概要

Cisco ACI ファブリックをパブリック クラウドに拡張する

Cisco Application Centric Infrastructure （ACI）プライベート クラウドを所有しているお客様は、パブリック クラウドでワークロードの一部を実行することがあります。ただし、ワークロードをパブリック クラウドに移行するには、別のインターフェイスを操作し、接続を設定してセキュリティ ポリシーを定義するさまざまな方法を学習する必要があります。これらの課題に対処すると、運用コストが増加し、一貫性が失われる可能性があります。

Cisco Application Policy Infrastructure Controller（APIC）リリース4.1(1) 以降では、Cisco ACI を使用してマルチサイト ファブリックを Amazon Web Services（AWS）パブリック クラウドに拡張できます。

APIC リリース4.2(1) 以降では、Cisco ACI を使用して、マルチサイト ファブリックを Microsoft Azure パブリック クラウドに拡張することもできます。

Cisco Cloud APIC とは

Cisco Cloud APIC は、クラウド ベースの仮想マシン（VM）に導入できる Cisco APIC のソフトウェア コンポーネントです。Cisco Cloud APICは次の機能を提供します。

- Amazon AWSまたはMicrosoft Azureパブリッククラウドと対話するための既存のインターフェイスと同様のインターフェイスを提供します。Cisco APIC
- クラウド接続の展開と設定を自動化します。

- クラウド ルータ コントロール プレーンを設定します。
- オンプレミス Cisco ACI ファブリックとクラウドサイト間のデータ パスを設定します。
- Cisco ACI ポリシーをクラウド ネイティブ ポリシーに変換します。
- エンドポイントを検出します。

Cisco ACI Extension からパブリック クラウドへのメリットを享受するには

Cisco Cloud APIC は、パブリック クラウドへの拡張の重要な部分です。Cisco ACICisco Cloud APICは、オンプレミスのデータセンターまたはパブリック クラウドの両方またはいずれかに展開されたワークロードに対して一貫したポリシー、セキュリティ、および分析を提供します。

パブリック クラウドへの Cisco ACI 拡張は、オンプレミスのデータセンターとパブリック クラウド間の自動接続を提供し、プロビジョニングとモニタリングを容易にします。また、オンプレミスのデータセンターとパブリック クラウド間、またはクラウド サイト間でポリシーを管理、監視、およびトラブルシューティングするための単一のポイントを提供します。

Azureガバメントサポート

リリース4.2(3) 以降では、オンプレミスからクラウドへの接続（ハイブリッドクラウドおよびハイブリッドマルチクラウド）、クラウドサイトからクラウドへの接続（マルチクラウド）、およびシングルクラウドの構成（クラウドファースト）について、Azure Government をサポートしています。

Cisco Cloud APIC は次の Azure 政府リージョンをサポートします。

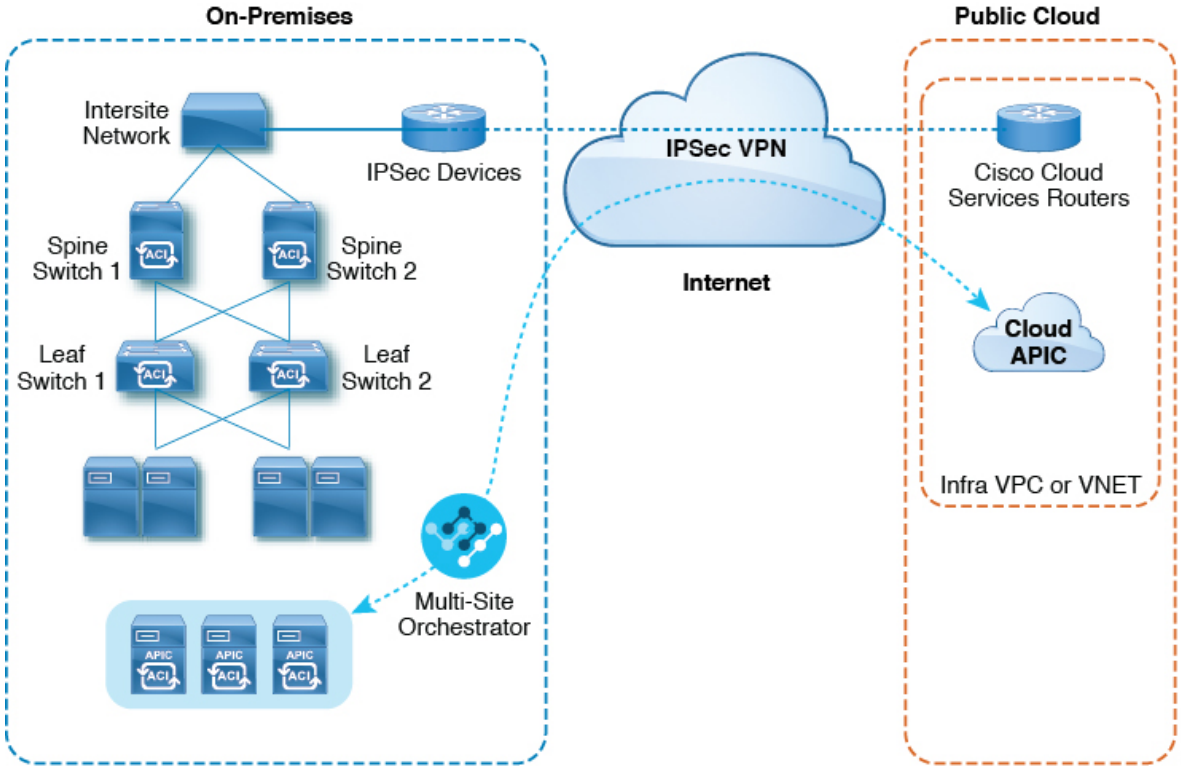
- US DoD セントラル
- US DoD 東部
- 米国政府、アリゾナ州
- 米国政府、テキサス州
- 米国政府、バージニア州

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コンポーネント

マルチサイト ファブリックを Microsoft Azure パブリック クラウドに拡張するには、それぞれに固有のロールを持つ複数のコンポーネントが必要です。

次の図は Cisco Cloud APIC のアーキテクチャの内容を示しています。

図 *1 : Cisco Cloud APIC*のアーキテクチャ



オンプレミスデータセンターコンポーネント

Cisco ACI ファブリックおよび Cisco APIC

Cisco ACI では、アプリケーション要件でネットワークを定義できます。このアーキテクチャにより、アプリケーションの導入ライフサイクル全体がシンプルになって最適化され、短時間で完了します。Cisco Application Policy Infrastructure Controller（APIC）の主要コンポーネントです。Cisco ACIこれにより、アプリケーションは、ネットワーク、コンピューティング、およびストレージ機能を含むセキュアで共有された高性能リソース プールに直接接続できます。

マルチサイト およびマルチサイト オーケストレータ/Cisco Nexus Dashboard Orchestrator

マルチサイトは、プログラムを利用してアプリケーションがネットワーク要件を定義することを可能にするアーキテクチャです。このアーキテクチャにより、アプリケーションの展開が簡素化・最適化され、そして促進されます。Cisco Cloud APIC を使用してファブリックをパブリック クラウドに拡張するには、マルチサイト をインストールする必要があります。

詳細については、Cisco.com のマルチサイトのマニュアルおよびこのガイドのマルチサイトの構成情報を参照してください。

Cisco Nexus Dashboard Orchestrator （NDO）は、複数のファブリック（サイト）で複数の Cisco Application Policy Infrastructure Controller（APIC）のインスタンスを管理します。

Cisco ACI ファブリックをパブリック クラウドに拡張すると、Cisco Nexus Dashboard Orchestrator はオンプレミスのデータセンターとパブリック クラウド間の接続を作成します。マルチサイト

を使用して、オンプレミスのデータセンターとパブリック クラウド全体にテナントを作成します。

（注） オンプレミス Cisco ACI ファブリックを設定する必要があります。ファブリック外部接続ポリシーを作成し、マルチサイトに必要なオーバーレイTEPおよびその他の情報を定義します。また、マルチサイト アーキテクチャにオンプレミス Cisco ACI ファブリックを追加する必要があります。Cisco.com で『*Cisco ACI* マルチサイト構成ガイド』を参照してください。

詳細については、Cisco.comのマルチサイトのマニュアルおよびこのガイドのマルチサイトの構成情報を参照してください。

IP セキュリティ（IPSec）ルータ

Microsoft Azureのオンプレミスサイトとクラウドサイトの間でIPsec接続を確立するには、インターネットプロトコルセキュリティ（IPsec）対応のルータが必要です。

Azureパブリッククラウドコンポーネント

Cisco Cloud APIC

Cisco Cloud APIC は次のアクションを実行します。

- パブリッククラウド上のサイトを定義し、クラウドインフラ仮想ネットワーク（VNET）をプロビジョニングし、すべてのリージョンで CCR を管理します。
- パブリッククラウドでポリシーモデルをレンダリングし、クラウドの健全性を管理します。Cisco ACI

詳細については、『Cisco Cloud APIC Release Notes』を参照してください。

CCR

CCR は、仮想およびクラウド環境で包括的な WAN ゲートウェイとネットワークサービスを提供します。CCR により、企業はWANをプロバイダーがホストするクラウドに拡張できます。Cisco Cloud APIC ソリューションには 2 つの CCR が必要です。

Cisco Cloud APIC で使用する CCR のタイプは、リリースによって異なります。

- 25.0(3) までのリリースでは、Cisco Cloud APIC では **CSR 1000v** をクラウド サービス ルータとして使用します。このCCRの詳細については、Cisco CSR 1000v のマニュアル を参照してください。
- リリース 25.0(3) 以降、Cisco Cloud APIC では **Cisco Catalyst 8000V** をクラウド サービス ルータとして使用します。この CCR の詳細については、Cisco CSR 8000v のマニュアル を参照してください。

Microsoft Azure パブリック クラウド

Microsoft Azureは、コンピューティング、ストレージ、ネットワーク、データベースなどのオンデマンドサービスを提供するクラウドベースのプラットフォームです。Azureのサブスクラ

イバは、ワークロードを実行できる仮想コンピュータにインターネット経由でアクセスできます。

詳細については、Microsoft Azure の Web サイトのマニュアルを参照してください。

オンプレミスデータセンターとパブリッククラウド間の接続

IPsec VPN

パブリックにルーティング可能なIPアドレスを含み、Microsoft Azure接続に十分な帯域幅を持つ、IPsecルータからのVPNとのインターネット接続が必要です。

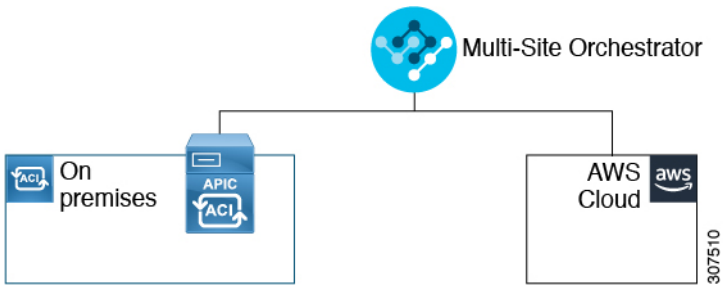
管理接続

オンプレミスのデータ センターの Nexus Dashboard Orchestrator と Microsoft Azure パブリック クラウドの Cisco Cloud APIC の間に管理接続が必要です。

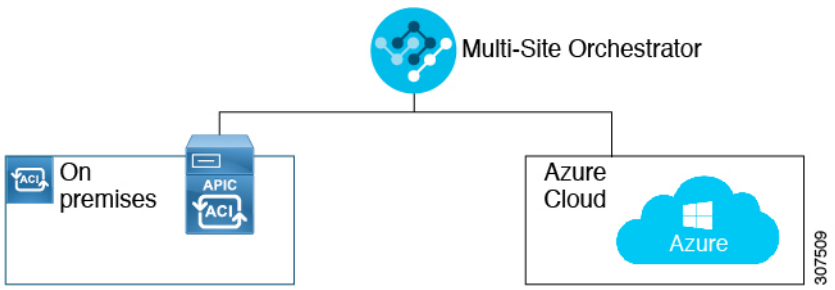
サポートされているクラウドコンピューティング プラットフォームと接続オプション

Cisco Cloud Network Controller は、次のクラウド コンピューティング プラットフォームをサポートしています。

- リリース 4.1(1) の Cisco Cloud Network Controller の初期リリースの一部として、オンプレミスからクラウドへの接続、またハイブリッド-クラウドに対するサポートが提供されており、シス コ Cisco Nexus Dashboard Orchestrator を使用してオンプレミス Cisco ACI サイトを拡張することができます。



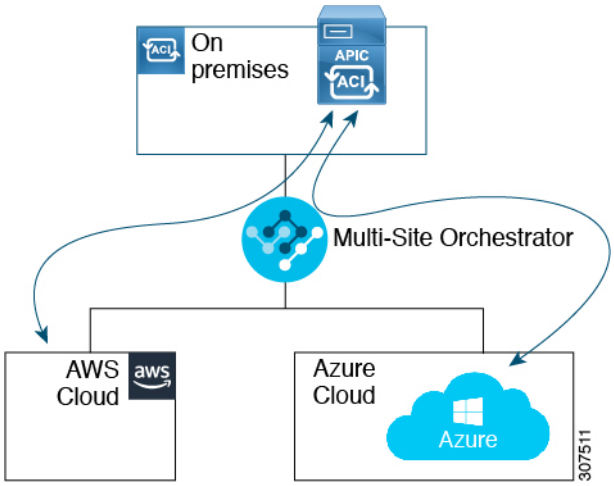
- リリース 4.2(1) 以降、Cisco Cisco Nexus Dashboard Orchestrator を使用してオンプレミス Cisco ACI サイトを Microsoft Azure パブリック クラウドに拡張できるようになりました。



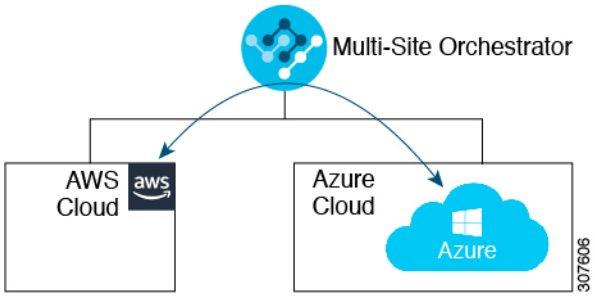
- Cisco Cisco Nexus Dashboard Orchestrator を使用してオンプレミス Cisco ACI サイトを Google Cloud パブリック クラウドに拡張するためのサポートを利用できます。

Cisco Nexus Dashboard Orchestrator を使用して、次のコンポーネント間の接続を確立することもできます。

- オンプレミスからクラウドへの接続：
  - 次のパブリッククラウドサイトの接続：
    - オンプレミス Cisco ACI および Amazon AWS パブリック クラウド サイト
    - オンプレミスおよびMicrosoft Azureパブリッククラウドサイト Cisco ACI
    - オンプレミス Cisco ACI と Google Cloud パブリック クラウド サイト
  - オンプレミスからシングルクラウドサイトへの接続（ハイブリッドクラウド）
  - オンプレミスから複数のクラウドサイトへの接続（ハイブリッドマルチクラウド）



- クラウドサイト間接続（マルチクラウド）：
  - Amazon AWSパブリッククラウドサイト間（Amazon AWSパブリッククラウドサイトからAmazon AWSパブリッククラウドサイト）
  - Microsoft Azureパブリッククラウドサイト間（Microsoft Azureパブリッククラウドサイトから Microsoft Azureパブリッククラウドサイト）
  - Google Cloud パブリック クラウド サイト間（Google Cloud パブリック クラウド サイトから Google Cloud パブリック クラウド サイトへ）
  - Amazon AWS 、Microsoft Azure、および Google Cloud パブリック クラウド サイト間



さらに、シングルクラウド設定（Cloud First）もサポートされます。

ポリシーの用語

Cisco Cloud APIC の主要な機能は、パブリック クラウドのネイティブ コンストラクトへの Cisco Application Centric Infrastructure（ACI）ポリシーの変換です。

Cisco ACI と Microsoft Azure 間のポリシー マッピング

次の表に、Microsoft Azure のポリシー用語と同等の用語を示します。Cisco ACI

Cisco ACI	Azure
テナント（リージョン、VRF）	リソース グループ
Virtual Routing and Forwarding（VRF）	仮想ネットワーク
BD サブネット	サブネット
契約、フィルタ	アウトバウンドルール、インバウンドルール
EP から EPG へのマッピング	アプリケーション セキュリティ グループ（ASG）、ネットワーク セキュリティ グループ（NSG）
エンドポイント	VM インスタンスのネットワーク アダプタ

テナント、ID、およびサブスクリプションについて

AzureにはActive Directory構造があります。最上位レベルの構造は組織であり、その下にディレクトリ（Azureテナントとも呼ばれます）があります。ディレクトリ内には、1つ以上のAzureサブスクリプションを設定できます。

特定のAzureコンポーネント間の関係は次のとおりです。

テナントサブスクリプションリソースグループリソース ＞＞＞

それぞれの説明は次のとおりです。

- 1つのテナントは複数のサブスクリプションを持つことができますが、各サブスクリプションは1つのテナントにのみ属することができます。
- 1つのサブスクリプションに複数のリソースグループを含めることができますが、各リソースグループは1つのサブスクリプションにのみ属することができます。
- 1つのリソースグループは複数のリソースを持つことができますが、各リソースは1つのサブスクリプションにのみ属することができます。

次のセクションでは、これらのコンポーネントについて詳しく説明します。

- Azure と Cisco Cloud APIC Component のマッピング （8 ページ）
- Azureサブスクリプションについて （8 ページ）
- テナントとアイデンティティについて （8 ページ）

Azure と Cisco Cloud APIC Component のマッピング

Cisco Cloud APIC, では、各 Azure リソース グループは 1 つの Cisco Cloud APIC テナントにマッピングされ、1 つの Cisco Cloud APIC テナントが複数の Azure リソース グループを持つことができます。

特定の Cisco Cloud APIC コンポーネント間の関係は次のとおりです。

テナントVRFリージョン ＞＞

Cisco Cloud APIC で VRF を作成すると、新しいリソース グループも Azure に作成されます。

Azureサブスクリプションについて

Azureサブスクリプションは、Azureクラウドサービスの支払いに使用されます。Azureサブスクリプションには、Azure Active Directory（Azure AD）との信頼関係があり、Azure ADを使用してユーザ、サービス、およびデバイスを認証します。複数のサブスクリプションは同じAzure ADを信頼できますが、各サブスクリプションは1つのAzure ADのみを信頼できます。

Azureでは、同じAzureサブスクリプションIDを複数のACIファブリックテナントに使用できます。これは、1つのAzureサブスクリプションを使用してインフラテナントを設定し、同じサブスクリプションで複数のユーザテナントを設定できることを意味します。ACIテナントはAzureサブスクリプションに関連付けられています。

テナントとアイデンティティについて

Azureおよび Cisco Cloud APIC で使用できるさまざまなタイプのテナントとアイデンティティを次に示します。

（注） リリース5.2（1）より前のリリースでは、管理対象アイデンティティのみがインフラテナントのアクセスタイプとしてサポートされ、管理対象アイデンティティとサービスプリンシパルの両方がユーザテナントのアクセスタイプとしてサポートされていました。

リリース5.2（1）以降、マネージドアイデンティティとサービスプリンシパルの両方が、インフラテナントとユーザテナントのアクセスタイプとしてサポートされるようになりました。

マネージドアイデンティティ

マネージドアイデンティティは、Azure AD認証をサポートするリソースに接続するときに使用するアプリケーションのアイデンティティを提供します。アプリケーションは管理対象IDを使用してAzure ADトークンを取得できます。たとえば、開発者が安全な方法でクレデンシャルを保存したり、ストレージアカウントにアクセスしたりするために、アプリケーションでマネージドアイデンティティを使用してAzure KeyVaultなどのリソースにアクセスできます。
https://docs.microsoft.com/en-us/azure/key-vault/general/overview

管理対象IDを使用する利点は次のとおりです。

- クレデンシャルにはアクセスできないため、クレデンシャルを管理する必要はありません。
- マネージドIDを使用して、独自のアプリケーションを含むAzure AD認証をサポートする任意のリソースを認証できます。
- マネージドIDは追加コストなしで使用できます。

Azureの管理対象アイデンティティの詳細については、以下を参照してください。

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

管理対象アイデンティティを使用して Cisco Cloud APIC でテナントを構成する場合は、Azure ポータルと Cisco Cloud APIC で次の構成を行います。

1. Azureポータルで、仮想マシンのロール割り当てを追加します。このオプションは、Azure サブスクリプションが（同じ組織の）同じAzureディレクトリにある場合に使用します。

（注） Azureサブスクリプションが異なるディレクトリにあり、マネージドIDを使用してテナントを設定する場合は、Azureコンソールに移動し、各サブスクリプションをクリックして同じAzureディレクトリの下にサブスクリプションを移動できます。これは、（異なるサブスクリプションを含む）ディレクトリが同じ親組織の子である場合にのみ実行できます。

仮想マシンのAzureにロール割り当てを追加する手順については、を参照してください。仮想マシンへのロール割り当ての追加

2. Cisco Cloud APIC では、Cisco Cloud APIC でテナントを構成するときに、**[自分自身の管理対象アイデンティティを作成する（Create Your Own Managed Identity）]** オプションを選

択します。このオプションは、テナントの設定 の手順を使用して Cisco Cloud APIC GUI で設定します。

サービス プリンシパル（Service Principal）

Azureサービスプリンシパルは、Azureリソースにアクセスするためのアプリケーション、ホステッドサービス、および自動化ツールで使用するために作成されたIDです。異なるサブスクリプションでテナントを設定する場合は、サービスプリンシパルIDを使用します。サブスクリプションが同じ組織内の異なる Azure ディレクトリ（Azure テナント）にあるか、サブスクリプションが異なる組織にある可能性があります。

サービス プリンシパルを使用して Cisco Cloud APIC でテナントを構成する場合は、Azure ポータルと Cisco Cloud APIC で次の構成を行います。

1. Azureポータルで、**アプリケーション**のロール割り当てを追加します。この場合、クラウドリソースは特定のアプリケーションを介して管理されます。

   アプリにAzureのロール割り当てを追加する手順については、を参照してください。アプリへのロール割り当ての追加

2. Cisco Cloud APIC では、Cisco Cloud APIC でテナントを構成するときに、**サービス プリンシパル** オプションを選択します。このページに入力するサブスクリプションは、同じ組織内の異なるAzureディレクトリ（Azureテナント）に配置することも、異なる組織に配置することもできます。このオプションは、テナントの設定 の手順を使用して Cisco Cloud APIC GUI で構成します。

共有テナント

Azureサブスクリプションを上記の2つの方法のいずれかにすでに関連付けており、そのサブスクリプションにさらにテナントを作成する場合は、このオプションを選択します。

Cisco Cloud APIC でテナントを**共有テナント**として構成する場合は、Azure ポータルと Cisco Cloud APICで次の構成を行います。

1. 上記の2つの方法のいずれかでAzureサブスクリプションをすでに関連付けているため、Azureで共有テナント専用の設定を行う必要はありません。共有テナントでは、既存のサブスクリプションにさらにテナントを作成します。

2. Cisco Cloud APIC では、Cisco Cloud APIC でテナントを構成するときに **[共有]** オプションを選択します。このオプションは、テナントの設定 の手順を使用して Cisco Cloud APIC GUI で構成します。

Cisco Cloud APIC ライセンシング

ここでは、Cisco Cloud Application Policy Infrastructure Controller（Cisco Cloud APIC）を使用するためのライセンス要件をリストします。

Cisco Cloud APIC と Cisco Cloud Router

（注） このセクションのライセンス情報は、リリース 25.0(3) より前のリリースで使用されていた Cisco Cloud Services Router 1000v に特に適用されます。リリース 25.0(3) 以降で使用される Cisco Catalyst 8000V のライセンス情報については、Cisco Catalyst 8000V （12 ページ） を参照してください。

シスコは、管理する仮想マシン（VM）インスタンスごとに Cisco Cloud APIC のライセンスしています。Cisco Cloud APIC バイナリ イメージは Microsoft Azure ポータルで利用可能で、Bring Your Own License（BYOL）モデルをサポートしています。

Essentials Cloud 階層には、パブリッククラウド上の単一のポリシー ドメイン用または単一の Cisco Cloud APIC インスタンス用のライセンスが含まれています。Cisco Cloud APIC の複数のインスタンスを展開する場合は、Cisco Cloud APIC が管理する VM インスタンスごとに Advantage Cloud ライセンスを購入します。

ライセンスの詳細は、『*Cisco Application Centric Infrastructure Ordering Guide*』を参照してください。

1 つ以上の Cisco Cloud APIC ライセンスを取得することに加えて、Cisco Smart Software Licensing に Cisco Cloud APIC を登録する必要があります。

シスコのスマート ライセンスは、複数のシスコ製品間でソフトウェア ライセンスを管理する統合ライセンス管理システムです。スマートソフトウェアライセンシングの詳細については、https：//www.cisco.com/go/smartlicensingを参照してください。

Cisco Cloud APIC および CCR を登録するには、次の手順を実行します。

1. 製品がインターネットにアクセスできること、またはネットワーク上にインストールされた Smart Software Manager サテライトにアクセスできることを確認してください。
2. スマートアカウントにログインします。
    1. Smart Software Manager : https://software.cisco.com/
    2. Smart Software Manager サテライト: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html
3. この製品インスタンスで使用するライセンスが含まれている仮想アカウントに移動します。
4. 製品インスタンスの登録トークン（これによりスマートアカウントを識別）を生成し、そのトークンをコピーするか、または保存します。

（注） Cisco Cloud APIC は、Cisco Cloud APIC セットアップ ウィザードの **[ルータの処理量（Throughput of the routers）]** フィールドで選択した設定に基づいて、適切なサイズの CCR を展開します。

（注） 将来のある時点で展開からCCRを削除すると（Cisco Cloud APIC GUIまたはクラウドコンソールまたはポータルを使用してCCRを削除することにより）、CCRスマートライセンスサーバがそのCCRから切断されます。削除されたCCRインスタンスは90日間は失効としてマークされ、その期間は他の新しいCCRによってライセンスを再利用できません。

この状況を回避するには、「Cisco CSR 1000v ライセンスの再ホスト」の手順を使用して、CSR 1000v ライセンスを再ホストします。

Cisco Catalyst 8000V

Cisco Catalyst 8000V は、サブスクリプション ベースのライセンスをサポートしています。

- ティアベースの Cisco Catalyst 8000V ライセンスの 1 つにサブスクライブする手順については、Cisco Catalyst 8000V Edge ソフトウェアを参照してください。
- 層に基づくさまざまなスループットの詳細については、Azure パブリック クラウドの要件を参照してください。

Cisco Cloud APICは、「Cisco DNA Advantage」サブスクリプションを利用します。「Cisco DNA Advantage」サブスクリプションでサポートされる機能については、Cisco DNA ソフトウェア SD-WAN およびルーティング マトリックスを参照してください。

オンプレミスの Cisco ACI ライセンス

1つ以上のクラウドサイトを持つ単一のオンプレミスCisco ACIサイトがある場合は、Essential、Advantage、Premierのいずれかのライセンスレベルでオンプレミス Cisco ACI ファブリックを実行できます。

Microsoft Azure

リリースに応じて、Microsoft Azure Marketplace から登録する必要があります。

- リリース 25.0(3) までのリリースでは、**Cisco Cloud Services Router（CSR）1000V-BYOL for Maximum Performance** に登録します。
- リリース 25.0(3) 以降では、 **Cisco Catalyst 8000V Edge Software - BYOL** に登録します。

Microsoft Azure Marketplaceからサブスクライブするには、の手順に従ってください。CCR のサブスクライブ

Cisco Cloud APIC 関連のマニュアル

Cisco Cloud APIC （APIC）、マルチサイト、および Microsoft Azure に関する情報は、さまざまなリソースから入手できます。

シスコのドキュメント

Cisco.com でシスコ製品のマニュアルを参照してください。

- 『Cisco Application Policy Infrastructure Controller Release Notes』

  他の Cisco Cloud APIC ドキュメントのリストが含まれています。

- Cisco Cloud APIC のドキュメント

  ビデオ、リリース ノート、基礎、インストール、設定、およびユーザ ガイドが含まれています。

- マルチサイトのドキュメント

  ビデオ、リリース ノート、インストール、設定、およびユーザ ガイドが含まれています。

- CCR のドキュメント

  リリース ノート、コマンド リファレンス、データ シート、インストール、アップグレード、および設定ガイドが含まれています。

Microsoft Azure のマニュアル

Microsoft Azure Web サイトで、ユーザ ガイド、FAQ、ケース スタディ、ホワイト ペーパーなどのドキュメントを検索できます。