



# BGP ベースのルーテッド ファブリックの管理

この章では、選択したルーティングプロトコルとして eBGP を使用して、典型的なスパインリーフベースのルーテッドファブリックを構成する方法について説明します。これは、大規模なスケーラブルデータセンター (MSDC) ネットワークに推奨される展開の選択肢です。Single-AS オプションと Multi-AS オプションの両方がサポートされています。ルーテッドファブリックには、リーフ間のレイヤ2ストレッチまたはサブネットストレッチはありません。つまり、ネットワークはリーフのペアまたはラックにローカルに配置され、リーフは直接接続されたサーバーワークロードのデフォルトゲートウェイをホストします。ラック全体のサブネットアドバタイズメントは、スパインを介して eBGP 経由で通信されるため、ルーテッドファブリック内での Any-to-Any の到達可能性が実現されます。

- [eBGP ベースのファブリックの作成, on page 1](#)
- [ファブリックへのスイッチの追加, on page 14](#)
- [ファブリック アンダーレイ eBGP ポリシーの展開 \(29 ページ\)](#)
- [eBGP ベースのファブリックにおけるネットワークの展開 \(31 ページ\)](#)

## eBGP ベースのファブリックの作成

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

**[ファブリックビルダ (Fabric Builder)]** 画面が表示されます。初めてログインしたときには、**[ファブリック (Fabrics)]** セクションにはまだエントリーはありません。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。

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

フィールドについて説明します。

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

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

Add Fabric ✕

\* Fabric Name :

\* Fabric Template : Easy\_Fabric\_eBGP ▼

| General  | EVPN | vPC | Protocols | Advanced | Manageability | Bootstrap | Configuration Backup |
|--|------|-----|-----------|----------|---------------|-----------|----------------------|
| <p>* BGP ASN for Spines <input type="text"/> ⓘ 1-4294967295   1-65535[0-65535]</p> <p>* BGP AS Mode Multi-AS ⓘ Multi-AS: Unique ASN per Leaf/Border<br/>Dual-AS: One ASN for all Leafs/Borders</p> <p>* Underlay Subnet IP Mask 30 ⓘ Mask for Underlay Subnet IP Range</p> <p>Manual Underlay IP Address Allocation <input type="checkbox"/> ⓘ Checking this will disable Dynamic Underlay IP Address Allocations</p> <p>* Underlay Routing Loopback IP Range 10.2.0.0/22 ⓘ Typically Loopback0 IP Address Range</p> <p>* Underlay Subnet IP Range 10.4.0.0/16 ⓘ Address range to assign Numbered and Peer Link SVI IPs</p> <p>* Subinterface Dot1q Range 2-511 ⓘ Per Border Dot1q Range For VRF Lite Connectivity (Min:2, Max:4096)</p> <p>NX-OS Software Image Version <input type="text"/> ⓘ If Set, Image Version Check Enforced On All Switches. Images Can Be Uploaded From Control:Image Upload</p> |      |     |           |          |               |           |                      |

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

[スパインの BGP ASN (BGP ASN for Spines) ] : ファブリックのスパインスイッチの BGP AS 番号を入力します。

[BGP AS モード (BGP AS Mode) ] : [Multi-AS] または [Dual-AS] を選択します。

**Multi-AS** ファブリックでは、スパインスイッチには一意の BGP AS 番号があり、各リーフスイッチには一意の AS 番号があります。2つのリーフスイッチが vPC スイッチペアを形成している場合、それらは同じ AS 番号を持ちます。

[Dual-AS] ファブリックでは、スパインスイッチには一意の BGP AS 番号があり、リーフスイッチには一意の AS 番号があります。

ファブリックは、スパインスイッチの AS 番号によって識別されます。

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

[手動アンダーレイ IP アドレス割り当て (Manual Underlay IP Address Allocation) ] : [動的アンダーレイ IP アドレス割り当て (Dynamic Underlay IP Address Allocation) ] を無効にするには、このチェックボックスをオンにします。

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

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

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

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

イメージアップロードオプションを使用してCisco NX-OS ソフトウェアイメージをアップロードすると、アップロードされたイメージがこのフィールドにリストされます。イメージを選択する場合、スイッチのバージョンが選択されているかどうか、システムがチェックします。選択されていない場合、エラーメッセージが表示されます。[解決 (Resolve) ] をクリックすることで、エラーを解決できます。イメージ管理画面が表示され、ISSU オプションを処理できます。その代わりに、リリース ナンバーを削除した後で保存することも可能です。

このフィールドでイメージを指定する場合、ファブリックのすべてのスイッチはそのイメージを実行する必要があります。一部のデバイスでイメージが実行されない場合、指定されたイメージへのインサーブिस ソフトウェア アップグレード (ISSU) を実行するように警告するプロンプトが表示されます。すべてのデバイスが指定されたイメージを実行するまで、展開プロセスは完了しません。

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

4. [EVPN] をクリックします。[EVPN VXLAN オーバーレイを有効にする (Enable EVPN VXLAN Overlay) ] オプションを明示的に無効にする必要があります。このチェックボックスはデフォルトで有効になっている点に注意してください。このオプションは、顧客が eBGP アンダーレイ/オーバーレイ ベースの VXLAN EVPN ファブリックを構築することを望むユースケースでのみ有効にします。

| General  | EVPN | vPC  | Protocols | Advanced       | Manageability | Bootstrap | Configuration Backup |
|--|------|--|-----------|----------------|---------------|-----------|----------------------|
| Enable EVPN VXLAN Overlay <input type="checkbox"/> ⓘ |      |  |           |                |               |           |                      |
| * First Hop Redundancy Protocol                      |      | hsrp   |           | ⓘ HSRP or VRRP |               |           |                      |
| Anycast Gateway MAC                                  |      | ⓘ Shared MAC address for all leaves (xxxx.xxxx.xxxx)   |           |                |               |           |                      |
| Enable VXLAN OAM                                     |      | <input checked="" type="checkbox"/> ⓘ Enable the Next Generation (NG) OAM feature for all switches in the fabric to aid in trouble-shooting VXLAN EVPN fabrics |           |                |               |           |                      |
| Enable Tenant DHCP                                   |      | <input checked="" type="checkbox"/> ⓘ  |           |                |               |           |                      |
| vPC advertise-pip                                    |      | <input type="checkbox"/> ⓘ For Primary VTEP IP Advertisement As Next-Hop Of Prefix Routes  |           |                |               |           |                      |
| Replication Mode                                     |      | ⓘ Replication Mode for BUM Traffic   |           |                |               |           |                      |
| Multicast Group Subnet                               |      | ⓘ Multicast address with prefix 16 to 30   |           |                |               |           |                      |
| Enable Tenant Routed Multicast                       |      | <input type="checkbox"/> ⓘ For Overlay Multicast Support In VXLAN Fabrics  |           |                |               |           |                      |
| Default MDT Address for TRM VRFs                     |      | ⓘ IPv4 Multicast Address   |           |                |               |           |                      |
| Rendezvous-Points                                    |      | ⓘ Number of spines acting as Rendezvous-Point (RP)   |           |                |               |           |                      |
| RP Mode  |      | ⓘ Multicast RP Mode  |           |                |               |           |                      |
| Underlay RP Loopback Id                              |      | ⓘ (Min:0, Max:1023)  |           |                |               |           |                      |
| Underlay Primary RP Loopback Id                      |      | ⓘ Used for Bidir-PIM Phantom RP (Min:0, Max:1023)  |           |                |               |           |                      |
| Underlay Backup RP Loopback Id                       |      | ⓘ Used for Fallback Bidir-PIM Phantom RP (Min:0, Max:1023)   |           |                |               |           |                      |
| Underlay Second Backup RP Loopback Id                |      | ⓘ Used for second Fallback Bidir-PIM Phantom RP (Min:0, Max:1023)  |           |                |               |           |                      |
| Underlay Third Backup RP Loopback Id                 |      | ⓘ Used for third Fallback Bidir-PIM Phantom RP (Min:0, Max:1023)   |           |                |               |           |                      |
| VRF Template   |      | ⓘ Default Overlay VRF Template For Leafs   |           |                |               |           |                      |
| Network Template                                     |      | ⓘ Default Overlay Network Template For Leafs   |           |                |               |           |                      |

[ルーテッドファブリック (Routed Fabric) ] : ルーテッドファブリックでは、スパイン/リーフ ネットワーク間の IP 到達可能性が確立されると、選択したファースト ホップ ルーティング プロトコル (FHRP) として HSRP または VRRP を使用し、リーフ上に

ネットワークを簡単に作成して展開することができます。詳細については、[ルーテッドファブリックのネットワークの概要, on page 31](#)を参照してください。

eBGP ルーテッドファブリックを作成すると、ファブリックは eBGP をコントロールプレーンとして使用して、ファブリック内接続を構築します。スパインスイッチとリーフスイッチ間のリンクは、eBGP ピアリングがその上に構築される、ポイントツーポイント (p2p) 番号付き IP アドレスで自動構成されます。

Routed\_Network\_Universal テンプレートは、ルーテッドファブリックにのみ適用されることに注意してください。

[ファースト ホップ冗長性プロトコル (First Hop Redundancy Protocol) ] : FHRP プロトコルを指定します。hsrp または vrrp のいずれかを選択します。このフィールドは、ルーテッドファブリックにのみ適用されます。



#### Note

- ネットワークの作成後に、このファブリック設定を変更することはできません。変更する場合は、すべてのネットワークを削除してから、FHRP 設定を変更する必要があります。
- [EVPN] タブセクションの残りのフィールドは、EVPN VXLAN オーバーレイを有効にする場合にのみ適用されます。

#### 5. [vPC] をクリックします。このタブのフィールドは次のとおりです。

| General | EVPN | vPC                                    | Protocols                               | Advanced  | 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               | <input type="text" value="360"/>        | ① Auto Recovery Time In Seconds (Min:240, Max:3600)                         |               |           |                      |
|         |      | * vPC Delay Restore Time               | <input type="text" value="150"/>        | ① vPC Delay Restore Time For vPC links in seconds (Min:1, Max:3600)         |               |           |                      |
|         |      | vPC Peer Link Port Channel Number      | <input type="text" value="500"/>        | ① Port Channel ID for vPC Peer Link (Min:1, Max:4096)                       |               |           |                      |
|         |      | vPC IPv6 ND Synchronize                | <input checked="" type="checkbox"/>     | ① Enable IPv6 ND synchronization between vPC peers                          |               |           |                      |
|         |      | Fabric wide vPC Domain Id              | <input type="checkbox"/>                | ① Enable to use same vPC Domain Id on all vPC pairs in the fabric           |               |           |                      |
|         |      | vPC Domain Id                          | <input type="text"/>                    | ① vPC Domain Id to be used on all vPC pairs in the fabric                   |               |           |                      |
|         |      | 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) ] : 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

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

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

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

**[vPC ピア リンク ポートチャンネル番号 (vPC Peer Link Port Channel Number)]** : 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。

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

6. **[プロトコル (Protocols)]** タブをクリックします。このタブのフィールドは次のとおりです。

| General  | EVPN | vPC | Protocols | Advanced | Manageability | Bootstrap | Configuration Backup |
|--|------|-----|-----------|----------|---------------|-----------|----------------------|
| * Routing Loopback Id <input type="text" value="0"/> ⓘ (Min:0, Max:1023)                                   |      |     |           |          |               |           |                      |
| VTEP Loopback Id <input type="text"/> ⓘ (Min:0, Max:1023)  |      |     |           |          |               |           |                      |
| * BGP Maximum Paths <input type="text" value="4"/> ⓘ (Min:1, Max:64)                                       |      |     |           |          |               |           |                      |
| Enable BGP Authentication <input type="checkbox"/> ⓘ   |      |     |           |          |               |           |                      |
| BGP Authentication Key Encryption Type <input type="text"/> ⓘ BGP Key Encryption Type: 3 - 3DES, 7 - Cisco |      |     |           |          |               |           |                      |
| BGP Authentication Key <input type="text"/> ⓘ Encrypted BGP Authentication Key based on type               |      |     |           |          |               |           |                      |
| Enable PIM Hello Authentication <input type="checkbox"/> ⓘ   |      |     |           |          |               |           |                      |
| PIM Hello Authentication Key <input type="text"/> ⓘ 3DES Encrypted   |      |     |           |          |               |           |                      |
| Enable BFD <input type="checkbox"/> ⓘ  |      |     |           |          |               |           |                      |
| Enable BFD For BGP <input type="checkbox"/> ⓘ  |      |     |           |          |               |           |                      |
| Enable BFD Authentication <input type="checkbox"/> ⓘ   |      |     |           |          |               |           |                      |
| BFD Authentication Key ID <input type="text"/> ⓘ   |      |     |           |          |               |           |                      |
| BFD Authentication Key <input type="text"/> ⓘ Encrypted SHA1 secret value                                  |      |     |           |          |               |           |                      |

**[ルーティング ループバック ID (Routing Loopback Id)]** : ループバック インターフェイス ID は、デフォルトで 0 として設定されます。BGP ルータ ID として使用されます。

**[BGP 最大パス (BGP Maximum Paths)]** : BGP 最大パスを指定します。

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

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

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



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

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

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

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

```
feature bfd
```



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

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

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

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

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

**[BFD 認証キー ID (BFD Authentication Key ID)]** : インターフェイス認証の BFD 認証キー ID を指定します。

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

BFD 認証パラメータを取得する方法については、『Cisco DCNM LAN ファブリック構成ガイド』の「暗号化された BFD 認証キーの取得」を参照してください。

7. [Advanced] タブをクリックします。このタブのフィールドは次のとおりです。

| General  | EVPN | vPC | Protocols | Advanced | Manageability | Bootstrap | Configuration Backup |
|--|------|-----|-----------|----------|---------------|-----------|----------------------|
| * Intra Fabric Interface MTU <input type="text" value="9216"/> ⓘ (Min:576, Max:9216). Must be an even number   |      |     |           |          |               |           |                      |
| * Layer 2 Host Interface MTU <input type="text" value="9216"/> ⓘ (Min:1500, Max:9216). Must be an even number  |      |     |           |          |               |           |                      |
| * Power Supply Mode <input type="text" value="ps-redundant"/> ⓘ Default Power Supply Mode For The Fabric   |      |     |           |          |               |           |                      |
| * CoPP Profile <input type="text" value="strict"/> ⓘ Fabric Wide CoPP Policy, Customized CoPP policy should be separately defined, when 'manual' is selected                                   |      |     |           |          |               |           |                      |
| VTEP HoldDown Time <input type="text"/> ⓘ NVE Source Interface HoldDown Time (Min:1, Max:1500) in seconds  |      |     |           |          |               |           |                      |
| * VRF Lite Subnet IP Range <input type="text" value="10.33.0.0/16"/> ⓘ Address range to assign P2P DCI Links   |      |     |           |          |               |           |                      |
| * VRF Lite Subnet Mask <input type="text" value="30"/> ⓘ Mask for Subnet Range (Min:8, Max:31)   |      |     |           |          |               |           |                      |
| Enable CDP for Bootstrapped Switch <input type="checkbox"/> ⓘ Enable CDP on management interface   |      |     |           |          |               |           |                      |
| Enable NX-API <input checked="" type="checkbox"/> ⓘ Enable NX-API on port 443  |      |     |           |          |               |           |                      |
| Enable NX-API on HTTP port <input checked="" type="checkbox"/> ⓘ Enable NX-API on port 80  |      |     |           |          |               |           |                      |
| Enable Strict Config Compliance <input type="checkbox"/> ⓘ Enable bi-directional compliance checks to flag additional configs in the running config that are not in the intent/expected config |      |     |           |          |               |           |                      |
| Enable AAA IP Authorization <input type="checkbox"/> ⓘ Enable only, when IP Authorization is enabled in the AAA Server   |      |     |           |          |               |           |                      |
| Enable DCNM as Trap Host <input checked="" type="checkbox"/> ⓘ Configure DCNM as a receiver for SNMP traps   |      |     |           |          |               |           |                      |
| Enable TCAM Allocation <input checked="" type="checkbox"/> ⓘ TCAM commands are automatically generated for VxLAN and vPC Fabric Peering when Enabled   |      |     |           |          |               |           |                      |
| * Greenfield Cleanup Option <input type="text" value="Disable"/> ⓘ Switch Cleanup Without Reload When PreserveConfig=no  |      |     |           |          |               |           |                      |
| Enable Default Queuing Policies <input type="checkbox"/> ⓘ   |      |     |           |          |               |           |                      |
| N9K Cloud Scale Platform Queuing Policy <input type="text"/> ⓘ Queuing Policy for all 92xx, -EX, -FX, -FX2, -FX3, -GX series switches in the fabric  |      |     |           |          |               |           |                      |
| N9K R-Series Platform Queuing Policy <input type="text"/> ⓘ Queuing Policy for all R-Series switches in the fabric   |      |     |           |          |               |           |                      |
| Other N9K Platform Queuing Policy <input type="text"/> ⓘ Queuing Policy for all other switches in the fabric   |      |     |           |          |               |           |                      |
| Enable MACsec <input type="checkbox"/> ⓘ Enable MACsec in the fabric   |      |     |           |          |               |           |                      |

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

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

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

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

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

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

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

[HTTP での NX-API の有効化 (Enable NX-API on HTTP) ] : HTTP での NX-API の有効化を指定します。HTTP を使用するには、[NX-API の有効化 (Enable NX-API) ] チェック

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~L7 サービス)、VXLAN OAM など、NX-API を使用し、Cisco DCNM がサポートするアプリケーションは、HTTP ではなく HTTPS の使用を開始します。



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

[厳密な構成コンプライアンスの有効化 (Enable Strict Config Compliance)] : このチェックボックスをオンにして、厳密な構成コンプライアンス機能を有効にします。

厳密な構成コンプライアンスについては、*Enhanced Monitoring and Monitoring Fabrics Guide* を参照してください。



**Note** ファブリックで厳密な構成コンプライアンスが有効になっている場合、Cisco DCNM のリソースで Network Insights を展開することはできません。

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

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

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

[グリーンフィールドクリーンアップオプション (Greenfield Cleanup Option)] : スイッチをリロードせずにスイッチのグリーンフィールドクリーンアップオプションを有効にします。このオプションは、通常、Cisco Nexus 9000v スイッチを使用するデータセンター環境でのみ推奨されます。

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

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

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

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

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

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

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

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

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

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

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

| General                | EVPN | vPC | Protocols | Advanced | Manageability | Bootstrap            | Configuration Backup   |
|------------------------|------|-----|-----------|----------|---------------|----------------------|--|
| DNS Server IPs         |      |     |           |          |               | <input type="text"/> | ? Comma separated list of IP Addresses(v4/v6)  |
| DNS Server VRFs        |      |     |           |          |               | <input type="text"/> | ? One VRF for all DNS servers or a comma separated list of VRFs, one per DNS server  |
| NTP Server IPs         |      |     |           |          |               | <input type="text"/> | ? Comma separated list of IP Addresses(v4/v6)  |
| NTP Server VRFs        |      |     |           |          |               | <input type="text"/> | ? One VRF for all NTP servers or a comma separated list of VRFs, one per NTP server  |
| Syslog Server IPs      |      |     |           |          |               | <input type="text"/> | ? Comma separated list of IP Addresses(v4/v6)  |
| Syslog Server Severity |      |     |           |          |               | <input type="text"/> | ? Comma separated list of Syslog severity values, one per Syslog server (Min:0, Max:7)   |
| Syslog Server VRFs     |      |     |           |          |               | <input type="text"/> | ? One VRF for all Syslog servers or a comma separated list of VRFs, one per Syslog server  |
| AAA Freeform Config    |      |     |           |          |               | <input type="text"/> | ? Note ! All configs should strictly match 'show run' output, with respect to case and newlines. Any mismatches will yield unexpected diffs during deploy. |

このタブのフィールドは次のとおりです。

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

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

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

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

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

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

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

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

ファブリック設定で AAA 構成が指定されている場合は、**switch\_freeform** PTI で、ソースが **UNDERLAY\_AAA**、説明が **AAA Configurations** であるものが作成されます。

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

| General  | EVPN | vPC | Protocols | Advanced | Manageability | Bootstrap | Configuration Backup |
|--|------|-----|-----------|----------|---------------|-----------|----------------------|
| <p><b>Enable Bootstrap</b> <input type="checkbox"/> <small>Automatic IP Assignment For POAP</small></p> <p>Enable Local DHCP Server <input type="checkbox"/> <small>Automatic IP Assignment For POAP From Local DHCP Server</small></p> <p>DHCP Version <input type="text"/></p> <p>DHCP Scope Start Address <input type="text"/> <small>Start Address For Switch Out-of-Band POAP</small></p> <p>DHCP Scope End Address <input type="text"/> <small>End Address For Switch Out-of-Band POAP</small></p> <p>Switch Mgmt Default Gateway <input type="text"/> <small>Default Gateway For Management VRF On The Switch</small></p> <p>Switch Mgmt IP Subnet Prefix <input type="text"/> <small>(Min:8, Max:30)</small></p> <p>Switch Mgmt IPv6 Subnet Prefix <input type="text"/> <small>(Min:64, Max:126)</small></p> <p>Enable AAA Config <input type="checkbox"/> <small>Include AAA configs from Manageability tab during device bootup</small></p> <p>Bootstrap Freeform Config <input type="text"/> <small>Note ! All configs should strictly match 'show run' output, with respect to case and newlines. Any mismatches will yield unexpected diffs during deploy.</small></p> <p>DHCPv4/DHCPv6 Multi Subnet Scope <input type="text"/> <small>Enter One Subnet Scope per line. Start_IP, End_IP, Gateway, Prefix e.g. 10.6.0.2, 10.6.0.9, 10.6.0.1, 24 10.7.0.2, 10.7.0.9, 10.7.0.1, 24 Or 21:0:1:1::10, 21:0:1:1::20, 21:0:1:1::1, 64 21:0:1:2::10, 21:0:1:2::20, 21:0:1:2::1, 64</small></p> |      |     |           |          |               |           |                      |

**[ブートストラップの有効化 (Enable Bootstrap)]** : このチェックボックスを選択し、ブートストラップ機能を有効にします。

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

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

**ローカル DHCP サーバの有効化 (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、DCNM は自動 IP アドレス割り当てにリモートまたは外部 DHCP サーバを使用します。

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



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

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

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

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

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

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

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

[ブートストラップ フリーフォームの構成 (Bootstrap Freeform Config)]: (オプション) 必要に応じて追加のコマンドを入力します。たとえば、AAA またはリモート認証関連の構成を使用している場合は、このフィールドにこれらの構成を追加してインテントを保存する必要があります。デバイスが起動すると、[Bootstrap Freeform Config] フィールドで定義されたインテントが含まれます。

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

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

スコープの形式は次の順で定義する必要があります。

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

例 : 10.6.0.2、10.6.0.9、16.0.0.1、24

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

General | EVPN | vPC | Protocols | Advanced | Manageability | Bootstrap | **Configuration Backup**

Hourly Fabric Backup  ? Backup hourly or on Re-sync only if there is any config deployment since last backup

Scheduled Fabric Backup  ? Backup at the specified time only if there is any config deployment since last backup

Scheduled Time  ? Time in 24hr format. (00:00 to 23:59)

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

新しいファブリック設定とインテントの1時間ごとのバックアップを有効にできます。前の時間に構成のプッシュがある場合、DCNM はバックアップを取得します。

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

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

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

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

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



- Note** 1 時間ごと、およびスケジュールされたバックアッププロセスは、次の定期的な構成コンプライアンス アクティビティ中のみ発生し、最大 1 時間の遅延が発生する可能性があります。即時バックアップをトリガーするには、次の手順を実行します。
- a. **[制御 (Control) ] > [ファブリック ビルダ (Fabric Builder) ]** を選択します。[Fabric Builder] 画面が表示されます。
  - b. 特定のファブリック ボックス内をクリックします。[ファブリック トポロジ (fabric topology)] 画面が表示されます。
  - c. 画面左側の **[アクション (Actions) ]** パネルで、**[ファブリックの再同期 (Re-Sync Fabric) ]** をクリックします。

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

関連情報を入力して更新したら、[保存 (Save) ] をクリックします。

### 特筆すべき点

- すべてのリーフスイッチには共通の AS 番号があるため、リーフ アンダーレイ ポリシーを一度にすべてのリーフスイッチに展開します。
- ブラウンフィールド移行は、eBGP ファブリックではサポートされていません。
- リーフスイッチの AS 番号は、作成後に再計算と展開 (Recalculate & Deploy) 操作を実行した後は変更できません。変更が必要になった場合は、**leaf\_bgp\_asn** ポリシーを削除し、再計算と展開 (Recalculate & Deploy) 操作を実行して、この AS に関連する BGP 構成を削除する必要があります。次に、新しい AS 番号を使用して、**leaf\_bgp\_asn** ポリシーを追加できます。
- Multi-AS モードと Dual-AS モードを切り替える場合は、モードを変更する前に、手動で追加されたすべての BGP ポリシー (リーフスイッチの **Leaf\_bgp\_asn** および **ebgp** オーバーレイ ポリシーを含む) を削除し、[保存と展開 (Save & Deploy) ] 操作を実行します。
- サポートされているロールは、リーフ、スパイン、ボーダー リーフです。
- ボーダー デバイスでは、VRF-Lite は手動モードでサポートされます。
- 機能ファブリックのリーフスイッチとスパインスイッチにポリシーを適用する必要があります。

## ファブリックへのスイッチの追加

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

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

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



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

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

## 既存のスイッチの検出

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



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

## 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)

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

Discover Existing Switches
PowerOn Auto Provisioning (POAP)

Discovery Information >
 Scan Details >

← Back
Import into fabric

| <input type="checkbox"/> | Name         | IP Address    | Model       | Version     | Status          | Progress |
|--------------------------|--------------|---------------|-------------|-------------|-----------------|----------|
| <input type="checkbox"/> | EVPN-Spine81 | 172.23.244.81 | N9K-C931... | 7.0(3)I5(2) | Unknown User... |          |
| <input type="checkbox"/> | leaf-91      | 172.23.244.91 | N9K-C939... | 7.0(3)I7(3) | manageable      |          |
| <input type="checkbox"/> | switch       | 172.23.244.88 | N9K-C937... | 7.0(3)I7(1) | not reachable   |          |
| <input type="checkbox"/> | EVPN-Spine85 | 172.23.244.85 | N9K-C939... | 7.0(3)I5(2) | Unknown User... |          |

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

Inventory Management ✕

Discover Existing Switches PowerOn Auto Provisioning (POAP)

Discovery Information > Scan Details >

← Back 2  
Import into fabric

| <input type="checkbox"/>            | Name         | IP Address    | Model       | Version     | Status          | Progress |
|-------------------------------------|--------------|---------------|-------------|-------------|-----------------|----------|
| <input type="checkbox"/>            | EVPN-Spine81 | 172.23.244.81 | N9K-C931... | 7.0(3)I5(2) | Unknown User... |          |
| <input checked="" type="checkbox"/> | leaf-91      | 172.23.244.91 | N9K-C939... | 7.0(3)I7(3) | manageable      |          |
| <input type="checkbox"/>            | Switch       | 172.23.244.88 | N9K-C937... | 7.0(3)I7(1) | not reachable   |          |
| <input type="checkbox"/>            | EVPN-Spine85 | 172.23.244.85 | N9K-C939... | 7.0(3)I5(2) | Unknown User... |          |

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

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



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

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

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



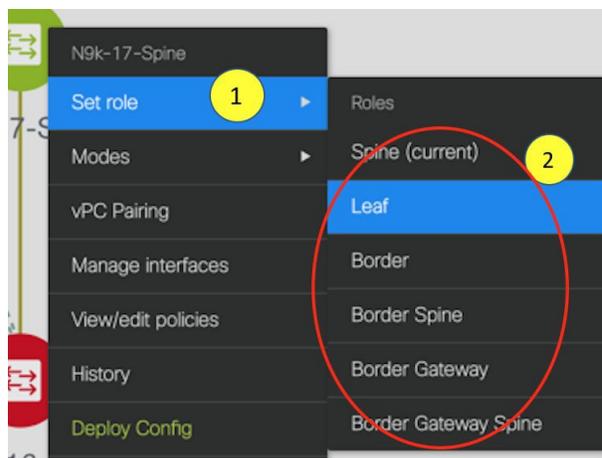
**Note** スwitchの検出中に次のエラーが発生することがあります。

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

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



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



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

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

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

Cisco DCNM を使用して新しい vPC ペアが正常に作成および展開されると、コマンドがスイッチに存在する場合でも、**no ip redirects CLI** のいずれかのピアが同期しなくなることがあります。この非同期は、実行構成で CLI を表示するためのスイッチの遅延が原因で発生

し、構成のコンプライアンスに相違が生じます。[構成の展開 (Config Deployment)] ウィンドウでスイッチを再同期して、差分を解決します。

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

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

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

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

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

### Config Deployment ✕

| Step 1. Configuration Preview > |            | Step 2. Configuration Deployment Status > |                |             |         |          |
|---------------------------------|------------|---|----------------|-------------|---------|----------|
| Switch Name                     | IP Address | Switch Serial                             | Preview Config | Status      | Re-sync | Progress |
| N9K-2-Leaf                      | 111.0.0.92 | SAL18422FVP                               | 0 lines        | In-sync     |         | 100%     |
| N9K-4-BGW                       | 111.0.0.94 | FDO20260UEK                               | 20 lines       | Out-of-sync |         | 100%     |
| N9K-3-BGW                       | 111.0.0.93 | FDO20291AVQ                               | 20 lines       | Out-of-sync |         | 100%     |
| N9K-1-Spine                     | 111.0.0.91 | SAL18432P2T                               | 0 lines        | In-sync     |         | 100%     |

Deploy Config

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

[再同期 (Re-sync)] 列のスイッチごとに [再同期 (Re-sync)] ボタンが表示されます。大規模なアウトオブバンド変更がある場合、または設定変更が DCNM に正しく登録されていない場合に、このオプションを使用して DCNM 状態を再同期します。再同期操作は、

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

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

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

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

DCNM 11 では、複数行のバナー motd 構成がサポートされています。マルチラインバナー motd 構成は、**switch\_freeform** を使用するスイッチごと、またはリーフ/スパイン自由形式構成を使用するファブリックごとのいずれかで、自由形式の構成ポリシーを使用して Cisco DCNM で構成できます。複数行のバナー motd が構成された後、ファブリック トポロジ画面 (の右上) で [保存と展開 (Save & Deploy)] オプションを実行して、ポリシーを展開します。そうしないと、ポリシーがスイッチに適切に展開されない可能性があります。バナーポリシーは、単一行のバナー設定のみを設定します。また、自由形式の設定/ポリシーに関連するバナーは1つだけ作成できます。バナー motd を構成するための複数のポリシーはサポートされていません。

#### 7. 画面 を閉じます。

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

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

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

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



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

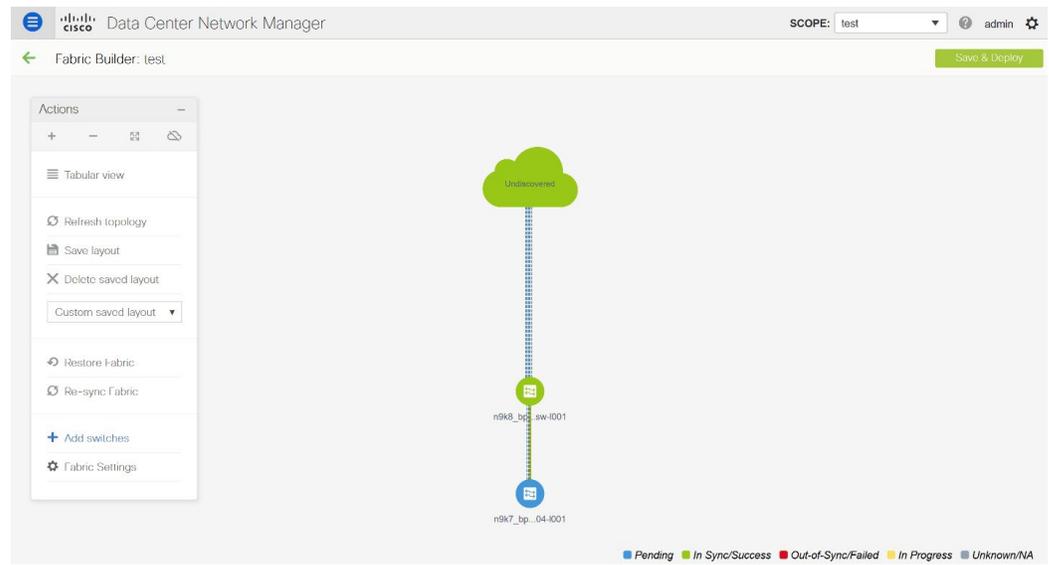
スイッチのリロードまたはRMA操作の後にリーフスイッチが起動すると、DCNMは、スイッチとそれに接続されている FEX デバイスの構成をプロビジョニングします。DCNM が FEX (ホスト インターフェイス) 構成をプロビジョニングした後に FEX 接続が起動し、構成が一致しない場合があります。不一致を解決するには、ファブリック トポロジ画面で **[保存と展開 (Save & Deploy)]** を再度クリックします。

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

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

## 新しいスイッチの検出

1. 新しい Cisco NX-OS デバイスの電源がオンになると、通常、そのデバイスにはスタートアップ構成も構成ステートもありません。その結果、NX-OS で電源が投入され、初期化後に POAP ループに入ります。デバイスは、`mgmt0` インターフェイスを含むアップ状態のすべてのインターフェイスで DHCP 要求の送信を開始します。
2. デバイスと DCNM の間に IP 到達可能性がある限り、デバイスからの DHCP 要求は DCNM に転送されます。ゼロデイデバイスを簡単に起動するには、前述のように、**ファブリック設定**でブートストラップ オプションを有効にする必要があります。
3. ファブリックに対してブートストラップが有効になっている場合、デバイスからの DHCP 要求は DCNM によって処理されます。DCNM によってデバイスに割り当てられた一時 IP アドレスは、デバイス モデル、デバイス NX-OS バージョンなどを含むスイッチに関する基本情報を学習するために使用されます。
4. DCNM GUI で、ファブリックに移動します (**[制御 (Control)]** > **[ファブリック ビルダ (Fabric Builder)]** をクリックし、ファブリックをクリックします)。ファブリック トポロジが表示されます。



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

5. [POAP] タブをクリックします。

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



**Note**

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

## Inventory Management



Discover Existing Switches

PowerOn Auto Provisioning (POAP)

*ⓘ Please note that POAP can take anywhere between 5 and 15 minutes to complete!*

Bootstrap

| <input type="checkbox"/> | Serial Number | Model | Version | IP Address | Hostname | Gateway |
|--------------------------|---------------|-------|---------|------------|----------|---------|
| No Data available        |               |       |         |            |          |         |

Close

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

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

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

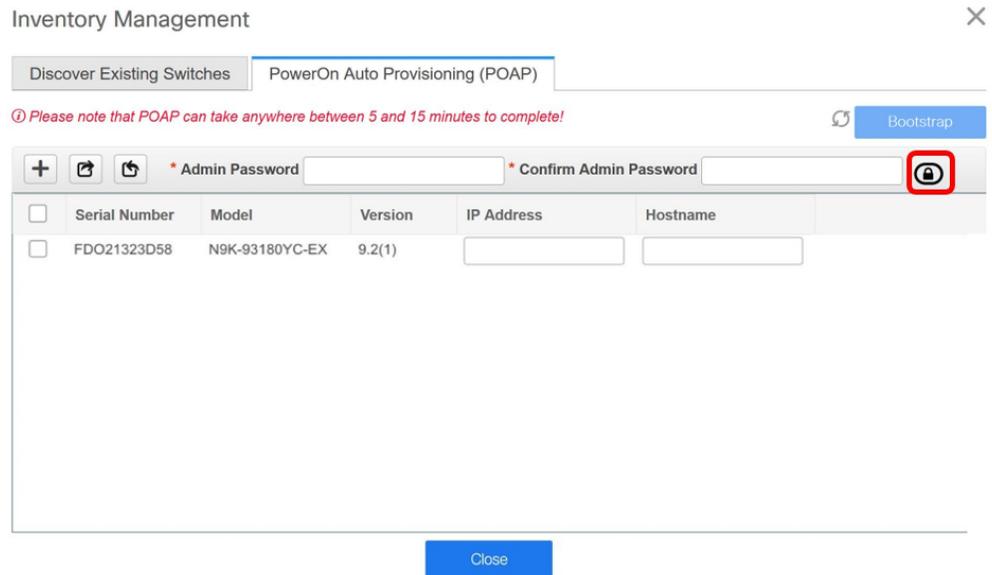
- [管理者パスワード (Admin Password)]** フィールドと **[管理者パスワードの確認 (Confirm Admin Password)]** フィールドに、新しいパスワードを入力します。

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

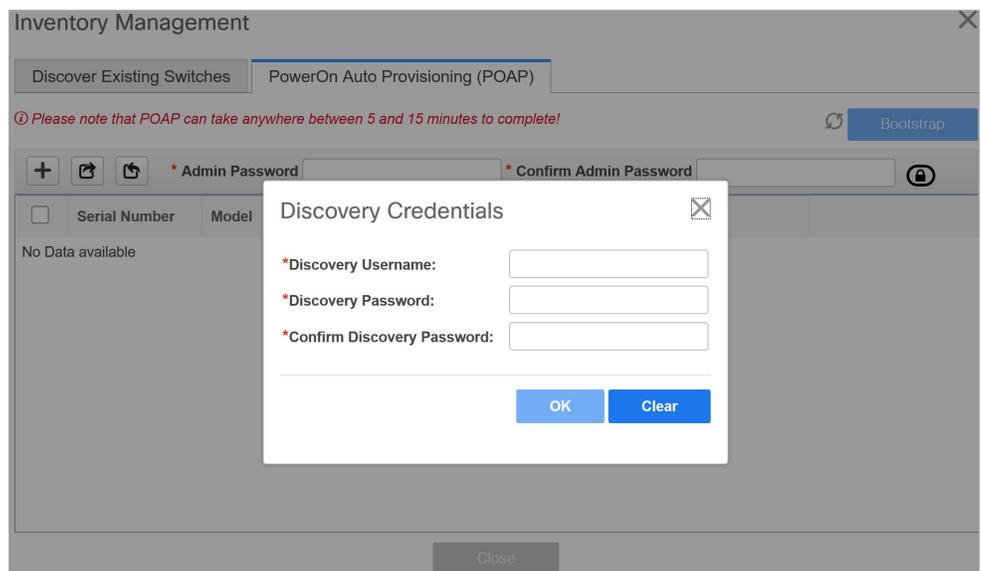


**Note** 管理者クレデンシャルを使用してスイッチを検出しない場合は、代わりに AAA 認証 (RADIUS または TACACS クレデンシャル) を使用できます。

- (任意) スwitchの検出に検出クレデンシャルを使用します。
  - [ディスカバリ クレデンシャルの追加 (Add Discovery Credentials)]** アイコンをクリックして、スイッチのディスカバリ クレデンシャルを入力します。



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



[OK] をクリックして、ディスカバリ クレデンシャルを保存します。

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

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

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

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



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

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

11. 保留中の設定が展開されると、すべてのスイッチの [進捗 (Progress)] 列に 100% と表示されます。
12. [閉じる (Close)] をクリックして、ファブリック ビルダ トポロジに戻ります。
13. [トポロジの更新 (Refresh Topology)] をクリックして、更新を表示します。すべてのスイッチは、機能していることを示す緑色でなければなりません。
14. スイッチとリンクが DCNM で検出されます。設定は、さまざまなポリシー (ファブリック、トポロジ、スイッチ生成ポリシーなど) に基づいて構築されます。スイッチイメージ (およびその他の必要な) 設定がスイッチで有効になっている。
15. DCNM GUI では、検出されたスイッチは スタンドアロン ファブリック トポロジで確認できます。このステップまでで、POAP は基本設定で完了します。追加構成を行うには、[制御 (Control)] > [インターフェイス (Interfaces)] オプションを使用してインターフェイスを設定する必要があります。以下が含まれますが、これらに限定されません。
  - vPC ペアリング。
  - ブレークアウト インターフェイス。
  - ポートチャネル、およびポートへのメンバーの追加。

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

## Fabric errors &amp; warnings



0 Errors, 2 Warnings, 0 Info

Delete all

**Warning** The Secondary IP address of the NVE source interface has been modified for switch SN [FDO20260UEK] and peer SN [FDO20291AVQ] due to vpc feature configuration. Please make sure to shut/noshut the nve interfaces from DCNM Interface Manager Screen.

Severity warning

Category Fabric

Entity type Fabric\_Template

Entity name configSave:vpcPairing:FDO20260UEK:FDO20291AVQ

Reported less than a minute ago 2019-03-17 09:30:00

Details [2]: [vpcPairing:FDO20260UEK:FDO20291AVQ]. Line/Col:[0/0]. Msg = [The Secondary IP address of the NVE source interface has been modified for switch SN [FDO20260UEK] and peer SN [FDO20291AVQ] due to vpc feature configuration. Please make sure to shut/noshut the nve interfaces from DCNM Interface Manager Screen.]

**Warning** The Secondary IP address of the NVE source interface has been modified for switch SN [FDO20291AVQ] and peer SN [FDO20260UEK] due to vpc feature configuration. Please make sure to shut/noshut the nve interfaces from DCNM Interface Manager Screen.

Severity warning

Category Fabric

Entity type Fabric\_Template

Entity name configSave:vpcPairing:FDO20291AVQ:FDO20260UEK

Reported less than a minute ago 2019-03-17 09:30:00

Details [1]: [vpcPairing:FDO20291AVQ:FDO20260UEK]. Line/Col:[0/0]. Msg = [The Secondary IP address of the NVE source interface has been modified for switch SN [FDO20291AVQ] and peer SN [FDO20260UEK] due to vpc feature configuration. Please make sure to shut/noshut the nve interfaces from DCNM Interface Manager Screen.]

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

## Interfaces

|                                     | Device Name | Name         | Admin | Oper | Reason            |
|-------------------------------------|-------------|--------------|-------|------|-------------------|
| <input type="checkbox"/>            | N9K-2-Leaf  | Ethernet2/6  |       |      | XCVR not inserted |
| <input type="checkbox"/>            | N9K-2-Leaf  | Ethernet2/7  |       |      | XCVR not inserted |
| <input type="checkbox"/>            | N9K-2-Leaf  | Ethernet2/8  |       |      | XCVR not inserted |
| <input type="checkbox"/>            | N9K-2-Leaf  | Ethernet2/9  |       |      | XCVR not inserted |
| <input type="checkbox"/>            | N9K-2-Leaf  | Ethernet2/10 |       |      | XCVR not inserted |
| <input type="checkbox"/>            | N9K-2-Leaf  | Ethernet2/11 |       |      | XCVR not inserted |
| <input type="checkbox"/>            | N9K-2-Leaf  | Ethernet2/12 |       |      | XCVR not inserted |
| <input checked="" type="checkbox"/> | N9K-2-Leaf  | nve1         |       |      | ok                |

スイッチを右クリックすると、さまざまなオプションを表示できます。

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



#### Note

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

- **モード**：メンテナンス モードとアクティブ/操作モード。
- **vPC ペアリング**：vPC のスイッチを選択し、そのピアを選択します。  
vPC ペアの仮想リンクを作成するか、既存の物理リンクをvPC ペアの仮想リンクに変更できます。
- **インターフェイスの管理**：スイッチ インターフェイスに構成を展開します。
- **ポリシーの表示/編集**：スイッチ ポリシーを参照し、必要に応じて編集します。
- **履歴**：スイッチの展開およびポリシーの変更履歴を表示します。

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

History for mini-leaf2(FDO21332E6X)

Deployment History Policy Change History

| Policy ID        | Template             | Description | PTI Operation | Generated Config                 | Entity Name     | Entity Type    | User  | Created On          |
|------------------|----------------------|-------------|---------------|----------------------------------|-----------------|----------------|-------|---------------------|
| PROFILE-VRF-1    | Default_VRF_Exten... |             | UPDATE        | <a href="#">Detailed History</a> | MyVRF_50000     | Config_Profile | admin | 2020/05/31-08:15:21 |
| PROFILE-VRF-1    | Default_VRF_Exten... |             | ADD           | <a href="#">Detailed History</a> | MyVRF_50000     | Config_Profile | admin | 2020/05/31-08:13:44 |
| PROFILE-NETWO... | Default_Network_E... |             | ADD           | <a href="#">Detailed History</a> | MyNetwork_30... | Config_Profile | admin | 2020/05/31-08:13:43 |

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

## Generated Config Details for FDO22471AXH



Generated Config Before

Generated Config After

hostname es-leaf1

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

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



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

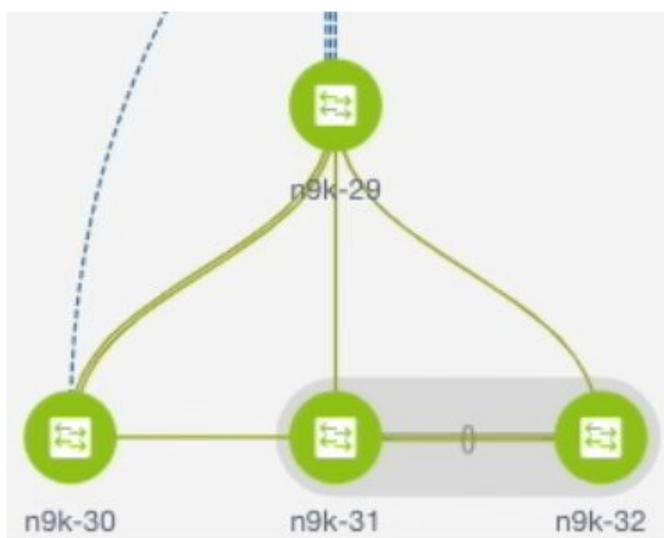
- **[構成のプレビュー (Preview Config)]** : 保留中の構成と、実行中の構成と予想される構成の比較を表示します。
- **展開構成** - スイッチ構成ごとに展開します。

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

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

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

## ファブリックアンダーレイ eBGP ポリシーの展開



このトポロジは、到達可能性情報を配信するためのルーティングプロトコルとして eBGP が有効になっているルーテッドファブリックを示しています。DCNM では、[[Easy\\_Fabric\\_eBGP](#)] テンプレートを持つファブリックが作成されます。1つのスパインスイッチ (n9k-29) と3つのリーフスイッチ (n9k-30、および vPC スイッチペア : n9k-31 と n9k-32) がインポートされています。

ファブリックには次の2種類があります。

- **マルチ AS モードファブリックの作成**：マルチ AS モードファブリックでは、スパインスイッチには共通の BGP AS 番号があり、各リーフスイッチには一意の BGP AS 番号があります。Dual-AS から Multi-AS モードへのファブリック変換にも同じ手順を使用します。

- **[Dual-AS モード ファブリックの作成 (Creating a Dual-AS mode fabric)]** : Dual-AS モードファブリックの作成については、別の手順が説明されています。Multi-AS から Dual-AS モードへのファブリック変換にも同じ手順を使用します。

Dual-AS ファブリックでは、すべてのスパインスイッチには共通の BGP AS 番号があり、すべてのリーフスイッチには共通の BGP AS 番号があります (スパインスイッチの BGP AS 番号とは異なります)。次のセクションで説明するように、ポリシーを展開する必要があります。

ファブリックアンダーレイ eBGP ポリシーを展開するには、各リーフスイッチに **leaf\_bgp\_asn** ポリシーを手動で追加して、スイッチで使用される BGP AS 番号を指定する必要があります。後ほど **[保存と展開 (Save & Deploy)]** 操作を実施すると、リーフスイッチとスパインスイッチ間の物理インターフェイス上に eBGP ピアリングが生成され、アンダーレイの到達可能性情報が交換されます。

1. 画面左側の **[表形式ビュー (Tabular View)]** をクリックします。 **Switches | Links** 画面が表示されます。
2. リーフスイッチ (たとえば、n9k-30 チェックボックス) を選択し、**[ポリシーの表示/編集 (View/Edit Policies)]** をクリックします。 **[ポリシーの表示/編集 (View/edit policies)]** 画面が表示されます。



(注) Dual-AS モードで eBGP ファブリックを作成する場合 (または Multi-AS モードから Dual-AS モードに変更する場合)、すべてのリーフスイッチを選択します。これは、共通の BGP AS 番号があるためです。

3. **[追加 (Add)]** をクリックします。 **[ポリシーの追加 (Add Policy)]** 画面が表示されます。
4. **[ポリシー (Policy)]** ドロップダウンボックスから、 **leaf\_bgp\_asn** を選択し、 **[BGP AS #]** フィールドに BGP AS 番号を入力します。
5. **[保存 (Save)]** をクリックします。
6. vPC スイッチに対してこの手順を繰り返します。vPC スイッチ ペアの場合は、両方のスイッチを選択し、 **leaf\_bgp\_asn** ポリシーを適用します。



(注) 前の手順で説明したように、Dual-AS モードでファブリックを作成 (または Dual-AS モードに変換) し、それらすべてに BGP AS 番号を割り当てている場合、この手順は必要ありません。

7. **[ポリシーの表示/編集 (View/Edit Policies)]** ウィンドウを閉じます
8. トポロジ画面で、画面の右上にある **[保存と展開 (Save & Deploy)]** をクリックします。
9. **構成展開** ウィザードに従って構成を展開します。

# eBGP ベースのファブリックにおけるネットワークの展開

## ルーテッドファブリックのネットワークの概要

Cisco DCNM リリース 11.3(1) 以降、DCNM を使用して、ルーテッドファブリックのトップダウン ネットワーク構成を作成できます。ルーテッドファブリックは、1つの VRF で実行されます。これがデフォルトの VRF です。ルーテッドファブリックでは、VRF の手動作成は無効になっていることに注意してください。ファブリックは IPv4 ファブリックであるため、ネットワーク内の IPv6 アドレスはサポートされていません。ルーテッドファブリックでは、レイヤ2のみのネットワークでない限り、ネットワークは1つのデバイスまたは vPC デバイスのペアにのみアタッチできます。



**Note** ルーテッドファブリック ネットワークの構成は、config-profile の下に置かれません。

eBGP ファブリックがルーテッドファブリック（EVPN が無効）として構成されている場合、ファブリックレベルで、ホストトラフィックのファーストホップ冗長性プロトコル（FHRP）として HSRP または VRRP のいずれかを選択できます。HSRP がデフォルト値です。

vPC ペアの場合、DCNM はファブリック設定に基づいてネットワーク レベルで HSRP または VRRP 構成を生成します。HSRP を選択した場合、各ネットワークは1つの HSRP グループと HSRP VIP アドレスを持つように構成されます。デフォルトでは、すべてのネットワークは DCNM によって割り当てられた同じ HSRP グループ番号を共有しますが、これはネットワークごとに上書きできます。VRRP サポートは HSRP に似ています。

### ガイドライン

- HSRP 認証または VRRP 認証はサポートされていません。認証を使用する場合は、ネットワークの自由形式構成に適切なコマンドを入力できます。
- vPC ピア ゲートウェイを使用すると、一部のサードパーティ デバイスが HSRP 仮想 MAC を無視し、ARP 学習に ARP パケット送信元 MAC を使用している場合に、ピアリンクの使用を最小限に抑えることができます。ルーテッドファブリック モードでは、DCNM は VPC デバイスの vPC ピア ゲートウェイ コマンドを生成します。
- eBGP ファブリックで、ネットワークと VRF が存在する場合、ルーテッドファブリック タイプと EVPN ファブリック タイプの間、または HSRP と VRRP の間で変更することはできません。ファブリックタイプまたは FHRP を変更する場合には、これらのネットワークと VRF を展開解除して削除する必要があります。詳細については、スタンドアロンファブリックのネットワークの展開解除およびスタンドアロンファブリックの VRF の展開解除を参照してください。
- DCNM リリース 11.2(1) から 11.3(1) へアップグレード後、ファブリックが以前にルーテッドファブリック モードで実行されていた場合、FHRP プロトコルやネットワーク VLAN 範囲などのデフォルトのファブリック値は、ルーテッドファブリックに対して内部的に設

定されます。異なる値を構成する場合は、ファブリック設定を編集する必要があります。ネットワーク構成を展開する前に、FHRP プロトコルファブリック構成を更新し、**[保存と展開 (Save & Deploy)]** をクリックする必要があります。

## ルーテッドファブリックでのネットワークの作成と展開

この手順は、ルーテッドファブリックでネットワークを作成して展開する方法を示しています。

### Before you begin

ルーテッドファブリックを作成し、必要なリーフおよびスパインポリシーを展開します。

### Procedure

---

- ステップ1 **[制御 (Control)]** > **[ネットワーク (Networks)]** に移動します。
- ステップ2 **[範囲 (SCOPE)]** ドロップダウンリストから、ルーテッドファブリックを選択します。
- ステップ3 **[ネットワーク (Networks)]** ウィンドウの **[追加 (Add)]** ボタンをクリックして、ネットワークを作成します。

Create Network
✕

▼ Network Information

\* Network Name

Layer 2 Only

\* Network Template

VLAN ID

---

▼ Network Profile

General

Advanced

IPv4 Gateway/NetMask  ? example 192.0.2.1/24. Address for VIP or st

Intf IPv4 addr on active  ? example 192.0.2.2. Interface IP address on

Intf IPv4 addr on stan...  ? example 192.0.2.3. Interface IP address on

Vlan Name  ? if > 32 chars enable:system vlan long-name

Interface Description  ? For interface on the standalone, or the activ

Standby Intf Descripti...  ? For interface on the standby/backup switch

MTU for L3 interface  ? 68-9216

Routing Tag  ? 0-4294967295

[Create Network](#)

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

**レイヤ 2 のみ** : オプションネットワークがレイヤ 2 のみであるかどうかを指定します。FHRP 構成は、レイヤ 2 のみのネットワークでは生成されません。

**Note** L3 ネットワーク テンプレートがスタンドアロン デバイスにアタッチされている場合、FHRP 構成は生成されません。

[ネットワーク テンプレート (Network Template)] : **Routed\_Network\_Universal** テンプレートを選択します。

**VLAN ID** : (オプション) ネットワークの対応するテナント VLAN ID を指定します。

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

[全般 (General)] タブ

[IPv4 ゲートウェイ/ネットマスク (IPv4 Gateway/NetMask)] : IPv4 ゲートウェイアドレスとサブネットを指定します。

**[アクティブ時のインターフェイス IPv4 アドレス (Intf IPv4 addr on active)]** : vPC ペアのアクティブ デバイスの IPv4 インターフェイス アドレスを指定します。このフィールドは、デバイスの vPC ペア用にネットワークを作成して展開する場合にのみ適用されます。

**[スタンバイ時のインターフェイス IPv4 アドレス (Intf IPv4 addr on standby)]** : vPC ペアのスタンバイ/バックアップ デバイスの IPv4 インターフェイス アドレスを指定します。このフィールドは、デバイスの vPC ペア用にネットワークを作成して展開する場合にのみ適用されます。

**Note** IPv4 ゲートウェイ アドレスとインターフェイス アドレスは同じサブネットになければなりません。

**[全般 (General)]** タブの次のフィールドはオプションです。

**[Vlan 名 (Vlan Name)]** : VLAN 名を指定します。

**[インターフェイスの説明 (Interface Description)]** : インターフェイスの説明を指定します。

**[スタンバイ インターフェイスの説明 (Standby Intf Description)]** : vPC ペアのスタンバイ インターフェイスの説明を指定します。

**[L3 インターフェイスの MTU (MTU for L3 interface)]** : レイヤ 3 インターフェイスの MTU を入力します。

**[ルーティング タグ (Routing Tag)]** : 各ゲートウェイの IP アドレス プレフィックスに関連付けられているルーティング タグを指定します。

**[詳細 (Advanced)]** タブ : このタブは、デバイスの vPC ペア用にネットワークを作成、展開している場合にのみ適用されます。

▼ Network Profile

|          |  |
|----------|--|
| General  |  |
| Advanced | <p>First Hop Redundanc... <input type="text" value="hsrp"/> ? <i>Read-only, from fabric setting</i></p> <p>Active/master Switch Priority <input type="text" value="120"/> ?</p> <p>Standby/backup Switch Priority <input type="text" value="100"/> ?</p> <p>Enable Preempt <input checked="" type="checkbox"/> ? <i>Overthrow lower priority Active routers</i></p> <p>HSRP/VRRP Group # <input type="text" value="1"/> ?</p> <p>Virtual MAC Address <input type="text" value="AA11.2222.3333"/> ?</p> <p>HSRP Version <input type="text" value="1"/> ? 1 or 2</p> |

[Create Network](#)

**[ファースト ホップ冗長性プロトコル (First Hop Redundancy Protocol)]** : ファブリック設定で選択された FHRP を指定する読み取り専用フィールド。

[**アクティブ/マスター スイッチの優先度 (Active/master Switch Priority)**] : アクティブまたはマスター デバイスの優先順位を指定します。

[**スタンバイ/バックアップ スイッチの優先順位 (Standby/backup Switch Priority)**] : スタンバイまたはバックアップ デバイスの優先順位を指定します。デフォルト値は 100 です。展開前にネットワーク構成をプレビューしても、このデフォルト値は表示されないことに注意してください。

[**プリエンプトを有効にする (Enable Preempt)**] : スタンバイ/バックアップ デバイスがアクティブ デバイスをプリエンプトできるかどうかを指定します。

[**HSRP/VRRP グループ (HSRP/VRRP Group)**] : HSRP または VRRP グループ番号を指定します。デフォルトでは、HSRP グループ番号は 1 です。

[**仮想 MAC アドレス (Virtual MAC Address)**] : オプション。仮想 MAC アドレスを指定します。デフォルトでは、VMAC は HSRP グループ番号 (0000.0c9f.f000 + グループ番号) に基づいて内部的に生成されます。仮想 MAC アドレスは、ファブリック設定で **hsrp** が選択されている場合にのみ適用されます。

[**HSRP バージョン (HSRP Version)**] : HSRP バージョンを指定します。デフォルト値は 1 です。[**HSRP バージョン (HSRP Version)**] フィールドは、HSRP にのみ適用されます。

**ステップ 4** [ネットワークの作成 (Create Network)] をクリックします。

**ステップ 5** [ネットワーク (Networks)] ウィンドウで、ネットワークの横にあるチェック ボックスをオンにして、[**続行 (Continue)**] をクリックします。

**Note** 非レイヤ2 ネットワークは、デバイスの vPC ペアまたは単一のデバイスにのみ適用できます。たとえば、1 つのデバイスにネットワークを展開した場合、別のデバイスまたはデバイスの vPC ペアに同じネットワークを展開することはできません。

**ステップ 6** ネットワークを展開するデバイスまたは vPC ペアを選択します。

**Note** ルーテッドファブリックで、アクティブまたはスタンバイ IP アドレスなしで vPC ペアにネットワークを接続しようとする、IP アドレス フィールドが入力されていないことを示すエラーが表示されます。IP アドレスを追加してネットワークを保存すると、ネットワークを再度接続しなくても、ネットワークの状態が **PENDING** に変わります。

**ステップ 7** [ネットワーク アタッチメント (Network Attachment)] ウィンドウで、vPC ペアのデバイスにアクティブ状態を割り当てます。

アクティブ デバイスの場合は **isActive** 列に **true** を入力し、スタンバイ デバイスの場合は **false** を入力します。

[**保存 (Save)**] をクリックします。

Network Attachment - Attach networks for given switch(es) ×

Fabric Name: bgp-routed

Deployment Options

① Select the row and click on the cell to edit and save changes

| MyNetwork_30000 | ▲ VLAN | Interfaces      | CLI Freeform    | Status | isActive |
|-----------------|--------|-----------------|-----------------|--------|----------|
|                 | 100    | ... Ethernet1/1 | Freeform config | NA     | true     |
|                 | 100    | ... Ethernet1/1 | Freeform config | NA     | false    |

Save

**Note** ルーテッドファブリックで、展開されたネットワークを編集し、変更を加えずに保存すると、ネットワークのステータスが **[保留中 (Pending)]** に変わります。同様に、展開されたネットワークに対して **[ネットワーク アタッチメント (Network Attachment)]** ウィンドウを開き、変更せずに保存すると、ネットワークのステータスが **[保留中 (Pending)]** に変わります。このような場合は、**[プレビュー (Preview)]** アイコンをクリックして構成をプレビューします。このアクションにより、ネットワークステータスが **展開済み (Deployed)** に戻ります。

**ステップ 8** (オプション) **[プレビュー (Preview)]** アイコンをクリックして、デバイスに展開された構成をプレビューします。

**[構成のプレビュー (Preview Configuration)]** ウィンドウが表示されます。

### Preview Configuration ✕

Select a Switch:  ▼

Select a Network:  ▼

Generated Configuration:

```
interface ethernet1/1
  switchport trunk allowed vlan add 100
interface Vlan100
  no ip redirects
  no ipv6 redirects
  ip address 100.1.1.2/24 tag 12345
  hsrp 1
  ip 100.1.1.1
  priority 120
  mac-address aa11.2222.3333
  preempt
  mtu 8000
  description test100_int
  no shutdown
vlan 100
  name test100
configure terminal
```

ステップ 9 [ネットワーク/VRF 展開 (Network/VRF Deployment)] ウィンドウの [展開 (Deploy)] ボタンをクリックします。

[ファブリックビルダ (Fabric Builder)] ウィンドウに移動し、[展開 (Deploy)] ボタンをクリックして、ネットワークを展開することもできます。

## ルーテッドファブリックと外部ファブリック間のファブリック間リンクの作成

DCNM リリース 11.3(1)以降、ファブリック間リンクを使用して、ルートファブリックをエッジルータに接続できます。このリンクは、物理インターフェイスで IP アドレスを構成し、デフォルトの vrf でエッジルータとの eBGP ピアリングを確立します。BGP 構成には、リーフスイッチへのデフォルトルートのアドバタイズが含まれます。



---

**Note** 外部ファブリック設定の **[ファブリック モニタ モード (Fabric Monitor Mode)]** チェックボックスはオフにすることができます。**[ファブリック モニタ モード (Fabric Monitor Mode)]** チェックボックスをオフにすると、DCNM が構成を外部ファブリックに展開できるようになります。詳細については、「[外部ファブリックの作成](#)」を参照してください。

---

### Procedure

---

- ステップ 1 **[制御 (Control)]** > **[ファブリック ビルダ (Fabric Builder)]** に移動します。
- ステップ 2 **ファブリック ビルダ (Fabric Builder)** ウィンドウで、ルーティングされたファブリックをクリックします。
- ステップ 3 ウィンドウの左側に表示される **[アクション (Actions)]** パネルの **[表形式ビュー (Tabular view)]** をクリックします。
- ステップ 4 **[リンク (Links)]** タブをクリックします。
- ステップ 5 **[追加 (Add)]** アイコンをクリックして、リンクを追加します。  
[リンク管理 – リンクの追加 (Link Management – Add Link)] ウィンドウが表示されます。

[リンク タイプ (Link Type) ]: [ファブリック間 (Inter-Fabric) ]を選択して、2つのファブリック間のボーダースイッチを介するファブリック間接続を作成します。

[リンク サブタイプ (Link Sub-Type) ]: このフィールドは IFC タイプを入力します。ドロップダウンリストから [ROUTED\_FABRIC] プロファイルを選択します。

[リンク テンプレート (Link Template) ]: リンク テンプレートが入力されます。テンプレートには、選択内容に基づいて、対応するパッケージ済みのデフォルトテンプレートが自動的に入力されます。ルーテッドファブリックの場合、**ext\_routed\_fabric** テンプレートが読み込まれます。

[送信元ファブリック (Source Fabric) ]: このフィールドには、送信元ファブリック名が事前に入力されます。

[接続先ファブリック (Destination Fabric) ]: このドロップダウンボックスから接続先ファブリックを選択します。

[送信元デバイス (Source Device) ]と [送信元インターフェイス (Source Interface) ]: 接続先デバイスに接続する送信元デバイスとイーサネット インターフェイスまたはポートチャネル インターフェイスを選択します。ボーダーのロールを持つデバイスのみを選択できます。

[接続先デバイス (Destination Device) ]と [接続先インターフェイス (Destination Interface) ]: 送信元デバイスに接続する接続先デバイスとイーサネット インターフェイスまたはポートチャネル インターフェイスを選択します。

送信元デバイスと送信元インターフェイスの選択に基づいて、Cisco Discovery Protocol 情報 (使用可能な場合) に基づいて宛先情報が自動入力されます。宛先外部デバイスが宛先ファブリックの一部であることを確認するために、追加の検証が実行されます。

[リンク プロファイル] セクションの [全般] タブ。

[BGP ローカル ASN (BGP Local ASN) ]: このフィールドには、**leaf\_bgp\_asn** ポリシーを作成して適用した場合、リーフの AS 番号が自動入力されます。

[IP アドレス/マスク (IP Address/Mask) ]: 接続先デバイスに接続する送信元インターフェイスの IP アドレスをこのフィールドに入力します。

[BGP NEIGHBOR IP (BGP ネイバー IP) ]: 接続先インターフェイスの IP アドレスをこのフィールドに入力します。

[BGP ネイバー ASN (BGP Neighbor ASN) ]: このフィールドには、宛先デバイスの AS 番号が自動入力されます。

[BGP の最大パス (BGP Maximum Paths) ]: サポートされる最大の BGP パスを指定します。

[詳細設定 (Advanced) ] タブには、次のオプションのフィールドが含まれています。

[送信元インターフェイスの説明 (Source Interface Description) ]および [宛先インターフェイスの説明 (Destination Interface Description) ]: 後で使用するためのリンクについて説明します。保存して展開すると、この説明が実行構成に反映されます。

[送信元インターフェイス フリーフォーム CLI (Source Interface Freeform CLIs) ]および [宛先インターフェイス フリーフォーム CLI (Destination Interface Freeform CLIs) ]: 送信元と宛先インターフェイスに固有のフリーフォーム構成を入力します。スイッチの実行構成に表示

されている設定を、インデントなしで追加する必要があります。詳細については、「ファブリック スイッチでの自由形式構成の有効化」を参照してください。

- ステップ 6 [保存 (Save) ] をクリックして、サイトの追加を終了します。
- ステップ 7 [戻る (Back) ] アイコンをクリックして、ファブリック ビルダ ウィンドウに戻ります。
- ステップ 8 外部ファブリックのエッジルータに接続しているデバイスを右クリックし、[構成の展開 (Deploy Config) ] を選択します。
- ステップ 9 [構成展開 (Config Deployment) ] ウィンドウで、[構成の展開 (Deploy Config) ] をクリックします。
- ステップ 10 [ファブリック ビルダ (Fabric Builder) ] ウィンドウで外部ファブリックに移動し、[アクション (Actions) ] パネルの [表形式ビュー (Tabular view) ] をクリックします。[リンク (Links) ] タブをクリックして、外部ファブリックのすべてのリンクを表示します。

作成されたファブリック間リンクが表示されます。

**Note** 外部ファブリックがモニタ モードでない場合、ファブリック間リンクが作成されません。

- ステップ 11 [戻る (Back) ] アイコンを 2 回クリックして、[ファブリック ビルダ (Fabric Builder) ] ウィンドウに戻ります。
  - ステップ 12 ルーティングされたファブリックに接続している外部ファブリックをクリックします。
  - ステップ 13 ルーテッドファブリックに接続しているデバイスを右クリックし、[構成の展開 (Deploy Config) ] を選択します。
  - ステップ 14 [構成展開 (Config Deployment) ] ウィンドウで、[構成の展開 (Deploy Config) ] をクリックします。
-

## 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。