Preparing for Installing Cisco Cloud APIC

Requirements for Extending the Cisco ACI Fabric to the Public Cloud

Before you can extend the Cisco Application Centric Infrastructure (ACI) to the public cloud, you must meet requirements for the Cisco ACI on-premises datacenter and the Amazon Web Services (AWS) deployment.

Requirements for the On-Premises Data Center

This section lists the on-premises data center requirements for extending the Cisco Application Centric Infrastructure (ACI) fabric to the public cloud.

- Ensure that the Cisco ACI fabric is installed with the following components:
  - At least two Cisco Nexus EX or FX spine switches, or Nexus 9332C and 9364C spine switches, running Cisco Nexus 9000 Series ACI Mode switch software release 14.1 or later.
  - At least two Cisco Nexus pre-EX, EX, or FX leaf switches running the Cisco Nexus 9000 Series ACI Mode switch software release 14.1 or later.
  - At least one Cisco Application Policy Infrastructure Controller (APIC) running release 4.1 or later and Cisco ACI Multi-Site Orchestrator (MSO) Release 2.2(x) or later.
- Cisco ACI Multi-Site Orchestrator 2.2(x) deployed with basic configuration.
- A router capable of terminating Internet Protocol Security (IPsec).
- You need to make sure that you have enough bandwidth for tenant traffic between on-premises and cloud sites.
- A Cisco SMART Licensing account and a Cisco ACI Leaf Advantage license.

  All leafs on the on-premises site or sites must have Cisco ACI leaf licenses.
- Workloads that are connected to the Cisco ACI fabric.

- An intersite network (ISN) that is configured between the Cisco ACI fabric (spine) and the IP Security (IPsec) termination device.

  For information about creating an ISN, see the "Multipod" chapter of the *Cisco APIC Layer 3 Networking Configuration Guide*.

- Certain firewall ports must be permitted if you are deploying firewalls between your on-premises and AWS deployments. These include HTTPS access for the Cisco Cloud APIC, IPsec ports for each AWS CSR, and SSH connectivity for AWS CSR remote management.

  These firewall ports are described in more detail in Cloud APIC Communication Ports, on page 4 in this guide.

Requirements for the AWS Public Cloud

This section lists the Amazon Web Services (AWS) requirements for extending the Cisco Application Centric Infrastructure (ACI) fabric to the public cloud.

AWS Accounts

You need one AWS account for the Infra tenant, and you need one AWS account for each user tenant.

For example, if you want to create two user tenants, you need three AWS accounts. You must have one account for each user tenant and one account for the infra tenant. The user tenant can be trusted or untrusted. For details, see the section Setting Up the AWS Account for the User Tenant in this guide.

AWS Resources

You need the following resources as part of the AWS deployment:

- Access to the Cisco APIC 5.0 Amazon Machine Image (AMI).

  Note To have access to the AMI, you must subscribe to the Cisco Cloud APIC in the Amazon Marketplace.

- Two instances of Elastic Cloud Computer (EC2), which function as virtual machines (VM) for applications running in the cloud.
- Virtual Private Clouds (VPCs), subnets, a virtual private gateway (VGW), an Internet gateway (IGW), security groups, and resources that are based on tasks you plan to perform.

Cisco Cloud Services Router (CSR)

Subscribe to the Cisco Cloud Services Router (CSR) Bring Your Own License (BYOL) through the AWS Marketplace. See Cisco Cloud APIC Licensing for more information.

Deploy the CSRs in the appropriate size, depending on the bandwidth requirement defined during the Cisco Cloud APIC setup.

The value for the throughput of the routers determines the size of the CSR instance that you deploy; a higher value for the throughput results in the deployment of a larger VM. CSR licensing is based on the throughput

configuration that you set as part of the Cisco Cloud APIC setup process. You need the equivalent or higher license in your Smart account and the AX feature set for compliance.

The following table lists what AWS EC2 instance is used for different router throughput settings:

CSR Throughput	AWS EC2 Instance
10 MB	c4.large
50 MB	c4.large
100 BM	c4.large
250 MB	c4.large
500 MB	c4.large
1 GB	c4.2xlarge
2.5 GB	c4.4xlarge
5 GB	c4.8xlarge
10 GB	c4.8xlarge

Make sure that your AWS account has an allowed limit to deploy the instances. You can check your account instance limits in the AWS Management Console: **Services** > **EC2** > **Limits**.

Elastic IP Addresses

Make sure that you have at least nine elastic IP addresses in the region where the infra VPC is deployed.

You need one elastic IP address for Cisco Cloud APIC and four for each CSR. Make sure that your account in the region of deployment is allowed nine or more elastic IP addresses. If it is not, raise an AWS case to increase the number of elastic IP addresses. We recommend ten or more.

Note The addresses must not be disassociated elastic IP address. You need enough resources for nine new elastic IP addresses. If you have unused elastic IP addresses, you can release them.

Cisco Cloud APIC

The type of AWS instance used for the Cisco Cloud APIC deployment varies, depending on the release:

- For releases prior to Release 5.0(x), Cisco Cloud APIC is deployed using the M4.2xlarge instance.
- For Release 5.0(x) and later, Cisco Cloud APIC is deployed using the M5.2xlarge instance.

Make sure that your account has limits that are allowed to deploy this instance. You can check the limits in the AWS Management Console: **Services** > **EC2** > **Limits**.

You can also see how many elastic IP addresses that are used in the AWS Management Console: **Services** > **EC2** > **NETWORK & SECURITY** > **Elastic IPs**.

Cloud APIC Communication Ports

When configuring your Cloud APIC environment, keep in mind that the following ports are required for network communications:

- For communication between the ACI Multi-Site Orchestrator and the Cloud APIC: HTTPS (TCP Port 443 inbound/outbound)

  For the Cloud APIC, use the same Cloud APIC management IP address that you will use to log into the Cloud APIC at the beginning of Configuring Cisco Cloud APIC Using the Setup Wizard.

- For communication between the on-premises IPsec device and the CSRs deployed by Cloud APIC in AWS: Standard IPsec ports (UDP port 500 and permit IP protocol numbers 50 and 51 inbound/outbound)

  For the two Amazon Web Services CSRs, the public IPsec peering IP uses the elastic IP address of the third network interface, as described in Locating CSR and Tenant Information or as provided if you download the ISN device configuration files using the instructions in Configuring the Intersite Infrastructure.

- If you want to connect and manage the CSRs deployed by Cloud APIC in AWS, allow port TCP 22 inbound/outbound to the public IP address of each CSR.
- For license registration (towards `tools.cisco.com`): Port 443 (outbound) is required
- For DNS: UDP Port 53 outbound
- For NTP: UDP Port 123 outbound
- If remote authentication is used (LDAP, Radius, TACACS+, SAML), open the proper ports
- If a certificate authority is used, open the proper ports

Cisco Cloud APIC Installation Workflow

This section provides a high-level description of the tasks that are required to install and deploy Cisco Cloud APIC. You perform installation tasks through AWS Management Console, the AWS Cloud Formation template, the Cloud APIC Setup Wizard, and Cisco Application Centric Infrastructure (ACI) Multi-Site.

1. Fulfill all prerequisites, which include tasks in the on-premises data center and the public cloud.

   See the section "Requirements for Extending the Cisco ACI Fabric to the Public Cloud, on page 1."

2. Deploy Cisco Cloud APIC through the AWS Cloud Formation template.

   This task includes creating a stack, uploading a template (or providing an AWS template URL), configuring template parameters, and submitting the template. You then capture the Cisco Cloud APIC IP address.

   You also must create an Amazon EC2 SSH keypair and subscribe to Cisco Cloud APIC in the AWS Marketplace.

   See the section "Deploying the Cloud APIC in AWS."

3. Configure Cisco Cloud APIC using the Setup Wizard.

   This task includes logging into Cisco Cloud APIC and configuring the Cisco Cloud ACI fabric for connecting to the public cloud. You also add the AWS region selection. You provide the Border Gateway

Protocol (BGP) autonomous system number (ASN) and OSPF area ID for intersite network (ISN) peering and add an external subnet. You then add the IPsec peer address.

See the section "Configuring Cisco Cloud APIC Using the Setup Wizard."

4. Configure Cisco Cloud APIC using Cisco ACI Multi-Site.

   This task includes logging into the Cisco ACI Multi-Site GUI, adding the on-premises and cloud site, configuring the fabric connectivity infra, and configuring the properties for the on-premises site. You then configure the Cisco ACI spines, BGP peering, and enable the connectivity between the on-premises site and the AWS Cloud APIC sites.

   See the section "Managing Cisco Cloud APIC Through Cisco ACI Multi-Site."

5. Use Cisco Cloud APIC to extend Cisco ACI policy into the AWS public cloud.

   See the sections "Navigating the Cisco Cloud APIC GUI" and "Configuring Cisco Cloud APIC Components."