

Cisco Cloud ACI Network Factory for AWS Control Tower

Table of Contents

Foreword	3
Solution overview and features	4
Architecture diagram	6
Pre-requisites	7
Deployment and Configuration Steps	10
What to expect	11
Additional Considerations	14
Best Practices	16
Solution Estimated Pricing	16
FAQs	17
Additional resources	17
Partner contact information	17

Foreword

The Cisco Cloud ACI (Application Centric Infrastructure) is an advanced multi-tenant cloud/hybrid-cloud networking automation solution. It uses an abstracted policy model to automate the provisioning and management of multi-tenant AWS networks that can span across multiple AWS regions, and/or connect to the on-premises data centers. The integration of Cisco Cloud ACI and AWS Control Tower allows the full AWS network automation, starting from account creation to Cloud ACI multi-tenant policy configuration that renders the actual AWS networking infrastructure with AWS native network components, such as VPCs, TGWs, IGWs, Security Groups, etc.

The purpose of this AWS Implementation Guide is to enable AWS Cisco Cloud ACI customer to seamlessly activate, deploy and configure the Cisco Cloud ACI site with the AWS Transit Gateways for inter-VPC and/or inter-regional connectivity in AWS Control Tower environment while taking full advantage of the resources pre-configured by AWS Control Tower as part of the initialization.

Solution overview and features

AWS Control Tower creates an abstraction or *orchestration* layer that combines and integrates the capabilities of several other [AWS services](#), including AWS Organizations, AWS Single Sign-on, and AWS Service Catalog. AWS Control Tower provides the easiest way to set up and govern a secure, compliant, multi-account AWS environment based on best practices established by working with thousands of enterprises. Central cloud administrators know that all accounts are aligned with centrally established, company-wide compliance policies.

AWS Marketplace offers third-party software integrated solutions with [AWS Control Tower](#). These solutions help solve common infrastructure and operational use cases. Those use cases include identity management, security for a multi-account environment, centralized networking, operational intelligence, and Security Information and Event Management (SIEM). The Cisco Cloud ACI solution with AWS Control Tower augments the centralized networking use case.

Cisco Cloud ACI on AWS:

1. Provides an advanced automation solution for AWS cloud/hybrid cloud networking
2. Provides a REST interface to configure AWS network infrastructure deployment automation
3. Accepts Cisco ACI Policy Model and other cloud-specific policies directly from the Cloud APIC controller for a specific AWS cloud site or from [Cisco Multi-site Orchestrator](#) in a hybrid-Cloud multi-site environment.
4. Performs endpoint discovery in AWS
5. Performs Cisco Cloud ACI Policy translation to the AWS native network policy
6. Configures the Cisco CSR1000v control plane for on-premises connectivity via IPsec VPN or AWS Direct Connect
7. Configures the data-path between the on-premises Cisco ACI Fabrics and the AWS cloud site

The Cisco Cloud ACI network solution with AWS Control Tower sets up network baselines such as VPCs and inter-VPC connectivity with AWS Transit Gateway with automated IP address management and more. Customers can utilize the solution to serve as a network factory within AWS Control Tower. This solution leverages the Account Factory in AWS Control Tower to provision AWS accounts. After an account is provisioned, a lambda lifecycle hook triggers API automation in Cisco Cloud ACI to provision a secure, best practice network blueprint consisting of an AWS VPC with subnets, secure access to the internet, and out of the box connectivity with a shared multi-account AWS Transit Gateway running in the Network Account of the Infrastructure OU.

The solution relies on *ApicTenantRole*, a cross account AWS Identity and Access Management (IAM) role that provides access to resources in the Business OU Account, which is a managed account in AWS Control Tower. This cross account IAM role is assumed by the cloud APIC Controller to provision and orchestrate the network infrastructure in the managed account. Cisco Cloud ACI uses the ACI group-based policy model to describe the abstracted network intends. It then performs network policy translation from the ACI policy to AWS EC2 Networking services. The diagram below depicts the policy mapping:

ACI Policy Model

Tenant
VRF
BD Subnet
EP to EPG Mapping
EPG
Taboo
Contracts, Filters
Consumed contracts
Provided contracts
End Point

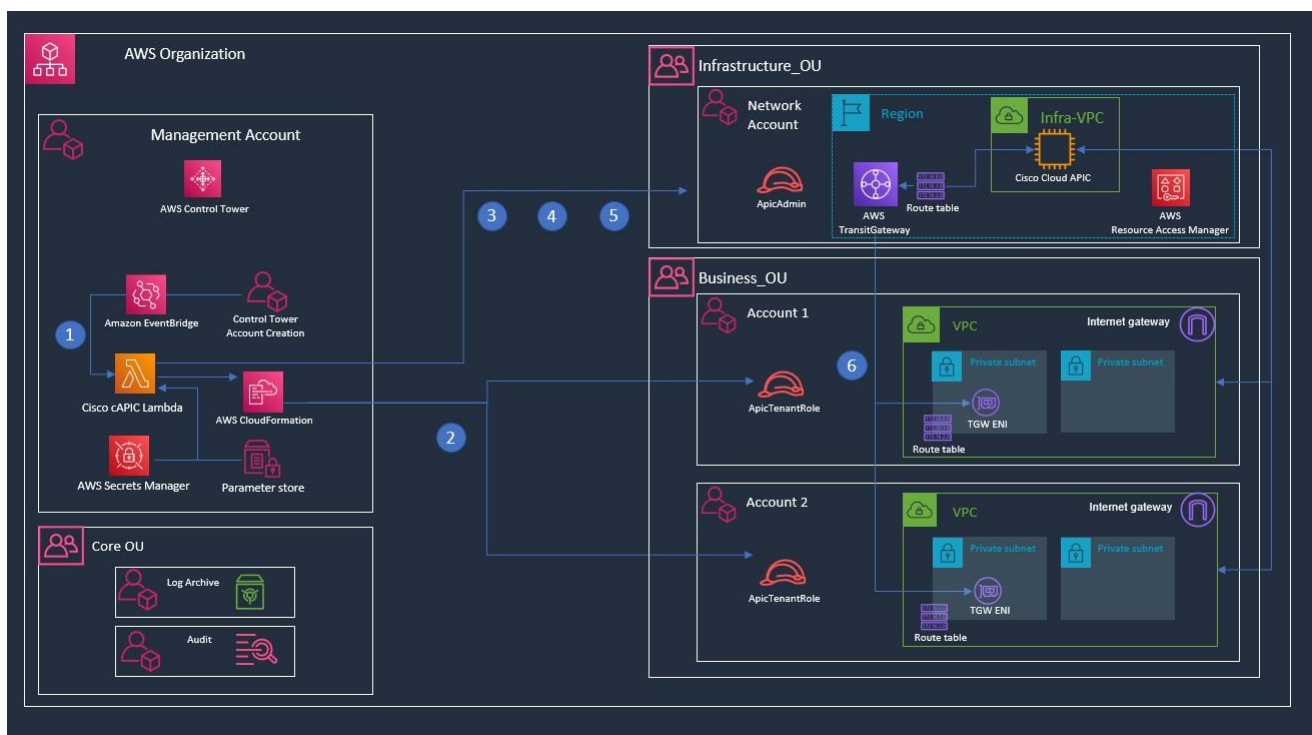
AWS Policy Model

User Account
Virtual Private Cloud
VPC subnet
Tag / Label
Security Group
Network Access List
Security Group Rule
Outbound rules
Inbound rules
EC2 Instance
Network Adapter

Source/Destination: Subnet or IP or Any or 'Internet'
Protocol
Port

Architecture diagram

Figure: Cisco Cloud APIC multi-account network architecture diagram



The creation of a multi-account network blueprint is an automated multi-step process. The workflow captured in the network architecture above is detailed below:

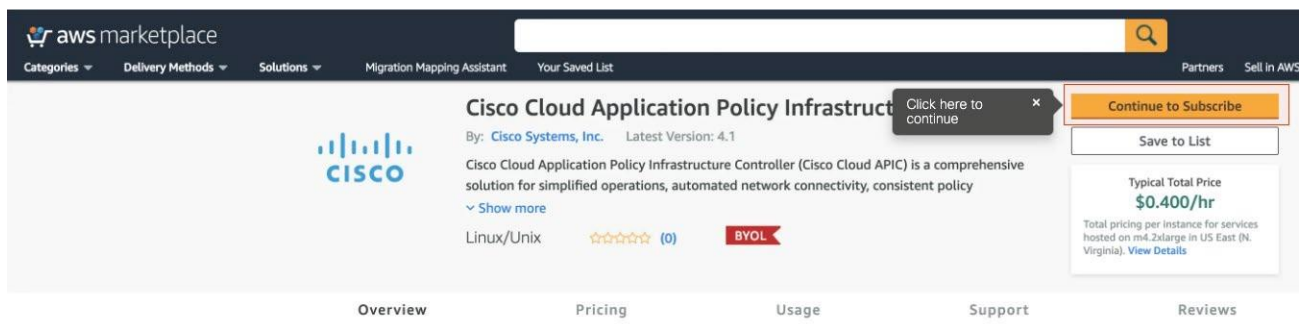
1. When a new AWS Account is created in a Business OU using Account factory, a life cycle event is generated. This event triggers the Cisco Cloud APIC lambda
2. The lambda deploys a CloudFormation stack Instance to create a cross account role from Network account in Infrastructure_OU to Account1 in Business_OU_A (the account created in step 1)
3. The Lambda makes a Cloud APIC API call to create and register the Account1 as a tenant in the Cloud ACI model
4. The Lambda makes a Cloud APIC API call to create an ACI policy configuration that deploys an AWS VPC with an AWS Internet Gateway in Account1 via Cloud APIC.
5. The Lambda makes a Cloud APIC API call to create subnets in the AWS VPC created in Step 4 in Account1
6. cAPIC attaches the VPC to TGW via a VPC attachment and configures corresponding routes based on ACI policy configuration in the VPC subnet route table to point to the AWS Transit Gateway.

Note:

1. By default, the communication between VPCs of Business OU Accounts are disallowed. The inter-VPC connectivity can be customized via Cisco Cloud ACI policies through EPG contracts.
2. This solution cannot be used to manage networking resources on 3 shared accounts of AWS Control Tower, which are the master account and isolated accounts for log archive and security audit. These three shared accounts are meant for AWS Control Tower functionality and it is not common to have networking resources in these accounts.

The following pre-requisite steps need to be performed before deploying the solution:

1. Setup AWS Control Tower in an existing AWS Organization or a new Organization
2. Create an Infrastructure_OU in your AWS Control Tower
3. Provision a Network Account in the Infrastructure_OU using the [Account Factory Enroll Account](#) feature. Provisioning a new account could take around 30 minutes
4. In the Network account, subscribe to the Cisco Cloud Application Policy Infrastructure Controller (APIC) on [AWS Marketplace](#).



5. [Deploy and setup](#) Cisco Cloud APIC and a Cloud ACI site in the Network Account.
 - i. During the **“Region Management”** setup process, select the **“TGW Enabled”** checkbox and select the AWS regions that you plan to deploy your VPCs

Use Transit Gateway ☒ Enabled

Regions to Manage *

Region Name	Region	Cloud Routers	Inter-Site Connectivity	TGW Stats
<input type="checkbox"/> Asia Pacific (Tokyo)	ap-northeast-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Asia Pacific (Seoul)	ap-northeast-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Asia Pacific (Osaka-Local)	ap-northeast-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Asia Pacific (Mumbai)	ap-south-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Asia Pacific (Singapore)	ap-southeast-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Asia Pacific (Sydney)	ap-southeast-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Canada (Central)	ca-central-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> EU (Frankfurt)	eu-central-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> EU (Stockholm)	eu-north-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> EU (Ireland)	eu-west-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> EU (London)	eu-west-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> EU (Paris)	eu-west-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> South America (São Paulo)	sa-east-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> US East (N. Virginia)	us-east-1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> US East (Ohio)	us-east-2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> US West (N. California)	us-west-1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> US West (Oregon)	us-west-2 <small>Cloud APIC Deployed</small>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

- ii. The cloud router (CSR 1Kv) is an optional component required only if the VPCs need on-prem connectivity. On-prem connectivity via CSR1Kv cloud router is not in the scope of this solution
- iii. This solution expects you to configure all appropriate regions and create a Hub network in Cloud APIC management console. If this is not configured already as part of the setup process earlier, follow below steps to configure this on the Cloud APIC UI:
 - a. Navigate to **Infrastructure, Inter-Region Connectivity** choose **Edit Region Management**
 - b. In **Setup – Region Management** screen, select **Enabled** under Use Transit Gateway
 - c. Under **Regions to Manage** select all applicable regions. Note down these regions list, you may want to pass this as parameter while deploying the solution in next section.
 - d. Click **Next**
 - e. Under Hub Network, choose **Add Hub Network** and create a hub network with unique BGP ASN. Note down the name of the Hub network, you need to provide the hub network name while deploying the solution in the next section.
Note: Please ensure that the BGP ASN is unique. The Hub network ASN cannot be modified later.

A single hub network can be used globally across AWS Transit Gateways across multiple regions.

Hub Network

Hub Networks ⓘ

Name	BGP Autonomous System Number
hub1	64521

+ Add Hub Network

6. Configure Cisco Cloud APIC license via [Cisco Smart Licensing](#)
 - a. Navigate to **Administrative > Smart Licensing** on the Cisco Cloud APIC UI
 - b. Follow the on-screen prompt to register Cloud APIC smart licensing
7. Copy the lambda function from the cisco ACI control tower GitHub repository <https://github.com/datacenter/cloud-aci-aws-control-tower> to an Amazon S3 bucket in AWS Control Tower home Region in the Management account.
 - a. Login to the Management account and select the **Region** where you enabled AWS Control Tower. You could use <https://console.aws.amazon.com/controltower/> to get in to AWS Control Tower home region.
 - b. Go to Amazon S3 Console and select **Create Bucket**. You could use <https://console.aws.amazon.com/s3/bucket/create> to open the create bucket screen directly.
 - c. Enter the **Bucket name** as *capic-lambda-<Your-AWS-Account-Id>-<Your-Region>*. Note down the Bucket name, you need it while deploying the solution.
 - d. Leave all the defaults and choose **Create bucket**. Copy the bucket name and save it as you will need it in the proceeding steps.
 - e. Download the *capic_deployment_package.zip* file from the following GitHub location: https://github.com/datacenter/cloud-aci-aws-control-tower/raw/main/functions/capic_deployment_package.zip
 - f. Upload the *capic_deployment_package.zip* file to the S3 bucket you just created.

Additional Considerations

- CIDR and Subnet management

This solution queries for the list of all allocated CIDR values from Cisco Cloud APIC and assigns a non-overlapping CIDR value to each new VPC that gets created. The CIDR range depends on the Parameters '**BaseCIDRRange**' and '**MaskLength**' that you provided while launching the solution.

As an example, with the default values of **BaseCIDRRange=10.0.0.0/16** and **MaskLength=24**, the solution will create VPCs with /24 CIDR range within the 10.0.0.0/16 network CIDR. The IPAM logic can detect overlapping CIDRs and only allocates an unused CIDR to a VPC. The entire CIDR range will be divided in to 2 to the subnet count (select) power and allocates the first set of CIDRs to the subnets and leaves the remaining subnets to allocate later as

needed. As an example, when 4 subnets are select, the VPC CIDR is divided in to 2 to the power of 4, total 16. The first 4 values are assigned to the subnets.

- Multi-region deployment

In order to provision VPCs in multiple regions, make sure the regions are selected in Region Management configuration in Cloud APIC. Refer to pre-requisites for configuration steps. In addition, you must provide these regions as comma separated values for the VPCRegion input parameter in the cloudformation template deployed in step 1.3e above. For multi-region deployments Cisco Cloud ACI provisions AWS Transit Gateways in each region and auto-configures inter-region peering attachments with unique ASNs and static routes. Every time a new account is enrolled into AWS Control Tower, it will create VPCs, Subnets and attach the VPCs as AWS VPC attachments to the AWS Transit Gateway in its respective region.

- TGW Routing

By default, Cisco Cloud ACI programs a route in the VPC subnet route table with that specifies AWS transit Gateway as the next hop for all inter-VPC traffic. Within the AWS Transit Gateway, Cisco Cloud ACI programs dedicated route tables for each user account/tenant with its VPCs. In each of the AWS Transit Gateway route tables, only the attached VPC's routes are propagated by default. In addition, for multi-region connectivity, there is a static route configured in the Transit Gateway route table that points to the peered attachment's network CIDR and attachment-id. For the peering attachment, routes from each of the attached VPC in a given region are propagated into the peering attachment route table.

By default, Cisco Cloud ACI does not program routes for inter-VPC communication i.e. traffic between VPCs within a region is not permitted. To allow inter-VPC traffic, EPG contracts can be programed from within the Cisco Cloud ACI. For more information on how to configure EPG contracts within Cisco Cloud ACI, refer to the following [link](#).

- Updating Solution Deployment Parameters

When you deployed this solution, you provided values to a set of Cloud APIC infra account

parameters like *cAPICloudInfraAddress*, *cAPICAdmin*, *AdminPassword*, and *cAPICHubNetworkName*. You also defined parameters like *BaseCIDRRange*, *MaskLength*, *NumberOfSubnets*, and *VPCRegion*. All these parameters can be changed by [updating the CloudFormation stack](#) with new values.

Please note that when you update the values in CloudFormation stack, the new settings are applied only to any new accounts that are created after the update. Updating existing accounts is not in the scope of this solution.

Solution Estimated Pricing

There are no additional charges for AWS Control Tower. However, you would incur costs for underlying services that AWS Control Tower uses. The services include, AWS Service Catalog, AWS CloudTrail, AWS Config, Amazon CloudWatch, Amazon Simple Notification Service (SNS), Amazon S3, and VPC based on your usage. You only pay for what you use. Refer to [AWS Control Tower pricing](#) page for additional details.

The Cisco Cloud ACI network factory for AWS Control Tower leverages the following additional components:

1. AWS Transit Gateway as a network hub. Refer to [AWS Transit Gateway pricing](#) page for additional details.
2. Cisco Cloud APIC from [AWS Marketplace](#). Refer to [AWS EC2 pricing page](#) for cloud APIC EC2 instance consumption charges
3. In addition to EC2 consumption charges, customers will pay for the Cisco Cloud ACI license which can be procured via [Cisco Smart Licensing](#).
4. [Optional]: Cisco CSR 1000v from [AWS marketplace](#). This is only needed if you want to extend the connectivity for Cloud ACI to on-premises ACI network.

CISCO ISE/ ACI/SD-WAN/ SD-ACCESS/ AI

50% OFF HURRY UP!



+91 8792633595
+91 9986886992



Mr. AZAM BASHA
(Senior Network Architect)