



Cisco ACI サイトの設定

- [ポッドプロファイルとポリシーグループ \(1 ページ\)](#)
- [すべての APIC サイトのファブリック アクセス ポリシーの設定 \(2 ページ\)](#)
- [リモートリーフスイッチを含むサイトの設定 \(6 ページ\)](#)
- [Cisco Mini ACI ファブリック \(8 ページ\)](#)

ポッドプロファイルとポリシーグループ

各サイトの APIC には、ポッドポリシーグループを持つポッドプロファイルが1つ必要です。サイトにポッドポリシーグループがない場合は、作成する必要があります。通常、これらの設定は、ファブリックを最初に展開したときに設定したとおりです。

手順

ステップ 1 サイトの APIC GUI にログインします。

ステップ 2 ポッドプロファイルにポッドポリシーグループが含まれているかどうかを確認します。

[**ファブリック (Fabric)**] > [**ファブリックポリシー (Fabric Policies)**] > [**ポッド (Pods)**] > [**プロファイル (Profiles)**] > [**ポッドプロファイルのデフォルト (Pod Profile default)**] に移動します。

ステップ 3 ポッドポリシーグループを必要に応じて、作成します。

- [**ファブリック (Fabric)**] > [**ファブリックポリシー (Fabric Policies)**] > [**ポッド (Pods)**] > [**ポリシーグループ (Policy Groups)**] の順に移動します。
- [**ポリシーグループ (Policy Groups)**] を右クリックし、[**ポッドポリシーグループの作成 (Create Pod Policy Group)**] を選択します。
- 適切な情報を入力して、[**送信 (Submit)**] をクリックします。

ステップ 4 新しいポッドポリシーグループをデフォルトのポッドプロファイルに割り当てます。

- [**ファブリック (Fabric)**] > [**ファブリックポリシー (Fabric Policies)**] > [**ポッド (Pods)**] > [**プロファイル (Profiles)**] > [**ポッドプロファイルのデフォルト (Pod Profile default)**] の順に移動します。
- デフォルトプロファイルを選択します。

- c) 新しいポッドポリシー グループを選択し、[アップデート (Update)] をクリックします。

すべての APIC サイトのファブリック アクセス ポリシーの設定

APIC ファブリックを追加するか、Nexus Dashboard Orchestrator により管理されるの前に、各サイトで設定される必要がある多くのファブリック指定のアクセス ポリシーがあります。

ファブリック アクセス グローバル ポリシーの設定

このセクションでは、Nexus Dashboard Orchestrator に追加および管理する前に、APIC サイトごとに作成する必要があるグローバル ファブリック アクセス ポリシーの設定について説明します。

手順

ステップ 1 サイトの APIC GUI に直接ログインします。

ステップ 2 メインナビゲーションメニューから、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] を選択します。

サイトを Nexus Dashboard Orchestrator に追加するには、いくつかのファブリック ポリシーを設定する必要があります。APIC の観点からは、ベアメタルホストを接続していた場合と同様に、ドメイン、AEP、ポリシー グループ、およびインターフェイス セレクタを設定することができます。同じマルチサイト ドメインに属するすべてのサイトに対して、スパインスイッチインターフェイスをサイト間ネットワークに接続するための同じオプションを設定する必要があります。

ステップ 3 VLAN プールを指定します。

最初に設定するのは、VLAN プールです。レイヤ 3 サブインターフェイスは VLAN 4 を使用してトラフィックにタグを付け、スパインスイッチをサイト間ネットワークに接続します。

- 左側のナビゲーションツリーで、[プール (Pools)] > [VLAN]] を参照します。
- [VLAN] カテゴリを右クリックし、[VLAN プールの作成 (Create VLAN Pool)] を選択します。

[VLAN プールの作成 (CREATE VLAN Pool)] ウィンドウで、次の項目を指定します。

- [名前 (name)] フィールドで、VLAN プールの名前 (たとえば、msite) を指定します。
- [Allocation Mode (割り当てモード)] の場合は、[スタティック割り当て (Static Allocation)] を指定します。
- [Encap ブロック (Encap Blocks)] の場合は、単一の VLAN 4 だけを指定します。両方の [Range (範囲)] フィールドに同じ番号を入力することによって、単一の VLAN を指定できます。

ステップ 4 接続可能アクセス エンティティ プロファイル (AEP) を作成します。

- a) 左側のナビゲーションツリーで、**[グローバル ポリシー (Global Policies)] > [接続可能なアクセス エントリー プロファイル (Attachable Access Entity Profiles)]** を参照します。
- b) **[接続可能なアクセス エンティティ プロファイル (Attachable Access Entry Profiles)]** を右クリックして、**[接続可能なアクセス エンティティ プロファイルの作成 (Create Attachable Access Entity Profiles)]** を選択します。

[接続可能アクセス エンティティ プロファイルの作成(Create Attachable Access Entity Profiles)] ウィンドウで、AEP の名前 (例: msite-aep) を指定します。

- c) **[次へ(Next)]** をクリックして **[送信(Submit)]** します。
インターフェイスなどの追加の変更は必要ありません。

ステップ 5 ドメインを設定します。

設定するドメインは、このサイトを追加するときに、Nexus Dashboard Orchestrator から選択するものになります。

- a) ナビゲーションツリーで、**[物理的ドメインと外部ドメイン(Physical and External Domains)] > [外部でルーテッドドメイン (External Routed Domains)]** を参照します。
- b) **[外部ルーテッドドメイン(External Routed Domains)]** カテゴリを右クリックし、**[レイヤ 3 ドメインの作成 (Create Layer 3 Domain)]** を選択します。

[レイヤ 3 ドメインの作成 (Create Layer 3 Domain)] ウィンドウで、次の項目を指定します。

- **[名前 (name)]** フィールドで、ドメインの名前を指定します。たとえば、msite-13です。
 - 関連付けられている接続可能エンティティ プロファイルの場合は、ステップ 4 で作成した AEP を選択します。
 - **VLAN プール** の場合は、ステップ 3 で作成した VLAN プールを選択します。
- c) **[送信 (Submit)]** をクリックします。
セキュリティ ドメインなどの追加の変更は必要ありません。

次のタスク

グローバルアクセスポリシーを設定した後も、[ファブリックアクセスインターフェイスポリシーの設定 \(3 ページ\)](#) の説明に従って、インターフェイスポリシーを追加する必要があります。

ファブリック アクセス インターフェイス ポリシーの設定

このセクションでは、各 APIC サイトの Nexus Dashboard Orchestrator で行わなければならないファブリック アクセス インターフェイスの設定について説明します。

始める前に

サイトの APIC では、[ファブリック アクセス グローバル ポリシーの設定 \(2 ページ\)](#) の説明に従って、VLAN プール、AEP、およびドメインなどのグローバルファブリック アクセス ポリシーを設定しておく必要があります。

手順

ステップ 1 サイトの APIC GUI に直接ログインします。

ステップ 2 メインナビゲーションメニューから、**[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)]** を選択します。

前のセクションで設定した VLAN、AEP、およびドメインに加えて、サイト間ネットワーク (ISN) に接続するファブリックのスパイン スイッチ インターフェイスに対してインターフェイス ポリシーを作成します。

ステップ 3 スパイン ポリシー グループを設定します。

a) 左ナビゲーション ツリーで、**[インターフェイス ポリシー (Interface Policie)] > [ポリシー グループ (Policy Groups)] > [スパイン ポリシー グループ (Spine Policy Groups)]** を参照します。

これは、ベアメタルサーバを追加する方法と類似していますが、リーフ ポリシーグループの代わりにスパイン ポリシー グループを作成する点異なります。

b) **[スパイン ポリシー グループ (Spine Policy Groups)]** カテゴリを右クリックして、**[スパイン アクセス ポート ポリシー グループの作成 (Create Spine Access Port Policy Group)]** を選択します。

[スパイン アクセス ポリシー グループの作成 (Create Spine Access Port Policy Group)] ウィンドウで、以下のとおり指定します。

- **[名前 (Name)]** フィールドの場合、ポリシー グループの名前を指定します。たとえば Spine1-PolGrp です。
- **[リンク レベル ポリシー (Link Level Policy)]** フィールドには、スパイン スイッチと ISN の間のリンク ポリシーを指定します。
- **[CDP ポリシー (CDP Policy)]** の場合、CDP を有効にするかどうかを選択します。
- **[添付したエンティティ プロファイル (Attached Entity Profil)]** の場合、前のセクションで設定した AEP を選択します。たとえば msite-aep です。

c) **[送信 (Submit)]** をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

ステップ 4 スパイン プロファイルを設定します。

a) 左ナビゲーション ツリーで、**[インターフェイス ポリシー (Interface Policies)] > [ポリシー グループ (Profiles)] > [スパイン ポリシー グループ (Spine Profiles)]** を参照します。

b) **[プロファイル (Profiles)]** カテゴリを右クリックし、**[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile)]** を選択します。

[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile)] ウィンドウで、次のとおり指定します。

- [名前 (name)] フィールドに、プロファイルの名前 (Spine1など) を指定します。
- [インターフェイス セレクタ (Interface Selectors)] では、+ 記号をクリックして、ISN に接続されるスパイン スイッチ上のポートを追加します。次に、[スパイン アクセス ポート セレクターの作成 (Create Spine Access Port Selector)] ウィンドウで、次のように指定します。
 - [名前 (name)] フィールドに、ポートセレクタの名前を指定します (例: Spine1)。
 - [インターフェイス ID (Interface IDs)] に、ISN に接続するスイッチ ポートを指定します (例 5/32)。
 - [インターフェイス ポリシー グループ (Interface Policy Group)] に、前の手順で作成したポリシー グループを選択します (例: Spine1-PolGrp)。

それから、[OK] をクリックして、ポートセレクタを保存します。

- c) [送信 (Submit)] をクリックしてスパイン インターフェイス プロファイルを保存します。

ステップ 5 スパイン スイッチ セレクター ポリシーを設定します。

- a) 左ナビゲーション ツリーで、[スイッチ ポリシー (Switch Policies)] > [プロファイル (Profiles)] > [スパイン プロファイル (Spine Profiles)] を参照します。
- b) [スパイン プロファイル (Spine Profiles)] [カテゴリを右クリックし、[スパイン プロファイルの作成 (Create Spine Profile)] を選択します。

[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile)] ウィンドウで、次のように指定します。

- [名前 (name)] フィールドに、プロファイルの名前を指定します (例: Spine1)。
 - [スパインセレクタ (Spine Selector)] で、+ をクリックしてスパインを追加し、次の情報を入力します。
 - [名前 (name)] フィールドで、セレクタの名前を指定します (例: Spine1)。
 - [ブロック (Blocks)] フィールドで、スパイン ノードを指定します (例: 201)。
- c) [更新 (Update)] をクリックして、セレクタを保存します。
- d) [次へ (Next)] をクリックして、次の画面に進みます。
- e) 前の手順で作成したインターフェイス プロファイルを選択します。
たとえば、Spine1-ISNなどです。
- f) [完了 (Finish)] をクリックしてスパイン プロファイルを保存します。

リモート リーフ スイッチを含むサイトの設定

リリース 2.1(2) 以降、マルチサイト アーキテクチャはリモート リーフ スイッチをもつ APIC サイトをサポートします。次のセクションでは、Nexus Dashboard Orchestrator がこれらのサイトを管理できるようにするために必要なガイドライン、制限事項、および設定手順を説明します。

リモート リーフのガイドラインと制限事項

Nexus Dashboard Orchestrator により管理されるリモート リーフをもつ APIC サイトを追加する場合、次の制約が適用されます。

- Cisco APIC をリリース 4.2(4) 以降にアップグレードする必要があります。
- このリリースでは、物理リモート リーフ スイッチのみがサポートされます
- -EX および-FX 以降のスイッチのみが、マルチサイトで使用するリモート リーフ スイッチとしてサポートされています。
- リモートリーフは、IPN スイッチを使用しないバックツーバック接続サイトではサポートされていません
- 1つのサイトのリモート リーフ スイッチで別のサイトの L3Out を使用することはできません
- あるサイトと別のサイトのリモート リーフ間のブリッジ ドメインの拡張はサポートされていません。

また、Nexus Dashboard Orchestrator でサイトを追加して管理するには、その前に次のタスクを実行する必要があります。

- 次の項で説明するように、リモートリーフの直接通信をイネーブルにし、APIC サイト内でルーティング可能なサブネットを直接設定する必要があります。
- リモート リーフ スイッチに接続しているレイヤ 3 ルータのインターフェイスに適用されている DHCP リレー設定で、Cisco APIC ノードのルーティング可能な IP アドレスを追加する必要があります。

各 APIC ノードのルーティング可能な IP アドレスは、[ルーティング可能 IP (Routable IP)] フィールド (APIC GUI の [システム (System)][コントローラ (Controllers)][<コントローラ名 >] 画面) に表示されます。 > >

リモート リーフ スイッチのルーティング可能なサブネットの設定

1つ以上のリモート リーフ スイッチを含むサイトを Nexus Dashboard Orchestrator に追加するには、その前に、リモート リーフ ノードが関連付けられているポッドのルーティング可能なサブネットを設定する必要があります。

手順

- ステップ 1 サイトの APIC GUI に直接ログインします。
- ステップ 2 メニューバーから、[ファブリック (Fabric)] > [インベントリ (Inventory)] を選択します。
- ステップ 3 [ナビゲーション (Navigation)] ウィンドウで、[ポッドファブリックセットアップポリシー (Pod Fabric Setup Policy)] をクリックします。
- ステップ 4 メインペインで、サブネットを設定するポッドをダブルクリックします。
- ステップ 5 ルーティング可能なサブネットエリアで、+ 記号をクリックしてサブネットを追加します。
- ステップ 6 IP アドレスと予約アドレスの数を入力し、状態をアクティブまたは非アクティブに設定してから、[更新 (Update)] をクリックしてサブネットを保存します。

ルーティング可能なサブネットを設定する場合は、/22~/29 の範囲のネットマスクを指定する必要があります。

- ステップ 7 [送信 (Submit)] をクリックして設定を保存します。

リモートリーフスイッチの直接通信の有効化

1 つ以上のリモートリーフスイッチを含むサイトを Nexus Dashboard Orchestrator に追加するには、その前に、そのサイトに対して直接リモートリーフ通信を設定する必要があります。リモートリーフ直接通信機能に関する追加情報については、*Cisco APIC レイヤ 3 ネットワーク コンフィギュレーションガイド* を参照してください。ここでは、Multi-Site との統合に固有の手順とガイドラインの概要を説明します。



- (注) リモートリーフスイッチの直接通信を有効にすると、スイッチは新しいモードでのみ機能します。

手順

- ステップ 1 サイトの APIC に直接ログインします。
- ステップ 2 リモートリーフスイッチの直接トラフィック転送を有効にします。
 - a) メニューバーから、[システム (System)] > [システムの設定 (System Settings)] に移動します。
 - b) 左側のサイドバーのメニューから [ファブリック全体の設定 (Fabric Wide Setting)] を選択します。
 - c) [リモートリーフ直接トラフィック転送 (Enable Remote Leaf Direct Traffic Forwarding)] チェックボックスをオンにします。

(注) 有効にした後は、このオプションを無効にすることはできません。

- d) [送信 (Submit)] をクリックして変更を保存します。

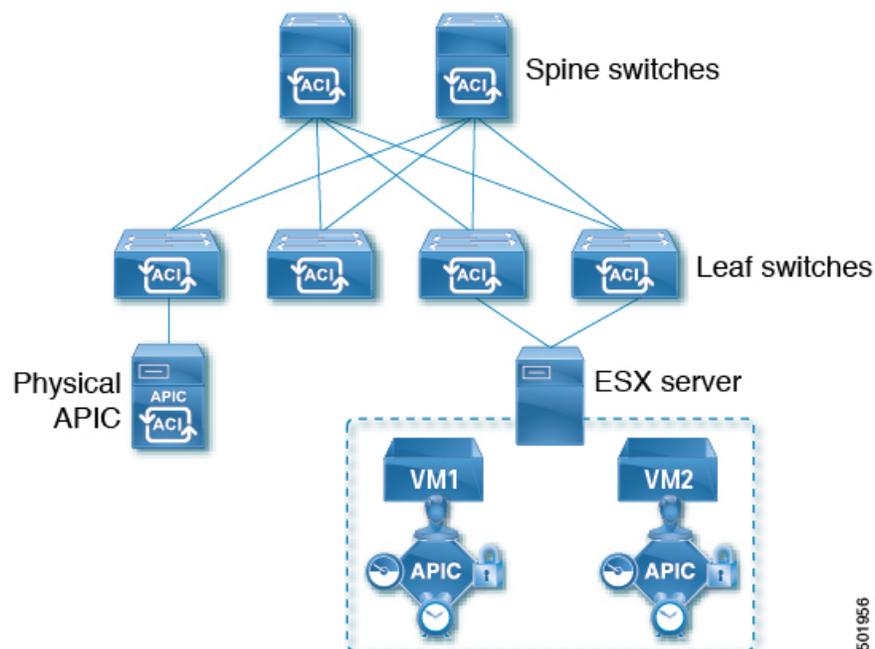
Cisco Mini ACI ファブリック

Cisco Multi-Site は、追加の設定を必要とせずに、一般的なオンプレミス サイトとして Cisco Mini ACI ファブリックをサポートします。ここでは、Mini ACI ファブリックの概要について説明します。このタイプのファブリックの導入と設定に関する詳細情報は、[Cisco Mini ACI ファブリックおよび仮想 APIC](#) で入手できます。

Cisco ACI リリース 4.0(1) では、小規模導入向けに Mini ACI ファブリックが導入されました。Mini ACI ファブリックは、仮想マシンで実行される 1 つの物理 APIC と 2 つの仮想 APIC (vAPIC) で構成されるクラスターで動作します。Cisco APIC により、APIC クラスターの物理的な設置面積とコストが削減され、ACI ファブリックをラックスペースまたは初期予算が限られたシナリオ（コロケーション施設やシングルルームデータセンターなど）に導入できるようになります。フルスケールの ACI インストールは物理的な設置面積や初期コストにより実用的でないことがあります。

次の図に、物理 APIC と 2 つの仮想 APIC (vAPIC) を備えたミニファブリックの例を示します。Cisco ACI

図 1: Cisco Mini ACI ファブリック



501956

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。