Cisco APIC サイトのインフラの設定

サイト接続性情報の更新

スパインの追加や削除、またはスパイン ノードの ID 変更などのインフラストラクチャへの変更が加えられた場合、Multi-Site ファブリック接続サイトの更新が必要になります。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、**[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、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 （オプション）オンプレミスサイトの場合、廃止されたスパインスイッチノード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スパイン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。

インフラの設定: オンプレミス サイトの設定

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 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（Infra 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、特定のオンプレミス サイトを選択します。

ステップ 5 **[オーバーレイ設定 (Overlay Configuration)]** を指定します。

a) 右側の **<サイト *(Site)*> [設定 (Settings)]** ペインで、**[オーバレイ設定 (Overlay Configuration)]** タブを選択します。

b) 右側の **<サイト *(Site)*> [設定 (Settings)]** ペインで、**[マルチサイト (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 n) **[CloudSec 暗号化 (CloudSec Encryption)]** ノブを有効にして、サイトを暗号化します。

CloudSec 暗号化は、サイト間トラフィックの暗号化機能を提供します。この機能の詳細については、*Cisco Multi-Site Configuration Guide* の「Infrastructure Management」の章を参照してください。

d) **[オーバレイ 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、単一のポッドまたはマルチポッド ファブリックであるかどうかには関わりなく、同じファブリックの一部であるすべてのスパイン スイッチに展開されます。

このアドレスは、元のファブリックのインフラ TEP プールのアドレス空間または `0.x.x.x` の範囲から取得することはできません。

e) （オプション）**[外部ルート ドメイン (External Routed Domain)]** ドロップダウンから、使用するドメインを選択します。

Cisco APIC GUI で作成した外部ルータ ドメインを選択します。使用している APIC リリースに固有の詳細については、『*Cisco APIC Layer 3 Networking Configuration Guide*』を参照してください。

f) **[BGP 自律システム番号 (BGP Autonomous System Number)]** を指定します。

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

h) （オプション）サイトの **[SR-MPLS 接続 (SR-MPLS Connectivity)]**を有効にします。

サイトが MPLS ネットワークを介して接続されている場合には、**[SR-MPLS 接続性 (SR-MPLS Connectivity)]** ノブを有効にして、セグメント ルーティング グローバル ブロック (SRGB) の範囲を指定します。

セグメント ルーティング グローバル ブロック（SRGB）は、ラベル スイッチング データベース (LSD) でセグメント ルーティング (SR) 用に予約されているラベル値の範囲です。これらの値は SR 対応ノードへのセグメント識別子（SID）として割り当てられ、ドメイン全体でグローバルな意味を持ちます。

デフォルトの範囲は `16000 ～ 23999` です。

サイトのMPLS接続を有効にする場合は、『*Cisco Multi-Site Configuration Guide for ACI Fabrics*』の「Sites Connected via SR-MPLS」の章で説明されている追加設定を行う必要があります。

ステップ 6 **[アンダーレイ設定 (Underlay Configuration)]** を指定します。

a) 右側の **<サイト *(Site)*> [設定 (Settings)]** ペインで、**[アンダーレイ設定 (Underlay Configuration)]** タブを選択します。

b) ドロップダウン メニューから **[OSPF エリア タイプ (OSPF Area Type)]**を選択します。

OSPF エリアタイプは、次のいずれかになります。

- `nssa`
- `regular`

c) サイトの OSPF 設定を行います。

既存のポリシー (たとえば `msc-ospf-policy-default`) をクリックして修正することも、**[+ ポリシー追加 (+Add Policy)]** をクリックして新しいOSPFポリシーを追加することもできます。それから、**[ポリシーの追加/更新(Add/Update Policy)]** ウィンドウで、以下を指定します。

- **[ポリシー名（Policy Name）]** フィールドにポリシー名を入力します。
- **[(ネットワーク タイプ (Network Type)]** フィールドで、`[ブロードキャスト (broadcast)]`、`[ポイントツーポイント (point-to-point)]`、または `[未指定 (unspecified)]` のいずれかを選択します。

  デフォルトは `[ブロードキャスト (broadcast)]` です。
- **[優先順位 (Priority)]** フィールドに、優先順位番号を入力します。

  デフォルトは `1` です。
- **[インターフェイスのコスト (Cost of Interface)]** フィールドに、インターフェイスのコストを入力します。

  デフォルト値は `0` です。
- **[インターフェイス コントロール(Interface Controls)]** ドロップダウン メニューで、以下のいずれかを選択します。
  - **アドバタイズサブネット (advertise-subnet)**
  - **BFD (bfd)**
  - **MTU 無視 (mtu-ignore)**
  - **受動的参加 (passive-participation)**
- **[Hello 間隔 (秒) (Hello Interval (Seconds))]** フィールドに、hello 間隔を秒単位で入力します。

デフォルト値は 10 です。

- **[Dead 間隔 (秒) (Dead Interval (Seconds))]** フィールドに、dead 間隔を秒単位で入力します。

  デフォルト値は 40 です。

- **[再送信間隔 (秒) (Retransmit Interval (Seconds))]** フィールドに、再送信間隔を秒単位で入力します。

  デフォルト値は 5 です。

- **[転送遅延 (秒) (Transmit Delay (Seconds))]** フィールドに、遅延を秒単位で入力します。

  デフォルトは 1 です。

ステップ 7 オンプレミスとクラウド サイト間のサイト間接続を設定します。

オンプレミス サイトとクラウドサイトの間にサイト間接続を作成する必要がない場合（たとえば、導入にクラウドのみまたはオンプレミス サイトのみが含まれる場合）は、この手順をスキップします。

オンプレミスとクラウド サイト間のアンダーレイ接続を設定する場合は、クラウド APIC の CSR がトンネルを確立する IPN デバイスの IP アドレスを指定し、クラウド サイトのインフラ設定を行う必要があります。

a) **[+ IPN デバイスの追加 (+ Add IPN Device)]** をクリックして、IPNデバイスを指定します。

b) ドロップダウンから、前に定義した IPN デバイスのいずれかを選択します。

IPNデバイスは、**[一般設定 (General Settings)]** > **[IPN デバイス (IPN Devices)]**リストですでに定義されている必要があります。 インフラの設定: 一般設定を参照してください。

c) クラウド サイトのサイト間接続を設定します。

クラウドサイトからこのオンプレミス サイトへの以前に設定された接続はすべてここに表示されますが、追加の設定は、Cisco Cloud APIC サイトのインフラの設定の説明に従ってクラウド サイト側から行う必要があります。

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。

インフラの設定: ポッドの設定

このセクションでは、各サイトでポッド固有の設定を行う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**で **[サイト]** をクリックします。

ステップ 3 **[サイト]** ビューで、**[インフラの構築]** 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、ポッドを選択します。

ステップ 6 右の **[ポッドのプロパティ (Pod Properties)]** ペインで、ポッドについてオーバーレイ ユニキャスト TEP を追加できます。

このIPアドレスは、同じポッドの一部であり、サイト間の既知のユニキャスト トラフィックに使用されるすべてのスパイン スイッチに導入されます。

ステップ 7 **[+ TEP プールの追加 (+Add TEP Pool)]** をクリックして、ルーティング可能な TEP プールを追加します。

外部ルーティング可能な TEP プールは、ISC 経由でルーティング可能な IP アドレスのセットを APIC ノード、スパイン スイッチ、および境界リーフ ノードに割り当てるために使用されます。これは、サイト間 L3Out 機能を有効にするために必要です。

以前にAPICでファブリックに割り当てられた外部TEPプールは、ファブリックがMulti-Siteドメインに追加されると、NDO によって自動的に継承され、GUI に表示されます。

ステップ 8 サイトの各ポッドに対してこの手順を繰り返します。

インフラの設定: スパイン スイッチ

このセクションでは、CiscoMulti-Siteのために各サイトのスパイン スイッチを設定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**で **[サイト]** をクリックします。

ステップ 3 **[サイト]** ビューで、**[インフラの構築]** 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、ポッド内のスパイン スイッチを選択します。

ステップ 6 右側の **[<スパイン> 設定 (Settings)]** ペインで、**[+ ポート追加(Add Port)]** をクリックします。

ステップ 7 **[ポートの追加（Add Port）]**ウィンドウで、次の情報を入力します。

- **[イーサネット ポート ID (Ethernet Port ID)]** フィールドに、ポート ID、たとえば `1/29` を入力します。
- **[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。

  NDC によって、指定されたポートで指定された IP アドレスを持つ VLAN 4 でサブインターフェイスが作成されます。
- [MTU] フィールドに、サーバの MTU を入力します。MTUを9150Bに設定する継承を指定するか、`576` ー `9000` の値を選択します。

  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。

- **[OSPF ポリシー (OSPF Policy)]** フィールドで、インフラの設定: オンプレミス サイトの設定 （2 ページ） で設定したスイッチの OSPF ポリシーを選択します。

  OSPF ポリシーの OSPF 設定は、IPN 側と一致させる必要があります。

- **[OSPF 認証 (OSPF Authentication)]** では、[なし (none)] または以下のいずれかを選択します。
  - MD5
  - Simple

ステップ 8 **[BGP ピアリング (BGP Peering)]** ノブを有効にします。

2つより多くのスパイン スイッチのある単一のポッドファブリックでは、BGP ピアリングは**BGP スピーカ (BGP Speakers)** と呼ばれるスパイン スイッチのペア (冗長性のためのもの) 上でのみ有効にします。他のすべてのスパイン スイッチでは、BGP ピアリングを無効にします。これらは**BGP フォワーダ (BGP Forwarders)** としてのみ機能します。

マルチポッド ファブリック BGP ピアリングは、それぞれが異なるポッドに展開された、2 台の BPG スピーカ スパイン スイッチ上でのみ有効にします。他のすべてのスパイン スイッチでは、BGP ピアリングを無効にします。これらは BGP フォワーダ (BGP Forwarders) としてのみ機能します。

ステップ 9 **[BGP-EVPN Router-ID (BGP-EVPN ルータ ID)]** フィールドでは、サイト間の BGP-eVPN セッションで使用する IP アドレスを指定します。

ステップ 10 すべてのスパイン スイッチで手順を繰り返します。