CLI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine Integrated Management Controller, Release 3.2.x

First Published: 2017-07-31

Last Modified: 2020-05-20

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

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

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

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

CONTENTS

PREFACE

CHAPTER 1

CHAPTER 2

Preface

This preface includes the following sections:

New and Changed Information

The following table provides an overview of the significant changes to this guide for the current release:

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	Provides an overview of the Cisco UCS E-Series Servers, the Cisco UCS E-Series Network Compute Engine, and the CIMC .

Chapter	Title	Description
Chapter 2	Installing the Server Operating System	Describes how to configure an operating system (OS) on the server.
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, and how to configure BIOS settings.
Chapter 4	Managing Storage Using RAID	Describes how to configure and manage RAID.
Chapter 5	Viewing Server Properties	Describes how to view the CPU, memory, power supply, storage, PCI adapter, and LOM properties of the server.
Chapter 6	Viewing Server Sensors	Describes how to view the temperature, voltage, and storage sensors.
Chapter 7	Managing Remote Presence	Describes how to configure and manage the virtual KVM, virtual media, and the serial over LAN connection.
Chapter 8	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 9	Configuring Network-Related Settings	Describes how to configure network interfaces, network settings, network security, NAM, and NTP settings.
Chapter 10	Configuring Communication Services	Describes how to configure server management communication by HTTP, SSH, IPMI, and SNMP.
Chapter 11	Managing Certificates	Describes how to generate, upload, and manage server certificates.
Chapter 12	Configuring Platform Event Filters	Describes how to configure and manage platform event filters.
Chapter 13	Firmware Management	Describes how to obtain, install, and activate firmware images.
Chapter 14	Viewing Faults and Logs	Describes how to view fault information and how to view, export, and clear the CIMC log and system event log messages.
Chapter 15	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 16	Diagnostic Tests	Describes how to run diagnostic tests.

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
User input	Text the user should enter exactly as shown or keys that a user should press appear in **`this font`**.
Document titles	Document titles appear in *this font*.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Arguments in a CLI command appear in *this 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*. Notes contain helpful suggestions or references to material not covered in the document.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

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 IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Documentation

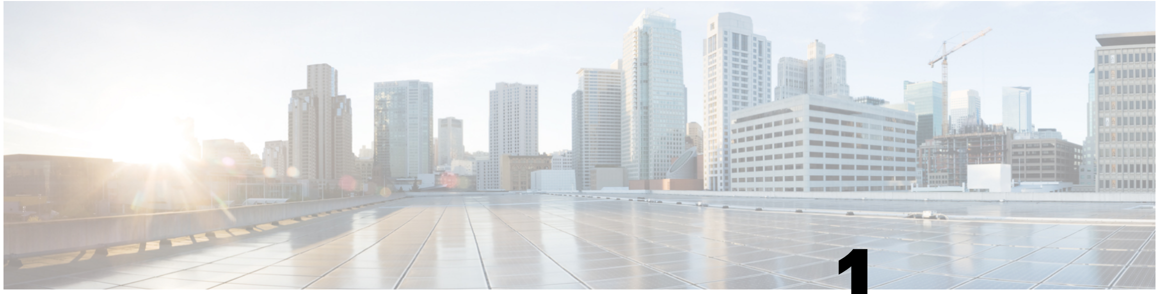
The Documentation Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine provides links to all product documentation.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Follow Cisco UCS Docs on Twitter to receive document update notifications.



CHAPTER 1

Overview

This chapter includes the following sections:

Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine Overview

The Cisco UCS E-Series Servers (E-Series Servers) and Cisco UCS E-Series Network Compute Engine (NCE) are a family of size-, weight-, and power-efficient blade servers that are housed within the Generation 2 Cisco Integrated Services Routers (Cisco ISR G2) and the Cisco ISR 4000 series. 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.

The E-Series Servers are purpose-built with powerful Intel Xeon processors for general purpose compute. They come in two form factors: single-wide and double-wide. The single-wide E-Series Server fits into one service module (SM) slot, and the double-wide E-Series Server fits into two SM slots.

The NCEs are price-to-power optimized modules that are built to host Cisco network applications and other lightweight general-purpose applications. They come in three form factors: SM, NIM, and EHWIC. The SM E-Series NCE fits into one SM slot, the NIM E-Series NCE fits into one NIM slot, and the EHWIC E-Series NCE fits into two EHWIC slots.

Note

- The EHWIC E-Series NCE can be installed in the the Cisco ISR G2 only.
- The NIM E-Series NCE can be installed in the Cisco ISR 4000 series only.
- The Cisco ISR 4331 has one SM slot. The Cisco ISR 4321 and the Cisco ISR 4431 have no SM slots.
- Citrix XenServer is supported on the E-Series Servers only.
- CIMC 3.2.x is not supported on EHWIC NCEs.

Note For information about the supported E-Series Servers and NCE, and the maximum number of servers that can be installed per router, see the "Hardware Requirements" section in the *Hardware Installation Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*.

Server Software

E-Series Servers and NCE 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 of the E-Series Server or NCE. 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 and NCE. 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 or NCE with a preinstalled Microsoft Windows Server or VMware vSphere Hypervisor, or you can install your own platform.

Note For information about the platforms that have been tested on the E-Series Servers or NCE, see the "Software Requirements" section in the *Release Notes for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*.

CIMC Overview

The Cisco Integrated Management Controller (CIMC) is the management service for the E-Series Servers and the NCE. 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

Note The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

- 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, IPv6, VLANs, and network security
- Configure communication services, including HTTP, SSH, IPMI over LAN, SNMP, and Redfish
- 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*:

- Use the CIMC GUI to invoke the CIMC CLI
- View a command that has been invoked through the CIMC CLI in the CIMC GUI
- Generate CIMC CLI output from the CIMC GUI

CIMC CLI

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

- By the serial port.
- Over the network by SSH.
- From the router. Use one of the following commands as appropriate:
    - **ucse** *slot* **session imc**—Use for E-Series Servers and the SM E-Series NCE installed in a Cisco ISR G2. Applicable from Cisco IOS Release 15.2(4)M to 15.4(2)T.
    - **ucse subslot** *slot/subslot* **session imc**—Use for E-Series Servers, SM E-Series NCE, and EHWIC E-Series NCE installed in a Cisco ISR G2. Applicable in Cisco IOS Release 15.4(3)M.
    - **hw-module subslot** *slot/subslot* **session imc**—Use for E-Series Servers and the NIM E-Series NCE installed in a Cisco ISR 4000 series.

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 #

Mode Name	Command to Access	Mode Prompt
`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 #
`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`	**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 #

Mode Name	Command to Access	Mode Prompt
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 #
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	**scope sol** command from EXEC mode	/sol #
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

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

- KVM console
- PXE installation server
- Host image mapping

Caution You must use only one method to map virtual drives. For example, you must use either the KVM console or the Host Image Mapping method. Using a combination of methods will cause the server to be in an undefined state.

KVM Console

The KVM console is an interface accessible from the 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.

  Note The CIMC Configuration Utility is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

- On Cisco UCS M1 and M2 servers, access the WebBIOS to configure RAID, by pressing **Ctrl-H** during bootup.

  On Cisco UCS M3 servers, access the MegaRAID controller to configure RAID, by pressing **Ctrl-R** during bootup.

  Note RAID is not supported on EHWIC E-Series NCE and NIM E-Series NCE. The **Ctrl-H** and **Ctrl-R** will not work on these SKUs.

Java Requirements to Launch the KVM Console

To launch the KVM console, you must have Java release 1.6 or later installed in your system.

If the KVM console fails to launch because the certificate is revoked by Java, you must change your Java settings. Do the following:

1. Access the Java control panel.
2. Click the **Advanced** tab
3. Under **Perform certificate revocation on**, choose the **Do not check (not recommended)** radio button. For more information, see http://www.java.com/en/download/help/revocation_options.xml.

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 and the Cisco UCS E-Series Network Compute Engine*.

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 VLAN, typically a dedicated provisioning VLAN. 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.

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

Step 2 Reboot the server.

Caution If you are using the shared LOM interfaces to access CIMC, make sure that you do not use the CIMC GUI during the server reboot process. If you use the CIMC GUI, the GUI will disconnect during PXE installation as the boot agent overrides the IP address that was previously configured on the Ethernet ports.

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 Microsoft Windows, Linux, or VMware from a remote FTP or HTTP server onto the CIMC internal repository, and then map the image onto the virtual drive of a USB controller in the E-Series Server or NCE. 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 or .img 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 in to the CIMC as a user with admin privileges.
- Obtain the host image file from the appropriate third-party.

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 host-image-mapping**	Enters the remote install command mode.
Step 2	Server /host-image-mapping # **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. **Note** The HTTP server does not support user authentication; only FTP supports user authentication.
Step 3	(Optional) Server /host-image-mapping # **show detail**	Displays the status of the image download.
Step 4	Server /host-image-mapping # **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 /host-image-mapping # **show detail**	Displays the status of the host image mapping.

Example

This example maps the host image:

```
Server# scope host-image-mapping
Server /host-image-mapping # download-image ftp 10.20.34.56 pub/hostimage.iso
---
```

```
Server /host-image-mapping # 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 /host-image-mapping # map-image
---
status: ok
---
Server /host-image-mapping # 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

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, on page 19.
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, on page 13.
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 an E-Series Server or NCE Option 1 (E-Series Server or NCE without a preinstalled operating system or hypervisor), and you installed your own version of the Microsoft Windows Server, you must install drivers.

The Microsoft Windows operating system requires that you install the following 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
- Intel Server Chipset Driver for Windows
- Intel Network Adapter Driver for Windows Server 2012 R2

Note The driver 'Intel Network Adapter Driver for Windows Server 2012 R2' is applicable only for the following servers:

- UCS-E160S-M3 Server
- UCS-EN140N-M2 Server
- UCS-EN120E-M2 Server
- UCS-E180D-M3/K9 Server
- UCS-E1120D-M3/K9 Server

Note Additional drivers are not needed for Windows 2012.

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

Step 1 Download the drivers from Cisco.com. See Obtaining Software from Cisco Systems, on page 142.

Step 2 Copy the driver files into a 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.

This step is applicable to E-Series Servers and the SM E-Series NCE. This step is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

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 in to the CIMC as a user with admin privileges.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope host-image-mapping**	Enters the remote install command mode.
Step 2	Server /host-image-mapping # **unmap-image**	Unmounts the image from the virtual drive of the USB controller.

	Command or Action	Purpose
Step 3	Server /host-image-mapping # **show detail**	(Optional) Displays the status of the host image unmapping.

Example

This example unmaps the host image:

```
Server# scope host-image-mapping
Server /host-image-mapping # unmap-image
Server /host-image-mapping # 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 in to the CIMC as a user with admin privileges.

Procedure

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

Example

This example deletes the host image:

```
Server# scope host-image-mapping
Server /host-image-mapping # delete-image
```

Configuring ESX Network Connectivity through MGF (GE1) Interface

On a UCS E-Series Server, the MGF(GE1) interface connects internally to the Ethernet Switch Module through the backplane. This section explains how to set up a communication link between the UCS E-Series hosts with the external network.

Note This feature is supported only on UCS E-Series Servers supported with EHWIC-4ESGP on ISR-G2 Series Routers.

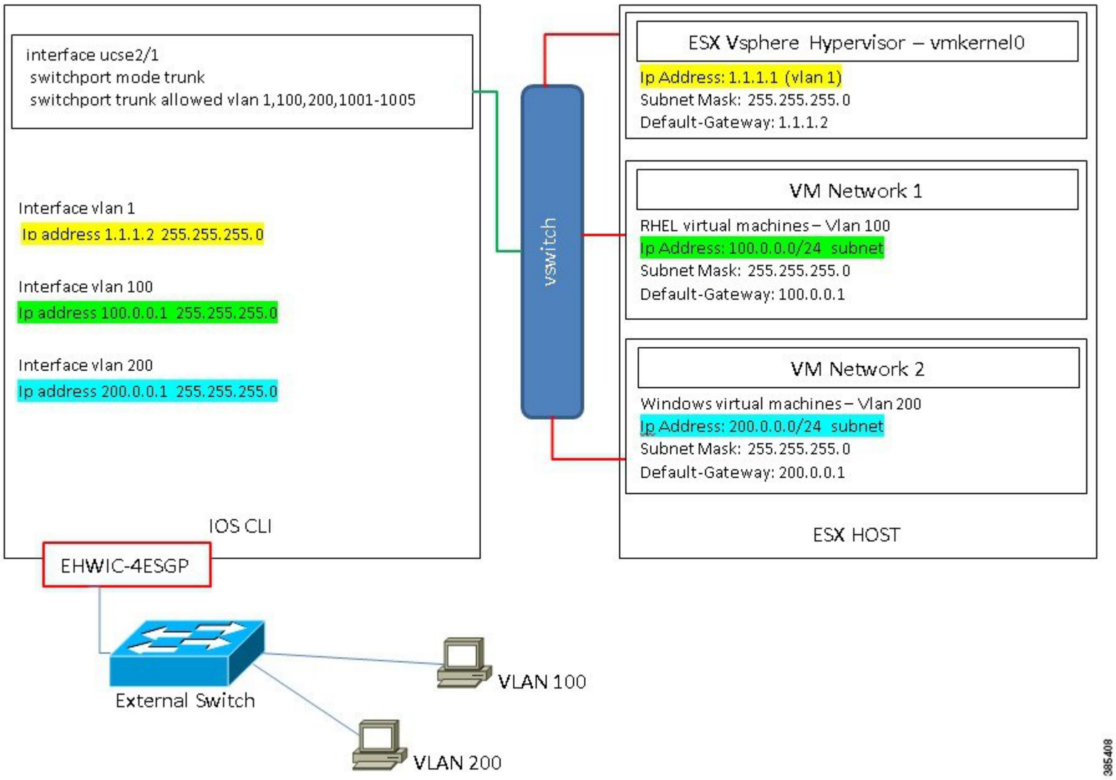
There are three scenarios where you can configure ESX Network Connectivity through the MGF (GE1) interface:

- L2 NETWORKING: Hosts and VMs in the Same Subnet
- L3 NETWORKING: Hosts and VMs in Different Networks
- L3 NETWORKING: Hosts and VMs in the Same Network

L2 NETWORKING: Hosts and VMs in the Same Subnet

In this scenario, the UCS E-Series blade is hosting the VMS in VLAN 100 and 200.The traffic enters the router through the MGF/UCSE2/1/ GE1 interface and switches to the physical hosts by the EHWIC module.

The following configuration setup shows how the VMs and physical hosts (in the same VLANs) communicate.



```
interface ucse2/1
 switchport mode trunk
 switchport trunk allowed vlan 1,100,200,1001-1005
```

```
Interface vlan 1
Ip address 1.1.1.2 255.255.255.0

Interface vlan 100
Ip address 100.0.0.1 255.255.255.0

Interface vlan 200
Ip address 200.0.0.1 255.255.255.0
```

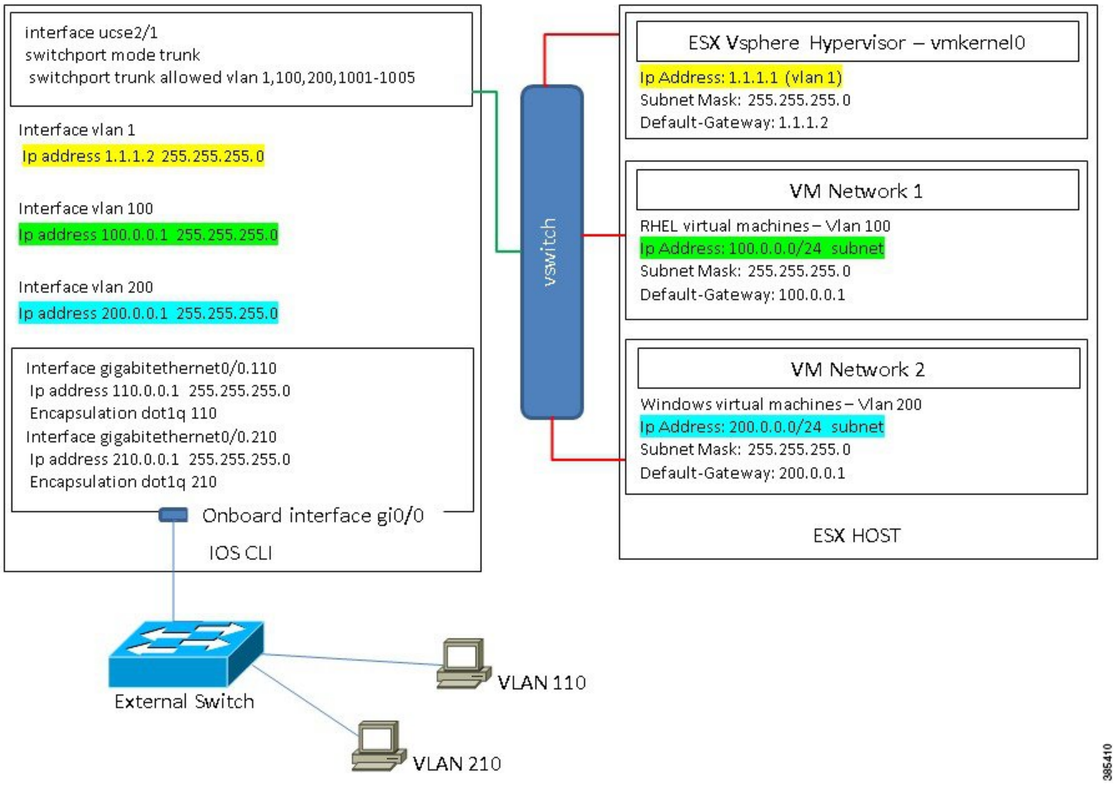
ESX Vsphere Hypervisor – vmkernel0
Ip Address: 1.1.1.1 (vlan 1)
Subnet Mask: 255.255.255.0
Default-Gateway: 1.1.1.2

VM Network 1
RHEL virtual machines – Vlan 100
Ip Address: 100.0.0.0/24 subnet
Subnet Mask: 255.255.255.0
Default-Gateway: 100.0.0.1

VM Network 2
Windows virtual machines – Vlan 200
Ip Address: 200.0.0.0/24 subnet
Subnet Mask: 255.255.255.0
Default-Gateway: 200.0.0.1

L3 NETWORKING: Hosts and VMs in Different Network

In this scenario, the VMs communicate with hosts in different subnet by sending the traffic to the router through the UCSE2/1. On the router, the traffic hits the VLAN interface and gets L3 routed by the ISRG2.



```
interface ucse2/1
 switchport mode trunk
 switchport trunk allowed vlan 1,100,200,1001-1005
Interface vlan 1
 Ip address 1.1.1.2 255.255.255.0
Interface vlan 100
Ip address 100.0.0.1 255.255.255.0
Interface vlan 200
Ip address 200.0.0.1 255.255.255.0
Interface gigabitethernet0/0.110
 Ip address 110.0.0.1 255.255.255.0
 Encapsulation dot1q 110
Interface gigabitethernet0/0.210
 Ip address 210.0.0.1 255.255.255.0
 Encapsulation dot1q 210
```

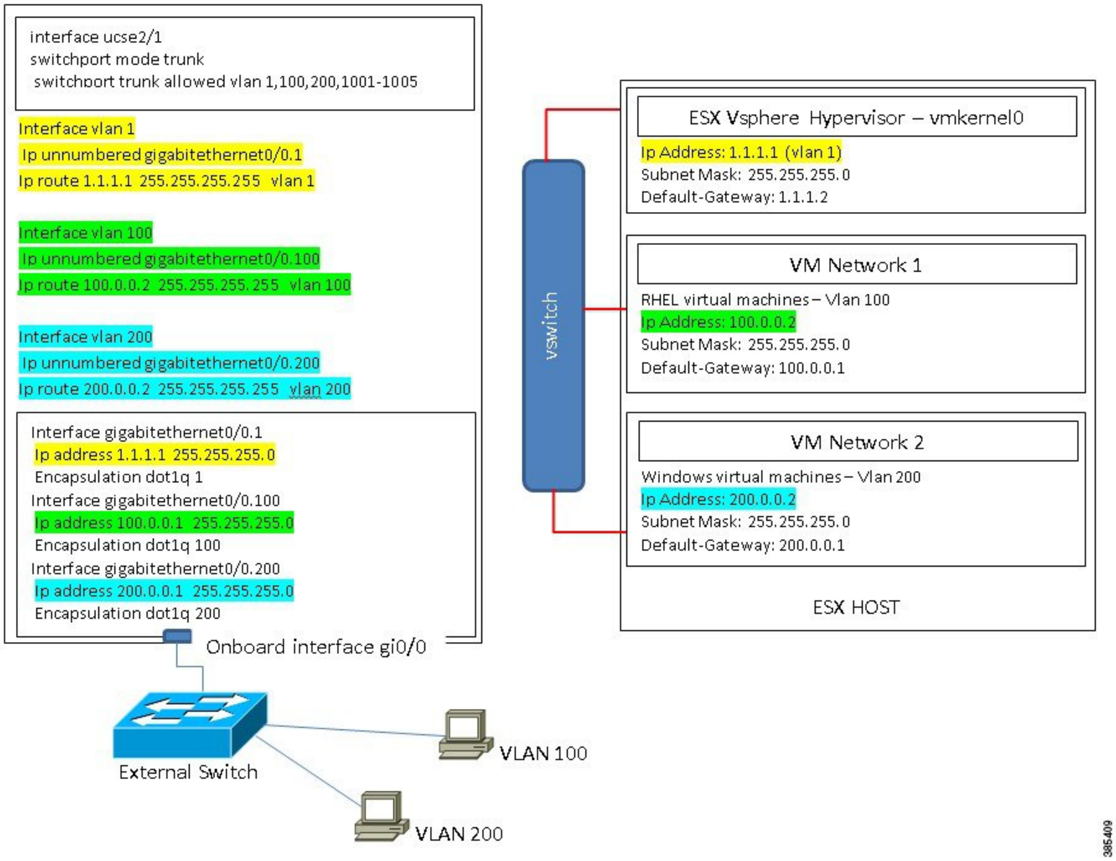
```
ESX Vsphere Hypervisor – vmkernel0
Ip Address: 1.1.1.1 (vlan 1)
Subnet Mask: 255.255.255.0
Default-Gateway: 1.1.1.2

VM Network 1
RHEL virtual machines – Vlan 100
Ip Address: 100.0.0.0/24 subnet
Subnet Mask: 255.255.255.0
Default-Gateway: 100.0.0.1

VM Network 2
Windows virtual machines – Vlan 200
Ip Address: 200.0.0.0/24 subnet
Subnet Mask: 255.255.255.0
Default-Gateway: 200.0.0.1
```

L3 NETWORKING: Hosts and VMs in the Same Network

In this scenario, the physical hosts are in the same subnet as the VMs, but no EHWIC is present on the router. The physical hosts can be connected to the onboard L3 interface with the following configuration to enable the communication between the VMs and the physical hosts.



```
interface ucse2/1
switchport mode trunk
 switchport trunk allowed vlan 1,100,200,1001-1005

Interface vlan 1
 Ip unnumbered gigabitethernet0/0.1
Ip route 1.1.1.1  255.255.255.255  vlan 1

Interface vlan 100
 Ip unnumbered gigabitethernet0/0.100
Ip route 100.0.0.2  255.255.255.255  vlan 100

Interface vlan 200
 Ip unnumbered gigabitethernet0/0.200
Ip route 200.0.0.2  255.255.255.255  vlan 200

Interface gigabitethernet0/0.1
 Ip address 1.1.1.1  255.255.255.0
 Encapsulation dot1q 1
Interface gigabitethernet0/0.100
 Ip address 100.0.0.1  255.255.255.0
 Encapsulation dot1q 100
Interface gigabitethernet0/0.200
 Ip address 200.0.0.1  255.255.255.0
 Encapsulation dot1q 200
```

ESX Vsphere Hypervisor – vmkernel0

Ip Address: 1.1.1.1 (vlan 1)
Subnet Mask: 255.255.255.0
Default-Gateway: 1.1.1.2

VM Network 1

RHEL virtual machines – Vlan 100
Ip Address: 100.0.0.2
Subnet Mask: 255.255.255.0
Default-Gateway: 100.0.0.1

VM Network 2

Windows virtual machines – Vlan 200
Ip Address: 200.0.0.2
Subnet Mask: 255.255.255.0
Default-Gateway: 200.0.0.1

CHAPTER 3

Managing the Server

This chapter includes the following sections:

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** *category:device1*[,*category:device2*[,*category:device3*[,*category:device4*[,*category:device5*]]]]	Specifies the boot device options and order. **Note** The options are not case sensitive. You can select one or more of the following: • cdrom—Bootable CD-ROM • Virtual-CD

	Command or Action	Purpose
		• fdd—Floppy disk drive • Virtual-Floppy • hdd—Hard disk drive • RAID • Cypress • Virtual-HiFd • pxe—PXE boot • GigEth0 • GigEth1 • GigEth2 • GigEth3 • efi—Extensible Firmware Interface
Step 3	Server /bios # **commit**	Commits the transaction to the system configuration.
Step 4	(Optional) Server /bios # **show detail**	Displays the server boot order.

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

Example

This example sets the boot order and commits the transaction:

```
Server# scope bios
Server /bios # set boot-order cdrom:Virtual-CD,hdd:raid,efi
To manage boot-order:
- Reboot server to have your boot-order settings take place
- Do not disable boot options via BIOS screens
- If a specified device type is not seen by the BIOS, it will be removed
  from the boot order configured on the BMC
- Your boot order sequence will be applied subject to the previous rule.
  The configured list will be appended by the additional device types
  seen by the BIOS
Server /bios *# commit
Server /bios #
Server /bios # show detail
BIOS:
    BIOS Version: "UCSES.1.5.0.1 (Build Date: 02/14/2013)"
    Boot Order: CDROM:Virtual-CD,HDD:RAID,EFI
    FW Update/Recovery Status: None, OK
    Active BIOS: main
```

Resetting the Server

Before you begin

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

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **power hard-reset**

DETAILED STEPS

	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 powering on the server. • Power hard-reset is the same as pressing the physical reset button on the server.

Example

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.

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **power shutdown**

DETAILED STEPS

	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. **Note** The NIM E-Series NCE might take up to 60 seconds to shut down. After two or three shut down attempts, if the NIM E-Series NCE does not shut down, enter the following commands from the router: **a.** Router # **hw-module subslot 0/***NIM-slot-number* **stop** **b.** Router # **hw-module subslot 0/***NIM-slot-number* **start**

Example

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
```

Locking Cisco IOS CLI Configuration Changes

Use this procedure to prevent configuration changes from being made using the Cisco IOS CLI.

Before you begin

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

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **show detail**
3. Server /chassis # **set ios-lockout locked**
4. Server /chassis* # **commit**
5. Server /chassis # **show detail**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the IOS lockout (whether it is locked or unlocked).
Step 3	Server /chassis # **set ios-lockout locked**	Prevents configuration changes from being made using the Cisco IOS CLI.
Step 4	Server /chassis* # **commit**	Commits the changes.
Step 5	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the IOS lockout (whether it is locked or unlocked).

Example

This example prevents configuration changes from being made using the Cisco IOS CLI:

```
Server# scope chassis
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
Server /chassis # set ios-lockout locked
Server /chassis* # commit
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: locked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
```

Unlocking Cisco IOS CLI Configuration Changes

Use this procedure to allow configuration changes to be made using the Cisco IOS CLI.

Before you begin

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

SUMMARY STEPS

1. Server# **scope chassis**

2. Server /chassis # **show detail**
3. Server /chassis # **set ios-lockout unlocked**
4. Server /chassis* # **commit**
5. Server /chassis # **show detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the IOS lockout (whether it is locked or unlocked).
Step 3	Server /chassis # **set ios-lockout unlocked**	Allows configuration changes to be made using the Cisco IOS CLI.
Step 4	Server /chassis* # **commit**	Commits the changes.
Step 5	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the IOS lockout (whether it is locked or unlocked).

Example

This example allows configuration changes to be made using the Cisco IOS CLI:

```
Server# scope chassis
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: locked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
Server /chassis # set ios-lockout unlocked
Server /chassis* # commit
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
```

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.

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **power on**

DETAILED STEPS

	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.

Example

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

Note This procedure is not applicable to the NIM E-Series NCE.

Before you begin

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

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **power off**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **power off**	Turns off the server. **Note** For the NIM E-Series NCE, we recommend that you use the **power shutdown** command. If a power off is necessary, use the following commands from the router: **a.** Router # **hw-module subslot 0**/*NIM-slot-number* **stop** **b.** Router # **hw-module subslot 0**/*NIM-slot-number* **start**

Example

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

Note This procedure is not applicable to the NIM E-Series NCE.

Before you begin

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

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **power cycle**

DETAILED STEPS

	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. **Note** • Power cycling the server is the same as pressing the physical power button to power off and then powering on the server. • Power hard-reset is the same as pressing the physical reset button on the server. **Note** For the NIM E-Series NCE, we recommend that you use the **power shutdown** command. If a power cycle is necessary, use one of the following commands from the router: • **a.** Router # **hw-module subslot 0/***NIM-slot-number* **stop** **b.** Router # **hw-module subslot 0/***NIM-slot-number* **start** • Router # **hw-module subslot 0/***NIM-slot-number* **reload** **Note** This command power-cycles the module. The CIMC and server reboot.

Example

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
```

Configuring the Power Restore Policy

The power restore policy determines how power is restored to the server after a chassis power loss.

Before you begin

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

Note These commands are supported only on ISR 4K routers, not on ISR G2. For ISR G2, refer to the BIOS configuration in CIMC.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters the cimc command mode.
Step 2	Server /cimc #**scope power-restore-policy**	Enters the power restore policy command mode.
Step 3	Server /cimc/power-restore-policy # **set policy** {**power-off** | **power-on** | **restore-last-state**}	Specifies the action to be taken when chassis power is restored. Select one of the following: • **power-off**—Server power will remain off until manually turned on. • **power-on**—Server power will be turned on when chassis power is restored. • **restore-last-state**—Restores the server to the same power state (off or on) that it was in when the power was lost. This is the default action.
Step 4	Server /cimc/power-restore-policy# **commit**	Commits the transaction to the system configuration.

Example

Modules on ISRG2

This example sets the power restore policy to power-on and commits the transaction:

```
Server# scope BIOS
Server /BIOS # scope server-management
Server /BIOS/server-management # set ResumeOnACPowerLoss power-on
Server /BIOS/server-management # commit
Server /BIOS/server-management #  show detail
Power Restore Policy:
    Power Restore Policy: power-on

Server /BIOS/server-management #
```

Note Even though you can see the changed settings in the CLI, you have to reboot the server for the settings to take effect.

Modules on ISR4K

This example sets the power restore policy to power-on and commits the transaction:

```
Server# scope CIMC
Server /CIMC # scope power-restore-policy
Server /CIMC/power-restore-policy # set policy power-on
Server /CIMC/power-restore-policy *# commit
Server /CIMC/power-restore-policy #  show detail
Power Restore Policy:
    Power Restore Policy: power-on

Server /CIMC/power-restore-policy #
```

Locking the Server's Front Panel Power Button

Use this procedure to disable the physical power button, which is located on the front panel of the physical server. Once the power button is disabled, you cannot use the front panel power button to turn the server power on or off.

Before you begin

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

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **show detail**
3. Server /chassis # **set power-button locked**
4. Server /chassis* # **commit**
5. Server /chassis # **show detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the power button (whether it is locked or unlocked).
Step 3	Server /chassis # **set power-button locked**	Disables the power button. You cannot use the front panel power button to turn the server power on or off.
Step 4	Server /chassis* # **commit**	Commits the changes.
Step 5	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the power button (whether it is locked or unlocked).

Example

This example disables the server's physical power button, which is located on the front panel of the physical server:

```
Server# scope chassis
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
Server /chassis # set power-button locked
Server /chassis* # commit
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: locked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
```

Unlocking the Server's Front Panel Power Button

Use this procedure to enable the physical power button, which is located on the front panel of the physical server. Once the power button is enabled, you can use the front panel power button to turn the server power on or off.

Before you begin

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

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **show detail**
3. Server /chassis # **set power-button unlocked**
4. Server /chassis* # **commit**
5. Server /chassis # **show detail**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the power button (whether it is locked or unlocked).
Step 3	Server /chassis # **set power-button unlocked**	Enables the power button. You can use the front panel power button to turn the server power on or off.
Step 4	Server /chassis* # **commit**	Commits the changes.
Step 5	Server /chassis # **show detail**	(Optional) Displays server properties, which allows you to determine the current status of the power button (whether it is locked or unlocked).

Example

This example enable the server's physical power button, which is located on the front panel of the physical server:

```
Server# scope chassis
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: locked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
Server /chassis # set power-button unlocked
Server /chassis* # commit
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
```

Configure the Boot Order

Configure the Server Boot Order Using UEFI Map and UEFIOS

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** {*hdd:,pxe:.fdd:.efi,uefimap,uefios.cdrom:*} Server /bios # **set boot-order** *uefimap,uefios*	Specifies the boot device options and order. **Note** The options are not case sensitive. You can select one or more of the following: • hdd—Hard disk drive • RAID • Cypress • Virtual-HiFd • pxe—PXE boot • GigEth0 • GigEth1 • GigEth2 • GigEth3 • fdd—Floppy disk drive • Virtual-Floppy • efi—Extensible Firmware Interface • uefimap—UEFI virtual-map boot option • uefios—UEFI Operating System • cdrom—Bootable CD-ROM • Virtual-CD
Step 3	Server /bios # **commit**	Commits the transaction to the system configuration.
Step 4	(Optional) Server /bios # **show detail**	Displays the server boot order.

The new boot order is used on the next BIOS boot.

Example

This example sets the boot order and commits the transaction:

```
Server# scope bios
Server /bios # set boot-order uefimap,uefios
To manage boot-order:
- Reboot server to have your boot-order settings take place
- Do not disable boot options via BIOS screens
- If a specified device type is not seen by the BIOS, it will be removed
  from the boot order configured on the BMC
- Your boot order sequence will be applied subject to the previous rule.
  The configured list will be appended by the additional device types
  seen by the BIOS
Server /bios *# commit
Server /bios #
Server /bios # show detail
BIOS:
    BIOS Version:"UCSEDM3.2.10b5 (Build Date:02/27/2020)"
    Boot Order: UEFIMAP,UEFIOS
    FW Update/Recovery Status: None, OK
    Active BIOS on next reboot: main
    UEFI Secure Boot: enabled
```

Note When you enable UEFI secure boot, only the UEFI options—efi, uefimap, uefios are available. Additionally, configure the UEFI secure boot on the M3 modules, this reduces their average boot time by approximately 45-50 seconds.

Configuring BIOS Settings

Viewing BIOS Status

SUMMARY STEPS

1. Server# **scope bios**
2. Server /bios # **show detail**

DETAILED STEPS

	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.

Name	Description
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.

Example

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 #
```

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 38 • Advanced: Memory BIOS Settings, on page 44 • Advanced: Serial Port BIOS Settings, on page 44 • Advanced: USB BIOS Settings, on page 45
Step 4	Server /bios/advanced # **commit**	Commits the transaction to the system configuration.

	Command or Action	Purpose
		Changes are applied on the next server reboot. If server power is on, you are prompted to choose whether to reboot now.

Example

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: - Server Management BIOS Settings, on page 45
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.

Example

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.

SUMMARY STEPS

1. Server# **scope bios**
2. Server /bios # **clear-cmos**

DETAILED STEPS

	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.

Example

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
```

Setting the BIOS Password

SUMMARY STEPS

1. Server/bios# **set password**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server/bios# **set password**	Sets the BIOS password.

Example

This example sets the BIOS password:

```
Server/bios# set password
Warning:

Strong Password Policy is enabled!


For CIMC protection your password must meet the following requirements:
        The password must have a minimum of 8 and a maximum of 20 characters.
        The password must not contain the User's Name.
        The password must contain characters from three of the following four categories.
            English uppercase characters (A through Z)
            English lowercase characters (a through z)
            Base 10 digits (0 through 9)
            Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, +, =)
```

Clearing the BIOS Password

SUMMARY STEPS

1. Server# **scope bios**
2. Server /bios # **clear-bios-password**

DETAILED STEPS

	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.

Example

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.

SUMMARY STEPS

1. Server# **scope bios**
2. Server /bios # **bios-setup-default**

DETAILED STEPS

	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.

Example

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.

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 **Intel Turbo Boost Technology**	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.

Name	Description
Enhanced Intel Speedstep Technology	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	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.
Number of Enabled Cores	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.

Name	Description
Execute Disable	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	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	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.
Intel VT-d Interrupt Remapping	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	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.

Name	Description
Intel VT-d Address Translation Services	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	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	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	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. • —The processor sends the C3 report using the ACPI C2 format. • —The processor sends the C3 report using the ACPI C3 format.
Processor C6 Report	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.

Name	Description
Hardware Prefetcher	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 to specify this value. For any value other than **Custom**, this option is overridden by the setting in the selected CPU performance profile.
Adjacent Cache-Line Prefetch	Whether the processor uses the Intel Adjacent Cache-Line Prefetch mechanism to fetch data when necessary. This can be one of the following: • **Disabled**—The Adjacent Cache-Line Prefetch mechanism is not used. • **Enabled**—The Adjacent Cache-Line Prefetch mechanism is used when cache issues are detected. **Note** You must select **Custom** in the in order to specify this value. For any value other than **Custom**, this option is overridden by the setting in the selected CPU performance profile.
Boot Option Rom	Sets the ROM type. This can be one of the following: • **Legacy**—The server launches the legacy Option ROM. • **UEFI**—The server launches the legacy UEFI ROM. • **Disabled**—Option ROM is not available.

Name	Description
Package C State Limit	The amount of power available to the server components when they are idle. This can be one of the following: • —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. • — System level coordination is in progress resulting in high power consumption. There might be performance issues until the coordination is complete. • —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. • —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. • —The server may enter any available C state. **Note** This option is used only if **CPU C State** is enabled.
Boot Order Rules	Whether the system boots according to the boot order that is specified in CIMC or specified in the BIOS setup utility. This can be one of the following: • **Strict**—The system boots according to the boot order specified in CIMC. • **Loose**—The system boots according to the boot order specified in the BIOS setup utility.
Patrol Scrub	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.

Name	Description
Demand Scrub	Whether the system allows a memory scrub to be performed on demand. This can be one of the following: • **Disabled**—The system does not allow a memory scrub to be performed on demand. • **Enabled**—The system allows a memory scrub to be performed on demand. If errors occur, the system attempts to fix them or marks the location as unreadable. This process makes the system run faster with fewer data processing errors.
Device Tagging	Whether the system allows devices and interfaces to be grouped based on a variety of information, including descriptions, addresses, and names. This can be one of the following: • **Disabled**—The system does not allow the devices and interfaces to be grouped. • **Enabled**—The system allows the devices and interfaces to be grouped.

Advanced: Memory BIOS Settings

Name	Description
Select Memory RAS	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • —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	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

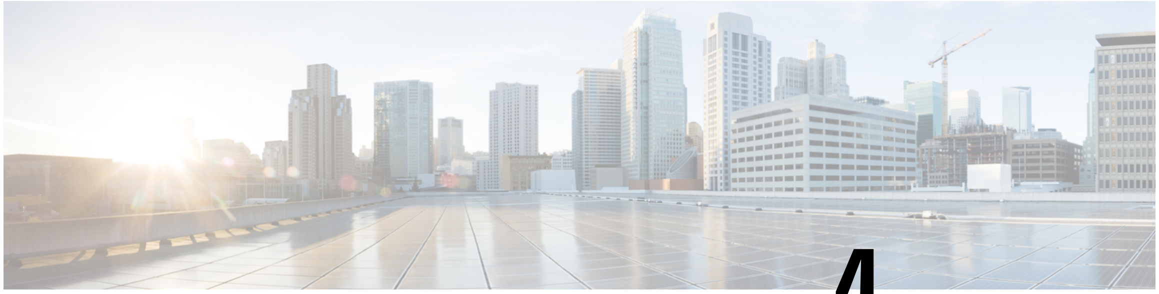
Name	Description
USB Port 0	Whether the processor uses USB port 0. This can be one of the following: • **Disabled**—The server does not use the USB port 0. • **Enabled**—The processor uses the USB port 0.
USB Port 1	Whether the processor uses USB port 1. This can be one of the following: • **Disabled**—The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

Name	Description
Console Redirection	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. • —Enables serial port A for console redirection during POST. This option is valid for blade servers and rack-mount servers. Note that **Serial Port A** option also requires that you enabled **Serial Port A** in the Advanced menu. **Note** If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.
Flow Control	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	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.

Name	Description
Terminal Type	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.
OS Boot Watchdog Timer	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
OS Boot Watchdog Timer Policy	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.



CHAPTER 4

Managing Storage Using RAID

This chapter includes the following sections:

RAID Options

Note The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

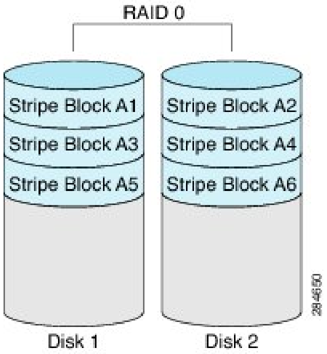
You can choose to store the E-Series Server data files on local Redundant Array of Inexpensive Disks (RAID). The following RAID levels are supported:

- The single-wide E-Series Server supports RAID 0 and RAID 1 levels.
- The double-wide E-Series Server supports RAID 0, RAID 1, and RAID 5 levels.
- The double-wide E-Series Server with the 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.

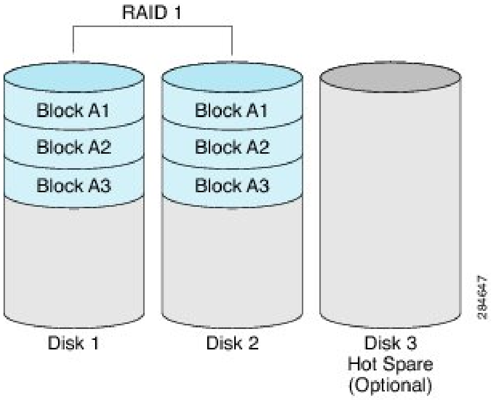
However, there is no fault tolerance, error checking, hot spare, or hot-swapping. If one disk drive fails, the data in the entire array is destroyed. Because there is no error checking or hot-swapping, the array is susceptible to unrecoverable errors.

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



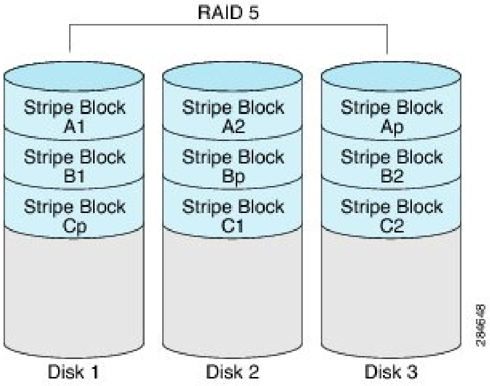
RAID 1 supports fault tolerance and hot-swapping. When one disk drive fails, you can remove the faulty disk drive and replace it with a new disk drive.

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.

RAID 10

RAID 10, a combination of RAID 0 and RAID 1, consists of striped data across mirrored spans. A RAID 10 drive group is a spanned drive group that creates a striped set from a series of mirrored drives. RAID 10 allows a maximum of eight spans. You must use an even number of drives in each RAID virtual drive in the span. The RAID 1 virtual drives must have the same stripe size. RAID 10 provides high data throughput and complete data redundancy but uses a larger number of spans.

Note RAID 10 is supported on DoubleWide M3 servers.

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 Option	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

Note The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

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-5**	Enters command mode for an installed storage card.

	Command or Action	Purpose
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. • (Optional) Drive cache options: • **DriveCacheDisable**—Caching is disabled on the physical drives. **Note** This is the default and recommended option. • **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. • (Optional) Strip size options: • **-strpsz64**—This is the default option.

	Command or Action	Purpose
		• **-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.

Example

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

Changing the Physical Drive State

Note The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

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-5**	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.

Example

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
```

Deleting a Virtual Drive

Note The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters the chassis command mode.
Step 2	Server /chassis # **scope storageadapter SLOT-5**	Enters command mode for an installed storage card.
Step 3	Server /chassis/storageadapter # **scope virtual-drive 0**	Displays virtual drive information that includes the virtual drive number, which is required to delete the virtual drive.
Step 4	Server /chassis/storageadapter/virtual-drive # **delete virtual-drive**	Deletes the specified virtual drive.

Example

This example shows how to delete a virtual drive.

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

Server /chassis /storageadapter # delete virtual-drive 0
VD 0 is the boot drive.  It is hosting the server's operating system.
All data on the drive will be lost.
Are you sure you want to delete this virtual drive?
Enter 'yes' to confirm -> yes

Server /chassis /storageadapter *# commit
```

Reconstructing the Virtual Drive Options

Note The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

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

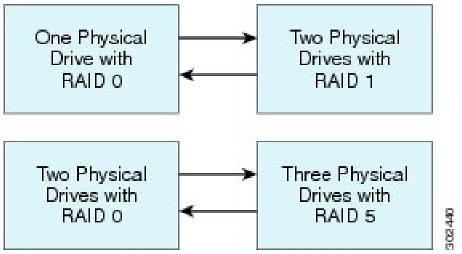
You can retain or increase the size of the virtual drive, but you cannot decrease its size. For example, if you have two physical drives with RAID 0, you cannot migrate to RAID 1 with the same number of drives. Because with RAID 1, a mirrored set of disk drives are created, which reduces the size of the virtual drive to half of what it was before, which is not supported.

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

Options for Retaining the Size of the Virtual Drive

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.

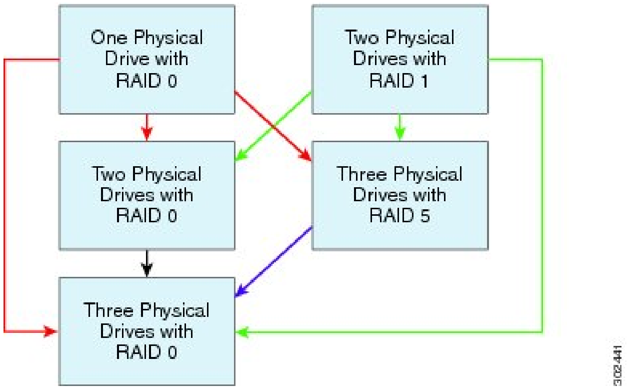
Table 1: Retaining the Virtual Drive Size

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.

Options for Increasing the Size of the Virtual Drive

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

Note The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

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, on page 57.

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-5**	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.

	Command or Action	Purpose
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.

Example

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
```

Making the Disk Drive Bootable

Note The RAID feature is applicable to E-Series Servers and the SM E-Series NCE. The RAID feature is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

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 # **scope storageadapter SLOT-5**	Enters command mode for an installed storage card.
Step 3	Server /chassis # **scope storageadapter SLOT-5**	Enters command mode for an installed storage card.
Step 4	Server /chassis/storageadapter # **scope virtual-drive 0**	Displays virtual drive information that includes the virtual drive number, which you is required to set the virtual drive.
Step 5	Server /chassis/storageadapter /virtual-drive# **set boot-drive**	Makes the disk drive bootable.

Example

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

```
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 0
Are you sure you want to set virtual drive 0 as the boot drive?
Enter 'yes' to confirm -> yes
```

CHAPTER 5

Viewing Server Properties

This chapter includes the following sections:

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.

Example

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 the Actual Boot Order

SUMMARY STEPS

1. Server# **scope bios**
2. Server /bios # **show actual-boot-order**

DETAILED STEPS

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

Example

The following examples display actual boot order:

```
E160S/bios# scope bios
Server /bios # show actual-boot-order
Boot Order   Type                      Boot Device
------------ ------------------------- -----------------------------------
1            Internal EFI Shell        Internal EFI Shell
2            CD/DVD                    Cisco vKVM-Mapped vDVD1.22
3            CD/DVD                    Cisco CIMC-Mapped vDVD1.22
4            Network Device (PXE)      TE2 - 10G Port 2
5            Network Device (PXE)      TE3 - 10G Port 3
6            Network Device (PXE)      GE0 - 1G Internal Port 0
7            Network Device (PXE)      GE1 - 1G Internal Port 1
8            FDD                       Internal Flash
9            FDD                       Cisco vKVM-Mapped vFDD1.22
10           HDD                       Cisco vKVM-Mapped vHDD1.22
11           HDD                       Cisco CIMC-Mapped vHDD1.22
12           HDD                       RAID Adapter
```

```
E1120D/bios# scope bios
Server /bios # show actual-boot-order
Boot Order   Type                      Boot Device
------------ ------------------------- -----------------------------------
1            CD/DVD                    Cisco vKVM-Mapped vDVD1.22
2            CD/DVD                    Cisco CIMC-Mapped vDVD1.22
3            HDD                       RAID Adapter
```

```
4           HDD                       Cisco
5           HDD                       Cisco vKVM-Mapped vHDD1.22
6           HDD                       Cisco CIMC-Mapped vHDD1.22
7           FDD                       Cisco vKVM-Mapped vFDD1.22
8           Network Device (PXE)      IBA XE Slot 0300 v2358
9           Network Device (PXE)      IBA XE Slot 0301 v2358
10          Network Device (PXE)      BRCM MBA Slot 0500 v15.2.7
11          Network Device (PXE)      BRCM MBA Slot 0501 v15.2.7
12          Internal EFI Shell        Internal EFI Shell
```

Viewing CIMC Information

Before you begin

Install the CIMC firmware on the server.

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **show** [**detail**]

DETAILED STEPS

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

Example

This example shows information about the 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
```

Viewing SD Card Information

Before you begin

Install the CIMC firmware on the server.

Note .

SD card is not supported on the M3 modules (UCS-E160S-M3, UCS-E180D-M3, and UCS-E1120D-M3).

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **show sd detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **show sd detail**	Displays the following information about the SD card: manufacturer and application ID, serial number, hardware and firmware revision, manufacture date, and whether the SD card is detected. If the card detected status is **yes**, it indicates that the SD card is present and is functional.

Example

This example shows information about the CIMC:

```
Server# scope cimc
Server /cimc # show sd detail
Manufacturer ID: Unigen 0x000045
    OEM/Application ID: 0x0024
    Serial Number: 0x39500025
    Hardware Revision: 0x2
    Firmware Revision: 0x0
    Manufacture Date: 06/2013
    Card Detected: yes
```

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.

Example

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.

Example

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
```

Viewing Power Supply Properties

Before you begin

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

Note Power-cap is not supported on ISR44XX. It is supported only on ISR-G2.

SUMMARY STEPS

1. Server# **scope power-cap**
2. Server /power-cap # **show** [**detail**]

DETAILED STEPS

	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.

Example

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 the CIMC. If an installed controller or storage device is not displayed, then it cannot be managed through the CIMC.
Step 3	Server /chassis # **scope storageadapter SLOT-5**	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.
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.

Example

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-5**	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.
Step 7	Server /chassis/storageadapter/physical-drive # **show status** [**detail**]	Displays status information about the specified physical drive.

Example

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-5**	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.

Example

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.

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **show pci-adapter** [**detail**]

DETAILED STEPS

	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.

Example

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

Before you begin

Note This is applicable only on ISR-G2 platforms.

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.

Example

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.

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **show hdd**

DETAILED STEPS

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

Example

This example displays power supply properties:

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

Viewing the MAC Address of an Interface

You can view the system defined interface names and the MAC address that is assigned to each host interface.

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **show lom-mac-list** [**detail**]

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	Server /cimc # **scope network**	Enters network command mode.
Step 3	Server /cimc/network # **show lom-mac-list** [**detail**]	Displays the system defined interface names and the MAC address that is assigned to each host interface.

Example

This example shows how to display the system defined interface names and the MAC address that is assigned to each host interface:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # show lom-mac-list
Interface                      MAC Address
------------------------------ --------------------
Console                        00:24:c4:f4:89:ee
GE1                            00:24:c4:f4:89:ef
GE2                            00:24:c4:f4:89:f0
GE3                            00:24:c4:f4:89:f1
```

For M3 servers, the interface GE is replaced by TE. This example shows the output for M3 servers:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # show lom-mac-list
Interface                      MAC Address
------------------------------ --------------------
Console                        28:6f:7f:ee:ac:0a
GE1                            28:6f:7f:ee:ac:0b
TE2                            28:6f:7f:ee:ac:0c
TE3                            28:6f:7f:ee:ac:0d
```

Viewing the Status of CIMC Network Connections

Before you begin

You must log in as a user with admin privileges to view the status of the CIMC network connections; whether the link is detected (physical cable is connected to the network interface) or not detected.

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **show link state [detail]**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **show link state [detail]**	Displays the status of the CIMC network connections; whether the link is detected (physical cable is connected to the network interface) or not detected.

Example

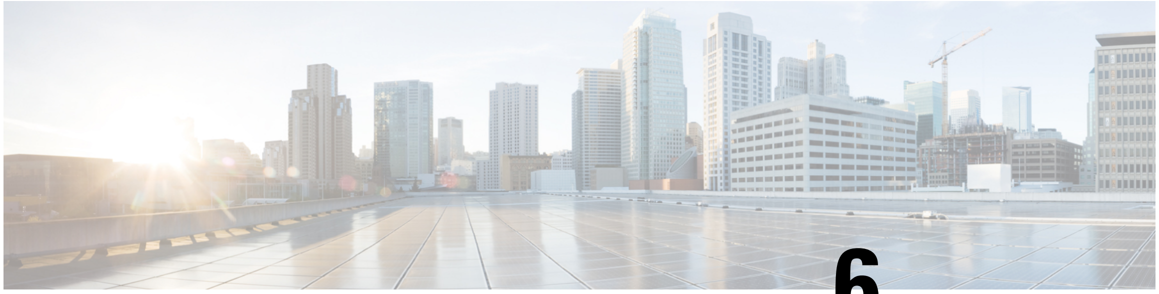
This example displays the status of the CIMC network connections:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # show link state
Interface                      State
------------------------------ --------------------
Console                        Link Detected
GE1                            No Link Detected
GE2                            No Link Detected
GE3                            No Link Detected
Dedicated                      Link Detected

Server /cimc/network # show link-state detail
Link State:
    Interface: Console
    State: Link Detected
Link State:
    Interface: GE1
    State: No Link Detected
Link State:
    Interface: GE2
    State: No Link Detected
Link State:
    Interface: GE3
    State: No Link Detected
Link State:
    Interface: Dedicated
    State: Link Detected
```

For M3 servers, the interface GE is replaced by TE. This example shows the output for M3 servers:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # show link state
Interface                      State
------------------------------ --------------------
Console                        Link Detected
GE1                            Link Detected
TE2                            No Link Detected
TE3                            No Link Detected
Dedicated                      No Link Detected
```



CHAPTER 6

Viewing Server Sensors

This chapter includes the following sections:

Viewing Temperature Sensors

SUMMARY STEPS

1. Server# **scope sensor**
2. Server /sensor # **show temperature** [**detail**]

DETAILED STEPS

	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.

Example

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

SUMMARY STEPS

1. Server# **scope sensor**
2. Server /sensor # **show voltage** [**detail**]

DETAILED STEPS

	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.

Example

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 LED Sensors

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# **scope chassis**	Enters chassis command mode.
Step 2	Server /chassis # **show led** [**detail**]	Displays the name, state, and color of the external LEDs.

Example

This example displays information about the external LEDs:

```
Server# scope chassis
Server /chassis # show led
LED Name                  LED State  LED Color
------------------------- ---------- --------
LED_SYS_ACT               OFF        GREEN
LED_HLTH_STATUS           ON         GREEN

Server /chassis #  show led detail
LEDs:
    LED Name: LED_SYS_ACT
    LED State: OFF
    LED Color: GREEN
LEDs:
    LED Name: LED_HLTH_STATUS
    LED State: ON
    LED Color: GREEN
ucs-e160dp-m1 /chassis #
```

Viewing Storage Sensors

SUMMARY STEPS

1. Server# **scope chassis**
2. Server /chassis # **show hdd** [**detail**]

DETAILED STEPS

	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.
LED Status column	The current LED color, if any. To make the physical LED on the storage device blink, select **Turn On** from the drop-down list. To let the storage device control whether the LED blinks, select **Turn Off**.

Example

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 7

Managing Remote Presence

This chapter includes the following sections:

Managing the Virtual KVM

KVM Console

The KVM console is an interface accessible from the 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.

Note The CIMC Configuration Utility is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.

- On Cisco UCS M1 and M2 servers, access the WebBIOS to configure RAID, by pressing **Ctrl-H** during bootup.

  On Cisco UCS M3 servers, access the MegaRAID controller to configure RAID, by pressing **Ctrl-R** during bootup.

Note RAID is not supported on EHWIC E-Series NCE and NIM E-Series NCE. The **Ctrl-H** and **Ctrl-R** will not work on these SKUs.

Java Requirements to Launch the KVM Console

To launch the KVM console, you must have Java release 1.6 or later installed in your system.

If the KVM console fails to launch because the certificate is revoked by Java, you must change your Java settings. Do the following:

1. Access the Java control panel.
2. Click the **Advanced** tab
3. Under **Perform certificate revocation on**, choose the **Do not check (not recommended)** radio button. For more information, see http://www.java.com/en/download/help/revocation_options.xml.

Configuring the Virtual KVM

Before you begin

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

SUMMARY STEPS

1. Server# **scope kvm**
2. Server /kvm # **set enabled** {**yes** | **no**}
3. Server /kvm # **set encrypted** {**yes** | **no**}
4. Server /kvm # **set kvm-port** *port*
5. Server /kvm # **set local-video** {**yes** | **no**}
6. Server /kvm # **set max-sessions** *sessions*
7. Server /kvm # **commit**
8. Server /kvm # **show** [**detail**]

DETAILED STEPS

	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.

	Command or Action	Purpose
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.

Example

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.

SUMMARY STEPS

1. Server# **scope kvm**
2. Server /kvm # **set enabled yes**
3. Server /kvm # **commit**
4. Server /kvm # **show** [**detail**]

DETAILED STEPS

	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.

Example

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.

SUMMARY STEPS

1. Server# **scope kvm**
2. Server /kvm # **set enabled no**
3. Server /kvm # **commit**
4. Server /kvm # **show** [**detail**]

DETAILED STEPS

	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.
Step 3	Server /kvm # **commit**	Commits the transaction to the system configuration.

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

Example

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 #
```

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 the 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.

SUMMARY STEPS

1. Server# **scope sol**
2. Server /sol # **set enabled** {**yes** | **no**}
3. Server /sol # **set baud-rate** {**9600** | **19200** | **38400** | **57600** | **115200**}
4. Server /sol # **commit**
5. Server /sol # **show** [**detail**]

DETAILED STEPS

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

Example

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

SUMMARY STEPS

1. Server# **connect host**

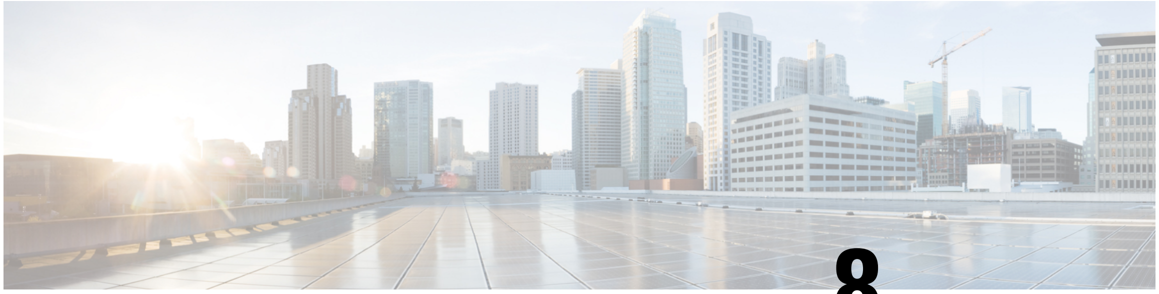
DETAILED STEPS

	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 8

Managing User Accounts

This chapter includes the following sections:

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 • Manage the power control options such as power on, power cycle, and power off

	Command or Action	Purpose
		- 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.

Example

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
```

LDAP Servers (Active Directory)

CIMC supports directory services that organize information in a directory, and manage access to this information. CIMC supports Lightweight Directory Access Protocol (LDAP), which stores and maintains directory information in a network. In addition, CIMC supports Microsoft Active Directory (AD). 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 LDAP.

When LDAP is enabled in the CIMC, user authentication and role authorization is performed by the LDAP server for user accounts not found in the local user database. The LDAP user authentication format is username@domain.com.

By checking the Enable Encryption check box in the **LDAP Settings** area, you can require the server to encrypt data sent to the LDAP server.

Configuring the LDAP Server

The CIMC can be configured to use LDAP for user authentication and authorization. To use LDAP, 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 LDAP 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.

Important For more information about altering the schema, see the article at http://technet.microsoft.com/en-us/library/bb727064.aspx.

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.

The following steps must be performed on the LDAP server.

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

Step 2 Using the 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 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 the article at http://technet.microsoft.com/en-us/library/bb727064.aspx.

What to do next

Use the CIMC to configure the LDAP server.

Configuring LDAP in CIMC

Configure LDAP in CIMC when you want to use an LDAP server for local user authentication and authorization.

Before you begin

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

SUMMARY STEPS

1. Server# **scope ldap**
2. Server /ldap # **set enabled** {**yes** | **no**}
3. Server /ldap # **set domain***LDAP domain name*
4. Server /ldap # **set timeout** *seconds*
5. Server /ldap # **set encrypted** {**yes** | **no**}
6. Server /ldap # **set base-dn** *domain-name*
7. Server /ldap # **set attribute** *name*
8. Server /ldap # **set filter-attribute**
9. Server /ldap # **commit**
10. Server /ldap # **show** [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope ldap**	Enters the LDAP command mode.
Step 2	Server /ldap # **set enabled** {**yes** | **no**}	Enables or disables LDAP security. When enabled, user authentication and role authorization is performed by LDAP for user accounts not found in the local user database.
Step 3	Server /ldap # **set domain***LDAP domain name*	Specifies an LDAP domain name.
Step 4	Server /ldap # **set timeout** *seconds*	Specifies the number of seconds the CIMC waits until the LDAP search operation times out. The value must be between 0 and 1800 seconds.
Step 5	Server /ldap # **set encrypted** {**yes** | **no**}	If encryption is enabled, the server encrypts all information sent to AD.
Step 6	Server /ldap # **set base-dn** *domain-name*	Specifies the Base DN that is searched on the LDAP server.
Step 7	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.

	Command or Action	Purpose
		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 denied.
Step 8	Server /ldap # **set filter-attribute**	Specifies the account name attribute. If Active Directory is used, then specify **sAMAccountName** for this field.
Step 9	Server /ldap # **commit**	Commits the transaction to the system configuration.
Step 10	Server /ldap # **show** [**detail**]	(Optional) Displays the LDAP configuration.

Example

This example configures LDAP using the CiscoAVPair attribute:

```
Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set domain sample-domain
Server /ldap *# set timeout 60
Server /ldap *# set encrypted yes
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# set filter-attribute sAMAccountName
Server /ldap *# commit
Server /ldap # show detail
LDAP Settings:
    Enabled: yes
    Encrypted: yes
    Domain: sample-domain
    BaseDN: example.com
    Timeout: 60
    Filter-Attribute: sAMAccountName
    Attribute: CiscoAvPair
Server /ldap #
```

What to do next

If you want to use LDAP groups for group authorization, see *Configuring LDAP Groups in CIMC*.

Configuring LDAP Groups in CIMC

Note When Active Directory (AD) group authorization is enabled and configured, user authentication is also done on the group level for users that are not found in the local user database or who are not individually authorized to use CIMC in the Active Directory.

Before you begin

- You must log in as a user with admin privileges to perform this task.
- Active Directory (or LDAP) must be enabled and configured.

SUMMARY STEPS

1. Server# **scope ldap**
2. Server /ldap# **scope ldap-group-rule**
3. Server /ldap/ldap-group-rule # **set group-auth** {**yes** | **no**}
4. Server /ldap # **scope role-group** *index*
5. Server /ldap/role-group # **set name** *group-name*
6. Server /ldap/role-group # **set domain** *domain-name*
7. Server /ldap/role-group # **set role** {**admin** | **user** | **readonly**}
8. Server /ldap/role-group # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope ldap**	Enters the LDAP command mode for AD configuration.
Step 2	Server /ldap# **scope ldap-group-rule**	Enters the LDAP group rules command mode for AD configuration.
Step 3	Server /ldap/ldap-group-rule # **set group-auth** {**yes** | **no**}	Enables or disables LDAP group authorization.
Step 4	Server /ldap # **scope role-group** *index*	Selects one of the available group profiles for configuration, where *index* is a number between 1 and 28.
Step 5	Server /ldap/role-group # **set name** *group-name*	Specifies the name of the group in the AD database that is authorized to access the server.
Step 6	Server /ldap/role-group # **set domain** *domain-name*	Specifies the AD domain the group must reside in.
Step 7	Server /ldap/role-group # **set role** {**admin** | **user** | **readonly**}	Specifies the permission level (role) assigned to all users in this AD group. This can be one of the following: • **admin**—The user can perform all actions available. • **user**—The user can perform the following tasks: • View all information • 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

	Command or Action	Purpose
		• **readonly**—The user can view information but cannot make any changes.
Step 8	Server /ldap/role-group # **commit**	Commits the transaction to the system configuration.

Example

This example shows how to configure LDAP group authorization:

```
Server# scope ldap
Server /ldap # scope ldap-group-rule
Server /ldap/ldap-group-rule # set group-auth yes
Server /ldap *# scope role-group 5
Server /ldap/role-group # set name Training
Server /ldap/role-group* # set domain example.com
Server /ldap/role-group* # set role readonly
Server /ldap/role-group* # commit
ucs-c250-M2 /ldap # show role-group
Group  Group Name       Domain Name      Assigned Role
------ -----------     --------------   --------------
1       (n/a)           (n/a)            admin
2       (n/a)           (n/a)            user
3       (n/a)           (n/a)            readonly
4       (n/a)           (n/a)            (n/a)
5      Training         example.com      readonly

Server /ldap/role-group #
```

TACACS+ Server

TACACS+ is a security protocol that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ server running, typically, on a UNIX or Windows NT workstation. You must configure a TACACS+ server before you configure the TACACS+ features on your network access server and make them available.

On the TACACS+ server, ensure you configure Cisco attribute-value (AV) pair privilege level (priv-lvl) for Cisco Integrated Management Controller (CIMC) service for the minimum privilege level of administrators and operators.

Note In CIMC 3.2.10 release or earlier, users with no privilege level or users with a privilege level less than the operator's privilege level were considered as auditors with read-only permissions.

From CIMC 3.2.10 release, users with privilege level zero do not have permissions to login to CIMC.

Restrictions TACACS+ Support for Cisco Integrated Management Controller

- CIMC 3.2.10 release supports connection to a single TACACS+ server. From CIMC 3.2.12 release onwards, configuring 3 TACACS+ server is supported.

- Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
- Accounting is not supported in CIMC 3.2.10 release. From CIMC 3.2.13 release onwards, TACACS accounting is supported. TACACS accounting will send all the configuration commands executed in CIMC GUI/CLI to TACACS server. Show commands executed in CIMC CLI/GUI will not be sent to TACACS.
- TACACS+ and LDAP configurations are exclusive, only one configuration is enabled at a time.
- Default time out is five seconds.
- Default TCP port connection is 49.
- Default login is PAP login where the username and password arrive at the network access server in a PAP protocol packet instead of details entered by the user.
- Support only for IPv4.
- Pre-shared key size is 15 characters. From CIMC 3.2.12 release onwards, shared key size got increased from 15 to 32.
- CIMC 3.2.12 release supports connection upto three TACACS+ server.
- Supported special characters in shared secret key are: **! @ % ^ * - _ & + =**

TACACS+ Operation

Before you begin

When a user attempts a simple ASCII login by authenticating to CIMC using TACACS+, the following option occurs:

CIMC eventually receives one of the following responses from the TACACS+ server:

- ACCEPT--The user is authenticated and service may begin. If CICM is configured to require authorization, authorization begins at this time.
- REJECT--The user has failed to authenticate. The user may be denied further access, or will be prompted to retry the login sequence depending on the TACACS+ server.
- CONTINUE--The user is prompted for additional authentication information.

What to do next

After authentication, CIMC sends authorization request to the TACACS+ server. Based on authorization result, CIMC assigns the user’s role.

Configure TACACS+ Server for CIMC Version 3.2.10 and 3.2.11

SUMMARY STEPS

1. Server# **scope tacacs**
2. Server/tacacs# **set tacacs-server** *ip-address*
3. Server/tacacs# **set tacacs-key** *key-string*
4. Server/tacacs# **set tacacs-enable {Yes | No}** *yes*
5. Server/tacacs# **set admin-priv 12**
6. Server/tacacs# **set oper-priv 5**
7. Server/tacacs# **commit**
8. Server/tacacs# **show [detail]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope tacacs**	Enters the scope TACACS configuration mode.
Step 2	Server/tacacs# **set tacacs-server** *ip-address*	Sets the TACACS server IP address.
Step 3	Server/tacacs# **set tacacs-key** *key-string*	Sets the pre-shared key to initiate authentication with the server.
Step 4	Server/tacacs# **set tacacs-enable {Yes | No}** *yes*	Enables or disables TACACS security for security authentication and role authorization for user accounts not found in the local user database.
Step 5	Server/tacacs# **set admin-priv 12**	Sets the administrator privilege to 12.
Step 6	Server/tacacs# **set oper-priv 5**	Sets the operator privilege to 5.
Step 7	Server/tacacs# **commit**	Commits the transaction to the system configuration.
Step 8	Server/tacacs# **show [detail]**	(Optional) Displays the TACACS configuration.

In this configuration, privilege level 14 is assigned to the administrator role, and privilege level 9 is assigned to the operator role. This means a user with privilege level 14 or higher has admin privileges when the user logs into the system, and a user with privilege level 9 or higher has all privileges of an operator at the time of login.

Privilege level below 9 has the read-only privileges.

These two are optional arguments. By default, admin-priv is 15 and oper-priv is 11.

Note After the software is downgraded to a version that supports 15 characters, ensure to change the shared key to 15 characters.

Configure TACACS+ Server for CIMC with Accounting

SUMMARY STEPS

1. Server# **scope tacacs**
2. Server/tacacs# **set tacacs-server1** *ip-address*
3. Server/tacacs# **set tacacs-key1** *key-string*
4. Server/tacacs# **set tacacs-server2** *ip-address*
5. Server/tacacs# **set tacacs-key2** *key-string*
6. Server/tacacs# **set tacacs-server3** *ip-address*
7. Server/tacacs# **set tacacs-key3** *key-string*
8. Server/tacacs# **set tacacs-enable {Yes | No}** *yes*
9. Server/tacacs# **set tacacs-cmd-acct-enable {Yes | No}** *yes*
10. Server/tacacs# **set admin-priv 12**
11. Server/tacacs# **set oper-priv 5**
12. Server/tacacs# **commit**
13. Server/tacacs# **show [detail]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope tacacs**	Enters the scope TACACS configuration mode.
Step 2	Server/tacacs# **set tacacs-server1** *ip-address*	Sets the TACACS server IP address
Step 3	Server/tacacs# **set tacacs-key1** *key-string*	Sets the pre-shared key to initiate authentication with the server. From CIMC 3.2.12 release onwards, the maximum length of the key is 32 characters.
Step 4	Server/tacacs# **set tacacs-server2** *ip-address*	Sets the TACACS server IP address
Step 5	Server/tacacs# **set tacacs-key2** *key-string*	Sets the pre-shared key to initiate authentication with the server. From CIMC release onwards, the maximum length of the key is 32 characters.
Step 6	Server/tacacs# **set tacacs-server3** *ip-address*	Sets the TACACS server IP address
Step 7	Server/tacacs# **set tacacs-key3** *key-string*	Sets the pre-shared key to initiate authentication with the server. From CIMC release onwards, the maximum length of the key is 32 characters.
Step 8	Server/tacacs# **set tacacs-enable {Yes | No}** *yes*	Enables or disables TACACS security for security authentication and role authorization for user accounts not found in the local user database.
Step 9	Server/tacacs# **set tacacs-cmd-acct-enable {Yes | No}** *yes*	Enable or Disable TACACS Server Command Accounting. TACACS Accounting will work only when TACACS and accounting is enabled. By default, TACACS accounting will be disabled.

	Command or Action	Purpose
Step 10	Server/tacacs# **set admin-priv 12**	Sets the administrator privilege to 12
Step 11	Server/tacacs# **set oper-priv 5**	Sets the operator privilege to 5
Step 12	Server/tacacs# **commit**	Commits the transaction to the system configuration.
Step 13	Server/tacacs# **show [detail]**	(Optional) Displays the TACACS configuration.

In this configuration, privilege level 14 is assigned to the administrator role, and privilege level 9 is assigned to the operator role. This means a user with privilge level 14 or higher has admin privileges when the user logs into the system, and a user with privilege level 9 or higher has all privileges of an operator at the time of login.

Privilege level below 9 has the read-only privileges.

These two are optional arguments. By default admin-priv is 15 and oper-priv is 11.

Note After the software is downgraded to a version that supports 15 characters, ensure to change the shared key to 15 characters.

Example: TACACS+ Server Configuration for CIMC Version 3.2.10 and 3.2.11

This example shows how to configure a TACACS server

```
Server /# scope tacacs
Server /tacacs# set tacacs-server1 192.168.1.1
Server /tacacs*# set tacacs-key testkey
Server /tacacs*# set tacacs-enable yes
Server /tacacs*# set admin-priv 12
Server /tacacs*# set oper-priv 5
Server /tacacs*# commit
```

Verify the TACACS+ Server Configuration

```
Server/tacacs# show detail
tacacs Settings:
Server domain name or IP address: 192.168.1.1
Enable tacacs: yes
shared-secret key: ******
admin-priv: 12
oper-priv: 5
```

Example: TACACS+ Server Configuration for CIMC with Accounting

Configure TACACS+ Server with Accounting

```
Server /# scope tacacs
Server /tacacs# set tacacs-server1 192.168.1.1
Server /tacacs*# set tacacs-key1 testkey1
Server /tacacs*# set tacacs-server2 192.168.1.2
Server /tacacs*# set tacacs-key2 testkey2
Server /tacacs*# set tacacs-server3 192.168.1.3
Server /tacacs*# set tacacs-key3 testkey3
Server /tacacs*# set tacacs-enable yes
Server /tacacs*# set tacacs-cmd-acct-enable yes
Server /tacacs*# set admin-priv 12
Server /tacacs*# set oper-priv 5
Server /tacacs*# commit
```

Verify the TACACS+ Server Configuration with Accounting

```
Server/tacacs# show detail
TACACS Settings:
Enable tacacs: yes
Enable tacacs cmd accounting: yes
Server1 domain name or IP addr: 192.168.1.1
Server2 domain name or IP addr: 192.168.1.2
Server3 domain name or IP addr: 192.168.1.3
Server1 Shared-secret key: ******
Server2 Shared-secret key: ******
Server3 Shared-secret key: ******
Admin-priv: 12
Oper-priv: 5
```

Viewing User Sessions

SUMMARY STEPS

1. Server# **show user-session**

DETAILED STEPS

	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.

Example

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.

SUMMARY STEPS

1. Server# **show user-session**
2. Server /user-session # **scope user-session** *session-number*
3. Server /user-session # **terminate**

DETAILED STEPS

	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.

Example

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 9

Configuring Network-Related Settings

This chapter includes the following sections:

CIMC NIC Configuration

CIMC NICs

Two NIC modes are available for connection to the CIMC.

Note In the case of M3 modules, GE2 and GE3 will be replaced by TE2 and TE3.

NIC Mode

- 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.

The following examples show the link state:

```
E160S /cimc/network # show link-state
Interface                      State
```

```
------------------------------ --------------------
Console                        Link Detected
GE1                            Link Detected
TE2                            Link Detected
TE3                            Link Detected
Dedicated                      No Link Detected
```

```
E1120D /cimc/network # show link-state
Interface                      State
------------------------------ --------------------
Console                        Link Detected
GE1                            Link Detected
TE2                            No Link Detected
TE3                            No Link Detected
```

The following examples show the LOM MAC list:

```
E160S /cimc/network # show lom-mac-list
Interface                      MAC Address
------------------------------ --------------------
Console                        00:f6:63:b9:65:d4
GE1                            00:f6:63:b9:65:d5
TE2                            00:f6:63:b9:65:d6
TE3                            00:f6:63:b9:65:d7
```

```
E1120D /cimc/network # show lom-mac-list
Interface                      MAC Address
------------------------------ --------------------
Console                        28:6f:7f:ee:ac:0a
GE1                            28:6f:7f:ee:ac:0b
TE2                            28:6f:7f:ee:ac:0c
TE3                            28:6f:7f:ee:ac:0d
```

Configuring CIMC NICs

Use this procedure to set the NIC mode and Interface.

Before you begin

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

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **set mode** {**dedicated** | **shared_lom**}
4. Server /cimc/network # **set interface** {**console** | **ge1**}
5. Server /cimc/network # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **set mode** {**dedicated** | **shared_lom**}	Sets the NIC mode to one of the following:

	Command or Action	Purpose
		• **dedicated**—The management Ethernet port is used to access the CIMC. • **shared LOM mode**—The LAN On Motherboard (LOM) Ethernet host ports are used to access the CIMC. **Note** In shared LOM mode, all host ports must belong to the same subnet.
Step 4	Server /cimc/network # **set interface** {**console** | **ge1**}	Sets the NIC interface to one of the following: • **console**—Internal interface, which is used to connect either the router's PCIe interface to the E-Series Server or the router's EHWIC interface to the NCE. • **ge1**—Internal interface, which is used to access the 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. **Note** All interface options that involve the GE3 interface are applicable for double-wide E-Series Servers only. **Note** For M3 servers, the interface GE is replaced by TE. **Note** If you are using the external GE2 interface on an EHWIC E-Series NCE or the NIM E-Series NCE to configure CIMC access, you might lose connectivity with CIMC during server reboot. This is expected behavior. If you must maintain connectivity with CIMC during a reboot, we recommend that you use one of the other network interfaces to configure CIMC access. See the "CIMC Access Configuration Options—EHWIC E-Series NCE" and the "CIMC Access Configuration Options—NIM E-Series NCE" sections in the *Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*.
Step 5	Server /cimc/network # **commit**	Commits the transaction to the system configuration.

	Command or Action	Purpose
		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.

Example

This example configures the CIMC network interface:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set mode shared_lom
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.

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **set hostname** *host-name*
4. Server /cimc/network # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **set hostname** *host-name*	Specifies the name of the host.
Step 4	Server /cimc/network # **commit**	Commits the transaction to the system configuration.

Example

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.

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **set dhcp-enabled** {**yes** | **no**}
4. Server /cimc/network # **set v4-addr** *ipv4-address*
5. Server /cimc/network # **set v4-netmask** *ipv4-netmask*
6. Server /cimc/network # **set v4-gateway** *gateway-ipv4-address*
7. Server /cimc/network # **set dns-use-dhcp** {**yes** | **no**}
8. Server /cimc/network # **set preferred-dns-server** *dns1-ipv4-address*
9. Server /cimc/network # **set alternate-dns-server** *dns2-ipv4-address*
10. Server /cimc/network # **commit**
11. Server /cimc/network # **show** [**detail**]

DETAILED STEPS

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

	Command or Action	Purpose
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.
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.

Example

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 IPv6

Before you begin

You must log in as a user with admin privileges to configure IPv6 network settings.

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **set v6-dhcp no**
4. Server /cimc/network # **set v6-enabled yes**
5. Server /cimc/network # **set v6-addr** *ipv6-address*
6. Server /cimc/network # **set v6-gateway** *gateway-ipv6address*
7. Server /cimc/network # **commit**
8. Server /cimc/network # **show** [**detail**]

DETAILED STEPS

	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 v6-dhcp no**	Disables DHCP.
Step 4	Server /cimc/network # **set v6-enabled yes**	Enables the IPv6 addressing.
Step 5	Server /cimc/network # **set v6-addr** *ipv6-address*	Specifies the IP address for the CIMC.
Step 6	Server /cimc/network # **set v6-gateway** *gateway-ipv6address*	Specifies the gateway for the IP address.
Step 7	Server /cimc/network # **commit**	Commits the transaction to the system configuration.
Step 8	Server /cimc/network # **show** [**detail**]	(Optional) Displays the IPv4 and IPv6 network settings.

Example

This example configures and displays the IPv6 network settings:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set v6-dhcp-no
Server /cimc/network # set v6-enabled yes
Server /cimc/network *# set v6-addr 2001:db8:101:f101:f2f7::14
Server /cimc/network *# set v6-gateway 2001:db8:101:f101:f2f7::1
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
    Network Setting:
    IPv4 Address: 10.197.82.23
    IPv4 Netmask: 255.255.255.192
    IPv4 Gateway: 10.197.82.1
    DHCP Enabled: no
    DDNS Enabled: yes
    DDNS Update Domain:
    Obtain DNS Server by DHCP: no
    Preferred DNS: 0.0.0.0
    Alternate DNS: 0.0.0.0
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Hostname: E160S
    MAC Address: 00:F6:63:B9:65:DB
    NIC Mode: shared_lom
    NIC Redundancy: none
    NIC Interface: te3
    IPv6 Enabled: yes
    IPv6 Address: 2600:0:c:87ee::12
    IPv6 Prefix: 64
    IPv6 Gateway: 2600:0:c:87ee::1
    IPv6 Link Local: fe80::2f6:63ff:feb9:65db
    IPv6 SLAAC Address: 2600:0:c:bfe7:2f6:63ff:feb9:65db
    IPV6 DHCP Enabled: no
    IPV6 Obtain DNS Server by DHCP: no
    IPV6 Preferred DNS: ::
    IPV6 Alternate DNS: ::
E160S /cimc/network #
```

Configuring the Server VLAN

Before you begin

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

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **set vlan-enabled** {**yes** | **no**}
4. Server /cimc/network # **set vlan-id** *id*
5. Server /cimc/network # **set vlan-priority** *priority*
6. Server /cimc/network # **commit**
7. Server /cimc/network # **show** [**detail**]

DETAILED STEPS

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

Example

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. The 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.

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **scope ipblocking**

4. Server /cimc/network/ipblocking # **set enabled** {**yes** | **no**}
5. Server /cimc/network/ipblocking # **set fail-count** *fail-count*
6. Server /cimc/network/ipblocking # **set fail-window** *fail-seconds*
7. Server /cimc/network/ipblocking # **set penalty-time** *penalty-seconds*
8. Server /cimc/network/ipblocking # **commit**
9. Server /cimc/network/ipblocking # **exit**
10. Server /cimc/network # **scope ipfiltering**
11. Server /cimc/network/ipfiltering # **set enabled** {**yes** | **no**}
12. Server /cimc/network/ipfiltering # **set filter-1** *IPv4 or IPv6 address or a range of IP addresses*
13. Server /cimc/network/ipfiltering # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **scope ipblocking**	Enters 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.
Step 9	Server /cimc/network/ipblocking # **exit**	Exits the IP blocking to the network command mode.
Step 10	Server /cimc/network # **scope ipfiltering**	Enters the IP filtering command mode.
Step 11	Server /cimc/network/ipfiltering # **set enabled** {**yes** | **no**}	Enables or disables IP filtering. At the prompt enter **y** to enable IP filtering.

	Command or Action	Purpose
Step 12	Server /cimc/network/ipfiltering # **set filter-1** *IPv4 or IPv6 address or a range of IP addresses*	You can set up to 20 IP filters. You can assign an IPv4 or IPv6 IP address or a range of IP addresses.
Step 13	Server /cimc/network/ipfiltering # **commit**	Commits the transaction to the system configuration.

Example

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 #
```

This example configures IP filtering:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope ipfiltering
Server /cimc/network/ ipfiltering# set enabled yes
Server /cimc/network/ ipfiltering# set filter-1 10.227.240.18
Server /cimc/network/ ipfiltering#commit
```

Configuring Network Analysis Module Capability

Before you begin

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

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **scope nam**
4. Server /cimc/network/nam # **set enabled yes**
5. Server /cimc/network/nam # **show detail**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	Server /cimc/network # **scope nam**	Enters Network Analysis Module (NAM) command mode.
Step 4	Server /cimc/network/nam # **set enabled yes**	Enables the NAM capability. To disable the NAM capability, use the **set enabled no** command.
Step 5	Server /cimc/network/nam # **show detail**	Verifies that the NAM capability is enabled or disabled.

Example

This example configures the common properties:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope nam
Server /cimc/network/nam # set enabled yes
Server /cimc/network/nam # show detail
Network Analysis Module:
    Enabled: yes
```

NTP Settings Configuration

NTP Settings

By default, when CIMC is reset, it synchronizes the time with the host. With the introduction of the Network Time Protocol (NTP) service, you can configure CIMC to synchronize the time with an NTP server. The NTP server does not run in CIMC by default. You must enable and configure the NTP service by specifying the IP or DNS address of at least one server or a maximum of four servers that function as NTP servers or time source servers. When you enable the NTP service, CIMC synchronizes the time with the configured NTP server. The NTP service can be modified only through CIMC.

Note To enable the NTP service, it is preferable to specify the IP address of a server rather than the DNS address.

Configuring NTP Settings

Before you begin

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

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope network**

3. Server /cimc/network # **scope ntp**
4. Server /cimc/network/ntp # **set enabled yes**
5. Server /cimc/network/ntp # **set** [**server-1** | **server-2** | **server-3** | **server-4**] *ip-address or domain-name*
6. Server /cimc/network/ntp # **show detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope network**	Enters CIMC network command mode.
Step 3	Server /cimc/network # **scope ntp**	Enters NTP command mode.
Step 4	Server /cimc/network/ntp # **set enabled yes**	Enables the NTP service. To disable the NTP service, use the **set enabled no** command.
Step 5	Server /cimc/network/ntp # **set** [**server-1** | **server-2** | **server-3** | **server-4**] *ip-address or domain-name*	Configures the IP address or domain name for the specified server to act as an NTP server or the time source server. You can configure a maximum of four servers.
Step 6	Server /cimc/network/ntp # **show detail**	Displays whether the NTP service is enabled and the IP address or domain name of the NTP servers.

Example

This example configures NTP settings:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope ntp
Server /cimc/network/ntp # set enabled yes
Server /cimc/network/ntp # set server-1 10.50.171.9
Server /cimc/network/ntp # set server-2 time.cisco.com
Server /cimc/network/ntp # show detail
NTP Service Settings:
    Enabled: yes
    Server 1: 10.50.171.9
    Server 2: time.cisco.com
    Server 3:
    Server 4:
```

CHAPTER 10

Configuring Communication Services

This chapter includes the following sections:

Configuring HTTP

Before you begin

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

SUMMARY STEPS

1. Server# **scope http**
2. Server /http # **set enabled** {**yes** | **no**}
3. Server /http # **set http-port** *number*
4. Server /http # **set https-port** *number*
5. Server /http # **set timeout** *seconds*
6. Server /http # **commit**

DETAILED STEPS

	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.

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

Example

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.

SUMMARY STEPS

1. Server# **scope ssh**
2. Server /ssh # **set enabled** {**yes** | **no**}
3. Server /ssh # **set ssh-port** *number*
4. Server /ssh # **set timeout** *seconds*
5. Server /ssh # **commit**
6. Server /ssh # **show** [**detail**]

DETAILED STEPS

	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.

	Command or Action	Purpose
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.

Example

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 #
```

Enabling Redfish

Before you begin

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

SUMMARY STEPS

1. Server# **scope redfish**
2. Server /redfish # **set enabled** {**yes** | **no**}
3. Server /redfish* # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope redfish**	Enters redfish command mode.
Step 2	Server /redfish # **set enabled** {**yes** | **no**}	Enables or disables redfish control of Cisco IMC.
Step 3	Server /redfish* # **commit**	Commits the transaction to the system configuration.

Example

This example enables redfish control of Cisco IMC and commits the transaction:

```
Server# scope redfish
Server /redfish # set enabled yes
Server /redfish *# commit
Server /redfish #  show detail
REDFISH Settings:
    Enabled: yes
    Active Sessions: 0
    Max Sessions: 4

Server /redfish #
```

For more information, see Cisco UCS C-Series Servers REST API Programmer's Guide, Release 3.0

Configuring the XML API

XML API for the CIMC

The Cisco CIMC XML application programming interface (API) is a programmatic interface to the CIMC for the E-Series Server. The API accepts XML documents through HTTP or HTTPS.

For detailed information about the XML API, see the *CIMC XML API Programmer's Guide for Cisco UCS E-Series Servers*.

Enabling the XML API

Before you begin

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

SUMMARY STEPS

1. Server# **scope xmlapi**
2. Server /xmlapi # **set enabled** {**yes** | **no**}
3. Server /xmlapi *# **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope xmlapi**	Enters XML API command mode.
Step 2	Server /xmlapi # **set enabled** {**yes** | **no**}	Enables or disables XML API control of the CIMC.
Step 3	Server /xmlapi *# **commit**	Commits the transaction to the system configuration.

Example

This example enables XML API control of the CIMC and commits the transaction:

```
Server# scope xmlapi
Server /xmlapi # set enabled yes
Server /xmlapi *# commit
Server /xmlapi #  show detail
XMLAPI Settings:
    Enabled: yes
    Active Sessions: 0
    Max Sessions: 4
```

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

	Command or Action	Purpose
		"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. • **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.

Example

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. For information on Management Information Base (MIB) files supported by CIMC, see the *MIB Quick Reference for Cisco UCS* at this URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/reference/UCS_MIBRef.html.

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.
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 # **setcommunity-access**	This can be one of the following : Disabled, Limited, or Full.
Step 6	Server /snmp # **settrap-community-str**	Specifies the SNMP community group to which trap information should be sent. The name can be up to 18 characters
Step 7	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 8	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 9	Server /snmp # **commit**	Commits the transaction to the system configuration.

Example

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 community-access Full
Server /snmp # set trap-community-str public
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: public
    SNMP Community access: Full
    Enabled: yes

Server /snmp #
```

What to do next

Configure SNMP trap settings as described in Configuring SNMP Trap Settings, on page 124.

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 # **scope trap-destinations** *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 15.
Step 3	Server /snmp/trap-destinations # **set enabled** {**yes** | **no**}	Enables or disables the SNMP trap destination.
Step 4	Server /snmp/trap-destinations # **set version** {**1** | **2** | **3**}	Specify the desired SNMP version of the trap message. **Note** SNMPv3 traps will be delivered only to locations where the SNMPv3 user and key values are configured correctly.
Step 5	Server /snmp/trap-destinations # **set type** {**trap** | **inform**}	Specifies whether SNMP notification messages are sent as simple traps or as inform requests requiring acknowledgment by the receiver. **Note** The inform option can be chosen only for V2 users.

	Command or Action	Purpose
Step 6	Server /snmp/trap-destinations # **set user** *user*	
Step 7	Server /snmp/trap-destination # **set v4-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.

Example

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

```
Server# scope snmp
Server /snmp # Scope trap-destinations 1
Server /snmp/trap-destination *# set enabled yes
Server /snmp/trap-destination *#  set version 2
Server /snmp/trap-destination *# set type inform
Server /snmp/trap-destination *# set user user1
Server /snmp/trap-destination *# set v4-addr 192.2.3.4
Server /snmp/trap-destination *# commit
Server /snmp/trap-destination # show detail
Trap Destination 1:
    Enabled: yes
    SNMP version: 2
    Trap type: inform
    SNMP user: user1
    IPv4 Address: 192.2.3.4
    Delete Trap: no
Server /snmp/trap-destination #
```

Note From CIMC 3.2.13 release, SNMP trap support for storage disk removal or insertion is supported in ENCS.

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 # **sendSNMPtrap**	Sends an SNMP test trap to the configured SNMP trap destination that are enabled. **Note** The trap must be configured and enabled in order to send a test message.

Example

This example sends a test message to all the enabled SNMP trap destinations:

```
Server# scope snmp
Server /snmp # sendSNMPtrap
SNMP Test Trap sent to the destination.
Server /snmp #
```

Configuring SNMPv3 Users

Before you begin

- You must log in as a user with admin privileges to perform this task.
- SNMP must be enabled and saved before these configuration commands are accepted.

SUMMARY STEPS

1. Server# **scope snmp**
2. Server /snmp # **scope v3users** *number*
3. Server /snmp/v3users # **set v3add** {**yes** | **no**}
4. Server /snmp/v3users # **set v3security-name** *security-name*
5. Server /snmp/v3users # **set v3security-level** {**noauthnopriv** | **authnopriv** | **authpriv**}
6. Server /snmp/v3users # **set v3proto** {**MD5** | **SHA**}
7. Server /snmp/v3users # **set v3auth-key** *auth-key*
8. Server /snmp/v3users # **set v3priv-proto** {**DES** | **AES**}
9. Server /snmp/v3users # **set v3priv-auth-key** *priv-auth-key*
10. Server /snmp/v3users # **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope snmp**	Enters the SNMP command mode.
Step 2	Server /snmp # **scope v3users** *number*	Enters the SNMPv3 users command mode for the specified user number.
Step 3	Server /snmp/v3users # **set v3add** {**yes** | **no**}	Adds or deletes an SNMPv3 user. This can be one of the following: • **yes**—This user is enabled as an SNMPv3 user and is allowed to access the SNMP OID tree. **Note** The security name and security level must also be configured at this time or the user addition will fail. • **no**—This user configuration is deleted.

	Command or Action	Purpose
Step 4	Server /snmp/v3users # **set v3security-name** *security-name*	Enter an SNMP username for this user.
Step 5	Server /snmp/v3users # **set v3security-level** {**noauthnopriv** | **authnopriv** | **authpriv**}	Select a security level for this user. This can be one of the following: • **noauthnopriv**—The user does not require an authorization or privacy password. • **authnopriv**—The user requires an authorization password but not a privacy password. If you select this option, you must configure an authentication key. • **authpriv**—The user requires both an authorization password and a privacy password. If you select this option, you must configure an authentication key and a private encryption key.
Step 6	Server /snmp/v3users # **set v3proto** {**MD5** | **SHA**}	Select an authentication protocol for this user.
Step 7	Server /snmp/v3users # **set v3auth-key** *auth-key*	Enter an authorization password for this user.
Step 8	Server /snmp/v3users # **set v3priv-proto** {**DES** | **AES**}	Select an encryption protocol for this user.
Step 9	Server /snmp/v3users # **set v3priv-auth-key** *priv-auth-key*	Enter a private encryption key (privacy password) for this user.
Step 10	Server /snmp/v3users # **commit**	Commits the transaction to the system configuration.

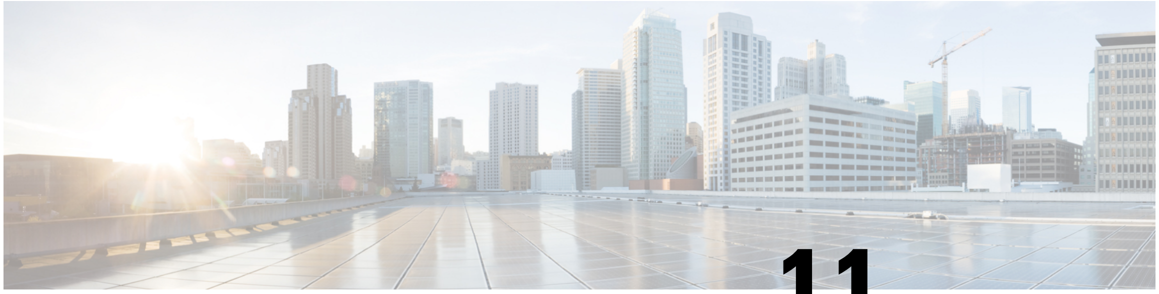
Example

This example configures SNMPv3 user number 2 and commits the transaction:

```
Server# scope snmp
Server /snmp # scope v3users 2
Server /snmp/v3users # set v3add yes
Server /snmp/v3users *# set v3security-name ucsSNMPV3user
Server /snmp/v3users *# set v3security-level authpriv
Server /snmp/v3users *# set v3proto SHA
Server /snmp/v3users *# set v3auth-key
Please enter v3auth-key:ex4mp1ek3y
Please confirm v3auth-key:ex4mp1ek3y
Server /snmp/v3users *# set v3priv-proto AES
Server /snmp/v3users *# set v3priv-auth-key
Please enter v3priv-auth-key:!1@2#3$4%5^6&7*8
Please confirm v3priv-auth-key:!1@2#3$4%5^6&7*8
Server /snmp/v3users *# commit
Settings are being applied ... allow a few minutes for the process to complete
Server /snmp/v3users # show detail
User 2:
    Add User: yes
    Security Name: ucsSNMPV3user
    Security Level: authpriv
    Auth Type: SHA
    Auth Key: ******
```

```
        Encryption: AES
        Private Key: ******

Server /snmp/v3users #
```



CHAPTER 11

Managing Certificates

This chapter includes the following sections:

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.

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.

SUMMARY STEPS

1. Server# **scope certificate**
2. Server /certificate # **generate-csr**

DETAILED STEPS

	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.

Example

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 the 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 the 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.

Example

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.

SUMMARY STEPS

1. Server# **scope certificate**
2. Server /certificate # **upload**

DETAILED STEPS

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

	Command or Action	Purpose
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.

Example

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 12

Configuring Platform Event Filters

This chapter includes the following sections:

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

SUMMARY STEPS

1. Server# **scope fault**
2. Server /fault # **set platform-event-enabled yes**
3. Server /fault # **commit**
4. Server /fault # **show** [**detail**]

DETAILED STEPS

	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.

	Command or Action	Purpose
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.

Example

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

SUMMARY STEPS

1. Server# **scope fault**
2. Server /fault # **set platform-event-enabled no**
3. Server /fault # **commit**
4. Server /fault # **show** [**detail**]

DETAILED STEPS

	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.

Example

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

SUMMARY STEPS

1. Server# **scope fault**
2. Server /fault # **scope pef** *id*
3. Server /fault/pef # **set action** {**none** | **reboot** | **power-cycle** | **power-off**}
4. Server /fault/pef # **set send-alert** {**yes** | **no**}
5. Server /fault/pef # **commit**

DETAILED STEPS

	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.

	Command or Action	Purpose
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. **Note** The **set send-alert** command is deprecated from Release 3.1.1 and later releases. Instead of this command, you can use SNMP to trigger alert.
Step 5	Server /fault/pef # **commit**	Commits the transaction to the system configuration.

Example

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

Interpreting Platform Event Traps

A CIMC platform event alert sent as an SNMP trap contains an enterprise object identifier (OID) in the form `1.3.6.1.4.1.3183.1.1.0.`*`event`*. The first ten fields of the OID represent the following information: `iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).wired_for_management(3183).PET(1).version(1).version(0)`, indicating an IPMI platform event trap (PET) version 1.0 message. The last field is an event number, indicating the specific condition or alert being notified.

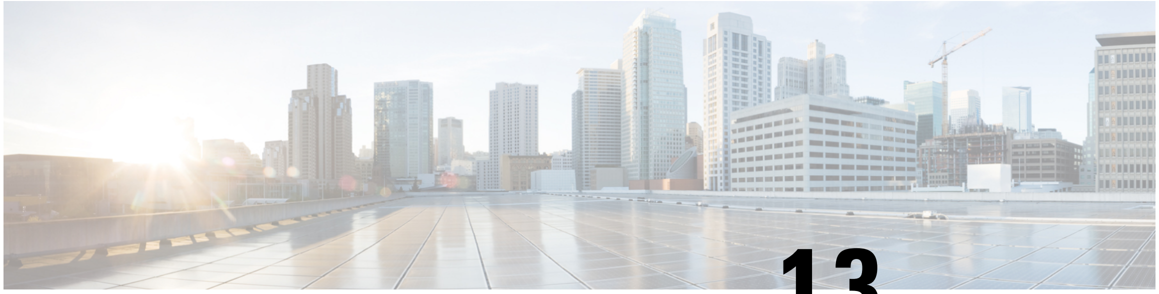
Platform Event Trap Descriptions

The following table provides a description of the event being notified in a platform event trap message, based on the event number in the trap OID.

Event Number [Note 1]		Platform Event Description
0	0h	Test Trap
65799	010107h	Temperature Warning
65801	010109h	Temperature Critical
131330	020102h	Under Voltage, Critical
131337	020109h	Voltage Critical
196871	030107h	Current Warning
262402	040102h	Fan Critical
459776	070400h	Processor related (IOH-Thermalert/Caterr sensor) – predictive failure deasserted
459777	070401h	Processor related (IOH-Thermalert/Caterr sensor) – predictive failure asserted
460032	070500h	Processor Power Warning – limit not exceeded
460033	070501h	Processor Power Warning – limit exceeded
524533	0800F5h	Power Supply Critical
524551	080107h	Power Supply Warning
525313	080401h	Discrete Power Supply Warning
527105	080B01h	Power Supply Redundancy Lost
527106	080B02h	Power Supply Redundancy Restored
552704	086F00h	Power Supply Inserted
552705	086F01h	Power Supply Failure
552707	086F03h	Power Supply AC Lost
786433	0C0001h	Correctable ECC Memory Errors, Release 1.3(1) and later releases, filter set to accept all reading types [Note 4]
786439	0C0007h	DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM), Generic Sensor [Notes 2,3]
786689	0C0101h	Correctable ECC Memory Errors, Release 1.3(1) and later releases
818945	0C7F01h	Correctable ECC Memory Errors, Release 1.2(x) and earlier releases
818951	0C7F07h	DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM), 1.2(x) and earlier releases [Note 3]
851968	0D0000h	HDD sensor indicates no fault, Generic Sensor [Note 2]
851972	0D0004h	HDD sensor indicates a fault, Generic Sensor [Note 2]
854016	0D0800h	HDD Absent, Generic Sensor [Note 2]
854017	0D0801h	HDD Present, Generic Sensor [Note 2]
880384	0D6F00h	HDD Present, no fault indicated

Event Number [Note 1]		Platform Event Description
880385	0D6F01h	HDD Fault
880512	0D6F80h	HDD Not Present
880513	0D6F81h	HDD is deasserted but not in a fault state
884480	0D7F00h	Drive Slot LED Off
884481	0D7F01h	Drive Slot LED On
884482	0D7F02h	Drive Slot LED fast blink
884483	0D7F03h	Drive Slot LED slow blink
884484	0D7F04h	Drive Slot LED green
884485	0D7F05h	Drive Slot LED amber
884486	0D7F01h	Drive Slot LED blue
884487	0D7F01h	Drive Slot LED read
884488	0D7F08h	Drive Slot Online
884489	0D7F09h	Drive Slot Degraded

Note When the event filter is set to accept all reading types, bits 15:8 of the hex event number are masked to 0. For example, event number 786689 (0C0101h) becomes 786433 (0C0001h).



CHAPTER 13

Firmware Management

This chapter includes the following sections:

Overview of Firmware

E-Series Servers use Cisco-certified firmware specific to the E-Series Server model that you are using. You can download new releases of the firmware for all supported server models from Cisco.com.

To avoid potential problems, we strongly recommend that you use the Host Upgrade Utility (HUU), which upgrades the CIMC, BIOS, and other firmware components to compatible levels. For detailed information about this utility, see the "Upgrading Firmware" chapter in the *Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*. This chapter also provides information about the compatible HUU, CIMC, and BIOS software releases.

Note If you are running CIMC version 2.2.x, first upgrade to version 2.3.2 and then upgrade to 3.2.x.

Note The HUU is supported on CIMC, release 2.1.0 and later releases.

If you choose to upgrade the CIMC and BIOS firmware manually—instead of using the HUU—you must update the CIMC firmware first, and then the BIOS firmware. Do not install the new BIOS firmware until after you have activated the compatible CIMC firmware or the server will not boot.

The CIMC firmware update process is divided into the following stages to minimize the amount of time the server will be offline:

- **Installation**—During this stage, CIMC installs the selected CIMC firmware in the non-active, or backup, slot on the server.
- **Activation**—During this stage, CIMC sets the non-active firmware version as active and reboots the server, causing a disruption in service. When the server reboots, the firmware in the new active slot becomes the running version.

After you activate the CIMC firmware, you can update the BIOS firmware. The server must be powered off during the entire BIOS update process. Once the CIMC finishes rebooting, the server can be powered on and returned to service.

Note You can either upgrade an older firmware version to a newer one, or downgrade a newer firmware version to an older one.

Options for Upgrading Firmware

You can use either the Cisco Host Upgrade Utility (HUU) to upgrade the firmware components or you can upgrade the firmware components manually.

- **HUU**—We recommend that you use the HUU ISO file to upgrade all firmware components, which include the CIMC and BIOS firmware.
- **Manual Upgrade**—To manually upgrade the CIMC and BIOS firmware, you must first obtain the firmware from Cisco Systems, and then use the CIMC GUI or the CIMC CLI to upgrade it. After you upgrade the firmware, reboot the system.

Obtaining Software from Cisco Systems

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

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 categories.

- **Unified Computing System (UCSE) Server Drivers**—Contains drivers.
- **Unified Computing System (UCSE) Server Firmware**—Contains the Host Upgrade Utility and the BIOS, CIMC, and PLD firmware images.
- **Unified Computing System (UCSE) Utilites**—Contains the diagnostics 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 a Remote Server

Note To avoid potential problems, we strongly recommend that you use the Host Upgrade Utility (HUU), which upgrades the CIMC, BIOS, and other firmware components to compatible levels. For detailed information about this utility, see the "Upgrading Firmware" chapter in the *Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*. This chapter also provides information about the compatible HUU, CIMC, and BIOS software releases.

If you choose to upgrade the CIMC and BIOS firmware manually—instead of using the HUU—you must update the CIMC firmware first, and then the BIOS firmware. Do not install the new BIOS firmware until after you have activated the compatible CIMC firmware or the server will not boot.

Before you begin

- Log into CIMC as a user with admin privileges.
- Obtain the CIMC firmware file from Cisco Systems. See Obtaining Software from Cisco Systems, on page 142.

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

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope firmware**
3. Server /cimc/firmware # **update** *protocol ip-address path*
4. (Optional) Server /cimc # **show detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope firmware**	Enters CIMC firmware command mode.
Step 3	Server /cimc/firmware # **update** *protocol ip-address path*	Specifies the protocol, IP address of the remote server, and the file path to the firmware file on the server. The protocol can be one of the following: • **tftp** • **ftp** • **sftp** • **scp**

	Command or Action	Purpose
		• **http**
Step 4	(Optional) Server /cimc # **show detail**	Displays the progress of the firmware update.

Example

This example updates the firmware:

```
Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # update tftp 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.

Important While the activation is in progress, do not:

- Reset, power off, or shut down the server.
- Reboot or reset the CIMC.
- Activate any other firmware.
- Export technical support or configuration data.

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

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **show** [**detail**]
3. Server /cimc # **activate** [**1** | **2**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters 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.

Example

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
```

Changing Password Storage Format

This procedure explains how to change the format of the password storage.

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **change-password-storage**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **change-password-storage**	Changes the format of the password storage. You will be prompted before changing the format.

Example

This example changes the format:

```
Server# scope cimc
Server /cimc # change-password-storage
```

```
This operation will change the user password storage form to be SHA512 with salt.
Note that, once you start this operation:
   1. You cannot change the password storage format back.
   2. The IPMI over LAN feature will stop working.
   3. You need to change the passwords of all local users to have them
      stored in the new format.
Are you sure you want to continue?[y|N]
```

Press Y to change the format.

Installing BIOS Firmware

Note To avoid potential problems, we strongly recommend that you use the Host Upgrade Utility (HUU), which upgrades the CIMC, BIOS, and other firmware components to compatible levels. For detailed information about this utility, see the "Upgrading Firmware" chapter in the *Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*. This chapter also provides information about the compatible HUU, CIMC, and BIOS software releases.

If you choose to upgrade the CIMC and BIOS firmware manually—instead of using the HUU—you must update the CIMC firmware first, and then the BIOS firmware. Do not install the new BIOS firmware until after you have activated the compatible CIMC firmware or the server will not boot.

Before you begin

Obtain the CIMC firmware file from Cisco Systems. See Obtaining Software from Cisco Systems, on page 142.

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

Note Before you update the BIOS firmware, power off the server.

SUMMARY STEPS

1. Server# **scope bios**
2. Server /bios # **update protocol** *ip-address path-and-filename*
3. (Optional) Server /bios # **show detail**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	Server /bios # **update protocol** *ip-address path-and-filename*	Starts the BIOS firmware update. Specifies the protocol, IP address of the remote server and the file path to the firmware file on the server. The protocol can be one of the following: • TFTP • SCP
Step 3	(Optional) Server /bios # **show detail**	Displays the progress of the BIOS firmware update.

Example: Installing BIOS Firmware

This example updates the BIOS firmware:

```
Server# scope bios
Server /bios # update tftp 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 #
```

Upgrading Programmable Logic Devices Firmware on the E-Series EHWIC NCE

Use this procedure to upgrade the Programmable Logic Devices (PLD) firmware image on the EHWIC E-Series NCE.

Before you begin

Obtain the PLD firmware image from Cisco Systems. See Obtaining Software from Cisco Systems, on page 142.

Procedure

	Command or Action	Purpose
Step 1	Router # **copy tftp flash**	Obtains the PLD image file from the specified TFTP server and copies it to the router flash.
Step 2	Router # **ucse subslot** *slot/port-adapter* **fpga-upgrade flash:***filename*	Upgrades the PLD firmware. Press **Enter** at the confirmation prompt to continue with the upgrade.
Step 3	Power cycle the router.	PLD firmware takes effect after the router power cycles.
Step 4	(Optional) EN120E-FOC181290L1 /cimc/firmware # **show detail**	From the EHWIC E-Series NCE, CIMC firmware command mode, look at the CPLD version number to verify that the PLD firmware is upgraded.

Example

This example updates the PLD firmware image:

```
Router# copy tftp flash
Address or name of remote host []? 10.20.34.56
Source filename []? test/pld/alpha_v3p0e_c.rbf
Destination filename [alpha_v3p0e_c.rbf]?
Accessing tftp://10.20.34.56/test/pld/alpha_v3p0e_c.rbf...
Loading test/pld/alpha_v3p0e_c.rbf from 10.20.34.56 (via GigabitEthernet0/0): !!
[OK - 442475 bytes]

442475 bytes copied in 1.824 secs (242585 bytes/sec)


Router# ucse subslot 1/0 fpga-upgrade flash:alpha_v3p0e_c.rbf
Start fpga upgrade? [confirm]
FPGA Upgrade process started...
Step 1: Reading file flash:alpha_v3p0e_c.rbf from flash.!!.. done reading 442475 bytes
Step 2: Erasing the module flash.eeeeeeeeeeeeeee... Done
Step 3: Downloading contents to module
flash.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!...
 Done
Step 4: Validating the flash
data.vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv...
 Done
Total time: 906 seconds
Fpga Upgraded successfully...!

EN120E-FOC181290L1 /cimc/firmware # show detail
  Firmware Image Information:
    Update Stage: NONE
    Update Progress: 0%
    Current FW Version: 2.3(1.20140808133703)
    FW Image 1 Version: 2.3(1.20140808133703)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 2.3(2.20140916114316)
    FW Image 2 State: BACKUP INACTIVATED
    Boot-loader Version: 2.3(1.20140808133703).33
    CPLD Version: 3.14
    Hardware Version: 2
```

Troubleshooting E-Series Server or NCE Access Issues

If you have problems accessing the E-Series Server or NCE, it could be that the CIMC firmware image is corrupted, or the SD card is faulty, or the file system is corrupted, or the CIMC firmware installation did not complete successfully. Do one of the following as appropriate:

- If the CIMC firmware image is corrupted, see Recovering from a Corrupted CIMC Firmware Image, on page 150.
- If the SD card is faulty, see Recovering from a Faulty SD Card, on page 153.
- If the file system is corrupted, see Recovering from a Corrupted File System, on page 156.
- If the CIMC firmware installation did not complete successfully, reinstall the CIMC firmware.

Important Due to security considerations, the **boot backup** command is disabled.

Recovering from a Corrupted CIMC Firmware Image

Before you begin

- Connect the server to your PC. Depending on the type of server, do one of the following as appropriate:
  - Double-wide E-Series Server—Connect one end of the serial cable to the E-Series Server serial port and the other end to your PC.
  - Single-wide E-Series Server and SM E-Series NCE—First, connect a KVM connector to the E-Series Server or SM E-Series NCE's KVM port; and then connect one end of a serial cable to the DB9 port of the KVM connector and the other end to your PC.
  - EHWIC E-Series NCE— Connect the mini-USB end of the cable to the EHWIC E-Series NCE's mini-USB port; and then connect the other end of the USB cable to the USB port on your PC.

    Note The mini-USB cable is not provided with the EHWIC E-Series NCE. You must purchase your own mini-USB cable.
- Depending on the interface option that you specify, do one of the following:
  - Dedicated—Attach an Ethernet cable to the Management (dedicated) port of the E-Series Server.

    Note Dedicated mode is not applicable to the EHWIC E-Series NCE.
  - Shared-Lom-GE2—Attach an Ethernet cable to the E-Series Server or the NCE's external GE2 interface.
  - Shared-Lom-Console—Use the Cisco IOS CLI to configure the E-Series Server or the NCE's internal Console interface.
- To view the serial output, start the Hyper Terminal or Minicom as appropriate. Do one of the following:
  - Microsoft Windows—Start Hyper Terminal.
  - Linux—Start Minicom.
- Make sure that the communications settings are configured as: 9600 baud, 8 bits, No parity, and 1 stop bit.

Procedure

	Command or Action	Purpose
Step 1	Router# **hw-module sm** *slot* **oir-stop**	Shuts down the power to the specified E-Series Server.

	Command or Action	Purpose
		Note The Cisco 2900 series ISR G2 does not support OIR of the E-Series Servers. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the E-Series Server from the Cisco 2900 ISR G2. **Note** The ISR G2 does not support OIR of the EHWIC E-Series NCE. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the EHWIC E-Series NCE from the router.
Step 2	Router# **hw-module sm** *slot* **oir-start**	Restarts the specified E-Series Server. **Note** The Cisco 2900 series ISR G2 does not support OIR of the E-Series Servers. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the E-Series Server from the Cisco 2900 ISR G2. **Note** The ISR G2 does not support OIR of the EHWIC E-Series NCE. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the EHWIC E-Series NCE from the router.
Step 3	***	From the Hyper Terminal or Minicom, enter the ******* command to enter the bootloader prompt.
Step 4	ucse-cimc > **boot current recovery**	Boots the E-Series Server from the current image.
Step 5	Recovery-shell # **interface [dedicated | shared-lom-console | shared-lom-ge1 | shared-lom-ge2 | shared-lom-ge3]** *interface-ip-address netmask gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway ip address of the specified interface. **Note** Dedicated mode is not applicable to the EHWIC E-Series NCE. GE3 is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.
Step 6	Recovery-shell # **ping** *tftp-ip-address*	Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.
Step 7	Recovery-shell # **update** *tftp-ip-address image-filename*	Installs the CIMC firmware image, which is located on a remote tftp server.
Step 8	Recovery-shell # **reboot**	Reboots CIMC.

Example

This example recovers the CIMC firmware image in an E-Series Server:

```
Router# hw-module subslot 2/0 stop
Router# hw-module subslot 2/0 start

***

ucse-cimc > boot current recovery
recovery-shell# interface shared-lom-ge2 192.168.0.138 255.255.255.0 192.168.0.1
Network configuration:
        IP config: addr: 192.168.0.138 Mask: 255.255.255.0
        Gateway: 192.168.0.1
recovery-shell# ping 10.20.34.56
PING 10.20.34.56 (10.20.34.56): 56 data bytes
64 bytes from 10.20.34.56: seq=0 ttl=60 time=10.000 ms
64 bytes from 10.20.34.56: seq=1 ttl=60 time=0.000 ms
--- 10.20.34.56 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.000/1.000/10.000 ms
recovery-shell# update 10.20.34.56 update_pkg-cimc.combined.bin
downloading firmware image "update_pkg-cimc.combined.bin" from " 10.20.34.56 "
download firmware image done, size in bytes: 22384144
installing firmware image, please wait ...
activating installed image
done
Stage: NONE
Status: SUCCESS
Error: Success
recovery-shell# reboot
```

This example recovers the CIMC firmware image in an EHWIC E-Series NCE.

```
***

ucse-cimc > boot current recovery
recovery-shell# interface shared-lom-ge2 192.168.0.138 255.255.255.0 192.168.0.1
Network configuration:
        IP config: addr: 192.168.0.138 Mask: 255.255.255.0
        Gateway: 192.168.0.1
recovery-shell# ping 10.20.34.56
PING 10.20.34.56 (10.20.34.56): 56 data bytes
64 bytes from 10.20.34.56: seq=0 ttl=60 time=10.000 ms
64 bytes from 10.20.34.56: seq=1 ttl=60 time=0.000 ms
--- 10.20.34.56 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.000/1.000/10.000 ms
recovery-shell# update 10.20.34.56 update_pkg-cimc.combined.bin
downloading firmware image "update_pkg-cimc.combined.bin" from " 10.20.34.56 "
download firmware image done, size in bytes: 22384144
installing firmware image, please wait ...
activating installed image
done
Stage: NONE
Status: SUCCESS
Error: Success
recovery-shell# reboot
```

Recovering from a Faulty SD Card

If you have problems booting the E-Series Server or NCE, it could be because the SD card is faulty. Use this procedure to recover the CIMC firmware image on a new SD card.

Caution Do not swap SD cards between UCS E-Series Servers.

Before you begin

- Connect the server to your PC. Depending on the type of server, do one of the following as appropriate:
  - Double-wide E-Series Server—Connect one end of the serial cable to the E-Series Server serial port and the other end to your PC.
  - Single-wide E-Series Server and SM E-Series NCE—First, connect a KVM connector to the E-Series Server or SM E-Series NCE's KVM port; and then connect one end of a serial cable to the DB9 port of the KVM connector and the other end to your PC.
  - EHWIC E-Series NCE— Connect the mini-USB end of the cable to the EHWIC E-Series NCE's mini-USB port; and then connect the other end of the USB cable to the USB port on your PC.

    Note The mini-USB cable is not provided with the EHWIC E-Series NCE. You must purchase your own mini-USB cable.

- Depending on the interface option that you specify, do one of the following:
  - Dedicated—Attach an Ethernet cable to the Management (dedicated) port of the E-Series Server.

    Note Dedicated mode is not applicable to the EHWIC E-Series NCE.

  - Shared-Lom-GE2—Attach an Ethernet cable to the E-Series Server or the NCE's external GE2 interface.
  - Shared-Lom-Console—Use the Cisco IOS CLI to configure the E-Series Server or the NCE's internal Console interface.
- To view the serial output, start the Hyper Terminal or Minicom as appropriate. Do one of the following:
  - Microsoft Windows—Start Hyper Terminal.
  - Linux—Start Minicom.
- Make sure that the communications settings are configured as: 9600 baud, 8 bits, No parity, and 1 stop bit.

Procedure

	Command or Action	Purpose
Step 1	Router# **hw-module sm** *slot* **oir-stop**	Shuts down the power to the specified E-Series Server. **Note** The Cisco 2900 series ISR G2 does not support OIR of the E-Series Servers. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the E-Series Server from the Cisco 2900 ISR G2. **Note** The ISR G2 does not support OIR of the EHWIC E-Series NCE. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the EHWIC E-Series NCE from the router.
Step 2	Remove the faulty SD card and insert a new one.	Replaces the faulty SD card.
Step 3	Router# **hw-module sm** *slot* **oir-start**	Restarts the specified E-Series Server. **Note** The Cisco 2900 series ISR G2 does not support OIR of the E-Series Servers. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the E-Series Server from the Cisco 2900 ISR G2. **Note** The ISR G2 does not support OIR of the EHWIC E-Series NCE. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the EHWIC E-Series NCE from the router.
Step 4	***	From the Hyper Terminal or Minicom, enter the ******* command to enter the bootloader prompt.
Step 5	ucse-cimc > **boot current recovery**	Boots the E-Series Server or NCE from the current image.
Step 6	Recovery-shell # **interface [dedicated | shared-lom-console | shared-lom-ge1 | shared-lom-ge2 | shared-lom-ge3]** *interface-ip-address netmask gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway ip address of the specified interface. **Note** Dedicated mode is not applicable to the EHWIC E-Series NCE. GE3 is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.
Step 7	Recovery-shell # **ping** *tftp-ip-address*	Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.

	Command or Action	Purpose
Step 8	Recovery-shell # **update** *tftp-ip-address image-filename*	Installs the CIMC firmware image, which is located on a remote tftp server.
Step 9	Recovery-shell # **reboot**	Reboots CIMC.

Example

This example recovers the CIMC firmware from the current image in an E-Series Server:

```
Router# hw-module subslot 2/0 stop
Router# hw-module subslot 2/0 start

***

ucse-cimc > boot current recovery
recovery-shell# interface shared-lom-ge2 192.168.0.138 255.255.255.0 192.168.0.1
Network configuration:
        IP config: addr: 192.168.0.138 Mask: 255.255.255.0
        Gateway: 192.168.0.1
recovery-shell# ping 10.20.34.56
PING 10.20.34.56 (10.20.34.56): 56 data bytes
64 bytes from 10.20.34.56: seq=0 ttl=60 time=10.000 ms
64 bytes from 10.20.34.56: seq=1 ttl=60 time=0.000 ms
--- 10.20.34.56 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.000/1.000/10.000 ms
recovery-shell# update 10.20.34.56 update_pkg-cimc.combined.bin
downloading firmware image "update_pkg-cimc.combined.bin" from " 10.20.34.56 "
download firmware image done, size in bytes: 22384144
installing firmware image, please wait ...
activating installed image
done
Stage: NONE
Status: SUCCESS
Error: Success
recovery-shell# reboot
```

This example recovers the CIMC firmware from the current image in an EHWIC E-Series NCE:

```
***

ucse-cimc > boot current recovery
recovery-shell# interface shared-lom-ge2 192.168.0.138 255.255.255.0 192.168.0.1
Network configuration:
        IP config: addr: 192.168.0.138 Mask: 255.255.255.0
        Gateway: 192.168.0.1
recovery-shell# ping 10.20.34.56
PING 10.20.34.56 (10.20.34.56): 56 data bytes
64 bytes from 10.20.34.56: seq=0 ttl=60 time=10.000 ms
64 bytes from 10.20.34.56: seq=1 ttl=60 time=0.000 ms
--- 10.20.34.56 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.000/1.000/10.000 ms
recovery-shell# update 10.20.34.56 update_pkg-cimc.combined.bin
downloading firmware image "update_pkg-cimc.combined.bin" from " 10.20.34.56 "
download firmware image done, size in bytes: 22384144
installing firmware image, please wait ...
```

```
activating installed image
done
Stage: NONE
Status: SUCCESS
Error: Success
recovery-shell# reboot
```

Recovering from a Corrupted File System

Use this procedure if you see the following error message in the CIMC boot log files.

```
UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY
```

Before you begin

- Connect the server to your PC. Depending on the type of server, do one of the following as appropriate:
    - Double-wide E-Series Server—Connect one end of the serial cable to the E-Series Server serial port and the other end to your PC.
    - Single-wide E-Series Server and SM E-Series NCE—First, connect a KVM connector to the E-Series Server or SM E-Series NCE's KVM port; and then connect one end of a serial cable to the DB9 port of the KVM connector and the other end to your PC.
    - EHWIC E-Series NCE— Connect the mini-USB end of the cable to the EHWIC E-Series NCE's mini-USB port; and then connect the other end of the USB cable to the USB port on your PC.

      Note The mini-USB cable is not provided with the EHWIC E-Series NCE. You must purchase your own mini-USB cable.

- Depending on the interface option that you specify, do one of the following:
    - Dedicated—Attach an Ethernet cable to the Management (dedicated) port of the E-Series Server.

      Note Dedicated mode is not applicable to the EHWIC E-Series NCE.

    - Shared-Lom-GE2—Attach an Ethernet cable to the E-Series Server or the NCE's external GE2 interface.
    - Shared-Lom-Console—Use the Cisco IOS CLI to configure the E-Series Server or the NCE's internal Console interface.
- To view the serial output, start the Hyper Terminal or Minicom as appropriate. Do one of the following:
    - Microsoft Windows—Start Hyper Terminal.
    - Linux—Start Minicom.
- Make sure that the communications settings are configured as: 9600 baud, 8 bits, No parity, and 1 stop bit.

Procedure

	Command or Action	Purpose
Step 1	Router# **hw-module sm** *slot* **oir-stop**	Shuts down the power to the specified E-Series Server. **Note** The Cisco 2900 series ISR G2 does not support OIR of the E-Series Servers. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the E-Series Server from the Cisco 2900 ISR G2. **Note** The ISR G2 does not support OIR of the EHWIC E-Series NCE. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the EHWIC E-Series NCE from the router.
Step 2	Router# **hw-module sm** *slot* **oir-start**	Restarts the specified E-Series Server. **Note** The Cisco 2900 series ISR G2 does not support OIR of the E-Series Servers. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the E-Series Server from the Cisco 2900 ISR G2. **Note** The ISR G2 does not support OIR of the EHWIC E-Series NCE. To avoid damaging the router, turn off the electrical power on the router and disconnect network cables before inserting or removing the EHWIC E-Series NCE from the router.
Step 3	***	From the Hyper Terminal or Minicom, enter the ******* command to enter the bootloader prompt.
Step 4	ucse-cimc > **boot current recovery**	Boots the E-Series Server or NCE from the current image.
Step 5	To check the file system of the specified partition and recover the corrupted file system, enter these commands.	**a.** Recovery-shell # **fs-check [p3 | p4]** **Note** You can only use p3 and p4 partitions with this command. Use this command on the partition that is corrupted. The corrupted partition is the one that displays the **run fsk** error message during CIMC bootup. **b.** Do the following: • If the command output displays **clean**, it indicates that the corrupted files are recovered. Enter the **reboot** command to reboot CIMC.

	Command or Action	Purpose
		Note Skip the steps that follow. • If the command output does not display **clean**, proceed to Step 6.
Step 6	(Optional) If the **fs-check [p3 | p4]** command does not recover the corrupted file system, and the output does not display **clean**, enter these commands to format the partitions.	**a.** Recovery-shell # **sd-card format [p3 | p4]** Formats the specified corrupted partition on the SD card. **Note** The corrupted partition is the one that displays the **run fsk** error message during CIMC bootup. **b.** Recovery-shell # **reboot** Reboots CIMC. **Note** Skip the steps that follow. **Note** When the p3 partition is formatted, the CIMC configuration is lost.
Step 7	(Optional) If the **sd-card format [p3 | p4]** command does not recover the corrupted file system, enter these commands to partition and format the SD card.	**a.** Recovery-shell # **sd-card partition** Creates partitions on the SD card. **b.** Recovery-shell # **sd-card format p3** Formats the p3 partition on the SD card. **c.** Recovery-shell # **sd-card format p4** Formats the p4 partition on the SD card. **d.** Recovery-shell # **reboot** Reboots CIMC. **e.** (Optional) Recovery-shell # **sd-partition show** Displays the current partition on the SD card. **Note** When you partition SD card or emmc, the contents of the SD card or emmc, such as, bmc configuration, ISO file and password are either lost or cleared.
Step 8	Recovery-shell # **interface [dedicated | shared-lom-console | shared-lom-ge1 | shared-lom-ge2 | shared-lom-ge3]** *interfa ce-ip-address netmask gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway ip address of the specified interface.

	Command or Action	Purpose
		Note Dedicated mode is not applicable to the EHWIC E-Series NCE. GE3 is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.
Step 9	Recovery-shell # **ping** *tftp-ip-address*	Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.
Step 10	Recovery-shell # **update** *tftp-ip-address image-filename*	Installs the CIMC firmware image, which is located on a remote tftp server.
Step 11	Recovery-shell # **reboot**	Reboots CIMC.

Example

Note SD card is used for UCSE M2, EMMC is used for UCSE M3 and ENCS.

This example recovers the CIMC firmware from the current image using the **fs-check p3** command in an E-Series Server:

```
Router# hw-module sm 2 oir-stop
Router# hw-module sm 2 oir-start

***

ucse-cimc > boot current recovery
recovery-shell# fs-check p3
e2fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p3: recovering journal
/dev/mmcblk0p3: clean, 429/7840 files, 3331/31296 blocks
recovery-shell# fs-check p4
e2fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p4: clean, 51/506912 files, 1880262/2025296 blocks
recovery-shell# reboot
```

This example recovers the CIMC firmware from the current image using the **fs-check p3** command in an EHWIC E-Series NCE:

```


***

ucse-cimc > boot current recovery
recovery-shell# fs-check p3
e2fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p3: recovering journal
/dev/mmcblk0p3: clean, 429/7840 files, 3331/31296 blocks
recovery-shell# fs-check p4
e2fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p4: clean, 51/506912 files, 1880262/2025296 blocks
recovery-shell# reboot
```

Recovery Shell Commands

Recovery Shell Commands	Description
Recovery-shell # **dedicated-interface** *interface-ip-address netmask gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway ip address of the dedicated interface.
Recovery-shell # **dedicated-interface (DEPRECATED)**	Shows the current configuration of the dedicated port.
Recovery-shell # **interface [dedicated | shared-lom-console | shared-lom-ge1 | shared-lom-ge2 | shared-lom-ge3]** *interface-ip-address netmask gateway-ip-address*	Specifies the IP address, subnet mask, and the gateway ip address of the specified interface.
Recovery-shell # **interface**	Shows the configuration on the interface.
Recovery-shell # **sd-card format [p3 | p4]**	Formats the specified corrupted partition on the SD card.
Recovery-shell # **sd-card partition**	Creates partitions on the SD card.
Recovery-shell # **sd-partition show**	Displays the current partition on the SD card.
Recovery-shell # **ping** *tftp-ip-address*	Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.
Recovery-shell # **update** *tftp-ip-address image-filename*	Installs the CIMC firmware image, which is located on a remote tftp server.
Recovery-shell # **fs-check [p3 | p4]**	Checks the file system of the specified partition and recover the corrupted file system.
Recovery-shell # **active image**	Shows the current active image that CIMC is running, which can be image 1 or image 2.
Recovery-shell # **active image [1 | 2]**	Changes the active image to 1 or 2. If the specified image is already active, a message is displayed. Otherwise, the specified image is made active. After you use the active image command, use the **reboot** command for the newly configured image to take effect.
Recovery-shell # **reboot**	Reboots the CIMC firmware.

Recovering Password

Before you begin

- Connect the server to your PC. Depending on the type of server, do one of the following as appropriate:

- Double-wide E-Series Server—Connect one end of the serial cable to the E-Series Server serial port and the other end to your PC.
- Single-wide E-Series Server and SM E-Series NCE—First, connect a KVM connector to the E-Series Server or SM E-Series NCE's KVM port; and then connect one end of a serial cable to the DB9 port of the KVM connector and the other end to your PC.
- EHWIC E-Series NCE— Connect the mini-USB end of the cable to the EHWIC E-Series NCE's mini-USB port; and then connect the other end of the USB cable to the USB port on your PC.

Note The mini-USB cable is not provided with the EHWIC E-Series NCE. You must purchase your own mini-USB cable.

- Depending on the interface option that you specify, do one of the following:
    - Dedicated—Attach an Ethernet cable to the Management (dedicated) port of the E-Series Server.

Note Dedicated mode is not applicable to the EHWIC E-Series NCE.

    - Shared-Lom-GE2—Attach an Ethernet cable to the E-Series Server or the NCE's external GE2 interface.
    - Shared-Lom-Console—Use the Cisco IOS CLI to configure the E-Series Server or the NCE's internal Console interface.
- To view the serial output, start the Hyper Terminal or Minicom as appropriate. Do one of the following:
    - Microsoft Windows—Start Hyper Terminal.
    - Linux—Start Minicom.
- Make sure that the communications settings are configured as: 9600 baud, 8 bits, No parity, and 1 stop bit.

Step 1 Router# **hw-module sm** *slot* **oir-stop**

Shuts down the power to the specified E-Series Server.

Step 2 Router# **hw-module sm** *slot* **oir-start**

Restarts the specified E-Series Server.

Step 3 ***

Type ******* when the CIMC boots.

Step 4 ucse-cimc > **boot current recovery**

Type **`boot current recovery`** to boot up into recovery mode.

Step 5 Recovery-shell#

By default, you can login as an admin or use the password.

a. Recovery-shell# **admin**

Recovery-shell# **password**

```
Password:
login[1021]: root login on 'ttyS0'
```

Recovery-shell#

Displays the current partitions on the EMMC card.

b. Recovery-shell # **emmc format p3**

Formats the p3 partition on the EMMC card that will clear the configuration including the password.

Note When you partition EMMC, the contents of the EMMC card, such as, bmc configuration, ISO file and password are either lost or cleared.

Example

This example recovers the password if you do not remember the CMIC password:

Router# hw-module sm 2 oir-stop

Router# hw-module sm 2 oir-start

***

type *** when the CIMC boots

ucse-cimc > boot current recovery

type 'boot current recovery' to boot up into recovery mode

CISCO-IMC login: admin

Password:

login[1021]: root login on 'ttyS0'

recovery-shell#

rrecovery-shell# emmc show

recovery-shell# emmc format p3

CHAPTER 14

Viewing Faults and Logs

This chapter includes the following sections:

Faults

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.

Example

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 #
```

System Event Log

Viewing the System Event Log

SUMMARY STEPS

1. Server# **scope sel**
2. Server /sel # **show entries** [**detail**]

DETAILED STEPS

	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.

Example

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

SUMMARY STEPS

1. Server# **scope sel**
2. Server /sel # **clear**

DETAILED STEPS

	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.

Example

This example clears the system event log:

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

Cisco IMC Log

Viewing the CIMC Log

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope log**
3. Server /cimc/log # **show** **entries** [**detail**]

DETAILED STEPS

	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.

Example

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

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope log**
3. Server /cimc/log # **clear**

DETAILED STEPS

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

Example

This example clears the log of CIMC events:

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

Configuring the CIMC Log Threshold

You can specify the lowest level of messages that will be included in the CIMC log.

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope log**
3. Server /cimc/log # **set local-syslog-severity** *level*
4. Server /cimc/log # **commit**
5. (Optional) Server /cimc/log # **show local-syslog-severity**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope log**	Enters CIMC log command mode.
Step 3	Server /cimc/log # **set local-syslog-severity** *level*	The severity *level* can be one of the following, in decreasing order of severity: • emergency • alert • critical • error • warning • notice

	Command or Action	Purpose
		• informational • debug **Note** The CIMC does not log any messages with a severity below the selected severity. For example, if you select **error**, then the CIMC log will contain all messages with the severity Emergency, Alert, Critical, or Error. It will not show Warning, Notice, Informational, or Debug messages.
Step 4	Server /cimc/log # **commit**	Commits the transaction to the system configuration.
Step 5	(Optional) Server /cimc/log # **show local-syslog-severity**	Displays the configured severity level.

Example

This example shows how to configure the logging of messages with a minimum severity of Warning:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # set local-syslog-severity warning
Server /cimc/log *# commit
Server /cimc/log # show local-syslog-severity
    Local Syslog Severity: warning

Server /cimc/log #
```

Sending the CIMC Log to a Remote Server

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

Procedure

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

Example

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 #
```

CHAPTER 15

Server Utilities

This chapter includes the following sections:

Exporting Technical Support Data to a Remote Server

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.

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **scope tech-support**
3. Server /cimc/tech-support # **set remote-ip** *ip-address*
4. Server /cimc/tech-support # **set remote-path** *path/filename*
5. Server /cimc/tech-support # **set remote-protocol** *protocol-type*
6. Server /cimc/tech-support # **set remote-username** *username*
7. Server /cimc/tech-support # **set remote-password** *password*
8. Server /cimc/tech-support # **commit**
9. Server /cimc/tech-support # **start**
10. Server /cimc/tech-support # **show detail**
11. Server /cimc/tech-support # **cancel**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope tech-support**	Enters tech-support command mode.

	Command or Action	Purpose
Step 3	Server /cimc/tech-support # **set remote-ip** *ip-address*	Specifies the IP address of the remote server on which the support data file should be stored.
Step 4	Server /cimc/tech-support # **set remote-path** *path/filename*	Specifies the filename for the support data to be stored on the server. When you enter this name, include the relative path for the file from the top of the server tree to the desired location.
Step 5	Server /cimc/tech-support # **set remote-protocol** *protocol-type*	Specifies the remote server protocol. The remote server protocol can be one of the following: • **tftp** • **ftp** • **sftp** • **scp** • **http**
Step 6	Server /cimc/tech-support # **set remote-username** *username*	(Optional) The username that the system should use to log in to the remote server. **Note** The username is not applicable if the remote server is TFTP or HTTP.
Step 7	Server /cimc/tech-support # **set remote-password** *password*	(Optional) The password for the remote username. **Note** The password is not applicable if the remote server is TFTP or HTTP.
Step 8	Server /cimc/tech-support # **commit**	Commits the transaction to the system configuration.
Step 9	Server /cimc/tech-support # **start**	Begins the transfer of the support data file to the remote server.
Step 10	Server /cimc/tech-support # **show detail**	Displays the status of the file upload.
Step 11	Server /cimc/tech-support # **cancel**	(Optional) Cancels the transfer of the support data file to the remote server.

Example

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 remote-ip 10.20.30.41
Server /cimc/tech-support *# set remote-path /user/user1/supportfile
Server /cimc/tech-support *# set remote-protocol tftp
Server /cimc/tech-support *# commit
Server /cimc/tech-support # start
```

```
 Tech Support upload started.
Server /cimc/tech-support # show detail
Tech Support:
    Server Address: 10.20.30.41
    Path: /user/user1/supportfile
    Protocol: tftp
    Username:
    Password: ******
    Progress(%): 0
    Status: COLLECTING
Server /cimc/tech-support # show detail
Tech Support:
    Server Address: 10.20.30.41
    Path: /user/user1/supportfile
    Protocol: tftp
    Username:
    Password: ******
    Progress(%): 85
    Status: COLLECTING
Server /cimc/tech-support # show detail
Tech Support:
    Server Address: 10.20.30.41
    Path: /user/user1/supportfile
    Protocol: tftp
    Username:
    Password: ******
    Progress(%): 100
    Status: COMPLETED
```

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.

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **reboot**

DETAILED STEPS

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

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

Example

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.

SUMMARY STEPS

1. Server# **scope cimc**
2. Server /cimc # **factory-default**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters 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.

Example

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, the CIMC will not apply the SNMP values when the file is imported.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope cimc**	Enters CIMC command mode.
Step 2	Server /cimc # **scope import-export**	Enters 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.

Example

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, the 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 CIMC command mode.
Step 2	Server /cimc # **scope import-export**	Enters import-export command mode.

	Command or Action	Purpose
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.

Example

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 16

Diagnostic Tests

This chapter includes the following sections:

Diagnostic Tests Overview

Diagnostics is a standalone utility that runs on the E-Series Server or NCE independent of the operating system or applications running on the server. If you experience problems with the E-Series Server or NCE, 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 or NCE at the time of purchase. You can also choose to download the most current diagnostics image from a specified FTP or HTTP 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 the Internal EFI Shell as the first boot device.

5. Reboot the server.

Note

- For E-Series Servers and SM E-Series NCE—On server reboot, the EFI Shell displays.
- For EHWIC E-Series NCE and NIM E-Series NCE—On server reboot, the AMIDiag EFI Shell displays.

6. Run diagnostic tests from the EFI Shell or the AMIDiag EFI Shell as appropriate.
7. Reset the virtual media boot order to its original setting.

Mapping the Diagnostics Image to the Host

Before you begin

- Backup data.
- Log in to the 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.

Example

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—E-Series Servers and SM E-Series NCE

From the EFI shell, use the following procedure to run diagnostic tests on the E-Series Servers and the SM E-Series NCE.

Before you begin

- Back up 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 back up 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.
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

	Command or Action	Purpose
		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.

Example

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.

Running Diagnostic Tests—EHWIC E-Series NCE and NIM E-Series NCE

Diagnostic tests are run on the server CPU, memory, and block devices. Block devices include SSD drive and USB drive.

Before you begin

- Back up 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 back up data before executing these tests.
- Delete previous versions of AMIDIAG_OBD.log files if any.
- Use the CIMC CLI or the CIMC GUI to download and map the diagnostics image onto the HDD virtual drive of the USB controller.
- Launch the KVM console.
- Reboot the server. The AMIDiag EFI Shell displays in the KVM console:

```
Found AMI DIAG on fs0:
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

Enter 'q' to quit, any other key to continue:

fs0:\>
```

Procedure

	Command or Action	Purpose
Step 1	From the AMIDiag EFI Shell, press any key (except q) to run the diagnostic tests.	Executes all available diagnostic tests and displays the progress. After the tests are completed, the **Pass** or **Fail** test status displays. **Note** Diagnostic tests can run for approximately 10 minutes.
Step 2	(Optional) fs0:\> **type AMIDIAG_OBD.log**	Displays the Onboard Diag log files with details.
Step 3	Server: fs0:\> **exit**	Exits from AMIDiag EFI Shell.
Step 4	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

	Command or Action	Purpose
		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.

What to do next

Reset the virtual media boot order to its original setting.