ブラウンフィールド VXLAN BGP EVPN ファブリックの管理

概要

このユースケースは、既存の VXLAN BGP EVPN ファブリックを Cisco NDFC に移行する方法を示しています。移行には、既存のネットワーク設定の Nexusダッシュボード ファブリック コントローラ への移行が含まれます。

通常、ファブリックは手動の CLI 構成またはカスタム自動化スクリプトによって作成および管理されます。これで、Nexusダッシュボード ファブリック コントローラ でファブリックの管理を開始できるようになりました。移行後、ファブリック アンダーレイとオーバーレイ ネットワークは NDFC によって管理されます。

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

前提条件

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

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

注意事項と制約事項

- すべてのスイッチをNDFCファブリックに追加して、ファブリック全体に対してブラウンフィールド インポートを完了する必要があります。
- **[ファブリックの作成（Create Fabric）]** ウィンドウで、**[詳細設定（Advanced）]** > **[オーバーレイ モード（Overlay Mode）]**ファブリック設定で、オーバーレイの移行方法を決定します。デフォルトの config-profile が設定されている場合、VRF およびネットワーク オーバーレイ構成プロファイルは、移行プロセスの一部としてスイッチに展開されます。さらに、重複するオーバーレイ CLI 構成の一部を削除するための diffs 機能があります。これらはネットワークに影響を与えません。
- **CLI が設定されている場合、[オーバーレイ モード（Overlay Mode）]** ドロップダウン リストからの VRF およびネットワーク オーバーレイの構成は、整合性の違いに対応するための変更をまったく、またはほとんど行うことなく、そのままスイッチに残されます。
- NDFC のブラウンフィールド インポートは、簡素化された NX-OS VXLAN EVPN 構成 CLI をサポートします。詳細については、Cisco Nexus 9000 シリーズ NX-OS VXLAN 構成ガイド、リリース 10.2(x) を参照してください。
- 次の機能はサポートされていません。
  - スーパー スパイン ロール
  - ToR
  - eBGP アンダーレイ
  - レイヤ 3 ポートチャネル
  - vPC ファブリック ピアリング
- 移行前に、スイッチ構成のバックアップを取り、保存します。
- 移行が完了するまで、スイッチの構成を変更してはなりません（このドキュメントで指示されている場合を除く）。変更すると、重大なネットワークの問題が発生する可能性があります。
- Cisco Nexusダッシュボード ファブリック コントローラ への移行は、Cisco Nexus 9000 スイッチでのみサポートされています。
- ボーダー スパインとボーダー ゲートウェイ スパインのロールは、ブラウンフィールド移行でサポートされています。
- まず、設定を更新する際のガイドラインについての注意を述べます。次に、各 VXLAN ファブリック設定タブについて説明します。

- 一部の値（BGP AS 番号、OSPF など）は、既存のファブリックへの基準ポイントと見なされるので、入力する値は既存のファブリックの値と一致させる必要があります。
- 一部のフィールド（IPアドレス範囲、VXLAN ID範囲など）の場合、自動入力または設定で入力された値は、将来の割り当てにのみ使用されます。移行中は、既存のファブリック値が優先されます。
- 一部のフィールドは、既存のファブリックに存在しない可能性のある新しい機能（advertise-pip など）に関連しています。必要に応じて有効または無効にします。
- ファブリックの移行が完了した後で、必要に応じて設定を更新できます。

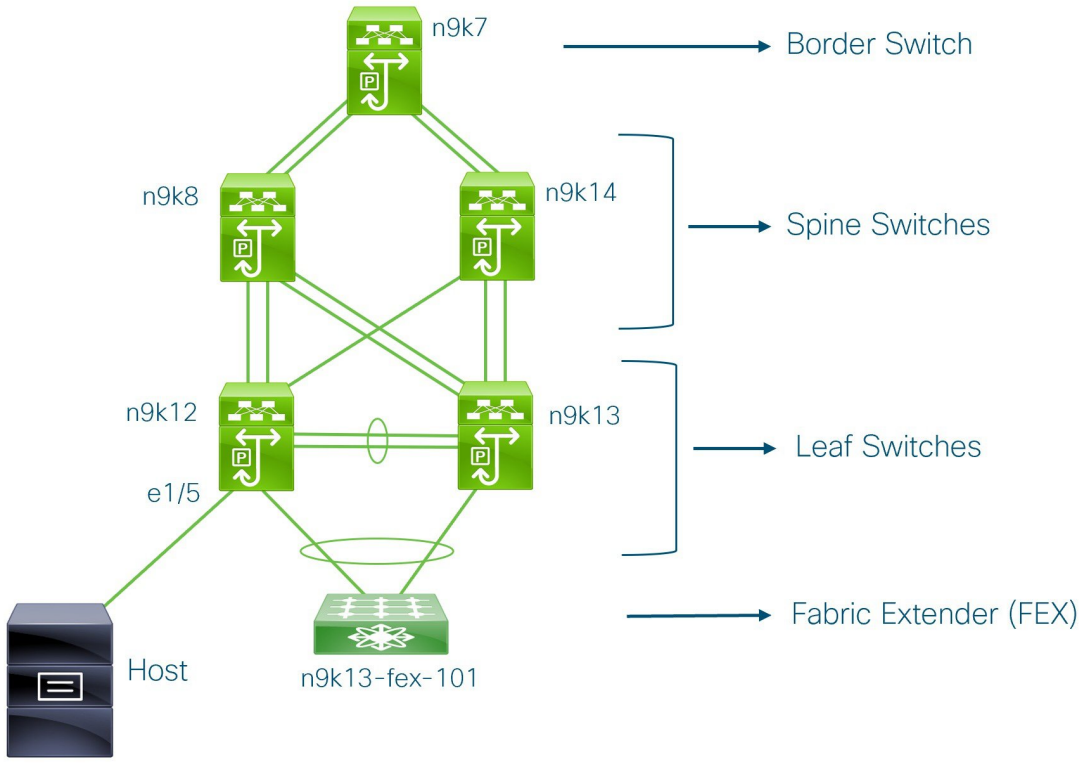
ファブリック トポロジの概要

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

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

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

既存のファブリックの移行を開始する前に、そのトポロジを見てみましょう。



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

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

NDFC ブラウンフィールド展開タスク

ブラウンフィールド移行には、次のタスクが含まれます。

1. 既存の VXLAN BGP EVPN ファブリックの確認 （5 ページ）
2. 新規 VXLAN BGP EVPN ファブリックの作成
3. スイッチの追加と VXLAN ファブリック管理の NDFC への移行 （30 ページ）

既存の VXLAN BGP EVPN ファブリックの確認

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

Procedure

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

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

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

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

ステップ 2 vPC の整合性と障害を確認します。

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

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

ステップ 3 **n9k-12** スイッチの EVPN ネイバーを確認します。

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

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

スパイン スイッチに対応する 2 つのネイバーがあることがわかります。

ASN が 65000 であることに注意してください。

ステップ 4 VRF 情報を確認します。

```
n9k12# show run vrf internet

!Command: show running-config vrf Internet
```

```
!Running configuration last done at: Fri Aug  9 01:38:02 2019
!Time: Fri Aug  9 02:48:03 2019

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

interface Vlan347
  vrf member Internet

interface Vlan349
  vrf member Internet

interface Vlan3962
  vrf member Internet

interface Ethernet1/25
  vrf member Internet

interface Ethernet1/26
  vrf member Internet
vrf context Internet
  description Internet
  vni 16777210
  ip route 204.90.141.0/24 204.90.140.129 name LC-Networks
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
router ospf 300
  vrf Internet
    router-id 204.90.140.3
    redistribute direct route-map allow
    redistribute static route-map static-to-ospf
router bgp 65000
  vrf Internet
    address-family ipv4 unicast
      advertise l2vpn evpn
```

VRF **インターネット**は、このスイッチで構成されています。

n9k-12 スイッチに接続されているホストは、VRF **インターネット**の一部です。

この VRF に関連付けられた VLAN を表示できます。

具体的には、ホストは **Vlan349** の一部です。

ステップ 5 レイヤ 3 インターフェイス情報を確認します。

```
n9k12# show run interface vlan349

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

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

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

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

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

```
n9k12# show run interface ethernet1/5

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

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

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

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

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

```
host# ping 204.90.140.134 count unlimited interval 1
PING 204.90.140.134 (204.90.140.134): 56 data bytes
64 bytes from 204.90.140.134: icmp_seq=0 ttl=254 time=1.078 ms
64 bytes from 204.90.140.134: icmp_seq=1 ttl=254 time=1.129 ms
64 bytes from 204.90.140.134: icmp_seq=2 ttl=254 time=1.151 ms
64 bytes from 204.90.140.134: icmp_seq=3 ttl=254 time=1.162 ms
64 bytes from 204.90.140.134: icmp_seq=4 ttl=254 time=1.84 ms
64 bytes from 204.90.140.134: icmp_seq=5 ttl=254 time=1.258 ms
64 bytes from 204.90.140.134: icmp_seq=6 ttl=254 time=1.273 ms
64 bytes from 204.90.140.134: icmp_seq=7 ttl=254 time=1.143 ms
```

既存のブラウンフィールド ファブリックを Nexusダッシュボード ファブリック コントローラに移行する間、ping コマンドをバックグラウンドで実行させます。

新規 VXLAN BGP EVPN ファブリックの作成

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

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

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

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

2. ファブリックの一意の名前を入力します。

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

使用可能なすべてのファブリック テンプレートのリストが表示されます。

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

   [選択（Select）] をクリックします。

   ファブリックを作成するために必要なフィールド値を入力します。

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

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

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

   [BGP ASN]：ファブリックが関連付けられている BGP AS 番号を入力します。これは、既存のファブリックと同じである必要があります。

   [IPv6 アンダーレイの有効化（Enable IPv6 Underlay）]：IPv6 アンダーレイ機能を有効にします。詳細については、Easy ファブリックの IPv6 アンダーレイ サポートを参照してください。

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

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

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

   [アンダーレイ サブネット IPv6 マスク（Underlay Subnet IPv6 Mask）]：ファブリック インターフェイスの IPv6 アドレスのサブネットマスクを指定します。

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

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

スパインデバイスを RR として展開するには、スパインデバイスをシリアル番号に基づいてソートし、2 つまたは 4 つのスパイン デバイスを RR として指定します。Nexusダッシュボード ファブリック コントローラスパイン デバイスを追加しても、既存の RR 設定は変更されません。

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

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

a. ドロップダウンボックスの値を 2 に変更します。

b. ルート リフレクタとして指定するスパイン スイッチを特定します。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   [アンダーレイ エニーキャスト ループバック ID（Underlay Anycast Loopback Id）]：ループバック インターフェイス ID はグレー表示され、VXLANv6 ファブリックの vPC ピアリングにのみ使用されます。

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

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

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

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

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

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

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

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

[IS-IS ネットワーク ポイントツーポイントの有効化（Enable IS-IS Network Point-to-Point）]：番号付きのファブリック インターフェイスでネットワーク ポイントツーポイントを有効にします。

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

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

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

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

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

[IS-IS オーバーロード ビットの設定（Set IS-IS Overload Bit）]：有効にすると、リロード後の一定時間、オーバーロード ビットを設定します。

[IS-IS オーバーロード ビットの経過時間（IS-IS Overload Bit Elapsed Time）]：経過時間（秒）の後にオーバーロード ビットをクリアできます。

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

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

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

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

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

[PIM Hello 認証の有効化（Enable PIM Hello Authentication）]：ファブリック内のスイッチのすべてのファブリック内インターフェイスで PIM hello 認証を有効にするには、このチェックボックスをオンにします。このチェックボックスは、マルチキャスト レプリケーション モードでのみ編集できます。このチェックボックスは、IPv4 アンダーレイに対してのみ有効です。

[PIM Hello 認証キー（PIM Hello Authentication Key）]：PIM hello 認証キーを指定します。詳細については、「PIM Hello 認証キーの取得」を参照してください。

PIM Hello 認証キーを取得するには、次の手順を実行します。

a. スイッチに SSH 接続します。

b. 未使用のスイッチインターフェイスで、次を有効にします。

```
switch(config)# interface e1/32
switch(config-if)# ip pim hello-authentication ah-md5 pimHelloPassword
```

この例では、pimHelloPassword が使用されたクリアテキスト パスワードです。

c. show run interface コマンドを入力して、PIM hello 認証キーを取得します。

```
switch(config-if)# show run interface e1/32 | grep pim
ip pim sparse-mode
ip pim hello-authentication ah-md5 3 d34e6c5abc7fecf1caa3b588b09078e0
```

この例では、d34e6c5abc7fecf1caa3b588b09078e0 がファブリック設定で指定される PIM hello 認証キーです。

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

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

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

```
feature bfd
```

BFD機能の互換性については、それぞれのプラットフォームのマニュアルを参照してください。サポートされているソフトウェアイメージについては、「Compatibility Matrix for Cisco」を参照してください。*Nexus*ダッシュボード ファブリック コントローラ

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

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

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

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

BFD グローバル ポリシーの例を次に示します。

```
router ospf <ospf tag>
   bfd

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

ip pim bfd

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

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

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

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

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

BFD 認証パラメータを取得する方法について。.

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

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

構成例では、パスワード 3 の後に 3DES パスワードが表示されます。

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

次のフィールドを使用して、さまざまな構成を指定できます。

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

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

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

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

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

[オーバーレイ モード（Overlay Mode）]：config-profile または CLI を使用した VRF/ネットワーク構成です。デフォルトは config-profile です。詳細については、オーバーレイモードを参照してください。

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

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

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

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

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

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

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

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

変数	説明
$$VNI$$	スイッチ構成で検出されたネットワーク VNI ID を指定します。これは、一意のネットワーク名を作成するために必要な必須キーワードです。

変数	説明
$$VLAN_ID$$	ネットワークに関連付けられた VLAN ID を指定します。 VLAN ID はスイッチに固有であるため、ネットワークが検出されたスイッチの 1 つから VLAN ID をランダムに選択し、名前に使用します。Nexusダッシュボードファブリックコントローラ VLAN ID が VNI のファブリック全体で一貫していない限り、これを使用しないことを推奨します。
<string>	この変数はオプションであり、ネットワーク名のガイドラインを満たす任意の数の英数字を入力できます。

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

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

- CLI ベースのオーバーレイ
- 構成プロファイルベースのオーバーレイ

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

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

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

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

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

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

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

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

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

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

[厳密な構成コンプライアンスの有効化（Enable Strict Config Compliance）]：このチェックボックスをオンにして、厳密な構成コンプライアンス機能を有効にします。これにより、双方向のコンプライアンス チェックが有効になり、インテント/期待されている構成に存在せず、実行構成内で追加された構成には、フラグが付けられます。デフォルトでは、この機能は無効になっています。

[AAA IP 認証の有効化（Enable AAA IP Authorization）]：IP 認証がリモート認証サーバで有効になっている場合に、AAA IP 認証を有効にします。これはNexusダッシュボード ファブリック コントローラをサポートするために必要で、カスタマがスイッチにアクセス可能な IP アドレスの厳密なコントロールをもつ場合のシナリオで必要です。

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

[エニーキャストボーダーゲートウェイのアドバタイズ-pip（Anycast Border Gateway advertise-pip）]：エニーキャスト ボーダー ゲートウェイの PIP を VTEP としてアドバタイズできるようにします。MSD ファブリックの「構成の再計算」で有効です。

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

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

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

展開設定中に PTP ループバック ID が見つからない場合は、次のエラーが生成されます。

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

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

[MPLS ハンドオフの有効化（Enable MPLS Handoff）]：MPLS ハンドオフ機能を有効にするには、このチェックボックスをオンにします。詳細については、『External/WAN Layer 3 Connectivity for VXLAN BGP EVPN Fabrics』の MPLS SR および LDP ハンドオフ章を参照してください。

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

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

[デフォルト キューイング ポリシーの有効化（Enable Default Queuing Policies）]：このファブリック内のすべてのスイッチに QoS ポリシーを適用するには、このチェックボックスをオンにします。すべてのスイッチに適用した QoS ポリシーを削除するには、このチェックボックスをオフにし、すべての設定を更新してポリシーへの参照を削除し、保

存して展開します。さまざまな Cisco Nexus 9000 シリーズ スイッチに使用できる定義済みの QoS 設定が含まれています。このチェックボックスをオンにすると、適切な QoS 設定がファブリック内のスイッチにプッシュされます。システム キューイングは、設定がスイッチに展開されると更新されます。インターフェイスごと自由形式ブロックに必要な設定を追加することにより、必要に応じて、定義されたキューイング ポリシーを使用してインターフェイス マーキングを実行できます。

テンプレート エディタでポリシー ファイルを開いて、実際のキューイング ポリシーを確認します。Cisco Web UI から、[操作（Operations）] > [テンプレート（Templates）] の順に選択します。Nexusダッシュボード ファブリック コントローラ ポリシー ファイル名でキューイング ポリシーを検索します（例：[queuing_policy_default_8q_cloudscale]）。ファイルを選択します。[アクション（Actions）] ドロップダウンリストから、[テンプレート コンテンツの編集（Edit template content）] を選択してポリシーを編集します。

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

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

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

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

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

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

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

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

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

9. [リソース（Resources）] タブをクリックします。

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

- デフォルトでは、定義されたプールから動的にアンダーレイ IP アドレス リソース（ループバック、ファブリック インターフェイスなど）を割り当てます。Nexusダッシュボードファブリック コントローラこのチェックボックスをオンにすると、割り当て方式が静的に切り替わり、動的IPアドレス範囲フィールドの一部が無効になります。
- 静的割り当ての場合、REST API を使用してアンダーレイ IP アドレス リソースをリソース マネージャ（RM）に入力する必要があります。
- マルチキャスト レプリケーションに BIDIR-PIM 機能が選択されている場合、[アンダーレイ RP ループバック IP 範囲（Underlay RP Loopback IP Range）] フィールドは有効のままになります。
- 静的割り当てから動的割り当てに変更しても、現在のIPリソースの使用情況は維持されます。それ以後の IP アドレス割り当て要求のみが動的プールから取得されます。

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

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

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

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

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

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

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

Underlay VTEP Loopback IPv6 Range：Loopback1およびAnycast Loopback IPv6 Address Rangeを指定します。

[アンダーレイ サブネット IPv6 範囲（Underlay Subnet IPv6 Range）]：番号付きおよびピアリンク SVI IP を割り当てる IPv6 アドレス範囲を指定します。

[IPv6アンダーレイの BGP ルータ ID 範囲（BGP Router ID Range for IPv6 Underlay）]：IPv6 アンダーレイの BGP ルータ ID 範囲を指定します。

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

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

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

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

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

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

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

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

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

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

a. L2 範囲を更新し、[保存（Save）] をクリックします。

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

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

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

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

このタブのフィールドは次のとおりです。

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

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

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

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

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

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

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

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

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

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

[ブートストラップの有効化（Enable Bootstrap）]：ブートストラップ機能を有効にします。ブートストラップは easy day-0 のインポートを可能にし、既存のファブリックで新規デバイスを立ち上げることができます。ブートストラップはNX-OS POAP機能を活用します。

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

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

ローカル DHCP サーバの有効化（Enable Local DHCP Server）：ローカル DHCP サーバを介した自動IPアドレス割り当ての有効化を開始するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、**[DHCP スコープ開始アドレス（DHCP Scope Start Address）]** および **[DHCP スコープ終了アドレス（DHCP Scope End Address）]** フィールドが編集可能になります。

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

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

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

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

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

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

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

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

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

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

スコープの形式は次の順で定義する必要があります。

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

例：10.6.0.2、10.6.0.9、16.0.0.1、24

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

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

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

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

時間単位のバックアップは、その時間の最初の 10 分間にトリガーされます。

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

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

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

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

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

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

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

Note 即時バックアップをトリガーするには、次の手順を実行します。

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

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

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

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

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

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

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

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

[Netflow エクスポータ（Netflow Exporter）]領域で、**[アクション（Actions）] > [追加（Add）]** の順にクリックして、1 つ以上の Netflow エクスポータを追加します。このエクスポータは、NetFlowデータの受信側です。この画面のフィールドは次のとおりです。

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

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

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

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

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

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

- **[モニター名（Monitor Name）]**：モニターの名前を指定します。
- **[レコード名（Record Name）]**：モニターのレコードの名前を指定します。

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

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

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

14. [ファブリック（Fabric）] をクリックして、スライドイン ペインに概要を表示します。[起動（Launch）] アイコンをクリックして、[ファブリックの概要（Fabric Overview）] を表示します。

スイッチの追加と VXLAN ファブリック管理の NDFC への移行

スイッチを検出して、新しく作成したファブリックに追加しましょう。

Procedure

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

[スイッチ（Switches）] タブをクリックします。

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

[スイッチの追加（Add Switches）] ウィンドウが表示されます。

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

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

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

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

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

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

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

ステップ 5 ファブリックにインポートする必要があるスイッチの横にあるチェックボックスをオンにして、**[ファブリックにインポート（Import into fabric）]** をクリックします。

1 回の試行で同時に複数のスイッチを検出することをお勧めします。スイッチは適切にケーブル接続しNDFCサーバーに接続する必要があり、スイッチのステータスは管理可能である必要があります。

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

ステップ 6 [ファブリックにインポート（Import into fabric）] をクリックします。

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

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

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

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

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

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

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

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

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

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

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

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

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

Note スイッチで L3 キープアライブが構成されている場合は、vPC ペアリングを手動で作成する必要があります。それ以外の場合、vPC 構成はスイッチから自動的に取得されます。

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

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

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

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

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

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

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

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

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

Note

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

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

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

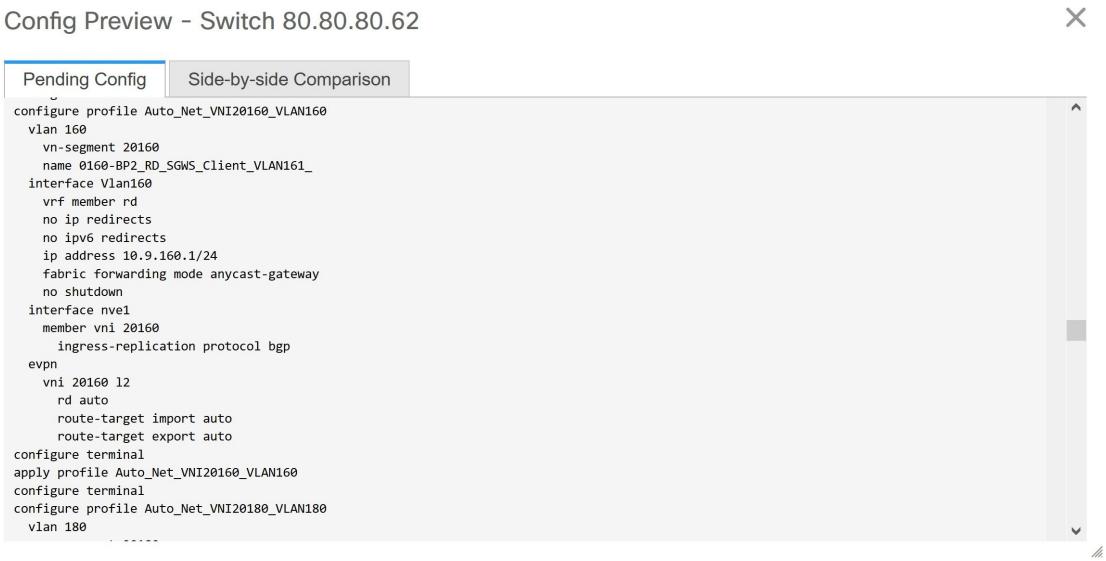
[並べて表示（Side-by-Side）] タブには、実行構成と予想される構成が並べて表示されます。

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

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

Note

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



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

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

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

ステップ 12 構成を確認したら、**[構成プレビュー スイッチ（Config Preview Switch）]** ウィンドウを閉じます。

ステップ 13 **[構成の展開（Deploy Config）]** をクリックして、構成をスイッチに展開します。

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

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

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

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

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

詳細については、ファブリックの概要を参照してください。

ブラウンフィールド移行の構成プロファイルのサポート

Cisco NDFC は、構成プロファイルでプロビジョニングされる VXLAN オーバーレイを使用した、ファブリックのブラウンフィールド インポートをサポートしています。このインポート プロセスは、構成プロファイルに基づいてオーバーレイ構成のインテントを再作成します。アンダーレイの移行は、通常のブラウンフィールド移行で実行されます。

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

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

以下は、構成プロファイルのサポートに関するガイドラインです。

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

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

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

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

Procedure

ステップ 1 ブラウンフィールド移行によって追加された RP 用に作成された **base_pim_bidir_11_1** ポリシーを確認します。各 **ip pim rp-address** *RP_IP* **group-list** *MULTICAST_GROUP* **bidir** コマンドで使用される RP IP およびマルチキャスト グループを確認します。

ステップ 2 各 **base_pim_bidir_11_1** ポリシーを新しいリーフまたはスパインの **[ポリシーの表示/編集（View/Edit Policies）]** ウィンドウから追加し、各 **base_pim_bidir_11_1** ポリシーの構成をプッシュします。

ボーダー ゲートウェイ スイッチを使用した MSD ファブリックの移行

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

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

    [両方を自動デプロイ（Auto Deploy Both）] チェックボックスをオフ（**[リソース（Resources）]** タブ）。
  - MSD_Fabric ファブリック

    [マルチサイト アンダーレイ IFC 自動展開フラグ（Multi-Site Underlay IFC Auto Deployment Flag）] チェックボックスをオフ（**[DCI]** タブ）。
- アンダーレイ マルチサイト ピアリング：サイト間のアンダーレイ拡張の eBGP ピアリングおよび対応するルーテッド インターフェイスは、**switch_freeform** および **routed_inerfaces**、オプションで **interface_freeform** 構成でキャプチャされます。この構成

には、マルチサイトのすべてのグローバル構成が含まれます。EVPN マルチサイトのループバックも、適切なインターフェイス テンプレートを介してキャプチャされます。

- オーバーレイ マルチサイト ピアリング：eBGP ピアリングは、**switch_freeform** の一部としてキャプチャされます。唯一の関連する構成が**ルータ bgp** の下にあるためです。
- ネットワークまたは VRF を含むオーバーレイ：対応するインテントは、**extension_type = MULTISITE** のボーダー ゲートウェイのプロファイルでキャプチャされます。

1. 必要なファブリック設定を使用して、Easy_Fabric および External_Fabric ファブリックを含むすべての必要なファブリックを作成します。上記のように [Auto VRF-Lite] 関連オプションを無効にします。詳細については、*VXLAN EVPN* ファブリックの作成および外部ファブリックセクションを参照してください。
2. すべてのスイッチを必要なすべてのファブリックにインポートし、それに応じてロールを設定します。
3. 各ファブリックで**[再計算して展開（Recalculate and Deploy）]** をクリックし、ブラウンフィールド移行プロセスが「展開」フェーズに到達することを確認します。ここでは、**[構成の展開（Deploy Configuration）]** をクリックしないでください。
4. ガイドラインに示すように、必要なファブリック設定で **MSD_Fabric** ファブリックを作成し、**[自動マルチサイト IFC（Auto MultiSite IFC）]** 関連オプションを無効にします。詳細については、『*Cisco DCNM LAN* ファブリック構成ガイド』の「*MSD* ファブリックの作成」を参照してください。
5. すべてのメンバーファブリックを MSD に移動します。この手順が正常に完了するまで、先に進まないでください。詳細については、『*Cisco DCNM LAN* ファブリック構成ガイド』の「*MSD-Parent-Fabric* での *Member1* ファブリックの移動」を参照してください。

（注） 各 Easy ファブリックのオーバーレイ ネットワークと VRF の定義は、対称である必要があります。それらが MSD に正常に追加されるためです。不一致が見つかった場合、エラーが報告されます。これらは、ファブリックのオーバーレイ情報を更新して MSD に追加することで修正する必要があります。

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

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

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

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

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

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

   この手順は、ファブリックで TRM が有効になっている場合に実行する必要があります。TRM が有効になっていない場合でも、各ネットワーク エントリを編集して保存する必要があります。
10. MSD ファブリックで **[再計算と展開（Recalculate and Deploy）]** をクリックしますが、**[構成の展開（Deploy Configuration）]** はクリックしないでください。
11. 各メンバー ファブリックに移動し、**[再計算と展開（Recalculate and Deploy）]** をクリックしてから、**[構成の展開（Deploy Configuration）]** をクリックします。

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

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

（注） MSD ファブリックを移行する前に、子ファブリックが MSD に追加されていることを確認してください。

1. MSD 子ファブリックをクリックし、**[ファブリック（Fabrics）]** > **[インターフェイス（Interfaces）]** に移動して、BGW を表示します。アンダーレイ IFC に使用する適切なレイヤ 3 ポート チャネルを選択します。
2. **[ポリシー（Policy）]** 列で、ドロップダウン リストから **int_port_channel_trunk_host_11_1** を選択します。関連付けられたポート チャネル インターフェイス メンバーを入力し、**[保存（Save）]** をクリックします。
3. MSD ファブリックの**表形式ビュー**に移動します。レイヤ 3 ポート リンクを編集し、マルチサイト アンダーレイ IFC リンク テンプレートを選択し、送信元と宛先の IP アドレスを入力します。これらの IP アドレスは、スイッチの既存の構成値と同じです。
4. 上記の手順 7 から 11 までの手順を実行します。

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。