

Installing Single Node Orchestrator

This chapter contains the following sections:

- Installing Single Node Orchestrator in VMware ESX, on page 1
- Installing Single Node Orchestrator in Service Engine, on page 3

Installing Single Node Orchestrator in VMware ESX

This section describes how to deploy a single node Cisco ACI Multi-Site Orchestrator in an ESX VM. Single node installations are supported for testing purposes only. Production Multi-Site deployments require a 3-node Orchestrator cluster, which is described in Deployment Overview.

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) Choose the Cisco ACI Multi-Site Orchestrator release version.

d) Download the *ACI Multi-Site Image* file (`msc-<version>.ova`) for the release.

Step 2 Deploy the OVA using the vCenter either the WebGUI or the vSphere Client.

Note
The OVA cannot be deployed directly in ESX, it must be deployed using vCenter.

Step 3 Configure the OVA properties.

In the **Properties** dialog box, enter the appropriate information for each VM:

- In the **Enter password** field, enter the root password for the VM.
- In the **Confirm password** field, enter the password again.
- In the **Hostname** field, enter the hostnames for each Cisco ACI Multi-Site Orchestrator node. You can use any valid Linux hostname.

- In the **Management Address** (network address) field, enter the network address or leave the field blank to obtain it via DHCP.

  Note
  The field is not validated prior to installation, providing an invalid value for this field will cause the deployment to fail.

- In the **Management Netmask** (network netmask) field, enter the netmask netmask or leave the field blank to obtain it via DHCP.
- In the **Management Gateway** (network gateway) field, enter the network gateway or leave the field blank to obtain it via DHCP.
- In the **Domain Name System Server** (DNS server) field, enter the DNS server or leave the field blank to obtain it via DHCP.
- In the **Time-zone string (Time-zone)** field, enter a valid time zone string.

  You can find the time zone string for your region in the IANA time zone database or using the `timedatectl list-timezones` Linux command. For example, *`America/Los_Angeles`* .
- In the **NTP-servers** field, enter Network Time Protocol servers separated by commas.
- In the **Application overlay** field, enter the default address pool to be used for Docker internal bridge networks.

  Application overlay must be a `/16` network. Docker then splits this network into two `/24` subnets used for the internal `bridge` and `docker_gwbridge` networks.

  For example, if you set the application overlay pool to `192.168.0.0/16`, Docker will use `192.168.0.0/24` for the `bridge` network and `192.168.1.0/24` for the `docker_gwbridge` network.

  You must ensure that the application overlay network is unique and does not overlap with any existing networks in the environment.

  Note
  The field is not validated prior to installation, providing an invalid value for this field will cause the deployment to fail.

- In the **Service overlay** field, enter the default Docker overlay network IP.

  Service overlay must be a `/24` network and is used for the `msc_msc` Orchestrator Docker service network.

  You must ensure that the service overlay network is unique and does not overlap with any existing networks in the environment.

  Note
  The field is not validated prior to installation, providing an invalid value for this field will cause the deployment to fail.

- Click **Next**.
- In the **Deployment settings** pane, check all the information you provided is correct.
- Click **Power on after deployment**.
- Click **Finish**.

In addition to the above parameters, a 10GHz CPU cycle reservation is automatically applied to each Orchestrator VM when deploying the OVA.

Step 4 Log in to the VM using SSH.

Step 5 Change into the deployment scripts directory.

```
# cd /opt/cisco/msc/builds/<build_number>/prod-standalone
```

Step 6 Run the initialization script.

```
# ./msc_cfg_init.py
```

Step 7 Run the deployment script.

```
# ./msc_deploy.py
```

Step 8 Log in to the Cisco ACI Multi-Site Orchestrator GUI.

You can access the GUI using any of the 3 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 more information about Day-0 Operations, see Adding Tenants and Schemas.

Installing Single Node Orchestrator in Service Engine

This section describes how to deploy a single node Cisco ACI Multi-Site Orchestrator in Cisco Application Service Engine. Single node installations are supported for testing purposes only. Production Multi-Site deployments require a 3-node Orchestrator cluster, which is described in Deployment Overview.

Before you begin

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

  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:

Procedure

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

a) Browse to the ACI Multi-Site Orchestrator download page on Cisco DC App Center.

b) Click **Download** to download the image.

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

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

a) Log in to your Services Engine 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 (`.ami`), 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
```

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