Installing Cisco APIC-EM on a Virtual Machine

About the Virtual Machine Installation

You can install the Cisco APIC-EM within a virtual machine in a VMware vSphere environment. You can then deploy the virtual machine with the controller within your network. The Cisco APIC-EM can be deployed as a single host (single virtual machine) or within a multi-host environment (multiple virtual machines).

Important We recommend that you install and deploy Cisco APIC-EM in a multi-host environment for enhanced scalability and redundancy. For information about multi-host support, see Multi-Host Support.

The following table lists the steps for installing the Cisco APIC-EM on a virtual machine.

Table 1: Cisco APIC-EM Virtual Machine Installation

Step	Description
1	Review the system requirements for a virtual machine installation. See System Requirements—Virtual Machine, on page 2
2	Review the pre-install checklists for the installation (standalone and multi-host modes). See Pre-Install Checklists
3	Review information about the ports for the controller. See Cisco APIC-EM Ports Reference

Step	Description
4	Download and verify the ISO image. See Verifying the Cisco ISO Image
5	Install the ISO image. See Installing the Cisco ISO Image, on page 10
6	Configure the Cisco APIC-EM in standalone or multi-host mode. Refer to the following sections for information about the configuration wizard process: • Configuring Cisco APIC-EM as a Single Host Using the Wizard • Configuring Cisco APIC-EM in Multi-Host Mode

System Requirements—Virtual Machine

The following table lists the minimum system requirements for a successful Cisco APIC-EM VMware vSphere installation. You must configure at a minimum 32 GB RAM for the virtual machine that contains the Cisco APIC-EM when a single host is being deployed. The single host server that contains the virtual machine must have this much RAM physically available. For a multi-host deployment (two or three hosts), 32 GB of RAM is required for each of the virtual machines that contains the Cisco APIC-EM.

Note The three server, multi-host deployment provides both software and hardware high availability. The two server, multi-host deployment only provides software high availability and does not provide hardware high availability. For this reason, we strongly recommend that for a multi-host deployment three servers be used. With either two or three servers, all of the servers must reside in the same subnet.

Table 2: Minimum System Requirements—Virtual Machine

Virtual Machine	VMware ESXi Version	5.1/5.5/6.0
	Image Format	ISO
	Virtual CPU (vCPU)	6 (minimum) **Note** 6 vCPUs is the minimum number required for your virtual machine configuration. For better performance, we recommend using 12 vCPUs.

	Datastores	We recommend that you do not share a datastore with any defined virtual machines that are not part of the designated Cisco APIC-EM cluster. If the datastore is shared, then disk I/O access contention may occur and cause a significant reduction of disk bandwidth throughput and a significant increase of I/O latency to the cluster.
Hardware Specifications	Memory	32 GB (minimum single host deployment) For specific Cisco APIC-EM scale requirements, see the *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*. **Note** For a multi-host hardware deployment of 2 or 3 hosts (with 3 hosts being the maximum number supported for a multi-host deployment) 32 GB of RAM is required for each host.
	Disk Capacity	200 GB
	CPU Speed	2.4 GHz
	Disk I/O Speed	200 MBps
	Network Adapter	1
Networking	Web Access	Required
	Browser	The following browsers are supported when viewing and working with the Cisco APIC-EM: • Google Chrome, version 56.0 or later • Mozilla Firefox, version 51.0 or later

	Network Timing	To avoid conflicting time settings, we recommend that you disable the time synchronization between the guest VM running the Cisco APIC-EM and the ESXi host. Instead, configure the timing of the guest VM to a NTP server. **Important** Ensure that the time settings on the ESXi host are also synchronized to the NTP server. This is especially important when upgrading the Cisco APIC-EM. Failure to ensure synchronization will cause the upgrade to fail.

Virtual Machine Scale Requirements

For the latest, detailed information about Cisco APIC-EM configured on a virtual machine and scale limits, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes*.

Pre-Install Checklists

Standalone Mode Checklists

Review the following checklists before beginning a single-host Cisco APIC-EM installation (standalone mode).

Note A host is defined as an appliance, physical server, or virtual machine with instances of a Grapevine root and clients running. The Grapevine root is located in the host OS and the clients are located within Linux containers. The clients run the services within the Linux containers. You can set up either a single host deployment or multi-host deployment (2 or 3 hosts) for your network. For high availability and scale, your multi-host deployment must contain three hosts. All inbound traffic to the controller in a single host deployment is through the host IP address that you configure using the configuration wizard. All inbound traffic to the controller in a multi-host deployment is through a Virtual IP that you configure using the configuration wizard.

Networking Requirements

This Cisco APIC-EM installation requires that the network adapters (NICs) on the host (physical or virtual) are connected to the following networks:

- Internet (network access required for **Make A Wish** requests and telemetry collection)
- Network with NTP server(s)
- Network with devices that are to be managed by the Cisco APIC-EM

Note The Cisco APIC-EM should never be directly connected to the Internet. It should not be deployed outside of a NAT configured or protected datacenter environment.

IP Address Requirements

Ensure that you have available at least one IP address for the network adapter (NIC) on the host.

The IP address is used as follows:

- Direct access to the Grapevine root
- Direct access to the Cisco APIC-EM controller (for GUI access)

Note If your host has 2 NICs, then you may want to have two IP addresses available and configure one IP address for each NIC.

Multi-Host Mode Checklists

Review the following checklist before beginning a multi-host Cisco APIC-EM installation (multi-host mode).

- You must satisfy the requirements for the single host installation as described in the previous section for each host.
- Additionally, you must establish a network connection between each of the hosts using either a switch or a router. Each host must be routable with the other two hosts.
- You must configure a virtual IP (VIP).

  You configure one or more NICs on each host using the configuration wizard. Each NIC that you configure must point to a non-routable network (if all your networks are routable, then you only need one NIC). A VIP is required per non-routable network. For example, if you configure 2 NICs on all 3 hosts in a multi-host cluster and each NIC points to a separate, non-routable network, then you need to configure 2 VIPs. The VIP provides an interface redundancy feature for your multi-host deployment. With a VIP, the IP address can float between the hosts.

  When deploying the controller in a multi-host configuration:

  - You provide a VIP address when configuring the controller using the wizard.
  - On startup, the controller will bring up the VIP on one of the hosts.
  - All inbound requests into controller from the external network are made via this VIP (instead of the host IP address), and the requests are routed to the services running on different hosts via the reverse-proxy service.

- If the host on which has the VIP fails, then Grapevine will bring up the VIP on one of the remaining two hosts.
- The VIP must reside in the same subnet as the three hosts.
- If you are planning to obtain a certificate issued for a multi-host environment, then it is important to get the certificate issued against the virtual IP or the host name resolvable to the virtual IP.

Multi-Host Deployment Virtual IP

A multi-host deployment has three physical IP addresses and one virtual IP that floats across the IP addresses by design in order to provide high availability. This capability to float also means that any SSH client that wants to connect to the virtual IP address will see different host-identity public SSH keys each time the virtual IP moves its residence from one host to another host. Most SSH clients will complain that the new host is not trusted, since an entry already exists (as you might have accepted the key earlier for the older host which owned that virtual IP address before). To prevent this inconvenience, you may want to add the host keys of all the three hosts to your known hosts list as described below.

For example on a Linux or Apple Mac OS client machine, run the **ssh-keyscan** command on each of the three host physical IP addresses as follows:

```
$ ssh-keyscan -t rsa 209.165.200.30
# 209.165.200.30 SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.3
209.165.200.30 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDA1B6/1JpKPFOmG3S82eE8OKZkGYmRd
SYnuCHfDiY5Pptt3BmaPgC6OlER4wwDL8VP2Rx2kxj3diIzFpUOyDqTbFxIRKVzlwtHHZdhO6G93MyLLGsWq
XSMWs4xVcqpembKeCrdjakPaPAXqiAeKW9oimdv.....


$ ssh-keyscan -t rsa 209.165.200.31
# 209.165.200.31 SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.3
209.165.200.31 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDF57F90z2His86tEj4s75pTc7h0nfzF
2c3QweHCNN2ov474HJJcPrnWTw4DAoPpPCU6zWvR0QLxunURDb+pMeZrIIyd49xn9+OBSmBpzrnety7UB2uP
XzL1RvVxayw8mkXkj779LhFh9vkXR4DtX7XLjg.....


$ ssh-keyscan -t rsa 209.165.200.32
# 209.165.200.32 SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.3
209.165.200.32 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9kwzodGzGkh/UFXVa9fptGe+sa3CBR
6SNerXxpCmfT9AOXH8xuk3/CBX+DDUQgGJVmqw6maCYKOy0RtAhGxdsNdPL6ETTKzxYB5uzw3KhcDJ6D6ob6
jdzkR6yRuXVFi2OE+u1Aqs7J8GO66FfdavU8.....
```

Next, change the IP address in the SSH key line of each output to the virtual IP address of the following and append all three key lines to the `~/.ssh/known_hosts` file and save it.

Assuming that 209.165.200.33 is the virtual IP address in the above multi-host example, you would add three lines in the `~/.ssh/known_hosts` file of your client machine as follows:

```
209.165.200.33 ssh-rsa

AAAAB3NzaC1yc2EAAAADAQABAAABAQDA1B6/1JpKPFOmG3S82eE8OKZkGYmRdSYnuCHfDiY5Pptt3BmaPgC6OlER4
wwDL8VP2Rx2kxj3diIzFpUOyDqTbFxIRKVzlwtHHZdhO6G93MyLLGsWqXSMWs4xVcqpembKeCrdjakPaPAXqiAeKW9
oimdvPbrQPua7Zg9oblDxaBPn0Fqj00YDjKqTkp/IkZHEfHbDM996GLEbWlOvoHeCCqeZ1nWgFIqzAF+ty8+X5Z/fh
hmGe+w2tQlMfrs9pcZDaEEmq/w1W+uRohxLKs+OHnHYAbMzC6O+5fLEr2BwaZf8W016eo1WpPsxUVK6StbXBOQZrcH0
bPsUbIjKJkzafpft9Dp73pSd/vwaoB3DrvNec/PiEJYk+R.....
```

After the above change, the client will have no trouble performing uninterrupted SSH into the virtual IP address of the hosts even with the IP address floating.

Cisco APIC-EM Ports Reference

The following tables list the Cisco APIC-EM ports that permit incoming traffic, as well as the Cisco APIC-EM ports that are used for outgoing traffic. You should ensure that these ports on the controller are open for both incoming and outgoing traffic flows.

Note Ensure that proper protections exist in your network for accessing port 22. For example, you can configure a proxy gateway or secure subnets to access this port.

Table 3: Cisco APIC-EM Incoming Traffic Port Reference

Port Number	Permitted Traffic	Protocol (TCP or UDP)
22	SSH	TCP
80	HTTP	TCP
123	NTP	UDP
162	SNMP	UDP
443 [1]	HTTPS	TCP
500	ISAKMP In order for deploying multiple hosts across firewalls in certain deployments, the IPSec ISAKMP (Internet Security Association and Key Management Protocol) UDP port 500 has to be allowed to be traversed.	UDP
16026	SCEP	TCP

[1] You can configure the TLS version for this port using the Cisco APIC-EM. For more information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Table 4: Cisco APIC-EM Outgoing Traffic Port Reference

Port Number	Permitted Traffic	Protocol (TCP or UDP)
22	SSH (to the network devices)	TCP
23	Telnet (to the network devices)	TCP

Port Number	Permitted Traffic	Protocol (TCP or UDP)
53	DNS	UDP
80	Port 80 may be used for an outgoing proxy configuration. Additionally, other common ports such as 8080 may also be used when a proxy is being configured by the Cisco APIC-EM configuration wizard (if a proxy is already in use for your network). **Note** To access Cisco supported certificates and trust pools, you can configure your network to allow for outgoing IP traffic from the controller to Cisco addresses at the following URL: http://www.cisco.com/security/pki/	TCP
123	NTP	UDP
161	SNMP agent	UDP
443[2]	HTTPS	TCP
500	ISAKMP In order for deploying multiple hosts across firewalls in certain deployments, the IPSec ISAKMP ((Internet Security Association and Key Management Protocol) UDP port 500 has to be allowed to be traversed.	UDP

[2] You can configure the TLS version for this port using the Cisco APIC-EM. For more information, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Verifying the Cisco ISO Image

Prior to deploying the Cisco APIC-EM, verify that the ISO image that you downloaded is a genuine Cisco image.

Note If you are deploying the Cisco APIC-EM from an ISO image that you downloaded, then perform this procedure. This procedure is not required, if deploying the controller with the Cisco APIC-EM Controller Appliance (Cisco APIC-EM ISO image pre-installed and tested).

Before You Begin

You must have received notification of the location of the Cisco APIC-EM ISO image or contacted Cisco support for the location of the Cisco APIC-EM ISO image.

Step 1 Download the ISO image from the location specified by Cisco.

Step 2 Download the Cisco public key for signature verification from the location specified by Cisco.
The Cisco public key is named:

```
cisco_image_verification_key.pub
```

Step 3 Obtain the secure hash algorithm (SHA512) checksum file for the ISO image from the location specified by Cisco.

Step 4 Obtain the specific release ISO image's signature file from Cisco support via email or by download from the secure Cisco website (if available).
For example, `apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.sig`.

Step 5 (Optional) Perform a SHA verification to determine whether the ISO image was corrupted due to a partial download.
For example, run one of the following commands (depending upon your operating system):

- On a system running MAC OS X version:

```
shasum -a 512 apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.iso
```

- On a Linux system:

```
sha512sum apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.iso
```

Microsoft Windows does not include a built-in checksum utility, but you can install a utility from Microsoft at this link: http://www.microsoft.com/en-us/download/details.aspx?id=11533

Compare the output of the above command (or Microsoft Windows utility) to the SHA512 checksum file obtained earlier in step 3. If the command output fails to match, download the ISO image again and run the appropriate command a second time. If the output still fails to match, contact Cisco support.

Step 6 Verify that the ISO image is genuine and from Cisco by verifying the signature. Run the following command on the ISO image:

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature
apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.sig apic-em-CA-0.8.2.4704-0.1.0.15.dev1300-gaafbb68.iso
```

If the ISO image is genuine, then running this command should result in a **Verified OK** message. If this message fails to appear, then do not install the ISO image and contact Cisco support.

Note The image name and the signature names used here are only examples. Use the exact names of these files that you downloaded from the Cisco website.

This command will work in both MAC and Linux environments. For Windows, you need to download and implement OpenSSL from www.openssl.org, if you have not already done so.

What to Do Next

After you verify that the ISO image is genuine and from Cisco, install the Cisco ISO image.

Installing the Cisco ISO Image

Perform the steps in the following procedure to install the Cisco ISO image on the host (virtual machine).

Note If you are deploying the Cisco APIC-EM from an ISO image that you downloaded, then perform this procedure. This procedure is not required, if deploying the controller with the Cisco APIC-EM Controller Appliance (ISO image pre-installed and tested).

Before You Begin

You must review the system requirements before beginning this procedure.

You must review the Cisco APIC-EM pre-deployment checklist before beginning this procedure.

You must have downloaded and verified the Cisco ISO image by performing the tasks in the previous procedure.

For installing the Cisco APIC-EM ISO image into a virtual machine using VMware, you must create an empty virtual machine that you will attach the Cisco APIC-EM ISO image to and then boot up. When creating this virtual machine, do not accept the VMware default settings but configure the settings as per the system requirements described in this chapter. For assistance with preparing the virtual machine with appropriate settings, see the following topics:

- Preparing a VMware System for Cisco APIC-EM Deployment
- Virtual Machine Configuration Recommendations
- Configuring Resource Pools Using vSphere Web Client
- Configuring a Virtual Machine Using vSphere Web Client

Step 1 Upload the Cisco APIC-EM ISO image directly to the virtual machine's datastore.

Step 2 Attach the Cisco APIC-EM ISO image as a virtual CD-ROM drive of the virtual machine.

Step 3 Boot up the host (virtual machine) and start the configuration wizard.

What to Do Next

Proceed to configure Cisco APIC-EM to run on either a single or multiple hosts. Refer to the following sections for information about the configuration wizard process:

- Configuring Cisco APIC-EM as a Single Host Using the Wizard
- Configuring Cisco APIC-EM in Multi-Host Mode