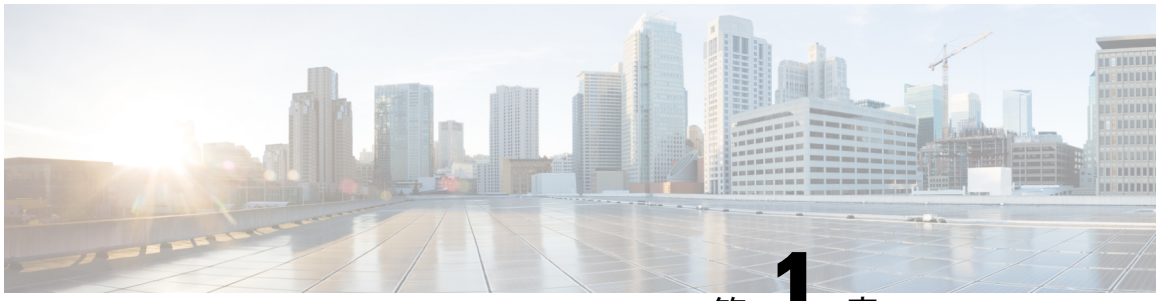
Cisco Cloud APIC AWS のインストール ガイド、リリース 5.2(x)

初版：2021 年 6 月 4 日

最終更新：2022 年 1 月 5 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

新機能および変更された機能に関する情報

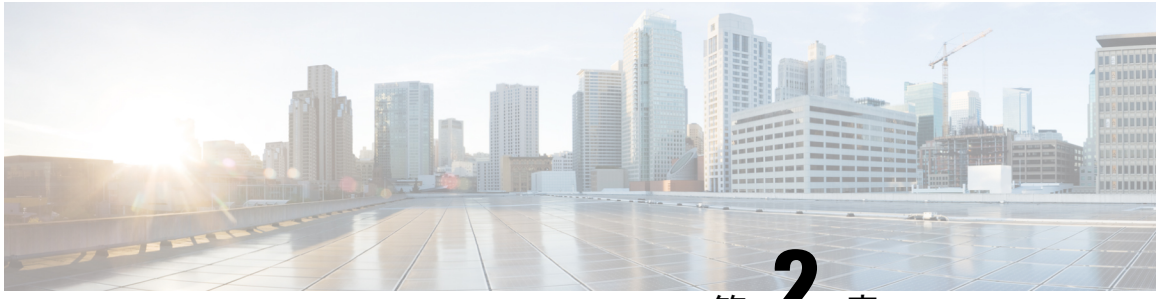
新機能および変更された機能に関する情報

次の表は、現行リリースに至るまでにガイドの編成と特徴に加えられた主な変更点の概要を示しています。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Cisco* クラウド *APIC Release 5.2(1)* の新機能と変更された動作

機能または変更	説明	参照先
Cisco Cloud Services Router （CSR）および Cisco Cloud APIC にアクセスするためのプライベート IP アドレスのサポート	リリース5.2（1）以降では、Cisco クラウドサービスルータ（CSR）にプライベート IP アドレスを割り当てることができます。Cisco Cloud APIC	
アップグレードとは無関係の CSR アップグレードのトリガーのサポートCisco Cloud APIC	リリース5.2（1）より前は、のアップグレードをトリガーするたびに CSR が自動的にアップグレードされました。Cisco Cloud APICリリース5.2（1）以降では、アップグレードに関係なく、手動で CSR のアップグレードをトリガーできます。Cisco Cloud APIC	クラウド サービス ルータのアップグレードのトリガー （81 ページ）

新機能および変更された機能に関する情報



第 2 章

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。

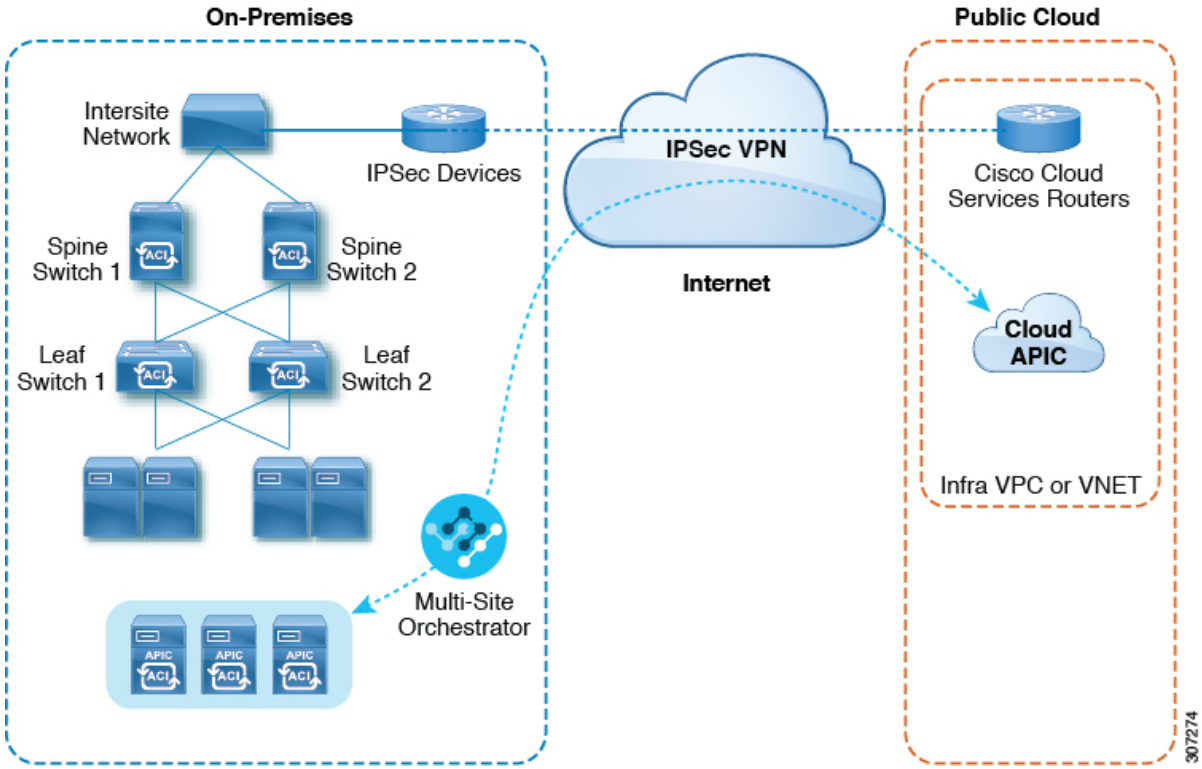
- 商用アカウントの CSR に登録します。
- 商用アカウントで Cisco Cloud APIC に登録します。
- 商用アカウントからクラウド形成テンプレートを起動し、ログインのために AWS GovCloud にリクエストをリダイレクトします。

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 （43 ページ）

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 （43 ページ）

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 （21 ページ） 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 （34 ページ） 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

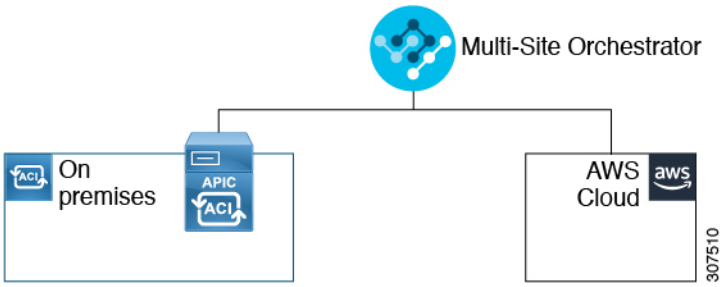
パブリックにルーティング可能な IP アドレスを含み、AWS または Microsoft Azure の接続に十分な帯域幅を持つ、IPsec ルータからの VPN とのインターネット接続が必要です。

管理接続

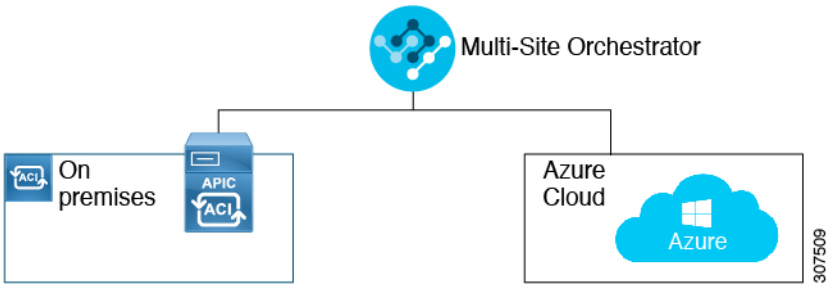
オンプレミスのデータ センターとパブリック クラウドの Multi-Site Orchestrator 間の管理接続が必要です。Cisco Cloud APIC

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

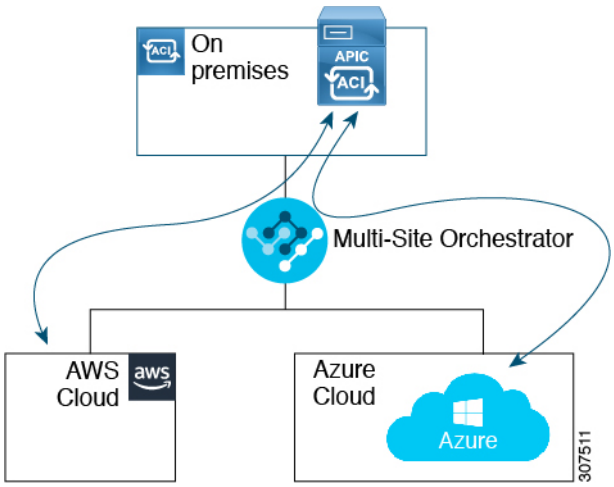


APIC リリース4.2(1) 以降、シスコを使用してオンプレミス サイトを Microsoft Azure パブリック クラウドに拡張できるようになりました。ACI マルチサイト オーケストレータCisco ACI

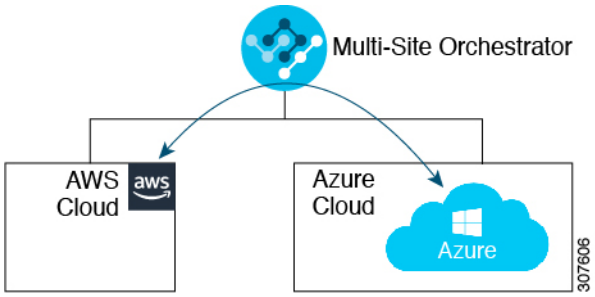


このリリースで利用可能な拡張機能により、シスコを使用して次のコンポーネント間の接続を確立することもできます。ACI マルチサイト オーケストレータ

- 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。

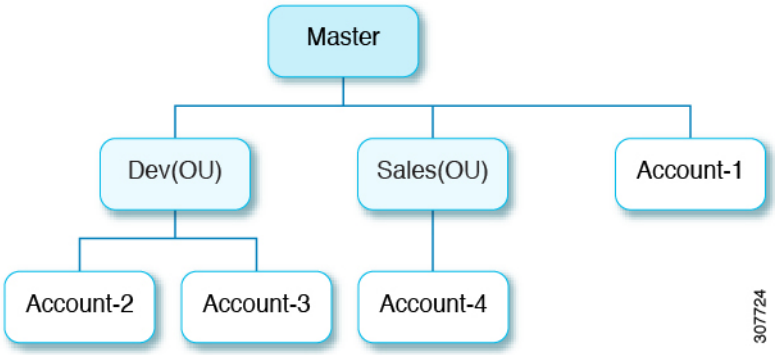
AWS Organizations と組織のユーザ テナントのサポート

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 （21 ページ）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 （50 ページ）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 （16 ページ）と セットアップ ウィザードを使用した Cisco Cloud APIC の設定 （34 ページ）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

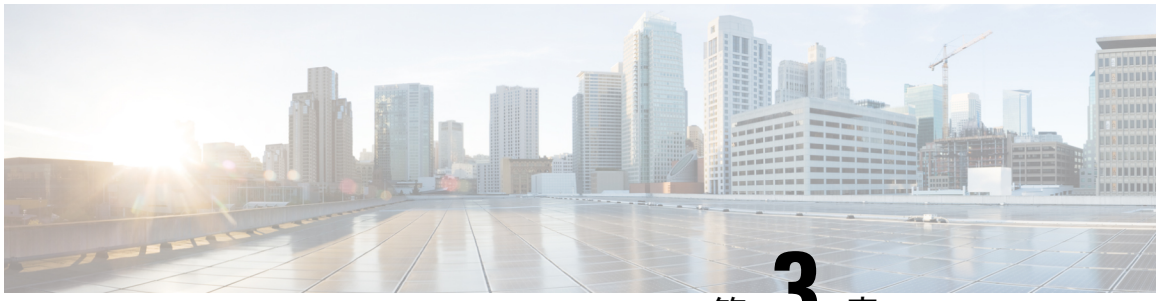
  ビデオ、リリース ノート、インストール、設定、およびユーザ ガイドが含まれています。

- 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。



第 3 章

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 （18 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 （25 ページ）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。

註 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 （11 ページ）」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 （34 ページ）

- 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 （97 ページ）サイト間インフラストラクチャの設定 （45 ページ）

- 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 （15 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 （21 ページ）」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 （34ページ）」を参照してください。

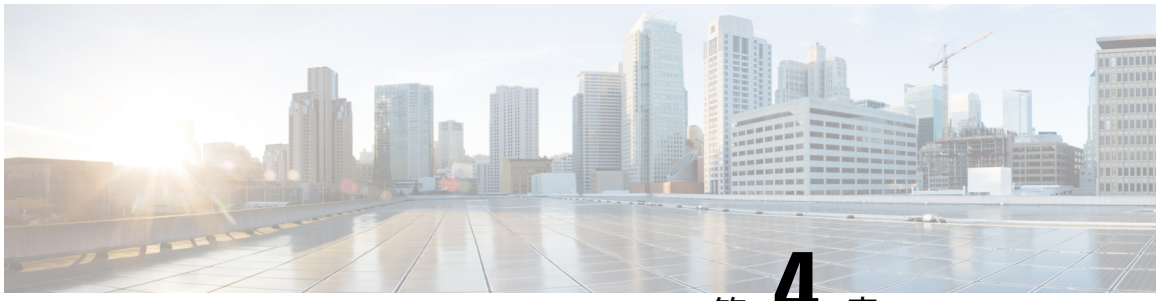
4. Cisco ACI マルチサイトを使用して Cisco Cloud APIC を設定します。

   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 （43 ページ）」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 （67 ページ）Cisco Cloud APIC コンポーネントの設定 （68 ページ）



第 4 章

Cisco Cloud APIC のクラウド形成テンプレート情報の設定

AWS で Cloud APIC を導入する

始める前に

- このセクションのタスクに進む前に、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 （15 ページ） に示されている要件を満たしていることを確認します。たとえば、エラスティック IP アドレスの数が正しいこと、およびインスタンス展開の許可の制限をチェックしたことを確認します。
- Cisco Cloud APIC のインストールと操作には、特定の AWS IAM ロールおよび権限が必要であるため、AWS で完全な管理者アクセス権を持っていることを確認します。

  CloudFormation テンプレート (CFT) を使用して Cloud APIC をインストールする場合は、AWS に完全な管理者アクセス権を持つユーザ (たとえば、権限ポリシー ARN **arn:aws:iam::aws:policy/AdministratorAccess**が、直接、ロール ポリシーにより、またはユーザ グループにより接続されているユーザ) によってインストールすることを推奨します。ただし、使用可能な AWS 管理者アクセス権がない場合は、Cloud APIC をインストールするユーザに最低限の権限セットが必要です。これらの AWS IAM ロールと権限の詳細については、AWS の IAM ロールと権限 （87 ページ） を参照してください。
- AWS 組織を使用してさまざまなアカウントのアクセス ポリシーと権限を制御し、Cloud APIC を使用して様々なアカウントを行う場合は、これらの手順で Cloud APIC を展開する AWS アカウント (Cloud APICインフラ テナント) が、その AWS 組織のマスター アカウントであることを確認します。Cloud APIC が AWS 組織のマスターアカウントに展開されている場合は、 Cloud APIC GUI を使用して、組織の一部である任意の AWS アカウントをテナントとして追加できます。詳細については、AWS Organizations と組織のユーザ テナントのサポート （9 ページ）および共有テナントの設定 （50 ページ）を参照してください。

- AWS GovCloudに展開する場合は、「AWS GovCloudサポート」のセクションに記載されている情報を参照して、それらの展開に固有の情報を確認してください。Cloud APICCisco ACI ファブリックをパブリック クラウドに拡張する （3 ページ）

ステップ 1 まだログインしていない場合は、Cloud APIC インフラテナントの Amazon Web Services アカウントにログインし、AWS 管理コンソールに移動します。

https://signin.aws.amazon.com/

https://console.aws.amazon.com/

ステップ 2 [AWS 管理コンソール (AWS Management Console)] 画面の右上隅で、リージョンが表示されている領域を見つけ、Cloud APIC で管理する AWS のリージョン (Cloud APIC AMI イメージが起動するリージョン) を選択します。

ステップ 3 Amazon EC2 SSH キーペアを作成します。

a) 画面の左上の領域にある **[サービス (Services)]** リンクをクリックし、**[EC2]** リンクをクリックします。

[EC2 ダッシュボード (EC2 Dashboard)] 画面が表示されます。

b) **[EC2 ダッシュボード (EC2 Dashboard)]** 画面で、**[キー ペア (Key Pair)]** リンクをクリックします。

[キー ペアの作成 (Create Key Pair)] 画面が表示されます。

c) **[キー ペアの作成 (Create Key Pair)]** をクリックします。

d) このキーペアの一意の名前 (たとえば、 `CloudAPICKeyPair`ペア) を入力し、**[作成 (Create)]** をクリックします。

AWSに保存されている公開キーを示す画面が表示されます。さらに、プライバシー強化メール(PEM)ファイルが、秘密キーとともにシステムにローカルにダウンロードされます。

e) 秘密キー PEM ファイルをシステム上の安全な場所に移動し、場所をメモします。

これらの手順の後の部分で、この場所に置かれた秘密キー PEM ファイルに戻ります。

ステップ 4 AWS Marketplace の Cloud APIC ページに移動します。

http://cs.co/capic-aws

ステップ 5 **[登録 (Subscribe)]** をクリックします。

ステップ 6 エンドユーザ ライセンス契約（EULA）を確認して、**[契約に同意 (Accept Terms)]** ボタンをクリックして同意します。

ステップ 7 1分後に、[サブスクリプションが処理されます `(Subscription shoulde be processed)` というメッセージが表示されます。**[設定を続行 (Continue to Configuration)]** ボタンをクリックします。

[このソフトウェアを設定 (Configure this software)] ページが表示されます。

ステップ 8 以下のパラメータを選択します。

- **[履行オプション (Fulfillment Option):]**Cisco Cloud APIC クラウド形成テンプレート (デフォルトで選択)

- ソフトウェアバージョン：クラウドAPICソフトウェアの適切なバージョンを選択します。
- **[リージョン (Region):]** クラウド APIC が展開されるリージョン

ステップ 9 **[続行して起動 (Continue to Launch)]** ボタンをクリックします。

[**このソフトウェアの起動 (Launch this software**)] ページが表示され、設定の概要が表示され、クラウド形成テンプレートを起動できます。

ステップ 10 **[起動 (Launch)]** をクリックして、正しい Amazon S3 テンプレート URL がすでに入力されている状態で、正しいリージョンの CloudFormation サービスに直接移動します。

ステップ 11 画面の下部にある**[次へ（Next）]** をクリックします。

[詳細の指定 (Specify Details)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

ステップ 12 **[詳細の指定 (Specify Details)]** ページに、以下の情報を入力します。

- **[スタック名 (Stack name):]** この Cloud APIC 設定の名前を入力します。
- **[ファブリック名 (Fabric name):]**デフォルト値のままにしておくか、ファブリック名を入力します。このエントリは、この Cloud APIC の名前になります。
- **[インフラ VPC プール(Infra VPC Pool):]**VPC (仮想プライベートクラウド) CIDR です。このフィールドには、デフォルト値の 10.10.0.0/24 が、CFT から自動的に入力されます。デフォルト値がオンプレミス ファブリックからのインフラ プールと重複している場合は、このフィールドの値を変更します。このエントリは /24 サブネットである必要があります。
- **[可用性ゾーン (Availability Zone):]**スクロールダウン メニューから、 Cloud APICサブネットのアベイラビリティ ゾーンを選択します。

  表示されるアベイラビリティ ゾーンのオプションは、ステップ 2 （22 ページ） で選択したリージョンに基づいています。アベイラビリティ ゾーンをリストから選択します。アベイラビリティ ゾーンのオプションとして `west-1a` と `us-west-1b` と表示されている場合は、たとえば、`us-west-1a` を選択します。
- **[パスワード/パスワードの確認 (Password/Confirm Password):]** 管理者パスワードを入力し、確認入力します。このエントリは、 SSH アクセスを有効にした後に Cloud APICにログインするために使用するパスワードです。
- **[SSH キーペア (SSH Key Pair):]** ステップ 3 （22 ページ） で作成した SSH キーペアの名前を選択します。

  Cloud APIC には、この SSH キーペアを使用してログインします。
- **[アクセス制御 (Access Control):]** Cloud APIC への接続を許可する外部ネットワークの IP アドレスとサブネットを入力します(たとえば、192.0.2.0/24)。このサブネットからの IP アドレスだけが、Cloud APIC への接続を許可されます。値 `0.0.0.0/0` を入力すると、誰でも Cloud APIC への接続が許可されます。
- その他のパラメータ：パブリックIPアドレスの割り当て：パブリックIPアドレスをアウトオブバンド（OOB）管理インターフェイスに割り当てるかどうかを選択します。Cloud APIC

リリース5.2（1）よりも前は、の管理インターフェイスにパブリックIPアドレスとプライベートIPアドレスが割り当てられていました。Cloud APICリリース5.2（1）以降、プライベートIPアドレスはの管理インターフェイスに割り当てられ、パブリックIPアドレスの割り当てはオプションです。Cloud APIC詳細については、『Cisco Cloud APIC for AWS User Guide、Release 5.2（1）』の「Private IP Address Support for Cisco Cloud APIC and Cisco Cloud Services Router」を参照してください。

- true：パブリックIPアドレスをのアウトオブバンド（OOB）管理インターフェイスに割り当てます。Cloud APIC
- false：パブリックIPアドレスを無効にし、プライベートIPアドレスをのアウトオブバンド（OOB）管理インターフェイスに割り当てます。Cloud APIC

ステップ 13 画面の下部にある **[次へ（Next）]** をクリックします。

[オプション (Option)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

ステップ 14 **[オプション (Options)]** 画面で、すべてのデフォルト値を受け入れます。

このページには、**[権限: IAM ロール (Permissions : IAM Role)]** 領域があります。IAM ロールは、Amazon Web Services にサービス リクエストを行うための一連の権限を定義する IAM エンティティです。ロールを使用しれば、通常は Amazon Web Services リソースにアクセスできないユーザ、アプリケーション、またはサービスに、アクセスを委任することができます。

Cloud APIC に関しては IAM ロール情報は必要ありませんが、別の理由で IAM ロールを割り当てる場合は、**[IAM ロール (IAM role)]** フィールドで適切なロールを選択します。

ステップ 15 **[次へ（Next）]** をクリックします (画面の下部にある **[オプション (Options)]**画面)。

[レビュー (Review)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

ステップ 16 **[レビュー (Review)]** ページのすべての情報が正しいことを確認します。

[レビュー (Review)] ページにエラーが表示された場合は、**[前へ (Previous)]** ボタンをクリックして、誤った情報を含むページに戻ります。

ステップ 17 **[レビュー (Review)]** ページのすべての情報が正しいことを確認したら、 **[AWS CloudFormation が IAM リソースをカスタム名で作成することを認める (I acknowledge that AWS CloudFormation might create IAM resources with custom names)]** の隣にあるボックスをオンにします。

ステップ 18 ページ下部にある **[作成 (Create)]** ボタンをクリックします。

[Cloudformation] ページが再び表示され、Cloud APIC作成したテンプレートが [ステータス (Status)] 列に **CREATE_IN_PROGRESS** というテキストとともに表示されます。

システムは、テンプレートに指定された情報を使用して Cisco Cloud APIC インスタンスを作成するようになりました。プロセスが完了するのに 5 ～ 10 分かかります。作成プロセスの進行状況をモニタするには、Cisco Cloud APIC テンプレートの名前の横にあるボックスをオンにし、[イベント (Events)] タブをクリックします。[イベント (Events)] タブの下の [ステータス (Status)] 列には、**CREATE_IN_PROGRESS** というテキストが表示されます。

ステップ 19 **CREATE_COMPLETE**メッセージが表示されたら、続行する前にインスタンスの準備が整っていることを確認します。

a) 画面の上部にある **[サービス (Services)]** リンクをクリックし、**[EC2]** リンクをクリックします。

[EC2 ダッシュボード (EC2 Dashboard)] 画面が表示されます。

b) [EC2 ダッシュボード (EC2 Dashboard)] 画面の **[リソース (Resources)]** 領域には、実行中のインスタンスの数を示すテキストが表示されます (たとえば、**[1 つの実行インスタンス (1 Running Instances)]**)。この実行中のインスタンスのリンクをクリックします。

[インスタンス (Instances)] 画面が表示されます。

c) 続行する前に、そのインスタンスの準備ができるまで待ちます。

[スタータス チェック (Status Checks)] の下で、新しいインスタンスが **[初期化 (Initializing)]** ステージを経過するのを確認できます。続行する前に、[スタータス チェック (Status Checks)]の下で、**[2/2 のチェックをパス (Check Passed)]** というメッセージが表示されるまで待ちます。

次のタスク

ユーザ テナントの AWS アカウントのセットアップ （25 ページ） に移動して、ユーザ テナントの AWS アカウントをセットアップします。

ユーザ テナントの AWS アカウントのセットアップ

次のいずれかの方法を使用して、ユーザ テナントの AWS アカウントを設定できます。

- CFT を使用して、Cloud APIC のユーザテナントが信頼されている場所。「CFT を使用した、信頼済みユーザ テナントのための AWS アカウントのセットアップ （25 ページ）」を参照してください。
- ここでは、AWS アクセス キー ID とシークレットアクセスキーを使用して、Cloud APIC のユーザテナントが信頼されていません。「AWS アクセス キー ID とシークレット アクセス キーを使用して、信頼されていないユーザ テナントの AWS アカウントをセットアップする （28 ページ）」を参照してください。
- ここでは、Cloud APIC を使用して AWS 組織アカウントのポリシーを管理できます。「組織のユーザ テナントの AWS アカウントのセットアップ （29 ページ）」を参照してください。

CFT を使用した、信頼済みユーザ テナントのための AWS アカウントのセットアップ

テナント アカウントでテナント ロール クラウド形成テンプレート (CFT) を使用すると、Cloud APIC が展開されるテナントとアカウントの間に信頼関係が確立されます。

テナントロール CFT を使用してユーザテナントの AWS アカウントをセットアップするには、次の手順を使用します。

始める前に

Cloud APIC ユーザ テナントを構成するためのルールと制限は次のとおりです。

- インフラ テナントとユーザ テナントに同じ AWS アカウントを使用することはできません。
- ユーザ テナントごとに 1 つの AWS アカウントが必要です。

ステップ 1 ユーザ テナントの Amazon Web Services アカウントにログインします。

https://signin.aws.amazon.com/

（注） ユーザ テナントのインフラ テナント アカウントを使用することはできません。

ステップ 2 画面の上部にある **[サービス (Services)]** リンクをクリックし、**[CloudFormation]** リンクをクリックします。

[CloudFormation] 画面が表示されます。

ステップ 3 **[スタックの作成（Create Stack）]** ボタンをクリックします。

（注） **[スタックの作成 (Create Stack)]** ボタンの横にあるドロップダウン リストからオプションを選択しないでください。代わりに、**[スタックの作成（Create Stack）]** ボタンを直接クリックします。

[テンプレートの選択 (Select Template)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

ステップ 4 ユーザ テナント設定の IAM ロールに使用するテンプレートをどのように選択するかを決定します。

- AWS アカウントからテナント ロール CFT をダウンロードする場合、または cisco.com アカウント (以前の CCO) からダウンロードした場合は、次の手順を実行します。

  1. AWS アカウントからテナント ロール CFT をダウンロードする場合は、テナント ロール CFT を見つけます。テナントロール CFT は、Cisco Cloud APIC インフラ テナントの AWS アカウントの S3 バケットにあります。S3 バケットの名前は「capic-common-[capicAccountId]-data」で、テナント ロールの CFT オブジェクトはそのバケット内の tenant-cft.json です。CapicAccountId は、Cisco Cloud APIC インフラ テナントの AWS アカウント番号です。これは、クラウド APIC が展開されているアカウントです。
  2. テナント ロール CFT をコンピュータ上の場所にダウンロードします。

     セキュリティ上の理由から、AWS でのこの S3 バケットへのパブリック アクセスは許可されていないため、このファイルをダウンロードしてテナントアカウントで使用する必要があります。
  3. AWS で、**[テンプレートの選択 (Choose a template)]** 領域で、**[テンプレートを Amazon S3 にアップロード (Upload a Template to Amazon S3)]**] の横にある円をクリックし、**[ファイルの選択 (Choose File)]** ボタンをクリックします。
  4. Cisco から受け取った JSON 形式のテナント ロール CFT (たとえば、`tenant-cft.json`) を保存したコンピュータ上の場所に移動し、そのテンプレートファイルを選択します。

- Cisco からのテナント ロール CFT URL を指定した場合は、**[テンプレートの選択 (Choose a template)]** 領域で、**Amazon S3 テンプレートの URL を指定 (Specify an Amazon S3 template URL)]** の横にある円をクリックし、Cisco から受け取ったテナント ロールの CFT URL をテキストの下のフィールドに入力します。

ステップ 5 画面の下部にある**[次へ（Next）]** をクリックします。

[詳細の指定 (Specify Details)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

ステップ 6 **[詳細の指定 (Specify Details)]** ページに、以下の情報を入力します。

- **[スタック名 (Stack name):]** ユーザ テナント設定のためのこの IAM ロールの名前を入力します (たとえば `IAM-Role`) 。
- **[infraAccountId:]**このフィールドが表示された場合は、AWS で Cloud APIC を導入する （21 ページ）の説明に従って、インフラ テナントの AWS アカウントを入力します。

  このフィールドは、cisco.com アカウントからテナント ロール CFT をダウンロードして使用した場合に表示されることに注意してください。AWS アカウントからテナント ロール CFT をダウンロードして使用した場合は表示されません。これは、インフラ AWS アカウントの S3 バケットからダウンロードした場合には、この infraAccountID 情報が CFT にあらかじめ入力されているためです。

ステップ 7 画面の下部にある **[次へ（Next）]** をクリックします。

[オプション (Option)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

ステップ 8 適切であれば、**[オプション (Options)]** 画面ですべてのデフォルト値を受け入れ、画面の下部にある **[次へ (Next)]** をクリックします。

[レビュー (Review)] ページが、**[スタックの作成 (Create stack)]** ページ内に表示されます。

ステップ 9 **[レビュー (Review)]** ページで、 **[AWS cloudformation がカスタムの名前を持つ IAM リソースを作成することを認める (I acknowledge that AWS CloudFormation might create IAM resources with custom names)]** の横にあるボックスをオンにし、ページの下部にある **[作成 (create)]** ボタンをクリックします。

[Cloudformation] ページが再び表示され、作成したテンプレートが [ステータス (Status)] 列に **CREATE_IN_PROGRESS** というテキストとともに表示されます。

システムは、テンプレートに指定された情報を使用して、ユーザテナントのIAMロールを作成するようになりました。プロセスが完了するのに 5 ～ 10 分かかります。作成プロセスの進行状況をモニタするには、テンプレートの名前の横にあるボックスをオンにし、[イベント (Events)] タブをクリックします。[イベント (Events)] タブの下の [ステータス (Status)] 列には、**CREATE_IN_PROGRESS** というテキストが表示されます。

CREATE_COMPLETEは、プロセスが完了したときに表示されます。

ステップ 10 **CREATE_COMPLETE**が表示されたら、適切な領域に移動して、ユーザテナントの IAM ロールが正常に作成されたことを確認します。

a) 画面の上部にある **[サービス (Services)]** リンクをクリックし、 **IAM**リンクをクリックします。
b) **[ロール (Roles)]**をクリックします。

Apictenantroleという名前のエントリがロール名の下に表示されます。

次のタスク

セットアップ ウィザードを使用した Cisco Cloud APIC の設定 （31 ページ） に移動して、Cisco Cloud APIC のセットアップを続行します。

AWS アクセス キー ID とシークレット アクセス キーを使用して、信頼されていないユーザ テナントの AWS アカウントをセットアップする

AWS アクセス キー ID とシークレットアクセス キーを使用して信頼できないユーザの AWS アカウントを設定する場合は、次の手順を使用します。この場合、信頼されていないユーザのテナントの AWS アカウントを手動で設定し、AWS IAM を使用して適切な権限を割り当てます。

始める前に

Cloud APIC ユーザ テナントを構成するためのルールと制限は次のとおりです。

- インフラ テナントとユーザ テナントに同じ AWS アカウントを使用することはできません。
- ユーザ テナントごとに 1 つの AWS アカウントが必要です。

ステップ 1 ユーザ テナントの Amazon Web Services アカウントにログインします。

https://signin.aws.amazon.com/

（注） ユーザ テナントのインフラ テナント アカウントを使用することはできません。

ステップ 2 AWS 管理コンソールに進みます。

https://console.aws.amazon.com/

ステップ 3 画面の一番上の **[サービス]** リンクをクリックし、**IAM** リンクをクリックします。

ステップ 4 左側のペインで、**[ユーザ]** をクリックし、[**[ユーザの追加]** ボタンをクリックします。

[ユーザの追加] ページが表示されます。

ステップ 5 **[ユーザ名]** フィールドに、`user1` などの AWS ユーザ アカウントの固有の名前を入力します。

ステップ 6 **[アクセス タイプ]** フィールドで、**プログラムによるアクセス**をオンにします。

ステップ 7 ページの下部にある **[新規 (New)]** ボタンをクリックします。

ステップ 8 **[アクセス許可の設定 (Set permissions)]** エリアで、**[既存のポリシーのアタッチ (Attach existing policies)]** を直接選択します。

画面が展開され、**フィルタ ポリシー**情報が表示されます。

ステップ 9 **[管理者アクセス (Administrator Access)]** の横にあるボックスをオンにし、ページの下部にある **[Next: Tags]** ボタンをクリックします。

ステップ 10 **[タグの追加 (Add tags)]** ページの情報をそのままにして、ページの下部にある **[確認 (Review)]** ボタンをクリックします。

ステップ 11 ページ下部にある **[ユーザの作成 (Create User)]** ボタンをクリックします。

警告が表示さる場合は、**[このユーザに権限がない]**ことを示す警告を無視します。

この時点で、アクセス キーが作成されます。

ステップ 12 この AWS アカウントのアクセス キー ID とシークレット アクセス キーの情報をメモしておきます。

- ユーザ テナントのアクセス キー ID とシークレット アクセス キー情報を、CSR とテナント情報の検索 （97 ページ） の適切な行にコピーします。
- .csv ファイルをダウンロードするか、または **[アクセス キー ID]** フィールドと **[シークレット アクセス キー]** フィールドからファイルに情報をコピーします。

ステップ 13 ページ下部にある **[閉じる (Close)]**ボタンをクリックします。

ステップ 14 必要に応じて、このトピックの手順を追加のユーザアカウントに対して繰り返します。

次のタスク

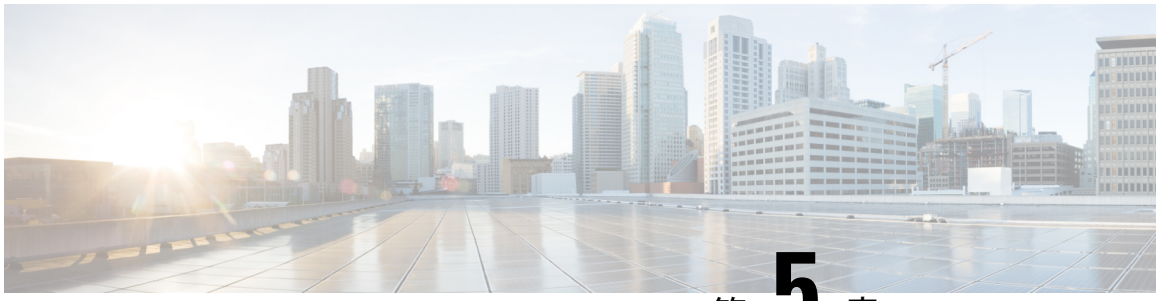
セットアップ ウィザードを使用した Cisco Cloud APIC の設定 （31 ページ） に移動して、Cisco Cloud APIC のセットアップを続行します。

組織のユーザ テナントの AWS アカウントのセットアップ

AWS Organizations と組織のユーザ テナントのサポート （9 ページ） の説明に従って、リリース 4.2(3) 以降では、Cloud APIC を介して AWS 組織アカウントのポリシーを管理できるようになりました。

組織テナントの AWS アカウントを設定するには、この機能を使用するために次の設定が必要です。

- Cloud APIC は、マスターアカウントに導入する必要があります。このドキュメントでは、AWS で Cloud APIC を導入する （21 ページ）に記載されている手順を使用して Cloud APIC を AWS に展開するときに、この AWS 組織のマスターアカウントに Cloud APIC (Cloud APICインフラ テナント) を導入したことを確認します。
- このドキュメントの後半では、共有テナントの設定 （50 ページ） 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ます。



第 5 章

セットアップウィザードを使用したCisco Cloud APICの設定

サイト間接続の設定と展開

の設定と展開を開始する前に、オンプレミス サイトをクラウド サイトに接続する場合は、とをオンプレミスで設定して展開する必要があります。Cloud APICCisco ACI マルチサイトCisco ACIそれぞれの実際の設定は、要件と設定によって異なります。オンプレミスサイトをクラウドサイトに接続する場合は、AWS で Cloud APIC によって展開された Cisco Cloud Services Router 1000V に接続するために、オンプレミスの Ipsec 終端デバイスを設定して展開する必要もあります。詳細については、「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 （5 ページ）」を参照してください。

次に、これらのコンポーネントの設定と展開のプロセスを支援するマニュアルを示します。

- Cisco ACIマニュアル： 『Cisco Application Policy Infrastructure Controller（APIC）』のマニュアル（『Operating Cisco Application Centric Infrastructure』および『Cisco APIC Basic Configuration Guide、Release 4.0（1）』など）で入手できます。
- Cisco ACI マルチサイト： 『Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide、Release 2.0（1）』などの Cisco ACI Multi-Siteのマニュアル を参照してください。
- Cisco Cloud Services Router（CSR）：
  - Cisco Cloud Services Router 1000v: Cisco CSR 1000v のマニュアルで入手できます。

オンプレミス設定情報の収集

（注） クラウドサイト間接続のみを設定している場合は、このセクションの情報を収集する必要はありません。Cisco Cloud APIC

次のリストを使用して、を設定するためにこれらの手順全体で必要なオンプレミスの設定情報を収集し、記録します。Cisco Cloud APIC

必要なオンプレミス情報	入力する値
オンプレミスの IPsec デバイスのパブリック IP アドレス	
IPsec 終端デバイスから CSR への OSPF エリア	
オンプレミス APIC IP アドレス	
Cisco Cloud APIC の IP アドレス	

サイト、リージョン、および CSR の数の制限について

このドキュメントでは、サイト、リージョン、および CSR のさまざまな設定を決定するよう求められます。次に、それぞれの設定を決定する際に留意すべき制限事項のリストを示します。

サイト（Sites）

使用できるサイトの合計数は、設定する設定のタイプによって異なります。Cloud APIC

- オンプレミスの ACI サイト間設定（AWS または Azure）：ACI Multi-Site マルチクラウド導入は、1 つまたは 2 つのクラウド サイト（AWS または Azure）と最大 1 つまたは 2 つのオンプレミス サイトの任意の組み合わせをサポートします。合計 4 つのサイトがあります。接続オプションは次のとおりです。
  - Hybrid-Cloud：オンプレミスから単一のクラウド サイトへの接続
  - Hybrid Multi-Cloud：オンプレミスから複数のクラウド サイトへの接続
- マルチクラウド：クラウド サイト間接続（AWS または Azure）：ACI マルチサイト マルチクラウド展開では、合計 2 つのサイトの任意の 2 つのクラウド サイト（AWS、Azure、またはその両方）の組み合わせをサポートします。
- Cloud First：シングルクラウド構成：ACI Multi-Site マルチクラウド導入は、単一のクラウド サイト（AWS または Azure）をサポートします。

[Regions]

各サイト内では、サイトごとに最大4つのリージョンを設定できます。は複数のリージョンを1つのサイトとして管理できます。Cloud APIC

CSR

一部のリージョン内には一定数の CSR を含めることができますが、次の制限があります。

- VNET 間（Azure）、VPC 間（AWS）、または VRF 間通信を行うには、少なくとも 1 つの CSR が導入されたリージョンが必要です。
- すべての地域に CSR を配置する必要はありません。
- 接続を有効にするために CSR が展開されている場合：
  - CSR は、4 つの管理対象リージョンすべてに導入できます。
  - 管理対象リージョンごとに最大 4 つの CSR がサポートされ、クラウド サイトごとに合計 16 の CSR がサポートされます。

注 管理対象リージョンあたりの CSR の数は、AWS と Azure で異なります。AWS ではリージョンごとに 4 つの CSR がサポートされ（クラウド サイトごとに合計 16 の CSR）、リリース5.1(2) 以降の場合は Azure で 8 つの CSR がサポートされます。（クラウド サイトあたり合計 32 の CSR）。

クラウド APIC の IP アドレスの特定

次の手順では、AWS サイトからの IP アドレスを見つける方法について説明します。Cloud APIC

ステップ 1 インフラ テナントの AWS アカウントに移動します。Cloud APIC

ステップ 2 画面の上部にある **[サービス (Services)]** リンクをクリックし、**[EC2]** リンクをクリックします。

[EC2 ダッシュボード (EC2 Dashboard)] 画面が表示されます。

ステップ 3 [EC2 ダッシュボード (EC2 Dashboard)] 画面の **[リソース (Resources)]** 領域には、実行中のインスタンスの数を示すテキストが表示されます (たとえば、**[1 つの実行インスタンス (1 Running Instances)]**)。この実行中のインスタンスのリンクをクリックします。

[インスタンス (Instances)] 画面が表示されます。

ステップ 4 [Capic-1] という名前のインスタンスを選択し、IPv4 パブリック IP 列に表示されている IP アドレスをコピーします。Cloud APIC

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

これは、Cloud APIC にログインするために使用する IP アドレスです。Cloud APIC

（注） また、CloudFormation ページに戻り、Cisco Cloud APIC の横にあるボックスをクリックして [出力（Outputs）] タブをクリックすることでも、IP アドレスを取得できます。Cloud APIC[値（Value）] 列に Cisco Cloud APIC の IP アドレスが表示されます。

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

Cloud APIC のクラウド インフラストラクチャ設定をセットアップするには、このトピックの手順に従います。Cloud APIC は、必要な AWS コンストラクトと必要な CSR を自動的に展開します。

始める前に

このタスクの前提条件は次のとおりです。

- このセクションのタスクに進む前に、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 （15 ページ） に示されている要件を満たしています。
- Cisco Cloud APIC のクラウド形成テンプレート情報の設定 （21 ページ） に記載されている手順を正常に完了しました。

ステップ 1 AWS サイトで IP アドレスを取得します。Cloud APIC

手順については、クラウド APIC の IP アドレスの特定 （33 ページ） を参照してください。

ステップ 2 ブラウザ ウィンドウを開き、セキュア バージョンの HTTP（`https://`）を使用して、URL フィールドに IP アドレスを貼り付け、Return を押してアクセスします。Cloud APIC

たとえば、`https://192.168.0.0` と入力します。

[リスクを無視して証明書を受け入れる（Ignore Risk and Accept Certificate）]というメッセージが表示された場合は、証明書を受け入れて続行します。

ステップ 3 Cloud APIC のログイン ページに次の情報を入力します。

- ユーザ名：このフィールドにadminと入力します。
- [パスワード（Password）]：手順の [詳細の指定（Specify Details）] ページで指定したパスワードを入力します。ステップ 12 （23 ページ）AWS で Cloud APIC を導入する （21 ページ）
- [ドメイン（Domain）]：[ドメイン（Domain）] フィールドが表示された場合は、デフォルトの [ドメイン（Domain）] エントリをそのままにします。

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

ステップ 4 ページの下部にある **[ログイン]** をクリックします。

（注） ログインしようとしたときに、RESTエンドポイントのユーザ認証データストアが初期化されていないなどのエラーメッセージが表示された場合は、このファブリックノードのファブリックメンバーシップステータスを確認し、数分待ってから数分後に再試行してください。ログインするためにページを更新する必要がある場合もあります。

[クラウド APIC へようこそ（Welcome to Cloud APIC）] セットアップ ウィザードのページが表示されます。

ステップ 5 [Begin Setup] をクリックします。

[基本設定（Let's Configure the Basics）] ページが表示され、次の領域が設定されます。

- **DNS サーバ**
- **リージョン管理**
- **スマート ライセンス**

ステップ 6 [DNS Servers] 行で、[Edit Configuration] をクリックします。

[DNS および NTP] ページが表示されます。

ステップ 7 **[DNS および NTP]** ページで、必要に応じて DNS サーバと NTP サーバを追加します。

- DNS サーバはデフォルトですでに設定されています。特定の DNS サーバを使用する場合は、DNS サーバを追加します。
- ただし、NTP サーバはデフォルトでは設定されないため、NTP サーバを設定することを推奨します。NTP サーバを設定し、DNS サーバを設定しない場合は、7.d （35 ページ） に進みます。

a) 特定の DNS サーバを使用する場合は、[DNS Servers] 領域で [+ Add DNS Provider] をクリックします。
b) DNS サーバの IP アドレスを入力し、必要に応じて [優先 DNS プロバイダー（Preferred DNS Provider）] の横にあるボックスをオンにします。
c) DNS サーバの横にあるチェック マークをクリックし、追加する追加の DNS サーバについて繰り返します。
d) [NTP Servers] 領域で、[+ Add Providers] をクリックします。
e) NTP サーバの IP アドレスを入力し、必要に応じて、[Preferred NTP Provider] の横にあるボックスをオンにします。
f) NTP サーバの横にあるチェック マークをクリックし、追加する NTP サーバを繰り返します。

ステップ 8 DNS サーバと NTP サーバの追加が完了したら、[保存して続行（Save and Continue）] をクリックします。

[Let's Configure the Basics] ページが再度表示されます。

ステップ 9 [Region Management] 行で、[Begin] をクリックします。

[地域 Management] ページが表示されます。

ステップ 10 サイト間接続が必要な場合は、[サイト間接続（Inter-Site Connectivity）] 領域の [有効（Enabled）] ボックスをクリックしてオンにします。

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

このリージョンを他のサイトに接続する場合（たとえば、このリージョンをオンプレミス サイトに接続する場合、または Cisco ACI Multi-Site を介してクラウド サイト間接続する場合）、このオプションを選択します。インフラ VPC または VNET は、サイト間接続用に選択されたすべてのリージョンに展開されます。リージョンのサイト間接続を選択すると、サイト間接続ハブ用に 2 つのクラウド ルータが展開されている必要があるため、このリージョンのクラウドルータ オプションも自動的に選択されることに注意してください。

このオプションを選択すると、ページ上部の [セットアップ-リージョン管理（Setup-Region Management）] の手順にサイト間接続の手順が追加されます。

ステップ 11 ホーム リージョンが選択されていることを確認します。Cloud APIC

ステップ 2 （22 ページ） で選択したリージョンがホーム リージョンであり、このページですでに選択されている必要があります。AWS で Cloud APIC を導入する （21 ページ）これは、Cloud APIC が展開されている地域（によって管理される地域）であり、[地域（Region）] 列にテキスト cAPICが表示されます。Cloud APIC

ステップ 12 Cloud APIC で追加のリージョンを管理し、場合によっては、他のリージョンで VPC 間通信と Hybrid-Cloud、Hybrid Multi-Cloud、または Multi-Cloud 接続を持つように CSR を展開する場合は、追加のリージョンを選択します。

CSR は、展開されているホームリージョンを含む 4 つのリージョンを管理できます。Cloud APIC

Cloud APIC は、複数のクラウド リージョンを単一のサイトとして管理できます。一般的な設定では、サイトは APIC クラスタで管理できるすべてのものを表します。Cisco ACIクラスタが 2 つのリージョンを管理する場合、これらの 2 つのリージョンは単一のサイトと見なされます。Cloud APICCisco ACI

ステップ 13 クラウド ルータをこのリージョンにローカルに展開するには、そのリージョンの [Cloud Routers] チェック ボックスをオンにします。

VPC 間または VNET 間通信を行うには、少なくとも 1 つのリージョンに CSR が展開されている必要があります。ただし、このページで複数のリージョンを選択した場合は、選択したすべてのリージョンに CSR を設定する必要はありません。詳細については、「サイト、リージョン、および CSR の数の制限について （32 ページ）」を参照してください。

ステップ 14 すべての適切なリージョンを選択したら、ページの下部にある [Next] をクリックします。

[General Connectivity] ページが表示されます。

ステップ 15 [General Connectivity] ページで次の情報を入力します。

a) [Hub Network] 領域で、[Add Hub Network] をクリックします。

[Add Hub Network] ウィンドウが表示されます。

b) **[Name]** フィールドにハブ ネットワークの名前を入力します。

c) [BGP Autonomous System Number] フィールドに、AWS でゼロを入力して番号を選択するか、各ハブネットワークの値を 64512 ー 65534 の範囲で入力し、フィールドの横にあるチェック マークをクリックします。

独自の BGP 自律番号を設定するには、各ハブネットワークに 64512 ー 65534 の値を入力します。

AWS トランジット ゲートウェイのインスタンスごとに異なる番号を使用することをお勧めします。

d) AWS Transit Gateway Connect機能を有効にする場合は、**[TGW Connect]** フィールドでチェック ボックスをクリックします。

AWS トランジット ゲートウェイ接続機能の詳細については、ドキュメント「AWS トランジット ゲートウェイまたは AWS トランジット ゲートウェイ コネクトを使用した VPC 間の帯域幅の増加」を参照してください。https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/cloud-apic/5-x/use-case/increasing-bandwidth-using-aws-transit-gateway-or-aws-transit-gateway-connect.html

e) **[CIDR]** 領域で、**[Add CIDR]** をクリックします。

これは、AWS トランジット ゲートウェイ接続 CIDR ブロックで、トランジット ゲートウェイ側の接続ピア IP アドレス（GRE 外部ピア IP アドレス）として使用されます。

1. **[Region]** フィールドで、適切な地域を選択します。
2. **[CIDR Block Range]** フィールドに、中継ゲートウェイ側の接続ピア IP アドレスとして使用される CIDR ブロックを入力します。
3. この CIDR ブロックのこれらの値を受け入れるには、チェック マークをクリックします。
4. AWS トランジット ゲートウェイ接続機能を使用するすべての管理対象リージョンに対して、これらの管理対象リージョンのそれぞれに使用する CIDR ブロックを追加します。

f) CSR のサブネット プールを追加するには、**[Add Subnet Pool for Cloud Router]** をクリックし、テキスト ボックスにサブネットを入力します。

最初の2つのリージョンの最初のサブネット プールが自動的に入力されます。3つ以上のリージョンを選択した場合は、追加の 2 つのリージョンのリストにクラウド ルータのサブネットを追加する必要があります。このサブネット プールからのアドレスは、最初の 2 つのリージョンの後にクラウドAPIC で管理する必要がある追加のリージョンのリージョン間接続に使用されます。これはマスク /24 の有効な Ipv4 サブネットである必要があります。

（注） クラウド APIC の導入時に提供される /24 サブネットは、最大 2 つのクラウド サイトに十分です。3つ以上のクラウドサイトを管理する必要がある場合は、さらにサブネットを追加する必要があります。

g) **[BGP Autonomous System Number for CSRs]** フィールドに値を入力します。

BGP ASN の範囲は 1 ー 65534 です。

（注） このフィールドでは、自律システム番号として **64512** を使用しないでください。

h) **[Assign Public IP to CSR Interface]** フィールドで、CSR インターフェイスにパブリック IP アドレスまたはプライベート IP アドレスを割り当てるかどうかを決定します。

- パブリック IP アドレスを CSR インターフェイスに割り当てるには、**[有効（Enabled）]** チェック ボックスをオンのままにします。デフォルトでは、この **[有効]** チェック ボックスはオンになっています。

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

- パブリック IP アドレスを CSR インターフェイスに割り当てるには、**[有効]** チェック ボックスをオンのままにします。この場合、接続にはプライベート IP アドレスが使用されます。

（注） パブリック IP アドレスの無効化または有効化は中断を伴う操作であり、トラフィック損失の原因となる可能性があります。 リリース 5.2(1) 以降では、CSR に割り当てられたパブリック IP アドレスとプライベート IP アドレスの両方が、[Cloud Resources] 領域にルータの他の詳細とともに表示されます。パブリック IP が CSR に割り当てられていない場合は、プライベート IP だけが表示されます。

i) **[Cloud Router Template]** 領域の **[Number of Routers Per Region]** フィールドで、各リージョンで使用される Cisco Cloud Services Router の数を選択します。

リージョンごとの CSR 数の制限の詳細については、サイト、リージョン、および CSR の数の制限について （32 ページ） を参照してください。

j) **[Username]** に、Cisco Cloud Services Router のユーザ名を入力します。

k) **[Password]** に、Cisco Cloud Services Router のパスワードを入力します。

l) **[Throughput of the routers]** フィールドで、Cisco Cloud Services Router のスループットを選択します。

このフィールドの値を変更すると、展開される CSR インスタンスのサイズが変更されます。スループットの値を高くすると、導入される VM のサイズが大きくなります。

（注） 将来のある時点でこの値を変更する場合は、CSR を削除してから、この章のプロセスを再度繰り返し、同じ **[ルータのスループット（Throughput of the routers）]** フィールドで新しい値を選択する必要があります。

また、CSR のライセンスはこの設定に基づきます。準拠するには、Smart アカウントに同等以上のライセンスが必要です。詳細については、「AWS パブリック クラウドの要件 （16 ページ）」を参照してください。

（注） クラウド ルータは、ルータのスループットまたはログイン クレデンシャルを変更する前に、すべてのリージョンから展開解除する必要があります。

m) 必要に応じて、**[TCP MSS]** フィールドに必要な情報を入力します。

リリース 5.0(2l) 以降では、TCP 最大セグメントサイズ（MSS）を設定するために **TCP MSS** オプションを使用できます。この値は、クラウドへの VPN トンネルとオンプレミス サイトまたは他のクラウド サイトへの外部トンネルを含む、すべてのクラウド ルータ インターフェイスに適用されます。クラウドへの VPN トンネルの場合、クラウド プロバイダーの MSS 値がこのフィールドに入力した値よりも小さい場合は、低い方の値が使用されます。それ以外の場合は、このフィールドに入力した値が使用されます。

MSS 値は TCP トラフィックにのみ影響し、ping トラフィックなどの他のタイプのトラフィックには影響しません。

n) **[License Token]** フィールドに、Cisco Cloud Services Router のライセンス トークンを入力します。

これは、シスコ スマート ソフトウェア ライセンシング アカウントからの製品インスタンス登録トークンです。このライセンス トークンを取得するには、http://software.cisco.com に移動し、[Smart

Software Licensing Inventory Virtual Account] に移動して、製品インスタンス登録トークンを見つけます。

（注） プライベート IP アドレスを使用して CSR のスマート ライセンスを登録する場合、パブリック IP アドレスが CSR に対して無効になっている場合、サポートされる唯一のオプションは、AWS Direct Connect または Azure Express Route to Cisco Smart Software Manager（CSSM）です（Administrative Smart Licensing に移動して使用可能）。15.h （37 ページ）この場合、AWS Direct Connect または Azure Express Route を介して CSSM への到達可能性を提供する必要があります。パブリック IP アドレスが無効になっている場合、プライベート IP アドレスが使用されているため、パブリック インターネットは使用できません。したがって、接続には AWS Direct Connect または Azure Express Route であるプライベート接続を使用する必要があります。

ステップ 16 サイト間接続を設定するかどうかに応じて、適切なボタンをクリックします。

- サイト間接続を設定しない場合（[リージョン管理（Region Management）]ページで管理するリージョンを選択したときに [サイト間接続（Inter-Site Connectivity）] を選択しなかった場合）、[保存して続行（Save and Continue）] をクリックします。[Let's Configure the Basics] ページが再度表示されます。ステップ 19 （40 ページ） にスキップします。
- サイト間接続を設定する場合（[リージョン管理（Region Management）] ページで管理するリージョンを選択したときに [サイト間接続（Inter-Site Connectivity）] を選択した場合）、ページの下部にある [次へ（Next）] をクリックします。[サイト間 Connectivity] ページが表示されます。

ステップ 17 [サイト間接続（Inter-Site Connectivity）] ページに次の情報を入力します。

- IPSec Tunnels to Inter-Site Routers：このフィールドは、クラウド サイトへのオンプレミス接続にのみ必要です。オンプレミス サイトがない場合は、このフィールドに情報を入力する必要はありません。

  この領域で、[Add Public IP of IPsec Tunnel Peer] フィールドの横にある [+] ボタンをクリックします。

  - オンプレミス デバイスへの IPsec トンネル終端のピア IP アドレスを入力します。
  - このピア IP アドレスを追加するには、チェック マークをクリックします。

- OSPF Area for Inter-Site Connectivity：オンプレミス ISN ピアリングで使用されるアンダーレイ OSPF エリア ID を入力します（0.0.0.1など）。
- [External Subnets for Inter-Site Connectivity] 見出しの下で、[+ Add External Subnet] フィールドの横にある [+] ボタンをクリックします。
  - AWS で使用されるサブネットトンネルエンドポイントプール（クラウドTEP）を入力します。これは、/16 ー /22 のマスクを持つ有効な IPv4 サブネットである必要があります（30.29.0.0/16など）。このサブネットは、オンプレミス接続に使用されるクラウド ルータの IPsec トンネル インターフェイスおよびループバックに対処するために使用され、他のオンプレミス TEP プールと重複することはできません。
  - 適切なサブネット プールに入力したら、チェック マークをクリックします。

セットアップ ウィザードを使用した Cisco Cloud APIC の設定

ステップ 18 このページに必要な情報をすべて入力したら、ページの下部にある [保存して続行（Save and Continue）] をクリックします。

[Let's Configure the Basics] ページが再度表示されます。

ステップ 19 [Smart Licensing] 行で、[Register] をクリックします。

[Smart Licensing] ページが表示されます。

ステップ 20 [Smart Licensing] ページに必要な情報を入力します。

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。お使いの Cloud APIC をシスコのスマート ライセンスに登録するには、以下のようにします。

- 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。
- スマート アカウントにログインします。
  - Smart Software Manager: https://software.cisco.com/
  - Smart Software Manager サテライト: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html
- 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。
- 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。

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。

ステップ 21 このページで必要なライセンス情報を入力した場合はページの下部にある [登録（Register）] をクリックします。代わりに評価モードで続行する場合は [評価モードで続行（Continue in Evaluation Mode）] をクリックします。

[概要（Summary）] ページが表示されます。

ステップ 22 [Summary] ページで情報を確認し、[Close] をクリックします。

この時点で、Cloud APIC の内部ネットワーク接続の設定は完了です。

Cloud APIC を初めて導入する場合は、このプロセスが正常に完了するまでにかなりの時間（30 分ほど）がかかることがあります。

次のタスク

Cisco Cloud APIC サイトとともに追加のサイトを管理するかどうかを決定します。

- Cisco Cloud APIC サイトとともに追加のサイト（オンプレミス サイトまたはクラウド サイト）を管理する場合（[リージョン管理（Region Management）] ページで [サイト間接続

（Inter-Site Connectivity）] オプションを選択した場合）。Cisco ACI マルチサイトを介した Cisco Cloud APIC の管理 （43 ページ）

- クラウド ファースト設定をセットアップする場合は、Cisco Cloud APIC サイトとともに他のサイトも管理しません（[リージョン管理（Region Management）] ページで [クラウド ルータ（Cloud Routers）] オプションのみを選択した場合）。追加設定用の Cisco ACI マルチサイトを使用する必要はありません。ただし、この場合、Cisco Cloud APIC GUI で追加の設定を実行する必要があります。Cisco Cloud APIC GUI の [Global Create] オプションを使用して、次のコンポーネントを設定します。
  - テナント
  - アプリケーション プロファイル
  - EPG

詳細については、「Cisco Cloud APIC GUI の操作 （67 ページ）」と「Cisco Cloud APIC コンポーネントの設定 （68 ページ）」を参照してください。

Cisco Cloud APIC セットアップ ウィザードの設定の確認

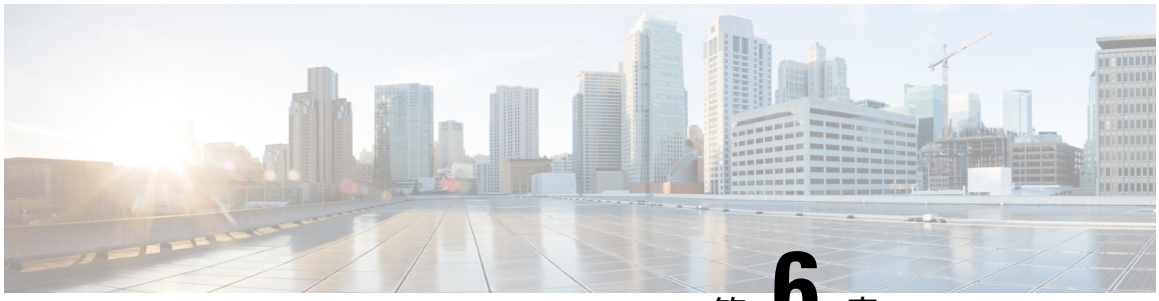
このトピックの手順を使用して、 Cloud APIC セットアップ ウィザードに入力した設定情報が正しく適用されていることを確認します。

Cisco Cloud APIC で、次の設定を確認します。

- **[クラウド リソース（Cloud Resources）]** で、**[リージョン（Regions）]** をクリックし、選択したリージョンが [管理ステート（Admin State] 列に **管理対象** として表示されていることを確認します。
- [インフラストラクチャ（Infrastructure）] で [リージョン間接続（Inter-Region Connectivity）] をクリックし、この画面の情報が正しいことを確認します。
- [インフラストラクチャ（Infrastructure）] で、[オンプレミス接続（On Premises Connectivity）] をクリックし、この画面の情報が正しいことを確認します。
- [ダッシュボード (Dashboard)] をクリックし、オンプレミス接続ステータスおよびリージョン間接続ステータス ボックスの情報を使用してセットアップ ウィザードとトンネル設定が適切であることを確認します。

次のタスク

Cisco ACI マルチサイトを介した Cisco Cloud APIC の管理 （43 ページ） に示す手順を使用して、マルチサイト設定を完了します。



第 6 章

Cisco ACI マルチサイトを介した Cisco Cloud APIC の管理

Cisco Cloud APIC と Cisco ACI マルチサイトについて

セットアップウィザードを使用して Cisco Cloud APIC を設定するときに **[サイト間接続 (Inter-Site Connectivity)]** オプションを **[リージョン管理 (Region Management)]** ページで選択した場合は、Cisco ACI マルチサイトを使用して、オンプレミス サイトやクラウド サイトなどの別のサイトを、Cisco Cloud APIC サイトとともに管理します。Cisco Cloud APIC のセットアップウィザードで、**[クラウド ルータ (Cloud Routesr)]** オプションだけを **[リージョン管理 (Region Management)]** ページで選択した場合は、Cisco ACI マルチサイトは必要ありません。

Cisco Cloud APIC の管理専用に使用される、いくつかの新しいページが ACI マルチサイト オーケストレータに導入されています。この章のトピックでは、これらの新しい Cisco Cloud APIC 管理ページについて説明します。これらの Cisco Cloud APIC 管理ページに必要な情報を入力すると、Cisco Cloud APIC は、実質的に、Cisco ACI マルチサイトを介して管理する別のサイトになります。

Cisco Cloud APIC サイトとともにオンプレミス サイトを管理している場合は、まだ設定していなければ、これらの手順を開始する前にオンプレミス サイトを設定しておくことを推奨します。これらの手順については、次の URL にある *CISCO ACI Multi Site Orchestrator Installation And Upgrade Guide* 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

Cisco ACI マルチサイトへの Cisco Cloud APIC サイトの追加

ステップ 1 まだログインしていない場合は、ACI マルチサイト オーケストレータ にログインします。

ステップ 2 メイン メニューで **[サイト]** をクリックします。

ステップ 3 **[サイト リスト]** ページで、**[サイトの追加 (ADD SITES)]** をクリックします。

ステップ 4 **[接続設定]** ページで、次の操作を実行します。

a) **[名前 (NAME)]** フィールドに、サイト名を入力します。

たとえば、`cloudsite1`です。

b) （任意） **[ラベル (LABELS)]** フィールドで、ラベルを選択するか作成します。

c) **[APIC CONTROLLER URL]** フィールドに、Cloud APIC の URL を入力します。これは、Amazon Web Services によって割り当てられるパブリック IP アドレスです。これは、セットアップウィザードを使用してCloud APIC設定Cisco Cloud APICする手順の開始時ににログインするために使用したのと同じパブリック IP アドレスです。

たとえば、`https://192.0.2.1`です。

d) **[ユーザ名 (USERNAME)]**フィールドにユーザ名を入力します。

たとえば、`admin`とします。`admin` と同じ権限を持つ任意のアカウントに登録することもできます。

e) **[パスワード (PASSWORD)]** フィールドに、パスワードを入力します。

f) このフィールドが自動的に入力されていない場合は、**[APIC SITE ID]** フィールドに、一意のサイト ID を入力します。

サイト ID は、Cloud APIC サイトの固有識別子である必要があります。範囲は 1 ～ 127 です。

g) **[保存 (SAVE)]** をクリックします。

ステップ 5 Cloud APIC サイトが正しく追加されたことを確認します。

複数のサイトを管理している場合は、ACI マルチサイト オーケストレータ の [サイト (Sites)] 画面にすべてのサイトを表示する必要があります。ACI マルチサイト オーケストレータ は、サイトがオンプレミスであるか、Cloud APIC サイトであるかを自動的に検出します。

次のタスク

サイト間インフラストラクチャの設定 （45 ページ） に進みます。

サイト間インフラストラクチャの設定

ステップ 1 **[サイト (Sites)]** ビューで、**[インフラの構築 (CONFIGURE INFRA)]** をクリックします。

[ファブリック接続インフラ (Fabric Connectivity Infra)] ページが表示されます。

ステップ 2 左側のペインの **[サイト (SITES)]** の下で、クラウド サイトをクリックします。

クラウドサイト領域のほとんどすべての情報は自動的に入力され、次のステップで説明する [BGP パスワード (BGP Password)] フィールドを除き、変更できません。

ステップ 3 オンプレミス サイトとクラウド サイト間でパスワードを設定するかどうかを決定します。

- オンプレミス サイトとクラウド サイトの間でパスワードを設定しない場合は、ステップ 4 （45 ページ）に進みます。
- オンプレミス サイトとクラウド サイト間でパスワードを設定するには、次のようにします。

a) 右側のペインで、**[BGP パスワード (BGP password)]** フィールドをクリックして、パスワードを入力します。

b) [CloudSite] ウィンドウの右上隅にある [更新 (Refresh)] アイコンをクリックします。

すべてのクラウド プロパティは、 Cloud APICから自動的に取得されます。サイトが正常に更新されたことを示すメッセージが表示され、すべてのクラウドプロパティが Cloud APIC から正常に取得されたことを確認します。

ステップ 4 クラウド サイトでマルチサイト接続を有効にするには、 **[ACI マルチサイト (ACI Multi-Site)]**ボタンをクリックします。

ステップ 5 サイト間インフラストラクチャを設定するために使用する展開のタイプを選択します。

画面の右上にある **[展開 (Deploy)]** ボタンをクリックすると、次のスクロールダウンメニューオプションが表示されます。

- **[展開のみ (Deploy Only):]** マルチクラウド (クラウドサイトからクラウドサイト) への接続を設定する場合は、このオプションを選択します。

  このオプションは、クラウドサイトとCloud APICサイトに設定をプッシュし、クラウド サイト間のエンドツーエンド インターコネクト接続を有効にします。

- **[展開 & IPN デバイス設定ファイルをダウンロード (Deploy & Download IPN Device config files:):]** オンプレミスの APIC サイトと Cloud APIC サイトの両方に設定をプッシュし、オンプレミスとクラウド サイト間のエンドツーエンド インターコネクト接続を有効にします。さらに、このオプションでは、AWS に導入された Cisco クラウド サービス ルータ（CSR）とオンプレミスの IPsec 終端 デバイスとの間の接続を有効にするための設定情報を含む zip ファイルをダウンロードします。すべてまたは一部

の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

- **[IPN デバイス設定ファイルのみをダウンロード (Download IPN Device config files only):]** AWS に展開された CSR とオンプレミスの IPsec 終端デバイス間の接続を有効にするために使用する、設定情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

Cisco Cloud APIC と ISN デバイス間の接続の有効化

（注） このセクションの手順は、オンプレミス サイトとクラウド サイト間の接続を有効にしている場合にのみ実行してください。オンプレミスサイトがない場合は、これらの手順をスキップして、 共有テナントの設定 （50 ページ） に進みます。

Amazon Web Services に展開された Cisco Cloud Services Router（CSR）とオンプレミスの IPsec ターミネーション デバイス間の接続を手動で有効にするには、次の手順に従います。

デフォルトでは、Cisco Cloud APIC は冗長 CSR のペアを展開します。このセクションの手順では、2 つのトンネルを作成します。1 つはオンプレミスの IPsec デバイスからこれらの各 CSR に対する IPsec トンネルです。

次の情報は、オンプレミスの IPsec ターミネーション デバイスとして CSR のコマンドを提供します。別のデバイスまたはプラットフォームを使用している場合は、同様のコマンドを使用します。

ステップ 1 AWS に導入された Csr とオンプレミスの IPsec ターミネーション デバイスとの間の接続を有効にするために必要な必要な情報を収集します。

- サイト間インフラストラクチャの設定 （45 ページ）で示されている手順の一部として ACI マルチサイト オーケストレータで、**IPN デバイス設定ファイルを展開してダウンロードする**か、**IPN デバイス設定ファイルのみをダウンロードする**ように選択した場合、ISN デバイスの設定ファイルが含まれている zip ファイルを見つけます。
- AWS に展開された CSR とオンプレミスの IPsec ターミネーション デバイスとの間の接続を有効にするために必要な情報を手動で検索する場合は、『*Cisco Cloud APIC* インストール ガイド』の付録で説明されているように、CSR とテナントの情報を収集します。

ステップ 2 オンプレミスの IPsec デバイスにログインします。

ステップ 3 最初の CSR のトンネルを設定します。

ACI マルチサイト オーケストレータ を使用して、ISN デバイスの設定ファイルをダウンロードした場合は、最初の CSR の設定情報を見つけて、その設定情報を入力します。

次に、最初の CSR の設定情報がどのように表示されるかの例を示します。

```
crypto isakmp policy 1
    encryption  aes
    authentication pre-share
    group  2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-<first-CSR-tunnel-ID>
    pre-shared-key address <first-CSR-elastic-IP-address> key <first-CSR-preshared-key>
exit

crypto isakmp profile infra:overlay-1-<first-CSR-tunnel-ID>
    local-address <interface>
    match identity address <first-CSR-elastic-IP-address>
    keyring infra:overlay-1-<first-CSR-tunnel-ID>
exit

crypto ipsec transform-set infra:overlay-1-<first-CSR-tunnel-ID> esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-<first-CSR-tunnel-ID>
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel <first-CSR-tunnel-ID>
    ip address <peer-tunnel-for-onprem-IPsec-to-first-CSR> 255.255.255.252
    ip virtual-reassembly
    tunnel source <interface>
    tunnel destination <first-CSR-elastic-IP-address>
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-<first-CSR-tunnel-ID>
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf <process-id> area <area-id>
    no shut
exit
```

それぞれの説明は次のとおりです。

- <first-CSR-tunnel-ID> は、このトンネルに割り当てる一意のトンネル ID です。
- <first-CSR-tunnel-ID> は、最初の CSR の 3 番目のネットワーク インターフェイスの柔軟な IP アドレスです。
- <first-CSR-preshared-key> は、最初の CSR の事前共有キーです。
- <interface> は、Amazon Web サービスに導入された CSR への接続に使用されるインターフェイスです。
- <peer-tunnel-for-onprem-IPsec-to-first-CSR> は、最初のクラウド CSR に対してオンプレミスの IPsec デバイスのピア トンネル IP アドレスとして使用されます。
- <process-id> は OSPF プロセス ID です。
- <area-id> は、OSPF エリア ID です。

次に例を示します。

```
crypto isakmp policy 1
    encryption  aes
    authentication pre-share
    group  2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-1000
    pre-shared-key address 192.0.2.20 key 12345678900987654321234567890
exit

crypto isakmp profile infra:overlay-1-1000
    local-address GigabitEthernet1
    match identity address 192.0.2.20
    keyring infra:overlay-1-1000
exit

crypto ipsec transform-set infra:overlay-1-1000 esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-1000
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel 1000
    ip address 30.29.1.2 255.255.255.252
    ip virtual-reassembly
    tunnel source GigabitEthernet1
    tunnel destination 192.0.2.20
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-1000
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf 1 area 1
    no shut
exit
```

ステップ 4 *2* 番目の CSR のトンネルを設定します。

ACI マルチサイト オーケストレータ を使用して、ISN デバイスの設定ファイルをダウンロードした場合は、2 番目の CSR の設定情報を見つけて、その設定情報を入力します。

次に、2 番目の CSR の設定情報がどのように見えるかの例を示します。

```
crypto isakmp policy 1
    encryption  aes
    authentication pre-share
    group  2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-<second-CSR-tunnel-ID>
    pre-shared-key address <second-CSR-elastic-IP-address> key <second-CSR-preshared-key>
```

```
exit

crypto isakmp profile infra:overlay-1-<second-CSR-tunnel-ID>
    local-address <interface>
    match identity address <second-CSR-elastic-IP-address>
    keyring infra:overlay-1-<second-CSR-tunnel-ID>
exit

crypto ipsec transform-set infra:overlay-1-<second-CSR-tunnel-ID> esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-<second-CSR-tunnel-ID>
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel <second-CSR-tunnel-ID>
    ip address <peer-tunnel-for-onprem-IPsec-to-second-CSR> 255.255.255.252
    ip virtual-reassembly
    tunnel source <interface>
    tunnel destination <second-CSR-elastic-IP-address>
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-<second-CSR-tunnel-ID>
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf <process-id> area <area-id>
    no shut
exit
```

次に例を示します。

```
crypto isakmp policy 1
    encryption  aes
    authentication pre-share
    group  2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-1001
    pre-shared-key address 192.0.2.21 key 12345678900987654321234567891
exit

crypto isakmp profile infra:overlay-1-1001
    local-address GigabitEthernet1
    match identity address 192.0.2.21
    keyring infra:overlay-1-1001
exit

crypto ipsec transform-set infra:overlay-1-1001 esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-1001
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel 1001
    ip address 30.29.1.6 255.255.255.252
```

```
    ip virtual-reassembly
    tunnel source GigabitEthernet1
    tunnel destination 192.0.2.21
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-1001
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf 1 area 1
    no shut
exit
```

ステップ 5 設定する必要があるその他の CSR について、これらの手順を繰り返します。

ステップ 6 オンプレミスの IPsec デバイスでトンネルがアップしていることを確認します。

次に例を示します。

```
ISN_CSR# show ip interface brief | include Tunnel
Interface              IP-Address      OK? Method Status                Protocol
Tunnel1000             30.29.1.2       YES manual up                    up
Tunnel1001             30.29.1.4       YES manual up                    up
```

両方のトンネルがアップとして表示されていない場合は、この項の手順で入力した情報を確認して、問題が発生している可能性がある場所を確認します。両方のトンネルがアップとして表示されるまで、次のセクションに進まないでください。

共有テナントの設定

オンプレミスサイトと Cloud APIC サイト間で共有されるテナントを設定するには、この項の手順に従います。

ステップ 1 ACI マルチサイト オーケストレータで、次の手順を実行します。

a) メイン メニューで、**[テナント (Tenants)]** をクリックします。

b) [テナント リスト (Tenants List)] エリアで、**[テナントの追加 (ADD TENANT)]** をクリックします。

c) [テナントの詳細 (Tenant Details)] ペインで、次の手順を実行します。

- **[表示名 (DISPLAY NAME)]** フィールドに、テナント名を入力します。
- **オプション: [説明 (DESCRIPTION)]** フィールドに、テナントについての簡潔な説明を入力します。
- **[関連するサイト (Associated Sites)]** セクションで、オンプレミスとクラウドのサイトを選択します。
- まだ選択していなければ、**[関連するユーザ (Associated Users)]** セクションで、ユーザを選択します。
- **[保存 (SAVE)]** をクリックします。

ステップ 2 Cloud APICサイトにログインし、このテナントの Amazon Web Services アカウントの詳細を設定します。

a) メインの Cloud APIC ページの **[アプリケーション管理 (Application Management)]** の下で、**[テナント (Tenant)]** をクリックします。

b) [テナント (Tenant)] ページで、前の手順の ACI マルチサイト オーケストレータ で作成したテナントをクリックします。

c) 画面の右上にある展開ボタンをクリックします。

これは、[閉じる (X)] ボタンの横にある、正方形と上向きの矢印が付いたボタンです。

d) [テナント (Tenant)] ページで、画面の右上にある編集ボタンをクリックします。これは、[アクション (Actions)] フィールドの横にある、鉛筆のアイコンが付いたボタンです。

e) [テナントの編集 (Edit Tenant)] ページで、[設定 (Settings)] 領域までスクロールし、 ユーザ テナントのアクセス タイプに応じて必要な情報を入力します。

- Cloud APIC のユーザ テナントが信頼されている場合 (CFT を使用して信頼できるテナントの AWS アカウントを設定した場合) は、このページに次の情報を入力します。
  - **[AWS アカウント ID (AWS Account ID):]** ユーザ テナントの AWS アカウント番号 (CFT を使用して、信頼できるテナントのAWSアカウントをセットアップしたときにログインしたAWSアカウント) を入力します。
  - [アクセスタイプ（Access Type）] : このフィールドで[信頼（Trusted）]を選択します。

    （注） **[クラウド アクセス キー ID (Cloud Access KEY ID)]** フィールドと **[クラウド秘密アクセス キー (Cloud Secret Access Key)]** フィールドは、**[アクセス タイプ（Access Type）]** として **[信頼済み（Trusted）]** を選択している場合、表示されません。これらのフィールドは、信頼できるテナントには必要ありません。

- Cloud APICのユーザ テナントが信頼されていない場合 (AWS アクセスキー ID と秘密アクセス キーを使用して、信頼できないユーザ テナントの AWS アカウントをセットアップした場合) は、このページで次の情報を入力します。
  - **[AWS アカウント ID (AWS Account ID):]** このフィールドには、ユーザ テナントの AWS アカウント番号を入力します。
  - Access Type：このフィールドで[Untrusted]を選択します。
  - **[クラウド アクセス キー ID (Cloud Access KEY ID):]** このフィールドには、ユーザ テナントの AWS アクセスキー ID 情報を入力します。
  - **[クラウド秘密アクセス キー (Cloud Secret Access Key):]** このフィールドには、ユーザ テナントの AWS 秘密アクセス キー情報を入力します。

- のユーザテナントがAWS組織のメンバーである場合（AWS組織を使用して組織を設定し、組織内にアカウントを作成するか、組織にアカウントを招待することでアカウントを追加した場合）、組織のマスターアカウントの場合は、次の情報を入力して組織タグをこのテナントに割り当てます。Cloud APICCloud APIC
  - **[AWS アカウント ID (AWS Account ID):]** このフィールドには、ユーザ テナントの AWS アカウント番号を入力します。

- [アクセスタイプ（Access Type）]：このフィールドで[組織（Organization）]を選択します。

  （注） このテナントに組織タグを割り当てる場合は、以下が適用されます。

  - このフィールドで[組織（Organization）]オプションがグレー表示されている場合は、AWS組織のマスターアカウント（インフラストラクチャテナント）を展開していません。Cloud APIC（インフラテナント）がAWS組織のマスターアカウントに展開されていない場合、テナントに組織タグを割り当てることはできません。Cloud APIC詳細については、「AWS で Cloud APIC を導入する （21 ページ）」を参照してください。
  - 既存の AWS アカウントに**招待された**マスターアカウントが組織に加わる場合、組織テナント用の AWS に設定された `OrganizationAccountAccessRole` IAM ロールがあり、Cloud APIC 関連の許可を使用可能であることを確認してください。詳細については、「AWS Organizations と組織のユーザ テナントのサポート （9 ページ）」を参照してください。

（注） **[クラウド アクセス キー ID (Cloud Access KEY ID)]** フィールドと **[クラウド秘密アクセス キー (Cloud Secret Access Key)]** フィールドは、**[アクセス タイプ（Access Type）]** として **[信頼済み（Trusted）]** を選択している場合、 表示されません。これらのフィールドは、組織テナントには必要ありません。

f) 画面の下部にある**[保存（Save）]** をクリックします。

次のタスク

スキーマの作成 （52 ページ） に進みます。

スキーマの作成

Cisco Cloud APIC に固有ではない一般的な Cisco ACI Multi-Site 手順がいくつかありますが、Cisco ACI Multi-Site を介してオンプレミスサイトと Cisco Cloud APIC サイトを管理している場合は Cisco Cloud APIC の全体的なセットアップの一部として実行する必要があります。ここでは、APIC の Cisco Cloud 全体的なセットアップの一部である Cisco ACI Multi-Site の一般的な手順について説明します。

Cisco Cloud APIC サイトの新しいスキーマを作成する場合は、この項の手順に従ってください。

Cisco Cloud APIC サイトに使用するスキーマがすでにある場合は、これらの手順をスキップして、サイトをスキーマに追加する （56 ページ） に移動することができます。

ステップ 1 メイン メニューで **[スキーマ]** をクリックします。

ステップ 2 [スキーマ] ページで、**[スキーマの追加]** をクリックします。

ステップ 3 [無題スキーマ] ページで、ページの上部にあるテキスト 無題スキーマを、作成するスキーマの名前 (たとえば、 `Cloudbursting スキーマ` に置き換えます。

ステップ 4 左側のペインで **[ロール (Roles)]** をクリックします。

ステップ 5 中央のペインで、**スキーマを作成するエリアをクリックしてテナントを選択してください**をクリックしてください。

ステップ 6 **[テナントの選択]** ダイアログ ボックスにアクセスし、ドロップダウン メニューから 共有テナントの設定（50 ページ） で作成したテナントを選択します。

アプリケーション プロファイルと EPG の設定

この手順では、アプリケーション プロファイルを設定し、2 つの EPG を追加する方法について説明します。1 つはクラウド サイト用、もう 1 つは、プロバイダ コントラクトが 1 つの EPG に関連付けられており、コンシューマ コントラクトが他の EPG に関連付けられている場合です。

ステップ 1 中央のペインで、[アプリケーション プロファイル (Application Profile)] エリアを見つけて、**[+ アプリケーション プロファイル (+ Application profile)]** をクリックします。

ステップ 2 右側のペインで、**[表示名 (DISPLAY NAME)]** フィールドにアプリケーション プロファイルの名前を入力します。

ステップ 3 中央のペインで、**[+ EPG の追加 (+ ADD EPG)]** をクリックして、クラウド サイトの EPG を作成します。

ステップ 4 右側のペインで、**[表示名 (DISPLAY NAME)]** フィールドに EPG の名前を入力します (たとえば `epg1`)。

ステップ 5 オンプレミス サイトの EPG を作成する場合には、中央のペインで、**[+ EPG の追加 (+ ADD EPG)]** をクリックします。

ステップ 6 右側のペインで、**[表示名 (DISPLAY NAME)]** フィールドに EPG の名前を入力します (たとえば `epg2`)。

ステップ 7 VRF を作成します。

a) 中央のペインで、[VRF] エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。

b) 右側のペインで、**[表示名 (DISPLAY NAME)]** フィールドに EPG の名前を入力します (たとえば `vrf1`)。

ステップ 8 **[保存 (SAVE)]** をクリックします。

ブリッジ ドメインの作成と VRF への関連付け

この項の手順に従って、オンプレミス サイトのブリッジ ドメインを作成し、それを VRF に関連付けます。これらの手順は、クラウドのみのスキーマには必要ではないことに注意してください。

ステップ 1 中央のペインで、**[EPG]** まで上にスクロールして戻り、以前にオンプレミス サイト用に作成した EPG をクリックします。

ステップ 2 右側のペインの**[オンプレミス プロパティ (ON-PREM PROPERTIES)]** エリアの **[ブリッジ ドメイン (BRIDGE DOMAIN)]**)] の下で、フィールドに名前を入力し (たとえば、 `bd1`)、**[作成 (create)]** エリアをクリックして新しいブリッジ ドメインを作成します。

ステップ 3 中央のペインで、今作成したブリッジ ドメインをクリックします。

ステップ 4 **[仮想ルーティング/フォワーディング (Virtual Routing & Forwarding)]** フィールドで、アプリケーション プロファイルと EPG の設定 （53 ページ） で作成した VRF を選択します。

ステップ 5 **[サブネット (SUBNETS)]** エリアまで下にスクロールし、 **[GATEEAY (ゲートウェイ)]** 見出しの下の **[サブネット (SUBNET)]** の横にある + をクリックします。

ステップ 6 **[サブネットの追加 (Add Subnet)]** ダイアログで、**[ゲートウェイ IP (Gateway IP)]**アドレスと、追加する予定のサブネットの説明を入力します。このゲートウェイ IP アドレスは、オンプレミスのサブネットのものです。

ステップ 7 **[範囲 (Scope)]** フィールドで、**[外部にアドバタイズ (Advertised Externally)]** を選択します。

ステップ 8 **[保存 (SAVE)]** をクリックします。

コントラクトのフィルタの作成

ステップ 1 中央のペインで、[コントラクト (Contract)] エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。

ステップ 2 右側のペインで、**[表示名 (DISPLAY NAME)]** フィールドにフィルタの名前を入力します。

ステップ 3 **[+ 入力(+ Entry)]** をクリックして、**[エントリの追加 (Add Entry)]** ディスプレイ上のスキーマ フィルタについての情報を入力します。

a) **Name** フィールド (**Add Entry** ダイアログ) のスキーマ フィルタ エントリの名前を入力します。

b) オプション。**Description** フィールドにフィルタの説明を入力します。

c) EPG の通信のフィルタ処理を行うために、必要に応じて詳細を入力します。

たとえば、フィルタを通過する HTTPS トラフィックを許可するエントリを追加するには、次のように選択します。

TYPE: IP、IP PROTOCOL: TCP、および DESTINATION PORT RANGE FROM および DESTINATION PORT range TO: https。

d) **[保存 (SAVE)]** をクリックします。

コントラクトの作成

ステップ 1 中央のペインで、[コントラクト (Contract)] エリアが表示されるまで下方にスクロールし、点線で囲まれたボックスの + をクリックします。

ステップ 2 右側のペインで、**[表示名 (DISPLAY name)]** フィールドにコントラクトの名前を入力します。

ステップ 3 **[範囲 (SCOPE)]** エリアで、VRF の選択をそのままにします。

ステップ 4 **[フィルタ チェーン (FILTER CHAIN)]** エリアで、**[+ フィルタ (+ FILTER)]** をクリックします。

[フィルタ チェーンの追加 (Add Filter Chain)] 画面が表示されます。

ステップ 5 **[名前 (NAME)]** フィールドで、コントラクトのフィルタの作成 （54 ページ） で作成したフィルタを選択します。

ステップ 6 中央のペインで、**[EPG]** までスクロールして戻り、クラウド サイト用に作成した EPG をクリックします。

ステップ 7 右側のペインで、**[+コントラクト (+ CONTRACT)]** をクリックします。

[コントラクトの追加] 画面が表示されます。

ステップ 8 **[コントラクト (contract)]** フィールドで、この手順で以前に作成したコントラクトを選択します。

ステップ 9 **[タイプ (TYPE)]** フィールドで、**コンシューマ**または**プロバイダ**のいずれかを選択します。

ステップ 10 **[クラウドのプロパティ (CLOUD PROPERTIES)]** エリアまでスクロールし、**[仮想ルーティングと転送 (VIRTUAL ROUTING & FORWARDING)]** エリアで、アプリケーション プロファイルと EPG の設定 （53 ページ） で作成した VRF を選択します。

ステップ 11 **[保存 (SAVE)]** をクリックします。

ステップ 12 中央のペインで、**[EPG]** までスクロールして戻り、オンプレミス サイト用に作成した EPG をクリックします。

ステップ 13 右側のペインで、**[+コントラクト (+ CONTRACT)]** をクリックします。

[コントラクトの追加] 画面が表示されます。

ステップ 14 **[コントラクト (contract)]** フィールドで、この手順で以前に作成したコントラクトを選択します。

ステップ 15 **[タイプ (TYPE)]** フィールドで、**[コンシューマ (CONSUMER)]** または **[プロバイダ (PROVIDER)]** を選択します。これは、前の EPG に選択しなかったものです

たとえば、最初の EPG に **[プロバイダ (PROVIDER)]** を選択した場合は、2番目の EPG の **[コンシューマ (CONSUMER)]** を選択します。

ステップ 16 **[クラウドのプロパティ (CLOUD PROPERTIES)]** エリアまでスクロールし、**[仮想ルーティングと転送 (VIRTUAL ROUTING & FORWARDING)]** エリアで、アプリケーション プロファイルと EPG の設定 （53 ページ） で作成したものと同じ VRF を選択します。

サイトをスキーマに追加する

ステップ 1 左側のペインで、**[サイト (Sites)]** の横にある + をクリックします。

ステップ 2 **[サイトの追加 (Add Sites)]** ページで、それぞれの横にあるボックスをオンにして、オンプレミスおよびクラウド サイトをスキーマに追加し、**[保存 (Save)]** をクリックします。

ステップ 3 左側のペインのクラウドサイトの下にあるテンプレートをクリックして、テンプレートのサイト ローカル プロパティを設定します。

ステップ 4 中央のペインで、VRF をクリックします。

ステップ 5 右側のペインの **[サイト ローカル プロパティ (SITE LOCAL PROPERITES)]** 領域で、次の情報を入力します。

a) **[リージョン (region)]** フィールドで、この VRF を導入する Amazon Web サービスのリージョンを選択します。

b) **CIDR**フィールドで、**+CIDR** をクリックします。

[クラウド CIDR の追加（ADD CLOUD CIDR）]ダイアログボックスが表示されます。次の情報を入力します。

- **CIDR**: VPC CIDR 情報を入力します。たとえば、 `11.11.0.0/16`とします。

  CIDR には、Amazon Web Services VPC で使用可能になるすべてのサブネットの範囲が含まれています。

  （注） このフィールドに入力した VPC CIDR 情報は、インフラ VPC CIDR と重複させることはできません。このフィールドに入力した CIDR 情報が、AWS で Cloud APIC を導入する（21 ページ） の ステップ 12 （23 ページ） の **[インフラ VPC プール (Infra VPC Pool)]** フィールドに入力したインフラ VPC CIDR 情報と重複していないことを確認します。

- **[CIDR タイプ (CIDR TYPE)]**: [プライマリ (Primary)] または [セカンダリ (Secondary)] を選択します。これが最初の CIDR の場合は、CIDR タイプとして [プライマリ (Primary)] を選択します。
- **[サブネット追加 (ADD SUBNETS)]**: サブネット情報を入力し、ゾーンを選択してから、チェックマークをクリックします。たとえば、 `11.11.1.0/24` とします。

  サブネットは、各アベイラビリティ ゾーンの CIDR ブロックの範囲内に割り当てます。

c) ウィンドウで **[保存 (Save)]** をクリックします。

AWS でのインスタンスの設定

Cloud APIC のためのエンドポイント セレクタを、Cloud APICGUI または ACI マルチサイト オーケストレータ GUI のいずれか使用して設定する場合には、Cloud APIC のために設定する

エンドポイント セレクタに対応し、AWS 内で必要なインスタンスについても、設定することが必要になります。

このトピックでは、AWS でインスタンスを設定する手順について説明します。Cloud APIC のためのエンドポイント セレクタを設定する前に、または後で、これらの手順を使用して AWS のインスタンスを設定することができます。たとえば、先に AWS のアカウントに移動し、AWS のカスタム タグまたはラベルを作成してから、ACI マルチサイト オーケストレータ のカスタム タグまたはラベルを使用して、エンドポイント セレクタを作成することができます。または、ACI マルチサイト オーケストレータ でカスタムタグまたはラベルを使用してエンドポイント セレクタを作成してから、AWS のアカウントに移動し、AWS のカスタム タグまたはラベルを作成することもできます。

ステップ 1 ACI マルチサイト オーケストレータ GUI または Cisco Cloud APIC GUI を使用してクラウド コンテキスト プロファイルを設定したかどうかを確認します。

クラウド コンテキスト プロファイルは、AWS インスタンス設定プロセスの一部として設定する必要があります。ここで、クラウド コンテキスト プロファイルは、VRF およびリージョンと組なって、そのリージョン内の AWS VPC を表します。Cisco Cloud APIC GUI を使用してクラウド コンテキスト プロファイルを設定すると、VRF やリージョンの設定などの設定情報は、AWS にプッシュされます。同様のアクションは、Cisco Cloud APIC を ACI マルチサイト オーケストレータ GUI を使用して設定した場合にも生じます。ここで、これらのクラウド コンテキスト プロファイル設定は、Cisco Cloud APIC 設定プロセスの一部として ACI マルチサイト オーケストレータ GUI によって設定され、AWS にプッシュされます。

- Cisco Cloud APIC を ACI マルチサイト オーケストレータ GUI を使用して設定する場合は、クラウド コンテキスト プロファイルを手動で設定する必要はありません。VRF やリージョン設定など、特定のクラウド コンテキスト プロファイル設定は、Cisco Cloud APIC 設定プロセスの一部として、前のセクションで実行した ACI マルチサイト オーケストレータ GUI により設定され、AWS にプッシュされます。
- クラウド コンテキスト プロファイルを Cisco Cloud APIC GUI を使用して設定する場合には、『*Cisco Cloud APIC User Guide, Release 4.1(x)*』で説明されている手順に従い、GUI または REST API を使用して、クラウド コンテキスト プロファイルを設定してください。

ステップ 2 クラウド コンテキスト プロファイルの設定を確認し、AWS インスタンスで使用する設定を決定します。

a) まだログインしていない場合は、Cisco Cloud APIC にログインします。

b) **[ナビゲーション (Navigation)]** メニューで、**[アプリケーション管理 (Application Management)]** タブを選択します。

[アプリケーション管理 (Application Management)] タブを展開すると、サブタブ オプションのリストが表示されます。

c) **[クラウド コンテキスト プロファイル (Cloud Context Profiles)]** サブタブ オプションを選択します。

Cisco Cloud APIC 用に作成したクラウド コンテキスト プロファイルのリストが表示されます。

d) この AWS インスタンス設定プロセスの一部として使用するクラウド コンテキスト プロファイルを選択します。

リージョン、VRF、IP アドレス、サブネットなど、このクラウド コンテキスト プロファイルのさまざまな設定パラメータが表示されます。AWS インスタンスを設定するときには、このウィンドウに表示される情報を使用します。

ステップ 3 まだログインしていない場合は、 Cisco Cloud APICユーザテナントの Amazon Web Services アカウントにログインします。

ステップ 4 **[サービス (Services)]** > **EC2** > **インスタンス (Instances)]** > **[インスタンスの起動 (Launch Instance)]** に移動します。

ステップ 5 **[Amazon マシン イメージ (AMI)の選択 (Choose Amazon Machine Image (AMI))]** ページで、Amazon マシン イメージ (AMI) を選択します。

ステップ 6 **[インスタンス タイプの選択 (Choose An Instance type)]** ページで、インスタンス タイプを選択し、**[インスタンスの詳細の設定 (Configure instance Detail)]** をクリックします。

ステップ 7 **[インスタンスの詳細の設定 (Configure instance Detail)]** ページで、該当するフィールドに必要な情報を入力します。

- **[ネットワーク (Network)]** フィールドで、Cloud APIC VRF を選択します。

  これは、この AWS インスタンス設定プロセスの一部として使用しているクラウド コンテキスト プロファイルに関連付けられている VRF です。

- **[サブネット (Subnet)]** フィールドに、サブネットを入力します。

- パブリック IP を使用する場合は、**[パブリック IP の自動割り当て (Auto Assign public IP)]** フィールドで、スクロールダウンメニューから **[有効 (Enable)]** を選択します。

ステップ 8 **[インスタンスの詳細の設定 (Configure Instance Details)]** ページに必要な情報を入力したら、**[ストレージを追加 (Add Storage)]** をクリックします。

ステップ 9 **[ストレージの追加 (Add Storage)]** ページで、デフォルト値を受け入れるか、必要に応じてこのページでストレージを設定し、**[タグの追加 (add Tags)]** をクリックします。

ステップ 10 **[タグの追加 (Add Tags)]** ページで、**[タグの追加 (add Tag)]** をクリックし、このページの該当するフィールドに必要な情報を入力します。

（注） これらの手順の後の部分で、エンドポイントセレクタのタイプに対して IP アドレス、リージョン、またはゾーンを使用する場合は、このページに情報を入力する必要はありません。このような状況では、AWS でインスタンスを開始すると、Cloud APIC によって IP アドレス、リージョン、またはゾーンが検出され、エンドポイントが EPG に割り当てられます。

- **[キー (Key):]** これらの手順で後で追加するエンドポイント セレクタのタイプのカスタム タグを作成するときに使用するキーを入力します。

- **[値 (Value):]** このキーで使用する値を入力します。

- **[インスタンス (Instance):]** このフィールドのチェックボックスをオンにします。

- **[ボリューム (Volume):]**このフィールドのチェックボックスをオンにします。

たとえば、これらの手順で後ほど、エンドポイントセレクタの特定のビルディングのカスタムタグを作成する予定の場合 (building6 など) は、このページの次のフィールドに次の値を入力できます。

- **[キー (Key):]** ロケーション
- **[値 (value):]** building6

ステップ 11 **[確認して起動する（Review and Launch）** をクリックします。

既存のキー ペアを選択するか、新しいキー ペアを作成します。キーペアの ページが表示されます。後ほどインスタンスに ssh 接続する場合は、このページの情報を使用します。

エンド ポイント セレクタの追加

Cisco Cloud APICでは、クラウドEPGは、同じセキュリティ ポリシーを共有するエンドポイントの集合です。クラウドEPGは、1つまたは複数のサブネット内にエンドポイントを持つことができ、VRF に関連付けられます。

Cisco Cloud APIC には、エンドポイントをクラウドEPGに割り当てるために使用される、エンドポイント セレクタと呼ばれる機能があります。エンドポイント セレクタは、基本的に言って、Cisco ACI によって管理される AWS VPC に割り当てられたクラウド インスタンスに対して実行される一連のルールです。エンドポイント インスタンスに一致するエンドポイント セレクタ ルールは、そのエンドポイントをクラウドEPGに割り当てます。エンドポイント セレクタは、Cisco ACI で使用可能な属性ベースのマイクロセグメンテーションに似ています。

エンドポイント セレクタは、 Cisco Cloud APIC GUI またはACI マルチサイト オーケストレータ GUI のいずれかを使用して設定できます。2 つの GUI 間で使用可能なオプションにはわずかな違いがありますが、エンドポイントセレクタを追加するための一般的な概念と全体的な手順は、基本的にこの 2 つの間で同じです。

このセクションの手順では、 ACI マルチサイト オーケストレータ GUI を使用してエンドポイント セレクタを設定する方法について説明します。Cisco Cloud APIC GUI を使用したエンドポイント セレクタの設定の詳細については、『*Cisco Cloud APIC User Guide, Release 4.1 (x)*』を参照してください。

ステップ 1 Cisco Cloud APIC のエンドポイント セレクタに使用できる Amazon Web Services サイトから、必要な情報を収集します。

手順については、AWS でのインスタンスの設定 （56 ページ）を参照してください。

（注） これらの手順は、最初に AWS でインスタンスを設定してから、その後に Cisco Cloud APIC のエンドポイントセレクタを追加することを前提としています。ただし、AWS でのインスタンスの設定 （56 ページ） で説明されているように、最初に Cisco Cloud APIC のエンドポイント セレクタを追加してから、この AWS インスタンスの設定手順を、これらのエンドポイント セレクタの手順の最後で実行することもできます。

ステップ 2 ログインしていない場合は、ACI マルチサイト オーケストレータ にログインします。

ステップ 3 左側のペインで、**[スキーマ (schema)]** をクリックし、以前に作成したスキーマを選択します。

ステップ 4 エンドポイント セレクタを作成する方法を決定します。

- 今後追加される、任意のクラウドサイトに適用できるエンドポイントセレクタを作成するには、次の手順を実行します。

  1. 左側のペインで、テンプレートを選択したままにします。

     これらの手順で特定のサイトを選択しないでください。

  2. 中央のペインで、クラウド サイト用に作成した EPG を選択します。

  3. 右側のペインの **[クラウドのプロパティ (CLOUD PROPERITES)]** 領域で、**+** (**[セレクタ (SELECTORS)]** の横にあるもの) をクリックして、エンドポイント セレクタを設定します。

  4. **[新しいエンドポイント セレクタの追加 (Add New End Point selector)]** ダイアログで、**[エンドポイント セレクタ名 (END POINT SELECTOR NAME)]** フィールドに、このエンドポイント セレクタで使用する分類に基づいて名前を入力します。

  5. **[+ 式 (Expression)]** をクリックし、エンドポイント セレクタのタイプを選択します。

     このように作成されたエンドポイントセレクタの場合、[キー (Key)] フィールドで使用できるオプションは `[EPG]` のみです。

  6. ステップ 5 （61 ページ） に進みます。

- このクラウド サイト専用のエンドポイント セレクタを作成するには、次の手順を実行します。

  1. 左ペインで、クラウド サイトを選択します。

  2. 中央のペインで、クラウド サイト用に作成した EPG を選択します。

  3. 右側のペインの **[サイトのローカルのプロパティ (SITE LOCAL PROPERITES)]** 領域の **[セレクタ (SELECTOR)]**領域で、**+** (**[セレクタ （SELECTOR)]** の横にあるもの) をクリックして、エンドポイント セレクタを設定します。

  4. **[新しいエンドポイント セレクタの追加 (Add New End Point selector)]** ダイアログで、**[エンドポイント セレクタ名 (END POINT SELECTOR NAME)]** フィールドに、このエンドポイント セレクタで使用する分類に基づいて名前を入力します。

     たとえば、IP サブネット分類のエンドポイントセレクタの場合は、`[IP-Subnet-EPSelector]` などの名前を使用できます。

  5. **[+ 式 (Expression)]** をクリックし、エンドポイント セレクタで使用するキーを選択します。

     - **[IP アドレス (IP Address)]**): IP アドレスまたはサブネットによって選択するために使用されます。
     - **[リージョン (Region)]**: エンドポイントの AWS リージョンで選択するために使用されます。
     - **[ゾーン (Zone)]**: エンドポイントの AWS アベイラビリティ ゾーンによって選択するために使用されます。
     - エンドポイントセレクタのカスタム タグを作成する場合は、**[検索または作成のために入力 (Type to search or create)] フィールド**で入力を開始してカスタム タグまたはラベルを入力

し、新しいフィールドで **[作成 (Create)]** をクリックして、新しいカスタム タグまたはラベルを作成します。

AWS にタグを追加するときに、これらの手順の前の例を使用すると、以前に AWS で追加したロケーション タグと一致するように、このフィールドにカスタム タグのロケーションを作成できます。

ステップ 5 **[演算子 (Operator)]** フィールドで、エンドポイント セレクタに使用する演算子を選択します。

（注） 4.2 (1) より前のリリースでは、オプションとして **[キーが存在 (Key Exist]]** と **[キーが存在しない (Key Not Exist)]** を使用していましたが、現在では**[キーを持つ (Has Key)]** と **[キーを持たない (Does Not Have Key)]** になっています。異なるのはオプションの名前だけで、機能はどちらのオプションのセットでも同じです。

次のオプションがあります。

- **[等しい (Equals)]**: [値 (value)] フィールドに 1 つの値がある場合に使用します。
- **[等しくない (Not Equals)]**: 値フィールドに 1 つの値がある場合に使用されます。
- **[の中にある (In)]**: [値 (Value)] フィールドに複数のカンマ区切り値がある場合に使用します。
- **[の中にない (Not In)]**: 値フィールドに複数のカンマ区切り値がある場合に使用されます。
- **[キーを持つ (Has Key)]**: 式にキーのみが含まれている場合に使用されます。
- **[キーを持たない (Does Not Have Key)]**: 式にキーのみが含まれている場合に使用されます。

ステップ 6 **[値 (value)]** フィールドで、2 つ前のフィールドに対して行った選択に基づいて、エンドポイント セレクタに使用する値を選択します。**[値 (Value)]** フィールドには、複数のカンマ区切りのエントリを含めることができます。このフィールドのエントリの間には論理 OR があるものとみなされます。

（注） **[キーを持つ (Has Key)]** または **[キーを持たない (Does Not Have Key)]**を選択していない場合には、[演算子 (Operator)] フィールドは表示されません。

たとえば、エンドポイント セレクタに、`us-west-1a` など特定の Amazon Web サービスのアベイラビリティ ゾーンを設定する場合には、この画面で次の項目を選択します。

- **[キー (Key):]** Zone
- **[演算子 (Operator):]** Equals
- **[値 (Value):]** us-west-1a

別の例として、これらのフィールドで次の値を使用したとします。

- **[キー (Key):]** IP
- **[演算子 (Operator):]** Has Key
- **[値 (Valuse):]**は、演算子 (Operator)] フィールドで [Has Key] が使用されているため、使用できません。

EPG ルールは、この状況で IP アドレスを持つすべてのエンドポイントに適用されます。

最後の例として、これらのフィールドで次の値を使用したとします。

- **[キー (Key):]** custom tag: Location
- **[演算子 (Operator):]** Has Key
- **[値 (Valuse):]**は、演算子 (Operator)] フィールドで [Has Key] が使用されているため、使用できません。

この場合、EPG ルールは、AWS タグキーとして Location を持つすべてのエンドポイントに、ロケーションの値に関係なく適用されます。

ステップ 7 このエンドポイント セレクタ式の作成が完了したら、チェックマークをクリックします。

ステップ 8 追加のエンドポイント セレクタ式を作成するかどうかを決定します。

単一のエンドポイント セレクタで複数の式を作成した場合、それらの式の間には論理 AND があるものとみなされます。たとえば、1つのエンドポイントセレクタで2つの式セットを作成したとします。

- エンドポイント セレクタ 1、式 1:
  - **[キー (Key):]** Zone
  - **[演算子 (Operator):]** Equals
  - **[値 (Value):]** us-west-1a
- エンドポイント セレクタ1、式 2:
  - **[キー (Key):]** IP
  - **[演算子 (Operator):]** Equals
  - **[値 (Value):]** 192.0.2.1/24

この場合、これらの式の両方が真になる場合 (アベイラビリティ ゾーンが us-west-1a で、IP アドレスがサブネット 192.0.2.1/24 に属している場合) に、そのエンドポイントはクラウド EPG に割り当てられます。

このエンドポイントセレクタで作成するすべての式を追加した後で、チェックマークをクリックします。

ステップ 9 このエンドポイント セレクタの式の作成が完了したら、**[保存 (SAVE)]** をクリックします。これは **[新しいエンドポイント セレクタの追加 (Add New End Point selector)]** の右下隅にあります。

EPGの下で複数のエンドポイントセレクタを作成した場合は、それらのエンドポイントセレクタの間には論理 OR があるものとみなされます。たとえば、前のステップで説明したようにエンドポイント セレクタ 1 を作成し、次に、次に示すように 2 番目のエンドポイント セレクタを作成したとします。

- エンドポイント セレクタ 2、式 1:
  - **[キー (Key):]** Region
  - **[演算子 (Operator):]** In

- **[値 (Value):]** us-east-1a, us-east-2

その場合、次のようになります。

- アベイラビリティ ゾーンが us-west-1a で、IP アドレスが 192.0.2.1/24 サブネットに属している (エンドポイント セレクタ 1 の式)

  または

- リージョンが us-east-1a または us-east-2 (エンドポイント セレクタ 2 の式) のいずれかである

その場合、エンドポイントがクラウド EPG に割り当てられます。

ステップ 10 エンドポイント セレクタの作成が完了したら、右上隅の **[保存 (SAVE)]** をクリックします。

ステップ 11 画面の右上隅にある **[サイトに展開 (DEPLOY TO SITES)]** ボタンをクリックして、スキーマをサイトに展開します。

`[正常に展開 (Successfully Deployed)]` されたというメッセージが表示されます。

次のタスク

Cisco ACI Multi-Site 設定の検証 （63 ページ） の手順を使用して、Cisco ACI マルチサイト エリアが正しく設定されていることを確認します。

Cisco ACI Multi-Site 設定の検証

このトピックの手順を使用して、ACI マルチサイト オーケストレータ に入力した設定が正しく適用されていることを確認します。

ステップ 1 Cloud APIC にログインし、次のことを確認します。

a) [ダッシュボード (Dashboard)] をクリックし、オンプレミス接続ステータスおよびリージョン間接続ステータスボックスの情報を使用して、次のことを確認します。

- トンネルは、AWS 上の Cisco Cloud Services Router 1000V から、オンプレミスの ISN (IPsec ターミネーションポイント)、およびユーザ VPC の VGW に対して動作しています。
- OSPF ネイバーが Cisco Cloud サービス ルータと ISN オンプレミス デバイスの間で起動していることを示します。
- VRF の BGP EVPN ルートにはクラウドとオンプレミスのルートが表示され、クラウドルートは ACI スパイン スイッチの BGP EVPN を介して入力されます。

b) [アプリケーション管理 (Application Management)] → [テナント] をクリックし、テナントが正しく設定されていることを確認します。

c) [アプリケーション管理(Application Management)] → [アプリケーションプロファイル] をクリックし、アプリケーションプロファイルが正しく設定されていることを確認します。
d) [アプリケーション管理 (Application Management)] → [EPG] をクリックし、EPG が正しく設定されていることを確認します。
e) [アプリケーション管理 (Application Management)] → [コントラクト] をクリックし、契約が正しく設定されていることを確認します。
f) [アプリケーション管理 (Application Management)] → [VRF] をクリックし、VRF が正しく設定されていることを確認します。
g) [アプリケーション管理 (Application Management)] → [クラウド コンテキスト Cloudプロファイル] をクリックし、クラウド コンテキスト プロファイルが正しく設定されていることを確認します。
h) [クラウド リソース (Cloud Resources)] → [リージョン] をクリックし、リージョンが正しく設定されていることを確認します。
i) [クラウド リソース (Cloud Resources)] → [VPC] をクリックし、VPC が正しく設定されていることを確認します。
j) [クラウド リソース (Cloud Resources)] → [クラウド エンドポイント] をクリックし、クラウド エンドポイントが正しく設定されていることを確認します。
k) [クラウド リソース (Cloud Resources)] → [ルータ] をクリックし、CSR が正しく設定されていることを確認します。

ステップ 2 オンプレミスの APIC サイトにログインし、APIC のスキーマを確認します。

ACI マルチサイト オーケストレータ で設定した共有テナントが APIC のテナントエリアに表示され、 ACI マルチサイト オーケストレータ スキーマから展開された VRF と EPG がオンプレミス APIC で設定されていることが確認できます。

ステップ 3 コマンド ラインから、AWS の Cisco Cloud サービス ルータ 1000V で VRF が 正しく作成されていることを確認します。

```
show vrf
```

テナント`t1`と VRF `v1`が ACI マルチサイト オーケストレータ から展開されている場合、CSR の出力は次のようになります。

```
Name                             Default RD            Protocols   Interfaces
t1:v1                            64514:3080192         ipv4        BD1
                                                                   Tu4
                                                                   Tu5
```

ステップ 4 コマンド ラインから、AWS サービス ルータ 1000V と ISN オンプレミス デバイスの間 Cisco Cloud でトンネルがアップしていることを確認します。

AWS または ISN オンプレミスのデバイスで、Cisco Cloud サービス ルータ 1000V で次のコマンドを実行できます。

```
show ip interface brief | inc Tunnel
```

以下のような出力が表示されます。

```
Interface        IP-Address        OK?        Method        Status        Protocol
Tunnel1          1.2.3.22          YES        manual        up            up
Tunnel2          1.2.3.30          YES        manual        up            up
```

```
Tunnel3          1.2.3.6          YES        manual        up            up
Tunnel4          1.2.3.14         YES        manual        up            up
```

ステップ 5 コマンド ラインから、OSPF ネイバーが AWS 上の Cisco Cloud サービス ルータ 1000V と ISN オンプレミス デバイスの間でアップしていることを確認します。

show ip ospf neighbor

以下のような出力が表示されます。

```
Neighbor ID      Pri              State      Dead Time     Address       Interface
10.200.10.201    0                FULL/ -    00:00:36      1.2.3.13      Tunnel4
20.30.40.50      0                FULL/ -    00:00:36      1.2.3.29      Tunnel2
10.202.101.202   0                FULL/ -    00:00:38      1.2.3.5       Tunnel3
```

ステップ 6 コマンド ラインから、オンプレミスの BGP EVPN ネイバーが Cisco Cloud サービス ルータ 1000V に存在することを確認します。

show bgp l2vpn evpn summary

以下のような出力が表示されます。

```
Neighbor     V     AS    MsgRcvd   MsgSent   TblVer   InQ    OutQ   Up/Down   State/PfxRcd
10.1.1.2     4     100   139       137       99       0      0      01:30:36  6
```

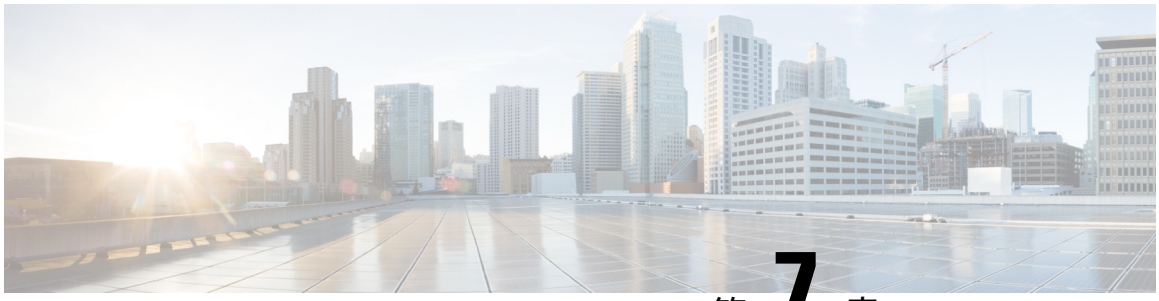
ステップ 7 コマンド ラインから、VRF の BGP ルートにクラウドとオンプレミスの両方のルートが表示されていることを確認します。

（注） 現在 Cloud APIC のワークフローでは、VRF は、対応する VPC が AWS で作成されるまで、Cisco Cloud サービスルータ 1000V で設定されません。

show ip route vrf t1:v1

以下のような出力が表示されます。

```
B     129.1.1.5/32[20/0] via 10.11.0.34, 01:12:41, BD|1
B     130.1.0.0/16[20/100] via 131.254.4.5, 01:09:55
```



第 7 章

Cisco Cloud APIC GUI について

Cisco Cloud APIC GUI の操作

インストール後、これを使用してAmazon Web Services（AWS）またはMicrosoft Azureパブリッククラウドに拡張（ACI）ポリシーを適用できます。Cisco Cloud APICCisco Application Centric Infrastructureこれは GUI を使用して行います。Cisco Cloud APIC

GUI では、テナントを作成し、アプリケーションプロファイル、エンドポイントグループ（EPG）、コントラクト、フィルタ、および VRF を設定できます。Cisco Cloud APICトポロジ、設定、およびリソースを表示することもできます。Cisco Cloud APIC

を使用して設定手順を実行します。インテント機能。インテント機能の使用方法については、を参照してください。Cisco Cloud APIC コンポーネントの設定 （68 ページ）また、『*Cisco Cloud APIC User Guide*』の「Understanding the Cisco Cloud APIC GUI アイコン」の項も参照してください。

の基本的なタスクを実行する手順は、通常の手順とは異なります。Cisco Cloud APICCisco APICただし、テナントの機能、アプリケーションプロファイル、およびその他の要素は同じです。Cisco APIC詳細については、Cisco.com の『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

左側のナビゲーション ペインで設定やその他の情報を表示します。**[ダッシュボード（デフォルト ビュー）（Dashboard (the default view)]**、**[トポロジー（Topology）]**、**[アプリケーション管理（Application Management）]**、**[クラウド リソース（Cloud Resources）]**、**[オペレーション（Operations）]**、**[インフラストラクチャ（Infrastructure）]**、および**[管理（Administrative）]**を選択できます。

アイコンの詳細については、Cisco.com の 『Cisco User Guide』の「Understanding the GUI アイコン」の項を参照してください。Cisco Cloud APIC*Cisco Cloud APIC*

Cisco Cloud APIC コンポーネントの設定

このセクションでは、テナント、アプリケーションプロファイル、およびエンドポイントグループ（EPG）の作成など、主要なタスクの実行の概要について説明します。Cisco Cloud APIC

始める前に

Cisco Cloud APIC がインストールされている必要があります。このガイドの前のインストールの項を参照してください。

ステップ 1 Cisco Cloud APIC にログインします。

ステップ 2 **[ダッシュボード（Dashboard）]**ペインの右上で、ブルズアイを指す矢印の付いたアイコンをクリックします。

このアイコンは、**[インテント（Intent)]** アイコンまたは機能と呼ばれることがあります。

ステップ 3 **[何をしますか。（What do you want to do?）]** ウィンドウで、検索ウィンドウに用語を入力して、オプションのリストを表示します。

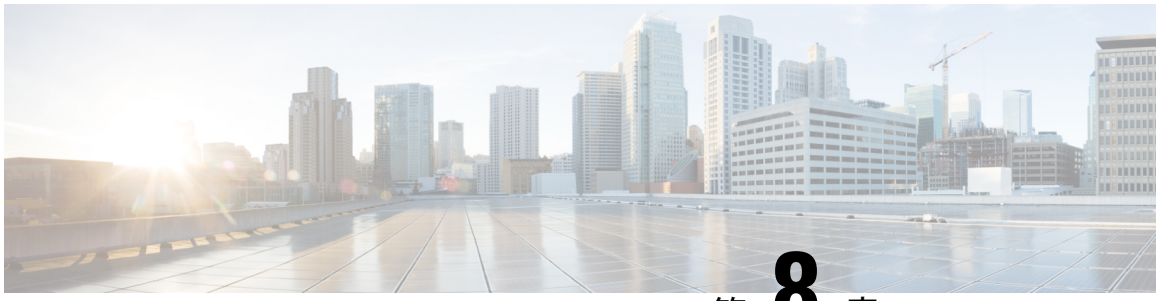
たとえば、テナントを設定する場合は、検索ウィンドウに tenant と入力します。検索は、テナントの作成と設定に関連するタスクのリストを返します。

ステップ 4 タスクをクリックし、開いたウィンドウで設定手順を実行します。

次のタスク

左側のナビゲーションペインで設定を確認できます。**[ダッシュボード（Dashboard）]** ペインの左上にあるハンバーガーアイコンをクリックして、ペインを展開します。該当する見出しを展開して設定を表示します。

たとえば、テナントを設定した場合は、**[アプリケーション管理（Application Management）]** を展開し、**[テナント（Tenants）]** をクリックします。テナントに関する情報が中央の作業ウィンドウに表示されます。



第 8 章

システムのアップグレード、ダウングレード、またはリカバリの実行

特記事項

のインストール、アップグレード、またはダウングレード手順に関する重要な注意事項を次に示します。Cisco Cloud APIC

- リリース 5.0（x）から以前のリリースにダウングレードすると、CSR が下位のリリースにダウングレードされるため、CSR で一部のトンネルが「ダウン」状態になることがあります。これは、AWS アカウントの古い VPN リソースがクリーンアップされなかったために発生する可能性があります。

  この問題を修正するには、古い VPN 接続を手動でクリーンアップします。

- に記載されているように、リリース 5.0（x）以降では、導入でサポートされるインスタンスタイプが変更されています。AWS パブリック クラウドの要件 （16 ページ） 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。

  4.2（x）リリースからリリース 5.0（x）以降にアップグレードする場合、ポリシーベースのアップグレードはサポートされません。これは、ポリシーベースのアップグレードではインスタンスタイプを変更できないためです。代わりに、これらのアップグレードでは、

に示す移行手順を使用してアップグレードする必要があります。移行ベースのアップグレード （71 ページ）

- 4.2（x）リリースからリリース5.0（x）以降にアップグレードする場合、atomic での replace オプションを使用した設定のインポートはサポートされません。手順のこの時点で、**[復元設定（Restore Configuration）]**領域で次のように選択します。
  - **[復元タイプ（Restore Type）]** フィールドで、**[結合（Merge）]** を選択します。
  - **[復元モード（Restore Mode）]** フィールドで、**[ベスト エフォート（Best Effort）]** を選択します。

この制限は、4.2（x）リリースからリリース 5.0（x）以降へのアップグレードにのみ適用されます。リリース5.0（x）から以降のリリースにアップグレードする場合、これらの制限は適用されません。

ソフトウェアのアップグレード

Cisco Cloud APIC ソフトウェアのアップグレードに使用する方法は、状況によって異なります。

- 4.2（x）リリースからリリース 5.0（x）にアップグレードする場合は、移行ベースのプロセスを使用してソフトウェアをアップグレードします。これらの指示については、移行ベースのアップグレード （71 ページ） にアクセスしてください。

注 で説明したように、アップグレードに使用したのと同じ移行ベースの手順をシステムリカバリにも使用できます。システム リカバリの実行 （81 ページ）

- リリース 5.0(1) からリリース 5.0(2) にアップグレードする場合は、ポリシーベースのプロセスを使用してソフトウェアをアップグレードします。これらの指示については、ポリシーベースのアップグレード （77 ページ） にアクセスしてください。

注 リリース 5.0(1) からリリース 5.0(2) へのポリシーベースのアップグレードが何らかの理由で機能しない場合は、に記載されている移行ベースのプロセスを使用してリリース 5.0(1) からリリース 5.0(2) にアップグレードできます。移行ベースのアップグレード （71 ページ）

CSR のアップグレード

Cisco Cloud APIC ソフトウェアのアップグレードに使用する方法に関係なく、クラウド APIC ソフトウェアをアップグレードするたびに、クラウドサービスルータ（CSR）もアップグレードする必要があります。

- リリース 5.2(1) より前のリリースでは、Cisco Cloud APIC のアップグレードをトリガーするたびに CSR が自動的にアップグレードされます。
- リリース 5.2(1) 以降では、Cisco Cloud APIC のアップグレードとは関係なく、CSR のアップグレードをトリガーし、それらの CSR のアップグレードをモニタできます。これは、管理プレーン（Cisco Cloud APIC）とデータプレーン（CSR）のアップグレードを分割できるため、トラフィック損失を削減するのに役立ちます。

詳細については、「クラウドサービスルータのアップグレードのトリガー （81 ページ）」を参照してください。

移行ベースのアップグレード

次の項では、トラフィック フローを失わずに 4.2(x) リリースからリリース5.0(x) 以降にアップグレードできる移行手順について説明します。

移行手順を使用したクラウドAPICソフトウェアのアップグレード

この項では、の4.2（x）リリースからリリース5.0（x）以降にアップグレードする場合に使用する移行手順を示します。Cisco Cloud APICこの移行によるトラフィックへの影響はありません。

ステップ 1 暗号化パスフレーズ制御が有効になっていない場合は、有効にします。

a) クラウドAPIC GUI で、**[インフラストラクチャシステム設定（Infrastructure System Configuration）]**

デフォルトでは、**[General]** タブが表示されます。そうでない場合は、**[General]** タブをクリックします。

b) 暗号化されたパスフレーズ制御がすでに有効になっているかどうかを確認します。

- [Global AES Encryption]領域で、[Encryption]フィールドと[Key Configured]フィールドの下に[Yes]と表示されている場合は、暗号化されたパスフレーズ制御がすでに有効になっています。ステップ 2 （72 ページ） に進みます。
- [Encryption]フィールドと[Key Configured]フィールドの下に[Yes]と表示されない場合は、次の手順を実行します。

1. [Global AES Encryption]領域の右上にある鉛筆アイコンをクリックします。

   [Global AES 暗号 Settings] ウィンドウが表示されます。

2. [Encryption：Enabled]エリアの横にあるボックスをクリックし、[Passphrase / Confirm Passphrase]フィールドにパスフレーズを入力して、ウィンドウの下部にある[Save]をクリックします。

ステップ 2 既存の Cloud APIC 設定をバックアップします。

クラウドAPICの設定をバックアップするには、さまざまな方法があります。詳細については、『Cloud APIC for AWS Users Guide』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リモートバックアップを使用する場合は、最初にリモートロケーションを追加する必要があることに注意してください。

ステップ 3 AWS infraアカウントからCloud APIC EC2インスタンスを終了します。

a) まだログインしていない場合は、Cloud APIC インフラ テナントの Amazon Web Services アカウントにログインし、AWS 管理コンソールに移動します。

https://signin.aws.amazon.com/

https://console.aws.amazon.com/

b) AWS 管理コンソールの EC2 ダッシュボードの**インスタンス**に移動します。

c) クラウドAPICインスタンスを見つけます。

クラウドAPICのインスタンスタイプとして**m4.2xlarge**が表示されます。これは5.0(1)より前のリリースでは正しいインスタンスタイプです。

d) Cloud APICインスタンスの横にあるチェックボックスをオンにして選択し、[Actions Instance State Terminate]をクリックします。

[Terminate Instances]ポップアップウィンドウで、[Yes、Terminate]を選択してこのインスタンスを終了します。

[Instances]ウィンドウが再表示され、クラウドAPICインスタンスの[Instance State]行のステータスが「shutting-down」に変わります。ここでCloud APICインスタンスを終了しても、Cloud APICのトラフィックはドロップされません。

ステップ 4 AWS Marketplace の Cloud APIC ページに移動します。

http://cs.co/capic-aws

ステップ 5 **[引き続きサブスクライブする（Continue to Subscribe）]** をクリックして登録します。

ステップ 6 [Subscribe to this software]ページで、[Continue to Configuration]ボタンをクリックします。

[このソフトウェアを設定 (Configure this software)] ページが表示されます。

ステップ 7 以下のパラメータを選択します。

- **[デリバリー方法（Delivery Method）:]** Cisco Cloud APIC クラウド形成テンプレート (デフォルトで選択)
- ソフトウェアバージョン：CloudAPICソフトウェアの適切なバージョンを選択します（例：5.0.1k）。
- **[リージョン (Region):]** クラウド APIC が展開されるリージョン

ステップ 8 **[続行して起動 (Continue to Launch)]** ボタンをクリックします。

[このソフトウェアの起動 (Launch this software)] ページが表示され、設定の概要が表示され、クラウド形成テンプレートを起動できます。

ステップ 9 **[アクションの選択（Choose Action）]** フィールドで、**[CloudFormation の起動（Launch CloudFormation）]** を選択し、**[起動（Launch）]** をクリックすると、すでに正しい Amazon S3 テンプレート URL が入力されている適切なリージョン内の [CloudFormation サービス] にダイレクトに移動します。**[テンプレートの指定（Specify Details）]** ページが、**[スタックの作成（Create stack）]** ページ内に表示されます。

ステップ 10 [テンプレートの指定（Specify template）]ページで、次の選択を行います。

- 前提条件-[テンプレートの準備（Prepare template）]フィールド：デフォルトの[テンプレートの準備（Template is ready）]オプションを選択したままにします。
- テンプレート領域の指定：
  - [テンプレートソース（Template source）]フィールドで、デフォルトのAmazon S3 URLオプションを選択したままにします。
  - [Amazon S3 URL]フィールドで、自動的に生成されたエントリをそのままにします。
  - [デザイナーで表示（View in Designer）]をクリックします。

ステップ 11 画面の下半分のtemplate1領域：

- [テンプレート言語の選択]を[JSON]のままにします。
- 1行目のテキスト文字列の先頭にカーソルを置き、Shiftキーを押しながらウィンドウの一番下までスクロールして、ウィンドウ内のテキスト文字列全体を選択し、このウィンドウ内のすべてのテキストをコピーします（Ctrl + Cを押すか、右クリックして **[コピー（Copy）]** を選択します）。

ステップ 12 ローカルコンピュータで、適切なフォルダに移動し、一意の名前を付けてテキストファイルを作成し、コピーしたテキスト文字列をテキストファイルに貼り付けます。

これはリリース5.0（1）のCloud APIC CFTで、M5.2xlargeインスタンスタイプがあります。

ステップ 13 テキストファイルを保存してテキストエディタを終了します。

ステップ 14 リリース5.0（1）のCloud APIC CFTをAWSにアップロードします。

a) AWS CloudFormation コンソールにログインします。

https://console.aws.amazon.com/cloudformation

b) AWS CloudFormationダッシュボードで、既存のCloud APICスタックをクリックし、[**Update**]をクリックします。

c) **Update Stack**ウィザードの **[Prepare template]** 画面で、**[Replace current template]** を選択します。

[テンプレート領域の指定（Specify template area）] が表示されます。

d) **Update Stack**ウィザードの[**Specify template**]領域で、**[Upload a template file]** を選択します。

[テンプレート ファイルのアップロード（Upload a template file）] のオプションが表示されます。

e) [Upload a template file]オプションの下にある[Choose file]をクリックし、リリース5.0（1）用のCloud APIC CFTを作成した領域に移動します。

f) リリース5.0（1）のCloud APIC CFTを選択し、[**Next**]をクリックします。

g) [**スタックの詳細の指定**（Specify stack details）]画面で、画面下部の[**その他のパラメータ**（Other parameters）]領域に表示されるインスタンスタイプが**m5.2xlarge**に正しく設定されていることを確認し、[次へ（**Next**）]をクリックします。

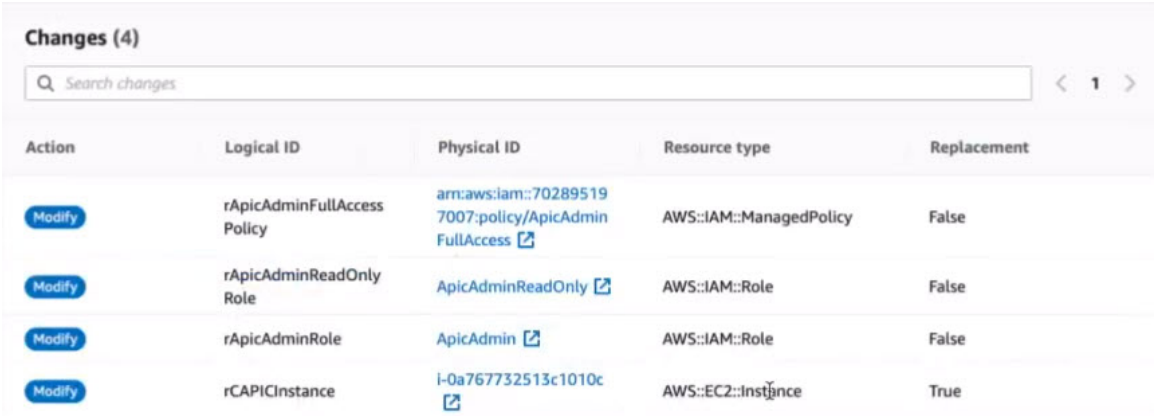
この手順では、インスタンスタイプを**m4.2xlarge**に変更しないでください。

h) **[スタック オプションの設定（Configure stack options）]** 画面で、**[次へ（Next）]** をクリックします。

i) [**Review**]画面で、[**Update stack**]をクリックします。

この時点で、次のアクションが実行されます。

- AWS infraは、更新される3つのIAMリソースを検出します（[Replacement]列に[False]と表示されます）。
- AWS infraは、置き換えられるEC2インスタンスを1つ検出します（[Replacement]列に[True]と表示されます）。



これにより、以前と同じパブリックIPアドレスを使用して、リリース5.0（1）イメージの新しいCloud APICインスタンスが起動します。AWS Management ConsoleのEC2ダッシュボードで[インスタンス（Instances）]に戻ることで、新しいクラウドAPICインスタンスの起動の進行状況を確認できます。

ステップ 15 **インスタンスの状態**が[**実行**中（Running）]に変化した場合は、以前に行ったようにクラウドAPICにログインできます。

クラウドAPICは、この時点で設定なしで起動します。

（注） ログインしようとしたときに、RESTエンドポイントのユーザ認証データストアが初期化されていないなどのエラーメッセージが表示された場合は、このファブリックノードのファブリックメンバーシップステータスを確認し、数分待ってから数分後に再試行してください。ログインするためにページを更新する必要がある場合もあります。

ステップ 16 同じ暗号化パスフレーズが使用可能です。

a) クラウド APIC GUIで、[インフラストラクチャ システム設定（Infrastructure System Configuration）]に移動します。

デフォルトでは、[一般（General）]タブが表示されます。そうでない場合は、[一般（General）]タブをクリックします。

b) [Global AES Encryption]領域で、[Global AES Encryption]領域の右上にある鉛筆アイコンをクリックします。

[Global AES 暗号 Settings] ウィンドウが表示されます。

c) [Encryption：**Enabled**]領域の横にあるボックスをクリックし、**[Passphrase / Confirm Passphrase]**フィールドに同じパスフレーズを入力してから、ウィンドウの下部にある[**Save**]をクリックします。ステップ 1 （71 ページ）

ステップ 17 リリース5.2（1）への移行ベースのアップグレードを実行している場合は、以前にバックアップした設定をインポートする前に、Pythonスクリプトを実行して必要な設定をクリーンアップします。

Cisco TACに連絡し、CSCvy42684で発生した問題に対処するPythonスクリプトを入手して、必要な設定をクリーンアップします。

https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

ステップ 18 バックアップした設定をインポートします。ステップ 2 （72 ページ）

設定のバックアップ時にリモートロケーションを設定した場合は、バックアップにアクセスするためにリモートロケーションを再度作成する必要があります。

a) クラウドAPIC GUIで、[Operations Backup & Restore]に移動します。
b) [Backup & Restore]ウィンドウで、[Backups]タブをクリックします。
c) [**Actions**]スクロールダウンメニューをクリックし、**[Restore Configuration]**を選択します。

[復元の設定（Restore Configuration）] ウィンドウが表示されます。

d) バックアップした設定を復元するために必要な情報を入力します。ステップ 2 （72 ページ）

4.2（x）リリースからリリース5.0（x）以降にアップグレードする場合は、この特定のバックアップの復元に、次の設定を使用します。

- **[復元タイプ（Restore Type）]** フィールドで、**[結合（Merge）]** を選択します。
- [Restore Mode]フィールドで、[Best Effort]を選択します。

このウィンドウに必要な情報を入力したら、[Restore Configuration]をクリックします。[バックアップと復元（Backup & Restore）]ウィンドウの[ジョブステータス（Job Status）]タブをクリックして、バックアップ復元のステータスを取得します。

ステップ 19 CapicTenantRole更新を実行して、すべての信頼できるテナントのセットを変更します。

a) テナントロールCFTを見つけます。

テナントロール CFT は、Cisco Cloud APIC インフラ テナントの AWS アカウントの S3 バケットにあります。S3 バケットの名前は「capic-common-[capicAccountId]-data」で、テナント ロールの CFT オブジェクトはそのバケット内の tenant-cft.json です。CapicAccountId は、Cisco Cloud APIC インフラ テナントの AWS アカウント番号です。これは、クラウド APIC が展開されているアカウントです。

b) テナントロールCFTリンクをクリックします。

このテナントロールCFTの[**概要**（Overview）]ページが表示されます。

c) [**Overview**]ページのtenant-cft.jsonエントリの横にあるボックスをクリックします。

このJSON形式のテナントロールCFTのスライドインペインが表示されます。

d) **[ダウンロード]** をクリックしてテナント ロール CFT をコンピュータ上の場所にダウンロードします。

セキュリティ上の理由から、AWS でのこの S3 バケットへのパブリック アクセスは許可されていないため、このファイルをダウンロードしてテナント アカウントで使用する必要があります。

e) AWSで、信頼できるテナントのユーザアカウントに移動し、[**CloudFormation**]をクリックします。

f) AWS CloudFormationダッシュボードで、信頼できるテナントスタックを見つけ、その信頼できるテナントのスタック名をクリックします。

この特定のスタックのスタックプロパティページが表示されます。

g) **[Change set]** タブをクリックします。

h) [Change set]領域で、[Create change set]をクリックします。

i) このスタックの[Create change set]ウィンドウで、[Replace current template]をクリックします。

j) **[テンプレートの指定（Specify template）]** 領域で、**[テンプレート ファイルにアップロード（Upload a Template File）]** の横にある円をクリックし、**[ファイルの選択（Choose File）]** ボタンをクリックします。

k) テナントロールCFTをダウンロードしたコンピュータ上の場所に移動し、そのテンプレートファイルを選択します。

l) このスタックの[Change set set]ウィンドウで[**Next**]をクリックします。

[Create Change Set]ポップアップが表示されます。

m) [Create Change Set]ポップアップウィンドウで[Create Change Set]をクリックします。

ステータスは、しばらくの間、**CREATE_PENDING**と表示され、その後、**CREATE_COMPLETE**に変わります。

n) 信頼できるテナントごとにこれらの手順を繰り返します。

信頼できる各テナントで、このtenant-cft.jsonファイルを使用して変更セットを作成し、その変更セットを実行します。

ステップ 20 クラウドAPIC GUIで、移行前にクラウドAPICに対して行ったすべての設定が存在することを確認します。

5.2（1）より前のリリースでは、CSRも16.xバージョンから17.xバージョンに自動的にアップグレードされます。これを確認するには、AWS Management ConsoleのEC2ダッシュボードで[インスタンス（Instances）]に移動し、CSRインスタンスを見つけて、それらもアップグレードされていることを確認します。

リリース5.2（1）以降では、のアップグレード時にCSRが自動的にアップグレードされないため、のアップグレードが完了した後にCSRアップグレードを個別にトリガーする必要があります。Cisco Cloud

APICCisco Cloud APIC詳細については、「クラウド サービス ルータのアップグレードのトリガー （81 ページ）」を参照してください。

ポリシーベースのアップグレード

リリース5.0(1) からリリース 5.0(2) にアップグレードする場合は、次の項の手順を使用して、Cisco Cloud APIC ソフトウェアのポリシーベースのアップグレードを実行します。

イメージのダウンロード中

ステップ 1 ログインしていない場合は、Cisco Cloud APIC にログインします。

ステップ 2 **[移動]** メニューから、**[オペレーションズ]** > **[ファームウェア管理]**を選択します。

[ファームウェア管理] ウィンドウが表示されます。

ステップ 3 **[ファームウェア管理]** ウィンドウの **[イメージ（Images）]** タブをクリックします。

ステップ 4 **[アクション（Actions）]** をクリックし、スクロールダウン メニューから **[ファームウェア イメージを追加（Add Firmware Image）]**を選択します。

[ファームウェア イメージを追加] ポップアップが表示されます。

ステップ 5 ファームウェア イメージをローカルまたはリモート ロケーションから追加するかを決めます。

- ローカル ロケーションからファームウェア イメージを追加する場合は、**[イメージの場所（Image Location）]** フィールドの **[ローカル]** ラジオボタンをクリックします。**[ファイルの選択（Choose File）]** ボタンをクリックし、インポートするファームウェアイメージがあるローカル システムのフォルダに移動します。ステップ 6 （78 ページ） に進みます。
- リモート ロケーションからファームウェアイメージをインポートする場合は、**[イメージの場所（Image Location）]** フィールドの **[リモート（Remote）]** オプション ボタンをクリックし、次の操作を実行します。

a) **[プロトコル（Protocol）]** フィールドで、**[HTTP]** または **[SCP]** のどちらかのオプション ボタンをクリックします。

b) **[URL]** フィールドに、イメージのダウンロード元の URL を入力します。

- 前の手順で **[HTTP]** オプション ボタンを選択した場合は、ソフトウェア イメージのダウンロードに使用する http ソースを入力します。URL の例は **`10.67.82.87:/home/<username>/ACI/aci-apic-dk9.1.0.2j.iso`** です。ステップ 6 （78 ページ） に進みます。
- 前の手順で **[SCP]** オプション ボタンを選択した場合は、**`<SCP サーバ>:/<パス>`** の形式を使用して、ソフトウェア イメージのダウンロードに使用する Secure Copy Protocol（SCP）ソースを入力します。URL の例は **`10.67.82.87:/home/<username>/ACI/aci-apic-dk9.1.0.2j.iso`** です。

c) **[Username]** フィールドに、セキュア コピーのユーザ名を入力します。

d) **[認証タイプ（Authentication Type）]** フィールドで、ダウンロードの認証タイプを選択します。次のタイプを選択できます。

- **Password**
- **SSH Key**

デフォルトは、「**Password**」です。

e) **[パスワード（Password）]** を選択した場合は、**[パスワード（Password）]** フィールドにセキュア コピーのパスワードを入力します。ステップ 6 （78 ページ） に進みます。

f) **[SSH 公開/秘密キー ファイルを使用（Use SSH Public/Private Key Files）]** を選択した場合は、次の情報を入力します。

- **[SSH キー コンテンツ（SSH Key Contents）]**：SSH キー コンテンツを使用して SSH キー ファイルを作成します。SSH キー ファイルは、ダウンロード用のリモート ロケーションの作成時に必要です。

  （注） 公開キーは、転送時に生成されます。転送後、バックグラウンドで生成されたキー ファイルは削除されます。一時的なキー ファイルは、Cisco Cloud APIC の dataexport ディレクトリに保存されます。

- **[SSH キー パスフレーズ（SSH Key Passphrase）]**：SSH キー パスフレーズを使用して SSH キー ファイルを作成します。SSH キー ファイルは、ダウンロード用のリモート ロケーションの作成時に必要です。

  （注） [パスフレーズ（Passphrase）] フィールドは空白にしておくことができます。

ステップ 6 **[選択（Select）]** をクリックします。
Cisco Cloud APIC のファームウェア イメージがダウンロードされるのを待ちます。

ポリシーベースのアップグレード プロセスを使用したソフトウェアのアップグレード

リリース 5.0(1) からリリース 5.0(2) にアップグレードする場合は、次の項の手順を使用して、ソフトウェアのポリシーベースのアップグレードを実行します。Cisco Cloud APIC

始める前に

- イメージのダウンロード中 （77 ページ） の手順を使用してイメージをダウンロードしました。

ステップ 1 GUI で、[移動（Navigation）] メニューから [ファームウェア管理のオペレーション（Operations Firmware Management）] を選択します。Cloud APIC

[ファームウェア管理] ウィンドウが表示されます。

ステップ 2 **[アップグレードのスケジュール設定]** をクリックします。

[アップグレードのスケジュール設定] ポップアップが表示されます。

ファブリックに障害があることを示すメッセージが表示された場合は、アップグレードを実行する前にこれらの障害を解決することを推奨します。詳細については、『Cisco Cloud APIC for AWS User Guide』の「Viewing Health Details Using the Cisco Cloud APIC GUI」を参照してください。

ステップ 3 **[ターゲット ファームウェア（Target Firmware）]**フィールドで、スクロールダウン メニューからファームウェア イメージを選択します。

ステップ 4 **[開始時間のアップグレード（Upgrade Start Time）]** フィールドで、アップグレードを今すぐ開始するか、後で開始するかを決定します。

- 今すぐアップグレードをスケジュールする場合は、**[今すぐ（Now）]** をクリックします。ステップ 5（79 ページ） に進みます。
- 後で日付または時刻にアップグレードをスケジュールする場合は、**[後で（Later）]** をクリックし、スケジュールされたアップグレードの日付と時刻をポップアップカレンダーから選択します。

ステップ 5 互換性チェック機能を無効にするように特に指示されている場合を除き、**[互換性チェックを無視 (Ignore Compatibility check)]** フィールドでは設定をデフォルトの [オフ (off)] のままにします。

クラウドAPIC内では、システムの現在稼働中のバージョンから特定の新しいバージョンへのアップグレード パスがサポートされているか否かを確認する互換性チェック機能が存在します。**[互換性チェックを無視]** 設定はデフォルトでは [オフ] に設定されているため、システムは可能なアップグレードの互換性をデフォルトで自動的にチェックします。

（注） **[互換性チェックを無視]** フィールドの隣のボックスにチェック マークを入力して互換性チェック機能を無効に設定することを選択する場合、システム内でサポートされていないアップグレードを発生させるリスクを生じ、これにより使用不能な状態を引き起こす可能性があります。

ステップ 6 **[アップグレードのスケジュール設定]** をクリックします。

[Upgrade Status] 領域のメインの [Firmware Management] ウィンドウで、アップグレードの進行状況をモニタできます。

ソフトウェアのダウングレード

次の項では、Cisco Cloud APIC ソフトウェアを正常にダウングレードするために必要な情報を提供します。

ソフトウェアのダウングレード

始める前に

5.0（2）から 5.0（2）より前のリリースにダウングレードする場合は、次の前提条件が適用されます。

- Cisco Cloud APIC が常にリリース 5.0（2）で実行されている場合（5.0（2）より前のリリースからリリース 5.0（2）にアップグレードしたことがない場合）、リリース 5.0（2）より前のリリースにダウングレードすることはできません。）。Cisco Cloud APIC が以前のリリースで実行されなかった 5.0（2）より前のリリースへのダウングレードはサポートされていません。
- Cisco Cloud APIC をリリース 5.0（2）にアップグレードし、その後に特定のリリース 5.0（2）固有の設定を完了し、リリース 5.0（2）より前のリリースにダウングレードする場合は、5.0（2）ダウングレード前の固有の設定を削除する必要があります。

ステップ 1 必要に応じて、ダウングレードする前に 5.0（2）固有の設定を削除します。

ステップ 2 イメージのダウンロード中 （77 ページ） で説明している手順を使用して、ダウングレードのイメージをダウンロードします。

ステップ 3 イメージが完全にダウンロードされたら、**[Navigation]** メニューから **[Operations > Firmware Management]**

[ファームウェア管理] ウィンドウが表示されます。

ステップ 4 **[アップグレードのスケジュール設定]** をクリックします。

[アップグレードのスケジュール設定] ポップアップが表示されます。

ファブリックに障害が存在することを示すメッセージが表示された場合は、ダウングレードを実行する前にこれらの障害を解決することを推奨します。詳細については、『*Cisco Cloud APIC for AWS User Guide*』の「Viewing Health Details Using the Cisco Cloud APIC GUI」を参照してください。

ステップ 5 **[ターゲット ファームウェア（Target Firmware）]**フィールドで、スクロールダウン メニューからファームウェア イメージを選択します。

ステップ 6 **[開始時間のアップグレード（Upgrade Start Time）]** フィールドで、ダウングレードを今すぐ開始するか、後で開始するかを決定します。

- ダウングレードを今すぐスケジュールする場合は、**[今すぐ（Now）]** をクリックします。ステップ 7 （80 ページ） に進みます。
- ダウングレードを後の日付または時刻にスケジュールする場合は、**[後で（Later）]**をクリックし、スケジュールされたダウングレードの日時をポップアップカレンダーから選択します。

ステップ 7 互換性チェック機能を無効にするように特に指示されている場合を除き、**[互換性チェックを無視 (Ignore Compatibility check)]** フィールドでは設定をデフォルトの [オフ (off)] のままにします。

クラウド APIC 内では、システムの現在稼働中のバージョンから特定の新しいバージョンへのダウングレード パスがサポートされているか否かを確認する互換性チェック機能が存在します。**[互換性チェックを無**

視] 設定はデフォルトでは [オフ] に設定されているため、システムは可能なダウングレードの互換性をデフォルトで自動的にチェックします。

（注） **[互換性チェックを無視]** フィールドの隣のボックスにチェック マークを入力して互換性チェック機能を無効に設定することを選択する場合、システム内でサポートされていないダウングレードを発生させるリスクを生じ、これにより使用不能な状態を引き起こす可能性があります。

ステップ 8 **[アップグレードのスケジュール設定]** をクリックします。

[ステータスのアップグレード（Upgrade Status）] 領域のメインの **[ファームウェア管理（Firmware Management）]** ウィンドウで、ダウングレードの進行状況をモニタできます。

システム リカバリの実行

システム リカバリを実行する手順は、移行ベースのアップグレードを実行する手順と同じです。これらの手順については、セクション 移行ベースのアップグレード （71 ページ） を参照してください。

クラウド サービス ルータのアップグレードのトリガー

次のトピックでは、クラウド サービス ルータ（CSR）のアップグレードをトリガーするための情報と手順について説明します。

クラウド サービス ルータのアップグレードのトリガー

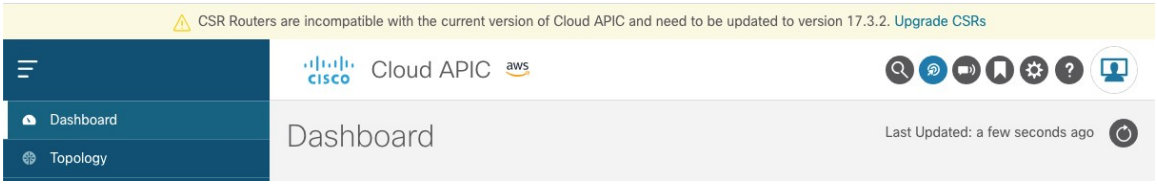
リリース 5.2(1) より前は、Cisco Cloud APIC のアップグレードをトリガーするたびに、クラウド サービス ルータ（CSR）が自動的にアップグレードされます。リリース 5.2(1) 以降では、CSR のアップグレードをトリガーし、Cisco Cloud APIC アップグレードとは無関係に CSR のアップグレードをモニタできます。これは、管理プレーン（Cisco Cloud APIC）とデータプレーン（CSR）のアップグレードを分割できるため、トラフィック損失を減らすのに役立ちます。

リリース 5.2(1) 以降、この機能はデフォルトで有効になっています。デフォルトの前提は、Cisco Cloud APIC へのアップグレードをトリガーした後に CSR へのアップグレードをトリガーすることです。この機能を有効にすると、無効にすることはできません。

この機能を有効にすると、Cisco Cloud APIC と CSR の適切なアップグレード シーケンスは次のようになります。

（注） 次に、CSR へのアップグレードをトリガーするための全体的なプロセスを説明する上位レベルの手順を示します。具体的な手順については、GUI を使用したクラウドサービス ルータのアップグレードのトリガーCisco Cloud APIC （83 ページ） を参照してください。

1. この章の手順に従って Cisco Cloud APIC をアップグレードします。
2. Cisco Cloud APIC のアップグレードが完了するまで待ちます。そのアップグレードが完了すると、システムは CSR が Cisco Cloud APIC と互換性がなくなったことを認識します。その後、CSR と Cisco Cloud APIC に互換性がなく、Cisco Cloud APIC に設定された新しいポリシーは CSR をアップグレードするまで CSR に適用されないことを示すメッセージが表示されます。



3. AWS ポータルで CSR の利用規約を確認し、同意します。
4. CSR アップグレードをトリガーして、Cisco Cloud APIC の互換バージョンになるようにします。

   次の 2 つの方法のいずれかを使用して、CSR アップグレードのトリガープロセスを開始できます。

   - 画面上部のバナーで、**[CSR のアップグレード（Upgrade CSRs）]** リンクをクリックします。
   - [ファームウェア管理（Firmware Management）] ページの [CSRs] 領域を使用します。次のとおりに移動します。

     [オペレーション（Operations）] > **[ファームウェア管理]**

     [CSR] タブをクリックし、**[CSR のアップグレード（Upgrade CSRs）]** を選択します。

また、REST API を使用して CSR のアップグレードをトリガーすることもできます。手順については、REST API を使用したクラウドサービスルータのアップグレードのトリガー（83 ページ） を参照してください。

注意事項と制約事項

- Cisco Cloud APIC をアップグレードした後、CSR と Cisco Cloud APIC に互換性がないことを示すメッセージが表示されない場合は、そのメッセージを表示するためにブラウザを更新する必要があります。
- Cisco Cloud APIC をアップグレードした後、CSR へのアップグレードをトリガーします。Cisco Cloud APIC をアップグレードする前に、CSR へのアップグレードをトリガーしないでください。
- CSR へのアップグレードをトリガーすると、停止することはできません。

- CSR へのアップグレードをトリガーした後にエラーが表示された場合は、それらのエラーを確認して解決します。これらの CSR アップグレード エラーが解決されると、CSR アップグレードが自動的に続行されます。

GUI を使用したクラウド サービス ルータのアップグレードのトリガー Cisco Cloud APIC

ここでは、GUI を使用してクラウド サービス ルータ（CSR）へのアップグレードをトリガーする方法について説明します。Cisco Cloud APIC詳細については、「クラウド サービス ルータのアップグレードのトリガー （81 ページ）」を参照してください。

ステップ 1 互換性のある CSR バージョンへの CSR アップグレードをトリガーするプロセスを開始します。

次の 2 つの方法のいずれかを使用して、CSR アップグレードのトリガー プロセスを開始できます。

- 画面上部のバナーで、**[CSR のアップグレード（Upgrade CSRs）]** リンクをクリックします。
- **[ファームウェア管理（Firmware Management）]** ページの **[CSRs]** 領域を使用します。次のとおりに移動します。

  [オペレーション（Operations）] > **[ファームウェア管理]**

  [CSR] タブをクリックし、**[CSR のアップグレード（Upgrade CSRs）]** を選択します。

[CSR のアップグレード（Upgrade CSRs）]をクリックすると、CSR をアップグレードすると CSR がリブートし、トラフィックが一時的に中断する可能性があることを示す警告が表示されます。

ステップ 2 この時点で CSR をアップグレードし、トラフィックが一時的に中断された場合は、警告メッセージで [Confirm Upgrade] をクリックします。
CSR ソフトウェアのアップグレードが開始されます。CSR のアップグレードが進行中であることを示すバナーが画面の上部に表示されます。メッセージ内の [CSR アップグレード ステータス（View CSR upgrade status）] をクリックして、CSR アップグレードのステータスを表示します。

ステップ 3 CSR のアップグレード中に発生する可能性のある障害を修正します。

アップグレード中に障害が発生した場合は、次の場所に移動して障害の詳細情報を取得できます。

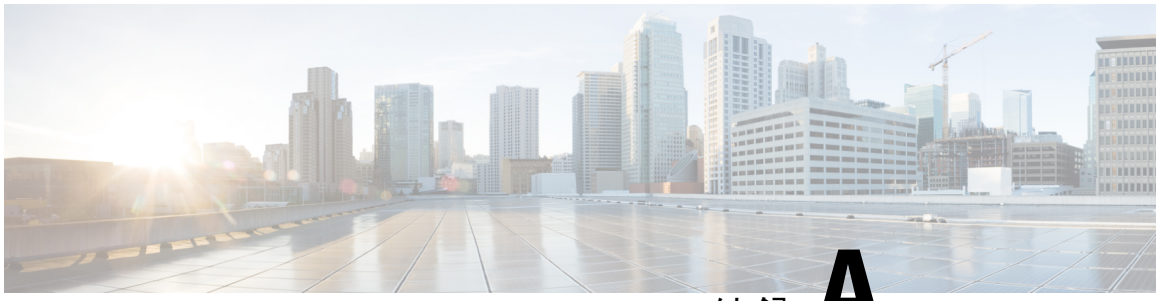
[オペレーション（Operations)] > **[イベント 分析（ Event Analytics）]** > **[失敗（Faults）]**

REST API を使用したクラウド サービス ルータのアップグレードのトリガー

ここでは、REST API を使用してクラウド サービス ルータ（CSR）へのアップグレードをトリガーする方法について説明します。詳細については、「クラウド サービス ルータのアップグレードのトリガー （81 ページ）」を参照してください。

クラウド テンプレートで routerUpgrade フィールドの値を「true」に設定し、REST API を介して CSR へのアップグレードをトリガーします（routerUpgrade = "true"）。

```
<polUni>
<fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
        <cloudtemplateProfile name="defaultxyz" routerUsername="SomeFirstName"
routerPassword="SomePass" routerUpgrade="true">
        </cloudtemplateProfile>
        <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>
        <cloudtemplateIntNetwork name="default">
            <cloudRegionName provider="aws" region="us-west-1"/>
            <cloudRegionName provider="aws" region="us-west-2"/>
        </cloudtemplateIntNetwork>
        <cloudtemplateExtNetwork name="default">
            <cloudRegionName provider="aws" region="us-west-2"/>
            <cloudtemplateVpnNetwork name="default">
                <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
                <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
                <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />
                <cloudtemplateOspf area="0.0.0.1"/>
            </cloudtemplateVpnNetwork>
          <cloudtemplateBgpEvpn peeraddr="34.1.1.1/32" asn="63000" siteId="123" password="abcd1234"
 />
        </cloudtemplateExtNetwork>
    </cloudtemplateInfraNetwork>
</fvTenant>
</polUni>
```



付録 A

AWS リソースと命名規則

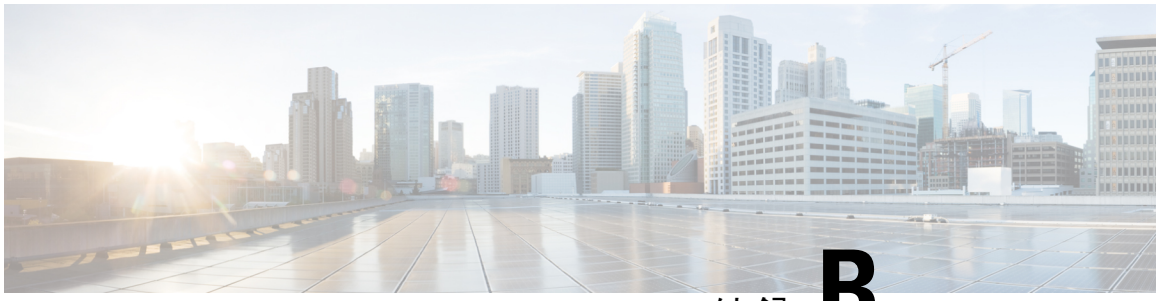
AWS リソースと命名規則

以下は、のインストール時にによって作成される AWS リソースと、で使用される命名規則のリストです。Cloud APICCloud APICこれらの AWS リソースをよりよく理解し、同様の名前を使用しないようにするには、このリストの情報を使用してください。

項目	使用されるアイテム数	アイテムの命名ルール
S3 バケット	• 1 つのグローバル（CFT テンプレートの保存に使用） • リージョンごとに 1 つ（CloudTrail ログの保存に使用）	Cloud APIC S3 バケットはプレフィックス `capic` で始まります。このプレフィックスで始まるバケットは使用しないでください。
タグ	最小 2、最大 8	使用されるタグ キーは次のとおりです。 • `AciDnTag` • `AciOwnerTag` • 名前（タグ値にはオブジェクトの相対名または RN が含まれます） • AciStaleTag（によってリソースが古いと見なされる場合にのみ表示）Cloud APIC

AWS リソースと命名規則

項目	使用されるアイテム数	アイテムの命名ルール
		• AciResolvedObjDnTag（VPC のみ）：解決されたオブジェクトの識別名（DN）を保持します。 • AciPeerDnTag（VPC ピアリング専用）：ピア VPC の DN を伝送します。 Aci または Capic で始まるタグは作成しないでください。
CloudTrails	リージョンにつき 1 つ	トレイル名はプレフィックス capic で始まります。このプレフィックスで始まる証跡は作成しないでください。
CloudWatch イベント	リージョンごとに 3 つ	ルールはプレフィックス capic で始まります。このプレフィックスで始まるルールは作成しないでください。
Simple Queue Service（SQS）キュー	リージョンにつき 1 つ	キュー名はプレフィックス capic で始まります。このプレフィックスで始まるキューは作成しないでください。



付録 B

AWS の IAM ロールと権限

AWS の IAM ロールと権限

（注） AWS IAM の役割と権限の詳細については*AWS* ユーザ ガイドの *Cisco Cloud APIC*、次のいずれかのタイプのテナントとして AWS プロバイダを設定する方法などを参照してください。

- 信頼できるテナント
- 信頼できないテナント
- 組織テナント、リリース 4.2(3) 以降でサポートされています。

AWS ユーザ ガイドの *Cisco Cloud APIC* は、次の ＵＲＬ から入手できます。

https://www.cisco.com/c/en/us/support/cloud-systems-management/cloud-application-policy-infrastructure-controller/tsd-products-support-series-home.html

Cisco Cloud APIC のインストールと操作には、特定の AWS IAM の役割と権限が必要です。

CloudFormation テンプレート (CFT) を使用して Cisco Cloud APIC をインストールする場合は、AWS に完全な管理者アクセス権を持つユーザ (たとえば、権限ポリシー ARN **arn:aws:iam::aws:policy/AdministratorAccess**が、直接、ロール ポリシーにより、またはユーザ グループにより接続されているユーザ)によってインストールすることを推奨します。ただし、使用可能な AWS 管理者アクセス権を持つユーザがいない場合は、Cisco Cloud APIC をインストールするユーザに次の最小権限セットが必要です。

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Effect": "Allow",
   "Action": "iam:*",
   "Resource": "*"
  },
  {
```

AWS の IAM ロールと権限

```
   "Effect": "Allow",
   "Action": "ec2:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "cloudformation:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "s3:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "sns:*",
   "Resource": "*"
  }
 ]
}
```

上記の権限セットは、CFT を使用して Cisco Cloud APIC をインストールするユーザに必要です。次に、**[アクション (Action)]**行に示すように、上記の必要な権限の詳細について説明します。

- **iam権限:** Cisco Cloud APICインスタンスは、 **ApicAdmin**という名前の AWS ロールで実行される AWS EC2 インスタンスです。このロールは、CloudFormation スタックによって作成される必要があります。**ApicAdmin**ロールを使用して Cisco Cloud APIC インスタンスを実行すると、Cisco Cloud APIC インスタンスは AWS メタデータ サービスを使用して一時的なクレデンシャルを取得できます。これにより、Cisco Cloud APIC インスタンスは、AWS API コールを行うために、固定のアクセス キー ID と秘密アクセス キーを使用する必要がなくなります。
- **ec2権限:**スタックが必要なVPC、サブネット、セキュリティグループなどを作成できるようにするために必要です。スタックによって、 Cisco Cloud APIC インスタンスが展開されるインフラ VPC が作成されます。
- **cloudformationの権限:** CFT 自体を実行するために必要です。
- **s3権限:** CFT が AWS CloudFormation スタックのニーズに基づいて S3 バケットに保存されるようにするために必要です。
- **sns権限:** CloudFormation スタックを実行するための通知を取得するために必要です。

操作の場合、Cisco Cloud APIC は **ApicAdmin** ロールで実行されます。このロールには 2 つのポリシーが付加されており、CloudFormation テンプレートの起動の一環として作成されます。

- **ApicAdminFullAccessポリシー:** このポリシーにリストされている権限によって、Cisco Cloud APIC は EC2 および VPC リソース、S3 バケット、リソースグループ、アカウント通知、およびログを作成および管理できます。Cisco Cloud APIC は、作成したリソースの管理のみを試行することに注意してください。他のアプリケーションによって作成されたリソースには処理しません。

  このポリシーには、次の権限が必要です。

AWS の IAM ロールと権限

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Action": "organizations:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "ec2:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "s3:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "sqs:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "elasticloadbalancing:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "acm:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "cloudtrail:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "cloudwatch:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "logs:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "resource-groups:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "events:*",
   "Resource": "*",
   "Effect": "Allow",
   "Sid": "CloudWatchEventsFullAccess"
  },
  {
   "Action": "autoscaling:*",
   "Resource": "*",
   "Effect": "Allow"
  }
```

AWS の IAM ロールと権限

```
 ]
}
```

- **ApicTenantsAccessポリシー:**このポリシーにリストされている権限によって、Cisco Cloud APIC は、テナント アカウントのロールと、それらのテナント AWS アカウントのコール AWS API を引き受けることができます。これにより、Cisco Cloud APIC は、テナント アカウントのハード クレデンシャルを使用せずにテナント アカウントにアクセスすることができます。

  このポリシーには、次の権限が必要です。

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Action": "sts:AssumeRole",
  "Resource": "*",
  "Effect": "Allow"
 }]
}
```

Cisco Cloud APIC 自体は、操作のために IAM 権限を必要としません。これは、インストール後に IAM ポリシーやロールが作成されないためです。

Cisco Cloud APIC は、それによって作成された AWS リソースの管理を試みますが、既存のリソースをインベントリとしてリストするのではなく、他のアプリケーションによって作成されたリソースの管理を試みません。同時に、これらのアカウント (インフラ アカウントと他のテナント アカウントの両方) の IAM ユーザは、Cisco Cloud APIC によって作成されたリソースに干渉しないようにする必要があります。したがって、AWS で Cisco Cloud APIC により作成されたすべてのリソースには、次の 2 つのタグのうち少なくとも 1 つが適用されます。

- **AciDnTag**
- **AciOwnerTag**

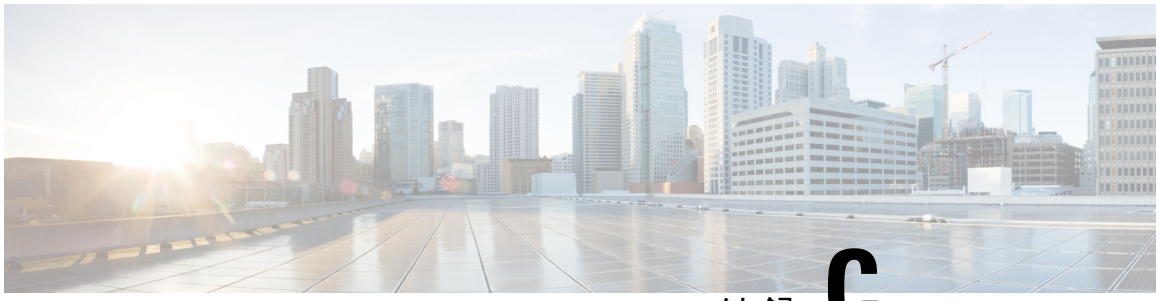
したがって、EC2、VPC、およびその他のリソースを作成、削除、または更新する権限を持つ AWS IAM ユーザを作成する場合、これらのユーザが Cisco Cloud APIC によって作成および管理されるリソースへアクセスすることや変更することを防止する必要があります。このような制限は、インフラとその他のユーザのテナントアカウントの両方に適用する必要があります。AWS アカウント管理者は、上記の2つのタグを使用して、ユーザが Cisco Cloud APIC によって作成および管理されるリソースへのアクセスや変更を防止する必要があります。

たとえば、次のようなアクセス ポリシーがある場合、Cisco Cloud APIC によって管理されているリソースへの意図しないアクセスを防止するために、IAM ユーザのアクセス ポリシーを設定することができます。

```
{
 "Effect": "Deny",
 "Action": [
  "ec2:*"
 ],
 "Resource": "*",
 "Condition": {
  "StringLike": {
```

```
      "ec2:ResourceTag/AciDnTag": "*"
    }
   }
  }
```

AWS の IAM ロールと権限



付録 C

テナントリージョン管理

テナントリージョン管理

異なるリージョンでのテナント ポリシーの展開

Cisco Cloud APIC 所有権チェックを適用して、意図的にまたは誤って行われた同じテナントとリージョンの組み合わせでポリシーが展開されないようにします。たとえば、1つ（CAPIC1）がリージョン R1 の AWS アカウント IA1 に展開されており、テナントをリージョン R2 のアカウント TA1 に展開するとします。Cisco Cloud APICこのテナント展開（TA1-R2 のアカウントとリージョンの組み合わせ）は、IA1-R1（CAPIC1）によって所有されています。別の（CAPIC2）が将来のある時点で TA1-R2 の同じテナントとリージョンの組み合わせを管理しようとした場合（たとえば、CAPIC2 がリージョン R3 の AWS アカウント IA2 に導入されている場合）、展開 TA1-R2 の所有者は IA1-R1（CAPIC1）です。Cisco Cloud APIC

これらの制限は、AWS リソース グループを使用して実現されます。次の例は、有効な展開と無効な展開の組み合わせを示しています。

Cisco Cloud APIC	テナント	Validity	理由
IA1-R1(CAPIC1)	TA1-R1	Valid	テナント TA1-R1 は IA1-R1（CAPIC1）によって所有されています。
IA1-R1(CAPIC1)	TA1-R2	Valid	テナント TA1-R2 は IA1-R1（CAPIC1）によって所有されています。

Cisco Cloud APIC	テナント	Validity	理由
IA1-R2(CAPIC2)	TA1-R1	無効	テナント TA1-R1 はすでに IA1-R1（CAPIC1）によって所有されています。
IA1-R2(CAPIC2)	TA1-R3	Valid	テナント TA1-R3 は IA1-R2（CAPIC2）によって所有されています。
IA2-R1(CAPIC3)	TA1-R1	無効	テナント TA1-R1 はすでに IA1-R1（CAPIC1）によって所有されています。
IA2-R1(CAPIC3)	TA1-R4	Valid	テナント TA1-R4 は IA2-R1（CAPIC3）によって所有されています。
IA2-R1(CAPIC3)	TA2-R4	Valid	テナント TA2-R4 は IA2-R1（CAPIC3）によって所有されています。

展開の適用は、インフラ テナントとユーザ テナントに対して実行されます。CAPIC1 がリージョン R1 のアカウント IA1 に導入されており、リージョン R2 と R3 を管理しようとしている場合、リージョン R1、R2、および R3 の同じアカウント IA1 を管理しようとする別のアカウント（たとえば、CAPIC2）は許可されません。Cisco Cloud APIC

テナント リージョンの所有権の検証は、AWS リソース グループを使用して行われます。テナントとリージョンの組み合わせごとに、構文CloudAPIC_TenantName_Regionを使用してリソース グループが作成されます（たとえば、リージョン R2 の アカウント TA1 に CAPIC_TA1_R2 という名前が展開されている場合）。また、Cisco Cloud APIC がリージョン R1 のアカウント IA1 に導入されている場合は、IA1_R1_TA1_R2 の所有権タグがあります。

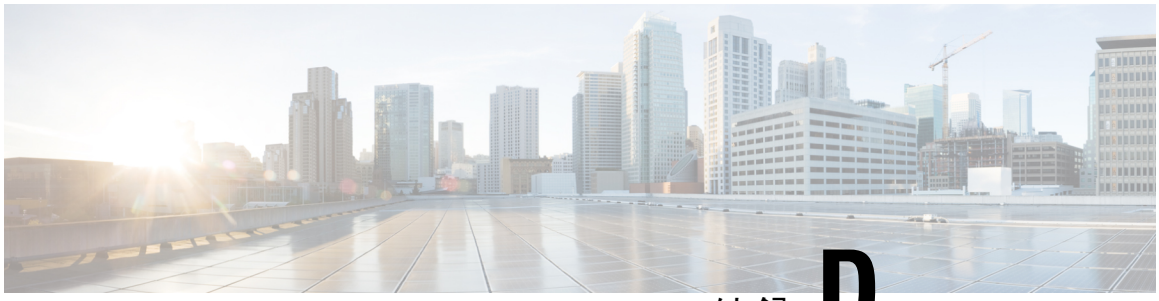
次に、AciOwnerTag の不一致が発生し、既存のテナント リージョンの導入が失敗する状況の例を示します。

- Cisco Cloud APIC が最初に 1 つのアカウントにインストールされた場合、破棄され、Cisco Cloud APIC は別のアカウントにインストールされました。この場合、同じテナントとリージョンの組み合わせを再度管理しようとすると、既存のすべてのテナントとリージョンの展開が失敗します。
- Cisco Cloud APIC が 1 つの地域に最初にインストールされた場合、その後切断され、Cisco Cloud APIC は別の地域にインストールされます。この場合、既存のすべてのテナント リージョンの展開が失敗します。

• 別のテナントが同じテナント リージョンを管理している場合。Cisco Cloud APIC

所有権が一致しない場合、Cisco Cloud APIC はテナント領域のセットアップの再試行を再度実行しません。所有権の不一致のケースを解決するには、他のテナントが同じテナントとリージョンの組み合わせを管理していない場合は、テナントの AWS アカウントにログインし、影響を受けるリソース グループ（CAPIC_123456789012_us-east-2など）を手動で削除します。Cisco Cloud APIC次に、Cisco Cloud APIC インスタンスをリロードするか、Cisco Cloud APIC からテナントを削除して再度追加します。

テナントリージョン管理



付録 D

CSR とテナント情報の検索

CSR とテナント情報の検索

Cloud APIC と ISN デバイス間の接続を有効にするために必要な Cisco Cloud サービスルータ (CSR) とテナント情報には、いくつかの部分があります。この情報は、ACI マルチサイト オーケストレータ から取得できるようにする必要があります (**[サイト]** > **[インフラの構成]** > **[IPN デバイス設定ファイルのみのダウンロード]**)。ただし、CSR とテナントの情報を手動で収集する必要があることが判明した場合は、次の項でこの情報を特定する手順を説明します。

クラウド CSR の情報

必要な AWS 情報	入力する値	AWS サイトでのこの情報の検索方法
クラウドCSR の 3 番目のネットワークインターフェイスの柔軟な IP アドレス		1. AWS 管理コンソールの EC2 ダッシュボードの**インスタンス**に移動します。 2. CSR インスタンスを選択します (CSR インスタンスの横にあるボックスをクリックします)。 3. 右側にネットワークインターフェイスが表示されるまで下にスクロールし、[eth2] リンクをクリックして、[パブリック IP アドレス] フィールドに表示されている IP アドレスを見つけます。

CSR とテナント情報の検索

必要な AWS 情報	入力する値	AWS サイトでのこの情報の検索方法
クラウド CSR のパブリック IP アドレス		1. AWS 管理コンソールの EC2 ダッシュボードの**インスタンス**に移動します。 2. CSR インスタンスを検索します。 3. その CSR インスタンスの `[IPv4 パブリック IP (IPv4 Public IP)]` 列に表示されている IP アドレスをコピーします。
クラウド CSR の事前共有キー		1. クラウド CSR にログインします。 **ssh *ip-address*** ここで、 *ip* アドレスはクラウド CSR のパブリック IP アドレスです。 2. 暗号キーリング情報を取得します。 **show running-config | include pre-shared-key** 事前共有キーが強調表示されている次のような出力が表示されます。 `pre-shared-key address 192.0.2.15 key 12345678900987654321234567890`
クラウド CSR へのオンプレミス IPsec デバイスのピア トンネル IP アドレス		1. クラウド CSR にログインします。 **ssh *ip-address*** ここで、 *ip* アドレスはクラウド CSR のパブリック IP アドレスです。 2. 次のコマンドを入力します。 **show ip interface brief | include Tunnel2** 次のような出力が表示されます。 `Tunnel2 30.29.1.1 YES NVRAM up down` 3. このトンネルの IP アドレスを取得し、アドレスを1つずつ増やして、オンプレミスの IPsec デバイスのピアトンネル IP アドレスをクラウド CSR に取得します。 たとえば、出力に表示されている IP アドレスが 30.29.1.1 の場合、クラウド CSR に対してオンプレミスの IPsec デバイスのピア トンネル IP アドレスが 30.29.1.2 ます。

インフラ テナントの情報

必要な AWS 情報	入力する値	AWS サイトでのこの情報の検索方法
インフラ テナントのクラウド アカウント ID		AWS で Cloud APIC を導入する （21 ページ） の説明に従って、インフラ テナントに AWS アカウントを使用します。

CSR とテナント情報の検索

必要な AWS 情報	入力する値	AWS サイトでのこの情報の検索方法
インフラ テナントのクラウド アクセスキー ID とクラウドシークレット アクセス キー		1. インフラ テナントの Amazon Web Services アカウントにログインします。 2. [IAM] に移動します。 3. 左側のペインで、**[ユーザ]** を選択します。 4. 管理アカウントのリンクをクリックします。 5. [サマリ] ページで、**[セキュリティ資格情報 (Security credentials)]** タブをクリックします。 6. Amazon Web Services アクセスキー ID をまだ持っていない場合は、**[アクセス キーの作成 (Create access key)]** をクリックします。 7. **[アクセス キー ID (Access KEY ID)]** フィールドと **[シークレット アクセス キー (Secret access key)]** フィールドから情報を見つけます。

ユーザ テナントの情報

必要な AWS 情報	入力する値	AWS サイトでのこの情報の検索方法
Cisco Cloud APIC ユーザ テナントのクラウド アカウント ID		ユーザ テナントの AWS アカウントのセットアップ （25 ページ） の説明に従って、ユーザ テナントに AWS アカウントを使用します。
Cisco Cloud APIC ユーザ テナントのクラウド アクセスキー ID とクラウド シークレット アクセス キー		1. ユーザ アカウントの Amazon Web Services アカウントにログインします。 2. [IAM] に移動します。 3. 左側のペインで、**[ユーザ]** を選択します。 4. クラウド APIC ユーザ テナント アカウントのリンクをクリックします。 5. [サマリ] ページで、**[セキュリティ資格情報 (Security credentials)]** タブをクリックします。 6. Amazon Web Services アクセスキー ID をまだ持っていない場合は、**[アクセス キーの作成 (Create access key)]** をクリックします。 7. **[アクセス キー ID (Access KEY ID)]** フィールドと **[シークレット アクセス キー (Secret access key)]** フィールドから情報を見つけます。

CSR とテナント情報の検索

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。