概要

- Extending the Cisco ACI Fabric to the Public Cloud, on page 1
- Components of Extending Cisco ACI Fabric to the Public Cloud, on page 2
- Changes in APIC Release 4.2(1), on page 5
- AWS Organizations と組織のユーザ テナントのサポート （6 ページ）
- ポリシーの用語 （8 ページ）
- Cisco Cloud APIC Licensing, on page 9
- Cisco Cloud APIC-Related Documentation, on page 10

Extending the Cisco ACI Fabric to the Public Cloud

Cisco Application Centric Infrastructure (ACI) customers who own a private cloud sometimes may run part of their workload on a public cloud. However, migrating workload to the public cloud requires working with a different interface and learning different ways to set up connectivity and define security policies. Meeting these challenges can result in increased operational cost and loss of consistency.

However, beginning in Cisco Application Policy Infrastructure Controller (APIC) Release 4.1(1), Cisco ACI can use Cisco Cloud APIC to extend a Cisco ACI multi-site fabric to Amazon Web Services (AWS) public clouds.

Beginning in APIC Release 4.2(1), Cisco ACI can also use Cisco Cloud APIC to extend a Cisco ACI multi-site fabric to Microsoft Azure public clouds.

What Cisco Cloud APIC Is

Cisco Cloud APIC is a software deployment of Cisco APIC that can be deployed on a cloud-based virtual machine (VM). Cisco Cloud APIC provides the following features:

- Provides an interface that is similar to the existing Cisco APIC to interact with the Amazon AWS or Microsoft Azure public clouds.
- Automates the deployment and configuration of cloud deployment.
- Configures the cloud router control plane.
- Configures the data path between the on-premises Cisco ACI fabric and the cloud site.
- Translates Cisco ACI policies to cloud native policies.
- Discovers endpoints.

How Users Can Benefit from Cisco ACI Extension to the Public Cloud

Cisco Cloud APIC is a key part of Cisco ACI extension to the public cloud. Cisco Cloud APIC provides consistent policy, security, and analytics for workloads deployed either on or across on-premises data centers and the public cloud.

Cisco ACI extension to the public cloud also provides an automated connection between on-premises data centers and the public cloud with easy provisioning and monitoring. It also provides a single point for managing, monitoring, and troubleshooting policies across on-premises data centers and the public cloud.

AWS GovCloud Support

Support for GovCloud varies on Cisco Cloud APIC, depending on the release:

- For release 4.1(2) up to release 5.0(1), Cisco Cloud APIC supports AWS GovCloud only for the us-gov-west region. The us-gov-east region is not supported in these releases.
- For release 5.0(1) up to release 5.2(1), Cisco Cloud APIC supports AWS GovCloud in the us-gov-west and us-gov-east regions. However, Cisco Cloud Service routers (CSRs) can only be deployed in the us-gov-west region. If you want to have intersite connectivity, we recommend that you deploy the Cisco Cloud APIC in the us-gov-west region only.
- For release 5.2(1), Cisco Cloud APIC continues to support AWS GovCloud in the us-gov-west and us-gov-east regions, as it did previously. However, beginning with release 5.2(1), Cisco CSRs can also be deployed in the us-gov-east region in addition to the previous support for deployment in the us-gov-west region.

Note that these areas have a unique configuration when you deploy a Cisco Cloud APIC on AWS GovCloud:

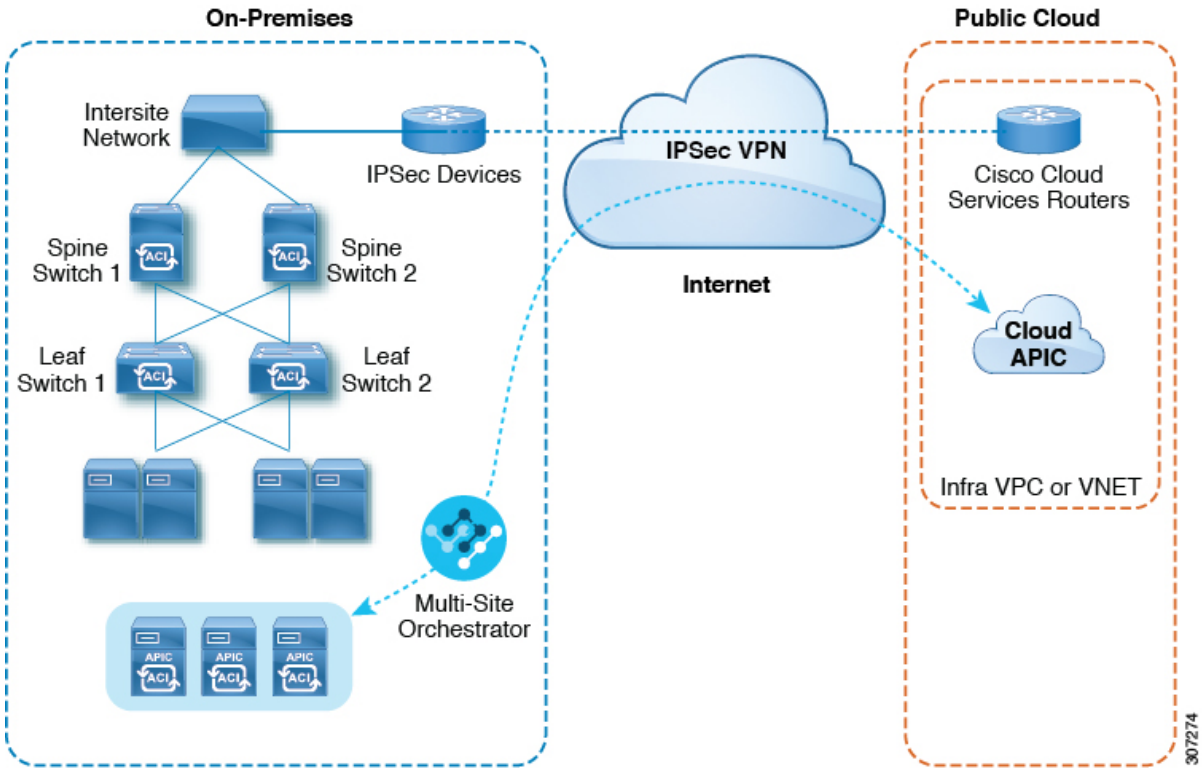
- You will subscribe to the CSR on the commercial account.
- You will subscribe to the Cisco Cloud APIC on the commercial account.
- You will launch the Cloud Formation template from the commercial account, which redirects the request to AWS GovCloud for the login.

Components of Extending Cisco ACI Fabric to the Public Cloud

Several components—each with its specific role—are required to extend the Cisco Application Centric Infrastructure (ACI) Multi-Site fabric to the public cloud.

The following illustration shows the architecture of Cisco Cloud APIC.

Figure 1: Cisco Cloud APIC Architecture



On-Premises Data Center Components

Cisco ACI Fabric and Cisco APIC

The Cisco ACI allows application requirements to define the network. This architecture simplifies, optimizes, and accelerates the entire application deployment life cycle. Cisco Application Policy Infrastructure Controller (APIC) is a key component of Cisco ACI. It enables applications to directly connect with a secure, shared, high-performance resource pool that includes network, compute, and storage capabilities.

Cisco ACI Multi-Site and Cisco ACI Multi-Site Orchestrator

Cisco ACI Multi-Site is an architecture that allows the application to define the networking requirements in a programmatic way. This architecture simplifies, optimizes, and accelerates application deployment. You must have Cisco ACI Multi-Site installed to use Cisco Cloud APIC to extend the fabric into the public cloud.

For more information, see the Cisco ACI Multi-Site documentation on Cisco.com and the section Cisco ACI マルチサイトを介した Cisco Cloud APIC の管理 in this guide.

Cisco ACI Multi-Site Orchestrator (MSO) manages multiple instances of Cisco Application Policy Infrastructure Controller (APICs) in multiple fabrics (sites).

When extending the Cisco ACI fabric to the public cloud, Cisco ACI Multi-Site Orchestrator creates connectivity between the on-premises data center and the public cloud. Use Cisco ACI Multi-Site to create tenants across the on-premises data center and the public cloud.

Note You must configure the on-premises Cisco ACI fabric: Create a Fabric Ext Connection Policy and define the overlay TEP and other information required for Multi-Site. You also must add the on-premises Cisco ACI fabric to the Multi-Site architecture. See the *Cisco ACI Multi-Site Configuration Guide* on Cisco.com.

For more information, see the Cisco ACI Multi-Site documentation on Cisco.com and the section Cisco ACI マルチサイトを介した Cisco Cloud APIC の管理 in this guide.

IP Security (IPsec) Router

A router capable of Internet Protocol Security (IPsec) is required to establish IPsec connections between the on-premises site and the public cloud site.

AWS Public Cloud Components

Cisco Cloud APIC

Cisco Cloud APIC performs the following actions:

- Defines a site on the public cloud, provisions the cloud infra virtual private clouds (VPCs) or virtual networks (VNETs) and manages the Cisco Cloud Services Router (CSR) across all regions.
- Renders the Cisco ACI policy model in the public cloud, and manages cloud health.

For more information, see *Cisco Cloud APIC Release Notes*. Also see the sections AWS で Cloud APIC を導入する and セットアップ ウィザードを使用した Cisco Cloud APIC の設定 in this guide.

Cisco Cloud Services Router

The Cisco Cloud Services Router (CSR) is a virtual router that delivers comprehensive WAN gateway and network services into virtual and cloud environments. The CSR enables enterprises to extend their WANs into provider-hosted clouds. Two CSRs are required for Cisco Cloud APIC solution.

The type of CSR that you will use with Cisco Cloud APIC varies depending on the release:

- For releases up to 25.0(3), Cisco Cloud APIC uses the **Cisco Cloud Services Router 1000v** as the cloud services router. For more information on this CSR, see the Cisco CSR 1000v documentation.
- For release 25.0(3) and later, Cisco Cloud APIC uses the **Cisco Catalyst 8000V** as the cloud services router. For more information on this CSR, see the Cisco CSR 8000v documentation.

AWS public cloud

AWS is a cloud-based platform that provides on-demand services such as compute, storage, network, and databases. Subscribers to AWS have access through the Internet to virtual computers where they can run their workloads.

For more information, see the documentation on the AWS website.

Connections Between the On-Premises Data Center and the Public Cloud

IPsec VPN

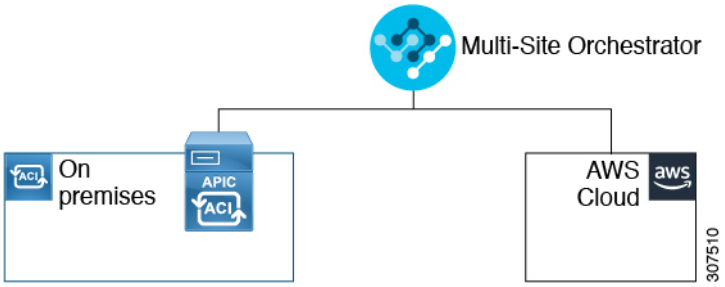
You need Internet connectivity with a VPN from the IPsec router, including a publicly routable IP address and with sufficient bandwidth for AWS or Microsoft Azure connectivity.

Management Connection

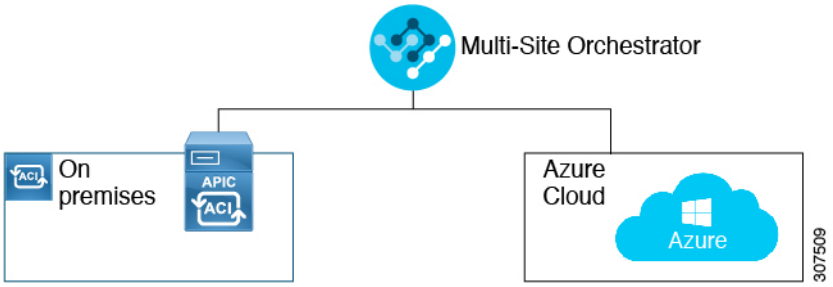
You need a management connection between the Multi-Site Orchestrator in the on-premises data center and Cisco Cloud APIC in the public cloud.

Changes in APIC Release 4.2(1)

As part of the initial release of the Cisco Cloud APIC in APIC Release 4.1(1), support was provided for the initial release of on-premises-to-cloud connectivity, or Hybrid-Cloud, where you could use the Cisco ACI マルチサイト オーケストレータ to extend an on-premises Cisco ACI site to Amazon AWS public clouds.

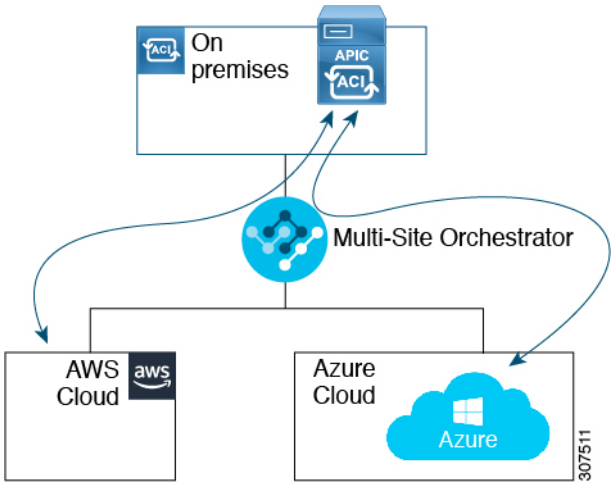


Beginning in APIC Release 4.2(1), you can now use the Cisco ACI マルチサイト オーケストレータ to extend an on-premises Cisco ACI site to Microsoft Azure public clouds.

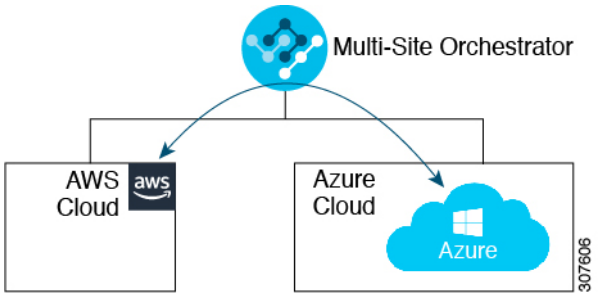


With the expanded functionality available in this release, you can also use the Cisco ACI マルチサイト オーケストレータ to establish connectivity between the following components:

- On-premises-to-cloud connectivity:
  - Connectivity for these public cloud sites:
    - On-premises Cisco ACI and Amazon AWS public cloud sites (available previously in APIC Release 4.1[1])
    - On-premises Cisco ACI and Microsoft Azure public cloud sites
  - On-premises-to-single cloud site connectivity (Hybrid-Cloud)
  - On-premises-to-multiple cloud sites connectivity (Hybrid Multi-Cloud)



- Cloud site-to-cloud site connectivity (Multi-Cloud):
  - Between Amazon AWS public cloud sites and Microsoft Azure public cloud sites
  - Between Amazon AWS public cloud sites (Amazon AWS public cloud site-to-Amazon AWS public cloud site)
  - Between Microsoft Azure public cloud sites (Microsoft Azure public cloud site-to-Microsoft Azure public cloud site)



In addition, support is also available for the single-cloud configuration (Cloud First).

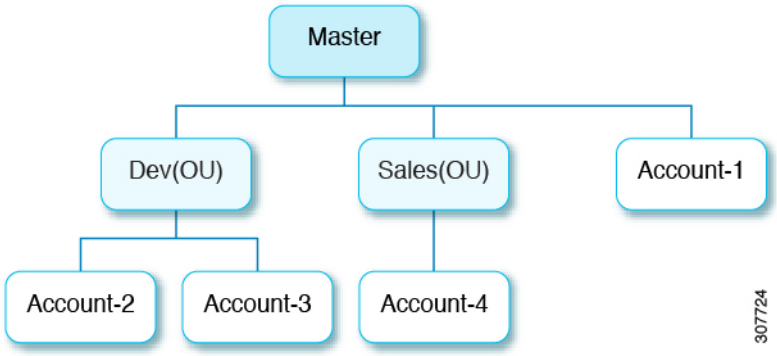
AWS Organizations と組織のユーザ テナントのサポート

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

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

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

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



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

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

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

作成済みまたは招待されたアカウントを AWS を介して組織に追加したら、Cloud APIC が AWS を通じてCloud APIC行った AWS Organizations の設定を認識するように、必要な設定を行います。

- を使用して AWS Organizations アカウントのポリシーを管理するCloud APIC場合はCloud APIC 、をマスターアカウントに展開する必要があります。にCloud APICAWS で Cloud APIC を導入する記載されている手順を使用してを AWS に展開する場合はCloud APIC 、このCloud APIC AWS 組織のマスターアカウントに (インフラテナント) を導入していることを確認してください。
- Cloud APIC は、AWS Organizations テナントのポリシーを管理するために、`OrganizationAccountAccessRole` IAM ロールを使用します。
  - マスター アカウント内の既存の組織内で AWS アカウントを**作成**した場合は、その作成した AWS アカウントに組織の `OrganizationAccountAccessRole` IAM ロールが自動的に割り当てられます。この場合、AWS の `OrganizationAccountAccessRole` の IAM ロールを手動で設定する必要はありません。
  - マスター アカウントが組織に参加するために既存の AWS アカウントを**招待**した場合は、AWS で`OrganizationAccountAccessRole` IAM ロールを手動で設定する必

要があります。組織テナントの AWS で `OrganizationAccountAccessRole` IAM ロールを設定し、Cloud APIC に関連する権限があることを確認します。

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

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

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

- その後、共有テナントの設定で説明されている手順を使用して、Cloud APIC GUI を介してテナントに組織タグを割り当てることができます。

ポリシーの用語

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

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

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

Cisco Cloud APIC Licensing

This section lists the licensing requirements to use Cisco Cloud Application Policy Infrastructure Controller (APIC).

Cisco Cloud APIC and Cisco Cloud Services Router

Cisco licenses Cisco Cloud APIC by each virtual machine (VM) instance that it manages. The Cisco Cloud APIC binary images are available on Amazon Web Services (AWS) Marketplace and support the Bring Your Own License (BYOL) model.

The Essential Cloud tier includes licenses for a single policy domain or a single instance of Cisco Cloud APIC on a public cloud. If you deploy multiple instances of Cisco Cloud APIC, buy an Advantage Cloud license for each VM instance that Cisco Cloud APIC manages.

For licensing details, see the *Cisco Application Centric Infrastructure Ordering Guide* .

In addition to obtaining one or more Cisco Cloud APIC licenses, you must register your Cisco Cloud APIC and Cisco Cloud Services Router (CSR) with Cisco Smart Software Licensing.

Cisco Smart Licensing is a unified license management system that manages software licenses across Cisco products. To learn more about Smart Software Licensing, visit https://www.cisco.com/go/smartlicensing.

Complete the following steps to register Cisco Cloud APIC and CSR:

1. Ensure that this product has access to the internet or a Smart Software Manager satellite that is installed on your network.
2. Log in to Smart Account:
   a. Smart Software Manager: https://software.cisco.com/
   b. Smart Software Manager Satellite: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html
3. Navigate to the Virtual Account containing the licenses to be used by this Product Instance.
4. Generate a Product Instance Registration Token (this identifies your Smart Account) and copy or save it.

Note Cisco Cloud APIC deploys the appropriate size of CSRs based on the setting chosen in the **Throughput of the routers** field in the Cisco Cloud APIC setup wizard. See AWS パブリック クラウドの要件 and セットアップ ウィザードを使用した Cisco Cloud APIC の設定 for more information.

Note If you remove a CSR from deployment at some point in the future (by deleting the CSR through the Cisco Cloud APIC GUI or through the cloud console or portal), this results in the CSR smart license server getting severed from that CSR. The CSR instance that got deleted will get marked as stale for 90 days and the license cannot be reused by any other new CSRs for that period of time.

To avoid this situation, rehost the CSR license depending on the release:

- For releases up to 25.0(3), rehost the **CSR 1000v** license using the instructions in Rehosting the Cisco CSR 1000v License
- For release 25.0(3) and later, rehost the **CSR 8000v** license using the instructions in ???

On-Premises Cisco ACI Licenses

If you have a single on-premises Cisco ACI site with one or more cloud sites, you can run your on-premises Cisco ACI fabric in either the Essential, Advantage, or Premier license tier.

Amazon Web Services (AWS)

You must subscribe to the CSR license through the AWS Marketplace depending on the release:

- For releases up to release 25.0(3), subscribe to **Cisco Cloud Services Router (CSR) 1000V - BYOL for Maximum Performance**.
- For release 25.0(3) and later, subscribe to **Cisco Catalyst 8000V Edge Software - BYOL**.

Cisco Cloud APIC-Related Documentation

You can find information about Cisco Cloud Application Policy Infrastructure Controller (APIC), Cisco ACI Multi-Site, and Amazon Web Services (AWS) from different resources.

Cisco Documentation

You can find documentation for Cisco products on Cisco.com:

- *Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release 4.1(1)*

  Includes list of other Cisco Cloud APIC documents.

- Cisco ACI and Cisco APIC documentation

  Includes videos, release notes, fundamentals, installation, configuration, and user guides.

- Cisco ACI Multi-Site documentation

  Includes videos, release notes, installation, configuration, and user guides.

- Cisco Cloud Services Router documentation

  Includes release notes, command reference, data sheets, installation, upgrade, and configuration guides.

AWS Documentation

You can find documentation, including user guides, FAQs, case studies, and white papers, on the AWS website.