CLI Configuration Guide for Cisco UCS E-Series Servers Integrated Management Controller, Release 1.0

First Published: September 07, 2012

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

Text Part Number: OL-26443-01

CONTENTS

Preface

Preface ix

Audience ix

Organization ix

Conventions xi

Related Documentation xii

Documentation Feedback xii

CHAPTER 1

Overview 1

Cisco UCS E-Series Servers Overview 1

Server Software 2

CIMC Overview 3

CIMC CLI 3

Command Modes 4

Command Mode Table 5

Completing or Exiting a Command 7

Command History 7

Committing, Discarding, and Viewing Pending Commands 7

Command Output Formats 8

Online Help for the CLI 9

CHAPTER 2

Installing the Server Operating System or Hypervisor 11

Operating System or Hypervisor Installation Methods 11

KVM Console 11

Installing an Operating System or Hypervisor Using the KVM Console 12

PXE Installation Servers 12

Installing an Operating System or Hypervisor Using a PXE Installation Server 12

Host Image Mapping 13

Mapping the Host Image 13
Installing Drivers for the Microsoft Windows Server 15
Unmapping the Host Image 15
Deleting the Host Image 16
Downloading the Customized VMware vSphere Hypervisor Image 16

CHAPTER 3

Managing the Server 19
Configuring the Server Boot Order 19
Resetting the Server 20
Shutting Down the Server 21
Managing Server Power 21
Powering On the Server 21
Powering Off the Server 22
Power Cycling the Server 22
Managing RAID 23
RAID Options 23
Configuring RAID 27
Making the Disk Drive Bootable 29
Modifying RAID Configuration 30
Enabling Auto Rebuild on the Storage Controller 30
Performing a Consistency Check on a Virtual Drive 31
Reconstructing the Virtual Drive Options 32
Reconstructing a Virtual Drive 35
Deleting RAID Configuration 36
Changing the Physical Drive State 37
Rebuilding the Physical Drive 38
Configuring BIOS Settings 39
Viewing BIOS Status 39
Installing BIOS Firmware from the TFTP Server 40
Configuring Advanced BIOS Settings 40
Configuring Server Management BIOS Settings 41
Clearing the BIOS CMOS 42
Clearing the BIOS Password 43
Restoring BIOS Defaults 43
Server BIOS Settings 43

CHAPTER 4 Viewing Server Properties 53
Viewing Server Properties 53
Viewing CPU Properties 54
Viewing Memory Properties 54
Viewing Power Supply Properties 55
Viewing Storage Properties 56
Viewing Storage Adapter Properties 56
Viewing Physical Drive Properties 57
Viewing Virtual Drive Properties 59
Viewing PCI Adapter Properties 59
Viewing Power Policy Statistics 60
Viewing Hard Drive Presence 61

CHAPTER 5 Viewing Server Sensors 63
Viewing the Fault Summary 63
Viewing Temperature Sensors 64
Viewing Voltage Sensors 64
Viewing Storage Sensors 65

CHAPTER 6 Managing Remote Presence 67
Managing the Virtual KVM 67
KVM Console 67
Configuring the Virtual KVM 68
Enabling the Virtual KVM 69
Disabling the Virtual KVM 69
Configuring Virtual Media 70
Managing Serial over LAN 71
Serial Over LAN 71
Guidelines and Restrictions for Serial Over LAN 71
Configuring Serial Over LAN 71
Launching Serial Over LAN 72

CHAPTER 7 Managing User Accounts 73
Configuring Local Users 73

Active Directory 74

Configuring the Active Directory Server 74

Configuring Active Directory in CIMC 76

Viewing User Sessions 77

Terminating a User Session 78

CHAPTER 8 **Configuring Network-Related Settings** 79

CIMC NIC Configuration 79

CIMC NICs 79

Configuring CIMC NICs 80

Configuring Common Properties 81

Configuring IPv4 82

Configuring the Server VLAN 83

Network Security Configuration 84

Network Security 84

Configuring Network Security 85

CHAPTER 9 **Configuring Communication Services** 87

Configuring HTTP 87

Configuring SSH 88

Configuring IPMI 89

IPMI Over LAN 89

Configuring IPMI over LAN 89

Configuring SNMP 90

SNMP 90

Configuring SNMP Properties 90

Configuring SNMP Trap Settings 91

Sending a Test SNMP Trap Message 92

CHAPTER 10 **Managing Certificates** 95

Managing the Server Certificate 95

Generating a Certificate Signing Request 95

Creating a Self-Signed Certificate 97

Uploading a Server Certificate 99

CHAPTER 11 Configuring Platform Event Filters 101

Platform Event Filters 101

Enabling Platform Event Alerts 101

Disabling Platform Event Alerts 102

Configuring Platform Event Filters 102

CHAPTER 12 CIMC Firmware Management 105

Overview of CIMC Firmware 105

Obtaining Software from Cisco Systems 106

Installing CIMC Firmware from the TFTP Server 107

Activating Installed CIMC Firmware 108

Viewing CIMC Information 109

CHAPTER 13 Viewing Logs 111

CIMC Log 111

Viewing the CIMC Log 111

Clearing the CIMC Log 112

Sending the CIMC Log to a Remote Server 112

System Event Log 113

Viewing the System Event Log 113

Clearing the System Event Log 114

CHAPTER 14 Server Utilities 115

Exporting Technical Support Data 115

Rebooting the CIMC 116

Resetting the CIMC to Factory Defaults 117

Exporting and Importing the CIMC Configuration 117

Exporting and Importing the CIMC Configuration 117

Exporting the CIMC Configuration 118

Importing a CIMC Configuration 119

CHAPTER 15 Diagnostic Tests 121

Diagnostic Tests Overview 121

Mapping the Diagnostics Image to the Host 122

Running Diagnostic Tests 123

Preface

This preface includes the following sections:

- Audience, page ix
- Organization, page ix
- Conventions, page xi
- Related Documentation, page xii
- Documentation Feedback, page xii

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Organization

This document includes the following chapters:

Chapter	Title	Description
Chapter 1	Overview	Describes the Cisco UCS E-Series Servers and the CIMC CLI .
Chapter 2	Installing the Server Operating System	Describes how to configure an operating system (OS) on the server.

Chapter	Title	Description
Chapter 3	Managing the Server	Describes how to configure the server boot device order, how to manage the server power, how to configure power policies, how to configure and manage RAID, and how to configure BIOS settings.
Chapter 4	Viewing Server Properties	Describes how to view the CPU, memory, power supply, storage, and PCI adapter properties of the server.
Chapter 5	Viewing Server Sensors	Describes how to view the fault, temperature, voltage, and storage sensors.
Chapter 6	Managing Remote Presence	Describes how to configure and manage the virtual KVM, virtual media, and the serial over LAN connection.
Chapter 7	Managing User Accounts	Describes how to add or modify user accounts, how to configure Active Directory to authenticate users, and how to manage user sessions.
Chapter 8	Configuring Network-Related Settings	Describes how to configure network interfaces, network settings, and network security.
Chapter 9	Configuring Communication Services	Describes how to configure server management communication by HTTP, SSH, IPMI, and SNMP.
Chapter 10	Managing Certificates	Describes how to generate, upload, and manage server certificates.
Chapter 11	Configuring Platform Event Filters	Describes how to configure and manage platform event filters.
Chapter 12	CIMC Firmware Management	Describes how to obtain, install, and activate firmware images.
Chapter 13	Viewing Logs	Describes how to view, export, and clear CIMC and system event log messages.
Chapter 14	Server Utilities	Describes how to export support data, how to export and import the server configuration, how to reset the server configuration to factory defaults, and how to reboot the management interface.
Chapter 15	Diagnostic Tests	Describes how to run diagnostic tests.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands, keywords, GUI elements, 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 that the system displays appear in `courier` font.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
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.

Note Means *reader take note*.

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

Caution Means *reader be careful*. In this situation, you might perform an action 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 Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.

Related Documentation

- Documentation Guide for Cisco UCS E-Series Servers—Provides links to all E-Series Server documentation
- *Release Notes for Cisco UCS E-Series Servers, Release 1.0*
- *Getting Started Guide for Cisco UCS E-Series Servers, Release 1.0*
- *Hardware Installation Guide for Cisco UCS E-Series Servers*
- *Cisco Network Modules, Server Modules, and Interface Cards Regulatory Compliance and Safety Information*
- *GUI Configuration Guide for Cisco UCS E-Series Servers Integrated Management Controller, Release 1.0*
- *CLI Configuration Guide for Cisco UCS E-Series Servers Integrated Management Controller, Release 1.0*
- *Troubleshooting Guide for Cisco UCS E-Series Servers*
- *Open Source Used in Cisco UCS E-Series Servers, Release 1.0*

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to ucs-docfeedback@external.cisco.com. We appreciate your feedback.

CHAPTER 1

Overview

This chapter includes the following sections:

- Cisco UCS E-Series Servers Overview, page 1
- Server Software, page 2
- CIMC Overview, page 3
- CIMC CLI, page 3

Cisco UCS E-Series Servers Overview

The Cisco UCS E-Series Servers (E-Series Servers) are the next generation of Cisco UCS Express servers. E-Series Servers are a family of size, weight, and power efficient blade servers that are housed within the Generation 2 Cisco Integrated Services Routers (ISR G2). These servers provide a general purpose compute platform for branch-office applications deployed either as bare-metal on operating systems, such as Microsoft Windows or Linux; or as virtual machines on hypervisors, such as VMware vSphere Hypervisor™, Microsoft Hyper-V, or Citrix XenServer.

E-Series Servers reside in the Cisco 2900 series or 3900 series ISR G2. The following E-Series Servers are supported:

- UCS-E140S—Single-wide E-Series Server
- UCS-E140D—Double-wide E-Series Server, 4 core CPU
- UCS-E160D—Double-wide E-Series Server, 6 core CPU
- UCS-E140DP—Double-wide E-Series Server, 4 core CPU, with PCIe
- UCS-E160DP—Double-wide E-Series Server, 6 core CPU, with PCIe

Note For information about the maximum number of E-Series Servers that can be installed per ISR G2, see the "Server Hardware" section in the *Getting Started Guide for Cisco UCS E-Series Servers*.

Server Software

E-Series Servers require three major software systems:

- CIMC Firmware
- BIOS Firmware
- Operating System or Hypervisor

CIMC Firmware

Cisco Integrated Management Controller (CIMC) is a separate management module built into the motherboard. A dedicated ARM-based processor, separate from the main server CPU, runs the CIMC firmware. The system ships with a running version of the CIMC firmware. You can update the CIMC firmware, but no initial installation is needed.

CIMC is the management service for the E-Series Servers. You can use a web-based GUI or SSH-based CLI to access, configure, administer, and monitor the server.

BIOS Firmware

BIOS initializes the hardware in the system, discovers bootable devices, and boots them in the provided sequence. It boots the operating system and configures the hardware for the operating system to use. BIOS manageability features allow you to interact with the hardware and use it. In addition, BIOS provides options to configure the system, manage firmware, and create BIOS error reports.

The system ships with a running version of the BIOS firmware. You can update the BIOS firmware, but no initial installation is needed.

Operating System or Hypervisor

The main server CPU runs on an operating system, such as Microsoft Windows or Linux; or on a Hypervisor. You can purchase an E-Series Server with pre-installed Microsoft Windows Server or VMware vSphere Hypervisor™, or you can install your own platform.

The following platforms have been tested on the E-Series Servers:

- Microsoft Windows:
    - Windows Server 2008 R2 Standard 64-bit
    - Windows Server 2008 R2 Enterprise 64-bit
- Linux:
    - Red Hat Enterprise Linux 6.2
    - SUSE Linux Enterprise 11, service pack 2
    - Oracle Enterprise Linux 6.0, update 2
- Hypervisor:
    - VMware vSphere Hypervisor™ 5.0, update 1
    - Hyper-V (Windows 2008 R2)

- ◦ Citrix XenServer 6.0

CIMC Overview

The Cisco Integrated Management Controller (CIMC) is the management service for the E-Series Servers. CIMC runs within the server. You can use a web-based GUI or the SSH-based CLI to access, configure, administer, and monitor the server.

You can use CIMC to perform the following server management tasks:

- Power on, power off, power cycle, reset and shut down the server
- Configure the server boot order
- Manage RAID levels
- View server properties and sensors
- Manage remote presence
- Create and manage local user accounts, and enable remote user authentication through the Active Directory
- Configure network-related settings, including NIC properties, IPv4, VLANs, and network security
- Configure communication services, including HTTP, SSH, IPMI Over LAN, and SNMP
- Manage certificates
- Configure platform event filters
- Update CIMC firmware
- Update BIOS firmware
- Install the host image from an internal repository
- Monitor faults, alarms, and server status
- Collect technical support data in the event of server failure

Almost all tasks can be performed in either the GUI interface or CLI interface, and the results of tasks performed in one interface are displayed in another. However, you cannot do the following:

- Cannot use the CIMC GUI to invoke the CIMC CLI
- Cannot view a command that has been invoked through CIMC CLI in the CIMC GUI
- Cannot generate CIMC CLI output from the CIMC GUI

CIMC CLI

The CIMC CLI is a command-line management interface for E-Series Servers. You can launch the CIMC CLI in the following ways:

- By the serial port.

- Over the network by SSH.
- From the router by using the **ucse** *slot* **session imc** command.

A CLI user can have one of the three roles: admin, user (can control but cannot configure), and read-only.

Command Modes

The CLI is organized into a hierarchy of command modes, with the EXEC mode being the highest-level mode of the hierarchy. Higher-level modes branch into lower-level modes. You use the **scope** command to move from higher-level modes to modes in the next lower level , and the **exit** command to move up one level in the mode hierarchy. The **top** command returns to the EXEC mode.

Note Most command modes are associated with managed objects. The **scope** command does not create managed objects and can only access modes for which managed objects already exist.

Each mode contains a set of commands that can be entered in that mode. Most of the commands available in each mode pertain to the associated managed object. Depending on your assigned role, you may have access to only a subset of the commands available in a mode; commands to which you do not have access are hidden.

The CLI prompt for each mode shows the full path down the mode hierarchy to the current mode. This helps you to determine where you are in the command mode hierarchy and can be an invaluable tool when you need to navigate through the hierarchy.

Command Mode Table

The following table lists the first four levels of command modes, the commands used to access each mode, and the CLI prompt associated with each mode.

Mode Name	Command to Access	Mode Prompt
EXEC	**top** command from any mode	#
bios	**scope bios** command from EXEC mode	/bios #
advanced	**scope advanced** command from bios mode	/bios/advanced #
main	**scope main** command from bios mode	/bios/main #
server-management	**scope server-management** command from bios mode	/bios/server-management #
certificate	**scope certificate** command from EXEC mode	/certificate #
chassis	**scope chassis** command from EXEC mode	/chassis #
dimm-summary	**scope dimm-summary** *index* command from chassis mode	/chassis/dimm-summary #
storageadapter	**scope storageadapter** *slot* command from chassis mode	/chassis/storageadapter #
physical-drive	**scope physical-drive** *drive-number* command from storageadapter mode	/chassis/storageadapter /physical-drive #
virtual-drive	**scope virtual-drive** *drive-number* command from storageadapter mode	/chassis/storageadapter /virtual-drive #
cimc	**scope cimc** command from EXEC mode	/cimc #
import-export	**scope import-export** command from cimc mode	/cimc/import-export #
log	**scope log** command from cimc mode	/cimc/log #
server		

Mode Name	Command to Access	Mode Prompt
	scope server *index* command from log mode	/cimc/log/server #
`network`	**scope network** command from cimc mode	/cimc/network #
`ipblocking`	**scope ipblocking** command from network mode	/cimc/network/ipblocking #
`tech-support`	**scope tech-support** command from cimc mode	/cimc/tech-support #
`fault`	**scope fault** command from EXEC mode	/fault #
`pef`	**scope pef** command from fault mode	/fault/pef #
`http`	**scope http** command from EXEC mode	/http #
`ipmi`	**scope ipmi** command from EXEC mode	/ipmi #
`kvm`	**scope kvm** command from EXEC mode	/kvm #
`ldap`	**scope ldap** command from EXEC mode	/ldap #
`power-cap`	**scope power-cap** command from EXEC mode	/power-cap #
`remote-install`	**scope remote-install** command from EXEC mode	/remote-install #
`sel`	**scope sel** command from EXEC mode	/sel #
`sensor`	**scope sensor** command from EXEC mode	/sensor #
`snmp`	**scope snmp** command from EXEC mode	/snmp #
`trap-destination`	**scope trap-destination** command from snmp mode	/snmp/trap-destination #
`sol`		/sol #

Mode Name	Command to Access	Mode Prompt
	scope sol command from EXEC mode	
`ssh`	**scope ssh** command from EXEC mode	/ssh #
`user`	**scope user** *user-number* command from EXEC mode	/user #
`user-session`	**scope user-session** *session-number* command from EXEC mode	/user-session #
`vmedia`	**scope vmedia** command from EXEC mode	/vmedia #

Completing or Exiting a Command

You can use the Tab key in any mode to complete a command. Partially typing a command name and pressing Tab causes the command to be displayed in full or to the point where another keyword must be chosen or an argument value must be entered.

When you are inside a scope, the **exit** command allows you to move one level up. For example, if the scope is **/chassis/dimm-summary**, and you enter **exit**, the scope will move one level up to **/chassis**.

Command History

The CLI stores all commands used in the current session. You can step through the previously used commands by using the Up Arrow or Down Arrow keys. The Up Arrow key steps to the previous command in the history, and the Down Arrow key steps to the next command in the history. If you get to the end of the history, pressing the Down Arrow key does nothing.

All commands in the history can be entered again by simply stepping through the history to recall the desired command and pressing Enter. The command is entered as if you had manually typed it. You can also recall a command and change it before you enter it.

Committing, Discarding, and Viewing Pending Commands

When you enter a configuration command in the CLI, the command is not applied until you enter the **commit** command. Until committed, a configuration command is pending and can be discarded by entering a **discard** command. When any command is pending, an asterisk (*) appears before the command prompt. The asterisk disappears when you enter the **commit** command, as shown in this example:

```
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# commit
Server /kvm #
```

You can accumulate pending changes in multiple command modes and apply them together with a single **commit** command. You can view the pending commands by entering the **show configuration pending** command in any command mode.

Note Committing multiple commands together is not an atomic operation. If any command fails, the successful commands are applied despite the failure. Failed commands are reported in an error message.

Caution The **commit** command must be used to commit changes that are made within the same scope. If you try to use the **commit** command to submit changes made in a different scope, you will get an error, and you will have to redo and recommit those changes.

Command Output Formats

Most CLI **show** commands accept an optional **detail** keyword that causes the output information to be displayed as a list rather than as a table.

Depending on how you want the output information of the **detail** command to be displayed, use one of the following commands:

- **set cli output default**—Default format for easy viewing. The command output is presented in a compact list.

  This example shows the command output in the default format:

  ```
  Server /chassis # set cli output default
  Server /chassis # show hdd detail
  Name HDD_01_STATUS:
      Status : present
  Name HDD_02_STATUS:
      Status : present
  Name HDD_03_STATUS:
      Status : present

  Server /chassis #
  ```

- **set cli output yaml**—YAML format for easy parsing by scripts. The command output is presented in the YAML Ain't Markup Language (YAML) data serialization language, delimited by defined character strings.

  This example shows the command output in the YAML format:

  ```
  Server /chassis # set cli output yaml
  Server /chassis # show hdd detail
  ---
      name: HDD_01_STATUS
      hdd-status: present

  ---
      name: HDD_02_STATUS
      hdd-status: present

  ---
      name: HDD_03_STATUS
      hdd-status: present

  ...
  ```

```
Server /chassis #
```

For detailed information about YAML, see http://www.yaml.org/about.html.

Online Help for the CLI

At any time, you can type the **?** character to display the options available at the current state of the command syntax. If you have not typed anything at the prompt, typing ? lists all available commands for the mode you are in. If you have partially typed a command, typing ? lists all available keywords and arguments available at your current position in the command syntax.

CHAPTER 2

Installing the Server Operating System or Hypervisor

This chapter includes the following sections:

- Operating System or Hypervisor Installation Methods, page 11
- KVM Console, page 11
- PXE Installation Servers, page 12
- Host Image Mapping, page 13

Operating System or Hypervisor Installation Methods

E-Series Servers support several operating systems and hypervisors. Regardless of the platform being installed, you can install it on your server using one of the following tools:

- KVM console
- PXE installation server
- Host image mapping

KVM Console

The KVM console is an interface accessible from CIMC that emulates a direct keyboard, video, and mouse connection to the server. The KVM console allows you to connect to the server from a remote location. Instead of using CD/DVD or floppy drives physically connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives. You can map any of the following to a virtual drive:

- CD/DVD or floppy drive on your computer
- Disk image files (ISO or IMG files) on your computer
- USB flash drive on your computer

You can use the KVM console to install an operating system or hypervisor on the server and to do the following:

- Access the BIOS setup menu by pressing **F2** during bootup.
- Access the CIMC Configuration Utility by pressing **F8** during bootup.
- Access the WebBIOS to configure RAID, by pressing the **Ctrl** and **H** keys during bootup.

Installing an Operating System or Hypervisor Using the KVM Console

Because the KVM console is operated only through the GUI, you cannot install an operating system or hypervisor using the CLI. To install a platform using the KVM console, follow the instructions in the "Installing an Operating System or Hypervisor Using the KVM Console" section of the *GUI Configuration Guide for Cisco UCS E-Series Servers*.

PXE Installation Servers

A Preboot Execution Environment (PXE) installation server allows a client to boot and install an operating system or hypervisor from a remote location. To use this method, a PXE environment must be configured and available on your LAN, typically a dedicated provisioning LAN. In addition, the server must be set to boot from the network. When the server boots, it sends a PXE request across the network. The PXE installation server acknowledges the request, and starts a sequence of events that installs the operating system or hypervisor on the server.

PXE servers can use installation disks, disk images, or scripts to install the operating system or hypervisor. Proprietary disk images can also be used to install the platform, additional components, or applications.

Note PXE installation is an efficient method for installing a platform on a large number of servers. However, considering that this method requires setting up a PXE environment, it might be easier to use another installation method.

Installing an Operating System or Hypervisor Using a PXE Installation Server

Before You Begin

- Verify that the server can be reached over a VLAN.

Note VMware vSphere Hypervisor™ requires a customized image. To download the customized image, see Downloading the Customized VMware vSphere Hypervisor Image .

Procedure

Step 1 Set the boot order to **PXE**.

Step 2 Reboot the server.
If a PXE install server is available on the VLAN, the installation process begins when the server reboots. PXE installations are typically automated and require no additional user input. Refer to the installation guide for the operating system or hypervisor being installed to guide you through the rest of the installation process.

What to Do Next

After the installation is complete, reset the LAN boot order to its original setting.

Host Image Mapping

The Host Image Mapping feature allows you to download, map, unmap, or delete a host image. Download a host image, such as a Microsoft Windows, Linux, or VMware from a remote FTP, FTPS, HTTP, or HTTPS server onto the CIMC internal repository, then map the image onto the virtual drive of a USB controller in the E-Series Server. After you map the image, set the boot order to make the virtual drive, in which the image is mounted, as the first boot device, and then reboot the server. The host image must have .iso as the file extension.

The Host Image Mapping feature also allows you to download and mount a diagnostics image. The diagnostics image must have .diag as the file extension.

Mapping the Host Image

Before You Begin

- Log into CIMC as a user with admin privileges.
- Obtain the host image file from the appropriate third-party.

Note VMware vSphere Hypervisor™ requires a customized image. To download the customized image, see Downloading the Customized VMware vSphere Hypervisor Image .

Note If you start an image update while an update is already in process, both updates will fail.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope remote-install**	Enters the remote install command mode.
Step 2	Server /remote-install # **download-image** {**ftp** | **ftps** | **http** | **https**} *server-ip-address path / filename* [**username** *username* **password** *password*]	Downloads the image from the specified remote server onto the CIMC internal repository. The host image must have .iso as the file extension. The remote server can be a FTP, FTPS, HTTP, or HTTPS server. If the remote server requires user authentication, you must add the username and password of the remote server. **Note** If the image file exceeds the size limit, an error message is displayed.
Step 3	(Optional) Server /remote-install # **show detail**	Displays the status of the image download.
Step 4	Server /remote-install # **map-image**	Mounts the image on a virtual drive of the USB controller. The virtual drive can be one of the following: • HDD—Hard disk drive • FDD—Floppy disk drive • CDROM—Bootable CD-ROM
Step 5	(Optional) Server /remote-install # **show detail**	Displays the status of the host image mapping.

This example maps the host image:

```
Server# scope remote-install
Server /remote-install # download-image ftp 10.20.34.56 pub/hostimage.iso
---
Server /remote-install # show detail
Host Image Info:
  Name: HostImage.iso
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Download Successful!!
Server /remote-install # map-image
---
status: ok
---
Server /remote-install # show detail
Host Image Info:
  Name: HostImage.iso
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Image mapped successfully!!
```

What to Do Next

Do the following:

1 Set the boot order to make the virtual drive in which the image is installed as the first boot device. See Configuring the Server Boot Order.

2 Reboot the server. If the image contains an answer file, the operating system installation is automated and the image is installed. Otherwise, the installation wizard displays. Follow the wizard steps to install the image.

3 If disk drives are not displayed after you install the operating system or hypervisor, you must install drivers. For instructions on how to install drivers on a Microsoft Windows Server, see Installing Drivers for the Microsoft Windows Server

4 After the installation is complete, reset the virtual media boot order to its original setting.

Installing Drivers for the Microsoft Windows Server

Note If you purchased E-Series Server Option 1 (E-Series Server without preinstalled operating system or hypervisor), and you installed your own version of the Microsoft Windows Server, you must install drivers.

Microsoft Windows operating system requires that you install three drivers:

- On-Board Network Drivers for Windows 2008 R2
- LSI Drivers (On-Board Hardware RAID Controller) for Windows 2008 R2
- Intel Drivers for Windows 2008 R2

If you have purchased a 10 Gigabit add-on card, you must also install the 10G PCIe Network Drivers for Windows 2008 R2.

Procedure

Step 1 Download the drivers from Cisco.com. See Obtaining Software from Cisco Systems.

Step 2 Copy the driver files into an USB flash drive.

Step 3 Install your own version of Microsoft Windows Server.
During the installation process, you will be prompted for the LSI Drivers.

Step 4 Plug the USB flash drive into the USB slot in the E-Series Server, and then install the LSI Drivers.

Step 5 After the Microsoft Windows Server installation is complete, install the On-Board Network Drivers (Broadcom) and the Intel Drivers.

Unmapping the Host Image

Before You Begin

Log into CIMC as a user with admin privileges.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope remote-install**	Enters the remote install command mode.
Step 2	Server /remote-install # **unmap-image**	Unmounts the image from the virtual drive of the USB controller.
Step 3	(Optional) Server /remote-install # **show detail**	Displays the status of the host image unmapping.

This example unmaps the host image:

```
Server# scope remote-install
Server /remote-install # unmap-image
Server /remote-install # show detail
Host Image Info:
  Name: HostImage.iso
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Image unmapped successfully!!
```

Deleting the Host Image

Before You Begin

Log into CIMC as a user with admin privileges.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope remote-install**	Enters the remote install mode.
Step 2	Server /remote-install # **delete-image**	Removes the image from the CIMC internal repository.

This example deletes the host image:

```
Server# scope remote-install
Server /remote-install # delete-image
```

Downloading the Customized VMware vSphere Hypervisor Image

Use this procedure to download the customized VMware vSpere Hypervisor™ image.

Procedure

Step 1 Navigate to https://my.vmware.com/web/vmware/login.
The VMware login page appears.

Step 2 Enter your VMware credentials, and then click **Log In**.
If you do not have an account with VMware, click **Register** to create a free account.

Step 3 Under the **Support Requests** pane, click **Knowledge Base**.

Step 4 In the **Search** field located on the top right corner, enter **ESXi-5.0.0-623860-custom-Cisco-2.0.1.6.iso**, and then click **Search**.

Step 5 From the **Search Results**, click **Download VMware View 5.1** to download the customized VMware vSpere Hypervisor™ image.

What to Do Next

Install the VMware vSpere Hypervisor™ image. For installation instructions, see Mapping the Host Image.

CHAPTER 3

Managing the Server

This chapter includes the following sections:

- Configuring the Server Boot Order, page 19
- Resetting the Server, page 20
- Shutting Down the Server, page 21
- Managing Server Power, page 21
- Managing RAID, page 23
- Configuring BIOS Settings, page 39

Configuring the Server Boot Order

Note Do not change the boot order while the host is performing BIOS power-on self test (POST).

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters bios command mode.
Step 2	Server /bios # **set boot-order** *device1*[,*device2*[,*device3* [,*device4*[,*device5*]]]]	Specifies the boot device options and order. You can select one or more of the following: • cdrom—Bootable CD-ROM • fdd—Floppy disk drive • hdd—Hard disk drive

	Command or Action	Purpose
		• pxe—PXE boot • efi—Extensible Firmware Interface
Step 3	Server /bios # **commit**	Commits the transaction to the system configuration.

The new boot order will be used on the next BIOS boot.

This example sets the boot order and commits the transaction:

```
Server# scope bios
Server /bios # set boot-order hdd,cdrom,fdd,pxe,efi
Server /bios *# commit
Server /bios #  show detail
BIOS:
    Boot Order: HDD,CDROM,FDD,PXE,EFI

Server /bios #
```

Resetting the Server

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **power hard-reset**	After a prompt to confirm, resets the server. **Note** • Power cycling the server is the same as pressing the physical power button to power off, and then power on the server. • Power hard-reset is the same as pressing the physical reset button on the server.

This example resets the server:

```
Server# scope chassis
Server /chassis # power hard-reset
This operation will change the server's power state.
Continue?[y|N]
```

Shutting Down the Server

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis mode.
Step 2	Server /chassis # **power shutdown**	After the prompt to confirm, shuts down the server.

This example shuts down the server:

```
Server# scope chassis
Server /chassis # power shutdown
This operation will change the server's power state.
Do you want to continue?[y|N]y
```

Managing Server Power

Powering On the Server

Note If the server was powered off other than through the CIMC, the server will not become active immediately when powered on. In this case, the server will enter standby mode until the CIMC completes initialization.

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **power on**	After the prompt to confirm, turns on the server power.

This example turns on the server:

```
Server# scope chassis
Server /chassis # power on
This operation will change the server's power state.
Continue?[y|N]y

Server /chassis # show
Power Serial Number Product Name   PID            UUID
----- ------------- -------------  -------------  ------------------------------------
on    FOC16161F1P   E160D          UCS-E160D-M... 1255F7F0-9F17-0000-E312-94B74999D9E7
```

Powering Off the Server

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **power off**	Turns off the server.

This example turns off the server:

```
Server# scope chassis
Server /chassis # power off
This operation will change the server's power state.
Continue?[y|N]y

Server /chassis # show
Power Serial Number Product Name   PID            UUID
----- ------------- -------------  -------------  ------------------------------------
off    FOC16161F1P   E160D          UCS-E160D-M... 1255F7F0-9F17-0000-E312-94B74999D9E7
```

Power Cycling the Server

Before You Begin

You must log in with user or admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **power cycle**	After the prompt to confirm, power cycles the server.

	Command or Action	Purpose
		Note • Power cycling the server is the same as pressing the physical power button to power off, and then power on the server. • Power hard-reset is the same as pressing the physical reset button on the server.

This example power cycles the server:

```
Server# scope chassis
Server /chassis # power cycle
This operation will change the server's power state.
Continue?[y|N]y
```

Managing RAID

RAID Options

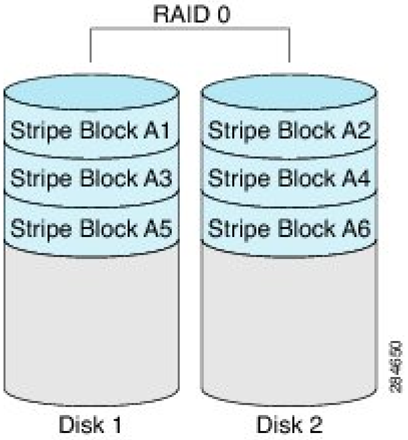
You can choose to store the E-Series Server data files on local Redundant Array of Inexpensive Disks (RAID). The following RAID levels are supported:

- Single-wide E-Series Server supports RAID 0 and RAID 1 levels.
- Double-wide E-Series Server supports RAID 0, RAID 1, and RAID 5 levels.
- Double-wide E-Series Server with PCIe option supports RAID 0 and RAID 1 levels.

RAID 0

With RAID 0, the data is stored evenly in stripe blocks across one or more disk drives without redundancy (mirroring). The data in all of the disk drives is different.

Figure 1: RAID 0



Compared to RAID 1, RAID 0 provides additional storage because both disk drives are used to store data. The performance is improved because the read and write operation occurs in parallel within the two disk drives.

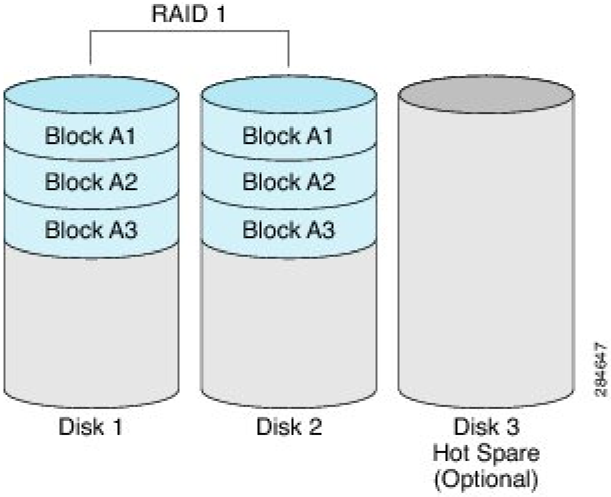
However, there is no fault tolerance, error checking, hot spare, or hot-swapping. If one disk drive fails, the data in the entire array is destroyed. Because there is no error checking or hot-swapping, the array is susceptible to unrecoverable errors.

RAID 1

RAID 1 creates a mirrored set of disk drives, where the data in both the disk drives is identical providing redundancy and high availability. If one disk drive fails, the other disk drive takes over, preserving the data.

RAID 1 also allows you to use a hot spare disk drive. The hot spare drive is always active and is held in readiness as a hot standby drive during a failover.

Figure 2: RAID 1



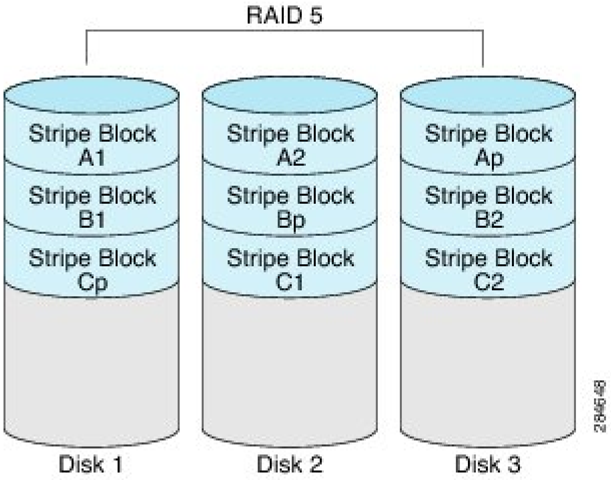
RAID 1 supports fault tolerance and hot-swapping. When one disk drive fails, you can remove the faulty disk drive and replace it with a new disk drive.

However, compared to RAID 0, there is less storage space because only half of the total potential disk space is available for storage and there is an impact on performance.

RAID 5

With RAID 5, the data is stored in stripe blocks with parity data staggered across all disk drives providing redundancy at a low cost.

Figure 3: RAID 5



RAID 5 provides more data storage capacity than RAID 1 and better data protection than RAID 0. It also supports hot swapping; however, RAID 1 offers better performance.

NON-RAID

When the disk drives of a computer are not configured as RAID, the computer is in non-RAID mode. Non-RAID mode is also referred to as Just a Bunch of Disks or Just a Bunch of Drives (JBOD). Non-RAID mode does not support fault tolerance, error checking, hot-swapping, hot spare, or redundancy.

Summary of RAID Options

RAID Options	Description	Advantages	Disadvantages
RAID 0	Data stored evenly in stripe blocks without redundancy	• Better storage • Improved performance	• No error checking • No fault tolerance • No hot-swapping • No redundancy • No hot spare
RAID 1	Mirrored set of disk drives and an optional hot spare disk drive	• High availability • Fault tolerance • Hot spare • Hot-swapping	• Less storage • Performance impact
RAID 5	Data stored in stripe blocks with parity data staggered across all disk drives	• Better storage efficiency than RAID 1 • Better fault tolerance than RAID 0 • Low cost of redundancy • Hot-swapping	• Slow performance
Non-RAID	Disk drives not configured for RAID Also referred to as JBOD	• Portable	• No error checking • No fault tolerance • No hot-swapping • No redundancy • No hot spare

Configuring RAID

Use this procedure to configure the RAID level, strip size, host access privileges, drive caching, and initialization parameters on a virtual drive.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **show storageadapter**	Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.
Step 3	Server /chassis # **scope storageadapter SLOT-***slot-number*	Enters command mode for an installed storage card.
Step 4	Server /chassis/storageadapter # **show physical-drive**	Displays physical disk drives. This information allows you to determine the status of the physical drives. **Note** To configure RAID, the status of the physical drives must be **unconfigured good**. To change the state of the physical drive, see Changing the Physical Drive State.
Step 5	Server /chassis/storageadapter # **create-virtualdrive** {**-r0** | **-r1** | **-r5**} *physical-drive-numbers* [**QuickInit** | **FullInit** | **NoInit**] [**RW** | **RO** | **Blocked**] [**DiskCacheUnchanged** | **DiskCacheEnable** | **DiskCacheDisable**] [**-strpsz64** | **-strpsz32** | **-strpsz16** | **-strpsz8**]	Creates a virtual drive with the specified RAID level on the physical drive. You can also specify the following options: **Note** The options are *not* case sensitive. • (Optional) Initialization options: ◦ **QuickInit**—Controller initialization the drive quickly. You can start writing data into the virtual drive in a few seconds. This is the default option. ◦ **FullInit**—Controller does a complete initialization of the new configuration. You cannot write data into the virtual drive until initialization is complete. If the drive is large, this can take a long time. ◦ **NoInit**—Controller does not initialize the drives. • (Optional) Access policy options: ◦ **RW**—The host has full access to the drive. This is the default option. ◦ **RO**—The host can only read data from the drive. ◦ **Blocked**—The host cannot access the drive.

	Command or Action	Purpose
		• (Optional) Drive cache options: ◦ **DriveCacheUnchanged**—The controller uses the caching policy specified on the physical drive. This is the default option. ◦ **DriveCacheEnable**—Caching is enabled on the physical drives. ◦ **DriveCacheDisable**—Caching is disabled on the physical drives. • (Optional) Strip size options: ◦ **-strpsz64**—This is the default option. ◦ **-strpsz32** ◦ **-strpsz16** ◦ **-strpsz8** **Caution** The smaller strip sizes have a known problem with VMware vSphere Hypervisor™ installation; therefore, if you are installing the vSphere platform, we recommend that you use the **strpsz64** option.
Step 6	Server /chassis/storageadapter # **show virtual-drive**	(Optional) Displays virtual drive information for the storage card. This information allows you to verify RAID configuration.

This example shows how to configure RAID.

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ----------------------------- -------------- ----------------------- --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092            LSI Logic   0 MB

Server /chassis # scope storageadapter SLOT-5

Server /chassis /storageadapter# show physical-drive

Slot Number  Controller Status               Manufacturer   Model        Drive  Firmware
Coerced Size   Type
----------- ---------- ------------------------------------ -------------- --------------
-------------- ---
1            SLOT-5     unconfigured good    TOSHIBA        MBF2600RC    5704   571250 MB
         HDD
2            SLOT-5     unconfigured good    ATA            ST9500620NS  SN01   475883 MB
         HDD

Server /chassis /storageadapter # create-virtualdrive -r0 1 FullInit RW DiskCacheEnable
-strpsz32
---
```

```
status: ok
----------------------
Server /chassis /storageadapter # show virtual-drive
Virtual Drive  Status               Name                      Size       RAID Level
-------------- -------------------- ------------------------ ---------- ----------
0              Optimal                                        571250 MB  RAID 0
```

What to Do Next

Make the disk drive bootable. See Making the Disk Drive Bootable

Making the Disk Drive Bootable

After you configure RAID, you must make the disk drive bootable. Use this procedure to make the disk drive bootable.

Before You Begin

- Configure RAID on the disk drive.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **show storageadapter**	Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.
Step 3	Server /chassis # **scope storageadapter SLOT-***slot-number*	Enters command mode for an installed storage card.
Step 4	Server /chassis/storageadapter # **show physical-drive**	Displays physical disk drives. **Note** The physical drive status could be one of the following: • **system**—JBOD mode. The drive is not configured as RAID. • **online**—RAID mode. • **unconfigured good**—The drive is ready to be assigned to a drive group or hot spare pool. No mode is configured on the drive. • **hotspare**—The drive is designated as a spare drive. No mode is configured on the drive.
Step 5	Server /chassis/storageadapter # **set boot-drive {pd1 | pd2 | pd3 | vd0}**	Makes the disk drive bootable.

	Command or Action	Purpose
		Note To make the disk drive bootable, the status of the drive must be **system**. The status **system** indicates that the drive is in JBOD (non-RAID) mode.
Step 6	Server /chassis/storageadapter # **commit**	Commits the changes.
Step 7	Server /chassis/storageadapter # **show settings**	Displays settings.

This example shows how to make the disk drive bootable using the CIMC CLI.

```
Server# scope chassis
Server /chassis# show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ----------------------------- ------------- ----------------------- --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092            LSI Logic   0 MB

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# show physical-drive

Slot Number  Controller Status               Manufacturer   Model         Drive  Firmware
Coerced Size   Type
----------- ---------- ------------------------------------ -------------- --------------
-------------- -----
1            SLOT-5     system               TOSHIBA        MBF2600RC     5704   571250 MB
         HDD
2            SLOT-5     unconfigured good    ATA            ST9500620NS   SN01   475883 MB
         HDD

   Server /chassis /storageadapter# set boot-drive pd1
Server /chassis /storageadapter*# commit
Server /chassis /storageadapter# show settings
Boot Drive: pd1
```

Modifying RAID Configuration

Enabling Auto Rebuild on the Storage Controller

Use this procedure to rebuild a disk drive automatically. If one of the disk drives that is configured with RAID gets degraded, and a new drive is plugged it, the rebuild process on the new drive starts automatically.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.

	Command or Action	Purpose
Step 2	Server /chassis # **show storageadapter**	Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.
Step 3	Server /chassis # **scope storageadapter SLOT-***slot-number*	Enters command mode for an installed storage card.
Step 4	Server /chassis/storageadapter # **set global-hotspare-for-newdrives true**	Enables auto rebuild on the storage controller.
Step 5	Server /chassis/storageadapter* # **commit**	Commits the changes.

This example shows how to enable auto rebuild on the storage controller.

```
Server# scope chassis
Server /chassis # show storageadapter
PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ----------------------------- -------------- ----------------------- --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# set global-hotspare-for-newdrives true
Server /chassis /storageadapter*# commit
```

Performing a Consistency Check on a Virtual Drive

Use this procedure to verify the drives for consistency.

- **For RAID 5**—This procedure checks if the data in all of the parity stripe blocks is correct.
- **For RAID 1**—This procedure checks if the data in both disk drives is identical.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **show storageadapter**	Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.
Step 3	Server /chassis # **scope storageadapter SLOT-***slot-number*	Enters command mode for an installed storage card.
Step 4	Server /chassis/storageadapter # **scope virtual-drive** *drive-number*	Enters command mode for the specified virtual drive.
Step 5	Server /chassis/storageadapter /virtual-drive # **verify**	Verifies the drive for consistency.

	Command or Action	Purpose
		• **For RAID 5**—Checks if the data in all of the parity stripe blocks is correct. • **For RAID 1**—Checks if the data in both disk drives is identical.
Step 6	Server /chassis/storageadapter /virtual-drive # **show detail**	Displays information about the specified virtual drive

This example shows how to perform a consistency check on a virtual drive.

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ----------------------------- ------------- ----------------------- --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# scope virtual-drive 0
Server /chassis /storageadapter/virtual-drive# verify
---
status: ok
...
Server /chassis /storageadapter/virtual-drive# show detail
Status: Optimal
    Name:
    Size: 475883 MB
    RAID Level: RAID 1
    Target ID: 0
    Stripe Size: 64 KB
    Drives Per Span: 2
    Span Depth: 1
    Access Policy: Read-Write
    Disk Cache Policy: Unchanged
    Write Cache Policy: Write Through
    Cache Policy: Direct
    Read Ahead Policy: None
    Auto Snapshot: false
    Auto Delete Oldest: true
    Allow Background Init: true
    Consistency Check Progress: 0 %
    Consistency Check Elapsed Seconds: 0 s
```

Reconstructing the Virtual Drive Options

To migrate (reconstruct) the virtual drive to a new RAID level, you must add or remove physical drives. When you add or remove the physical drives, the size of the virtual drive is either retained or increased.

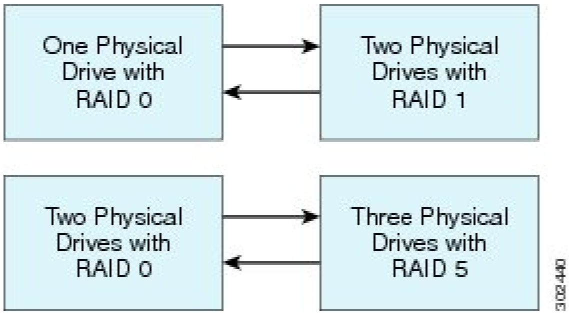
You can retain or increase the size of the virtual drive but you cannot decrease its size. For example, if you have two physical drives with RAID 0, you cannot migrate to RAID 1 with the same number of drives. Because RAID 1 creates a mirrored set of disk drives, the RAID 0 to RAID 1 migration would cause the size of the virtual drive to decrease, which is not supported.

Caution The virtual drive reconstruction process might take several hours to complete. You can continue to use the system during the reconstruction process.

Retaining the Size of the Virtual Drive Options

See the following figure and the table that follows for options that retain the size of the virtual drive when you migrate the virtual drive to a new RAID level.

Figure 4: Retaining the Virtual Drive Size Options


One Physical Drive with RAID 0
Two Physical Drives with RAID 1
Two Physical Drives with RAID 0
Three Physical Drives with RAID 5
302440

The following table lists the options that retain the size of the virtual drive and provides information about how many physical drives you must add or remove to migrate the virtual drive to a specific RAID level.

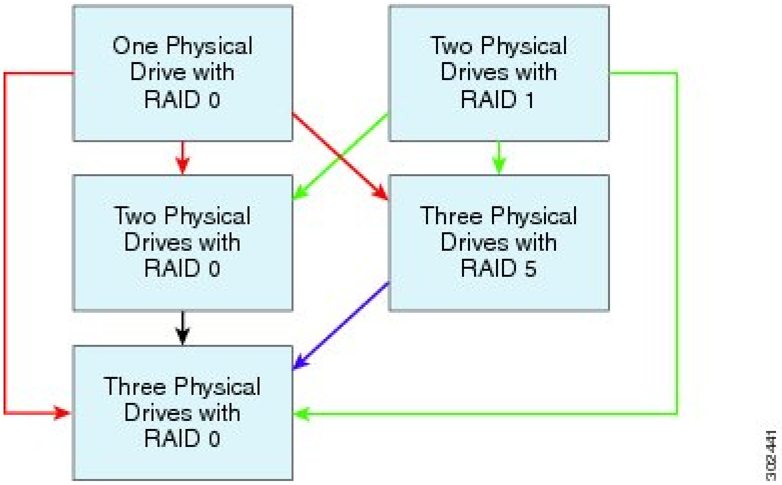
Table 1: Retaining the Virtual Drive Size

From:	Migrate to:	Add or Remove Disks
One physical drive with RAID 0	Two physical drives with RAID 1	Add one disk.
Two physical drives with RAID 1	One physical drive with RAID 0	Remove one disk.
Two physical drives with RAID 0	Three physical drives with RAID 5	Add one disk.
Three physical drives with RAID 5	Two physical drives with RAID 0	Remove one disk.

Increasing the Size of the Virtual Drive Options

See the following figure and the table that follows for options that increase the size of the virtual drive when you migrate the virtual drive to a new RAID level.

Figure 5: Increasing the Virtual Drive Size Options


One Physical Drive with RAID 0
Two Physical Drives with RAID 1
Two Physical Drives with RAID 0
Three Physical Drives with RAID 5
Three Physical Drives with RAID 0
302441

The following table lists the options that increase the size of the virtual drive and provides information about how many physical drives you must add or remove to migrate the virtual drive to a specific RAID level.

Table 2: Increasing the Virtual Drive Size

From:	Migrate to:	Add or Remove Disks
One physical drive with RAID 0 See the **Red** arrows in the figure.	Two physical drives with RAID 0	Add one disk.
	Three physical drives with RAID 5	Add two disks.
	Three physical drives with RAID 0	Add two disks.
Two physical drives with RAID 1 See the **Green** arrows in the figure.	Two physical drives with RAID 0	—
	Three physical drives with RAID 5	Add one disk.
	Three physical drives with RAID 0	Add one disk.
Two physical drives with RAID 0 See the **Black** arrow in the figure.	Three physical drives with RAID 0	Add one disk.
Three physical drives with RAID 5 See the **Purple** arrow in the figure.	Three physical drives with RAID 0	—

Reconstructing a Virtual Drive

Use this procedure to add or remove the physical drive in order to migrate the virtual drive to the specified RAID level.

Before You Begin

- See Reconstructing the Virtual Drive Options.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **show storageadapter**	Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.
Step 3	Server /chassis # **scope storageadapter SLOT-***slot-number*	Enters command mode for an installed storage card.
Step 4	Server /chassis/storageadapter # **scope virtual-drive** *drive-number*	Enters command mode for the specified virtual drive.
Step 5	Server /chassis/storageadapter /virtual-drive # **reconstruct** {**-r0** | **-r1** | **-r5**} [**-add** | **-rmv**] *new-physical-drive-slot-number(s)*	Adds or removes the physical drive to migrate the virtual drive to the new specified RAID level. • **-r0** | **-r1** | **-r5**—Available RAID levels are: RAID 0, RAID 1, or RAID 5. • **-add** | **-rmv** —Adds or removes the physical drive.
Step 6	Server /chassis/storageadapter /virtual-drive # **show detail**	Displays information about the specified virtual drive.

This example shows how to migrate one of two discs that was initially configured as RAID 1 to RAID 0.

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product       Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ---------------------------- -------------- ----------------------- --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092            LSI Logic   0 MB

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# scope virtual-drive 0
Server /chassis /storageadapter/virtual-drive# reconstruct -r0 -rmv 1
---
status: ok
...
Server /chassis /storageadapter/virtual-drive# show detail
Status: Optimal
    Status: Optimal
    Name:
    Size: 475883 MB
    RAID Level: RAID 1
    Target ID: 0
    Stripe Size: 64 KB
    Drives Per Span: 2
    Span Depth: 1
    Access Policy: Read-Write
    Disk Cache Policy: Unchanged
    Write Cache Policy: Write Through
    Cache Policy: Direct
    Read Ahead Policy: None
    Auto Snapshot: false
    Auto Delete Oldest: true
    Allow Background Init: true
    ReConstruct Progress: 0 %
    ReConstruct Elapsed Seconds: 3 s
```

Deleting RAID Configuration

Use this procedure to clear all RAID configuration.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **show storageadapter**	Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.
Step 3	Server /chassis # **scope storageadapter SLOT-***slot-number*	Enters command mode for an installed storage card.
Step 4	Server /chassis /storageadapter # **clear-all-raid-config**	Clears all RAID configuration. At the confirmation prompts answer Yes. **Note** When RAID configuration is cleared, all existing data on th disk drive is lost.

This example shows how to delete RAID configuration.

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ----------------------------- -------------- ----------------------- --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB

Server /chassis # scope storageadapter SLOT-5
Server /chassis /storageadapter # clear-all-raid-config
This operation will clear all RAID configuration.
Warning: All data in the disks would be lost!!!
Are you sure you want to proceed? [Yes|No] Yes
Are you really sure you want to clear all RAID configuration and lose all data? [Yes|No]
Yes
```

Changing the Physical Drive State

Use this procedure to change the state of the physical drive. Options are: hotspare, jbod, or unconfigured good.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **show storageadapter**	Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.
Step 3	Server /chassis # **scope storageadapter SLOT-***slot-number*	Enters command mode for an installed storage card.
Step 4	Server /chassis/storageadapter # **show physical-drive**	Displays physical disk drives.
Step 5	Server /chassis/storageadapter # **scope physical-drive** *slot-number*	Enters command mode for the specified physical drive.
Step 6	Server /chassis/storageadapter /physical-drive # **show detail**	Displays information about the specified physical drive.
Step 7	Server /chassis/storageadapter /physical-drive # **set state {unconfiguredgood | jbod | hotspare}**	Changes the state of the physical drive. Options are: hotspare, jbod, or unconfigured good.
Step 8	Server /chassis/storageadapter /physical-drive* # **commit**	Commits the changes.
Step 9	Server /chassis/storageadapter /physical-drive # **show detail**	Displays information about the specified physical drive.

This example shows how to change the state of the physical drive.

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ----------------------------- -------------- ----------------------- --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# show physical-drive

Slot Number  Controller Status                Manufacturer   Model        Drive  Firmware
Coerced Size   Type
----------- ---------- ------------------------------------ -------------- --------------
-------------- -----
1            SLOT-5     system                TOSHIBA        MBF2600RC    5704   571250 MB
         HDD
2            SLOT-5     unconfigured good     ATA            ST9500620NS  SN01   475883 MB
```

```
          HDD

Server /chassis /storageadapter# scope physical-drive 1
Server /chassis /storageadapter/physical-drive# show detail

Slot Number 1:
    Controller: SLOT-5
    Status: system
    Manufacturer: TOSHIBA
    Model: MBF2600RC
    Drive Firmware: 5704
    Coerced Size: 571250 MB
    Type: HDD

Server /chassis /storageadapter/physical-drive# set state hotspare
Server /chassis /storageadapter/physical-drive*# commit
Server /chassis /storageadapter/physical-drive# show detail

Slot Number 1:
    Controller: SLOT-5
    Status: hotspare
    Manufacturer: TOSHIBA
    Model: MBF2600RC
    Drive Firmware: 5704
    Coerced Size: 571250 MB
    Type: HDD
```

Rebuilding the Physical Drive

Use this procedure to manually start the rebuild process on the physical drive.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **show storageadapter**	Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.
Step 3	Server /chassis # **scope storageadapter SLOT-***slot-number*	Enters command mode for an installed storage card.
Step 4	Server /chassis/storageadapter # **show physical-drive**	Displays physical disk drives.
Step 5	Server /chassis/storageadapter # **scope physical-drive** *slot-number*	Enters command mode for the specified physical drive.
Step 6	Server /chassis/storageadapter /physical-drive # **rebuild**	Rebuilds the physical drive.

This example shows how to change the state of the physical drive.

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
```

```
-------- ----------------------------- -------------- ----------------------- --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# show physical-drive

Slot Number  Controller Status               Manufacturer   Model        Drive  Firmware
Coerced Size   Type
----------- ---------- ------------------------------------ ------------- ---------------
-------------- -----
1            SLOT-5     system               TOSHIBA        MBF2600RC    5704   571250 MB
         HDD
2            SLOT-5     unconfigured good    ATA            ST9500620NS  SN01   475883 MB
         HDD

Server /chassis /storageadapter# scope physical-drive 1
Server /chassis /storageadapter/physical-drive# rebuild
```

Configuring BIOS Settings

Viewing BIOS Status

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters the BIOS command mode.
Step 2	Server /bios # **show detail**	Displays details of the BIOS status.

The BIOS status information contains the following fields:

Name	Description
BIOS Version	The version string of the running BIOS.
Boot Order	The order of bootable target types that the server will attempt to use.
FW Update/Recovery Status	The status of any pending firmware update or recovery action.
FW Update/Recovery Progress	The percentage of completion of the most recent firmware update or recovery action.

This example displays the BIOS status:

```
Server# scope bios
Server /bios # show detail
    BIOS Version: "C460M1.1.2.2a.0 (Build Date: 01/12/2011)"
    Boot Order: EFI,CDROM,HDD
    FW Update/Recovery Status: NONE
    FW Update/Recovery Progress: 100
```

```
Server /bios #
```

Installing BIOS Firmware from the TFTP Server

Before You Begin

Obtain the BIOS firmware from Cisco Systems and store the file on a local TFTP server. See Obtaining Software from Cisco Systems.

Note If you start an update while an update is already in process, both updates will fail.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters the BIOS command mode.
Step 2	Server /bios # **update** *tftp-ip-address path-and-filename*	Starts the BIOS firmware update. The server will obtain the update firmware at the specified path and file name from the TFTP server at the specified IP address.
Step 3	(Optional) Server /bios # **show detail**	Displays the progress of the BIOS firmware update.

This example updates the BIOS firmware:

```
Server# scope bios
Server /bios # update 10.20.34.56 //test/dnld-ucs-k9-bundle.1.0.2h.bin
  <CR>  Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /bios #
```

Configuring Advanced BIOS Settings

Note Depending on your installed hardware, some configuration options described in this topic may not appear.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters the BIOS command mode.
Step 2	Server /bios # **scope advanced**	Enters the advanced BIOS settings command mode.
Step 3	Configure the BIOS settings.	For the CLI commands, descriptions and information about the options for each BIOS setting, see the following topics: • Advanced: Processor BIOS Settings, on page 44 • Advanced: Memory BIOS Settings, on page 49 • Advanced: Serial Port BIOS Settings, on page 49 • Advanced: USB BIOS Settings, on page 49
Step 4	Server /bios/advanced # **commit**	Commits the transaction to the system configuration. Changes are applied on the next server reboot. If server power is on, you are prompted to choose whether to reboot now.

This example shows how to enable Intel virtualization technology:

```
Server# scope bios
Server /bios # scope advanced
Server /bios/advanced # set IntelVTD Enabled
Server /bios/advanced *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N] n
Changes will be applied on next reboot.
Server /bios/advanced #
```

Configuring Server Management BIOS Settings

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters the BIOS command mode.
Step 2	Server /bios # **scope server-management**	Enters the server management BIOS settings command mode.
Step 3	Configure the BIOS settings.	For the CLI commands, descriptions and information about the options for each BIOS setting, see the following topic:

	Command or Action	Purpose
		- Server Management BIOS Settings, on page 50
Step 4	Server /bios/server-management # **commit**	Commits the transaction to the system configuration. Changes are applied on the next server reboot. If server power is on, you are prompted to choose whether to reboot now.

This example shows how to set the BAUD rate to 9.6k :

```
Server# scope bios
Server /bios # scope server-management
Server /bios/server-management # set BaudRate 9.6k
Server /bios/server-management *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N] n
Changes will be applied on next reboot.
Server /bios/server-management #
```

Clearing the BIOS CMOS

On rare occasions, troubleshooting a server may require you to clear the server's BIOS CMOS memory. This procedure is not part of the normal maintenance of a server.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters the BIOS command mode.
Step 2	Server /bios # **clear-cmos**	After a prompt to confirm, clears the CMOS memory.

This example clears the BIOS CMOS memory:

```
Server# scope bios
Server /bios # clear-cmos
This operation will clear the BIOS CMOS.
Note: Server should be in powered off state to clear CMOS.
Continue?[y|N] y
```

Clearing the BIOS Password

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters the BIOS command mode.
Step 2	Server /bios # **clear-bios-password**	Clears the BIOS password. You must reboot the server for the clear password operation to take effect. You are prompted to create a new password when the server reboots.

This example clears the BIOS password:

```
Server# scope bios
Server /bios # clear-bios-password
This operation will clear the BIOS Password.
Note: Server should be rebooted to clear BIOS password.
Continue?[y|N]y
```

Restoring BIOS Defaults

Before You Begin

You must log in as a user with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope bios**	Enters the BIOS command mode.
Step 2	Server /bios # **bios-setup-default**	Restores BIOS default settings. This command initiates a reboot.

This example restores BIOS default settings:

```
Server# scope bios
Server /bios # bios-setup-default
This operation will reset the BIOS set-up tokens to factory defaults.
All your configuration will be lost.
Changes to BIOS set-up parameters will initiate a reboot.
Continue?[y|N]y
```

Server BIOS Settings

The tables in the following sections list the server BIOS settings that you can view and configure.

For each setting, the CLI **set** command appears below the setting name in the table, and the command options are listed in the setting description. To view the default for each setting, type the **set** command followed by a question mark. In the displayed option keywords, the default option is marked with an asterisk.

Note We recommend that you verify the support for BIOS settings in your server. Depending on your installed hardware, some settings may not be supported.

Advanced: Processor BIOS Settings

Name	Description
Intel Turbo Boost Technology **set IntelTurboBoostTech**	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • **Disabled**—The processor does not increase its frequency automatically. • **Enabled**—The processor utilizes Turbo Boost Technology if required.
Enhanced Intel Speedstep Technology **set EnhancedIntelSpeedStep**	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **Disabled**—The processor never dynamically adjusts its voltage or frequency. • **Enabled**—The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Intel Hyper-Threading Technology **set IntelHyperThread**	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **Disabled**—The processor does not permit hyperthreading. • **Enabled**—The processor allows for the parallel execution of multiple threads. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Number of Enabled Cores **set CoreMultiProcessing**	Sets the state of logical processor cores in a package. If you disable this setting, Hyper Threading is also disabled. This can be one of the following: • **All**—Enables multi processing on all logical processor cores. • **1** through *n*—Specifies the number of logical processor cores that can run on the server. To disable multi processing and have only one logical processor core running on the server, select 1. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disable **set ExecuteDisable**	Classifies memory areas on the server to specify where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **Disabled**—The processor does not classify memory areas. • **Enabled**—The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Intel Virtualization Technology **set IntelVT**	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
Intel VT for Directed IO **set IntelVTD**	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **Disabled**—The processor does not use virtualization technology. • **Enabled**—The processor uses virtualization technology.

Name	Description
Intel VT-d Interrupt Remapping **set InterruptRemap**	Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following: • **Disabled**—The processor does not support remapping. • **Enabled**—The processor uses VT-d Interrupt Remapping as required.
Intel VT-d Coherency Support **set CoherencySupport**	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.
Intel VT-d Address Translation Services **set ATS**	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled**—The processor does not support ATS. • **Enabled**—The processor uses VT-d ATS as required.
Intel VT-d PassThrough DMA **set PassThroughDMA**	Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following: • **Disabled**—The processor does not support pass-through DMA. • **Enabled**—The processor uses VT-d Pass-through DMA as required.
Direct Cache Access **set DirectCacheAccess**	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • **Disabled**—Data from I/O devices is not placed directly into the processor cache. • **Enabled**—Data from I/O devices is placed directly into the processor cache.
Processor C3 Report **set ProcessorC3Report**	Whether the processor sends the C3 report to the operating system. This can be one of the following: • **Disabled**—The processor does not send the C3 report. • **ACPI_C2**—The processor sends the C3 report using the ACPI C2 format. • **ACPI_C3**—The processor sends the C3 report using the ACPI C3 format.

Name	Description
Processor C6 Report **set ProcessorC6Report**	Whether the processor sends the C6 report to the operating system. This can be one of the following: • **Disabled**—The processor does not send the C6 report. • **Enabled**—The processor sends the C6 report.
Hardware Prefetcher **set HardwarePrefetch**	Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following: • **Disabled**—The hardware prefetcher is not used. • **Enabled**—The processor uses the hardware prefetcher when cache issues are detected. **Note** You must select **Custom** in the **CPU Performance** setting to specify this value. For any value other than **Custom**, this option is overridden by the setting in the selected CPU performance profile.
Package C State Limit **set PackageCstateLimit**	The amount of power available to the server components when they are idle. This can be one of the following: • **C0_state**—The server provides all server components with full power at all times. This option maintains the highest level of performance and requires the greatest amount of power. • **C2_state**— System level coordination is in progress resulting in high power consumption. There might be performance issues until the coordination is complete. • **C6_state**—When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0 or C2, but there might be performance issues until the server returns to full power. • **C7_state**—When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves the maximum amount of power but it also requires the longest time for the server to return to high performance mode. • **No_Limit**—The server may enter any available C state. **Note** This option is used only if **CPU C State** is enabled.

Name	Description
Patrol Scrub **set PatrolScrub**	Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following: • **Disabled**—The system checks for memory ECC errors only when the CPU reads or writes a memory address. • **Enabled**—The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running.
Demand Scrub **set DemandScrub**	Whether the system allows you to perform a memory scrub on demand. This can be one of the following: • **Disabled**—The system does not allow you to perform a memory scrub on demand. • **Enabled**—The system allows you to perform a memory scrub on demand. If errors are found, the system attempts to fix them or marks the location as unreadable. This process allows the system to run faster and with fewer data processing errors.
Device Tagging **set DeviceTagging**	Whether the system allows you to group devices and interfaces based on a variety of information, including descriptions, addresses, and names. This can be one of the following: • **Disabled**—The system does not allow you to group devices and interfaces. • **Enabled**—The system allows you to group devices and interfaces based on a variety of information, including descriptions, addresses, and names.

Advanced: Memory BIOS Settings

Name	Description
Select Memory RAS **set SelectMemoryRAS**	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **Maximum_Performance**—System performance is optimized. • **Mirroring**—System reliability is optimized by using half the system memory as backup. • **Sparing**—System reliability is enhanced with a degree of memory redundancy while making more memory available to the operating system than mirroring.

Advanced: Serial Port BIOS Settings

Name	Description
Serial A Enable **set Serial-PortA**	Whether serial port A is enabled or disabled. This can be one of the following: • **Disabled**—The serial port is disabled. • **Enabled**—The serial port is enabled.

Advanced: USB BIOS Settings

Name	Description
USB Port 0 **set USBPort0**	Whether the processor uses USB port 0. This can be one of the following: • **Disabled**—The server does not use the USB port 0. • **Enabled**—The processor uses the USB port 0.
USB Port 1 **set USBPort1**	Whether the processor uses USB port 1. This can be one of the following: • **Disabled**—The server does not use the USB port 1. • **Enabled**—The processor uses the USB port 1.

Server Management BIOS Settings

Name	Description
Assert NMI on SERR **set AssertNMIOnSERR**	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs. This can be one of the following: • **Disabled**—The BIOS does not generate an NMI or log an error when a SERR occurs. • **Enabled**—The BIOS generates an NMI and logs an error when a SERR occurs. You must enable this setting if you want to enable **Assert NMI on PERR**.
Assert NMI on PERR **set AssertNMIOnPERR**	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs. This can be one of the following: • **Disabled**—The BIOS does not generate an NMI or log an error when a PERR occurs. • **Enabled**—The BIOS generates an NMI and logs an error when a PERR occurs. You must enable **Assert NMI on SERR** to use this setting.
FRB2 Enable **set FRB-2**	Whether the FRB2 timer is used by CIMC to recover the system if it hangs during POST. This can be one of the following: • **Disabled**—The FRB2 timer is not used. • **Enabled**—The FRB2 timer is started during POST and used to recover the system if necessary.
Console Redirection **set ConsoleRedir**	Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following: • **Disabled**—No console redirection occurs during POST. • **Serial_Port_A**—Enables serial port A for console redirection during POST. This option is valid for blade servers and rack-mount servers. **Note** If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.

Name	Description
Flow Control **set FlowCtrl**	Whether a handshake protocol is used for flow control. Request to Send/Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following: • **None**—No flow control is used. • **RTS-CTS**—RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.
Baud Rate **set BaudRate**	What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following: • **9.6k**—A 9600 BAUD rate is used. • **19.2k**—A 19200 BAUD rate is used. • **38.4k**—A 38400 BAUD rate is used. • **57.6k**—A 57600 BAUD rate is used. • **115.2k**—A 115200 BAUD rate is used. **Note** This setting must match the setting on the remote terminal application.
Terminal Type **set TerminalType**	What type of character formatting is used for console redirection. This can be one of the following: • **PC-ANSI**—The PC-ANSI terminal font is used. • **VT100**—A supported vt100 video terminal and its character set are used. • **VT100-PLUS**—A supported vt100-plus video terminal and its character set are used. • **VT-UTF8**—A video terminal with the UTF-8 character set is used. **Note** This setting must match the setting on the remote terminal application.

Name	Description
OS Boot Watchdog Timer **set OSBootWatchdogTimer**	Whether the BIOS programs the watchdog timer with a specified timeout value. If the operating system does not complete booting before the timer expires, the CIMC resets the system and an error is logged. This can be one of the following: • **Disabled**—The watchdog timer is not used to track how long the server takes to boot. • **Enabled**—The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified by the **set OSBootWatchdogTimerTimeout** command, the CIMC logs an error and takes the action specified by the **set OSBootWatchdogTimerPolicy** command.
OS Boot Watchdog Timer Policy **set OSBootWatchdogTimerPolicy**	The action the system takes when the watchdog timer expires. This can be one of the following: • **Do Nothing**—The state of the server power does not change when the watchdog timer expires during OS boot. • **Power Down**—The server is powered off if the watchdog timer expires during OS boot. • **Reset**—The server is reset if the watchdog timer expires during OS boot. **Note** This option is only applicable if you enable the OS Boot Watchdog Timer.
set ResumeOnACPowerLoss	

CHAPTER 4

Viewing Server Properties

This chapter includes the following sections:

- Viewing Server Properties, page 53
- Viewing CPU Properties, page 54
- Viewing Memory Properties, page 54
- Viewing Power Supply Properties, page 55
- Viewing Storage Properties, page 56
- Viewing PCI Adapter Properties, page 59
- Viewing Power Policy Statistics, page 60
- Viewing Hard Drive Presence, page 61

Viewing Server Properties

Before You Begin

The server must be powered on, or the properties will not display.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show detail**	Displays server properties.

This example displays server properties:

```
Server# scope chassis
Server /chassis # show detail
Chassis:
    Power: on
    Power Button: unlocked
    IOS Lockout: unlocked
    Serial Number: FOC16161F1P
    Product Name: E160D
    PID : UCS-E160D-M1/K9
    UUID: 1255F7F0-9F17-0000-E312-94B74999D9E7
    Description
```

Viewing CPU Properties

Before You Begin

The server must be powered on, or the properties will not display.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show cpu** [**detail**]	Displays CPU properties.

This example displays CPU properties:

```
Server# scope chassis
Server /chassis # show cpu
Name         Cores    Version
------------ -------- --------------------------------------------------
CPU1         4        Intel(R) Xeon(R) CPU     E5-2418L 0 @ 2.00GHz

Server /chassis #
```

Viewing Memory Properties

Before You Begin

The server must be powered on, or the properties will not display.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show dimm** [**detail**]	Displays memory properties.
Step 3	Server /chassis # **show dimm-summary**	Displays DIMM summary information.

This example displays memory properties:

```
Server# scope chassis
Server /chassis # show dimm
```

```
Name                 Capacity        Channel Speed (MHz) Channel Type
-------------------- --------------- ------------------- ---------------

Node0_Dimm0          8192 MB         1333                DDR3
Node0_Dimm1          8192 MB         1333                DDR3
Node0_Dimm2          8192 MB         1333                DDR3
```

This example displays detailed information about memory properties:

```
Server# scope chassis
Server /chassis # show dimm detail
Name Node0_Dimm0:
 Capacity: 8192 MB
 Channel Speed (MHz): 1333
 Channel Type: DDR3
 Memory Type Detail: Registered (Buffered)
 Bank Locator: Node0_Bank0
 Visibility: Yes
 Operability: Operable
 Manufacturer: Samsung
 Part Number: M393B1K70DH0-
 Serial Number: 86A7D514
 Asset Tag: Dimm0_AssetTag
 Data Width: 64 bits
 Name Node0_Dimm1:
 Capacity: 8192 MB
```

This example displays DIMM summary information:

```
Server# scope chassis
Server /chassis # show dimm-summary
DIMM Summary:
 Memory Speed: 1334 MHz
 Total Memory: 24576 MB
 Effective Memory: 24576 MB
 Redundant Memory: 0 MB
 Failed Memory: 0 MB
 Ignored Memory: 0 MB
 Number of Ignored Dimms: 0
 Number of Failed Dimms: 0
 Memory RAS possible: Reserved
 Memory Configuration: Maximum Performance
```

Viewing Power Supply Properties

Before You Begin

The server must be powered on, or the properties will not display.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope power-cap**	Enters the power cap command mode.
Step 2	Server /power-cap # **show** [**detail**]	Displays the server power consumption information.

This example displays the detailed power supply properties for a single-wide E-Series Server:

```
 Server# scope power-cap
 Server /power-cap # show detail
  Cur Consumption (W): 36.10 W
  Max Consumption (W): 075
  Min Consumption (W): 36.10 W
Server /power-cap #
```

This example displays the detailed power supply properties for a double-wide E-Series Server:

```
 Server# scope power-cap
 Server /power-cap # show detail
  Cur Consumption (W): 43.1 W
  Max Consumption (W): 160
  Min Consumption (W): 43.1 W
Server /power-cap #
```

Viewing Storage Properties

Viewing Storage Adapter Properties

Before You Begin

The server must be powered on, or the properties will not display.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **show storageadapter** [*slot*] [**detail**]	Displays installed storage cards. **Note** This command displays all MegaRAID controllers on the server that can be managed through CIMC. If an installed controller or storage device is not displayed, then it cannot be managed through CIMC.
Step 3	Server /chassis # **scope storageadapter SLOT-***slot-number*	Enters command mode for an installed storage card.
Step 4	Server /chassis/storageadapter # **show capabilites** [**detail**]	Displays RAID levels supported by the storage card.
Step 5	Server /chassis/storageadapter # **show error-counters** [**detail**]	Displays number of errors seen by the storage card.
Step 6	Server /chassis/storageadapter # **show firmware-versions** [**detail**]	Displays firmware version information for the storage card.

	Command or Action	Purpose
Step 7	Server /chassis/storageadapter # **show hw-config** [**detail**]	Displays hardware information for the storage card.
Step 8	Server /chassis/storageadapter # **show pci-info** [**detail**]	Displays adapter PCI information for the storage card.
Step 9	Server /chassis/storageadapter # **show running-firmware-images** [**detail**]	Displays running firmware information for the storage card.
Step 10	Server /chassis/storageadapter # **show settings** [**detail**]	Displays adapter firmware settings for the storage card.

This example displays storage properties:

```
Server# scope chassis
Server /chassis # show storageadapter

Controller Product Name                Firmware Package Build Product ID     Cache Memory
Size
---------- --------------------------- --------------------- -------------- -----------------

SLOT-5     LSI MegaRAID SAS 2004 ROMB  20.10.1-0092           LSI Logic      0 MB
```

Viewing Physical Drive Properties

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **scope storageadapter SLOT-***slot-number*	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # **show physical-drive** [*slot-number*] [**detail**]	Displays physical drive information for the storage card.
Step 4	Server /chassis/storageadapter # **show physical-drive-count** [**detail**]	Displays the number of physical drives on the storage card.
Step 5	Server /chassis/storageadapter # **scope physical-drive** *slot-number*	Enters command mode for the specified physical drive.
Step 6	Server /chassis/storageadapter/physical-drive # **show general** [**detail**]	Displays general information about the specified physical drive.

	Command or Action	Purpose
Step 7	Server /chassis/storageadapter/physical-drive # **show security** [**detail**]	Displays inquiry data about the specified physical drive.
Step 8	Server /chassis/storageadapter/physical-drive # **show status** [**detail**]	Displays status information about the specified physical drive.

This example displays general information about the physical drive number 1 on the storage card named SLOT-5:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-5
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show general
Slot Number 1:
    Controller: SLOT-5
    Enclosure Device ID: 64
    Device ID: 3
    Sequence Number: 2
    Media Error Count: 0
    Other Error Count: 12
    Predictive Failure Count: 0
    Link Speed: 6.0 Gb/s
    Interface Type: SATA
    Media Type: HDD
    Block Size: 512
    Block Count: 1953525168
    Raw Size: 953869 MB
    Non Coerced Size: 953357 MB
    Coerced Size: 952720 MB
    SAS Address 0: 4433221100000000
    SAS Address 1:
    Connected Port 0:
    Connected Port 1:
    Connected Port 2:
    Connected Port 3:
    Connected Port 4:
```

This example provides status information about the physical drive number 1 on the storage card named SLOT-5:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-5
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show status
Slot Number 1:
   Controller: SLOT-5
   State: system
   Online: true
   Fault: false
```

Viewing Virtual Drive Properties

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **scope storageadapter SLOT-***slot-number*	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # **show virtual-drive** [*drive-number*] [**detail**]	Displays virtual drive information for the storage card.
Step 4	Server /chassis/storageadapter # **show virtual-drive-count** [**detail**]	Displays the number of virtual drives configured on the storage card.
Step 5	Server /chassis/storageadapter # **scope virtual-drive** *drive-number*	Enters command mode for the specified virtual drive.
Step 6	Server /chassis/storageadapter/virtual-drive # **show physical-drive** [**detail**]	Displays physical drive information about the specified virtual drive.

This example displays power supply properties:

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-5
Server /chassis/storageadapter # show virtual-drive
Virtual Drive  Status               Name                     Size       RAID Level
-------------- -------------------- ------------------------ ---------- ----------
0              Optimal                                       571250 MB  RAID 1

Server /chassis/storageadapter # show virtual-drive-count
PCI Slot SLOT-5:
    Virtual Drive Count: 1
    Degraded Virtual Drive Count: 0
    Offline Virtual Drive Count: 0
Server /chassis/storageadapter # scope virtual-drive 0
Server /chassis/storageadapter/virtual-drive # show physical-drive
Span  Physical Drive Status     Starting Block Number Of Blocks
----- -------------- ---------- -------------- ----------------
0     2              online     0              1169920000
0     1              online     0              1169920000
```

Viewing PCI Adapter Properties

Before You Begin

The server must be powered on, or the properties will not display.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **show pci-adapter** [**detail**]	Displays PCI adapter properties.

This example displays PCI adapter properties:

```
Server# scope chassis
Server /chassis # show pci-adapter
Name             Slot  Vendor ID    Device ID    Product Name
---------------- ----- ------------ ------------ -------------------------
PCIe Adapter1    1     0x1137       0x0042       Cisco UCS P81E Virtual...
PCIe Adapter2    5     0x1077       0x2432       Qlogic QLE2462 4Gb dua...

Server /chassis #
```

Viewing Power Policy Statistics

Procedure

	Command or Action	Purpose
Step 1	Server# **show power-cap [detail]**	Displays the server power consumption statistics and the power cap policy.

The displayed fields are described in the following table:

Name	Description
Current Consumption	The power currently being used by the server, in watts.
Maximum Consumption	The maximum number of watts consumed by the server since the last time it was rebooted.
Minimum Consumption	The minimum number of watts consumed by the server since the last time it was rebooted.

This example displays the detailed power statistics for a single-wide E-Series Server:

```
  Server# scope power-cap
  Server /power-cap # show detail
   Cur Consumption (W): 36.10 W
   Max Consumption (W): 075
   Min Consumption (W): 36.10 W
 Server /power-cap #
```

This example displays the detailed power statistics for a double-wide E-Series Server:

```
  Server# scope power-cap
  Server /power-cap # show detail
   Cur Consumption (W): 43.1 W
   Max Consumption (W): 160
   Min Consumption (W): 43.1 W
 Server /power-cap #
```

Viewing Hard Drive Presence

Before You Begin

The server must be powered on, or the properties will not display.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **show hdd**	Displays the hard drives.

This example displays power supply properties:

```
Server# scope chassis
Server /chassis # show hdd
    Name             Status
-------------------- --------------------
HDD1_PRS             inserted
HDD2_PRS             inserted
HDD3_PRS             inserted
```

CHAPTER 5

Viewing Server Sensors

This chapter includes the following sections:

- Viewing the Fault Summary, page 63
- Viewing Temperature Sensors, page 64
- Viewing Voltage Sensors, page 64
- Viewing Storage Sensors, page 65

Viewing the Fault Summary

Procedure

	Command or Action	Purpose
Step 1	Server# **scope fault**	Enters fault command mode.
Step 2	Server /fault # **show discrete-alarm [detail]**	Displays a summary of faults from discrete sensors.
Step 3	Server /fault # **show threshold-alarm [detail]**	Displays a summary of faults from threshold sensors.
Step 4	Server /fault # **show pef [detail]**	Displays a summary of platform event filters.

This example displays a summary of faults from discrete sensors:

```
Server# scope fault
Server /fault # show discrete-alarm
Name         Reading              Sensor Status
------------ -------------------- ------------------------------------
PSU2_STATUS  absent               Critical

Server /fault #
```

Viewing Temperature Sensors

Procedure

	Command or Action	Purpose
Step 1	Server# **scope sensor**	Enters sensor command mode.
Step 2	Server /sensor # **show temperature** [**detail**]	Displays temperature sensor statistics for the server.

This example displays temperature sensor statistics:

```
Server# scope sensor
Server /sensor # show temperature
Name                      Sensor Status  Reading    Units      Min. Warning Max. Warning
Min. Failure Max. Failure
------------------------- -------------- ---------- ---------- ------------ ------------
------------ ------------
IOH_TEMP_SENS             Normal         32.0       C          N/A          80.0
N/A          85.0
P2_TEMP_SENS              Normal         31.0       C          N/A          80.0
N/A          81.0
P1_TEMP_SENS              Normal         34.0       C          N/A          80.0
N/A          81.0
DDR3_P2_D1_TMP            Normal         20.0       C          N/A          90.0
N/A          95.0
DDR3_P1_A1_TMP            Normal         21.0       C          N/A          90.0
N/A          95.0
FP_AMBIENT_TEMP           Normal         28.0       C          N/A          40.0
N/A          45.0

Server /sensor #
```

Viewing Voltage Sensors

Procedure

	Command or Action	Purpose
Step 1	Server# **scope sensor**	Enters sensor command mode.
Step 2	Server /sensor # **show voltage** [**detail**]	Displays voltage sensor statistics for the server.

This example displays voltage sensor statistics:

```
Server# scope sensor
Server /sensor # show voltage
Name                      Sensor Status  Reading    Units      Min. Warning Max. Warning
Min. Failure Max. Failure
------------------------- -------------- ---------- ---------- ------------ ------------
------------ ------------
```

```
P3V_BAT_SCALED           Normal       3.022      V          N/A          N/A
2.798        3.088
P12V_SCALED              Normal       12.154     V          N/A          N/A
11.623       12.331
P5V_SCALED               Normal       5.036      V          N/A          N/A
4.844        5.157
P3V3_SCALED              Normal       3.318      V          N/A          N/A
3.191        3.381
P5V_STBY_SCALED          Normal       5.109      V          N/A          N/A
4.844        5.157
PV_VCCP_CPU1             Normal       0.950      V          N/A          N/A
0.725        1.391
PV_VCCP_CPU2             Normal       0.891      V          N/A          N/A
0.725        1.391
P1V5_DDR3_CPU1           Normal       1.499      V          N/A          N/A
1.450        1.548
P1V5_DDR3_CPU2           Normal       1.499      V          N/A          N/A
1.450        1.548
P1V1_IOH                 Normal       1.087      V          N/A          N/A
1.068        1.136
P1V8_AUX                 Normal       1.773      V          N/A          N/A
1.744        1.852

Server /sensor #
```

Viewing Storage Sensors

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show hdd** [**detail**]	Displays storage sensor information.

The displayed fields are described in the following table:

Name	Description
Name column	The name of the storage device. This can be: **HDD***X***_PRS**—Indicates the presence or absence of each hard drive.
Status column	A brief description of the status of the storage device.

This example displays storage sensor information:

```
Server# scope chassis
Server /chassis # show hdd
Name                 Status
-------------------- --------------------
HDD1_PRS             inserted
HDD2_PRS             inserted
HDD3_PRS             inserted

Server /chassis #
```

CHAPTER 6

Managing Remote Presence

This chapter includes the following sections:

- Managing the Virtual KVM, page 67
- Configuring Virtual Media, page 70
- Managing Serial over LAN, page 71

Managing the Virtual KVM

KVM Console

The KVM console is an interface accessible from CIMC that emulates a direct keyboard, video, and mouse connection to the server. The KVM console allows you to connect to the server from a remote location. Instead of using CD/DVD or floppy drives physically connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives. You can map any of the following to a virtual drive:

- CD/DVD or floppy drive on your computer
- Disk image files (ISO or IMG files) on your computer
- USB flash drive on your computer

You can use the KVM console to install an operating system or hypervisor on the server and to do the following:

- Access the BIOS setup menu by pressing **F2** during bootup.
- Access the CIMC Configuration Utility by pressing **F8** during bootup.
- Access the WebBIOS to configure RAID, by pressing the **Ctrl** and **H** keys during bootup.

Configuring the Virtual KVM

Before You Begin

You must log in as a user with admin privileges to configure the virtual KVM.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kvm**	Enters KVM command mode.
Step 2	Server /kvm # **set enabled** {**yes** | **no**}	Enables or disables the virtual KVM.
Step 3	Server /kvm # **set encrypted** {**yes** | **no**}	If encryption is enabled, the server encrypts all video information sent through the KVM.
Step 4	Server /kvm # **set kvm-port** *port*	Specifies the port used for KVM communication.
Step 5	Server /kvm # **set local-video** {**yes** | **no**}	If local video is **yes**, the KVM session is also displayed on any monitor attached to the server.
Step 6	Server /kvm # **set max-sessions** *sessions*	Specifies the maximum number of concurrent KVM sessions allowed. The *sessions* argument is an integer between 1 and 4.
Step 7	Server /kvm # **commit**	Commits the transaction to the system configuration.
Step 8	Server /kvm # **show** [**detail**]	(Optional) Displays the virtual KVM configuration.

This example configures the virtual KVM and displays the configuration:

```
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# set encrypted no
Server /kvm *# set kvm-port 2068
Server /kvm *# set max-sessions 4
Server /kvm *# set local-video yes
Server /kvm *# commit
Server /kvm # show detail
KVM Settings:
    Encryption Enabled: no
    Max Sessions: 4
    Local Video: yes
    Active Sessions: 0
    Enabled: yes
    KVM Port: 2068

Server /kvm #
```

What to Do Next

Launch the virtual KVM from the GUI.

Enabling the Virtual KVM

Before You Begin

You must log in as a user with admin privileges to enable the virtual KVM.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kvm**	Enters KVM command mode.
Step 2	Server /kvm # **set enabled yes**	Enables the virtual KVM.
Step 3	Server /kvm # **commit**	Commits the transaction to the system configuration.
Step 4	Server /kvm # **show** [**detail**]	(Optional) Displays the virtual KVM configuration.

This example enables the virtual KVM:

```
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# commit
Server /kvm # show
Encryption Enabled Local Video      Active Sessions Enabled KVM Port
------------------ ---------------- --------------- ------- --------
no                 yes              0               yes     2068

Server /kvm #
```

Disabling the Virtual KVM

Before You Begin

You must log in as a user with admin privileges to disable the virtual KVM.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope kvm**	Enters KVM command mode.
Step 2	Server /kvm # **set enabled no**	Disables the virtual KVM. **Note** Disabling the virtual KVM disables access to the virtual media feature, but does not detach the virtual media devices if virtual media is enabled.

	Command or Action	Purpose
Step 3	Server /kvm # **commit**	Commits the transaction to the system configuration.
Step 4	Server /kvm # **show** [**detail**]	(Optional) Displays the virtual KVM configuration.

This example disables the virtual KVM:

```
Server# scope kvm
Server /kvm # set enabled no
Server /kvm *# commit
Server /kvm # show
Encryption Enabled Local Video      Active Sessions Enabled KVM Port
------------------ ---------------- --------------- ------- --------
no                 yes              0               no      2068

Server /kvm #
```

Configuring Virtual Media

Before You Begin

You must log in as a user with admin privileges to configure virtual media.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope vmedia**	Enters virtual media command mode.
Step 2	Server /vmedia # **set enabled** {**yes** | **no**}	Enables or disables virtual media. By default, virtual media is disabled. **Note** Disabling virtual media detaches the virtual CD, virtual floppy, and virtual HDD devices from the host.
Step 3	Server /vmedia # **set encrypted** {**yes** | **no**}	Enables or disables virtual media encryption.
Step 4	Server /vmedia # **commit**	Commits the transaction to the system configuration.
Step 5	Server /vmedia # **show** [**detail**]	(Optional) Displays the virtual media configuration.

This example configures virtual media encryption:

```
Server# scope vmedia
Server /vmedia # set enabled yes
Server /vmedia *# set encrypted yes
Server /vmedia *# commit
Server /vmedia # show detail
vMedia Settings:
    Encryption Enabled: yes
    Enabled: yes
    Max Sessions: 1
    Active Sessions: 0
Server /vmedia #
```

What to Do Next

Use the KVM to attach virtual media devices to a host.

Managing Serial over LAN

Serial Over LAN

Serial over LAN (SoL) is a mechanism that enables the input and output of the serial port of a managed system to be redirected via an SSH session over IP. SoL provides a means of reaching the host console via CIMC.

Guidelines and Restrictions for Serial Over LAN

For redirection to SoL, the server console must have the following configuration:

- console redirection to serial port A
- no flow control
- baud rate the same as configured for SoL
- VT-100 terminal type
- legacy OS redirection disabled

The SoL session will display line-oriented information such as boot messages, and character-oriented screen menus such as BIOS setup menus. If the server boots an operating system or application with a bitmap-oriented display, such as Windows, the SoL session will no longer display. If the server boots a command-line-oriented operating system (OS), such as Linux, you may need to perform additional configuration of the OS in order to properly display in an SoL session.

In the SoL session, your keystrokes are transmitted to the console except for the function key F2. To send an F2 to the console, press the Escape key, then press 2.

Configuring Serial Over LAN

Before You Begin

You must log in as a user with admin privileges to configure SoL.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope sol**	Enters SoL command mode.

	Command or Action	Purpose
Step 2	Server /sol # **set enabled** {**yes** | **no**}	Enables or disables SoL on this server.
Step 3	Server /sol # **set baud-rate** {**9600** | **19200** | **38400** | **57600** | **115200**}	Sets the serial baud rate the system uses for SoL communication. **Note** The baud rate must match the baud rate configured in the server serial console.
Step 4	Server /sol # **commit**	Commits the transaction to the system configuration.
Step 5	Server /sol # **show** [**detail**]	(Optional) Displays the SoL settings.

This example configures SoL:

```
Server# scope sol
Server /sol # set enabled yes
Server /sol *# set baud-rate 115200
Server /sol *# commit
Server /sol # show
Enabled Baud Rate(bps)
------- ---------------
yes     115200

Server /sol #
```

Launching Serial Over LAN

Procedure

	Command or Action	Purpose
Step 1	Server# **connect host**	Opens an SoL connection to the redirected server console port. You can enter this command in any command mode.

What to Do Next

Press **Ctrl** and **X** keys to disconnect from SoL and return to the CLI session.

Note When you enable SoL, the output from the serial port is redirected; therefore, when you try to session into the host from Cisco IOS CLI, you will not see any output.

CHAPTER 7

Managing User Accounts

This chapter includes the following sections:

- Configuring Local Users, page 73
- Active Directory, page 74
- Viewing User Sessions, page 77
- Terminating a User Session, page 78

Configuring Local Users

Before You Begin

You must log in as a user with admin privileges to configure or modify local user accounts.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope user** *usernumber*	Enters user command mode for user number *usernumber*.
Step 2	Server /user # **set enabled** {**yes** | **no**}	Enables or disables the user account on the CIMC.
Step 3	Server /user # **set name** *username*	Specifies the username for the user.
Step 4	Server /user # **set password**	You are prompted to enter the password twice.
Step 5	Server /user # **set role** {**readonly** | **user** | **admin**}	Specifies the role assigned to the user. The roles are as follows: • readonly—This user can view information but cannot make any changes. • user—This user can do the following: • View all information

	Command or Action	Purpose
		• Manage the power control options such as power on, power cycle, and power off • Launch the KVM console and virtual media • Clear all logs • Toggle the locator LED • admin—This user can perform all actions available through the GUI, CLI, and IPMI.
Step 6	Server /user # **commit**	Commits the transaction to the system configuration.

This example configures user 5 as an admin:

```
Server# scope user 5
Server /user # set enabled yes
Server /user *# set name john
Server /user *# set password
Please enter password:
Please confirm password:
Server /user *# set role readonly
Server /user *# commit
Server /user #  show
User   Name             Role     Enabled
------ ---------------- -------- --------
5      john             readonly yes
```

Active Directory

Active Directory is a technology that provides a variety of network services including LDAP-like directory services, Kerberos-based authentication, and DNS-based naming. The CIMC utilizes the Kerberos-based authentication service of Active Directory.

When Active Directory is enabled in the CIMC, user authentication and role authorization is performed by Active Directory for user accounts not found in the local user database.

By enabling encryption in the configuration of Active Directory on the server, you can require the server to encrypt data sent to Active Directory.

Configuring the Active Directory Server

The CIMC can be configured to use Active Directory for user authentication and authorization. To use Active Directory, configure users with an attribute that holds the user role and locale information for the CIMC. You can use an existing LDAP attribute that is mapped to the CIMC user roles and locales or you can modify the Active Directory schema to add a new custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1. For more information about altering the Active Directory schema, see http://technet.microsoft.com/en-us/library/bb727064.aspx.

Use this procedure to create a custom attribute on the Active Directory server.

Note This example creates a custom attribute named CiscoAVPair, but you can also use an existing LDAP attribute that is mapped to the CIMC user roles and locales.

Procedure

Step 1 Ensure that the Active Directory schema snap-in is installed.

Step 2 Using the Active Directory schema snap-in, add a new attribute with the following properties:

Properties	Value
Common Name	CiscoAVPair
LDAP Display Name	CiscoAVPair
Unique X500 Object ID	1.3.6.1.4.1.9.287247.1
Description	CiscoAVPair
Syntax	Case Sensitive String

Step 3 Add the CiscoAVPair attribute to the user class using the Active Directory snap-in:

a) Expand the **Classes** node in the left pane and type U to select the user class.
b) Click the **Attributes** tab and click **Add**.
c) Type C to select the CiscoAVPair attribute.
d) Click **OK**.

Step 4 Add the following user role values to the CiscoAVPair attribute, for the users that you want to have access to CIMC:

Role	CiscoAVPair Attribute Value
admin	shell:roles="admin"
user	shell:roles="user"
read-only	shell:roles="read-only"

Note For more information about adding values to attributes, see http://technet.microsoft.com/en-us/library/bb727064.aspx.

What to Do Next

Use the CIMC to configure Active Directory.

Configuring Active Directory in CIMC

Configure Active Directory (AD) in CIMC when you want to use an AD server for local user authentication and authorization.

Before You Begin

You must log in as a user with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope ldap**	Enters the LDAP command mode for AD configuration.
Step 2	Server /ldap # **set enabled** {**yes** | **no**}	Enables or disables AD. When AD is enabled, user authentication and role authorization is performed by AD for user accounts not found in the local user database.
Step 3	Server /ldap # **set timeout** *seconds*	Specifies the number of seconds the CIMC waits until the LDAP search operation times out.
Step 4	Server /ldap # **set encrypted** {**yes** | **no**}	If encryption is enabled, the server encrypts all information sent to AD.
Step 5	Server /ldap # **set base-dn** *domain-name*	Specifies the domain that all users must be in.
Step 6	Server /ldap # **set attribute** *name*	Specify an LDAP attribute that contains the role and locale information for the user. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. You can use an existing LDAP attribute that is mapped to the CIMC user roles and locales or you can create a custom attribute, such as the CiscoAVPair attribute, which has the following attribute ID: `1.3.6.1.4.1.9.287247.1` **Note** If you do not specify this property, user access is restricted to read-only.
Step 7	Server /ldap # **commit**	Commits the transaction to the system configuration.
Step 8	Server /ldap # **show** [**detail**]	(Optional) Displays the AD configuration.

This example configures AD using the CiscoAVPair attribute:

```
Server# scope ldap
Server /ldap # set enabled yes

Server /ldap *# set timeout 60
Server /ldap *# set encrypted yes
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# commit
Server /ldap # show detail
LDAP Settings:
    Domain Controller 1: 192.0.20.123
    Domain Controller 2: 0.0.0.0
    Domain Controller 3: 0.0.0.0
    BaseDN: example.com
    Encrypted: yes
    Timeout: 60
    Enabled: yes
    Attribute: CiscoAvPair
    Group Authorization: no
    Global Catalog 1: 192.0.20.11
    Global Catalog 2: 0.0.0.0
    Global Catalog 3: 0.0.0.0

Server /ldap #
```

Viewing User Sessions

Procedure

	Command or Action	Purpose
Step 1	Server# **show user-session**	Displays information about current user sessions.

The command output displays the following information about current user sessions:

Name	Description
Session ID column	The unique identifier for the session.
Username column	The username for the user.
IP Address column	The IP address from which the user accessed the server.
Type column	The method by which the user accessed the server. For example, CLI, vKVM, and so on.
Action column	If your user account is assigned the **admin** user role, this column displays **Terminate** if you can force the associated user session to end. Otherwise it displays **N/A**. **Note** You cannot terminate your current session from this tab.

This example displays information about current user sessions:

```
Server# show user-session
ID     Name             IP Address        Type         Killable
------ ---------------- ----------------- ------------ --------
15     admin            10.20.30.138      CLI          yes

Server /user #
```

Terminating a User Session

Before You Begin

You must log in as a user with admin privileges to terminate a user session.

Procedure

	Command or Action	Purpose
Step 1	Server# **show user-session**	Displays information about current user sessions. The user session to be terminated must be eligible to be terminated (killable) and must not be your own session.
Step 2	Server /user-session # **scope user-session** *session-number*	Enters user session command mode for the numbered user session that you want to terminate.
Step 3	Server /user-session # **terminate**	Terminates the user session.

This example shows how the admin at user session 10 terminates user session 15:

```
Server# show user-session
ID     Name             IP Address        Type         Killable
------ ---------------- ----------------- ------------ --------
10     admin            10.20.41.234      CLI          yes
15     admin            10.20.30.138      CLI          yes
Server# scope user-session 15
Server /user-session # terminate
User session 15 terminated.

Server /user-session #
```

CHAPTER 8

Configuring Network-Related Settings

This chapter includes the following sections:

- CIMC NIC Configuration, page 79
- Configuring Common Properties, page 81
- Configuring IPv4, page 82
- Configuring the Server VLAN, page 83
- Network Security Configuration, page 84

CIMC NIC Configuration

CIMC NICs

Two NIC modes are available for connection to the CIMC.

NIC Mode

The CIMC network settings determine which ports can reach the CIMC. The following network mode options are available, depending on your platform:

- Dedicated—A connection to the CIMC is available through the management Ethernet port or ports.
- Shared LOM—A connection to the CIMC is available through the LAN On Motherboard (LOM) Ethernet host ports and through the router's PCIe and MGF interfaces.

Note In shared LOM mode, all host ports must belong to the same subnet.

NIC Redundancy

The CIMC network redundancy settings determine how NIC redundancy is handled:

- None—Redundancy is not available.

- Active-Standby—One port fails over to the other.

The available redundancy modes vary depending on the selected network mode and your platform.

Configuring CIMC NICs

Use this procedure to set the NIC mode and NIC redundancy.

Before You Begin

You must log in as a user with admin privileges to configure the NIC.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters the CIMC network command mode.
Step 3	Server /cimc/network # **set mode** {**dedicated** | **shared_lom**}	Sets the NIC mode to one of the following: • Dedicated—The management Ethernet port is used to access the CIMC. • Shared LOM—The LAN On Motherboard (LOM) Ethernet host ports are used to access the CIMC. **Note** If you select Shared LOM, make sure that all host ports belong to the same subnet.
Step 4	Server /cimc/network # **set redundancy** {**none** | **active-standby**}	Sets the NIC redundancy mode when the NIC mode is Shared LOM. The redundancy mode can be one of the following: • **none**—The LOM Ethernet ports operate independently and do not fail over if there is a problem. • **active-standby**—If one LOM Ethernet port fails, traffic fails over to another LOM port.
Step 5	Server /cimc/network # **set interface** {**console** | **ge1** | **ge2** | **ge3** | **ge1-ge2** | **ge1-ge3** | **ge2-ge3** | **ge1-ge2-ge3**}	Sets the NIC interface to one of the following: • **console**—Internal interface, which is used to connect the router's PCIe interface to the E-Series Server. • **ge1**—Internal interface, which is used to access CIMC over a high-speed backplane switch. • **ge2**—External interface, which can be used as a primary interface or as a backup interface. • **ge3**—External interface, which can be used as a primary interface or as a backup interface.

	Command or Action	Purpose
		• **ge1-ge2**—Failover between the GE1 and GE2 interfaces (active-standby only). • **ge1-ge3**—Failover between the GE1 and GE3 interfaces (active-standby only). • **ge2-ge3**—Failover between the GE2 and GE3 interfaces (active-standby only). • **ge1-ge2-ge3**—Failover between the GE1, GE2, and GE3 interfaces (active-standby only). **Note** All interface options that involve the GE3 interface are applicable for double-wide E-Series Servers only.
Step 6	Server /cimc/network # **commit**	Commits the transaction to the system configuration. **Note** The available NIC mode and NIC redundancy mode options may vary depending on your platform. If you select a mode not supported by your server, an error message displays when you save your changes.

This example configures the CIMC network interface:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set mode dedicated
Server /cimc/network *# commit
Server /cimc/network #
```

Configuring Common Properties

Use common properties to describe your server.

Before You Begin

You must log in as a user with admin privileges to configure common properties.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters the CIMC network command mode.
Step 3	Server /cimc/network # **set hostname** *host-name*	Specifies the name of the host.

	Command or Action	Purpose
Step 4	Server /cimc/network # **commit**	Commits the transaction to the system configuration.

This example configures the common properties:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set hostname Server
Server /cimc/network *# commit
Server /cimc/network #
```

Configuring IPv4

Before You Begin

You must log in as a user with admin privileges to configure IPv4 network settings.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters the CIMC network command mode.
Step 3	Server /cimc/network # **set dhcp-enabled** {**yes** | **no**}	Selects whether the CIMC uses DHCP. **Note** If DHCP is enabled, we recommend that the DHCP server be configured to reserve a single IP address for the CIMC. If the CIMC is reachable through multiple ports on the server, the single IP address must be reserved for the full range of MAC addresses of those ports.
Step 4	Server /cimc/network # **set v4-addr** *ipv4-address*	Specifies the IP address for the CIMC.
Step 5	Server /cimc/network # **set v4-netmask** *ipv4-netmask*	Specifies the subnet mask for the IP address.
Step 6	Server /cimc/network # **set v4-gateway** *gateway-ipv4-address*	Specifies the gateway for the IP address.
Step 7	Server /cimc/network # **set dns-use-dhcp** {**yes** | **no**}	Selects whether the CIMC retrieves the DNS server addresses from DHCP.
Step 8	Server /cimc/network # **set preferred-dns-server** *dns1-ipv4-address*	Specifies the IP address of the primary DNS server.

	Command or Action	Purpose
Step 9	Server /cimc/network # **set alternate-dns-server** *dns2-ipv4-address*	Specifies the IP address of the secondary DNS server.
Step 10	Server /cimc/network # **commit**	Commits the transaction to the system configuration.
Step 11	Server /cimc/network # **show** [**detail**]	(Optional) Displays the IPv4 network settings.

This example configures and displays the IPv4 network settings:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set dhcp-enabled no
Server /cimc/network *# set v4-addr 10.20.30.11
Server /cimc/network *# set v4-netmask 255.255.248.0
Server /cimc/network *# set v4-gateway 10.20.30.1
Server /cimc/network *# set dns-use-dhcp-enabled no
Server /cimc/network *# set preferred-dns-server 192.168.30.31
Server /cimc/network *# set alternate-dns-server 192.168.30.32
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
    IPv4 Address: 10.20.30.11
    IPv4 Netmask: 255.255.248.0
    IPv4 Gateway: 10.20.30.1
    DHCP Enabled: no
    Obtain DNS Server by DHCP: no
    Preferred DNS: 192.168.30.31
    Alternate DNS: 192.168.30.32
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Hostname: Server
    MAC Address: 01:23:45:67:89:AB
    NIC Mode: dedicated
    NIC Redundancy: none

Server /cimc/network #
```

Configuring the Server VLAN

Before You Begin

You must be logged in as admin to configure the server VLAN.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters the CIMC network command mode.

	Command or Action	Purpose
Step 3	Server /cimc/network # **set vlan-enabled** {**yes** | **no**}	Selects whether the CIMC is connected to a VLAN.
Step 4	Server /cimc/network # **set vlan-id** *id*	Specifies the VLAN number.
Step 5	Server /cimc/network # **set vlan-priority** *priority*	Specifies the priority of this system on the VLAN.
Step 6	Server /cimc/network # **commit**	Commits the transaction to the system configuration.
Step 7	Server /cimc/network # **show** [**detail**]	(Optional) Displays the network settings.

This example configures the server VLAN:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set vlan-enabled yes
Server /cimc/network *# set vlan-id 10
Server /cimc/network *# set vlan-priority 32
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
    IPv4 Address: 10.20.30.11
    IPv4 Netmask: 255.255.248.0
    IPv4 Gateway: 10.20.30.1
    DHCP Enabled: yes
    Obtain DNS Server by DHCP: no
    Preferred DNS: 192.168.30.31
    Alternate DNS: 192.168.30.32
    VLAN Enabled: yes
    VLAN ID: 10
    VLAN Priority: 32
    Hostname: Server
    MAC Address: 01:23:45:67:89:AB
    NIC Mode: dedicated
    NIC Redundancy: none

Server /cimc/network #
```

Network Security Configuration

Network Security

The CIMC uses IP blocking as network security. IP blocking prevents the connection between a server or website and certain IP addresses or ranges of addresses. IP blocking effectively bans undesired connections from those computers to a website, mail server, or other Internet servers.

IP banning is commonly used to protect against denial of service (DoS) attacks. CIMC bans IP addresses by setting up an IP blocking fail count.

Configuring Network Security

Configure network security if you want to set up an IP blocking fail count.

Before You Begin

You must log in as a user with admin privileges to configure network security.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters the CIMC network command mode.
Step 3	Server /cimc/network # **scope ipblocking**	Enters the IP blocking command mode.
Step 4	Server /cimc/network/ipblocking # **set enabled** {**yes** | **no**}	Enables or disables IP blocking.
Step 5	Server /cimc/network/ipblocking # **set fail-count** *fail-count*	Sets the number of times a user can attempt to log in unsuccessfully before the system locks that user out for a specified length of time. The number of unsuccessful login attempts must occur within the time frame specified in the IP Blocking Fail Window field. Enter an integer between 3 and 10.
Step 6	Server /cimc/network/ipblocking # **set fail-window** *fail-seconds*	Sets the length of time, in seconds, in which the unsuccessful login attempts must occur in order for the user to be locked out. Enter an integer between 60 and 120.
Step 7	Server /cimc/network/ipblocking # **set penalty-time** *penalty-seconds*	Sets the number of seconds the user remains locked out if they exceed the maximum number of login attempts within the specified time window. Enter an integer between 300 and 900.
Step 8	Server /cimc/network/ipblocking # **commit**	Commits the transaction to the system configuration.

This example configures IP blocking:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope ipblocking
Server /cimc/network/ipblocking # set enabled yes
Server /cimc/network/ipblocking *# set fail-count 5
Server /cimc/network/ipblocking *# set fail-window 90
Server /cimc/network/ipblocking *# set penalty-time 600
Server /cimc/network/ipblocking *# commit
Server /cimc/network/ipblocking #
```

CHAPTER 9

Configuring Communication Services

This chapter includes the following sections:

- Configuring HTTP, page 87
- Configuring SSH, page 88
- Configuring IPMI, page 89
- Configuring SNMP, page 90

Configuring HTTP

Before You Begin

You must log in as a user with admin privileges to configure HTTP.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope http**	Enters the HTTP command mode.
Step 2	Server /http # **set enabled** {**yes** | **no**}	Enables or disables HTTP and HTTPS service on the CIMC.
Step 3	Server /http # **set http-port** *number*	Sets the port to use for HTTP communication. The default is 80.
Step 4	Server /http # **set https-port** *number*	Sets the port to use for HTTPS communication. The default is 443.
Step 5	Server /http # **set timeout** *seconds*	Sets the number of seconds to wait between HTTP requests before the CIMC times out and terminates the session. Enter an integer between 60 and 10,800. The default is 1,800 seconds.

	Command or Action	Purpose
Step 6	Server /http # **commit**	Commits the transaction to the system configuration.

This example configures HTTP for the CIMC:

```
Server# scope http
Server /http # set enabled yes
Server /http *# set http-port 80
Server /http *# set https-port 443
Server /http *# set timeout 1800
Server /http *# commit
Server /http # show
HTTP Port  HTTPS Port Timeout  Active Sessions Enabled
---------- ---------- -------- --------------- -------
80         443        1800     0               yes

Server /http #
```

Configuring SSH

Before You Begin

You must log in as a user with admin privileges to configure SSH.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope ssh**	Enters the SSH command mode.
Step 2	Server /ssh # **set enabled** {**yes** | **no**}	Enables or disables SSH on the CIMC.
Step 3	Server /ssh # **set ssh-port** *number*	Sets the port to use for secure shell access. The default is 22.
Step 4	Server /ssh # **set timeout** *seconds*	Sets the number of seconds to wait before the system considers an SSH request to have timed out. Enter an integer between 60 and 10,800. The default is 300 seconds.
Step 5	Server /ssh # **commit**	Commits the transaction to the system configuration.
Step 6	Server /ssh # **show** [**detail**]	(Optional) Displays the SSH configuration.

This example configures SSH for the CIMC:

```
Server# scope ssh
Server /ssh # set enabled yes
Server /ssh *# set ssh-port 22
Server /ssh *# set timeout 600
Server /ssh *# commit
Server /ssh # show
```

```
SSH Port   Timeout  Active Sessions Enabled
---------- -------- --------------- -------
22         600      1               yes

Server /ssh #
```

Configuring IPMI

IPMI Over LAN

Intelligent Platform Management Interface (IPMI) defines the protocols for interfacing with a service processor embedded in a server platform. This service processor is called a Baseboard Management Controller (BMC) and resides on the server motherboard. The BMC links to a main processor and other on-board elements using a simple serial bus.

During normal operations, IPMI lets a server operating system obtain information about system health and control system hardware. For example, IPMI enables the monitoring of sensors, such as temperature, fan speeds and voltages, for proactive problem detection. If the server temperature rises above specified levels, the server operating system can direct the BMC to increase fan speed or reduce processor speed to address the problem.

Configuring IPMI over LAN

Configure IPMI over LAN when you want to manage the CIMC with IPMI messages.

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope ipmi**	Enters the IPMI command mode.
Step 2	Server /ipmi # **set enabled** {**yes** | **no**}	Enables or disables IPMI access on this server.
Step 3	Server /ipmi # **set privilege-level** {**readonly** | **user** | **admin**}	Specifies the highest privilege level that can be assigned to an IPMI session on this server. This can be: • **readonly** —IPMI users can view information but cannot make any changes. If you select this option, IPMI users with the "Administrator", "Operator", or "User" user roles can only create read-only IPMI sessions, regardless of their other IPMI privileges. • **user** —IPMI users can perform some functions but cannot perform administrative tasks. If you select this option, IPMI users with the "Administrator" or "Operator" user role can create user and read-only sessions on this server.

	Command or Action	Purpose
		• **admin** —IPMI users can perform all available actions. If you select this option, IPMI users with the "Administrator" user role can create admin, user, and read-only sessions on this server.
Step 4	Server /ipmi # **set encryption-key** *key*	Sets the IPMI encryption key to use for IPMI communications. The key value must be 40 hexadecimal numbers.
Step 5	Server /ipmi # **commit**	Commits the transaction to the system configuration.

This example configures IPMI over LAN for the CIMC:

```
Server# scope ipmi
Server /ipmi # set enabled yes
Server /ipmi *# set privilege-level admin
Server /ipmi *# set encryption-key abcdef01234567890abcdef01234567890abcdef
Server /ipmi *# commit
Server /ipmi # show
Enabled Encryption Key                            Privilege Level Limit
------- ---------------------------------------- ---------------------
yes     abcdef01234567890abcdef01234567890abcdef admin

Server /ipmi #
```

Configuring SNMP

SNMP

The Cisco UCS E-Series Servers support the Simple Network Management Protocol (SNMP) for viewing server configuration and status and for sending fault and alert information by SNMP traps.

Configuring SNMP Properties

Before You Begin

You must log in as a user with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope snmp**	Enters SNMP command mode.
Step 2	Server /snmp # **set enabled** {**yes** | **no**}	Enables or disables SNMP. **Note** SNMP must be enabled and saved before additional SNMP configuration commands are accepted.

	Command or Action	Purpose
Step 3	Server /snmp # **commit**	Commits the transaction to the system configuration.
Step 4	Server /snmp # **set community-str** *community*	Specifies the default SNMP v1 or v2c community name that CIMC includes on any trap messages it sends to the SNMP host. The name can be up to 18 characters.
Step 5	Server /snmp # **set sys-contact** *contact*	Specifies the system contact person responsible for the SNMP implementation. The contact information can be up to 254 characters, such as an email address or a name and telephone number. To enter a value that contains spaces, you must enclose the entry with quotation marks.
Step 6	Server /snmp # **set sys-location** *location*	Specifies the location of the host on which the SNMP agent (server) runs. The location information can be up to 254 characters. To enter a value that contains spaces, you must enclose the entry with quotation marks.
Step 7	Server /snmp # **commit**	Commits the transaction to the system configuration.

This example configures the SNMP properties and commits the transaction:

```
Server# scope snmp
Server /snmp # set enabled yes
Server /snmp *# commit
Server /snmp # set community-str cimcpublic
Server /snmp *# set sys-contact "User Name <username@example.com> +1-408-555-1212"
Server /snmp *# set sys-location "San Jose, California"
Server /snmp *# commit
Server /snmp #  show detail
SNMP Settings:
    SNMP Port: 161
    System Contact: User Name <username@example.com> +1-408-555-1212
    System Location: San Jose, California
    SNMP Community: cimcpublic
    SNMP Trap community: 0
    Enabled: yes
    SNMP Trap Version: 1
    SNMP Inform Type: inform

Server /snmp #
```

What to Do Next

Configure SNMP trap settings as described in Configuring SNMP Trap Settings, on page 91.

Configuring SNMP Trap Settings

Before You Begin

- You must log in with admin privileges to perform this task.
- SNMP must be enabled and saved before trap settings can be configured.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope snmp**	Enters the SNMP command mode.
Step 2	Server /snmp # **set trap-community-str** *string*	Enter the name of the SNMP community to which trap information should be sent.
Step 3	Server /snmp # **set trap-ver** {**1** | **2**}	Specify the desired SNMP version of the trap message.
Step 4	Server /snmp # **set inform-type** {**trap** | **inform**}	Specifies whether SNMP notification messages are sent as simple traps or as inform requests requiring acknowledgment by the receiver.
Step 5	Server /snmp # **scope trap-destination** *number*	Enters the SNMP trap destination command mode for the specified destination. Four SNMP trap destinations are available. The destination *number* is an integer between 1 and 4.
Step 6	Server /snmp/trap-destination # **set enabled** {**yes** | **no**}	Enables or disables the SNMP trap destination.
Step 7	Server /snmp/trap-destination # **set addr** *ip-address*	Specifies the destination IP address to which SNMP trap information is sent.
Step 8	Server /snmp/trap-destination # **commit**	Commits the transaction to the system configuration.

This example configures general SNMP trap settings and trap destination number 1 and commits the transaction:

```
Server# scope snmp
Server /snmp # set trap-community-str public
Server /snmp *# set trap-ver 2
Server /snmp *# set inform-type inform
Server /snmp *# scope trap-destination 1
Server /snmp/trap-destination *# set enabled yes
Server /snmp/trap-destination *# set addr 192.0.20.41
Server /snmp/trap-destination *# commit
Server /snmp/trap-destination # show
Trap Destination IP Address       Enabled
---------------- ---------------- --------
1                192.0.20.41      yes
```

Sending a Test SNMP Trap Message

Before You Begin

You must log in with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope snmp**	Enters the SNMP command mode.
Step 2	Server /snmp # **scope trap-destination** *number*	Enters the SNMP trap destination command mode for the specified destination. Four SNMP trap destinations are available. The destination *number* is an integer between 1 and 4.
Step 3	Server /snmp/trap-destination # **sendSNMPtrap**	Sends an SNMPv1 test trap to the configured SNMP trap destination. **Note** The trap must be configured and enabled in order to send a test message.

This example sends a test message to SNMP trap destination 1:

```
Server# scope snmp
Server /snmp # scope trap-destination 1
Server /snmp/trap-destination # sendSNMPtrap
SNMP Test Trap sent to Destination:1
Server /snmp/trap-destination #
```

CHAPTER 10

Managing Certificates

This chapter includes the following sections:

- Managing the Server Certificate, page 95
- Generating a Certificate Signing Request, page 95
- Creating a Self-Signed Certificate, page 97
- Uploading a Server Certificate, page 99

Managing the Server Certificate

You can generate a certificate signing request (CSR) to obtain a new certificate, and you can upload the new certificate to the CIMC to replace the current server certificate. The server certificate may be signed either by a public Certificate Authority (CA), such as Verisign, or by your own certificate authority.

Procedure

Step 1 Generate the CSR from the CIMC.

Step 2 Submit the CSR file to a certificate authority that will issue and sign your certificate. If your organization generates its own self-signed certificates, you can use the CSR file to generate a self-signed certificate.

Step 3 Upload the new certificate to the CIMC.

Note The uploaded certificate must be created from a CSR generated by the CIMC. Do not upload a certificate that was not created by this method.

Generating a Certificate Signing Request

Before You Begin

You must log in as a user with admin privileges to configure certificates.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope certificate**	Enters the certificate command mode.
Step 2	Server /certificate # **generate-csr**	Launches a dialog for the generation of a certificate signing request (CSR).

You will be prompted to enter the following information for the certificate signing request:

Common Name (CN)	The fully qualified hostname of the CIMC.
Organization Name (O)	The organization requesting the certificate.
Organization Unit (OU)	The organizational unit.
Locality (L)	The city or town in which the company requesting the certificate is headquartered.
StateName (S)	The state or province in which the company requesting the certificate is headquartered.
Country Code (CC)	The two-letter ISO country code for the country in which the company is headquartered.
Email	The administrative email contact at the company.

After you have entered the requested information, the system will generate and display a certificate signing request in the console output. A CSR file will not be created, but you can copy the CSR information from the console output and paste the information into a text file.

This example generates a certificate signing request:

```
Server# scope certificate
Server /certificate # generate-csr
Common Name (CN): test.example.com
Organization Name (O): Example, Inc.
Organization Unit (OU): Test Department
Locality (L): San Jose
StateName (S): CA
Country Code (CC): US
Email: user@example.com
Continue to generate CSR?[y|N]y


-----BEGIN CERTIFICATE REQUEST-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
```

```
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE REQUEST-----

Copy everything from "-----BEGIN ..."  to "END CERTIFICATE REQUEST-----",
paste to a file, send to your chosen CA for signing,
and finally upload the signed certificate via upload command.
              ---OR---
Continue to self sign CSR and overwrite the current certificate?
All HTTPS and SSH sessions will be disconnected. [y|N]N
```

What to Do Next

Perform one of the following tasks:

- If you do not want to obtain a certificate from a public certificate authority, and if your organization does not operate its own certificate authority, you can allow CIMC to internally generate a self-signed certificate from the CSR and upload it immediately to the server. Type **y** after the final prompt in the example to perform this action.
- If your organization operates its own certificate server for generating self-signed certificates, copy the command output from "-----BEGIN ..." to "END CERTIFICATE REQUEST-----" and paste to a file named csr.txt. Input the CSR file to your certificate server to generate a self-signed certificate.
- If you will obtain a certificate from a public certificate authority, copy the command output from "-----BEGIN ..." to "END CERTIFICATE REQUEST-----" and paste to a file named csr.txt. Submit the CSR file to the certificate authority to obtain a signed certificate.

If you did not use the first option, in which CIMC internally generates and uploads a self-signed certificate, you must upload the new certificate using the **upload** command in certificate command mode.

Creating a Self-Signed Certificate

As an alternative to using a public Certificate Authority (CA) to generate and sign a server certificate, you can operate your own CA and sign your own certificates. This section shows commands for creating a CA and generating a server certificate using the OpenSSL certificate server running on Linux. For detailed information about OpenSSL, see http://www.openssl.org.

Note These commands are to be entered on a Linux server with the OpenSSL package, not in the CIMC CLI.

Before You Begin

Obtain and install a certificate server software package on a server within your organization.

Procedure

	Command or Action	Purpose
Step 1	**openssl genrsa -out** *CA_keyfilename keysize* **Example:** `# openssl genrsa -out ca.key 1024`	This command generates an RSA private key that will be used by the CA. **Note** To allow the CA to access the key without user input, do not use the -des3 option for this command. The specified file name contains an RSA key of the specified key size.
Step 2	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename* **Example:** `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	This command generates a new self-signed certificate for the CA using the specified key. The certificate is valid for the specified period. The command prompts the user for additional certificate information. The certificate server is an active CA.
Step 3	**echo "nsCertType = server" > openssl.conf** **Example:** `# echo "nsCertType = server" > openssl.conf`	This command adds a line to the OpenSSL configuration file to designate the certificate as a server-only certificate. This designation is a defense against a man-in-the-middle attack, in which an authorized client attempts to impersonate the server. The OpenSSL configuration file openssl.conf contains the statement "nsCertType = server".
Step 4	**openssl x509 -req -days** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial 04 -CAkey** *CA_keyfilename* **-out** *server_certfilename* **-extfile openssl.conf** **Example:** `# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf`	This command directs the CA to use your CSR file to generate a server certificate. Your server certificate is contained in the output file.

This example shows how to create a CA and to generate a server certificate signed by the new CA. These commands are entered on a Linux server running OpenSSL.

```
#  /usr/bin/openssl genrsa -out ca.key 1024
Generating RSA private key, 1024 bit long modulus
.............++++++
.....++++++
e is 65537 (0x10001)
#  /usr/bin/openssl req -new -x509 -days 365 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:admin@example.com
#  echo "nsCertType = server" > openssl.conf
#  /usr/bin/openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt
-extfile openssl.conf
Signature ok
subject=/C=US/ST=California/L=San Jose/O=Example Inc./OU=Unit
A/CN=example.com/emailAddress=john@example.com
Getting CA Private Key
#
```

What to Do Next

Upload the new certificate to the CIMC.

Uploading a Server Certificate

Before You Begin

You must log in as a user with admin privileges to upload a certificate.

The certificate to be uploaded must be available as readable text. During the upload procedure, you will copy the certificate text and paste it into the CLI.

Note You must first generate a CSR using the CIMC certificate management CSR generation procedure, and you must use that CSR to obtain the certificate for uploading. Do not upload a certificate that was not obtained by this method.

Note All current HTTPS and SSH sessions are disconnected when the new server certificate is uploaded.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope certificate**	Enters the certificate command mode.
Step 2	Server /certificate # **upload**	Launches a dialog for entering and uploading the new server certificate.

Copy the certificate text, paste it into the console when prompted, and type CTRL+D to upload the certificate.

This example uploads a new certificate to the server:

```
Server# scope certificate
Server /certificate # upload
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE-----
<CTRL+D>
```

CHAPTER 11

Configuring Platform Event Filters

This chapter includes the following sections:

- Platform Event Filters, page 101
- Enabling Platform Event Alerts, page 101
- Disabling Platform Event Alerts, page 102
- Configuring Platform Event Filters, page 102

Platform Event Filters

A platform event filter (PEF) can trigger an action and generate an alert when a critical hardware-related event occurs. For each PEF, you can choose the action to be taken (or take no action) when a platform event occurs. You can also choose to generate and send an alert when a platform event occurs. Alerts are sent as an SNMP trap, so you must configure an SNMP trap destination before the alerts can be sent.

You can globally enable or disable the generation of platform event alerts. When disabled, alerts are not sent even if PEFs are configured to send them.

Enabling Platform Event Alerts

Procedure

	Command or Action	Purpose
Step 1	Server# **scope fault**	Enters the fault command mode.
Step 2	Server /fault # **set platform-event-enabled yes**	Enables platform event alerts.
Step 3	Server /fault # **commit**	Commits the transaction to the system configuration.

	Command or Action	Purpose
Step 4	Server /fault # **show** [**detail**]	(Optional) Displays the platform event alert configuration.

This example enables platform event alerts:

```
Server# scope fault
Server /fault # set platform-event-enabled yes
Server /fault *# commit
Server /fault # show
Platform Event Enabled
-----------------------
yes

Server /fault #
```

Disabling Platform Event Alerts

Procedure

	Command or Action	Purpose
Step 1	Server# **scope fault**	Enters the fault command mode.
Step 2	Server /fault # **set platform-event-enabled no**	Disables platform event alerts.
Step 3	Server /fault # **commit**	Commits the transaction to the system configuration.
Step 4	Server /fault # **show** [**detail**]	(Optional) Displays the platform event alert configuration.

This example disables platform event alerts:

```
Server# scope fault
Server /fault # set platform-event-enabled no
Server /fault *# commit
Server /fault # show
Platform Event Enabled
-----------------------
no

Server /fault #
```

Configuring Platform Event Filters

You can configure actions and alerts for the following platform event filters:

ID	Platform Event Filter
1	Temperature Critical Assert Filter
2	Temperature Warning Assert Filter
3	Voltage Critical Assert Filter
4	Processor Assert Filter
5	Memory Critical Assert Filter
6	Drive Slot Assert Filter
7	LSI Critical Assert Filter
8	LSI Warning Assert Filter

Procedure

	Command or Action	Purpose
Step 1	Server# **scope fault**	Enters the fault command mode.
Step 2	Server /fault # **scope pef** *id*	Enters the platform event filter command mode for the specified event. See the Platform Event Filter table for event ID numbers.
Step 3	Server /fault/pef # **set action** {**none** | **reboot** | **power-cycle** | **power-off**}	Selects the desired system action when this event occurs. The action can be one of the following: • **none** —No system action is taken. • **reboot** —The server is rebooted. • **power-cycle** —The server is power cycled. • **power-off** —The server is powered off.
Step 4	Server /fault/pef # **set send-alert** {**yes** | **no**}	Enables or disables the sending of a platform event alert for this event. **Note** For an alert to be sent, the filter trap settings must be configured properly and platform event alerts must be enabled.
Step 5	Server /fault/pef # **commit**	Commits the transaction to the system configuration.

This example configures the platform event alert for an event:

```
Server# scope fault
Server /fault # scope pef 1
Server /fault/pef # set action reboot
Server /fault/pef # set send-alert yes
Server /fault/pef *# commit
Server /fault/pef # show
Platform Event Filter Event                               Action      Send Alert
--------------------- ----------------------------------- ----------- -----------
1                     Temperature Critical Assert Filter  reboot      yes

Server /fault/pef #
```

What to Do Next

If you configure any PEFs to send an alert, complete the following tasks:

- Enable platform event alerts
- Configure SNMP trap settings

CHAPTER 12

CIMC Firmware Management

This chapter includes the following sections:

- Overview of CIMC Firmware, page 105
- Obtaining Software from Cisco Systems, page 106
- Installing CIMC Firmware from the TFTP Server, page 107
- Activating Installed CIMC Firmware, page 108
- Viewing CIMC Information, page 109

Overview of CIMC Firmware

E-Series Servers use firmware downloaded from cisco.com. This firmware is certified by Cisco to upgrade on a E-Series Server.

The CIMC firmware you download is packaged in a .zip file. After you have downloaded a firmware .zip from Cisco, you can use it to update the firmware on your server. Cisco also provides release notes with each image, which you can obtain from the same website from which you obtained the image.

Caution Do not use the .zip file to update your server.

You use a .bin file to reimage. You must extract the proper .bin upgrade file from this .zip file. You can extract this .bin to a TFTP server or your local machine. You can update using a TFTP server.

Note When you update the firmware, you can either upgrade an older firmware version to a newer one, or downgrade a newer firmware version to an older one.

The CIMC separates the firmware update process into stages to ensure that you can install the firmware to a component while the server is running without affecting its uptime. Because you do not need to reboot the server until after you activate, you can perform that task overnight or during other maintenance periods. When you update firmware, the following stages occur:

Install

During this stage, the CIMC transfers the selected firmware version to the server. The install process always overwrites the firmware in the non-active slot on the server. You can install the firmware using either of the following methods:

- Through a browser client—This method allows you to browse for a firmware image on your computer and install it on the server.
- From a TFTP server—This method allows you to install a firmware image residing on a TFTP server.

Activate

During this stage, the CIMC sets the non-active firmware version as active and reboots the server. When the server reboots, the non-active slot becomes the active slot, and the active slot becomes the non-active slot. The firmware in the new active slot becomes the running version.

Obtaining Software from Cisco Systems

Use this procedure to download drivers, BIOS and CIMC firmware, and the diagnostics image.

Procedure

Step 1 Navigate to http://www.cisco.com/.

Step 2 If you are not already logged in, click **Log In** at the top right-hand edge of the page and log in using your Cisco.com credentials.

Step 3 In the menu bar at the top, click **Support**.
A roll-down menu appears.

Step 4 From the Downloads (center) pane, click **All Downloads** (located at the bottom right corner).
The **Download Software** page appears.

Step 5 From the left pane, click **Products**.

Step 6 From the center pane, click **Unified Computing and Servers**.

Step 7 From the right pane, click **Cisco UCS E-Series Software**.

Step 8 From the right pane, click the name of the server model for which you want to download the software.
The **Download Software** page appears with the following list of software categories that you can download:

- **Unified Computing System (UCSE) Server Drivers**—Contains the following drivers:
  - On-Board Network Drivers for Windows 2008 R2
  - 10G PCIe Network Drivers for Windows 2008 R2 and Linux
  - LSI Drivers (On-Board Hardware RAID Controller) for Windows 2008 R2
  - Intel Drivers for Windows 2008 R2
- **Unified Computing System (UCSE) Server Firmware**—Contains the following BIOS and CIMC firmware images:
  - Double-Wide BIOS

    - Single-Wide BIOS
    - BMC/CIMC Image

- **Unified Computing System (UCSE) Utilites**—Contains the following diagnostics image:
    - On-Board Diag Image

Step 9 Click the appropriate software category link.

Step 10 Click the **Download** button associated with software image that you want to download.
The **End User License Agreement** dialog box appears.

Step 11 (Optional) To download multiple software images, do the following:

a) Click the **Add to cart** button associated with the software images that you want to download.

b) Click the **Download Cart** button located on the top right .
All the images that you added to the cart display.

c) Click the **Download All** button located at the bottom right corner to download all the images.
The **End User License Agreement** dialog box appears.

Step 12 Click **Accept License Agreement**.

Step 13 Do one of the following as appropriate:

- Save the software image file to a local drive.
- If you plan to install the software image from a TFTP server, copy the file to the TFTP server that you want to use.

  The server must have read permission for the destination folder on the TFTP server.

What to Do Next

Install the software image.

Installing CIMC Firmware from the TFTP Server

Before You Begin

Obtain the CIMC firmware from Cisco Systems and store the file on a local TFTP server. See Obtaining Software from Cisco Systems.

Note If you start an update while an update is already in process, both updates will fail.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **update** *tftp-ip-address path-and-filename*	Starts the firmware update. The server will obtain the update firmware at the specified path and file name from the TFTP server at the specified IP address.
Step 3	(Optional) Server /cimc # **show detail**	Displays the progress of the firmware update.

This example updates the firmware:

```
Server# scope cimc
Server /cimc # update 10.20.34.56 //test/dnld-ucs-k9-bundle.1.0.2h.bin
  <CR>  Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /cimc #
```

What to Do Next

Activate the new firmware.

Activating Installed CIMC Firmware

Before You Begin

Install the CIMC firmware on the server.

Note If you start an activation while an update is in process, the activation will fail.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **show** [**detail**]	Displays the available firmware images and status.
Step 3	Server /cimc # **activate** [**1** | **2**]	Activates the selected image. If no image number is specified, the server activates the currently inactive image.

This example activates firmware image 1:

```
Server# scope cimc
Server /cimc # show detail
```

```
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 1.0(0.74)
    FW Image 1 Version: 1.0(0.66a)
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 1.0(0.74)
    FW Image 2 State: RUNNING ACTIVATED

Server /cimc # activate 1
```

Viewing CIMC Information

Before You Begin

Install the CIMC firmware on the server.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **show** [**detail**]	Displays the CIMC firmware, current time, and boot loader version.

This example shows information about CIMC:

```
Server# scope cimc
Server /cimc # show detail
CIMC:
    Firmware Version: 1.0(1.20120417172632)
    Current Time: Thu Apr 26 12:11:44 2012
    Boot-loader Version: 1.0(1.20120417172632).16
```

CHAPTER 13

Viewing Logs

This chapter includes the following sections:

- CIMC Log, page 111
- System Event Log, page 113

CIMC Log

Viewing the CIMC Log

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **scope log**	Enters the CIMC log command mode.
Step 3	Server /cimc/log # **show entries** [**detail**]	Displays CIMC events, including timestamp, the software module that logged the event, and a description of the event.

This example displays the log of CIMC events:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # show entries
Time                Source           Description
------------------- ---------------- ----------------------------------------
1970 Jan 4 18:55:36 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:306:I2c Controller-4 DAT is stuck-low,
 issuing One Clock Pulse.
1970 Jan 4 18:55:36 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:301:I2c Controller-4 Loop:[0].
1970 Jan 4 18:55:36 BMC:kernel:-     "
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:422: Controller-4 has a stuck bus,
attempting to clear it now... "
1970 Jan 4 18:55:36 BMC:kernel:-     "
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:402: Controller-4 Initiating I2c recovery
 sequence. "
1970 Jan 4 18:55:36 BMC:IPMI:480     last message repeated 22 times
1970 Jan 4 18:55:28 BMC:IPMI:480     "  mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
failed to read Bus[f4].Dev[5e]! ErrorStatus[77] "
1970 Jan 4 18:55:33 BMC:IPMI:486     last message repeated 17 times
1970 Jan 4 18:55:28 BMC:IPMI:486     "  mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
failed to read Bus[f4].Dev[b0]! ErrorStatus[77] "
1970 Jan 4 18:55:31 BMC:IPMI:486     last message repeated 17 times
1970 Jan 4 18:55:26 BMC:IPMI:486     "  mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
failed to read Bus[f4].Dev[b2]! ErrorStatus[77] "
1970 Jan 4 18:55:26 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:306:I2c Controller-4 DAT is stuck-low,
 issuing One Clock Pulse.
1970 Jan 4 18:55:26 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:301:I2c Controller-4 Loop:[8].
--More--
```

Clearing the CIMC Log

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **scope log**	Enters the CIMC log command mode.
Step 3	Server /cimc/log # **clear**	Clears the CIMC log.

This example clears the log of CIMC events:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # clear
```

Sending the CIMC Log to a Remote Server

You can configure profiles for one or two remote syslog servers to receive CIMC log entries.

Before You Begin

- The remote syslog server must be configured to receive logs from a remote host.
- The remote syslog server must be configured to receive all types of logs, including authentication-related logs.
- The remote syslog server's firewall must be configured to allow syslog messages to reach the syslog server.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **scope log**	Enters the CIMC log command mode.
Step 3	Server /cimc/log # **scope server** {**1** | **2**}	Selects one of two remote syslog server profiles and enters the command mode for configuring the profile.
Step 4	Server /cimc/log/server # **set server-ip** *ip-address*	Specifies the remote syslog server IP address.
Step 5	Server /cimc/log/server # **set enabled** {**yes** | **no**}	Enables the sending of CIMC log entries to this syslog server.
Step 6	Server /cimc/log/server # **commit**	Commits the transaction to the system configuration.

This example shows how to configure a remote syslog server profile and enable the sending of CIMC log entries:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # scope server 2
Server /cimc/log/server # set server-ip 192.0.2.34
Server /cimc/log/server *# set enabled yes
Server /cimc/log/server *# commit
Server /cimc/log/server #
```

System Event Log

Viewing the System Event Log

Procedure

	Command or Action	Purpose
Step 1	Server# **scope sel**	Enters the system event log (SEL) command mode.
Step 2	Server /sel # **show entries** **[detail]**	For system events, displays timestamp, the severity of the event, and a description of the event. The **detail** keyword displays the information in a list format instead of a table format.

This example displays the system event log:

```
Server# scope sel
Server /sel # show entries
Time                Severity      Description
------------------- ------------- ----------------------------------------
[System Boot]      Informational " LED_PSU_STATUS: Platform sensor, OFF event was asserted"

[System Boot]       Informational " LED_HLTH_STATUS: Platform sensor, GREEN was asserted"
[System Boot]       Normal        " PSU_REDUNDANCY: PS Redundancy sensor, Fully Redundant
was asserted"
[System Boot]       Normal        " PSU2 PSU2_STATUS: Power Supply sensor for PSU2, Power
Supply input lost (AC/DC) was deasserted"
[System Boot]      Informational " LED_PSU_STATUS: Platform sensor, ON event was asserted"

[System Boot]       Informational " LED_HLTH_STATUS: Platform sensor, AMBER was asserted"
[System Boot]       Critical      " PSU_REDUNDANCY: PS Redundancy sensor, Redundancy Lost
was asserted"
[System Boot]       Critical      " PSU2 PSU2_STATUS: Power Supply sensor for PSU2, Power
Supply input lost (AC/DC) was asserted"
[System Boot]       Normal        " HDD_01_STATUS: Drive Slot sensor, Drive Presence was
asserted"
[System Boot]       Critical      " HDD_01_STATUS: Drive Slot sensor, Drive Presence was
deasserted"
[System Boot]      Informational " DDR3_P2_D1_INFO: Memory sensor, OFF event was asserted"

2001-01-01 08:30:16 Warning       " PSU2 PSU2_VOUT: Voltage sensor for PSU2, failure event
 was deasserted"
2001-01-01 08:30:16 Critical     " PSU2 PSU2_VOUT: Voltage sensor for PSU2, non-recoverable
 event was deasserted"
2001-01-01 08:30:15 Informational " LED_PSU_STATUS: Platform sensor, ON event was asserted"

2001-01-01 08:30:15 Informational " LED_HLTH_STATUS: Platform sensor, AMBER was asserted"
2001-01-01 08:30:15 Informational " LED_HLTH_STATUS: Platform sensor, FAST BLINK event was
 asserted"
2001-01-01 08:30:14 Non-Recoverable " PSU2 PSU2_VOUT: Voltage sensor for PSU2, non-recoverable
 event was asserted"
2001-01-01 08:30:14 Critical      " PSU2 PSU2_VOUT: Voltage sensor for PSU2, failure event
 was asserted"
--More--
```

Clearing the System Event Log

Procedure

	Command or Action	Purpose
Step 1	Server# **scope sel**	Enters the system event log command mode.
Step 2	Server /sel # **clear**	You are prompted to confirm the action. If you enter **y** at the prompt, the system event log is cleared.

This example clears the system event log:

```
Server# scope sel
Server /sel # clear
This operation will clear the whole sel.
Continue?[y|N]y
```

CHAPTER 14

Server Utilities

This chapter includes the following sections:

- Exporting Technical Support Data, page 115
- Rebooting the CIMC, page 116
- Resetting the CIMC to Factory Defaults, page 117
- Exporting and Importing the CIMC Configuration, page 117

Exporting Technical Support Data

Perform this task when requested by the Cisco Technical Assistance Center (TAC). This utility creates a summary report containing configuration information, logs and diagnostic data that will help TAC in troubleshooting and resolving a technical issue.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **scope tech-support**	Enters the tech-support command mode.
Step 3	Server /cimc/tech-support # **set tftp-ip** *ip-address*	Specifies the IP address of the TFTP server on which the support data file should be stored.
Step 4	Server /cimc/tech-support # **set path** *path/filename*	Specifies the file name in which the support data should be stored on the server. When you enter this name, include the relative path for the file from the top of the TFTP tree to the desired location.
Step 5	Server /cimc/tech-support # **commit**	Commits the transaction to the system configuration.
Step 6	Server /cimc/tech-support # **start**	Begins the transfer of the support data file to the TFTP server.

	Command or Action	Purpose
Step 7	Server /cimc/tech-support # **show detail**	Displays the status of the file upload.
Step 8	Server /cimc/tech-support # **cancel**	(Optional) Cancels the transfer of the support data file to the TFTP server.

This example creates a support data file and transfers the file to a TFTP server:

```
Server# scope cimc
Server /cimc # scope tech-support
Server /cimc/tech-support # set tftp-ip 10.20.30.41
Server /cimc/tech-support *# set path /user/user1/supportfile
Server /cimc/tech-support *# commit
Server /cimc/tech-support # start
Server /cimc/tech-support # show detail
```

What to Do Next

Provide the generated report file to Cisco TAC.

Rebooting the CIMC

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reboot the CIMC. This procedure is not part of the normal maintenance of a server. After you reboot the CIMC, you are logged off and the CIMC will be unavailable for a few minutes.

Note If you reboot the CIMC while the server is performing power-on self test (POST) or is operating in the Extensible Firmware Interface (EFI) shell, the server will be powered down until the CIMC reboot is complete.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **reboot**	After the prompt to confirm, reboots the CIMC.

This example reboots the CIMC:

```
Server# scope cimc
Server /cimc # reboot
This operation will reboot the CIMC.
Continue?[y|N]y
```

Resetting the CIMC to Factory Defaults

On rare occasions, such as an issue with the current running firmware, troubleshooting a server may require you to reset the CIMC to the factory default. When this happens, all user-configurable settings are reset.

This procedure is not part of the normal server maintenance. After you reset the CIMC, you are logged off and must log in again. You may also lose connectivity and may need to reconfigure the network settings.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **factory-default**	After a prompt to confirm, the CIMC resets to factory defaults.

The CIMC factory defaults include the following conditions:

- SSH is enabled for access to the CIMC CLI.
- HTTPS is enabled for access to the CIMC GUI.
- A single user account exists (user name is **admin**, and the password is **password**).
- DHCP is enabled on the management port.
- The boot order is EFI, CDROM, PXE (using LoM), FDD, HDD.
- KVM and vMedia are enabled.
- USB is enabled.
- SoL is disabled.

This example resets the CIMC to factory defaults:

```
Server# scope cimc
Server /cimc # factory-default
This operation will reset the CIMC configuration to factory default.
All your configuration will be lost.
Continue?[y|N]
```

Exporting and Importing the CIMC Configuration

Exporting and Importing the CIMC Configuration

To perform a backup of the CIMC configuration, you take a snapshot of the system configuration and export the resulting CIMC configuration file to a location on your network. The export operation saves information from the management plane only; it does not back up data on the servers. Sensitive configuration information such as user accounts and the server certificate are not exported.

You can restore an exported CIMC configuration file to the same system or you can import it to another CIMC system, provided that the software version of the importing system is the same as or is configuration-compatible with the software version of the exporting system. When you import a configuration file to another system as a configuration template, you must modify system-specific settings such as IP addresses and host names. An import operation modifies information on the management plane only.

The CIMC configuration file is an XML text file whose structure and elements correspond to the CIMC command modes.

When performing an export or import operation, consider these guidelines:

- You can perform an export or an import while the system is up and running. While an export operation has no impact on the server or network traffic, some modifications caused by an import operation, such as IP address changes, can disrupt traffic or cause a server reboot.
- You cannot execute an export and an import simultaneously.

Exporting the CIMC Configuration

Note For security reasons, this operation does not export user accounts or the server certificate.

Before You Begin

- Obtain the backup TFTP server IP address.
- If you want the option to restore the SNMP configuration information when you import the configuration file, make sure that SNMP is enabled on this server before you create the configuration file. If SNMP is disabled when you export the configuration, CIMC will not apply the SNMP values when the file is imported.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **scope import-export**	Enters the import-export command mode.
Step 3	Server /cimc/import-export # **export-config** *tftp-ip-address path-and-filename*	Starts the backup operation. The configuration file will be stored at the specified path and file name on the TFTP server at the specified IP address.

To determine whether the export operation has completed successfully, use the **show detail** command. To abort the operation, type CTRL+C.

This example shows how to back up the CIMC configuration:

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # export-config 192.0.2.34 /ucs/backups/cimc5.xml
Export config started. Please check the status using "show detail".
```

```
Server /cimc/import-export # show detail
Import Export:
    Operation: EXPORT
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE

Server /cimc/import-export #
```

Importing a CIMC Configuration

Before You Begin

If you want to restore the SNMP configuration information when you import the configuration file, make sure that SNMP is disabled on this server before you do the import. If SNMP is enabled when you perform the import, CIMC does not overwrite the current values with those saved in the configuration file.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the CIMC command mode.
Step 2	Server /cimc # **scope import-export**	Enters the import-export command mode.
Step 3	Server /cimc/import-export # **import-config** *tftp-ip-address path-and-filename*	Starts the import operation. The configuration file at the specified path and file name on the TFTP server at the specified IP address will be imported.

To determine whether the import operation has completed successfully, use the **show detail** command. To abort the operation, type CTRL+C.

This example shows how to import a CIMC configuration:

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # import-config 192.0.2.34 /ucs/backups/cimc5.xml
Import config started. Please check the status using "show detail".
Server /cimc/import-export #
```

CHAPTER 15

Diagnostic Tests

This chapter includes the following sections:

- Diagnostic Tests Overview, page 121
- Mapping the Diagnostics Image to the Host, page 122
- Running Diagnostic Tests, page 123

Diagnostic Tests Overview

Diagnostics is a standalone utility that runs on the E-Series Server independent of the operating system or applications running on the server. If you experience problems with the E-Series Server, you can use diagnostics tests to run a preliminary check and isolate the problem. Diagnostic tests can be executed on the server CPU, memory, and block devices. Block devices include hard drive, USB drive, and SD cards.

If the diagnostic tests pass successfully, it indicates that there is no problem with the server CPU, memory, or block devices. The problem could be with some other hardware component or with the software configuration. Open a service request with Cisco Technical Assistance Center (TAC) at: http://www.cisco.com/cisco/web/support/index.html to isolate the problem.

If the diagnostic tests fail, open a service request with Cisco TAC for further assistance.

Caution Diagnostic tests are non-destructive, but if there is a power or equipment failure when the tests are running, there is a possibility that the disk data might get corrupted. We highly recommend that you backup the data before running these tests.

Basic Workflow for Executing Diagnostic Tests

1. Backup data.
2. The diagnostics image is pre-installed on the E-Series Server at the time of purchase. You can also choose to download the most current diagnostics image from a specified FTP, FTPS, HTTP, or HTTPS server onto the CIMC internal repository.
3. Mount the diagnostics image onto the HDD virtual drive of a USB controller.

4 Set the boot order to make EFI Shell as the first boot device.

5 Reboot the server.

6 Run diagnostic tests from the EFI Shell.

7 Reset the virtual media boot order to its original setting.

Mapping the Diagnostics Image to the Host

Before You Begin

- Backup data.
- Log into CIMC as a user with admin privileges.
- The diagnostics image is pre-installed on the E-Series Server at the time of purchase. You can also choose to download the most current diagnostics image from a specified FTP, FTPS, HTTP, or HTTPS server onto the CIMC internal repository. See Obtaining Software from Cisco Systems.

Note If you start an image update while an update is already in process, both updates will fail.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope remote-install**	Enters the remote install command mode.
Step 2	Server /remote-install # **download-image** {**ftp** | **ftps** | **http** | **https**} *server-ip-address path / filename* [**username** *username* **password** *password*]	Downloads the image from the specified remote server onto the CIMC internal repository. The diagnostics image must have .diag as the file extension. The remote server can be a FTP, FTPS, HTTP, or HTTPS server. If the remote server requires user authentication, you must add the username and password of the remote server. **Note** If the image file exceeds the size limit, an error message is displayed.
Step 3	(Optional) Server /remote-install # **show detail**	Displays the status of the diagnostics image download.
Step 4	Server /remote-install # **map-diagnostics**	Mounts the image on the HDD virtual drive of the USB controller.
Step 5	(Optional) Server /remote-install # **show detail**	Displays the status of the diagnostics image mapping.

This example maps a diagnostics image:

```
Server# scope remote-install
Server /remote-install # download-image ftp 10.20.34.56 pub/diagnostics-image.diag
---
Server /remote-install # show detail
Host Image Info:
  Name: DiagnosticsImage.diag
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Download Successful!!
Server /remote-install # map-diagnostics
---
status: ok
---
Server /remote-install # show detail
Host Image Info:
  Name: DiagnosticsImage.diag
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Image mapped successfully!!
```

What to Do Next

1. Set the boot order to make **EFI Shell** as the first boot device.
2. Reboot the server. The EFI Shell appears.
3. Run diagnostic tests.

Running Diagnostic Tests

From the EFI Shell, use the following procedure to run diagnostic tests.

Before You Begin

- Backup data. All tests are non-destructive, but if there is power or equipment failure when the tests are running, there is a possibility that the disk data might get corrupted. We highly recommend that you backup data before executing these tests.
- Use the CIMC CLI or the CIMC GUI to download and map the diagnostics image onto the HDD virtual drive of the USB controller.
- Reboot the server. The EFI Shell displays.

Procedure

	Command or Action	Purpose
Step 1	Shell > **dir** *virtual-media-drive-name***:**	Displays all the file packages that exist in the specified virtual media drive. The drive name starts with fs0 and can be fs0, fs1, fs2, and so on. **Note** Make sure that you add a colon after the virtual media drive name. For example, **dir fs1:**
Step 2	Shell > *virtual-media-drive-name***:**	Enters the virtual media drive in which the diagnostic file is located.

	Command or Action	Purpose
Step 3	Virtual Media Drive :\> **cp** *package-file-name* **dsh.pkg**	Copies the package file for which you are running diagnostics into the diagnostics shell package file.
Step 4	Virtual Media Drive :\> **dsh**	Enters the Diagnostics Shell. At the confirmation prompt, answer **y**.
Step 5	Server: SRV > **run all**	Executes all available diagnostic tests and displays the progress and status of the tests. Diagnostic tests are run on the server CPU, memory, and block devices. Block devices include hard drive, USB drive, and SD cards. To execute a specific diagnostic test on the server, use the **run** *test-name* command where *test-name* can be one of the following: • **cpux64**—CPU diagnostic test. • **diskx64**—Block devices diagnostic test. Block devices include hard drive, USB drive, and SD cards. • **memoryx64**—Memory diagnostic test. **Note** Diagnostic tests can run for approximately 10 minutes.
Step 6	(Optional) Server: SRV > **results**	Displays a summary of the diagnostic test with **Passed** or **Failed** test status. **Note** The summary report indicates the number of tests that failed and passed. It does not provide information about which tests failed or passed. To determine which tests failed and passed, see the output of the **run all** command.
Step 7	(Optional) Server: SRV > **show**	Displays a list of global parameters and diagnostic test modules that were administered on the server.
Step 8	Server: SRV > **exit**	Exits from Diagnostic Shell.
Step 9	Open a service request with Cisco TAC.	If the diagnostic tests pass successfully, it indicates that there is no problem with the server CPU, memory, or block devices. The problem could be with some other hardware component or with the software configuration. Open a service request with Cisco TAC to isolate the problem. If the diagnostic tests fail, open a service request with Cisco TAC for further assistance.

This example runs all diagnostic tests:

```
Shell > dir fs1:
  06/27/12  07:48p           1,435,424  Dsh.efi
  06/27/12  08:03p              10,036  dsh-e140d.pkg
  06/25/12  06:00p              10,140  dsh-e140s.pkg
  06/27/12  08:04p              10,042  dsh-e160d.pkg
          4 File(s)   1,465,642 bytes
Shell > fs1:
```

```
fs1:\> cp dsh-e140d.pkg dsh.pkg
copying fs0:\OBD\dsh-e140d.pkg -> fs0:\OBD\dsh.pkg
- [ok]
fs1:\> dsh
Diagnostics is a standalone utility that runs on the server module independent
of the operating system or applications running on the module.All tests are
non-destructive, but there is a possibility of disk datacorruption during
power or equipment failure when the tests are in progress. Therefore, before
executing these tests, we highly recommend that you backup the data.


For questions or concerns with this utility, please open a Service Request
with Cisco TAC at http://www.cisco.com/cisco/web/support/index.html

(Y)es to continue test. (N)o to exit(y/n): Y
Cisco Diagnostics  Shell 1.03(0.3) Thu 06/28/-16:35:08.95-canis-diag@cisco.com
UCS-E140D-M1/K9:SRV>

Server: SRV > run all
Server: SRV > results
Test Name          : all
Test Status        : Passed
Failed/Run History : 0/17
Start Time         : 06/27/12 14:38:19
End Time           : 06/27/12 14:43:36
Diag Version       : 1.03(0.3) Mon 04/02/-17:07:57.19-canis-diag@cisco.com
Board S/N          : FOC160724BY

Server: SRV > show
Server: SRV > exit
```

What to Do Next

Reset the virtual media boot order to its original setting.

INDEX

A

Active Directory 74, 76
- configuring in CIMC 76

adapter 59
- PCI 59

auto rebuild, enabling 30

B

backing up 117, 118
- CIMC configuration 117, 118

BIOS 40, 42, 43, 106
- CMOS 42
  - clearing 42
- firmware 40
  - installing from TFTP server 40
- obtaining firmware from Cisco 106
- password 43
  - clearing 43

BIOS CMOS 42
- clearing 42

BIOS firmware 40
- installing from TFTP server 40

BIOS password 43
- clearing 43

BIOS settings 40, 41, 43
- about 43
- advanced 40
- restoring defaults 43
- server management 41

BIOS status 39
- viewing 39

boot order, configuring 19

C

certificate management 99
- uploading a certificate 99

CIMC 105, 106, 107, 108, 109, 111, 112, 117
- clearing log 112
- firmware 105, 107, 108
  - about 105
  - activating 108
  - installing from TFTP server 107
- firmware details 109
- obtaining firmware from Cisco 106
- resetting to factory defaults 117
- sending log 112
- viewing log 111

CIMC CLI 3

CIMC firmware 108
- activating 108

CIMC firmware details 109
- viewing 109

CIMC NICs 79

CIMC overview 3

common properties 81

communication services properties 87, 88, 89
- HTTP properties 87
- IPMI over LAN properties 89
- SSH properties 88

configuration 117, 118, 119
- backing up 118
- exporting 117
- importing 119

CPU properties 54

D

deleting 16

diagnostics 123
- test, running 123

diagnostics image 122

disabling KVM 69

disk drive bootable 29
- using CIMC CLI 29

E

E-Series Server 1
- overview 1

enabling KVM 68, 69
encrypting virtual media 70
event filters, platform 101, 102
- about 101
- configuring 102

event log, system 113, 114
- clearing 114
- viewing 113

events 101, 102
- platform 101, 102
  - disabling alerts 102
  - enabling alerts 101

exporting 117, 118
- CIMC configuration 117, 118

F

fault summary 63
- viewing 63

faults 63
- viewing summary 63

firmware 105, 106, 107
- about 105
- installing from TFTP server 107
- obtaining from Cisco 106

floppy disk emulation 70

H

hard drive presence 61
host image 13, 15, 16
Host Image Mapping 13
HTTP properties 87

I

importing 119
- CIMC configuration 119

IP blocking 84
IPMI over LAN 89
- description 89

IPMI over LAN properties 89
IPv4 properties 82

K

KVM 68, 69
- configuring 68
- disabling 69
- enabling 68, 69

KVM console 11, 67

L

LDAP, See Active Directory
local users 73

M

mapping 13
mapping to host 122
memory properties 54

N

network properties 80, 81, 82, 83
- common properties 81
- IPv4 properties 82
- NIC properties 80
- VLAN properties 83

network security 85
NIC properties 80

O

OS installation 11, 12
- methods 11
- PXE 12

P

PCI adapter 59
- viewing properties 59

physical drive 38
- rebuilding 38

physical drive state 37
- changing 37

platform event filters 101, 102
- about 101
- configuring 102

Platform events 101, 102
- diabling alerts 102

Platform events *(continued)*
  enabling alerts 101
power cycling the server 22
power policy statistics 60
  viewing 60
power supply properties 55
powering off the server 22
powering on the server 21
PXE installation 12

R

RAID 27, 36
  configuring 27
  deleting 36
RAID options 23
remote presence 68, 69, 70, 71, 72
  configuring serial over LAN 71
  launching serial over LAN 72
  virtual KVM 68, 69
  virtual media 70
resetting the server 20

S

self-signed certificate 97
sensors 64
  temperature 64
  voltage 64
serial over LAN 71, 72
  configuring 71
  launching 72
server management 19, 20, 21, 22
  configuring the boot order 19
  power cycling the server 22
  powering off the server 22
  powering on the server 21
  resetting the server 20
  shutting down the server 21
server properties 53
server software 2
shutting down the server 21
SNMP 90, 91, 92
  configuring properties 90
  configuring trap settings 91
  sending test message 92
software 16
  obtaining from VMware 16
SSH properties 88
storage properties 56, 57, 59
  viewing adapter properties 56
  viewing physical drive properties 57
  viewing virtual drive properties 59
storage sensors 65
  viewing 65
syslog 112
  sending CIMC log 112
system event log 113, 114
  clearing 114
  viewing 113

T

technical support data, exporting 115
temperature sensors 64

U

unmapping 15
uploading a server certificate 99
user management 73, 76, 77, 78
  Active Directory 76
  local users 73
  terminating user sessions 78
  viewing user sessions 77
user sessions 77, 78
  terminating 78
  viewing 77

V

virtual drive 31, 32, 35
  performing consistency check 31
  reconstruct 35
  reconstructing options 32
virtual KVM 68, 69
virtual media 70
VLAN properties 83
VMware 16
  obtaining software 16
voltage sensors 64

Y

YAML 8