iCare Console

User's Guide

REFERENCE
86 A1 71FA 07

iCare Console

User's Guide

Hardware

June 2011

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

REFERENCE
86 A1 71FA 07
V1.3.0.0

Trademarks and Acknowledgements

The information in this document is subject to change without notice. Bull will not be liable for errors contained herein, or for incidental or consequential damages in connection with the use of this material.

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 the manufacturer may cause harmful interference and void the FCC authorization to operate this equipment. An FCC regulatory label is affixed to the equipment.

Canadian Compliance Statement (Industry Canada)

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

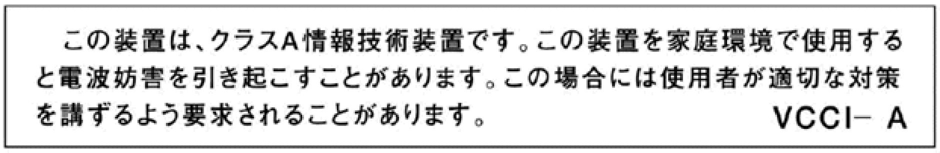
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

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

- ICES-003
- NMB-003

VCCI Statement

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



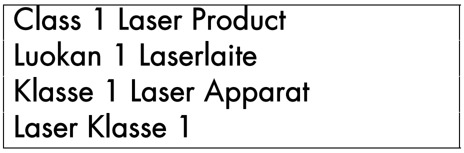
この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI– A

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

Laser Compliance Notice (if applicable)

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

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



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

Safety Information

Definition of Safety Notices

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

Waste Management

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

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

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)
- Linux Fedora Core 12 (or later)
- Linux RedHat 5 (or later)

Note The Bull Support Web site may be consulted for product information, documentation, updates and service offers:

http://support.bull.com

Note The iCare Console monitors and maintains different Bull Systems. The screenshots in this guide are therefore non-specific to a particular system.

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:

- Installing iCare Console Software, on page 1-2
- Displaying Software Version Information, on page 1-3
- Starting the iCare Console, on page 1-4
- iCare Console Overview, on page 1-6
- Initial Configuration, on page 1-10
- Stopping the iCare Console, on page 1-11

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:

- Linux Fedora Core 12 (or later)
- Windows XP, Vista (or later)
- Windows Server 2003, 2008 (or later)

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 2-21 and Importing Resources, on page 2-2 for details.

Prerequisites

- The firewall is configured to open the following network ports:
  - TCP Port 80 or 8080: HTTP
  - TCP Ports 20 and 21: FTP (Autocalls)
  - UDP Ports 161 and 162: SNMP
  - UDP Port 623: IPMITOOL
- Firefox (where applicable) is configured to accept cookies
- To use the iCare Console help in line with Firefox:
  - From the Firefox Tools > Options, click Applications:
  - On the line « Adobe Acrobat Document (application/pdf) » check the value is « Use Adobe Acrobat (in Firefox) »
- Internet Explorer (where applicable) 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
- Java Runtime Environment (JRE) is installed
- At least 140 MB disk space is available
- Adobe Reader to use the iCare Console help in line with Firefox

Procedure

1. From the *Resource and Documentation CD*, open the iCare folder.
2. Follow the instructions set out in the installation manual, according to the required Operating System (Windows or Linux).

   Once installed, users can connect remotely to the iCare Console using a Web browser.

1.2. Displaying Software Version Information

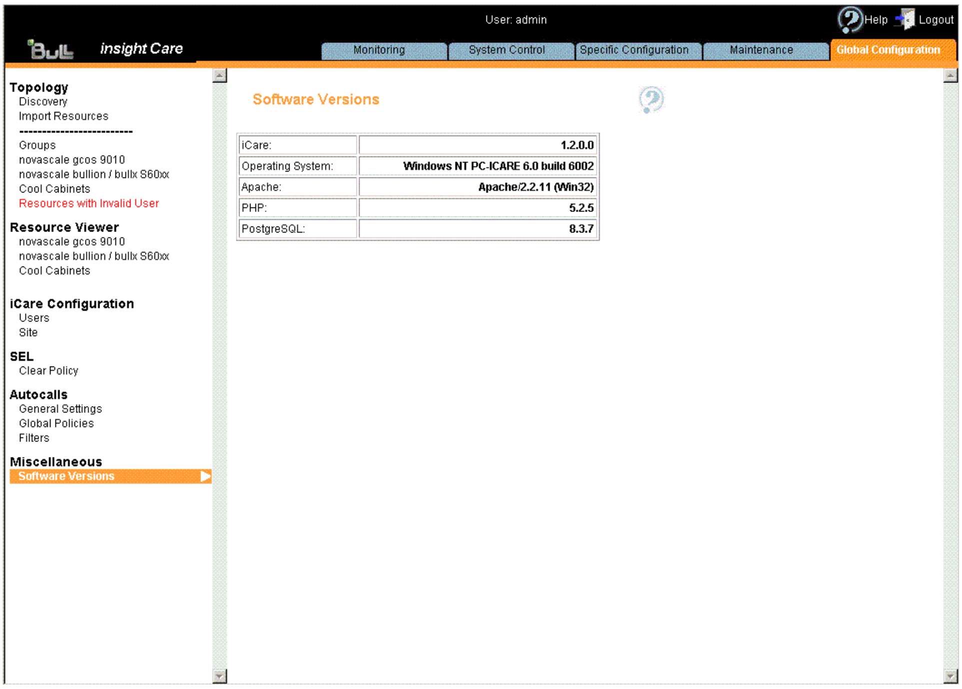
If needed for maintenance and troubleshooting operations, for example checking current software versions prior to an upgrade, you can display iCare Console and other software version information.

Prerequisites

None

Procedure

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



Software Versions

iCare:	1.2.0.0
Operating System:	Windows NT PC-ICARE 6.0 build 6002
Apache:	Apache/2.2.11 (Win32)
PHP:	5.2.5
PostgreSQL:	8.3.7

Figure 1-1. 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.

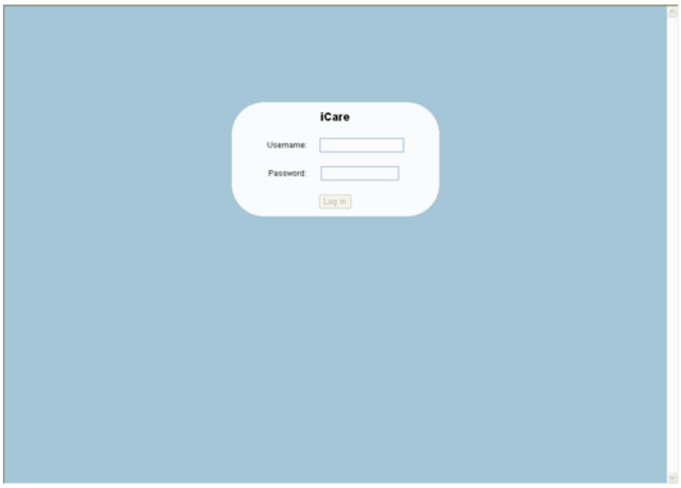
Prerequisites

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** (**http://xxx.xxx.xxx.xxx/icare**). The login page opens.



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

Figure 1-2. Login page description

Note Internet Explorer:

If IIS is active, TCP Port 80 is not available and iCare will use TCP Port 8080. In this case you must add the port number to the IP address, as follows: http://xxx.xxx.xxx.xxx:8080/icare

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)

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

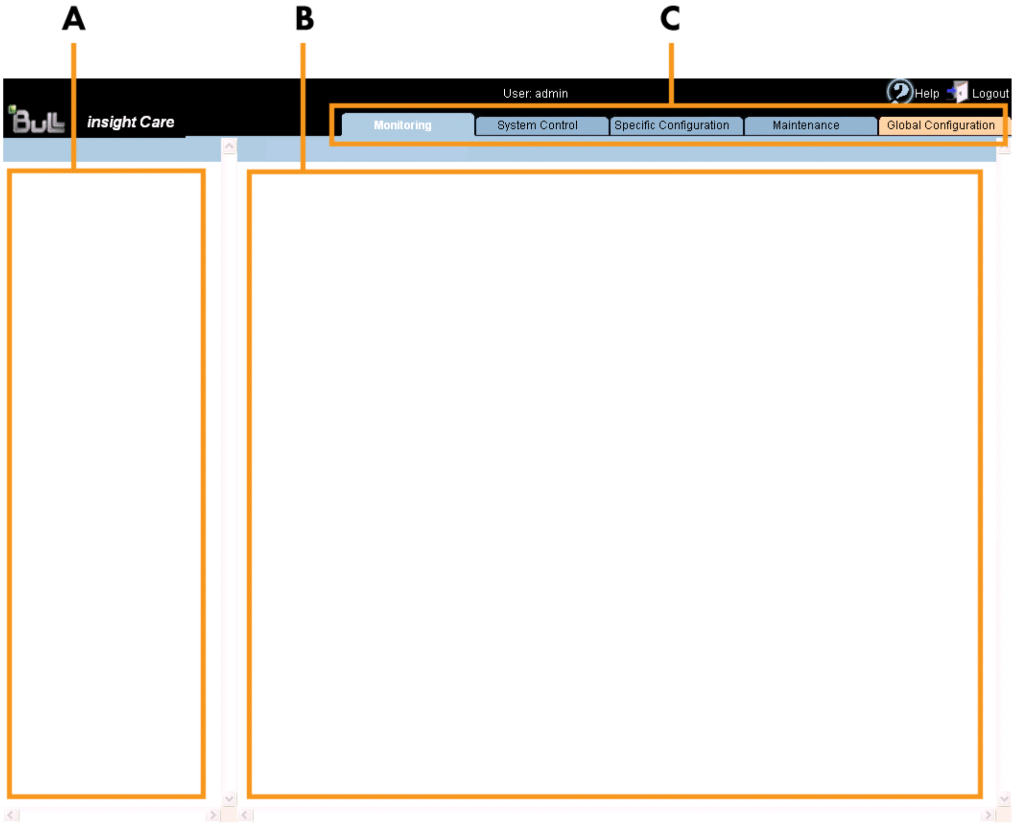
The following table lists the features available from the interface and their related sections in this guide.

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 4-1 • 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, BIOS and MCE status Logs • Automatic Clear System Event Log option
Managing Servicing Information, on page 5-1 • 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 iCare Users, on page 3-1

Table 1-1. 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**.

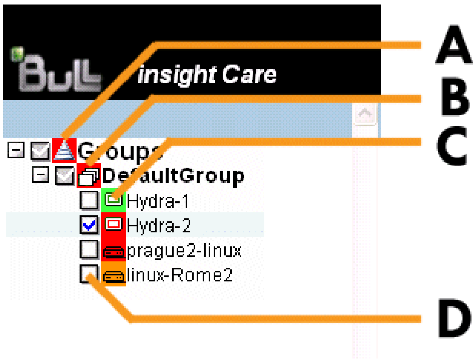


Interface Structure	
A: Tree pane	The **Tree pane** is tab-dependent: • When a **blue** tab is selected, the Tree pane displays the **Resource tree**. • When the **orange** tab is selected, the Tree pane displays the **Navigation tree**.
B: Work pane	The **Work pane** is tab-dependent: • When a **blue** 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 1-3. 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 1-4. Resource tree

Note See Monitoring Resources, on page 2-31 for more details about managing resource status.

Menu Bar

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

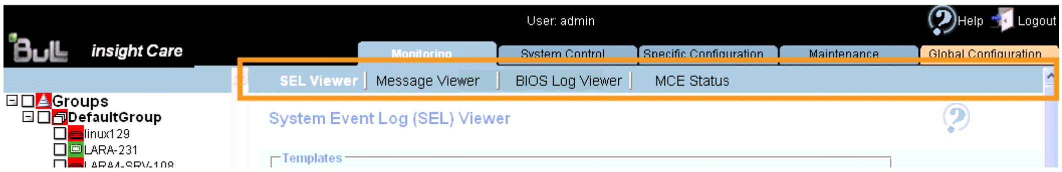


Figure 1-5. Menu Bar location

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:

- Importing Resources, on page 2-2
- Configuring Autocalls, on page 5-3, 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.

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:

- Importing Resources, on page 2-2
- Managing Imported Resources, on page 2-14
- Managing Resource Custom Groups, on page 2-24
- Monitoring Resources, on page 2-31
- Viewing Resource Details, on page 2-35
- Connecting to a Resource Console, on page 2-36

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 2-21 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 2-6
- Manually Importing a Single Resource, on page 2-10

Note For a graphical description of Resource tree features, see Figure 1-4. Resource tree, on page 1-8.

Important **According to the embedded management controller firmware version on imported hardware resources, you may need to perform a management 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.

Important **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 2-6
- Manually Importing a Single Resource, on page 2-10

Prerequisites

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.

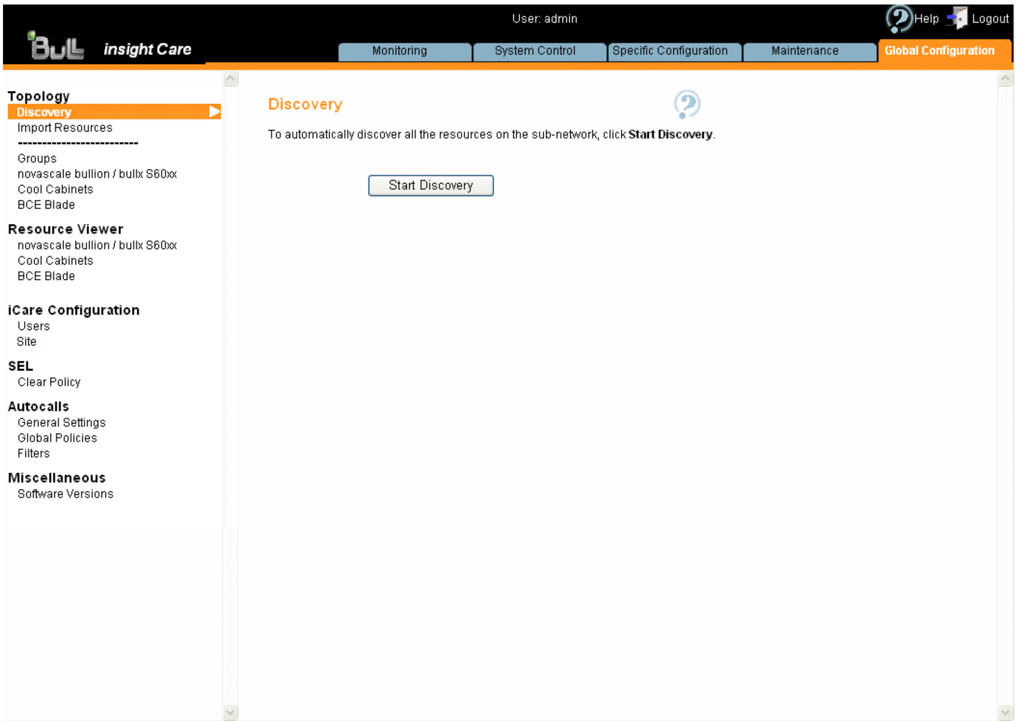
The user account you want to use to connect to the hardware resource BMC is created on the hardware resource BMC.

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 2-21 before importing them into the current console.

Note RESTRICTION:
When the iCare Console is installed on a Linux 64-bit Operating System, automatic discovery does not work. Resources must be declared using manual import or import using an XML template. See:
Using an XML File to Import Multiple Resources, on page 2-8
Manually Importing a Single Resource, on page 2-10

Procedure

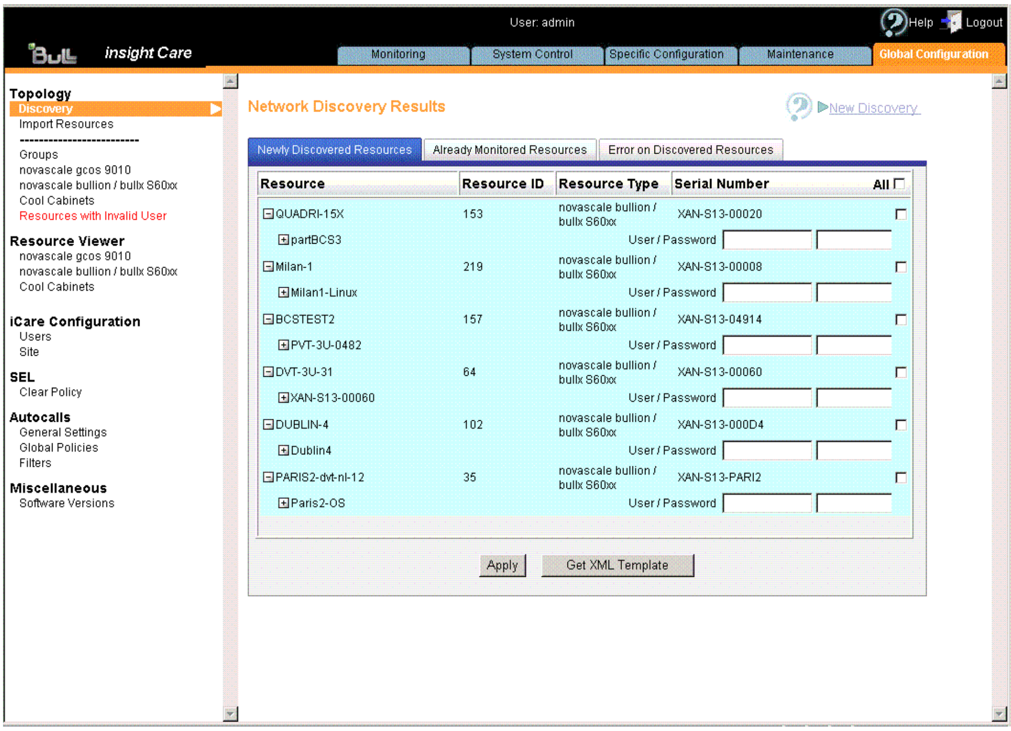
1. From the **Global Configuration** tab, click **Topology > Discovery**. The **Discovery** page appears.



To automatically discover all the resources on the sub-network, click **Start Discovery**.

Figure 2-1. Discovery page

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



Resource	Resource ID	Resource Type	Serial Number	All □
⊟ QUADRI-15X	153	novascale bullion / bullx S60xx	XAN-S13-00020	□
⊞ partBCS3		User / Password		
⊟ Milan-1	219	novascale bullion / bullx S60xx	XAN-S13-00008	□
⊞ Milan1-Linux		User / Password		
⊟ BCSTEST2	157	novascale bullion / bullx S60xx	XAN-S13-04914	□
⊞ PVT-3U-0482		User / Password		
⊟ DVT-3U-31	64	novascale bullion / bullx S60xx	XAN-S13-00060	□
⊞ XAN-S13-00060		User / Password		
⊟ DUBLIN-4	102	novascale bullion / bullx S60xx	XAN-S13-000D4	□
⊞ Dublin4		User / Password		
⊟ PARIS2-dvt-nl-12	35	novascale bullion / bullx S60xx	XAN-S13-PARI2	□
⊞ Paris2-OS		User / Password		

Figure 2-2. Network Discovery Results page - Multiple Resources

3. From the Newly Discovered Resources tab, select the resources you want to monitor, complete the User / Password fields and click Apply.

Notes
- The User / Password fields are mandatory.
- For more information about the Network Discovery Results page, see Managing Imported Resources, on page 2-14.

4. 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 perform a management 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.**

2.1.2. 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.

Important **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.

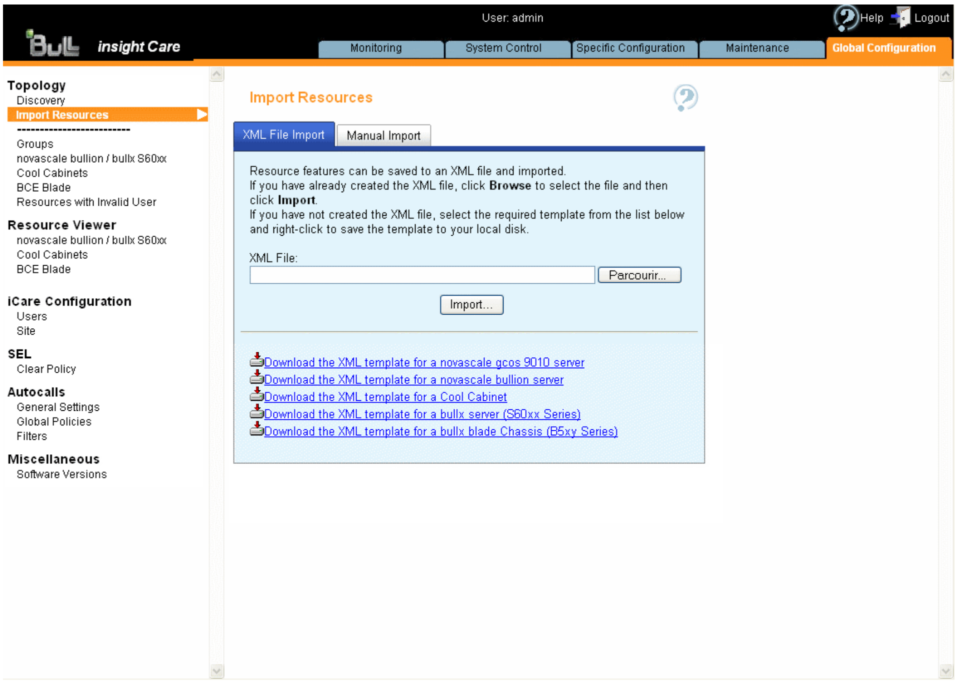
Important **The following procedure describes how to create an XML import file from the Import Resources page. Note that you can also get an XML import file using the automatic discovery feature. For details, see Adding Newly Discovered Resources to the Tree, on page 2-15.**

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.



Resource features can be saved to an XML file and imported.
If you have already created the XML file, click **Browse** to select the file and then click **Import**.
If you have not created the XML file, select the required template from the list below and right-click to save the template to your local disk.

XML File:

Download the XML template for a novascale gcos 9010 server
Download the XML template for a novascale bullion server
Download the XML template for a Cool Cabinet
Download the XML template for a bullx server (S60xx Series)
Download the XML template for a bullx blade Chassis (B5xy Series)

Figure 2-3. 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**.
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.

   For multi-module configuration, duplicate partition node according to the number of partitions in the server and duplicate module node according to the number of modules in the partition.
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.

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.

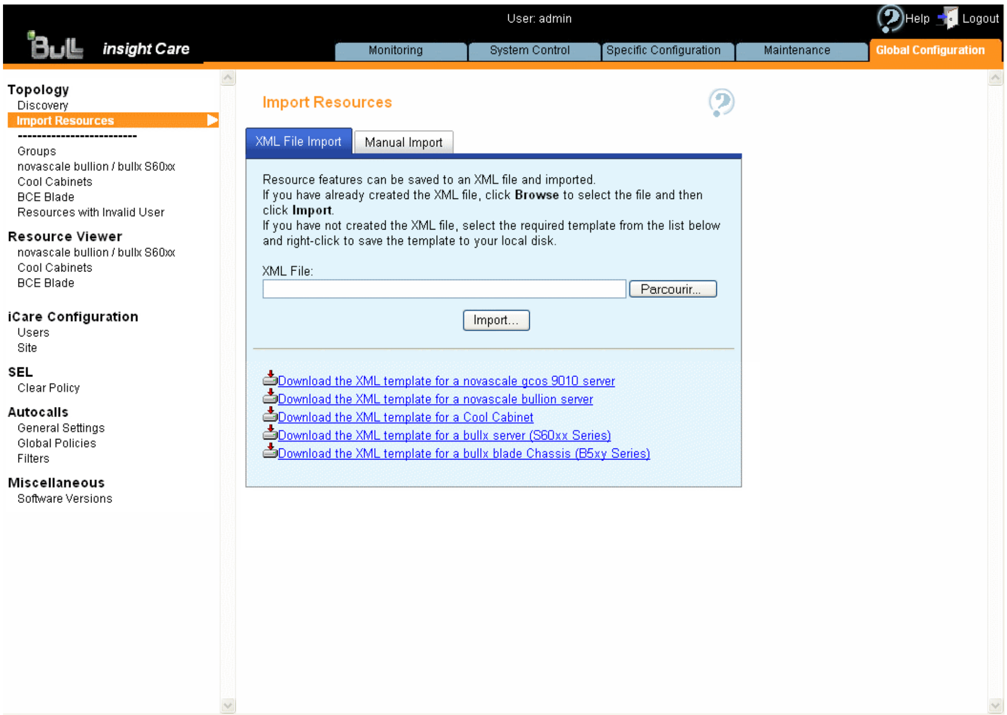
Prerequisites

The 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 2-21 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.

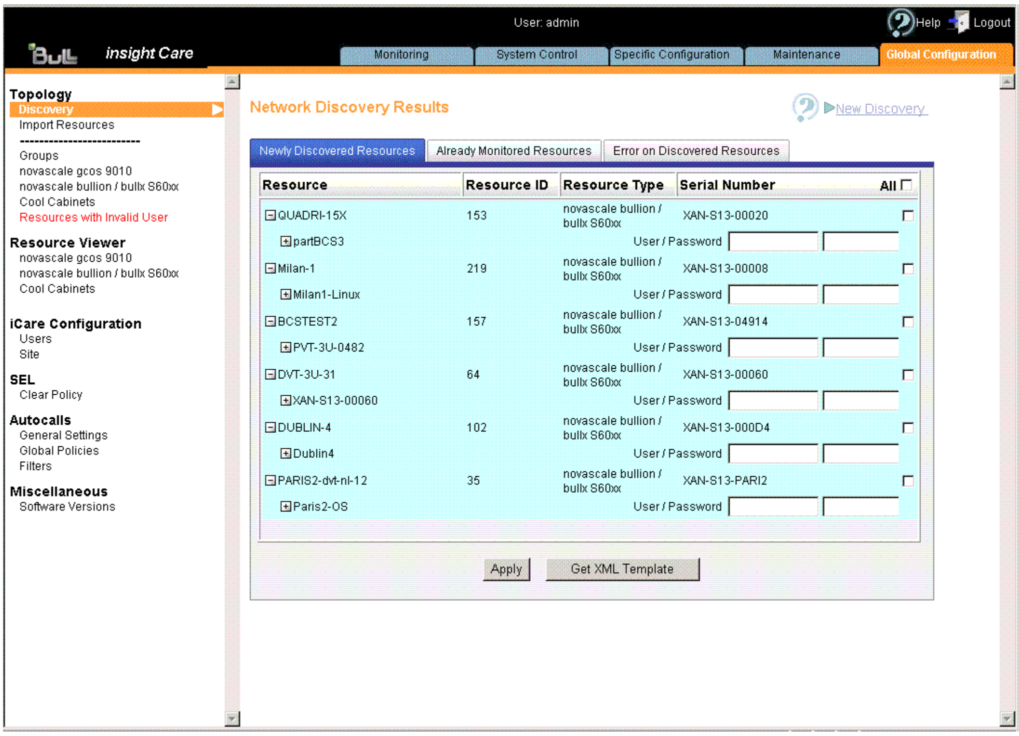


Resource features can be saved to an XML file and imported.
If you have already created the XML file, click **Browse** to select the file and then click **Import**.
If you have not created the XML file, select the required template from the list below and right-click to save the template to your local disk.

Download the XML template for a novascale gcos 9010 server
Download the XML template for a novascale bullion server
Download the XML template for a Cool Cabinet
Download the XML template for a bullx server (S60xx Series)
Download the XML template for a bullx blade Chassis (B5xy Series)

Figure 2-4. 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:



Network Discovery Results

Resource	Resource ID	Resource Type	Serial Number	All ☐
⊟QUADRI-15X	153	novascale bullion / bullx S60xx	XAN-S13-00020	☐
⊞partBCS3		User / Password		
⊟Milan-1	219	novascale bullion / bullx S60xx	XAN-S13-00008	☐
⊞Milan1-Linux		User / Password		
⊟BCSTEST2	157	novascale bullion / bullx S60xx	XAN-S13-04914	☐
⊞PVT-3U-0482		User / Password		
⊟DVT-3U-31	64	novascale bullion / bullx S60xx	XAN-S13-00060	☐
⊞XAN-S13-00060		User / Password		
⊟DUBLIN-4	102	novascale bullion / bullx S60xx	XAN-S13-000D4	☐
⊞Dublin4		User / Password		
⊟PARIS2-dvt-nl-12	35	novascale bullion / bullx S60xx	XAN-S13-PARI2	☐
⊞Paris2-OS		User / Password		

Figure 2-5. 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 2-14.

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 perform a management 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.**

2.1.3. 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.

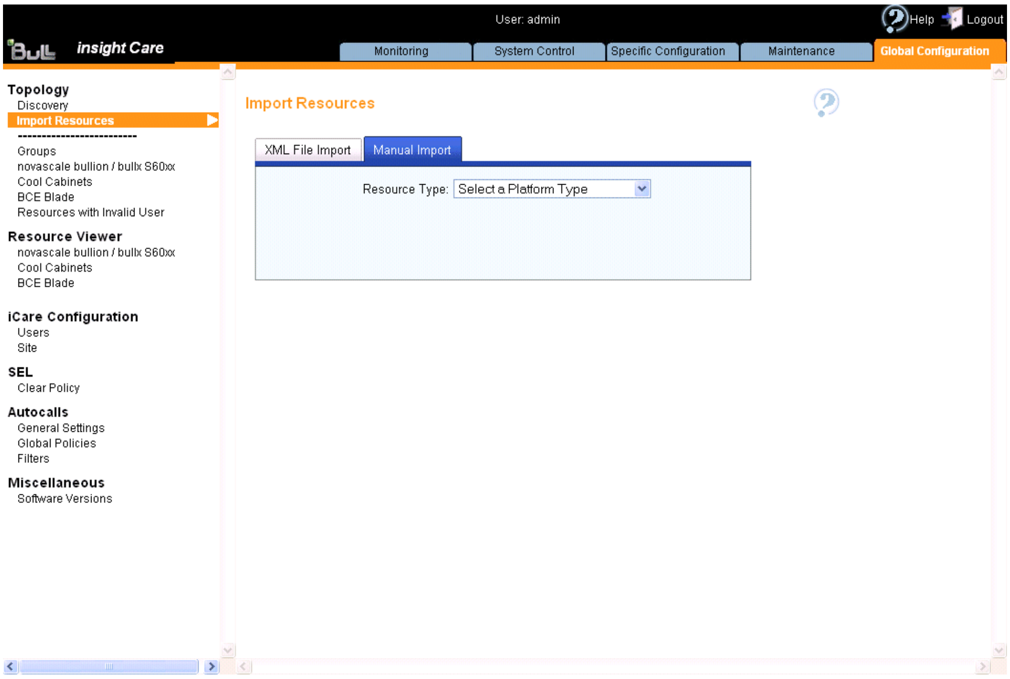
Important **If the hardware resource you want to import is on the same subnetwork as the iCare Console and is compatible, you are strongly advised to use the automatic discovery feature. See Automatically Importing Resources, on page 2-3.**

Prerequisites

The 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 2-21 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.



Resource Type: Select a Platform Type

Figure 2-6. Import Resources page - Manual Import tab

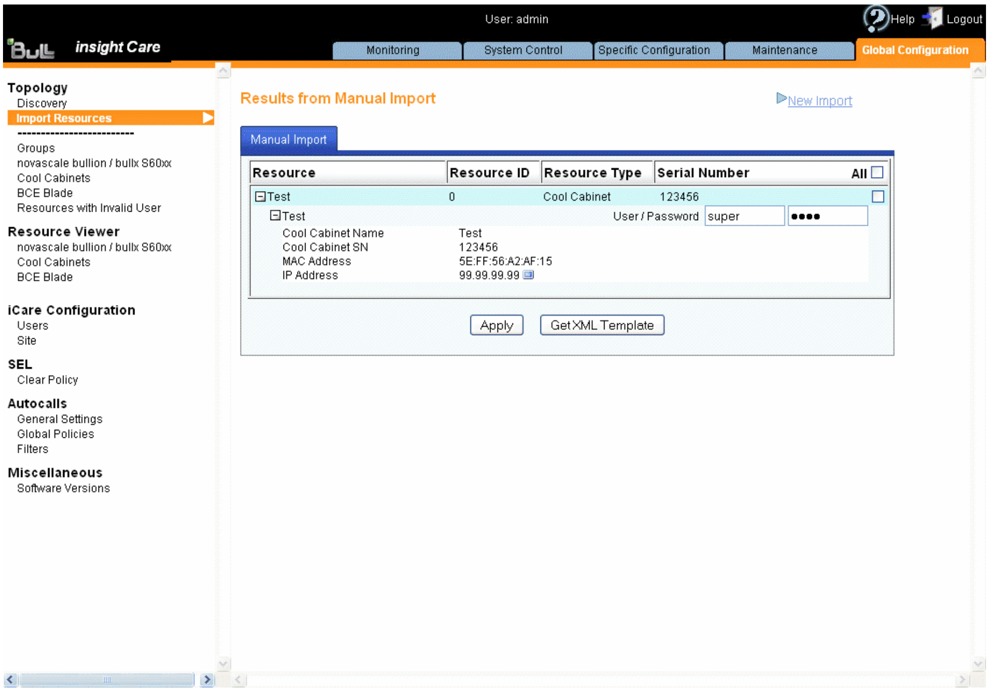
3. Use the resource Hardware Console configuration data to complete the fields, as explained in the following table:

Manual Import - novascale gcos 9010	
Resource Name	novascale gcos 9010 name - 16 characters maximum
Resource Serial Number	novascale gcos 9010 serial number - 13 characters
Resource ID	novascale gcos 9010 ID - Value between 0 and 65535
Partition Name	Partition name - 16 characters maximum
User	User account name and password used to connect to the resource (this account is set up on the hardware resource).
Password	
Partition Composition	Reserved.
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 - novascale bullion / bullx S6000	
Platform description	
Resource Name	Resource name - 16 characters maximum
Resource Serial Number	Resource serial number - 13 characters
Resource ID	Resource ID - Value between 0 and 65535
Module Count	Reserved. Automatically incremented.
Flexible	Reserved for futur usage.
Add Partition	Allow to add partition(s) into the platform
Partition description	
Partition Name	Partition name - 16 characters maximum
User	User account name and password used to connect to the resource (this account is set up on the hardware resource).
Password	
Partition Composition	Reserved. Automatically updated. 4 digits describing the presence of the 4 modules in the partition. One digit per module from the module ID 0, on the right, to the module ID 3, on the left. The digit is 1 if presence, 0 otherwise.
Master Module ID	Module ID of the partition used as the Master Module ID (the module IDs are set up on the hardware resource. You can use any module of the partition as the master module).
Add Module	Allow to add module(s) into the partition
Module description	
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)
Module ID	Module ID (single number inside the plaform).

Manual Import - Cool Cabinets and bullx Blade Chassis	
Resource Name	Resource name - 16 characters maximum
Resource Serial Number	Resource serial number - 13 characters
IP Address	BMC static IP address - decimal values (example: 129.192.1.10)
MAC Address	BMC MAC address - hexadecimal values (example: 5E:FF:56:A2:AF:15)
User	User account name and password used to connect to the resource (this account is set up on the hardware resource).
Password	

Table 2-1. Manual import data

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



Results from Manual Import

Resource	Resource ID	Resource Type	Serial Number	All □
⊟Test	0	Cool Cabinet	123456	□

⊟Test — User / Password: super ●●●●

Cool Cabinet Name: Test
Cool Cabinet SN: 123456
MAC Address: 5E:FF:56:A2:AF:15
IP Address: 99.99.99.99

Figure 2-7. 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 2-14.

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 perform a management 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.**

2.2. 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 Tree, on page 2-15
- Displaying Monitored Resources, on page 2-17
- Troubleshooting Resource Discovery Errors, on page 2-18

2.2.1. Adding Newly Discovered Resources to the 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.

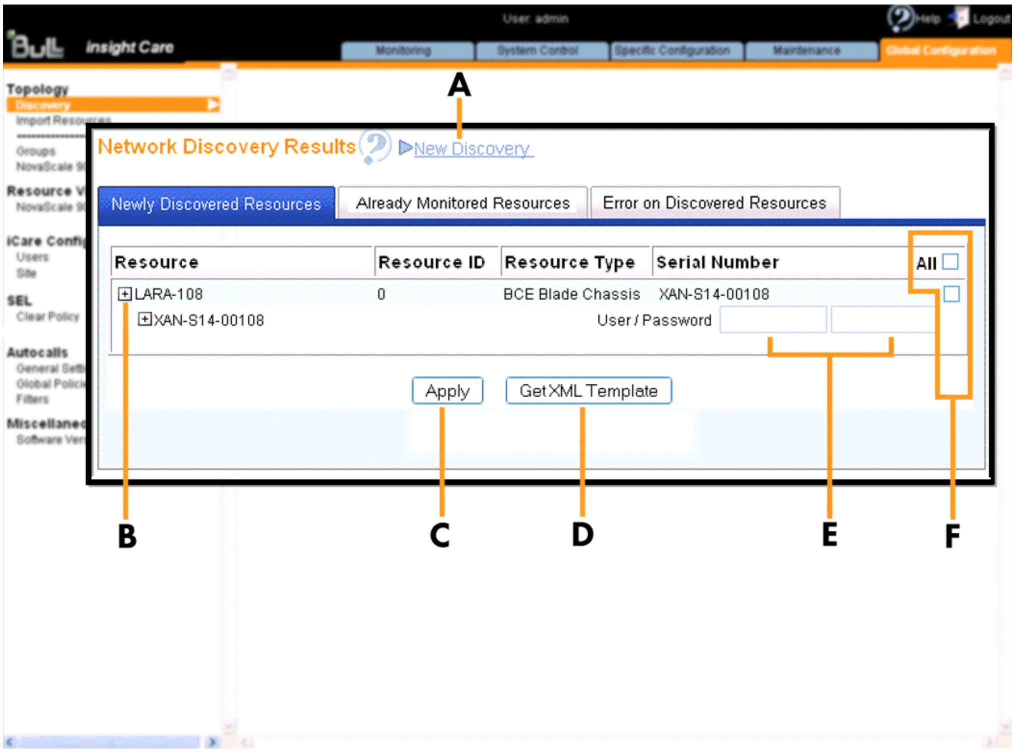
Note If the automatic discovery feature does not detect any new resources, the message **No resources discovered** is displayed.

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.



Network Discovery Results ▷New Discovery

Newly Discovered Resources | Already Monitored Resources | Error on Discovered Resources

Resource	Resource ID	Resource Type	Serial Number	All □
⊞LARA-108	0	BCE Blade Chassis	XAN-S14-00108	□
⊞XAN-S14-00108		User / Password		

Apply | Get XML Template

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: **Get XML Template** button	Click **Get XML Template** to save the selected resources into an XML file. Use this button when you want to import automatically discovered resources that are not on the same subnetwork as the iCare Console that should be used to manage them. For details on how to download the file on the appropriate iCare Console, see Using an XML File to Import Multiple Resources, on page 2-8.
E: **User/Password** fields	Name and password of the user account used to connect to the resource (this account is set up on the hardware resource).
F: 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 2-8. Network Discovery Results page (Newly Discovered Resources tab)

2.2.2. Displaying Monitored Resources

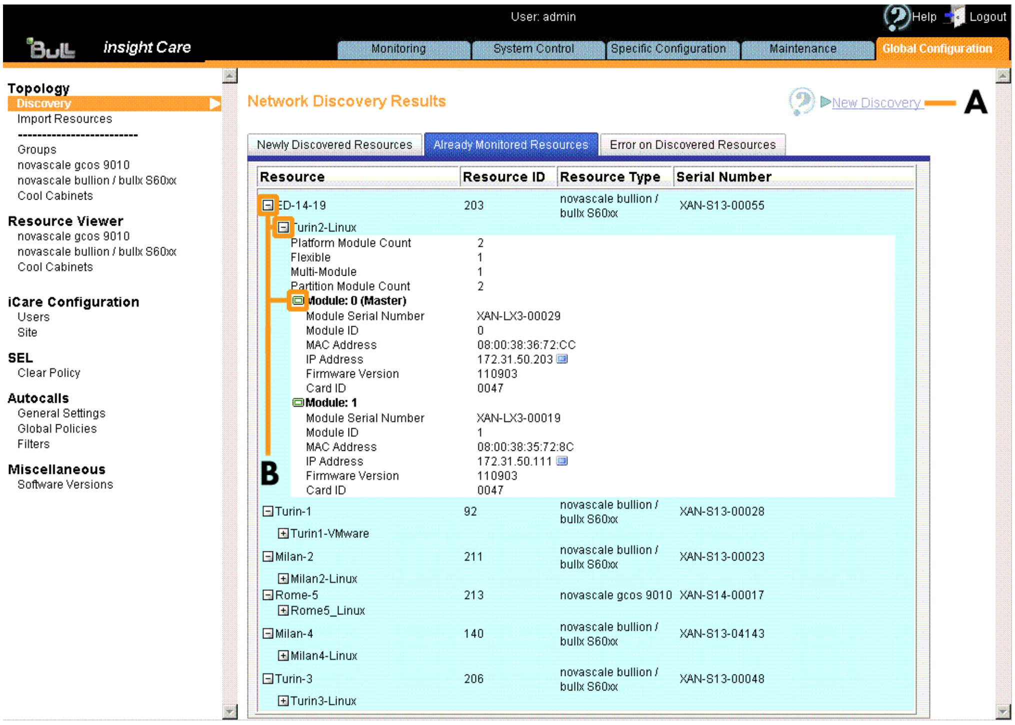
When hardware resources that are already monitored are re-discovered, they are displayed under the **Already Monitored Resources** tab in the **Network Discovery Results** page, allowing you to view detailed information about these resources.

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.



Network Discovery Results

Resource	Resource ID	Resource Type	Serial Number
⊟ ED-14-19	203	novascale bullion / bullx S60xx	XAN-S13-00055
⊟ Turin2-Linux			
Platform Module Count	2		
Flexible	1		
Multi-Module	1		
Partition Module Count	2		
Module: 0 (Master)			
Module Serial Number	XAN-LX3-00029		
Module ID	0		
MAC Address	08:00:38:36:72:CC		
IP Address	172.31.50.203		
Firmware Version	110903		
Card ID	0047		
Module: 1			
Module Serial Number	XAN-LX3-00019		
Module ID	1		
MAC Address	08:00:38:35:72:8C		
IP Address	172.31.50.111		
Firmware Version	110903		
Card ID	0047		
⊟ Turin-1	92	novascale bullion / bullx S60xx	XAN-S13-00028
⊞ Turin1-VMware			
⊟ Milan-2	211	novascale bullion / bullx S60xx	XAN-S13-00023
⊞ Milan2-Linux			
⊟ Rome-5	213	novascale gcos 9010	XAN-S14-00017
⊞ Rome5_Linux			
⊟ Milan-4	140	novascale bullion / bullx S60xx	XAN-S13-04143
⊞ Milan4-Linux			
⊟ Turin-3	206	novascale bullion / bullx S60xx	XAN-S13-00048
⊞ Turin3-Linux			

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 2-9. Network Discovery Results page (Already Monitored Resources tab)

2.2.3. Troubleshooting Resource Discovery Errors

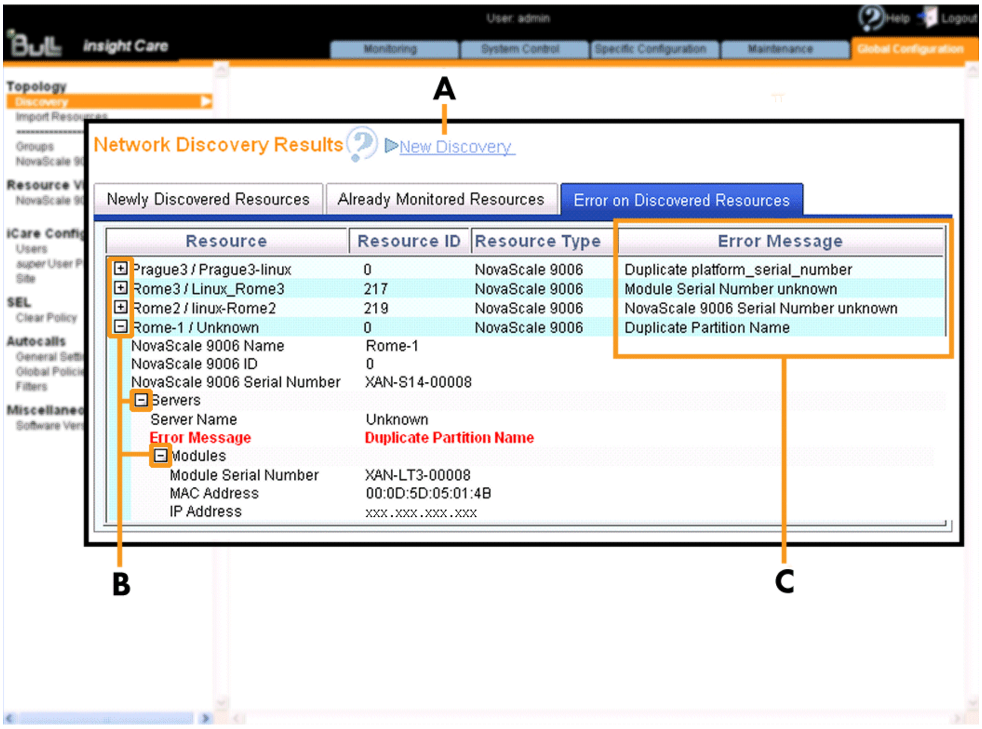
When hardware resources are discovered but cannot be imported, they are displayed under the **Error on Discovered Resources** tab in the **Network Discovery Results** page, allowing you to easily troubleshoot discovery errors.

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.



Network Discovery Results ▷New Discovery

Resource	Resource ID	Resource Type	Error Message
⊞ Prague3 / Prague3-linux	0	NovaScale 9006	Duplicate platform_serial_number
⊞ Rome3 / Linux_Rome3	217	NovaScale 9006	Module Serial Number unknown
⊞ Rome2 / linux-Rome2	219	NovaScale 9006	NovaScale 9006 Serial Number unknown
⊟ Rome-1 / Unknown	0	NovaScale 9006	Duplicate Partition Name
NovaScale 9006 Name	Rome-1		
NovaScale 9006 ID	0		
NovaScale 9006 Serial Number	XAN-S14-00008		
⊟ Servers			
Server Name	Unknown		
Error Message	Duplicate Partition Name		
⊟ Modules			
Module Serial Number	XAN-LT3-00008		
MAC Address	00:0D:5D:05:01:4B		
IP Address	xxx.xxx.xxx.xxx		

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 2-10. 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
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 2-2. Duplicate partition name error

Message	Duplicate platform name
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 2-3. Duplicate platform name error

Message	Duplicate platform ID
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 2-4. Duplicate platform ID error

Message	Duplicate platform serial number
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 2-5. Duplicate platform serial number error

Message	Platform serial number unknown
Description	The module serial number may not be engraved.
Actions	Contact your Customer Service Engineer.

Table 2-6. Platform serial number unknown error

Message	Duplicate module serial number
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 2-7. Duplicate module serial number error

Message	Module serial number unknown
Description	The module serial number may not be engraved.
Actions	Contact your Customer Service Engineer.

Table 2-8. Module serial number unknown error

Message	Module count does not match the number of modules
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 2-9. Module count does not match the number of modules error

Message	Duplicate MAC address
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 2-10. Duplicate MAC address error

Message	Duplicate IP address
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 2-11. Duplicate IP address error

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

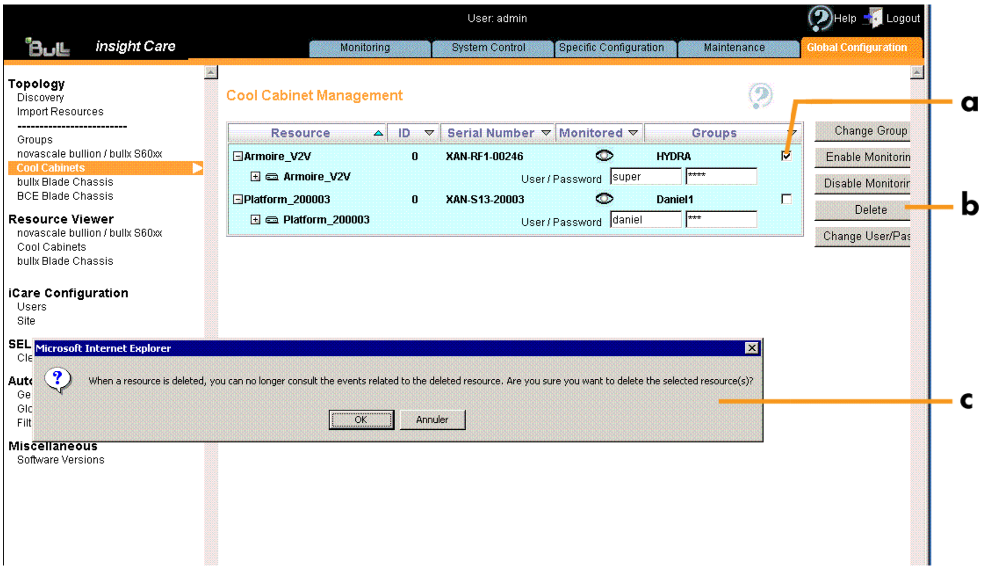
The hardware resource is present in the Resource tree

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.



Resource	ID	Serial Number	Monitored	Groups	
⊟Armoire_V2V	0	XAN-RF1-00246	◉	HYDRA	☑
⊞ Armoire_V2V		User / Password	super	****	
⊟Platform_200003	0	XAN-S13-20003	◉	Daniel1	□
⊞ Platform_200003		User / Password	daniel	***	

When a resource is deleted, you can no longer consult the events related to the deleted resource. Are you sure you want to delete the selected resource(s)?

Figure 2-11. Deleting a Resource

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

2.2.5. Changing a Resource User Account

The iCare Console connects to the hardware resource it monitors using a user account. This account is configured on the BMC embedded in the hardware resource through its Hardware Console. If this user account is updated, you must also update it through the iCare Console.

Prerequisites

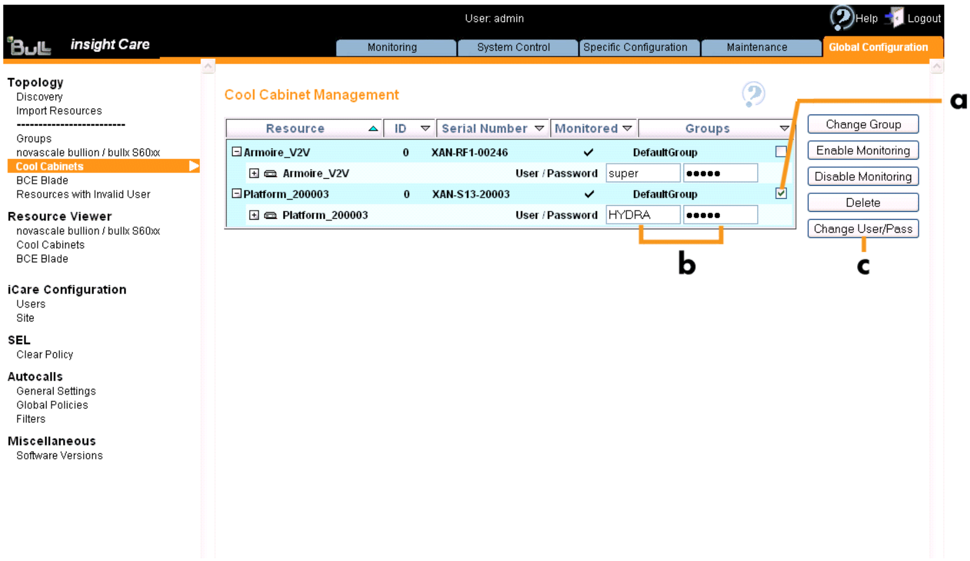
You have the updated user account information.

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 for which you want to update the user account information (a), complete the **User/Password** fields (b) and click **Change User/Pass** (c). The user account of the selected resource is updated and a confirmation box appears.



Cool Cabinet Management

Resource	ID	Serial Number	Monitored	Groups	
⊟ Armoire_V2V	0	XAN-RF1-00246	✓	DefaultGroup	□
⊞ Armoire_V2V			User / Password	super ●●●●●	
⊟ Platform_200003	0	XAN-S13-20003	✓	DefaultGroup	☑
⊞ Platform_200003			User / Password	HYDRA ●●●●●	

Figure 2-12. Changing a resource user account.

2.2.6. Troubleshooting Resources with Invalid User Accounts

When user acounts used to connect to resources are not correctly configured in the iCare Console, they are listed in the **Resources with Invalid User/Password** page, allowing you to easily troubleshoot invalid user accounts.

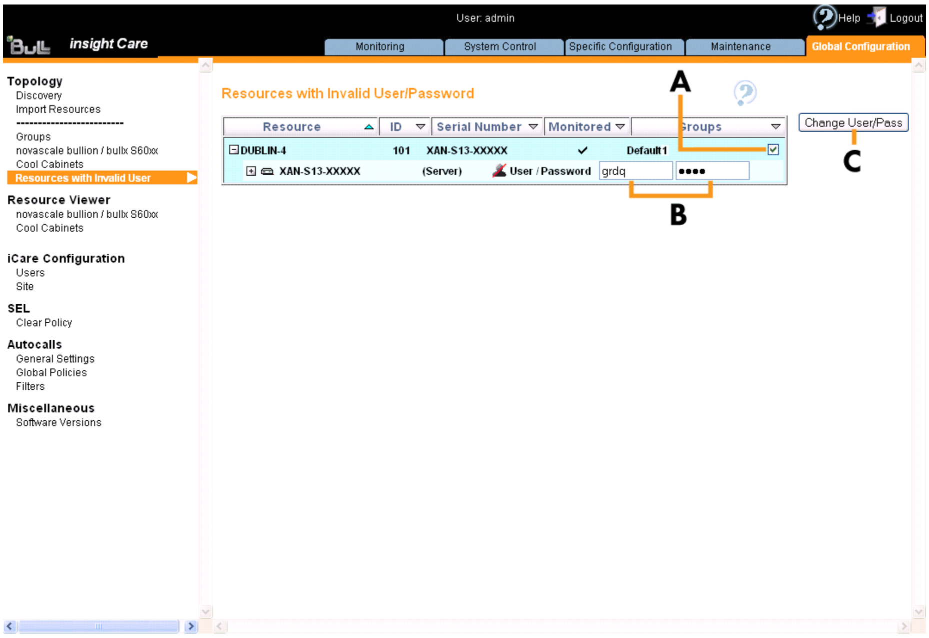
Note The item **Resources with Invalid User**, located in the Tree pane and which allows you to display the **Resources with Invalid User/Password** page is generated dynamically. If the iCare Console does not detect any resources with invalid user account, the item **Resources with Invalid User** is not displayed.

Prerequisites

- Resources with invalid user accounts are detected.
- User accounts set up for iCare Console are created in the resources.

Procedure

1. From the **Global Configuration** tab, click **Topology** > **Resources with Invalid User**. The **Resources with Invalid User/Password** page appears.
2. Select the hardware resource for which you want to modify the user account data (a), complete the **User/Password** fields (b) and click **Change User/Pass** (c). The selected resource is updated with the new user account values.



Resources with Invalid User/Password

Resource	ID	Serial Number	Monitored	Groups	
⊟ DUBLIN-4	101	XAN-S13-XXXXX	✓	Default1	☑
⊞ XAN-S13-XXXXX	(Server)	User / Password	grdq	●●●●	

Figure 2-13. Troubleshooting resources with invalid user account.

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 2-24
- Editing Resource Custom Group Details, on page 2-27
- Deleting a Resource Custom Group, on page 2-28
- Switching a Resource to a Custom Group, on page 2-29

Note For a graphical description of Resource tree features, refer to Figure 1-4. Resource tree, on page 1-8.

2.3.1. Creating a Resource Custom Group

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

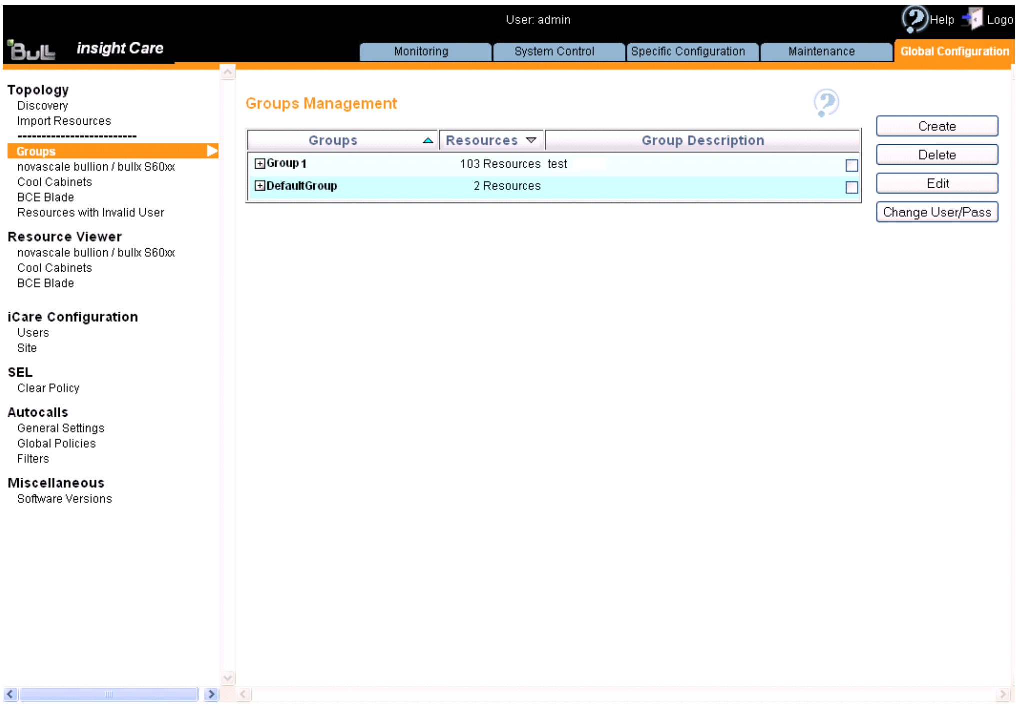
To allow you to organize your hardware resources to suit your needs, you can create your own resource groups or **Custom Groups**.

Prerequisites

None

Procedure

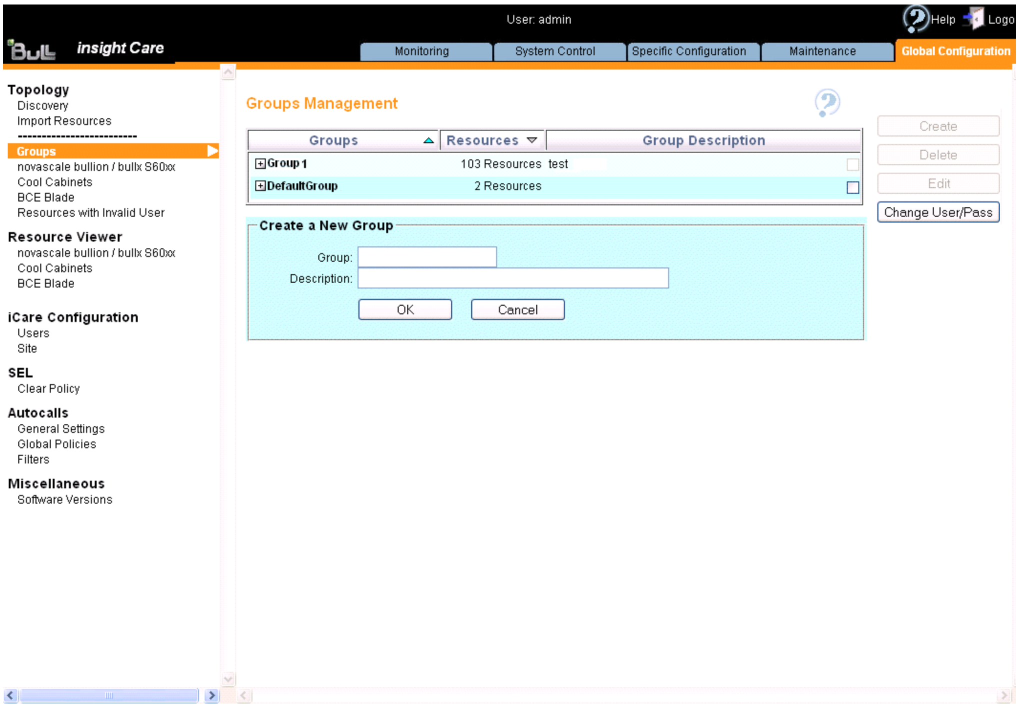
1. From the **Global Configuration** tab, click **Topology > Groups**. The **Groups Management** page appears.



Groups	Resources	Group Description	
⊞ Group 1	103 Resources	test	□
⊞ DefaultGroup	2 Resources		□

Figure 2-14. Groups Management page

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



Groups	Resources	Group Description
Group 1	103 Resources	test
DefaultGroup	2 Resources	

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 2-15. 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 Switching a Resource to a Custom Group, on page 2-29.

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

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.

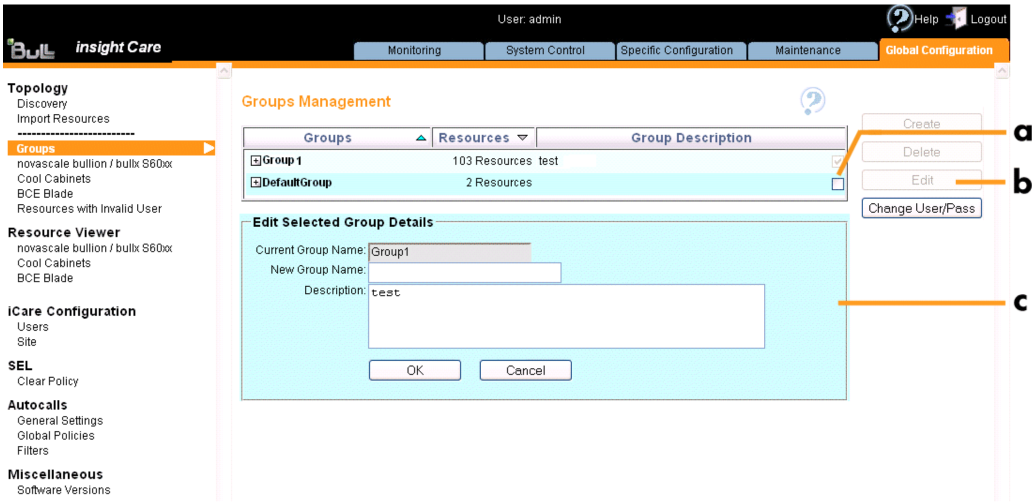
Note The predefined group **DefaultGroup** cannot be edited.

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).



Groups	Resources	Group Description
Group1	103 Resources	test
DefaultGroup	2 Resources	

Edit Selected Group Details

Current Group Name: Group1

New Group Name:

Description: test

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 2-16. Edit Selected Group Details box

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

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

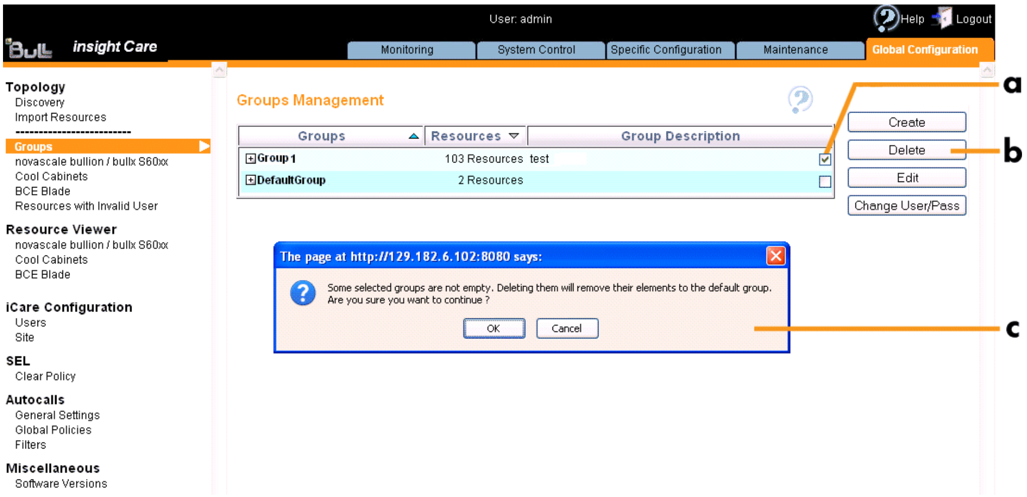
- The predefined group **DefaultGroup** cannot be deleted.
- If you delete a group that still contains hardware resources, these resources are automatically associated with the predefined group **DefaultGroup**.

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).



Groups	Resources	Group Description	
⊞Group 1	103 Resources	test	☑
⊞DefaultGroup	2 Resources		□

The page at http://129.182.6.102:8080 says:

Some selected groups are not empty. Deleting them will remove their elements to the default group.
Are you sure you want to continue ?

Figure 2-17. Groups Management page - Group deletion

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

2.3.4. Switching a Resource to a Custom Group

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

Prerequisites

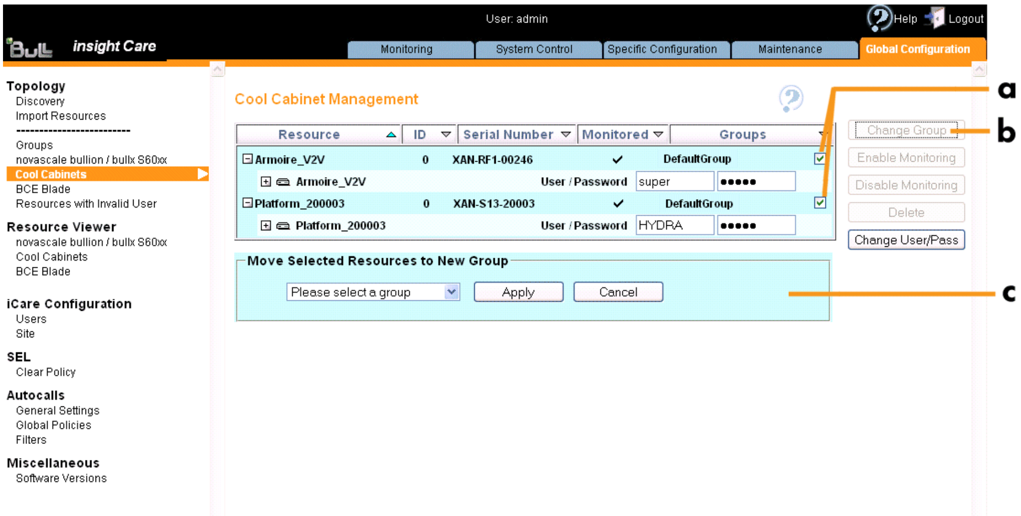
At least one custom group is created (for details, see Creating a Resource Custom Group, on page 2-24).

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).



Resource	ID	Serial Number	Monitored	Groups	
⊟ Armoire_V2V	0	XAN-RF1-00246	✓	DefaultGroup	☑
⊞ Armoire_V2V		User / Password	super	●●●●●	
⊟ Platform_200003	0	XAN-S13-20003	✓	DefaultGroup	☑
⊞ Platform_200003		User / Password	HYDRA	●●●●●	

Figure 2-18. Moving Resources - example

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.

2.3.5. Changing the User Account of Resources Belonging to the Same Group

When an identical user account is updated on many resources monitored by the iCare Console, you must also update it through the iCare Console. Instead of changing the user account resource by resource, you can declare the updated user account once, provided that the resources belong to the same group.

Prerequisites

You have the updated user account information.

The user account is the same for all the resources to update.

The resources to update belong to the same group.

Procedure

1. From the **Global Configuration** tab, click **Topology > Groups**. The **Groups Management** page appears.
2. Expand (a) and select (b) the group containing the hardware resources for which you want to update the user account information, complete the **User** and **Password** fields (c) and click **Change User/Pass** (d). The user accounts of all the resources associated with the selected group are updated and a confirmation box appears.

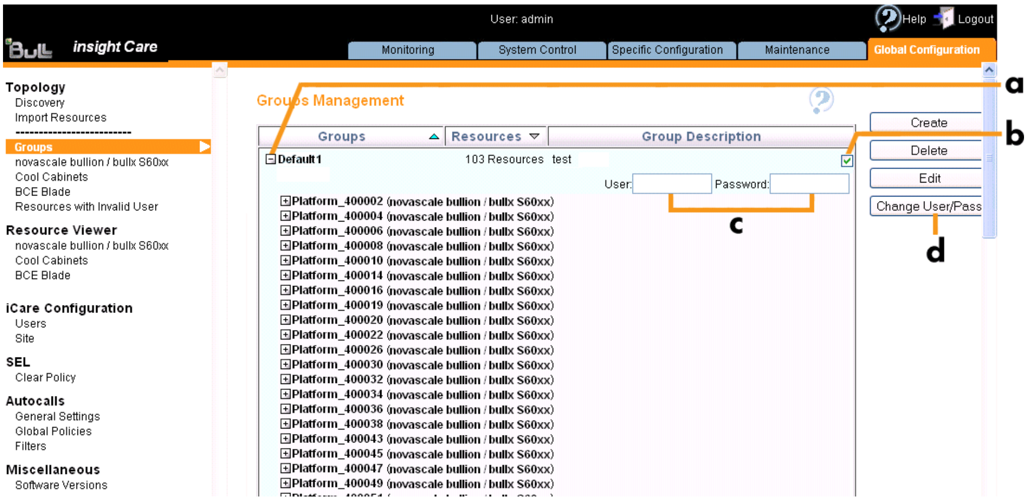

User: admin
Help
Logout
insight Care
Monitoring
System Control
Specific Configuration
Maintenance
Global Configuration
Topology
Discovery
Import Resources
Groups
novascale bullion / bullx S60xx
Cool Cabinets
BCE Blade
Resources with Invalid User
Resource Viewer
novascale bullion / bullx S60xx
Cool Cabinets
BCE Blade
iCare Configuration
Users
Site
SEL
Clear Policy
Autocalls
General Settings
Global Policies
Filters
Miscellaneous
Software Versions
Groups Management
Groups
Resources
Group Description
Default1
103 Resources
test
☑
User:
Password:
Platform_400002 (novascale bullion / bullx S60xx)
Platform_400004 (novascale bullion / bullx S60xx)
Platform_400006 (novascale bullion / bullx S60xx)
Platform_400008 (novascale bullion / bullx S60xx)
Platform_400010 (novascale bullion / bullx S60xx)
Platform_400014 (novascale bullion / bullx S60xx)
Platform_400016 (novascale bullion / bullx S60xx)
Platform_400019 (novascale bullion / bullx S60xx)
Platform_400020 (novascale bullion / bullx S60xx)
Platform_400022 (novascale bullion / bullx S60xx)
Platform_400026 (novascale bullion / bullx S60xx)
Platform_400030 (novascale bullion / bullx S60xx)
Platform_400032 (novascale bullion / bullx S60xx)
Platform_400034 (novascale bullion / bullx S60xx)
Platform_400036 (novascale bullion / bullx S60xx)
Platform_400038 (novascale bullion / bullx S60xx)
Platform_400043 (novascale bullion / bullx S60xx)
Platform_400045 (novascale bullion / bullx S60xx)
Platform_400047 (novascale bullion / bullx S60xx)
Platform_400049 (novascale bullion / bullx S60xx)
Create
Delete
Edit
Change User/Pass
a
b
c
d

Figure 2-19. Changing a resource user account.

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 enabled for a hardware resource, the BIOS logs already present on the hardware resource are collected into the iCare Console database. The next BIOS logs will be sent to the iCare Console database. See Building and Checking BIOS Logs, on page 4-15**
When monitoring is disabled for a hardware resource, it disappears from the Resource tree and events are no longer recorded.
Events and BIOS logs 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 2-21.

Prerequisites

The hardware resource is present in the Resource tree

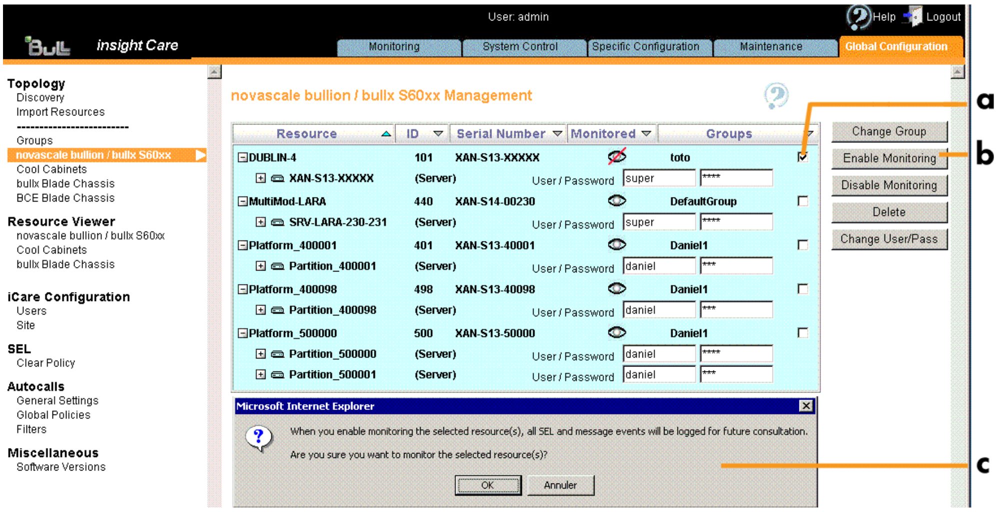
Procedure

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.



novascale bullion / bullx S60xx Management

Resource	ID	Serial Number	Monitored	Groups			
⊟DUBLIN-4	101	XAN-S13-XXXXX	⊘	toto			☑
⊞ XAN-S13-XXXXX	(Server)		User / Password		super	****	
⊟MultiMod-LARA	440	XAN-S14-00230	👁	DefaultGroup			☐
⊞ SRV-LARA-230-231	(Server)		User / Password		super	****	
⊟Platform_400001	401	XAN-S13-40001	👁	Daniel1			☐
⊞ Partition_400001	(Server)		User / Password		daniel	***	
⊟Platform_400098	498	XAN-S13-40098	👁	Daniel1			☐
⊞ Partition_400098	(Server)		User / Password		daniel	***	
⊟Platform_500000	500	XAN-S13-50000	👁	Daniel1			☐
⊞ Partition_500000	(Server)		User / Password		daniel	****	
⊞ Partition_500001	(Server)		User / Password		daniel	***	

Microsoft Internet Explorer

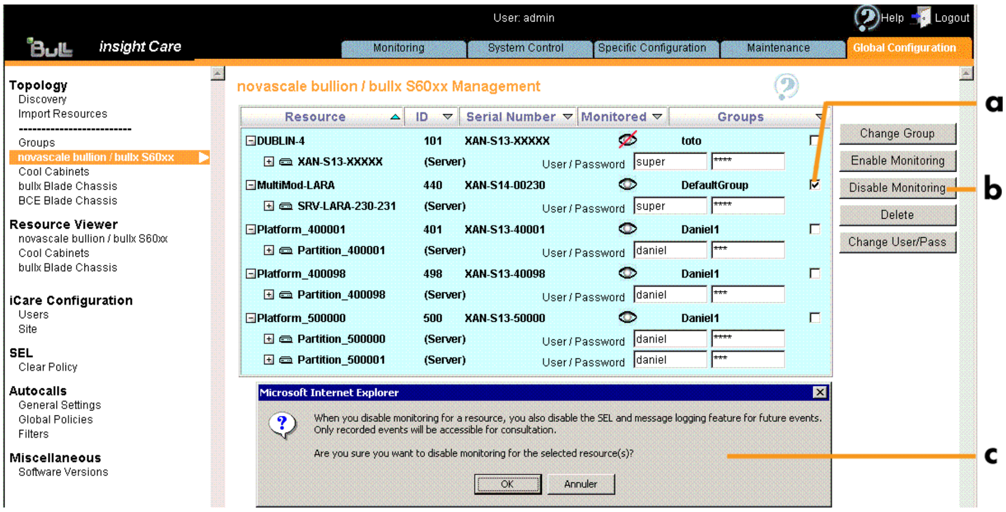
When you enable monitoring the selected resource(s), all SEL and message events will be logged for future consultation.

Are you sure you want to monitor the selected resource(s)?

OK Annuler

Figure 2-20. 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.



novascale bullion / bullx S60xx Management

Resource	ID	Serial Number	Monitored	Groups			
⊟DUBLIN-4	101	XAN-S13-XXXXX	⊘	toto			☐
⊞ XAN-S13-XXXXX	(Server)		User / Password		super	****	
⊟MultiMod-LARA	440	XAN-S14-00230	👁	DefaultGroup			☑
⊞ SRV-LARA-230-231	(Server)		User / Password		super	****	
⊟Platform_400001	401	XAN-S13-40001	👁	Daniel1			☐
⊞ Partition_400001	(Server)		User / Password		daniel	***	
⊟Platform_400098	498	XAN-S13-40098	👁	Daniel1			☐
⊞ Partition_400098	(Server)		User / Password		daniel	***	
⊟Platform_500000	500	XAN-S13-50000	👁	Daniel1			☐
⊞ Partition_500000	(Server)		User / Password		daniel	****	
⊞ Partition_500001	(Server)		User / Password		daniel	***	

Microsoft Internet Explorer

When you disable monitoring for a resource, you also disable the SEL and message logging feature for future events.
Only recorded events will be accessible for consultation.

Are you sure you want to disable monitoring for the selected resource(s)?

OK Annuler

Figure 2-21. 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 perform a management 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.**

2.4.2. 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 2-12. You can then query the database to view the event and analyze the problem, as explained in Building and Checking System Event Logs (SEL), on page 4-2.

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 2-12. Resource status icons

2.5. Viewing Resource Details

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

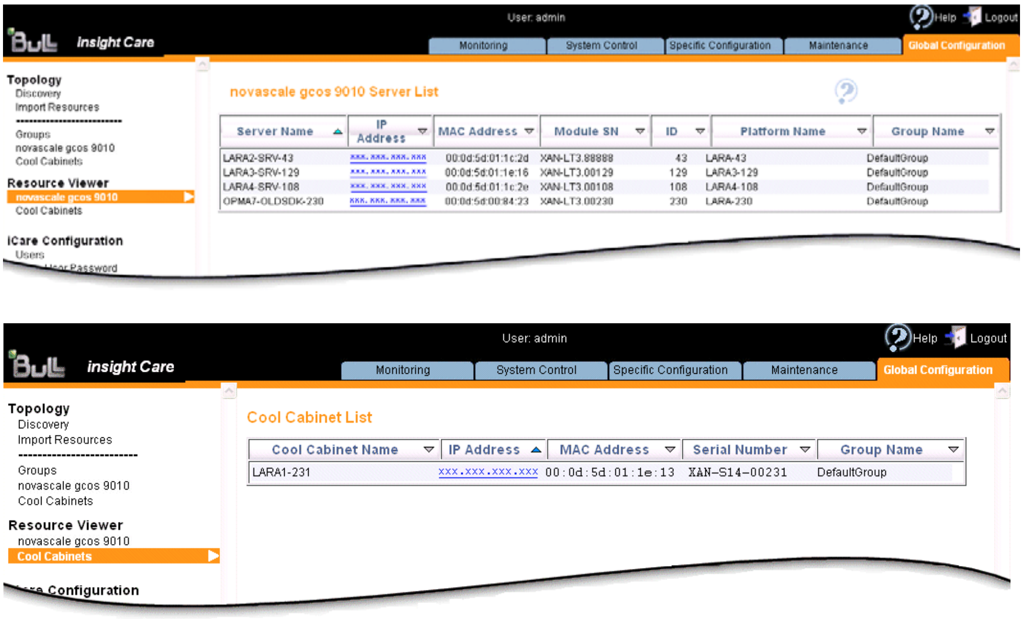
- IP and MAC addresses
- Serial number
- Server name, Group name, Platform name and ID

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.



novascale gcos 9010 Server List

Server Name	IP Address	MAC Address	Module SN	ID	Platform Name	Group Name
LARA2-SRV-43	xxx.xxx.xxx.xxx	00:0d:5d:01:1c:2d	XAN-LT3.88888	43	LARA-43	DefaultGroup
LARA3-SRV-129	xxx.xxx.xxx.xxx	00:0d:5d:01:1e:16	XAN-LT3.00129	129	LARA3-129	DefaultGroup
LARA4-SRV-108	xxx.xxx.xxx.xxx	00:0d:5d:01:1c:2e	XAN-LT3.00108	108	LARA4-108	DefaultGroup
OPMA7-OLDSDK-230	xxx.xxx.xxx.xxx	00:0d:5d:00:84:23	XAN-LT3.00230	230	LARA-230	DefaultGroup

Cool Cabinet List

Cool Cabinet Name	IP Address	MAC Address	Serial Number	Group Name
LARA1-231	xxx.xxx.xxx.xxx	00:0d:5d:01:1e:13	XAN-S14-00231	DefaultGroup

Figure 2-22. 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 2-36

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.

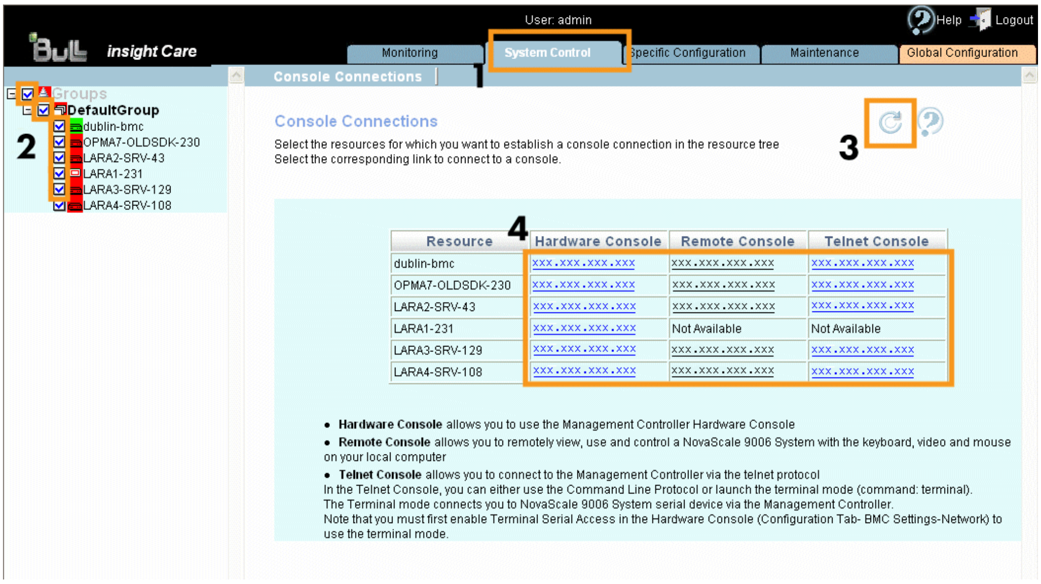
Resource console access is also available from other iCare Console pages, as explained in Managing System Event Logs (SEL), on page 4-7 and Viewing Resource Details, on page 2-35.

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

Select the resources for which you want to establish a console connection in the resource tree
Select the corresponding link to connect to a console.

Resource	Hardware Console	Remote Console	Telnet Console
dublin-bmc	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
OPMA7-OLDSDK-230	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
LARA2-SRV-43	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
LARA1-231	xxx.xxx.xxx.xxx	Not Available	Not Available
LARA3-SRV-129	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
LARA4-SRV-108	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx

- **Hardware Console** allows you to use the Management Controller Hardware Console
- **Remote Console** allows you to remotely view, use and control a NovaScale 9006 System with the keyboard, video and mouse on your local computer
- **Telnet Console** allows you to connect to the Management Controller via the telnet protocol

In the Telnet Console, you can either use the Command Line Protocol or launch the terminal mode (command: terminal).
The Terminal mode connects you to NovaScale 9006 System serial device via the Management Controller.
Note that you must first enable Terminal Serial Access in the Hardware Console (Configuration Tab- BMC Settings-Network) to use the terminal mode.

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 2-23. 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.

Chapter 3. Managing iCare Users

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.

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

- Creating a User Account, on page 3-2
- Deleting a User Account, on page 3-3
- Changing a User Account Password, on page 3-4

3.1. Creating a User Account

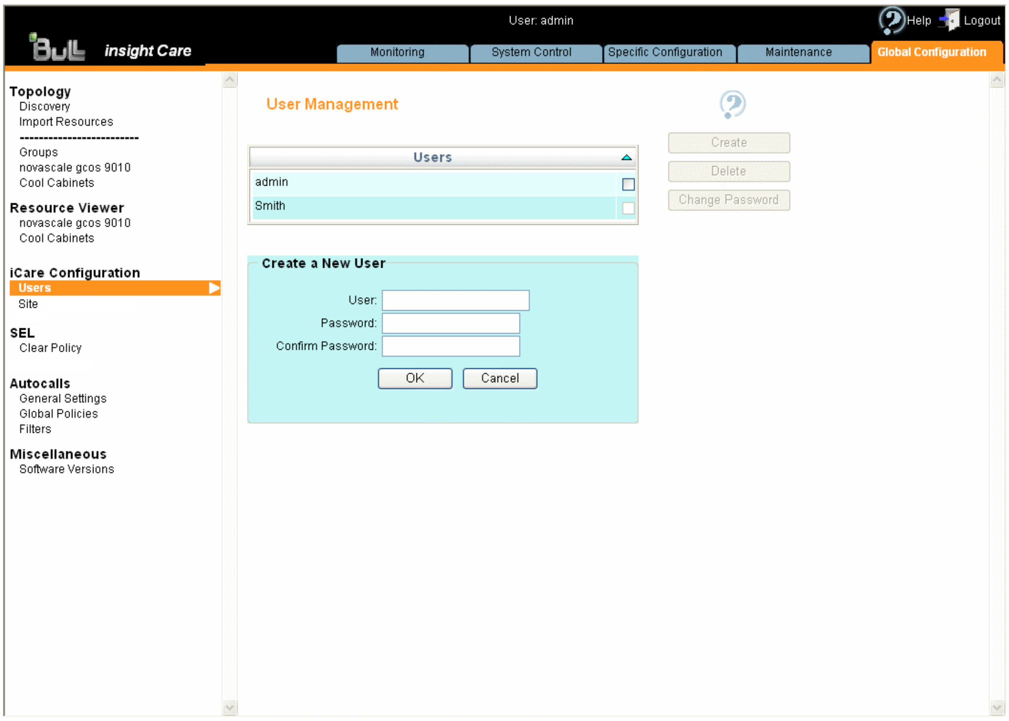
You can create a personal user account for each person that needs to log onto and use the iCare Console.

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.



<table>
<tr><th colspan="2">Create a New User</th></tr>
<tr><td>User</td><td>Name the user will use to log on.
• Name limited to 16 characters - CASE SENSITIVE.
• The following characters are not allowed: /\"`&'+*%=><:!?;,~| and space.</td></tr>
<tr><td>Password</td><td rowspan="2">Password the user will use to log on.
• Maximum password length: 16 characters
• No character restriction - CASE SENSITIVE.</td></tr>
<tr><td>Confirm Password</td></tr>
</table>

Figure 3-1. 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.

3.2. 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.

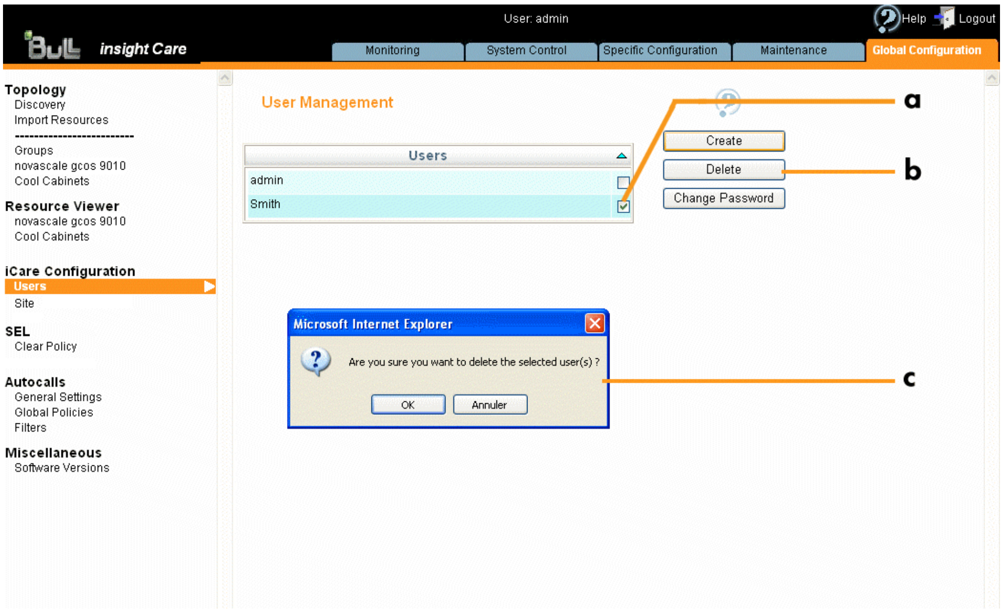
Note You cannot delete the predefined user account **admin**. However, the default **admin** user password can be changed, as detailed in Changing a User Account Password, on page 3-4.

Prerequisites

None

Procedure

1. From the **Global 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.



Users	
admin	□
Smith	☑

Are you sure you want to delete the selected user(s) ?

Figure 3-2. User Management page (Delete User Account)

3.3. Changing a User Account Password

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

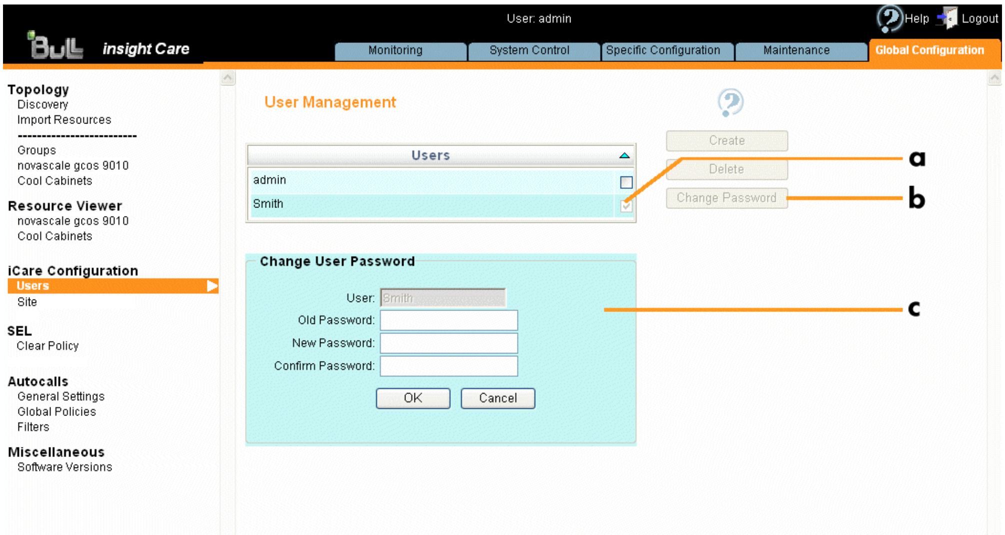
Note You are strongly advised to change the factory-default admin user password before using the console for the first time.

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).



Change User Password

User: Smith

Old Password:

New Password:

Confirm Password:

Figure 3-3. 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.

Chapter 4. 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:

- Building and Checking System Event Logs (SEL), on page 4-2
- Managing System Event Logs (SEL), on page 4-7
- Enabling/Disabling the Automatic Clear SEL Policy, on page 4-10
- Building and Checking Board and Security Message Logs, on page 4-11
- Managing Board and Security Message Logs, on page 4-13
- Building and Checking BIOS Logs, on page 4-15
- Managing BIOS Logs, on page 4-17
- Building and Checking MCE Status Logs, on page 4-19
- Managing Database, on page 4-22

4.1. Building and Checking 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.

Important **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

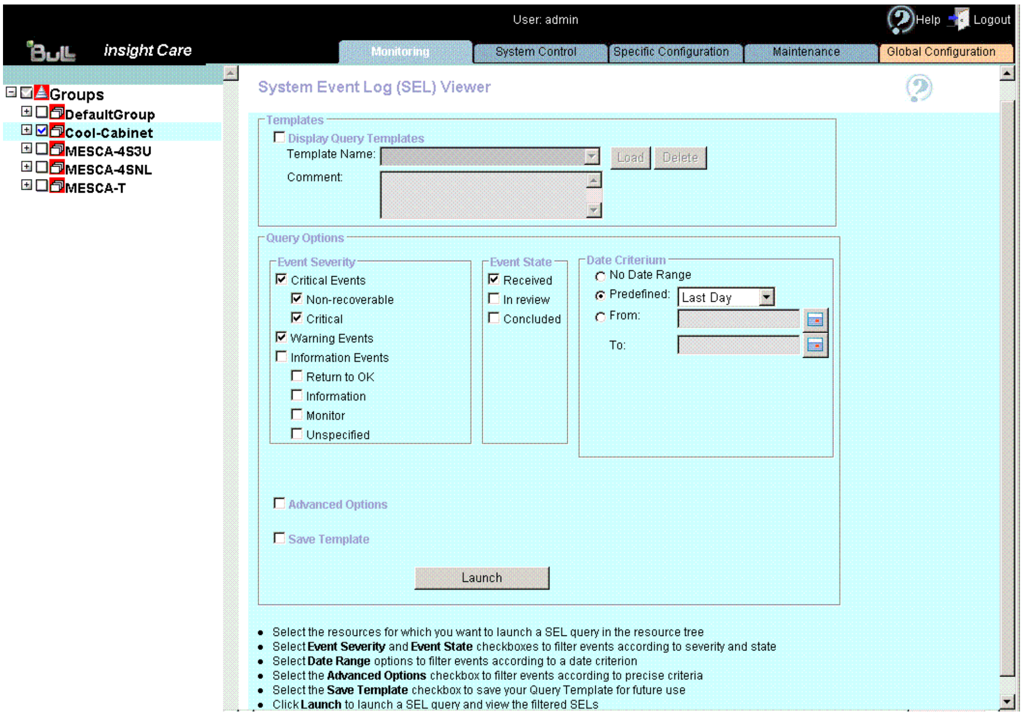
- System Event Logs (SEL) are also collected when an Action Request Package is created to troubleshoot hardware resources. See Creating an Action Request Package, on page 5-20.
- Each resource records IPMI-compliant events in its System Event Log (SEL) and non-IPMI-compliant information in its Board & 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.

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.



- ☑ Groups
  - □ DefaultGroup
  - ☑ Cool-Cabinet
  - □ MESCA-4S3U
  - □ MESCA-4SNL
  - □ MESCA-T

System Event Log (SEL) Viewer

Templates
□ Display Query Templates
Template Name:
Load Delete
Comment:

Query Options

Event Severity
☑ Critical Events
☑ Non-recoverable
☑ Critical
☑ Warning Events
□ Information Events
□ Return to OK
□ Information
□ Monitor
□ Unspecified

Event State
☑ Received
□ In review
□ Concluded

Date Criterium
○ No Date Range
● Predefined: Last Day
○ From:
To:

□ Advanced Options

□ Save Template

Launch

- Select the resources for which you want to launch a SEL query in the resource tree
- Select **Event Severity** and **Event State** checkboxes to filter events according to severity and state
- Select **Date Range** options to filter events according to a date criterion
- Select the **Advanced Options** checkbox to filter events according to precise criteria
- Select the **Save Template** checkbox to save your Query Template for future use
- Click **Launch** to launch a SEL query and view the filtered SELs

Figure 4-1. System Event Log (SEL) Viewer page

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

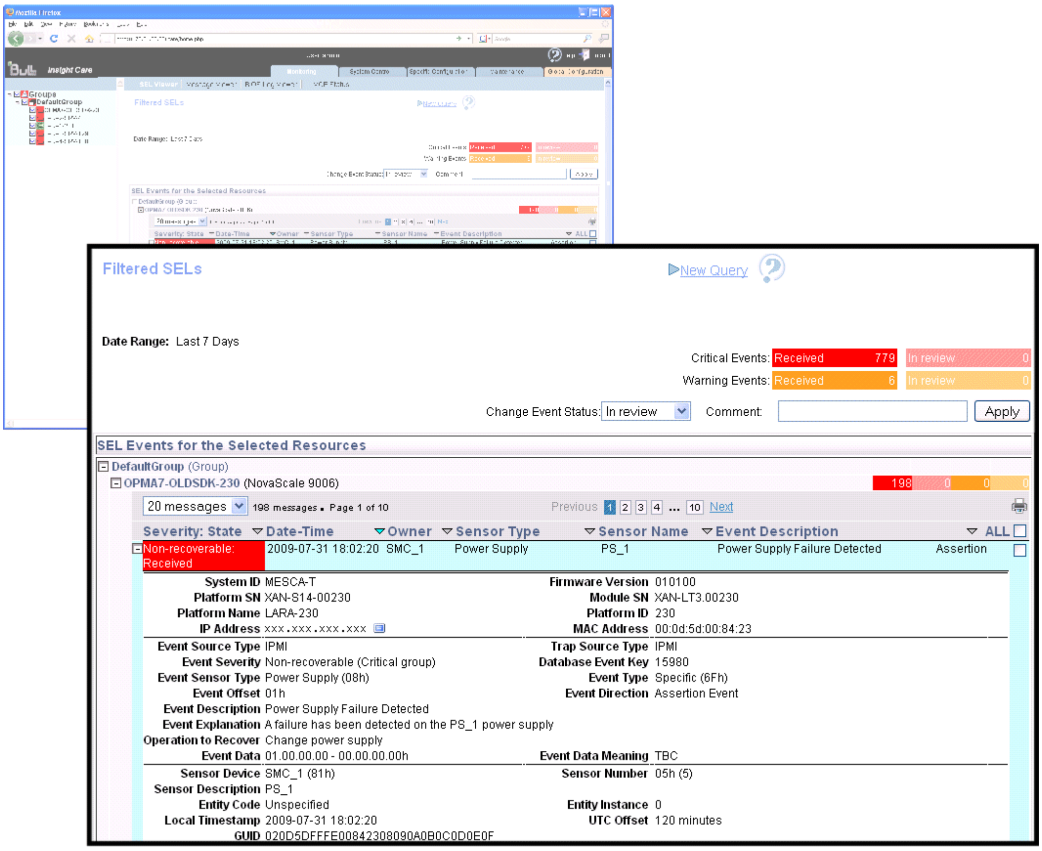
System Event Log (SEL) Viewer Template and Query Options			
a	Optional	**Templates: Load**	• Select the **Display Query Templates** check box. • From the **Template Name** drop-down list, select the required template and click **Load**. Template parameters are displayed. • Proceed to Step 4.
		Templates: 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 Criterium**	Select the **Date Criterium** appropriate fields to filter, or not filter, events according to a specific date or a 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 4-1. 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 4-7.



Filtered SELs

Date Range: Last 7 Days

Critical Events: Received 779 In review 0

Warning Events: Received 6 In review 0

Change Event Status: In review Comment:

SEL Events for the Selected Resources

DefaultGroup (Group)

OPMA7-OLDSDK-230 (NovaScale 9006) 198 0 0 0

20 messages 198 messages . Page 1 of 10 Previous 1 2 3 4 ... 10 Next

Severity: State	Date-Time	Owner	Sensor Type	Sensor Name	Event Description		ALL □
Non-recoverable: Received	2009-07-31 18:02:20	SMC_1	Power Supply	PS_1	Power Supply Failure Detected	Assertion	□

System ID	MESCA-T	**Firmware Version**	010100
Platform SN	XAN-S14-00230	**Module SN**	XAN-LT3.00230
Platform Name	LARA-230	**Platform ID**	230
IP Address	xxx.xxx.xxx.xxx	**MAC Address**	00:0d:5d:00:84:23
Event Source Type	IPMI	**Trap Source Type**	IPMI
Event Severity	Non-recoverable (Critical group)	**Database Event Key**	15980
Event Sensor Type	Power Supply (08h)	**Event Type**	Specific (6Fh)
Event Offset	01h	**Event Direction**	Assertion Event
Event Description	Power Supply Failure Detected		
Event Explanation	A failure has been detected on the PS_1 power supply		
Operation to Recover	Change power supply		
Event Data	01.00.00.00 - 00.00.00.00h	**Event Data Meaning**	TBC
Sensor Device	SMC_1 (81h)	**Sensor Number**	05h (5)
Sensor Description	PS_1		
Entity Code	Unspecified	**Entity Instance**	0
Local Timestamp	2009-07-31 18:02:20	**UTC Offset**	120 minutes
GUID	020D5DFFFE00842308090A0B0C0D0E0F		

Figure 4-2. Filtered SELs page

4.2. 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.

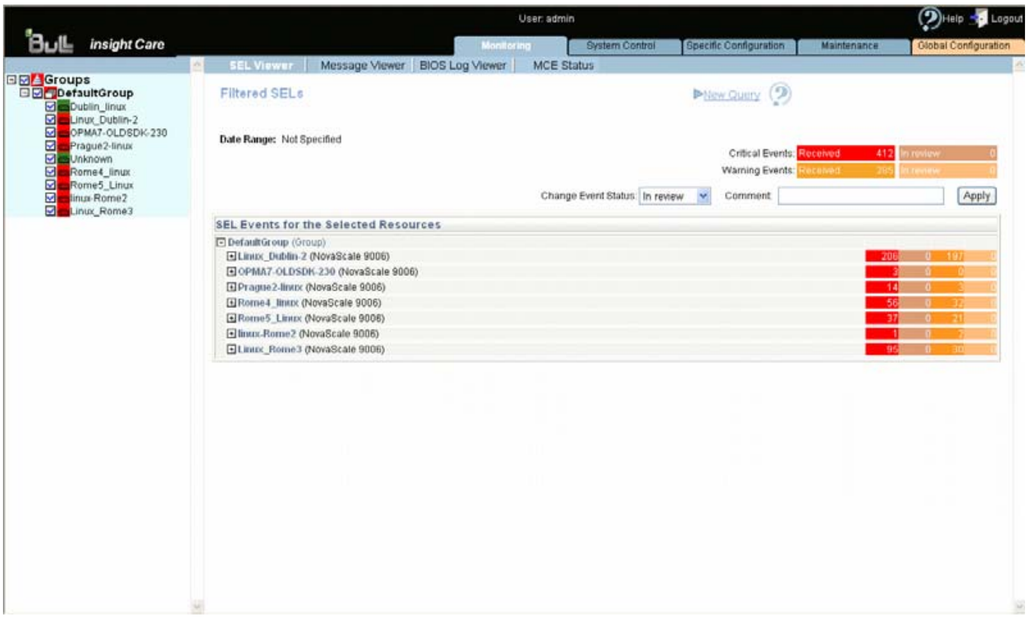
You can query the database to view events to help you analyze hardware failure or perform preventive maintenance.

Prerequisites

None

Procedure

1. Launch a SEL query as explained in Building and Checking System Event Logs (SEL), on page 4-2.
   By default, the **Filtered SELs** page lists the SEL events for the selected resources, within the specified date range (where applicable).



Filtered SELs

Date Range: Not Specified

Critical Events: Received 412 In review 0
Warning Events: Received 285 In review 0

Change Event Status: In review
Comment:

SEL Events for the Selected Resources

DefaultGroup (Group)

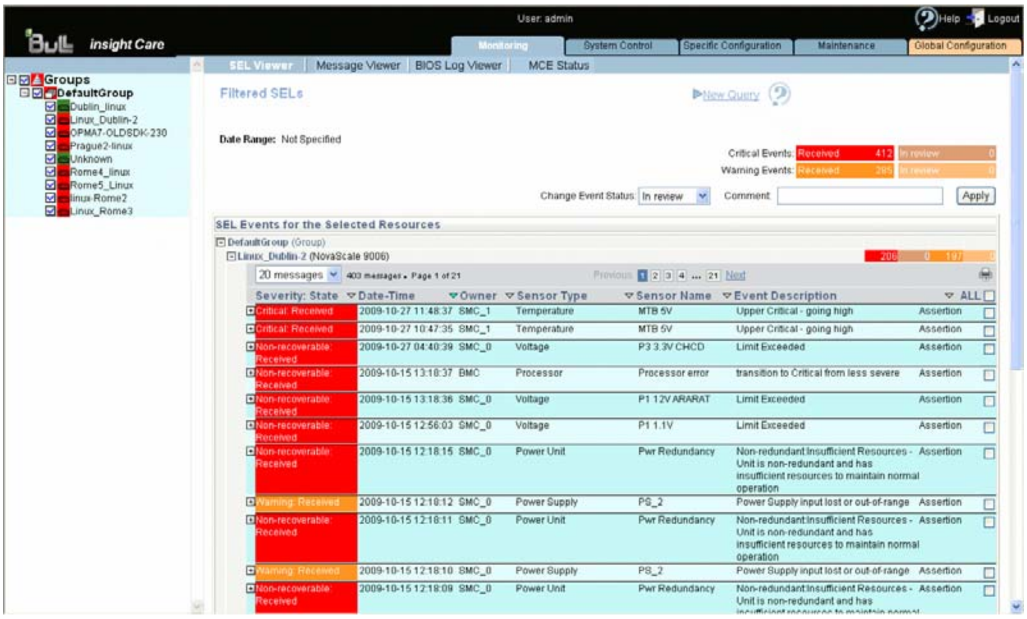
Linux_Dublin-2 (NovaScale 9006)	206	0	197	0
OPMA7-OLDSDK-230 (NovaScale 9006)	3	0	0	0
Prague2-linux (NovaScale 9006)	14	0	3	0
Rome4_linux (NovaScale 9006)	56	0	32	0
Rome5_Linux (NovaScale 9006)	37	0	21	0
linux-Rome2 (NovaScale 9006)	1	0	7	0
Linux_Rome3 (NovaScale 9006)	95	0	30	0

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 4-3. Filtered SELs page

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



Filtered SELs

Date Range: Not Specified

Critical Events: Received 412 In review 0

Warning Events: Received 285 In review 0

Change Event Status: In review

Comment:

SEL Events for the Selected Resources

DefaultGroup (Group)

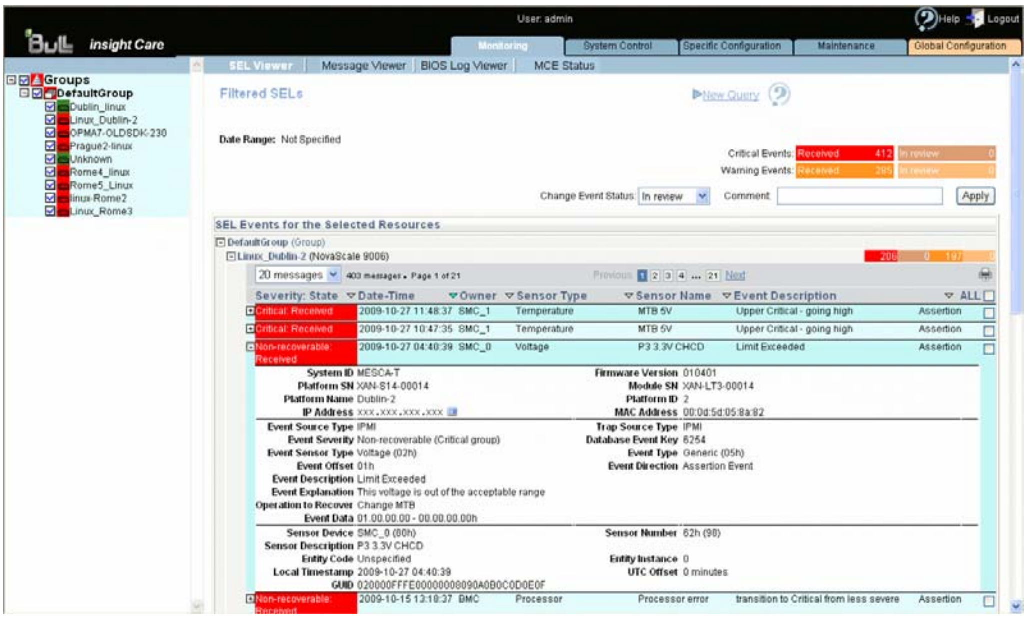
Linux_Dublin-2 (NovaScale 9006) 206 0 197 0

20 messages 403 messages • Page 1 of 21 Previous 1 2 3 4 ... 21 Next

Severity: State	Date-Time	Owner	Sensor Type	Sensor Name	Event Description		ALL ☐
Critical: Received	2009-10-27 11:48:37	SMC_1	Temperature	MTB 5V	Upper Critical - going high	Assertion	☐
Critical: Received	2009-10-27 10:47:35	SMC_1	Temperature	MTB 5V	Upper Critical - going high	Assertion	☐
Non-recoverable: Received	2009-10-27 04:40:39	SMC_0	Voltage	P3 3.3V CHCD	Limit Exceeded	Assertion	☐
Non-recoverable: Received	2009-10-15 13:18:37	BMC	Processor	Processor error	transition to Critical from less severe	Assertion	☐
Non-recoverable: Received	2009-10-15 13:18:36	SMC_0	Voltage	P1 12V ARARAT	Limit Exceeded	Assertion	☐
Non-recoverable: Received	2009-10-15 12:56:03	SMC_0	Voltage	P1 1.1V	Limit Exceeded	Assertion	☐
Non-recoverable: Received	2009-10-15 12:18:15	SMC_0	Power Unit	Pwr Redundancy	Non-redundant:Insufficient Resources - Unit is non-redundant and has insufficient resources to maintain normal operation	Assertion	☐
Warning: Received	2009-10-15 12:18:12	SMC_0	Power Supply	PS_2	Power Supply input lost or out-of-range	Assertion	☐
Non-recoverable: Received	2009-10-15 12:18:11	SMC_0	Power Unit	Pwr Redundancy	Non-redundant:Insufficient Resources - Unit is non-redundant and has insufficient resources to maintain normal operation	Assertion	☐
Warning: Received	2009-10-15 12:18:10	SMC_0	Power Supply	PS_2	Power Supply input lost or out-of-range	Assertion	☐
Non-recoverable: Received	2009-10-15 12:18:09	SMC_0	Power Unit	Pwr Redundancy	Non-redundant:Insufficient Resources - Unit is non-redundant and has	Assertion	☐

Figure 4-4. Filtered SELs page - SEL Event List

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



Filtered SELs

Date Range: Not Specified

Critical Events: Received 412 In review 0

Warning Events: Received 285 In review 0

Change Event Status: In review Comment:

SEL Events for the Selected Resources

DefaultGroup (Group)

Linux_Dublin-2 (NovaScale 9006) 206 0 197 0

20 messages 403 messages • Page 1 of 21

Severity: State	Date-Time	Owner	Sensor Type	Sensor Name	Event Description		ALL □
Critical: Received	2009-10-27 11:48:37	SMC_1	Temperature	MTB 5V	Upper Critical - going high	Assertion	□
Critical: Received	2009-10-27 10:47:35	SMC_1	Temperature	MTB 5V	Upper Critical - going high	Assertion	□
Non-recoverable: Received	2009-10-27 04:40:39	SMC_0	Voltage	P3 3.3V CHCD	Limit Exceeded	Assertion	□

System ID MESCA-T
Platform SN XAN-S14-00014
Platform Name Dublin-2
IP Address xxx.xxx.xxx.xxx
Firmware Version 010401
Module SN XAN-LT3-00014
Platform ID 2
MAC Address 00:0d:5d:05:8a:82

Event Source Type IPMI
Event Severity Non-recoverable (Critical group)
Event Sensor Type Voltage (02h)
Event Offset 01h
Event Description Limit Exceeded
Event Explanation This voltage is out of the acceptable range
Operation to Recover Change MTB
Event Data 01.00.00.00 - 00.00.00.00h
Trap Source Type IPMI
Database Event Key 6254
Event Type Generic (05h)
Event Direction Assertion Event

Sensor Device SMC_0 (80h)
Sensor Description P3 3.3V CHCD
Entity Code Unspecified
Local Timestamp 2009-10-27 04:40:39
GUID 020000FFFE00000008090A0B0C0D0E0F
Sensor Number 62h (98)
Entity Instance 0
UTC Offset 0 minutes

Severity: State	Date-Time	Owner	Sensor Type	Sensor Name	Event Description		ALL □
Non-recoverable: Received	2009-10-15 13:18:37	BMC	Processor	Processor error	transition to Critical from less severe	Assertion	□

Figure 4-5. 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**.

4.3. 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.

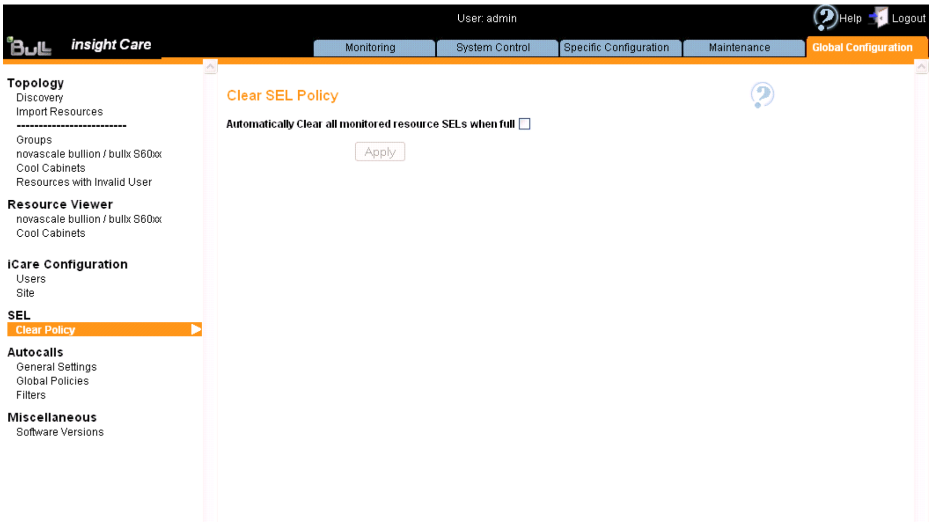
Note Even if the SEL limit is reached, events are still recorded in the iCare Console event database.

Prerequisites

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

Procedure

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



Clear SEL Policy

Automatically Clear all monitored resource SELs when full □

Figure 4-6. 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**.

4.4. Building and Checking Board and Security Message Logs

Each hardware resource in the Resource tree records events. These events could be 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 5-20.

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.

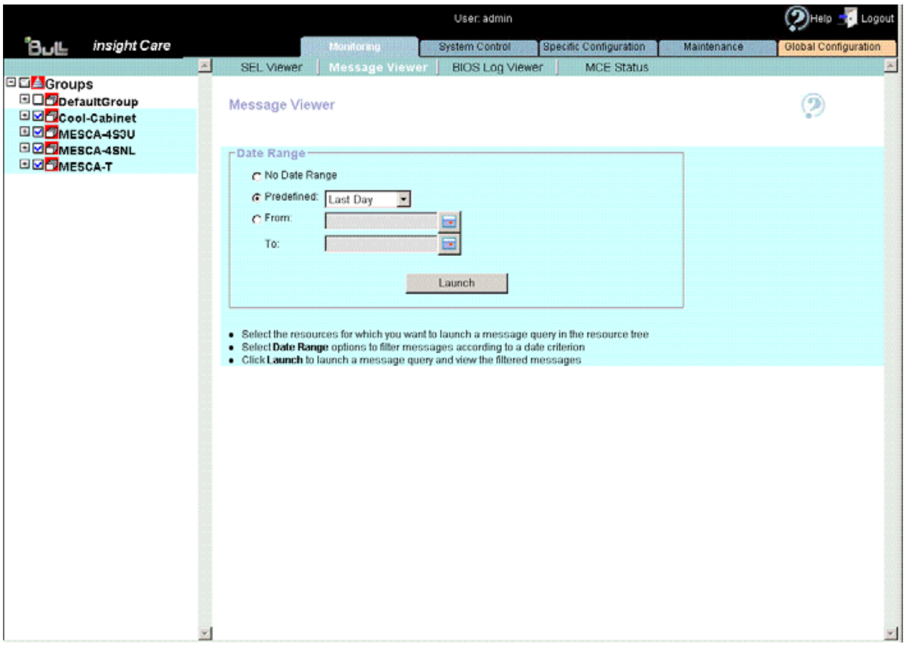
Prerequisites

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.

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.



Message Viewer

Date Range

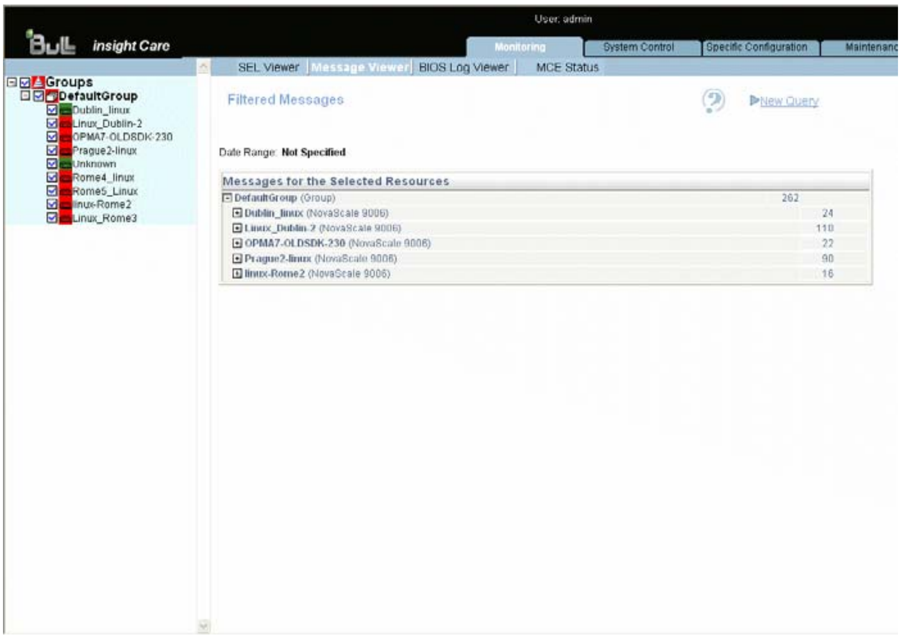
○ No Date Range
● Predefined: Last Day
○ From:
To:

- Select the resources for which you want to launch a message query in the resource tree
- Select **Date Range** options to filter messages according to a date criterion
- Click **Launch** to launch a message query and view the filtered messages

Figure 4-7. 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 4-13.



Filtered Messages

Date Range: **Not Specified**

Messages for the Selected Resources	
⊟ **DefaultGroup** (Group)	262
⊞ **Dublin_linux** (NovaScale 9006)	24
⊞ **Linux_Dublin-2** (NovaScale 9006)	110
⊞ **OPMA7-OLDSDK-230** (NovaScale 9006)	22
⊞ **Prague2-linux** (NovaScale 9006)	90
⊞ **linux-Rome2** (NovaScale 9006)	16

Figure 4-8. Filtered Messages page - Default display

4.5. 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

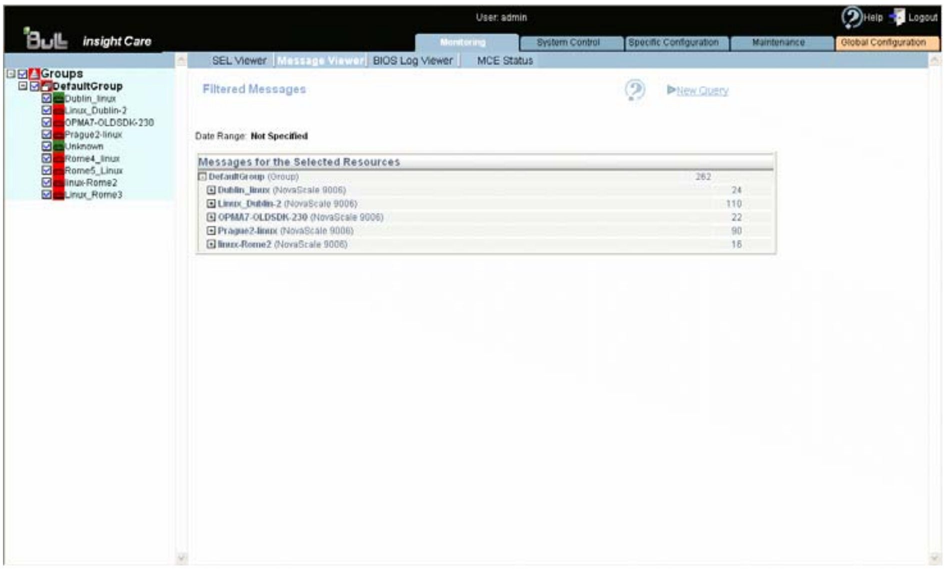
The hardware resources requiring attention are present in the Resource tree.

The same **super** user password has been set up on all monitored resources and in the iCare Console, as detailed in Changing a User Account Password, on page 3-4.

Procedure

1. Launch a Message query as explained in Building and Checking Board and Security Message Logs, on page 4-11.

   The **Filtered Messages** page lists all the Messages for the selected resources within the specified date range (where applicable).



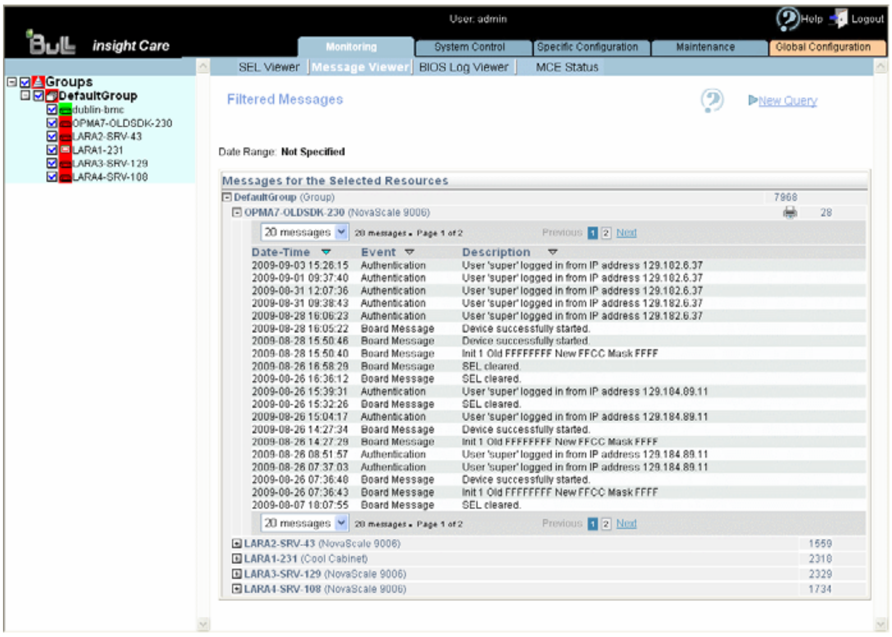
Filtered Messages

Date Range: **Not Specified**

Messages for the Selected Resources	
DefaultGroup (Group)	262
Dublin_linux (NovaScale 9006)	24
Linux_Dublin-2 (NovaScale 9006)	110
OPMA7-OLDSDK-230 (NovaScale 9006)	22
Prague2-linux (NovaScale 9006)	90
linux-Rome2 (NovaScale 9006)	16

Figure 4-9. Filtered Message List

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



Filtered Messages

Date Range: **Not Specified**

Messages for the Selected Resources

DefaultGroup (Group)	7968
OPMA7-OLDSDK-230 (NovaScale 9006)	28

20 messages • Page 1 of 2

Date-Time	Event	Description
2009-09-03 15:26:15	Authentication	User 'super' logged in from IP address 129.182.6.37
2009-09-01 09:37:40	Authentication	User 'super' logged in from IP address 129.182.6.37
2009-08-31 12:07:36	Authentication	User 'super' logged in from IP address 129.182.6.37
2009-08-31 09:38:43	Authentication	User 'super' logged in from IP address 129.182.6.37
2009-08-28 16:06:23	Authentication	User 'super' logged in from IP address 129.182.6.37
2009-08-28 16:05:22	Board Message	Device successfully started.
2009-08-28 15:50:46	Board Message	Device successfully started.
2009-08-28 15:50:40	Board Message	Init 1 Old FFFFFFFF New FFCC Mask FFFF
2009-08-26 16:58:29	Board Message	SEL cleared.
2009-08-26 16:36:12	Board Message	SEL cleared.
2009-08-26 15:39:31	Authentication	User 'super' logged in from IP address 129.184.89.11
2009-08-26 15:32:26	Board Message	SEL cleared.
2009-08-26 15:04:17	Authentication	User 'super' logged in from IP address 129.184.89.11
2009-08-26 14:27:34	Board Message	Device successfully started.
2009-08-26 14:27:29	Board Message	Init 1 Old FFFFFFFF New FFCC Mask FFFF
2009-08-26 08:51:57	Authentication	User 'super' logged in from IP address 129.184.89.11
2009-08-26 07:37:03	Authentication	User 'super' logged in from IP address 129.184.89.11
2009-08-26 07:36:48	Board Message	Device successfully started.
2009-08-26 07:36:43	Board Message	Init 1 Old FFFFFFFF New FFCC Mask FFFF
2009-08-07 18:07:55	Board Message	SEL cleared.

20 messages • Page 1 of 2

LARA2-SRV-43 (NovaScale 9006)	1559
LARA1-231 (Cool Cabinet)	2318
LARA3-SRV-129 (NovaScale 9006)	2329
LARA4-SRV-108 (NovaScale 9006)	1734

Figure 4-10. Filtered Messages - Details

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

4.6. Building and Checking BIOS Logs

Each 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 collected when the hardware resource is enabled. See Enabling/Disabling Resource Monitoring, on page 2-31
BIOS logs are also collected when an Action Request Package is created to troubleshoot hardware resources. See Creating an Action Request Package, on page 5-20.
BIOS logs recorded when the hardware resource was monitored remain in the iCare Console database.

Introduction

In case of UNCORRECTABLE ERRORS or FATAL ERRORS detected by the processor of the resource, the BIOS logs all the registers containing CORRECTABLE ERRORS, UNCORRECTABLE ERRORS or FATAL ERRORS. The BIOS log is a binary file. It can be download (See Downloading BIOS Logs, on page 4-18). You can read it very easily with the viewing action (See Viewing BIOS Logs, on page 4-17).

Prerequisites

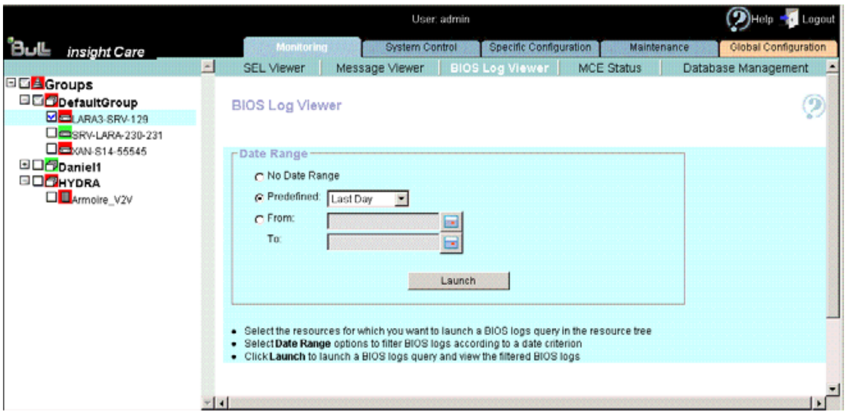
The hardware resources requiring attention are present in the Resource tree

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.



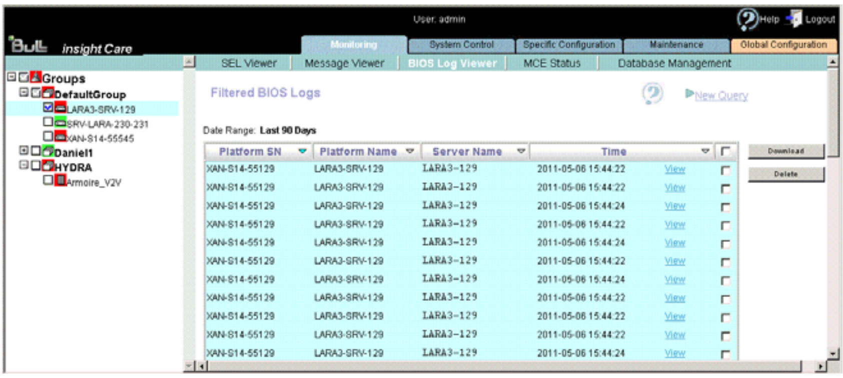
○ No Date Range
● Predefined: Last Day
○ From:
To:

- Select the resources for which you want to launch a BIOS logs query in the resource tree
- Select **Date Range** options to filter BIOS logs according to a date criterion
- Click **Launch** to launch a BIOS logs query and view the filtered BIOS logs

Figure 4-11. 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 4-17.



Filtered BIOS Logs

Date Range: **Last 90 Days**

Platform SN	Platform Name	Server Name	Time		□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:24	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:24	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:24	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:24	View	□

Figure 4-12. Filtered BIOS Logs page

4.7. Managing BIOS Logs

Once you have obtained the list of BIOS logs, you can select log files for downloading and/or deletion. The BIOS logs file is a binary file. It can be read very easily with the viewing action.

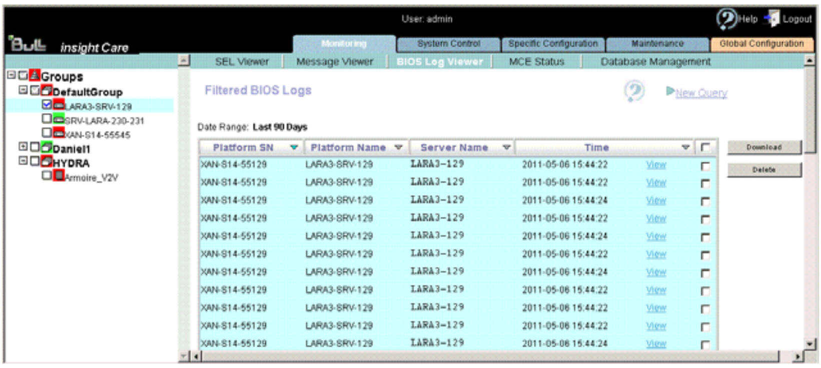
Prerequisites

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

4.7.1. Viewing BIOS Logs

Procedure

1. Launch a BIOS query as explained in Building and Checking BIOS Logs, on page 4-15. The **Filtered BIOS Logs** page lists all the BIOS log for the selected resources within the specified date range (where applicable).



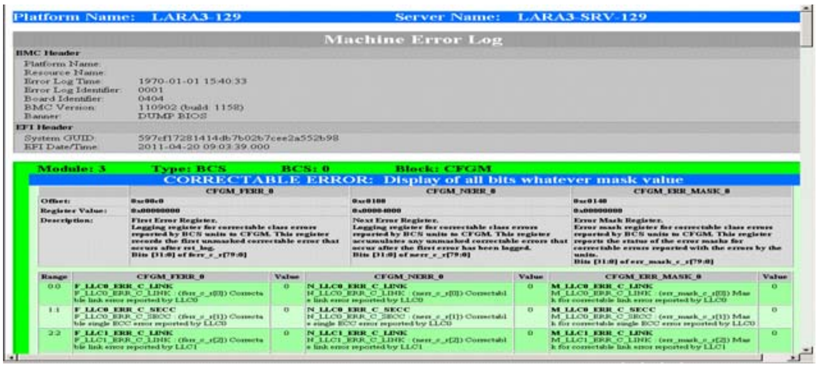
Filtered BIOS Logs

Date Range: **Last 90 Days**

Platform SN	Platform Name	Server Name	Time		□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:24	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:24	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:24	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:24	View	□

Figure 4-13. Filtered BIOS Logs - Viewing

2. Click **View** corresponding to the resource BIOS logs you want to read.



Platform Name: LARA3-129 Server Name: LARA3-SRV-129

Machine Error Log

BMC Header

```
Platform Name:
Resource Name:
Error Log Time:        1970-01-01 15:40:33
Error Log Identifier:  0001
Board Identifier:      0404
BMC Version:           110902 (build 1158)
Banner:                DUMP BIOS
```

EFI Header

```
System GUID:    597cf17281414db7b02b7cee2a552b98
EFI Date/Time:  2011-04-20 09:03:39.000
```

Module: 3 Type: BCS BCS: 0 Block: CFGM

CORRECTABLE ERROR: Display of all bits whatever mask value

	CFGM_FERR_0	CFGM_NERR_0	CFGM_ERR_MASK_0
Offset:	0x00c0	0x0100	0x0140
Register Value:	0x00000000	0x00004000	0x00000000
Description:	First Error Register. Logging register for correctable class errors reported by BCS units to CFGM. This register records the first unmasked correctable error that occurs after rst_log. Bits [31:0] of ferr_c_r[79:0]	Next Error Register. Logging register for correctable class errors reported by BCS units to CFGM. This register accumulates any unmasked correctable errors that occur after the first error has been logged. Bits [31:0] of nerr_c_r[79:0]	Error Mask Register. Error mask register for correctable class errors reported by BCS units to CFGM. This register reports the status of the error masks for correctable errors reported with the errors by the units. Bits [31:0] of err_mask_c_r[79:0]

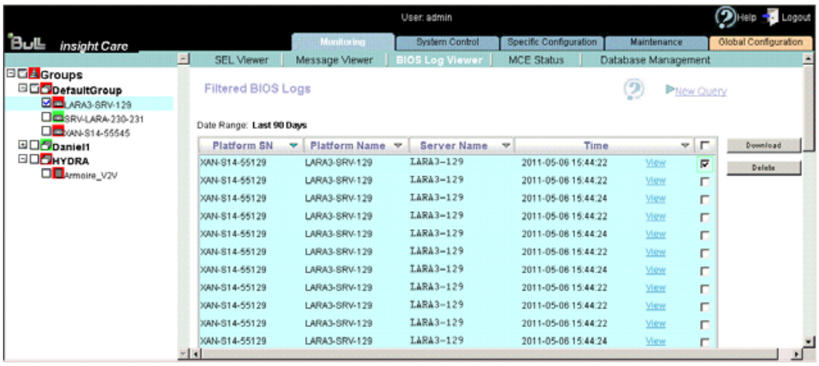
Range	CFGM_FERR_0	Value	CFGM_NERR_0	Value	CFGM_ERR_MASK_0	Value
0:0	F_LLC0_ERR_C_LINK F_LLC0_ERR_C_LINK : (ferr_c_r[0]) Correctable link error reported by LLC0	0	N_LLC0_ERR_C_LINK N_LLC0_ERR_C_LINK : (nerr_c_r[0]) Correctable link error reported by LLC0	0	M_LLC0_ERR_C_LINK M_LLC0_ERR_C_LINK : (err_mask_c_r[0]) Mask for correctable link error reported by LLC0	0
1:1	F_LLC0_ERR_C_SECC F_LLC0_ERR_C_SECC : (ferr_c_r[1]) Correctable single ECC error reported by LLC0	0	N_LLC0_ERR_C_SECC N_LLC0_ERR_C_SECC : (nerr_c_r[1]) Correctable single ECC error reported by LLC0	0	M_LLC0_ERR_C_SECC M_LLC0_ERR_C_SECC : (err_mask_c_r[1]) Mask for correctable single ECC error reported by LLC0	0
2:2	F_LLC1_ERR_C_LINK F_LLC1_ERR_C_LINK : (ferr_c_r[2]) Correctable link error reported by LLC1	0	N_LLC1_ERR_C_LINK N_LLC1_ERR_C_LINK : (nerr_c_r[2]) Correctable link error reported by LLC1	0	M_LLC1_ERR_C_LINK M_LLC1_ERR_C_LINK : (err_mask_c_r[2]) Mask for correctable link error reported by LLC1	0

Figure 4-14. Filtered BIOS Logs - View

4.7.2. Downloading BIOS Logs

Procedure

1. Launch a BIOS query as explained in Building and Checking BIOS Logs, on page 4-15. The **Filtered BIOS Logs** page lists all the BIOS log files for the selected resources within the specified date range (where applicable).



Filtered BIOS Logs

Date Range: **Last 90 Days**

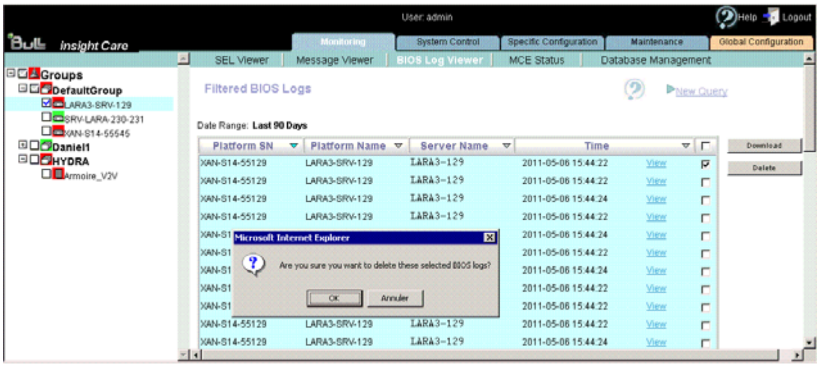
Platform SN	Platform Name	Server Name	Time		□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	☑
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:24	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:24	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:24	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:24	View	□

Figure 4-15. 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.

4.7.3. Deleting BIOS Logs

1. Launch a BIOS query as explained in Building and Checking BIOS Logs, on page 4-15. The **Filtered BIOS Logs** page lists all the BIOS log files for the selected resources within the specified date range (where applicable).



Filtered BIOS Logs

Date Range: **Last 90 Days**

Platform SN	Platform Name	Server Name	Time		□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	☑
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:24	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S1			2011-05-06 15:44:24	View	□
XAN-S1			2011-05-06 15:44:22	View	□
XAN-S1			2011-05-06 15:44:24	View	□
XAN-S1			2011-05-06 15:44:22	View	□
XAN-S1			2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:22	View	□
XAN-S14-55129	LARA3-SRV-129	LARA3-129	2011-05-06 15:44:24	View	□

Are you sure you want to delete these selected BIOS logs?

Figure 4-16. 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.

Note BIOS logs are deleted from the iCare Console database when the resource is deleted. See Deleting a Resource Custom Group, on page 2-28

4.8. Building and Checking MCE Status Logs

bullx servers and novascale bullion servers running Linux Fedora Core 12 (or later) can be configured to send Memory Machine Check Error (MCE) logs to the iCare Console database.

You can query the database to directly view correctable memory error status. The result is displayed in the form of a table, indicating the number of correctable error events recorded for each DIMM.

To help you correct identified errors, you can consult the SEL log for details, as explained below.

Note This feature requires the installation of the *mce-icare tool* on the monitored server. Please refer to the associated documentation available on the *Resource and Documentation CD* for installation and configuration details.

Prerequisites

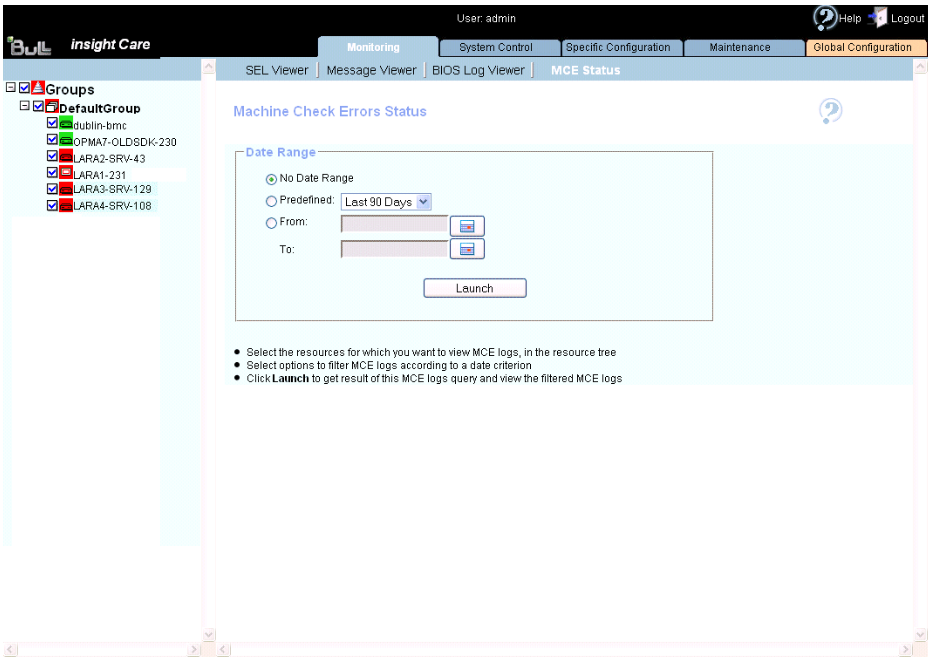
The servers requiring attention are in the Resource tree

Linux Fedora Core 12 (or later) is the Operating System

The *mce-icare tool* is installed

Procedure

1. From the **Monitoring** tab, click **MCE Status** to open the **Machine Check Error Status** page.
2. From the **Resource** tree, select the resource(s) for which you want to query the database.



Machine Check Errors Status

Date Range

● No Date Range

○ Predefined: Last 90 Days

○ From:

To:

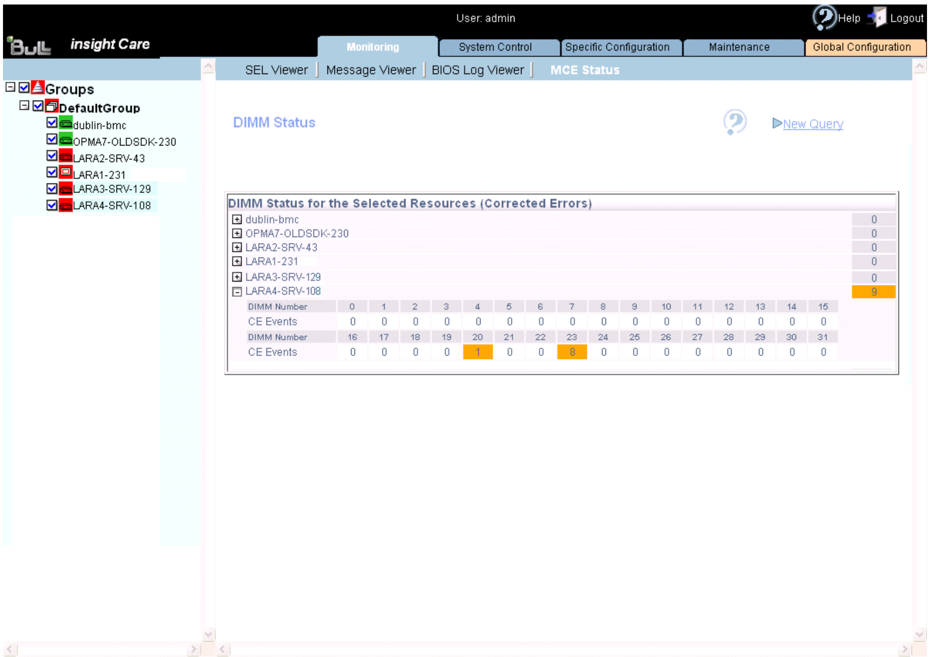
- Select the resources for which you want to view MCE logs, in the resource tree
- Select options to filter MCE logs according to a date criterion
- Click **Launch** to get result of this MCE logs query and view the filtered MCE logs

Figure 4-17. Machine Check Error Status page

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

4. Click **Launch**. The **DIMM Status** page appears.

   This page displays the number of corrected DIMM errors recorded on each DIMM for the selected resource.



DIMM Status

DIMM Status for the Selected Resources (Corrected Errors)

⊞ dublin-bmc	0
⊞ OPMA7-OLDSDK-230	0
⊞ LARA2-SRV-43	0
⊞ LARA1-231	0
⊞ LARA3-SRV-129	0
⊟ LARA4-SRV-108	9

DIMM Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CE Events	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
DIMM Number	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
CE Events	0	0	0	0	1	0	0	8	0	0	0	0	0	0	0	0

Figure 4-18. DIMM Status page

By default, the *mce-icare tool* is configured to trigger and to send an event:

- on the 10th corrected memory error within a 5 minute period
- at 5- minute intervals (to avoid corrected error bursts)

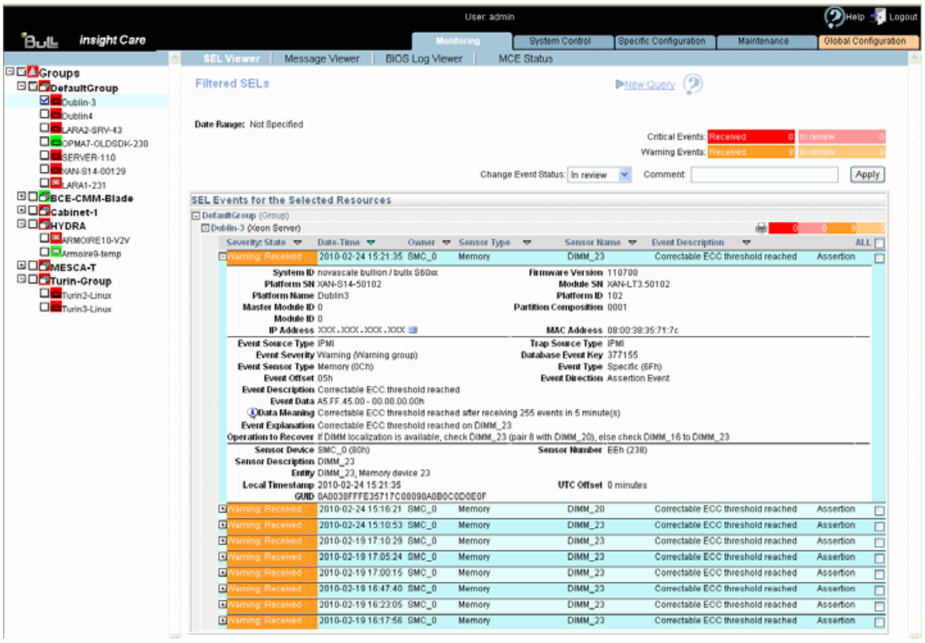
Each event indicates that the configured memory error threshold has been exceeded. These settings can be changed to suit your needs. Please refer to the associated documentation available on the *Resource and Documentation CD* for details.

5. If one or more DIMMs are faulty, you can consult the SEL log for details, by selecting **SEL Viewer** to open the **System Event Log (SEL) Viewer** page.

6. Query the database using the following **Advanced Options**:

   - 1. Choose an Attribute or Relationship: **Sensor Type**
   - 2. Choose Operator : **Equals**
   - 3. Choose and element in the list below : **Memory**

The **Filtered SELs** page is displayed, allowing you to manage and/or print to PDF the event list and detailed information. For more details, refer to Managing System Event Logs (SEL), on page 4-7.



Filtered SELs

Date Range: Not Specified

Critical Events: Received 0 In review 0
Warning Events: Received 9 In review 0

Change Event Status: In review Comment: Apply

SEL Events for the Selected Resources

DefaultGroup (Group)

Dublin-3 (Xeon Server) 0 0 9 0

Severity: State	Date-Time	Owner	Sensor Type	Sensor Name	Event Description		ALL ☐
Warning: Received	2010-02-24 15:21:35	SMC_0	Memory	DIMM_23	Correctable ECC threshold reached	Assertion	☐

System ID novascale bullion / bullx S60xx
Platform SN XAN-S14-50102
Platform Name Dublin3
Master Module ID 0
Module ID 0
IP Address XXX.XXX.XXX.XXX
Firmware Version 110700
Module SN XAN-LT3.50102
Platform ID 102
Partition Composition 0001
MAC Address 08:00:38:35:71:7c

Event Source Type IPMI
Event Severity Warning (Warning group)
Event Sensor Type Memory (0Ch)
Event Offset 05h
Event Description Correctable ECC threshold reached
Event Data A5.FF.45.00 - 00.00.00.00h
Data Meaning Correctable ECC threshold reached after receiving 255 events in 5 minute(s)
Event Explanation Correctable ECC threshold reached on DIMM_23
Operation to Recover If DIMM localization is available, check DIMM_23 (pair 8 with DIMM_20), else check DIMM_16 to DIMM_23
Trap Source Type IPMI
Database Event Key 377155
Event Type Specific (6Fh)
Event Direction Assertion Event

Sensor Device SMC_0 (80h)
Sensor Description DIMM_23
Entity DIMM_23, Memory device 23
Local Timestamp 2010-02-24 15:21:35
GUID 0A0030FFFE35717C08090A0B0C0D0E0F
Sensor Number EEh (238)
UTC Offset 0 minutes

Severity: State	Date-Time	Owner	Sensor Type	Sensor Name	Event Description		ALL ☐
Warning: Received	2010-02-24 15:16:21	SMC_0	Memory	DIMM_20	Correctable ECC threshold reached	Assertion	☐
Warning: Received	2010-02-24 15:10:53	SMC_0	Memory	DIMM_23	Correctable ECC threshold reached	Assertion	☐
Warning: Received	2010-02-19 17:10:29	SMC_0	Memory	DIMM_23	Correctable ECC threshold reached	Assertion	☐
Warning: Received	2010-02-19 17:05:24	SMC_0	Memory	DIMM_23	Correctable ECC threshold reached	Assertion	☐
Warning: Received	2010-02-19 17:00:15	SMC_0	Memory	DIMM_23	Correctable ECC threshold reached	Assertion	☐
Warning: Received	2010-02-19 16:47:40	SMC_0	Memory	DIMM_23	Correctable ECC threshold reached	Assertion	☐
Warning: Received	2010-02-19 16:23:05	SMC_0	Memory	DIMM_23	Correctable ECC threshold reached	Assertion	☐
Warning: Received	2010-02-19 16:17:56	SMC_0	Memory	DIMM_23	Correctable ECC threshold reached	Assertion	☐

Figure 4-19. Filtered SELs - Memory Events

Important According to the server's BIOS version, the DIMM localization feature may be restricted. In this case, please understand that errors from:

- **DIMM [0-7] are attributed to DIMM 7**
- **DIMM [8-15] are attributed to DIMM 15**
- **DIMM [16-23] are attributed to DIMM 23**
- **DIMM [24-31] are attributed to DIMM 31**

Please contact your Customer Service Representative for further information.

4.9. Managing Database

The events, messages or BIOS logs are recorded in the iCare Console database. You can clean the database, save it and restore it.

The following tasks are explained in this section:

- Deleting Logs , on page 4-22: you can purge the useless logs from iCare Console database: clean the specified logs for a selected resource.
- Saving Restoring Database, on page 4-23: you can backup the whole iCare Console database, for all the resources. The data are stored in a file that you could restore later.

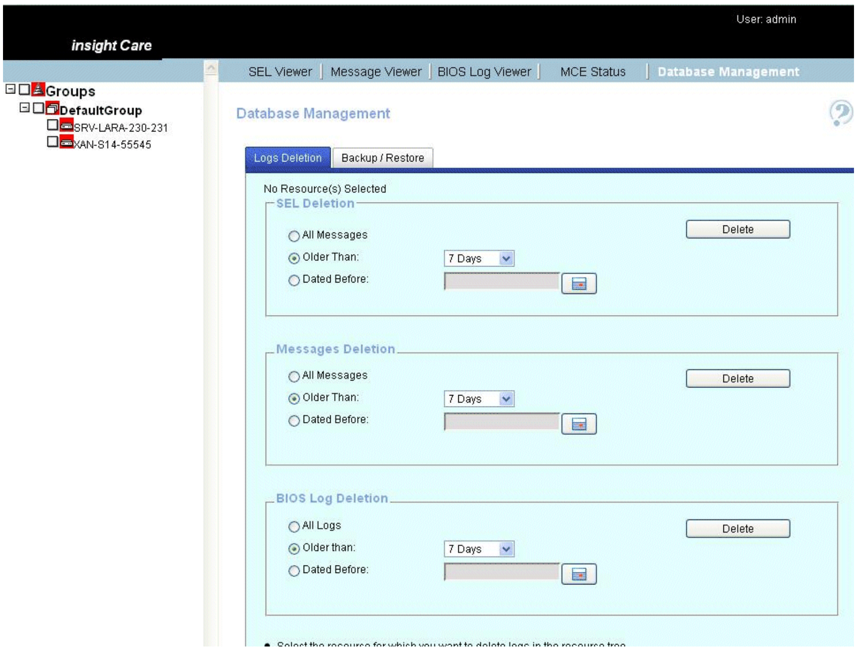
Note The **Delete** action is applied for a specified resource and a specified log.

The **Backup** and the **Restore** actions are applied to the whole iCare Console database.

4.9.1. Deleting Logs

Procedure

1. From the **Monitoring** tab, click **Database Management** to open the **Database Management Logs Deletion** page.
2. From the **Resource** tree, select the resource(s) for which you want to clean some logs.
3. Complete the data range to filter the specific older logs to delete.
4. Click **Detele**.



No Resource(s) Selected

SEL Deletion

○ All Messages
● Older Than: 7 Days
○ Dated Before:

Delete

Messages Deletion

○ All Messages
● Older Than: 7 Days
○ Dated Before:

Delete

BIOS Log Deletion

○ All Logs
● Older than: 7 Days
○ Dated Before:

Delete

- Select the resource for which you want to delete logs in the resource tree

Figure 4-20. Database Deleting Logs page

Important **The Delete action is definitive: the deleted logs could not be restored.**

4.9.2. Saving Restoring Database

Procedure

1. From the **Monitoring** tab, click **Database Management** to open the **Database Management Backup/Restore** page.
2. Click **Backup** to save the whole iCare Console database.
3. Or select the backup file and click **Restore** to restore the whole iCare Console database.

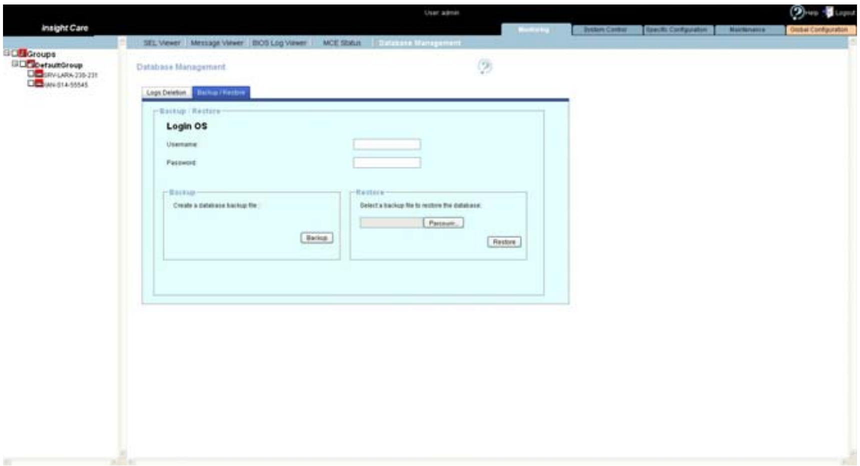


Figure 4-21. Database Backup Restore page

Important **The Restore action is comprehensive: the active database will be entirely replaced with the saved one.**

Chapter 5. Managing Servicing Information

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:

- Completing the Site Form, on page 5-2
- Configuring Autocalls, on page 5-3
- Managing Autocalls, on page 5-4
- Selecting Global Autocall Policies, on page 5-7
- Selecting Specific Autocall Policies, on page 5-9
- Configuring Autocall Filters, on page 5-11
- Creating an Intervention Report, on page 5-18
- Viewing the List of Intervention Reports, on page 5-19
- Creating an Action Request Package, on page 5-20

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.

5.1. Completing the Site Form

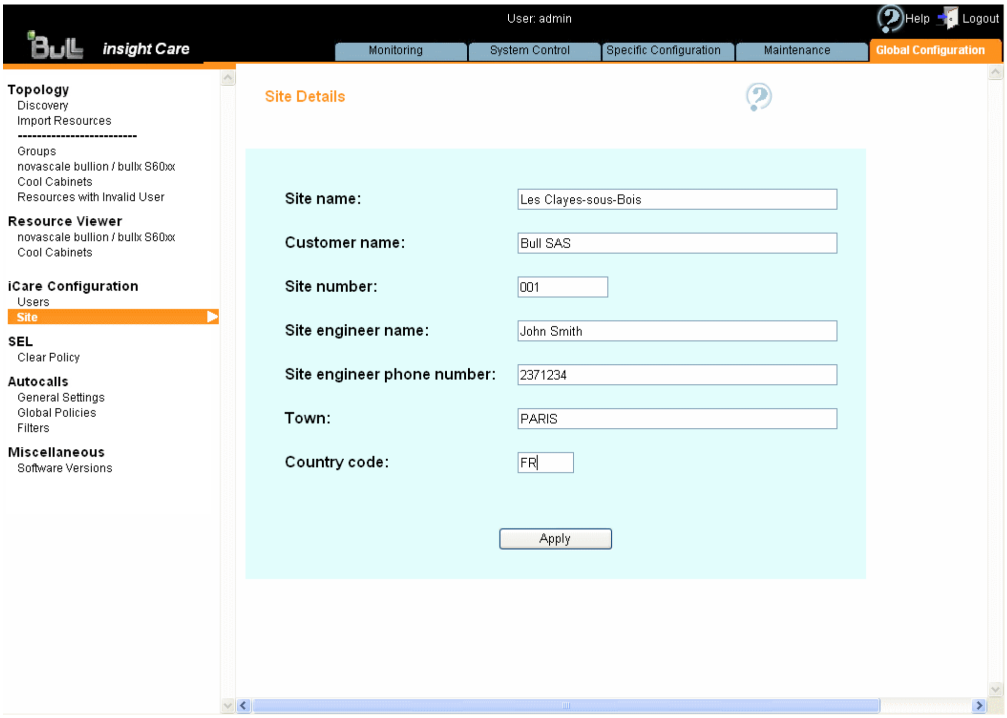
The site form should be completed to ensure that site-relevant information is included in the Autocalls and the Action Request Packages sent to Bull Support services.

Prerequisites

None

Procedure

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



Site Details

Site name:	Les Clayes-sous-Bois
Customer name:	Bull SAS
Site number:	001
Site engineer name:	John Smith
Site engineer phone number:	2371234
Town:	PARIS
Country code:	FR

Figure 5-1. Site Parameters page - Example

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

5.2. 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 Managing Autocalls, on page 5-4.
- Select a default autocall policy for each hardware resource type, as explained in Selecting Global Autocall Policies, on page 5-7.

Optionally, you can also:

- Select a specific autocall policy for specific hardware resources, as explained in Selecting Specific Autocall Policies, on page 5-9.
- Create specific autocall filters to track specific events, as explained in Configuring Autocall Filters, on page 5-11.

Important **It is strongly recommended to complete the site form before configuring autocalls. For details, see Completing the Site Form, on page 5-2.**

5.3. Managing Autocalls

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

Prerequisites

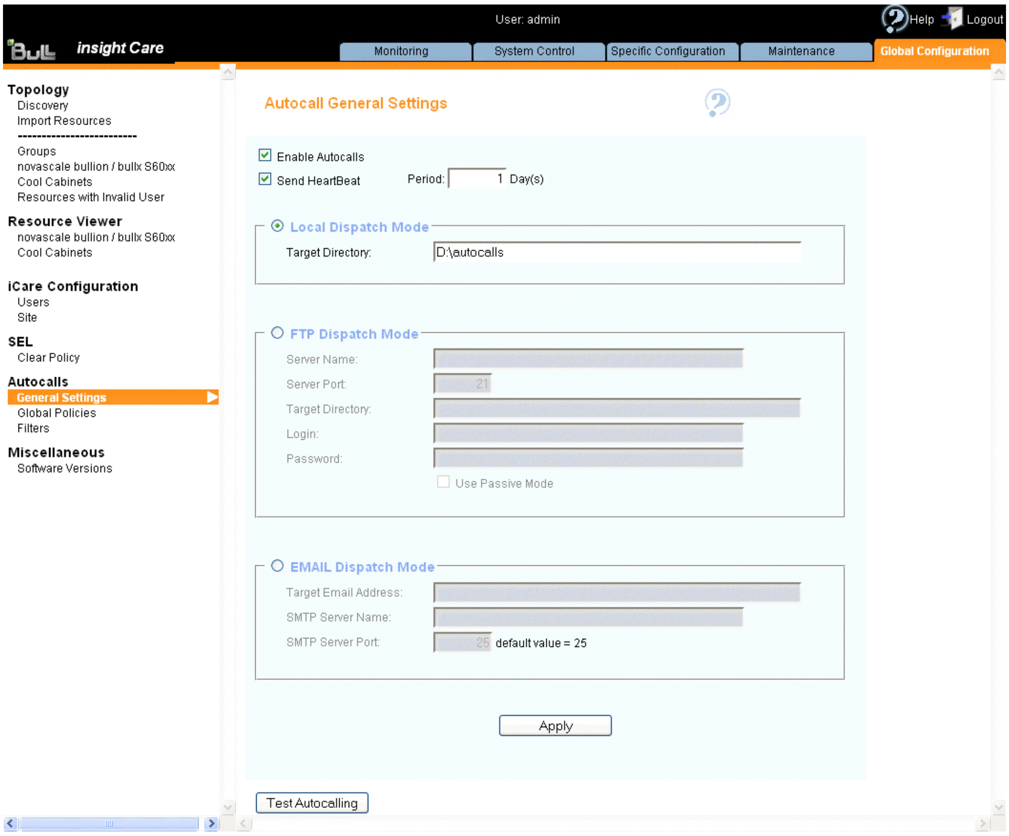
Your maintenance contract includes the autocall feature

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.



Autocall General Settings

☑ Enable Autocalls

☑ Send HeartBeat Period: 1 Day(s)

● Local Dispatch Mode

Target Directory: D:\autocalls

○ FTP Dispatch Mode

Server Name:

Server Port: 21

Target Directory:

Login:

Password:

□ Use Passive Mode

○ EMAIL Dispatch Mode

Target Email Address:

SMTP Server Name:

SMTP Server Port: 25 default value = 25

Figure 5-2. Autocall General Settings page (Autocall Enabled)

Autocall General Settings	
Enable Autocalls	Select this check box to enable the autocall feature.
Send HeartBeat and **Period** field	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 FTP server hostname or IP address
Server Port	Remote maintenance FTP 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)
EMAIL Dispatch Mode	
The EMAIL dispatch mode sends one XML file per autocall to the specified email address. To enable the EMAIL dispatch mode, first select the **Enable Autocalls** checkbox and then complete the fields as follows:	
Target Email Address	Email address to which the autocall XML file attachment is to be sent
SMTP Server Name	Hostname or IP address of the SMTP server used to route emails
SMTP Server Port	SMTP server port (25 by default)
Note: SMTP Authentication (SMTP AUTH) is not supported.	

Table 5-1. Autocall dispatch mode settings

2. Select the **Enable Autocalls** check box and configure the autocall dispatch mode as explained in Table 5-1.
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.

Important **This action tests the connexion between the iCare Console and the Bull Support Center. It doesn't test the connexion between the iCare Console and the resource.**

Note The Test Autocalling result includes the platform serie and the module number.

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 5-7. 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.

5.4. 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.

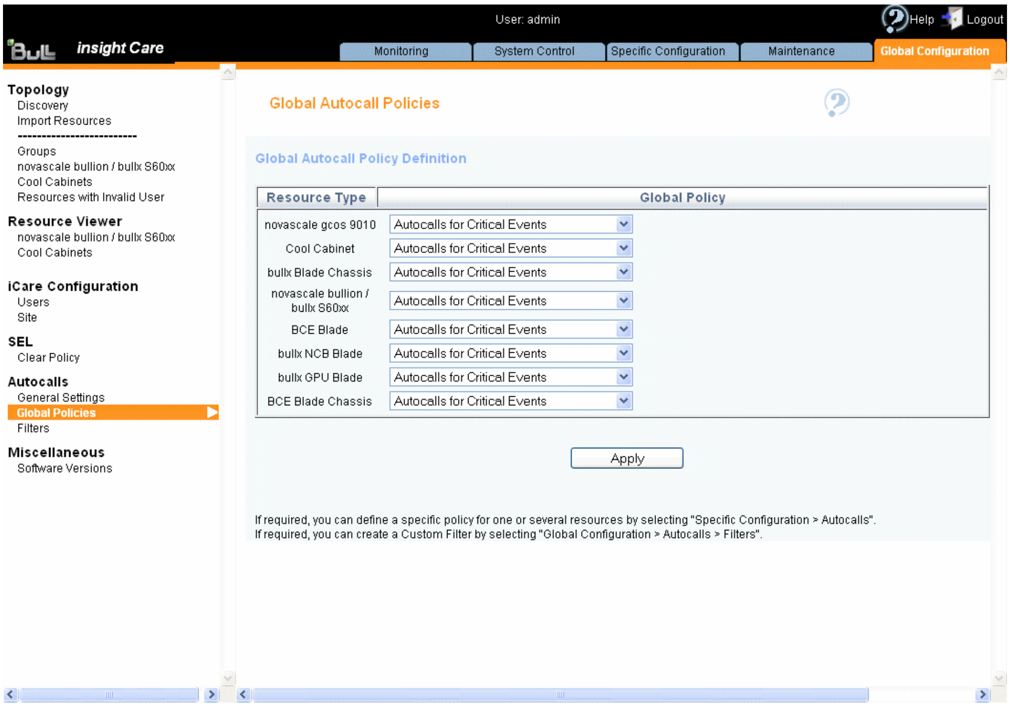
According to your needs, you can select global policies based on event severity or on event type. If you select global policies based on event type, you can decide whether to apply default filters or to create and apply custom filters.

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.



Global Autocall Policies

Global Autocall Policy Definition

Resource Type	Global Policy
novascale gcos 9010	Autocalls for Critical Events
Cool Cabinet	Autocalls for Critical Events
bullx Blade Chassis	Autocalls for Critical Events
novascale bullion / bullx S60xx	Autocalls for Critical Events
BCE Blade	Autocalls for Critical Events
bullx NCB Blade	Autocalls for Critical Events
bullx GPU Blade	Autocalls for Critical Events
BCE Blade Chassis	Autocalls for Critical Events

If required, you can define a specific policy for one or several resources by selecting "Specific Configuration > Autocalls".
If required, you can create a Custom Filter by selecting "Global Configuration > Autocalls > Filters".

Figure 5-3. 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 Displaying Default or Custom Filter Details, on page 5-11.
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 5-11

Table 5-2. 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 5-9.

5.5. 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.

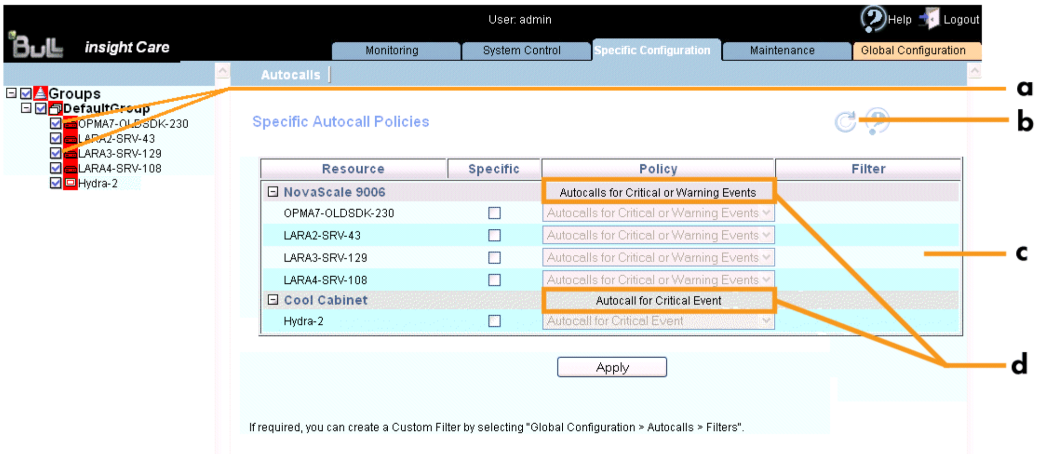
Prerequisites

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).



Resource	Specific	Policy	Filter
⊟ NovaScale 9006		Autocalls for Critical or Warning Events	
OPMA7-OLDSDK-230	☐	Autocalls for Critical or Warning Events	
LARA2-SRV-43	☐	Autocalls for Critical or Warning Events	
LARA3-SRV-129	☐	Autocalls for Critical or Warning Events	
LARA4-SRV-108	☐	Autocalls for Critical or Warning Events	
⊟ Cool Cabinet		Autocall for Critical Event	
Hydra-2	☐	Autocall for Critical Event	

If required, you can create a Custom Filter by selecting "Global Configuration > Autocalls > Filters".

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 Displaying Default or Custom Filter Details, on page 5-11.
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 5-11

Figure 5-4. Specific Autocall Policy page

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

5.6. 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:

- Displaying Default or Custom Filter Details, on page 5-11
- Creating a Custom Filter, on page 5-13
- Editing a Custom Filter, on page 5-14
- Deleting a Custom Filter, on page 5-17

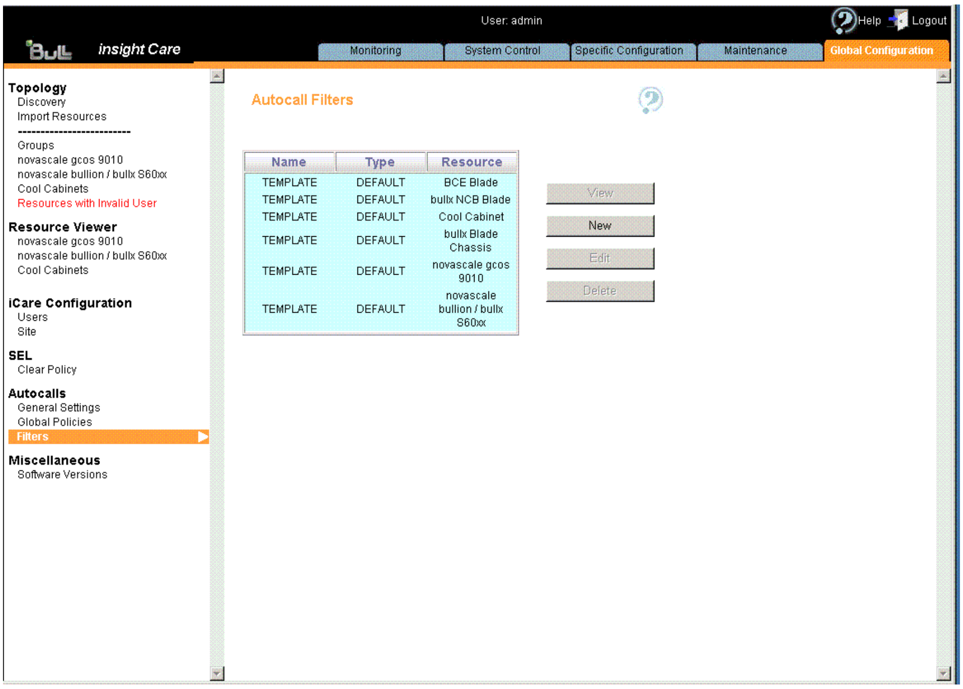
5.6.1. Displaying Default or Custom Filter Details

Prerequisites

None

Procedure

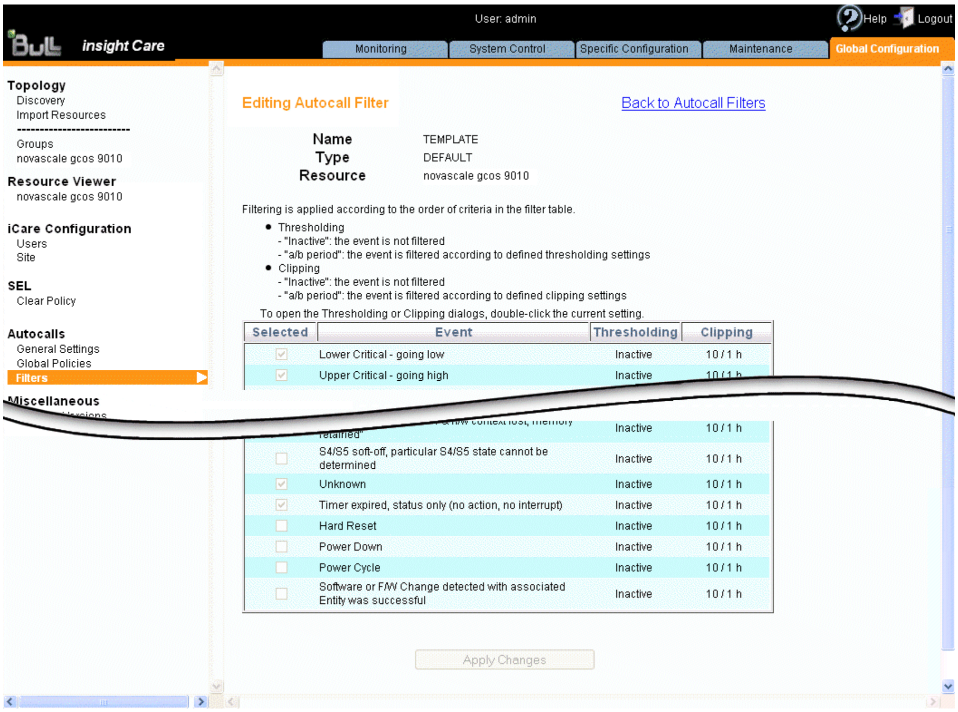
1. From the **Global Configuration** tab, click **Autocalls** > **Filters**. The **Autocall Filters** page appears.



Name	Type	Resource
TEMPLATE	DEFAULT	BCE Blade
TEMPLATE	DEFAULT	bullx NCB Blade
TEMPLATE	DEFAULT	Cool Cabinet
TEMPLATE	DEFAULT	bullx Blade Chassis
TEMPLATE	DEFAULT	novascale gcos 9010
TEMPLATE	DEFAULT	novascale bullion / bullx S60xx

Figure 5-5. 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.



Editing Autocall Filter

Back to Autocall Filters

Name	TEMPLATE
Type	DEFAULT
Resource	novascale gcos 9010

Filtering is applied according to the order of criteria in the filter table.

- Thresholding
  - "Inactive": the event is not filtered
  - "a/b period": the event is filtered according to defined thresholding settings
- Clipping
  - "Inactive": the event is not filtered
  - "a/b period": the event is filtered according to defined clipping settings

To open the Thresholding or Clipping dialogs, double-click the current setting.

Selected	Event	Thresholding	Clipping
☑	Lower Critical - going low	Inactive	10 / 1 h
☑	Upper Critical - going high	Inactive	10 / 1 h
	& h/w context lost, memory retained"	Inactive	10 / 1 h
☐	S4/S5 soft-off, particular S4/S5 state cannot be determined	Inactive	10 / 1 h
☑	Unknown	Inactive	10 / 1 h
☑	Timer expired, status only (no action, no interrupt)	Inactive	10 / 1 h
☐	Hard Reset	Inactive	10 / 1 h
☐	Power Down	Inactive	10 / 1 h
☐	Power Cycle	Inactive	10 / 1 h
☐	Software or F/W Change detected with associated Entity was successful	Inactive	10 / 1 h

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 5-14.

Figure 5-6. Viewing Autocall Filter page

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

5.6.2. Creating a Custom Filter

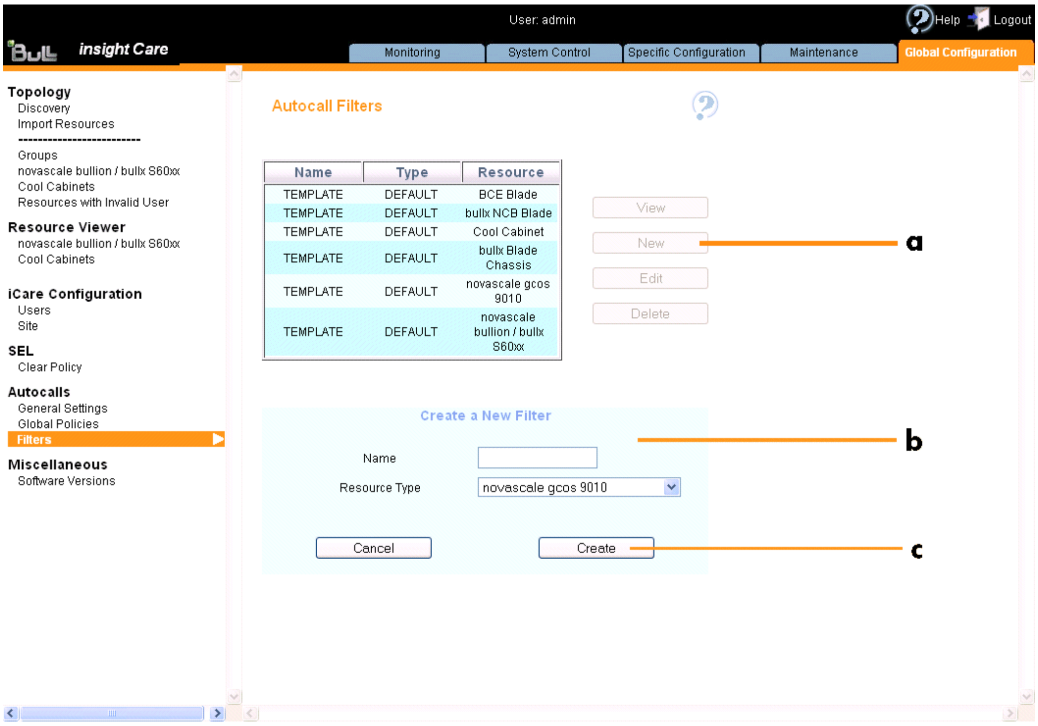
The iCare Console allows you to create your own autocall custom filter to finely tune event type filtering when the default filters supplied with the console do not cover your needs.

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).



Name	Type	Resource
TEMPLATE	DEFAULT	BCE Blade
TEMPLATE	DEFAULT	bullx NCB Blade
TEMPLATE	DEFAULT	Cool Cabinet
TEMPLATE	DEFAULT	bullx Blade Chassis
TEMPLATE	DEFAULT	novascale gcos 9010
TEMPLATE	DEFAULT	novascale bullion / bullx S60xx

Create a New Filter

Name

Resource Type: novascale gcos 9010

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 5-7. 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 5-14.

5.6.3. 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.

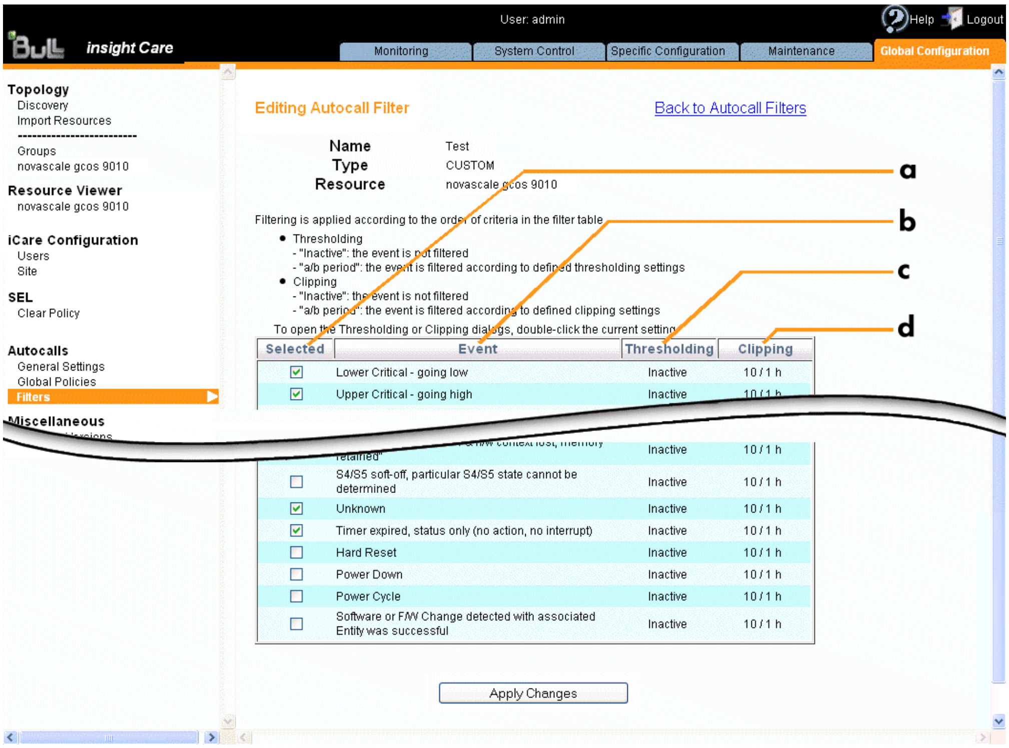
Prerequisites

The custom filter has been created, as explained in Creating a Custom Filter, on page 5-13.

Procedure

Note Criteria differ according to hardware resource type.

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

Name Test
Type CUSTOM
Resource novascale gcos 9010

Filtering is applied according to the order of criteria in the filter table
- Thresholding
  - "Inactive": the event is not filtered
  - "a/b period": the event is filtered according to defined thresholding settings
- Clipping
  - "Inactive": the event is not filtered
  - "a/b period": the event is filtered according to defined clipping settings

To open the Thresholding or Clipping dialogs, double-click the current setting

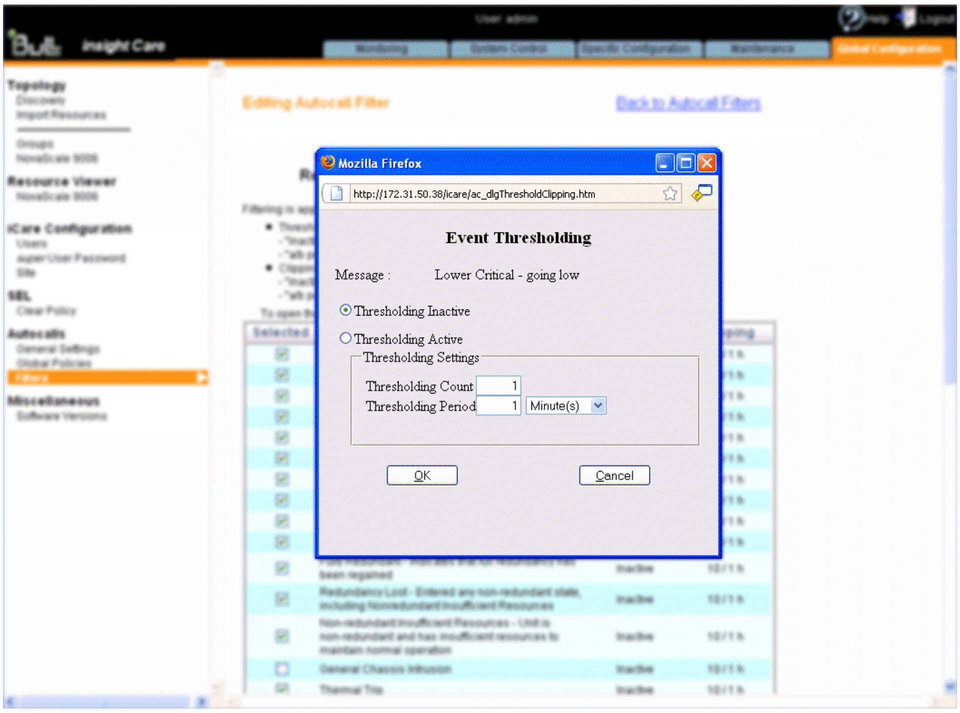
Selected	Event	Thresholding	Clipping
☑	Lower Critical - going low	Inactive	10 / 1 h
☑	Upper Critical - going high	Inactive	10 / 1 h
	& H/W context lost, memory retained"	Inactive	10 / 1 h
□	S4/S5 soft-off, particular S4/S5 state cannot be determined	Inactive	10 / 1 h
☑	Unknown	Inactive	10 / 1 h
☑	Timer expired, status only (no action, no interrupt)	Inactive	10 / 1 h
□	Hard Reset	Inactive	10 / 1 h
□	Power Down	Inactive	10 / 1 h
□	Power Cycle	Inactive	10 / 1 h
□	Software or F/W Change detected with associated Entity was successful	Inactive	10 / 1 h

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 5-8. 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**.



http://172.31.50.38/icare/ac_dlgThresholdClipping.htm

Event Thresholding

Message : Lower Critical - going low

● Thresholding Inactive

○ Thresholding Active

Thresholding Settings

Thresholding Count 1

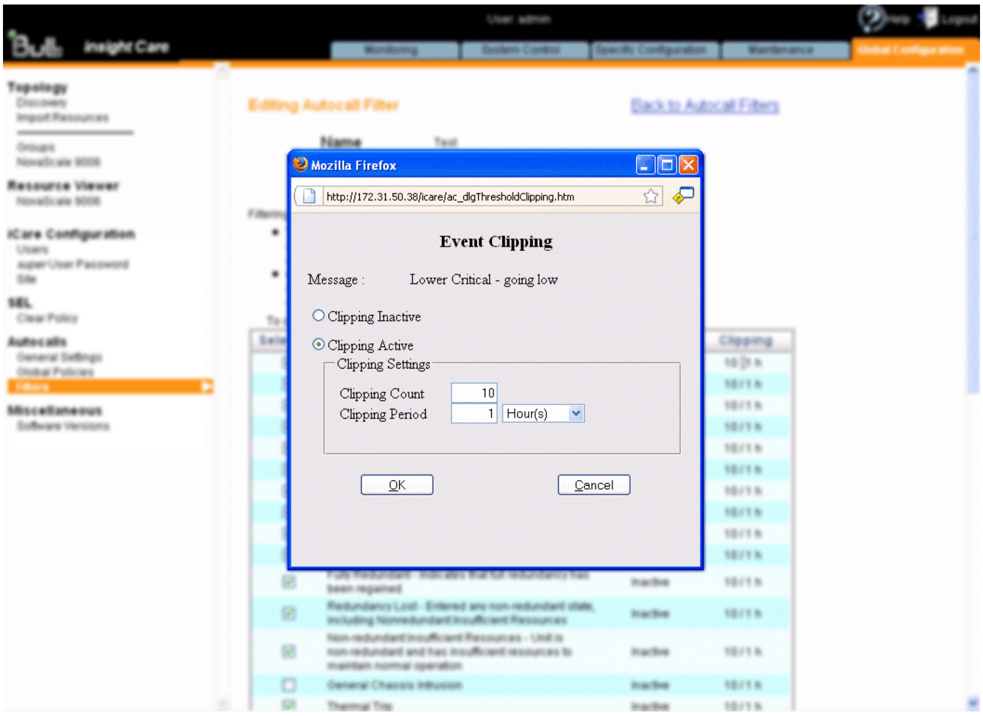
Thresholding Period 1 Minute(s)

OK Cancel

<table>
<tr><th colspan="2">Event Thresholding Box</th></tr>
<tr><td colspan="2">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 <b>Thresholding Count</b> field is reached within the period of time indicated in the <b>Thresholding Period</b> field, this event message is selected for transmission.</td></tr>
<tr><td><b>Thresholding Inactive</b></td><td>Deactivates thresholding: if the event is selected, all messages are transmitted as autocalls.</td></tr>
<tr><td><b>Thresholding Active</b></td><td>Activates thresholding using the values displayed in the <b>Thresholding Count</b> and <b>Thresholding Period</b> fields.</td></tr>
<tr><td><b>Thresholding Count</b></td><td>Number of identical event messages to be reached.</td></tr>
<tr><td><b>Thresholding Period</b></td><td>Period of time, in seconds, minutes, hours or days.</td></tr>
</table>

Figure 5-9. Event Thresholding box description

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



Mozilla Firefox

http://172.31.50.38/icare/ac_dlgThresholdClipping.htm

Event Clipping

Message : Lower Critical - going low

○ Clipping Inactive

● Clipping Active

Clipping Settings

Clipping Count 10

Clipping Period 1 Hour(s)

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 transmission.	
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 5-10. 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**.

5.6.4. Deleting a Custom Filter

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

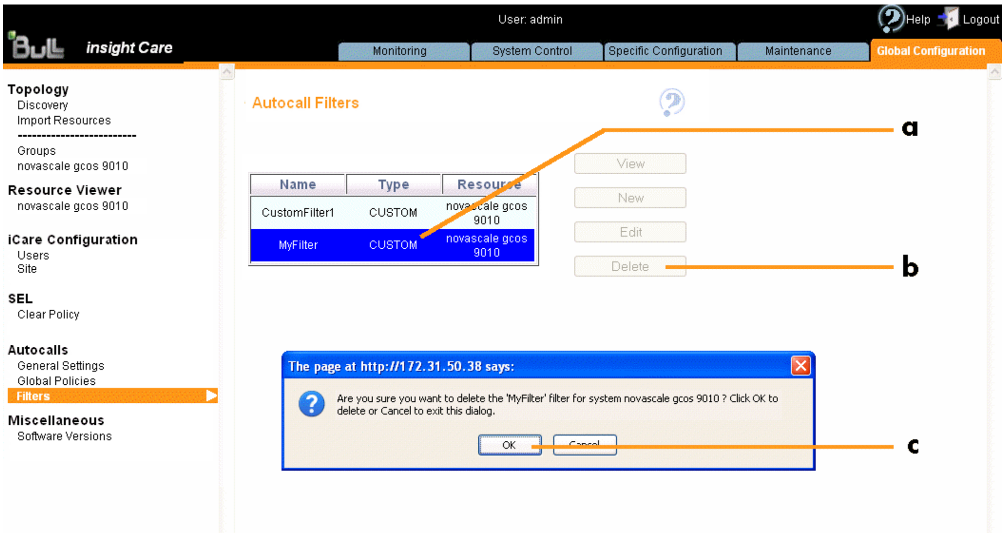
Note You cannot delete default autocall filters.

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).



Name	Type	Resource
CustomFilter1	CUSTOM	novascale gcos 9010
MyFilter	CUSTOM	novascale gcos 9010

The page at http://172.31.50.38 says:

Are you sure you want to delete the 'MyFilter' filter for system novascale gcos 9010 ? Click OK to delete or Cancel to exit this dialog.

Figure 5-11. Autocall Filters page (Delete a filter)

5.7. Creating an Intervention Report

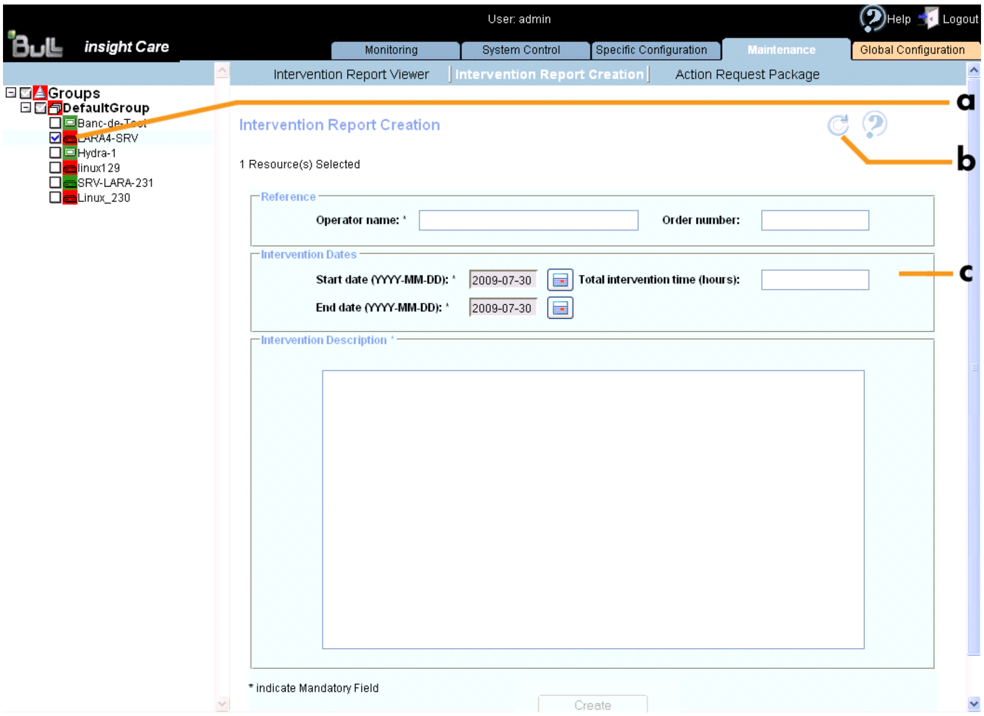
You are advised to create an intervention report when you perform preventive or corrective maintenance or problem analysis operations on hardware resources monitored by the iCare Console. These reports allow you to keep track of the operations performed on monitored hardware resources stored in the iCare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



Intervention Report Creation

1 Resource(s) Selected

Reference

Operator name: *

Order number:

Intervention Dates

Start date (YYYY-MM-DD): * 2009-07-30

Total intervention time (hours):

End date (YYYY-MM-DD): * 2009-07-30

Intervention Description *

* indicate Mandatory Field

Figure 5-12. 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**.

5.8. Viewing the List of Intervention Reports

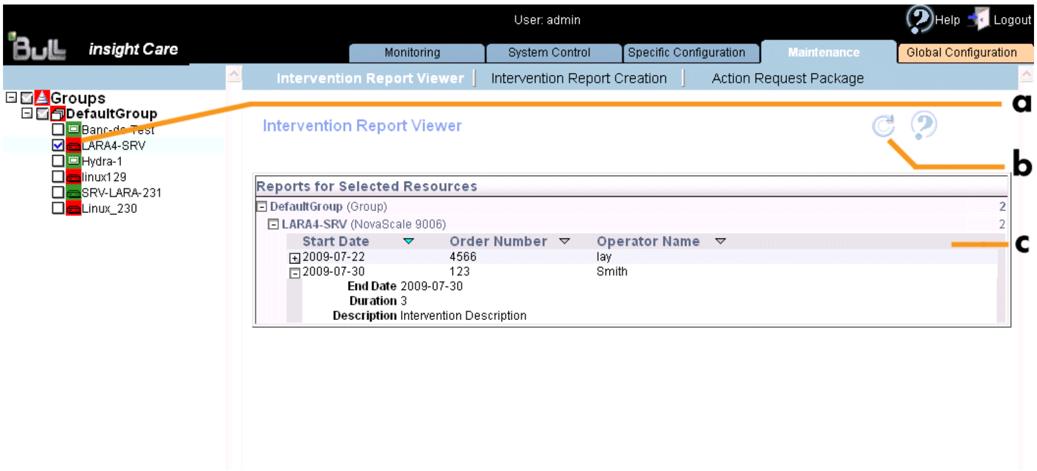
You can display intervention reports on monitored resources at any time to help you perform preventive or corrective maintenance or problem analysis operations.

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).



Intervention Report Viewer

Reports for Selected Resources

⊟ DefaultGroup (Group) 2

⊟ LARA4-SRV (NovaScale 9006) 2

Start Date	Order Number	Operator Name
⊞ 2009-07-22	4566	lay
⊟ 2009-07-30	123	Smith

End Date 2009-07-30
Duration 3
Description Intervention Description

Figure 5-13. 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.

5.9. 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 4. Building, Viewing and Managing Resource Logs.

Prerequisites

You have completed the Site form, as detailed in Completing the Site Form, on page 5-2.

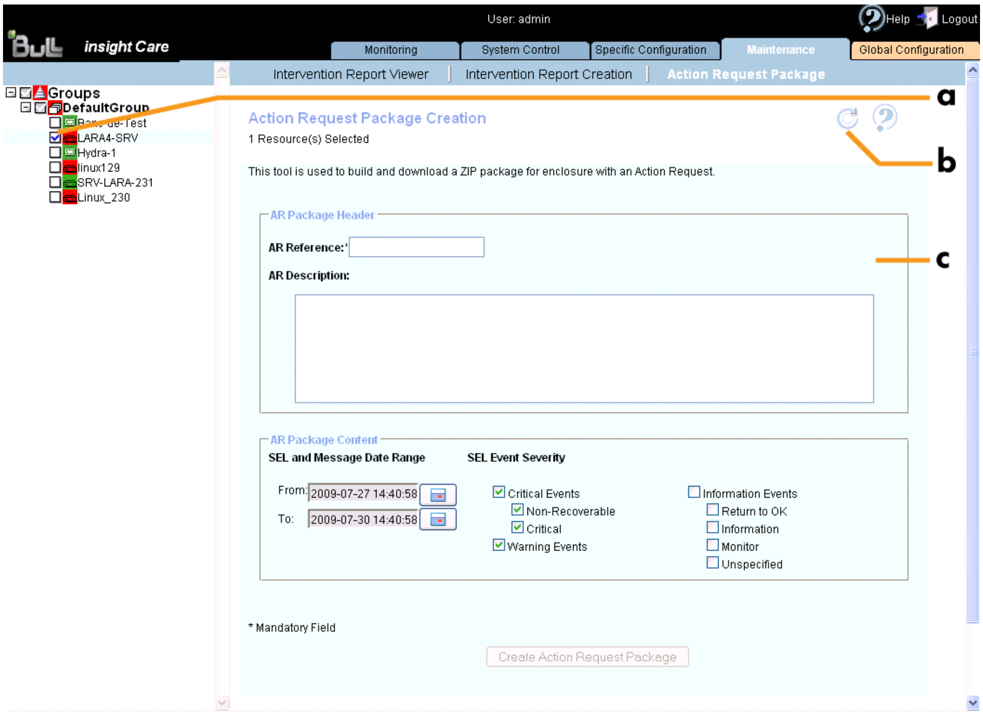
Your browser is configured to accept cookies and downloads.

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).



Action Request Package Creation

1 Resource(s) Selected

This tool is used to build and download a ZIP package for enclosure with an Action Request.

AR Package Header

AR Reference:*

AR Description:

AR Package Content

SEL and Message Date Range

From: 2009-07-27 14:40:58

To: 2009-07-30 14:40:58

SEL Event Severity

☑ Critical Events
- ☑ Non-Recoverable
- ☑ Critical

☑ Warning Events

☐ Information Events
- ☐ Return to OK
- ☐ Information
- ☐ Monitor
- ☐ Unspecified

* Mandatory Field

Figure 5-14. 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.

Glossary

This glossary may contain entries that are not relevant to your system.

A

ABR
Automatic BIOS Recovery.

ACPI
Advanced Configuration and Power Interface.
An industry specification for the efficient handling of power consumption in desktop and mobile computers. ACPI specifies how a computer's BIOS, operating system, and peripheral devices communicate with each other about power usage.

ADM1069
The ADM1069 Super Sequencer® is a configurable supervisory/ sequencing device that offers a single-chip solution for supply monitoring and sequencing in multiple supply systems.

ARU
Add / Removeable Unit. A hardware logical unit, or a group of logical units, that can be viewed / handled by an Operating System, or the BIOS, or the Platform Management Software. An ARU can be nested and is not necessarily separable from other ARUs. An ARU is also known as a PMU.

ASR
Automatic Server Restart.

ASIC
Application Specific Integrated Circuit.

B

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

BCE
Elementary calculation block.

BCEA
ASIC elementary calculation block.

BCEF
FPGA elementary calculation block.

BCS
Bull 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.

BHC
See Blade Hardware Console.

BIOS
Basic Input / Output System. A program stored in flash EPROM or ROM that controls the system startup process.

BIST
Built-In Self-Test. See POST.

Blade Hardware Console
Graphical user interface used to access the management software embedded in the blade module.

BMC
Baseboard Management Controller. See Embedded Management Controller.

BOOTP
Network protocol used by a network client to obtain an IP address from a configuration server.

BSM
Bull System Manager. A software package that allows the management of data centers. BSM is capable of supporting many different types of servers.

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).

C

Chassis Hardware Console
Graphical user interface used to access the management software embedded in the Chassis Management Module.

CHC
See Chassis Hardware Console.

Clipping
An Event filter criterion. Clipping is defined on a Count / Time basis aimed at routing a pre-defined number of messages only. Identical messages are counted and when the number of messages indicated in the **Count** field is reached within the period of time indicated in the **Time** field, no other messages will be selected for routing.

CMB
Chassis Management Board.

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

CMC
Chassis Management Controller.

CMM
Chassis Management Module.

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

CRU
Customer Replaceable Unit. A component (board, module, fan, power supply, etc.) that is replaced or added by the End User as a single entity.

CSE
Customer Service Engineer.

D

DES
Data Encryption Standard.

DHCP
Dynamic Host Configuration Protocol.

DMA
Direct Memory Access. Allows data to be sent directly from a component (e.g. disk drive) to the memory on the motherboard). The microprocessor does not take part in data transfer enhanced system performance.

DNS
Domain Name Server.

DSIB/DSIBL
Dummy System Interface Board. The boards designed by Bull when there is not a BCS in the system.

E

EEPROM
Electrically Erasable Programmable Read-Only Memory. A type of memory device that stores password and configuration data.

EFI
Extensible Firmware Interface. A specification for a firmware-OS interface.

EFI Shell
Simple, interactive user interface that allows EFI device drivers to be loaded, EFI applications to be launched, and operating systems to be booted. In addition, the EFI Shell provides a set of basic commands used to manage files and the system environment variables. See Shell.

Embedded Management Controller
Also known as BMC (Baseboard Management Controller). This controller, embedded on the main system board, provides out-of-band access to platform instrumentation, sensors and effectors.

EMM
Embedded Management Module. Software embedded in the server module to implement management functions and accessible from the Hardware Console graphical interface.

EPROM
Erasable Programmable Read-Only Memory. A type of memory device that is used to store the system BIOS code. This code is not lost when the computer is powered off.

ESB
Ethernet Switch Board.

ESM
Ethernet Switch Module.

F

FC-LGA
Flip-Chip Land Grid Array.

FDB
Fan Distribution Board.

Flash EPROM
Flash Erasable Programmable Read-Only Memory. A type of memory device that is used to store the system firmware code. This code can be replaced by an updated code from a floppy disk, but is not lost when the computer is powered off.

FPGA
Field Programmable Gate Array.

FQDN
Fully Qualified Domain Name.

FRU
Field Replaceable Unit. A component (board, module, fan, power supply, etc.) that is replaced or added by Customer Service Engineers as a single entity.

G

GPU
Graphical Processing Unit.

GUI
Graphical User Interface.

H

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

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

Hardware Partition
A set of hardware components that can boot and run a Base OS image.

Hard Partitioning
Ability to split a platform into a number of independent smaller hardware partitions or to merge multiple independent hardware partitions to form a single larger hardware partition.

HDD
Hard Disk Drive.

HPC
High Performance Computing.

HPC Cluster
High Performance Computing Cluster. A group of computers linked together to form a single computer.

Host Operating System
The Operating System that is booted at initialization and that is a Virtual Machine Monitor (VMM) and a number of guest OS.

Hot-Plugging
The operation of adding a component without interrupting system activity.

Hot-Swapping
The operation of removing and replacing a faulty component without interrupting system activity.

HT
HyperThreading. See Multi-Threading.

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.

iBMC
Integrated Baseboard Management Controller. See Embedded Management Controller.

iCare
The iCare Console (insight Care) is a web-based administration application which provides tools for hardware unit maintenance.

ICH
Input/Output Hub. Provides a connection point between various I/O components and Intel processors.

ICMB
Intelligent Chassis Management Bus. Name for the architecture, specifications, and protocols used to interconnect intelligent chassis via an RS-485-based serial bus for the purpose of platform management.

ILB / ILBL
I/O Legacy Boards.The Bull-designed I/O boards for the MESCA modules.

INCA
INtegrated Cluster Architecture.

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

IPMB
Intelligent Platform Management Bus. Abbreviation for the architecture and protocol used to interconnect intelligent controllers via an I2C based serial bus for the purpose of platform management.

IPMI
Intelligent Platform Management Interface. A specification owned by Intel which describes mechanisms and devices to completely offload the task of managing system hardware from the primary CPU.

J

JOEM
JTAG Over Ethernet Module.

JTAG
Joint Test Action Group.

K

No entries.

L

LAN
Local Area Network.

LCD
Liquid Crystal Display.

LCP
Local Control Panel. Module consisting of a controller, a LCD color display, a green and a blue LED and a Power ON button.

LDAP
Lightweight Directory Access Protocol.

LED
Light Emitting Diode.

Logical Partition
When the Base Operating System is a Virtual Machine Monitor, a logical partition is the software environment used to run a Guest Operating System.

Logical Processor
See Thread.

M

MAC
Media Access Control.

MCA
A Machine Check Abort exception occurs when an error condition has arisen that requires corrective action.

MESCA
Multiple Environments on a Scalable Csi-based Architecture.

MIB
Management Interface Base.

MIMD
Multiple Instruction Multiple Data

MMX
MultiMedia eXtensions.

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

MTBF
Mean Time Between Failure.

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

Multi-Threading
The ability of a single processor core to provide software visibility similar to that of several cores and execute several threads in apparent (to software) simultaneity while using limited additional hardware resources with respect to a core without multi-threading.
Depending on core design, the instructions issued for execution by the core at a given cycle may be either **Hyper-Threading** (HT) - from a single thread, switching to another thread upon occurrence of specific events (e.g. cache misses) or **Simultaneous Multi-Threading** (SMT) - from both threads.

MXB/MXBC
Memory and Xeon Board / Memory and Xeon Board Controller.

N

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

NFS
Network File System.

NIC
Network Interface Controller.

NUMA
Non Uniform Memory Access.

NVRAM
Non-Volatile Random Access Memory.

O

Off-Lining
See On-Lining / Off-Lining.

On-Lining / Off-Lining
On-lining and off-lining are dynamic logical operations. On-lining is the non-physical addition of an ARU to the running OS. The on-lined unit already exists in the configuration as an inactive unit (present and connected). Off-lining is the non-physical removal of an ARU from the running OS. The off-lined unit remains in the configuration as an inactive unit, ready to be on-lined.

OOB
Out Of Band. Access to system platform management that does not go through the OS or other software running on the main processors of the managed system.

OPMA
Open Platform Management Architecture.

P

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

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.

PIROM
The Processor Information ROM contains information about the specific processor in which it resides. This information includes robust addressing headers to allow for flexible programming and forward compatibility, core and L2 cache electrical specifications, processor part and S-spec numbers, and a 64-bit processor number.

PMU
Physically Manageable Unit. A hardware logical unit, or a group of logical units, that can be viewed / handled by an Operating System, or the BIOS, or the Platform Management Software. A PMU can be nested and is not necessarily separable from other PMUs. A PMU is also known as an ARU.

POST
Power On Self Test.

Processor
Each processor contains one or more dies in a single package. Each die contains one or more cores. Each core contains one or more threads (logical processors). Each processor is housed in a processor socket.

PSMI
Power Supply Management Interface.

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

PSWB
PCI SWitch Board.

PSWM
PCI SWitch Module.

PWM
Pulse Width Modulation.

Q

QDR
Quad Data Rate. Communication signalling technique where data is transmitted at four points in the clock cycle.

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

QSB
Quad Switch Board.

QSFP
Quad Small Form-factor Pluggable. Low-power interconnect technology.

QSMB
Quad Switch Module. InfiniBand Switch.

R

RADIUS
Remote Authentication Dial-In User Service.

RAS
Reliability, Availability, Serviceability.

RMII
Reduced Media Independent Interface. A standard that reduceds the number of signals/pins required to connect an Ethernet chip to physical layer transceiver. See MII.

RTC
Real Time Clock.

S

SAS
Serial Attached SCSI. A data transfer technology used to move data to and from computer storage devices such as hard drives and tape drives.

SATA
Serial ATA. A computer bus technology for connecting hard disks and other devices.

SEL
System Event Log. A record of system management events. The information stored includes the name of the event, the date and time the event occurred and event data. Event data may include POST error codes that reflect hardware errors or software conflicts within the system.
A non-volatile storage area into the BMC and associated interfaces for storing System platform Event information for later retrieval.

Server Hardware Console
Graphical user interface used to access the management software embedded in the server module.

SHC
See Server Hardware Console.

SIB/SIBL
System Interface Board. The boards designed by BULL which contain the BCS (Bull Coherent Switch).

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.

SMTP
Simple Mail Transfer Protocol.

SNC
Scalable Node Controller. The processor system bus interface and memory controller for the Intel870 chipset. The SNC supports both the Itanium2 processors, DDR SDRAM main memory, a Firmware Hub Interface to support multiple Firmware hubs, and two scalability ports for access to I/O and coherent memory on other nodes, through the FSS.

SNMP
Simple Network Management Protocol.

SoC
System on Chip.

Socket
Central Processing Unit 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.

SO-DIMM
Small Outline Dual In-line Memory.

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

SSD
Solid State Drive.

SSH
Secured Shell.

SSL
Secure Socket Layer.

T

TELNET
TELecommunication NETwork. Protocol used on the Internet or Local Area Networks to provide a bidirectional interactive communications facility.

Thread
A thread or logical processor is the execution context within a single core and the software visibility of multi-threading. A single multi-threaded processor contains two or more threads (or logical processors).

Thresholding
An Event filter criterion. Thresholding is defined on a Count / Time basis aimed at routing significant messages only. Identical messages are counted and when the number of messages indicated in the **Count** field is reached within the period of time indicated in the **Time** field, this message is selected for routing.

TKW
TUKWILA Intel Itanium Processor (4 cores per socket).

TSM
Ten Gigabit Ethernet Switch Module.

U

UCM
Ultra Capacitor Module.

V

VMM
Virtual Machine Monitor.

W

WOL
Wake On Lan. A feature that provides the ability to remotely power on a system through a network connection.

X

XCSI

Extended Common System Interface. High-speed point-to-point Bull interface, used to interconnect servers. XCSI ports are located and managed in the BCS (node controller).

XNC

External Node Controller. See BCS.

Y

No entries.

Z

No entries.

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

REFERENCE
86 A1 71FA 07