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.

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 component 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 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 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.

Azure Government Support

Cisco Cloud Network Controller 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 Network Controller supports the following Azure Government regions:

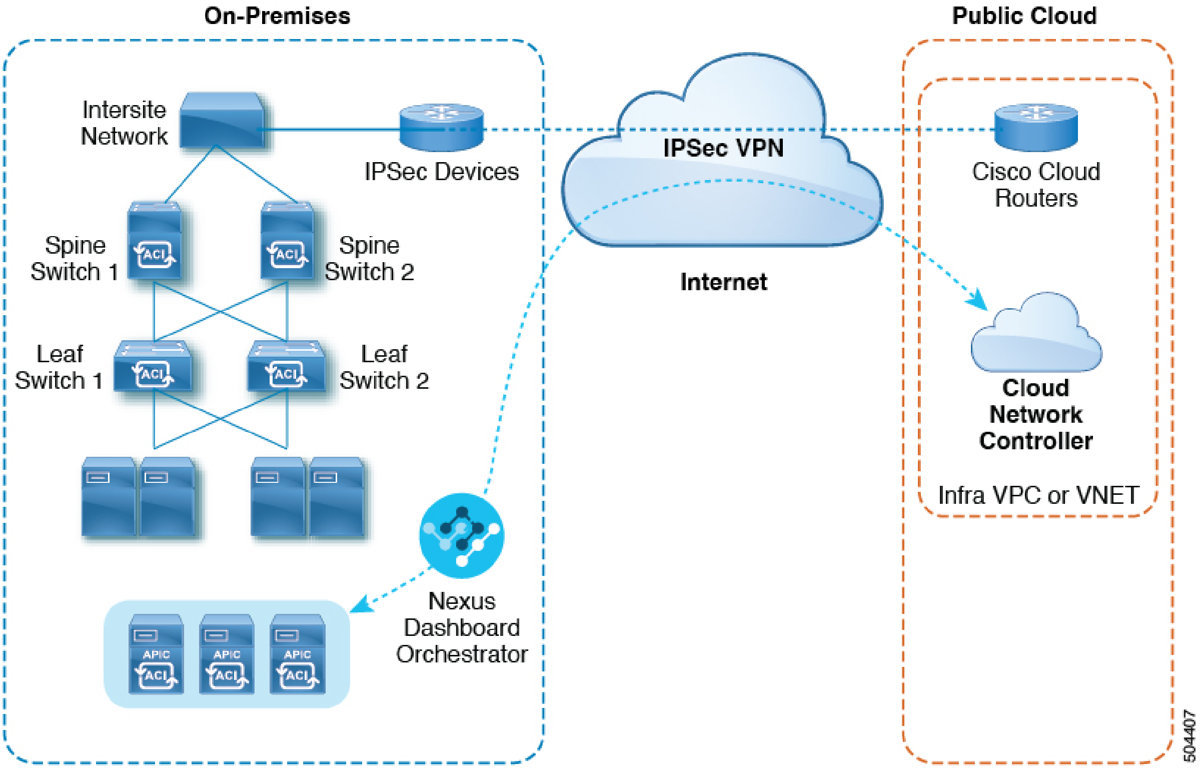
- US DoD Central
- US DoD East
- US Gov Arizona
- US Gov Texas
- US Gov Virginia

Components of Extending Cisco ACI Fabric to the Public Cloud

Several components, each with its specific role, are required to extend the Multi-Site fabric to the Microsoft Azure 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 Multi-Site documentation on Cisco.com and the configuration information for 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 *Multi-Site Configuration Guide* on Cisco.com.

For more information, see the Multi-Site documentation on Cisco.com and the configuration information for 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 Network Controller

Cisco Cloud Network Controller performs the following actions:

- Defines a site on the public cloud, provisions the cloud infra virtual networks (VNETs) and manages the 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*.

CCR

The 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.

Cisco Cloud Network Controller uses the **Cisco Catalyst 8000V** as the cloud services router. For more information on this CCR, see the Cisco CCR 8000v 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 Nexus Dashboard Orchestrator in the on-premises data center and Cisco Cloud Network Controller in the Microsoft Azure public cloud.

Supported Cloud Computing Platforms and Connectivity Options

You can 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).

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.

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
BD subnet	Subnet
Contract, filter	Outbound rule, inbound rule

Cisco ACI	Azure
EP-to-EPG mapping	Application Security Group (ASG), Network Security Group (NSG)
Endpoint	Network adapter on VM instances

Understanding Tenants, Identities, and Subscriptions

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.

The relationship between certain Azure components is as follows:

Tenants > **Subscriptions** > **Resource Groups** > **Resources**

Where:

- One tenant can have multiple subscriptions, but each subscription can belong to only one tenant.
- One subscription can have multiple resource groups, but each resource group can belong to only one subscription.
- One resource group can have multiple resources, but each resource can belong to only one subscription.

The following sections provide more detail about each of these components:

- Mapping Azure and Cisco Cloud Network Controller Components, on page 6
- About Azure Subscriptions, on page 6
- About Tenants and Identities, on page 7

Mapping Azure and Cisco Cloud Network Controller Components

In Cisco Cloud Network Controller, each Azure resource group is mapped to one Cisco Cloud Network Controller tenant, and one Cisco Cloud Network Controller tenant can have multiple Azure resource groups.

The relationship between certain Cisco Cloud Network Controller components is as follows:

Tenants > **VRFs** > **Regions**

When you create a VRF in Cisco Cloud Network Controller, a new resource group is also created on Azure.

About Azure Subscriptions

An Azure subscription is used to pay for Azure cloud services. An Azure subscription has a trust relationship with Azure Active Directories (Azure ADs), where the subscription uses the Azure AD to authenticate users, services, and devices. While multiple subscriptions can trust the same Azure AD, each subscription can trust only one Azure AD.

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.

About Tenants and Identities

Following are the different types of tenants and identities available through Azure and Cisco Cloud Network Controller.

> **Note** Both managed identity and service principal is supported as an access type for the infra tenants and the user tenants.

Managed Identity

Managed identities provide an identity for applications to use when connecting to resources that support Azure AD authentication. Applications can use the managed identity to obtain Azure AD tokens. For example, an application could use a managed identity to access resources like Azure Key Vault, where developers can store credentials in a secure manner or to access storage accounts.

Following are several benefits to using managed identities:

- You don't need to manage credentials, since credentials are not even accessible to you.
- You can use managed identities to authenticate to any resource that supports Azure AD authentication, including your own applications.
- Managed identities can be used without any additional cost.

For additional information on managed identities in Azure, see:

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

If you are configuring tenants in the Cisco Cloud Network Controller using **managed identity**, then you will make the following configurations in the Azure portal and in the Cisco Cloud Network Controller:

1. In the Azure portal, you will add a role assignment for a **virtual machine**. You 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.

2. In the Cisco Cloud Network Controller , you will choose the **Create Your Own Managed Identity** option when configuring a tenant in Cisco Cloud Network Controller . You will configure this option in the Cisco Cloud Network Controller GUI using the procedures in Configuring a Tenant.

Service Principal

An Azure **service principal** is an identity created for use with applications, hosted services, and automated tools to access Azure resources. You would use the service principal identity 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.

If you are configuring tenants in the Cisco Cloud Network Controller using **service principal**, then you will make the following configurations in the Azure portal and in the Cisco Cloud Network Controller:

1. 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.

2. In the Cisco Cloud Network Controller, you will choose the **Service Principal** option when configuring a tenant in Cisco Cloud Network Controller. The subscriptions that you enter in this page can be in different Azure directories (Azure tenants) in the same organization, or the subscriptions can be in different organizations. You will configure this option in the Cisco Cloud Network Controller GUI using the procedures in Configuring a Tenant.

Shared Tenant

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.

If you are configuring a tenant in the Cisco Cloud Network Controller as **shared tenant**, then you will make the following configurations in the Azure portal and in the Cisco Cloud Network Controller:

1. 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.

2. In the Cisco Cloud Network Controller, you will choose the **Shared** option when configuring a tenant in Cisco Cloud Network Controller. You will configure this option in the Cisco Cloud Network Controller GUI using the procedures in Configuring a Tenant.

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 Cisco Catalyst 8000V supports subscription-based licensing.

- 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 Requirements for the Azure Public Cloud.

Cisco Cloud Network Controller makes use of the “Cisco DNA Advantage” subscription. For features supported by the “Cisco DNA Advantage” subscription, see Cisco DNA Software SD-WAN and Routing Matrices.

PAYG Licensing Model

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 enabling the PAYG license 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 Azure 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

Microsoft Azure

You must subscribe through the Microsoft Azure 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**.

To subscribe through the Microsoft Azure Marketplace, follow the instructions in Subscribing to the Cisco Cloud Router 8000V.

Cisco Cloud Network Controller Related Documentation

You can find information about Cisco Cloud Network Controller, Nexus Dashboard, and Microsoft Azure 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.

Microsoft Azure Documentation

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