Deploying in Cisco Application Services Engine

This chapter contains the following sections:

- Prerequisites and Guidelines, on page 1
- Deploying Orchestrator in Application Services Engine, on page 2
- Migrating Existing Cluster to Application Service Engine, on page 5

Prerequisites and Guidelines

This chapter covers deployment of a 3-node Multi-Site Orchestrator cluster. If you want to set up a single-node Orchestrator (for example, for testing purposes), follow the instruction in the Installing Single Node Orchestrator chapter instead.

Application Services Engine

You must have Cisco Application Services Engine installed and the cluster configured in Fabric External Mode as described in *Cisco Application Services Engine User Guide*.

Cisco Application Service Engine itself can be deployed using a number of different form factors, such as a Cisco Application Service physical appliance (`.iso`), in a VMware ESX virtual machine (`.ova`), in Amazon Web Services (`.ami`), or in Linux KVM (`.qcow`), all of which are supported for Multi-Site Orchestrator installations. Keep in mind however, you must use the same form factor Service Engine for all Orchestrator nodes, mixing different form factors within the same Orchestrator cluster is not supported.

Note that if you are deploying Services Engine in AWS, by default only PEM-based login is enabled for each node. If you'd like to be able to SSH into the nodes using a password, you will need to explicitly enable password-based logins. You can do that by logging into each node separately using the PEM file the first time, then executing the following command:

```
# acidiag login prompt enable
```

Internal Service Engine Networks

When first configuring Application Services Engine, two of the parameters that you provide are Application Overlay Network and Service Network.

The application overlay network defines the address space used by the application's services running in the Service Engine, such as the Multi-Site Orchestrator. Each Orchestrator node is assigned an IP address from this network, which is then used to communicate with each site's Cisco APIC. The services network is an internal network used by the Service Engine and its processes.

Both of these networks must be unique and not overlap with any other services in your environment.

Network Time Protocol (NTP)

Multi-Site Orchestrator uses NTP for clock synchronization, so you must have an NTP server configured in your environment. NTP server information is provided as part of the Application Services Engine installation procedure.

Application Services Engine Requirements

The following table summarizes the Application Services Engine requirements for Cisco ACI Multi-Site Orchestrator.

Table 1: Application Services Engine Requirements

Orchestrator Version	Requirements

Release 2.2(3) and 2.2(4)
Note
For all Multi-Site Orchestrator, Release 3.0(x) information including upgrades, see Cisco ACI Multi-Site Orchestrator Installation and Upgrade Guide, Release 3.x
	Cisco Application Services Engine, Release 1.1.2i
	If the Application Services Engine is deployed in an ESX or KVM virtual machine, the following additional requirements apply:
	• The hypervisor must be one of the following:
	  • ESXi 6.0 or later
	  • Linux Kernel `3.10.0-957.el7.x86_64` or later with KVM `libvirt-4.5.0-23.el7_7.1.x86_64` or later
	• 16 vCPUs
	  10 GHz CPU reservation is applied automatically
	• 48 GB of RAM
	  36 GB reservation is applied automatically
	• 100 GB disk
	  We recommend thin provisioning with a maximum size of 620 GB with each Application Services Engine VM running on its own disk.
	• We recommend that each Application Services Engine VM is deployed in a different ESX or KVM server.

Deploying Orchestrator in Application Services Engine

This section describes how to deploy Cisco ACI Multi-Site Orchestrator in Cisco Application Services Engine.

Before you begin

- Ensure that you meet the requirements and guidelines described in Prerequisites and Guidelines, on page 1.

Procedure

Step 1 Download the Cisco ACI Multi-Site Orchestrator Image.

a) Browse to the Software Download link:
https://software.cisco.com/download/home/285968390/type

b) Click **ACI Multi-Site Software**.

c) From the left sidebar, choose the Cisco ACI Multi-Site Orchestrator release version.

d) Download the *ACI Multi-Site App Image* file (`Cisco-MSO-<version>.aci`) for the release.

Step 2 Copy the Orchestrator image to the Application Services Engine.

If your Cisco Application Services Engine is deployed in VMware ESX (`.ova`), Linux KVM (`.qcow`), or as a physical appliance (`.iso`), or you have enabled password-based logins for your AWS (`.ami`) deployment, use the following command to copy the Orchestrator image into the `tmp` directory on the Services Engine:

```
# scp <app-local-path> rescue-user@<service-engine-ip>:/tmp/
```

However, if your Application Service Engine is deployed in AWS and you have not enabled password-based login, you must use the certificate (`.pem`) file that you created during the Application Services Engine deployment:

```
# scp <app-local-path>.aci -i <pem-file-name>.pem rescue-user@<service-engine-ip>:/tmp/
```

For example, assuming you're running the `scp` command from the same directory where you saved the Orchestrator image:

- For password-based authentication:

  ```
  # scp ./Cisco-MSO-2.2.3.aci rescue-user@10.30.11.147:/tmp/
  ```

- For PEM-based authentication:

  ```
  # scp ./Cisco-MSO-2.2.3.aci -i <pem-file-name>.pem rescue-user@10.30.11.147:/tmp/
  ```

Step 3 Install the Orchestrator app in your Application Services Engine.

When deploying the Orchestrator app, you need to install it in only one of the Service Engine nodes. The application will be replicated to the other nodes in the cluster automatically.

a) Log in to any one of your Services Engine nodes as `rescue-user`.

If your Cisco Application Services Engine is deployed in VMware ESX (`.ova`), Linux KVM (`.qcow`), or as a physical appliance (`.iso`), simply SSH in using the following command:

```
# ssh rescue-user@<service-engine-ip>
```

However, if your Application Services Engine is deployed in AWS and you have not enabled password-based login, you must login using the certificate (`.pem` file) that you created during the Application Services Engine deployment:

```
# ssh -i <pem-file-name>.pem rescue-user@<service-engine-ip>
```

b) Verify Services Engine health.

```
# acidiag health
All components are healthy
```

c) Install the Orchestrator.

In the following command, replace <*application-path*> with the full path to the application image you copied in the previous step.

```
# acidiag app install <application-path>
```

For example:

```
# acidiag app install /tmp/Cisco-MSO-2.2.3.aci
Image uploaded succesfully
check image status using: acidiag image show cisco-mso-2.2.3.aci
```

Note
In certain cases, the Service Engine's `app install` command may return the following error:
`HTTPSConnectionPool(host='localhost', port=9090): Max retries exceeded with url: /api/v1/firmware/uploads (Caused by NewConnectionError('<urllib3.connection.VerifiedHTTPSConnection object at 0x788b6e1d2f50>: Failed to establish a new connection: [Errno 111] Connection refused').`

In this case, wait a couple of minutes and rerun the `acidiag app install` command again.

d) Verify that the application was loaded.

Use the following command to check the `operState` of the application.

While the application is loading and installing it will go through a number of operational states, which will be reflected in the `operState` field, for example `'operState': 'Initialize'`. This process can take up to 20 minutes and you must ensure that the state changes to `Disabled` before proceeding to the next step.

After the application's state changes to `Disabled`, make a note of the application's `id`, you will use it in the next step to enable the application.

```
# acidiag app show
[   {   'adminState': 'Disabled',
        'apiEntrypoint': '/query',
        'appID': 'MSO',
        'creationTimestamp': '2020-02-10T20:30:36.195960295Z',
        'description': 'Multi-Site Orchestrator application',
        'displayName': 'ACI Multi-Site Orchestrator',
        'id': 'cisco-mso:2.2.3',
        'name': 'cisco-mso',
        'operStage': 'PostInstall',
        'operState': 'Disabled',
        'schemaversion': '',
        'uiEntrypoint': '/ui/app-start.html',
        'vendorID': 'Cisco',
        'version': '2.2.3'}]
```

Step 4 Enable the Orchestrator app.

After installation is complete, the application will remain in the `Disabled` state by default and you must enable it.

In the following command, replace <*app-id*> with the application ID from the previous step:

```
# acidiag app enable <app-id>
```

For example:

```
# acidiag app enable cisco-mso:2.2.3
Application enabled succesfully
```

Step 5 Verify that the cluster was deployed successfully.

a) Verify that the application was enabled successfully.

While the application is being enabled, it will go through multiple operational states. You can use `acidiag app show` command to check the current state.

In the following output, ensure that the highlighted fields are `Enabled`, `Enable`, and `Running` respectively.

```
## acidiag app show
[   {   'adminState': 'Enabled',
        'apiEntrypoint': '/query',
        'appID': 'MSO',
        'creationTimestamp': '2020-02-10T20:30:36.195960295Z',
        'description': 'Multi-Site Orchestrator application',
        'displayName': 'ACI Multi-Site Orchestrator',
        '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'}]
```

b) Log in to the Cisco ACI Multi-Site Orchestrator GUI.

Note
After the application is enabled as described in the previous step, it may take up to 20 additional minutes for all the Orchestrator services to start and the GUI to become available.

After the GUI becomes available, you can access it by browsing to any one of your Application Services Engine nodes' IP addresses. The default log in is **admin** and the default password is **We1come2msc!**.

When you first log in, you will be prompted to change the password.

What to do next

For information on migrating your existing Mutli-Site Orchestrator configuration deployed in VMware ESX to Cisco Application Services Engine cluster, see #unique_25.

For more information about Day-0 Operations, see Adding Tenants and Schemas.

Migrating Existing Cluster to Application Service Engine

This section provides an overview of how to migrate your existing Multi-Site deployment to a new cluster deployed in Cisco Application Service Engine.

Because the two platforms are vastly different in how they implement clustering and infrastructure, the migration process involves parallel deployment of the new platform and manual transfer of the current configuration database from the existing Orchestrator cluster.

Procedure

Step 1 Deploy a brand new Orchestrator cluster in Application Service Engine.

The procedure is described in the Deploying in Cisco Application Services Engine, on page 1 chapter of this document.

Step 2 Backup existing deployment configuration.

a) Log in to your existing Cisco ACI Multi-Site Orchestrator.
b) From the left navigation pane, select **Admin** > **Backups**.
c) In the main window, click **New Backup**.

A **New Backup** window opens.

d) In the **Name** field, provide the name for the backup file.

The name can contain up to 10 alphanumeric characters, but no spaces or underscores (_).

e) Choose the **Backup Location**.

You can save the backup file locally on the Orchestrator nodes or export it to a remote location.

If you want to save the backup file locally, choose **Local**.

Otherwise, if you want to save the backup file to a remote location, choose **Remote** and provide the following:

- From the **Remote Location** dropdown menu, select the remote location.
- In the **Remote Path**, either leave the default target directory or you can choose to append additional subdirectories to the path. However, the directories must be under the default configured path and must have been already created on the remote server.

f) Click **Save** to create the backup.

Step 3 Copy the Backup file from the existing Orchestrator.

If you created the backup using a remote location, you can skip this step.

Otherwise, in the main window, click the actions ( ) icon next to the backup and select **Download**. This will download the backup file to your system.

Step 4 Bring down the existing Multi-Site Orchestrator cluster VMs.

Step 5 Import the backup file to your new Orchestrator cluster deployed on the Application Service Engine.

If you saved the backup locally, simply import the file:

a) Log in to your existing Cisco ACI Multi-Site Orchestrator.
b) From the left navigation menu, select **Admin** > **Backups**.
c) In the main window, click **Import**.
d) In the **Import from file** window that opens, click **Select File** and choose the backup file you want to import.

Importing a backup will add it to the list of the backups displayed the **Backups** page.

If you saved the backup to a remote location, add the remote location to the new Multi-Site Orchestrator:

a) Log in to your Cisco ACI Multi-Site Orchestrator.

b) From the left navigation pane, select **Admin** > **Remote Locations**.
c) In the top right of the main window, click **Add Remote Location**.

An **Add New Remote Location** screen appears.

d) Provide the same information for the remote location that you used in your old Orchestrator.
e) Click **Save** to add the remote server.

Step 6 Restore the configuration.

a) From the left navigation menu, select **Admin** > **Backups**.
b) In the main window, click the actions ( ) icon next to the backup you want to restore and select **Rollback to this backup**.

If the version of the selected backup is different from the running Multi-Site version, the rollback could cause a removal of the features that are not present in the backup version.

c) Click **Yes** to confirm that you want to restore the backup you selected.

If you click **Yes**, the system terminates the current session and the user is logged out.