Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide, Release 1.6.x

First Published: 2017-02-21

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

Audience

This publication is for experienced network administrators who will install the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) in their network. Use this guide to install and configure the Cisco APIC-EM.

For information about using the controller's GUI for the first time, see the *Cisco APIC-EM Quick Start Guide*.

Note The Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) is also referred to within this deployment guide as a controller.

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Courier` font	Terminal sessions and information the system displays appear in `courier` font.

Convention	Description
`Bold Courier` font	**`Bold Courier`** font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document may use the following conventions for reader alerts:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem.*

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time.* You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documentation

This section lists the Cisco APIC-EM and related documents available on Cisco.com at the following url:

http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-series-home.html

- Cisco APIC-EM Documentation:
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes*
  - *Cisco APIC-EM Quick Start Guide* (directly accessible from the controller's GUI)
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Installation Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*
  - *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*
  - *Open Source Used In Cisco APIC-EM*
- Cisco EasyQoS Application for Cisco APIC-EM
  - *Cisco EasyQoS Application for APIC-EM Release Notes*
  - *Cisco EasyQoS Application for APIC-EM Supported Platforms*
  - *Cisco EasyQoS Application for APIC-EM User Guide*
- Cisco Network Visibility Application for the Cisco APIC-EM
  - *Cisco Network Visibility Application for APIC-EM Release Notes*
  - *Cisco Network Visibility Application for APIC-EM Supported Platforms*
  - *Cisco Network Visibility Application for APIC-EM User Guide*
- Cisco Path Trace Application for Cisco APIC-EM
  - *Cisco Path Trace Application for APIC-EM Release Notes*
  - *Cisco Path Trace Application for APIC-EM Supported Platforms*
  - *Cisco Path Trace Application for APIC-EM User Guide*

- Cisco IWAN Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco IWAN*
  - *Release Notes for Cisco Intelligent Wide Area Network Application (Cisco IWAN App)*
  - *Configuration Guide for Cisco IWAN on Cisco APIC-EM*
  - *Software Configuration Guide for Cisco IWAN on APIC-EM*
  - *Open Source Used in Cisco IWAN and Cisco Network Plug and Play*
- Cisco Network Plug and Play Documentation for the Cisco APIC-EM:
  - *Release Notes for Cisco Network Plug and Play*
  - *Solution Guide for Cisco Network Plug and Play*
  - *Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM*
  - *Cisco Network Plug and Play Agent Configuration Guide* or *Cisco Open Plug-n-Play Agent Configuration Guide* (depending on the Cisco IOS XE release)
  - *Mobile Application User Guide for Cisco Network Plug and Play*
- Cisco Active Advisor Documentation for the Cisco APIC-EM:
  - *Cisco Active Advisor for APIC-EM Release Notes*
- Cisco Integrity Verification Documentation for the Cisco APIC-EM:
  - *Cisco Integrity Verification Application (Beta) for APIC-EM Release Notes*
  - *Cisco Integrity Verification Application (Beta) for APIC-EM User Guide*
- Cisco Remote Troubleshooter Documentation for the Cisco APIC-EM:
  - *Cisco Remote Troubleshooter Application for APIC-EM Release Notes*
  - *Cisco Remote Troubleshooter Application for APIC-EM User Guide*

Note For information about developing your own application that interacts with the controller by means of the northbound REST API, see the https://developer.cisco.com/site/apic-em/ Web site.

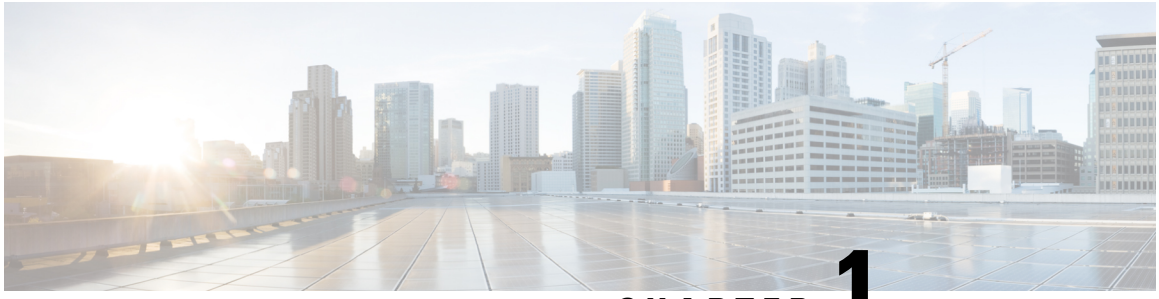
Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.

PART I

Installation

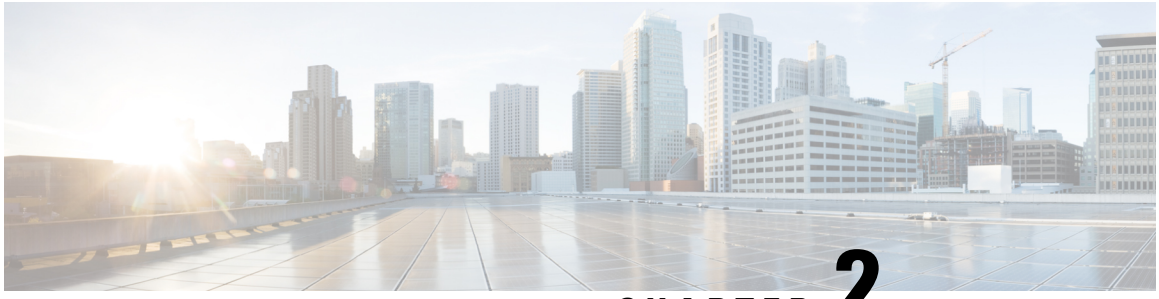


CHAPTER 1

New and Changed Information

New and Changed Information

For this release, there are no changes in this installation guide from its previous version. For information about all of the new features for this release, see the Release Notes. For the latest caveats, see the Bug Search Tool at https://tools.cisco.com/bugsearch/.



CHAPTER 2

Overview

About the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM)

The Cisco Application Policy Infrastructure Controller - Enterprise Module (APIC-EM) is Cisco's Software Defined Networking (SDN) Controller for Enterprise Networks (Access, Campus, WAN and Wireless).

The platform hosts multiple applications (SDN apps) that use open northbound REST APIs that drive core network automation solutions. The platform also supports a number of south-bound protocols that enable it to communicate with the breadth of network devices that customers already have in place, and extend SDN benefits to both greenfield and brownfield environments.

The Cisco APIC-EM platform supports both wired and wireless enterprise networks across the Campus, Branch and WAN infrastructures. It offers the following benefits:

- Creates an intelligent, open, programmable network with open APIs
- Saves time, resources, and costs through advanced automation
- Transforms business intent policies into a dynamic network configuration
- Provides a single point for network wide automation and control

The following table describes the features and benefits of the Cisco APIC-EM.

Table 1: Cisco APIC Enterprise Module Features and Benefits

Feature	Description
Network Information Database	The Cisco APIC-EM periodically scans the network to create a “single source of truth” for IT. This inventory includes all network devices, along with an abstraction for the entire enterprise network.

Feature	Description
Network topology visualization	The Cisco APIC-EM automatically discovers and maps network devices to a physical topology with detailed device-level data. The topology of devices and links can also be presented on a geographical map. You can use this interactive feature to troubleshoot your network.
EasyQoS application	The EasyQoS application abstracts away the complexity of deploying Quality of Service across a heterogeneous network. It presents users with a workflow that allows them to think of QoS in terms of business intent policies that are then translated by Cisco APIC-EM into a device centric configuration.
Cisco Network Plug and Play (PnP) application	The Cisco Network PnP solution extends across Cisco's enterprise portfolio. It provides a highly secure, scalable, seamless, and unified zero-touch deployment experience for customers across Cisco routers, switches and wireless access points. **Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*.
Cisco Intelligent WAN (IWAN) application	The separately licensed IWAN application for APIC-EM simplifies the provisioning of IWAN network profiles with simple business policies. The IWAN application defines business-level preferences by application or groups of applications in terms of the preferred path for hybrid WAN links. Doing so improves the application experience over any connection and saves telecom costs by leveraging cheaper WAN links. **Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*.

Feature	Description
Cisco Active Advisor application	The Cisco Active Advisor application for APIC-EM offers personalized life cycle management for your network devices by keeping you up-to-date on: • End-of-life milestones for hardware and software • Product advisories, including Product Security Incident Response Team (PSIRT) bulletins and field notices • Warranty and service contract status **Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*.
Cisco Integrity Verification application	The Cisco Integrity Verification (IV) application provides automated and continuous monitoring of network devices, noting any unexpected or invalid results that may indicate compromise. The objective of the Cisco IV application is early detection of the compromise, so as to reduce its impact. The Cisco IV application operates within the Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) as a beta version for this release. **Note** This application is not bundled with the Cisco APIC-EM controller for this release. You need to download, install, and enable this application to use it. For information about these procedures, see the *Cisco Application Infrastructure Controller Enterprise Module Upgrade Guide*.
Cisco Remote Troubleshooter application	The Cisco Remote Troubleshooter application uses the Cisco IronPort infrastructure to create a tunnel that enables a support engineer to connect to an APIC-EM cluster and troubleshoot issues with your system. The app uses outbound SSH to create a secure connection to the cluster through this tunnel. As an administrator, you can use the Remote Troubleshooter application to control when a support engineer has access to a particular cluster and for how long (since a support engineer cannot establish a secure tunnel on their own). You will receive indication that a support engineer establishes a remote access session, and you can end a session at any time by disabling the tunnel they are using.
Public Key Infrastructure (PKI) server	The Cisco APIC-EM provides an integrated PKI service that acts as Certificate Authority (CA) or sub-CA to automate X.509 SSL certificate lifecycle management. Applications, such as IWAN and PnP, use the capabilities of the embedded PKI service for automatic SSL certificate management.

Feature	Description
Path Trace application	The path trace application helps to solve network problems by automating the inspection and interrogation of the flow taken by a business application in the network.
High Availability (HA)	HA is provided in N+ 1 redundancy mode with full data persistence for HA and Scale. All the nodes work in Active-Active mode for optimal performance and load sharing.
Back Up and Restore	The Cisco APIC-EM supports complete back up and restore of the entire database from the controller GUI.
Audit Logs	The audit log captures user and network activity for the Cisco APIC-EM applications.

Cisco APIC-EM Installation Methods

You can install Cisco APIC-EM using any one of the following methods:

- **Appliance Installation**—As a dedicated Cisco APIC-EM physical appliance purchased from Cisco with an ISO image pre-installed. For information about this type of installation, see About the Appliance Installation, on page 9.
- **Bare-Metal Hardware Installation**—As a downloadable ISO image that you can burn to a dual-layer DVD or a bootable USB flash drive, and then use either the DVD or flash drive to install the ISO image onto a server. For information about this type of installation, see About the Bare-Metal Hardware Installation, on page 41.

  Note that this platform (bare-metal hardware) is recommended over the following virtual machine option
- **Virtual Machine Installation**—As a downloadable ISO image that you can install into a virtual machine within a VMware vSphere environment. For information about this type of installation, see About the Virtual Machine Installation, on page 53.

Primary Components

The following are the primary components required for a Cisco APIC-EM installation:

- The Cisco APIC-EM software either pre-installed on a Cisco appliance or provided as an ISO image downloaded from the Cisco website.
- Supported Cisco routing and switching platforms

The Cisco APIC-EM ISO image (either preinstalled on the appliance or downloaded from the Cisco website) consists of the following components:

- Ubuntu 14.04.5 LTS 64-bit
- Open-VM-Tools
- Cisco APIC-EM services

- Grapevine Elastic Services Platform, consisting of a Grapevine root and client template

Note Open-VM-Tools is only installed if the ISO image is installed within a virtual machine running on vSphere. The tools will not be installed if the ISO image is installed on a bare-metal or on a hypervisor from another vendor.

The Cisco APIC-EM makes use of the Ubuntu operating system environment and Linux containers (LXC). The Grapevine root runs within the host's operating system. The Grapevine clients run in LXCs within the host. The Cisco APIC-EM services that run on the Grapevine Elastic Services Platform provide the controller with its core functionality. For information about the services, see *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

IP Connectivity

The Cisco APIC-EM communicates with its supported platforms using the following protocols:

- SNMPv2c or SNMPv3
- Telnet or SSH

Note Currently, the Cisco APIC-EM supports IPv4 only. IPv6 support is planned for a future release.

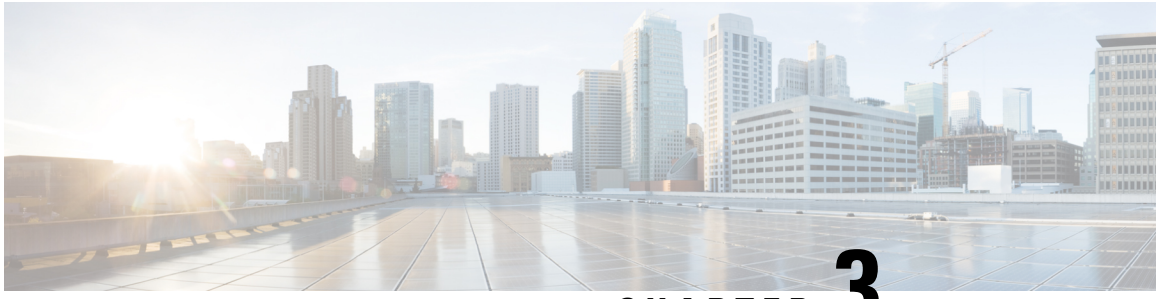
Supported Cisco Platforms and Software Releases

For information about the supported Cisco platforms and software releases, see the relevant controller and/or application documentation. For information about and access to all of the Cisco APIC-EM controller and application documentation, see:

http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-series-home.html

Supported Northbound REST APIs

The Cisco APIC-EM provides northbound REST APIs that you can use to that you can use to issue requests to the controller and exchange data with the controller in a platform-agnostic way. For detailed information about supported northbound REST APIs, see the internal, interactive documentation located within the GUI itself. Click the **API** button at the top right of the GUI to view this documentation.



CHAPTER 3

Installing the Cisco APIC-EM Appliance

About the Appliance Installation

Cisco offers a physical appliance that can be purchased with the ISO image pre-installed and tested. You can deploy this appliance within your network. The Cisco APIC-EM can be deployed as a single host (single appliance in standalone mode) or within a multi-host environment (multiple appliances in multi-host mode).

Important We recommend that you install and deploy Cisco APIC-EM in multi-host mode for enhanced scalability and redundancy. For information about multi-host support, see Multi-Host Support, on page 137.

The following table lists the steps for installing the Cisco APIC-EM appliance.

Table 2: Cisco APIC-EM Appliance Installation

Step	Description
1	Review the pre-install checklists for the appliance (standalone and multi-host modes). See Pre-Install Checklists, on page 11.

Step	Description
2	Review information about the different types of appliances and their specifications, including the following: • Physical • Environmental • Power • Front and rear panels See Cisco APIC-EM Series Appliances, on page 13.
3	Review information about port usage for the controller. See Cisco APIC-EM Ports Reference, on page 19.
4	Prepare the appliance for installation. See Preparing for Appliance Installation, on page 21.
5	(Optional) Install the appliance in a rack. See Installing the Appliance In a Rack, on page 24.
6	Connect power to the appliance and power it on. See Connecting and Powering On the Appliance, on page 28.
7	Check the appliance LEDs. See Checking the LEDs, on page 29.
8	(Optional) Install and/or replace appliance components, if necessary. See Installing or Replacing Appliance Components , on page 32.
9	(Optional) Install a new ISO on the appliance, if necessary. See Installing a New ISO on the Appliance, on page 32.
10	Proceed to 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, on page 72 • Configuring Cisco APIC-EM in Multi-Host Mode, on page 93

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.
  - For a multi-host configuration with Cisco APIC-EM located behind a NAT within your network, note the following information and requirement:
    - The Virtual IP address of the Cisco APIC-EM controller is intended as a destination address for HTTP(S) traffic such as Cisco PnP and PKI download requests.
    - Any outbound connections initiated from the Cisco APIC-EM controller, such as during a Discovery, Inventory Collection, etc., will use the host IP address of one of the three Cisco APIC-EM hosts.
    - Therefore, you need to PAT (Port Address Translation) the host IP addresses of the Cisco APIC-EM hosts to a global public facing IP address for outbound connections from Cisco APIC-EM controller.

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 Series Appliances

Cisco provides a dedicated Cisco APIC-EM physical appliance that can be purchased from Cisco with the ISO image preinstalled and tested. The following physical appliances are currently available for purchase from Cisco:

- Cisco APIC-EM Controller Appliance 10C-64G-2T (Part Number APIC-EM-APL-R-K9)
- Cisco APIC-EM Controller Appliance 20C-128G-4T (Part Number APIC-EM-APL-G-K9)

The following table describes the basic system configurations for these appliances.

Platform	APIC-EM-APL-R-K9	APIC-EM-APL-G-K9
Physical CPU	1 physical CPU	2 physical CPUs
CPU (cores)	10 **Note** Hyper-threading is enabled by default, therefore 20 logical processors are available for this appliance.	20 **Note** Hyper-threading is enabled by default, therefore 40 logical processors are available for this appliance.
RAM	64 GB	128 GB
Total Disk Space	1.7 TB	3.4 TB
Ethernet NICs	2 (Gigabit Ethernet ports)	2 (Gigabit Ethernet ports)

Appliance Scale Limits

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

Physical Specifications

The following table lists the physical specifications for the Cisco APIC-EM appliances.

Table 3: Physical Specifications

Description	Specification
Height	1.7 in. (4.3 cm)
Width	16.9 in. (42.9 cm)
Depth (length)	29.8 in. (75.8 cm)
Maximum weight (fully loaded chassis)	SFF 8-drive: 37.9 lb. (17.2 Kg) LFF 4-drive: 39.9 lb. (18.1 Kg)

Environmental Specifications

The following table lists the environmental specifications for the Cisco APIC-EM appliances.

Table 4: Environmental Specifications

Description	Specification
Temperature, operating	41 to 95°F (5 to 35°C) Derate the maximum temperature by 1°C per every 305 meters of altitude above sea level.
Temperature, non-operating (when the server is stored or transported)	–40 to 149°F (–40 to 65°C)
Humidity (RH), operating	10 to 90%
Humidity, non-operating	5 to 93%
Altitude, operating	0 to 10,000 feet
Altitude, non-operating (when the server is stored or transported)	0 to 40,000 feet
Sound power level Measure A-weighted per ISO7779 LwAd (Bels) Operation at 73°F (23°C)	5.4
Sound pressure level Measure A-weighted per ISO7779 LpAm (dBA) Operation at 73°F (23°C)	37

Power Specifications

The power specifications for the power supply are listed in the following section.

Note You can get more specific power information for your exact appliance configuration by using the Cisco UCS Power Calculator: http://ucspowercalc.cisco.com

Caution Do not mix power supply types in the appliance. Both power supplies must be identical.

770 W AC Power Supply

The following table lists the specifications for each 770 W AC power supply (Cisco part number UCSC-PSU1-770W).

Table 5: AC Power Supply Specifications

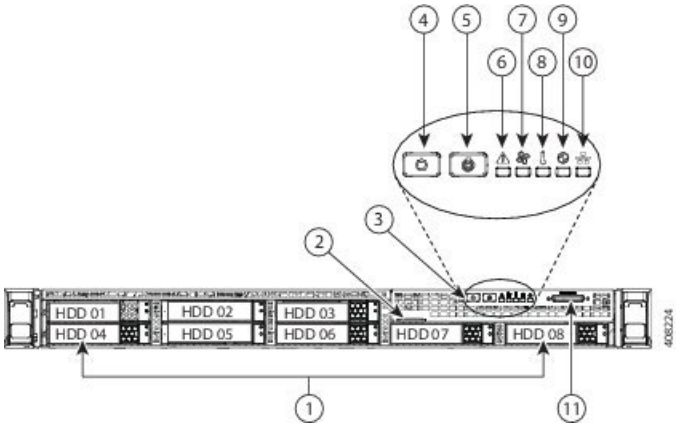
Description	Specification
AC input voltage	Nominal range: 100–120 VAC, 200–240 VAC (Range: 90–132 VAC, 180–264 VAC)
AC input frequency	Nominal range: 50 to 60Hz (Range: 47–63 Hz)
Maximum AC input current	9.5 A at 100 VAC 4.5 A at 208 VAC
Maximum input volt-amperes	950 VA at 100 VAC
Maximum output power per PSU	770 W
Maximum inrush current	15 A (sub-cycle duration)
Maximum hold-up time	12 ms at 770 W
Power supply output voltage	12 VDC
Power supply standby voltage	12 VDC
Efficiency rating	Climate Savers Platinum Efficiency (80Plus Platinum certified)
Form factor	RSP2
Input connector	IEC320 C14

Cisco APIC-EM Series Front and Rear Panels

The following figure displays the Cisco APIC-EM appliance front panel (APIC-EM-APL-G-K9).

Note The Cisco APIC-EM appliance front panel (APIC-EM-APL-R-K9) shares a similar design.

Figure 1: Cisco APIC-EM Appliance Front Panel (APIC-EM-APL-G-K9)

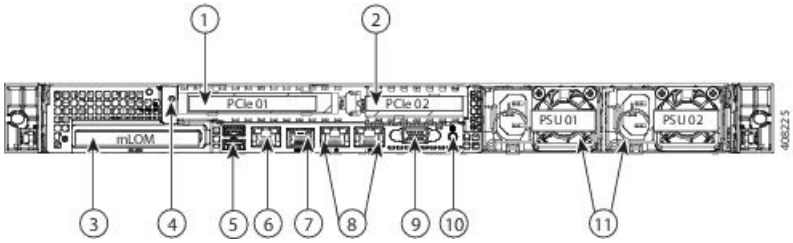


Component	Description
1	Drives (up to eight 2.5-inch drives)
2	Pull-out asset tag
3	Operations panel buttons and LEDs
4	Power button/power status LED
5	Unit identification button/LED
6	System status LED
7	Fan status LED
8	Temperature status LED
9	Power supply status LED
10	Network link activity LED
11	KVM connector (used with KVM cable that provides two USB 2.0, one VGA, and one serial connector)

The following figure displays the Cisco APIC-EM appliance rear panel (APIC-EM-APL-G-K9).

Note The Cisco APIC-EM appliance rear panel (APIC-EM-APL-R-K9) shares a similar design.

Figure 2: Cisco APIC-EM Appliance Rear Panel (APIC-EM-APL-G-K9)



Component	Description
1	PCIe riser 1/slot 1
2	PCIe riser 2/slot 2
3	Modular LAN-on-motherboard (mLOM) card slot
4	Grounding-lug hole (for DC power supplies)
5	USB 3.0 ports (two)
6	1-Gb Ethernet dedicated management port
7	Serial port (RJ-45 connector)
8	Dual 1-Gb Ethernet ports (LAN1 and LAN2)
9	VGA video port (DB-15)
10	Rear unit identification button/LED
11	Power supplies (up to two, redundant as 1+1)

Summary of Appliance Series Features

The following table lists the Cisco APIC-EM appliance series features.

Table 6: Cisco APIC-EM Appliance Series Features

Feature	Description
Chassis	One rack-unit (1RU) chassis.
Processors	Up to two Intel Xeon CPU E5-2650 v3 Series processors.
Memory	24 DDR4 DIMM sockets on the motherboard (12 each CPU).
Baseboard management	BMC, running Cisco Integrated Management Controller (Cisco IMC) firmware. Depending on your Cisco IMC settings, Cisco IMC can be accessed through the 1-Gb dedicated management port, the 1-Gb Ethernet LOM ports, or a Cisco virtual interface card.

Feature	Description
Network and Management I/O	Supported connectors:[1] • One 1-Gb Ethernet dedicated management port • Two 1-Gb BASE-T Ethernet LAN ports • One RS-232 serial port (RJ-45 connector) • One 15-pin VGA2 connector • Two USB3 3.0 connectors • One front-panel KVM connector that is used with the KVM cable, which provides two USB 2.0, one VGA, and one serial (DB-9) connector
Modular LOM	Dedicated socket that can be used to add an mLOM card for additional rear-panel connectivity (up to four 1-Gb or 10-Gb Ethernet ports).
Power	Two power supplies: • AC power supplies 770 W AC each. Do not mix power supply types or wattages in the server. Redundant as 1+1.
Cooling	Six hot-swappable fan modules for front-to-rear cooling.
Storage	• APIC-EM-APL-R-K9: 4 SAS HDD of 900 GB each • APIC-EM-APL-G-K9: 8 SAS HDD of 900 GB each
Disk Management (RAID)	Hardware-based RAID at RAID Level 10
Video	VGA video resolution up to 1920 x 1200, 16 bpp at 60 Hz, and up to 256 MB of video memory.

[1] The Intel X520 2 Port 10G PCI adapter (Part No. N2XX-AIPCI01) and 10G SFP+ (Part No. CDE2-SFP-1WSR=) is now supported for the Cisco APIC-EM Appliance Server.

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 7: 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 [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
16026	SCEP	TCP

[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*.

Table 8: 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
53	DNS	UDP

Port Number	Permitted Traffic	Protocol (TCP or 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 [3]	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

[3] 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*.

Preparing for Appliance Installation

This section provides information about preparing for the Cisco APIC-EM series appliance installation.

Unpack and Inspect the Appliance

⚠

Caution When handling internal appliance components, wear an ESD strap and handle modules by the carrier edges only.

Tip Keep the shipping container in case the appliance requires shipping in the future.

Note The chassis is thoroughly inspected before shipment. If any damage occurred during transportation or any items are missing, contact your customer service representative immediately.

Step 1 Remove the appliance from its cardboard container and save all packaging material.

Step 2 Compare the shipment to the equipment list provided by your customer service representative. Verify that you have all items.

Step 3 Check for damage and report any discrepancies or damage to your customer service representative. Have the following information ready:

- Invoice number of shipper (see the packing slip)
- Model and serial number of the damaged unit
- Description of damage
- Effect of damage on the installation

Installation Guidelines

Warning **To prevent the system from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of: 40° C (104° F).** Statement 1047

Warning **The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.** Statement 1019

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 250 V, 15 A.** Statement 1005

Warning **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

Caution To ensure proper airflow it is necessary to rack the appliances using rail kits. Physically placing the units on top of one another or “stacking” without the use of the rail kits blocks the air vents on top of the appliances, which could result in overheating, higher fan speeds, and higher power consumption. We recommend that you mount your appliances on rail kits when you are installing them into the rack because these rails provide the minimal spacing required between the appliances. No additional spacing between the appliances is required when you mount the units using rail kits.

Caution Avoid UPS types that use ferroresonant technology. These UPS types can become unstable with systems such as the Cisco UCS, which can have substantial current draw fluctuations from fluctuating data traffic patterns.

When you are installing an appliance, use the following guidelines:

- Plan your site configuration and prepare the site before installing the appliance. For reference, see the Cisco UCS Site Preparation Guide for the recommended site planning tasks.
- Ensure that there is adequate space around the appliance to allow for servicing the appliance and for adequate airflow. The airflow in this appliance is from front to back.
- Ensure that the air-conditioning meets the thermal requirements listed in the Environmental Specifications, on page 14.
- Ensure that the cabinet or rack meets the requirements listed in the following "Rack Requirements" section.
- Ensure that the site power meets the power requirements listed in the Power Specifications, on page 15. If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

Review the Rack Requirements

This section provides the requirements for the standard open racks.

The rack must be of the following type:

- A standard 19-in. (48.3-cm) wide, four-post EIA rack, with mounting posts that conform to English universal hole spacing, per section 1 of ANSI/EIA-310-D-1992.
- The rack post holes can be square 0.38-inch (9.6 mm), round 0.28-inch (7.1 mm), #12-24 UNC, or #10-32 UNC when you use the supplied slide rails.
- The minimum vertical rack space per server must be one RU, equal to 1.75 in. (44.45 mm).

Review the Equipment Requirements

The slide rails sold by Cisco Systems for this appliance do not require tools for installation.

Supported Slide Rail Kits

This appliance supports two rail kit options:

- Cisco part UCSC-RAILB-M4= (ball-bearing rail kit).
- Cisco part UCSC-RAILF-M4= (friction rail kit).

Do not attempt to use a rail kit that was for the Cisco UCS C220 M3 server; the rail kits for the Cisco APIC-EM appliance have been designed specifically for it.

Slide Rail Adjustment Range and Cable Management Arm Dimensions

The slide rails for this server have an adjustment range of 24 to 36 inches (610 to 914 mm).

The optional cable management arm (CMA) adds additional length requirements:

- The additional distance from the rear of the server to the rear of the CMA is 5.4 inches (137.4 mm).
- The total length of the server including the CMA is 35.2 inches (894 mm).

Installing the Appliance In a Rack

Installing the Slide Rails

This section describes how to install the appliance in a rack using the rack kits that are sold by Cisco.

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety: This unit should be mounted at the bottom of the rack if it is the only unit in the rack. When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack. If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack**.

Statement 1006

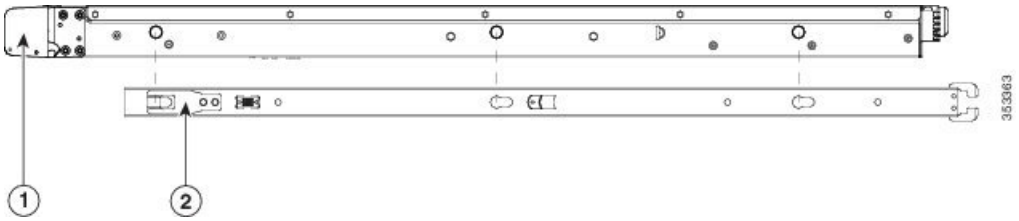
Step 1 Attach the inner rails to the sides of the server:

a) Align an inner rail with one side of the server so that the three keyed slots in the rail align with the three pegs on the side of the server (see below figure).

b) Set the keyed slots over the pegs, and then slide the rail toward the front to lock it in place on the pegs. The front slot has a metal clip that locks over the front peg.

c) Install the second inner rail to the opposite side of the server.

Figure 3: Attaching Inner Rail to Side of Server

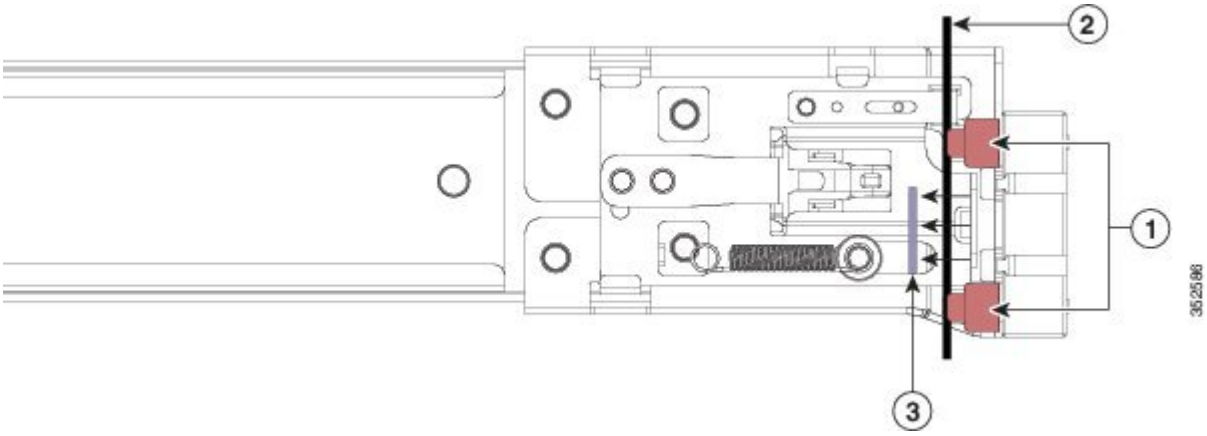


1	Front of server
2	Locking clip on inner rail

Step 2 Open the front securing plate on both slide-rail assemblies.

The front end of the slide-rail assembly has a spring-loaded securing plate that must be open before you can insert the mounting pegs into the rack-post holes. On the outside of the assembly, push the green arrow button toward the rear to open the securing plate.

Figure 4: Front Securing Mechanism, Inside of Front End



1	Front mounting pegs
2	Rack post
3	Securing plate shown pulled back to open position

Step 3 Install the outer slide rails into the rack:

a) Align one slide-rail assembly front end with the front rack-post holes that you want to use.

The slide rail front-end wraps around the outside of the rack post and the mounting pegs enter the rack-post holes from the outside-front

Note The rack post must be between the mounting pegs and the open securing plate.

b) Push the mounting pegs into the rack-post holes from the outside-front.

c) Press the securing plate release button, marked PUSH. The spring-loaded securing plate closes to lock the pegs in place.

d) Adjust the slide-rail length, and then push the rear mounting pegs into the corresponding rear rack-post holes. The slide rail must be level front-to-rear.

The rear mounting pegs enter the rear rack-post holes from the inside of the rack post.

e) Attach the second slide-rail assembly to the opposite side of the rack. Ensure that the two slide-rail assemblies are at the same height with each other and are level front-to-back.

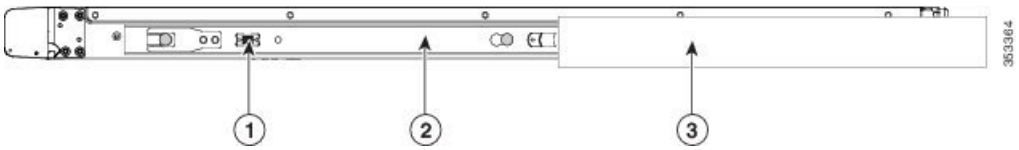
f) Pull the inner slide rails on each assembly out toward the rack front until they hit the internal stops and lock in place.

Step 4 Insert the server into the slide rails:

Caution This server can weigh up to 67 pounds (59 kilograms) when fully loaded with components. We recommend that you use a minimum of two people or a mechanical lift when lifting the server. Attempting this procedure alone could result in personal injury or equipment damage.

a) Align the rear of the inner rails that are attached to the server sides with the front ends of the empty slide rails on the rack
b) Push the inner rails into the slide rails on the rack until they stop at the internal stops.
c) Slide the release clip toward the rear on both inner rails, and then continue pushing the server into the rack until its front slam latches engage with the rack posts.

Figure 5: Inner Rail Release Clip



1	Inner rail release clip
2	Inner rail attached to server and inserted into outer rail
3	Outer rail attached to rack post

Step 5 (Optional) Secure the server in the rack more permanently by using the two screws that are provided with the slide rails. Perform this step if you plan to move the rack with servers installed.

With the server fully pushed into the slide rails, open a hinged slam latch lever on the front of the server and insert the screw through the hole that is under the lever. The screw threads into the static part of the rail on the rack post and prevents the server from being pulled out. Repeat for the opposite slam latch.

What to do next

If necessary for your installation, install the cable management arm.

Installing the Cable Management Arm (Optional)

The following procedure describes how to install the cable management arm.

Before you begin

The CMA is reversible left to right. To reverse the CMA, see Reversing the Cable Management Arm (Optional) section, before installation.

Step 1 With the server pushed fully into the rack, slide the CMA tab of the CMA arm that is farthest from the server onto the end of the stationary slide rail that is attached to the rack post (see the figure below). Slide the tab over the end of the rail until it clicks and locks.

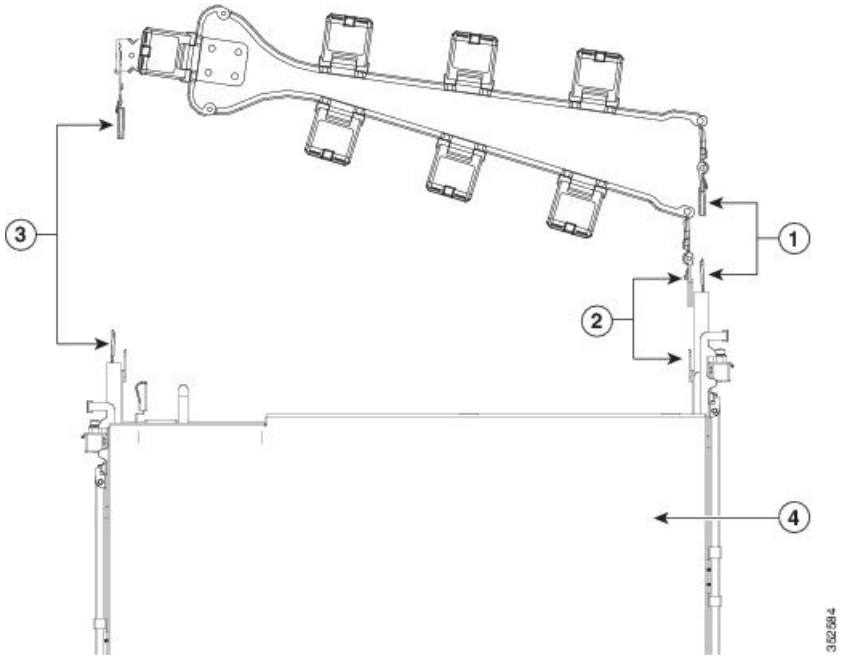
Step 2 Slide the CMA tab that is closest to the server over the end of the inner rail that is attached to the server (see the figure below). Slide the tab over the end of the rail until it clicks and locks.

Step 3 Pull out the width-adjustment slider that is at the opposite end of the CMA assembly until it matches the width of your rack (see the figure below).

Step 4 Slide the CMA tab that is at the end of the width-adjustment slider onto the end of the stationary slide rail that is attached to the rack post (see figure below). Slide the tab over the end of the rail until it clicks and locks.

Step 5 Open the hinged flap at the top of each plastic cable guide and route your cables through the cable guides as desired.

Figure 6: Installing the Cable Management Arm



The following table describes the components of the CMA.

1	CMA tab on arm farthest from server and end of stationary outer slide rail
2	CMA tab on arm closest to the server and end of inner slide rail attached to server
3	CMA tab on width-adjustment slider and end of stationary outer slide rail
4	Rear of server

Reversing the Cable Management Arm (Optional)

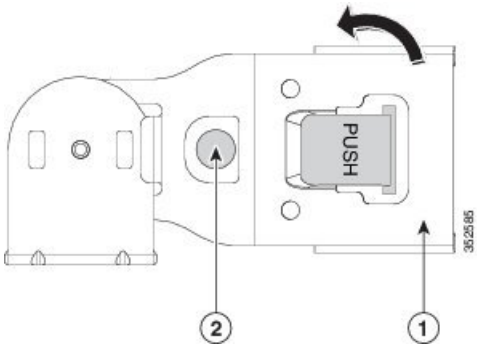
The following procedure describes how to reverse the cable management arm.

Step 1 Rotate the entire CMA assembly 180 degrees. The plastic cable guides must remain pointing upward.

Step 2 Flip the tabs at the end of each CMA arm so that they point toward the rear of the server.

Step 3 Pivot the tab that is at the end of the width-adjustment slider. Depress and hold the metal button on the outside of the tab and pivot the tab 180 degrees so that it points toward the rear of the server.

Figure 7: Reversing the Cable Management Arm



Refer to the following figure when reversing the cable management arm.

1	CMA tab on end of width-adjustment slider
2	Metal button for rotating

Connecting and Powering On the Appliance

This section describes how to power on the appliance and assign an IP address to connect to it.

Step 1 Attach a supplied power cord to each power supply in the appliance and then attach the power cord to a grounded AC power outlet. See the Power Specifications, for power specifications.

Wait for approximately two minutes to let the appliance boot in standby power during the first bootup.

You can verify the power status by looking at the Power Status LED:

- Off—There is no AC power present in the appliance.
- Amber—The appliance is in standby power mode. Power is supplied only to the CIMC and some motherboard functions.
- Green—The appliance is in main power mode. Power is supplied to all appliance components.

Note During bootup, the appliance beeps once for each USB device that is attached to the appliance. Even if there are no external USB devices attached, there is a short beep for each virtual USB device such as a virtual floppy drive, CD/DVD drive, keyboard, or mouse. A beep is also emitted if a USB device is hot-plugged or hot-unplugged during BIOS power-on self-test (POST), or while you are accessing the BIOS Setup utility or the EFI shell.

Step 2 Connect a USB keyboard and VGA monitor by using the supplied KVM cable connected to the KVM connector on the front panel.

Note Alternatively, you can use the VGA and USB ports on the rear panel. However, you cannot use the front panel VGA and the rear panel VGA at the same time. If you are connected to one VGA connector and you then connect a video device to the other connector, the first VGA connector is disabled.

Step 3 Refer to the following sections for configuring and using CIMC to assign an IP address to the appliance:

- Configuring CIMC, on page 34
- Using CIMC to Configure a Cisco APIC-EM Series Appliance, on page 37

Checking the LEDs

When the Cisco APIC-EM series appliances have been started up and are running, observe the state of the front-panel and rear-panel LEDs. The following sections describe the LED color, its power status, activity, and other important status indicators that are displayed for the Cisco APIC-EM series appliance.

Front Panel LEDs and Buttons

The following table describes the appliance front panel LEDs and buttons on the appliance.

Note The minimum network interface speed for the appliance should be 1 GB a second.

Table 9: Front Panel LEDs and Buttons

LED Name	State
Front Panel LEDs and Buttons	Off—There is no AC power to the appliance. Amber—The appliance is in standby power mode. Power is supplied only to the CIMC and some motherboard functions. Green—The appliance is in main power mode. Power is supplied to all server components.
Identification	Off—The Identification LED is not in use. Blue—The Identification LED is activated.

LED Name	State
System status	Green—The appliance is running in a normal operating condition. Green, blinking—The appliance is performing system initialization and memory checks. Amber, steady—The appliance is in a degraded operational state, which may be due to one of the following: – Power supply redundancy is lost. – CPUs are mismatched. – At least one CPU is faulty. – At least one DIMM is faulty. – At least one drive in a RAID configuration failed. Amber, blinking—The appliance is in a critical fault state, which may be due to one of the following: – Boot failed. – Fatal CPU and/or bus error is detected. – Server is in an over-temperature condition.
Fan status	Green—All fan modules are operating properly. Amber, steady—One fan module has failed. Amber, blinking—Critical fault, two or more fan modules have failed.
Temperature status	Green—The appliance is operating at normal temperature. Amber, steady—One or more temperature sensors have exceeded a warning threshold. Amber, blinking—One or more temperature sensors have exceeded a critical threshold
Power supply status	Green—All power supplies are operating normally. Amber, steady—One or more power supplies are in a degraded operational state. Amber, blinking—One or more power supplies are in a critical fault state.
Network link activity	Off—The Ethernet link is idle. Green—One or more Ethernet LOM ports are link-active, but there is no activity. Green, blinking—One or more Ethernet LOM ports are link-active, with activity.

LED Name	State
Hard drive fault	Off—The hard drive is operating properly. Amber—The hard drive has failed. Amber, blinking—The device is rebuilding.
Hard drive activity	Off—There is no hard drive in the hard drive sled (no access, no fault). Green—The hard drive is ready. Green, blinking—The hard drive is reading or writing data.

Rear Panel LEDs and Buttons

The following table describes the appliance rear panel LEDs and buttons on the appliance.

Note The minimum network interface speed for the appliance should be 1 GB a second.

Table 10: Rear Panel LEDs and Buttons

LED Name	State
Power supply fault	Off—The power supply is operating normally. Amber, blinking—An event warning threshold has been reached, but the power supply continues to operate. Amber, solid—A critical fault threshold has been reached, causing the power supply to shut down (for example, a fan failure or an over-temperature condition).
Power supply AC OK	Off—There is no AC power to the power supply. Green, blinking—AC power OK, DC output not enabled. Green, solid—AC power OK, DC outputs OK.
1 Gb Ethernet dedicated management link speed	Off—link speed is 10 Mbps. Amber—link speed is 100 Mbps. Green—link speed is 1 Gbps.

LED Name	State
1 Gb Ethernet dedicated management link status	Off—No link is present. Green—Link is active. • Green, blinking—Traffic is present on the active link.
1 Gb Ethernet link speed	Off—link speed is 10 Mbps. Amber—link speed is 100 Mbps. Green—link speed is 1 Gbps.
1 Gb Ethernet link status	Off—No link is present. Green—Link is active. Green, blinking—Traffic is present on the active link.
Identification	Off—The Identification LED is not in use. Blue—The Identification LED is activated.

Installing or Replacing Appliance Components

Refer to the Cisco UCS C220 Server Installation and Service Guide for information on how to install or replace the Cisco APIC-EM appliance components.

Installing a New ISO on the Appliance

Under certain circumstances, you may need to install a new or the latest Cisco ISO image on the appliance. This section describes the following procedures that you can use to perform this task:

- Downloading the Cisco APIC-EM ISO image
- Installing the Cisco APIC-EM ISO image on the Cisco APIC-EM series appliances using one of the following procedures:
  - Install the ISO image using the CIMC Remote Management Utility
  - Install the ISO image using a USB flash drive
  - Install the ISO image using an external DVD drive with a USB port

Downloading the Cisco APIC-EM ISO Image

You can download the latest Cisco APIC-EM ISO image from Cisco.com

Step 1 Go to the following URL address:

http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/tsd-products-support-general-information.html

You must already have valid Cisco.com login credentials to access this link.

Step 2 Click **Download Software for this Product**.

Proceed to download the ISO file to a secure location on your network.

Installing the ISO Image on the Cisco APIC-EM Series Appliance

After you download the ISO image, you can perform a fresh installation on your Cisco APIC-EM series appliance by using any of the following methods:

- Install the ISO image using the CIMC Remote Management Utility.
  1. Configure CIMC.
  2. Install the Cisco APIC-EM software release remotely.

Important You must configure the CIMC to perform this remote installation. For information about configuring CIMC, see Configuring CIMC, on page 34.

- Install the ISO image using a USB flash drive.
  1. Create a bootable USB disk from the USB flash drive.
  2. Connect the bootable USB disk to the Cisco APIC-EM series appliance.
  3. Install the Cisco APIC-EM software release using the local KVM or remotely using the CIMC KVM.

Note For information about creating a bootable USB disk from a USB flash drive, see Creating a Bootable USB Disk and Attaching the ISO, on page 36.

- Install the ISO using an external DVD drive with a USB port.
  1. Burn the ISO image on to a DVD.
  2. Connect the external USB DVD to the Cisco APIC-EM series appliance.
  3. Install the Cisco APIC-EM software release via the local KVM or remotely using the CIMC KVM.

Note If your Cisco APIC-EM series appliance is running an earlier version of the controller software, you can upgrade it to the latest version by following the upgrade procedure using the GUI as described in the *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*. Currently, reimaging your existing Cisco APIC-EM series appliance to perform an upgrade to the latest release is not supported.

Note For installing the Cisco APIC-EM software release using a USB flash device or an external DVD with a USB port, the CIMC configuration is optional. Choose one of these options if you do not prefer a remote installation.

Configuring CIMC

You can perform all operations on Cisco APIC-EM series appliances using the CIMC. To do this, you must first configure an IP address and IP gateway to access the CIMC from a web-based browser.

Step 1 Attach a keyboard and monitor to the USB ports on the rear panel of the appliance or by using a KVM cable and connector to access the appliance console.

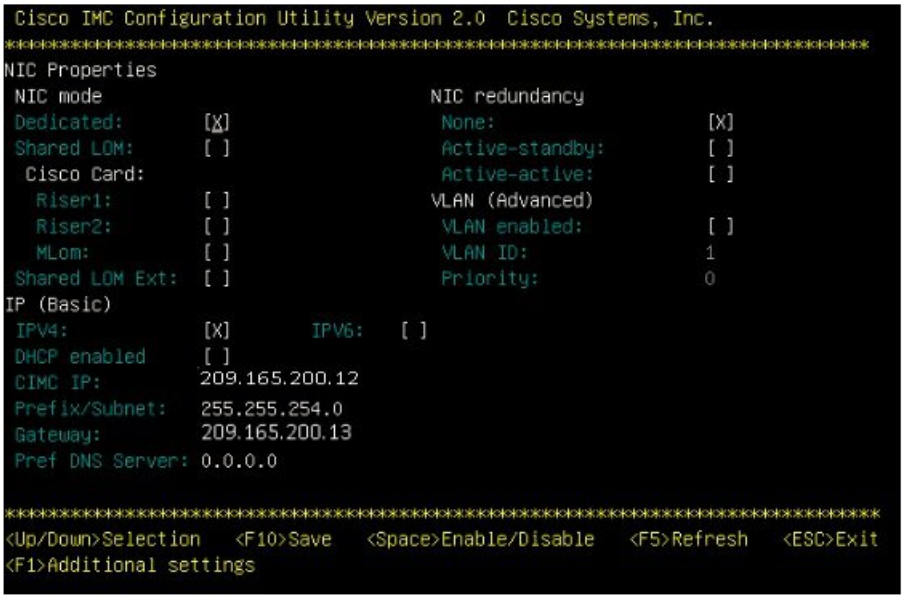
Step 2 Plug in the power cord.

Step 3 Press the **Power** button to boot the server. Watch for the prompt to press **F8** as shown in the following screen.

Figure 8: CIMC Opening Screen

Step 4 During bootup, press **F8** when prompted to open the BIOS CIMC Configuration Utility. The following screen appears.

Figure 9: CIMC Configuration Utility



Step 5 In the Configuration Utility window, change the following fields as specified:

- **NIC mode**—Select Dedicated.
- **IP (Basic)**—Select IPV4.
- **CIMC IP**—Enter the IP address of the CIMC.
- **Prefix/Subnet**—Enter the subnet of the CIMC.
- **Gateway**—Enter the Gateway address.
- **Pref DNS Server**—Enter the preferred DNS server address, if available.
- **NIC Redundancy**—None

Step 6 Press **F1** to specify additional settings.

Step 7 Make the following changes on the Additional Settings window:

- For **Common Properties**, enter a hostname for CIMC.
- For **Common Properties**, turn off Dynamic DNS.
- Turn off the **Factory Defaults**.
- Enter the admin password. If you leave the password field blank, the default password is *password*.

- Enter new **Port Properties** or accept the default.
- Turn off the **Port Profiles**.

Step 8 Press **F10** to save the settings.

Step 9 Press **escape** to exit and reboot the server.

Step 10 After the settings are saved, open a browser and enter the following URL:

`https://CIMC_ip_address` where `CIMC_IP_address` is the IP address that you entered in Step 5.

What to do next

Use CIMC to install the Cisco APIC-EM software release on a Cisco APIC-EM series appliance. For information about this procedure, see Using CIMC to Configure a Cisco APIC-EM Series Appliance, on page 37.

Creating a Bootable USB Disk and Attaching the ISO

Follow the procedure described below to create a bootable USB disk for the Cisco APIC-EM appliance.

Important There are many ways to create a bootable USB disk and this procedure is only one example of such a process of creating a bootable USB disk. This procedure uses the Rufus freeware utility (version 2.6.818) to create a bootable USB disk using a Windows machine. The URL for the Rufus freeware utility download is located at: https://rufus.akeo.ie/.

Before you begin

The USB flash drive that you are using to create a bootable USB disk should have a minimum capacity of at least 8 GB.

Step 1 Download a freeware utility to create a bootable USB disk to your Windows machine (laptop or desktop).

After download, open and install the utility.

Note The Rufus freeware utility will open and self-install.

Step 2 Connect your USB drive to your Windows machine where you downloaded the utility.

After connecting your USB drive, the utility GUI appears. Review the following default values from the drop-down menus for the bootable USB disk:

- **Partition scheme and target system type**: MBR partition scheme for BIOS or UEFI
- **File system**: FAT32
- **Cluster size**: 4096 bytes
- **Quick format** : (Checked)
- **Create a bootable disk using FreeDOS**: (Checked)

- **Create extended label and icon files**: (Checked)

Important Do not change any of the displayed default values in the GUI.

Step 3 Click the **Click to select image** icon located in the middle of the GUI.

The **Click to select image** icon is an image of a CD-ROM that is located in the middle of the GUI field. It is next to the Format Option, **Create a bootable disk using**, with **FreeDOS** selected from the drop-down menu.

Important Keep the drop-down menu set at **FreeDOS**.

Step 4 Navigate to the Cisco APIC-EM ISO image on your network and select it.

Step 5 Click **Start** to begin copying the ISO image to the USB drive.

This action creates the USB drive as a bootable USB disk with the Cisco APIC-EM ISO image installed.

Step 6 Remove the bootable USB disk from the laptop or desktop and use it wherever you will install the controller.

What to do next

Insert the bootable USB disk into the server or appliance where you will install the controller.

Using CIMC to Configure a Cisco APIC-EM Series Appliance

After you configure the CIMC for your appliance, you can use it to manage a Cisco APIC-EM series appliance. You can perform all operations including BIOS configuration through the CIMC.

Before you begin

Ensure that you have connected and powered up the appliance by following the recommended procedures in this guide.

Ensure that you have configured the CIMC on your appliance. For information about this procedure, see Configuring CIMC, on page 34

Ensure that you have the Cisco APIC-EM ISO image on the client machine from which you are accessing the CIMC or you have a bootable USB with the image for installation.

Ensure that you have your Cisco APIC-EM program parameter information available and the requirements ready for deployment (for example, NTP servers).

Step 1 Connect to the CIMC for appliance management.

Connect the Ethernet cables from the LAN to the appliance using the ports selected by the Network Interface Card (NIC) Mode setting. The active-active and active-passive NIC redundancy settings require you to connect to two ports.

Step 2 Use a browser and the IP address of the CIMC to log in to the CIMC Setup Utility.

The IP address is based on the CIMC configuration that you made.

The default username for the server is admin. The default password is *password*.

Step 3 Click **Launch KVM Console** in the CIMC GUI .

Step 4 Use your CIMC credentials to log into the KVM console.

Step 5 Click **Virtual Media** on the **KVM Console** menu bar.

Step 6 Click **Activate Virtual Devices** from the **Virtual Media** drop down menu.

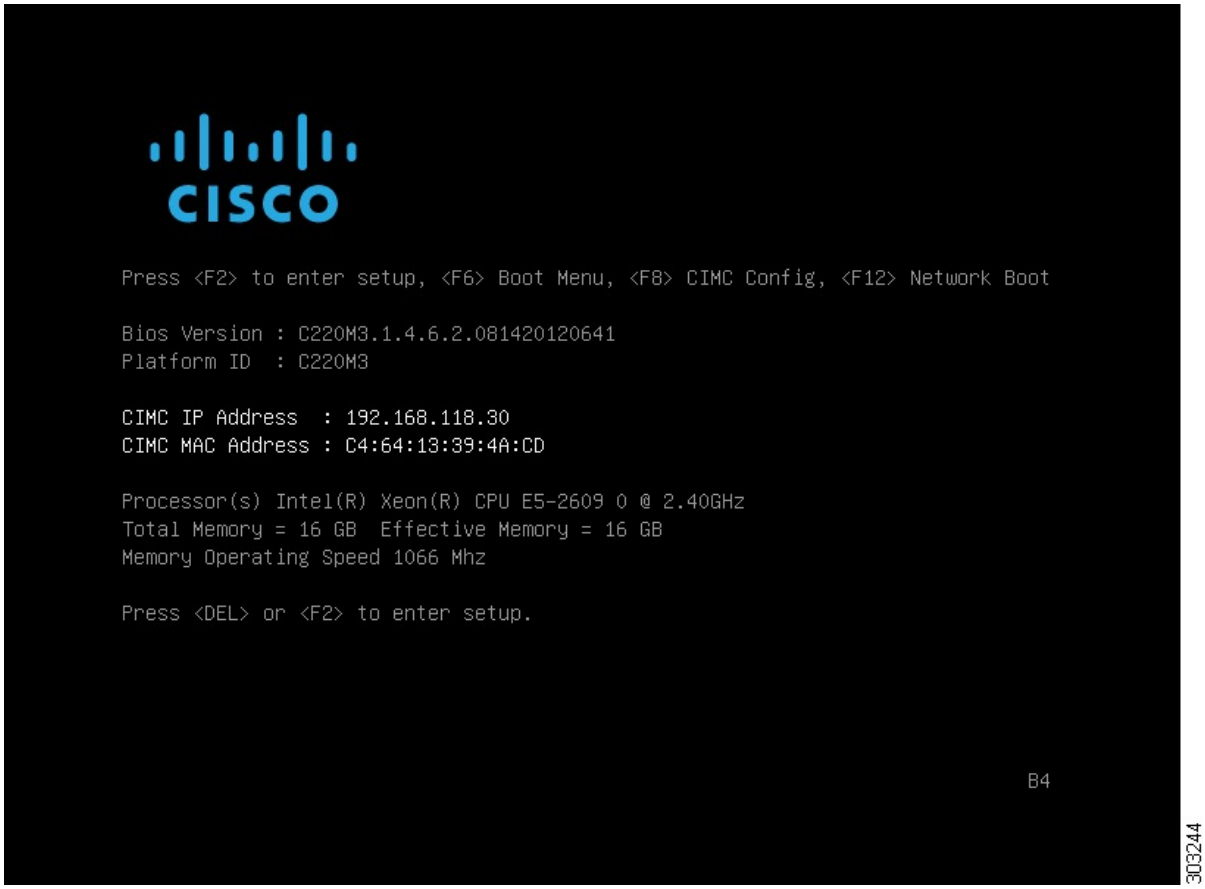
Step 7 Browse to the Cisco APIC-EM ISO image in the **Virtual Media - Map CD/DVD** window.

Step 8 Once the Cisco APIC-EM ISO image appears in the **Drive/Image File** field, click the **Map Device** button.

The **Read Only** check box should be checked in this window.

Step 9 Choose **Macros** | **Static Macros** | **Ctrl-Alt-Del** to boot the Cisco APIC-EM series appliance using the ISO image. A screen similar to the one shown in the following figure appears.

Figure 10: CIMC Window



Step 10 Press **F6** to bring up the boot menu. A screen similar to the following one appears.

Figure 11: Boot Device Window

Step 11 Choose the DVD that you mapped and press **Enter**.

After pressing **Enter**, the Cisco APIC-EM ISO software and files are installed on your appliance.

After these files are installed, the Ubuntu screen briefly appears. Next, the Cisco APIC-EM configuration wizard starts.

Step 12 Proceed to configure the Cisco APIC-EM using the wizard.

If the configuration wizard does not start, then enter the **config_wizard** command initiate the configuration process.

Refer to the following sections for information about the configuration wizard process:

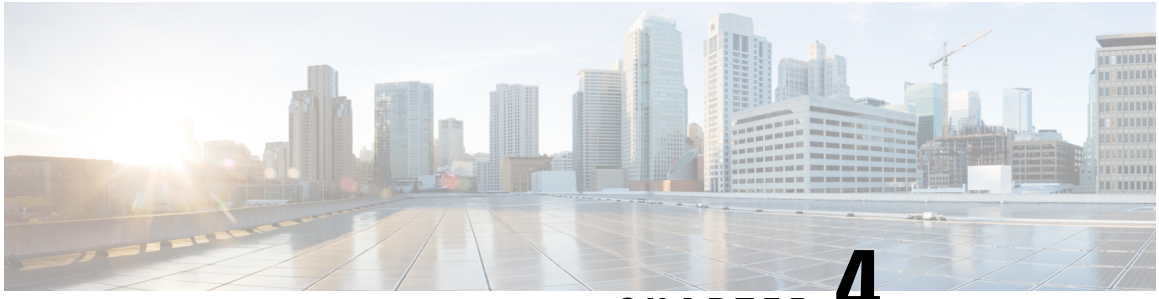
- Configuring Cisco APIC-EM as a Single Host Using the Wizard, on page 72
- Configuring Cisco APIC-EM as a Multi-Host Cluster Using the Wizard, on page 101

After you are done with the configuration wizard and have rebooted, the Cisco APIC-EM GUI Login window appears. The Cisco APIC-EM is now ready to use.

What to do next

At the Cisco APIC-EM GUI Login window, you are prompted to enter the web-based admin login credentials (username and password) to access the Cisco APIC-EM user interface. You can initially access the web interface by using the GUI admin user's username and password that you defined during the setup process.

After you log in to the Cisco APIC-EM user interface, you can then configure your controller settings including discovery credentials, SNMP values, and certificates. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*, for information about configuring the controller settings.



CHAPTER 4

Installing Cisco APIC-EM on Bare-Metal Hardware

About the Bare-Metal Hardware Installation

You can install the Cisco APIC-EM on a server (bare-metal hardware) and then deploy it within your network. The Cisco APIC-EM can be deployed as a single host (single server) or within a multi-host environment (multiple servers).

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, on page 137.

The following table lists the steps for installing the Cisco APIC-EM on a server (bare-metal hardware).

Table 11: Cisco APIC-EM Bare-Metal Hardware Installation

Step	Description
1	Review Cisco UCS server support for Cisco APIC-EM. See Cisco UCS Server Support for Cisco APIC-EM
2	Review the listed considerations for a bare metal installation. See Before You Begin a Bare Metal Installation

Step	Description
3	Review the system requirements for a bare-metal hardware installation. See System Requirements—Server (Bare-Metal Hardware)
4	Review the pre-install checklists for the installation (standalone and multi-host modes). See Pre-Install Checklists
5	Review information about port usage for the controller. See Cisco APIC-EM Ports Reference
6	Download and verify the ISO image. See Verifying the Cisco ISO Image
7	Install the ISO image. See Installing the Cisco ISO Image
8	Proceed to 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, on page 72 • Configuring Cisco APIC-EM in Multi-Host Mode, on page 93

Cisco UCS Server Support for Cisco APIC-EM

The Cisco APIC-EM is available as an ISO image that can be downloaded from Cisco.com and installed on any Cisco UCS server that meets the minimum server (bare-metal hardware) requirements as listed in the following section.

Cisco APIC-EM has been tested and qualified to run on the following Cisco UCS servers:

- Cisco UCS C220 M4S Server
- Cisco UCS C220 M3S Server
- Cisco UCS C22 M3S Server

- For more information about Cisco UCS servers, see the following documentation:

  Cisco Integrated Management Controller documentation:

  http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-integrated-management-controller/tsd-products-support-series-home.html

  Cisco UCS C220 M4 Rack Server Specifications Sheet:

  http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m4-sff-spec-sheet.pdf

  Cisco UCS C220 Server Installation and Service Guide:

  http://www.cisco.com/c/en/td/docs/unified_computing/ucs/hw/C220/install/C220.html

Before You Begin a Bare Metal Installation

Before you begin your bare-metal hardware installation, note the following:

- You must configure RAID on your bare metal hardware before you begin the installation process.
  - Refer to the Cisco APIC-EM hardware specifications for the RAID requirements.

    See System Requirements—Server (Bare-Metal Hardware)
  - Refer to the following Cisco UCS documentation for information about configuring RAID on a Cisco UCS server.

    See: http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/ucsscu/user/guide/30/UCS_SCU/bootraid.html#wp1073012%0A
- If you're using the Cisco server UCS C220 M4S, then change the LOM from shared to dedicated, and change the port speed to Auto-negotiate or 1 Gbps.
- After starting the installation of the ISO, the Cisco APIC-EM software packages will be installed. The bare metal hardware system will reset twice.

Important Do not press any the **Escape** key or any other keys on the keyboard once the installation process has started. Pressing a key will cause the system logs to be displayed during the installation process.

- If you are installing the Cisco APIC-EM ISO using a bootable disk, then you may encounter a known issue with mounting the media (bootable disk). If this occurs, you will receive the following error message:

```
There was a problem reading data from the CD-ROM.
Please make sure it is in the drive. If retrying does not work,
you should check the integrity of your CD-ROM.

Failed to copy file from CD-ROM. Retry?
```

If this occurs, then you need to unmount the media and mount it as a CD-ROM. For example, the following Linux commands can be used to mount the media as a CD-ROM. Log onto the bare metal console to enter these commands.

1. `mount`
2. `unmount /dev/<sda>/`
3. `mount /dev/<sda> /cdrom`

The following is an example of entering these Linux commands:

```
~ #
~ # mount

rootfs on / type rootfs (rw, size=32927728k,nr_inodes=823192)
none on /run type tmpfs (rw, nousid, relatime, size=6586808k,mode=755)
none on /proc type proc (rw, relatime)
none on /sys type sysfs (rw, relatime)
devtmpfs on /dev type devtmpfs (rw, relatime, size=32927744k, nr_inodes-8231936, mode=755)
```

```
devpts on /dev/pts type devpts (re, nosuid, noexec, relatime, gid=5, mode=620,
ptmxmode=000)
/dev/sr0 on /media type iso9660 (ro, relatime)

~ #
~ #
~ # umount /dev/sr0
~ # mount /dev/sr0/cdrom
~ #
~ #
~ #
~ #
~ #
~ #
```

Note For information about and an example of creating a bootable USB disk from a USB flash drive and attaching the ISO to it, see Creating a Bootable USB Disk and Attaching the ISO, on page 36. For additional information about this issue, see https://bugs.launchpad.net/ubuntu/+source/debian-installer/+bug/1347726.

- During the installation process, you may be prompted to install the Linux GNU GRUB boot loader package. If so prompted, select the option to install the GRUB boot loader package and proceed with the installation.

System Requirements—Server (Bare-Metal Hardware)

The following table lists the minimum system requirements for a successful Cisco APIC-EM server (bare-metal hardware) installation. The minimum system requirements for each server in a multi-host deployment are the same as in a single-host deployment, except that the multi-host deployment requires two or three servers.

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.

Caution You must dedicate the entire server for the Cisco APIC-EM. You cannot use the server for any other software programs, packages, or data. During the Cisco APIC-EM installation, any other software programs, packages or data on the server will be deleted.

Table 12: Minimum System Requirements—Server

Server Option	Image Format	Bare metal/ISO

Hardware Specifications	CPU (cores)	6 (minimum) **Note** 6 CPUs is the minimum number required for your server. For better performance, we recommend using 12 CPUs.
	Memory	32 GB (minimum single-host deployment) **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 of available/usable storage after hardware RAID
	RAID Level[4]	Hardware-based RAID at RAID Level 10
	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

[4] For information about RAID configuration on Cisco UCS servers, refer to the *Cisco UCS Server Configuration Utility, Release 3.0 User Guide*. See http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/ucsscu/user/guide/30/UCS_SCU/bootraid.html#wp1073012%0A

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.
  - For a multi-host configuration with Cisco APIC-EM located behind a NAT within your network, note the following information and requirement:
    - The Virtual IP address of the Cisco APIC-EM controller is intended as a destination address for HTTP(S) traffic such as Cisco PnP and PKI download requests.
    - Any outbound connections initiated from the Cisco APIC-EM controller, such as during a Discovery, Inventory Collection, etc., will use the host IP address of one of the three Cisco APIC-EM hosts.
    - Therefore, you need to PAT (Port Address Translation) the host IP addresses of the Cisco APIC-EM hosts to a global public facing IP address for outbound connections from Cisco APIC-EM controller.

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 13: 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 [5]	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

[5] 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 14: 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
53	DNS	UDP

Port Number	Permitted Traffic	Protocol (TCP or 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 [6]	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

[6] 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 (bare-metal hardware or server).

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.

Step 1 Burn the ISO image onto a DVD or copy it onto a bootable USB disk.

Step 2 If the ISO image was burned onto a DVD, then insert the DVD into the DVD drive of the server.

Note If your server does not come with a DVD drive, you can connect an external USB DVD drive to the server and insert the disk into that external drive.

Step 3 Alternatively, if the ISO image was copied onto a bootable USB disk, then insert this bootable USB disk into the server.

Important For information about and an example of creating a bootable USB disk from a USB flash drive and attaching the ISO to it, see Creating a Bootable USB Disk and Attaching the ISO, on page 36.

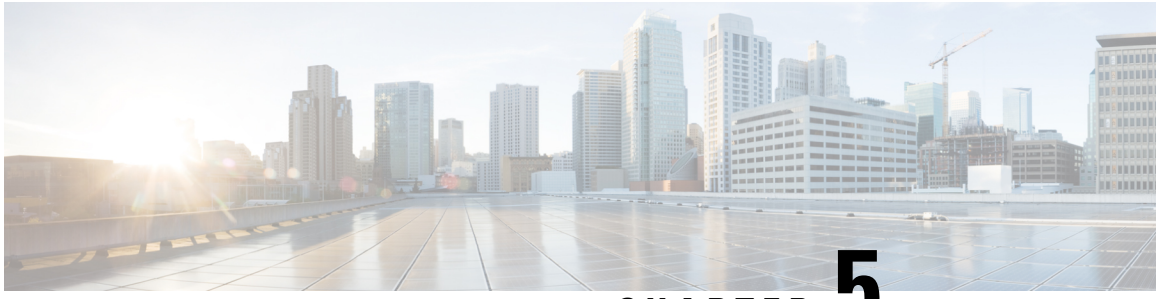
Note Cisco UCS servers provide an additional method of installing a remote ISO using a Virtual KVM console. See your Cisco UCS server documentation for information about this procedure. Note that installing the ISO image using a Virtual KVM console may take longer than the above methods.

Step 4 Boot up the host (server) 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, on page 72
- Configuring Cisco APIC-EM in Multi-Host Mode, on page 93



CHAPTER 5

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, on page 137.

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

Table 15: Cisco APIC-EM Virtual Machine Installation

Step	Description
1	Review the system requirements for a virtual machine installation. See System Requirements—Virtual Machine
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
4	Download and verify the ISO image. See Verifying the Cisco ISO Image

Step	Description
5	Install the ISO image. See Installing the Cisco ISO Image
6	Proceed to 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, on page 72 • Configuring Cisco APIC-EM in Multi-Host Mode, on page 93

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 16: Minimum System Requirements—Virtual Machine

Virtual Machine	VMware ESXi Version	5.1/5.5/6.0/6.5
	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.
- For a multi-host configuration with Cisco APIC-EM located behind a NAT within your network, note the following information and requirement:
  - The Virtual IP address of the Cisco APIC-EM controller is intended as a destination address for HTTP(S) traffic such as Cisco PnP and PKI download requests.
  - Any outbound connections initiated from the Cisco APIC-EM controller, such as during a Discovery, Inventory Collection, etc., will use the host IP address of one of the three Cisco APIC-EM hosts.
  - Therefore, you need to PAT (Port Address Translation) the host IP addresses of the Cisco APIC-EM hosts to a global public facing IP address for outbound connections from Cisco APIC-EM controller.

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 17: 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 [7]	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

[7] 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 18: 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
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 [8]	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

[8] 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, on page 119
- Virtual Machine Configuration Recommendations, on page 119
- Configuring Resource Pools Using vSphere Web Client, on page 122
- Configuring a Virtual Machine Using vSphere Web Client, on page 125

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.

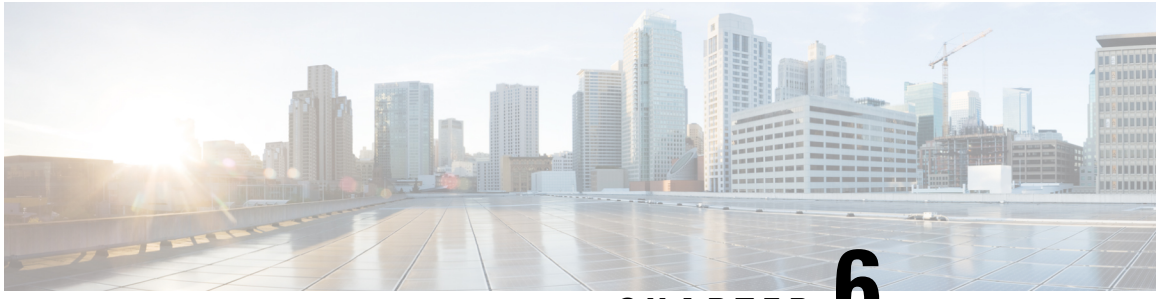
What to do next

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, on page 72
- Configuring Cisco APIC-EM in Multi-Host Mode, on page 93

PART II

Configuration



CHAPTER 6

Configuring Cisco APIC-EM in Standalone Mode

Reviewing Cisco APIC-EM Configuration Wizard Parameters

When the Cisco APIC-EM configuration begins, an interactive wizard prompts you to enter information to configure the controller. The following table displays the information that you will be prompted for to complete the configuration.

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 19: Cisco APIC-EM Configuration Wizard Parameters

Configuration Wizard Prompt	Description	Example
(Optional) Bonded NICs	Choose to configure or not configure bonded NICs on the controller's interfaces. Enter 'yes' to proceed with configuring NIC bonding on the interfaces. Enter 'no' to bypass NIC bonding completely, and be presented with the option for VLAN configuration.	Enter 'yes'.

Configuration Wizard Prompt	Description	Example
Bonding mode	If you chose to configure bonded NICs, then configure either 'balance-xor' or '802.3ad' for the bonded NICs. Entering 'balance-xor' will configure static bonding on the selected NICs. Entering '802.3ad' will configure LACP bonding on the selected NICs. **Important** Entering '802.3ad' requires that a separate LACP configuration be made on the switches that are connected to the Ethernet ports. Entering 'balance-xor ' will require a configuration on the connected switches for the static configuration. Generally, this means that the appropriate ports be grouped together in a Cisco EtherChannel configuration for the static configuration. Refer to your Cisco switch documentation for information about configuring the switches. For this release, only one bonded interface with multiple NICs can be configured on the controller.	Enter '802.3ad '.
(Optional) VLAN	Choose to configure or not configure VLANs on the controller's interfaces. The NICs on the controller (whether an appliance, server, or virtual machine) can be configured with a VLAN interface. Both bonded NICs and standalone NICs can be configured with VLANs. The management interface of the appliance, server, or virtual machine can also be selected and configured with a VLAN interface. **Note** The same VLAN cannot be used on multiple interfaces.	Enter 'yes' The VLAN range is limited (1-1001, 1005-4094).

Configuration Wizard Prompt	Description	Example
Host IP address	Enter a host IP address. 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. **Note** This host IP address must be a valid IPv4 address.	10.0.0.12
(Optional) Virtual IP address	Enter a virtual IP 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. **Note** The virtual IP address must be a valid IPv4 address.	10.12.13.14
Netmask IP address	Enter a netmask IP address. This must be a valid IPv4 netmask.	255.255.255.0
Default Gateway IP address	Enter a default gateway IP address. This must be a valid IPv4 address for the default gateway.	10.12.13.1
Primary DNS server	Enter a primary DNS server address. This must be a valid IPv4 address for the primary DNS 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.

Configuration Wizard Prompt	Description	Example
Primary NTP server	Enter a primary NTP server address. This must be a valid IPv4 address or hostname of a Network Time Protocol (NTP) server. **Note** Before you deploy the Cisco APIC-EM, make sure that the time on the controller's system clock is current or that you are using a Network Time Protocol (NTP) server that is keeping the correct time.	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	This 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.
(Optional) HTTPS proxy server	Enter an HTTPS proxy server address. This must be a valid IPv4 address for the HTTPS proxy with port number.	https://209.165.200.11:3128
Admin Username	Enter the admin user name. 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

Configuration Wizard Prompt	Description	Example

Admin Password	Enter the 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	Enter a 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	Enter a 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 'yes' or 'no' for **RESET EXISTING CONTROLLER NETWORK CONFIG**.

Step 4 Select the **Reset Networking Configuration** option for your configuration.

For an initial deployment, enter 'no' and proceed with the configuration. For an upgrade for your deployment, enter 'yes' and proceed with the configuration

Note Entering 'yes' will remove the current networking configuration for the controller on this host.

You are then prompted to enter values for the **NETWORK ADAPTER BONDING mode (OPTIONAL)**.

Step 5 Select the **NETWORK ADAPTER BONDING mode (OPTIONAL)** for your configuration.

Enter either 'yes' or 'no' for this step.

Enter 'yes' to proceed with configuring NIC bonding on the interfaces (create a single logical port from two Ethernet ports (NICs) on the controller). Enter 'no' to bypass NIC bonding completely, and be presented with the option for VLAN configuration (see Step 7 below).

After entering a value, click **next>>** to proceed.

Step 6 If you entered 'yes', then enter the bonding mode in the **NETWORK ADAPTER 0 (bond0)** screen.

Enter either 'balance-xor' or '802.3ad' for this step.

This step permits you to create a single logical port from two or more Ethernet ports (NICs) on the controller that the configuration wizard discovers and displays. Entering 'balance-xor' will configure static bonding on the selected NICs. Entering '802.3ad' will configure LACP bonding on the selected NICs.

For this release, only a single bonded interface with multiple NICs can be configured on the controller.

Important Entering '802.3ad' requires a separate LACP configuration be made on the switches that are connected to the Ethernet ports. Entering 'balance-xor ' will require a configuration on the connected switches for the static configuration. Generally, this means that the appropriate ports be grouped together in a Cisco EtherChannel configuration for the static configuration. Refer to your Cisco switch documentation for information about configuring the switches.

Step 7 Select the individual Ethernet ports (for example, eth0 and eth1) to bond together as a single logical port.

Use the **Tab** key to navigate to the Ethernet port fields in the configuration wizard. User the **space bar** to select (check) the Ethernet port.

Note When navigating to an Ethernet port, the configuration wizard displays the port's MAC address and speeds (in Mb/s). Both the actual and supported speeds are displayed. The actual speed is defined as the negotiated speed retrieved from the kernel itself (when the interface is down, 'NA' will be displayed). The supported speed is defined as the maximum speed supported by the NIC.

When finished with this step, click **next>>** to proceed.

Step 8 Select the **NETWORK ADAPTER VLAN Mode (Optional)**

Enter either 'yes' or 'no' for this step.

Entering 'yes' permits you to configure VLANs on the interface(s) in the next step. Entering 'no' bypasses VLAN configuration.

Note For a multi-host cluster, all the VLANs must be configured the same on each host.

After entering a value, click **next>>** to proceed.

Step 9 (Optional) If you entered yes, then enter the management interface in the **ADD VIRTUAL NETWORK ADAPTERS** screen.

The management interface can be either an Ethernet port (bonded or not) or a VLAN. For a VLAN, use the following format:

interface.vlan_id

For example, **bond0.300** or **eth0.300**

Step 10 (Optional) Add virtual adapters for each of the interfaces in the **ADD VIRTUAL NETWORK ADAPTERS** screen.

If you created a bonded port in the previous steps, then that bonded port will be displayed in this screen. Navigate to the bonded port displayed on the screen using the **Tab** key on your keyboard. Proceed to configure one or more VLANs on the bonded port.

If you did not create a bonded port in the previous steps, then each Each Ethernet port discovered by the configuration wizard will be displayed in this screen. Navigate to the Ethernet ports displayed on the screen using the **Tab** key on your keyboard. Proceed to configure one or more VLANs on these Ethernet ports.

Note You can use a comma separated list of VLANs (for example, 100, 200, 300) for this step. The VLAN range is limited (1-1001, 1005-4094). The same VLAN cannot be used on multiple interfaces. Up to 5 VLANs can be configured per Cisco APIC-EM cluster.

Click **next>>** to proceed.

Step 11 Enter configuration values for the **NETWORK ADAPTER #1** 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 step header changes to reflect your prior configuration selections. For example, if you configured a bonded NIC, then the header will display **NETWORK ADAPTER #1 (bond0)**, if you configured this bonded NIC as the management interface, then the header will display **NETWORK ADAPTER #1 (bond0) MANAGEMENT INT**, and so forth.

Important 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 12
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 12 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**. Additionally, if the **HTTPS PROXY** step appears because the Gateway is unreachable for a short period of time due to network delay, then you can choose **Next** and skip back to the **HTTPS PROXY** step.

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 13 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 don't have a CCO username and password or if you don't want access to cisco.com from your APIC-EM installation, then fill out the **Username** and **Password** fields with any information, but ensure that you do not include spaces in the username. This will permit you to proceed through the config-wizard process. Values entered for this field are used for telemtry collection. For information about telemtry collection, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrators Guide*.
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 14 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 Requirements section in Chapter 2, Securing the Cisco APIC-EM in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **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 15 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 Requirements section in Chapter 2, Securing the Cisco APIC-EM in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **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 16 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 17 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 18 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 19 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 20 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 21 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 22 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 23 In the **Login** window, enter the administrator username and password that you configured above and click the **Log In** button.

What to do next

Start to use the Cisco APIC-EM to manage and configure your network. For assistance with navigating the controller's GUI and becoming familiar with the its features, use the *Cisco APIC-EM Quick Start Guide*.

If you are deploying a multi-host configuration, then review the following multi-host configuration procedure.

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.

Managing Admin Accounts

Admin User Right Differences

The usernames and passwords that you configure by using the Cisco APIC-EM configuration wizard are intended to be used for administrative access to the Cisco APIC-EM Grapevine root (Linux) and the Cisco APIC-EM GUI interface.

The administrator that has access to the Cisco APIC-EM Grapevine root is called the Linux admin user. By default, the username for the Linux admin user is 'grapevine' and the password is user-defined during the configuration wizard setup process. There is no default password.

Both the username and password for the Cisco APIC-EM GUI is user-defined during the configuration wizard process. There is no default username or password.

The Cisco APIC-EM Linux admin user has different rights and capabilities than the Cisco APIC-EM GUI-based admin user and can perform other administrative tasks.

Tasks Performed by Linux (Grapevine) Admin Users

The following tasks can be performed by the Linux (Grapevine) admin user:

- Displaying audit and system logs on the Cisco APIC-EM.
- Reviewing the status of Cisco APIC-EM services on the appliance.
- Resetting the configuration values back to their original configuration settings.
- Restoring the Cisco APIC-EM back to the factory default.
- Creating a support file that you can then email to Cisco support for assistance.

- Updating or changing your Cisco APIC-EM configuration wizard settings (for example, updating the NTP configuration settings).

GUI-based admin users that are created by using the Cisco APIC-EM user interface cannot automatically log into the Cisco APIC-EM and access the Grapevine root and clients located on the appliance. Only Linux admin users can access the Cisco APIC-EM Grapevine root and clients on the appliance.

Note See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide* for information about the supported Grapevine root (Linux) commands and accessible logs.

Tasks Performed by GUI Admin Users

The following tasks can be performed by the GUI admin user:

- Initiate and work with the base applications (Discovery, Inventory, Topology, Path Trace, and EasyQoS) and solution applications (Network PnP and iWAN).
- Back up and restore the Cisco APIC-EM database and files.
- Display the service logs on the Cisco APIC-EM.
- Apply Cisco APIC-EM software patches, maintenance releases, and upgrades.

Note See the following for detailed information about the above supported controller GUI operations:

- *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*

Creating GUI Admin Users

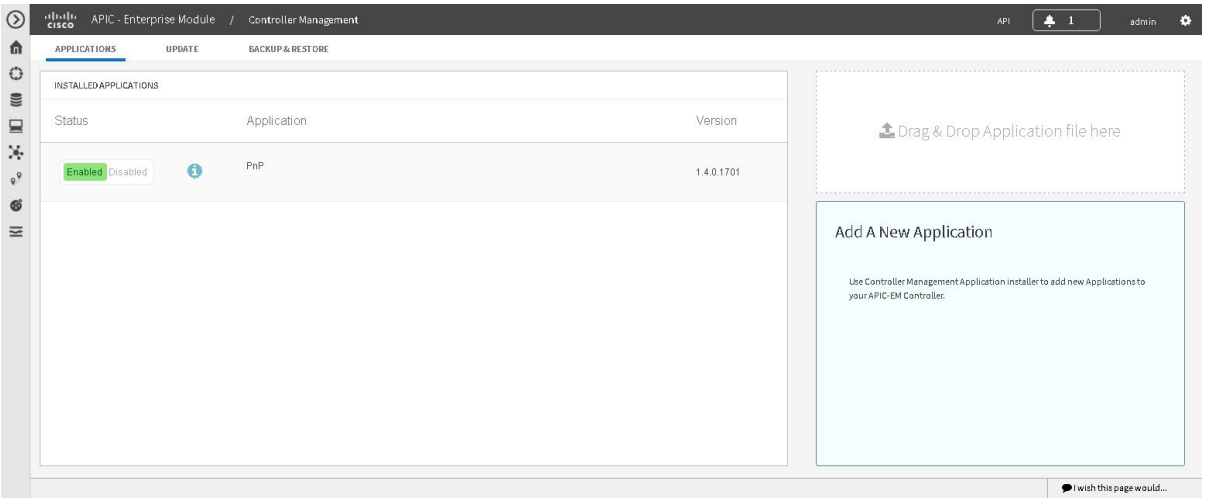
For first-time GUI-based access to Cisco APIC-EM system, the administrator username and password is configured during the configuration wizard setup.

Note You can add GUI admin users through the GUI interface itself. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide* for more information.

Installing Cisco APIC-EM Applications

The application installation procedure is simple, the application bundle provided by Cisco must be dropped in the browser window under **admin** (Settings Icon) in **App Management**.

Figure 12: App Management Window



Perform the following procedure to install additional applications.

Important Perform this procedure only after you have completed your Cisco APIC-EM configuration. If you are setting up a multi-host Cisco APIC-EM configuration, then perform this procedure when finished setting up all of the hosts in your multi-host configuration.

Before you begin

You have installed Cisco APIC-EM, following the procedures described in this guide.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings" in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Step 1 Download the application bundle or bundles from Cisco.com.

Save the bundle or bundles to a secure location on your laptop or network.

Step 2 In your browser address bar, enter the IP address of the Cisco APIC-EM in the following format:

https://*IP address*

Step 3 On the launch page, enter your username and password.

The **Home** window of the APIC-EM controller now appears.

Step 4 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 5 Click the **App Management** link from the drop-down menu.

Step 6 Drag and drop the application bundle onto the dedicated drag and drop field of the **App Management** window on the browser.

Note This step initiates the application installation process which can take several minutes to complete

Step 7 Once the application is uploaded and installed, toggle the switch next to the application's name to enable it.

What to do next

If needed for your network deployment, repeat the above steps to upload, install, and enable another application.

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 an entire multi-host cluster. This procedure describes how to perform these procedures.

For information about powering down and powering up only a single host within a multi-host cluster, see Powering Down and Powering Up a Single Host Within a Multi-Host Cluster, on page 111.

Before you begin

You should have installed 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.

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.

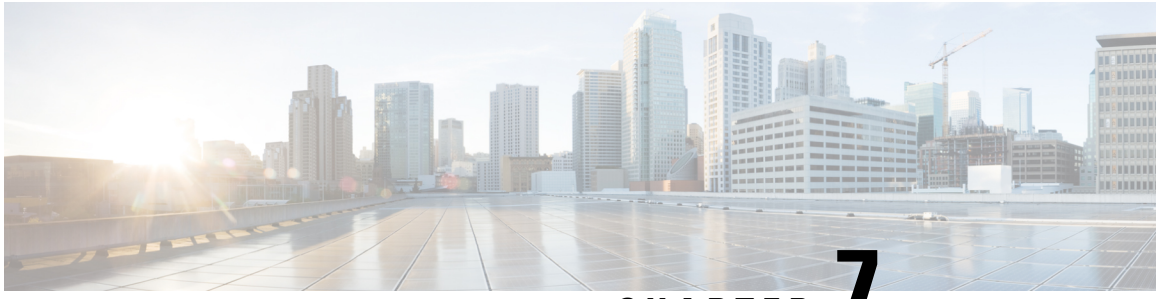
You are then prompted to confirm your intent to run the **reset_grapevine factory** command.

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)



CHAPTER 7

Configuring Cisco APIC-EM in Multi-Host Mode

Reviewing Cisco APIC-EM Configuration Wizard Parameters

When the Cisco APIC-EM configuration begins, an interactive wizard prompts you to enter information to configure the controller. The following table displays the information that you will be prompted for to complete the configuration.

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 20: Cisco APIC-EM Configuration Wizard Parameters

Configuration Wizard Prompt	Description	Example
(Optional) Bonded NICs	Choose to configure or not configure bonded NICs on the controller's interfaces. Enter 'yes' to proceed with configuring NIC bonding on the interfaces. Enter 'no' to bypass NIC bonding completely, and be presented with the option for VLAN configuration.	Enter 'yes'.

Configuration Wizard Prompt	Description	Example
Bonding mode	If you chose to configure bonded NICs, then configure either 'balance-xor' or '802.3ad' for the bonded NICs. Entering 'balance-xor' will configure static bonding on the selected NICs. Entering '802.3ad' will configure LACP bonding on the selected NICs. **Important** Entering '802.3ad' requires that a separate LACP configuration be made on the switches that are connected to the Ethernet ports. Entering 'balance-xor ' will require a configuration on the connected switches for the static configuration. Generally, this means that the appropriate ports be grouped together in a Cisco EtherChannel configuration for the static configuration. Refer to your Cisco switch documentation for information about configuring the switches. For this release, only one bonded interface with multiple NICs can be configured on the controller.	Enter '802.3ad '.
(Optional) VLAN	Choose to configure or not configure VLANs on the controller's interfaces. The NICs on the controller (whether an appliance, server, or virtual machine) can be configured with a VLAN interface. Both bonded NICs and standalone NICs can be configured with VLANs. The management interface of the appliance, server, or virtual machine can also be selected and configured with a VLAN interface. **Note** The same VLAN cannot be used on multiple interfaces.	Enter 'yes' The VLAN range is limited (1-1001, 1005-4094).

Configuration Wizard Prompt	Description	Example
Host IP address	Enter a host IP address. 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. **Note** This host IP address must be a valid IPv4 address.	10.0.0.12
(Optional) Virtual IP address	Enter a virtual IP 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. **Note** The virtual IP address must be a valid IPv4 address.	10.12.13.14
Netmask IP address	Enter a netmask IP address. This must be a valid IPv4 netmask.	255.255.255.0
Default Gateway IP address	Enter a default gateway IP address. This must be a valid IPv4 address for the default gateway.	10.12.13.1
Primary DNS server	Enter a primary DNS server address. This must be a valid IPv4 address for the primary DNS 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.

Configuration Wizard Prompt	Description	Example
Primary NTP server	Enter a primary NTP server address. This must be a valid IPv4 address or hostname of a Network Time Protocol (NTP) server. **Note** Before you deploy the Cisco APIC-EM, make sure that the time on the controller's system clock is current or that you are using a Network Time Protocol (NTP) server that is keeping the correct time.	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	This 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.
(Optional) HTTPS proxy server	Enter an HTTPS proxy server address. This must be a valid IPv4 address for the HTTPS proxy with port number.	https://209.165.200.11:3128
Admin Username	Enter the admin user name. 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

Configuration Wizard Prompt	Description	Example

Admin Password	Enter the 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	Enter a 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	Enter a 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

Supported Multi-Host Configurations

The Cisco APIC-EM supports a single-host, two-host, or three-host cluster configuration. With a single-host configuration, 32 GB of RAM is required for that host. With a two or three-host cluster configuration, 32 GB of RAM is required for each host in the cluster.

Note Cisco APIC-EM does not support a cluster with more than three hosts. For example, a multi-host cluster with five or seven hosts is not currently supported.

The three-host cluster provides *both* software and hardware high availability. The single-host or two-host cluster only provides software high availability; they do not provide hardware high availability. For this reason, we strongly recommend that for a multi-host configuration three hosts be used.

A hardware failure occurs when the physical host itself malfunctions or fails. A software failure occurs when a service on a host fails. Software high availability involves the ability of the services on the host or hosts to be restarted and respun. For example, on a single host, if a service fails then that service is respun on that host. In a two-host cluster, if a service fails on one host then that service is re-spun on the remaining host. In a three-host cluster, if a service fails on one host, then that service is re-spun on one of the two remaining hosts.

When setting up a two-host or three-host cluster, you should never set up the hosts to span a LAN across slow links. This may impact the recovery time if a service fails on one of the hosts. Additionally, when configuring either a two-host or three-host cluster, all of the hosts in that cluster must reside in the same subnet.

For additional detailed information about multi-host clusters, see Multi-Host Support, on page 137.

Configuring Cisco APIC-EM in Multi-Host Mode

Configuring Cisco APIC-EM in multi-host mode involves the following procedures:

1. Configure Cisco APIC-EM as a single host using the configuration wizard.
2. Configure Cisco APIC-EM on a second host and to join it to the first, pre-existing host to create a cluster.
3. Configure Cisco APIC-EM on a third host and join it to the pre-existing cluster.

Perform the following procedures in this section to configure multi-host mode for the controller.

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 'yes' or 'no' for **RESET EXISTING CONTROLLER NETWORK CONFIG**.

Step 4 Select the **Reset Networking Configuration** option for your configuration.

For an initial deployment, enter 'no' and proceed with the configuration. For an upgrade for your deployment, enter 'yes' and proceed with the configuration

Note Entering 'yes' will remove the current networking configuration for the controller on this host.

You are then prompted to enter values for the **NETWORK ADAPTER BONDING mode (OPTIONAL)**.

Step 5 Select the **NETWORK ADAPTER BONDING mode (OPTIONAL)** for your configuration.

Enter either 'yes' or 'no' for this step.

Enter 'yes' to proceed with configuring NIC bonding on the interfaces (create a single logical port from two Ethernet ports (NICs) on the controller). Enter 'no' to bypass NIC bonding completely, and be presented with the option for VLAN configuration (see Step 7 below).

After entering a value, click **next>>** to proceed.

Step 6 If you entered 'yes', then enter the bonding mode in the **NETWORK ADAPTER 0 (bond0)** screen.

Enter either 'balance-xor' or '802.3ad' for this step.

This step permits you to create a single logical port from two or more Ethernet ports (NICs) on the controller that the configuration wizard discovers and displays. Entering 'balance-xor' will configure static bonding on the selected NICs. Entering '802.3ad' will configure LACP bonding on the selected NICs.

For this release, only a single bonded interface with multiple NICs can be configured on the controller.

Important Entering '802.3ad' requires a separate LACP configuration be made on the switches that are connected to the Ethernet ports. Entering 'balance-xor ' will require a configuration on the connected switches for the static configuration. Generally, this means that the appropriate ports be grouped together in a Cisco EtherChannel configuration for the static configuration. Refer to your Cisco switch documentation for information about configuring the switches.

Step 7 Select the individual Ethernet ports (for example, eth0 and eth1) to bond together as a single logical port.

Use the **Tab** key to navigate to the Ethernet port fields in the configuration wizard. User the **space bar** to select (check) the Ethernet port.

Note When navigating to an Ethernet port, the configuration wizard displays the port's MAC address and speeds (in Mb/s). Both the actual and supported speeds are displayed. The actual speed is defined as the negotiated speed retrieved from the kernel itself (when the interface is down, 'NA' will be displayed). The supported speed is defined as the maximum speed supported by the NIC.

When finished with this step, click **next>>** to proceed.

Step 8 Select the **NETWORK ADAPTER VLAN Mode (Optional)**

Enter either 'yes' or 'no' for this step.

Entering 'yes' permits you to configure VLANs on the interface(s) in the next step. Entering 'no' bypasses VLAN configuration.

Note For a multi-host cluster, all the VLANs must be configured the same on each host.

After entering a value, click **next>>** to proceed.

Step 9 (Optional) If you entered yes, then enter the management interface in the **ADD VIRTUAL NETWORK ADAPTERS** screen.

The management interface can be either an Ethernet port (bonded or not) or a VLAN. For a VLAN, use the following format:

interface.vlan_id

For example, **bond0.300** or **eth0.300**

Step 10 (Optional) Add virtual adapters for each of the interfaces in the **ADD VIRTUAL NETWORK ADAPTERS** screen.

If you created a bonded port in the previous steps, then that bonded port will be displayed in this screen. Navigate to the bonded port displayed on the screen using the **Tab** key on your keyboard. Proceed to configure one or more VLANs on the bonded port.

If you did not create a bonded port in the previous steps, then each Each Ethernet port discovered by the configuration wizard will be displayed in this screen. Navigate to the Ethernet ports displayed on the screen using the **Tab** key on your keyboard. Proceed to configure one or more VLANs on these Ethernet ports.

Note You can use a comma separated list of VLANs (for example, 100, 200, 300) for this step. The VLAN range is limited (1-1001, 1005-4094). The same VLAN cannot be used on multiple interfaces. Up to 5 VLANs can be configured per Cisco APIC-EM cluster.

Click **next>>** to proceed.

Step 11 Enter configuration values for the **NETWORK ADAPTER #1** 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 step header changes to reflect your prior configuration selections. For example, if you configured a bonded NIC, then the header will display **NETWORK ADAPTER #1 (bond0)**, if you configured this bonded NIC as the management interface, then the header will display **NETWORK ADAPTER #1 (bond0) MANAGEMENT INT**, and so forth.

Important 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 12
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 12 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**. Additionally, if the **HTTPS PROXY** step appears because the Gateway is unreachable for a short period of time due to network delay, then you can choose **Next** and skip back to the **HTTPS PROXY** step.

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 13 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 don't have a CCO username and password or if you don't want access to cisco.com from your APIC-EM installation, then fill out the **Username** and **Password** fields with any information, but ensure that you do not include spaces in the username. This will permit you to proceed through the config-wizard process. Values entered for this field are used for telemtry collection. For information about telemtry collection, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrators Guide*.
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 14 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 Requirements section in Chapter 2, Securing the Cisco APIC-EM in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **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 15 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 Requirements section in Chapter 2, Securing the Cisco APIC-EM in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **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 16 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 17 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 18 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 19 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 20 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 21 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 22 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 23 In the **Login** window, enter the administrator username and password that you configured above and click the **Log In** button.

What to do next

Start to use the Cisco APIC-EM to manage and configure your network. For assistance with navigating the controller's GUI and becoming familiar with the its features, use the *Cisco APIC-EM Quick Start Guide*.

If you are deploying a multi-host configuration, then review the following multi-host configuration procedure.

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 performed the following prerequisites:

- 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.
- Additionally, you must have checked the controller's health on the first host using the **SYSTEM HEALTH** tab in the GUI. The **SYSTEM HEALTH** tab is directly accessible from the **HOME** page. For information about this procedure, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

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.

You are then prompted to enter values for the **NETWORK ADAPTER BONDING mode (OPTIONAL)**.

Step 4 Select the **NETWORK ADAPTER BONDING mode (OPTIONAL)** for your configuration.

Enter either 'yes' or 'no' for this step.

Enter 'yes' to proceed with configuring NIC bonding on the interfaces (create a single logical port from two Ethernet ports (NICs) on the controller). Enter 'no' to bypass NIC bonding completely, and be presented with the option for VLAN configuration (see Step 7 below).

After entering a value, click **next>>** to proceed.

Step 5 If you entered 'yes', then enter the bonding mode in the **NETWORK ADAPTER 0 (bond0)** screen.

Enter either 'balance-xor' or '802.3ad' for this step.

This step permits you to create a single logical port from two or more Ethernet ports (NICs) on the controller that the configuration wizard discovers and displays. Entering 'balance-xor' will configure static bonding on the selected NICs. Entering '802.3ad' will configure LACP bonding on the selected NICs.

For this release, only a single bonded interface with multiple NICs can be configured on the controller.

Important Entering '802.3ad' requires a separate LACP configuration be made on the switches that are connected to the Ethernet ports. Entering 'balance-xor ' will require a configuration on the connected switches for the static configuration. Generally, this means that the appropriate ports be grouped together in a Cisco EtherChannel configuration for the static configuration. Refer to your Cisco switch documentation for information about configuring the switches.

Step 6 Select the individual Ethernet ports (for example, eth0 and eth1) to bond together as a single logical port.

Use the **Tab** key to navigate to the Ethernet port fields in the configuration wizard. User the **space bar** to select (check) the Ethernet port.

Note When navigating to an Ethernet port, the configuration wizard displays the port's MAC address and speeds (in Mb/s). Both the actual and supported speeds are displayed. The actual speed is defined as the negotiated speed retrieved from the kernel itself (when the interface is down, 'NA' will be displayed). The supported speed is defined as the maximum speed supported by the NIC.

When finished with this step, click **next>>** to proceed.

Step 7 Select the **NETWORK ADAPTER VLAN Mode (Optional)**

Enter either 'yes' or 'no' for this step.

Entering 'yes' permits you to configure VLANs on the interface(s) in the next step. Entering 'no' bypasses VLAN configuration.

Note For a multi-host cluster, all the VLANs must be configured the same on each host.

After entering a value, click **next>>** to proceed.

Step 8 (Optional) If you entered yes, then enter the management interface in the **ADD VIRTUAL NETWORK ADAPTERS** screen.

The management interface can be either an Ethernet port (bonded or not) or a VLAN. For a VLAN, use the following format:

interface.vlan_id

For example, **bond0.300** or **eth0.300**

Step 9 (Optional) Add virtual adapters for each of the interfaces in the **ADD VIRTUAL NETWORK ADAPTERS** screen.

If you created a bonded port in the previous steps, then that bonded port will be displayed in this screen. Navigate to the bonded port displayed on the screen using the **Tab** key on your keyboard. Proceed to configure one or more VLANs on the bonded port.

If you did not create a bonded port in the previous steps, then each Ethernet port discovered by the configuration wizard will be displayed in this screen. Navigate to the Ethernet ports displayed on the screen using the **Tab** key on your keyboard.

Proceed to configure one or more VLANs on these Ethernet ports.

Note You can use a comma separated list of VLANs (for example, 100, 200, 300) for this step. The VLAN range is limited (1-1001, 1005-4094). The same VLAN cannot be used on multiple interfaces. Up to 5 VLANs can be configured per Cisco APIC-EM cluster.

Click **next>>** to proceed.

Step 10 Enter configuration values for the **NETWORK ADAPTER #1** 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 The step header changes to reflect your prior configuration selections. For example, if you configured a bonded NIC, then the header will display **NETWORK ADAPTER #1 (bond0)**, if you configured this bonded NIC as the management interface, then the header will display **NETWORK ADAPTER #1 (bond0) MANAGEMENT INT**, and so forth.

Important 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 11 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 Requirements section in Chapter 2, Securing the Cisco APIC-EM in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*. **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 12 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 12

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 13 (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 14 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 15 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 16 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 17 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 18 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.

After configuring each host be sure to check the controller's health on the host using the **SYSTEM HEALTH** tab in the GUI. The **SYSTEM HEALTH** tab is directly accessible from the **HOME** page. For information about this procedure, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

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.

Managing Admin Accounts

Admin User Right Differences

The usernames and passwords that you configure by using the Cisco APIC-EM configuration wizard are intended to be used for administrative access to the Cisco APIC-EM Grapevine root (Linux) and the Cisco APIC-EM GUI interface.

The administrator that has access to the Cisco APIC-EM Grapevine root is called the Linux admin user. By default, the username for the Linux admin user is 'grapevine' and the password is user-defined during the configuration wizard setup process. There is no default password.

Both the username and password for the Cisco APIC-EM GUI is user-defined during the configuration wizard process. There is no default username or password.

The Cisco APIC-EM Linux admin user has different rights and capabilities than the Cisco APIC-EM GUI-based admin user and can perform other administrative tasks.

Tasks Performed by Linux (Grapevine) Admin Users

The following tasks can be performed by the Linux (Grapevine) admin user:

- Displaying audit and system logs on the Cisco APIC-EM.
- Reviewing the status of Cisco APIC-EM services on the appliance.
- Resetting the configuration values back to their original configuration settings.
- Restoring the Cisco APIC-EM back to the factory default.
- Creating a support file that you can then email to Cisco support for assistance.
- Updating or changing your Cisco APIC-EM configuration wizard settings (for example, updating the NTP configuration settings).

GUI-based admin users that are created by using the Cisco APIC-EM user interface cannot automatically log into the Cisco APIC-EM and access the Grapevine root and clients located on the appliance. Only Linux admin users can access the Cisco APIC-EM Grapevine root and clients on the appliance.

Note See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide* for information about the supported Grapevine root (Linux) commands and accessible logs.

Tasks Performed by GUI Admin Users

The following tasks can be performed by the GUI admin user:

- Initiate and work with the base applications (Discovery, Inventory, Topology, Path Trace, and EasyQoS) and solution applications (Network PnP and iWAN).
- Back up and restore the Cisco APIC-EM database and files.
- Display the service logs on the Cisco APIC-EM.
- Apply Cisco APIC-EM software patches, maintenance releases, and upgrades.

Note See the following for detailed information about the above supported controller GUI operations:

- *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*

Creating GUI Admin Users

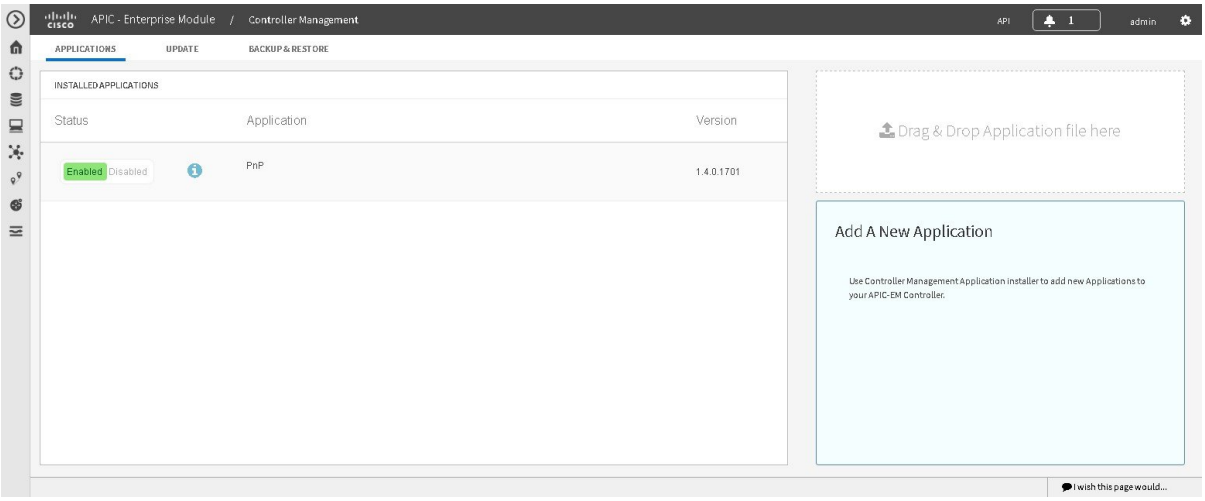
For first-time GUI-based access to Cisco APIC-EM system, the administrator username and password is configured during the configuration wizard setup.

Note You can add GUI admin users through the GUI interface itself. See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide* for more information.

Installing Cisco APIC-EM Applications

The application installation procedure is simple, the application bundle provided by Cisco must be dropped in the browser window under **admin** (Settings Icon) in **App Management**.

Figure 13: App Management Window



Perform the following procedure to install additional applications.

Important Perform this procedure only after you have completed your Cisco APIC-EM configuration. If you are setting up a multi-host Cisco APIC-EM configuration, then perform this procedure when finished setting up all of the hosts in your multi-host configuration.

Before you begin

You have installed Cisco APIC-EM, following the procedures described in this guide.

You must have administrator (ROLE_ADMIN) permissions and either access to all resources (RBAC scope set to ALL) or an RBAC scope that contains all of the resources that you want to group. For example, to create a group containing a specific set of resources, you must have access to those resources (custom RBAC scope set to all of the resources that you want to group).

For information about user permissions and RBAC scopes required to perform tasks using the Cisco APIC-EM, see "User Settings" in the chapter, "Configuring the Cisco APIC-EM Settings" in the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*.

Step 1 Download the application bundle or bundles from Cisco.com.

Save the bundle or bundles to a secure location on your laptop or network.

Step 2 In your browser address bar, enter the IP address of the Cisco APIC-EM in the following format:

https://*IP address*

Step 3 On the launch page, enter your username and password.

The **Home** window of the APIC-EM controller now appears.

Step 4 In the **Home** window, click either **admin** or the **Settings** icon (gear) at the top right corner of the screen.

Step 5 Click the **App Management** link from the drop-down menu.

Step 6 Drag and drop the application bundle onto the dedicated drag and drop field of the **App Management** window on the browser.

Note This step initiates the application installation process which can take several minutes to complete

Step 7 Once the application is uploaded and installed, toggle the switch next to the application's name to enable it.

What to do next

If needed for your network deployment, repeat the above steps to upload, install, and enable another application.

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 an entire multi-host cluster. This procedure describes how to perform these procedures.

For information about powering down and powering up only a single host within a multi-host cluster, see Powering Down and Powering Up a Single Host Within a Multi-Host Cluster, on page 111.

Before you begin

You should have installed 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 only 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 *********
```

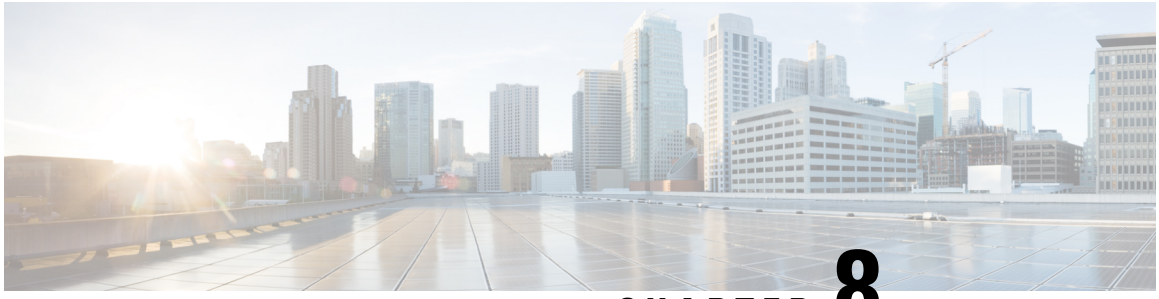
After entering this command a warning appears that the **reset_grapevine factory** command will shut down the controller.

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)



CHAPTER 8

Performing Post-Installation Tasks

Accessing Cisco APIC-EM Using a Web Browser

Cisco APIC-EM supports a web interface using the following HTTPS-enabled browsers:

- Google Chrome—version 56.0 or later
- Mozilla Firefox—version 51.0 or later

Administrator Lockout Following Failed Login Attempts

If you enter an incorrect password for your specified administrator user ID eight times, the Cisco APIC-EM user interface “locks you out” of the system.

See the *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide* for information about recovering from an administrator lockout.

Logging In to the Cisco APIC-EM GUI

After you have installed Cisco APIC-EM, you can log into its web-based interface. You must use only supported HTTPS-enabled browsers.

Step 1 After the Cisco APIC-EM appliance reboot has completed, launch your browser.

Step 2 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 3 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 4 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 5 In the **Login** window, enter the administrator username and password that you configured above and click the **Log In** button.

Logging Out of the Cisco APIC-EM GUI

To log out of the Cisco APIC-EM web-based interface, click **Log Out** on the Cisco APIC-EM main window toolbar. This ends your administrative session and logs you out.

Note For security reasons, we recommend that you log out when you complete your administrative session. If you do not log out, the Cisco APIC-EM GUI interface logs you out after 30 minutes of inactivity.

Installing Certificates

See the *Cisco Application Policy Infrastructure Controller Enterprise Module Administrator's Guide* for information about installing certificates on the controller.

Updating the Cisco APIC-EM Configuration Using the Wizard

If you need to reconfigure your Cisco APIC-EM configuration, you must use the configuration wizard to do so. You cannot use the Linux CLI. Perform the steps in this procedure to change the Cisco APIC-EM configuration wizard settings, including the external network settings, NTP server address, and/or password for the Linux grapevine user. The external network settings that could be changed include:

- Host IP address
- Virtual IP address
- DNS server
- Default gateway
- Static routes

Note In order to change the external network settings, NTP server address, and/or the Linux grapevine user password in a multi-host deployment, you need to first break up the multi-host cluster. Therefore, when performing this procedure controller downtime occurs. For this reason, we recommend that you perform this procedure during a maintenance time period.

Step 1 Using a Secure Shell (SSH) client, log into one of the hosts in your cluster.

Log in using 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 When prompted, enter your Linux username ('grapevine') and password for SSH access.

Step 3 Enter the following command to access the configuration wizard.

```
$ config_wizard
```

Step 4 Review the **Welcome to the APIC-EM Configuration Wizard!** screen and choose the option to remove the host from the cluster:

- **Remove this host from its APIC-EM cluster**

Step 5 A message appears with the following options:

- **[cancel]**—Exit the configuration wizard.
- **[proceed]**—Begin the process to remove this host from its cluster.

Choose **proceed>>** to begin. After choosing **proceed>>**, the configuration wizard begins to remove this host from its cluster.

At the end of this process, this host is removed from the cluster.

Step 6 Repeat the above steps (steps 1-5) on a second host in the cluster.

Note You must repeat the above steps on each host in your cluster, until you only have a single host remaining. You must make your configuration changes on this final remaining host.

Step 7 Using a Secure Shell (SSH) client, log into that final host in your cluster and run the configuration wizard.

```
$ config_wizard
```

After logging into the host, begin the configuration process.

Step 8 Make any necessary changes to the configuration values for the external network settings, NTP server address, and/or password for the Linux grapevine user using the wizard.

After making your configuration change(s), continue through the configuration process to the final message.

Step 9 At the end of the configuration process, 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 10 Log into the other hosts in your multi-host cluster and use the configuration wizard to recreate the cluster.

Refer to the procedure in this guide for information about this process: Configuring Cisco APIC-EM as a Multi-Host Cluster Using the Wizard, on page 101.

APPENDIX A

Preparing Virtual Machines for Cisco APIC-EM

Preparing a VMware System for Cisco APIC-EM Deployment

To ensure that the Cisco APIC-EM works well within a virtual environment, configure the virtual machine with recommended resource pool values. A resource pool is a logical abstraction for the virtual machines that can be used to manage resources. Resource pools can be grouped into hierarchies and then used to partition CPU and memory resources.

You can configure and prepare the virtual machine using either the VMware vSphere Client or Web Client. We recommend that you use the VMware vSphere Web Client, since the **Latency Sensitivity** setting for resource pools must be configured as **High**. The **Latency Sensitivity** setting can only be configured using the VMware vSphere Web Client.

Note When deploying the Cisco APIC-EM in a virtual environment, you must first configure the VMware system before installing Cisco APIC-EM. To install Cisco APIC-EM, you need to download the ISO image containing the controller from Cisco.com and then map the ISO image to the VMware system and boot from it.

Virtual Machine Configuration Recommendations

The following table lists the recommended configuration settings for a successful Cisco APIC-EM VMware vSphere installation, including resource pools. When installing Cisco APIC-EM on a supported virtual machine, we recommend that the following configuration settings are used.

Note When preparing the virtual machine for the Cisco APIC-EM, the configuration settings terminology may differ depending upon the VMware application and GUI that your are using.

Table 21: Virtual Machine Configuration Recommendations (Including Resource Pools)

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. **Note** When configuring the virtual machine, you can select any of the VMware virtual machine provisioning polices for the virtual disk file (Thick Provision Lazy Zeroed, Thick Provision Eager Zeroed, or Thin Provision).
Resource Pool: CPU Resources	• Shares—Normal • Reservation—14400 MHz is minimum configuration setting for this value • Reservation Type—Check box for Expandable • Limit—Unlimited
Resource Pool: Memory Resources	• Shares—Normal • Reservation—Refer to the *Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes* for detailed information about RAM requirements. • Reservation Type—Check box for Expandable • Limit—Unlimited
VMware ESXi Version	5.1/5.5/6.0/6.5
Guest OS: Family and Version	• Guest OS Family—Linux • Guest OS Version—Ubuntu Linux (64-bit)

Virtual Hardware: CPU	• CPU— 6 cores (minimum) • Reservation—14400 MHz is minimum configuration setting for this value • Limit—Unlimited • Shares—Normal **Note** 6 CPUs is the minimum number required for your virtual machine configuration. For better performance, we recommend using 12 CPUs. Additionally, the number of sockets used when setting up CPUs to a virtual machine in VMware does not impact the controller's performance.
Virtual Hardware: Memory	• Memory—Refer to the *Cisco Application Policy Infrastructure Controller Enterprise Module Release Notes* for detailed information about RAM requirements. • Reserve all memory—Check box to Enable.
Virtual Hardware: New Hard disk	500 GB (minimum)
Virtual Hardware: New SCSI controller	VMware Paravirtual
Virtual Hardware: New network	• New network value—Enter the network IP address that the controller will connect to for this value. • Status—Check box to enable Connect at Power On • Adapter type—VMXNET3
Virtual Hardware: New CD/DVD Drive	Select Datastore ISO file from the drop down and the configure the location of the ISO file in the File window
VM Options: Advanced	Choose High for Latency Sensitivity **Note** You can configure and prepare the virtual machine using either the VMware vSphere Client or Web Client. We recommend that you use the VMware vSphere Web Client, since the Latency Sensitivity setting for resource pools must be configured as High. The Latency Sensitivity setting can only be configured using the VMware vSphere Web Client.

Configuring Resource Pools Using vSphere Web Client

To ensure that the Cisco APIC-EM works well within a virtual environment, you should configure resource pools with the recommended values. A resource pool is a logical abstraction for the virtual machines that can be used to manage resources. Resource pools can be grouped into hierarchies and then used to partition CPU and memory resources.

Note You should first create a new resource pool with the recommended configuration values as described in this procedure, and then subsequently create a virtual machine (where the Cisco APIC-EM will be installed) on that resource pool.

Before you begin

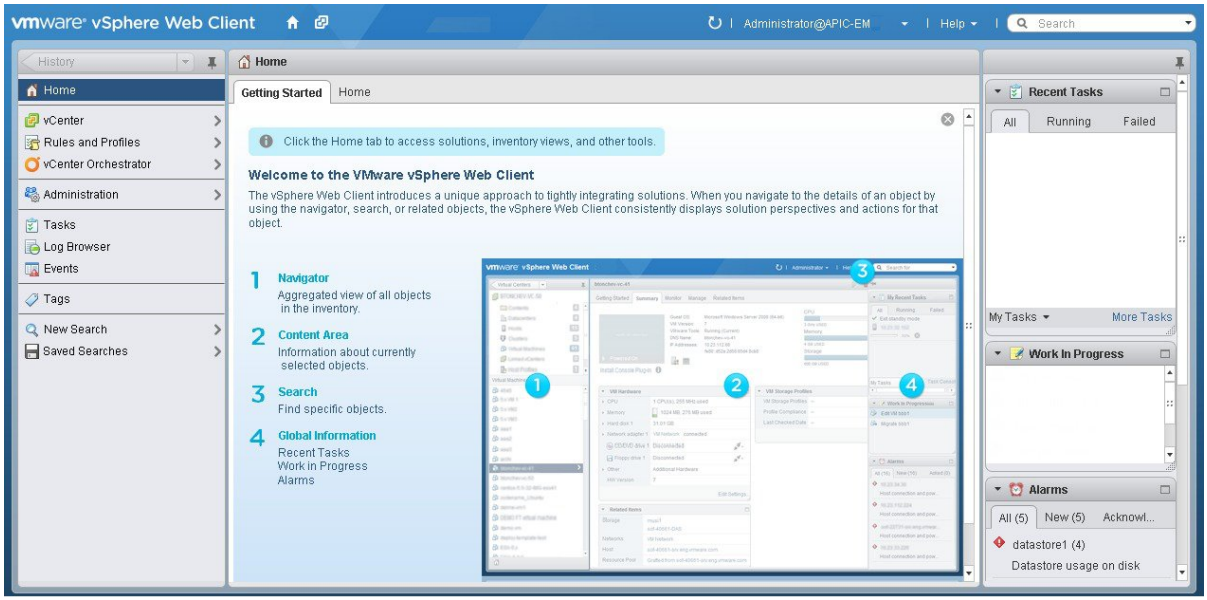
You have reviewed your VMware documentation concerning resource pools and their configuration.

You are familiar with the VMware vSphere Web Client and have a basic knowledge of how to create, manage and troubleshoot virtual machines using it.

You have your host and virtual datastores already set up and accessible in vSphere Web Client for this procedure.

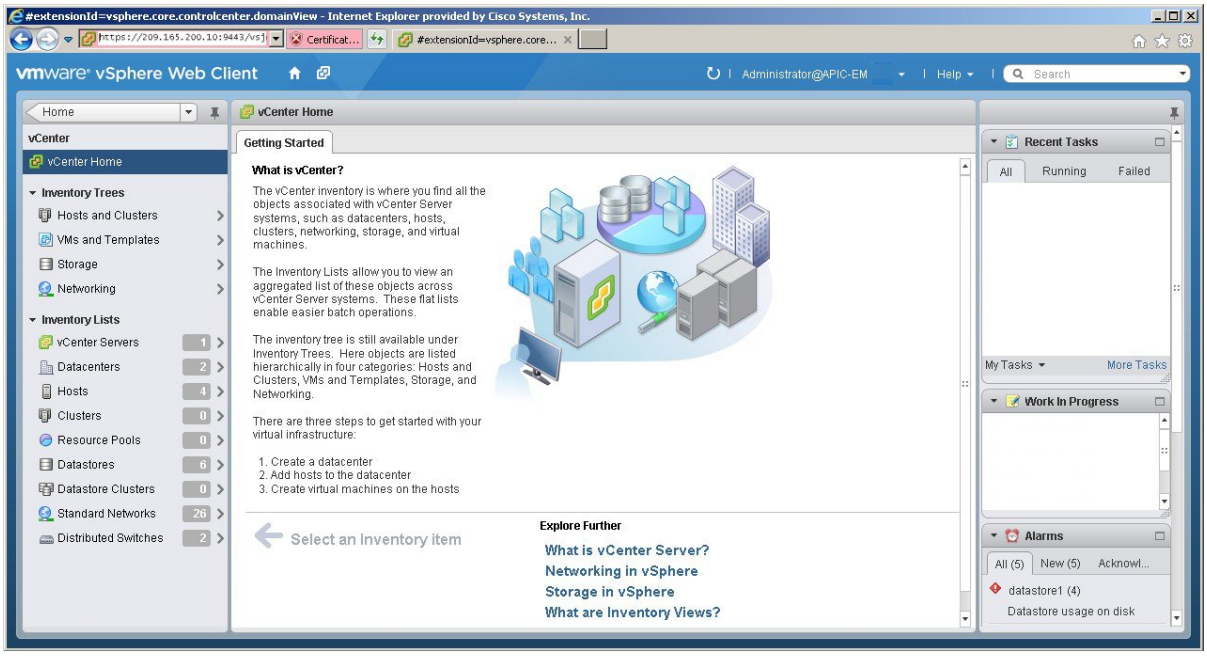
Step 1 Open the VMware vSphere Web Client to perform the procedure.

Figure 14: VMware vSphere Web Client



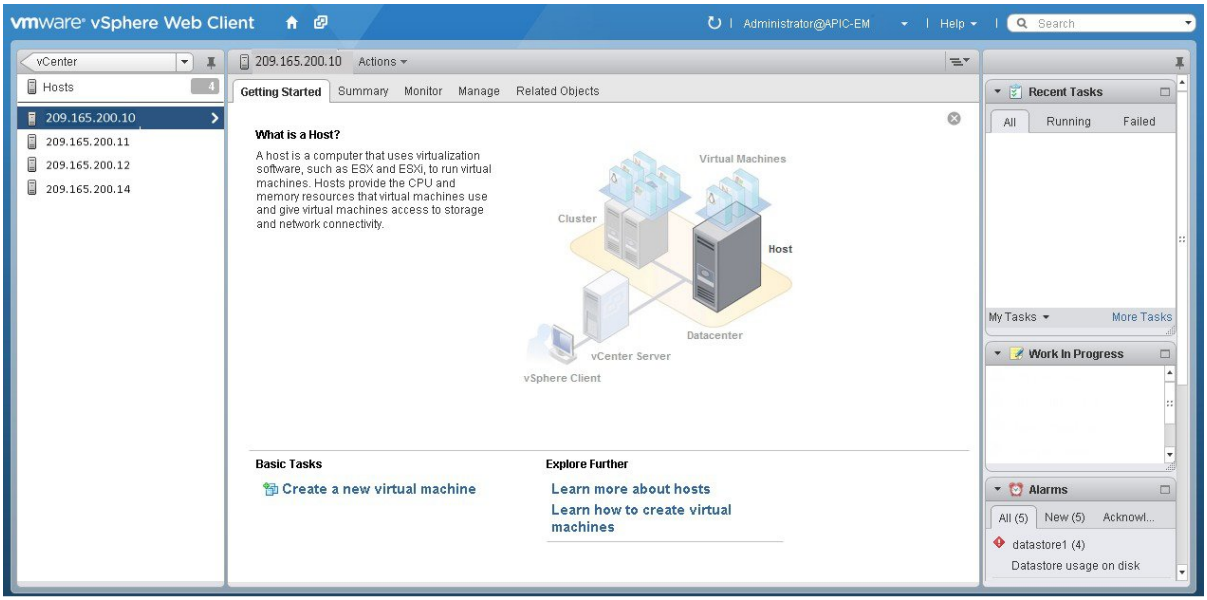
Step 2 Click **vCenter** in the **Navigator**.

Figure 15: vCenter Home



Step 3 Click on **Hosts**.

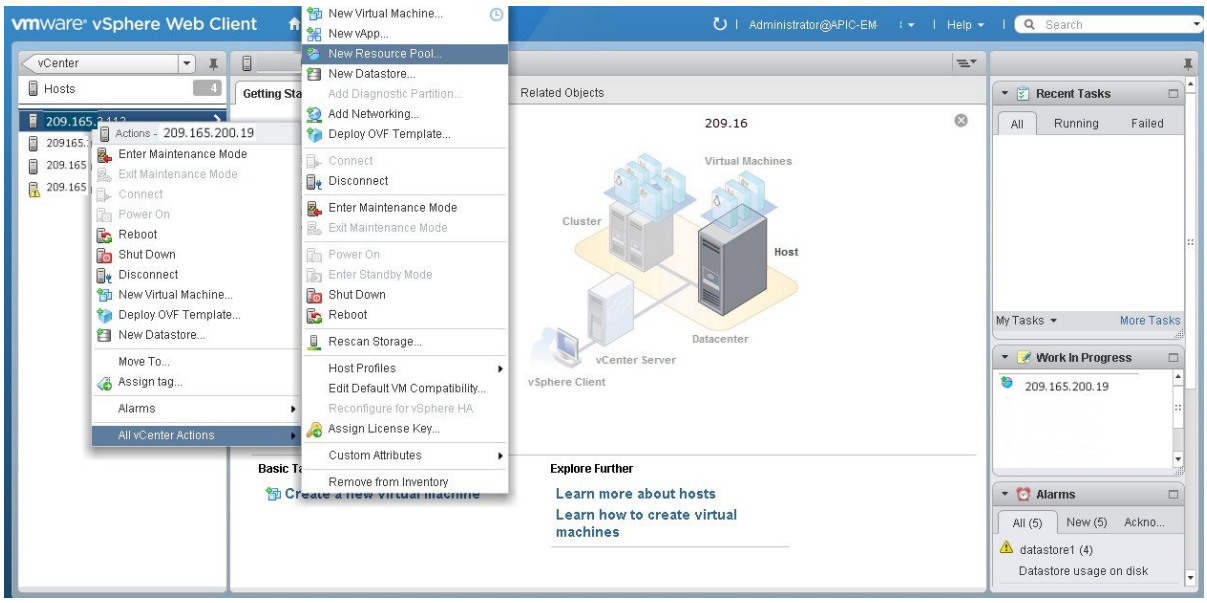
Figure 16: Hosts



Choose a host where you will create the resource pool.

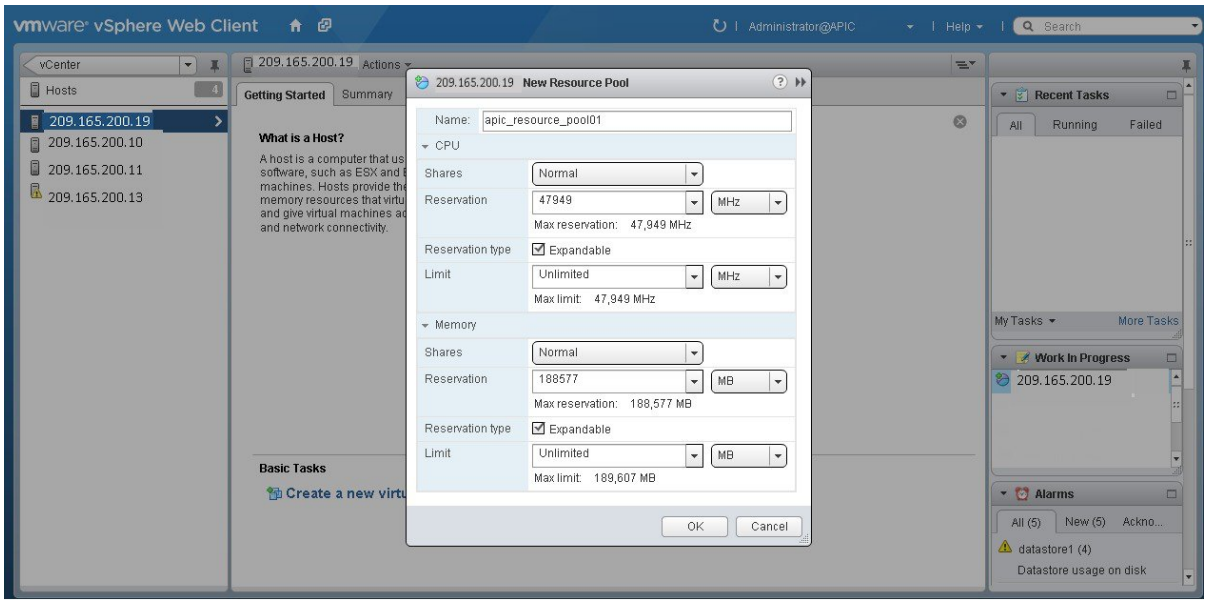
Step 4 Right-click on the selected host and click **All vCenter Actions | New Resource Pool**.

Figure 17: New Resource Pool



Step 5 Enter a name and specify values for the resource pool in the **New Resource Pool** dialog box.

Figure 18: New Resource Pool



We recommend entering the following resource pool values in this dialog box:

- **CPU Resources**
  - **Shares**—Choose **Normal** from the drop-down menu
  - **Reservation**—14400 MHz is minimum configuration setting for this value
  - **Reservation Type**—Check box for Expandable

- **Limit**—Set to Maximum Limit

- **Memory Resources**
  - **Shares**—Choose **Normal** from the drop-down menu
  - **Reservation**—32 GB or 64 GB is the minimum configuration setting for this value, depending upon your hardware.
  - **Reservation Type**—Check box for Expandable
  - **Limit**—Set to Maximum Limit

Step 6 Click **OK** to save the configured resource pool values.

What to do next

Proceed to create a new virtual machine on this resource pool. For assistance with this procedure, see the following procedure, Configuring a VMware Server Using vSphere Web Client.

Configuring a Virtual Machine Using vSphere Web Client

To ensure that the Cisco APIC-EM properly functions in a virtual environment, create the virtual machine(s) following the procedure described below with the recommended settings.

Note You must create this virtual machine on the resource pool that you earlier configured, as described in the previous procedure.

Before you begin

You have reviewed the minimum system requirements for a successful Cisco APIC-EM VMware vSphere installation, as previously described in this guide.

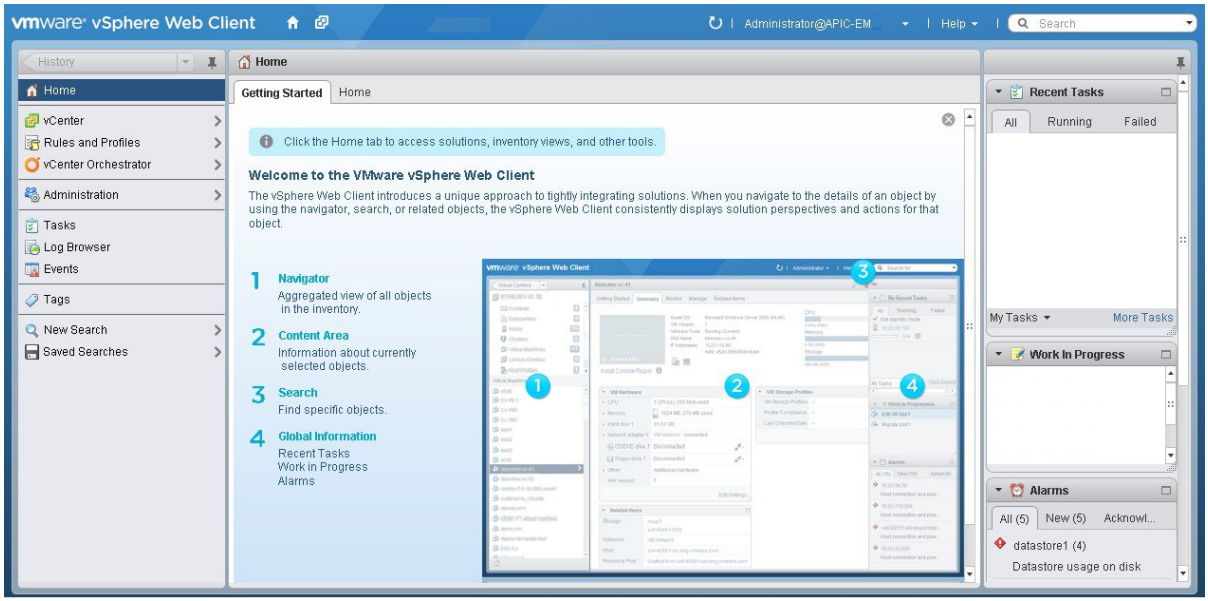
You are familiar with the VMware vSphere Web Client and have a basic knowledge of how to create, manage and troubleshoot virtual machines using the Web Client.

You have your host and virtual datastores already set up and accessible in vSphere Web Client for this procedure.

You have already created a resource pool on the host, following the steps described in the previous procedure, Configuring Resource Pools Using vSphere Web Client.

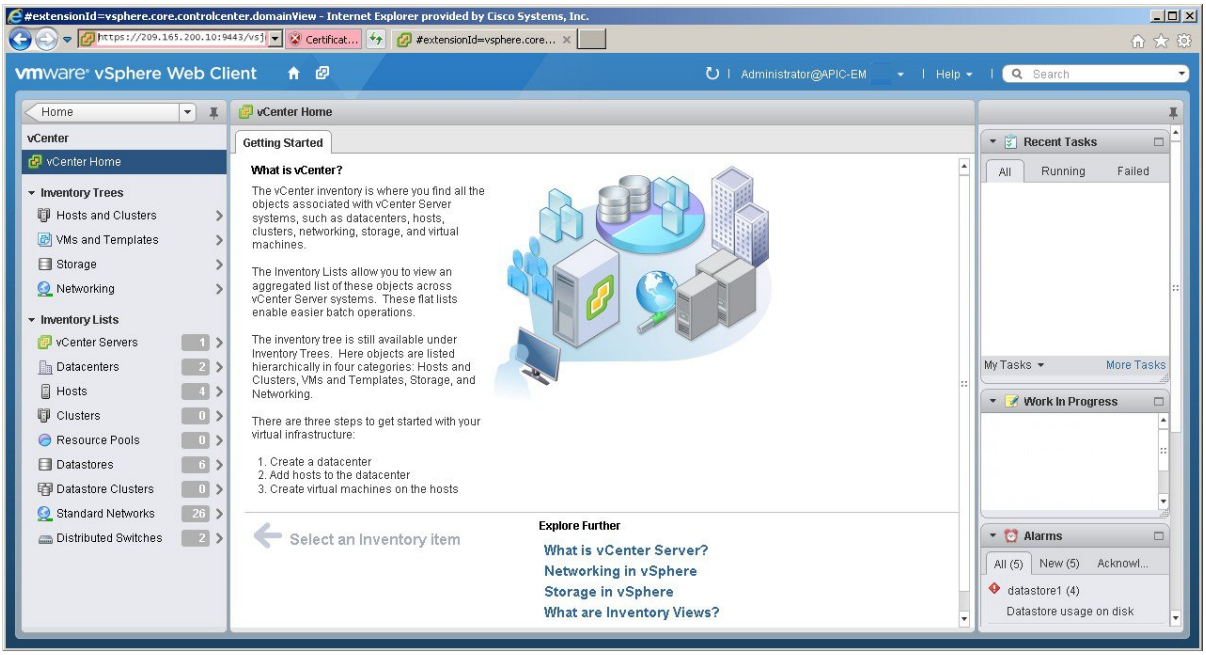
Step 1 Open the VMware vSphere Web Client to perform the procedure.

Figure 19: VMware vSphere Web Client



Step 2 Click **vCenter** in the **Navigator**.

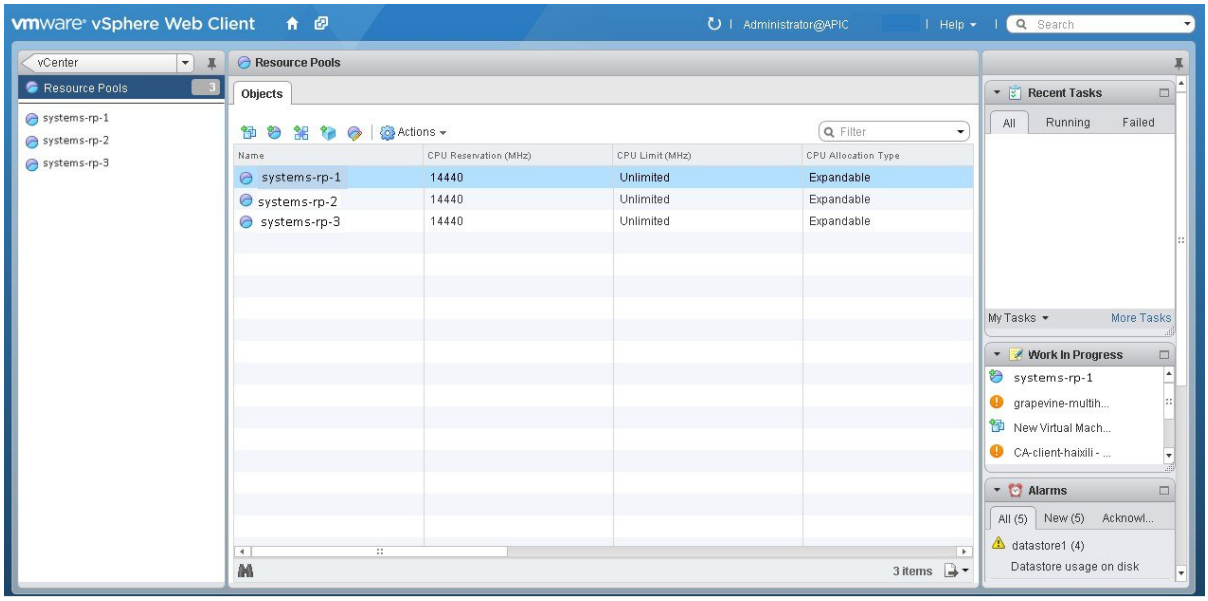
Figure 20: vCenter



Step 3 Click **Resource Pools** in the **Inventory Lists** in **vCenter**.

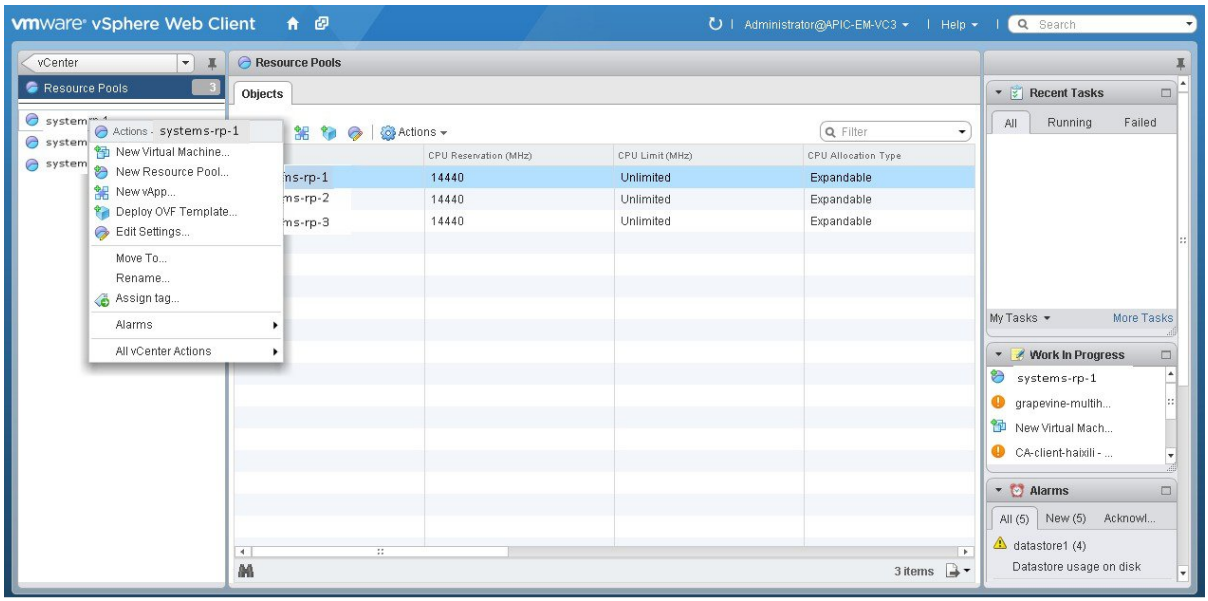
Step 4 Choose the resource pool where you will install the virtual machine from the list.

Figure 21: Resource Pools



Step 5 Right click on the resource pool and select **New Virtual Machine** from the menu.

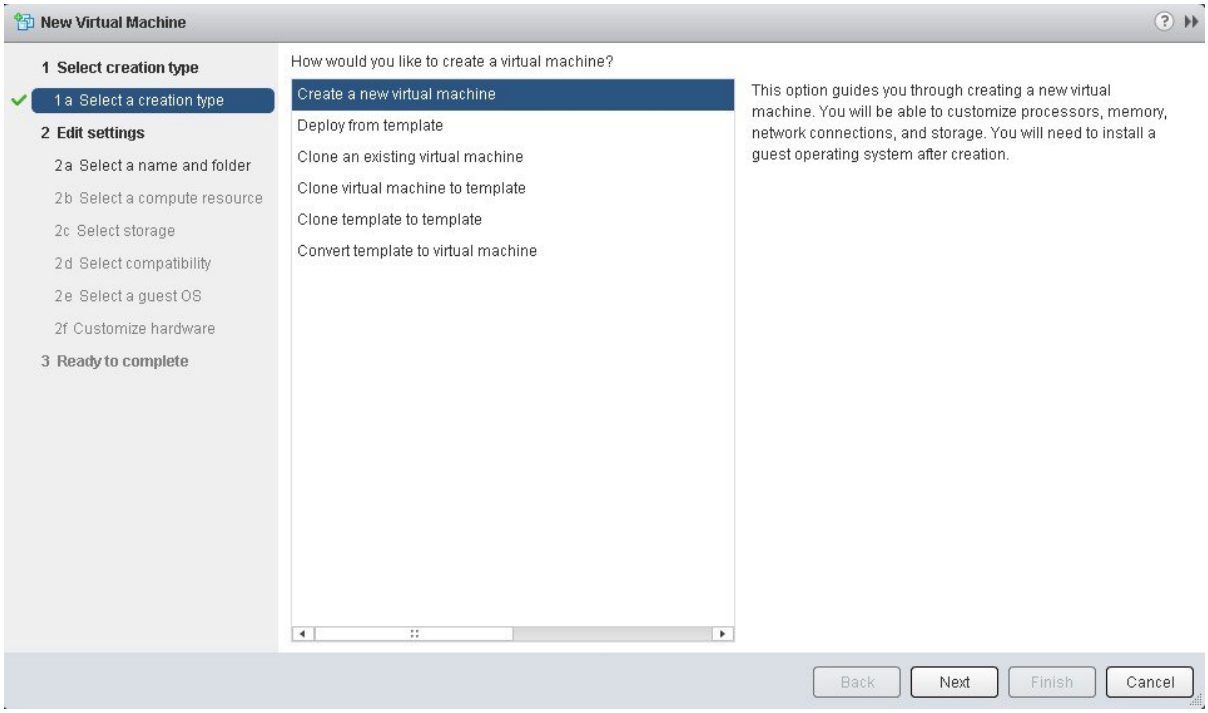
Figure 22: New Virtual Machine



Note We strongly recommend that only a single virtual machine be created under the resource pool.

Step 6 Click **Create a new virtual machine** in the **New Virtual Machine** dialog box under **1a Select creation type**.

Figure 23: Select Creation Type

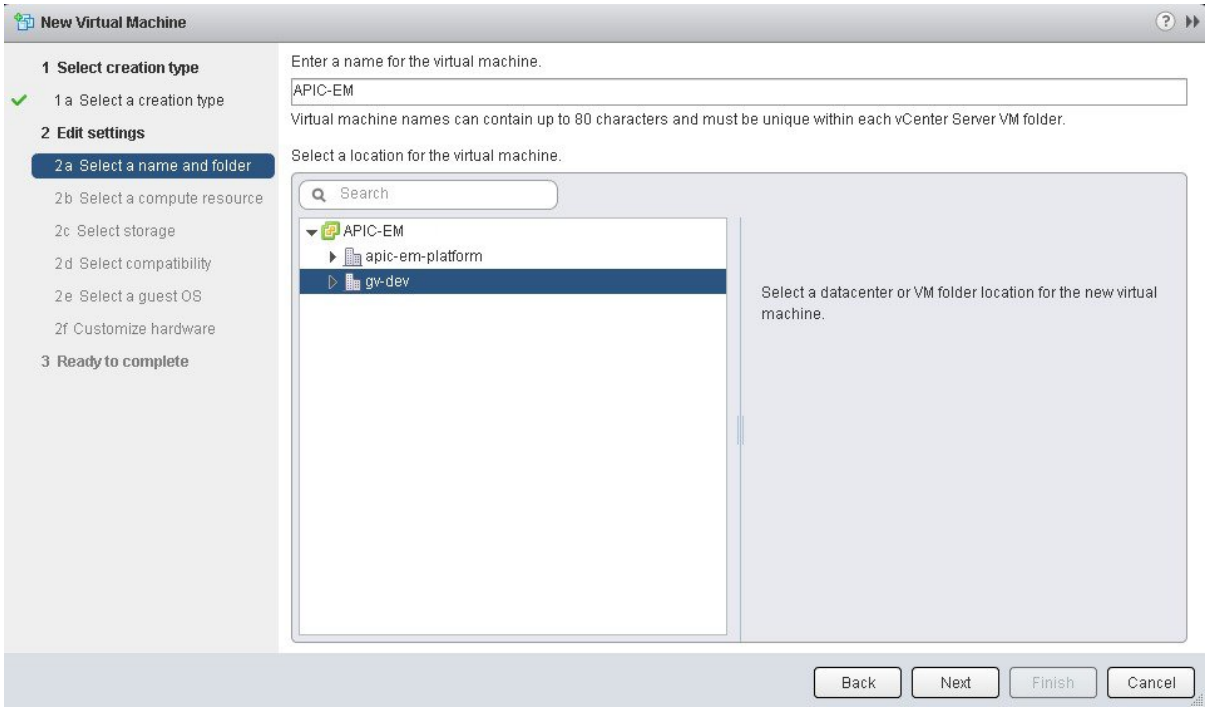


Click **Next** to proceed to the next step.

Step 7 In the **New Virtual Machine** dialog box under **2 Edit Settings**, click **2a Select a name and folder**.

Enter a name for the virtual machine and a location for the virtual machine.

Figure 24: Select Name and Folder

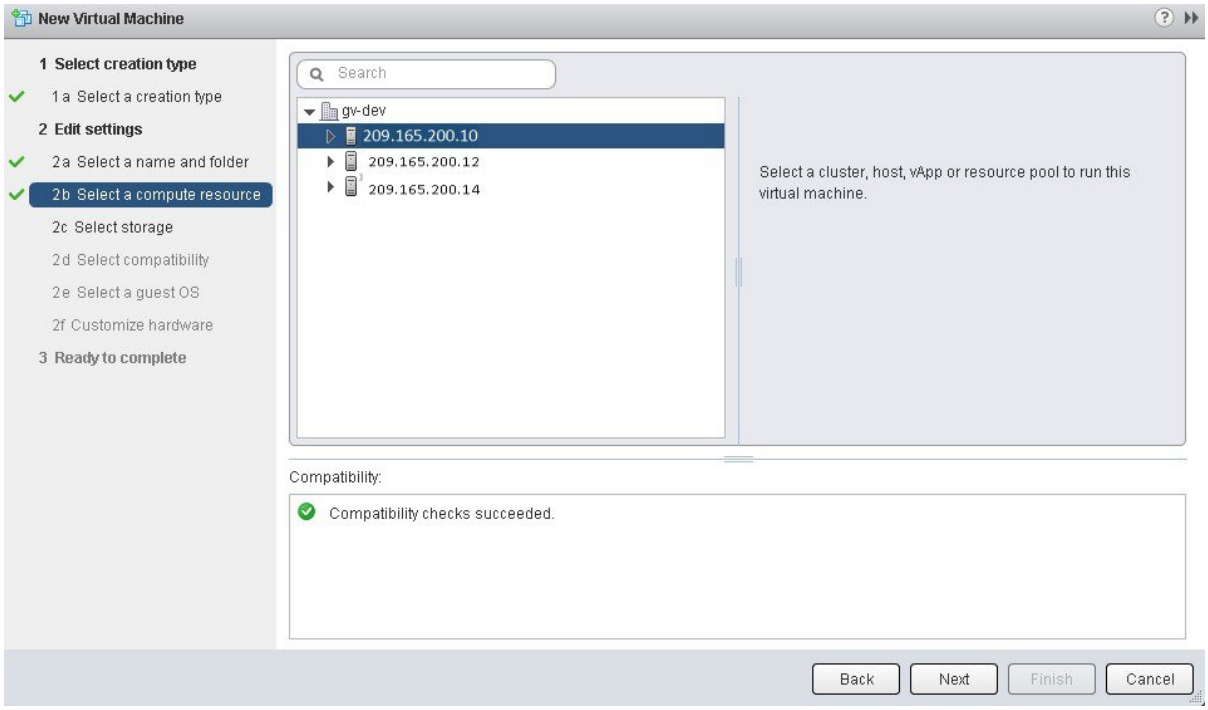


Click **Next** to proceed to the next step.

Step 8 Click **2b Select a computer resource**.

Select the resource pool that was created in the previous procedure.

Figure 25: Select Computer Resource

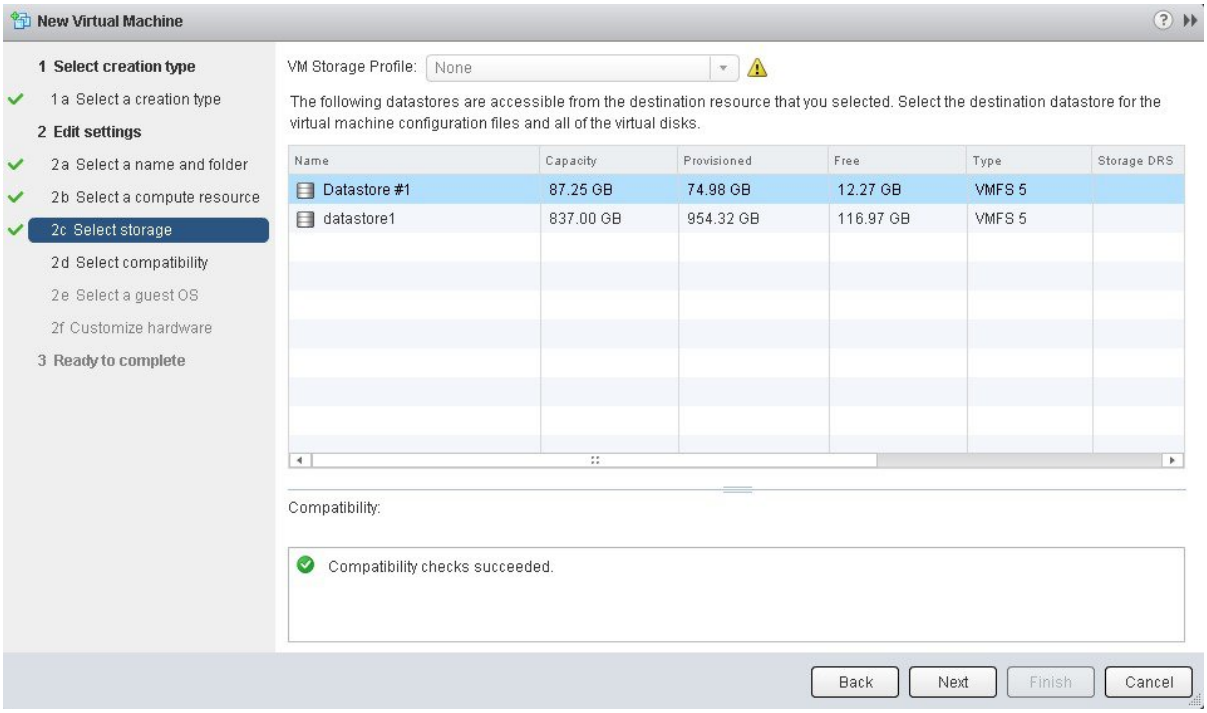


Click **Next** to proceed to the next step.

Step 9 Click **2c Select storage**.

Select a datastore for your virtual machine.

Figure 26: Select Storage

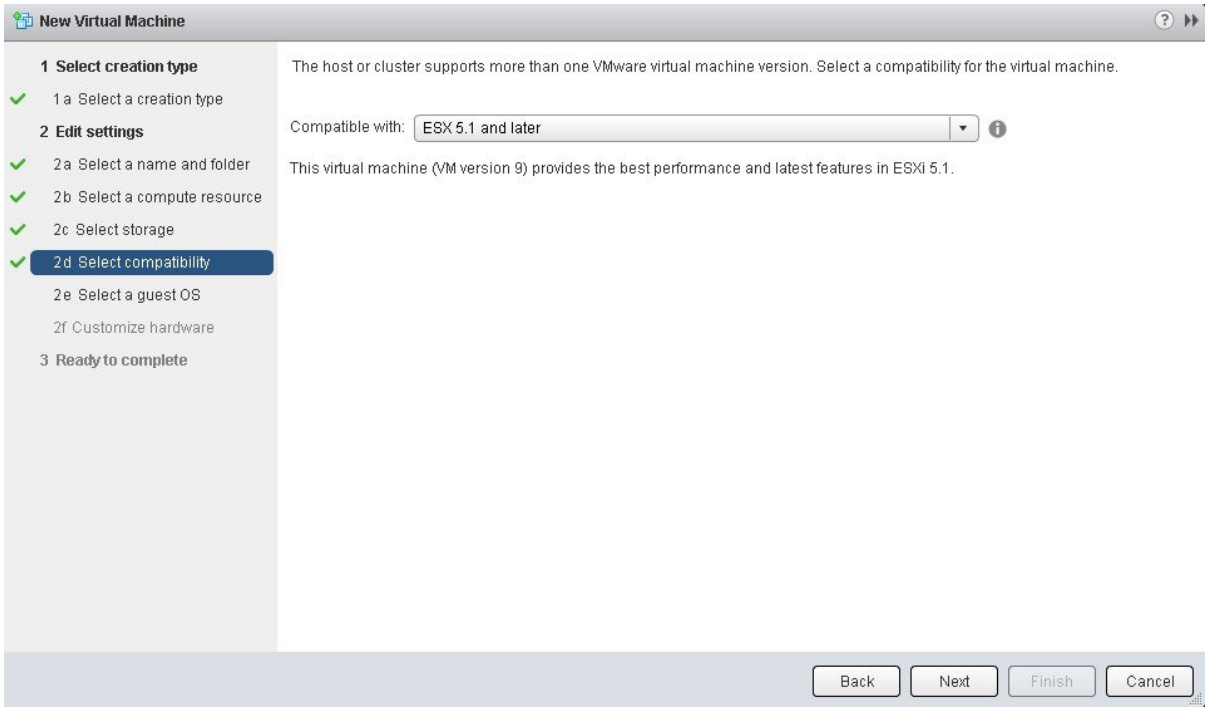


Click **Next** to proceed to the next step.

Step 10 Click **2d Select compatibility**.

Select **ESX 5.1 and later** from the drop down menu.

Figure 27: Select Compatibility



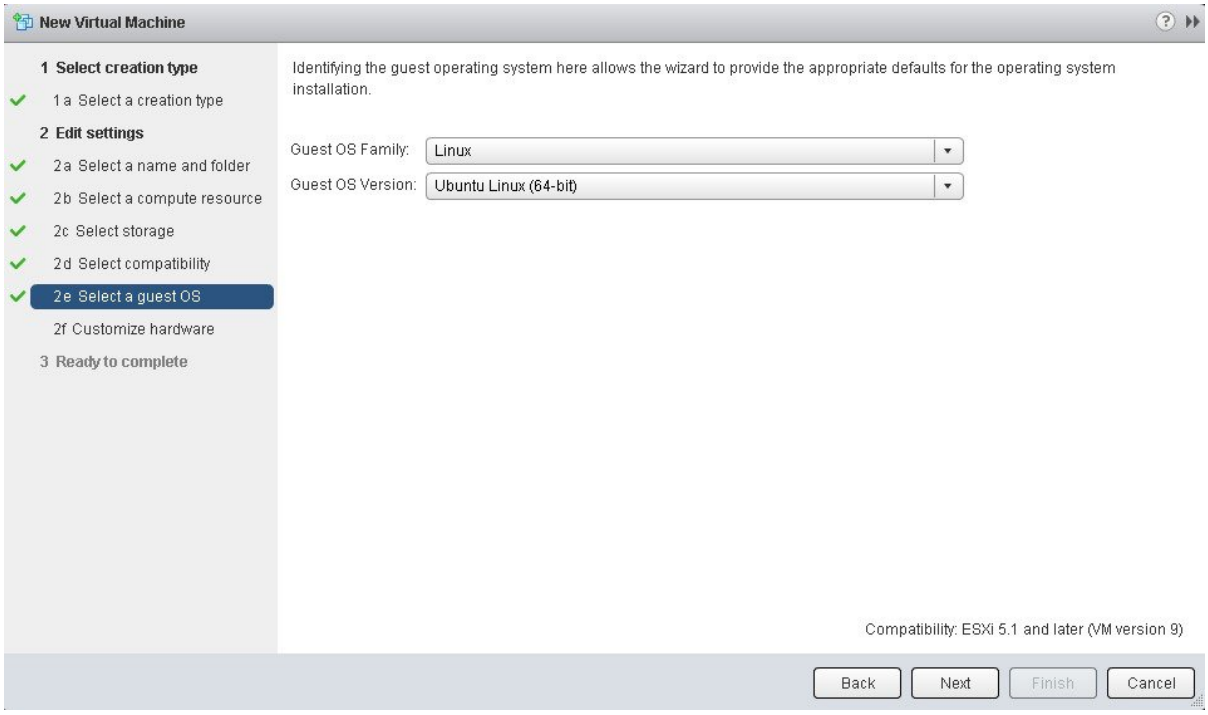
Click **Next** to proceed to the next step.

Step 11 Click **2e Select a guest OS**.

Select the following values from the drop down menus:

- **Guest OS Family**: Linux
- **Guest OS Version**: Ubuntu Linux (64-bit)

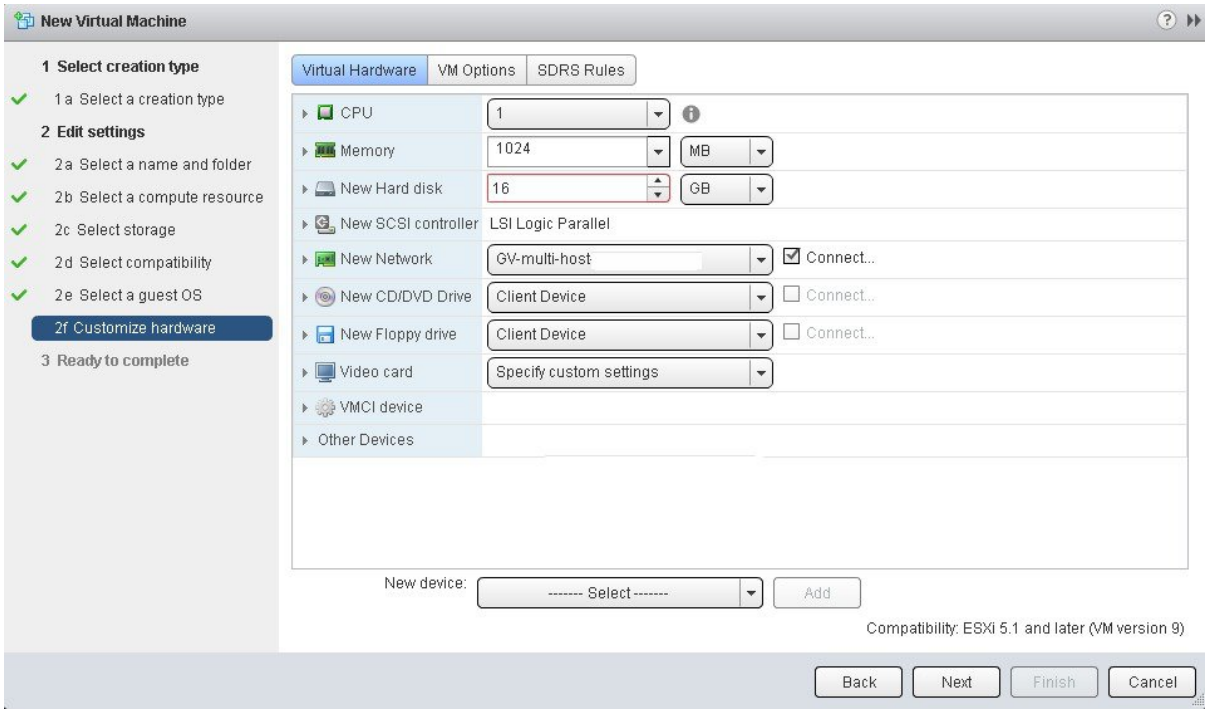
Figure 28: Select Guest OS



Click **Next** to proceed to the next step.

Step 12 Click **2f Customize hardware**.

Figure 29: Customize Hardware



Step 13 In the **Virtual Hardware** tab, ensure that the following **CPU** values are selected.

CPU	Enter a value of 6 cores. **Note** 6 cores is the minimum number to enter for your virtual machine configuration. For better performance, we recommend entering and using 12 cores.
Reservation	Enter a minimum value of at least 14400 MHz.
Limit	Select **Unlimited** from the drop down menu
Shares	Select **Normal** from the drop down menu.

Note The above dedicated CPU resources for the host are required for the Cisco APIC-EM.

Step 14 In the **Virtual Hardware** tab, ensure that the following **Memory** values are selected.

Memory	Enter a minimum value of 32 GB or 64 GB, depending on your hardware.
Reserve all guest memory (all locked)	Check this box.

Note The above dedicated memory resources for the host are required for the Cisco APIC-EM.

Step 15 In the **Virtual Hardware** tab, ensure that the following **New Hard disk** value is entered.

New Hard disk	Increase to at least 500 GB minimum.

Step 16 In the **Virtual Hardware** tab, ensure that the following **New SCSI controller** value is entered.

New SCSI controller	Select **VMware Paravirtual** from the drop down menu.

Step 17 In the **Virtual Hardware** tab, ensure that the following **New Network** values are entered.

New network value	Enter the network that the controller will connect to for this value.
Status	Check the box for **Connect at Power On**.
Adapter type	Select **VMXNET3** from the drop down menu.

Step 18 In the **Virtual Hardware** tab, ensure that the following **New CD/DVD Drive** value is entered.

New CD/DVD Drive	Select **Datastore ISO file** from the drop down and configure the location of the ISO file in the **File** window.
Status	Check the box for **Connect at Power On**.

Step 19 Click the **VM Options** tab to open it and ensure that the following values are entered.

Advanced	Choose **High for Latency sensitivity** from the drop down menu.

Click **Ok** to save your configuration and to proceed to the next step.

Step 20 Click **3 Ready to complete**.

Click **Finish** to finish the virtual machine configuration.

Step 21 In the virtual machine, map the Cisco APIC-EM ISO image onto the local drive (CD/DVD).

Step 22 Boot up the virtual machine and choose the **CD-ROM** option from the **Boot Menu**.

Step 23 Choose **Install Grapevine Appliance** from the **Ubuntu** window that appears in the virtual machine.

What to do next

Proceed to configure the controller by following the configuration wizard prompts.

For information about the configuration process, see following sections:

- Configuring Cisco APIC-EM as a Single Host Using the Wizard, on page 72
- Configuring Cisco APIC-EM as a Multi-Host Cluster Using the Wizard, on page 101

APPENDIX B

Cisco APIC-EM Multi-Host Support

Multi-Host Support

A host is defined as an appliance, physical server, or virtual machine with Linux containers running instances of the Grapevine clients. The Grapevine root itself runs directly on the host's operating system and not in the Linux containers. You can set up either a single host or multi-host deployment. A multi-host deployment with three hosts is best practice for both high availability and scale. Each Grapevine root in a multi-host configuration maintains an Active/Active status with the other Grapevine roots and is therefore able to coordinate with the other Grapevine roots the overall management of the cluster.

Note Active/Active is defined as all Grapevine roots being operational and active.

Each host must be running the same controller software in the multi-host configuration. You are able to mix and match physical and virtual appliances in the multi-host configuration.

The multi-host configuration has the following requirements and features:

- Each host in a multi-host configuration requires a minimum of 32 GB of memory.
- A multi-host cluster comprised of 3 hosts is able to tolerate the loss of one of the hosts and supports a single fail-over (although with only two hosts, there is only software high availability, but no hardware high availability).

  Note If a second host also fails in the three host cluster, the remaining host in the cluster will become inoperable and the cluster will go down. Therefore, in the event of the loss of one of the hosts, we recommend that you remove this host from the cluster using the configuration wizard and then either repair and rejoin this host to the cluster or join a new host to the cluster.

- As each host is configured with 32 GB of memory, if a host failure occurs then the remaining hosts would have a total 64 GB of memory which is sufficient to run the controller.
- All three hosts must reside in the same subnet.

- For a multi-host configuration with Cisco APIC-EM located behind a NAT within your network, note the following information and requirement:
  - The Virtual IP address of the Cisco APIC-EM controller is intended as a destination address for HTTP(S) traffic such as Cisco PnP and PKI download requests.
  - Any outbound connections initiated from the Cisco APIC-EM controller, such as during a Discovery, Inventory Collection, etc., will use the host IP address of one of the three Cisco APIC-EM hosts.
  - Therefore, you need to PAT (Port Address Translation) the host IP addresses of the Cisco APIC-EM hosts to a global public facing IP address for outbound connections from Cisco APIC-EM controller.

Clustering and Database Replication

The clustering feature of the Cisco APIC-EM provides a mechanism for distributing processing and database replication among multiple hosts that run the exact same version of the controller. Clustering provides both a sharing of resources and features, and enables system high availability and scalability.

Security Replication

In a multi-host environment, the security features of a single host are replicated among the other two hosts, including any X.509 certificates or trustpools. Once you join a host to another host or to a cluster, the Cisco APIC-EM credentials are shared and become the same as that of the host you are joining or the pre-existing cluster. The Cisco APIC-EM credentials are cluster-wide (across hosts) and not per-host.

Note We strongly suggest that any multi-host cluster that you set up be located within a secure network environment. For this release, privacy is not enabled for all of the communications between the hosts.

Service Redundancy

The Cisco APIC-EM provides high availability support using service redundancy. A Cisco APIC-EM cluster can be set up across multiple Linux containers within multiple hosts. On each host, the Grapevine root is an application running on the host and the Grapevine clients are created and reside in the containers. Both the Cisco APIC-EM services and database are then instantiated across the clients within the Linux containers:

- Cisco APIC-EM Services:
  - For service high availability, if a service fails then Grapevine (the Elastics Service Platform) spins up a new instance to replace it. If Grapevine is unable to spin up the new instance on the same container after a sole instance fails, then it spins up a new container and then spins up the new instance on this container.
  - Cisco APIC-EM supports a replacement service instance model. For example, assume that one of the roots on a single host spins up an instance. If that host and its root goes down, then another host on another root spins up an instance to ensure continuity of that service.
- Cisco APIC-EM Database:

- The Cisco APIC-EM services use a PostgreSQL database management system. PostgreSQL has a built-in master-slave model for synchronizing data across replicated databases to respond to any failover situation.
- The master and slave postgres instances are grown across different Linux containers and across different hosts. The data of these postgresSql instances are synchronized using PostgresSQL's built-in data streaming replication mechanism. With three hosts, there is one master (with a master postgres instances) and two slaves (each with a slave postgres instance).
- If the master fails, then the slave seamlessly takes over.
- In the event of a failure by the master, an election process occurs among the remaining hosts to determine which becomes the new master. This election process can also be triggered by resetting the controller using the CLI or rebooting the host.

Caution To protect against any hardware failure, you must deploy the Cisco APIC-EM on a cluster with three hosts.

Multi-Host Synchronization

Whenever there is a configuration change on one of the hosts, Grapevine synchronizes the change with the other two hosts. The supported types of synchronization include:

- Database—Synchronization includes any database updates related to the configuration, performance, and monitoring data.
- File—Synchronization includes any changes to the configuration files.

Multi-Host Monitor Process

Grapevine is the main component that manages high availability operations in a cluster. To ensure proper cluster high availability operation, Grapevine uses both health checks and heart beats.

Health checks are used to monitor processes that are low performing and not running properly. Services that run on Grapevine have health checks that are periodically invoked. If there is any indication of an unhealthy service, Grapevine will harvest and regrow that service.

In addition to the health checks, Grapevine also uses heart beats between the services, clients, and roots to monitor the status of the cluster. Grapevine monitors these heart beats for any processes that may have failed. If there is no heart beat, then this indicates that a process has failed and to correct for this situation, Grapevine regrows the service.

Grapevine also uses a heart beat to monitor for adequate memory and storage capability for the cluster. If a heart beat indicates that the cluster's memory or storage fails below an appropriate level necessary for successful operations, then Grapevine will not grow any new services.

Split Brain and Network Partition

When Cisco APIC-EM is configured as a multi-host cluster, a private network connection is set up between the hosts. This private network connection is used by each host to monitor the health and status of the other

cluster hosts. A split brain occurs when there is a temporary failure of the network connection between the hosts, for example, due to any of the following occurrences:

- Physical disconnection of the network connection from a host
- Loss of power to one or more hosts
- Cisco APIC-EM appliance failure

During a split brain occurrence, situations can arise where each separate host is sending commands to a given network device without any coordination with the other hosts, and the results can be problematic.

To correct for a split brain event, when the private network connection fails between one of the hosts, the other two hosts create a quorum and establish a network partition between themselves and the failed host with the following results:

- The split brain or network partition scenarios are be handled by ensuring quorum (majority reads and rights) to the controller database.
- The side of the partition with the "minority" stops operating, since it is be unable to perform quorum (majority reads and rights) to the controller database.
- The side of the partition with the "majority" continues to operate, since they are *able* to perform quorum (majority reads and rights) to the controller database.

INDEX

U

V