Cisco Cloud APIC for AWS Installation Guide, Release 4.2(x)

First Published: 2019-09-30

Last Modified: 2019-12-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

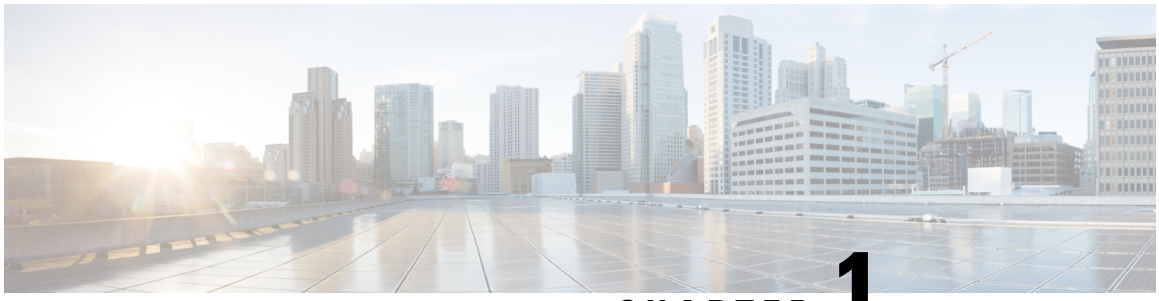
Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Trademarks



CHAPTER 1

New and Changed Information

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 4.2(3)

Feature or Change	Description	Where Documented
Support for AWS Organizations and Organization user tenant	Support is available for AWS Organizations and assigning an Organization tag to a Cloud APIC user tenant.	• Support for AWS Organizations and Organization User Tenant, on page 8 • Configuring a Shared Tenant, on page 44

Table 2: New Features and Changed Behavior in Cisco Cloud APIC Release 4.2(1)

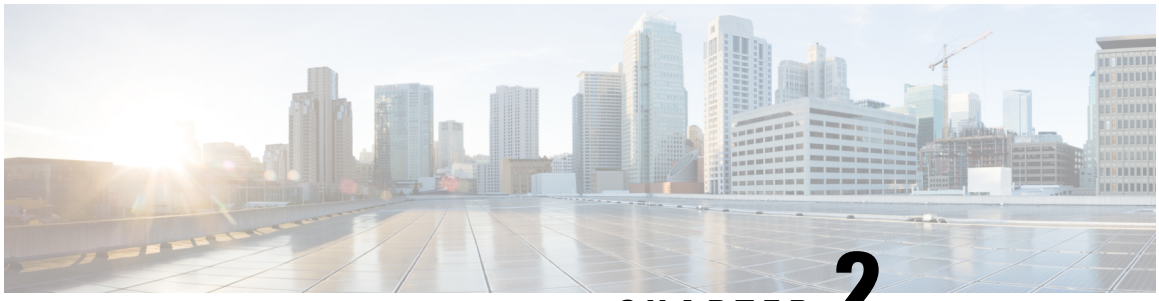
Feature or Change	Description	Where Documented
Support for Microsoft Azure	You can now use Cisco Cloud APIC to extend a Cisco ACI Multi-Site fabric to Microsoft Azure public cloud.	
Support for cloud site-to-cloud site connectivity (Multi-Cloud)	Support is available for cloud site-to-cloud site connectivity, where the cloud sites could be either Amazon AWS public cloud sites or Microsoft Azure public cloud sites.	

Table 3: New Features and Changed Behavior in Cisco Cloud APIC Release 4.1(2)

Feature or Change	Description	Where Documented
Some support for AWS GovCloud	Cisco Cloud APIC now supports AWS GovCloud only for the us-gov-west region. The us-gov-east region is not supported at this time.	Extending the Cisco ACI Fabric to the Public Cloud, on page 3

Table 4: New Features and Changed Behavior in Cisco Cloud APIC Release 4.1(1)

Feature or Change	Description	Where Documented
First release of product	First release of this product	



CHAPTER 2

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 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.

However, 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 deployment 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 deployment.
- 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.

AWS GovCloud Support

Starting with release 4.1(2), Cisco Cloud APIC supports AWS GovCloud only for the us-gov-west region. The us-gov-east region is not currently supported.

Note that these areas have a unique configuration when you deploy a Cisco Cloud APIC on AWS GovCloud:

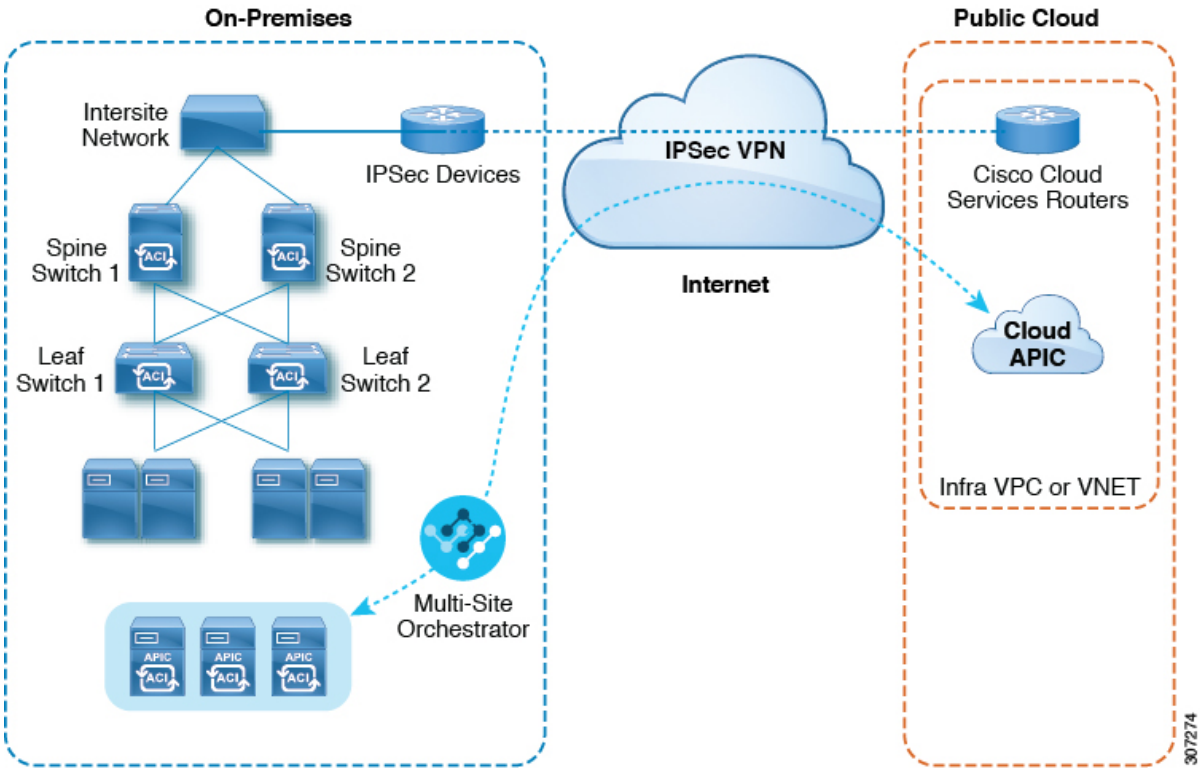
- You will subscribe to the CSR on the commercial account
- You will subscribe to the Cisco Cloud APIC on the commercial account
- You will launch the Cloud Formation template from the commercial account, which redirects the request to AWS GovCloud for the login

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 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 section Managing Cisco Cloud APIC Through Cisco ACI Multi-Site, on page 37 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 section Managing Cisco Cloud APIC Through Cisco ACI Multi-Site, on page 37 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 public cloud site.

AWS 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 private clouds (VPCs) 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*. Also see the sections Deploying the Cloud APIC in AWS, on page 19 and Configuring Cisco Cloud APIC Using the Setup Wizard, on page 30 in this guide.

Cisco Cloud Services Router

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

Cisco Cloud APIC uses the **Cisco Cloud Services Router 1000v** as the cloud services router. For more information on this CSR, see the Cisco CSR 1000v documentation.

AWS public cloud

AWS is a cloud-based platform that provides on-demand services such as compute, storage, network, and databases. Subscribers to AWS have access through the Internet to virtual computers where they can run their workloads.

For more information, see the documentation on the AWS website.

Connections Between the On-Premises Data Center and the Public Cloud

IPsec VPN

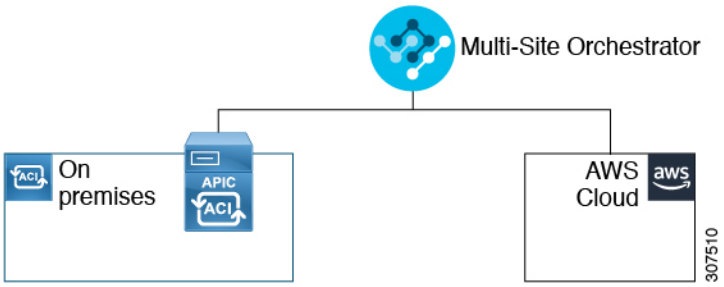
You need Internet connectivity with a VPN from the IPsec router, including a publicly routable IP address and with sufficient bandwidth for AWS or Microsoft Azure connectivity.

Management Connection

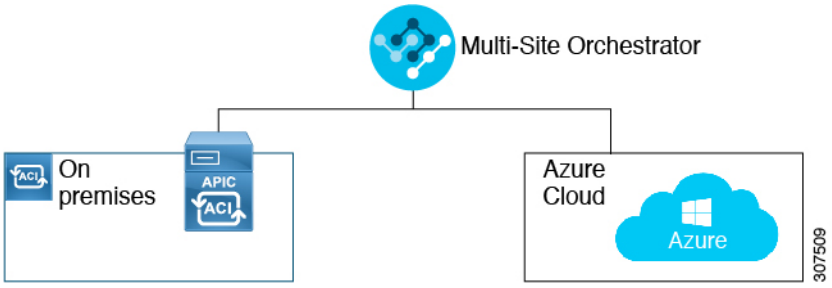
You need a management connection between the Multi-Site Orchestrator in the on-premises data center and Cisco Cloud APIC in the public cloud.

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.

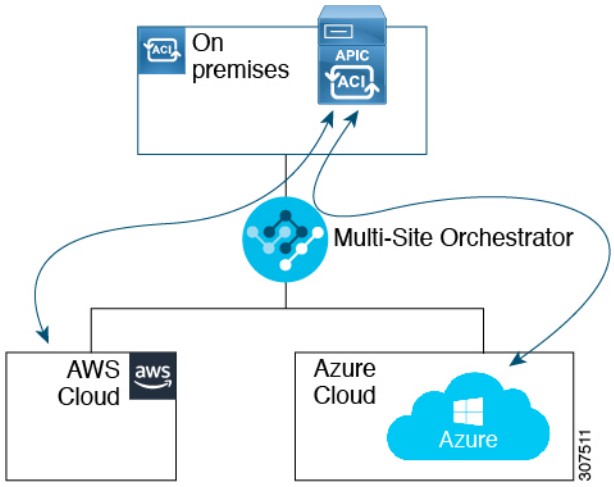


Beginning in APIC Release 4.2(1), you can now use the Cisco ACI Multi-Site Orchestrator to extend an on-premises Cisco ACI site to Microsoft Azure public clouds.

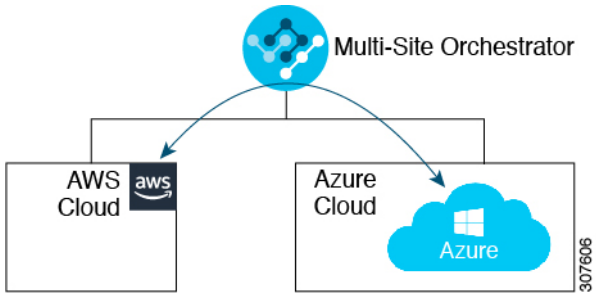


With the expanded functionality available in this release, you can also use the Cisco ACI Multi-Site Orchestrator to establish connectivity between the following components:

- 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).

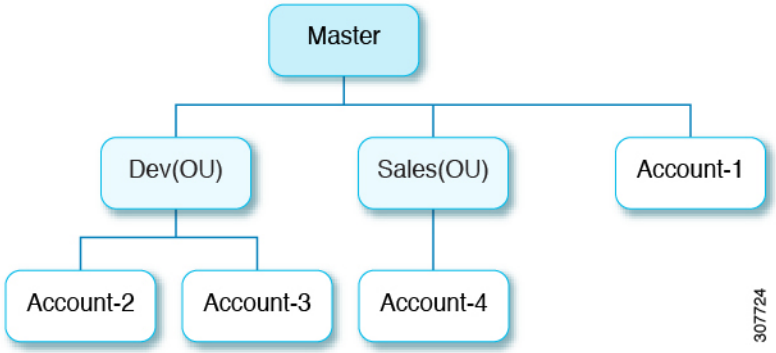
Support for AWS Organizations and Organization User Tenant

With multiple accounts in an organization, it is not easy to control access policies and permissions for various accounts individually, whereas it is easier to do so at the organizational level or at a sub-organizational level within the organization.

Using AWS Organizations, an enterprise might have multiple AWS accounts managed in an organization, as explained here:

https://aws.amazon.com/organizations/

This control of the access policies for accounts (or sub-accounts) in the organization is done by the master account of the organization, which is at the root of accounts hierarchy in the organization. The figure below shows an example setup of accounts in an organization.



There are two ways that AWS accounts become part of an AWS Organization:

- **Created**: Within the existing organization in the master account, you can create an AWS account that is automatically part of your AWS organization using the AWS GUI or the AWS API.
- **Invited**: For accounts that are created outside the organization but need to be joined to the organization, an invitation needs to be sent by the master account to the account owner. After accepting the invitation, the invited account becomes a sub-account within the organization.

If you are using AWS Organizations to consolidate and manage your AWS accounts, you will use AWS Organizations to set up your organization and add the created or invited accounts, as you would normally. See Creating an Organization for more information.

Once you have added the created or invited accounts to your organization through AWS, you will then make the necessary Cloud APIC configurations so that the Cloud APIC recognizes the AWS Organization configurations that you've made through AWS:

- If you want to manage policies for AWS Organization accounts through the Cloud APIC, the Cloud APIC must be deployed in the master account. When you deploy the Cloud APIC in AWS using the instructions provided in Deploying the Cloud APIC in AWS, on page 19, verify that you are deploying the Cloud APIC (the Cloud APIC infra tenant) in the master account for this AWS organization.
- The Cloud APIC uses the `OrganizationAccountAccessRole` IAM role to manage policies for AWS Organization tenants.
  - If you **created** an AWS account within the existing organization in the master account, the `OrganizationAccountAccessRole` IAM role is automatically assigned to that created AWS account. You do not have to manually configure the `OrganizationAccountAccessRole` IAM role in AWS in this case.
  - If the master account **invited** an existing AWS account to join the organization, then you must manually configure the `OrganizationAccountAccessRole` IAM role in AWS. Configure the `OrganizationAccountAccessRole` IAM role in AWS for the organization tenant and verify that it has Cloud APIC-related permissions available.

    The `OrganizationAccountAccessRole` IAM role, together with the SCP (Service Control Policy) used for the organization or the account, must have the minimum permissions that are required by the Cloud APIC to manage policies for the tenants. The access policy requirement is the same as the requirement for the trusted or untrusted tenants.

    For more information, see the "Configure a Tenant AWS Provider" section in the *Cisco Cloud APIC for AWS User Guide*, Version 4.2(x) or later, located here:

https://www.cisco.com/c/en/us/support/cloud-systems-management/cloud-application-policy-infrastructure-controller/products-installation-and-configuration-guides-list.html

- You can then assign the Organization tag to tenants through the Cloud APIC GUI using procedures described in Configuring a Shared Tenant, on page 44.

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.

The following table lists Cisco ACI policy terms and the equivalent terms in Amazon Web Services (AWS).

Cisco ACI	AWS
Tenant	User account
AAA user, security domain	Identity and Access Management (IAM)
Virtual Routing and Forwarding (VRF)	VPC
BD subnet	Virtual Private Cloud (VPC) subnet (CIDR)
ACI infra (or ACI infra tenant)	VPC (named Infra VPC by Cloud APIC)
Contract, filter	Security Group Rule
Taboo	Network access list
EPG	Security group
EP-to-EPG mapping	Tag, label
Endpoint	Network adapter on EC2 instances

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 Amazon Web Services (AWS) Marketplace 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. See Requirements for the AWS Public Cloud, on page 14 and Configuring Cisco Cloud APIC Using the Setup Wizard, on page 30 for more information.

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 **CSR 1000v** license using the instructions in 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.

Amazon Web Services (AWS)

You must subscribe to the **Cisco Cloud Services Router (CSR) 1000V - BYOL for Maximum Performance** CSR license through the AWS Marketplace.

Cisco Cloud APIC-Related Documentation

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

Cisco Documentation

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

- *Cisco Cloud Application Policy Infrastructure Controller Release Notes, Release 4.1(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

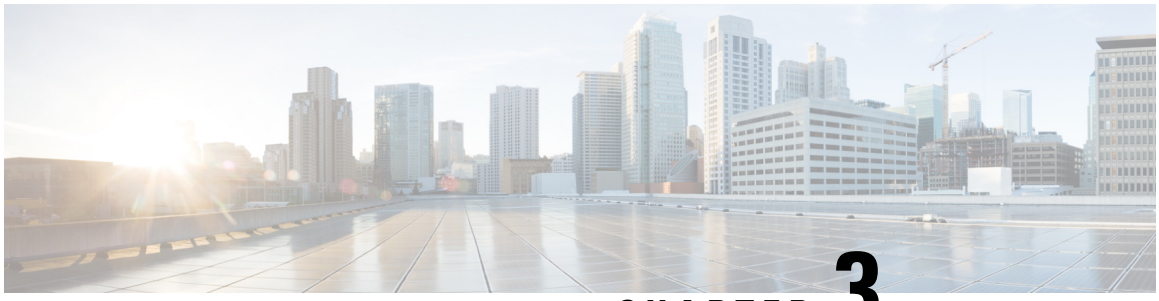
  Includes videos, release notes, installation, configuration, and user guides.

- Cisco Cloud Services Router documentation

  Includes release notes, command reference, data sheets, installation, upgrade, and configuration guides.

AWS Documentation

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



CHAPTER 3

Preparing for Installing Cisco Cloud APIC

Requirements for Extending the Cisco ACI Fabric to the Public Cloud

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

Requirements for the On-Premises Data Center

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

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

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

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

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

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

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

Requirements for the AWS Public Cloud

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

AWS Accounts

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

For example, if you want to create two user tenants, you need three AWS accounts. You must have one account for each user tenant and one account for the infra tenant. The user tenant can be trusted or untrusted. For details, see the section Setting Up the AWS Account for the User Tenant, on page 22 in this guide.

AWS Resources

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

- Access to the Cisco APIC 4.1 Amazon Machine Image (AMI).

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

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

Cisco Cloud Services Router (CSR)

Subscribe to the Cisco Cloud Services Router (CSR) Bring Your Own License (BYOL) through the AWS Marketplace. See Cisco Cloud APIC Licensing, on page 10 for more information.

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

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

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

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

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

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

Elastic IP Addresses

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

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

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

Cisco Cloud APIC

Cisco Cloud APIC is deployed using the M4.2xlarge instance.

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

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

Cloud APIC Communication Ports

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

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

  For the Cloud APIC, use the same Cloud APIC management IP address that you will use to log into the Cloud APIC at the beginning of Configuring Cisco Cloud APIC Using the Setup Wizard, on page 30.

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

  For the two Amazon Web Services CSRs, the public IPsec peering IP uses the elastic IP address of the third network interface, as described in Locating CSR and Tenant Information, on page 67 or as provided if you download the ISN device configuration files using the instructions in Configuring the Intersite Infrastructure, on page 38.

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

Cisco Cloud APIC Installation Workflow

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

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

   See the section "Requirements for Extending the Cisco ACI Fabric to the Public Cloud, on page 13."

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

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

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

   See the section "Deploying the Cloud APIC in AWS, 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 AWS region selection. You provide the Border Gateway

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

See the section "Configuring Cisco Cloud APIC Using the Setup Wizard, on page 30."

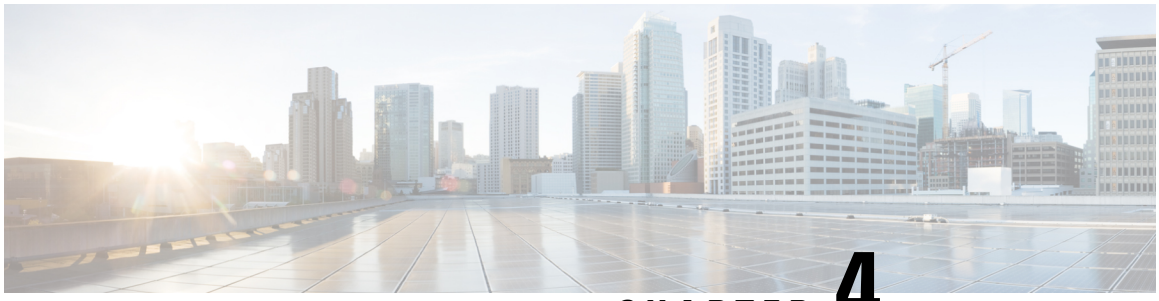
4. Configure Cisco Cloud APIC using Cisco ACI Multi-Site.

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

   See the section "Managing Cisco Cloud APIC Through Cisco ACI Multi-Site, on page 37."

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

   See the sections "Navigating the Cisco Cloud APIC GUI, on page 57" and "Configuring Cisco Cloud APIC Components, on page 57."



CHAPTER 4

Configuring the Cloud Formation Template Information for the Cisco Cloud APIC

Deploying the Cloud APIC in AWS

Before you begin

- Verify that 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. For example, verify that you have the correct number of elastic IP addresses and that you have checked the limits allowed to deploy the instances.
- Verify that you have the full Administrator Access on AWS, because specific AWS IAM roles and permissions are required for the installation and operation of the Cisco Cloud APIC.

  When installing Cloud APIC using the CloudFormation template (CFT), we recommend installation by a user who has the full Administrator Access on AWS (for example, by a user who has the permission policy ARN **arn:aws:iam::aws:policy/AdministratorAccess** attached to it, either directly, by using a role policy, or with a user group). However, if there is no one with AWS Administrator Access available, the person installing Cloud APIC must have a minimum set of permissions. See AWS IAM Roles and Permissions, on page 61 for more information on these AWS IAM roles and permissions.
- If you are using AWS Organizations to control access policies and permissions for various accounts and you want to use Cloud APIC to manage these accounts, verify that the AWS account where you are deploying the Cloud APIC in these procedures (the Cloud APIC infra tenant) is the master account for that AWS organization. When the Cloud APIC is deployed in the master account for an AWS organization, you can add any AWS accounts that are part of the organization as tenants through the Cloud APIC GUI. See Support for AWS Organizations and Organization User Tenant, on page 8 and Configuring a Shared Tenant, on page 44 for more information.
- If you are deploying Cloud APIC on AWS GovCloud, review the information provided in the "AWS GovCloud Support" section in Extending the Cisco ACI Fabric to the Public Cloud, on page 3 for information specific to those deployments.

Step 1 Log into your Amazon Web Services account for the Cloud APIC infra tenant and go to the AWS Management Console, if you are not there already:

https://signin.aws.amazon.com/

https://console.aws.amazon.com/

Step 2 In the upper right corner of the AWS Management Console screen, locate the area that shows a region, and choose the region in AWS that you want to have managed by Cloud APIC (where the Cloud APIC AMI image will be brought up).

Step 3 Create an Amazon EC2 SSH key pair:

a) Click the **Services** link at the top left area of the screen, then click the **EC2** link.

The **EC2 Dashboard** screen appears.

b) In the **EC2 Dashboard** screen, click the **Key Pairs** link.

The **Create Key Pair** screen appears.

c) Click **Create Key Pair**.

d) Enter a unique name for this key pair (for example, `CloudAPICKeyPair`), then click **Create**.

A screen is displayed that shows the public key that is stored in AWS. In addition, a Privacy Enhanced Mail (PEM) file is downloaded locally to your system with the private key.

e) Move the private key PEM file to a safe location on your system and note the location.

You will navigate back to the private key PEM file in this location in a step later in these procedures.

Step 4 Go to the Cloud APIC page on the AWS Marketplace:

http://cs.co/capic-aws

Step 5 Click **Subscribe**.

Step 6 Review and accept the End User License Agreement (EULA) by clicking the **Accept Terms** button.

Step 7 After a minute, you should see the message `Subscription should be processed`. Click the **Continue to Configuration** button.

The **Configure this software** page appears.

Step 8 Select the following parameters:

- **Fulfillment Option:** Cisco Cloud APIC Cloud Formation Template (selected by default)
- **Software Version:** (4.1(1x)) (selected by default)
- **Region:** Region where Cloud APIC will be deployed.

Step 9 Click the **Continue to Launch** button.

The **Launch this software** page appears, which shows a summary of your configuration and lets you launch the cloud formation template.

Step 10 Click **Launch** to go directly to the CloudFormation service in the correct region, with the correct Amazon S3 template URL already populated.

Step 11 Click **Next** at the bottom of the screen.

The **Specify Details** page appears within the **Create stack** page.

Step 12 Enter the following information on the **Specify Details** page.

- **Stack name:** Enter the name for this Cloud APIC configuration.
- **Fabric name:** Leave the default value as-is or enter a fabric name. This entry will be the name for this Cloud APIC.
- **Infra VPC Pool:** The VPC (Virtual Private Cloud) CIDR. This field is automatically populated from the CFT 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.
- **Availability Zone:** Select an availability zone for the Cloud APIC subnets from the scroll-down menu.

  The availability zone options that are presented will be based on the region that you selected in Deploying the Cloud APIC in AWS, on page 19. Select the lowest availability zone from the list. For example, if you see `us-west-1a` and `us-west-1b` as the availability zone options, select `us-west-1a`.
- **Password/Confirm Password:** Enter and confirm an admin password. This entry is the password that you will use to log into the Cloud APIC after you have enabled SSH access.
- **SSH Key Pair:** Choose the name of the SSH key pair that you created in Deploying the Cloud APIC in AWS, on page 19.

  You will use this SSH key pair to log into the Cloud APIC.
- **Access Control:** 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.

Step 13 Click **Next** at the bottom of the screen.

The **Options** page appears within the **Create stack** page.

Step 14 Accept all the default values in the **Options** screen.

There is a **Permissions: IAM Role** area on this page. An IAM role is an IAM entity that defines a set of permissions for making Amazon Web Services service requests. You can use roles to delegate access to users, applications, or services that don't normally have access to your Amazon Web Services resources.

There is no need for IAM role information with regards to the Cloud APIC, but if you want to assign an IAM role for another reason, choose the appropriate role in the **IAM Role** field.

Step 15 Click **Next** at the bottom of the **Options** screen.

The **Review** page appears within the **Create stack** page.

Step 16 Verify that all the information on the **Review** page is correct.

If you see any errors on the **Review** page, click the **Previous** button to go back to the page with the incorrect information.

Step 17 When you have verified that all the information on the **Review** page is correct, check the box next to the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** area.

Step 18 Click the **Create** button at the bottom of the page.

The **CloudFormation** page reappears, and the Cloud APIC template that you created is displayed with the text **CREATE_IN_PROGRESS** displayed in the Status column.

The system now uses the information that you provided in the template to create the Cisco Cloud APIC instance. This process takes 5-10 minutes to complete. You can monitor the progress of the creation process by checking the box next to the name of your Cisco Cloud APIC template, then clicking on the Events tab. The text **CREATE_IN_PROGRESS** is displayed in the Status column under the Events tab.

Step 19 When the **CREATE_COMPLETE** message is shown, verify that the instance is ready before proceeding.

a) Click the **Services** link at the top of the screen, then click the **EC2** link.

The **EC2 Dashboard** screen appears.

b) In the EC2 Dashboard screen, you should see text displaying the number of running instances in the **Resources** area (for example, **1 Running Instances**). Click this running instances link.

The **Instances** screen appears.

c) Wait until you see that instance is ready before proceeding.

You will see the new instance going through the **Initializing** stage under Status Checks. Wait until you see the **2/2 Checks Passed** message under Status Checks before proceeding.

What to do next

Go to Setting Up the AWS Account for the User Tenant, on page 22 to set up the AWS account for the user tenant.

Setting Up the AWS Account for the User Tenant

You can set up the AWS account for the user tenant using one of the following methods:

- Where the user tenant in Cloud APIC is trusted, using the CFT. See Setting Up the AWS Account for a Trusted User Tenant Using the CFT, on page 22.
- Where the user tenant in Cloud APIC is untrusted, using the AWS access key ID and secret access key. See Setting Up the AWS Account for an Untrusted User Tenant Using the AWS Access Key ID and Secret Access Key, on page 24.
- Where you can manage policies for AWS Organization accounts through the Cloud APIC. See Setting Up the AWS Account for an Organization User Tenant, on page 25.

Setting Up the AWS Account for a Trusted User Tenant Using the CFT

Using the tenant role Cloud Formation template (CFT) in the tenant account establishes a trust relationship between the tenant and the account where the Cloud APIC is deployed.

Use the following procedures to set up the AWS account for the user tenant using the tenant role CFT.

Before you begin

Following are the rules and restrictions for configuring the Cloud APIC user tenant:

- You cannot use the same AWS account for the infra tenant and the user tenant.

- You need one AWS account for each user tenant.

Step 1 Log into your Amazon Web Services account for the user tenant:

https://signin.aws.amazon.com/

Note Do not use the infra tenant account for the user tenant.

Step 2 Click the **Services** link at the top of the screen, then click the **CloudFormation** link.

The **CloudFormation** screen appears.

Step 3 Click the **Create Stack** button.

Note Do not choose any options from the drop-down list next to the **Create Stack** button. Click directly on the **Create Stack** button instead.

The **Select Template** page appears within the **Create stack** page.

Step 4 Determine how you will select the template to use for the IAM role for the user tenant configuration.

- If you want to download the tenant role CFT from your AWS account, or if you downloaded it from your cisco.com account (formerly CCO), follow these procedures:

  a. If you want to download the tenant role CFT from your AWS account, locate the tenant role CFT. The tenant role CFT is located in the S3 bucket in the AWS account for the Cisco Cloud APIC infra tenant. The name of the S3 bucket is capic-common-[capicAccountId]-data and the tenant role CFT object is tenant-cft.json in that bucket. The capicAccountId is the AWS account number for the Cisco Cloud APIC infra tenant, which is the account in which Cloud APIC is deployed.

  b. Download the tenant role CFT to a location on your computer.

  For security reasons, public access to this S3 bucket in AWS is not allowed, so you must download this file and use it in the tenant account.

  c. In AWS, in the **Choose a template** area, click the circle next to **Upload a template to Amazon S3**, then click the **Choose File** button.

  d. Navigate to the location on your computer where you saved the JSON-formatted tenant role CFT that you received from Cisco (for example, `tenant-cft.json`) and select that template file.

- If you were given a tenant role CFT URL from Cisco, in the **Choose a template** area, click the circle next to **Specify an Amazon S3 template URL**, then enter the tenant role CFT URL that you received from Cisco into the field below the text.

Step 5 Click **Next** at the bottom of the screen.

The **Specify Details** page appears within the **Create stack** page.

Step 6 Enter the following information on the **Specify Details** page.

- **Stack name:** Enter the name for this IAM role for the user tenant configuration (for example, `IAM-Role`).
- **infraAccountId:** If you see this field, enter the AWS account for the infra tenant as described in Deploying the Cloud APIC in AWS, on page 19.

Note that this field is displayed if you downloaded and used the tenant role CFT from your cisco.com account. It is not displayed if you downloaded and used the tenant role CFT from your AWS account because the infraAccountId information is pre-populated in the CFT when it is downloaded from the S3 bucket in the infra AWS account.

Step 7 Click **Next** at the bottom of the screen.

The **Options** page appears within the **Create stack** page.

Step 8 Accept all the default values in the **Options** screen, if applicable, then click **Next** at the bottom of the screen.

The **Review** page appears within the **Create stack** page.

Step 9 In the **Review** page, check the box next to the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** area, then click the **Create** button at the bottom of the page.

The **CloudFormation** page reappears, and the Cisco Cloud APIC template that you created is displayed with the text **CREATE_IN_PROGRESS** displayed in the Status column.

The system now uses the information that you provided in the template to create the IAM role for the user tenant. This process takes 5-10 minutes to complete. You can monitor the progress of the creation process by checking the box next to the name of the template, then clicking on the Events tab. The text **CREATE_IN_PROGRESS** is displayed in the Status column under the Events tab.

CREATE_COMPLETE is shown when the process is completed.

Step 10 When the **CREATE_COMPLETE** is shown, navigate to the appropriate area to verify that the IAM role for the user tenant was created successfully.

a) Click the **Services** link at the top of the screen, then click the **IAM** link.
b) Click **Roles**.

An entry with the name **ApicTenantRole** should appear under the Role name.

What to do next

Go to Configuring Cisco Cloud APIC Using the Setup Wizard, on page 27 to continue setting up the Cisco Cloud APIC.

Setting Up the AWS Account for an Untrusted User Tenant Using the AWS Access Key ID and Secret Access Key

Use the following procedures if you want to set up the AWS account for an untrusted user using the AWS access key ID and secret access key, where you will manually set up the AWS account for an untrusted user tenant and assign the appropriate permissions through AWS IAM.

Before you begin

Following are the rules and restrictions for configuring the Cloud APIC user tenant:

- You cannot use the same AWS account for the infra tenant and the user tenant.
- You need one AWS account for each user tenant.

Step 1 Log into your Amazon Web Services account for the user tenant:

https://signin.aws.amazon.com/

Note Do not use the infra tenant account for the user tenant.

Step 2 Go to the AWS Management Console:

https://console.aws.amazon.com/

Step 3 Click the **Services** link at the top of the screen, then click the **IAM** link.

Step 4 In the left pane, click **Users**, then click the **Add user** button.

The **Add User** page appears.

Step 5 In the **User name** field, enter a unique name for this AWS user account, such as `user1`.

Step 6 In the **Access type** field, check **Programmatic access**.

Step 7 Click the **Next: Permissions** button at the bottom of the page.

Step 8 In the **Set permissions** area, select **Attach existing policies directly**.

The screen expands to display **Filter policies** information.

Step 9 Check the box next to **Administrator Access**, then click the **Next: Tags** button at the bottom of the page.

Step 10 Leave the information in the **Add tags** page as-is and click the **Next: Review** button at the bottom of the page.

Step 11 Click the **Create User** button at the bottom of the page.

Ignore the warning that states **This user has no permissions** if that warning appears.

An access key is created for you at this point.

Step 12 Make a note of the Access Key ID and Secret Access Key information for this AWS account.

- Copy the Access Key ID and the Secret Access Key information for the user tenant to the appropriate rows in Locating CSR and Tenant Information, on page 67.
- Download the .csv file or copy the information from the **Access key ID** and **Secret access key** fields to a file.

Step 13 Click the **Close** button at the bottom of the page.

Step 14 Repeat the steps in this topic for additional user accounts, if necessary.

What to do next

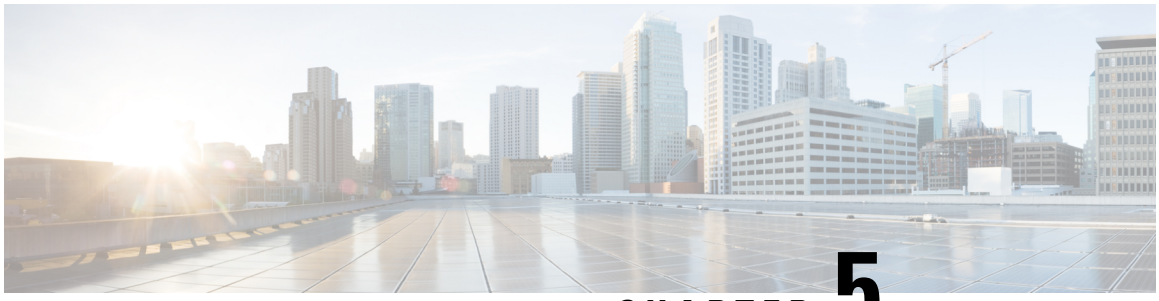
Go to Configuring Cisco Cloud APIC Using the Setup Wizard, on page 27 to continue setting up the Cisco Cloud APIC.

Setting Up the AWS Account for an Organization User Tenant

As described in Support for AWS Organizations and Organization User Tenant, on page 8, beginning with Release 4.2(3), you can now manage policies for AWS Organization accounts through the Cloud APIC.

To set up the AWS account for an organization tenant, you must have the following configurations in order to use this feature:

- The Cloud APIC must be deployed in the master account. Earlier in this document, when you deployed the Cloud APIC in AWS using the instructions provided in Deploying the Cloud APIC in AWS, on page 19, verify that you deployed the Cloud APIC (the Cloud APIC infra tenant) in the master account for this AWS organization.
- Later in this document, you will assign the Organization tag to tenants through the Cloud APIC GUI, using procedures described in Configuring a Shared Tenant, on page 44.



CHAPTER 5

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 AWS. 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.
    - The number of CSRs supported per managed region varies, depending on the release:
      - For releases prior to 5.1(2), a maximum of four CSRs per managed region is supported, for a total of 16 CSRs per cloud site.
      - For Release 5.1(2) and later, a maximum of eight CSRs per managed region is supported, for a total of 32 CSRs per cloud site. For more information on increasing the number of CSRs, see the *Cloud APIC for AWS User Guide*.

Locating the Cloud APIC IP Address

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

Step 1 Go to the AWS account for the Cloud APIC infra tenant.

Step 2 Click the **Services** link at the top of the screen, then click the **EC2** link.

The **EC2 Dashboard** screen appears.

Step 3 In the EC2 Dashboard screen, you should see text displaying the number of running instances in the **Resources** area (for example, **1 Running Instances**). Click this running instances link.

The **Instances** screen appears.

Step 4 Choose the Cloud APIC instance named `Capic-1` and copy the IP address that is shown in the **IPv4 Public IP** column.

This is the Cloud APIC IP address that you will use to log into the Cloud APIC.

Note You can also get the Cloud APIC IP address by going back to the **CloudFormation** page, clicking on the box next to the Cisco Cloud APIC and then clicking on the **Outputs** tab. The Cisco Cloud APIC IP address is shown in the **Value** column.

Configuring Cisco Cloud APIC Using the Setup Wizard

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 AWS 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 Configuring the Cloud Formation Template Information for the Cisco Cloud APIC, on page 19.

Step 1 In the AWS site, get the Cloud APIC IP address.

See Locating the Cloud APIC IP Address, on page 29 for those instructions.

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 on the Specify Details page from Step 12, on page 21 in the Deploying the Cloud APIC in AWS, on page 19 procedures.
- **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 Servers**
- **Region Management**
- **Smart Licensing**

Step 6 In the **DNS 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 31 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 Verify that the Cloud APIC home region is selected.

The region that you selected in Step 2, on page 20 in Deploying the Cloud APIC in AWS, on page 19 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 `cAPIC deployed` in the Region column.

Step 11 Select additional regions if you want the Cloud APIC to manage additional regions, and to possibly deploy CSRs to have inter-VPC communication and Hybrid-Cloud, Hybrid Multi-Cloud, or Multi-Cloud connectivity on those other regions.

The CSR can manage 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 cluster 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-VPC or inter-VNET 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 28 for more information.
- **Inter-Site Connectivity:** This option is shown as **On Premises Connectivity** in releases prior to 4.2(1).

  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 VPCs or VNETs 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 12 When you have selected all the appropriate regions, click **Next** at the bottom of the page.

The **General Connectivity** page appears.

Step 13 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 Do not use **64512** as the autonomous system number in this field.

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 that will be used in each region.

See Understanding Limitations for Number of Sites, Regions and CSRs, on page 28 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.

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 AWS 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 4.2(4q), the **TCP MSS** option is available to configure the TCP maximum segment size (MSS). This value will be applied to all cloud router tunnel interfaces, including VPN tunnels towards the cloud and external tunnels towards the on-premises site 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 14 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 17, on page 33.
- 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 15 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 AWS. 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 16 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 17 In the **Smart Licensing** row, click **Register**.

The **Smart Licensing** page appears.

Step 18 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 19 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 20 Verify the information on the **Summary** page, then click **Close**.

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.

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 37.
- 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. 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 57 and Configuring Cisco Cloud APIC Components, on page 57 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 **On Premises 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 37.

CHAPTER 6

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 SITES**.

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 Amazon Web Services, which is the same public IP address that you used to log into the Cloud APIC at the beginning of 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 Configuring the Intersite Infrastructure, on page 38.

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 39.
- 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 AWS 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 AWS 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 Configuring a Shared Tenant, on page 44.

Follow these procedures to manually enable connectivity between Cisco Cloud Services Router 1000V (CSR) deployed in Amazon Web Services 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 AWS 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 38, 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 AWS 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 Amazon Web Services.
- <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 12345678900987654321234567891
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.

Configuring a Shared Tenant

Use the procedures in this section to configure a tenant that is shared between the on-premises site and the Cloud APIC site.

Step 1 In the ACI Multi-Site Orchestrator:

a) In the Main menu, click **Tenants**.
b) In the Tenants List area, click **ADD TENANT**.
c) In the Tenant Details pane, perform the following actions:

- In the **DISPLAY NAME** field, enter the tenant name.
- **Optional:** In the **DESCRIPTION** field, enter the a brief description of the tenant.
- In the **Associated Sites** section, choose the on-premises and the cloud sites.
- In the **Associated Users** section, choose the users if they are not already selected.
- Click **SAVE**.

Step 2 Log into the Cloud APIC site and configure the Amazon Web Services account details for this tenant:

a) On the main Cloud APIC page, under **Application Management**, click **Tenants**.
b) On the Tenants page, click on the tenant that you just created through the ACI Multi-Site Orchestrator in the previous step.
c) Click the expand button at the top right of the screen.

This is the button with the square and up-right-pointing arrow next to the close (X) button.

d) On the Tenant page, click the Edit button at the top right of the screen. This is the button with the pencil icon next to the Actions field.
e) On the Edit Tenant page, scroll to the Settings area and enter the necessary information, depending on the access type for the user tenant:

- If the user tenant in Cloud APIC is trusted (if you set up the AWS account for Trusted Tenant using CFT), enter the following information in this page:
  - **AWS Account ID:** Enter the AWS account number for the user tenant (the AWS account that you logged into when setting up the AWS account for Trusted Tenant using the CFT).
  - **Access Type:** Select **Trusted** in this field.

  Note The **Cloud Access Key ID** and the **Cloud Secret Access Key** fields are not displayed when you select **Trusted** as the **Access Type**. These fields are not needed for a trusted tenant.

- If the user tenant in Cloud APIC is untrusted (if you set up the AWS account for an Untrusted User Tenant using the AWS access key ID and secret access key), enter the following information in this page:
  - **AWS Account ID:** Enter the AWS account number for the user tenant in this field.
  - **Access Type:** Select **Untrusted** in this field.
  - **Cloud Access Key ID:** Enter the AWS access key ID information for the user tenant in this field.

- **Cloud Secret Access Key:** Enter the AWS secret access key information for the user tenant in this field.

- If the user tenant in Cloud APIC is a member of an AWS Organization (if you used AWS Organizations to set up your organization and added accounts to this organization either by creating accounts within the organization or by inviting accounts into the organization), and you have deployed Cloud APIC in the master account of the organization, enter the following information to assign the Organization tag to this tenant:
  - **AWS Account ID:** Enter the AWS account number for the user tenant in this field.
  - **Access Type:** Select **Organization** in this field.

    Note The following applies if you are assigning the Organization tag to this tenant:
    - If the **Organization** option is grayed out in this field, that means that you did not deploy the Cloud APIC (the infra tenant) in the master account for an AWS organization. You cannot assign the Organization tag to a tenant if the Cloud APIC (the infra tenant) was not deployed in the master account for an AWS organization. See Deploying the Cloud APIC in AWS, on page 19 for more information.
    - If the master account **invited** an existing AWS account to join the organization, verify that you have the `OrganizationAccountAccessRole` IAM role configured in AWS for the organization tenant and that it has Cloud APIC-related permissions available. See Support for AWS Organizations and Organization User Tenant, on page 8 for more information.

Note The **Cloud Access Key ID** and the **Cloud Secret Access Key** fields are not displayed when you select **Organization** as the **Access Type**. These fields are not needed for an organization tenant.

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

What to do next

Go to Creating a Schema, on page 45.

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 48.

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 Shared Tenant, on page 44 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 Configuring an Application Profile and the EPGs, on page 46.

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 Creating a Filter for a Contract, on page 47.

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 Configuring an Application Profile and the EPGs, on page 46.

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 Configuring an Application Profile and the EPGs, on page 46.

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 Amazon Web Services 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 VPC 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 Amazon Web Services VPC.

  Note The VPC CIDR information that you enter in this field cannot overlap with the infra VPC CIDR. Verify that the CIDR information that you enter in this field does not overlap with the infra VPC CIDR information that you entered in the **Infra VPC Pool** field in Step 12, on page 21 in Deploying the Cloud APIC in AWS, on page 19.

- **CIDR TYPE** — Select Primary or Secondary. If this is your first CIDR, select Primary for the CIDR type.
- **ADD SUBNETS** — Enter the subnet information and select the zone, then click the check mark. For example, `11.11.1.0/24`

  Allocate a subnet within the range of the CIDR block for each availability zone.

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

Configuring Instances in AWS

When you configure endpoint selectors for Cloud APIC, either through the Cloud APIC GUI or through the ACI Multi-Site Orchestrator GUI, you will also need to configure the instances that you will need in AWS that will correspond with the endpoint selectors that you configure for Cloud APIC.

This topic provides the instructions for configuring the instances in AWS. You can use these procedures to configure the instances in AWS either before you configure the endpoint selectors for Cloud APIC or afterward. For example, you might go to your account in AWS and create a custom tag or label in AWS first, then create an endpoint selector using a custom tag or label in ACI Multi-Site Orchestrator afterward. Or you might create an endpoint selector using a custom tag or label in ACI Multi-Site Orchestrator first, then go to your account in AWS and create a custom tag or label in AWS afterward.

Step 1 Determine if you configured the cloud context profile through the ACI Multi-Site Orchestrator GUI or through the Cisco Cloud APIC GUI.

You must configure a cloud context profile as part of the AWS instance configuration process, where the cloud context profile, in conjunction with a VRF and a region, represents the AWS VPC in that region. When you configure a cloud context profile using the Cisco Cloud APIC GUI, the configurations, such as the VRF and region settings, are pushed out to AWS afterward. A similar action takes place when you configure a Cisco Cloud APIC through the ACI Multi-Site Orchestrator GUI, where these cloud context profile settings are pushed out to AWS as part of the Cisco Cloud APIC configuration process through the ACI Multi-Site Orchestrator GUI.

- If you are configuring the Cisco Cloud APIC through the ACI Multi-Site Orchestrator GUI, then you do not have to manually configure a cloud context profile. Certain cloud context profile configuration settings, such as the VRF and region settings, are pushed out to AWS as part of the Cisco Cloud APIC configuration process through the ACI Multi-Site Orchestrator GUI that you performed in previous sections.
- If you are configuring the cloud context profile through the Cisco Cloud APIC GUI, follow the procedures in the *Cisco Cloud APIC User Guide, Release 4.1(x)* to configure the cloud context profile, either through the GUI or through the REST API.

Step 2 Review your cloud context profile configuration settings and determine which settings you will use with your AWS instance.

a) Log in to your Cisco Cloud APIC, if you are not already logged in.
b) From the **Navigation** menu, choose the **Application Management** tab.

When the **Application Management** tab expands, a list of subtab options appear.

c) Choose the **Cloud Context Profiles** subtab option.

A list of the cloud context profiles that you have created for your Cisco Cloud APIC are displayed.

d) Select the cloud context profile that you will use as part of this AWS instance configuration process.

Various configuration parameters are displayed for this cloud context profile, such as the region, VRF, IP address and subnets. Use the information displayed in this window when you configure the AWS instance.

Step 3 Log in to the Amazon Web Services account for the Cisco Cloud APIC user tenant, if you are not logged in already.

Step 4 Go to **Services** > **EC2** > **Instances** > **Launch Instance**.

Step 5 In the **Choose an Amazon Machine Image (AMI)** page, select an Amazon Machine Image (AMI).

Step 6 In the **Choose an Instance Type** page, select an instance type, then click **Configure Instance Details**.

Step 7 In the **Configure Instance Details** page, enter the necessary information in the appropriate fields.

- In the **Network** field, select your Cloud APIC VRF.

  This would be the VRF that is associated with the cloud context profile that you are using as part of this AWS instance configuration process.

- In the **Subnet** field, select the subnet.

- In the **Auto-assign Public IP** field, if you want to have a public IP, select **Enable** from the scroll-down menu.

Step 8 When you have finished entering the necessary information into the **Configure Instance Details** page, click **Add Storage**.

Step 9 In the **Add Storage** page, accept the default values or configure the storage in this page, if necessary, and click **Add Tags**.

Step 10 In the **Add Tags** page, click **Add Tag** and enter the necessary information in the appropriate fields in this page.

Note If you will be using IP Address, Region or Zone for the type of endpoint selector later in these procedures, you do not have to enter any information in this page. In those situations, when you start the instance in AWS, the IP address, region or zone will be discovered by the Cloud APIC and the endpoint will be assigned to the EPG.

- **Key:** Enter the key that you will use when you create a custom tag for the type of endpoint selector that you are adding later in these procedures.
- **Value:** Enter the value that you will be using for this key.
- **Instances:** Check the box for this field.
- **Volumes:** Check the box for this field.

For example, if you are planning on creating a custom tag for a specific building for your endpoint selector later in these procedures (such as building6), you might enter the following values in these fields on this page:

- **Key:** Location
- **Value:** building6

Step 11 Click **Review and Launch**.

The **Select an existing key pair or create a new key pair** page appears. Use the information in this page if you want to ssh to the instance later on.

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 AWS VPC 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 4.1(x)*.

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

See Configuring Instances in AWS, on page 48 for those instructions.

Note These steps assume that you are configuring the instance in AWS first, then adding an endpoint selector for Cisco Cloud APIC afterward; however, as described in Configuring Instances in AWS, on page 48, you can also add an endpoint selector in Cisco Cloud APIC first, then perform this AWS 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 52.

- 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.

- **Region**: Used to select by the AWS region of the endpoint.
- **Zone**: Used to select by the AWS availability zone 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 AWS, you might create the custom tag `Location` in this field, to match the Location tag that you added in AWS earlier.

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

Note In releases prior to 4.2(1), options **Key Exist** and **Key Not Exist** were used instead of **Has Key** and **Does Not Have Key**. Only the names of the options differ; the functionality is the same between both sets of options.

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 **Does Not Have Key** is selected for the Operator field.

For example, if you want to have a specific Amazon Web Services availability zone for the endpoint selector, such as `us-west-1a`, you might make the following selections in this screen:

- **Key:** Zone
- **Operator:** Equals
- **Value:** us-west-1a

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 AWS 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:** Zone
  - **Operator:** Equals
  - **Value:** us-west-1a
- 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 availability zone is us-west-1a 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:** us-east-1, us-east-2

In this case:

- If the availability zone is us-west-1a AND the IP address belongs to the 192.0.2.1/24 subnet (endpoint selector 1 expressions)

  OR

- If the region is either us-east-1 or us-east-2 (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, on page 54.

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 On Premises 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 AWS to the ISN (IPsec termination point) on-premises and to the VGWs in the user VPCs.
- 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 → VPCs and verify that the VPCs 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 AWS:

```
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 AWS and the ISN on-premises devices.

You can run the following command on either the Cisco Cloud Services Router 1000V on AWS 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 AWS 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
```

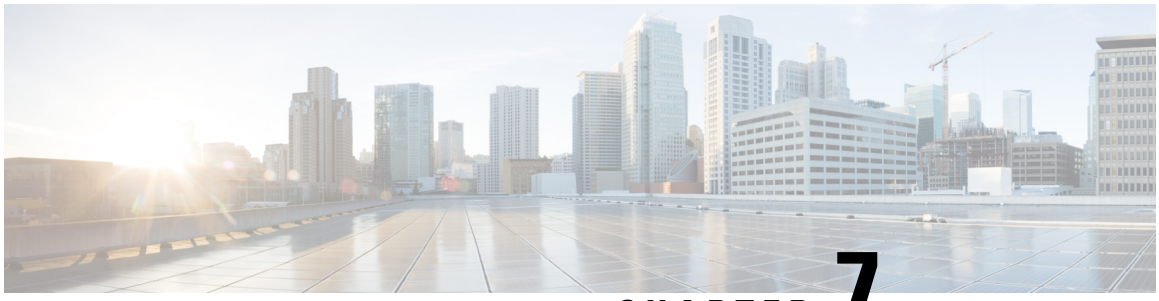
Step 7 From a command line, verify that the BGP routes for the VRF show both the cloud and on-premises routes.

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

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 57. 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.

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.

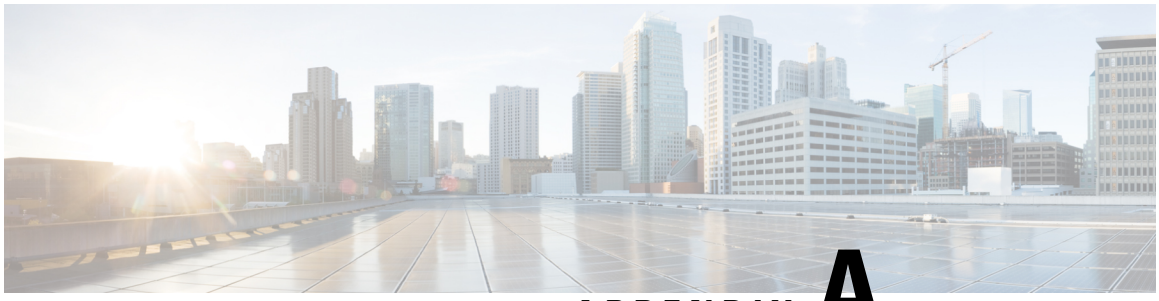
For example, if you want to configure a tenant, type the word tenant in the search window. The search returns a list of tasks that are related to creating and configuring tenants.

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.



APPENDIX A

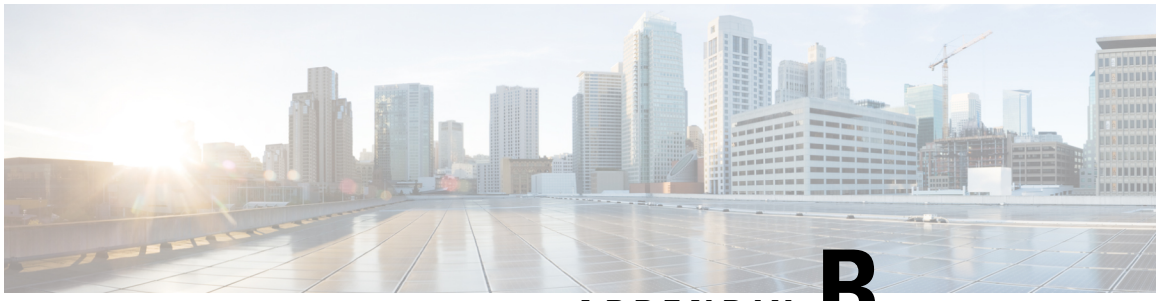
AWS Resources and Naming Conventions

AWS Resources and Naming Conventions

Following is a list of AWS resources created by the Cloud APIC when it is installed, and the naming conventions used in the Cloud APIC. Use the information in this list to better understand these AWS resources and to avoid using similar names.

Item	Number of Items Used	Naming Convention for Item
S3 buckets	• One global (used to store the CFT templates) • One per region (used to store the CloudTrail logs)	Cloud APIC S3 buckets begin with the prefix `capic`. Avoid using buckets that begin with this prefix.
Tags	Minimum of two, maximum of eight	Following are the tag keys used: • `AciDnTag` • `AciOwnerTag` • Name (tag value contains object relative name, or RN) • `AciStaleTag` (present only if a resource is considered stale by Cloud APIC) • `AciResolvedObjDnTag` (only for VPC – it carries the Distinguished Name, or DN, for the resolved object) • `AciPeerDnTag` (only for VPC peering – it carries the DN for the peer VPC)

Item	Number of Items Used	Naming Convention for Item
		Avoid creating tags starting with `Aci` or `Capic`.
CloudTrails	One per region	Trail names begin with the prefix `capic`. Avoid creating trails that begin with this prefix.
CloudWatch events	Three per region	Rules begin with the prefix `capic`. Avoid creating rules that begin with this prefix.
Simple Queue Service (SQS) queues	One per region	Queue names begin with the prefix `capic`. Avoid creating queues that begin with this prefix.



APPENDIX B

AWS IAM Roles and Permissions

AWS IAM Roles and Permissions

Note Additional information on AWS IAM roles and permissions is available in the *Cisco Cloud APIC for AWS User Guide*, including how to configure an AWS provider as one of the following types of tenants:

- Trusted tenant
- Untrusted tenant
- Organization tenant, supported in Release 4.2(3) and later

The *Cisco Cloud APIC for AWS User Guide* is available here:

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

Specific AWS IAM roles and permissions are required for the installation and operation of the Cisco Cloud APIC.

When installing Cisco Cloud APIC using the CloudFormation template (CFT), we recommend installation by a user who has the full Administrator Access on AWS (for example, by a user who has the permission policy ARN **arn:aws:iam::aws:policy/AdministratorAccess** attached to it, either directly, by using a role policy, or with a user group). However, if there is no user with AWS Administrator Access available, the user installing Cisco Cloud APIC must have this minimum set of permissions:

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Effect": "Allow",
   "Action": "iam:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "ec2:*",
   "Resource": "*"
```

```
  },
  {
   "Effect": "Allow",
   "Action": "cloudformation:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "s3:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "sns:*",
   "Resource": "*"
  }
 ]
}
```

The above permission set is necessary for a user who installs Cisco Cloud APIC using the CFT. Following are more detailed descriptions of each of the required permissions presented above, as shown in the **Action** lines:

- **iam Permissions:** The Cisco Cloud APIC instance is an AWS EC2 instance that runs with an AWS role called **ApicAdmin**. This role needs to be created by the CloudFormation stack. Running the Cisco Cloud APIC instance with the **ApicAdmin** role allows the Cisco Cloud APIC instance to get temporary credentials using the AWS metadata service. This frees the Cisco Cloud APIC instance from having to use fixed access key IDs and secret access keys for making AWS API calls.
- **ec2 Permissions:** Needed so that the stack can create the needed VPC, subnets, security groups, and so on. The stack creates the infra VPC, where the Cisco Cloud APIC instance is deployed.
- **cloudformation Permissions:** Needed to run the CFT itself.
- **s3 Permissions:** Needed so that the CFT is saved in an S3 bucket based on the needs of the AWS CloudFormation stack.
- **sns Permissions:** Needed to get notifications for running the CloudFormation stack.

For operations, Cisco Cloud APIC runs with **ApicAdmin** role. This role has two policies attached, and they get created as part of launching the CloudFormation template:

- **ApicAdminFullAccess Policy:** Permissions listed in this policy allows Cisco Cloud APIC to create and manage EC2 and VPC resources, S3 buckets, Resource Groups, account notifications and logs. Note that Cisco Cloud APIC only tries to manage the resources it creates. It does not deal with resources created by any other applications.

  This policy should have the following permissions:

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Action": "organizations:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "ec2:*",
   "Resource": "*",
```

```
   "Effect": "Allow"
  },
  {
   "Action": "s3:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "sqs:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "elasticloadbalancing:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "acm:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "cloudtrail:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "cloudwatch:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "logs:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "resource-groups:*",
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": "events:*",
   "Resource": "*",
   "Effect": "Allow",
   "Sid": "CloudWatchEventsFullAccess"
  },
  {
   "Action": "autoscaling:*",
   "Resource": "*",
   "Effect": "Allow"
  }
 ]
}
```

- **ApicTenantsAccess Policy:** Permissions listed in this policy allows Cisco Cloud APIC to assume the role of tenant accounts and call AWS APIs on those tenant AWS accounts. This allows Cisco Cloud APIC to access tenant accounts without having to use the hard credentials of those tenant accounts.

  This policy should have the following permissions:

```
{
```

```
 "Version": "2012-10-17",
 "Statement": [{
  "Action": "sts:AssumeRole",
  "Resource": "*",
  "Effect": "Allow"
 }]
}
```

Note that Cisco Cloud APIC itself does not need IAM permissions for its operation because it does not create any IAM policies or roles after its installation.

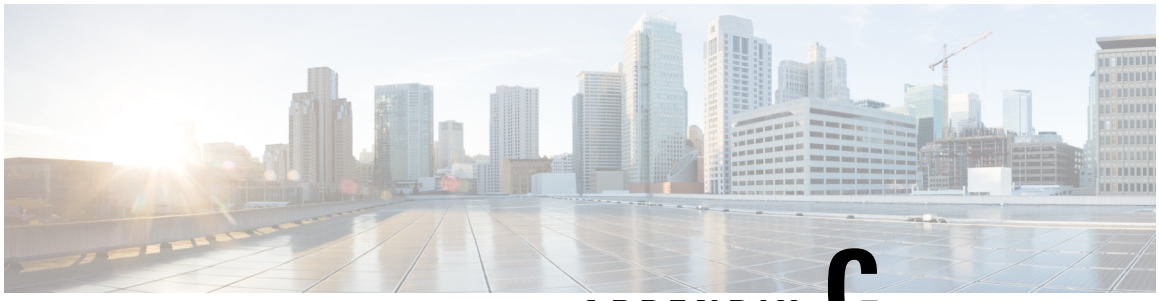
Cisco Cloud APIC will attempt to manage the AWS resources that are created by it, but it will not attempt to manage resources created by other applications, other than listing existing resources as inventory. At the same time, AWS IAM users in those accounts (both the infra account and other tenant accounts) should not interfere with the resources created by Cisco Cloud APIC. Therefore, all resources created by Cisco Cloud APIC on AWS have at least one of these two tags applied on them:

- **AciDnTag**
- **AciOwnerTag**

Therefore, when you create AWS IAM users who have permission to create, delete or update EC2, VPC and other resources, you must prevent these users from accessing or modifying the resources created and managed by Cisco Cloud APIC. Such restrictions should apply on both the infra and other user tenant accounts. AWS account administrators should use the above two tags to prevent users from accessing or modifying the resources created and managed by Cisco Cloud APIC.

For example, you might have an access policy similar to the following for an IAM user to prevent unintended access to resources managed by Cisco Cloud APIC:

```
{
 "Effect": "Deny",
 "Action": [
  "ec2:*"
 ],
 "Resource": "*",
 "Condition": {
  "StringLike": {
   "ec2:ResourceTag/AciDnTag": "*"
  }
 }
}
```



APPENDIX C

Tenant-Region Management

Tenant-Region Management

Deploying Tenant Policies in Different Regions

Cisco Cloud APIC enforces ownership checks to prevent deployment of policies in the same tenant-region combination, done either intentionally or by mistake. For example, assume that one Cisco Cloud APIC (CAPIC1) is deployed in AWS account IA1 in the region R1, and you want to deploy a tenant in account TA1 in region R2. This tenant deployment (the account-region combination of TA1-R2) is now owned by IA1-R1 (CAPIC1). If another Cisco Cloud APIC (CAPIC2) attempts to manage the same tenant-region combination of TA1-R2 at some point in the future (for example, if CAPIC2 is deployed in AWS account IA2 in the region R3), this will not be allowed because the current owner for the deployment TA1-R2 is IA1-R1 (CAPIC1).

These restrictions are achieved using AWS Resource Groups. The following example provides several valid and invalid deployment combinations.

Cisco Cloud APIC	Tenant	Validity	Reason
IA1-R1 (CAPIC1)	TA1-R1	Valid	Tenant TA1-R1 is owned by IA1-R1 (CAPIC1)
IA1-R1 (CAPIC1)	TA1-R2	Valid	Tenant TA1-R2 is owned by IA1-R1 (CAPIC1)
IA1-R2 (CAPIC2)	TA1-R1	Invalid	Tenant TA1-R1 is already owned by IA1-R1 (CAPIC1)
IA1-R2 (CAPIC2)	TA1-R3	Valid	Tenant TA1-R3 is owned by IA1-R2 (CAPIC2)
IA2-R1 (CAPIC3)	TA1-R1	Invalid	Tenant TA1-R1 is already owned by IA1-R1 (CAPIC1)
IA2-R1 (CAPIC3)	TA1-R4	Valid	Tenant TA1-R4 is owned by IA2-R1 (CAPIC3)

Cisco Cloud APIC	Tenant	Validity	Reason
IA2-R1 (CAPIC3)	TA2-R4	Valid	Tenant TA2-R4 is owned by IA2-R1 (CAPIC3)

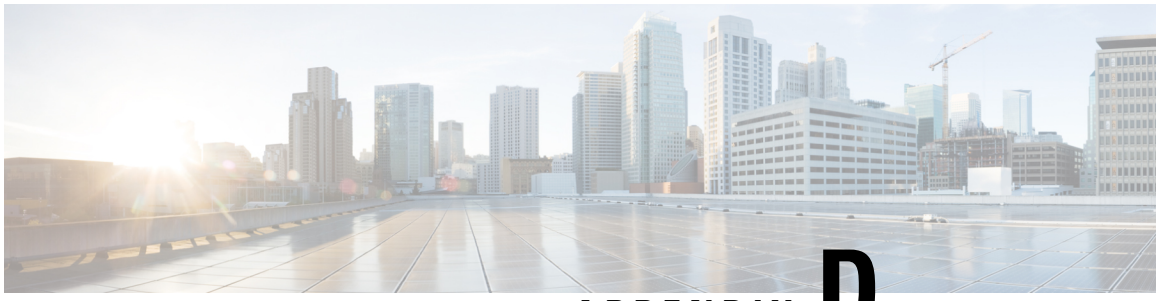
Deployment enforcement is done for the infra tenant as well as for user tenants. If CAPIC1 is deployed in the account IA1 in the region R1 and is also trying to manage the regions R2 and R3, another Cisco Cloud APIC (for example, CAPIC2) trying to manage the same account IA1 for regions R1, R2 and R3 would not be allowed.

The validation for the tenant-region ownership is done using AWS Resource Groups. For every tenant-region combination, a Resource Group is created using the syntax CloudAPIC_*TenantName_Region* (for example, the name CAPIC_TA1_R2 would be created if a tenant is deployed in account TA1 in region R2). It would also have an ownership tag of IA1_R1_TA1_R2, if the Cisco Cloud APIC is deployed in account IA1 in region R1.

Following are examples of situations where there might be an AciOwnerTag mismatch, where existing tenant-region deployments would fail:

- If a Cisco Cloud APIC was initially installed in one account, was then torn down and the Cisco Cloud APIC was installed in a different account. In this case, all existing tenant-region deployments would fail if you try to manage the same tenant-region combinations again.
- If a Cisco Cloud APIC was initially installed in one region, was then torn down and the Cisco Cloud APIC is installed in a different region. In this case, all existing tenant-region deployments would fail.
- If another Cisco Cloud APIC is managing the same tenant-region.

In ownership mismatch cases, Cisco Cloud APIC does not perform a retry of the tenant-region setup again. To resolve ownership mismatch cases, if you are positive that no other Cisco Cloud APIC is managing the same tenant-region combination, log in to the tenant's AWS account and manually remove the affected Resource Group (for example, `CAPIC_123456789012_us-east-2`). Then either reload the Cisco Cloud APIC instance or delete the tenant from the Cisco Cloud APIC and add it again.



APPENDIX D

Locating CSR and Tenant Information

Locating CSR and Tenant Information

There are several pieces of Cisco Cloud Services Router (CSR) and tenant information that you need to enable connectivity between the Cloud APIC and the ISN devices. You should be able to get this information through ACI Multi-Site Orchestrator (**Sites** > **Configure Infra** > **Download IPN Device Config files only**). However, if you find that you need to manually gather the CSR and tenant information, the following sections provide instructions for locating this information.

Information for the Cloud CSR

Necessary AWS Information	Your Entry	How To Locate This Information in the AWS Site
Elastic IP address of the third network interface of a cloud CSR		1. Go into **Instances** in the EC2 Dashboard in the AWS Management Console. 2. Choose a CSR instances (click the box next to a CSR instance). 3. Scroll down until you see `Network interfaces` on the right side, then click the `eth2` link and locate the IP address shown in the `Public IP address` field.
Public IP address for a cloud CSR		1. Go into **Instances** in the EC2 Dashboard in the AWS Management Console. 2. Locate a CSR instance. 3. Copy the IP address shown in the `IPv4 Public IP` column for that CSR instance.

Necessary AWS Information	Your Entry	How To Locate This Information in the AWS Site

Preshared key for a cloud CSR		1. Log into a cloud CSR:
		`ssh ip-address`
		where *ip-address* is the public IP address for the cloud CSR.
		2. Get the crypto keyring information:
		`show running-config | include pre-shared-key`
		Output similar to the following appears, where the preshared key is highlighted:
		`pre-shared-key address 192.0.2.15 key 12345678900987654321234567890`

Peer tunnel IP address for the on-premises IPsec device to a cloud CSR		1. Log into a cloud CSR:
		`ssh ip-address`
		where *ip-address* is the public IP address for the cloud CSR.
		2. Enter the following command:
		`show ip interface brief | include Tunnel2`
		Output similar to the following appears:
		`Tunnel2 30.29.1.1 YES NVRAM up down`
		3. Take the IP address for this tunnel and increment the address by one to get the peer tunnel IP address for the on-premises IPsec device to the cloud CSR.
		For example, if the IP address shown in the output is 30.29.1.1, then the peer tunnel IP address for the on-premises IPsec device to the cloud CSR would be 30.29.1.2.

Information for the Infra Tenant

Necessary AWS Information	Your Entry	How To Locate This Information in the AWS Site
Cloud Account ID for infra tenant		Use the AWS account for the infra tenant as described in Deploying the Cloud APIC in AWS, on page 19.

Necessary AWS Information	Your Entry	How To Locate This Information in the AWS Site
Cloud Access Key ID and Cloud Secret Access Key for infra tenant		1. Log into the Amazon Web Services account for the infra tenant. 2. Go to IAM. 3. In the left pane, select **Users**. 4. Click the link for your admin account. 5. On the Summary page, click the **Security credentials** tab. 6. Click **Create access key** if you do not already have an Amazon Web Services access key ID. 7. Locate the information from the **Access key ID** and **Secret access key** fields.

Information for the User Tenant

Necessary AWS Information	Your Entry	How To Locate This Information in the AWS Site
Cloud Account ID for Cisco Cloud APIC user tenant		Use the AWS account for the user tenant as described in Setting Up the AWS Account for the User Tenant, on page 22.
Cloud Access Key ID and Cloud Secret Access Key for Cisco Cloud APIC user tenant		1. Log into the Amazon Web Services account for the user account. 2. Go to IAM. 3. In the left pane, select **Users**. 4. Click the link for your Cloud APIC user tenant account. 5. On the Summary page, click the **Security credentials** tab. 6. Click **Create access key** if you do not already have an Amazon Web Services access key ID. 7. Locate the information from the **Access key ID** and **Secret access key** fields.

Locating CSR and Tenant Information