Preparing for Installing Cisco Cloud Network Controller

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.

Note Even though Cisco Nexus pre-EX leaf switches are supported, we recommend using later-generation leaf switches, such as EX or FX leaf switches, due to the End-of-Life announcement for these older pre-EX leaf switches as described in End-of-Sale and End-of-Life Announcement for the Cisco Nexus 9372PX and 9372TX Switches.

- At least one on-premises Cisco Application Policy Infrastructure Controller (APIC) running release 4.1 or later and Cisco Nexus Dashboard Orchestrator (NDO) Release 2.2(x) or later.

- Cisco Nexus Dashboard 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.
- Verify that all leaf switches on the on-premises sites have the appropriate Cisco ACI license:
  - 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

Note These licensing requirements for the on-premises data center are independent of the number of Cisco Cloud Network Controllers deployed on public clouds. For Cisco Cloud Network Controller licensing requirements, see Cisco Cloud Network Controller and On-Premises ACI Licensing Summary.

- 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 Network Controller, IPsec ports for each AWS CCR, and SSH connectivity for AWS CCR remote management.

  These firewall ports are described in more detail in Cisco Cloud Network Controller Communication Ports, on page 5 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.

Note You can run only one Cloud Network Controller in the infra account. Running multiple Cloud Network Controllers in the same infra account is not supported.

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 Network Controller 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.

CCR

There are two types of licensing models available:

- BYOL (Bring Your Own License)
- PAYG (Pay as You Go)

BYOL

Subscribe to the CCR Bring Your Own License (BYOL) through the AWS Marketplace. See Cisco Cloud Network Controller Licensing for more information.

Deploy the CCRs in the appropriate size, depending on the bandwidth requirement defined during the Cisco Cloud Network Controller setup.

The value for the throughput of the routers determines the size of the CCR instance that you deploy; a higher value for the throughput results in the deployment of a larger VM. CCR licensing is based on the throughput configuration that you set as part of the Cisco Cloud Network Controller setup process. You need the equivalent or higher license in your Smart account and the AX feature set for compliance.

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**.

The Cisco Catalyst 8000V supports tier-based (T0/T1/T2/T3) throughput options. The following table lists what AWS EC2 instance is used for different router throughput settings for the Cisco Catalyst 8000V:

CCR Throughput	AWS EC2 Instance
T0 (up to 15M throughput)	c5.xlarge
T1 (up to 100M throughput)	c5.xlarge
T2 (up to 1G throughput)	c5.xlarge
T3 (up to 10G throughput)	c5.9xlarge

Tier2 (T2) is the default throughput supported by Cisco Cloud Network Controller.

PAYG

Cisco Cloud Network Controller will support a range of AWS EC2 instances for cloud networking needs powered by Cisco's Catalyst 8000V virtual router. The table below shows the cloud instance type supported by Cisco Cloud Network Controller on AWS.

AWS EC2 Instance	CCR Throughput	vCPUs	Memory
c5.xlarge	up to 5 Gigabit throughput	4	8 GiB
c5.2xlarge	up to 10 Gigabit throughput	8	16 GiB
c5.4xlarge	up to 10 Gigabit throughput	16	32 GiB
c5.9xlarge	up to 10 Gigabit throughput	36	72 GiB
c5n.xlarge	up to 25 Gigabit throughput	4	10.5 GiB
c5n.2xlarge	up to 25Gigabit throughput	8	21 GiB
c5n.4xlarge	up to 25 Gigabit throughput	16	42 GiB
c5n.9xlarge	up to 50 Gigabit throughput	36	96 GiB

Changing the value in the **VM Type** field in the First Time Setup changes the other factors of the CCR as listed in the table above. Choosing a higher value for the VM size results in higher throughput.

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 Network Controller and four for each CCR. 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 Network Controller

Cisco Cloud Network Controller is deployed using the m5.2xlarge AWS 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**.

Cisco Cloud Network Controller Communication Ports

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

- For communication between the Cisco Nexus Dashboard Orchestrator and the Cisco Cloud Network Controller : HTTPS (TCP Port 443 inbound/outbound)

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

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

  For the two Amazon Web Services CCRs, the public IPsec peering IP uses the elastic IP address of the third network interface, as described in Locating CCR 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 CCRs deployed by Cisco Cloud Network Controller in AWS, allow port TCP 22 inbound/outbound to the public IP address of each CCR.
- 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 Network Controller Installation Workflow

This section provides a high-level description of the tasks that are required to install and deploy Cisco Cloud Network Controller. You perform installation tasks through AWS Management Console, the AWS Cloud Formation template, the Cisco Cloud Network Controller Setup Wizard, and Nexus Dashboard Orchestrator.

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 Network Controller 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 Network Controller IP address.

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

   See the section "Deploying the Cisco Cloud Network Controller in AWS."

3. Configure Cisco Cloud Network Controller using the Setup Wizard.

   This task includes logging into Cisco Cloud Network Controller and configuring the fabric managed by the Cisco Cloud Network Controller 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 Network Controller Using the Setup Wizard."

4. Configure Cisco Cloud Network Controller using Nexus Dashboard Orchestrator.

   This task includes logging into the Nexus Dashboard Orchestrator 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 Cisco Cloud Network Controller sites.

   See the section "Managing Cisco Cloud Network Controller Through Multi-Site."

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

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