選択します。



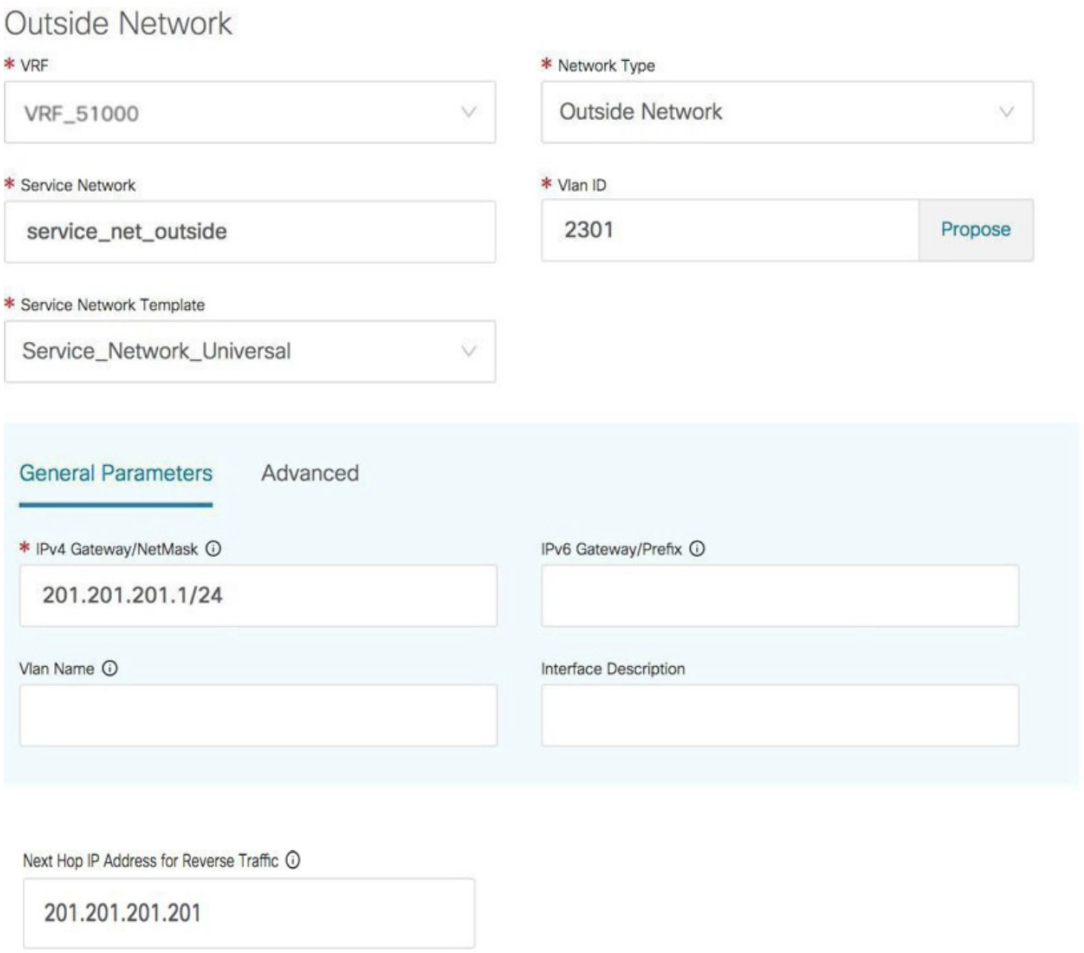
ステップ 2 **[内部ネットワーク（Inside Network）]** で、**[VRF]** ドロップダウンリストから既に存在している VRF を選択し、**[内部ネットワーク（Inside Network）]** を **[ネットワーク タイプ（Network Type）]** で選択します。

[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、DCNM 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] 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。



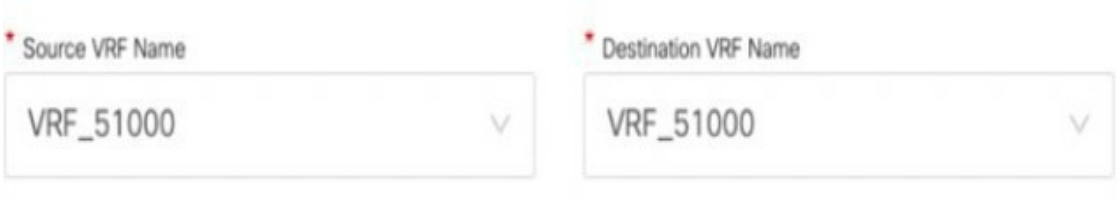
ステップ 4 **[次へ（Next）]** をクリックして、作成したルート ピアリングを保存します。

3. サービス ポリシーの作成

Procedure

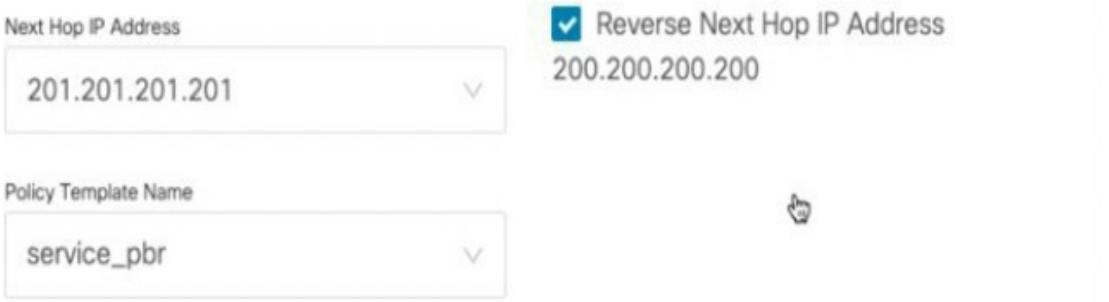
ステップ 1 ポリシーの名前を指定し、**[ピアリング名（Peering Name）]** ドロップダウン リストからルート ピアリングを選択します。

ステップ 2 **[送信元 VRF 名（Source VRF Name）]** および **[接続先 VRF 名（Destination VRF Name）]** ドロップダウンリストから、送信元および接続先 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。



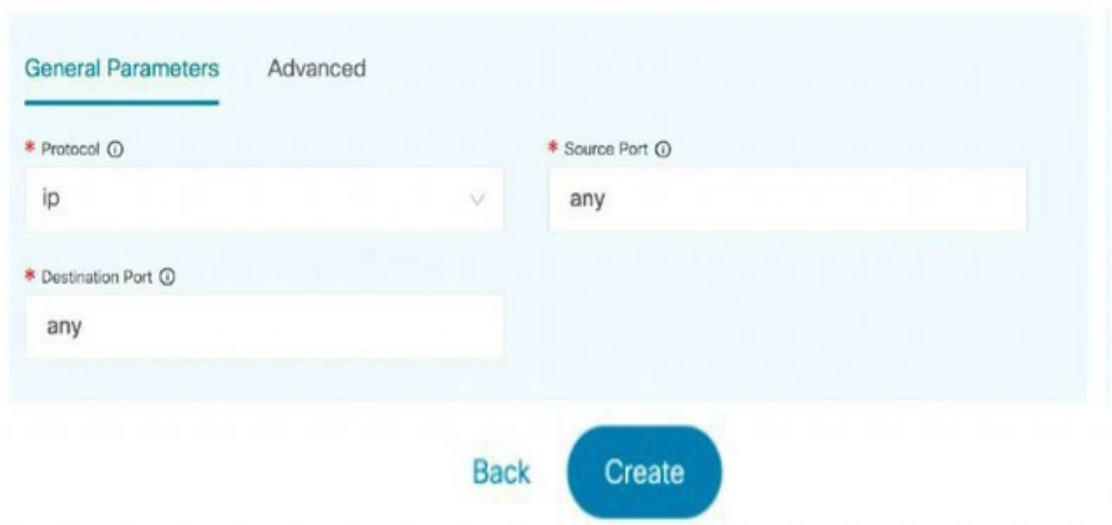
ステップ 3 **[送信元ネットワーク（Source Network）]** および **[接続先ネットワーク（Destination Network）]** ドロップダウンリストから、送信元ネットワークと接続先ネットワークを選択するか、**[制御（Control）] > [ファブリック（Fabrics）] > [ネットワーク（Networks）]** ウィンドウで定義されたネットワーク サブネット内にある送信元ネットワークまたは接続先ネットワークを指定します。

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。

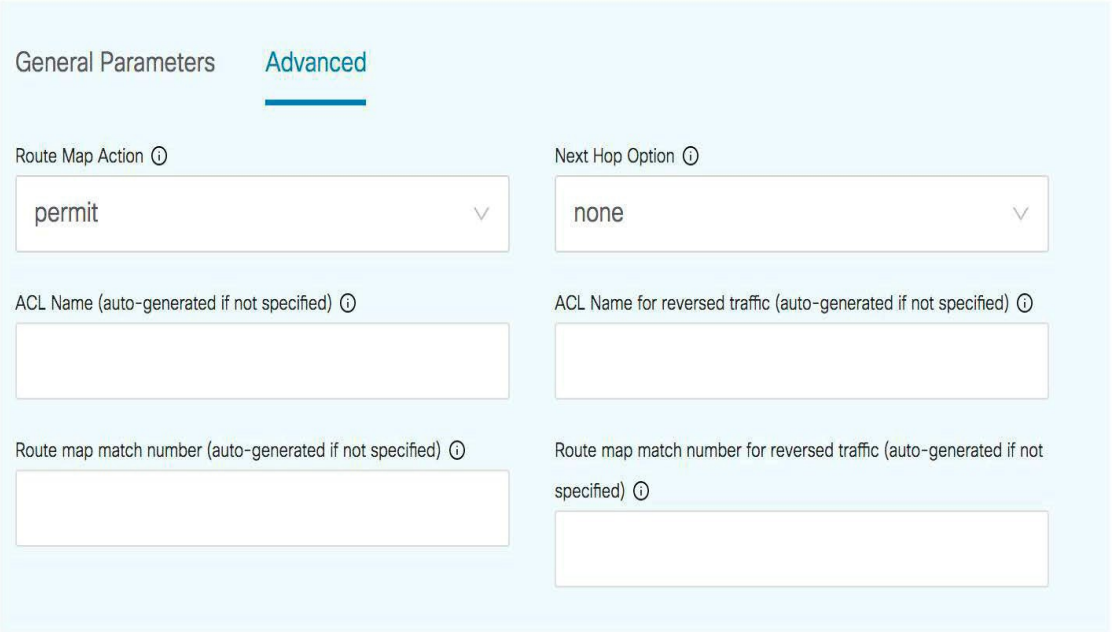


ステップ 5 ポリシー テンプレートの **[一般パラメータ（General Parameters）]** タブで、**[ip]** を **[プロトコル（Protocol）]** ドロップダウンリストから選択します。また、**[任意（any）]** を **[送信元ポート（Source Port）]** および **[宛て先ポート（Destination Port）]** フィールドで指定します。

Note **[ip]** および **[icmp]** プロトコルの場合、**[任意（any）]** の送信元ポートと宛て先ポートが常に 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。DCNM 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（Advanced）]** タブでは、デフォルトで、**[ルートマップアクション（Route Map Action）]** には **[permit（許可）]**、**[ネクストホップオプション（Next Hop Option）]** には **[none（なし）]** が選択されています。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」を参照してください。



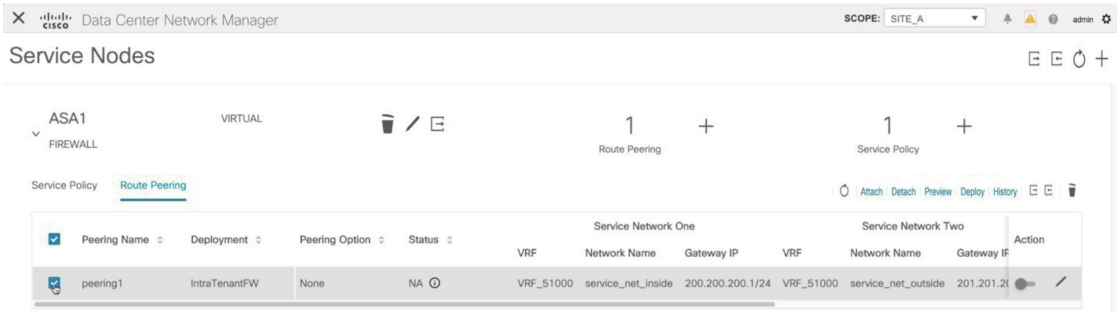
ステップ 7 **[作成（Create）]** をクリックして、作成したサービス ポリシーを保存します。

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。

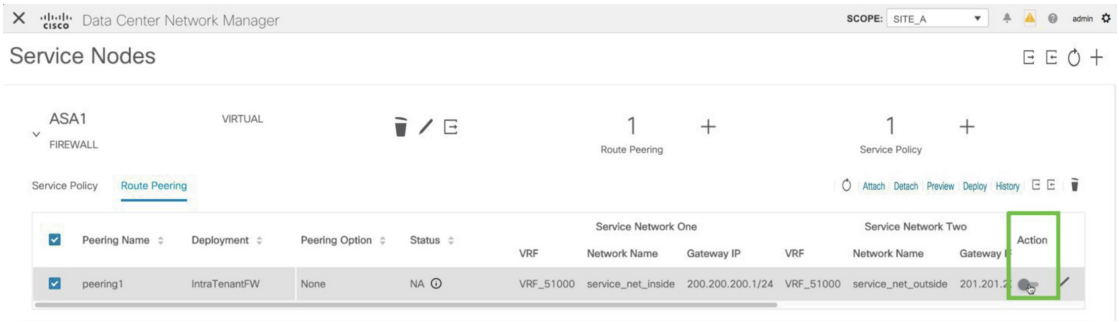
4. ルート ピアリングを展開する

Procedure

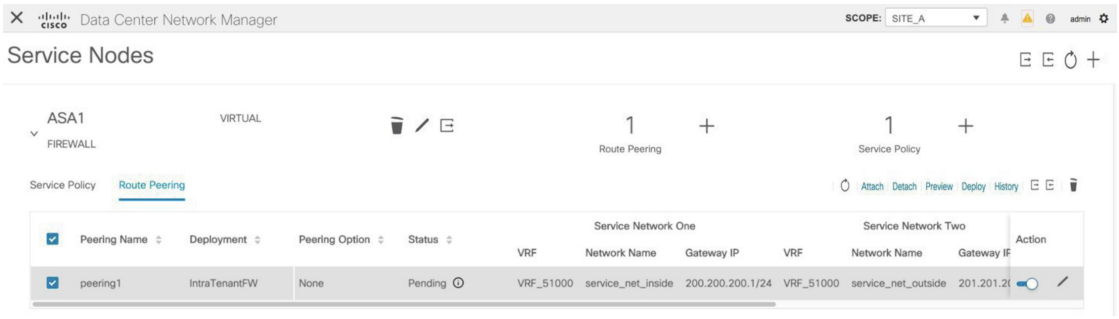
ステップ 1 **[サービス ノード（Service Nodes）]** ウィンドウの **[ルート ピアリング（Route Peering）]** タブで、必要なピアリングを選択します。



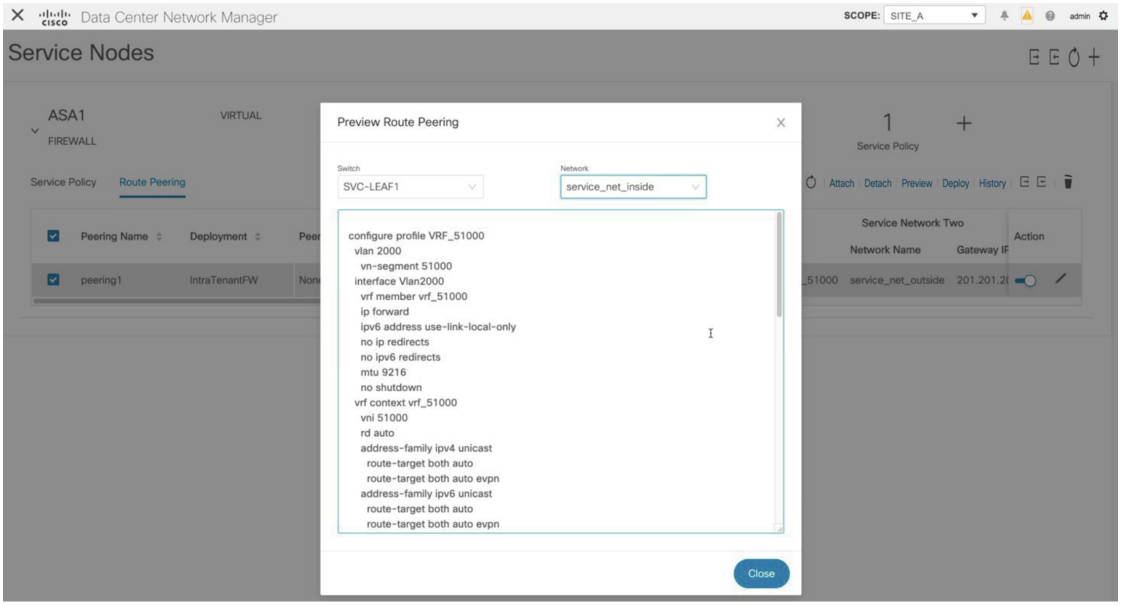
ステップ 2 **[アクション（Action）]** の下のトグルボタンをクリックして、サービス ネットワークをサービス リーフに接続します。



ステップ 3 **[プレビュー（Preview）]** をクリックして、サービス リーフにプッシュされる構成を表示します。

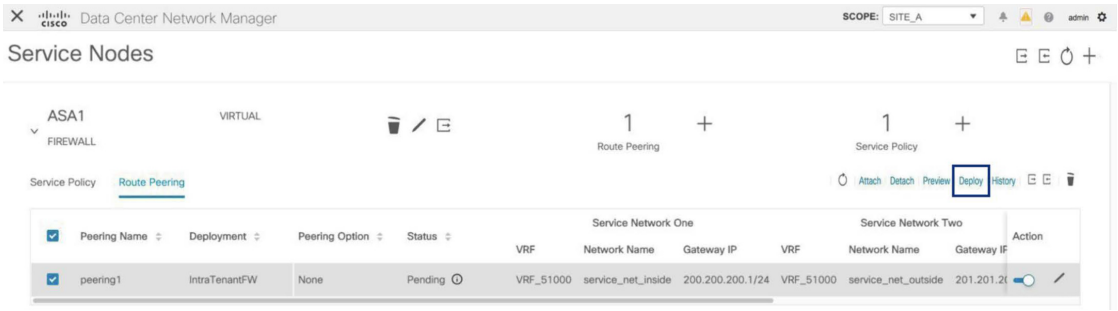


以前は、内部および外部のサービス ネットワークを作成していました。サービス リーフにプッシュされるこれらのネットワーク構成を表示できます。

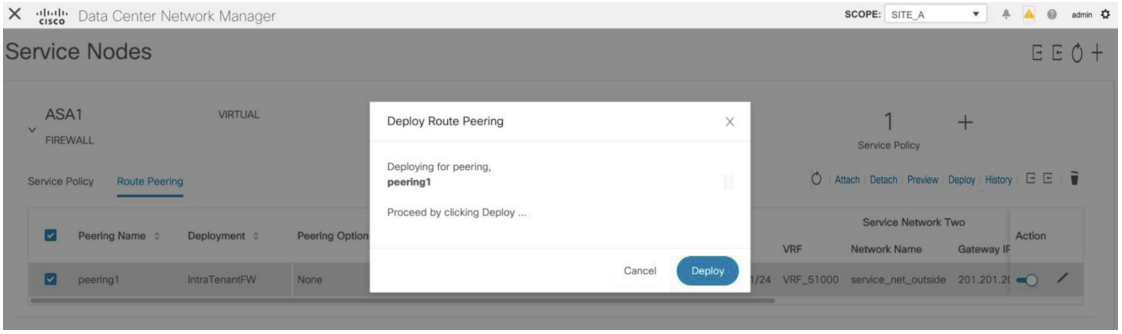


ステップ 4 **[閉じる（Close）]** をクリックして、**[ルート ピアリングのプレビュー（Preview Route Peering）]** ウィンドウを閉じます。

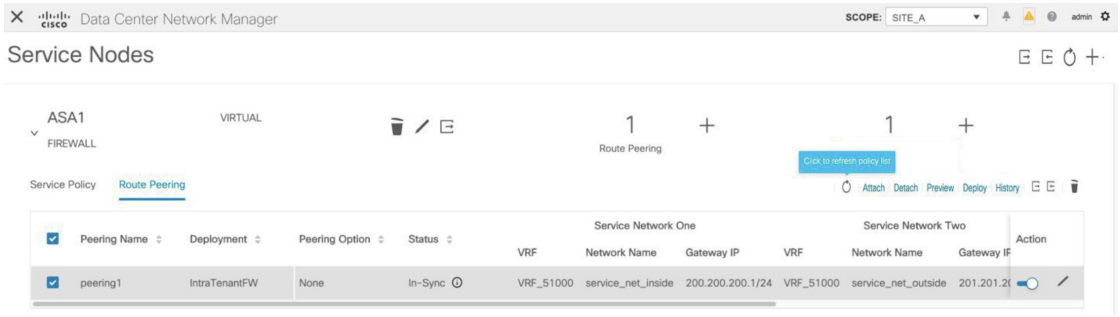
ステップ 5 **[サービス ノード（Service Nodes）]** ウィンドウで **[展開（Deploy）]** をクリックして、接続されたスイッチ（ルート ピアリング用のサービス リーフ）に構成を展開します。



ポップアップ ウィンドウの **[展開（Deploy）]** ボタンをクリックして、展開を確認します。



ステップ 6 最新のピアリング構成のアタッチメントと展開のステータスについては、**[更新（Refresh）]**アイコンをクリックします。

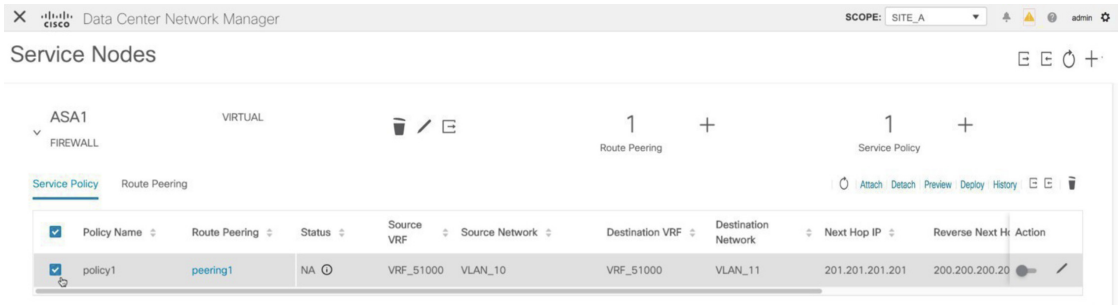


5. サービス ポリシーの展開

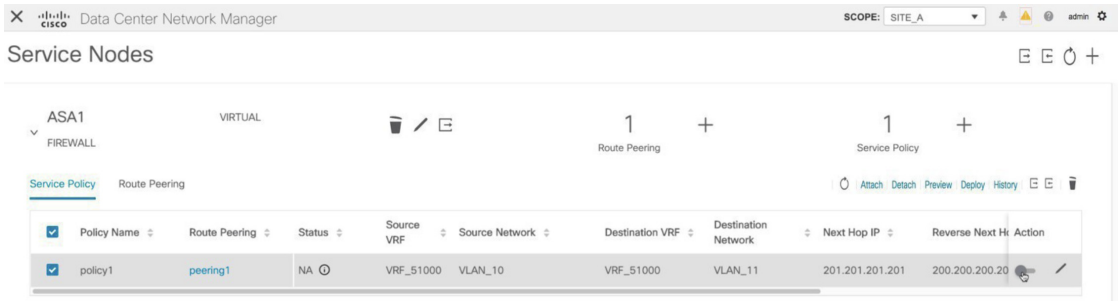
サービス ポリシーを展開するには、次の手順を実行します。このポリシーの対応する構成は、送信元および接続先ネットワークが接続されているスイッチおよびサービス リーフに展開されます。

Procedure

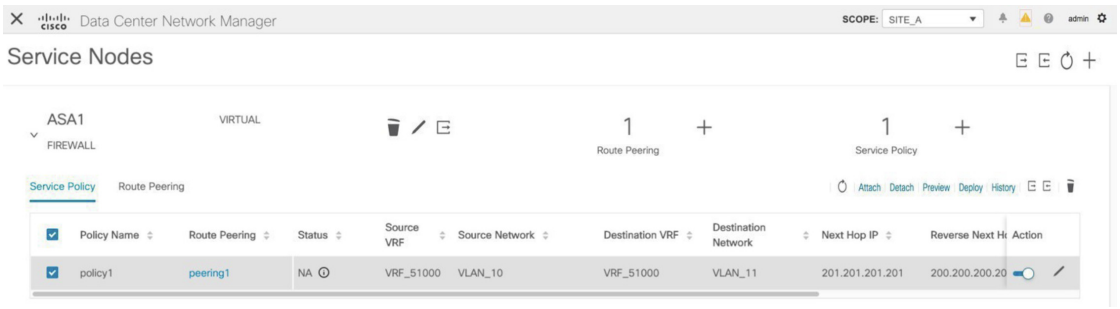
ステップ 1 **[サービス ポリシー（Service Policy）]**タブで、必要なポリシーの横にあるチェックボックスを選択します。



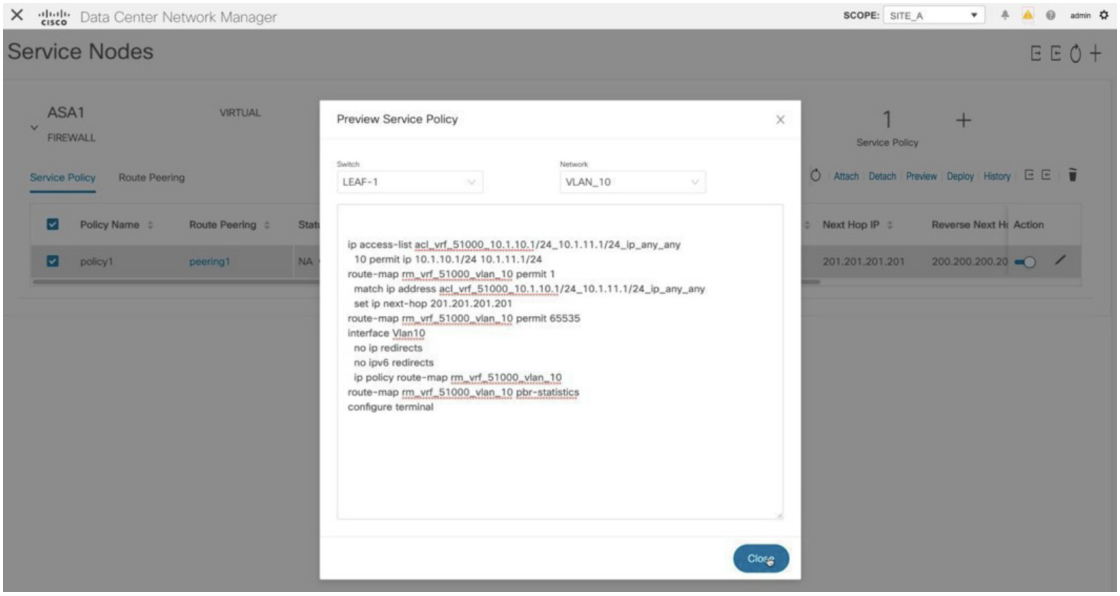
ステップ 2 **[アクション（Action）]**の下のトグルボタンをクリックして、このポリシーを有効にします。



ステップ 3 **[プレビュー（Preview）]**をクリックして、選択したネットワークの構成を表示します。

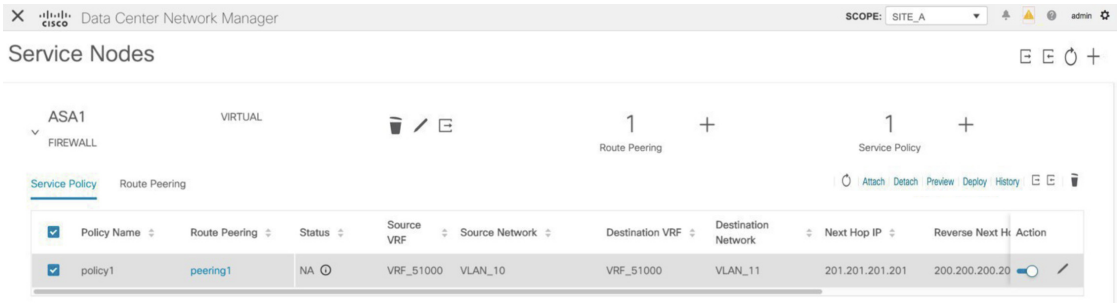


ステップ 4 ドロップダウンリストからスイッチと送信元、接続先、またはサービスネットワークを選択して、選択したスイッチ上の特定の送信元、接続先、またはサービスネットワークの目的の構成を表示します。このウィンドウでは、ルートマップで作成されるアクセスリストがあることがわかります。この構成は SVI にプッシュされます。

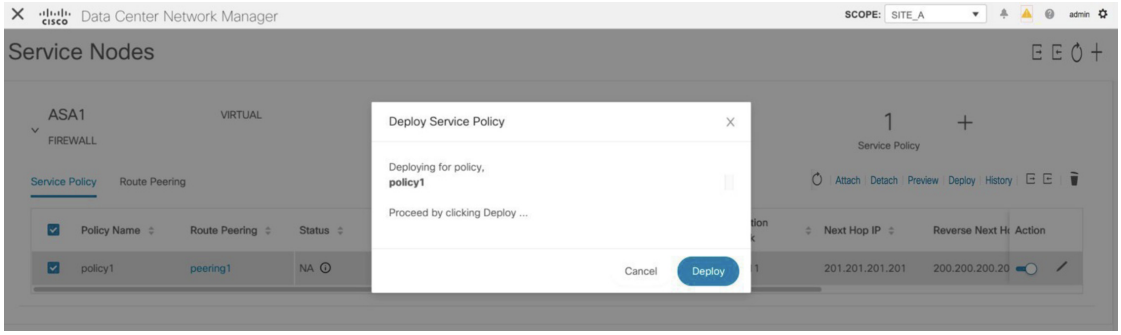


[閉じる（Close）] をクリックして、[サービス ポリシーのプレビュー（Preview Service Policy）] ウィンドウを閉じます。

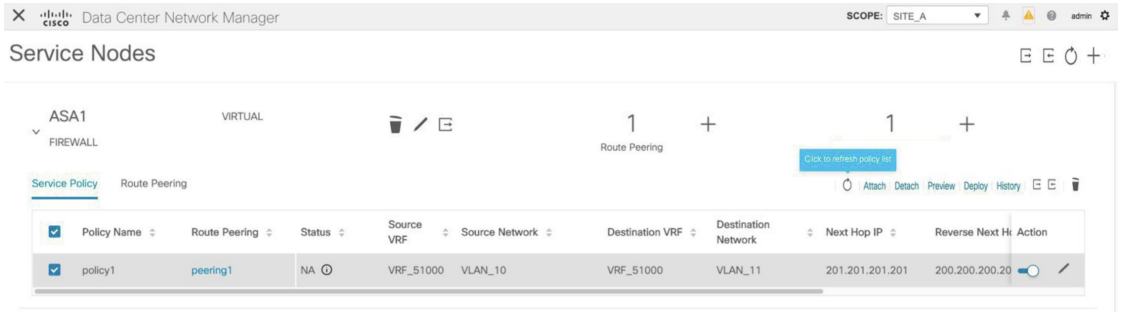
ステップ 5 **[サービス ノード（Service Nodes）]** ウィンドウで **[展開（Deploy）]** をクリックして、接続されたスイッチ（サービス リーフ）に構成を展開します。



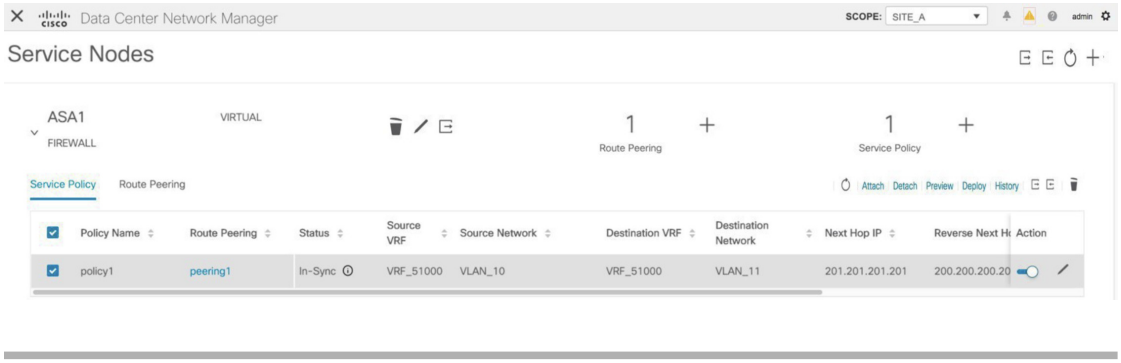
ポップアップ ウィンドウの **[展開（Deploy）]** ボタンをクリックして、展開を確認します。



ステップ 6 最新のポリシー アタッチメントと展開のステータスについては、**[更新（Refresh）]** アイコンをクリックします。



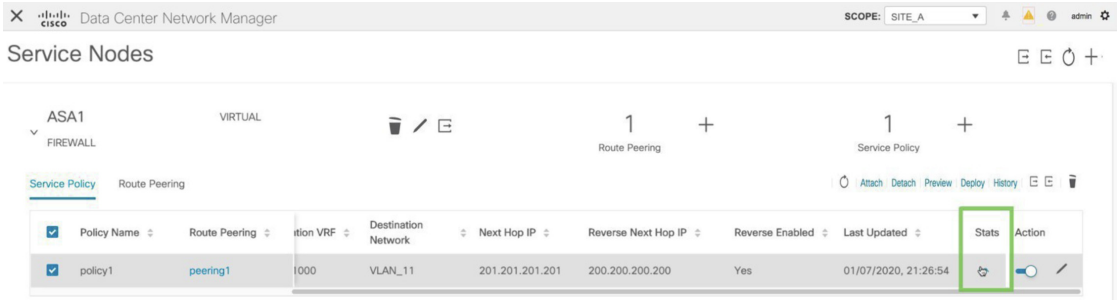
このポリシーは、送信元ネットワークと接続先ネットワークが接続されているスイッチ、およびサービス リーフにプッシュされます。ポリシーをプッシュすると、ステータス列に **[In-Sync]** と表示されます。



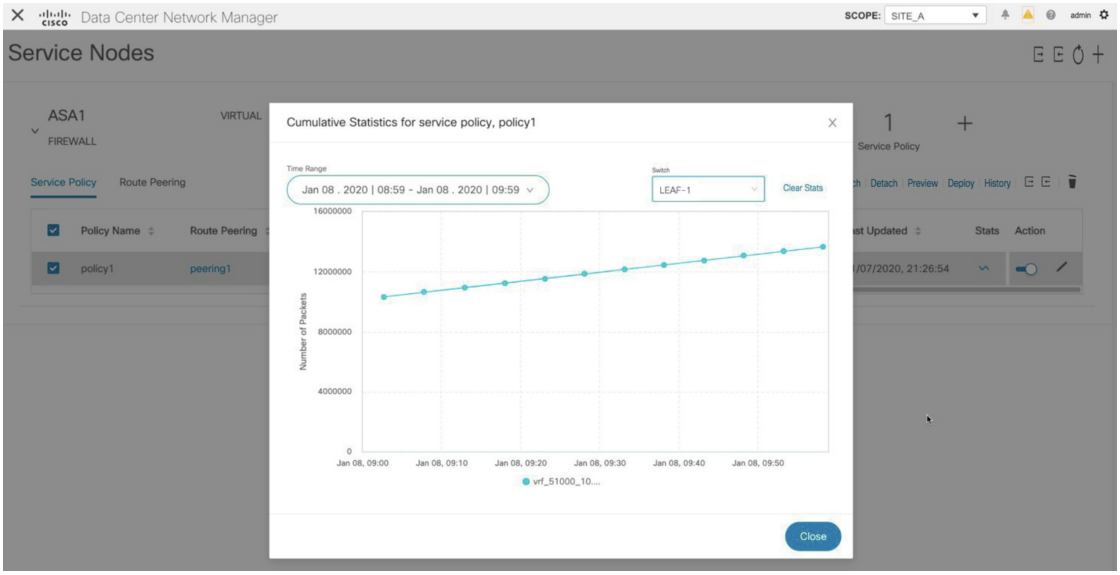
6. 統計情報を表示する

それぞれのリダイレクト ポリシーが展開されたので、ping 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。

DCNM でこのシナリオを視覚化するには、**[Stats]** 列の下にあるアイコンをクリックします。



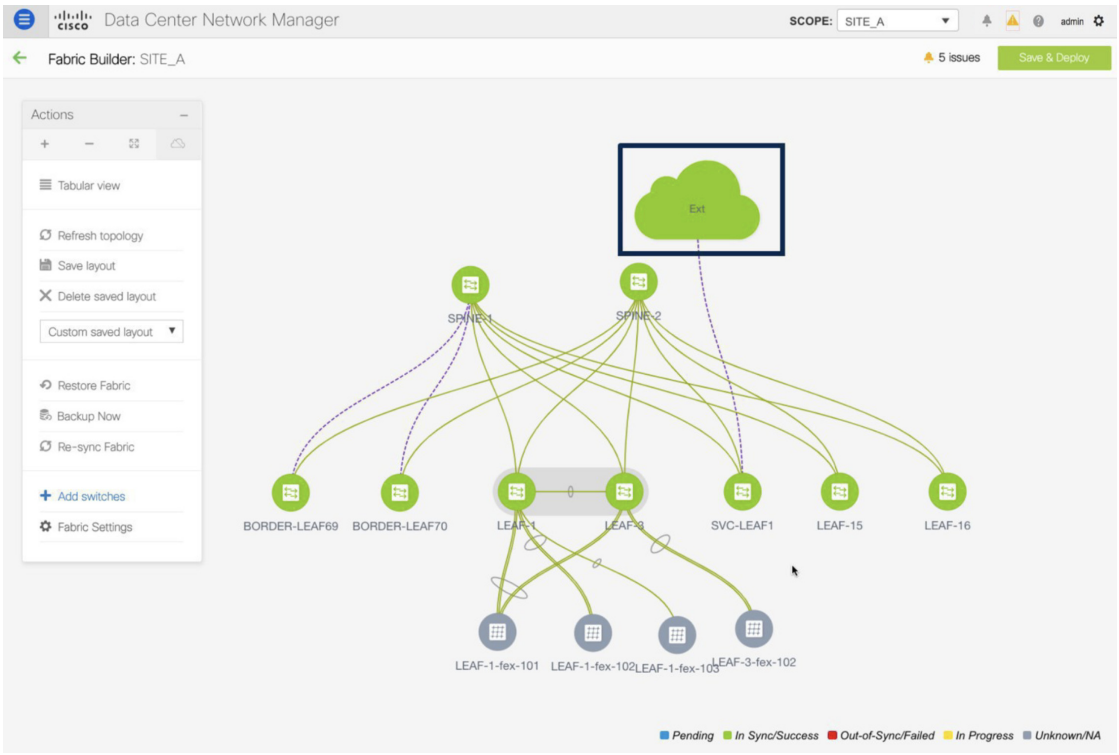
指定した時間範囲のポリシーの累積統計を表示できます。



送信元スイッチの転送トラフィック、接続先スイッチのリバース トラフィック、およびサービス スイッチの両方向のトラフィックの統計が表示されます。

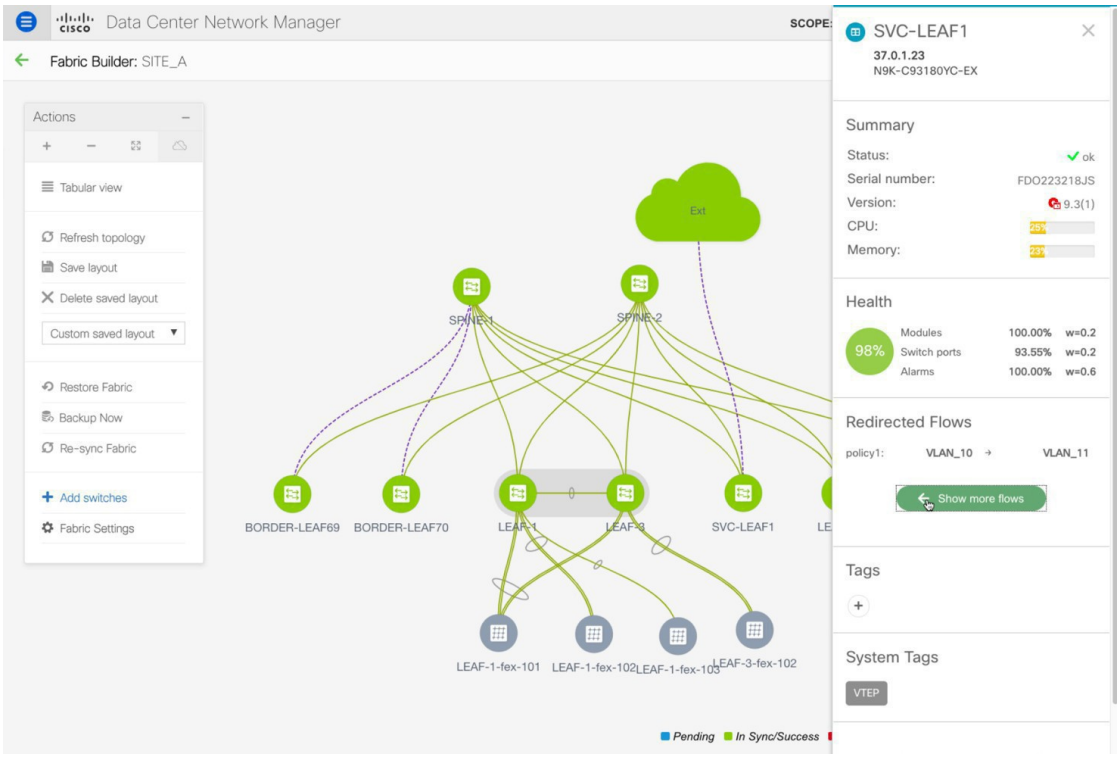
7. Fabric Builder でのトラフィック フローの表示

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ファブリック ビルダの DCNM トポロジでクラウド アイコンとして表示されます。

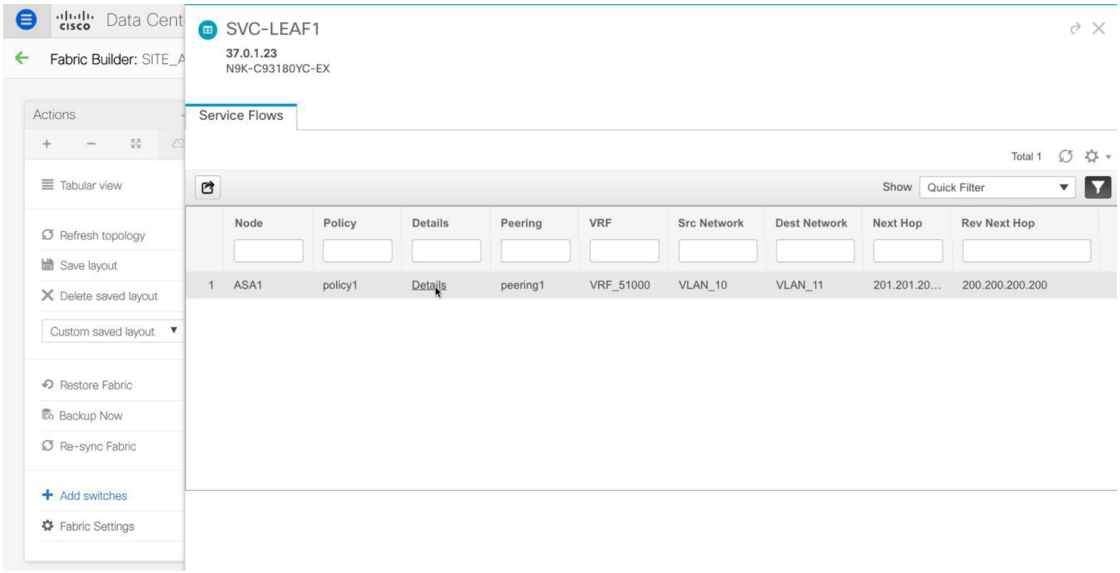


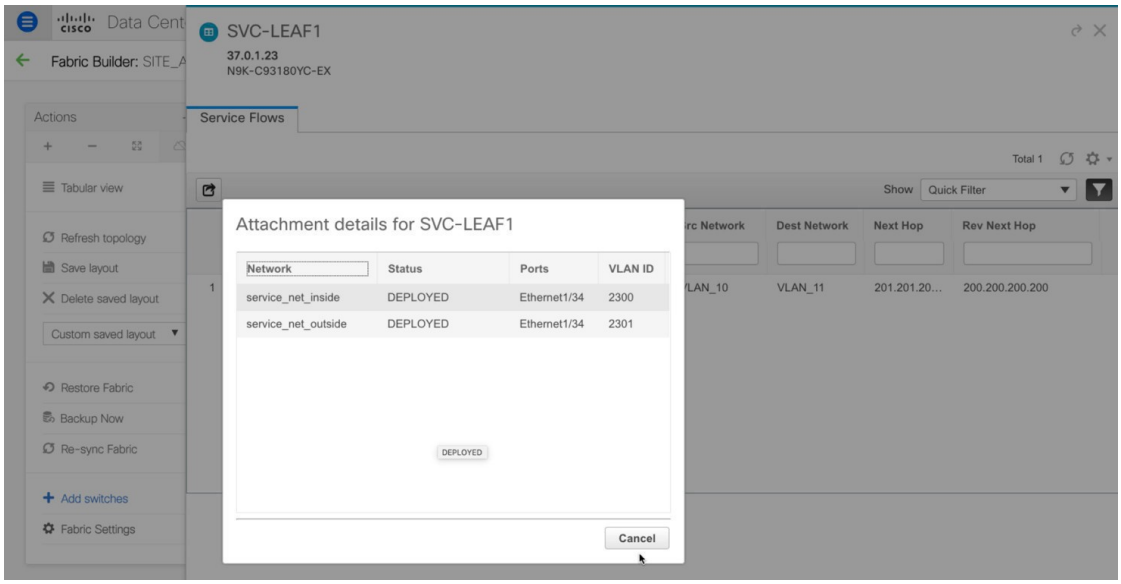
Procedure

ステップ 1 サービス リーフをクリックし、**[さらにフローを表示（Show more flows）]** をクリックします。リダイレクトされた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、付属ファイルの詳細を表示します。

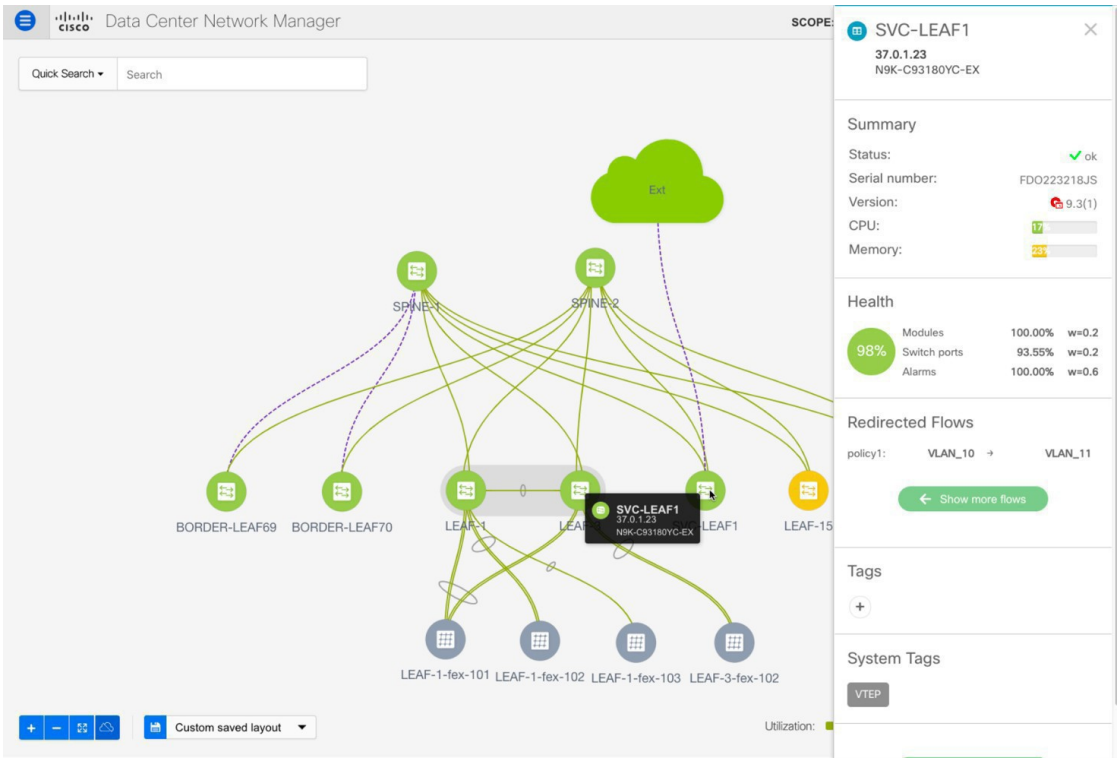




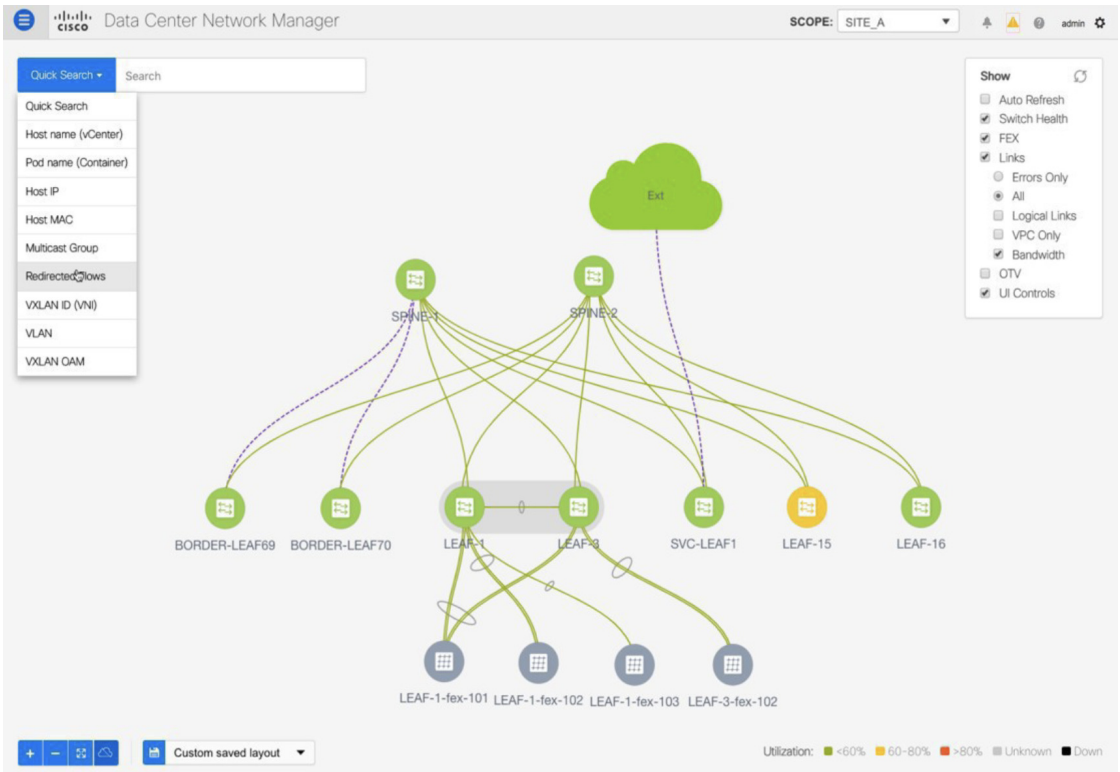
8.[トポロジ（Topology）]ウィンドウでの宛先へリダイレクトされたフローの視覚化

Procedure

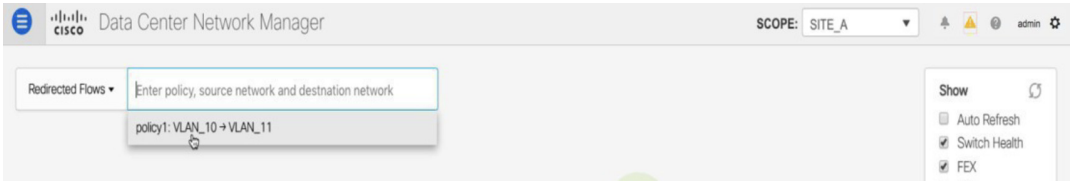
ステップ 1 **[トポロジ（Topology）]** をクリックし、リーフをクリックして、宛先にリダイレクトされたフローを視覚化します。



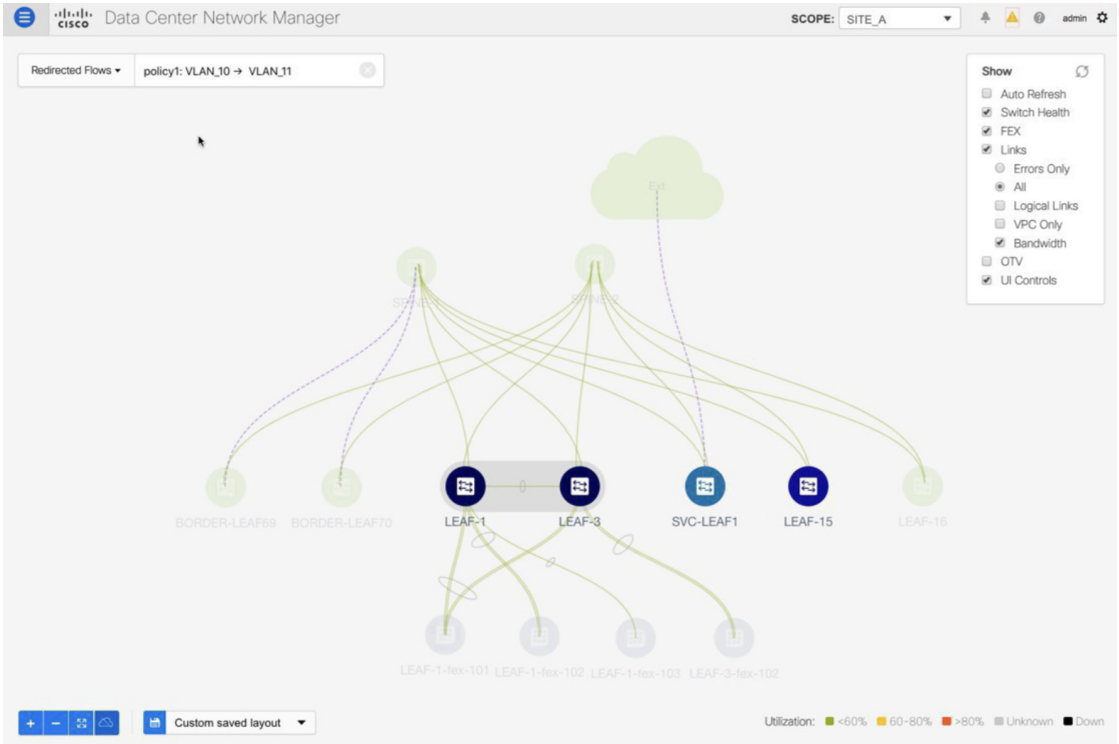
ステップ 2　ドロップダウンリストから**[リダイレクトされたフロー（Redirected Flows）]**を選択します。



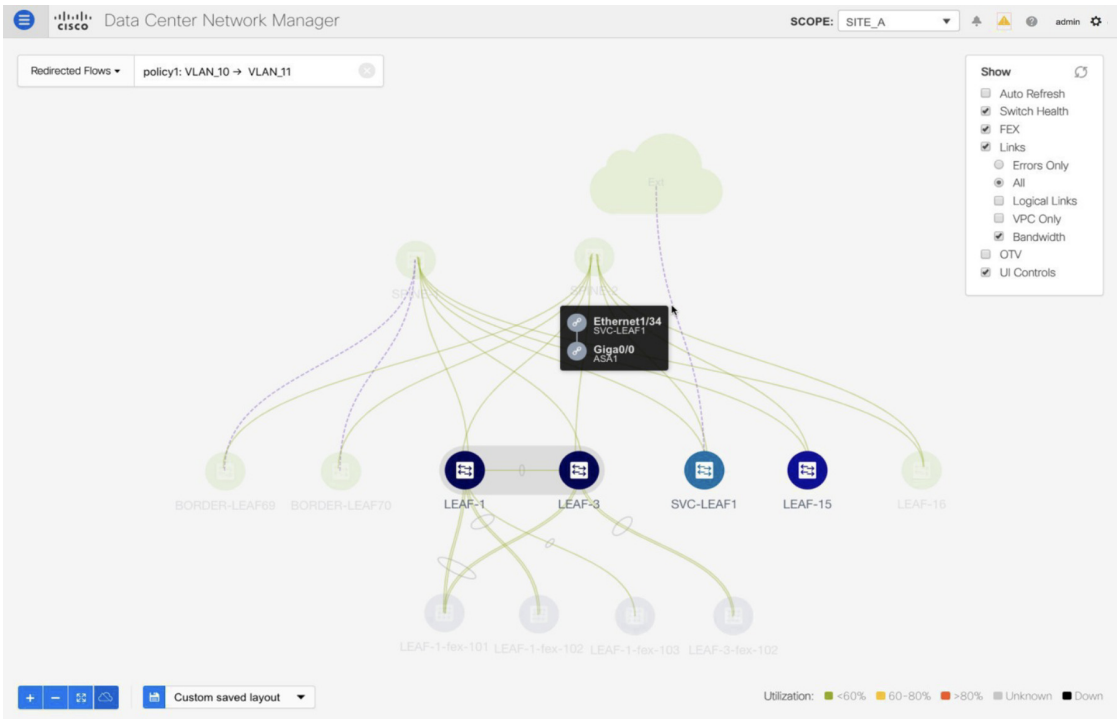
ステップ 3 ドロップダウンリストからポリシーを選択するか、検索フィールドにポリシー名、送信元ネットワーク、および接続先ネットワークを入力して検索を開始します。検索フィールドへの入力を始めると、自動的に補完されます。



送信元ネットワークと接続先ネットワークが接続され、フローがリダイレクトされたスイッチは、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、DCNM 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。

[制御（Control）] > [ファブリック（Fabrics）] > [サービス（Services）] の順に選択します。

このユースケースは、次の手順で構成されます。

Note

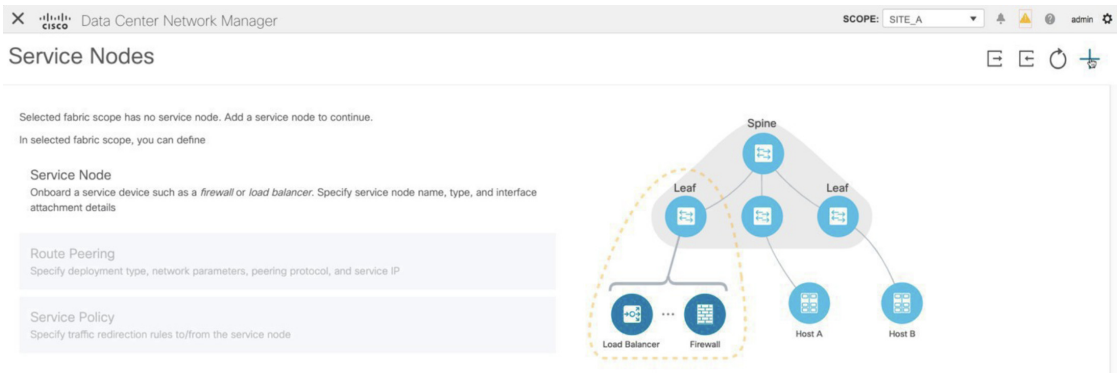
- 一部の手順は、テナント内ファイアウォール展開のユースケースで示されている手順に似ているため、そのユースケースへの参照リンクが含められています。
- サービス ポリシーは、テナント間ファイアウォールの展開には適用されません。

1. サービス ノードの作成

Procedure

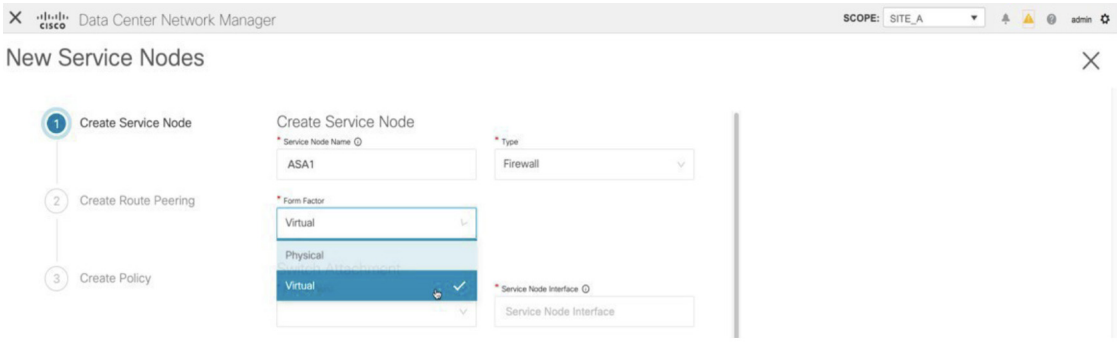
ステップ 1 **[範囲（Scope）]** ドロップダウンリストから、**[Site_A]** を選択します。

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。



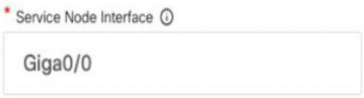
ステップ 3 ノード名を入力し、**[ファイアウォール（Firewall）]** を指定します（**[タイプ（Type）]** ドロップダウン ボックス）。**[サービス ノード名（Service Node Name）]** は一意である必要があります。

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。DCNM 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 **[次へ（Next）]** 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 1060 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

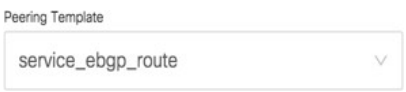
ステップ 1 ピアリング名を入力し、**[テナント間ファイアウォール（Inter-Tenant Firewall）]** を **[展開（Deployment）]** ドロップダウン リストから選択します。**[ピアリング オプション（Peering Option）]** ドロップダウン リストから、**[eBGP ダイナミック ピアリング（eBGP Dynamic Peering）]** を選択します。

ステップ 2 **[内部ネットワーク（Inside Network）]** で、**[VRF]** ドロップダウンリストから既に存在する 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。

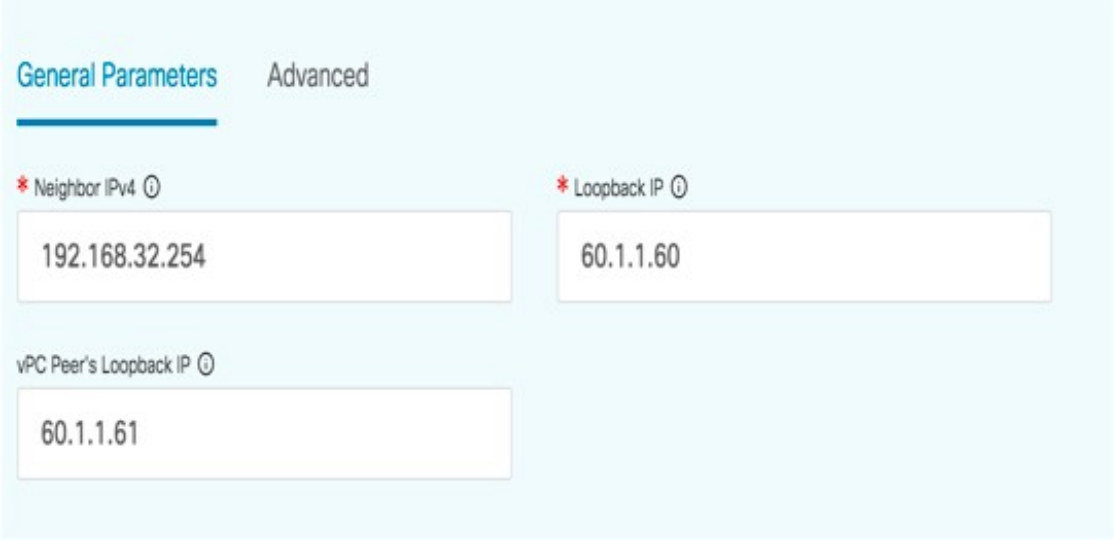
[サービス ネットワーク（Service Network）] の名前を入力し、**[Vlan ID]** を指定します。**[提案（Propose）]** をクリックして、DCNM が次に使用可能な VLAN ID をファブリック設定で指定されたサービス ネットワーク VLAN ID の範囲からフェッチできるようにすることもできます。デフォルトの**[サービス ネットワーク テンプレート（Service Network Template）]** は **Service_Network_Universal** です。

[一般パラメータ] 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。



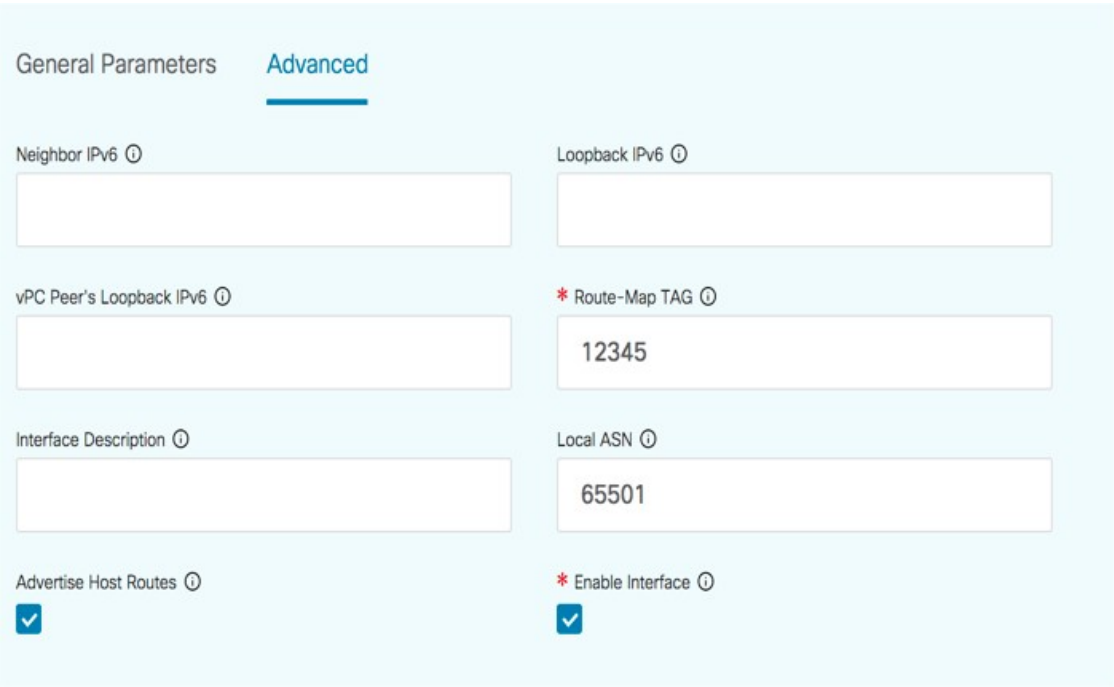
[一般パラメータ（General Parameters）] タブで、**[ネイバー IPv4（Neighbor IPv4）]** アドレス、**[ループバック IP（Loopback IP）]** アドレス、および **[vPC ピアのループバック IP（vPC Peer's Loopback IP）]** アドレスを指定します。ボーダー スイッチは vPC ペアです。



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。

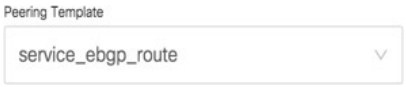
[ホスト ルートのアドバタイズ（Advertise Host Routes）] チェック ボックスがオンになっている場合、/32 および /128 ルートがアドバタイズされます。このチェックボックスが選択されていない場合、プレフィックス ルートがアドバタイズされます。

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。

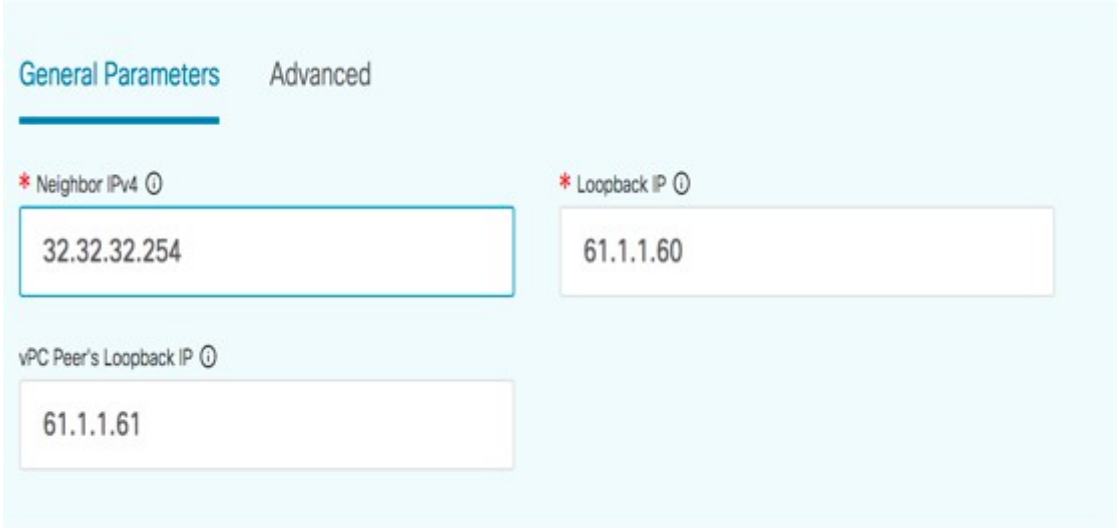


ステップ 5 **[外部ネットワーク（Outside Network）]** で必要なパラメータを指定し、**[リバース トラフィックのネクスト ホップ IP アドレス（Next Hop IP Address for Reverse Traffic）]** を指定します。リバース トラフィックのこのネクスト ホップ アドレスは、「外部サービス ネットワーク」サブネット内にある必要があります。

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。



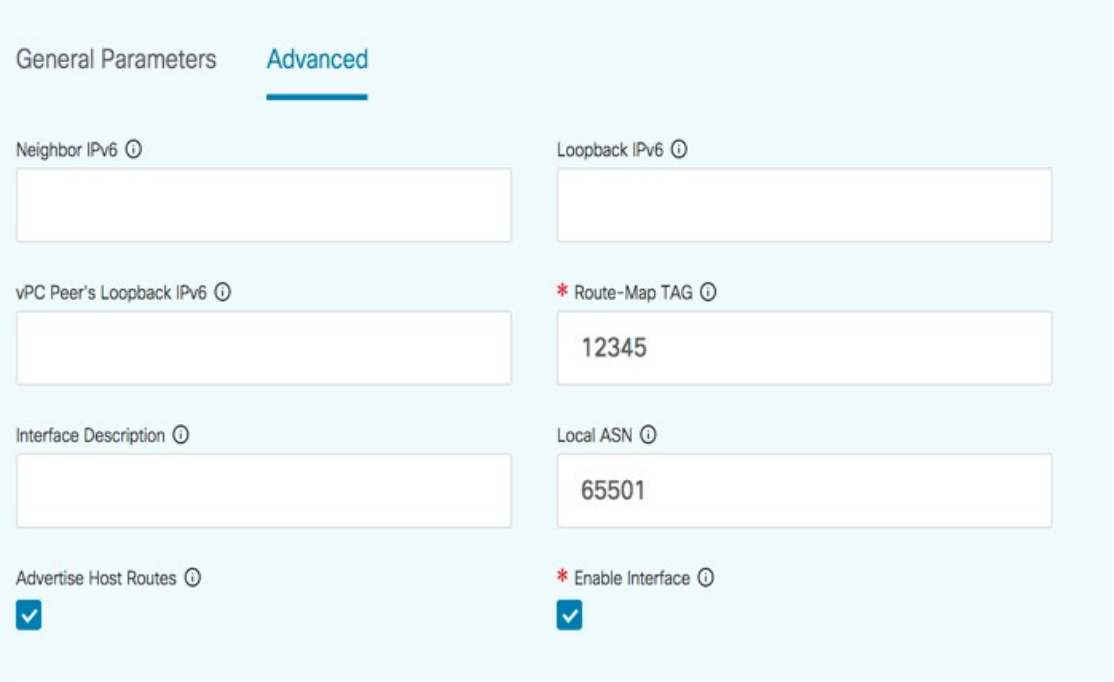
[一般パラメータ（General Parameters）] タブの、**[ネイバー IPv4（Neighbor IPv4）]** アドレス、**[ループバック IP（Loopback IP）]** アドレス、および **[vPC ピアのループバック IP（vPC Peer's Loopback IP）]** アドレスです。リーフ スイッチは vPC ペアです。



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 **[次へ（Next）]** 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 1068 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に注意してください。

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、DCNM 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。

[制御（Control）] > [ファブリック（Fabrics）] > [サービス（Services）] の順に選択します。

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、そのユースケースへの参照リンクが含められています。

1. サービス ノードの作成

Procedure

ステップ 1 **[範囲（Scope）]** ドロップダウンリストから、**Site_A** を選択します。

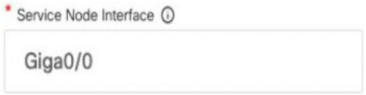
ステップ 2 **[追加（Add）]** アイコン（**[サービス ノード（Service Nodes）]** ウィンドウ）をクリックします。

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。

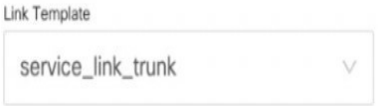
ステップ 5 **[スイッチの接続（Switch Attachment）]** セクションで、**[外部ファブリック（External Fabric）]** ドロップダウン リストから、サービス ノード（たとえば、ASA ファイアウォール）が配置されている外部ファブリックを選択します。サービス ノードは外部ファブリックに属している必要があることに注意してください。これは、サービス ノードを作成する際の前提条件です。

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。

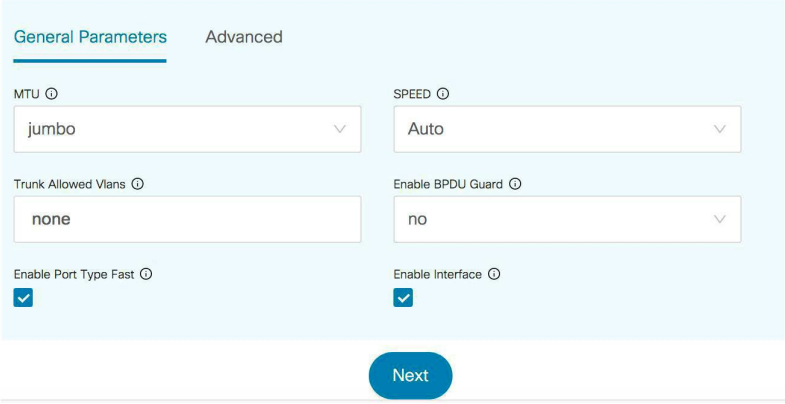


ステップ 7 サービス リーフである接続されたスイッチと、サービス リーフ上の対応するインターフェイスを選択します。

ステップ 8 **service_link_trunk** テンプレートを選択します。DCNM 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 **[次へ（Next）]** 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 1060 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

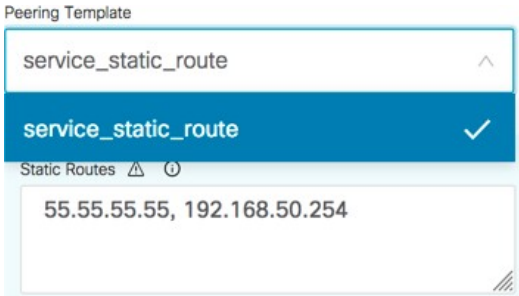
ステップ 1 ピアリング名を入力し、**[ワンアーム モード（One-Arm Mode）]** を選択します（**[展開（Deployment）]** ドロップダウン リスト）。また、**[ピアリング オプション（Peering Option）]** ドロップダウン リストから、**[静的ピアリング（Static Peering）]** を選択します。

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すでに存在する 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、DCNM 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。

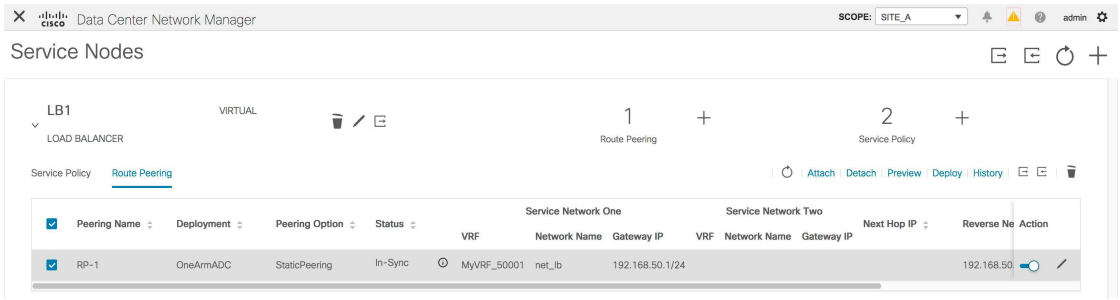
[一般パラメータ] タブで、サービス ネットワークのゲートウェイ アドレスを指定します。**[ネクストホップ IP アドレス（Next Hop IP Address）]** を指定します。このネクスト ホップ アドレスは、最初のアームのサブネット内にある必要があります。**[詳細設定（Advanced）]** タブの、デフォルトの **[ルーティング タグ（Routing Tag）]** 値は 12345 です。

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 **[次へ（Next）]** 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

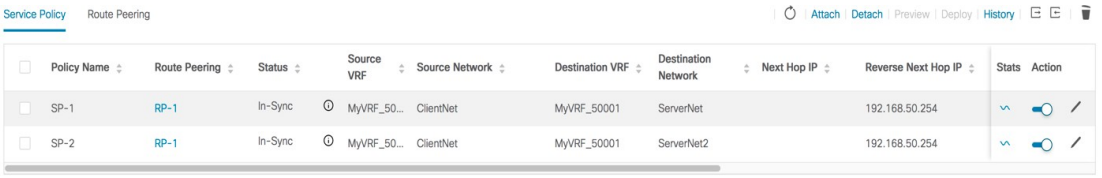
Intra-Tenant ファイアウォール展開のユースケースの 3. サービス ポリシーの作成, on page 1065 を参照してください。

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の 4. ルート ピアリングを展開する, on page 1068 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の 5. サービス ポリシーの展開, on page 1070 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 1072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 1073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 1076を参照してください。

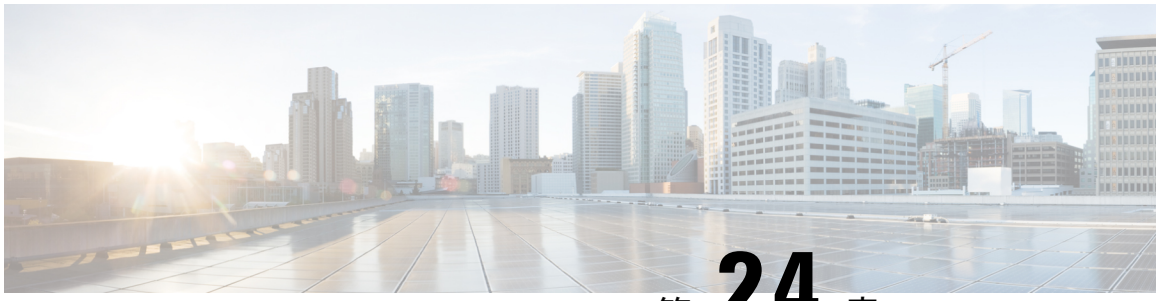
サービス リーフの VRF 構成は以下のとおりです。

```
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
```

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

第 VI 部

パブリッククラウドの接続



第 24 章

Cisco データセンターとパブリッククラウドの接続

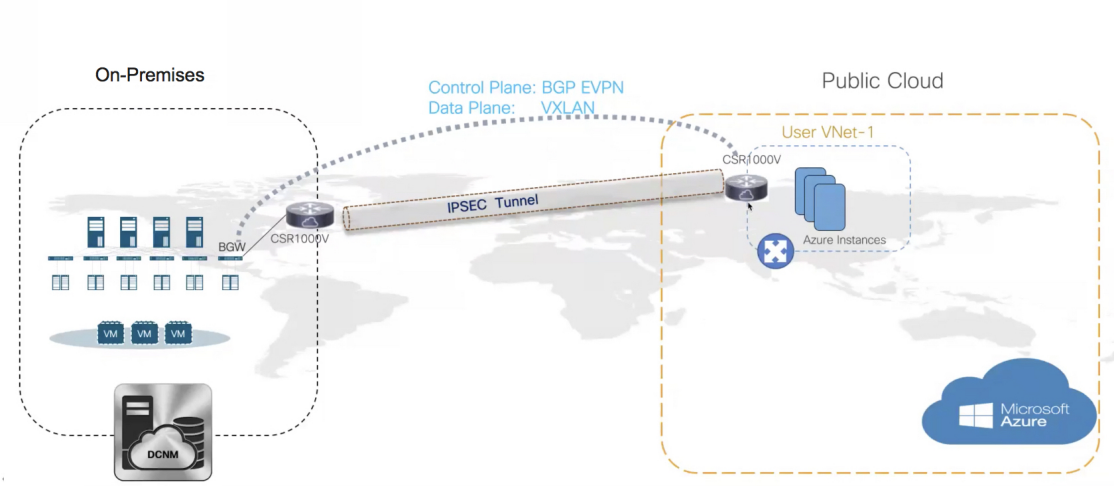
Cisco データセンターとパブリッククラウドの接続

このセクションでは、Cisco DCNM でプロビジョニングされた VXLAN EVPN ファブリックから Microsoft Azure パブリッククラウドへのパブリッククラウド接続を可能にする 機能について説明します。 レイヤ 3 接続により、オンプレミスのワークロードと Microsoft Azure クラウド間のシームレスで安全な通信が保証されます。接続は、Cisco DCNM によって管理される シスコ クラウド サービス ルータ 1000v（Cisco CSR 1000v）を介してプロビジョニングされます。コントロール プレーンには BGP EVPN が採用され、データ プレーンには VXLAN が採用されています。オンプレミスの Cisco CSR 1000v とパブリッククラウドの Cisco CSR 1000v の間に、セキュアな IPsec トンネルが確立されます。

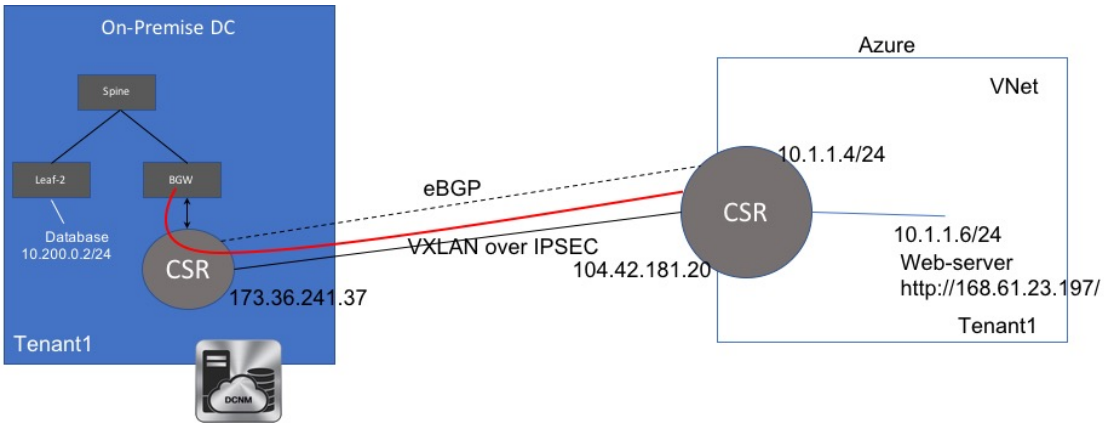
（注） Cisco DCNM は、 Cisco CSR 1000v の検出と管理をサポートします。この機能は、Cisco DCNM リリース 11.2(1) のプレビュー機能です。Cisco DCNM リリース 11.3(1) へのインライン アップグレード後、この機能はデフォルトで有効になります。

トポロジ概要

図 *11* : トポロジの概要



オンプレミスのデータセンターには、必要なスイッチがあります。これらのスイッチの 1 つは、パブリッククラウドへの WAN 接続向けに、コア ルータとインターフェイス接続するボーダーゲートウェイ（BGW）です。Cisco CSR 1000v は、この使用例のコア ルータです。このコア ルータを Cisco DCNM の外部ファブリックにインポートできます。次の図は、採用されているサンプル トポロジを示しています。



この例では、スタンドアロン リーフの背後にある VM と特定のユーザ VNET 内の Microsoft Azure クラウド内の VM との間にレイヤ 3 接続を提供するために必要なタスクをリストします。

パブリッククラウドには、Cisco CSR 1000v、Microsoft Azure インスタンス、Azure 仮想ネットワーク（Azure VNet）、および VM があります。クラウドの Cisco CSR 1000v には、VM とのインターフェイスがあります。

アンダーレイ ルーティングと到達可能性を交換するために、2 つのコア ルータ間で eBGP を使用しています。VXLAN は、オンプレミスの BGW と Microsoft Azure のコア ルータを IPsec トンネル経由で接続します。

このユースケースでは、次のようにセットアップを構成します。

ガイドラインと制約事項

オンプレミス データ センターとパブリッククラウドを接続するためのガイドラインと制限は次のとおりです。

- Cisco CSR 1000v シリーズ ルータは、ルートベースの IP セキュリティ（IPsec）トンネル インターフェイスをサポートしています。
- Cisco DCNM の VXLAN EVPN Easy ファブリックで Cisco Nexus 9000 シリーズ スイッチまたは Cisco Nexus 3000 シリーズ スイッチを使用します。
- このドキュメントで指定されている IP アドレスは、サンプル アドレスです。セットアップに実稼働ネットワークで使用されている IP アドレスが反映されていることを確認します。

前提条件

- Microsoft Azure でアカウントを作成します。
- Microsoft Azure でパブリッククラウド コア ルータの VNet を作成します。
- Microsoft Azure に Cisco CSR 1000v を展開します。この Cisco CSR 1000v は、パブリッククラウド コア ルータです。詳細については、Microsoft Azure での Cisco CSR 1000v の展開（1119 ページ）を参照してください。
- ボーダーゲートウェイが必要なため、Cisco NX-OS リリース 7.0(3)I7(x) 以降のバージョンをサポートするスイッチを使用します。
- パブリック インターネットにアクセスできるように、DMZ または同等のゾーン内の Cisco DCNM、スイッチ、Cisco CSR 1000v、およびその他のデバイスをセットアップします。
- 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 DCNM を介した構成に精通していること。
- MSD ファブリックに精通していること。

（注） 設定に必要なさまざまなタスクについては、『*Cisco DCNM LAN* ファブリックの構成ガイド』の「制御」の章を参照してください。

タスクの概要

次のセクションでは、オンプレミスデータセンターとパブリッククラウド間の接続を確立するためのタスクの概要を示します。

オンプレミス データセンター

1. ポーリング時間を設定します。
2. オンプレミスデータセンター用のスイッチを備えたファブリックを作成し、いずれかのスイッチに BGW ロールを構成します。
3. オンプレミス コア ルータの外部ファブリックを作成します。コア ルータとして Cisco CSR 1000v を検出します。
4. BGW 上のオンプレミス ホストとして IP アドレスをシミュレートします。

パブリック クラウド

1. パブリッククラウド コア ルータの外部ファブリックを作成します。
2. コア ルータであるパブリッククラウドの Cisco CSR 1000v を検出します。

接続

1. MSD ファブリックを作成し、以前に作成したファブリックをインポートします。
2. BGW とオンプレミスのコア ルータを接続します。
3. オンプレミス コア ルータとパブリッククラウド コア ルータの間に IPsec トンネルを作成します。
4. IPsec トンネル上で実行されるコア ルータ間に eBGP アンダーレイ接続を作成します。
5. VXLAN EVPN を使用して、BGW とパブリッククラウド コア ルータを接続します。
6. ファブリック内の VRF を拡張します。

このセクションの各タスクに含まれる手順については、次のセクションで説明します。

ポーリング時間の設定

Cisco DCNM は、オンプレミス コア ルータにクエリを実行し、設定したポーリング時間に応じてルーティング テーブルの状態を更新します。Cisco DCNM Web UI からのポーリング時間を設定するには、次の手順を実行します。

Procedure

ステップ 1 **[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** を選択します。

[サーバー プロパティ（Server Properties）] ウィンドウが表示されます。

ステップ 2 **[プライベート クラウドとパブリッククラウドの接続（Private and public cloud connectivity）]** プロパティを見つけます。

ステップ 3 **[private_public_cloud_connectivity.stats.polling_time]** フィールドにポーリング時間を設定します。

値はミリ秒単位です。

```
# Private and public cloud connectivity
#
                                    preview_features.enable true

        private_public_cloud_connectivity.stats.polling_time 300000


#
```

ステップ 4 [Apply Changes] をクリックします。

ステップ 5 **appmgr restart dcnm** コマンドを使用して Cisco DCNM を再起動します。

Cisco DCNM Web UI にログインすると、有効になっているプレビュー機能に関する警告が表示されます。

Note これはプレビューのみの機能です。この機能は、実稼働環境ではなく、実験用セットアップでのみ使用することが推奨されています。

CSR1000vを使用したオンプレミスの外部ファブリックのセットアップ

オンプレミス エッジ ルータの外部ファブリックを作成します。

外部ファブリックの作成

Cisco DCNM Web UI から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。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 [ファブリックの作成（Create Fabric）] をクリックします。

[ファブリックの追加（Add Fabric）] ダイアログボックスが表示されます。

ステップ 3 **[ファブリック名（Fabric Name）]** フィールドにファブリック名を **[CSR-OnPrem]** として入力します。

ステップ 4 [ファブリック テンプレート（Fabric Template）] ドロップダウンリストから **[External_Fabric_11_1]** を選択します。

ステップ 5 **[BGP AS #]** フィールドに BGP AS 番号を入力します。

ステップ 6 **[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。

ステップ 7 [保存（Save）] をクリックします。

ファブリックが作成され、[ファブリック トポロジ（fabric topology）] ウィンドウが表示されます。

What to do next

オンプレミスのコア ルータを検出します。

オンプレミス コア ルータの検出

Cisco CSR 1000v は、オンプレミスのコア ルーティングに使用されます。ファブリック トポロジ ウィンドウでコア ルータを検出するには、次の手順を実行します。

Before you begin

コア ルータのログイン情報を確認してください。

Procedure

ステップ 1 [アクション（Actions）] ペインで **[スイッチの追加（Add switches）]** をクリックします。

[インベントリ管理（Inventory Management）] ダイアログボックスが表示されます。

ステップ 2 [既存スイッチの検出（Discover Existing Switches）] タブの次のフィールドに値を入力します。

フィールド	説明
シードIP	コア ルータの IP アドレスを入力します。
デバイスタイプ（Device Type）	ドロップダウンリストから **[IOS XE]** を選択して、**[CSR]** ラジオ ボタンをクリックします。
ユーザ名	SSH アクセス向けのコア ルータのユーザー名を入力します。
パスワード	SSH アクセス向けのコア ルータのパスワードを入力します。

Note すでに検出されているスイッチを検出しようとすると、エラーが表示されます。

ステップ 3 [検出の開始（Start Discovery）] をクリックします。

ファブリック トポロジ ウィンドウが表示され、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。

Note スイッチの検出には時間がかかる場合があります。

ステップ 4 [アクション（Actions）] ペインで **[表形式ビュー（Tabular view）]** をクリックします。

スイッチとリンクのウィンドウが表示され、スキャンの詳細を確認できます。検出が進行中の場合、検出ステータスは赤色の [検出中（discovering）] でありその横に警告アイコンが表示されます。

ステップ 5 コア ルータの詳細を表示します。

ルーターが検出された後：

- 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）]** 列のルータの値が **[同期中（In-Sync）]** と表示されます。

ステップ 6 ファブリック トポロジ ウィンドウに戻り、トポロジを更新します。

What to do next

ルータのロールを **[コア ルータ（Core Router）]** に設定します。ルータを右クリックして、**[ロールの設定（Set role）] > [コア ルータ（Core Router）]** を選択します。

BGW を備えたオンプレミス データセンターの VXLAN EVPN ファブリックを設定します。

VXLAN EVPN ファブリックの設定

BGW のファブリックを作成します。

VXLAN EVPN ファブリックの作成

Cisco DCNM Web UI から VXLAN EVPN ファブリックを作成するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 [ファブリックの作成（Create Fabric）] をクリックします。

[ファブリックの追加（Add Fabric）] ダイアログボックスが表示されます。

ステップ 3 **[ファブリック名（Fabric Name）]** フィールドにファブリック名を **[site2]** として入力します。

ステップ 4 **[ファブリック テンプレート（Fabric Template）]** ドロップダウンリストから **[Easy_Fabric_11_1]** を選択します。

ステップ 5 すべての必須フィールドに値を入力します。

ステップ 6 [保存（Save）] をクリックします。

ファブリックが作成され、[ファブリック トポロジ（fabric topology）] ウィンドウが表示されます。

What to do next

このファブリックにスイッチを追加し、いずれかのスイッチに BGW ロールを割り当てます。

BGW ロールの割り当て

BGW スイッチにロールを割り当てるには、次の手順を実行します。

Before you begin

[site2] ファブリックにスイッチを追加します。

Procedure

ステップ 1 BGW ロールを設定する必要があるスイッチを右クリックします。

スイッチで実行できるアクションのリストが表示されます。

ステップ 2 **[ロールの設定（Set role）] > [ボーダーゲートウェイ（Border Gateway）]** を選択します。

What to do next

パブリッククラウドのファブリックを設定します。

Azure での CSR を使用した外部ファブリックのセットアップ

パブリッククラウド コア ルータの外部ファブリックを作成します。

外部ファブリックの作成

Cisco DCNM Web UI から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。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 [ファブリックの作成（Create Fabric）] をクリックします。

[ファブリックの追加（Add Fabric）] ダイアログボックスが表示されます。

ステップ 3 **[ファブリック名（Fabric Name）]** フィールドにファブリック名を **[CSR-Azure]** として入力します。

ステップ 4 **[ファブリック テンプレート（Fabric Template）]** ドロップダウンリストから **[External_Fabric_11_1]** を選択します。

ステップ 5 **[BGP AS # フィールド（BGP AS # field）]** に BGP AS 番号を入力します。

ステップ 6 **[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。

ステップ 7 [保存（Save）] をクリックします。

ファブリックが作成され、[ファブリック トポロジ（fabric topology）] ウィンドウが表示されます。

What to do next

このファブリックでパブリッククラウド コア ルータを検出します。

コア ルータの検出

Cisco CSR 1000v シリーズ ルータは、パブリッククラウド コア ルーティングにも使用されます。ファブリック トポロジ ウィンドウでコア ルータを検出するには、次の手順を実行します。

Before you begin

コア ルータのログイン情報を確認してください。

Procedure

ステップ 1 [アクション（Actions）] ペインで [スイッチの追加（Add switches）] をクリックします。

[インベントリ管理（Inventory Management）] ダイアログボックスが表示されます。

ステップ 2 [既存スイッチの検出（Discover Existing Switches）] タブの次のフィールドに値を入力します。

フィールド	説明
シードIP	コア ルータの IP アドレスを入力します。
デバイスタイプ（Device Type）	ドロップダウンリストから **[IOS XE]** を選択して、**[CSR]** ラジオ ボタンをクリックします。
ユーザ名	SSHアクセス向けのコア ルータのユーザー名を入力します。

フィールド	説明
パスワード	SSHアクセス向けのコアルータのパスワードを入力します。

Note すでに検出されているスイッチ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。

ステップ 3 [検出の開始（Start Discovery）] をクリックします。

ファブリック トポロジ ウィンドウが表示され、右下にスイッチ検出に関するポップアップ メッセージが表示されます。次に例を示します。 **<ip-address> added for discovery**

Note スイッチの検出には時間がかかる場合があります。

ステップ 4 **[アクション（Actions）]** ペインで **[表形式ビュー（Tabular view）]** をクリックします。

スイッチとリンクのウィンドウが表示され、スキャンの詳細を確認できます。検出が進行中の場合、検出ステータスは赤色の [検出中（discovering）] でありその横に警告アイコンが表示されます。

ステップ 5 コア ルータの詳細を表示します。

ルータの検出後：

- 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）]** 列のルータの値が **[同期中（In-Sync）]** に変わります。

ステップ 6 ファブリック トポロジ ウィンドウに戻り、トポロジを更新します。

What to do next

ルータのロールを **[コア ルータ（Core Router）]** に設定します。ルータを右クリックして、**[ロールの設定（Set role）] > [コア ルータ（Core Router）]** を選択します。

MSD ファブリックを作成し、以前に作成した他のファブリックをそこにインポートします。

MSD ファブリックの接続の設定

接続のためにすべてのスタンドアロン ファブリックを結合する MSD ファブリックを作成します。

MSD ファブリックの作成

Cisco DCNM Web UI から MSD ファブリックを作成するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [ファブリック ビルダ（Fabric Builder）]** を選択します。

[ファブリック ビルダー（Fabric Builder）] ウィンドウが表示されます。

ステップ 2 [ファブリックの作成（Create Fabric）] をクリックします。

[ファブリックの追加（Add Fabric）] ダイアログボックスが表示されます。

ステップ 3 **[ファブリック名（Fabric Name）]** フィールドにファブリック名を **[Cloud-Connect]** として入力します。

ステップ 4 **[ファブリック テンプレート（Fabric Template）]** ドロップダウンリストから **[MSD_Fabric_11_1]** を選択します。

ステップ 5 すべての必須フィールドに値を入力します。

ステップ 6 [保存（Save）] をクリックします。

ファブリックが作成され、[ファブリック トポロジ（fabric topology）] ウィンドウが表示されます。

What to do next

他のファブリックをこの MSD ファブリックに移動します。

他のファブリックを MSD ファブリックに移動する

他のファブリックをファブリック トポロジ ウィンドウから **[Cloud-Connect]** ファブリックに移動するには、次の手順を実行します。

Procedure

ステップ 1 **[アクション（Actions）]** ペインで **[ファブリックの移動（Move Fabric）]** をクリックします。

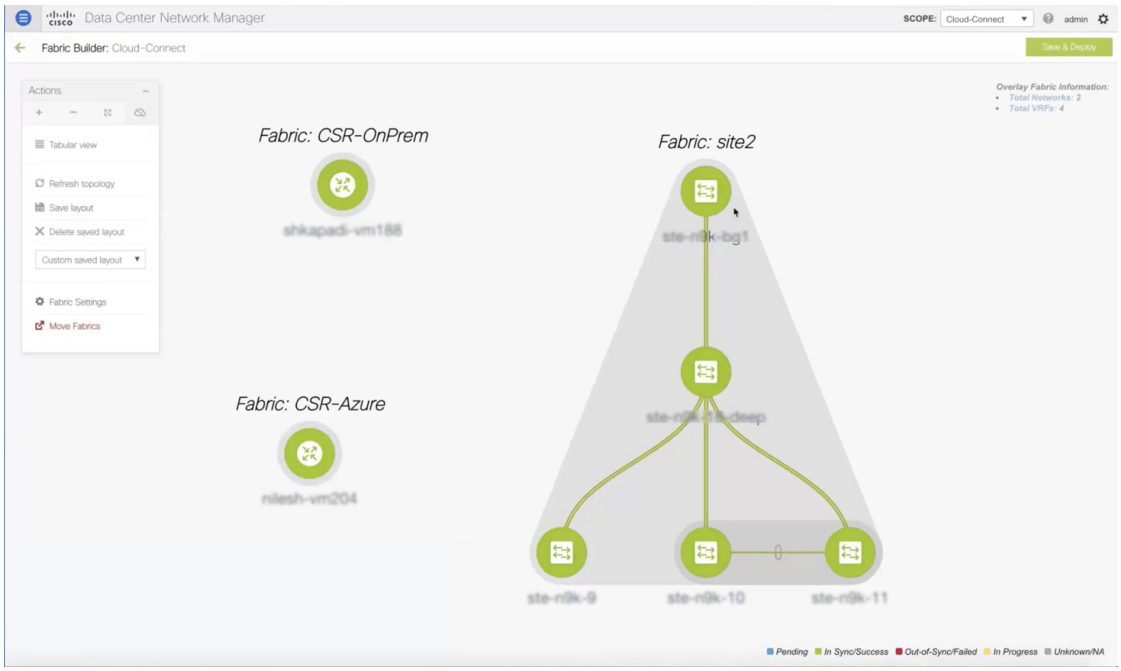
[ファブリックの移動（Move Fabric）] ダイアログボックスが表示されます。ファブリックのリストが含まれています。

ステップ 2 **[CSR-OnPRem]**、**[site2]**、および **[CSR-Azure]** ファブリックを選択します。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 ダイアログボックスを閉じて、ファブリック トポロジを更新します。

すべてのメンバー ファブリックが **[Cloud-Connect]** ファブリックに表示されます。



What to do next

ファブリック間の接続をセットアップします。

接続設定

異なるリンクを使用して、以前に作成したファブリックを接続します。

オンプレミス BGW とオンプレミス コア ルータの接続

オンプレミス BGW とオンプレミス コア ルータの間にリンクを追加するには、次の手順を実行します。

Procedure

ステップ 1 **[Cloud-Connect]** トポロジ ウィンドウの任意の場所を右クリックします。

ファブリックで実行できるアクションがリストに表示されます。または、ファブリック トポロジ ウィンドウから、**[アクション（Actions）]** ペインの **[表形式ビュー（Tabular view）]** を選択し、**[リンク（Links）]** タブをクリックします。

ステップ 2 **[リンクの追加（Add Link）]** を選択します。

[リンク管理（Link Management）- リンクの追加（Add Link）] ダイアログボックスが表示されます。

ステップ 3 次のフィールドに値を入力します。

フィールド	説明
リンクタイプ	ドロップダウンリストから **[ファブリック間（Inter-Fabric）]** リンク タイプを選択します。
リンク サブタイプ	ドロップダウンリストから **[MULTISITE_UNDERLAY]** リンク サブタイプを選択します。
リンク テンプレート	ドロップダウンリストから **[csr_ext_multisite_underlay_setup]** リンク テンプレートを選択します。 **Note** このテンプレートは、プレビュー機能を有効にして DCNM を再起動した後にのみ使用できます。
送信元ファブリック	ドロップダウンリストから送信元ファブリックとして **[site2]** を選択します。
接続先ファブリック	ドロップダウンリストから接続先ファブリックとして **[CSR-OnPrem]** を選択します。
送信元デバイス（Source Device）	ドロップダウン リストから BGW を選択します。
送信元インターフェイス（Source Interface）	BGW のインターフェースを選択します。
接続先デバイス	ドロップダウンリストからオンプレミス コア ルータを選択します。
宛先インターフェイス	ドロップダウンリストからオンプレミス コア ルータのインターフェイスを選択します。

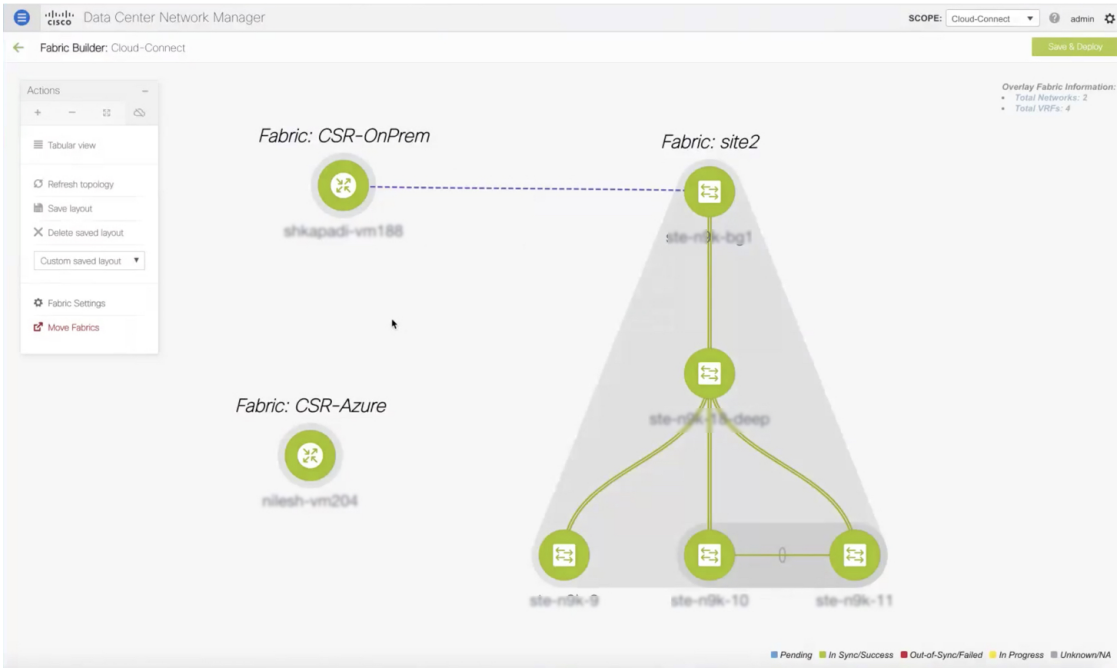
ステップ 4 **[全般（General）]** タブの **[リンク プロファイル（Link Profile）]** エリアにある次のフィールドに値を入力します。

フィールド	説明
IP_MASK	サブネットを持つ送信元インターフェイスの IPv4 アドレスを入力します。
NEIGHBOR_IP	接続先インターフェイスの IPv4 アドレスを入力します。

Cisco DCNM Web UI から IP アドレスを確認するには、**[制御（Control）] > [ファブリック（Fabrics）] > [インターフェイス（Interfaces）]** を選択します。**[範囲（Scope）]** ドロップダウンリストからファブリックを選択し、デバイスを検索します。デバイスの IP アドレスが **[IP/プレフィックス（IP/Prefix）]** 列に表示されます。

ステップ 5 [保存（Save）] をクリックします。

[ファブリック トポロジ（fabric topology）] ウィンドウが更新されます。**site2** ファブリックのオンプレミス BGW と **CSR-OnPrem** ファブリックのオンプレミス コア ルータの間にリンクが追加されます。



What to do next

オンプレミス コア ルータとパブリック クラウド コア ルータを接続します。

IPsec トンネルを使用したオンプレミス コア ルータとパブリッククラウド コア ルータの接続

オンプレミス コア ルータ とパブリッククラウド コア ルータの間にリンクを追加するには、次の手順を実行します。

Procedure

ステップ 1 **[Cloud-Connect]** トポロジ ウィンドウの任意の場所を右クリックします。

ファブリックで実行できるアクションがリストに表示されます。または、ファブリック トポロジ ウィンドウから、**[アクション（Actions）]** ペインの **[表形式ビュー（Tabular view）]** を選択し、**[リンク（Links）]** タブをクリックします。

ステップ 2 **[リンクの追加（Add Link）]** を選択します。

[リンク管理（Link Management）- リンクの追加（Add Link）] ダイアログボックスが表示されます。

ステップ 3 次のフィールドに値を入力します。

フィールド	説明
リンクタイプ	ドロップダウンリストから**[ファブリック間（Inter-Fabric）]** リンク タイプを選択します。
リンク サブタイプ	ドロップダウンリストから **[BGP_OVER_IPSEC]** リンク サブタイプを選択します。
リンク テンプレート	ドロップダウンリストから **[csr_link_template]** リンク テンプレートを選択します。
送信元ファブリック	ドロップダウンリストから送信元ファブリックとして **[CSR-OnPrem]** を選択します。
接続先ファブリック	ドロップダウンリストから接続先ファブリックとして **[CSR-Azure]** を選択します。
送信元デバイス（Source Device）	ドロップダウンリストからオンプレミス コア ルータを選択します。
送信元インターフェイス（Source Interface）	オンプレミス コア ルータのインターフェイスを選択します。
接続先デバイス	ドロップダウンリストからパブリッククラウド コア ルータを選択します。
宛先インターフェイス	ドロップダウンリストからパブリッククラウド コア ルータのインターフェイスを選択します。

ステップ 4 **[全般（General）]** タブの **[リンク プロファイル（Link Profile）]** エリアで、IPSec トンネルに使用されるパス キーを **[SHARED_KEY]** フィールドに入力します。

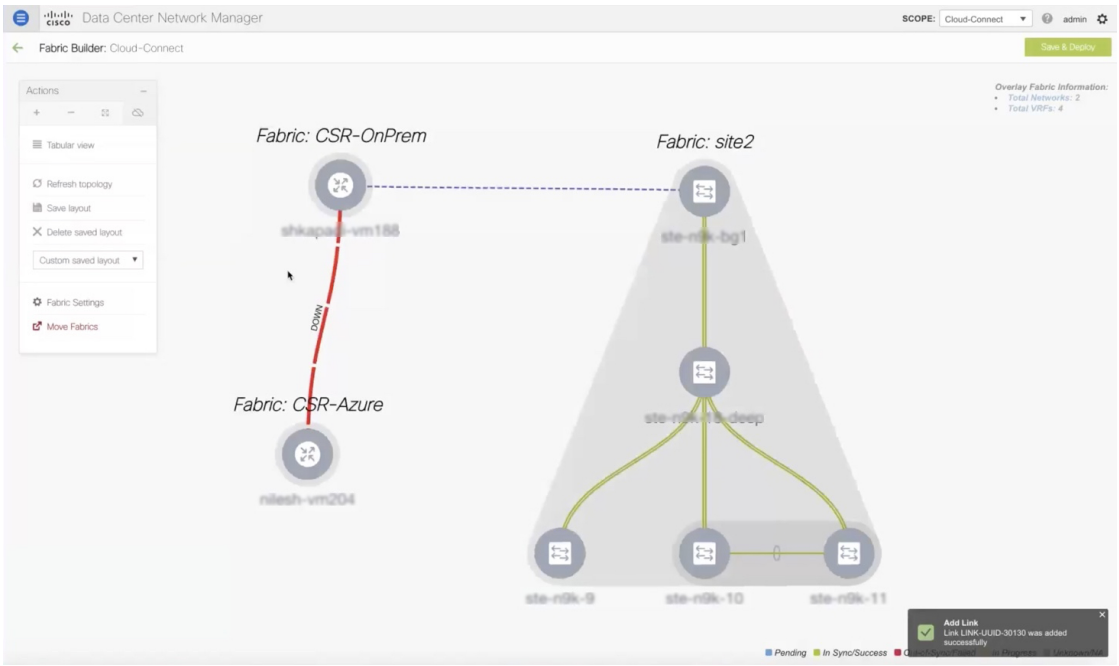
ステップ 5 (Optional) [リンク プロファイル（Link Profile）] エリアで、**[詳細（Advanced）]** タブを選択します。

このタブの下のフィールドには、デフォルト値が入力されています。必要に応じて値を変更します。これにより、2 つのコア ルータ間で eBGP ピアリングが構成されるループバックが作成されます。

ステップ 6 [保存（Save）] をクリックします。

ファブリック トポロジ ウィンドウが更新され、**[CSR-OnPrem]** ファブリックのコア ルータと **[CSR-Azure]** ファブリックのコア ルータの間にリンクが追加されます。

Note 構成内にプッシュするまで、リンク ダウンします。



What to do next

オンプレミス BGW とパブリッククラウド コア ルータを接続します。

EVPN ピアリングを使用したオンプレミス BGW とパブリッククラウド コア ルータの接続

オンプレミス コア ルータ とパブリッククラウド コア ルータの間にリンクを追加するには、次の手順を実行します。

Procedure

ステップ 1 **[Cloud-Connect]** トポロジ ウィンドウの任意の場所を右クリックします。

ファブリックで実行できるアクションがリストに表示されます。または、ファブリック トポロジ ウィンドウから、**[アクション（Actions）]** ペインの **[表形式ビュー（Tabular view）]** を選択し、**[リンク（Links）]** タブをクリックします。

ステップ 2 **[リンクの追加（Add Link）]** を選択します。

[リンク管理（Link Management）- リンクの追加（Add Link）] ダイアログボックスが表示されます。

ステップ 3 次のフィールドに値を入力します。

フィールド	説明
リンクタイプ	ドロップダウンリストから **[ファブリック間（Inter-Fabric）]** リンク タイプを選択します。
リンク サブタイプ	ドロップダウンリストから **[MULTISITE_OVERLAY]** リンク サブタイプを選択します。
リンク テンプレート	ドロップダウンリストから **[csr_ext_evpn_multisite_overlay_setup]** リンク テンプレートを選択します。
送信元ファブリック	ドロップダウンリストから送信元ファブリックとして **[site2]** を選択します。
接続先ファブリック	ドロップダウンリストから接続先ファブリックとして **[CSR-Azure]** を選択します。
送信元デバイス（Source Device）	ドロップダウンリストからオンプレミス BGW を選択します。
送信元インターフェイス（Source Interface）	オンプレミス BGW のループバック インターフェイスを選択します。
接続先デバイス	ドロップダウンリストからパブリッククラウド コア ルータを選択します。
宛先インターフェイス	ドロップダウンリストからパブリッククラウド コア ルータのインターフェイスを選択します。 **Note** インターフェイスを作成していない場合、接続先インターフェイスはドロップダウンリストに表示されないため、接続先インターフェイスを入力する必要があります。

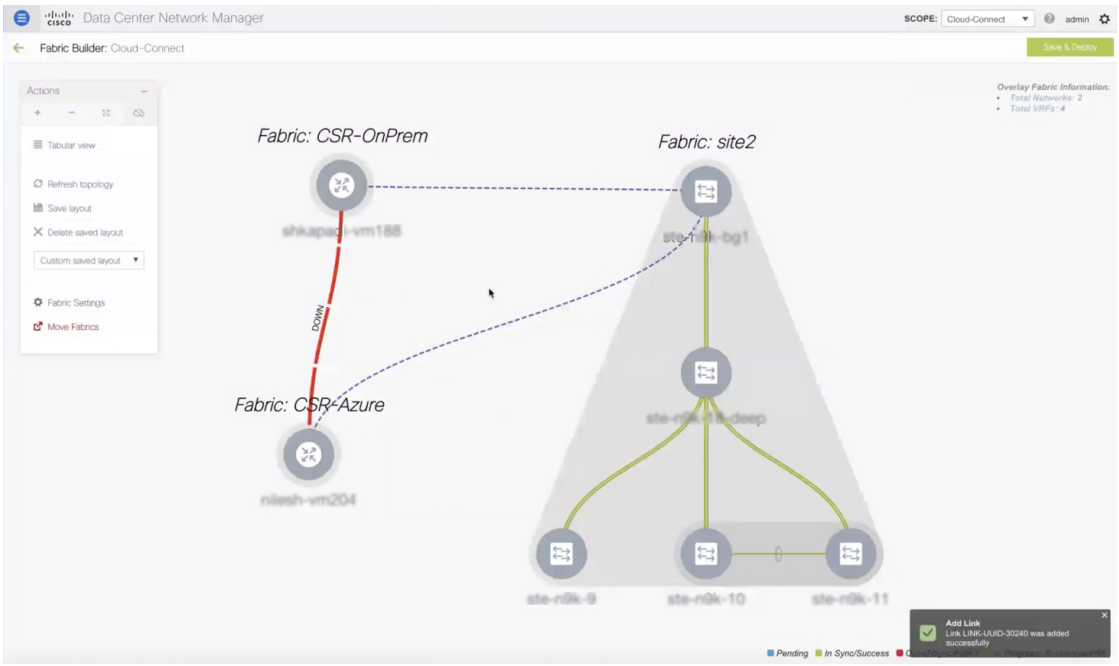
ステップ 4 **[全般（General）]** タブの **[リンク プロファイル（Link Profile）]** エリアにある次のフィールドに値を入力します。

フィールド	説明
IP_MASK	サブネットを持つ送信元インターフェイスの IPv4 アドレスを入力します。
NEIGHBOR_IP	接続先インターフェイスの IPv4 アドレスを入力します。

ステップ 5 [保存（Save）] をクリックします。

ファブリック トポロジ ウィンドウが更新され、**[site2]** ファブリックの BGW と **[CSR-Azure]** ファブリックのコア ルータの間にリンクが追加されます。

Note 構成内にプッシュするまで、リンク ダウンします。



What to do next

構成を保存して展開します。

構成の保存と展開

ファブリック トポロジ ウィンドウで構成を保存して展開するには、次の手順を実行します。

Procedure

ステップ 1 [保存して展開（Save & Deploy）] をクリックします。

[構成の展開（Config Deployment）] ダイアログ ボックスが表示され、**[構成のプレビュー（Configuration Preview）]** ステップが表示されます。BGW、オンプレミス データセンター、パブリッククラウドの間で作成されたリンクのインテントが生成されます。

ステップ 2 (Optional) **[構成のプレビュー（Preview Config）]** 列で BGW の反対側のフィールドをクリックします。

BGW の **[構成プレビュー（Config Preview）]** ダイアログ ボックスが表示されます。

ステップ 3 (Optional) **[保留中の構成（Pending Config）]** 列で構成の詳細を表示します。

アンダーレイ ピアリングとオーバーレイ ピアリングに関する詳細が含まれています。

ステップ 4 (Optional) **[構成のプレビュー（Preview Config）]** 列でオンプレミス コア ルータの反対側のフィールドをクリックします。

オンプレミス コア ルータの **[構成プレビュー（Config Preview）]** ダイアログ ボックスが表示されます。

ステップ 5 (Optional) **[保留中の構成（Pending Config）]** 列で構成の詳細を表示します。

これには、インターフェイス、IPsec トンネル、共有キー、コア ルータ間の BGP ピアリング、および EVPN ピアリングに関する詳細が含まれます。すべての BGP トラフィックとデータ トラフィックがトンネルを通過する必要があることを示すルートマップが追加されます。

ステップ 6 (Optional) **[構成のプレビュー（Preview Config）]** 列でパブリッククラウド コア ルータの反対側のフィールドをクリックします。

オンプレミス コア ルータの **[構成プレビュー（Config Preview）]** ダイアログ ボックスが表示されます。

ステップ 7 (Optional) **[保留中の構成（Pending Config）]** 列で構成の詳細を表示します。

これには、オンプレミス コア ルータについて説明されている詳細に加えて、VTEP に関する詳細が含まれています。

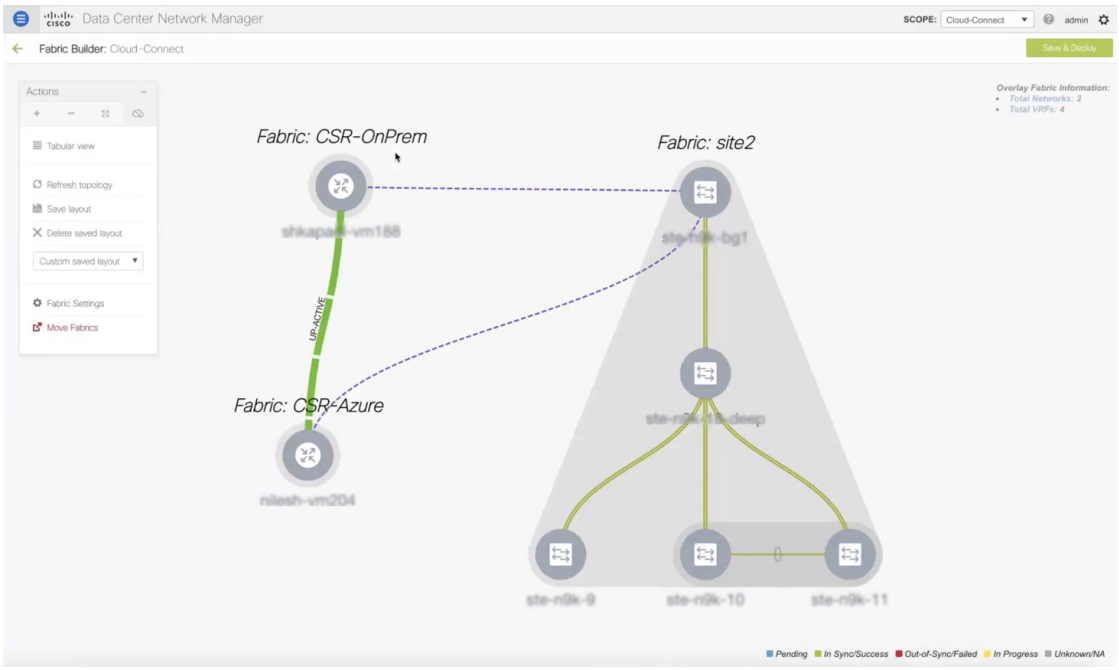
ステップ 8 **[構成の展開（Deploy Config）]** をクリックします。

[構成の展開ステータス（Configuration Deployment Status）] ステップが表示され、構成の展開ステータスを確認できます。

ステップ 9 正常に展開された後、**[閉じる（Close）]** をクリックします。

ファブリック トポロジ ウィンドウが表示されます。IPsec トンネルが起動し、アクティブになります。

Note 展開には時間がかかる場合があります。



What to do next

VRF を拡張して展開します。

VRF の拡張

VRFは、データセンターとパブリッククラウドの間でワークロードを共有できるように拡張されています。

VRF オンプレミス コア ルータの展開と拡張

MSD ファブリックのファブリック トポロジ ウィンドウから VRF を拡張してオンプレミス コア ルータに展開するには、次の手順を実行します。

Procedure

ステップ 1 **[保存と展開（Save & Deploy）]** アイコンの下にある **[オーバーレイ ファブリック情報（Overlay Fabric Information）]** エリアの **[トータル VRF（Total VRF）]** リンクをクリックします。

ファブリックの VRF ウィンドウの **[ネットワーク / VRF 選択（Network / VRF Selection）]** エリアが表示されます。

ステップ 2 オンプレミス コア ルータの VRF を選択し、**[続行（Continue）]** をクリックします。

VRF ウィンドウの **[ネットワーク / VRF 展開（Network / VRF Deployment）]** エリアが表示されます。ファブリックのネットワーク トポロジが表示されます。未検出のクラウドを隠すことができます。

ステップ 3 BGW をダブルクリックします。

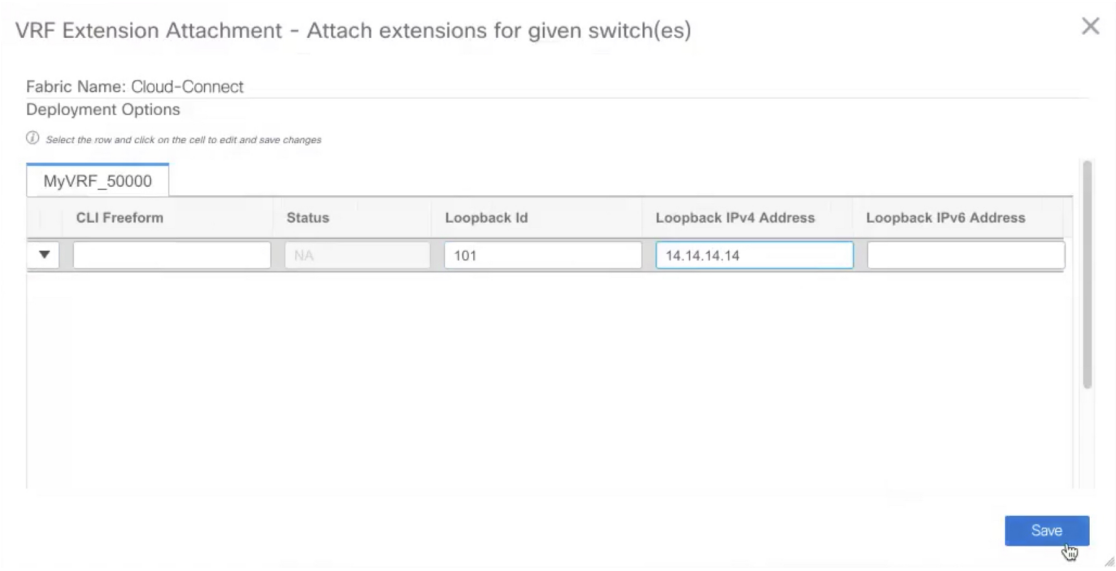
[VRF 拡張アタッチメント（VRF Extension Attachment）] ダイアログボックスが表示されます。

ステップ 4 BGW を選択し、**[拡張（Extend）]** 列の下にある編集アイコンをクリックして、マルチサイトを有効にします。

[拡張（Extend）] 列の下にドロップダウンリストが表示されます。

ステップ 5 ドロップダウンリストから **[MULTISITE]** を選択します。

ステップ 6 ループバック ID とループバック IPv4 アドレスをそれぞれの列に入力して、BGW のホストをシミュレートします。



ステップ 7 [保存（Save）] をクリックします。

ファブリックのネットワーク トポロジが表示され、BGW が青色に変わり、展開が保留中であることを示します。

ステップ 8 [プレビュー（Preview）] オプションをクリックします。

[構成のプレビュー（Preview Configuration）] ダイアログボックスが表示されます。EVPN 構成がプッシュされ、ループバック インターフェイスが作成されます。

ステップ 9 **[展開（Deploy）]** をクリックします。

What to do next

VRF を作成し、パブリッククラウドに展開します。

パブリッククラウドでの VRF の作成と展開

VRF を拡張して、ファブリック トポロジ ウィンドウからパブリッククラウド コア ルータに展開するには、次の手順を実行します。

Before you begin

VM が稼働していることを確認します。VM は、パブリッククラウド コア ルータに接続する必要があります。

Procedure

ステップ 1 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウから **[CSR-Azure]** 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 パブリッククラウド コア ルータを右クリックします。

ルータで実行できるアクションのリストが表示されます。

ステップ 3 リストから **[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）] ダイアログボックスが表示されます。

ステップ 4 **[ポリシーの追加（Add Policy）]** アイコンをクリックします。

[ポリシーの追加（Add Policy）] ダイアログボックスが表示されます。

ステップ 5 **[ポリシー（Policy）]** ドロップダウンリストから **[csr_vrf_evpn]** ポリシーを選択します。

ステップ 6 **[全般（General）]** タブの必須フィールドに値を入力します。

ステップ 7 [保存（Save）] をクリックします。

[ポリシーの表示/編集（View/Edit Policies）] ダイアログボックスが表示されます。

ステップ 8 **[すべて表示（View All）]** をクリックして、作成されたネットワークとインターフェイスを表示します。

[生成された構成（Generated Config）] ダイアログ ボックスが表示されます。VRF、ブリッジ ドメイン、およびマッピングされた VNI に関する詳細も、このダイアログ ボックスで表示できます。

What to do next

パブリッククラウド内の VM のパブリッククラウド コア ルータでデフォルトゲートウェイを構成します。

VM のデフォルトゲートウェイの構成

ファブリック トポロジ ウィンドウからパブリッククラウド コア ルータのデフォルトゲートウェイを構成するには、次の手順を実行します。

Procedure

ステップ 1 [ファブリック ビルダ（Fabric Builder）] ウィンドウから **[CSR-Azure]** 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 パブリッククラウド コア ルータを右クリックします。

ルータで実行できるアクションのリストが表示されます。

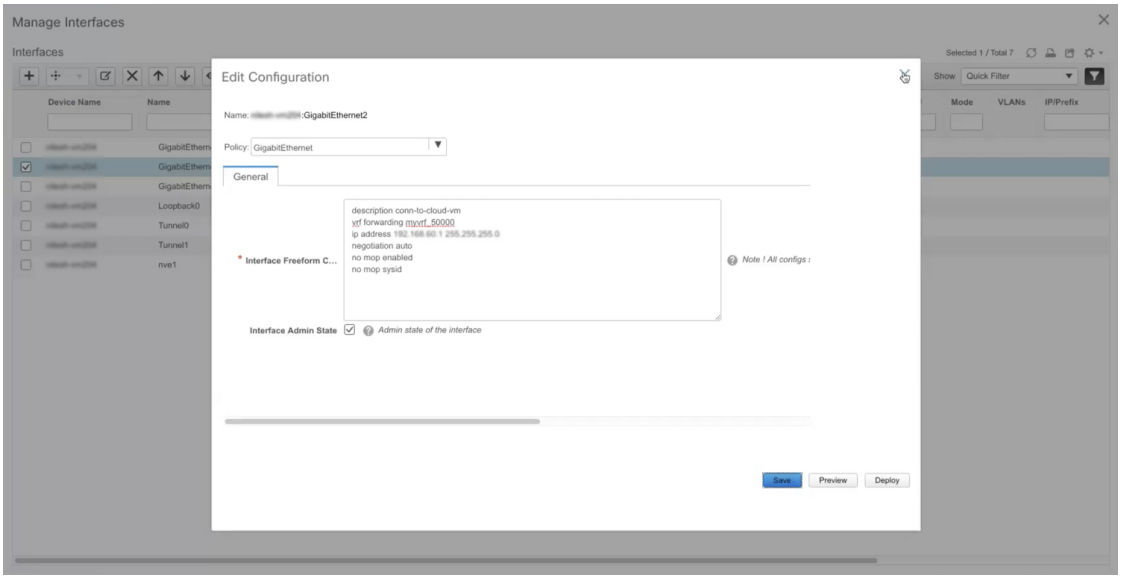
ステップ 3 リストから **[インターフェイスの管理（Manage Interface）]** を選択します。

[インターフェイスの管理（Manage Interface）] ダイアログボックスが表示されます。

ステップ 4 **[構成の編集（Edit Configuration）]** をクリックして、ポリシーを作成するインターフェイスを編集します。

[構成の編集（Edit Configuration）] ダイアログボックスが表示されます。

ステップ 5 自由形式構成を編集し、**[保存（Save）]** をクリックして、**[インターフェイスの管理（Manage Interfaces）]** ダイアログ ボックスを閉じます。



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 6 パブリッククラウド コア ルータを右クリックし、リストから **[構成の展開（Deploy Config）]** を選択します。

[構成展開（Config Deployment）] ダイアログ ボックスが表示されます。

ステップ 7 **[構成のプレビュー（Preview Config）]** 列の下の値をクリックして、構成のプレビューを確認します。

ステップ 8 構成を展開するには、**[展開の展開（Deploy Config）]** をクリックします。

構成がプッシュされて展開されます。

ステップ 9 [閉じる（Close）] をクリックします。

ステップ 10 CLI にログオンして、トラフィック フローを表示します。

トラフィックはコア ルータ間を流れ、VRF を経由します。

接続の確認

Cisco DCNM Web UI からオンプレミス データセンターとパブリッククラウド間の接続を確認するには、次の手順を実行します。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック（Fabrics）] > [VRF]** を選択します。

[VRF] ウィンドウが表示されます。

ステップ 2 **[Cloud-Connect]** ファブリックを選択します。

このファブリックの VRF が一覧表示されます。

ステップ 3 VRF を選択して **[続行（Continue）]** をクリックします。

ステップ 4 BGW を右クリックします。

[VRF 拡張アタッチメント（VRF Extension Attachment）] ダイアログボックスが表示されます。

ステップ 5 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。

[ネットワークトポロジ（network topology）] ウィンドウが表示されます。

ステップ 6 **[展開（Deploy）]** をクリックして、構成をプッシュします。

BGW で VRF が無効になっています。

ステップ 7 CLI を確認します。

トラフィックが停止します。

ステップ 8 BGW で VRF を再度有効にします。

ステップ 9 CLI を確認します。

トラフィックが流れます。または、パブリッククラウドの Web サーバーの HTTP アドレスにアクセスします。**[データベースの到達可能性（Database Reachable）** メッセージが表示されます。

Microsoft Azure での Cisco CSR 1000v の展開

Microsoft Azure に Cisco CSR 1000v を展開するには、次の手順を実行します。

Procedure

ステップ 1 **[Microsoft Azure]** UI から、**[仮想マシン（Virtual Machines）]** を選択します。

[仮想マシン] ウィンドウが表示されます。

ステップ 2 [追加（Add）] をクリックします。

[仮想マシンの作成（Create a virtual machine）] ウィンドウが表示されます。

ステップ 3 **[Azure マーケットプレイスから VM を作成（Create VM from Azure Marketplace）]** ハイパーリンクをクリックします。

標準のクラシック VM を検索できる **[マーケットプレイス（Marketplace）]** ウィンドウが表示されます。

ステップ 4 マーケットプレイスで CSR 展開を検索します。

ステップ 5 検索結果から **[シスコ クラウド サービス ルータ（CSR）1000V（Cisco Cloud Services Router（CSR）1000V）]** を選択します。

ステップ 6 **[ソフトウェア プランの選択（Select a software plan）]** ドロップダウンリストから **[Cisco CSR 1000V 個人所有ライセンス可 - XE 16.9（Cisco CSR 1000V Bring Your Own License – XE 16.9）]** 以降のバージョンを選択します。

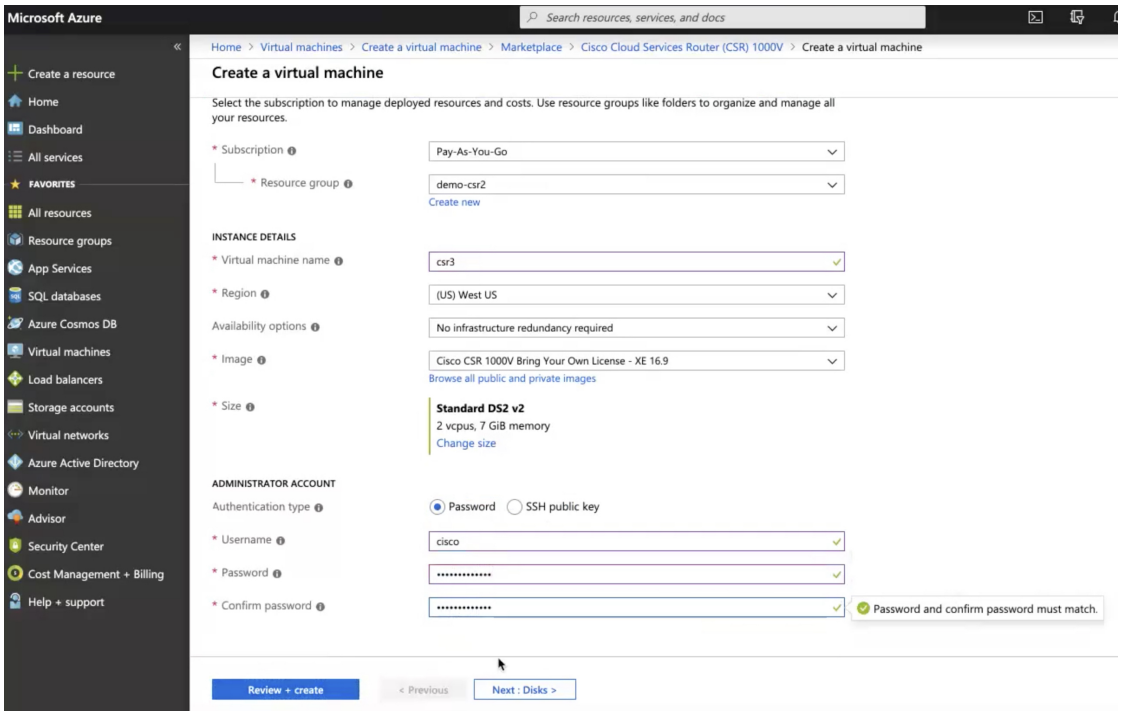
ステップ 7 [作成（Create）] をクリックします。

ステップ 8 **[仮想マシンの作成（Create a virtual machine）]** ウィンドウで、プロジェクトの詳細とインスタンスの詳細を入力します。

ステップ 9 管理者アカウントのセクションでは **[パスワード（Password）]** 認証タイプを選択します。

Cisco DCNM は、SSH 公開キーをサポートしていません。

ステップ 10 ユーザー名とパスワードを作成します。



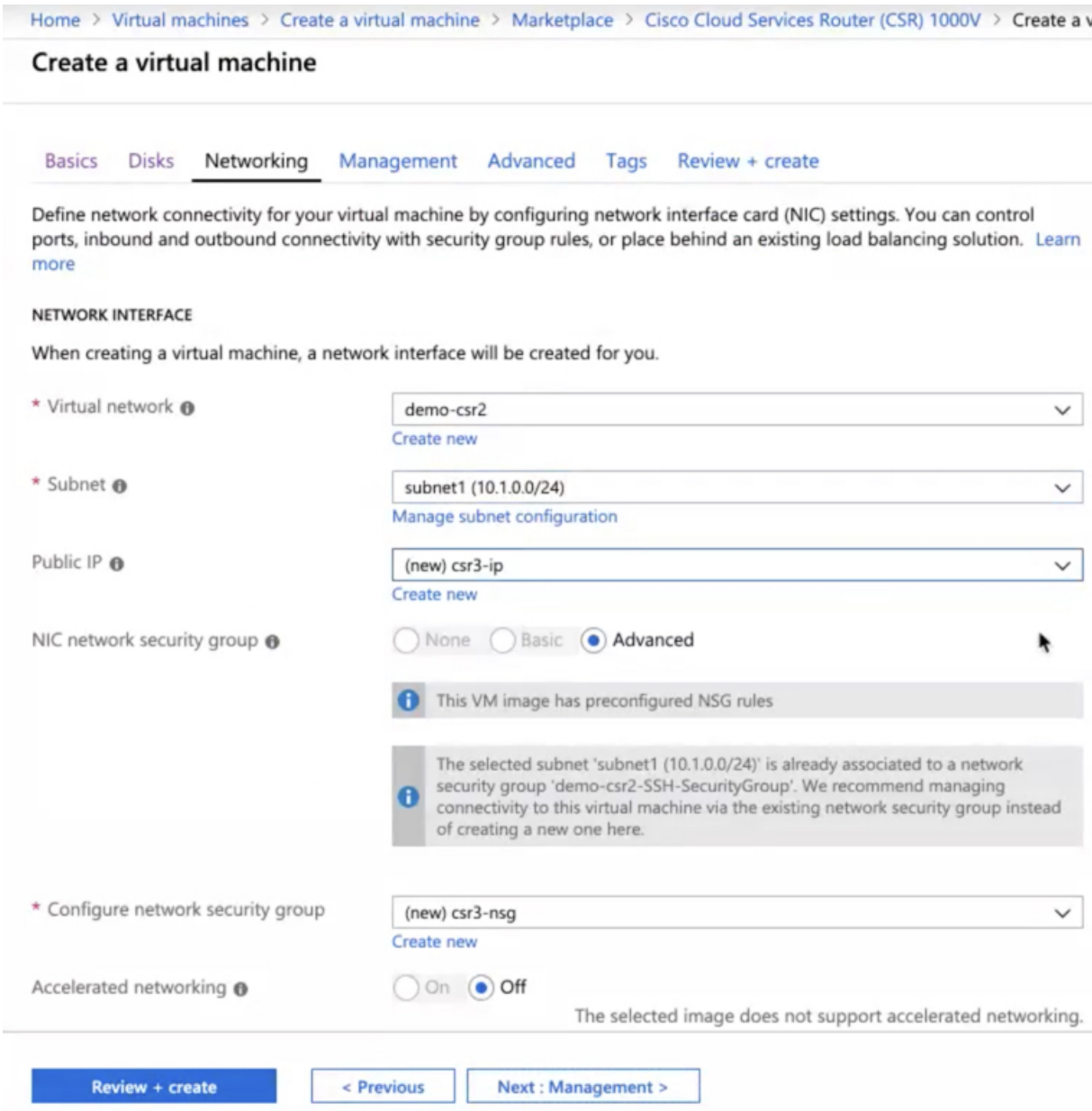
ステップ 11 **[次へ：ディスク >（Next : Disks >）]** をクリックします。

ステップ 12 OS ディスク タイプのドロップダウンリストから、**[標準 HDD（Standard HDD）]** を選択します。

ステップ 13 **[次へ：ネットワーキング >（Next : Networking >）]** をクリックします。

ステップ 14 必要なフィールドに値を入力します。

ステップ 15 ネットワークのパブリック IP を選択します。



ステップ 16 他のフィールドではデフォルト値を使用します。

ステップ 17 **[確認して作成（Review + create）]** をクリックします。

パブリック IP アドレスを使用して、Microsoft Azure に Cisco CSR 1000v 用の VM が作成されます。

What to do next

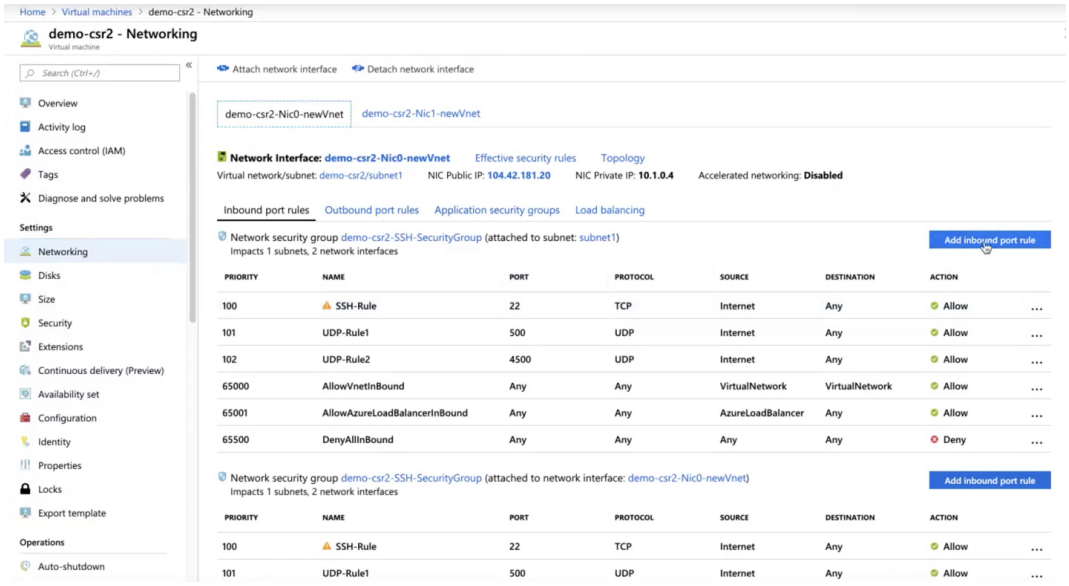
- ネットワーク インターフェイスの接続

1. VM の **[ネットワーキング（Networking）]** 設定を選択します。
2. **[ネットワーク インターフェイスの接続（Attach network interface）]** を選択して、NIC を追加します。

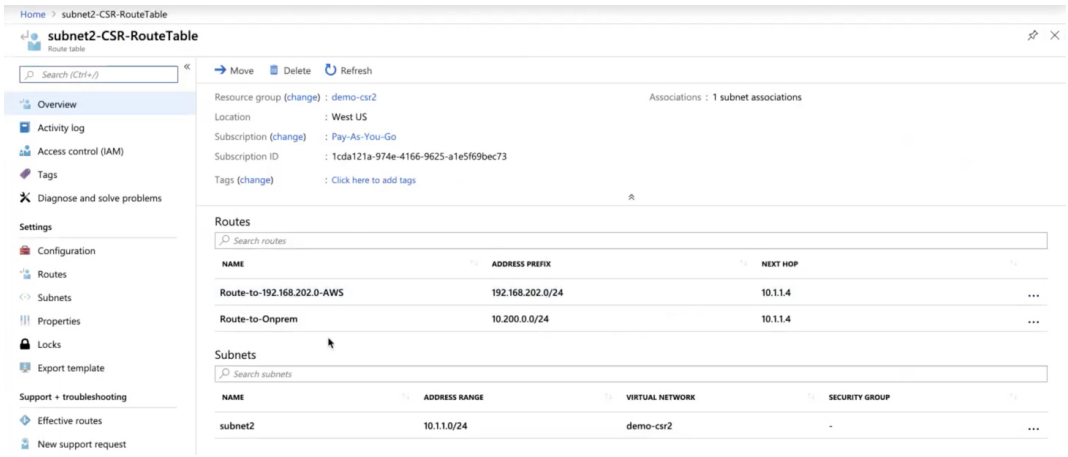
   両方のサブネットにそれぞれ 1 つの NIC を接続します。IP アドレスが自動的に割り当てられます。
3. ポート 22 を使用して SSH ルールを追加して、コア ルータの SSH アクセスを有効にします。

   Cisco DCNM は、この SSH アクセスを使用してコア ルータを検出します。

Note IPsec トンネルを有効にするためにポート 500 と 4500 を使用する 2 つの UDP ルールが自動的に追加されます。



- VM の **[ルート（Routes）]** 設定でルートを作成して、オンプレミス データ センターと Microsoft Azure 間のトラフィック ルートを作成します。デフォルトルートを使用して、トラフィックを VNet から Cisco CSR 1000v にリダイレクトできます。



詳細については、「*Microsoft Azure* 向け *Cisco CSR 1000v* 導入ガイド」を参照してください。

リンクおよびコア ルータの詳細の表示

ファブリック トポロジ ウィンドウからリンクとコア ルータの詳細を表示するには、次の手順を実行します。

Procedure

ステップ 1 **[アクション（Actions）]** ペインで、**[表形式ビュー（Tabular view）] > [リンク（Links）]** を選択します。

[リンク（Links）] ウィンドウが表示されます。

ステップ 2 ウィンドウを更新します。

作成した 3 つのリンクがリストに表示されます。

ステップ 3 (Optional) オンプレミスのコア ルータをダブルクリックして、IP ルート情報を表示します。

[IP ルート情報（IP Route Information）] ダイアログボックスが表示されます。

ステップ 4 (Optional) **[暗号セッション（Crypto Session）]** タブをクリックして、IPsec トンネルの詳細を表示します。

ステップ 5 (Optional) **[BGP セッション（BGP Session）]** タブをクリックして、BGP セッションに関する詳細を表示します。

ステップ 6 (Optional) **[パケット カウンタ（Packet Counter）]** タブをクリックして、パケット カウンタの詳細を表示します。

[パケット カウンタ（Packet Counter）] タブに表示されるカウンタ値をリセットできます。詳細については、API を使用したパケット カウンタのリセット, on page 1124を参照してください。

API を使用したパケット カウンタのリセット

ピーク カウンタをリセットするには、次の手順を実行します。

Procedure

ステップ 1 Cisco DCNM にログインします。

ステップ 2 https:// *DCNM-IP* /api-docs URL に移動します。

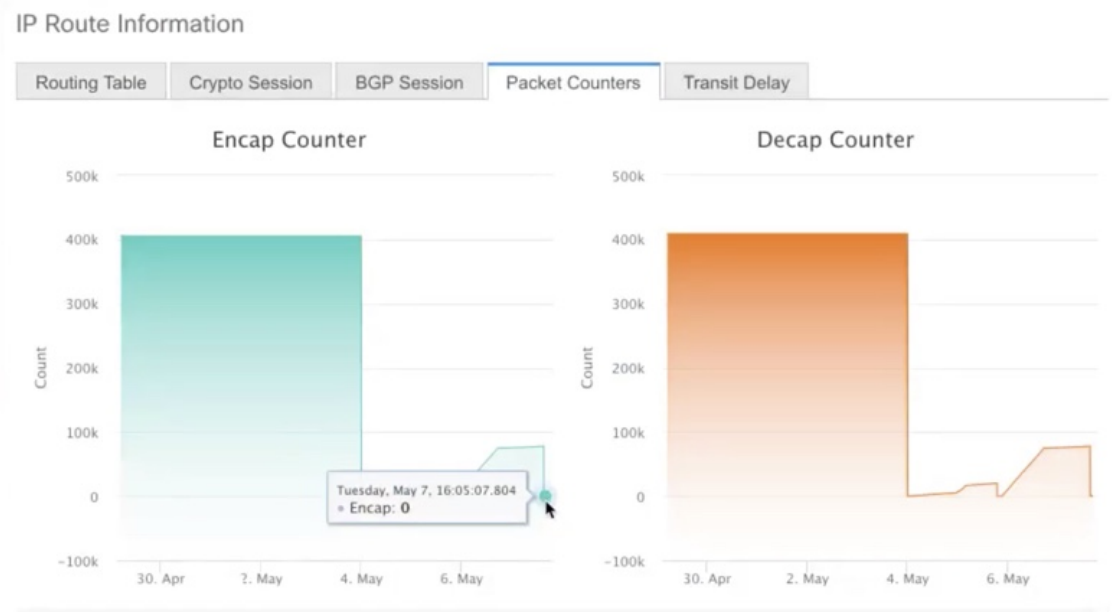
ステップ 3 クラウド拡張の下にある GET **/cloud-extension/status/{ipAddress}** API を展開します。

ステップ 4 on-prem コア ルータの IP アドレスを入力します。

ステップ 5 **[fetchLatestFromSwitch]** 値を **[true]** に設定します。

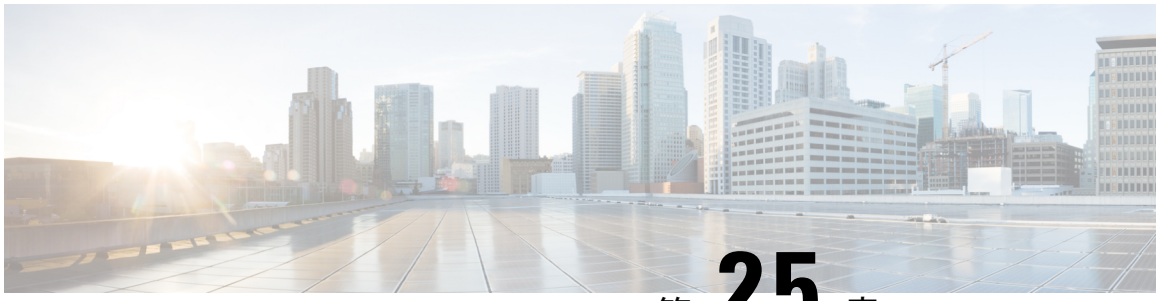
ステップ 6 [試行する（Try it out）] をクリックします。

パケット カウンタがクリアされ、カウントがゼロになります。



第 VII 部

MSDC 展開の Easy プロビジョニング



第 25 章

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。Single-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ローカルに配置され、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。

eBGP ベースのファブリックの作成

1. **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。

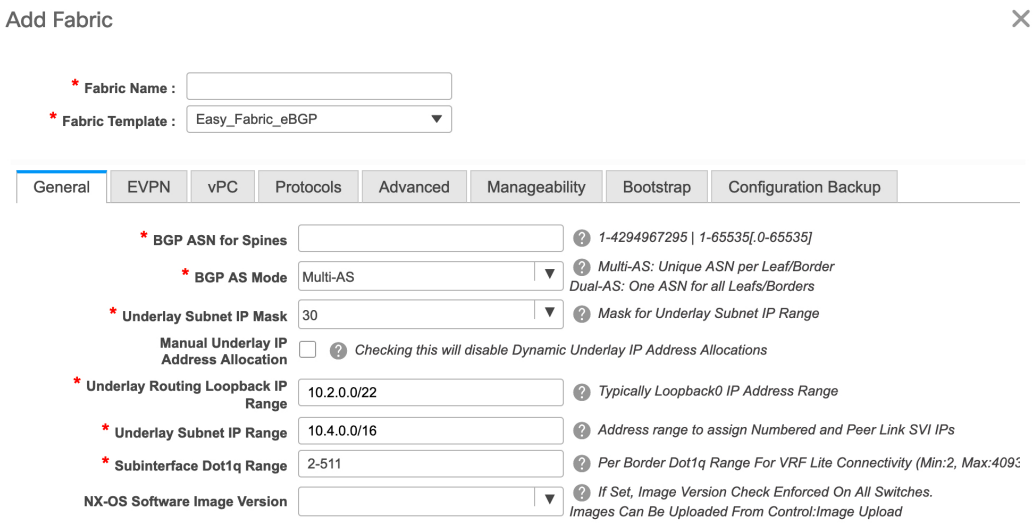
   [ファブリック ビルダ（Fabric Builder）] 画面が表示されます。初めてログインしたときには、**[ファブリック（Fabrics）]** セクションにはまだエントリはありません。ファブリックを作成すると、**[ファブリック ビルダ（Fabric Builder）]** 画面に表示されます。長方形のボックスが各ファブリックを表します。

2. [ファブリックの作成（Create Fabric）] をクリックします。**[ファブリックの追加（Add Fabric）]** 画面が表示されます。

   フィールドについて説明します。

   [ファブリック名（Fabric Name）]：ファブリックの名前を入力します。

[ファブリック テンプレート（Fabric Template）]：ドロップダウンメニューから、**[Easy_Fabric_eBGP]** ファブリック テンプレートを選択します。スタンドアロン ルーテッド ファブリックを作成するためのファブリック設定が表示されます。



3. デフォルトでは **[全般（General）]** タブが表示されます。このタブのフィールドは次のとおりです。

   [スパインの BGP ASN（BGP ASN for Spines）]：ファブリックのスパイン スイッチの BGP AS 番号を入力します。

   [BGP AS モード（BGP AS Mode）]：**[Multi-AS]** または **[Dual-AS]** を選択します。

   Multi-AS ファブリックでは、スパイン スイッチには一意の BGP AS 番号があり、各リーフ スイッチには一意の AS 番号があります。2 つのリーフ スイッチが vPC スイッチ ペアを形成している場合、それらは同じ AS 番号を持ちます。

   [Dual-AS] ファブリックでは、スパイン スイッチには一意の BGP AS 番号があり、リーフスイッチには一意の AS 番号があります。

   ファブリックは、スパイン スイッチの AS 番号によって識別されます。

   [アンダーレイ サブネット IP マスク（Underlay Subnet IP Mask）]：ファブリック インターフェイスの IP アドレスのサブネットマスクを指定します。

   [手動アンダーレイ IP アドレス割り当て（Manual Underlay IP Address Allocation）]：[動的アンダーレイ IP アドレス割り当て（Dynamic Underlay IP Address Allocation）] を無効にするには、このチェックボックスをオンにします。

   [アンダーレイ ルーティング ループバック IP 範囲（Underlay Routing Loopback IP Range）]：プロトコル ピアリングのループバック IP アドレスを指定します。

   [アンダーレイ サブネット IP 範囲（Underlay Subnet IP Range）]：インターフェイス間のアンダーレイ P2P ルーティング トラフィックの IP アドレスです。

   [サブインターフェイス Dot1q 範囲（Subinterface Dot1q Range）]：L3 サブインターフェイスを使用する場合のサブインターフェイスの範囲を指定します。

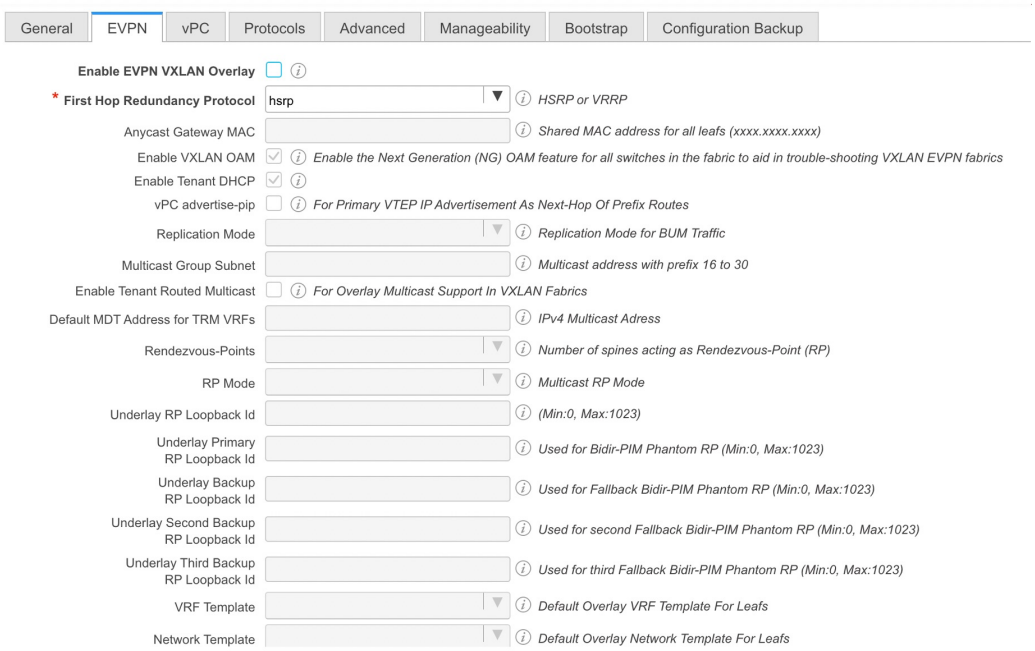
[NX-OSソフトウェア イメージ バージョン（NX-OS Software Image Version）]：ドロップダウンリストからイメージを選択します。

イメージアップロードオプションを使用してCisco NX-OS ソフトウェアイメージをアップロードすると、アップロードされたイメージがこのフィールドにリストされます。イメージを選択する場合、スイッチのバージョンが選択されているかどうか、システムがチェックします。選択されていない場合、エラー メッセージが表示されます。[解決（Resolve）] をクリックすることで、エラーを解決できます。イメージ管理画面が表示され、ISSU オプションを処理できます。その代わりに、リリース ナンバーを削除した後で保存することも可能です。

このフィールドでイメージを指定する場合、ファブリックのすべてのスイッチはそのイメージを実行する必要があります。一部のデバイスでイメージが実行されない場合、指定されたイメージへのインサービス ソフトウェア アップグレード（ISSU）を実行するように警告するプロンプトが表示されます。すべてのデバイスが指定されたイメージを実行するまで、展開プロセスは完了しません。

ファブリック スイッチに複数のタイプのソフトウェア イメージを展開する場合は、イメージを指定しないでください。イメージが指定されている場合は削除します。

4. **[EVPN]** をクリックします。[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点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。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 1157を参照してください。

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。

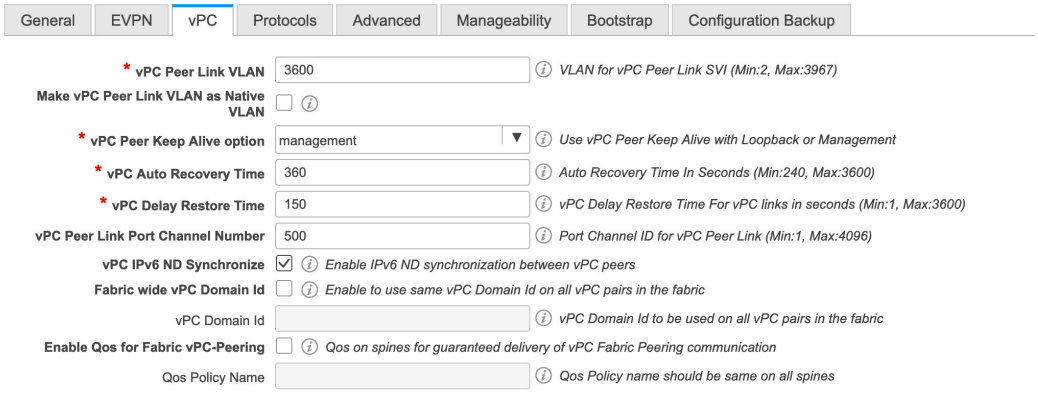
Routed_Network_Universal テンプレートは、ルーテッド ファブリックにのみ適用されることに注意してください。

[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。

5. **[vPC]** をクリックします。このタブのフィールドは次のとおりです。



[vPC ピア リンク VLAN（vPC Peer Link VLAN）]：vPC ピア リンク SVI に使用される VLAN です。

[vPC ピア リンク VLAN をネイティブ VLAN とする（Make vPC Peer Link VLAN as Native VLAN）]：vPC ピア リンク VLAN をネイティブ VLAN として有効にします。

[vPC ピア キープアライブ オプション（vPC Peer Keep Alive option）]：管理またはループバック オプションを選択します。管理ポートおよび管理 VRF に割り当てられた IP アドレスを使用する場合は、[管理（management）]を選択します。ループバック インターフェイス（および非管理 VRF）に割り当てられた IP アドレスを使用する場合は、ルー

プバックを選択します。IPv6 アドレスを使用する場合は、ループバック ID を使用する必要があります。

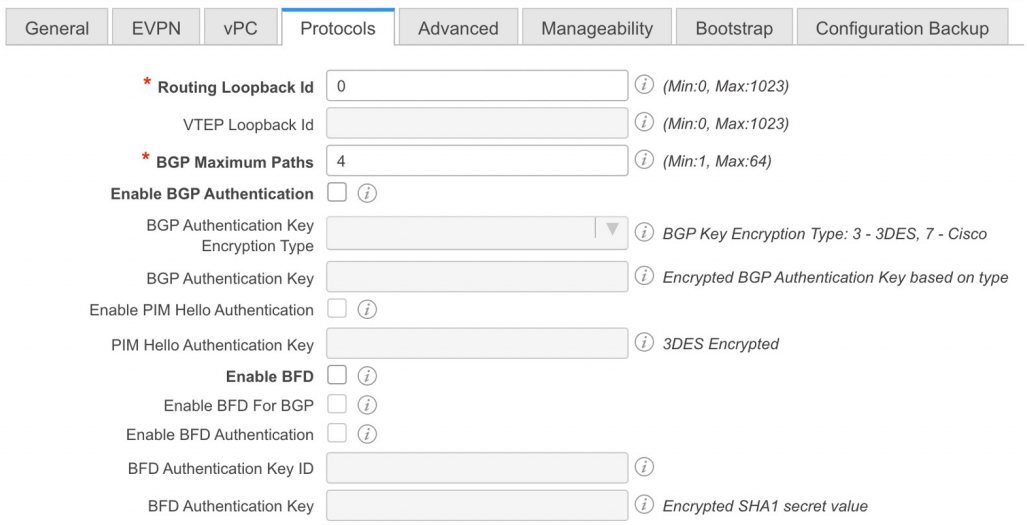
[vPC 自動回復時間（vPC Auto Recovery Time）]：vPC 自動回復タイムアウト時間を秒単位で指定します。

[vPC 遅延復元時間（vPC Delay Restore Time）]：vPC 遅延復元時間を秒単位で指定します。

[vPC ピア リンク ポートチャネル番号（vPC Peer Link Port Channel Number）]：vPC ピア リンクのポートチャネル ID を指定します。デフォルトでは、このフィールドの値は 500 です。

[vPC IPv6 ND 同期（vPC IPv6 ND Synchronize）]：vPC スイッチ間の IPv6 ネイバー探索同期を有効にします。デフォルトでチェックボックスはオンになっています。機能を無効にするにはチェックボックスをクリアします。

6. **[プロトコル（Protocols）]** タブをクリックします。このタブのフィールドは次のとおりです。



[ルーティング ループバック ID（Routing Loopback Id）]：ループバック インターフェイス ID は、デフォルトで 0 として設定されます。BGP ルータ ID として使用されます。

[BGP 最大パス（BGP Maximum Paths）]：BGP 最大パスを指定します。

[BGP 認証の有効化（Enable BGP Authentication）]：BGP 認証を有効にするにはチェックボックスをオンにします。無効にするにはチェックボックスをオフにします。このフィールドを有効にすると、[BGP 認証キー暗号化タイプ（BGP Authentication Key Encryption Type）] および [BGP 認証キー（BGP Authentication Key）] フィールドが有効になります。

[BGP 認証キー暗号化タイプ（BGP Authentication Key Encryption Type）]：3DES 暗号化タイプの場合は 3、Cisco 暗号化タイプの場合は 7 を選択します。

[BGP 認証キー（BGP Authentication Key）]：暗号化タイプに基づいて暗号化キーを入力します。

Note プレーン テキスト パスワードはサポートされていません。スイッチにログインし、暗号化されたキーを取得して、[BGP 認証キー（BGP Authentication Key）] フィールドに入力します。詳細については、「認証キーの取得」の項を参照してください。

[BFD の有効化（Enable BFD）]：ファブリック内のすべてのスイッチで機能 [bfd] を有効にするには、このチェックボックスをオンにします。この機能は、IPv4 アンダーレイでのみ有効で、範囲はファブリック内にあります。

Cisco DCNM リリース 11.3(1) 以降、ファブリック内の BFD はネイティブにサポートされます。ファブリック設定では、BFD機能はデフォルトで無効になっています。有効にすると、デフォルト設定のアンダーレイ プロトコルに対して BFD が有効になります。カスタムの必須BFD構成は、スイッチごとの自由形式またはインターフェイスごとの自由形式ポリシーを使用して展開する必要があります。

[BFD の有効化（Enable BFD）] チェックボックスをオンにすると、次の構成がプッシュされます。

```
feature bfd
```

Note BFD が有効になっている DCNM リリース 11.2(1) から DCNM リリース 11.3(1) にアップグレードすると、次の構成がすべての P2P ファブリック インターフェイスにプッシュされます。

```
no ip redirects
no ipv6 redirects
```

BFD機能の互換性については、それぞれのプラットフォームのマニュアルを参照してください。サポートされているソフトウェア画像については、「*Cisco DCNM* の互換性マトリクス」を参照してください。

[BGP 向け BFD の有効化（Enable BFD for BGP）]：BGP ネイバーの BFD を有効にするには、このチェックボックスをオンにします。このオプションは、デフォルトで無効です。

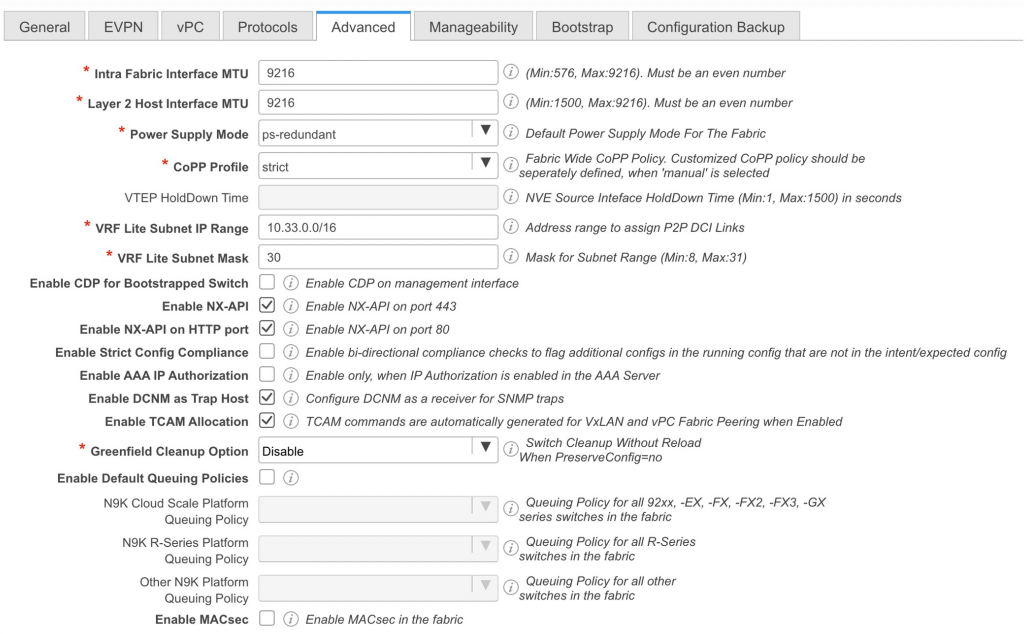
[BGP 認証の有効化（Enable BGP Authentication）]：BGP 認証を有効にするにはチェックボックスをオンにします。このフィールドを有効にすると、[BFD 認証キー ID（BFD Authentication Key ID）] フィールドと [BFD 認証キー（BFD Authentication Key）] フィールドが編集可能になります。

[BFD 認証キー ID（BFD Authentication Key ID）]：インターフェイス認証の BFD 認証キー ID を指定します。

[BFD 認証キー（BFD Authentication Key）]：BFD 認証キーを指定します。

BFD 認証パラメータを取得する方法については、『*Cisco DCNM LAN* ファブリック構成ガイド』の「暗号化された *BFD* 認証キーの取得」を参照してください。

7. [Advanced] タブをクリックします。このタブのフィールドは次のとおりです。



[イントラ ファブリック インターフェイス MTU（Intra Fabric Interface MTU）]：ファブリック内インターフェイスの MTU を指定します。この値は偶数にする必要があります。

[レイヤ 2 ホスト インターフェイス MTU（Layer 2 Host Interface MTU）]：レイヤ 2 ホスト インターフェイスの MTU を指定します。この値は偶数にする必要があります。

電源モード（Power Supply Mode）：適切な電源モードを選択します。

[CoPP プロファイル（CoPP Profile）]：ファブリックの適切なコントロール プレーン ポリシング（CoPP）プロファイル ポリシーを選択します。デフォルトでは、strict オプションが入力されます。

[VRF Lite サブネット IP 範囲（VRF Lite Subnet IP Range）] および [VRF Lite サブネット マスク（VRF Lite Subnet Mask）]：これらのフィールドには、DCI サブネットの詳細が入力されます。必要に応じて、次のフィールドを更新します。

[ブートストラップ スイッチの CDP を有効にする（Enable CDP for Bootstrapped Switch）]：チェックボックスをオンにして、ブートストラップ スイッチの CDP を有効にします。

[NX-API の有効化（Enable NX-API）]：HTTPS での NX-API の有効化を指定します。このチェックボックスは、デフォルトでオンになっています。

[HTTP での NX-API の有効化（Enable NX-API on HTTP）]：HTTP での NX-API の有効化を指定します。HTTP を使用するには、[NX-API の有効化（Enable NX-API）] チェッ

クボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。このチェックボックスをオフにすると、エンドポイント ロケータ（EPL）、レイヤ 4～レイヤ 7 サービス（L4ーL7 サービス）、VXLAN OAM など、NX-API を使用し、Cisco DCNM がサポートするアプリケーションは、HTTP ではなく HTTPS の使用を開始します。

Note [NX-API の有効化（Enable NX-API）] チェックボックスと [HTTP での NX-API の有効化（Enable NX-API on HTTP）] チェックボックスをオンにすると、アプリケーションは HTTP を使用します。

[厳密な構成コンプライアンスの有効化（Enable Strict Config Compliance）]：このチェックボックスをオンにして、厳密な構成コンプライアンス機能を有効にします。

厳密な構成コンプライアンスについては、*Enhanced Monitoring and Monitoring Fabrics Guide*を参照してください。

Note ファブリックで厳密な構成コンプライアンスが有効になっている場合、Cisco DCN M のリソースで Network Insights を展開することはできません。

[AAA IP 認証の有効化（Enable AAA IP Authorization）]：AAA サーバで IP 認証が有効になっている場合に、AAA IP 認証を有効にします。

[トラップホストとして有効にする（Enable as Trap Host）]：トラップホストとして有効にする場合は、このチェックボックスをオンにします。

[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）]：このファブリック内のすべてのスイッチに QoS ポリシーを適用するには、このチェックボックスをオンにします。すべてのスイッチに適用した QoS ポリシーを削除するには、このチェックボックスをオフにし、すべての設定を更新してポリシーへの参照を削除し、保存して展開します。Cisco DCNM リリース 11.3(1) 以降、さまざまな Cisco Nexus 9000 シリーズ スイッチに使用できる定義済みの QoS 設定が含まれています。このチェックボックスをオンにすると、適切な QoS 設定がファブリック内のスイッチにプッシュされます。システム キューイングは、設定がスイッチに展開されると更新されます。インターフェイスごと自由形式ブロックに必要な設定を追加することにより、必要に応じて、定義されたキューイング ポリシーを使用してインターフェイス マーキングを実行できます。

テンプレート エディタでポリシー ファイルを開いて、実際のキューイング ポリシーを確認します。Cisco DCNM Web UI から、**[制御（Control）] > [テンプレート ライブラリ（Template Library）]** を選択します。ポリシー ファイル名でキューイング ポリシーを検索します（例：[queuing_policy_default_8q_cloudscale]）。ファイルを選択し、**[テンプレートの変更/表示（Modify/View template）]** アイコンをクリックしてポリシーを編集します。

プラットフォーム特有の詳細については、『*Cisco Nexus 9000 Series NX-OS Quality of Service* コンフィグレーション ガイド』を参照してください。

[N9K クラウド スケール プラットフォームのキューイング ポリシー（N9K Cloud Scale Platform Queuing Policy）]：ファブリック内の EX、FX、および FX2 で終わるすべての Cisco Nexus 9200 シリーズスイッチおよび Cisco Nexus 9000 シリーズスイッチに適用するキューイング ポリシーをドロップダウン リストから選択します。有効な値は [queuing_policy_default_4q_cloudscale] および [queuing_policy_default_8q_cloudscale] です。FEX には [queuing_policy_default_4q_cloudscale] ポリシーを使用します。FEX がオフラインの場合にのみ、[queuing_policy_default_4q_cloudscale] ポリシーから [queuing_policy_default_8q_cloudscale] ポリシーに変更できます。

[N9K R シリーズ プラットフォーム キューイング ポリシー（N9K R-Series Platform Queuing Policy）]：ドロップダウンリストから、ファブリック内の R で終わるすべての Cisco Nexus スイッチに適用するキューイング ポリシーを選択します。有効な値は [queuing_policy_default_r_series] です。

[その他の N9K プラットフォーム キューイング ポリシー（Other N9K Platform Queuing Policy）]：ドロップダウンリストからキューイング ポリシーを選択し、ファブリック内にある、上記 2 つのオプションで説明したスイッチ以外の他のすべてのスイッチに適用します。有効な値は [queuing_policy_default_other] です。

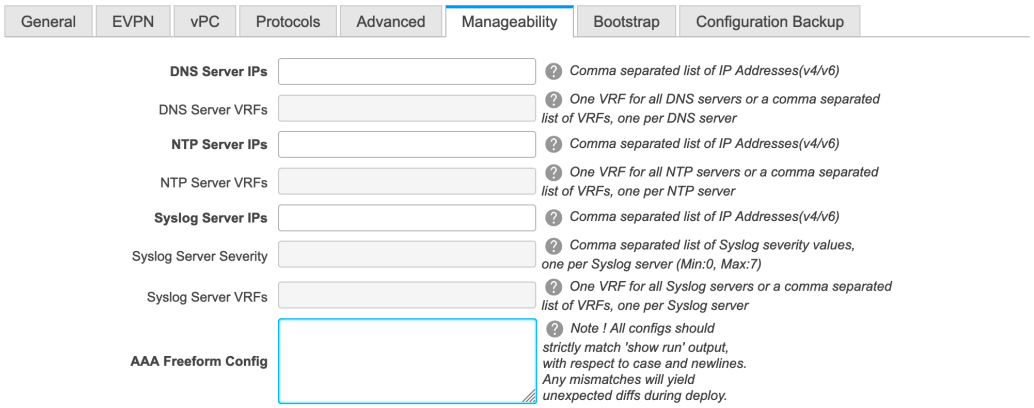
[MACsec の有効化（Enable MACsec）]：ファブリックの MACsec を有効にします。詳細については、Easy ファブリックおよび eBGP ファブリックでの MACsec サポート, on page 231を参照してください。

[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、およびボーダーゲートウェイ スパインのロールを持つスイッチに追加する必要がある CLI を追加します。

[ファブリック内リンクの追加設定（Intra-fabric Links Additional Config）]：ファブリック内リンクに追加する CLI を追加します。

8. **管理能力（Manageability）** タブをクリックします。



このタブのフィールドは次のとおりです。

[DNS サーバ IP（DNS Server IPs）]：ドメイン ネーム システム（DNS) サーバの IP アドレス（v4/v6）のカンマ区切りリストを指定します。

[DNS サーバ VRF（DNS Server VRFs）]：すべての DNS サーバに 1 つの VRF を指定するか、DNS サーバごとに 1 つの VRF を、カンマ区切りリストで指定します。

[NTP サーバ IP（NTP Server IPs）]：NTP サーバの IP アドレス（v4/v6）のカンマ区切りリストを指定します。

[NTP サーバ VRF（NTP Server VRFs）]：すべての NTP サーバに 1 つの VRF を指定するか、NTP サーバごとに 1 つの VRF を、カンマ区切りリストで指定します。

[Syslog サーバ IP（Syslog Server IPs）]：syslog サーバの IP アドレスのカンマ区切りリスト（v4/v6）を指定します（使用する場合）。

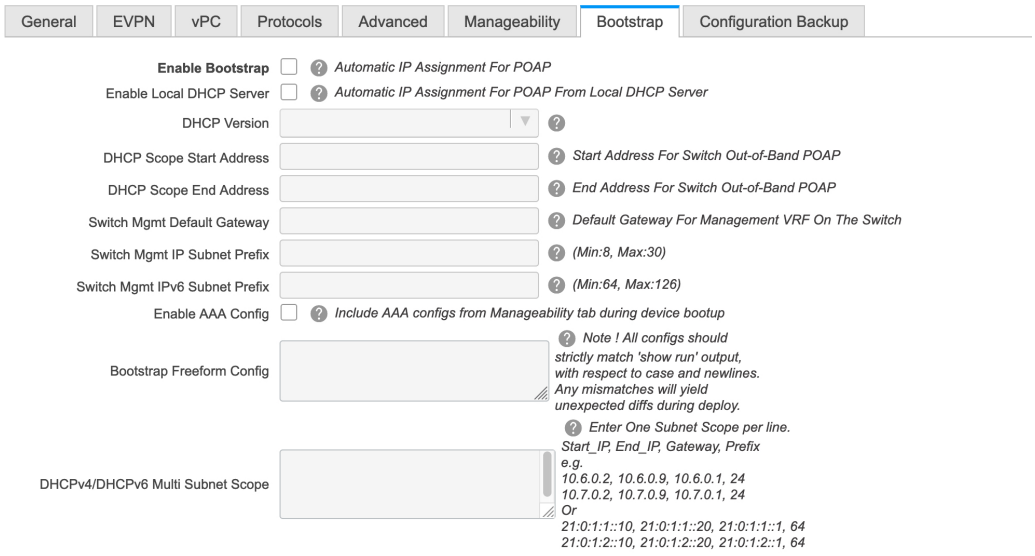
[Syslog サーバのシビラティ（重大度）（Syslog Server Severity）]：syslog サーバごとに 1 つの syslog シビラティ（重大度）値のカンマ区切りリストを指定します。最小値は 0 で、最大値は 7 です。高いシビラティ（重大度）を指定するには、大きい数値を入力します。

[Syslog サーバ VRF（Syslog Server VRFs）]：すべての syslog サーバに 1 つの VRF を指定するか、syslog サーバごとに 1 つの VRF を指定します。

[AAA 自由形式の構成（AAA Freeform Config）]：AAA 自由形式の構成を指定します。

ファブリック設定で AAA 構成が指定されている場合は、**switch_freeform** PTI で、ソースが **UNDERLAY_AAA**、説明が **AAA Configurations** であるものが作成されます。

9. **[ブートストラップ（Bootstrap）]** タブをクリックします。



[ブートストラップの有効化（Enable Bootstrap）]：このチェックボックスを選択し、ブートストラップ機能を有効にします。

ブートストラップをイネーブルにした後、次のいずれかの方法を使用して、DHCP サーバで IP アドレスの自動割り当てをイネーブルにできます。

- 外部 DHCP サーバ（External DHCP Server）：[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）] および [スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）] 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 サーバーの有効化（Enable Local DHCP Server）：ローカル DHCP サーバーを介した自動 IP アドレス割り当ての有効化を開始するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、**[DHCP スコープ開始アドレス（DHCP Scope Start Address）]** および **[DHCP スコープ終了アドレス（DHCP Scope End Address）]** フィールドが編集可能になります。

このチェックボックスをオンにしない場合、DCNM は自動 IP アドレス割り当てにリモートまたは外部DHCPサーバを使用します。

[DHCP バージョン（DHCP Version）]：このドロップダウンリストから [DHCPv4] または [DHCPv6] を選択します。DHCPv4 を選択すると、**[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]** フィールドが無効になります。DHCPv6 を選択すると、**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** は無効になります。

Note Cisco DCNM IPv6 POAP は、Cisco Nexus 7000 シリーズ スイッチではサポートされていません。Cisco Nexus 9000 および 3000 シリーズ スイッチは、スイッチが L2 隣接（eth1 またはアウトオブバンド サブネットは /64 が必須）、またはスイッチがいくつかの IPv6 /64 サブネット内に存在する L3 隣接である場合にのみ、IPv6 POAP をサポートします。/64 以外のサブネット プレフィックスはサポートされません。

[DHCP スコープ開始アドレス（DHCP Scope Start Address）] および [DHCP スコープ終了アドレス（DHCP Scope End Address）] : スイッチのアウトオブバンド POAP に使用される IP アドレス範囲の最初と最後の IP アドレスを指定します。

[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）] : スイッチの管理 VRF のデフォルト ゲートウェイを指定します。

[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）] : スイッチの Mgmt0 インターフェイスのプレフィックスを指定します。プレフィックスは 8 ～ 30 の間である必要があります。

DHCP スコープおよび管理デフォルト ゲートウェイ *IP* アドレスの仕様（*DHCP scope and management default gateway IP address specification*）：管理デフォルト ゲートウェイ IP アドレスを 10.0.1.1 に、サブネット マスクを 24 に指定した場合、DHCP スコープが指定したサブネット、10.0.1.2 ～ 10.0.1.254 の範囲内であることを確認してください。

[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）] : スイッチの Mgmt0 インターフェイスの IPv6 プレフィックスを指定します。プレフィックスは 112 ー 126 の範囲で指定する必要があります。このフィールドは DHCP の IPv6 が有効な場合に編集できます。

[AAA 構成を有効化（Enable AAA Config）] : デバイスの起動時に [管理性（Manageability）] タブから AAA 構成を含めるには、このチェックボックスをオンにします。

[ブートストラップ フリーフォームの構成（Bootstrap Freeform Config）] :（オプション）必要に応じて追加のコマンドを入力します。たとえば、AAA またはリモート認証関連の構成を使用している場合は、このフィールドにこれらの構成を追加してインテントを保存する必要があります。デバイスが起動すると、[Bootstrap Freeform Config]フィールドで定義されたインテントが含まれます。

NX-OSスイッチの実行コンフィギュレーションに示されているように、running-configを正しいインデントで自由形式の設定フィールドにコピーアンドペーストします。freeform config は running config と一致する必要があります。詳細については、スイッチでのフリーフォーム構成エラーの解決を参照してください。ファブリック スイッチでのフリーフォーム構成の有効化に記されています。

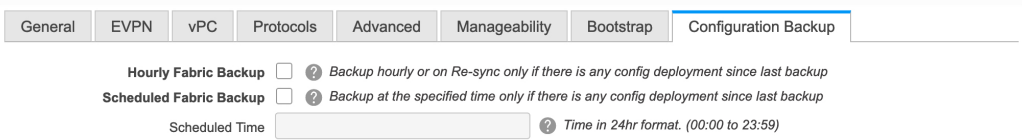
[DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）] : 1行に1つのサブネット スコープを入力して、フィールドを指定します。**[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）]** チェックボックスをオンにした後で、このフィールドは編集可能になります。

スコープの形式は次の順で定義する必要があります。

[DHCP スコープ開始アドレス、DHCP スコープ終了アドレス、スイッチ管理デフォルト ゲートウェイ、スイッチ管理サブネット プレフィックス（DHCP Scope Start Address, DHCP Scope End Address, Switch Management Default Gateway, Switch Management Subnet Prefix）]

例：10.6.0.2、10.6.0.9、16.0.0.1、24

10. **[構成のバックアップ（Configuration Backup）]** タブをクリックします。このタブのフィールドは次のとおりです。



[毎時ファブリック バックアップ（Hourly Fabric Backup）]：ファブリック構成とインテントの毎時バックアップを有効にします。

新しいファブリック設定とインテントの1時間ごとのバックアップを有効にできます。前の時間に構成のプッシュがある場合、DCNM はバックアップを取得します。

インテントとは、DCNM に保存されているが、まだスイッチにプロビジョニングされていない構成を指します。

[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]：毎日のバックアップを有効にします。このバックアップは、構成のコンプライアンスによって追跡されないファブリック デバイスの実行構成の変更を追跡します。

[スケジュール済みの時間（Scheduled Time）]：スケジュールされたバックアップ時間を 24 時間形式で指定します。[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]チェックボックスをオンにすると、このフィールドが有効になります。

両方のチェックボックスをオンにして、両方のバックアップ プロセスを有効にします。

[保存（Save）]をクリックすると、バックアップ プロセスが開始されます。

Note 1 時間ごと、およびスケジュールされたバックアップ プロセスは、次の定期的な構成コンプライアンス アクティビティ中にのみ発生し、最大 1 時間の遅延が発生する可能性があります。即時バックアップをトリガーするには、次の手順を実行します。

a. **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** を選択します。[Fabric Builder] 画面が表示されます。

b. 特定のファブリック ボックス内をクリックします。[ファブリック トポロジ (fabric topology)] 画面が表示されます。

c. 画面左側の **[アクション（Actions）]** パネルで、**[ファブリックの再同期（Re-Sync Fabric）]** をクリックします。

ファブリック トポロジ ウィンドウでファブリック バックアップを開始することもできます。[アクション（Actions）] ペインで [今すぐバックアップ（Backup Now）] をクリックします。

関連情報を入力して更新したら、**[保存（Save）]** をクリックします。

特筆すべき点

- すべてのリーフスイッチには共通の AS 番号があるため、リーフ アンダーレイ ポリシーを一度にすべてのリーフスイッチに展開します。
- ブラウンフィールド移行は、eBGP ファブリックではサポートされていません。
- リーフスイッチの AS 番号は、作成後に再計算と展開（Recalculate & Deploy）操作を実行した後は変更できません。変更が必要になった場合は、**leaf_bgp_asn** ポリシーを削除し、再計算と展開（Recalculate & Deploy）操作を実行して、この AS に関連する BGP 構成を削除する必要があります。次に、新しい AS 番号を使用して、leaf_bgp_asn ポリシーを追加できます。
- Multi-AS モードと Dual-AS モードを切り替える場合は、モードを変更する前に、手動で追加されたすべての BGP ポリシー（リーフスイッチの Leaf_bgp_asn および ebgp オーバーレイ ポリシーを含む）を削除し、**[保存と展開（Save & Deploy）]** 操作を実行します。
- サポートされているロールは、リーフ、スパイン、ボーダー リーフです。
- ボーダー デバイスでは、VRF-Lite は手動モードでサポートされます。
- 機能ファブリックのリーフスイッチとスパイン スイッチにポリシーを適用する必要があります。

ファブリックへのスイッチの追加

各ファブリックのスイッチは一意であるため、各スイッチは 1 つのファブリックにのみ追加できます。

[アクション（Actions）] パネルから **[スイッチの追加（Add Switches）]** オプションをクリックして、DCNM で作成されたファブリックにスイッチを追加します。**[インベントリ管理（Inventory Management）]** 画面が表示されます。画面には 2 つのタブがあり、1 つは既存のスイッチを検出するためのもので、もう 1 つは新しいスイッチを検出するためのものです。両方のオプションについて説明します。

さらに、スイッチとインターフェイスを事前プロビジョニングできます。詳細については、デバイスの事前プロビジョニング , on page 104およびイーサネット インターフェイスの事前プロビジョニング, on page 109を参照してください。

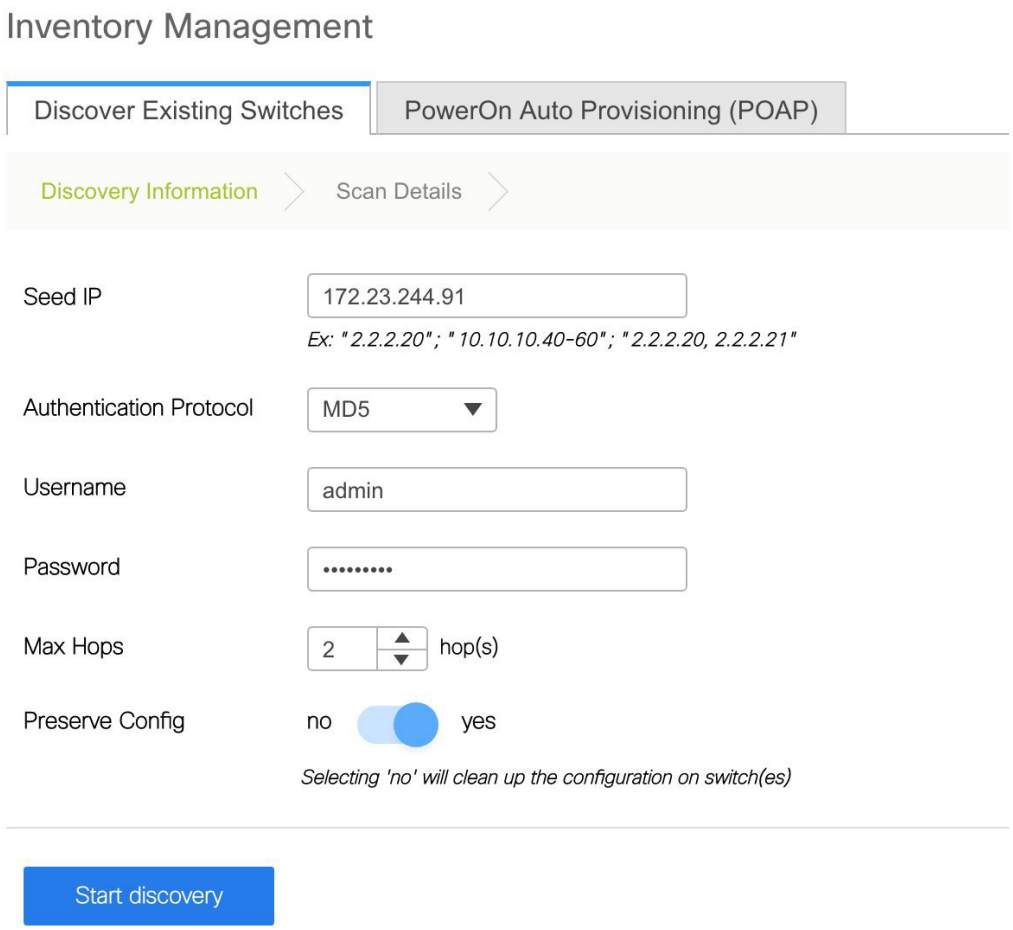
Note DCNM でピリオド文字（.）を含むホスト名を持つスイッチが検出されると、ドメイン名として扱われ、切り捨てられます。ピリオド文字（.）の前のテキストのみがホスト名と見なされます。次に例を示します。

- ホスト名が **[leaf.it.vxlan.bgp.org1-XYZ]** の場合、DCNM で **[leaf]** のみが表示されます。
- ホスト名が **[leaf-itvxlan.bgp.org1-XYZ]** の場合、DCNM で **[leafit-vxlan]** のみが表示されます。

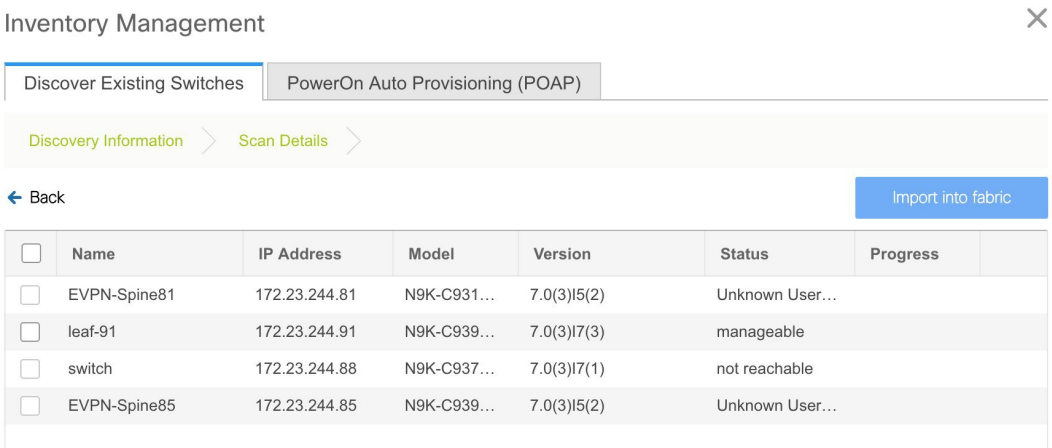
既存のスイッチの検出

1. **[スイッチの追加（Add Switches）]** をクリックした後、**[既存のスイッチの検出（Discover Existing Switches）]** タブを使用して、1 つ以上の既存のスイッチをファブリックに追加します。この場合、既知のクレデンシャルと事前プロビジョニングされた IP アドレスを持つスイッチがファブリックに追加されます。スイッチの IP アドレス（シード IP）、管理者名、ユーザー名、およびパスワード（**[ユーザー名（Username）]** フィールドと **[パスワード（Password）]** フィールド）は、ユーザーによる入力として提供されます。**[構成の保持（Preserve Config）]** ノブは、デフォルトで **[yes]** に設定されています。これは、ファブリックへのデバイスのブラウンフィールドインポートに対してユーザが選択するオプションです。デバイス構成がインポートプロセスの一部としてクリーンアップされるグリーンフィールドインポートの場合、ユーザーは **[構成の保持（Preserve Config）]** ノブを **[no]** に設定する必要があります。

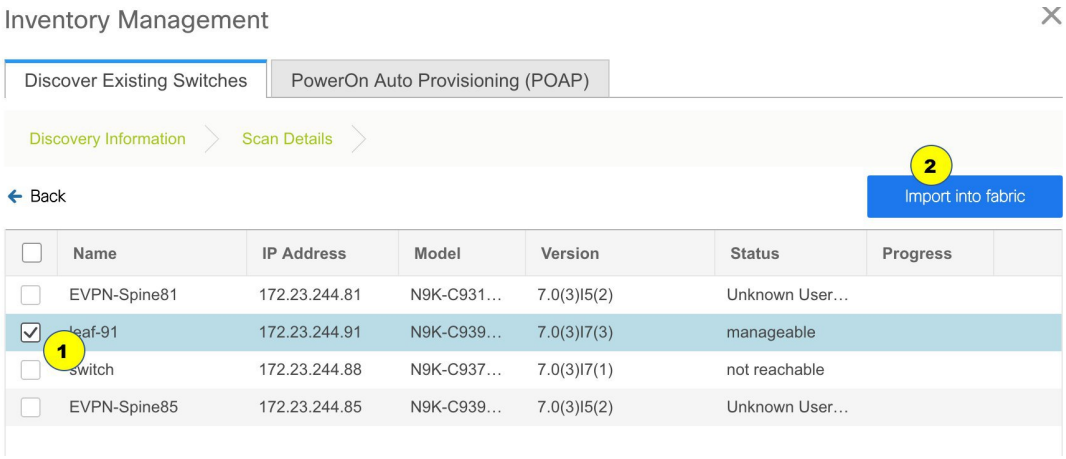
Note Easy_Fabric_eBGP は、ファブリックへのデバイスのブラウンフィールドインポートをサポートしていません。



2. [検出の開始（Start discovery）] をクリックします。**[スキャン詳細（Scan Details）]** ウィンドウが間もなく表示されます。**[最大ホップ（Max Hops）]** フィールドに 2 が入力されているため（デフォルト）、指定された IP アドレス（リーフ 91）を持つスイッチとそのスイッチからの 2 つのホップが **[スキャン詳細（Scan Details）]** の結果に入力されます。



3. DCNM がスイッチに対して正常なシャロー検出を実行できた場合、ステータスに **[管理性（Manageable）]** と表示されます。適切なスイッチの横にあるチェックボックスをオンにして、**[ファブリックにインポート（Import into fabric）]** をクリックします。



この例では 1 つのスイッチの検出について説明しますが、複数のスイッチを同時に検出できます。

スイッチ検出プロセスが開始されます。**[進行状況（Progress）]** 列には、選択したすべてのスイッチの進行状況が表示されます。完了時に各スイッチの**完了**を表示します。

Note 選択したすべてのスイッチがインポートされるか、エラーメッセージが表示されるまで、画面を閉じないでください（また、スイッチを再度追加してください）。

エラー メッセージが表示された場合は、画面を閉じます。[ファブリック トポロジ(fabric topology)] 画面が表示されます。エラーメッセージは、画面の右上に表示されます。必要に応じてエラーを解決し、[アクション（Actions）] パネルの **[スイッチの追加（Add Switches）]** をクリックしてインポート プロセスを再度開始します。

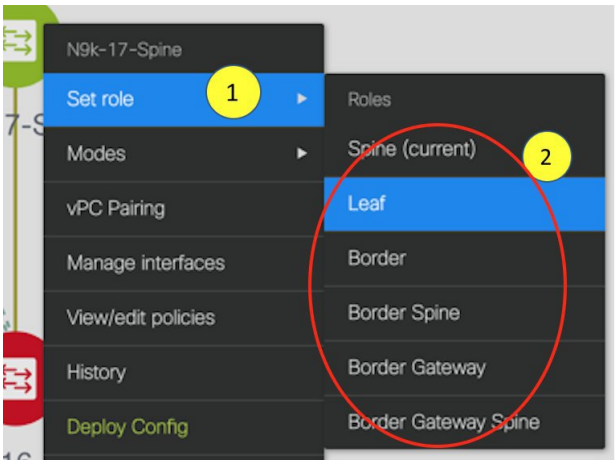
DCNM がすべてのスイッチを検出し、[進行状況（Progress）] 列にすべてのスイッチの **[done]** が表示されたら、画面を閉じます。*[*スタンドアロン ファブリック トポロジ（Standalone fabric topology）] 画面が再び表示されます。追加されたスイッチのスイッチアイコンが表示されます。

Note スイッチの検出中に次のエラーが発生することがあります。

4. 最新のトポロジ ビューを表示するには、**[トポロジの更新（Refresh topology）]** をクリックします。

すべてのスイッチが追加され、ロールが割り当てられると、ファブリック トポロジにはスイッチとスイッチ間の接続が含まれます。

5. デバイスを検出したら、各デバイスに適切なロールを割り当てます。このためには、デバイスをクリックし、**[ロールの設定]** オプションを使用して適切なロールを設定します。代わりに、表形式のビューを使用して、一度に複数のデバイスに同じロールを割り当てることもできます。



表示用に階層レイアウトを選択すると（[アクション（Actions）] パネルで）、トポロジはロールの割り当てに従って自動的に配置され、リーフ デバイスが下部に、スパイン デバイスが上部に接続され、境界デバイスが上部に配置されます。

vPC スイッチ ロールの割り当て：スイッチのペアを vPC スイッチ ペアとして指定するには、スイッチを右クリックし、スイッチのリストから vPC ピア スイッチを選択します。

AAA サーバ パスワード：（**[管理性（Manageability）]** タブで）AAA サーバ情報を入力した場合は、各スイッチで AAA サーバ パスワードを更新する必要があります。そうでない場合、スイッチの検出は失敗します。

Cisco DCNM を使用して新しい vPC ペアが正常に作成および展開されると、コマンドがスイッチに存在する場合でも、**no ip redirects** CLI のいずれかのピアが同期しなくなることがあります。この非同期は、実行構成で CLI を表示するためのスイッチの遅延が原因で発生

し、構成のコンプライアンスに相違が生じます。**[構成の展開（Config Deployment）]** ウィンドウでスイッチを再同期して、差分を解決します。

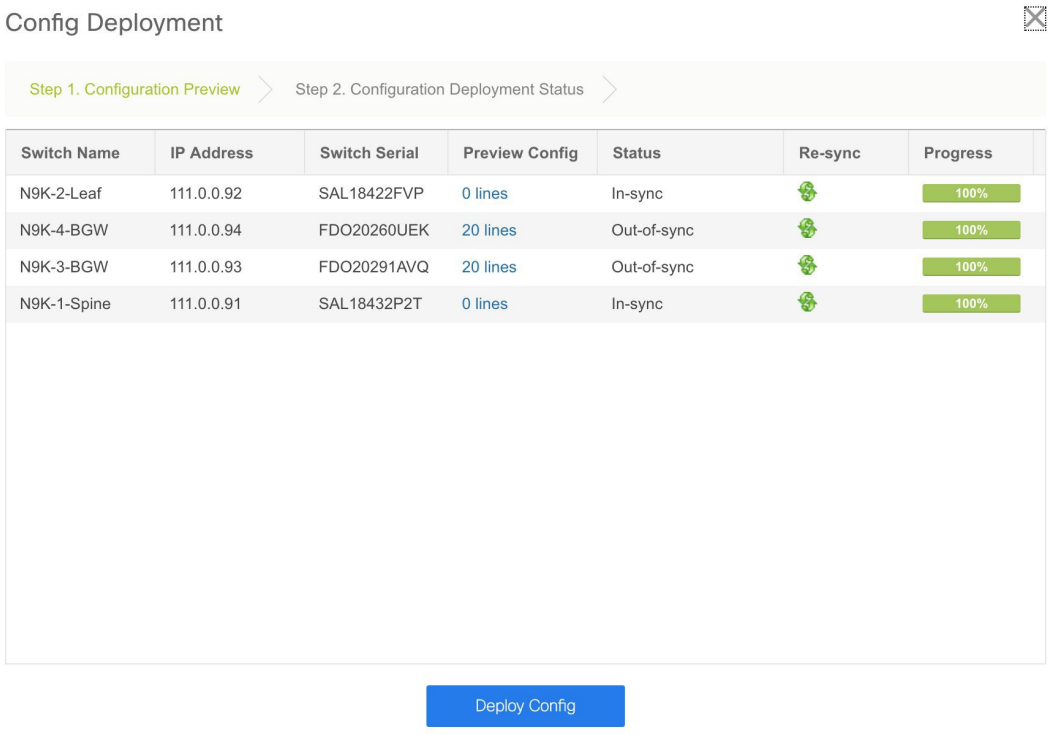
6. 画面の右上にある **[保存と展開（Save & Deploy）]** をクリックします。

テンプレートとインターフェイスの設定は、スイッチのアンダーレイ ネットワーク構成を形成します。また、ファブリック構成の一部として入力されたフリーフォーム CLI（[詳細（Advanced）]タブで入力されたリーフおよびスパイン スイッチのフリー フォーム設定）も展開されます。自由形式構成の詳細については、「ファブリック スイッチでのフリーフォーム設定の有効化」を参照してください。

構成のコンプライアンス：プロビジョニングされた構成とスイッチの構成が一致しない場合、**[ステータス（Status）]** 列に非同期が表示されます。たとえば、CLI を使用してスイッチの機能を手動で有効にすると、設定が一致しなくなります。

Cisco DCNM からファブリックにプロビジョニングされた構成が正確であることを確認したり、逸脱（アウトオブバンド変更など）を検出したりするために、DCNM の構成コンプライアンス エンジンは、必要な修復構成を報告し、提供します。

[保存と展開（Save & Deploy）] をクリックすると、**[構成の展開（Config Deployment）]** ウィンドウが表示されます。



ステータスが非同期の場合は、デバイスの DCNM との構成に不整合があることを示しています。

[再同期（Re-sync）] 列のスイッチごとに [再同期（Re-sync）] ボタンが表示されます。大規模なアウトオブバンド変更がある場合、または設定変更が DCNM に正しく登録されていない場合に、このオプションを使用して DCNM 状態を再同期します。再同期操作は、

スイッチに対して完全な CC 実行を実行し、「show run」および「show run all」コマンドをスイッチから再収集します。再同期プロセスを開始すると、進行状況メッセージが画面に表示されます。再同期中に、実行構成がスイッチから取得されます。スイッチの Out-of-Sync/In-Sync ステータスは、DCNM で定義されたインテントに基づいて再計算されます。

[構成のプレビュー（Preview Config）] 列エントリ（特定の行数で更新）をクリックします。[構成のプレビュー (Config Preview)] 画面が表示されます。

[保留中の構成（PendingConfig）] タブには、正常な展開の保留中の構成が表示されます。

[Side-by-sideComparison] タブには、現在の構成と予想される構成が一緒に表示されます。

DCNM 11 では、複数行のバナー motd 構成がサポートされています。マルチライン バナー motd 構成は、**switch_freeform** を使用するスイッチごと、またはリーフ/スパイン自由形式構成を使用するファブリックごとのいずれかで、自由形式の構成ポリシーを使用して Cisco DCNM で構成できます。複数行のバナー motd が構成された後、ファブリック トポロジ画面（の右上）で **[保存と展開（Save & Deploy）]** オプションを実行して、ポリシーを展開します。そうしないと、ポリシーがスイッチに適切に展開されない可能性があります。**バナー**ポリシーは、単一行のバナー設定のみを設定します。また、自由形式の設定/ポリシーに関連するバナーは1つだけ作成できます。バナー motd を構成するための複数のポリシーはサポートされていません。

7. 画面 を閉じます。

   構成展開の画面で、画面下部の [構成の展開（Deploy Config）] をクリックして、保留中の構成をスイッチに展開開始します。[ステータス（Status）] カラムには、「FAILED」または「SUCCESS」の状態が表示されます。FAILED ステータスの場合は、問題の解決に失敗した理由を調査します。

   構成が正常にプロビジョニングされた後（すべてのスイッチで 100% の進捗が表示された場合）、画面を閉じます。

   ファブリック トポロジが表示されます。構成が成功すると、スイッチのアイコンが緑色に変わります。

   スイッチ アイコンが赤色の場合、スイッチと DCNM の構成が同期していないことを示します。スイッチで展開が保留中の場合、スイッチは青色で表示されます。保留状態は、保留中の展開または保留中の再計算があることを示します。スイッチをクリックし、**[プレビュー（Preview）]** または **[構成の展開（Deploy Config）]** オプションを使用して保留中の展開を確認するか、**[保存と展開（Save & Deploy）]** をクリックしてスイッチの状態を再計算できます。

Note CLI の実行で警告またはエラーが発生した場合は、**[Fabric Builder]** ウィンドウに通知が表示されます。自動解決可能な警告またはエラーには、**[解決（Resolve）]** オプションがあります。

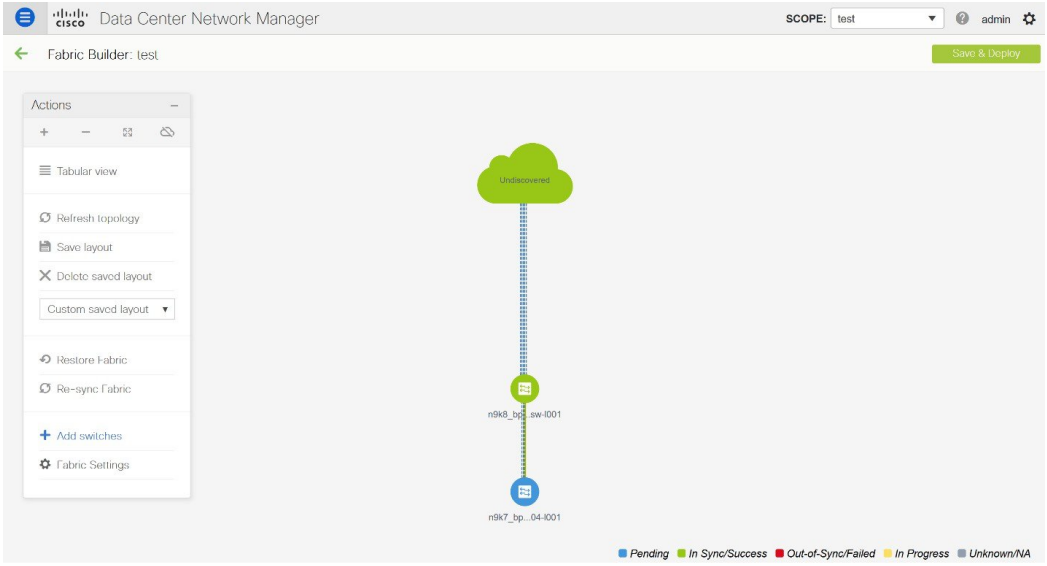
スイッチのリロードまたはRMA操作の後にリーフスイッチが起動すると、DCNMは、スイッチとそれに接続されているFEXデバイスの構成をプロビジョニングします。DCNMがFEX（ホストインターフェイス）構成をプロビジョニングした後にFEX接続が起動し、構成が一致しない場合があります。不一致を解決するには、ファブリック トポロジ画面で**[保存と展開（Save & Deploy）]**を再度クリックします。

Cisco NX-OSリリース11.4(1)以降、**[トポロジ（Topology）]**ウィンドウの**[FEX]**チェックボックスをオフにすると、FEXデバイスは**[ファブリック ビルダ（Fabric Builder）]**トポロジウィンドウでも非表示になります。**Fabric Builder**でFEXを表示するには、このチェックボックスをオンにする必要があります。このオプションはすべてのファブリックに適用でき、セッションごとに保存されるか、DCNMからログアウトするまで保存されます。ログアウトしてDCNMにログインすると、FEXオプションはデフォルトにリセットされます。つまり、デフォルトで有効になります。詳細については、パネルを表示, on page 29を参照してください。

[構成の展開（Deploy Config）]オプションの使用例は、スイッチ レベルの自由形式の設定です。詳細については、「ファブリック スイッチでのフリーフォーム設定の有効化」を参照してください。

新しいスイッチの検出

1. 新しいCisco NX-OSデバイスの電源がオンになると、通常、そのデバイスにはスタートアップ構成も構成ステートもありません。その結果、NX-OSで電源が投入され、初期化後にPOAPループに入ります。デバイスは、mgmt0インターフェイスを含むアップ状態のすべてのインターフェイスでDHCP要求の送信を開始します。
2. デバイスとDCNMの間にIP到達可能性がある限り、デバイスからのDHCP要求はDCNMに転送されます。ゼロデイデバイスを簡単に起動するには、前述のように、**ファブリック設定**でブート ストラップ オプションを有効にする必要があります。
3. ファブリックに対してブートストラップが有効になっている場合、デバイスからのDHCP要求はDCNMによって処理されます。DCNMによってデバイスに割り当てられた一時IPアドレスは、デバイス モデル、デバイスNX-OSバージョンなどを含むスイッチに関する基本情報を学習するために使用されます。
4. DCNM GUIで、ファブリックに移動します（**[制御（Control）] > [ファブリック ビルダ（Fabric Builder）]**をクリックし、ファブリックをクリックします）。ファブリック トポロジが表示されます。



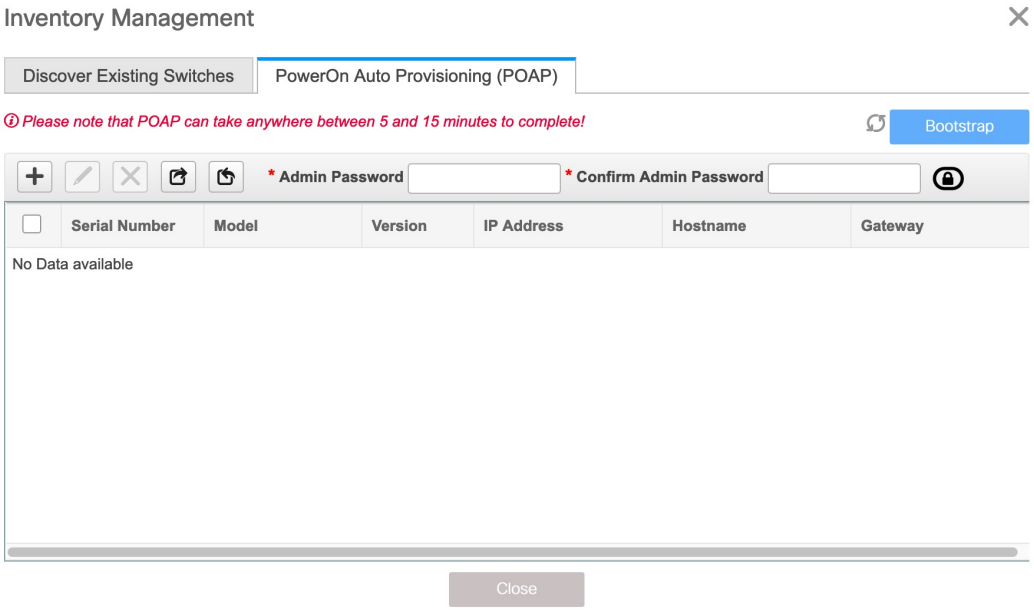
ファブリック トポロジ ウィンドウに移動し、**[アクション（Actions）]** パネルから **[スイッチの追加（Add switches）]** オプションをクリックします。[インベントリ管理（Inventory Management）] ウィンドウが表示されます。

5. **[POAP]** タブをクリックします。

前述のように、DCNM はデバイスからシリアル番号、モデル番号、およびバージョンを取得し、それらを [インベントリ管理（Inventory Management）] ウィンドウに表示します。また、IP アドレス、ホスト名、およびパスワードを追加するオプションが使用可能になります。スイッチ情報が取得されない場合は、ウィンドウを更新します。

Note

- ウィンドウの左上には、スイッチ情報を含む .csv ファイルをエクスポートおよびインポートするためのエクスポートおよびインポート オプションがあります。インポート オプションを使用してデバイスを事前プロビジョニングすることもできます。



スイッチの横にあるチェックボックスを選択し、スイッチのクレデンシャル（IP アドレスとホスト名）を入力します。

デバイスの IP アドレスに基づいて、**[IP アドレス（IP Address）]** フィールドに IPv4 または IPv6 アドレスを追加できます。

リリース 11.2(1) 以降、デバイスを事前にプロビジョニングできます。デバイスの事前プロビジョニングについては、デバイスの事前プロビジョニング , on page 104 を参照してください。

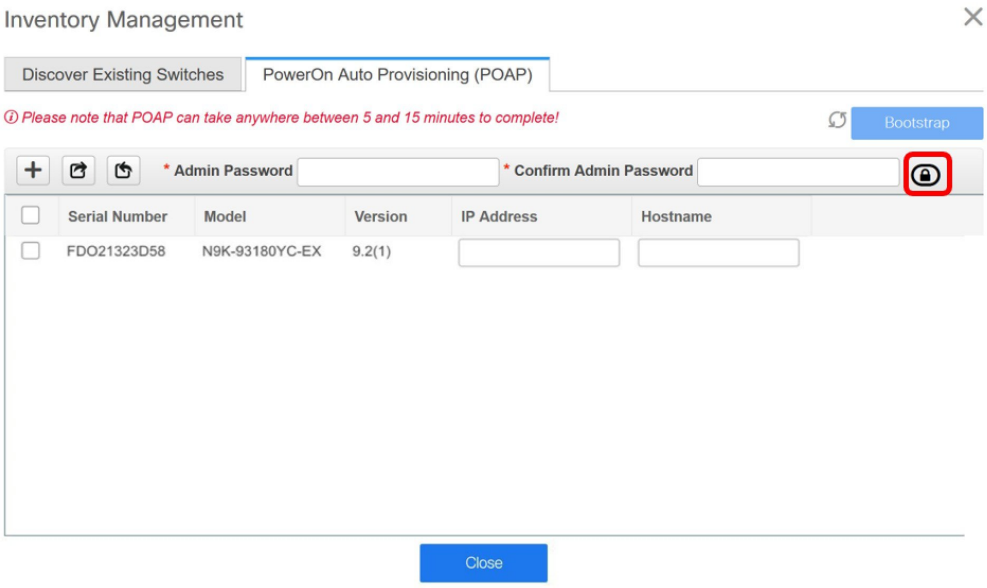
6. **[管理者パスワード（Admin Password）]** フィールドと **[管理者パスワードの確認（Confirm Admin Password）]** フィールドに、新しいパスワードを入力します。

   この管理者パスワードは、POAP ウィンドウに表示されるすべてのスイッチに適用されます。

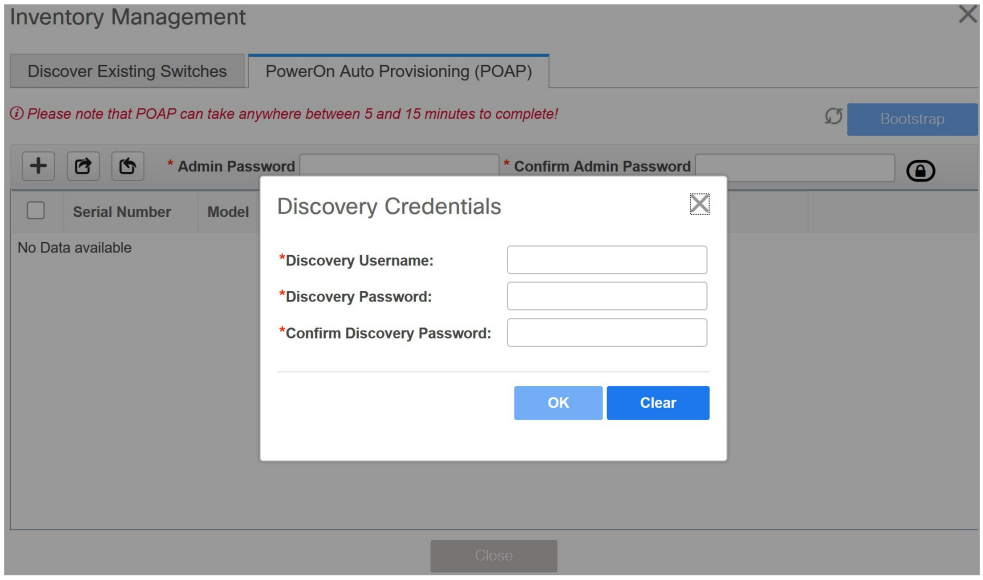
Note 管理者クレデンシャルを使用してスイッチを検出しない場合は、代わりに AAA 認証（RADIUS または TACACS クレデンシャル）を使用できます。

7. （任意）スイッチの検出に検出クレデンシャルを使用します。

   a. **[ディスカバリ クレデンシャルの追加（Add Discovery Credentials）]** アイコンをクリックして、スイッチのディスカバリ クレデンシャルを入力します。



b. **[ディスカバリ クレデンシャル（Discovery Credentials）]** ウィンドウで、ディスカバリ ユーザ名やパスワードなどのディスカバリ クレデンシャルを入力します。



[OK] をクリックして、ディスカバリ クレデンシャルを保存します。

検出クレデンシャルが指定されていない場合は、DCNM は管理者ユーザとパスワードを使用してスイッチを検出します。

8. 画面右上の **[ブートストラップ（Bootstrap）]** をクリックします。

DCNM は管理IPアドレスおよびその他のクレデンシャルをスイッチにプロビジョニングします。この単純化された POAP プロセスでは、すべてのポートが開かれます。

9. 最新情報を入手するには、**[トポロジの更新（Refresh Topology）]** ボタンをクリックします。追加されたスイッチは、POAP サイクルを実行します。スイッチをモニタし、POAP 完了を確認します。

10. 追加されたスイッチが POAP を完了すると、ファブリック ビルダ トポロジページが追加されたスイッチで更新され、検出された物理接続が示されます。スイッチに適切なロールを設定し、ファブリック レベルで [保存と展開（Save & Deploy）] 操作を実行します。ファブリック設定、スイッチロール、トポロジなどが Fabric Builder によって評価され、スイッチの適切な意図された設定が保存操作の一部として生成されます。保留中の設定は、新しいスイッチをインテントと同期させるために新しいスイッチに導入する必要がある設定のリストを提供します。

Note ファブリックで変更が発生して Out-of-Sync が発生した場合は、変更を展開する必要があります。このプロセスは、「既存スイッチの検出」の項で説明したものと同じです。

ファブリックの作成時に、**[管理性（Manageability）]** タブに AAA サーバ情報を入力した場合は、各スイッチの AAA サーバパスワードを更新する必要があります。そうでない場合、スイッチの検出は失敗します。

11. 保留中の設定が展開されると、すべてのスイッチの **[進捗（Progress）]** 列に 100% と表示されます。

12. **[閉じる（Close）]** をクリックして、ファブリック ビルダ トポロジに戻ります。

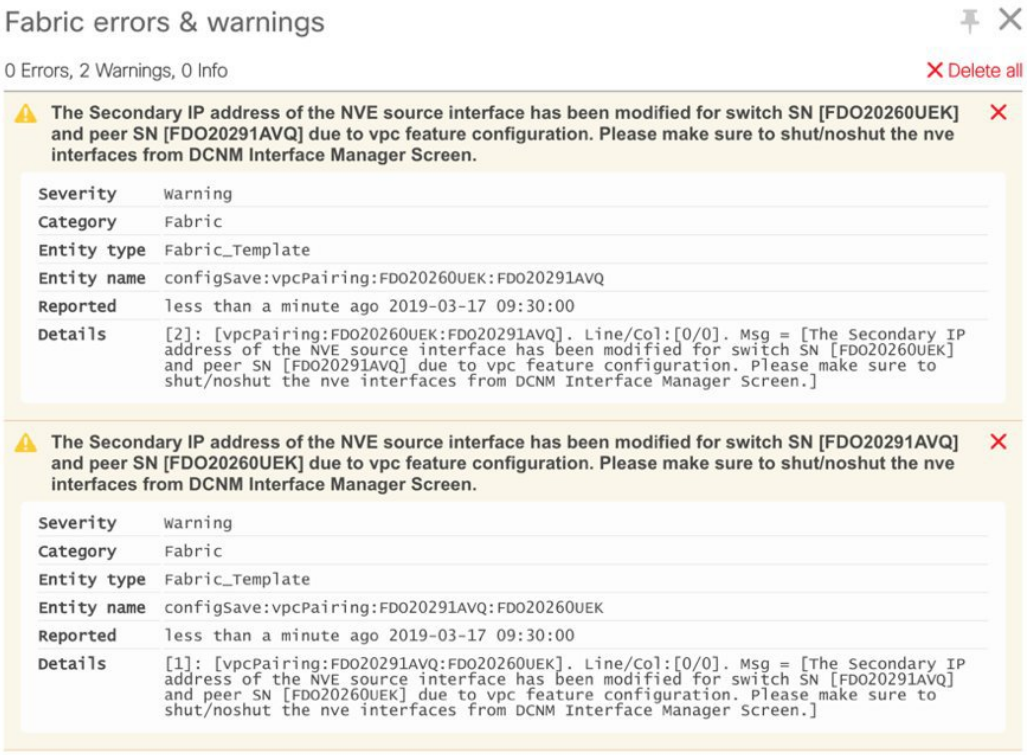
13. **[トポロジの更新（Refresh Topology）]** をクリックして、更新を表示します。すべてのスイッチは、機能していることを示す緑色でなければなりません。

14. スイッチとリンクが DCNM で検出されます。設定は、さまざまなポリシー（ファブリック、トポロジ、スイッチ生成ポリシーなど）に基づいて構築されます。スイッチイメージ（およびその他の必要な）設定がスイッチで有効になっている。

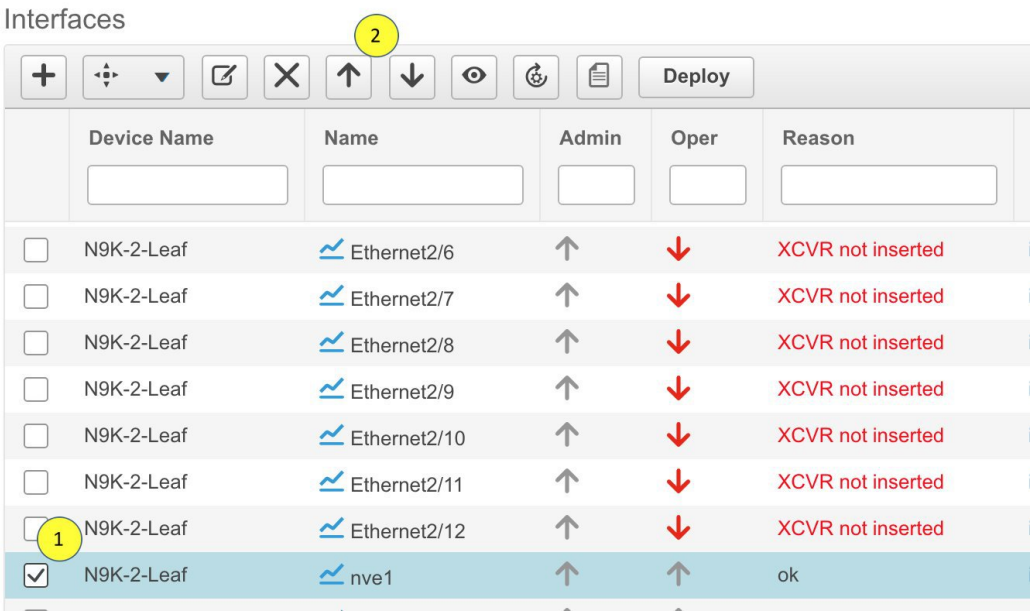
15. DCNM GUIでは、検出されたスイッチは スタンドアロン ファブリック トポロジで確認できます。このステップまでで、POAP は基本設定で完了します。追加構成を行うには、**[制御（Control）] > [インターフェイス（Interfaces）]** オプションを使用してインターフェイスを設定する必要があります。以下が含まれますが、これらに限定されません。

    - vPC ペアリング。
    - ブレークアウト インターフェイス。
    - ポートチャネル、およびポートへのメンバーの追加。

    vPCのペアリング/ペアリング解除または advertise-pip オプションを有効または無効にするか、マルチサイト構成を更新する場合は、**[保存と展開（Save & Deploy）]** 操作を使用する必要があります。操作の終了時に、nve インターフェイスで **shutdown** または **no shutdown** コマンドを設定するように求めるエラーが表示されます。vPC 設定を有効にした場合のエラー スクリーンショットのサンプル：



解決するには、[制御（Control）]>[インターフェイス（Interfaces）]画面に移動し、nve インターフェイスでシャットダウン操作を展開してから、No Shutdown 構成を実行します。これを次の図に示します。上矢印は No Shutdown 操作に対応し、下矢印はShutdown 操作に対応します。



スイッチを右クリックすると、さまざまなオプションを表示できます。

- **ロールの設定**：スイッチにロールを割り当てます（スパイン、ボーダーゲートウェイなど）。

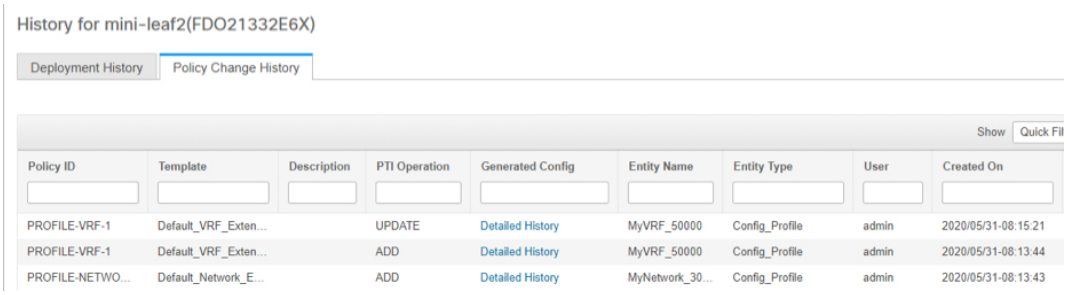
Note

- スイッチのロールの変更は、**[保存と展開（Save & Deploy）]** を実行する前にのみ許可されます。
- DCNM 11.1(1) 以降、スイッチのロールは、スイッチ上にオーバーレイがない場合に変更できますが、スイッチ操作, on page 244 で指定された許可されたスイッチ ロール変更のリストに従ってのみ変更できます。

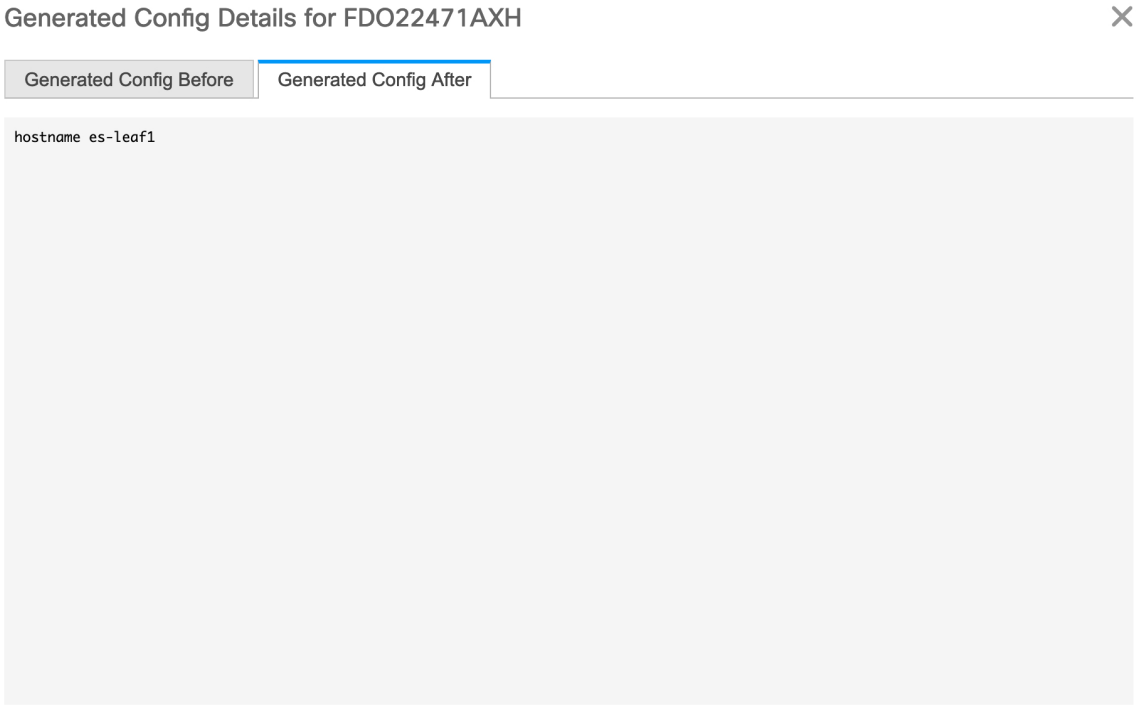
- **モード**：メンテナンス モードとアクティブ/操作モード。
- **vPC** ペアリング：vPC のスイッチを選択し、そのピアを選択します。

  vPCペアの仮想リンクを作成するか、既存の物理リンクをvPCペアの仮想リンクに変更できます。
- **インターフェイスの管理**：スイッチ インターフェイスに構成を展開します。
- **ポリシーの表示/編集**：スイッチ ポリシーを参照し、必要に応じて編集します。
- **履歴**：スイッチの展開およびポリシーの変更履歴を表示します。

  [ポリシー変更履歴（Policy Change History）]タブには、追加、更新、削除などの変更を行ったユーザとともにポリシーの履歴が一覧表示されます。



ポリシーの **[ポリシー変更履歴（Policy Change History）]** タブで、**[生成された構成（Generated Config）]** 列の **[詳細な履歴（Detailed History）]** をクリックして、前後の生成された構成を表示します。



次の表に、ポリシーテンプレートインスタンス（PTI）の前後に生成される構成の概要を示します。

PTI の操作	前に生成された構成	生成後の構成
追加	Empty	構成が含まれています
更新	変更前の構成が含まれています	変更後の構成が含まれています
マーク - 削除	削除する設定が含まれます。	色を変更して削除する構成が含まれます。
削除	構成が含まれています	Empty

Note ポリシーまたはプロファイルテンプレートが適用されると、テンプレートのアプリケーションごとにインスタンスが作成されます。これは、ポリシー テンプレート インスタンスまたは PTI と呼ばれます。

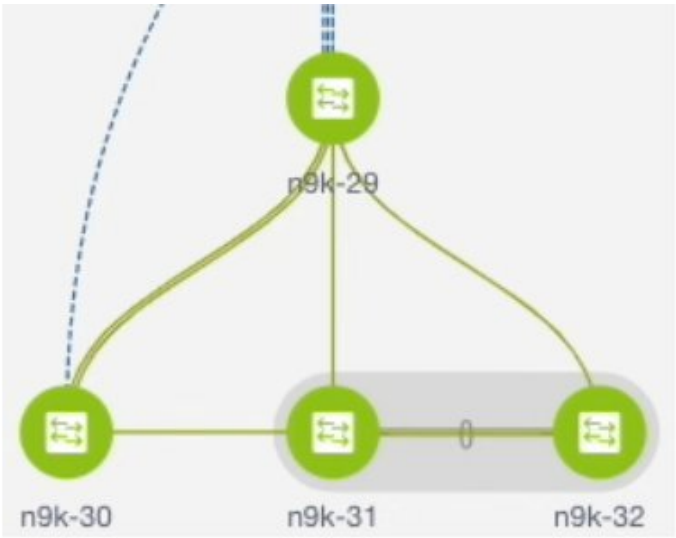
- **[構成のプレビュー（Preview Config）]**：保留中の構成と、実行中の構成と予想される構成の比較を表示します。
- **展開構成** - スイッチ構成ごとに展開します。

- 検出：このオプションを使用して、スイッチのクレデンシャルを更新し、スイッチをリロードし、スイッチを再検出し、ファブリックからスイッチを削除できます。

新しいファブリックが作成され、ファブリック構成スイッチが DCNM で検出され、アンダーレイ構成がそれらのスイッチでプロビジョニングされ、DCNM との間の構成が同期されます。その他のタスクは、次のとおりです。

- vPC、ループバック インターフェイス、サブインターフェイス設定などのインターフェイス構成をプロビジョニングします。[「インターフェイス」を参照してください]。
- ネットワークを作成し、スイッチに展開します。[「ネットワークおよび VRF の作成と展開 」を参照してください]。

ファブリック アンダーレイ eBGP ポリシーの展開



このトポロジは、到達可能性情報を配信するためのルーティング プロトコルとして eBGP が有効になっているルーテッド ファブリックを示しています。DCNM では、**[Easy_Fabric_eBGP]** テンプレートを持つファブリックが作成されます。1 つのスパイン スイッチ（n9k-29）と 3 つのリーフスイッチ（n9k-30、および vPC スイッチ ペア：n9k-31 と n9k-32）がインポートされています。

ファブリックには次の 2 種類があります。

- **マルチ AS モード ファブリックの作成**：マルチ AS モード ファブリックでは、スパイン スイッチには共通の BGP AS 番号があり、各リーフ スイッチには一意の BGP AS 番号があります。Dual-AS から Multi-AS モードへのファブリック変換にも同じ手順を使用します。

- **[Dual-AS モード ファブリックの作成（Creating a Dual-AS mode fabric）]**：Dual-AS モードファブリックの作成については、別の手順が説明されています。Multi-AS から Dual-AS モードへのファブリック変換にも同じ手順を使用します。

  Dual-AS ファブリックでは、すべてのスパイン スイッチには共通の BGP AS 番号があり、すべてのリーフスイッチには共通の BGP AS 番号があります（スパイン スイッチの BGP AS 番号とは異なります）。次のセクションで説明するように、ポリシーを展開する必要があります。

ファブリック アンダーレイ eBGP ポリシーを展開するには、各リーフ スイッチに **leaf_bgp_asn** ポリシーを手動で追加して、スイッチで使用される BGP AS 番号を指定する必要があります。後ほど **[保存と展開（Save & Deploy）]** 操作を実施すると、リーフスイッチとスパイン スイッチ間の物理インターフェイス上に eBGP ピアリングが生成され、アンダーレイの到達可能性情報が交換されます。

1. 画面左側の **[表形式ビュー（Tabular View）]** をクリックします。**Switches | Links** 画面が表示されます。
2. リーフスイッチ（たとえば、n9k-30 チェックボックス）を選択し、**[ポリシーの表示/編集（View/Edit Policies）]** をクリックします。[ポリシーの表示/編集（View/edit policies）] 画面が表示されます。

（注） Dual-AS モードで eBGP ファブリックを作成する場合（または Multi-AS モードから Dual-AS モードに変更する場合）、すべてのリーフスイッチを選択します。これは、共通の BGP AS 番号があるためです。

3. [追加（Add）] をクリックします。**[ポリシーの追加（Add Policy）]** 画面が表示されます。
4. [ポリシー（Policy）] ドロップダウンボックスから、**leaf_bgp_asn** を選択し、**[BGP AS #]** フィールドに BGP AS 番号を入力します。
5. [保存（Save）] をクリックします。
6. vPC スイッチに対してこの手順を繰り返します。vPC スイッチ ペアの場合は、両方のスイッチを選択し、**leaf_bgp_asn** ポリシーを適用します。

（注） 前の手順で説明したように、Dual-AS モードでファブリックを作成（または Dual-AS モードに変換）し、それらすべてに BGP AS 番号を割り当てている場合、この手順は必要ありません。

7. **[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウを閉じます
8. トポロジ画面で、画面の右上にある **[保存と展開（Save & Deploy）]** をクリックします。
9. **構成展開** ウィザードに従って構成を展開します。

eBGPベースのファブリックにおける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

Cisco DCNM リリース 11.3(1) 以降、DCNM 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、DCNM 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 構成を生成します。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 DCNM 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、DCNM 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。
- DCNM リリース 11.2(1) から 11.3(1) へアップグレード後、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 ファブリック構成を更新し、**[保存と展開（Save & 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

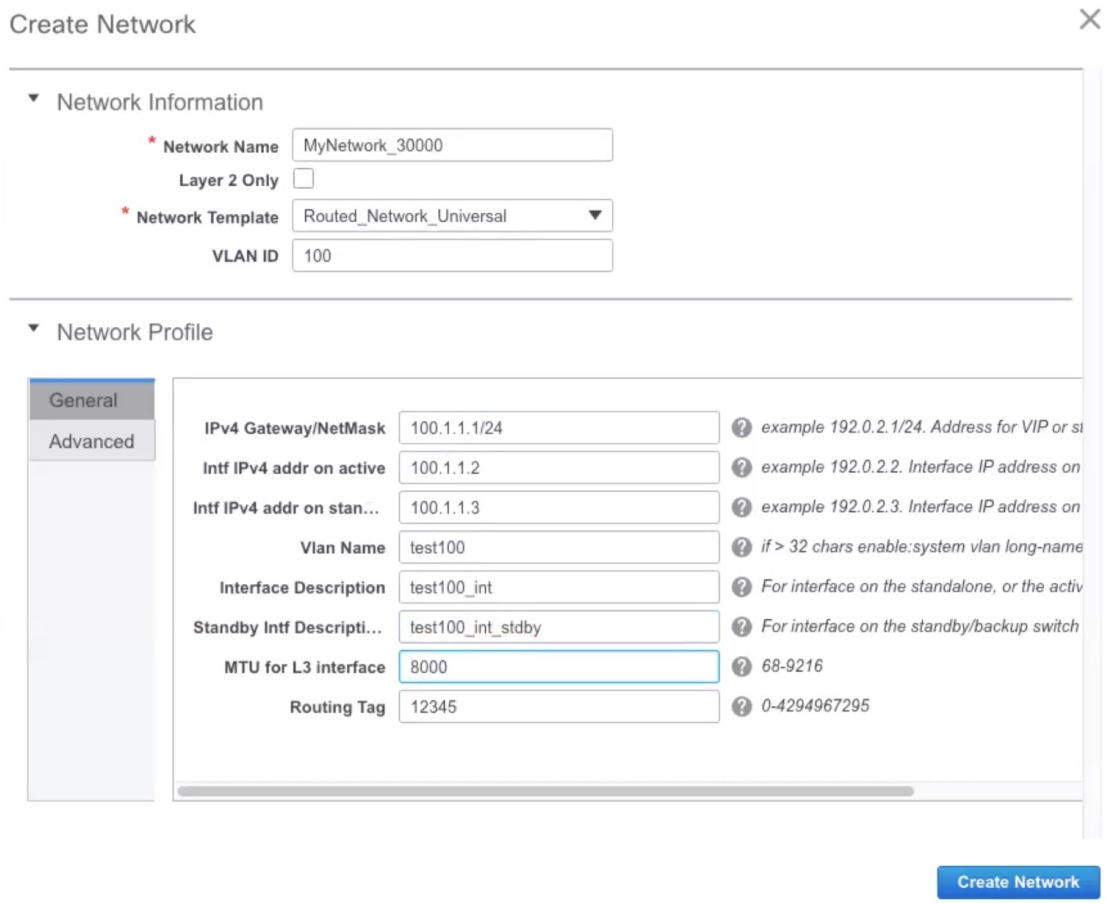
ルーテッド ファブリックを作成し、必要なリーフおよびスパイン ポリシーを展開します。

Procedure

ステップ 1 **[制御（Control）] > [ネットワーク（Networks）]** に移動します。

ステップ 2 **[範囲（SCOPE）]** ドロップダウン リストから、ルーテッド ファブリックを選択します。

ステップ 3 **[ネットワーク（Networks）]** ウィンドウの **[追加（Add）]** ボタンをクリックして、ネットワークを作成します。



[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：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、[全般（General）] タブと [詳細（Advanced）] タブがあります。

[全般（General）] タブ

[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 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。

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。

[全般（General）] 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。

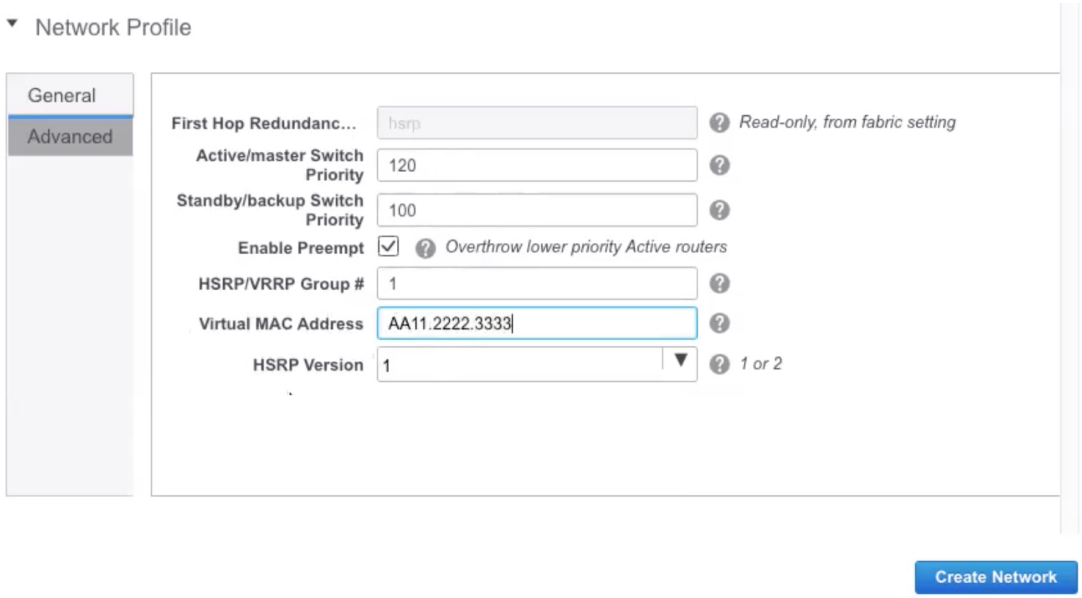
[インターフェイスの説明 (Interface Description)]：インターフェイスの説明を指定します。

[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 デバイスの優先順位を指定します。

[スタンバイ/バックアップ スイッチの優先順位（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順位を指定します。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 4 [ネットワークの作成（Create Network）] をクリックします。

ステップ 5 **[ネットワーク（Networks）]** ウィンドウで、ネットワークの横にあるチェック ボックスをオンにして、**[続行（Continue）]** をクリックします。

Note 非レイヤ2ネットワークは、デバイスの vPC ペアまたは単一のデバイスにのみ適用できます。たとえば、1 つのデバイスにネットワークを展開した場合、別のデバイスまたはデバイスの vPC ペアに同じネットワークを展開することはできません。

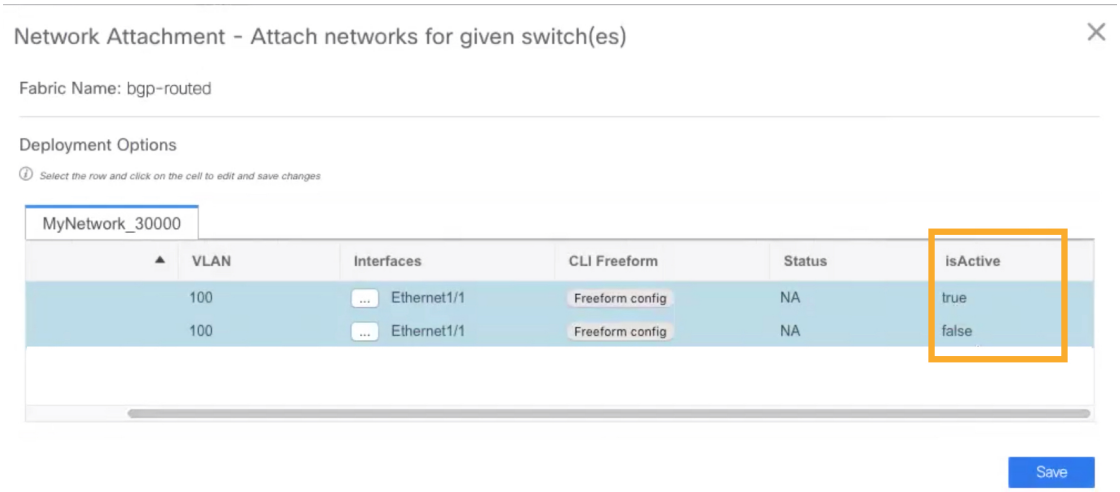
ステップ 6 ネットワークを展開するデバイスまたは vPC ペアを選択します。

Note ルーテッド ファブリックで、アクティブまたはスタンバイ IP アドレスなしで vPC ペアにネットワークを接続しようとすると、IP アドレス フィールドが入力されていないことを示すエラーが表示されます。IPアドレスを追加してネットワークを保存すると、ネットワークを再度接続しなくても、ネットワークの状態が **PENDING** に変わります。

ステップ 7 **[ネットワーク アタッチメント（Network Attachment）]** ウィンドウで、vPC ペアの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** 列に **true** を入力し、スタンバイ デバイスの場合は **false** を入力します。

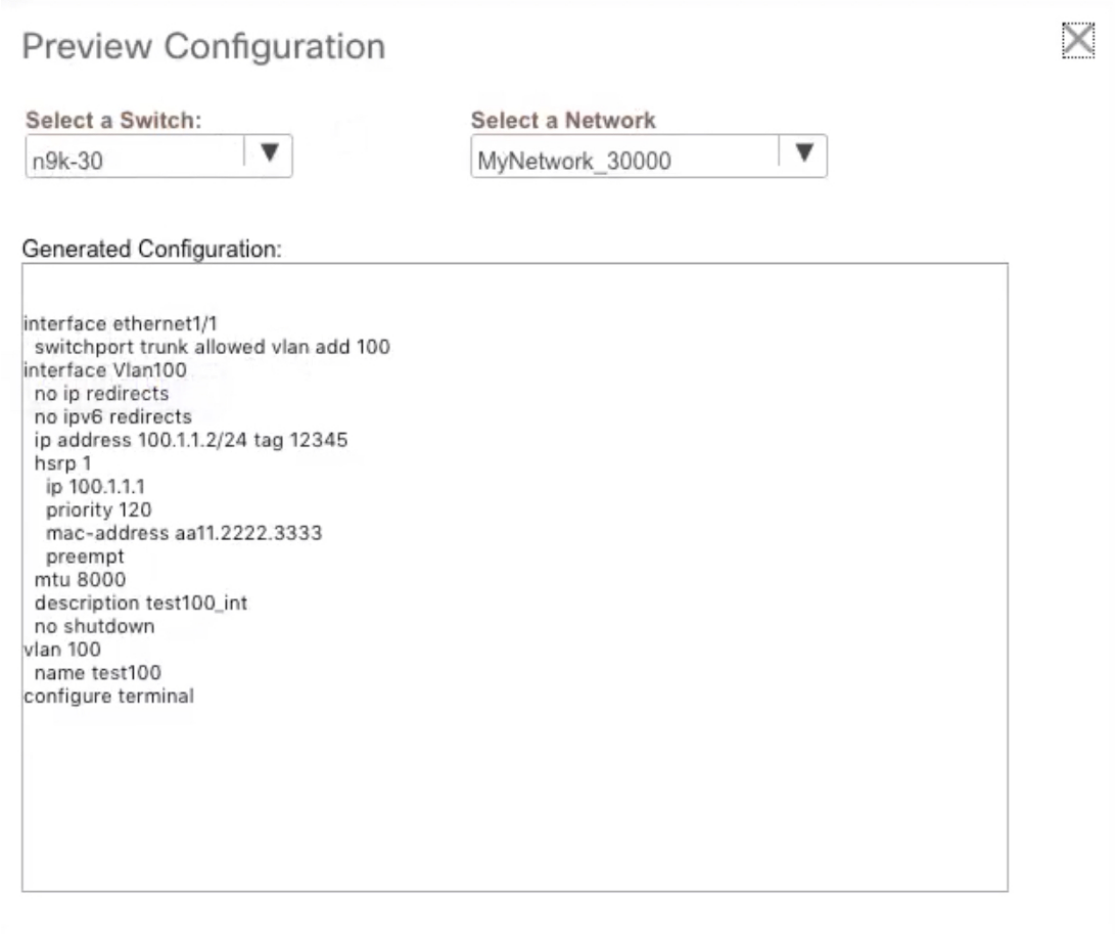
[保存（Save）] をクリックします。



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 8 （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 9 **[ネットワーク / VRF 展開（Network / VRF Deployment）]** ウィンドウの **[展開（Deploy）]** ボタンをクリックします。

[ファブリック ビルダ（Fabric Builder）] 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

DCNM リリース 11.3(1) 以降、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 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 モード（Fabric Monitor Mode）]** チェックボックスをオフにすると、DCNM が構成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」を参照してください。

Procedure

ステップ 1 **[制御（Control）] > [ファブリック ビルダ (Fabric Builder)]** に移動します。

ステップ 2 **ファブリック ビルダ（Fabric Builder）** ウィンドウで、ルーティングされたファブリックをクリックします。

ステップ 3 ウィンドウの左側に表示される **[アクション（Actions）]** パネルの **[表形式ビュー（Tabular view）]** をクリックします。

ステップ 4 **[リンク（Links）]** タブをクリックします。

ステップ 5 **[追加（Add）]** アイコンをクリックして、リンクを追加します。

[リンク管理 – リンクの追加（Link Management – Add 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入力されます。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。

[接続先ファブリック（Destination Fabric）]：このドロップダウンボックスから接続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）]**：接続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。

[接続先デバイス（Destination Device）] と **[接続先インターフェイス（Destination Interface）]**：送信元デバイスに接続する接続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。

[BGP ローカル ASN（BGP Local 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。

[IP アドレス/マスク（IP Address/Mask）]：接続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。

[BGP NEIGHBOR IP（BGP ネイバー IP）]：接続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。

[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。

[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。

[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 スイッチでの自由形式構成の有効化」を参照してください。

ステップ 6 **[保存（Save）]** をクリックして、サイトの追加を終了します。

ステップ 7 **[戻る（Back）]** アイコンをクリックして、ファブリック ビルダ ウィンドウに戻ります。

ステップ 8 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右クリックし、**[構成の展開（Deploy Congif）]** を選択します。

ステップ 9 **[構成展開（Config Deployment）]** 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 **[ファブリック ビルダ（Fabric Builder）]** ウィンドウで外部ファブリックに移動し、**[アクション（Actions）]** パネルの **[表形式ビュー（Tabular view）]** をクリックします。**[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モニタ 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 11 **[戻る（Back）]** アイコンを 2 回クリックして、**[ファブリック ビルダ（Fabric Builder）]** ウィンドウに戻ります。

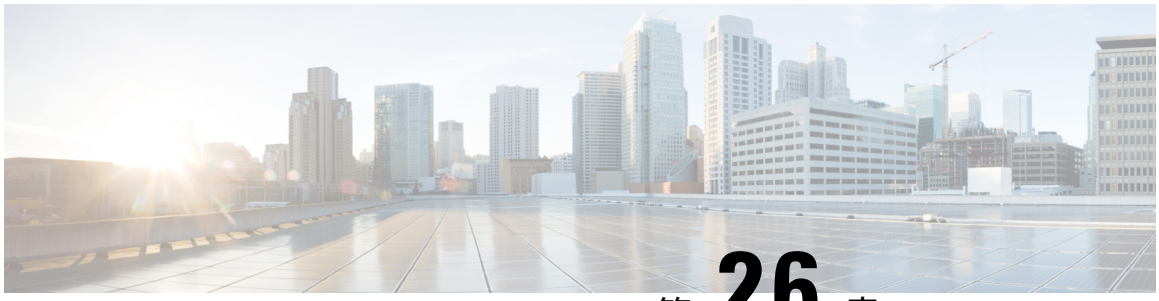
ステップ 12 ルーティングされたファブリックに接続している外部ファブリックをクリックします。

ステップ 13 ルーテッド ファブリックに接続しているデバイスを右クリックし、**[構成の展開（Deploy Config）]** を選択します。

ステップ 14 **[構成展開（Config Deployment）]** ウィンドウで、**[構成の展開（Deploy Config）]** をクリックします。

第 VIII 部

テンプレートの使用方法



第 26 章

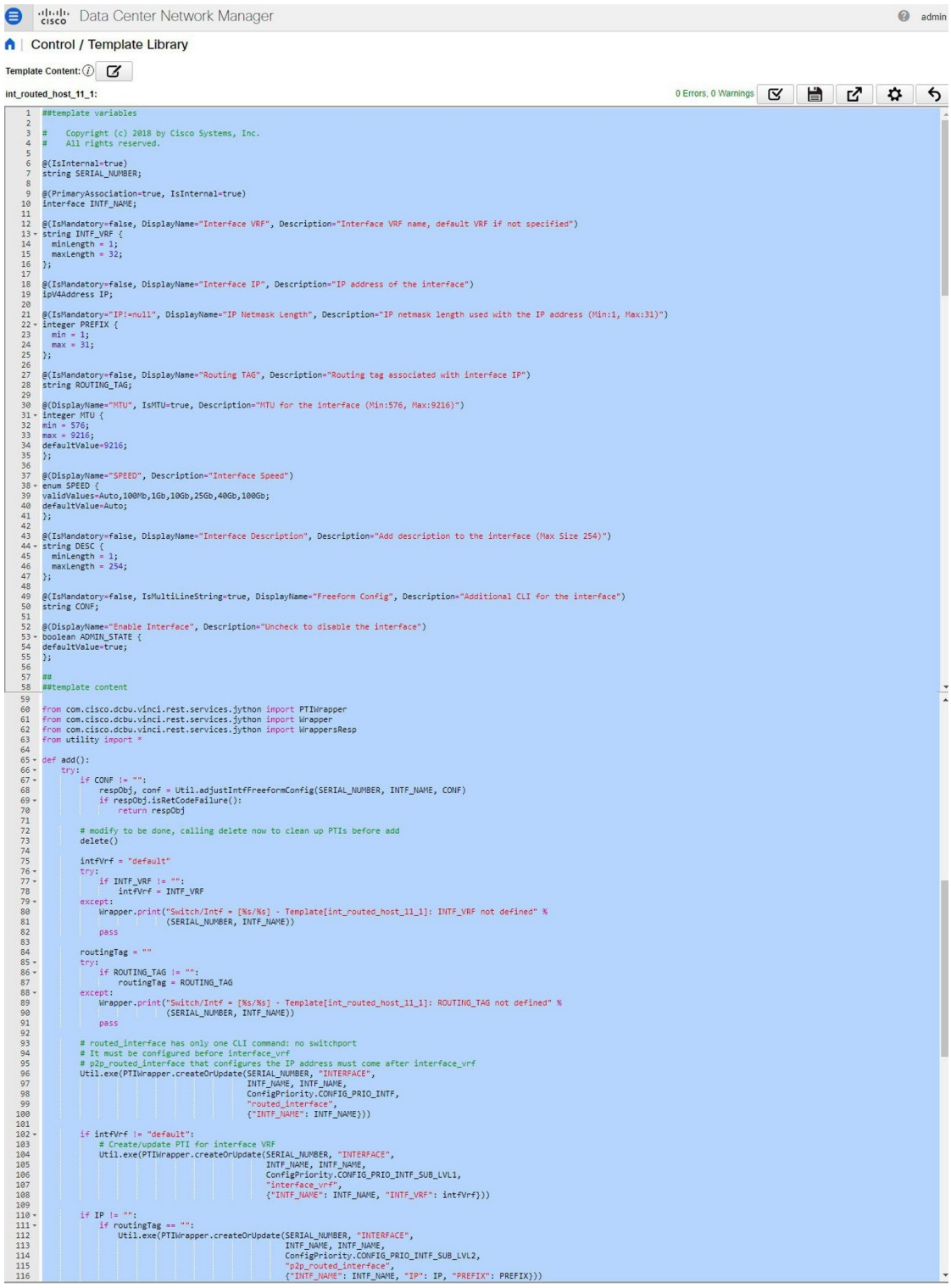
Cisco DCNM LAN ファブリックの展開でのテンプレートの使用

templateType	使用するテンプレートのタイプを指定します。	• CLI • ポリシー • SHOW • プロファイル • [抽象（ABSTRACT）]

ポリシーテンプレート

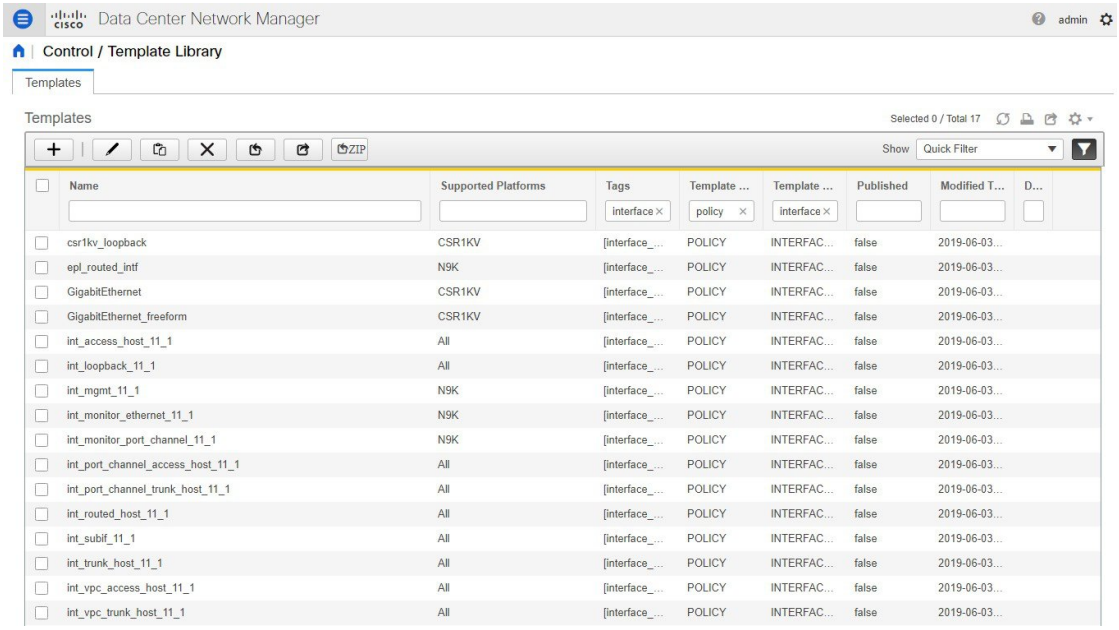
ポリシー テンプレートには、CLI と PYTHON の 2 つのテンプレート コンテンツ タイプがあります。CLI コンテンツ タイプでは、ポリシー テンプレートはパラメータ化された CLI テンプレートです。それらは多くの変数と CLI を持つことができます。通常、CLI ポリシー テンプレートは小さく、if-else-for などのような構造はありません。AAA サーバー構成の CLI ポリシー テンプレートの例を以下に示します。

ただし、テンプレート コンテンツ タイプ PYTHON のポリシー テンプレートを使用することもできます。基本的に、これにより、複数の CLI ポリシー テンプレートを共通の「送信元」と組み合わせて、一度にすべての適用/適用解除を行うことができます。たとえば、vPC ホストポートを作成する場合、vPC ペアの一部である両方のピアで対称的に作成する必要があります。さらに、ポートチャネル、メンバー インターフェイス、チャネル グループなどを作成する必要があります。これが、Python vPC ホスト ポリシーテンプレートが追加された理由です。ルーテッド インターフェイスを設定するためのインターフェイス PYTHON テンプレートの例を以下に示します。

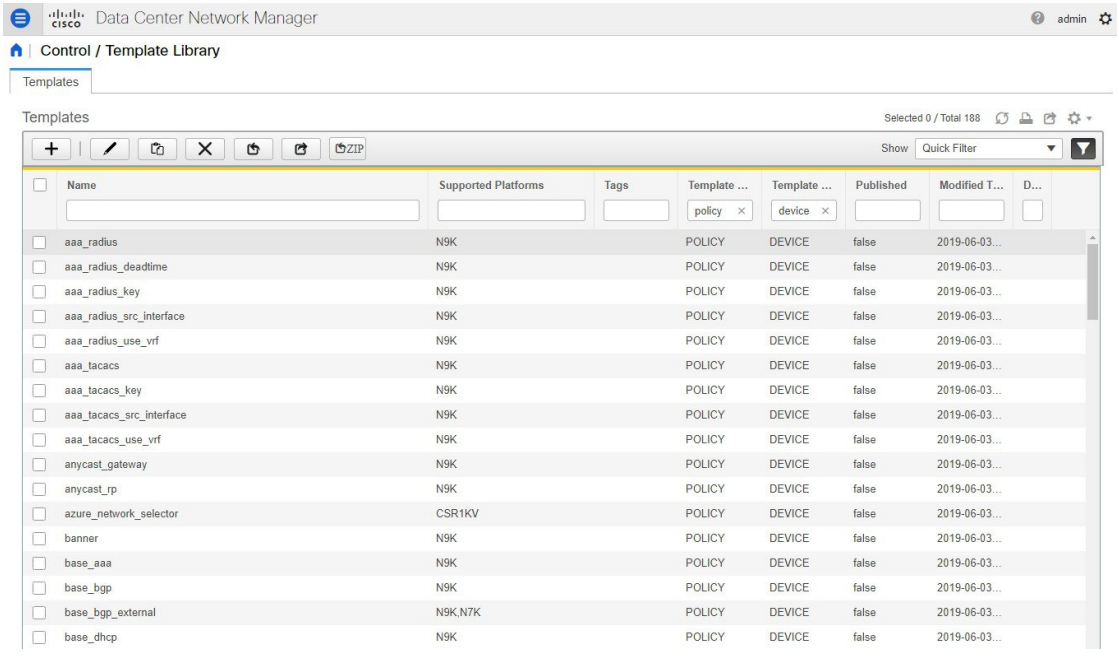


各ポリシー テンプレートには、DEVICE、INTERFACE などのテンプレート サブタイプがあります。これにより、適切なポリシーテンプレートが適切な選択ポイントに表示されます。たと

えば、[インターフェイス（Interface）] ウィンドウには、インターフェイス ポリシー テンプレートのみが表示されます。



ファブリック ビルダの [ポリシーの表示/編集（View/Edit Policies）] ウィンドウには、デバイス ポリシー テンプレートのみが表示されます。



これらのテンプレートのいずれかをコピーして、必要に応じてカスタマイズできます。これは、カスタマイズの典型的なユースケースです。 既存のポリシーを変更**せず**にコピーを作成し、要件に従ってカスタマイズしてください。そうしないと、DCNMのアップグレード後に変更が失われる可能性があります。

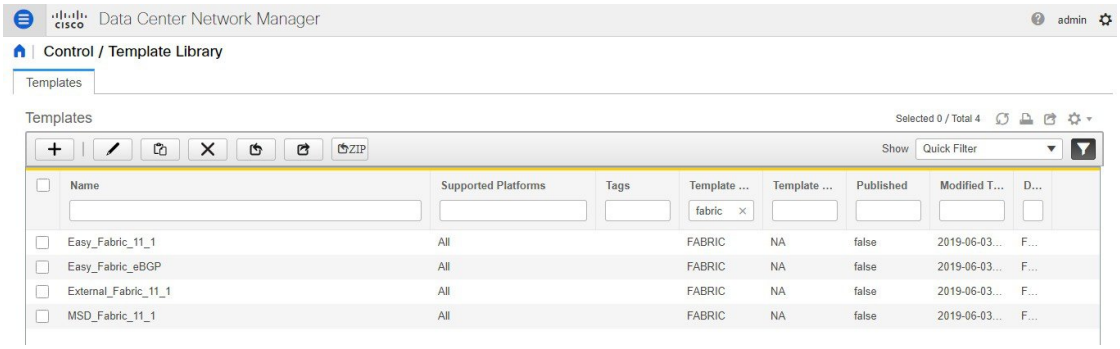
一般に、すでに使用されているテンプレート、つまりファブリック内のスイッチにすでに適用されているテンプレートは編集できません。

（注） LANファブリックインストールモードでは、Type-CLIテンプレートは使用されません。それらはすべて、スーパー セットであるより強力なポリシー テンプレートに置き換えられます。

ファブリックのテンプレート

ファブリック テンプレートは基本的にpythonテンプレート、具体的にはjython、つまりjava+pythonです。ファブリック テンプレートは非常に包括的であり、ファブリック全体内のすべてのスイッチの目的の構成を生成するために必要なすべてのロジックを含む、ファブリックの展開に必要なルールが組み込まれています。構成は、公開されているシスコのベストプラクティス ガイドラインに基づいて生成されます。組み込みルールに加えて、ファブリック テンプレートは、リソース マネージャ、トポロジデータベース、デバイス ロール、構成コンプライアンスなどの他のエンティティとも統合し、ファブリック内のすべてのデバイスに応じて構成を生成します。これは、DCNM ファブリック ビルダに固有の部分です。

ユーザーが独自のファブリック テンプレートを作成しないことが望ましいです。DCNMには、Easyファブリック、外部ファブリック、MSDファブリック、eBGPファブリック（DCNM 11.2で導入）など、すぐに使用できるいくつかのファブリック テンプレートが用意されています。



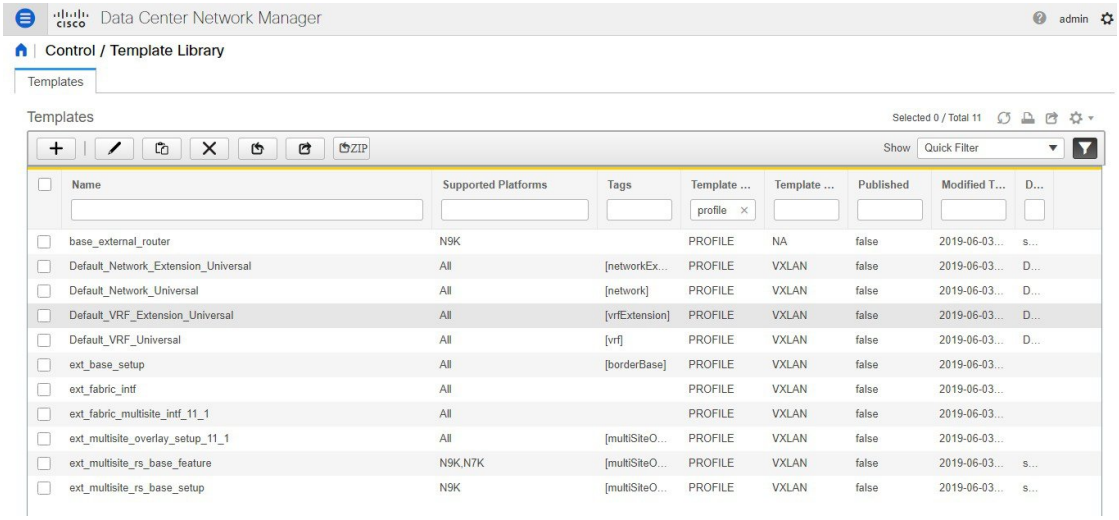
プロファイル テンプレート

プロファイル テンプレートは、オーバーレイ（ネットワークまたはVRF）のプロビジョニングに使用されます。オーバーレイ構成を適用する場合、複数の構成要素を組み合わせる必要があるという考え方です。たとえば、VXLAN EVPN ファブリックの有効なレイヤ3ネットワーク構成には、VLAN、SVI、int nve構成、EVPN ルート ターゲットなどが必要です。これらの要素はすべて、いわゆる構成プロファイル（NX-OS コンストラクト）にまとめられます。そして、一度に効果的に適用されます。スイッチ上で、構成プロファイル全体が適用されるか、何も適用されません。このようにして、スイッチにぶら下がったり迷い込んだりする構成が残

されることはありません。リーフまたはボーダーのいずれの種類のオーバーレイ構成でも、DCNM はプロファイル テンプレートを使用します。

以下に示すように、タグで区別される 4 種類のプロファイル テンプレートがあります。

- ネットワーク プロファイル（ロール リーフを持つすべてのデバイスに適用）
- ネットワーク拡張プロファイル（ロール「border*」を持つすべてのデバイスに適用）
- VRF プロファイル（ロール リーフを持つすべてのデバイスに適用）
- VRF 拡張プロファイル（ロール「border*」を持つすべてのデバイスに適用）



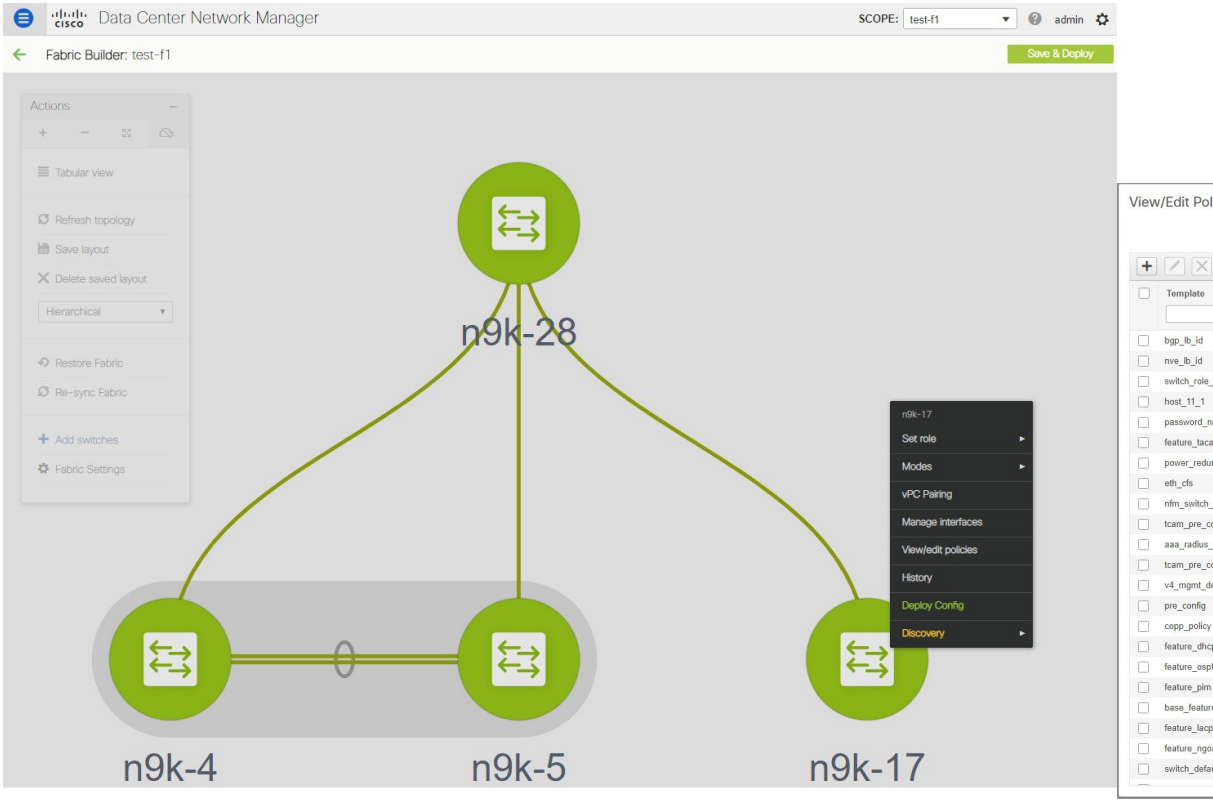
DCNM のネットワークと VRF ワークフローを介してオーバーレイ構成を適用する方法の詳細については、「ネットワークと *VRF* の作成と展開」セクションを参照してください。

補足事項

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。これに使用される一般的な用語は、ポリシーテンプレートインスタンスまたは PTI です。PTI は、実質的にポリシーまたはプロファイルテンプレート + 置換後の特定のインスタンスを与える名前と値のペアです。デバイス用に作成された PTI は、ファブリック ビルダのそのデバイスの [ポリシーの表示/編集（View/Edit policies）] オプションで表示できます。表形式のビューでは、[ポリシーの表示/編集（View/Edit policies）] ボタンを使用して、ファブリック全体のデバイスのサブセット全体でポリシーの選択と一括作成/削除を行うことができます。詳細については、「ポリシーの表示と編集」セクションを参照してください。

ポリシーの表示、編集、および追加

[ポリシーの表示/編集（View/Edit Policies）] ウィンドウに移動するには、[ファブリック ビルダ（Fabric Builder）] ウィンドウでデバイスを右クリックし、[ポリシーの表示/編集（View/edit policies）] を選択します。



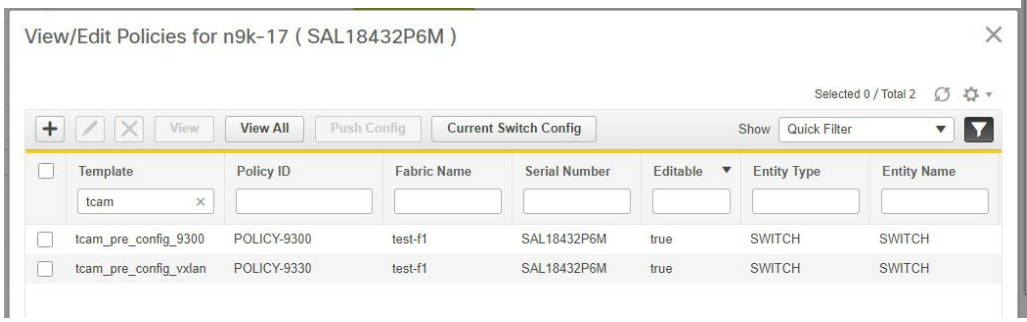
[ポリシーの表示/編集（View/Edit Policies）] ウィンドウを使用して、デバイスのポリシーを表示、編集、または作成できます。インターフェイス ポリシーは表示のみが可能で、[ポリシーの表示/編集（View/Edit Policies）] ウィンドウから編集/作成することはできないことに注意してください。インターフェイスは、[インターフェイス（Interfaces）] ウィンドウからのみ編集、作成、または削除できます。

ポリシーの表示

デバイスの特定のポリシーを表示するには、各フィールドの下にある空のボックスに検索条件を指定することにより、フィルタを使用できます。ポリシーが見つかったら、複数のポリシーを選択して [表示（View）] ボタンをクリックすると、コンテンツを表示できます。以下は、フィルタの使用方法と、ポリシーインスタンスに関連付けられた構成を表示する方法を示す例です。

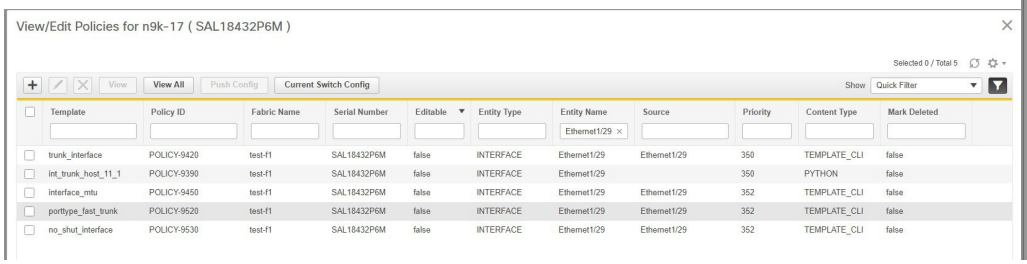
例：デバイスのポリシーの表示

検索フィールドにtcamと入力してテンプレートをフィルタリングし、表示するテンプレートを選択し、[表示（View）] ボタンをクリックして、デバイス用に作成されたTCAM ポリシーを表示します。



例：インターフェイスのポリシーの表示

エンティティ名の下にある検索フィールドにインターフェース名を入力して、インターフェースをフィルタ処理します。インターフェイスを選択し、[表示（View）] ボタンをクリックして、インターフェイス用に作成されたポリシーを表示します。



（注）
- 各インターフェイスは、1 つのインターフェイス jython ポリシー テンプレートに関連付ける必要があります。
- インターフェイス jython ポリシー テンプレートには、そのコンテンツに CLI が含まれていませんが、CLI ポリシー テンプレートの PTI が作成されます。これらすべての PTI が組み合わされて、インターフェイスに関連付けられた完全な構成が生成されます。

ポリシーの編集

すべてのデバイス ポリシーを [ポリシーの表示/編集（View/Edit policies）] ウィンドウから編集できるわけではありません。空の送信元で作成され、フラグ Editable = true を持つポリシーのみを編集できます。

Procedure

ステップ 1 デバイス ポリシーを編集するには、既存のポリシーを選択し、編集または [鉛筆（Pencil）] ボタンをクリックします。[ポリシーの編集 (Edit Policy)] ウィンドウが開きます。

ステップ 2 1 つ以上の名前と値のペアを変更したら、[保存（Save）] ボタンを押して [ポリシーの編集（Edit Policy）] ウィンドウで変更を保存します。

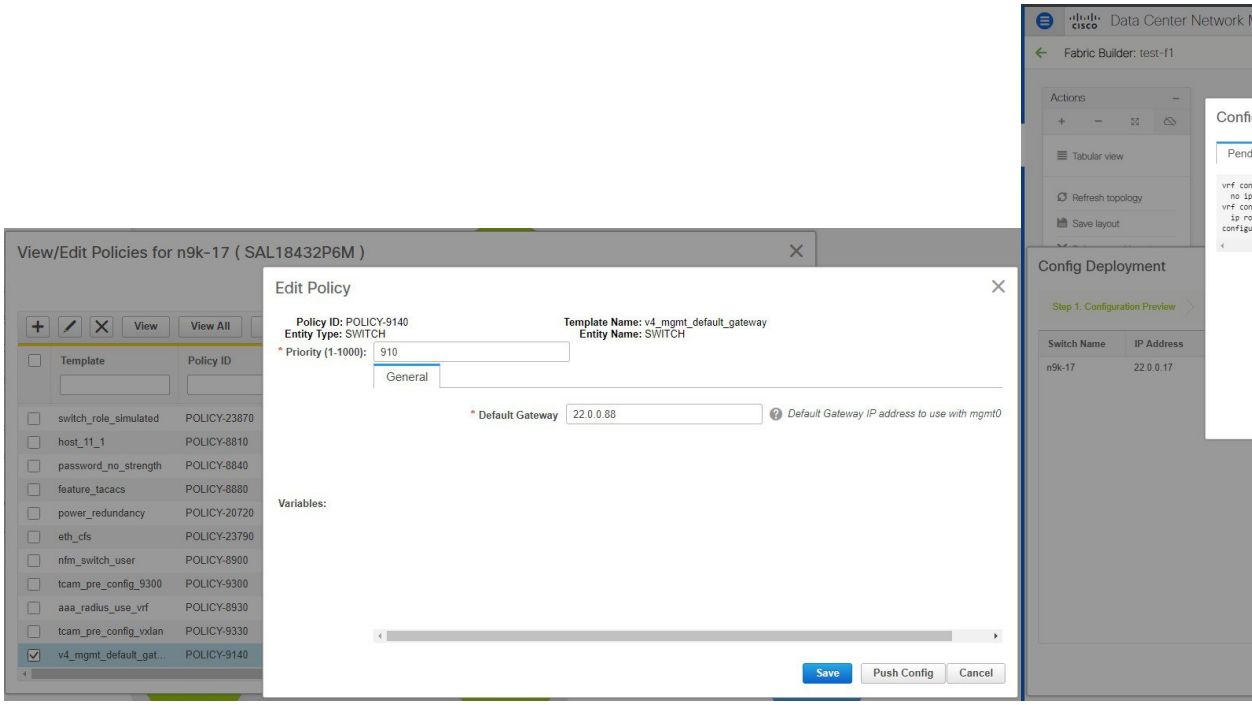
ステップ 3 変更した構成を展開するには、[ファブリック ビルダ（Fabric Builder）] ウィンドウに戻り、デバイスを右クリックして [構成の展開（Deploy Config）] を選択します。

これにより、構成コンプライアンスが呼び出され、デバイスの保留中の構成が生成されます。保留中の構成は、スイッチの現在の構成と新しいインテント構成の差分です。

ステップ 4 保留中の構成が正しい場合は、[構成の展開（Deploy Config）] をクリックして保留中の構成をスイッチにプッシュします。

例：ポリシーの編集

この例は、IPv4 管理デフォルトゲートウェイを変更する方法を示しています。



ポリシーの追加

Procedure

ステップ 1 ポリシーをデバイスに追加するには、[ポリシーの表示/編集（View/Edit Policies）] ページで [+] ボタンをクリックします。

[ポリシーの追加（Add Policy）] ウィンドウが開きます。

ステップ 2 [ポリシー（Policy）] ドロップダウンリストから、デバイスに追加するポリシーを選択します。

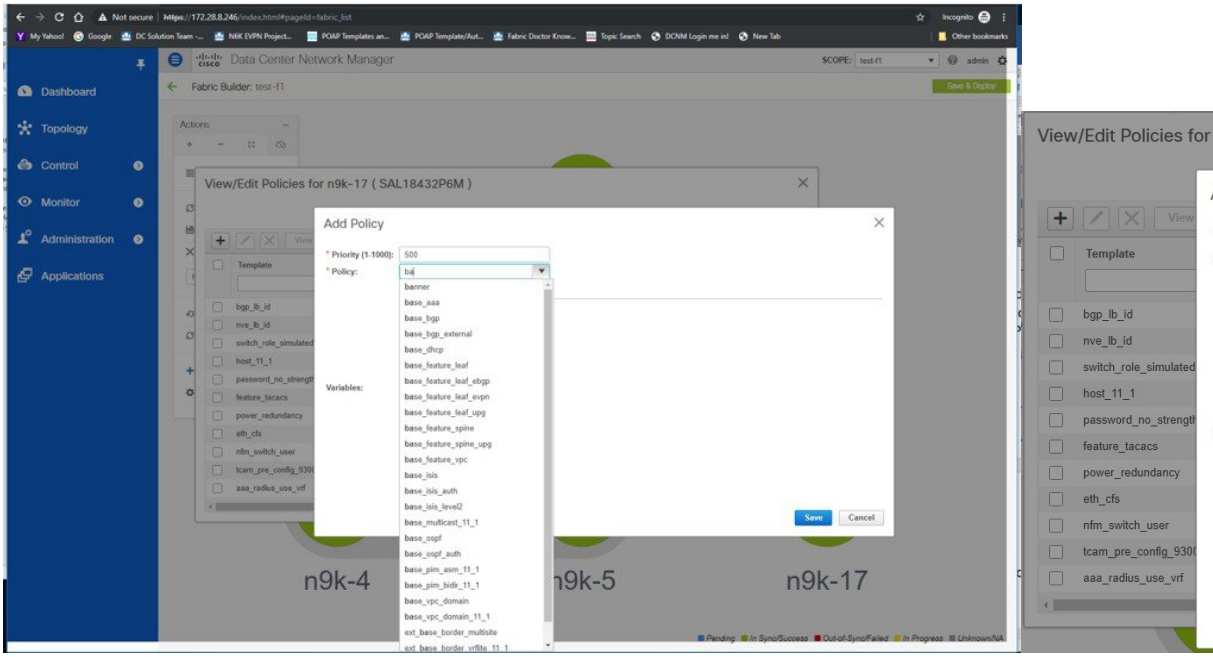
ステップ 3 ポリシーの優先順位を設定し、必須フィールドに入力します。

ステップ 4 [保存（Save）] ボタンをクリックして保存し、ポリシーの追加を完了します。

Note ポリシーの優先順位は、構成がスイッチに適用される順序を決定するために使用されます。望ましい構成またはインテントでは、優先順位の低い PTI が優先順位の高い PTI の前に配置されます。これが、展開モジュールを介して構成がプッシュされる順序になります。デフォルトの優先順位は 500 です。

バナー ポリシーの追加

この例は、バナー ポリシーをデバイスに追加する方法を示しています。



新しい構成の展開

新しい構成を展開するには、次の 2 つの方法があります。

1. [ファブリック ビルダ（Fabric Builder）] ウィンドウに移動し、デバイスを右クリックして [構成の展開（Deploy Config）] を選択します（この方法が推奨されています）。
2. [ポリシーの表示/編集（View/Edit Policies）] ウィンドウで、新しく追加したポリシーを選択し、[表示（View）] をクリックして構成を確認します。新しい構成が適切に見える場合は、[構成のプッシュ（Push Config）] ボタンをクリックして、新しい構成をデバイスにプッシュします。[構成のプッシュ（Push Config）] は構成コンプライアンスをバイパスすることに注意してください。このオプションは、新しいユーザまたはSNMPユーザをスイッチに追加する必要がある場合などの例外シナリオにのみ使用してください。

switch_freeform テンプレートの使用

[switch_freeform] は、ユーザーがデバイスに任意の自由形式構成を指定できるようにする特別なポリシー テンプレートです。テンプレートの使用方法は次のとおりです。

- **[スイッチ自由形式構成（Switch Freeform Config）]** パラメータでスイッチ レベルの構成を指定します。
- 指定された構成は、大文字と小文字と改行に関して **[show run]** 出力と一致する必要があります。不一致があると、展開中に予期しない差分が発生します。
- 指定された構成に対して、内部の **[switch_freeform_config]** CLI ポリシーが作成されます。

- 現在、SVI インターフェイスはインターフェイス ページで構成できないため、SVI インターフェイス以外のインターフェイス構成にはこのテンプレートを使用しないでください。
- ユーザーは、さまざまな構成に対して多くの **[switch_freeform]** ポリシーを作成できます。
- **[switch_freeform]** PTI は、ポリシーの優先順位に基づいて他の PTI と一緒に並べ替えられます。
- **[switch_freeform]** ポリシーは、構成の展開前または展開後に編集できます。
- 構成コンテンツに変更がある場合、以前に作成された内部 **[switch_freeform_config]** ポリシー優先順位が正の数から負の数に変更され、新しい構成に対して新しい内部ポリシーが作成されます。
- **[負（negative）]** の優先順位 PTI は、PTI 内の CLI を削除する必要があることを意味します。**[構成コンプライアンス（Configuration Compliance）]** は、それに応じて **[no]** コマンドを生成します。
- **[switch_freeform]** ポリシーを削除すると、その内部ポリシーの PTI 優先順位が負の数に変更されます。

次のセクションでは、**[switch_freeform]** ポリシーを作成し、ポリシーを展開し、その後、更新されたポリシーを編集して再展開する方法を示します。

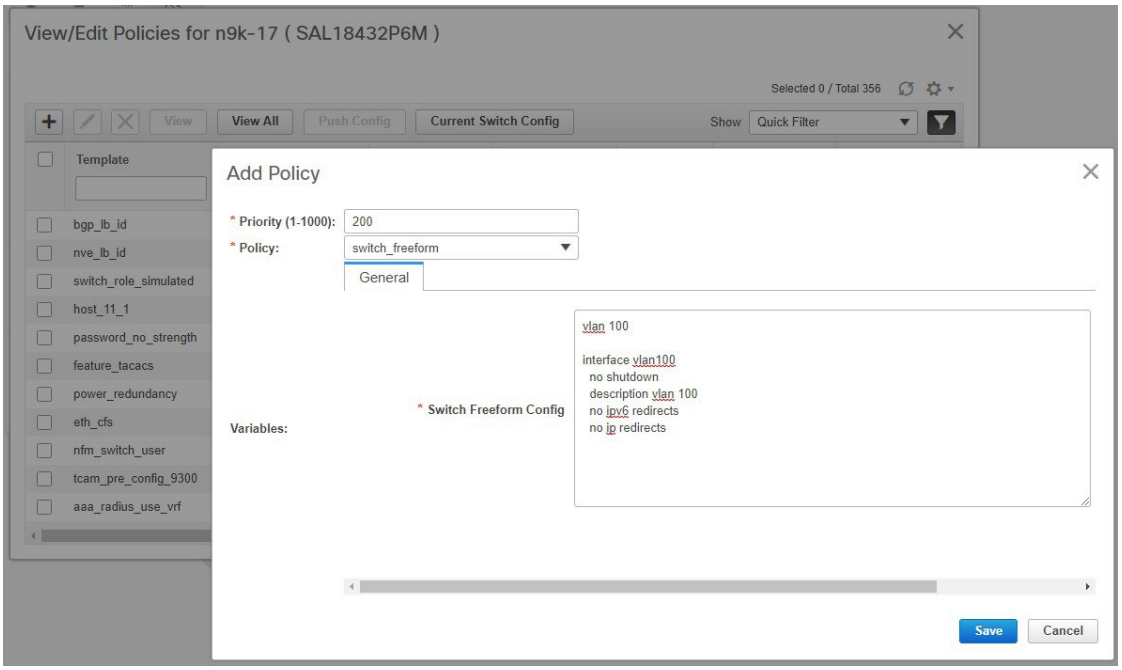
例：switch_freeform ポリシーの作成

[switch_freeform] ポリシーを作成するには、次の手順を実行します。

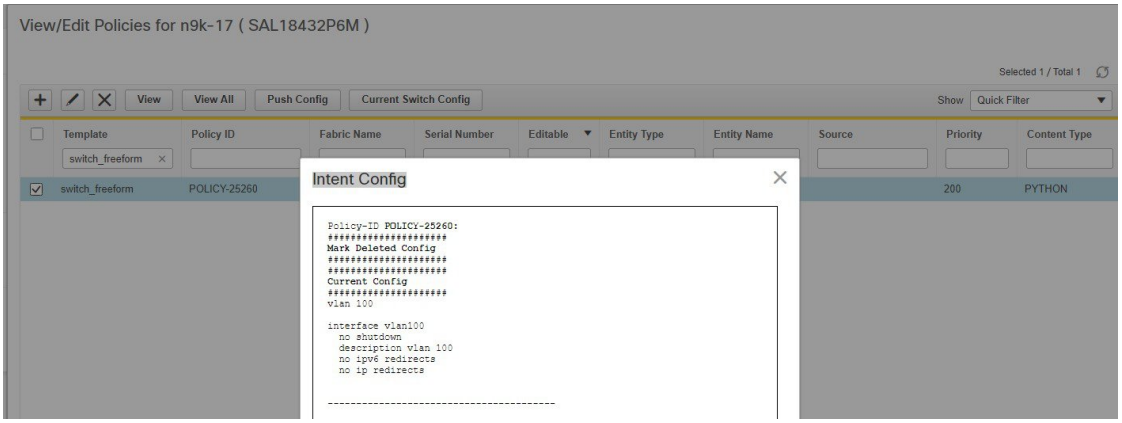
Procedure

ステップ 1 **[ポリシーの追加（Add Policy）]** 画面のポリシー リストから、**[switch_freeform]** テンプレートを選択します。

優先順位を設定し、自由形式構成を切り替えます。ポリシーを保存します。



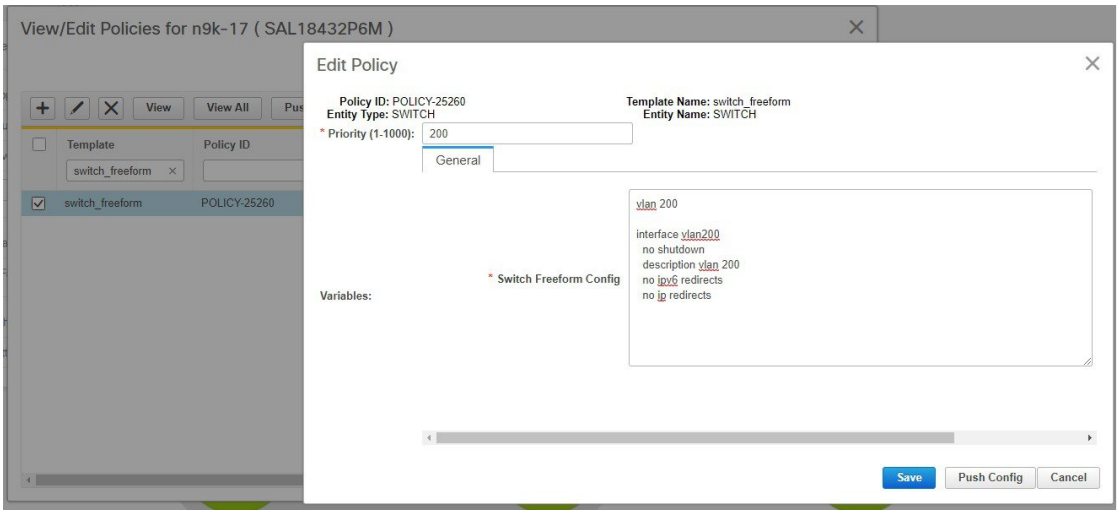
ステップ 2 **[switch_freeform]** ポリシーのインテント構成を表示します。



ステップ 3 ファブリック ビルダから switch_freeform ポリシーを展開します。

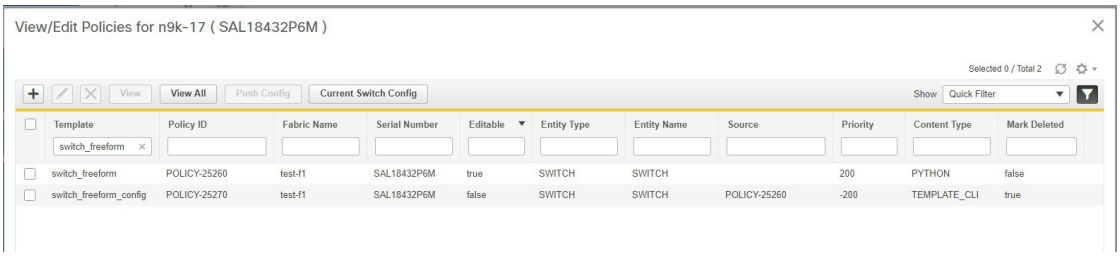
ステップ 4 [ポリシーの表示/編集（View/Edit Policies）] ウィンドウから、switch_freeform ポリシーを編集します。

構成を変更します。

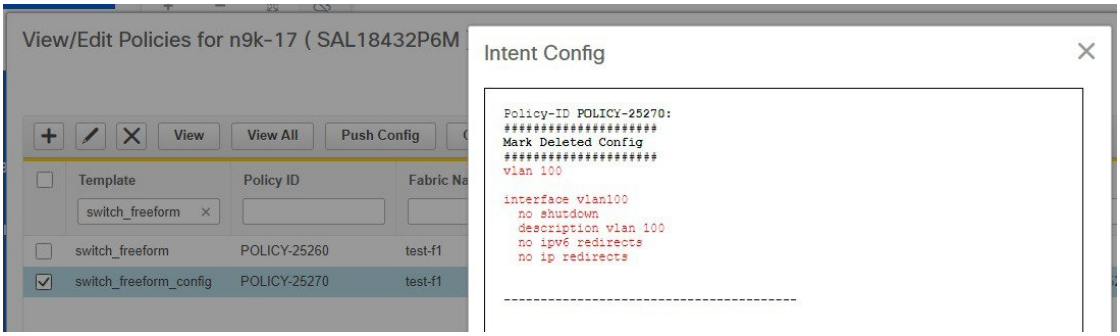


ステップ 5 変更を保存します。

以下に示すように、以前に作成された内部 **[switch_freeform_config]** ポリシーの優先順位が負の数（-200）に変更され、**[削除済みとマークする（Mark Deleted）]** フラグが true に設定されています。ただし、設計により、新しく作成された内部 **[switch_freeform_config]** ポリシーは表示されません。

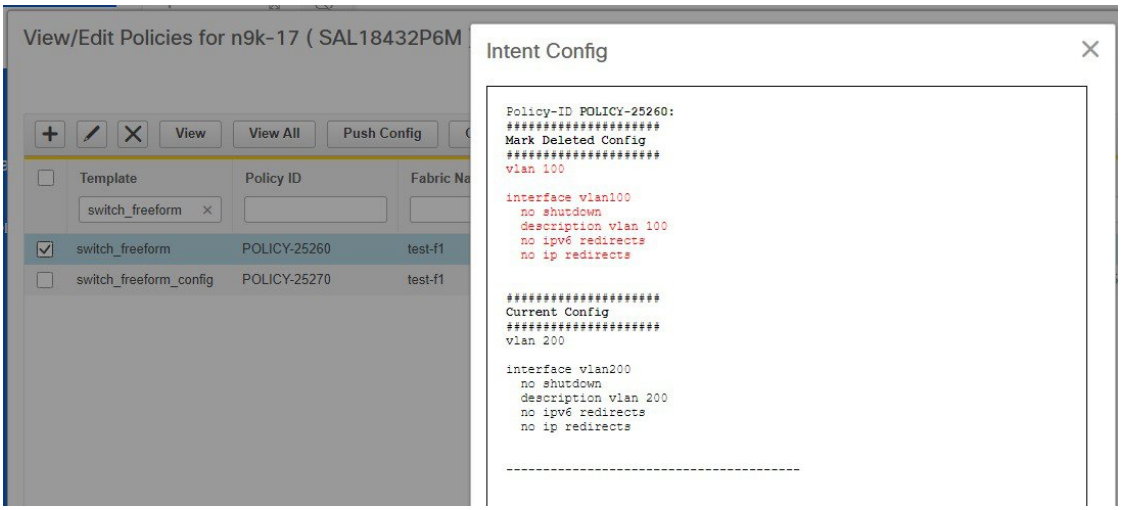


ステップ 6 **[削除済みとマークする（mark deleted）]** 内部ポリシーのインテント構成を表示します。

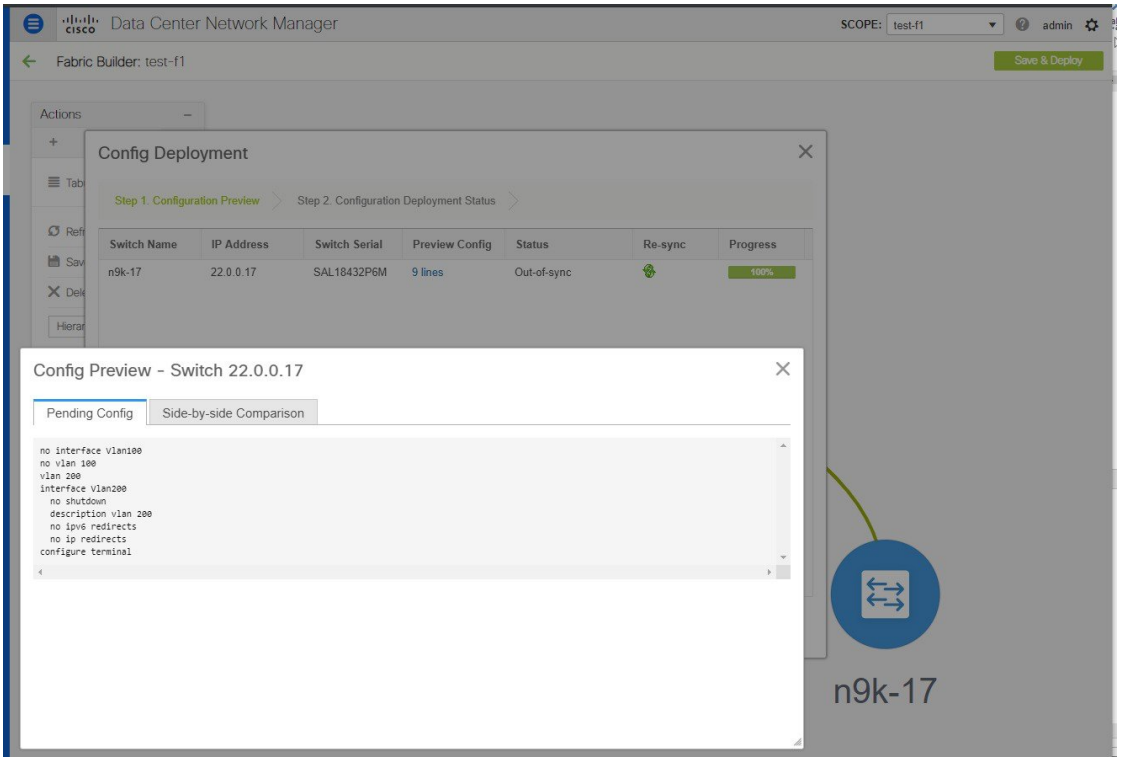


ステップ 7 展開の前に、**[変更された（changed）]** switch_freeform ポリシーのインテント構成を表示します。

[mark-deleted] 構成と**[現在の構成（current configs）]** の両方が表示されることに注意してください。



ステップ 8 変更した構成をファブリック ビルダから展開します。



使用中テンプレートのコンテンツの変更

一般に、テンプレートは、ポリシー、ファブリック、またはプロファイルテンプレートのいずれであっても、インスタンス化されると変更できません。ただし、テンプレートのバグを修正したり、すでに展開されている構成を変更したりするなど、テンプレートのコンテンツを編集

したい場合もあります。これは、**[管理（Administration）] > [サーバー プロパティ（Server Properties）]** タブで **[template.in_use.check]** オプションを切り替えることで実現できます。

Procedure

ステップ 1 **[template.in_use.check]** を **[true（デフォルト）]** から **[false]** に変更します。

ステップ 2 右上角にある [変更を適用（Apply Changes）] をクリックします。

DCNM の再起動が必要であることを示す警告がポップアップ表示されます。

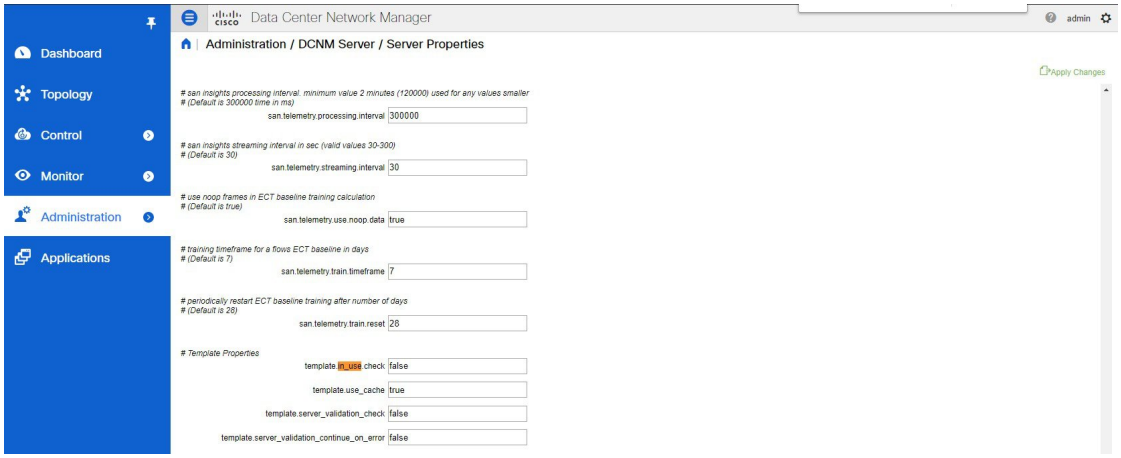
in_use フラグを有効にするために再起動する必要はないため、この警告は無視してください。

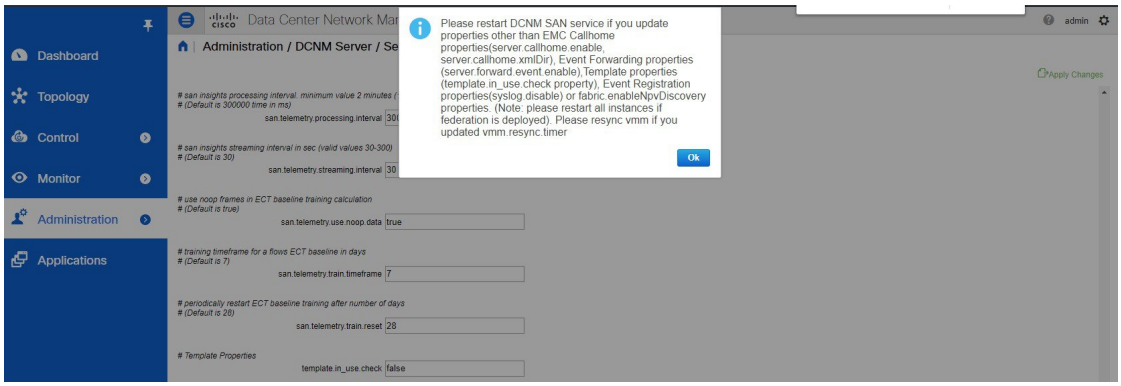
ステップ 3 目的のテンプレートを編集します。

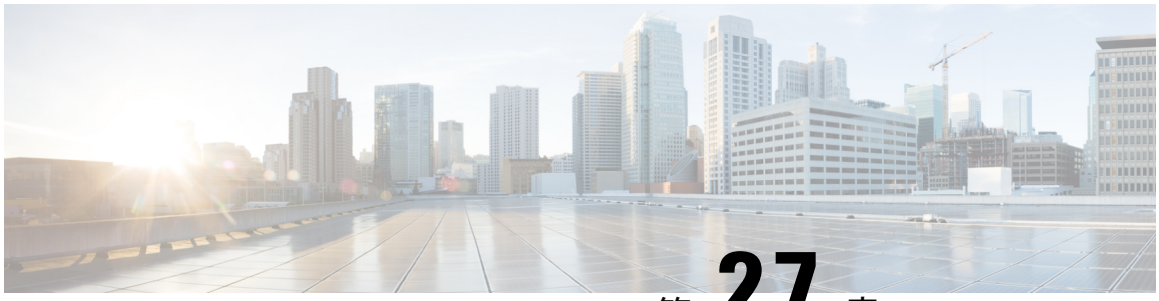
ステップ 4 ファブリック ビルダのページに移動し、ファブリック全体に対して [保存と展開（Save & Deploy）] をクリックします。

これにより PTI が再生成され、更新されたコンテンツが取得され、望む構成（またはインテント）に使用されます。

ステップ 5 コンテンツが再生成されて展開されたら、パフォーマンスの問題を回避するために、**[template.in_use.check]** を **[true]** に戻します。







第 27 章

プログラマブル レポートのガイドライン

前提条件

計画

1. レポートがファブリック全体またはデバイス全体に対して実行されることを意図しているかどうかを判断します。
2. 必要なデータを収集するために、どの **[show]** コマンドをスイッチで実行する必要があるかを調べます。
   - CLI 出力が xml または json をサポートしているか、どちらもサポートしていないかを調べます。
   - どちらでもない場合、スイッチはプレーンな CLI 出力を返します。
   - 実行されたコマンドを含む CLI 応答を elasticsearch に保存する必要があるかどうかを判断します。応答を保存すると、ストレージが大幅に増加する可能性があるため、注意が必要です。
3. 繰り返し、期間などのレポート作成入力を事前検証する必要があるかどうかを判断します。たとえば、レポート ジョブは定期的なレポートをサポートしていますか。また、ジョブはどのくらいの頻度で実行する必要がありますか。

レポートのプレゼンテーション

1. **サマリー**が必要な場合は、データを表示する形式を選択します。
   - キーと値のペア

- 表
- チャート（縦棒、円、折れ線）

2. **セクション**（詳細ビュー）で、データを表示する形式を選択します。
   - キーと値のペア
   - JSON オブジェクトの配列
   - チャート（縦棒、円、折れ線）
3. **フォーマッタ**の場合、以下が適用されます。
   - UI に表示される値にフォーマットを追加する
   - サポートされているマーカー：ERROR、SUCCESS、WARNING、INFO

レポート間のデータ比較

1. レポートで現在のレポートと古いレポートのデータを比較する必要があるかどうかを判断します。
2. 「はい」の場合、レポートインフラ API を使用すると、次のような以前のレポートを取得できます。
   - 1 つまたは複数の以前に生成されたレポート
   - レポート ジョブの最も古いレポート
   - 特定のレポートのサマリ
   - reportCLI 出力プロセスの特定のセクション

CLI 出力プロセス

XML形式

CLI 出力が XML 形式でデータを返す場合、レポートインフラストラクチャで提供される XML ユーティリティを使用して、XML データを読み取ることができます。

From reportlib.preport import *:

- getxmltree(xml_string, tag)
- getxmlrows(xml_tree, tag_xpath)
- getnodevalue(xml_tree, node_xpath)
- has_tag(xml_tree, tag)

例については、レポート テンプレート **switch_inventory** を参照してください。

[JSON 形式（JSON Format）]

CLI 出力が JSON 形式でデータを返す場合は、Python の json モジュールをインポートし、**json.loads()** メソッドを使用して JSON 文字列を解析します。

import json

json_string =<CLI response>

json_obj = json.loads(json_string)

例については、レポート テンプレート **fabric_nve_vni_counter** を参照してください。

プレーンな CLI 出力

CLI 出力が CLI UI に表示されるのと同じ形式でデータを返す場合、独自の解析メソッドを記述して、CLI 応答でデータを読み取る必要があります。

ロガー

Logger を使用すると、レポート テンプレートからメッセージをログに記録できます。ログに記録されたメッセージは、/usr/local/cisco/dcm/fm/logs/preport_jython.log に書き込まれます。

レポート テンプレート

テンプレートのプロパティ

次の必須テンプレート プロパティを指定します。

```
name = <template-name>;
tags = fabric or device;
userDefined = true or false;
templateType = REPORT;
templateSubType = GENERIC;
contentType = PYTHON;
```

（注）

- ファブリックに対してレポートが実行される場合は、**tags = Fabric** を設定します。デバイスに対してレポートが実行される場合は、**tags = device** を設定します。
- テンプレートがお客様によって作成された場合は、**userDefined = true** を設定します。テンプレートが DCNM 開発者によって作成された場合は、**userDefined = false** を設定します。

テンプレート変数

```
Specify the following template variables:
##template variables
@(IsInternal=true)
```

```
string fabric_name or serial_number;
string user_input;
```

（注）
- **tags = fabric** の場合、変数 *fabric_name* を構成します
- **tags = device** の場合、変数 *serial_number* を構成します
- ユーザー変数はオプションです。DCNM テンプレート インフラでサポートされているすべてのデータ タイプと注釈を使用できます。

テンプレートの内容

インポート済みライブラリ

次の 2 つの Python ライブラリが必要です。**reportlib.preport** には、すべてのレポート インフラストラクチャ API が含まれていることに注意してください。

```
##template content
from com.cisco.dcbu.vinci.rest.services.jython import WrappersResp
from reportlib.preport import *
```

テンプレート関数

generateReport()

generateReport() は入力関数であり、レポートの生成中に呼び出されます。すべてのレポート導入ロジックをここに提供する必要があります。この関数は、コンテキスト オブジェクトを受け取ります。「コンテキスト」パラメータは、レポート ジョブの作成時にレポート インフラストラクチャによって作成されます。

```
def generateReport(context):

    report = Report("Report title")   ## Create a report object
     ## Gather data and fill in content for the report

    respObj = WrappersResp.getRespObj()
    respObj.setSuccessRetCode()
    respObj.setValue(report)
    return respObj
```

（注）
- この関数は WrappersResp オブジェクトを返す必要があります。
- レポートの生成にエラーがない場合、この関数内で作成されたレポート オブジェクトは、**WrappersResp** オブジェクトが返される前に **WrappersResp.setValue()** で設定する必要があります。

CLI を実行し、CLI 応答を処理する

以下は、1 つまたは複数のデバイスに **show** コマンドを送信する方法、およびデバイスからの応答を処理する方法に関するサンプル コードです。

```
show_cmd1 = 'show xxx'
show_cmd2 = 'show yyy'
device_list = [device1,device2]
## run the command(s) on each device in the device_list


cli_responses = show(device_list, show_cmd1, show_cmd2)
## run the command(s) on each device in the device_list and store the CLI response(s)

cli_responses = show_and_store(device_list, show_cmd1, show_cmd2)
```

For resp in cli_responses:

```
command = resp['command'].strip()

    if show_cmd1 in command:
        cmd1_response = resp['response'].strip()
        ## process show_cmd1 response

    elif show_cmd2 in command:
        cmd2_response = resp['response'].strip()
        ## process show_cmd1 response
```

validate()

validate() 関数はオプションの関数であり、繰り返し、期間などのレポート作成入力の事前検証を実行するために使用されます。この関数が定義されている場合、レポートジョブの作成中に呼び出されます。レポート ジョブは、この関数が SuccessRetCode で WrappersResp を返す場合にのみ作成されます。検証が失敗した場合、エラーを含むFailureRetCodeを持つWrappersRespが返されます。

```
def validate(context):
    respObj = WrappersResp.getRespObj()
    ## Validation content

    if validation_failed:
        respObj.addErrorReport(…)
        respObj.setFailureRetCode()
    else:
        respObj.setSuccessRetCode()
    return respObj
```

report.add_summary

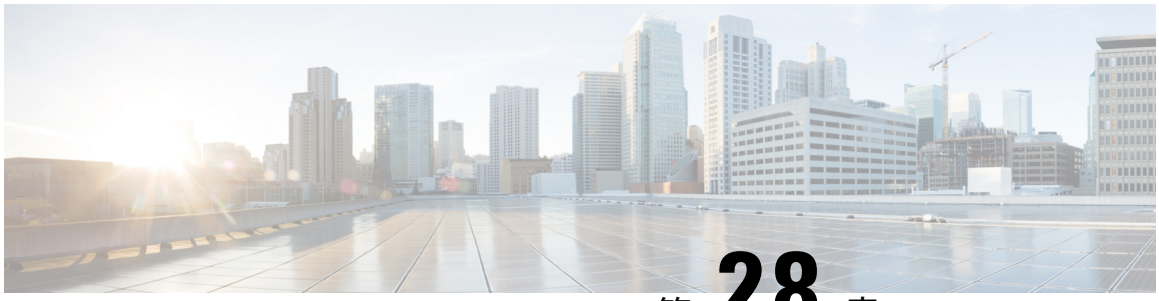
各レポートには1つのサマリを含めることができ、コンテンツはPythonディクショナリです。

```
summary = report.add_summary()
summary[key] = value
summary.add_message(msg)
## Present the summary in a table format

table = summary.add_table(title,_id)   ## _id must be a unique id for the table
table.append(value,_id)   ## adding rows to table
## Present the summary in a chart format

chart = summary.add_chart(ChartType,_id)
## ChartTypes: ChartTypes.COLUMN_CHART, ChartTypes.PIE_CHART, ChartTypes.LINE_CHART
```

report.add_section

セクションは、レポート コンテンツの論理グループです。セクションの詳細は、**[詳細の表示（View Details）]** に表示されます。

```
section = report.add_section(title,_id)   ## _id must be a unique id for the section
section[key] = value
section.append(key, json_obj, _id)   ## adding rows of json objects to section
## Present the section details in a chart format

chart = section.add_chart(ChartType,_id)
## ChartTypes: ChartTypes.COLUMN_CHART, ChartTypes.PIE_CHART, ChartTypes.LINE_CHART
```



第 28 章

Cisco DCNM プログラマブル レポート API

テンプレート

Cisco DCNM リリース 11.4(1) では、新しいテンプレート タイプ「REPORT」が 2 つのサブタイプ、UPGRADE および GENERIC とともに追加されています。テンプレート タイプは python であり、「generateReport」メソッドの実装を提供する必要があります。

アップグレード

UPGRADE テンプレートは、ISSU の前後の ISSU 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。

GENERIC

GENERIC テンプレートは、一般的なレポート目的で使用できます。たとえば、インベントリ レポートの収集です。

テンプレート構造

次の図は、テンプレート構造の例を示しています。

```
##template variables


@(IsInternal=true)
String serial_number/fabric_name;

String user_input;

##
##template content


from com.cisco.dcbu.vinci.rest.services.jython import WrappersResp
from reportlib.preport import *

def validate(context):

    respObj = WrappersResp.getRespObj()
    respObj.setSuccessRetCode()
    return respObj


def generateReport(context):

    report = Report("Report title")

    ##Report content

    respObj = WrappersResp.getRespObj()
    respObj.setSuccessRetCode()
    respObj.setValue(report)
    return respObj
##
```

serial_number or fabric_name based on the scope selected while scheduling the report. In case of UPGRADE report, always serial number will be injected

Template variable section. **All data types, annotations supported in DCNM template can be used here. User should provide these inputs while creating the report

Import necessary python lib.

Report can have optional validation method, This method will be invoked while creating the report job. Job will be created only if this method return success. This method is invoked only once and serial_number or fabric_name will not be available inside this method. More information check the API guide

report must provide implementation of generateReport(context) method.

generateReport method should return an object of type WrapperResp. Report object created above must be stored in wrappersResp using wrappersResp.setValue() API

テンプレート機能

generateReport メソッド

レポートの生成中に generateReport メソッドが呼び出されます。すべてのレポート導入ロジックを提供する必要があります。このメソッドは、コンテキストオブジェクトを受け入れます。前述のように、このメソッドは WrappersResp オブジェクトを返す必要があります。

検証メソッド

検証メソッドはオプションです。テンプレートでこのメソッドが定義されている場合、レポートアプリケーションはこのメソッドを呼び出して、ジョブの作成中に事前検証を実行します。このメソッドは、選択されたデバイスまたはファブリックに関係なく、ジョブが作成され、1回だけ呼び出された場合にのみ呼び出されます。

検証を通過した場合、このメソッドは WrappersResp を SuccessRetCode とともに返し、失敗の場合は FailureRetCode をエラー リストのエラーとともに返す必要があります。

次に例を示します。

検証に失敗しました

```
def validate (context):
```

```
    respObj = WrappersResp.getRespObj()

    ## Validation logic here

    respObj.setFailureRetcode()
    respObj.addErrorReport(template_name,error)
    return respObj
```

検証に成功しました

```
def validate (context):
    respObj = WrappersResp.getRespObj()

    ## Validation logic here

    respObj.setSuccessRetcode()
    return respObj
```

コンテキスト パラメータの内容に基づいて検証を実行できます。

コンテキスト パラメータ

コンテキスト パラメータは、次の属性で構成されます。

1. ユーザ名：ジョブを作成したユーザの名前
2. ユーザーロール：ジョブを作成したユーザのロール
3. Job ID
4. 再発：現在、1 回、毎日、毎週、毎月、オンデマンド、または定期
5. 期間：繰り返しが定期的である場合、期間には頻度が選択されます。たとえば、10 分です。

これらの値をコンテキストから読み取るには、「ジョブ コンテキスト情報の取得」で説明されている API を参照してください。

レポート レイアウト

レポートには次のコンポーネントがあります。

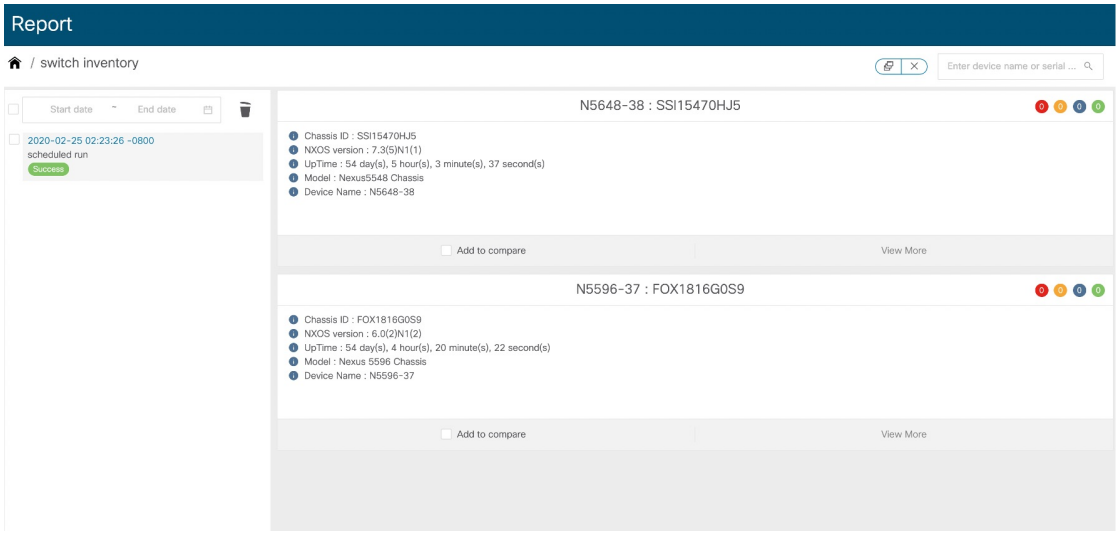
1. 要約
    1. キーと値
    2. メッセージ – 推論
2. 詳細/セクション
    1. キーと値
    2. JSON ドキュメント – カード

3. JSON ドキュメントの配列 – テーブル

3. コマンド ログ

一覧ビュー

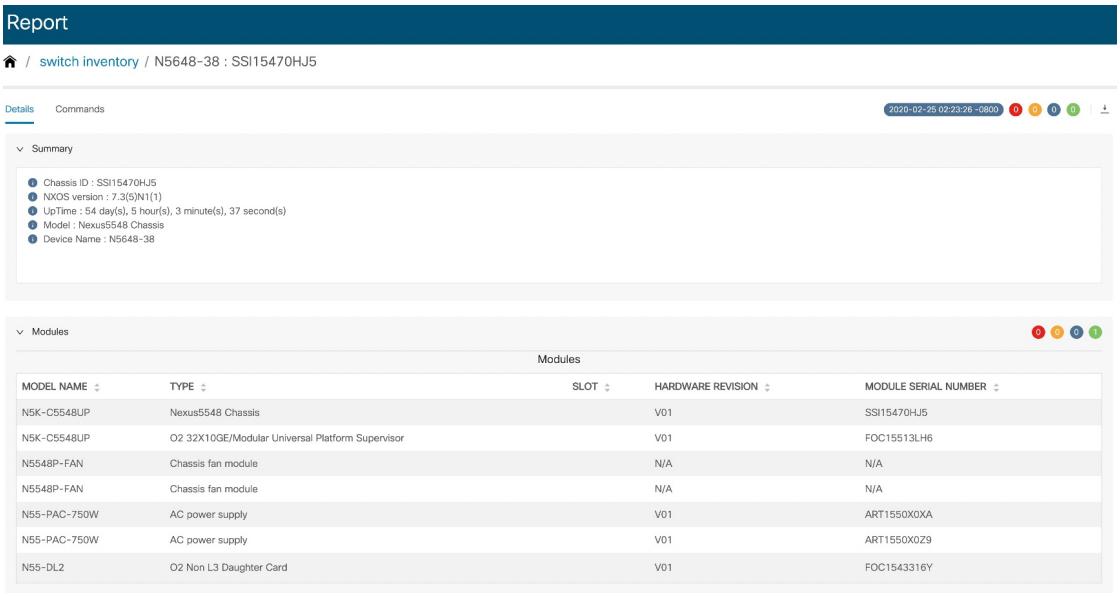
このビューには、レポートに含まれる各エンティティのサマリが表示されます。



詳細ビュー

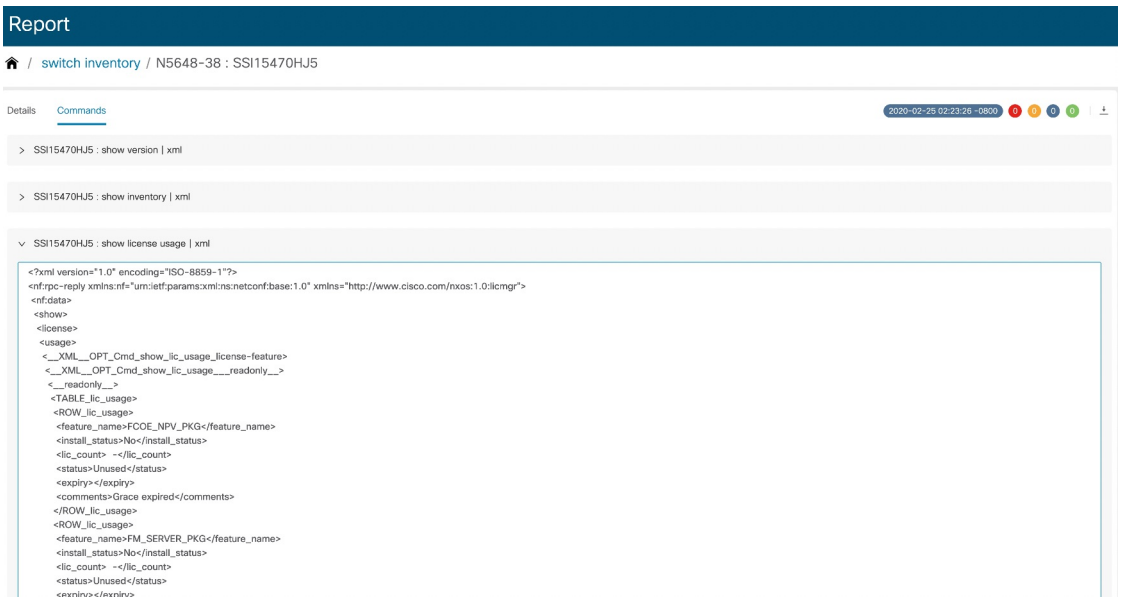
詳細表示には、サマリとともに完全なレポート JSON データが表示されます。レポートの詳細は、論理的にセクションにグループ化されます。各セクションは、折りたたみ可能なウィジェットで個別に表示されます。

サマリ表示と詳細表示の両方で、レポートで生成されたエラー、警告、情報、成功メッセージの数が表示されます。



コマンド ログ

コマンド ログには、コマンドの実行に使用された API に基づいて、レポートで実行されたすべてのコマンドが含まれます。



レポート Python ライブラリ

レポートインフラストラクチャは、レポートJSONモデルを生成するための使いやすく軽量なPython ライブラリを提供します。この API を使用するには、テンプレートに次のインポートステートメントを追加する必要があります。

```
from reportlib.preport import Report
```

レポート API

レポート オブジェクトの作成

すべてのレポートは、最初のステップとして「レポート」オブジェクトを作成する必要があります。

```
report = Report (“Report title”)
```

サマリの追加

すべてのレポートには1つのサマリを含めることができ、それはPythonディクショナリです。サマリは次のように追加できます。

```
summary = report.add_summary()
```

サマリへのコンテンツの追加

キーと値

```
summary [‘NXOS Version’] = ‘8.1(0)’
```

メッセージ – 推論

```
summary.add_message (“Simple message”)
```

（注） DCNM 11.4(1) では、DCNM はサマリの値として JSON オブジェクトをサポートしていません。次の例はサポートされていません。

```
summary[“info”] = {“key”:”value”,”key-2”:”value-2”}
```

サマリのテーブル

```
table = summary.add_table(title,_id)
```

- title：テーブルのタイトル
- _id：テーブルの一意の識別子

テーブルへの行の追加

```
table.append(value, _id)
```

- value：JSON オブジェクトです。ネストされた JSON はサポートされません。

- _id : テーブルの一意の識別子

例：

```
table.append({'column1': 'value1','column2’:’value2’},” FOX1816G0S9”)
```

セクションの追加

セクションは、レポートの内容を論理的にグループ化したものです。ユーザの判断により、これらのセクションを作成し、表示する情報を追加します。

セクションは次のように追加できます。

```
section = report.add_section (“Section title”,_id)
```

- _id : テーブルの一意の識別子
- セクション : ディクショナリです

セクションへのコンテンツの追加

キーと値

以下に示すように、単純なキーと値のペアをセクションに追加できます。

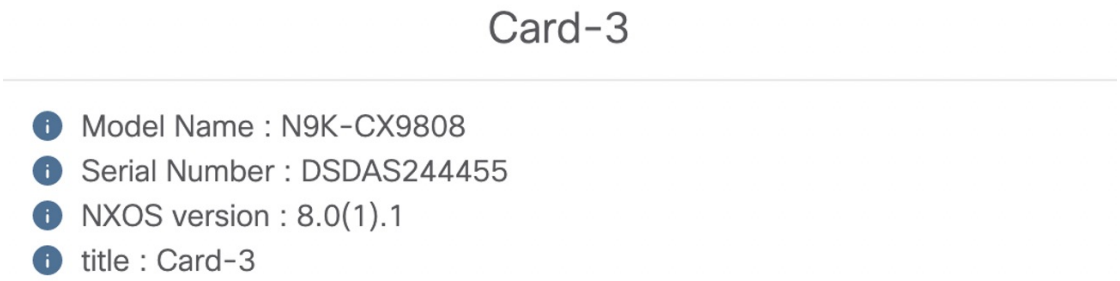
```
section[‘key’] = ‘value’
```

JSON ドキュメント – カード

任意のキーと値のペアと同じように、単一の JSON ドキュメントを追加できます。ネストされた JSON は 11.4(1) ではサポートされていません

```
section[‘key’] = {‘key’:’value’,’key-2’:’value’}
```

JSON ドキュメントは、次のようにカード ウィジェットに表示されます。



JSON ドキュメントの配列 – テーブル

section.append API を使用すると、ユーザはテーブルを作成し、行を追加できます（次の制限が付きます）。

1. すべての JSON ドキュメントには同じキーのセットが必要です
2. ネストされた JSON はサポートされません

```
section.append(key, dictionary, _id)
```

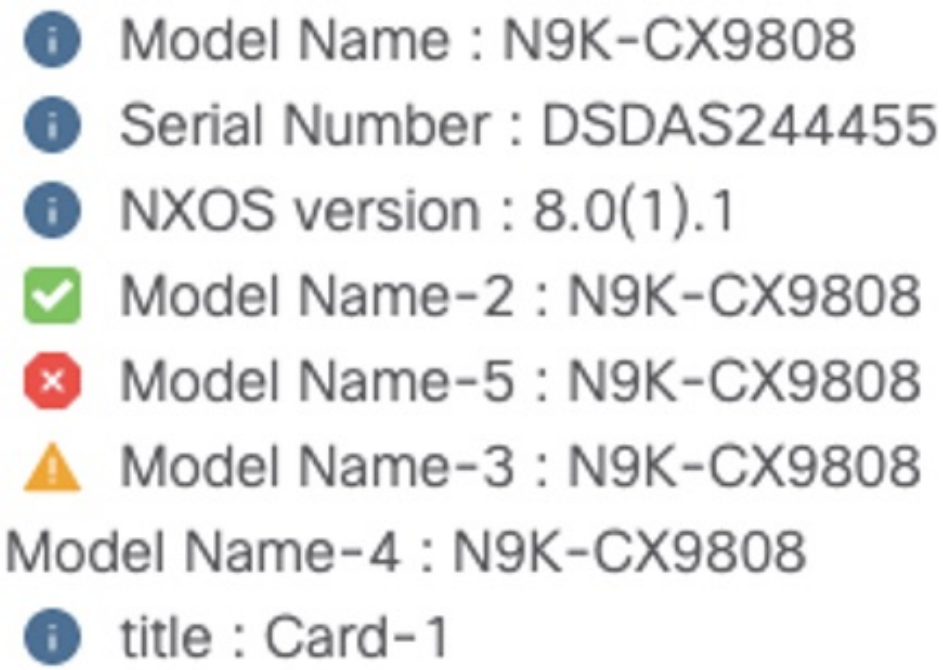
_id：テーブルの行を一意に識別する一意の識別子。_idが重複すると、一意のid違反エラーが発生します。

例：

```
section.append('Switch Details', {'name': 'N5K'},'DSDAS244455')
section.append('Switch Details', {'name': 'N6K'}, 'CSDAS244456')
section.append('Switch Details', {'name': 'N7K'}, 'ASDAS244457')
```

Formatters

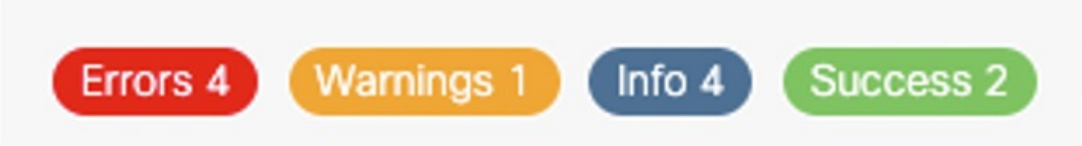
Formatter を使用すると、UI に表示される値に追加のフォーマットを追加できます。



示されているように、値を次のようにマークできます。

1. エラー
2. 成功
3. 警告
4. INFO

これらのマーカーをレポートに追加すると、対応するカウントエラー、警告、成功、情報がUI に表示されるように自動的に更新されます。




```
Formatter.add_marker(value,marker)
```

- value：マーカーを追加する値。
- マーカー：Marker.ERROR,Marker.SUCCESS,Marker.WARNING,Marker.INFO

例：

```
Formatter.add_marker (“NXOS version”,Marker.INFO)
```

グラフ

レポートは、サマリとセクションの両方でのグラフの追加をサポートしています。

サマリへのチャートの追加

```
report = Report(“title”)
summary = report.add_summary()
summary.add_chart(ChartType, _id)
```

- **ChartType**: ChartTypes.COLUMN_CHART, ChartTypes.PIE_CHART, ChartTypes.LINE_CHART.
- **_id**：チャートの一意の ID

セクションへのグラフの追加

```
report = Report(“title”)
section = report.add_section(“Section title”,_id)
section.add_chart(ChartType, _id)
```

- **ChartType**: ChartTypes.COLUMN_CHART, ChartTypes.PIE_CHART, ChartTypes.LINE_CHART
- **_id**：チャートの一意の ID

円グラフ

設定とサブタイトルのタイトル

```
pie_chart.set_title("Chart title")
pie_chart.set_subtitle(“Sub title”)
```

付加価値を加えてください。

```
pie_chart.add_value("key",value)
```

- キー：文字列キー
- 値：数字の値

縦棒グラフ

設定とサブタイトルのタイトル

```
column_chart.set_title("Chart title")
column_chart.set_subtitle(“Sub title”)
```

X 軸と Y 軸のタイトルを設定する

```
column_chart.set_xAxis_title("X-Axis title")
column_chart.set_yAxis_title("y-Axis title")
```

値の追加

```
bar_chart.add_value("key",value,category)
```

- キー：文字列キー
- 値：数字の値
- カテゴリ：棒グラフは、データを「カテゴリ」と呼ばれる論理グループに分割します。指定されたキーには、各カテゴリの値が必要です。

たとえば、デバイス数がキーで、ファブリック名がカテゴリです。チャートには、ファブリックごと、つまりカテゴリごとにデバイス数が含まれている必要があります。

折れ線グラフ

設定とサブタイトルのタイトル

```
line_chart.set_title("Chart title")
line_chart.set_subtitle(“Sub title”)
```

X 軸と Y 軸のタイトルを設定する

```
line_chart.set_xAxis_title("X-Axis title")
line_chart.set_yAxis_title("y-Axis title")
```

値の追加

```
line_chart.add_value("key",value,category)
```

- キー：文字列キー
- 値：数字の値
- カテゴリ：折れ線グラフは、データをカテゴリと呼ばれる論理グループに分割します。指定されたキーには、各カテゴリの値が必要です。

たとえば、デバイス数がキーで、ファブリック名がカテゴリです。チャートには、ファブリックごと、つまりカテゴリごとにデバイス数が含まれている必要があります。

デバイスでの CLI の実行

コマンドの表示

```
from reportlib.preport import show
cli_responses = show (serial_number ,*commands)
```

- serial_number：コマンドを実行するデバイスのシリアル番号。VDC の場合、シリアル番号は serial_number:vdc_name である必要があります。シリアル番号のリストを渡して、複数のデバイスで同じコマンド セットを実行できます。
- *commands：デバイスで実行するコマンド。可変引数です。複数のコマンドを指定できます。

例：

- 単一のスイッチでコマンドを実行する：

  ```
  cli_responses = show(“FOX1816G0S9”,'show version | xml', 'show inventory | xml',
  'show license usage | xml')
  ```

- 複数のスイッチでコマンドを実行する：

  ```
  cli_responses = show( [“FOX1816G0S9”,”SSI15470HJ5”],'show version | xml', 'show
  inventory | xml', 'show license usage | xml')
  ```

コマンドの表示と応答の保存

```
from reportlib.preport import show_and_store
cli_responses = show_and_store(report,serial_number,*commands)
```

report：レポート オブジェクトが作成されました。

serial_number：コマンドを実行するデバイスのシリアル番号。VDC の場合、シリアル番号は serial_number:vdc_name である必要があります。シリアル番号のリストを渡して、複数のデバイスで同じコマンド セットを実行できます。

*commands：デバイスで実行するコマンド。可変引数です。複数のコマンドを指定できます。

例：

- 単一のスイッチでコマンドを実行する：

  ```
  cli_responses = show_and_store(report, “FOX1816G0S9”, 'show version | xml', 'show
  inventory | xml', 'show license usage | xml')
  ```

- 複数のスイッチでコマンドを実行する：

  ```
  cli_responses = show_and_store(report, [“FOX1816G0S9”,”SSI15470HJ5”], 'show version
   | xml', 'show inventory | xml', 'show license usage | xml')
  ```

注意：この API は、デバイスからの応答をレポートとともに elasticsearch に保存します。すべての応答を保存するとストレージが大幅に増加する可能性があるため、ユーザはこの API を使用する際に注意する必要があります。

戻り値

戻り値 API は応答のリストを返し、各応答は次の構造を持つディクショナリです。

```
{
 'status': 'success' | 'failed,
 'response':<response from device>,
 'command':<cli command>,
 'serial_number': <device serial number>
}
```

複数のスイッチの場合、応答はスイッチごとのエントリを含む応答のリストです。

```
[
{
 'status': 'success',
 'response':<response from device>,
 'command':'show version',
 'serial_number': 'FOX1816G0S9'
},
{
 'status': 'success',
 'response':<response from device>,
 'command':'show version',
 'serial_number': 'SSI15470HJ5
}
]
```

ジョブ コンテキスト情報の取得

APP からジョブをスケジュールしているときに選択された繰り返しを取得します

```
get_recurrence(context)
```

この API は、ジョブの作成中に選択された繰り返しを返します。戻り値は、NOW、ONCE、DAILY、WEEKLY、MONTHLY、ONDEMAND、および PERIODIC です。

get_period

ジョブが定期的にスケジュールされている場合、API を使用して期間情報にアクセスできます。

```
period = get_period(context)
period.get_period() will return the period
period.get_time_unit() will return time Unit (HOURS, MINUTES)
```

履歴レポートの分析

以前に生成されたレポートの取得

「get_previous_reports()」メソッドを使用すると、過去に生成されたレポートを取得できます。これは、現在のデータと履歴データに基づいて分析を実行するために使用できます。この API は、作成された時間の降順でレポートを返します。

```
List of reports = get_previous_reports (context,entity,count)
```

この API は、レポートのリストを返します。

コンテキスト：generateReport(context) メソッドから入力として受け取ったオブジェクト

エンティティ：serial_number またはファブリック名

カウント：取得するレポートの数

最も古いレポートを取得

```
oldest_report = get_oldest_report(context,entity)
```

コンテキスト：generateReport(context) メソッドから入力として受け取ったオブジェクト

エンティティ：serial_number またはファブリック名

上記の API はどちらも、情報を取得するために次の API を使用して Report オブジェクトを返します。

1. **概要を取得する**：report.get_summary()
2. **セクションの取得**：report.get_section(_id)

```
report.get_section(_id)
```

_id：セクションの一意の識別子

XML ユーティリティ

XML ツリーを取得

```
from reportlib.preport import getxmltree
xml_element_tree = getxmltree(xml_string,tag)
```

この API は、指定されたタグの下にある XML ツリーを返します。

xml_string：デバイスからの XML 応答。

タグ：XML タグ。このタグの下の完全な XML は、ElementTree として返されます。

xml_element_tree：この API は xml.etree.ElementTree オブジェクトを返します。

XML 行を取得する

CLI 応答に行がある場合、getxmlrows API を使用して行の配列を取得できます。

```
from reportlib.preport import getxmlrows
rows = getxmlrows(xml_tree,tag_xpath)
```

xml_tree：xml.etree.ElementTree オブジェクト

tag_xpath：XML レコードの xpath。詳細については、https://docs.python.org/2/library/xml.etree.elementtree.html#xpath-support を参照してください。

行：行の配列

ノード値を取得

XML ノード値は、**getnodevalue** API を使用して読み取ることができます。この API は、プリミティブ型のノード値を取得するために使用する必要があります。

```
from reportlib.preport import getnodevalue
value = getnodevalue(xml_tree,node_xpath)
```

ノードが存在するかどうかを確認する

```
from reportlib.preport import has_tag
has_tag(xml_tree,tag)
```

この API は、指定されたタグが XML ツリーに存在するかどうかに基づいて true または false を返します。

WrapperResp

すべてのレポートは、WrapperResp タイプのオブジェクトを返す必要があります。

WrapperResp は次のようにインスタンス化できます。

```
respObj = WrappersResp.getRespObj()
```

WrapperResp のリターン コードは、レポートが正常に実行されたかどうかを示します。

1. すべてのコマンドが実行され、必要な情報が抽出された場合、レポートは成功 **respObj.setSuccessRetCode()** を返します。
2. コマンドの失敗などの例外が発生した場合、レポートは失敗 **respObj.setFailureRetCode()** を返します。
3. エラーの場合、エラーの理由を **respObj.addErrorReport(template_name,error_message)** として追加できます。

Report セクションで作成されたレポート オブジェクトは、次のように WrappersResp の値に設定する必要があります。

```
respObj.setValue(report)
```

Logger

Logger を使用すると、レポート テンプレートからメッセージをログに記録できます。Logger を使用して記録されたすべての情報
は、`/usr/local/cisco/dcm/fm/logs/preport_jython.log`に記録されます。

```
Logger.info(“message”)
Logger.debug(“message”)
Logger.error(“message”)
Logger.trace(“message”)
Logger.warn(“message”)
```

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。