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 （1 ページ）
- 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 （3 ページ）
- 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 （5 ページ）
- AWS Organizations と組織のユーザ テナントのサポート （7 ページ）
- ポリシーの用語 （9 ページ）
- Cisco Cloud APIC ライセンシング （9 ページ）
- Cisco Cloud APIC 関連のマニュアル （13 ページ）

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 プライベート クラウドを所有している（ACI）顧客は、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で作業し、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。

ただし、Cisco Application Policy Infrastructure Controller（APIC）リリース4.1(1) 以降では、Cisco ACI は Cisco Cloud APIC 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 は Cisco Cloud APIC 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）に導入できるのソフトウェア導入です。Cisco APICCisco 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
- クラウド導入の導入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 センターおよびパブリック クラウド全体でポリシーを管理、モニタリング、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。

AWS GovCloud のサポート

GovCloud のサポートは、リリースによって Cisco Cloud APIC で異なります。

- リリース 4.1(2) ー リリース5.0(1) では、Cisco Cloud APIC は us-gov-west リージョンでのみ AWS GovCloud をサポートします。us-gov-east リージョンは、これらのリリースではサポートされていません。
- リリース 5.0(1) ー リリース 5.2(1) では、Cisco Cloud APIC は us-gov-west および us-gov-east リージョンで AWS GovCloud をサポートします。ただし、CCR は us-gov-west リージョンにのみ展開できます。サイト間接続が必要な場合は、Cisco Cloud APIC を us-gov-west リージョンにのみ展開することを推奨します。
- リリース 5.2(1) では、以前と同様に、Cisco Cloud APIC は us-gov-west および us-gov-east リージョンで AWS GovCloud をサポートします。ただし、リリース 5.2(1) 以降では、us-gov-west リージョンでの展開の以前のサポートに加えて、us-gov-east リージョンでも Cisco CCR を展開できます。

AWS GovCloud に Cisco Cloud APIC を展開する場合、これらの領域には固有の設定があることに注意してください。

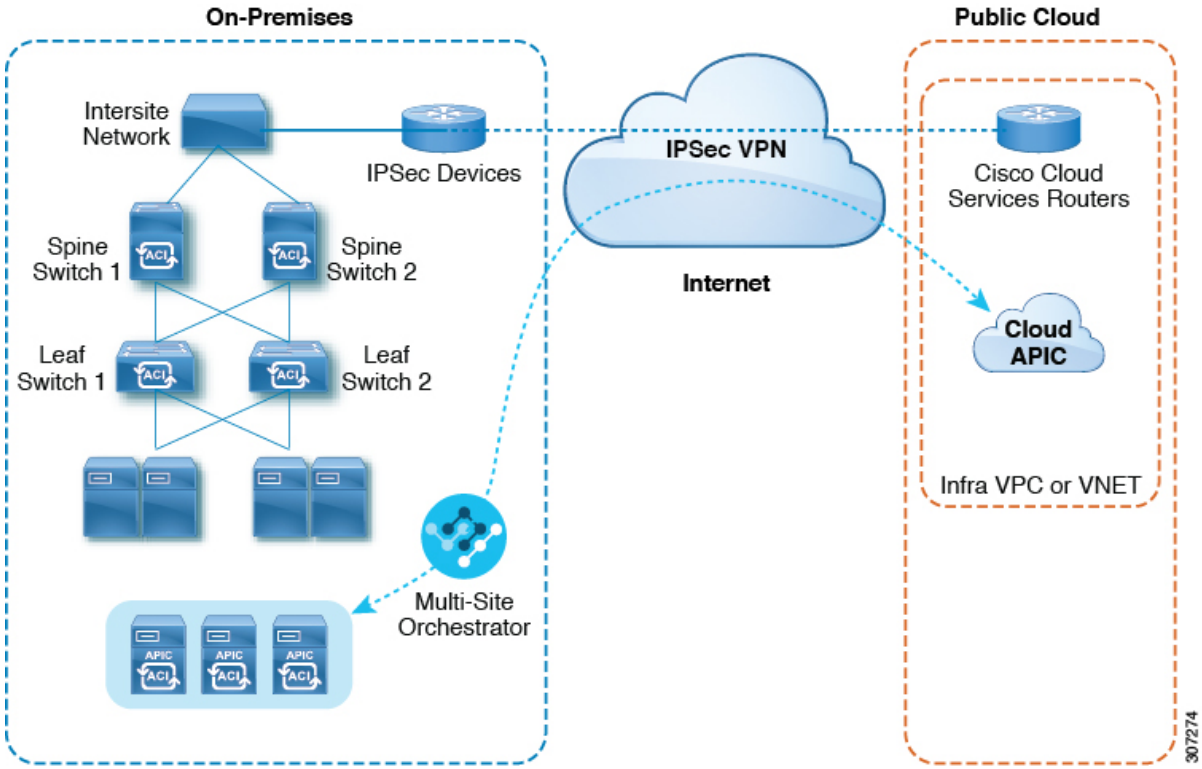
- 商用アカウントで CCR に登録します。
- 商用アカウントで Cisco Cloud APIC に登録します。
- 商用アカウントからクラウド形成テンプレートを起動し、ログインのために AWS GovCloud にリクエストをリダイレクトします。

Cisco ACI ファブリックをパブリック クラウドに拡張するためのコンポーネント

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

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

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、Multi-Site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『Multi-Siteのマニュアル』およびこのガイドの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。

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。Cisco ACIまた、マルチサイトアーキテクチャにオンプレミスファブリックを追加する必要があります。Cisco ACICisco.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『Multi-Siteのマニュアル』およびこのガイドの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。

IP セキュリティ（IPSec）ルータ

オンプレミス サイトとパブリック クラウド サイト間の 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。

AWS 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 インフラ仮想プライベート クラウド（VPC）または仮想ネットワーク（VNET）をプロビジョニングし、すべてのリージョンで Cisco クラウド ルータ（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。このガイドの AWS で Cloud APIC を導入する および セットアップ ウィザードを使用した Cisco Cloud APIC の設定 も参照してください。

Cisco Cloud ルータ

シスコ クラウド ルータ（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 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CSR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。https://www.cisco.com/c/en/us/support/routers/cloud-services-router-1000v-series/tsd-products-support-series-home.html
- 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、『CSR 8000v のマニュアル』 を参照してください。

AWS パブリック クラウド

AWS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。AWS のサブスクライバは、インターネット経由でワークロードを実行できる仮想コンピュータにアクセスできます。

詳細については、AWS 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、AWS または Microsoft Azure の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。

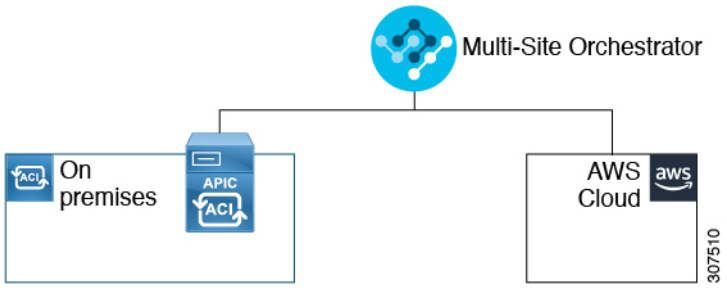
管理接続

オンプレミスのデータセンターの Nexus DashboardOrchestrator とパブリッククラウドの Cisco Cloud APIC 間の管理接続が必要です。

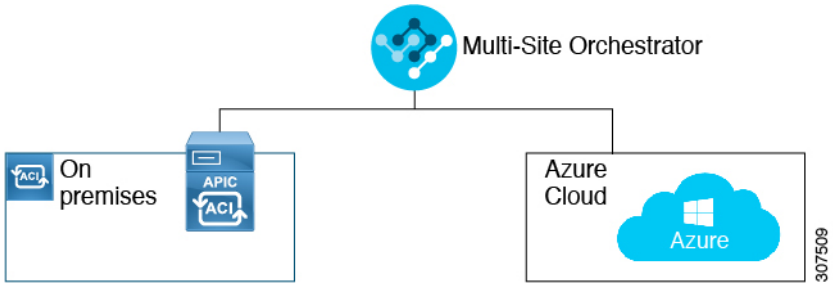
サポートされているクラウドコンピューティング プラットフォームと接続オプション

Cisco Cloud APIC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 APIC 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Amazon AWS パブリッククラウドへ拡張することができます。



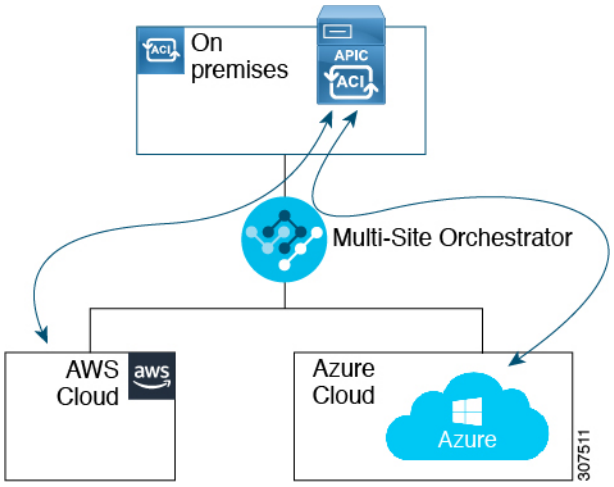
- リリース 4.2(1) 以降、Cisco Cisco Nexus Dashboard Orchestrator を使用してオンプレミス Cisco ACI サイトを Microsoft Azure パブリック クラウドに拡張できるようになりました。



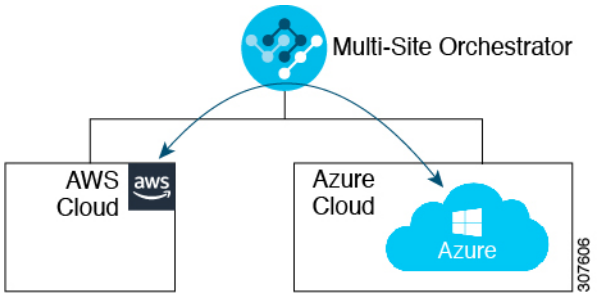
- Cisco Cisco Nexus Dashboard Orchestrator を使用してオンプレミス Cisco ACI サイトを Google Cloud パブリック クラウドに拡張するためのサポートを利用できます。

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。

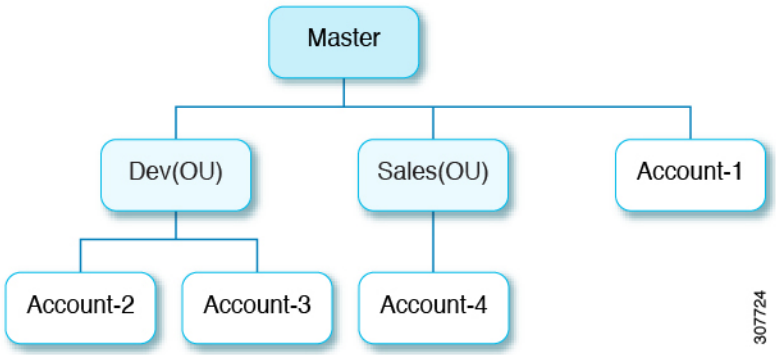
AWS Organizations と組織のユーザ テナントのサポート

組織内の複数のアカウントを使用すると、さまざまなアカウントのアクセスポリシーとアクセス許可を個別に制御するのは簡単ではありませんが、組織内の組織レベルまたは組織内のサブ組織レベルで簡単に行うことができます。

企業では、AWS Organizations を使用して、次に説明するように、組織内で複数の AWS アカウントを管理することができます。

https://aws.amazon.com/organizations/

組織内のアカウント(またはサブアカウント)のアクセスポリシーの管理は、組織内のアカウント階層のルートにある組織のマスターアカウントによって行われます。次の図は、組織におけるアカウントの設定例を示しています。



AWS アカウントが AWS Organizations の一部になる方法は 2 つあります。

- **作成**: マスターアカウント内の既存の組織内では、AWS GUI または AWS API を使用して、AWS Organizations に自動的に含まれる AWS アカウントを作成できます。
- **招待**: 組織の外部で作成されたが、組織に参加する必要があるアカウントの場合は、マスターアカウントからアカウント所有者に招待を送信する必要があります。招待状に同意すると、招待されたアカウントは組織内のサブアカウントになります。

AWS Organizations を使用して AWS アカウントを統合および管理する場合は、通常のように、AWS Organizations を使用して組織を設定し、作成されたまたは招待されたアカウントを追加します。詳細については、「組織の作成」を参照してください。

作成済みまたは招待されたアカウントを AWS を介して組織に追加したら、Cloud APIC が AWS を通じて行った AWS Organizations の構成を Cloud APIC が認識するように、必要な構成を行います。Cloud APIC は、AWS Organizations テナントのポリシーを管理するために、`OrganizationAccountAccessRole` IAM ロールを使用します。

- マスター アカウント内の既存の組織内で AWS アカウントを**作成**した場合は、その作成した AWS アカウントに組織の `OrganizationAccountAccessRole` IAM ロールが自動的に割り当てられます。この場合、AWS の`OrganizationAccountAccessRole` の IAM ロールを手動で設定する必要はありません。
- マスター アカウントが組織に参加するために既存の AWS アカウントを**招待**した場合は、AWS で`OrganizationAccountAccessRole` IAM ロールを手動で設定する必要があります。組織テナントの AWS で `OrganizationAccountAccessRole` IAM ロールを設定し、Cloud APIC に関連する権限があることを確認します。

  `OrganizationAccountAccessRole` IAM ロールは、組織またはアカウントに使用される SCP(サービス制御ポリシー)とともに、組織またはアカウントに対して、組織またはアカウントに使用する SCP(サービス制御ポリシー)とともに、組織のポリシーを管理するために Cloud APIC に必要な最小限の権限が付与されている必要があります。アクセス ポリシーの要件は、信頼できるテナントまたは信頼できないテナントの要件と同じです。

詳細については、次の URLl にある『 *Cisco Cloud APIC for AWS* ユーザ ガイド, Version 4.2 (x) 以降 』の「テナント AWS プロバイダの設定」の項を参照してください。

https://www.cisco.com/c/en/us/support/cloud-systems-management/cloud-application-policy-infrastructure-controller/products-installation-and-configuration-guides-list.html

その後、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ることができます。

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。

次の表に、Amazon Web Services（AWS）のポリシー用語と同等の用語を示します。Cisco ACI

Cisco ACI	AWS
テナント	ユーザー アカウント
AAA ユーザ、セキュリティ ドメイン	Identity and Access Management（IAM）
Virtual Routing and Forwarding（VRF）	VPC
BD サブネット	Virtual Private Cloud（VPC）のサブネット CIDR
ACI インフラ（または ACI インフラ テナント）	VPC（名前は Infra VPC）Cloud APIC
契約、フィルタ	セキュリティ グループ ルールの作成
タブー	ネットワーク アクセス リスト
EPG	セキュリティ グループ
EP から EPG へのマッピング	タグ、ラベル
エンドポイント	EC2 インスタンスのネットワーク アダプタ

Cisco Cloud APIC ライセンシング

ここでは、使用するライセンシング要件Cisco Cloud Application Policy Infrastructure Controller（APIC）を示します。

Cisco Cloud APIC および シスコ クラウド サービス ルータ 1000v

（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 （11 ページ） を参照してください。

シスコが管理する各仮想マシン（VM）インスタンスごとのシスコライセンス。Cisco Cloud APICバイナリ イメージは Amazon Web Services（AWS）マーケットプレイスで入手でき、Bring Your Own License（BYOL）モデルをサポートしています。Cisco Cloud APIC

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。の複数のインスタンスを展開する場合は、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。Cisco Cloud APICCisco Cloud APIC

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 および CCR 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 を登録するためのステップは以下のとおりです。

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 **[ルータのスループット（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。詳細については、「AWS パブリック クラウドの要件」と「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。

（注） 将来のある時点で展開から CCR を削除すると（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 サーバーがその CCR から切断されます。Cisco Cloud APIC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

リリース 25.0(4) 以降、Cisco Cloud APIC 上の Cisco Catalyst 8000V は次のライセンス モデルをサポートしています。

1. **所有ライセンス持ち込み（BYOL）**ライセンス モデル
2. **ペイアズユーゴー（PAYG）**ライセンス モデル

（注） 25.0(4) より前のリリースの場合、Cisco Cloud APIC 上の Cisco Catalyst 8000V は、**所有ライセンス持ち込み（BYOL）**ライセンス モデルのみをサポートします。

BYOL ライセンス モデル

Cisco Catalyst 8000V の BYOL ライセンス モデルでは、Cisco から Catalyst 8000V Cisco DNA ライセンスを購入し、クラウドに展開する必要があります。

- 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。
- 階層に基づくさまざまなスループットの詳細については、Cisco Cloud APIC for AWS User Guide の「About the Cisco Catalyst 8000V」の「Throughput」セクション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。

PAYGライセンス モデル

25.0(4) リリース以降、Cisco Cloud APIC は Cisco Catalyst 8000V でのペイアズユーゴー（PAYG）ライセンス モデルをサポートしています。これにより、ユーザは VM サイズに基づいてクラウドに Catalyst 8000V インスタンスを展開し、時間単位で使用料を購入できます。

スループットを得るために VM サイズに完全に依存しているため、PAYG ライセンス モデルを有効にするには、まず現在の Cisco Catalyst 8000V の展開を解除してから、新しい VM サイズでの初回セットアップを使用して再度展開します。詳細については、「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。

（注） 使用可能な 2 つのライセンス タイプを切り替える場合も、PAYG ライセンスを有効にする手順を使用できます。

（注） AWS マーケットプレイスでライセンスを使用するには、**Catalyst 8000V Cisco DNA Essentials** と **Catalyst 8000V Cisco DNA Advantage** の 2 つの PAYG オプションがあります。Cisco Cloud APIC は、**Catalyst 8000V Cisco DNA Advantage** 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 Software 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。

Cisco Cloud APIC およびオンプレミス ACI ライセンスの概要

- オンプレミス Cisco ACI サイトのすべてのリーフスイッチのライセンス要件：
  - 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。
- Cloud APIC インスタンスによって管理されるすべての VM インスタンスのライセンス要件：
  - クラウド上の Cisco ACI に Cloud APIC が 1 つしかない場合は、Cloud ACI に Essentials クラウド ライセンス層（またはそれ以上）を使用します。
  - クラウド上の Cisco ACI に Cloud APIC が 1 つ以上ある場合は、Cloud ACI に Advantage クラウド ライセンス階層（またはそれ以上）を使用します。

Amazon Web Services（AWS）

リリースに基づき、AWS Marketplace を介して 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。

- リリース 25.0(4) 以降では、 **Cisco Catalyst 8000V Edge Software - PAYG** に登録します。

Cisco Cloud APIC 関連のマニュアル

Cisco Cloud Application Policy Infrastructure Controller（APIC）、マルチサイト、および Amazon Web Services（AWS）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 Cloud APIC のドキュメント ライブラリ

  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。

- Nexus ダッシュボードのドキュメント

  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。

AWS ドキュメント

AWS 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。

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。