Cisco Cloud APIC for Azure Installation Guide, Release 5.0(x)

First Published: 2020-05-15

Last Modified: 2020-07-02

Trademarks

CONTENTS

New and Changed Information

- New and Changed Information, on page 1

New and Changed Information

The following table provides an overview of the significant changes to the organization and features in this guide up to this current release. The table does not provide an exhaustive list of all changes made to the guide or of the new features up to this release.

Table 1: New Features and Changed Behavior in Cisco Cloud APIC Release 5.0(2)

Feature or Change	Description	Where Documented
Custom naming rules for cloud resources	You can create a global naming policy on the Cloud APIC, which allows you to define a custom cloud resources naming convention for all objects deployed from the Cloud APIC into the Azure cloud.	Cloud Resources Naming, on page 41

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.

Beginning in Cisco Application Policy Infrastructure Controller (APIC) Release 4.1(1), Cisco ACI can use Cisco Cloud APIC to extend a Cisco ACI Multi-Site fabric to Amazon Web Services (AWS) public clouds.

Beginning in APIC Release 4.2(1), Cisco ACI can also use Cisco Cloud APIC to extend a Cisco ACI Multi-Site fabric to Microsoft Azure public clouds.

What Cisco Cloud APIC Is

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

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

Starting with Release 4.2(3), Cisco Cloud APIC 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 APIC 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 Cisco Application Centric Infrastructure (ACI) Multi-Site fabric to the Microsoft Azure public cloud.

The following illustration shows the architecture of Cisco Cloud APIC.

Figure 1: Cisco Cloud APIC Architecture
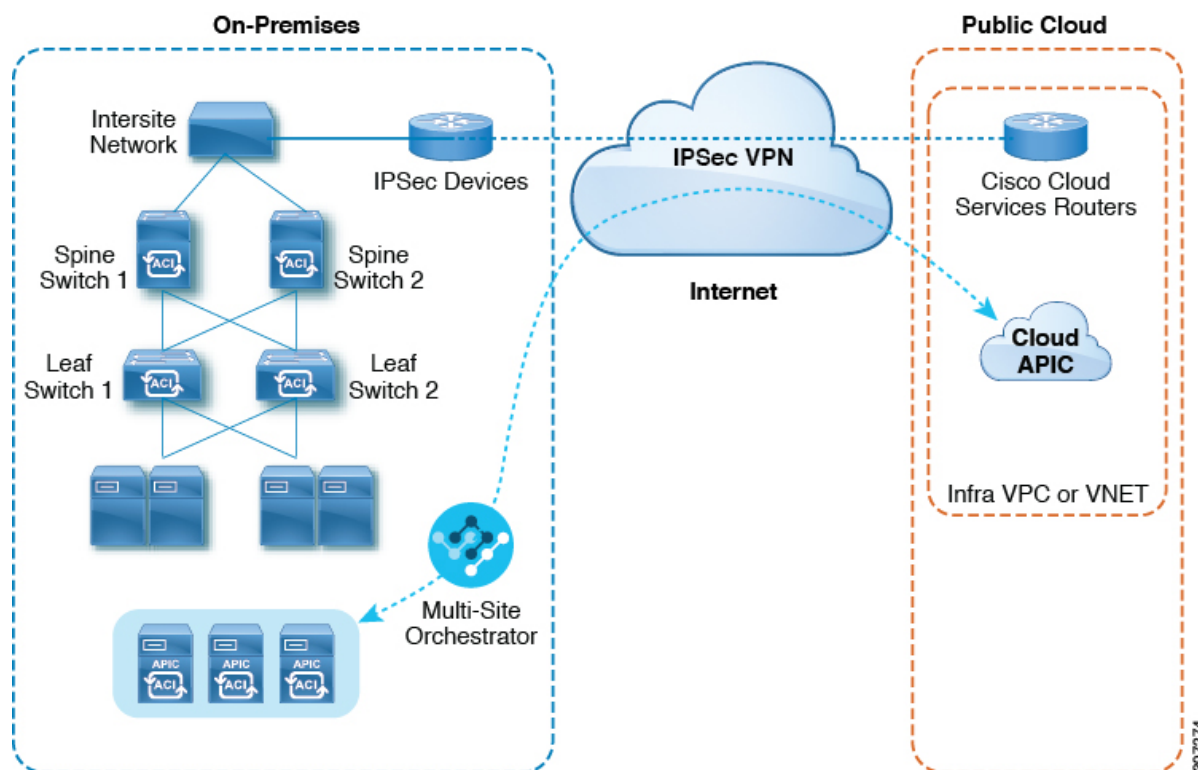
On-Premises Data Center Components

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.

Cisco ACI Multi-Site and Cisco ACI Multi-Site Orchestrator

Cisco ACI 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 Cisco ACI Multi-Site installed to use Cisco Cloud APIC to extend the fabric into the public cloud.

For more information, see the Cisco ACI Multi-Site documentation on Cisco.com and the configuration information for Cisco ACI Multi-Site in this guide.

Cisco ACI Multi-Site Orchestrator (MSO) 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 ACI Multi-Site Orchestrator creates connectivity between the on-premises data center and the public cloud. Use Cisco ACI 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 *Cisco ACI Multi-Site Configuration Guide* on Cisco.com.

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

Cisco Cloud APIC performs the following actions:

- Defines a site on the public cloud, provisions the cloud infra virtual networks (VNETs) and manages the Cisco Cloud Services Router (CSR) across all regions.

- Renders the Cisco ACI policy model in the public cloud, and manages cloud health.

For more information, see *Cisco Cloud APIC Release Notes*.

Cisco Cloud Services Router

The Cisco Cloud Services Router 1000V (CSR 1000V) is a virtual router that delivers comprehensive WAN gateway and network services into virtual and cloud environments. The CSR 1000V enables enterprises to extend their WANs into provider-hosted clouds. Two CSR 1000Vs are required for Cisco Cloud ACI solution.

For more information, see the Cisco CSR 1000v 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 Multi-Site Orchestrator in the on-premises data center and Cisco Cloud APIC in the Microsoft Azure public cloud.

Changes in APIC Release 4.2(1)

As part of the initial release of the Cisco Cloud APIC in APIC Release 4.1(1), support was provided for the initial release of on-premises-to-cloud connectivity, or Hybrid-Cloud, where you could use the Cisco ACI Multi-Site Orchestrator to extend an on-premises Cisco ACI site to Amazon AWS public clouds.
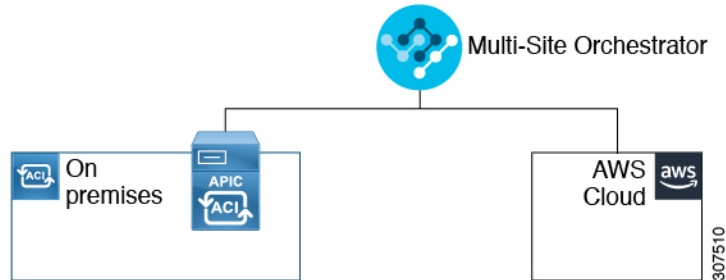
Beginning in APIC Release 4.2(1), you can now use the Cisco ACI Multi-Site Orchestrator to extend an on-premises Cisco ACI site to Microsoft Azure public clouds.
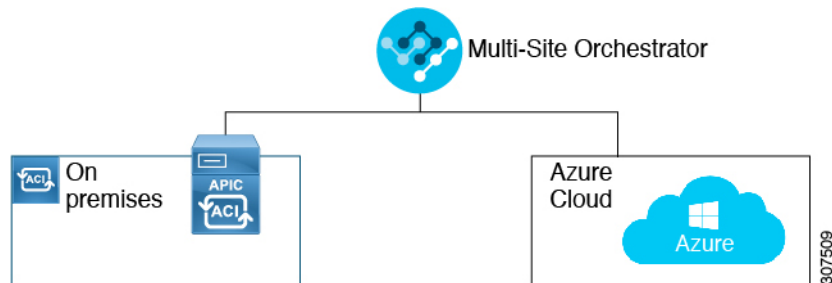
With the expanded functionality available in this release, you can also use the Cisco ACI Multi-Site Orchestrator to establish connectivity between the following components:

- On-premises-to-cloud connectivity:

    - Connectivity for these public cloud sites:

        - On-premises Cisco ACI and Amazon AWS public cloud sites (available previously in APIC Release 4.1[1])

        - On-premises Cisco ACI and Microsoft Azure public cloud sites

    - On-premises-to-single cloud site connectivity (Hybrid-Cloud)

    - On-premises-to-multiple cloud sites connectivity (Hybrid Multi-Cloud)
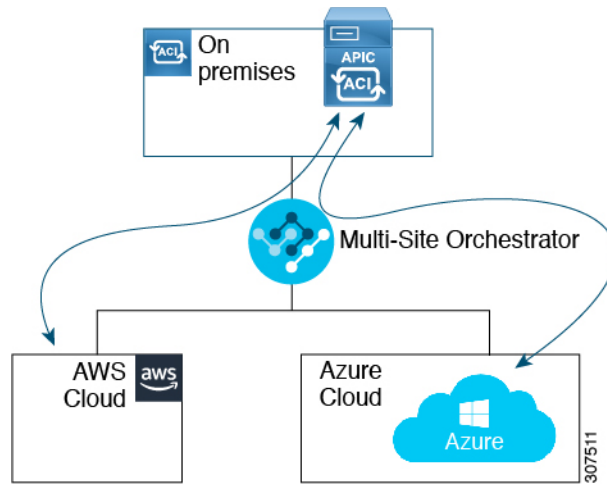
- Cloud site-to-cloud site connectivity (Multi-Cloud):

  - Between Amazon AWS public cloud sites and Microsoft Azure public cloud sites

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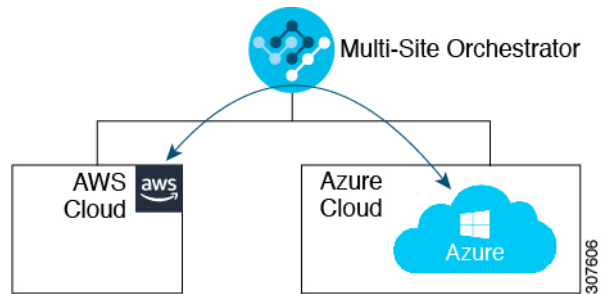
In addition, support is also available for the single-cloud configuration (Cloud First).

Policy Terminology

A key feature of Cisco Cloud APIC 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

Cisco ACI	Azure
BD subnet	Subnet
Contract, filter	Outbound rule, inbound rule
EP-to-EPG mapping	Application Security Group (ASG), Network Security Group (NSG)
Endpoint	Network adapter on VM instances

About Tenants

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.

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.

As part of the Cloud APIC configuration, you will configure tenants in two areas:

Configuring Cloud APIC Tenant Accounts

When configuring a tenant in Cloud APIC, you will choose from one of these options:

- **Create Your Own Managed Identity:** You will choose this option when the Azure subscriptions are in the same directory (of the same organization).

- **Create Your Own Unmanaged Identity:** You will choose this option 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.

- **Shared:** 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.

You will be making these configurations in the Cloud APIC GUI using the procedures in Configuring a Tenant, on page 62.

Configuring Azure Tenant Accounts

Once you have decided on the type of tenant that you will be configuring in the Cloud APIC, you will then have to make the necessary subscription configurations in the Azure portal to allow for that type of Cloud APIC tenant. You will be making the necessary subscription configurations in the Azure portal before you configure the tenant in your Cloud APIC.

- If you will be configuring tenants in the Cloud APIC using **managed identity**, then, in the Azure portal, you will be adding a role assignment for a **virtual machine**. You can 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, on page 32.

- If you will be configuring tenants in the Cloud APIC using **unmanaged identity**, then, 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 for an App, on page 34.

- If you will be configuring tenants in the Cloud APIC using the **shared** option, 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.

Cisco Cloud APIC Licensing

This section lists the licensing requirements to use Cisco Cloud Application Policy Infrastructure Controller (APIC).

Cisco Cloud APIC and Cisco Cloud Services Router

Cisco licenses Cisco Cloud APIC by each virtual machine (VM) instance that it manages. The Cisco Cloud APIC binary images are available on Microsoft Azure portal and support the Bring Your Own License (BYOL) model.

The Essential Cloud tier includes licenses for a single policy domain or a single instance of Cisco Cloud APIC on a public cloud. If you deploy multiple instances of Cisco Cloud APIC, buy an Advantage Cloud license for each VM instance that Cisco Cloud APIC manages.

For licensing details, see the *Cisco Application Centric Infrastructure Ordering Guide*.

In addition to obtaining one or more Cisco Cloud APIC licenses, you must register your Cisco Cloud APIC and Cisco Cloud Services Router (CSR) with Cisco Smart Software Licensing.

Cisco Smart Licensing is a unified license management system that manages software licenses across Cisco products. To learn more about Smart Software Licensing, visit https://www.cisco.com/go/smartlicensing.

Complete the following steps to register Cisco Cloud APIC and CSR:

1. Ensure that this product has access to the internet or a Smart Software Manager satellite that is installed on your network.

2. Log in to Smart Account:

   a. Smart Software Manager: https://software.cisco.com/

   b. Smart Software Manager Satellite:
   https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html

3. Navigate to the Virtual Account containing the licenses to be used by this Product Instance.

4. Generate a Product Instance Registration Token (this identifies your Smart Account) and copy or save it.

Note Cisco Cloud APIC deploys the appropriate size of CSRs based on the setting chosen in the **Throughput of the routers** field in the Cisco Cloud APIC setup wizard.

Note If you remove a CSR from deployment at some point in the future (by deleting the CSR through the Cisco Cloud APIC GUI or through the cloud console or portal), this results in the CSR smart license server getting severed from that CSR. The CSR instance that got deleted will get marked as stale for 90 days and the license cannot be reused by any other new CSRs for that period of time.

To avoid this situation, rehost the new CSR to the old license by following the procedures provided here:

Rehosting the Cisco CSR 1000v License

On-Premises Cisco ACI Licenses

If you have a single on-premises Cisco ACI site with one or more cloud sites, you can run your on-premises Cisco ACI fabric in either the Essential, Advantage, or Premier license tier.

Microsoft Azure

You must subscribe to the Cisco Cloud Services Router (CSR) 1000V - Bring Your Own License (BYOL) for Maximum Performance. To subscribe through the Microsoft Azure Marketplace, follow the instructions in Subscribing to the Cisco Cloud Services Router 1000V, on page 19.

Cisco Cloud APIC-Related Documentation

You can find information about Cisco Cloud Application Policy Infrastructure Controller (APIC), Cisco ACI Multi-Site, and Microsoft Azure from different resources.

Cisco Documentation

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

   • *Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release 4.2(1)*

   Includes list of other Cisco Cloud APIC documents.

- Cisco ACI and Cisco APIC documentation

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

- Cisco ACI Multi-Site documentation

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

- Cisco Cloud Services 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.

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 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.

  - At least one on-premises 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, Release 4.0(1)*.

- 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 CSR, and SSH connectivity for Azure CSR remote management.

  These firewall ports are described in more detail in Cloud APIC Communication Ports, on page 16 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.
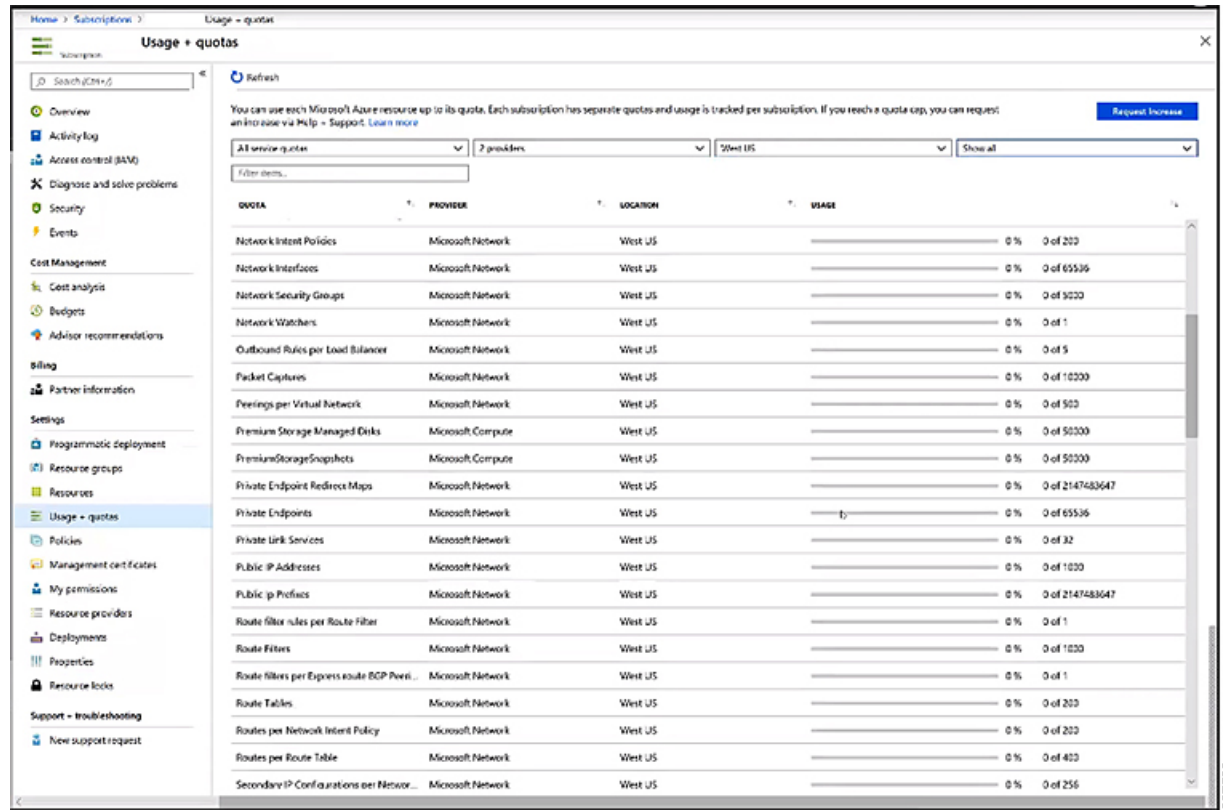
Azure Resources

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
Application Gateways	Network	1
Virtual Machines	Compute	3
Standard DSv2 Family vCPUs	Compute	16
Standard DSv3 Family vCPUs	Compute	8

Resource Name	Resource Type	Minimum Requirement
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 .

Cisco Cloud Services Router (CSR)

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 Azure VM sizes are needed for different router throughput settings:

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

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 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 .

- For communication between the on-premises IPsec device and the CSRs deployed by Cloud APIC in Azure: Standard IPsec ports (UDP ports 500 and 4500 should be open)

For the two Azure CSRs, the public IPsec peering IP as provided if you download the ISN device configuration files using the instructions in Configuring the Intersite Infrastructure, on page 56.

- If you want to connect and manage the CSRs deployed by Cloud APIC in Azure, 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 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 13."

2. Deploy Cisco Cloud APIC in Azure.

   This task includes subscribing to the Cisco Cloud Services Router 1000V, 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, on page 19."

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, on page 39."

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

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

   See the section "Managing Cisco Cloud APIC Through Cisco ACI Multi-Site, on page 55."

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

   See the sections "Navigating the Cisco Cloud APIC GUI, on page 73" and "Configuring Cisco Cloud APIC Components, on page 73."

C H A P T E R 4

Deploying the Cloud APIC in Azure

Subscribing to the Cisco Cloud Services Router 1000V

You must subscribe to the Cisco Cloud Services Router (CSR) 1000V - Bring Your Own License (BYOL) for Maximum Performance. To subscribe through the Microsoft Azure Marketplace:

Step 1   In the Azure Marketplace search text field, type *Cisco Cloud Services Router (CSR) 1000V* and select the option that appears.

The **Cisco Cloud Services Router (CSR) 1000V** option appears as a search suggestion.

Step 2   Click the **Cisco Cloud Services Router (CSR) 1000V** option.

You should be redirected to the **Cisco Cloud Services Router (CSR) 1000V** page in the Microsoft Azure Marketplace.

Step 3   Locate the **Select a software plan** drop-down menu.

If you do not see the **Select a software plan** drop-down menu in the main page, you might have to click the **Plans + Pricing** tab, if that option is available, to access the **Select a software plan** drop-down menu.

Step 4   In the **Select a software plan** drop-down menu, locate the area that lists the **Cisco CSR 1000V Bring Your Own License** options.

Cisco CSR1000V- AX Pkg. Max Performance- XE 17.2.1

Cisco CSR1000V-AX Pkg. Max Performance-XE 16.12.4a

Cisco CSR1000V-AX Pkg. Max Performance-XE 17.3.2

Cisco CSR 1000V Bring Your Own License - XE 16.9

Cisco CSR 1000V Bring Your Own License - XE 16.7

Cisco CSR 1000V Bring Your Own License - XE 16.10

Cisco CSR 1000V Bring Your Own License - XE 16.12

Cisco CSR 1000V Bring Your Own License - XE 17.1

Cisco CSR 1000V Bring Your Own License - XE 17.2.1

Cisco CSR 1000V Bring Your Own License -XE 17.3.1a

Cisco CSR 1000V Bring Your Own License-XE 16.12.4a

Cisco CSR 1000V Bring Your Own License -XE 17.3.2

Step 5   Select the appropriate option, depending on the Cisco Cloud APIC software release:

For Cloud APIC Release	Select this specific option
Release 4.2x	Cisco CSR 1000V Bring Your Own License - XE **16.12**
Release 5.0(1)	Cisco CSR 1000V Bring Your Own License - XE **16.12**
Release 5.0(2)	Cisco CSR 1000V Bring Your Own License - XE **17.1**
Release 5.1(2)	Cisco CSR 1000V Bring Your Own License - XE **17.3.1(a)**

Step 6   Locate the **Want to deploy programmability?** field and click **Get Started**.

Step 7   In the **Configure Programmability Deployment** page, scroll down to your subscription and, in the Status column, change the status from **Disable** to **Enable** for your subscription.

Step 8   Click **Save**.

What to do next

Go to .

Registering the Necessary 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`

These procedures describe how to register these necessary resource providers for a subscription.

Step 1   Access the area in Azure where you can view the resource providers:

a) From the main Azure management portal page, click the **All services** link in the left nav bar, then click the **Subscriptions** link.
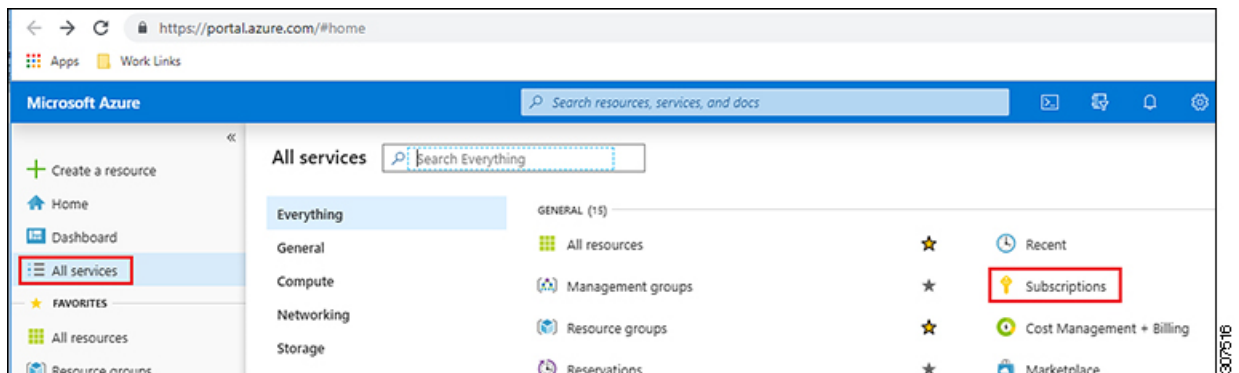
b) In the **Subscriptions** page in the Azure management portal, click the subscription account for your Microsoft account.

The overview information for that subscription is displayed.

c) From the overview page for that subscription, locate the **Resource providers** link in the left nav bar and click that link.

The Resource Providers page for that subscription is displayed.
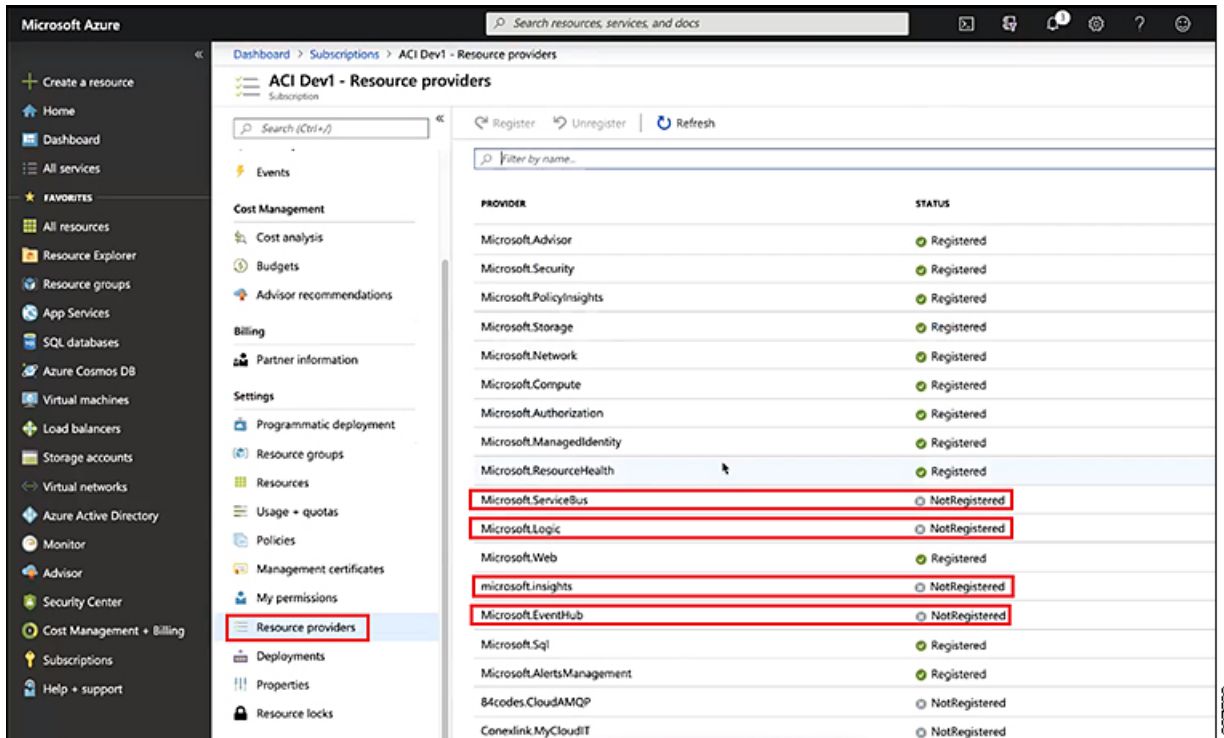
Step 2   Locate the following four resource providers in the list of providers, as shown in the preceding screenshot:

- microsoft.insights

- Microsoft.EventHub

- Microsoft.Logic

- Microsoft.ServiceBus

Step 3   Determine if all four of the resource providers are in the `Registered` or `NotRegistered` state.

- If all four of the resource providers are shown as `Registered` in the Status column, then you do not have to do anything further to register these resource providers for this subscription.

- For every resource provider that is shown as `NotRegistered` in the Status column:

  a.   Click on that specific resource provider that is shown as `NotRegistered`.

  b.   Click on Register at the top of the screen to register that resource provider.
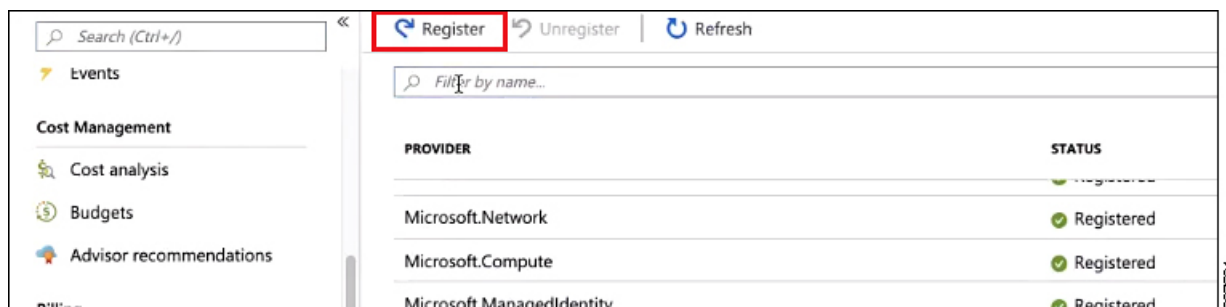
The Status will change from `NotRegistered` to `Registering`, then to `Registered` when the registration process is completed.

   c. Repeat these steps for every resource provider that is shown as `NotRegistered` until all four resource providers are shown as `Registered`.

Creating an Application in Azure

Follow these instructions to create an application in Azure, if necessary. You will need these procedures if you are creating a new subscription for the tenant and you are selecting **Unmanaged Identity** to manage the cloud resources through a specific application.

Note An application in Azure is also referred to as a Service Principal.

Step 1 Log into your Azure account for the Cloud APIC infra tenant and go to the Azure management portal, if you are not there already:

https://portal.azure.com/#home

Step 2 From the main Azure management portal page, click the **Azure Active Directory** link in the left nav bar, then click the **App registrations** link.

Step 3 In the **App registrations** page, click + **New registration**.

Step 4 Enter the necessary information in the **Register an application** page:

- **Name**

- **Supported Account Types**: Select the first option (Accounts in this organizational directory only)

- (Optional) **Redirect URI**

Then click **Register**.

The overview page for this application appears.

Step 5 Click **Certificates & secrets** in the left nav bar, then enter the necessary information in the **Add a client secret** area and click **Add**.

This generates the necessary information that you will need for the **Application Secret** field later on in these procedures.

Step 6 Open a text file and copy-and-paste the necessary information into the text file:

- **Client Secret**: Copy the text in the **Value** field in the **Client Secrets** area in the **Clients & Secrets** page.

- **Application ID**: Navigate to **Home** > **App registrations** > **<application-name>**, then, in the **Overview** page, copy the text from **Application (client) ID** field.

- **Azure Active Directory ID**: Navigate to **Home** > **App registrations** > **<application-name>**, then, in the **Overview** page, copy the text from **Directory (tenant) ID** field.

Step 7   Save the text file and note its location.

You will refer to this information when you are going through the procedures in Configuring a Tenant, on page 62 later on in this document.

Generating an SSH Key Pair for Azure

As part of the Cloud APIC setup process, you will be asked to provide the Admin Public Key (the SSH public key) in the Azure Resource Manager (ARM) template for your Cloud APIC. The following sections provide instructions for generating the SSH public and private key pair in Windows or Linux systems.

Generating an SSH Key Pair in Windows

These procedures describe how to generate an SSH public and private key pair in Windows. For instructions on generate an SSH public and private key pair in Linux, see Generating an SSH Key Pair in Linux or MacOS, on page 26.

Step 1   Download and install the PuTTY Key Generator (puttygen):

https://www.puttygen.com/download-putty

Step 2   Run the PuTTY Key Generator by navigating to **Windows** > **Start Menu** > **All Programs** > **PuTTY** > **PuTTYgen**.

You will see a window for the PuTTY Key Generator on your screen.
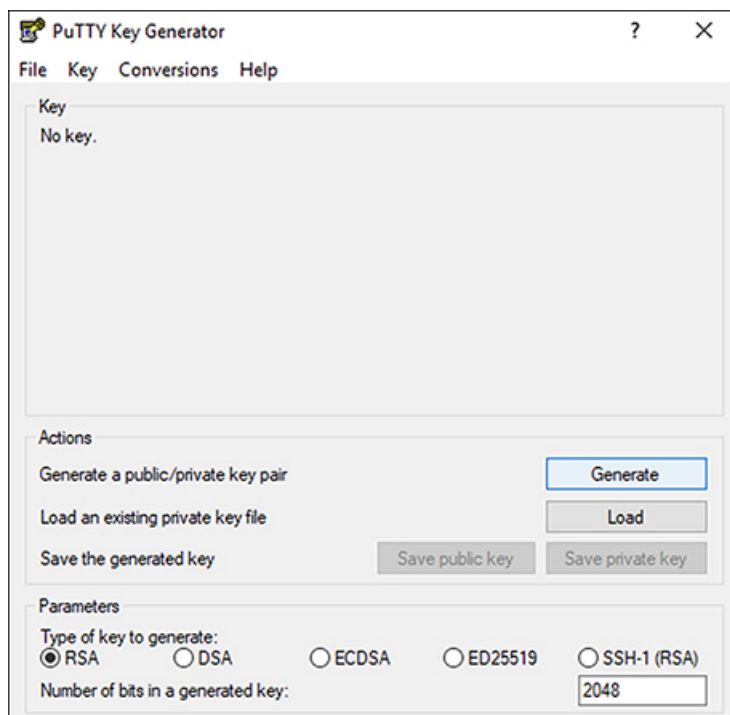
Step 3   Click **Generate**.

A screen appears, asking you to move the mouse over the blank area to generate a public key.

Step 4   Move your cursor around the blank area to generate random characters for a public key.
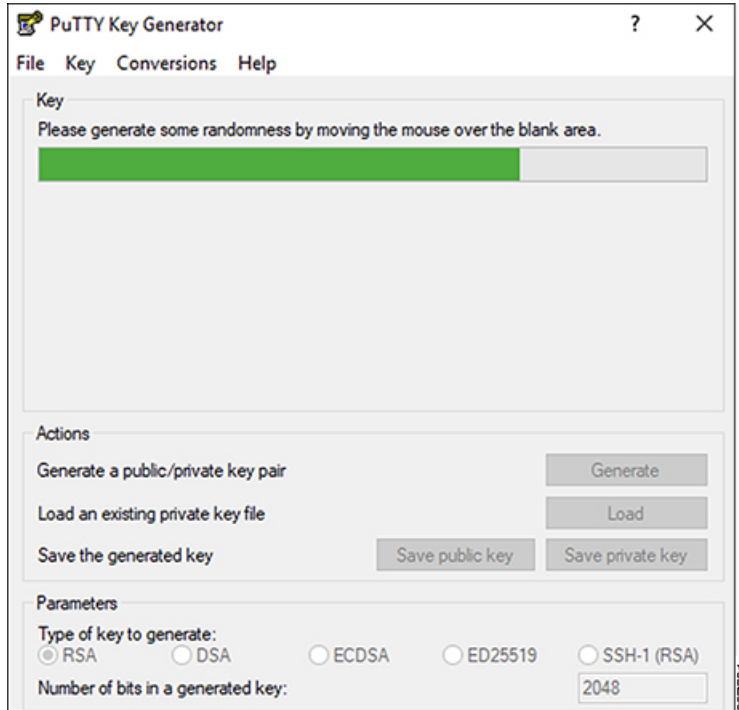
Step 5   Save the public key.

a) Navigate to a folder on your laptop where you want to save the public key file and create a text file for this public key.

b) Copy the information in the PuTTY Key Generator.

Copy the public key information in the window, with these inclusions and exclusions:

- Including the **ssh-rsa** text at the beginning of the public key.

- Excluding the following text string at the end:

    `== rsa-key-<date-stamp>`

Truncate the key so that it does not include the **== rsa-key-<date-stamp>** text string at the end.

Note   In the next set of procedures, you will paste the public key information into the Azure ARM template. If the form does not accept the key in this format, add == back to the end of the key, as this format is required in some regions.

If the key is not in the correct format, the Cloud APIC will not complete its installation.
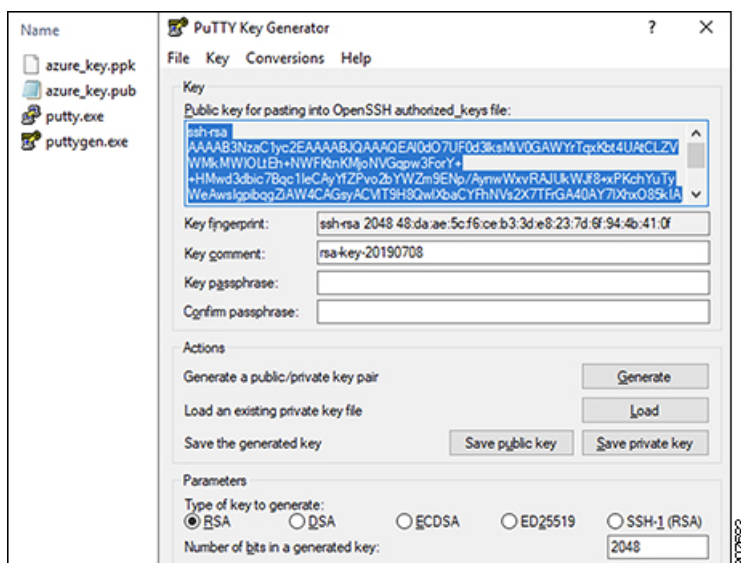
c) Paste the information in the public key text file that you created in 5.a, on page 25 and save the file, giving it a unique file name.

This public key text file will now contain a key that is on a single line of text. You will need the information in this public key text file in the next set of procedures.

Note Do not save the public key using the **Save public key** option in the PuTTY Key Generator. Doing so saves the key in a format that has multiple lines of text, which is not compatible with the Cloud APIC deployment process.

Step 6 Save the private key.

a) Click **Save private key**.

A screen appears, asking if you want to save the file without a passphrase. Click **Yes** on this screen.

b) Navigate to a folder on your laptop and save the private key file, giving it a unique file name.

Note The private key file is not used in the installation process. However, you might need it for other reasons, such as logging into your Cloud APIC through SSH, as described in Logging Into Cloud APIC Through SSH, on page 97.

What to do next

Follow the instructions in Deploying the Cloud APIC in Azure, on page 28 to continue the Azure configuration process, which includes pasting the public key information into the Azure ARM template.

Generating an SSH Key Pair in Linux or MacOS

These procedures describe how to generate an SSH public and private key pair in Linux or MacOS. For instructions on generate an SSH public and private key pair in Windows, see Generating an SSH Key Pair in Windows, on page 24.

Step 1 On your Linux virtual machine or Mac, create a public and private key pair using ssh-keygen, directing the output to a file.

ssh-keygen -f *filename*

For example:

ssh-keygen -f azure_key

Output similar to the following appears. Press the Enter key without entering any text when you are asked to enter a passphrase (leave the field empty so that there is no passphrase).

```
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in azure_key.
Your public key has been saved in azure_key.pub.
The key fingerprint is:
SHA256:gTsQIIAadjgNsgcguifIloh4XGpVWMdcXVV6U0dyBNs
...
```

Step 2 Locate the public and private key files that you saved.

ls

Two files should be displayed, where:

- The file with the .pub suffix contains the public key information

- The file with the same name, but with no suffix, contains the private key information

For example, if you directed the output to a file named azure_key, you should see the following output:

```
# ls
azure_key
azure_key.pub
```

In this case:

- The azure_key.pub file contains the public key information

- The azure_key file contains the private key information

Step 3 Open the public key file and copy the public key information from that file, without the username@hostname information at the end.

Note The private key file is not used in the installation process. However, you might need it for other reasons, such as logging into your Cloud APIC through SSH, as described in Logging Into Cloud APIC Through SSH, on page 97.

What to do next

Follow the instructions in Deploying the Cloud APIC in Azure, on page 28 to continue the Azure configuration process, which includes pasting the public key information from the public key file into the Azure ARM template.

Deploying the Cloud APIC in Azure

Before you begin

- Verify that you have met the requirements outlined in Requirements for Extending the Cisco ACI Fabric to the Public Cloud, on page 13 before proceeding with the tasks in this section. For example, verify that you have the correct number of elastic IP addresses and that you have checked the limits that are allowed to deploy the instances.

Step 1   Log into your Azure account for the Cloud APIC infra tenant and go to the Azure management portal, if you are not there already:

https://portal.azure.com/#home

Step 2   From the main Azure management portal page, in the search text field, type *Cisco Cloud APIC*.

Step 3   In the **Cisco Cloud APIC** page, click **Create**.

The **Basics** page for the **Cisco Cloud APIC** screen appears.

Step 4   Complete the necessary fields in the **Basics** page:

- **Subscription**: Select the Cloud APIC infra subscription account from the drop-down list.

- **Resource group**: Choose an existing resource group from the drop-down list or click **Create new** to enter a name for a new resource group.

  A resource group is a container that holds related resources for an Azure solution.

  Starting with Release 5.0(2), you can define custom naming rules for most cloud resources created by the Cloud APIC, with the exception of the resource group for the Cloud APIC itself. Ensure that the resource group name you select here is correct.

- **Region**: Select the location from the drop-down list where you want to deploy the virtual machine for the Cloud APIC.

- **Virtual Machine name**: Enter a virtual machine name. This entry will be the name for the virtual machine for this Cloud APIC. The virtual machine name must be only alphanumeric characters, but can be separated by dashes (for example, `CloudAPIC`).

- **Password**: Enter an admin password. This entry is the password that you will use to log into the Cloud APIC after you have enabled SSH access.

  The password must have the following characteristics:

  - Must be between 12 and 72 characters in length

  - Must have three of the following:

    - 1 lower case letter

    - 1 upper case letter

    - 1 number

    - 1 of the following acceptable special characters:

@$!%*#?&

- **Confirm Password**: Enter the admin password again.

- **SSH Public Key**: Paste the public key information that you copied at the end of one of these procedures:

You will use this SSH key pair to log into the Cloud APIC. Note that the **ssh-rsa** string should remain at the beginning of the public key string that you paste into this field.

Note   If you generated an SSH key pair in Windows, the key in the PuTTY Key Generator ends with == **rsa-key-<date-stamp>**. Truncate the key so that it does not include == **rsa-key-<date-stamp>**. If the form does not accept the key in this format, add == back to the end of the key, as this format is required in some regions.

If the key is not in the correct format, the Cloud APIC will not complete its installation.

Step 5   When you have finished completing the fields in this page, click **Next: ACI Settings**.

The **ACI Settings** page for the **Cisco Cloud APIC** screen appears.

Step 6   Complete the necessary fields in the **ACI Settings** page:

- **ACI Fabric Name**: Leave the default value as-is or enter a fabric name. This entry will be the name for this Cloud APIC. The fabric name must be only alphanumeric characters, but can be separated by dashes (for example, `ACI-Cloud-Fabric`).

- **Virtual machine size**: The virtual machine size is automatically set to the default deployment size of Standard_D8s_v3. You cannot change the default virtual machine size setting.

- **Image Version**: Choose **5.0(2)** in this field.

- **Infra Subnet**: The infra pool for your Cloud APIC. This field is automatically populated with a default value of 10.10.0.0/24. Change the value in this field if the default value overlaps with your infra pool from your on-premises fabric. This entry must be a /24 subnet.

- **External Subnets**: Enter the IP addresses and subnets of the external networks that you will allow to connect to Cloud APIC (for example, 192.0.2.0/24). Only the IP addresses from this subnet are allowed to connect to Cloud APIC. Entering a value of `0.0.0.0/0` means that anyone is allowed to connect to Cloud APIC.

- **Public IP Address**: Set the public IP address to **static**.

  a. In the **Public IP Address** field, click **Create New**.

      The **Create public IP address** field appears on the right side of the page.

  b. In the **SKU** area, choose either the **Basic** or the **Standard** SKU.

      For more information on the differences between the Basic and the Standard SKU, see the *Public IP Addresses in Azure* document in the Microsoft documentation site.

  c. In the **Assignment** area, choose **Static**.

      Do not leave the setting as Dynamic in the **Assignment** area.

    d. Click **OK** in the **Create public IP address** area.

- **DNS Prefix for the public IP Address**: The Cloud APIC DNS name prefix. When the Cloud APIC is deployed, you can access the Cloud APIC using the DNS name.

    Note   Due to an Azure restriction, you cannot use periods (.) in the Cloud APIC DNS name prefix that you enter in this field.

- **Virtual Network Name**: Leave the default entry for the virtual network name as-is or change the entry in this field, if desired.

- **Management Nsg Name**: Leave the default entry for the management network security group name as-is or change the entry in this field, if desired.

- **Management Asg Name**: Leave the default entry for the management application security group name as-is or change the entry in this field, if desired.

- **Subnet Prefix**: Leave the default entry for the subnet prefix as-is or change the entry in this field, if desired.

Step 7   When you have finished completing the fields in this page, click **Next: Review + create**.

    The **Review + create** page for the **Cisco Cloud APIC** screen appears.

Step 8   Review the information in the **Review + create** page, then click **Create**.

    The system now uses the information that you provided in the template to create the Cloud APIC VM instance. This process takes 5-10 minutes to complete. Click the Notifications icon (the bell-shaped icon) to check the status of the deployment of your Cloud APIC.
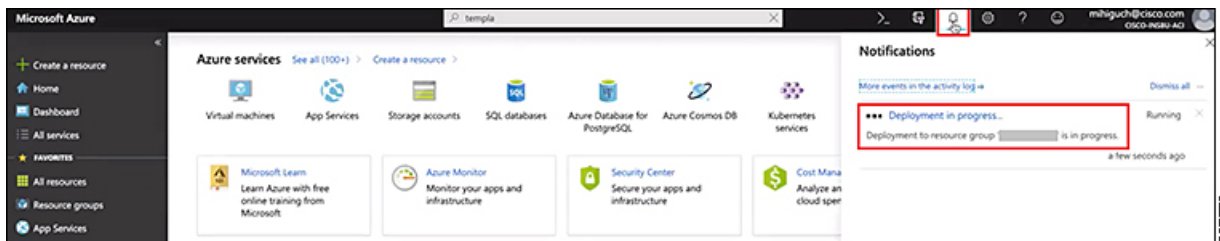
Step 9   When the deployment is complete, add a **User Access Administrator** role assignment.

    a) From the main Azure management portal page, click the **All services** link in the left nav bar, then click the **Subscriptions** link.
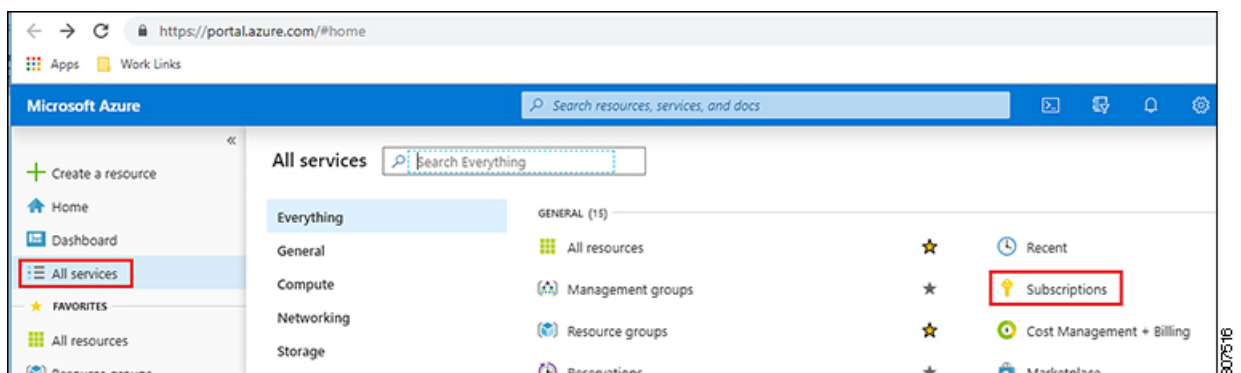
b) In the **Subscriptions** page in the Azure management portal, click the subscription account to which Cloud APIC was deployed.

The overview information for that subscription is displayed.

c) From the overview page for that subscription, locate the **Access control (IAM)** link in the left nav bar and click that link.

The Access Control page for that subscription is displayed.

d) Click + **Add**, then select **Add role assignment** from the drop-down menu.
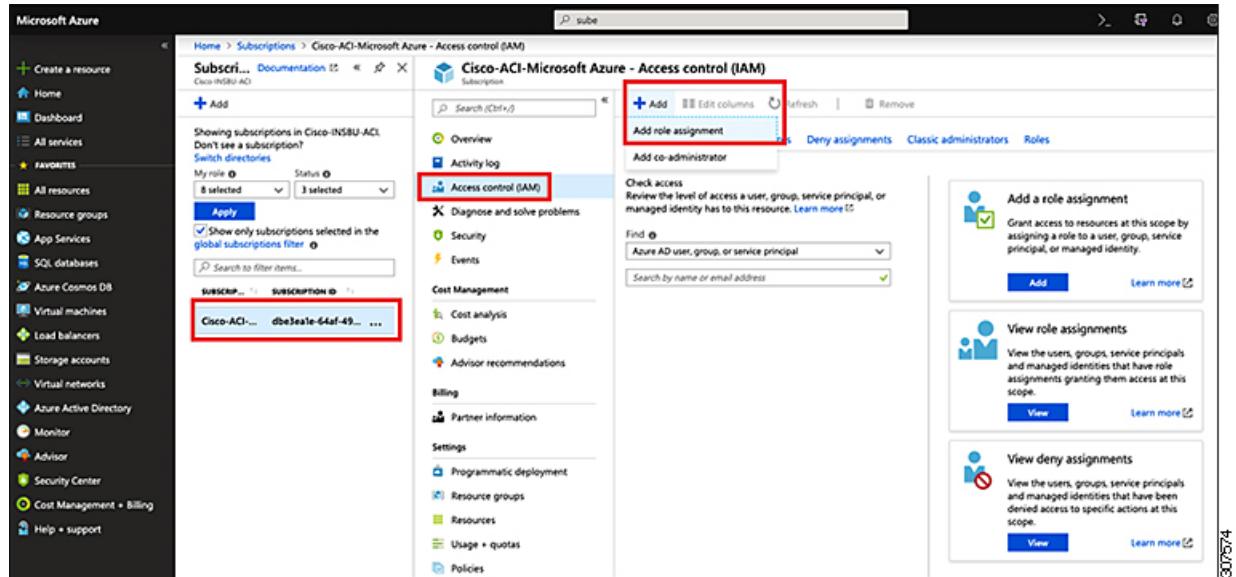
e) In the **Add role assignment** page, make the following selections:

   • In the **Role** field, select **User Access Administrator** from the drop-down menu.

   • In the **Assign access to** field, select **Virtual Machine**.

   • In the **Subscription** field, select the subscription where the Cloud APIC is deployed.

   • Select the Cloud APIC virtual machine.

f) Click **Save** at the bottom of the screen.

What to do next

Go to to determine if you need to add a role assignment for a managed identity or unmanaged identity for the access type.

Adding a Role Assignment

The type of role assignment that you add depends on whether you have a managed identity or unmanaged identity for the access type:

- If you have a **managed** identity for the access type, then you must add a role assignment for the user tenant. Go to Adding a Role Assignment for a Virtual Machine, on page 32.

  Note that this access type would apply if you make either of the following selections when you are entering information in the **Associate Account** page in the Configuring a Tenant, on page 62 procedures later in this manual:

  - You choose **Mode: Create Own** and you selected **Managed Identity** in the **Associate Account** page, or

  - You choose **Mode: Select Shared** and you are sharing with the infra tenant

- If you have an **unmanaged** identity for the access type, then the cloud resources will be managed through a specific application. Go to Adding a Role Assignment for an App, on page 34.

  Note that this access type would apply if you select **Unmanaged Identity** in the **Associate Account** page in the Configuring a Tenant, on page 62 procedures later in this manual.

Adding a Role Assignment for a Virtual Machine

Follow the procedures in this section if you have a **managed** identity for the access type, where you must add a role assignment for the user tenant. See About Tenants, on page 9 for more information about the relationship between Azure subscription types and Cloud APIC tenants.

✎

Note   If you have an **unmanaged** identity for the access type, where the cloud resources will be managed through a specific application, follow the procedures in Adding a Role Assignment for an App, on page 34 instead.

Step 1   From the main Azure management portal page, click the **All services** link in the left nav bar, then click the **Subscriptions** link.

Step 2   In the **Subscriptions** page in the Azure management portal, click the subscription account to which Cloud APIC was deployed.

The overview information for that subscription is displayed.

Step 3   From the overview page for that subscription, locate the **Access control (IAM)** link in the left nav bar and click that link.

The Access Control page for that subscription is displayed.

Step 4   Click + **Add**, then select **Add role assignment** from the drop-down menu.

Step 5   Add a **Contributor** role assignment.

a)   In the **Add role assignment** page, make the following selections:

• In the **Role** field, select **Contributor** from the drop-down menu.

• In the **Assign access to** field, select **Virtual Machine**.

• In the **Subscription** field, select the subscription where the Cloud APIC is deployed.

• Select the Cloud APIC virtual machine.

b) Click **Save** at the bottom of the screen.

Step 6 Add a **User Access Administrator** role assignment.

a) In the **Add role assignment** page, make the following selections:

- In the **Role** field, select **User Access Administrator** from the drop-down menu.

- In the **Assign access to** field, select **Virtual Machine**.

- In the **Subscription** field, select the subscription where the Cloud APIC is deployed.

- Select the Cloud APIC virtual machine.

b) Click **Save** at the bottom of the screen.

Note If you are sharing a subscription for the user tenant, it could take up to 30 minutes for a new IAM role assignment to take effect in Azure. Wait for at least 30 minutes before proceeding to the next section.

What to do next

Go to Configuring Cisco Cloud APIC Using the Setup Wizard, on page 39 to continue setting up the Cloud APIC.

Adding a Role Assignment for an App

Follow the procedures in this section if you have an **unmanaged** identity for the access type, where the cloud resources will be managed through a specific application. See About Tenants, on page 9 for more information about the relationship between Azure subscription types and Cloud APIC tenants.

Note If you have a **managed** identity for the access type, where you must add a role assignment for the user tenant, follow the procedures in Adding a Role Assignment for a Virtual Machine, on page 32 instead.

Step 1 From the main Azure management portal page, click the **All services** link in the left nav bar, then click the **Subscriptions** link.

Step 2   In the **Subscriptions** page in the Azure management portal, click the subscription account to which Cloud APIC was deployed.

The overview information for that subscription is displayed.

Step 3   From the overview page for that subscription, locate the **Access control (IAM)** link in the left nav bar and click that link.

The Access Control page for that subscription is displayed.

Step 4   Click + **Add**, then select **Add role assignment** from the drop-down menu.

Step 5   Add a **Contributor** role assignment.

    a)   In the **Add role assignment** page, make the following selections:

        • In the **Role** field, select **Contributor** from the drop-down menu.

        • In the **Assign access to** field, select **Azure AD user, group, or service principal**.

        • In the **Select** field, select the credentials that are associated with the Azure application.

Add role assignment   ✕

Role ⓘ

| Contributor   ∨ |

Assign access to ⓘ

| Azure AD user, group, or service principal   ∨ |

Select ⓘ

| App1   ✓ |

Selected members:

App1   Remove

| Save | | Discard |

b) Click **Save** at the bottom of the screen.

Step 6   Add a **User Access Administrator** role assignment.

    a) In the **Add role assignment** page, make the following selections:

        • In the **Role** field, select **User Access Administrator** from the drop-down menu.

        • In the **Assign access to** field, select **Azure AD user, group, or service principal**.

        • In the **Select** field, select the credentials that are associated with the Azure application.

b) Click **Save** at the bottom of the screen.

Note   It could take up to 30 minutes for a new IAM role assignment to take effect in Azure. Wait for at least 30 minutes before proceeding to the next chapter. If you attempt to configure the Cloud APIC using the setup wizard before the IAM role assignment takes effect in Azure, then the CSR deployment will fail.

What to do next

Go to Configuring Cisco Cloud APIC Using the Setup Wizard, on page 39 to continue setting up the Cloud APIC.

Configuring Cisco Cloud APIC Using the Setup Wizard

Configuring and Deploying Inter-Site Connectivity

Before you can begin to configure and deploy your Cloud APIC, you must first configure and deploy your Cisco ACI Multi-Site and your on-premises Cisco ACI, if you are connecting an on-premises site to cloud sites. The actual configuration for each varies, depending on your requirements and setup. If you are connecting an on-premises site to cloud sites, you will also need to configure and deploy an on-premises IPsec termination device to connect to the Cisco Cloud Services Router 1000Vs deployed by Cloud APIC in Microsoft Azure. See Components of Extending Cisco ACI Fabric to the Public Cloud, on page 4 for more information.

Following are documents that will aid you in the process of configuring and deploying these components:

- Cisco ACI documentation: Available at Cisco Application Policy Infrastructure Controller (APIC) documentation, such as Operating Cisco Application Centric Infrastructure and Cisco APIC Basic Configuration Guide, Release 4.0(1).

- Cisco ACI Multi-Site: Available at Cisco ACI Multi-Site documentation, such as Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide, Release 2.0(1).

- Cisco Cloud Services Router 1000V: Available at Cisco CSR 1000v documentation.

Gathering On-Premises Configuration Information

Note   You do not have to gather any information in this section if you are only configuring cloud site-to-cloud site connectivity for your Cisco Cloud APIC.

Use the following list to gather and record the necessary on-premises configuration information that you will need throughout these procedures to set up your Cisco Cloud APIC:

Necessary On-Premises Information	Your Entry
On-premises IPsec device public IP address	
IPsec termination device to CSR OSPF area	
On-premises APIC IP address	
Cisco Cloud APIC IP address	

Understanding Limitations for Number of Sites, Regions and CSRs

Throughout this document, you will be asked to decide on various configurations for sites, regions and CSRs. Following is a list of limitations for each that you should keep in mind as you're making configuration decisions for each.

Sites

The total number of sites that you can have with Cloud APIC depends on the type of configuration that you are setting up:

- **On-premises ACI site-to-cloud site configuration (AWS or Azure)**: ACI Multi-Site multi-cloud deployments support any combination of one or two cloud sites (AWS or Azure) and one or two on-premises sites for a maximum total of four sites. The connectivity options are:

    - Hybrid-Cloud: On-premises-to-single cloud site connectivity

    - Hybrid Multi-Cloud: On-premises-to-multiple cloud sites connectivity

- **Multi-Cloud: Cloud site-to-cloud site connectivity (AWS or Azure)**: ACI Multi-Site multi-cloud deployments support a combination of any two cloud sites (AWS, Azure, or both) for a total of two sites.

- **Cloud First: Single-Cloud Configuration**: ACI Multi-Site multi-cloud deployments support a single cloud site (AWS or Azure)

Regions

Within each site, you can have a maximum of four regions per site. Cloud APIC can manage multiple regions as a single site.

CSRs

You can have a certain number of CSRs within some regions, with the following limitations:

- You must have at least one region with CSRs deployed to have inter-VNET (Azure), inter-VPC (AWS), or inter-VRF communications.

- You do not have to have CSRs in every region.

- For regions with CSRs deployed to enable connectivity, the number of CSRs that you can deploy in each region varies:

    - For cloud site-to-cloud site configurations (Multi-Cloud):

        - CSRs can be deployed on a maximum of two managed regions.

        - A maximum of two CSRs per managed region is supported, for a total of four CSRs per cloud site.

    - For on-premises-to-cloud site (Hybrid-Cloud or Hybrid Multi-Cloud) or for single-cloud (Cloud First) configurations :

        - CSRs can be deployed on all four managed regions.

        - A maximum of four CSRs per managed region is supported, for a total of 16 CSRs per cloud site.

Cloud Resources Naming

Prior to Cloud APIC Release 5.0(2), the cloud resources created by the Cloud APIC in Azure were assigned names that were derived from the names of the ACI objects:

- Resource groups were created based on the Tenant, VRF, and region. For example, `CAPIC_<tenant>_<vrf>_<region>`.

- VNET names matched the name of the Cloud APIC VRF.

- Subnet names were derived from the CIDR address space. For example, `subnet-10.10.10.0_24` for the `10.10.10.0/24` cloud subnet.

- The cloud application name was derived from the EPG name and the application profile name. For example, `<epg-name>_cloudapp_<app-profile-name>`

This approach is not ideal for deployments with strict cloud resource naming conventions and it does not follow the Azure best practices for naming and tagging of cloud resources.

Starting with Cloud APIC Release 5.0(2), you can create a global naming policy on the Cloud APIC, which allows you to define a custom cloud resources naming convention for all objects deployed from the Cloud APIC into the Azure cloud. You can define custom naming rules for all cloud resources during the first time setup wizard of the Cloud APIC, with the exception of the **Resource group** name used for the Cloud APIC

ARM template deployment. The resource group name for the template is defined when you first deploy it and cannot be changed after. In addition to the global policy, you can also explicitly define the names of the cloud resources created from each Cloud APIC object using the REST API.

Note
Keep in mind that even with custom naming policy, once a cloud resource is created, you will not be able to modify the name. If you want to change the name of an existing cloud resource, you would need to delete all configured cloud resources and recreate them. Cloud resources to be deleted include overlay-2 CIDR and subnets, Cisco Cloud Services Router 1000Vs deployed by Cloud APIC and therefore IPSec tunnels from the CSRs to every remote site.

Variables Available for Naming Rules

When creating your cloud resources naming policy, you can use the following variables to dynamically define the name of the cloud resource based on the Cloud APIC objects:

- `${tenant}` – the resource will include the name of the Tenant

- `${ctx}` – the resource will include the name of the VRF

- `${ctxprofile}` – the resources will include the cloud context profile, which is a VRF deployed in a given cloud region

- `${app}` – the resource will include the name of the application profile.

- `${epg}` – the resource will include the name of the EPG.

- `${contract}` – the resource will include the name of the contract

- `${region}` – the resource will include the name of the cloud region

- `${priority}` – the resource will include the name of the network security group (NSG) rule priority. This number is allocated automatically to ensure that each NSG rule name is unique

When you define a global naming policy using one or more of the above variables, Cloud APIC validates the string to ensure that all mandatory variables are present and no invalid string is specified.

There is a maximum name length limit in Azure. If the length of the name exceeds the length supported by the cloud provider, it rejects the config and Cloud APIC raises a fault that the resource creation failed. You can then check the fault for details and correct the naming rules. The maximum length limits at the time of Cloud APIC, Release 5.0(2) are listed below, for the latest up-to-date information and any changes to the length limit, consult the Azure documentation.

The following table provides a summary of which cloud resources support each of the naming variables above. Cells denoted with an asterisk (*) indicate variables that are mandatory for that type of cloud resource. Cells denoted with a plus sign (+) indicate that at least one of these variables is mandatory for that type of cloud resource; for example, for VNET resources you can provide `${ctx}`, or `${ctxprofile}`, or both.

Table 2: Supported Variables for Cloud Resources

Azure Resource	${tenant}	${ctx}	${cbprofile}	${subnet}	${app}	${epg}	${contract}	${region}	${priority}
Resource Group Max Length: 90	Yes*	Yes*						Yes*	
Virtual Network (VNET) Max Length: 64	Yes	Yes+	Yes+					Yes	
Subnet Max Length: 80	Yes	Yes	Yes	Yes*				Yes	
Application Security Group (ASG) Max Length: 80	Yes				Yes*	Yes*		Yes	
Network Security Group (NSG) Max Length: 80	Yes				Yes*	Yes*		Yes	
Network Security Group Rule Max Length: 80	Yes						Yes		Yes* (auto)

Naming Rules Guidelines and Limitations

When configuring custom rules for naming cloud resources, the following restrictions apply:

- You define global naming policy during the Cloud APIC's first time setup using two sets of naming rules:

  - **Hub Resource Naming Rules** define names for the Hub Resource Group, Hub VNET, and Overlay-1 CIDR subnet in the Infra Tenant, as well as the subnet prefixes for subnets that are created automatically by the system in the Infra tenant.

  - **Cloud Resource Naming Rules** define the names of the Network Security Group (NSG), Application Security Group (ASG), and subnets you create in the Infra Tenant, as well as the names of all resources (Resource Groups, Virtual Networks, Subnets, NSG, ASG) in user Tenants.

  After you define the naming rules, you will be required to review and confirm them. Keep in mind that you must confirm the naming rules before any cloud resources are deployed.

- Once a cloud resource is created, its name cannot be changed and the naming policy cannot be updated in the GUI. If you upgrade your Cloud APIC to Release 5.0(2) with some resources already deployed in Azure, you will also not be able to change the global custom naming rules.

  If you want to change the names of the existing cloud resources or the policy, you would need to delete the deployed resources before being able to update the global naming policy in the GUI.

In these cases you can use the REST API to explicitly assign custom names to any new resources you create.

- When updating cloud resources naming via REST API, we recommend you do not import configuration at the same time.

We recommend you define any naming rules first. Then any tenant configuration.

We recommend that you do not change the naming policy after the tenant configuration is deployed.

Locating the Cloud APIC IP Address

These procedures describe how to locate the IP address for the Cloud APIC through the Azure site.

Step 1 From the main Azure management portal page, click the **All services** link in the left nav bar, then click the **Subscriptions** link.
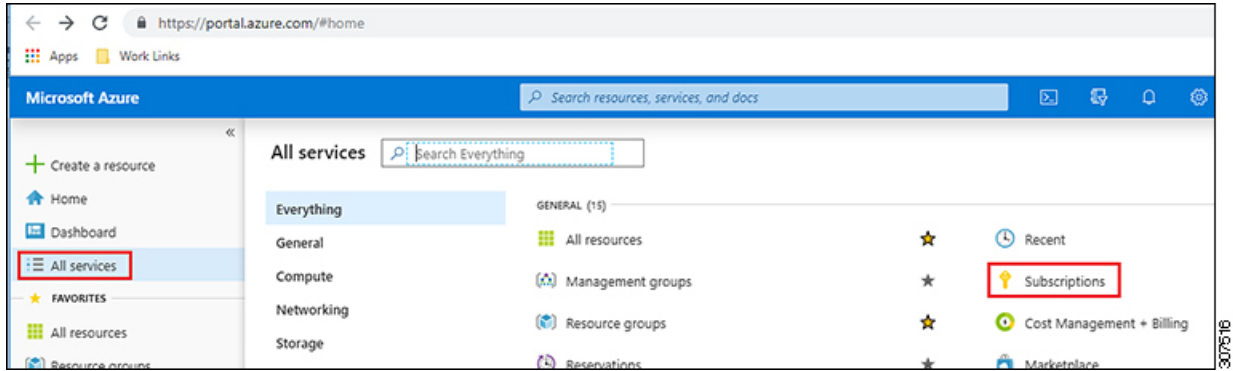
Step 2 In the **Subscriptions** page in the Azure management portal, click the subscription account that you just created.

The overview information for that subscription is displayed.

Step 3 From the overview page for that subscription, locate the **Resource groups** link in the left nav bar and click that link.

The resource groups for that subscription is displayed.

Step 4 Choose the resource group that you chose or created in .

The overview information for that resource group is displayed.

Step 5 In the overview page for the resource group, locate your Cloud APIC VM instance (shown as **Virtual machine** under the TYPE column), and click the link for that VM instance.
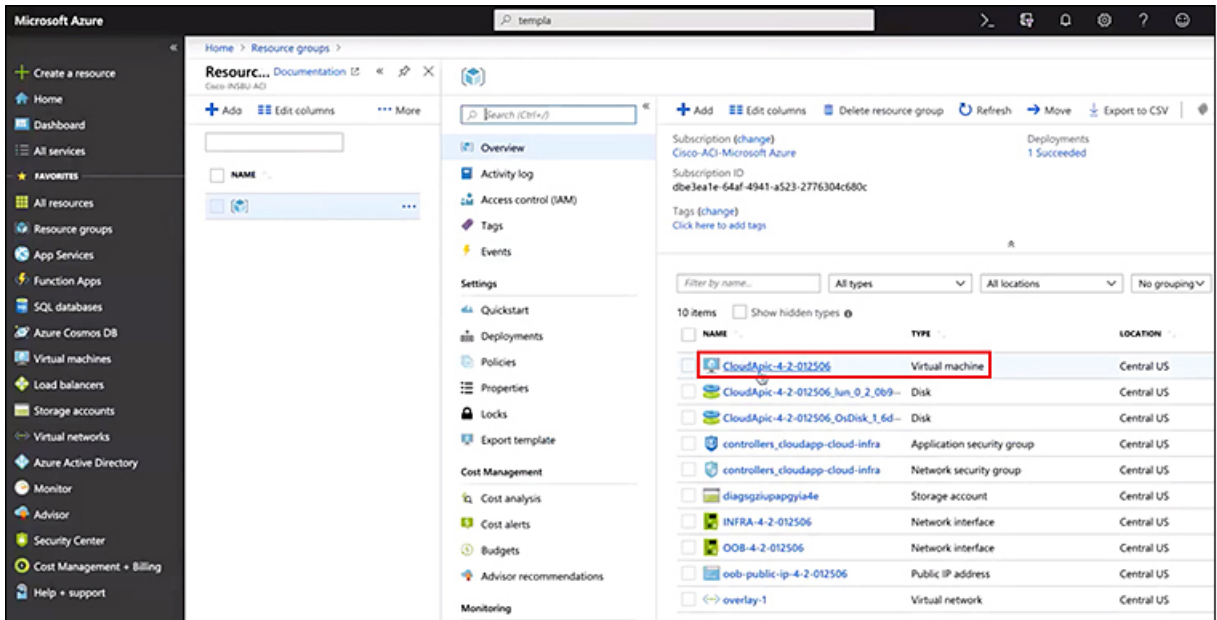
The overview information for the Cloud APIC VM instance is displayed.

Step 6   Locate the entry in the **Public IP address** field in this page and copy that IP address entry.
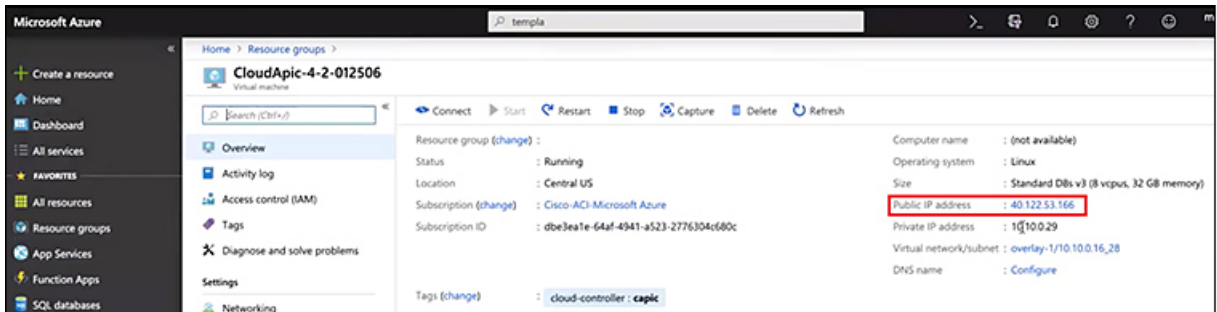
This is the Cloud APIC IP address that you will use to log into the Cloud APIC.

Configuring Cisco Cloud APIC Using the Setup Wizard

Follow the procedures in this topic to set up the cloud infrastructure configuration for your Cloud APIC. Cloud APIC will automatically deploy the required Azure constructs and the necessary CSRs.

Before you begin

Following are the prerequisites for this task:

- You have met the requirements that are outlined in Requirements for Extending the Cisco ACI Fabric to the Public Cloud, on page 13 before proceeding with the tasks in this section.

- You have successfully completed the procedures that are provided in Deploying the Cloud APIC in Azure, on page 19.

Step 1   Locate the IP address for your Cloud APIC.

Step 2   Open a browser window and, using the secure version of HTTP (`https://`), paste the IP address into the URL field, then press Return to access this Cloud APIC.

For example, `https://192.168.0.0`.

If you see a message asking you to **Ignore Risk and Accept Certificate**, accept the certificate to continue.

Step 3   Enter the following information in the login page for the Cloud APIC:

- **Username:** Enter **admin** for this field.

- **Password:** Enter the password that you provided to log into the Cloud APIC.

- **Domain:** If you see the **Domain** field, leave the default Domain entry as-is.

Step 4   Click **Login** at the bottom of the page.

Note   If you see an error message when you try to log in, such as `REST Endpoint user authentication datastore is not initialized - Check Fabric Membership Status of this fabric node`, wait for several minutes, then try again after a few minutes. You might also have to refresh the page in order to log in.

The Welcome to Cloud APIC setup wizard page appears.

Step 5   Click **Begin Set Up**.

The **Let's Configure the Basics** page appears, with these areas to be configured:

- **DNS and NTP Servers**

- **Region Management**

- **Smart Licensing**

Step 6   In the **DNS and NTP Servers** row, click **Edit Configuration**.

The **DNS and NTP** page appears.

Step 7   In the **DNS and NTP** page, add the DNS, if necessary, and NTP servers.

- A DNS server is already configured by default. Add a DNS server if you want to use a specific DNS server.

- An NTP server is not configured by default, however, so we recommend that you configure an NTP server. Skip to 7.d, on page 46 if you want to configure an NTP server and you do not want to configure a DNS server.

a)   If you want to use a specific DNS server, under the **DNS Servers** area, click **+Add DNS Provider**.
b)   Enter the IP address for the DNS servers and, if necessary, check the box next to Preferred DNS Provider.
c)   Click the check mark next to the DNS server, and repeat for any additional DNS servers that you want to add.
d)   Under the **NTP Servers** area, click **+Add Providers**.

    e)   Enter the IP address for the NTP servers and, if necessary, check the box next to Preferred NTP Provider.

    f)   Click the check mark next to the NTP server, and repeat for any additional NTP servers that you want to add.

Step 8   When you have finished adding the DNS and NTP servers, click **Save and Continue**.

            The **Let's Configure the Basics** page appears again.

Step 9   In the **Region Management** row, click **Begin**.

            The **Region Management** page appears.

Step 10   Determine the type of connectivity that you want for the internal network and make the appropriate selection in the **Connectivity for Internal Network** area.

- To enable Azure VNet peering, click **Virtual Network Peering**.

  This enables VNet peering at the Cloud APIC level, deploying NLBs in all the regions with a CSR. For more information on the VNet peering feature, see the *Configuring VNet Peering for Cloud APIC for Azure* document in the Cisco Cloud APIC documentation page.

- To enable the traditional VPN connectivity through the CSRs instead of through VNet peering, click **VPN Connectivity via CSR**.

Step 11   If you want connectivity to the on-premises site or another cloud site—in addition to connectivity within a region—check the **Inter-Site Connectivity** check box.

Step 12   Verify that the Cloud APIC home region is selected.

            The region that you selected when you were configuring your cloud site is the home region and should be selected already in this page. This is the region where the Cloud APIC is deployed (the region that will be managed by Cloud APIC), and will be indicated with the text `Cloud APIC Deployed` in the Region column.

            Note   If you enabled Azure VNet peering in Step 10, on page 47, you must also check the box in the Cloud Routers column for the Cloud APIC home region, if it is not checked already.

Step 13   Select additional regions if you want the Cloud APIC to manage additional regions, and to possibly deploy CSRs to have inter-VNET communication and Hybrid-Cloud, Hybrid Multi-Cloud, or Multi-Cloud connectivity on those other regions.

            The CSR can manage up to four regions, including the home region where Cloud APIC is deployed.

            A Cloud APIC can manage multiple cloud regions as a single site. In a typical Cisco ACI configuration, a site represents anything that can be managed by an APIC cluster. If a Cloud APIC manages two regions, those two regions are considered a single site by Cisco ACI.

            The following options are available on the row for any region that you select:

- **Cloud Routers:** Select this option if you want to deploy CSRs in this region. You must have at least one region with CSRs deployed to have inter-VNET or inter-VPC communications. However, if you choose multiple regions in this page, you do not have to have CSRs in every region that you choose. See Understanding Limitations for Number of Sites, Regions and CSRs, on page 40 for more information.

- **Inter-Site Connectivity:** Select this option if you want this region to connect to other sites (for example, if you want this region to connect to an on-premises site, or to connect cloud site-to-cloud site, through Cisco ACI Multi-Site). Infra VNETs or VPCs are deployed on all regions selected for inter-site connectivity. Note that when you select inter-site connectivity for a region, the cloud routers option is also selected automatically for this region because you must have two cloud routers deployed for inter-site connectivity hubs.

Step 14   When you have selected all the appropriate regions, click **Next** at the bottom of the page.

The **General Connectivity** page appears.

Step 15   Enter the following information on the **General Connectivity** page.

a) In the **Fabric Autonomous System Number** field, enter the BGP autonomous system number (ASN) that is unique to this site.

Note the following Microsoft Azure ASN restrictions:

- Do not use 64518 as the autonomous system number in this field.

- Do not use 32-bit ASNs. Azure VPN Gateways support 16-Bit ASNs at this time.

- The following ASNs are reserved by Azure for both internal and external peerings:

    - Public ASNs: 8074, 8075, 12076

    - Private ASNs: 65515, 65517, 65518, 65519, 65520

    You cannot specify these ASNs for your on-premises VPN devices when connecting to Azure VPN gateways.

- The following ASNs are reserved by IANA and cannot be configured on your Azure VPN Gateway: 23456, 64496-64511, 65535-65551 and 429496729

b) In the **Subnet for Cloud Router** field, enter the subnet for the cloud router.

The first subnet pool for the first two regions is automatically populated. If you selected more than two regions, you will need to add a subnet for the cloud router to the list for the additional two regions. Addresses from this subnet pool will be used for inter-region connectivity for any additional regions that are added that need to be managed by the Cloud APIC after the first two regions. This must be a valid IPv4 subnet with mask /24.

c) Under the **Cloud Router Template** area, in the **Number of Routers Per Region** field, choose the number of Cisco Cloud Services Routers (CSRs) that will be used in each region.

See Understanding Limitations for Number of Sites, Regions and CSRs, on page 40 for more information on any limitations on the number of CSRs per region.

d) In the **Username**, enter the username for the Cisco Cloud Services Router.

Note   Do not use `admin` as a username for the Cisco Cloud Services Router when connecting to an Azure cloud site.

e) In the **Password** field, enter the password for the Cisco Cloud Services Router.

f) In the **Throughput of the routers** field, choose the throughput of the Cisco Cloud Services Router.

Changing the value in this field changes the size of the CSR instance that is deployed. Choosing a higher value for the throughput results in a larger VM being deployed.

Note   If you wish to change this value at some point in the future, you must delete the CSR, then repeat the processes in this chapter again and select the new value that you would like in the same **Throughput of the routers** field.

In addition, the licensing of the CSR is based on this setting. You will need the equivalent or higher license in your Smart account for it to be compliant. See Requirements for the Azure Public Cloud, on page 14 for more information.

Note   Cloud routers should be undeployed from all regions before changing the router throughput or login credentials.

g) Enter the necessary information in the **TCP MSS** field, if applicable.

Beginning with Release 5.0(2i), the **TCP MSS** option is available to configure the TCP maximum segment size (MSS). This value will be applied to all cloud router interfaces, including data Gigabit Ethernet interfaces, IPSec tunnel interfaces of cloud routers, and VPN tunnel interfaces toward cloud, on-premises, or other cloud sites. For VPN tunnels towards the cloud, if the cloud provider's MSS value is less than the value that you enter in this field, then the lower value is used; otherwise, the value that you enter in this field is used.

The MSS value affects only TCP traffic, and has no impact on other types of traffic, such as ping traffic.

h) In the **License Token** field, enter the license token for the Cisco Cloud Services Router.

This is the Product Instance Registration token from your Cisco Smart Software Licensing account. To get this license token, go to http://software.cisco.com, then navigate to **Smart Software Licensing** > **Inventory** > **Virtual Account** to find the Product Instance Registration token.

Step 16 Click the appropriate button, depending on whether you are configuring inter-site connectivity or not.

- If you are not configuring inter-site connectivity (if you did not select **Inter-Site Connectivity** when you were selecting regions to manage in the **Region Management** page), click **Save and Continue**. The **Let's Configure the Basics** page appears again. Skip to Step 22, on page 50.

- If you are configuring inter-site connectivity (if you selected **Inter-Site Connectivity** when you were selecting regions to manage in the **Region Management** page), click **Next** at the bottom of the page. The **Inter-Site Connectivity** page appears.

Step 17 Enter the following information in the **Inter-Site Connectivity** page:

- **IPSec Tunnels to Inter-Site Routers**: This field is necessary only for on-premises connectivity to cloud sites. There is no need to enter information in this field if you don't have an on-premises site.

  In this area, click the + button next to the **Add Public IP of IPsec Tunnel Peer** field.

  - Enter the peer IP address for the IPsec tunnel termination to the on-premises device.

  - Click the check mark to add this peer IP address.

- **OSPF Area for Inter-Site Connectivity**: Enter the underlay OSPF area ID that will be used with on-premises ISN peering (for example, `0.0.0.1`)

- Under the **External Subnets for Inter-Site Connectivity** heading, click the + button next to the +**Add External Subnet** field.

  - Enter the subnet tunnel endpoint pool (the cloud TEP) that will be used in Azure. It must be a valid IPv4 subnet with a mask between /16 and /22 (for example, `30.29.0.0/16`). This subnet will be used to address the IPsec tunnel interfaces and loopbacks of the Cloud Routers used for on-premises connectivity, and cannot overlap with other on-premises TEP pools.

  - Click the check mark after you have entered in the appropriate subnet pools.

Step 18 When you have configured all the connectivity options, click **Next** at the bottom of the page.

The **Cloud Resource Naming Rules** page appears.

Step 19 Choose **Cloud Resource Naming** mode.

Starting with Release 5.0(2), you can create a global naming policy on the Cloud APIC, which allows you to define a custom cloud resources naming convention for all objects deployed from the Cloud APIC into the Azure cloud. Additional details about naming rules, available object name variables, guidelines, and limitations are available in the earlier Cloud Resources Naming, on page 41 section of this chapter.

You can choose one of the following:

- **Default**, in which case the cloud resources created by the Cloud APIC in Azure will be assigned names that are derived from the names of the ACI objects. For example, resource groups' names will be based on the Tenant, VRF, and region: `CAPIC_<tenant>_<vrf>_<region>`.

- **Custom**, in which case you can define your own rules for how each of the cloud resources is named.

  When you select the custom naming, an **Edit** icon appears next to each cloud resource. You can click the edit icon to define the naming convention for one or more of the displayed resources.

  The variables that are available for this type of resource are listed under the naming rule text box. The variables are divided into the **Required Keyword** and **Optional Keywords**, you must include all the required keywords for the rule you are updating. For example, when defining the naming rule for Azure's Resource Groups, you must include the Tenant name, VRF name, and the Region keywords.

Step 20   Confirm you have reviewed and accept the global resource naming policy.

Once a cloud resource is created, its name cannot be changed. As such, you must review and accept the global naming policy you have defined in the previous step before any cloud resources can be deployed. When ready, enable the **Deploy cloud resources based on these naming rules** checkbox.

Note that you can leave the checkbox unchecked and choose to proceed, in which case any changes you have made will be saved but no configuration will be deployed. You would need to come back to this screen to accept the naming policy to deploy.

Step 21   When you have entered all the necessary information on this page, click **Save and Continue** at the bottom of the page.

The **Let's Configure the Basics** page appears again.

Step 22   In the **Smart Licensing** row, click **Register**.

The **Smart Licensing** page appears.

Step 23   Enter the necessary information in the **Smart Licensing** page.

Cisco Smart Licensing is a unified license management system that manages software licenses across Cisco products. To register your Cloud APIC with Cisco Smart Software Licensing, do the following

- Ensure that this product has access to the internet or a Smart Software Manager satellite installed on your network.

- Log in to Smart Account:

  - Smart Software Manager: https://software.cisco.com/

  - Smart Software Manager Satellite: https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html

- Navigate to the Virtual Account containing the licenses to be used by this Product Instance.

- Generate a Product Instance Registration Token (this identifies your Smart Account) and copy or save it.

To learn more about Smart Software Licensing, visit https://www.cisco.com/go/smartlicensing.

Step 24   Click **Register** at the bottom of the page if you entered the necessary licensing information on this page, or click **Continue in Evaluation Mode** if you want to continue in evaluation mode instead.

The **Summary** page appears.

Step 25   Verify the information on the **Summary** page, then click **Finish**.

At this point, you are finished with the internal network connectivity configuration for your Cloud APIC.

If this is the first time that you are deploying your Cloud APIC, this process might take quite a bit of time, possibly 30 minutes or so before the process is successfully completed.

Step 26   Verify that the CSRs were successfully deployed.

a) From the main Azure management portal page, click the **All services** link in the left nav bar, then click the **Subscriptions** link.
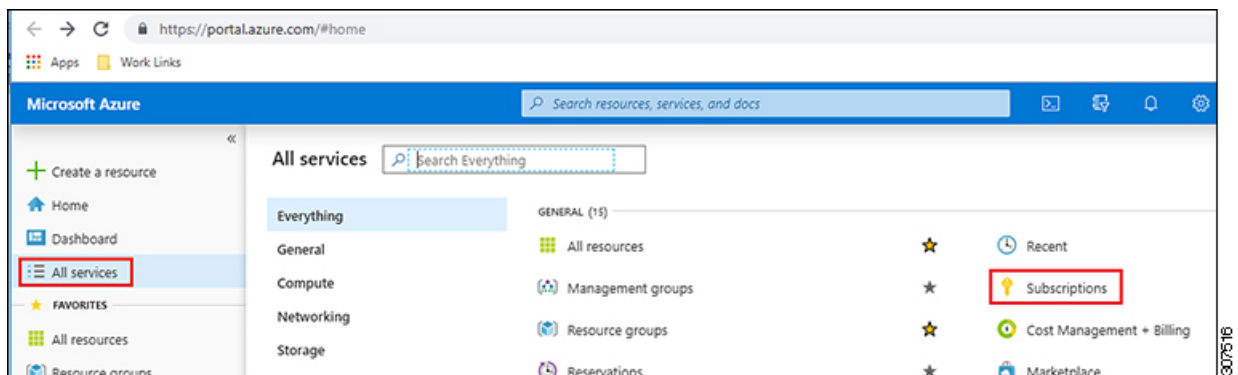
b) In the **Subscriptions** page in the Azure management portal, click the subscription account that you created.

The overview information for that subscription is displayed.

c) From the overview page for that subscription, locate the **Resource groups** link in the left nav bar and click that link.

The resource groups for that subscription is displayed.

d) Choose the resource group that you chose or created in the **Custom deployment** page in .

The overview information for that resource group is displayed.

e) In the overview page for the resource group, locate your CSR VM instance (shown as **Virtual machine** under the TYPE column), and click the link for that VM instance.

The CSR VM instance will have a name with a `ct_routerp_region_x_0` format, where:

- *region* is the managed region (for example, `westus`, `westus2`, `centralus`, or `eastus`)

- *x* is the CSR count, starting from zero

For example: `ct_routerp_centralus_0_0` or `ct_routerp_centralus_1_0`

The overview information for the CSR VM instance is displayed.

f) Locate the **Status** field at the top left area in the page.

- If you see the text **Creating** in the **Status** field, then the CSRs are not fully deployed yet.

• If you see the text **Running** in the **Status** field, then the CSRs are fully deployed.

What to do next

Determine if you are managing additional sites along with the Cisco Cloud APIC site or not:

- If you are managing additional sites (an on-premises site or cloud sites) along with the Cisco Cloud APIC site (if you selected the **Inter-Site Connectivity** option in the **Region Management** page), go to Managing Cisco Cloud APIC Through Cisco ACI Multi-Site, on page 55.

- If you are setting up a Cloud First configuration, where you are not managing any other sites along with the Cisco Cloud APIC site (if you selected only the **Cloud Routers** option in the **Region Management** page), you will not need to use the Cisco ACI Multi-Site for additional configurations. However, you will have additional configurations that you must perform in the Cisco Cloud APIC GUI in this case.

  You also need to create a tenant using the Cisco Cloud APIC GUI using the instructions in Creating a Tenant Using the Cisco Cloud APIC GUI, on page 73.

  Use the Global Create option in the Cisco Cloud APIC GUI to configure the following components:

    - Tenant

    - Application Profile

    - EPG

  See Navigating the Cisco Cloud APIC GUI, on page 73 and Configuring Cisco Cloud APIC Components, on page 73 for more information.

Verifying the Cisco Cloud APIC Setup Wizard Configurations

Use the procedures in this topic to verify that the configuration information that you entered in the Cloud APIC Setup Wizard are applied correctly.

In Cisco Cloud APIC, verify the following settings:

- Under **Cloud Resources**, click on **Regions** and verify that the regions that you selected are shown as **managed** in the Admin State column.

- Under **Infrastructure**, click on **Inter-Region Connectivity** and verify the information in this screen is correct.

- Under **Infrastructure**, click on **Inter-Site Connectivity** and verify the information in this screen is correct.

- Click on Dashboard and use the information in the On Premises Connectivity Status and the Inter-Region Connectivity Status boxes to verify that the setup wizard and tunnel configurations were done properly.

What to do next

Complete the multi-site configuration using the procedures provided in Managing Cisco Cloud APIC Through Cisco ACI Multi-Site, on page 55.

Managing Cisco Cloud APIC Through Cisco ACI Multi-Site

About Cisco Cloud APIC and Cisco ACI Multi-Site

If you selected the **Inter-Site Connectivity** option in the **Region Management** page when configuring Cisco Cloud APIC using the setup wizard, you will use Cisco ACI Multi-Site to manage another site, such as an on-premises site or cloud sites, along with the Cisco Cloud APIC site. You do not need the Cisco ACI Multi-Site if you selected only the **Cloud Routers** option in the **Region Management** page in the Setup Wizard for Cisco Cloud APIC.

Several new pages have been introduced in the ACI Multi-Site Orchestrator that are used specifically for the management of the Cisco Cloud APIC. The topics in this chapter provide information on these new Cisco Cloud APIC management pages. Once you have entered the necessary information in these Cisco Cloud APIC management pages, the Cisco Cloud APIC essentially becomes another site that you manage through the Cisco ACI Multi-Site.

If you are managing an on-premises site along with the Cisco Cloud APIC site, we recommend that you set up your on-premises site before beginning these procedures, if it is not set up already. See the *Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide* for those procedures, located here:

https://www.cisco.com/c/en/us/support/cloud-systems-management/
application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Adding the Cisco Cloud APIC Site to Cisco ACI Multi-Site

Step 1   Log in to the ACI Multi-Site Orchestrator, if you aren't already logged in.

Step 2   In the Main menu, click **Sites**.

Step 3   In the **Sites List** page, click **ADD SITE**.

Step 4   In the **Connection Settings** page, perform the following actions:

a)   In the **NAME** field, enter the site name.

For example, `cloudsite1`.

b)   (Optional) In the **LABELS** field, choose or create a label.

c)   In the **APIC CONTROLLER URL** field, enter the URL of the Cloud APIC. This is the public IP address allocated by Azure, which will be the same public IP address that you used to log into the Cloud APIC at the beginning of the procedures for configuring Cisco Cloud APIC using the setup wizard.

For example, `https://192.0.2.1`.

d)   In the **USERNAME** field, enter a username.

For example, `admin`. Note that you can also register with any account that has the same privilege as `admin`.

e)   In the **PASSWORD** field, enter the password.

f)   In the **APIC SITE ID** field, enter a unique site ID, if this field is not already populated automatically.

The site ID must be a unique identifier of the Cloud APIC site. The range must be from 1 to 127.

g)   Click **SAVE**.

Step 5   Verify that Cloud APIC site was added correctly.

If you are managing multiple sites, all sites should be displayed in the Sites screen in the ACI Multi-Site Orchestrator. The ACI Multi-Site Orchestrator automatically detects if the site is an on-premises or a Cloud APIC site.

What to do next

Go to the section Configuring the Intersite Infrastructure.

Configuring the Intersite Infrastructure

Step 1   In the **Sites** screen, click **CONFIGURE INFRA**.

The **Fabric Connectivity Infra** page appears.

Step 2   In the left pane, under **SITES**, click on the cloud site.

Almost all of the information in the cloud site area is automatically populated and cannot be changed, with the exception of the BGP Password field, described in the next step.

Step 3   Determine if you want to configure a password between your on-premises site and your cloud site:

- If you do *not* want to configure a password between your on-premises site and your cloud site, skip to Step 4, on page 57.

- If you want to configure a password between your on-premises site and your cloud site:

a)   In the right pane, click on the **BGP Password** field and enter a password.

b)   Click the Refresh icon at the upper right corner of the CloudSite window.

   All of the cloud properties are automatically fetched from the Cloud APIC. A `Site refreshed successfully` message appears, verifying that all the cloud properties were successfully fetched from the Cloud APIC.

Step 4   Click the **ACI Multi-Site** button to toggle this on to enable Multi-Site connectivity in the cloud site.

Step 5   Choose the type of deployment that you would like to use to configure the intersite infrastructure.

When you click the **Deploy** button at the top right of the screen, it shows the following scroll-down menu options:

- **Deploy Only:** Select this option if you are configuring Multi-Cloud (cloud site-to-cloud site) connectivity.

   This option pushes the configuration to the cloud sites and the Cloud APIC site and enables the end-to-end interconnect connectivity between the cloud sites.

- **Deploy & Download IPN Device config files:** Pushes the configuration to both the on-premises APIC site and the Cloud APIC site and enables the end-to-end interconnect connectivity between the on-premises and the cloud site. In addition, this option downloads a zip file that contains configuration information that you will use to enable connectivity between the Cisco Cloud Services Router 1000V (CSR) deployed in Azure and the on-premises IPsec termination device. A followup screen appears that allows you to select all or some of the configuration files to download.

- **Download IPN Device config files only:** Downloads a zip file that contains configuration information that you will use to enable connectivity between the Cisco Cloud Services Router 1000V (CSR) deployed in Azure and the on-premises IPsec termination device. A followup screen appears that allows you to select all or some of the configuration files to download.

Enabling Connectivity Between the Cisco Cloud APIC and the ISN Devices

Note   Follow the procedures in this section only if you are enabling connectivity between the on-premises site and the cloud site. If you do not have an on-premises site, skip these procedures and go to Creating a Security Domain Using the Cisco Cloud APIC GUI, on page 62.

Follow these procedures to manually enable connectivity between Cisco Cloud Services Router 1000V (CSR) deployed in Azure and the on-premises IPsec termination device.

By default, the Cisco Cloud APIC will deploy a pair of redundant Cisco Cloud Services Router 1000Vs. The procedures in this section creates two tunnels, one IPsec tunnel from the on-premises IPsec device to each of these Cisco Cloud Services Router 1000Vs.

The following information provides commands for Cisco Cloud Services Router 1000V as your on-premises IPsec termination device. Use similar commands if you are using a different device or platform.

Step 1 Gather the necessary information that you will need to enable connectivity between the CSRs deployed in Azure and the on-premises IPsec termination device.

- If you selected either the **Deploy & Download IPN Device config files** or the **Download IPN Device config files only** option in ACI Multi-Site Orchestrator as part of the procedures provided in Configuring the Intersite Infrastructure, on page 56, locate the zip file that contains the configuration files for the ISN devices.

- If you are manually locating the information that you need to enable connectivity between the CSRs deployed in Azure and the on-premises IPsec termination device, gather the CSR and Tenant information, as described in the Appendix of the *Cisco Cloud APIC Installation Guide*.

Step 2 Log into the on-premises IPsec device.

Step 3 Configure the tunnel for the *first* CSR.

If you downloaded the configuration files for the ISN devices through ACI Multi-Site Orchestrator, locate the configuration information for the first CSR and enter that configuration information.

Following is an example of what the configuration information for the first CSR might look like:

```
crypto isakmp policy 1
    encryption  aes
    authentication pre-share
    group  2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-<first-CSR-tunnel-ID>
    pre-shared-key address <first-CSR-elastic-IP-address> key <first-CSR-preshared-key>
exit

crypto isakmp profile infra:overlay-1-<first-CSR-tunnel-ID>
    local-address <interface>
    match identity address <first-CSR-elastic-IP-address>
    keyring infra:overlay-1-<first-CSR-tunnel-ID>
exit

crypto ipsec transform-set infra:overlay-1-<first-CSR-tunnel-ID> esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-<first-CSR-tunnel-ID>
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel <first-CSR-tunnel-ID>
    ip address <peer-tunnel-for-onprem-IPsec-to-first-CSR> 255.255.255.252
    ip virtual-reassembly
    tunnel source <interface>
```

```
        tunnel destination <first-CSR-elastic-IP-address>
        tunnel mode ipsec ipv4
        tunnel protection ipsec profile infra:overlay-1-<first-CSR-tunnel-ID>
        ip mtu 1476
        ip tcp adjust-mss 1460
        ip ospf <process-id> area <area-id>
        no shut
exit
```

Where:

- <first-CSR-tunnel-ID> is a unique tunnel ID that you assign to this tunnel.

- <first-CSR-elastic-IP-address> is the elastic IP address of the third network interface of the first CSR.

- <first-CSR-preshared-key> is the preshared key of the first CSR.

- <interface> is the interface that is used for connecting to the Cisco Cloud Services Router 1000V deployed in Azure.

- <peer-tunnel-for-onprem-IPsec-to-first-CSR> is the peer tunnel IP address for the on-premises IPsec device to the first cloud CSR.

- <process-id> is the OSPF process ID.

- <area-id> is the OSPF area ID.

For example:

```
crypto isakmp policy 1
    encryption  aes
    authentication pre-share
    group  2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-1000
    pre-shared-key address 192.0.2.20 key 12345678900987654321234567890
exit

crypto isakmp profile infra:overlay-1-1000
    local-address GigabitEthernet1
    match identity address 192.0.2.20
    keyring infra:overlay-1-1000
exit

crypto ipsec transform-set infra:overlay-1-1000 esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-1000
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel 1000
    ip address 30.29.1.2 255.255.255.252
    ip virtual-reassembly
    tunnel source GigabitEthernet1
    tunnel destination 192.0.2.20
    tunnel mode ipsec ipv4
```

```
        tunnel protection ipsec profile infra:overlay-1-1000
        ip mtu 1476
        ip tcp adjust-mss 1460
        ip ospf 1 area 1
        no shut
    exit
```

Step 4   Configure the tunnel for the *second* CSR.

If you downloaded the configuration files for the ISN devices through ACI Multi-Site Orchestrator, locate the configuration information for the second CSR and enter that configuration information.

Following is an example of what the configuration information for the second CSR might look like:

```
crypto isakmp policy 1
    encryption   aes
    authentication pre-share
    group  2
    lifetime 86400
    hash sha
exit

crypto keyring infra:overlay-1-<second-CSR-tunnel-ID>
    pre-shared-key address <second-CSR-elastic-IP-address> key <second-CSR-preshared-key>
exit

crypto isakmp profile infra:overlay-1-<second-CSR-tunnel-ID>
    local-address <interface>
    match identity address <second-CSR-elastic-IP-address>
    keyring infra:overlay-1-<second-CSR-tunnel-ID>
exit

crypto ipsec transform-set infra:overlay-1-<second-CSR-tunnel-ID> esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-<second-CSR-tunnel-ID>
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel <second-CSR-tunnel-ID>
    ip address <peer-tunnel-for-onprem-IPsec-to-second-CSR> 255.255.255.252
    ip virtual-reassembly
    tunnel source <interface>
    tunnel destination <second-CSR-elastic-IP-address>
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-<second-CSR-tunnel-ID>
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf <process-id> area <area-id>
    no shut
exit
```

For example:

```
crypto isakmp policy 1
    encryption   aes
    authentication pre-share
```

```
      group  2
      lifetime 86400
      hash sha
exit

crypto keyring infra:overlay-1-1001
    pre-shared-key address 192.0.2.21 key 123456789009876543211234567891
exit

crypto isakmp profile infra:overlay-1-1001
    local-address GigabitEthernet1
    match identity address 192.0.2.21
    keyring infra:overlay-1-1001
exit

crypto ipsec transform-set infra:overlay-1-1001 esp-aes esp-sha-hmac
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-1001
    set pfs group2
    set security-association lifetime seconds 86400
exit

interface tunnel 1001
    ip address 30.29.1.6 255.255.255.252
    ip virtual-reassembly
    tunnel source GigabitEthernet1
    tunnel destination 192.0.2.21
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-1001
    ip mtu 1476
    ip tcp adjust-mss 1460
    ip ospf 1 area 1
    no shut
exit
```

Step 5   Repeat these steps for any additional CSRs that you need to configure.

Step 6   Verify that the tunnels are up on your on-premises IPsec device.

For example:

```
ISN_CSR# show ip interface brief | include Tunnel
Interface            IP-Address      OK? Method Status          Protocol
Tunnel1000           30.29.1.2       YES manual up              up
Tunnel1001           30.29.1.4       YES manual up              up
```

If you do not see that both tunnels are shown as up, verify the information that you entered in the steps in this section to determine where you might have an issue. Do not proceed to the next section until you see that both tunnels are shown as up.

Creating a Security Domain Using the Cisco Cloud APIC GUI

A security domain restricts the tenant to the security domains that you add. If you do not add a security domain, all security domains will have access to this tenant. You will be given the choice of choosing these security domains when you configure a shared tenant using the procedures in Configuring a Tenant, on page 62.

This section explains how to create a security domain using the Cloud APIC GUI.

Step 1	Log into your Cloud APIC system.
Step 2	Click the **Intent** icon. The **Intent** menu appears.
Step 3	Click the drop-down arrow below the **Intent** search box and choose **Administrative**.
	A list of **Administrative** options appear in the **Intent** menu.
Step 4	From the **Administrative** list in the **Intent** menu, click **Create Security Domain**. The **Create Security Domain** dialog box appears.
Step 5	In the **Name** field, enter the name of the security domain.
Step 6	In the **Description** field, enter a description of the security domain.
Step 7	Click **Save** when finished.

Configuring a Tenant

Use the procedures in this section to configure a tenant that is shared between the on-premises site and the Cloud APIC site. See About Tenants, on page 9 for more information about the relationship between Azure subscription types and Cloud APIC tenants.

Step 1	Log in to your Multi-Site Orchestrator GUI.
Step 2	In the left navigation menu, click **Tenants**.
Step 3	In the main pane, click **Add Tenant**.
Step 4	In the **Add Tenant** window, provide a name for the tenant.
	You may also choose to provide a description of the tenant.
Step 5	If the tenant needs to be deployed to an on-premises site, in the **Associated Sites** area, select the on-premises site by checking the check box next to it.
	(Optional) You can also choose a security domain from the drop-down list for the site.
Step 6	To add an Azure cloud site to the tenant, in the **Associated Sites** area, select the Azure cloud site by checking the check box next to it.
	When associating an Azure cloud site with a tenant, you must also provide the Azure subscription information.
Step 7	After you check an Azure site, select the security domain from the drop-down list, if available, then click **Associate Account** next to it.
Step 8	Select the mode for the Azure account.

- Choose **Mode: Create Own** if you want to associate the tenant with a new Azure subscription, then enter information in the following fields:

  a. In the **Azure Subscription ID** field, provide the ID of the Azure subscription.

  You can obtain the subscription ID by logging into your Azure account and navigating to **Home** > **Subscriptions**. You must use the **Subscription ID** and not **Subscription Name** as listed in the Azure portal.

  b. (Optional) In the **Security Domain** field, select the security domains under the cloud account if you want to share this cloud account with other security domains.

  For more information, see Creating a Security Domain Using the Cisco Cloud APIC GUI, on page 62.

  c. In the **Access Type** field, choose the access type between the Cloud APIC VM and the tenant.

    - Select **Unmanaged Identity** to manage the cloud resources through a specific application.

    This can be used 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.

    In this case, you must also provide the application's credentials to the Cloud APIC. Refer to the information that you saved at the end of the procedures in Creating an Application in Azure, on page 23:

      - **Application ID:** Enter the application ID for the Azure application. This ID is listed in **Home** > **App registrations** > **<application-name>**, in the **Application (client) ID** field.

      - **Client Secret:** Enter the application secret. You can create a secret under **Home** > **App registrations** > **<application-name>** > **Certificates & secrets** > **New client secret**.

      - **Azure Active Directory ID:** Enter the application directory ID for the Azure application. This ID is listed in **Home** > **App registrations** > **<application-name>**, in the **Directory (tenant) ID** field.

    | **Note** | You will also have to add a role assignment for the app in this case. See Adding a Role Assignment for an App, on page 34 for those procedures. |

    - Select **Managed Identity** to allow the Cloud APIC VM to manage the cloud resources.

    This can be used when the Azure subscriptions are in the same directory (of the same organization).

    | **Note** | You will also have to add a role assignment for the VM in this case. See Adding a Role Assignment for a Virtual Machine, on page 32 for those procedures. |

- Choose **Mode: Select Shared** if you want to use an existing subscription that is shared with an existing tenant.

  Azure allows you to create multiple tenants using the same subscription.

  If you choose **Select Shared**, you can then select a cloud account from the drop-down list. The cloud accounts available in the drop-down list are based on the security domain that you selected in Step 7, on page 62. Your new tenant will be associated with the same Azure subscription as the selected account.

  | **Note** | If you configured a security domain, then the cloud account that you select must have been shared with the same security domain that you selected for the tenant. All tenants sharing the same Azure subscription must be in the same security domain. |

Step 9   If necessary, in the **Associated Users** area, select which users have access to the tenant.

Step 10   (Optional) Enable consistency checker.

You may choose to enable scheduled consistency checker for this tenant. Additional information about consistency check is available in the *Cisco ACI Multi-Site Configuration Guide*.

Step 11   Click **Save** to add the tenant.

What to do next

Go to Creating a Schema, on page 64 to create a schema.

Creating a Schema

There are several general Cisco ACI Multi-Site procedures that are not specific to the Cisco Cloud APIC, but that must be performed as part of the overall Cisco Cloud APIC setup if you are managing an on-premises site and a Cisco Cloud APIC site through Cisco ACI Multi-Site. The following topics provide these general Cisco ACI Multi-Site procedures that are part of the overall Cisco Cloud APIC setup.

Follow the instructions in this section if you want to create a new schema for the Cisco Cloud APIC site.

If you already have a schema that you want to use for the Cisco Cloud APIC site, you can skip these steps and go straight to Adding Sites to the Schema, on page 66.

Step 1   In the Main menu, click **Schemas**.

Step 2   On the Schema page, click the **Add Schema** button.

Step 3   On the Untitled Schema page, replace the text `Untitled Schema` at the top of the page with a name for the schema that you intend to create (for example, `Cloudbursting-Schema`).

Step 4   In the left pane, click **Template 1**.

Step 5   In the middle pane, click the area **To build your schema please click here to select a tenant**.

Step 6   In the right pane, access the **Select A Tenant** dialog box and select the tenant that you created in Configuring a Tenant, on page 62 from the drop-down menu.

Configuring an Application Profile and the EPGs

This procedure describes how to configure an application profile and add two EPGs, one for cloud site and one for the on-premises site, where the provider contract is associated with one EPG and the consumer contract is associated with the other EPG.

Step 1   In the middle pane, locate the Application Profile area, then click + **Application Profile**.

Step 2   In the right pane, enter the Application Profile name in the **DISPLAY NAME** field.

Step 3   In the middle pane, click + **Add EPG** to create an EPG for the cloud site.

Step 4   In the right pane, enter an EPG name in the **DISPLAY NAME** field (for example, `epg1`).

Step 5   In the middle pane, click + **Add EPG** again, if you want to create an EPG for the on-premises site.

Step 6   In the right pane, enter an EPG name in the **DISPLAY NAME** field (for example, `epg2`).

Step 7 Create a VRF:

a) In the middle pane, scroll down until you see the VRF area, then click the + in the dotted box.

b) In the right pane, enter the VRF name in the **DISPLAY NAME** field (for example, `vrf1`).

Step 8 Click **SAVE**.

Creating and Associating a Bridge Domain with a VRF

Follow the procedures in this section to create a bridge domain for the on-premises site and associate it with the VRF. Note that these procedures are not necessary for a cloud-only schema.

Step 1 In the middle pane, scroll back up to **EPG** and click on the EPG that you created earlier for the on-premises site.

Step 2 In the right pane, in the **ON-PREM PROPERTIES** area, under **BRIDGE DOMAIN**, create a new bridge domain by typing a name in the field (for example, `bd1`), then click the **Create** area.

Step 3 In the middle pane, click the bridge domain that you just created.

Step 4 In the **Virtual Routing & Forwarding** field, select the VRF that you created in .

Step 5 Scroll down to the **SUBNETS** area and click on the + next to **SUBNET** under the **GATEWAY** heading.

Step 6 On the **Add Subnet** dialog, enter the **Gateway IP** address and a description for the subnet you plan to add. The Gateway IP address is the on-premises subnet.

Step 7 In the **Scope** field, select **Advertised Externally**.

Step 8 Click **SAVE**.

Creating a Filter for a Contract

Step 1 In the middle pane, scroll down until you see the Filter area, then click + in the dotted box.

Step 2 In the right pane, enter a name for the filter in the **DISPLAY NAME** field.

Step 3 Click + **Entry** to provide information for your schema filter on the **Add Entry** display:

a) Enter a name for the schema filter entry in the **Name** field on the **Add Entry** dialog.

b) Optional. Enter a description for the filter in the **Description** field.

c) Enter the details as appropriate to filter EPG communication.

For example, to add an entry allowing HTTPS traffic through a filter, choose:

TYPE: IP, IP PROTOCOL: TCP, and DESTINATION PORT RANGE FROM and DESTINATION PORT RANGE TO: https.

d) Click **SAVE**.

Creating a Contract

Step 1   In the middle pane, scroll down until you see the Contract area, then click + in the dotted box.

Step 2   In the right pane, enter a name for the contract in the **DISPLAY NAME** field.

Step 3   In the **SCOPE** area, leave the selection at VRF.

Step 4   In the **FILTER CHAIN** area, click + **FILTER**.

                The Add Filter Chain screen appears.

Step 5   In the **NAME** field, select the filter that you created in .

Step 6   In the middle pane, scroll back up to **EPG** and click on the EPG that you created for the cloud site.

Step 7   In the right pane, click + **CONTRACT**.

                The Add Contract screen appears.

Step 8   In the **CONTRACT** field, select the contract that you created earlier in this procedure.

Step 9   In the **TYPE** field, select either **CONSUMER** or **PROVIDER**.

Step 10   Scroll to the **CLOUD PROPERTIES** area, then, in the **VIRTUAL ROUTING & FORWARDING** area, choose the VRF that you created in .

Step 11   Click **SAVE**.

Step 12   In the middle pane, scroll back up to **EPG** and click on the EPG that you created for the on-premises site.

Step 13   In the right pane, click + **CONTRACT**.

                The Add Contract screen appears.

Step 14   In the **CONTRACT** field, select the same contract that you created earlier in this procedure.

Step 15   In the **TYPE** field, select either **CONSUMER** or **PROVIDER**, whatever you did not select for the previous EPG.

                For example, if you selected **PROVIDER** for the first EPG, select **CONSUMER** for the second EPG.

Step 16   Scroll to the **CLOUD PROPERTIES** area, then, in the **VIRTUAL ROUTING & FORWARDING** area, choose the same VRF that you created in .

Adding Sites to the Schema

Step 1   In the left pane, click the + next to **Sites**.

Step 2   On the **Add Sites** page, add the on-premises and cloud sites to the schema by checking the box next to each, then click **Save**.

Step 3   Click on the template underneath the cloud site in the left pane to configure the site local properties for the template.

Step 4   In the middle pane, click on the VRF.

Step 5   In the right pane, in the **SITE LOCAL PROPERITES** area, enter the following information:

          a)   In the **REGIONS** field, select the Azure region that this VRF will be deployed on.

b) In the **CIDRS** field, click +**CIDR**.

The **ADD CLOUD CIDR** dialog appears. Enter the following information:

- **CIDR** — Enter the VNET CIDR information. For example, `11.11.0.0/16`.

  The CIDR includes the scope of all subnets that are going to be available to an Azure VNET.

  Note The VNET CIDR information that you enter in this field cannot overlap with the infra pool. Verify that the CIDR information that you enter in this field does not overlap with the infra pool information that you entered in the **Infra Subnet** field in Step 6, on page 29 in Deploying the Cloud APIC in Azure, on page 28.

- **CIDR TYPE** — Select Primary or Secondary. If this is your first CIDR, select Primary for the CIDR type.

- **ADD SUBNETS** — Enter the subnet information, then click the check mark. For example, `11.11.1.0/24`.

  For the Cisco Cloud APIC, the subnet should be a valid subnet with subnet mask, and not an IP address with a subnet mask. For example, `11.11.0.0/24` is a valid subnet and subnet mask, whereas `11.11.0.1` is an IP address and subnet mask, but is not a valid subnet to use with the Cisco Cloud APIC.

  Note You must add one subnet specifically for the VGW. Select **Used by VGW** for this particular subnet.

c) Click **SAVE** in the window.

Adding an Endpoint Selector

On the Cisco Cloud APIC, a cloud EPG is a collection of endpoints that share the same security policy. Cloud EPGs can have endpoints in one or more subnets and are tied to a VRF.

The Cisco Cloud APIC has a feature called endpoint selector, which is used to assign an endpoint to a Cloud EPG. The endpoint selector is essentially a set of rules run against the cloud instances assigned to the Azure VNET managed by Cisco ACI. Any endpoint selector rules that match endpoint instances will assign that endpoint to the Cloud EPG. The endpoint selector is similar to the attribute-based microsegmentation available in Cisco ACI.

You can configure the endpoint selector either through the Cisco Cloud APIC GUI or through the ACI Multi-Site Orchestrator GUI. There are slight differences in the options available between the two GUIs, but the general concept and overall procedures to add endpoint selectors is essentially the same between the two.

The procedures in this section describe how to set up the endpoint selectors using the ACI Multi-Site Orchestrator GUI. For information on setting up the endpoint selectors using the Cisco Cloud APIC GUI, see the *Cisco Cloud APIC User Guide, Release 4.2(x)*.

Step 1 Gather the necessary information from the Azure site that you could use for your Cisco Cloud APIC endpoint selector.

  Note These steps assume that you are configuring the instance in Azure first, then adding an endpoint selector for Cisco Cloud APIC afterward; however, you can also add an endpoint selector in Cisco Cloud APIC first, then perform this Azure instance configuration step afterward, at the end of these endpoint selector procedures.

Step 2 Log into the ACI Multi-Site Orchestrator, if you aren't already logged in.

Step 3   In the left pane, click **Schemas**, then select the schema that you created earlier.

Step 4   Determine how you want to create the endpoint selector.

- If you want to create an endpoint selector that could be applied to any additional cloud site in the future, follow these procedures:

  a.   In the left pane, leave the template selected.

  Do not select a specific site for these procedures.

  b.   In the middle pane, select the EPG that you created for the cloud site.

  c.   In the right pane, in the **CLOUD PROPERITES** area, click + next to **SELECTORS** to configure the endpoint selector.

  d.   In the **Add New End Point Selector** dialog, enter a name in the **END POINT SELECTOR NAME** field, based on the classification that you use for this endpoint selector.

  e.   Click + **Expression**, then select the type of endpoint selector.

  For an endpoint selector created this way, the only option available under the Key field is `EPG`.

  f.   Go to Step 5, on page 69.

- If you want to create an endpoint selector specifically for this cloud site, follow these procedures:

  a.   In the left pane, select the cloud site.

  b.   In the middle pane, select the EPG that you created for the cloud site.

  c.   In the right pane, in the **SITE LOCAL PROPERITES** area, under the **SELECTORS** area, click + next to **SELECTOR** to configure the endpoint selector.

  d.   In the **Add New End Point Selector** dialog, enter a name in the **END POINT SELECTOR NAME** field, based on the classification that you use for this endpoint selector.

  For example, for an endpoint selector with the IP Subnet classification, you might use a name such as `IP-Subnet-EPSelector`.

  e.   Click + **Expression**, then select the key that you want to use for the endpoint selector.

  - **IP Address**: Used to select by the IP address or subnet. The value for an IP address as an endpoint selector should fall under the user subnet created under the CIDR in Adding Sites to the Schema, on page 66.

    In addition, specifically for Azure scale set VMs, the value for an IP address as an endpoint selector must be a complete subnet that was configured in Adding Sites to the Schema, on page 66 where that scale set resides. It cannot be an IP address within the subnet.

    For example, if you used the following values in these fields for Azure scale set VMs:

    - **CIDR**: `10.1.0.0/16`

    - **Subnet**: `10.1.0.0/24`

    Then a valid value for an IP address as an endpoint selector would be `10.1.0.0/24`. Entries of `10.1.0.1/32` or `10.1.0.0/16` would not be valid values for an IP address as an endpoint for Azure scale set VMs.

  - **Region**: Used to select by the Azure region of the endpoint.

       • If you want to create a custom tag for the endpoint selector, start typing in the **Type to search or create field** to enter the custom tag or label, then click **Create** on the new field to create a new custom tab or label.

       Using the example earlier in these procedures when you were adding a tag in Azure, you might create the custom tag `Location` in this field, to match the Location tag that you added in Azure earlier.

Step 5   In the **Operator** field, choose the operator that you want to use for the endpoint selector.

The options are:

      • **Equals**: Used when you have a single value in the Value field.

      • **Not Equals**: Used when you have a single value in the Value field.

      • **In**: Used when you have multiple comma-separated values in the Value field.

      • **Not In**: Used when you have multiple comma-separated values in the Value field.

      • **Has Key**: Used if the expression contains only a key.

      • **Does Not Have Key**: Used if the expression contains only a key.

Step 6   In the **Value** field, choose which value that you want to use for the endpoint selector, based on the choices that you made for the two previous fields. You can have multiple comma-separated entries in the **Value** field, where a logical OR exists between the entries in this field.

    Note   The Value field is not displayed if **Has Key** or **Key Not Exist** is selected for the Operator field.

For example, if you want to have a specific Azure region for the endpoint selector, such as `westus`, you might make the following selections in this screen:

      • **Key:** Region

      • **Operator:** Equals

      • **Value:** westus

As another example, assume that you used the following values in these fields:

      • **Key:** IP

      • **Operator:** Has Key

      • **Value:** Not available because Has Key was used in the Operator field.

The EPG rules will be applied to all endpoints with an IP address in this situation.

As a final example, assume that you used the following values in these fields:

      • **Key:** custom tag: Location

      • **Operator:** Has Key

      • **Value:** Not available because Has Key was used in the Operator field.

In this situation, the EPG rules will be applied to all endpoints with the Azure tag key Location, regardless of the location value.

Step 7   Click the checkmark when you have finished creating this endpoint selector expression.

Step 8   Determine if you want to create additional endpoint selector expressions.

If you create more than one expression under a single endpoint selector, a logical AND exists between those expressions. For example, assume you created two sets of expressions under a single endpoint selector:

- Endpoint selector 1, expression 1:

    - **Key:** Region

    - **Operator:** Equals

    - **Value:** eastus

- Endpoint selector 1, expression 2:

    - **Key:** IP

    - **Operator:** Equals

    - **Value:** 192.0.2.1/24

In this case, if *both* of these expressions are true (if the region is eastus AND if the IP address belongs to subnet 192.0.2.1/24), then that endpoint will be assigned to the Cloud EPG.

Click the checkmark after every additional expression that you want to create under this endpoint selector.

Step 9   When you have finished creating the expressions for this endpoint selector, click **SAVE** in the lower right corner of the **Add New End Point Selector**.

If you create more than one endpoint selector under an EPG, a logical OR exists between those endpoint selectors. For example, assume you had created endpoint selector 1 as described in the previous step, and then you created a second endpoint selector as described below:

- Endpoint selector 2, expression 1:

    - **Key:** Region

    - **Operator:** In

    - **Value:** centralus, eastus2

In this case:

- If the region is eastus AND the IP address belongs to the 192.0.2.1/24 subnet (endpoint selector 1 expressions)

    OR

- If the region is either centralus or eastus2 (endpoint selector 2 expression)

Then that end point is assigned to the Cloud EPG.

Step 10   When you have finished creating the endpoint selectors, click **SAVE** in the upper right corner.

Step 11   Click on the **DEPLOY TO SITES** button at the top right corner of the screen to deploy the schema to the sites.

You should see a message saying `Successfully Deployed` at this point.

What to do next

Verify that the Cisco ACI Multi-Site areas were configured correctly using the instructions in .

Verifying the Cisco ACI Multi-Site Configurations

Use the procedures in this topic to verify that the configurations that you entered in the ACI Multi-Site Orchestrator are applied correctly.

Step 1 Log into the Cloud APIC and verify the following:

a) Click on Dashboard and use the information in the Inter-Site Connectivity Status and the Inter-Region Connectivity Status boxes to verify the following:

- That the tunnels are up from the Cisco Cloud Services Router 1000V on Azure to the ISN (IPsec termination point) on-premises and to the VGWs in the user VNETs.

- That the OSPF neighbors are coming up between the Cisco Cloud Services Router and the ISN on-premises devices.

- That the BGP EVPN routes for the VRF show the cloud and on-premises routes, and that the cloud routes are populated through the BGP EVPN in the ACI spine switch.

b) Click on Application Management → Tenants and verify that the tenants were configured correctly.

c) Click on Application Management → Application Profiles and verify that the application profiles were configured correctly.

d) Click on Application Management → EPGs and verify that the EPGs were configured correctly.

e) Click on Application Management → Contracts and verify that the contracts were configured correctly.

f) Click on Application Management → VRFs and verify that the VRFs were configured correctly.

g) Click on Application Management → Cloud Context Profiles and verify that the cloud context profiles were configured correctly.

h) Click on Cloud Resources → Regions and verify that the regions were configured correctly.

i) Click on Cloud Resources → VNETs and verify that the VNETs were configured correctly.

j) Click on Cloud Resources → Cloud Endpoints and verify that the cloud endpoints were configured correctly.

k) Click on Cloud Resources → Routers and verify that the CSRs were configured correctly.

Step 2 Log into on-premises APIC site and verify the schema in APIC.

You should see the shared tenant that you configured in the ACI Multi-Site Orchestrator is displayed in the tenants area in APIC and the VRF and EPG deployed from the ACI Multi-Site Orchestrator schema is configured in the on-premises APIC.

Step 3 From a command line, verify that the VRFs were created properly on the Cisco Cloud Services Router 1000V on Azure:

```
show vrf
```

If the tenant `t1` and the VRF `v1` is deployed from the ACI Multi-Site Orchestrator, the CSR output will be similar to the following:

```
Name                      Default RD        Protocols   Interfaces
```

```
t1:v1                                 64514:3080192         ipv4        BD1
                                                                        Tu4
                                                                        Tu5
```

Step 4   From a command line, verify that the tunnels are up between the Cisco Cloud Services Router 1000V on Azure and the ISN on-premises devices.

You can run the following command on either the Cisco Cloud Services Router 1000V on Azure or on the ISN on-premises devices.

show ip interface brief | inc Tunnel

Output similar to the following should appear:

```
Interface       IP-Address      OK?      Method        Status        Protocol
Tunnel1         1.2.3.22        YES      manual        up            up
Tunnel2         1.2.3.30        YES      manual        up            up
Tunnel3         1.2.3.6         YES      manual        up            up
Tunnel4         1.2.3.14        YES      manual        up            up
```

Step 5   From a command line, verify that the OSPF neighbors are up between the Cisco Cloud Services Router 1000V on Azure and the ISN on-premises devices:

show ip ospf neighbor

Output similar to the following should appear:

```
Neighbor ID     Pri               State      Dead Time     Address       Interface
10.200.10.201   0                 FULL/ -    00:00:36      1.2.3.13      Tunnel4
20.30.40.50     0                 FULL/ -    00:00:36      1.2.3.29      Tunnel2
10.202.101.202  0                 FULL/ -    00:00:38      1.2.3.5       Tunnel3
```

Step 6   From a command line, verify that the on-premises BGP EVPN neighbors are present in the Cisco Cloud Services Router 1000V:

show bgp l2vpn evpn summary

Output similar to the following should appear:

```
Neighbor    V     AS    MsgRcvd    MsgSent    TblVer    InQ    OutQ    Up/Down    State/PfxRcd
10.1.1.2    4     100   139        137        99        0      0       01:30:36   6
```

Step 7   From a command line, verify that the BGP routes for the VRF show both the cloud and on-premises routes.

Note   In the current Cloud APIC workflow, a VRF will not be configured on the Cisco Cloud Services Router 1000V until the corresponding VNET is created in Azure.

show ip route vrf t1:v1

Output similar to the following should appear:

```
B     129.1.1.5/32[20/0] via 10.11.0.34, 01:12:41, BD|1
B     130.1.0.0/16[20/100] via 131.254.4.5, 01:09:55
```

CHAPTER 7

Understanding the Cisco Cloud APIC GUI

Navigating the Cisco Cloud APIC GUI

After you install Cisco Cloud APIC, you can use it for extending Cisco Application Centric Infrastructure (ACI) policy to the Amazon Web Services (AWS) or Microsoft Azure public cloud. You do so through the Cisco Cloud APIC GUI.

In the Cisco Cloud APIC GUI, you can create a tenant, configure application profiles, endpoint groups (EPGs), contracts, filters, and VRFs. You can also view Cisco Cloud APIC topology, configurations, and resources.

You perform configuration steps with the. **Intent** feature. For instructions on using the **Intent** feature, see the section Configuring Cisco Cloud APIC Components, on page 73. Also see the section "Understanding the Cisco Cloud APIC GUI Icons" in the *Cisco Cloud APIC User Guide*.

The steps for performing basic tasks in Cisco Cloud APIC differ from the steps in regular Cisco APIC. However, the functions of the tenant, application profile, and other elements of Cisco APIC are the same. For more information, see the *Cisco Application Centric Infrastructure Fundamentals Guide* on Cisco.com.

You view configurations and other information with the left navigation pane. You can choose **Dashboard** (the default view), **Topology**, **Application Management**, **Cloud Resources**, **Operations**, **Infrastructure**, and **Administrative**.

For information abut the icons, see the section "Understanding the Cisco Cloud APIC GUI Icons" in the *Cisco Cisco Cloud APIC User Guide* on Cisco.com.

Creating a Tenant Using the Cisco Cloud APIC GUI

The following sections describe how to create a tenant using the Cisco Cloud APIC GUI.

Configuring Cisco Cloud APIC Components

This section provides an overview of performing key tasks in Cisco Cloud APIC, including creating a tenant, application profile, and endpoint group (EPG).

Before you begin

You must have installed Cisco Cloud APIC. See the previous installation sections in this guide.

Step 1   Log into Cisco Cloud APIC.

Step 2   At the upper right of the **Dashboard** pane, click the icon with an arrow pointing to a bull's-eye.

This icon might be referred to as the **Intent** icon or feature.

Step 3   In the **What do you want to do?** window, type a term in the search window to bring up a list of options.

For example, if you want to configure a tenant, type the word tenant in the search window. The search returns a list of tasks that are related to creating and configuring tenants.

Step 4   Click a task and perform the configuration steps in the windows that open.

What to do next

You can view the configuration in the left navigation pane. Expand the pane by clicking the hamburger icon at the upper left of the **Dashboard** pane. Expand the appropriate heading to view the configurations.

For example, if you've configured a tenant, expand **Application Management** and click **Tenants**. Information about tenants appears in the central work pane.

Performing a System Upgrade, Downgrade or Recovery

Upgrading the Software

The method that you use to upgrade your Cisco Cloud APIC software varies, depending on the situation:

- If you are upgrading from a pre-5.0(1) release to Release 5.0(2), you will use a migration-based process to upgrade your software. Go to Migration-Based Upgrade, on page 76 for those instructions.

  Note The same migration-based procedures used for an upgrade can also be used for a system recovery, as described in Performing a System Recovery, on page 95.

- If you are upgrading from Release 5.0(1) to Release 5.0(2), you will use a policy-based process to upgrade your software. Go to Policy-Based Upgrade, on page 89 for those instructions.

  Note If the policy-based upgrade from Release 5.0(1) to Release 5.0(2) does not work for some reason, you can upgrade from Release 5.0(1) to Release 5.0(2) using the migration-based process as described in Migration-Based Upgrade, on page 76.

Guidelines and Limitations For Upgrading the Software

Following are the guidelines and limitations that you must be aware of before upgrading the Cisco Cloud APIC software:

Beginning with release 5.0(2), the configuration drift feature became available as described in the "Configuration Drifts" chapter in the Cisco Cloud APIC for Azure User Guide, Release 5.0(x) or later. After you upgrade your Cisco Cloud APIC, if you had configuration drifts enabled prior to the upgrade, you will see that the configuration drift feature is restarted after the upgrade is completed. When the feature is restarted, the previous configuration drift analysis is cleared (no configuration drifts are shown after the upgrade) and a fresh analysis is started for the configuration drift when the feature is restarted after the upgrade. This is expected behavior.

Migration-Based Upgrade

Follow these procedures if you are upgrading from Release 4.2(4) or earlier to Release 5.0(2), where you will use a migration-based process to upgrade your software.

> ✎
>
> **Note**   These migration-based procedures used for an upgrade can also be used for a system recovery, as described in Performing a System Recovery, on page 95.

Gathering Existing Cloud APIC Configuration Information

Before upgrading your Cisco Cloud APIC software, follow the instructions in this topic to locate the existing configuration information for certain fields and make a note of the entries for each of these fields. You will use the same entries for these fields below, in a step later in the following procedures, when you use the Release 5.0(2) recovery template to upgrade your Cisco Cloud APIC.

For each of the following fields, make a note of the entries that you entered as part of the original deployment that you performed in Deploying the Cloud APIC in Azure, on page 28:

- Subscription, on page 76
- Resource Group, on page 77
- Location, on page 77
- Fabric Name, on page 77
- External Subnets, on page 78
- Virtual Machine Name, on page 78
- Infra VNET Pool, on page 78
- Storage Account Name, on page 79

Subscription

1. Navigate to **Application Management** > **Tenants**.

2. Locate the row for the tenant that has **infra** underneath the name in the **Name** column.

3. Note the value in the **Azure Subscription** column.

   This is the **Subscription** entry for your Cisco Cloud APIC.

Resource Group

1. Navigate to **Cloud Resources** > **Virtual Machines**.

   The **Virtual Machines** window appears.

2. Locate and note the Cisco Cloud APIC VM in the VM list.

   The value for the VM is typically shown with the format *<vm_name>*(*<resource_group>*), where:

   - *<vm_name>* is the virtual machine name, as described in .

   - (*<resource_group>*) is the **Resource Group** entry for your Cisco Cloud APIC.

Location

1. Navigate to **Cloud Resources** > **Virtual Machines**.

   The **Virtual Machines** window appears.

2. Locate the Cisco Cloud APIC VM in the VM list.

3. Click the value for the Cisco Cloud APIC VM in the VM list.

   A nav panel with details about the Cisco Cloud APIC VM slides in from the right side of the screen.

4. In the **General** area, locate and note the value in the **Region** field.

   This is the **Location** entry for your Cisco Cloud APIC.

Fabric Name

1. SSH to your Cisco Cloud APIC through the CLI:

   ```
   # ssh admin@<cloud_apic_ip_address>
   ```

   Enter the password if prompted.

2. Enter the following in the CLI:

   ```
   ACI-Cloud-Fabric-1# acidiag avread
   ```

3. Locate the **FABRIC_DOMAIN** area in the output:

```
Local appliance ID=1 ADDRESS=10.100.0.13 TEP ADDRESS=10.100.0.12/30 ROUTABLE IP
ADDRESS=0.0.0.0
CHASSIS_ID=afe36d66-042a-11eb-ab21-7b2dc494b182

Cluster of 1 lm(t):1(zeroTime) appliances (out of targeted 1
lm(t):1(2020-10-01T21:15:48.743+00:00))
with FABRIC_DOMAIN name=ACI-Cloud-Fabric set to version=5.0(2i)
lm(t):1(2020-10-01T21:15:48.746+00:00);
discoveryMode=PERMISSIVE lm(t):0(zeroTime); drrMode=OFF lm(t):0(zeroTime); kafkaMode=OFF
 lm(t):0(zeroTime)

appliance id=1 address=10.100.0.13 lm(t):1(2020-10-01T21:14:23.001+00:00) tep
address=10.100.0.12/30
lm(t):1(2020-10-01T21:14:23.001+00:00) routable address=0.0.0.0 lm(t):1(zeroTime)
oob address=10.100.0.29/28 lm(t):1(2020-10-01T21:14:26.723+00:00) version=5.0(2i)
lm(t):1(2020-10-01T21:14:26.841+00:00) chassisId=afe36d66-042a-11eb-ab21-7b2dc494b182
lm(t):1(2020-10-01T21:14:26.841+00:00) capabilities=0X7EEFFFFFFFFF--0X2020--0X1
lm(t):1(2020-10-01T21:20:27.483+00:00) rK=(stable,present,0X206173722D687373)
```

```
lm(t):1(2020-10-01T21:14:26.728+00:00) aK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) oobrK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) oobaK=(stable,present,0X206173722D687373)
lm(t):1(2020-10-01T21:14:26.728+00:00) cntrlSbst=(APPROVED, E8E6DDB1D800)
lm(t):1(2020-10-01T21:14:26.841+00:00) (targetMbSn= lm(t):0(zeroTime),
failoverStatus=0 lm(t):0(zeroTime)) podId=1 lm(t):1(2020-10-01T21:14:23.001+00:00)
commissioned=YES lm(t):1(zeroTime) registered=YES lm(t):1(2020-10-01T21:14:23.001+00:00)

standby=NO lm(t):1(2020-10-01T21:14:23.001+00:00) DRR=NO lm(t):0(zeroTime) apicX=NO
lm(t):1(2020-10-01T21:14:23.001+00:00) virtual=YES lm(t):1(2020-10-01T21:14:23.001+00:00)

active=YES(2020-10-01T21:14:23.001+00:00) health=(applnc:255
lm(t):1(2020-10-01T21:16:16.514+00:00) svc's)
-------------------------------------------
clusterTime=<diff=-1 common=2020-10-02T07:46:19.717+00:00
local=2020-10-02T07:46:19.718+00:00
pF=<displForm=0 offsSt=0 offsVlu=0 lm(t):1(2020-10-01T21:15:50.026+00:00)>>
-------------------------------------------
```

This is the **Fabric Name** entry for your Cisco Cloud APIC.

External Subnets

1. Navigate to **Application Management** > **EPGs**.

2. Locate the EPG with the name **ext-networks** and click that EPG.

   A nav panel slides in from the right side of the screen.

3. In the nav panel, click the **Details** icon (⬀).

   The **Overview** page for this EPG appears.

4. In the **Endpoints** area, locate the row for **ext-Network1** and note the value in the **Subnet** column.

   This is the **External Subnets** entry for your Cisco Cloud APIC. Note that a value of 0.0.0.0/0 meant that anyone is allowed to connect to your Cisco Cloud APIC.

Virtual Machine Name

1. Navigate to **Cloud Resources** > **Virtual Machines**.

   The **Virtual Machines** window appears.

2. Locate and note the value for the Cisco Cloud APIC VM in the list.

   The value for the VM is typically shown with the format *<vm_name>*(*<resource_group>*), where:

   - *<vm_name>* is the **Virtual Machine Name** entry for your Cisco Cloud APIC.

   - (*<resource_group>*) is the resource group, as described in Resource Group, on page 77.

Infra VNET Pool

For the infra VNET pool, you might have multiple infra subnet pools, so be sure to locate the information for the infra subnet that was used when you launched the original Cisco Cloud APIC through the ARM template as part of the procedures in Deploying the Cloud APIC in Azure, on page 28.

1. In your Cisco Cloud APIC GUI, click the Intent icon (🅟) and choose **cAPIC Setup**.

2. In the Region Management area, click **Edit Configuration**.

   The **Regions to Manage** window appears.

3. Click **Next**.

   The **General Connectivity** window appears.

4. In the **Subnet Pools for Cloud Routers** area underneath **General**, locate the row that has a **System Internal** value in the **Created By** column and note the value in the **Subnet** column.

   This is the **Infra VNET Pool** entry for your Cisco Cloud APIC.

Storage Account Name

Navigate to the **Storage accounts** page in Azure under the resource group where the Cisco Cloud APIC was deployed previously:

1. Log into your Azure account for the Cloud APIC infra tenant and go to the Azure management portal, if you are not there already:

   https://portal.azure.com/#home

2. Under **Services**, select **Storage accounts**.

   The **Storage accounts** page appears.

3. Locate and note the storage account name for your Cisco Cloud APIC resource group.

   This is the **Storage Account Name** entry for your Cisco Cloud APIC.

What to do next

Follow the procedures in .

Performing Pre-Upgrade Procedures

Before you begin

Complete the procedures in before proceeding with these procedures.

Step 1   Enable the encrypted passphrase control, if it is not enabled already.

a) In your Cisco Cloud APIC GUI, navigate to **Infrastructure** > **System Configuration**.

   It should be underneath the **General** tab by default; if not, click the **General** tab.

b) Determine if the encrypted passphrase control is enabled already.

   - In the **Global AES Encryption** area, if you see **Yes** underneath the **Encryption** and **Key Configured** fields, then you have the encrypted passphrase control enabled already. Go to .

   - If you do not see **Yes** underneath the **Encryption** and **Key Configured** fields:

   1. Click the pencil icon at the upper right part of the **Global AES Encryption** area.

The **Global AES Encryption Settings** window appears.

2. Click the box next to the **Encryption: Enabled** area, enter a passphrase in the **Passphrase/Confirm Passphrase** fields, then click **Save** at the bottom of the window.

   Make a note of the passphrase that you entered in this step, as you will need it in a step later in the following procedures.

Step 2   Back up your existing Cisco Cloud APIC configuration.

There are a number of different ways that you can back up your Cisco Cloud APIC configuration. See the *Cloud APIC for Azure Users Guide* for more information. Note that if you want to use a remote backup, you will also need to add a remote location first.

Step 3   If you have non-home region CSRs in your deployment, remove the CSRs from all regions *except the home region*.

Note   You do not have to perform the procedures in this step if you do not have non-home region CSRs in your deployment. Skip to in that case.

a) In your Cisco Cloud APIC GUI, click the Intent icon (🔵) and choose **cAPIC Setup**.
b) In the Region Management area, click **Edit Configuration**.

   The **Regions to Manage** window appears.

c) Make a note of the regions that have boxes selected in the **Cloud Routers** column.

   You will be unselecting the boxes in the **Cloud Routers** column in the next step. When you restore the backed-up configuration later in these procedures, these same cloud router selections should be selected automatically. However, you can use the list that you note in this step if you want to verify that the same cloud routers were correctly selected.

d) Unselect (remove checks from boxes) in the **Cloud Routers** column for every region in the window except for the home region (the region that has the text **Cloud APIC Deployed**).

e) Click **Next**, then enter the necessary information in the following page and click **Save and Continue**.

   After you click **Save and Continue**, wait until the following changes to take place:

   • All of the non-home region CSR virtual machines are deleted from the Azure portal

   • All of the public IP addresses for the CSR interfaces are deleted from the Azure portal

   • All of the **Network interfaces** assigned to these virtual machines are deleted from the Azure portal

   The process of removing the CSRs might take roughly a half hour. You can monitor the process of the CSR removal by looking at the virtual machines for the infra resource group in the Azure portal.

Step 4   Delete the Cisco Cloud APIC VM.

a) In the Microsoft Azure portal, navigate to **Services** > **Virtual Machines**.
b) Locate the Cisco Cloud APIC VM in the **Virtual Machines** window and click on the Cloud APIC VM.

   The **Overview** page for the Cisco Cloud APIC VM appears.

c) Click **Delete**, then click **Yes** when asked for confirmation of this action.

   You can view the deletion process in the Notifications area.

What to do next

Follow the procedures in Downloading and Deploying the Recovery Template, on page 81.

Downloading and Deploying the Recovery Template

Before you begin

Complete the procedures in Performing Pre-Upgrade Procedures, on page 79 before proceeding with these procedures.

Step 1 Download the Release 5.0(2) recovery template for Cisco Cloud APIC.

a) Go to the Cisco Software Download site for Cisco Cloud APIC and select the latest release, if it is not selected already:

https://software.cisco.com/download/home/286323635/type/286325191/release/

b) Locate the **Cloud ACI image for recovery template** entry and click the download icon to download the json file.

Accept the license agreement when prompted to initiate the download.

Step 2 Deploy the Release 5.0(2) recovery template in the Azure portal.

a) In the Azure portal, go to the **All Services** page:

https://portal.azure.com/#allservices

b) In the **General** area, click **Templates**.

c) In the **Templates** page, click Add.

The **Add Template** page appears.

d) Enter the necessary information in the **Add Template** page.

- **Name**: Enter a unique name that will identify this template as the Release 5.0(2) recovery template (for example, `template-502-recovery`).

- **Description**: Enter descriptive text for this template, if necessary.

e) Click **OK**.

The **ARM Template** page appears.

f) In the **ARM Template** page, delete the default text that is automatically added in the template.

g) Navigate to the area where you downloaded the Release 5.0(2) recovery template in Step 1, on page 81.

h) Using a text editor, open the Release 5.0(2) recovery template and copy the contents in the template.

i) In the Azure portal window, paste the contents into the **ARM Template** page.

j) Click **OK**.

The **Add Template** page appears again.

k) Click **Add**.

The new Release 5.0(2) recovery template is added to the **Templates** page. If you do not see the new Release 5.0(2) recovery template in the **Templates** page, click **Refresh** to refresh the page.

Step 3 Use the recovery template to deploy the Cisco Cloud APIC VM in the same resource group.

a) In the Templates page, click the new Release 5.0(2) recovery template that you just added.

b) Click **Deploy**.

 The **Custom Deployment** page appears.

c) Enter the necessary information in the recovery template.

- **Basics**:

    - **Subscription**: Choose the same subscription that you used when you first deployed your Cisco Cloud APIC, as described in Subscription, on page 76.

    - **Resource Group**: You must choose the same resource group that you used when you first deployed your Cisco Cloud APIC, as described in Resource Group, on page 77.

    - **Location**: Select the same region that you used when you first deployed your Cisco Cloud APIC, as described in Location, on page 77.

        Note   The **Location** option might not be available when you are using the same resource group.

- **Settings**:

    - **Vm Name**: Enter the same VM name that was used previously, as described in Virtual Machine Name, on page 78.

    - **Vm Size**: Select the size for the VM.

    - **Image Sku**: Select the `5_0_2_byol` image SKU.

    - **Admin Username**: Leave the default entry for this field as-is. The admin username login will work once the Cisco Cloud APIC is up.

    - **Admin Password or Key**: Enter an admin password.

    - **Admin Public Key**: Enter the admin public key (the ssh key).

    - **Fabric Name**: Enter the same fabric name that was used previously, as described in Fabric Name, on page 77.

    - **Infra VNET Pool**: Enter the same infra subnet pool that was used previously, as described in Infra VNET Pool, on page 78.

    - **External Subnets**: Enter the IP addresses and subnets of the external networks that were used previously to allow access to the Cisco Cloud APIC, as described in External Subnets, on page 78. This would be the same external subnet pool for Cisco Cloud APIC access that you entered as part of the original deployment that you performed in Deploying the Cloud APIC in Azure, on page 28.

    - **Storage Account Name**: Enter the same storage account name that was used previously, as described in Storage Account Name, on page 79.

    - **Virtual Network Name**: The name for the virtual network.

        - If you are performing an upgrade from Release 4.2(4) or 5.0(1) to Release 5.0(2), do not modify the values of these parameter. Leave the default value for the virtual network name as-is for this field.

        - If you are performing a recovery from 5.0(2), verify that the virtual network name in this field matches the virtual network name that was originally used to deploy the Cisco Cloud APIC.

    - **Mgmt Nsg Name**: The name for the management network security group.

- If you are performing a recovery or an upgrade from Release 4.2(4) or 5.0(1) to Release 5.0(2), do not modify the values of these parameter. Leave the default value for the management network security group name as-is for this field.

- If you are performing a recovery from 5.0(2), verify that the management network security group name in this field matches the management network security group name that was originally used to deploy the Cisco Cloud APIC.

- **Mgmt Asg Name**: The name for the management application security group.

  - If you are performing a recovery or an upgrade from Release 4.2(4) or 5.0(1) to Release 5.0(2), do not modify the values of these parameter. Leave the default value for the management application security group name as-is for this field.

  - If you are performing a recovery from 5.0(2), verify that the management application security group name in this field matches the management application security group name that was originally used to deploy the Cisco Cloud APIC.

- **Subnet Prefix**: The entry for this field will be the subnet prefix that needs to be used for the automatically-configured infra subnet.

  - If you are performing an upgrade from Release 4.2(4) or 5.0(1) to Release 5.0(2), do not modify the values of these parameter. Leave the default values as-is for this field.

  - If you are performing a recovery from 5.0(2), verify that the subnet prefix in this field matches the subnet prefix that was originally used to deploy the Cisco Cloud APIC. You can check that prefix by looking at the format of the subnet names on the Cisco Cloud APIC Virtual Network. For example, if subnet names shown there are **subnet-10.10.0.0_28**, then the subnet prefix for this field should be **subnet-**.

d) Click the box next to the agreement statement, then click **Purchase**.

The **Azure services** window appears, with a small popup window saying **Deployment in progress**. Click the Notifications icon to continue to monitor the progress of the deployment. The deployment usually takes roughly five or so minutes to complete.

After a period of time, you will see the **Deployment succeeded** window.

What to do next

Follow the procedures in .

Performing Post-Upgrade Procedures

Before you begin

Complete the procedures in before proceeding with these procedures.

Step 1 Give the contributor role to the Cisco Cloud APIC VM on the infra subscription.

a) In the Microsoft Azure portal, under **Services**, select **Subscription**.

b) Select the subscription where Cisco Cloud APIC was deployed.

c) Select **Access Control (IAM)**.

d) On the top menu, click **Add** > **Add role assignment**.

e) In the **Role** field, select **Contributor**.

f) In the **Assign access to** field, select **Virtual Machine**.

g) In the **Subscription** field, select the subscription where the Cisco Cloud APIC was deployed.

h) In **Select**, click on the Cisco Cloud APIC Virtual Machine.

i) Click **Save**.

> **Note**   Also give the contributor role to the Cisco Cloud APIC VM if you have managed user tenants. You must do this on user subscriptions that are used to deploy the user tenants. See About Tenants, on page 9 and Adding a Role Assignment for a Virtual Machine, on page 32 for more information.

Step 2   Enable the same encryption passphrase.

a) In the Microsoft Azure portal, under **Services**, select **Virtual machines**.

b) In the **Virtual machines** window, click the Cisco Cloud APIC.

The **Overview** page for the Cisco Cloud APIC appears.

c) Locate the **Public IP address** field and copy the IP address.

d) In another browser window, enter the IP address and hit Return:

`https://<IP_address>`

The **Welcome to Cloud APIC** screen appears after logging in for the first time.

e) Click **Begin First Time Setup**.

The **Let's Configure the Basics** window appears. Click the **X** in the upper right corner to exit out of this window to proceed with procedures to enable the same encryption passphrase.

f) In your Cisco Cloud APIC GUI, navigate to **Infrastructure** > **System Configuration**.

It should be underneath the **General** tab by default; if not, click the **General** tab.

After first login, welcome screen appears. Click begin first time setup.first time setup page opens, close the first time setup pagethen user can proceed to setting the pass phrase.

g) In the **Global AES Encryption** area, click the pencil icon at the upper right part of the **Global AES Encryption** area.

The **Global AES Encryption Settings** window appears.

h) Click the box next to the **Encryption: Enabled** area, enter the same passphrase in the **Passphrase/Confirm Passphrase** fields that you used in Step 1, on page 79 in Performing Pre-Upgrade Procedures, on page 79, then click **Save** at the bottom of the window.

Step 3   Import the configuration that you backed up in Step 2, on page 80 in Performing Pre-Upgrade Procedures, on page 79.

If you configured a remote location when you backed up your configuration, you might have to create the remote location again to access the backup.

a) In your Cisco Cloud APIC GUI, navigate to **Operations** > **Backup & Restore**.

b) In the **Backup & Restore** window, click the **Backups** tab.

c) Click the **Actions** scrolldown menu, then choose **Restore Configuration**.

The **Restore Configuration** window appears.

d) Enter the necessary information to restore the configuration that you backed up in in .

If you are upgrading from a 4.2(x) release to Release 5.0(x) or later, for this particular backup restore, use the following settings:

- In the **Restore Type** field, choose **Merge**.

- In the **Restore Mode** field, choose **Best Effort**.

Click **Restore Configuration** when you have entered the necessary information in this window.

e) Wait until the restore process is complete before proceeding to the next step.

Click the **Job Status** tab in the **Backup & Restore** window to get the status of the restore process and verify that the restore process was successful.

Step 4 Review the naming policy.

a) In your Cisco Cloud APIC GUI, click the Intent icon ( ) and choose **cAPIC Setup**.
b) In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

c) Verify that the selections that you had prior to the migration were transferred over successfully with the backup import, then click **Next**.

Note   Do not modify the managed region or CSR configuration at this point.

d) Navigate to the last page in the setup and review the information in the **Cloud Resource Naming Rules** area.

- If you are performing a recovery or an upgrade from Release 4.2(4) or 5.0(1) to Release 5.0(2), do not modify the default cloud resource naming rules. Leave the default cloud resource naming rules as-is in this case.

- If you are performing a recovery from 5.0(2), verify that the cloud resource naming rules match the cloud resource naming rules that were originally used to deploy the Cisco Cloud APIC.

Click the box next to **Deploy cloud resources based on these naming rules**, then click **Save and Continue** after reviewing the information in this screen. Resources will not be deployed to the cloud until the naming rules have been reviewed and accepted.

At this point in the process, the non-home region CSRs will be deployed automatically with the new CSR image.

Note   Allow for some time to pass for the Cisco Cloud APIC to clear all of the faults before proceeding to the next step. See "Viewing Health Details Using the Cisco Cloud APIC GUI" in the *Cisco Cloud APIC for Azure User Guide* for more information.

Step 5 Wait for the non-home region CSRs to come up on the cloud, and ensure that all of the VGW tunnels are up with the newly-created CSRs and the configuration reconciliation is complete.

In addition, you may see that the home region CSR is deleted and recreated at this point in the process if a CSR upgrade is required. Ignore these actions and any faults that might appear as a result, as they will clear up when you complete the following steps in this procedure.

Wait until the home region CSRs are upgraded to the latest CSR version in this case. For example, for Release 5.0(2i), the latest CSR version would be 17_1.

Step 6 (Optional) If you have intersite connectivity and you want to avoid a complete intersite traffic drop, reconfigure the non-home region intersite tunnels and bring up the tunnels through the ACI Multi-Site Orchestrator before bringing down the home region CSRs in the next step.

This step is not necessary if you do not have intersite connectivity or if you have intersite connectivity but you're not concerned with traffic loss.

a) In the ACI Multi-Site Orchestrator, in the **Sites** screen, click **CONFIGURE INFRA**.

The **Fabric Connectivity Infra** page appears.

b) In the left pane, under **SITES**, click on the cloud site.
c) Click **Reload Site Data**.
d) Verify that the new CSRs are added in the UI.
e) Click the **Deploy** button at the top right of the screen, then choose the **Deploy & Download IPN Device config files** option.

This action pushes the configuration to both the on-premises APIC site and the Cloud APIC site and enables the end-to-end interconnect connectivity between the on-premises and the cloud site. In addition, this option downloads a zip file that contains configuration information that you will use to enable connectivity between the Cisco Cloud Services Router 1000V (CSR) deployed in Azure and the on-premises IPsec termination device. A followup screen appears that allows you to select all or some of the configuration files to download.

Note If you delete and recreate intersite tunnels on the cloud CSRs from the Cisco Cloud APIC in this step, and you need to program the new keys on the on-premises IPsec termination device, where you are going to change the key for the same public IP address of the cloud CSRs, you must first manually delete the existing keys on the on-premises IPsec termination device and add a new key. There should be only one matching IPsec pre-shared key for a given cloud CSR destination IP address on the on-premises IPsec termination device.

Step 7 Undeploy the home region CSRs.

Note If you are upgrading from 4.2(3) to 5.0(2), undeploying and redeploying the home region CSRs also migrates the CSR public IP SKU from the basic SKU to the standard SKU.

a) In your Cisco Cloud APIC GUI, click the Intent icon (🌀) and choose **cAPIC Setup**.
b) In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

c) Locate the home region (the region that has the text **Cloud APIC Deployed**) and unselect the boxes in the **Cloud Routers** column for the home region.
d) Click **Save**.

This removes the old CSRs for the home region.

e) Wait for home region CSR VMs, CSR NICs, and CSR public IP addresses to get deleted on the cloud.

Once the home region CSR VMs, CSR NICs, and CSR public IP addresses are deleted on the cloud, you can redeploy the CSRs back in the home region.

Step 8 Redeploy the home region CSRs.

The previously-configured home region CSRs are deleted and the new home region CSRs are re-created in this step.

a) Click **Previous** to return to the **Regions to Manage** screen, then click the boxes in the **Cloud Routers** column for the home region to re-enable the CSRs for the home region.

b) Click **Save**.

If you are upgrading from 4.2(3) to 5.0(2), this action migrates the CSR Public IP SKU to the standard SKU for the home region.

Step 9 (Optional) Complete the procedures in this step if intersite connectivity is required.

- If intersite connectivity is not required, then you do not have to complete the procedures in this step. Skip to Migrating to VNet Peering (Optional), on page 87 in that case.

- If intersite connectivity is required, then complete the following procedures:

a) Once the new home region CSRs come up, in the ACI Multi-Site Orchestrator, in the **Sites** screen, click **CONFIGURE INFRA**.

The **Fabric Connectivity Infra** page appears.

b) In the left pane, under **SITES**, click on the cloud site.
c) Click **Reload Site Data**.
d) Verify that the new CSRs are added in the UI.
e) Click the **Deploy** button at the top right of the screen, then choose the **Deploy & Download IPN Device config files** option.
f) Reconfigure the IPN IPsec tunnels on the on-premises CSR with the downloaded IPN configuration.

See Enabling Connectivity Between the Cisco Cloud APIC and the ISN Devices, on page 57.

Note If you delete and recreate intersite tunnels on the cloud CSRs from the Cisco Cloud APIC for any reason, and you need to program the new keys on the on-premises IPsec termination device, where you are going to change the key for the same public IP address of the cloud CSRs, you must first manually delete the existing keys on the on-premises IPsec termination device and add a new key. There should be only one matching IPsec pre-shared key for a given cloud CSR destination IP address on the on-premises IPsec termination device.

What to do next

If you want to migrate to Azure VNet peering for inter-VNet connectivity, follow the procedures in Migrating to VNet Peering (Optional), on page 87.

Migrating to VNet Peering (Optional)

Follow the procedures in this task if you want to migrate to Azure VNet peering for inter-VNet connectivity rather than using the traditionial tunnel-based VPN connectivity through the CSRs. For more information on the VNet peering feature, see the *Configuring VNet Peering for Cloud APIC for Azure* document.

Note Migrating to VNet peering mode is a disruptive operation. Be aware that there will be traffic loss during the process.

Before you begin

Complete the procedures in Performing Post-Upgrade Procedures, on page 83 before proceeding with these procedures.

Step 1   In your Cisco Cloud APIC GUI, click the Intent icon (🅐) and choose **cAPIC Setup**.

Step 2   In the **Region Management** area, click **Edit Configuration**.

The **Regions to Manage** window appears.

Step 3   Locate the **Connectivity for Internal Network** area and verify that the **Virtual Network Peering** is available.

Step 4   Click **Virtual Network Peering** to enable the Azure VNet peering feature.

This enables VNet peering at the Cisco Cloud APIC level, deploying NLBs in all the regions with CSRs in the infra VNet.

After you have enabled VNet peering at the Cisco Cloud APIC level, on each user cloud context profile, you will have to enable the **VNet Peering** option and disable the **VNet Gateway Router** option.

Note   The following steps describe now to enable VNet peering on each cloud context profile through the Cisco Cloud APIC GUI. You can also perform the following steps through the ACI Multi-Site Orchestrator, if you want.

Step 5   In the left navigation bar, navigate to **Application Management** > **Cloud Context Profiles**.

The existing cloud context profiles are displayed.

Step 6   Click Actions and choose **Create Cloud Context Profile**.

The **Create Cloud Context Profile** dialog box appears.

Step 7   Locate the **VNet Gateway Router** field and click to uncheck (disable) the **VNet Gateway Router** check box.

Step 8   Locate the **VNet Peering** field and click to check (enable) the **VNet Peering** check box.

Step 9   Click **Save** when finished.

Step 10   Configure the Network Contributor role for both the infra and user tenant subscriptions.

For example, assume the following:

- The infra tenant is using subscription **S1** with access credentials/service principal **C1**

- The user tenant is using subscription **S2** with access credentials/service principal **C2**

In this situation, you will have to configure the following for peering to work between the user tenant and the infra VNets:

- You will have to give C1 Network Contributor role permissions to S2 for the hub to spoke peering link

- You will have to give C2 Network Contributor role permissions to S1 for the spoke to hub peering link

a)   In the yellow window that appears, copy the **az** command provided.

- If you have configure the Network Contributor role for the user tenant, copy the text in the area **Command to run for User Subscription**.

- If you have configure the Network Contributor role for the infra tenant, copy the text in the area **Command to run for Infra Subscription**.

b) Return to the Azure management portal and click **Registrations** in the left navigation bar.

c) Open the Cloud Shell.

d) Select **Bash**.

e) Paste the **az** command that you copied in 10.a, on page 88.

Policy-Based Upgrade

Use the procedures in the following sections to perform a policy-based upgrade of your Cisco Cloud APIC software, if you are upgrading from Release 5.0(1) to Release 5.0(2).

Downloading an Image

Step 1 Log in to your Cisco Cloud APIC, if you aren't logged in already.

Step 2 From the **Navigation** menu, choose **Operations** > **Firmware Management**.

The **Firmware Management** window appears.

Step 3 Click the **Images** tab in the **Firmware Management** window.

Step 4 Click **Actions**, then choose **Add Firmware Image** from the scroll-down menu.

The **Add Firmware Image** pop-up appears.

Step 5 Determine if you want to add the firmware image from a local or a remote location.

- If you want to add the firmware image from a *local* location, click the **Local** radio button in the **Image Location** field. Click the **Choose File** button, then navigate to the folder on your local system with the firmware image that you want to import and select the file. Go to Step 6, on page 90.

- If you want to import the firmware image from a *remote* location, click the **Remote** radio button in the **Image Location** field, then perform the following actions:

a) In the **Protocol** field, click either the **HTTP** or the **SCP** radio button.

b) In the **URL** field, enter the URL from where the image will be downloaded.

- If you selected the **HTTP** radio button in the previous step, enter the http source that you want to use to download the software image. An example URL is
`10.67.82.87:/home/<username>/ACI/aci-apic-dk9.1.0.2j.iso`. Go to Step 6, on page 90.

- If you selected the **SCP** radio button in the previous step, enter the Secure Copy Protocol (SCP) source that you want to use to download the software image, using the format `<SCP server>:/<path>`. An example URL is `10.67.82.87:/home/<username>/ACI/aci-apic-dk9.1.0.2j.iso`.

c) In the **Username** field, enter your username for secure copy.

d) In the **Authentication Type** field, select the type of authentication for the download. The type can be:

- **Password**

- **SSH Key**

The default is **Password**.

e) If you selected **Password**, in the **Password** field, enter your password for secure copy. Go to Step 6, on page 90.

f) If you selected **SSH Key**, enter the following information:

- **SSH Key Content** — The SSH Key Content is used to create the SSH Key File which is required when creating a Remote location for the download.

   Note   The public key is generated at the time of the transfer. After the transfer the key files that were generated in the background are deleted. The temporary key files are stored in dataexport directory of the Cisco Cloud APIC.

- **SSH Key Passphrase** — The SSH Key Passphrase is used to create the SSH Key File which is required when creating a Remote location for the download.

   Note   The Passphrase field can remain empty.

Step 6   Click **Select**.
Wait for the Cisco Cloud APIC firmware images to download.

Upgrading the Software Using the Policy-Based Upgrade Process

Use the procedures in the following sections to perform a policy-based upgrade of your Cisco Cloud APIC software, if you are upgrading from Release 5.0(1) to Release 5.0(2).

Before you begin

- You have downloaded an image using the procedures provided in Downloading an Image, on page 89.

Step 1   Subscribe to the 17.1 image for the Cisco Cloud Services Router (CSR) 1000V - Bring Your Own License (BYOL) for Release 5.0(2).

a) In the Azure Marketplace search text field, type *Cisco Cloud Services Router (CSR) 1000V* and select the option that appears.

The **Cisco Cloud Services Router (CSR) 1000V** option appears as a search suggestion.

b) Click the **Cisco Cloud Services Router (CSR) 1000V** option.

You should be redirected to the **Cisco Cloud Services Router (CSR) 1000V** page in the Microsoft Azure Marketplace.

c) Locate the **Select a software plan** drop-down menu.

If you do not see the **Select a software plan** drop-down menu in the main page, you might have to click the **Plans + Pricing** tab, if that option is available, to access the **Select a software plan** drop-down menu.

d) In the **Select a software plan** drop-down menu, select the **Cisco CSR 1000V Bring Your Own License - XE 17.1** option.

e) Locate the **Want to deploy programmability?** field and click **Get Started**.

f) In the **Configure Programmability Deployment** page, scroll down to your subscription and, in the Status column, change the status from **Disable** to **Enable** for your subscription.

g) Click **Save**.

Step 2   Remove the CSRs from all regions *except the home region*.

Note	Do not remove the CSR from the home region at this point. Removing the CSR for the home region at this point will cause an outage.

a) In your Cloud APIC GUI, click the Intent icon ( ) and choose **cAPIC Setup**.

b) In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

c) Make a note of the regions that have boxes selected in the **Cloud Routers** column.

You will be unselecting the boxes in the **Cloud Routers** column in the next step, so make sure you know which regions will need to selected again at the end of this procedure.

d) Unselect (remove checks from boxes) in the **Cloud Routers** column for every region in the window except for the home region (the region that has the text **Cloud APIC Deployed**).

e) Click **Next**, then enter the necessary information in the following page and click **Save and Continue**.

The process of removing the CSRs might take roughly a half hour. You can monitor the process of the CSR removal by looking at the virtual machines for the resource group in the Azure portal.

Step 3 When the necessary CSRs have been completely removed, from the **Navigation** menu, choose the **Operations** > **Firmware Management**.

The **Firmware Management** window appears.

Step 4 Click **Schedule Upgrade**.

The **Schedule Upgrade** pop-up appears.

If you see a message that says that faults are present in your fabric, we recommend that you resolve these faults before performing a upgrade. See "Viewing Health Details Using the Cisco Cloud APIC GUI" in the *Cisco Cloud APIC for Azure User Guide* for more information.

Step 5 In the **Target Firmware** field, choose a firmware image from the scroll-down menu.

Step 6 In the **Upgrade Start Time** field, determine if you want to begin the upgrade now or later.

- Click **Now** if you want to schedule the upgrade for now. Go to Step 7, on page 91.

- Click **Later** if you want to schedule the upgrade for a later date or time, then select the date and time from the pop-up calendar for the scheduled upgrade.

Step 7 In the **Ignore Compatibility Check** field, leave the setting in the default off (unchecked) setting, unless you are specifically told to disable the compatibility check feature.

In Cloud APIC, there is a compatibility check feature that verifies if an upgrade path from the currently-running version of the system to a specific newer version is supported or not. The **Ignore Compatibility Check** setting is set to off by default, so the system automatically checks the compatibility for possible upgrades by default.

Note	If you choose to disable the compatibility check feature by entering a check mark in the box next to the **Ignore Compatibility Check** field, you run the risk of making an unsupported upgrade to your system, which could result in your system going to an unavailable state.

Step 8 Click **Schedule Upgrade**.

You can monitor the progress of the upgrade in the main **Firmware Management** window, under the **Upgrade Status** area.

Step 9 When the upgrade is completed, add the necessary CSRs back again.

Verify that the home region CSR is stabilized before adding the CSRs in the other regions back again.

a) In your Cloud APIC GUI, click the Intent icon (⊚) and choose **cAPIC Setup**.
b) In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

c) Locate all of the regions that had CSRs and check the boxes in the **Cloud Routers** column for each of those regions to add the CSRs back again.
d) Click Next, then enter the necessary information in the following page and click **Save and Continue**.

Step 10 Determine if you want to migrate to Azure VNet peering for inter-VNet connectivity rather than using the traditionial tunnel-based VPN connectivity through the CSRs.

For more information on the VNet peering feature, see the *Configuring VNet Peering for Cloud APIC for Azure* document.

Note Migrating to VNet peering mode is a disruptive operation. Be aware that there will be traffic loss during the process.

Follow these instructions to enable the VNet peering feature:

a) In your Cloud APIC GUI, click the Intent icon (⊚) and choose **cAPIC Setup**.
b) In the **Region Management** area, click **Edit Configuration**.

The **Regions to Manage** window appears.

c) Locate the **Connectivity for Internal Network** area and verify that the **Virtual Network Peering** is available.

- If the **Virtual Network Peering** is available, then the home region CSR has already been successfully migrated from the basic SKU to the standard SKU. Go to in this case.

- If the **Virtual Network Peering** is not available, that means that the home region CSR is still set to the basic SKU rather than the updated standard SKU. Continue to to migrate the home region CSR to the standard SKU.

d) Locate the home region (the region that has the text **Cloud APIC Deployed**) and unselect the box in the **Cloud Routers** column for the home region.
e) Click **Save**.

This action removes the CSR with the basic SKU for the home region.

f) Click **Previous** to return to the **Regions to Manage** screen, then click the box in the **Cloud Routers** column for the home region to re-enable the CSR for the home region.
g) Click **Save**.

This action adds the CSR with the standard SKU for the home region.

h) Click **Previous** to return to the **Regions to Manage** screen, then locate the **Connectivity for Internal Network** area and verify that the **Virtual Network Peering** is available.
i) Click **Virtual Network Peering** to enable the Azure VNet peering feature.

This enables VNet peering at the Cloud APIC level, deploying NLBs in all the regions with CSRs in the infra VNet.

Note The **VPN Connectivity via CSR** option is used to enable the traditional VPN connectivity through the overlay IPsec tunnels between CSRs and Azure VPN Gateway routers, instead of using VNet peering.

After you have enabled VNet peering at the Cloud APIC level, on each user cloud context profile, you will have to enable the **VNet Peering** option and disable the **VNet Gateway Router** option.

j) In the left navigation bar, navigate to **Application Management** > **Cloud Context Profiles**.

The existing cloud context profiles are displayed.

k) Click Actions and choose **Create Cloud Context Profile**.

The **Create Cloud Context Profile** dialog box appears.

l) Locate the **VNet Gateway Router** field and click to uncheck (disable) the **VNet Gateway Router** check box.

m) Locate the **VNet Peering** field and click to check (enable) the **VNet Peering** check box.

n) Click **Save** when finished.

Downgrading the Software

The following sections provide the necessary information that you will need to successfully downgrade your Cisco Cloud APIC software.

Downgrading the Software

Before you begin

The following prerequisites apply if you are downgrading from 5.0(2) to a release prior to 5.0(2):

- If your Cisco Cloud APIC has always been running on Release 5.0(2) [if you never upgraded from a release prior to 5.0(2) to Release 5.0(2)], then you cannot downgrade to a release prior to Release 5.0(2) on your Cisco Cloud APIC. Downgrading to a release prior to 5.0(2) when your Cisco Cloud APIC never ran on that prior release is not supported.

- If you upgraded your Cisco Cloud APIC to Release 5.0(2) and you completed certain Release 5.0(2)-specific configurations afterwards, such as VNet peering, and you want to downgrade to a release prior to Release 5.0(2), you will have to remove the CSRs from all the regions except the home region. Go to for those instructions.

- If you upgraded your Cisco Cloud APIC to Release 5.0(2) but you never completed any Release 5.0(2)-specific configurations afterwards, such as VNet peering, and you want to downgrade to a release prior to Release 5.0(2), you do not have to remove CSRs from any regions. Go to in that case.

Step 1 Remove the 5.0(2)-specific configurations before downgrading.

For example, to remove the VNet peering configurations, first disable Azure VNet peering at the local level, through the Cloud Context Profile:

a) Navigate to the **Create Cloud Context Profile** page:

Application Management > **Cloud Context Profiles**, then click **Actions** and choose **Create Cloud Context Profile**

    b) Double-click the cloud context profile where you want to disable VNet peeriing.

    c) Uncheck (disable) the **Hub Network Peering** field.

Then disable Azure VNet peering at the global level:

    a) In the Cloud APIC GUI, click the Intent icon (🅿) and select **cAPIC Setup**. In the **Region Management** area, click **Edit Configuration**.

    b) In the **Regions to Manage** screen, change the **Connectivity for Internal Network** setting from **Virtual Network Peering** to **VPN Connectivity via CSR**.

Step 2   Remove the CSRs from all regions except the home region.

    a) In your Cloud APIC GUI, click the Intent icon (the icon with an arrow pointing into several circles) and choose **cAPIC Setup**.

    b) In the Region Management area, click **Edit Configuration**.

       The **Regions to Manage** window appears.

    c) Make a note of the regions that have boxes selected in the **Cloud Routers** column.

       You will be unselecting the boxes in the **Cloud Routers** column in the next step, so make sure you know which regions will need to selected again at the end of this procedure.

    d) Unselect (remove checks from boxes) in the **Cloud Routers** column for every region in the window except for the home region (the region that has the text **Cloud APIC Deployed**).

    e) Click Next, then enter the necessary information in the following page and click **Save and Continue**.

       The process of removing the CSRs might take roughly a half hour.

Step 3   Verify that the necessary CSRs have been completely removed before proceeding.

    a) Click the Intent icon again and choose **cAPIC Setup**.

    b) In the Region Management area, click **Edit Configuration**.

       The **Regions to Manage** window appears.

    c) Locate the **Connectivity for Internal Network** area and wait for the **Virtual Network Peering** option to become available.

       If the **Virtual Network Peering** is not available, that means that the CSRs are still in the process of being deleted.

       Wait for the **Virtual Network Peering** option to become available before proceeding with the next step.

Step 4   Download an image for the downgrade using the procedures provided in .

Step 5   When the image is fully downloaded, from the **Navigation** menu, choose the **Operations** > **Firmware Management**.

       The **Firmware Management** window appears.

Step 6   Click **Schedule Upgrade**.

       The **Schedule Upgrade** pop-up appears.

       If you see a message that says that faults are present in your fabric, we recommend that you resolve these faults before performing a downgrade. See "Viewing Health Details Using the Cisco Cloud APIC GUI" in the *Cisco Cloud APIC for Azure User Guide* for more information.

Step 7   In the **Target Firmware** field, choose a firmware image from the scroll-down menu.

Step 8   In the **Upgrade Start Time** field, determine if you want to begin the downgrade now or later.

• Click **Now** if you want to schedule the downgrade for now. Go to Step 9, on page 95.

• Click **Later** if you want to schedule the downgrade for a later date or time, then select the date and time from the pop-up calendar for the scheduled downgrade.

Step 9   In the **Ignore Compatibility Check** field, leave the setting in the default off (unchecked) setting, unless you are specifically told to disable the compatibility check feature.

In Cloud APIC, there is a compatibility check feature that verifies if an downgrade path from the currently-running version of the system to a specific newer version is supported or not. The **Ignore Compatibility Check** setting is set to off by default, so the system automatically checks the compatibility for possible downgrades by default.

Note   If you choose to disable the compatibility check feature by entering a check mark in the box next to the **Ignore Compatibility Check** field, you run the risk of making an unsupported downgrade to your system, which could result in your system going to an unavailable state.

Step 10   Click **Schedule Upgrade**.

You can monitor the progress of the downgrade in the main **Firmware Management** window, under the **Upgrade Status** area.

Step 11   When the downgrade is completed, add the necessary CSRs back again.

a)   In your Cloud APIC GUI, click the Intent icon ( ) and choose **cAPIC Setup**.

b)   In the Region Management area, click **Edit Configuration**.

The **Regions to Manage** window appears.

c)   Locate all of the regions that had CSRs and check the boxes in the **Cloud Routers** column for each of those regions to add the CSRs back again.

d)   Click **Next**, then enter the necessary information in the following page and click **Save and Continue**.

Performing a System Recovery

The procedures for performing a system recovery is identical to the procedures for performing a migration-based upgrade. Refer to the section Migration-Based Upgrade, on page 76 for those procedures.

APPENDIX A

Logging Into Cloud APIC Through SSH

Normally, you will log into your Cloud APIC through a browser, as described in Configuring Cisco Cloud APIC Using the Setup Wizard, on page 45. If you need to log into your Cloud APIC through SSH for any reason, however, the following sections describe how to log into the Cloud APIC using the SSH keys that you generated in the previous sections or using SSH password authentication.

- Log Into Cloud APIC Using SSH Keys, on page 97
- Log Into Cloud APIC Using SSH Password Authentication, on page 98

Log Into Cloud APIC Using SSH Keys

Step 1 Log into your Azure account for the Cloud APIC infra tenant and go to the Azure management portal, if you are not there already:

https://portal.azure.com/#home

Step 2 From the main Azure management portal page, click the **All services** link in the left nav bar, then click the **Virtual Machines** link.

Step 3 Locate the Cloud APIC system in the Virtual Machines page, then locate the IP address shown in the Public IP address column.

Step 4 Log into your Cloud APIC using the SSH keys.

- For Linux systems, enter the following to log into your Cloud APIC:

  `# ssh -i private-key-file admin@public-IP-address`

  where the private-key-file is the private key file that you created in Generating an SSH Key Pair in Linux or MacOS, on page 26.

  For example:

  `# ssh -i azure_key admin@192.0.2.1`

- For Windows systems, use PuTTY to log into your Cloud APIC:

  a. Run the PuTTY Configuration program by navigating to **Windows** > **Start Menu** > **All Programs** > **PuTTY** > **PuTTY**.

  b. In the left nav bar, click **Session**, then enter the public IP address for the Cloud APIC.
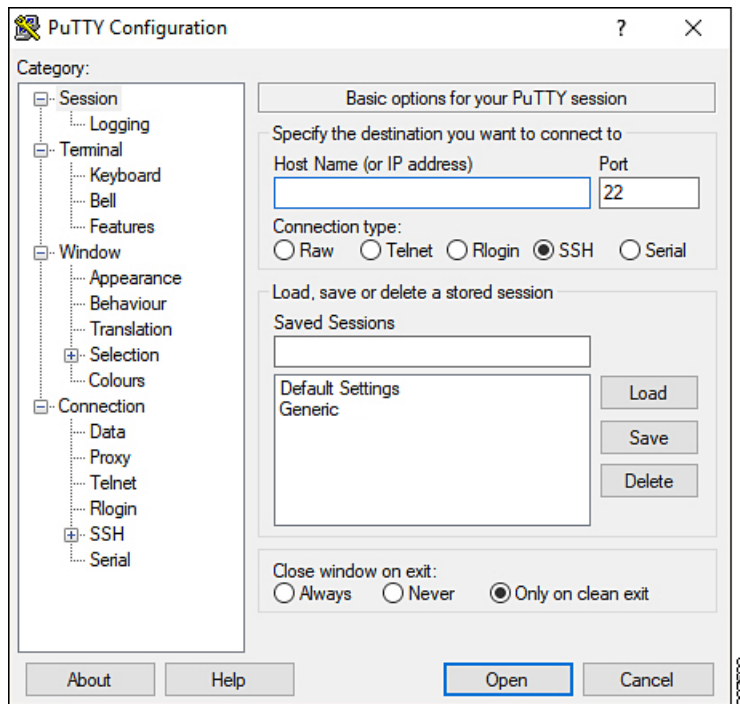
c. In the left nav bar, click **Connection** > **SSH** > **Auth**.

d. In the Authentication parameters area, locate the Private key file for authentication field and click the **Browse...** button.

e. Navigate to the private key file that you created in Generating an SSH Key Pair in Windows, on page 24 and click **Open**.

f. In the main PuTTY window, click **Open** to log into the Cloud APIC. A login prompt appears.

g. Log into the Cloud APIC as `admin`.

Log Into Cloud APIC Using SSH Password Authentication

Unlike SSH using a public key, SSH Password Authentication is disabled by default. Use these procedures to enable SSH Password Authentication so that you can SSH into your Cloud APIC with a username and password.

Step 1 Open a browser window and, using the secure version of HTTP (`https://`), paste the IP address into the URL field, then press Return to access this Cloud APIC.

For example, `https://192.0.2.1`.

Step 2 Enter the following information in the login page for the Cloud APIC:

- **Username**: Enter admin for this field.

> • **Password**: Enter the password that you provided to log into the Cloud APIC.
>
> • **Domain**: If you see the Domain field, leave the default Domain entry as-is.

Step 3   Click **Login** at the bottom of the page.

Step 4   Navigate to **Infrastructure** > **System Configuration**, then click the **Management Access** tab in the **System Configuration** page.

Step 5   Click the pencil icon in the upper right corner of the screen to edit the SSH settings.

The Settings page appears for SSH.

Step 6   In the Password Authentication State field, select Enabled.

Step 7   Click **Save**.

You can now SSH into your Cloud APIC without having to access the public and private key files:

```
# ssh admin@192.0.2.1
```