bullx S6000 Server Hardware Console

User's Guide

extreme computing



REFERENCE 86 A1 50FD 06

bullx S6000 Server Hardware Console

User's Guide

Hardware

August 2011

Bull Cedoc 357 avenue Patton BP 20845 49008 Angers Cedex 01 FRANCE

REFERENCE 86 A1 50FD 06 V11.07.13 The following copyright notice protects this book under Copyright laws which prohibit such actions as, but not limited to, copying, distributing, modifying, and making derivative works.

Copyright ©Bull SAS 2011 Printed in France

Trademarks and Acknowledgements

We acknowledge the right of proprietors of trademarks mentioned in this manual.

All brand names and software and hardware product names are subject to trademark and/or patent protection. Quoting of brand and product names is for information purposes only and does not represent trademark misuse.

Table of Contents

| Legal I | Informatio | on | xi | | | |
|--|-----------------------------|--|------------|--|--|--|
| | Regulator | y Declarations and Disclaimers | xi | | | |
| | Declaration | on of the Manufacturer or Importer | xi | | | |
| | Safety Compliance Statement | | | | | |
| European Community (EC) Council Directives | | | | | | |
| | | laration of Conformity | xii xii | | | |
| | | n Compliance Statement (Industry Canada) | xii | | | |
| | | npliance Notice (if applicable) | xii | | | |
| | | ormation | xiii | | | |
| | | of Safety Notices | xiii | | | |
| | Electrical | Safety | xiii | | | |
| | Laser Saf | ety Information (if applicable) | xiv | | | |
| | Data Integ | grity and Verification | xiv | | | |
| | | anagement | xiv | | | |
| | Safety Re | commendations | xiv | | | |
| Preface | e | | xvii | | | |
| Intended Readers | | | | | | |
| Highlighting | | | | | | |
| | Related Publications | | | | | |
| | | | xviii | | | |
| Chapte | | Getting to Know the Server | 1-1 | | | |
| | 1.1. | Overview | 1-2 | | | |
| | 1.2. | Components, Controls, LEDs and Ports | 1-4 | | | |
| | | 1.2.1. bullx S6030 server | 1-4 | | | |
| | | 1.2.2. bullx S6010 server | 1-8 | | | |
| Chapte | er 2. | Getting Started | 2-1 | | | |
| | 2.1. | Starting the Hardware Console | 2-2 | | | |
| | 2.2. | Hardware Console Overview | 2-4 | | | |
| | 2.3. | Stopping the Hardware Console | 2-7 | | | |
| | 2.4. | Initial Configuration | 2-8 | | | |
| | 2.5. | Installing the KiraTool Utility | 2-9 | | | |
| Chanta | | Managing Device | 2 1 | | | |
| Chapte | | Managing Power | 3-1 | | | |
| | 3.1. | Power Management Features Overview | 3-2 | | | |
| | 3.2. | Checking Power Status | 3-4 | | | |
| | 3.3. | Powering On the Server from the Console | 3-6 | | | |
| | 3.4. | Powering Off the Server from the Console | 3-8 | | | |
| | 3.5. | Forcibly Powering Off / Resetting the Server | 8-10 | | | |

| Chapter 4. | Using the Remote System Console | | | |
|------------|--|------------------------------|--|--|
| 4.1. | Setting Up the Remote System Console4.1.1.Configuring User Specific Settings4.1.2.Configuring the Keyboard and Mouse4.1.3.Sharing Local Drives | 4-2 4-3 4-6 4-8 | | |
| 4.2. | Launching the Remote System Console4.2.1.Remote System Console Overview4.2.2.Remote System Console Menus4.2.3.Remote System Console Toolbar | 4-10 4-11 4-12 4-13 | | |
| 4.3. | Virtualizing Media4.3.1.Virtualizing a Local Drive4.3.2.Virtualizing an Image File4.3.3.Virtualizing a Local Folder | 4-14 4-15 4-16 4-17 | | |
| 4.4. | Stopping the Remote System Console | 4-18 | | |
| Chapter 5. | Monitoring the Server | 5-1 | | |
| 5.1. | Initial Messaging and Alert Configuration | 5-2 | | |
| 5.2. | Checking Monitoring Sensors | | | |
| 5.3. | Checking and Clearing the System Event Log (SEL) | | | |
| 5.4. | Checking the Board and Security Messages Log | 5-7 | | |
| 5.5. | Downloading and Deleting BIOS Log | 5-8 | | |

| Chapter 6. | Configuring the Server Management Controller | | | | |
|------------|--|--|--|--|--|
| 6.1. | Configuring Platform Identification Settings | 6-2 | | | |
| 6.2. | Configuring the Managed Server Name | 6-3 | | | |
| 6.3. | Modifying Functional Profile Settings | 6-4 | | | |
| 6.4. | Configuring Network Settings for Remote Access | | | | |
| 6.5. | Modifying Internal Clock Settings | | | | |
| 6.6. | , 6 | | | | |
| 6.7. | Managing Users6.7.1.Creating a User Account6.7.2.Displaying User Account Details6.7.3.Modifying a User Account6.7.4.Disabling/Enabling User Accounts6.7.5.Forcing User Password Changes6.7.6.Deleting a User Account6.7.7.Manually Unlocking a User Account6.7.8.Modifying the Password6.7.9.Creating a Group6.7.10.Configuring Permissions6.7.11.Viewing Group Membership | 6-14 6-16 6-18 6-20 6-21 6-22 6-23 6-24 6-25 6-27 6-31 | | | |
| 6.8. | 6.7.12. Deleting a Group Configuring Security Parameters 6.8.1. Forcing HTTPS Connections 6.8.2. Getting and Installing a New SSL Certificate 6.8.3. Configuring the Logon Policy 6.8.4. Managing Authentication 6.8.5. Enabling/Disabling the LCP Power Button 6.8.6. Configuring User Account Lockout | 6-32 6-34 6-34 6-36 6-38 6-40 6-43 6-44 | | | |
| 6.9. | Configuring Alerts6.9.1.Configuring SNMP and SMTP Servers6.9.2.Configuring LAN Destinations6.9.3.Configuring Alert Policies6.9.4.Managing Predefined Event Filters6.9.5.Customizing an Event Filter | 6-47 6-47 6-49 6-52 6-54 6-57 | | | |
| Chapter 7. | Using Maintenance Features | 7-1 | | | |
| 7.1. | Getting Management Controller Information | 7-2 | | | |
| 7.2. | Getting FRU Information | 7-3 | | | |
| 7.3. | Displaying Firmware Versions | | | | |
| 7.4. | Updating Firmware | 7-5 | | | |
| 7.5. | Performing Reset Operations | | | | |
| 7.6. | Enabling/Disabling the Identification LED | | | | |
| 7.7. | Excluding/Including Processors | | | | |
| 7.8. | Excluding/Including a Server Module | 7-10 | | | |
| 7.9. | Displaying Connected Users | 7-11 | | | |
| 7.10. | Backing Up Configuration Data | | | | |
| 7.11. | Restoring Configuration Data | 7-13 | | | |

| Appendix A. | Appendix A. Troubleshooting the Server | | | |
|-------------|--|------|--|--|
| A.1. | Predefined Alert Filters Description | A-2 | | |
| A.2. | System Event Log (SEL) Messages | A-9 | | |
| | A.2.1. SEL Messages: External Environment | A-10 | | |
| | A.2.2. SEL Messages: Power System Board | A-11 | | |
| | A.2.3. SEL Messages: Sub-chassis | A-11 | | |
| | A.2.4. SEL Messages: Power Supply | A-13 | | |
| | A.2.5. SEL Messages: Power Unit | A-14 | | |
| | A.2.6. SEL Messages: ILB | A-15 | | |
| | A.2.7. SEL Messages: MTB/MXB | A-25 | | |
| | A.2.8. SEL Messages: Processor | A-28 | | |
| | A.2.9. SEL Messages: Fan Device / Cooling Unit | A-39 | | |
| | A.2.10. SEL Messages: PDB | A-41 | | |
| | A.2.11. SEL Messages: Ultra Capacitor | A-42 | | |
| | A.2.12. SEL Messages: LCP | A-49 | | |
| | A.2.13. SEL Messages: BMC | A-50 | | |
| | A.2.14. SEL Messages: Memory | A-57 | | |
| | A.2.15. Power Steps: BMC | A-58 | | |
| | A.2.16. Power Steps: SMC | A-60 | | |
| Appendix B. | Serial-Over-LAN Console | B-1 | | |
| B.1. | Introducing the SOL Console | B-2 | | |
| B.2. | Using the SOL Console with ipmitool | B-3 | | |
| B.3. | Using the SOL Console with telnet | B-5 | | |
| Glossary | | g-1 | | |
| Index | | x-1 | | |

List of Figures

| Figure 1-1. | bullx S6010 server | 1-2 | | | | |
|--------------|---|------|--|--|--|--|
| Figure 1-2. | bullx S6030 server | | | | | |
| Figure 1-3. | bullx S6000 series | 1-3 | | | | |
| Figure 1-4. | Server components - Exploded view | 1-5 | | | | |
| Figure 1-5. | erver LEDs and buttons - Front view | | | | | |
| Figure 1-6. | erver LEDs and buttons - Rear view | | | | | |
| Figure 1-7. | erver connection ports - Rear view | | | | | |
| Figure 1-8. | Server components - Exploded view | | | | | |
| Figure 1-9. | Server LEDs and buttons - Front view | 1-9 | | | | |
| Figure 1-10. | Server LEDs and buttons - Rear view | 1-10 | | | | |
| Figure 1-11. | Mono-module Server connection ports - Rear view | 1-11 | | | | |
| Figure 2-1. | Logon | 2-2 | | | | |
| Figure 2-2. | Hardware Console overview | 2-4 | | | | |
| Figure 2-3. | KiraTool Commands and Options - Windows | 2-9 | | | | |
| Figure 2-4. | KiraTool Commands and Options - Linux | 2-10 | | | | |
| Figure 3-1. | Power management features overview | 3-3 | | | | |
| Figure 3-2. | Checking power status | 3-4 | | | | |
| Figure 3-3. | Powering on the server from the console | 3-7 | | | | |
| Figure 3-4. | Powering off the server from the console | 3-8 | | | | |
| Figure 3-5. | Emergency Power Off | 3-11 | | | | |
| Figure 4-1. | Remote System Console - User Specific Settings | | | | | |
| Figure 4-2. | Remote System Console - Keyboard and Mouse Settings | | | | | |
| Figure 4-3. | Drive Redirection | 4-9 | | | | |
| Figure 4-4. | Remote Console Preview | 4-10 | | | | |
| Figure 4-5. | Remote System Console overview | 4-11 | | | | |
| Figure 4-6. | Remote System Console menus | 4-12 | | | | |
| Figure 4-7. | Remote System Console toolbar | 4-13 | | | | |
| Figure 4-8. | Virtual Media - Local Drive | 4-15 | | | | |
| Figure 4-9. | Virtual Media - Image File | 4-16 | | | | |
| Figure 4-10. | Virtual Media - Local Folder | 4-17 | | | | |
| Figure 5-1. | Sensor Status | 5-4 | | | | |
| Figure 5-2. | System Event Log | 5-6 | | | | |
| Figure 5-3. | Board & Security Messages | 5-7 | | | | |
| Figure 5-4. | BIOS Logs | 5-8 | | | | |
| Figure 6-1. | Platform Settings | 6-2 | | | | |
| Figure 6-2. | Managed Server Settings | 6-3 | | | | |
| Figure 6-3. | Functional Profiles Settings | 6-5 | | | | |
| Figure 6-4. | Network Settings - factory-default values | 6-8 | | | | |
| Figure 6-5. | Date/Time Settings - factory-default values | 6-11 | | | | |
| Figure 6-6. | Event Management Settings - factory-default values | 6-13 | | | | |
| Figure 6-7. | User Management - User Creation | | | | | |
| Figure 6-8. | User Management - Account Details | | | | | |

| Figure 6-9. | User Account Deletion | | | | | |
|--------------|---|------|--|--|--|--|
| Figure 6-10. | User Management - Locked-out user | | | | | |
| Figure 6-11. | Password Management | | | | | |
| Figure 6-12. | roup Management - Group Creation | | | | | |
| Figure 6-13. | roup Permissions | | | | | |
| Figure 6-14. | Group Management | | | | | |
| Figure 6-15. | Group Management - Group Deletion | 6-33 | | | | |
| Figure 6-16. | Encryption Management - factory-default values | 6-36 | | | | |
| Figure 6-17. | SSL Certificate Management | 6-38 | | | | |
| Figure 6-18. | User Logon Policy Management - factory-default values | 6-39 | | | | |
| Figure 6-19. | Authentication Settings - factory-default values | 6-43 | | | | |
| Figure 6-20. | Power Button Lockout Management | 6-44 | | | | |
| Figure 6-21. | User Lockout Management - factory-default values | 6-45 | | | | |
| Figure 6-22. | Alert General Settings | 6-48 | | | | |
| Figure 6-23. | LAN Destination Settings | 6-50 | | | | |
| Figure 6-24. | Alert Settings: LAN Destination Edit | 6-51 | | | | |
| Figure 6-25. | Alert policy settings | | | | | |
| Figure 6-26. | Alert policy settings - Modification | | | | | |
| Figure 6-27. | Managing predefined filters | | | | | |
| Figure 6-28. | Modifying predefined filters | | | | | |
| Figure 6-29. | Customizing an event filter | | | | | |
| Figure 6-30. | Configurable Filters - Modification | | | | | |
| Figure 7-1. | Management Controller Information | | | | | |
| Figure 7-2. | FRU Information | | | | | |
| Figure 7-3. | Viewing Firmware Information - Server Example | 7-4 | | | | |
| Figure 7-4. | Reset Operations | 7-6 | | | | |
| Figure 7-5. | Identification LED Management | 7-7 | | | | |
| Figure 7-6. | Hardware Exclusions | 7-8 | | | | |
| Figure 7-7. | Excluding/Including Modules | 7-10 | | | | |
| Figure 7-8. | Connected Users Information | | | | | |
| Figure B-1. | SOL Console - Launching with ipmitool | | | | | |
| Figure B-2. | SOL Console - Closing with ipmitool | | | | | |
| Figure B-3. | Telnet session | | | | | |
| Figure B-4. | Telnet commands | | | | | |
| Figure B-5. | SOL Console - Launching with telnet | | | | | |
| Figure B-6. | SOL Console - Closing with telnet | | | | | |

List of Tables

| Table 1-1. | Server product data | 1-3 |
|------------|--|------|
| Table 2-1. | Interface features and permissions | 2-6 |
| Table 3-1. | Power information - potential last restart reasons | 3-5 |
| Table 6-1. | Hardware Console: Non-configurable permissions | 6-29 |
| Table 6-2. | Hardware Console: Configurable permissions | 6-31 |
| Table 6-3. | IPMI: Out-of-Band privileges | 6-31 |
| Table A-1. | Predefined Event Filters | A-8 |

Legal Information

Regulatory Declarations and Disclaimers

Declaration of the Manufacturer or Importer

We hereby certify that this product is in compliance with:

- European Union EMC Directive 2004/108/EC, using standards EN55022 (Class A) and EN55024 and Low Voltage Directive 2006/95/EC, using standard EN60950
- International Directive IEC 60297 and US ANSI Directive EIA-310-E

Safety Compliance Statement

- UL 60950 (USA)
- IEC 60950 (International)
- CSA 60950 (Canada)

European Community (EC) Council Directives

This product is in conformity with the protection requirements of the following EC Council Directives:

Electromagnetic Compatibility

• 2004/108/EC

Low Voltage

• 2006/95/EC

EC Conformity

• 93/68/EEC

Telecommunications Terminal Equipment

• 1999/5/EC

Neither the provider nor the manufacturer can accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product.

Compliance with these directives requires:

- An EC declaration of conformity from the manufacturer
- An EC label on the product
- Technical documentation

Mechanical Structures

- IEC 60297
- EIA-310-E

FCC Declaration of Conformity

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Neither the provider nor the manufacturer are responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

Pursuant to Part 15.21 of the FCC Rules, any changes or modifications to this equipment not expressly approved by the manufacturer may cause harmful interference and void the FCC authorization to operate this equipment. An FCC regulatory label is affixed to the equipment.

Canadian Compliance Statement (Industry Canada)

This Class A digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This product is in conformity with the protection requirements of the following standards:

- ICES-003
- NMB-003

VCCI Statement

This equipment complies with the VCCI V-3/ 2008-4 requirements.

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用する と電波妨害を引き起こすことがあります。この場合には使用者が適切な対策 を講ずるよう要求されることがあります。 VCCI-A

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions. A VCCI regulatory label is affixed to the equipment.

Laser Compliance Notice (if applicable)

This product that uses laser technology complies with Class 1 laser requirements.

A CLASS 1 LASER PRODUCT label is affixed to the laser device.

Class 1 Laser Product Luokan 1 Laserlaite Klasse 1 Laser Apparat Laser Klasse 1

Safety Information

Definition of Safety Notices



A Danger notice indicates the presence of a hazard that has the potential of causing death or serious personal injury.

A *Caution* notice indicates the presence of a hazard that has the potential of causing moderate or minor personal injury.

A *Warning* notice indicates an action that could cause damage to a program, device, system, or data.

Electrical Safety

The following safety instructions shall be observed when connecting or disconnecting devices to the system.



DANGER

The Customer is responsible for ensuring that the AC electricity supply is compliant with national and local recommendations, regulations, standards and codes of practice. An incorrectly wired and grounded electrical outlet may place hazardous voltage on metal parts of the system or the devices that attach to the system and result in an electrical shock. It is mandatory to remove power cables from electrical outlets before relocating the system.



CAUTION

This unit has more than one power supply cable. Follow procedures for removal of power from the system when directed.

Laser Safety Information (if applicable)

The optical drive in this system unit is classified as a Class 1 level Laser product. The optical drive has a label that identifies its classification.

The optical drive in this system unit is certified in the U.S. to conform to the requirements of the Department of Health and Human Services 21 Code of Federal Regulations (DHHS 21 CFR) Subchapter J for Class 1 laser products. Elsewhere, the drive is certified to conform to the requirements of the International Electrotechnical Commission (IEC) 60825-1: 2001 and CENELEC EN 60825-1: 1994 for Class 1 laser products.

CAUTION

Invisible laser radiation when open. Do not stare into beam or view directly with optical instruments.

Class 1 Laser products are not considered to be hazardous. The optical drive contains internally a Class 3B gallium-arsenide laser that is nominally 30 milliwatts at 830 nanometers. The design incorporates a combination of enclosures, electronics, and redundant interlocks such that there is no exposure to laser radiation above a Class 1 level during normal operation, user maintenance, or servicing conditions.

Data Integrity and Verification

WARNING

Products are designed to reduce the risk of undetected data corruption or loss. However, if unplanned outages or system failures occur, users are strongly advised to check the accuracy of the operations performed and the data saved or transmitted by the system at the time of outage or failure.

Waste Management

This product has been built to comply with the Restriction of Certain Hazardous Substances (RoHS) Directive 2002/95/EC.

This product has been built to comply with the Waste Electrical and Electronic (WEEE) Directive 2002/96/EC.

Safety Recommendations

Danger and Warning Notices



DANGER

Only hot-pluggable components can be serviced (added, removed, replaced) without powering down the equipment.

If the component is NOT hot-swappable, the equipment must be powered down PRIOR to servicing and the AC power cables must be disconnected from the electrical outlet.

DANGER

Failure to disconnect AC power cables before servicing the equipment may result in personal injury and damage to equipment.

It is mandatory to remove AC power cables from electrical outlets before relocating cabinets and systems.



Hazardous voltage, current, and energy levels are present inside the power supply. Hazardous electrical conditions may be present on power, telephone, and communication cables.

Energy hazard:

Remove all jewelry before servicing.



DANGER

The Ultracapacitor may retain a charge after power is removed. This charge may result in personal injury and damage to equipment.

It is mandatory not to touch any parts until the Ultracapacitor has fully discharged.

A faulty Ultracapacitor may release electrolyte fluid.

It is mandatory to wear protection gloves and protection glasses to avoid contact with skin and eyes when handling the Ultracapacitor.



DANGER

The onboard battery should be replaced regularly. It must be replaced with the same or an equivalent type recommended by the manufacturer. There is a danger of explosion if another type is used. Dispose of used batteries according to the manufacturer's instructions.

DANGER Basic electrical safety precautions should be followed to protect yourself from harm and the

drawer from damage. If an electrical accident occurs, shutdown the power by removing the power cord from the

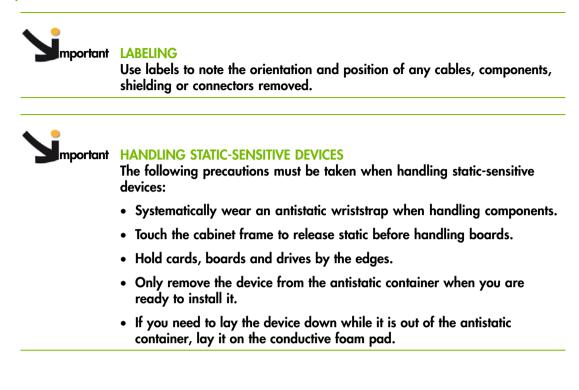
server.



WARNING

Optimum cooling and airflow is ensured when cabinets and systems are closed. Once the maintenance / service intervention has been completed, all cabinet and system covers and doors should be refitted and closed rapidly.

Important Notices



Preface

This guide explains how to use the Hardware Console to manage your server.

Note The Bull Support Web site may be consulted for product information, documentation, updates and service offers: http://support.bull.com

Intended Readers

This guide is intended for use by Bull System Administrators and Operators.

Highlighting

The following highlighting conventions are used in this guide:

| Bold | Identifies the following: |
|-----------|--|
| | • Interface objects such as menu names, labels, buttons and icons. |
| | File, directory and path names. |
| | Keywords to which particular attention must be paid. |
| Italics | Identifies references such as manuals or URLs. |
| monospace | Identifies portions of program codes, command lines, or messages displayed in command windows. |
| < > | Identifies parameters to be supplied by the user. |
| | Identifies the FRONT of a component. |
| | Identifies the REAR of a component. |

Related Publications

This list is not exhaustive. Useful documentation is supplied on the Resource & Documentation CD(s) delivered with your system. You are strongly advised to refer carefully to this documentation before proceeding to configure, use, maintain, or update your system.

- Site Preparation Guide, 86 A1 40FA explains how to prepare a Data Processing Center for Bull Systems, in compliance with the standards in force. This guide is intended for use by all personnel and trade representatives involved in the site preparation process.
- *bullx S6030 Installation Guide*, 86 A1 26FE explains how to install and start the server for the first time. This guide is intended for use by qualified support personnel.
- bullx S6030 Service Guide, 86 A7 85FB explains how to service the server. This guide is intended for use by qualified support personnel.
- *bullx S6010 Installation Guide*, 86 A1 86FB explains how to install and start the server for the first time. This guide is intended for use by qualified support personnel.
- *bullx S6010 Service Guide*, 86 A7 87FB explains how to service the server. This guide is intended for use by qualified support personnel.
- bullx Cabling Guide, 86 A1 94FE explains how to cable a bullx multi-modules configuration. This guide is intended for use by server administrators, operators and qualified support personnel.
- *iCare Console User's Guide,* 86 A1 71FA explains how to use the console to monitor and maintain Bull Systems. This guide is intended for use by Bull System Administrators and Operators and qualified support personnel.
- Resource and Documentation CD contains the tools and documentation required to configure, operate and maintain the equipment.

Chapter 1. Getting to Know the Server

This chapter gives an overview of server features and components. It includes the following topics:

- Overview, on page 1-2
- Components, Controls, LEDs and Ports , on page 1-4

1.1. Overview

Bull servers for business and scientific applications are based upon the MESCA architecture (Multiple Environments on a SCalable Architecture), leveraging the latest generation of Intel Xeon processors, Intel QPI protocol, Bull BCS technology and Infiniband QDR interconnect. Servers are designed to attain petascale performance while optimizing power consumption and heat dissipation. Two types of systems are available, according to your needs:

bullx S6010 server

The bullx S6010 server high-density compute node provides up to 4 processor sockets, 32 memory DIMMs, and 1 internal hard disk drive per 1.5U drawer. Its unique "L" design allows 2 modules to be slotted together to offer up to 8 processor sockets, 64 memory DIMMs and 2 internal hard disk drives per 3U assembly.

Up to 4 bullx S6010 servers can be interconnected via the BCS (Bull Coherence Switch) to form a 6U SMP compute node providing up to 16 processor sockets and 128 memory DIMMs in a 6U assembly.





bullx S6030 server

The bullx S6030 server compute and/or service node provides up to 4 processor sockets, 32 memory DIMMs, 6 PCI-e slots, and 8 internal hard disk drives per 3U drawer. Optionally, a DVD drive can be installed in a disk drive slot.

Up to 4 bullx S6030 servers can be interconnected via the BCS (Bull Coherence Switch) to form a 12U SMP compute and/or service node providing up to 16 processor sockets, 128 memory DIMMs and 24 PCI-e slots. The addition of LSI boards provides 8 up to 32 internal disks.



Figure 1-2. bullx S6030 server

Servers are rack-mounted in Bull cabinets for optimized deployment time and enhanced reliability.



Figure 1-3. bullx S6000 series

For future reference, you are advised to record the following data indicated on the labels affixed to the server drawer:

| System | Data |
|----------------------|------|
| Product Name | |
| Product Code | |
| Product Number | |
| System Serial Number | |

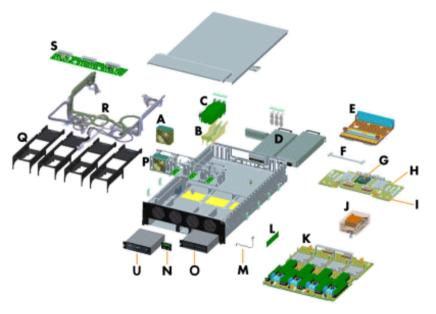
Table 1-1. Server product data

1.2. Components, Controls, LEDs and Ports

1.2.1. bullx \$6030 server

Components (Exploded view)

The following diagram shows an exploded view of server components:



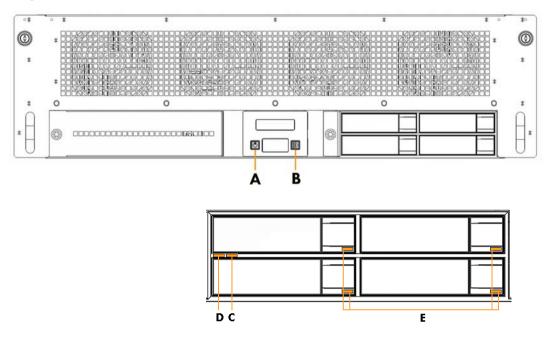
| Mark | Description | Quantity |
|---------------------------------------|--|----------|
| A | Fan Unit | 8 |
| В | PCle Separator | 2 to 4 |
| С | PCle Card | Up to 6 |
| D | Power Supply Unit | 1 or 2 |
| E | Dummy CSI Interconnect Board (DSIB) or CSI Interconnect Board (SIB) | 1 |
| F | Prepositioner | 1 |
| G | Embedded Management Controller | 1 |
| Н | I/O Legacy Board (ILB) | 1 |
| I | ICH battery | 1 |
| J Nehalem Assembly Processor Assembly | | Up to 4 |
| K Memory Xeon Board (MXB) | | 1 |
| L Memory Module | | Up to 32 |
| м | Anti-Intrusion Switch | 1 |
| N | Local Control Panel (LCP) | 1 |
| 0 | Hard Disk Box (HDX) | 1 or 2 |
| Р | Fan Box | 1 |
| Q | Air Duct | 4 |
| R | Internal Cable Kit | 1 |
| S | Power Distribution Board Unit (PDBU) | 1 |

| Mark | Description | Quantity |
|-----------------|------------------------|----------|
| Not illustrated | Ultra Capacitor | 1 |
| U | U DVD Drive (Optional) | |

Figure 1-4. Server components - Exploded view

Controls and LEDs (Front view)

The server is equipped with LEDs and buttons on both the front and rear. The following diagram shows the LEDs and buttons on the front of the server.

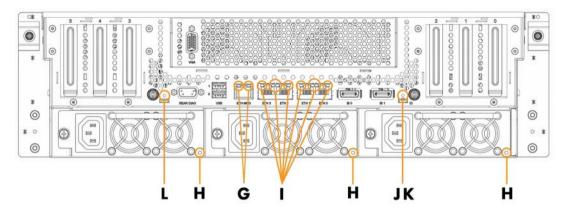


| Mark | LED/Button | Color | Description |
|------|-------------------------|----------------|---|
| А | Power LED/Button | Blinking Green | Server power on stand-by. |
| | | Solid Green | Server powered up. |
| В | ID LED/Button | Blinking Blue | ID button pressed or activated from the Server Hardware Console; simultaneously lights the BLUE ID LED (G) on the rear of the server. |
| С | Disk Fan Failure LED | Blinking Amber | Disk Fan failure. |
| D | Disk Overheat LED | Blinking Amber | Disk overheat failure. |
| E | Disk Activity LED | Blinking Green | Disk active. |

Figure 1-5. Server LEDs and buttons - Front view

Controls and LEDs (Rear view)

The server is equipped with LEDs and buttons on both the front and rear. The following diagram shows the LEDs and buttons on the rear of the server.

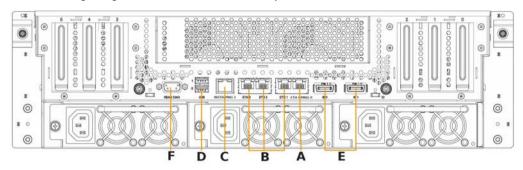


| Mark | LED/Button | Color | Description |
|------|------------------------------|----------------|---|
| G | | Solid Green | Link active. |
| | Left LED | Blinking Green | Link inactive. |
| G | Management Port | Solid Orange | 100 MBit/s. |
| | Right LED | Off | 10 MBit/s. |
| Н | Power Supply Unit | Solid Green | Power supply unit powered up. |
| | LED | Blinking Green | Power supply unit on stand-by. |
| | | Blinking Amber | Power supply unit fault. |
| I | Gbit Port Left LED | Green | 1 GBit/s. |
| | | Orange | 100 MBit/s. |
| | | Off | 10 MBit/s. |
| I | Gbit Port Right LED | Solid Green | Link established. |
| | | Blinking Green | Link active. |
| J | Reset Button | N/A | Resets the Embedded Management Controller. |
| К | ID LED | Blinking Blue | ID button (B) on the front of the server pressed or activated from the Server Hardware Console. |
| L | Return to Defaults Button | N/A | Returns the Embedded Management Controller settings to default values. |

Figure 1-6. Server LEDs and buttons - Rear view

Connection Ports (Rear view)

The following diagram shows the connection ports on the rear of the server.



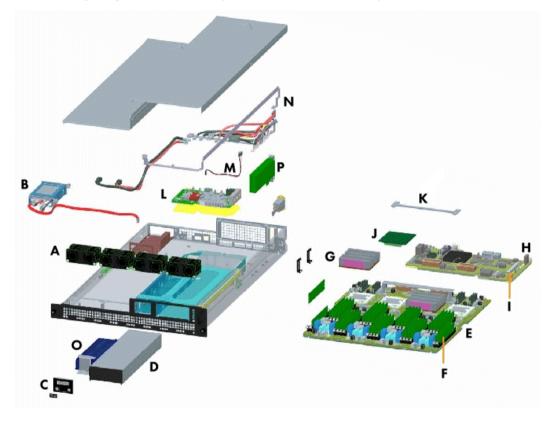
| Mark | Description |
|------|--|
| A | ETHO/MNG0 (RJ45) port: Shared Management / Host network port, or Host network port only if INTER/MNG1 (C) is used for the Management network |
| В | ETH1, ETH2, ETH3 (RJ45) ports: Enterprise network port |
| С | INTER/MNG1 (RJ45): Dedicated Management network / module interconnexion port |
| D | USB key ports |
| E | INFINIBAND ports: Infiniband network port (Optional) |
| F | VGA port |

Figure 1-7. Server connection ports - Rear view

1.2.2. bullx \$6010 server

Components (Exploded view)

The following diagram shows an exploded view of server components:

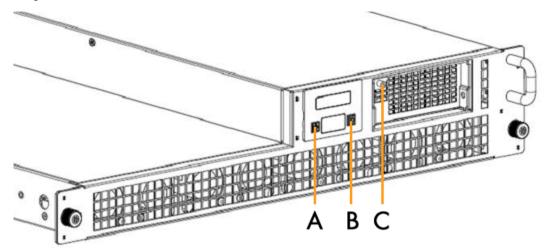


| Label | Description | Quantity |
|-------|---|----------|
| А | Cooling Unit | 4 |
| В | Hard Disk Drive (HDD) | 1 |
| С | Local Control Panel (LCP) | 1 |
| D | Power Supply Unit | 1 |
| E | Memory Xeon Board (MXB) | 1 |
| F | Memory Module | Up to 32 |
| G | Nehalem Assembly Processor | Up to 4 |
| Н | I/O Legacy Board (ILBL) | 1 |
| 1 | ICH battery | 1 |
| J | Dummy CSI Interconnect Legacy Board (DSIBL) | 1 |
| К | Prepositioner | 1 |
| L | Power Distribution Board Unit (PDBU) | 1 |
| Μ | Anti-Intrusion Switch | 1 |
| N | Internal Cable Kit | 1 |
| 0 | Ultra Capacitor | 1 |
| Р | PCle Card | 1 |

Figure 1-8. Server components - Exploded view

Controls and LEDs (Front view)

The server is equipped with LEDs and buttons on both the front and rear. The following diagram shows the LEDs and buttons on the front of the server.

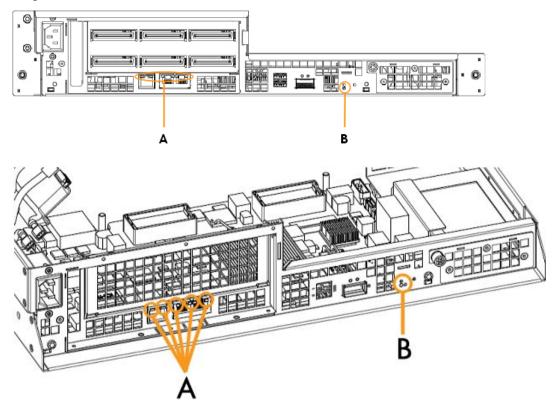


| | Label Name | Description |
|---|---------------------------|---|
| А | Power LED/Button | Flashing Green: server power on stand-by. Still Green: server powered up. |
| В | ID LED/Button | Flashing Blue: ID button pressed or activated from the Server Hardware Console. Simultaneous lights the BLUE ID LED on the rear of the server. |
| С | Power Supply Unit Leds | Still Green: power supply unit powered up. Flashing Green: power supply unit on stand-by. Flashing Amber: power supply unit fault. |

Figure 1-9. Server LEDs and buttons - Front view

Control and LEDs (Rear view)

The server is equipped with LEDs and buttons on both the front and rear. The following diagram shows the LEDs and buttons on the rear of the server.



| Label | Name | Description |
|-------|------------------------|---|
| | | Indicates network activity status. There is one management port and 2 Gbit ports. |
| | | For the management port: Left LED: Still Green: link active. Flashing Green: link inactive. |
| A | Ethernet Activity LEDs | Right LED: Still Orange: rate 100MB/s Extinguished: rate 10 MB/s |
| | | For the Gbit ports: (to the right of each port) Left LED: Green: rate 1GB/s Orange: 100 MB/s Extinguished: 10 MB/s |
| | | Right LED: Still Green: link established. Flashing Green: link active. |
| В | ID LED | Flashing Blue |

Figure 1-10. Server LEDs and buttons - Rear view

Connection ports (Rear view)

The following diagram shows the connection ports on the rear of the server.

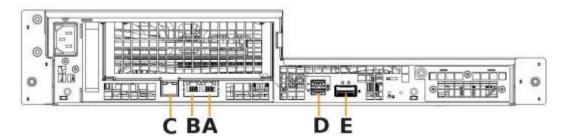


Figure 1-11. Mono-module Server connection ports - Rear view

| Mark | Description |
|------|--|
| A | ETHO/MNGO (RJ45) port: Shared Management / Host network port, or Host network port only if INTER/MNG1 (C) is used for the Management network |
| В | ETH1 (RJ45) port: Enterprise network port |
| С | INTER/MNG1 (RJ45): Dedicated Management network port, or server interconnection port (multi-module models) |
| D | USB ports |
| E | INFINIBAND port: Infiniband network port |

Chapter 2. Getting Started

This chapter describes Hardware Console features and explains how to start and stop the console from a Web browser. It includes the following topics:

- Starting the Hardware Console, on page 2-2
- Hardware Console Overview, on page 2-4
- Stopping the Hardware Console, on page 2-7
- Initial Configuration, on page 2-8
- Installing the KiraTool Utility, on page 2-9

2.1. Starting the Hardware Console

The hardware console is launched from a Web browser using a standard or secure IP address or host name, according to settings.

Prerequisites

The server is connected to the site power supply and to the enterprise LAN.

Procedure

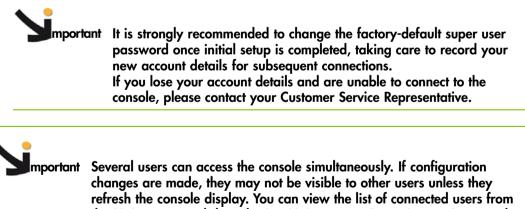
1. Launch your web browser and enter the standard or secure IP address or host name, according to settings. The authentication page opens.

| Server Hardware Console | |
|-------------------------|--|
| Password | |
| Log On | |
| | |
| | |
| | |

| Hardware Console | | |
|---|--|--|
| Username Factory-default name: super | | |
| Password Factory-default password: pass | | |

Figure 2-1. Logon

2. Complete the Username and Password fields and click Log On. Once you are authenticated, the System Control tab opens.



refresh the console display. You can view the list of connected users from the Maintenance tab by selecting Maintenance Operations > Connected Users.

What To Do if an Incident Occurs?

If you cannot connect to the console or if the web pages are displayed incorrectly, one of the following problems may be the cause:

- Network failure
- Incorrect network settings
- Incorrect browser settings (proxy configuration)

2.2. Hardware Console Overview

The Hardware Console is a web-based administration application embedded on the management controller. You can use the Hardware Console to remotely operate, monitor and maintain hardware and to configure the embedded management controller. The Hardware Console can be accessed via the enterprise LAN using a Microsoft Internet Explorer or Mozilla Firefox browser.

mportant Several users can access the console simultaneously. If configuration changes are made, they may not be visible to other users unless they refresh the console display. You can view the list of connected users from the Maintenance tab by selecting Maintenance Operations > Connected Users.

| | | | | | Lo |
|-----------------------------------|--|----------------|--|---------------|-------------|
| | User: super | System Control | Monitoring | Configuration | Maintenance |
| ower | Power Management | | | | |
| Power Management | Power Information | | | | |
| emote Console Preview | Power State: On | - | | | |
| aunch | Last Restart Reason: chassis power control of | ommand | Refresh | | |
| irtual Media Drive Redirection | - Standard Power Operations | | | | |
| Drive receivection | Power On with OS Boot | | Power On | | |
| | Power Off with OS Shutdown Request | | Power Off | | |
| | Force Power Off without OS Shutdown Reques Hardware Reset with OS Reboot Pulse Diagnostic Interrupt. Used to cause the Dump (OS dependent) Power On using Back-Up BIOS | | Force Power C Hard Reset Diagnostic Du Power On (Back-U | t mp | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| Console Overview | | |
|--------------------|--|--|
| A: Navigation tree | Provides access to console features. Note that displayed features differ according to the tab selected. | |
| B: Work pane | The work pane displays the commands and information associated with the item selected in the navigation tree. | |
| C: Tabs | Four tabs allow access to four sets of features accessible from the associated navigation trees: System Control, Monitoring, Configuration and Maintenance. | |

Figure 2-2. Hardware Console overview

Console Interface Features

The following table lists the features available from the interface and associated permissions.

| Tab | 0 | Node | Feature | ce and associated permissions. Permission |
|----------------|-------------------------------|-------------------------|---|---|
| | | Power | Power Information | None |
| | Power Management | Power | Standard Power Operations | Power Control |
| System Control | Managemen | Power | Emergency Power Operations | Power Control |
| 1 | Remote | Preview | Preview | Remote Control Access |
| 1 | Console | Launch | - | Remote Control Access |
| l | Virtual Media | Drive Redirection | Drive Redirection | Virtual Media Upload |
| | | Sensor Status | Viewing and Refreshing | None |
| Monitoring | System Health | System Event Log | Viewing and Refreshing | |
| Monnoring | | , , | Clearing | Alert Settings & Clear SEL |
| | | Messages | Viewing and Clearing | Log View |
| l | | Platform | Platform Settings | Network Settings |
| l | Global Settings | Managed Server | Managed Server Settings | Network Settings |
| | | Functional Profiles | Functional Profile Settings | Network Settings |
| | BMC Settings | Network | Network Settings | Network Settings SSH/Telnet Access (necessary to use options available in the Network Settings page) |
| 1 | Divic beilings | Date-Time | Date/Time Settings | Date/Time Settings |
| | | Messages | Event Management Settings | Log Settings Network Settings |
| l | DMC II | Users | User Management | Lissa/Casura Managamant |
| l | BMC User Management | Groups | Group Management | User/Group Management |
| l | Mullugemenn | Password | Password Management | Change Password |
| 1 | | Encryption | Encryption Management | Security Settings |
| | | SSL Certificate | SSL Certificate Management | SSL Certificate Management |
| | | User Logon Policy | User Logon Policy Management | Security Settings |
| | Security | Authentication | Authentication Management | Authentication Settings |
| Configuration | | Power Button Lockout | Power Button Lockout Management | Security Settings |
| | | User Lockout | User Lockout Management | |
| | | | User Specific RC Settings Reset Keyboard/Mouse (USB) Reset USB Reset Video Engine | Remote Console Access |
| | | | Transmission Encoding | RC Settings (Encoding) |
| | Remote Console Settings | User Specific | Miscellaneous RC Settings | RC Settings (Monitor Mode) RC Settings (Exclusive Access) |
| 1 | | | Mouse Hotkey Remote Console Button Key | RC Settings (Hotkeys) |
| | | | Key | |
| | | Keyboard/ Mouse | Keyboard/Mouse Settings | RC Keyboard/Mouse Settings |

| Tab | Tre | e Node | Feature | Permission |
|-------------|--------------------|--------------------------|--|----------------------------|
| | Alert Settings | Policies | Policy Settings | Alert Settings & Clear SEL |
| | Aleri Sellings | LAN Destinations | LAN Destination Settings | Aleri Sellings & Clear SEL |
| | | General | General Settings | |
| | Hardware | Management Controller | Management Controller Information | |
| | Information | FRU | FRU Information | None |
| | | Firmware Version | Firmware Information | |
| | Firmware Update | Listed firmware | Firmware Update | Firmware Update |
| | | | Reset Management Controller | Maintenance/Board Reset |
| Maintenance | Maintenance | Unit Reset | Reset Keyboard/Mouse (USB) Reset USB Reset Video Engine | Remote Console Access |
| | Operations | Identification LED | ID LED Management | Alert Settings & Clear SEL |
| | | Hardware Exclusion | Hardware Exclusions | Maintenance/Board Reset |
| | | Connected Users | Connected Users Information | None |

Table 2-1. Interface features and permissions

2.3. Stopping the Hardware Console

You can stop the console at any time by clicking the Logout link () in the upper-right corner of the console.

You can stop the console at any time by clicking the Logout button.

2.4. Initial Configuration

When the server is first delivered, you will need to perform a few basic configuration tasks to ensure correct operation and identification by management software. These configuration tasks are explained in detail in Chapter 6, Configuring the Server Management Controller, and are listed below by order of priority:

- Configuring Network Settings for Remote Access, on page 6-6
- Configuring the Managed Server Name, on page 6-3
- Configuring Platform Identification Settings, on page 6-2
- Modifying Internal Clock Settings, on page 6-10
- Setting Up the Remote System Console, on page 4-2

Note The other configuration tasks can be performed when required.



mportant If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for installation instructions.

2.5. Installing the KiraTool Utility

KiraTool allowing you to backup and restore your configuration data is available on the *Resource and Documentation CD*.

You are advised to install this utility so that you can back up and restore your configuration data.

Note For updated information concerning *KiraTool*, refer to the associated documentation available on the *Resource and Documentation CD*.

Windows Version

- 1. Locate the *KiraTool* self-extracting executable file (for example, KiraTool.exe) on the *Resource and Documentation CD*.
- 2. Double-click the file with your left mouse-button and follow the instructions on the screen.
- 3. At the end of the procedure, select FINISH and a KiraTool icon will automatically appear on your desktop.
- 4. To use the KiraTool utility, click the icon to open a standard Windows Command Line box in the correct directory.

The following commands and options are available:

| 🔏 KiraTool Environment | - 🗆 × |
|--|-------|
| Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp. | - |
| C:\Program Files\KiraTool>kiratool No command provided! Usage: kiratool [options] command [parameters] | |
| Possible options are: | |
| -a | 5 |
| Possible commands are: | |
| info Show information about the BMC ver Show program version and information reset Reset the device fw Firmware operations cfg Backup or restore device configuration serial Serial number operations defaults Reset device to factory settings ip Read or set IP address gw Read or set subnet mask mac Read or set subnet mask ipsrc Get or specify IP source configuration adnin Show admin name or set name and password raw Execute some self tests | |
| C:\Program Files\KiraTool> | |
| | - |

Figure 2-3. KiraTool Commands and Options - Windows

Linux Version

- 1. Locate the KiraTool executable file (for example KiraTool) on the *Resource and Documentation CD*.
- 2. Copy the executable file to a directory in your \$PATH environment, for example /usr/local/bin. As such \$PATH system directories are protected, you must log on as root:

linux # cp kiratool /usr/local/bin linux # chmod 755 /usr/bin/local/kiratool

3. Load the sg kernel module (required to run the KiraTool utility):

modprobe sg

4. Start the KiraTool utility by invoking the executable file. The following commands and options are available:



Figure 2-4. KiraTool Commands and Options - Linux

Chapter 3. Managing Power

This chapter explains how to use server power controls. It includes the following topics:

- Power Management Features Overview, on page 3-2
- Checking Power Status, on page 3-4
- Powering On the Server from the Console, on page 3-6
- Powering Off the Server from the Console, on page 3-8
- Forcibly Powering Off / Resetting the Server, on page 3-10

3.1. Power Management Features Overview

The **Power Management** page allows you to check system power status, perform standard power on/off sequences, and forcibly power off and/or retrieve the system after a crash or in the event of an emergency.

Power management options are described in Figure 3-1 below.

Procedure

• From the System Control tab, click Power > Power Management to open the Power Management page.

| | | - €Logout |
|-----------------------------------|---|------------------|
| | User : super System Control Monitoring Configuration Maint | tenance |
| ∇Power Power Management | Power Management | ^ |
| ⊳Remote Console | Power Information Power State: On | |
| ⊳Virtual Media | Last Restart Reason: chassis power control command Refresh | |
| | Standard Power Operations Power On with OS Boot Power Off with OS Shutdown Request Power Off | |
| | Emergency or Unresponsive System Power Operations The following actions do not initiate a clean shut-down of the Operating System. | |
| | Force Power Off without OS Shutdown Request Force Power Off | |
| | Force Power Off without OS Shutdown Request & Power On Force Power Cycle | = |
| | Hardware Reset with OS Reboot Hard Reset | |
| | Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump (OS dependent) | |
| | Power On using Back-Up BIOS Power On (Back-Up BIOS) | |
| | | • |

The Power Management page is divided into three areas:

- Power Information used to check system power status.
- Standard Power Operations used to perform routine power on/off sequences.
- Emergency or Unresponsive System Power Operations used to perform power on/off sequences after a system crash or in the event of an emergency.

| | Power Information |
|-----------------------------------|--|
| Power State | 2 possible values: • On |
| | • Off |
| Last Restart Reason | Several possible values explaining which action last caused a restart, as detailed in Table 3-1 below. |
| Refresh button | Allows you to update displayed data. |
| | Standard Power Operations |
| | Accessible only when the system is powered off. |
| Power On button | Launches the power up sequence. During this sequence, hardware is powered up to the main power mode and the Operating System is booted. Note: If an error occurs during this sequence, the system is automatically powered down to standby. |
| | Accessible only when the system is powered on. |
| Power Off button | Requests the Operating System to perform a graceful power down. During this sequence the Operating System saves data, closes open applications and shuts down. Note: The Operating System must be configured to accept the power off request. |
| Emerger | ncy or Unresponsive System Power Operations |
| | y be used if the Operating System is unable to respond to a er off request. These sequences may result in data loss and file |
| Force Power Off button | Performs a power down sequence independently of the Operating System. |
| Force Power Cycle button | Performs a power down sequence independently of the Operating System and automatically re-launches the powering up sequence. |
| Hard Reset button | Performs a power cycle (power off / power on) sequence independently of the Operating System and is used as a last resort to forcibly retrieve the system when it freezes. All cache information is erased. |
| Diagnostic Dump button | Triggers a Pulse Diagnostic Interrupt for error debugging and diagnosis. The Operating System dumps the contents of memory to disk and the system is reset. |
| Power On (Back-Up BIOS) button | Performs a power up sequence using a back-up version of the BIOS. This feature is used to restart the server when BIOS integrity is no longer ensured. |

Figure 3-1. Power management features overview

3.2. Checking Power Status

System power status can be checked at all times from the Power Management page Power Information box.

mportant The Power status display is not updated dynamically, therefore displayed status may not reflect actual status. You can update power status by using the Refresh button.

Procedure

• From the System Control tab, click Power > Power Management to open the Power Management page.

| | User:super | System Control | Monitoring | Configuration | Maintenance |
|-------------------------------|---|----------------|--------------------|---------------|-------------|
| er | Power Management | | | | |
| wer Management ote Console | Power Information | | | | |
| | Power State: On | | | | |
| ial Media | Last Restart Reason: chassis power control command | | Refresh | | |
| | Standard Power Operations | | | | |
| | Power On with OS Boot | | Power On | | |
| | Power Off with OS Shutdown Request | | Power Off | | |
| | Emergency or Unresponsive System Power Op | erations | | | |
| | The following actions do not initiate | | of the Operating S | System. | |
| | Force Power Off without OS Shutdown Request | | Force Power Of | f | |
| | Force Power Off without OS Shutdown Request & Pow | er On | Force Power Cyc | le | |
| | Hardware Reset with OS Reboot | | Hard Reset | | |
| | Pulse Diagnostic Interrupt. Used to cause the OS to do Dump (OS dependent) | a Diagnostic | Diagnostic Dum | p | |
| | Power On using Back-Up BIOS | P | ower On (Back-Up | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | 2 |
| | Power Inform | | | | |

| | Power Information |
|---|--|
| Note: For details on other power man | agement features, see Figure 3-1, on page 3-3. |
| | 2 possible values: |
| Power State | • On |
| | • Off |
| Last Restart Reason | Several possible values explaining which action last caused a restart, as detailed in Table 3-1 below. |
| Refresh button | Allows you to update displayed data. |

Figure 3-2. Checking power status

The following table details the values that may potentially appear in the Last Restart Reason field of the Power Information box.

| Last Restart Reason | Explanation |
|--|---|
| Chassis power control command | The server was restarted from the Hardware Console or by IPMITOOL via the LAN. |
| Reset via push-button | The server was reset with the server push-button. |
| Power-up via push-button | The server was restarted with the server push-button. |
| Watchdog expired | The server was automatically restarted when the IPMI watchdog time expired. |
| Reset via PEF (Platform Event Filtering) | The server was reset further to the transmission of an event configured to automatically perform the reset action. |
| Power-cycle via PEF | The server was power-cycled further to the transmission of an event configured to automatically perform the power-cycle action. |
| Power-up due to always-restore power policy | The server was automatically restarted when AC power was applied or returned after a power cut, in compliance with system power management settings. |
| Power-up due to restore-previous power policy | The server was automatically restarted when AC power was applied or returned after a power cut, in compliance with system power management settings. |
| OEM | The server was automatically restarted further to the reception of a Wake-on-LAN signal. |

Table 3-1. Power information - potential last restart reasons

3.3. Powering On the Server from the Console

The server can be powered on from the Power Management page Standard Power Operations box.

mportant The Power status display is not updated dynamically, therefore displayed status may not reflect actual status and the Power On button may not be enabled although the system is powered off. You can update power status by using the Refresh button.

Prerequisites

You have Power Control permission

The Power On button is enabled

Procedure

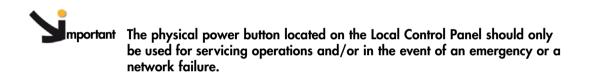
1. From the System Control tab, click Power > Power Management to open the Power Management page.

| | | anagement | | • | | |
|-----------|-----------|--|------------|----------------------|--------|--|
| | - Power M | anagement | | | | |
| e Console | | ver Information | | | | |
| Media | | wer State: Off t Restart Reason: chassis power control command | | efresh | | |
| meura | Las | a Restant Reason: chassis power control command | IN | 61631 | | |
| | - Star | ndard Power Operations | | | | |
| | Por | wer On with OS Boot | F | ^p ower On | | |
| | Por | wer Off with OS Shutdown Request | F | Power Off | | |
| | | | | | | |
| | | ergency or Unresponsive System Power Opera The following actions do not initiate a cl | | of the Operating S | ystem. | |
| | For | rce Power Off without OS Shutdown Request | | Force Power Off | | |
| | For | rce Power Off without OS Shutdown Request & Power O | n 📃 | Force Power Cycl | | |
| | Ha | rdware Reset with OS Reboot | | Hard Reset | | |
| | | lse Diagnostic Interrupt. Used to cause the OS to do a C mp (OS dependent) | liagnostic | Diagnostic Dump | | |
| | Por | wer On using Back-Up BIOS | P | ower On (Back-Up E | IOS) | |

| Standard Power Operations | | | | | |
|------------------------------------|--|--|--|--|--|
| Note: For details on other powe | r management features, see Figure 3-1, on page 3-3. | | | | |
| Power On button | Launches the power up sequence. During this sequence, hardware is powered up to the main power mode and the Operating System is booted. Note: | | | | |
| | If an error occurs during this sequence, the system is automatically powered down to standby. | | | | |
| Power Off button | Accessible only when the system is powered on. | | | | |

Figure 3-3. Powering on the server from the console

- 2. From the Standard Power Operations box, click Power On to launch the power up sequence, which may take a few minutes to complete.
- 3. From the Power Information box, click the Refresh button to update power status. Once the power up sequence has completed, the Power State value switches from Off to On and the Power Off button is enabled.
- 4. Connect to the Remote System Console to follow the power on sequence, as explained in Launching the Remote System Console, on page 4-10.



What To Do if an Incident Occurs?

- The power cable may be detached.
- The power sequence has not completed.
- The power supply may be damaged.

3.4. Powering Off the Server from the Console

The server can be powered off from the Power Management page Standard Power Operations box.

mportant The Power status display is not updated dynamically, therefore displayed status may not reflect actual status and the Power Off button may not be enabled although the system is powered up. You can update power status by using the Refresh button.

Prerequisites

You have Power Control permission

The Power Off button is enabled

Procedure

 From the System Control tab, click Power > Power Management to open the Power Management page.

| Power Management Power Information Power State: On Last Restart Reason: chassis power control command Refresh Standard Power Operations Power On with OS Boot Power Off with OS Shutdown Request Power Off Emergency or Unresponsive System Power Operations The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off Hardware Reset with OS Reboot Hardware Reset with OS Reboot Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Dump (OS dependent) Power On using Back-Up BIOS Power On (Back-Up BIOS) Power On (Back-Up B | Management Console Media Power Information Power State: On Last Restart Reason: chassis power control command Refresh Standard Power Operations Power Off with OS Boot Power Off with OS Shutdown Request Power Off Emergency or Unresponsive System Power Operations The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Power On Force Power Off Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump | | User : super System | em Control | Monitoring | Configuration | Maintenan |
|---|---|------|---|------------|--------------------|---------------|-----------|
| te Console I Media Power Information Power State: On Last Restart Reason: chassis power control command Refresh Standard Power Operations Power On with OS Boot Power Off Power Off with OS Shutdown Request Emergency or Unresponsive System Power Operations The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request Force Power Off Force Power Off Hardware Reset with OS Reboot Hardware Reset with OS Reboot Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Dump (OS dependent) | Console Power Information Power State: On Last Restart Reason: chassis power control command Refination Power Operations Power On with OS Boot Power On Power Off with OS Shutdown Request Power Off Emergency or Unresponsive System Power Operations The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Porce Power Off without OS Shutdown Request Force Power Off Porce Power Off without OS Shutdown Request & Power On Force Power Off Power Off without OS Shutdown Request & Power On Force Power Off Puble Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump Dump (OS dependent) Diagnostic Dump | | Power Management | | | | |
| Power State: Un Last Restart Reason: chassis power control command Refresh Standard Power Operations Power On with OS Boot Power Off Power Off with OS Shutdown Request Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request Force Power Off Hardware Reset with OS Reboot Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Dump (OS dependent) | Aedia Power State: Un Last Restart Reason: chassis power control command Refresh Standard Power Operations Power On Power Off with OS Boot Power Off Power Off with OS Shutdown Request Power Off Emergency or Unresponsive System Power Operations The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request Force Power Off Power Off without OS Shutdown Request & Power On Force Power Off Poue Power Off without OS Shutdown Request & Power On Force Power Off Puble Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump Dump (OS dependent) Diagnostic Dump | | Power Information | | | | |
| Standard Power Operations Power On Power Off with OS Shutdown Request Power Off Emergency or Unresponsive System Power Operations The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Power On Force Power Off Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump | Standard Power Operations Power On with OS Boot Power Off with OS Shutdown Request Emergency or Unresponsive System Power Operations The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Power On Force Power Off Hardware Reset with OS Reboot Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump | | Power State: On | _ | | | |
| Power On with OS Boot Power On Power Off with OS Shutdown Request Power Off Emergency or Unresponsive System Power Operations The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Power On Force Power Off Force Power Off without OS Shutdown Request & Power On Force Power Off Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump | Power On with OS Boot Power On Power Off with OS Shutdown Request Power Off Emergency or Unresponsive System Power Operations The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Power On Force Power Cycle Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump | edia | Last Restart Reason: chassis power control command | R | Refresh | | |
| Power Off with OS Shutdown Request Power Off Emergency or Unresponsive System Power Operations The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Porce Power Cycle Hardware Reset with OS Reboot Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump | Power Off with OS Shutdown Request Power Off Emergency or Unresponsive System Power Operations The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Porce Power Oyle Force Power Cycle Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump | | Standard Power Operations | | | | |
| Emergency or Unresponsive System Power Operations The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Power On Force Power Cycle Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump | Emergency or Unresponsive System Power Operations The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Power On Force Power Cycle Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump | | Power On with OS Boot | F | Power On | | |
| The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Power On Force Power Cycle Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Dump (OS dependent) Diagnostic Dump | The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Power On Force Power Cycle Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump | | Power Off with OS Shutdown Request | F | Power Off | | |
| The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Power On Force Power Cycle Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump | The following actions do not initiate a clean shut-down of the Operating System. Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Power On Force Power Cycle Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump | | | | | | |
| Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Power On Force Power Cycle Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump OS dependent) Diagnostic Dump | Force Power Off without OS Shutdown Request Force Power Off Force Power Off without OS Shutdown Request & Power On Force Power Cycle Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump Dump (OS dependent) Diagnostic Dump | | | | | | |
| Force Power Off without OS Shutdown Request & Power On Force Power Cycle Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Dump (OS dependent) | Force Power Off without OS Shutdown Request & Power On Force Power Cycle Hardware Reset with OS Reboot Hard Reset Pulee Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Dump (OS dependent) | | The following actions do not initiate a clean | shut-down | | - | |
| Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Dump (OS dependent) Diagnostic Dump | Hardware Reset with OS Reboot Hard Reset Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Dump (OS dependent) Diagnostic Dump | | Force Power Off without OS Shutdown Request | | Force Power Off | r | |
| Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Dump (OS dependent) | Pulse Diagnostic Interrupt Used to cause the OS to do a Diagnostic Diagnostic Dump (OS dependent) | | Force Power Off without OS Shutdown Request & Power On | | Force Power Cyc | le | |
| Dump (OS dependent) | Dump (OS dependent) | | Hardware Reset with OS Reboot | | Hard Reset | | |
| Power On using Back-Up BIOS Power On (Back-Up BIOS) | Power On using Back-Up BIOS Power On (Back-Up BIOS) | | Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagr Dump (OS dependent) | nostic | Diagnostic Dump | 2 | |
| | | | Power On using Back-Up BIOS | P | ower On (Back-Up E | 3IOS) | |
| | | | • • • • • • • | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

| Sta | ndard Power Operations Box |
|--------------------------------|--|
| Note: For details on other pow | er management features, see Figure 3-1, on page 3-3. |
| Power On button | Accessible only when the system is powered off. |
| | Requests the Operating System to perform a graceful power down. |
| Power Off button | During this sequence the Operating System saves data, closes open applications and shuts down. Note: The Operating System must be configured to accept the power off request. |

Figure 3-4. Powering off the server from the console

- 2. From the Standard Power Operations box, click Power Off to launch the routine power down sequence, which may take a few minutes to complete.
- 3. From the Power Information box, click the Refresh button to update power status. Once the power down sequence has completed, the Power State value switches from On to Off and the Power On button is enabled.
- 4. Connect to the Remote System Console to follow the power off sequence, as explained in Launching the Remote System Console, on page 4-10.

Important The physical power button located on the Local Control Panel should only be used for servicing operations and/or in the event of an emergency or a network failure.

What To Do if an Incident Occurs?

If the system remains in the **Power On** state after a **Power Off** operation, one of the following problems may be the cause:

- The power off sequence has not completed.
- The system is frozen.
- The system is not set up to accept the power off sequence.

You may need to forcibly power down the system using one of the power off buttons accessible from the Emergency or Unresponsive System Power Operations Box.

3.5. Forcibly Powering Off / Resetting the Server

In the event of a system crash or freeze, the system can be forcibly powered off or reset from the Power Management page Emergency or Unresponsive System Power Operations box.

mportant The Power status display is not updated dynamically, therefore displayed status may not reflect actual status and buttons may not be enabled. You can update power status by using the Refresh button.

Prerequisites

You have Power Control permission

The system remains in the Power On state after a Power Off operation

Procedure



The Emergency or Unresponsive System Power Operations buttons should only be used if the Operating System is unable to respond to a standard power off request. These sequences may result in data loss and file corruption.

 From the System Control tab, click Power > Power Management to open the Power Management page and access the Emergency or Unresponsive System Power Operations box.

| | Power Management |
|-------------------------|--|
| wer 'ower Management | r over management |
| mote Console | Power Information Power State: On |
| tual Media | Power State: On Last Restart Reason: chassis power control command Refresh |
| | |
| | Standard Power Operations Power On with OS Boot Power On |
| | |
| | Power Off with OS Shutdown Request Power Off |
| | Emergency or Unresponsive System Power Operations |
| | The following actions do not initiate a clean shut-down of the Operating System. |
| | Force Power Off without OS Shutdown Request Force Power Off |
| | Force Power Off without OS Shutdown Request & Power On Force Power Cycle |
| | Hardware Reset with OS Reboot Hard Reset |
| | Pulse Diagnostic Interrupt. Used to cause the OS to do a Diagnostic Diagnostic Dump (OS dependent) |
| | Power On using Back-Up BIOS Power On (Back-Up BIOS) |
| | |

| Emergency or | Emergency or Unresponsive System Power Operations | | | |
|---|--|--|--|--|
| Important: These buttons should only be used if the Operating System is unable to respond to a standard (graceful) power off request. These sequences may result in data loss and file corruption. | | | | |
| Note: For details on other power management features, see Figure 3-1, on page 3-3. | | | | |
| Force Power Off button Performs a power down sequence independently of the Operating System. | | | | |
| Force Power Cycle buttonPerforms a power down sequence independently Operating System and automatically re-launches powering up sequence. | | | | |
| Hard Reset button | Restarts the Operating System without powering down the system. All cache information is erased. Use it as a last resort to forcibly retrieve the Operating System when it freezes. | | | |
| Diagnostic Dump button Triggers a Pulse Diagnostic Interrupt for error debugging and diagnosis. The Operating System dumps the contents of memory to disk and the syste is reset. | | | | |
| Power On (Back-Up BIOS) button Performs a power up sequence using a back-up version of the BIOS. This feature is used to restart the server when BIOS integrity is no longer ensured. | | | | |

Figure 3-5. Emergency Power Off

- 2. From the Emergency or Unresponsive System Power Operations box, carefully select the required operation and click the corresponding button to launch the selected sequence, which may take a few minutes to complete.
- 3. From the Power Information box, click the Refresh button to update power status.

Chapter 4. Using the Remote System Console

This chapter explains how to set up and use the remote system console. It includes the following topics:

- Setting Up the Remote System Console, on page 4-2
- Launching the Remote System Console, on page 4-10
- Stopping the Remote System Console, on page 4-18

4.1. Setting Up the Remote System Console

The Remote System Console feature is used to connect directly to the server from the Hardware Console, allowing you to remotely view, use and control the server with the keyboard, video and mouse on your local computer.

This feature can be used in conjunction with the Virtual Media feature to perform remote software and firmware installations.

Notes For everyday use, end users will remotely connect to the server by using the remote desktop client compatible with their Operating System (e.g. Terminal Server for Microsoft Windows or Xming for Linux).

The Remote System Console can be configured to suit your needs from the Hardware Console, as explained in the following sections.

Note Writing data to a virtual CD/DVD media is NOT supported.

Prerequisites

The Remote System Console is a Java Applet that establishes a TCP connection to the system's embedded management controller (BMC) using the RFB protocol and requires the installation of Java Runtime Environment (JRE) version 1.4 or higher on your computer.

To be able to use the Remote System Console feature, your network must be configured to support the RFB protocol.

4.1.1. Configuring User Specific Settings

The Remote Console Settings page allows you to configure certain parameters in order to:

- Improve Remote System Console display performance.
- Set default start options.
- Specify a keystroke shortcut to launch the mouse synchronization process.
- Configure the keystroke combinations button displayed in the Remote System Console Control bar.

Prerequisites

User Specific Remote Console Settings: you are using the super user account Transmission Encoding: you have the RC Settings (Encoding) permission

Exclusive Access: you have the RC Settings (Exclusive Access) permission

Monitor Mode: you have the RC Settings (Monitor Mode) permission

Mouse Hotkey and Remote Console Button keys: you have the RC Settings (Hotkeys) permission

Procedure

1. From the Configuration tab, click Remote Console Settings > User Specific. The Remote Console Settings page appears.

| | | | Connected on I | Nodule: 0 (Master) | | |
|--|----------------------|---|---|--------------------|---------------|-------------|
| | | User : super | System Control | Monitoring | Configuration | Maintenance |
| ▶ Global Settings | A Remote Console Set | ttings | | | | ^ |
| | | | | | | |
| ▷BMC Settings | | User Specific Remote Conso The settings on this page are | | ationa will affect | | |
| BMC User Management | | | ected user only. | ations will allect | | |
| ⊳Security | | supe | r 🖌 Update | | | |
| ✓ Remote Console Settings User Specific | | Transmission Encoding —— | | | | |
| Keyboard/Mouse | | Automatic Detection * | | | | |
| ▷Alert Settings | | Pre-configured | | | | |
| | | Network Speed | LAN (high color) | * | | |
| | | Manually | | | | |
| | | Compression | 0 - none | | | |
| | | Color Depth | 16 bit - high col 🗸 | * | | |
| | | - Miscellaneous Remote Cons | ole Settings | | | |
| | | 📃 Start in M | - | | | |
| | | 🔲 Start in Ex | clusive Access Mode | * | | |
| | | - Mouse Hotkey | | | _ | |
| | | Hotkey (Help) Alt+F12 | * | | | |
| | | Used for fast mouse synchro to free the grabbed m | nization (in Double Mo ouse (in Single Mouse | | | |
| | | Remote Console Button Key | 2 | | | |
| | | | iition (Help) Name | | | |
| | | Button Key 1 confirm Ctrl+*Alt+*De | elete * | | * | |
| | | Button Key 2 ALT+F1 | | | * | |
| | | Button Key 3 ALT+F2 | | | * | |
| | | Button Key 4 F2 | | | * | |
| | | Button Key 5 F12 | | | * | |
| | | Button Key 6 ALT+F11 | | | * | |
| | | | lore entries | | | |
| | | | | | | |
| | | Apply * Stored value | View Defaults | | | |
| | | Groted value | is equal to the delaut | | | ~ |

| User S | Specific Remote Console Settings | | |
|---|---|--|--|
| page for your own user accour | re the Remote System Console settings available in this nt or for another user. Select in the drop-down list a user order to view/modify the Remote System Console | | |
| | Transmission Encoding | | |
| | ge the image-encoding algorithm used to transmit the m Console in order to improve or optimize the display | | |
| Automatic Detection | The video encoding and the compression level is computed automatically according to the available bandwidth and the current video data. | | |
| Pre-configured Select in the Network Speed drop-down list the pre-configured setting that corresponds to your network specifications. | | | |
| | Use this option to adjust manually the compression rate and the color depth. Note that values displayed in the Color Depth drop-down list differ depending on the selected value in the Compression drop-down list. | | |
| Manually | The standard color depth is 16 Bit (65536 colors). The other color depths are intended for slower network speeds to allow a faster transmission of data. Therefore compression level 0 (no compression) uses only 16 Bit or 8 Bit (256 colors) color depth. At lower bandwidths only 4 Bit (16 colors) and 2 Bit (4 gray scales) are recommended for typical desktop interfaces. Photo-like pictures have best results with 4 Bit (16 gray scales). 1 Bit color depth (black/white) should only be used for extremely slow network connections. | | |
| Miscel | aneous Remote Console Settings | | |
| Start in Monitor Mode Select this option to start the Remote System Console with the Monitor only option enabled. | | | |
| Start in Exclusive Access Mode | Select this option to start the Remote System Console with the Exclusive Access option enabled. | | |
| | Mouse Hotkey | | |
| Hotkey | This field allows you to specify a hotkey combination which starts the mouse synchronization process if pressed in the Remote System Console. This hotkey works only if you have selected the Linux Mouse Type, as described in Configuring the Keyboard and Mouse, on page 4-6. | | |

| Remote Console Button Keys | | | | |
|---|--|--|--|--|
| This box allows you to define up to 32 key combinations that can be sent to the remote server. By default, the confirm Control+Alt+Delete key combination is defined for Button Key 1, where confirm means that a confirmation dialog will request the user to confirm this action before the key combination is sent to the remote server. | | | | |
| More Entries To add more entries, select this button and complete the Key Definition as explained in the associated Help topic. | | | | |
| Key Definition | Key combination to be sent to the remote server. | | | |
| Name Optional name for easy identification of the action associated with the key combination. | | | | |
| Help Explains how to define key combinations. | | | | |
| | | | | |
| View Defaults button Allows you to display factory-default values. Click Apply to restore factory-default configuration. | | | | |

Figure 4-1. Remote System Console - User Specific Settings

- 2. Complete the required fields and click Apply.
- 3. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required.

4.1.2. Configuring the Keyboard and Mouse

This page allows you to configure Keyboard and Mouse settings to use your local mouse and keyboard to control the remote server through the Remote System Console.

Prerequisites

You have the RC Keyboard/Mouse Settings permission

Procedure

1. From the Configuration tab, click Remote Console Settings > Keyboard/Mouse. The Keyboard/Mouse Settings page appears.

| | User: super | System Control | Monitoring | Configuration | + Logout Maintenance |
|--|--|--|------------|---------------|-------------------------|
| ∇ Global Settings Platform Managed Server Functional Profiles | Keyboard/Mouse Settings | e Settings | | | <u> </u> |
| ▽BMC Settings Network Date-Time SNMP Messages | Keyboard Model Key release timeout Timeout after | 50 💌 msec * | | | |
| ✓ BMC User Management Users Groups Password ✓ Security Encryption | USB Mouse Type Mouse speed | Enable key release timeout if you experier during poor network perfo Other Operating Systems • • Auto • • Fixed scaling : 1.00 • | | rokes | |
| SSL Certificate User Logon Policy Authentication Power Button Lockout User Lockout VRemote Console Settings | | Apply View Defaults * Stored value is equal to the default. | | | |
| Viende Console Sectings User Specific Keyboard/Mouse | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| Keyboard/Mouse Settings | | | |
|-------------------------|--|--|--|
| Keyboard Model | Use the drop-down list to select your keyboard type. | | |
| Key Release Timeout | Enable this option if you experience unwanted repeated keystrokes when using your local keyboard to control the remote system. This issue usually occurs in a context of slow LAN performance. | | |
| | Note that when this option is enabled, the keystroke is automatically considered as released upon the Key Release Timeout, even if the key is maintained pressed. | | |
| Timeout After | Value of the Key Release Timeout in milliseconds. | | |
| USB Mouse Type | Mice transmit their movement using absolute or relative values, depending on the remote operating system. | | |
| | By default, Auto is selected: this mode detects automatically the speed and acceleration settings of your mouse to determine the position of the mouse pointer on the remote screen. | | |
| Mouse Speed | Select Fixed Scaling if you have synchronization issues between the remote mouse pointer and your local mouse. This mode translates the mouse movements as follows: one pixel move on your local workstation leads to "n" pixel moves on the remote system. Use the trial and error method to select the best "n" value in the drop-down list. This option works only if mouse acceleration is turned off on the remote system. | | |
| | | | |
| View Defaults button | Allows you to display factory-default values. Click Apply to restore factory-default configuration. | | |

Figure 4-2. Remote System Console - Keyboard and Mouse Settings

- 2. Change the keyboard and mouse parameters as required and click Apply.
- 3. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required.

4.1.3. Sharing Local Drives

The virtual media drive redirection feature allows you to mount floppy or CD-ROM image files and to share your local drives (floppy drives, CD-ROM, USB keys, hard disks...) with the remote system over a TCP network connection. You can connect image files either using the Hardware Console or through the Remote System Console. The local drives sharing feature is available using the Remote System Console only.

This section describes how to enable/disable the Remote System Console drive redirection feature. You can also enable write support so that the remote system can write data to the shared drives.

Note Writing data to a virtual CD/DVD media is NOT supported.

Prerequisites

You have Virtual Media Upload permission

Note To enable/disable the Hardware Console drive redirection feature, assign/remove the Virtual Media Upload permission.

Procedure

1. From the System Control tab, click Virtual Media > Drive Redirection to open the Drive Redirection page.

| | | | | | | - ≁Logout |
|--|-------------------|--|--------------------------|------------|---------------|------------------|
| | | User : super | System Control | Monitoring | Configuration | Maintenance |
| ♥ Power Power Management ♥ Remote Console Preview Launch ♥ Virtual Media Drive Redirection | Drive Redirection | Active Image - Drive No Drive Redirection - Drive Redirection (floppy, CD-RO) Disable Drive Re Force read-only Appl | disk emulation set. 2 | isks) with | | |
| | | | | | | ~ |

| Active Image - Drive # Boxes | | | |
|------------------------------|---|--|--|
| Active Image - Drive # | Displays details about the current connected image or drive and provides command buttons, which may differ depending on the connected component. | | |
| | When no image or drive is connected, the message No disk emulation is set is displayed. | | |
| | Drive Redirection Box | | |
| Disable Drive Redirection | Clear this check box to enable the Remote System Console virtual media drive redirection feature. | | |
| | Select this check box to disable Remote System Console virtual media drive redirection feature. | | |
| Force read-only connections | Select this check box to disable write support, shared drives are read-only. Data can be read by the remote system, but not overwritten for enhanced data integrity and system security - Recommended. | | |
| | Clear this check box to enable write support. | | |
| | WARNING: enable write support with care as you may damage data and file systems. | | |
| View Defaults button | Allows you to display factory-default values. | | |

Figure 4-3. Drive Redirection

2. Select or clear the check boxes depending on your needs and click Apply.

4.2. Launching the Remote System Console

The Remote System Console can be previewed and/or launched, at any time, directly from the Hardware Console.

Note If a security warning message, prompting you to install and run a Java plug-in, check the plug-in's authenticity and click **Yes** to install and run the plug-in.

Procedure

This procedure describes how to launch and/or preview the Remote System Console.

- 1. From the System Control tab, expand the Remote Console menu.
 - If you want to preview the Remote System Console, go to step 2.
 - If you want to preview and then launch the Remote System Console, go to step 3.
 - If you want to launch the Remote System Console directly, go to step 4.
- 2. To preview the Remote System Console from the Hardware Console, click Preview to open the Remote Console Preview page.

The display is not refreshed dynamically. If required, click the **Refresh** button to update the display.



| Preview Box | | | |
|---|---|--|--|
| Click to launch link Click this link to launch the Remote System Console. | | | |
| Refresh button | The display is not refreshed dynamically, click this button to refresh the Remote System Console display. | | |
| Desktop size information Current Remote System Console desktop size. | | | |

Figure 4-4. Remote Console Preview

- To preview and then launch the Remote System Console, click Preview to open the Remote Console Preview page and then click the Click to launch link. The Remote System Console opens in a new window.
- 4. To directly launch the Remote System Console, click Launch. The Remote System Console opens in a new window.

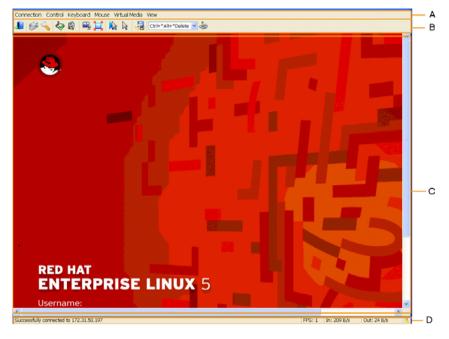
What To Do if an Incident Occurs?

- Network settings are incorrect.
- Java Runtime Environment (JRE) version 1.4 or higher is not installed on your computer.
- Your network is not configured to support the RFB protocol.

Contact your network administrator.

4.2.1. Remote System Console Overview

Once you have connected to the Remote System Console, it behaves as if you were sitting in front of the remote system, using your local keyboard and mouse.



| Item | Description |
|-------------------|---|
| | The Menu bar gives access to the following menus: |
| | Connection |
| | Control |
| A: Menu bar | • Keyboard |
| A. Menu bar | • Mouse |
| | Virtual Media |
| | • View |
| | For details, see Remote System Console Menus, on page 4-12. |
| | The Toolbar gives access to the following controls: |
| | • Exit |
| | • Screenshot |
| | Properties |
| | Enter/Leave Monitor Only Mode |
| | Enter/Leave Exclusive Access Mode |
| B: Toolbar | • Scaling |
| D. IOOIDUI | Full Screen Mode |
| | Virtual Media |
| | Select Keyboard Macro |
| | Send Keyboard Macro |
| | Sync Mouse (Reserved) |
| | Single Cursor Mode |
| | For details, see Remote System Console Toolbar, on page 4-13. |
| C: Remote desktop | This area displays the remote system desktop screen. |
| D: Statusbar | The Statusbar provides connection information. |

Figure 4-5. Remote System Console overview

4.2.2. Remote System Console Menus

This section describes the features available to configure and use the Remote System Console **menu** bar.

| Menu Name | Menu Items | Description |
|------------------|-----------------------------|--|
| Connection | Properties | Select to display and define remote video options. |
| | Connection Info | Select to display remote connection information, such as Device Address, Connection Port, Incoming/Outgoing Speed, |
| | Save Screenshot | Select to save the remote screen. |
| | Screenshot to Clipboard | Select to copy the remote screen to clipboard. |
| | Exit | Select to close the remote connection. |
| | Enter Monitor Only Mode | Select to disable remote keyboard and mouse interaction. |
| Control | Enter Exclusive Access Mode | Select to force the remote sessions of all other users to close until the exclusive user disables the option or exits. |
| | Chat Window | Select to display a chat window allowing you to interact with other users logged on to the remote system console. |
| Keyboard | Keyboard Macros | Select the required keyboard macro from the list displayed. |
| 1 | Local Keyboard Mapping | Select keyboard language from the list displayed. |
| | Sync Mouse | Reserved. |
| Mouse | Single Cursor Mode | Select to disable / enable the local mouse. Press Alt+F12 to leave this mode. |
| Virtual Media | Virtual Media | Select to display and connect virtual media. See Virtualizing Media, on page 4-14 for details. |
| | Scaling | Select to display and define remote window scaling type and quality options. |
| View | Full Screen Mode | Select to display the remote console in Full Screen Mode. Press Ctrl+Alt+F to leave this mode. |
| | Show Toolbar | Select to show the remote console toolbar. Deselect to hide the remote system console toolbar. |
| | Show Statusbar | Select to show the remote console statusbar. Deselect to hide the remote console statusbar. |

Connection Control Keyboard Mouse Virtual Media View

Figure 4-6. Remote System Console menus

mportant If you experience a problem with your keyboard, click Keyboard > Local Keyboard Mapping. Select any other keyboard language and then reselect the required keyboard language. The problem should be resolved.

4.2.3. Remote System Console Toolbar

This section describes the features available from the Remote System Console Toolbar.

| 🎩 🚱 💫 🤣 🖳 其 ኲ 🔤 🚰 Ctrl+*Alt+*Delete 🖌 旧 | | | |
|--|-----------------------------|--|--|
| Button Icon | Button Name | Description | |
| " | Exit | Select to close the remote connection. | |
| | Screenshot to Clipboard | Select to copy the remote screen to clipboard. | |
| 2 | Properties | Select to display and define remote video options. | |
| ie in the second | Enter Monitor Only Mode | Select to disable remote keyboard and mouse interaction. A red cross appears. Select again to cancel. | |
| | Enter Exclusive Access Mode | Select to force the remote sessions of all other users to close until the exclusive user disables the option or exits. A red cross appears. Select again to cancel. | |
| | Scaling | Select to display and define remote window scaling type and quality options. | |
| K R | Full Screen Mode | Select to display the remote console in Full Screen Mode. Press Ctrl+Alt+F to leave this mode. | |
| | Virtual Media | Select to display and connect virtual media. See Virtualizing Media, on page 4-14 for details. | |
| Ctrl+*Alt+*Delete 💌 | Keyboard Macros | Select the required keyboard macro from the list displayed. | |
| ÷. | Send Keyboard Macro | Send the selected keyboard macro. | |
| | Sync Mouse | Reserved. | |
| A | Single Cursor Mode | Select to disable / enable the local mouse. Press Alt+F12 to leave this mode. | |

Figure 4-7. Remote System Console toolbar

4.3. Virtualizing Media

Using the Virtual Media feature, you can virtualize up to two images or drives, allowing any floppy or CD-ROM image, floppy drive, optical drive and/or USB mass storage device available on your local computer or anywhere on the network to be used from the Remote System Console.

The remote system then has access to the virtual media on your local computer and can read from and write to that media as if it were physically present on the remote system. These virtual drives can then be used for operations such as installing software and firmware, updating drivers or installing new Operating Systems.

This section guides you through the following procedures:

- Virtualizing a Local Drive, on page 4-15
- Virtualizing an Image File, on page 4-16
- Virtualizing a Local Folder, on page 4-17

4.3.1. Virtualizing a Local Drive

You can select any of the local drives and make them accessible to the remote server.

Prerequisites

Drive redirection is enabled from the Hardware Console

Procedure

.

1. From the Remote System Console menu bar, select Virtual Media, or select the Virtual Media button () from the toolbar. The Virtual Media dialog opens, displaying

Current Virtual Media Sessions status and Local Drive tab options in the Create New Virtual Media Session field.

| Current Virtual Media Sessions | | | |
|---|------------|--|--|
| Virtual Drive 1: Not connected | Disconnect | | |
| Virtual Drive 2: Not connected | Disconnect | | |
| Create New Virtual Media Session | | | |
| Local Drive Image File Local Folder | | | |
| Please select a Drive for Virtual Media | | | |
| C: (Hard Disk Partition) | | | |
| Enable Write Support | | | |
| Select Drive Number 1 💟 Connect | | | |
| Close | | | |

| Current Virtual Media Sessions | | |
|--|---|--|
| Virtual Drive X | Two possible values: Connected / Not connected | |
| Disconnect button | Press this button to disconnect a drive. When no drive is connected, this button is grayed out. | |
| Create New Virtual Media Session - Local Drive Tab | | |
| Select a Drive for Virtual Media list | Press the scroll arrow to select the required local drive. | |
| Enable Write Support checkbox | Select this checkbox to allow data to be written to the local drive. | |
| Select Drive Number list | Press the scroll arrow to select the required drive mount number. | |
| Update button | Press this button to update the local drive list. | |
| Connect button | Press the Connect button to mount the drive. Virtual Drive X: Connected appears in the Current Virtual Media Sessions area and the corresponding Disconnect button is enabled. | |

Figure 4-8. Virtual Media - Local Drive

2. Configure the local drive as explained above and click **Connect**. The local drive is now mounted and can be used by the remote server to read and/or write (if enabled) data.

4.3.2. Virtualizing an Image File

You can emulate up to two image files as USB devices and make them accessible to the remote server.

Prerequisites

Drive redirection is enabled from the Hardware Console

The image file has been created

Procedure

 From the Remote System Console menu bar, select Virtual Media, or select the Virtual Media button () from the toolbar. The Virtual Media dialog opens, displaying

Current Virtual Media Sessions status and Local Drive tab options in the Create New Virtual Media Session field.

2. Select the Image File tab.

| Current Virtual Media Sessions | | | | |
|---|------------|--|--|--|
| Virtual Drive 1: Not connected | Disconnect | | | |
| Virtual Drive 2: Not connected | Disconnect | | | |
| Create New Virtual Media Session | | | | |
| Local Drive Image File Local Folder | | | | |
| Please select an Image File for Virtual Media | | | | |
| | Browse | | | |
| | | | | |
| | | | | |
| Select Drive Number 1 🗸 Connect | | | | |
| Close | | | | |

| Current Virtual Media Sessions | | |
|---|--|--|
| Virtual Drive X | Two possible values: Connected / Not connected | |
| Disconnect button | Press this button to disconnect a drive. When no drive is connected, this button is grayed out. | |
| Create New Virtual Media Session - Image File Tab | | |
| Select an Image File for Virtual Media list | Press the Browse button to select the required image file. | |
| Select Drive Number list | Press the scroll arrow to select the required drive mount number. | |
| Connect button | Press the Connect button to mount the image file. Virtual Drive X: Connected appears in the Current Virtual Media Sessions area and the corresponding Disconnect button is enabled. | |

Figure 4-9. Virtual Media - Image File

3. Mount the image file as explained above and click **Connect**. The image file is now mounted and can be used by the remote server.

4.3.3. Virtualizing a Local Folder

You can select any of the local folders on your local computer and make them accessible to the remote server.

Prerequisites

Drive redirection is enabled from the Hardware Console

Procedure

1. From the Remote System Console menu bar, select Virtual Media, or select the Virtual Media button () from the toolbar. The Virtual Media dialog opens, displaying

Current Virtual Media Sessions status and Local Drive tab options in the Create New Virtual Media Session field.

2. Select the Local Folder tab.

| Current Virtual Media Session | ns |
|--|------------|
| Virtual Drive 1: Not connected | Disconnect |
| Virtual Drive 2: Not connected | Disconnect |
| Create New Virtual Media Sess Local Drive Image File Local Folder | sion |
| Please select a Folder for Virtual Media | |
| | Browse |
| Enable Write Support | |
| Select Drive Number 🛽 💙 Conn | ect |
| Close | |

| Current Virtual Media Sessions | | |
|---|---|--|
| Virtual Drive X | Two possible values: Connected / Not connected | |
| Disconnect button | Press this button to disconnect a drive. When no drive is connected, this button is grayed out. | |
| Create New Virtual Media Session - Local Folder Tab | | |
| Select a Folder for Virtual Media list | Press the Browse button to select the required image file. | |
| Enable Write Support checkbox | Select this checkbox to allow data to be written to the local folder. | |
| Select Drive Number list | Press the scroll arrow to select the required drive mount number. | |
| Connect button | Press the Connect button to mount the drive. Virtual Drive X: Connected appears in the Current Virtual Media Sessions area and the corresponding Disconnect button is enabled. | |

Figure 4-10. Virtual Media - Local Folder

3. Configure the local folder as explained above and click **Connect**. The local folder is now mounted and can be used by the remote server to read and/or write (if enabled) data.

4.4. Stopping the Remote System Console

The Remote System Console can be stopped at any time by selecting Connection > Exit from the menu bar, or selecting the Exit button (

Chapter 5. Monitoring the Server

This chapter explains how to monitor server activity and view and manage system event logs and messages. It includes the following topics:

- Initial Messaging and Alert Configuration, on page 5-2
- Checking Monitoring Sensors, on page 5-3
- Checking and Clearing the System Event Log (SEL), on page 5-5
- Checking the Board and Security Messages Log, on page 5-7
- Downloading and Deleting BIOS Log, on page 5-8

mportant Information to help you troubleshoot the server in the event of incorrect operation is given in Troubleshooting the server on page A-1.

5.1. Initial Messaging and Alert Configuration

When the server is first delivered, you will need to perform a few basic configuration tasks to benefit from all the messaging and alert features available. These configuration tasks are explained in detail in Chapter 6, Configuring the Server Management Controller, and are listed below:

- Configuring the Board and Security Message Log, on page 6-12
- Configuring Alert Settings, on page 6-47

5.2. Checking Monitoring Sensors

The system is equipped with various sensors that monitor the status of hardware components, such as:

- Power status
- Presence, absence, redundancy of components
- Voltage values
- Temperature values
- Fan speed
- Physical intrusion
- etc.

Procedure

- From the Monitoring tab, click System Health > Sensors to display the Sensor Status page.
- 2. Click Refresh and check that all component icons are green.

If a component icon is not green, see Appendix A Troubleshooting the Server for more information.

| | ∠ _{Sensor} s | User:super | | System Control Mon | itoring Configuration | Maintena |
|---|-----------------------|----------------------------------|-----------------|--------------------|-----------------------|----------|
| stem Health ensors ystem Event Log essages | | | R | efresh | | |
| messayes | | BMC Sensor Status Sensor Type | Sensor Name | Sensor Status | Sensor Readin | Ig |
| | | System ACPI Power State | ACPI Pwr State | SD/GO: working | | |
| | r S | MC Sensor Status | | | | _ |
| | | Sensor Type | Sensor Name | Sensor Status | Sensor Readin | ng |
| | | Physical Security | Mod. Intrusion | No intrusion | | |
| | | Power Supply | PS 0 | Presence detected | | |
| | | Power Supply | PS_1 | Presence detected | | |
| | | Power Supply | PS_2 | Device Absent | | |
| | | Power Unit | Pwr Redundancy | | | |
| | | Power | Pwr Consumption | | 936 Watts | |
| | | Processor | PROC_0 | Presence detected | | |
| | | Processor | PROC_1 | Presence detected | | |
| | | Processor | PROC_2 | Presence detected | | |
| | | Processor | PROC_3 | Presence detected | | |
| | • | 🕨 🗄 Temperature | | | | |
| | | 🗈 🗉 Voltage | | | | |
| | | 🕨 🗄 Cooling | | | | |

| | Sensor Status Page | | | |
|--|--|--|--|--|
| Refresh button The Sensor Status page is not automatically up therefore the display may not reflect current set status. Use this button, located at the top and the page, to update the display. | | | | |
| | Status Icons Description | | | |
| | eft of certain sensors indicate the status of the monitored to nominal threshold values. | | | |
| and globally. By defaul sensors is reflected by t select the corresponding | dual sensor becomes critical (RED), the corresponding global | | | |
| GREEN | NORMAL Operation correct. No problem has been detected. | | | |
| RED | CRITICAL A problem has been detected. Immediate preventive or corrective action is required. | | | |
| | If a component icon is not green, see Appendix A | | | |

Figure 5-1. Sensor Status

GRAY

Important Values and readings are detailed in Predefined Alert Filters Description, on page A-2.

Sensor not available.

Troubleshooting the Server for more information.

5.3. Checking and Clearing the System Event Log (SEL)

The System Event Log records events compliant with the IPMI standard, in particular those concerning:

- Power supplies
- FANs
- Temperature sensors
- Events recorded in this log can be transmitted via the event alerting system to an Notes SNMP Manager or to personnel by email.
 - You can access another log, which is called the Board and Security Messages log. This log records non-IPMI events.



WARNING

The System Event Log can only store up to 512 entries at a time. Once this limit is reached, the LOG IS NOT AUTOMATICALLY EMPTIED to allow for the arrival of new events. Beyond the 512-entry limit, NEW EVENTS ARE NOT RECORDED. It is strongly recommended to empty this log regularly, using the Clear button, so that the latest events can be logged.

Note that cleared entries are deleted and cannot be retrieved.

The iCare Console automatically collects System Event Logs and can be configured Note to automatically empty the System Event Log. Please refer to the iCare Console User's Guide for details.

Prerequisites

Viewing: none

Clearing: you have Alert Settings & Clear SEL permission

Procedure

• From the Monitoring tab, click System Health > System Event Log to open the System Event Log page.

| | | U | ser:super | | System Control Monito | ring Configuration | Maintenance |
|---------------------------------------|------------|------------|-----------|-----------------|---------------------------|--------------------|-------------|
| | System Eve | nt Log | | | | | |
| r <mark>stem Health</mark> Sensors | - | | | | | | |
| ystem Event Log | | - Log | | | | | |
| 1essages | | Clear R | efresh | | Used Entries: 155 / 512 | | |
| | | Date | Time | Sensor Name | Description | Direction | |
| | | 2009-10-23 | 18:10:44 | ILB 1.2V IB | Limit Exceeded | Assertion Event | |
| | | 2009-10-23 | 18:10:42 | PROC_3 | Presence detected | Assertion Event | |
| | | 2009-10-23 | 18:10:42 | PROC_2 | Presence detected | Assertion Event | |
| | | 2009-10-23 | 18:10:42 | PROC_1 | Presence detected | Assertion Event | |
| | | 2009-10-23 | 18:10:42 | PROC_0 | Presence detected | Assertion Event | |
| | | 2009-10-23 | 18:10:41 | FANPR_3 Redund. | Fully Redundant | Assertion Event | |
| | | 2009-10-23 | 18:10:41 | FANPR_2 Redund. | Fully Redundant | Assertion Event | |
| | | 2009-10-23 | 18:10:41 | FANPR_1 Redund. | Fully Redundant | Assertion Event | |
| | | 2009-10-23 | 18:10:41 | FANPR_0 Redund. | Fully Redundant | | |
| | | 2009-10-23 | 18:10:38 | CANLA | r uny Redundant | Assertion Event | |
| | | 2000-10-22 | 16:00:36 | FANPR_0 Redund. | Fully Redundant | Assertion Event | |
| | | 2009-10-22 | 16:00:32 | FAN_7 Presence | Device Present | Assertion Event | |
| | | 2009-10-22 | 16:00:32 | FAN_6 Presence | Device Present | Assertion Event | |
| | | 2009-10-22 | 16:00:32 | FAN_5 Presence | Device Present | Assertion Event | |
| | | 2009-10-22 | 16:00:32 | FAN_4 Presence | Device Present | Assertion Event | |
| | | 2009-10-22 | 16:00:32 | FAN_3 Presence | Device Present | Assertion Event | |
| | | 2009-10-22 | 16:00:32 | FAN_2 Presence | Device Present | Assertion Event | |
| | | 2009-10-22 | 16:00:32 | FAN_1 Presence | Device Present | Assertion Event | |
| | | 2009-10-22 | 16:00:32 | FAN_0 Presence | Device Present | Assertion Event | |
| | | 2009-10-22 | 16:00:31 | ACPI Pwr State | S0/G0: working | Assertion Event | |
| | | 2009-10-22 | 16:00:31 | PS_2 | Presence detected | Assertion Event | |
| | | 2009-10-22 | 16:00:31 | Pwr Redundancy | Fully Redundant | Assertion Event | |
| | | 2009-10-22 | 16:00:31 | PS_1 | Presence detected | Assertion Event | |
| | | 2009-10-22 | 16:00:31 | PS_0 | Presence detected | Assertion Event | |
| | | 2009-10-22 | 16:00:30 | Mod. Intrusion | General Chassis intrusion | Assertion Event | |
| | | Clear Re | efresh | | Used Entries: 155 / 512 | | |

Figure 5-2. System Event Log

- Use the Refresh button to update the display at any time.
- Use the Clear button to empty the log. Entries are deleted and cannot be retrieved.
- **Note** SEL messages and associated operations to recover are explained in Appendix A Troubleshooting the Server.

5.4. Checking the Board and Security Messages Log

The Board and Security Messages log records non-IPMI events, such as power-on errors, user authentication, connection to the remote console, security violation, log deletion or firmware upgrade.

Note Events compliant with the IPMI standard are recorded in the System Event log.

Prerequisites

You have Log View permission

Procedure

 From the Monitoring tab, click System Health > Messages to open the Board & Security Messages page.

| lessages | Clear Messages | | 84 Messages . Page 1 of 5 | < 1 2 3 4 5 > | |
|----------|---------------------|---------------|------------------------------|---|---|
| | Date-Time | Message | Description | | 1 |
| | 10/27/2009 16:54:10 | Access Logout | User 'super' from host '129. | 182.6.119' logged out. | |
| | 10/27/2009 16:53:56 | Access Login | User 'super' from host '129. | 182.6.119' logged in. | |
| | 10/27/2009 16:34:33 | Access Logout | User 'super' from host '129. | 182.6.119' logged out. | |
| | 10/27/2009 16:00:57 | Access Login | User 'super' from host '129. | 182.6.119' logged in. | |
| | 10/27/2009 15:21:12 | Access Login | User 'super' from host '129. | 182.109.123' logged in. | - I - I - I - I - I - I - I - I - I - I |
| | 10/27/2009 15:15:19 | Access Logout | User 'super' from host '129. | 182.6.37" logged out. | |
| | 10/27/2009 15:10:05 | Access Login | User 'super' from host '129. | 182.6.37' logged in. | |
| | 10/27/2009 11:42:50 | Access Logout | User 'super' from host '129. | 182.6.119' logged out. | |
| | 10/27/2009 11:42:48 | Access Login | User 'super' from host '129. | 182.6.119' logged in. | |
| | 10/27/2009 09:43:05 | Access Logout | User 'super' from host '129. | 182.6.119' logged out. | |
| | 10/27/2009 09:42:35 | Access Login | User 'super' from host '129. | 182.6.119' logged in. | - I - I - I - I - I - I - I - I - I - I |
| | 10/23/2009 18:35:18 | Access Logout | User 'super' from host '129. | 182.109.122' logged out. | |
| | 10/23/2009 18:34:42 | Access Login | User 'super' from host '129. | 182.109.122' logged in. | |
| | 10/23/2009 18:15:37 | Access Logout | User 'super' from host '129. | 182.6.189' logged out. | |
| | 10/23/2009 18:13:59 | Access Login | User 'super' from host '129. | 182.6.189' logged in. | |
| | 10/23/2009 18:10:58 | Access Logout | User 'super' from host '129. | 182.6.189' logged out. | |
| | 10/23/2009 18:10:54 | Access Login | User 'super' from host '129. | 182.6.189' logged in. | |
| | 10/23/2009 18:10:40 | BMC Startup | Device started. | | |
| | 10/23/2009 18:09:51 | BMC Shutdown | Device reset performed by | user 'super' from host '129.182.6.189'. | |
| | 10/23/2009 18:04:13 | Access Login | User 'super' from host '129. | 182.6.189' logged in. | |
| | Clear Messages | | 84 Messages . Page 1 of 5 | | |

Figure 5-3. Board & Security Messages

2. Browse messages, as required, using the navigation arrows or page number buttons.



5.5. Downloading and Deleting BIOS Log

The BIOS logs are sent to the EMM. If your server is not monitored by the iCare Console, you can obtain and delete these BIOS logs with the Hardware Console.

Note You are adviced to monitor your servers with iCare Console. The BIOS logs are then collected in the iCare Console database. You can read, delete and restore the database with the iCare Console interface. The BIOS logs are managed by the iCare Console and suppressed from the EMM.



Don't use this Hardware Console feature to manage BIOS Logs if your server is monitored by iCare Console.

You can query the BIOS logs to help your hardware failure analyze or to perform preventive maintenance.

In case of UNCORRECTABLE ERRORS or FATAL ERRORS detected by the processor of the resource, the BIOS logs all the registers containing CORRECTABLE ERROR, UNCORRECTABLE ERROR, or FATAL ERRORS.

Prerequisites

You have Log View permission

Procedure

 From the Maintenance tab, click Maintenance Operations > BIOS Logs to open the BIOS Logs page.



Figure 5-4. BIOS Logs

Note Over 15 UNCORRECTABLE ERRORS and 6 FATAL ERRORS collected by the EMM logs are lost.

Chapter 6. Configuring the Server Management Controller

This chapter explains how you can configure the server embedded management controller to suit your working environment. It includes the following topics:

- Configuring Platform Identification Settings, on page 6-2
- Configuring the Managed Server Name, on page 6-3
- Modifying Functional Profile Settings, on page 6-4
- Configuring Network Settings for Remote Access, on page 6-6
- Modifying Internal Clock Settings, on page 6-10
- Configuring the Board and Security Message Log, on page 6-12
- Managing Groups, Users and Permissions, on page 6-14
- Configuring Security Parameters, on page 6-34
- Setting up Alert Transmission, on page 6-47



If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

6.1. Configuring Platform Identification Settings



If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

Each server drawer must be given a **unique** Platform ID and Platform Name for easy and reliable identification by management and maintenance software such as Bull System Manager (BSM) and iCare.

Prerequisites

You have Network Settings permission

Procedure

 From the Configuration tab, click Global Settings > Platform to open the Platform Settings page.

| | | | | | | Logout |
|---|--|-----------------|----------------|------------|---------------|-------------|
| Se | erver Hardware Consol | le User : super | System Control | Monitoring | Configuration | Maintenance |
| ⊽ Global Platfo Mana Funct ⊳ BMC Se | Settings om ged Server ional Profiles titings er Management | Platform Settir | * | | | |
| | | | | | | - |

Figure 6-1. Platform Settings

2. Complete the fields and click Apply.

Note The Module Count field is read-only.

6.2. Configuring the Managed Server Name

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

Prerequisites

You have Network Settings permission

Procedure

 From the Configuration tab, click Global Settings > Managed Server to open the Managed Server Settings page.

| | User: super | System Control | Monitoring | Configuration | Maintenance |
|---|--|-----------------------------|-------------------|--------------------|--------------|
| ✓ Global Settings Platform Hunniged Server Functional Profiles ✓ BMC Settings Network Date-Time SIMMP Messages ▷ BMC User Management ▷ Security ▷ Remote Console Settings ▷ Alert Settings | Managed Server Name The Managed Server Name is the name given to the ser Controller (BMC). The Managed Server Name can also be set via an inband Operating System Name parameter). Managed Server Name (Managed Server Name) | ver and associated Operatin | ig System managed | J by this Baseboar | d Management |
| | | | | | |
| | 1 | | | | ~ |

Figure 6-2. Managed Server Settings

2. Complete the field and click Apply.

6.3. Modifying Functional Profile Settings

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

A Functional Profile is a set of parameters defining the Power Restore Policy and the use of Full Fan Speed at system power-on. You can define up to two Functional Profiles (0 or 1) for your system and select one or the other at power-on.

Note When the system power state is ON, the current Functional Profile is displayed, but cannot be modified.

Prerequisites

System is powered OFF

You have Network Settings permission

Procedure

1. From the Configuration tab, click Global Settings > Functional Profiles to open the Functional Profiles Settings page.

| | | User : super | System Control | Monitoring | Configuration | Maintenance |
|---------------------------------------|---------------------|--------------------------------|---|---------------------|---------------|-------------|
| ⊽ Global Settings Platform | Functional Profiles | | | | | ^ |
| Managed Server Functional Profiles | | Power Information Power S | tate: On Refresh | | | |
| ▶BMC Settings | | The Current Functional Profile | e cannot be modified wh | en Power State is O | N. | |
| ▶BMC User Management | | Current Functional Profile | | | _ | |
| ⊳Security | | Current Functional Pro | ofile: 🛛 🗸 * | | | |
| ⊳Remote Console Settings | | Functional Profile 0 | | | | |
| PAlert Settings | | | e Policy OFF | * | | |
| | | | n Speed 🗌 * | | | |
| | | Functional Profile 1 | | | | |
| | | Power Restor | e Policy OFF | * * | | |
| | | Force Full Fa | n Speed 🔲 * | | | |
| | | Apply * Stored val | View Defaults ue is equal to the default | t. | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | _ |
| | | | | | | ~ |
| | - | | | | | |

| | Power Information Box | | | |
|--|--|--|--|--|
| Power State | 2 possible values: | | | |
| | • On | | | |
| | • Off | | | |
| Refresh button | Allows you to update displayed data. | | | |
| | Current Functional Profile Box | | | |
| Current Functional Profile drop-down list | Use the drop-down list to define a Functional Profile or to select the Functional Profile you want to apply at the next power-on. | | | |
| | Note: when the system power state is ON, the Current Functional Profile is displayed, but cannot be modified. | | | |
| Functional Profile <x> Box</x> | | | | |
| Power Restore Policy drop-down list | Use the drop-down list to select the power restore policy you want to apply when AC power returns after a system AC power loss: | | | |
| | • Select OFF if you want the system to remain off when AC power returns. | | | |
| | • Select RESTORE if you want the system to return to the same power state as before the AC power loss. | | | |
| | • Select ON if you want the system to power on when AC power returns. | | | |
| Force Full Fan Speed check box | Select the check box to force full fan speed. At next power-on, the fan speed will always be set at maximum speed, without any regulation by firmware. | | | |
| View Defaults button | Allows you to display factory-default values. Click Apply to restore factory-default configuration. | | | |

Figure 6-3. Functional Profiles Settings

2. Complete the page to comply with your requirements and click Apply.

Configuring Network Settings for Remote Access 6.4.



If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

The Network Settings page allows you to configure or modify the embedded management controller network settings for remote access to the console from a computer or workstation with a Web browser.

Prerequisites

You have Network Settings permission



WARNING

Good knowledge in network administration is required to complete this page. If new network settings are incorrect, you may lose the connection to the console. You are advised to note current settings before proceeding to enter new values so that you can restore the connection to the console if a problem arises.

Procedure

1. From the Configuration tab, click BMC Settings > Network to display the Network Settings page.

| ✓ Global Settings Platform Managed Sever Functional Profiles ✓ BMC Settings ✓ BMC Settings ✓ BMC Settings ✓ BMC User Management ▷ Security ▷ Remote Console Settings ▷ Allert Settings ✓ Allert Settings ✓ Allert Settings | applying changes so th | nnection to the BMC. |
|---|---|---|
| V Global Settings Platform Managed Server Functional Profiles V BMC Settings Network Network Network Security PRemote Console Settings PAlert Settings Advanced Advanced Changing BMC network settings may result in a Plase ensure that all the values are correct before remotely to the BMC. General IP Auto-Configuration Preferred Host Name (DHCP only) Preferred Host Name (DHCP only) Preferred Host Name (DHCP only) Subnet Mask 22 Gateway IP Address Secondary DNS Server IP Address Changing BMC network settings Advanced Plase Show Plase | applying changes so th | nnection to the BMC. lat you can reconnect |
| Network General IP Auto-Configuration Date-Time Messages IP Auto-Configuration IP Auto-Configuration >BMC User Management Preferred Host Name (DHCP only) IP Address >Remote Console Settings Subnet Mask 2 >Alert Settings Gateway IP Address Primary DNS Server IP Address Secondary DNS Server IP Address Advanced IP En SSH Port 2 IP Address IP Address | | |
| Primary DNS Server IP Address Secondary DNS Server IP Address Advanced TELNET Port 2 SSH Port 2 SSH Port 2 | | |
| Advanced TELNET Port 2 SSH Port 2 SSH Port 2 File SSH Port 2 File | | |
| | nable SSH Access * 2 * nable CLP-SSH Access 4 * 4 * 0 * nable Serial Terminal Acc isable Setup Protocol * | |
| MNG0 Network Adapter Configuration MNG0 Ethernet Port for Management ETHD | PHY Reset of the shared I | Ethernet |

| | General Box |
|------------------------------------|--|
| IP Auto-Configuration | This drop-down list allows you to enable or disable network auto-configuration via a DHCP or BOOTP server: |
| | • None: auto-configuration is disabled. |
| | • DHCP: network settings are retrieved from a DHCP server (Factory-default value). |
| | BOOTP: network settings are retrieved from a BOOTP server. |
| Preferred host name (DHCP only) | Accessible only if DHCP is selected. The host name that you want to pass to the DHCP server. |
| IP Address | Accessible only if None is selected. The static IP address you want to use (Factory-default value: 192.x.x.x). |
| Subnet Mask | Accessible only if None is selected. The subnet mask you want to use (Factory-default value: 255.255.255.0). |
| Gateway IP Address | Accessible only if None is selected. Your default gateway IP address, if applicable. |
| Primary DNS Server IP Address | Accessible only if None is selected. Your primary DNS server IP address, if applicable. |
| Secondary DNS Server IP Address | Accessible only if None is selected. Your secondary DNS server IP address, if applicable. |
| | Advanced Box |
| Enable TELNET Access | Select this option to allow connection using a Telnet client. You need SSH/Telnet Access permission. |
| TELNET Port | The Telnet port number (Factory-default: 23). |
| Enable SSH Access | Select this option to allow connection using an SSH client. You need SSH/Telnet Access permission. |
| SSH Port | The Secure Shell (SSH) port number (Factory-default: 22). |
| Enable CLP-SSH Access | Select this option to allow connection from an SSH Command Line Prompt (CLP). You need SSH/Telnet Access permission. |
| CLP-SSH Port | The CLP-SSH port number (Factory-default: 44). |
| Remote Console & HTTPS Port | The port number used for standard HTTPS connectons (Factory-default: 443). |
| HTTP Port | The port number used for standard HTTP connections (Factory-default: 80). |
| Enable Serial Terminal Access | Select this option to open a Telnet connection to the server serial port in order to connect the server in terminal mode. You need SSH/Telnet Access permission. |
| Disable Setup Protocol | Select this option to prevent the <i>psetup (Windows) tool</i> and/or <i>mc-setup (Linux) tool</i> , used to discover the server on the LAN during initial setup, from re-detecting this server when installing new servers. |

| | Advanced Box |
|---|---|
| Ethernet Interface for Management | The Ethernet port number used to connect the embedded management controller to the Enterprise LAN. By default, Ethernet port ETH0/MNG0 is used : both the management and host networks share this connection and the network cable is connected to ETH0/MNG0. Alternatively, you can separate management and host networks by using Ethernet port INTER/MNG1 for the management network and MNG0 for the host network In this case, select MNG1 and then connect the management network cable to INTER/MNG1 and the host network cable to MNG0. |
| MNG | 0 Network Adapter Configuration |
| MNG0 Ethernet Port for Management | Select Ethernet port ETHO or ETH1 |
| Inhibit the PHY Reset of the shared Ethernet Controller | Select this option to prevent the Ethernet Controller from being reset when the server is reset. |
| MNG | 1 Network Adapter Configuration |
| Current Parameters | Displays current network adapter settings. |
| Speed | LAN interface speed. |
| | Autodetect: automatically adjusts the interface speed (Factory-default value). |
| | • 10Mbps: fixed speed according to network. |
| | • 100Mbps: fixed speed according to network. |
| | Autodetect is selected by default. If you encounter connection problems, select the fixed speed required by your network infrastructure. |
| Duplex Mode | LAN interface duplex mode. |
| | • Autodetect: automatically sets the duplex mode as required by your network infrastructure (Factory-default value). |
| | Half Duplex: fixed duplex mode according to network. |
| | • Full Duplex: fixed duplex mode according to network. |
| | Autodetect is selected by default. If you encounter connection problems, select the fixed duplex mode required by your network infrastructure. |
| View Defaults button | Allows you to display factory-default values. Click Apply to restore factory-default configuration. |

Note * According to server model and network configuration both MNGx Network Adapter Configuration Boxes may not be visible.

Figure 6-4. Network Settings - factory-default values

- 2. Complete the fields to comply with your network requirements and click Apply.
- 3. Log off the console.
- 4. Start the console with the new network settings from a remote computer or workstation to test the connection.
- 5. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

What To Do if an Incident Occurs?

If you are unable to connect to the console from a remote computer or workstation, one of the following problems may be the cause:

- The LAN cable may be detached.
- Network settings are incorrect.
- Your network may be down.

Modifying Internal Clock Settings 6.5.

WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

The Date/Time Settings page allows you to set up the embedded management controller's internal clock. You can either set the clock manually or connect to a Network Time Protocol (NTP) server.



WARNING

If you do not use an NTP server, the date and time will not be persistent. You will have to reset the date and time in the event of a power cut.

Prerequisites

You have Date/Time Settings permission

If you want to use NTP, you must have the IP addresses of the NTP servers you want to use

Procedure

 From the Configuration tab, click BMC Settings > Date-Time to display the Date/Time Settings page.

| | User : su | uper | System Control | Monitoring | Configuration | Maintenance |
|--|--|---|---------------------|--------------------------|-------------------|-------------|
| ✓ Global Settings Platform Managed Server Functional Profiles ✓ BMC Settings Network Date Time SNMP Messages ▷ BMC User Management ▷ Security ▷ Remote Console Settings ▷ Alert Settings | General — Time Zone 〔 ☑ Aa ④ Us | GMT +00:00) England, Irelan djust for daylight savings tim ser Specified Time * Date (Month, Day, Year) Time ynchronize with NTP server Primary Time Server Secondary Time Server Apply | id, Portugal e * | 27 , 2009]: 32 (hh.n |] nm:ss)]* | |
| | | | | | | ~ |

| General | | | | | |
|----------------------------------|---|--|--|--|--|
| Time Zone | Use this drop-down list to set the difference between local and universal time. | | | | |
| Adjust for daylight savings time | Select this option to automatically adjust to local daylight savings time (DST). | | | | |
| User Specified Time | This option allows you to manually set the server internal clock. Enter manually both the date and local time and check that the Time Zone setting is correct. | | | | |
| Synchronize with NTP Server | This option allows you to enter the IP addresses of the NTP servers you want to use. You must use the Time Zone drop-down list. | | | | |
| | | | | | |
| View Defaults button | Allows you to display factory-default values. | | | | |

Figure 6-5. Date/Time Settings - factory-default values

- 2. If required, change the Time Zone value and select or clear the Adjust for daylight savings time check box.
- 3. Click either User Specified Time or Synchronize with NTP Server, complete the appropriate fields and click Apply.
- 4. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.6. Configuring the Board and Security Message Log

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

This section describes how to configure the Board and Security Messages log, which records non-IPMI events, such as power-on errors, user authentication, connections, security violation, log deletion or firmware upgrade.

Note Events compliant with the IPMI standard are recorded in the System Event log. You can set up SEL messaging policies through Alert Settings.

mportant Alert and message transmission to the iCare Console must be set up directly from the iCare Console interface. Please refer to the *iCare Console User's Guide* for details.

Prerequisites

You have Log Settings permission

You have configured your SMTP / SNMP server for messaging

You have configured your Syslog / SNMP server for messaging

Procedure

 From the Configuration tab, click BMC Settings > Messages to display the Event Management - Settings page:

| | User : super | ſ | Power Control | Monitoring | Configuration | Maintenance |
|--|-----------------------------|----------------------------|------------------------------------|---------------|---------------|-------------|
| | Event Management - Settings | 3 | | | | ^ |
| General Settings BCE Blade Network Date-Time | SNMP Configurat | | | | | 7 |
| SNMP | | Logging Enabled * | | | | |
| Messages FPIF Image Selection | Destination IP | Port # | | Community | | 1. |
| ©User Management | | *162 | | *public | | - |
| - | | * 162 | | *public | | * |
| ▷Security Management | | * 162 | | * public | | * |
| ▷Alert Settings | | * 162 | | * public | | * |
| | | *162 | | *public | | * |
| | | Click here to view | the kira100 SNN | <u>IP MIB</u> | | |
| | SysLog Configura | ntion | | | | _ |
| | 🔲 Ena | ble Syslog Forwarding | * | | | ≡ |
| | | IP Addres | s | | * | |
| | | Apply * Stored value is | View Defaults s equal to the de |] fault. | | |

| | SNMP Configuration | | | | |
|--------------------------|---|--|--|--|--|
| SNMP Logging Enabled | When selected, this option allows Board and Security messages to be sent by SNMP trap. | | | | |
| Destination IP | SNMP manager IP address and port number | | | | |
| Port # | | | | | |
| Community | SNMP community name for the SNMP manager (example: public) | | | | |
| Click here to view link | This link allows you to view and save, as a .txt file, the system MIB file. This file is required by your SNMP Manager to interpret trap messages. | | | | |
| | SysLog Configuration | | | | |
| Enable Syslog Forwarding | When selected, this option allows Board and Security messages to be sent by the syslog protocol, to centralize the Board and Security logs on a Linux platform. | | | | |
| IP Address | Linux platform IP address. | | | | |

Figure 6-6. Event Management Settings - factory-default values

- 2. Complete the fields as required.
- 3. Click Apply.
- 4. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.7. Managing Users



If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

Access to console features and data is based on users, groups and permissions. From the **Configuration** tab, use the **User Management** menu to implement a permission-based user management policy that enables users to only access the features and data they require.

6.7.1. Creating a User Account

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

The server is delivered with two predefined groups and one predefined user:

- Admin group with full permissions for full system access and one default super user.
- users group with no permissions and no predefined users.

You can create and manage users and associated permissions to suit your needs.

Note Predefined groups and users cannot be renamed or deleted, but the default **super** user password can be changed. Permissions for the default **Admin** group are not modifiable. Permissions for the default **users** group are modifiable.



mportant The system is equipped with a host-independent processor and memory unit which are limited in terms of processing instructions and memory space. To guarantee an acceptable response time, you are advised:

- Not to exceed 25 simultaneous user connections.
- Not to exceed 150 user accounts.

Prerequisites

You have User/Group Management permission

You have created the group that the user is to be a member of

Note If you have not created the group that the user is to be a member of, the newly created user will be attached to the predefined **users** group.

- 1. From the Configuration tab, click BMC User Management > Users to display the User Management page.
- 2. Click Create to display the User Creation dialog.

| | | | | | | | +2Logout |
|---|----------|-----------------------------|---|----------------------|--------------------|---------------|-------------|
| | | Use | r: super | System Control | Monitoring | Configuration | Maintenance |
| ∇ Global Settings Platform Managed Server Functional Profiles | User Mai | nagement ┌─ General ──── | | Create | 3 | | |
| ⊽ BMC Settings Network Date-Time SNMP Messages | | | User Accounts super | Modify | | | |
| ⊽BMC User Management | | | | | | | J |
| Users Groups | | User Creation | | | | | ן 🗌 |
| Password | | User Name * | | Full Use | r Name | | |
| ⊳Security | | Password * | | ength:4) Confirm Pas | sword * | | |
| ⊳Remote Console Settings | | Group Membership | users (default setting) ⊻ | | | | |
| ⊳Alert Settings | | Email Address | | | | | |
| | | Phone Number | | | | | ≣ |
| | | | User must change passwor (Note that the Change Passwork) | | he evenled for the | | |
| | | | Account is enabled | ora permission must | be enabled for the | group) | |
| | | | Create | Cancel | | | |
| | | * Mandatory | | | | | |
| | | | | | | | J |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | ~ |
| | | | | | | | |

| | User Creation |
|------------------|---|
| User Name | Name the user will use to log on (often a "short name"). |
| | Name limited to 32 characters. |
| | The following characters are not allowed: \"'`&*% ~?/ and space. |
| Full User Name | The user's full name. |
| | Name limited to 32 characters. |
| | The following characters are not allowed: \"'`&*% ~?/ and space. |
| Password | The password the user will use to log on. |
| | Minimum password length: 4 characters. |
| Confirm Password | Maximum password length: 32 characters. |
| | • The following character is not allowed: space. |
| Group Membership | Use this drop-down list to select the group that this user is to be a member of, according to the permissions you want the user to have. Note: If you do not select a group, the newly created user is automatically attached to the predefined users group. The Change Password permission is NOT enabled for the predefined users group. |

| User Creation | | | | |
|--|--|--|--|--|
| Email Address | User's email address. Example: john.smith@acme.com. | | | |
| Phone Number | User's phone number. Use only arabic numerals and optionally the characters+ with NO spaces. Examples: 0625252525, +33.1.25.25.25.25 | | | |
| User must change password at next logon | When selected, this option forces the user to change his/her password at next logon. Note: The Change Password permission must be enabled for the group otherwise the user will not be able to log on. | | | |
| Account is enabled | When cleared, this option makes the user account unavailable: the user's account information is maintained but it is no longer possible to log on using this account. | | | |

Figure 6-7. User Management - User Creation

- 3. Complete the fields as required.
- 4. Click Apply. The user is created and appears in the User Accounts box.
- 5. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.7.2. Displaying User Account Details



If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

For easy user management, you can display the basic details of any user account at any time. You may want to use this feature, for example, to check user account details after the creation or modification of a user account or to check whether a user is locked out or not.

Prerequisites

You have User/Group Management permission

- 1. From the Configuration tab, click BMC User Management > Users to display the User Management page.
- 2. In the User Accounts list, select a user to display the Account Details box.

| | | | | | | -togout |
|---|-----------------|--|--|------------|---------------|-------------|
| | | User : super | System Control | Monitoring | Configuration | Maintenance |
| ✓ Global Settings Platform Managed Server Functional Profiles ✓ BMC Settings Network Date-Time SNMP Messages ✓ BMC User Management | User Management | Genera User Acco super | Create | | | |
| Usern Groups Password ▷Security ▷Alent Console Settings ▷Alert Settings | | User na Full use Group n User V Acce | nt Details me: Supervis nembership: Admin runust change password at next ount is enabled ter is not locked out and may lo | t logon | | |

| Account Details | | | | |
|--|--|--|--|--|
| User name | Name the user uses to log on (often a "short name"). | | | |
| Full user name | The user's full name. | | | |
| Group membership | Group that this user is a member of (and consequently the permissions the user has). | | | |
| Email address | User's email address. This entry does not appear if the field is not completed when the user is created. | | | |
| Phone number | User's phone number. This entry does not appear if the field is not completed when the user is created. | | | |
| User must change password at next logon | When selected, this option forces the user to change his/her password at next logon. Note: The Change Password permission must be enabled for the group otherwise the user will not be able to log on. | | | |
| Account is enabled | When selected, the user account is active and the user is able to log on. | | | |

Figure 6-8. User Management - Account Details

6.7.3. Modifying a User Account

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

You can edit user account information at any time.

6.7.3.1. Updating Details

You can change user account details (user name, full user name, password, email address and phone number) at any time. You might want to do this, for example, if a resource name is changed or if a resource changes roles in your organization.

Note You cannot change the account details of the predefined **super** user. However, the default **super** user password can be changed through the **Password Management** page, as detailed in Modifying the Password, on page 6-24.

Prerequisites

You have User/Group Management permission.

Procedure

- 1. From the Configuration tab, click BMC User Management > Users to display the User Management page.
- 1. From the Configuration tab, click > Users to display the User Management page.
- 2. Select the user account you want to modify in the User Accounts list box and click Modify to open the User Account Modification box.
- 3. Modify one (or more) of the following fields depending on your needs:
 - User Name,
 - Full User Name,
 - Password and Confirm Password,
 - Email Address,
 - Phone Number.

Note For details about these fields, see Figure 6-7, on page 6-16.

- 4. Click Modify. User account details are changed.
- 5. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.7.3.2. Changing Group

A group is a collection of users who have the same permission requirements. Users automatically inherit the permissions of the group to which they belong. You can change permissions assigned to users by changing the group they are member of.

Prerequisites

The group must be created

You have User/Group Management permission

Procedure

- 1. From the Configuration tab, click BMC User Management > Users to display the User Management page.
- 2. Select the user account you want to modify in the User Accounts list box and click Modify to open the User Account Modification box.
- 3. Select in the Group Membership drop-down list the wanted group, according to the permissions you want the user to have.
- 4. Click Modify. The user's group membership is updated.
- 5. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.7.4. Disabling/Enabling User Accounts

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

At times, you may need to make user accounts unavailable. You may want to use this feature, for example, when a maintenance intervention is scheduled. When you disable a user account, that user's account information is maintained but the user can no longer log on. The user account remains inactive until it is reenabled.

Prerequisites

You have User/Group Management permission

Procedure

- From the Configuration tab, click BMC User Management > Users to display the User Management page.
- 2. Select the user account you want to modify in the User Accounts list box and click Modify to open the User Account Modification box.
- 3. To disable the account, clear the Account is enabled check box; to enable the account, select it.
- 4. Click Modify. The account is updated.
- Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.7.5. Forcing User Password Changes



If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

The following procedure describes how to force a user to change his/her password at the next logon.

Prerequisites

You have User/Group Management permission

The Group has Change Password permission

- 1. Check that Change Password permission is enabled for the group to which the user belongs:
 - a. From the Configuration tab, click User Management > Groups to display the Group Management page.
 - b. Select the group to which the user belongs and click **Permissions** to display the **Group Permissions** page.
 - c. Check that Change Password permission is enabled for the group. If this is not the case, enable the Change Password permission for the group.
- 2. From the Configuration tab, click User Management > Users to display the User Management page.
- Select the user account in the User Accounts list box and click Modify to open the User Account Modification box.
- 4. Select the User must change password at next logon check box.
- 5. Click Modify. The user will be requested to change his/her password the next time he/she tries to log on.
 - Note Once the user has changed his/her password, the User must change password at next logon check box of his/her account is automatically cleared.

6.7.6. Deleting a User Account



If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

You can delete a user account when no longer needed. The deleted user account will be removed from the associated group.

Prerequisites

You have User/Group Management permission

- 1. From the Configuration tab, click BMC User Management > Users to display the User Management page.
- 2. Select a user in the User Account list box and click Delete. The User Account Deletion box appears.

| | | | | | | Logout |
|--|-----------------|--|-----------------------------------|------------|---------------|-------------|
| | | User : super | System Control | Monitoring | Configuration | Maintenance |
| ♥ Global Settings Platform Managed Server Functional Profiles ♥ BMC Settings Network Date-Time SIM/P Messages | User Management | General User Accounts smith super | Create Modify Delete | | | ^ |
| ♥ BMC User Management Hency Groups Password ▷ Security ▷ Remote Console Settings ▷ Alert Settings | | User Account Dele Are you sure you wa Delete | etion ant to delete user accou | nt smith? | | |
| | | | | | | ~ |

Figure 6-9. User Account Deletion

- 3. Click Delete to confirm. The user is removed from the list and from the associated group.
- 4. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.7.7. Manually Unlocking a User Account

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

The user lockout feature disables a user account when a certain number of failed logons occur due to wrong passwords. When a user lockout duration is specified, the user account is automatically unlocked after the specified time. If a user lockout duration is not specified, the user account must be unlocked manually.

Prerequisites

You have User/Group Management permission

- From the Configuration tab, click BMC User Management > Users to display the User Management page.
- 2. Select the locked-out user in the User Account list. The following message is displayed in the Account Details box.

| | | | | | | 📲 Logout |
|--|-----------------|--------------|--|---------------------------|---------------|-------------|
| | | User : super | System Control | Monitoring | Configuration | Maintenance |
| ✓ Global Settings Platform Managed Server Functional Profiles ✓ BMC Settings Network Date-Time SNMP Messages ✓ BMC User Management User Groups Password ▷ Security ▷ Remote Console Settings ▷ Alert Settings | User Management | Account is e | Modify Delete ills ust change password at next | smith users : logon | | |
| | | | | | | ~ |
| | | | | | | |

Figure 6-10. User Management - Locked-out user

3. Click Modify to display the User Account Modification box.

| | | | | | 📲 Logout |
|---|--|---|---------------------|---------------|-------------|
| | User : super | System Control | Monitoring | Configuration | Maintenance |
| ∀ Global Settings Platform Managed Server | User Management | | | |] |
| Functional Profiles ▽BMC Settings Network Date-Time SNMP Messages | User Accou smith super | Create Create Modify Delete | | | |
| ♥BMC User Management Users Groups Password | User Account Modification User Name * | Full User 1 | Name | |] |
| ⊳Security | Password * | (min length:4) Confirm Passw | vord * | | |
| ⊳Remote Console Settings ⊳Alert Settings | Group Membership users (default setting Email Address Phone Number | | | | |
| | (Note that the Chang ✓ Account is enable | password at next logon. Je Password permission must be d Modify Cancel | e enabled for the g | iroup) | |
| | This user is locked out a | nd may not log on (indefinitely) | | Unblock | |
| | | | | | |
| | | | | | |
| | | | | | * |

4. Click Unblock. The user account is unlocked and the user can now log on again.

6.7.8. Modifying the Password



If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

The following procedure explains how to change the current user account password.

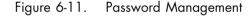
Prerequisites

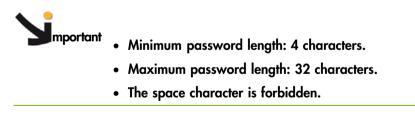
You have Change Password permission

Procedure

 From the Configuration tab, click BMC User Management > Password to display the Password Management page.

| | | | | | | Logout |
|---|---------------------|----------------------|---------------------|------------|---------------|-------------|
| | User : | super | System Control | Monitoring | Configuration | Maintenance |
| ∇ Global Settings Platform | Password Management | | | | | ^ |
| Managed Server Functional Profiles | | Current User Passy | vord Modification — | | | |
| ∀ BMC Settings | | Old Password | | | | |
| Network | | New Password | | | | |
| Date-Time SNMP | | Confirm New Password | | | | |
| Messages | | | Apply | | | |
| ♥BMC User Management Users Groups Password | | | | | | |
| ⊳Security | | | | | | |
| ⊳Remote Console Settings | | | | | | |
| PAlert Settings | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | _ |
| | | | | | | ~ |
| | | | | | | |





- 2. Complete the 3 fields.
- 3. Click Apply. The new password is now valid and must be used when you next log on.

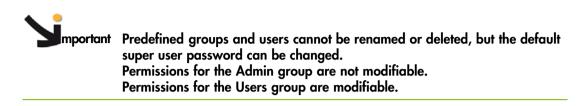
6.7.9. Creating a Group

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

The Hardware Console is delivered with two predefined groups and one predefined user:

- Admin group with full permissions for full system access and one default super user.
- Users group with no permissions and no predefined users.

You can create and manage new groups and associated permissions to suit your needs.



Prerequisites

You have User/Group Management permission

- 1. From the Configuration tab, click BMC User Management > Groups to display the Group Management page.
- 2. Click Create to open the Group Creation box.

| | | | | | | 📲 Logout |
|---|---------------|--------------------------|----------------|-------------------|---------------|-------------|
| | | User:super | System Control | Monitoring | Configuration | Maintenance |
| ∇ Global Settings Platform Managed Server Functional Profiles | Group Managen | nent - General | | | | <u></u> |
| ⊽ BMC Settings Network Date-Time SNMP Messages | | Groups Admin users | Select | ied Group Members | | |
| ♥ BMC User Management Users Groups Password | | | | | | |
| ⊳Security | | Create Permissions | Delete | | | |
| ⊳Remote Console Settings | L | | | | | |
| ▷Alert Settings | 5 | Group Creation | | | | |
| | | New Group Name | Create | Cancel | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | ~ |

| Group Creation | | | | |
|---|--|--|--|--|
| New Group Name Name given to the group. Restrictions: | | | | |
| | • Name limited to 32 characters. | | | |
| | • Forbidden characters: \"'`&*% ~?/ and space. | | | |

Figure 6-12. Group Management - Group Creation

- 3. Enter the group name in the New Group Name field and click Create. The group is created and appears in the Groups box. You can now proceed to define permissions and set up users for the group.
- 4. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.7.10. Configuring Permissions

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

The features accessible to a user depend on the permissions defined for the group the user belongs to. This section describes how to specify and update the permissions that apply to users associated with a group.

Prerequisites

You have User/Group Management permission

You have created the group for which you want to set permissions

Procedure

1. From the Configuration tab, click BMC User Management > Groups to display the Group Management page.

2. Select the group and click **Permissions** to display the **Group Permissions** page.

| | | | | | | ⊲ ∐Logout |
|---------------------------------------|-------------------|-------------|---|------------|---------------|------------------|
| | | User: super | System Control | Monitoring | Configuration | Maintenance |
| | Group Permissions | | | | | ^ |
| ∇ Global Settings Platform | | | | | | |
| Managed Server Functional Profiles | | | ermissions /iew / Modify permissions for | | | |
| ▽BMC Settings | | | Group users 👻 | | | |
| Network Date-Time SNMP | | | Web Connection Permissions | | | |
| Messages | | Alert S | ettings & Clear SEL : No 💌 | | | |
| ∀BMC User Management Users | | Auti | nentication Settings : No 💌 | | | |
| Groups | | | Change Password : No 🍟 | | | |
| Password | | | Date/Time Settings : No 🛛 | | | |
| ⊳Security | | | Firmware Update : No 👻 | | | |
| ▶Remote Console Settings | | IPMI ma | ny use SOL payload : No 🛛 | | | |
| PAlert Settings | | | Log Settings : No 🔽 | | | |
| | | | Log View : No 😽 | | | |
| | | Mainte | enance/Board Reset : No 👻 | | | |
| | | | Network Settings : No 😽 | | | |
| | | | Power Control : No 😽 | | | |
| | | RC Keybo | ard/Mouse Settings : No 🔽 | | | |
| | | RC | settings (Encoding) : No 😽 | | | |
| | | RC settings | s (Exclusive Access) : No 🔽 | | | |
| | | R | C settings (Hotkeys) : No 🍟 | | | |
| | | RC setti | ings (Monitor Mode) : 🛛 No 🔤 | | | |
| | | | RC settings (Type) : No 🍟 | | | |
| | | Rem | ote Console Access : No 🍟 | | | |
| | | | SNMP Settings : No 🍟 | | | |
| | | | SSH/Telnet Access : No 💌 | | | |
| | | SSL Certi | ficate Management : No 🛛 | | | |
| | | | Security Settings : No 👻 | | | |
| | | User/0 | Group Management : No 🛛 | | | |
| | | | irtual Media Upload : No 💌 | - | | |
| | | | of-Band Connection Permission | | | |
| | | | PMI Privilege Level : No Acc SNMP v3 Access : Deny | cess 🕶 | | |
| | | | | | | |
| | | | Apply View Defaults | | | |

| | Group Permissions |
|--|--|
| View / Modify Permissions for Group | This drop-down list allows you to select a group in order to view and/or modify the permissions set for the selected group. |
| Web Connection Permissions | This list allows you to enable or disable console features for the selected group. Select either 'Yes' or 'No' to enable or disable the feature(s) associated with each permission and click 'Apply'. Use Tables 6-1 and 6-2 to help you select permissions. Note: Certain features are accessible to all users and the associated non-configurable permissions are not listed in this page. |
| Out-of-Band Connection Permissions | The 'IPMI Privilege Level' drop-down list allows you to set a role for the selected group. See Table 6-3 and the IPMI specification for more details. |
| SNMP v3 Access | User accounts with this permission can send SNMP v3 commands through the LAN. |

Figure 6-13. Group Permissions

- 3. Use Tables 6-1 and 6-2 below to help you select the permissions you want to assign to the selected group.
- 4. Click Apply to validate the selected permissions for the group.
- 5. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

The following tables list permissions and associated features.

Console: Non-Configurable Permissions

| Feature | Tab |
|---|----------------|
| Power Information: Viewing & Refreshing | System Control |
| Sensor Status | Monitoring |
| System Event Log: Viewing & Refreshing | Monitoring |
| Management Controller | Maintenance |
| FRU | Maintenance |
| Firmware Version | Maintenance |
| Connected Users | Maintenance |

 Table 6-1.
 Hardware Console: Non-configurable permissions

Console: Configurable Permissions

| Configurable Permission | Feature | Tab |
|-----------------------------------|--|----------------|
| Alert Settings & Clear SEL | System Event Log: Clearing | Monitoring |
| | Filters | Configuration |
| | Policies | Configuration |
| | LAN Destinations | Configuration |
| | General | Configuration |
| | Identification LED | Maintenance |
| Authentication Settings | Authentication | Configuration |
| Change Password | Password | Configuration |
| Date/Time Settings | Date-Time | Configuration |
| Firmware Update | Listed Firmware Upgrades | Maintenance |
| IPMI may use SOL payload | Serial-Over-Lan connection (User accounts with this permission can launch a SOL session) | - |
| Log Settings | Messages | Configuration |
| Log View | Messages | Monitoring |
| Maintenance/Board Reset | Reset Management Controller | Maintenance |
| Maintenance/Board Reset | Hardware Exclusion | Maintenance |
| Network Settings | Platform | Configuration |
| | Managed Server | Configuration |
| | Functional Profile Settings | Configuration |
| Network Settings | Network | Configuration |
| Power Control | Power Management | Power Control |
| RC Keyboard/Mouse Settings | Keyboard & Mouse | Configuration |
| RC settings (Encoding) | Transmission Encoding | Configuration |
| RC settings (Exclusive Access) | Miscellaneous Remote Console Settings (Exclusive Access Mode) | Configuration |
| RC settings (Hotkeys) | Mouse Hotkey Remote Console Button Key | Configuration |
| RC settings (Monitor mode) | Miscellaneous Remote Console Settings (Monitor Mode) | Configuration |
| RC settings (Type) | Reserved | - |
| Remote Console Access | Preview | System Control |
| | Launch | System Control |
| Remote Console Access | Reset Keyboard/Mouse (USB) Reset USB Reset Video Engine | Maintenance |
| SSH/Telnet Access | SSH/Telnet connection (User accounts with this permission can send SSH/Telnet commands through the LAN) | - |
| SSL Certificate Management | SSL Certificate | Configuration |

| Configurable Permission | Feature | Tab |
|-------------------------|----------------------|----------------|
| Security Settings | Encryption | Configuration |
| | User Logon Policy | Configuration |
| | Power Button Lockout | Configuration |
| | User Lockout | Configuration |
| User/Group Management | Users | Configuration |
| | Groups: Management | Configuration |
| | Groups: Permissions | Configuration |
| Virtual Media Upload | Listed Virtual Media | System Control |

Table 6-2. Hardware Console: Configurable permissions

| Out-of-Band Con | nection Permissions |
|----------------------|--|
| IPMI Privilege Level | Possible values: |
| | No Access (default) |
| | • Callback |
| | • User |
| | Operator |
| | • Administrator |
| | • OEM |
| | For more details about IPMI privilege levels, refer to the IPMI specification. |
| SNMP v3 Access | SNMP v3 connection (User accounts with this permission can send SNMP v3 commands through the LAN). Possible values: |
| | • Deny (default) |
| | • Read-only |
| | • Read-Write |

Table 6-3. IPMI: Out-of-Band privileges

6.7.11. Viewing Group Membership

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

For easy group management, you can display the members of any group at any time. You may want to use this feature, for example, to check group membership after the creation or modification of a user account.

Prerequisites

You have User/Group Management permission

Procedure

- 1. From the Configuration tab, click BMC User Management > Groups to display the Group Management page.
- 2. In the Groups list, select a group. The group members appear in the Selected Group Members list.

| | | User : super | System Control | Monitoring | Configuration | Maintenance |
|---|--------------|--------------------------|-----------------|------------------|---------------|-------------|
| ∇ Global Settings Platform Managed Server Functional Profiles | Group Manage | General | | | | |
| ∀ BMC Settings Network Date-Time SNMP Messages | | Groups Admin users | Selection Smith | ed Group Members | | |
| ▽ BMC User Management Users Groups Password | | | <u>8</u> | | <u>~</u> | |
| ⊳Security | | Create Permissions | Delete | | | |
| ⊳Remote Console Settings | | | | | | |
| ▷Alert Settings | | | | | | |
| | | | | | | |
| | | | | | | ~ |
| | | | | | | |

Figure 6-14. Group Management

6.7.12. Deleting a Group

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

You can delete an empty group when no longer needed.



Prerequisites

You have User/Group Management permission

No users are members of the group to be deleted, i.e. users have been deleted or moved to another group

Procedure

- 1. From the Configuration tab, click BMC User Management > Groups to display the Group Management page.
- 2. Select the group you want to delete in the **Groups** list box and click **Delete** to open the **Group Deletion** box.

| | Us | er : super System | m Control Monitoring | Configuration | Maintenance |
|---|---------------------------------------|-------------------------------|------------------------|---------------|-------------|
| Global Settings Platform Managed Server Functional Profiles | Group Management | | | | î |
| ▽ BMC Settings Network Date-Time SNMP Messages | Groups Admin stoups If users | | Selected Group Members | | |
| ♥BMC User Management Users Stours Password | | | × | ~ | |
| Security | C | reate Permissions Delete | | | |
| PRemote Console Settings | | | | | |
| PAlert Settings | Group De | letion | | | |
| | | Are you sure you want to dele | te group groupTest? | | |
| | | Delete | Cancel | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | ~ |

Note If the selected group contains users, the **Delete** button is not available.

Figure 6-15. Group Management - Group Deletion

- 3. Click Delete. The group is deleted and disappears from the Groups box.
- 4. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.8. Configuring Security Parameters



If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

For optimum security, a comprehensive set of security features can be customized to suit your requirements. These features range from securing web connections to controlling the use of the physical power button.

6.8.1. Forcing HTTPS Connections

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

This feature allows you to secure Web connections to the console and to control the encryption mode of the KVM protocol, which is activated when using the Remote System Console.



ant By default, a generic certificate is delivered to connect to the console with the HTTPS protocol. For optimum security, you are advised to generate and install your own certificate.

Note By default, HTTPS connections use port 443. You may have changed this value, as described in Configuring Network Settings for Remote Access, on page 6-6.

Prerequisites

You have Security Settings permission

Procedure

 From the Configuration tab, click Security > Encryption to display the Encryption Management page.

| | User : su | per l | System Control | Monitoring | Maintenance |
|--|------------------------|--|----------------|------------|-------------|
| ∇ Global Settings Platform Managed Server Functional Profiles | Lencryption Management | HTTP Encryption | (HTTPS) | , | ^ |
| ♥ BMC Settings Network Date-Time SNMP Messages ♥ BMC User Management Users Groups Password | | KVM Encryption - KVM Encryption C (Apply) | | Force | |
| ✓ Security Encryption SSL Certificate User Logon Policy Authentication Power Button Lockout User Lockout VserMote Console Settings | | | | | |
| PAlert Settings | | | | | |
| | | | | | ~ |

| | HTTP Encryption (HTTPS) |
|----------------------------|--|
| Force HTTPS for Web Access | The HTTPS protocol requires the use of an URL in one of the following formats: |
| | • https:// <ip address=""></ip> |
| | • https:// <hostname></hostname> |
| | IMPORTANT: if this option is selected, the HTTP protocol (http:// <ip address="" hostname="" or="">) can no longer be used to connect to the console.</ip> |
| | KVM Encryption |
| KVM Encryption | This option controls the encryption of the KVM protocol. This protocol is used by the Remote System Console to transmit the screen data to the administrator machine and the keyboard and mouse data back to the host. |
| | • If set to Off, encryption is disabled. |
| | • If set to Try, the Remote System Console tries to make an encrypted connection. If the encrypted connection cannot be established, an unencrypted connection is used instead. |
| | • If set to Force, the Remote System Console tries to make an encrypted connection. If the encrypted connection cannot be established, an error is reported. |
| | · |
| View Defaults button | Allows you to display factory-default values. Click Apply to restore factory-default configuration. |

Figure 6-16. Encryption Management - factory-default values

- 2. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.
- 3. Select the required options and click Apply.

6.8.2. Getting and Installing a New SSL Certificate

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

You can secure Web connections by configuring the console to use the HTTPS protocol.

A valid SSL certificate is required to use the HTTPS protocol. By default, a temporary certificate is delivered. For optimum security, you are advised to generate and install your own certificate.

Note By default, HTTPS connections use port 443. You may have changed this value, as described in Configuring Network Settings for Remote Access, on page 6-6.

Prerequisites

You have SSL Certificate Management permission

Procedure

1. From the Configuration tab, click Security > SSL Certificate to display the SSL Certificate Management page.

| | | | | | | -√_ Logo | but |
|---|-------------------------|---|---|------------|---------------|-----------------|-----|
| | Us | er : super | System Control | Monitoring | Configuration | Maintenance | |
| ⊽ Global Settings Platform Managed Server Functional Profiles | SSL Certificate Managem | ent — Certificate Signing Req | uest (CSR) ——— | | | | ^ |
| ✓ BMC Settings Network Date-Time SNMP Messages ✓ BMC User Management Users Groups Password ✓ Security Encryption SSL Certificate User Logon Policy Authentication Power Button Lockout User Lockout ▷ Remote Console Settings ▷ Altert Settings | | Common Name Organizational Unit Organization Locality/City State/Province Country (ISO Code) Email Challenge Password Confirm Challenge Password Key Length (bits) * Stored value | 1024 v = Create is equal to the default | | | | |
| | | | | | | | ~ |

| Cer | tificate Signing Request (CSR) |
|----------------------------|--|
| Common Name | "Fully Qualified Domain Name" (FQDN) (example: hostName.DomainName.Top-LevelDomain). If the Common Name differs from the network name, a security warning will pop up when the system is accessed using HTTPS. |
| Organizational Unit | Generally the name of the department (within your organization) using the system (example: Research and Development). |
| Organization | Name of your organization. |
| Locality/City | Name of your city. |
| State/Province | Name of your state, province or region. |
| Country (ISO Code) | ISO Code for your country (example: FR for France). |
| Email | Generally the administrator's email address. |
| Challenge Password | Depending on your certification authority, you may need to define a challenge password to authorize later changes to the certificate (example: revocation of the |
| Confirm Challenge Password | certificate). The minimum length of this password is four characters. |
| Key Length (bits) | Length of the generated key in bits. |
| | Generally 1024 bits. Longer keys may result in slower connection response time. |

Figure 6-17. SSL Certificate Management

- 2. Complete the fields and click Create to generate your CSR.
- Click Download to save the CSR to your computer and send it to the Certification Authority, which will check your information, generate a signed Certificate and send it back to you.
- 4. When you receive your signed certificate, use the Certificate Upload box to install the certificate.
- 5. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.8.3. Configuring the Logon Policy

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

This page allows you to define how a user session should be managed in terms of the number of open sessions, password aging and idle timeout.

Prerequisites

You have Security Settings permission

You log on with the user account you want to configure

Procedure

1. From the Configuration tab, click Security > User Logon Policy to display the User Logon Policy Management page.

| | | | | | | -Logout |
|---|-----------------------|------------|--|------------|---------------|-------------|
| | | User:super | System Control | Monitoring | Configuration | Maintenance |
| ✓ Global Settings Platform Managed Server Functional Profiles ✓ BMC Settings Network Date-Time SIN/IP | User Logon Policy Mar | - General | | - | | 1 |
| Messages ▼BMC User Management Users Groups Password | | Apply | View Defaults is equal to the default | l. | | |
| ▼ Security Encryption SSL Certificate User Logon Policy Authentication Power Button Lockout User Lockout | | | | | | |
| ▷Remote Console Settings | | | | | | |
| ⊳Alert Settings | | | | | | |
| | | | | | | ~ |

| General | | | | | |
|--|---|--|--|--|--|
| Enable User Single Logon | When this check box is selected, the current user account is limited to a single session logon: once connected, it is not possible to log on to the console again using the same user account. | | | | |
| Enable User Password Aging | When this check box is selected, the user has to change his/her password at the specified interval. | | | | |
| User Password Aging Interval (Days) | Password change interval, in days. | | | | |
| Idle Timeout (Minutes) | Time after which the user is automatically disconnected, in minutes. | | | | |
| View Defaults button | Allows you to display factory-default values. Click Apply to restore factory-default configuration. | | | | |

Figure 6-18. User Logon Policy Management - factory-default values

- 2. Select or clear the check boxes as required and click Apply.
- 3. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.8.4. Managing Authentication

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

By default, the console is configured to use its own Local Authentication mechanism to authenticate and connect users. You can either use this mechanism and manually create groups and user accounts or use your organization's LDAP or RADIUS server to use existing user accounts.



- If you select LDAP authentication management, the LDAP database is only used for password verification. User permissions and private settings are still stored locally. You need to create user accounts via the console (User Management page) if you want users to log on using an LDAP server.
- The default "super" user account can always be used, whatever the authentication settings.

Prerequisites

You have Authentication Settings permission

For LDAP or RADIUS authentication management, you have configured the DNS server from the Enterprise Network Settings page

For RADIUS authentication management, you have declared the console as a RADIUS client (name and IP address) and have defined the shared secret

Procedure

1. From the Configuration tab, click Security > Authentication to display the Authentication Management page.

| | | User: super | | System Control | Monitoring | Configuration | - Log Maintenance |
|---|--------------------|--|--------------------|----------------------|--------------------------|---------------|----------------------|
| Global Settings Platform Managed Server | ⊿ _{Authe} | ntication Management | | Cjotolin Collact | | J | |
| Functional Profiles | | General General Local Authentication * | | | | | |
| BMC Settings Network | | O LDAP | | | | | |
| Date-Time SNMP | | User LDAP Server | | | * | | |
| Messages | | Г | Enable Secure LDAP | * | | | |
| BMC User Management | | Port | 389 * | | | | |
| Users Groups | | Secure LDAP Port | 636 * | | | | |
| Password | | Certificate File | | Parcou | | | |
| Security Encryption | | LDAP server Base DN | | | * | | |
| SSL Certificate User Logon Policy | | LDAP Server Type | Generic LDAP S | erver 💙 * | | | |
| Authentication Power Button Lockout | | Login-name Attribute | | | * | | |
| User Lockout | | User-entry ObjectClass | | | * | | |
| Remote Console Settings | | User Search Subfilter | | | * | | |
| Alert Settings | | Active Directory Domain | | | * | | |
| | | 0.0400 | | | | | |
| | | O RADIUS | | | | | |
| | | Server | Shared Secret | | Acc. Time Port (sec.) | | |
| | | 1. | | 1812 * | 1813 * 1 | * 3 | * |
| | | | | | Global Authentica | tion Type PAP | * * |
| | | | | More Entries | | | |
| | | | | | | | |
| | | | Apply | View Defaults | | | |
| | | | | is equal to the defa | ult. | | |

| | General |
|--|--|
| Local Authentication | Select to enable local console authentication. |
| LDAP | Select to enable LDAP server authentication. |
| User LDAP Server | Enter LDAP server hostname or IP address. |
| Enable Secure LDAP | Select to enable secure LDAP server authentication. |
| • Port | Enter the LDAP server port number used to listen to authentication requests. |
| Secure LDAP Port | Enter the secure LDAP server port number used to listen to authentication requests. |
| Certificate File | Browse to select the secure connection certificate supplied by the secure LDAP server administrator. |
| LDAP Server Base DN | Enter the starting node to search for user accounts. Example: dc=users,dc=domain,dc=com |
| LDAP Server Type | Enter LDAP server type: |
| | Novell Directory Service if you are using Novell eDirectory. |
| | Microsoft Active Directory. |
| | Generic LDAP Server if you are using any other LDAP directory. |
| Login-name Attribute | If you have selected Novell Directory Service or Microsoft Active Directory, leave these fields blank to use the directory's default value. |
| | • Logon Name Attribute: LDAP attribute used as user name to connect to the LDAP directory Example: cn. |
| | User Entry Object Class: object class that identifies a user in the directory Example: organizationalPerson. |
| User-entry ObjectClass | If you have selected Novell Directory Service or Microsoft Active Directory, leave these fields blank to use the directory's default value. |
| | Logon Name Attribute: LDAP attribute used as user name to connect to the LDAP directory Example: cn. |
| | • User Entry Object Class: object class that identifies a user in the directory Example: organizationalPerson. |
| User Search Subfilter | Restricts the search to certain user accounts. (example: (&(objectClass=person)(ou=System Validation))) |
| Active Directory Domain | (Microsoft Active Directory only): Active Directory domain as it is configured in your Active Directory server. Example: users.domain.com |
| RADIUS | Select to enable RADIUS authentication |
| Server | Enter the RADIUS server hostname or IP address. |

| | General |
|----------------------------|---|
| • Shared Secret | A shared secret is a text string used as a password between the RADIUS client and the RADIUS server. You can use any standard alphanumeric and special characters. A shared secret may consist of up to 128 characters in length and may contain both lowercase and uppercase letters (A-Z,a-z), numerals (0-9) and other symbols (all characters not defined as letters or numerals) such as an exclamation mark (!) or an asterisk (*). |
| Auth. Port | Enter the RADIUS server port number used to listen to authentication requests (#1812 by default). |
| Acc. Port | Enter the RADIUS server port number used to listen to accounting requests (#1813 by default). |
| • Timeout (sec.) | Enter the maximum time in seconds to wait for the completion of the request. If the requested job is not completed within this interval of time it is cancelled. |
| Retries | Enter the maximum number of retries if a request cannot be completed. |
| Global Authentication Type | Select the authentication type used by the RADIUS server. |
| More Entries | If you use more than one RADIUS server, click this button to add authentication configurations. |
| View Defaults button | Allows you to display factory-default values. Click Apply to restore factory-default configuration. |

Figure 6-19. Authentication Settings - factory-default values

- 2. Depending on your needs, click Local Authentication, LDAP or RADIUS and complete the appropriate fields and click Apply.
- Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.8.5. Enabling/Disabling the LCP Power Button

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

The server is equipped with a physical power button located on the Local Control Panel (LCP). This power button can be locked to prevent tampering.

Prerequisites

You have Security Settings permission

Procedure

 From the Configuration tab, click Security > Power Button Lockout to open the Power Button Lockout Management page.

| | | | | Maadaa | 5 % | Logout |
|--|----------------------------|------------------|---------------------|------------|---------------|-------------|
| | User: sup | | System Control | Monitoring | Configuration | Maintenance |
| ∇ Global Settings Platform Managed Server Functional Profiles | Power Button Lockout Manag | General | t State: Not active | | | |
| ▽BMC Settings Network Date-Time SNMP Messages | | Activate Lockout | Deactivate Loci | Kout | | |
| ♥ BMC User Management Users Groups Password | | | | | | |
| ▼ Security Encryption SSL Certificate User Logon Policy Authentication Power Button Lockout User Lockout | | | | | | |
| ⊳Remote Console Settings | | | | | | |
| ⊳Alert Settings | | | | | | |
| | | | | | | ~ |

| | General |
|--------------------|---|
| Lockout State | 2 possible values: |
| | • Active: the power button is locked. |
| | • Not active: the power button is unlocked. |
| Activate Lockout | Disables the power button. |
| Deactivate Lockout | Enables the power button. |

Figure 6-20. Power Button Lockout Management

2. Click Activate Lockout or Deactivate Lockout, as required.

6.8.6. Configuring User Account Lockout

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

The user lockout feature disables a user account when a certain number of failed logons occur due to wrong passwords.

Prerequisites

You have Security Settings permission

You have logged on with the user account to configure

Procedure

1. From the Configuration tab, click Security > User Lockout to display the User Lockout Management page.

| | | | | | 4 | Logout |
|--|-------------------|---|---|------------|---------------|-------------|
| | <i>0</i> | User:super | System Control | Monitoring | Configuration | Maintenance |
| ✓ Global Settings Platform Managed Server Functional Profiles ✓ BMC Settings Network Date-Time SINMP Messages | User Lockout Mana | General User Lockout Threshold User Lockout Duration (Apply) | Invalid Logon Attempt Minutes (Empty = Un View Defaults | limited) * | ted) * | |
| ▽BMC User Management Users Groups Password | | - Stored Val | ue is equal to the defaul | | | |
| ▼ Security Encryption SSL Certificate User Logon Policy Authentication Power Button Lockout User Lockout | | | | | | 2 |
| ⊳Remote Console Settings | | | | | | |
| CAlert Settings | | | | | | |
| | | | | | | |

| General | | | | | |
|------------------------|---|--|--|--|--|
| User Lockout Threshold | Maximum number of invalid logon attempts before locking the user account. Note: If you leave this field empty, the user account will never be locked. | | | | |
| User Lockout Duration | Enter a time in minutes during which the user account is to remain locked. Once this time is passed, the user account is automatically unlocked. Note: If you leave this field empty, a locked user account stays locked until you unlock it manually. | | | | |
| View Defaults button | Allows you to display factory-default values. Click Apply to restore factory-default configuration. | | | | |

Figure 6-21. User Lockout Management - factory-default values

- 2. Complete the fields and click Apply.
- 3. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

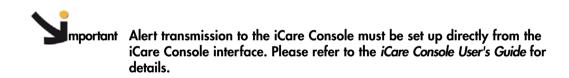
6.9. Configuring Alerts

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

The alert transmission feature allows you to report selected events as alerts to one or more SNMP managers and/or email recipients.

When you set up alert transmission for the first time, you need to:

- Configure the event trap server community string and email server IP and sender addresses. For details, see Configuring SNMP and SMTP Servers, on page 6-47.
- Configure the event trap server IP address(es) and/or email recipient address(es). For details, see Configuring LAN Destinations, on page 6-49.
- Configure the alert transmission policy(ies). For details, see Configuring Alert Policies, on page 6-52.
- Select the events you want to report. For details, see Managing Predefined Event Filters, on page 6-54 and Customizing an Event Filter, on page 6-57.
- **Note** This section explains how to set up the alert transmission feature to suit standard needs. Advanced users may consult the official *IPMI Specification* for information about advanced alert transmission options.



6.9.1. Configuring SNMP and SMTP Servers



WARNING

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

To be able to send events as alerts to SNMP managers and/or email recipients, you need to supply event trap server and email server details.

Prerequisites

You have Alert Settings & Clear SEL permission

Procedure

1. From the Configuration tab, click Alert Settings > General to display the General Settings page.

| | | User : super | System Control | Monitoring | Configuration | Maintenance |
|--|------------------|----------------------|----------------|------------|---------------|-------------|
| ∇ Global Settings Platform Managed Server Functional Profiles | General Settings | Event Trap | | | | ~ |
| ♥ BMC Settings Network Date-Time SNMP Messages | | Community Strin | ng public | | | |
| ▼BMC User Management Users Groups Password | | Email Sender Address | Apply | | | |
| ▼ Security Encryption SSL Certificate User Logon Policy Authentication Power Button Lockout User Lockout | | | | | | |
| ∇ Remote Console Settings User Specific Keyboard/Mouse | | | | | | |
| ♥ Alert Settings Filters Policies LAN Destinations General | | | | | | |
| | | | | | | ~ |

| LAN Alert | | | | | |
|-----------------------|--|--|--|--|--|
| Community String | If you want to use Platform Event Trap (PET) alert messaging, enter the same Community String value as the one used by the SNMP trap server. | | | | |
| | Default value: public. | | | | |
| SMTP Server and Email | If you want to use Email alert messaging, enter: | | | | |
| Sender Address | SMTP Server: name or IP address of the outgoing SMTP email server used to send the email alert messages. | | | | |
| | • Email Sender Address: email server's sender address as it will appear in the header of the email. | | | | |

Figure 6-22. Alert General Settings

- 2. Complete the fields as required and click Apply.
- 3. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.9.2. Configuring LAN Destinations

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

To be able to send events as alerts to SNMP managers or email recipients, you need to configure the corresponding event trap server IP address(es) and/or email recipient address(es). These addresses are also called LAN destinations.



mportant Do not configure alert settings if you are using the iCare Console: alert and message transmission is automatically set up during the creation of the resources tree (resources discovery) through the iCare Console.

Prerequisites

You have Alert Settings & Clear SEL permission

Procedure

1. From the Configuration tab, click Alert Settings > LAN Destinations to display the LAN Destination Settings page.

| ▼ BMC Settings 0 SMMP trap Network 1 SMMP trap Date-Time 1 SMMP trap SMMP 2 SNMP trap Messages 3 SMMP trap V BMC User Management 4 SMMP trap Users 5 SMMP trap Groups 6 SMMP trap Password 6 SMMP trap V Security 6 SMMP trap Encryption 8 SMMP trap User Logon Policy 10 SMMP trap Authentication 9 SMP trap User Specific 11 SMP trap User Specific 13 SMP trap User Specific 14 SMP trap | IP 0.0.0.0 | 12 3 | [Hodify] [Hodify] [Hodify] [Hodify] [Hodify] [Hodify] [Hodify] | |
|---|--|---|--|--|
| ID Type Para BMC Settings 0 SNHP Isne Date Time SNMP Isne Isne SINMP 2 SNMP Isne Messages 3 SNMP Isne 7 BMC User Management 2 SNMP Isne Users 6 SNMP Isne Password 5 SNMP Isne 7 Security 6 SNMP Isne Encryption 5 SNMP Isne User Logno Policy 10 SNMP Isne Authentication 9 SNMP Isne Power Button Lockout 12 SNMP Isne User Specific 13 SNMP Isne Keyboard/Mouse 14 SNMP Isne | IP 0.0.0.0 IP 0.0.0.0 IP 0.0.0.0 IP 0.0.0.0 IP 0.0.0.0 IP 0.0.0.0 IP 0.0.0.0 IP 0.0.0.0 | 12 3 - | [Modify] [Modify] [Modify] [Modify] [Modify] [Modify] | |
| Z BMC Settings 0 SNHP trap Network 1 SNHP trap Date-Time 1 SNHP trap SNMP 2 SNHP trap Messages 3 SNHP trap Z BMC User Management 4 SNHP trap Users 5 SNHP trap Groups 6 SNHP trap Password 7 Still trap 7 Security 8 SNMP trap User Logon Policy 4 SNHP trap Authentication 10 SNHP trap User Logon Policy 11 SNHP trap Vere Button Lockout 12 SNHP trap User Specific 13 SNHP trap Keyboard/Muses 14 SNHP trap | IP 0.0.00 IP 0.0.00 IP 0.0.00 IP 0.0.00 IP 0.0.00 IP 0.0.00 IP 0.0.00 | 12 3 | [Modify] [Modify] [Modify] [Modify] [Modify] [Modify] | |
| Date-Time 1 SNMP trap SNMP 2 SNMP trap Messages 3 SNMP trap ZBMC User Management 4 SNMP trap Users 5 SNMP trap Groups 5 SNMP trap Password 7 Sourity Encryption 8 SNMP trap User Logon Policy 9 SNMP trap Authentication 11 SNMP trap Power Button Lockout 12 SNMP trap User Logon Autor 13 SNMP trap Vser Logon Moley 13 SNMP trap Vser Logon Moley 14 SNMP trap | IP 0.0.00 IP 0.0.00 IP 0.0.00 IP 0.0.00 IP 0.0.00 IP 0.0.00 IP 0.0.00 | 12 3 | [Modify] [Modify] [Modify] [Modify] [Modify] [Modify] | |
| 2 SNMP 2 SNMP trap Messages 3 SNMP trap 3 SNMP trap 4 SNMP trap 5 SNMP trap 6 SNMP trap 7 Some 6 9 SNMP trap 7 Some 6 9 SNMP trap 0 SNMP trap 0 SNMP trap 0 SNMP trap 10 SNMP trap 10 SNMP trap 11 SNMP trap 12 SNMP trap 13 SNMP trap 14 SNMP trap 7 Athentication 14 13 SNMP trap | IP 0.0.00 IP 0.0.00 IP 0.0.00 IP 0.0.00 IP 0.0.00 IP 0.0.00 IP 0.0.00 | | [Modify] [Modify] [Modify] [Modify] [Modify] | |
| Messages 3 SNMP trap 'BMC User Management Users Groups Password 4 SNMP trap 'S courity Encryption SSL Certificate User Logon Policy Authentication Power Button Lockout User Lockout 6 SNMP trap 'S emote Console Settings User Specific Keyboar/Mouse 13 SNMP trap | IP 0.0.0.0 IP 0.0.0.0 IP 0.0.0.0 IP 0.0.0.0 IP 0.0.0.0 | | [Modify] [Modify] [Modify] [Modify] | |
| BMC User Management 4 SNMP trap Users 5 SNMP trap Groups 6 SNMP trap Password 7 SNMP trap 7 Security 8 SNMP trap 8 SNMP trap 10 SNMP trap 9 SNMP trap 10 SNMP trap 10 SNMP trap 10 SNMP trap 10 SNMP trap 11 SNMP trap 11 SNMP trap 13 SNMP trap 12 SNMP trap 13 SNMP trap 13 SNMP trap 14 SNMP trap | IP 0.0.0.0 IP 0.0.0.0 IP 0.0.0.0 IP 0.0.0.0 | | [Modify] [Modify] [Modify] | |
| Users Groups Password Security Encryption SSL Certificate User Logon Policy Authentication Power Button Lackout User Lockout User Lockout User Lockout User Lockout User Lockout User Lockout User Lockout User Lockout 11 SNHP trap 13 SNHP trap 13 SNHP trap 14 SNHP trap 24 Lockout 14 SNHP trap | IP 0.0.0.0 IP 0.0.0.0 IP 0.0.0.0 IP 0.0.0.0 | | [Modify] [Modify] | |
| Groups Password 6 SNHP trap Security Encryption 7 SNHP trap SSL Certificate 9 SNHP trap User Logon Policy Authentication 10 SNHP trap Power Buiton Lockout 11 SNHP trap User Lockout 12 SNHP trap Remote Console Settings User Specific Keyboar/Mouse 13 SNHP trap | IP 0.0.0.0 IP 0.0.0.0 IP 0.0.0.0 | | [Modify] | |
| 7 SNHP trap Security 8 SNHP trap Encryption 9 SNHP trap User Logon Policy 10 SNHP trap Authentication 9 SNHP trap Power Button Lockout 11 SNHP trap User Lockout 12 SNHP trap Veryboar/Mouse 13 SNHP trap | IP 0.0.0.0 IP 0.0.0.0 | | | |
| 7 Security 8 SNMP trap Encryption SSL Certificate 9 SNMP trap User Logon Policy Authentication Power Button Lockout User Lockout 12 SNMP trap 7 Remote Console Settings User Specific Keyboard/Mouse 7 Alert Settings 7 Alert Settings | IP 0.0.0.0 | | | |
| SSL Certificate 9 SNMP trap User Logon Policy 10 SNMP trap Authentication 11 SNMP trap Power Button Lockout 12 SNMP trap User Lockout 13 SNMP trap User Specific 14 SNMP trap | | | [Modify] | |
| User Logon Policy Authentication Power Button Lockout User Lockout User Specific User Specific User Specific Keyboard/Mouse | | | [Modify] | |
| Authentication Power Button Lackout User Lockout User Lockout I1 SNMP trap I2 SNMP trap I3 SNMP trap User Specific Keyboard/Mouse 7 Alert Settings | IP 0.0.0.0 | | [Modify] | |
| 7 Remote Console Settings User Lockout 12 SNHP trap 13 SNHP trap 14 SNHP trap 14 SNHP trap 7 Alert Settings | IP 0.0.0.0 | | [Modify] | |
| 7 Remote Console Settings User Specific Keyboard/Mouse 7 Alert Settings | IP 0.0.0.0 | | [Modify] | |
| User Specific 14 SNMP trap | IP 0.0.0.0 | | [Modify] | |
| Keyboard/Mouse | IP 0.0.0.0 | | [Modify] | |
| | 11 0101010 | | Inodityl | |
| Filters Policies LAN Destinations General | | | | |

Figure 6-23. LAN Destination Settings

2. Select the first free LAN destination line (IP 0.0.0.0) and click Modify to display the Alert Settings: LAN Destination Edit page.

| | | | | | | -**Logout |
|---|------------------------------|------------------------------|-------------------------------|-------------|---------------|-------------|
| | User : | super | System Control | Monitoring | Configuration | Maintenance |
| ∇ Global Settings Platform Managed Server Functional Profiles | Alert Settings: Lan Destinat | ion Edit | Edit | | | <u>^</u> |
| ∀BMC Settings | | Destination Number | | 0 | | |
| Network Date-Time | | Acknowledge | require 🗆 | acknowledge | | |
| SNMP | | Timeout | | 0 | | |
| Messages | | Retries | | 0 | | |
| ✓ BMC User Management Users | | Alert Type | PET alert | | | |
| Groups Password | | Trap destination: 0.0.0.0 | | | | |
| ✓ Security | | 0.0.0.0 | EMail Alert | | | |
| Encryption | | | C Email Alert | | | |
| SSL Certificate User Logon Policy | | r | Apply | | | |
| Authentication Power Button Lockout | | L | White | | | E |
| User Lockout | | | | | | |
| ✓ Remote Console Settings User Specific | | | | | | |
| Keyboard/Mouse | | | | | | |
| ⊽ Alert Settings | | | | | | |
| Filters Policies | | | | | | |
| LAN Destinations General | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | ~ |

| | IPMI LAN Destination Edit |
|--------------------|---|
| Destination Number | Read-only. Predefined number used to identify the destination to which alert messages are to be sent. |
| Acknowledge | PET alerts only. Select if you require alert message acknowledgement. |
| Timeout | PET alerts only. Time in seconds to wait for acknowledgement before retrying. |
| Retries | PET alerts only. Number of retries to make before aborting. |
| Alert Type | Alert messaging format and method: |
| | PET alert (Platform Event Trap): sends a PET alert to the specified trap address. |
| | • Email alert: generates an email alert to the specified email address. |
| Trap destination | PET alerts only. SNMP manager IP address. Example: 192.x.x.x. |
| EMail Alert | Email alerts only. Recipient's email address. Example: john.smith@bull.net |

Figure 6-24. Alert Settings: LAN Destination Edit

- 3. Complete the fields as required and click Apply.
- 4. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.9.3. Configuring Alert Policies

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

Alert policies allow you to define alert messaging strategies.

Note Some of the features described below are reserved for advanced users. For details about advanced alert transmission options, consult the official *IPMI Specification*.

Prerequisites

You have Alert Settings & Clear SEL permission

Procedure

1. From the Configuration tab, click Alert Settings > Policies to display the Policy Settings page.

| | | | User:supe | r | | System Contro | | Monitoring | Configuration | Maintenanc |
|--|-----------------|----------|-----------|------------|--------|-----------------|----------|------------|---------------|------------|
| 7 Global Settings Platform Managed Server Functional Profiles | Policy Settings | – Polici | es — | | | | | | | |
| | | Index | Status | Policy Set | Policy | Channel No. Des | tination | | | |
| BMC Settings Network | | 1 | Enabled | 0 | Always | LAN (1) | 1 | 0 | [Modify] | |
| Date-Time | | 2 | Disabled | 0 | Always | 0 | 0 | 0 | [Modify] | |
| SNMP | | 3 | Disabled | 0 | Always | 0 | 0 | 0 | [Modify] | |
| Messages | | 4 | Disabled | 0 | Always | 0 | 0 | 0 | [Modify] | |
| ⁷ BMC User Management | | 5 | Disabled | 0 | Always | 0 | 0 | 0 | [Modify] | |
| Users | | 6 | Disabled | 0 | Always | 0 | 0 | 0 | [Modify] | |
| Groups Password | | 7 | Disabled | 0 | Always | 0 | 0 | 0 | [Modify] | |
| | | 8 | Disabled | 0 | Always | 0 | 0 | 0 | [Modify] | |
| 7 Security | | 9 | Disabled | 0 | Always | 0 | 0 | 0 | [Modify] | |
| Encryption SSL Certificate | | 10 | Disabled | 0 | Always | 0 | 0 | 0 | [Modify] | |
| User Logon Policy | | | Disabled | | Alwavs | 0 | 0 | | [Modify] | |
| Authentication Power Button Lockout | | | Disabled | | Alwavs | 0 | 0 | | [Modify] | |
| Power Button Lockout User Lockout | | | Disabled | | Always | 0 | 0 | | [Modify] | |
| | | | Disabled | | Always | 0 | 0 | | [Modify] | |
| 7 Remote Console Settings User Specific | | | Disabled | | Always | 0 | 0 | - | [Modify] | |
| Keyboard/Mouse | | | Disabled | | Always | 0 | 0 | | | |
| | | | | | Always | 0 | 0 | | [Modify] | |
| 7 Alert Settings Filters | | | Disabled | | | | | | [Modify] | |
| | | | Disabled | | Always | 0 | 0 | | [Modify] | |
| LAN Destinations General | | 19 | Disabled | 0 | Always | 0 | 0 | 0 | [Modify] | |

Figure 6-25. Alert policy settings

2. Select the first free **disabled** alert policy and click **Modify** to display the **Policy Modification** page.

| | | User: su | per | System Contr | ol Monitoring | Configuration | Maintenance |
|---------------------------------|---|------------|--------------------------------------|--------------------------------------|--------------------------|-----------------------|---------------|
| - Poli | cy Settings | | | | | | |
| orm | | | | | | | |
| aged Server Poli | cy Modification – | | | | | | |
| | Index | Status | Policy Set P | olicy | | ation Alert String | |
| Settings /ork | 1 | Enable 🚩 | 0 / | Always | ✓ 1 | 0 | |
| -Time | | | | Apply | | | |
| IP sages (D) n | | | | Chbul | | | |
| - VPI | olicy Options: Iways | Akusus | send alert to th | a destination | | | |
| · · | 1 C C C C C C C C C C C C C C C C C C C | | | ination was successful, d | n not send alert to this | destination Proceed | to next entry |
| ip o | kip this destination | in this p | olicy set. | | | | |
| sword | top alerting | If alert 1 | o previous des tries in this poli | tination was successful, o | do not send alert to th | is destination. Do no | t proceed any |
| ity | | | | cy set. ination was successful, d | not cand alart to this | destination Process | to next entry |
| | estination type | | | to a different destination t | | destination. Troceet | ro next entry |
| Logon Policy | | | - | | | | |
| entication er Button Lockout | | | | | | | |
| Lockout | | | | | | | |
| te Console Settings | | | | | | | |
| Specific | | | | | | | |
| ooard/Mouse | | | | | | | |
| Settings | | | | | | | |
| rs cies | | | | | | | |
| Destinations | | | | | | | |
| eral | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

| | Policy Modification |
|------------|---|
| Index | Read-only. |
| Status | Two possible values: |
| | Disable (default value): the alert policy is not applied when an event occurs. |
| | • Enable: the alert policy is applied when an event occurs, according to the strategy selected from the Policy drop-down list and the destination number indicated in the Destination field. |
| Policy Set | Policies can be grouped into different policy sets, if required. This is a feature for advanced users. Only one policy set, Policy Set 0, is implemented for the predefined event filters. For details about advanced alert transmission options, you may consult the official <i>IPMI Specification</i> . |

| | Policy Modification |
|--------------|--|
| Policy | This drop-down list allows you to define an event messaging strategy for the current policy. This strategy is dependent on the strategies defined for preceding policies belonging to the same policy set. According to the strategy you want to apply, select one of the following values: |
| | • Always: always send the alert to this destination. |
| | Skip this destination: if the alert has already been sent to a preceding destination by a preceding policy, ignore this destination and go to the next destination in the table. |
| | • Stop alerting: if the alert has already been sent to a preceding destination by a preceding policy, ignore this destination and all subsequent destinations in the table. |
| | • Skip to next different destination type: if the alert has already been sent to a preceding destination by a preceding policy, ignore this destination and go to the next destination using a different transmission method (PET alert vs Email alert). |
| Destination | Enter the predefined number used to identify the destination to which alert messages are to be sent. Note: |
| | This number corresponds to the number in the ID column on the LAN Destination Settings page. |
| Alert String | 0 Read-only. |

Figure 6-26. Alert policy settings - Modification

- 3. Complete the required fields and click Apply.
- 4. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

```
Note Event Message Transmission Processing
When an event occurs, filter table entries are analyzed according to their index
number: from 1 through to the last index number in the list.
When several enabled event filters match the event, the filter with the lowest policy
set number is selected to transmit the alert.
When several enabled event filters match the event in the selected policy set, the
filter with the highest severity is selected to transmit the alert.
When several enabled filters match the event in the selected policy set and they all
have the same severity, the filter with the lowest index is selected to transmit the
alert.
```

6.9.4. Managing Predefined Event Filters

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

Several event filters are factory-predefined and enabled by default. These predefined filters, listed in the Filter Table, cover all potential events. They cannot be modified, but can be enabled/disabled according to your needs. The last filter in the list of predefined filters covers ALL events.

For details, refer to Predefined Alert Filters Description, on page A-2.

Note You can also define custom or "configurable" event filters. This is an advanced option. For details about advanced alert transmission options, you may consult the official *IPMI Specification* and Customizing an Event Filter, on page 5-5.



Prerequisite

You have Alert Settings & Clear SEL permission

Procedure

 From the Configuration tab, click Alert Settings > Filters to display the Filter Settings page.

| - Filter | s — | | | | | | | | | | | | | | | | | | | | | |
|----------|---------|-------------|--------|---------------|---------------------|------------|-------|----------------|---------------|---------|----|--------------|-----|--------|------|-------|-------------|-----|----------------|-----------------------|----|---------|
| Index | Status | Filter Type | Action | Policy Set | Severity | Gene ID | rator | Sensor Type | Sensor No. | Trigger | | ffset ask | | ata 1 | (| Data | 2 | 0 | ata | 3 | | |
| 1 | Enabled | Predefined | Ålert | 0 | Information | ff | ff | 22 | Of | 6f | f | f fi | É O | 0 ff 0 | 00 | 100 | f 0 | 0 0 | 0 f | f | 00 | [Modif |
| 2 | Enabled | Predefined | Alert | 0 | Information | 11 | 11 | 14 | 11 | 11 | 11 | 1 11 | 0 | 0 11 0 | 00 | 100 | 1 0 | 0 0 | 01 | 1 0 | 00 | [Nodif |
| 3 | Enabled | Predefined | Alert | 0 | Information | ff | ff | 08 | ff | 6f | 0 | 1 00 | 0 | 0 ff 0 | 00 | 10 t | f O | 0 0 | 0 f | fO | 00 | [Modif |
| 4 | Enabled | Predefined | Alert | 0 | Non- recoverable | ££ | 11 | 08 | ff | 61 | 03 | 2 00 | 0 | 0 11 0 | 00 | 100 | f O | 0 0 | 0 1 | f | 00 | [Nodif |
| 5 | Enabled | Predefined | Ålert | 0 | Non- critical | ff | ff | 08 | ff | 6f | 10 | 0 00 | 0 | 0 11 0 | 00 | 100 | f | 0 0 | 0 f | f | 00 | [Modif |
| 6 | Enabled | Predefined | Ålert | 0 | Information | ff | ff | 08 | ff | ef | 0 | 1 00 | 0 0 | 0 ff 0 | 00 | 100 | f 0 | 0 0 | 0 f | f | 00 | [Modif |
| 7 | Enabled | Predefined | Alert | 0 | OK | 11 | 11 | 08 | 11 | ef | 12 | 2 00 | 0 0 | 0 11 0 | 00 | 100 | 1 0 | 0 0 | 01 | 10 | 00 | [Nodif |
| 8 | Enabled | Predefined | Alert | 0 | Information | ff | ff | 09 | ff | Ob | 0: | 1 00 | 0 0 | 0 ff 0 | 00 0 | 10 f | f O | 0 0 | 0 f | f | 00 | [Modif |
| 9 | Enabled | Predefined | Alert | 0 | Non- critical | ff. | 11 | 09 | 11 | d0 | 12 | 2 00 | 0 | 0 11 0 | 00 | 100 | £ 0 | 0 0 | 0 1 | 10 | 00 | [Nodif |
| 10 | Enabled | Predefined | Alert | 0 | Non- recoverable | ff | ff | 09 | ff | dD | 21 | 0 00 | 0 | 0 ff 0 | 00 | 100 | f O | 0 0 | 0 f | f | 00 | [Modif |
| 11 | Enabled | Predefined | Alert | 0 | Non- recoverable | 11 | 11 | 02 | 11 | 05 | 03 | 2 00 | 0 | 0 11 0 | 00 | 100 | 1 0 | 0 0 | 0 1 | 1 0 | 00 | [Nodif |
| 12 | Enabled | Predefined | Alert | 0 | Information | 11 | 11 | 02 | 11 | 85 | 03 | 2 00 | 0 | 0 11 0 | 00 | 100 | 1 0 | 0 0 | 01 | 10 | 00 | [Nodif |
| 13 | Enabled | Predefined | Alert | 0 | Non- recoverable | ff | ff | 07 | ft | 6f | 03 | 2 04 | 1 0 | 0 11 0 | 00 | 100 | f | 0 0 | o f | f | 00 | [Nodif |
| 14 | Enabled | Predefined | Alert | 0 | Information | ff | ÍÍ | 07 | ff | 61 | 8 | 0 0: | 1 0 | 0 ff 0 | 00 | 100 | f O | 0 0 | 0 f | f | 00 | [Nodif |
| 15 | Enabled | Predefined | Alert | 0 | Information | ff | ff | 07 | ff | ef | 82 | 2 0: | 1 0 | 0 ff 0 | 00 | 100 | f O | 0 0 | 0 1 | 10 | 10 | Modifie |
| 16 | Enabled | Predefined | Alert | 0 | OK | ff | ff | 07 | ff | | | - | - | - | - | 10000 | Constant of | - | and the second | and the second second | | |

Figure 6-27. Managing predefined filters

2. Select the required predefined filter, using the table in Predefined Alert Filters Description, on page A-2, and click Modify to display the Filter Modification box.

| | User: super | System Cor | ntrol | Monitoring | Configuration | Maintenance |
|--|--|-----------------------------------|--------|------------|--------------------|-------------|
| | ☐ Filter Settings | | | | | |
| Global Settings Platform | Ŭ | | | | | |
| Managed Server Functional Profiles | Filter Modification | | | | | _ |
| | Filter No. | | | | 1 | |
| BMC Settings Network | Status | Enable 💌 | | | | |
| Date-Time SNMP | Filter Type | Predefined Fil | lter | | | |
| Messages BMC User Management Users | Action | Alert 🗹 Reset 📄 Power Off 📄 | | | | |
| Groups Password | Alert Policy | Power Cycle | | | 0 | |
| Security | | | | | U | |
| Encryption SSL Certificate | Event Severity | information | ~ | | | - |
| User Logon Policy | Generator ID | 0x ff | 0x ff | | | _ |
| Authentication Power Button Lockout | Sensor Type | | | | 0x 22 | |
| User Lockout | Sensor No. | | | | OxOf | |
| Remote Console Settings User Specific | Event Trigger | | | | 0x <mark>6f</mark> | |
| Keyboard/Mouse | Data 1 Offset Mask | Mask bits 7:0 |) Oxff | Mask bits | 15:8 Oxff | - |
| Alert Settings | Event Data 1 (AND mask, compare1, compare2 | 0x00 | Oxff | 0x 00 | | |
| Filters Policies | Event Data 2 (AND mask, compare1, compare2 | 0x00 | 0x ff | 0x00 | | |
| LAN Destinations General | Event Data 3 (AND mask, compare1, compare2 | 0x00 | Oxff | 0x00 | _ | |
| | 1 | | | | | |
| | | Apply | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| | Filter Modification |
|--------------------|--|
| Filter No. | Read-only, according to order in the Filter List. |
| Status | Two possible values: |
| | Disable (default value): the filter is not taken into account when an event occurs. |
| | • Enable: the action specified in the Action field is executed if an event matches filter parameters. |
| Filter Type | Read-only: Predefined Filter |
| Action | Read-only: Alert. |
| | Alert: the event is sent to the specified destination(s) (for details, see Configuring LAN Destinations, on page 6-49) |
| | • Reset: the server is reset. |
| | • Power Off: the server is powered down. |
| | • Power Cycle: the server is restarted |
| Alert Policy | Read-only: 0. |
| Event Severity | Read-only, according to predefined severity. |
| Generator ID | Read-only. |
| Sensor Type | For further details, you may consult the official IPMI Specification. |
| Sensor No. | |
| Event Trigger | |
| Data 1 Offset Mask | |

| | Filter Modification |
|---|---------------------|
| Event Data 1 (AND mask, compare1, compare2) | |
| Event Data 2 (AND mask, compare1, compare2) | |
| Event Data 3 (AND mask, compare1, compare2) | |

Figure 6-28. Modifying predefined filters

- 3. In the Status drop-down list, select either Enable or Disable depending on your needs and click Apply.
- 4. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

6.9.5. Customizing an Event Filter

If the system is part of a computing cluster, refer to the documentation delivered with the cluster software for configuration instructions. You are advised to use the configuration feature pages in read-only mode only and not to modify configuration features unless instructed to do so in the cluster software documentation.

You may use the configurable event filters to create a custom event filter, for example if you want to define a different severity for the filter or if you want to associate the filter with a different policy set.

When you set up a configurable event filter, you must disable the corresponding predefined event filter to ensure that the configurable event filter is applied.

Note You are advised to consult the official *IPMI Specification* for information about advanced alert transmission options.

Prerequisites

You have Alert Settings & Clear SEL permission

Procedure

1. From the Configuration tab, click Alert Settings > Filters to display the Filter Settings page.

| | - Filter Index | s Status | Filter Type | Action | Policy Set | Severity | Ger ID | erate | or Sen Typ | sor S e N | ensor Io. | Trigger | Of Ma | fset isk | Da | ıta 1 | | Da | ta 2 | | Data | a 3 | | |
|---|-------------------|-------------|--------------|--------|---------------|--|-----------|-----------------------|---------------|--------------|--------------|---------|----------------|-------------|----|-------|----|------|------|------|------|------|------|-------|
| | 1 | Enabled | Predefined | Alert | 0 | Information | f | £ 1 | f | 22 | Of | 6f | ff | ff | 00 | ff | 00 | 00 | ff | 00 | 00 | ff (| 1 00 | Modif |
| | 2 | Enabled | Predefined | Alert | 0 | Information | 1 | 1 1 | 1 | 14 | 11 | 11 | 11 | 11 | 00 | 11 | 00 | 00 | 11 | 00 | 00 | £1 (| 1 00 | Nodif |
| | 3 | Enabled | Predefined | Alert | 0 | Information | f | £ 3 | f | 08 | ff | 6f | 01 | 00 | 00 | ff | 00 | 00 | ff | 00 | 00 | ££ (| 1 00 | Modif |
| | 4 | Enabled | Predefined | Ålert | 0 | Non- recoverable | | e 3 | f | 08 | ff | 6f | 02 | 00 | 00 | ff | 00 | 00 | 11 | 00 | 00 | £1 (| 1 00 | Modif |
| | 5 | Enabled | Predefined | Hort | 0 | Non- | f | | | | _ | - | - | - | - | | | | | | | 1100 | 100 | [Modi |
| | | Lindo red | Frederined | ATCLO | - | critical | | | | | - | 001 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 0 | _ | - | - | [Modi |
| | | | | _ | | Unspecifie | ed | 00 | 00 | 0 | 00 | 00 | 00 | - | _ | | | | | | | | | [Modi |
| Π | 55 | Disabled | Configurable | Ì | 0 | Unspecifie | ed | 00 | 00 | 0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0 0 | Ĵ 00 | 00 | [Modi |
| | 56 | Disabled | Configurable | ĺ | 0 | Unspecifie | ed | 00 | 00 | 0 | 00 | 00 | 00 | 00 | 00 | 00 | | ac İ | | | - | - | 1000 | |
| | 57 | Disabled | Configurable | Ì | 0 | Unspecifie | ed | 00 | 00 | | - | - | and the second | | - | | | | | | | | | |
| | 58 | Dischled | Configurable | È | - | the second s | | and the second second | 2 | | | | | | | | | | | | | | | |

Figure 6-29. Customizing an event filter

2. Select the first free configurable filter in the list and click Modify to display the Filter Modification box.

| | | User: super | System Co | ontrol | Monitoring | Conf | | Maintenance |
|--|------------------|---|----------------------|-----------|------------|--------|------|-------------|
| | L Filter Setting | 10 | | | | | | |
| Global Settings | The Setting | 35 | | | | | | |
| Platform Managed Server | FF | ilter Modification | | | | | | 7 |
| Functional Profiles | | ilter No. | | | | | 36 | |
| BMC Settings | | | | | | | 120 | |
| Network Date-Time | | Status | Disable N | | | | | |
| SNMP | | ilter Type | User Config | gurable | | | | |
| Messages | | | Alert 🗖 Reset 🗖 | | | | | |
| BMC User Management | 4 | Action | Reset 🛄 Power Off | | | | | |
| Users | | | Power Cyc | | | | | |
| Groups Password | | Alert Policy | | | | | 0 | |
| Security | E | vent Severity | Unspecifie | ed 🔽 | | | | |
| Encryption | | Senerator ID | 0×00 | 0× 00 | | | | |
| SSL Certificate User Logon Policy | | Sensor Type | | | | 0. | × 00 | |
| Authentication | | , | _ | | | | | |
| Power Button Lockout User Lockout | 8 | Sensor No. | | | | 0; | × 00 | |
| | E | vent Trigger | | | | 0) | × 00 | |
| Remote Console Settings User Specific | 0 |)ata 1 Offset Mask | Mask bits 7 | 7:0 0x 00 | Mask bits | 15:8 0 | x 00 | |
| Keyboard/Mouse | E | vent Data 1 (AND mask, compare1, compare2 |) 0×00 | 0x 00 | 0x 00 |] | | |
| Alert Settings | Ē | vent Data 2 (AND mask, compare1, compare2 |) 0×00 | 0× 00 | 0× 00 | 1 | | |
| Filters Policies | 1 - | vent Data 3 (AND mask, compare1, compare2 | | 0× 00 | 0x 00 |] | | |
| LAN Destinations | | ten bata 5 (And mask, comparer, comparez | 10/00 | 3400 | 54.00 | 1 | | |
| General | | ſ | Apply | | | | | |
| | | l | | | | | | |

| | Filter Modification |
|--------------|---|
| Filter No. | Filter number (read-only field). |
| Status | Two possible values: |
| | Disable (default value): the filter is not taken into account when an event occurs. |
| | Enable: the action specified in the Action field is executed if an event matches filter parameters. |
| Filter Type | This read-only field displays User Configurable to specify that you are editing a configurable event filter. |
| Action | Possible values: |
| | Alert: the event is sent to the specified destination(s) (for details, see Configuring LAN Destinations, on page 6-49) |
| | • Reset: the server is reset. |
| | • Power Off: the server is powered off. |
| | Power Cycle: the server is powered off then powered on |
| Alert Policy | Default value: 0. |
| | Policies can be grouped into different policy sets, if required. This is a feature for advanced users. Only one policy set, Policy Set 0, is implemented for the predefined event filters. For details about advanced alert transmission options, you may consult the official <i>IPMI Specification</i> . |

~

| Filter Modification | | | | | | |
|---|---|--|--|--|--|--|
| Event Severity | Select the severity value that you want to send when the event matches the filter parameters. | | | | | |
| Generator ID | These bit fields allow you to specify the event that you | | | | | |
| Sensor Type | want to filter. You are advised to copy the values entered for the corresponding predefined event filter | | | | | |
| Sensor No. | that you are customizing. | | | | | |
| Event Trigger | For further details, you may consult the official IPMI | | | | | |
| Data 1 Offset Mask | Specification or your Customer Representative. | | | | | |
| Event Data 1 (AND mask, compare1, compare2) | | | | | | |
| Event Data 2 (AND mask, compare1, compare2) | | | | | | |
| Event Data 3 (AND mask, compare1, compare2) | | | | | | |

Figure 6-30. Configurable Filters - Modification

- 3. Complete the required fields and click Apply.
- 4. Use the KiraTool utility, provided on the Resource and Documentation CD, to back up configuration data if required. For details, see Backing Up Configuration Data, on page 7-12.

Chapter 7. Using Maintenance Features

This chapter explains the maintenance operations you can perform from the Hardware Console and how to use the utilities provided on the *Resource and Documentation CD*. It includes the following topics:

- Getting Management Controller Information, on page 7-2
- Getting FRU Information, on page 7-3
- Updating Firmware, on page 7-5
- Performing Reset Operations, on page 7-6
- Enabling/Disabling the Identification LED, on page 7-7
- Excluding/Including Processors, on page 7-8
- Displaying Connected Users, on page 7-11
- Backing Up Configuration Data, on page 7-12
- Restoring Configuration Data, on page 7-13

Note The Hardware Console can be used to perform firmware updates. These operations may only be performed by qualified support personnel and are not documented in this guide. Please contact your Customer Service Representative for further information.

7.1. Getting Management Controller Information

You can display and/or save to an XML file embedded management controller and firmware information. This feature is particularly useful for maintenance and troubleshooting (checking current firmware version prior to an upgrade or sending the XML file to the support team, for example).

Procedure

1. From the Maintenance tab, click Hardware Information > Management Controller to display the Management Controller Information page.

| | | | | | ⊰ _Logout |
|---|---------------|--|---|---------------|------------------|
| Server Hardware Consol | le User:super | System Control | Monitoring | Configuration | Maintenance |
| ✓ Hardware Information Management Controller FRU Firmware Version ✓ Firmware Update BMC MXBC ILBC ✓ Maintenance Operations Unit Reset Identification LED Hardware Exclusion Connected Users | | ontroller Informat IP Address: MAC Address: Type: Firmware Version: Firmware Build No Firmware Build No Firmware Descript Parsed Topology F Hardware Revision | tion wpcm450 : 11.09.05 imber: 1167 tion: Final Editio Files: standard | n 20110623 | |

- Figure 7-1. Management Controller Information
- **Note** The Firmware Version and Firmware Build Number values identify the current firmware version and build number.

7.2. Getting FRU Information

The IPMI-compliant information engraved on the FRU (Field Replaceable Unit) can be viewed online and/or saved to an XML file and downloaded for offline analysis and archiving. This feature is particularly useful to the support team.

Procedure

 From the Maintenance tab, click Hardware Information > FRU to display the FRU Information page. As FRU information for all system components must be collected, the page may take several minutes to load.

| | | User | super | | System C | ontrol Monitoring | Configuration | Maintenance |
|---|-----------------|----------|-------------------------------------|---------------------|--------------------------|---------------------------------|---------------|-------------|
| ♥ Hardware Information Management Controller FRU Firmware Version ₱Firmware Update ₱Maintenance Operations | FRU Information | Plat | form FRU Name System Iules | Get System Chass | Identity Card Descrip | | | ^ |
| | | | Module | FRU Name | Instance | Description | | |
| | | + | O | Module | 0 | Drawer module | | |
| | | | | | | | | |
| | | Boa | | | | | | |
| | | | Module | FRU Name | Instance | Description | | |
| | | + + | 0 | PDB | 0 | Power Management | | |
| | | ± | 0 | ILB MTB | 0 | System Board Processor Board | | |
| | | • | 0 | LCP | 0 | Front Panel Board | | |
| | | E | 0 | PS 0 | 0 | Power Supply | | |
| | | | 0 | PS_1 | 1 | Power Supply | | |
| | | | | | | i onor odppij | | |
| | | [Pro | cessors— | | | | | |
| | | | Module | FRU Name | Instance | | | |
| | | + | 0 | PROC_0 | 0 | | | |
| | | ± | 0 | PROC_1 | 1 | | | |
| | | • | 0 | PROC_2 PROC_3 | 2 3 | | | |
| | | | U | PROC_3 | 3 | | | |
| | | | | | | | | × |



Note The plus button next to a FRU name indicates that the line can be expanded to show more information on the FRU. Note that the plus buttons next to the processor names are displayed only when the server is powered on.

2. To save and download FRU information in XML format, click Get Identity Card and follow the instructions on the screen.

7.3. Displaying Firmware Versions

This feature is particularly useful for maintenance and troubleshooting (checking the current firmware version prior to an upgrade or sending information to the support team, for example).

Procedure

• From the Maintenance tab, click Hardware Information > Firmware Version to display the Firmware Information page.

| Server Hardware Conso | de lleru runn | System Control | Monitoring | Configuration | |
|---|-----------------|-------------------|----------------|---------------------|-------------|
| Server Haruware consc | ole User:super | aystem Control | wontoning | Conliguration | maintenance |
| ∀ Hardware Information Management Controller | Firmware Inform | | rmware Version | | ^ |
| FRU Firmware Version | BMC: | | 11.09.05 | | |
| ▼Firmware Update BMC | BIOS: | | | 07.06/01/2011.12:10 | 1:52 |
| MXBC | MXBC | Functional Image: | C.4.5.0.02.04 | | |
| ILBC | MXBC | Running: | C.4.5.0.02.04 | | |
| ADM1069 ▼Maintenance Operations | ILBC F | unctional Image: | B.4.5.0.02.06 | | |
| V Maintenance Operations Unit Reset Identification LED Hardware Exclusion Connected Users | ILBC R | unning: | B.4.5.0.02.06 | | |
| | ILBC B | oot Image: | A.4.0.0.01.00 | | |
| | ADM10 | 69_4_A_98: | 12.01.10 | | |
| | ADM10 | 69_4_A_9A: | 12.02.10 | | |
| | ADM10 | 69_4_A_9C: | 12.03.10 | | |
| | ADM10 | 69_4_A_9E: | 12.04.10 | | |
| | ADM10 | 69_3_B_98: | 44.01.10 | | |
| | ADM10 | 69_3_B_9A: | 44.02.10 | | |
| | ADM10 | 69_3_A_98: | 44.05.10 | | |
| | ADM10 | 69_3_A_9A: | 44.06.10 | | |
| | ADM10 | 69_3_A_9C: | 44.07.10 | | |
| | ADM10 | 69_3_A_9E: | 44.08.10 | | |
| | ADM10 | 69_3_B_9C: | 44.03.10 | | |
| | | 69_3_B_9E: | 44.04.10 | | |
| | LCP: | | 20 | | |
| | PDBPI | C: | 4 | | |
| | | | | | × |

Figure 7-3. Viewing Firmware Information - Server Example

Note According to server model, other firmware image types may be displayed.

Note For certain firmware, more than one type of image is displayed:

- MXBC Functional Image: MXBC image loaded in the SPI Flash EEPROM
- MXBC Running Image: MXBC image loaded in the associated FPGA RAM
- ILBC Functional Image: ILBC image loaded in the SPI Flash EEPROM
- ILBC Running Image: ILBC image loaded in the associated FPGA RAM
- ILBC Boot Image: ILBC boot image loaded in the SPI Flash EEPROM

7.4. Updating Firmware

The firmware on the boards listed below can be updated to install new features or to ensure system integrity after a maintenance operation.

- Embedded Management Controller (BMC)
- Memory and Xeon Board (MXBC)
- I/O Legacy Board (ILBC)
- ADM 1069
- FPGA PCIe Interface images(FPIF IMGA and FPIF IMGB)
- Local Control Panel (LCP)

Qualified support personnel only is authorized to update server firmware. These operations are hazardous and are not documented in this guide. Please contact your Customer Service Representative for further information.

7.5. Performing Reset Operations

The embedded management controller, the virtual keyboard/mouse, USB and video engine can be reset when needed, for example if the system hangs or if the virtual keyboard/mouse or screen no longer respond.

Note The embedded management controller is automatically reset after a BMC firmware update.

Prerequisites

Reset Management Controller: you have Maintenance/Board Reset permission

Reset Keyboard/Mouse, USB, Video Engine: you have Remote Console Access permission All users have disconnected from the console

Procedure

Note The Reset Management Controller command will disconnect any connected users.

1. From the Maintenance tab, click Maintenance Operations > Unit Reset to open the Reset Operations page.

| | | User: super | System Control | Monitoring | Configuration | Maintenance |
|---|------------------|---|-----------------------------|------------|---------------|-------------|
| PHardware Information PFinware Update Viantenance Operations Hardware Exclusion Connected Users | Reset Operations | Reset Keyboard/Mouse Reset USB Reset Video Engine Reset Management Col | (USB) (Reset) (Reset) | | | |
| | | | | | | |

| Feature | Explanation |
|------------------------------------|--|
| Reset Keyboard/Mouse (USB) button | Resets the virtual keyboard/mouse. |
| Reset USB button | Resets the virtual USB. |
| Reset Video Engine button | Resets the virtual monitor. |
| Reset Management Controller button | Stops and restarts the embedded management controller. |

Figure 7-4. Reset Operations

2. Click the required Reset button.

7.6. Enabling/Disabling the Identification LED

The server has two identification LEDs, located at the front and at the rear of the drawer. These two blue ID LEDs provide a visual indication of the drawer being serviced.

Prerequisites

You have Alert Settings & Clear SEL permission

Procedure

1. From the Maintenance tab, click Maintenance Operations > Identification LED to open the Identification LED Management page.

| | | | | | | ut |
|--|--------------|--|------------|---------------|-------------|----|
| | User : super | System Control | Monitoring | Configuration | Maintenance | |
| ▷Hardware Information ▷Firmware Update ♥ Maintenance Operations Unit Reset Identification LED Hardware Exclusion Connected Users | User: super | Identification LED LED Flash Duration Off Identify | Monitoring | Configuration | | |
| | | | | | | |
| | | | | | | ~ |

Figure 7-5. Identification LED Management

2. Select in the LED Flash Duration drop-down list the required value and click Identify.

7.7. Excluding/Including Processors

The console allows you to exclude and include processors statically: the server must be powered off to select the processors to exclude/include and the modification is taken into account at the next power on.

Note Processors are only excluded logically. They remain powered on to ensure system operation.

Prerequisites

You have Maintenance/Board Reset permission

The server is powered off

Procedure



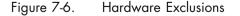
tant Excluding processors is a special task that you must perform only in case of failure.

 From the System Control tab, check that the server is powered down to the standby mode by selecting Power Management and clicking the Refresh button in the Power Information box.

If the displayed power state is Off, proceed to Step 2, otherwise power down the system first and then proceed to Step 2.

2. From the Maintenance tab, click Maintenance Operations > Hardware Exclusion to display the Hardware Exclusions window.

| | | | | | -+∑Logout |
|---|---|---|------------------|---------------------------------------|-------------|
| Server Hardware Consol | e User:super | System Control | Monitoring | Configuration | Maintenance |
| ✓ Hardware Information Management Controller FRU Firmware Version ✓ Firmware Update BMC MXBC ILBC ADM1069 ✓ Maintenance Operations Unit Reset Identification LED Hardware Exclusion Connected Users | Hardware Exclu Exclusions Processor 0 System Power must Select the Power Ma system. Selected processors a Note: Processors are excluded | Processor 1 t be Off, to include anagement page u nd/or modules will b ied LOGICALLY. | inder the System | ssors and/or mod Control Tab to Po | wer Off the |



mportant If the server is not powered down to the standby mode, a message is displayed requesting you to do so. Go to Step 1.

- 3. Either select the check box(es) corresponding to the processors to exclude or clear the check box(es) corresponding to the processors to include and click Apply.
- 4. Power on the server to apply the modification.

7.8. Excluding/Including a Server Module

The console allows you to exclude and include server modules statically: the server module must be powered off before selecting the components to exclude/include, and the modification is taken into account at the next power on.

Note Modules are excluded physically.

Prerequisites

You have Maintenance/Board Reset permission

The server is powered off

Procedure



mportant Excluding server modules is a special task that you must perform only in case of failure.

 From the Power Control tab, check that the server module is powered down to the standby mode by selecting Power Management and clicking the Refresh button in the Power Information box.

If the displayed power state is Off, proceed to Step 2, otherwise power down the system first and then proceed to Step 2.

2. From the Maintenance tab, click Maintenance Operations > Hardware Exclusion to open the Hardware Exclusions page.

| | | | | | Logout |
|--|-------------------------|----------------|---------------------------------------|---------------|-------------|
| Server Hardware Conso | ole User:super | System Control | Monitoring | Configuration | Maintenance |
| PHardware Information PFirmware Update ▼ Maintenance Operations Unit Reset Identification LED Hardware Exclusion Connected Users | Note: Processors are | | Apply s will be excluded or LY. | | |

Figure 7-7. Excluding/Including Modules

mportant If the server module is not powered down to the standby mode, a message is displayed requesting you to do so. Go to Step 1.

- 3. Either select the check box(es) corresponding to the server module to exclude or clear the check box(es) corresponding to the module to include and click Apply.
- 4. Power on the server module to apply the modification.

7.9. Displaying Connected Users

You may see if other users are connected to the console before performing configuration tasks or prior to a maintenance intervention.



Procedure

• From the Maintenance tab, click Maintenance Operations > Connected Users to display the Connected Users Information page.

| | User: super | System | n Control 👖 Monitorin | g Configuration | Haintena |
|---------------------------------------|---------------------------------|-----------------------------|--------------------------|------------------------------|-----------|
| | • | oyster | | g Connigeration | maintella |
| rdware Information | onnected Users Information | | | | |
| mware Update | Compared History | | | | |
| intenance Operations Jnit Reset | Connected Users | Connected IP Address | Session Type Curre | ent Activity | |
| dentification LED | super | EPRIMED NEW T23 | Web Active | - | |
| lardware Exclusion Connected Users | super | | Remote Console Active | 9 | |
| | | | | | |
| | According to HTTP connection ty | rpe, the Connected IP Addre | ess may be that of a rem | ote host or of a proxy serve | er. |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Figure 7-8. Connected Users Information

7.10. Backing Up Configuration Data

Note Backing up configuration data is an administrative task and requires extensive permissions. You are advised to use the default **super** user account.

Main provided on the *Resource and Documentation CD* to back up data.

- 1. Check that the KiraTool utility is installed.
- 2. Refer to the KiraTool documentation available on the Resource and Documentation CD.
- 3. From the KiraTool utility, launch the backup command as described in the documentation.
- 4. Carefully note the backup file name and transmit it to the system administrator. The file will be used to restore configuration data when required.

mportant Two operations may be necessary to back up respectively:

- configuration data (cfg backup conf)
- alert settings data (cfg backup pef)

7.11. Restoring Configuration Data

Note Restoring configuration data is an administrative task and requires extensive permissions. You are advised to use the default **super** user account.

mportant Follow the instructions set out in the *KiraTool* utility documentation provided on the *Resource and Documentation CD* to restore data.

- 1. Check that the KiraTool utility is installed.
- 2. Request the backup file name and path from the system administrator.
- 3. Refer to the KiraTool documentation available on the Resource and Documentation CD.
- 4. From the KiraTool utility, launch the restore command as described in the documentation.



mportant Two operations may be necessary to restore respectively:

- configuration data (cfg restore conf)
- alert settings data (cfg restore pef)

Appendix A. Troubleshooting the Server

This chapter describes how to troubleshoot the server. It includes the following topics:

- Predefined Alert Filters Description, on page A-2
- System Event Log (SEL) Messages, on page A-9

A.1. Predefined Alert Filters Description

This appendix lists predefined event filters. A set of predefined filters, covering all the hardware events likely to occur during system operation, are available for the transmission of alerts to an SNMP Trap Manager, such as Bull System Manager (BSM) or to an email recipient.

Predefined Alert Filters Description

For guidance, the following sets of filters are available, according to component type and server model:

| Component Type | Filter Index |
|---|--|
| Power system board | 1 |
| Sub-chassis | 2, 35, 36 |
| Power supply | 3, 4, 5, 6, 7 |
| Power unit | 8, 9, 10, 40 |
| System board (ILB) | 11, 12, 23, 47 |
| Processor board (MXB) | 11, 12, 23, 47 |
| Processor | 11, 12, 13, 14, 15, 16, 44 |
| Fan device / Cooling unit | 17, 18, 19, 20, 21, 23, 47 |
| Power distribution board (PDB) | 23, 47 |
| Ultra capacitor | 23, 45, 46, 47, 48, 49, 50 |
| Control panel (LCP) | 23, 47 |
| Embedded Management Controller (BMC) | 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 37, 39, 41, 42, 43 |
| Memory | 38 |
| External Environment | 22, 23, 47 |
| All | 51 |

Notes • Pre-defined filters are not modifiable, they can only be enabled or disabled. On system delivery, all predefined filters are enabled.

 If a pre-defined filter does not suit your needs, you can create a custom filter. In this case, you must disable the corresponding predefined filter to ensure that your custom filter is processed.

The use and configuration of event filters is explained in Configuring Alerts, on page 6-47. The following table details the events associated with each predefined filter.

| N° | Component | Source | Event Description | Severity | Meaning |
|----|--------------------------|----------------|--|-----------------|--|
| 1 | Power system board | ACPI Pwr State | SO/GO: working | Information | The system is powered on. |
| 1 | Power system board | ACPI Pwr State | S4/S5: soft off | Information | The system is powered off. |
| 2 | Sub-chassis | Power button | Button pressed | Information | The power button has been pressed. |
| 3 | Power supply | PS_X | Presence detected | Information | The PS_X power supply is present. |
| 4 | Power supply | PS_X | Power supply failure detected | Non-recoverable | A failure has been detected on the PS_X power supply. |
| 5 | Power supply | PS_X | Power supply input lost or out of range | Non-critical | An AC failure has been detected by the PS_X power supply. |
| 6 | Power supply | PS_X | Presence detected | Information | The PS_X power supply is not or no more present. |
| 7 | Power supply | PS_X | Power supply failure detected | Return to OK | The previous failure on the PS_0 power supply disappeared. |
| 7 | Power supply | PS_X | Power supply input lost | Return to OK | The PS_0 power supply AC input is now correct. |
| 8 | Power unit | Pwr Redundancy | Fully redundant | Information | The three power supplies are up and running. |
| 9 | Power unit | Pwr Redundancy | Redundancy lost | Non-critical | Two power supplies are up and running. |
| 9 | Power unit | Pwr Redundancy | Non redundant: Sufficient resources from Insufficient resources | Non-critical | Two power supplies are up and running. |
| 10 | Power unit | Pwr Redundancy | Non redundant: Insufficient resources | Non-recoverable | Only one power supply is up and running. |
| 11 | System board (ILB) | ILB_X | Limit exceeded | Non-recoverable | This voltage is out of the acceptable range. |
| 11 | Processor board (MTB) | MTB_X | Limit exceeded | Non-recoverable | This voltage is out of the acceptable range. |
| 11 | Processor board (MXB) | MXB_X | Limit exceeded | Non-recoverable | This voltage is out of the acceptable range. |
| 11 | Processor | PX_X | Limit exceeded | Non-recoverable | This voltage is out of the acceptable range. |
| 12 | System board (ILB) | ILB_X | Limit exceeded | Information | This voltage is now OK. |
| 12 | Processor board (MTB) | MTB_X | Limit exceeded | Information | This voltage is now OK. |
| 12 | Processor board (MXB) | MXB_X | Limit exceeded | Information | This voltage is now OK. |
| 12 | Processor | PX_X | Limit exceeded | Information | This voltage is now OK. |
| 13 | Processor | PROC_X | Thermal trip | Non-recoverable | PROC_X reached the highest temperature limit and stopped. |
| 14 | Processor | PROC_X | Processor presence detected | Information | PROC_X is present. |
| 14 | Processor | PROC_X | Processor disabled | Information | PROC_X is disabled. |
| 15 | Processor | PROC_X | Thermal trip | Information | PROC_X runs normally. |
| 15 | Processor | PROC_X | Processor presence detected | Information | PROC_X is absent. |
| 15 | Processor | PROC_X | Processor disabled | Information | PROC_X is enabled. |
| 16 | Processor | PROC_X | Processor automatically throttled | Return to OK | PROC_X runs normally. |

| N° | Component | Source | Event Description | Severity | Meaning |
|----|--------------------------------------|---------------------------|---|-----------------|--|
| 17 | Cooling unit | FANPR_X Redund. | Fully redundant | Information | Both of the fans in the fan pair are up and running. |
| 18 | Cooling unit | FANPR_X Redund. | Redundancy lost | Non-critical | Only one fan in the fan pair is up and running. |
| 19 | Cooling unit | FANBX_X Redund. | Non redundant: Insufficient resources | Non-recoverable | No fans are working in the fan pair. |
| 20 | Cooling unit | FANUNIT_X Pres | Device removed / Device absent | Non-recoverable | The fan unit is not or no more present. |
| 20 | Fan device | FAN_X Presence | Device removed / Device absent | Non-recoverable | In the fan pair #X the fan#Y is not or no more present. |
| 21 | Cooling unit | FANUNIT_X Pres | Device inserted / Device present | Return to OK | The fan unit is (now) present. |
| 21 | Fan device | FAN_X Presence | Device inserted / Device present | Return to OK | In the fan pair #X the fan#Y is (now) present. |
| 22 | External Environment | Ambient Temp. | At or above upper critical threshold (going high) | Non-recoverable | The external temperature is above the defined threshold. By default a power off has been executed. |
| 23 | Cooling unit | ROTOR_XY Speed | At or below lower critical threshold (going low) | Return to OK | In the fan unit #X, the rotor #Y speed is now at normal speed. |
| 23 | Fan device | FAN_X Speed | At or below lower critical threshold (going low) | Return to OK | In the fan pair # X the fan #Y is now at normal speed. |
| 23 | System board (ILB) | ILB Temperature | At or below lower critical threshold (going low) | Return to OK | The ILB temperature is now OK. |
| 23 | System board (ILB) | ILB Temperature | At or above upper critical threshold (going high) | Return to OK | The ILB temperature is now OK. |
| 23 | Processor board (MTB) | MTB Temperature | At or below lower critical threshold (going low) | Return to OK | The MTB temperature is now OK. |
| 23 | Processor board (MTB) | MTB Temperature | At or above upper critical threshold (going high) | Return to OK | The MTB temperature is now OK. |
| 23 | Processor board (MXB) | MXB Temperature | At or below lower critical threshold (going low) | Return to OK | The MXB temperature is now OK. |
| 23 | Processor board (MXB) | MXB Temperature | At or above upper critical threshold (going high) | Return to OK | The MXB temperature is now OK. |
| 23 | Power distribution board (PDB) | PDB Temperature | At or below lower critical threshold (going low) | Return to OK | The PDB temperature is now OK. |
| 23 | Power distribution board (PDB) | PDB Temperature | At or above upper critical threshold (going high) | Return to OK | The PDB temperature is now OK. |
| 23 | Ultra capacitor | Ultra Capa Temperature | At or below lower critical threshold (going low) | Return to OK | The UltraCapa temperature is now OK. |
| 23 | Ultra capacitor | Ultra Capa Temperature | At or above upper critical threshold (going high) | Return to OK | The UltraCapa temperature is now OK. |
| 23 | Ultra capacitor | UC XX V | At or below lower critical threshold (going low) | Return to OK | This voltage is now OK. |

| N° | Component | Source | Event Description | Severity | Meaning |
|----|-------------------------|-----------------|---|-----------------|---|
| 23 | Ultra capacitor | UC XX V | At or above upper critical threshold (going high) | Return to OK | This voltage is now OK. |
| 23 | Ultra capacitor | UC VCAP | At or above upper critical threshold (going high) | Return to OK | This voltage is now OK. |
| 23 | Ultra capacitor | UC VCAP | At or above upper critical threshold (going high) | Return to OK | This voltage is now OK. |
| 23 | Ultra capacitor | UC VBOOST | At or below lower critical threshold (going low) | Return to OK | This voltage is now OK. |
| 23 | Ultra capacitor | UC VBOOST | At or above upper critical threshold (going high) | Return to OK | This voltage is now OK. |
| 23 | Ultra capacitor | UC VREF | At or below lower critical threshold (going low) | Return to OK | This voltage is now OK. |
| 23 | Ultra capacitor | UC VREF | At or above upper critical threshold (going high) | Return to OK | This voltage is now OK. |
| 23 | Control panel (LCP) | LCP Temperature | At or below lower critical threshold (going low) | Return to OK | The LCP temperature is now OK. |
| 23 | Control panel (LCP) | LCP Temperature | At or above upper critical threshold (going high) | Return to OK | The LCP temperature is now OK. |
| 23 | External Environment | Ambient Temp. | At or above upper critical threshold (going high) | Return to OK | The external temperature is now OK. |
| 24 | ВМС | Chipset Error | Transition to Critical from less severe | Non-recoverable | A chipset uncorrectable error has occurred. |
| 24 | ВМС | Chipset Error | Transition to Non-Recoverable | Non-recoverable | A chipset uncorrectable error has occurred |
| 25 | ВМС | Processor Error | Transition to Critical from less severe | Non-recoverable | A processor uncorrectable error has occurred. |
| 25 | ВМС | Processor Error | Transition to Non-Recoverable | Non-recoverable | A processor fatal error has occurred. |
| 26 | ВМС | Version Change | Management controller firmware change was successful. | Information | A version change event has occurred. |
| 26 | ВМС | Version Change | System firmware change was successful | Information | A version change event has occurred. |
| 26 | ВМС | Version Change | Programmable hardware change was successful | Information | A version change event has occurred. |
| 27 | ВМС | Version Change | Management controller firmware change was unsuccessful | Non-critical | A version change event has occurred. |
| 27 | ВМС | Version Change | System firmware change was unsuccessful | Non-critical | A version change event has occurred. |

| N° | Component | Source | Event Description | Severity | Meaning |
|----|--------------------|--|--|-----------------|--|
| 27 | ВМС | Version Change | Programmable hardware change was unsuccessful | Non-critical | A version change event has occurred. |
| 28 | BMC | SEL | Sel log full | Non-critical | No more room for a new event in the System Event Log. |
| 28 | BMC | SEL | Sel almost full | Non-critical | The System Event Log is 75% full. |
| 29 | ВМС | System Event | A system boot event has occurred | Non-recoverable | See SEL Messages: BMC. |
| 30 | ВМС | Watchdog | Timeout - no specific action | Critical | Timeout during BIOS init step which causes the configured action. |
| 30 | BMC | Watchdog | Timeout followed by hard reset | Critical | Timeout during BIOS init step which causes the configured action. |
| 30 | ВМС | Watchdog | Timeout followed by Power Down | Critical | Timeout during BIOS init step which causes the configured action. |
| 30 | ВМС | Watchdog | Timeout followed by Power Cycle | Critical | Timeout during BIOS init step which causes the configured action. |
| 31 | ВМС | Platform Security Violation Attempt | Out-of-band access password violation | Non-critical | An out of band IPMI access failed due to password violation. |
| 32 | ВМС | System Event | Entry added to auxiliary log | Information | A corrected machine error has been logged by BIOS in the non-volatile area. |
| 33 | BMC | System Event | Entry added to auxiliary log | Critical | An uncorrected machine error has been logged by BIOS in the non-volatile area. |
| 34 | BMC | System Event | Entry added to auxiliary log | Non-recoverable | A fatal machine error has been logged by BIOS in the non-volatile area. |
| 35 | Sub-chassis | Mod. Intrusion | General chassis intrusion | Critical | The enclosure is opened. |
| 36 | Sub-chassis | Mod. Intrusion | General chassis intrusion | Return to OK | The enclosure is now closed. |
| 37 | BMC | Chipset Error | Transition to OK | Return to OK | Return to normal temperature. |
| 38 | Memory | DIMM_XX | Correctable ECC threshold reached | Warning | Correctable ECC threshold reached on DIMM_XX. |
| 39 | ВМС | Chipset Error | Informational | Information | A chipset correctable error has occured. |
| 40 | Power unit | Pwr Consumption | Power Consumption Level | Information | This event does not appear in the System Event Log (SEL) |
| 41 | ВМС | Version Change | Firmware or software change | Information | BIOS recovery |
| 42 | BMC | System Boot Init | Initiated by hard reset | Information | System Boot Init |
| 42 | BMC | System Boot Init | OS / run-time software initiated hard (warm)reset | Information | System Boot Init |
| 42 | BMC | System Boot Init | System restart | Information | System Boot Init |
| 43 | BMC | OS Stop | OS graceful stop | Information | OS Stop |
| 43 | BMC | OS Stop | OS graceful shutdown | Information | OS Stop |
| 44 | Processor | Proc_X | Processor automatically throttled | Critical | PROC_X runs slowly to limit temperature or power consumption. |
| 45 | Ultra Capacitor | UC VCAP | At or above upper non recoverable threshold (going high) | Non recoverable | This voltage is out of the acceptable range. The module is powered off and disabled. |

| N° | Component | Source | Event Description | Severity | Meaning |
|----|--------------------------------------|---------------------------|---|--------------|---|
| 46 | Ultra Capacitor | UC VCAP | At or above upper non recoverable threshold (going high). | Return to OK | This voltage is now OK |
| 47 | Cooling unit | ROTOR_XY Speed | At or below lower critical threshold (going low) | Critical | In the fan unit #X, the rotor #Y speed is lesser than the minimum required. |
| 47 | Fan device | FAN_X Speed | At or below lower critical threshold (going low) | Critical | In the fan pair # X the fan #Y speed is lower than the minimum required. |
| 47 | System board (ILB) | ILB Temperature | At or below lower critical threshold (going low) | Critical | The ILB temperature is lower than the minimum. |
| 47 | System board (ILB) | ILB Temperature | At or above upper critical threshold (going high) | Critical | The ILB temperature is above the maximum. |
| 47 | Processor board (MXB) | MXB Temperature | At or below lower critical threshold (going low) | Critical | The MXB temperature is lower than the minimum. |
| 47 | Processor board (MXB) | MXB Temperature | At or above upper critical threshold (going high) | Critical | The MXB temperature is above the maximum. |
| 47 | Power distribution board (PDB) | PDB Temperature | At or below lower critical threshold (going low) | Critical | The PDB temperature is lower than the minimum. |
| 47 | Power distribution board (PDB) | PDB Temperature | At or above upper critical threshold (going high) | Critical | The PDB temperature is above the maximum. |
| 47 | Power distribution board (PDB) | UltraCapa Temp. | At or below lower critical threshold (going low) | Critical | The Ultra Capa temperature is lower than the minimum. |
| 47 | Power distribution board (PDB) | UltraCapa Temp. | At or above upper critical threshold (going high) | Critical | The Ultra Capa temperature is above the maximum. |
| 47 | Control panel (LCP) | LCP Temperature | At or below lower critical threshold (going low) | Critical | The LCP temperature is lower than the minimum. |
| 47 | Control panel (LCP) | LCP Temperature | At or above upper critical threshold (going high) | Critical | The LCP temperature is above the maximum. |
| 47 | External Environment | Ambient Temp. | At or above upper non-critical threshold (going high) | Critical | The external temperature is above the non critical threshold. |
| 47 | Ultra Capacitor | Ultra Capa Temperature | At or below lower critical threshold (going high) | Critical | The UltraCapa temperature is lower than the minimum. |
| 47 | Ultra Capacitor | Ultra Capa Temperature | At or above upper critical threshold (going high) | Critical | The UltraCapa temperature is higher than the maximum. |
| 47 | Ultra Capacitor | UC XX V | At or below lower critical threshold (going high) | Critical | This voltage is out of the acceptable range. |
| 47 | Ultra Capacitor | UC XX V | At or above upper critical threshold (going high) | Critical | This voltage is out of the acceptable range. |
| 47 | Ultra Capacitor | UC VCAP | At or above upper critical threshold (going high) | Critical | This voltage is out of the acceptable range. The UltraCapa has been disabled. |

| N° | Component | Source | Event Description | Severity | Meaning |
|----|--------------------|--------------------|---|--------------|---|
| 47 | Ultra Capacitor | UC VBOOST | At or below lower critical threshold (going high) | Critical | This voltage is out of the acceptable range. |
| 47 | Ultra Capacitor | UC VBOOST | At or above upper critical threshold (going high) | Critical | This voltage is out of the acceptable range. |
| 47 | Ultra Capacitor | UC VREF | At or below lower critical threshold (going high) | Critical | This voltage is out of the acceptable range. |
| 47 | Ultra Capacitor | UC VREF | At or above upper critical threshold (going high) | Critical | This voltage is out of the acceptable range. |
| 48 | Ultra capacitor | UC Failure | Battery failed | Critical | A fault has been detected on the UltraCapa (overvoltage, UVLO or charger timeout) |
| 49 | Ultra Capacitor | UC Failure | Battery failed | Return to OK | The Ultra Capacitor is now OK |
| 50 | Ultra capacitor | UC Power Outage | State asserted | Information | A Power Outage occurs |
| 51 | All | All | All | Unspecified | All events are picked up |

A.2. System Event Log (SEL) Messages

This appendix lists System Event Log (SEL) messages and explains actions to recover, where applicable. It includes the following topics:

- SEL Messages: External Environment, on page A-10
- SEL Messages: Power System Board, on page A-10
- SEL Messages: Sub-chassis, on page A-11
- SEL Messages: Power Supply, on page A-13
- SEL Messages: Power Unit, on page A-14
- SEL Messages: ILB, on page A-15
- SEL Messages: MTB/MXB, on page A-25
- SEL Messages: Processor, on page A-28
- SEL Messages: Fan Device / Cooling Unit, on page A-39
- SEL Messages: PDB, on page A-41
- SEL Messages: Ultra Capacitor, on page A-42
- SEL Messages: LCP, on page A-49
- SEL Messages: BMC, on page A-50
- SEL Messages: Memory, on page A-57
- Power Steps: BMC, on page A-58
- Power Steps: SMC, on page A-60

Note The following topics list the entirety of the messages that can be recorded in the SEL, regardless of the server model. Entries may not be relevant to your system.

A.2.1. SEL Messages: External Environment

Ambient Temperature: At or above upper critical threshold (going high)

| Description | The external temperature is above the defined threshold. By default a power off has been executed. |
|---------------|--|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 22. |
| Actions | Check environmental conditions (fan, air conditioning). |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Ambient Temperature: At or above upper critical threshold (going high)

| Description | The external temperature is now OK | |
|---------------|---|--|
| Severity | Return to OK. | |
| Direction | Deassertion. | |
| Filter Number | 23. | |
| Actions | None. | |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. | |

Ambient Temperature: At or above upper non-critical threshold (going high)

| Description | The external temperature is above the non-critical threshold. |
|---------------|---|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Check environmental conditions (fan, air conditioning). |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Ambient Temperature: At or above upper non-critical threshold (going high)

| Description | The external temperature is now OK | |
|---------------|---|--|
| Severity | Return to OK. | |
| Direction | Deassertion. | |
| Filter Number | 23. | |
| Actions | None. | |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. | |

A.2.2. SEL Messages: Power System Board

ACPI Pwr State: S0/G0 working

| Description | The system is powered on. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 1. |
| Actions | None. |
| Comments | Notice that there is no deassertion event. For more information about filters, see Configuring Alerts, on page 6-47. |

ACPI Pwr State: S4/S5 soft off

| Description | The system is powered off. | |
|---------------|---|--|
| Severity | Information. | |
| Direction | Assertion. | |
| Filter Number | 1. | |
| Actions | None. | |
| Comments | Notice that there is no deassertion event. | |
| | For more information about filters, see Configuring Alerts, on page 6-47. | |

A.2.3. SEL Messages: Sub-chassis

Sub-Chassis: Button pressed

| Description | The power button has been pressed. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 2. |
| Actions | None. |
| Comments | Notice that there is no deassertion event. For more information about filters, see Configuring Alerts, on page 6-47. |

Sub-Chassis: General chassis intrusion

| Description | The enclosure is opened. |
|---------------|---|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 35. |
| Actions | Close the enclosure. |
| Comments | Notice that there is no deassertion event. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

Sub-Chassis: General chassis intrusion

| Description | The enclosure is now closed. | |
|---------------|---|--|
| Severity | Return to OK. | |
| Direction | Assertion. | |
| Filter Number | 36. | |
| Actions | None. | |
| Comments | Notice that there is no deassertion event. | |
| | For more information about filters, see Configuring Alerts, on page 6-47. | |

A.2.4. SEL Messages: Power Supply

PS_X: Presence detected

| Description | The PS_X power supply is present. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 3. |
| Actions | None. |
| Comments | X=0, 1 or 2. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PS_X: Presence detected

| Description | The PS_X power supply is not or no more present. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 6. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0, 1 or 2. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PS_X: Power supply failure detected

| Description | A failure has been detected on the PS_X power supply. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 4. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0, 1 or 2. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PS_X: Power supply failure detected

| Description | The previous failure on the PS_X power supply disappeared. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 7. |
| Actions | None. |
| Comments | X=0, 1 or 2. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PS_X: Power supply input lost or out of range

| Description | An AC failure has been detected by the PS_X power supply. |
|---------------|---|
| Severity | Non-critical. |
| Direction | Assertion. |
| Filter Number | 5. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0, 1 or 2. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PS_X: Power supply input lost or out of range

| Description | The PS_X power supply AC input is now correct. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 7. |
| Actions | None. |
| Comments | X=0, 1 or 2. For more information about filters, see Configuring Alerts, on page 6-47. |

A.2.5. SEL Messages: Power Unit

Pwr Redundancy: Fully redundant

| Description | The three power supplies are up and running. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 8. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Pwr Redundancy: Redundancy lost

| Description | Two power supplies are up and running. |
|---------------|---|
| Severity | Non critical. |
| Direction | Assertion. |
| Filter Number | 9. |
| Actions | In a redundant configuration: If the problem persists, contact your Customer Service Engineer. In a non-redundant configuration: None |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Pwr Redundancy: Non redundant. Sufficient resources from insufficient resources

| Description | Two power supplies are up and running. |
|---------------|---|
| Severity | Non critical. |
| Direction | Assertion. |
| Filter Number | 9. |
| Actions | In a redundant configuration: If the problem persists, contact your Customer Service Engineer. In a non-redundant configuration: None |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Pwr Redundancy: Non redundant. Insufficient resources

| Description | Only one power supply is up and running. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 10. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Pwr Consumption: Power Consumption Level

| Description | This event does not appear in the System Event Log (SEL) |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 40. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

A.2.6. SEL Messages: ILB

ILB 0.9V SD: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 0.9V SD: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 0.9V VID: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 0.9V VID: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 0.9V S MNG: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 0.9V S MNG: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 0.9V XDP: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 0.9V XDP: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.0V S GBE: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.0V S GBE: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.05V ICH: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.05V ICH: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.1V IOHO: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.1V IOH0: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.1V IOH1: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.1V IOH1: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.1V SL: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.1V SL: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.2V IB: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.2V IB: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.2V VID: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.2V VID: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.5V LEG: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.5V LEG: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Actions | None. |
| Filter Number | 12. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.8V: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.8V: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.8V S: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.8V S: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.8V XDP: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 1.8V XDP: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 2.5V IB: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 2.5V IB: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 3.3V: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 3.3V: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 3.3V S: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 3.3V S: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 3.3V SL: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 3.3V SL: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 5V LEG: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 5V LEG: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 5V S LEG: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 5V S LEG: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 12V: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB 12V: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB Temperature: At or below lower critical threshold (going low)

| Description | The ILB temperature is lower than the minimum required. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB Temperature: At or above higher critical threshold (going high)

| Description | The ILB temperature is higher than the maximum allowed. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB Temperature: At or below lower critical threshold (going low)

| Description | The ILB temperature is now OK. |
|---------------|---|
| Severity | Return to OK |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ILB Temperature: At or above higher critical threshold (going high)

| Description | The ILB temperature is now OK. |
|---------------|---|
| Severity | Return to OK |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

A.2.7. SEL Messages: MTB/MXB

MTB/MXB 1.2V: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

MTB/MXB 1.2V: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

MTB/MXB 3.3V SD: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

MTB/MXB 3.3V SD: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

MTB/MXB 3.3V SL: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

MTB/MXB 3.3V SL: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

MTB/MXB 5V: Limit Exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

MTB/MXB 5V: Limit Exceeded

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

| Description | The MTB/MXB temperature is lower than the minimum required. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

MTB/MXB Temperature: At or below lower critical threshold (going low)

MTB/MXB Temperature: At or above upper critical threshold (going high)

| Description | The MTB/MXB temperature is higher than the maximum allowed. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

MTB/MXB Temperature: At or below lower critical threshold (going low)

| Description | The MTB/MXB temperature is now OK. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

MTB/MXB Temperature: At or above upper critical threshold (going high)

| Description | The MTB/MXB temperature is now OK. |
|---------------|---|
| Severity | Return to OK |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

A.2.8. SEL Messages: Processor

Proc_X: Thermal trip

| Description | PROC_X reached the highest temperature limit and stopped. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 13. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

Proc_X: Thermal trip

| Description | PROC_X runs normally. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 15. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

Proc_X: Processor presence detected

| Description | PROC_X is present. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 14. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

Proc_X: Processor presence detected

| Description | PROC_X is absent. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 15. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

Proc_X: Processor disabled

| Description | PROC_X is disabled. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 14. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

Proc_X: Processor disabled

| Description | PROC_X is enabled. |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 15. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

Proc_X: Processor automatically throttled

| Description | PROC_X runs slowly to limit temperature or power consumption. |
|---------------|---|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 44. |
| Actions | check environmental conditions (fan, air conditioning). |
| | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

Proc_X: Processor automatically throttled

| Description | PROC_X runs normally. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 16. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 1.1V: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 1.1V: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 1.8V: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 1.8V: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 1.8V MB0: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 1.8V MB0: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Filter Number | 12. |
| Direction | Deassertion. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 1.8V MB1: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 1.8V MB1: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Filter Number | 12. |
| Direction | Deassertion. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 3.3V CHAB: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 3.3V CHAB: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Filter Number | 12. |
| Direction | Deassertion. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 3.3V CHCD: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 3.3V CHCD: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 3.3V TKW: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 3.3V TKW: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 3.3V CPU: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 3.3V CPU: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 12V ARARAT: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX 12V ARARAT: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VCACHE: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VCACHE: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VCORE: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VCORE: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VIO: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VIO: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VCC 0: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VCC 0: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VCC 1: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Filter Number | 11. |
| Direction | Assertion. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VCC 1: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VTT 0: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VTT 0: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VTT 1: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Filter Number | 11. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VTT 1: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VDD 0: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VDD 0: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VDD 1: Limit exceeded

| Description | This voltage is out of the acceptable range. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 11. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

PX VDD 1: Limit exceeded

| Description | This voltage is now OK |
|---------------|---|
| Severity | Information. |
| Direction | Deassertion. |
| Filter Number | 12. |
| Actions | None. |
| Comments | X=0 to 3. |
| | For more information about filters, see Configuring Alerts, on page 6-47. |

A.2.9. SEL Messages: Fan Device / Cooling Unit

FANPR_X Redund: Fan pair_X Fully redundant

| Description | Both of the fans in the fan pair are up and running. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 17. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

FANPR_X Redund: Fanpair_X Redundancy lost

| Description | Only one fan in the fan pair is up and running. |
|---------------|---|
| Severity | Non-critical. |
| Direction | Assertion. |
| Filter Number | 18. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

FANPR_X Redund: Fanpair_X Non redundant: Insufficient resources

| Description | No fans are working in the fan pair. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 19. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

FAN_Y Presence: Device removed / Device absent

| Description | In the fan pair #X, the fan #Y is not or no more present. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 20. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

FAN_Y Presence: Device inserted / Device present

| Description | In the fan pair #X, the fan #Y is (now) present. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Assertion. |
| Filter Number | 21. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

| Description | In the fan pair #X, the fan #Y speed is lesser than the minimum required. |
|---------------|---|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

FAN_Y Speed: At or below lower critical threshold (going low)

FAN_Y Speed: At or below lower critical threshold (going low)

| Description | In the fan pair #X, the fan #Y speed is now at normal speed. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

FANUNIT_X Presence: Device removed / Device absent

| Description | The fan unit #X is not or no more present. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 20. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

FANUNIT_X Presence: Device inserted / Device present

| Description | The fan unit #X is (now) present. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Assertion. |
| Filter Number | 21. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ROTOR_XY Speed: At or below lower critical threshold (going low)

| Description | In the fan unit# X, the rotor #Y speed is lesser than the minimum required. |
|---------------|---|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

| Description | In the fan unit #X, the rotor#Y speed is now at normal speed. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

ROTOR_XY Speed: At or below lower critical threshold (going low)

A.2.10. SEL Messages: PDB

PDB Temperature: At or below lower critical threshold (going low)

| Description | The PDB temperature is lower than the minimum required. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

PDB Temperature: At or above higher critical threshold (going high)

| Description | The PDB temperature is higher than the minimum required. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

PDB Temperature: At or below lower critical threshold (going low)

| Description | The PDB temperature is now OK. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

PDB Temperature: At or above higher critical threshold (going high)

| Description | The PDB temperature is now OK. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

A.2.11. SEL Messages: Ultra Capacitor

UC Failure: Battery failed

| Description | A fault has been detected on the UltraCapa (overvoltage, UVLO or charger timeout). |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 48. |
| Actions | Change the Ultra Capa device and the PDBL board. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC Failure: Battery failed

| Description | The UltraCapa is now OK. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 49. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC Availability: Device Disabled

| Description | The UltraCapa has been disabled due to other error or operator request. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 50. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC Availability: Device Enabled

| Description | The UltraCapa is now available. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 50. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

| Description | The ultra capa temperature is lower than the minimum required. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Ultra Capa Temperature: At or below lower critical threshold (going low)

Ultra Capa Temperature: At or above higher critical threshold (going high)

| Description | The ultra capa temperature is higher than the minimum required. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Check environmental conditions (fan, air conditioning). If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Ultra Capa Temperature: At or below lower critical threshold (going low)

| Description | The ultra capa temperature is now OK. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Ultra Capa Temperature: At or above higher critical threshold (going high)

| Description | The ultra capa temperature is now OK. |
|---------------|---|
| Severity | Return to OK |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC Power Outage: State asserted

| Description | A Power Outage occurs. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 50. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC 3.3V At or below lower critical threshold (going low)

| Description | This voltage is out of the acceptable range. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Change the PDB/PDBL board.If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC 3.3V : At or above higher critical threshold (going high)

| Description | This voltage is out of the acceptable range. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Change the PDB/PDBL board If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC 3.3V : At or below lower critical threshold (going low)

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC 3.3V: At or above higher critical threshold (going high)

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Return to OK |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC 5V At or below lower critical threshold (going low)

| Description | This voltage is out of the acceptable range. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Change the PDB/PDBL board.If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

| Description | This voltage is out of the acceptable range. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Change the PDB/PDBL board If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC 5V : At or above higher critical threshold (going high)

UC 5V : At or below lower critical threshold (going low)

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC 5V: At or above higher critical threshold (going high)

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Return to OK |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC 12V At or below lower critical threshold (going low)

| Description | This voltage is out of the acceptable range. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Change the PDB/PDBL board.If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC 12V : At or above higher critical threshold (going high)

| Description | This voltage is out of the acceptable range. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Change the PDB/PDBL board If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC 12V : At or below lower critical threshold (going low)

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC 12V: At or above higher critical threshold (going high)

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Return to OK |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC VCAP: At or above upper non-recoverable threshold (going high)

| Description | Over voltage on the ultra capa VCAP voltage. |
|---------------|--|
| Severity | Non recoverable. |
| Direction | Assertion. |
| Filter Number | 45. |
| Actions | The Module has been powered off and excluded. The power on will be refused. For safety reasons, disconnect AC power. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC VCAP: At or above upper critical threshold (going high)

| Description | Over voltage on the ultra capa VCAP voltage. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | The Module has been powered off and excluded. The power on will be refused. For safety reasons, disconnect AC power. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC VCAP: At or above upper non-recoverable threshold (going high)

| Description | The UltraCapa VCAP voltage is now OK. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 46. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC VCAP: At or above upper critical threshold (going high)

| Description | The Ultra Capa VCAP voltage is now OK. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC VBOOST : At or below lower critical threshold (going low)

| Description | This voltage is out of the acceptable range. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Change the PDB/PDBL board.If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC VBOOST : At or above higher critical threshold (going high)

| Description | This voltage is out of the acceptable range. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Change the PDB/PDBL board If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC VBOOST : At or below lower critical threshold (going low)

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC VBOOST : At or above higher critical threshold (going high)

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Return to OK |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC VREF : At or below lower critical threshold (going low)

| Description | This voltage is out of the acceptable range. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Change the PDB/PDBL board.If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC VREF : At or above higher critical threshold (going high)

| Description | This voltage is out of the acceptable range. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Change the PDB/PDBL board If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC VREF : At or below lower critical threshold (going low)

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

UC VREF : At or above higher critical threshold (going high)

| Description | This voltage is now OK. |
|---------------|---|
| Severity | Return to OK |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

A.2.12. SEL Messages: LCP

LCP Temperature: At or below lower critical threshold (going low)

| Description | The LCP temperature is lower than the minimum required. |
|---------------|---|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Check environmental conditions (fan, air conditioning).If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

LCP Temperature: At or above higher critical threshold (going high)

| Description | The LCP temperature is higher than the maximum allowed. |
|---------------|---|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 47. |
| Actions | Check environmental conditions (fan, air conditioning).If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

LCP Temperature: At or below lower critical threshold (going low)

| Description | The LCP temperature is now OK. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

LCP Temperature: At or above higher critical threshold (going high)

| Description | The LCP temperature is now OK. |
|---------------|---|
| Severity | Return to OK |
| Direction | Deassertion. |
| Filter Number | 23. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

A.2.13. SEL Messages: BMC

Chipset Error: Transition to Critical from less severe

| Description | A chipset uncorrectable error has occurred. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 24. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Chipset Error: Transition to Non-Recoverable

| Description | A chipset uncorrectable error has occurred. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 24. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Chipset Error: Transition to OK

| Description | Return to normal temperature. |
|---------------|---|
| Severity | Return to OK. |
| Direction | Assertion. |
| Filter Number | 37. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Chipset Error: Informational

| Description | A chipset correctable error has occurred. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 39. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Processor Error: Transition to Critical from less severe

| Description | A processor uncorrectable error has occurred. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 25. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Processor Error: Transition to Non-Recoverable

| Description | A processor uncorrectable error has occurred. |
|---------------|---|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 25. |
| Actions | If the problem persists, contact your Customer Service Engineer. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Version Change: Management controller firmware change was successful

| Description | A version change event has occurred. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 26. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Version Change: Management controller firmware change was unsuccessful

| Description | A version change event has occurred. |
|---------------|---|
| Severity | Non-critical. |
| Direction | Deassertion. |
| Filter Number | 27. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Version Change: System firmware change was successful

| Description | A version change event has occurred. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 26. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Version Change: System firmware change was unsuccessful

| Description | A version change event has occurred. |
|---------------|---|
| Severity | Non-critical. |
| Direction | Deassertion. |
| Filter Number | 27. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Version Change: Programmable hardware change was successful

| Description | A version change event has occurred. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 26. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Version Change: Programmable hardware change was unsuccessful

| Description | A version change event has occurred. |
|---------------|---|
| Severity | Non-critical. |
| Direction | Deassertion. |
| Filter Number | 27. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Version Change: Firmware or software change

| Description | BIOS recovery. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 41. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Sel: Sel log full

| Description | No more room for a new event in the System Event Log. |
|---------------|---|
| Severity | Non-critical. |
| Direction | Assertion. |
| Filter Number | 28. |
| Actions | Clear the System Event Log. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Sel: Sel log almost full

| Description | The System Event Log is 75% full. |
|---------------|---|
| Severity | Non-critical. |
| Direction | Assertion. |
| Filter Number | 28. |
| Actions | Clear the System Event Log as soon as possible. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

System Event

| Description | A system boot event has occurred Event data 2 [7:5] Message class 0 Processor 0 error 1 Processor 1 error 2 Processor 2 error 3 Processor 3 error 4 ILB power error 5 FPGA error 6 System / Environment error 7 Software error [4:0] BMC/SMC step nb : 0-31 see Power Steps: BMC, on page A-58 and Power Steps: SMC, on page A-60 Event data 3 [7:6] Sequence nb 0 Power OFF sequence 1 Power ON sequence 2 Reset sequence 3 RFU [5:0] Error nb : 0-63 see Operation to Recover in the <i>bullx S6030 Service Guide</i> or <i>bullx</i> |
|---------------|--|
| <u> </u> | S6010 Service Guide. |
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 29. |
| Actions | See Operation to Recover in the <i>bullx S6030 Service Guide</i> or <i>bullx S6010 Service Guide</i> . |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

System Event: Undetermined system hardware failure

| Description | Overvoltage on the UltraCapa VCAP voltage. The Module has been powered off and excluded. The power on will be refused. |
|---------------|--|
| Severity | Non-recoverable. |
| Direction | Assertion. |
| Filter Number | 29. |
| Actions | For safety reasons, disconnect AC power. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Watchdog: Timeout – No specific action

| Description | Timeout during BIOS init step which causes the configured action. |
|---------------|---|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 30. |
| Actions | Check other events, then see BIOS postcode. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Watchdog: Timeout followed by hard reset

| Description | Timeout during BIOS init step which causes the configured action. |
|---------------|---|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 30. |
| Actions | Check other events, then see BIOS postcode. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Watchdog: Timeout followed by Power Down

| Description | Timeout during BIOS init step which causes the configured action. |
|---------------|---|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 30. |
| Actions | Check other events, then see BIOS postcode. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

Watchdog: Timeout followed by power Cycle

| Description | Timeout during BIOS init step which causes the configured action. | | |
|---------------|---|--|--|
| Severity | Critical. | | |
| Direction | Assertion. | | |
| Filter Number | 30. | | |
| Actions | Check other events, then see BIOS postcode. | | |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. | | |

Platform Security Violation Attempt: Out-of-band access password violation

| Description | An out of band IPMI access failed due to password violation. | | |
|---------------|---|--|--|
| Severity | Non-critical. | | |
| Direction | Assertion. | | |
| Filter Number | 31. | | |
| Actions | Information. | | |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. | | |

System Event: Entry added to Auxiliary Log

| Description | A corrected machine error has been logged by BIOS in the non-volatile area. | | |
|---------------|---|--|--|
| Severity | Information. | | |
| Direction | Assertion. | | |
| Filter Number | 32. | | |
| Actions | Analyze the log with the iCare Console. | | |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. | | |

System Event: Entry added to Auxiliary Log

| Description | An uncorrected machine error has been logged by BIOS in the non-volatile area. |
|---------------|--|
| Severity | Critical. |
| Direction | Assertion. |
| Filter Number | 33. |
| Actions | Analyze the log with the iCare Console. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

System Event: Entry added to Auxiliary Log

| Description | A fatal machine error has been logged by BIOS in the non-volatile area. | | | |
|---------------|---|--|--|--|
| Severity | lon-recoverable. | | | |
| Direction | Assertion. | | | |
| Filter Number | 34. | | | |
| Actions | Analyze the log with the iCare Console. | | | |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. | | | |

System Boot Init: Initiated by Hard Reset

| Description | System Boot init. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 42. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

System Boot Init: OS / Run-time Software Initiated (Hard/Warm) Reset

| Description | System boot init. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 42. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

System Boot Init: System Restart

| Description | System boot init. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 42. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

OS Stop: OS Graceful Stop

| Description | OS stop. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 43. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

OS Stop: OS Graceful Shutdown

| Description | OS stop. |
|---------------|---|
| Severity | Information. |
| Direction | Assertion. |
| Filter Number | 43. |
| Actions | None. |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. |

A.2.14. SEL Messages: Memory

DIMM_X: Correctable ECC threshold reached

| Description | Correctable ECC threshold reached on DIMM_X | | |
|---------------|---|--|--|
| Severity | Warning. | | |
| Direction | Assertion. | | |
| Filter Number | 38. | | |
| Actions | If the problem persists, contact your Customer Service Engineer | | |
| Comments | For more information about filters, see Configuring Alerts, on page 6-47. | | |

A.2.15. Power Steps: BMC

| Sequence nb = 1 | Step | Action (MTB board) | Action (MXB board) |
|--------------------------------|------|---|--|
| Power ON in normal mode | 0 | [BMC PWR] Build partition composition structure | [BMC PWR] Build partition composition structure |
| | 1 | [BMC PWR] Powering on drawer | [BMC PWR] Powering on drawer |
| | 2 | [BMC PWR] Receiving SMC answer | [BMC PWR] Receiving SMC answer |
| | 3 | [BMC PWR] Update hw presence in SMC | [BMC PWR] Update hw presence in SMC |
| | 4 | [BMC PWR] Init scratchpad registers | [BMC PWR] Init scratchpad registers |
| | 5 | [BMC PWR] Start IPMI watchdog timer | [BMC PWR] Start IPMI watchdog timer |
| | 6 | [BMC PWR] Resume BIOS initialization | [BMC PWR] Resume BIOS initialization |
| | 7 | [BMC PWR] Set ACPI legacy on state | [BMC PWR] Set ACPI legacy on state |
| Power ON light standby | 0 | [BMC PWR] Powering on light standby | [BMC PWR] Powering on light standby |
| | 1 | [BMC PWR] Receiving SMC answer | [BMC PWR] Receiving SMC answer |
| | 2 | [BMC PWR] Set ACPI legacy on state | [BMC PWR] Set ACPI legacy on state |
| Power ON deep standby | 0 | [BMC PWR] Powering on deep standby | [BMC PWR] Powering on deep standby |
| | 1 | [BMC PWR] Receiving SMC answer | [BMC PWR] Receiving SMC answer |
| | 2 | [BMC PWR] Set ACPI legacy on state | [BMC PWR] Set ACPI legacy on state |
| Power ON in north bios mode | 0 | [BMC PWR] Build partition composition structure | [BMC PWR] Build partition composition structure |
| | 1 | [BMC PWR] Powering on drawer in BIOS north mode | [BMC PWR] Powering on drawer in BIOS north mode |
| | 2 | [BMC PWR] Receiving SMC answer | [BMC PWR] Receiving SMC answer |
| | 3 | [BMC PWR] Set ACPI legacy on state | [BMC PWR] Set ACPI legacy on state |
| | 4 | | [BMC PWR] Init scratchpad registers |
| | 5 | | [BMC PWR] Start IPMI watchdog timer |
| | 6 | | [BMC PWR] Resume BIOS initialization |
| | 7 | | [BMC PWR] Set ACPI legacy on state |

| Sequence nb = 0 | Step | Action (MTB board) | Action (MXB board) |
|---------------------------------|------|---|---|
| Power OFF in normal mode | 0 | [BMC PWR] Stop IPMI watchdog timer | [BMC PWR] Stop IPMI watchdog timer |
| | 1 | [BMC PWR] Powering off drawer | [BMC PWR] Powering off drawer |
| | 2 | [BMC PWR] Receiving SMC answer | [BMC PWR] Receiving SMC answer |
| | 3 | [BMC PWR] Set ACPI legacy off state | [BMC PWR] Set ACPI legacy off state |
| Power OFF light standby | 0 | [BMC PWR] Powering off drawer | [BMC PWR] Powering off drawer |
| | 1 | [BMC PWR] Receiving SMC answer | [BMC PWR] Receiving SMC answer |
| | 2 | [BMC PWR] Set ACPI legacy off state | [BMC PWR] Set ACPI legacy off state |
| Power OFF deep standby | 0 | [BMC PWR] Powering off deep standby | [BMC PWR] Powering off deep standby |
| | 1 | [BMC PWR] Receiving SMC answer | [BMC PWR] Receiving SMC answer |
| | 2 | [BMC PWR] Set ACPI legacy off state | [BMC PWR] Set ACPI legacy off state |
| Power OFF in north bios mode | 0 | [BMC PWR] Powering off drawer in BIOS north mode | [BMC PWR] Powering off drawer in BIOS north mode |
| | 1 | [BMC PWR] Receiving SMC answer | [BMC PWR] Receiving SMC answer |
| | 2 | [BMC PWR] Set ACPI legacy off state | [BMC PWR] Set ACPI legacy off state |
| Sequence nb = 2 | Step | Action (MTB board) | Action (MXB board) |
| Warm reset | 0 | [BMC PWR] Reset drawer | [BMC PWR] Reset drawer |
| | 1 | [BMC PWR] Receiving SMC answer | [BMC PWR] Receiving SMC answer |
| | 2 | [BMC PWR] Start IPMI watchdog timer | [BMC PWR] Start IPMI watchdog timer |
| | 3 | [BMC PWR] Resume BIOS initialization | [BMC PWR] Resume BIOS initialization |

A.2.16. Power Steps: SMC

| Sequence nb = 1 | Step | Action (MTB board) | Action (MXB board) |
|----------------------------|------|--|--|
| Power ON in normal mode | 0 | [SMC PWR] LCP Display powering on | [SMC PWR] LCP Display powering on |
| | 1 | [SMC PWR] Check ILBC is loaded | [SMC PWR] Check ILBC is loaded |
| | 2 | [SMC PWR] Check power redundancy | [SMC PWR] Power on 12v power supplies |
| | 3 | [SMC PWR] Power on 12v power supplies | [SMC PWR] Power on fans |
| | 4 | [SMC PWR] Power on fans | [SMC PWR] Check ADM1069 firmwares |
| | 5 | [SMC PWR] Check ADM1069 firmwares | [SMC PWR] Load MXBC FPGA |
| | 6 | [SMC PWR] Load MTBC FPGA | [SMC PWR] Check MXBC is loaded |
| | 7 | [SMC PWR] Check MTBC is loaded | [SMC PWR] Get module configuration |
| | 8 | [SMC PWR] Set FPGA reset mode | [SMC PWR] Set FPGA reset mode |
| | 9 | [SMC PWR] Power on light standby voltages | [SMC PWR] Set FPGA CPU modes |
| | 10 | [SMC PWR] Light standby condition is true | [SMC PWR] Enable clock drivers |
| | 11 | [SMC PWR] Pulse PWRBTN signal | [SMC PWR] Power on light standby voltages |
| | 12 | [SMC PWR] Get module configuration | [SMC PWR] Light standby condition is true |
| | 13 | [SMC PWR] Set FPGA CPU modes | [SMC PWR] Pulse PWRBTN signal |
| | 14 | [SMC PWR] Power on ILBC main voltages | [SMC PWR] Power on main voltages |
| | 15 | [SMC PWR] Power on MTBC main voltages | [SMC PWR] Main power condition is true |
| | 16 | [SMC PWR] Main power condition is true | [SMC PWR] LCP Display BIOS init |
| | 17 | [SMC PWR] Enable clock drivers | [SMC PWR] Check PLTRST signal deasserted |
| | 18 | [SMC PWR] Assert XDP power good | [SMC PWR] Chipset access condition is true |
| | 19 | [SMC PWR] Chipset access condition is true | [SMC PWR] Check processor boot mode |
| | 20 | [SMC PWR] Assert IOH power good | [SMC PWR] Light on LCP green led |
| | 21 | [SMC PWR] LCP Display BIOS init | [SMC PWR] Drawer is powered on |
| | 22 | [SMC PWR] Assert ICH power good | [SMC PWR] Monitoring condition is true |

| Sequence nb = 1 | Step | Action (MTB board) | Action (MXB board) |
|---------------------------|------|--|---|
| | 23 | [SMC PWR] Check PLTRST signal deasserted | [SMC PWR] Set OS running |
| | 24 | [SMC PWR] Chipset access condition is true | |
| | 25 | [SMC PWR] Check processor boot mode | |
| | 26 | [SMC PWR] Light on LCP green led | |
| | 27 | [SMC PWR] Drawer is powered on | |
| | 28 | [SMC PWR] Monitoring condition is true | |
| | 29 | [SMC PWR] Set OS running | |
| Sequence nb = 1 | Step | Action (MTB board) | Action (MXB board) |
| Power ON deep standby | 0 | [SMC PWR] Drawer is powered on | [SMC PWR] Drawer is powered on |
| Sequence nb = 1 | Step | Action (MTB board) | Action (MXB board) |
| Power ON light standby | 0 | [SMC PWR] LCP Display powering on | [SMC PWR] LCP Display powering on |
| | 1 | [SMC PWR] Check ILBC is loaded | [SMC PWR] Check ILBC is loaded |
| | 2 | [SMC PWR] Power on 12v power supplies | [SMC PWR] Power on 12v power supplies |
| | 3 | [SMC PWR] Power on fans | [SMC PWR] Power on fans |
| | 4 | [SMC PWR] Load MTBC FPGA | [SMC PWR] Load MXBC FPGA |
| | 5 | [SMC PWR] Check MTBC is loaded | [SMC PWR] Check MXBC is loaded |
| | 6 | [SMC PWR] Set FPGA reset mode | [SMC PWR] Set FPGA reset mode |
| | 7 | [SMC PWR] Power on light standby voltages | [SMC PWR] Power on light standby voltages |
| | 8 | [SMC PWR] Light standby condition is true | [SMC PWR] Light standby condition is true |
| | 9 | [SMC PWR] Light on LCP green led | [SMC PWR] Light on LCP green led |
| | 10 | [SMC PWR] LCP Display light standby | [SMC PWR] LCP Display light standby |
| | 11 | [SMC PWR] Drawer is powered on | [SMC PWR] Drawer is powered on |

| Sequence nb = 1 | Step | Action (MTB board) | Action (MXB board) |
|--------------------------------|------|--|---|
| Power ON in north bios mode | 0 | [SMC PWR] LCP Display powering on | [SMC PWR] LCP Display powering on |
| | 1 | [SMC PWR] Check ILBC is loaded | [SMC PWR] Check ILBC is loaded |
| | 2 | [SMC PWR] Power on 12v power supplies | [SMC PWR] Power on 12v power supplies |
| | 3 | [SMC PWR] Power on fans | [SMC PWR] Power on fans |
| | 4 | [SMC PWR] Check ADM1069 firmwares | [SMC PWR] Check ADM1069 firmwares |
| | 5 | [SMC PWR] Load MTBC FPGA | [SMC PWR] Load MXBC FPGA |
| | 6 | [SMC PWR] Check MTBC is loaded | [SMC PWR] Check MXBC is loaded |
| | 7 | [SMC PWR] Set FPGA reset mode | [SMC PWR] Get module configuration |
| | 8 | [SMC PWR] Power on light standby voltages | [SMC PWR] Set FPGA reset mode |
| | 9 | [SMC PWR] Light standby condition is true | [SMC PWR] Set FPGA CPU modes |
| | 10 | [SMC PWR] Pulse PWRBTN signal | [SMC PWR] Enable clock drivers |
| | 11 | [SMC PWR] Get module configuration | [SMC PWR] Power on light standby voltages |
| | 12 | [SMC PWR] Set FPGA CPU modes | [SMC PWR] Light standby condition is true |
| | 13 | [SMC PWR] Power on ILBC main voltages | [SMC PWR] Pulse PWRBTN signal |
| | 14 | [SMC PWR] Power on MTBC main voltages | [SMC PWR] Power on main voltages |
| | 15 | [SMC PWR] Main power condition is true | [SMC PWR] Main power condition is true |
| | 16 | [SMC PWR] Enable clock drivers | [SMC PWR] LCP Display BIOS init |
| | 17 | [SMC PWR] Assert XDP power good | [SMC PWR] Check PLTRST signal deasserted |
| | 18 | [SMC PWR] Assert processors power good | [SMC PWR] Chipset access condition is true |
| | 19 | [SMC PWR] Assert IOH power good | [SMC PWR] Check processor boot mode |
| | 20 | [SMC PWR] LCP Display BIOS update | [SMC PWR] Light on LCP green led |
| | 21 | [SMC PWR] Assert ICH power good | [SMC PWR] Drawer is powered on |
| | 22 | [SMC PWR] Check PLTRST signal deasserted | [SMC PWR] Monitoring condition is true |
| | 23 | [SMC PWR] Chipset access condition is true | [SMC PWR] Set OS running |

| Sequence nb = 1 | Step | Action (MTB board) | Action (MXB board) |
|-----------------------------|------|---|---|
| | 24 | [SMC PWR] Check processor boot mode | |
| | 25 | [SMC PWR] Light on LCP green led | |
| | 26 | [SMC PWR] Drawer is powered on | |
| Sequence nb = 0 | Step | Action (MTB board) | Action (MXB board) |
| Power OFF in normal mode | 0 | [SMC PWR] LCP Display powering off | [SMC PWR] LCP Display powering off |
| | 1 | [SMC PWR] Reset OS running | [SMC PWR] Reset OS running |
| | 2 | [SMC PWR] Monitoring condition is false | [SMC PWR] Monitoring condition is false |
| | 3 | [SMC PWR] Chipset access condition is false | [SMC PWR] Chipset access condition is false |
| | 4 | [SMC PWR] Deassert ICH power good | [SMC PWR] Main power condition is false |
| | 5 | [SMC PWR] Deassert IOH power good | [SMC PWR] Power off main voltages |
| | 6 | [SMC PWR] Deassert processors power good | [SMC PWR] Light standby condition is false |
| | 7 | [SMC PWR] Deassert XDP power good | [SMC PWR] Power off light standby voltages |
| | 8 | [SMC PWR] Disable clock drivers | [SMC PWR] Disable clock drivers |
| | 9 | [SMC PWR] Main power condition is false | [SMC PWR] Reset FPGA reset mode |
| | 10 | [SMC PWR] Power off MTBC main voltages | [SMC PWR] Power off fans |
| | 11 | [SMC PWR] Power off ILBC main voltages | [SMC PWR] Power off 12V power supplies |
| | 12 | [SMC PWR] Light standby condition is false | [SMC PWR] Blink LCP green led |
| | 13 | [SMC PWR] Power off light standby voltages | [SMC PWR] Drawer is powered off |
| | 14 | [SMC PWR] Reset FPGA reset mode | |
| | 15 | [SMC PWR] Power off fans | |
| | 16 | [SMC PWR] Power off 12v power supplies | |
| | 17 | [SMC PWR] Blink LCP green led | |
| | 18 | [SMC PWR] Drawer is powered off | |

| Sequence nb = 0 | Step | Action (MTB board) | Action (MXB board) |
|----------------------------|------|--|--|
| Power OFF light standby | 0 | [SMC PWR] LCP Display powering off | [SMC PWR] LCP Display powering off |
| | 1 | [SMC PWR] Light standby condition is false | [SMC PWR] Light standby condition is false |
| | 2 | [SMC PWR] Power off light standby voltages | [SMC PWR] Power off light standby voltages |
| | 3 | [SMC PWR] Reset FPGA reset mode | [SMC PWR] Reset FPGA reset mode |
| | 4 | [SMC PWR] Power off fans | [SMC PWR] Power off fans |
| | 5 | [SMC PWR] Power off 12v power supplies | [SMC PWR] Power off 12v power supplies |
| | 6 | [SMC PWR] Blink LCP green led | [SMC PWR] Blink LCP green led |
| | 7 | [SMC PWR] Drawer is powered off | [SMC PWR] Drawer is powered off |

| Sequence nb = 0 | Step | Action (MTB board) | Action (MXB board) |
|---------------------------------|------|---|---|
| Power OFF deep standby | 0 | [SMC PWR] Drawer is powered off | [SMC PWR] Drawer is powered off |
| Sequence nb = 0 | Step | Action (MTB board) | Action (MXB board) |
| Power OFF in north bios mode | 0 | [SMC PWR] LCP Display powering off | [SMC PWR] LCP Display powering off |
| | 1 | [SMC PWR] Chipset access condition is false | [SMC PWR] Reset OS running |
| | 2 | [SMC PWR] Deassert ICH power good | [SMC PWR] Monitoring condition is false |
| | 3 | [SMC PWR] Deassert IOH power good | [SMC PWR] Chipset access condition is false |
| | 4 | [SMC PWR] Deassert processors power good | [SMC PWR] Main power condition is false |
| | 5 | [SMC PWR] Deassert XDP power good | [SMC PWR] Power off main voltages |
| | 6 | [SMC PWR] Disable clock drivers | [SMC PWR] Light standby condition is false |
| | 7 | [SMC PWR] Main power condition is false | [SMC PWR] Power on light standby voltages |
| | 8 | [SMC PWR] Power off MTBC main voltages | [SMC PWR] Disable clock drivers |
| | 9 | [SMC PWR] Power off ILBC main voltages | [SMC PWR] Reset FPGA reset mode |
| | 10 | [SMC PWR] Light standby condition is false | [SMC PWR] Power off fans |
| | 11 | [SMC PWR] Power off light standby voltages | [SMC PWR] Power off 12v power supplies |
| | 12 | [SMC PWR] Reset FPGA reset mode | [SMC PWR] Blink LCP green led |

| Sequence $nb = 0$ | Step | Action (MTB board) | Action (MXB board) |
|-------------------|------|---|---------------------------------|
| | 13 | [SMC PWR] Power off fans | [SMC PWR] Drawer is powered off |
| | 14 | [SMC PWR] Power off 12v power supplies | |
| | 15 | [SMC PWR] Blink LCP green led | |
| | 16 | [SMC PWR] Drawer is powered off | |

Appendix B. Serial-Over-LAN Console

This appendix explains how to set up and use the Serial-Over-Lan (SOL) Console. It includes the following topics:

- Introducing the SOL Console, on page B-2
- Using the SOL Console with ipmitool, on page B-3
- Using the SOL Console with telnet, on page B-5

B.1. Introducing the SOL Console

The IPMI Serial-Over-Lan (SOL) tool provides access to the system over the management LAN, via the motherboard's embedded management controller (BMC), allowing you to remotely view the text-based console and perform diagnosis and repair tasks such as:

- reconfigure the Operating System or run utilities,
- remotely view boot sequences,
- receive alerts and view messages,
- remotely configure the BIOS.

For further details about SOL Console options, refer to the *ipmitool Guide* delivered on the *Resource & Documentation CD* and the *telnet Guide* delivered with your Operating System.

Note Only one SOL Console can be opened at a time.

mportant SOL requires BIOS Version 01.003.00.014 or higher and Hardware Console Firmware Build Number 1033 or higher.

There are two methods for accessing the SOL Console:

- ipmitool for Linux Operating Systems,
- telnet for Linux and Windows Operating Systems.



mportant To be able to use the SOL Console, you must:

- configure the BIOS,
- set up the required network and SOL permissions from the embedded management controller's (BMC) Hardware Console,
- install the ipmitool / telnet packages (as applicable),
- perform the necessary Operating System configuration tasks. Refer to the documentation delivered with your Operating System for details.

B.2. Using the SOL Console with ipmitool

The **ipmitool command** can be used to connect the SOL Console using a Linux Operating System.

Prerequisites

The BIOS is configured

The required network and SOL permissions are configured on the Hardware Console

The ipmitool package is installed

The Operating System is configured

Procedure

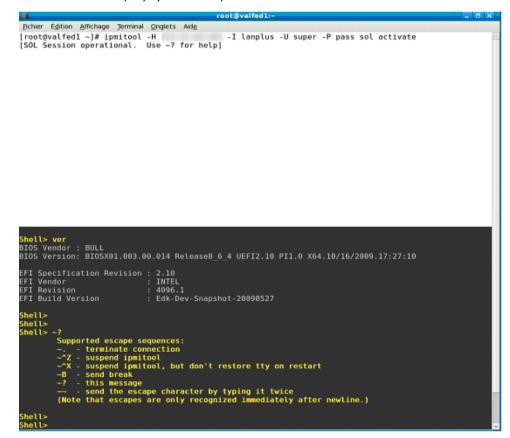
This procedure explains how to open and close the SOL Console with the **ipmitool command**.

- 1. Open a Linux session.
- 2. Open the SOL Console by running the following command:

ipmitool -H <BMC IP address or host name> -I lanplus -U <user> -P <password> sol activate

A SOL session screen opens.

- 3. Press Enter to take control of the remote system.
- 4. Press <~ ?> to display ipmi sol help.





5. Close the SOL Console by pressing <~.>.

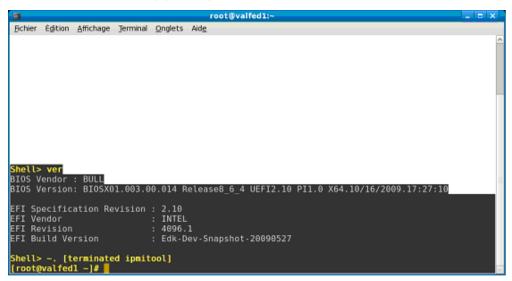


Figure B-2. SOL Console - Closing with ipmitool

B.3. Using the SOL Console with telnet

The **telnet command** can be used to connect the SOL Console using a Linux or Windows Operating System.

Prerequisites

The BIOS is configured

The required network and SOL permissions are configured on the Hardware Console

telnet is installed

The Operating System is configured

Procedure

This procedure explains how to open and close the SOL Console with the telnet command.

- 1. Open a Linux or Windows session.
- 2. Run the telnet command on Port 23.

A telnet session screen opens.

3. Enter the embedded management controller's (BMC) login and password.

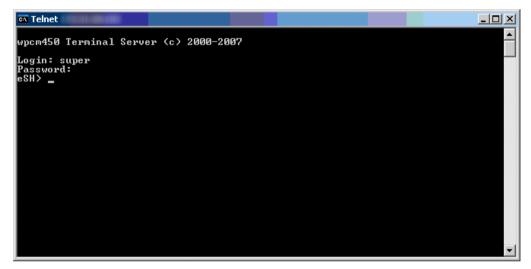


Figure B-3. Telnet session

4. Press <?> to display available commands



Figure B-4. Telnet commands

5. Type **terminal** and press **Enter** TWICE to open the SOL Console and take control of the remote system.

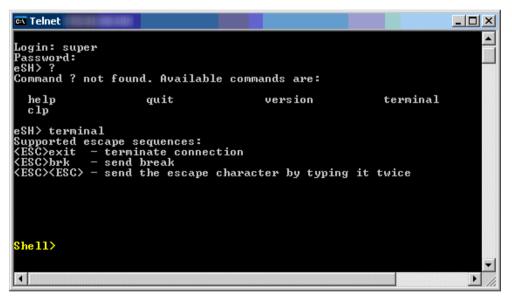


Figure B-5. SOL Console - Launching with telnet

- 6. _Close the SOL Console by pressing <Esc> and typing exit simultaneously.
- 7. Type quit to close the session.

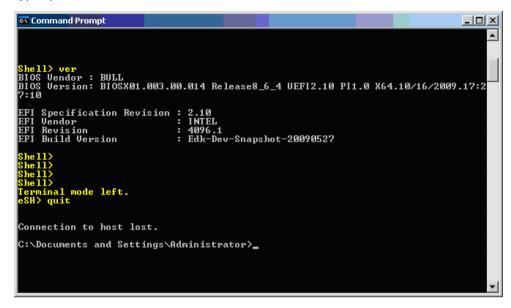


Figure B-6. SOL Console - Closing with telnet

Glossary

A

ABR

Automatic BIOS Recovery.

ACPI

Advanced Configuration and Power Interface.

An industry specification for the efficient handling of power consumption in desktop and mobile computers. ACPI specifies how a computer's BIOS, operating system, and peripheral devices communicate with each other about power usage.

ADM1069

The ADM1069 Super Sequencer® is a configurable supervisory/ sequencing device that offers a single-chip solution for supply monitoring and sequencing in multiple supply systems.

ARU

Add / Removeable Unit. A hardware logical unit, or a group of logical units, that can be viewed / handled by an Operating System, or the BIOS, or the Platform Management Software. An ARU can be nested and is not necessarily separable from other ARUs. An ARU is also known as a PMU.

ASR

Automatic Server Restart.

ASIC

Application Specific Integrated Circuit.

B

Base Operating System

The Operating System that is booted at initialization.

BCE

Elementary calculation block.

BCEA

ASIC elementary calculation block.

BCEF

FPGA elementary calculation block.

BCS

Bull Coherence Switch. This is the Bull eXternal Node Controller providing SMP upgradeability up to 16 processors. The BCS ensures global memory and cache coherence, with optimized traffic and latencies, in both IPF-preferred and XPF-preferred variants.

BHC

See Blade Hardware Console.

BIOS

Basic Input / Output System. A program stored in flash EPROM or ROM that controls the system startup process.

BIST

Built-In Self-Test. See POST.

Blade Hardware Console

Graphical user interface used to access the management software embedded in the blade module.

BMC

Baseboard Management Controller. See Embedded Management Controller.

BOOTP

Network protocol used by a network client to obtain an IP address from a configuration server.

BT

Block Transfer. One of the three standardized IPMI System interfaces used by system software for transferring IPMI messages to the BMC. A per-block handshake is used to transfer data (higher performance).

С

Chassis Hardware Console

Graphical user interface used to access the management software embedded in the Chassis Management Module.

CHC

See Chassis Hardware Console.

Clipping

An Event filter criterion. Clipping is defined on a Count / Time basis aimed at routing a pre-defined number of messages only. Identical messages are counted and when the number of messages indicated in the **Count** field is reached within the period of time indicated in the **Time** field, no other messages will be selected for routing.

СМВ

Chassis Management Board.

CMC

A Corrected Memory Check condition is signaled when hardware corrects a machine check error or when a machine check abort condition is corrected by firmware. See MCA.

CMC

Chassis Management Controller.

CMM

Chassis Management Module.

Core

Core is the short name for the processor execution core implemented on a processor. A core contains one or more threads (logical processors).

CRU

Customer Replaceable Unit. A component (board, module, fan, power supply, etc.) that is replaced or added by the End User as a single entity.

CSE

Customer Service Engineer.

D

DES

Data Encryption Standard.

DHCP

Dynamic Host Configuration Protocol.

DMA

Direct Memory Access. Allows data to be sent directly from a component (e.g. disk drive) to the memory on the motherboard). The microprocessor does not take part in data transfer enhanced system performance.

DNS

Domain Name Server.

E

EEPROM

Electrically Erasable Programmable Read-Only Memory. A type of memory device that stores password and configuration data.

EFI

Extensible Firmware Interface. A specification for a firmware-OS interface.

EFI Shell

Simple, interactive user interface that allows EFI device drivers to be loaded, EFI applications to be launched, and operating systems to be booted. In addition, the EFI Shell provides a set of basic commands used to manage files and the system environment variables. See Shell.

Embedded Management Controller

Also known as BMC (Baseboard Management Controller). This controller, embedded on the main system board, provides out-of-band access to platform instrumentation, sensors and effectors.

EMM

Embedded Management Module. Software embedded in the server module to implement management functions and accessible from the Hardware Console graphical interface.

EPROM

Erasable Programmable Read-Only Memory. A type of memory device that is used to store the system BIOS code. This code is not lost when the computer is powered off.

ESB

Ethernet Switch Board.

ESM

Ethernet Switch Module.

F

FC-LGA

Flip-Chip Land Grid Array.

Flash EPROM

Flash Erasable Programmable Read-Only Memory. A type of memory device that is used to store the system firmware code. This code can be replaced by an updated code from a floppy disk, but is not lost when the computer is powered off.

FPGA

Field Programmable Gate Array.

FQDN

Fully Qualified Domain Name.

FRU

Field Replaceable Unit. A component (board, module, fan, power supply, etc.) that is replaced or added by Customer Service Engineers as a single entity.

G

GPU

Graphical Processing Unit.

GUI

Graphical User Interface.

Η

HA

High Availability. Refers to a system or component that is continuously operational for a desirably long length of time.

Hardware

The physical parts of a system, including the keyboard, monitor, disk drives, cables and circuit cards.

Hardware Partition

A set of hardware components that can boot and run a Base OS image.

Hard Partitioning

Ability to split a platform into a number of independent smaller hardware partitions or to merge multiple independent hardware partitions to form a single larger hardware partition.

HPC

High Performance Computing.

HPC Cluster

High Performance Computing Cluster. A group of computers linked together to form a single computer.

Host Operating System

The Operating System that is booted at initialization and that is a Virtual Machine Monitor (VMM) and a number of guest OS.

Hot-Plugging

The operation of adding a component without interrupting system activity.

Hot-Swapping

The operation of removing and replacing a faulty component without interrupting system activity.

ΗT

HyperThreading. See Multi-Threading.

I2C

Intra Integrated Circuit. The I2C (Inter-IC) bus is a bi-directional two-wire serial bus that provides a communication link between integrated circuits (ICs). The I2C bus supports 7-bit and 10-bit address space devices and devices that operate under different voltages.

IB

InfiniBand.

iBMC

Integrated Baseboard Management Controller. See Embedded Management Controller.

iCare

The iCare Console (insight Care) is a web-based administration application which provides tools for hardware unit maintenance.

ICH

Input/Output Hub. Provides a connection point between various I/O components and Intel processors.

ICMB

Intelligent Chassis Management Bus. Name for the architecture, specifications, and protocols used to interconnect intelligent chassis via an RS-485-based serial bus for the purpose of platform management.

ILB / ILBC

I/O Legacy Board / I/O Legacy Board Controller.

INCA

INtegrated Cluster Architecture.

IOH

Input/Output Hub. An Intel QPI agent that handles I/O requests for processors.

IPMB

Intelligent Platform Management Bus. Abbreviation for the architecture and protocol used to interconnect intelligent controllers via an I2C based serial bus for the purpose of platform management.

IPMI

Intelligent Platform Management Interface. A specification owned by Intel which describes mechanisms and devices to completely offload the task of managing system hardware from the primary CPU.

J

JOEM

JTAG Over Ethernet Module.

JTAG

Joint Test Action Group.

K

No entries.

L

LAN

Local Area Network.

LCD

Liquid Crystal Display.

LCP

Local Control Panel. Module consisting of a controller, a LCD color display, a green and a blue LED and a Power ON button.

LDAP

Lightweight Directory Access Protocol.

LED

Light Emitting Diode.

Logical Partition

When the Base Operating System is a Virtual Machine Monitor, a logical partition is the software environment used to run a Guest Operating System.

Logical Processor

See Thread.

Μ

MAC

Media Access Control.

MCA

A Machine Check Abort exception occurs when an error condition has arisen that requires corrective action.

MESCA

Multiple Environments on a Scalable Csi-based Architecture.

MIB

Management Interface Base.

MIMD

Multiple Instruction Multiple Data

MMX

MultiMedia eXtensions.

MTB/MTBC

Memory and Tukwila Board / Memory and Tukwila Board Controller.

MTBF

Mean Time Between Failure.

Multicore

Presence of two or more processors on a single chip.

Multi-Threading

The ability of a single processor core to provide software visibility similar to that of several cores and execute several threads in apparent (to software) simultaneity while using limited additional hardware resources with respect to a core without multi-threading.

Depending on core design, the instructions issued for execution by the core at a given cycle may be either Hyper-Threading (HT) - from a single thread, switching to another thread upon occurrence of specific events (e.g. cache misses) or Simultaneous Multi-Threading (SMT) - from both threads.

MXB/MXBC

Memory and Xeon Board / Memory and Xeon Board Controller.

Ν

Nehalem

NEHALEM Intel Xeon Processor (8 cores per die).

NFS

Network File System.

NIC

Network Interface Controller.

NUMA

Non Uniform Memory Access.

NVRAM

Non-Volatile Random Access Memory.

0

Off-Lining

See On-Lining / Off-Lining.

On-Lining / Off-Lining

On-lining and off-lining are dynamic logical operations. On-lining is the non-physical addition of an ARU to the running OS. The on-lined unit already exists in the configuration as an inactive unit (present and connected). Off-lining is the non-physical removal of an ARU from the running OS. The off-lined unit remains in the configuration as an inactive unit, ready to be on-lined.

OOB

Out Of Band. Access to system platform management that does not go through the OS or other software running on the main processors of the managed system.

OPMA

Open Platform Management Architecture.

P

PCI

Peripheral Component Interconnect. Bus architecture supporting high-performance peripherals.

PCle

PCI Express. Latest standard in PCI expansion cards.

PDB

Power Distribution Board. Sub-assembly of the Power Supply Module.

PDU

Power Distribution Unit. Power bus used for the connection of peripheral system components.

Platform Event

A platform event is an event that originates directly from platform firmware (BIOS) or platform hardware, independently of the state of the Operating System or System Mangement Hardware.

PEF

Platform Event Filtering.

A feature in IPMI that enables the BMC to generate a selectable action (e.g. power on/off, reset, send Alert, etc.) when a configurable event occurs on the management system.

PET

The Platform Event Trap format is used for sending a platform event in an SNMP Trap. See Platform Event.

PIROM

The Processor Information ROM contains information about the specific processor in which it resides. This information includes robust addressing headers to allow for flexible programming and forward compatibility, core and L2 cache electrical specifications, processor part and S-spec numbers, and a 64-bit processor number.

PMU

Physically Manageable Unit. A hardware logical unit, or a group of logical units, that can be viewed / handled by an Operating System, or the BIOS, or the Platform Management Software. A PMU can be nested and is not necessarily separable from other PMUs. A PMU is also known as an ARU.

POST

Power On Self Test.

Processor

Each processor contains one or more dies in a single package. Each die contains one or more cores. Each core contains one or more threads (logical processors). Each processor is housed in a processor socket.

PSMI

Power Supply Management Interface.

PSU

Power Supply Unit. Sub-assembly of the Power Supply Module.

PSWB

PCI SWitch Board.

PSWM

PCI SWitch Module.

PWM

Pulse Width Modulation.

Q

QDR

Quad Data Rate. Communication signalling technique where data is transmitted at four points in the clock cycle.

QPI

Quick Path Interconnect. High-speed point-to-point Intel interface, used to interconnect processors and I/O Hubs, and optionally node controllers (BCS).

QSB

Quad Switch Board.

QSFP

Quad Small Form-factor Pluggable. Low-power interconnect technology.

QSMB

Quad Switch Module. InfiniBand Switch.

R

RADIUS

Remote Authentication Dial-In User Service.

RAS

Reliability, Availability, Serviceability.

RMII

Reduced Media Independent Interface. A standard that reduceds the number of signals/pins required to connect an Ethernet chip to physical layer transceiver. See MII.

RTC

Real Time Clock.

S

SAS

Serial Attached SCSI. A data transfert technology used to move data to and from computer storage devices such as hard drives and tape drives.

SATA

Serial ATA. A computer bus technology for connecting hard disks and other devices.

SEL

System Event Log. A record of system management events. The information stored includes the name of the event, the date and time the event occurred and event data. Event data may include POST error codes that reflect hardware errors or software conflicts within the system.

A non-volatile storage area into the BMC and associated interfaces for storing System platform Event information for later retrieval.

Server Hardware Console

Graphical user interface used to access the management software embedded in the server module.

SHC

See Server Hardware Console.

Simultaneous Multi-Threading

See Multi-Threading.

SMBIOS

System Management BIOS.

SM-BUS

System Management Bus.

SMI

System Management Interrupt.

SMP

Symmetrical Multi Processor. The processing of programs by multiple processors that share a common operating system and memory.

SMT

Simultaneous Multi-Threading.

SMTP

Simple Mail Transfer Protocol.

SNC

Scalable Node Controller. The processor system bus interface and memory controller for the Intel870 chipset. The SNC supports both the Itanium2 processors, DDR SDRAM main memory, a Firmware Hub Interface to support multiple Firmware hubs, and two scalability ports for access to I/O and coherent memory on other nodes, through the FSS.

SNMP

Simple Network Management Protocol.

SoC

System on Chip.

Socket

Central Processing Unit mutiticore interface.

SOL

Serial Over LAN. Mechanism that enables the input and output of the serial port of a managed system to be redirected via an IPMI session over IP.

SO-DIMM

Small Outline Dual In-line Memory.

SR

Scratch Register. Internal registers of both the Tukwila processor and the I/O Hub used as scratch area.

SSH

Secured Shell.

SSL

Secure Socket Layer.

T

TELNET

TELecommunication NETwork. Protocol used on the Internet or Local Area Networks to provide a bidirectional interactive communications facility.

Thread

A thread or logical processor is the execution context within a single core and the software visibility of multi-threading. A single multi-threaded processor contains two or more threads (or logical processors).

Thresholding

An Event filter criterion. Thresholding is defined on a Count / Time basis aimed at routing significant messages only. Identical messages are counted and when the number of messages indicated in the Count field is reached within the period of time indicated in the Time field, this message is selected for routing.

TKW

TUKWILA Intel Itanium Processor (4 cores per socket).

U

UCM

Ultra Capacitor Module.

UVLO

Under Voltage Latch Output.

V

VMM

Virtual Machine Monitor.

W

WOL

Wake On Lan. A feature that provides the ability to remotely power on a system through a network connection.

X

XCSI

Extended Common System Interface. High-speed point-to-point Bull interface, used to interconnect servers. XCSI ports are located and managed in the BCS (node controller).

XNC

External Node Controller. See BCS.

Y

No entries.

Z

No entries.

Index

A

Alert filters description, A-2 predefined, A-2 Alert policies, setup, 6-52 Alert transmission, setup, 6-47 Alerts, initial configuration, 5-2 Authentication settings, configuring, 6-40

B

Backing up, configuration data, 2-9 Backup, configuration data, 7-12 Backup tool, installing, 2-9 BMC configuring, 6-1 embedded management controller, 7-2 SEL, messages, A-50 Board and security messages setup, 6-12 viewing, 5-7 Buttons console, remote, 4-13 remote, console, system, 4-13

С

Changing, user account details, 6-18 group membership, 6-20 Checking, power, status, 3-4 Clearing, system event log, 5-5 Clock settings, modifying, 6-10 Components, server, 1-4 Configurable event filter, setup, 6-57 Configuration data backup, 7-12 data restoring, 7-13 initial, 2-8 alerts, 5-2 messaging, 5-2 Configuration data backup, 2-9 restoration, 2-9 Configuring authentication settings, 6-40 email recipient address, 6-49 email server, 6-47 event trap community string, 6-47

server IP address, 6-49 LAN destinations, 6-49 logon policy settings, 6-38 platform identification settings, 6-2 security parameters, 6-34 server BMC, 6-1 embedded management controller, 6-1 user lockout parameters, 6-44 user specific settings, 4-3 Connected users, viewing, 7-11 Connecting image file, remote console, 4-16 local drive, remote console, 4-15 local folder, remote console, 4-17 Console features, 2-4 overview, 2-4 remote launching, 4-10 previewing, 4-10 stopping, 4-18 virtual media, 4-14 remote system, 4-1, 4-2 Serial-Over-Lan, B-1 SOL, B-1 ipmitool, B-3 setting up, B-2 telnet, B-5 starting, 2-1 stopping, 2-1 Controls power, server, 3-1 server, 1-4 Cooling unit, SEL, messages, A-39 Creating group, 6-25 user account, 6-14 Current password, modifying, 6-24

D

Date settings, modifying, 6-10 Default user name, 2-2 Default user password, 2-2 Deleting group, 6-32 user account, 6-22 Devices, resetting, 7-6 Disabling identification LED, 7-7 power button, 6-43 predefined event filter, 6-54 user account, 6-20 Drive Redirection disabling, 4-8 enabling, 4-8 Dump, emergency, 3-11

E

Editing, user account, 6-18 Electrical safety, xiii Email recipient address, configuring, 6-49 Email server, configuring, 6-47 Embedded management controller BMC, 7-2 configuring, 6-1 saving, device information, 7-2 SEL, messages, A-50 viewing, device information, 7-2 Emergency dump, 3-11 force power cycle, 3-11 force power off, 3-11 hard reset, 3-11 hard reset & dump, 3-11 power off, 3-10 reset, 3-10, 3-11 Enabling identification LED, 7-7 power button, 6-43 predefined event filter, 6-54 user account, 6-20 Event log, server, monitoring, 5-1 Event trap, configuring, 6-47, 6-49 Excluding hardware, 7-8 processors, 7-8 server module, 7-10 External Environment, SEL, messages, A-10

F

Fan device, SEL, messages, A-39 Features console, 2-4 interface, 2-5 server, 1-4 Filters, alert, A-2 Firmware updating, 7-5 viewing, information, 7-4 Firmware information, viewing, 7-4 Force power cycle, emergency, 3-11 Force power off, emergency, 3-11 Forcing HTTPS connections, 6-34 password change, 6-21 FRU information, viewing and saving, 7-3 Functional profiles, modifying, 6-4

G

Getting an SSL Certificate, 6-36 Glossary, g-1 Group creating, 6-25 deleting, 6-32 Group members, viewing, 6-31 Group permissions, 6-27 Groups, managing, 6-14

Η

Hard reset, emergency, 3-11 Hard reset & dump, emergency, 3-11 Hardware, excluding, 7-8 Hardware Console, starting, 2-2 HTTPS connections, forcing, 6-34

Identification LED (enabling/disabling), 7-7 ILB, SEL, messages, A-15 Image file, virtualizing, 4-16 Including, server module, 7-10 Initial, configuration, 2-8 alerts, 5-2 messaging, 5-2 Installing, backup tool, 2-9 Installing an SSL Certificate, 6-36 Interface features, 2-5 permissions, 2-5 ipmitool, SOL, using, B-3

LAN destinations, configuring, 6-49 Laser safety, xiv Launching, remote console, 4-10 LEDs, server, 1-4 Local Control Panel (LCP), SEL, messages, A-49 Local drive, virtualizing, 4-15 Local folder, virtualizing, 4-17 Lockout parameters power button, 6-43 user, 6-44 Logon policy, configuring, 6-38

M

Maintenance, features, 7-1 Managed server, name, setting, 6-3 Management controller, setting up messages, 6-12 Managing groups, 6-14 permissions, 6-14 users, 6-14 Media, virtual connecting, 4-14 disconnecting, 4-14 Memory, SEL, messages, A-57 Menus console, remote, 4-12 remote, console, system, 4-12 Messages SEL BMC, A-50 cooling unit, A-39 embedded management controller, A-50 external environment, A-10 fan device, A-39 ILB, A-15 Local Control Panel (LCP), A-49 memory, A-57 MTB, Á-25 MXB, A-25 PDB, A-41 power supply, A-13 power system board, A-11 power unit, A-14 processor, A-28 sub-chassis, A-11 ultra capacitor, A-42 server, monitoring, 5-1 Messaging, initial configuration, 5-2 Modifying clock settings, 6-10 current password, 6-24 functional profiles settings, 6-4 Monitoring sensors, 5-3 server, 5-1 event log, 5-1 messages, 5-1 MTB, SEL, messages, A-25 MXB, SEL, messages, A-25

Ν

Notices electrical safety, xiii laser safety, xiv safety, xiii

0

Overview console, 2-4 remote console, system, 4-11 server, 1-2

Ρ

Password change, 6-21 Password modification, 6-24 PDB, SEL, messages, A-41 Permissions, 6-27 interface, 2-5 managing, 6-14 Platform, identification settings, configuring, 6-2 Power management, 3-2 status, checking, 3-4 Power controls, server, 3-1 Power off emergency, 3-10 system, hang, 3-10 Power supply, SEL, messages, A-13 Power system board, SEL, messages, A-11 Power unit, SEL, messages, A-14 Powering off, system, 3-8 Powering on, system, 3-6 Predefined alert filters, description, A-2 Predefined event filter, enabling and disabling, 6-54 Previewing, remote console, 4-10 Processor, SEL, messages, A-28 Processors, excluding, 7-8

R

Recommendations, safety, xiv Remote console overview, 4-11 system buttons, 4-13 menus, 4-12 virtual media, 4-14 system, console, 4-2 buttons, 4-13 menus, 4-12 system, console, 4-3, 4-6 system console, setting up, 4-2 Remote console connecting image file, 4-16 local drive, 4-15 local folder, 4-17 launching, 4-10 previewing, 4-10 stopping, 4-18 Remote System Console, 4-1 user specific settings, 4-3 Reset emergency, 3-10, 3-11 system, hang, 3-10 Resetting, devices, 7-6 Restoring, configuration data, 2-9, 7-13

S

Safety notices, xiii recommendations, xiv Saving embedded management controller, information, 7-2 FRU information, 7-3 Secure connections. See HTTPS connections Security messages setup, 6-12 viewing, 5-7 Security parameters, configuring, 6-34 SEL BMC, messages, A-50 cooling unit, messages, A-39 embedded management controller, messages, A-50 external environment, messages, A-10 fan device, messages, A-39 ILB, messages, A-15 Local Control Panel (LCP), messages, A-49 memory, messages, A-57 MTB, messages, A-25 MXB, messages, A-25 PDB, messages, A-41 power supply, messages, A-13 power system board, messages, A-11 power unit, messages, A-14 processor, messages, A-28 sub-chassis, messages, A-11 ultra capacitor, messages, A-42 SEL messages, A-9 Sensors, monitoring, 5-3 Serial-Over-Lan, console, B-1 setting up, B-2 using ipmitool, B-3 telnet, B-5 Server BMC, configuring, 6-1 components, 1-4 controls, 1-4 embedded management controller, configuring, 6-1 features, 1-4 LEDs, 1-4 monitoring, 5-1 overview, 1-2 power, 3-1 Server module excluding, 7-10 including, 7-10 Servicing, features, 7-1 Setting managed server, name, 6-3 permissions, 6-27 Setting up, 6-12 alert policies, 6-52 alert transmission, 6-47 board and security messages, 6-12 configurable event filter, 6-57 console, SOL, B-2 system console, remote, 4-2 Settings keyboard, remote system console, 4-6 mouse, remote system console, 4-6 user specific, remote system console, 4-3

SOL console, B-1 setting up, console, B-2 using ipmitool, B-3 telnet, B-5 SSL Certificate, get and install, 6-36 Starting console, 2-1 Hardware Console, 2-2 Status, power, checking, 3-4 Stopping console, 2-1 remote console, 4-18 Sub-chassis, SEL, messages, A-11 System console, remote buttons, 4-13 menus, 4-12 powering off, 3-8 powering on, 3-6 remote console launching, 4-10 overview, 4-11 previewing, 4-10 stopping, 4-18 System console, remote, settings, 4-3, 4-6 System event log clearing, 5-5 viewing, 5-5

T

telnet, SOL, using, B-5 Time settings, modifying, 6-10

U

Ultra Capacitor, SEL messages, A-42 Unlocking, user account, 6-23 Unlocking a user, 6-23 Updating, firmware, 7-5 User account changing details, 6-18 group membership, 6-20 creating, 6-14 deleting, 6-22 details, viewing, 6-16 disabling, 6-20 editing, 6-18 enabling, 6-20 forcing, password change, 6-21 unlocking, 6-23 User lockout parameters, 6-44 User permissions, 6-27 User specific settings, 4-3 Users, managing, 6-14

Using, SOL ipmitool, B-3 telnet, B-5

V

Viewing

board and security messages, 5-7 connected users, 7-11 embedded management controller, information, 7-2 FRU information, 7-3 group members, 6-31 system event log, 5-5 user account, details, 6-16 Virtual media connecting, 4-14 disconnecting, 4-14 image file, 4-16 local drive, 4-15 local folder, 4-17 Virtualizing image file, 4-16 local drive, 4-15 local folder, 4-17

W

Write support disabling, 4-8 enabling, 4-8

Bull Cedoc 357 avenue Patton BP 20845 49008 Angers Cedex 01 FRANCE

REFERENCE 86 A1 50FD 06