

グリーンフィールド VXLAN BGP EVPN ファ ブリックの管理

この章では、グリーンフィールドVXLAN BGP EVPN ファブリックを管理する方法について説明します。

- VXLAN BGP EVPN ファブリックのプロビジョニング (1ページ)
- •新規 VXLAN BGP EVPN ファブリックの作成, on page 5
- ・ファブリックへのスイッチの追加, on page 31
- eBGP EVPN を使用した VXLAN EVPN の展開 (45 ページ)

VXLAN BGP EVPN ファブリックのプロビジョニング

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

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

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

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

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

ファブリックの作成、編集、および削除:

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

新しいスイッチでのデバイス検出とプロビジョニングの起動設定:

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

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

アンダーレイのプロビジョニング:

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

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

オーバーレイ ネットワークのプロビジョニング

- (ファブリックの作成で指定された範囲から)新しいオーバーレイネットワークとVRF を作成します。
- ファブリックのスイッチでオーバーレイネットワークとVRFをプロビジョニングします。

- スイッチからネットワークと VRF を展開解除します。
- DCNM でファブリックからプロビジョニングを削除します。

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

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

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

VXLAN BGP EVPN ファブリック プロビジョニングのガイドライン

- ・スイッチを DCNM に正しくインポートするには、検出/インポート用に指定されたユー ザーに次の権限が必要です。
 - ・スイッチへの SSH アクセス
 - ・SNMPv3 クエリを実行する権限
 - show run、show interfaces などを含む show コマンドを実行する権限
- スイッチ検出ユーザーには、スイッチの設定を変更する権限は必要ありません。主に読み 取りアクセスに使用されます。
- ・無効なコマンドが DCNM によってデバイスに展開された場合、たとえば、ファブリック 設定の無効なエントリが原因で無効なキーチェーンを持つコマンドが生じた場合には、この問題を示すエラーが生成されます。このエラーは、無効なファブリックエントリを修正 した後もクリアされません。エラーをクリアするには、無効なコマンドを手動でクリーン アップまたは削除する必要があります。

コマンドの実行に関連するファブリックエラーは、失敗したのと同じコマンドが後続の展 開で成功した場合にのみ、自動的にクリアされることに注意してください。

- LAN クレデンシャルは、デバイスへの書き込みアクセスを実行する必要があるすべての ユーザーに設定する必要があります。LAN ログイン情報は、デバイスごと、ユーザーご とに DCNM に設定する必要があります。ユーザーがデバイスを Easy ファブリックにイン ポートし、そのデバイスに LAN ログイン情報が設定されていない場合、DCNM はこのデ バイスを移行モードに移動します。ユーザーがそのデバイスに適切な LAN ログイン情報 を設定し、その後で [保存と展開(Save & Deploy)]を選択すると、デバイスインポート プロセスが再トリガーされます。
- •[保存と展開(Save & Deploy)]ボタンをクリックすると、ファブリック全体のインテントの再生成と、ファブリック内のすべてのスイッチの設定コンプライアンスチェックがトリガーされます。このボタンは以下の場合に必須ですが、それらに限定されません。

- スイッチまたはリンクが追加された、またはトポロジが変更されたとき
- ファブリック全体で共有する必要があるファブリック設定が変更されたとき
- •スイッチが取り外された、または削除されたとき
- 新しい vPC のペアリングまたはペアリングの解除が実行されたとき
- デバイスのロールが変更されたとき

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

スイッチのアイコンを右クリックして、[構成の展開(Deploy Config)]オプションを選 択すれば、スイッチごとの構成を展開できます。このオプションは、スイッチのローカル 操作です。つまり、スイッチの予想される構成またはインテントが現在の実行構成に対し て評価され、構成のコンプライアンスチェックが実行されて、スイッチがIn-Syncまたは Out-of-Syncステータスを取得します。スイッチが同期していない場合、ユーザには、そ の特定のスイッチで実行されているすべての設定のプレビューが提供されます。これらの 設定は、それぞれのスイッチに対してユーザが定義した意図とは異なります。

 ・永続的な設定の差分は、コマンドラインsystem nve infra-vlan *int* forceで確認できます。永 続的な差分は、スイッチにフリーフォームの設定を介してこのコマンドを展開すると、発 生します。スイッチは展開時に force キーワードを必要としますが、DCNM 内でスイッチ から取得された実行構成では force キーワードは表示されません。したがって、system nve infra-vlan *int* force コマンドは常に diff として表示されます。

DCNM のインテントには次の行が含まれます:

system nve infra-vlan int force

実行設定には次の行が含まれいます:

system nve infra-vlan int

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

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

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

 スイッチに、hardware access-list tcam region arp-ether 256 コマンドが含まれている場合、 このコマンドは、double-wide キーワードなしでは非推奨になり、次の警告が表示されます。 警告:「double-wide」なしで arp-ether 領域を設定すると、非 vxlan パケットのドロップが 発生する可能性があります。(WARNING: Configuring the arp-ether region without "double-wide" is deprecated and can result in silent non-vxlan packet drops.) arp-ether リージョンの TCAM ス ペースを分割する場合は、「double-wide」キーワードを使用します。

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

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

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

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

元の tcam コマンドが上書きされていることがわかります。

新規 VXLAN BGP EVPN ファブリックの作成

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

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

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

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

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

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

X

フィールドについて説明します。

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

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

Add Fabric

* Fab * Fabric	Template : Easy_l	Fabric_11	_1	▼						
General	Replication	vPC	Protocols	Advanced	Reso	irces	Manageability	Bootstrap	Configuration Backup	
En	* Bi Enable IPv6 U Jable IPv6 Link-Local	GP ASN Inderlay				() 1-4	294967295 1-65535[[.0-65535]		
*	Fabric Interface Nur	mbering	p2p		▼	🕜 Nu	mbered(Point-to-Point)) or Unnumbered		
	* Underlay Subnet	IP Mask	30		▼	Mask for Underlay Subnet IP Range				
	Underlay Subnet IP	v6 Mask			W	🕜 Ma	sk for Underlay Subne	t IPv6 Range		
*1	Link-State Routing F	Protocol	ospf		▼	🕐 Su	opported routing proto	cols (OSPF/IS-IS))	
	* Route-Re	flectors	2			🕜 Nu	mber of spines acting a	as Route-Reflecto	ors	
	* Anycast Gatew	ay MAC	2020.0000.00a	aa		🕐 Sh	ared MAC address for	all leafs (xxxx.xxx	(x.xxxx)	
NX-	OS Software Image	Version			▼	Images	Set, Image Version Che Can Be Uploaded Fro	eck Enforced On A m Control:Image	All Switches. Upload	

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



Note

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

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

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

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

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

[ファブリックインターフェイスの番号付け(Fabric Interface Numbering)]:ポイント ツーポイント([p2p])またはアンナンバードネットワークのどちらを使用するかを指定 します。 [アンダーレイサブネットIPマスク(Underlay Subnet IP Mask)]:ファブリックインター フェイスの IP アドレスのサブネットマスクを指定します。

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

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

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

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

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

- a. ドロップダウンボックスの値を2に変更します。
- b. ルートリフレクタとして指定するスパインスイッチを特定します。

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

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

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

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

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

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

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

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

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

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

General	Replication	vPC	Protocols	Advanced	Reso	urces	Manageability	Bootstrap	Configuration Backup			
	* Replica	tion Mode	Multicast	·	•	Replication Mode for BUM Traffic						
	* Multicast Grou	up Subnet	239.1.1.0/25			🕜 Mu	lticast address with pr	əfix 16 to 30				
Enable Ten	ant Routed Multic	ast (TRM)	🗌 🕐 For Ov	erlay Multicast Su	Ipport In \	/XLAN F	abrics					
Default	MDT Address for 7	TRM VRFs				🕜 IPv	4 Multicast Address					
	* Rendezvo	us-Points	2		•	🕜 Nu	mber of spines acting	as Rendezvous-F	Point (RP)			
	*	RP Mode	asm		▼	@ Multicast RP Mode						
•	* Underlay RP Lo	opback Id	254			🕐 (Min:0, Max:1023)						
	Underla RP Lo	ay Primary oopback Id				(Min:0,	ed for Bidir-PIM Phant Max:1023)	om RP				
	Underl RP Lo	ay Backup oopback Id				(Min:0,	ed for Fallback Bidir-Pi Max:1023)	IM Phantom RP				
	Underlay Seco RP Lo	nd Backup oopback Id				(Min:0,	ed for second Fallback Max:1023)	Bidir-PIM Phante	om RP			
	Underlay Th RP Lo	ird Backup oopback Id				(Min:0,	ed for third Fallback Bi Max:1023)	dir-PIM Phantom	RP			

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

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

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

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

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

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

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

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

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

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

Note

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

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

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

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

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

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

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

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

General	Replication	vPC	Protocols	Advanced	Resources	Manageability	Bootstrap	Configuration Backup				
	* vPC Peer Li	nk VLAN	3600		i) VL	AN for vPC Peer Link S	SVI (Min:2, Max:3	967)				
Make vP	C Peer Link VLAN	as Native VLAN	i i									
*	vPC Peer Keep Aliv	ve option	management		Management							
	* vPC Auto Recov (In S	very Time Seconds)	360		i) (Mi	n:240, Max:3600)						
	* vPC Delay Restore Time (In Seconds) 150					(i) (Min:1, Max:3600)						
vP	vPC Peer Link Port Channel ID 500					n:1, Max:4096)						
	vPC IPv6 ND Syn	chronize	🗹 i Enable	IPv6 ND synchro	nization between v	PC peers						
	vPC adve	ertise-pip	🧻 🧿 For Prin	mary VTEP IP Ad	vertisement As Ne	xt-Hop Of Prefix Route	s					
Enal	ole the same vPC D for all v	omain Id PC Pairs	i) (Not Re	ecommended)								
	VPC [Domain Id			i vP	C Domain Id to be used	l on all vPC pairs					
	vPC Domain	ld Range	1-1000		(i) vPi	C Domain id range to u	se for new pairing	15				
Enable	Qos for Fabric vPC	-Peering	i Qos on	spines for guara	nteed delivery of vi	PC Fabric Peering com	munication					
	Qos Pol	licy Name			(j) Qo	(j) Qos Policy name should be same on all spines						

Save Cancel

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

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

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

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

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

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

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

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

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

特定の vPC で アドバタイズ PIP 機能をイネーブルにすることもできます。詳細について は、vPC で PIP をアドバタイズするを参照してください。 [すべての vPC ペアに同じ vPC ドメイン ID を有効にする (Enable the same vPC Domain Id for all vPC Pairs)]: すべての vPC ペアに同じ vPC ドメイン ID を有効にします。この フィールドを選択すると、[vPC ドメイン ID (vPC Domain Id)]フィールドが編集可能に なります。

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

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

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



Note

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

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

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

Add Fabric	c												×
* Fab	oric Name : Template :	Easy_Fa	abric_11	_1	v								
General	Replicat	ion v	PN depl vPC	Protocols	Advanced	3000 swit	urces	Manageability	Boots	strap	Configuration Backup		
	Ena Enable BF BFD Auth	ble BFD F D Authent entication	or PIM ication Key ID	(i) (i) Valid fo	or P2P Interfaces	only	(j)	minterl SH&1 secret ve	alue				
	iBGP Peer-1	Femplate (Config							Spefici spines v This field ' templa This mu Note ! A strictly n with res Any mis unexped	es the config used for RR and vith border or border gateway is d should begin with te peer' or 'template peer-sess st have 2 leading spaces. Il configs should natch 'show run' output, bect to case and newlines. matches will yield ted diffs during deploy.	role. sion'.	
L	.eaf/Border/I iBGP Peer-]	Border Ga ſemplate (iteway Config						Q III	Specifi border g If this fiel iBGP Pe enabled border c i) This fiel i) This fiel i) This fiel i) This fiel i) This mu Note ! A strictly r with res Any mis unexpec	es the config used for leaf, bou aldeway. Id is emply, the peer template per-Template Config is used or devices (RRs, leafs, n border gateway roles), d should begin with te peer or 'template peer-ses st have 2 leading spaces. It configs should natch 'show run' output, pect to case and newlines. matches will yield vated diffs during deploy.	rder or defined in a all BGP sion'.	
												Save	Cancel

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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



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

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

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



Note

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

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

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

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

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

feature bfd



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

no ip redirects no ipv6 redirects

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

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

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

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

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

```
router ospf <ospf tag>
   bfd
router isis <isis tag>
   address-family ipv4 unicast
   bfd
ip pim bfd
router bgp <bgp asn>
   neighbor <neighbor ip>
   bfd
```

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

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

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

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

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

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

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

構成例では、パスワード3の後に3DESパスワードが表示されます。

router bgp 65000

password 3 sd8478fswerdfw3434fsw4f4w34sdsd8478fswerdfw3434fsw4f4w

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

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

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

ブラウンフィールド移行では、スパインとリーフが異なるピアテンプレート名を使用す る場合、[iBGP ピアテンプレート構成(iBGP Peer-Template Config)]フィールドと[リー フ/境界/境界ゲートウェイ iBGP ピアテンプレート構成(Leaf/Border/Border Gateway iBGP Peer-Template Config)]フィールドの両方をスイッチ構成に従って設定する必要がありま す。スパインとリーフが同じピアテンプレート名とコンテンツを使用する場合

(「route-reflector-client」CLIを除く)、ファブリック設定の[iBGP ピアテンプレート構成(iBGP Peer-Template Config)]フィールドのみを設定する必要があります。iBGP ピア テンプレートのファブリック設定が既存のスイッチ構成と一致しない場合、エラーメッ セージが生成され、移行は続行されません。

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

General	Replication	vPC	Protocols	Advanced	Resou	rces	Manageability	Bootstrap	Configuration Backup	
	* VRF	⁼ Template	Default_VRF_U	Jniversal	▼	? D	efault Overlay VRF Ter	mplate For Leafs		
	* Network	k Template	Default_Netwo	rk_Universal	▼	② Default Overlay Network Template For Leafs				
	* VRF Extension	n Template	Default_VRF_E	Extension_Universa		? D	efault Overlay VRF Ter	mplate For Borde	rs	
* N	letwork Extensior	n Template	Default_Netwo	rk_Extension_Unive	ersa 🔻	? D	efault Overlay Network	Template For Bo	orders	
		Site Id				Pefaul	or EVPN Multi-Site Sup ts to Fabric ASN	port (Min:1, Max	: 281474976710655).	
•	* Intra Fabric Inte	rface MTU	9216			()	/in:576, Max:9216). Mu	ist be an even ni	ımber	
*	Layer 2 Host Inte	rface MTU	9216			()	/in:1500, Max:9216). N	lust be an even r	number	
	* Power Su	pply Mode	ps-redundant		▼	0 D	efault Power Supply Me	ode For The Fab	ric	
	* Co	PP Profile	strict		Ţ	Provide	abric Wide CoPP Policy ed when 'manual' is sel	y. Customized Co lected	PP policy should be	
	VTEP HoldE	Oown Time	180			? N	VE Source Inteface Ho	ldDown Time (Mi	in:1, Max:1500) in seconds	

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

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

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

[イントラ ファブリック インターフェイス MTU (Intra Fabric Interface MTU)]:ファ ブリック内インターフェイスの MTU を指定します。この値は偶数にする必要がありま す。 [レイヤ2ホストインターフェイス MTU(Layer 2 Host Interface MTU)]: レイヤ2ホ ストインターフェイスの MTU を指定します。この値は偶数にする必要があります。

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

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

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

[ブラウンフィールドオーバーレイネットワーク名の形式(Brownfield Overlay Network Name Format)]: ブラウンフィールドのインポートまたは移行時にオーバーレイネット ワーク名を作成するために使用する形式を入力します。ネットワーク名は、アンダース コア()およびハイフン(-)を除く特殊文字または空のスペースが含まれないように してください。ブラウンフィールドの移行が開始されたら、ネットワーク名を変更しな いでください。ネットワーク名の命名規則については、「スタンドアロンファブリック のネットワークの作成」の項を参照してください。構文は[<string>|\$\$VLAN_ID\$\$]

\$\$VNI\$\$ [<string>| \$\$VLAN_ID\$\$]です。デフォルト値は

[Auto_Net_VNI\$\$VNI\$\$_VLAN\$\$VLAN_ID\$\$]です。ネットワークを作成すると、指定 した構文に従って名前が生成されます。次の表で構文内の変数について説明します。

変数	説明
\$\$VNI\$\$	スイッチ構成で検出されたネットワーク VNIID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></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

- ^{te} グリーンフィールド展開では、このフィールドを無視します。ブラウンフィールドオー バーレイネットワーク名の形式は、次のブラウンフィールドインポートに適用されます。
 - ・CLI ベースのオーバーレイ
 - 構成プロファイルが Cisco DCNM リリースで作成された構成プロファイルベースの オーバーレイ

10.4(2) で作成された構成プロファイルベースのオーバーレイ

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

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

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

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

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

Note

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

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

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

n'
111

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

[ポリシーベース ルーティング (PBR) の有効化 (Enable Policy-Based Routing

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

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

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

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

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

[精密時間プロトコル (PTP) の有効化 (Enable Precision Time Protocol (PTP))]:ファ ブリック全体で PTP を有効にします。このチェックボックスをオンにすると、PTP がグ ローバルに有効になり、コアに面するインターフェイスで有効になります。また、[PTP 送信元ループバック ID (PTP Source Loopback Id)]および [PTP ドメイン ID (PTP Domain Id)]フィールドが編集可能になります。詳細については、Easyファブリック向 け高精度時間プロトコルを参照してください。 [PTP 送信元ループバック ID (PTP Source Loopback Id)]: すべての PTP パケットの送 信元 IP アドレスとして使用されるループバック インターフェイス ID ループバックを指 定します。有効な値の範囲は 0 ~ 1023 です。 PTP ループバック ID を RP、ファントム RP、NVE、または MPLS ループバック ID と同じにすることはできません。そうでない 場合は、エラーが生成されます。 PTP ループバック ID は、DCNM から BGP ループバッ クまたは作成元のユーザー定義ループバックと同じにすることができます。

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

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

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

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

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

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

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

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

テンプレート エディタでポリシー ファイルを開いて、実際のキューイング ポリシーを 確認します。Cisco DCNM Web UI から、[制御(Control)] > [テンプレート ライブラリ (Template Library)]を選択します。ポリシー ファイル名でキューイング ポリシーを 検索します(例:[queuing_policy_default_8q_cloudscale])。ファイルを選択し、[テンプ レートの変更/表示 (Modify/View template)]アイコンをクリックしてポリシーを編集し ます。 プラットフォーム特有の詳細については、『*Cisco Nexus 9000 Series NX-OS Quality of Service* コンフィグレーション ガイド』を参照してください。

[N9K クラウドスケール プラットフォームのキューイング ポリシー (N9K Cloud Scale Platform Queuing Policy)]: ファブリック内の EX、FX、および FX2 で終わるすべての Cisco Nexus 9200 シリーズスイッチおよび Cisco Nexus 9000 シリーズスイッチに適用する キューイング ポリシーをドロップダウン リストから選択します。有効な値は

[queuing_policy_default_4q_cloudscale] および [queuing_policy_default_8q_cloudscale] です。 FEX には [queuing_policy_default_4q_cloudscale] ポリシーを使用します。FEX がオフラインの場合にのみ、[queuing_policy_default_4q_cloudscale] ポリシーから [queuing_policy_default_8q_cloudscale] ポリシーに変更できます。

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

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

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

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

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

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

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

8. [リソース (Resources)]タブをクリックします。

General Replication vPC	Protocols	Advanced	Resources	Manageability	Bootstrap	Configuration Backup						
Manual Underlay IP Address Allocation	🗌 (į́) Checking	g this will disable	Dynamic Underla	y IP Address Allocation	ıs							
* Underlay Routing Loopback IP Range	10.2.0.0/22		і Тур	⑦ Typically Loopback0 IP Address Range								
* Underlay VTEP Loopback IP Range	10.3.0.0/22		і) Тур	(i) Typically Loopback1 IP Address Range								
* Underlay RP Loopback IP Range	10.254.254.0/24	1	(i) Ang	cast or Phantom RP II	Address Range							
* Underlay Subnet IP Range	10.4.0.0/16		(i) Add	dress range to assign I	lumbered and Pe	er Link SVI IPs						
Underlay MPLS Loopback IP Range			(i) Us	ed for VXLAN to MPLS	SR/LDP Handoff							
Underlay Routing Loopback IPv6 Range			і) Тур	ically Loopback0 IPv6	Address Range							
Underlay VTEP Loopback IPv6 Range			і Тур	nically Loopback1 and A	Anycast Loopback	k IPv6 Address Range						
Underlay Subnet IPv6 Range			i) IPv	6 Address range to as	sign Numbered ar	nd Peer Link SVI IPs						
BGP Router ID Range for IPv6 Underlay			i									
* Layer 2 VXLAN VNI Range	30000-49000		(i) Ov	erlay Network Identifier	Range (Min:1, M	ax:16777214)						
* Layer 3 VXLAN VNI Range	50000-59000		(i) Ov	erlay VRF Identifier Ra	nge (Min:1, Max:1	16777214)						
* Network VLAN Range	2300-2999		(i) Per	r Switch Overlay Netwo	rk VLAN Range (Min:2, Max:3967)						
* VRF VLAN Range	2000-2299		(i) Per	Switch Overlay VRF	/LAN Range (Min	:2, Max:3967)						
* Subinterface Dot1o Range	2-511		(i) Per	Border Dot1a Range	For VRF Lite Con	nectivity (Min:2. Max:4093)						
							Sava					

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

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

詳細については、『Cisco REST API 参照ガイド、リリース 11.2(2)』を参照してくだ さい。スイッチをファブリックに追加した後、REST APIを呼び出してから [保存し て展開(Save & Deploy)]オプションを使用する必要があります。

- マルチキャストレプリケーションに BIDIR-PIM 機能が選択されている場合、[アン ダーレイ RP ループバック IP 範囲(Underlay RP Loopback IP Range)]フィールドは 有効のままになります。
- •静的割り当てから動的割り当てに変更しても、現在のIPリソースの使用情況は維持 されます。それ以後のIPアドレス割り当て要求のみが動的プールから取得されま す。

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

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

[アンダーレイ RP ループバック IP 範囲(Underlay RP Loopback IP Range)]: エニー キャストまたはファントム RP の IP アドレス範囲を指定します。 [アンダーレイ サブネット IP 範囲(Underlay Subnet IP Range)]: インターフェイス間 のアンダーレイ P2P ルーティング トラフィックの IP アドレスです。

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

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

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

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

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

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

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

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

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

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

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



- Note 値の範囲を更新する場合は、他の範囲と重複しないようにしてください。一度に更新で きる値の範囲は1つだけです。複数の値の範囲を更新する場合は、別のインスタンスで 実行します。たとえば、L2とL3の範囲を更新する場合は、次の手順を実行する必要があ ります。
 - **a.** L2 範囲を更新し、[保存(Save)] をクリックします。
 - b. [ファブリックの編集(Edit Fabric)]オプションをもう一度クリックし、L3範囲を更新して[保存(Save)]をクリックします。

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

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

9. 管理能力(Manageability) タブをクリックします。

General	Replication	vPC	Protocols	Advanced	Resources	Manageability	Bootstrap	Configuration Backup			
	DNS	Server IPs			🕜 Col	mma separated list of	IP Addresses(v4/	v6)			
	DNS Se	erver VRFs			Iist of VI	e VRF for all DNS sen RFs, one per DNS ser	vers or a comma ver	separated			
	NTP	Server IPs			🕜 Col	mma separated list of	IP Addresses(v4/	v6)			
	NTP Server VRFs		One VRF for all NTP servers or a comma separated list of VRFs, one per NTP server								
	Syslog	Server IPs			Comma separated list of IP Addresses(v4/v6)						
	Syslog Serve	er Severity			One per	mma separated list of Syslog server (Min:0,	Syslog severity v Max:7)	alues,			
	Syslog Se	erver VRFs			Iist of VI	e VRF for all Syslog se RFs, one per Syslog s	ervers or a comm erver	a separated			
	AAA Freeform Config					Note ! . strictly mate with respec Any mismai unexpected	All configs should ch 'show run' outp t to case and new tches will yield I diffs during deplo	i ut, dines. py.			

このタブのフィールドは次のとおりです。

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

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

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

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

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

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

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

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

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

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

General	Replication vPC	Protocols	Advanced	Resou	urces	Manageability	Bootstrap	Configuration Backup		
	Enable Bootstrap Enable Local DHCP Server	Auton	atic IP Assignmer atic IP Assignmer	nt For POA nt For POA	\P \P From	Local DHCP Server				
	DHCP Version				?					
	DHCP Scope Start Address				Start Address For Switch Out-of-Band POAP					
	DHCP Scope End Address				🕐 En	d Address For Switch C	Dut-of-Band PO	AP		
:	Switch Mgmt Default Gateway				🕜 De	fault Gateway For Man	agement VRF C	Dn The Switch		
	Switch Mgmt IP Subnet Prefix		(Min:8, Max:30)							
Sv	witch Mgmt IPv6 Subnet Prefix				(Min:64, Max:126)					
	Enable AAA Config	🗌 🕜 Includ	e AAA configs fror	n Manage	ability ta	b during device bootup				
	Bootstrap Freeform Config				strictly with re Any m unexp	lote ! All configs should v match 'show run' outpu sspect to case and new hismatches will yield bected diffs during deplo	ut, lines. vy.			
DHCPv4/DHCPv6 Multi Subnet Scope Image: Control of the state of the s										

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

スコープの形式は次の順で定義する必要があります。

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

例:10.6.0.2、10.6.0.9、16.0.0.1、24

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

General	Replication	vPC	Protocols	Advanced	Resources	Manageability	Bootstrap	Configuration Backup	
	Hourly Fabr	ic Backup	🗌 🕜 Backu	hourly or on Re-	sync only if there is	s any config deployme	nt since last back	up	
Scheduled Fabric Backup							q		
	Scheo	duled Time			🕜 Tin	ne 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。

時間単位のバックアップは、その時間の最初の10分間にトリガーされます。

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

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

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

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

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

バックアップ構成ファイルは、DCNM にある次のパスに保存されま す:/usr/local/cisco/dcm/dcnm/data/archive 保持できるアーカイブファイルの数は、[サーバ プロパティ(Server Properties)] ウィン ドウの [保持するデバイスあたりのアーカイブ ファイル数(# Number of archived files per device to be retained:)] フィールドで設定します。



- a. [制御(Control)]>[ファブリック ビルダ (Fabric Builder)] を選択します。[Fabric Builder] 画面が表示されます。
- **b.** 特定のファブリック ボックス内をクリックします。[ファブリック トポロジ (fabric topology)] 画面が表示されます。
- c. 画面左側の[アクション (Actions)]ペインで、[ファブリックの再同期 (Re-Sync Fabric)]をクリックします。

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

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

General	Replication	vPC	Protocols	Advanced	Resources	Manageability	Bootstrap	Configuration Backup	ThousandEyes Agent				
Thous	Enable Fabric Ov andEyes Agent In	erride for stallation	_ (j)										
Т	housandEyes Acco	unt Group Token			(i) Tok	en from ThousandEye	s Agent Settings f	or Agent Installation					
VRF	on Switch for Thou Agent Collector Re	isandEyes eachability			(i) NX-	OS VRF that provides	Internet Reachab	ility					
	DN	IS Domain			i) DN	(i) DNS Domain Configuration							
	DNS	Server IPs			(i) Cor	(i) Comma separated list of IP Addresses(v4/v6)							
	NTPS	Server IPs			(i) Cor	mma separated list of I	P Addresses(v4/v	6)					
Ena	ible Proxy for Interr	net Access	🗌 (i) Proxy S	Settings for NX-O	S Switch Internet A	ccess							
	Proxy Ir	nformation			i) Pro	xy-Server:port							
	Pro	xy Bypass			(i) Cor	mma separated No-pro	oxy server list						

Save Cancel

このタブのフィールドは次のとおりです。



Note

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

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

- [ThousandEyes アカウントグループトークン (ThousandEyes Account Group Token)] : インストール用の ThousandEyes Enterprise Agent アカウント グループ トークンを指 定します。
- [ThousandEyes Agent コレクタ到達可能性のスイッチ上の VRF (VRF on Switch for ThousandEyes Agent Collector Reachability)]: インターネットの到達可能性を提供 する VRF データを指定します。
- •[ドメインネームシステム (DNS) ドメイン (DNS Domain)]: スイッチのドメイ ンネームシステム (DNS) ドメイン構成を指定します。
- ・[ドメインネームシステム (DNS) サーバ IP (DNS Server IPs)]: ドメインネームシステム (DNS) サーバの IP アドレス (v4/v6) のカンマ区切りリストを指定します。DNS サーバには、最大3つの IP アドレスを入力できます。
- [NTP サーバ IP (NTP Server IPs)]: Network Time Protocol (NTP) サーバの IP アドレス (v4/v6) のコンマ区切りリストを指定します。NTP サーバには、最大 3 つの IP アドレスを入力できます。
- •[プロキシを有効にする(Enable Proxy)]: チェックボックスをオンにして、NX-OS スイッチのインターネットアクセスのプロキシ設定を選択します。
- •[プロキシ情報(Proxy Information)]:プロキシサーバのポート情報を指定します。
- •[プロキシバイパス(Proxy Bypass)]: プロキシをバイパスするサーバ リストを指 定します。
- 13. 関連情報を入力して更新したら、[保存 (Save)]をクリックします。画面の右下に、ファ ブリックが作成されたことを示すメモが短時間表示されます。ファブリックが作成され ると、ファブリックのページが表示されます。画面左上に生地名が表示されます。

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

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

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

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

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

[未検出(Undiscovered)] クラウドを表示するために[クラウド(Cloud)] アイコン をまたクリックします。 [範囲 (SCOPE)]:右上の[範囲 (SCOPE)]ドロップダウンボックスを使用して、ファブリックを切り替えることができます。現在のファブリックは、強調表示されます。MSD とそのメンバーファブリックが明確に表示され、メンバーファブリックはMSD ファブリックの下にくぼんで表示されます。

ファブリックへのスイッチの追加

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

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

さらに、スイッチとインターフェイスを事前プロビジョニングできます。詳細については、デ バイスの事前プロビジョニング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。

新しいスイッチの検出

- 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。
- 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。

 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 Manage	ment				×
Discover Existing Swite	ches PowerOn	Auto Provisio	oning (POAP)		
I Please note that POAP ca	n take anywhere betw	een 5 and 15 m	inutes to complete!		D Bootstrap
	* Admin Pa	ssword	* C	onfirm Admin Password	۲
Serial Number	Model	Version	IP Address	Hostname	Gateway
No Data available					

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。

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

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



Note

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

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

Inver	ntory Manage	ement					×
Disc	over Existing Swi	tches PowerOr	Auto Provisi	oning (POAP)			
(i) Plea	se note that POAP c	an take anywhere betw	veen 5 and 15 n	ninutes to complete!		Ø	Bootstrap
+	C (A	dmin Password		* Confirm A	dmin Password		
	Serial Number	Model	Version	IP Address	Hostname		
	FDO21323D58	N9K-93180YC-EX	9.2(1)				
				Close			

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。

Inventory Management				×
Discover Existing Switches	PowerOn Auto Provisioning (PC	DAP)		
⑦ Please note that POAP can take any	where between 5 and 15 minutes to c	complete!		Ø Bootstrap
+ 🖻 🖆 * Admin Pass	word	* Confirm Admin Passw	vord	
Serial Number Model	Discovery Credentials		×	
No Data available	*Discovery Username:			
	*Discovery Password: *Confirm Discovery Password:		_	
		OK Clea	ar	
			_	
	Clos	5e		

[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。
- 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。
- 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:

ŦΧ Fabric errors & warnings 0 Errors, 2 Warnings, 0 Info X Delete all 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:FD020260UEK:FD020291AVQ Reported less than a minute ago 2019-03-17 09:30:00 [2]: [vpcPairing:FD020260UEK:FD020291AVQ]. Line/Col:[0/0]. Msg = [The Secondary IP address of the NVE source interface has been modified for switch SN [FD020260UEK] and peer SN [FD020291AVQ] due to vpc feature configuration. Please make sure to shut/noshut the nve interfaces from DCNM Interface Manager Screen.] Details A 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:FD020291AVQ:FD020260UEK less than a minute ago 2019-03-17 09:30:00 Reported [1]: [vpcPairing:FD020291AVQ:FD020260UEK]. Line/col:[0/0]. Msg = [The Secondary IP address of the NVE source interface has been modified for switch SN [FD020291AVQ] and peer SN [FD020260UEK] due to vpc feature configuration. Please make sure to shut/noshut the nve interfaces from DCNM Interface Manager Screen.] Details

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。

Interf	aces	2			
+	+ • C X			Deploy	
	Device Name	Name	Admin	Oper	Reason
	N9K-2-Leaf	∠ Ethernet2/6	1	\mathbf{V}	XCVR not inserted
	N9K-2-Leaf	∠ Ethernet2/7	\mathbf{T}	\checkmark	XCVR not inserted
	N9K-2-Leaf	∠ Ethernet2/8	$\mathbf{\uparrow}$	$\mathbf{+}$	XCVR not inserted
	N9K-2-Leaf	∠ Ethernet2/9	$\mathbf{\uparrow}$	$\mathbf{+}$	XCVR not inserted
	N9K-2-Leaf	Z Ethernet2/10	$\mathbf{\uparrow}$	$\mathbf{+}$	XCVR not inserted
	N9K-2-Leaf	Z Ethernet2/11	$\mathbf{\uparrow}$	\checkmark	XCVR not inserted
	N9K-2-Leaf	Z Ethernet2/12	$\mathbf{\uparrow}$	$\mathbf{+}$	XCVR not inserted
	N9K-2-Leaf	🚄 nve1	1	1	ok

グリーンフィールド VXLAN BGP EVPN ファブリックの管理

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)。



- •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(FDO21332	2E6X)						
Deployment History	Policy Change His	story						
								Show Quick Fit
Policy ID	Template	Description	PTI Operation	Generated Config	Entity Name	Entity Type	User	Created On
PROFILE-VRF-1	Default_VRF_Exten		UPDATE	Detailed History	MyVRF_50000	Config_Profile	admin	2020/05/31-08:15:21
PROFILE-VRF-1	Default_VRF_Exten		ADD	Detailed History	MyVRF_50000	Config_Profile	admin	2020/05/31-08:13:44
PROFILE-NETWO	Default_Network_E		ADD	Detailed History	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。

X

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 す	変更後の構成が含まれています
マーク - 削 除	削除する設定が含まれます。	色を変更して削除する構成が含まれます。
削除	構成が含まれています	Empty



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

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

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

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

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

既存のスイッチの検出

 [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。

Х

Inventory Management

Discover Existing Sw	ches PowerOn Auto Provisioning (POAP)
Discovery Information	Scan Details
Seed IP	172.23.244.91 Ex: "2.2.2.20"; "10.10.10.40-60"; "2.2.2.20, 2.2.2.21"
Authentication Protocol	MD5 V
Username	admin
Password	••••••
Max Hops	2 hop(s)
Preserve Config	no yes
	Selecting 'no' will clean up the configuration on switch(es)

[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。

Disc							
Disc	covery Information	Scan Details					
🗲 Bac	k					Import into f	abric
	Name	IP Address	Model	Version	Status	Progress	
	EVPN-Spine81	172.23.244.81	N9K-C931	7.0(3)I5(2)	Unknown User		
	leaf-91	172.23.244.91	N9K-C939	7.0(3)17(3)	manageable		
	switch	172.23.244.88	N9K-C937	7.0(3)I7(1)	not reachable		
	EVPN-Spine85	172.23.244.85	N9K-C939	7.0(3)I5(2)	Unknown User		

Inventory Management

Start discovery

Х

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

Disc							
Disc	overy Information	Scan Details					
🗲 Bac	x					Import into fa	abric
	Name	IP Address	Model	Version	Status	Progress	
	EVPN-Spine81	172.23.244.81	N9K-C931	7.0(3)I5(2)	Unknown User		
	leaf-91	172.23.244.91	N9K-C939	7.0(3)17(3)	manageable		
	switch	172.23.244.88	N9K-C937	7.0(3)I7(1)	not reachable		
	EVPN-Spine85	172.23.244.85	N9K-C939	7.0(3)15(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 スイッチの検出中に次のエラーが発生することがあります。

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

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



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



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

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

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

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

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

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

witch Name	IP Address	Switch Serial	Preview Config	Status	Re-sync	Progress
9K-2-Leaf	111.0.0.92	SAL18422FVP	0 lines	In-sync		100%
9K-4-BGW	111.0.0.94	FDO20260UEK	20 lines	Out-of-sync		100%
9K-3-BGW	111.0.0.93	FDO20291AVQ	20 lines	Out-of-sync		100%
9K-1-Spine	111.0.0.91	SAL18432P2T	0 lines	In-sync		100%

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、

 \mathbf{N}

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

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

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

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

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

7. 画面を閉じます。

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

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

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

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

Note CLI の実行で警告またはエラーが発生した場合は、[Fabric Builder] ウィンドウに通知が 表示されます。自動解決可能な警告またはエラーには、[解決(Resolve)] オプションが あります。 スイッチのリロードまたはRMA 操作の後にリーフスイッチが起動すると、DCNM は、スイッ チとそれに接続されている FEX デバイスの構成をプロビジョニングします。DCNM が FEX (ホストインターフェイス)構成をプロビジョニングした後に FEX 接続が起動し、構成が一 致しない場合があります。不一致を解決するには、ファブリックトポロジ画面で[保存と展開 (Save & Deploy)]を再度クリックします。

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

eBGP EVPN を使用した VXLAN EVPN の展開

eBGP ベースのアンダーレイを使用した eBGP の新しい VXLAN EVPN の 作成

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

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

[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 Fabri	С								×
* Fal * Fabric	bric Name : Template :	Easy_Fab	ric_eBGP	•					
General	EVPN	vPC	Protocols	Advanced	Manageabil	ty Boo	otstrap	Configuration Backup	
	* BGP	ASN for Sp	ines	1-4294967295 1-65535[.0-65535]					
	*	BGP AS N	lode Multi-AS	Multi-AS Multi-AS Multi-AS: Uniqu Dual-AS: One ASN			S: Unique / e ASN for	ASN per Leaf/Border all Leafs/Borders	
	* Underlay	Subnet IP N	lask 30	30 V 🕢 Mask for Underlay Subnet IP Range			v Subnet IP Range		
	Man Add	ual Underla ress Alloca	ay IP 🗌 🕜	Checking this will	disable Dynamic	Underlay IP	Address A	llocations	
* Un	derlay Routi	ng Loopbao Ra	k IP 10.2.0.0	/22		Typically	y Loopbac	k0 IP Address Range	
,	* Underlay S	ubnet IP Ra	ange 10.4.0.0	/16		Address	range to	assign Numbered and Peer Li	nk SVI IPs
,	* Subinterfac	e Dot1q Ra	ange 2-511			Per Bor	der Dot1q	Range For VRF Lite Connecti	vity (Min:2, Max:4093
NX-OS Software Image Version					▼	If Set, Ir Images Can	nage Vers Be Upload	ion Check Enforced On All Sw ded From Control:Image Uploa	vitches. ad

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

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

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

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

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

ファブリックは、スパインスイッチのAS番号によって識別されます。

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

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

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

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

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

[NX-OSソフトウェアイメージバージョン (NX-OS Software Image Version)]:ドロッ プダウンリストからイメージを選択します。 イメージアップロードオプションを使用して Cisco NX-OS ソフトウェアイメージをアッ プロードすると、アップロードされたイメージがこのフィールドにリストされます。イ メージを選択すると、システムはスイッチに選択したバージョンがあるかどうかを確認 します。選択されていない場合、エラーメッセージが表示されます。[解決(Resolve)] をクリックすることで、エラーを解決できます。イメージ管理画面が表示され、ISSUオ プションを処理できます。その代わりに、リリースナンバーを削除した後で保存するこ とも可能です。

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

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

4. [EVPN] をクリックします。このタブのほとんどのフィールドは自動入力されます。該 当するフィールドは次のとおりです。

General	EVPN	vPC	Pro	tocols	Advanced	Manage	abil	ity	Bootstrap	Configuration Backup	
F	nable EVPN		verlav								
Fi	rst Hop Redu	Indancy Pro	otocol					(2) HSRP or VRRP			
	* Anycas	t Gateway	MAC	2020.00	000.00aa			0	Shared MAC add	ress for all leafs (xxxx.xxxx.xx	(X)
	Enab	le VXLAN	OAM	✓ 0	For Operations, A	dministratio	n, an	d Ma	nagement Of VXL	AN Fabrics	
Enable Tenant DHCP											
vPC advertise-pip			e-pip		For Primary VTEF	PIP Advertis	eme	nt As Next-Hop Of Prefix Routes			
* Replication Mode			Mode	Multicast			0	Replication Mode for BUM Traffic			
	* Multicas	t Group Su	ubnet	239.1.1.0/25			()	Multicast address	with prefix 16 to 30		
Enal	ble Tenant R	outed Mul	ticast	For Overlay Multicast Support In V				IXLAN Fabrics			
Default	MDT Addres	s for TRM	VRFs					0	IPv4 Multicast Ad	iress	
	* Ren	dezvous-P	oints	2				0	Number of spines	s acting as Rendezvous-Point	RP)
		* RP I	Mode	asm			•	0	Multicast RP Mod	le	
	* Underlay F	RP Loopba	ack Id	254				?	(Min:0, Max:1023)	
	ι	Jnderlay Pr RP Loopba	imary ack Id					?	Used for Bidir-PI	M Phantom RP (Min:0, Max:10	23)
	ι	Jnderlay Ba RP Loopba	ackup ack Id					?	Used for Fallback	a Bidir-PIM Phantom RP (Min:0	, Max:1023)
	Underlay	Second Ba RP Loopba	ackup ack Id					?	Used for second	Fallback Bidir-PIM Phantom R	P (Min:0, Max:1023)
	Underl	ay Third Ba RP Loopba	ackup ack Id					?	Used for third Fal	lback Bidir-PIM Phantom RP (Min:0, Max:1023)
		VRF Tem	plate	Default_	VRF_Universal		▼	?	Default Overlay V	/RF Template For Leafs	
	* Ne	twork Tem	plate	Default_	Network_Universa	ıl	▼	?	Default Overlay N	letwork Template For Leafs	
	* VRF Exte	nsion Tem	plate	Default_	VRF_Extension_L	Iniversal	▼	?	Default Overlay V	/RF Template For Borders	
* N	etwork Exte	nsion Tem	plate	Default_	Network_Extensio	n_Universa	▼	?	Default Overlay N	letwork Template For Borders	
* Underla	y VTEP Loop	back IP R	ange	10.3.0.0)/22			?	Typically Loopbac	ck1 IP Address Range	
* Unde	rlay RP Loop	back IP R	ange	10.254.	254.0/24			?	Anycast or Phant	om RP IP Address Range	
*	Layer 2 VX	LAN VNI R	ange	30000-4	19000			?	Overlay Network	Identifier Range (Min:1, Max:1	6777214)
*	Layer 3 VX	LAN VNI R	ange	50000-5	59000			?	Overlay VRF Ider	ntifier Range (Min:1, Max:1677	7214)
	* Netwo	rk VLAN R	ange	2300-29	999			?	Per Switch Overla	ay Network VLAN Range (Min:	2, Max:3967)
	* VF	RF VLAN R	ange	2000-22	299			?	Per Switch Overla	ay VRF VLAN Range (Min:2, N	lax:3967)
	* VRF L	ite Deploy	ment	Manual			▼	?	VRF Lite Inter-Fa	bric Connection Deployment C	ptions

[EVPN VXLAN オーバーレイを有効にする(Enable EVPN VXLAN Overlay)]: ファブ リックの VXLAN オーバーレイ プロビジョニングを有効にします。

このオプションを選択すると、ルーテッドファブリックをVXLAN対応のファブリック に変換できます。ファブリックでVXLANが有効になっている場合、オーバーレイネッ トワークまたはVRFを作成して展開できます。ネットワークまたはVRFを作成して展 開する手順は、Easy_Fabric_11_1の場合と同じです。詳細については、『*Cisco DCNM LANファ*ブリックの構成ガイド』の「ネットワークおよび*VRF*の作成と展開」章を参照 してください。

[ルーテッドファブリック (Routed Fabric)]: ルーテッドファブリック (VXLAN カプ セル化のないIPファブリック)を作成するためには、EVPN VXLAN オーバーレイフィー ルドの有効化を無効にする必要があります。ルーテッドファブリックでは、ネットワー クを作成して展開できます。詳細については、ルーテッドファブリックのネットワーク の概要を参照してください。

eBGP ルーテッドまたは eBGP VXLAN ファブリックを作成する場合、ファブリックは eBGP をコントロール プレーンとして使用して、ファブリック内接続を構築します。ス パインスイッチとリーフスイッチ間のリンクは、上側で eBGP ピアリングが構築された ポイント ツー ポイント (p2p) 番号付き IP アドレスで自動構成されます。

ファブリック内にネットワークまたはVRFが作成されている場合、[EVPNVXLANオー バーレイを有効にする(Enable EVPN VXLAN Overlay)] チェック ボックスを選択し て、VXLAN EVPN モードとルーテッド ファブリック モードを切り替えることはできま せん。ファブリック設定を変更するには、これらのネットワークまたはVRFを削除する 必要があります。

Routed_Network_Universal テンプレートは、ルーテッドファブリックにのみ適用される ことに注意してください。ルーテッドファブリックを EVPN VXLAN ファブリックに変 換する場合は、ネットワーク テンプレートとネットワーク拡張テンプレートを、EVPN VXLAN に定義されているものに設定します: Default_Network_Universal と Default_Network_Universal です。EVPN VXLAN ファブリック用にカスタマイズされた

[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。

テンプレートがある場合は、それを使用することも選択できます。



Note

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

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

[VXLAN OAM を有効にする(Enable VXLAN OAM)]:既存のスイッチの VXLAN OAM機能を有効にします。この設定はデフォルトでイネーブルになっています。VXLAN OAM 機能を無効にするにはチェックボックスをクリアします。

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



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

[テナント DHCP を有効にする(Enable Tenant DHCP)]: テナント DHCP サポートを有 効にします。

[vPC advertise-pip]: アドバタイズ PIP 機能を有効にするには、[vPC advertise-pip] チェッ クボックスをオンにします。 [レプリケーションモード (Replication Mode)]:ファブリック、入力レプリケーション、またはマルチキャストで使用されるレプリケーションのモードです。

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

[テナントルーテッドマルチキャストを有効にする(Enable Tenant Routed Multicast)]: ファブリックオーバーレイマルチキャストプロトコルとしてテナントルーテッドマル チキャスト(TRM)を有効にするには、チェックボックスをオンにします。

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

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

[RPモード (RP mode)]: ASM (エニーソース マルチキャスト (ASM) の場合)また は BiDir (双方向 PIM (BIDIR-PIM) の場合)の、サポート対象の2つのマルチキャスト モードからいずれかを選択します。[ASM]を選択すると、[BiDir] 関連のフィールドは有 効になりません。[BiDir] を選択すると、[BiDir] 関連フィールドが有効になります。

Ø

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

[アンダーレイ RP ループバック ID (Underlay RP Loopback ID)]: ファブリック アン ダーレイでのマルチキャスト プロトコル ピアリングの目的で、ランデブーポイント (RP) に使用されるループバック ID です。デフォルトは 254 です。

[双方向(bidir)]を選択すると、以下のフィールドが有効になります。RPカウントに応じて、2つまたは4つのファントム RP ループバック ID フィールドが有効になります。

- •[アンダーレイ プライマリ RP ループバック ID (Underlay Primary RP Loopback ID)]:ファブリック アンダーレイでマルチキャストプロトコル ピアリングのため にファントム RP に使用されるプライマリ ループバック ID です。
- 「アンダーレイ バックアップ RP ループバック ID (Underlay Backup RP Loopback ID)]:ファブリックアンダーレイでマルチキャストプロトコル ピアリングを目的 として、ファントム RP に使用されるセカンダリ(つまりバックアップ)ループバッ ク ID です。

次のループバック ID オプションは、RP カウントが 4 の場合にのみ適用されます。

•[アンダーレイセカンドバックアップRPループバックID (Underlay Second Backup RP Loopback ID)]: ファブリックアンダーレイでマルチキャストプロトコルピア リングを目的としてファントム RP に使用される、第二のバックアップ ループバッ ク ID です。

•[アンダーレイ サード バックアップ RP ループバック ID (Underlay Third Backup RP Loopback ID)]: ファブリック アンダーレイでマルチキャスト プロトコル ピア リングを目的としてファントム RP に使用される、第三のバックアップ ループバッ ク ID です。

[VRF テンプレート (VRF Template)]および [VRF 拡張テンプレート (VRF Extension Template)]: VRF を作成するための VRF テンプレートと、他のファブリックで VRF 拡張を有効にするための VRF 拡張テンプレートを指定します。

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

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

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

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

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

[VRF Lite の展開(VRF Lite Deployment)]:ファブリック間接続を拡張するためのVRF Lite 方式を指定します。[手動(Manual)] オプションのみがサポートされています。

5. [vPC] をクリックします。このタブのフィールドは次のとおりです。

General	EVPN	vPC	Pro	otocols	Advanced	Manageabi	lity	Bootstrap	Configuration Backup	
Make vP	* vPC F C Peer Link V	Peer Link \ VLAN as N	/LAN ative	3600] (j)			i) V	LAN for vPC Pee	r Link SVI (Min:2, Max:3967)	
*.	vPC Peer Ke	ep Alive o	ption	managen	nent	•	i) U	se vPC Peer Kee	p Alive with Loopback or Mana	gement
	* vPC Auto	Recovery	Time	360			i) A	uto Recovery Tim	e In Seconds (Min:240, Max:3	600)
	* vPC Dela	y Restore	Time	150			i) vi	PC Delay Restore	Time For vPC links in second	s (Min:1, Max:3600)
vPC Peer	Link Port C	hannel Nu	mber	500			i) P	ort Channel ID for	vPC Peer Link (Min:1, Max:40	<i>)96)</i>
	vPC IPv6 N	ID Synchro	onize	✓ (i) E	nable IPv6 ND sy	nchronization be	tween	vPC peers		
	Fabric wide	vPC Doma	ain Id	(i) E	nable to use sam	ə vPC Domain Ic	l on al	I vPC pairs in the	fabric	
		vPC Dom	ain Id				i) vi	PC Domain Id to b	be used on all vPC pairs in the	fabric
Enable	Qos for Fabr	ic vPC-Pe	ering	(i) G	los on spines for g	guaranteed deliv	ery of	vPC Fabric Peerii	ng communication	
	c	os Policy N	lame				(j) Q	os Policy name s	hould 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 プバックを選択します。IPv6 アドレスを使用する場合は、ループバック ID を使用する 必要があります。

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

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

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

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

[ファブリック全体の vPC ドメイン ID (Fabric wide vPC Domain Id)]: ファブリック内 のすべての vPC ペアで同じ vPC ドメイン ID の使用を有効にします。このフィールドを 選択すると、[vPC ドメイン ID (vPC Domain Id)]フィールドが編集可能になります。

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

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

[QoS ポリシー名(QoS Policy Name)]: すべてのスパインで同じにする必要がある QoS ポリシー名を指定します。

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

General	EVPN	vPC	Prot	tocols	Advanced	Manageab	ility	Bootstrap	Configuration Backup
			-						
	* Routir	ng Loopba	ck Id	0			(i)	(Min:0, Max:1023)	
	* VTE	EP Loopba	ck Id	1			(i)	(Min:0, Max:1023)	
	* BGP N	/laximum F	Paths	4			(i)	(Min:1, Max:64)	
	Enable BGP	Authentic	ation [(<i>i</i>)					
	BGP Au	thenticatior Encryption	n Key Type			▼	<i>i</i>)	BGP Key Encryptio	n Type: 3 - 3DES, 7 - Cisco
	BGP Au	thentication	n Key				(i)	Encrypted BGP Aut	hentication Key based on type
Enab	le PIM Hello	Authentic	ation [(<i>i</i>)					
	PIM Hello Au	thentication	n Key				(i)	3DES Encrypted	
		Enable	BFD	(i)					
	Enab	le BFD For	BGP	(i)					
	Enable BFI	D Authentic	cation	i					
	BFD Authe	entication K	ey ID				(i)		
	BFD Au	thentication	n Key				i	Encrypted SHA1 se	cret 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。

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

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

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

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

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

Note

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

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

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

[BFDの有効化(Enable BFD)]:ファブリック内のすべてのスイッチで機能[bfd]を有効 にするには、このチェックボックスをオンにします。この機能は、IPv4アンダーレイで のみ有効で、範囲はファブリック内にあります。 Cisco DCNM リリース 11.3(1) 以降、ファブリック内の BFD はネイティブにサポートされます。ファブリック設定では、BFD機能はデフォルトで無効になっています。有効にすると、デフォルト設定のアンダーレイ プロトコルに対して BFD が有効になります。カスタムの必須 BFD 構成は、スイッチごとの自由形式またはインターフェイスごとの自由形式ポリシーを使用して展開する必要があります。

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

feature bfd

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

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

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

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

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

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

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

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

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

General	EVPN	vPC	Protocols	Advanced	Manageabilit	/ Bootstrap	Configuration Backup	
	* Intra Fabrio	: Interface N	9216		(1) (Min:576, Max:921	6). Must be an even number	
*	Layer 2 Hos	t Interface N	ITU 9216		(i) (Min:1500, Max:92	16). Must be an even number	
	* Powe	er Supply Me	ps-redun	dant	V) Default Power Sup	ply Mode For The Fabric	
		* CoPP Pro	file strict		▼ (i	Fabric Wide CoPP seperately defined,	Policy. Customized CoPP polic when 'manual' is selected	ry should be
	VTEP H	loldDown T	me 180		() NVE Source Intefa	ce HoldDown Time (Min:1, Max	c:1500) in seconds
3	* VRF Lite S	ubnet IP Ra	10.33.0.	0/16	(i) Address range to a	ssign P2P DCI Links	
	* VRF Lif	e Subnet M	ask 30		(i) Mask for Subnet R	ange (Min:8, Max:31)	
Enable C	DP for Boots	trapped Swi	tch 🗌 i E	nable CDP on ma	anagement interfac	9		
		Enable NX-	api 🗹 i e	nable NX-API on	port 443			
E	Enable NX-AF	l on HTTP p	ort 🗹 🤅 E	nable NX-API on	port 80			
Enab	le Strict Con	fig Complia	nce 🗌 i E	nable bi-direction	al compliance cheo	ks to flag additional o	configs in the running config tha	t are not in the intent/expected config
E	nable AAA II	P Authorizat	ion 🗌 i E	nable only, when	IP Authorization is	enabled in the AAA S	Server	
	Enable DCN	M as Trap H	ost 🗹 (i) (Configure DCNM a	as a receiver for SN	MP traps		
	Greenfield	Cleanup Opt	ion Disable		▼ (i	Switch Cleanup W When PreserveCon	ithout Reload fig=no	
Enat	ole Default Q	euing Polic	ies 🗌 i					
	N9K Cloue	d Scale Platfo Queuing Po	licy			Queuing Policy for series switches in th	all 92xx, -EX, -FX, -FX2, -FX3 e fabric	
	N9K R	Series Platfo	orm		▼ (i	Queuing Policy for	all R-Series	

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

テンプレート エディタでポリシー ファイルを開いて、実際のキューイング ポリシーを 確認します。Cisco DCNM Web UI から、[制御(Control)] > [テンプレート ライブラリ

(Template Library)]を選択します。ポリシー ファイル名でキューイング ポリシーを 検索します(例:[queuing_policy_default_8q_cloudscale])。ファイルを選択し、[テンプ レートの変更/表示(Modify/View template)]アイコンをクリックしてポリシーを編集し ます。

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

[N9K クラウドスケール プラットフォームのキューイング ポリシー (N9K Cloud Scale Platform Queuing Policy)]: ファブリック内の EX、FX、および FX2 で終わるすべての Cisco Nexus 9200 シリーズスイッチおよび Cisco Nexus 9000 シリーズスイッチに適用する キューイング ポリシーをドロップダウン リストから選択します。有効な値は [queuing policy default 4q cloudscale]および [queuing policy default 8q cloudscale]です。

FEX には [queuing_policy_default_4q_cloudscale] ポリシーを使用します。FEX がオフラインの場合にのみ、[queuing_policy_default_4q_cloudscale] ポリシーから [queuing policy default 8q cloudscale] ポリシーに変更できます。

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

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

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

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

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

8. 管理能力(Manageability) タブをクリックします。

General	EVPN	vPC	Protocols	Advanced	Manageability	Bootstrap	Configuration Backup
	D	NS Server	IPs		0	Comma separated	d list of IP Addresses(v4/v6)
	DN	S Server VI	RFs		list of	One VRF for all D f VRFs, one per D	INS servers or a comma separated DNS server
	N	TP Server	IPs		0	Comma separated	d list of IP Addresses(v4/v6)
	NTI	P Server VI	RFs		list of	One VRF for all N f VRFs, one per N	ITP servers or a comma separated ITP server
	Sysl	log Server	IPs		0	Comma separated	d list of IP Addresses(v4/v6)
	Syslog S	Server Seve	erity		one j	Comma separated per Syslog server	d list of Syslog severity values, (Min:0, Max:7)
	Syslo	g Server VI	RFs		list of	One VRF for all S f VRFs, one per S	yslog servers or a comma separate Syslog server
	AAA Fre	eform Co	nfig		eestrict with Any unex	Note ! All configs ly match 'show ru respect to case ar mismatches will y pected diffs durin	should n' output, nd newlines. ield a denlov.

このタブのフィールドは次のとおりです。

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

[DNS サーバー VRF (DNS Server VRFs)]: すべての DNS サーバーに 1 つの VRF を指 定するか、DNS サーバーごとに 1 つの VRF を、カンマ区切りリストで指定します。 [**NTP サーバー IP** (**NTP Server IPs**)]: NTP サーバーの IP アドレス (v4/v6) のカンマ 区切りリストを指定します。

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

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

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

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

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

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

9. [ブートストラップ (Bootstrap)] タブをクリックします。

General	EVPN	vPC	Protocols	Advanced	Manageabi	ility	Bootstrap	Configuration Backup	
	Er Enable Loc	able Boot	strap 🗌 🕜 /	Automatic IP Assig Automatic IP Assig	gnment For POA gnment For POA	P P From	n Local DHCP Se	erver	
		DHCP Ve	ersion			?			
	DHCP Sco	be Start Ad	dress			? s	tart Address For	Switch Out-of-Band POAP	
	DHCP Sco	pe End Ad	dress			e	nd Address For	Switch Out-of-Band POAP	
	Switch Mgmt	Default Gat	eway			e C	efault Gateway I	For Management VRF On The S	Switch
	Switch Mgmt	IP Subnet F	Prefix			()	Min:8, Max:30)		
Sv	witch Mgmt IP	v6 Subnet F	Prefix			()	Min:64, Max:126)		
	En	able AAA C	onfig 🗌 🕜	nclude AAA config	gs from Manage	ability t	ab during device	bootup	
	Bootstrap	Freeform C	config			stric with Any unex	Note ! All configs tly match 'show r respect to case a mismatches will opected diffs duri	s should un' output, and newlines. yield ng deploy.	
DHCPv4	4/DHCPv6 Mu	lti Subnet S	icope			? Sta e.g 10. 10. 0r 21: 21:	Enter One Subi rt_IP, End_IP, Ga 6.0.2, 10.6.0.9, 1 7.0.2, 10.7.0.9, 1 0:1:1::10, 21:0:1: 0:1:2::10, 21:0:1:	net Scope per line. ateway, Prefix 0.6.0.1, 24 0.7.0.1, 24 1::20, 21:0:1:1::1, 64 2::20, 21:0:1:2::1, 64	

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

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

外部 DHCP サーバ(External DHCP Server): [スイッチ管理デフォルト ゲートウェイ(Switch Mgmt Default Gateway)]および[スイッチ管理 IP サブネット プレフィックス(Switch Mgmt IP Subnet Prefix)]外部 DHCP サーバに関する情報を入力します。

•[ローカル DHCP サーバー(Local DHCP Server)]: [ローカル DHCP サーバー(Local DHCP Server)]チェックボックスを有効にして、残りの必須フィールドに詳細を入力します。

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

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

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



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

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

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

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

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

[スイッチ管理 IPv6 サブネット プレフィックス(Switch Mgmt IPv6 Subnet Prefix)]:ス イッチの Mgmt0 インターフェイスの IPv6 プレフィックスを指定します。プレフィック スは 112 ~ 126 の範囲で指定する必要があります。このフィールドは DHCP の IPv6 が有 効な場合に編集できます。 [AAA 構成を有効化(Enable AAA Config)]: デバイスの起動時に[管理性 (Manageability)]タブから AAA 構成を含めるには、このチェックボックスをオンにし ます。

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

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

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

スコープの形式は次の順で定義する必要があります。

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

例:10.6.0.2、10.6.0.9、16.0.0.1、24

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

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		? 7	Time in 24hr forma	at. (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にのみ発生し、最大1時間の遅延が発生する可能性が あります。即時バックアップをトリガーするには、次の手順を実行します。
 - a. [制御(Control)]>[ファブリックビルダ(Fabric Builder)] を選択します。[Fabric Builder] 画面が表示されます。
 - **b.** 特定のファブリック ボックス内をクリックします。[ファブリック トポロジ(fabric topology)] 画面が表示されます。
 - **c.** 画面左側の [**アクション**(Actions)]パネルで、[**ファブリックの再同期**(Re-Sync Fabric)]をクリックします。

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

関連情報を入力して更新したら、[保存(Save)]をクリックします。

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

General	Replication	vPC	Protocols	Advanced	Resources	Manageability	Bootstrap	Configuration Backup	ThousandEyes Agent	
Thous	Enable Fabric Ov sandEyes Agent Ir	verride for stallation	(j)							
Т	housandEyes Acco	ount Group Token			(i) Tok	en from ThousandEye	es Agent Settings	for Agent Installation		
VRF	on Switch for Thou Agent Collector R	usandEyes eachability			(i) NX-	-OS VRF that provides	s Internet Reachal	bility		
	DN	IS Domain			i DN	S Domain Configuratio	n			
	DNS	Server IPs			(i) Cor	mma separated list of	IP Addresses(v4/v	r6)		
	NTP	Server IPs			(i) Cor	mma separated list of	IP Addresses(v4/v	6)		
Ena	able Proxy for Inter	net Access	i Proxy 3	Settings for NX-OS	S Switch Internet A	ccess				
	Proxy I	nformation			i) Pro	xy-Server:port				
	Pro	oxy Bypass			(i) Cor	nma separated No-pr	oxy server list			
									Save	Ca

このタブのフィールドは次のとおりです。

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

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

eBGP アンダーレイを備えた VXLAN ファブリック:ポインタ

- ・すべてのリーフスイッチには共通のAS番号があるため、リーフオーバーレイポリシー とアンダーレイポリシーを一度にすべてのリーフスイッチに展開します。
- ・ブラウンフィールド移行は、eBGPファブリックではサポートされていません。
- リーフスイッチのAS番号は、作成後に再計算と展開(Recalculate & Deploy)操作を実行した後は変更できません。変更が必要になった場合は、leaf_bgp_asnポリシーを削除し、再計算と展開(Recalculate & Deploy)操作を実行して、このASに関連するBGP構成を削除する必要があります。次に、新しいAS番号を使用して、leaf_bgp_asnポリシーを追加できます。

- Multi-ASモードと Dual-ASモードを切り替える場合は、モードを変更する前に、手動で追加されたすべての BGP ポリシー (リーフスイッチの Leaf_bgp_asn および ebgp オーバーレイポリシーを含む)を削除し、[保存と展開(Save & Deploy)]操作を実行します。
- デバイスに ebgp オーバーレイ ポリシーが存在する場合、リーフスイッチの leaf_bsp_asn ポリシーを変更または削除することはできません。最初に ebgp オーバーレイ ポリシーを 削除してから、leaf bgp asn ポリシーを削除する必要があります。
- サポートされているロールは、リーフ、スパイン、ボーダーリーフです。
- ボーダーデバイスでは、VRF-Liteは手動モードでサポートされます。外部接続のマルチ サイトサポートはありません。
- TRM はサポートされています。
- 機能ファブリックのリーフスイッチとスパインスイッチにポリシーを適用する必要があります。
- VXLAN対応ファブリックの場合、Easy Fabric と同じ方法でオーバーレイネットワークと VRFを作成して展開できます。詳細については、『Cisco DCNM LAN ファブリックの構成 ガイド』の「ネットワークおよび VRF の作成と展開」章を参照してください。

ファブリック アンダーレイ eBGP ポリシーの展開



トポロジは、eBGP アンダーレイが有効化された VXLAN ファブリックを表示します。DCNM では、[Easy_Fabric_eBGP] テンプレートを持つファブリックが作成されます。1つのスパイン スイッチ (n9k-29) と 3 つのリーフスイッチ (n9k-30、および vPC スイッチ ペア: n9k-31 と n9k-32) がインポートされています。

ファブリックには次の2種類があります。

- マルチASモードファブリックの作成:マルチASモードファブリックでは、スパイン スイッチには共通のBGPAS番号があり、各リーフスイッチには一意のBGPAS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。
- 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。



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

ファブリック オーバーレイ eBGP ポリシーの展開

オーバーレイ ピアリングの eBGP オーバーレイ ポリシーは手動で追加する必要があります。 DCNM は、リーフおよびスパイン スイッチに手動で追加して EVPN オーバーレイ ピアリング を形成できる eBGP リーフおよびスパイン オーバーレイ ピアリング ポリシー テンプレートを 提供します。

スパイン スイッチ オーバーレイ ポリシーの展開

ebgp_overlay_spine_all_neighbor ポリシーをスパイン スイッチ n9k-29 に追加します。このポリ シーは、すべてのスパインスイッチで同じフィールド値を共有するため、一度にすべてのスパ イン スイッチに展開できます。

Policy: ebg	p_overlay_spine_all_neighbor]	
G	eneral		
	* Leaf IP List	10.2.0.2,10.2.0.3,10.2.0.4	Iist of leaf IP address for peering list e.g. 10.
	* Leaf BGP ASN	30,31,31	BGP ASN of each leaf, separated by ,
	* BGP Update-Source Interface	loopback0	Source of BGP session and updates
	Enable Tenant Routed Multicast	Tenant Routed Multicast setting network	eeds to match the fabric setting
/ariables:	Enable BGP Authentication	BGP Authentication needs to mate	ch the fabric setting

この画面のフィールドは次のとおりです。

[リーフIP リスト(Leaf IP List)]: リーフスイッチルーティングループバックインターフェ イスの IP アドレス。

10.2.0.2 は、リーフスイッチ n9k-30 のループバック 0 ピアリング IP アドレスです。10.2.0.3 および 10.2.0.4 は、vPC スイッチ ペア n9k-31 および n9k-32 の IP アドレスです。

[リーフ BGP ASN (Leaf BGP ASN)]: リーフ スイッチの BGP AS 番号。vPC スイッチの AS 番号は同じ 31 であることに注意してください。

Save

Cancel



 (注) デュアル AS モードでファブリックを作成する場合(またはデュアル AS モードに変換す る場合)、すべてのリーフスイッチが属する共通のBGP AS 番号でこのフィールドを更新 する必要があります。

[**BGP アップデート送信元インターフェイス (BGP Update-Source Interface)**]: BGP アップ デートの送信元インターフェイスです。このフィールドでは loopback0、つまり、アンダーレ イ ルーティングのループバック インターフェイスを使用できます。

[テナントルーテッドマルチキャストを有効にする(Enable Tenant Routed Multicast)]: チェッ クボックスをオンにして、オーバーレイマルチキャストトラフィックを処理するためのTRM を有効にします。TRM の有効化は、ファブリック設定と一致する必要があります。

[**BGP 認証の有効化(Enable BGP Authentication**)]: BGP 認証を有効にするにはチェックボッ クスをオンにします。

BGP認証は、ファブリック設定と一致する必要があります。BGP認証の詳細については、「認証キーの取得」セクションを参照してください。

リーフ スイッチ オーバーレイ ポリシーの展開

すべてのリーフスイッチに ebgp_overlay_leaf_all_neighbor ポリシーを追加して、スパインス イッチへの eBGP オーバーレイ ピアリングを確立します。このポリシーは、すべてのリーフ スイッチで同じフィールド値を共有するため、一度にすべてのリーフスイッチに展開できま す。

Add Policy			×
* Priority (1-1000):	500		
* Policy:	ebgp_overlay_leaf_all_neighbor		
	General		
			O list of anima ID address for a series list and 40.0
	[^] Spine IP List	10.2.0.1	Ist of spine IP address for peering list e.g. 10.2.
	* BGP Update-Source Interface	loopback0	Source of BGP session and updates
	Enable Tenant Routed Multicast	For Overlay Multicast Support In V	/XLAN Fabrics
	Enable BGP Authentication	BGP Authentication needs to mate	ch the fabric setting
Variables:			

Save Cancel

1

この画面のフィールドは次のとおりです。

[スパインIPリスト (Spine IP List)]: スパインスイッチルーティングループバックインター フェイスの IP アドレス。

10.2.0.1 は、スパイン スイッチ n9k-29 のループバック 0 ピアリング IP アドレスです。

[**BGP アップデート送信元インターフェイス**(**BGP Update-Source Interface**)]: BGP アップ デートの送信元インターフェイスです。このフィールドでは loopback0、つまり、アンダーレ イ ルーティングのループバック インターフェイスを使用できます。

[テナントルーテッドマルチキャストを有効にする(Enable Tenant Routed Multicast)]: チェッ クボックスをオンにして、オーバーレイマルチキャストトラフィックを処理するためのTRM を有効にします。TRM の有効化は、ファブリック設定と一致する必要があります。

[**BGP 認証の有効化(Enable BGP Authentication**)]: BGP 認証を有効にするにはチェックボッ クスをオンにします。

BGP認証は、ファブリック設定と一致する必要があります。BGP認証の詳細については、「認 証キーの取得」セクションを参照してください。

画面の右上にある [保存と展開(Save & Deploy)]をクリックして、構成展開ウィザードごと に構成を展開します。または、[ポリシーの表示/編集(View/Edit Policy)]オプションを使用 し、[構成のプッシュ(Push Config)]をクリックして構成を展開します。

リーフ スイッチ オーバーレイ ポリシーの展開

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。