Deploying the Cisco APIC-EM

Information about the Cisco APIC-EM Deployment

You can deploy the Cisco APIC-EM on either a server (bare-metal hardware) or within a virtual machine in a VMware vSphere environment. You can also deploy the Cisco APIC-EM as either a single host or in a multi-host environment.

Note We recommend that you deploy the Cisco APIC-EM in a multi-host environment for enhanced scalability and redundancy.

Pre-Deployment Checklists

Single Host Checklists

Review the following checklists before beginning your single-host Cisco APIC-EM deployment.

Note A host is defined as 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 deployment 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 might want to have two IP addresses available and configure one IP address for each NIC.

Multi-Host Checklists

Review the following checklist before beginning your multi-host Cisco APIC-EM deployment.

- You must satisfy the requirements for the single host deployment 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.

Verifying the Cisco ISO Image

Prior to deploying the Cisco APIC-EM, you can 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 Download 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 downloaded 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 (server or 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 (Cisco APIC-EM 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 previously listed in this guide.

Note See the VMware documentation for information about creating and configuring new virtual machines.

Perform one of the following procedures:

- For installing the Cisco APIC-EM ISO image on a server and from local media:
  - Burn the ISO image onto a DVD or a bootable USB flash drive.
  - Insert the DVD into the DVD drive of the physical appliance.

    If your physical appliance does not come with a DVD drive, you can connect an external USB DVD drive to the appliance and insert the disk into that external drive.
  - You can also connect a bootable USB flash drive where you burnt the ISO image to into the appliance.

    Note Cisco UCS servers provide an additional method of installing a remote ISO using a Virtual KVM console. See your Cisco UCS server documentation for information about this procedure. Note that installing the ISO image using a Virtual KVM console may take longer than the above methods.

- For installing the Cisco APIC-EM ISO image on a virtual machine:
  - Upload the Cisco APIC-EM ISO image directly to the virtual machine's datastore.
  - Attach the Cisco APIC-EM ISO image as a virtual CD-ROM drive of the virtual machine.

What to do next

Boot up the host (server or virtual machine) and run the wizard to configure the Cisco APIC-EM.

Cisco APIC-EM Configuration Wizard Parameters

When the Cisco APIC-EM software configuration begins, an interactive configuration wizard prompts you to enter required parameters to configure the controller.

Note Ensure that the DNS and NTP servers are reachable before you run the configuration wizard and whenever a Cisco APIC-EM host reboots in the deployment.

Table 1: Cisco APIC-EM Configuration Wizard Parameters

Configuration Wizard Prompt	Description	Example
Host IP address	Must be a valid IPv4 address for the host. This IP address is used for the network adapter (eth0) on the host and connects to the external network or networks. For multiple network adapters, have several IP addresses available.	10.0.0.12
(Optional) Virtual IP address	Must be a valid IPv4 address. This virtual IP address is used for the network adapter (eth0) on the host. You should only configure a virtual IP address, if you are setting up a multi-host deployment.	10.12.13.14
Netmask IP address	Must be a valid IPv4 netmask.	255.255.255.0
Default Gateway IP address	Must be a valid IPv4 address for the default gateway.	10.12.13.1
Primary server	Must be a valid IPv4 address for the primary server.	10.15.20.25 **Note** Enter either a single IP address for a single primary server, or multiple IP addresses separated by spaces for DNS servers.
Primary NTP server	Must be a valid IPv4 address or hostname of a Network Time Protocol (NTP) server.	10.12.13.10 Enter either a single IP address for a single NTP primary server, or multiple IP addresses separated by spaces for several NTP servers. We recommend that you configure three NTP servers for your deployment.
Add/Edit another NTP server	Must be a valid NTP domain.	10.12.13.11 Allows you to configure multiple NTP servers. **Note** We recommend that you configure three NTP servers for your deployment.

Configuration Wizard Prompt	Description	Example
HTTPS proxy server	Must be a valid IPv4 address for the HTTPS proxy with port number.	https://209.165.200.11:3128
Admin Username	Identifies the administrative username used for GUI access to the Cisco APIC-EM controller. We recommend that the username be three to eight characters in length and be composed of valid alphanumeric characters (A–Z, a–z, or 0–9).	admin2780

Admin Password	Identifies the administrative password that is used for GUI access to the Cisco APIC-EM controller. You must create this password because there is no default. The password meet the following requirements:
	• Eight character minimum length.
	• Does NOT contain a tab or a line break.
	• Does contain characters from at least three of the following categories:
	  • Uppercase alphabet
	  • Lowercase alphabet
	  • Numeral
	  • Special characters (for example, ! or #)
		MyIseYPass2

Linux Username	Identifies the Linux (Grapevine) username used for CLI access to the Grapevine root and clients.	The default is 'grapevine' and cannot be changed.

Configuration Wizard Prompt	Description	Example

Linux Password	Identifies the Linux (Grapevine) password that is used for CLI access to the Grapevine roots and clients. You must create this password because there is no default. The password meet the following requirements:
	• Eight character minimum length.
	• Does NOT contain a tab or a line break.
	• Does contain characters from at least three of the following categories:
	  • Uppercase alphabet
	  • Lowercase alphabet
	  • Numeral
	  • Special characters (for example, ! or #)
		MyGVPass01

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

Perform the steps in the following procedure to configure Cisco APIC-EM as a single host using the wizard.

Before you begin

You must have either received the Cisco APIC-EM Controller Appliance with the Cisco APIC-EM pre-installed or you must have downloaded, verified, and installed the Cisco ISO image onto a server or virtual machine as described in the previous procedures.

Step 1 Boot up the host.

Step 2 Review the **APIC-EM License Agreement** screen that appears and choose either **<view license agreement>** to review the license agreement or **accept>>** to accept the license agreement and proceed.

Note You will not be able to proceed without accepting the license agreement.

After accepting the license agreement, you are then prompted to select a configuration option.

Step 3 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the **Create a new APIC-EM cluster** option to begin.

You are then prompted to enter values for the **NETWORK ADAPTER #1 (eth0)**.

Step 4 Enter configuration values for the **NETWORK ADAPTER #1 (eth0)** on the host.

The configuration wizard discovers and prompts you to confirm values for the network adapter or adapters on your host. For example, if your host has three network adapters you are prompted to confirm configuration values for network adapter #1 (eth0), network adapter #2 (eth1), and network adapter #3 (eth2) respectively.

Note The primary interface for the controller is eth0 and it is best practice to ensure that this interface is made highly available.

On Cisco UCS servers, the NIC labeled with number 1 would be the physical NIC. The NIC labeled with the number 2 would be eth1.

Host IP address	Enter the host IP address to use for the network adapter. This host IP address (and network adapter) connects to the external network or networks. These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI. **Note** The configuration wizard validates the value entered and issues an error message if incorrect. If you receive an error message for the host IP address, then check to ensure that eth0 (ethernet interface) is connected to the correct network adapter.
Virtual IP	(Optional) Enter a virtual IP address to use for this network adapter. You should only configure a virtual IP address, if you are setting up a multi-host deployment. **Note** For additional information about virtual IP, see Multi-Host Deployment Virtual IP, on page 3
Netmask	Enter the netmask for the network adapter's IP address.
Default Gateway IP address	Enter a default gateway IP address to use for the network adapter. **Note** If no other routes match the traffic, traffic will be routed through this IP address.
DNS Servers	Enter the DNS server or servers IP addresses (separated by spaces) for the network adapter.

Static Routes	If required for your network, enter a space separated list of static routes in this format: <network>/<netmask>/<gateway> Static routes, which define explicit paths between two routers, cannot be automatically updated; you must manually reconfigure static routes when network changes occur. You should use static routes in environments where network traffic is predictable and where the network design is simple. You should not use static routes in large, constantly changing networks because static routes cannot react to network changes.

Once satisfied with the controller network adapter settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered. After validation and if your host has two network adapters, you are prompted to enter values for **NETWORK ADAPTER #2 (eth1)**. If your host has three network adapters, you are prompted to enter values for **NETWORK ADAPTER #2 (eth1)** and **NETWORK ADAPTER #3 (eth2)**. If you do not have any additional network adapters or if you do not have more than one non-routable network, then proceed directly to the next step.

Step 5 If the controller is being deployed in your network behind a proxy server and the controller's access to the Internet is through this proxy server, then enter configuration values for the **HTTPS PROXY**.

Note If there is no proxy server between the controller and access to the Internet, then this step will not appear. Instead, you will be prompted to enter values for **CLOUD CONNECTIVITY**.

HTTPS Proxy	Enter the protocol (HTTP or HTTPS), IP address, and port number of the proxy. For example, enter **https://209.165.200.11:3128**
HTTPS Proxy Username	Enter the username, if authentication is required for the proxy.
HTTPS Proxy Password	Enter the password, if authentication is required for the proxy.

After configuring the **HTTPS PROXY**, enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values for **CLOUD CONNECTIVITY**.

Step 6 Enter configuration values for **CLOUD CONNECTIVITY**.

CCO Username	Enter a Cisco Connection Online (CCO) username for cloud connectivity. For example, enter the username that you use to log into the Cisco website to access restricted locations as either a Cisco customer or partner. **Note** If you do not have a CCO username and password, then enter your company name in the username and company name fields and leave the password field empty for this step. This will permit you to proceed through the config-wizard process. Values entered for this step are used for telemetry collection. For information about telemetry collection, see Telemetry Collection.
CCO Password	Enter a Cisco Connection Online (CCO) password for the CCO *username*. For example, enter the password that you use to log into the Cisco website to access restricted locations as either a Cisco customer or partner.
Company Name	Enter the company or organization's name with which you are affiliated.

Once satisfied with the cloud connectivity settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values entered. After validation, you are then prompted to enter values for the **LINUX USER SETTINGS**.

Step 7 Enter configuration values for the **LINUX USER SETTINGS**.

Linux Password	Enter a Linux password. The Linux password is used to ensure security for both the Grapevine root and clients located on the host (appliance, server, or virtual machine). Access to the Grapevine root and clients by you or the controller requires this password. The default username is grapevine. For information about the requirements for a Linux password, see the Password Policy section, in Chapter 3, Cisco APIC-EM Security. **Note** The Linux password is encrypted and hashed in the controller database.
Re-enter Linux Password	Confirm the Linux password by entering it a second time.
Seed Phrase Password Generation	(Optional) Instead of creating and entering your own password in the above **Linux Password** fields, you can enter a seed phrase and have the configuration wizard generate a random and secure password using that seed phrase. Enter a seed phrase and then press <**Generate Password**> to generate the password.

Auto Generated Password	(Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto generated password. **Note** When finished with the password, be sure to save it to a secure location for future reference. Press <**Use Generated Password**> to save the password.

After configuring the Linux password, enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values for the **APIC-EM ADMIN USER SETTINGS**.

Step 8 Enter configuration values for the **APIC-EM ADMIN USER SETTINGS**.

Administrator Username	Enter an administrator username. Your administrator username and password are used to ensure security for the controller itself. Access to the controller's GUI requires that you enter this username and password.
Administrator Password	Enter an administrator password. For information about the requirements for an administrator password, see the Password Policy section, in Chapter 3, Cisco APIC-EM Security. **Note** The administrator password is encrypted and hashed in the controller database.
Re-enter Administrator Password	Confirm the administrator password by entering it a second time.
Seed Phrase Password Generation	(Optional) Instead of creating and entering your own password in the above **Administrator Password** fields, you can enter a seed phrase and have the configuration wizard generate a random and secure password using that seed phrase. Enter a seed phrase and then press <**Generate Password**> to generate the password.
Auto Generated Password	(Optional) The seed phrase appears as part of a random and secure password. If desired, you can either use this password "as is", or you can further edit this auto generated password. **Note** When finished with the password, be sure to save it to a secure location for future reference. Press <**Use Generated Password**> to save the password.

After configuring the administrator password, enter **next>>** to proceed.

After entering **next>>**, you are then prompted to enter values for either the **NTP SERVER SETTINGS**.

Step 9 Enter configuration values for **NTP SERVER SETTINGS**.

NTP servers	Enter a single NTP server address or a list of NTP servers each separated by a space. The Elastic Services Platform (Grapevine) manages a Network Time Protocol (NTP) server to provide time synchronization for the Grapevine clients. You must configure the NTP server for the clients. The NTP server is external to the cluster. **Note** We recommend that for redundancy purposes, you configure at least three NTP servers for your Cisco APIC-EM deployment.

Note Cisco routers can also be configured as NTP servers.

After configuring the NTP server(s), enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values for **INTER-HOST COMMUNICATION**.

Step 10 Enter configuration values for **INTER-HOST COMMUNICATION**.

Enable IPSec Encryption	You can configure IPSec tunneling for communications between the hosts in a multi-host cluster. By selecting *yes*, you configure IPSec tunneling. The default is IPSec and the default option is set to *yes*.

Once satisfied with the inter-host communication setting, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered.

Step 11 Enter configuration values for **CONTROLLER CLEAN-UP**.

Harvest All Virtual Disks	Entering **yes** will delete all Grapevine virtual disks that belong to the controller for this specific deployment. For an initial configuration, enter **no**.
Delete All Clients	Entering **yes** will delete all Grapevine clients that belong to the controller for this specific deployment. For an initial configuration, enter **no**.

For an initial configuration, enter **no** for both options.

After configuring the controller clean-up, enter **next>>** to proceed. After entering **next>>**, you are then prompted to enter values to finish the configuration and begin the configuration wizard installation.

Step 12 A final message appears stating that the wizard is now ready to proceed with applying the configuration.

The following options are available:

- **[back]**—Review and verify your configuration settings.
- **[cancel]**—Discard your configuration settings and exit the configuration wizard.

- **[save & exit]**—Save your configuration settings and exit the configuration wizard.
- **[proceed]**—Save your configuration settings and begin applying them.

Enter **proceed>>** to complete the installation. After entering **proceed>>**, the configuration wizard applies the configuration values that you entered above.

At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message appears.

Step 13 Open your browser and enter the host IP address to access the Cisco APIC-EM GUI.

You can use the displayed IP address of the Cisco APIC-EM GUI at the end of the configuration process.

Step 14 After entering the IP address in the browser, a message stating that "Your connection is not private" appears.

Ignore the message and click the **Advanced** link.

Step 15 After clicking the **Advanced** link, a message stating that the site's security certificate is not trusted appears.

Ignore the message and click the link.

Note This message appears because the controller uses a self-signed certificate. You will have the option to upload a trusted certificate using the controller GUI after installation completes.

Step 16 In the **Login** window, enter the administrator username and password that you configured above and click the **Log In** button.

What to do next

For a multi-host deployment, perform the following procedure to configure another host and join it with this host to create a cluster.

For a single-host deployment, begin to use the Cisco APIC-EM to manage and configure your network.

Note You can send feedback about the Cisco APIC-EM by clicking the Feedback icon ("I wish this page would....") at the lower right of each window in the GUI. Clicking on this icon opens an email. Use this email to send a comment on the current window or to send a request to the Cisco APIC-EM development team.

Configuring Cisco APIC-EM as a Multi-Host Cluster Using the Wizard

Perform the steps in this procedure to configure Cisco APIC-EM on your host and to join it to another, pre-existing host to create a cluster. Configuring the Cisco APIC-EM on multiple hosts to create a cluster is best practice for both high availability and scale.

Caution

- When joining a host to a cluster as described in the procedure below, there is no merging of the data on the two hosts. The data that currently exists on the host that is joining the cluster is erased and replaced with the data that exists on the cluster that is being joined to.
- When joining the additional hosts to form a cluster be sure to join only a single host at a time. You should not join multiple hosts at the same time, as doing so will result in unexpected behavior.
- You should also expect some service downtime when the adding or removing hosts to a cluster, since the services are then redistributed across the hosts. Be aware that during the service redistribution, there will be downtime.

Before you begin

You must have either received a Cisco APIC-EM Controller Appliance with the Cisco APIC-EM pre-installed or you must have downloaded, verified, and installed the Cisco ISO image onto a second server or virtual machine.

You must have already configured Cisco APIC-EM on the first host (server or virtual machine) in your planned multi-host cluster following the steps in the previous procedure. This procedure must be run on the second host that you are joining to the cluster. When joining the new host to the cluster, you must specify an existing host in the cluster to connect to.

Note The Cisco APIC-EM multi-host configuration supports the following two workflows:

- You first configure a single host running Cisco APIC-EM in your network. After performing this procedure, you then use the wizard to configure and join two additional hosts to form a cluster.
- If you already have several single hosts configured with Cisco APIC-EM, you can use the configuration wizard to join two additional hosts to a single host to form a cluster.

Step 1 Boot up the host.

Step 2 Review the **APIC-EM License Agreement** screen that appears and choose either **<view license agreement>** to review the license agreement or **accept>>** to accept the license agreement and proceed with the deployment.

Note You will not be able to proceed without accepting the license agreement.

After accepting the license agreement, you are then prompted to select a configuration option.

Step 3 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose one of the two displayed options to begin.

- **Create a new APIC-EM cluster**
- **Add this host to an existing APIC-EM cluster**

For the multi-host deployment, click the **Add this host to an existing APIC-EM cluster** option.

Step 4 Enter configuration values for the **NETWORK ADAPTER #1 (eth0)** on the host.

The configuration wizard discovers and prompts you to confirm values for the network adapter or adapters on your host. For example, if your host has two network adapters you are prompted to confirm configuration values for network adapter #1 (eth0) and network adapter #2 (eth1).

Note On Cisco UCS servers, the NIC labeled with number 1 would be the physical NIC. The NIC labeled with the number 2 would be eth1.

Host IP address	Enter a host IP address to use for the network adapter. This host IP address connects to the external network or networks. **Note** The network adapter(s) connect to the external network or networks. These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI.
Netmask	Enter the netmask for the network adapter's IP address.

Later in this procedure, the following information will be discovered and copied from the cluster to the configuration file of this host:

- Default Gateway IP address
- DNS Servers
- Static Routes

Once satisfied with the controller network adapter settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered. After validation, you are then prompted to enter values for the **APIC-EM CLUSTER SETTINGS**.

Step 5 Enter configuration values for the **APIC-EM CLUSTER SETTINGS**.

Remote Host IP	Enter the eth0 IP address of the pre-configured host that you are now joining to form a cluster. **Note** If a virtual IP address has already been configured on another host for a multi-host cluster, you may also enter that IP address value. This field accepts either the IP address of a pre-configured host to the cluster or the virtual IP address of the cluster.
Administrator Username	Enter an administrator username. This is the administrator username on the pre-configured host that you are now joining to form a cluster.

Administrator Password	Enter an administrator password. This is the administrator password on the pre-configured host that you are now joining to form a cluster. For information about the requirements for an administrator password, see the Password Policy section, in Chapter 3, Cisco APIC-EM Security. **Note** The administrator password is encrypted and hashed in the controller database.

After configuring the administrator cluster settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard then proceeds to prepare the host to join the cluster.

You will receive a message to please wait, while the remote cluster is being queried and data is retrieved.

Step 6 Enter configuration values for the **Virtual IP**.

Note If you are joining the host to a cluster where the virtual IP has already been configured, then you will not be prompted for virtual IP configuration values. If you are joining the host to a cluster where a virtual IP has not yet been configured, then you will be prompted for virtual IP configuration values.

Virtual IP	Enter the virtual IP address to use for the network that the controller is directed to. **Note** For additional information about virtual IP, see Multi-Host Deployment Virtual IP, on page 3

Once satisfied with the virtual IP address settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered.

Step 7 (Optional) Enter additional configuration values for the **Virtual IP**.

The configuration wizard proceeds to continue its discovery of any pre-existing configuration values on the hosts in the cluster. Depending upon what the configuration wizard discovers, you may be prompted to enter additional configuration values. For example:

- If eth1 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for eth1. You are also prompted for a VIP, if it has not yet been configured for this NIC.
- If eth2 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for eth2. You are also prompted for a VIP, if it has not yet been configured for this NIC.
- If eth3 was configured on a pre-existing host in the cluster, then you are prompted to enter the host IP address that was configured for this eth3. You are also prompted for a VIP, if it has not yet been configured for this NIC.

Note This configuration wizard discovery process and prompting continues for the number of configured Ethernet ports in the cluster.

Virtual IP	Enter the virtual IP address to use for the network that the controller is directed to.

IP address	Enter an IP address to use for this network adapter. This IP address connects to the external network or networks. **Note** The network adapter(s) connect to the external network or networks. These external network(s) consists of the network devices, NTP servers, as well as providing access to the northbound REST APIs. The external network(s) also provides access to the controller GUI.

Once satisfied with the virtual IP address settings, enter **next>>** to proceed. After entering **next>>**, the configuration wizard proceeds to validate the values you entered.

Step 8 A final message appears stating that the wizard is now ready to proceed to join the host to the cluster.

The following options are available:

- **[back]**—Review and verify or modify your configuration settings.
- **[cancel]**—Discard your configuration settings and exit the configuration wizard.
- **[proceed]**—Save your configuration settings and begin the process to join this host to the specified Cisco APIC-EM.

Enter **proceed>>** to proceed. After entering **proceed>>**, the configuration wizard applies the configuration values that you entered above.

At the end of the configuration process, a successful configuration message appears.

Step 9 Open your browser and enter an IP address to access the Cisco APIC-EM GUI.

You can use the first displayed IP address of the Cisco APIC-EM GUI at the end of the configuration process.

Note The first displayed IP address can be used to access the Cisco APIC-EM GUI. The second displayed IP address accesses the network where the devices reside.

Step 10 After entering the IP address in the browser, a message stating that "Your connection is not private" appears.

Ignore the message and click the **Advanced** link.

Step 11 After clicking the **Advanced** link, a message stating that the site's security certificate is not trusted appears.

Ignore the message and click the link.

Note This message appears because the controller uses a self-signed certificate. You will have the option to upload a trusted certificate using the controller GUI after installation completes.

Step 12 In the **Login** window, enter the administrator username and password that you configured above and click the **Log In** button.

What to do next

Proceed to follow the same procedure described here to join the third and final host to the multi-host cluster.

Note You can send feedback about the Cisco APIC-EM by clicking the Feedback icon ("I wish this page would....") at the lower right of each window in the GUI. Clicking on this icon opens an email. Use this email to send a comment on the current window or to send a request to the Cisco APIC-EM development team.

Powering Down and Powering Up a Single Host or Multi-Host Cluster

Under certain circumstances such as troubleshooting, you might want to gracefully power down and then power up either a single host or a multi-host cluster. This procedure describes how to perform these procedures.

For information about powering down and powering up a single host within a multi-host cluster, see Powering Down and Powering Up a Single Host Within a Multi-Host Cluster, on page 22.

Before you begin

You should have deployed the Cisco APIC-EM following the procedures in this guide.

Step 1 Using a Secure Shell (SSH) client, log into the host (appliance, server, or virtual machine) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the **harvest_all_clients** command to harvest (gracefully shut down) all services on a single host or on multiple hosts within a multi-host cluster.

```
$ sudo /home/grapevine/bin/harvest_all_clients
```

Important For a multi-host cluster, you only need to enter this command on one of the hosts to harvest (gracefully shut down) all services on all of hosts in the cluster.

Step 4 Review the command output and subsequent directions.

```
$ sudo /home/grapevine/bin/harvest_all_clients

Disabled Grapevine policy
Harvesting client 1f481f49-fabc-44f9-af5a-0481bd823165...
Harvesting client 6dac3f56-fb05-4fd0-be06-d5c6869e23cd...
Harvesting client c800924c-7603-4092-b1f8-0c19f5141acc...
Waiting on task 05b9192c-9484-11e6-bdc2-0050569f3bee...
Task '05b9192c-9484-11e6-bdc2-0050569f3bee' completed successfully
Waiting on task 05da80da-9484-11e6-bdc2-0050569f3bee...
Task '05da80da-9484-11e6-bdc2-0050569f3bee' completed successfully

Successfully harvested all clients
```

```
PLEASE NOTE:
Grapevine policy has been DISABLED so that services and clients can be harvested.
To start all services again, run the following command:

   grape config update enable_policy true
```

Step 5 Power down the host, by entering the following command:

```
$ sudo shutdown -h now
```

Enter your password a second time when prompted.

For a multi-host cluster, you will need to enter this command on each of the hosts in the multi-host cluster to shut them all down.

Important You need to ensure that the last host that was shutdown in a multi-host cluster is the very first host that is then restarted. Be sure to track the order in which the hosts are shutdown in a multi-host cluster.

Step 6 Review the command output as the host shuts down.

Note The **sudo shutdown** command also powers off the host.

Step 7 Power up the Grapevine root process by turning the host or hosts (in a multi-host cluster) back on.

Important For a multi-host cluster, be sure to restart the host that was shutdown last in the multi-host cluster. This must be the first host restarted.

Step 8 Using a Secure Shell (SSH) client, log back into the host with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 9 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 10 Enable Grapevine, by entering the following command on the Grapevine root:

```
$ grape config update enable_policy true
```

Wait a few minutes for the Cisco APIC-EM services to start up again.

Important For a multi-host cluster, you only need to enter this command on one of the hosts after all of the hosts have been successfully powered on.

What to do next

Log back into the controller's GUI and begin working with the Cisco APIC-EM to manage and monitor the devices within your network.

Powering Down and Powering Up a Single Host Within a Multi-Host Cluster

Under certain circumstances such as troubleshooting, you might want to gracefully power down and then power up a single host within a multi-host cluster. For example, to perform maintenance on that host while keeping the Cisco APIC-EM controller running and functional. This procedure describes how to perform this procedure.

Important This procedure uses the **grape host evacuate** command. The **grape host evacuate** command only works in a 3 host cluster (not a 1 or 2 host cluster). For a 2 host cluster, instead of using **grape host evacuate** command, use the standard host removal process to first remove the host you want to remove from the cluster, then reattach it back into the cluster. For detailed information, see "Troubleshooting Cisco APIC-EM Multi-Host" in the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*.

Before you begin

You should have deployed the Cisco APIC-EM following the procedures in this guide.

All of the hosts in a multi-host cluster need to be functional and running prior to beginning this procedure.

Step 1 Using a Secure Shell (SSH) client, log into the host (appliance, server, or virtual machine) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 2 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the **grape host display** command to review the command output and determine the *host_id* of the host that you want to power off.

Step 4 Enter the **grape host evacuate** command to harvest (gracefully shut down) the services on the host.

Use the *host_id* for this command that you determined in the previous step.

```
$ grape host evacuate host_id
```

This command harvests all services running on the specified host (*host_id*) using the **grape host evacuate** command. In a multi-host cluster, the services on the specified host are harvested and transferred to the other two hosts in the cluster.

Important The **grape host evacuate** command only works in a 3 host cluster (not a 1 or 2 host cluster). For a 2 host cluster, instead of using **grape host evacuate** command, use the standard host removal process to first remove the host you want to remove from the cluster, then reattach it back into the cluster. For detailed information, see "Troubleshooting Cisco APIC-EM Multi-Host" in the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*.

Step 5 Power down the host, by entering the following command:

```
$ sudo shutdown -h now
```

Note Enter your password a second time when prompted.

Step 6 Review the command output as the host shuts down.

Note The **sudo shutdown** command also powers off the host.

Step 7 Power up the Grapevine root process by turning the host back on.

Step 8 Using a Secure Shell (SSH) client, log back into the host with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the host to the external network.

Step 9 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 10 Enable Grapevine, by entering the following command on the Grapevine root:

```
$ grape host enable host_id
```

The host ID to enter for this command must be the same as the host ID used in the **grape host evacuate** command in step 4.

Wait a few minutes for the Cisco APIC-EM services to start up again.

What to do next

Log back into the controller's GUI and begin working with the Cisco APIC-EM to manage and monitor the devices within your network.

Uninstalling the Cisco APIC-EM

The following procedure describes how to uninstall the Cisco APIC-EM.

Note If you plan to reinstall the Cisco APIC-EM after uninstalling it, then you must follow the procedure described below to avoid any possible problems. You should have also contacted Cisco support for the link to download the latest Cisco APIC-EM ISO image. Be aware that this procedure shuts down both the Cisco APIC-EM and the host (physical or virtual) on which it resides. At the end of this procedure and if you are reinstalling the Cisco APIC-EM, then you will need to access the host and restart it.

Step 1 Using a Secure Shell (SSH) client, log into the host (appliance, server, or virtual machine) with the IP address that you specified using the configuration wizard.

Note The IP address to enter for the SSH client is the IP address that you configured for the network adapter. This IP address connects the appliance to the external network.

Step 2 Enter the Linux username ('grapevine') and password when prompted.

Step 3 Enter the **reset_grapevine factory** command at the prompt.

```
$ reset_grapevine factory
```

Step 4 Enter your Linux grapevine password a second time to start the reset process.

```
$ sudo password for grapevine *********
```

After entering this command a warning appears that the **reset_grapevine factory** command will shut down the controller.

You are then prompted to confirm your intent to run the **reset_grapevine factory** command.

Step 5 Enter **Yes** to confirm that you want to run the **reset_grapevine factory** command.

The controller then performs the following tasks:

- Stops all running clients and services
- Stops and shuts down any Linux containers
- Deletes all cluster data
- Deletes all user data
- Deletes the configuration files including secrets and private keys
- Shuts down the controller
- Shuts down the host (physical or virtual)