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. Cisco ACI can use Cisco Cloud APIC to extend a Cisco ACI Multi-Site fabric to Amazon Web Services (AWS) and Microsoft Azure public clouds.

Benefits of 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.

Cisco Cloud APIC

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 AWS public cloud
- 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

Detailed information about Cisco APIC requirements and installation procedures is available from one of the following two documents based on the public cloud type:

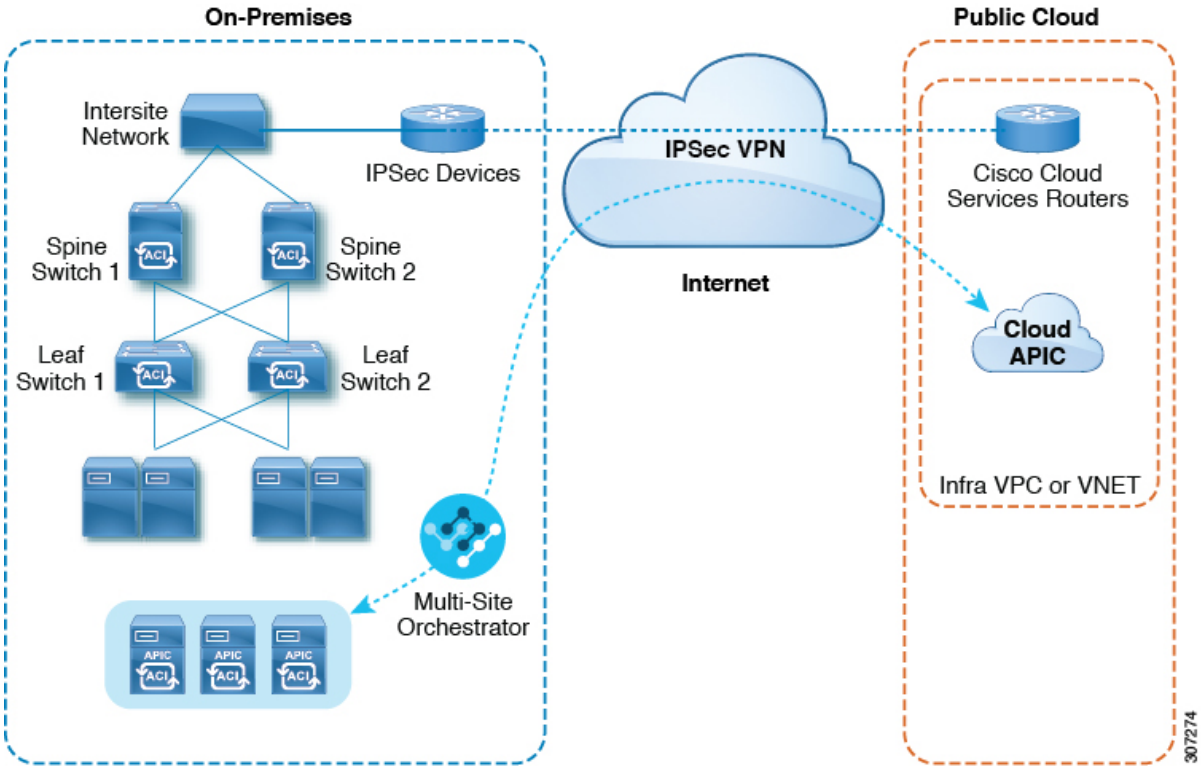
- *Cisco Cloud APIC for AWS Installation Guide, Release 5.0(x)*
- *Cisco Cloud APIC for Azure Installation Guide, Release 5.0(x)*

Components of Extending Cisco ACI Fabric to the Public Cloud

Several components—each with its specific role—are required to extend the Cisco ACI fabric into the 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.

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.

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.

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.