



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 \(1 ページ\)](#)
- [前提条件, on page 2](#)
- [ガイドラインと制約事項, on page 3](#)
- [ファブリック トポロジの概要 \(5 ページ\)](#)
- [DCNM ブラウンフィールド展開タスク \(6 ページ\)](#)
- [既存の VXLAN BGP EVPN ファブリックの確認, on page 6](#)
- [VXLAN BGP EVPN ファブリックの作成, on page 9](#)
- [スイッチの追加と VXLAN ファブリック管理の DCNM への移行, on page 27](#)
- [VXLAN BGP EVPN ファブリックのインポートの確認 \(39 ページ\)](#)
- [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, on page 47](#)
- [ボトムアップ VXLAN ファブリックを DCNM に移行する, on page 48](#)
- [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 \(56 ページ\)](#)
- [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, on page 61](#)
- [ブラウンフィールドでインポートされた BIDIR 構成の変更, on page 64](#)
- [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, on page 65](#)
- [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 \(65 ページ\)](#)

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 (dcm_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ダーレイ ランデブー ポイント ループバック ID。
- BGP 構成では、「router-id」を使用します。これはルーティング ループバック インターフェイスの IP アドレスです。
- iBGP ピアテンプレートが構成されている場合は、リーフ スイッチとルート リフレクタで構成する必要があります。リーフ リフレクタとルート リフレクタの間で使用する必要があるテンプレート名は同じにするべきです。
- BGP ルート リフレクタおよびマルチキャスト ランデブー ポイント（該当する場合）機能が、スパイン スイッチに実装されていること。リーフ スイッチはこの機能をサポートしていません。
- VXLAN BGP EVPN ファブリックの概念と、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クゲートウェイ スパインのロールは、ブラウ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、VXLANID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。

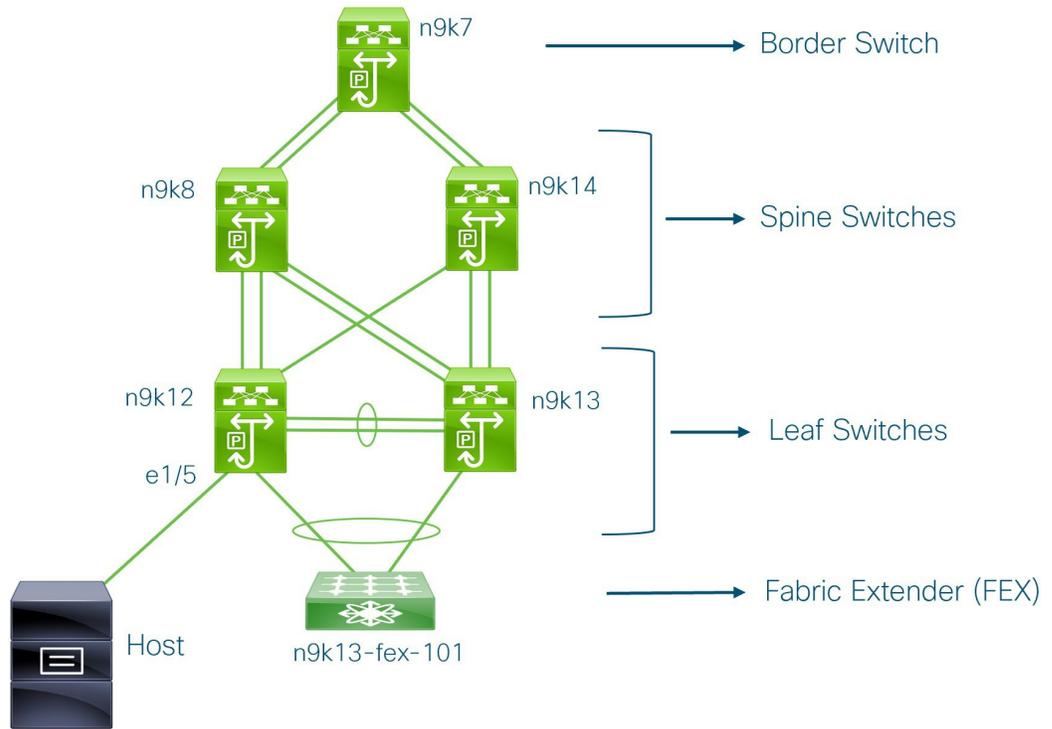
ファブリック トポロジの概要

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 (6 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 (39 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ーはありません。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。

Add Fabric ✕

* Fabric Name :

* Fabric Template : Easy_Fabric_11_1

General	Replication	vPC	Protocols	Advanced	Resources	Manageability	Bootstrap	Configuration Backup
* BGP ASN <input type="text"/> <small>1-4294967295 1-65535[0-65535]</small>								
Enable IPv6 Underlay <input type="checkbox"/>								
Enable IPv6 Link-Local Address <input checked="" type="checkbox"/>								
* Fabric Interface Numbering <input type="text" value="p2p"/> <small>Numbered(Point-to-Point) or Unnumbered</small>								
* Underlay Subnet IP Mask <input type="text" value="30"/> <small>Mask for Underlay Subnet IP Range</small>								
Underlay Subnet IPv6 Mask <input type="text"/> <small>Mask for Underlay Subnet IPv6 Range</small>								
* Link-State Routing Protocol <input type="text" value="ospf"/> <small>Supported routing protocols (OSPF/IS-IS)</small>								
* Route-Reflectors <input type="text" value="2"/> <small>Number of spines acting as Route-Reflectors</small>								
* Anycast Gateway MAC <input type="text" value="2020.0000.00aa"/> <small>Shared MAC address for all leafs (xxxx.xxxx.xxxx)</small>								
NX-OS Software Image Version <input type="text"/> <small>If Set, Image Version Check Enforced On All Switches. Images Can Be Uploaded From Control:Image Upload</small>								

[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umberド ネットワークのどちらか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트는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트의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트의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트를 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 を事前を選択できます。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。

General	Replication	vPC	Protocols	Advanced	Resources	Manageability	Bootstrap	Configuration Backup
	<p>* Replication Mode <input type="text" value="Multicast"/> ? Replication Mode for BUM Traffic</p> <p>* Multicast Group Subnet <input type="text" value="239.1.1.0/25"/> ? Multicast address with prefix 16 to 30</p> <p>Enable Tenant Routed Multicast (TRM) <input type="checkbox"/> ? For Overlay Multicast Support In VXLAN Fabrics</p> <p>Default MDT Address for TRM VRFs <input type="text"/> ? IPv4 Multicast Address</p> <p>* Rendezvous-Points <input type="text" value="2"/> ? Number of spines acting as Rendezvous-Point (RP)</p> <p>* RP Mode <input type="text" value="asm"/> ? Multicast RP Mode</p> <p>* Underlay RP Loopback Id <input type="text" value="254"/> ? (Min:0, Max:1023)</p> <p>Underlay Primary RP Loopback Id <input type="text"/> ? Used for Bidir-PIM Phantom RP (Min:0, Max:1023)</p> <p>Underlay Backup RP Loopback Id <input type="text"/> ? Used for Fallback Bidir-PIM Phantom RP (Min:0, Max:1023)</p> <p>Underlay Second Backup RP Loopback Id <input type="text"/> ? Used for second Fallback Bidir-PIM Phantom RP (Min:0, Max:1023)</p> <p>Underlay Third Backup RP Loopback Id <input type="text"/> ? Used for third Fallback Bidir-PIM Phantom RP (Min:0, Max:1023)</p>							

[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。

General	Replication	vPC	Protocols	Advanced	Resources	Manageability	Bootstrap	Configuration Backup
		* vPC Peer Link VLAN	<input type="text" value="3600"/>	① VLAN for vPC Peer Link SVI (Min:2, Max:3967)				
		Make vPC Peer Link VLAN as Native VLAN	<input type="checkbox"/>	①				
		* vPC Peer Keep Alive option	<input type="text" value="management"/>	① Use vPC Peer Keep Alive with Loopback or Management				
		* vPC Auto Recovery Time (In Seconds)	<input type="text" value="360"/>	① (Min:240, Max:3600)				
		* vPC Delay Restore Time (In Seconds)	<input type="text" value="150"/>	① (Min:1, Max:3600)				
		vPC Peer Link Port Channel ID	<input type="text" value="500"/>	① (Min:1, Max:4096)				
		vPC IPv6 ND Synchronize	<input checked="" type="checkbox"/>	① Enable IPv6 ND synchronization between vPC peers				
		vPC advertise-pip	<input type="checkbox"/>	① For Primary VTEP IP Advertisement As Next-Hop Of Prefix Routes				
		Enable the same vPC Domain Id for all vPC Pairs	<input type="checkbox"/>	① (Not Recommended)				
		vPC Domain Id	<input type="text"/>	① vPC Domain Id to be used on all vPC pairs				
		vPC Domain Id Range	<input type="text" value="1-1000"/>	① vPC Domain id range to use for new pairings				
		Enable Qos for Fabric vPC-Peering	<input type="checkbox"/>	① Qos on spines for guaranteed delivery of vPC Fabric Peering communication				
		Qos Policy Name	<input type="text"/>	① Qos Policy name should be same on all spines				

[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 ポートチャンネル ID (vPC Peer Link Port Channel ID)**] : vPC ピア リンクのポートチャンネル 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](#)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 CiscoIisisAuth
  key 127
  key-string 7 075e731f
```

この例では、キーチェーン名は **CiscoIisisAuth**、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、ブラウフィー

ルー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。

General	Replication	vPC	Protocols	Advanced	Resources	Manageability	Bootstrap	Configuration Backup
				<p>* VRF Template <input type="text" value="Default_VRF_Universal"/> ? Default Overlay VRF Template For Leafs</p> <p>* Network Template <input type="text" value="Default_Network_Universal"/> ? Default Overlay Network Template For Leafs</p> <p>* VRF Extension Template <input type="text" value="Default_VRF_Extension_Universal"/> ? Default Overlay VRF Template For Borders</p> <p>* Network Extension Template <input type="text" value="Default_Network_Extension_Universa"/> ? Default Overlay Network Template For Borders</p> <p>Site Id <input type="text"/></p> <p>* Intra Fabric Interface MTU <input type="text" value="9216"/> ? (Min:576, Max:9216). Must be an even number</p> <p>* Layer 2 Host Interface MTU <input type="text" value="9216"/> ? (Min:1500, Max:9216). Must be an even number</p> <p>* Power Supply Mode <input type="text" value="ps-redundant"/> ? Default Power Supply Mode For The Fabric</p> <p>* CoPP Profile <input type="text" value="strict"/> ? Fabric Wide CoPP Policy. Customized CoPP policy should be provided when 'manual' is selected</p> <p>VTEP HoldDown Time <input type="text" value="180"/> ? NVE Source Inteface HoldDown Time (Min:1, Max:1500) in seconds</p>				

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ー (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 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、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](#) 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。

General	Replication	vPC	Protocols	Advanced	Resources	Manageability	Bootstrap	Configuration Backup
Manual Underlay IP Address Allocation <input type="checkbox"/> ? Checking this will disable Dynamic Underlay IP Address Allocations								
* Underlay Routing Loopback IP Range		10.2.0.0/22	? Typically Loopback0 IP Address Range					
* Underlay VTEP Loopback IP Range		10.3.0.0/22	? Typically Loopback1 IP Address Range					
* Underlay RP Loopback IP Range		10.254.254.0/24	? Anycast or Phantom RP IP Address Range					
* Underlay Subnet IP Range		10.4.0.0/16	? Address range to assign Numbered and Peer Link SVI IPs					
Underlay MPLS Loopback IP Range			? Used for VXLAN to MPLS SR/LDP Handoff					
Underlay Routing Loopback IPv6 Range			? Typically Loopback0 IPv6 Address Range					
Underlay VTEP Loopback IPv6 Range			? Typically Loopback1 and Anycast Loopback IPv6 Address Range					
Underlay Subnet IPv6 Range			? IPv6 Address range to assign Numbered and Peer Link SVI IPs					
BGP Router ID Range for IPv6 Underlay			?					
* Layer 2 VXLAN VNI Range		30000-49000	? Overlay Network Identifier Range (Min:1, Max:16777214)					
* Layer 3 VXLAN VNI Range		50000-59000	? Overlay VRF Identifier Range (Min:1, Max:16777214)					
* Network VLAN Range		2300-2999	? Per Switch Overlay Network VLAN Range (Min:2, Max:3967)					
* VRF VLAN Range		2000-2299	? Per Switch Overlay VRF VLAN Range (Min:2, Max:3967)					
* Subinterface Dot1q Range		2-511	? Per Border Dot1q Range For VRF Lite Connectivity (Min:2, Max:4093)					
* VRF Lite Deployment		Manual	? VRF Lite Inter-Fabric Connection Deployment Options					
* VRF Lite Subnet IP Range		10.33.0.0/16	? Address range to assign P2P Interfabric Connections					
* VRF Lite Subnet Mask		30	? (Min:8, Max:31)					
* Service Network VLAN Range		3000-3199	? Per Switch Overlay Service Network VLAN Range (Min:2, Max:3967)					
* Route Map Sequence Number Range		1-65534	? (Min:1, Max:65534)					

[**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。

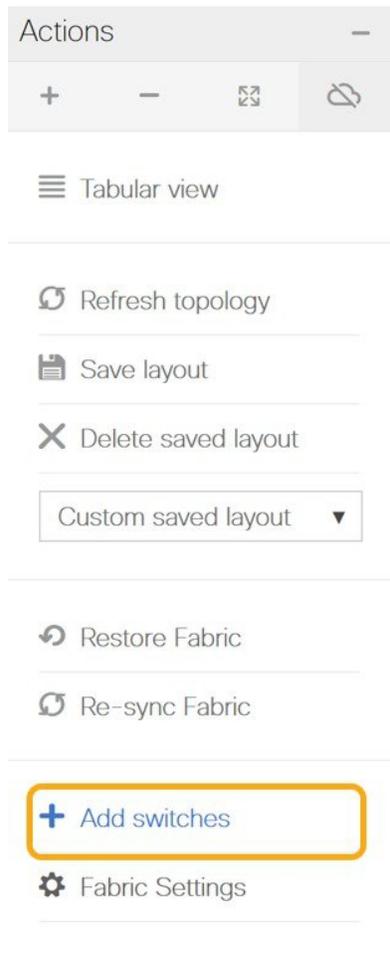
画面左側にある [操作 (Actions)] パネルでは、さまざまな機能を実行できます。それらの1つは、ファブリックにスイッチを追加する [スイッチの追加 (Add switches)] オプションです。ファブリックを作成したら、ファブリックデバイスを追加する必要があります。このプロセスは、次で説明されます。

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。

Inventory Management
✕

Discover Existing Switches

PowerOn Auto Provisioning (POAP)

Discovery Information

Scan Details

Seed IP
Ex: "2.2.2.20"; "10.10.10.40-60"; "2.2.2.20, 2.2.2.21"

Authentication Protocol

Username

Password

Max Hops

Preserve Config no yes
Selecting 'no' will clean up the configuration on switch(es)

Start discovery

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。

Inventory Management ✕

Discover Existing Switches
PowerOn Auto Provisioning (POAP)

Discovery Information
>
Scan Details
>

Seed IP
Ex: *2.2.2.20*; *10.10.10.40-60*; *2.2.2.20, 2.2.2.21*

Authentication Protocol

Username

Password

Max Hops hop(s)

Preserve Config no yes
Selecting 'no' will clean up the configuration on switch(es)

Start discovery

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。

Inventory Management ✕

Discover Existing Switches | PowerOn Auto Provisioning (POAP)

Discovery Information > Scan Details >

← Back Note: Preserve Config selection is 'yes'. Import into fabric

<input type="checkbox"/>	Name	IP Address	Model	Version	Status	Progress
<input checked="" type="checkbox"/>	n9k13	80.80.80.63	N9K-C939...	7.0(3)I7(6)	manageable	
<input checked="" type="checkbox"/>	n9k8	80.80.80.58	N9K-C939...	7.0(3)I7(6)	manageable	
<input checked="" type="checkbox"/>	n9k12	80.80.80.62	N9K-C939...	7.0(3)I7(6)	manageable	
<input checked="" type="checkbox"/>	n9k7	80.80.80.57	N9K-C939...	7.0(3)I7(6)	manageable	
<input checked="" type="checkbox"/>	n9k14	80.80.80.64	N9K-C921...	7.0(3)I7(6)	manageable	

Close

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。

Inventory Management

Discover Existing Switches
PowerOn Auto Provisioning (POAP)

Discovery Information >
Scan Details >

← Back
Note: Preserve Config selection is 'yes'.
Import into fabric

<input type="checkbox"/>	Name	IP Address	Model	Version	Status	Progress
<input checked="" type="checkbox"/>	n9k13	80.80.80.63	N9K-C939...	7.0(3)I7(6)	manageable	done
<input checked="" type="checkbox"/>	n9k8	80.80.80.58	N9K-C939...	7.0(3)I7(6)	manageable	done
<input checked="" type="checkbox"/>	n9k12	80.80.80.62	N9K-C939...	7.0(3)I7(6)	manageable	done
<input checked="" type="checkbox"/>	n9k7	80.80.80.57	N9K-C939...	7.0(3)I7(6)	manageable	done
<input checked="" type="checkbox"/>	n9k14	80.80.80.64	N9K-C921...	7.0(3)I7(6)	manageable	done

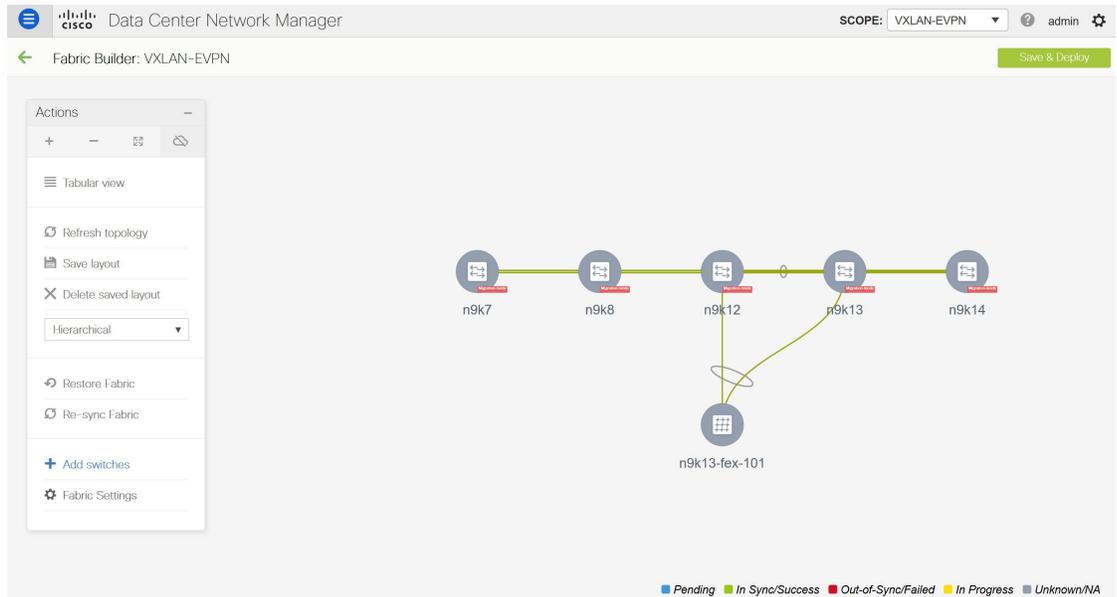
Show All ▼

Close

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

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

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。



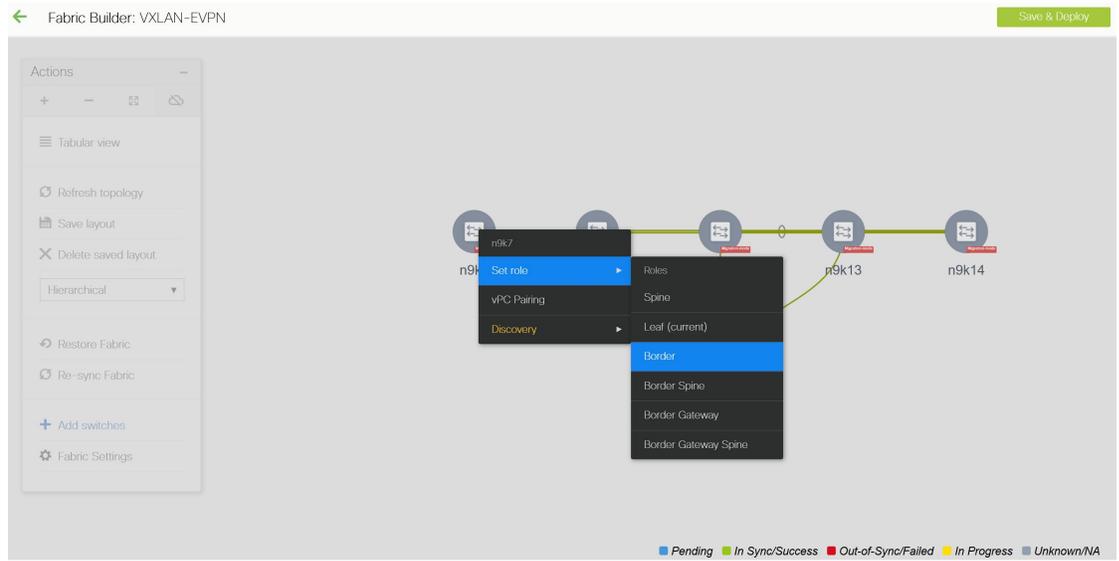
いくつかのスイッチでスイッチ ディスカバリ プロセスが失敗し、ディスカバリ エラーメッセージが表示されることがあります。それでも、そのようなスイッチは引き続きファブリック トポロジに表示されます。このようなスイッチをファブリックから削除し（スイッチアイコンを右クリックし、**[検出 (Discovery)]** > **[ファブリックから削除 (Remove from fabric)]** をクリックします)、再度インポートする必要があります。

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。

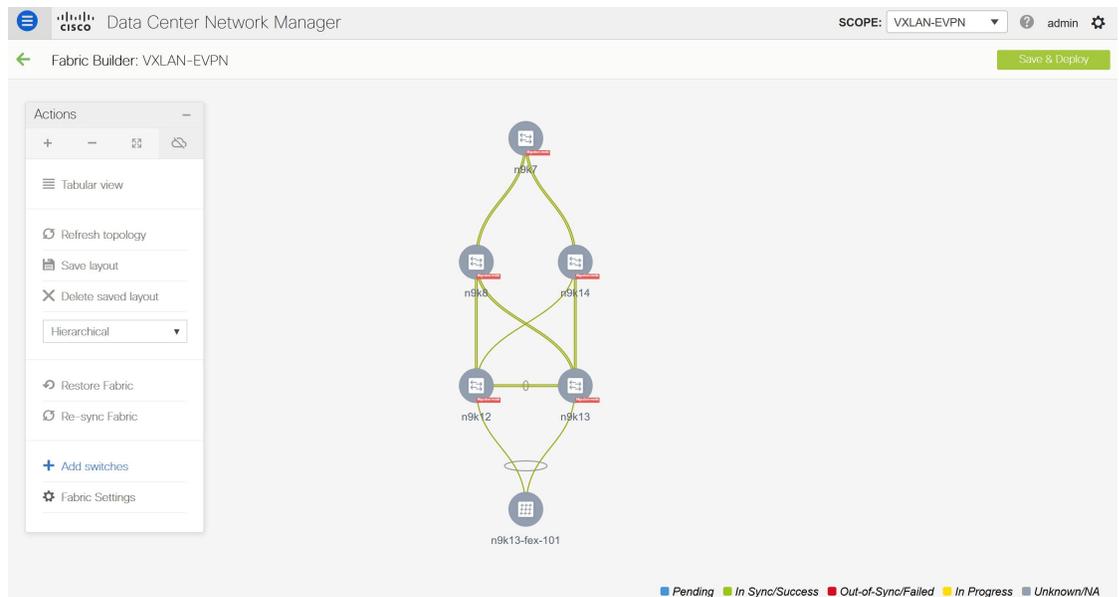
Note Cisco NX-OS リリース 7.0(3)I4(8b) および 7.0(4)I4(x) イメージのスイッチでサポートされるロールは、ボーダーリーフ、ボーダースパイン、リーフ、およびスパインです。

ステップ 8 **[n9k-7]** スwitch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。



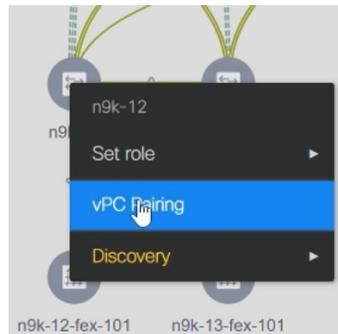
同様に、スパイン ロールを **n9k-14** および **n9k-8** スパイン スイッチで設定します。

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](#)を参照してください。



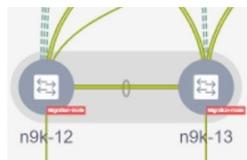
vPC ペアリング : vPC ペアリングは、レイヤ 3 vPC ピア キープ アライブが使用されているスイッチに対して行う必要があります。vPC ピア キープ アライブが管理オプションによって確立されると、vPC 構成はスイッチから自動的に取得されます。このペアリングは、移行が完了した後のみ GUI に反映されます。

- 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。

Config Deployment
✕

Step 1. Configuration Preview >
Step 2. Configuration Deployment Status >

Switch Name	IP Address	Switch Serial	Preview Config	Status	Re-sync	Progress
n9k12	80.80.80.62	SAL18422FX8	2405 lines	Out-of-sync		<div style="width: 100%; height: 10px; background-color: green;"></div> 100%
n9k13	80.80.80.63	SAL18422FXE	2405 lines	Out-of-sync		<div style="width: 100%; height: 10px; background-color: green;"></div> 100%
n9k7	80.80.80.57	SAL1833YM64	2200 lines	Out-of-sync		<div style="width: 100%; height: 10px; background-color: green;"></div> 100%
n9k14	80.80.80.64	SAL2016NXXB	2 lines	Out-of-sync		<div style="width: 100%; height: 10px; background-color: green;"></div> 100%
n9k8	80.80.80.58	SAL1833YMOV	3 lines	Out-of-sync		<div style="width: 100%; height: 10px; background-color: green;"></div> 100%

Deploy Config

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。

Config Preview - Switch 80.80.80.62

```

Pending Config | Side-by-side Comparison
-----
configure profile Auto_Net_VNI20160_VLAN160
vlan 160
  vn-segment 20160
  name 0160-BP2_RD_SGWS_Client_VLAN161_
interface Vlan160
  vrf member rd
  no ip redirects
  no ipv6 redirects
  ip address 10.9.160.1/24
  fabric forwarding mode anycast-gateway
  no shutdown
interface nve1
  member vni 20160
  ingress-replication protocol bgp
evpn
  vni 20160 12
  rd auto
  route-target import auto
  route-target export auto
configure terminal
apply profile Auto_Net_VNI20160_VLAN160
configure terminal
configure profile Auto_Net_VNI20180_VLAN180
vlan 180
  .....
```

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。

Config Preview - Switch 80.80.80.62

```

Pending Config | Side-by-side Comparison
-----
no vlan 160
no vlan 159
no vlan 158
no vlan 157
no vlan 156
no vlan 155
no vlan 154
no vlan 126
no vlan 125
no vlan 124
no vlan 122
no vlan 1141
no vlan 10
no interface Vlan9
no interface Vlan899
no interface Vlan84
no interface Vlan820
no interface Vlan819
no interface Vlan818
no interface Vlan817
no interface Vlan816
no interface Vlan815
no interface Vlan814
no interface Vlan813
```

[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。

Config Deployment
✕

Step 1. Configuration Preview >
Step 2. Configuration Deployment Status >

Switch Name	IP Address	Status	Status Description	Progress
n9k14	80.80.80.64	COMPLETED	Deployed successfully	100%
n9k8	80.80.80.58	COMPLETED	Deployed successfully	100%
n9k12	80.80.80.62	COMPLETED	Deployed successfully	100%
n9k7	80.80.80.57	COMPLETED	Deployed successfully	100%
n9k13	80.80.80.63	COMPLETED	Deployed successfully	100%

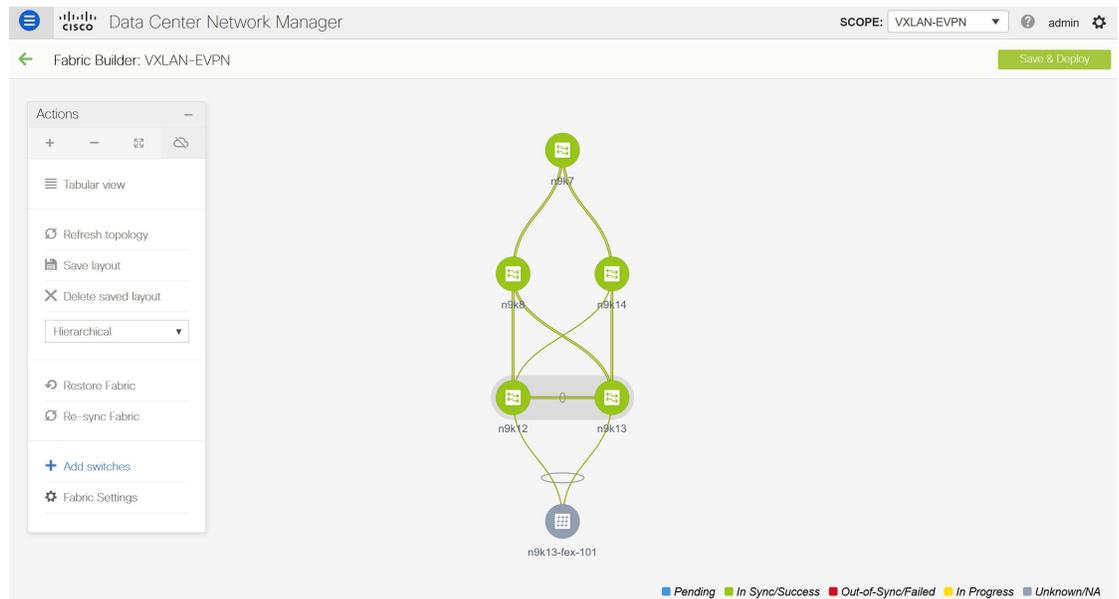
Close

[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せん。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せん。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。

The diagram shows a network topology with five switches and one host. The switches are labeled n9k7, n9k8, n9k12, n9k13, and n9k14. The host is labeled n9k13-fex-101. The switches are connected in a mesh topology. A legend at the bottom indicates that blue represents 'Pending' and green represents 'In Sync/Success'. The switches n9k7, n9k8, n9k12, and n9k14 are green, while n9k13 is blue.

Summary	
Status:	✓ ok
Serial number:	SAL18422FX8
CPU:	22%
Memory:	30%
VPC Domain ID: 2	
Role:	Secondary
Peer:	n9k13
Peerlink State:	Peer is OK
Keep Alive State:	Peer is alive
Consistency State:	Consistent
Send Interface:	mgmt0
Receive Interface:	mgmt0
Tags	
+	
System Tags	
VTEP	
← Show more details	

ステップ2 [VXLAN (VXLAN)] タブをクリックします。

n9k12
80.80.80.62
N9K-C9396PX

System Info Modules FEX License Features **VXLAN** Port Capacity

VXLAN Total 84

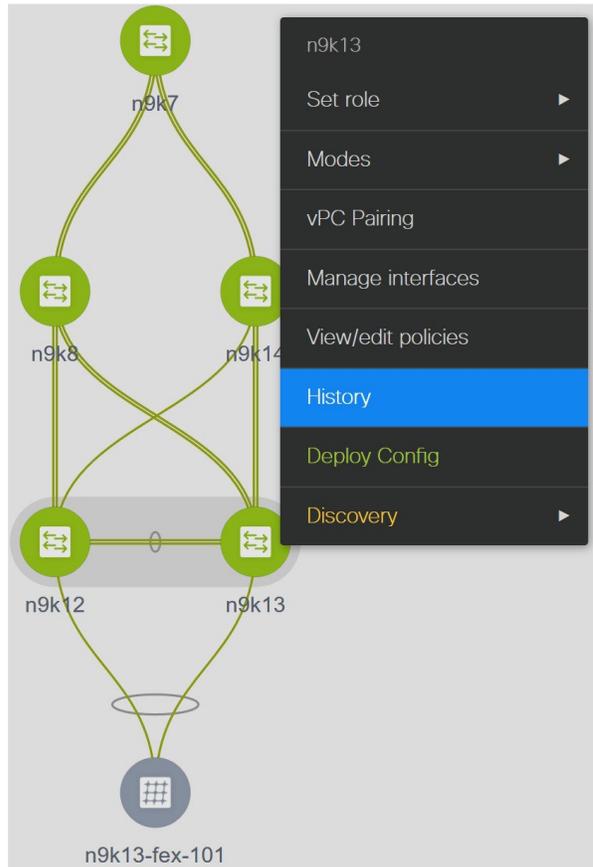
Show Quick Filter

NVE Interface	VNI	Multicast Address	VNI Status	Mode	Type	VRF	Mapped VLAN
nve1	20006	UnicastBGP	Up	Control-Plane	Layer-2	-	6
nve1	20009	UnicastBGP	Up	Control-Plane	Layer-2	-	9
nve1	20010	UnicastBGP	Up	Control-Plane	Layer-2	-	10
nve1	20017	UnicastBGP	Up	Control-Plane	Layer-2	-	17
nve1	20018	UnicastBGP	Up	Control-Plane	Layer-2	-	18
nve1	20027	UnicastBGP	Up	Control-Plane	Layer-2	-	27
nve1	20028	UnicastBGP	Up	Control-Plane	Layer-2	-	28
nve1	20029	UnicastBGP	Up	Control-Plane	Layer-2	-	29
nve1	20030	UnicastBGP	Up	Control-Plane	Layer-2	-	30
nve1	20031	UnicastBGP	Up	Control-Plane	Layer-2	-	31
nve1	20036	UnicastBGP	Up	Control-Plane	Layer-2	-	36
nve1	20040	UnicastBGP	Up	Control-Plane	Layer-2	-	40

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。

Policy Deployment History for n9k13 (SAL18422FXE)

Entity Name	Entity Type	Source	Status	Status Description	User	Time of Completion
SAL18422FXE	SWITCH	DCNM	SUCCESS	Successfully deployed	admin	2019-08-08 22:47:13.353
SWITCH	SWITCH	UNDERLAY	SUCCESS	Successfully deployed	admin	2019-08-08 22:36:32.101
SWITCH	SWITCH	UNDERLAY	SUCCESS	Successfully deployed	admin	2019-08-08 22:36:14.783
SWITCH	SWITCH	UNDERLAY	SUCCESS	Successfully deployed	admin	2019-08-08 22:36:07.129
SWITCH	SWITCH	UNDERLAY	SUCCESS	Successfully deployed	admin	2019-08-08 22:36:06.122
SWITCH	SWITCH	UNDERLAY	SUCCESS	Successfully deployed	admin	2019-08-08 22:36:05.116
SWITCH	SWITCH	UNDERLAY	SUCCESS	Successfully deployed	admin	2019-08-08 22:36:04.109
SWITCH	SWITCH	UNDERLAY	SUCCESS	Successfully deployed	admin	2019-08-08 22:36:03.102
SWITCH	SWITCH	UNDERLAY	SUCCESS	Successfully deployed	admin	2019-08-08 22:36:02.095
SWITCH	SWITCH	UNDERLAY	SUCCESS	Successfully deployed	admin	2019-08-08 22:36:01.089
SWITCH	SWITCH	UNDERLAY	SUCCESS	Successfully deployed	admin	2019-08-08 22:36:00.081
SWITCH	SWITCH	UNDERLAY	SUCCESS	Successfully deployed	admin	2019-08-08 22:35:59.275

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。

SCOPE: VXLAN-EVPN admin

Control / Management / Resources

Resource Allocation Selected 0 / Total 429

Scope Type	Scope	Device Name	Device IP	Allocated Resource	Allocated To	Resource Type	Is Allocated?	Allocated On
Device	SAL18422FX8	n9k12	80.80.80.62	80	Auto_Net_VNI20080_VL...	TOP_DOWN_NE...	Yes	09/08/2019,...
Device	SAL18422FX8	n9k12	80.80.80.62	500	loopback500	LOOPBACK_ID	Yes	09/08/2019,...
Device	SAL18422FX8	n9k12	80.80.80.62	501	loopback501	LOOPBACK_ID	Yes	09/08/2019,...
Device	SAL1833YM64	n9k7	80.80.80.57	101	port-channel101	PORT_CHANNEL...	Yes	09/08/2019,...
Device	SAL1833YM64	n9k7	80.80.80.57	3957	ECD	TOP_DOWN_VR...	Yes	09/08/2019,...
Device	SAL1833YM64	n9k7	80.80.80.57	3959	LC-DMZ	TOP_DOWN_VR...	Yes	09/08/2019,...
Device	SAL1833YM64	n9k7	80.80.80.57	3958	RD	TOP_DOWN_VR...	Yes	09/08/2019,...
Device	SAL1833YM64	n9k7	80.80.80.57	3965	COMMON-MGMT	TOP_DOWN_VR...	Yes	09/08/2019,...
Device	SAL1833YM64	n9k7	80.80.80.57	3961	DCI	TOP_DOWN_VR...	Yes	09/08/2019,...
Device	SAL1833YM64	n9k7	80.80.80.57	58	Auto_Net_VNI20058_VL...	TOP_DOWN_NE...	Yes	09/08/2019,...
Device	SAL1833YM64	n9k7	80.80.80.57	57	Auto_Net_VNI20057_VL...	TOP_DOWN_NE...	Yes	09/08/2019,...
Device	SAL1833YM64	n9k7	80.80.80.57	3964	COMMON-DMZ	TOP_DOWN_VR...	Yes	09/08/2019,...
Device	SAL1833YM64	n9k7	80.80.80.57	3963	LC	TOP_DOWN_VR...	Yes	09/08/2019,...
Device	SAL1833YM64	n9k7	80.80.80.57	3967	switchpool-default	TOP_DOWN_VR...	Yes	09/08/2019,...
Device	SAL1833YM64	n9k7	80.80.80.57	3960	IALAB	TOP_DOWN_VR...	Yes	09/08/2019,...
Device	SAL1833YM64	n9k7	80.80.80.57	3962	Internet	TOP_DOWN_VR...	Yes	09/08/2019,...

VLAN ID、ポートチャンネル 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。

Network / VRF Selection > Network / VRF Deployment

Fabric Selected: VXLAN-EVPN

Selected 0 / Total 1

Network Name	Network ID	VRF Name	IPv4 Gateway/Subnet	IPv6 Gateway/Prefix	Status	VLAN ID
Auto_Net_VNI20349_VLAN...	20349	Internet	204.90.140.134/29		DEPLOYED	349

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 つであることを注意してください。

Name	Network ID	VLAN ID	Switch	Ports	Status	Role
Auto_Net_VNI20349_VLAN...	20349	349	n9k12	Ethernet1/5, Port-channel500, Port-channel502	DEPLOYED	leaf
Auto_Net_VNI20349_VLAN...	20349	349	n9k13	Port-channel503, Port-channel505	DEPLOYED	leaf
Auto_Net_VNI20349_VLAN...	20349	349	n9k7		DEPLOYED	border

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。

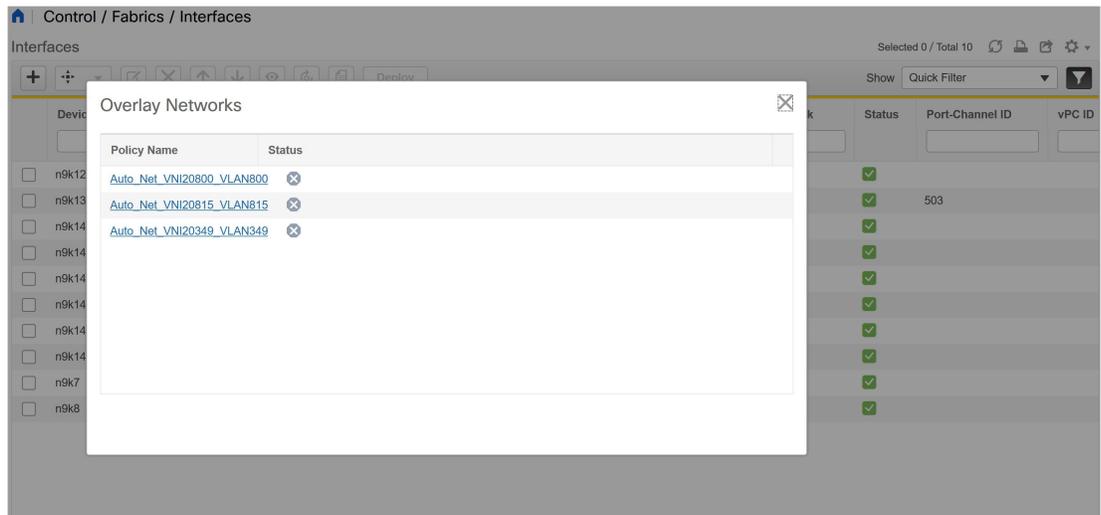
ポートチャネル、vPC、および mgmt0 インターフェイスを含む、インポートされたすべてのインターフェイスが [インターフェイス (Interfaces)] ウィンドウに表示されます。

ステップ 6 [名前 (Name)] フィールドに、[Ethernet1/5] と入力します。

Device Name	Name	Admin	Oper	Reason	Policy	Overlay Network	Status	Port-Channel ID	vPC ID
n9k12	Ethernet1/5	↑	↑	ok	int_trunk_host_11_1	Networks	✓		
n9k13	Ethernet1/5	↑	↓	XCVR not inserted	int_vpc_trunk_po_membr	NA	✓	503	
n9k14	Ethernet1/5	↑	↓	XCVR not inserted	int_trunk_host_11_1	NA	✓		
n9k14	Ethernet1/50	↑	↓	Link not connected	int_trunk_host_11_1	NA	✓		
n9k14	Ethernet1/51	↑	↓	XCVR not inserted	int_trunk_host_11_1	NA	✓		
n9k14	Ethernet1/52	↑	↓	XCVR not inserted	int_trunk_host_11_1	NA	✓		
n9k14	Ethernet1/53	↑	↓	XCVR not inserted	int_trunk_host_11_1	NA	✓		
n9k14	Ethernet1/54	↑	↓	XCVR not inserted	int_trunk_host_11_1	NA	✓		
n9k7	Ethernet1/5	↑	↓	XCVR not inserted	int_trunk_host_11_1	Networks	✓		
n9k8	Ethernet1/5	↑	↓	XCVR not inserted	int_trunk_host_11_1	NA	✓		

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。

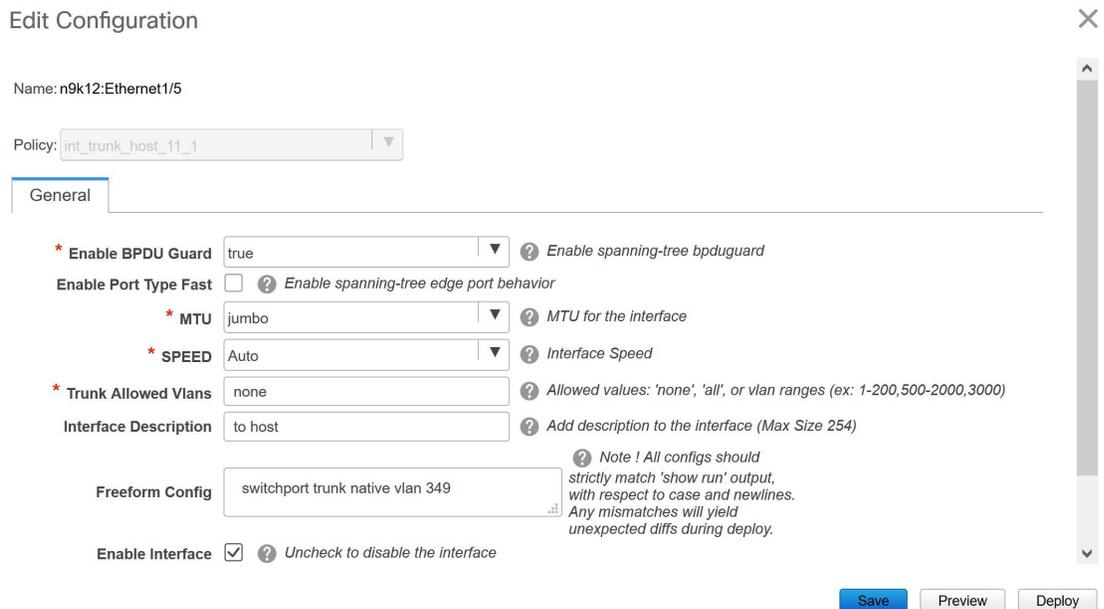


これらは、イーサネット 1/5 インターフェイスに接続されているネットワークです。

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フィールド移行がサポートされています。
- スwitch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、ブラウフィールド移行と同じです。詳細については、「ブラウフィールド展開： **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。

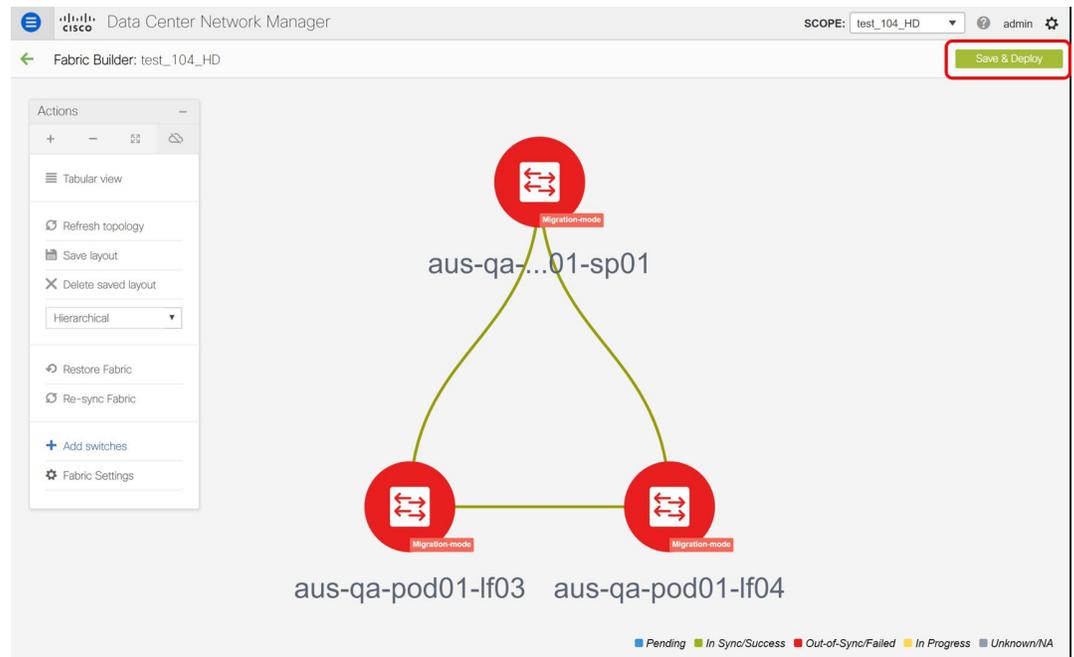
1. **VXLAN BGP EVPN** ファブリックを作成します。

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。

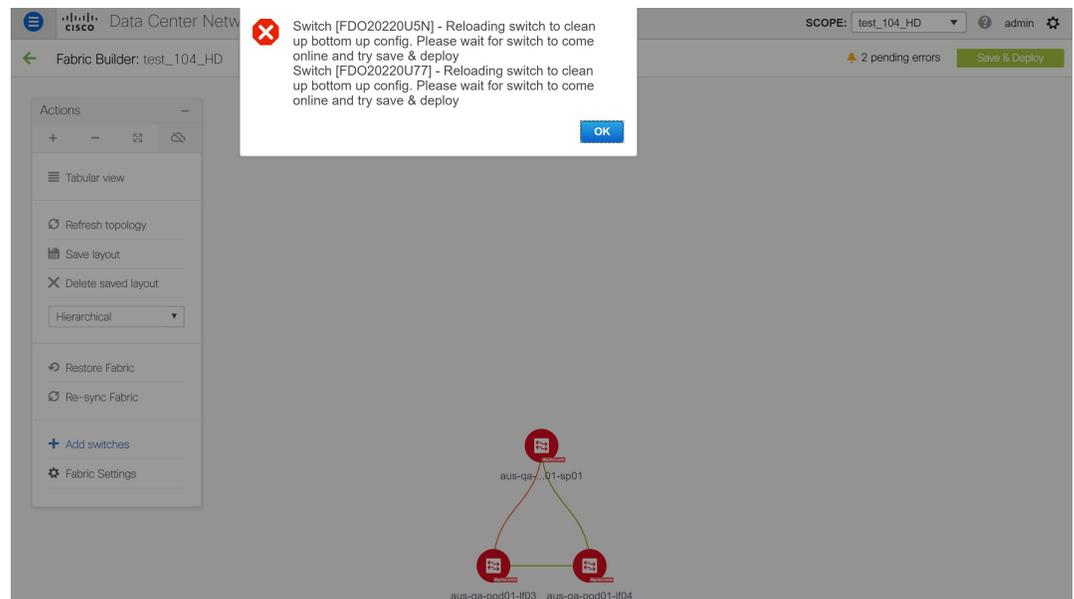
2. ファブリックにスイッチ インスタンスを追加します。

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。

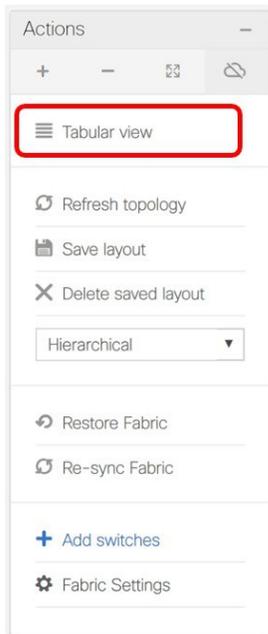


追加されたスイッチにボトムアップ構成が含まれている場合、次のエラーが表示されます。「ボトムアップ構成をクリーンアップするためにスイッチを再ロードしています。」スイッチがオンラインになるまで待つから、**[保存と展開 (Save & Deploy)]**を試行してください。

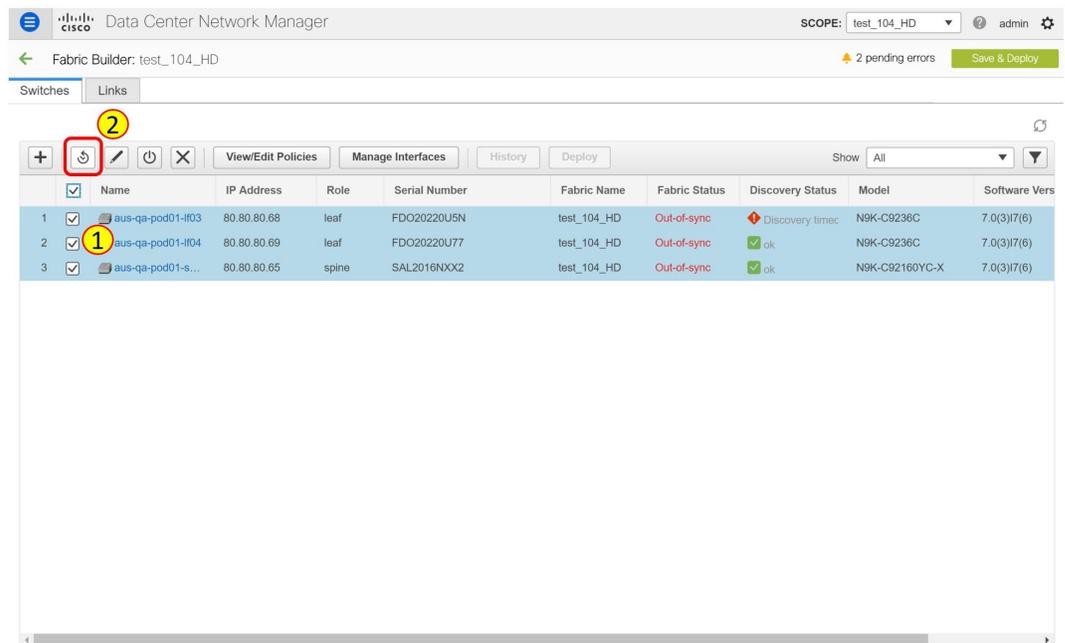


4. スイッチがリロード操作を完了するまで待ちます。**[アクション (Actions)]**メニューの**[表形式ビュー (Tabular view)]**をクリックして、スイッチのステータスを表示します。

ボトムアップ VXLAN ファブリックを DCNM に移行する



- （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。

- 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。

	<input type="checkbox"/>	Name	IP Address	Role	Serial Number	Fabric Name	Fabric Status
1	<input type="checkbox"/>	aus-qa-pod01-If03	80.80.80.68	leaf	FDO20220U5N	test_104_HD	Out-of-sync
2	<input type="checkbox"/>	aus-qa-pod01-If04	80.80.80.69	leaf	FDO20220U77	test_104_HD	Out-of-sync
3	<input type="checkbox"/>	aus-qa-pod01-s...	80.80.80.65	spine	SAL2016NXX2	test_104_HD	Out-of-sync

- [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。

Config Deployment

Step 1. Configuration Preview > Step 2. Configuration Deployment Status >

Switch Name	IP Address	Switch Serial	Preview Config	Status	Re-sync	Progress
aus-qa-pod01-...	80.80.80.68	FDO20220U5N	498 lines	Out-of-sync		100%
aus-qa-pod01-...	80.80.80.65	SAL2016NXX2	0 lines	In-sync		100%
aus-qa-pod01-...	80.80.80.69	FDO20220U77	534 lines	Out-of-sync		100%

Deploy Config

[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。

Config Preview - Switch 80.80.80.68

Pending Config | Side-by-side Comparison

```

router bgp 65500
  no neighbor 10.96.32.2
  nxapi http port 80
  vpc domain 998
  auto-recovery reload-delay 360
  configure profile Auto_Net_VNI30113_VLAN113
  vlan 113
  vn-segment 30113
  name aus-qa-sf1-prim
  interface vlan113
  description aus-qa-sf1-prim
  vrf member qa:common
  no ip redirects
  no ipv6 redirects
  ip address 172.18.113.1/24 tag 12345
  ip dhcp relay address 172.20.16.79
  fabric forwarding mode anycast-gateway
  no shutdown
  interface nve1
  member vni 30113
  mcast-group 239.1.1.20
  suppress-arp
  evpn
  .....
```

[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。

Config Deployment
✕

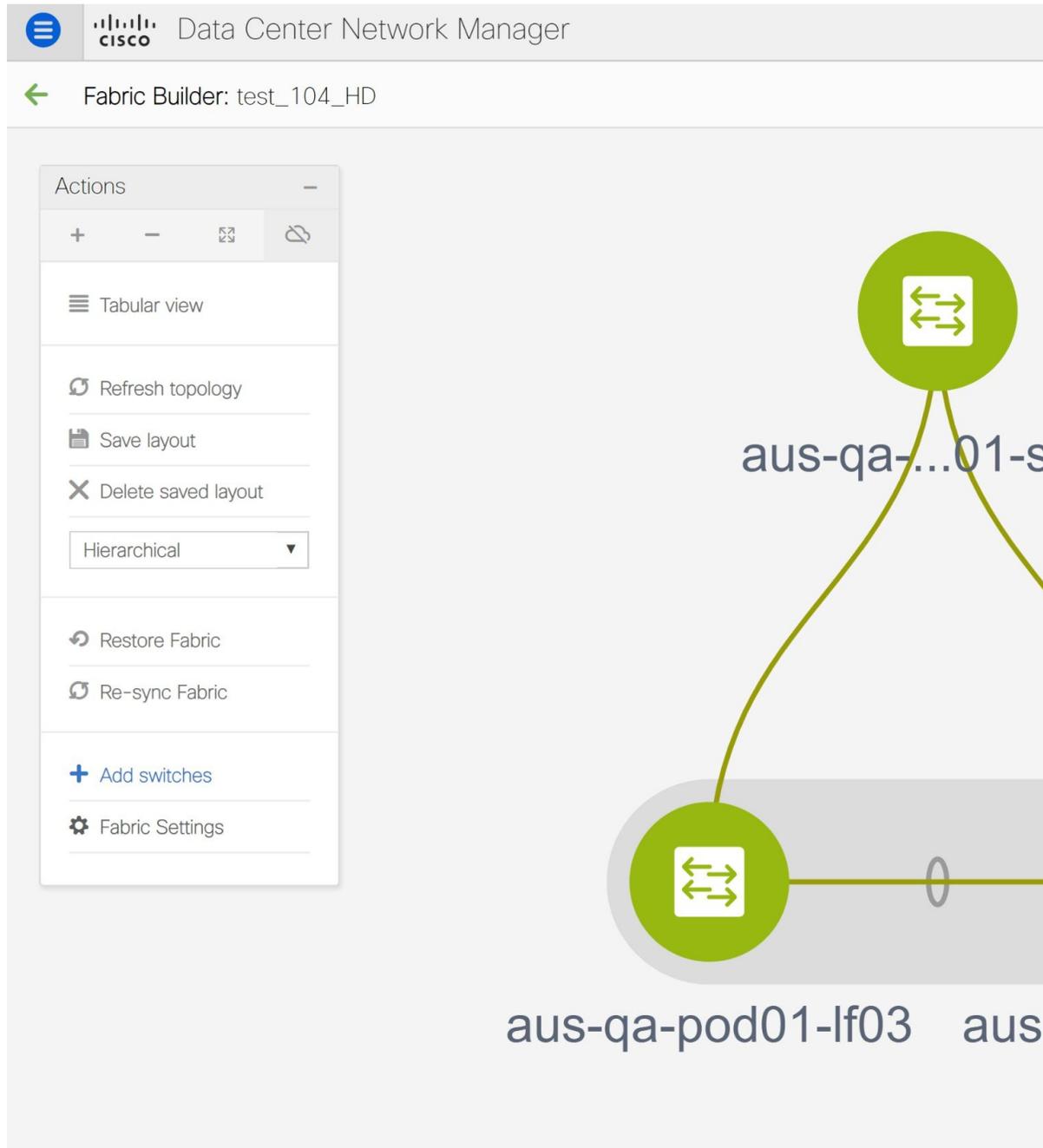
Step 1. Configuration Preview >
Step 2. Configuration Deployment Status >

Switch Name	IP Address	Status	Status Description	Progress
aus-qa-pod01-...	80.80.80.65	COMPLETED	No Commands to execute.	100%
aus-qa-pod01-...	80.80.80.69	COMPLETED	Deployed successfully	100%
aus-qa-pod01-...	80.80.80.68	COMPLETED	Deployed successfully	100%

Close

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。

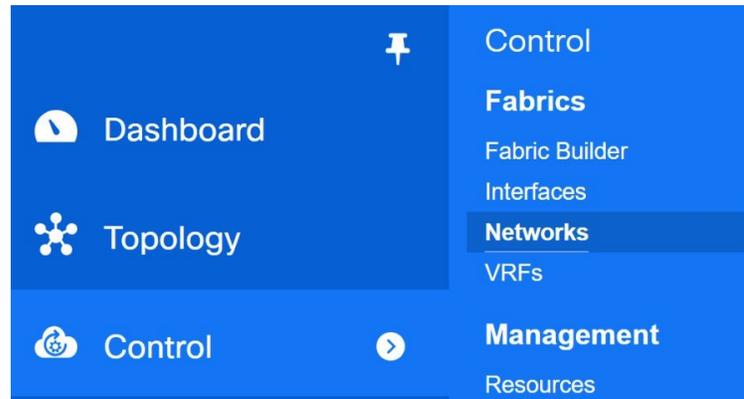
ファブリック トポロジ ウィンドウでは、インポートされたすべてのスイッチインスタンスが緑色で表示され、構成が成功したことを示します。また、移行モードラベルは、どのスイッチアイコンでも表示されなくなります。



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。

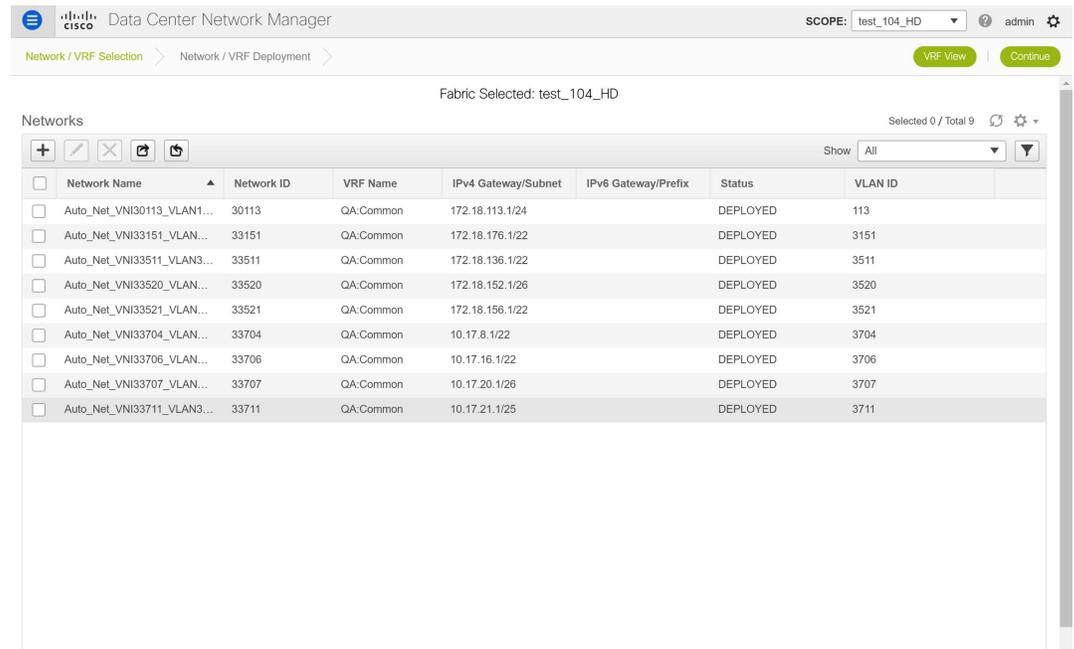
1. [制御 (Control)] > [ファブリック (Fabrics)] > [ネットワーク (Networks)] を選択します。



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。

Config Deployment ✕

Step 1. Configuration Preview > Step 2. Configuration Deployment Status >

Switch Name	IP Address	Switch Serial	Preview Config	Status	Re-sync	Progress
n9k7_bp2-lfsw...	80.80.80.57	SAL1833YM64	1 lines	Out-of-sync		100%
n9k8_bp2-sps...	80.80.80.58	SAL1833YM0V	0 lines	In-sync		100%

[Deploy Config](#)

- (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。

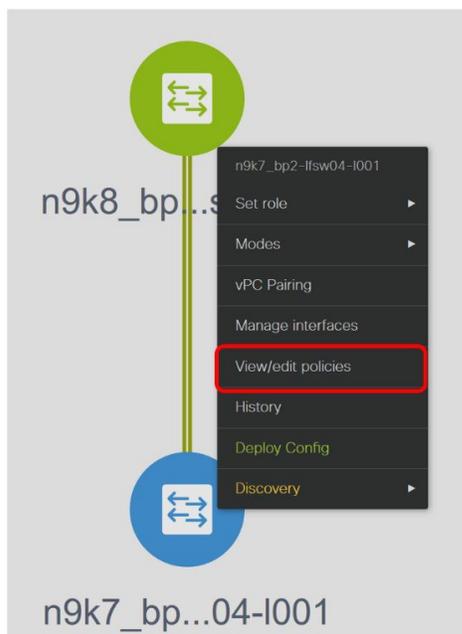
Config Preview - Switch 80.80.80.57 ✕

Pending Config Side-by-side Comparison

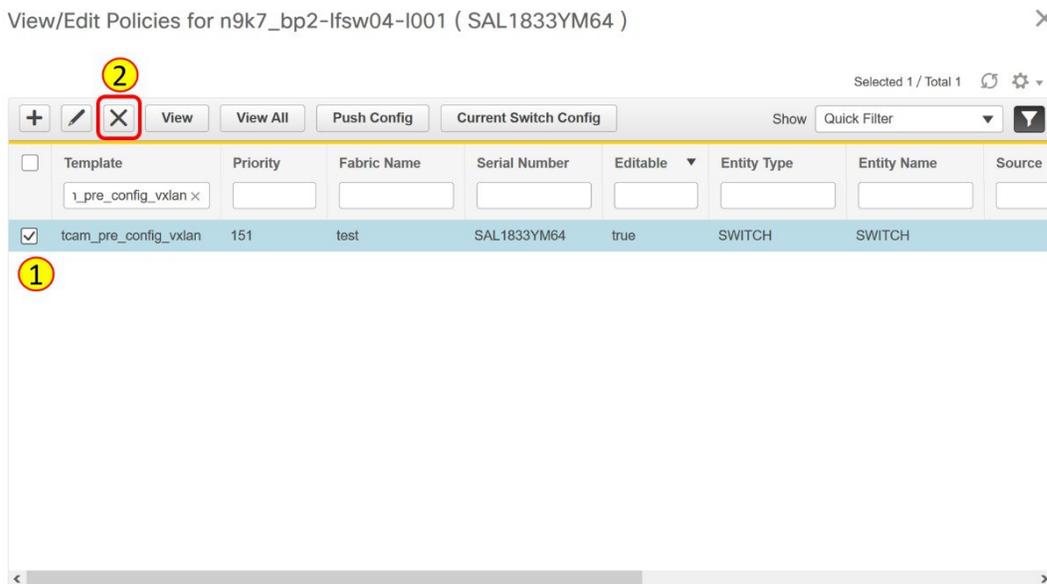
```
hardware access-list tcam region arp-ether 256 double-wide
```

[構成プレビュー (Config Preview)] ウィンドウを閉じます。

- 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。

Config Deployment

Step 1. Configuration Preview > Step 2. Configuration Deployment Status >

Switch Name	IP Address	Switch Serial	Preview Config	Status	Re-sync	Progress
n9k7_bp2-lfsw...	80.80.80.57	SAL1833YM64	0 lines	In-sync		100%
n9k8_bp2-sps...	80.80.80.58	SAL1833YM0V	0 lines	In-sync		100%

[Deploy Config](#)

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。

View/Edit Policies for n9k7_bp2-lfsw04-l001 (SAL1833YM64)

Selected 1 / Total 1

+ [View](#) [View All](#) [Push Config](#) [Current Switch Config](#) Show

<input type="checkbox"/>	Template	Priority	Fabric Name	Serial Number	Editable	Entity Type	Entity Name	Source
--------------------------	----------	----------	-------------	---------------	----------	-------------	-------------	--------

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。

Add Policy ×

* Priority (1-1000):

* Policy:

Variables:

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。

View/Edit Policies for n9k7_bp2-lfsw04-l001 (SAL1833YM64) ×

Selected 1 / Total 1

Template	Priority	Fabric Name	Serial Number	Editable	Entity Type	Entity Name	Source
<input type="checkbox"/> <code>_pre_config_vxlan</code>	<input type="text"/>						
<input checked="" type="checkbox"/> <code>tcam_pre_config_vxlan</code>	151	test	SAL1833YM64	true	SWITCH	SWITCH	

①

[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。

The screenshot shows the 'Edit Network' configuration window. The 'Network Profile' section is expanded, showing a list of tabs: 'General' and 'Advanced'. The 'General' tab is active, displaying several configuration fields. The 'Vlan Name' field is highlighted with a red rectangular box and is currently empty. Other fields include 'IPv4 Gateway/NetMask' (172.16.6.1/24), 'IPv6 Gateway/Prefix' (1111::2222/48), 'Interface Description', 'MTU for L3 interface' (1500), 'IPv4 Secondary GW1' (2.2.2.2/24), and 'IPv4 Secondary GW2' (3.3.3.3/24). Each field has a help icon (question mark) and an example value. At the bottom right, there are 'Save' and 'Cancel' buttons.

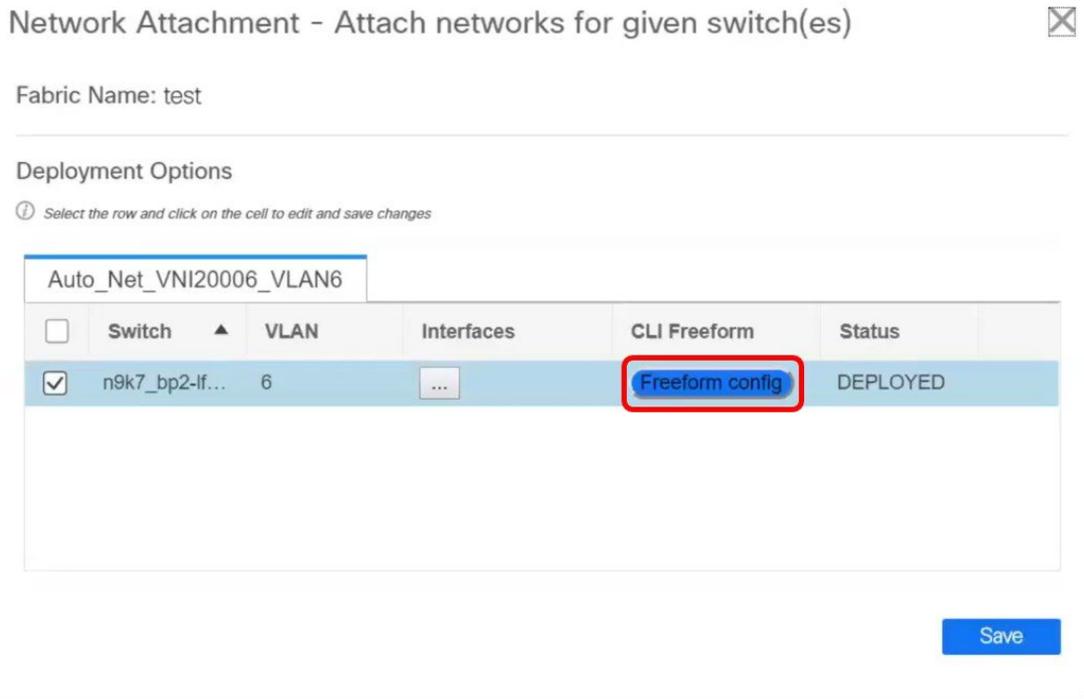
[ネットワークの編集 (Edit Network)] ウィンドウでは、DCNM がオーバーレイ プロファイルでこの情報をキャプチャしていないため、[VLAN 名 (Vlan Name)] フィールドは空です。代

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witch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。

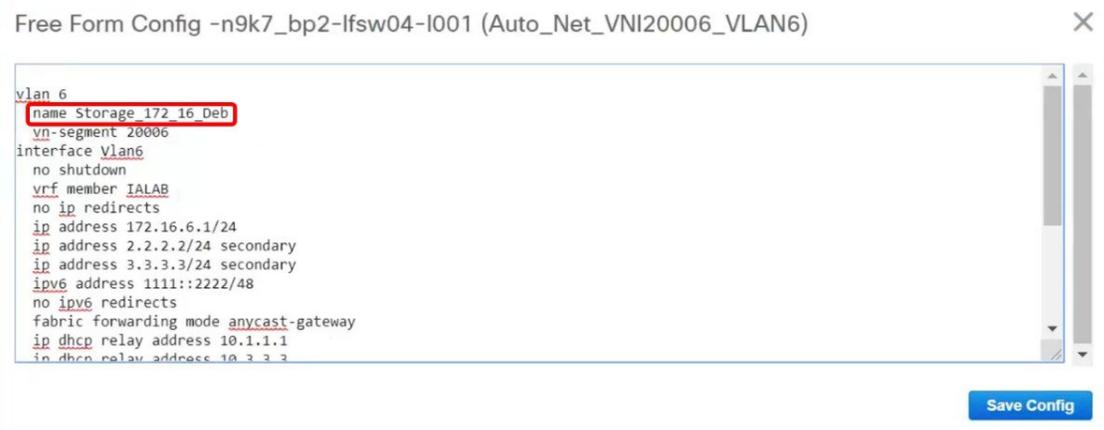


ステップ 8 [自由形式構成 (Free Form Config)] ウィンドウで VLAN 名を変更し、[構成の保存 (Save Config)] をクリックします。

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

General	DCI	Resources	Configuration Backup
* Multi-Site Overlay IFC Deployment Method		Manual	Manual ① Auto Overlay EVPN Peering to Route Servers, Auto Overlay EVPN Direct Peering to Border Gateways
Multi-Site Route Server List			① Multi-Site Router-Server peer list, e.g. 128.89.0.1, 128.89.0.2
Multi-Site Route Server BGP ASN List			① 1-4294967295 1-65535[0-65535], e.g. 65000, 65001
Multi-Site Underlay IFC Auto Deployment Flag		<input type="checkbox"/>	①

- 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_interfaces**、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パバックも、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 **ルーター 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. 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。

- 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ン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。