Cisco Application Policy Infrastructure Controller Enterprise Module Hardware Installation Guide

First Published: 2015-11-17

Last Modified: 2016-10-25

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS

Preface

Purpose

This hardware installation guide provides the following types of information about the Cisco APIC-EM:

- Prerequisites for a hardware installation for a Cisco APIC-EM series appliance
- Procedures for installing the Cisco APIC-EM software on a supported appliance
- Procedures for installing the Cisco APIC-EM software on a supported VMware virtual machine
- Technical specifications for the Cisco APIC-EM series appliance

Cisco APIC-EM offers a choice of two appliance platforms. Your choice depends on the size of your network:

- Small network—APIC-EM-APL-R-K9
- Large network—APIC-EM-APL-G-K9

You can upgrade an existing Cisco APIC-EM series appliance to the latest software release. For information about the latest software release version and the supported upgrade path options, see the latest Release Notes for the Cisco APIC-EM.

Audience

This publication is for experienced network administrators who will deploy the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM) series appliance in their network. Use this guide to deploy, make secure, access, verify, and troubleshoot the Cisco APIC-EM series appliance.

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 guide as a controller.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.**

Statement 1030

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.
`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.

Convention	Description
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:
    - *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*
    - *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module*
    - *Cisco APIC-EM Quick Start Guide* (directly accessible from the controller's GUI)
    - *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*
    - *Cisco Application Policy Infrastructure Controller Enterprise Module Upgrade Guide*
    - *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*
    - *Cisco Application Policy Infrastructure Controller Enterprise Module Hardware Installation Guide*
    - *Cisco Application Policy Infrastructure Controller Enterprise Module Troubleshooting Guide*
    - *Open Source Used In Cisco APIC-EM*

- 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*[1]

      Cisco IWAN on Cisco APIC-EM Configuration Guide
    - *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 Open Plug-n-Play Agent Configuration Guide*
    - *Mobile Application User Guide for Cisco Network Plug and Play*

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

[1] This is an updated and renamed version of the previous version of this document (*Cisco IWAN on Cisco APIC-EM Configuration Guide*).

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.

CHAPTER 1

Cisco APIC-EM Appliance Networks

This chapter describes several network deployment scenarios, provides information about how to deploy the Cisco APIC-EM Series appliance, and provides a pointer to the switch and Wireless LAN Controller configurations that are needed to support Cisco APIC-EM.

Architecture Overview

The Cisco APIC-EM architecture includes the following components:

- Cisco APIC-EM (deployed as a standalone controller or on multiple hosts for high availability)
- Network Devices (routers, switches, wireless LAN controllers)
- Hosts
- Access points

Related Topics

Supported Cisco Platforms and Software Releases, on page 1

Supported Cisco Platforms and Software Releases

For information about the supported Cisco platforms and software releases:

- See the *Supported Platforms for the Cisco Application Policy Infrastructure Controller Enterprise Module* for the list of supported platforms and software releases for the base controller applications (Discovery, Inventory, Topology,EasyQoS and Path Trace).
- See the *Release Notes for Cisco IWAN on APIC-EM* for the list of supported platforms and software releases for the IWAN application.

- See the *Release Notes for Cisco Network Plug and Play* for the list of supported platforms and software releases for the Cisco Network Plug and Play application.

Related Topics

Architecture Overview, on page 1

Stand Alone and Distributed Deployments

A deployment that has a single Cisco APIC-EM node or host is called a standalone deployment.

A deployment that has more than one Cisco APIC-EM host is called a distributed or multi-host deployment. To support hardware high availability and to improve performance, you can set up a deployment with multiple Cisco APIC-EM hosts in a distributed fashion.

Note A single host or two hosts provide software high availability. Three hosts are required for both software and hardware high availability. With multiple hosts (two or three), all of the hosts must reside in the same subnet. For detailed information about multi-host configurations, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.

In a Cisco APIC-EM distributed deployment, administration, monitoring, and processing activities are distributed across the hosts. Depending on your performance needs, you can scale your deployment.

Deployment Size and Scaling Recommendations

The following table provides guidance on the type of appliance that you would need for your network deployment type.

Table 1: Cisco APIC-EM Scaling Requirements

Deployment Type	Appliance	Appliance Part Number
Small	Cisco APIC-EM Controller Appliance 10C-64G-2T	APIC-EM-APL-R-K9
Large	Cisco APIC-EM Controller Appliance 20C-128G-4T	APIC-EM-APL-G-K9

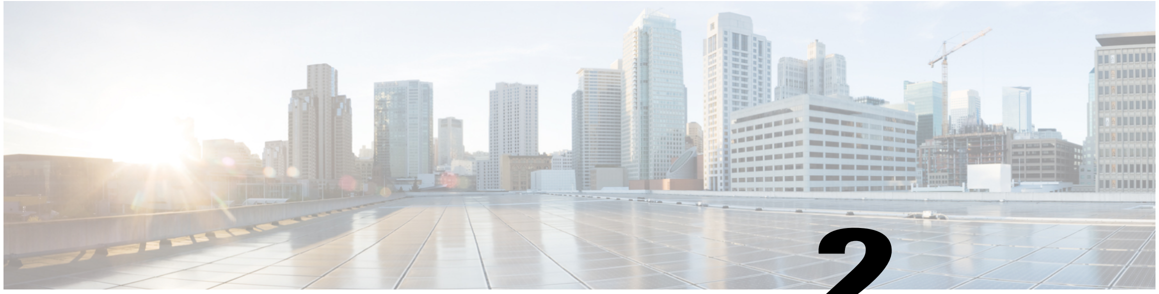
Network Device Configurations Required to Support Cisco APIC-EM Functions

For some types of network devices, you must perform additional configuration procedures to ensure support for Cisco APIC-EM functionality. These additional configuration procedures include the following:

- Enable SNMP traps on the devices that connect to the hosts within your network.

- Enable the NETCONF protocol for the Cisco ASR 9000 router or for any other Cisco device that requires NETCONF support for their device pack.
- Adjust certain specific Wireless LAN controller SNMP configurations.

See the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*, Appendix A, "Required Device Configuration" for information about the above and other required configuration procedures.



CHAPTER 2

Cisco APIC-EM Series Appliances

This chapter describes Cisco APIC-EM series appliances specifications.

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 two 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

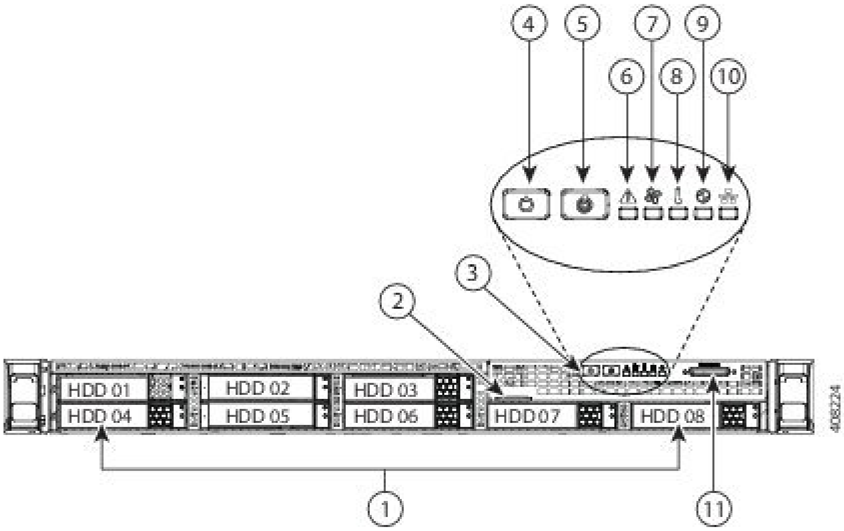
Platform	APIC-EM-APL-R-K9	APIC-EM-APL-G-K9
Ethernet NICs	2 (Gigabit Ethernet ports)	2 (Gigabit Ethernet ports)

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)



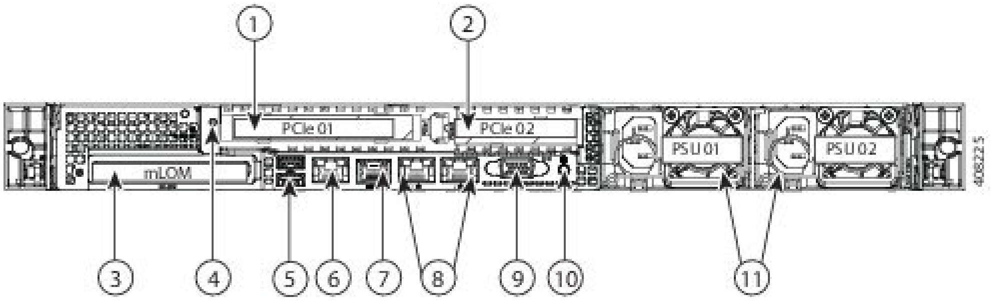
Component	Description
1	Drives (up to eight 2.5-inch drives)
2	Pull-out asset tag
3	Operations panel buttons and LEDs
4	Power button/power status LED
5	Unit identification button/LED
6	System status LED
7	Fan status LED

Component	Description
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)

Component	Description
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 hardware features.

Table 2: Cisco APIC-EM Appliance Series Hardware 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.
Network and Management I/O	Supported connectors: • 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).

Feature	Description
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.

Cisco UCS Server Support for Cisco APIC-EM

The Cisco APIC-EM is available and can be deployed using the following methods:

- As a dedicated Cisco APIC-EM physical appliance purchased from Cisco with the ISO image preinstalled and tested.
- 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 *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*.

  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

- As an ISO image that can be downloaded from Cisco.com and installed in a virtual machine that meets the minimum virtual machine system requirements as listed in the *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*.

CHAPTER 3

Installing and Configuring a Cisco APIC-EM Appliance

This chapter describes how to install the Cisco APIC-EM ISO image on the appliance and configure it.

Installing the Cisco APIC-EM Series Appliance in a Rack

Refer to Installing the Cisco APIC-EM Series Appliance in a Rack, on page 51 for information on safety guidelines, site requirements, and guidelines that you must observe before installing the Cisco APIC-EM series appliance.

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.

  You must configure the CIMC to perform this remote installation.

- Install the ISO image using a USB flash drive.

  1. Create a bootable USB flash drive.
  2. Connect the USB flash device 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.

- 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 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

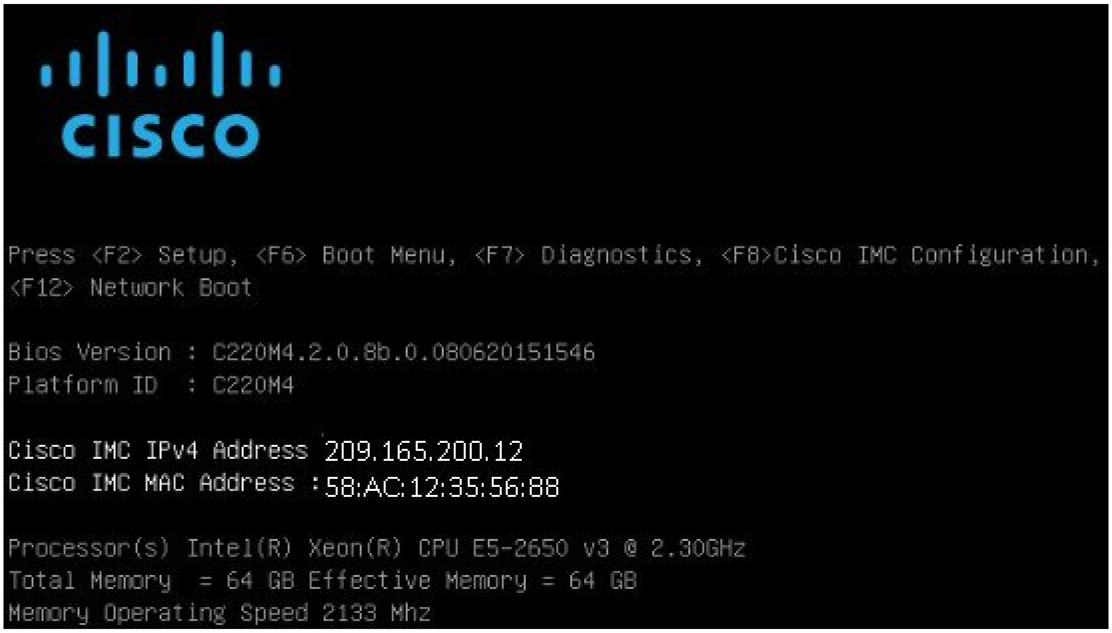
You can perform all operations on Cisco APIC-EM series appliances using the CIMC. To do this, you must first configure an IP address and IP gateway to access the CIMC from a web-based browser.

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.

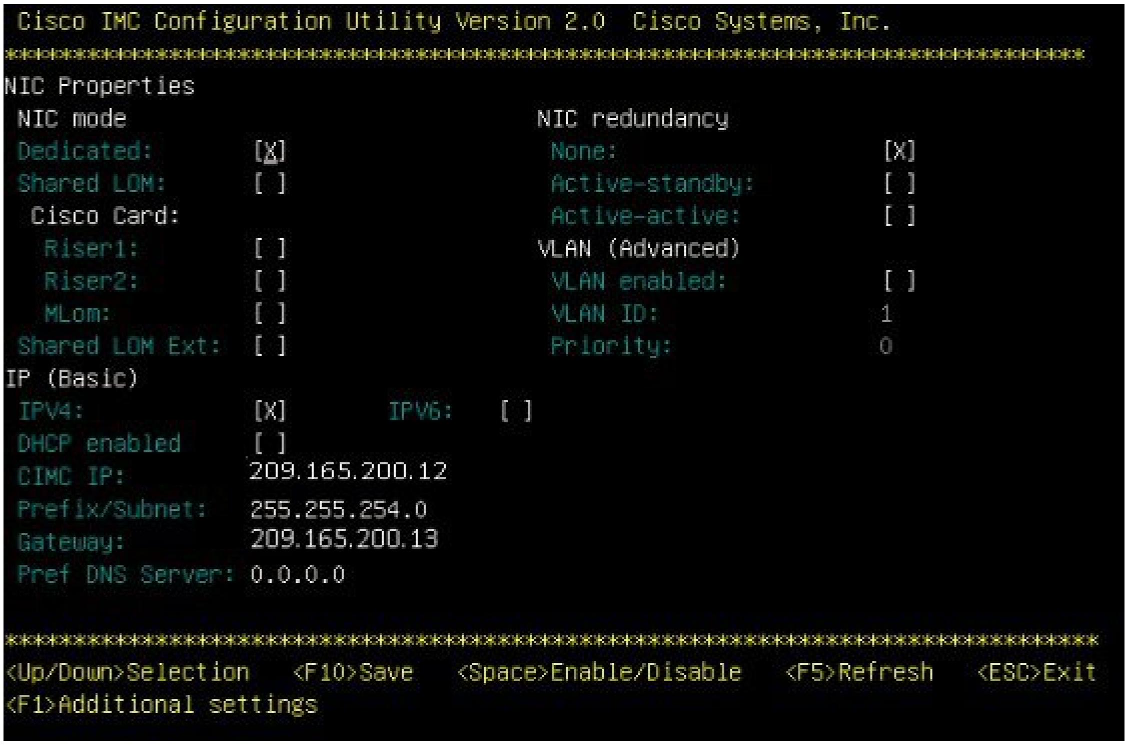
Figure 3: CIMC Opening Screen



```
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8>Cisco IMC Configuration,
<F12> Network Boot

Bios Version : C220M4.2.0.8b.0.080620151546
Platform ID  : C220M4

Cisco IMC IPv4 Address 209.165.200.12
Cisco IMC MAC Address :58:AC:12:35:56:88

Processor(s) Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz
Total Memory  = 64 GB Effective Memory = 64 GB
Memory Operating Speed 2133 Mhz
```

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

Figure 4: CIMC Configuration Utility



```
 Cisco IMC Configuration Utility Version 2.0  Cisco Systems, Inc.
*****************************************************************************
NIC Properties
 NIC mode                              NIC redundancy
 Dedicated:        [X]                  None:                    [X]
 Shared LOM:       [ ]                  Active-standby:          [ ]
  Cisco Card:                           Active-active:           [ ]
   Riser1:         [ ]                 VLAN (Advanced)
   Riser2:         [ ]                  VLAN enabled:            [ ]
   MLom:           [ ]                  VLAN ID:                 1
 Shared LOM Ext:   [ ]                  Priority:                0
IP (Basic)
 IPV4:             [X]        IPV6:    [ ]
 DHCP enabled      [ ]
 CIMC IP:         209.165.200.12
 Prefix/Subnet:   255.255.254.0
 Gateway:         209.165.200.13
 Pref DNS Server: 0.0.0.0

*****************************************************************************
<Up/Down>Selection   <F10>Save   <Space>Enable/Disable   <F5>Refresh   <ESC>Exit
<F1>Additional settings
```

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 20.

Creating a Bootable USB Drive

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

Note As an example, this procedure uses the Rufus freeware utility (version 2.6.818) to create a bootable USB drive. The URL for the Rufus freeware utility download is located at: https://rufus.akeo.ie/

Before You Begin

The bootable USB drive should have a minimum capacity of at least 8 GB.

Step 1 Download a freeware utility to create a bootable USB drive to your 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 laptop or desktop where you downloaded the utility. After connecting your USB drive, the utility GUI appears.

Enter or choose the following values for the bootable USB drive:

- Partition scheme and target system type: MBR partition scheme for BIOS or UEFI
- File system: FAT32
- Cluster size: 4096 bytes
- Quick format
- Create a bootable disk using FreeDOS
- Create extended label and icon files

Note For the Rufus freeware utility, do not change the displayed values in the GUI.

Step 3 For the Rufus freeware utility, click the **Click to select image** icon in the middle of the GUI.

Step 4 Browse 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 drive with the Cisco APIC-EM ISO image installed.

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

What to Do Next

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

Prerequisites for Configuring Cisco APIC-EM Series Appliance

Cisco APIC-EM series appliances are preinstalled with the latest Cisco APIC-EM software.

Make sure that you identify all of the following configuration settings for your deployment before proceeding:

- Hostname
- IP address for the Gigabit Ethernet 0 (eth0) interface
- Netmask
- Default gateway
- Domain Name System (DNS) domain
- Primary name server
- Primary Network Time Protocol (NTP) servers

Note We recommend three NTP servers for the deployment.

- HTTPS proxy server
- Controller GUI username

- Controller GUI password
- Linux (Grapevine) username
- Linux (Grapevine) password

Note For details about the differences between the controller (GUI) admin user and the Linux (Grapevine) admin user, see Admin User Right Differences, on page 43.

Cisco APIC-EM Configuration Wizard Parameters

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

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

Table 3: Cisco APIC-EM Configuration Wizard Parameters

Configuration Wizard Prompt	Description	Example
Host IP address	Must be a valid IPv4 address for the host. This IP address is used for the network adapter (eth0) on the host and connects to the external network or networks. For multiple network adapters, have several IP addresses available.	10.0.0.12
(Optional) Virtual IP address	Must be a valid IPv4 address. This virtual IP address is used for the network adapter (eth0) on the host. You should only configure a virtual IP address, if you are setting up a multi-host deployment.	10.12.13.14
Netmask IP address	Must be a valid IPv4 netmask.	255.255.255.0
Default Gateway IP address	Must be a valid IPv4 address for the default gateway.	10.12.13.1

Configuration Wizard Prompt	Description	Example
Primary server	Must be a valid IPv4 address for the primary server.	10.15.20.25 **Note** Enter either a single IP address for a single primary server, or multiple IP addresses separated by spaces for DNS servers.
Primary NTP server	Must be a valid IPv4 address or hostname of a Network Time Protocol (NTP) server.	10.12.13.10 Enter either a single IP address for a single NTP primary server, or multiple IP addresses separated by spaces for several NTP servers. We recommend that you configure three NTP servers for your deployment.
Add/Edit another NTP server	Must be a valid NTP domain.	10.12.13.11 Allows you to configure multiple NTP servers. **Note** We recommend that you configure three NTP servers for your deployment.
HTTPS proxy server	Must be a valid IPv4 address for the HTTPS proxy with port number.	https://209.165.200.11:3128
Admin Username	Identifies the administrative username used for GUI access to the Cisco APIC-EM controller. We recommend that the username be three to eight characters in length and be composed of valid alphanumeric characters (A–Z, a–z, or 0–9).	admin2780

Configuration Wizard Prompt	Description	Example
Admin Password	Identifies the administrative password that is used for GUI access to the Cisco APIC-EM controller. You must create this password because there is no default. The password meet the following requirements: • Eight character minimum length. • Does NOT contain a tab or a line break. • Does contain characters from at least three of the following categories: ◦ Uppercase alphabet ◦ Lowercase alphabet ◦ Numeral ◦ Special characters (for example, ! or #)	MyIseYPass2
Linux Username	Identifies the Linux (Grapevine) username used for CLI access to the Grapevine root and clients.	The default is 'grapevine' and cannot be changed.

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

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 13

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.

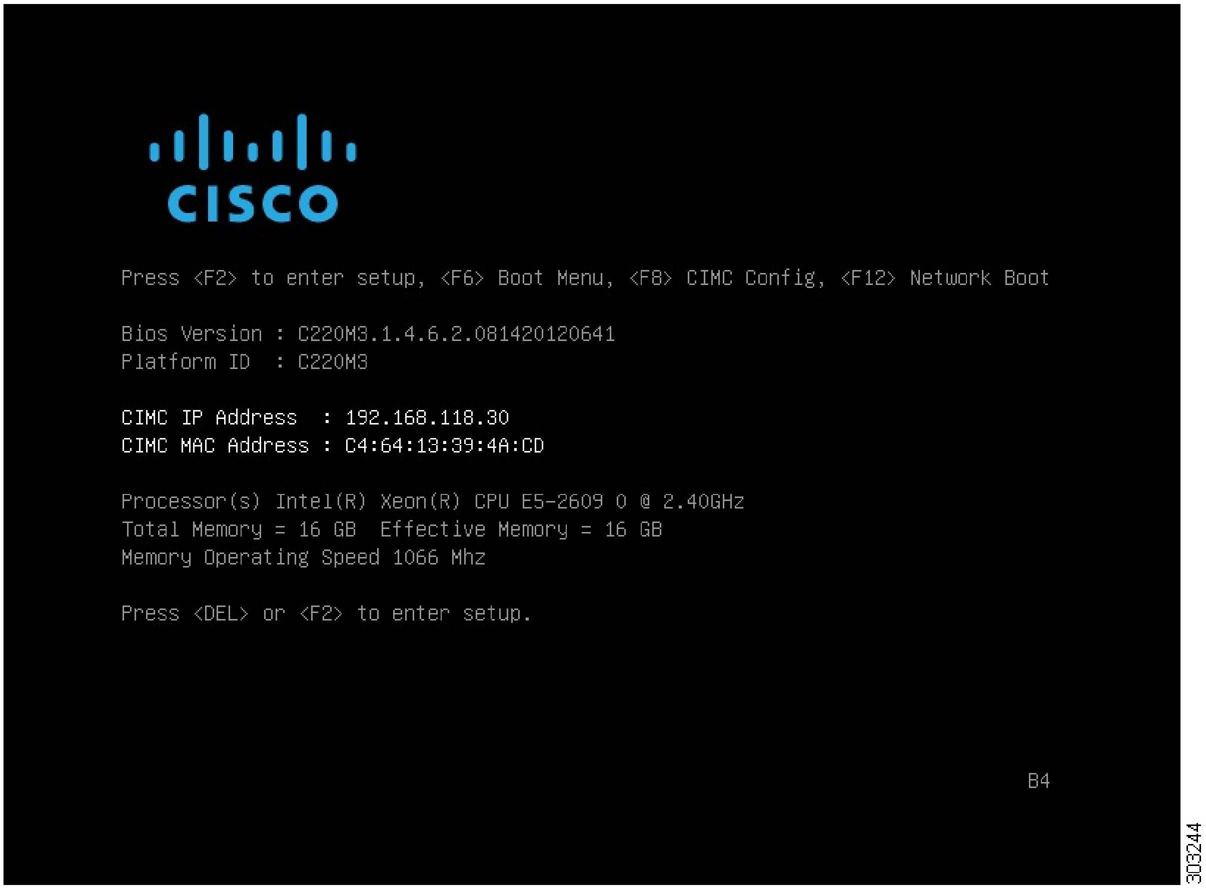
Step 6 Click **Activate Virtual Devices** from the **Virtual Media** drop down menu.

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.

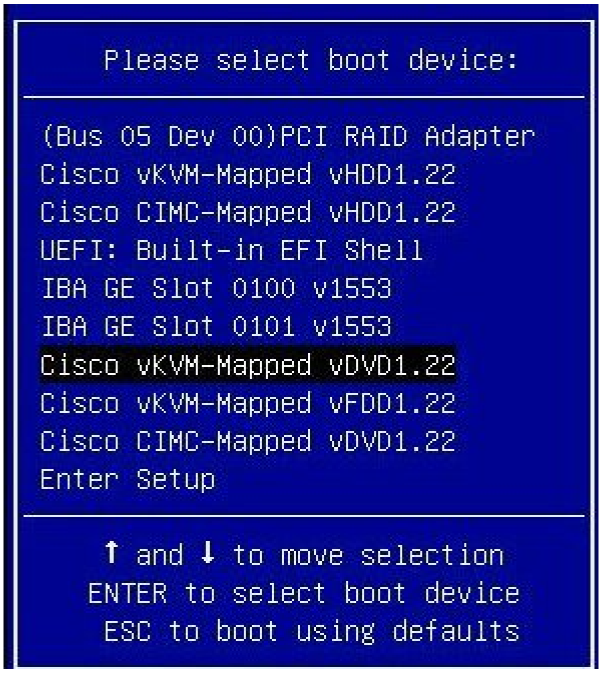
Figure 5: CIMC Window



```
Press <F2> to enter setup, <F6> Boot Menu, <F8> CIMC Config, <F12> Network Boot

Bios Version : C220M3.1.4.6.2.081420120641
Platform ID  : C220M3

CIMC IP Address  : 192.168.118.30
CIMC MAC Address : C4:64:13:39:4A:CD

Processor(s) Intel(R) Xeon(R) CPU E5-2609 0 @ 2.40GHz
Total Memory = 16 GB  Effective Memory = 16 GB
Memory Operating Speed 1066 Mhz

Press <DEL> or <F2> to enter setup.

                                                                    B4
```

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

Figure 6: Boot Device Window



```
     Please select boot device:
 ------------------------------------
 (Bus 05 Dev 00)PCI RAID Adapter
 Cisco vKVM-Mapped vHDD1.22
 Cisco CIMC-Mapped vHDD1.22
 UEFI: Built-in EFI Shell
 IBA GE Slot 0100 v1553
 IBA GE Slot 0101 v1553
 Cisco vKVM-Mapped vDVD1.22
 Cisco vKVM-Mapped vFDD1.22
 Cisco CIMC-Mapped vDVD1.22
 Enter Setup
 ------------------------------------
     ↑ and ↓ to move selection
    ENTER to select boot device
     ESC to boot using defaults
```

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.

See the “Configuring Cisco APIC-EM as a Single Host Using the Wizard” section in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, for information about the configuration wizard process.

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 " Configuring the Cisco APIC-EM Settings" chapter in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, for information about configuring the controller settings.

CHAPTER 4

Installing Cisco APIC-EM on a VMware Virtual Machine

In addition to acquiring a dedicated Cisco APIC-EM physical appliance with the ISO image preinstalled and tested, you can also install the Cisco APIC-EM ISO image in a supported virtual environment. You may want to do this for testing the controller within your network, prior to setting up the appliance.

This chapter describes the system requirements and procedures for installing Cisco APIC-EM on a VMware virtual machine.

Cisco APIC-EM VMware vSphere Requirements

The following table lists the minimum system requirements for a successful Cisco APIC-EM VMware vSphere installation.

In addition to the minimum system requirements listed below, we recommend that you also configure specific resource pools for the virtual machine(s). For information about these additional recommended configurations, see the following section about preparing your virtual machines for the Cisco APIC-EM.

Note 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 (2 or 3 hosts), 32 GB of RAM is required for each of the virtual machines that contains the Cisco APIC-EM. Three servers are required for high availability and redundancy

Note As with running an application on any virtualization technology, you might observe a degradation in performance when you run the Cisco APIC-EM in a virtual machine compared to running the Cisco APIC-EM directly on physical hardware.

Table 4: Cisco APIC-EM VMware vSphere Requirements

Virtual Machine Options	VMware ESXi Version	5.1/5.5/6.0
	Server 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	CPU (speed)	2.4 GHz
	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 deployment (2 or 3 hosts) 32 GB of RAM is required for each host.
	Disk Capacity	500 GB
	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 50.0 or later • Mozilla Firefox, version 46.0 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.

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 5: Virtual Machine Configuration Recommendations (Including Resource Pools)

Resource Pool: CPU Resources	Reservation—14400 MHz is minimum configuration setting for this value Limit—Unlimited Shares—Normal
vCPU	6 (minimum) **Note** 6 vCPUs is the minimum number required for your virtual machine configuration. For better performance, we recommend using 12 CPUs.
Resource Pool: Memory	Memory—32 GB or 64 GB is the minimum configuration setting for this value, depending upon your hardware. Reserve all guest memory—Enable
SCSI controller value	VMware Paravirtual
New network value	New network value—Enter the network that the controller will connect to. Status—Connect at power on Adapter type—VMXNET3
Advanced	Choose High for the Latency sensitivity

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

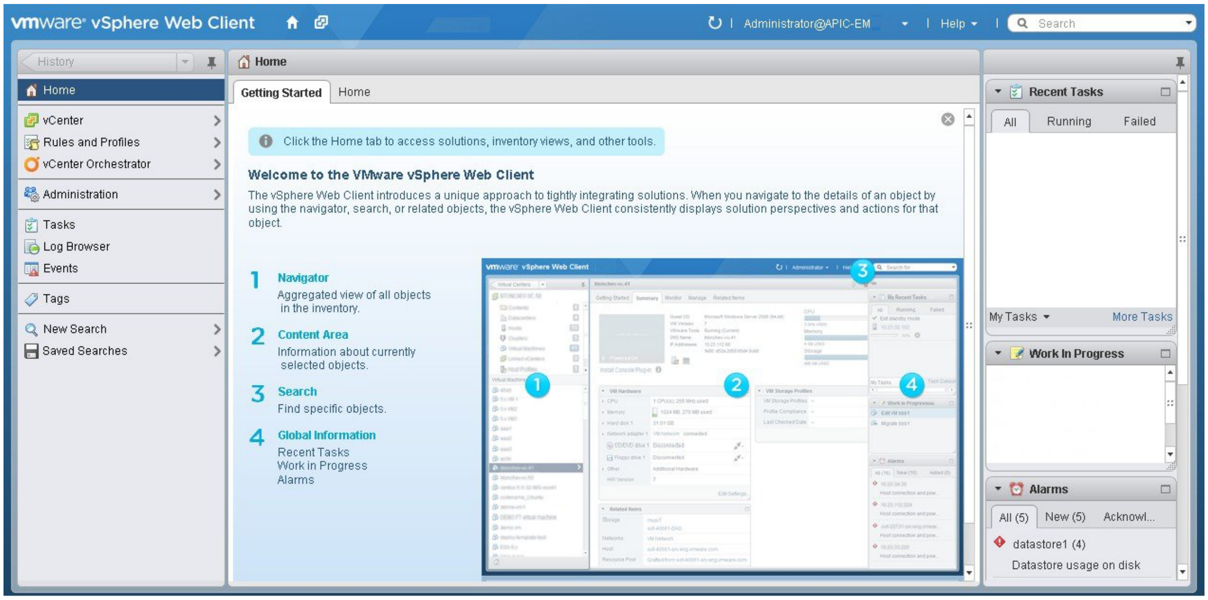
You have reviewed your VMware documentation concerning resource pools and their configuration.

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 7: VMware vSphere Web Client



Click the Home tab to access solutions, inventory views, and other tools.

Welcome to the VMware vSphere Web Client

The vSphere Web Client introduces a unique approach to tightly integrating solutions. When you navigate to the details of an object by using the navigator, search, or related objects, the vSphere Web Client consistently displays solution perspectives and actions for that object.

1 Navigator
Aggregated view of all objects in the inventory.

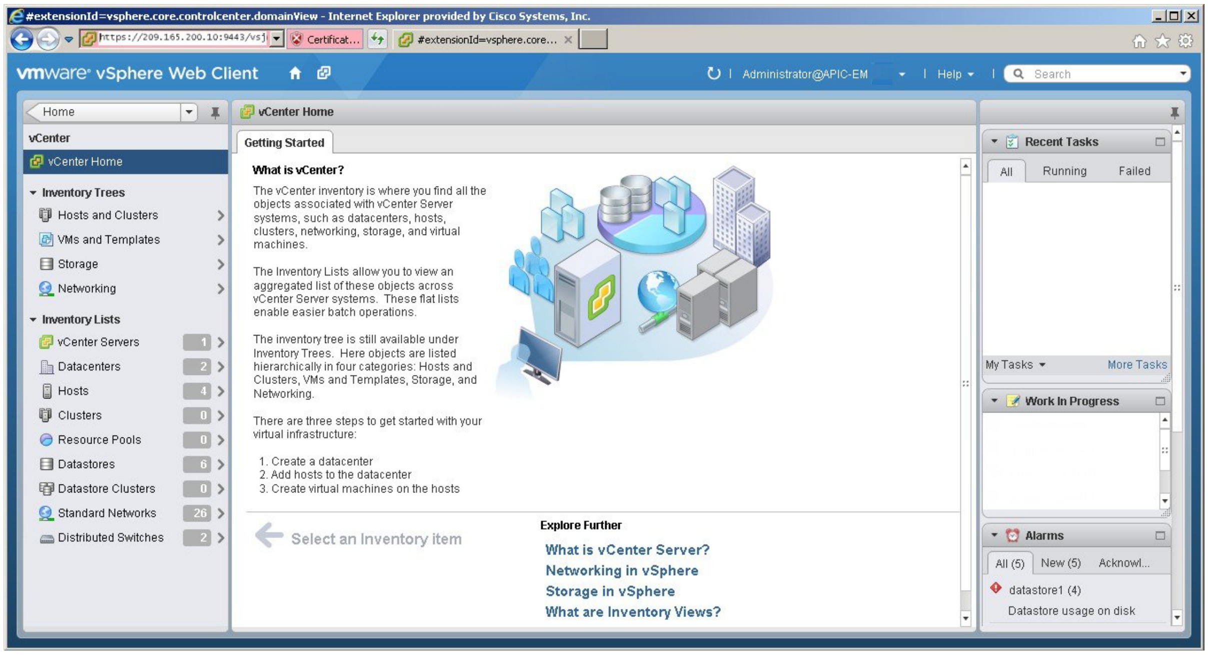
2 Content Area
Information about currently selected objects.

3 Search
Find specific objects.

4 Global Information
Recent Tasks
Work in Progress
Alarms

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

Figure 8: vCenter Home



What is vCenter?

The vCenter inventory is where you find all the objects associated with vCenter Server systems, such as datacenters, hosts, clusters, networking, storage, and virtual machines.

The Inventory Lists allow you to view an aggregated list of these objects across vCenter Server systems. These flat lists enable easier batch operations.

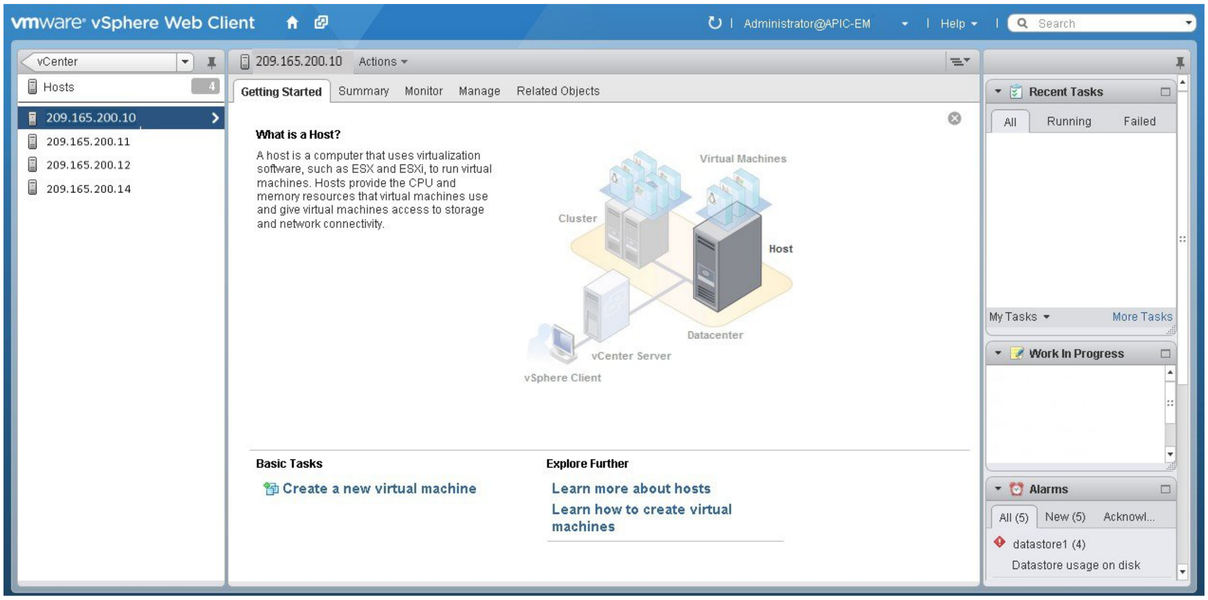
The inventory tree is still available under Inventory Trees. Here objects are listed hierarchically in four categories: Hosts and Clusters, VMs and Templates, Storage, and Networking.

There are three steps to get started with your virtual infrastructure:

1. Create a datacenter
2. Add hosts to the datacenter
3. Create virtual machines on the hosts

Step 3 Click on **Hosts**.

Figure 9: Hosts



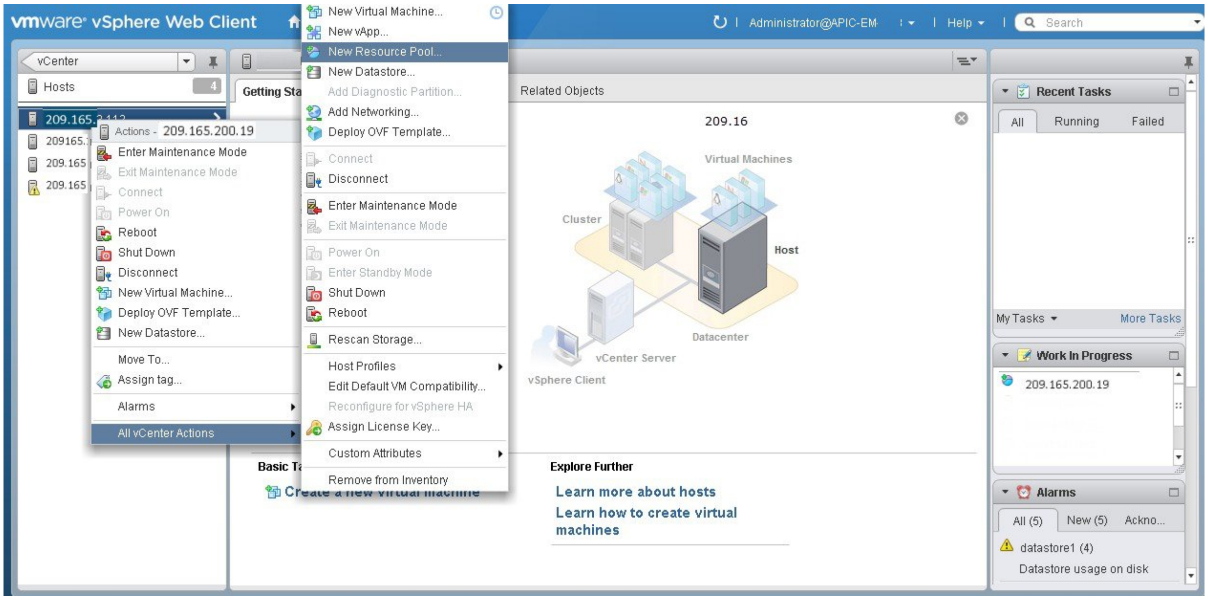
What is a Host?

A host is a computer that uses virtualization software, such as ESX and ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

Choose a host where you will create the resource pool.

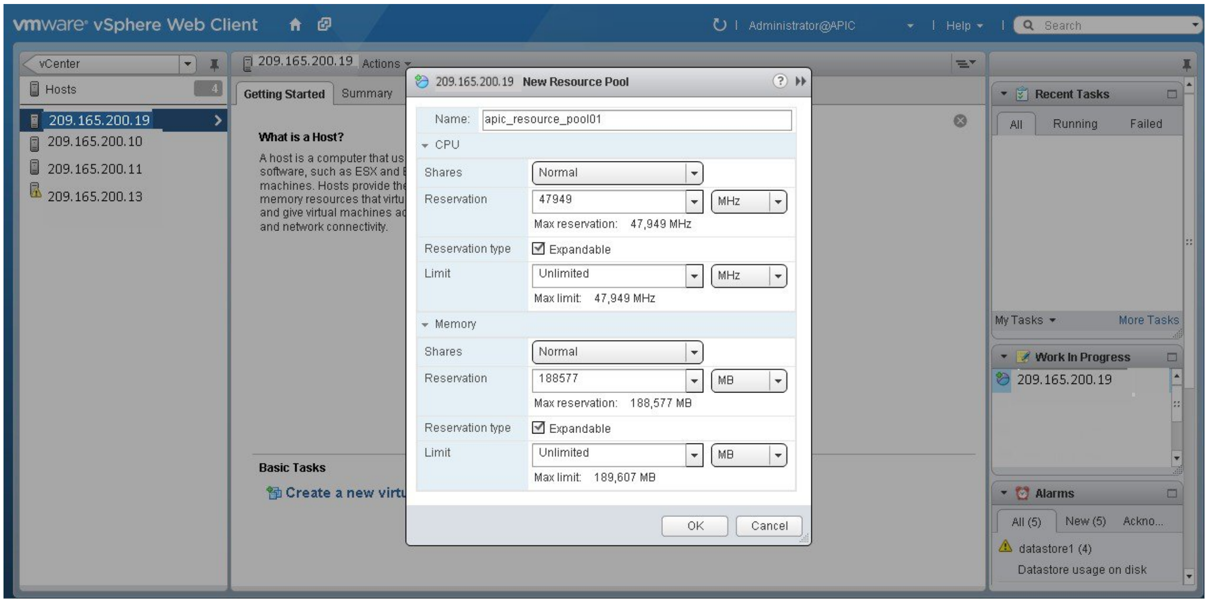
Step 4 Right-click on the selected host and click **All vCenter Actions | New Resource Pool**.

Figure 10: New Resource Pool



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

Figure 11: New Resource Pool



209.165.200.19 New Resource Pool

Name: apic_resource_pool01

CPU

Shares	Normal
Reservation	47949 MHz Max reservation: 47,949 MHz
Reservation type	☑ Expandable
Limit	Unlimited MHz Max limit: 47,949 MHz

Memory

Shares	Normal
Reservation	188577 MB Max reservation: 188,577 MB
Reservation type	☑ Expandable
Limit	Unlimited MB Max limit: 189,607 MB

OK Cancel

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.

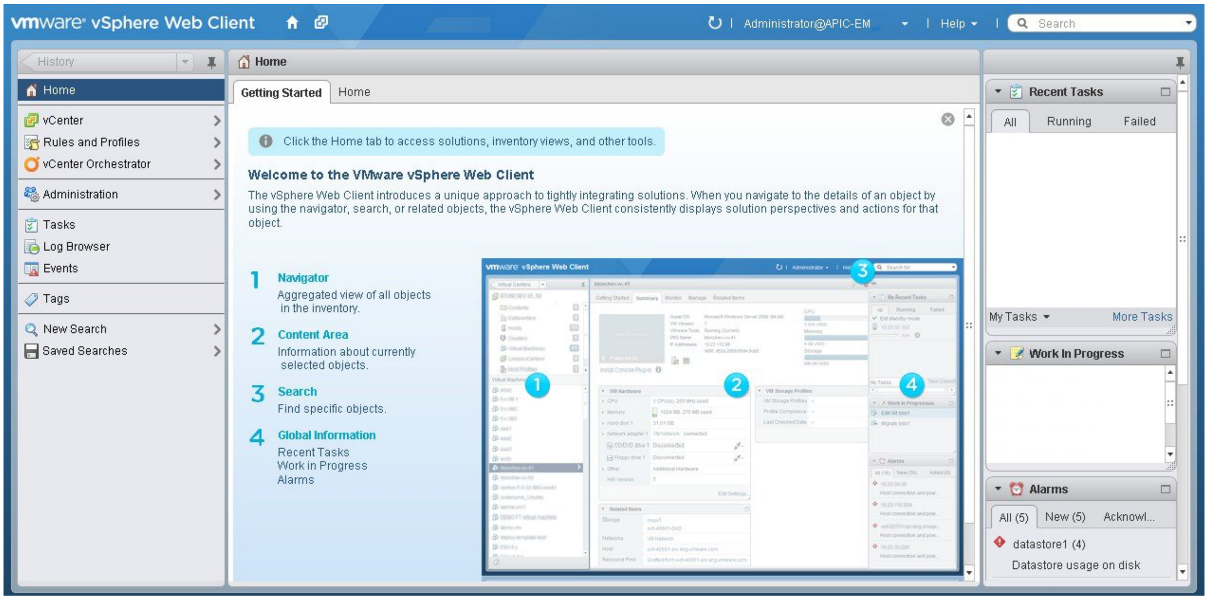
You are familiar with the VMware vSphere Web Client and have a basic knowledge of how to create, manage and troubleshoot virtual machines using the Web Client.

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 12: VMware vSphere Web Client



Click the Home tab to access solutions, inventory views, and other tools.

Welcome to the VMware vSphere Web Client

The vSphere Web Client introduces a unique approach to tightly integrating solutions. When you navigate to the details of an object by using the navigator, search, or related objects, the vSphere Web Client consistently displays solution perspectives and actions for that object.

1 Navigator
Aggregated view of all objects in the inventory.

2 Content Area
Information about currently selected objects.

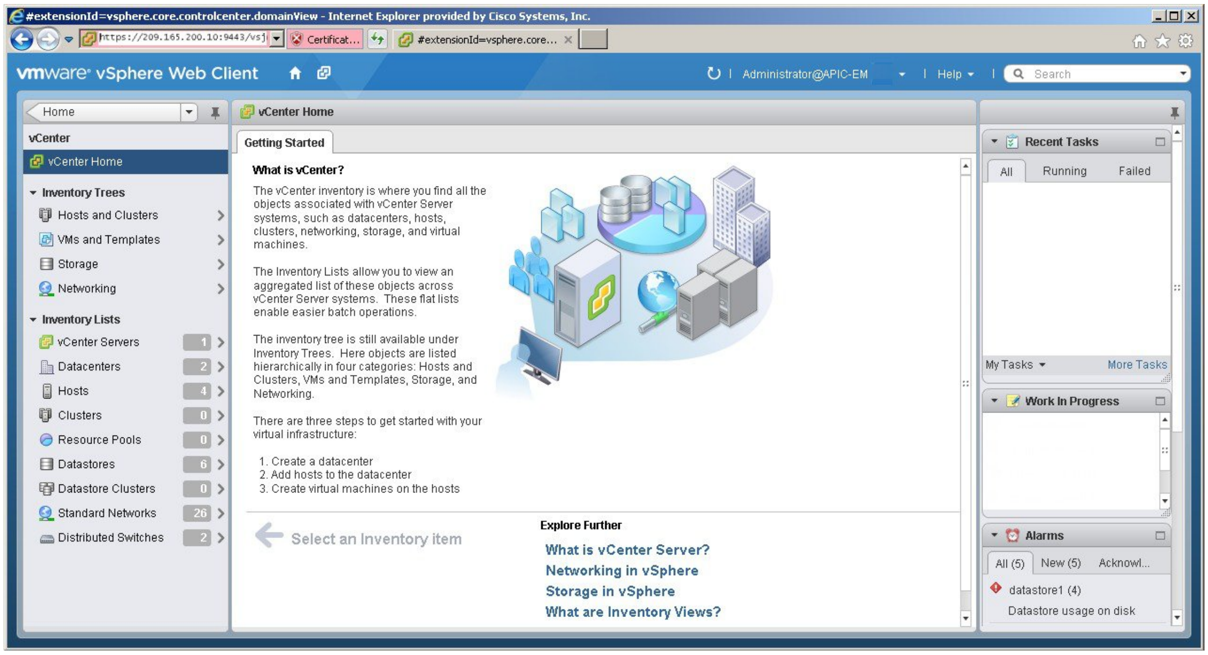
3 Search
Find specific objects.

4 Global Information
Recent Tasks
Work in Progress
Alarms

datastore1 (4)
Datastore usage on disk

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

Figure 13: vCenter



What is vCenter?

The vCenter inventory is where you find all the objects associated with vCenter Server systems, such as datacenters, hosts, clusters, networking, storage, and virtual machines.

The Inventory Lists allow you to view an aggregated list of these objects across vCenter Server systems. These flat lists enable easier batch operations.

The inventory tree is still available under Inventory Trees. Here objects are listed hierarchically in four categories: Hosts and Clusters, VMs and Templates, Storage, and Networking.

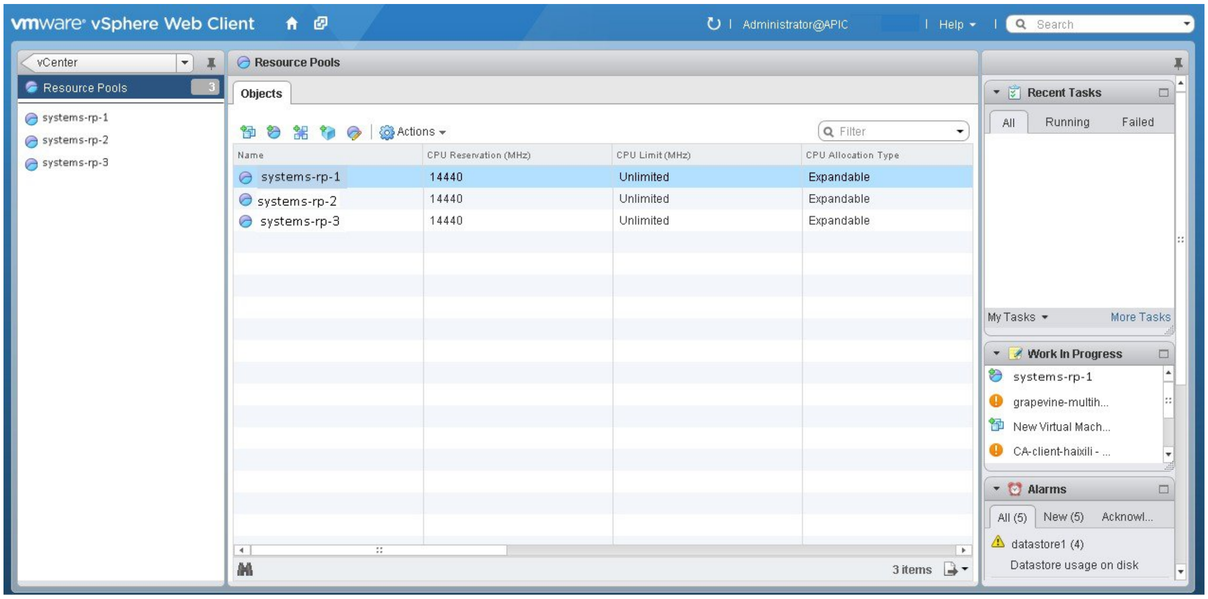
There are three steps to get started with your virtual infrastructure:

1. Create a datacenter
2. Add hosts to the datacenter
3. Create virtual machines on the hosts

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.

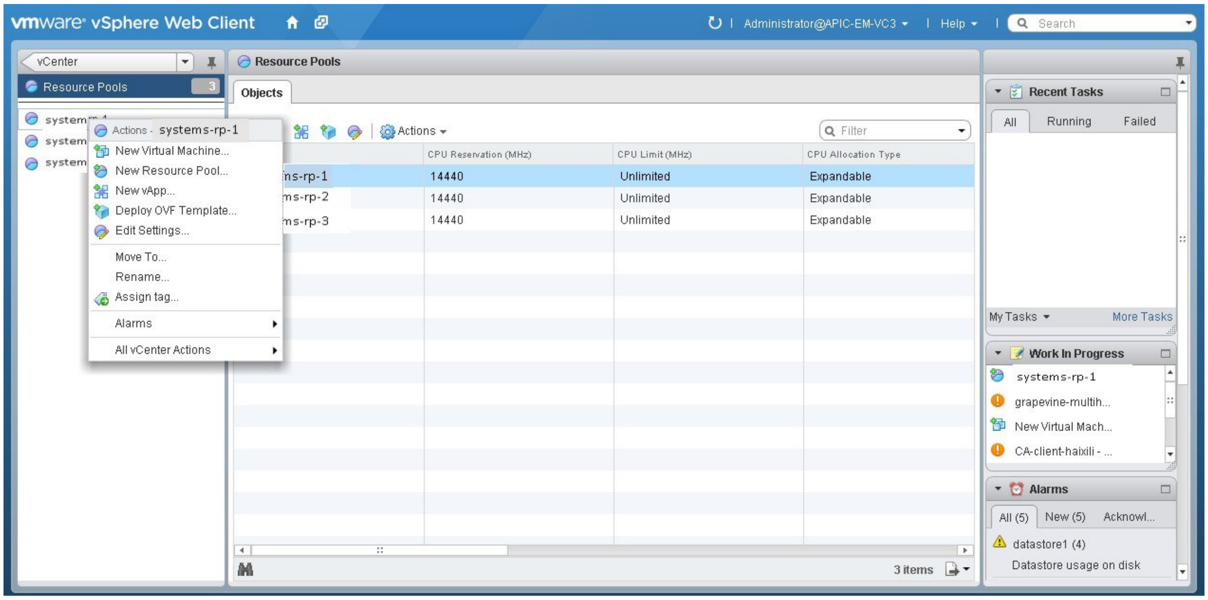
Figure 14: Resource Pools



Name	CPU Reservation (MHz)	CPU Limit (MHz)	CPU Allocation Type
systems-rp-1	14440	Unlimited	Expandable
systems-rp-2	14440	Unlimited	Expandable
systems-rp-3	14440	Unlimited	Expandable

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

Figure 15: New Virtual Machine

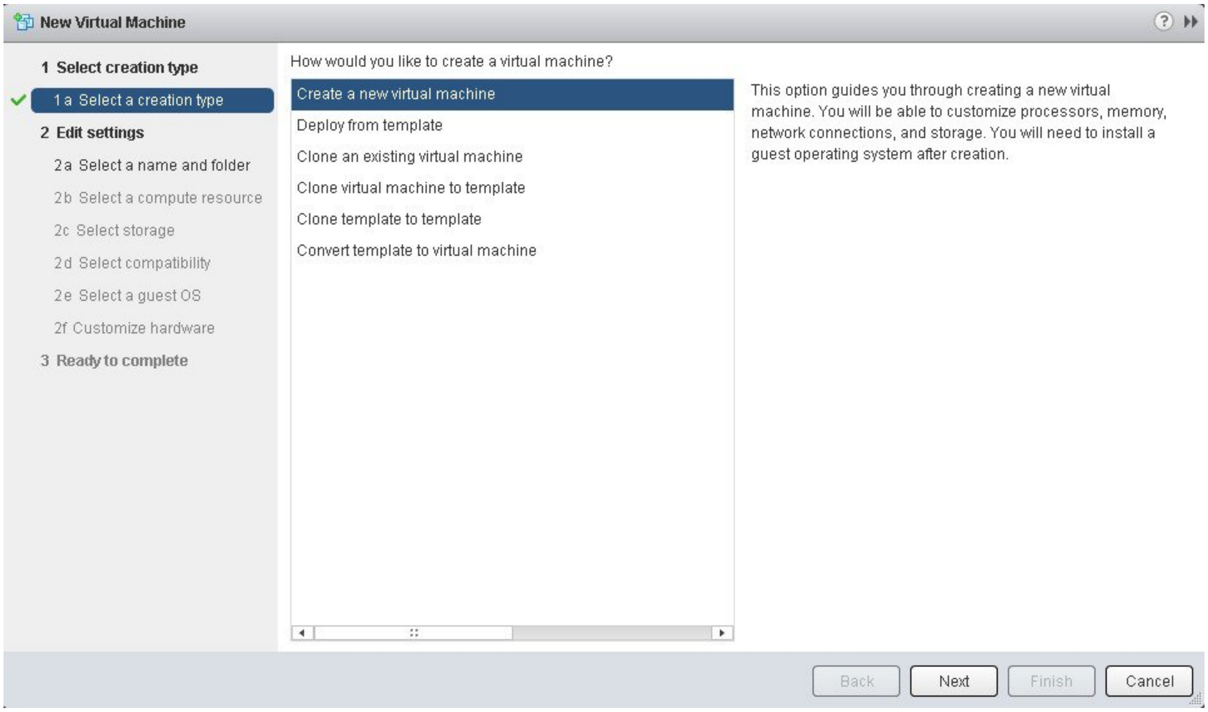


	CPU Reservation (MHz)	CPU Limit (MHz)	CPU Allocation Type
ms-rp-1	14440	Unlimited	Expandable
ms-rp-2	14440	Unlimited	Expandable
ms-rp-3	14440	Unlimited	Expandable

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 16: Select Creation Type

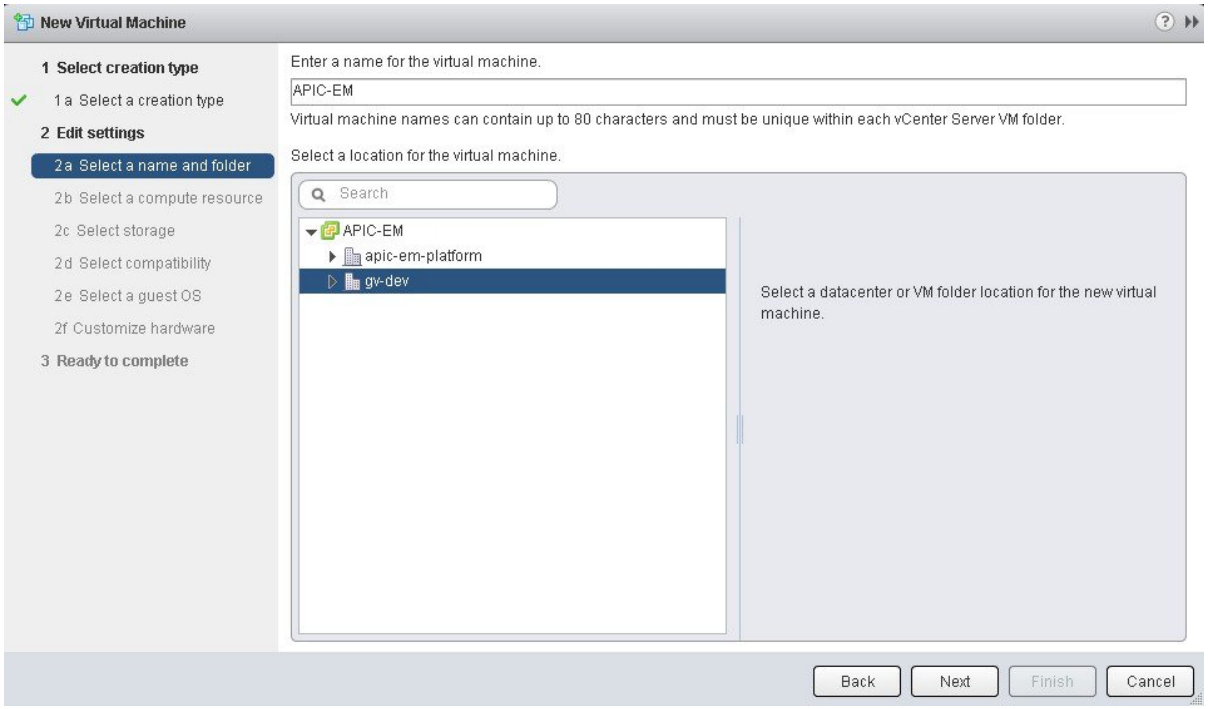

New Virtual Machine
1 Select creation type
✓ 1a Select a creation type
2 Edit settings
2a Select a name and folder
2b Select a compute resource
2c Select storage
2d Select compatibility
2e Select a guest OS
2f Customize hardware
3 Ready to complete
How would you like to create a virtual machine?
Create a new virtual machine
Deploy from template
Clone an existing virtual machine
Clone virtual machine to template
Clone template to template
Convert template to virtual machine
Back
Next
Finish
Cancel

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.

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 17: Select Name and Folder



New Virtual Machine

Enter a name for the virtual machine.

APIC-EM

Virtual machine names can contain up to 80 characters and must be unique within each vCenter Server VM folder.

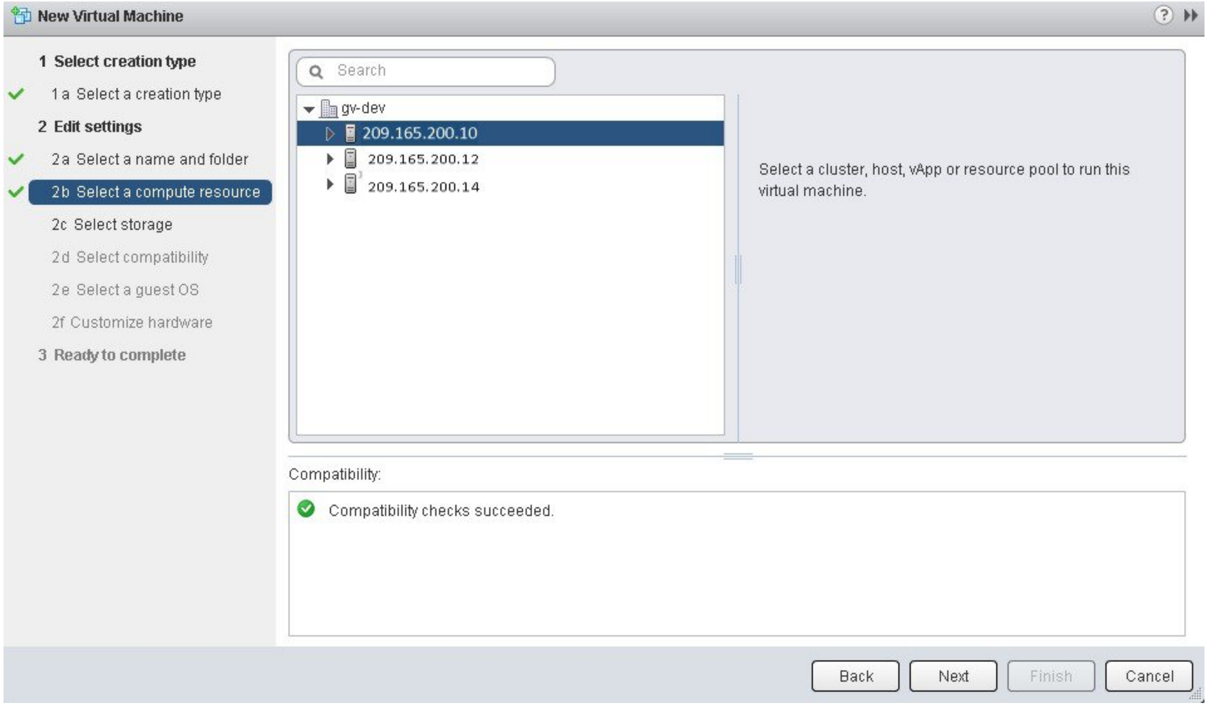
Select a location for the virtual machine.

Select a datacenter or VM folder location for the new virtual machine.

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 18: Select Computer Resource



Select a cluster, host, vApp or resource pool to run this virtual machine.

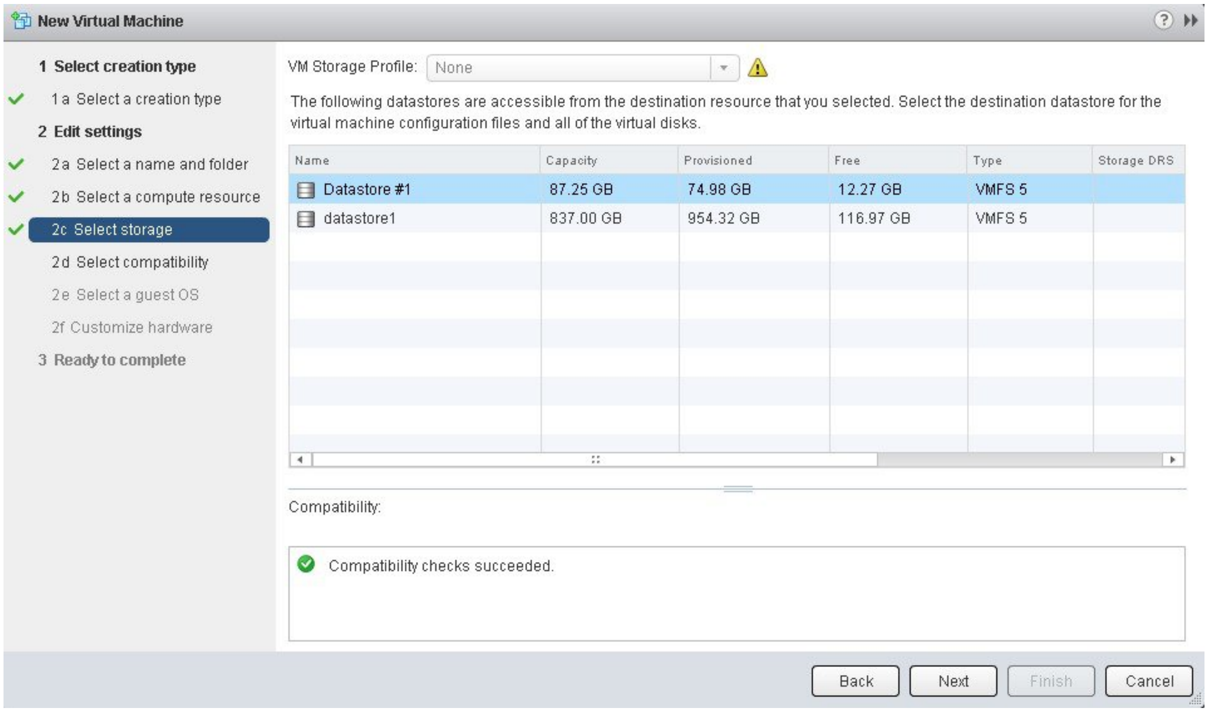
Compatibility:

Compatibility checks succeeded.

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

Step 9 Click **2c Select storage**.
Select a datastore for your virtual machine.

Figure 19: Select Storage



VM Storage Profile: None

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Provisioned	Free	Type	Storage DRS
Datastore #1	87.25 GB	74.98 GB	12.27 GB	VMFS 5	
datastore1	837.00 GB	954.32 GB	116.97 GB	VMFS 5	

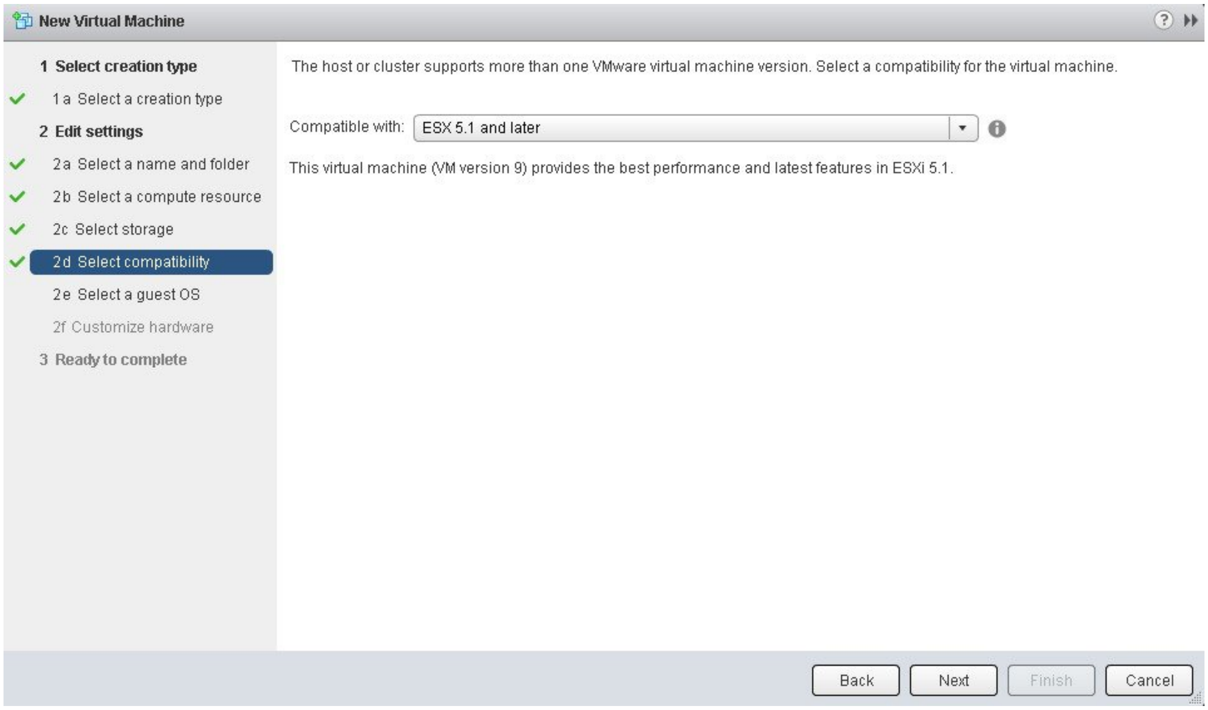
Compatibility:

Compatibility checks succeeded.

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 20: Select Compatibility



The host or cluster supports more than one VMware virtual machine version. Select a compatibility for the virtual machine.

Compatible with: ESX 5.1 and later

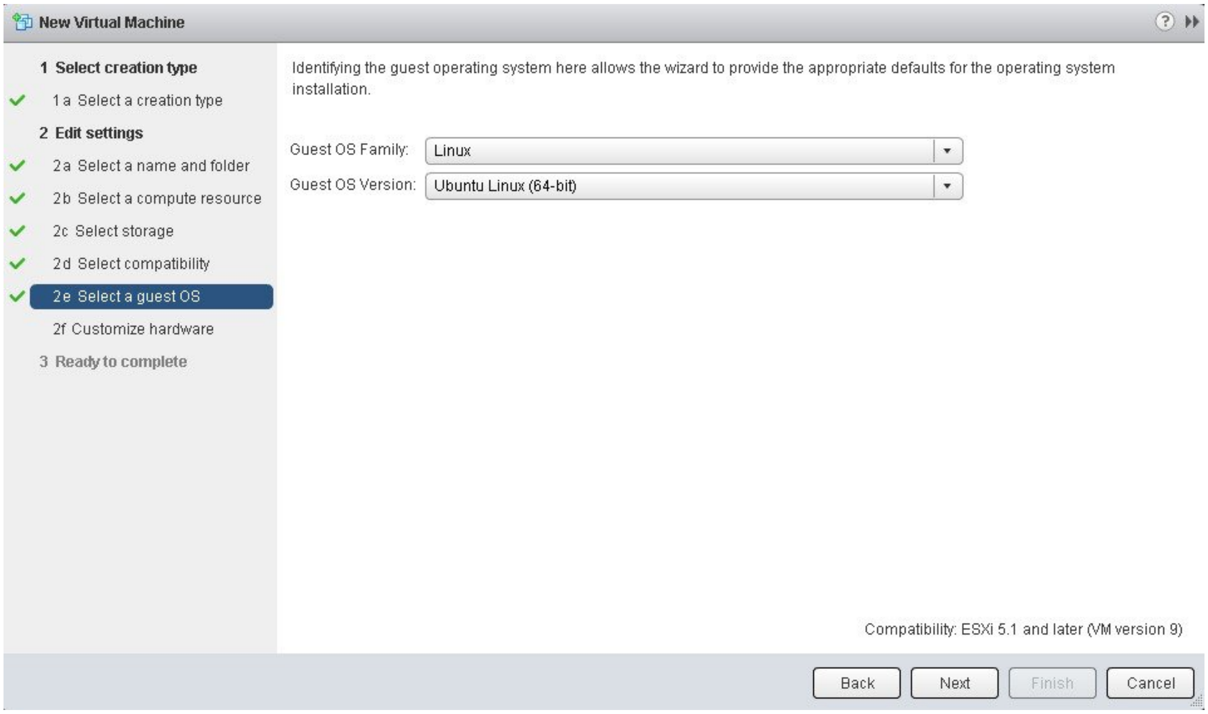
This virtual machine (VM version 9) provides the best performance and latest features in ESXi 5.1.

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 21: Select Guest OS



Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Guest OS Family: Linux

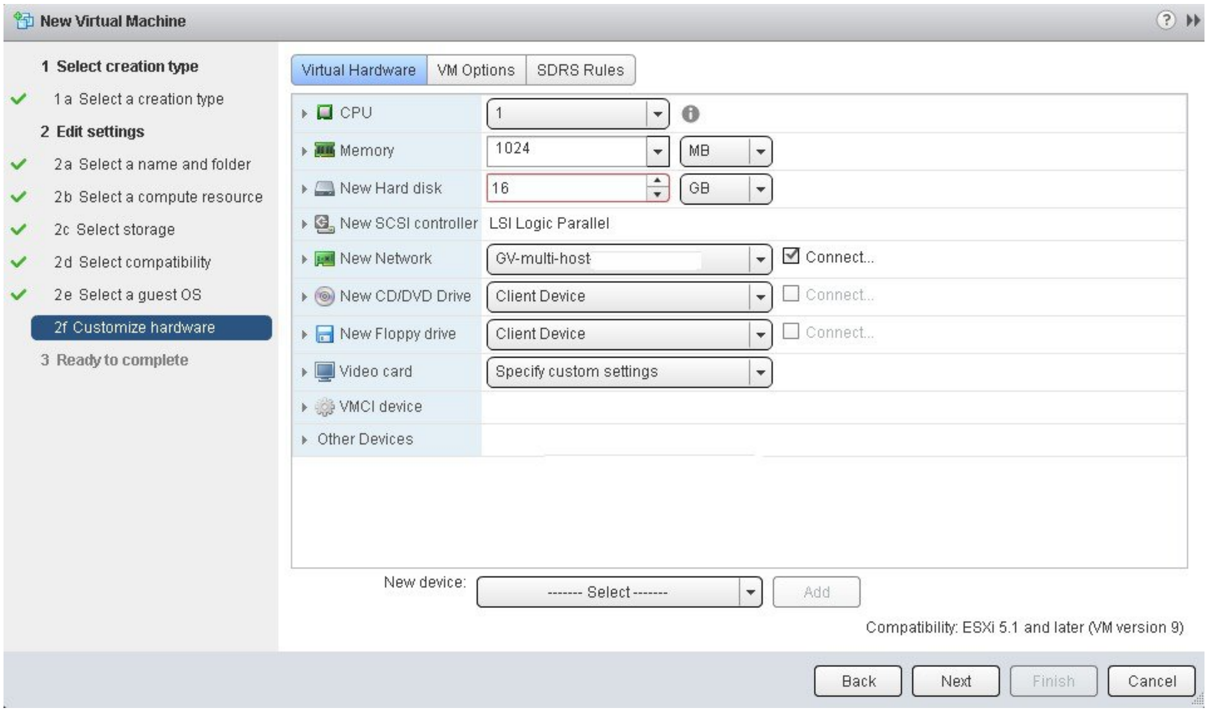
Guest OS Version: Ubuntu Linux (64-bit)

Compatibility: ESXi 5.1 and later (VM version 9)

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

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

Figure 22: Customize Hardware



New Virtual Machine

1 Select creation type
✓ 1a Select a creation type
2 Edit settings
✓ 2a Select a name and folder
✓ 2b Select a compute resource
✓ 2c Select storage
✓ 2d Select compatibility
✓ 2e Select a guest OS
2f Customize hardware
3 Ready to complete

Virtual Hardware | VM Options | SDRS Rules

CPU	1		
Memory	1024	MB	
New Hard disk	16	GB	
New SCSI controller	LSI Logic Parallel		
New Network	GV-multi-host		☑ Connect...
New CD/DVD Drive	Client Device		□ Connect...
New Floppy drive	Client Device		□ Connect...
Video card	Specify custom settings		
VMCI device			
Other Devices			

New device: ------- Select ------- Add

Compatibility: ESXi 5.1 and later (VM version 9)

Back Next Finish Cancel

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 the configure the location of the ISO file in the **File** window.

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 deploy the controller by following the configuration wizard prompts.

For information about the deployment process and configuration wizard options, see Chapter 4 in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*, and the following sections:

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

CHAPTER 5

Managing Administrator Accounts

This chapter describes the two types of administrator accounts in Cisco APIC-EM, their privileges, and how to create these accounts.

Admin User Right Differences

The username 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 setup 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 guides for detailed information about the above supported controller GUI operations:

- *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*
- *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration 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 Configuration Guide* for more information.

CHAPTER 6

Performing Post-Installation Tasks

This chapter describes several tasks that you must perform after successfully completing the installation and configuration of the Cisco APIC-EM.

Accessing Cisco APIC-EM Using a Web Browser

Cisco APIC-EM series appliances support a web interface using the following HTTPS-enabled browsers:

- Google Chrome—version 50.0 or later
- Mozilla Firefox—version 46.0 or later

Administrator Lockout Following Failed Login Attempts

If you enter an incorrect password for your specified administrator user ID enough 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

When you log in to the Cisco APIC-EM web-based interface for the first time, you must use only the supported HTTPS-enabled browsers listed in the previous section. After you have installed Cisco APIC-EM as described in this guide, you can log in to the Cisco APIC-EM web-based interface.

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.

What to Do Next

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

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

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

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 a License

See Appendix D, Cisco APIC-EM Licenses for information about Cisco APIC-EM and licenses.

Installing Certificates

See Chapter 5, Configuring the Cisco APIC-EM Settings, in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for information about installing certificates.

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.

Note

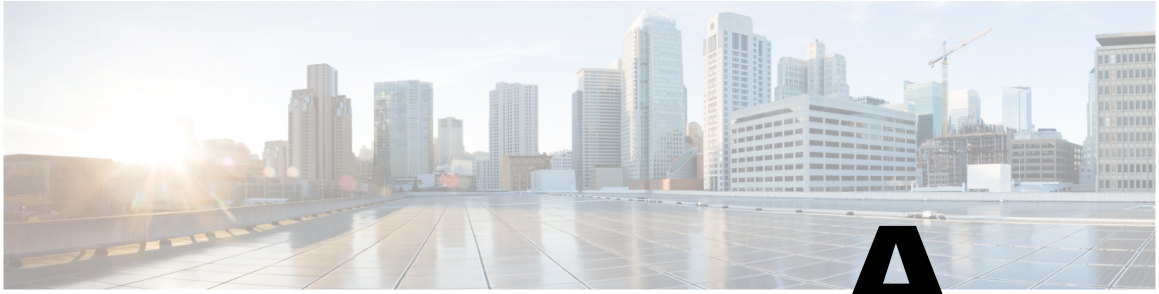
At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message appears.

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, *Configuring Cisco APIC-EM as a Multi-Host Cluster Using the Wizard* in the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide* for information about this process.

Configuring the Cisco APIC-EM

By using the Cisco APIC-EM graphical user interface menus and options, you can configure the Cisco APIC-EM to suit your requirements:

- For details on configuring the controller for your network devices (including configuring Discovery, Path Trace, and EasyQoS), as well as other features, menus, and options, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*.
- For details on configuring the controller settings (including discovery credentials, certificates, trust pools, and SNMP values), as well as other features, see the *Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide*.
- For the most current information about this release, see the *Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module*.



APPENDIX A

Installing the Cisco APIC-EM Series Appliance in a Rack

This appendix describes how to install the Cisco APIC-EM appliance in a rack.

Note Before you install, operate, or service a Cisco APIC-EM series appliance, review the Regulatory Compliance and Safety Information for Cisco UCS C-Series Servers for important safety information.

IMPORTANT SAFETY INSTRUCTIONS

Warning **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

Unpacking and Inspecting 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

What to Do Next

Prepare for the appliance installation.

Preparing for Appliance Installation

This section provides information about preparing for the Cisco APIC-EM series appliance 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 Cisco APIC-EM Appliance Specifications.
- 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 Cisco APIC-EM Appliance Specifications. If available, you can use an uninterruptible power supply (UPS) to protect against power failures.

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).

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.

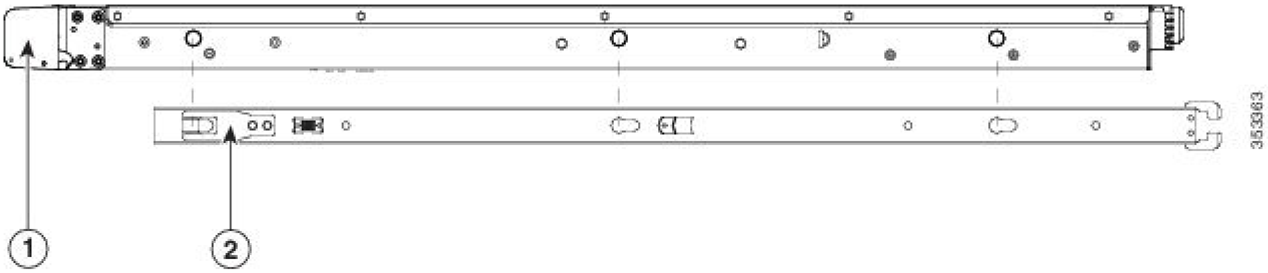
Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety: This unit should be mounted at the bottom of the rack if it is the only unit in the 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.

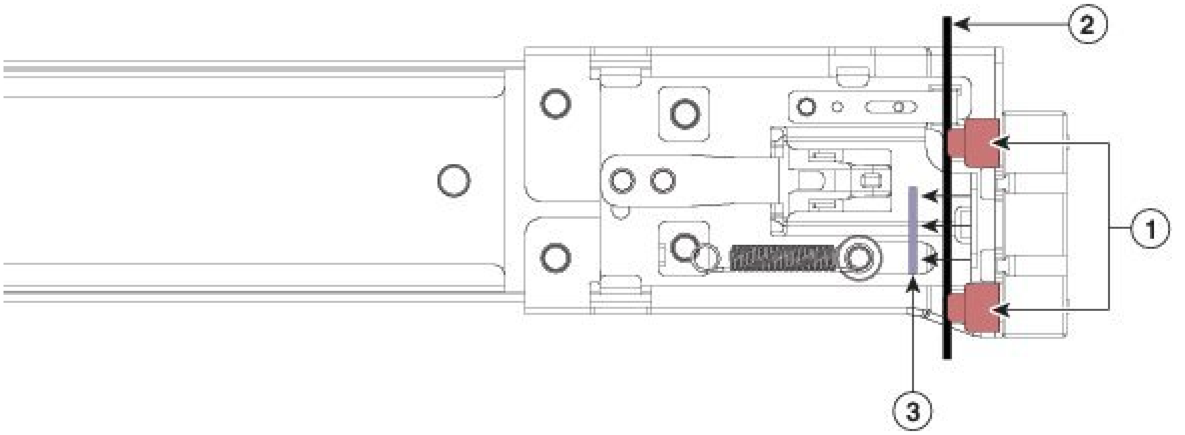
Figure 23: Attaching Inner Rail to Side of Server



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 24: 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:

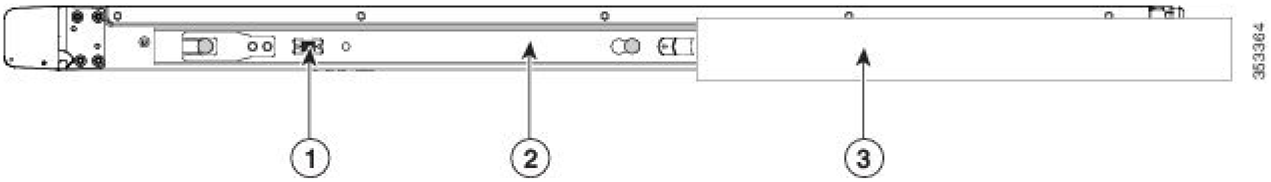
Caution This server can weigh up to 67 pounds (59 kilograms) when fully loaded with components. We recommend that you use a minimum of two people or a mechanical lift when lifting the server. Attempting this procedure alone could result in personal injury or equipment damage.

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 25: 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.

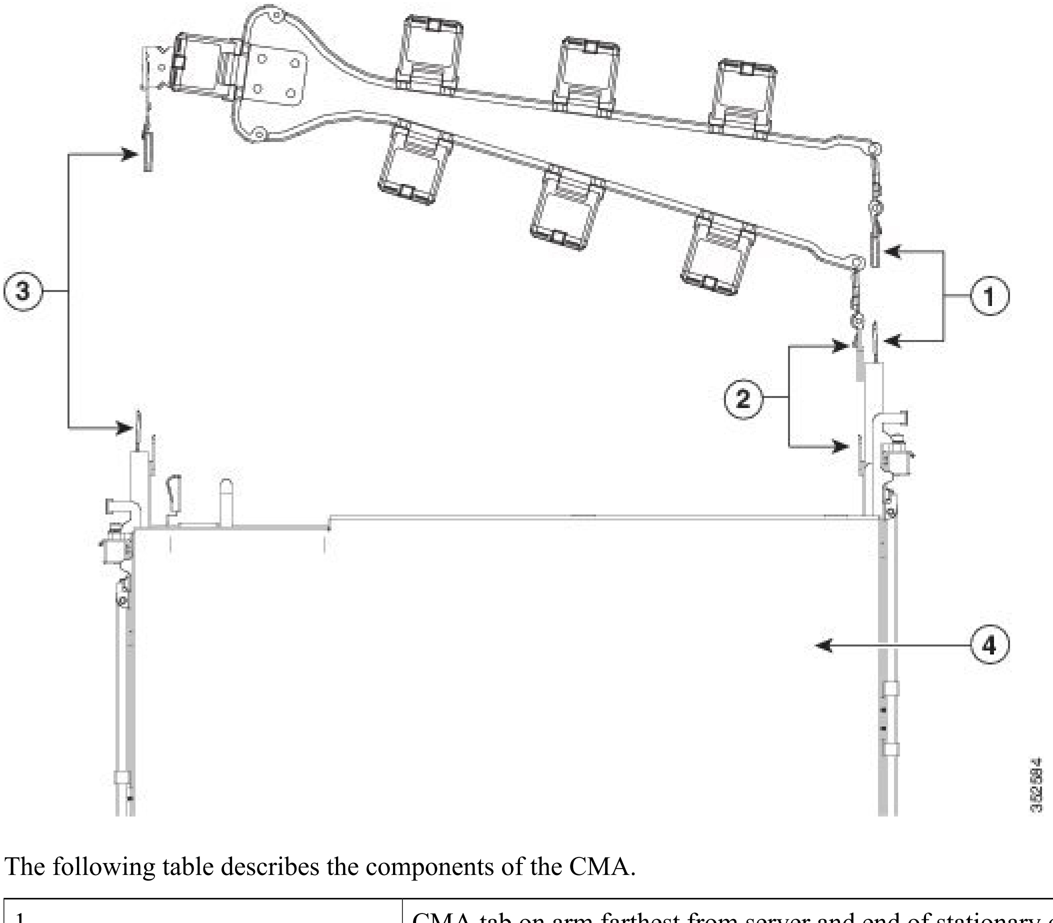
Step 2 Slide the CMA tab that is closest to the server over the end of the inner rail that is attached to the server (see the figure below). Slide the tab over the end of the rail until it clicks and locks.

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 26: 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)

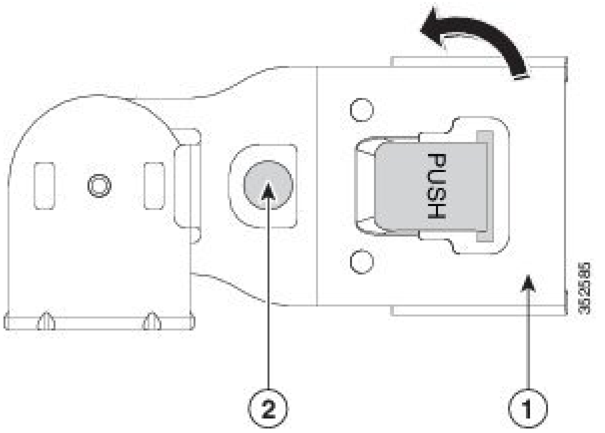
The following procedure describes how to reverse the cable management arm.

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 27: 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 13
- Using CIMC to Configure a Cisco APIC-EM Series Appliance, on page 20

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 topics 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 6: 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.
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.

LED Name	State
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.
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 7: 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.
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.

APPENDIX B

Cisco APIC-EM Appliance Specifications

This appendix lists the technical specifications for the Cisco APIC-EM series appliance.

Physical Specifications

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

Table 8: 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 appliance.

Table 9: 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 options 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.

Related Topics

770 W AC Power Supply, on page 67

770 W AC Power Supply

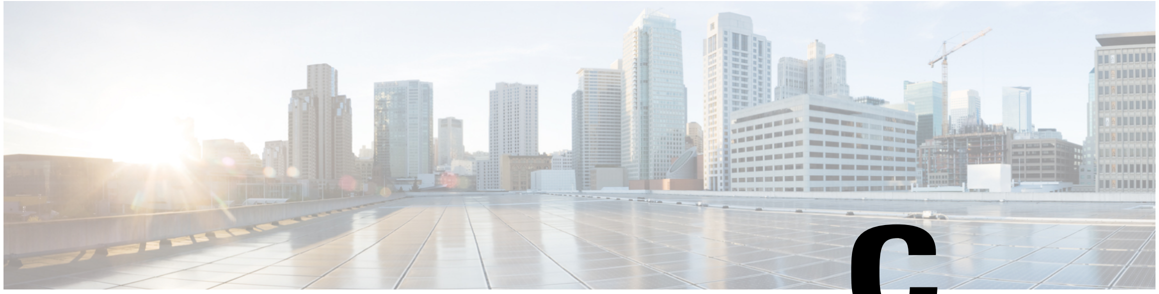
The following table lists the specifications for each 770 W AC power supply (Cisco part number UCSC-PSU1-770W).

Table 10: 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

Related Topics

Power Specifications, on page 66



APPENDIX C

Cisco APIC-EM Appliance Port Reference

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 ports 22 and 14141. For example, you can configure a proxy gateway or secure subnets to access these ports.

Table 11: Cisco APIC-EM Incoming Traffic Port Reference

Port Number	Permitted Traffic	Protocol (TCP or UDP)
22	SSH	TCP
67	bootps	UDP
80	HTTP	TCP
123	NTP	UDP
162	SNMP	UDP
443 [2]	HTTPS	TCP

Port Number	Permitted Traffic	Protocol (TCP or UDP)
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
14141	Grapevine APIs	TCP
16026	SCEP	TCP

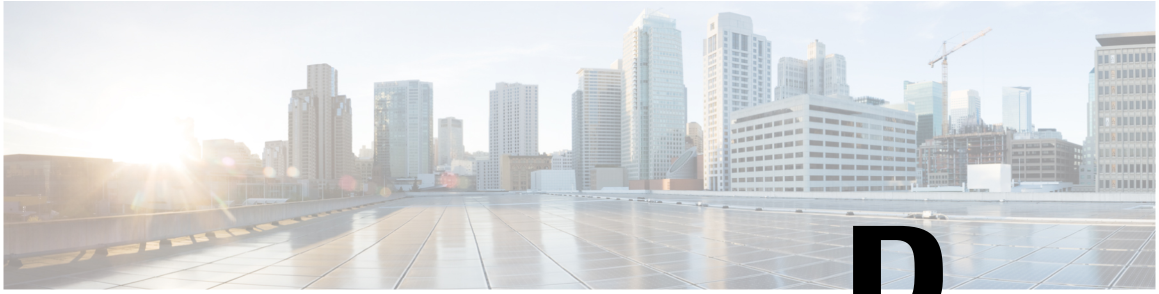
[2] You can configure the TLS version for this port using the Cisco APIC-EM. For more information, see the Cisco APIC-EM Deployment Guide.

Table 12: 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

Port Number	Permitted Traffic	Protocol (TCP or 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 APIC-EM Deployment Guide.



APPENDIX D

Cisco APIC-EM Licenses

Cisco APIC-EM Licensing

The following are the licensing requirements for Cisco APIC-EM and its applications (apps):

- Cisco APIC-EM controller software and its basic apps (for example, Network PnP, Inventory, Topology, and EasyQoS):
    - No fee-based license is required. The controller software and basic apps are offered at no cost to the user.
    - You can download the controller software (ISO Image) and run it on bare-metal Cisco UCS servers or run the ISO image on a virtual machine in a VMware ESXi environment. In both cases, you need to ensure the required CPU, memory, and storage resources are available.
- Solution apps (for example, IWAN and any similar Cisco-developed solution app):
    - A per-device license is required to run the solution apps.
    - The solution apps licenses can only be acquired by purchasing Cisco® Enterprise Management 3.x device licenses, which also include the Cisco Prime™ Infrastructure licenses. The process for acquiring Cisco Prime Infrastructure 3.x device licenses is explained in the Cisco Enterprise Management Ordering Guide:

      Cisco Enterprise Management 3.x, Prime Infrastructure 3. x APIC-EM Ordering and Licensing Guides

Note The same license-acquisition process will also provide you with the right-to-use (RTU) licenses for APIC-EM solution apps. RTU licenses do not involve license files.

Cisco APIC-EM Technical Support

The following Cisco APIC-EM technical support options are provided:

- Cisco APIC-EM hardware appliance:

  Hardware support is provided through the Cisco SMARTnet® Service.

- Cisco APIC-EM controller, basic apps, and services:

  Cisco® TAC support is offered at no additional cost, if you have SMARTnet on any Cisco networking device.

- Cisco APIC-EM solutions apps and services:

  TAC support is offered at no additional cost, if you have a SWSS (maintenance contract) on Cisco® Enterprise Management 3.x device licenses.

INDEX