Overview

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.
- Starting with Release 5.0(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.

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

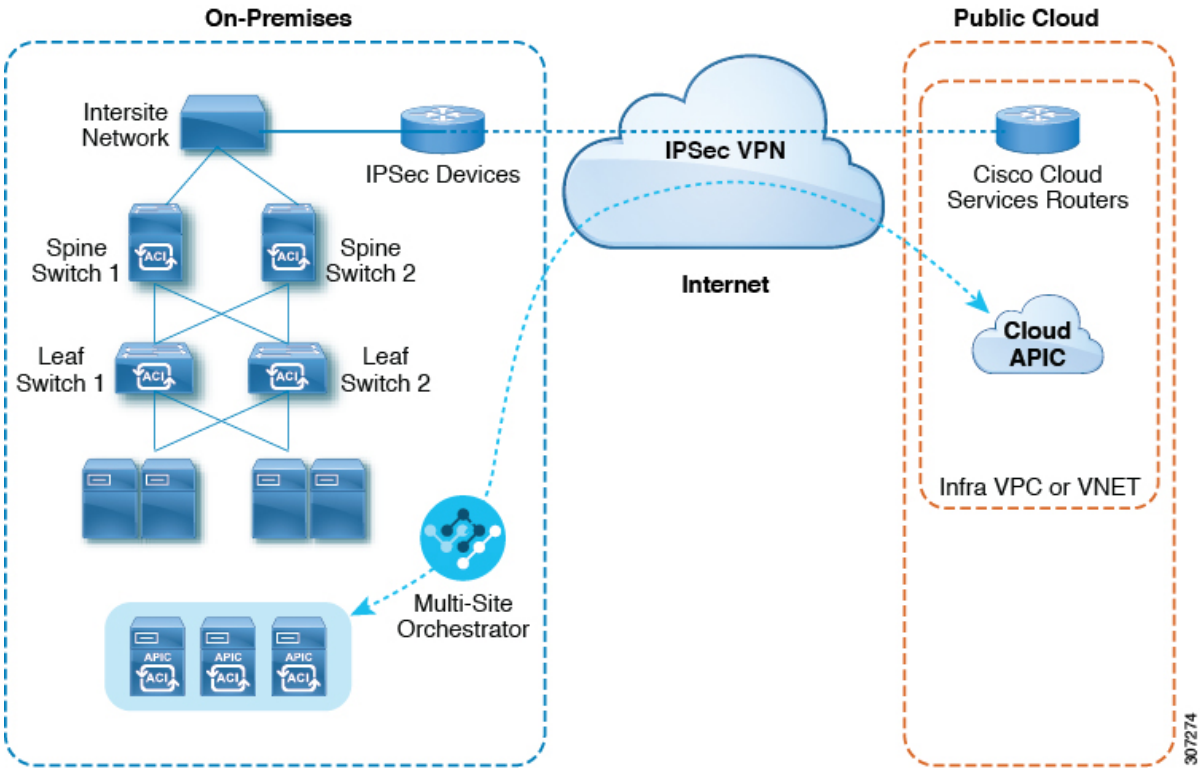
- You will subscribe to the CSR on the commercial account
- You will subscribe to the Cisco Cloud APIC on the commercial account
- You will launch the Cloud Formation template from the commercial account, which redirects the request to AWS GovCloud for the login

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 Managing Cisco Cloud APIC Through Cisco ACI Multi-Site 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 Managing Cisco Cloud APIC Through Cisco ACI Multi-Site 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 Deploying the Cloud APIC in AWS and Configuring Cisco Cloud APIC Using the Setup Wizard in this guide.

Cisco Cloud Services Router

The Cisco Cloud Services Router 1000V (CSR 1000V) is a virtual router that delivers comprehensive WAN gateway and network services into virtual and cloud environments. The CSR 1000V enables enterprises to extend their WANs into provider-hosted clouds. Two CSR 1000Vs are required for Cisco Cloud ACI solution.

For more information, see the Cisco CSR 1000v 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

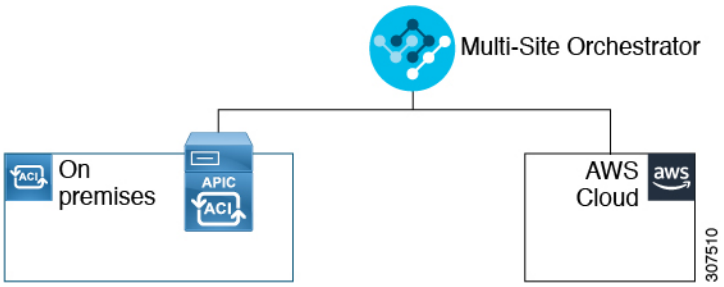
You need Internet connectivity with a VPN from the IPsec router, including a publicly routable IP address and with sufficient bandwidth for AWS or Microsoft Azure connectivity.

Management Connection

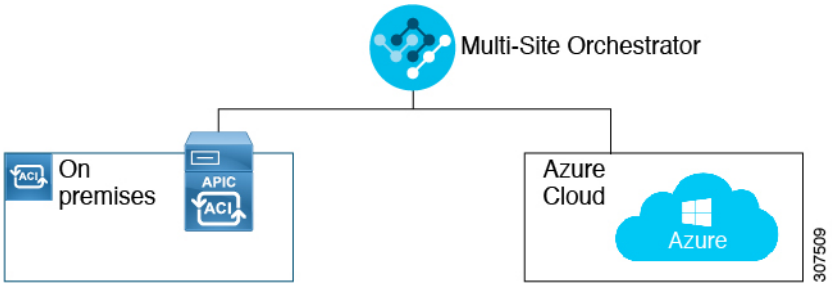
You need a management connection between the Multi-Site Orchestrator in the on-premises data center and Cisco Cloud APIC in the public cloud.

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 Multi-Site Orchestrator to extend an on-premises Cisco ACI site to Amazon AWS public clouds.

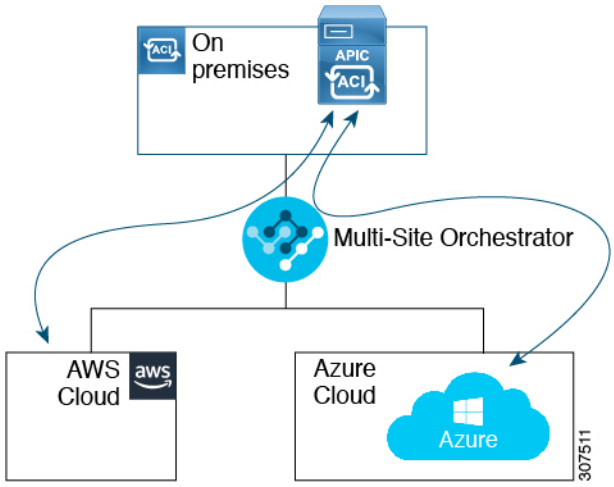


Beginning in APIC Release 4.2(1), you can now use the Cisco ACI Multi-Site Orchestrator to extend an on-premises Cisco ACI site to Microsoft Azure public clouds.

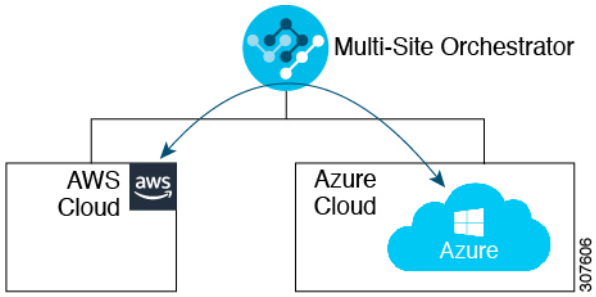


With the expanded functionality available in this release, you can also use the Cisco ACI Multi-Site Orchestrator to establish connectivity between the following components:

- 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).

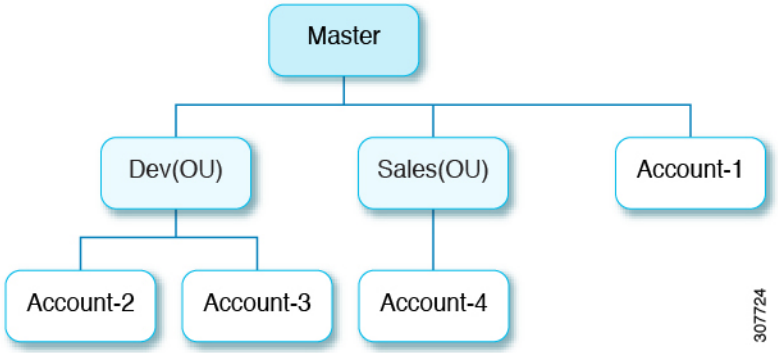
Support for AWS Organizations and Organization User Tenant

With multiple accounts in an organization, it is not easy to control access policies and permissions for various accounts individually, whereas it is easier to do so at the organizational level or at a sub-organizational level within the organization.

Using AWS Organizations, an enterprise might have multiple AWS accounts managed in an organization, as explained here:

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

This control of the access policies for accounts (or sub-accounts) in the organization is done by the master account of the organization, which is at the root of accounts hierarchy in the organization. The figure below shows an example setup of accounts in an organization.



There are two ways that AWS accounts become part of an AWS Organization:

- **Created**: Within the existing organization in the master account, you can create an AWS account that is automatically part of your AWS organization using the AWS GUI or the AWS API.
- **Invited**: For accounts that are created outside the organization but need to be joined to the organization, an invitation needs to be sent by the master account to the account owner. After accepting the invitation, the invited account becomes a sub-account within the organization.

If you are using AWS Organizations to consolidate and manage your AWS accounts, you will use AWS Organizations to set up your organization and add the created or invited accounts, as you would normally. See Creating an Organization for more information.

Once you have added the created or invited accounts to your organization through AWS, you will then make the necessary Cloud APIC configurations so that the Cloud APIC recognizes the AWS Organization configurations that you've made through AWS:

- If you want to manage policies for AWS Organization accounts through the Cloud APIC, the Cloud APIC must be deployed in the master account. When you deploy the Cloud APIC in AWS using the instructions provided in Deploying the Cloud APIC in AWS, verify that you are deploying the Cloud APIC (the Cloud APIC infra tenant) in the master account for this AWS organization.
- The Cloud APIC uses the `OrganizationAccountAccessRole` IAM role to manage policies for AWS Organization tenants.
    - If you **created** an AWS account within the existing organization in the master account, the `OrganizationAccountAccessRole` IAM role is automatically assigned to that created AWS account. You do not have to manually configure the `OrganizationAccountAccessRole` IAM role in AWS in this case.
    - If the master account **invited** an existing AWS account to join the organization, then you must manually configure the `OrganizationAccountAccessRole` IAM role in AWS. Configure the `OrganizationAccountAccessRole` IAM role in AWS for the organization tenant and verify that it has Cloud APIC-related permissions available.

      The `OrganizationAccountAccessRole` IAM role, together with the SCP (Service Control Policy) used for the organization or the account, must have the minimum permissions that are required by the Cloud APIC to manage policies for the tenants. The access policy requirement is the same as the requirement for the trusted or untrusted tenants.

      For more information, see the "Configure a Tenant AWS Provider" section in the *Cisco Cloud APIC for AWS User Guide*, Version 4.2(x) or later, located here:

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

- You can then assign the Organization tag to tenants through the Cloud APIC GUI using procedures described in Configuring a Shared Tenant.

Policy Terminology

A key feature of Cisco Cloud APIC is translation of Cisco Application Centric Infrastructure (ACI) policy to the native constructs of the public cloud.

The following table lists Cisco ACI policy terms and the equivalent terms in Amazon Web Services (AWS).

Cisco ACI	AWS
Tenant	User account
AAA user, security domain	Identity and Access Management (IAM)
Virtual Routing and Forwarding (VRF)	VPC
BD subnet	Virtual Private Cloud (VPC) subnet (CIDR)
ACI infra (or ACI infra tenant)	VPC (named Infra VPC by Cloud APIC)
Contract, filter	Security Group Rule
Taboo	Network access list
EPG	Security group
EP-to-EPG mapping	Tag, label
Endpoint	Network adapter on EC2 instances

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 Requirements for the AWS Public Cloud and Configuring Cisco Cloud APIC Using the Setup Wizard 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 new CSR to the old license by following the procedures provided here:

Rehosting the Cisco CSR 1000v License

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 Cisco CSR on the AWS website.

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.