# インフラストラクチャ管理



## Cisco ACI マルチサイト and Cisco APIC Interoperability Support

リリース 2.2(1) より前では、すべてのサイトで同じ APIC バージョンを実行する必要があり、その APIC リリースに対応する Orchestrator のバージョンも実行する必要がありました。ファブリックのアップグレード中には、マルチサイト Orchestrator をアップグレードする前に、まずすべての APIC サイトをアップグレードする必要がありました。たとえば、APIC リリース 4.0(1) からリリース 4.1(1) にファブリックをアップグレードしている場合、すべてのサイトが APIC リリース 4.1(1) になるまで、Orchestrator のリリース 2.0 (1) を維持する必要がありました。

リリース 2.2(1) 以降では、マルチサイト Orchestrator リリースは APIC リリースから分離されています。各サイトと Orchestrator 自体の APIC クラスタは、相互に独立してアップグレードし、混合動作モードで実行することができるようになりました。

混合操作モードは、次の APIC リリースのいずれかを実行しているサイトでサポートされています。

- 3.2(6) 以降
- 4.0(1) 以降
- 4.1(1) 以降

• 4.2(1) 以降

ただし、1つまたは複数のサイトで APIC クラスタをアップグレードする前に Orchestrator をアップグレードすると、新しい Orchestrator 機能が以前の APIC リリースでまだサポートされていない可能性があることに注意してください。この場合、各テンプレートでチェックが実行され、すべての設定済みオプションがターゲットサイトでサポートされていることを確認します。このチェックは、テンプレートを保存するか、テンプレートを展開するときに実行されます。テンプレートがすでにサイトに割り当てられている場合、サポートされていない設定オプションは保存されません。テンプレートがまだ割り当てられていない場合は、サイトに割り当てることができますが、サイトがサポートしていない設定が含まれている場合は、スキーマを保存したり展開したりすることはできません。サポートされていない設定が検出されると、エラーメッセージが表示されます。例: この APIC サイトバージョン<サイトのバージョン>は、MSO ではサポートされていません。この<機能>に必要な最小バージョンは<必要なバージョン>以降です。

次の表に、各機能と、それぞれに必要な最小限の APIC リリースを示します。

| 機能 | 最小バージョン |
|---|---|
| ACI マルチポッドのサポート | Release 3.2(1) |
| サービス グラフ (L4 ~ L7 サービス) | リリース 3.2(1) |
| 外部 EPG | リリース 3.2(1) |
| ACI 仮想エッジ VMM のサポート | リリース 3.2(1) |
| DHCP Support | リリース 3.2(1) |
| 整合性チェッカー | リリース 3.2(1) |
| CloudSec 暗号化 | リリース 4.0(1) |
| レイヤ 3 マルチキャスト | リリース 4.0(1) |
| OSPF の MD5 認証 | リリース 4.0(1) |
| EPG 優先グループ | リリース 4.0(2) |
| ホストベースのルーティング | リリース 4.1(1) |
| サイト内 L3Out | リリース 4.2(1) |

# Cisco ACI マルチサイト 通信ポート

Cisco ACI マルチサイト 環境を設定する際は、下記のポートが Cisco ACI マルチサイト Orchestrator によって Cisco ACI マルチサイト 環境内のネットワーク通信に使用されることに注意してください。

Cisco ACI マルチサイト Orchestrator と Cisco APIC（サイト）間のネットワーク通信に必要なポートは次のとおりです。

- TCP ポート 80/443（APIC REST の設定展開用）

Cisco ACI マルチサイト Orchestrator ノード間のネットワーク通信に必要なポートは次のとおりです。

- TCP ポート 2377（クラスタ管理通信用）
- TCP および UDP ポート 7946（Manager 間の通信用）
- UDP ポート 4789（Docker オーバーレイ ネットワーク トラフィック用）

Cisco ACI マルチサイト Orchestrator ノード間のすべてのコントロールプレーンおよびデータプレーン トラフィックは、IP プロトコル番号 50 を使用して IPSec のカプセル化セキュリティペイロード (ESP) によって暗号化され、セキュリティを提供し、最大 150 ミリ秒の往復時間間隔でクラスタの展開を可能にします。いずれかの Orchestrator ノード間にファイアウォールがある場合は、このトラフィックを許可するために適切なルールを追加する必要があります。

# 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 Multi-Site Orchestrator に追加するか、Multi-Site Orchestrator により管理されるには、Multi-Site Orchestrator に追加する前に、各サイトで設定されなければならない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、Multi-Site 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。

**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 Multi-Site 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VLAN4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。

a) 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。
b) **[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 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 Multi-Site Orchestrator から選択するものです。

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-l3`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 （5 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 Multi-Site 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 （3 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。

**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が異なります。

b) **[スパイン ポリシー グループ (Spine Policy Groups)]** カテゴリーを右クリックして、**[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 Profiel)]**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 Selectora)]**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。

---

**次のタスク**

自分のサイトにリモート リーフ スイッチが含まれる場合、リモート リーフ スイッチを含むサイトの設定 （7 ページ） の説明に従って、ファブリック固有の設定をさらに変更する必要があります。

そうではない場合は、サイトの追加 （9 ページ） の説明に従って、Multi-Site Orchestrator へのサイト追加に進みます。

# 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) 以降では、 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使用する APIC サイトをサポートしています。ここでは、マルチサイト 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、および設定手順について説明します。

## マルチサイト リモート リーフのガイドラインと制限事項

マルチサイト 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 4.1(2) 以降にアップグレードする必要があります。
- マルチサイト Orchestrator をリリース 2.1(2) 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、 マルチサイト 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APICにし、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、]<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 マルチサイト 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。

**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 (Routable Subnets)]**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 (Reserve Address Count)]** を入力し、状態を`[アクティブ (Active)]` または `[非アクティブ (Inactive)]`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 マルチサイト 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、マルチサイト 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。

**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 Traffice 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。

# サイトの追加

このセクションでは、Cisco ACI マルチサイト Orchestrator GUI を使用してサイトを追加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、各サイトの APIC でサイト固有の構成を完了している必要があります。

**ステップ 1** マルチサイト GUI にログインし、[Main menu] で、[Sites] をクリックします。

初めてログインしている場合、**admin** ユーザとして、デフォルト パスワード **We1come2msc!** を使用してログインすると、デフォルト パスワードを変更するように指示するプロンプトが表示されます。新しいパスワードの要件は、次のとおりです。

- 最低 12 文字
- 最低 1 つの英字
- 最低 1 つの数字
- * およびスペースとは異なる、少なくとも 1 つの特殊文字

**ステップ 2** メイン ペインの右上にある **[サイトの追加 (Add Site)]** をクリックします。

**ステップ 3** **[サイトの追加(Add Site)]** 画面で、サイトの詳細を指定します。

a) **[名前 (Name)]** フィールドに、サイト名を入力します。

b) **[ラベル (Labels)]** フィールドで、ラベルを選択するか作成します。

サイトに対して複数のラベルを指定することができます。

c) **[APIC Controller URL]** フィールドに、Cisco APIC の URL を入力します。

APIC URL に対して、`http` または `https` プロトコルと IP アドレスまたは DNS ホスト名を使用できます。たとえば、`https://<ip-address>` または `https://<dns-hostname>` です。

d) ファブリックの APIC のクラスタがある場合は、**[+APIC Controller URL]** をクリックして、追加の URL を指定します。

e) **[ユーザ名]** フィールドに、サイトの APIC の管理者ユーザのユーザ名を入力します。

f) **[パスワード]**フィールドに、ユーザのパスワードを入力します。

g) サイトのドメイン名を指定する場合には、**[サイトのログイン ドメインの指定 (Specify Login Domain for Site)]** スイッチをオンにします。

このオプションをオンにした場合、**[ドメイン名]** フィールドにドメイン名を入力します。

h) **[APIC サイト ID]** フィールドに、固有なサイト ID を入力します。

サイト ID は Cisco APIC サイトの固有識別子で、1 ～ 127 の範囲になければなりません。サイト ID が指定されると、サイト ID は Cisco APIC を工場出荷時にリセットせずに、変更できません。

**ステップ 4** [**保存 (Save)**] をクリックして、サイトを追加します。

**ステップ 5** プロンプトが表示されたら、プロキシ設定の更新を確認します。

プロキシ サーバを使用するように Orchestrator を構成し、「プロキシなし」リストにまだ含まれていないオンプレミス サイトを追加する場合、Orchestrator はプロキシ設定の更新を通知します。

プロキシ設定の詳細については、『*Cisco ACI Multi-Site* 設定ガイド』の「管理オプション」の章を参照してください。

**ステップ 6** サイトを追加するには、これらの手順を繰り返します。

# インフラの前提条件とガイドラインの設定

次のセクションでは、全般な設定と、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。これには、以下が含まれます。

- 各サイトのファブリック アクセス ポリシーの設定。
- リモート リーフ スイッチを使用したサイトの直接通信およびルーティング可能なサブネットの設定。

さらに、次の点に注意してください。

- スパイン スイッチまたはスパイン ノード ID の変更の追加や削除などのインフラストラクチャの変更には、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（11 ページ） に記載されている マルチサイト ファブリック接続情報の更新が必要です。
- Orchestrator に割り当てられているオーバーレイ ユニキャスト TEP、オーバーレイ マルチキャスト TEP、および BGP EVPN ルータ ID IP 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。

# 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 ACI マルチサイト Orchestrator GUI にログインします。

**ステップ 2** **[メイン メニュー (Main menu)]**で **[サイト (Site)]** をクリックします。

**ステップ 3** **[サイト (Sites)]** ビューで、**[インフラ設定 (Configure Infra)]** をクリックします。

**ステップ 4** 左側のペインの **[設定 (settings)]** で、**[一般設定 (General Settings)]** をクリックします。

**ステップ 5** **[BGP ピアリング タイプ (BGP Peering Type)]** ドロップダウンから、[フルメッシュ (full-mesh)] または [ルートリフレクタ (route-reflector)] のいずれかを選択します。

[ルートリフレクタ (route-reflector)]オプションは、すべてのサイトが同じ BGP 自律システム (AS) に属している場合にのみ有効です。

**ステップ 6** **[キープアライブ間隔 (秒) (Keepalive Interval (Seconds))]** フィールドに、キープアライブ間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

**ステップ 7** **[保留間隔 (秒) (Hold Interval (Seconds))]** フィールドに、保留間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

**ステップ 8** **[失効間隔 (秒) (Stale Interval (Seconds))]** フィールドに、失効間隔を秒単位で入力します。

デフォルト値を維持することを推奨します。

**ステップ 9** **[グレースフル ヘルパー (Graceful Helper)]** オプションをオンにするかどうかを選択します。

**ステップ 10** **[最大AS 制限値 (Maximum AS Limit)]** フィールドで、最大 AS 制限値を入力します。

**ステップ 11** **[ピア間 BGP TTL (BGP TTL Between Peer)]** フィールドで、ピア間の BGP TTL を入力します。

# 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、マルチサイト 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 ACI マルチサイト Orchestrator GUI にログインします。

**ステップ 2** **[メイン メニュー (Main menu)]**で **[サイト (Site)]** をクリックします。

**ステップ 3** **[サイト (Sites)]** ビューで、**[インフラ設定 (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簿宅をクリックします。

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: サイトの設定

ここでは、サイトごと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 ACI マルチサイト Orchestrator GUI にログインします。

**ステップ 2** **[メイン メニュー (Main menu)]**で **[サイト (Site)]** をクリックします。

**ステップ 3** **[サイト (Sites)]** ビューで、**[インフラ設定 (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、特定のサイトを選択します。

**ステップ 5** 右側の **[ <サイト> 設定 (Settings)]** ペインで、**[ACI マルチサイト (ACI Multi-Site)]** ノブを有効にして Orchestrator でサイトを管理できるようにします。

**ステップ 6** (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 ACI Multi-Site Configuration Guide*の Infrastructure Management の章を参照してください。

**ステップ 7** **[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。

**ステップ 8** **[BGP 自律システム番号 (BGP Autonomous System Number)]** を指定します。

**ステップ 9** **[BGP パスワード (BGP Password)]** を指定します。

**ステップ 10** **[OSPF Area ID (OSPF エリア ID)]** を指定します。

マルチサイト インフラ OSPF の詳細を設定する際には、OSPF エリア `0` を使用することを推奨します。`0` 以外のエリア ID を使用する場合、次の手順ではそれを`regular` OSPF エリア タイプとして設定することになります。 `stub` エリア タイプにはなりません。

**ステップ 11** 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`
- `stub`

**ステップ 12** ドロップダウン メニューから外部ルート ドメインを選択します。

APIC GUI で作成した外部ルータ ドメインを選択します。

**ステップ 13** 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。

# 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 ACI マルチサイト Orchestrator GUI にログインします。

**ステップ 2** **[メイン メニュー (Main menu)]**で **[サイト (Site)]** をクリックします。

**ステップ 3** **[サイト (Sites)]** ビューで、**[インフラ設定 (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]** 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]** 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。

ルーティング可能な TEP プールは、サイト間接続のパブリック IP アドレスに使用されます。

**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、Cisco ACI マルチサイト 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 ACI マルチサイト Orchestrator GUI にログインします。

**ステップ 2** **[メイン メニュー (Main menu)]**で **[サイト (Site)]** をクリックします。

**ステップ 3** **[サイト (Sites)]** ビューで、**[インフラ設定 (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。

Orchestrator によって、指定された IP アドレスを持ち、指定されたポートを使用する、VLAN 4 の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。`[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。

  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: サイトの設定 （12 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 ルータ ID (BGP-EVPN Router-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。

# インフラ設定の展開

ここでは、各 APIC 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。

**ステップ 1** Cisco ACI マルチサイト Orchestrator GUI にログインします。

**ステップ 2** **[メイン メニュー (Main menu)]**で **[サイト (Site)]** をクリックします。

**ステップ 3** **[サイト (Sites)]** ビューで、**[インフラ設定 (Configure Infra)]** をクリックします。

**ステップ 4** メインペインの右上にある **[展開 (deploy)]** をクリックして、設定を展開します。

インフラストラクチャ設定を各サイトに展開する前に、この章の前の項で説明したように、必要なすべての一般的な設定とサイトローカルの設定が完了していることを確認します。

# マルチサイト Orchestrator GUI を使用したサイトの削除

このセクションでは、マルチサイト GUI を使用してサイトを削除する方法を説明します。

**ステップ 1** マルチサイト GUI にログインします。
**ステップ 2** サイトの削除を試みる前に、どのスキーマからもサイトがアンバインドされていることを確認します。
**ステップ 3** **Main menu** で **Sites** をクリックします。
**ステップ 4** **Sites List** ページで、さくをするサイトにマウスを合わせて **Action** > **Delete** を選択します。
**ステップ 5** **YES** をクリックします。

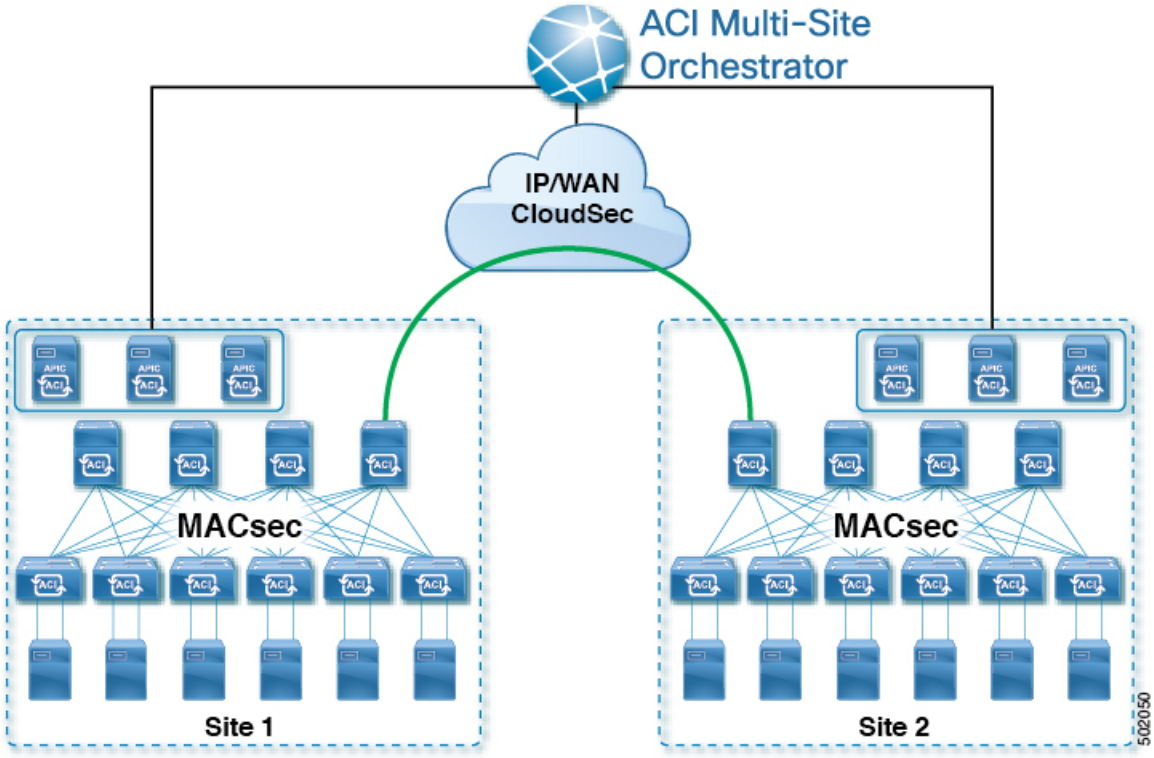
# Cisco ACI CloudSec 暗号化

ほとんどの Cisco ACI 展開で、ディザスタ リカバリとスケーリングに対処する Cisco ACI マルチサイト アーキテクチャを採用しているため、ローカル サイト内で MACsec 暗号化を使用する現在のセキュリティ実装は、個別のファブリックを相互接続する安全でない外部 IP ネットワークによって接続された複数のサイトにわたるデータセキュリティと整合性を保証するには不十分になっています。Cisco ACI マルチサイト Orchestrator リリース 2.0(1) は、トラフィックのサイト間暗号化を提供するために設計された CloudSec 暗号化を導入しています。

Cisco ACI マルチサイト トポロジはサイト間の接続を提供するために、3 個のトンネル エンドポイント (TEP) IP アドレスを使用します。これらの TEP アドレスは、Cisco ACI マルチサイト Orchestrator の管理者により設定され、各サイトの Cisco APIC にプッシュ ダウンされます。次いで、それらはスパイン スイッチで設定されます。これらの 3 つのアドレスは、トラフィックがリモート サイトに送信されるタイミングを決定するために使用されます。この場合、2 つのスパイン スイッチ間に暗号化された CloudSec トンネルが作成され、サイト間ネットワーク (ISN) を介して 2 つのサイト間の物理接続が提供されます。

次の図は、サイト間トラフィックの暗号化のために、ローカル サイト トラフィックの MACsec と CloudSec を組み合わせる全体的な暗号化アプローチを示しています。

図 *1 : CloudSec* 暗号化




# CloudSec の要件とガイドライン

CloudSec 暗号化機能は、リモート リーフ ダイレクト、仮想ポッド (vPOD)、SDA、サイト間 L3Out、またはその他のルート可能な TEP 設定ではサポートされていません。

### ハードウェア要件

次の表に、CloudSec 暗号化に対応したハードウェア プラットフォームとポート範囲を示します。

| ハードウェア プラットフォーム | ポート範囲 |
|---|---|
| N9K C9364C スパインスイッチ | ポート 49-64 |
| N9K-C9332C スパインスイッチ | ポート 25-32 |
| N9K-X9736C-FX ラインカード | ポート 29-36 |

CloudSec がサイトに対して有効になっているが、暗号化がポートでサポートされていない場合、サポートされていないインターフェイスのエラーメッセージで障害が発生します。

CloudSec 暗号化のパケット カプセル化は、DWDM-C SFP10G などの Cisco QSFP から SFP へのアダプタ (QSA) がサポートされている光ファイバで使用されている場合にサポートされます。

サポートされている光ファイバの完全なリストは、https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html のリンクから入手できます。

### ソフトウェアとライセンスの要件

Cisco ACI CloudSec 暗号化には、次のものが必要です。

- Cisco ACI 各サイトの APIC クラスタを使用したスパイン リーフ アーキテクチャ
- Cisco ACI 各サイトを管理するためのマルチサイト Orchestrator
- ファブリック内のリーフごとの Cisco Digital Network Architecture (DNA) アドバンテージ ライセンス
- 暗号化のためのスパイン スイッチごとのアドオン ライセンス ACI-SEC-GX:
  - 固定スパイン スイッチの場合: ACI-SEC-XF
  - モジュール型スパイン スイッチの場合: ACI-SEC-XM

# CloudSec 暗号化に関する用語

CloudSec暗号化機能は、サイト間の初期キーとキー再生成の要件に応じて、安全なアップストリーム対称キーの割り当てと配布方法を提供します。この章では、次の用語を使用します。

- アップストリーム デバイス: CloudSec 暗号化ヘッダを追加し、ローカルで生成された対称暗号化キーを使用してリモート サイトへの送信時に VXLAN パケット ペイロードの暗号化を行うデバイス。
- ダウンストリーム デバイス: Cloudsec 暗号化ヘッダーを解釈し、リモートサイトによって生成された暗号キーを使用して受信時に VXLAN パケット ペイロードの復号化を行うデバイス。
- アップストリーム サイト: 暗号化された VXLAN パケットを発信するデータセンター ファブリック。
- ダウンストリーム サイト: 暗号化されたパケットを受信して復号化するデータセンター ファブリック。
- TX キー: 平文の VXLAN パケット ペイロードを暗号化するために使用される暗号キー。ACI では、すべてのリモート サイトに対して TX キーを 1 つだけアクティブにすることができます。
- RX キー: 暗号化された VXLAN パケット ペイロードを復号化するために使用される暗号キー。ACI では、リモートサイトごとに 2 つの RX キーをアクティブにすることができます。

  キーの再生成プロセス中には、2つのRXキーを同時にアクティブにすることができます。ダウンストリームサイトは、新しいキーの展開が終了した後も、一定時間古いRXキーと

新しい RX キーを保持します。これは、順序どおりでないパケット配信が行われた場合でも、どちらかのキーを使用して適切に復号することができるようにするためです。

- 対称キー：同じ暗号キーを使用して、アップストリーム デバイスとダウンストリーム デバイスによるパケット ストリームの暗号化 (TX キー) と復号 (RX キー) を行います。
- キー再生成: 古いキーの有効期限が切れた後に、アップストリーム サイトが開始する、すべてのダウンストリーム サイトの古いキーを新しいキーに置き換えるプロセスです。
- セキュアチャネル識別子 (SCI): サイト間のセキュリティ アソシエーションを表す、64 ビットの識別子です。CloudSec ヘッダの暗号化パケットで送信され、パケット復号化のためにダウンストリーム デバイスで RX キーを導出するために使用されます。
- アソシエーション番号 (AN): 暗号化されたパケットの CloudSec ヘッダーで送信される 2 ビットの数値 (0、1、2、3) です。復号化のため、ダウンストリーム デバイスでキーを取得するために使用されます。これにより、ダウンストリームデバイスで複数のキーをアクティブにできます。キー再生成操作後に、同じアップストリームデバイスからパケットが順番通りではなく到着した場合でも、処理できるようにするためです。

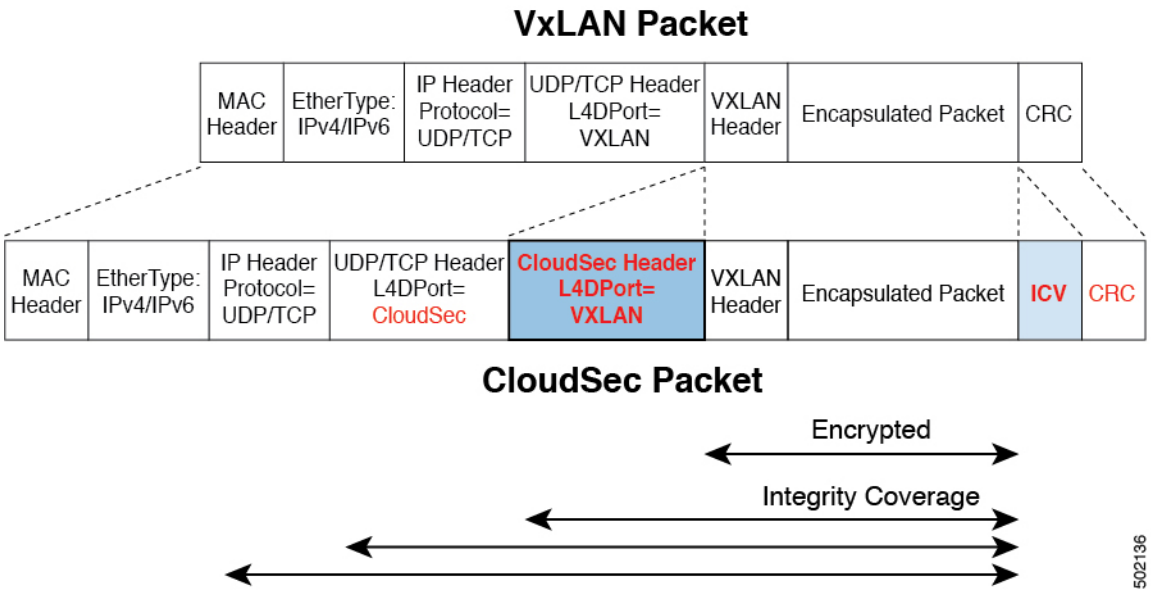
  ACI において、2 つのアクティブな RX キーには、2 つのアソシエーション番号値 (0 と 1) だけが使用されます。任意の時点で、TX キーには、1 つのアソシエーション番号値 (0 または 1) だけが使用されます。
- 事前共有キー (PSK): CloudSec TX および RX キーを生成するためのランダムシードとして使用されるように、Cisco APIC GUI で1つ以上のキーを設定する必要があります。複数の PSK が設定される場合、各キーの再生成プロセスはインデックス順で次の PSK を使用します。さらに高いインデックスの PSK がない場合、最下位のインデックスの PSK が使用されます。各 PSK は、64 文字の 16 進数文字列である必要があります。Cisco APIC は最大 256 の事前共有キーをサポートします。

# CloudSec の暗号化と復号の処理

リリース 2.0(1)以降では、データ セキュリティと整合性の両方に対応する、完全に統合されたシンプルでコスト効率の高いソリューションを提供するために、Cisco ACI マルチサイト はマルチサイト ファブリック間の完全な送信元から宛先へのパケット暗号化を可能にする CloudSec 暗号化機能を提供します。

次の図は、CloudSec カプセル化の前後のパケット ダイアグラムと、その後の暗号化および復号化プロセスの説明を示しています。

図 *2 : CloudSec* パケット




### パケット暗号化

次に、CloudSec が発信トラフィック パケットを処理する方法の概要を示します。

- パケットは、外部 IP ヘッダーとレイヤ 4 宛先ポート情報を使用してフィルタ処理され、一致するパケットは暗号化の対象としてマークされます。
- 暗号化に使用するオフセットは、パケットのフィールドに基づいて計算されます。たとえば、オフセットは、802.1q VLAN があるかどうか、またはパケットが IPv4 または IPv6 パケットであるかどうかによって異なります。
- 暗号キーはハードウェアテーブルでプログラムされ、パケット IP ヘッダーを使用してテーブルから検索されます。

パケットに暗号化のマークが付けられると、暗号キーがロードされ、暗号化を開始するパケットの先頭からのオフセットが判明すると、次の追加の手順が実行されます。

- UDP 宛先ポート番号は、UDP ヘッダーから CloudSec フィールドにコピーされ、パケットが暗号解読されるときにリカバリされます。
- UDP 宛先ポート番号は、CloudSec パケットであることを示すシスコ独自のレイヤ 4 ポート番号 (ポート `9999`) で上書きされます。
- [UDP 長(UDP length)] フィールドは、追加されるバイト数を反映するように更新されます。
- CloudSec ヘッダーは、UDP ヘッダーの後に直接挿入されます。
- 整合性チェック値 (ICV) は、ペイロードと CRC の間のパケットの最後に挿入されます。

- ICV では、128 ビットの初期化ベクトルを構築する必要があります。CloudSec の場合、ICV のために送信元 MAC アドレスを使用すると、SCI ごとのプログラム可能な値に置き換えられます。
- CRC は、パケットのコンテンツの変更を反映するように更新されます。

### パケットの暗号解読

CloudSec が受信パケットを処理する方法は、上記で説明した発信パケット アルゴリズムと対称的です。

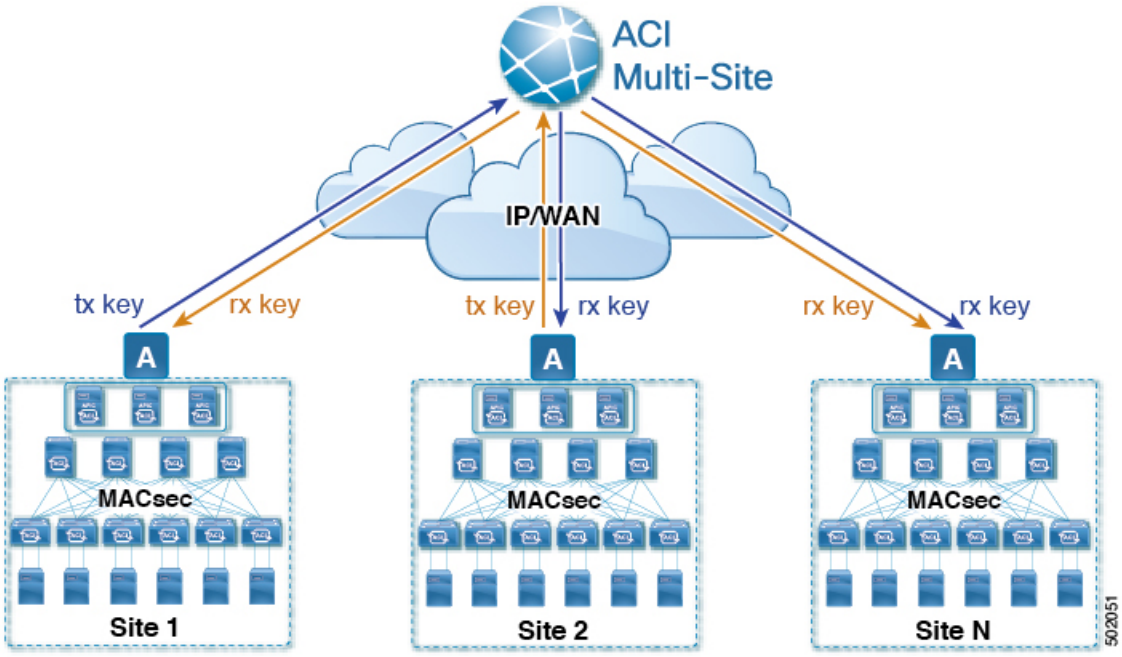
- 受信したパケットが CloudSec パケットである場合は、暗号解読され、ICV が検証されます。

  ICV 検証に合格すると、追加フィールドが削除され、UDP 宛先ポート番号が CloudSec ヘッダーから UDP ヘッダーに移動され、CRC が更新され、パケットの暗号解読と CloudSec ヘッダーの削除後に宛先に転送されます。そうでない場合、パケットはドロップされます。
- キー ストアが2つ以上の可能な暗号解読キーを返す場合、CloudSec ヘッダーの Association Number (AN) フィールドを使用して、使用するキーを選択します。
- パケットが CloudSec パケットでない場合、パケットはそのまま残ります。

# CloudSec 暗号化キーの割り当てと配布

## 初期キー構成

図 *3 : CloudSec* キーの配布




次に、上記の図に示されている CloudSec 暗号キーの初期割り当ておよび配信プロセスの概要を示します。

- アップストリームサイトの Cisco APIC は、サイトから送信された VXLAN パケットのデータ暗号化に使用されるためのローカル対称キーを生成します。アップストリームサイトが暗号化に使用するのと同じキーが、ダウンストリームリモート受信サイトのパケットの復号に使用されます。

  各サイトはほかのサイトに送信するトラフィックのためのアップストリームサイトです。複数のサイトが存在する場合、各サイトは独自のサイトツーサイトキーを生成し、そのキーを暗号化に使用してからリモートサイトに送信します。

- 生成された対称キーは、ダウンストリーム リモート サイトに配布するために、アップストリーム サイトの Cisco APIC によって Cisco ACI マルチサイト Orchestrator (MSO) にプッシュされます。

- MSO はメッセージ ブローカとして機能し、生成された対称キーをアップストリーム サイトの Cisco APIC から収集し、それをダウンストリーム リモート サイトの Cisco APIC に配布します。

- 各ダウンストリーム サイトの Cisco APIC は、受信したキーを、キーを生成したアップストリームサイトからのトラフィックを受信することを目的としたローカルスパインスイッチの RX キーとして設定します。

- 各ダウンストリーム サイトの Cisco APIC は、ローカル スパイン スイッチから RX キーの展開ステータスを収集し、MSO にプッシュします。
- MSOは、すべてのダウンストリーム リモート サイトからアップストリーム サイトの Cisco APIC に戻って、主要な展開ステータスを中継します。
- アップストリームサイトはCisco APIC 、すべてのダウンストリーム リモート サイトから受信したキー展開ステータスが成功したかどうかを確認します。
  - ダウンストリームデバイスから受信した展開ステータスが成功した場合、アップストリーム サイトはスパイン スイッチの TX キーとしてローカル対称キーを展開し、ダウンストリーム サイトに送信される VXLAN パケットの暗号化を有効にします。
  - ダウンストリームデバイスから受け取った展開ステータスが失敗した場合、失敗した Cisco APIC サイトで障害が発生し、MSOで構成された「セキュア モード」設定に基づいて処理されます。「セキュアが必須(must secure)」モードでは、パケットはドロップされ、「セキュアであるべき (should secure)」モードでは、パケットは宛先サイトに平文 (暗号化されていない) で送信されます。

（注） 現在のリリースでは、モードは常に「セキュアであるべき (should secure)」に設定されており、変更できません。

### キー再生成プロセス

生成された各 TX / RX キーは、設定された時間が経過すると有効期限が切れます。デフォルトでは、キーの有効期限は 15 分に設定されています。TX/RX キーの初期セットが期限切れになると、キー再生成プロセスが行われます。

キーの再割り当てプロセスには、同じ一般的なキーの割り当てと配布フローが適用されます。キー再生成プロセスは「ブレーク前に作成 (make before break)」ルールに従います。つまり、新しい TX キーがアップストリーム サイトに展開される前に、ダウンストリーム サイトのすべての RX キーが展開されます。これを実現するために、アップストリーム サイトは、ローカル アップストリーム サイトのデバイスに新しい TX キーを構成する前に、ダウンストリーム サイトからの新しい RX キーの展開ステータスを待ちます。

ダウンストリームサイトが新しいRXキーの展開で障害ステータスを報告した場合、キー再生成プロセスは終了し、古いキーはアクティブなままになります。ダウンストリームサイトは、新しいキーの展開が一定期間終了した後、古い RX キーと新しい RX キーを保持し、いずれかのキーを適切に復号することで、順序どおりでないパケット配信が可能になるようにします。

（注） スパイン スイッチのメンテナンス中のキー再生成プロセスに関しては、特別な注意が必要です。詳細については、スパイン スイッチ メンテナンス中のキー再生成プロセス （28 ページ）を参照してください。

### キー再生成プロセスの失敗

ダウンストリームサイトがキー再生成プロセスによって生成された新しい暗号化キーの展開に失敗した場合、新しいキーは破棄され、アップストリーム デバイスは以前の有効なキーを TX キーとして引き続き使用します。このアプローチにより、アップストリームサイトは、ダウンストリームサイトのセットごとに複数の TX キーを維持する必要がなくなります。ただし、このアプローチでは、いずれかのダウンストリームサイトでキー再生成の展開エラーが発生し続ける場合、キー更新プロセスが遅延する可能性もあります。マルチサイト管理者は、キー再生成を成功させるために、キーの展開の失敗の問題を修正するための行動を取ることが期待されています。

### Cisco APICキー管理のロール

Cisco APIC は、キー割り当て(初期キーとキー再配布の両方)、スパイン スイッチからのキー展開ステータス メッセージの収集、および他のサイトへの配布のための各キーのステータスに関する Cisco ACI マルチサイト Orchestrator への通知に責任をもちます。

### Cisco ACI マルチサイト キー管理における Orchestrator の役割

Cisco ACI マルチサイト Orchestrator は、アップストリーム サイトから TX キー（初期キーと後続のキーの再生成の両方）を収集し、RX キーとして展開するためにすべてのダウンストリーム サイトに配布します。MSO はまた、ダウンストリーム サイトから RX キーの展開ステータス情報を収集し、成功した RX キー展開ステータスで TX キーを更新するために、アップストリーム サイトに通知します。

### アップストリーム モデル

MPLS など、ダウンストリーム キー割り当てを使用する他のテクノロジーとは対照的に、CloudSec のアップストリーム モデルには次の利点があります。

- このモデルはシンプルで、運用とネットワークへの導入が容易です。
- モデルは、Cisco ACI マルチサイト のユース ケースに適しています。
- 複数の宛先サイトに送信される複製パケットの各コピーに同じキーと CloudSec ヘッダーを使用できるため、マルチキャスト トラフィックに利点があります。ダウンストリーム モデルでは、各コピーは暗号化中にサイトごとに異なるセキュリティ キーを使用する必要があります。
- 障害が発生した場合のトラブルシューティングが容易になり、複製されたユニキャスト パケットとマルチキャスト パケットの両方に対して、送信元から宛先へのパケットのトレーサビリティが一貫して向上します。

# CloudSec 暗号化の Cisco APIC の設定

CloudSec 暗号と復号キーを生成するために、Cisco APIC で使用する 1 個以上の事前共有キー (PSK) を設定する必要があります。PSK は再キー プロセス中のランダム シードとして使用されます。複数の PSK が設定される場合、各再キー プロセスはインデックスの順序で次の PSK

を使用します。さらに高いインデックスの PSK がない場合、最下位のインデックスの PSK が使用されます。

PSK は暗号キー生成のシードとして使用されるため、複数の PSK を設定すると、生成された暗号キーの過剰な脆弱性が低減され、セキュリティが強化されます。

（注） Cisco APIC で事前共有キーが設定されていない場合、CloudSec はそのサイトに対して有効にはなりません。その場合、CloudSec 設定を Cisco ACI マルチサイト でオンにすると、エラーが生じます。

新しい PSK で前に追加した PSK を更新したい場合はいつでも、新しいキーを追加するときと同様の手順を繰り返すだけですが、インデックスは既存のものを指定してください。

1 つ以上の事前共有キーを次の 3 通りの方法のいずれかを使用して設定できます。

- GUI を使用した CloudSec 暗号化の Cisco APIC の設定 （25 ページ） の説明に従って、Cisco APIC GUI を使用する
- NX-OS Style CLI を使用した CloudSec 暗号化に対する Cisco APIC の設定 （26 ページ） の説明に従って、Cisco APIC NX-OS Style CLI を使用する
- REST API を使用した CloudSec 暗号化の Cisco APIC の設定 （27 ページ） の説明に従って、Cisco APIC REST API を使用する

## GUI を使用した CloudSec 暗号化の Cisco APIC の設定

このセクションでは、Cisco APIC GUI を使用して 1 つ以上の事前共有キー (PSK) を設定する方法について説明します。

**ステップ 1** APIC にログインします。

**ステップ 2** **[テナント (Tenants)]** > **[インフラ (Infra)]** > **[ポリシー (Policies)]** > **[CloudSec 暗号化 (CloudSec Encription)]**に移動します。

**ステップ 3** **[SA キーの有効期限 (Sa Key Expiry Time)]**を指定します。

このオプションは、各キーが有効な時間 (分) を指定します。それぞれの生成された TX/RX キーは、キー再設定プロセスをトリガした後、指定の時間で期限切れになります。期限は 5 ～ 1440 分の範囲で入力できます。

**ステップ 4** **[事前共有キー (Pre-Shared Keys)]**テーブルの + アイコンをクリックします。

**ステップ 5** 追加する事前共有キーの**[インデックス (Index)]**を指定し、その後、**[事前共有(Pre-Shared Key)]** キー自体を指定します。

**[インデックス (Index)]** フィールドでは、事前共有キーを使用する順序を指定します。最後 (最大のインデックス) のキーが使用された後は、プロセスは最初 (最小のインデックス) のキーで続行されます。Cisco APIC は最大 256 個の事前共有キーをサポートするので、PSK インデックスは 1 ～ 256 でなければなりません。

各**[事前共有キー(Pre-Shared Key)]** は、64 文字の 16 進数文字列である必要があります。

## NX-OS Style CLI を使用した CloudSec 暗号化に対する Cisco APIC の設定

このセクションでは、 Cisco APIC NX OS Style CLI を使用して1つ以上の事前共有キー (PSK) を設定する方法について説明します。

**ステップ 1** Cisco APIC NX OS スタイル CLI にログインします。

**ステップ 2** コンフィギュレーション モードを入力します。

**例**：

```
apic1# configure
apic1 (config)#
```

**ステップ 3** デフォルト CloudSec プロファイルのコンフィグレーション モードを入力します。

**例**：

```
apic1(config)# template cloudsec default
apic1(config-cloudsec)#
```

**ステップ 4** 事前共有キー (PSK) の有効期限を指定します。

このオプションは、各キーが有効な時間 (分) を指定します。それぞれの生成された TX/RX キーは、キー再設定プロセスをトリガした後、指定の時間で期限切れになります。期限は 5 ～ 1440 分の範囲で入力できます。

**例**：

```
apic1(config-cloudsec)# sakexpirytime <duration>
```

**ステップ 5** 1 つまたは複数の事前共有キーを指定します。

次のコマンドでは、設定している PSK のインデックスと PSK 文字列自体を指定します。

**例**：

```
apic1(config-cloudsec)# pskindex <psk-index>
apic1(config-cloudsec)# pskstring <psk-string>
```

<*psk-index*> パラメータは、事前共有キーが使用される順序を指定します。最後 (最上位のインデックス) キーが使用された後で、プロセスは最初 (最下位のインデックス) キーで続けられます。Cisco APIC は最大 256 個の事前共有キーをサポートするので、PSK インデックスチは 1 ～ 256 でなければなりません。

<*psk-string*>パラメータは、実際の PSK を指定します。これは、64 文字の 16 進数文字列である必要があります。

**ステップ 6** (オプション) 現在の PSK 設定を表示します。

現在設定されている PSK の数とその期間を表示するには、次のコマンドを使用します。

**例**：

```
apic1(config-cloudsec)# show cloudsec summary
```

## REST API を使用した CloudSec 暗号化の Cisco APIC の設定

このセクションは、Cisco APIC REST API を使用して 1 つ以上の事前共有キー (PSK) を設定する方法について説明します。

PSK 有効期限、インデックス、文字列を設定します。

次の XML POST で、次を置換します。

- 各 PSK の期限をもつ **sakExpiryTime** の値。

  この **sakExpiryTime** パラメータは各キーが有効な時間 (分) を指定します。それぞれの生成された TX/RX キーは、キー再設定プロセスをトリガした後、指定の時間で期限切れになります。期限は 5 ～ 1440 分の範囲で入力できます。

- 設定している PSK のインデックスをもつ **インデックス** の値。

  **インデックス** パラメータは、事前共有キーが使用される順序を指定します。最後 (最高位のインデックス) キーが使用された後で、プロセスは最初 (最下位のインデックス) キーで続けられます。Cisco APIC は最大 256 個の事前共有キーをサポートするので、PSK インデックスチは 1 ～ 256 でなければなりません。

- 設定している PSK のインデックスをもつ **pskString** の値。

  **pskString** パラメータは実際の PSK を指定します。これは 16 進文字列で長さ 64 文字でなければなりません。

**例**：

```
<fvTenant annotation="" descr="" dn="uni/tn-infra" name="infra" nameAlias="" ownerKey="" ownerTag="">

    <cloudsecIfPol descr="cloudsecifp" name="default" sakExpiryTime="10" stopRekey= "false" status=""
 >
        <cloudsecPreSharedKey index="1"
pskString="1234567812345678123456781234567812345678123456781234567812345678" status=""/>
    </cloudsecIfPol>
</fvTenant>
```

# Cisco ACI マルチサイト Orchestrator GUI を使用した CloudSec 暗号化の有効化

CloudSec 暗号化は、サイトごとに個別に有効または無効にすることができます。ただし、2 つのサイト間の通信は、この機能が両方のサイトで有効になっている場合にのみ暗号化されます。

### 始める前に

2つ以上のサイト間でCloudSec暗号化を有効にする前に、次のタスクを完了しておく必要があります。

- 『*Cisco APIC* のインストール、アップグレード、ダウングレードガイド』で説明されているように、複数のサイトに Cisco APIC クラスタをインストールして設定します。
- 『*Cisco ACI* マルチサイト *Orchestrator* インストレーションおよびアップグレードガイド』の説明に従って、インストールおよび設定された Cisco ACI マルチサイト Orchestrator。
- 『*Cisco ACI* マルチサイトコンフィギュレーションガイド』の説明に従って、各 Cisco APIC サイトを Cisco ACI マルチサイト Orchestrator に追加しました。

**ステップ 1** Cisco ACI マルチサイト Orchestrator にログインします。

**ステップ 2** 左側のサイドバーから、**[サイト (Sites)]** ビューを選択します。

**ステップ 3** メインウィンドウの右上にある **[Infra の構成]** ボタンをクリックします。

**ステップ 4** 左側のサイドバーから、CloudSec 設定を変更するサイトを選択します。

**ステップ 5** 右側のサイドバーで、**[Cloudsec 暗号化 (Cloudsec encryption)]** 設定を切り替えて、サイトの CloudSec 暗号化機能を有効または無効にします。

# スパイン スイッチ メンテナンス中のキー再生成プロセス

次に、この機能が有効になっているスパイン スイッチの一般的なメンテナンス シナリオでの CloudSec キー再生成プロセスの概要を示します。

- **通常のデコミッション**: CloudSec 対応スパイン スイッチがデコミッションされると、CloudSec キー再生成プロセスが自動的に停止します。デコミッションされたノードが再起動されるか、解放されたノード ID が次から削除されるまで、キー再生成プロセスは再度開始されません: Cisco APIC
- **スパイン スイッチのソフトウェア アップグレード**: スパイン スイッチがソフトウェアのアップグレードによりリロードされると、CloudSec キー再生成プロセスは自動的に停止します。キー再生成プロセスは、スパイン スイッチのリロードが完了すると、再開されます。
- **メンテナンス (GIR モード)** : CloudSec キー再生成プロセスは、NX OS スタイル CLI を使用したキー再生成プロセスの無効化と再有効化 （29 ページ）に記載されている手順を使用して、手動で停止する必要があります。キー再生成は、ノードがトラフィックを転送する準備が再度整った後にのみ、有効にできます。
- **Cisco APICからのデコミッションと削除** : CloudSec キー再生プロセスは、NX OS スタイル CLI を使用したキー再生成プロセスの無効化と再有効化 （29 ページ） に記載されている手順を使用して、手動で停止する必要があります。キー再生成は、Cisco APICからノードが削除された後にのみ有効にできます。

## NX OS スタイル CLI を使用したキー再生成プロセスの無効化と再有効化

キーの再生成プロセスは、手動で停止し、再開することが可能です。特定の状況でキーの再生成プロセスを手動で管理することが必要な場合があります。たとえば、デコミッションとメンテナンスの切り替えなどです。ここでは、NX OS スタイル CLI をCisco APIC使用して設定を切り替える方法について説明します。

**ステップ 1** Cisco APIC NX OS スタイル CLI にログインします。

**ステップ 2** コンフィギュレーション モードを入力します。

**例**：

```
apic1# configure
apic1(config)#
```

**ステップ 3** デフォルト CloudSec プロファイルのコンフィグレーション モードを入力します。

**例**：

```
apic1(config)# template cloudsec default
apic1(config-cloudsec)#
```

**ステップ 4** キー再生成プロセスを停止または再起動します。

キー再生成プロセスを停止するには、次の手順を実行します。

**例**：

```
apic1(config-cloudsec)# stoprekey yes
```

キー再生成プロセスを再起動するには、次の手順を実行します。

**例**：

```
apic1(config-cloudsec)# stoprekey no
```

## REST API を使用したキー再生成プロセスの無効化と再有効化

キーの再生成プロセスは、手動で停止し、再開することが可能です。特定の状況でキーの再生成プロセスを手動で管理することが必要な場合があります。たとえば、デコミッションとメンテナンスの切り替えなどです。ここでは、Cisco APICREST API を使用して設定を切り替える方法について説明します。

**ステップ 1** キー再生成プロセスは、次のXML メッセージを使用して無効にすることができます。

**例**：

```
<fvTenant annotation="" descr="" dn="uni/tn-infra" name="infra" nameAlias="" ownerKey="" ownerTag="">

    <cloudsecIfPol descr="cloudsecifp" name="default" sakExpiryTime="10" stopRekey= "true" status=""
 />
</fvTenant>
```

**ステップ 2** キー再生成プロセスは、次のXML メッセージを使用して有効にすることができます。

例：

```
<fvTenant annotation="" descr="" dn="uni/tn-infra" name="infra" nameAlias="" ownerKey="" ownerTag="">

    <cloudsecIfPol descr="cloudsecifp" name="default" sakExpiryTime="10" stopRekey= "false" status=""
 />
</fvTenant>
```

# Cisco APIC への マルチサイト のクロス起動

マルチサイトは現在、テナントを作成してサイトを設定するときに選択する基本パラメータをサポートしています。マルチサイト は、ほとんどのテナント ポリシーをサポートしていますが、いくつかの拡張パラメータを設定することもできます。

マルチサイトGUIを使用して、設定する基本的なプロパティを管理します。高度なプロパティを設定する場合のために、マルチサイト GUI から直接 Cisco APIC GUI をクロス起動する機能が提供されます。Cisco APIC に直接、追加のプロパティを設定することもできます。

APIC にクロス起動できる場所とは別に、3 つの異なるアクセス ポイントが マルチサイト GUI にあります。マルチサイト のこれらのアクセス ポイントから、Cisco APIC へのアクセス権を持つ新しいブラウザ タブを開くことができます。最初に、Cisco APIC にログインします。それから Cisco APIC GUI に関連付けられた画面が表示されます。

## サイトから Cisco APIC をクロス起動する

**始める前に**

- 少なくとも 1 つのサイトは マルチサイト で設定する必要があります。
- サイトでは、少なくとも 1 つ、VRF とブリッジ ドメインのようなエンティティが設定されているテナントを含んでいる必要があります。

**ステップ 1** 左側のサイドバーで、**[サイト (Sites)]** ビューを開きます。

**ステップ 2** [**サイト (Sites)**] リストから、適切なサイトの名前の上にカーソルを合わせて、行の末尾の **[アクション (Action)]** アイコンをクリックし、[**APIC ユーザ インターフェイスで開く(Open in APIC User Interface)**] を選択して、Cisco APIC GUI にアクセスします。

APIC GUI ログイン画面が表示されるので、APIC GUI の資格情報でログインできます。

# スキーマからの Cisco APIC のクロス起動

始める前に

- マルチサイトでテンプレートに基づいて少なくとも1つのサイトを設定する必要があります。
- サイトは、少なくとも 1 つ、VRF とブリッジ ドメインのようなエンティティが設定されているテナントを含んでいる必要があります。

**ステップ 1** 左側のサイドバーから、**[スキーマ (schema)]** ビューを開きます。

**ステップ 2** **[スキーマ (schema)]** リストから、適切な **<スキーマ名>** をクリックします。

**ステップ 3** 左側のサイドバーの **[サイト (Sites)]** リストから、該当するサイトの名前の上にカーソルを移動し、行の最後にある **[アクション (Actions)]** アイコンをクリックし、**[APIC ユーザ インターフェイスで開く (Open in APIC User Interface)]** を選択して、Cisco APIC GUI にアクセスします。

APIC GUI ログイン画面が表示されるので、APIC GUI の資格情報でログインできます。

# プロパティ ペインから Cisco APIC をクロス起動する

始める前に

- 少なくとも 1 つのサイトは マルチサイト で設定する必要があります。
- サイトは、少なくとも 1 つ、VRF とブリッジ ドメインのようなエンティティが設定されているテナントを含んでいる必要があります。

**ステップ 1** 左側のサイドバーから、**[スキーマ (schema)]** ビューを開きます。

**ステップ 2** **[スキーマ (schema)]** リストから、適切な **<スキーマ名>** をクリックします。

**ステップ 3** 左側のサイドバーの [**サイト (Sites)**] リストから、適切なサイトを選択します。

**ステップ 4** **Canvas** で、特定のエンティティの名前を選択します。

たとえば、使用可能なVRF、契約、ブリッジドメイン、または必要に応じて別のエンティティを選択します。

その特定のエンティティの詳細が右側の **[プロパティ(Property)] ペイン** に表示されます。

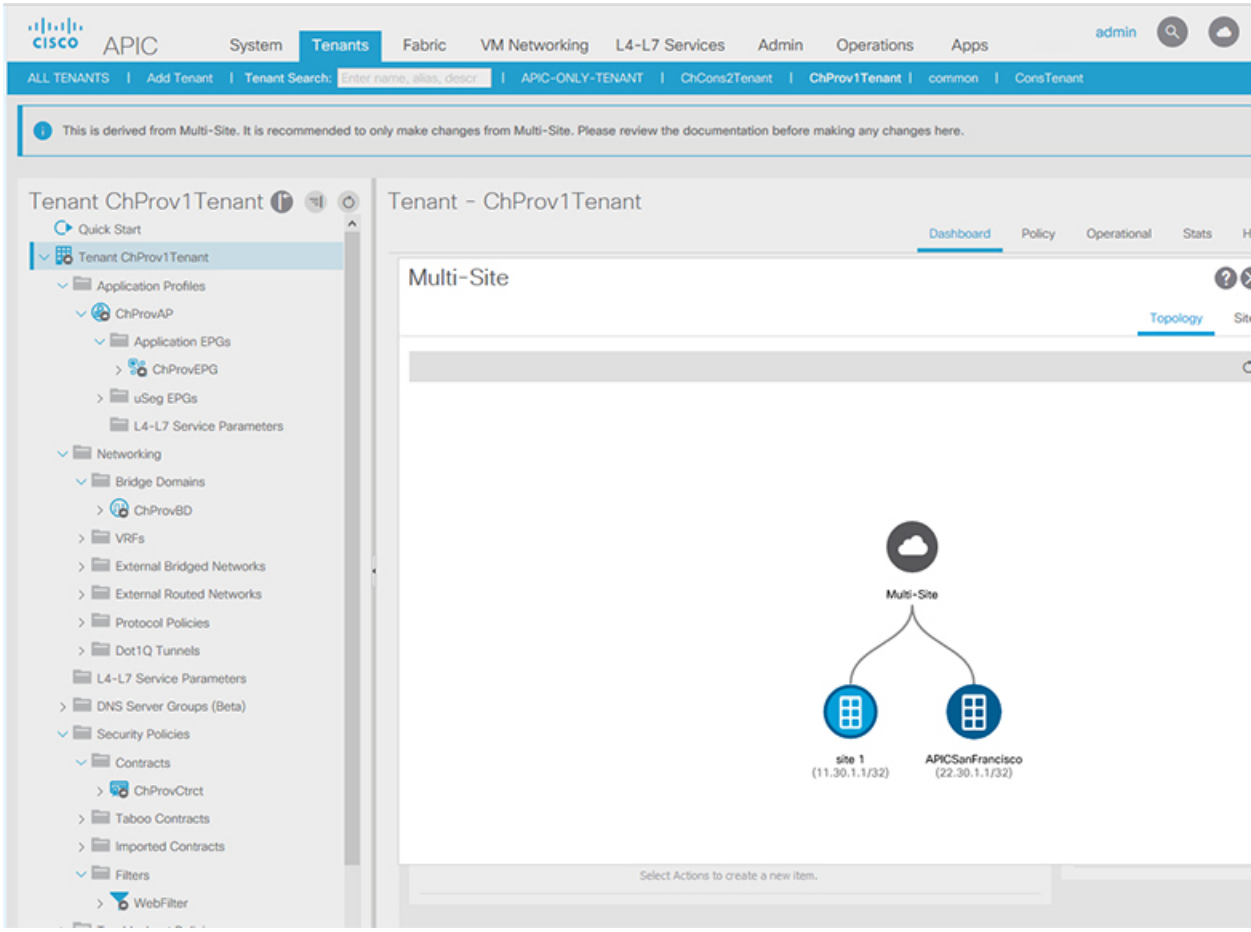
**ステップ 5** **[Property] ペイン**の右上にある [**APIC ユーザ インターフェイスで開く(Open in APIC Interface)**] アイコンをクリックして、Cisco APIC GUI にアクセスします。

APIC GUI ログイン画面が表示されるので、APIC GUI の資格情報でログインできます。

# Cisco ACI マルチサイト の管理対象オブジェクトを Cisco APIC GUI を使用して表示する。

APIC クラスタが マルチサイト によって管理されている場合、クラウド アイコンが他のサイトとの関係を示します。

**図 *4:* マルチサイト の管理対象オブジェクトを *APIC GUI* を使用して表示する。**




### 始める前に

APIC クラスタ/サイトは、Cisco ACI マルチサイト を使用して管理されるようセットアップされている必要があります。

**ステップ 1** APIC サイトと他のサイトとの関係を表示するには、設定アイコンの隣の、右上にあるクラウド アイコンをクリックします。

図において、ライトブルーのサイト アイコンにマウスを合わせるとローカル サイトの詳細が、ダーク ブルーのアイコンに合わせるとリモート サイトの詳細が表示されます。

画像において、T1 およびアプリケーション プロファイル、EPG、BD、VRF、および契約には、クラウドのアイコンが付けられます。これは、それらが マルチサイト によって管理されていることを示しています。これらのオブジェクトに変更を加えるには、マルチサイト GUI だけを使用することを推奨します。

**ステップ 2** 情報ページに **Show Usage** ボタンが表示されている VRF、ブリッジ ドメイン、またはその他のオブジェクトのローカライズまたは拡大された使用状況を表示するには、次の手順に従います。ここではブリッジ ドメインと VRF を例にします:

a) メニュー バーで、**Tenants** をクリックして、マルチサイト で管理されているテナントをダブルクリックします。

b) **Networking** > **Bridge Domains** > ***BD-name*** または **Networking** > **VRFs** > ***vrf-name*** をクリックします。

**ステップ 3** **Show Usage** をクリックします。

ここでは、オブジェクトを使用しているノードまたはポリシーを表示できます。

（注） 管理対象のポリシーを変更する場合には、マルチサイト GUI だけを使用することを推奨します。

**ステップ 4** この BD または VRF の導入の通知設定を範囲を設定するには、**Change Deployment Settings** をクリックします。**Policy** タブでは、オブジェクトのすべての削除と変更に対する警告を有効にすることができます。

**ステップ 5** グローバルな警告を有効または無効にするには、**(Global) Show Deployment Warning on Delete/Modify** チェック ボックスをオンまたはオフにします。

**ステップ 6** ローカルな警告を有効または無効にするには、**Yes** または **No** を **(Local) Show Deployment Warning on Delete/Modify** フィールドで選択します。

**ステップ 7** 過去の警告を表示するには、**History** タブ **Events** または **Audit Logs** をクリックします。

**Cisco ACI** マルチサイト の管理対象オブジェクトを **Cisco APIC GUI** を使用して表示する。