



Cisco Cloud APIC サイトのインフラの設定

- [クラウド サイト接続性情報の更新 \(1 ページ\)](#)
- [インフラの設定: クラウド サイトの設定 \(2 ページ\)](#)

クラウド サイト接続性情報の更新

CSR やリージョンの追加や削除などのインフラストラクチャの変更には、Multi-Site ファブリック接続サイトの更新が必要です。このセクションでは、各サイトの APIC 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 [メイン メニュー (Main menu)] で、[インフラストラクチャ (Infrastructure)] > [インフラの設定 (Infra Configuration)] を選択します。

ステップ 3 右上にある [インフラの構成 (Infra Configuration)] ビューで、[インフラの設定 (Configure Infra)] ボタンをクリックします。

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 [更新 (Refresh)] ボタンをクリックして、新規または変更された CSR およびリージョンを検出します。

ステップ 6 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、新規または削除された CSR およびリージョンが検出されます。

ステップ 7 [導入 (Deploy)] をクリックして、クラウドサイトの変更を、接続している他のサイトに伝達します。

クラウドサイトの接続を更新し、CSR またはリージョンが追加または削除された後、インフラ設定を展開して、そのクラウドサイトへのアンダーレイ接続がある他のサイトが更新された設定を取得する必要があります。

インフラの設定: クラウドサイトの設定

ここでは、クラウド APIC 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 Cisco Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 2 [メインメニュー (Main menu)] 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 メインペインの右上にある [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、特定のクラウドサイトを選択します。

ステップ 5 [サイト間接続 (Inter-Site Connectivity)] 情報を入力します。

[オーバーレイ設定 (Overlay Configuration)] を入力します。

- a) 右側の [<Site> 設定 (Settings)] ペインで、[サイト間接続 (Inter-Site Connectivity)] タブを選択します。
- b) [オーバーレイ設定 (Overlay Configuration)] 領域で、[Multi-Site] ノブを有効にします。

これは、オーバーレイ接続がこのサイトと他のサイト間で確立されるかどうかを定義します。

- c) (オプション) [BGP パスワード (BGP Password)] を指定します。

[サイト間接続 (Inter-Site Connectivity)] 情報を入力します。

- a) [アンダーレイ設定 (Underlay Configuration)] 領域で、[接続の追加 (Add Connectivity)] をクリックします。
- b) [サイト (Site)] ドロップダウンから、接続を確立するサイトを選択します。
- c) [接続タイプ (Connection Type)] ドロップダウンから、サイト間の接続のタイプを選択します。

次のオプションを使用できます。

- [パブリックインターネット (Public Internet)] : 2つのサイト間の接続は、インターネットを介して確立されます。
このタイプは、任意の2つのクラウドサイト間、またはクラウドサイトとオンプレミスサイト間でサポートされます。
- [プライベート接続 (Private Connection)] : 2つのサイト間のプライベート接続を使用して接続が確立されます。
このタイプは、クラウドサイトとオンプレミスサイトの間でサポートされます。
- [クラウド バックボーン (Cloud Backbone)] : クラウドバックボーンを使用して接続が確立されます。
このタイプは、Azure-to-AzureやAWS-to-AWSなど、同じタイプの2つのクラウドサイト間でサポートされます。

複数のタイプのサイト (オンプレミス、AWS、Azure) がある場合、サイトの異なるペアは異なる接続タイプを使用できます。

- d) (オプション) **[IPsec]** を有効にします。

次のオプションを使用できます。

- パブリック インターネット接続の場合、IPsec は常に有効です。
- クラウド バックボーン接続の場合、IPsec は常に無効です。
- プライベート接続の場合、IPsec は有効または無効にすることができます。

- e) IPsec を有効にする場合は、**IKE バージョン** を選択します。

IP Security (IPSec) プロトコル確立のためのインターネットキー交換 (IKE) 設定に応じ、使用するプロトコルのバージョンとして IKEv1 (バージョン 1) または IKEv2 (バージョン 1) を選択できます。

- f) **[保存 (Save)]** をクリックして、設定を保存します。

site1 から site2 への接続情報を保存すると、site2 から site1 へのリバース接続が自動的に作成されます。これは、他のサイトを選択し、**[アンダーレイ設定 (Underlay Configuration)]** タブを選択することで確認できます。

- g) 他のサイトのサイト間接続を追加するには、この手順を繰り返します。

site1 から site2 へのアンダーレイ接続を確立すると、リバース接続が自動的に行われます。

ただし、site1 から site3 へのサイト間接続も確立する場合は、そのサイトに対してもこの手順を繰り返す必要があります。

ステップ 6 [外部接続 (External Connectivity)] 情報を入力します。

NDOによって管理されていない外部サイトまたはデバイスへの接続を設定する予定がない場合は、この手順をスキップできます。そうでなければ、次の情報を入力します。

- a) 右側の **[<Site> 設定 (Settings)]** ペインで、**[外部接続 (External Connectivity)]** タブを選択します。
b) **[外部接続の追加 (Add External Connectivity)]** をクリックします。

[外部接続の追加 (Add External Connectivity)] ダイアログが開きます。

- c) **[VRF]** ドロップダウンから、外部接続に使用する VRF を選択します。

これは、クラウドルートをリークするために使用される VRF です。**[リージョン (Regions)]** セクションには、この設定を適用する CSR を含むクラウドリージョンが表示されます。

- d) **[外部デバイス (External Devices)]** セクションの **[名前 (Name)]** ドロップダウンから、外部デバイスを選択します。

これは、一般的なインフラストラクチャ設定時に**[一般設定 (General Settings)]>[外部デバイス (External Devices)]** リストに追加した外部デバイスであり、**インフラの設定: 一般設定**の説明に従ってすでに定義されている必要があります。

- e) **[トンネル IKE バージョン (Tunnel IKE Version)]** ドロップダウンから、クラウドサイトの CSR と外部デバイス間の IPSec トンネルの確立に使用する IKE バージョンを選択します。

- f) (任意) **[トンネルサブネットプール (Tunnel Subnet Pool)]** ドロップダウンから、名前付きサブネットプールのいずれかを選択します。

名前付きサブネットプールは、クラウドサイトの CSR と外部デバイス間の IPSec トンネルに IP アドレスを割り当てるために使用されます。ここで**名前付きサブネットプール**を指定しない場合、**外部サブネットプール**が IP 割り当てに使用されます。

外部デバイス接続用の専用サブネットプールを提供することは、特定のサブネットがすでに外部ルータに IP アドレスを割り当てるために使用されており、それらのサブネットを NDO およびクラウドサイトの IPSec トンネルに引き続き使用する場合に役立ちます。

この接続に特定のサブネットプールを提供する場合は、[インフラの設定:一般設定](#)の説明に従って作成済みである必要があります。

- g) (オプション) **[事前共有キー (Pre-Shared Key)]** フィールドに、トンネルの確立に使用するカスタムキーを入力します。
- h) 必要に応じて、同じ外部接続 (同じ VRF) に対して追加する外部デバイスについて、前のサブステップを繰り返します。
- i) 必要に応じて、追加の外部接続 (異なる VRF) に対してこの手順を繰り返します。

CSR と外部デバイス間のトンネルエンドポイントには 1 対 1 の関係があるため、異なる VRF を使用して追加の外部接続を作成できますが、同じ外部デバイスに追加の接続を作成することはできません。

次のタスク

必要なサイト間接続情報をすべて設定しましたが、まだサイトにプッシュされていません。[インフラ設定の展開](#)の説明に従って、設定を展開する必要があります。