Cisco Cloud APIC のクラウド形成テンプレート情報の設定

AWS で Cloud APIC を導入する

始める前に

- このセクションのタスクに進む前に、Cisco ACI ファブリックをパブリック クラウドに拡張するための要件に示されている要件を満たしていることを確認します。たとえば、エラスティック IP アドレスの数が正しいこと、およびインスタンス展開の許可の制限をチェックしたことを確認します。
- Cisco Cloud APIC のインストールと操作には、特定の AWS IAM ロールおよび権限が必要であるため、AWS で完全な管理者アクセス権を持っていることを確認します。

  CloudFormation テンプレート (CFT) を使用して Cloud APIC をインストールする場合は、AWS に完全な管理者アクセス権を持つユーザ (たとえば、権限ポリシー ARN **arn:aws:iam::aws:policy/AdministratorAccess**が、直接、ロール ポリシーにより、またはユーザ グループにより接続されているユーザ) によってインストールすることを推奨します。ただし、使用可能な AWS 管理者アクセス権がない場合は、Cloud APIC をインストールするユーザに最低限の権限セットが必要です。これらの AWS IAM ロールと権限の詳細については、AWS の IAM ロールと権限 を参照してください。
- AWS 組織を使用してさまざまなアカウントのアクセス ポリシーと権限を制御し、Cloud APIC を使用して様々なアカウントを行う場合は、これらの手順で Cloud APIC を展開する AWS アカウント (Cloud APICインフラ テナント) が、その AWS 組織のマスター アカウントであることを確認します。Cloud APIC が AWS 組織のマスターアカウントに展開されている場合は、 Cloud APIC GUI を使用して、組織の一部である任意の AWS アカウントをテナントとして追加できます。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および共有テナントの設定を参照してください。

- AWS GovCloudに展開する場合は、「AWS GovCloudサポート」のセクションに記載されている情報を参照して、それらの展開に固有の情報を確認してください。Cloud APICExtending the Cisco ACI Fabric to the Public Cloud

---

ステップ 1 まだログインしていない場合は、Cloud APIC インフラテナントの Amazon Web Services アカウントにログインし、AWS 管理コンソールに移動します。

https://signin.aws.amazon.com/

https://console.aws.amazon.com/

ステップ 2 [AWS 管理コンソール (AWS Management Console)] 画面の右上隅で、リージョンが表示されている領域を見つけ、Cloud APIC で管理する AWS のリージョン (Cloud APIC AMI イメージが起動するリージョン) を選択します。

ステップ 3 Amazon EC2 SSH キーペアを作成します。

a) 画面の左上の領域にある **[サービス (Services)]** リンクをクリックし、**[EC2]** リンクをクリックします。

[EC2 ダッシュボード (EC2 Dashboard)] 画面が表示されます。

b) **[EC2 ダッシュボード (EC2 Dashboard)]** 画面で、**[キー ペア (Key Pair)]** リンクをクリックします。

[キー ペアの作成 (Create Key Pair)] 画面が表示されます。

c) **[キー ペアの作成 (Create Key Pair)]** をクリックします。

d) このキーペアの一意の名前 (たとえば、`CloudAPICKeyPair`ペア) を入力し、**[作成 (Create)]** をクリックします。

AWSに保存されている公開キーを示す画面が表示されます。さらに、プライバシー強化メール(PEM)ファイルが、秘密キーとともにシステムにローカルにダウンロードされます。

e) 秘密キー PEM ファイルをシステム上の安全な場所に移動し、場所をメモします。

これらの手順の後の部分で、この場所に置かれた秘密キー PEM ファイルに戻ります。

ステップ 4 AWS Marketplace の Cloud APIC ページに移動します。

http://cs.co/capic-aws

ステップ 5 **[登録 (Subscribe)]** をクリックします。

ステップ 6 エンドユーザ ライセンス契約（EULA）を確認して、**[契約に同意 (Accept Terms)]** ボタンをクリックして同意します。

ステップ 7 1分後に、[サブスクリプションが処理されます (`Subscription shoulde be processed`) というメッセージが表示されます。**[設定を続行 (Continue to Configuration)]** ボタンをクリックします。

[このソフトウェアを設定 (Configure this software)] ページが表示されます。

ステップ 8 以下のパラメータを選択します。

- **[履行オプション (Fulfillment Option):]**Cisco Cloud APIC クラウド形成テンプレート (デフォルトで選択)

- ソフトウェアバージョン：クラウドAPICソフトウェアの適切なバージョンを選択します。
- **[リージョン (Region):]** クラウド APIC が展開されるリージョン

ステップ 9 **[続行して起動 (Continue to Launch)]** ボタンをクリックします。

[**このソフトウェアの起動 (Launch this software**)] ページが表示され、設定の概要が表示され、クラウド形成テンプレートを起動できます。

ステップ 10 **[起動 (Launch)]** をクリックして、正しい Amazon S3 テンプレート URL がすでに入力されている状態で、正しいリージョンの CloudFormation サービスに直接移動します。

ステップ 11 画面の下部にある**[次へ（Next）]** をクリックします。

[詳細の指定 (Specify Details)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

ステップ 12 **[詳細の指定 (Specify Details)]** ページに、以下の情報を入力します。

- **[スタック名 (Stack name):]** この Cloud APIC 設定の名前を入力します。
- **[ファブリック名 (Fabric name):]**デフォルト値のままにしておくか、ファブリック名を入力します。このエントリは、この Cloud APIC の名前になります。
- **[インフラ VPC プール(Infra VPC Pool):]**VPC (仮想プライベートクラウド) CIDR です。このフィールドには、デフォルト値の 10.10.0.0/24 が、CFT から自動的に入力されます。デフォルト値がオンプレミス ファブリックからのインフラ プールと重複している場合は、このフィールドの値を変更します。このエントリは /24 サブネットである必要があります。
- **[可用性ゾーン (Availability Zone):]**スクロールダウン メニューから、 Cloud APICサブネットのアベイラビリティ ゾーンを選択します。

  表示されるアベイラビリティ ゾーンのオプションは、ステップ 2 （2 ページ） で選択したリージョンに基づいています。アベイラビリティ ゾーンをリストから選択します。アベイラビリティ ゾーンのオプションとして `west-1a` と `us-west-1b` と表示されている場合は、たとえば、`us-west-1a` を選択します。
- **[パスワード/パスワードの確認 (Password/Confirm Password):]** 管理者パスワードを入力し、確認入力します。このエントリは、 SSH アクセスを有効にした後に Cloud APICにログインするために使用するパスワードです。
- **[SSH キーペア (SSH Key Pair):]** ステップ 3 （2 ページ） で作成した SSH キーペアの名前を選択します。

  Cloud APIC には、この SSH キーペアを使用してログインします。
- **[アクセス制御 (Access Control):]** Cloud APIC への接続を許可する外部ネットワークの IP アドレスとサブネットを入力します(たとえば、192.0.2.0/24)。このサブネットからの IP アドレスだけが、Cloud APIC への接続を許可されます。値 `0.0.0.0/0` を入力すると、誰でも Cloud APIC への接続が許可されます。
- その他のパラメータ：パブリックIPアドレスの割り当て：パブリックIPアドレスをアウトオブバンド（OOB）管理インターフェイスに割り当てるかどうかを選択します。Cloud APIC

リリース5.2（1）よりも前は、の管理インターフェイスにパブリックIPアドレスとプライベートIPアドレスが割り当てられていました。Cloud APICリリース5.2（1）以降、プライベートIPアドレスはの管理インターフェイスに割り当てられ、パブリックIPアドレスの割り当てはオプションです。Cloud APIC詳細については、『Cisco Cloud APIC for AWS User Guide、Release 5.2（1）』の「Private IP Address Support for Cisco Cloud APIC and Cisco Cloud Services Router」を参照してください。

- true：パブリックIPアドレスをのアウトオブバンド（OOB）管理インターフェイスに割り当てます。Cloud APIC
- false：パブリックIPアドレスを無効にし、プライベートIPアドレスをのアウトオブバンド（OOB）管理インターフェイスに割り当てます。Cloud APIC

ステップ 13 画面の下部にある **[次へ（Next）]** をクリックします。

[オプション (Option)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

ステップ 14 **[オプション (Options)]** 画面で、すべてのデフォルト値を受け入れます。

このページには、**[権限: IAM ロール (Permissions : IAM Role)]** 領域があります。IAM ロールは、Amazon Web Services にサービス リクエストを行うための一連の権限を定義する IAM エンティティです。ロールを使用しれば、通常は Amazon Web Services リソースにアクセスできないユーザ、アプリケーション、またはサービスに、アクセスを委任することができます。

Cloud APIC に関しては IAM ロール情報は必要ありませんが、別の理由で IAM ロールを割り当てる場合は、**[IAM ロール (IAM role)]** フィールドで適切なロールを選択します。

ステップ 15 **[次へ（Next）]** をクリックします (画面の下部にある **[オプション (Options)]**画面)。

[レビュー (Review)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

ステップ 16 **[レビュー (Review)]** ページのすべての情報が正しいことを確認します。

[レビュー (Review)] ページにエラーが表示された場合は、**[前へ (Previous)]** ボタンをクリックして、誤った情報を含むページに戻ります。

ステップ 17 **[レビュー (Review)]** ページのすべての情報が正しいことを確認したら、 **[AWS CloudFormation が IAM リソースをカスタム名で作成することを認める (I acknowledge that AWS CloudFormation might create IAM resources with custom names)]** の隣にあるボックスをオンにします。

ステップ 18 ページ下部にある **[作成 (Create)]** ボタンをクリックします。

[Cloudformation] ページが再び表示され、Cloud APIC作成したテンプレートが [ステータス (Status)] 列に **CREATE_IN_PROGRESS** というテキストとともに表示されます。

システムは、テンプレートに指定された情報を使用して Cisco Cloud APIC インスタンスを作成するようになりました。プロセスが完了するのに 5 ～ 10 分かかります。作成プロセスの進行状況をモニタするには、Cisco Cloud APIC テンプレートの名前の横にあるボックスをオンにし、[イベント (Events)] タブをクリックします。[イベント (Events)] タブの下の [ステータス (Status)] 列には、**CREATE_IN_PROGRESS** というテキストが表示されます。

ステップ 19 **CREATE_COMPLETE**メッセージが表示されたら、続行する前にインスタンスの準備が整っていることを確認します。

a) 画面の上部にある **[サービス (Services)]** リンクをクリックし、**[EC2]** リンクをクリックします。

[EC2 ダッシュボード (EC2 Dashboard)] 画面が表示されます。

b) [EC2 ダッシュボード (EC2 Dashboard)] 画面の **[リソース (Resources)]** 領域には、実行中のインスタンスの数を示すテキストが表示されます (たとえば、**[1 つの実行インスタンス (1 Running Instances)]**)。この実行中のインスタンスのリンクをクリックします。

[インスタンス (Instances)] 画面が表示されます。

c) 続行する前に、そのインスタンスの準備ができるまで待ちます。

[スタータス チェック (Status Checks)] の下で、新しいインスタンスが **[初期化 (Initializing)]** ステージを経過するのを確認できます。続行する前に、[スタータス チェック (Status Checks)]の下で、**[2/2 のチェックをパス (Check Passed)]** というメッセージが表示されるまで待ちます。

次のタスク

ユーザ テナントの AWS アカウントのセットアップ （5 ページ） に移動して、ユーザ テナントの AWS アカウントをセットアップします。

ユーザ テナントの AWS アカウントのセットアップ

次のいずれかの方法を使用して、ユーザ テナントの AWS アカウントを設定できます。

- CFT を使用して、Cloud APIC のユーザテナントが信頼されている場所。「CFT を使用した、信頼済みユーザ テナントのための AWS アカウントのセットアップ （5 ページ）」を参照してください。
- ここでは、AWS アクセス キー ID とシークレットアクセスキーを使用して、Cloud APIC のユーザテナントが信頼されていません。「AWS アクセス キー ID とシークレット アクセス キーを使用して、信頼されていないユーザ テナントの AWS アカウントをセットアップする （8 ページ）」を参照してください。
- ここでは、Cloud APIC を使用して AWS 組織アカウントのポリシーを管理できます。「組織のユーザ テナントの AWS アカウントのセットアップ （9 ページ）」を参照してください。

CFT を使用した、信頼済みユーザ テナントのための AWS アカウントのセットアップ

テナント アカウントでテナント ロール クラウド形成テンプレート (CFT) を使用すると、Cloud APIC が展開されるテナントとアカウントの間に信頼関係が確立されます。

テナントロール CFT を使用してユーザテナントの AWS アカウントをセットアップするには、次の手順を使用します。

始める前に

Cloud APIC ユーザ テナントを構成するためのルールと制限は次のとおりです。

- インフラ テナントとユーザ テナントに同じ AWS アカウントを使用することはできません。
- ユーザ テナントごとに 1 つの AWS アカウントが必要です。

ステップ 1 ユーザ テナントの Amazon Web Services アカウントにログインします。

https://signin.aws.amazon.com/

（注） ユーザ テナントのインフラ テナント アカウントを使用することはできません。

ステップ 2 画面の上部にある **[サービス (Services)]** リンクをクリックし、**[CloudFormation]** リンクをクリックします。

[CloudFormation] 画面が表示されます。

ステップ 3 **[スタックの作成（Create Stack）]** ボタンをクリックします。

（注） **[スタックの作成 (Create Stack)]** ボタンの横にあるドロップダウン リストからオプションを選択しないでください。代わりに、**[スタックの作成（Create Stack）]** ボタンを直接クリックします。

[テンプレートの選択 (Select Template)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

ステップ 4 ユーザ テナント設定の IAM ロールに使用するテンプレートをどのように選択するかを決定します。

- AWS アカウントからテナント ロール CFT をダウンロードする場合、または cisco.com アカウント (以前の CCO) からダウンロードした場合は、次の手順を実行します。

  1. AWS アカウントからテナント ロール CFT をダウンロードする場合は、テナント ロール CFT を見つけます。テナントロール CFT は、Cisco Cloud APIC インフラ テナントの AWS アカウントの S3 バケットにあります。S3 バケットの名前は「capic-common-[capicAccountId]-data」で、テナント ロールの CFT オブジェクトはそのバケット内の tenant-cft.json です。CapicAccountId は、Cisco Cloud APIC インフラ テナントの AWS アカウント番号です。これは、クラウド APIC が展開されているアカウントです。
  2. テナント ロール CFT をコンピュータ上の場所にダウンロードします。

     セキュリティ上の理由から、AWS でのこの S3 バケットへのパブリック アクセスは許可されていないため、このファイルをダウンロードしてテナントアカウントで使用する必要があります。
  3. AWS で、**[テンプレートの選択 (Choose a template)]** 領域で、**[テンプレートを Amazon S3 にアップロード (Upload a Template to Amazon S3)]**] の横にある円をクリックし、**[ファイルの選択 (Choose File)]** ボタンをクリックします。
  4. Cisco から受け取った JSON 形式のテナント ロール CFT (たとえば、 `tenant-cft.json`) を保存したコンピュータ上の場所に移動し、そのテンプレートファイルを選択します。

- Cisco からのテナント ロール CFT URL を指定した場合は、**[テンプレートの選択 (Choose a template)]** 領域で、**Amazon S3 テンプレートの URL を指定 (Specify an Amazon S3 template URL)]** の横にある円をクリックし、Cisco から受け取ったテナント ロールの CFT URL をテキストの下のフィールドに入力します。

ステップ 5 画面の下部にある**[次へ（Next）]** をクリックします。

[詳細の指定 (Specify Details)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

ステップ 6 **[詳細の指定 (Specify Details)]** ページに、以下の情報を入力します。

- **[スタック名 (Stack name):]** ユーザ テナント設定のためのこの IAM ロールの名前を入力します (たとえば `IAM-Role`) 。
- **[infraAccountId:]**このフィールドが表示された場合は、AWS で Cloud APIC を導入する （1 ページ）の説明に従って、インフラ テナントの AWS アカウントを入力します。

  このフィールドは、cisco.com アカウントからテナント ロール CFT をダウンロードして使用した場合に表示されることに注意してください。AWS アカウントからテナント ロール CFT をダウンロードして使用した場合は表示されません。これは、インフラ AWS アカウントの S3 バケットからダウンロードした場合には、この infraAccountID 情報が CFT にあらかじめ入力されているためです。

ステップ 7 画面の下部にある **[次へ（Next）]** をクリックします。

[オプション (Option)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

ステップ 8 適切であれば、**[オプション (Options)]** 画面ですべてのデフォルト値を受け入れ、画面の下部にある **[次へ (Next)]** をクリックします。

[レビュー (Review)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

ステップ 9 **[レビュー (Review)]** ページで、 **[AWS cloudformation がカスタムの名前を持つ IAM リソースを作成することを認める (I acknowledge that AWS CloudFormation might create IAM resources with custom names)]** の横にあるボックスをオンにし、ページの下部にある **[作成 (create)]** ボタンをクリックします。

[Cloudformation] ページが再び表示され、作成したテンプレートが [ステータス (Status)] 列に **CREATE_IN_PROGRESS** というテキストとともに表示されます。

システムは、テンプレートに指定された情報を使用して、ユーザテナントのIAMロールを作成するようになりました。プロセスが完了するのに 5 ～ 10 分かかります。作成プロセスの進行状況をモニタするには、テンプレートの名前の横にあるボックスをオンにし、[イベント (Events)] タブをクリックします。[イベント (Events)] タブの下の [ステータス (Status)] 列には、**CREATE_IN_PROGRESS** というテキストが表示されます。

CREATE_COMPLETEは、プロセスが完了したときに表示されます。

ステップ 10 **CREATE_COMPLETE**が表示されたら、適切な領域に移動して、ユーザテナントの IAM ロールが正常に作成されたことを確認します。

a) 画面の上部にある **[サービス (Services)]** リンクをクリックし、 **IAM**リンクをクリックします。
b) **[ロール (Roles)]**をクリックします。

Apictenantroleという名前のエントリがロール名の下に表示されます。

次のタスク

セットアップ ウィザードを使用した Cisco Cloud APIC の設定 に移動して、Cisco Cloud APIC のセットアップを続行します。

AWS アクセス キー ID とシークレット アクセス キーを使用して、信頼されていないユーザ テナントの AWS アカウントをセットアップする

AWS アクセス キー ID とシークレットアクセス キーを使用して信頼できないユーザの AWS アカウントを設定する場合は、次の手順を使用します。この場合、信頼されていないユーザのテナントの AWS アカウントを手動で設定し、AWS IAM を使用して適切な権限を割り当てます。

始める前に

Cloud APIC ユーザ テナントを構成するためのルールと制限は次のとおりです。

- インフラ テナントとユーザ テナントに同じ AWS アカウントを使用することはできません。
- ユーザ テナントごとに 1 つの AWS アカウントが必要です。

ステップ 1 ユーザ テナントの Amazon Web Services アカウントにログインします。

https://signin.aws.amazon.com/

（注） ユーザ テナントのインフラ テナント アカウントを使用することはできません。

ステップ 2 AWS 管理コンソールに進みます。

https://console.aws.amazon.com/

ステップ 3 画面の一番上の **[サービス]** リンクをクリックし、**IAM** リンクをクリックします。

ステップ 4 左側のペインで、**[ユーザ]** をクリックし、[**[ユーザの追加]** ボタンをクリックします。

[ユーザの追加] ページが表示されます。

ステップ 5 **[ユーザ名]** フィールドに、`user1` などの AWS ユーザ アカウントの固有の名前を入力します。

ステップ 6 **[アクセス タイプ]** フィールドで、**プログラムによるアクセス**をオンにします。

ステップ 7 ページの下部にある **[新規 (New)]** ボタンをクリックします。

ステップ 8 **[アクセス許可の設定 (Set permissions)]** エリアで、**[既存のポリシーのアタッチ (Attach existing policies)]** を直接選択します。

画面が展開され、**フィルタ ポリシー**情報が表示されます。

ステップ 9 **[管理者アクセス (Administrator Access)]** の横にあるボックスをオンにし、ページの下部にある **[Next: Tags]** ボタンをクリックします。

ステップ 10 **[タグの追加 (Add tags)]** ページの情報をそのままにして、ページの下部にある **[確認 (Review)]** ボタンをクリックします。

ステップ 11 ページ下部にある **[ユーザの作成 (Create User)]** ボタンをクリックします。

警告が表示さる場合は、**[このユーザに権限がない]**ことを示す警告を無視します。

この時点で、アクセス キーが作成されます。

ステップ 12 この AWS アカウントのアクセス キー ID とシークレット アクセス キーの情報をメモしておきます。

- ユーザ テナントのアクセス キー ID とシークレット アクセス キー情報を、CSR とテナント情報の検索 の適切な行にコピーします。
- .csv ファイルをダウンロードするか、または **[アクセス キー ID]** フィールドと **[シークレット アクセス キー]** フィールドからファイルに情報をコピーします。

ステップ 13 ページ下部にある **[閉じる (Close)]**ボタンをクリックします。

ステップ 14 必要に応じて、このトピックの手順を追加のユーザアカウントに対して繰り返します。

次のタスク

セットアップ ウィザードを使用した Cisco Cloud APIC の設定 に移動して、Cisco Cloud APIC のセットアップを続行します。

組織のユーザ テナントの AWS アカウントのセットアップ

AWS Organizations と組織のユーザ テナントのサポート の説明に従って、リリース 4.2(3) 以降では、Cloud APIC を介して AWS 組織アカウントのポリシーを管理できるようになりました。

組織テナントの AWS アカウントを設定するには、この機能を使用するために次の設定が必要です。

- Cloud APIC は、マスターアカウントに導入する必要があります。このドキュメントでは、AWS で Cloud APIC を導入する （1 ページ）に記載されている手順を使用して Cloud APIC を AWS に展開するときに、この AWS 組織のマスターアカウントに Cloud APIC (Cloud APICインフラ テナント) を導入したことを確認します。
- このドキュメントの後半では、共有テナントの設定 で説明されている手順を使用して、Cloud APIC GUI を介してテナントに組織タグを割り当てます。