



Cisco ACI マルチサイトを介した Cisco Cloud APIC の管理

- [Cisco Cloud APIC と Cisco ACI マルチサイトについて](#) (1 ページ)
- [Cisco ACI マルチサイトへの Cisco Cloud APIC サイトの追加](#) (2 ページ)
- [サイト間インフラストラクチャの設定](#) (3 ページ)
- [Cisco Cloud APIC と ISN デバイス間の接続の有効化](#) (4 ページ)
- [共有テナントの設定](#) (8 ページ)
- [スキーマの作成](#) (10 ページ)
- [アプリケーションプロファイルと EPG の設定](#) (11 ページ)
- [ブリッジドメインの作成と VRF への関連付け](#) (11 ページ)
- [コントラクトのフィルタの作成](#) (12 ページ)
- [コントラクトの作成](#) (13 ページ)
- [サイトをスキーマに追加する](#) (14 ページ)
- [AWS でのインスタンスの設定](#) (14 ページ)
- [エンドポイントセレクタの追加](#) (17 ページ)
- [Cisco ACI Multi-Site 設定の検証](#) (21 ページ)

Cisco Cloud APIC と Cisco ACI マルチサイトについて

セットアップウィザードを使用して Cisco Cloud APIC を設定するときに [サイト間接続 (**Inter-Site Connectivity**)] オプションを [リージョン管理 (**Region Management**)] ページで選択した場合は、Cisco ACI マルチサイトを使用して、オンプレミスサイトやクラウドサイトなどの別のサイトを、Cisco Cloud APIC サイトとともに管理します。Cisco Cloud APIC のセットアップウィザードで、[クラウドルータ (**Cloud Routers**)] オプションだけを [リージョン管理 (**Region Management**)] ページで選択した場合は、Cisco ACI マルチサイトは必要ありません。

Cisco Cloud APIC の管理専用で使用される、いくつかの新しいページが ACI マルチサイト オペレータに導入されています。この章のトピックでは、これらの新しい Cisco Cloud APIC 管理ページについて説明します。これらの Cisco Cloud APIC 管理ページに必要な情報を入力すると、Cisco Cloud APIC は、実質的に、Cisco ACI マルチサイトを介して管理する別のサイトになります。

Cisco Cloud APIC サイトとともにオンプレミスサイトを管理している場合は、まだ設定していなければ、これらの手順を開始する前にオンプレミスサイトを設定しておくことを推奨します。これらの手順については、次の URL にある *CISCO ACI Multi Site Orchestrator Installation And Upgrade Guide* を参照してください。 <https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

Cisco ACI マルチサイトへの Cisco Cloud APIC サイトの追加

-
- ステップ 1** まだログインしていない場合は、ACI マルチサイト オーケストレータにログインします。
- 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 リスト]** ページで、**[サイトの追加 (ADD SITES)]** をクリックします。
- ステップ 4** **[接続設定]** ページで、次の操作を実行します。
- [名前 (NAME)]** フィールドに、サイト名を入力します。
たとえば、cloudsite1です。
 - (任意) **[ラベル (LABELS)]** フィールドで、ラベルを選択するか作成します。
 - [APIC CONTROLLER URL]** フィールドに、Cloud APIC の URL を入力します。これは、Amazon Web Services によって割り当てられるパブリック IP アドレスです。これは、セットアップウィザードを使用して Cloud APIC 設定 Cisco Cloud APIC する手順の開始時にログインするために使用したのと同じパブリック IP アドレスです。
たとえば、https://192.0.2.1です。
 - [ユーザ名 (USERNAME)]** フィールドにユーザ名を入力します。
たとえば、adminとします。admin と同じ権限を持つ任意のアカウントに登録することもできます。
 - [パスワード (PASSWORD)]** フィールドに、パスワードを入力します。
 - このフィールドが自動的に入力されていない場合は、**[APIC SITE ID]** フィールドに、一意のサイト ID を入力します。
サイト ID は、Cloud APIC サイトの固有識別子である必要があります。範囲は 1 ~ 127 です。
 - [保存 (SAVE)]** をクリックします。
- ステップ 5** Cloud APIC サイトが正しく追加されたことを確認します。
- 複数のサイトを管理している場合は、ACI マルチサイト オーケストレータの **[サイト (Sites)]** 画面にすべてのサイトを表示する必要があります。ACI マルチサイト オーケストレータは、サイトがオンプレミスであるか、Cloud APIC サイトであるかを自動的に検出します。
-

次のタスク

[サイト間インフラストラクチャの設定 \(3 ページ\)](#) に進みます。

サイト間インフラストラクチャの設定

ステップ 1 [サイト (Sites)] ビューで、[インフラの構築 (CONFIGURE INFRA)] をクリックします。

[ファブリック接続インフラ (Fabric Connectivity Infra)] ページが表示されます。

ステップ 2 左側のペインの [サイト (SITES)] の下で、クラウドサイトをクリックします。

クラウドサイト領域のほとんどすべての情報は自動的に入力され、次のステップで説明する [BGP パスワード (BGP Password)] フィールドを除き、変更できません。

ステップ 3 オンプレミス サイトとクラウド サイト間でパスワードを設定するかどうかを決定します。

- オンプレミス サイトとクラウド サイトの間でパスワードを設定しない場合は、[ステップ 4 \(3 ページ\)](#) に進みます。
- オンプレミス サイトとクラウド サイト間でパスワードを設定するには、次のようにします。
 - a) 右側のペインで、[BGP パスワード (BGP password)] フィールドをクリックして、パスワードを入力します。
 - b) [CloudSite] ウィンドウの右上隅にある [更新 (Refresh)] アイコンをクリックします。

すべてのクラウド プロパティは、Cloud APIC から自動的に取得されます。サイトが正常に更新されたことを示すメッセージが表示され、すべてのクラウド プロパティが Cloud APIC から正常に取得されたことを確認します。

ステップ 4 クラウド サイトでマルチサイト接続を有効にするには、[ACI マルチサイト (ACI Multi-Site)] ボタンをクリックします。

ステップ 5 サイト間インフラストラクチャを設定するために使用する展開のタイプを選択します。

画面の右上にある [展開 (Deploy)] ボタンをクリックすると、次のスクロールダウンメニューオプションが表示されます。

- **[展開のみ (Deploy Only):]** マルチクラウド (クラウドサイトからクラウドサイト) への接続を設定する場合は、このオプションを選択します。

このオプションは、クラウドサイトと Cloud APIC サイトに設定をプッシュし、クラウドサイト間のエンドツーエンドインターコネクト接続を有効にします。
- **[展開 & IPN デバイス設定ファイルをダウンロード (Deploy & Download IPN Device config files):]** オンプレミスの APIC サイトと Cloud APIC サイトの両方に設定をプッシュし、オンプレミスとクラウドサイト間のエンドツーエンドインターコネクト接続を有効にします。さらに、このオプションでは、AWS に導入された Cisco クラウド サービス ルータ (CSR) とオンプレミスの IPsec 終端 デバイスとの間の接続を有効にするための設定情報を含む zip ファイルをダウンロードします。すべてまたは一部

の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

- **[IPN デバイス設定ファイルのみをダウンロード (Download IPN Device config files only):]** AWS に展開された CSR とオンプレミスの IPsec 終端デバイス間の接続を有効にするために使用する、設定情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

Cisco Cloud APIC と ISN デバイス間の接続の有効化



- (注) このセクションの手順は、オンプレミス サイトとクラウド サイト間の接続を有効にしている場合にのみ実行してください。オンプレミス サイトがない場合は、これらの手順をスキップして、[共有テナントの設定 \(8 ページ\)](#) に進みます。

Amazon Web Services に展開された Cisco Cloud Services Router (CSR) とオンプレミスの IPsec ターミネーション デバイス間の接続を手動で有効にするには、次の手順に従います。

デフォルトでは、Cisco Cloud APIC は冗長 CSR のペアを展開します。このセクションの手順では、2 つのトンネルを作成します。1 つはオンプレミスの IPsec デバイスからこれらの各 CSR に対する IPsec トンネルです。

次の情報は、オンプレミスの IPsec ターミネーション デバイスとして CSR のコマンドを提供します。別のデバイスまたはプラットフォームを使用している場合は、同様のコマンドを使用します。

ステップ 1 AWS に導入された Csr とオンプレミスの IPsec ターミネーション デバイスとの間の接続を有効にするために必要な情報を収集します。

- [サイト間インフラストラクチャの設定 \(3 ページ\)](#) で示されている手順の一部として ACI マルチサイト オーケストレータで、**IPN デバイス設定ファイルを展開してダウンロードするか、IPN デバイス設定ファイルのみをダウンロードする**ように選択した場合、ISN デバイスの設定ファイルが含まれている zip ファイルを見つけます。
- AWS に展開された CSR とオンプレミスの IPsec ターミネーション デバイスとの間の接続を有効にするために必要な情報を手動で検索する場合は、『*Cisco Cloud APIC インストール ガイド*』の付録で説明されているように、CSR とテナントの情報を収集します。

ステップ 2 オンプレミスの IPsec デバイスにログインします。

ステップ 3 最初の CSR のトンネルを設定します。

ACI マルチサイト オーケストレータ を使用して、ISN デバイスの設定ファイルをダウンロードした場合は、最初の CSR の設定情報を見つけて、その設定情報を入力します。

次に、最初の CSR の設定情報がどのように表示されるかの例を示します。

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 2
  lifetime 86400
  hash sha
exit

crypto keyring infra:overlay-1-<first-CSR-tunnel-ID>
  pre-shared-key address <first-CSR-elastic-IP-address> key <first-CSR-preshared-key>
exit

crypto isakmp profile infra:overlay-1-<first-CSR-tunnel-ID>
  local-address <interface>
  match identity address <first-CSR-elastic-IP-address>
  keyring infra:overlay-1-<first-CSR-tunnel-ID>
exit

crypto ipsec transform-set infra:overlay-1-<first-CSR-tunnel-ID> esp-aes esp-sha-hmac
  mode tunnel
exit

crypto ipsec profile infra:overlay-1-<first-CSR-tunnel-ID>
  set pfs group2
  set security-association lifetime seconds 86400
exit

interface tunnel <first-CSR-tunnel-ID>
  ip address <peer-tunnel-for-onprem-IPsec-to-first-CSR> 255.255.255.252
  ip virtual-reassembly
  tunnel source <interface>
  tunnel destination <first-CSR-elastic-IP-address>
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile infra:overlay-1-<first-CSR-tunnel-ID>
  ip mtu 1476
  ip tcp adjust-mss 1460
  ip ospf <process-id> area <area-id>
  no shut
exit
```

それぞれの説明は次のとおりです。

- <first-CSR-tunnel-ID> は、このトンネルに割り当てる一意のトンネル ID です。
- <first-CSR-tunnel-ID> は、最初の CSR の 3 番目のネットワーク インターフェイスの柔軟な IP アドレスです。
- <first-CSR-preshared-key> は、最初の CSR の事前共有キーです。
- <interface> は、Amazon Web サービスに導入された CSR への接続に使用されるインターフェイスです。
- <peer-tunnel-for-onprem-IPsec-to-first-CSR> は、最初のクラウド CSR に対してオンプレミスの IPsec デバイスのピア トンネル IP アドレスとして使用されます。
- <process-id> は OSPF プロセス ID です。
- <area-id> は、OSPF エリア ID です。

次に例を示します。

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 2
  lifetime 86400
  hash sha
exit

crypto keyring infra:overlay-1-1000
  pre-shared-key address 192.0.2.20 key 123456789009876543211234567890
exit

crypto isakmp profile infra:overlay-1-1000
  local-address GigabitEthernet1
  match identity address 192.0.2.20
  keyring infra:overlay-1-1000
exit

crypto ipsec transform-set infra:overlay-1-1000 esp-aes esp-sha-hmac
  mode tunnel
exit

crypto ipsec profile infra:overlay-1-1000
  set pfs group2
  set security-association lifetime seconds 86400
exit

interface tunnel 1000
  ip address 30.29.1.2 255.255.255.252
  ip virtual-reassembly
  tunnel source GigabitEthernet1
  tunnel destination 192.0.2.20
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile infra:overlay-1-1000
  ip mtu 1476
  ip tcp adjust-mss 1460
  ip ospf 1 area 1
  no shut
exit
```

ステップ 4 2 番目の CSR のトンネルを設定します。

ACI マルチサイト オーケストレータ を使用して、ISN デバイスの設定ファイルをダウンロードした場合は、2 番目の CSR の設定情報を見つけて、その設定情報を入力します。

次に、2 番目の CSR の設定情報がどのように見えるかの例を示します。

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 2
  lifetime 86400
  hash sha
exit

crypto keyring infra:overlay-1-<second-CSR-tunnel-ID>
  pre-shared-key address <second-CSR-elastic-IP-address> key <second-CSR-preshared-key>
```

```
exit

crypto isakmp profile infra:overlay-1-<second-CSR-tunnel-ID>
  local-address <interface>
  match identity address <second-CSR-elastic-IP-address>
  keyring infra:overlay-1-<second-CSR-tunnel-ID>
exit

crypto ipsec transform-set infra:overlay-1-<second-CSR-tunnel-ID> esp-aes esp-sha-hmac
  mode tunnel
exit

crypto ipsec profile infra:overlay-1-<second-CSR-tunnel-ID>
  set pfs group2
  set security-association lifetime seconds 86400
exit

interface tunnel <second-CSR-tunnel-ID>
  ip address <peer-tunnel-for-onprem-IPsec-to-second-CSR> 255.255.255.252
  ip virtual-reassembly
  tunnel source <interface>
  tunnel destination <second-CSR-elastic-IP-address>
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile infra:overlay-1-<second-CSR-tunnel-ID>
  ip mtu 1476
  ip tcp adjust-mss 1460
  ip ospf <process-id> area <area-id>
  no shut
exit
```

次に例を示します。

```
crypto isakmp policy 1
  encryption aes
  authentication pre-share
  group 2
  lifetime 86400
  hash sha
exit

crypto keyring infra:overlay-1-1001
  pre-shared-key address 192.0.2.21 key 123456789009876543211234567891
exit

crypto isakmp profile infra:overlay-1-1001
  local-address GigabitEthernet1
  match identity address 192.0.2.21
  keyring infra:overlay-1-1001
exit

crypto ipsec transform-set infra:overlay-1-1001 esp-aes esp-sha-hmac
  mode tunnel
exit

crypto ipsec profile infra:overlay-1-1001
  set pfs group2
  set security-association lifetime seconds 86400
exit

interface tunnel 1001
  ip address 30.29.1.6 255.255.255.252
```

```

ip virtual-reassembly
tunnel source GigabitEthernet1
tunnel destination 192.0.2.21
tunnel mode ipsec ipv4
tunnel protection ipsec profile infra:overlay-1-1001
ip mtu 1476
ip tcp adjust-mss 1460
ip ospf 1 area 1
no shut
exit

```

ステップ 5 設定する必要があるその他の CSR について、これらの手順を繰り返します。

ステップ 6 オンプレミスの IPsec デバイスでトンネルがアップしていることを確認します。

次に例を示します。

```

ISN_CSR# show ip interface brief | include Tunnel
Interface          IP-Address      OK? Method Status          Protocol
Tunnel1000         30.29.1.2      YES manual up              up
Tunnel1001         30.29.1.4      YES manual up              up

```

両方のトンネルがアップとして表示されていない場合は、この項の手順で入力した情報を確認して、問題が発生している可能性がある場所を確認します。両方のトンネルがアップとして表示されるまで、次のセクションに進まないでください。

共有テナントの設定

オンプレミスサイトと Cloud APIC サイト間で共有されるテナントを設定するには、この項の手順に従います。

ステップ 1 ACI マルチサイト オーケストレータで、次の手順を実行します。

- a) メインメニューで、**[テナント (Tenants)]** をクリックします。
- b) [テナントリスト (Tenants List)] エリアで、**[テナントの追加 (ADD TENANT)]** をクリックします。
- c) [テナントの詳細 (Tenant Details)] ペインで、次の手順を実行します。
 - **[表示名 (DISPLAY NAME)]** フィールドに、テナント名を入力します。
 - **オプション: [説明 (DESCRIPTION)]** フィールドに、テナントについての簡潔な説明を入力します。
 - **[関連するサイト (Associated Sites)]** セクションで、オンプレミスとクラウドのサイトを選択します。
 - まだ選択していなければ、**[関連するユーザ (Associated Users)]** セクションで、ユーザを選択します。
 - **[保存 (SAVE)]** をクリックします。

ステップ 2 Cloud APICサイトにログインし、このテナントの Amazon Web Services アカウントの詳細を設定します。

- a) メインの Cloud APIC ページの **[アプリケーション管理 (Application Management)]** の下で、**[テナント (Tenant)]** をクリックします。
- b) **[テナント (Tenant)]** ページで、前の手順の ACI マルチサイト オーケストレータ で作成したテナントをクリックします。
- c) 画面の右上にある展開ボタンをクリックします。
これは、**[閉じる (X)]** ボタンの横にある、正方形と上向きの矢印が付いたボタンです。
- d) **[テナント (Tenant)]** ページで、画面の右上にある編集ボタンをクリックします。これは、**[アクション (Actions)]** フィールドの横にある、鉛筆のアイコンが付いたボタンです。
- e) **[テナントの編集 (Edit Tenant)]** ページで、**[設定 (Settings)]** 領域までスクロールし、ユーザテナントのアクセスタイプに応じて必要な情報を入力します。

- Cloud APIC のユーザテナントが信頼されている場合 (CFT を使用して信頼できるテナントの AWS アカウントを設定した場合) は、このページに次の情報を入力します。

- **[AWS アカウント ID (AWS Account ID):]** ユーザテナントの AWS アカウント番号 (CFT を使用して、信頼できるテナントの AWS アカウントをセットアップしたときにログインした AWS アカウント) を入力します。

- **[アクセスタイプ (Access Type)]:** このフィールドで**[信頼 (Trusted)]** を選択します。

(注) **[クラウドアクセスキー ID (Cloud Access KEY ID)]** フィールドと **[クラウド秘密アクセスキー (Cloud Secret Access Key)]** フィールドは、**[アクセスタイプ (Access Type)]** として **[信頼済み (Trusted)]** を選択している場合、表示されません。これらのフィールドは、信頼できるテナントには必要ありません。

- Cloud APICのユーザテナントが信頼されていない場合 (AWS アクセスキー ID と秘密アクセスキーを使用して、信頼できないユーザテナントの AWS アカウントをセットアップした場合) は、このページで次の情報を入力します。

- **[AWS アカウント ID (AWS Account ID):]** このフィールドには、ユーザテナントの AWS アカウント番号を入力します。

- **Access Type :** このフィールドで**[Untrusted]** を選択します。

- **[クラウドアクセスキー ID (Cloud Access KEY ID):]** このフィールドには、ユーザテナントの AWS アクセスキー ID 情報を入力します。

- **[クラウド秘密アクセスキー (Cloud Secret Access Key):]** このフィールドには、ユーザテナントの AWS 秘密アクセスキー情報を入力します。

- のユーザテナントがAWS組織のメンバーである場合 (AWS組織を使用して組織を設定し、組織内にアカウントを作成するか、組織にアカウントを招待することでアカウントを追加した場合) 、組織のマスターアカウントの場合は、次の情報を入力して組織タグをこのテナントに割り当てます。Cloud APICCloud APIC

- **[AWS アカウント ID (AWS Account ID):]** このフィールドには、ユーザテナントの AWS アカウント番号を入力します。

- [アクセスタイプ (Access Type)] : このフィールドで[組織 (Organization)]を選択します。
 - (注) このテナントに組織タグを割り当てる場合は、以下が適用されます。
 - このフィールドで[組織 (Organization)]オプションがグレー表示されている場合は、AWS組織のマスターアカウント (インフラストラクチャテナント) を展開していません。Cloud APIC (インフラテナント) がAWS組織のマスターアカウントに展開されていない場合、テナントに組織タグを割り当てることはできません。Cloud APIC詳細については、「[AWS で Cloud APIC を導入する](#)」を参照してください。
 - 既存のAWSアカウントに招待されたマスターアカウントが組織に加わる場合、組織テナント用のAWSに設定された OrganizationAccountAccessRole IAM ロールがあり、Cloud APIC 関連の許可を使用可能であることを確認してください。詳細については、「[AWS Organizations と組織のユーザ テナントのサポート](#)」を参照してください。
- (注) [クラウドアクセス キー ID (Cloud Access KEY ID)] フィールドと [クラウド秘密アクセス キー (Cloud Secret Access Key)] フィールドは、[アクセス タイプ (Access Type)] として [信頼済み (Trusted)] を選択している場合、表示されません。これらのフィールドは、組織テナントには必要ありません。

f) 画面の下部にある[保存 (Save)] をクリックします。

次のタスク

[スキーマの作成 \(10 ページ\)](#) に進みます。

スキーマの作成

Cisco Cloud APIC に固有ではない一般的な Cisco ACI Multi-Site 手順がいくつかありますが、Cisco ACI Multi-Site を介してオンプレミスサイトと Cisco Cloud APIC サイトを管理している場合は Cisco Cloud APIC の全体的なセットアップの一部として実行する必要があります。ここでは、APIC の Cisco Cloud 全体的なセットアップの一部である Cisco ACI Multi-Site の一般的な手順について説明します。

Cisco Cloud APIC サイトの新しいスキーマを作成する場合は、この項の手順に従ってください。

Cisco Cloud APIC サイトに使用するスキーマがすでにある場合は、これらの手順をスキップして、[サイトをスキーマに追加する \(14 ページ\)](#) に移動することができます。

ステップ 1 メインメニューで[スキーマ]をクリックします。

ステップ 2 [スキーマ] ページで、[スキーマの追加] をクリックします。

- ステップ 3** [無題スキーマ] ページで、ページの上にあるテキスト 無題スキーマを、作成するスキーマの名前 (たとえば、Cloudbursting スキーマ) に置き換えます。
- ステップ 4** 左側のペインで [ロール (Roles)] をクリックします。
- ステップ 5** 中央のペインで、スキーマを作成するエリアをクリックしてテナントを選択してくださいをクリックしてください。
- ステップ 6** [テナントの選択] ダイアログ ボックスにアクセスし、ドロップダウン メニューから [共有テナントの設定 \(8 ページ\)](#) で作成したテナントを選択します。

アプリケーション プロファイルと EPG の設定

この手順では、アプリケーション プロファイルを設定し、2 つの EPG を追加する方法について説明します。1 つはクラウドサイト用、もう 1 つは、プロバイダ コントラクトが 1 つの EPG に関連付けられており、コンシューマ コントラクトが他の EPG に関連付けられている場合です。

- ステップ 1** 中央のペインで、[アプリケーション プロファイル (Application Profile)] エリアを見つけて、[+ アプリケーション プロファイル (+ Application profile)] をクリックします。
- ステップ 2** 右側のペインで、[表示名 (DISPLAY NAME)] フィールドにアプリケーション プロファイルの名前を入力します。
- ステップ 3** 中央のペインで、[+ EPG の追加 (+ ADD EPG)] をクリックして、クラウドサイトの EPG を作成します。
- ステップ 4** 右側のペインで、[表示名 (DISPLAY NAME)] フィールドに EPG の名前を入力します (たとえば epg1)。
- ステップ 5** オンプレミスサイトの EPG を作成する場合には、中央のペインで、[+ EPG の追加 (+ ADD EPG)] をクリックします。
- ステップ 6** 右側のペインで、[表示名 (DISPLAY NAME)] フィールドに EPG の名前を入力します (たとえば epg2)。
- ステップ 7** VRF を作成します。
- 中央のペインで、[VRF] エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。
 - 右側のペインで、[表示名 (DISPLAY NAME)] フィールドに EPG の名前を入力します (たとえば vrf1)。
- ステップ 8** [保存 (SAVE)] をクリックします。

ブリッジ ドメインの作成と VRF への関連付け

この項の手順に従って、オンプレミスサイトのブリッジ ドメインを作成し、それを VRF に関連付けます。これらの手順は、クラウドのみのスキーマには必要ではないことに注意してください。

-
- ステップ 1** 中央のペインで、**[EPG]**まで上にスクロールして戻り、以前にオンプレミスサイト用に作成した EPG をクリックします。
- ステップ 2** 右側のペインの**[オンプレミス プロパティ (ON-PREMPROPERTIES)]** エリアの**[ブリッジドメイン (BRIDGE DOMAIN)]**の下で、フィールドに名前を入力し(たとえば、bd1)、**[作成 (create)]** エリアをクリックして新しいブリッジドメインを作成します。
- ステップ 3** 中央のペインで、今作成したブリッジドメインをクリックします。
- ステップ 4** **[仮想ルーティング/フォワーディング (Virtual Routing & Forwarding)]** フィールドで、[アプリケーションプロファイルと EPG の設定 \(11 ページ\)](#) で作成した VRF を選択します。
- ステップ 5** **[サブネット (SUBNETS)]** エリアまで下にスクロールし、**[GATEWAY (ゲートウェイ)]** 見出しの下の**[サブネット (SUBNET)]**の横にある + をクリックします。
- ステップ 6** **[サブネットの追加 (Add Subnet)]** ダイアログで、**[ゲートウェイ IP (Gateway IP)]** アドレスと、追加する予定のサブネットの説明を入力します。このゲートウェイ IP アドレスは、オンプレミスのサブネットのもです。
- ステップ 7** **[範囲 (Scope)]** フィールドで、**[外部にアドバタイズ (Advertised Externally)]** を選択します。
- ステップ 8** **[保存 (SAVE)]** をクリックします。
-

コントラクトのフィルタの作成

- ステップ 1** 中央のペインで、**[コントラクト (Contract)]** エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。
- ステップ 2** 右側のペインで、**[表示名 (DISPLAY NAME)]** フィールドにフィルタの名前を入力します。
- ステップ 3** **[+ 入力 (+ Entry)]** をクリックして、**[エントリの追加 (Add Entry)]** ディスプレイ上のスキーマフィルタについての情報を入力します。
- Name** フィールド (**Add Entry** ダイアログ) のスキーマ フィルタ エントリの名前を入力します。
 - オプション。 **Description** フィールドにフィルタの説明を入力します。
 - EPG の通信のフィルタ処理を行うために、必要に応じて詳細を入力します。

たとえば、フィルタを通過する HTTPS トラフィックを許可するエントリを追加するには、次のように選択します。

TYPE: IP、IP PROTOCOL: TCP、および DESTINATION PORT RANGE FROM および DESTINATION PORT range TO: https。
 - [保存 (SAVE)]** をクリックします。
-

コントラクトの作成

- ステップ 1 中央のペインで、[コントラクト (Contract)] エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。
- ステップ 2 右側のペインで、[表示名 (DISPLAY name)] フィールドにコントラクトの名前を入力します。
- ステップ 3 [範囲 (SCOPE)] エリアで、VRF の選択をそのままにします。
- ステップ 4 [フィルタ チェーン (FILTER CHAIN)] エリアで、[+ フィルタ (+ FILTER)] をクリックします。
[フィルタ チェーンの追加 (Add Filter Chain)] 画面が表示されます。
- ステップ 5 [名前 (NAME)] フィールドで、[コントラクトのフィルタの作成 \(12 ページ\)](#) で作成したフィルタを選択します。
- ステップ 6 中央のペインで、[EPG] までスクロールして戻り、クラウドサイト用に作成した EPG をクリックします。
- ステップ 7 右側のペインで、[+コントラクト (+ CONTRACT)] をクリックします。
[コントラクトの追加] 画面が表示されます。
- ステップ 8 [コントラクト (contract)] フィールドで、この手順で以前に作成したコントラクトを選択します。
- ステップ 9 [タイプ (TYPE)] フィールドで、[コンシューマ](#)または[プロバイダ](#)のいずれかを選択します。
- ステップ 10 [クラウドのプロパティ (CLOUD PROPERTIES)] エリアまでスクロールし、[仮想ルーティングと転送 (VIRTUAL ROUTING & FORWARDING)] エリアで、[アプリケーションプロファイルと EPG の設定 \(11 ページ\)](#) で作成した VRF を選択します。
- ステップ 11 [保存 (SAVE)] をクリックします。
- ステップ 12 中央のペインで、[EPG] までスクロールして戻り、オンプレミスサイト用に作成した EPG をクリックします。
- ステップ 13 右側のペインで、[+コントラクト (+ CONTRACT)] をクリックします。
[コントラクトの追加] 画面が表示されます。
- ステップ 14 [コントラクト (contract)] フィールドで、この手順で以前に作成したコントラクトを選択します。
- ステップ 15 [タイプ (TYPE)] フィールドで、[[コンシューマ \(CONSUMER\)](#)] または [[プロバイダ \(PROVIDER\)](#)] を選択します。これは、前の EPG に選択しなかったものです
たとえば、最初の EPG に [[プロバイダ \(PROVIDER\)](#)] を選択した場合は、2番目の EPG の [[コンシューマ \(CONSUMER\)](#)] を選択します。
- ステップ 16 [クラウドのプロパティ (CLOUD PROPERTIES)] エリアまでスクロールし、[仮想ルーティングと転送 (VIRTUAL ROUTING & FORWARDING)] エリアで、[アプリケーションプロファイルと EPG の設定 \(11 ページ\)](#) で作成したものと同一 VRF を選択します。

サイトをスキーマに追加する

- ステップ 1** 左側のペインで、[**サイト (Sites)**] の横にある + をクリックします。
- ステップ 2** [**サイトの追加 (Add Sites)**] ページで、それぞれの横にあるボックスをオンにして、オンプレミスおよびクラウドサイトをスキーマに追加し、[**保存 (Save)**] をクリックします。
- ステップ 3** 左側のペインのクラウドサイトの下にあるテンプレートをクリックして、テンプレートのサイトローカルプロパティを設定します。
- ステップ 4** 中央のペインで、VRF をクリックします。
- ステップ 5** 右側のペインの [**サイト ローカル プロパティ (SITE LOCAL PROPERITES)**] 領域で、次の情報を入力します。
- [**リージョン (region)**] フィールドで、この VRF を導入する Amazon Web サービスのリージョンを選択します。
 - CIDR** フィールドで、+**CIDR** をクリックします。

[**クラウド CIDR の追加 (ADD CLOUD CIDR)**] ダイアログボックスが表示されます。次の情報を入力します。

- **CIDR**: VPC CIDR 情報を入力します。たとえば、11.11.0.0/16とします。

CIDR には、Amazon Web Services VPC で使用可能になるすべてのサブネットの範囲が含まれています。

(注) このフィールドに入力した VPC CIDR 情報は、インフラ VPC CIDR と重複させることはできません。このフィールドに入力した CIDR 情報が、[AWS で Cloud APIC を導入するの 12](#) の [**インフラ VPC プール (Infra VPC Pool)**] フィールドに入力したインフラ VPC CIDR 情報と重複していないことを確認します。

- [**CIDR タイプ (CIDR TYPE)**]: [プライマリ (Primary)] または [セカンダリ (Secondary)] を選択します。これが最初の CIDR の場合は、CIDR タイプとして [プライマリ (Primary)] を選択します。
- [**サブネット追加 (ADD SUBNETS)**]: サブネット情報を入力し、ゾーンを選択してから、チェックマークをクリックします。たとえば、11.11.1.0/24 とします。

サブネットは、各アベイラビリティゾーンの CIDR ブロックの範囲内に割り当てます。

- c) ウィンドウで [**保存 (Save)**] をクリックします。

AWS でのインスタンスの設定

Cloud APIC のためのエンドポイントセレクタを、Cloud APIC GUI または ACI マルチサイトオーケストレータ GUI のいずれかを使用して設定する場合には、Cloud APIC のために設定する

エンドポイントセレクタに対応し、AWS 内で必要なインスタンスについても、設定することが必要になります。

このトピックでは、AWS でインスタンスを設定する手順について説明します。Cloud APIC のためのエンドポイントセレクタを設定する前に、または後で、これらの手順を使用して AWS のインスタンスを設定することができます。たとえば、先に AWS のアカウントに移動し、AWS のカスタム タグまたはラベルを作成してから、ACI マルチサイト オーケストレータのカスタム タグまたはラベルを使用して、エンドポイントセレクタを作成することができます。または、ACI マルチサイト オーケストレータ でカスタム タグまたはラベルを使用してエンドポイントセレクタを作成してから、AWS のアカウントに移動し、AWS のカスタム タグまたはラベルを作成することもできます。

ステップ 1 ACI マルチサイト オーケストレータ GUI または Cisco Cloud APIC GUI を使用してクラウド コンテキスト プロファイルを設定したかどうかを確認します。

クラウド コンテキスト プロファイルは、AWS インスタンス設定プロセスの一部として設定する必要があります。ここで、クラウド コンテキスト プロファイルは、VRF およびリージョンと組なって、そのリージョン内の AWS VPC を表します。Cisco Cloud APIC GUI を使用してクラウド コンテキスト プロファイルを設定すると、VRF やリージョンの設定などの設定情報は、AWS にプッシュされます。同様のアクションは、Cisco Cloud APIC を ACI マルチサイト オーケストレータ GUI を使用して設定した場合にも生じます。ここで、これらのクラウド コンテキスト プロファイル設定は、Cisco Cloud APIC 設定プロセスの一部として ACI マルチサイト オーケストレータ GUI によって設定され、AWS にプッシュされます。

- Cisco Cloud APIC を ACI マルチサイト オーケストレータ GUI を使用して設定する場合は、クラウド コンテキスト プロファイルを手動で設定する必要はありません。VRF やリージョン設定など、特定のクラウド コンテキスト プロファイル設定は、Cisco Cloud APIC 設定プロセスの一部として、前のセクションで実行した ACI マルチサイト オーケストレータ GUI により設定され、AWS にプッシュされます。
- クラウド コンテキスト プロファイルを Cisco Cloud APIC GUI を使用して設定する場合には、『Cisco Cloud APIC User Guide, Release 4.1(x)』で説明されている手順に従い、GUI または REST API を使用して、クラウド コンテキスト プロファイルを設定してください。

ステップ 2 クラウド コンテキスト プロファイルの設定を確認し、AWS インスタンスで使用する設定を決定します。

- a) まだログインしていない場合は、Cisco Cloud APIC にログインします。
- b) **[ナビゲーション (Navigation)]** メニューで、**[アプリケーション管理 (Application Management)]** タブを選択します。

[アプリケーション管理 (Application Management)] タブを展開すると、サブタブ オプションのリストが表示されます。

- c) **[クラウド コンテキスト プロファイル (Cloud Context Profiles)]** サブタブ オプションを選択します。
Cisco Cloud APIC 用に作成したクラウド コンテキスト プロファイルのリストが表示されます。
- d) この AWS インスタンス設定プロセスの一部として使用するクラウド コンテキスト プロファイルを選択します。

リージョン、VRF、IP アドレス、サブネットなど、このクラウドコンテキストプロファイルのさまざまな設定パラメータが表示されます。AWS インスタンスを設定するときには、このウィンドウに表示される情報を使用します。

- ステップ 3** まだログインしていない場合は、Cisco Cloud APIC ユーザテナントの Amazon Web Services アカウントにログインします。
- ステップ 4** [サービス (Services)] > EC2 > インスタンス (Instances) > [インスタンスの起動 (Launch Instance)] に移動します。
- ステップ 5** [Amazon マシン イメージ (AMI) の選択 (Choose Amazon Machine Image (AMI))] ページで、Amazon マシン イメージ (AMI) を選択します。
- ステップ 6** [インスタンス タイプの選択 (Choose An Instance type)] ページで、インスタンス タイプを選択し、[インスタンスの詳細の設定 (Configure instance Detail)] をクリックします。
- ステップ 7** [インスタンスの詳細の設定 (Configure instance Detail)] ページで、該当するフィールドに必要な情報を入力します。

- [ネットワーク (Network)] フィールドで、Cloud APIC VRF を選択します。

これは、この AWS インスタンス設定プロセスの一部として使用しているクラウドコンテキストプロファイルに関連付けられている VRF です。

- [サブネット (Subnet)] フィールドに、サブネットを入力します。
- パブリック IP を使用する場合は、[パブリック IP の自動割り当て (Auto Assign public IP)] フィールドで、スクロールダウンメニューから [有効 (Enable)] を選択します。

- ステップ 8** [インスタンスの詳細の設定 (Configure Instance Details)] ページに必要な情報を入力したら、[ストレージを追加 (Add Storage)] をクリックします。
- ステップ 9** [ストレージの追加 (Add Storage)] ページで、デフォルト値を受け入れるか、必要に応じてこのページでストレージを設定し、[タグの追加 (add Tags)] をクリックします。
- ステップ 10** [タグの追加 (Add Tags)] ページで、[タグの追加 (add Tag)] をクリックし、このページの該当するフィールドに必要な情報を入力します。

(注) これらの手順の後の部分で、エンドポイントセレクトアのタイプに対して IP アドレス、リージョン、またはゾーンを使用する場合は、このページに情報を入力する必要はありません。このような状況では、AWS でインスタンスを開始すると、Cloud APIC によって IP アドレス、リージョン、またはゾーンが検出され、エンドポイントが EPG に割り当てられます。

- [キー (Key):] これらの手順で後で追加するエンドポイントセレクトアのタイプのカスタム タグを作成するときに使用するキーを入力します。
- [値 (Value):] このキーで使用する値を入力します。
- [インスタンス (Instance):] このフィールドのチェックボックスをオンにします。
- [ボリューム (Volume):] このフィールドのチェックボックスをオンにします。

たとえば、これらの手順で後ほど、エンドポイントセレクトアの特定のビルディングのカスタム タグを作成する予定の場合 (building6 など) は、このページの次のフィールドに次の値を入力できます。

- [キー (Key):] ロケーション
- [値 (value):] building6

ステップ 11 [確認して起動する (Review and Launch)] をクリックします。

既存のキーペアを選択するか、新しいキーペアを作成します。キーペアの ページが表示されます。後ほどインスタンスに ssh 接続する場合は、このページの情報を使用します。

エンドポイントセレクタの追加

Cisco Cloud APICでは、クラウド EPGは、同じセキュリティポリシーを共有するエンドポイントの集合です。クラウド EPGは、1つまたは複数のサブネット内にエンドポイントを持つことができ、VRFに関連付けられます。

Cisco Cloud APICには、エンドポイントをクラウド EPGに割り当てるために使用される、エンドポイントセレクタと呼ばれる機能があります。エンドポイントセレクタは、基本的に言って、Cisco ACIによって管理される AWS VPCに割り当てられたクラウドインスタンスに対して実行される一連のルールです。エンドポイントインスタンスに一致するエンドポイントセレクタルールは、そのエンドポイントをクラウド EPGに割り当てます。エンドポイントセレクタは、Cisco ACIで使用可能な属性ベースのマイクロセグメンテーションに似ています。

エンドポイントセレクタは、Cisco Cloud APIC GUI または ACI マルチサイト オークストレータ GUI のいずれかを使用して設定できます。2つの GUI 間で使用可能なオプションにはわずかな違いがありますが、エンドポイントセレクタを追加するための一般的な概念と全体的な手順は、基本的にこの2つの間で同じです。

このセクションの手順では、ACI マルチサイト オークストレータ GUI を使用してエンドポイントセレクタを設定する方法について説明します。Cisco Cloud APIC GUI を使用したエンドポイントセレクタの設定の詳細については、『Cisco Cloud APIC User Guide, Release 4.1 (x)』を参照してください。

ステップ 1 Cisco Cloud APIC のエンドポイントセレクタに使用できる Amazon Web Services サイトから、必要な情報を収集します。

手順については、[AWS でのインスタンスの設定 \(14 ページ\)](#) を参照してください。

(注) これらの手順は、最初に AWS でインスタンスを設定してから、その後に Cisco Cloud APIC のエンドポイントセレクタを追加することを前提としています。ただし、[AWS でのインスタンスの設定 \(14 ページ\)](#) で説明されているように、最初に Cisco Cloud APIC のエンドポイントセレクタを追加してから、この AWS インスタンスの設定手順を、これらのエンドポイントセレクタの手順の最後で実行することもできます。

ステップ 2 ログインしていない場合は、ACI マルチサイト オークストレータ にログインします。

ステップ 3 左側のペインで、[スキーマ (schema)] をクリックし、以前に作成したスキーマを選択します。

ステップ 4 エンドポイント セレクタを作成する方法を決定します。

- 今後追加される、任意のクラウドサイトに適用できるエンドポイントセレクタを作成するには、次の手順を実行します。
 1. 左側のペインで、テンプレートを選択したままにします。
これらの手順で特定のサイトを選択しないでください。
 2. 中央のペインで、クラウドサイト用に作成した EPG を選択します。
 3. 右側のペインの **[クラウドのプロパティ (CLOUD PROPERITES)]** 領域で、+ **([セレクタ (SELECTORS)]** の横にあるもの) をクリックして、エンドポイント セレクタを設定します。
 4. **[新しいエンドポイント セレクタの追加 (Add New End Point selector)]** ダイアログで、**[エンドポイント セレクタ名 (END POINT SELECTOR NAME)]** フィールドに、このエンドポイント セレクタで使用する分類に基づいて名前を入力します。
 5. **[+ 式 (Expression)]** をクリックし、エンドポイント セレクタのタイプを選択します。
このように作成されたエンドポイントセレクタの場合、**[キー (Key)]** フィールドで使用できるオプションは **[EPG]** のみです。
 6. **ステップ 5 (19 ページ)** に進みます。
- このクラウドサイト専用のエンドポイント セレクタを作成するには、次の手順を実行します。
 1. 左ペインで、クラウドサイトを選択します。
 2. 中央のペインで、クラウドサイト用に作成した EPG を選択します。
 3. 右側のペインの **[サイトのローカルのプロパティ (SITE LOCAL PROPERITES)]** 領域の **[セレクタ (SELECTOR)]** 領域で、+ **([セレクタ (SELECTOR)]** の横にあるもの) をクリックして、エンドポイント セレクタを設定します。
 4. **[新しいエンドポイント セレクタの追加 (Add New End Point selector)]** ダイアログで、**[エンドポイント セレクタ名 (END POINT SELECTOR NAME)]** フィールドに、このエンドポイント セレクタで使用する分類に基づいて名前を入力します。
たとえば、IPサブネット分類のエンドポイントセレクタの場合は、**[IP-Subnet-EPSelector]** などの名前を使用できます。
 5. **[+ 式 (Expression)]** をクリックし、エンドポイント セレクタで使用するキーを選択します。
 - **[IP アドレス (IP Address)]**: IP アドレスまたはサブネットによって選択するために使用されます。
 - **[リージョン (Region)]**: エンドポイントの AWS リージョンで選択するために使用されます。
 - **[ゾーン (Zone)]**: エンドポイントの AWS アベイラビリティ ゾーンによって選択するために使用されます。
 - エンドポイントセレクタのカスタムタグを作成する場合は、**[検索または作成のために入力 (Type to search or create)]** フィールドで入力を開始してカスタム タグまたはラベルを入力

し、新しいフィールドで **[作成 (Create)]** をクリックして、新しいカスタム タグまたはラベルを作成します。

AWS にタグを追加するときに、これらの手順の前の例を使用すると、以前に AWS で追加したロケーション タグと一致するように、このフィールドにカスタム タグのロケーションを作成できます。

ステップ 5 **[演算子 (Operator)]** フィールドで、エンドポイントセレクタに使用する演算子を選択します。

(注) 4.2(1) より前のリリースでは、オプションとして **[キーが存在 (Key Exist)]** と **[キーが存在しない (Key Not Exist)]** を使用していましたが、現在では **[キーを持つ (Has Key)]** と **[キーを持たない (Does Not Have Key)]** になっています。異なるのはオプションの名前だけで、機能はどちらのオプションのセットでも同じです。

次のオプションがあります。

- **[等しい (Equals)]:** [値 (value)] フィールドに 1 つの値がある場合に使用します。
- **[等しくない (Not Equals)]:** 値フィールドに 1 つの値がある場合に使用されます。
- **[の中にある (In)]:** [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。
- **[の中にない (Not In)]:** 値フィールドに複数のカンマ区切り値がある場合に使用されます。
- **[キーを持つ (Has Key)]:** 式にキーのみが含まれている場合に使用されます。
- **[キーを持たない (Does Not Have Key)]:** 式にキーのみが含まれている場合に使用されます。

ステップ 6 **[値 (value)]** フィールドで、2 つ前のフィールドに対して行った選択に基づいて、エンドポイントセレクタに使用する値を選択します。 **[値 (Value)]** フィールドには、複数のカンマ区切りのエントリを含めることができます。このフィールドのエントリの間には論理 OR があるものとみなされます。

(注) **[キーを持つ (Has Key)]** または **[キーを持たない (Does Not Have Key)]** を選択していない場合には、 **[演算子 (Operator)]** フィールドは表示されません。

たとえば、エンドポイントセレクタに、us-west-1a など特定の Amazon Web サービスのアベイラビリティゾーンを設定する場合には、この画面で次の項目を選択します。

- **[キー (Key):]** Zone
- **[演算子 (Operator):]** Equals
- **[値 (Value):]** us-west-1a

別の例として、これらのフィールドで次の値を使用したとします。

- **[キー (Key):]** IP
- **[演算子 (Operator):]** Has Key
- **[値 (Value):]** は、演算子 (Operator) フィールドで **[Has Key]** が使用されているため、使用できません。

EPG ルールは、この状況で IP アドレスを持つすべてのエンドポイントに適用されます。

最後の例として、これらのフィールドで次の値を使用したとします。

- **[キー (Key):]** custom tag: Location
- **[演算子 (Operator):]** Has Key
- **[値 (Value):]** は、演算子 (Operator) フィールドで [Has Key] が使用されているため、使用できません。

この場合、EPG ルールは、AWS タグキーとして Location を持つすべてのエンドポイントに、ロケーションの値に関係なく適用されます。

ステップ 7 このエンドポイントセクタ式の作成が完了したら、チェックマークをクリックします。

ステップ 8 追加のエンドポイントセクタ式を作成するかどうかを決定します。

単一のエンドポイントセクタで複数の式を作成した場合、それらの式の間には論理 AND があるものとみなされます。たとえば、1つのエンドポイントセクタで2つの式セットを作成したとします。

- エンドポイントセクタ 1、式 1:
 - **[キー (Key):]** Zone
 - **[演算子 (Operator):]** Equals
 - **[値 (Value):]** us-west-1a
- エンドポイントセクタ 1、式 2:
 - **[キー (Key):]** IP
 - **[演算子 (Operator):]** Equals
 - **[値 (Value):]** 192.0.2.1/24

この場合、これらの式の両方が真になる場合 (アベイラビリティゾーンが us-west-1a で、IP アドレスがサブネット 192.0.2.1/24 に属している場合) に、そのエンドポイントはクラウド EPG に割り当てられません。

このエンドポイントセクタで作成するすべての式を追加した後で、チェックマークをクリックします。

ステップ 9 このエンドポイントセクタの式の作成が完了したら、**[保存 (SAVE)]** をクリックします。これは **[新しいエンドポイントセクタの追加 (Add New End Point selector)]** の右下隅にあります。

EPG の下で複数のエンドポイントセクタを作成した場合は、それらのエンドポイントセクタの間には論理 OR があるものとみなされます。たとえば、前のステップで説明したようにエンドポイントセクタ 1 を作成し、次に、次に示すように 2 番目のエンドポイントセクタを作成したとします。

- エンドポイントセクタ 2、式 1:
 - **[キー (Key):]** Region
 - **[演算子 (Operator):]** In

- [値 (Value):] us-east-1a, us-east-2

その場合、次のようになります。

- アベイラビリティ ゾーンが us-west-1a で、IP アドレスが 192.0.2.1/24 サブネットに属している (エンドポイント セレクタ 1 の式)

または

- リージョンが us-east-1a または us-east-2 (エンドポイント セレクタ 2 の式) のいずれかである

その場合、エンドポイントがクラウド EPG に割り当てられます。

ステップ 10 エンドポイント セレクタの作成が完了したら、右上隅の [保存 (SAVE)] をクリックします。

ステップ 11 画面の右上隅にある [サイトに展開 (DEPLOY TO SITES)] ボタンをクリックして、スキーマをサイトに展開します。

[正常に展開 (Successfully Deployed)] されたというメッセージが表示されます。

次のタスク

[Cisco ACI Multi-Site 設定の検証 \(21 ページ\)](#) の手順を使用して、Cisco ACI マルチサイト エリアが正しく設定されていることを確認します。

Cisco ACI Multi-Site 設定の検証

このトピックの手順を使用して、ACI マルチサイト オーケストレータ に入力した設定が正しく適用されていることを確認します。

ステップ 1 Cloud APIC にログインし、次のことを確認します。

- a) [ダッシュボード (Dashboard)] をクリックし、オンプレミス接続ステータスおよびリージョン間接続ステータスボックスの情報を使用して、次のことを確認します。
 - トンネルは、AWS 上の Cisco Cloud Services Router 1000V から、オンプレミスの ISN (IPsec ターミネーションポイント)、およびユーザ VPC の VGW に対して動作しています。
 - OSPF ネイバーが Cisco Cloud サービス ルータと ISN オンプレミス デバイスの間で起動していることを示します。
 - VRF の BGP EVPN ルートにはクラウドとオンプレミスのルートが表示され、クラウドルートは ACI スパインスイッチの BGP EVPN を介して入力されます。
- b) [アプリケーション管理 (Application Management)] → [テナント] をクリックし、テナントが正しく設定されていることを確認します。

- c) [アプリケーション管理 (Application Management)] → [アプリケーションプロファイル] をクリックし、アプリケーションプロファイルが正しく設定されていることを確認します。
- d) [アプリケーション管理 (Application Management)] → [EPG] をクリックし、EPG が正しく設定されていることを確認します。
- e) [アプリケーション管理 (Application Management)] → [コントラクト] をクリックし、契約が正しく設定されていることを確認します。
- f) [アプリケーション管理 (Application Management)] → [VRF] をクリックし、VRF が正しく設定されていることを確認します。
- g) [アプリケーション管理 (Application Management)] → [クラウド コンテキスト Cloud プロファイル] をクリックし、クラウド コンテキスト プロファイルが正しく設定されていることを確認します。
- h) [クラウドリソース (Cloud Resources)] → [リージョン] をクリックし、リージョンが正しく設定されていることを確認します。
- i) [クラウドリソース (Cloud Resources)] → [VPC] をクリックし、VPC が正しく設定されていることを確認します。
- j) [クラウドリソース (Cloud Resources)] → [クラウド エンドポイント] をクリックし、クラウド エンドポイントが正しく設定されていることを確認します。
- k) [クラウドリソース (Cloud Resources)] → [ルータ] をクリックし、CSR が正しく設定されていることを確認します。

ステップ 2 オンプレミスの APIC サイトにログインし、APIC のスキーマを確認します。

ACI マルチサイト オーケストレータ で設定した共有テナントが APIC のテナントエリアに表示され、ACI マルチサイト オーケストレータ スキーマから展開された VRF と EPG がオンプレミス APIC で設定されていることが確認できます。

ステップ 3 コマンドラインから、AWS の Cisco Cloud サービス ルータ 1000V で VRF が正しく作成されていることを確認します。

```
show vrf
```

テナント t1 と VRF v1 が ACI マルチサイト オーケストレータ から展開されている場合、CSR の出力は次のようになります。

Name	Default RD	Protocols	Interfaces
t1:v1	64514:3080192	ipv4	BD1 Tu4 Tu5

ステップ 4 コマンドラインから、AWS サービス ルータ 1000V と ISN オンプレミス デバイスの間 Cisco Cloud でトンネルがアップしていることを確認します。

AWS または ISN オンプレミスのデバイスで、Cisco Cloud サービス ルータ 1000V で次のコマンドを実行できます。

```
show ip interface brief | inc Tunnel
```

以下のような出力が表示されます。

Interface	IP-Address	OK?	Method	Status	Protocol
Tunnel1	1.2.3.22	YES	manual	up	up
Tunnel2	1.2.3.30	YES	manual	up	up

Tunnel3	1.2.3.6	YES	manual	up	up
Tunnel4	1.2.3.14	YES	manual	up	up

ステップ5 コマンドラインから、OSPF ネイバーが AWS 上の Cisco Cloud サービス ルータ 1000V と ISN オンプレミス デバイスの間でアップしていることを確認します。

```
show ip ospf neighbor
```

以下のような出力が表示されます。

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.200.10.201	0	FULL/ -	00:00:36	1.2.3.13	Tunnel4
20.30.40.50	0	FULL/ -	00:00:36	1.2.3.29	Tunnel2
10.202.101.202	0	FULL/ -	00:00:38	1.2.3.5	Tunnel3

ステップ6 コマンドラインから、オンプレミスの BGP EVPN ネイバーが Cisco Cloud サービス ルータ 1000V に存在することを確認します。

```
show bgp l2vpn evpn summary
```

以下のような出力が表示されます。

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.1.1.2	4	100	139	137	99	0	0	01:30:36	6

ステップ7 コマンドラインから、VRF の BGP ルートにクラウドとオンプレミスの両方のルートが表示されていることを確認します。

(注) 現在 Cloud APIC のワークフローでは、VRF は、対応する VPC が AWS で作成されるまで、Cisco Cloud サービスルータ 1000V で設定されません。

```
show ip route vrf t1:v1
```

以下のような出力が表示されます。

```
B 129.1.1.5/32[20/0] via 10.11.0.34, 01:12:41, BD|1
B 130.1.0.0/16[20/100] via 131.254.4.5, 01:09:55
```

