iCare

iCare Console

User's Guide

REFERENCE
86 A1 71FA 02

iCare

iCare Console

User's Guide

Hardware

December 2009

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

REFERENCE
86 A1 71FA 02

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

List of Figures

List of Tables

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 Bull SAS 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

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

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

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

WARNING
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

Bull product 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.

Preface

This guide explains how to use the iCare Console to monitor and maintain Bull Systems. The iCare Console runs on the following operating systems:

- Windows XP, Vista (or later)
- Windows Server 2003, 2008 (or later)

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 Hardware Administrators and Operators and qualified support personnel.

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

Please refer to the documention delivered with the systems monitored and maintained via the iCare Console.

Chapter 1. Getting Started

This chapter explains how to install iCare Console software, start and stop the iCare Console from a web browser and view software version information. It also describes console features and outlines initial configuration tasks. It includes the following topics:

1.1. Installing iCare Console Software

The iCare Console is used to monitor and maintain Bull systems. The software is supplied on the *Resource and Documentation CD* and can be installed on any PC running:

- Windows XP, Vista (or later)
- Windows Server 2003, 2008 (or later)

Hardware resources can only be monitored and maintained by ONE iCare Console at a given time.
If you want to transfer the monitoring and maintenance of hardware resources to another iCare Console running on another PC, you MUST delete the hardware resources concerned from the current Resource tree before importing them into another Resource tree to ensure correct operation.
See Deleting a Resource from the Tree, on page 2-20 and Importing Resources, on page 2-2 for details.

Procedure

1. From the *Resource and Documentation CD*, open the iCare folder.
2. Launch **iCaresetup.exe** to install the software and follow the instructions on the screen.

   Once the software has been installed, the **iCarewebsite** shortcut icon appears on your desktop.
3. Double-click the **iCarewebsite** shortcut to start the iCare Console.

   Users can now connect remotely to the iCare Console using a Microsoft Internet Explorer or Mozilla Firefox browser.

Note For the iCare Console to function correctly with a Web browser, please check the following settings:
Firefox: the browser is configured to accept cookies
Internet Explorer: the browser is configured to allow file downloads:

- From the **Tools** menu, select **Internet Options > Security > Custom Level > Downloads**
- Check that the **Automatic prompting for file downloads** and **File download** parameters are **Enabled**

Related Topics

- Starting the iCare Console, on page 1-4
- iCare Console Overview, on page 1-5
- Displaying Software Version Information, on page 1-3
- Initial Configuration, on page 1-8
- Stopping the iCare Console, on page 1-8

1.2. Displaying Software Version Information

If needed for maintenance and troubleshooting operations, for example checking current software versions prior to an upgrade, you can display iCare Console and other software version information.

Prerequisites

None

Procedure

- From the **Global Configuration** tab, click **Miscellaneous > Software Versions** to display the **Software Versions** page.

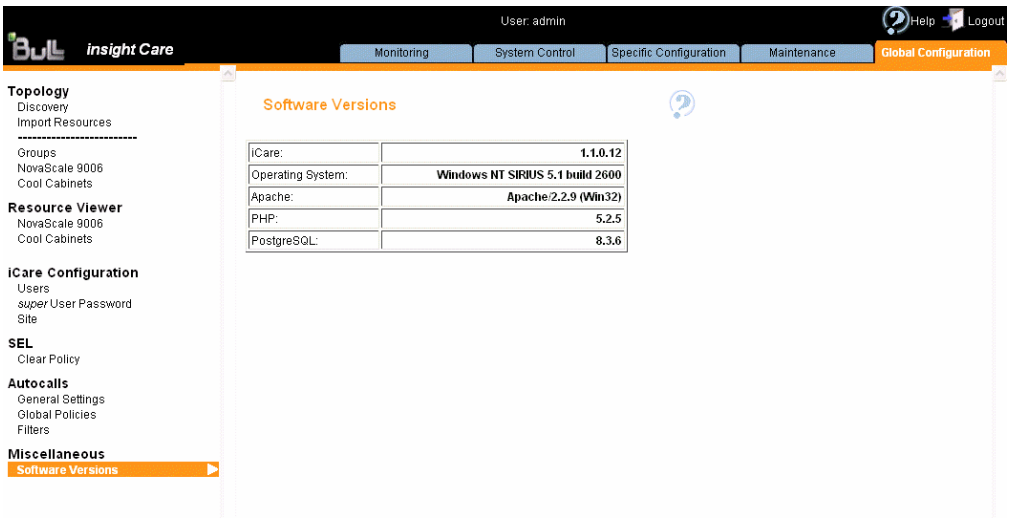


Figure 1. Software Versions page

1.3. Starting the iCare Console

Once the iCare Console has been installed, you can start the iCare Console using a Microsoft Internet Explorer or Mozilla Firefox browser.

Prerequisites

The PC hosting the iCare Console is running

The Web browser is configured to accept cookies and to allow file downloads

Procedure

1. Double-click the iCare Console icon located on your desktop or launch your web browser and enter the iCare Console IP address or host name followed by **/icare** (example: **http://192.168.1.1:8080/icare**). The login page opens.

iCare	
Username	Factory-default username: **admin**
Password	Factory-default password: **pass**

Figure 2. Login page description

2. Complete the **Username** and **Password** fields and click **Log in**. Once you are authenticated, the **Monitoring** tab opens.

Important **It is strongly recommended to change the factory-default admin user password once initial setup is completed, taking care to record your new account details for subsequent connections.**
If you lose your account details and are unable to connect to the console, please contact your Customer Service Representative.

What To Do if an Incident Occurs?

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

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

Related Topics

- Stopping the iCare Console, on page 1-8
- Changing a User Account Password, on page 5-4

1.4. iCare Console Overview

The iCare Console is a web-based hardware administration application which provides tools for the supervision and maintenance of hardware resources.

Once imported, monitored hardware resources are displayed in the iCare Console Resource tree which displays the status of each monitored resource using a color code.

Traps are sent by the hardware resources monitored by the iCare Console to the iCare Console database for easy consultation in the event of incidents on one or more resources.

The console receives three types of traps:

- IPMI PET LAN traps with retry mechanism (ack) (Events)
- Non-IPMI platform specific SNMP Traps (Messages)
- BIOS logs

Console Features

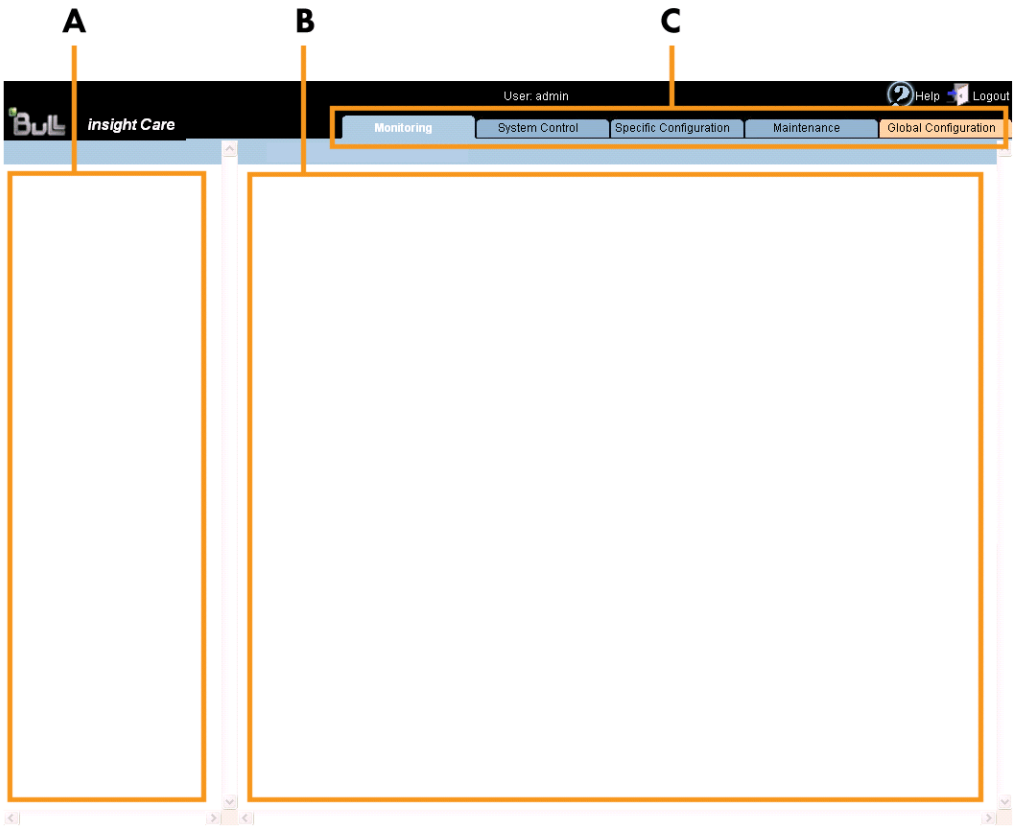
The following table lists the features available from the interface and their related sections in this guide.

Features
Importing, Managing and Monitoring Resources, on page 2-1 • Automatic discovery of hardware resources for resources in the same subnetwork • Import of hardware resources using XML files • Manual import • Direct connection to resource Web consoles • Serial Over LAN connection to managed host serial console
Building, Viewing and Managing Resource Logs, on page 3-1 • Severity color-based synthesis of received alerts • Advanced analysis of trap content • IPMI standard PET LAN, IPMI OEM PET LAN and platform specific SNMP trap decoding • Platform specific trap data field decoding • Simple or complex query options • Query template and result saving • Collection of SEL, Board & Security and BIOS Logs • Automatic Clear System Event Log option
Setting Up Autocalls, Action Requests and Intervention Reports, on page 4-1 • Comprehensive autocall transmission policy and filter options • Autocall transmission to GTS application in XML format • Intervention report generation and display • Action Request Package generation
Managing Users, on page 5-1

Table 1. Console features and related sections

Interface Structure

The user interface is divided into three areas in the browser window: a **Tree pane**, a **Work pane**, and **Tabs**.

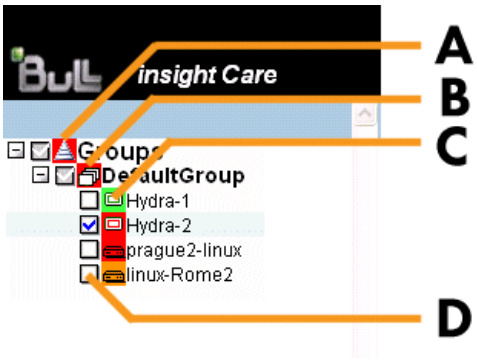


Interface Structure	
A: Tree pane	The **Tree pane** is tab-dependent: • When a **blue** tab is selected, the Tree pane displays the **Resource tree**. • When the **orange** tab is selected, the Tree pane displays the **Navigation tree**.
B: Work pane	The **Work pane** is tab-dependent: • When a **blue** tab is selected, the Work pane displays commands and information associated with the item selected in the **menu bar**. • If the **orange** tab is selected, the Work pane displays commands and information associated with the item selected in the **Navigation tree**.
C: Tabs	Five tabs are available and are organized by color: • The **Monitoring**, **System Control**, **Specific Configuration** and **Maintenance** tabs are blue. They provide access to features associated with the resource(s) selected in the Resource tree. • The **Global Configuration** tab is orange. It provides access to configuration features (especially initial configuration) that apply to all monitored resources.

Figure 3. Interface Structure

The Resource Tree

The Resource tree appears in the Tree pane when a blue tab is selected. It displays a hierarchal view of monitored resources and their status. The Resource tree is automatically refreshed at regular intervals.



Resource Tree	
Each item in the Resource tree is associated with an icon that indicates the current status of the monitored hardware resource: • GREEN: no problem • ORANGE: a warning event has been sent by the resource • RED: a critical event has been sent by the resource	
A: Global status icon	The Global status icon is located on the root node and allows you to check all monitored resources at a glance: • **Green**: all monitored resources are operating correctly • **Orange**: at least one monitored resource has sent a warning event • **Red**: at least one monitored resource has sent a critical event
B: Group status icon	The Group status icon allows you to check all the monitored resources in the group at a glance: • **Green**: all resources in the monitored group are operating correctly • **Orange**: at least one resource in the monitored group has sent a warning event • **Red**: at least one resource in the monitored group has sent a critical event
C: Resource status icon	The Resource status icon indicates the current status of the selected resource.
D: Check box	A check box is associated with each item in the Resource tree, allowing you to select the resource(s) for which you want to perform the action displayed in the Work pane (blue tab only).

Figure 4. Resource tree

Note See Monitoring Resources, on page 2-26 for more details about managing resource status.

Menu Bar

When a blue tab is selected, the Work pane displays a menu bar.

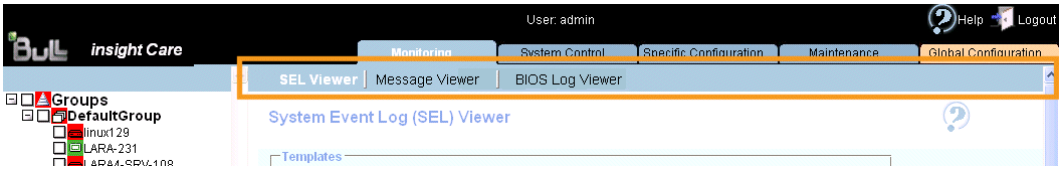


Figure 5. Menu Bar location

1.5. Initial Configuration

When you start the iCare Console for the first time, just after installation, you need to perform a few preliminary configuration tasks to ensure correct operation. These configuration tasks are listed below by order of priority:

- Setting Up the BMC Super User Password, on page 5-5
- Importing Resources, on page 2-2
- Configuring Autocalls, on page 4-3, if you have subscribed to Bull's Remote Maintenance service offer.

Note Other configuration tasks can be performed when required.

1.6. Stopping the iCare Console

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

Related Topics

- Starting the iCare Console, on page 1-4

Chapter 2. Importing, Managing and Monitoring Resources

This chapter explains how to import and manage hardware resources using the Resource tree which displays a hierarchal view of monitored resources and their status. It includes the following topics:

2.1. Importing Resources

The Resource tree displays a hierarchal view of resource status icons and is automatically refreshed at regular intervals. It appears in the left frame of the iCare Console when a blue tab is selected.

When you first set up the iCare Console to monitor resources or when you want to add or remove resources to or from the iCare Console perimeter, you must build and/or update the Resource tree.

Once a hardware resource has been imported into the Resource tree, it is automatically monitored and SEL and Board and Security Message logs are enabled.

Important **Hardware resources can only be monitored and maintained by ONE iCare Console at a given time.**
If you want to transfer the monitoring and maintenance of hardware resources to another iCare Console running on another PC, you MUST delete the hardware resources concerned from the current Resource tree before importing them into another Resource tree to ensure correct operation.
See Deleting a Resource from the Tree, on page 2-20 and Importing Resources, on page 2-2 for details.

The following tasks are explained in this section:

- Automatically Importing Resources, on page 2-3
- Manually Importing Multiple Resources, on page 2-5
- Manually Importing a Single Resource, on page 2-10
- Deleting a Resource from the Tree, on page 2-20
- Enabling/Disabling Resource Monitoring, on page 2-26

Note For a graphical description of Resource tree features, see Figure 4. Resource tree, on page 1-7.

Important **According to the embedded management controller firmware version on imported hardware resources, you may need to peform a mangement controller reset to synchronize with the iCare Console to ensure that alert transmission functions correctly.**

- **Check embedded management controller firmware version for a resource by connecting to the resource's Hardware Console.**
- **From the Maintenance tab, select Hardware Information > Management Board/Controller > Firmware Version:**
  - **if the first two digits are >10, synchronization is automatic,**
  - **if the first two digits are <10, you must perform a reset to synchronize with the iCare Console.**
- **If required, reset the resource by selecting Maintenance Operations > Unit Reset > Reset Management Controller > Reset.**

2.1.1. Automatically Importing Resources

The automatic discovery feature scans the subnetwork, detects any hardware resources that can be monitored by the iCare Console and adds them to the Resource tree.

You are strongly advised to use the automatic discovery feature to import compatible resources on the same subnetwork as the iCare Console. The manual import features are reserved for non-compatible resources or for resources on a different subnetwork to the iCare Console.

To import hardware resources outside the subnetwork or non-compatible with the automatic discovery feature, see the following sections:

- Manually Importing Multiple Resources, on page 2-5
- Manually Importing a Single Resource, on page 2-10

Prerequisites

The same **super** user password has been set up on all the hardware resources you want to discover and monitor from the iCare Console, as detailed in Setting Up the BMC Super User Password, on page 5-5.

The hardware resources you want to discover and monitor are on the same subnetwork as the iCare Console.

The hardware resources you want to discover and monitor are compatible with the automatic discovery feature.

The hardware resources you want to discover and monitor are not already monitored and maintained by another iCare Console. If this is the case, delete them from that console as explained in Deleting a Resource from the Tree, on page 2-20 before importing them into the current console.

Procedure

1. From the **Global Configuration** tab, click **Topology > Discovery**. The **Discovery** page appears.

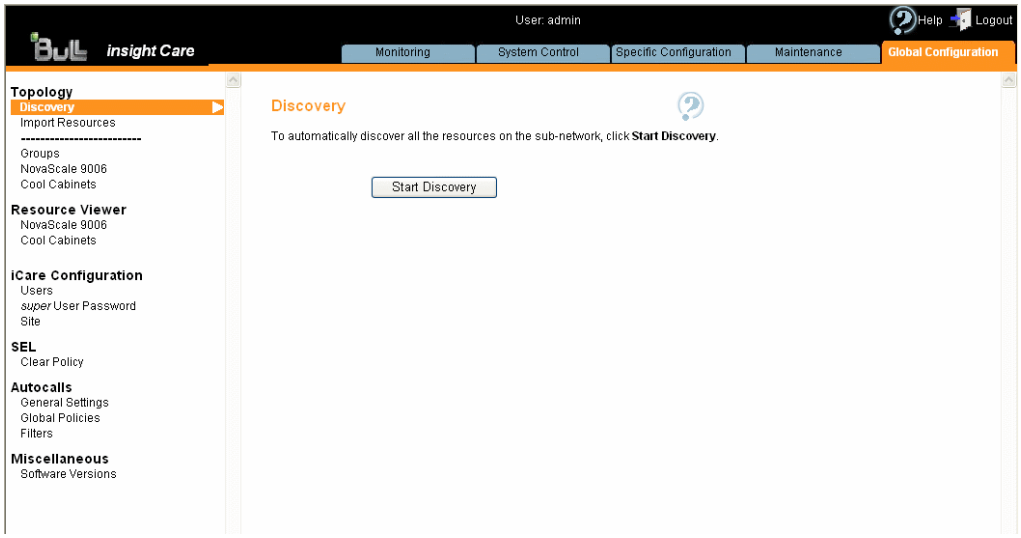


Figure 6. Discovery page

2. Click **Start Discovery**. The **Network Discovery Results** page appears.

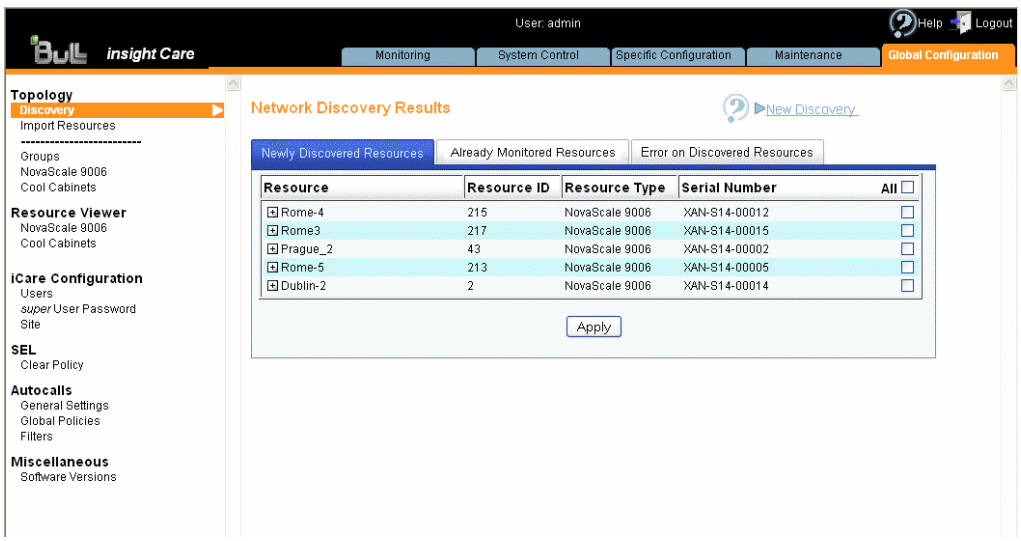


Figure 7. Network Discovery Results page - Multiple Resources

3. From the **Newly Discovered Resources** tab, select the resources you want to monitor and click **Apply**.

Note For more information about the **Network Discovery Results** page, see Managing Imported Resources, on page 2-13.

4. Click a blue tab to display the updated Resource tree.

According to the embedded management controller firmware version on imported hardware resources, you may need to peform a mangement controller reset to synchronize with the iCare Console to ensure that alert transmission functions correctly.

- **Check embedded management controller firmware version for a resource by connecting to the resource's Hardware Console.**
- **From the Maintenance tab, select Hardware Information > Management Board/Controller > Firmware Version:**
  - **if the first two digits are >10, synchronization is automatic,**
  - **if the first two digits are <10, you must perform a reset to synchronize with the iCare Console.**
- **If required, reset the resource by selecting Maintenance Operations > Unit Reset > Reset Management Controller > Reset.**

Related Topics

- Managing Imported Resources, on page 2-13
- Using an XML File to Import Multiple Resources , on page 2-8
- Manually Importing a Single Resource, on page 2-10
- Deleting a Resource from the Tree, on page 2-20
- Managing Resource Custom Groups, on page 2-21
- Viewing Resource Details, on page 2-29
- Connecting to a Resource Console, on page 2-30

2.1.2. Manually Importing Multiple Resources

When you want to import multiple hardware resources and these resources are not on the same subnetwork as the iCare Console or are not supported by the automatic discovery feature, you can create and use an XML import file.

You must first download the XML file template from the console and complete it with the required values.

If the hardware resources you want to import are on the same subnetwork as the iCare Console and are compatible, you are strongly advised to use the automatic discovery feature. For details, see Automatically Importing Resources, on page 2-3.

2.1.2.1. Creating a Hardware Resource XML Import File

Hardware resource XML import files are created by downloading the appropriate template(s) from the iCare Console and adding the information indicated in the file.

Although different templates are available according to hardware resource type, the resulting XML import files can either be used separately or merged into a single XML import file when you are ready to import resources.

Prerequisites

You have the information required to complete the XML import template file fields

Procedure

1. From the **Global Configuration** tab, click **Topology > Import Resource**. The **Import Resources** page appears.
2. Check that the **XML File Import** tab is selected.

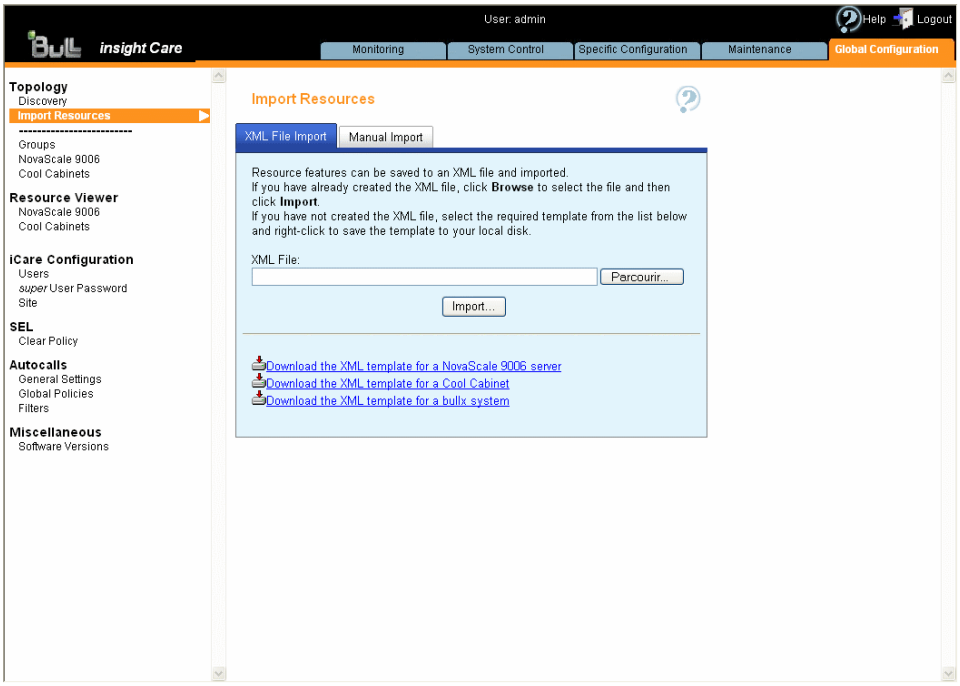


Figure 8. Import Resources page - XML File Import tab

3. Right-click the link corresponding to the XML template file you want to download and select **Save link as** (Firefox) or **Save target as** (Internet Explorer).

4. Open the saved XML template file with **Notepad**. The following figure shows an example of an XML template file opened with Notepad:

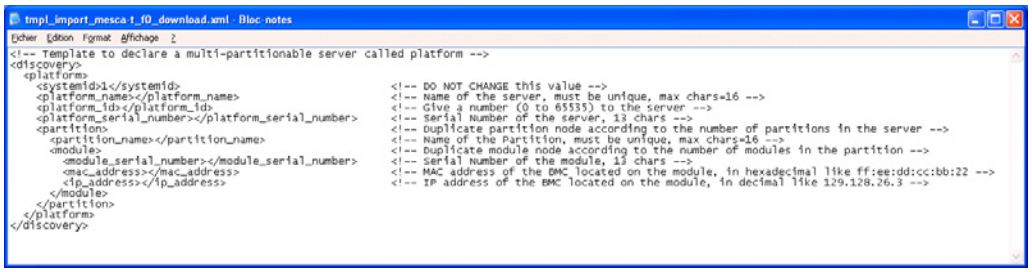


Figure 9. XML template file - NovaScale 9006 Server example

5. Edit the file by reading the XML comments (example: `<!--- DO NOT CHANGE this value -->`).
   The information required to complete the file can be found by connecting to the corresponding resource Hardware Console.
6. Save the XML import file.
7. Repeat this operation for each type of hardware resource that you want to import into the Resource tree. Once you have prepared all the required XML import files, you can use them separately or merge them into a single file to import resources, as detailed in Using an XML File to Import Multiple Resources , on page 2-8.

Related Topics

- Using an XML File to Import Multiple Resources , on page 2-8
- Manually Importing a Single Resource, on page 2-10
- Managing Resource Custom Groups, on page 2-21
- Viewing Resource Details, on page 2-29
- Connecting to a Resource Console, on page 2-30

2.1.2.2. Using an XML File to Import Multiple Resources

Hardware resource XML import files are created by downloading the appropriate template(s) from the iCare Console and adding the information indicated in the file.

Although different templates are available according to hardware resource type, the resulting XML import files can either be used separately or merged into a single XML file when you are ready to import resources.

Prerequisites

The same **super** user password has been set up on all the hardware resources you want to import and monitor from the iCare Console, as detailed in Setting Up the BMC Super User Password, on page 5-5.

The required hardware resource XML import file has been created, as explained in Creating a Hardware Resource XML Import File, on page 2-6.

The hardware resources you want to discover and monitor are not already monitored and maintained by another . If this is the case, delete them from that console as explained in Deleting a Resource from the Tree, on page 2-20 before importing them into the current console.

Procedure

1. From the **Global Configuration** tab, click **Topology > Import Resources**. The **Import Resources** page appears.
2. Check that the **XML File Import** tab is selected.

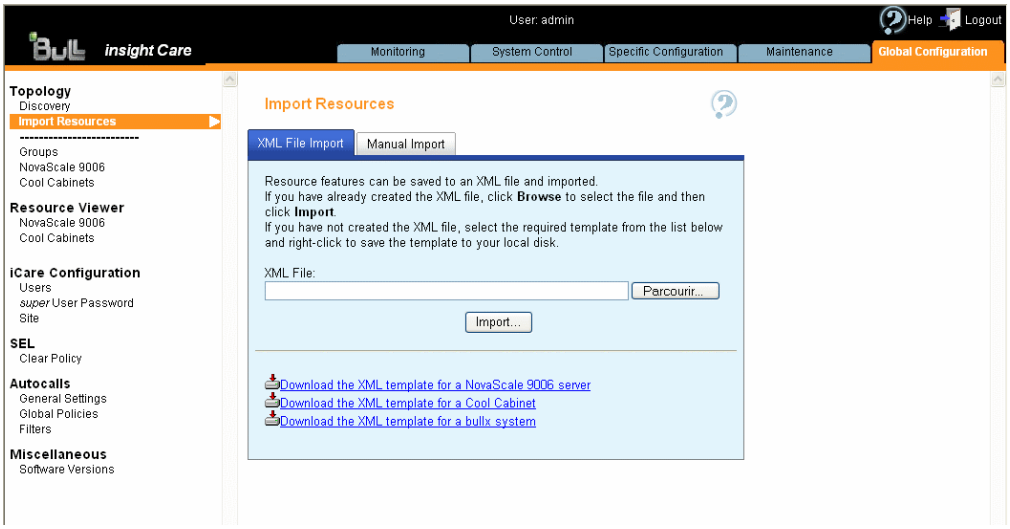


Figure 10. Import Resources page - XML File Import tab

3. Click **Browse** to locate and specify the required XML file path.

4. Click **Import**. A consistency check is performed on the XML import file and the discovered hardware resources appear as shown in the following page:

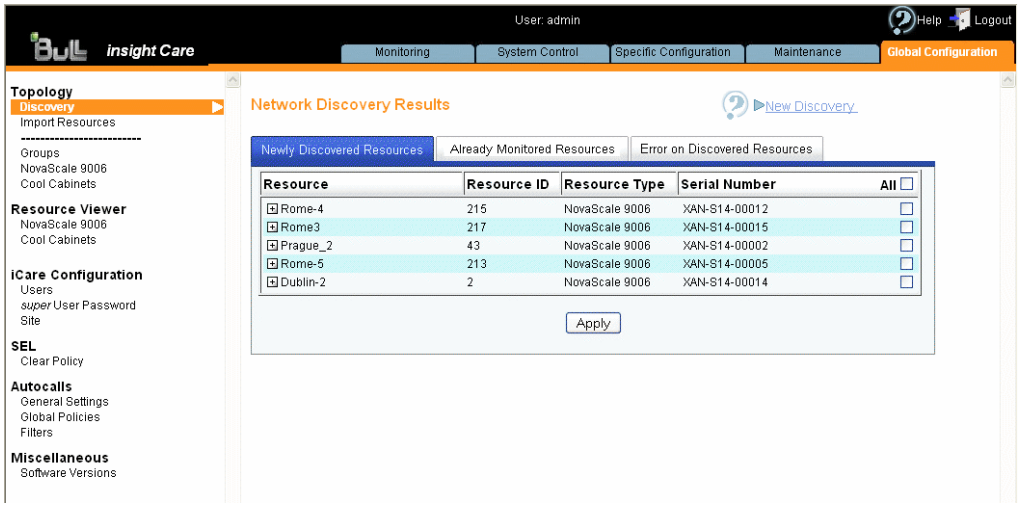


Figure 11. Network Discovery Results page - Multiple Resources

5. From the list of discovered hardware resources, select the resources you want to monitor and click **Apply**.

> **Note** For more information about the Network Discovery Results page, see Managing Imported Resources, on page 2-13.

6. Click a blue tab to display the updated Resource tree.

Important **According to the embedded management controller firmware version on imported hardware resources, you may need to peform a mangement controller reset to synchronize with the iCare Console to ensure that alert transmission functions correctly.**

1. **Check embedded management controller firmware version for a resource by connecting to the resource's Hardware Console.**
2. **From the Maintenance tab, select Hardware Information > Management Board/Controller > Firmware Version:**
   - **if the first two digits are >10, synchronization is automatic,**
   - **if the first two digits are <10, you must perform a reset to synchronize with the iCare Console. Go to Step 3.**
3. **If required, reset the resource by selecting Maintenance Operations > Unit Reset > Reset Management Controller > Reset.**

Related Topics

- Managing Imported Resources, on page 2-13
- Creating a Hardware Resource XML Import File, on page 2-6
- Automatically Importing Resources, on page 2-3
- Manually Importing a Single Resource, on page 2-10
- Deleting a Resource from the Tree, on page 2-20
- Managing Resource Custom Groups, on page 2-21
- Viewing Resource Details, on page 2-29
- Connecting to a Resource Console, on page 2-30

2.1.3. Manually Importing a Single Resource

The iCare Console includes a manual import feature that you can use to add a single resource on a different subnetwork to the iCare Console.

Important **If the hardware resource you want to import is on the same subnetwork as the iCare Console and is compatible, you are strongly advised to use the automatic discovery feature. See Automatically Importing Resources, on page 2-3.**

Prerequisites

The same **super** user password has been set up on all the resources you want to import and monitor, as detailed in Setting Up the BMC Super User Password, on page 5-5.

The hardware resources you want to discover and monitor are not already monitored and maintained by another iCare Console. If this is the case, delete them from that console as explained in Deleting a Resource from the Tree, on page 2-20 before importing them into the current console.

Procedure

1. From the **Global Configuration** tab, click **Topology > Import Resources**. The **Import Resources** page appears.
2. Click the **Manual Import** tab and select the type of hardware resource you want to import from the **Resource Type** drop-down list.

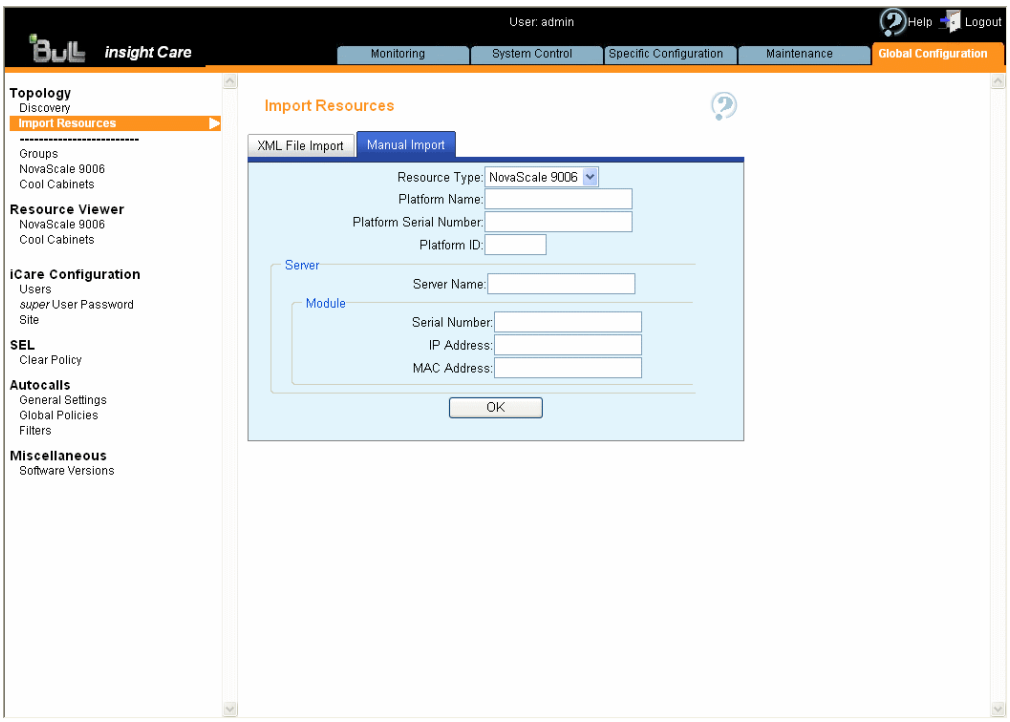


Figure 12. Import Resources page - Manual Import tab

3. Use the resource Hardware Console configuration data to complete the fields, as explained in the following table:

Manual Import - Serv ers	
Platform Name	Platform name - 16 characters maximum
Platform Serial Number	Platform serial number - 13 characters
Platform ID	Platform ID - Value between 0 and 65535
Server Name	Server name - 16 characters maximum
Serial Number	Module serial number - 13 characters
IP Address	BMC IP address - decimal values (example: 129.192.1.10)
MAC Address	Module MAC address - hexadecimal values (example: 5E:FF:56:A2:AF:15)
Manual Import - Cool Cabinets	
Name	Cool Cabinet name - 16 characters maximum
Serial Number	Cool Cabinet serial number - 13 characters
IP Address	Cool Cabinet BMC static IP address - decimal values (example: 129.192.1.10)
MAC Address	Cool Cabinet BMC MAC address - hexadecimal values (example: 5E:FF:56:A2:AF:15)

Table 2. Manual import data

4. Once you have completed all the fields, click **OK**. The **Network Discovery Results** page appears:

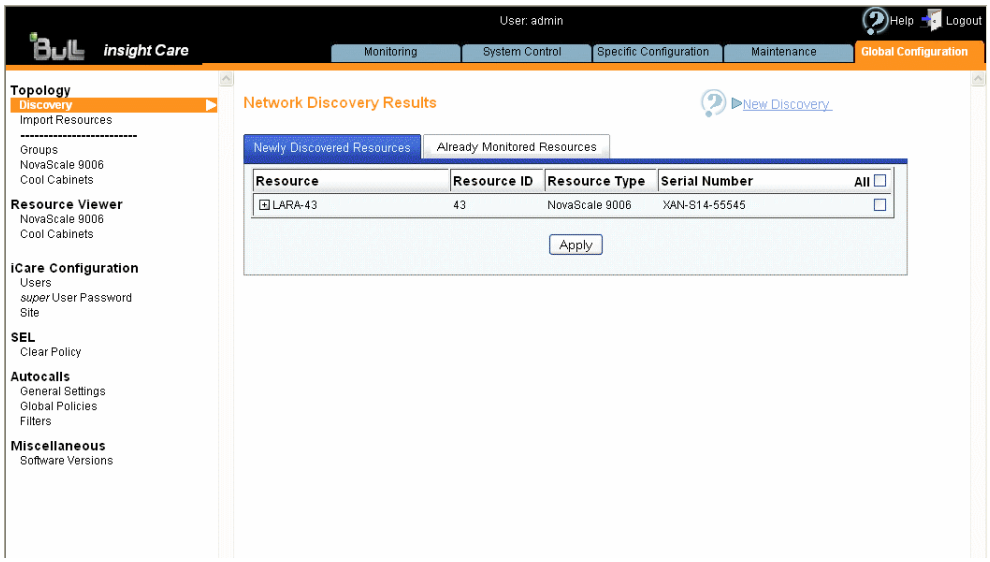


Figure 13. Network Discovery Results page - Single Resource

5. Select the resource and click Apply.

Note For more information about the Network Discovery Results page, see Managing Imported Resources, on page 2-13.

6. Click a blue tab to display the updated Resource tree.

Important **According to the embedded management controller firmware version on imported hardware resources, you may need to peform a mangement controller reset to synchronize with the iCare Console to ensure that alert transmission functions correctly.**

- **Check embedded management controller firmware version for a resource by connecting to the resource's Hardware Console.**
- **From the Maintenance tab, select Hardware Information > Management Board/Controller > Firmware Version:**
  - **if the first two digits are >10, synchronization is automatic,**
  - **if the first two digits are <10, you must perform a reset to synchronize with the iCare Console.**
- **If required, reset the resource by selecting Maintenance Operations > Unit Reset > Reset Management Controller > Reset.**

Related Topics

- Managing Imported Resources, on page 2-13
- Automatically Importing Resources, on page 2-3
- Using an XML File to Import Multiple Resources , on page 2-8
- Deleting a Resource from the Tree, on page 2-20
- Managing Resource Custom Groups, on page 2-21
- Viewing Resource Details, on page 2-29
- Connecting to a Resource Console, on page 2-30

2.2. Managing Imported Resources

The **Network Discovery Results** page is automatically displayed when you build the Resource tree using one of the procedures described in:

- Automatically Importing Resources, on page 2-3
- Using an XML File to Import Multiple Resources , on page 2-8
- Manually Importing a Single Resource, on page 2-10

According to results, this page can contain up to three tabs which are detailed in the following sections:

- Adding Newly Discovered Resources to the Resource Tree, on page 2-14
- Viewing Already Monitored Resources, on page 2-15
- Troubleshooting Errors on Discovered Resources, on page 2-16

2.2.1. Adding Newly Discovered Resources to the Resource Tree

When new hardware resources are imported, they are displayed under the **Newly Discovered Resources** tab in the **Network Discovery Results** page, allowing you to select the new resources you want to add to the Resource tree and monitor.

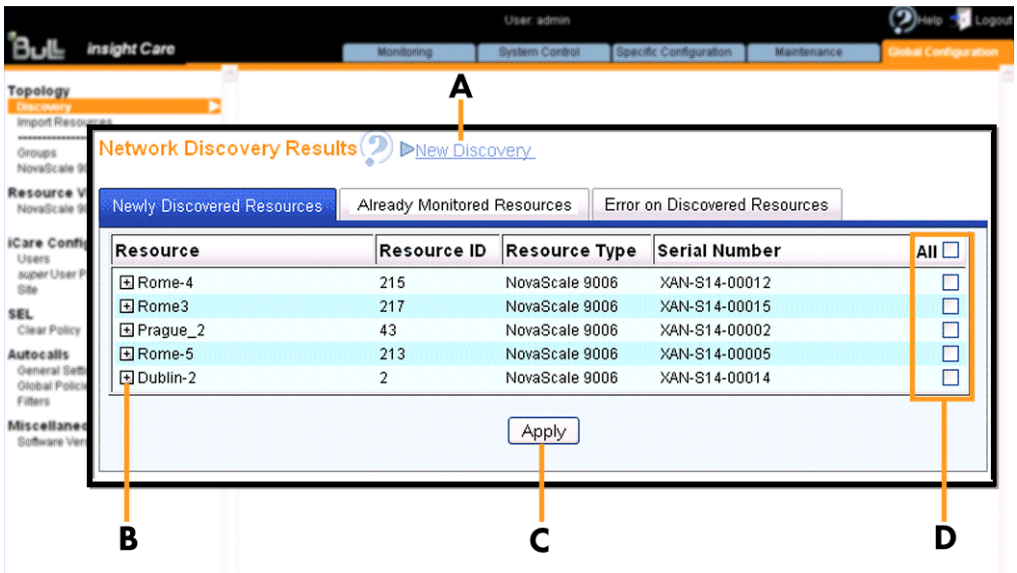
Note If the automatic discovery feature does not detect any new resources, the message **No resources discovered** is displayed.

Prerequisites

You have imported hardware resources using one of the import methods explained in Importing Resources, on page 2-2.

Procedure

1. When the **Network Discovery Results** page appears displaying the results of the import procedure previsouly launched, open the **Newly Discovered Resources** tab.
2. Select the hardware resources you want to add to the Resource tree and monitor, as explained in the table below.



Newly Discovered Resources	
A: **New Discovery** link	Click this link to launch a new discovery
B: **Expand/Collapse** button	Click this button to show/hide detailed resource information
C: **Apply** button	Click **Apply** to import the selected resources into the Resource tree
D: Check boxes	Click **All** to select all the displayed resources, or select the individual check boxes corresponding to the specific resources you want to import

Figure 14. Network Discovery Results page (Newly Discovered Resources tab)

Related Topics

- Viewing Already Monitored Resources, on page 2-15
- Troubleshooting Errors on Discovered Resources, on page 2-16

2.2.2. Viewing Already Monitored Resources

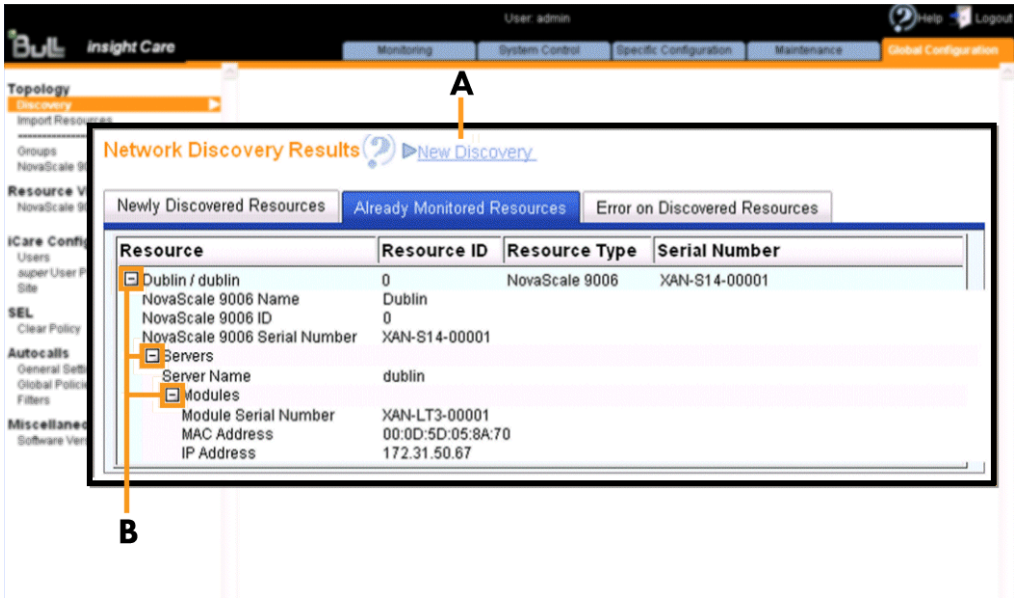
When hardware resources that are already monitored are re-discovered, they are displayed under the **Already Monitored Resources** tab in the **Network Discovery Results** page, allowing you to view detailed information about these resources.

Prerequisites

You have imported hardware resources using one of the import methods explained in Importing Resources, on page 2-2.

Procedure

1. When the **Network Discovery Results** page appears displaying the results of the import procedure previsouly launched, open the **Already Monitored Resources** tab.
2. Select the hardware resources for which you want to view details and use the **Expand** button to display information, as explained in the table below.



Already Monitored Resources	
A: New Discovery link	Click this link to launch a new discovery
B: Expand/Collapse button	Click this button to show/hide detailed resource information

Figure 15. Network Discovery Results page (Already Monitored Resources tab)

Related Topics

- Adding Newly Discovered Resources to the Resource Tree, on page 2-14
- Troubleshooting Errors on Discovered Resources, on page 2-16

2.2.3. Troubleshooting Errors on Discovered Resources

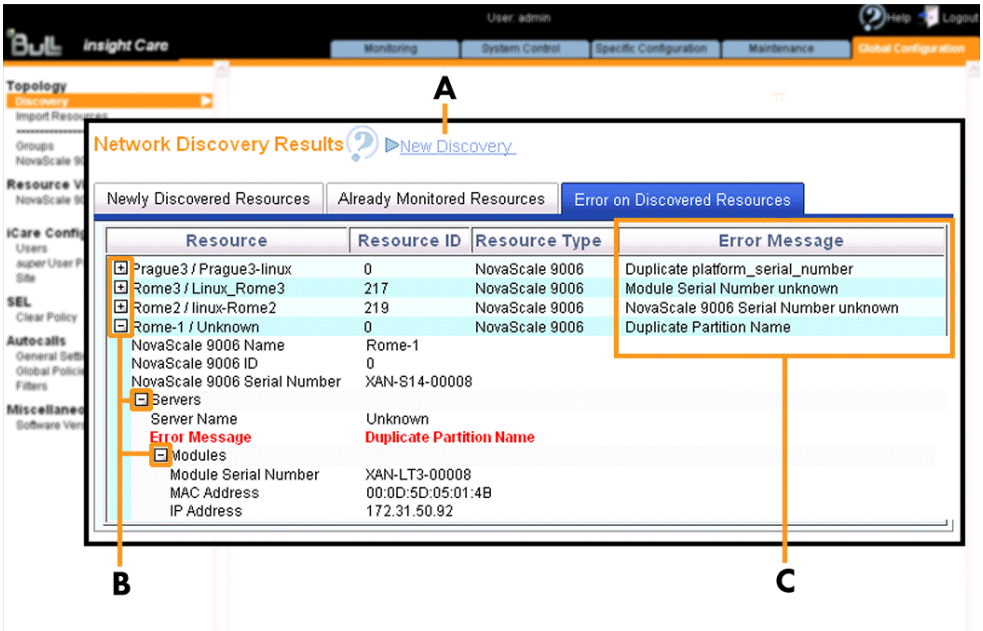
When hardware resources are discovered but cannot be imported, they are displayed under the **Error on Discovered Resources** tab in the **Network Discovery Results** page, allowing you to easily troubleshoot discovery errors.

Prerequisites

You have tried to import hardware resources using one of the import methods explained in Importing Resources, on page 2-2.

Procedure

1. When the **Network Discovery Results** page appears displaying the results of the import procedure previsouly launched, open the **Error on Discovered Resources** tab.
2. Select the hardware resources for which you want to view details and use the **Expand** button to display error messages, as explained in the table below.



Error on Discovered Resources	
A: **New Discovery** link	Click this link to launch a new discovery
B: **Expand/Collapse** button	Click this button to show/hide detailed information about the error message
C: **Error Message** column	Displays the error message label

Figure 16. Network Discovery Results page (Error on Discovered Resources tab)

3. Use the following **Discovery Error Messages and Troubleshooting Actions** tables to resolve problems before launching a new discovery.

Discovery Error Messages and Troubleshooting Actions

Message	Duplicate partition name
Resource Type	• NovaScale 9006 Servers • bullx systems
Description	2 (or more) resources use the same partition name
Actions	• Start the resource hardware console, check and if required, change the partition name value (**Configuration** tab, **Global Settings > Managed Server** menu, **Managed Server Name** field), then re-import the resource. • XML File Import - typing error: change the resource `<partition_name>` XML tag value, then re-import the XML file. • Manual Import - typing error: re-import the resource.

Table 3. Duplicate partition name error

Message	Duplicate platform name
Resource Type	• NovaScale 9006 Servers • Cool Cabinets • bullx systems
Description	2 (or more) resources use the same platform name
Actions	• Start the resource hardware console, check and if required, change the platform name value (**Configuration** tab, **Global Settings > Platform** menu, **Platform Name** field), then re-import the resource. • XML File Import - typing error: change the resource `<platform_name>` XML tag value, then re-import the XML file. • Manual Import - typing error: re-import the resource.

Table 4. Duplicate platform name error

Message	Duplicate platform ID
Resource Type	• NovaScale 9006 Servers • bullx systems
Description	2 (or more) resources use the same platform ID
Actions	• Start the resource hardware console, check and if required, change the platform ID value (**Configuration** tab, **Global Settings > Platform** menu, **Platform ID** field), then re-import the resource. • XML File Import - typing error: change the resource `<platform_id>` XML tag value, then re-import the XML file. • Manual Import - typing error: re-import the resource.

Table 5. Duplicate platform ID error

Message	Duplicate platform serial number
Resource Type	• NovaScale 9006 Servers • Cool Cabinets • bullx systems
Description	2 (or more) resources use the same platform serial number
Actions	• XML File Import - typing error: change the resource <platform_serial_number> XML tag value, then re-import the XML file. • Manual Import - typing error: re-import the resource. • If this is not a typing error, contact your Customer Service Engineer.

Table 6. Duplicate platform serial number error

Message	Platform serial number unknown
Resource Type	• NovaScale 9006 Servers • bullx systems
Description	The module serial number may not be engraved.
Actions	Contact your Customer Service Engineer.

Table 7. Platform serial number unknown error

Message	Duplicate module serial number
Resource Type	• NovaScale 9006 Servers • bullx systems
Description	2 (or more) resources use the same module serial number
Actions	• XML File Import - typing error: change the resource <module_serial_number> XML tag value, then re-import the XML file. • Manual Import - typing error: re-import the resource. • If this is not a typing error, contact your Customer Service Engineer.

Table 8. Duplicate module serial number error

Message	Module serial number unknown
Resource Type	• NovaScale 9006 Servers • bullx systems
Description	The module serial number may not be engraved.
Actions	Contact your Customer Service Engineer.

Table 9. Module serial number unknown error

Message	Module count does not match the number of modules
Resource Type	• NovaScale 9006 Servers • bullx systems
Description	The number of <module> <\module> XML tags is not correct.
Actions	Change the number of <module> <\module> XML tags, then re-import the file.

Table 10. Module count does not match the number of modules error

Message	Duplicate MAC address
Resource Type	• NovaScale 9006 Servers • Cool Cabinets • bullx systems
Description	2 (or more) resources use the same MAC address
Actions	• XML File Import - typing error: change the resource <mac_address> (platform or module) XML tag value, then re-import the XML file. • Manual Import - typing error: re-import the resource. • If this is not a typing error, contact your Customer Service Engineer.

Table 11. Duplicate MAC address error

Message	Duplicate IP address
Resource Type	• NovaScale 9006 Servers • Cool Cabinets • bullx systems
Description	2 (or more) resources use the same IP address
Actions	• XML File Import - typing error: change the resource <ip_address> (platform or module) XML tag value, then re-import the XML file. • Manual Import - typing error: re-import the resource. • If this is not a typing error, contact your Network administrator.

Table 12. Duplicate IP address error

Related Topics

- Adding Newly Discovered Resources to the Resource Tree, on page 2-14
- Viewing Already Monitored Resources, on page 2-15

2.2.4. Deleting a Resource from the Tree

When you no longer want to monitor a hardware resource from the iCare Console or if you want to transfer monitoring and maintenance to another iCare Console, you must delete it from the Resource tree.

Important Once a hardware resource is deleted, it disappears from the Resource tree and database entries are no longer accessible for this resource.

Prerequisites

The hardware resource is present in the Resource tree

Procedure

1. From the **Global Configuration** tab, select the hardware resource type under **Topology**. The resource management page appears.

   Note The list of hardware resource types is generated dynamically. If the Resource tree is empty, no resource type is available for selection.

2. Select the hardware resource(s) you want to delete (a), click **Delete** (b) and then click OK in the displayed confirmation box (c). The selected hardware resource(s) is removed from the Resource tree.

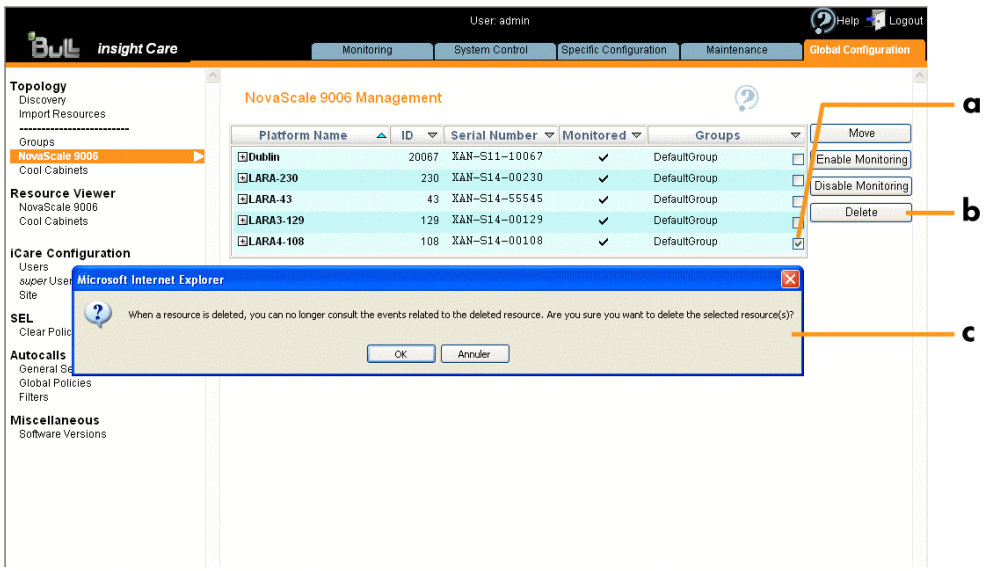


Figure 17. Deleting a Resource

3. Click a blue tab to display the updated Resource tree.

Related Topics

- Adding a Resource to a Resource Group, on page 2-25
- Enabling/Disabling Resource Monitoring, on page 2-26

2.3. Managing Resource Custom Groups

When hardware resources are imported into the Resource tree, they are automatically monitored and added to the predefined resource group called **DefaultGroup**, which is used by default to represent a set of hardware resources. This group cannot be renammed or deleted.

To allow you to organize and monitor your hardware resources according to your needs, you can create your own resource groups or **Custom Groups** and then edit, delete or move resources between groups.

The following tasks are explained in this section:

- Creating a Resource Custom Group, on page 2-21
- Editing Resource Custom Group Details, on page 2-23
- Deleting a Resource Custom Group, on page 2-24
- Adding a Resource to a Resource Group, on page 2-25

Note For a graphical description of Resource tree features, refer to Figure 4. Resource tree, on page 1-7.

2.3.1. Creating a Resource Custom Group

The iCare Console is delivered with one predefined group, **DefaultGroup**, which cannot be modified or deleted.

To allow you to organize your hardware resources to suit your needs, you can create your own resource groups or **Custom Groups**.

Prerequisites

None

Procedure

1. From the **Global Configuration** tab, click **Topology > Groups**. The **Groups Management** page appears.

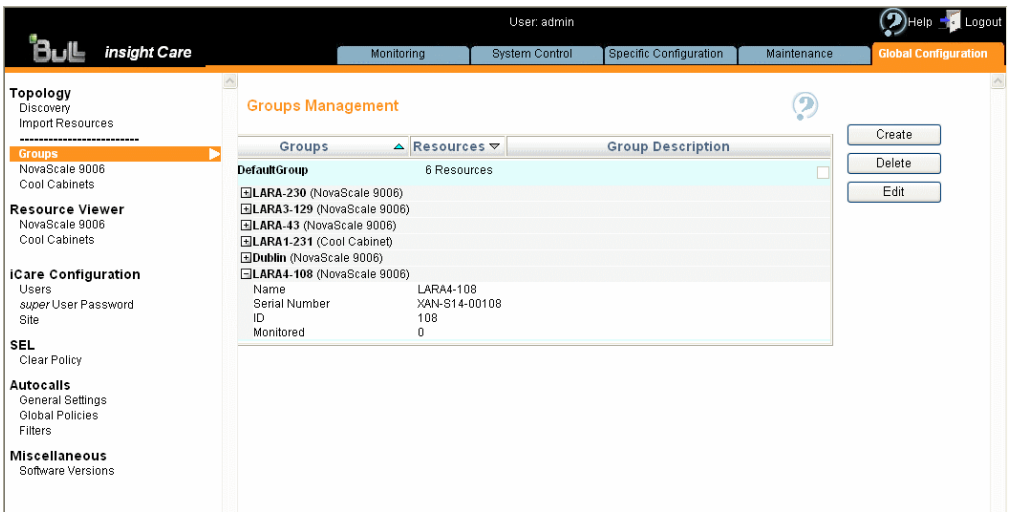
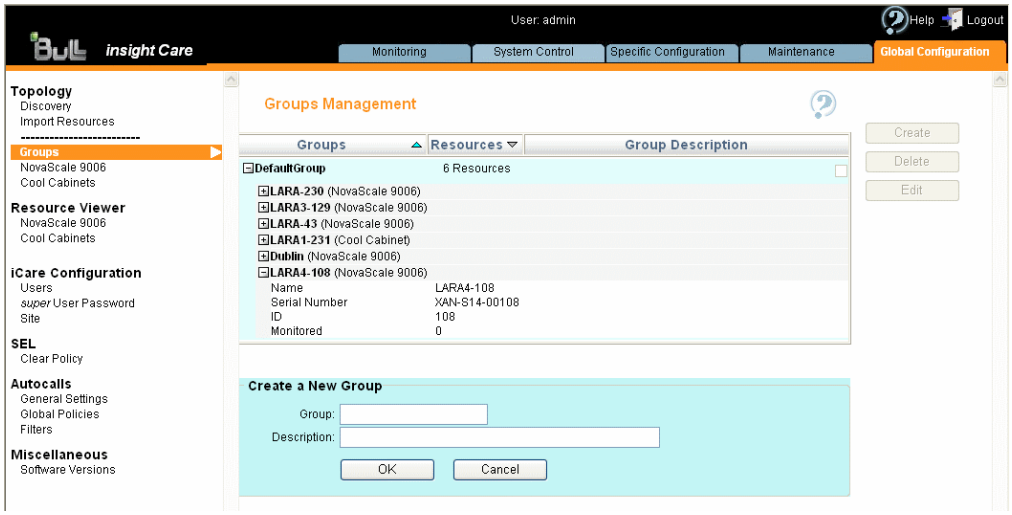


Figure 18. Groups Management page

2. Click **Create**. The **Create a New Group** box appears.



Create a New Group	
Group	Name given to the group. The group name is limited to 16 characters. The following characters are not allowed: /\"`&'+*%=><:!?;,~| and space.
Description	(Optional) Additional information on the group

Figure 19. Create a New Group box

3. Click **OK**. The group appears in the **Groups Management** page.
4. You can now associate hardware resources with the new group. See Adding a Resource to a Resource Group, on page 2-25.

Note The new group only appears in the Resource tree when a hardware resource has been associated with the group.

Related Topics

- Editing Resource Custom Group Details, on page 2-23
- Deleting a Resource Custom Group, on page 2-24
- Adding a Resource to a Resource Group, on page 2-25
- Manually Importing Multiple Resources, on page 2-5

2.3.2. Editing Resource Custom Group Details

You can change a custom group name and/or description at any time to reflect changes in your working environment.

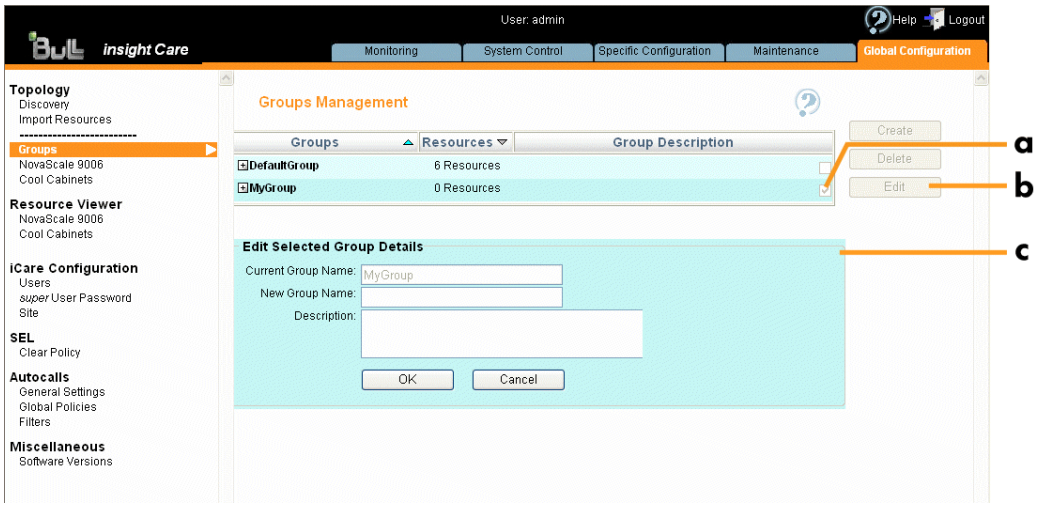
Note The predefined group **DefaultGroup** cannot be edited.

Prerequisites

None

Procedure

1. From the **Global Configuration** tab, click **Topology > Groups**. The **Groups Management** page appears.
2. Select the group you want to modify (a) and click **Edit** (b). The **Edit Selected Group Details** box appears (c).



Edit Selected Group Details	
Current Group Name	Read-only field
New Group Name	The new group name is limited to 16 characters. The following characters are not allowed: /\"`&'+*%=><:!?;,~| and space.
Description	(Optional) Additional information about the group

Figure 20. Edit Selected Group Details box

3. Complete the box and click **OK** to apply changes.

Related Topics

- Manually Importing Multiple Resources, on page 2-5
- Deleting a Resource Custom Group, on page 2-24
- Creating a Resource Custom Group, on page 2-21

2.3.3. Deleting a Resource Custom Group

Any custom groups that you no longer need due to changes in your working environment, for example, can be deleted at any time.

Notes
- The predefined group **DefaultGroup** cannot be deleted.
- If you delete a group that still contains hardware resources, these resources are automatically associated with the predefined group **DefaultGroup**.

Prerequisites

None

Procedure

1. From the **Global Configuration** tab, click **Topology > Groups**. The **Groups Management** page appears.
2. Select the group you want to delete (a) and click **Delete** (b). A confirmation box appears (c).

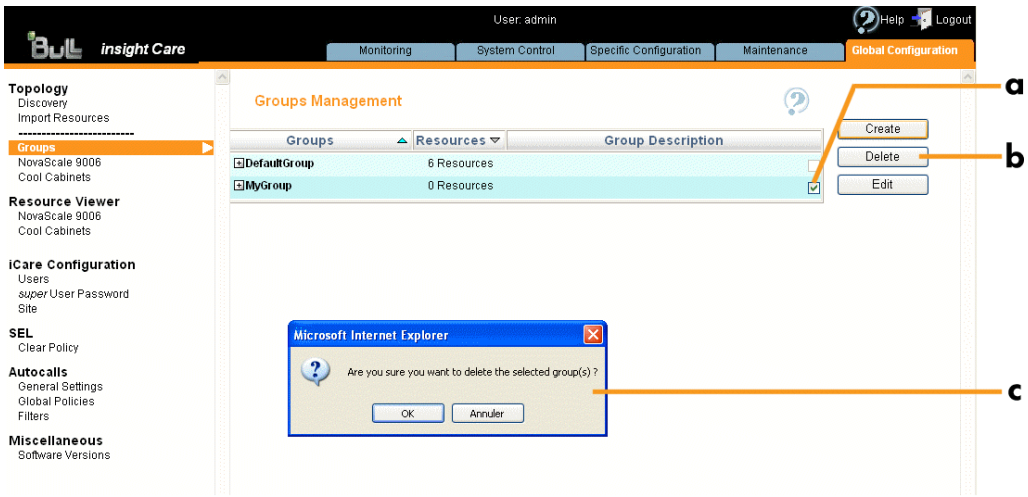


Figure 21. Groups Management page - Group deletion

3. Click **OK** to delete the custom group.

Related Topics

- Creating a Resource Custom Group, on page 2-21
- Editing Resource Custom Group Details, on page 2-23

2.3.4. Adding a Resource to a Resource Group

Hardware resources can be freely moved to and from custom groups and/or the default group, according to your needs.

Prerequisites

At least one custom group is created (for details, see Creating a Resource Custom Group, on page 2-21).

Procedure

1. From the **Global Configuration** tab, select the resource type under **Topology**. The resource management page appears.

   Note The list of hardware resource types is generated dynamically. If the Resource tree is empty, no resource type is available for selection.: if the resource tree is not built, no item is available.

2. Select the hardware resources you want to add to another group (a) and click **Move** (b). The **Move Selected Resources to New Group** box appears (c).

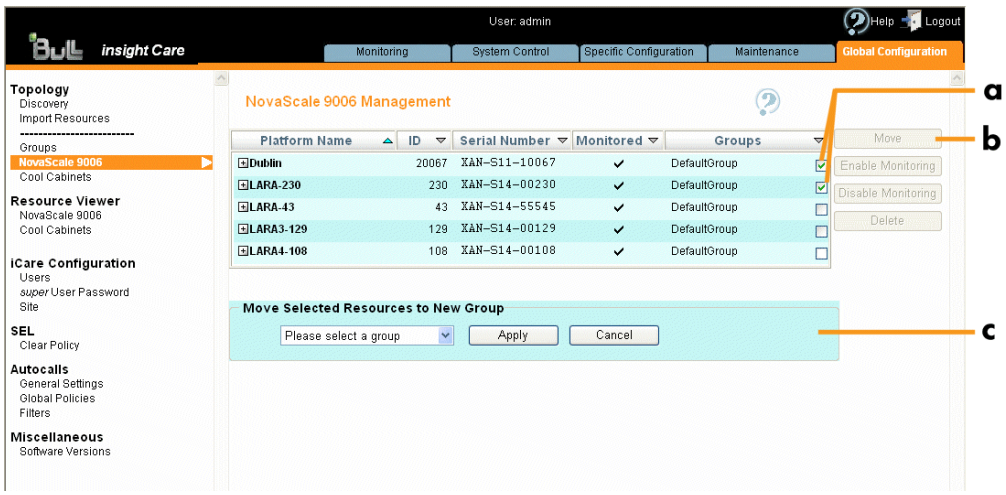


Figure 22. Moving Resources (example with Novascale 9006 servers)

3. From the drop-down list, select the group to which you want to add the selected resource(s) and click **Apply**.
4. Click a blue tab to display the updated Resource tree.

Related Topics

- Managing Resource Custom Groups, on page 2-21
- Enabling/Disabling Resource Monitoring, on page 2-26
- Deleting a Resource from the Tree, on page 2-20

2.4. Monitoring Resources

A hardware resource imported into the iCare Console is automatically monitored, which implies that:

- The resource appears in the Resource tree and is associated with an icon that indicates its current status.
- The SEL event tracking feature is enabled.

2.4.1. Enabling/Disabling Resource Monitoring

You can enable or disable the monitoring feature for any imported hardware resource.

Important **When monitoring is disabled for a hardware resource, it disappears from the Resource tree and events are no longer recorded.**
Events recorded when the hardware resource was monitored remain in the iCare Console database. To consult them, you must re-enable monitoring for the hardware resource.
If you want to permanently stop monitoring a hardware resource from the current iCare Console, you are advised to delete the hardware resource from the Resource tree. For details, see Deleting a Resource from the Tree, on page 2-20.

Prerequisites

The hardware resource is present in the Resource tree

Procedure

1. From the Global Configuration tab, select the hardware resource type under Topology. The resource management page appears.

   Note The list of hardware resource types is generated dynamically. If the Resource tree is empty, no hardware resource type is available.

2. Do one of the following:

   a. To enable monitoring for one or more hardware resource(s), select the resource(s) (a), click Enable Monitoring (b) and then click OK in the displayed confirmation box (c). The selected resources re-appear in the Resource tree and event logging starts again.

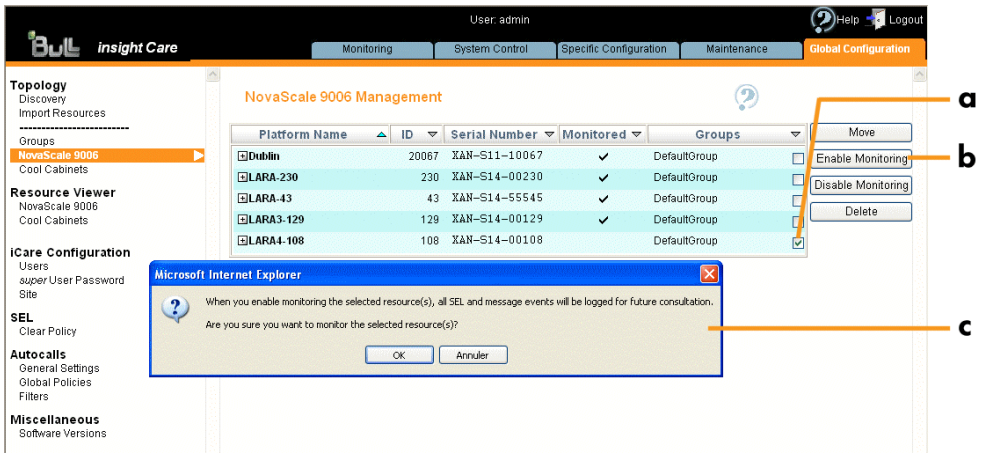


Figure 23. Enabling Resource Monitoring

b. To disable monitoring for one or more hardware resource(s), select the resource(s) (a), click **Disable Monitoring** (b) and then click **OK** in the displayed confirmation box (c). The selected resources disappear from the Resource tree and event logging stops.

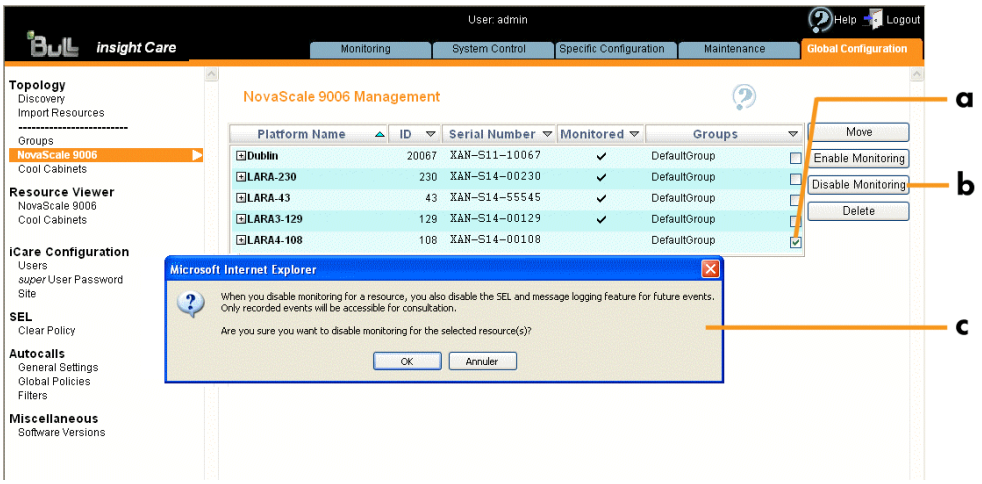


Figure 24. Disabling Resource Monitoring

3. Click a blue tab to display the updated Resource tree.

Important **According to the embedded management controller firmware version on imported hardware resources, you may need to peform a mangement controller reset to synchronize with the iCare Console to ensure that alert transmission functions correctly.**

- **Check embedded management controller firmware version for a resource by connecting to the resource's Hardware Console.**
- **From the Maintenance tab, select Hardware Information > Management Board/Controller > Firmware Version:**
  - **if the first two digits are >10, synchronization is automatic,**
  - **if the first two digits are <10, you must perform a reset to synchronize with the iCare Console.**
- **If required, reset the resource by selecting Maintenance Operations > Unit Reset > Reset Management Controller > Reset.**

Related Topics

- Monitoring Resources, on page 2-26
- Adding a Resource to a Resource Group, on page 2-25
- Deleting a Resource from the Tree, on page 2-20

2.4.2. Understanding Resource Status

Resource status can be easily viewed from the Resource tree, which is automatically refreshed at regular intervals.

Status indicators are available at three levels in the Resource tree:

- **Global status** icon, located on the root node
- **Group status** icon, associated with the resource group node
- **Resource status** icon, associated with each individual resource

When an event is received in the iCare Console database, the status icons change color to reflect event severity, as explained in Table 13. You can then query the database to view the event and analyze the problem, as explained in Building and Viewing System Event Logs (SEL), on page 3-2.

Status Icons	
Global status icon	This icon is located on the root node and indicates the status of all monitored resources: • **Green**: all resources are operating correctly • **Orange**: at least one warning event has been received • **Red**: at least one critical event has been received
Resource Group status icon	This icon indicates the status of all the monitored resources in the resource group: • **Green**: all resources in the group are operating correctly • **Orange**: at least one warning event has been received • **Red**: at least one critical event has been received
Resource status icon	This icon indicates the status of the resource: • **GREEN**: the resource is operating correctly • **ORANGE**: a warning event has been received • **RED**: a critical event has been received

Table 13. Resource status icons

Related Topics

- iCare Console Overview, on page 1-5
- Enabling/Disabling Resource Monitoring, on page 2-26
- Building and Viewing System Event Logs (SEL), on page 3-2
- Managing System Event Logs (SEL), on page 3-6

2.5. Viewing Resource Details

The Resource details pages give you a synthetic view of significant resource data, such as:

- IP and MAC addresses
- Serial number
- Server name, Group name, Platform name and ID

Prerequisites

The hardware resources for which you want to view data are present in the Resource tree.

Procedure

1. From the **Global Configuration** tab, select the required resource type under the **Resource Viewer** menu. The resource list appears.

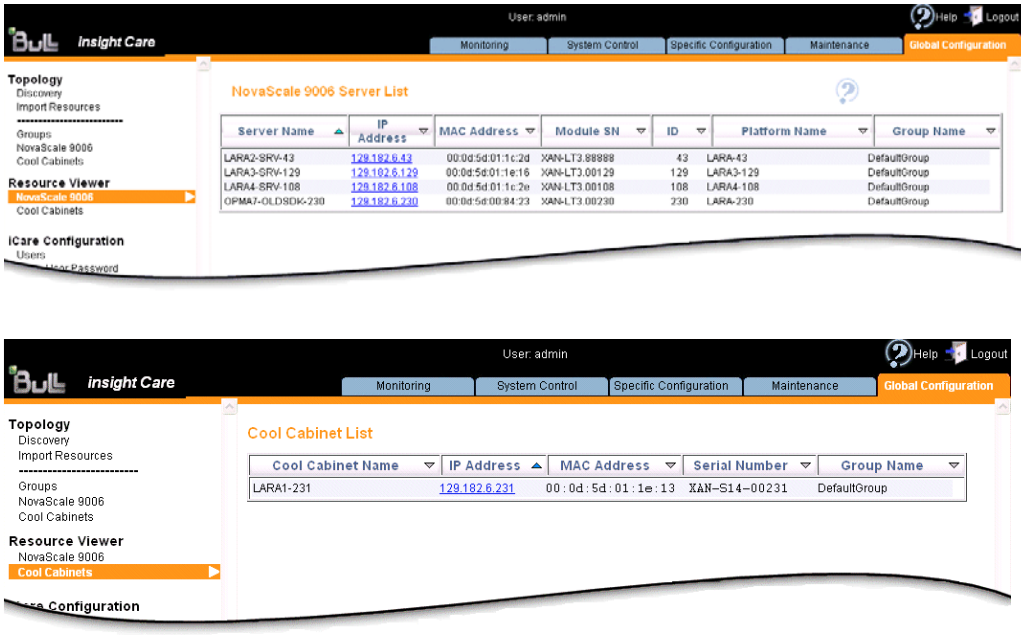


Figure 25. Resource Viewer page - Examples

2. You can now manage displayed data as required:
   - Use the **Sort** icons in the table headers to sort data according to type.
   - Use the **IP Address Links** to directly connect to the selected resources' hardware consoles.

Related Topics

- Connecting to a Resource Console, on page 2-30

2.6. Connecting to a Resource Console

Resource consoles can be accessed directly from the iCare Console through the **System Control** tab. According to your hardware resource type and your needs, you can connect to the hardware resource's **Hardware Console**, **Remote System Console** and/or **Telnet Console**.

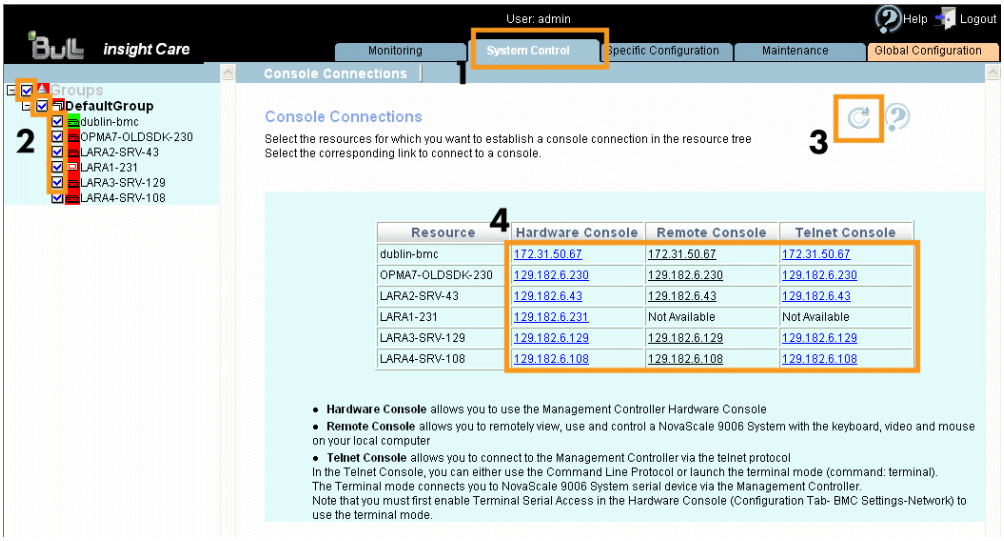
Notes
Hardware Console access is available for all resource types.
Remote System Console and **Telnet Console** access is reserved for certain resource types only. Refer to the documentation delivered with your hardware resource for details.
Resource console access is also available from other iCare Console pages, as explained in Managing System Event Logs (SEL), on page 3-6 and Viewing Resource Details, on page 2-29.

Prerequisite

The hardware resource has been set up for remote access, as explained in the documentation delivered with your hardware resource.

Procedure

1. Click the **System Control** tab to display the **Console Connections** page
2. If required, from the Resource tree, select the resource(s) for which you want to start a console
3. Click **Refresh** to update the page. The resource list appears.



Console Connections	
Hardware Console	Allows you to use the resource's Hardware Console.
Remote Console	Allows you to remotely view, use and control a server with the keyboard, video and mouse on your local computer.
Telnet Console	Allows you to connect to the server's management controller using the telnet protocol.

Figure 26. System Control tab

4. Click the required IP address link to start the console. The console appears in a new window or in a new tab, depending on your browser configuration.

Related Topics

- Managing System Event Logs (SEL), on page 3-6
- Viewing Resource Details, on page 2-29

Chapter 3. Building, Viewing and Managing Resource Logs

This chapter explains how to monitor resources and in particular how to use iCare Console features to analyze hardware events and to perform preventive maintenance. It includes the following topics:

3.1. Building and Viewing System Event Logs (SEL)

Each hardware resource in the Resource tree is equipped with sensors that monitor operational parameters such as power status, presence/absence of components, voltage values, temperature values, fan speed...

The information collected by these sensors is IPMI-compliant and is recorded in the resource's System Event Log (SEL). It is also sent to the iCare Console database.

You can query the database to view events to help you analyze hardware failure or perform preventive maintenance.

Event filters must be enabled from the monitored hardware resource's Hardware Console to ensure transmission to the iCare Console database.
To check that required event filters are enabled, connect to the resource's Hardware Console and open the Configuration tab. Select Alert Settings > Filters and check that Enabled is displayed in the Status column for the required event filter(s).
The last filter in the list of predefined filters covers ALL events.
For further information about resource event filters, refer to the relevant Hardware Console documentation.

Notes

- System Event Logs (SEL) are also collected when an Action Request Package is created to troubleshoot hardware resources. See Creating an Action Request Package, on page 4-19.
- Each resource records IPMI-compliant events in its System Event Log (SEL) and non-IPMI-compliant information in its Board & Security Messages log.
  All events, whether IPMI-compliant or not, are recorded in the iCare Console database providing that the corresponding resource filters are enabled from the resource's Hardware Console.

Prerequisites

The hardware resources requiring attention are present in the Resource tree.

The same **super** user password has been set up on all monitored resources and in the iCare Console, as detailed in Setting Up the BMC Super User Password, on page 5-5.

Procedure

1. From the **Monitoring** tab, click **SEL Viewer** to open the **System Event Log (SEL) Viewer** page.
2. From the **Resource** tree, select the resource(s) for which you want to query the database.

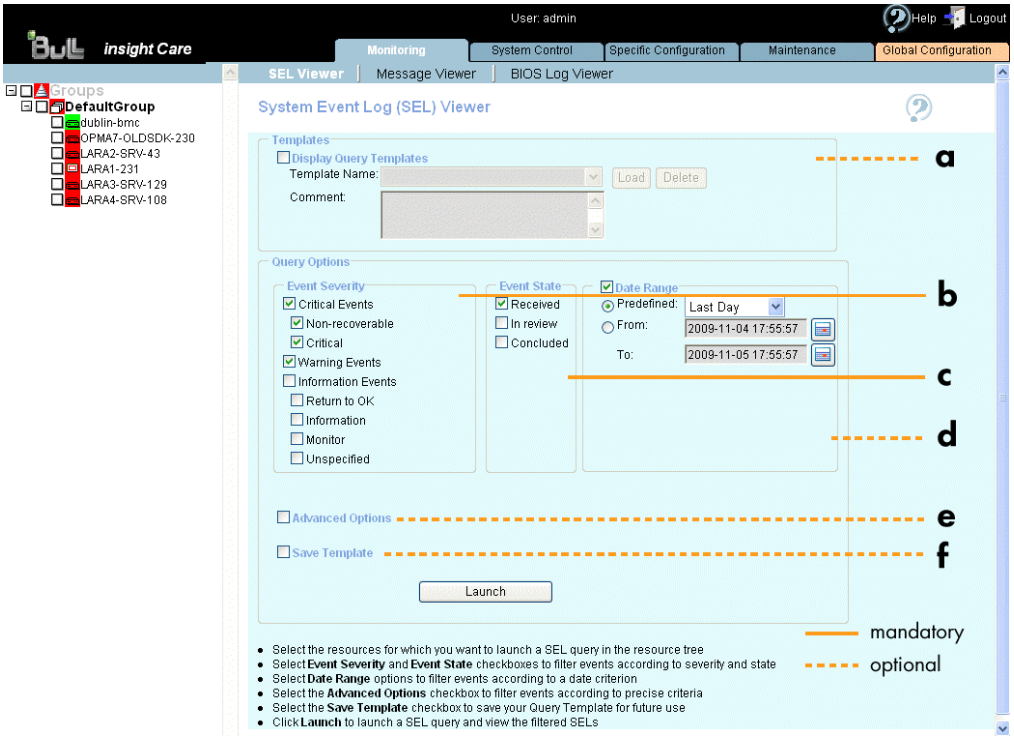


Figure 27. System Event Log (SEL) Viewer page

3. Complete the **System Event Log (SEL) Viewer** template and query fields as explained in the following table:

System Event Log (SEL) Viewer Template and Query Options			
a	Optional	Templates: Load	• Select the **Display Query Templates** check box. • From the **Template Name** drop-down list, select the required template and click **Load**. Template parameters are displayed. • Proceed to Step 4.
a		Templates: Delete	• Select the **Display Query Templates** check box. • From the **Template Name** drop-down list, select the required template and click **Delete**. The template is deleted.
b	Mandatory	Query Options: Event Severity	Select event severity filter(s), as required: • **Critical Events (red):** **Non-Recoverable** **Critical** • **Warning Events (orange)** • **Information Events (green):** **Return to OK** **Information** **Monitor** **Unspecified**
c		Query Options: Event State	Select event state, as required: • **Received** Events awaiting investigation • **In review** Events under investigation • **Concluded** Events that are closed
d	Optional	Date Range	Select the the **Date Range** check box and fill in the appropriate fields to filter events according to a specific date and time range.
e		Advanced Options	Select the **Advanced Options** check box and complete the appropriate fields to filter events according to advanced criteria such as Event Source Type or Sensor Type.
f		Save Template	• Select the **Save Template** check box. • Enter a name in the **Template Name** field (limited to 16 characters. The following characters are not allowed: /\"`&'+*%=><:!?;,~| and space). • If required, enter a description in the **Comment** field. The template will be saved when you launch the query.

Table 14. SEL template and query options

4. Click **Launch**. The **Filtered SELs** page appears.

   You can now consult and manage events as described in Managing System Event Logs (SEL), on page 3-6.

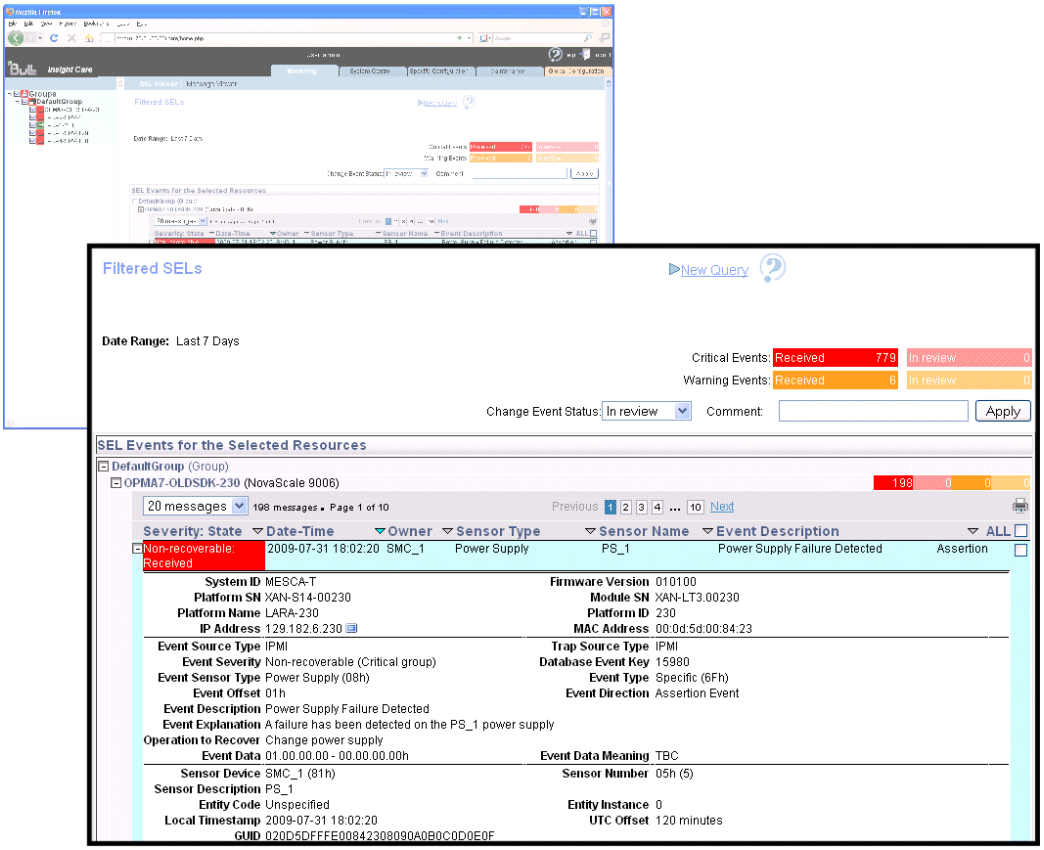


Figure 28. Filtered SELs page

Related Topics

- Managing System Event Logs (SEL), on page 3-6
- Enabling/Disabling the Automatic Clear SEL Policy, on page 3-9
- Building and Viewing Board and Security Message Logs, on page 3-10
- Managing Board and Security Message Logs, on page 3-12
- Building and Viewing BIOS Logs, on page 3-13
- Managing BIOS Logs, on page 3-15
- Creating an Action Request Package, on page 4-19
- Setting Up the BMC Super User Password, on page 5-5
- Manually Importing Multiple Resources, on page 2-5

3.2. Managing System Event Logs (SEL)

The iCare Console provides a SEL event tracking feature for each monitored resource. When an event occurs on a monitored resource, it is recorded in the resource's System Event Log (SEL) and then sent to the iCare Console database.

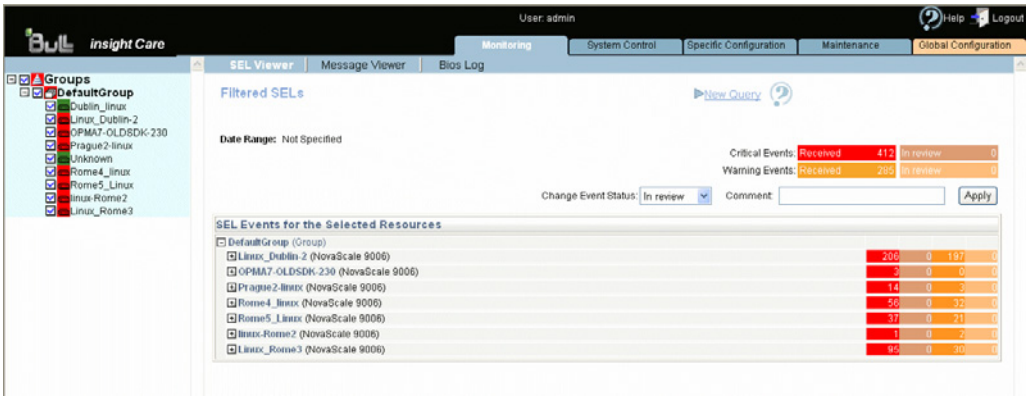
You can query the database to view events to help you analyze hardware failure or perform preventive maintenance.

Prerequisites

None

Procedure

1. Launch a SEL query as explained in Building and Viewing System Event Logs (SEL), on page 3-2. By default, the **Filtered SELs** page lists the SEL events for the selected resources, within the specified date range (where applicable).



Filtered SELs Page	
New Query link	Click this link to launch a new SEL query.
Global Event Status bars	**Red** bar: number of **critical** events **received** **Pink** bar: number of **critical** events **in review** **Orange** bar: number of **warning** events **received** **Peach** bar: number of **warning** events **in review**
Event Status states	**Received**: the event has been received but is not under investigation. The corresponding icons in the Resource tree are red or orange, according to event severity. **In review**: the event is under investigation; The corresponding icons in the Resource tree are still red or orange, according to event severity. **Concluded**: the event has been investigated. The corresponding icons in the Resource tree are now green again.
Change Event Status drop-down list	Use this drop-down list to change event status states.
Comment field	Use this field to add a comment for future reference when you change an event status state.
Resource Event Status bars	Event status states for each selected resource. **Red** bar: number of **critical** events **received** **Pink** bar: number of **critical** events **in review** **Orange** bar: number of **warning** events **received** **Peach** bar: number of **warning** events **in review**

Figure 29. Filtered SELs page

2. Select the required resource and click the corresponding + button to expand and display the SEL event list.

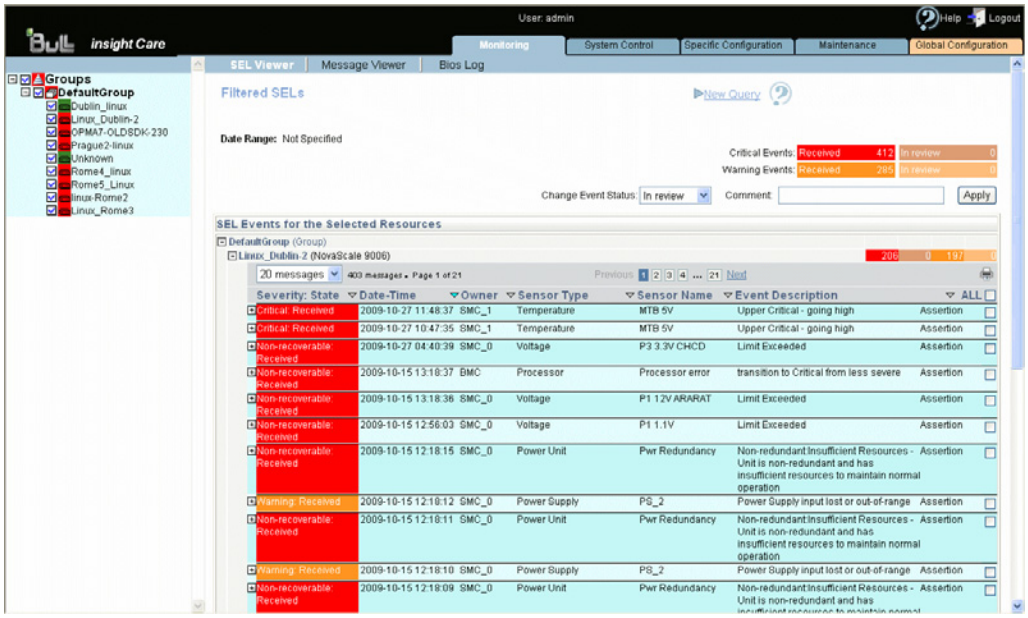


Figure 30. Filtered SELs page - SEL Event List

3. Select the required event and click the corresponding + button to expand and display detailed event information.

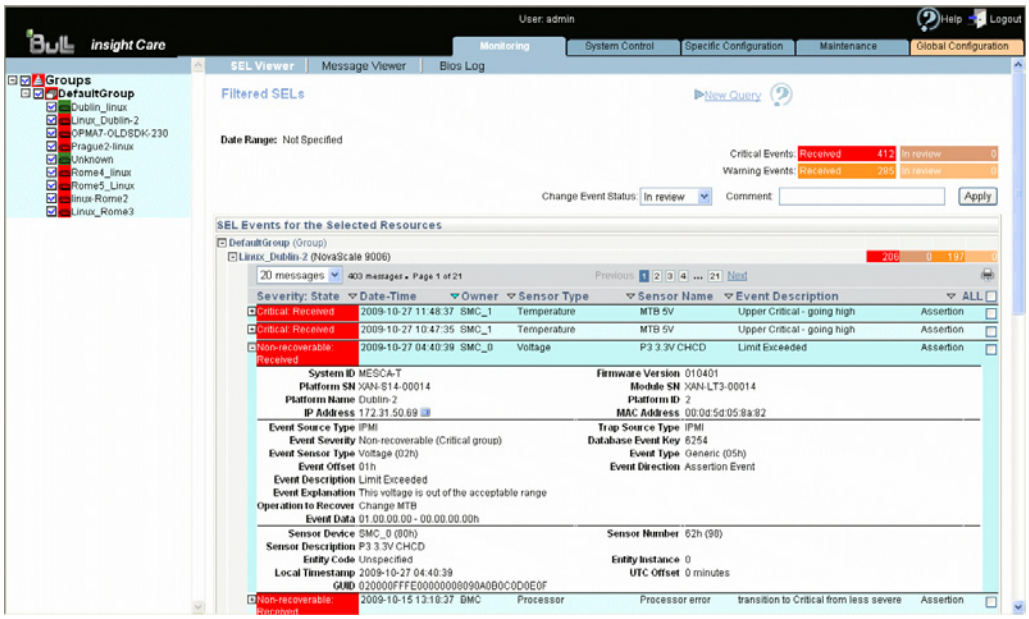


Figure 31. Filtered SELs page - SEL Event details

Note The printer icon allows you to print to PDF the event list (with detailed information) for the selected hardware resource.

4. Select the check box(es) corresponding to the event(s) that you want to manage.

> **Note** Click ALL to select all the events listed in the page.

5. In the **Change Event Status** drop-down list, select the new status you want to apply to the selected event(s):
   - Change from **Received** to **In review** to indicate that the event is under investigation
   - Change from **In review** to **Concluded** to indicate that the event has been investigated and closed
6. Complete the comment field, as required.
7. Click **Apply**.

Related Topics

- Building and Viewing System Event Logs (SEL), on page 3-2
- Monitoring Resources, on page 2-26

3.3. Enabling/Disabling the Automatic Clear SEL Policy

The System Event Log of each monitored hardware resource 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.

Use the automatic clear SEL option to automatically empty SEL logs when the limit is reached so that the latest events can be logged.

Note Even if the SEL limit is reached, events are still recorded in the iCare Console event database.

Prerequisites

The hardware resources are present and monitored in the Resource tree.

The same **super** user password is set up on all monitored resources. For details, see Setting Up the BMC Super User Password, on page 5-5.

Procedure

1. From the **Global Configuration** tab, click **SEL > Clear Policy**. The **Clear SEL Policy** page appears.

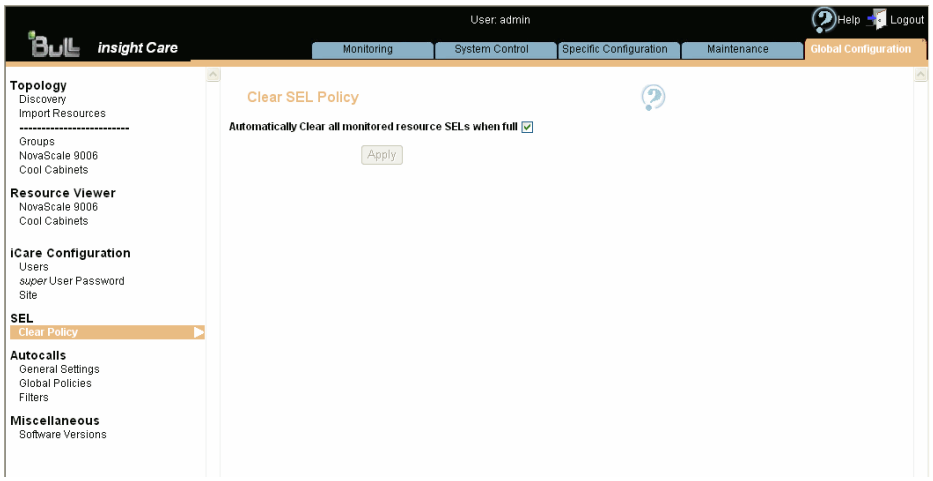


Figure 32. Clear SEL Policy page

2. Proceed as follows:
   a. To enable the automatic clear SEL option, select the **Automatically Clear all monitored resource SELs when full** check box and click **Apply**.
   b. To disable the option, clear the check box and click **Apply**.

Related Topics

- Building and Viewing System Event Logs (SEL), on page 3-2
- Managing System Event Logs (SEL), on page 3-6
- Manually Importing Multiple Resources, on page 2-5
- Setting Up the BMC Super User Password, on page 5-5

3.4. Building and Viewing Board and Security Message Logs

Each hardware resource in the Resource tree records events, such as power-on actions and errors, user authentication, remote console connections, security violations, log deletions or firmware upgrades...

This information is non-IPMI-compliant and is recorded in the resource's Board & Security Messages Log. It is also sent to the iCare Console database.

You can query the database to view events to help you analyze hardware failure or perform preventive maintenance.

Note Board and Security Message logs are also collected when an Action Request Package is created to troubleshoot hardware resources. See Creating an Action Request Package, on page 4-19.

Note Each resource records IPMI-compliant events in its System Event Log (SEL) and non-IPMI-compliant information in its Board & Security Messages log.
All events, whether IPMI-compliant or not, are recorded in the iCare Console database providing that the corresponding resource filters are enabled from the resource's Hardware Console.

Prerequisites

The hardware resources requiring attention are present in the Resource tree.

The messaging feature has been enabled for the hardware resources. For further information, refer to the relevant Hardware Console documentation.

The same **super** user password has been set up on all monitored resources and in the iCare Console, as detailed in Setting Up the BMC Super User Password, on page 5-5.

Procedure

1. From the **Monitoring** tab, click **Message Viewer** to open the **Message Viewer** page.
2. From the **Resource** tree, select the resource(s) for which you want to query the database.

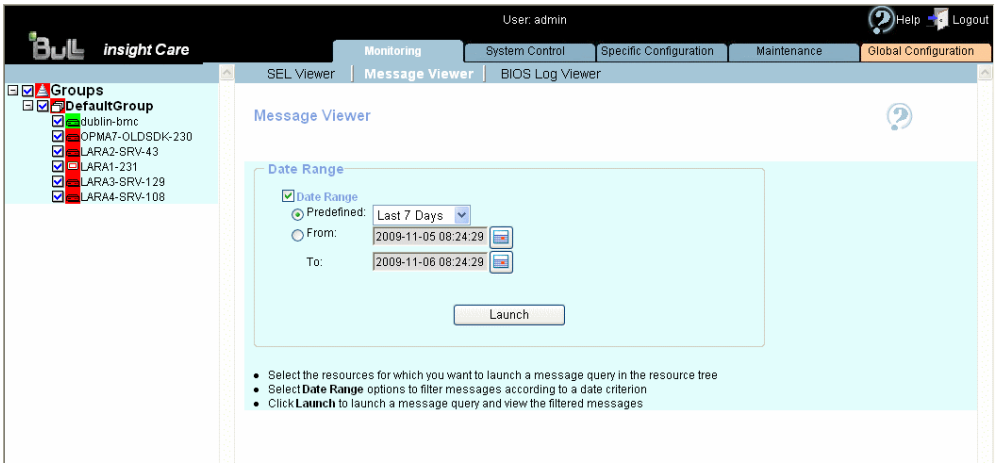


Figure 33. Message Viewer page

3. If required, complete the **Date Range** field to filter messages according to a specific date and time range.
4. Click **Launch**. The **Filtered Messages** page appears.

You can now consult and manage messages as described in Managing Board and Security Message Logs, on page 3-12.

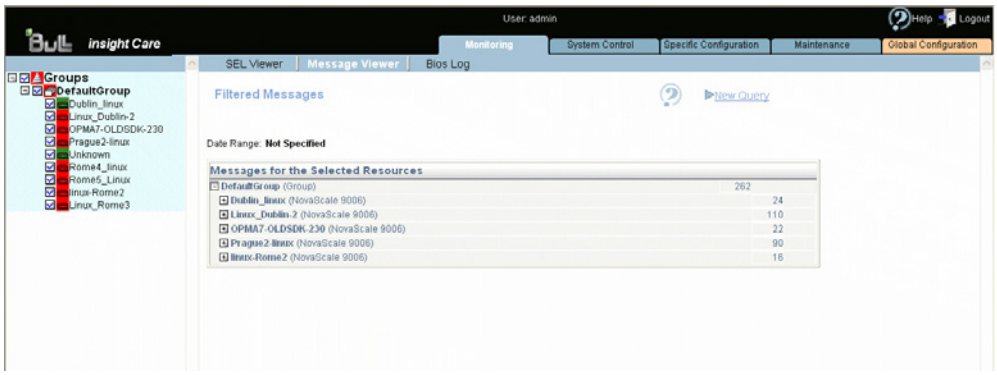


Figure 34. Filtered Messages page - Default display

Related Topics

- Managing Board and Security Message Logs, on page 3-12
- Building and Viewing System Event Logs (SEL), on page 3-2
- Managing System Event Logs (SEL), on page 3-6
- Building and Viewing BIOS Logs, on page 3-13
- Managing BIOS Logs, on page 3-15
- Creating an Action Request Package, on page 4-19
- Setting Up the BMC Super User Password, on page 5-5
- Manually Importing Multiple Resources, on page 2-5

3.5. Managing Board and Security Message Logs

Once you have obtained the list of Board and Security message logs, you can select log files and print them to PDF for offline consultation.

Prerequisites

The hardware resources requiring attention are present in the Resource tree.

The same **super** user password has been set up on all monitored resources and in the iCare Console, as detailed in Setting Up the BMC Super User Password, on page 5-5.

Procedure

1. Launch a Message query as explained in Building and Viewing Board and Security Message Logs, on page 3-10. The **Filtered Messages** page lists all the Messages for the selected resources within the specified date range (where applicable).

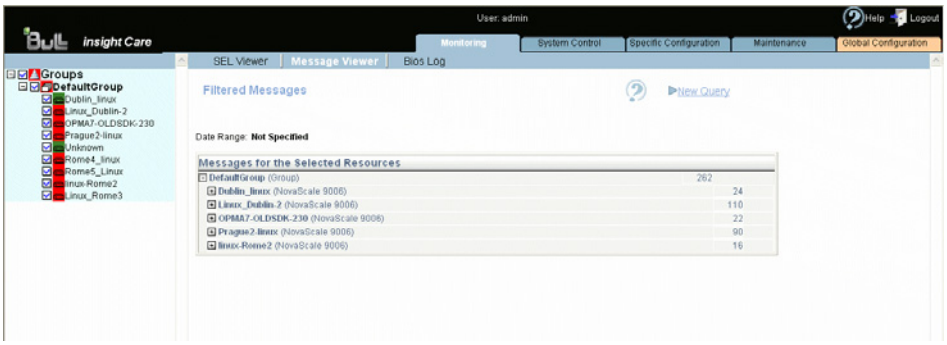


Figure 35. Filtered Message List

2. Select the required resource and click the corresponding + button to expand and display the Messages list.

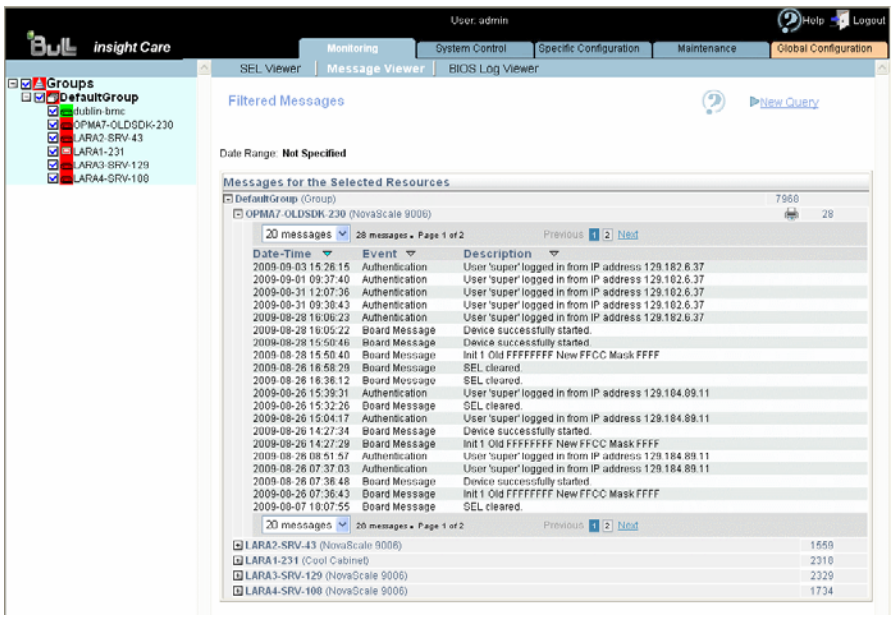


Figure 36. Filtered Messages - Details

3. Click the printer icon to print to PDF the Message list for the selected hardware resource.

Related Topics

- Building and Viewing Board and Security Message Logs, on page 3-10
- Creating an Action Request Package, on page 4-19

3.6. Building and Viewing BIOS Logs

Each NovaScale 9006 Server in the Resource tree records BIOS logs that are also sent to the iCare Console database.

You can query the database to view and download logs to help you analyze hardware failure or perform preventive maintenance online and/or offline.

Note BIOS logs are also collected when an Action Request Package is created to troubleshoot hardware resources. See Creating an Action Request Package, on page 4-19.

Prerequisites

The hardware resources requiring attention are present in the Resource tree

The same **super** user password has been set up on all monitored resources and in the iCare Console, as detailed in Setting Up the BMC Super User Password, on page 5-5

Note If you are using Internet Explorer, check the following security parameters:

- From the **Tools** menu, select **Internet Options > Security > Custom Level > Downloads**
- Check that the **Automatic prompting for file downloads** and **File download** parameters are **Enabled**

Procedure

1. From the **Monitoring** tab, click **BIOS Log Viewer** to open the **BIOS Log** page.
2. From the **Resource** tree, select the resource(s) for which you want to query the database.

Figure 37. BIOS Log Viewer page

3. If required, complete the **Date Range** field to filter BIOS logs according to a specific date and time range.

4. Click **Launch**. The **Filtered BIOS Logs** page appears.

   You can now consult and manage BIOS log files as described in Managing BIOS Logs, on page 3-15.

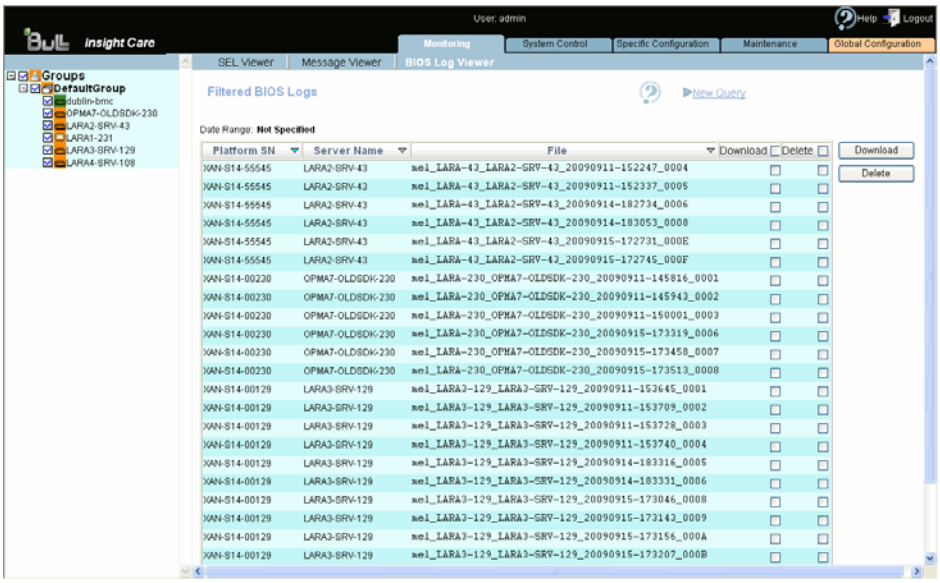


Figure 38. Filtered BIOS Logs page

Related Topics

- Managing BIOS Logs, on page 3-15
- Building and Viewing System Event Logs (SEL), on page 3-2
- Managing System Event Logs (SEL), on page 3-6
- Building and Viewing Board and Security Message Logs, on page 3-10
- Managing Board and Security Message Logs, on page 3-12
- Creating an Action Request Package, on page 4-19
- Setting Up the BMC Super User Password, on page 5-5
- Manually Importing Multiple Resources, on page 2-5

3.7. Managing BIOS Logs

Once you have obtained the list of BIOS logs, you can select log files for downloading and/or deletion.

Prerequisites

The hardware resources requiring attention are present in the Resource tree.

The same **super** user password has been set up on all monitored resources and in the iCare Console, as detailed in Setting Up the BMC Super User Password, on page 5-5.

3.7.1. Downloading BIOS Logs

Procedure

1. Launch a BIOS query as explained in Building and Viewing BIOS Logs, on page 3-13. The **Filtered BIOS Logs** page lists all the BIOS log files for the selected resources within the specified date range (where applicable).

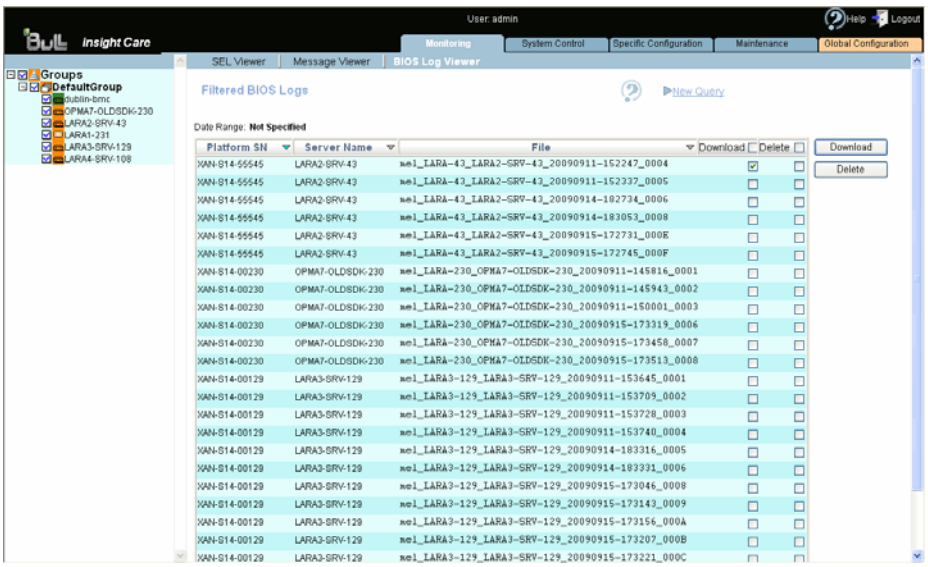


Figure 39. Filtered BIOS Logs - Downloading

2. Select the check box(es) corresponding to the BIOS log files you want to download. Files can be sorted by **Platform SN**, **Server Name** or **File Name**.
3. Click **Download**. A message appears indicating that a ZIP file is being created.
4. Follow the instructions on the screen to save the ZIP file to the media of your choice.

3.7.2. Deleting BIOS Logs

1. Launch a BIOS query as explained in Building and Viewing BIOS Logs, on page 3-13. The **Filtered BIOS Logs** page lists all the BIOS log files for the selected resources within the specified date range (where applicable).

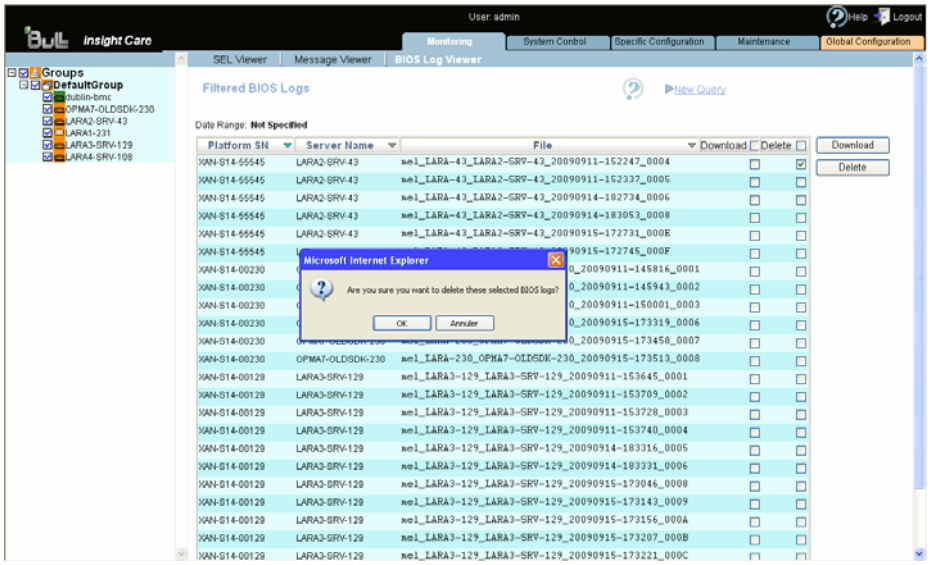


Figure 40. Filtered BIOS Logs - Deleting

2. Select the check box(es) corresponding to the BIOS log files you want to delete. Files can be sorted by **Platform SN**, **Server Name** or **File Name**.
3. Click **Delete**. The selected files are deleted from the iCare Console database.

Related Topics

- Building and Viewing BIOS Logs, on page 3-13
- Creating an Action Request Package, on page 4-19

Chapter 4. Setting Up Autocalls, Action Requests and Intervention Reports

This chapter explains how to set up the autocall feature to transmit alerts to the Bull Support Center and how to create and manage intervention reports and action request packages to facilitate preventive and corrective maintenance operations. It includes the following topics:

Note The Autocall feature is reserved for customers who have subscribed to Bull's Remote Maintenance service offer. For more information, please contact your Bull representative.

4.1. Completing the Site Form

The site form should be completed to ensure that site-relevant information is included in the Autocalls and the Action Request Packages sent to Bull Support services.

Prerequisites

None

Procedure

1. From the **Global Configuration** tab, click **iCare Configuration > Site** to display the **Site Details** page.

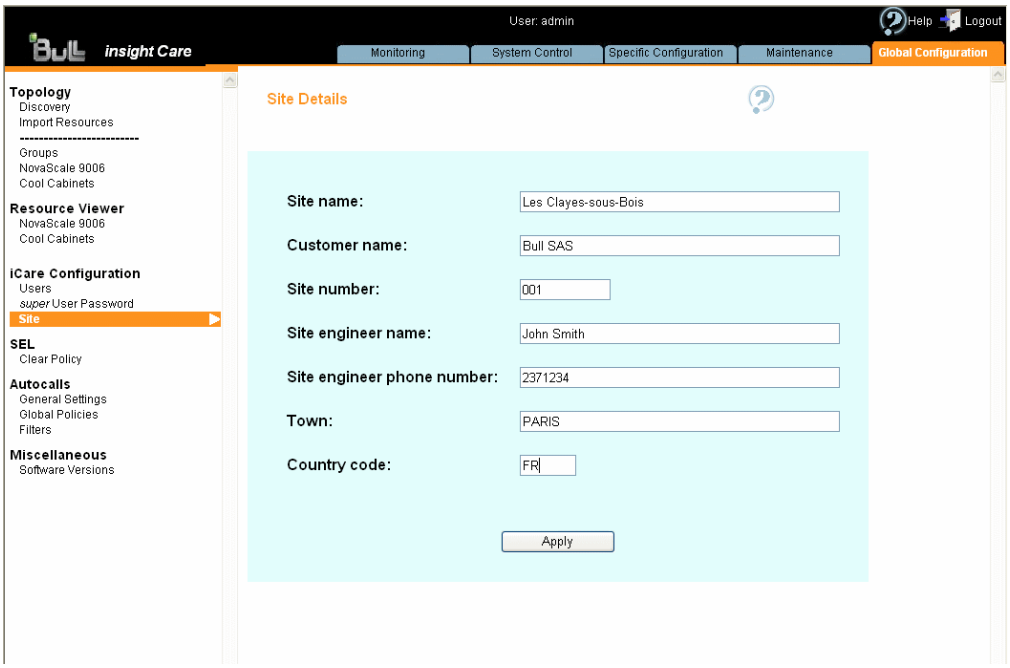


Figure 41. Site Parameters page - Example

2. Complete the form and click **Apply**.

Related Topics

- Configuring Autocalls, on page 4-3
- Viewing the List of Intervention Reports, on page 4-18
- Creating an Action Request Package, on page 4-19

4.2. Configuring Autocalls

An autocall is a message sent by the iCare Console to Bull Support services when a problem occurs on a monitored hardware resource. This section describes how to enable and configure autocalls.

Note The Autocall feature is reserved for customers who have subscribed to Bull's Remote Maintenance service offer. For more information, please contact your Bull representative.

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

- Enable the feature, then select and configure the autocall dispatch mode, as explained in Enabling/Disabling and Testing Autocalls, on page 4-4.
- Select a default autocall policy for each hardware resource type, as explained in Selecting Global Autocall Policies, on page 4-6.

Optionally, you can also:

- Select a specific autocall policy for specific hardware resources, as explained in Selecting Specific Autocall Policies, on page 4-8.
- Create specific autocall filters to track specific events, as explained in Configuring Autocall Filters, on page 4-10.

Important **It is strongly recommended to complete the site form before configuring autocalls. For details, see Completing the Site Form, on page 4-2.**

4.3. Enabling/Disabling and Testing Autocalls

The autocall feature is disabled by default and must be enabled and the dispatch mode configured to start autocall transmission.

Prerequisites

Your maintenance contract includes the autocall feature

You know dispatch mode settings

The target directory is already present on the workstation

Procedure

1. From the **Global Configuration** tab, click **Autocalls > General Settings** to display the **Autocall General Settings** page.

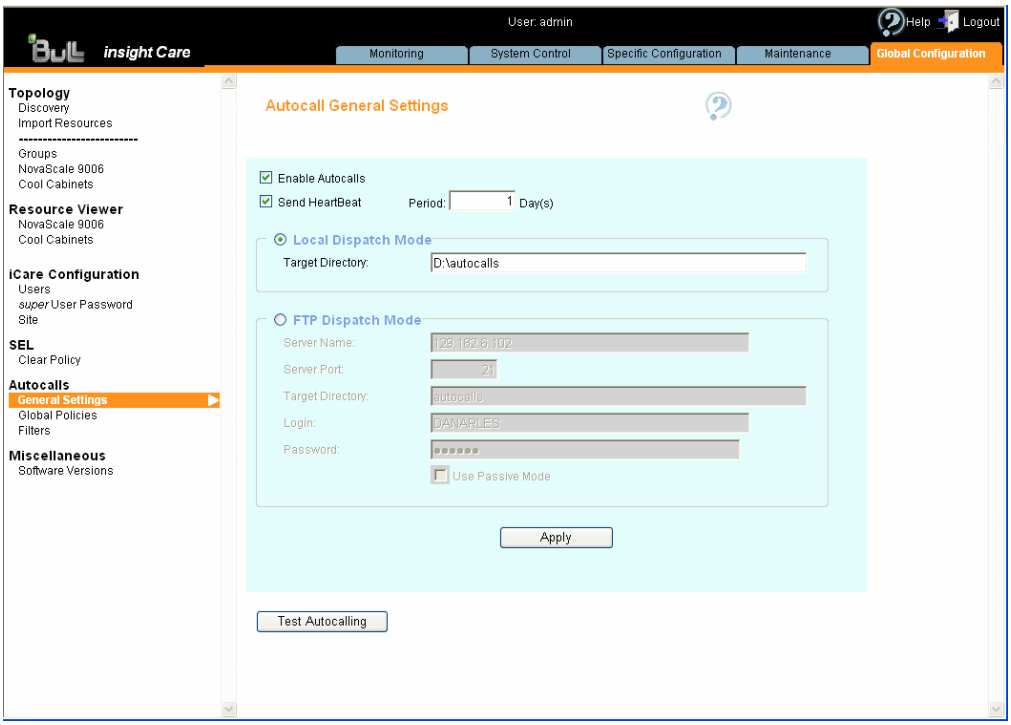


Figure 42. Autocall General Settings page (Autocall Enabled)

Autocall General Settings	
Enable Autocalls	Select this check box to enable the autocall feature.
Send HeartBeat	Select this check box to verify the autocall liaison between the Customer site and the Bull Support Center at the interval indicated in the **Period** field. The default verification interval is **1 Day**. This period can be modified by entering the required interval in the **Period** field.
Local Dispatch Mode	
The local dispatch mode (default mode) records one XML file per autocall in the local directory specified in the **Target Directory** field. To enable the local dispatch mode: • The target directory must already be present on the workstation. • You must enter the full directory pathname (example: C:\Autocalls).	
FTP Dispatch Mode	
The FTP dispatch mode sends one XML file per autocall to the specified remote maintenance server. To enable the FTP dispatch mode, complete the fields as follows:	
Server Name	Remote maintenance server hostname or IP address
Server Port	Server port (21 by default)
Target Directory	Target directory containing the autocall XML file (example: /autocall) Note that the target directory must already be present on the workstation
Login and Password	User account used to log onto the FTP server
Use Passive Mode	Select this option to enable passive FTP (secure data transfer mode)

Table 15. Autocall dispatch mode settings

2. Select the **Enable Autocalls** check box and configure the autocall dispatch mode as explained in Table 15.
3. Select the **Send HeartBeat** check box to enable periodic autocall liaison verification.
4. Click **Apply** to save settings. The **Test Autocalling** button appears.
5. Click **Test Autocalling** and check that the autocall has reached the local or FTP directory according to dispatch mode type.

Note If required, you can define a custom global autocall policy for each hardware resource type, as described in Selecting Global Autocall Policies, on page 4-6. If not, the default global autocall policy will be applied: Autocalls for Critical Events.

Note If you want to temporarily disable autocalls, deselect the **Enable Autocalls** check box.

Related Topics

- Selecting Global Autocall Policies, on page 4-6
- Selecting Specific Autocall Policies, on page 4-8
- Configuring Autocall Filters, on page 4-10

4.4. Selecting Global Autocall Policies

Global autocall policies are available for all hardware resources of the same type and are supplied with the console. The global policies are configured to cover the standard autocall requirements for each type of hardware resource.

According to your needs, you can select global policies based on event severity or on event type. If you select global policies based on event type, you can decide whether to apply default filters or to create and apply custom filters.

Prerequisites

Where applicable, the required custom filter(s) have been created

Procedure

1. From the **Global Configuration** tab, click **Autocalls > Global Policy** to display the **Global Autocall Policies** page.

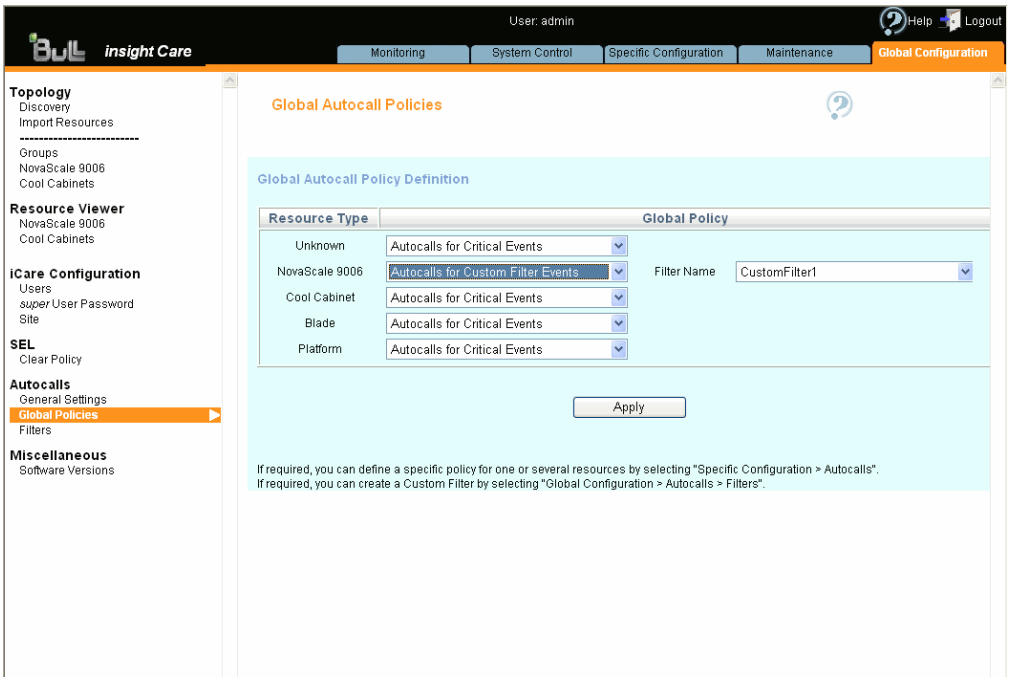


Figure 43. Global Autocall Policy page

2. Select the global autocall policy to use for each resource type, as explained in the following table:

Global Autocall Policy Based on Event Severity	
None	No autocall will be sent.
Autocalls for Critical Events	Value selected by default. An autocall is sent when a CRITICAL event occurs.
Autocalls for Critical or Warning Events	An autocall is sent when a CRITICAL or WARNING event occurs.
Global Autocall Policy Based on Event Type Filters	
Autocalls for Default Filter Events	An autocall is sent when an event message matches the default filter criteria. You can view the default filter criteria, as detailed in Viewing Default or Custom Filter Details, on page 4-10.
Autocall for Custom Filter Events	An autocall is sent when an event message matches the custom filter criteria. Note that the custom filter must be created before selecting this option. For details, see Configuring Autocall Filters, on page 4-10

Table 16. Global autocall policy options

3. Click **Apply**. The selected global autocall policy will be applied to each resource type.

Note You can assign a different autocall policy to one or more specific resources as explained in Selecting Specific Autocall Policies, on page 4-8.

Related Topics

- Viewing Default or Custom Filter Details, on page 4-10
- Creating a Custom Filter, on page 4-12
- Selecting Specific Autocall Policies, on page 4-8
- Enabling/Disabling and Testing Autocalls, on page 4-4

4.5. Selecting Specific Autocall Policies

Global autocall policies are available for all hardware resources of the same type and are supplied with the console. The global policies are configured to cover the standard autocall requirements for each type of hardware resource.

If the global autocall policies for one or more specific hardware resources do not meet your needs, you can apply one or more specific autocall policies to these hardware resources while still maintaining the global policies for all the other hardware resources.

Furthermore, you can apply specific policies based on event severity or on event type. If you select specific policies based on event type, you can decide whether to apply default filters or to create and apply custom filters.

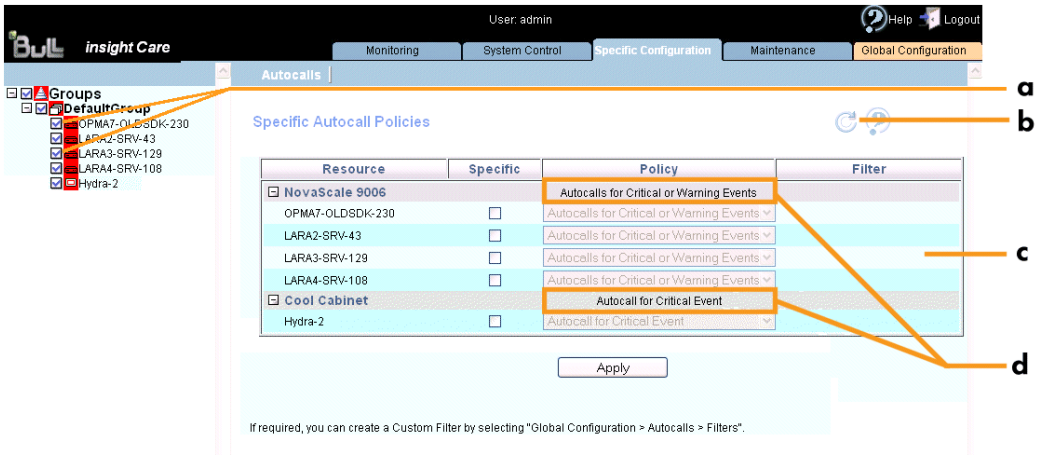
Prerequisites

Where applicable, the required custom filter(s) have been created

The hardware resources to which you want to apply a specific autocall policy are present in the Resource tree

Procedure

1. Click the **Specific Configuration** tab to display the **Specific Autocall Policies** page.
2. From the **Resource** tree, select the resource(s) to which you want to apply a specific autocall policy (a) and click the **Refresh** button (b). The autocall specific configuration table appears (c).



Note The global autocall policies currently in use are displayed for each listed resource type (d).

3. Select the **Specific** check box for the required resource(s) and then select the specific autocall policy to apply to the selected resource(s) from the **Policy** drop-down list, as explained in the following table:

Specific Autocall Policy Based on Event Severity	
None	No autocall will be sent.
Autocalls for Critical Events	Value selected by default. An autocall is sent when a CRITICAL event occurs.
Autocalls for Critical or Warning Events	An autocall is sent when a CRITICAL or WARNING event occurs.
Specific Autocall Policy Based on Event Type Filters	
Autocalls for Default Filter Events	An autocall is sent when an event message matches the default filter criteria. You can view the default filter criteria, as detailed in Viewing Default or Custom Filter Details, on page 4-10.
Autocalls for Custom Filter Events	An autocall is sent when an event message matches the custom filter criteria. Note that the custom filter must be created before selecting this option. For details, see Configuring Autocall Filters, on page 4-10

Figure 44. Specific Autocall Policy page

4. Click **Apply**. The selected specific autocall policy will be applied to each selected resource.

Related Topics

- Creating a Custom Filter, on page 4-12
- Viewing Default or Custom Filter Details, on page 4-10
- Enabling/Disabling and Testing Autocalls, on page 4-4
- Selecting Global Autocall Policies, on page 4-6

4.6. Configuring Autocall Filters

Autocall filters are used when autocall policies are based on event types and not on event severity. When an event type matches the autocall filter criteria, an autocall is transmitted.

Note If you select an autocall policy based on event severity, you do not need to configure autocall filters.

The iCare Console allows you to use two types of autocall filters:

- Default filters: supplied with the console and configured the standard autocall requirements for each type of hardware resource.
- Custom filters: set up by users to finely tune event type filtering.

The following tasks are explained in this section:

- Viewing Default or Custom Filter Details, on page 4-10
- Creating a Custom Filter, on page 4-12
- Editing a Custom Filter, on page 4-13
- Deleting a Custom Filter, on page 4-16

4.6.1. Viewing Default or Custom Filter Details

Prerequisites

None

Procedure

1. From the **Global Configuration** tab, click **Autocalls > Filters**. The **Autocall Filters** page appears.

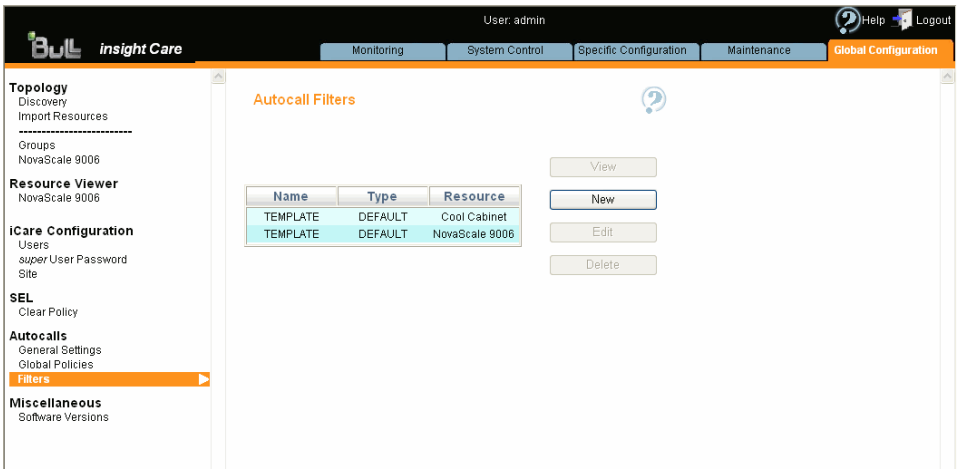
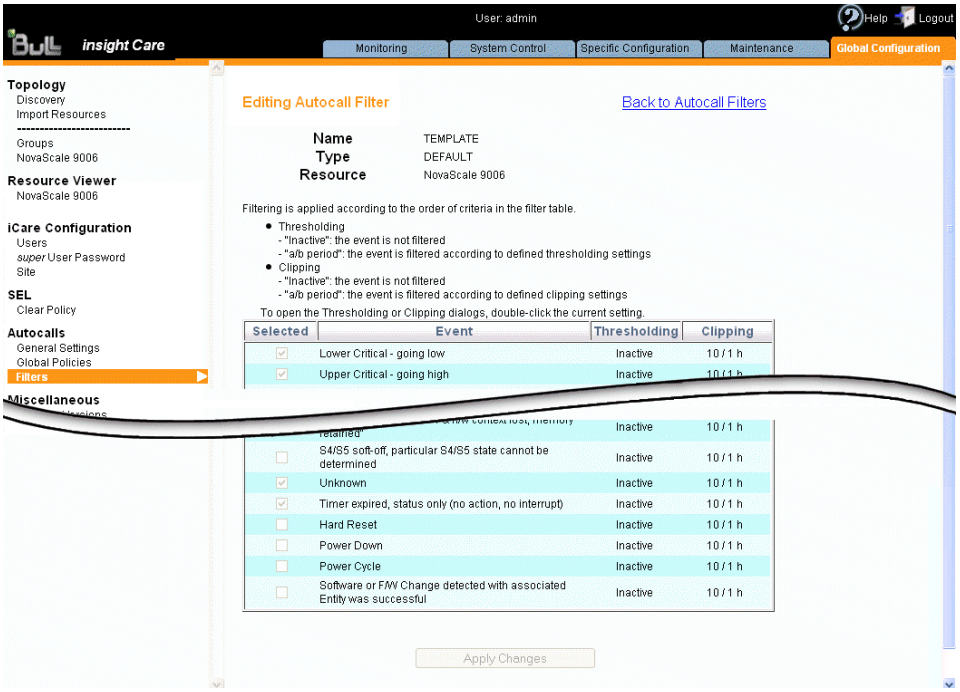


Figure 45. Autocall Filters page

2. From the list of autocall filters, select the required filter and click **View**. The **Viewing Autocall Filter** page appears, displaying filter details.



Note This page is in read-only mode and displays the list of events selected to trigger autocalls. For details on the **Thresholding** and **Clipping** parameters, see Editing a Custom Filter, on page 4-13.

Figure 46. Viewing Autocall Filter page

3. Click **Back to Autocall Filters** to return to the **Autocall Filters** page.

Related Topics

- Creating a Custom Filter, on page 4-12
- Editing a Custom Filter, on page 4-13
- Deleting a Custom Filter, on page 4-16

4.6.2. Creating a Custom Filter

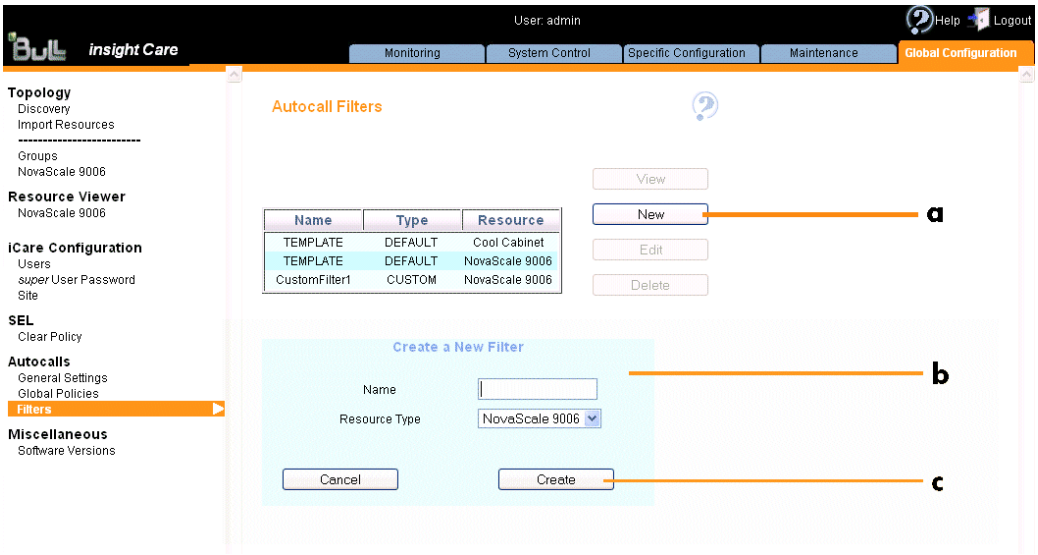
The iCare Console allows you to create your own autocall custom filter to finely tune event type filtering when the default filters supplied with the console do not cover your needs.

Prerequisites

None

Procedure

1. From the **Global Configuration** tab, click **Autocalls > Filters**. The **Autocall Filters** page appears.
2. Click **New** (a) to display the **Create a New Filter** box (b).



Create a New Filter	
Name	Autocall custom filter name, limited to 16 characters.
Resource Type	Hardware resource type associated with the custom filter. Note that the list of events differs according to hardware resource type.

Figure 47. Autocall Filters (Create a New Filter)

3. Complete the box and click **Create** (c). The new custom filter appears in the list of filters.

> **Note** The new custom filter is created with the same criteria as the default filter for the selected hardware resource type.

4. Edit the created custom filter to change criteria, as detailed in Editing a Custom Filter, on page 4-13.

Related Topics

- Editing a Custom Filter, on page 4-13
- Deleting a Custom Filter, on page 4-16

4.6.3. Editing a Custom Filter

Custom filter criteria can be modified at any time. In particular, when you create a new custom filter, you will use the editing option to tune criteria to your needs.

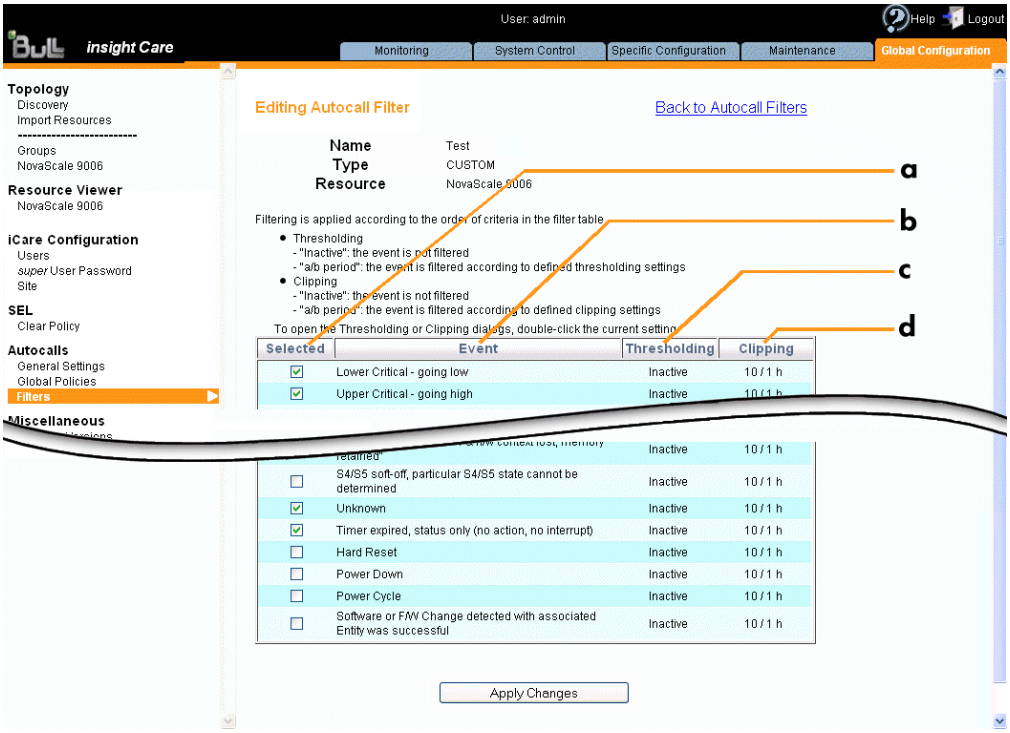
Prerequisites

The custom filter has been created, as explained in Creating a Custom Filter, on page 4-12.

Procedure

Note Criteria differ according to hardware resource type.
The hardware resource type illustrated in this procedure is a NovaScale 9006 Server.

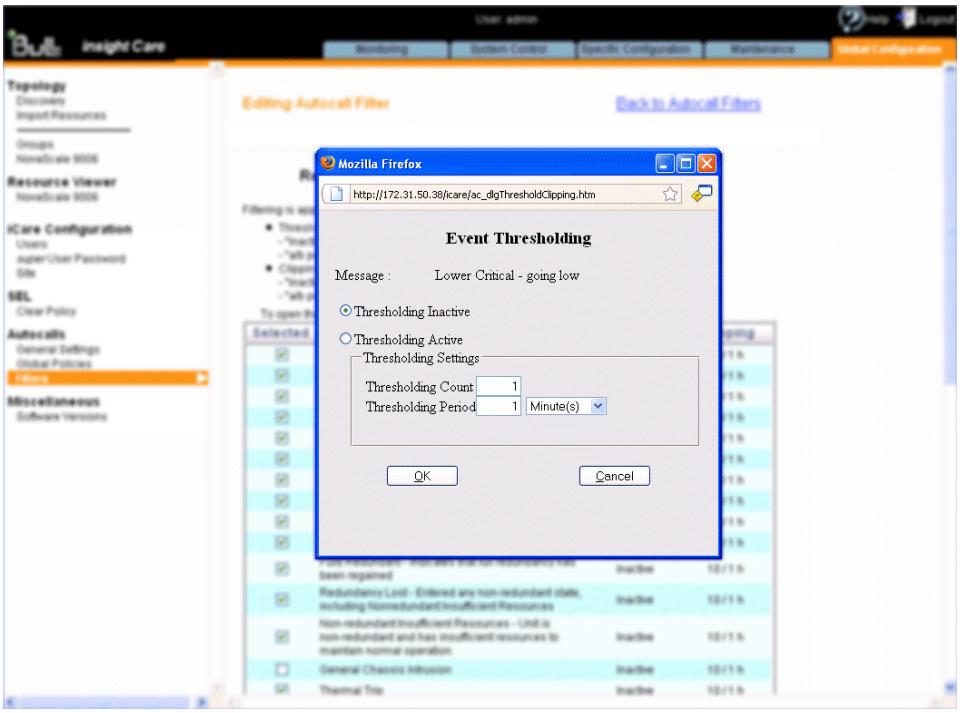
1. From the **Global Configuration** tab, click **Autocalls > Filters**. The **Autocall Filters** page appears.
2. From the list of autocall filters, select the required filter and click **Edit**. The **Editing Autocall Filter** page appears.



Editing Autocall Filter	
Selected column (a)	By default, the selected check boxes are the same as for the default autocall filter for the hardware resource type. When a check box is selected, the corresponding event message is included in the custom filter.
Event column (b)	Message associated with the event.
Thresholding column (c)	By default, the thresholding and clipping values are the same as for the default autocall filter. Thresholding and Clipping are advanced filtering criteria that are to be used with care. They are detailed below.
Clipping column (d)	

Figure 48. Editing Autocall Filter page

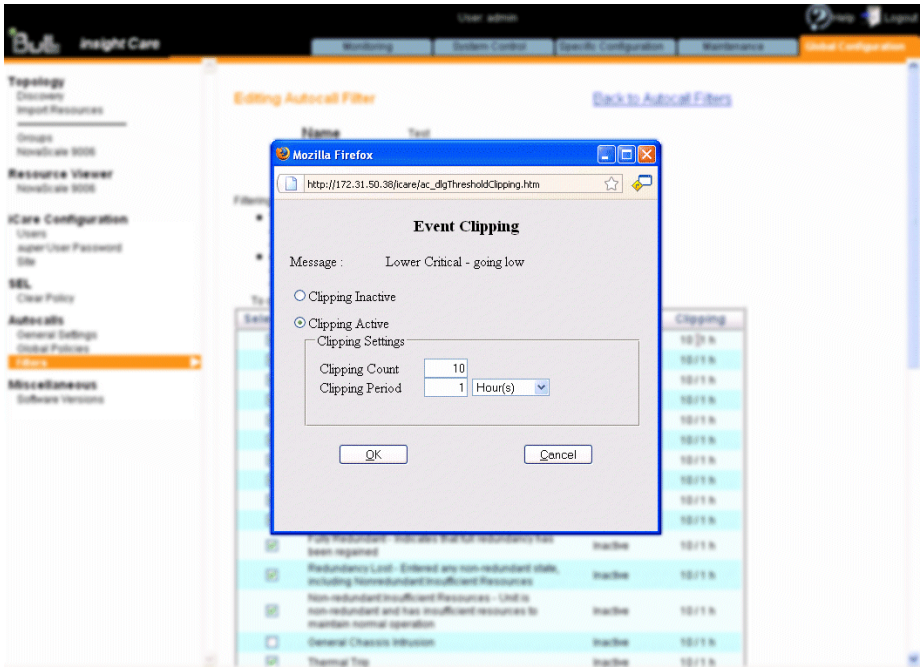
3. For each listed event:
   - Select the check box (a) to include or clear the check box (a) to exclude the corresponding event (b).
   - Double-click the **Thresholding** value (c). The **Event Thresholding** box appears.
   - Complete the box as described below and click **OK**.



Event Thresholding Box	
Thresholding is defined on a Count / Period basis aimed at transmitting significant event messages only. Identical event messages are counted and if the number of event messages indicated in the **Thresholding Count** field is reached within the period of time indicated in the **Thresholding Period** field, this event message is selected for transmission.	
Thresholding Inactive	Deactivates thresholding: if the event is selected, all messages are transmitted as autocalls.
Thresholding Active	Activates thresholding using the values displayed in the **Thresholding Count** and **Thresholding Period** fields.
Thresholding Count	Number of identical event messages to be reached.
Thresholding Period	Period of time, in seconds, minutes, hours or days.

Figure 49. Event Thresholding box description

- Double-click the **Clipping** value (d). The **Event Clipping** box appears.
- Complete the box as described below and click OK.



Event Clipping Box	
Clipping is defined on a Count / Period basis aimed at transmitting a pre-defined number of event messages only. Identical event messages are counted and when the number of event messages indicated in the **Clipping Count** field is reached within the period of time indicated in the **Clipping Period** field, no other event messages will be selected for transmssion.	
Clipping Inactive	Deactivates clipping: if the event is selected, all the event messages are transmitted as autocalls.
Clipping Active	Activates clipping using the values displayed in the **Clipping Count** and **Clipping Period** fields.
Clipping Count	Maximum number of autocalls to send in the clipping period.
Clipping Period	Period of time, in seconds, minutes, hours or days.

Important **The Thresholding and Clipping processes are sequential. Event messages are first processed by the Thresholding mechanism and only the retained messages are processed by the Clipping mechanism.**

Figure 50. Event Clipping box description

4. Click **Apply Changes** to save your custom autocall filter.

Note If this custom filter is already in use, new values are immediately taken into account when you click **Apply Changes**.

Related Topics

- Creating a Custom Filter, on page 4-12
- Deleting a Custom Filter, on page 4-16
- Selecting Global Autocall Policies, on page 4-6
- Selecting Specific Autocall Policies, on page 4-8

4.6.4. Deleting a Custom Filter

You can delete a custom filter at any time if it is no longer needed and no longer in use.

Note You cannot delete default autocall filters.

Prerequisites

The custom filter you want to delete is no longer used in a default or specific **Use Custom Filter** autocall policy.

Procedure

1. From the **Global Configuration** tab, click **Autocalls > Filters**. The **Autocall Filters** page appears.
2. From the list of autocall filters, select the required filter (a) and click **Delete** (b). Then, in the displayed confirmation box, click **OK** (c).

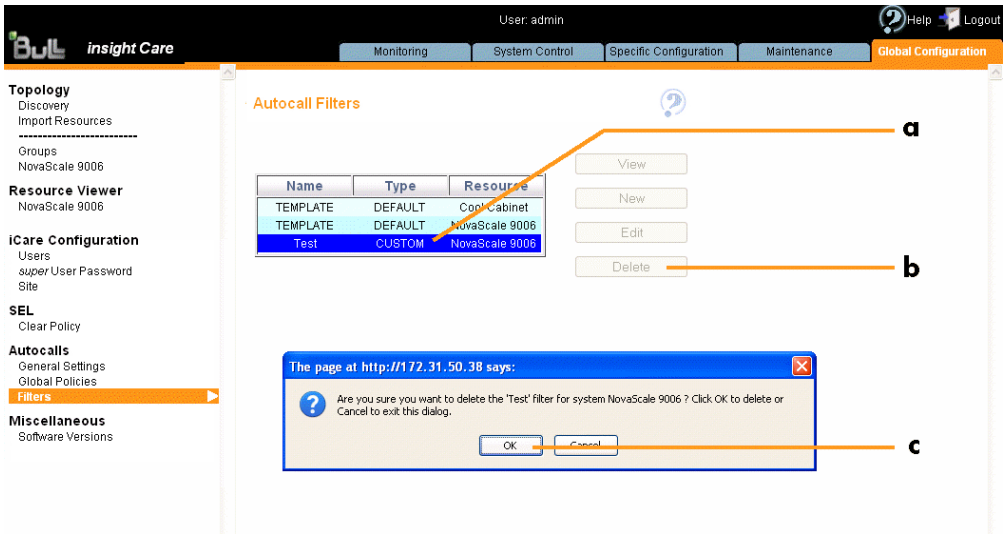


Figure 51. Autocall Filters page (Delete a filter)

Related Topics

- Creating a Custom Filter, on page 4-12
- Selecting Global Autocall Policies, on page 4-6
- Selecting Specific Autocall Policies, on page 4-8

4.7. Creating an Intervention Report

You are advised to create an intervention report when you perform preventive or corrective maintenance or problem analysis operations on hardware resources monitored by the iCare Console. These reports allow you to keep track of the operations performed on monitored hardware resources stored in the iCare Console database for easy access when needed.

Prerequisites

The hardware resource for which you want to create an intervention report is in the Resource tree.

Procedure

1. From the **Maintenance** tab, select **Intervention Report Creation**.
2. From the Resource tree, select the hardware resource(s) concerned by the intervention (a) and click **Refresh** (b). The intervention report form appears (c).

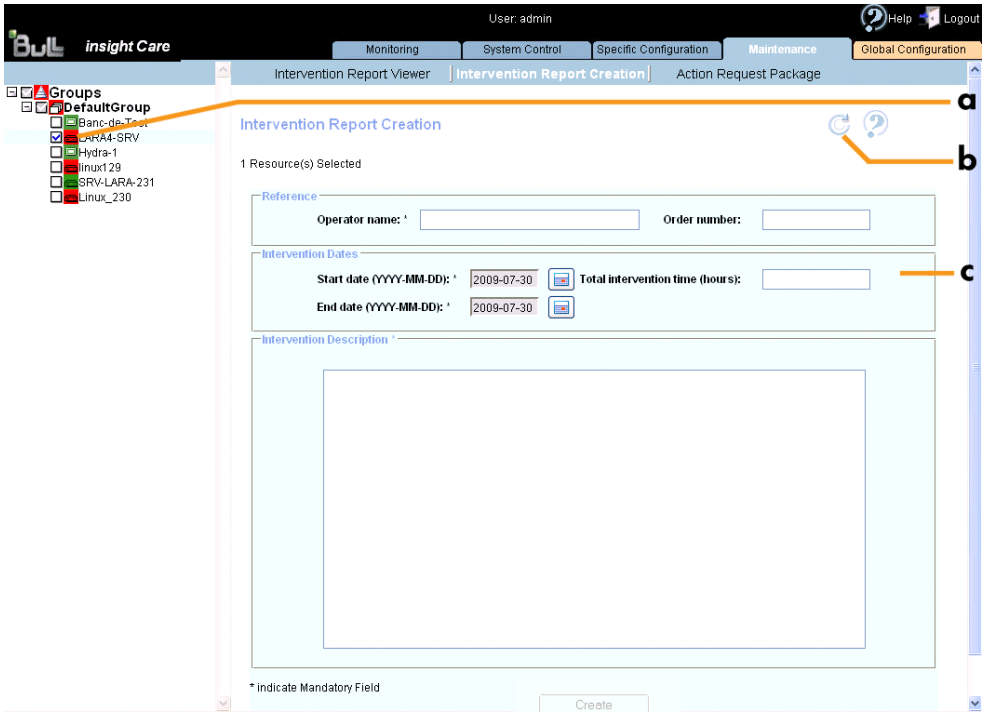


Figure 52. Intervention Report Creation page

3. Complete the form, taking care to provide as much information as possible in the **Intervention Description** box. Click **Create** to generate the report.

> **Note** If you have selected several hardware resources, a separate report is created for each resource, but the information entered in the **Intervention Description** box is the same.

You can now view the report(s) using the **Intervention Report Viewer**.

Related Topics

- Viewing the List of Intervention Reports, on page 4-18
- Creating an Action Request Package, on page 4-19

4.8. Viewing the List of Intervention Reports

You can display intervention reports on monitored resources at any time to help you perform preventive or corrective maintenance or problem analysis operations.

Prerequisites

The hardware resources for which you want to view intervention reports are in the Resource tree.

Procedure

1. From the **Maintenance** tab, select **Intervention Report Viewer**.
2. From the Resource tree, select the hardware resource(s) for which you want to view intervention reports (a) and click **Refresh** (b). The intervention report list appears (c).

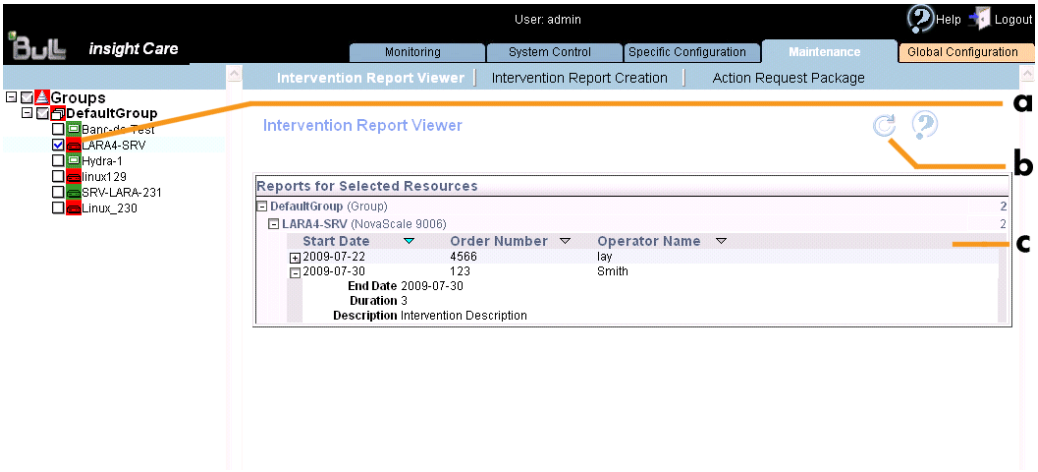


Figure 53. Intervention Report Viewer page

3. Use the **Expand/Collapse** button to display or hide intervention report details.

Note If no reports have been generated for a given hardware resource, the message No **reports available** is displayed.

Related Topics

- Creating an Intervention Report, on page 4-17
- Creating an Action Request Package, on page 4-19

4.9. Creating an Action Request Package

You can collect all the files required to troubleshoot monitored hardware resources using the Action Request Package feature. Once collected, files are compressed to a ZIP archive file for easy transfer to the Bull Support Center.

Note The Action Request Package ZIP file contains System Event Logs (SEL), Board and Security Messages, BIOS logs along with the Identity Card for the selected resources. Logs and messages can also be consulted online from the iCare Console Monitoring tab. For details, see Chapter 3. Building, Viewing and Managing Resource Logs.

Prerequisites

You have completed the Site form, as detailed in Completing the Site Form, on page 4-2.

Your browser is configured to accept cookies and downloads.

The hardware resources for which you want to create an action request package are in the Resource tree.

You have the Action Request Package reference number sent by the Bull Support Center.

Procedure

1. From the **Maintenance** tab, select **Action Request Package**.
2. From the Resource tree, select the hardware resource(s) for which you want to create an action request package (a) and click **Refresh** (b). The **Action Request Package Creation** form appears (c).

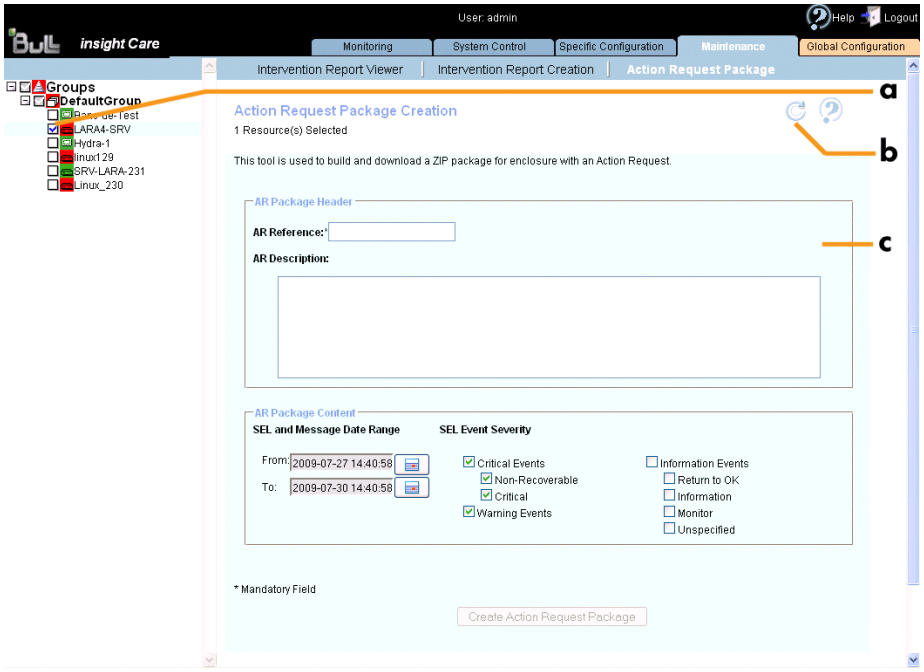


Figure 54. Action Request Package Creation page

3. Complete the form, taking care to provide as much information as possible in the **AR Description** field and correct values in the **AR Package Content** box (Date Range and SEL Event Severity).
4. Click **Create Action Request Package** to create a ZIP archive file containing four files for each hardware resource: **System Event Logs (SEL)**, **Board and Security Messages**, **BIOS logs** and **Identity Card**.
5. When requested, save the ZIP file and send it to the Bull Support Center for analysis.

Related Topics

- Creating an Intervention Report, on page 4-17
- Viewing the List of Intervention Reports, on page 4-18

Chapter 5. Managing Users

This chapter explains how to manage user access to the iCare Console. It includes the following topics:

5.1. Managing User Accounts

Access to the iCare Console is based on user accounts to ensure that only authorized users have access to the console. The console is delivered with the predefined user account **admin**, but you can define as many other user accounts as required.

5.1.1. Creating a User Account

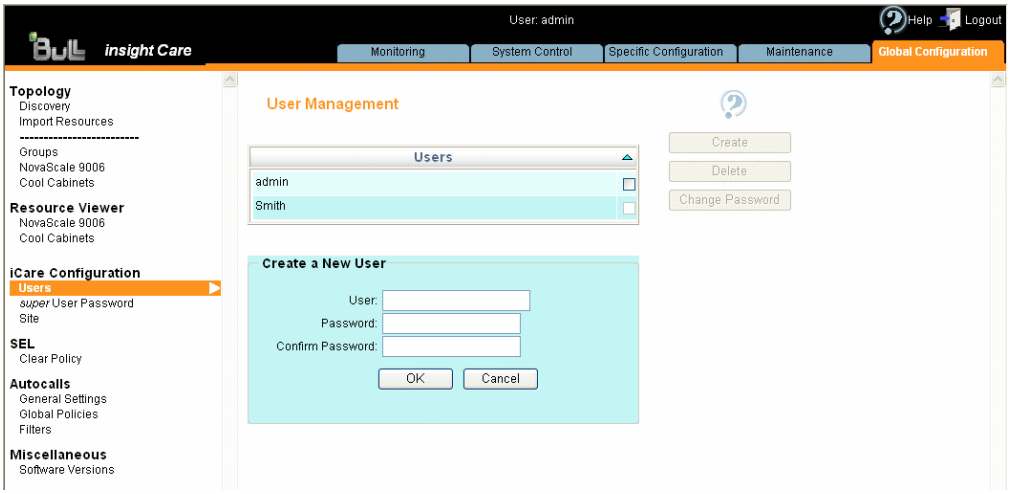
You can create a personal user account for each person that needs to log onto and use the iCare Console.

Prerequisites

None

Procedure

1. From the **Global Configuration** tab, click **iCare Configuration > Users**. The **User Management** page appears.
2. Click **Create** to display the **Create a New User** box.



Create a New User	
User	Name the user will use to log on. • Name limited to 16 characters - CASE SENSITIVE. • The following characters are not allowed: /\"`&'+*%=><:!?;,~| and space.
Password	Password the user will use to log on. • Maximum password length: 16 characters • No character restriction - CASE SENSITIVE.
Confirm Password	

Figure 55. User Management page (Create a New User box)

3. Complete the fields and click **OK**. The user account is created and appears in the **User Management** page.

Related Topics

- Deleting a User Account, on page 5-3
- Changing a User Account Password, on page 5-4
- Setting Up the BMC Super User Password, on page 5-5

5.1.2. Deleting a User Account

You can delete a user account when no longer needed or when a user has lost his password and a new user account needs to be created.

Note You cannot delete the predefined user account **admin**. However, the default **admin** user password can be changed, as detailed in Changing a User Account Password, on page 5-4.

Prerequisites

None

Procedure

1. From the **Gobal Configuration** tab, click **iCare Configuration > Users**. The **User Management** page appears.
2. Select the user account you want to delete (a), click **Delete** (b) and click **OK** in the displayed confirmation box (c). The user account is deleted and disappears from the **User Management** page.

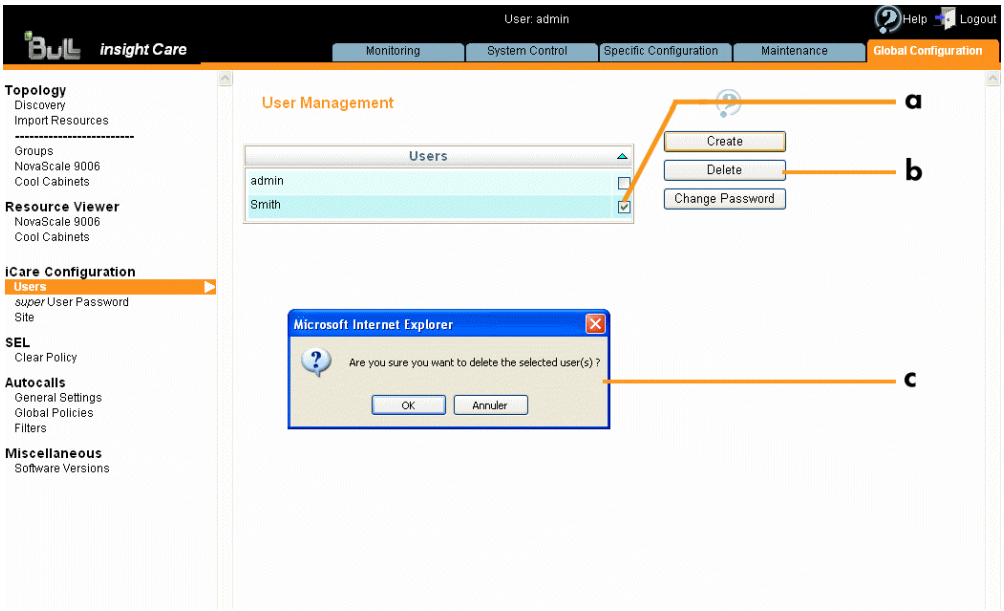


Figure 56. User Management page (Delete User Account)

Related Topics

- Creating a User Account, on page 5-2
- Changing a User Account Password, on page 5-4

5.1.3. Changing a User Account Password

You can change a user account password, as needed, to suit your site security requirements.

Note You are strongly advised to change the factory-default admin user password before using the console for the first time.

Prerequisites

You know the current password. If the current password has been lost, you must delete and re-create the user account in order to configure a new password.

Procedure

1. From the **Global Configuration** tab, click **iCare Configuration > Users**. The **User Management** page appears.
2. Select the user account you want to modify (a) and click **Change Password** (b). The **Change User Password** box appears (c).

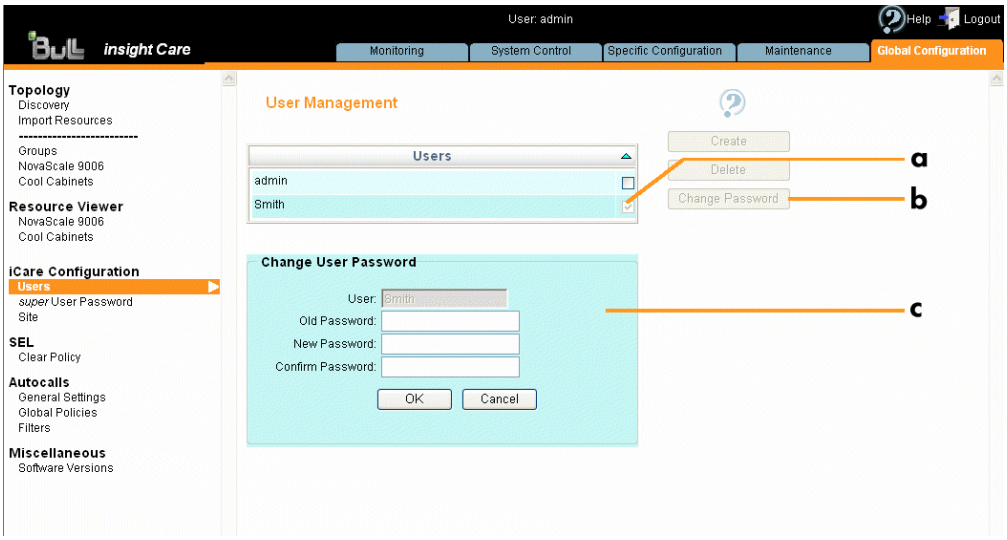


Figure 57. User Management page (Change User Password box)

3. Complete the fields in compliance with the following rules:
   - Maximum password length: 16 characters.
   - No character restriction - CASE SENSITIVE.
4. Click **OK**. The new password is now valid and must be used at the next logon.

Related Topics

- Creating a User Account, on page 5-2
- Deleting a User Account, on page 5-3

5.2. Setting Up the BMC Super User Password

The iCare Console communicates with the hardware resources it monitors via the Baseboard Management Controllers (BMC) embedded on each of these hardware resources. The iCare Console connects to the hardware resource BMCs using the super user account.
An **identical super user account** must be set up, using the resource's hardware console, for each resource monitored via the iCare Console. Once you have set up this account on all the hardware resources you want to monitor, you must then declare the same super user password in the iCare Console.

Note On delivery, the BMC embedded in the hardware resource is configured with a factory-default super user account configured as follows:

- login: **super**
- password: **pass**

Although this account cannot be renamed or deleted, the default password must be changed for security reasons.

Important

- **If the default super user account password (pass) has not been changed, you do not need to declare the password in the iCare Console.**
- **Declaring the super user password in the iCare Console DOES NOT change the hardware resource super user password.**
- **If different super user account passwords have been given to different hardware resources you want to monitor via the iCare Console, you must choose a single password and update super user account details on all the hardware resources concerned. See the documentation delivered with the hardware resource for details.**

Prerequisites

Each hardware resource you want to add to the Resource tree and monitor has the same **super** user password.

Procedure

1. From the Global Configuration tab, click iCare Configuration > *super* User Password to display the Hardware Console *super* User Password page.

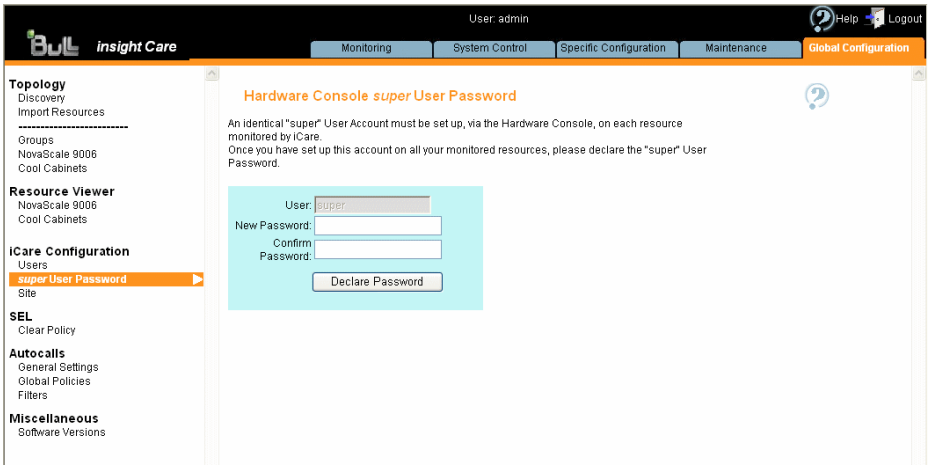


Figure 58. *super* User Password page

2. Complete the fields and click **Declare Password**.

Related Topics

- Connecting to a Resource Console, on page 2-30
- Manually Importing Multiple Resources, on page 2-5

Glossary

A

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.

B

Backup
A copy of data for safe-keeping. The data is copied form computer memory or disk to a floppy disk, magnetic tape or other media.

Base Operating System
The Operating System that is booted at initialization.

BCS
Bull Coherent 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.

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.

Bit
Derived from BInary digiT. A bit is the smallest unit of information a computer handles.

BMC
Baseboard Management Controller. See Embedded Management Controller.

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).

Byte
A group of eight binary digits (bit) long that represents a letter, number, or typographic symbol.

C

Cache Memory
A very fast, limited portion of RAM set aside for temporary storage of data for direct access by the microprocessor.

CD-ROM
Compact DisK Read-Only Memory. High-capacity read-only memory in the form of an optically readable compact disk.

CIM
Common Information Model Standard DMTF. Provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions.

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.

CMC
A Corrected Memory Check condition is signaled when hardware corrects a machine check error or when a mahcine check abort condition is corrected by firmware. See MCA.

CMCI
Corrected Memory Check Interrupt.

CMCV
Corrected Memory Check Vector.

CMOS
Complementary Metal Oxide Semiconductor. A type of low-power integrated circuits. System startup parameters are stored in CMOS memory. They can be changed via the system setup utility.

Cold Reset
A reset operation immediately following power-up. Also called Power-up reset.

Core
Core is the short name for the processor execution core implemented on a processor. A core contains one or more threads (logical processors).

CPLD
Complex Programmable Logic Device. A programmable logic device with a non volatile memory.

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

Default Setting
The factory setting your server uses unless instructed otherwise.

Device Driver
A software program used by a computer to recognize and operate hardware.

DIMM
Dual In-line Memory Module. The smallest system memory component.

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. A server that retains the addresses and routing information for TCP/IP LAN users.

DPS
Distributed Power Supply.

DRAM
Dynamic Random Access Memory is the most common type of random access memory (RAM).

DSIB
Dummy BCS Interconnect Board.

DVO
Digital Video Out.

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.

EMI
Electro-Magnetic Interference.

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.

ERP
Error Recovery Procedure.

Error
Manifestation of a fault. All faults do not result in an error. See Fault.

Error Detection
The process that determines the deviation between observed behavior and specified behavior.

ESD
ElectroStatic Discharge. An undesirable discharge of static electricity that can damage equipment and degrade electrical circuitry.

Event
The generation of a message (event message) by a software component and that is directed to the Event Manager.

Exclude
See Include / Exclude.

F

Fail-Over
Backup operational mode in which the functions of a system component (such as a processor, server, network, or database, for example) are assumed by secondary system components when the primary component becomes unavailable through either failure or scheduled down time.

Fatal Error
A fatal error may compromise system integrity and it may not be possible to continue operation. See Error.

Fault
An erroneous state resulting from observed behavior deviating from specified behavior. Some faults may result in an error. See Error.

Flash EPROM
Flash Erasable Programmable Read-Only Memory. A type of memory device that is used to store the 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.

Firewall
A set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks.

Firmware
An ordered set of instructions and data stored to be functionally independent of main storage.

FPGA
Field Programmable Gate Array. Device containing programmable logic components and programmable interconnects.

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.

FTP
File Transfer Protocol. A standard Internet protocol: the simplest way of exchanging files between computers on the Internet. FTP is an application protocol that uses Internet TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It is also commonly used to download programs and other files from other servers.

G

GUI
Graphical User Interface.

H

HA
High Availability. Refers to a system or component that is continuously operational for a desirably long length of time.

Hard Reset
A reset event in the system that initializes all components and invalidates caches.

Hardware
The physical parts of a system, including the keyboard, monitor, disk drives, cables and circuit cards.

Hardware Corrected Error
Correctable errors are corrected by hardware while software is completely oblivious to their occurence. See Error.

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.

Hardware Uncorrected Error
Uncorrectable errors are not corrected by hardware, but are contained. System state remains intact and the process and system are restartable. A system shutdown may be required. See Error.

HPC
High Performance Computing.

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.

HT
HyperThreading. See Multi-Threading.

HTTP
HyperText Transfer Protocol. In the World Wide Web, a protocol that facilitates the transfer of hypertext-based files between local and remote systems.

I

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.

IC
Integrated Circuit. An electronic device that contains miniaturized circuitry. See Chip.

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.

Interface
A connection between a computer and a peripheral device enabling the exchange of data. See Parallel Port and Serial Port.

Include / Exclude
A physically present ARU can be logically connected to / disconnected from the hardware partition at boot time, under control of the Platform Management software. This is a static logical operation.
An excluded ARU can be reserved as a spare, locked for future user (Pay-As-You-Grow), or marked as failed.

Initialization
The set of firmware or micro-code sequences that follow warm or cold reset.

I/O
Input /Output. Describes any operation, program, or device that transfers data to or from a computer.

IOH
Input/Output Hub. An Intel QPI agent that handles I/O requests for processors.

IP
Internet Protocol. The protocol by which data is sent from one computer to another via the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

IPL
Initial Program Load. It defines the firmware functional phases during the system initialization.

IPM
Intelligent Platform Management.

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

Jumper
A small electrical connector used for configuration on computer hardware.

K

KCS
Keyboard Controller Style. One of the standardized IPMI System interface, that system software can use for transferring IPMI messages to the BMC. Data are transferred using a per-byte handshake.

KVM
Keyboard Video Mouse. Hardware device that allows a user to control multiple computers from a single keyboard, video monitor and mouse.

L

LAN
Local Area Network. A group of computers linked together within a limited area to exchange data.

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. Application protocol for querying and modifying directory services running over TCP/IP.

LED
Light Emitting Diode. A small electronic device that glows when current flows through it.

Legacy Application
An application in which a company or organization has already invested considerable time and money. Typically, legacy applications are database management systems (DBMSs) running on mainframes or minicomputers.

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.

LUN
Logical Unit Number. Term used to designate Logical Storage Units (logical disks) defined through the configuration of physical disks stored in a mass storage cabinet.

M

MAC
Media Access Control. A data communication protocol sub-layer that provides addressing and channel access control mechanisms allowing several terminals or network nodes to communicate within a multipoint network, typically a local area network (LAN).

MC
Management Controller.

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.

Memory
Computer circuitry that stores data and programs. See RAM and ROM.

Microprocessor
An integrated circuit that processes data and controls basic computer functions.

MII
Media Independent Interface. A standard interface used to connect a Fast Ethernet (i.e. 100Mb/s) chip to a physical layer tranceiver. The MII may connect to an external transceiver device via a pluggable connector or simply connect two chips on the same printed circuit board. See MAC.

MIMD
Multiple Instruction Multiple Data

Mirrored volumes
A mirrored volume is a fault-tolerant volume that duplicates your data on two physical disks. If one of the physical disks fails, the data on the failed disk becomes unavailable, but the system continues to operate using the unaffected disk.

MTB/MTBC
Memory and Tukwila Board / Memory and Tukwila Board Controller.

MTBF
Mean Time Between Failure. An indicator of expected system reliability calculated on a statistical basis from the known failure rates of various components of the system. Note: MTBF is usually expressed in hours.

Multicore
Presence of two or more processors on a single chip.

Multimedia
Information presented through more than one type of media. On computer systems, this media includes sound, graphics, animation and text.

Multi-Tasking
The ability to perform several tasks simultaneously. Multi-tasking allows you to run multiple applications at the same time and exchange information among them. See Task.

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.

N

Nehalem
NEHALEM Intel Xeon Processor (8 cores per die).

NFS
Network File System. A proprietary distributed file system that is widely used by TCP/IP vendors. Note: NFS allows different computer systems to share files, and uses user datagram protocol (UDP) for data transfer.

NIC
Network Interface Controller.

NUMA
Non Uniform Memory Access. A method of configuring a cluster of microprocessors in a multiprocessing system so that they can share memory locally, improving performance and the ability of the system to be expanded.

NVRAM
Non Volatile Random Access Memory. A type of RAM that retains its contents even when the computer is powered off. See RAM and SRAM.

O

OF
Open Firmware. Firmware controlling a computer prior to the Operating System.

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.

Operating System
See OS.

OPMA
Open Platform Management Architecture Board.

OS
Operating System. The software which manages computer resources and provides the operating environment for application programs.

P

Password
A security feature that prevents an unauthorized user from operating the system.

PCI
Peripheral Component Interconnect. Bus architecture supporting high-performance peripherals.

PCIe
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.

ping
A basic Internet program that lets you verify that a particular IP address exists and can accept requests. The verb "to ping" means the act of using the ping utility or command.

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.

Plugging / Unplugging
Plugging and unplugging are static physical operations and represent the physical insertion / removal of a standard ARU. Plugging and unplugging procedures guarantee the electrical protection of live parts.

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.

PNP
Plug aNd Play. The ability to plug a device into a computer and have the computer recognize that the device is there.

POR
Power On Reset. Operation performed at the power on of the system.

POST
Power On Self Test. When power is turned on, POST (Power-On Self-Test) is the diagnostic testing sequence (or "starting program") that a computer runs to determine if hardware is working correctly.

Power-up Reset
See Cold Reset.

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. definition

PROM
Programmable Read-Only Memory.

PSB
Power Supply Box. AC powering unit providing DC to a server. Each Power Supply Module comprises a certain number of Power Supply Units (PSU) and a Power Distribution Board (PDB).

PSMI
Power Supply Management Interface.

PSU
Power Supply Unit. Sub-assembly of the Power Supply Module.

Q

QPI
Quick Path Interconnect. High-speed point-to-point Intel interface, used to interconnect processors and I/O Hubs, and optionally node controllers (BCS).

R

RADIUS
Remote Authentication Dial-In User Service. Authentication protocol. Radius is a server for remote user authentication and accounting. Its primary use is for Internet Service Providers, though it may be used on any network that needs a centralized authentication and/or accounting service for its workstations.

RAID
Redundant Array of Independent Disks. A method of combining hard disk drives into one logical storage unit for disk-fault tolerance.

RAM
Random Access Memory. A temporary storage area for data and programs. This type of memory must be periodically refreshed to maintain valid data and is lost when the computer is powered off. See NVRAM and SRAM.

RAS
Reliability, Availability, Serviceability.

Real-Time Clock
The Integrated Circuit in a computer that maintains the time and date.

Reset
A set of hardware-based events that result in a deterministic initial hardware state.

Recoverable Error
Recoverable errors include errors that are software correctable or hardware / software uncorrectable, for which servicing may be required for containment and restoration. See Error.

RFB
Remote Frame Buffer. Simple protocol for remote access to graphical user interfaces.

RFI
Radio Frequency Interference.

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.

RJ45
8-contact regular jack.

ROM
Read-Only Memory. A type of memory device that is used to store the system BIOS code. This code cannot be altered and is not lost when the computer is powered off. See BIOS, EPROM and Flash EPROM.

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.

SDR
Sensor Data Record. SDRs provide the information that tells management software what sensors, events, management controllers, and FRU information is available from a given IPMI implementation.

SDRR
Sensor Data Record Repository. A required feature of an embedded management controller, this is the material list for IPMI.

SDRAM
Synchronous Dynamic Random Access Memory.
A type of DRAM that runs at faster clock speeds than conventional memory. See DRAM.

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. See Hardware Console.

SIB
BCS Interconnect Board.

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.

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. The protocol governing network management and the monitoring of network devices and their functions.

SOAP
Simple Object Access Protocol. A call-response mechanism for XML documents.

Socket
Central Processing Unit mutlticore 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.

SPD
Serial Presence Detect. DIMM PROM.

SR
Scratch Register. Internal registers of both the Tukwila processor and the I/O Hub used as scratch area.

SRAM
Static RAM. A temporary storage area for data and programs. This type of memory does not need to be refreshed, but is lost when the system is powered off. See NVRAM and RAM.

SSH
Secure Shell. Network protocol that allows data to be exchanged using a secure channel between two networked devices.

Surprise Reset
A warm reset operation occuring during software operations, without allowing the OS to perform a graceful shutdown. The hardware partition may be in a hang-up situation preventing normal software partitions.

SVGA
Super Video Graphics Array.

T

TCP
Transmission Control Protocol. A set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet.

TCP/IP
Transmission Control Protocol / Internet Protocol. The basic communication language or protocol of the Internet.

T&D
Tests and Diagnostics.

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 die).

U

Unplugging
See Plugging / Unplugging.

URL
Uniform / Universal Resource Locator. The address of a file (resource) accessible on the Internet.

USB
Universal Serial Bus. A plug-and-play interface between a computer and add-on devices. The USB interface allows a new device to be added to your computer without having to add an adapter card or even having to turn the computer off.

V

VGA
Video Graphics Array.

VLAN
Virtual Local Area Network. A local area network with a definition that maps workstations on some other basis than geographic location (for example, by department, type of user, or primary application).

VMM
Virtual Machine Monitor.

W

WAN
Wide Area Network. Geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN).

Warm Reset
The second and successive reset after a cold reset. See Cold Reset.

WOL
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).

XML
eXtended MarkUp Language. A flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere.

XNC
External Node Controller. See BCS.

Y

No entries.

Z

ZOAR
Double port Intel GB Ethernet chips.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

Q

R

S

T

U

V

W

X

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

REFERENCE
86 A1 71FA 02