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 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、（APIC）リリース4.1(1) 以降では、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。Cisco Application Policy Infrastructure ControllerCisco ACICisco Cloud APICCisco ACI

APICリリース4.2(1) 以降では、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 ACICisco Cloud APICCisco ACI

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 ルーターのコントロール プレーンを設定します。
- オンプレミス 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。Cisco ACI
- エンドポイントを検出します。

Cisco ACI Extension to the Public Cloud のメリット

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 クラウドに導入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。

Cisco ACI パブリック クラウドへの拡張により、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も提供され、プロビジョニングとモニタリングが容易になります。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、Cisco Cloud Service ルータ（CSR）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 CSR 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。

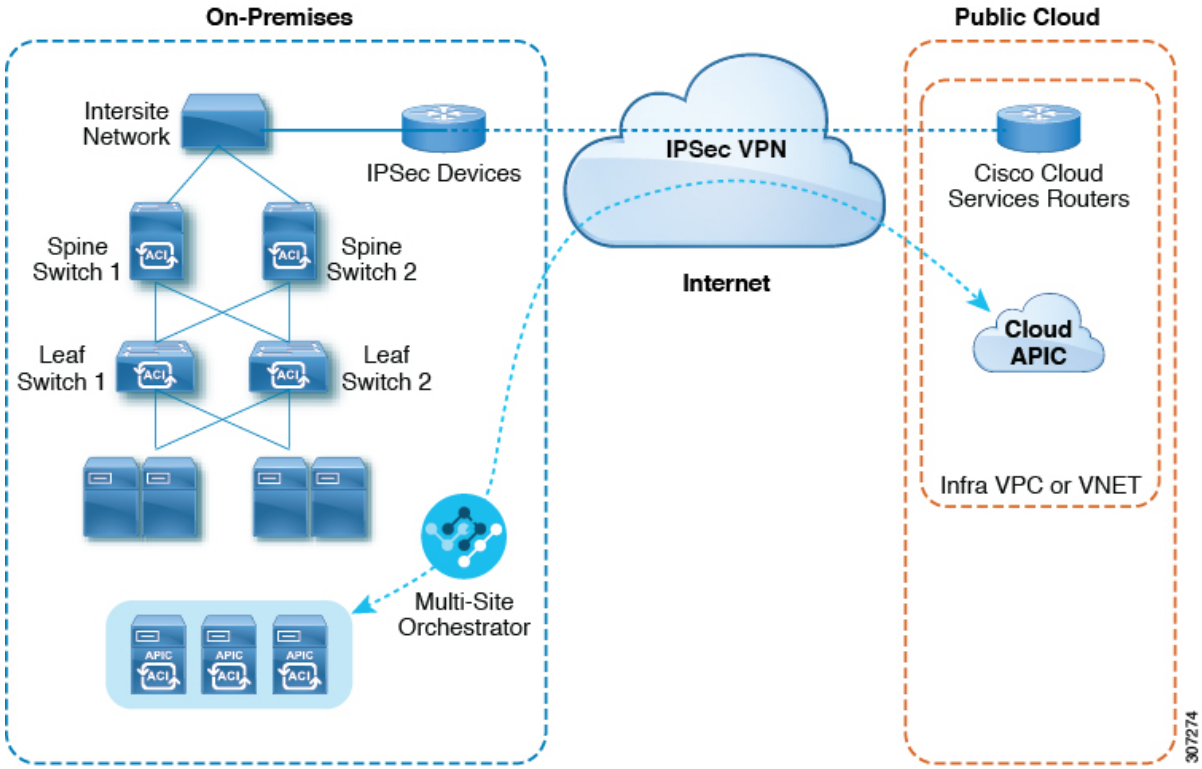
- 商用アカウントの CSR に登録します。
- 商用アカウントで Cisco Cloud APIC に登録します。
- 商用アカウントからクラウド形成テンプレートを起動し、ログインのために AWS GovCloud にリクエストをリダイレクトします。

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

（ACI）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。Cisco Application Centric Infrastructure

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

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。Cisco ACIこのアーキテクチャにより、アプリケーションの展開ライフサイクル全体が簡素化、最適化、および促進されます。（APIC）の主要コンポーネントです。Cisco Application Policy Infrastructure ControllerCisco 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、安全な共有の高パフォーマンス リソース プールと直接接続することができます。

Cisco ACI マルチサイト および Cisco ACI マルチサイト オーケストレータ

Cisco ACI 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。Cisco ACI

詳細については、Cisco.com の Cisco ACI Multi-Site のマニュアルおよびこのガイドのセクション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#ACI_Multi-SiteCisco ACI マルチサイトを介した Cisco Cloud APIC の管理

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

ファブリックをパブリック クラウドに拡張すると、Multi-Site 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。Cisco ACICisco ACI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。Cisco ACI

（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 ACIポリシーについては、『*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 Cisco ACI Multi-Site のマニュアルおよびこのガイドのセクション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#ACI_Multi-SiteCisco ACI マルチサイトを介した Cisco Cloud APIC の管理

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 クラウド 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 サービス ルータ（CSR）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。

シスコ クラウド サービス ルータ

シスコ クラウド サービス ルータ（CSR）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。CSR 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。ソリューションには 2 つの CSR が必要です。Cisco Cloud APIC

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

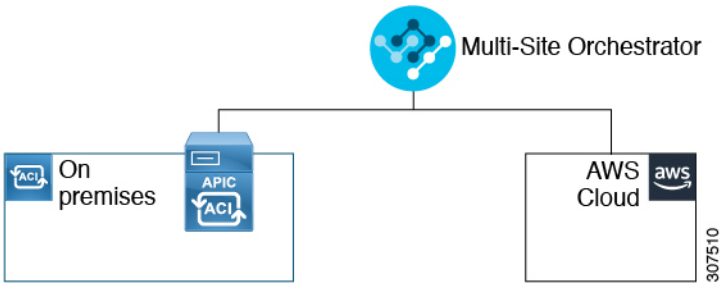
パブリックにルーティング可能な IP アドレスを含み、AWS または Microsoft Azure の接続に十分な帯域幅を持つ、IPsec ルータからの VPN とのインターネット接続が必要です。

管理接続

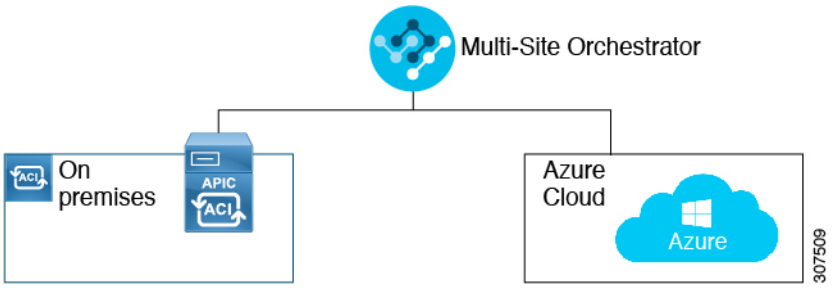
オンプレミスのデータ センターとパブリック クラウドの Multi-Site Orchestrator 間の管理接続が必要です。Cisco Cloud APIC

APIC リリース 4.2(1) での変更点

APICリリース4.1(1)の最初の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、またはシスコを使用してオンプレミスを拡張できる初期リリースのサポートが提供されました。サイトを Amazon AWS パブリック クラウドに接続します。Cisco Cloud APICACI マルチサイト オーケストレータCisco ACI

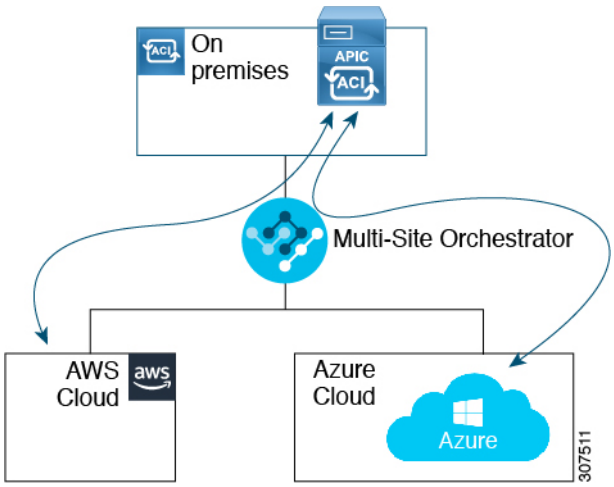


APIC リリース4.2(1) 以降、シスコを使用してオンプレミス サイトを Microsoft Azure パブリック クラウドに拡張できるようになりました。ACI マルチサイト オーケストレータCisco ACI

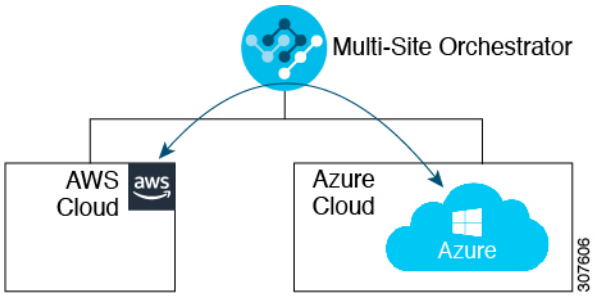


このリリースで利用可能な拡張機能により、シスコを使用して次のコンポーネント間の接続を確立することもできます。ACI マルチサイト オーケストレータ

- 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：
    - オンプレミスおよび Amazon AWS パブリック クラウド サイト（以前は APIC リリース4.1 [1]で利用可能）Cisco ACI
    - 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 サイトと Microsoft Azure 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）



さらに、シングル クラウド設定（Cloud First）もサポートされます。

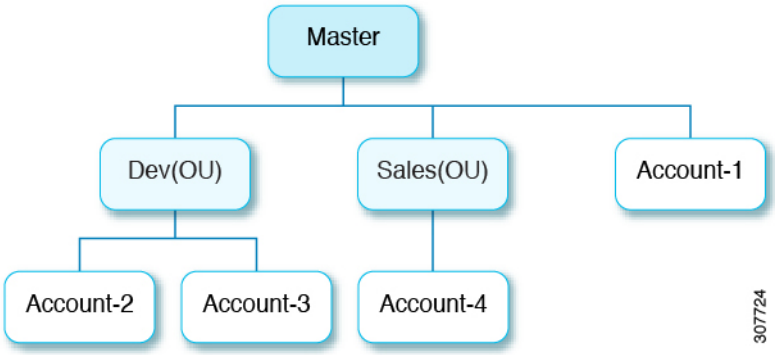
AWS Organizations と組織のユーザ テナントのサポート

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Cloud APIC行った AWS Organizations の設定を認識するように、必要な設定を行います。

- を使用して AWS Organizations アカウントのポリシーを管理するCloud APIC場合はCloud APIC 、をマスターアカウントに展開する必要があります。にCloud APICAWS で Cloud APIC を導入する記載されている手順を使用してを AWS に展開する場合はCloud APIC 、このCloud APIC AWS 組織のマスターアカウントに (インフラテナント) を導入していることを確認してください。
- 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構成要素への（ACI）ポリシーの変換です。Cisco Application Centric Infrastructure

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 アカウント
AAA ユーザ、セキュリティ ドメイン	アイデンティティとアクセス管理（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 ライセンス

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

Cisco Cloud APIC およびシスコ クラウド サービス ルータ

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 つ以上のライセンスを取得することに加えて、シスコ スマート ソフトウェア ライセンシングにとシスコ クラウド サービス ルータ（CSR）を登録する必要があります。Cisco Cloud APICCisco Cloud APIC

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 CSR 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） セットアップ ウィザードの **[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 CSR を展開します。Cisco Cloud APICCisco Cloud APIC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 CSR 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 CSR を削除することにより）、CSR スマート ライセンス サーバがその CSR から切断されます。Cisco Cloud APIC削除された CSR 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 CSR 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、次の手順に従って、新しいライセンスを古いライセンスに再ホストします。

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 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 ファブリックを実行できます。Cisco ACICisco ACI

Amazon Web Services（AWS）

AWS Marketplace から適切な CSR ライセンスに登録する必要があります。

Cisco Cloud APIC 関連のマニュアル

（APIC）、Cisco ACI Multi-Site、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。Cisco Cloud Application Policy Infrastructure Controller

シスコ マニュアル

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 Application Policy Infrastructure Controller* のリリース ノート、リリース *4.1(1)*』

  他のドキュメントのリストが含まれます。Cisco Cloud APIC

- Cisco ACI および Cisco APIC のマニュアル

  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。

- Cisco ACI マルチサイトのマニュアル

  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。

- Cisco Cloud Services Router のマニュアル

  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。