Preparing for Installing Cisco Cloud APIC

- Requirements for Extending the Cisco ACI Fabric to the Public Cloud, on page 1
- Cloud APIC Communication Ports, on page 5
- Cisco Cloud APIC Installation Workflow, on page 6

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 Microsoft Azure 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 network device capable of terminating Internet Protocol Security (IPsec).
- Verify 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 Cloud APICs deployed on public clouds. For Cloud APIC licensing requirements, see Cisco Cloud APIC 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 Azure deployments. These include HTTPS access for the Cisco Cloud APIC, IPsec ports for each Azure CCR, and SSH connectivity for Azure CCR remote management.

  These firewall ports are described in more detail in Cloud APIC Communication Ports, on page 5 in this guide.

Requirements for the Azure Public Cloud

This section lists the Microsoft Azure requirements for extending the Cisco Application Centric Infrastructure (ACI) fabric to the public cloud.

Azure Accounts

You must have at least one Azure account. You will then create a subscription in your Azure account, where you can choose to deploy multiple tenants within the same subscription or you can create multiple subscriptions for the tenants.

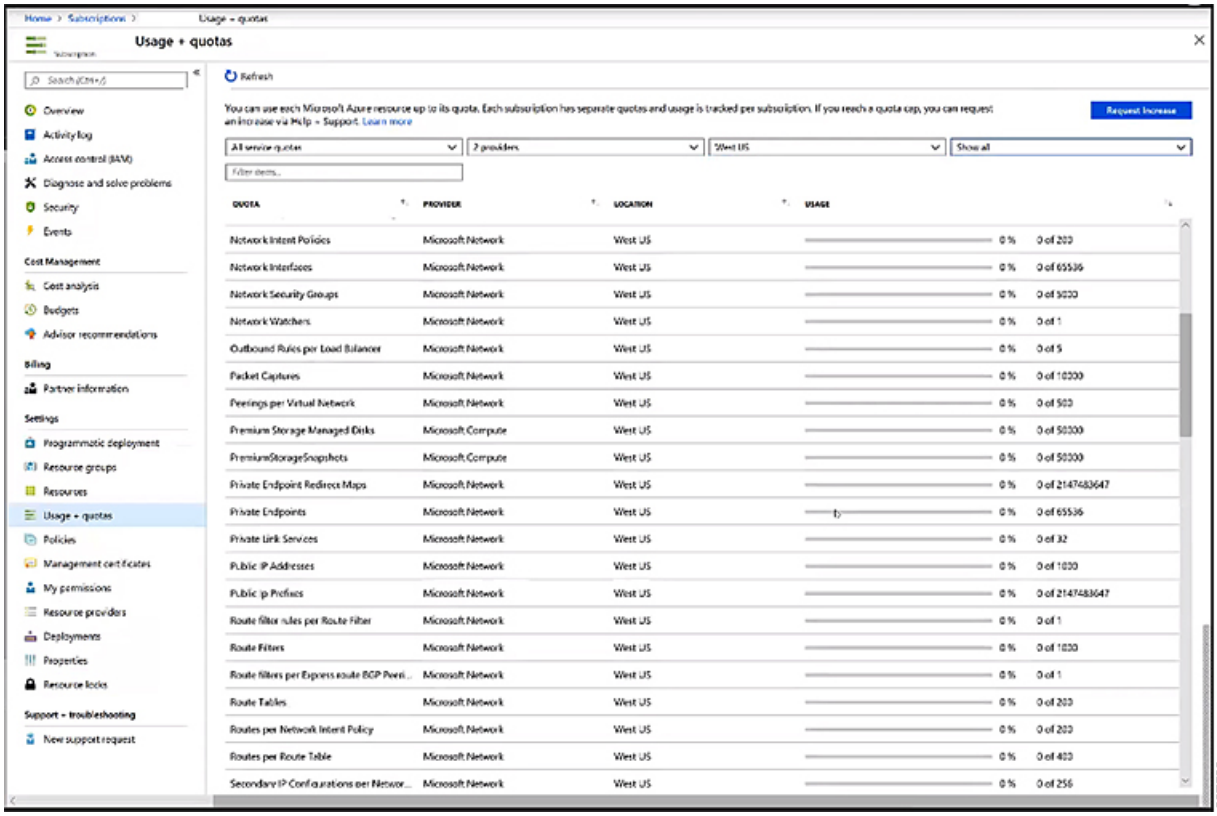
Azure Quota Limits

Verify that you have the appropriate Azure quota limits:

1. Navigate to **Subscriptions** > **Settings: Usage + quotas**.
2. In the **Select a provider** field, select:
   - Microsoft.Compute
   - Microsoft.Network

3. In the **Select a location** field, select your region (for example, **West US**).
4. In the last field, change **Show only items with usage** to **Show all**.

Output similar to the following appears. Use this output to verify that you have the appropriate Azure quota limits.



Azure Resources

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

- Access to the Azure Marketplace offer. Locate the Cisco Cloud APIC offer on the Azure Marketplace and follow the steps in that page:

  https://azuremarketplace.microsoft.com/en-us/marketplace/apps/cisco.cisco-aci-cloud-apic

- The following cloud resource requirements (assumes one tenant, one VRF):

Resource Name	Resource Type	Minimum Requirement
Virtual Networks	Network	2
Static Public IP Addresses	Network	9
Network Security Groups	Network	5
Application Security Groups	Network	5

Resource Name	Resource Type	Minimum Requirement
Application Gateways	Network	1
Virtual Machines	Compute	3
Standard DSv2 Family vCPUs	Compute	16
Standard DSv3 Family vCPUs	Compute	8
Premium Storage Managed Disks	Compute	4

Azure Resource Providers

For every subscription that you use with the Cloud APIC, including for tenants that have subscriptions that you might add later, you must register the following resource providers:

- `microsoft.insights`
- `Microsoft.EventHub`
- `Microsoft.Logic`
- `Microsoft.ServiceBus`

For more information, see Registering the Necessary Resource Providers.

CCR

Deploy the CCRs 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 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 APIC setup process. You need the equivalent or higher license in your Smart account and the AX feature set for compliance.

Cisco Cloud Services Router 1000v

The following table lists what Azure VM sizes are needed for different router throughput settings for the Cisco Cloud Services Router 1000v:

CSR Throughput	Azure VM Size	Premium Storage	Accelerated Networking
Up to 1 GB	DS3_v2	Yes	On
1 GB - 5 GB	DS4_v2	Yes	On

Beginning with Release 5.1(2), up to 40G throughput is supported by version 17.3 CSRs for the Cisco Cloud Services Router 1000v. The maximum throughput a CSR supports depends on the instance type. For achieving 40G throughput, a minimum of eight CSRs are required.

The following table lists the number of CSRs required and the instance type to achieve 40G throughput (per region):

Throughput per CSR	CSR Instance Type	Number of CSRs
5 Gbps	F16s_v2	8

Cisco Catalyst 8000V

The Cisco Catalyst 8000V supports tier-based (T0/T1/T2/T3) throughput options. The following table lists what Azure VM sizes are needed for different router throughput settings for the Cisco Catalyst 8000V:

CCR Throughput	Azure VM Size
T0 (up to 15M throughput)	DS3_v2
T1 (up to 100M throughput)	DS3_v2
T2 (up to 1G throughput)	DS3_v2
T3 (up to 10G throughput)	F16s_v2

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

Cisco Cloud APIC

Cisco Cloud APIC is deployed using Standard_D8s_v3.

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 Cisco Nexus Dashboard 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 CCRs deployed by Cloud APIC in Azure: Standard IPsec ports (UDP ports 500 and 4500 should be open)

  For the two Azure CCRs, the public IPsec peering IP 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 Cloud APIC in Azure, 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 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 Azure management portal, the Azure Resource Manager (ARM) 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 in Azure.

   This task includes subscribing to the CCR, registering the necessary resource providers, and creating an application in Azure.

   You also must create an Azure SSH keypair, deploy the Cisco Cloud APIC in Azure, and add a role assignment for a VM.

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

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 Azure 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 Multi-Site.

   - For on-premises-to-cloud connectivity, this task includes logging into the Cisco 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 Azure cloud sites.
   - For cloud-to-cloud connectivity, this task includes logging into the Cisco Nexus Dashboard Orchestrator GUI, adding the cloud sites, enabling the **Multi-Site** option and selecting the **Deploy Only** option when you are deploying the configuration.

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

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

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