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 the 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.

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 component 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 connectivity.
- 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 or between cloud sites.

Azure Government Support

Starting with Release 4.2(3), Cisco Cloud APIC supports Azure Government for on-premises-to-cloud connectivity (Hybrid-Cloud and Hybrid Multi-Cloud), cloud site-to-cloud site connectivity (Multi-Cloud), and single-cloud configurations (Cloud First).

Cisco Cloud APIC supports the following Azure Government regions:

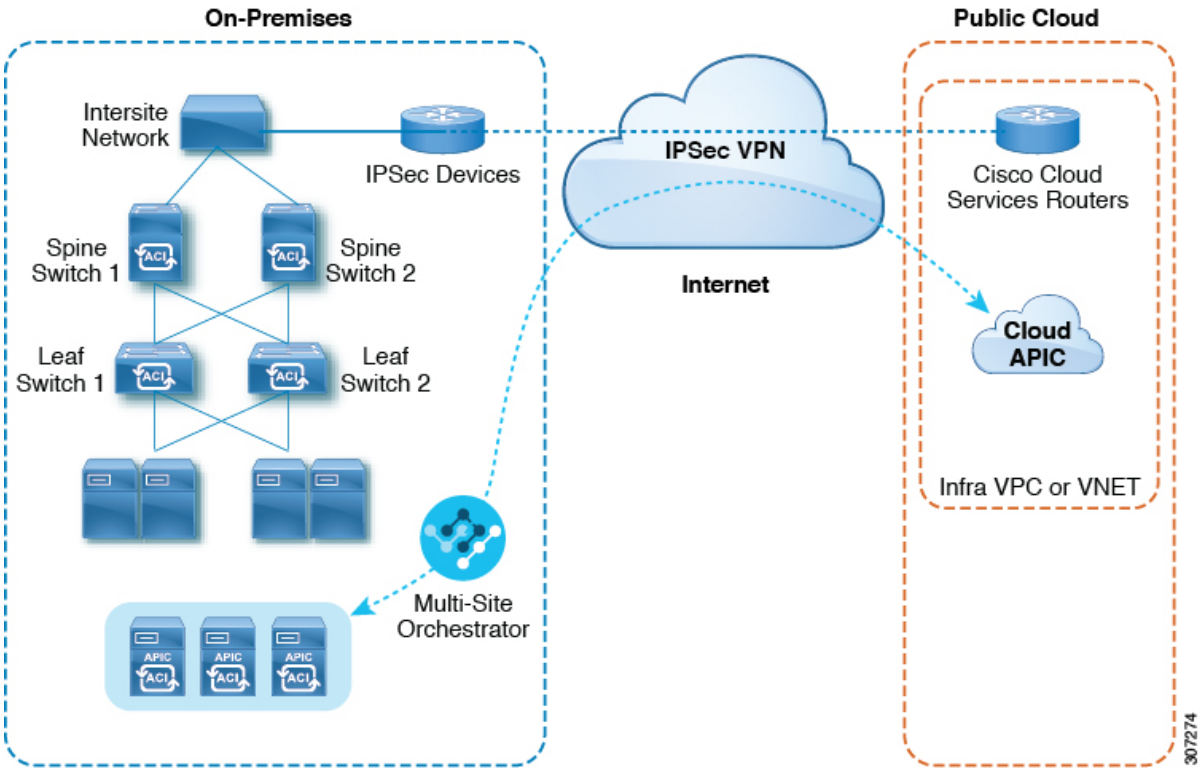
- US DoD Central
- US DoD East
- US Gov Arizona
- US Gov Texas
- US Gov Virginia

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 Microsoft Azure 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 configuration information for 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 configuration information for 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 cloud site in Microsoft Azure.

Azure 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 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*.

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.

Microsoft Azure public cloud

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

For more information, see the documentation on the Microsoft Azure website.

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

IPsec VPN

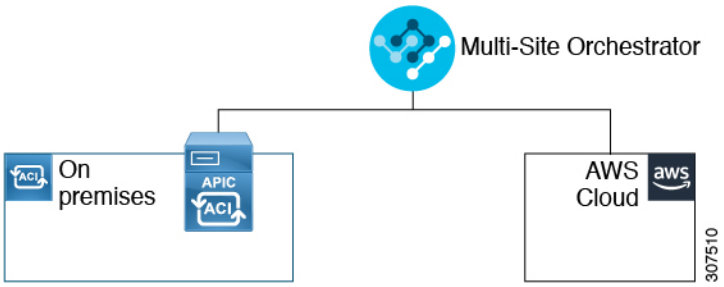
You need Internet connectivity with a VPN from the IPsec router, including a publicly routable IP address and with sufficient bandwidth for Microsoft Azure connectivity.

Management Connection

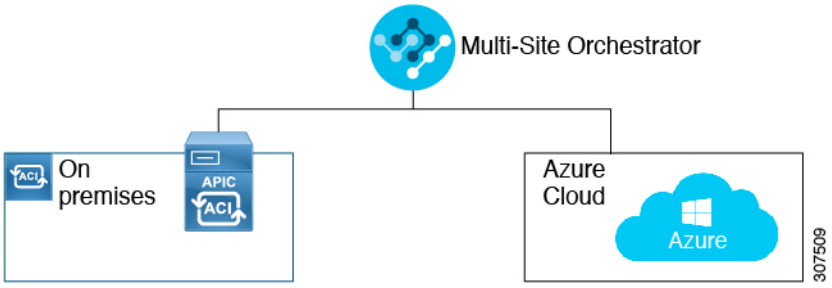
You need a management connection between the Multi-Site Orchestrator in the on-premises data center and Cisco Cloud APIC in the Microsoft Azure public cloud.

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.

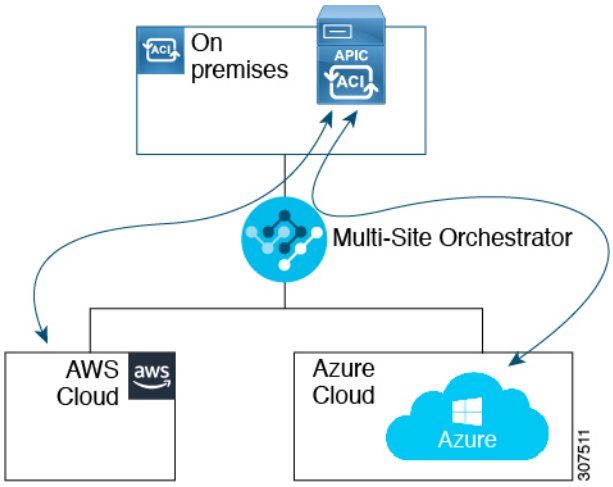


Beginning in APIC Release 4.2(1), you can now use the Cisco ACI Multi-Site Orchestrator to extend an on-premises Cisco ACI site to Microsoft Azure public clouds.

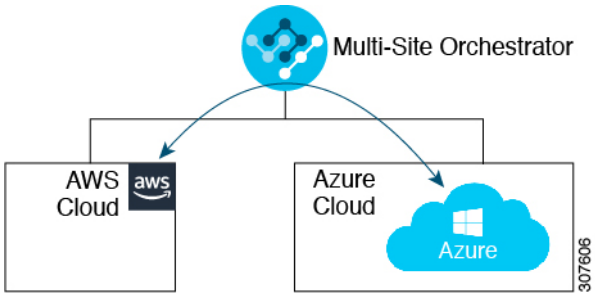


With the expanded functionality available in this release, you can also use the Cisco ACI Multi-Site Orchestrator to establish connectivity between the following components:

- 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).

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.

Policy Mapping Between Cisco ACI and Microsoft Azure

The following table lists Cisco ACI policy terms and the equivalent terms in Microsoft Azure.

Cisco ACI	Azure
Tenant (Region, VRF)	Resource group
Virtual Routing and Forwarding (VRF)	Virtual network

Cisco ACI	Azure
BD subnet	Subnet
Contract, filter	Outbound rule, inbound rule
EP-to-EPG mapping	Application Security Group (ASG), Network Security Group (NSG)
Endpoint	Network adapter on VM instances

About Tenants

Azure has an active directory structure. The top level structure is the organization, and underneath the organization are the directories (also known as Azure tenants). Inside the directories, you can have one or more Azure subscriptions.

In Azure, the same Azure subscription ID can be used for multiple ACI fabric tenants. This means that you could configure the infra tenant using one Azure subscription, and then configure more user tenants in the same subscription. ACI tenants are tied to Azure subscriptions.

As part of the Cloud APIC configuration, you will configure tenants in two areas:

- Configuring Cloud APIC Tenant Accounts, on page 7
- Configuring Azure Tenant Accounts, on page 7

Configuring Cloud APIC Tenant Accounts

When configuring a tenant in Cloud APIC, you will choose from one of these options:

- **Create Your Own Managed Identity:** You will choose this option when the Azure subscriptions are in the same directory (of the same organization).
- **Create Your Own Unmanaged Identity:** You will choose this option when you want to configure tenants in different subscriptions. The subscriptions are either in different Azure directories (Azure tenants) in the same organization, or the subscriptions can be in different organizations.
- **Shared:** You will choose this option when you have already associated Azure subscriptions with either of the two methods above and want to create more tenants in that subscription.

You will be making these configurations in the Cloud APIC GUI using the procedures in Configuring a Tenant.

Configuring Azure Tenant Accounts

Once you have decided on the type of tenant that you will be configuring in the Cloud APIC, you will then have to make the necessary subscription configurations in the Azure portal to allow for that type of Cloud APIC tenant. You will be making the necessary subscription configurations in the Azure portal before you configure the tenant in your Cloud APIC.

- If you will be configuring tenants in the Cloud APIC using **managed identity**, then, in the Azure portal, you will be adding a role assignment for a **virtual machine**. You can use this option when the Azure subscriptions are in the same Azure directory (of the same organization).

Note If your Azure subscriptions are in different directories and you want to configure tenants using **managed identity**, you can go to the Azure console and click on each of the subscriptions and move the subscriptions under the same Azure directory. You can only do this if the directories (containing the different subscriptions) are a child of the same parent organization.

The procedures for adding a role assignment in Azure for a virtual machine are provided in Adding a Role Assignment for a Virtual Machine.

- If you will be configuring tenants in the Cloud APIC using **unmanaged identity**, then, in the Azure portal, you will be adding a role assignment for an **app**, where the cloud resources will be managed through a specific application.

  The procedures for adding a role assignment in Azure for an app are provided in Adding a Role Assignment for an App.

- If you will be configuring tenants in the Cloud APIC using the **shared** option, you do not have to make any configurations in Azure specifically for a shared tenant, because you will have already associated Azure subscriptions with either of the two methods above. With the shared tenant, you will just create more tenants in that existing subscription.

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 Microsoft Azure portal 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.

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.

Microsoft Azure

You must subscribe to the Cisco Cloud Services Router (CSR) 1000V - Bring Your Own License (BYOL) for Maximum Performance. To subscribe through the Microsoft Azure Marketplace, follow the instructions in Subscribing to the Cisco Cloud Services Router 1000V.

Cisco Cloud APIC-Related Documentation

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

Cisco Documentation

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

- *Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release 4.2(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.

Microsoft Azure Documentation

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