



Cisco DCNM サイトのインフラの設定

- [前提条件とガイドライン](#) (1 ページ)
- [インフラの設定: 一般設定](#) (1 ページ)
- [サイト接続性情報の更新](#) (3 ページ)
- [インフラの設定: DCNM サイトの設定](#) (3 ページ)
- [インフラ設定の展開](#) (6 ページ)

前提条件とガイドライン

次のセクションでは、全般とサイト固有のファブリックインフラ設定を行うために必要な手順について説明します。

インフラの設定を進める前に、前のセクションで説明したようにサイトを設定して追加する必要があります。

さらに、次の点に注意してください。

- 境界ゲートウェイスイッチの追加または削除には、Nexus Dashboard Orchestrator ファブリックの接続情報の更新が必要です。これは、一般インフラ設定の手順の一部として、[サイト接続性情報の更新](#) (3 ページ) で説明されています。

インフラの設定: 一般設定

ここでは、すべてのサイトの一般的なインフラ設定を構成する方法について説明します。

-
- ステップ 1** Cisco Nexus Dashboard Orchestrator の GUI にログインします。
 - ステップ 2** 左側のナビゲーションメニューで、[インフラストラクチャ (Infrastructure)] > [インフラの設定 (Infrastructure Configuration)] を選択します。
 - ステップ 3** メインペインにある [インフラの設定 (Configure Infra)] をクリックします。
 - ステップ 4** 左側のサイドバーで、[全般設定 (General Settings)] を選択します。
 - ステップ 5** [コントロールプレーン BGP (Control Plane BGP)] を設定します。

- a) **[コントロールプレーン BGP (Control Plane BGP)]** タブを選択します。
- b) **[BGP ピアリングタイプ (Bgp Peering Type)]** を選択します。
 - **full-mesh** : 各サイトのすべてのボーダー ゲートウェイ スイッチは、リモート サイトのボーダー ゲートウェイ スイッチとのピア接続を確立します。
 - **route-server** : route-server オプションを使用すると、各サイトが MP-BGP EVPN セッションを確立する 1 つ以上のコントロールプレーン ノードを指定できます。ルートサーバノードは、従来の BGP ルートリフレクタと同様の機能を実行しますが、EBGP (iBGP ではない) セッション用です。ルートサーバノードを使用すると、NDO によって管理されるすべての VXLAN EVPN サイト間で MP-BGP EVPN フルメッシュ隣接関係が作成されなくなります。
- c) **[BGP ピアリングタイプ (BGP Peering Type)]** を **[route-server]** に設定する場合は、**[+ルートサーバの追加 (+Add Route Server)]** をクリックして 1 つ以上のルートサーバを追加します。

[ルートサーバの追加 (Add Route Server)] ウィンドウが開きます。

- **[サイト (Site)]** ドロップダウンから、ルートサーバに接続するサイトを選択します。
- **ASN** フィールドには、サイトの ASN が自動的に入力されます。
- **[コア ルータ デバイス (Core Router Device)]** ドロップダウンから、接続するルートサーバを選択します。
- **[インターフェイス (Interface)]** ドロップダウンから、コア ルータ デバイスのインターフェイスを選択します。

ルートサーバは最大 4 つまで追加できます。複数のルートサーバを追加すると、すべてのサイトがすべてのルートサーバに対して MP-BGP EVPAN 隣接関係を確立します。

- d) **[キープアライブ間隔 (秒) (Keepalive Interval (Seconds))]**、**[ホールド間隔 (秒) (Hold Interval (Seconds))]**、**[ステート間隔 (秒) (State Interval (Seconds))]**、**[グレースフル ヘルパー (Graceful Helper)]**、**[最大 AS 制限 (Maximum AS Limit)]**、および **[ピア間の BGP TTL (BGP TTL Between Peers)]** フィールドは、Cisco ACI ファブリックにのみ関連するため、デフォルト値のままにします。
- e) Cisco Cloud ACI ファブリックのみに関連するため、**[OSPF エリア ID (OSPF Area ID)]** および **[外部サブネット プール (External Subnet Pool)]** フィールドをスキップします。

ステップ 6 [IPN デバイス (IPN Devices)] タブの設定をスキップします。

[IPN デバイス (IPN Devices)] タブの設定は、オンプレミス APIC サイトとクラウド APIC サイト間の Cisco ACI サイト間接続用です。Cisco DCNM サイトのみを管理する場合は、これらの設定をスキップできます。

ステップ 7 [DCNM 設定 (DCNM Settings)] を構成します。

- a) **[DCNM 設定 (DCNM Settings)]** タブを選択します。
- b) **L2 VXLAN VNI 範囲** を指定します。
- c) **L3 VXLAN VNI 範囲** を指定します。
- d) **マルチサイトルーティンググループバック IP 範囲** を指定します。

このフィールドは、各ファブリックの **Multi-Site TEP** フィールドに自動入力するために使用されます。
[インフラの設定: DCNM サイトの設定 \(3 ページ\)](#)

以前に DCNM のマルチサイトドメイン (MSD) の一部であったサイトの場合、このフィールドには以前に定義された値が事前に入力されます。

- e) エニーキャスト ゲートウェイ MAC を入力します。

サイト接続性情報の更新

ボーダーゲートウェイスイッチの追加や削除などのインフラストラクチャの変更には、Nexus Dashboard Orchestrator ファブリック接続の更新が必要です。このセクションでは、各サイトのコントローラ から直接最新の接続性情報を取得する方法を説明します。

- ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2 左側のナビゲーションメニューで、[インフラストラクチャ (Infrastructure)] > [インフラの設定 (Infrastructure Configuration)] を選択します。
- ステップ 3 メインペインにある [インフラの設定 (Configure Infra)] をクリックします。
- ステップ 4 左側のサイドバーの [サイト (Sites)] の下で、特定のサイトを選択します。
- ステップ 5 メインウィンドウで、コントローラ からファブリック情報を取得するために [更新 (Refresh)] ボタンをクリックします。
- ステップ 6 (任意) 使用停止されたボーダーゲートウェイスイッチの設定を削除する場合は、[確認 (Confirmation)] ダイアログで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有効にすると、現在使用されていないボーダーゲートウェイスイッチのすべての設定情報がデータベースから削除されます。
- ステップ 7 最後に、[はい (Yes)] をクリックして確認し、接続情報をロードします。

これにより、新しいスパインや削除されたスパインを検出し、すべてのサイトに関連したファブリックの接続をサイトのコントローラからインポートし直します。

インフラの設定: DCNM サイトの設定

ここでは、サイトとして、オンプレミスにサイト固有のインフラ設定を構成する方法について説明します。

- ステップ 1 Cisco Nexus Dashboard Orchestrator の GUI にログインします。
- ステップ 2 左側のナビゲーションメニューで、[インフラストラクチャ (Infrastructure)] > [インフラの設定 (Infrastructure Configuration)] を選択します。
- ステップ 3 メインペインにある [インフラの設定 (Configure Infra)] をクリックします。

ステップ 4 左側のペインの [サイト (Sites)] の下で、特定の DCNM を選択します。

ステップ 5 右側の <Site> [設定 (Settings)] サイドバーで、**マルチサイト VIP** を指定します。

このアドレスは、サイト間の L2 BUM および L3 マルチキャストトラフィックのために使用されます。この IP アドレスは、同じファブリックの一部であるすべてのボーダー ゲートウェイ スイッチに導入されます。

(注) 設定するサイトが DCNM マルチサイト ドメイン (MDS) の一部である場合、このフィールドには DCNM からインポートされた情報が事前に入力されます。この場合、値を変更してインフラ設定を再展開すると、MDS の一部であるサイト間のトラフィックに影響します。

[自動割り当て (Auto Allocate)] フィールドを選択すると、前のセクションで定義した **マルチサイト ルーティンググループバック IP 範囲** から次に使用可能なアドレスが割り当てられます。

ステップ 6 <fabric-name> タイル内で、ボーダー ゲートウェイを選択します。

ステップ 7 右側 <border-gateway> サイドバーを設定し、**BGP-EVPN ROUTER-ID** と **BGW PIP** を指定します。

vPC ドメインの一部であるボーダー ゲートウェイの場合は、**VPC VIP** も指定する必要があります。

ステップ 8 [ポートの追加 (Add Port)] をクリックして、IPN に接続するポートを設定します。

(注) このリリースでは、DCNM からのポート設定のインポートはサポートされていません。設定するサイトがすでに DCNM マルチサイト ドメイン (MDS) の一部である場合は、DCNM ですでに設定されている値と同じ値を使用する必要があります。

Update Port ✕

* Ethernet Port ID
Ethernet1/1 ✕ ▼

* IP Address
10.10.1.9/30

* Remote Address
10.10.1.10

* Remote ASN
65002

* MTU
9216

BGP Authentication
 None Simple

Save

このボーダー ゲートウェイをコア スイッチまたは別のボーダー ゲートウェイに接続するポートの展開に固有の次の情報を入力します。

- **[イーサネット ポート ID (Ethernet Port ID)]** ドロップダウンから、IPN に接続するポートを選択します。
- **[IP アドレス (IP Address)]** フィールドに、IP アドレス/ネットマスクを入力します。
- **[リモート アクセス (Remote Address)]** フィールドに、ポートが接続されているリモートデバイスの IP アドレスを入力します。
- **[リモート ASN (Remote ASN)]** フィールドに、リモートサイトの ID を入力します。
- **[MTU]** フィールドに、ポートの MTU を入力します。

スパイン ポートの MTU は、IPN 側の MTU と一致させる必要があります。

[継承 (inherit)] を指定することも、576 ~ 9000 の値を指定することもできます。

- **BGP 認証** の場合は、[なし (None)] または [シンプル (Simple)] (MD5) を選択できます。

[シンプル (Simple)] を選択した場合は、**[認証キー (Authentication Key)]** も指定する必要があります。

インフラ設定の展開

ここでは、各 DCNM サイトにインフラ設定を展開する方法について説明します。

始める前に

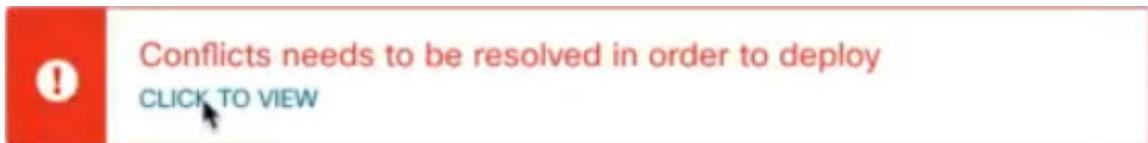
一般およびサイト指定のインフラ設定を完了しておく必要があります。このチャプターの前のセクションで説明されています。

ステップ 1 設定の競合がないことを確認するか、必要に応じて解決します。

各サイトですでに設定されている設定との設定の競合がある場合、[展開 (Deploy)] ボタンが無効になり、警告が表示されます。たとえば、同じ名前の VRF またはネットワークが複数のサイトに存在し、各サイトで異なる VNI を使用している場合です。

設定が競合する場合：

- a) 競合通知ポップアップの [クリックして確認 (Click to View)] リンクをクリックします。



- b) 競合の原因となっている特定の設定を書き留めます。

たとえば、次のレポートでは、fab1 サイトと fab2 サイトの VRF とネットワーク間に ID の不一致があります。

Error Type	Error Message
IDMismatch	Policy Name MyVRF_50001 Policy ID 50001 Sites [fab2] conflicting with Policy Name MyVRF_50001 Policy ID 60001 Sites [fab1]
IDMismatch	Policy Name MyNetwork_30000 Policy ID 40000 Sites [fab2] conflicting with Policy Name MyNetwork_30000 Policy ID 30000 Sites [fab1]

- c) [X] ボタンをクリックしてレポートを閉じ、インフラ設定画面を終了します。
 d) **サイトの削除** の説明に従って、NDO でサイトを管理解除します。

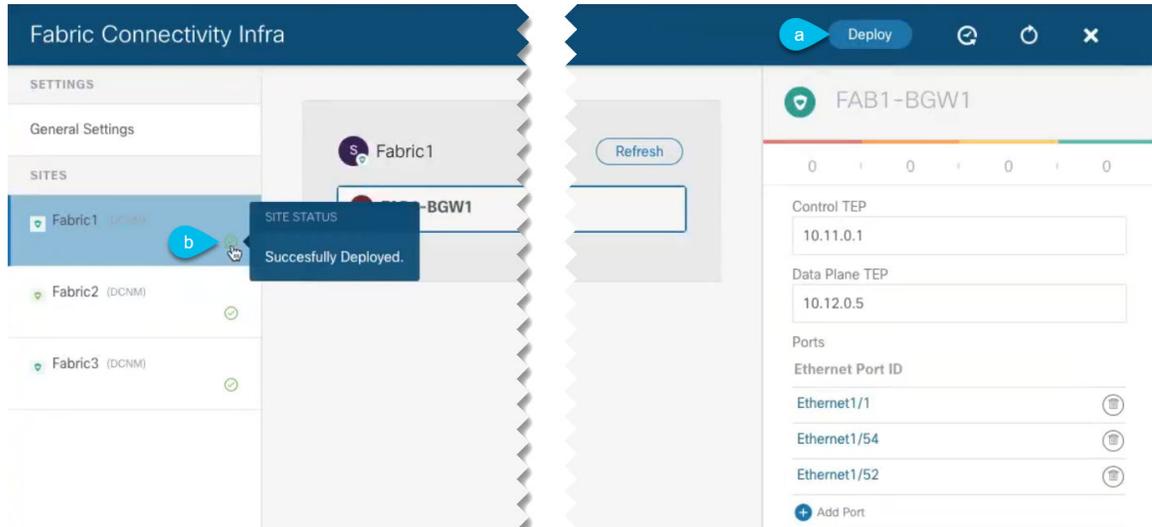
Nexus Dashboard からサイトを削除する必要はありません。NDO GUI でサイトを管理解除するだけです。

- e) 既存の設定の競合を解決します。
 f) の説明に従って、サイトを再度管理します。 [Cisco DCNM サイトの追加](#)

サイトはすでに Nexus Dashboard に追加されているため、NDO で管理できるようにします。

- g) すべての競合が解決され、[展開 (Deploy)] ボタンが使用可能であることを確認します。

ステップ2 設定の導入



- a) [ファブリック接続インフラ (Fabric Connectivity Infra)] 画面の右上で、適切な [展開 (Deploy)] オプションを選択して設定を展開します。

DCNM サイトのみを設定する場合は、[展開 (Deploy)] をクリックしてインフラ設定を展開します。

- b) 設定が展開されるのを待ちます。

インフラ設定を展開すると、NDO は DCNM にシグナリングして、ボーダーゲートウェイ間のアンダーレイと EVPN オーバーレイを設定します。

設定が正常に展開されると、[ファブリック接続インフラ (Fabric Connectivity Infra)] 画面のサイトの横に緑色のチェックマークが表示されます。

