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.

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: http://www.cisco.com/go/trademarks. 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. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface xi
   New and Changed Information xi
   Audience xii
   Organization xii
   Conventions xiii
   Related Documentation xv
   Obtaining Documentation and Submitting a Service Request xv

CHAPTER 1 Overview 1
   Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine
      Overview 1
   Server Software 2
   CIMC Overview 3
   CIMC CLI 4
      Command Modes 4
         Command Mode Table 5
      Completing or Exiting a Command 7
      Command History 7
      Committing, Discarding, and Viewing Pending Commands 8
      Command Output Formats 8
   Online Help for the CLI 9

CHAPTER 2 Installing the Server Operating System or Hypervisor 11
   Operating System or Hypervisor Installation Methods 11
   KVM Console 11
      Installing an Operating System or Hypervisor Using the KVM Console 12
   PXE Installation Servers 13

CLI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine
Integrated Management Controller, Release 3.1.1
Installing an Operating System or Hypervisor Using a PXE Installation Server 13

Host Image Mapping 14

Mapping the Host Image 14

Installing Drivers for the Microsoft Windows Server 16

Unmapping the Host Image 17

Deleting the Host Image 17

Downloading the Customized VMware vSphere Hypervisor Image 18

Configuring ESX Network Connectivity through MGF (GE1) Interface 18

C H A P T E R  3

Managing the Server 23

Configuring the Server Boot Order 23

Resetting the Server 25

Shutting Down the Server 25

Locking Cisco IOS CLI Configuration Changes 26

Unlocking Cisco IOS CLI Configuration Changes 27

Managing Server Power 28

Powering On the Server 28

Powering Off the Server 28

Power Cycling the Server 29

Configuring the Power Restore Policy 30

Locking the Server's Front Panel Power Button 31

Unlocking the Server's Front Panel Power Button 32

Configuring BIOS Settings 33

Viewing BIOS Status 33

Configuring Advanced BIOS Settings 34

Configuring Server Management BIOS Settings 35

Clearing the BIOS CMOS 36

Clearing the BIOS Password 36

Restoring BIOS Defaults 37

Server BIOS Settings 37

C H A P T E R  4

Managing Storage Using RAID 47

RAID Options 47

Configuring RAID 51

Deleting the RAID Configuration 53
Changing the Physical Drive State 54
Rebuilding the Physical Drive 55
Erasing the Contents of a Physical Drive 56
Enabling Auto Rebuild on the Storage Controller 58
Deleting a Virtual Drive 58
Performing a Consistency Check on a Virtual Drive 59
Reconstructing the Virtual Drive Options 61
Reconstructing a Virtual Drive 63
Making the Disk Drive Bootable 64

CHAPTER 5

Viewing Server Properties 67

Viewing Server Properties 67
Viewing the Actual Boot Order 68
Viewing CIMC Information 68
Viewing SD Card Information 69
Viewing CPU Properties 70
Viewing Memory Properties 70
Viewing Power Supply Properties 71
Viewing Storage Properties 72
Viewing Storage Adapter Properties 72
Viewing Physical Drive Properties 73
Viewing Virtual Drive Properties 74
Viewing PCI Adapter Properties 75
Viewing Power Policy Statistics 76
Viewing Hard Drive Presence 77
Viewing the MAC Address of an Interface 77
Viewing the Status of CIMC Network Connections 78

CHAPTER 6

Viewing Server Sensors 81

Viewing Temperature Sensors 81
Viewing Voltage Sensors 82
Viewing LED Sensors 82
Viewing Storage Sensors 83

CHAPTER 7

Managing Remote Presence 85
Managing the Virtual KVM 85
  KVM Console 85
  Configuring the Virtual KVM 86
  Enabling the Virtual KVM 87
  Disabling the Virtual KVM 88
Configuring Virtual Media 88
  Configuring a CIMC-Mapped vMedia Volume 89
  Viewing CIMC-Mapped vMedia Volume Properties 91
  Removing a CIMC-Mapped Mounted vMedia Volume 91
Managing Serial over LAN 92
  Serial over LAN 92
    Guidelines and Restrictions for Serial over LAN 92
  Configuring Serial Over LAN 92
  Launching Serial over LAN 93

CHAPTER 8
Managing User Accounts 95
  Configuring Local Users 95
  LDAP Servers (Active Directory) 96
    Configuring the LDAP Server 96
    Configuring LDAP in CIMC 98
    Configuring LDAP Groups in CIMC 99
  Viewing User Sessions 101
  Terminating a User Session 101

CHAPTER 9
Configuring Network-Related Settings 103
  CIMC NIC Configuration 103
    CIMC NICs 103
    Configuring CIMC NICs 104
  Configuring Common Properties 105
  Configuring IPv4 106
  Configuring the Server VLAN 107
  Network Security Configuration 108
    Network Security 108
    Configuring Network Security 109
    Configuring Network Analysis Module Capability 110
NTP Settings Configuration 110
NTP Settings 110
Configuring NTP Settings 111

CHAPTER 10
Configuring Communication Services 113
Configuring HTTP 113
Configuring SSH 114
Configuring the XML API 115
XML API for the CIMC 115
Enabling the XML API 115
Configuring IPMI 116
IPMI over LAN 116
Configuring IPMI over LAN 116
Configuring SNMP 117
SNMP 117
Configuring SNMP Properties 117
Configuring SNMP Trap Settings 119
Sending a Test SNMP Trap Message 120
Configuring SNMPv3 Users 120

CHAPTER 11
Managing Certificates 123
Managing the Server Certificate 123
Generating a Certificate Signing Request 123
Creating a Self-Signed Certificate 125
Uploading a Server Certificate 127

CHAPTER 12
Configuring Platform Event Filters 129
Platform Event Filters 129
Enabling Platform Event Alerts 129
Disabling Platform Event Alerts 130
Configuring Platform Event Filters 130
Interpreting Platform Event Traps 132

CHAPTER 13
Firmware Management 135
Overview of Firmware 135
Options for Upgrading Firmware  136
Obtaining Software from Cisco Systems  136
Installing CIMC Firmware from a Remote Server  138
Activating Installed CIMC Firmware  139
Installing BIOS Firmware from the TFTP Server  140
Upgrading Programmable Logic Devices Firmware on the E-Series EHWIC NCE  141
Troubleshooting E-Series Server or NCE Access Issues  142
  Recovering from a Corrupted CIMC Firmware Image  142
  Recovering from a Faulty SD Card  145
  Recovering from a Corrupted File System  148
  Recovery Shell Commands  151

CHAPTER 14  
Viewing Faults and Logs  153
Faults  153
  Viewing the Fault Summary  153
System Event Log  154
  Viewing the System Event Log  154
  Clearing the System Event Log  155
Cisco IMC Log  155
  Viewing the CIMC Log  155
  Clearing the CIMC Log  156
  Configuring the CIMC Log Threshold  156
  Sending the CIMC Log to a Remote Server  157

CHAPTER 15  
Server Utilities  159
  Exporting Technical Support Data to a Remote Server  159
  Rebooting the CIMC  161
  Resetting the CIMC to Factory Defaults  161
  Exporting and Importing the CIMC Configuration  162
    Exporting and Importing the CIMC Configuration  162
    Exporting the CIMC Configuration  163
    Importing a CIMC Configuration  164

CHAPTER 16  
Diagnostic Tests  165
  Diagnostic Tests Overview  165
Contents

Mapping the Diagnostics Image to the Host 166
Running Diagnostic Tests—E-Series Servers and SM E-Series NCE 167
Running Diagnostic Tests—EHWIC E-Series NCE and NIM E-Series NCE 169
Preface

This preface includes the following sections:

• New and Changed Information, page xi
• Audience, page xii
• Organization, page xii
• Conventions, page xiii
• Related Documentation, page xv
• Obtaining Documentation and Submitting a Service Request, page xv

New and Changed Information

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

Table 1: New Features and Significant Behavioral Changes in Cisco Integrated Management Controller Software, Release 3.1.1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support UCS-E160S-M3/K9 servers</td>
<td>Support added to install the UCS-E160S-M3/K9 into the Cisco ISR 4000 series.</td>
<td>Overview, on page 1</td>
</tr>
</tbody>
</table>

Table 2: New Features and Significant Behavioral Changes in Cisco Integrated Management Controller Software, Release 3.0.1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIM E-Series Network Compute Engine</td>
<td>Support for the NIM E-Series Network Compute Engine (NIM E-Series NCE).</td>
<td>Overview, on page 1</td>
</tr>
<tr>
<td>Faults and Logs</td>
<td></td>
<td>Viewing Faults and Logs, on page 153</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>Overview</td>
<td>Provides an overview of the Cisco UCS E-Series Servers, the Cisco UCS E-Series Network Compute Engine, and the CIMC.</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>Installing the Server Operating System</td>
<td>Describes how to configure an operating system (OS) on the server.</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Managing the Server</td>
<td>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.</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Managing Storage Using RAID</td>
<td>Describes how to configure and manage RAID. <strong>Note</strong>: 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.</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>Viewing Server Properties</td>
<td>Describes how to view the CPU, memory, power supply, storage, PCI adapter, and LOM properties of the server.</td>
</tr>
<tr>
<td>Chapter 6</td>
<td>Viewing Server Sensors</td>
<td>Describes how to view the temperature, voltage, and storage sensors.</td>
</tr>
<tr>
<td>Chapter 7</td>
<td>Managing Remote Presence</td>
<td>Describes how to configure and manage the virtual KVM, virtual media, and the serial over LAN connection.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Analysis Module (NAM) and Network Time Protocol (NTP) Settings</td>
<td>Support added to enable the NAM capability and NTP service.</td>
<td>Configuring Network-Related Settings, on page 103</td>
</tr>
<tr>
<td>Chapter</td>
<td>Title</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Chapter 8</td>
<td>Managing User Accounts</td>
<td>Describes how to add or modify user accounts, how to configure Active Directory to authenticate users, and how to manage user sessions.</td>
</tr>
<tr>
<td>Chapter 9</td>
<td>Configuring Network-Related Settings</td>
<td>Describes how to configure network interfaces, network settings, network security, NAM, and NTP settings.</td>
</tr>
<tr>
<td>Chapter 10</td>
<td>Configuring Communication Services</td>
<td>Describes how to configure server management communication by HTTP, SSH, IPMI, and SNMP.</td>
</tr>
<tr>
<td>Chapter 11</td>
<td>Managing Certificates</td>
<td>Describes how to generate, upload, and manage server certificates.</td>
</tr>
<tr>
<td>Chapter 12</td>
<td>Configuring Platform Event Filters</td>
<td>Describes how to configure and manage platform event filters.</td>
</tr>
<tr>
<td>Chapter 13</td>
<td>Firmware Management</td>
<td>Describes how to obtain, install, and activate firmware images.</td>
</tr>
<tr>
<td>Chapter 14</td>
<td>Viewing Faults and Logs</td>
<td>Describes how to view fault information and how to view, export, and clear the CIMC log and system event log messages.</td>
</tr>
<tr>
<td>Chapter 15</td>
<td>Server Utilities</td>
<td>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.</td>
</tr>
<tr>
<td>Chapter 16</td>
<td>Diagnostic Tests</td>
<td>Describes how to run diagnostic tests.</td>
</tr>
</tbody>
</table>

**Conventions**

<table>
<thead>
<tr>
<th>Text Type</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI elements</td>
<td>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.</td>
</tr>
<tr>
<td>User input</td>
<td>Text the user should enter exactly as shown or keys that a user should press appear in this font.</td>
</tr>
<tr>
<td>System output</td>
<td>Terminal sessions and information that the system displays appear in this font.</td>
</tr>
<tr>
<td>Text Type</td>
<td>Indication</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
</tr>
<tr>
<td>CLI commands</td>
<td>CLI command keywords appear in <strong>this font</strong>. Arguments in a CLI command appear in <strong>this font</strong>.</td>
</tr>
<tr>
<td>[]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>

**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.
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.
Overview

This chapter includes the following sections:

- Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine Overview, page 1
- Server Software, page 2
- CIMC Overview, page 3
- CIMC CLI, page 4

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.
- Cisco UCS-E160S-M3/K9 servers are supported on the ISR 4000 series only.

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.

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

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 NIME-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, VLANs, and network security
- Configure communication services, including HTTP, SSH, IPMI over LAN, and SNMP
- Manage certificates
- Configure platform event filters
- Update CIMC firmware
- Update BIOS firmware
- Install the host image from an internal repository
- Monitor faults, alarms, and server status
- Collect technical support data in the event of server failure
Almost all tasks can be performed in either the GUI interface or CLI interface, and the results of tasks performed in one interface are displayed in another. However, you cannot:

- 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 NIME 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.

<table>
<thead>
<tr>
<th>Mode Name</th>
<th>Command to Access</th>
<th>Mode Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td>top command from any mode</td>
<td>#</td>
</tr>
<tr>
<td>bios</td>
<td>scope bios command from EXEC mode</td>
<td>/bios #</td>
</tr>
<tr>
<td>advanced</td>
<td>scope advanced command from bios mode</td>
<td>/bios/advanced #</td>
</tr>
<tr>
<td>main</td>
<td>scope main command from bios mode</td>
<td>/bios/main #</td>
</tr>
<tr>
<td>server-management</td>
<td>scope server-management command from bios mode</td>
<td>/bios/server-management #</td>
</tr>
<tr>
<td>certificate</td>
<td>scope certificate command from EXEC mode</td>
<td>/certificate #</td>
</tr>
<tr>
<td>chassis</td>
<td>scope chassis command from EXEC mode</td>
<td>/chassis #</td>
</tr>
<tr>
<td>dimm-summary</td>
<td>scope dimm-summary index command from chassis mode</td>
<td>/chassis/dimm-summary #</td>
</tr>
<tr>
<td>storageadapter</td>
<td>scope storageadapter slot command from chassis mode</td>
<td>/chassis/storageadapter #</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This command mode is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.</td>
<td></td>
</tr>
<tr>
<td>physical-drive</td>
<td>scope physical-drive drive-number command from storageadapter mode</td>
<td>/chassis/storageadapter /physical-drive #</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This command mode is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.</td>
<td></td>
</tr>
<tr>
<td>virtual-drive</td>
<td>scope virtual-drive drive-number command from storageadapter mode</td>
<td>/chassis/storageadapter /virtual-drive #</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This command mode is not applicable to the EHWIC E-Series NCE and the NIM E-Series NCE.</td>
<td></td>
</tr>
<tr>
<td>cimc</td>
<td>scope cimc command from EXEC mode</td>
<td>/cimc #</td>
</tr>
<tr>
<td>import-export</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mode Name</td>
<td>Command to Access</td>
<td>Mode Prompt</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>log</td>
<td><code>scope log</code> command from cimc mode</td>
<td>/cimc/log #</td>
</tr>
<tr>
<td>server</td>
<td><code>scope server index</code> command from log mode</td>
<td>/cimc/log/server #</td>
</tr>
<tr>
<td>network</td>
<td><code>scope network</code> command from cimc mode</td>
<td>/cimc/network #</td>
</tr>
<tr>
<td>ipblocking</td>
<td><code>scope ipblocking</code> command from network mode</td>
<td>/cimc/network/ipblocking #</td>
</tr>
<tr>
<td>tech-support</td>
<td><code>scope tech-support</code> command from cimc mode</td>
<td>/cimc/tech-support #</td>
</tr>
<tr>
<td>fault</td>
<td><code>scope fault</code> command from EXEC mode</td>
<td>/fault #</td>
</tr>
<tr>
<td>pef</td>
<td><code>scope pef</code> command from fault mode</td>
<td>/fault/pef #</td>
</tr>
<tr>
<td>http</td>
<td><code>scope http</code> command from EXEC mode</td>
<td>/http #</td>
</tr>
<tr>
<td>ipmi</td>
<td><code>scope ipmi</code> command from EXEC mode</td>
<td>/ipmi #</td>
</tr>
<tr>
<td>kvm</td>
<td><code>scope kvm</code> command from EXEC mode</td>
<td>/kvm #</td>
</tr>
<tr>
<td>ldap</td>
<td><code>scope ldap</code> command from EXEC mode</td>
<td>/ldap #</td>
</tr>
<tr>
<td>power-cap</td>
<td><code>scope power-cap</code> command from EXEC mode</td>
<td>/power-cap #</td>
</tr>
<tr>
<td>remote-install</td>
<td><code>scope remote-install</code> command from EXEC mode</td>
<td>/remote-install #</td>
</tr>
<tr>
<td>sel</td>
<td><code>scope sel</code> command from EXEC mode</td>
<td>/sel #</td>
</tr>
<tr>
<td>sensor</td>
<td><code>scope sensor</code> command from EXEC mode</td>
<td>/sensor #</td>
</tr>
<tr>
<td>snmp</td>
<td></td>
<td>/snmp #</td>
</tr>
</tbody>
</table>
## 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.

<table>
<thead>
<tr>
<th>Mode Name</th>
<th>Command to Access</th>
<th>Mode Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>scope snmp</code> command from EXEC mode</td>
<td></td>
</tr>
<tr>
<td><code>trap-destination</code></td>
<td><code>scope trap-destination</code> command from snmp mode</td>
<td><code>/snmp/trap-destination #</code></td>
</tr>
<tr>
<td><code>sol</code></td>
<td><code>scope sol</code> command from EXEC mode</td>
<td><code>/sol #</code></td>
</tr>
<tr>
<td><code>ssh</code></td>
<td><code>scope ssh</code> command from EXEC mode</td>
<td><code>/ssh #</code></td>
</tr>
<tr>
<td><code>user</code></td>
<td><code>scope user user-number</code> command from EXEC mode</td>
<td><code>/user #</code></td>
</tr>
<tr>
<td><code>user-session</code></td>
<td><code>scope user-session session-number</code> command from EXEC mode</td>
<td><code>/user-session #</code></td>
</tr>
<tr>
<td><code>vmedia</code></td>
<td><code>scope vmedia</code> command from EXEC mode</td>
<td><code>/vmedia #</code></td>
</tr>
</tbody>
</table>
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.
Installing the Server Operating System or Hypervisor

This chapter includes the following sections:

- Operating System or Hypervisor Installation Methods, page 11
- KVM Console, page 11
- PXE Installation Servers, page 13
- Host Image Mapping, page 14
- Configuring ESX Network Connectivity through MGF (GE1) Interface, page 18

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 boot up.
- Access the CIMC Configuration Utility by pressing **F8** during boot up.

**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 boot up.

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

**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

### 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.

---

**Note**

The VMware vSphere Hypervisor requires a customized image. To download the customized image, see *Downloading the Customized VMware vSphere Hypervisor Image*, on page 18.

---

**Procedure**

**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

The VMware vSphere Hypervisor requires a customized image. To download the customized image, see Downloading the Customized VMware vSphere Hypervisor Image, on page 18.

Note

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope host-image-mapping</td>
<td>Enters the remote install command mode.</td>
</tr>
</tbody>
</table>
| Step 2 | Server /remote-install # download-image {ftp | ftps | http | https} server-ip-address path /filename [username username password password] | Downloads the image from the specified remote server onto the CIMC internal repository. The host image must have .iso as the file extension. The remote server can be a FTP, FTPS, HTTP, or HTTPS server. If the remote server requires user authentication, you must add the username and password of the remote server.

Note

If the image file exceeds the size limit, an error message is displayed.

Note

The HTTP server does not support user authentication; only FTP supports user authentication. |
| Step 3 | (Optional) Server /remote-install # show detail | Displays the status of the image download. |
Purpose

Command or Action | Purpose
--- | ---
**Step 4** | Server /remote-install # map-image

Mounts the image on a virtual drive of the USB controller. The virtual drive can be one of the following:

- HDD—Hard disk drive
- FDD—Floppy disk drive
- CDROM—Bootable CD-ROM

**Step 5** | (Optional) Server /remote-install # show detail

Displays the status of the host image mapping.

This example maps the host image:

```plaintext
Server# scope host-image-mapping
Server /remote-install # download-image ftp 10.20.34.56 pub/hostimage.iso
---
Server /remote-install # show detail
Host Image Info:
Name: HostImage.iso
Size: 6626848
Host Image Status: Download Successful!!
Server /remote-install # map-image
---
status: ok
---
Server /remote-install # show detail
Host Image Info:
Name: HostImage.iso
Size: 6626848
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 23.
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 16.
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

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.

Procedure

Step 1 Download the drivers from Cisco.com. See Obtaining Software from Cisco Systems, on page 136.

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 NIME-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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope host-image-mapping</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /remote-install # unmap-image</td>
</tr>
<tr>
<td>Step 3</td>
<td>Server /remote-install # show detail</td>
</tr>
</tbody>
</table>

This example unmaps the host image:

Server# scope host-image-mapping
Server /remote-install # unmap-image
Server /remote-install # show detail
Host Image Info:
Name: HostImage.iso
Size: 6626848
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope host-image-mapping</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /remote-install # delete-image</td>
</tr>
</tbody>
</table>

This example deletes the host image:

Server# scope host-image-mapping
Server /remote-install # delete-image
Downloading the Customized VMware vSphere Hypervisor Image

Procedure

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

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

Step 3 Click Downloads, and then select All Products from the drop-down list.

Step 4 Do one of the following as appropriate:

• To download the VMware vSphere Hypervisor 5.1 image, enter ESXi-5.1.0-799733-custom-Cisco-2.1.0.3.iso in the Search field, and then click the Search icon. From the Search Results, click VMware vSphere > Drivers & Tools > Cisco Custom Image for ESXi 5.1.0 GA Install CD, and then click Download.

• To download the VMware vSphere Hypervisor 5.5 image, enter ESXi-5.5.0-1331820-custom-Cisco-5.5.0.1.iso, in the Search field, and then click the Search icon. From the Search Results, click VMware vSphere > Drivers & Tools > CISCO Custom Image for ESXi 5.5.0 GA Install CD, and then click Download.

What to Do Next
Install the VMware vSphere Hypervisor 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 1,100,200,1061-1095

interface vlan 1
ip address 1.1.1.2 255.255.255.0

interface vlan 100
ip address 100.1.1.1 255.255.255.0

interface vlan 200
ip address 200.1.1.1 255.255.255.0

ESX Network - vmkernel0
In Address: 1.1.1.3 (vlan 1)
Subnet Mask: 255.255.255.0
Default Gateway: 1.1.1.2

VM Network 1
RHEL virtual machines - VLAN 100
In Address: 100.1.1.1 (vlan 100)
Subnet Mask: 255.255.255.0
Default Gateway: 100.0.0.1

VM Network 2
Windows virtual machines - VLAN 200
In Address: 200.1.1.1 (vlan 200)
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.
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.
Installing the Server Operating System or Hypervisor

Configuring ESX Network Connectivity through MGF (GE1) Interface

CLI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine
Integrated Management Controller, Release 3.1.1
Installing the Server Operating System or Hypervisor

Configuring ESX Network Connectivity through MGF (GE1) Interface
CHAPTER 3

Managing the Server

This chapter includes the following sections:

- Configuring the Server Boot Order, page 23
- Resetting the Server, page 25
- Shutting Down the Server, page 25
- Locking Cisco IOS CLI Configuration Changes, page 26
- Unlocking Cisco IOS CLI Configuration Changes, page 27
- Managing Server Power, page 28
- Configuring BIOS Settings, page 33

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope bios</td>
<td>Enters bios command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /bios # set boot-order category:device1[,...]</td>
<td>Specifies the boot device options and order.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: The options are not case sensitive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>You can select one or more of the following:</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>- cdrom—Bootable CD-ROM</td>
</tr>
<tr>
<td>- Virtual-CD</td>
</tr>
<tr>
<td>- fdd—Floppy disk drive</td>
</tr>
<tr>
<td>- Virtual-Floppy</td>
</tr>
<tr>
<td>- hdd—Hard disk drive</td>
</tr>
<tr>
<td>- RAID</td>
</tr>
<tr>
<td>- Cypress</td>
</tr>
<tr>
<td>- Virtual-HiFd</td>
</tr>
<tr>
<td>- pxe—PXE boot</td>
</tr>
<tr>
<td>- GigEth0</td>
</tr>
<tr>
<td>- GigEth1</td>
</tr>
<tr>
<td>- GigEth2</td>
</tr>
<tr>
<td>- GigEth3</td>
</tr>
<tr>
<td>- efi—Extensible Firmware Interface</td>
</tr>
</tbody>
</table>

### 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.

This example sets the boot order and commits the transaction:

```text
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 # 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
```
Reseting the Server

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Server# scope chassis</td>
<td>Enters chassis command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 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. |

This example resets the server:

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

Shutting Down the Server

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Server# scope chassis</td>
<td>Enters chassis mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 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:  
  1  Router # hw-module subslot 0/NIM-slot-number stop  
  2  Router # hw-module subslot 0/NIM-slot-number start |
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.

**Procedure**

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

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
```
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.

Procedure

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

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

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

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# scope chassis</td>
<td>Enters chassis command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Server/chassis # power on</td>
<td>After the prompt to confirm, turns on the server power.</td>
</tr>
</tbody>
</table>

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-E312-94B7499909E7
```

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.
**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope chassis</td>
</tr>
<tr>
<td></td>
<td>Enters chassis command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /chassis # power off</td>
</tr>
<tr>
<td></td>
<td>Turns off the server.</td>
</tr>
<tr>
<td></td>
<td>For the NIME-Series NCE, we recommend that you use the power shutdown command. If a power off is necessary, use the following commands from the router:</td>
</tr>
<tr>
<td></td>
<td>1. Router # hw-module subslot 0/NIM-slot-number stop</td>
</tr>
<tr>
<td></td>
<td>2. Router # hw-module subslot 0/NIM-slot-number start</td>
</tr>
</tbody>
</table>

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 NIME E-Series NCE.

---

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope chassis</td>
</tr>
<tr>
<td></td>
<td>Enters chassis command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /chassis # power cycle</td>
</tr>
<tr>
<td></td>
<td>After the prompt to confirm, power cycles the server.</td>
</tr>
<tr>
<td></td>
<td>• Power cycling the server is the same as pressing the physical power button to power off and then powering on the server.</td>
</tr>
<tr>
<td></td>
<td>• Power hard-reset is the same as pressing the physical reset button on the server.</td>
</tr>
</tbody>
</table>
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:

1. `Router # hw-module subslot 0/NIM-slot-number stop`
2. `Router # hw-module subslot 0/NIM-slot-number start`

- `Router # hw-module subslot 0/NIM-slot-number reload`  
  This command powers-cycle the module. The CIMC and server reboot.

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.

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# scope cimc</td>
<td>Enters the cimc command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Server /cimc #scope power-restore-policy</td>
<td>Enters the power restore policy command mode.</td>
</tr>
</tbody>
</table>
| **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. |
Purpose

- **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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Server /cimc/power-restore-policy# commit</code></td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

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

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

### Locking the Server's Front Panel Power Button

**Note**

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

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.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# scope chassis</td>
<td>Enters chassis command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Server /chassis # show detail</td>
<td>(Optional) Displays server properties, which allows you to determine the current status of the power button (whether it is locked or unlocked).</td>
</tr>
<tr>
<td><strong>Step 3</strong> Server /chassis # set power-button locked</td>
<td>Disables the power button. You cannot use the front panel power button to turn the server power on or off.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Server /chassis* # commit</td>
<td>Commits the changes.</td>
</tr>
</tbody>
</table>
### Unlocking the Server's Front Panel Power Button

#### Purpose
(Optional) Displays server properties, which allows you to determine the current status of the power button (whether it is locked or unlocked).

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action: <code>Server/chassis # show detail</code></th>
<th>Purpose</th>
</tr>
</thead>
</table>

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

```plaintext
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

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

- **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.

- **Procedure**

<table>
<thead>
<tr>
<th>Command or Action: <code>Server# scope chassis</code></th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enters chassis command mode.</td>
</tr>
</tbody>
</table>
### Purpose

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).

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

---

### Configuring BIOS Settings

#### Viewing BIOS Status

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope bios</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /bios # show detail</td>
</tr>
</tbody>
</table>
The BIOS status information contains the following fields:

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

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
```

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope bios</td>
</tr>
<tr>
<td></td>
<td>Enters the BIOS command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /bios # scope advanced</td>
</tr>
<tr>
<td></td>
<td>Enters the advanced BIOS settings command mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure the BIOS settings.</td>
</tr>
<tr>
<td></td>
<td>For the CLI commands, descriptions and information about the options for each BIOS setting, see the following topics:</td>
</tr>
<tr>
<td></td>
<td>• Advanced: Processor BIOS Settings, on page 37</td>
</tr>
<tr>
<td></td>
<td>• Advanced: Memory BIOS Settings, on page 43</td>
</tr>
<tr>
<td></td>
<td>• Advanced: Serial Port BIOS Settings, on page 43</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 4</strong> Server /bios/advanced # commit</td>
<td>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.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# <code>scope bios</code></td>
<td>Enters the BIOS command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Server /bios # <code>scope server-management</code></td>
<td>Enters the server management BIOS settings command mode.</td>
</tr>
</tbody>
</table>
| **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 44 |
| **Step 4** Server /bios/server-management # `commit` | Commits the transaction to the system configuration. Changes are applied on the next server reboot. If server power is on, you are prompted to choose whether to reboot now. |

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

Server# `scope bios`  
Server /bios # `scope server-management`  
Server /bios/server-management # `set BaudRate 9.6k`  
Server /bios/server-management *# `commit`
Clearing the BIOS CMOS

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Server# scope bios</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Server /bios # clear-cmos</strong></td>
</tr>
</tbody>
</table>

**Note**
If you run the `clear-cmos` command on Cisco UCS-E160S-M3/K9 servers (UCS-E M3 servers), the CPU goes into a temporary default state, and that causes the boot time to be exceedingly long (35-40 minutes) the next time you power on the server. To work around this issue, during the long boot, wait for one or two minutes and then power-cycle the server again. The boot time will be normal again.

This example clears the BIOS CMOS memory:

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

Clearing the BIOS Password

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Server# scope bios</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Server /bios # clear-bios-password</strong></td>
</tr>
</tbody>
</table>

This example clears the BIOS password:

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

Restoring BIOS Defaults

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope bios</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /bios # bios-setup-default</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel Turbo Boost Technology</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• Disabled—The processor does not increase its frequency automatically.</td>
</tr>
<tr>
<td>Intel Turbo Boost Technology</td>
<td>• Enabled—The processor utilizes Turbo Boost Technology if required.</td>
</tr>
</tbody>
</table>
### 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.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 I/O   | 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. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel VT-d Address Translation Services</td>
<td>Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The processor does not support ATS.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The processor uses VT-d ATS as required.</td>
</tr>
<tr>
<td>Intel VT-d PassThrough DMA</td>
<td>Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The processor does not support pass-through DMA.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The processor uses VT-d Pass-through DMA as required.</td>
</tr>
<tr>
<td>Direct Cache Access</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—Data from I/O devices is not placed directly into the processor cache.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—Data from I/O devices is placed directly into the processor cache.</td>
</tr>
<tr>
<td>Processor C3 Report</td>
<td>Whether the processor sends the C3 report to the operating system. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The processor does not send the C3 report.</td>
</tr>
<tr>
<td></td>
<td>• —The processor sends the C3 report using the ACPI C2 format.</td>
</tr>
<tr>
<td></td>
<td>• —The processor sends the C3 report using the ACPI C3 format.</td>
</tr>
<tr>
<td>Processor C6 Report</td>
<td>Whether the processor sends the C6 report to the operating system. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The processor does not send the C6 report.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The processor sends the C6 report.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hardware Prefetcher</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The hardware prefetcher is not used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The processor uses the hardware prefetcher when cache issues are detected.</td>
</tr>
<tr>
<td>Adjacent Cache-Line Prefetch</td>
<td>Whether the processor uses the Intel Adjacent Cache-Line Prefetch mechanism to fetch data when necessary. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The Adjacent Cache-Line Prefetch mechanism is not used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The Adjacent Cache-Line Prefetch mechanism is used when cache issues are detected.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Package C State Limit</td>
<td>The amount of power available to the server components when they are idle. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• System level coordination is in progress resulting in high power consumption. There might be performance issues until the coordination is complete.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• The server may enter any available C state.</td>
</tr>
<tr>
<td>Note</td>
<td>This option is used only if CPU C State is enabled.</td>
</tr>
<tr>
<td>Patrol Scrub</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• Disabled—The system checks for memory ECC errors only when the CPU reads or writes a memory address.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td>Demand Scrub</td>
<td>Whether the system allows a memory scrub to be performed on demand. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Disabled—The system does not allow a memory scrub to be performed on demand.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
</tbody>
</table>
### Device Tagging

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Select Memory RAS | How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following:  
  - **System**—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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB Port 0</td>
<td>Whether the processor uses USB port 0. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The server does not use the USB port 0.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The processor uses the USB port 0.</td>
</tr>
<tr>
<td>USB Port 1</td>
<td>Whether the processor uses USB port 1. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The server does not use the USB port 1.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The processor uses the USB port 1.</td>
</tr>
</tbody>
</table>

## Server Management BIOS Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assert NMI on SERR</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The BIOS does not generate an NMI or log an error when a SERR occurs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—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.</td>
</tr>
<tr>
<td>Assert NMI on PERR</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The BIOS does not generate an NMI or log an error when a PERR occurs.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The BIOS generates an NMI and logs an error when a PERR occurs. You must enable Assert NMI on SERR to use this setting.</td>
</tr>
<tr>
<td>FRB2 Enable</td>
<td>Whether the FRB2 timer is used by CIMC to recover the system if it hangs during POST. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>—The FRB2 timer is not used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>—The FRB2 timer is started during POST and used to recover the system if necessary.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Console Redirection| <ul><li>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:</li></ul>  
  
  - **Disabled**—No console redirection occurs during POST.  
  - **Enable**—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. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminal Type</td>
<td>What type of character formatting is used for console redirection. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>PC-ANSI</strong>— The PC-ANSI terminal font is used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VT100</strong>— A supported vt100 video terminal and its character set are used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VT100-PLUS</strong>— A supported vt100-plus video terminal and its character set are used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>VT-UTF8</strong>— A video terminal with the UTF-8 character set is used.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This setting must match the setting on the remote terminal application.</td>
</tr>
<tr>
<td>OS Boot Watchdog Timer</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disabled</strong>— The watchdog timer is not used to track how long the server takes to boot.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enabled</strong>— The watchdog timer tracks how long the server takes to boot. If the server does not boot within the length of time specified</td>
</tr>
<tr>
<td>OS Boot Watchdog Timer Policy</td>
<td>The action the system takes when the watchdog timer expires. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Do Nothing</strong>— The state of the server power does not change when the watchdog timer expires during OS boot.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Power Down</strong>— The server is powered off if the watchdog timer expires during OS boot.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Reset</strong>— The server is reset if the watchdog timer expires during OS boot.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This option is only applicable if you enable the OS Boot Watchdog Timer.</td>
</tr>
</tbody>
</table>
CHAPTER 4

Managing Storage Using RAID

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.

This chapter includes the following sections:

- RAID Options, page 47
- Configuring RAID, page 51
- Deleting the RAID Configuration, page 53
- Changing the Physical Drive State, page 54
- Rebuilding the Physical Drive, page 55
- Erasing the Contents of a Physical Drive, page 56
- Enabling Auto Rebuild on the Storage Controller, page 58
- Deleting a Virtual Drive, page 58
- Performing a Consistency Check on a Virtual Drive, page 59
- Reconstructing the Virtual Drive Options, page 61
- Making the Disk Drive Bootable, page 64

RAID Options

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*

```
RAID 0

Disk 1
Stripe Block A1
Stripe Block A3
Stripe Block A5

Disk 2
Stripe Block A2
Stripe Block A4
Stripe Block A6
```

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

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

**RAID 1**

RAID 1 creates a mirrored set of disk drives, where the data in both the disk drives is identical, providing redundancy and high availability. If one disk drive fails, the other disk drive takes over, preserving the data.
RAID 1 also allows you to use a hot spare disk drive. The hot spare drive is always active and is held in readiness as a hot standby drive during a failover.

**Figure 2: RAID 1**

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

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

**RAID 5**

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

**Figure 3: RAID 5**
RAID 5 provides more data storage capacity than RAID 1 and better data protection than RAID 0. It also supports hot swapping; however, RAID 1 offers better performance.

**Non-RAID**

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

**Summary of RAID Options**

<table>
<thead>
<tr>
<th>RAID Option</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| 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

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Server# scope chassis</td>
<td>Enters the chassis command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Server /chassis # show storageadapter</td>
<td>Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>Server /chassis # scope storageadapter SLOT-5</td>
<td>Enters command mode for an installed storage card.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>Server /chassis/storageadapter # show physical-drive</td>
<td>Displays physical disk drives. This information allows you to determine the status of the physical drives.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>Server /chassis/storageadapter # create-virtualdrive {-r0</td>
<td>-r1</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RO</strong>—The host can only read data from the drive.</td>
<td></td>
</tr>
<tr>
<td><strong>Blocked</strong>—The host cannot access the drive.</td>
<td></td>
</tr>
</tbody>
</table>

• (Optional) Drive cache options:
  - **DriveCacheDisable**—Caching is disabled on the physical drives.
  - **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.
  - **-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

(Optionalal) Displays virtual drive information for the storage card. This information allows you to verify RAID configuration.

This example shows how to configure RAID.

Server# **scope chassis**
Server /chassis # **show storageadapter**

<table>
<thead>
<tr>
<th>PCI Slot</th>
<th>Product</th>
<th>Name</th>
<th>Serial Number</th>
<th>Firmware Package Build</th>
<th>Product ID</th>
<th>Cache Memory Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>LSI</td>
<td>MegaRAID SAS</td>
<td>2004 ROMB 20.10.1-0092</td>
<td>LSI Logic 0 MB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Server /chassis # **scope storageadapter SLOT-5**

Server /chassis /storageadapter# **show physical-drive**

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Controller Status</th>
<th>Manufacturer</th>
<th>Model</th>
<th>Drive</th>
<th>Firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Managing Storage Using RAID

Deleting the RAID Configuration

---

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 clear all RAID configuration.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# scope chassis</td>
<td>Enters the chassis command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Server /chassis # show storageadapter</td>
<td>Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Server /chassis # scope storageadapter SLOT-5</td>
<td>Enters command mode for an installed storage card.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Server /chassis /storageadapter # clear-all-raid-config</td>
<td>Clears all RAID configuration. At the confirmation prompts answer Yes.</td>
</tr>
</tbody>
</table>

Note When RAID configuration is cleared, all existing data on the disk drive is lost.

This example shows how to delete RAID configuration.

Server# scope chassis
Server /chassis # show storageadapter

<table>
<thead>
<tr>
<th>PCI Slot</th>
<th>Product</th>
<th>Name</th>
<th>Serial Number</th>
<th>Firmware Package Build</th>
<th>Product ID</th>
<th>Cache Memory Size</th>
</tr>
</thead>
</table>

---

CLI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine
Integrated Management Controller, Release 3.1.1
Changing the Physical Drive State

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server#/scope chassis</td>
<td>Enters the chassis command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /chassis # show storageadapter</td>
<td>Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Server /chassis # scope storageadapter</td>
<td>Enters command mode for an installed storage card.</td>
</tr>
<tr>
<td></td>
<td>SLOT-5</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Server /chassis/storageadapter # show</td>
<td>Displays physical disk drives.</td>
</tr>
<tr>
<td></td>
<td>physical-drive</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>Server /chassis/storageadapter # scope</td>
<td>Enters command mode for the specified physical drive.</td>
</tr>
<tr>
<td></td>
<td>physical-drive slot-number</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>Server /chassis/storageadapter/physical-drive # show detail</td>
<td>Displays information about the specified physical drive.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Server /chassis/storageadapter/physical-drive # set state {unconfiguredgood</td>
<td>jbod</td>
</tr>
<tr>
<td>Step 8</td>
<td>Server /chassis/storageadapter/physical-drive* # commit</td>
<td>Commits the changes.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Server /chassis/storageadapter/physical-drive # show detail</td>
<td>Displays information about the specified physical drive.</td>
</tr>
</tbody>
</table>
This example shows how to change the state of the physical drive.

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

<table>
<thead>
<tr>
<th>PCI Slot</th>
<th>Product Name</th>
<th>Serial Number</th>
<th>Firmware Package Build</th>
<th>Product ID</th>
<th>Cache Memory Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>LSI MegaRAID SAS</td>
<td>2004 ROMB</td>
<td>20.10.1-0092</td>
<td>LSI Logic</td>
<td>0 MB</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Controller Status</th>
<th>Manufacturer</th>
<th>Model</th>
<th>Drive Firmware</th>
<th>Coerced Size</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SLOT-5 system</td>
<td>TOSHIBA</td>
<td>MBF2600RC</td>
<td>5704</td>
<td>571250 MB</td>
<td>HDD</td>
</tr>
<tr>
<td>2</td>
<td>SLOT-5 unconfigured good</td>
<td>ATA</td>
<td>ST9500620NS</td>
<td>SN01</td>
<td>475883 MB</td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

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

Rebuilding the Physical Drive

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 manually start the rebuild process on the physical drive.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Server# scope chassis</td>
<td>Enters the chassis command mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Server /chassis # show storageadapter</strong></td>
<td>Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Server /chassis # scope storageadapter SLOT-5</strong></td>
<td>Enters command mode for an installed storage card.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Server /chassis/storageadapter # show physical-drive</strong></td>
<td>Displays physical disk drives.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Server /chassis/storageadapter # scope physical-drive slot-number</strong></td>
<td>Enters command mode for the specified physical drive.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>Server /chassis/storageadapter/physical-drive # rebuild</strong></td>
<td>Rebuilds the physical drive.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>Server /chassis/storageadapter/physical-drive # rebuild abort</strong></td>
<td>(Optional) Stops the rebuild process.</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>PCI Slot</th>
<th>Product</th>
<th>Serial Number</th>
<th>Firmware Package</th>
<th>Build</th>
<th>Product ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>LSI MegaRAID SAS</td>
<td>2004 ROMB</td>
<td>20.10.1-0092</td>
<td>2092</td>
<td>LSI Logic 0 MB</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Coerced Size</th>
<th>Type</th>
<th>Controller Status</th>
<th>Manufacturer</th>
<th>Model</th>
<th>Drive</th>
<th>Firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SLOT-5</td>
<td>HDD</td>
<td>system</td>
<td>TOSHIBA</td>
<td>MBF2600RC</td>
<td>5704</td>
<td>571250 MB</td>
</tr>
<tr>
<td>2</td>
<td>SLOT-5</td>
<td>HDD</td>
<td>unconfigured</td>
<td>ATA</td>
<td>ST9500620NS</td>
<td>SN01</td>
<td>475883 MB</td>
</tr>
</tbody>
</table>
```

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

### Erasing the Contents of a Physical 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 erase all of the contents of a physical drive and set it to zero.
# Managing Storage Using RAID

## Erasing the Contents of a Physical Drive

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope chassis</td>
<td>Enters the chassis command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /chassis # show storageadapter</td>
<td>Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Server /chassis # scope storageadapter SLOT-5</td>
<td>Enters command mode for an installed storage card.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Server /chassis/storageadapter # show physical-drive</td>
<td>Displays physical disk drives.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Server /chassis/storageadapter # scope physical-drive slot-number</td>
<td>Enters command mode for the specified physical drive.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Server /chassis/storageadapter /physical-drive # erase</td>
<td>Erases all of the contents of a physical drive and sets it to zero. <strong>Note</strong> The erase process takes a few hours to complete.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Server /chassis/storageadapter /physical-drive # erase abort</td>
<td>(Optional) Stops the erase process.</td>
</tr>
</tbody>
</table>

This example shows how to erase the contents of a physical drive.

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

PCI Slot Product Name Serial Number Firmware Package Build Product ID Cache Memory Size
-------- -------------------------------------------------------------- ------------------- ---------        |
--- 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# erase
Server /chassis /storageadapter/physical-drive# erase abort
```
Enabling Auto Rebuild on the Storage Controller

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope chassis</td>
<td>Enters the chassis command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /chassis # show storageadapter</td>
<td>Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Server /chassis # scope storageadapter SLOT-5</td>
<td>Enters command mode for an installed storage card.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Server /chassis/storageadapter # set global-hotspare-for-newdrives true</td>
<td>Enables auto rebuild on the storage controller.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Server /chassis/storageadapter* # commit</td>
<td>Commits the changes.</td>
</tr>
</tbody>
</table>

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

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

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

Deleting a Virtual Drive

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope chassis</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /chassis # show storageadapter</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Server /chassis # scope storageadapter SLOT-5</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Server /chassis/storageadapter # show virtual-drive</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Server /chassis/storageadapter # delete virtual-drive drive-number</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Server /chassis/storageadapter* # commit</td>
</tr>
</tbody>
</table>

This example shows how to delete a virtual drive.

```plaintext
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 virtual-drive
Virtual Drive Status Name Size RAID Level
----- -------------------- ------------------------ ------
0 Optimal 571250 MB RAID 0

Server /chassis /storageadapter # delete virtual-drive 0
Server /chassis /storageadapter *# commit
```

### Performing a Consistency Check on 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 verify the drives for consistency.

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server/chassis command mode. Enter the chassis command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Server /chassis # scope storageadapter SLOT-5. Enters command mode for an installed storage card.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Server /chassis/storageadapter # scope virtual-drive drive-number. Enters command mode for the specified virtual drive.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Server /chassis/storageadapter /virtual-drive # verify. Verifies the drive for consistency.</td>
</tr>
<tr>
<td></td>
<td>• For RAID 5—Checks if the data in all of the parity stripe blocks is correct.</td>
</tr>
<tr>
<td></td>
<td>• For RAID 1—Checks if the data in both disk drives is identical.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Server /chassis/storageadapter /virtual-drive # verify abort. (Optional) Stops the verify process.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Server /chassis/storageadapter /virtual-drive # show detail. Displays information about the specified virtual drive.</td>
</tr>
</tbody>
</table>

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

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

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

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# scope virtual-drive 0
Server /chassis /storageadapter/virtual-drive# verify
---
status: ok
...
Server /chassis /storageadapter/virtual-drive# show detail
Status: Optimal
   Name: 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
```
Reconstructing the Virtual Drive Options

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.

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

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 3: Retaining the Virtual Drive Size

<table>
<thead>
<tr>
<th>From:</th>
<th>Migrate to:</th>
<th>Add or Remove Disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>One physical drive with RAID 0</td>
<td>Two physical drives with RAID 1</td>
<td>Add one disk.</td>
</tr>
<tr>
<td>Two physical drives with RAID 1</td>
<td>One physical drive with RAID 0</td>
<td>Remove one disk.</td>
</tr>
<tr>
<td>Two physical drives with RAID 0</td>
<td>Three physical drives with RAID 5</td>
<td>Add one disk.</td>
</tr>
<tr>
<td>Three physical drives with RAID 5</td>
<td>Two physical drives with RAID 0</td>
<td>Remove one disk.</td>
</tr>
</tbody>
</table>

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

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 4: Increasing the Virtual Drive Size

<table>
<thead>
<tr>
<th>From:</th>
<th>Migrate to:</th>
<th>Add or Remove Disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>One physical drive with RAID 0</td>
<td>Two physical drives with RAID 0</td>
<td>Add one disk.</td>
</tr>
<tr>
<td>Three physical drives with RAID 5</td>
<td>Add two disks.</td>
<td></td>
</tr>
<tr>
<td>Three physical drives with RAID 0</td>
<td>Add two disks.</td>
<td></td>
</tr>
</tbody>
</table>
Reconstructing a Virtual Drive

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 61.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# scope chassis</td>
<td>Enters the chassis command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Server /chassis # show storageadapter</td>
<td>Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Server /chassis # scope storageadapter SLOT-5</td>
<td>Enters command mode for an installed storage card.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Server /chassis/storageadapter # scope virtual-drive drive-number</td>
<td>Enters command mode for the specified virtual drive.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Server /chassis/storageadapter /virtual-drive # reconstruct {-r0</td>
<td>-r1</td>
</tr>
</tbody>
</table>

- **-r0 | -r1 | -r5**—Available RAID levels are: RAID 0, RAID 1, or RAID 5.
### Making the Disk Drive Bootable

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.

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>`-add</td>
<td>-rmv`</td>
</tr>
</tbody>
</table>

**Step 6**

Server /chassis/storageadapter /virtual-drive # show detail  
Displays information about the specified virtual drive.

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

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

PCI Slot  Product       Name    Serial Number  Firmware Package Build  Product ID  Cache
----------  ---------------  --------  ---------------  -------------------------  ----------  ------
---        ----------------  --------  ---------------  -------------------------  ----------  ------
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: 475883 MB
   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
```
## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope chassis</td>
<td>Enters the chassis command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /chassis # show storageadapter</td>
<td>Displays information about installed storage cards. This information allows you to determine the slot in which the storage card is installed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Server /chassis # scope storageadapter SLOT-5</td>
<td>Enters command mode for an installed storage card.</td>
</tr>
</tbody>
</table>
| Step 4 | Server /chassis/storageadapter # show physical-drive | Displays physical disk drives. **Note** The physical drive status could be one of the following:  
  - **system**—JBOD mode. The drive is not configured as RAID.  
  - **online**—RAID mode.  
  - **unconfigured good**—The drive is ready to be assigned to a drive group or hot spare pool. No mode is configured on the drive.  
  - **hotspare**—The drive is designated as a spare drive. No mode is configured on the drive. |
| Step 5 | Server /chassis/storageadapter # set boot-drive \{pd1 | pd2 | pd3 | vd0\} | Makes the disk drive bootable. **Note** To make the disk drive bootable, the status of the drive must be **system**. The status **system** indicates that the drive is in JBOD (non-RAID) mode. |
| Step 6 | Server /chassis/storageadapter # commit | Commits the changes. |
| Step 7 | Server /chassis/storageadapter # show settings | Displays settings. |

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

Server# scope chassis  
Server /chassis# show storageadapter  

<table>
<thead>
<tr>
<th>PCI Slot</th>
<th>Product</th>
<th>Name</th>
<th>Serial Number</th>
<th>Firmware</th>
<th>Package</th>
<th>Build</th>
<th>Product ID</th>
<th>Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>---</td>
<td>LSI MegaRAID SAS 2004 ROMB</td>
<td>20.10.1-0092</td>
<td>LSI Logic</td>
<td>0 MB</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Slot Number</th>
<th>Controller Status</th>
<th>Manufacturer</th>
<th>Model</th>
<th>Drive</th>
<th>Firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Managing Storage Using RAID

#### Making the Disk Drive Bootable

<table>
<thead>
<tr>
<th>Slot</th>
<th>System</th>
<th>Model</th>
<th>Size</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SLOT-5</td>
<td>TOSHIBA MBF2600RC</td>
<td>5704</td>
<td>571250 MB</td>
</tr>
<tr>
<td>2</td>
<td>SLOT-5</td>
<td>unconfigured good ATA ST9500620NS SN01</td>
<td>475883 MB</td>
<td></td>
</tr>
</tbody>
</table>

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

This chapter includes the following sections:

- Viewing Server Properties, page 67
- Viewing the Actual Boot Order, page 68
- Viewing CIMC Information, page 68
- Viewing SD Card Information, page 69
- Viewing CPU Properties, page 70
- Viewing Memory Properties, page 70
- Viewing Power Supply Properties, page 71
- Viewing Storage Properties, page 72
- Viewing PCI Adapter Properties, page 75
- Viewing Power Policy Statistics, page 76
- Viewing Hard Drive Presence, page 77
- Viewing the MAC Address of an Interface, page 77
- Viewing the Status of CIMC Network Connections, page 78

Viewing Server Properties

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

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope chassis</td>
<td>Enters chassis command mode.</td>
</tr>
</tbody>
</table>
Command or Action | Purpose
--- | ---
Server /chassis # show detail | Displays server properties.

This example displays server properties:

```text
Server# scope chassis
Server /chassis # show detail
Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: unlocked
  Serial Number: P0C16161F1P
  Product Name: UCS-E160D-M1/K9
  UUID: 1255F7F0-9F17-0000-E312-94B74999D9E7
  Description
```

### Viewing the Actual Boot Order

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server# scope bios</td>
<td>Enters the BIOS command mode.</td>
</tr>
<tr>
<td>Server /bios # show actual-boot-order</td>
<td>Displays details of the BIOS status.</td>
</tr>
</tbody>
</table>

This example displays actual boot order:

```text
Server# scope bios
Server /bios # show actual-boot-order
Boot Order | Type | Boot Device
--- | --- | ---
1 | Internal EFI Shell | Internal EFI Shell
2 | CD/DVD | Linux Virtual CD/DVD 0324
3 | HDD | Cypress
4 | HDD | Linux Virtual FDD/HDD 0324
5 | FDD | Linux Virtual Floppy 0324
6 | Network Device (PXE) | BRCM MBA Slot 0301 v15.2.7
7 | Network Device (PXE) | BRCM MBA Slot 0302 v15.2.7
8 | Network Device (PXE) | BRCM MBA Slot 0300 v15.2.7
```

### Viewing CIMC Information

**Before You Begin**

Install the CIMC firmware on the server.
## Viewing SD Card Information

### Before You Begin

Install the CIMC firmware on the server.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope cimc</td>
<td>Enters CIMC command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /cimc # show [detail]</td>
<td>Displays the CIMC firmware, current time, and boot loader version.</td>
</tr>
</tbody>
</table>

This example shows information about the CIMC:

```text
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
```

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters chassis command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Displays CPU properties.</td>
</tr>
</tbody>
</table>

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
```

## Viewing Memory Properties

**Before You Begin**
The server must be powered on, or the properties will not display.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters chassis command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Displays memory properties.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Displays DIMM summary information.</td>
</tr>
</tbody>
</table>

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: M393B1K70DB0-
  Serial Number: 86A7D514
  Asset Tag: Dimm0_AssetTag
  Data Width: 64 bits
  Name Node0_Dimm1:
  Capacity: 8192 MB
```

This example displays DIMM summary information:

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

---

**Viewing Power Supply Properties**

**Before You Begin**

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

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Server# scope power-cap</td>
<td>Enters the power cap command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /power-cap # show [detail]</td>
<td>Displays the server power consumption information.</td>
</tr>
</tbody>
</table>

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

**Note**

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

**Before You Begin**

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# scope chassis</td>
<td>Enters the chassis command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Server /chassis # show storageadapter [slot] [detail]</td>
<td>Displays installed storage cards.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Server /chassis # scope storageadapter SLOT-5</td>
<td>Enters command mode for an installed storage card.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Server /chassis/storageadapter # show capabilities [detail]</td>
<td>Displays RAID levels supported by the storage card.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Server /chassis/storageadapter # show error-counters [detail]</td>
<td>Displays number of errors seen by the storage card.</td>
</tr>
<tr>
<td><strong>Step 6</strong> Server /chassis/storageadapter # show firmware-versions [detail]</td>
<td>Displays firmware version information for the storage card.</td>
</tr>
<tr>
<td><strong>Step 7</strong> Server /chassis/storageadapter # show hw-config [detail]</td>
<td>Displays hardware information for the storage card.</td>
</tr>
</tbody>
</table>
### Viewing Server Properties

#### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 8: Server/chassis/storageadapter # show pci-info [detail]</td>
<td>Displays adapter PCI information for the storage card.</td>
</tr>
</tbody>
</table>

This example displays storage properties:

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

<table>
<thead>
<tr>
<th>Controller</th>
<th>Product Name</th>
<th>Firmware Package</th>
<th>Build</th>
<th>Product ID</th>
<th>Cache Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLOT-5</td>
<td>LSI MegaRAID SAS 2004 ROMB</td>
<td>20.10.1-0092</td>
<td>LSI Logic</td>
<td>0 MB</td>
<td></td>
</tr>
</tbody>
</table>

### Viewing Physical Drive Properties

#### Note

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

#### Procedure

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

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

**Step 8** | Server /chassis/storageadapter/physical-drive # show status [detail]
| Displays status information about the specified physical drive.

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

```bash
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:

```bash
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

**Note**

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

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

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**

**Note**

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

**Before You Begin**

The server must be powered on, or the properties will not display.
# Viewing Power Policy Statistics

## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# scope chassis</td>
<td>Enters the chassis command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Server /chassis # show pci-adapters [detail]</td>
<td>Displays PCI adapter properties.</td>
</tr>
</tbody>
</table>

This example displays PCI adapter properties:

```
Server# scope chassis
Server /chassis # show pci-adapters
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...
```

## Viewing Power Policy Statistics

## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# show power-cap [detail]</td>
<td>Displays the server power consumption statistics and the power cap policy.</td>
</tr>
</tbody>
</table>

The displayed fields are described in the following table:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Consumption</td>
<td>The power currently being used by the server, in watts.</td>
</tr>
<tr>
<td>Maximum Consumption</td>
<td>The maximum number of watts consumed by the server since the last time it was rebooted.</td>
</tr>
<tr>
<td>Minimum Consumption</td>
<td>The minimum number of watts consumed by the server since the last time it was rebooted.</td>
</tr>
</tbody>
</table>

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

```
Server# scope power-cap
Server /power-cap # show detail
Cur Consumption (W): 36.10 W
Max Consumption (W): 075
Min Consumption (W): 36.10 W
Server /power-cap #
```
This example displays the detailed power statistics for a double-wide E-Series Server:

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

### Viewing Hard Drive Presence

**Before You Begin**

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope chassis</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /chassis # show hdd</td>
</tr>
</tbody>
</table>

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.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope cimc</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /cimc # scope network</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Server /cimc/network # show lom-mac-list [detail]</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>00:24:c4:f4:89:ee</td>
</tr>
<tr>
<td>GE1</td>
<td>00:24:c4:f4:89:ef</td>
</tr>
<tr>
<td>GE2</td>
<td>00:24:c4:f4:89:f0</td>
</tr>
<tr>
<td>GE3</td>
<td>00:24:c4:f4:89:f1</td>
</tr>
</tbody>
</table>

### 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.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope cimc</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /cimc # scope network</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Server /cimc/network # show link state [detail]</td>
</tr>
</tbody>
</table>

This example displays the status of the CIMC network connections:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # show link state
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Link Detected</td>
</tr>
<tr>
<td>GE1</td>
<td>No Link Detected</td>
</tr>
<tr>
<td>GE2</td>
<td>No Link Detected</td>
</tr>
<tr>
<td>GE3</td>
<td>No Link Detected</td>
</tr>
<tr>
<td>Dedicated</td>
<td>Link Detected</td>
</tr>
</tbody>
</table>

```
Server /cimc/network # show link-state detail
```

**Link State:**
- **Interface:** Console
  - **State:** Link Detected
- **Interface:** GE1
  - **State:** No Link Detected
- **Interface:** GE2
  - **State:** No Link Detected
- **Interface:** GE3
  - **State:** No Link Detected
- **Interface:** Dedicated
  - **State:** Link Detected
State: Link Detected
## Viewing Temperature Sensors

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Server#</td>
<td>scope sensor</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Server /sensor #</td>
<td>show temperature [detail]</td>
</tr>
</tbody>
</table>

This example displays temperature sensor statistics:

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Reading</th>
<th>Units</th>
<th>Min. Warning</th>
<th>Max. Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOH_TEMP_SENS</td>
<td>Normal</td>
<td>32.0</td>
<td>C</td>
<td>N/A</td>
<td>80.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P2_D1_TMP</td>
<td>Normal</td>
<td>20.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
<tr>
<td>DDR3_P1_A1_TMP</td>
<td>Normal</td>
<td>21.0</td>
<td>C</td>
<td>N/A</td>
<td>90.0</td>
</tr>
</tbody>
</table>

This chapter includes the following sections:

- **Viewing Temperature Sensors**, page 81
- **Viewing Voltage Sensors**, page 82
- **Viewing LED Sensors**, page 82
- **Viewing Storage Sensors**, page 83
Viewing Voltage Sensors

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# scope sensor</td>
<td>Enters sensor command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Server /sensor # show voltage [detail]</td>
<td>Displays voltage sensor statistics for the server.</td>
</tr>
</tbody>
</table>

This example displays voltage sensor statistics:

```
Server# scope sensor
Server /sensor # show voltage
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Sensor Status</th>
<th>Reading</th>
<th>Units</th>
<th>Min. Warning</th>
<th>Max. Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>P3V_BAT_SCALED</td>
<td>Normal</td>
<td>3.022</td>
<td>V</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>P12V_SCALED</td>
<td>Normal</td>
<td>12.154</td>
<td>V</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>P5V_SCALED</td>
<td>Normal</td>
<td>5.036</td>
<td>V</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>P3V3_SCALED</td>
<td>Normal</td>
<td>3.318</td>
<td>V</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>P5V_STBY_SCALED</td>
<td>Normal</td>
<td>5.109</td>
<td>V</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>PV_VCCP_CPU1</td>
<td>Normal</td>
<td>0.950</td>
<td>V</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>PV_VCCP_CPU2</td>
<td>Normal</td>
<td>0.891</td>
<td>V</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>P1V5_DDR3_CPU1</td>
<td>Normal</td>
<td>1.499</td>
<td>V</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>P1V5_DDR3_CPU2</td>
<td>Normal</td>
<td>1.499</td>
<td>V</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>P1V1_IOH</td>
<td>Normal</td>
<td>1.087</td>
<td>V</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>P1V8_AUX</td>
<td>Normal</td>
<td>1.773</td>
<td>V</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Viewing LED Sensors

Before You Begin

The server must be powered on, or the information will not display.
### Viewing Server Sensors

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope chassis</td>
<td>Enters chassis command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /chassis # show led [detail]</td>
<td>Displays the name, state, and color of the external LEDs.</td>
</tr>
</tbody>
</table>

This example displays information about the external LEDs:

```plaintext
Server# scope chassis
Server /chassis # show led
<table>
<thead>
<tr>
<th>LED Name</th>
<th>LED State</th>
<th>LED Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>LED_SYS_ACT</td>
<td>OFF</td>
<td>GREEN</td>
</tr>
<tr>
<td>LED_HLTH_STATUS</td>
<td>ON</td>
<td>GREEN</td>
</tr>
</tbody>
</table>

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

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope chassis</td>
<td>Enters chassis command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /chassis # show hdd [detail]</td>
<td>Displays storage sensor information.</td>
</tr>
</tbody>
</table>

The displayed fields are described in the following table:

<table>
<thead>
<tr>
<th>Name column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the storage device. This can be: HDD_X_PRS—Indicates the presence or absence of each hard drive.</td>
</tr>
<tr>
<td>Status</td>
<td>A brief description of the status of the storage device.</td>
</tr>
</tbody>
</table>
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**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LED Status</td>
<td>The current LED color, if any.</td>
</tr>
<tr>
<td></td>
<td>To make the physical LED on the storage device blink, select <strong>Turn On</strong> from the drop-down list. To let the storage device control whether the LED blinks, select <strong>Turn Off</strong>.</td>
</tr>
</tbody>
</table>

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 #
Managing Remote Presence

This chapter includes the following sections:

- Managing the Virtual KVM, page 85
- Configuring Virtual Media, page 88
- Managing Serial over LAN, page 92

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.


---

## Configuring the Virtual KVM

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

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Server# scope kvm</td>
<td>Enters KVM command mode.</td>
</tr>
<tr>
<td>2</td>
<td>Server /kvm # set enabled {yes</td>
<td>no}</td>
</tr>
<tr>
<td>3</td>
<td>Server /kvm # set encrypted {yes</td>
<td>no}</td>
</tr>
<tr>
<td>4</td>
<td>Server /kvm # set kvm-port port</td>
<td>Specifies the port used for KVM communication.</td>
</tr>
<tr>
<td>5</td>
<td>Server /kvm # set local-video {yes</td>
<td>no}</td>
</tr>
<tr>
<td>6</td>
<td>Server /kvm # set max-sessions sessions</td>
<td>Specifies the maximum number of concurrent KVM sessions allowed. The sessions argument is an integer between 1 and 4.</td>
</tr>
<tr>
<td>7</td>
<td>Server /kvm # commit</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
<tr>
<td>8</td>
<td>Server /kvm # show [detail]</td>
<td>(Optional) Displays the virtual KVM configuration.</td>
</tr>
</tbody>
</table>
This example configures the virtual KVM and displays the configuration:

```plaintext
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# set encrypted no
Server /kvm *# set kvm-port 2068
Server /kvm *# set max-sessions 4
Server /kvm *# set local-video yes
Server /kvm *# commit
Server /kvm *# show detail

KVM Settings:
Encryption Enabled: no
Max Sessions: 4
Local Video: yes
Active Sessions: 0
Enabled: yes
KVM Port: 2068

Server /kvm #
```

**What to Do Next**
Launch the virtual KVM from the GUI.

---

**Enabling the Virtual KVM**

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

**Procedure**

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

This example enables the virtual KVM:

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

Server /kvm #
```
Disabling the Virtual KVM

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# scope kvm</td>
<td>Enters KVM command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Server /kvm # set enabled no</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Server /kvm # commit</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Server /kvm # show [detail]</td>
<td>(Optional) Displays the virtual KVM configuration.</td>
</tr>
</tbody>
</table>

This example disables the virtual KVM:

Server# scope kvm
Server /kvm # set enabled no
Server /kvm # commit
Server /kvm #

Encryption Enabled Local Video Active Sessions Enabled KVM Port
------------------ ---------------- --------------- ------- --------
no yes 0 no 2068

Server /kvm #

Configuring Virtual Media

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# scope vmedia</td>
<td>Enters virtual media command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Server /vmedia # set enabled {yes</td>
<td>no}</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Server /vmedia # set encryption {yes</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Server /vmedia # set low-power-usb-enabled {yes</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> While mapping an ISO to a server which has a UCS VIC P81E card and the NIC is in Cisco Card mode:</td>
</tr>
<tr>
<td></td>
<td>• If the low power USB is enabled, after mapping the ISO and rebooting the host the card resets and ISO mapping is lost. The virtual drives are not visible on the boot selection menu.</td>
</tr>
<tr>
<td></td>
<td>• If the low power USB is disabled, after mapping the ISO, and rebooting the host and the CIMC, the virtual drivers appear on the boot selection menu as expected.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Server /vmedia # commit Commits the transaction to the system configuration.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Server /vmedia # show [detail] (Optional) Displays the virtual media configuration.</td>
</tr>
</tbody>
</table>

This example configures virtual media encryption:

```
Server# scope vmedia
Server /vmedia # set enabled yes
Server /vmedia *# set encryption yes
Server /vmedia *# set low-power-usb-enabled no
Server /vmedia *# commit
Server /vmedia # show detail
vMedia Settings:
  Encryption Enabled: yes
  Enabled: yes
  Max Sessions: 1
  Active Sessions: 0
  Low Power USB Enabled: no
```

**What to Do Next**

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

---

**Configuring a CIMC-Mapped vMedia Volume**

**Before You Begin**

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server # scope vmedia</td>
<td>Enters the virtual media command mode.</td>
</tr>
</tbody>
</table>
| **Step 2** Server /vmedia # map-cifs {volume-name | remote-share | remote-file-path} [mount options] | Maps a CIFS file for vMedia. You must specify the following:  
  - Name of the volume to create  
  - Remote share including IP address and the exported directory  
  - Path of the remote file corresponding to the exported directory.  
  - (Optional) Mapping options  
  - Username and password to connect to the server |
| **Step 3** Server /vmedia # map-nfs {volume-name | remote-share | remote-file-path} [mount options] | Maps an NFS file for vMedia. You must specify the following:  
  - Name of the volume to create  
  - Remote share including IP address and the exported directory  
  - Path of the remote file corresponding to the exported directory.  
  - (Optional) Mapping options |
| **Step 4** Server /vmedia # map-www {volume-name | remote-share | remote-file-path} [mount options] | Maps an HTTPS file for vMedia. You must specify the following:  
  - Name of the volume to create  
  - Remote share including IP address and the exported directory  
  - Path of the remote file corresponding to the exported directory.  
  - (Optional) Mapping options  
  - Username and password to connect to the server |

This example shows how to create a CIFS CIMC-mapped vmedia settings:

Server # scope vmedia  
Server /vmedia # map-cifs sample-volume //10.10.10.10/project /test/sample  
Server username:  
Server password: ****  
Confirm password: ****  
Server /vmedia #
### Viewing CIMC-Mapped vMedia Volume Properties

**Before You Begin**

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

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Server # scope vmedia</td>
<td>Enters the virtual media command mode.</td>
</tr>
<tr>
<td>2</td>
<td>Server /vmedia # show mappings detail</td>
<td>Displays information on all the vmedia mapping that are configured.</td>
</tr>
</tbody>
</table>

This example shows how to view the properties of all the configured vmedia mapping:

```
Server # scope vmedia
Server /vmedia # show mappings

Volume Map-status Drive-type remote-share remote-file mount-type
------- --------- ----------- ------------------ -------------- --------------
```

### Removing a CIMC-Mapped Mounted vMedia Volume

**Before You Begin**

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

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Server # scope vmedia</td>
<td>Enters the virtual media command mode.</td>
</tr>
<tr>
<td>2</td>
<td>Server /vmedia # unmap volume_name</td>
<td>Specifies the volume name to unmap.</td>
</tr>
</tbody>
</table>

This example shows how to unmap a CIMC-mapped vmedia volume:

```
Server # scope vmedia
Server /vmedia # show mappings

Volume Map-status Drive-type remote-share remote-file mount-type
------- --------- ----------- ------------------ -------------- --------------
```
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.
Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope sol</td>
<td>Enters SoL command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /sol # set enabled {yes</td>
<td>no}</td>
</tr>
<tr>
<td>Step 3</td>
<td>Server /sol # set baud-rate {9600</td>
<td>19200</td>
</tr>
<tr>
<td>Step 4</td>
<td>Server /sol # commit</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Server /sol # show [detail]</td>
<td>(Optional) Displays the SoL settings.</td>
</tr>
</tbody>
</table>

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
```

Launching Serial over LAN

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# connect host</td>
</tr>
</tbody>
</table>

**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.
Managing User Accounts

This chapter includes the following sections:

- Configuring Local Users, page 95
- LDAP Servers (Active Directory), page 96
- Viewing User Sessions, page 101
- Terminating a User Session, page 101

Configuring Local Users

Before You Begin

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope user usernumber</td>
<td>Enters user command mode for user number usernumber.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /user # set enabled {yes</td>
<td>no}</td>
</tr>
<tr>
<td>Step 3</td>
<td>Server /user # set name username</td>
<td>Specifies the username for the user.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Server /user # set password</td>
<td>You are prompted to enter the password twice.</td>
</tr>
</tbody>
</table>
| 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 |
Managing User Accounts

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Manage the power control options such as power on, power cycle, and power off</td>
<td></td>
</tr>
<tr>
<td>• Launch the KVM console and virtual media</td>
<td></td>
</tr>
<tr>
<td>• Clear all logs</td>
<td></td>
</tr>
<tr>
<td>• Toggle the locator LED</td>
<td></td>
</tr>
<tr>
<td>• admin—This user can perform all actions available through the GUI, CLI, and IPMI.</td>
<td></td>
</tr>
</tbody>
</table>

Step 6  
Server /user # commit  
Commits the transaction to the system configuration.

This example configures user 5 as an admin:

```bash
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.


**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.

**Procedure**

**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:

<table>
<thead>
<tr>
<th>Properties</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Name</td>
<td>CiscoAVPair</td>
</tr>
<tr>
<td>LDAP Display Name</td>
<td>CiscoAVPair</td>
</tr>
<tr>
<td>Unique X500 Object ID</td>
<td>1.3.6.1.4.1.9.287247.1</td>
</tr>
<tr>
<td>Description</td>
<td>CiscoAVPair</td>
</tr>
<tr>
<td>Syntax</td>
<td>Case Sensitive String</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Role</th>
<th>CiscoAVPair Attribute Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>shell:roles=&quot;admin&quot;</td>
</tr>
<tr>
<td>user</td>
<td>shell:roles=&quot;user&quot;</td>
</tr>
<tr>
<td>read-only</td>
<td>shell:roles=&quot;read-only&quot;</td>
</tr>
</tbody>
</table>
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.

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# <code>scope ldap</code> Enters the LDAP command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /ldap # `set enabled {yes</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Server /ldap # <code>set domain/LDAP domain name</code> Specifies an LDAP domain name.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Server /ldap # <code>set timeout seconds</code> Specifies the number of seconds the CIMC waits until the LDAP search operation times out. The value must be between 0 and 1800 seconds.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Server /ldap # `set encrypted {yes</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Server /ldap # <code>set base-dn domain-name</code> Specifies the Base DN that is searched on the LDAP server.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Server /ldap # <code>set attribute name</code> Specify an LDAP attribute that contains the role and locale information for the user. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. You can use an existing LDAP attribute that is mapped to the CIMC user roles and locales or you can create a custom attribute, such as the CiscoAVPair attribute, which has the following attribute ID: 1.3.6.1.4.1.9.287247.1</td>
</tr>
</tbody>
</table>

**Note** If you do not specify this property, user access is denied.
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.
## Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Server# scope ldap</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Server /ldap# scope ldap-group-rule</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**Server /ldap/ldap-group-rule # set group-auth {yes</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Server /ldap # scope role-group index</strong></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Server /ldap/role-group # set name group-name</strong></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>Server /ldap/role-group # set domain domain-name</strong></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>**Server /ldap/role-group # set role {admin</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>Server /ldap/role-group # commit</strong></td>
</tr>
</tbody>
</table>

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) (n/a) admin
```
Viewing User Sessions

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td><code>Server# show user-session</code></td>
<td>Displays information about current user sessions.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID column</td>
<td>The unique identifier for the session.</td>
</tr>
<tr>
<td>Username column</td>
<td>The username for the user.</td>
</tr>
<tr>
<td>IP Address column</td>
<td>The IP address from which the user accessed the server.</td>
</tr>
<tr>
<td>Type column</td>
<td>The method by which the user accessed the server. For example, CLI, vKVM, and so on.</td>
</tr>
<tr>
<td>Action column</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Note** You cannot terminate your current session from this tab.

This example displays information about current user sessions:

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

Terminating a User Session

**Before You Begin**

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

Terminating a User Session

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# show user-session</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Server /user-session # scope user-session session-number</td>
<td>Enters user session command mode for the numbered user session that you want to terminate.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Server /user-session # terminate</td>
<td>Terminates the user session.</td>
</tr>
</tbody>
</table>

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, page 103
- Configuring Common Properties, page 105
- Configuring IPv4, page 106
- Configuring the Server VLAN, page 107
- Network Security Configuration, page 108
- Configuring Network Analysis Module Capability, page 110
- NTP Settings Configuration, page 110

CIMC NIC Configuration

CIMC NICs

Two NIC modes are available for connection to the CIMC.

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.

Note

Dedicated mode is not applicable to the EHWIC E-Series NCE.
**NIC Redundancy**

- None—Redundancy is not available.
- Active-Standby—One port fails over to the other.

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

---

**Configuring CIMC NICs**

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

**Before You Begin**

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Server# scope cimc</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Server/cimc # scope network</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>**Server/cimc/network # set mode {dedicated</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>**Server/cimc/network # set redundancy {none</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>**Server/cimc/network # set interface {console</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>ge2</td>
<td>External interface, which can be used as a primary interface or as a backup interface.</td>
</tr>
<tr>
<td>ge3</td>
<td>External interface, which can be used as a primary interface or as a backup interface.</td>
</tr>
<tr>
<td>ge1-ge2</td>
<td>Failover between the GE1 and GE2 interfaces (active-standby only).</td>
</tr>
<tr>
<td>ge1-ge3</td>
<td>Failover between the GE1 and GE3 interfaces (active-standby only).</td>
</tr>
<tr>
<td>ge2-ge3</td>
<td>Failover between the GE2 and GE3 interfaces (active-standby only).</td>
</tr>
<tr>
<td>ge1-ge2-ge3</td>
<td>Failover between the GE1, GE2, and GE3 interfaces (active-standby only).</td>
</tr>
</tbody>
</table>

**Note**
All interface options that involve the GE3 interface are applicable for double-wide E-Series Servers only.

**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 6
Server /cimc/network # commit

Commits the transaction to the system configuration.

**Note**
The available NIC mode and NIC redundancy mode options may vary depending on your platform. If you select a mode not supported by your server, an error message displays when you save your changes.

This example configures the CIMC network interface:

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Server# scope cimc</td>
<td>Enters CIMC command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Server /cimc # scope network</td>
<td>Enters CIMC network command mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>Server /cimc/network # set hostname</td>
<td>Specifies the name of the host.</td>
</tr>
<tr>
<td>host-name</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>Server /cimc/network # commit</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

This example configures the common properties:

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

**Configuring IPv4**

**Before You Begin**

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Server# scope cimc</td>
<td>Enters CIMC command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Server /cimc # scope network</td>
<td>Enters CIMC network command mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>Server /cimc/network # set dhcp-enabled</td>
<td>Selects whether the CIMC uses DHCP.</td>
</tr>
<tr>
<td>{yes</td>
<td>no}</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>Server /cimc/network # set v4-addr</td>
<td>Specifies the IP address for the CIMC.</td>
</tr>
<tr>
<td>ipv4-address</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Network-Related Settings

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Server /cimc/network # set v4-netmask ipv4-netmask</strong>&lt;br&gt;Specifies the subnet mask for the IP address.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>Server /cimc/network # set v4-gateway gateway-ipv4-address</strong>&lt;br&gt;Specifies the gateway for the IP address.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>**Server /cimc/network # set dns-use-dhcp {yes</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>Server /cimc/network # set preferred-dns-server dns1-ipv4-address</strong>&lt;br&gt;Specifies the IP address of the primary DNS server.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>Server /cimc/network # set alternate-dns-server dns2-ipv4-address</strong>&lt;br&gt;Specifies the IP address of the secondary DNS server.</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>Server /cimc/network # commit</strong>&lt;br&gt;Commits the transaction to the system configuration.</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>Server /cimc/network # show [detail]</strong>&lt;br&gt;(Optional) Displays the IPv4 network settings.</td>
</tr>
</tbody>
</table>

This example configures and displays the IPv4 network settings:
```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set dhcp-enabled no
Server /cimc/network *# set v4-addr 10.20.30.11
Server /cimc/network *# set v4-netmask 255.255.248.0
Server /cimc/network *# set v4-gateway 10.20.30.1
Server /cimc/network *# set dns-use-dhcp-enabled no
Server /cimc/network *# set preferred-dns-server 192.168.30.31
Server /cimc/network *# set alternate-dns-server 192.168.30.32
Server /cimc/network *# commit
Server /cimc/network # show detail
```

**Network Setting:**
- IPv4 Address: 10.20.30.11
- IPv4 Netmask: 255.255.248.0
- IPv4 Gateway: 10.20.30.1
- DHCP Enabled: no
- Obtain DNS Server by DHCP: no
- Preferred DNS: 192.168.30.31
- Alternate DNS: 192.168.30.32
- VLAN Enabled: no
- VLAN ID: 1
- VLAN Priority: 0
- Hostname: Server
- MAC Address: 01:23:45:67:89:AB
- NIC Mode: dedicated
- NIC Redundancy: none

```
Server /cimc/network #
```

### Configuring the Server VLAN

**Before You Begin**

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

#### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# <code>scope cimc</code> Enters CIMC command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /cimc # <code>scope network</code> Enters CIMC network command mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Server /cimc/network # <code>scope ipblocking</code> Enters IP blocking command mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Server /cimc/network/ipblocking # `set enabled {yes</td>
</tr>
</tbody>
</table>
| **Step 5** | Server /cimc/network/ipblocking # `set fail-count fail-count` Sets the number of times a user can attempt to log in unsuccessfully before the system locks that user out for a specified length of time. 
The number of unsuccessful login attempts must occur within the time frame specified in the IP Blocking Fail Window field. Enter an integer between 3 and 10. |
| **Step 6** | Server /cimc/network/ipblocking # `set fail-window fail-seconds` Sets the length of time, in seconds, in which the unsuccessful login attempts must occur in order for the user to be locked out. Enter an integer between 60 and 120. |
| **Step 7** | Server /cimc/network/ipblocking # `set penalty-time penalty-seconds` Sets the number of seconds the user remains locked out if they exceed the maximum number of login attempts within the specified time window. Enter an integer between 300 and 900. |
| **Step 8** | Server /cimc/network/ipblocking # `commit` Commits the transaction to the system configuration. |

This example configures IP blocking:

```
Server# `scope cimc`
Server /cimc # `scope network`
Server /cimc/network # `scope ipblocking`
Server /cimc/network/ipblocking # `set enabled yes`
```
Configuring Network Analysis Module Capability

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Enters CIMC command mode.</strong></td>
</tr>
<tr>
<td>Server# scope cimc</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Enters CIMC network command mode.</strong></td>
</tr>
<tr>
<td>Server /cimc # scope network</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Enters Network Analysis Module (NAM) command mode.</strong></td>
</tr>
<tr>
<td>Server /cimc/network # scope nam</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Enables the NAM capability.</strong></td>
</tr>
<tr>
<td>Server /cimc/network/nam # set enabled yes</td>
<td>To disable the NAM capability, use the set enabled no command.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Verifies that the NAM capability is enabled or disabled.</strong></td>
</tr>
<tr>
<td>Server /cimc/network/nam # show detail</td>
<td></td>
</tr>
</tbody>
</table>

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.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters CIMC command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters CIMC network command mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters NTP command mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables the NTP service.</td>
</tr>
<tr>
<td></td>
<td>To disable the NTP service, use the <code>set enabled no</code> command.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures the IP address or domain name for the specified server to act as an NTP server or the time source server.</td>
</tr>
<tr>
<td></td>
<td>You can configure a maximum of four servers.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Displays whether the NTP service is enabled and the IP address or domain name of the NTP servers.</td>
</tr>
</tbody>
</table>

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, page 113
- Configuring SSH, page 114
- Configuring the XML API, page 115
- Configuring IPMI, page 116
- Configuring SNMP, page 117

Configuring HTTP

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

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server# scope http</td>
<td>Enters the HTTP command mode.</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /http # set enabled {yes</td>
<td>no}</td>
</tr>
<tr>
<td>Step 3</td>
<td>Server /http # set http-port number</td>
<td>Sets the port to use for HTTP communication. The default is 80.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Server /http # set https-port number</td>
<td>Sets the port to use for HTTPS communication. The default is 443.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Server /http # set timeout seconds</td>
<td>Sets the number of seconds to wait between HTTP requests before the CIMC times out and terminates the session.</td>
</tr>
</tbody>
</table>
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
```

<table>
<thead>
<tr>
<th>HTTP Port</th>
<th>HTTPS Port</th>
<th>Timeout</th>
<th>Active Sessions</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>443</td>
<td>1800</td>
<td>0</td>
<td>yes</td>
</tr>
</tbody>
</table>

```
Server /http #
```

## Configuring SSH

### Before You Begin

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

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# <code>scope ssh</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /ssh # `set enabled {yes</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Server /ssh # <code>set ssh-port number</code></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Server /ssh # <code>set timeout seconds</code></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Server /ssh # <code>commit</code></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Server /ssh # <code>show [detail]</code></td>
</tr>
</tbody>
</table>

This example configures SSH for the CIMC:

```
Server# `scope ssh
Server /ssh # `set enabled yes
Server /ssh *# `set ssh-port 22
```
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.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope xmlapi</td>
<td>Enters XML API command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server/xmlapi # set enabled {yes</td>
<td>no}</td>
</tr>
<tr>
<td>Step 3</td>
<td>Server/xmlapi *# commit</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

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

Server# scope xmlapi
Server /xmlapi # set enabled yes
Server /xmlapi *# commit
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters the IPMI command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables or disables IPMI access on this server.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies the highest privilege level that can be assigned to an IPMI session on this server. This can be:</td>
</tr>
</tbody>
</table>

- **readonly** — IPMI users can view information but cannot make any changes. If you select this option, IPMI users with the "Administrator", "Operator", or "User" user roles can only create read-only IPMI sessions, regardless of their other IPMI privileges.

- **user** — IPMI users can perform some functions but cannot perform administrative tasks. If you select this option, IPMI users with the "Administrator" or "Operator" user role can create user and read-only sessions on this server.

- **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.
### Purpose

**Command or Action**

**Purpose**

| Step 4 | Server /ipmi # set encryption-key key | Sets the IPMI encryption key to use for IPMI communications. The key value must be 40 hexadecimal numbers. |
| Step 5 | Server /ipmi # commit | Commits the transaction to the system configuration. |

This example configures IPMI over LAN for the CIMC:

```
Server# scope ipmi
Server /ipmi # set enabled yes
Server /ipmi *# set privilege-level admin
Server /ipmi *# set encryption-key abcdef01234567890abcdef01234567890abcdef
Server /ipmi *# commit
Server /ipmi *# show
```

<table>
<thead>
<tr>
<th>Enabled Encryption Key</th>
<th>Privilege Level Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>yes</td>
<td>abcdef01234567890abcdef01234567890abcdef</td>
</tr>
</tbody>
</table>

### Configuring SNMP

**SNMP**


### Configuring SNMP Properties

**Before You Begin**

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope snmp</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /snmp # set enabled {yes</td>
</tr>
<tr>
<td>Step 3</td>
<td>Server /snmp # commit</td>
</tr>
</tbody>
</table>
## Configuring SNMP Properties

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> Server /snmp # set community-str community</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Server /snmp # setcommunity-access</td>
<td>This can be one of the following: Disabled, Limited, or Full.</td>
</tr>
<tr>
<td><strong>Step 6</strong> Server /snmp # settrap-community-str</td>
<td>Specifies the SNMP community group to which trap information should be sent. The name can be up to 18 characters.</td>
</tr>
<tr>
<td><strong>Step 7</strong> Server /snmp # set sys-contact contact</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 8</strong> Server /snmp # set sys-location location</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 9</strong> Server /snmp # commit</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

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
```

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 119.
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope snmp</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /snmp # scope trap-destinations number</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Server /snmp/trap-destinations # set enabled {yes</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Server /snmp/trap-destinations # set version {1</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Server /snmp/trap-destinations # set type {trap</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Server /snmp/trap-destinations # set user user</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Server /snmp/trap-destination # set v4-addr ip-address</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Server /snmp/trap-destination # commit</td>
</tr>
</tbody>
</table>

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 #

Sending a Test SNMP Trap Message

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Server# scope snmp</td>
<td>Enters the SNMP command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Server /snmp # sendSNMPtrap</td>
<td>Sends an SNMP test trap to the configured SNMP trap destination that are enabled.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td>The trap must be configured and enabled in order to send a test message.</td>
<td></td>
</tr>
</tbody>
</table>

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.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>Server# scope snmp</td>
<td>Enters the SNMP command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Server /snmp # scope v3users number</td>
<td>Enters the SNMPv3 users command mode for the specified user number.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>Server /snmp/v3users # set v3add {yes</td>
<td>no}</td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action** | **Purpose**
--- | ---
• *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.

**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.

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:*examplekey3y*  
Please confirm v3auth-key:*examplekey3y*  
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 #
Managing Certificates

This chapter includes the following sections:

- Managing the Server Certificate, page 123
- Generating a Certificate Signing Request, page 123
- Creating a Self-Signed Certificate, page 125
- Uploading a Server Certificate, page 127

Managing the Server Certificate

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

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Generate the CSR from the CIMC.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>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.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Upload the new certificate to the CIMC.</td>
</tr>
</tbody>
</table>

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

Generating a Certificate Signing Request

Before You Begin

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope certificate</td>
<td>Enters the certificate command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /certificate # generate-csr</td>
<td>Launches a dialog for the generation of a certificate signing request (CSR).</td>
</tr>
</tbody>
</table>

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

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

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

This example generates a certificate signing request:

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

-----BEGIN CERTIFICATE REQUEST-----
MIIB/zCCAwGAQAwgZkxZa9JaBqNVBAYTA1VTM2awCQYDVQQIEwJDQTEVFVMgMA1UE
BkMUU2FtZ2pvc2UsIENBMRUwEwYDVQQKEwFPeGFrQStcSx1IEluYy4xZzARBgNVBAsT
ClRlc3QgR3VxAxATBgNVBAMTEHRlc3QxMS8xNzE2MDQwNi0xOzAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDaw
gYEAG6iCaJoJaVMHzC1903o6Mg5izqlzXcz75+Vfj2I6rH9aackClid3mkOVx5gJU
Pt55CVqpNgNLdvbDFSszXrays0OhqHmp9+Clv8FDuy1CDYfuaLtvlWvfevsKV0j6
mK3Ku+Yio8nv6Oxhr0oqa8t/hyt/L43I7TPN1HbOi3oha4=

-----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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | `openssl genrsa -out CA_keyfilename keysize` | 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.  
|  | Example:  
# openssl genrsa -out ca.key 1024 | |
| **Step 2** | `openssl req -new -x509 -days numdays -key CA_keyfilename -out CA_certfilename` | 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. |
|  | Example:  
# openssl req -new -x509 -days 365 -key ca.key -out ca.crt | |
| **Step 3** | `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". |
|  | Example:  
# echo "nsCertType = server" > openssl.conf | |
| **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` | 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:  
# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf | |

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.

```bash
# /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,
```
Country Name (2 letter code) [GB]: US
State or Province Name (full name) [Berkshire]: California
Locality Name (e.g., city) [Newbury]: San Jose
Organization Name (e.g., company) [My Company Ltd]: Example Incorporated
Organizational Unit Name (e.g., section) [blank]: Unit A
Common Name (e.g., your name or your server's hostname) [blank]: example.com
Email Address [blank]: admin@example.com

# echo "nsCertType = server" > openssl.conf
# /usr/bin/openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt -extfile openssl.conf
Signature ok
subject=/C=US/ST=California/L=San Jose/O=Example Inc./OU=Unit A/CN=example.com/emailAddress=john@example.com
Getting CA Private Key

What to Do Next
Upload the new certificate to the CIMC.

Uploading a Server Certificate

Before You Begin
You must log in as a user with admin privileges to upload a certificate.
The certificate to be uploaded must be available as readable text. During the upload procedure, you will copy the certificate text and paste it into the CLI.

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

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Server# scope certificate</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Server /certificate # upload</strong></td>
</tr>
</tbody>
</table>

Copy the certificate text, paste it into the console when prompted, and type CTRL+D to upload the certificate.
This example uploads a new certificate to the server:

```bash
Server# scope certificate
Server /certificate # upload
```

Please paste your certificate here, when finished, press CTRL+D.

```
-----BEGIN CERTIFICATE-----
MIIB/zCCAMgCAQAwg2kxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvcs2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEMBIGAoGBAM
-----END CERTIFICATE-----
```

<CTRL+D>
Configuring Platform Event Filters

This chapter includes the following sections:

- Platform Event Filters, page 129
- Enabling Platform Event Alerts, page 129
- Disabling Platform Event Alerts, page 130
- Configuring Platform Event Filters, page 130
- Interpreting Platform Event Traps, page 132

Platform Event Filters

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

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

Enabling Platform Event Alerts

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope fault</td>
<td>Enters the fault command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /fault # set platform-event-enabled yes</td>
<td>Enables platform event alerts.</td>
</tr>
</tbody>
</table>
### Disabling Platform Event Alerts

#### Procedure

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

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

#### Configuring Platform Event Filters

You can configure actions and alerts for the following platform event filters:
### Platform Event Filter ID

<table>
<thead>
<tr>
<th>ID</th>
<th>Platform Event Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Temperature Critical Assert Filter</td>
</tr>
<tr>
<td>2</td>
<td>Temperature Warning Assert Filter</td>
</tr>
<tr>
<td>3</td>
<td>Voltage Critical Assert Filter</td>
</tr>
<tr>
<td>4</td>
<td>Processor Assert Filter</td>
</tr>
<tr>
<td>5</td>
<td>Memory Critical Assert Filter</td>
</tr>
<tr>
<td>6</td>
<td>Drive Slot Assert Filter</td>
</tr>
<tr>
<td>7</td>
<td>LSI Critical Assert Filter</td>
</tr>
<tr>
<td>8</td>
<td>LSI Warning Assert Filter</td>
</tr>
</tbody>
</table>

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters the fault command mode.</td>
</tr>
</tbody>
</table>
| **Step 2**        | Enters the platform event filter command mode for the specified event.  
See the Platform Event Filter table for event ID numbers. |
| **Step 3**        | Selects the desired system action when this event occurs. The action can be one of the following:  
  - none — No system action is taken.  
  - reboot — The server is rebooted.  
  - power-cycle — The server is power cycled.  
  - power-off — The server is powered off. |
| **Step 4**        | 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**        | Commits the transaction to the system configuration. |
This example configures the platform event alert for an event:

Server# scope fault
Server /fault # scope pef 1
Server /fault/pef # set action reboot
Server /fault/pef # set send-alert yes
Server /fault/pef *# commit
Server /fault/pef # show

<table>
<thead>
<tr>
<th>Platform Event Filter</th>
<th>Event Description</th>
<th>Action</th>
<th>Send Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Temperature Critical Assert Filter</td>
<td>reboot</td>
<td>yes</td>
</tr>
</tbody>
</table>

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:


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.

<table>
<thead>
<tr>
<th>Event Number [Note 1]</th>
<th>Platform Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0h Test Trap</td>
</tr>
<tr>
<td>65799</td>
<td>010107h Temperature Warning</td>
</tr>
<tr>
<td>65801</td>
<td>010109h Temperature Critical</td>
</tr>
<tr>
<td>131330</td>
<td>020102h Under Voltage, Critical</td>
</tr>
<tr>
<td>131337</td>
<td>020109h Voltage Critical</td>
</tr>
<tr>
<td>196871</td>
<td>030107h Current Warning</td>
</tr>
<tr>
<td>262402</td>
<td>040102h Fan Critical</td>
</tr>
<tr>
<td>459776</td>
<td>070400h Processor related (IOH-Thermalert/Caterr sensor) – predictive failure deasserted</td>
</tr>
<tr>
<td>459777</td>
<td>070401h Processor related (IOH-Thermalert/Caterr sensor) – predictive failure asserted</td>
</tr>
<tr>
<td>Event Number [Note 1]</td>
<td>Platform Event Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>460032 070500h</td>
<td>Processor Power Warning – limit not exceeded</td>
</tr>
<tr>
<td>460033 070501h</td>
<td>Processor Power Warning – limit exceeded</td>
</tr>
<tr>
<td>524533 0800F5h</td>
<td>Power Supply Critical</td>
</tr>
<tr>
<td>524551 080107h</td>
<td>Power Supply Warning</td>
</tr>
<tr>
<td>525313 080401h</td>
<td>Discrete Power Supply Warning</td>
</tr>
<tr>
<td>527105 080B01h</td>
<td>Power Supply Redundancy Lost</td>
</tr>
<tr>
<td>527106 080B02h</td>
<td>Power Supply Redundancy Restored</td>
</tr>
<tr>
<td>552704 086F00h</td>
<td>Power Supply Inserted</td>
</tr>
<tr>
<td>552705 086F01h</td>
<td>Power Supply Failure</td>
</tr>
<tr>
<td>552707 086F03h</td>
<td>Power Supply AC Lost</td>
</tr>
<tr>
<td>786433 0C0001h</td>
<td>Correctable ECC Memory Errors, Release 1.3(1) and later releases, filter set to accept all reading types [Note 4]</td>
</tr>
<tr>
<td>786439 0C0007h</td>
<td>DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM), Generic Sensor [Notes 2,3]</td>
</tr>
<tr>
<td></td>
<td>Note: Displayed for the E-Series Servers and the SM E-Series NCE. Not displayed for the EHWIC E-Series NCE and the NIM E-Series NCE.</td>
</tr>
<tr>
<td>786689 0C0101h</td>
<td>Correctable ECC Memory Errors, Release 1.3(1) and later releases</td>
</tr>
<tr>
<td>818945 0C7F01h</td>
<td>Correctable ECC Memory Errors, Release 1.2(x) and earlier releases</td>
</tr>
<tr>
<td>818951 0C7F07h</td>
<td>DDR3_INFO sensor LED - RED bit asserted (Probable ECC error on a DIMM), 1.2(x) and earlier releases [Note 3]</td>
</tr>
<tr>
<td></td>
<td>Note: Displayed for the E-Series Servers and the SM E-Series NCE. Not displayed for the EHWIC E-Series NCE and the NIM E-Series NCE.</td>
</tr>
<tr>
<td>851968 0D0000h</td>
<td>HDD sensor indicates no fault, Generic Sensor [Note 2]</td>
</tr>
<tr>
<td>851972 0D0004h</td>
<td>HDD sensor indicates a fault, Generic Sensor [Note 2]</td>
</tr>
<tr>
<td>854016 0D0800h</td>
<td>HDD Absent, Generic Sensor [Note 2]</td>
</tr>
<tr>
<td>854017 0D0801h</td>
<td>HDD Present, Generic Sensor [Note 2]</td>
</tr>
<tr>
<td>880384 0D6F00h</td>
<td>HDD Present, no fault indicated</td>
</tr>
<tr>
<td>880385 0D6F01h</td>
<td>HDD Fault</td>
</tr>
<tr>
<td>880512 0D6F80h</td>
<td>HDD Not Present</td>
</tr>
<tr>
<td>880513 0D6F81h</td>
<td>HDD is deasserted but not in a fault state</td>
</tr>
<tr>
<td>884480 0D7F00h</td>
<td>Drive Slot LED Off</td>
</tr>
<tr>
<td>884481 0D7F01h</td>
<td>Drive Slot LED On</td>
</tr>
<tr>
<td>Event Number [Note 1]</td>
<td>Platform Event Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>884482</td>
<td>0D7F02h   Drive Slot LED fast blink</td>
</tr>
<tr>
<td>884483</td>
<td>0D7F03h   Drive Slot LED slow blink</td>
</tr>
<tr>
<td>884484</td>
<td>0D7F04h   Drive Slot LED green</td>
</tr>
<tr>
<td>884485</td>
<td>0D7F05h   Drive Slot LED amber</td>
</tr>
<tr>
<td>884486</td>
<td>0D7F01h   Drive Slot LED blue</td>
</tr>
<tr>
<td>884487</td>
<td>0D7F01h   Drive Slot LED read</td>
</tr>
<tr>
<td>884488</td>
<td>0D7F08h   Drive Slot Online</td>
</tr>
<tr>
<td>884489</td>
<td>0D7F09h   Drive Slot Degraded</td>
</tr>
</tbody>
</table>

**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).
### 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.

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.

  ---

  **Note**

- **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.

**Procedure**

| 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) Utilities**—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

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 136.

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Server# scope cimc</td>
<td>Enters CIMC command mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Server /cimc # scope firmware</td>
<td>Enters CIMC firmware command mode.</td>
</tr>
</tbody>
</table>
| 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  
  - http |
| Step 4 | (Optional) Server /cimc # show detail | Displays the progress of the firmware update. |
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.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope cimc</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /cimc # show [detail]</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Server /cimc # activate [1</td>
</tr>
</tbody>
</table>

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)
Installing BIOS Firmware from the TFTP Server

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 136.

Note

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope bios</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /bios # update tftp-ip-address path-and-filename</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) Server /bios # show detail</td>
</tr>
</tbody>
</table>

This example updates the BIOS firmware:

Server# scope bios
Server /bios # update 10.20.34.56 //test/dnld-ucs-k9-bundle.1.0.2h.bin
<CR> Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /bios #
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 136.

Procedure

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

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
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.eeeeeeeeeee... Done
Step 3: Downloading contents to module flash.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!... Done
Step 4: Validating the flash data.vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv... Done
Total time: 906 seconds
Fpga Upgraded successfully...!

EN120E-FOC181290L1 /cimc/firmware # show detail
Firmware Image Information:
```

CLI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine
Integrated Management Controller, Release 3.1.1

141
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 142.
• If the SD card is faulty, see Recovering from a Faulty SD Card, on page 145.
• If the file system is corrupted, see Recovering from a Corrupted File System, on page 148.
• 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.
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Router# hw-module sm slot oir-stop</td>
<td>Shuts down the power to the specified E-Series Server.</td>
</tr>
<tr>
<td><strong>Note</strong> 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong> 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.</td>
<td></td>
</tr>
</tbody>
</table>

| **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. |
Purpose

**Command or Action**  
**Purpose**

**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.

---

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
```

---

Firmware Management - Recovering from a Corrupted CIMC Firmware Image

---

CLI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine Integrated Management Controller, Release 3.1.1
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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 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 | ucs-cimc > boot current recovery | Boots the E-Series Server or NCE from the current image. |
| Step 6 | Recovery-shell # interface | 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. |

| ded | shared-lom-console |
### Command or Action | Purpose
--- | ---
```
sorted-lom-ge1 | sorted-lom-ge2 | sorted-lom-ge3
interface-ip-address netmask
gateway-ip-address
```
**Step 7** | Recovery-shell # `ping`
tftp-ip-address | Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.

**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.

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
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>Router# hw-module sm slot oir-stop</code></td>
<td>Shuts down the power to the specified E-Series Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>Router# hw-module sm slot oir-start</code></td>
<td>Restarts the specified E-Series Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Step 3</td>
<td>***</td>
<td>From the Hyper Terminal or Minicom, enter the *** command to enter the bootloader prompt.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ucse-cimc &gt; boot current recovery</code></td>
<td>Boots the E-Series Server or NCE from the current image.</td>
</tr>
</tbody>
</table>
| Step 5 | To check the file system of the specified partition and recover the corrupted file system, enter these commands. | 1. `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.  
   2. Do the following:  
      - If the command output displays `clean`, it indicates that the corrupted files are recovered. Enter the `reboot` command to reboot CIMC.  
      - **Note** Skip the steps that follow.  
      - If the command output does not display `clean`, proceed to Step 6. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **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. | **1** 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.  
**2** 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. | **1** Recovery-shell # `sd-card partition`  
Creates partitions on the SD card.  
**2** Recovery-shell # `sd-card format p3`  
Formats the p3 partition on the SD card.  
**3** Recovery-shell # `sd-card format p4`  
Formats the p4 partition on the SD card.  
**4** Recovery-shell # `reboot`  
Reboots CIMC.  
**5** (Optional) Recovery-shell # `sd-partition show`  
Displays the current partition on the SD card.  
**Note** When you partition the SD card, the contents of the SD card, such as, the configuration and ISO file, are lost. |
| **Step 8**| 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 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. |
This example recovers the CIMC firmware from the current image using the `fs-check p3` command in an E-Series Server:

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

```bash
ucse-cimc > boot current recovery
recovery-shell# fs-check p3
fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p3: recovering journal
/dev/mmcblk0p3: clean, 429/7840 files, 3331/31296 blocks
recovery-shell# fs-check p4
fsck 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:

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

## Recovery Shell Commands

<table>
<thead>
<tr>
<th>Recovery Shell Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery-shell # dedicated-interface</td>
<td>Specifies the IP address, subnet mask, and the gateway ip address of the dedicated interface.</td>
</tr>
<tr>
<td>interface-ip-address netmask gateway-ip-address</td>
<td></td>
</tr>
<tr>
<td>Recovery-shell # dedicated-interface</td>
<td>Shows the current configuration of the dedicated port.</td>
</tr>
<tr>
<td>(DEPRECATED)</td>
<td></td>
</tr>
<tr>
<td>Recovery-shell # interface [dedicated</td>
<td>shared-lom-console</td>
</tr>
<tr>
<td>Recovery-shell # interface</td>
<td>Shows the configuration on the interface.</td>
</tr>
<tr>
<td>Recovery-shell # sd-card format [p3</td>
<td>p4]</td>
</tr>
<tr>
<td>Recovery-shell # sd-card partition</td>
<td>Creates partitions on the SD card.</td>
</tr>
<tr>
<td>Recovery-shell # sd-partition show</td>
<td>Displays the current partition on the SD card.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recovery-shell # <strong>ping</strong> <code>tftp-ip-address</code></td>
<td>Pings the remote TFTP server in which the CIMC firmware is located to verify network connectivity.</td>
</tr>
<tr>
<td>Recovery-shell # <strong>update</strong> <code>tftp-ip-address</code> <em>image-filename</em></td>
<td>Installs the CIMC firmware image, which is located on a remote tftp server.</td>
</tr>
<tr>
<td>Recovery-shell # <strong>fs-check</strong> `[p3</td>
<td>p4]`</td>
</tr>
<tr>
<td>Recovery-shell # <strong>active image</strong></td>
<td>Shows the current active image that CIMC is running, which can be image 1 or image 2.</td>
</tr>
<tr>
<td>Recovery-shell # <strong>active image</strong> `[1</td>
<td>2]`</td>
</tr>
<tr>
<td>Recovery-shell # <strong>reboot</strong></td>
<td>Reboots the CIMC firmware.</td>
</tr>
</tbody>
</table>
Viewing Faults and Logs

This chapter includes the following sections:

- Faults, page 153
- System Event Log, page 154
- Cisco IMC Log, page 155

## Faults

### Viewing the Fault Summary

**Procedure**

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

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope sel</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server/sel # show entries [detail]</td>
</tr>
</tbody>
</table>

For system events, displays timestamp, the severity of the event, and a description of the event. The `detail` keyword displays the information in a list format instead of a table format.

This example displays the system event log:

```
Server# scope sel
Server/sel # show entries

Time                  Severity Description
--------------------- ------------- -----------------------------------------------------
2001-01-01 08:30:16   Warning     " PSU2 PSU2_VOUT: Voltage sensor for PSU2, non-recoverable event was asserted"
2001-01-01 08:30:15   Informational " LED_PSU_STATUS: Platform sensor, ON event was asserted"
2001-01-01 08:30:14   Critical    " PSU2 PSU2_VOUT: Voltage sensor for PSU2, non-recoverable event was asserted"
2001-01-01 08:30:14   Informational " LED_PSU_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 08:30:13   Critical    " PSU2 PSU2_VOUT: Voltage sensor for PSU2, failure event was asserted"
```

--More--
Clearing the System Event Log

Procedure

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

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

Procedure

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

This example displays the log of CIMC events:
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # show entries

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1970 Jan 4 18:55:36</td>
<td>BMC:kernel:</td>
<td>&lt;7&gt;/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:422: Controller-4 has a stuck bus, attempting to clear it now...</td>
</tr>
</tbody>
</table>
Clearing the CIMC Log

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Server# scope cimc</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Server /cimc # scope log</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Server /cimc/log # clear</strong></td>
</tr>
</tbody>
</table>

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.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Server# scope cimc</strong></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Server /cimc # scope log</strong></td>
</tr>
</tbody>
</table>
| **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

CLI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine
Integrated Management Controller, Release 3.1.1
### 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Server# scope cimc</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enters CIMC command mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Server /cimc # scope log</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enters CIMC log command mode.</td>
<td></td>
</tr>
</tbody>
</table>

| Step 3 | Server /cimc/log # scope server {1 | 2} | Purpose |
|--------|-----------------------------------------|---------|
|        | Selects one of two remote syslog server profiles and enters the command mode for configuring the profile. |

---

**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.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Server /cimc/log # commit</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Commits the transaction to the system configuration.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Server /cimc/log # show local-syslog-severity</th>
<th>(Optional) Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Displays the configured severity level.</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Server /cimc/log/server # set server-ip ip-address</th>
<th>Specifies the remote syslog server IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>Server /cimc/log/server # set enabled {yes</td>
<td>no}</td>
</tr>
<tr>
<td>Step 6</td>
<td>Server /cimc/log/server # commit</td>
<td>Commits the transaction to the system configuration.</td>
</tr>
</tbody>
</table>

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 #
```
**Server Utilities**

This chapter includes the following sections:

- Exporting Technical Support Data to a Remote Server, page 159
- Rebooting the CIMC, page 161
- Resetting the CIMC to Factory Defaults, page 161
- Exporting and Importing the CIMC Configuration, page 162

**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.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# scope cimc</td>
<td>Enters CIMC command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Server /cimc # scope tech-support</td>
<td>Enters tech-support command mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Server /cimc/tech-support # set remote-ip ip-address</td>
<td>Specifies the IP address of the remote server on which the support data file should be stored.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Server /cimc/tech-support # set remote-path path/filename</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Server /cimc/tech-support # set remote-protocol protocol-type</td>
<td>Specifies the remote server protocol. The remote server protocol can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• tftp</td>
</tr>
<tr>
<td></td>
<td>• ftp</td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
---|---
• 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.

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
```
Rebooting the CIMC

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

**Note**

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope cimc</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /cimc # reboot</td>
</tr>
</tbody>
</table>

This example reboots the CIMC:

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

Resetting the CIMC to Factory Defaults

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

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

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope cimc</td>
</tr>
</tbody>
</table>

Username:  
Password: ******  
Progress(%): 100  
Status: COMPLETED

What to Do Next

Provide the generated report file to Cisco TAC.
The CIMC factory defaults include the following conditions:

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

This example resets the CIMC to factory defaults:

```bash
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

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Server# scope cimc</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Server /cimc # scope import-export</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Server /cimc/import-export # export-config tfip-ip-address path-and-filename</td>
</tr>
</tbody>
</table>

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

This example shows how to back up the CIMC configuration:

Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # export-config 192.0.2.34 /ucs/backups/cimc5.xml
Export config started. Please check the status using "show detail".
Server /cimc/import-export # show detail
Import Export:
  Operation: EXPORT
  Status: COMPLETED
  Error Code: 100 (No Error)
  Diagnostic Message: NONE

Server /cimc/import-export #
Importing a CIMC Configuration

Before You Begin

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

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters CIMC command mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters import-export command mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

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

This example shows how to import a CIMC configuration:

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

This chapter includes the following sections:

- Diagnostic Tests Overview, page 165
- Mapping the Diagnostics Image to the Host, page 166
- Running Diagnostic Tests—E-Series Servers and SM E-Series NCE, page 167
- Running Diagnostic Tests—EHWIC E-Series NCE and NIM E-Series NCE, page 169

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Server# scope remote-install</td>
<td>Enters the remote install command mode.</td>
</tr>
</tbody>
</table>
| **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. |
## 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.

### 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.
### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Shell &gt; <code>dir virtual-media-drive-name:</code></td>
<td>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. <strong>Note</strong> Make sure that you add a colon after the virtual media drive name. For example, <code>dir fs1:</code></td>
</tr>
<tr>
<td>Step 2</td>
<td>Shell &gt; <code>virtual-media-drive-name:</code></td>
<td>Enters the virtual media drive in which the diagnostic file is located.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Virtual Media Drive <code>&gt;</code> <code>cp package-file-name dsh.pkg</code></td>
<td>Copies the package file for which you are running diagnostics into the diagnostics shell package file.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Virtual Media Drive <code>&gt;</code> <code>dsh</code></td>
<td>Enters the Diagnostics Shell. At the confirmation prompt, answer <code>y</code>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Server: SRV &gt; <code>run all</code></td>
<td>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 <code>test-name</code> command where <code>test-name</code> can be one of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>cpux64</code>—CPU diagnostic test.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>diskx64</code>—Block devices diagnostic test. Block devices include hard drive, USB drive, and SD cards.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <code>memoryx64</code>—Memory diagnostic test. <strong>Note</strong> Diagnostic tests can run for approximately 10 minutes.</td>
</tr>
<tr>
<td>Step 6</td>
<td>(Optional) Server: SRV &gt; <code>results</code></td>
<td>Displays a summary of the diagnostic test with Passed or Failed test status. <strong>Note</strong> 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 <code>all</code> command.</td>
</tr>
<tr>
<td>Step 7</td>
<td>(Optional) Server: SRV &gt; <code>show</code></td>
<td>Displays a list of global parameters and diagnostic test modules that were administered on the server.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Server: SRV &gt; <code>exit</code></td>
<td>Exits from Diagnostic Shell.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Open a service request with Cisco TAC.</td>
<td>If the diagnostic tests pass successfully, it indicates that there is no problem with the server CPU, memory, or block devices. The problem could be with some other hardware component or with the software configuration. Open a service request with Cisco TAC to isolate the problem.</td>
</tr>
</tbody>
</table>
This example runs all diagnostic tests:

```bash
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 data corruption 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 data corruption 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the AMIDiag EFI Shell, press any key (except q) to run the diagnostic tests.</td>
<td>Executes all available diagnostic tests and displays the progress. After the tests are completed, the Pass or Fail test status displays. <strong>Note</strong>: Diagnostic tests can run for approximately 10 minutes.</td>
</tr>
<tr>
<td>Step 2</td>
<td>(Optional) fs0:&gt; type AMIDIAG_OBD.log</td>
<td>Displays the Onboard Diag log files with details.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Server: fs0:&gt; exit</td>
<td>Exits from AMIDiag EFI Shell.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Open a service request with Cisco TAC.</td>
<td>If the diagnostic tests pass successfully, it indicates that there is no problem with the server CPU, memory, or block devices. The problem could be with some other hardware component or with the software configuration. Open a service request with Cisco TAC to isolate the problem. If the diagnostic tests fail, open a service request with Cisco TAC for further assistance.</td>
</tr>
</tbody>
</table>

What to Do Next

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

A

Active Directory 96, 99
   configuring groups 99
adapter 75
   PCI 75
auto rebuild, enabling 58

B

backing up 162, 163
   CIMC configuration 162, 163
BIOS 36, 136, 140
   CMOS 36
      clearing 36
      firmware 140
         installing from TFTP server 140
   obtaining firmware from Cisco 136
   obtaining firmware from Cisco options 136
   password 36
      clearing 36
   BIOS CMOS 36
      clearing 36
   BIOS firmware 140
      installing from TFTP server 140
   BIOS password 36
      clearing 36
   BIOS settings 34, 35, 37
      about 37
      advanced 34
      restoring defaults 37
      server management 35
   BIOS status 33
      viewing 33
   boot order 68
      viewing 68
   boot order, configuring 23

C

certificate management 127
   uploading a certificate 127
CIMC 68, 135, 136, 138, 139, 155, 156, 157, 161
   clearing log 156
   configuring log threshold 156
   firmware 138, 139
      activating 139
         installing from remote server 138
   firmware details 68
   firmware overview 135
   resetting to factory defaults 161
   sending log 157
   viewing log 155
CIMC CLI 4
   CIMC firmware 139, 142
      activating 139
         recovering from corrupted image 142
   CIMC firmware details 68
      viewing 68
   CIMC NICs 103
   CIMC overview 3
   CIMC-mapped vmedia volume 89, 91
      cifs 89
      nfs 89
      removing 91
      viewing properties 91
      www 89
common properties 105
communication services properties 113, 114, 116
   HTTP properties 113
   IPMI over LAN properties 116
   SSH properties 114
configuration 162, 163, 164
   backing up 163
   exporting 162
   importing 164
CPU properties 70
D

deleting 17, 58
diagnostics 167, 169
   E-Series Servers and SM E-Series NCE 167
   EHWIC E-Series NCE 169
   NIM E-Series NCE 169
test, running 167, 169
diagnostics image 166
disabling KVM 88
disk drive bootable 64
   using CIMC CLI 64

E

E-Series Server 1
   overview 1
enabling KVM 86, 87
encrypting virtual media 88
event filters, platform 129, 130
   about 129
   configuring 130
   event log, system 154, 155
   clearing 155
   viewing 154
   events 129, 130
   platform 129, 130
      disabling alerts 130
      enabling alerts 129
exporting 162, 163
   CIMC configuration 162, 163

F

fault summary 153
   viewing 153
faults 153
   viewing summary 153
firmware 135, 136, 138
   about 135
   installing from remote server 138
   obtaining from Cisco 136
   upgrading 136
floppy disk emulation 88

H

hard drive presence 77
host image 14, 17
HTTP properties 113

I

importing 164
   CIMC configuration 164
   IP blocking 108
   IPMI over LAN 116
      description 116
   IPMI over LAN properties 116
   IPv4 properties 106

K

KVM 86, 87, 88
   configuring 86
   disabling 88
   enabling 86, 87
KVM console 11, 85

L

LDAP 98
   See also Active Directory
      configuring in CIMC 98
   See also Active Directory
LDAP Server 96
LED sensors 82
link state 78
local users 95
locking IOS CLI configuration 26
locking server power button 31
LOM ports 77
   viewing properties 77

M

MAC address 77
   interface 77
mapping 14
mapping to host 166
memory properties 70

N

NAM 110
NCE 1
   overview 1
   network analysis module 110
   network connections 78
      status 78
network properties 104, 105, 106, 107
common properties 105
IPv4 properties 106
NIC properties 104
VLAN properties 107
network security 109
network time protocol 111
NIC properties 104
NTP settings 110
NTP Settings 111

RAID options 47
recovering from corrupt firmware 142
remote presence 86, 87, 88, 92, 93
configuring serial over LAN 92
launching serial over LAN 93
virtual KVM 86, 87, 88
virtual media 88
resetting the server 25

S
SD card 69
details 69
SD Card 145, 148
recovering from faulty 145, 148
SD card details 69
viewing 69
self-signed certificate 125
sensors 81, 82
temperature 81
voltage 82
serial over LAN 92, 93
configuring 92
launching 93
server management 23, 25, 28, 29
configuring the boot order 23
power cycling the server 29
powering off the server 28
powering on the server 28
resetting the server 25
shutting down the server 25
server properties 67
server software 2
shutting down the server 25
SNMP 117, 119, 120
configuring properties 117
configuring SNMPv3 users 120
configuring trap settings 119
sending test message 120
software 18
obtaining from VMware 18
SSH properties 114
storage properties 72, 73, 74
viewing adapter properties 72
viewing physical drive properties 73
viewing virtual drive properties 74
storage sensors 83
viewing 83
syslog 157
sending CIMC log 157
system event log 154, 155
clearing 155

PCI adapter 75
viewing properties 75
physical drive 55, 56
erasing 56
rebuilding 56
physical drive state 54
changing 54
platform event filters 129, 130
about 129
configuring 130
platform events 132
interpreting traps 132
Platform events 129, 130
diabling alerts 130
enabling alerts 129
PLD firmware 141
upgrading 141
power cycling the server 29
power policy statistics 76
viewing 76
power restore policy 30
power supply properties 71
powering off the server 28
powering on the server 28
PXE installation 13

RAID 51, 53
configuring 51
deleting 53

SD card 69
details 69
SD Card 145, 148
recovering from faulty 145, 148
SD card details 69
viewing 69
self-signed certificate 125
sensors 81, 82
temperature 81
voltage 82
serial over LAN 92, 93
configuring 92
launching 93
server management 23, 25, 28, 29
configuring the boot order 23
power cycling the server 29
powering off the server 28
powering on the server 28
resetting the server 25
shutting down the server 25
server properties 67
server software 2
shutting down the server 25
SNMP 117, 119, 120
configuring properties 117
configuring SNMPv3 users 120
configuring trap settings 119
sending test message 120
software 18
obtaining from VMware 18
SSH properties 114
storage properties 72, 73, 74
viewing adapter properties 72
viewing physical drive properties 73
viewing virtual drive properties 74
storage sensors 83
viewing 83
syslog 157
sending CIMC log 157
system event log 154, 155
clearing 155
### Index

**system event log** *continued*
- viewing 154

**T**
- technical support data, exporting 159
- temperature sensors 81

**U**
- unlocking IOS CLI configuration 27
- unlocking server power button 32
- unmapping 17
- uploading a server certificate 127
- user management 95, 98, 101
  - LDAP 98
  - local users 95
  - terminating user sessions 101
  - viewing user sessions 101
- user sessions 101
  - terminating 101
  - viewing 101

**V**
- virtual drive 59, 61, 63
  - performing consistency check 59
  - reconstruct 63
  - reconstructing options 61
- virtual KVM 86, 87, 88
- virtual media 88
- VLAN properties 107
- VMware 18
  - obtaining software 18
  - voltage sensors 82

**X**
- XML API 115
  - description 115
  - enabling 115

**Y**
- YAML 8