

Deployment Overview

This chapter contains the following sections:

- Deployment Options, on page 1
- Multi-Site Orchestrator Communication Ports, on page 2
- Multi-Site Orchestrator and Cisco APIC Interoperability Support, on page 3

Deployment Options

A typical Cisco ACI Multi-Site deployment requires a 3-node Multi-Site Orchestrator cluster to manage all the sites' fabrics in your ACI Multi-Site environment. You can choose to deploy the Orchestrator cluster in one of the following ways:

- You can deploy the Multi-Site Orchestrator (MSO) cluster in a Cisco Application Services Engine (ASE).

  We recommend this approach for all new ACI Multi-Site deployments, because it provides a common platform to streamline multi-product integrations, additional security through Cisco Secured Development Lifecyle (CSDL) and removal of `root` access to Orchestrator application, file system protection, and single click upgrades to future releases.

  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. Installing and configuring the Application Service Engine is outside the scope of this document and is described in *Cisco Application Services Engine User Guide*.

  Note AWS deployments of Multi-Site Orchestrator support managing only public cloud sites and not on-premises fabrics.

  Installing and configuring the Orchestrator cluster in Application Services Engine is described in the Deploying in Cisco Application Services Engine. Upgrading Services Engine MSO deployments is described in the Upgrading or Downgrading Orchestrator Deployments in Application Service Engine.

- Alternatively, you can deploy each Orchestrator node directly in VMware ESX VMs.

  When deploying in ESX VMs, you can choose one of the following 2 approaches:

- Use Cisco-provided Python scripts to deploy the entire Multi-Site Orchestrator cluster. The scripts allow you to execute the deployment and later upgrades remotely, for example from your laptop, as long as you have access to the vCenter where the Orchestrator VMs are to be deployed.

  This is the preferred approach when deploying an Orchestrator cluster in ESX VMs as it automates a number of manual steps and allows remote execution of Cisco ACI Multi-Site Orchestrator installation and subsequent software upgrades.

- Using an OVA image to deploy each Orchestrator VM individually. In this case you can also choose to deploy the image either using the vCenter or directly on the ESX server.

Installing and configuring the Orchestrator cluster in VMware ESX VMs is described in the Deploying in VMware ESX. Upgrading VMware ESX Orchestrator deployments is described in the Upgrading Orchestrator Deployments in VMware ESX.

Single Node Lab Deployments

While production Multi-Site Orchestrator deployments require a 3-node high availability (HA) cluster, single node Orchestrator deployments are supported for lab and testing purposes. The installation and upgrade steps for single node Orchestrator differ slightly from the 3-node cluster deployments and are covered in detail in the Installing Single Node Orchestrator.

Multi-Site Orchestrator Communication Ports

There are three types of network communication to or from the Multi-Site Orchestrator cluster:

- Client traffic to the Multi-Site Orchestrator cluster.

  Multi-Site Orchestrator uses TCP port 443 (`https`) to allow user access via GUI or REST API for creating, managing, and deploying policy configurations.

- REST API traffic from the Multi-Site Orchestrator to the APIC controllers of the ACI fabrics that are part of the Multi-Site domain

  Multi-Site Orchestrator uses TCP port 443 for REST API traffic to deploy policies to each site.

- Intra-cluster communication.

  All control-plane and data-plane traffic between Cisco ACI Multi-Site Orchestrator nodes (including intra-cluster communication and container overlay network traffic) is encrypted with IPSec's Encapsulating Security Payload (ESP) using IP protocol number 50 to provide security and allow the cluster deployments over a round-trip time distance of up to 150ms. If there is firewall between any Orchestrator nodes, proper rules must be added to allow this traffic.

  If your Multi-Site Orchestrator cluster is deployed directly in VMware ESX without the Application Services Engine, the following ports are used for Docker communications between the cluster nodes:



Note The following TCP and UDP ports are listed for educational perspective only as no traffic is ever sent in clear text across the network leveraging these ports.

- TCP port 2377 for Cluster Management Communications

- TCP and UDP port 7946 for Inter-Manager Communication
- UDP port 4789 for Docker Overlay Network Traffic

Multi-Site Orchestrator and Cisco APIC Interoperability Support

Multi-Site Orchestrator (MSO) does not require a specific version of APIC to be running in all sites. The APIC clusters in each site as well as the MSO itself can be upgraded independently of each other and run in mixed operation mode as long as each fabric is running APIC Release 3.2(6) or later. As such, we recommend that you always upgrade to the latest release of the Multi-Site Orchestrator.

However, keep in mind that if you upgrade the MSO before upgrading the APIC clusters in one or more sites, some of the new MSO features may not yet be supported by an earlier APIC release. In that case a check is performed on each template to ensure that every configured option is supported by the target sites.

The check is performed when you save a template or deploy a template. If the template is already assigned to a site, any unsupported configuration options will not be saved; if the template is not yet assigned, you will be able to assign it to a site, but not be able to save or deploy the schema if it contains configuration unsupported by that site.

In case an unsupported configuration is detected, an error message will show, for example: `This APIC site version <site-version> is not supported by MSO. The minimum version required for this <feature> is <required-version> or above.`

The following table lists the features and the minimum required APIC release for each one:

Feature	Minimum APIC Version
ACI Multi-Pod Support	Release 3.2(6)
Service Graphs (L4-L7 Services)	Release 3.2(6)
External EPGs	Release 3.2(6)
ACI Virtual Edge VMM Support	Release 3.2(6)
DHCP Support	Release 3.2(6)
Consistency Checker	Release 3.2(6)
vzAny	Release 3.2(6)
Host Based Routing	Release 4.0(1)
CloudSec Encryption	Release 4.0(1)
Layer 3 Multicast	Release 4.0(1)
MD5 Authentication for OSPF	Release 4.0(1)
EPG Preferred Group	Release 4.0(2)
Intersite L3Out	Release 4.2(1)