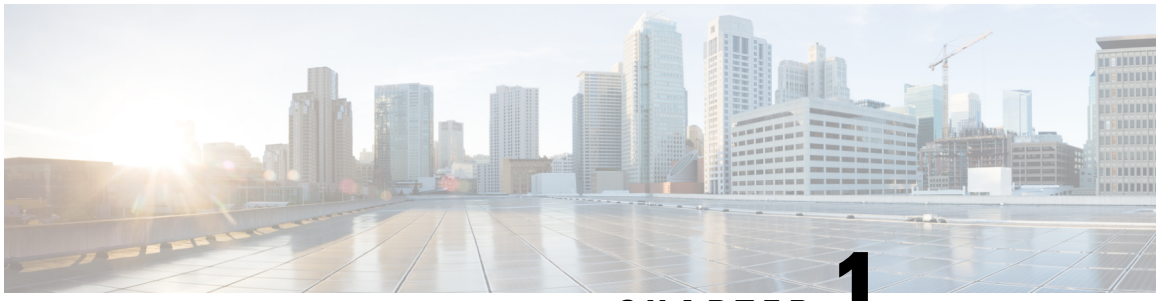
Cisco Application Services Engine Installation Guide, Release 1.1.2

First Published: 2019-12-17

Last Modified: 2020-02-27

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

CONTENTS



CHAPTER 1

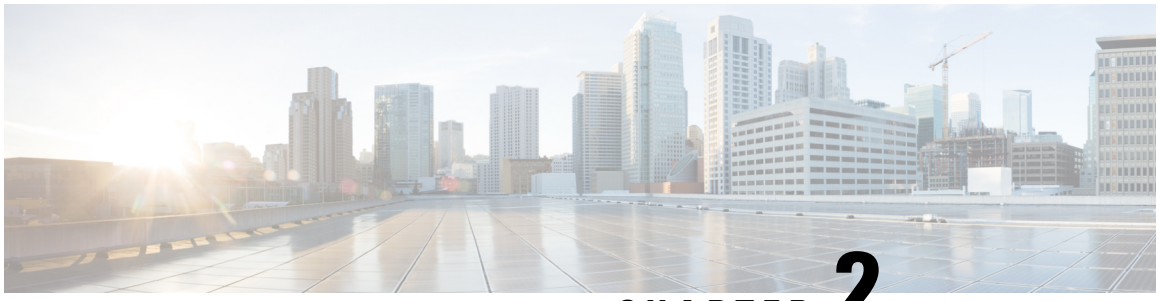
New and Changed

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the Cisco Application Services Engine, Release 1.1.2

Table 1: New Features and Changed Behavior in the Cisco Application Services Engine, Release 1.1.2

Feature	Description	Release	Where Documented
Cisco Application Services Engine	This guide was first published.	1.1.2	



CHAPTER 2

Deployment Modes for Cisco Application Services Engine

Cisco Application Services Engine Overview

Cisco Application Services Engine provides a common platform for deploying Cisco Data Center applications. These applications provide real time analytics, visibility, and assurance for policy and infrastructure.

Cisco Data Center apps are resource intensive applications that rely on modern technology stacks. Cisco Application Services Engine can host containerized applications on a common platform.

Cisco Application Services Engine is deployed as a cluster of three service nodes. This clustering provides reliability and high-availability software framework.

Cisco Application Service Engine can be deployed in two modes :

- **Fabric internal mode:**

  In the fabric internal mode, the configuration is obtained from the Cisco Application Services Engine app running on Cisco APIC. The node is automatically discovered by the Cisco ACI fabric. The registration, managing nodes, and roles management is performed using Cisco APIC.

  Note Only Cisco Network Insights Resources application and Cisco Network Insights Advisor application are supported on fabric internal mode.

  Only the physical form factor is supported fabric internal mode.

  Refer to Cisco Application Services Engine Release Notes for more information.

- **Fabric external mode:**

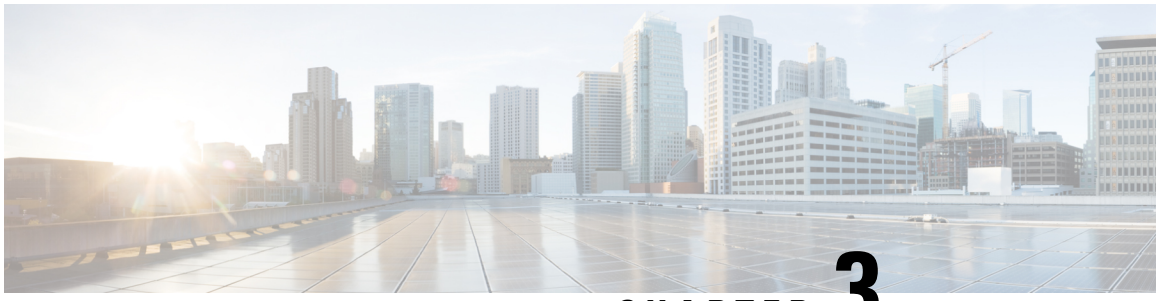
  In this mode, the Cisco ACI fabric does not provide the configuration and roles. Cisco Application Services Engine can be deployed in the fabric external mode using a number of different form factors, such as:

  - Physical appliance form factor:

- Deploying the Cisco Application Services Engine in a Physical Appliance (ISO) (Fabric External Mode).

- Virtual form factors:
  - Deploying the Cisco Application Services Engine in AWS (Fabric External Mode).
  - Deploying the Cisco Application Services Engine in VMware vCenter (OVA) (Fabric External Mode).
  - Deploying the Cisco Application Services Engine in KVM (Fabric External Mode).

Note Cisco Application Services Engine, Release 1.1.2 (fabric external mode only) supports the deployment of only the Cisco ACI Multi-Site Orchestrator application (starting with Release 2.2(3)).



CHAPTER 3

Deploying the Cisco Application Services Engine in Fabric Internal Mode

Prerequisites

- You have access to the Cisco APIC, Release 4.1 or later.
- You have the IP addresses, subnet mask, and gateway information for the Cisco Application Services Engine appliance.
- Cisco Application Services Engine is deployed as a cluster, using the In-band management interface to access the management network of the Cisco ACI fabric. Make sure that the In-Band IP address configuration is completed before setting up the Cisco Application Services Engine app.

Note See the Cisco APIC and Static Management Access for information on network connectivity.

- The Cisco APIC on the Cisco Application Services Engine allows smaller subnets. However, it is recommended to use /16 subnets.
- You have the IP addresses of the primary and secondary DNS server.
- You have the IP addresses of the primary and secondary NTP server.

Workflow for Setting Up the Cisco Application Services Engine App

Use this procedure to deploy and set up the Cisco Application Services Engine app from the Cisco Data Center App Center.

Step 1 Adding Cisco Application Services Engine to Cisco APIC
Step 2 Configuring the Cisco Application Services Engine Cluster
Step 3 Registering the Service Node

Adding Cisco Application Services Engine to Cisco APIC

Use this procedure to download the Cisco Application Services Engine app from the Cisco DC App Center and add it to Cisco APIC.

Step 1 Log in to the Cisco DC App Center as an end user.

The **Introducing the Cisco App Center** banner appears.

Step 2 On the **Introducing the Cisco App Center** banner, click **Browse apps** to view the available apps.

The apps available for download are displayed in the **All** window.

Step 3 Search for the Cisco Application Services Engine app and click **Download**.

Step 4 Review the license agreement and click **Agree and download**.

The Cisco Application Services Engine app is downloaded to your local machine.

Step 5 Log in to the Cisco APIC as an admin user.

Step 6 On the menu bar, choose **Apps**, then click **All Apps**. Click the + icon to add an app.

Step 7 Click **Browse** and locate the Cisco Application Services Engine app.

Step 8 Click **Submit** to upload the app.

After the Cisco Application Services Engine app is uploaded, the thumbnail of the app is displayed under the **All Apps** tab.

Step 9 Click **Install** to install the Cisco Application Services Engine app. You can also select **Install** from the **Actions** drop-down list to install the Cisco Application Services Engine app.

Once the Cisco Application Services Engine is installed, it is displayed on the **Apps** tab.

Step 10 To launch Cisco Application Services Engine, select the app from the **Apps** tab.

Configuring the Cisco Application Services Engine Cluster

Use this procedure to set up the Cisco Application Services Engine cluster.

Before you begin

You have added the Cisco Application Services Engine app to the Cisco APIC.

Step 1 Log in to the Cisco APIC as an admin user.

Step 2 To launch , select the app from the **Apps** tab.

Cisco Application Services Engine

Step 3 Click **Enable**.

Step 4 Click **Open** tab on the thumbnail.

Cisco Application Services Engine

The **Welcome to Service Engine** window appears. Click **Begin Set Up** tab. Proceed in the following order:

a. The **In-Band IP Configuration** is marked with a green check mark. If not, ensure that the In-Band IP address configuration is completed before setting up the Cisco Application Services Engine app.

b. Click **Begin** set up the cluster configuration.

Step 5 In the **Cluster Configuration** page, enter a name for the cluster, following the standard host name conventions. Do not use special characters or spaces in the cluster name.

Step 6 Enter the **In-Band Management Subnet** and associate **APIC In-Band EPG** from the drop-down list.

Cisco Application Services Engine

Step 7 Enter the **App Subnet** and **Service Subnet** IP addresses.

We recommend to use /16 app subnet.

Step 8 Enter the **VLAN** range. The default range is 100-200. Do not include the infra VLAN.

Step 9 Click **Next**.

Step 10 Enter the **NTP Servers** hostname or the IP address.

Step 11 Enter the **DNS** domain name and DNS provider.

More than one NTP server and DNS provider can be added.

Step 12 Click **Save and Finish**.

Registering the Service Node

Use this procedure to register the service node.

Before you begin

- You have configured the Cisco Application Services Engine cluster.

Step 1 Click **Begin** to set up the **Service Node Registration**.

Step 2 If the service nodes are detected, perform the following action:

a) Select a service node and click **Register**.

b) The **Name** and the **Serial Number** of the appliance are auto populated.

Step 3 If the service nodes are not detected, perform the following action:

a) From the **Actions** drop-down list, click **Register new node**.

b) Enter the **Name** and the **Serial Number** of the appliance.

Step 4 Enter the **In-Band Management**. This should be the same as the cluster's In-Band subnet.

Step 5 Enter the **Out-of-Band Management** and **Out-of-Band Gateway** IP addresses for each service node.

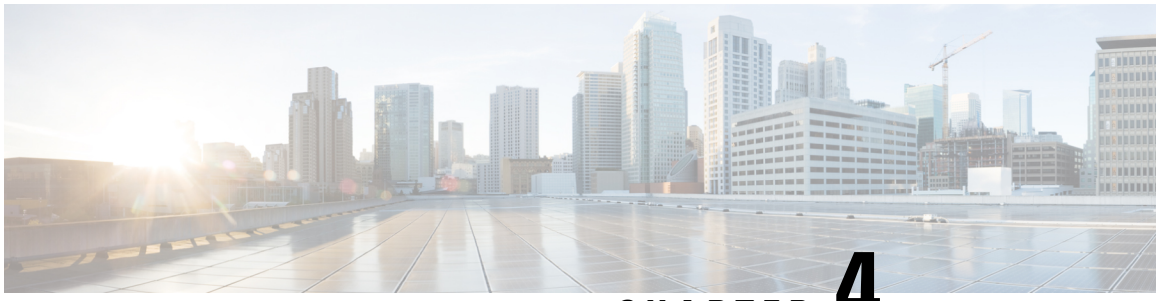
Step 6 Click **Save**.

Step 7 Repeat steps 1- 5 for each service node.

Step 8 Click **Dashboard** to return to the app page.

Cisco Application Services Engine

The dashboard shows the cluster configuration and registered service nodes. The **Operational State** of the service nodes should be **Active**.



CHAPTER 4

Deploying the Cisco Application Services Engine in a Physical Appliance (ISO) (Fabric External Mode)

Prerequisites

Complete the following pre-requisites before you start:

- For configuring the Cisco Application Services Engine, you must provide application overlay network. This network must not overlap with any other services in your fabric.
- You must have a NTP server configured in your environment. You must have provided the NTP server information as part of the Cisco Application Services Engine installation procedure.

Note All nodes for fabric internal deployment must be in POD1.

Deploying the Cisco Application Services Engine in a Physical Appliance (ISO)

This procedure is used for setting up fabric external mode of the Cisco Application Services Engine cluster.

Step 1 Download the Cisco Application Services Engine image.

a) Navigate to the Software Download page.

b) Choose the Cisco Application Services Engine ISO image (apic-sn-dk9.1.1.2h.iso).

Step 2 Begin the apic-sn setup utility.

a) Specify the mode. To specify that the configuration is not obtained from the Cisco APIC cluster enter **n**.

b) Enter the serial number and a unique hostname for the service node.
c) Enter the domain name for the service node. The domain name is equivalent to the name of the cluster or the domain name of the fabric.
d) Enter the password for the rescue-user.

```
Setup utility for apic-sn with SerialNumber CiscoSN01 and running version
2019-07-15.0-se-h1-0-gf2543725
Is this running in ACI mode? (y/n) n
Enter node hostname: atomix1
Enter node domain: atomix.local
Enter the password for rescue-user:
Reenter the password for rescue-user:
```

Step 3 Enter the physical network management IP address and mask.

The physical network management IP address is the out-of-band management IPv4 or IPv6 address used to access the Cisco Application Services Engine GUI, CLI, or API.

```
Enter physical network management IP address and mask: 192.168.3.2/24
```

Step 4 Enter the physical network gateway IP address.

The physical network gateway IP address is used for communication to the external networks using out-of-band management.

```
Enter physical network gateway IP address: 192.168.3.1
```

Step 5 Enter the number of masters in the cluster.

```
Enter number of masters in the cluster (recommended is 3) 3
```

Step 6 Enter the management IP address and serial number of the other master nodes in the cluster.

Step 7 You must assign one node in the cluster as the first master in the cluster. If the cluster already exists, enter **n**.

```
Is this the first node in a new cluster? (y/n) y
```

Step 8 Enter the application overlay network IP address and mask.

It is the private IP address block, /16 network that is required for the container or pod network.

```
Enter application overlay network IP address and mask: 1.1.0.0/16
```

Step 9 Enter the service network IP address and mask.

It is the private IP address block, /16 network that is required for the container or pod network.

```
Enter service network IP address and mask: 2.2.0.0/16
```

Step 10 Enter the search domain.

```
Enter the search domain as a space-separated list: cisco.com
```

Step 11 Enter the addresses of the DNS name servers.

It is the IP address list required for resolving DNS names outside the cluster.

```
Enter nameserver addresses as a space-separated list: 171.70.168.183
```

Step 12 Enter the IP address of the NTP servers. It is required to sync the clock between all the master nodes in the cluster.

```
Enter the ntp servers as a space-separated list: 192.168.13.101
```

Step 13 Perform steps 1- 11 on the other two service nodes.

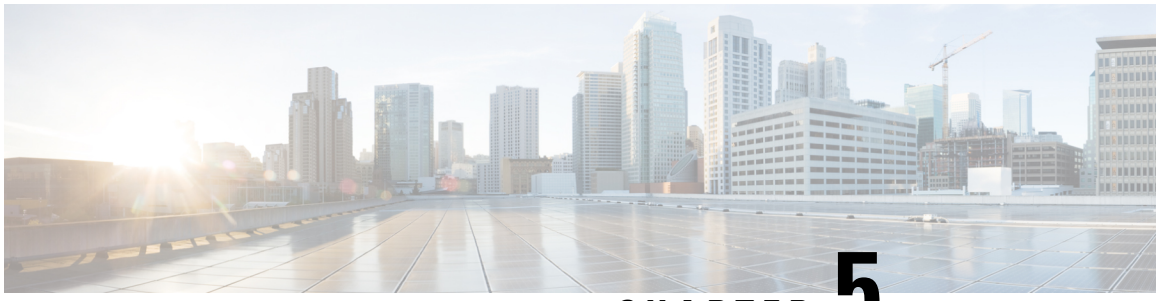
For node two and three, the management IP addresses, and the serial number of the other master nodes in the cluster are different.

Step 14 After all three service nodes are bootstrapped, wait for 15-30 mins and execute the following command:

```
Server # acidiag health
cluster is healthy
```

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

Step 15 Cisco Application Services Engine is available to deploy the Cisco MSO application.



CHAPTER 5

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

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:

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

b) 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.

c) Click **Create Key Pairs**.

d) 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.

e) 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 prerequiste.

    ```
    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 '-'.

    ```
    aws-se-node
    ```

  - **Node DNS domain:** Node domain name must be alphanumeric characters separated by '-' or '.'.

    ```
    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

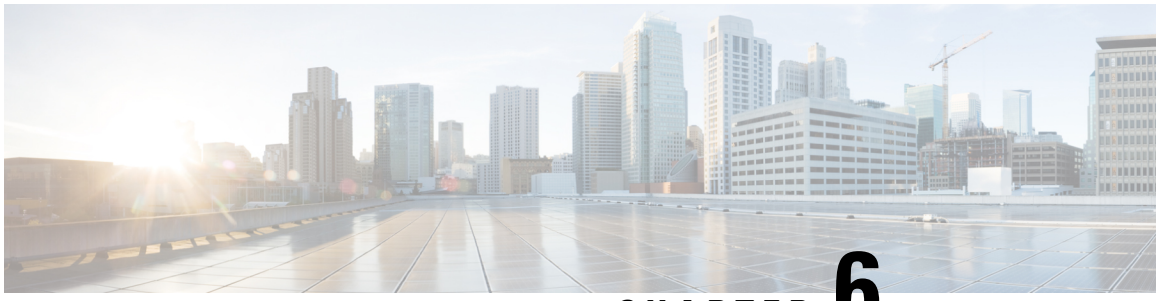
When the Cisco Application Services Engine is deployed in AWS (`.ami`), you must login using the certificate (`.pem` file) that you created during the Cisco Application Services Engine deployment.

```
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:

acidiag loginprompt enable / disable



CHAPTER 6

Deploying the Cisco Application Services Engine in VMware vCenter (OVA) (Fabric External Mode)

Prerequisites

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

- Ensure that the NTP server is configured and reachable from the Orchestrator VMs and the VMware Tools periodic time synchronization is disabled.
- Ensure that you have the required system requirements for each VM service node:
  - vCPU: 16
  - RAM : 48GB
  - Disk space: 600 GB
  - ESX version 5.5 and above

Deploying the Cisco Application Services Engine in VMware vCenter (OVA)

This section describes how to deploy the Cisco Application Services Engine using an OVA in the VMware vCenter.

Step 1 Download the Cisco Application Services Engine image.

a) Navigate to the Software Download page.

b) Choose the Cisco Application Services Engine OVA image (apic-sn-dk9-1.1.2h.ova).

Step 2 Deploy OVA using the VMware vCenter GUI or the VMware vSphere Client.

a) Right-click and select **Deploy OVF Template**.

b) The **Deploy OVF Template** wizard appears.

Step 3 On the **Select an OVF Template** page, specify the location of the source OVF or OVA template and click **Next**

a) Choose the **local file** tab.

b) Click **choose file** and select the OVA file already downloaded in Step 1. If you do not select the required files, a warning message displays.

Step 4 For Cisco Application Services Engine, we must deploy three nodes to form a cluster. On the **Select a name and folder** page, enter a unique name for the first node. Select a deployment location, and click **Next**.

Step 5 On the **Select a compute resource** page, select a resource where to run the deployed VM template, and click **Next**.

Step 6 On the **Review details** page, verify the OVF or OVA template details and click **Next**.

Step 7 On the **Select storage** page, define where and how to store the files for the deployed OVF or OVA template.

a) Select the disk format for the virtual machine virtual disks. Choose **Thick Provision Lazy Zeroed**.

b) Select the local datastore which has enough capacity to deploy the OVA.

The configuration file and virtual disk files are stored on the datastore. Select a datastore large enough to accommodate the virtual machine and all associated virtual disk files.

Note Unique datastore should be assigned to each node.

Step 8 On the **Select networks** page, select a source network and map it to a destination network and click **Next**.

Choose **Source Network** and **Destination Network**. All the network communications occur through this portal.

Step 9 In the **Customize Template** page configure the OVA properties.

In the **Node Configuration** dialog box, enter the appropriate information for each node:

a. In the **Node ID** field, enter the node number.

```
Node ID   1
```

b. In the **Node Serial Number** field, enter the serial number which is unique across the cluster.

```
CiscoSN01
```

c. In the **Hostname** field, enter the hostnames for each node. Use any valid Linux hostname.

```
CiscoSN01
```

d. In the **Rescue User Password** field, select a password. Re-enter the password to confirm.

e. In the **Domain Name** field, enter the domain name of the node.

```
sn.cisco.com
```

Note User must configure the same domain name for all the nodes in the cluster.

In the **Network Configuration** dialog box, enter the appropriate information for each node:

a. In the **Management Address and Subnet** (network address) field, enter the Out-of-Band Management network address and enter the IP address and subnet.

```
10.197.145.244/24
```

Note This field is not validated prior to installation. Providing an invalid value for this field will cause the deployment to fail.

b. In the **Gateway IP** (network gateway) field, enter the Out-of-Band Management network gateway IP address.

```
10.197.145.1
```

c. In the **Application overlay Network IP Subnet** field, enter the IP/subnet to be used for Docker internal bridge networks.

```
2.2.0.0/16
```

Application overlay and the service network must be a `/16` network. Both the networks must not overlap with management or external networks.

Note This field is not validated prior to installation. Providing an invalid value for this field will cause the deployment to fail.

d. In the **Service Network IP subnet** field, enter the IP/subnet.

```
1.1.0.0/16
```

e. In the **NTP-servers** field, enter the Network Time Protocol servers separated by space.

```
10.197.145.2
```

f. In the **Name Server IP list**, enter the IP address of the name server

```
10.197.145.3
```

g. In the **Domain Search List** field, enter the list of domains to search separated by space.

```
cisco.com
```

In the **Cluster Configuration** dialog box, enter the appropriate information for each node:

a. In the **First Master** field, check the First Master check-box if it is the first node to be configured.

```
Is this node the first master node? Y
```

b. In the **Number of cluster masters** for Cisco Application Services Engine, enter 3.

```
Number of masters in the cluster 3
```

c. In the **List of IP serial numbers** field, enter the list of IP address of peer nodes in the cluster separated by a comma.

```
10.197.145.245,CiscoSN02 10.197.145.246,CiscoSN03
```

d. In the **Enter the latest dgbtoken from the master node in the cluster** field, enter any string of at least length 11 characters for the master node. For the peer nodes, enter the latest dgb token from the master node.

```
aaabbbcccdd
```

e. Click **Next**.

f. Reboot the VM, log-in as a rescue userlog in to the first node, execute the **acidiag dbgtoken** command to obtain the dgbtoken.

Step 10 The second node in the cluster needs to be configured in a similar manner.

In the **Cluster Configuration** dialog box, enter the appropriate information for each node:

- In the **First Master** field, check the check-box only if it is the first node to be configured.

```
Is this node the first master node? N
```

- The **Number of cluster masters** for Cisco Application Services Engine is always 3.

```
Number of masters in the cluster 3
```

- In the **List of IP serial numbers** field, enter the list of IP serial numer of peer nodes in the cluster separated by a comma.

  ```
  10.197.145.245,CiscoSN01 10.197.145.246,CiscoSN03
  ```

- For the **Enter the latest dgbtoken from the master node in the cluster**,enter the value for node 2 as acquired in step 9(f).

  ```
  0HSQETJXWDHC
  ```

- Click **Next**.

Step 11 The third node in the cluster needs to be configured in a similar manner.

In the **Cluster Configuration** dialog box, enter the appropriate information for each node.

- In the **First Master** field, check the box only if it is the first node to be configured.

  ```
  Is this node the first master node? N
  ```

- The **Number of cluster masters** for Cisco Application Services Engine is always 3.

  ```
  Number of masters in the cluster 3
  ```

- In the **List of IP, serial numbers** field, enter the list of IP and serial number of peer nodes in the cluster separated by a comma.

  ```
  10.197.145.244,CiscoSN01 10.197.145.245,CiscoSN02
  ```

- For the **Enter the latest dgbtoken from the master node in the cluster**, enter the value for node 3 as acquired in step 9(f).

  ```
  0HSQETJXWDHC
  ```

- Click **Next**.

Step 12 On the **Ready to complete** page, review the settings and click **Finish**.

Step 13 Re-boot all the VMs to form the cluster.

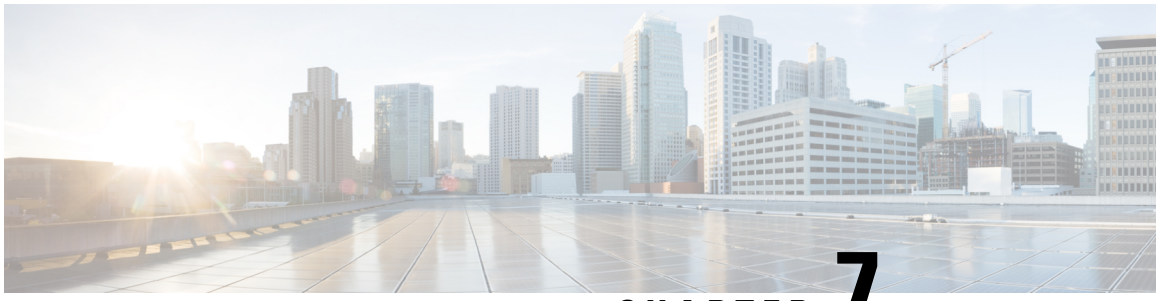
Step 14 After all three nodes are bootstrapped, wait for 15-30 mins, log in to SSH and execute the following command:

```
Server # acidiag health
cluster is healthy
```

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

Step 15 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



CHAPTER 7

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

Prerequisites

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

- Deploying Cisco Application Services Engine in supported on Linux operating system such as CentOS, Ubuntu or RedHat.
- Ensure that the following minimum Kernel and Virsh requirements are met:
  - Linux Kernel: 3.10.0-957.el7.x86_64
  - Virsh: libvirt-4.5.0-23.el7_7.1.x86_64
- Each cluster node requires a dedicated disk partition and minimum of 800 GB of disk space.
- The disk must have I/O latency less than 20ms. Assuming, /home is the disk/partition then,

```
# mkdir /home/test_data
```

```
# fio --rw=write --ioengine=sync --fdatasync=1 --directory=test-data_with_se --size=22m
 --bs=2300 --name=mytest
```

  Check for **99.00th=[<VALUE>]** under **fsync/fdatasync/sync_file_range** section. It should be less than 20 ms.
- Memory: 48G for each service node
- vCPUs: 16 for each service node
- You have installed all the required packages for QEMU-KVM support.

Deploying the Cisco Application Services Engine in KVM

This procedure is used for setting up Cisco Application Services Engine cluster in Linux KVM.

Step 1 Choose the Cisco Application Services Engine ISO image image.

a) Browse to the Software Download page.

b) Choose the Cisco Application Services Engine image for KVM (apic-sn-dk9.1.1.2(x).qcow2).

Step 2 Create a directory for service node base qcow2 image and download the **apic-sn-dk9.1.1.2h.qcow2** file.

Note Execute this on all the KVM hosts for all cluster nodes.

Note Each node needs to have its qcow2 path on a unique disk partition.

```
[ node1 ] # mkdir -p /home/sn_base/qcow2
[ node1 ] # cd /home/sn_base/qcow2
[ node1 ] # <wget/scp file from CCO to this location>
[ node1 ] # ls
apic-sn-dk9.1.1.2h.qcow2
[ node1 ] #
```

Step 3 Create a directory for the data path for the service node on each host and create a snapshot of the base image. The service node will always write to this snapshot.

Note Perform this action on all the service nodes in the cluster.

```
[ node1 ] # mkdir -p /home/mso-node1/
[ node1 ] # cd /home/mso-node1
[ node1 ] # qemu-img create -f qcow2 -b /home/sn_base/qcow2/apic-sn-dk9.1.1.2h.qcow2
/home/mso-node1/disk0.qcow2
```

Step 4 Open the KVM console and click **New Virtual Machine**.

Step 5 On the **New VM**, choose **import existing disk image option**. Click **Forward**.

Step 6 In the **provide existing storage path** tab, choose the **/home/mso-node1/disk0.qcow2** file.

Note Each node needs to have its qcow2 path on a unique disk partition.

Step 7 Choose the **Generic** value for the operating system and the version. Click **Forward**.

Step 8 For memory, choose the value 48000. For CPU, choose the value 16. Click **Forward**.

Step 9 Enter the name of the virtual machine **`mso-node1`**. Select the **customize configuration before install**. Choose the appropriate option from **Network selection** and click **Finish**.

Step 10 In the window **mso-node1 on QEMU/KVM**, choose the appropriate option from **Network selection**.

a) Select the NIC for the **Virtual Network Interface** and choose the device model as **e1000**.

b) Leave the default **Mac address**.

c) Click **Apply**.

d) Click **Begin Installation**.

The virtual machine should boot from **disk0.qcow2**.The first-boot prompt is displayed.

a) Specify the mode. To specify that the configuration is not obtained from the Cisco APIC cluster enter **n**.

b) Enter the serial number and a unique hostname for the service node.

c) Enter the domain name for the service node. The domain name is equivalent to the name of the cluster or the domain name of the fabric.

```
Setup utility for apic-sn with SerialNumber Not Specified and running version 1.1.2h
Is this running in ACI mode? (y/n) n
Enter node serialnumber: Mynode01
Enter node hostname: mso-node1
```

```
Enter node domain: example.com
Enter the password for rescue-user:
Reenter the password for rescue-user:
```

Step 11 Enter the physical network management IP address and mask.

It is the out-of-band management IPv4/ or Pv6 addresses used to access the Cisco Application Services Engine GUI, CLI, or API.

```
Enter physical network management IP address and mask:192.168.10.100/24
```

Step 12 Enter the physical network gateway IP address.

It is used for communicating to the external networks using out-of-band management.

```
Enter physical network gateway IP address:192.168.10.1
```

Step 13 Enter the number of masters in the cluster.

```
Enter number of Masters in the cluster (recommended is 3) 3
```

Step 14 Enter IP addresses, serial number of other master nodes in the cluster.

If the cluster size is 1, leave it blank.

```
Enter details of other Masters in the cluster, one at a time?
Select 'n' for a space-separated list (y/n) y
1) Enter IP Address: 192.168.10.101
Enter SerialNumber: Mynode02
2) Enter IP Address: 192.168.11.102
Enter SerialNumber: Mynode03
```

Step 15 You must assign one node in the cluster as the first master. If the cluster already exists, enter **n**.

```
Is this the first node in a new cluster? (y/n) y
```

Step 16 Enter the application overlay network IP address and mask.

It is the private IP address block, /16 network is required for container or pod network.

```
Enter application overlay network IP address and mask: 1.1.0.0/16
```

Step 17 Enter the service network IP address and mask.

It is the private IP address block, /16 network that is required for container or pod network.

```
Enter service network IP address and mask: 2.2.0.0/16
```

Step 18 Enter the search domain.

```
Enter the search domain as a space-separated list: mydomain.com
```

Step 19 Enter the addresses of the DNS name servers.

It is the IP address list required for resolving DNS names outside the cluster.

```
Enter nameserver addresses as a space-separated list: 192.168.12.100 192.168.12.101
```

Step 20 Enter the IP addresses of the NTP servers.

Enter the IP address of the NTP servers. It is required to sync the clock between all the master nodes in the cluster.

```
Enter the ntp servers as a space-separated list: 192.168.13.101
```

Step 21 Review the configuration.

```
Please review the config:
Number Masters cluster: 3
application overlay network: 1.1.0.0/16
first Master: true
management IP: 192.168.10.100/24
nameservers list: [192.168.12.100 192.168.12.101]
node domain: example.com
node hostname: mso-node1
node serialnumber: Mynode01
ntp servers list: [192.168.13.101]
physical gateway IP: 192.168.10.1
rescue-user password: <hidden>

search list: [mydomain.com]
seed list:
- {ipAddress: 192.168.10.101, name: mso-node02, serialNumber: Mynode02}
- {ipAddress: 192.168.11.102, name: mso-node03, serialNumber: Mynode03}
service network: 2.2.0.0/16
Do you wish to reenter the bootstrap config? (y/N) N

mso-node1 login:
```

Step 22 Generate the dbgtoken

a) Log in to SSH

```
$ssh rescue-user@192.168.10.100
password:
bash-4.2$ acidiag dbgtoken
0M080NDSGPRH
bash-4.2$
```

Step 23 Configure the second node similarly.

```
Please review the config:
Number Masters cluster: 3
application overlay network: 1.1.0.0/16
first Master: false
management IP: 192.168.10.101/24
nameservers list: [192.168.12.100 192.168.12.101]
node domain: example.com
node hostname: mso-node2
node serialnumber: Mynode02
ntp servers list: [192.168.13.101]
physical gateway IP: 192.168.10.1
rescue-user password: <hidden>
search list: [mydomain.com]
seed list:
- {ipAddress: 192.168.10.100, name: mso-node01, serialNumber: Mynode01}
- {ipAddress: 192.168.11.102, name: mso-node03, serialNumber: Mynode03}
service network: 2.2.0.0/16
Do you wish to reenter the bootstrap config? (y/N) N
Enter the latest dbgtoken from other active node in the cluster: 0M080NDSGPRH
mso-node2 login:
```

Step 24 For the **Enter the latest dbgtoken from other active node in the cluster**, go to Step 22. Obtain the dbgtoken by logging into the first node using the SSH. Enter the value for node 2.

Note: Always use the latest dbgtoken from the SSH to log in to the nodes.

Step 25 Configure the third node.

```
Please review the config:
Number Masters cluster: 3
application overlay network: 1.1.0.0/16
```

```
first Master: false
management IP: 192.168.11.102/24
nameservers list: [192.168.12.100 192.168.12.101]
node domain: example.com

node hostname: mso-node3
node serialnumber: Mynode03
ntp servers list: [192.168.13.101]
physical gateway IP: 192.168.11.1
rescue-user password: <hidden>
search list: [mydomain.com]
seed list:
- {ipAddress: 192.168.10.100, name: mso-node01, serialNumber: Mynode01}
- {ipAddress: 192.168.10.101, name: mso-node02, serialNumber: Mynode02}
service network: 2.2.0.0/16
Do you wish to reenter the bootstrap config? (y/N) N
Enter the latest dbgtoken from other active node in the cluster: 0M080NDSGPRH
mso-node3 login:
```

Step 26 For the **Enter the latest dbgtoken from other active node in the cluster**, go to Step 22. Obtain the dbgtoken by logging into the first node using the SSH. Enter the value for node 3.

Note: Always use the latest dbgtoken from the SSH to log in to the nodes.

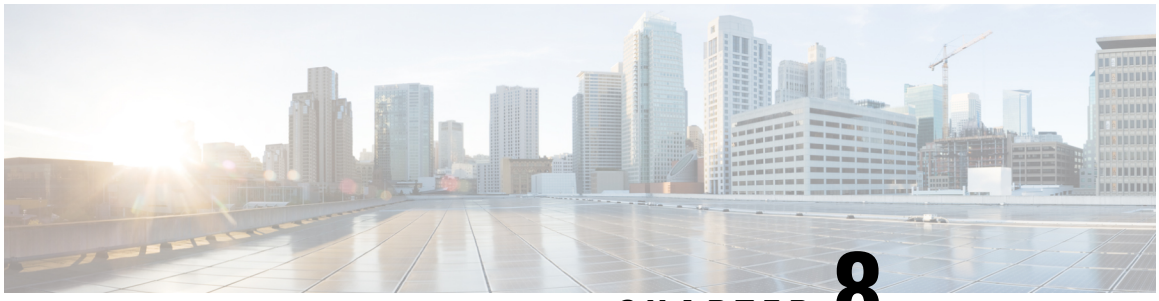
Step 27 After all three nodes are bootstrapped, wait for 15-30 mins and execute the following command using SSH:

```
Server # acidiag health
cluster is healthy
```

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

Step 28 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



CHAPTER 8

Upgrading Cisco Application Services Engine

Upgrading Cisco Application Services Engine

You can use this procedure to upgrade the Cisco Application Services Engine for all form factors.

Same procedure has to be performed on each service node separately

Before you begin

- You must have Cisco Application Services Engine installed and the cluster configured.
- Ensure that you have a working software image for the upgrade.

Note Upgrade from version 1.1.0d to 1.1.2i is supported for fabric internal mode only.

Step 1 Log in to the Cisco Application Services Engine server as a rescue-user.

Step 2 Copy the ISO image file into the /tmp directory.

Step 3 Start the upgrade using the **acidiag installer update** -f *iso_filepath* command.

```
node # acidiag installer update -f /tmp/apic-sn-dk9.1.1.2h.iso
```

Run the command on all nodes individually. Once the command is executed successfully, reboot the service nodes.

Step 4 Reboot individual nodes using the **acidiag reboot** command.

```
node # acidiag reboot
```

Step 5 Verify the version after the upgrade using the **acidiag version** command.

```
node # acidiag version
```

Working with Cisco Application Services Engine

You can use the following commands to perform various operations in Cisco Application Services Engine.

Command(s) for app operations:

- **acidiag app show**: Displays the installed application(s).

```
acidiag app show
```

- **acidiag app install**: Installs application(s).

```
acidiag app install <filepath or url>
```

- **acidiag app enable**: Enables an installed (or disabled) application (s).

```
acidiag app enable <application id>
bash-4.2$ acidiag app
[ { 'adminState': 'Enabled',
'apiEntrypoint': '/query',
'appID': 'MSO',
'creationTimestamp': '2019-12-08T22:02:08.513217541Z',
'description': 'Multi-Site Orchestrator application',
'displayName': 'cisco-mso',
'id': 'cisco-mso:2.2.3',
'name': 'cisco-mso',
'operStage': 'Enable',
'operState': 'Running',
'schemaversion': '',
'uiEntrypoint': '/ui/app-start.html',
'vendorID': 'Cisco',
'version': '2.2.3'}]
bash-4.2$
```

- **acidiag app disable**: Disables an enabled application (s).

```
acidiag app disable <application id>
```

- **acidiag app delete**: Deletes an application (s).

```
acidiag app delete <application id>
```

Command(s) for app image operations:

- **acidiag image show**: Displays all the application images present.

```
acidiag image show
```

- **acidiag image show <image file name>**: Displays information about the specified application image.

```
acidiag image show <image file name>
```

Command(s) for app import operations:

- **acidiag import show**: Displays information on all the application imports made to the Cisco Application Services Engine.

```
acidiag import show
```

- **acidiag import show <import id>**: Displays info about the specified import. Import id is an optional parameter.

```
acidiag import show <import id>
```

Command(s) for Tech Support:

- **acidiag techsupport collect**

```
acidiag techsupport collect
Started: TS collection may take 15-20 minutes to complete. Monitor /techsupport/ for
the file
```