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。

（注） Cisco Nexus pre-EX リーフ スイッチはサポートされていますが、「Cisco Nexus 9372PX および 9372TX スイッチの販売終了およびサポート終了のお知らせ」で説明されているように、これらの古い pre-EX リーフ スイッチのサポート終了が発表されているため、EX または FX リーフ スイッチなどの新しい世代のリーフ スイッチを使用することをお勧めします。

- リリース 4.1 以降および Cisco Nexus Dashboard Orchestrator（NDO）リリース 2.2(x) 以降を実行している少なくとも1つのオンプレミス Cisco Application Policy Infrastructure Controller（APIC）。

- Cisco Nexus Dashboard Orchestrator 2.2(x) は基本設定で展開されています。
- 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。
- オンプレミス サイトのすべてのリーフスイッチに適切な Cisco ACI ライセンスがあることを確認します。
  - Cisco ACI オンプレミス サイトが単一サイトの場合、オンプレミス リーフスイッチには Essentials ライセンス階層（またはそれ以上）を使用します。
  - Cisco ACI オンプレミス サイトがマルチサイトの場合、オンプレミス リーフスイッチには Advantage ライセンス階層（またはそれ以上）を使用します。

（注） オンプレミスデータセンターのこれらのライセンス要件は、パブリック クラウドに展開された Cloud APIC の数とは無関係です。Cloud APIC のライセンス要件については、Cisco Cloud APIC およびオンプレミス ACI ライセンスの概要 を参照してください。

- 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 CCR の IPsec ポート、AWS CCR 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 （5 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。

CCR

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

Cisco Cloud APIC の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 CCR を展開します。

ルータのスループットの値によって、展開する CCR 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。CCR ライセンスは、Cisco Cloud APIC のセットアップ プロセスの一部として設定したスループット構成に基づきます。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。

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。AWS 管理コンソールのアカウント インスタンスの制限は、**[ザービス（Services）]** > **[EC2]** > **Limits** から確認できます。

Cisco クラウドサービスルータ 1000v

次の表に、シスコ クラウド サービス ルータ 1000v 向けのさまざまなルータ 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。

CCR 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

Cisco Catalyst 8000V

Cisco Catalyst 8000V は、ティアベース（T0/T1/T2/T3）のスループット オプションをサポートしています。次の表に、Cisco Catalyst 8000V 向けのさまざまなルータ 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。

CCR スループット	AWS EC2 インスタンス
T0（最大 15M のスループット）	c5.xlarge
T1（最大 100M のスループット）	c5.xlarge
T2（最大 1G のスループット）	c5.xlarge
T3（最大 10G のスループット）	c5.9xlarge

Tier2（T2）は、Cisco Cloud APIC でサポートされるデフォルトのスループットです。

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、CCR 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。

- Cisco Nexus Dashboard Orchestrator と Cloud APIC の間の通信用：HTTPS（TCP ポート 443 インバウンド/アウトバウンド）

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

- AWS の Cloud APIC で導入されたオンプレミス IPsec デバイスと CCR 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）

2 つの Amazon Web Services CCR の場合、CCR およびテナント情報の検索 で説明されているように、または サイト間インフラストラクチャの設定 の手順に従って ISN デバイス構成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。

- AWS で Cloud APIC によって導入された CCR を接続して管理する場合は、各 CCR 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、およびマルチサイトを使用して実行します。

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. マルチサイトを使用して Cisco Cloud APIC を構成します。

   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構成、およびオンプレミス サイトのプロパティの構成が含まれます。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「マルチサイトを通じた 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

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

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。