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 Network Controller to extend a multi-site fabric to Amazon Web Services (AWS), Microsoft Azure, and Google Cloud public clouds.

What Cisco Cloud Network Controller Is

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

- Provides an interface that is similar to the existing Cisco APIC to interact with the Amazon AWS, Microsoft Azure, or Google Cloud 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 Network Controller is a key part of Cisco ACI extension to the public cloud. Cisco Cloud Network Controller 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.

AWS GovCloud Support

Cisco Cloud Network Controller supports AWS GovCloud in the us-gov-west and us-gov-east regions. Cisco CCRs can also be deployed in the us-gov-east region.

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

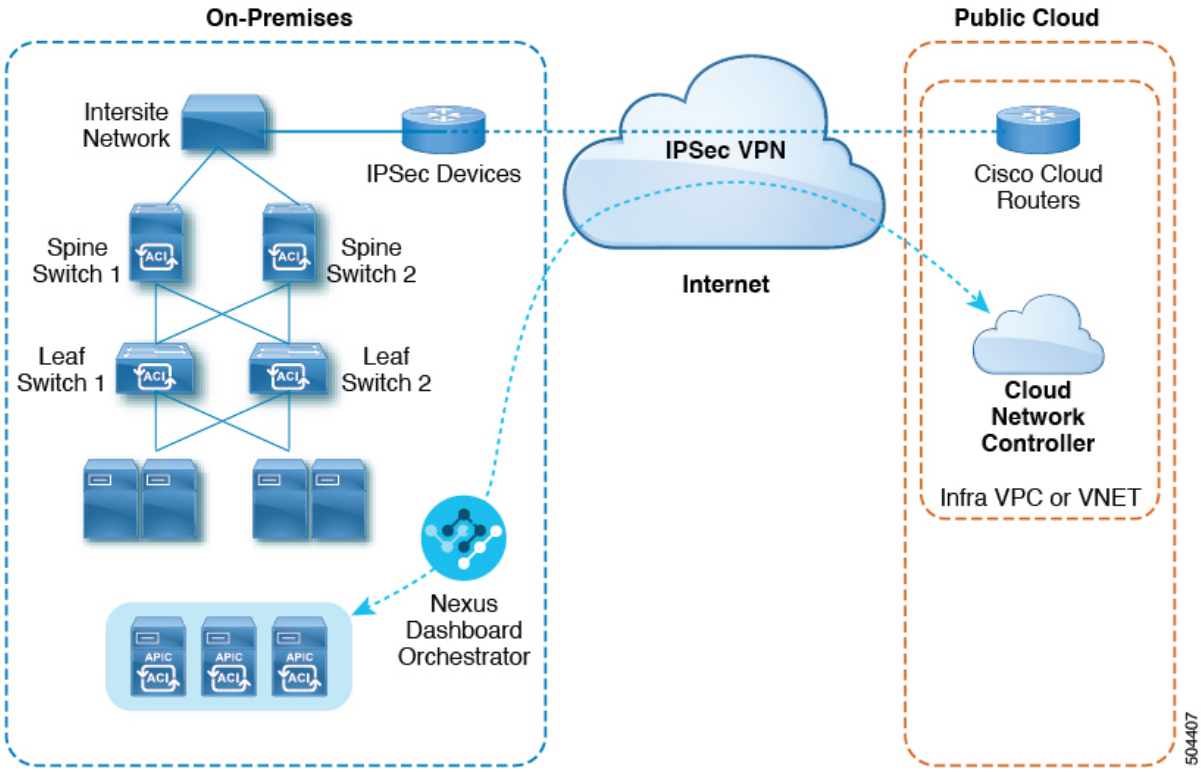
- You will subscribe to the CCR on the commercial account.
- You will subscribe to the Cisco Cloud Network Controller on the commercial account.
- You will launch the Cloud Formation template from the commercial account, which redirects the request to AWS GovCloud for the login.

Components of Extending Cisco ACI Fabric to the Public Cloud

Several components—each with its specific role—are required to extend the Multi-Site fabric to the public cloud.

The following illustration shows the architecture of Cisco Cloud Network Controller.

Figure 1: Cisco Cloud Network Controller 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.

Multi-Site and Multi -Site Orchestrator/Cisco Nexus Dashboard Orchestrator

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 Multi-Site installed to use Cisco Cloud Network Controller to extend the fabric into the public cloud.

For more information, see the Nexus Dashboard documentation on Cisco.com and the section Managing Cisco Cloud Network Controller Through Multi-Site in this guide.

Cisco Nexus Dashboard Orchestrator (NDO) 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 Nexus Dashboard Orchestrator creates connectivity between the on-premises data center and the public cloud. Use 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 *Nexus Dashboard Configuration Guide* on Cisco.com.

For more information, see the Nexus Dashboard documentation on Cisco.com and the section Managing Cisco Cloud Network Controller Through 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 Network Controller

Cisco Cloud Network Controller 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 Router (CCR) across all regions.
- Renders the Cisco ACI policy model in the public cloud, and manages cloud health.

For more information, see *Cisco Cloud Network Controller Release Notes*. Also see the sections Deploying the Cisco Cloud Network Controller in AWS and Configuring Cisco Cloud Network Controller Using the Setup Wizard in this guide.

Cisco Cloud Router

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

For release 25.0(3) and later, Cisco Cloud Network Controller uses the **Cisco Catalyst 8000V** as the cloud services router. For more information on this CCR, see the CCR 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.

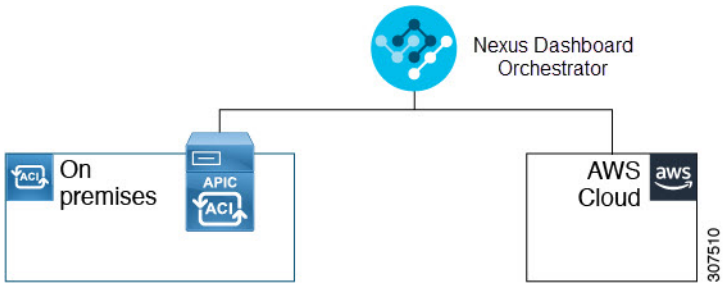
Management Connection

You need a management connection between the Nexus Dashboard Orchestrator in the on-premises data center and Cisco Cloud Network Controller in the public cloud.

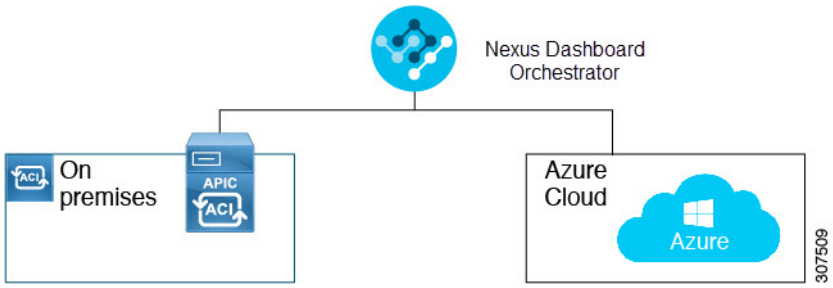
Supported Cloud Computing Platforms and Connectivity Options

Cisco Cloud Network Controller is supported on the following cloud computing platforms:

- As part of the initial release of the Cisco Cloud Network Controller in release 4.1(1), support is provided for on-premises-to-cloud connectivity, or Hybrid-Cloud, where you could use the Cisco Cisco Nexus Dashboard Orchestrator to extend an on-premises Cisco ACI site to Amazon AWS public clouds.



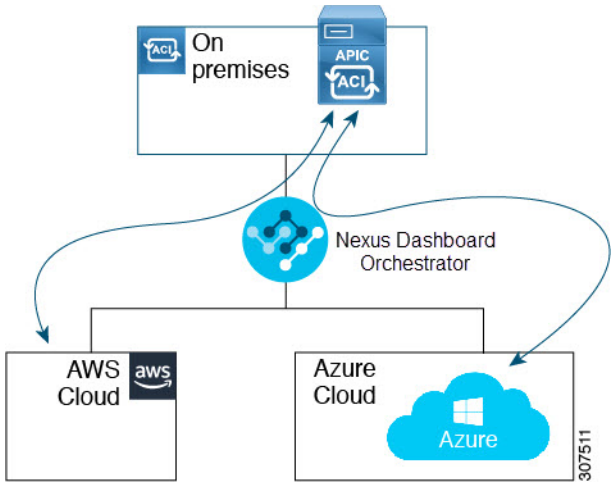
- Beginning in release 4.2(1), support is available for using the Cisco Cisco Nexus Dashboard Orchestrator to extend an on-premises Cisco ACI site to Microsoft Azure public clouds.



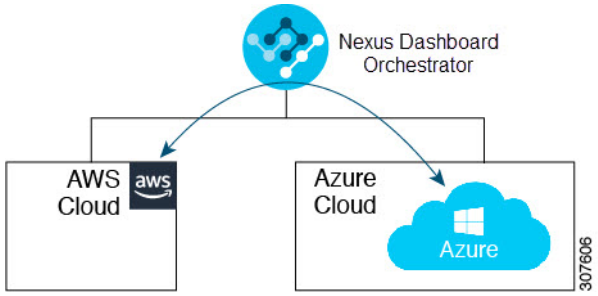
- Support is available for using the Cisco Cisco Nexus Dashboard Orchestrator to extend an on-premises Cisco ACI site to Google Cloud public clouds.

You can also use the Cisco Nexus Dashboard 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
    - On-premises Cisco ACI and Microsoft Azure public cloud sites
    - On-premises Cisco ACI and Google Cloud 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 (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)
  - Between Google Cloud public cloud sites (Google Cloud public cloud site-to-Google Cloud public cloud site)
  - Between Amazon AWS, Microsoft Azure, and Google Cloud public cloud sites



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

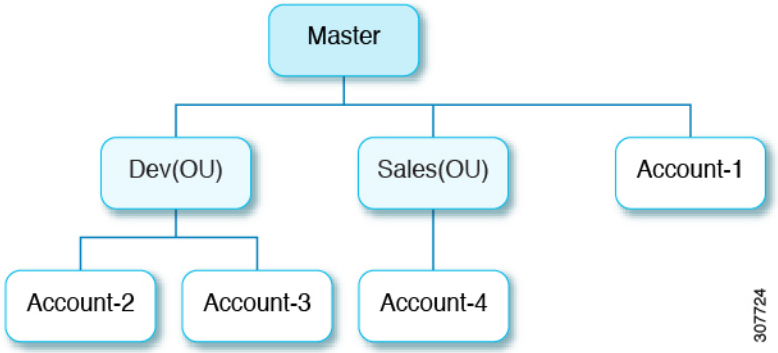
Support for AWS Organizations and Organization User Tenant

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 Cisco Cloud Network Controller configurations so that the Cisco Cloud Network Controller recognizes the AWS Organization configurations that you've made through AWS. The Cisco Cloud Network Controller 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 Cisco Cloud Network Controller -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 Cisco Cloud Network Controller 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 Network Controller for AWS User Guide

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

Policy Terminology

A key feature of Cisco Cloud Network Controller 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 Cisco Cloud Network Controller)
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 Network Controller Licensing

This section lists the licensing requirements to use Cisco Cloud Network Controller.

Cisco Catalyst 8000V

The Cisco Catalyst 8000V on Cisco Cloud Network Controller supports the following licensing models:

1. **Bring Your Own License (BYOL)** Licensing Model
2. **Pay As You Go (PAYG)** Licensing Model

BYOL Licensing Model

The BYOL licensing model on Cisco Catalyst 8000V which requires you to purchase your Catalyst 8000V Cisco DNA license from Cisco and deploy it in the cloud.

- For instructions on subscribing to one of the tier-based Cisco Catalyst 8000V licenses, see Cisco Catalyst 8000V Edge Software.
- For more information on different throughputs based on the tiers, see the "Throughput" section in "About the Cisco Catalyst 8000V" in the Cisco Cloud Network Controller for AWS User Guide.

PAYG Licensing Model

Beginning with the 25.0(4) release, Cisco Cloud Network Controller supports Pay-As-You-Go (PAYG) Licensing Model on Cisco Catalyst 8000V which allows users to deploy a Catalyst 8000V instance in the cloud based on the VM size and purchase the usage on an hourly basis.

As you completely depend on the VM size to get the throughput, the PAYG licensing model can be enabled only by first un-deploying the current Cisco Catalyst 8000V and then re-deploying it using the First Time Set Up with the new VM size. For more information, see Configuring Cisco Cloud Network Controller Using the Setup Wizard.

Note The procedure for switching between licenses can also be used if you would like to switch between the two licensing types available.

Note There are two PAYG options for consuming licenses in the AWS marketplace: **Catalyst 8000V Cisco DNA Essentials** and **Catalyst 8000V Cisco DNA Advantage** . Cisco Cloud Network Controller will make use of **Catalyst 8000V Cisco DNA Advantage**. For features supported by the "Cisco DNA Advantage" subscription, see Cisco DNA Software SD-WAN and Routing Matrices

Cisco Cloud Network Controller and On-Premises ACI Licensing Summary

- Licensing requirements for all leaf switches on the on-premises Cisco ACI sites:
  - If the Cisco ACI on-premises site is a single site, then use the Essentials license tier (or higher) for the on-premises leaf switches
  - If the Cisco ACI on-premises site is a multi-site, then use the Advantage license tier (or higher) for the on-premises leaf switches
- Licensing requirements for all VM instances managed by Cisco Cloud Network Controller instances:
  - If the Cisco ACI on the cloud has only one Cisco Cloud Network Controller, then use the Essentials Cloud license tier (or higher) for Cisco Cloud Network Controller
  - If the Cisco ACI on the cloud has more than one Cisco Cloud Network Controller, then use the Advantage Cloud license tier (or higher) for Cisco Cloud Network Controller

Amazon Web Services (AWS)

You must subscribe through the AWS Marketplace, depending on the type of license:

- For **BYOL Licensing Model**, subscribe to **Cisco Catalyst 8000V Edge Software - BYOL**.
- For **PAYG Licensing Model**, subscribe to **Cisco Catalyst 8000V Edge Software – PAYG**

Cisco Cloud Network Controller Related Documentation

You can find information about Cisco Cloud Network Controller, Nexus Dashboard, and Amazon Web Services (AWS) from different resources.

Cisco Documentation

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

- Cisco Cloud Network Controller documentation

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

- Nexus Dashboard documentation

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

- Cisco Cloud 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.