



Deploying the Cisco Application Services Engine in AWS (Fabric External Mode)

- [Prerequisites, on page 1](#)
- [Deploying the Cisco Application Services Engine in AWS, on page 2](#)
- [Enabling Username Password based Authentication, on page 5](#)

Prerequisites

Complete the following one time pre-requisites before you start:

1. Create a VPC (Virtual Private Cloud):

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances.

- Choose **Networking & Content Delivery Tools > VPC**.
- Click **Your VPCs**. Click **Create VPC > Create**.
- Enter the **Name Tag**. This creates a tag with a key of 'Name' and a value that you specify.
- Enter the **IPv4 CIDR block** in block format. It is the range of IPv4 addresses for your VPC in CIDR block format. Block sizes must be between /16 netmask and /28 netmask. For example, 10.0.0.0/24.

2. Create the Internet Gateway. Internet gateway is a virtual router that allows a VPC to connect to the internet.

- Choose **VPC Dashboard > Internet Gateway**. Click **Create Internet Gateway > Create**.
- Enter the **Name Tag**. To create a new internet gateway specify the name for the gateway . This creates a tag with a key of a 'Name' and a value that you specify.
- Click **Actions**. Select the **Name Tag** created in the previous step. Choose **attach to VPC** from the drop-down menu. Choose the VPC created in step 1 to create the internet gateway.

3. Create Route Tables. Create route tables to connect the subnets within your VPC, the internet, and internet gateway to Cisco Application Services Engine.

- Click **VPC Dashboard > Route Tables**. Select the route table that has been already created for the VPC from Step 1.

- Click **Routes** > **Edit routes**.
- Click **Add route**. Enter the external subnet in the **Destination** field. Enter the Internet gateway created in step 2 in the **Target** field. Click **Save Routes**.

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

- Access to the Cisco Application Services Engine Amazon Machine image (AMI).
- Verify that you have a full administrator access on the AWS.
- You have permissions to launch Elastic Compute Cloud (m4. 2 x large EC2), which functions as a virtual machine (VM) for the applications running in the cloud. For the purpose of installing Cisco Application Services Engine cluster, permissions to launch more than 3 instances are recommended.

Deploying the Cisco Application Services Engine in AWS

Cisco Application Services Engine can be deployed in the fabric external mode using a CFT template for the AWS.

Step 1 Log into your Amazon Web Services account and navigate to the AWS Management Console:

<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 the AWS where the Cisco Application Services Engine AMI image will be brought up.

Step 3 Create an Amazon EC2 SSH key pair:

- Click the **Services**, then click **EC2** link.
- Click **Key Pairs** under **Resources**.

The key pair, consisting of a private key and a public key, is a set of security credentials that is used to prove your identity when connecting to an instance.

- Click **Create Key Pairs**.
- Enter a unique name for this key pair.

The name can be up to 255 characters long. Valid characters include `_`, `-`, `a-z`, `A-Z`, and `0-9`.

- Choose the **pem** file format (for use with OpenSSH), then click **Create Key Pairs**. 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 later step.

Step 4 In the AWS Marketplace, search for the Cisco Application Services Engine page.

The Cisco Application Services Engine page in AWS appears.

Step 5 Click **Continue to Subscribe**.

Step 6 Review and click the **Accept Terms** to accept the End User License Agreement (EULA).

Step 7 After a minute, Subscription should be processed message is displayed and **Subscribe to the Software** page appears. Click **Continue to Configuration**.

The **Configure this software** page appears.

Step 8 Select the following parameters:

- **Fulfillment Option:** Cloud Formation Template and select Cisco Application Services Engine cloud.
- **Software Version:** Select the applicable release.
- **Region:** Region where Cisco Application Services Engine for cloud formation template will be deployed.

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

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

Step 10 From the **Choose Action**, select **Launch CloudFormation** and click **Launch**.

Step 11 The **Create Stack** page appears.

Step 12 In the **Specify Template** field, choose **Amazon S3 URL** as the template source. This will be populated automatically.

Step 13 Click **Next**.

Step 14 Enter the following information on the **Specify Stack Details** page.

- **Stack Name**

- **Stack name:** Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

`SE-Cluster`

- **Parameters for SE Cluster Configuration**

- **VPC Identifier:** It is the VPC ID required for the Cisco Application Services Engine cluster. The VPC was created as a prerequisite.

`vpc-038f83026b6a48e98 (10.21.0.0/16)`

- **SE Cluster subnet-CIDR:** It is the VPC Subnet CIDR block required for the launch in Cisco Application Services Engine cluster.

`10.21.1.0/24`

- **Host name:** Service node name must be alphanumeric characters separated by '-'.
Example: `aws-se-node`

`aws-se-node`

- **Node DNS domain:** Node domain name must be alphanumeric characters separated by '-' or '!'.
Example: `user.local`

`user.local`

- **NTP servers:** NTP server IP address must be in the format x.x.x.x.

`192.168.100.100`

- **Name servers:** DNS server IP address must be in the format x.x.x.x.

`2.2.2.2`

- **DNS search domains list:** DNS search domain must be of length: 6-128 characters.

`domain.com`

- **Application IP subnet:** Cisco Application Services Engine application overlay IP subnet must be in the format x.x.x.x/x.
10.101.0.0/16
- **Service IP subnet:** Cisco Application Services Engine services IP subnet must be in the format x.x.x.x/x.
10.102.0.0/16
- **Password:** Rescue-user password for the service node. The password must contain atleast 1 letter, number and special characters such as @\$!%*#?& length: 8-64 characters.
- **Confirm Password:** Re-enter the rescue-user password for the service node.
- **SSH Key Pair:** Name of an existing SSH KeyPair to enable SSH access to the Cisco Application Services Engine.
keypair

Step 15 Click **Next**.

Step 16 The **Configure stack options** page appears. Click **Next**.

Step 17 The **Review** page appears. Verify that all the information on the **Review** page is accurate.

If you see any errors on the **Review** page, click **Previous** and update the information.

Step 18 Click **Create Stack**.

The **CloudFormation** page reappears. The Cisco Application Services Engine template that you created is displayed with the text and in the **Status** column. The Cisco Application Services Engine template that you created is displayed with the text **CREATE_IN_PROGRESS**.

Step 19 Wait for 5-10 minutes, until the **CREATE_COMPLETE** message is shown before proceeding.

a) Click **Services**, then click the **EC2** link.

The **EC2 Dashboard** page appears.

b) In the **EC2 Dashboard** page, navigate to the text containing the number of running instances in the **Resources** area. Click this **Running instances** link.

The **Instances** page appears.

c) Wait for 5-10 minutes, until you see that Cisco Application Services Engine instance is ready before proceeding. When the instance is ready, it displays 2/2 checks under the **Status Checks** tab. All the three Cisco Application Services Engine instances should display the 2/2 checks.

Step 20 After all the three Cisco Application Services Engine instances display the 2/2 checks, wait for 5-10 mins. Log in to the SSH node using the public IP address of Cisco Application Services Engine instance using the command **ssh -i pem-filename.pem rescue-user@service-engine-ip**

Step 21 After you log in to SSH, execute the following command:

```
bash-4.2$ acidiag health
All components are healthy
bash-4.2$
```

Verify that “healthy” status is displayed to indicate that the installation was performed successfully.

Step 22 Cisco Application Services Engine is available to deploy the apps that can be hosted on the Cisco Application Services Engine.

Note Cisco Application Services Engine, Release 1.1.2 supports the deployment of only the Cisco ACI Multi-Site Orchestrator application (starting with Release 2.2(3)). Refer to the [ACI Multi-Site Orchestrator Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide](#) for more information

Enabling Username Password based Authentication

When the Cisco Application Services Engine is deployed in AWS (.ami), you must login using the certificate (.pem file) that you created during the Cisco Application Services Engine deployment.

```
ssh -i pem-filename.pem rescue-user@service-engine-ip
```

By default only cert based authentication are allowed on AMI service nodes.

Enable the Username / password based authentication on each service node individually by executing the following command:

acdiag loginprompt enable / disable

