



Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 1.1(1)

First Published: 03/30/2010

Americas Headquarters

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

Text Part Number: OL-22347-01

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)

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

© 2010 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface **vii**

Audience **vii**

Organization **vii**

Conventions **viii**

Related Documentation **ix**

Documentation Feedback **ix**

Obtaining Documentation and Submitting a Service Request **x**

Overview **1**

Overview of the Cisco UCS C-Series Rack-Mount Servers **1**

Cisco Integrated Management Controller **2**

CIMC CLI **3**

Command Modes **3**

Command Mode Table **3**

Complete a Command **5**

Command History **5**

Committing, Discarding, and Viewing Pending Commands **5**

Command Output Formats **5**

Online Help for the CLI **6**

Managing the Server **7**

Toggling the Locator LED **7**

Resetting the Server Boot Order **8**

Powering On the Server **8**

Powering Off the Server **9**

Power Cycling the Server **9**

Resetting the Server **10**

Shutting Down the Server **10**

Viewing Server Properties **11**

Viewing CPU Properties **11**

Viewing Memory Properties	12
Viewing Power Supply Properties	12
Viewing Storage Properties	13
Viewing Server Sensors	15
Viewing Current Sensors	15
Viewing Power Supply Sensors	16
Viewing Fan Sensors	16
Viewing Temperature Sensors	17
Viewing Voltage Sensors	17
Managing Remote Presence	19
Managing the Virtual KVM	19
KVM Console	19
Enabling the Virtual KVM	19
Disabling the Virtual KVM	20
Configuring the Virtual KVM	21
Configuring Virtual Media	22
Managing Serial over LAN	22
Serial Over LAN	22
Guidelines and Restrictions for Serial Over LAN	23
Configuring Serial Over LAN	23
Launching Serial Over LAN	24
Managing User Accounts	25
Configuring Local Users	25
Configuring Active Directory	26
Active Directory	26
Configuring the Active Directory Server	26
Configuring Active Directory in the CIMC	28
Viewing User Sessions	29
Terminating a User Session	30
Configuring Network-Related Settings	31
Server NIC Configuration	31
Server NICs	31
Configuring Server NICs	32
Configuring Common Properties	33
Configuring IPv4	34

Configuring the Server VLAN	35
Network Security Configuration	36
Network Security	36
Configuring Network Security	36
Configuring Communication Services	39
Configuring HTTP	39
Configuring SSH	40
IPMI Over LAN Configuration	41
IPMI Over LAN	41
Configuring IPMI over LAN	41
Managing Certificates	43
Managing the Server Certificate	43
Generating a Certificate Signing Request	44
Creating a Self-Signed Certificate	45
Uploading a Server Certificate	47
Configuring Platform Event Filters	49
Platform Event Filters	49
Enabling Platform Event Alerts	49
Disabling Platform Event Alerts	50
Configuring Platform Event Filters	50
Configuring SNMP Trap Settings	52
CIMC Firmware Management	55
Overview of Firmware	55
Obtaining CIMC Firmware from Cisco	56
Installing CIMC Firmware from the TFTP Server	57
Activating Installed Firmware	58
Viewing Logs	59
CIMC Log	59
Viewing the CIMC Log	59
Clearing the CIMC Log	60
System Event Log	60
Viewing the System Event Log	60
Clearing the System Event Log	61
Server Utilities	63
Exporting Technical Support Data	63

Resetting the CIMC to Factory Defaults 64

Rebooting the CIMC 65

Clearing the BIOS CMOS 65

Recovering from a Corrupted BIOS 66



Preface

This preface includes the following sections:

- [Audience, page vii](#)
- [Organization, page vii](#)
- [Conventions, page viii](#)
- [Related Documentation, page ix](#)
- [Documentation Feedback , page ix](#)
- [Obtaining Documentation and Submitting a Service Request , page x](#)

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:

Title	Description
Overview	Describes the Cisco UCS C-Series Rack-Mount Servers and the CIMC CLI.
Managing the Server	Describes the CLI commands. Describes how to configure the boot device order, how to control power to the server, and how to reset the server.

Title	Description
Viewing Server Properties	Describes how to view the CPU, memory, power supply, and storage properties of the server.
Viewing Server Sensors	Describes how to view the power supply, fan, temperature, current, and voltage sensors.
Managing Remote Presence	Describes how to configure and manage the virtual KVM, virtual media, and the serial over LAN connection.
Managing User Accounts	Describes how to add, delete, and authenticate users, and how to manage user sessions.
Configuring Network-Related Settings	Describes how to configure network interfaces, network settings, and network security.
Configuring Communication Services	Describes how to configure server management communication by HTTP, SSH, and IPMI.
Managing Certificates	Describes how to generate, upload, and manage server certificates.
Configuring Platform Event Filters	Describes how to configure and manage platform event filters and SNMP settings.
CIMC Firmware Management	Describes how to obtain, install, and activate firmware images.
Viewing Logs	Describes how to view and clear log messages.
Server Utilities	Describes how to export support data, how to reset the server configuration to factory defaults, and how to reboot the management interface.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands, keywords, GUI elements, and user-entered text appear in bold font .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	Elements in square brackets are optional.
{x y z}	Required alternative keywords are grouped in braces and separated by vertical bars.

Convention	Indication
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<code>courier font</code>	Terminal sessions and information the system displays appear in <code>courier font</code> .
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

**Note**

Means *reader take note*.

**Tip**

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

**Caution**

Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

**Timesaver**

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

**Warning**

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

Related Documentation

Documentation for Cisco UCS C-Series Rack-Mount Servers is available at the following URL:

<http://www.cisco.com/go/unifiedcomputing/c-series-doc>

Documentation Feedback

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

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, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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.



CHAPTER 1

Overview

This chapter includes the following sections:

- [Overview of the Cisco UCS C-Series Rack-Mount Servers, page 1](#)
- [Cisco Integrated Management Controller, page 2](#)
- [CIMC CLI, page 3](#)

Overview of the Cisco UCS C-Series Rack-Mount Servers

Following are the Cisco UCS C-Series rack-mount servers:

- Cisco UCS C200 M1 Rack-Mount Server
- Cisco UCS C210 M1 Rack-Mount Server
- Cisco UCS C250 M1 Rack-Mount Server

UCS C200 M1 Rack-Mount Server

The Cisco UCS C200 M1 server is a high-density, two-socket, 1 RU rack-mount server. This server is built for production-level network infrastructure, web services, and mainstream data centers, and branch and remote-office applications.

UCS C210 M1 Rack-Mount Server

The Cisco UCS C210 M1 server is a general-purpose, two-socket, 2 RU rack-mount server. It is designed to balance performance, density, and efficiency for storage-intensive workloads. This server is built for applications such as network file and appliances, storage, database, and content-delivery.

UCS C250 M1 Rack-Mount Server

The Cisco UCS C250 M1 server is a high-performance, memory-intensive, two-socket, 2 RU rack-mount server. It is designed to increase performance, and it has the capacity for demanding virtualization and large-data-set workloads. The C250 M1 server also can reduce the cost of smaller memory footprints.

Cisco Integrated Management Controller

The Cisco Integrated Management Controller (CIMC) is the management service for the C-Series servers. CIMC runs within the server.

Management Interfaces

You can use a web-based GUI or SSH-based CLI to access, configure, administer, and monitor the server. Almost all tasks can be performed in either interface, and the results of tasks performed in one interface are displayed in another. However, you cannot do the following:

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

Tasks You Can Perform in CIMC

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

- Power on, power off, power cycle, reset and shut down the server
- Toggle the locator LED
- Configure the server boot order
- View server properties and sensors
- Manage remote presence
- Create and manage local user accounts, and enable remote user authentication through Active Directory
- Configure network-related settings, including NIC properties, IPv4, VLANs, and network security
- Configure communication services, including HTTP, SSH, and IPMI Over LAN
- Manage certificates
- Configure platform event filters
- Update CIMC firmware
- Monitor faults, alarms, and server status

No Operating System or Application Provisioning or Management

CIMC provisions servers, and as a result, exists below the operating system on a server. Therefore, you cannot use it to provision or manage operating systems or applications on servers. For example, you cannot do the following:

- Deploy an OS, such as Windows or Linux
- Deploy patches for software, such as an OS or an application
- Install base software components, such as anti-virus software, monitoring agents, or backup clients
- Install software applications, such as databases, application server software, or web servers

- Perform operator actions, including restarting an Oracle database, restarting printer queues, or handling non-CIMC user accounts
- Configure or manage external storage on the SAN or NAS storage

CIMC CLI

The CIMC CLI is a command-line management interface for Cisco UCS C-Series servers. You can launch the CIMC CLI and manage the server by the serial port or over the network by SSH or Telnet. By default, Telnet access is disabled.

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



Note To recover from a lost admin password, see the Cisco UCS C-Series server installation and service guide for your platform.

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 main command modes, the commands used to access each mode, and the CLI prompt associated with each mode.

Table 1: Main Command Modes and Prompts

Mode Name	Commands Used to Access	Mode Prompt
EXEC	top command from any mode	#
bios	scope bios command from EXEC mode	/bios #

Mode Name	Commands Used to Access	Mode Prompt
certificate	scope certificate command from EXEC mode	/certificate #
chassis	scope chassis command from EXEC mode	/chassis #
cimc	scope cimc command from EXEC mode	/cimc #
firmware	scope firmware command from cimc mode	/cimc/firmware #
log	scope log command from cimc mode	/cimc/ log #
network	scope network command from cimc mode	/cimc/network #
ip-blocking	scope ip-blocking command from network mode	/cimc/network/ip-blocking #
tech-support	scope tech-support command from cimc mode	/cimc/tech-support #
fault	scope fault command from EXEC mode	/fault #
pef	scope pef command from fault mode	/fault/pef #
trap-destination	scope trap-destination command from fault mode	/fault/trap-destination #
http	scope http command from EXEC mode	/http #
ipmi	scope ipmi command from EXEC mode	/ipmi #
kvm	scope kvm command from EXEC mode	/kvm #
ldap	scope ldap command from EXEC mode	/ldap #
sel	scope sel command from EXEC mode	/sel #
sensor	scope sensor command from EXEC mode	/sensor #
sol	scope sol command from EXEC mode	/sol #
ssh	scope ssh command from EXEC mode	/ssh #
user	scope user <i>user-number</i> command from EXEC mode	/user #
user-session	scope user-session <i>session-number</i> command from EXEC mode	/user-session #
vmedia	scope vmedia command from EXEC mode	/vmedia #

Complete 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.

Command History

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

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

Committing, Discarding, and Viewing Pending Commands

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

```
Server# scope chassis
Server /chassis # set locator-led off
Server /chassis *# commit
Server /chassis #
```

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.

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 a table. You can configure either of two presentation formats for displaying the output information when the **detail** keyword is used. The format choices are as follows:

- Default—For easy viewing, the command output is presented in a compact list.

This example shows 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
```

```
Name HDD_04_STATUS:
  Status : present
```

```
Server /chassis #
```

- **YAML**—For easy parsing by scripts, the command output is presented in the YAML™ (YAML Ain't Markup Language) data serialization language, delimited by defined character strings.

This example shows 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
```

```
---
  name: HDD_04_STATUS
  hdd-status: present
```

```
...
```

```
Server /chassis #
```

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

In most CLI command modes, you can enter **set cli output default** to configure the default format, or **set cli output yaml** to configure the YAML format.

Online Help for the CLI

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



CHAPTER 2

Managing the Server

This chapter includes the following sections:

- [Toggling the Locator LED, page 7](#)
- [Resetting the Server Boot Order, page 8](#)
- [Powering On the Server, page 8](#)
- [Powering Off the Server, page 9](#)
- [Power Cycling the Server, page 9](#)
- [Resetting the Server, page 10](#)
- [Shutting Down the Server, page 10](#)

Toggling the Locator LED

Before You Begin

You must have user privileges for all power control operations including this operation.

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # set locator-led {on off}	Enables or disables the chassis locator LED.
Step 3	Server /chassis # commit	Commits the transaction to the system configuration.

This example disables the chassis locator LED and commits the transaction:

```
Server# scope chassis
Server /chassis # set locator-led off
Server /chassis *# commit

Server /chassis #
```

Resetting the Server Boot Order



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

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters bios command mode.
Step 2	Server /bios # set boot-order <i>device1</i> [, <i>device2</i> [, <i>device3</i> [, <i>device4</i> [, <i>device5</i>]]]]	Specifies the boot device options and order. You can select one or more of the following: <ul style="list-style-type: none"> • cdrom—Bootable CD-ROM • fdd—Floppy disk drive • hdd—Hard disk drive • pxe—PXE boot • efi—Extensible Firmware Interface
Step 3	Server /bios # commit	Commits the transaction to the system configuration.

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

This example sets the boot order and commits the transaction:

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

Powering On the Server



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

Procedure

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

	Command or Action	Purpose
Step 2	Server /chassis # power on	Turns on the server.

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  UUID
-----
on      Not Specified Not Specified 208F0100020F000000BEA80000DEAD00
```

Powering Off the Server

Procedure

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

This example turns off the server:

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

Server /chassis # show
Power Serial Number Product Name  UUID
-----
off     Not Specified Not Specified 208F0100020F000000BEA80000DEAD00
```

Power Cycling the Server

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # power cycle	Power cycles the server.

This example power cycles the server:

```
Server# scope chassis
Server /chassis # power cycle
```

Resetting the Server

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # power hard-reset	After a prompt to confirm, resets the server.

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis mode.
Step 2	Server /chassis # power shutdown	Shuts down the server.

The following example shuts down the server:

```
Server# scope chassis
Server /chassis # power shutdown
```



CHAPTER 3

Viewing Server Properties

This chapter includes the following sections:

- [Viewing CPU Properties, page 11](#)
- [Viewing Memory Properties, page 12](#)
- [Viewing Power Supply Properties, page 12](#)
- [Viewing Storage Properties, page 13](#)

Viewing CPU Properties

Before You Begin

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

Procedure

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

This example displays CPU properties:

```
Server# scope chassis
Server /chassis # show cpu
Name          Cores    Version
-----
CPU1          4        Intel(R) Xeon(R) CPU           E5520 @ 2.27GHz
CPU2          4        Intel(R) Xeon(R) CPU           E5520 @ 2.27GHz

Server /chassis #
```

Viewing Memory Properties

Before You Begin

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

Procedure

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

This example displays memory properties:

```
Server# scope chassis
Server /chassis # show dimm
Name          Capacity (MB)  Speed (MHz)    Type
-----
DIMM_A1       2048           1067           Other
DIMM_A2       0              1067           Other
DIMM_B1       0              1067           Other
DIMM_B2       0              1067           Other
DIMM_C1       0              1067           Other
DIMM_C2       0              1067           Other
DIMM_D1       2048           1067           Other
DIMM_D2       0              1067           Other
DIMM_E1       0              1067           Other
DIMM_E2       0              1067           Other
DIMM_F1       0              1067           Other
DIMM_F2       0              1067           Other

Server /chassis #
```

Viewing Power Supply Properties

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope chassis	Enters chassis command mode.
Step 2	Server /chassis # show psu [detail]	Displays power supply properties.

This example displays power supply properties:

```
Server# scope chassis
Server /chassis # show psu
Name          In. Power (Watts)  Out. Power (Watts)  Firmware  Status
-----
PSU1          74                 650                 R0E       Present
PSU2          83                 650                 R0E       Present
```

```
Server /chassis #
```

Viewing Storage Properties

Before You Begin

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

Procedure

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

This example displays storage properties:

```
Server# scope chassis
Server /chassis # show hdd
Name                Status
-----
HDD_01_STATUS      present
HDD_02_STATUS      present
HDD_03_STATUS      present
HDD_04_STATUS      present

Server /chassis #
```




CHAPTER 4

Viewing Server Sensors

This chapter includes the following sections:

- [Viewing Current Sensors, page 15](#)
- [Viewing Power Supply Sensors, page 16](#)
- [Viewing Fan Sensors, page 16](#)
- [Viewing Temperature Sensors, page 17](#)
- [Viewing Voltage Sensors, page 17](#)

Viewing Current Sensors

Procedure

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

This example displays current sensor statistics:

```
Server# scope sensor
Server /sensor # show current
Name                               Sensor Status  Reading    Units    Min. Warning Max. Warning
Min. Failure Max. Failure
-----
VR_P2_IMON                          Normal         16.00     AMP      N/A         147.20
N/A                                  164.80
VR_P1_IMON                          Normal         27.20     AMP      N/A         147.20
N/A                                  164.80

Server /sensor #
```

Viewing Power Supply Sensors

Procedure

	Command or Action	Purpose
Step 1	Server# scope sensor	Enters sensor command mode.
Step 2	Server /sensor # show psu [detail]	Displays power supply sensor statistics for the server.
Step 3	Server /sensor # show psu-redundancy [detail]	Displays power supply redundancy sensor status for the server.

This example displays power supply sensor statistics:

```

Server# scope sensor
Server /sensor # show psu
Name                Sensor Status      Reading  Units      Min. Warning  Max. Warning
  Min. Failure      Max. Failure
-----
PSU1_STATUS         Normal              present
PSU2_STATUS         Normal              present

Server /sensor # show psu-redundancy
Name                Reading  Sensor Status
-----
PSU_REDUNDANCY     full    Normal

Server /sensor #

```

Viewing Fan Sensors

Procedure

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

This example displays fan sensor statistics:

```

Server# scope sensor
Server /sensor # show fan
Name                Sensor Status      Reading  Units      Min. Warning  Max. Warning
  Min. Failure      Max. Failure
-----
W793_FAN2_TACH1    Normal              2400    RPM        N/A           N/A
800                N/A
W793_FAN2_TACH2    Normal              2400    RPM        N/A           N/A
800                N/A
W793_FAN3_TACH1    Normal              2300    RPM        N/A           N/A
800                N/A
W793_FAN3_TACH2    Normal              2300    RPM        N/A           N/A

```

```

800          N/A
W793_FAN4_TACH1 Normal      2400      RPM      N/A      N/A
800          N/A
W793_FAN4_TACH2 Normal      1600      RPM      N/A      N/A
800          N/A

Server /sensor #

```

Viewing Temperature Sensors

Procedure

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

This example displays temperature sensor statistics:

```

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

Server /sensor #

```

Viewing Voltage Sensors

Procedure

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

This example displays voltage sensor statistics:

```

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

```

```

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

```

```
Server /sensor #
```



CHAPTER 5

Managing Remote Presence

This chapter includes the following sections:

- [Managing the Virtual KVM, page 19](#)
- [Configuring Virtual Media, page 22](#)
- [Managing Serial over LAN, page 22](#)

Managing the Virtual KVM

KVM Console

The KVM console is an interface accessible from CIMC that emulates a direct keyboard, video, and mouse (KVM) 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 on your computer
- CD/DVD or floppy drive on the network
- Disk image files on the network

You can use the KVM console to install an OS on the server.

Enabling the Virtual KVM

Before You Begin

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

Procedure

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

This example enables the virtual KVM:

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

Server /kvm #
```

Disabling the Virtual KVM

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope kvm	Enters KVM command mode.
Step 2	Server /kvm # set enabled no	Disables the virtual KVM. Note Disabling the virtual KVM disables access to the virtual media feature, but does not detach the virtual media devices if virtual media is enabled.
Step 3	Server /kvm # commit	Commits the transaction to the system configuration.
Step 4	Server /kvm # show [detail]	(Optional) Displays the virtual KVM configuration.

This example disables the virtual KVM:

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

```
Server /kvm #
```

Configuring the Virtual KVM

Before You Begin

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

Procedure

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

This example configures the virtual KVM and displays the configuration:

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

Server /kvm #
```

What to Do Next

Launch the virtual KVM from the GUI.

Configuring Virtual Media

Before You Begin

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

Procedure

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

This example configures virtual media encryption:

```
Server# scope vmedia
Server /vmedia # set enabled yes
Server /vmedia *# set encryption yes
Server /vmedia *# commit
Server /vmedia # show detail
vMedia Settings:
  Encryption Enabled: yes
  Enabled: yes
  Max Sessions: 4
  Active Sessions: 0

Server /vmedia #
```

What to Do Next

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

Managing Serial over LAN

Serial Over LAN

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

Guidelines and Restrictions for Serial Over LAN

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

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

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

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

Configuring Serial Over LAN

Before You Begin

You must log in as a user with admin privileges to configure serial over LAN (SoL).

Procedure

	Command or Action	Purpose
Step 1	Server# scope sol	Enters SoL command mode.
Step 2	Server /sol # set enabled {yes no}	Enables or disables SoL on this server.
Step 3	Server /sol # set baud-rate {9600 19200 38400 57600 115200}	Sets the serial baud rate the system uses for SoL communication. Note The baud rate must match the baud rate configured in the server serial console.
Step 4	Server /sol # commit	Commits the transaction to the system configuration.
Step 5	Server /sol # show [detail]	(Optional) Displays the SoL settings.

This example configures SoL:

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

```
yes      115200
Server /sol #
```

Launching Serial Over LAN

Procedure

	Command or Action	Purpose
Step 1	Server# connect host	Opens a serial over LAN (SoL) connection to the redirected server console port. You can enter this command in any command mode.

What to Do Next

To end the SoL session, you must close the CLI session. For example, to end an SoL session over an SSH connection, disconnect the SSH connection.



CHAPTER 6

Managing User Accounts

This chapter includes the following sections:

- [Configuring Local Users, page 25](#)
- [Configuring Active Directory, page 26](#)
- [Viewing User Sessions, page 29](#)
- [Terminating a User Session, page 30](#)

Configuring Local Users

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope user <i>usernumber</i>	Enters user command mode for user number <i>usernumber</i> .
Step 2	Server /user # set enabled { yes no }	Enables or disables the user account on the CIMC.
Step 3	Server /user # set name <i>username</i>	Specifies the username for the user.
Step 4	Server /user # set password	You are prompted to enter the password twice.
Step 5	Server /user # set role { readonly user admin }	Specifies the role assigned to the user. The roles are as follows: <ul style="list-style-type: none">• readonly—This user can view information but cannot make any changes.• user—This user can do the following:<ul style="list-style-type: none">• View all information

	Command or Action	Purpose
		<ul style="list-style-type: none"> • Manage the power control options such as power on, power cycle, and power off • Launch the KVM console and virtual media • Clear all logs • Toggle the locator LED <p>• admin—This user can perform all actions available through the GUI, CLI, and IPMI.</p>
Step 6	Server /user # commit	Commits the transaction to the system configuration.

This example configures user 5 as an admin:

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

Configuring Active Directory

Active Directory

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

When Active Directory is enabled in the CIMC, all user authentication and role authorization is performed by Active Directory, and the CIMC ignores the local database. If the CIMC cannot connect to Active Directory, it reverts to the local database.

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

Configuring the Active Directory Server

The CIMC can be configured to use Active Directory for user authentication and authorization. To use Active Directory, configure users with an attribute that holds the user role and locale information for the CIMC. You can use an existing LDAP attribute that is mapped to the CIMC user roles and locales or you can modify the Active Directory schema to add a new custom attribute, such as the CiscoAVPair attribute, which has an

attribute ID of 1.3.6.1.4.1.9.287247.1. For more information about altering the Active Directory schema, see the article at <http://technet.microsoft.com/en-us/library/bb727064.aspx>.

The following steps are to be performed on the Active Directory server.



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

Procedure

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

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

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

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

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

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

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

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

What to Do Next

Use the CIMC to configure Active Directory.

Configuring Active Directory in the CIMC

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

Before You Begin

You must be logged in as admin to configure Active Directory.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ldap	Enters the Active Directory command mode.
Step 2	Server /ldap # set enabled {yes no}	Enables or disables Active Directory. When Active Directory is enabled, all user authentication and role authorization is performed by Active Directory, and the CIMC ignores the local user database. Note If the CIMC cannot establish a connection to Active Directory, the CIMC reverts to using the local user database.
Step 3	Server /ldap # set server-ip <i>ip-address</i>	Specifies the Active Directory server IP address.
Step 4	Server /ldap # set timeout <i>seconds</i>	Specifies the number of seconds the CIMC waits until it assumes the connection to Active Directory cannot be established.
Step 5	Server /ldap # set encrypted {yes no}	If encryption is enabled, the server encrypts all information sent to Active Directory.
Step 6	Server /ldap # set base-dn <i>domain-name</i>	Specifies the domain that all users must be in.
Step 7	Server /ldap # set attribute <i>name</i>	Specify an LDAP attribute that contains the role and locale information for the user. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. You can use an existing LDAP attribute that is mapped to the CIMC user roles and locales or you can create a custom attribute, such as the CiscoAVPair attribute, which has the following attribute ID: 1.3.6.1.4.1.9.287247.1 Note If you do not specify this property, user access is restricted to read-only.
Step 8	Server /ldap # commit	Commits the transaction to the system configuration.
Step 9	Server /ldap # show [detail]	(Optional) Displays the Active Directory configuration.

This example configures Active Directory using the CiscoAVPair attribute:

```

Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set server-ip 10.10.10.123
Server /ldap *# set timeout 60
Server /ldap *# set encrypted on
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# commit
Server /ldap # show
Server IP          BaseDN          Encrypted Timeout  Enabled Attribute
-----
10.10.10.123      example.com    yes          60           yes    CiscoAvPair
Server /ldap #
    
```

Viewing User Sessions

Procedure

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

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

Name	Description
ID	The unique identifier for the session.
Name	The username for the user.
IP Address	The IP address from which the user accessed the server.
Type	The method by which the user accessed the server.
Killable	If your user account has admin privileges, this column displays yes if you can force the associated user session to end. Otherwise it displays N/A . Note You cannot terminate your current session.

This example displays information about current user sessions:

```

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

Terminating a User Session

Before You Begin

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

Procedure

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

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

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

Server /user-session #
```




CHAPTER 7

Configuring Network-Related Settings

This chapter includes the following sections:

- [Server NIC Configuration, page 31](#)
- [Configuring Common Properties, page 33](#)
- [Configuring IPv4, page 34](#)
- [Configuring the Server VLAN, page 35](#)
- [Network Security Configuration, page 36](#)

Server NIC Configuration

Server NICs

Two NIC modes are available for connection to the CIMC. In one mode, you can also choose an active-active or active-standby redundancy mode, depending on your platform.

NIC Mode

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

- **Dedicated**—A connection to the CIMC is available through the management Ethernet port or ports.
- **Shared LOM**—A connection to the CIMC is available only through the LAN On Motherboard (LOM) Ethernet host ports.



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

- **Shipping (if supported)**—A connection to the CIMC is available through the management Ethernet port or ports using a limited factory default configuration.



Note Shipping mode is intended only for your initial connection to the CIMC. Configure another mode for operation.

NIC Redundancy

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

- None—Redundancy is not available.
- Active-Active—All Ethernet ports operate simultaneously. This mode provides multiple paths to the CIMC.
- Active-Standby—One port fails over to the other.

The available redundancy modes vary depending on the selected network mode and your platform. For the available modes, see the Installation and Service Guide for your platform.

Configuring Server NICs

Configure a server NIC when you want to set the NIC mode and NIC redundancy.

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc/network # set mode {dedicated shared_lom shipping}	Sets the NIC mode to one of the following: <ul style="list-style-type: none"> • Dedicated—The management Ethernet port is used to access the CIMC. • Shared LOM—The LAN On Motherboard (LOM) Ethernet host ports are used to access the CIMC. <p>Note If you select Shared LOM, make sure that all host ports belong to the same subnet.</p> • Shipping—A limited configuration for initial connection. Select another mode for normal operation.
Step 4	Server /cimc/network # set redundancy {none active-active active-standby}	Sets the NIC redundancy mode when the NIC mode is Shared LOM. The redundancy mode can be one of the following: <ul style="list-style-type: none"> • none—The LOM Ethernet ports operate independently and do not fail over if there is a problem.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • active-active—If supported, all LOM Ethernet ports are utilized. • active-standby—If one LOM Ethernet port fails, traffic fails over to another LOM port.
Step 5	Server /cimc/network # commit	Commits the transaction to the system configuration. Note The available NIC mode and NIC redundancy mode options may vary depending on your platform. If you select a mode not supported by your server, an error message displays when you save your changes.

This example configures the CIMC network interface:

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

Configuring Common Properties

Use common properties to describe your server.

Before You Begin

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

Procedure

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

This example configures the common properties:

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

Configuring IPv4

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc/network # set dhcp-enabled {yes no}	Selects whether the CIMC uses DHCP. Note If DHCP is enabled, we recommend that the DHCP server be configured to reserve a single IP address for the CIMC. If the CIMC is reachable through multiple ports on the server, the single IP address must be reserved for the full range of MAC addresses of those ports.
Step 4	Server /cimc/network # set v4-addr <i>ipv4-address</i>	Specifies the IP address for the CIMC.
Step 5	Server /cimc/network # set v4-netmask <i>ipv4-netmask</i>	Specifies the subnet mask for the IP address.
Step 6	Server /cimc/network # set v4-gateway <i>gateway-ipv4-address</i>	Specifies the gateway for the IP address.
Step 7	Server /cimc/network # set dns-use-dhcp {yes no}	Selects whether the CIMC retrieves the DNS server addresses from DHCP.
Step 8	Server /cimc/network # set preferred-dns-server <i>dns1-ipv4-address</i>	Specifies the IP address of the primary DNS server.
Step 9	Server /cimc/network # set alternate-dns-server <i>dns2-ipv4-address</i>	Specifies the IP address of the secondary DNS server.
Step 10	Server /cimc/network # commit	Commits the transaction to the system configuration.
Step 11	Server /cimc/network # show [detail]	(Optional) Displays the IPv4 network settings.

This example configures and displays the IPv4 network settings:

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set dhcp-enabled yes
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: yes
  Obtain DNS Server by DHCP: no
  Preferred DNS: 192.168.30.31
  Alternate DNS: 192.168.30.32
  VLAN Enabled: no
  VLAN ID: 1
  VLAN Priority: 0
  Hostname: Server
  MAC Address: 01:23:45:67:89:AB
  NIC Mode: dedicated
  NIC Redundancy: none

Server /cimc/network #

```

Configuring the Server VLAN

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc/network # set vlan-enabled {yes no}	Selects whether the CIMC is connected to a VLAN.
Step 4	Server /cimc/network # set vlan-id <i>id</i>	Specifies the VLAN number.
Step 5	Server /cimc/network # set vlan-priority <i>priority</i>	Specifies the priority of this system on the VLAN.
Step 6	Server /cimc/network # commit	Commits the transaction to the system configuration.
Step 7	Server /cimc/network # show [detail]	(Optional) Displays the network settings.

This example configures the server VLAN:

```

Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set vlan-enabled yes
Server /cimc/network *# set vlan-id 10
Server /cimc/network *# set vlan-priority 32
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
  IPv4 Address: 10.20.30.11
  IPv4 Netmask: 255.255.248.0
  IPv4 Gateway: 10.20.30.1
  DHCP Enabled: yes
  Obtain DNS Server by DHCP: no

```

```

Preferred DNS: 192.168.30.31
Alternate DNS: 192.168.30.32
VLAN Enabled: yes
VLAN ID: 10
VLAN Priority: 32
Hostname: Server
MAC Address: 01:23:45:67:89:AB
NIC Mode: dedicated
NIC Redundancy: none

```

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

Network Security Configuration

Network Security

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

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

Configuring Network Security

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

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope network	Enters the CIMC network command mode.
Step 3	Server /cimc/network # scope ipblocking	Enters the IP blocking command mode.
Step 4	Server /cimc/network/ipblocking # set enabled {yes no}	Enables or disables IP blocking.
Step 5	Server /cimc/network/ipblocking # set fail-count <i>fail-count</i>	<p>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.</p> <p>The number of unsuccessful login attempts must occur within the time frame specified in the IP Blocking Fail Window field.</p> <p>Enter an integer between 3 and 10.</p>

	Command or Action	Purpose
Step 6	Server /cimc/network/ipblocking # set fail-window <i>fail-seconds</i>	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 <i>penalty-seconds</i>	Sets the number of seconds the user remains locked out if they exceed the maximum number of login attempts within the specified time window. Enter an integer between 300 and 900.
Step 8	Server /cimc/network/ipblocking # commit	Commits the transaction to the system configuration.

This example configures IP blocking:

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




CHAPTER 8

Configuring Communication Services

This chapter includes the following sections:

- [Configuring HTTP, page 39](#)
- [Configuring SSH, page 40](#)
- [IPMI Over LAN Configuration, page 41](#)

Configuring HTTP

Before You Begin

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

Procedure

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

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

This example configures HTTP for the CIMC:

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

Configuring SSH

Before You Begin

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

Procedure

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

This example configures SSH for the CIMC:

```
Server# scope ssh
Server /ssh # set enabled yes
Server /ssh *# set ssh-port 22
Server /ssh *# set timeout 600
Server /ssh *# commit
Server /ssh # show
SSH Port  Timeout  Active Sessions Enabled
-----
22        600     1                      yes
Server /ssh #
```

IPMI Over LAN Configuration

IPMI Over LAN

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 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 as a user with admin privileges to configure IPMI over LAN.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ipmi	Enters the IPMI command mode.
Step 2	Server /ipmi # set enabled { yes no }	Enables or disables IPMI access on this server.
Step 3	Server /ipmi # set privilege-level { readonly user admin }	Specifies the user role that must be assigned to users accessing the system through IPMI. The user roles are as follows: <ul style="list-style-type: none"> • readonly—This user can view information but cannot make any changes. • user—This user can do the following: <ul style="list-style-type: none"> • View all information • Manage the power control options such as power on, power cycle, and power off • Launch the KVM console and virtual media • Clear all logs • Toggle the locator LED • admin—This user can perform all actions available through the GUI, CLI, and IPMI.

	Command or Action	Purpose
		Note The value of this field must match exactly the role assigned to the user attempting to log in. For example, if this field is set to readonly and a user with the admin role attempts to log in through IPMI, that login attempt will fail.
Step 4	Server /ipmi # set encryption-key <i>key</i>	Sets the IMPI encryption key to use for IPMI communications. The key value must be 40 hexadecimal numbers.
Step 5	Server /ipmi # commit	Commits the transaction to the system configuration.

This example configures IPMI over LAN for the CIMC:

```

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

```



CHAPTER 9

Managing Certificates

This chapter includes the following sections:

- [Managing the Server Certificate, page 43](#)
- [Generating a Certificate Signing Request, page 44](#)
- [Creating a Self-Signed Certificate, page 45](#)
- [Uploading a Server Certificate, page 47](#)

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

	Command or Action	Purpose
Step 1	Generate the CSR from the CIMC.	
Step 2	Submit the CSR file to a certificate authority that will issue and sign your certificate. If your organization generates its own self-signed certificates, you can use the CSR file to generate a self-signed certificate.	
Step 3	Upload the new certificate to the CIMC.	Note The uploaded certificate must be created from a CSR generated by the CIMC. Do not upload a certificate that was not created by this method.

Generating a Certificate Signing Request

Before You Begin

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

Procedure

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

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

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

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

This example generates a certificate signing request:

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

-----BEGIN CERTIFICATE REQUEST-----
MIIB/zCCAQwCAQAwgZkxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBgNVBAst
```

```

ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWZHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YccYU
ZgAMivycsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAGMBAAGGJTajBqkq
hkiG9w0BCQcxPhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG6lCaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckClD3mkOVx5gJU
Ptt5CVQpNgNLdvdDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtlv1Wvfhevskv0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE REQUEST-----

```

Copy everything from "-----BEGIN ..." to "END CERTIFICATE REQUEST-----", paste to a file, send to your chosen CA for signing, and finally upload the signed certificate via upload command.

---OR---

Continue to self sign CSR and overwrite the current certificate?
All HTTPS and SSH sessions will be disconnected. [y|N]N

What to Do Next

Perform one of the following tasks:

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

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

Creating a Self-Signed Certificate

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



Note

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

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	<pre>openssl genrsa -out CA_keyfilename keysize</pre> <p>Example: # openssl genrsa -out ca.key 1024</p>	<p>This command generates an RSA private key that will be used by the CA.</p> <p>Note To allow the CA to access the key without user input, do not use the <code>-des3</code> option for this command.</p> <p>The specified file name contains an RSA key of the specified key size.</p>
Step 2	<pre>openssl req -new -x509 -days numdays -key CA_keyfilename -out CA_certfilename</pre> <p>Example: # openssl req -new -x509 -days 365 -key ca.key -out ca.crt</p>	<p>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.</p> <p>The certificate server is an active CA.</p>
Step 3	<pre>echo "nsCertType = server" > openssl.conf</pre> <p>Example: # echo "nsCertType = server" > openssl.conf</p>	<p>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.</p> <p>The OpenSSL configuration file <code>openssl.conf</code> contains the statement <code>"nsCertType = server"</code>.</p>
Step 4	<pre>openssl x509 -req -days numdays -in CSR_filename -CA CA_certfilename -set_serial 04 -CAkey CA_keyfilename -out server_certfilename -extfile openssl.conf</pre> <p>Example: # openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf</p>	<p>This command directs the CA to use your CSR file to generate a server certificate.</p> <p>Your server certificate is contained in the output file.</p>

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

```
# /usr/bin/openssl genrsa -out ca.key 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
# /usr/bin/openssl req -new -x509 -days 365 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
```



```
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:admin@example.com
# echo "nsCertType = server" > openssl.conf
# /usr/bin/openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt
-extfile openssl.conf
Signature ok
subject=/C=US/ST=California/L=San Jose/O=Example Inc./OU=Unit
A/CN=example.com/emailAddress=john@example.com
Getting CA Private Key
#
```

What to Do Next

Upload the new certificate to the CIMC.

Uploading a Server Certificate

Before You Begin

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

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



Note

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



Note

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

Procedure

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

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

This example uploads a new certificate to the server:

```
Server# scope certificate
Server /certificate # upload
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBgNVBAst
C1Rlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bf5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzC190306Mg51zq1zXcz75+VFj2I6rH9ascK1d3mkOVx5gJU
Ptt5CVQpNgNldvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvLWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L4317IPN1HhOi3oha4=
-----END CERTIFICATE-----
<CTRL+D>
```



CHAPTER 10

Configuring Platform Event Filters

This chapter includes the following sections:

- [Platform Event Filters, page 49](#)
- [Enabling Platform Event Alerts, page 49](#)
- [Disabling Platform Event Alerts, page 50](#)
- [Configuring Platform Event Filters, page 50](#)
- [Configuring SNMP Trap Settings, page 52](#)

Platform Event Filters

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

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

Enabling Platform Event Alerts

Procedure

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

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

The following example enables platform event alerts:

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

Disabling Platform Event Alerts

Procedure

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

The following example disables platform event alerts:

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

Configuring Platform Event Filters

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

ID	Platform Event Filter
1	Temperature Critical Assert Filter
2	Temperature Warning Assert Filter

ID	Platform Event Filter
3	Voltage Critical Assert Filter
4	Voltage Warning Assert Filter
5	Current Assert Filter
6	Fan Critical Assert Filter
7	Fan Warning Assert Filter
8	Processor Assert Filter
9	Power Supply Critical Assert Filter
10	Power Supply Warning Assert Filter
11	Power Supply Redundancy Lost Filter
12	Discrete Power Supply Assert Filter
13	Memory Assert Filter
14	Drive Slot Assert Filter

Procedure

	Command or Action	Purpose
Step 1	Server# scope fault	Enters the fault command mode.
Step 2	Server /fault # scope pef id	Enters the platform event filter command mode for the specified event. See the Platform Event Filter table for event ID numbers.
Step 3	Server /fault/pef # set action { none reboot power-cycle power-off }	Selects the desired system action when this event occurs. The action can be one of the following: <ul style="list-style-type: none"> • none—An alert is sent but no other action is taken. • reboot—An alert is sent and the server is rebooted. • power-cycle—An alert is sent and the server is power cycled. • power-off—An alert is sent and the server is powered off.
Step 4	Server /fault/pef # set send-alert { yes no }	Enables or disables the sending of a platform event alert for this event.

	Command or Action	Purpose
		Note For an alert to be sent, the filter trap settings must be configured properly and platform event alerts must be enabled.
Step 5	Server /fault/pef # commit	Commits the transaction to the system configuration.

This example configures the platform event alert for an event:

```
Server# scope fault
Server /fault # scope pef 13
Server /fault/pef # set action reboot
Server /fault/pef *# set send-alert yes
Server /fault/pef *# commit
Server /fault/pef # show
Platform Event Filter Event                Action      Send Alert
-----
13                Memory Assert Filter      reboot      yes

Server /fault/pef #
```

What to Do Next

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

- Enable platform event alerts
- Configure SNMP trap settings

Configuring SNMP Trap Settings

Procedure

	Command or Action	Purpose
Step 1	Server# scope fault	Enters the fault command mode.
Step 2	Server /fault # set community-str <i>string</i>	Enter the name of the SNMP community to which trap information should be sent.
Step 3	Server /fault # scope trap-destination <i>number</i>	Enters the SNMP trap destination command mode for the specified destination. Four SNMP trap destinations are available. The destination <i>number</i> is an integer between 1 and 4.
Step 4	Server /fault/trap-destination # set enabled {yes no}	Enables or disables the SNMP trap destination.
Step 5	Server /fault/trap-destination # set addr <i>ip-address</i>	Specifies the destination IP address to which SNMP trap information is sent.
Step 6	Server /fault/trap-destination # commit	Commits the transaction to the system configuration.

This example configures the SNMP trap destination:

```
Server# scope fault
Server /fault # set community-str public
Server /fault *# scope trap-destination 1
Server /fault/trap-destination # set enabled yes
Server /fault/trap-destination *# set addr 10.20.30.41
Server /fault/trap-destination *# commit
Server /fault/trap-destination # show
Trap Destination IP Address      Enabled
-----
1                               10.20.30.41  yes
Server /fault/trap-destination #
```




CHAPTER 11

CIMC Firmware Management

This chapter includes the following sections:

- [Overview of Firmware, page 55](#)
- [Obtaining CIMC Firmware from Cisco, page 56](#)
- [Installing CIMC Firmware from the TFTP Server, page 57](#)
- [Activating Installed Firmware, page 58](#)

Overview of Firmware

C-Series servers use firmware downloaded from cisco.com. This firmware is certified by Cisco to upgrade firmware on a C-Series server.

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



Warning

Do not use the .zip file to reimage your server.

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



Note

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

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

Install

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

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

Activate

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

Obtaining CIMC Firmware from Cisco

Procedure

- Step 1** Navigate to cisco.com.
- Step 2** Click **Support** on the top toolbar, and then select Software Download from the drop-down menu.
- Step 3** Click the **Unified Computing** link in the lower left corner, and then log in.
- Step 4** Expand the **Cisco C-Series Rack-Mount Servers** node.
You will see the following links:
 - Cisco UCS C250 M1 Extended-Memory Rack-Mount Server.
 - Cisco UCS C210 M1 General-Purpose Rack-Mount Server.
 - Cisco UCS C200 M1 High-Density Rack-Mount Server.
- Step 5** Click the appropriate link.
- Step 6** Click the **Unified Computing System (UCS) Integrated Management Controller Firmware** link, and then click the appropriate release version link.
- Step 7** Click **Download Now**.
The **Download Cart** dialog box appears.
- Step 8** Review the information in the **Download Cart** dialog box, and then click **Proceed with Download**.
The **Software Download Rules** page appears.
- Step 9** Review the download rules, and click **Agree**.
A dialog box listing your download appears. The **Select Location** dialog box also appears. This dialog box has the focus.
- Step 10** Select a location in the **Select Location** dialog box, and then click **Open**.
The download begins.
- Step 11** Click **Close** when the download is finished.
The file that you downloaded is a .zip file.

Warning Do not use the .zip file to reimage your server.

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

The name of the proper .bin you extract file depends on the model server you are reimaging. Following are examples of 1.0.2 firmware update files:

- C200 and C210—upd-pkg-c200-m1-cimc.full.1.0.2.bin
- C250—upd-pkg-c250-m1-cimc.full.1.0.2.bin

What to Do Next

Install the CIMC firmware on the server.

Installing CIMC Firmware from the TFTP Server

Before You Begin

Obtain the CIMC firmware from Cisco and store the file on a local TFTP server.



Note

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope firmware	Enters the CIMC firmware command mode.
Step 3	Server /cimc/firmware # update <i>tftp-ip-address path-and-filename</i>	Starts the firmware update. The server will obtain the update firmware at the specified path and file name from the TFTP server at the specified IP address.
Step 4	(Optional) Server /cimc/firmware # 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 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/firmware #
```

What to Do Next

Activate the new firmware.

Activating Installed Firmware

Before You Begin

Install the CIMC firmware on the server.

**Note**

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # scope firmware	Enters the firmware command mode.
Step 3	Server /cimc/firmware # show [detail]	Displays the available firmware images and status.
Step 4	Server /cimc/firmware # activate [1 2]	Activates the selected image. If no image number is specified, the server activates the currently inactive image.

This example activates firmware image 1:

```
Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # show detail
Firmware Image Information:
  Update Stage: NONE
  Update Progress: 100
  Current FW Version: 1.0(0.74)
  FW Image 1 Version: 1.0(0.66a)
  FW Image 1 State: BACKUP INACTIVATED
  FW Image 2 Version: 1.0(0.74)
  FW Image 2 State: RUNNING ACTIVATED

Server /cimc/firmware # activate 1
```



CHAPTER 12

Viewing Logs

This chapter includes the following sections:

- [CIMC Log, page 59](#)
- [System Event Log, page 60](#)

CIMC Log

Viewing the CIMC Log

Procedure

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

This example displays the log of CIMC events:

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # show entries
Time          Source          Description
-----
1970 Jan 4 18:55:36 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:306:I2c Controller-4 DAT is stuck-low,
issuing One Clock Pulse.
1970 Jan 4 18:55:36 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:301:I2c Controller-4 Loop:[0].
1970 Jan 4 18:55:36 BMC:kernel:-
"
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:422: Controller-4 has a stuck bus,
attempting to clear it now... "
1970 Jan 4 18:55:36 BMC:kernel:-
"
```

```

<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:402: Controller-4 Initiating I2c recovery
sequence. "
1970 Jan 4 18:55:36 BMC:IPMI:480      last message repeated 22 times
1970 Jan 4 18:55:28 BMC:IPMI:480      " mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
failed to read Bus[f4].Dev[5e]! ErrorStatus[77] "
1970 Jan 4 18:55:33 BMC:IPMI:486      last message repeated 17 times
1970 Jan 4 18:55:28 BMC:IPMI:486      " mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
failed to read Bus[f4].Dev[b0]! ErrorStatus[77] "
1970 Jan 4 18:55:31 BMC:IPMI:486      last message repeated 17 times
1970 Jan 4 18:55:26 BMC:IPMI:486      " mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
failed to read Bus[f4].Dev[b2]! ErrorStatus[77] "
1970 Jan 4 18:55:26 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:306:I2c Controller-4 DAT is stuck-low,
issuing One Clock Pulse.
1970 Jan 4 18:55:26 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:301:I2c Controller-4 Loop:[8].
--More--

```

Clearing the CIMC Log

Procedure

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

The following example clears the log of CIMC events:

```

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

```

System Event Log

Viewing the System Event Log

Procedure

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

This example displays the system event log:

```

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

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

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

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

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

```

Clearing the System Event Log

Procedure

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

This example clears the system event log:

```

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

```




CHAPTER 13

Server Utilities

This chapter includes the following sections:

- [Exporting Technical Support Data, page 63](#)
- [Resetting the CIMC to Factory Defaults, page 64](#)
- [Rebooting the CIMC, page 65](#)
- [Clearing the BIOS CMOS, page 65](#)
- [Recovering from a Corrupted BIOS, page 66](#)

Exporting Technical Support Data

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

Procedure

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

	Command or Action	Purpose
Step 6	Server /cimc/tech-support # start	Begins the transfer of the support data file to the TFTP server.
Step 7	Server /cimc/tech-support # cancel	(Optional) Cancels the transfer of the support data file to the TFTP server.

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

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

What to Do Next

Provide the generated report file to Cisco TAC.

Resetting the CIMC to Factory Defaults

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

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

Procedure

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

The CIMC factory defaults include the following conditions:

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

This example resets the CIMC to factory defaults:

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

Rebooting the CIMC

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



Note

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

Procedure

	Command or Action	Purpose
Step 1	Server# scope cimc	Enters the CIMC command mode.
Step 2	Server /cimc # reboot	The CIMC reboots.

This example reboots the CIMC:

```
Server# scope cimc
Server /cimc # reboot
```

Clearing the BIOS CMOS

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

Procedure

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

This example clears the BIOS CMOS memory:

```
Server# scope bios
Server /bios # clear-cmos
```

This operation will clear the BIOS CMOS.

```
Note: Server should be in powered off state to clear CMOS.
Continue?[y|n] y

Server /bios #
```

Recovering from a Corrupted BIOS

Before You Begin

- You must be logged in as admin to recover from a corrupted BIOS.
- Have the BIOS recovery ISO image ready. You will find the BIOS recovery ISO image under the Recovery folder of the firmware distribution package.
- Schedule some down time for the server because it will be power cycled at the end of the recovery procedure.

Procedure

	Command or Action	Purpose
Step 1	Server# scope bios	Enters the bios command mode.
Step 2	Server# recover	Launches a dialog for loading the BIOS recovery image.

This example shows how to recover from a corrupted BIOS:

```
Server# scope bios
Server /bios # recover
This operation will automatically power on the server to perform BIOS FW recovery.
Continue?[y|N]y
```

What to Do Next

Power cycle or reset the server.



INDEX

A

active directory [28](#)
Active Directory [26](#)

B

bios
 recovering corrupt [66](#)

C

certificate management
 uploading a certificate [47](#)
CIMC
 clearing log [60](#)
 firmware
 about [55](#)
 activating [58](#)
 installing from TFTP server [57](#)
 obtaining from Cisco [56](#)
 resetting to factory defaults [64](#)
 viewing log [59](#)
CIMC CLI [3](#)
CIMC overview [2](#)
common properties [33](#)
communication services properties
 HTTP properties [39](#)
 IPMI over LAN properties [41](#)
 SSH properties [40](#)
CPU properties [11](#)
current sensors [15](#)

D

disabling KVM [20](#)

E

enabling KVM [19, 21](#)
encrypting virtual media [22](#)
event filters, platform
 about [49](#)
 configuring [50](#)
event log, system
 clearing [61](#)
 viewing [60](#)
events
 platform
 disabling alerts [50](#)
 enabling alerts [49](#)

F

fan sensors [16](#)
firmware
 about [55](#)
 activating [58](#)
 installing from TFTP server [57](#)
 obtaining from Cisco [56](#)
floppy disk emulation [22](#)

H

HTTP properties [39](#)

I

IP blocking [36](#)
IPMI over LAN [41](#)
IPMI over LAN properties [41](#)
IPv4 properties [34](#)

- K**
- KVM
 - configuring [21](#)
 - disabling [20](#)
 - enabling [19,21](#)
 - KVM console [19](#)
- L**
- local users [25](#)
- M**
- memory properties [12](#)
- N**
- network properties
 - common properties [33](#)
 - IPv4 properties [34](#)
 - NIC properties [32](#)
 - VLAN properties [35](#)
 - network security [36](#)
 - NIC properties [32](#)
- P**
- platform event filters
 - about [49](#)
 - configuring [50](#)
 - Platform events
 - disabling alerts [50](#)
 - enabling alerts [49](#)
 - power cycling the server [9](#)
 - power supply properties [12](#)
 - power supply sensors [16](#)
 - powering off the server [9](#)
 - powering on the server [8](#)
- R**
- recovering from a corrupted bios [66](#)
 - remote presence
 - configuring serial over LAN [23](#)
 - launching serial over LAN [24](#)
 - virtual KVM [19,20,21](#)
 - virtual media [22](#)
 - resetting the boot order [8](#)
 - resetting the server [10](#)
- S**
- self-signed certificate [45](#)
 - sensors
 - current [15](#)
 - fan [16](#)
 - power supply [16](#)
 - temperature [17](#)
 - voltage [17](#)
 - serial over LAN [22,23,24](#)
 - configuring [23](#)
 - launching [24](#)
 - server management
 - power cycling the server [9](#)
 - powering off the server [9](#)
 - powering on the server [8](#)
 - resetting the boot order [8](#)
 - resetting the server [10](#)
 - shutting down the server [10](#)
 - tooggling the locator LED [7](#)
 - server NICs [31](#)
 - server overview [1](#)
 - shutting down the server [10](#)
 - SNMP trap configuration [52](#)
 - SSH properties [40](#)
 - storage properties [13](#)
 - system event log
 - clearing [61](#)
 - viewing [60](#)
- T**
- technical support data, exporting [63](#)
 - temperature sensors [17](#)
 - tooggling the locator LED [7](#)
- U**
- uploading a server certificate [47](#)
 - user management
 - active directory [28](#)
 - local users [25](#)
 - terminating user sessions [30](#)
 - viewing user sessions [29](#)
 - user sessions
 - terminating [30](#)
 - viewing [29](#)

V

virtual KVM [19, 20, 21](#)
virtual media [22](#)
VLAN properties [35](#)
voltage sensors [17](#)

Y

YAML [5](#)

