Cisco Cloud APIC のインストールの準備

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

Cisco Application Centric Infrastructure (ACI) をパブリッククラウドに拡張するには、その前に、Cisco ACI オンプレミスのデータセンターと AMAZON Web Services (AWS) の展開要件を満たす必要があります。

オンプレミス データ センターの要件

このセクションでは、（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オンプレミ スデータ センター要件を示します。Cisco Application Centric Infrastructure

- ファブリックに次のコンポーネントが取り付けられていることを確認します。Cisco ACI
  - Cisco Nexus 9000 シリーズ ACI モード スイッチ ソフトウェア リリース 14.1 以降を実行している、少なくとも 2 つの Cisco Nexus EX または FX スパイン スイッチ、または Nexus 9332C および 9364C スパイン スイッチ。
  - Cisco Nexus 9000 シリーズ ACI モード スイッチ ソフトウェア リリース 14.1 以降を実行している少なくとも 2 台の Cisco Nexus pre-EX、EX、または FX リーフ スイッチ。
  - リリース 4.1 以降および Cisco ACI Multi-Site Orchestrator（MSO）リリース 2.2(x) 以降を実行している 1 つ（APIC）。Cisco Application Policy Infrastructure Controller
- 基本設定で展開された Cisco ACI Multi-Site Orchestrator 2.2(x)。
- インターネット プロトコル セキュリティ（IPsec）を終端できるルータ。

- オンプレミスとクラウド サイト間のテナント トラフィックに十分な帯域幅があることを確認する必要があります。
- Cisco SMART Licensing アカウントと Leaf Advantage ライセンス。Cisco ACI

  オンプレミス サイト上のすべてのリーフには、リーフ ライセンスが必要です。Cisco ACI
- ファブリックに接続されているワークロード。Cisco ACI
- ファブリック（スパイン）と IP セキュリティ（IPsec）終端デバイス間で設定されるサイト間ネットワーク（ISN）。Cisco ACI

  ISN の作成については、『Cisco APIC Layer 3 Networking Configuration Guide』の「Multipod」の章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
- オンプレミス展開と AWS 展開の間にファイアウォールを展開する場合は、特定のファイアウォール ポートを許可する必要があります。これには、Cisco Cloud APIC の HTTPS アクセス、各 AWS CSR の Ipsec ポート、AWS CSR リモート管理の SSH 接続が含まれます。

  これらのファイアウォール ポートについては、このガイドで詳しく説明します。Cloud APIC 通信ポート （4 ページ）

AWS パブリック クラウドの要件

このセクションでは、パブリック クラウドに（ACI）ファブリックを拡張するための Amazon Web Services（AWS）の要件を示します。Cisco Application Centric Infrastructure

AWSアカウント

インフラ テナント用に 1 つの AWS アカウントが必要であり、ユーザ テナントごとに 1 つの AWS アカウントが必要です。

たとえば、2 つのユーザ テナントを作成する場合は、3 つの AWS アカウントが必要です。各ユーザ テナントに 1 つのアカウントと、インフラ テナントに 1 つのアカウントが必要です。ユーザ テナントは、信頼できる場合と信頼できない場合があります。詳細は、このガイドのユーザ テナントの AWS アカウントのセットアップを参照してください。

AWS リソース

AWS 展開の一部として次のリソースが必要です。

- Cisco APIC 5.0 Amazon マシン イメージ（AMI）にアクセスします。

注 AMI にアクセスするには、Amazon マーケット プレイスで Cisco Cloud APIC に登録する必要があります。

- クラウドで実行されるアプリケーションの仮想マシン（VM）として機能する Elastic Cloud Computer（EC2）の 2 つのインスタンス。
- バーチャル プライベート クラウド（VPC）、サブネット、バーチャル プライベート ゲートウェイ（VGW）、インターネット ゲートウェイ（IGW）、セキュリティ グループ、および実行予定のタスクに基づくリソース。

Cisco Cloud Services Router（CSR）

AWS マーケット プレイスから Cisco Cloud Services Router（CSR）Bring Your Own License（BYOL）に登録します。詳細については、「Cisco Cloud APIC ライセンス」を参照してください。

セットアップ時に定義した帯域幅要件に応じて、適切なサイズで CSR を展開します。Cisco Cloud APIC

ルータのスループットの値によって、展開する CSR インスタンスのサイズが決まります。スループットの値を大きくすると、より大きな VM が展開されます。CSR ライセンスは、Cisco Cloud APIC セットアップ プロセスの一部として設定したスループット設定に基づきます。コンプライアンスのために、Smart アカウントに同等以上のライセンスと AX フィーチャ セットが必要です。

次の表に、さまざまなルータ スループット設定に使用される AWS EC2 インスタンスを示します。

CSR スループット	AWS EC2 インスタンス
10 MB	c4.large
50 MB	c4.large
100 BM	c4.large
250 MB	c4.large
500 MB	c4.large
1 GB	c4.2xlarge
[2.5 GB]	c4.4xlarge
5 GB	c4.8xlarge
10 GB	c4.8xlarge

AWSアカウントに、インスタンスを展開するための許可された制限があることを確認します。アカウント インスタンスの制限は、AWS Management Console：Services EC2 Limits で確認できます。

Elastic IP アドレス

インフラ VPC が展開されているリージョンに少なくとも 9 つの Elastic IP アドレスがあることを確認します。

Cisco Cloud APIC には 1 つの Elastic IP アドレスが必要で、CSR ごとに 4 つ必要です。導入地域のアカウントに 9 つ以上の Elastic IP アドレスが許可されていることを確認します。そうでない場合は、AWS のケースを上げて Elastic IP アドレスの数を増やします。10 以上を推奨します。

（注） アドレスは、関連付け解除された Elastic IP アドレスであってはなりません。9 つの新しい Elastic IP アドレスに十分なリソースが必要です。未使用の Elastic IP アドレスがある場合は、それらを解放できます。

Cisco Cloud APIC

導入に使用される AWS インスタンスのタイプは、リリースによって異なります。Cisco Cloud APIC

- リリース 5.0(x) より前のリリースでは、Cisco Cloud APIC は M4.2xlarge インスタンスを使用して展開されます。
- リリース 5.0(x) 以降では、Cisco Cloud APIC は M5.2xlarge インスタンスを使用して展開されます。

アカウントに、このインスタンスを展開できる制限があることを確認します。AWS Management Console：Services EC2 Limitsで制限を確認できます。

また、AWS Management Console：Services EC2 NETWORK & SECURITY Elastic IPs で使用されている Elastic IP アドレスの数も確認できます。

Cloud APIC 通信ポート

Cloud APIC 環境を設定する際は、下記のポートがネットワーク通信に必要であることに注意してください。

- ACI マルチサイト オーケストレータ と間 Cloud APIC の通信用：HTTPS（TCP ポート 443 インバウンド/アウトバウンド）

  には、の開始時ににログインするために使用するものと同じ管理IPアドレスを使用します。Cloud APICCloud APICCloud APICセットアップ ウィザードを使用した Cisco Cloud APIC の設定

- AWS で導入されたオンプレミス IPsec デバイスと CSR 間の通信：標準 IPsec ポート（UDP ポート 500 および許可 IP プロトコル番号 50 および 51 のインバウンド/アウトバウンド）Cloud APIC

2 つの Amazon Web Services CSR の場合、で説明されているように、またはの手順に従ってISNデバイス設定ファイルをダウンロードした場合に提供されているように、パブリック IPsec ピアリング IP は 3 番目のネットワーク インターフェイスの Elastic IP アドレスを使用します。CSR とテナント情報の検索サイト間インフラストラクチャの設定

- AWS で Cloud APIC によって導入された CSR を接続して管理する場合は、各 CSR のパブリック IP アドレスへのポートTCP 22 インバウンド/アウトバウンドを許可します。
- ライセンス登録の場合（tools.cisco.comへ）：ポート 443（アウトバウンド）が必要です。
- DNS の場合：UDP ポート 53 アウトバウンド
- NTP の場合：UDP ポート 123 アウトバウンド
- リモート認証（LDAP、Radius、TACACS+、SAML）を使用する場合は、適切なポートを開きます。
- 認証局を使用する場合は、適切なポートを開きます。

Cisco Cloud APIC のインストール ワークフロー

このセクションでは、Cisco Cloud APIC をインストールして展開するために必要なタスクの概要について説明します。インストール タスクは、AWS マネジメント コンソール、AWS クラウド形成テンプレート、クラウド APIC セットアップ ウィザード、および（ACI）マルチサイトを使用して実行します。Cisco Application Centric Infrastructure

1. オンプレミス データ センターとパブリック クラウドのタスクを含む、すべての前提条件を満たします。

   セクション「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 （1 ページ）」を参照してください。

2. AWS クラウド形成テンプレートを使用して展開します。Cisco Cloud APIC

   このタスクには、スタックの作成、テンプレートのアップロード（またはAWSテンプレート URL の提供）、テンプレート パラメータの設定、およびテンプレートの送信が含まれます。次に、IP アドレスをキャプチャします。Cisco Cloud APIC

   また、Amazon EC2 SSH キーペアを作成し、AWS Marketplace でサブスクライブする必要があります。Cisco Cloud APIC

   セクション「AWS で Cloud APIC を導入する」を参照してください。

3. セットアップ ウィザードを使用して Cisco Cloud APIC を設定します。

   このタスクには、パブリック クラウドに接続するための Cisco Cloud ACI ファブリックへのログインと設定が含まれます。Cisco Cloud APICAWS リージョンの選択も追加します。サイト間ネットワーク（ISN）ピアリング用のボーダー ゲートウェイ プロトコル（BGP）自律システム番号（ASN）と OSPF エリア ID を指定し、外部サブネットを追加します。次に、IPsec ピア アドレスを追加します。

セクション「セットアップ ウィザードを使用した Cisco Cloud APIC の設定」を参照してください。

4. Cisco ACI マルチサイトを使用して Cisco Cloud APIC を設定します。

   このタスクには、Multi-Site GUI へのログイン、オンプレミスとクラウド サイトの追加、インフラストラクチャ ファブリック接続の設定、およびオンプレミス サイトのプロパティの設定が含まれます。Cisco ACI次に、スパイン、BGP ピアリングを設定し、オンプレミス サイトと AWS クラウド APIC サイト間の接続を有効にします。Cisco ACI

   セクション「Cisco ACI マルチサイトを介した Cisco Cloud APIC の管理」を参照してください。

5. AWS パブリック クラウドにポリシーを拡張するために使用します。Cisco Cloud APICCisco ACI

   「」および「」の項を参照してください。Cisco Cloud APIC GUI の操作Cisco Cloud APIC コンポーネントの設定