



Cisco NDFC サイトのインフラの構成

- [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](#) (5 ページ)
- [インフラの構成: NDFC インフラ サイト固有の設定](#) (5 ページ)
- [インフラ設定の展開](#) (7 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や削除には、一般的なインフラの設定手順の一部として、[サイト接続性情報の更新](#) (5 ページ) に記載されている、Nexus Dashboard Orchestrator のファブリック接続情報の更新が必要です。

インフラの設定: 一般設定

このセクションでは、Nexus Dashboard Orchestrator によって搭載および管理される NDFC 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 Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。

ステップ 2 左のナビゲーションメニューから、[インフラストラクチャ (Infrastructure)] > [サイト接続 (Site Connectivity)] を選択します。

ステップ 3 メインペインにある [構成 (Configure)] 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設定 (Control Plane Configuration)] を指定します。

- a) [コントロールプレーン設定 (Control Plane Configuration)] 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。ルートサーバー 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) セッションでは使用しません。ルートサーバー 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、[+ルートサーバーを追加 (+ Add Route Server)] をクリックして、1 台以上のルートサーバーを追加します。

[ルートサーバーの追加 (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、ルートサーバー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ーを選択します。
- [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。

ルートサーバーは最大 4 台まで追加できます。複数のルートサーバーを追加すると、すべてのサイトがすべてのルートサーバーに対して MP-BGP EVPN 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)], [ステール間隔 (秒) (Stale Interval (Seconds))], [グレースフルヘルパー (Graceful Helper)], [最大 AS 限界 (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) Cloud Network Controller 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)] フィールドは、デフォルト値でスキップします。

ステップ 6 [オンプレミス IPsec デバイス情報 (On Premises IPsec Device)] を提供します。

オンプレミスとクラウドサイト間接続でプライベート接続を使用し、IPsec をエネーブル化しない場合は、この手順をスキップできます。パブリック インターネット経由の接続では、IPsec が常に有効になっており、この手順で情報を提供する必要があります。

後のセクションで説明するように、オンプレミスとクラウドサイト間のサイトアンダーレイ接続を設定する場合は、クラウド CSR への接続を確立するオンプレミス IPN デバイスを選択する必要があります。これらの IPN デバイスは、オンプレミスのサイト設定画面で使用可能になる前に、ここで定義する必要があります。

- a) [オンプレミス IPsec デバイス (On Premises IPsec Devices)] タブを選択します。
- b) + [オンプレミス IPsec デバイス (On Premises IPsec Devices)] の追加をクリックします。

- c) デバイスが[管理されていない (Unmanaged)]か[管理されている (Managed)]かを選択し、デバイス情報を入力します。

デバイスが NDFC に管理されているか否かを定義します:

- [管理されていない (Unmanaged)] IPN デバイスにはシンプルにデバイスの[名前 (Name)]と[IP アドレス (IP Address)]を入力してください。

指定した IP アドレスは、IPN デバイスの管理 IP アドレスではなく、クラウド CSR からのトンネルピアアドレスとして使用されます。

- [管理されている (Managed)] IPN デバイスには、デバイスが入っている NDFC [サイト (Site)]を選択し、そのサイトの[デバイス (Device)]を選択します。

インターネットに向いているデバイスに[インターフェイス (Interface)]を選択し、インターネット接続のゲートウェイの IP アドレスである[ネクストホップ (Next Hop)] IP アドレスを入力します。

- d) チェック マーク アイコンをクリックして、デバイス情報を保存します。
e) 追加する IPN デバイスについて、この手順を繰り返します。

ステップ 7 [IPSec トンネル サブネット プール (IPSec Tunnel Subnet Pools)] 情報を入力します。

ここで指定できるサブネットプールには、次の 2 つのタイプがあります。

- **外部サブネット プール**: クラウドサイトの CSR と他のサイト (クラウドまたはオンプレミス) 間の接続に使用されます。

これらは、Nexus Dashboard Orchestrator によって管理される大規模なグローバルサブネットプールです。Orchestrator は、これらのプールからより小さなサブネットを作成し、サイト間 IPsec トンネルと外部接続 IPsec トンネルで使用するサイトに割り当てます。

1 つ以上のクラウドサイトから外部接続を有効にする場合は、少なくとも 1 つの外部サブネットプールを提供する必要があります。

- **サイト固有のサブネット プール**: クラウドサイトの CSR と外部デバイス間の接続に使用されます。

これらのサブネットは、外部接続 IPsec トンネルが特定の範囲内にあることが必要な場合に定義できません。たとえば、外部ルータに IP アドレスを割り当てるために特定のサブネットがすでに使用されており、それらのサブネットを NDO およびクラウドサイトの IPsec トンネルで引き続き使用する場合があります。これらのサブネットは Orchestrator によって管理されず、各サブネットはサイト全体に割り当てられ、外部接続 IPsec トンネルにローカルで使用されます。

名前付きサブネットプールを指定しない場合でも、クラウドサイトの CSR と外部デバイス間の接続を設定すると、外部サブネットプールが IP 割り当てに使用されます。

(注) 両方のサブネットプールの最小マスク長は /24 です。

1 つ以上の外部サブネットプールを追加するには:

- a) [IPSec トンネル サブネット プール (IPSec Tunnel Subnet Pools)] タブを選択します。
b) [外部サブネット プール (External Subnet Pool)] エリアで、[+IP アドレスの追加 (+Add IP Address)] をクリックして、1 つ以上の外部サブネットプールを追加します。

このサブネットは、以前の Nexus Dashboard Orchestrator リリースでサイト間接続用に Cloud Network Controller で以前に設定した、オンプレミス接続に使用されるクラウドルータの IPsec トンネルインターフェイスとループバックに対処するために使用されます。

サブネットは、他のオンプレミス TEП プールと重複してはならず、0.xxx または 0.0.xx で始まってはならず、/16 と /24 の間のネットワーク マスク (30.29.0.0/16 など) が必要です。

- c) チェックマーク アイコンをクリックして、サブネット情報を保存します。
- d) 追加するサブネット プールについて、これらのサブステップを繰り返します。

1 つ以上の [サイト固有のサブネット プール (Site-Specific Subnet Pools)] を追加するには :

- a) [IPSec トンネル サブネット プール (IPSec Tunnel Subnet Pools)] タブを選択します。
- b) [サイト固有のサブネット プール (Site-Specific Subnet Pools)] エリアで、[+IP アドレスの追加 (+Add IP Address)] をクリックして、1 つ以上の外部サブネット プールを追加します。

[名前付きサブネットプールの追加 (Add Named Subnet Pool)] ダイアログが開きます。

- c) サブネットの [名前 (Name)] を入力します。
後ほど、サブネットプールの名前を使用して、IP アドレスを割り当てるプールを選択できます。
- d) [+IP アドレスの追加 (+Add IP Address)] をクリックして、1 つ以上のサブネットプールを追加します。
サブネットには /16 と /24 の間のネットワークが必要で、0.x.x.x または 0.0.x.x で始めることはできません。たとえば、30.29.0.0/16 のようにします。
- e) チェックマーク アイコンをクリックして、サブネット情報を保存します。
同じ名前付きサブネット プールに複数のサブネットを追加する場合は、この手順を繰り返します。
- f) [保存 (Save)] をクリックして、名前付きサブネットプールを保存します。
- g) 追加する名前付きサブネット プールについて、これらのサブステップを繰り返します。

ステップ 8 [NDFC 設定 (NDFC Settings)] を構成します。

- a) [NDFC 設定 (NDFC Settings)] タブを選択します。
- b) [L2 VXLAN VNI 範囲 (L2 VXLAN VNI Range)] 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ループバック IP 範囲 (Multi-Site Routing Loopback IP Range)] を指定します。

このフィールドは、各ファブリックの [マルチサイト TEП (Multi-Site TEП)] フィールドに自動入力するために使用されます。 [インフラの構成: NDFC インフラ サイト固有の設定 \(5 ページ\)](#) で説明します。

以前に NDFC 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 (Anycast Gateway 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 ファブリックの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** 左のナビゲーションメニューから、[インフラストラクチャ (Infrastructure)] > [サイト接続 (Site Connectivity)] を選択します。
- ステップ 3** メインペインの右上にある [構成 (Configure)] 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、特定のサイトを選択します。
- ステップ 5** メイン ウィンドウで、APIC 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 APIC からインポートし直します。

インフラの構成: NDFC インフラ サイト固有の設定

ここでは、オンプレミスサイト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** Nexus Dashboard にログインし、Nexus Dashboard Orchestrator サービスを開きます。
- ステップ 2** 左のナビゲーションメニューから、[インフラストラクチャ (Infrastructure)] > [サイト接続 (Site Connectivity)] を選択します。
- ステップ 3** メインペインにある [構成 (Configure)] 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 NDFC を選択します。
- ステップ 5** 右側の <Site>[設定 (Settings)] サイドバーで、[オーバーレイ マルチキャスト TEP (Overlay Multicast TEP)] 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 NDFC 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 NDFC 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、NDFC 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 NDFC マルチサイトドメイン (MDS) の一部である場合は、NDFC 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 アドレスとネットマスクを入力します。
- **[リモートアドレス (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、サーバーの 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** 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 NDFC 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

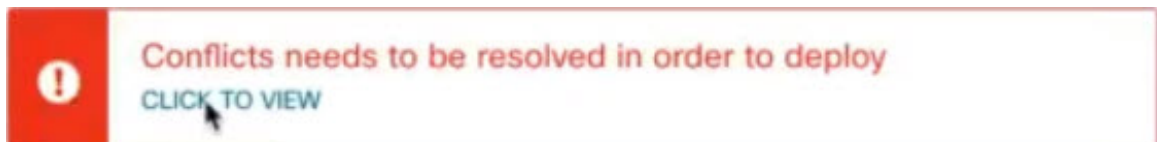
この章の前のセクションで説明したように、全般的な、およびサイト固有のインフラ設定を完了している必要があります。

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 **[クリックして表示 (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 でサイトの管理を解除します。

Nexus ダッシュボードからサイトを削除する必要はありません。NDO GUI でサイトの管理を解除するだけです。

- e) 既存の設定の競合を解決します。
- f) **Cisco NDFC サイトの追加**の説明に従って、サイトを再度管理状態にします。
サイトはすでに Nexus ダッシュボード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 設定を展開します。

- 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。

NDFC 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NDFCに信号を送り、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。

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。