

iCare Console

User's Guide

iCare



REFERENCE
86 A1 71FA 00

iCare

iCare Console

User's Guide

Hardware

September 2009

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

REFERENCE
86 A1 71FA 00

The following copyright notice protects this book under Copyright laws which prohibit such actions as, but not limited to, copying, distributing, modifying, and making derivative works.

Copyright ©Bull SAS 2009

Printed in France

Trademarks and Acknowledgements

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

All brand names and software and hardware product names are subject to trademark and/or patent protection.

Quoting of brand and product names is for information purposes only and does not represent trademark misuse.

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

Legal Information	viii
Regulatory Declarations and Disclaimers	viii
Declaration of the Manufacturer or Importer	viii
Safety Compliance Statement	viii
European Community (EC) Council Directives	viii
Electromagnetic Compatibility	viii
Low Voltage	viii
EC Conformity	viii
Telecommunications Terminal Equipment	viii
Mechanical Structures	viii
FCC Declaration of Conformity	ix
Canadian Compliance Statement (Industry Canada)	ix
Laser Compliance Notice (if applicable)	ix
Safety Information	x
Definition of Safety Notices	x
Electrical Safety	x
Laser Safety Information (if applicable)	xi
Data Integrity and Verification	xi
Waste Management	xi
Preface	xii
Intended Readers	xii
Highlighting	xii
Related Publications	xii
Chapter 1. Getting Started	1-1
1.1. Starting the iCare Console	1-2
1.2. iCare Console Overview	1-3
1.3. Initial Configuration	1-6
1.4. Stopping the iCare Console	1-7
Chapter 2. Managing the Resource Tree	2-1
2.1. Importing Hardware Resources	2-2
2.1.1. Automatically Importing Hardware Resources	2-2
2.1.2. Manually Importing Multiple Hardware Resources	2-4
2.1.2.1. Creating a Hardware Resource XML Import File	2-4
2.1.2.2. Using an XML File to Import Multiple Hardware Resources ..	2-7
2.1.3. Manually Importing a Single Hardware Resource	2-9

2.2.	Managing Imported Hardware Resources	2-12
2.2.1.	Adding Newly Discovered Resources to the Resource Tree	2-12
2.2.2.	Viewing Already Monitored Resources	2-14
2.2.3.	Troubleshooting Errors on Discovered Resources	2-15
2.2.4.	Deleting a Hardware Resource from the Tree	2-19
2.2.5.	Enabling/Disabling Hardware Resource Monitoring	2-20
2.3.	Managing Hardware Resource Custom Groups	2-22
2.3.1.	Creating a Hardware Resource Custom Group	2-22
2.3.2.	Editing Hardware Resource Custom Group Details	2-24
2.3.3.	Deleting a Hardware Resource Custom Group	2-26
2.3.4.	Adding a Hardware Resource to a Resource Group	2-27
<hr/>		
Chapter 3.	Connecting to a Resource Console	3-1
<hr/>		
Chapter 4.	Monitoring Resources	4-1
4.1.	Building SEL Query Reports	4-2
4.2.	Building Messages Query Reports	4-5
4.3.	Managing SEL Event Status	4-7
4.4.	Viewing Resource Details	4-10
<hr/>		
Chapter 5.	Configuring Autocalls	5-1
5.1.	Introducing the Autocall Feature	5-2
5.2.	Enabling/Disabling and Testing Autocalls	5-2
5.3.	Selecting Global Autocall Policies	5-4
5.4.	Selecting Specific Autocall Policies	5-6
5.5.	Configuring Autocall Filters	5-8
5.5.1.	Viewing Default or Custom Filter Details	5-8
5.5.2.	Creating a Custom Filter	5-10
5.5.3.	Editing a Custom Filter	5-11
5.5.4.	Deleting a Custom Filter	5-15
<hr/>		
Chapter 6.	Managing Intervention Reports and Action Requests	6-1
6.1.	Creating an Intervention Report	6-2
6.2.	Viewing the List of Intervention Reports	6-3
6.3.	Creating an Action Request Package	6-4
<hr/>		
Chapter 7.	Performing Other Configuration Tasks	7-1
7.1.	Managing User Accounts	7-2
7.1.1.	Creating a User Account	7-2
7.1.2.	Deleting a User Account	7-3
7.1.3.	Changing a User Account Password	7-4
7.2.	Setting Up the BMC Super User Password	7-5
7.3.	Completing the Site Form	7-7
7.4.	Enabling/Disabling the Automatic Clear SEL Policy	7-8
7.5.	Displaying iCare and Other Software Version Information	7-9

Glossary	g-1
-----------------------	------------

Index	x-1
--------------------	------------

List of Figures

Figure 1.	Login page description	1-2
Figure 2.	Interface Structure	1-4
Figure 3.	Resource tree	1-5
Figure 4.	Menu Bar location	1-6
Figure 5.	Logout link	1-7
Figure 6.	Discovery page	2-3
Figure 7.	Network Discovery Results page - Multiple Resources	2-3
Figure 8.	Import Resources page - XML File Import tab	2-5
Figure 9.	XML template file - NovaScale 9006 Server example	2-5
Figure 10.	Import Resources page - XML File Import tab	2-7
Figure 11.	Network Discovery Results page - Multiple Resources	2-8
Figure 12.	Import Resources page - Manual Import tab	2-9
Figure 13.	Network Discovery Results page - Single Resource	2-11
Figure 14.	Network Discovery Results page (Newly Discovered Resources tab)	2-13
Figure 15.	Network Discovery Results page (Already Monitored Resources tab)	2-14
Figure 16.	Network Discovery Results page (Error on Discovered Resources tab)	2-15
Figure 17.	Deleting a Resource	2-19
Figure 18.	Enabling Resource Monitoring	2-21
Figure 19.	Disabling Resource Monitoring	2-21
Figure 20.	Groups Management page	2-23
Figure 21.	Create a New Group box	2-24
Figure 22.	Edit Selected Group Details box	2-25
Figure 23.	Groups Management page - Group deletion	2-26
Figure 24.	Moving Resources (example with Novascale 9006 servers)	2-27
Figure 25.	System Control tab	3-2
Figure 26.	Build SEL Query Report page	4-2
Figure 27.	SEL Query Report page	4-4
Figure 28.	Build Message Query Report page	4-5
Figure 29.	Message Query Report page	4-6
Figure 30.	SEL Query Report page - Default display	4-7
Figure 31.	SEL Query Report page - SEL Event List	4-8
Figure 32.	SEL Query Report page - SEL Event details	4-8
Figure 33.	Resource Viewer page - Examples	4-10
Figure 34.	Autocall General Settings page (Autocall Enabled)	5-3
Figure 35.	Global Autocall Policy page	5-4
Figure 36.	Specific Autocall Policy page	5-7
Figure 37.	Autocall Filters page	5-8
Figure 38.	Viewing Autocall Filter page	5-9
Figure 39.	Autocall Filters (Create a New Filter)	5-10
Figure 40.	Editing Autocall Filter page	5-12
Figure 41.	Event Thresholding box description	5-13
Figure 42.	Event Clipping box description	5-14
Figure 43.	Autocall Filters page (Delete a filter)	5-15

Figure 44. Intervention Report Creation page	6-2
Figure 45. Intervention Report Viewer page	6-3
Figure 46. Action Request Package Creation page	6-5
Figure 47. User Management page (Create a New User box)	7-2
Figure 48. User Management page (Delete User Account)	7-3
Figure 49. User Management page (Change User Password box)	7-4
Figure 50. super User Password page	7-6
Figure 51. Site Parameters page	7-7
Figure 52. Clear SEL Policy page	7-8
Figure 53. Software Versions page	7-9

List of Tables

Table 1.	Console features and related sections	1-3
Table 2.	XML import template file data	2-6
Table 3.	Manual import data	2-10
Table 4.	Duplicate partition name error	2-16
Table 5.	Duplicate platform name error	2-16
Table 6.	Duplicate platform ID error	2-16
Table 7.	Duplicate platform serial number error	2-17
Table 8.	Duplicate module serial number error	2-17
Table 9.	Module serial number unknown error	2-17
Table 10.	Module count does not match the number of modules error	2-17
Table 11.	Duplicate MAC address error	2-18
Table 12.	Duplicate IP address error	2-18
Table 13.	SEL query options	4-3
Table 14.	Message query options	4-6
Table 15.	Autocall dispatch mode settings	5-3
Table 16.	Global autocall policy options	5-5

Legal Information

Regulatory Declarations and Disclaimers

Declaration of the Manufacturer or Importer

We hereby certify that this product is in compliance with:

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

Safety Compliance Statement

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

European Community (EC) Council Directives

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

Electromagnetic Compatibility

- 2004/108/EC

Low Voltage

- 2006/95/EC

EC Conformity

- 93/68/EEC

Telecommunications Terminal Equipment

- 1999/5/EC

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

Compliance with these directives requires:

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

Mechanical Structures

- IEC 60297
- EIA-310-E

FCC Declaration of Conformity

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

Federal Communications Commission (FCC) Statement

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

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

Pursuant to Part 15.21 of the FCC Rules, any changes or modifications to this equipment not expressly approved by Bull SAS may cause harmful interference and void the FCC authorization to operate this equipment.

An FCC regulatory label is affixed to the equipment.

Canadian Compliance Statement (Industry Canada)

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

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

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

- ICES-003
- NMB-003

Laser Compliance Notice (if applicable)

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

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

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

Safety Information

Definition of Safety Notices



DANGER

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



CAUTION

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



WARNING

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

Electrical Safety

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



DANGER

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



CAUTION

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

Laser Safety Information (if applicable)

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

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



CAUTION

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

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

Data Integrity and Verification



WARNING

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

Waste Management

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

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

Preface

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

- Windows XP, Vista (or later)
- Windows Server 2003, 2008 (or later)
- Red Hat Enterprise Linux 5.3 (or later)



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

Intended Readers

This guide is intended for use by Bull System Hardware Administrators and Operators and qualified support personnel.

Highlighting

The following highlighting conventions are used in this guide:

Bold	Identifies the following: <ul style="list-style-type: none">• Interface objects such as menu names, labels, buttons and icons.• File, directory and path names.• Keywords to which particular attention must be paid.
<i>Italics</i>	Identifies references such as manuals or URLs.
<code>monospace</code>	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 documentation delivered with the systems monitored and maintained via the iCare Console.

Chapter 1. Getting Started

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

- Starting the iCare Console, on page 1-2
- iCare Console Overview, on page 1-3
- Initial Configuration, on page 1-6
- Stopping the iCare Console, on page 1-7

1.1. Starting the iCare Console

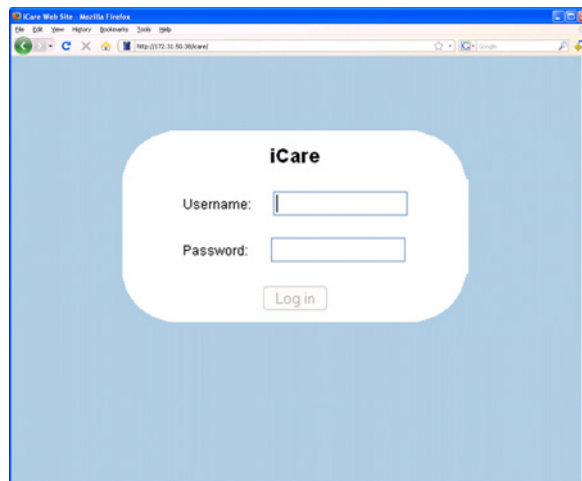
You can start the iCare Console using a Microsoft Internet Explorer or Mozilla Firefox browser.

Prerequisites

- Firefox only: your web browser is configured to accept cookies.

Procedure

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



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

Figure 1. Login page description

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



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

Related Topics

- Stopping the iCare Console, on page 1-7
- Changing a User Account Password, on page 7-4

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).

1.2. iCare Console Overview

The iCare Console is a web-based hardware administration application which provides tools for the supervision and maintenance of hardware resources. The hardware resources monitored by the iCare Console send event traps that are recorded in the iCare Console database.

The console receives two types of event traps:

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

Once discovered or imported, monitored hardware resources are displayed in the iCare Console Resource tree, which indicates the status of each monitored resource using colored icons. When an alarm arises on a resource, you can easily perform queries in the event database to analyze resource problems using the complete and detailed information available for each recorded event.

Console Features

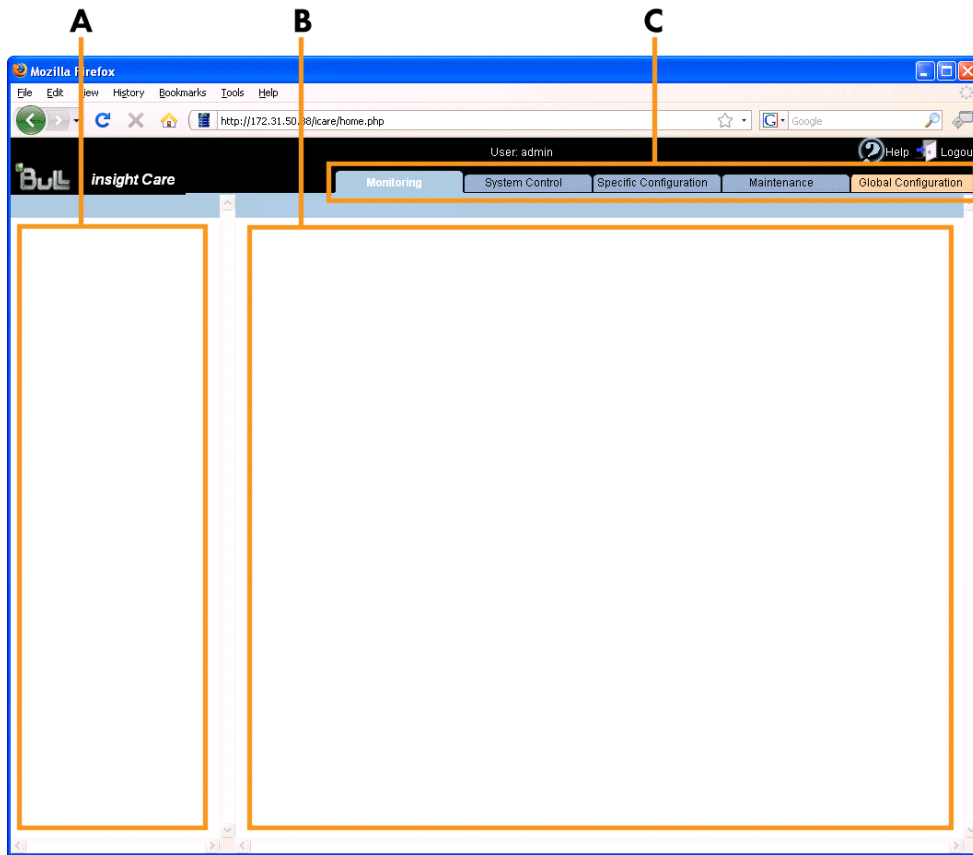
The following table lists the features available from the interface and their related sections in this guide.

Features
<p>Manually Importing Multiple Hardware Resources, on page 2-4</p> <ul style="list-style-type: none"> • Automatic discovery of hardware resources for resources in the same subnetwork • Import of hardware resources using XML files, from clusterDB for example • Manual import
<p>Monitoring Resources, on page 4-1</p> <ul style="list-style-type: none"> • 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
<p>Building SEL Query Reports, on page 4-2</p> <ul style="list-style-type: none"> • Simple or complex query options • Query template and result saving
<p>Configuring Autocalls, on page 3-1</p> <ul style="list-style-type: none"> • Comprehensive autocall transmission policy and filter options • Autocall transmission to GTS application in XML format
<p>Enabling/Disabling the Automatic Clear SEL Policy, on page 7-8</p> <ul style="list-style-type: none"> • Automatic Clear System Event Log option <p>Connecting to a Resource Console, on page 3-1</p> <ul style="list-style-type: none"> • Direct connection to resource Web consoles • Serial Over LAN connection to managed host serial console <p>Managing Intervention Reports and Action Requests, on page 6-1</p> <ul style="list-style-type: none"> • Intervention report generation

Table 1. Console features and related sections

Interface Structure

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

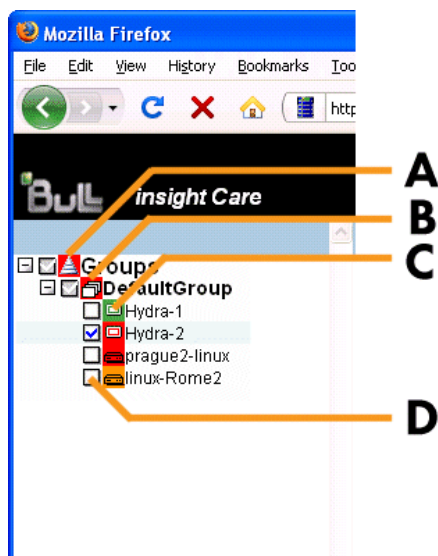


Interface Structure	
A: Tree pane	<p>The Tree pane is tab-dependent:</p> <ul style="list-style-type: none"> • When a blue tab is selected, the Tree pane displays the Resource tree. • When the orange tab is selected, the Tree pane displays the Navigation tree.
B: Work pane	<p>The Work pane is tab-dependent:</p> <ul style="list-style-type: none"> • 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	<p>Four tabs are available and are organized by color:</p> <ul style="list-style-type: none"> • The Monitoring, 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 2. Interface Structure

The Resource Tree

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



Resource Tree	
<p>Each item in the Resource tree is associated with an icon that indicates the current status of the monitored hardware resource:</p> <ul style="list-style-type: none"> • 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	<p>The Global status icon is located on the root node and allows you to check all monitored resources at a glance:</p> <ul style="list-style-type: none"> • 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	<p>The Group status icon allows you to check all the monitored resources in the group at a glance:</p> <ul style="list-style-type: none"> • 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	<p>The Resource status icon indicates the current status of the selected resource.</p>
D: Check box	<p>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).</p>

Figure 3. Resource tree

Menu Bar

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



Figure 4. Menu Bar location

1.3. Initial Configuration

When you start the iCare Console for the first time, just after installation, you have to perform a few configuration tasks to ensure correct operation. These configuration tasks are explained in detail in *Performing Other Configuration Tasks*, on page 7-1, and are listed below by order of priority:

- Setting Up the BMC Super User Password, on page 7-5
- Importing Hardware Resources, on page 2-2
- Configuring Autocalls, on page 3-1, if you have subscribed to Bull's Remote Maintenance service offer.

Note The other configuration tasks detailed in *Performing Other Configuration Tasks*, on page 7-1 can be performed when required.

1.4. Stopping the iCare Console

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

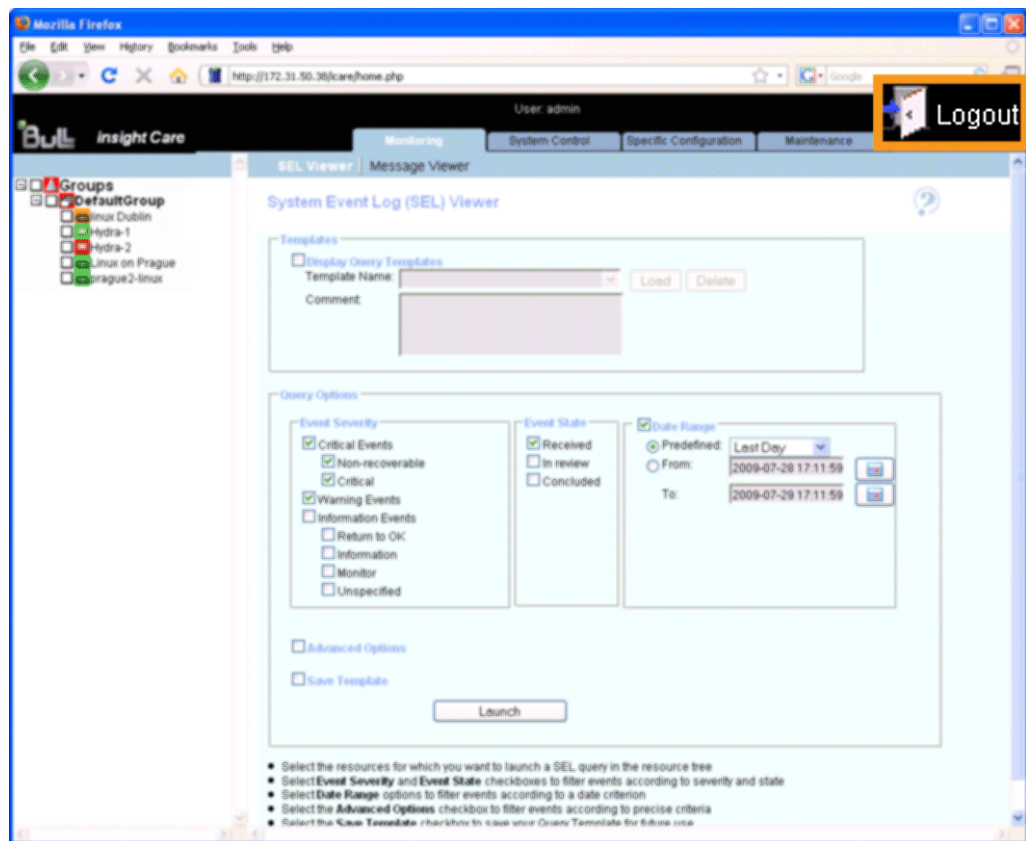


Figure 5. Logout link

Related Topics

- Starting the iCare Console, on page 1-2

Chapter 2. Managing the Resource Tree

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

- Importing Hardware Resources, on page 2-2
- Managing Imported Hardware Resources, on page 2-12
- Managing Hardware Resource Custom Groups, on page 2-22

2.1. Importing Hardware 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.

The following tasks are explained in this section:

- Automatically Importing Hardware Resources, on page 2-2
- Manually Importing Multiple Hardware Resources, on page 2-4
- Manually Importing a Single Hardware Resource, on page 2-9
- Deleting a Hardware Resource from the Tree, on page 2-19
- Enabling/Disabling Hardware Resource Monitoring, on page 2-20

Note For a graphical description of Resource tree features, see Figure 3. Resource tree, on page 1-5.

2.1.1. Automatically Importing Hardware 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.

To date, the following resources can be automatically discovered:

- NovaScale 9006 Servers
- Cool Cabinets



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 other hardware resources, such as bullx systems, or resources outside the subnetwork, see the following sections:

- Manually Importing Multiple Hardware Resources, on page 2-4
- Manually Importing a Single Hardware Resource, on page 2-9

Prerequisites

- The same **super** user password has been set up on all the hardware resources you want to discover and monitor from the iCare Console, as detailed in Setting Up the BMC Super User Password, on page 7-5.
- The hardware resources you want to discover and monitor are on the same subnetwork as the iCare Console.
- The hardware resources you want to discover and monitor are compatible with the automatic discovery feature.

Procedure

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

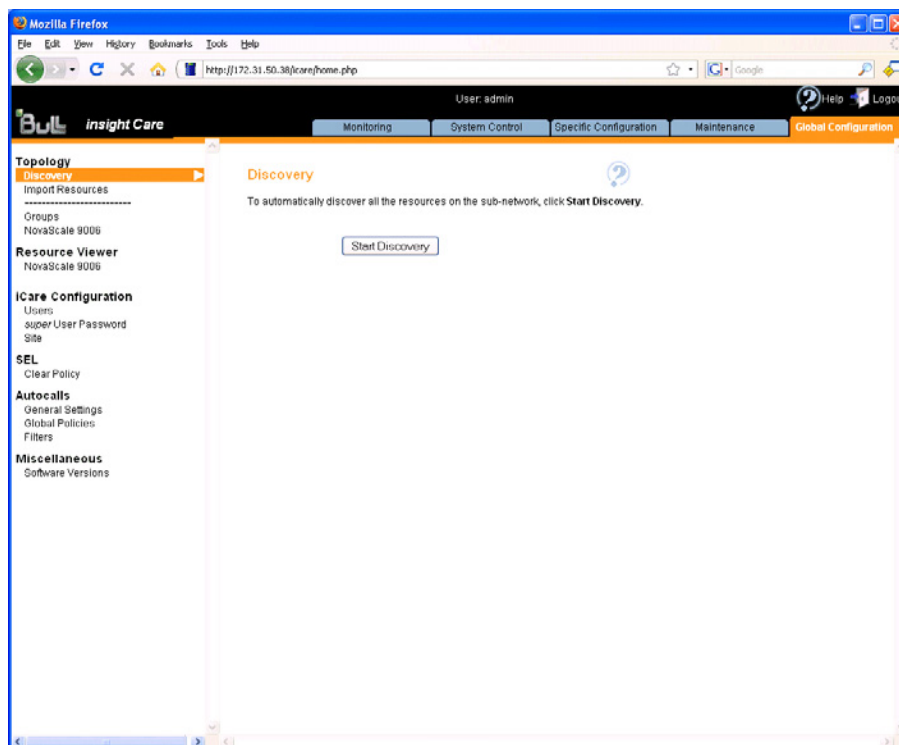


Figure 6. Discovery page

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

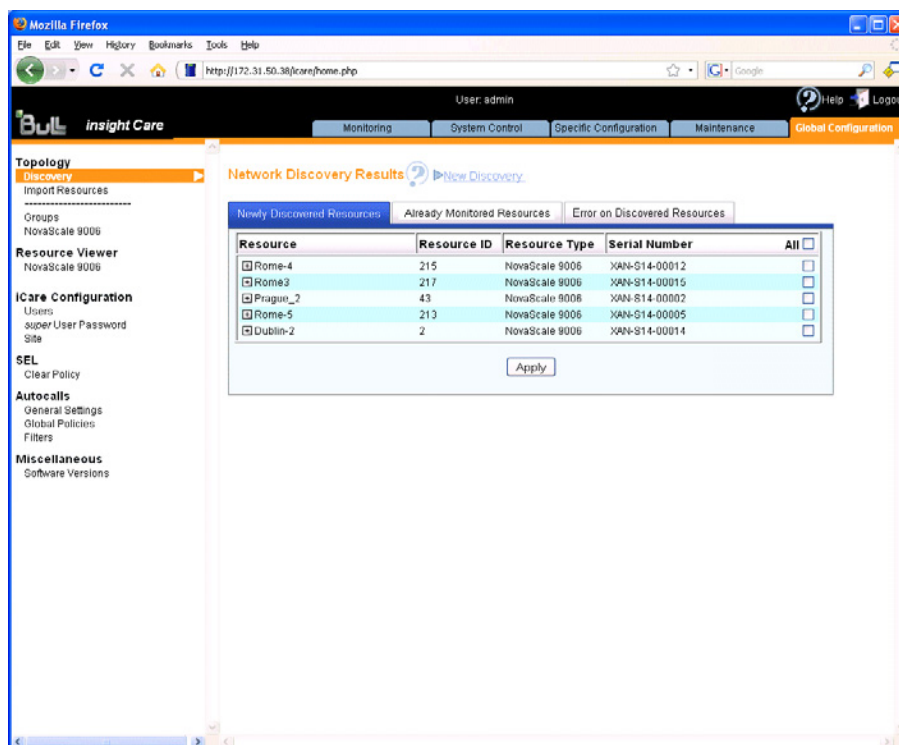


Figure 7. Network Discovery Results page - Multiple Resources

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

Note For more information about the **Network Discovery Results** page, see **Managing Imported Hardware Resources**, on page 2-12.

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

Related Topics

- [Managing Imported Hardware Resources](#), on page 2-12
- [Using an XML File to Import Multiple Hardware Resources](#), on page 2-7
- [Manually Importing a Single Hardware Resource](#), on page 2-9
- [Managing Hardware Resource Custom Groups](#), on page 2-22
- [Connecting to a Resource Console](#), on page 3-1

2.1.2. Manually Importing Multiple Hardware 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. Templates are currently available for the following hardware resources:

- NovaScale 9006 Servers
- bullx systems
- Cool Cabinets



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 Hardware Resources](#), on page 2-2.

2.1.2.1. Creating a Hardware Resource XML Import File

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

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

Prerequisites

- You have the information required to complete the XML import template file fields, as detailed in [Table 2. XML import template file data](#), on page 2-6.

Procedure

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

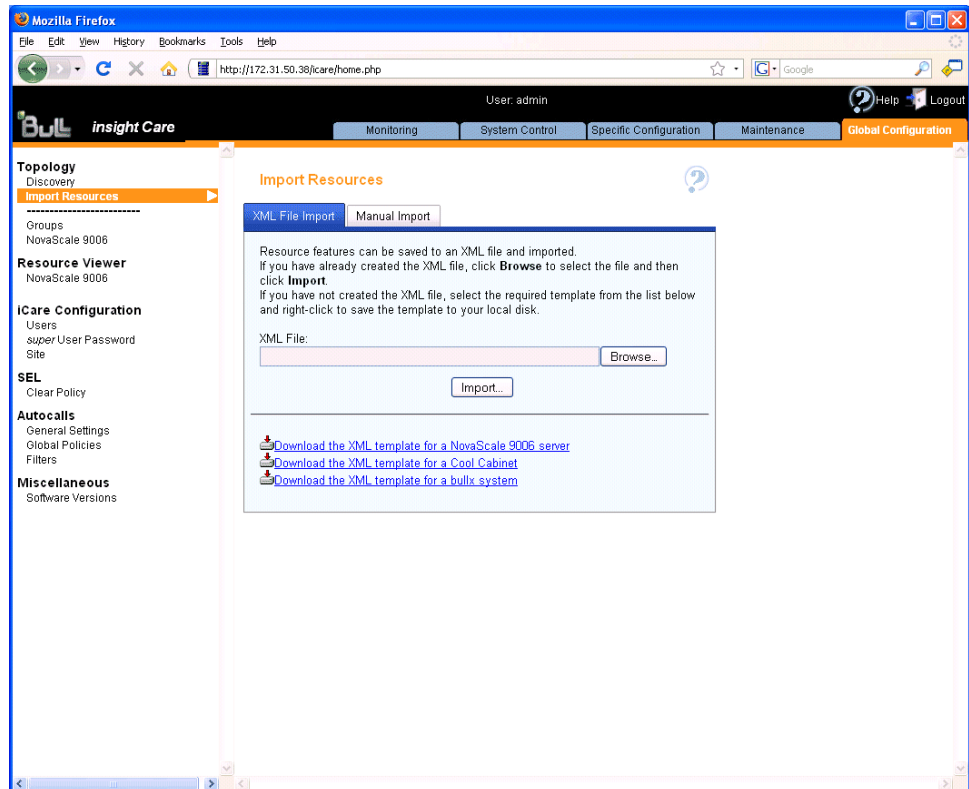


Figure 8. Import Resources page - XML File Import tab

3. Right-click the link corresponding to the XML template file you want to download and select Save link as (Firefox) or Save target as (Internet Explorer).
4. Open the saved XML template file with Notepad. The following figure shows an example of an XML template file opened with Notepad:

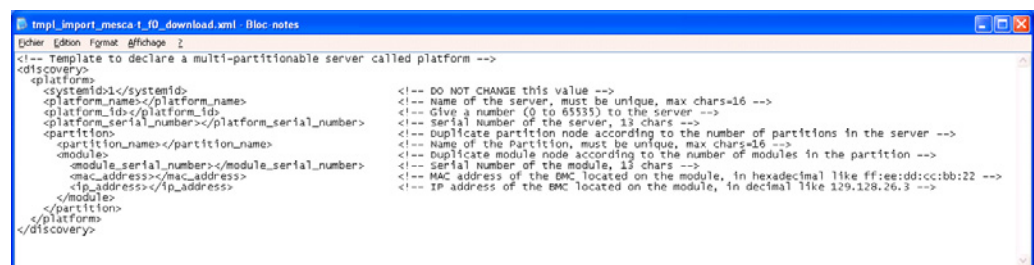


Figure 9. XML template file - NovaScale 9006 Server example

5. Edit the file by reading the XML comments (example: <!-- DO NOT CHANGE this value -->). The following table details the information you need to complete the XML template files, according to hardware resource type. This information can be found by connecting to the corresponding resource Hardware Console.

XML Tag	System	Required Value
<discovery>	All	None
<platform>	All	None

XML Tag (continued)	System (continued)	Required Value (cont'd)
<systemid>	All	None
<platform_name>	All	Unique system name (max. 16 characters).
<platform_id>	NovaScale 9006 Servers	Unique identification number (between 0 and 65535).
	bullx systems	None
<platform_serial_number>	All	System serial number (13 characters).
<mac_address>	Cool Cabinets	BMC MAC address.
	bullx systems	CMC network MAC address (bullx chassis).
<ip_address>	Cool Cabinets	BMC IP address.
	bullx systems	CMC network IP address (bullx chassis)
<partition>	NovaScale 9006 Servers bullx systems	None
<partition_name>	NovaScale 9006 Servers bullx systems	Unique Managed server name (max. 16 char.).
<module>	NovaScale 9006 Servers bullx systems	None
<module_serial_number>	NovaScale 9006 Servers bullx systems	Module serial number (13 characters).
<mac_address>	NovaScale 9006 Servers bullx systems	Module BMC MAC address.
<ip_address>	NovaScale 9006 Servers bullx systems	Module BMC IP address.

Table 2. XML import template file data

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 Hardware Resources*, on page 2-7.

Related Topics

- *Using an XML File to Import Multiple Hardware Resources*, on page 2-7
- *Manually Importing a Single Hardware Resource*, on page 2-9
- *Managing Hardware Resource Custom Groups*, on page 2-22
- *Connecting to a Resource Console*, on page 3-1

2.1.2.2. Using an XML File to Import Multiple Hardware Resources

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

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

Prerequisites

- The same **super** user password has been set up on all the hardware resources you want to import and monitor from the iCare Console, as detailed in Setting Up the BMC Super User Password, on page 7-5.
- The required hardware resource XML import file has been created, as explained in Creating a Hardware Resource XML Import File, on page 2-4.

Procedure

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

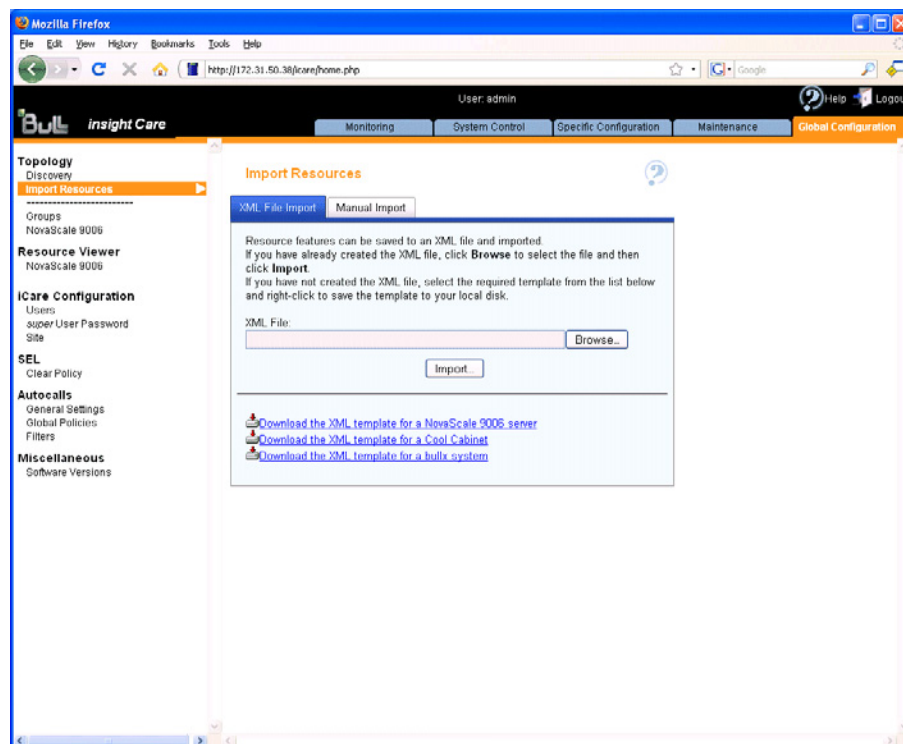


Figure 10. Import Resources page - XML File Import tab

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

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

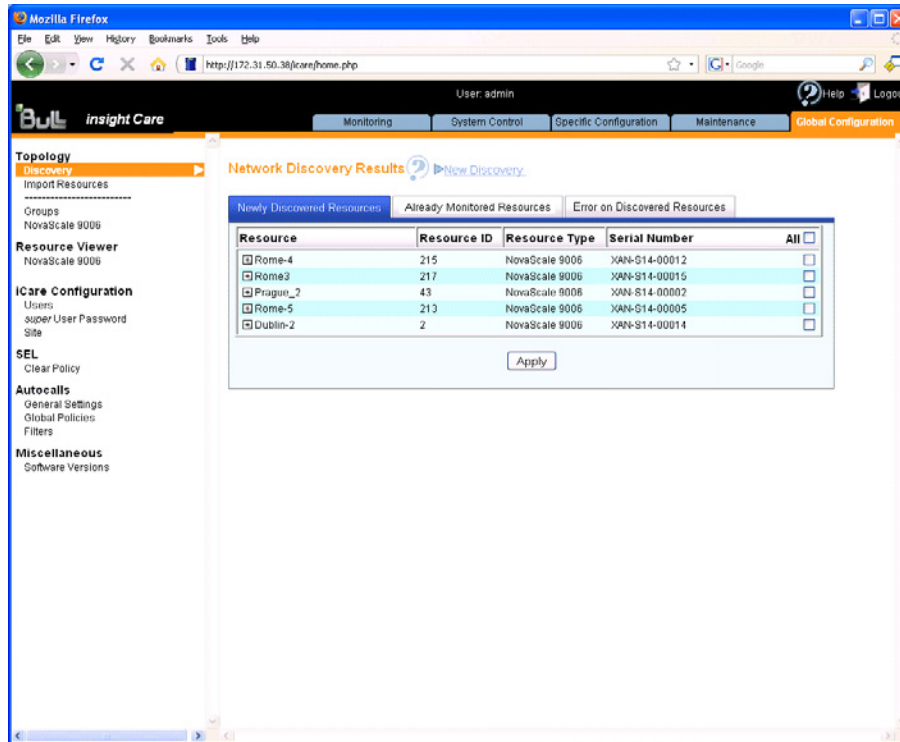


Figure 11. Network Discovery Results page - Multiple Resources

- 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 Hardware Resources*, on page 2-12.

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

Related Topics


- *Managing Imported Hardware Resources*, on page 2-12
- *Creating a Hardware Resource XML Import File*, on page 2-4
- *Automatically Importing Hardware Resources*, on page 2-2
- *Manually Importing a Single Hardware Resource*, on page 2-9
- *Managing Hardware Resource Custom Groups*, on page 2-22
- *Connecting to a Resource Console*, on page 3-1

2.1.3. Manually Importing a Single Hardware 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.

To date, the following hardware resources can be added to the Resource tree using the manual import feature:

- NovaScale 9006 Servers
- Cool Cabinets

 **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 Hardware Resources](#), on page 2-2.

Prerequisites

- The same super user password has been set up on all the resources you want to import and monitor, as detailed in [Setting Up the BMC Super User Password](#), on page 7-5.

Procedure

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

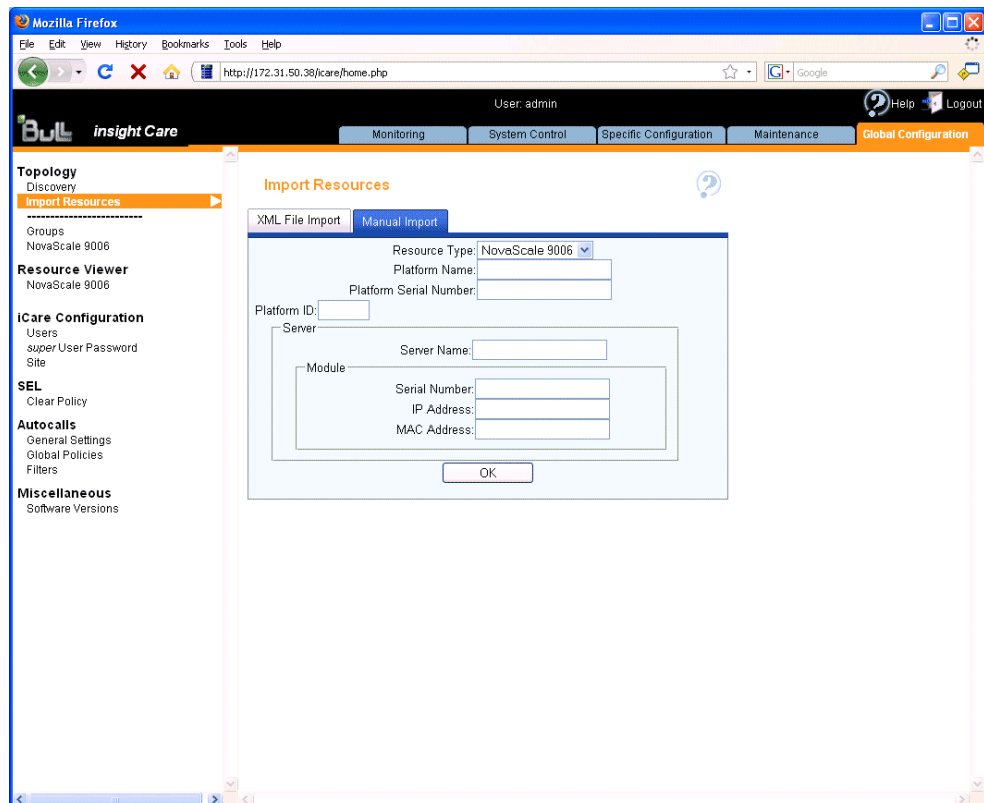


Figure 12. Import Resources page - Manual Import tab

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

Manual Import - NovaScale 9006 Servers	
Platform Name	NovaScale 9006 platform name - 16 characters maximum.
Platform Serial Number	NovaScale 9006 platform serial number - 13 characters.
Platform ID	NovaScale 9006 platform ID - Value between 0 and 65535.
Server Name	NovaScale 9006 server name - 16 characters maximum.
Serial Number	Module serial number - 13 characters
IP Address	IP address of the Module Baseboard Management Controller (BMC) - decimal values (example: 129.192.1.10)
MAC Address	Module MAC address - hexadecimal values (example: 5E:FF:56:A2:AF:15)
Manual Import - Cool Cabinets	
Name	Cool Cabinet name - 16 characters maximum.
Serial Number	Cool Cabinet serial number - 13 characters
IP Address	Cool Cabinet static IP address of the Baseboard Management Controller (BMC) - decimal values (example: 129.192.1.10)
MAC Address	Cool Cabinet MAC address of the Baseboard Management Controller (BMC) - hexadecimal values (example: 5E:FF:56:A2:AF:15)

Table 3. Manual import data

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

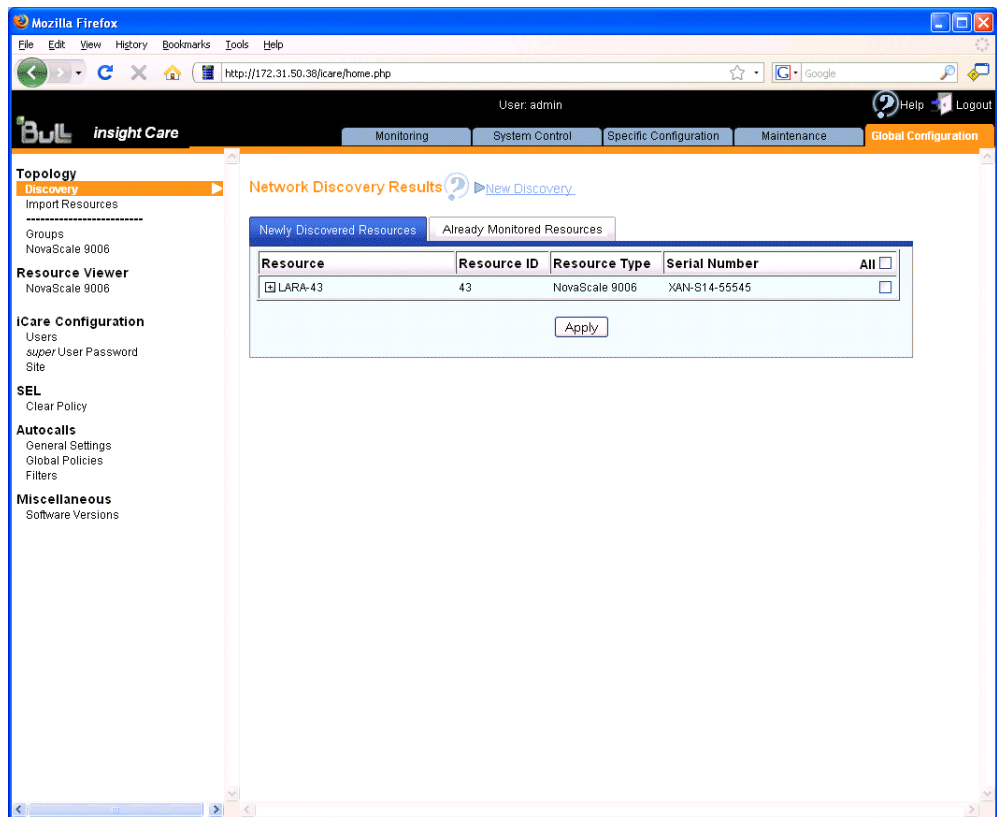


Figure 13. Network Discovery Results page - Single Resource

5. Select the resource and click Apply.

Note For more information about the Network Discovery Results page, see *Managing Imported Hardware Resources*, on page 2-12.

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

Related Topics

- *Managing Imported Hardware Resources*, on page 2-12
- *Automatically Importing Hardware Resources*, on page 2-2
- *Using an XML File to Import Multiple Hardware Resources*, on page 2-7
- *Managing Hardware Resource Custom Groups*, on page 2-22
- *Connecting to a Resource Console*, on page 3-1

2.2. Managing Imported Hardware Resources

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

- [Automatically Importing Hardware Resources](#), on page 2-2
- [Using an XML File to Import Multiple Hardware Resources](#), on page 2-7
- [Manually Importing a Single Hardware Resource](#), on page 2-9

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

- [Adding Newly Discovered Resources to the Resource Tree](#), on page 2-12
- [Viewing Already Monitored Resources](#), on page 2-14
- [Troubleshooting Errors on Discovered Resources](#), on page 2-15

2.2.1. Adding Newly Discovered Resources to the Resource Tree

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

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

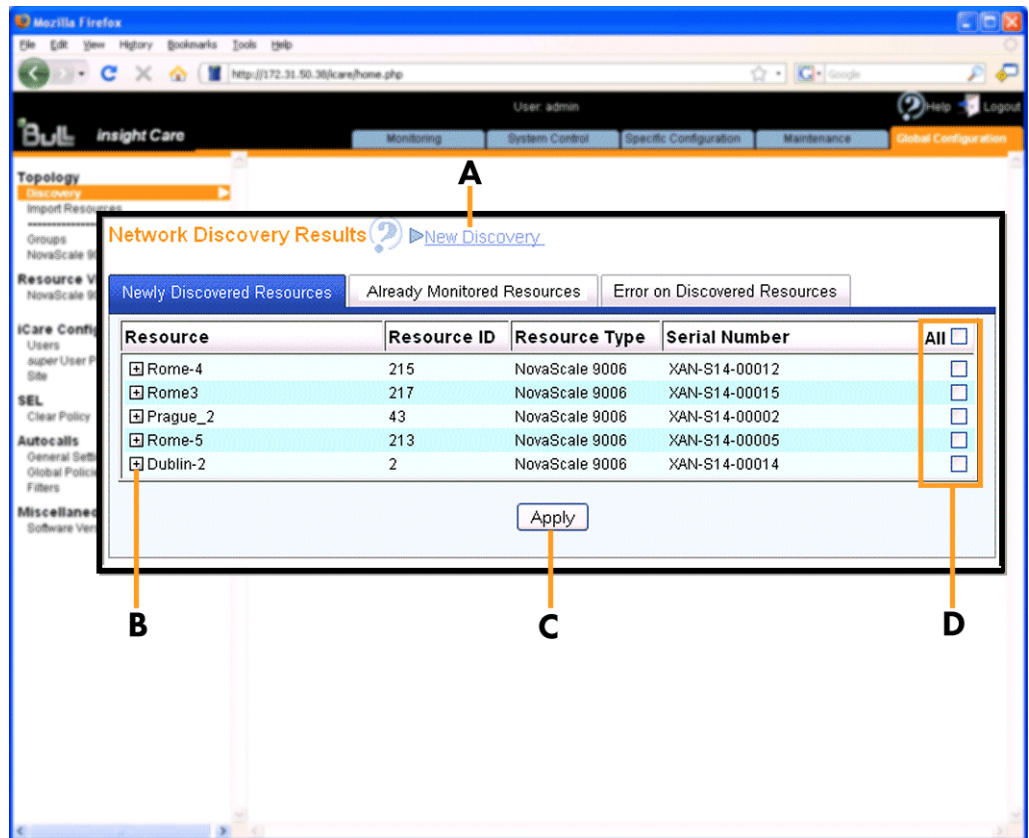
Prerequisites

- You have imported hardware resources using one of the import methods explained in [Importing Hardware Resources](#), on page 2-2.

Procedure

1. When the **Network Discovery Results** page appears displaying the results of the import procedure previously launched, open the **Newly Discovered Resources** tab.

2. Select the hardware resources you want to add to the Resource tree and monitor, as explained in the table below.



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

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

Related Topics

- Viewing Already Monitored Resources, on page 2-14
- Troubleshooting Errors on Discovered Resources, on page 2-15

2.2.2. Viewing Already Monitored Resources

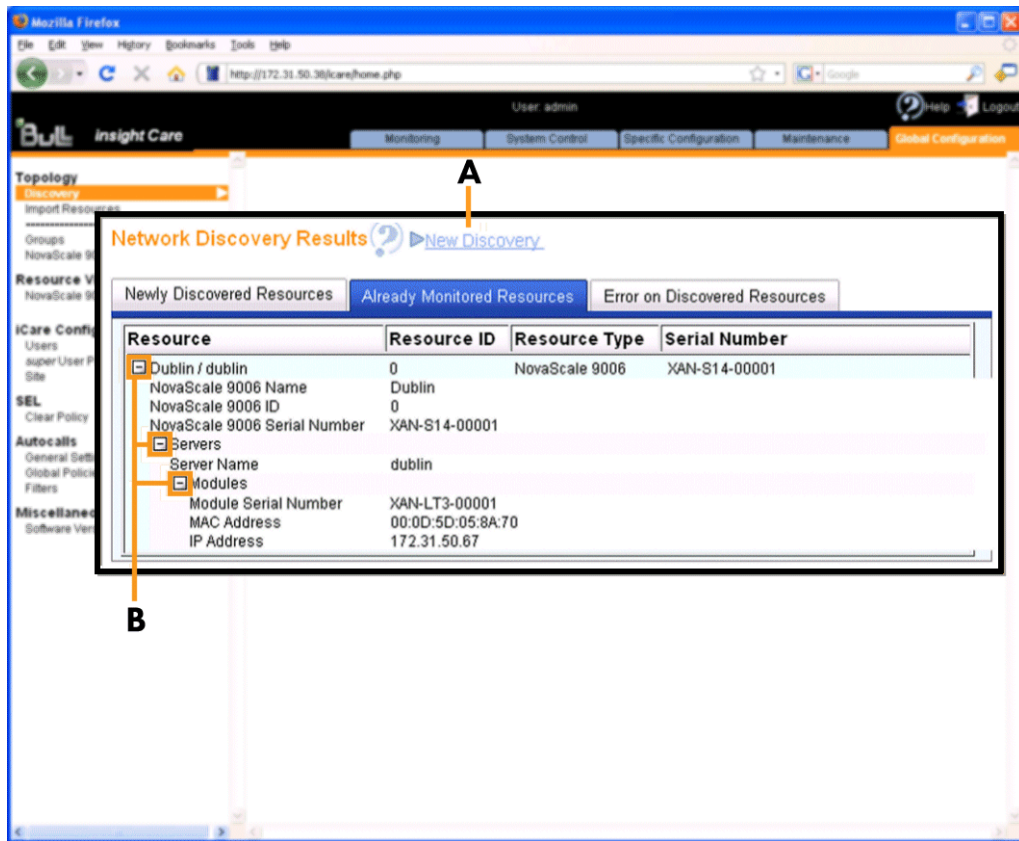
When hardware resources that are already monitored are re-discovered, they are displayed under the **Already Monitored Resources** tab in the **Network Discovery Results** page, allowing you to view detailed information about these resources.

Prerequisites

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

Procedure

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



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

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

Related Topics

- Adding Newly Discovered Resources to the Resource Tree, on page 2-12
- Troubleshooting Errors on Discovered Resources, on page 2-15

2.2.3. Troubleshooting Errors on Discovered Resources

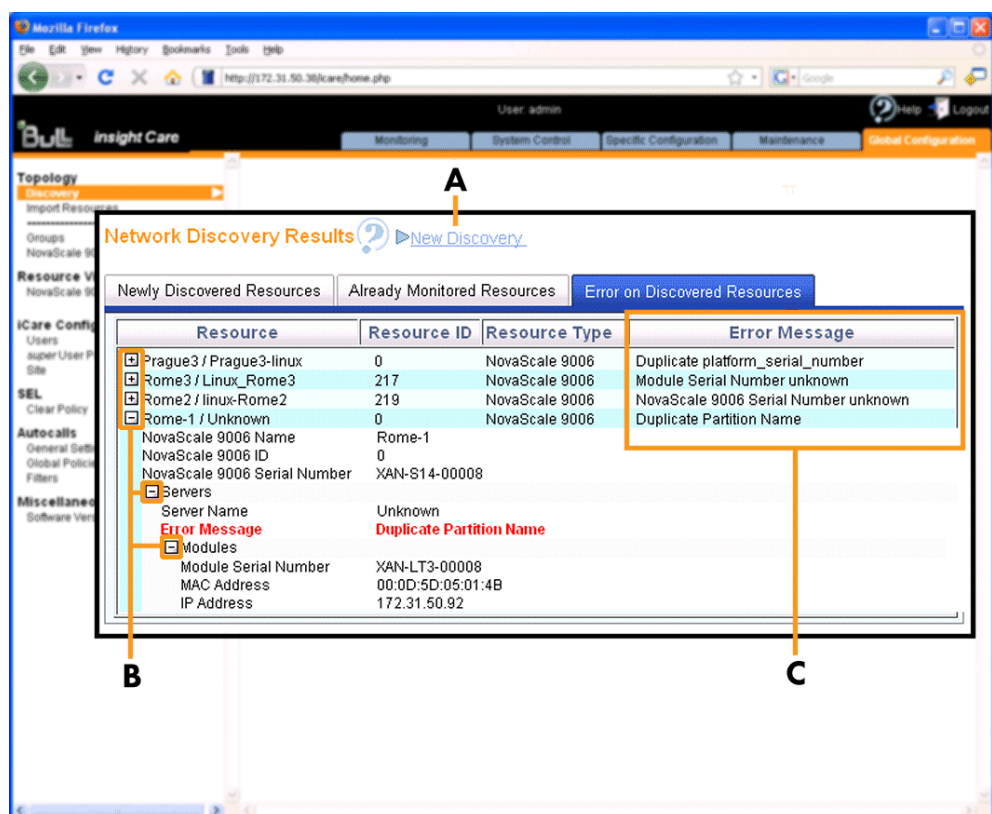
When hardware resources are discovered but cannot be imported, they are displayed under the Error on Discovered Resources tab in the Network Discovery Results page, allowing you to easily troubleshoot discovery errors.

Prerequisites

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

Procedure

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



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

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

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

Discovery Error Messages and Troubleshooting Actions

Message	Duplicate partition name
Resource Type	<ul style="list-style-type: none"> NovaScale 9006 Servers bullx systems
Description	2 (or more) resources use the same partition name
Actions	<ul style="list-style-type: none"> 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 4. Duplicate partition name error

Message	Duplicate platform name
Resource Type	<ul style="list-style-type: none"> NovaScale 9006 Servers Cool Cabinets bullx systems
Description	2 (or more) resources use the same platform name
Actions	<ul style="list-style-type: none"> 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 5. Duplicate platform name error

Message	Duplicate platform ID
Resource Type	<ul style="list-style-type: none"> NovaScale 9006 Servers bullx systems
Description	2 (or more) resources use the same platform ID
Actions	<ul style="list-style-type: none"> 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 6. Duplicate platform ID error

Message	Duplicate platform serial number
Resource Type	<ul style="list-style-type: none"> • NovaScale 9006 Servers • Cool Cabinets • bullx systems
Description	2 (or more) resources use the same platform serial number
Actions	<ul style="list-style-type: none"> • XML File Import - typing error: change the resource <code><platform_serial_number></code> 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 7. Duplicate platform serial number error

Message	Duplicate module serial number
Resource Type	<ul style="list-style-type: none"> • NovaScale 9006 Servers • bullx systems
Description	2 (or more) resources use the same module serial number
Actions	<ul style="list-style-type: none"> • XML File Import - typing error: change the resource <code><module_serial_number></code> XML tag value, then re-import the XML file. • Manual Import - typing error: re-import the resource. • If this is not a typing error, contact your Customer Service Engineer.

Table 8. Duplicate module serial number error

Message	Module serial number unknown
Resource Type	<ul style="list-style-type: none"> • NovaScale 9006 Servers • bullx systems
Description	The module serial number is not engraved.
Actions	Contact your Customer Service Engineer.

Table 9. Module serial number unknown error

Message	Module count does not match the number of modules
Resource Type	<ul style="list-style-type: none"> • NovaScale 9006 Servers • bullx systems
Description	The number of <code><module></code> <code><\module></code> XML tags is not correct.
Actions	Change the number of <code><module></code> <code><\module></code> XML tags, then re-import the file.

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

Message	Duplicate MAC address
Resource Type	<ul style="list-style-type: none"> • NovaScale 9006 Servers • Cool Cabinets • bullx systems
Description	2 (or more) resources use the same MAC address
Actions	<ul style="list-style-type: none"> • XML File Import - typing error: change the resource <mac_address> (platform or module) XML tag value, then re-import the XML file. • Manual Import - typing error: re-import the resource. • If this is not a typing error, contact your Customer Service Engineer.

Table 11. Duplicate MAC address error

Message	Duplicate IP address
Resource Type	<ul style="list-style-type: none"> • NovaScale 9006 Servers • Cool Cabinets • bullx systems
Description	2 (or more) resources use the same IP address
Actions	<ul style="list-style-type: none"> • XML File Import - typing error: change the resource <ip_address> (platform or module) XML tag value, then re-import the XML file. • Manual Import - typing error: re-import the resource. • If this is not a typing error, contact your Network administrator.

Table 12. Duplicate IP address error

Related Topics

- [Adding Newly Discovered Resources to the Resource Tree](#), on page 2-12
- [Viewing Already Monitored Resources](#), on page 2-14

2.2.4. Deleting a Hardware Resource from the Tree

When you no longer want to monitor a hardware resource from the iCare Console, you can delete it from the Resource tree.



WARNING

When a hardware resource is deleted from the Resource tree, all associated events are no longer available for consultation.

Prerequisites

- The hardware resource is present in the Resource tree.

Procedure

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

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

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

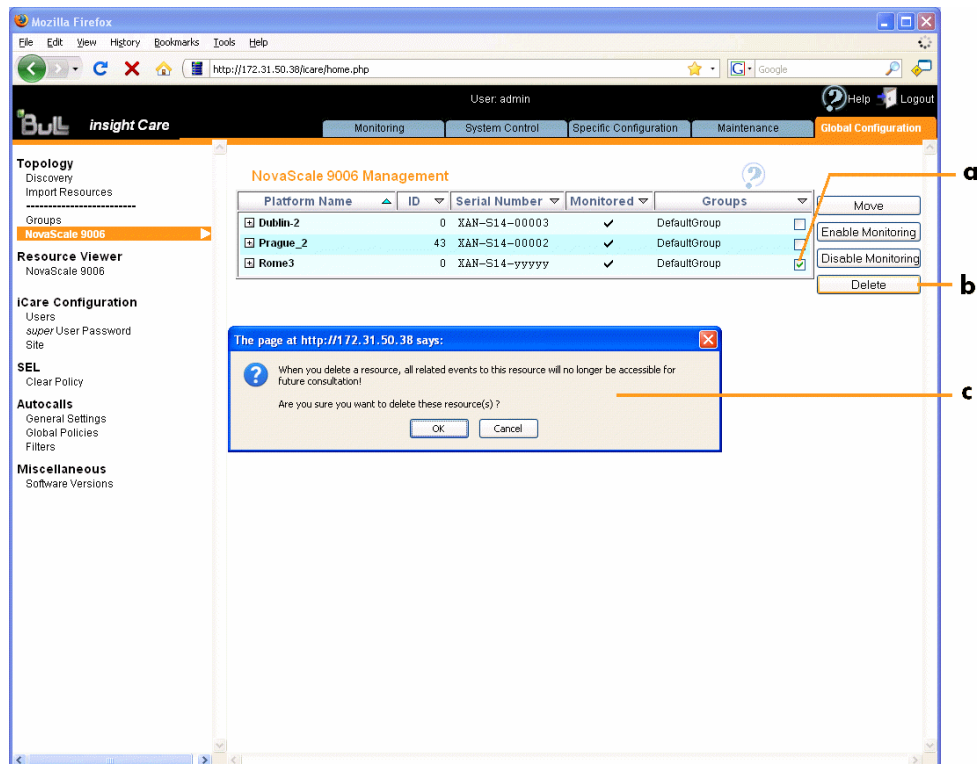


Figure 17. Deleting a Resource

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

Related Topics

- Adding a Hardware Resource to a Resource Group, on page 2-27
- Enabling/Disabling Hardware Resource Monitoring, on page 2-20

2.2.5. Enabling/Disabling Hardware Resource Monitoring

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 (which records events compliant with the IPMI standard, in particular those concerning power supplies, FANs, temperature sensors) and the Board and Security Messages log (which records non-IPMI events, such as power-on errors, user authentication, security violation or firmware upgrade) are enabled.

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



Important When monitoring is disabled for a hardware resource, it disappears from the Resource tree and events are no longer recorded in the SEL and Board and Security Messages. Events recorded when the hardware resource was monitored remain in the iCare Console database. To consult them, you must re-enable monitoring for the hardware resource.

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 re-starts.

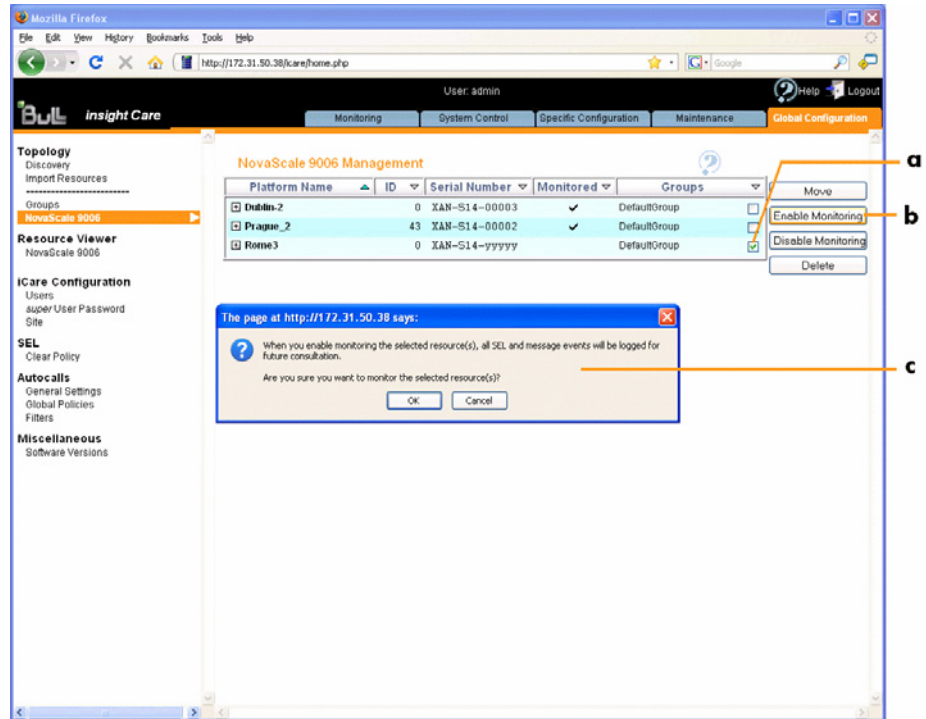


Figure 18. Enabling Resource Monitoring

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

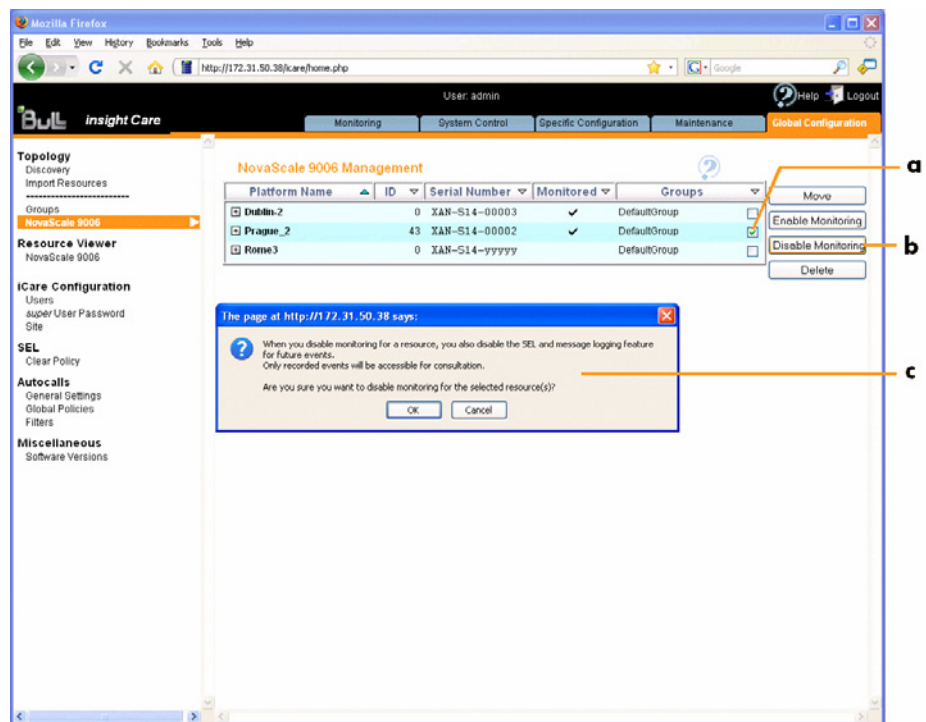


Figure 19. Disabling Resource Monitoring

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

Related Topics

- Adding a Hardware Resource to a Resource Group, on page 2-27
- Deleting a Hardware Resource from the Tree, on page 2-19

2.3. Managing Hardware 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 renamed 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 Hardware Resource Custom Group, on page 2-22
- Editing Hardware Resource Custom Group Details, on page 2-24
- Deleting a Hardware Resource Custom Group, on page 2-26
- Adding a Hardware Resource to a Resource Group, on page 2-27

Note For a graphical description of Resource tree features, refer to Figure 3. Resource tree, on page 1-5.

2.3.1. Creating a Hardware Resource Custom Group

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

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

Prerequisites

- None.

Procedure

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

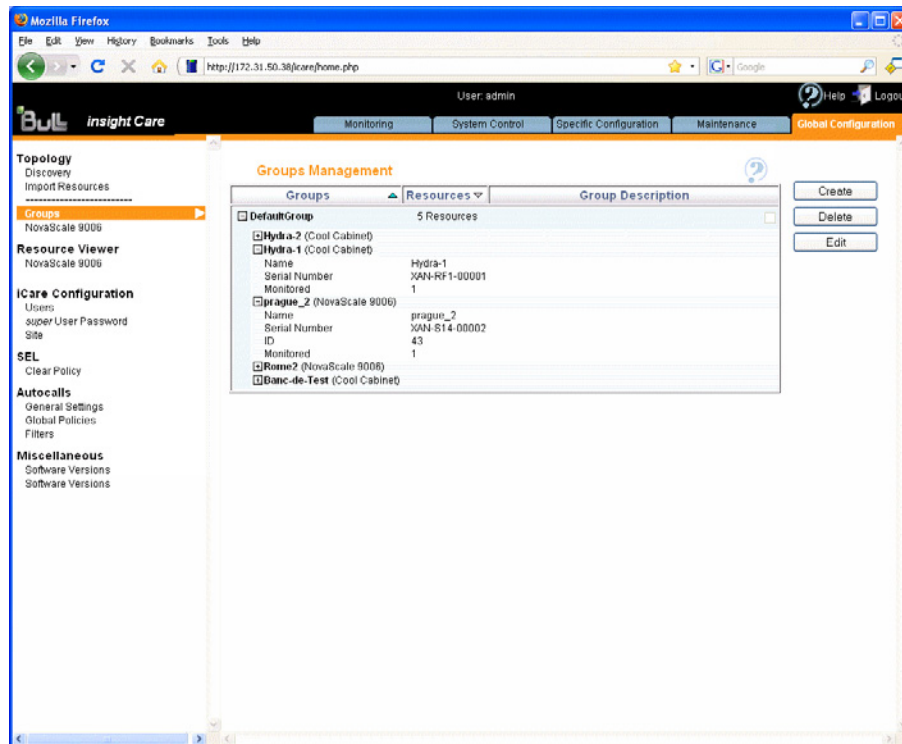
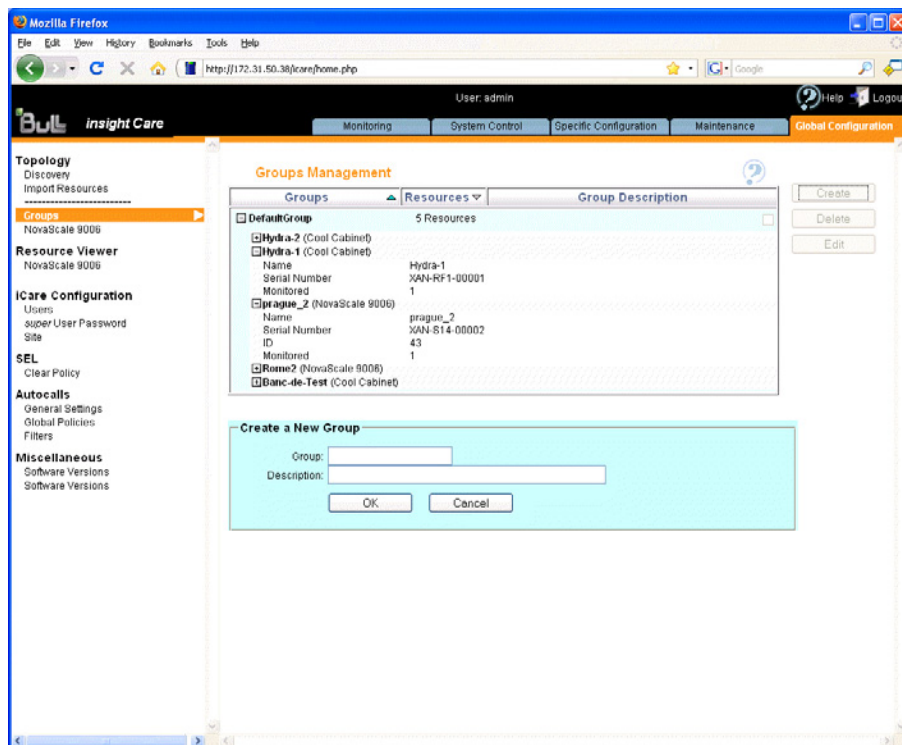


Figure 20. Groups Management page

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



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

Figure 21. Create a New Group box

3. Click OK. The group appears in the **Groups Management** page.
4. You can now associate hardware resources with the new group. See **Adding a Hardware Resource to a Resource Group**, on page 2-27.

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

Related Topics

- [Editing Hardware Resource Custom Group Details](#), on page 2-24
- [Deleting a Hardware Resource Custom Group](#), on page 2-26
- [Adding a Hardware Resource to a Resource Group](#), on page 2-27
- [Manually Importing Multiple Hardware Resources](#), on page 2-4

2.3.2. Editing Hardware Resource Custom Group Details

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

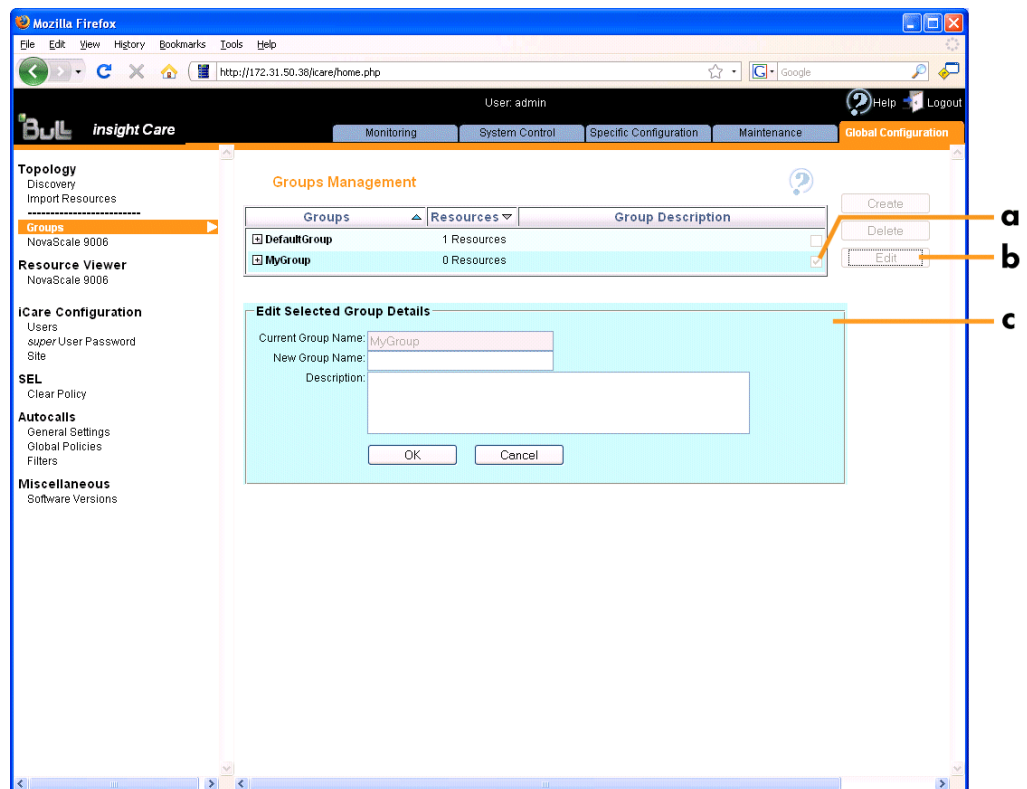
Note The predefined group `DefaultGroup` cannot be edited.

Prerequisites

- None.

Procedure

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



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

Figure 22. Edit Selected Group Details box

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

Related Topics

- Manually Importing Multiple Hardware Resources, on page 2-4
- Deleting a Hardware Resource Custom Group, on page 2-26
- Creating a Hardware Resource Custom Group, on page 2-22

2.3.3. Deleting a Hardware Resource Custom Group

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

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

Prerequisites

- None.

Procedure

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

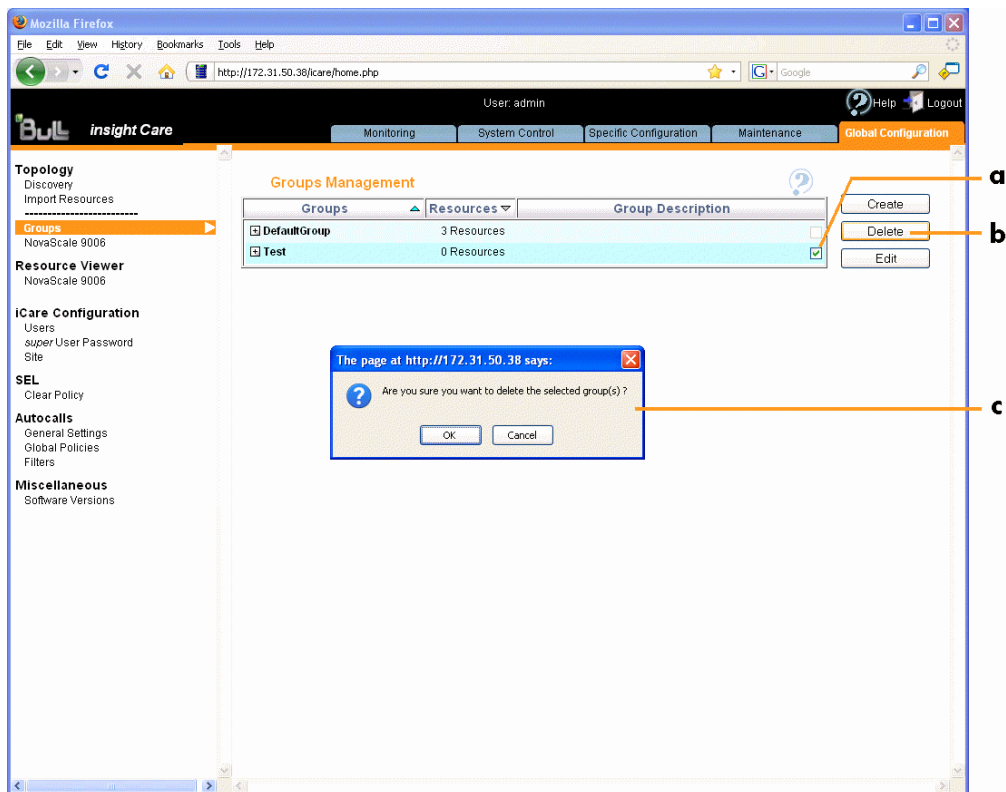


Figure 23. Groups Management page - Group deletion

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

Related Topics

- Creating a Hardware Resource Custom Group, on page 2-22
- Editing Hardware Resource Custom Group Details, on page 2-24

2.3.4. Adding a Hardware Resource to a Resource Group

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

Prerequisites

- At least one custom group is created (for details, see [Creating a Hardware Resource Custom Group](#), on page 2-22).

Procedure

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

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

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

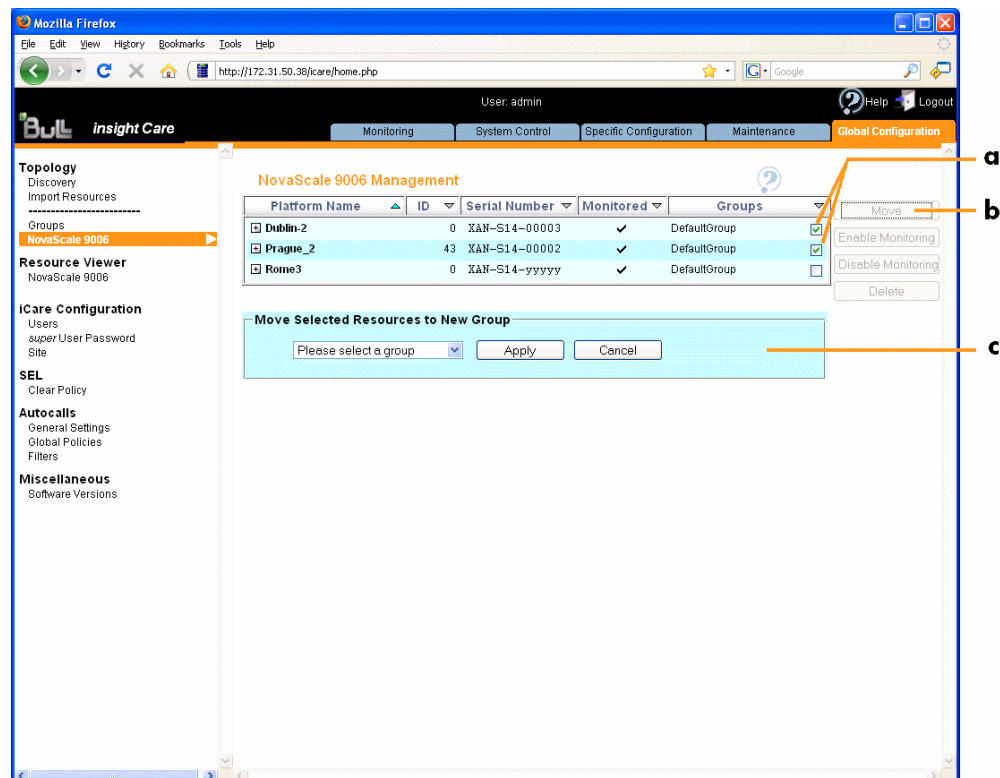


Figure 24. Moving Resources (example with Novascale 9006 servers)

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

Related Topics

- [Managing Hardware Resource Custom Groups](#), on page 2-22
- [Enabling/Disabling Hardware Resource Monitoring](#), on page 2-20
- [Deleting a Hardware Resource from the Tree](#), on page 2-19

Chapter 3. Connecting to a Resource Console

Resource consoles can be started directly from the iCare Console through the System Control tab. You can connect to three types of consoles:

- Hardware Consoles, which are web-based administration applications embedded on an electronic board.

Notes For information on how to use hardware consoles, refer to:

- *NovaScale 9006 Server Hardware Console User's Guide*
 - *Cool Cabinet Console User's Guide*
-

- Remote Consoles, which are Java Applets that allow you to remotely view, use and control the resource with the keyboard, video and mouse on your local computer. The Remote Console is a feature of Hardware Consoles.

Note The Remote Console feature is not available with the .

- Telnet Consoles, which are Java applications that allow you to connect to the resource using Telnet.

Note Telnet Consoles are not available with with the resources.

Prerequisite

In Telnet Consoles, you can either use the Command Line Protocol or launch the terminal mode (type `terminal` in the telnet console).

The Terminal mode connects you to the NovaScale 9006 Server serial device via the Management Controller.

To use the terminal mode, you must first enable the Terminal Serial Access option in the resource Hardware Console (Configuration tab, BMC Settings > Network menu).

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.

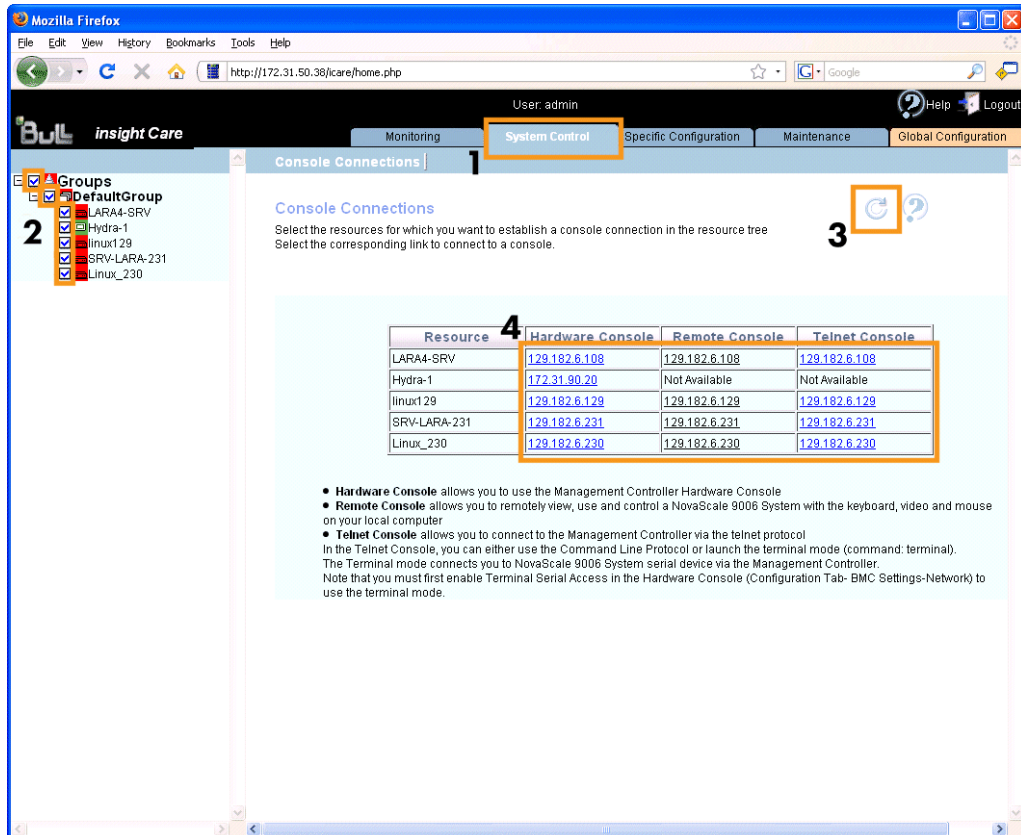


Figure 25. System Control tab

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

Related Topics

You can connect to resources Hardware Consoles through other iCare Console pages, as indicated in the following sections:

- **Managing SEL Event Status**, on page 4-7
- **Viewing Resource Details**, on page 4-10

Chapter 4. Monitoring Resources

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 SEL Query Reports, on page 4-2
- Building Messages Query Reports, on page 4-5
- Managing SEL Event Status, on page 4-7
- Viewing Resource Details, on page 4-10

4.1. Building SEL Query Reports

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 event database.

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

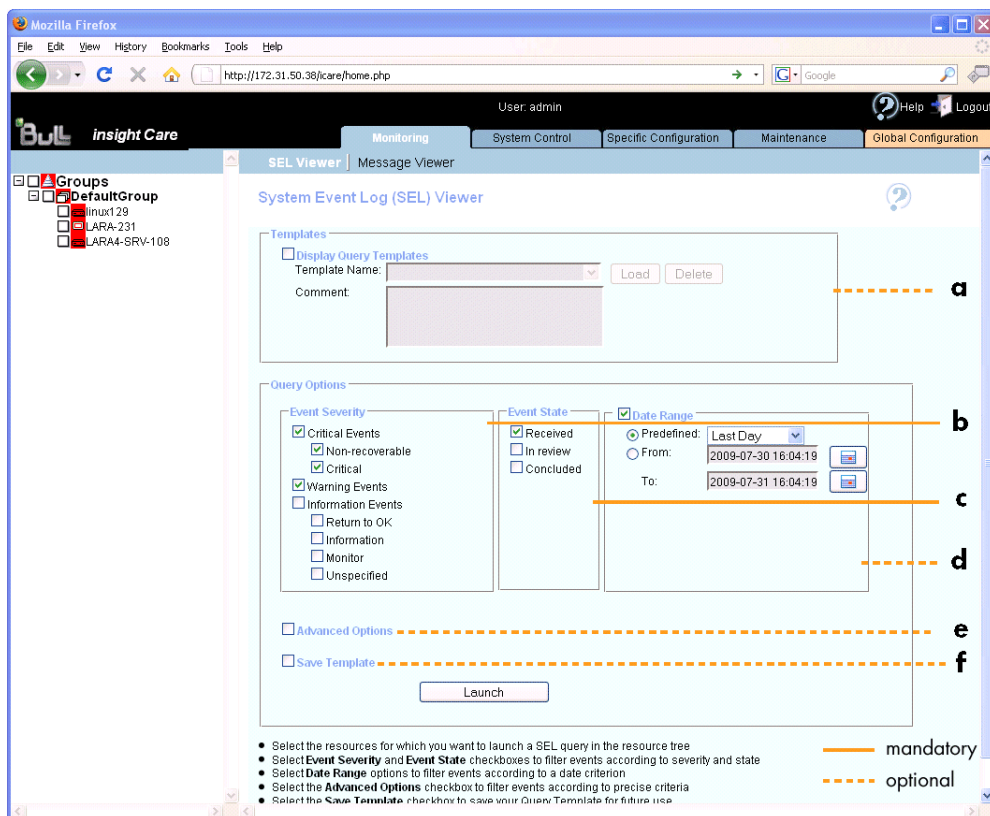
Note Each resource records IPMI-compliant events in its System Event Log (SEL) and non-IPMI-compliant information in its Board & Security Messages log. All events, whether IPMI-compliant or not, are recorded in the iCare Console event database.

Prerequisites

- The hardware resources requiring attention are present in the Resource tree.
- The same super user password has been set up on all monitored resources and in the iCare Console, as detailed in Setting Up the BMC Super User Password, on page 7-5.

Procedure

1. From the Monitoring tab, click SEL Viewer to open the Build SEL Query Report page.
2. From the Resource tree, select the resource(s) for which you want to build the SEL query report.



3. Complete the Build SEL Query Report page fields as explained in the following table:

Build SEL Query Report on Selected Resources			
a	Optional	Load query template	<ul style="list-style-type: none"> • Select the Get Query List check box. • In the Query Name drop-down list, select the query to load. • Click Load. The query parameters appear in the page. • Proceed to Step 4.
a	Optional	Delete query template	<ul style="list-style-type: none"> • Select the Get Query List check box. • In the Query Name drop-down list, select the query to delete • Click the Delete button. The query template is deleted.
b	Mandatory	Select event level filter	Select the required event level to filter as explained below: <ul style="list-style-type: none"> • CRITICAL (red) for Non-Recoverable and Critical events. • WARNING (orange) for Warning events. • INFORMATION (green) for Return to OK, Information, Monitor and Unspecified events.
c	Mandatory	Select event status filter	Select the required event status to filter as explained below: <ul style="list-style-type: none"> • Received Events awaiting investigation • In review Events under investigation • Concluded Events that are closed
d	Optional	Select event date and time	Select the the Date Range check box and fill in the appropriate fields to filter events according to a specific date and time range.
e	Optional	Select 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	Optional	Save the query template	<ul style="list-style-type: none"> • Select the Save Query check box. • Enter the name of the query in the Query Name field (limited to 16 characters. The following characters are not allowed: <code>\`&' + *%=><:;!?,~ </code> and space). • Enter a description for the query in the Comment field (optional). The query template will be saved when you launch the query.

Table 13. SEL query options

4. Click **Build Query Report**. The SEL Query Report page appears.

You can now consult and manage events as described in *Managing SEL Event Status*, on page 4-7.

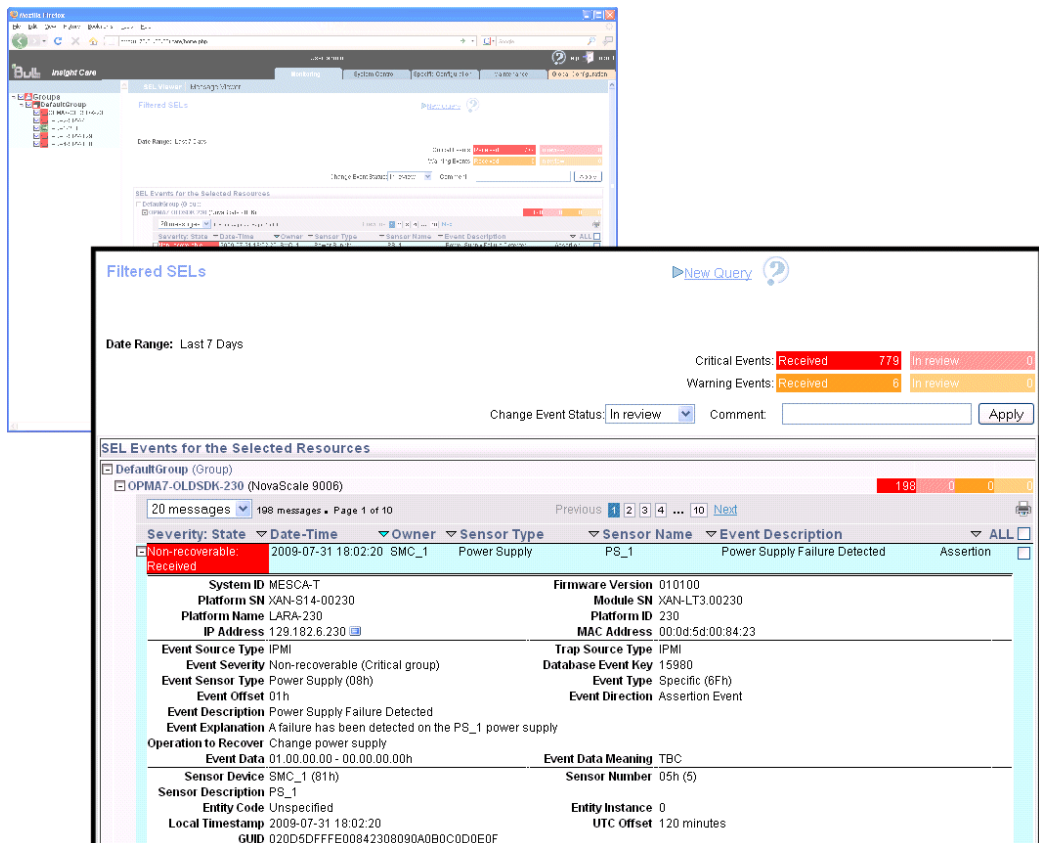


Figure 27. SEL Query Report page

Related Topics

- *Managing SEL Event Status*, on page 4-7
- *Building Messages Query Reports*, on page 4-5
- *Setting Up the BMC Super User Password*, on page 7-5
- *Manually Importing Multiple Hardware Resources*, on page 2-4

4.2. Building Messages Query Reports

Each hardware resource in the Resource tree records events, such as power-on actions and errors, user authentication, remote console connections, security violations, log deletions or firmware upgrades... This information is non-IPMI-compliant and is recorded in the resource's Board & Security Messages Log. It is also sent to the iCare Console event database.

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

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 event database.

Prerequisites

- The hardware resources requiring attention are present in the Resource tree.
- The same super user password has been set up on all monitored resources and in the iCare Console, as detailed in Setting Up the BMC Super User Password, on page 7-5.



Important Monitored hardware resources may be configured to filter the messages recorded in its Board & Security Messages Log. If this is the case, only the filtered messages are recorded in the iCare Console event database. For further information about resource messaging filters, refer to the relevant Hardware Console documentation.

Procedure

1. From the Monitoring tab, click Messages to open the Build Message Query Report page.
2. From the Resource tree, select the resource(s) for which you want to build the Message query report.

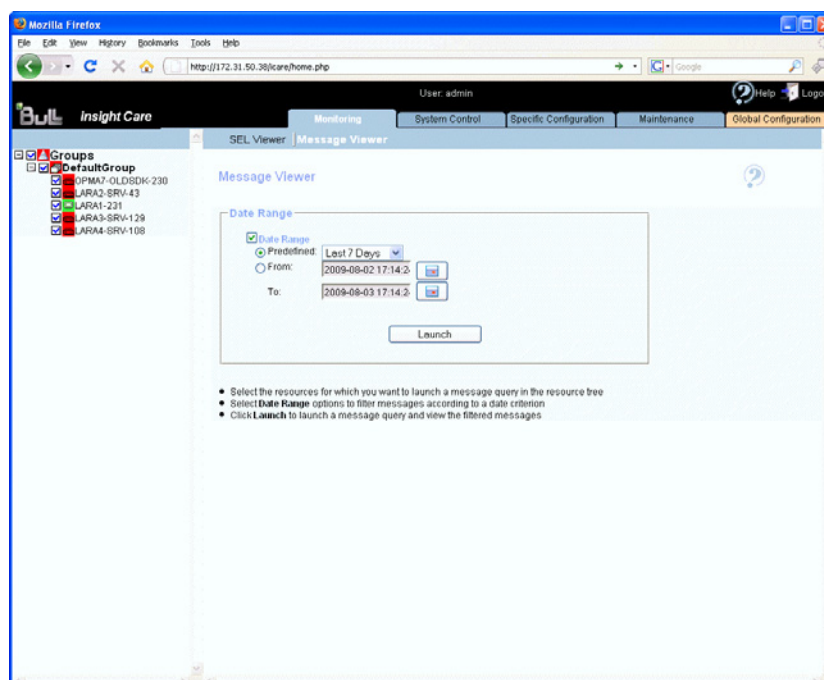


Figure 28. Build Message Query Report page

- Complete the Build Message Query Report page fields as explained in the following table:

Build Messaging Query Report on Selected Resources	
Date Range	Select this check box to filter event messages according to a specific date and time range.

Table 14. Message query options

- Click **Build Query**. The Message Query Report page appears allowing you to consult messages.

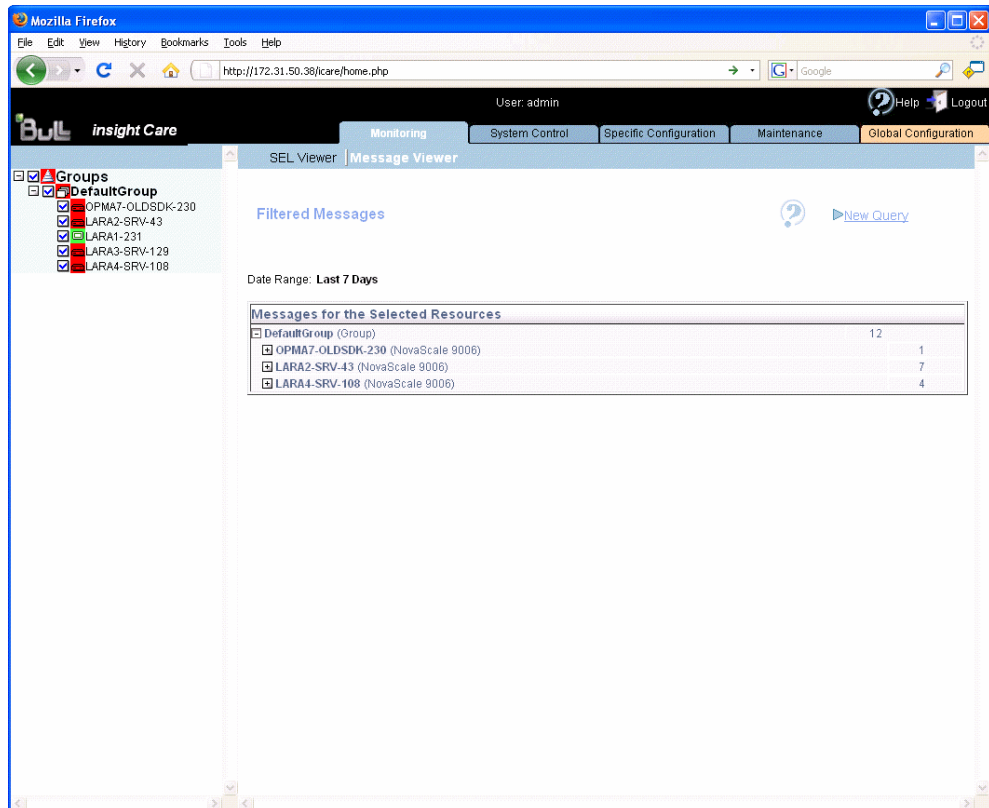


Figure 29. Message Query Report page

Related Topics

- Building Messages Query Reports, on page 4-5
- NovaScale 9006 Server Hardware Console User's Guide*
- Cool Cabinet Console User's Guide*

4.3. Managing SEL Event Status

The iCare Console provides a SEL event tracking feature to help you monitor, analyze and troubleshoot hardware failures.

Prerequisites

- None

Procedure

1. Launch a SEL query as explained in Building SEL Query Reports, on page 4-2.
By default, the SEL Query Report page lists the resources with SEL events.

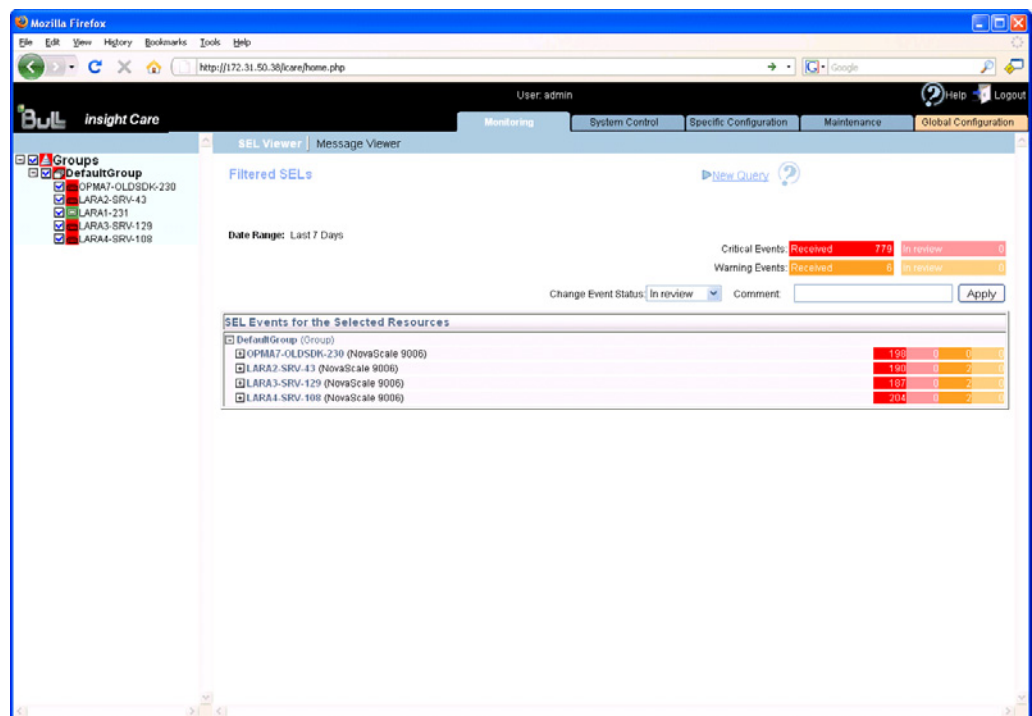


Figure 30. SEL Query Report page - Default display

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

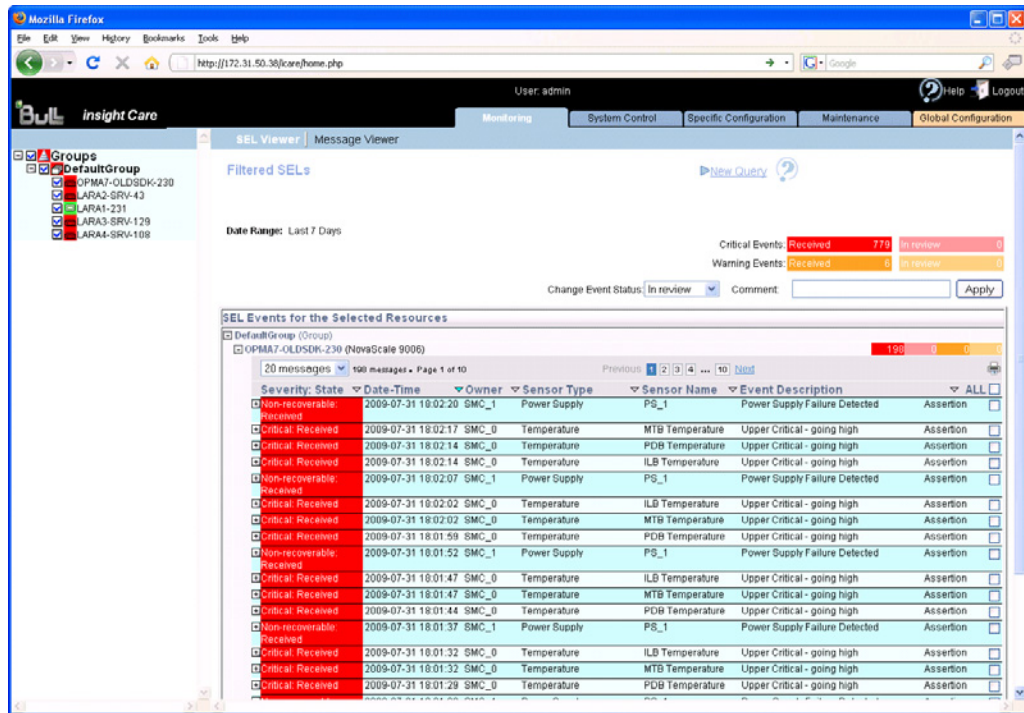


Figure 31. SEL Query Report page - SEL Event List

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

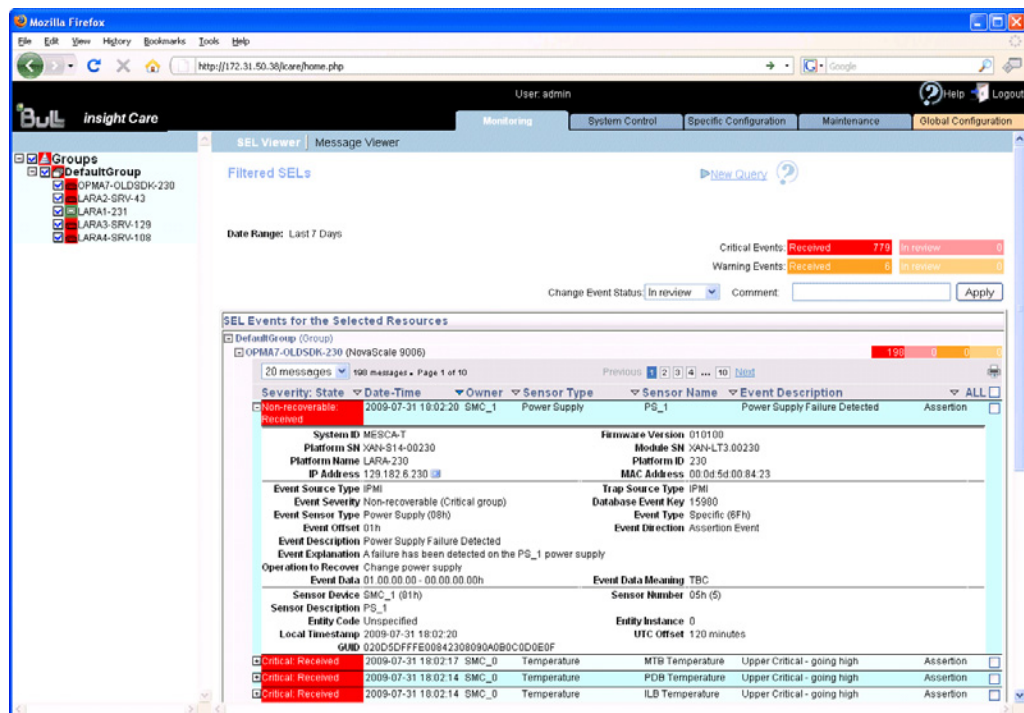


Figure 32. SEL Query Report page - SEL Event details

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

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

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

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

Related Topics

- [Building SEL Query Reports](#), on page 4-2

4.4. Viewing Resource Details

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

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

Prerequisites

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

Procedure

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

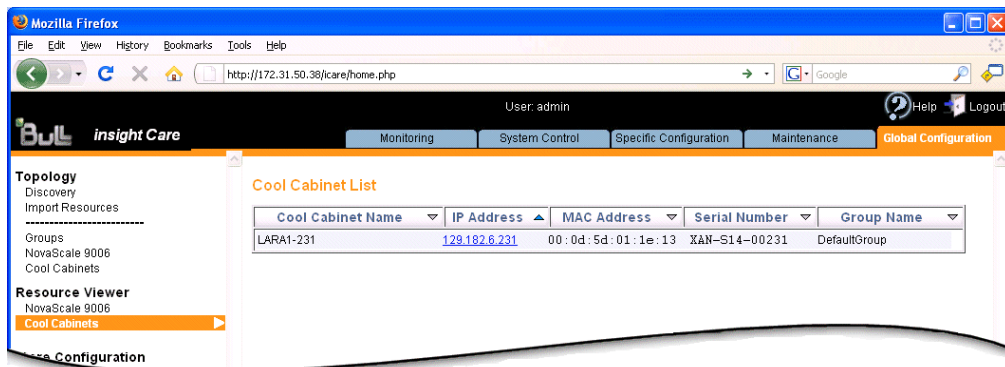
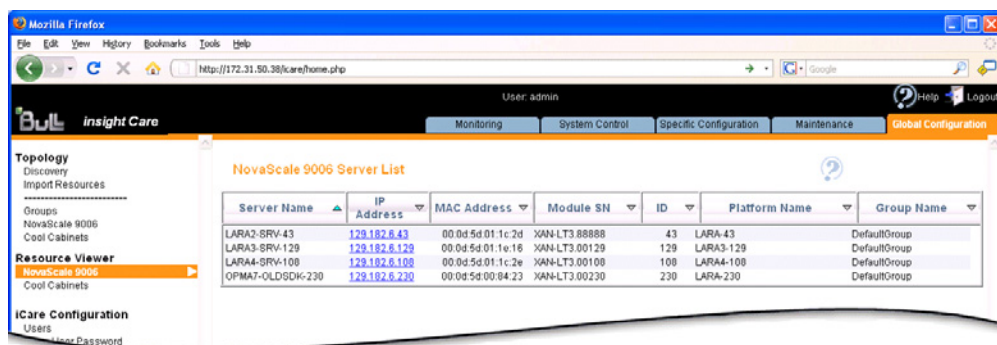


Figure 33. Resource Viewer page - Examples

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 3-1

Chapter 5. Configuring Autocalls

This chapter explains how to configure and enable the autocall feature used to send messages to the Bull Support Center when a problem occurs on a monitored hardware resource. It includes the following topics:

- Introducing the Autocall Feature, on page 5-2
- Enabling/Disabling and Testing Autocalls, on page 5-2
- Selecting Global Autocall Policies, on page 5-4
- Selecting Specific Autocall Policies, on page 5-6
- Configuring Autocall Filters, on page 5-8

Note This 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. Introducing the Autocall Feature

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.

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

- Enable the feature, then select and configure the autocall dispatch mode, as explained in [Enabling/Disabling and Testing Autocalls](#), on page 5-2.
- Select a default autocall policy for each hardware resource type, as explained in [Selecting Global Autocall Policies](#), on page 5-4.

Optionally, you can also:

- Select a specific autocall policy for specific hardware resources, as explained in [Selecting Specific Autocall Policies](#), on page 5-6.
- Create specific autocall filters to track specific events, as explained in [Configuring Autocall Filters](#), on page 5-8.



Important It is strongly recommended to complete the site form before configuring autocalls. For details, see [Completing the Site Form](#), on page 7-7.

5.2. Enabling/Disabling and Testing Autocalls

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

Prerequisites

- Your maintenance contract includes the autocall feature.
- You know dispatch mode settings.
- The target directory is already present on the workstation.

Procedure

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

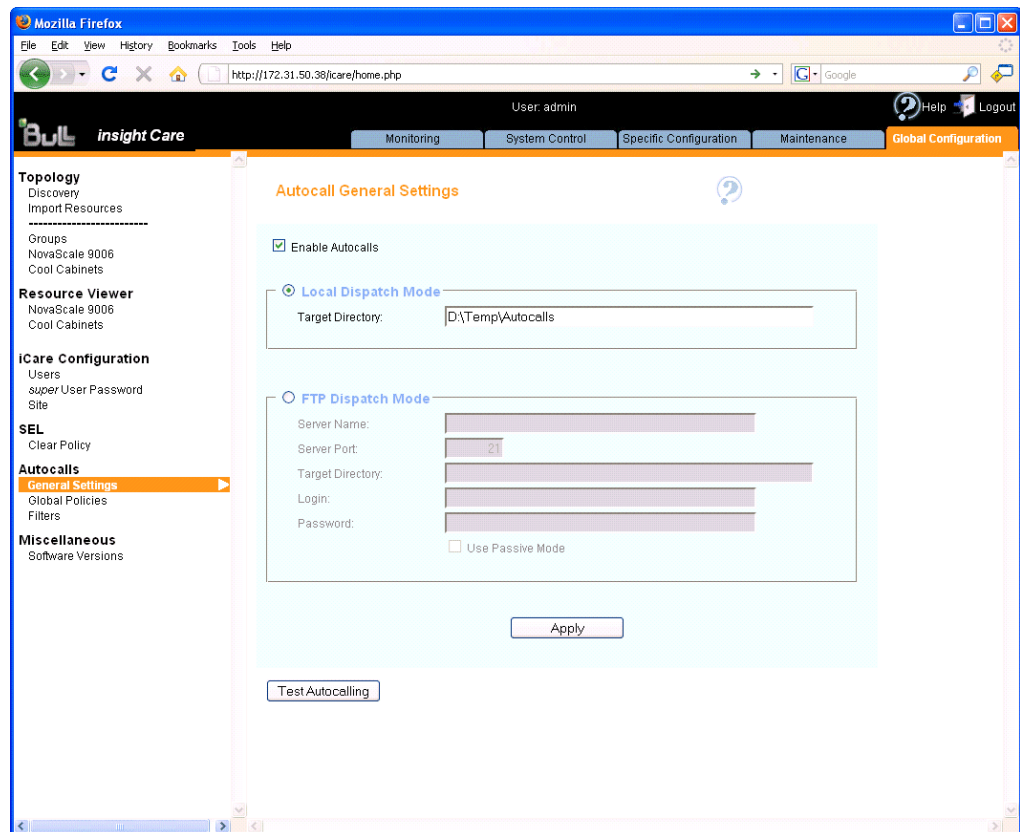


Figure 34. Autocall General Settings page (Autocall Enabled)

2. Select the Enable Autocalls check box and configure the autocall dispatch mode as explained in the following table:

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:	
<ul style="list-style-type: none"> • The target directory must already be present on the workstation. • You must enter the full directory pathname (example: C:\Autocalls). 	
FTP Dispatch Mode	
The FTP dispatch mode sends one XML file per autocall to the specified remote maintenance server. To enable the FTP dispatch mode, complete the fields as follows:	
Server Name	Remote maintenance server hostname or IP address
Server Port	Server port (21 by default)
Target Directory	Target directory containing the autocall XML file (example: /autocall) Note that the target directory must already be present on the workstation
Login and Password	User account used to log onto the FTP server

Table 15. Autocall dispatch mode settings

3. Click **Apply** to save settings. The **Test Autocalling** button appears.
4. Click **Test Autocalling** and check that the autocall has reached the local or FTP directory according to dispatch mode type.
5. Proceed to define a global autocall policy for each hardware resource type, as described in *Selecting Global Autocall Policies*, on page 5-4.

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

Related Topics

- *Selecting Global Autocall Policies*, on page 5-4
- *Selecting Specific Autocall Policies*, on page 5-6
- *Configuring Autocall Filters*, on page 5-8

5.3. Selecting Global Autocall Policies

Global autocall policies are available for all hardware resources of the same type and are supplied with the console. The global policies are configured to cover the standard autocall requirements for each type of hardware resource. According to your needs, you can select global policies based on event severity or on event type. If you select global policies based on event type, you can decide whether to apply default filters or to create and apply custom filters.

Prerequisites

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

Procedure

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

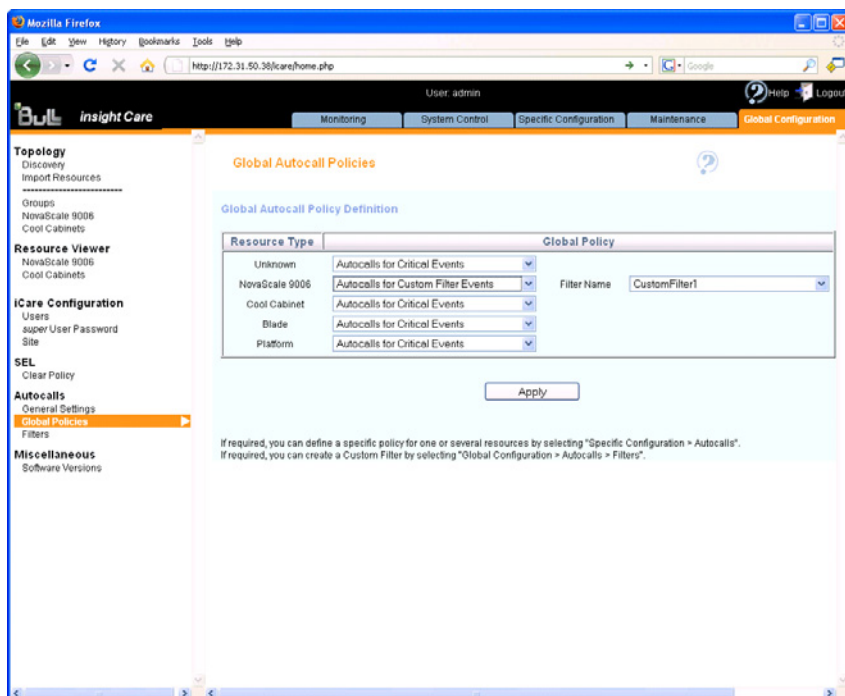


Figure 35. Global Autocall Policy page

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

Global Autocall Policy Based on Event Severity	
None	No autocall will be sent.
Autocalls for Critical Events	Value selected by default. An autocall is sent when a CRITICAL event occurs.
Autocalls for Critical or Warning Events	An autocall is sent when a CRITICAL or WARNING event occurs.
Global Autocall Policy Based on Event Type Filters	
Autocalls for Default Filter Events	An autocall is sent when an event message matches the default filter criteria. You can view the default filter criteria, as detailed in Viewing Default or Custom Filter Details, on page 5-8.
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 5-8

Table 16. Global autocall policy options

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

Note You can assign a different autocall policy to one or more specific resources as explained in [Selecting Specific Autocall Policies](#), on page 5-6.

Related Topics

- [Viewing Default or Custom Filter Details](#), on page 5-8
- [Creating a Custom Filter](#), on page 5-10
- [Selecting Specific Autocall Policies](#), on page 5-6
- [Enabling/Disabling and Testing Autocalls](#), on page 5-2

5.4. 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).

The screenshot shows the iCare console interface. The 'Specific Configuration' tab is active, displaying the 'Specific Autocall Policies' page. On the left, a 'Groups' tree shows a 'DefaultGroup' containing several resources: OPMA7-OLDSDK-230, LARA2-SRV-43, LARA3-SRV-129, LARA4-SRV-108, and Hydra-2. The main area contains a table with the following data:

Resource	Specific	Policy	Filter
<input type="checkbox"/> NovaScale 9006		Autocalls for Critical or Warning Events	
<input type="checkbox"/> OPMA7-OLDSDK-230	<input type="checkbox"/>	Autocalls for Critical or Warning Events	
<input type="checkbox"/> LARA2-SRV-43	<input type="checkbox"/>	Autocalls for Critical or Warning Events	
<input type="checkbox"/> LARA3-SRV-129	<input type="checkbox"/>	Autocalls for Critical or Warning Events	
<input type="checkbox"/> LARA4-SRV-108	<input type="checkbox"/>	Autocalls for Critical or Warning Events	
<input type="checkbox"/> Cool Cabinet		Autocall for Critical Event	
<input type="checkbox"/> Hydra-2	<input type="checkbox"/>	Autocall for Critical Event	

Below the table is an 'Apply' button. At the bottom of the page, a note reads: '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 autocal policy to apply to the selected resource(s) from the Policy drop-down list, as explained in the following table:

Specific Autocall Policy Based on Event Severity	
None	No autocall will be sent.
Autocalls for Critical Events	Value selected by default. An autocall is sent when a CRITICAL event occurs.
Autocalls for Critical or Warning Events	An autocall is sent when a CRITICAL or WARNING event occurs.
Specific Autocall Policy Based on Event Type Filters	
Autocalls for Default Filter Events	An autocall is sent when an event message matches the default filter criteria. You can view the default filter criteria, as detailed in Viewing Default or Custom Filter Details, on page 5-8.
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 5-8

Figure 36. Specific Autocall Policy page

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

Related Topics

- Creating a Custom Filter, on page 5-10
- Viewing Default or Custom Filter Details, on page 5-8
- Enabling/Disabling and Testing Autocalls, on page 5-2
- Selecting Global Autocall Policies, on page 5-4

5.5. Configuring Autocall Filters

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

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

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

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

The following tasks are explained in this section:

- Viewing Default or Custom Filter Details, on page 5-8
- Creating a Custom Filter, on page 5-10
- Editing a Custom Filter, on page 5-11
- Deleting a Custom Filter, on page 5-15

5.5.1. Viewing Default or Custom Filter Details

Prerequisites

- None.

Procedure

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

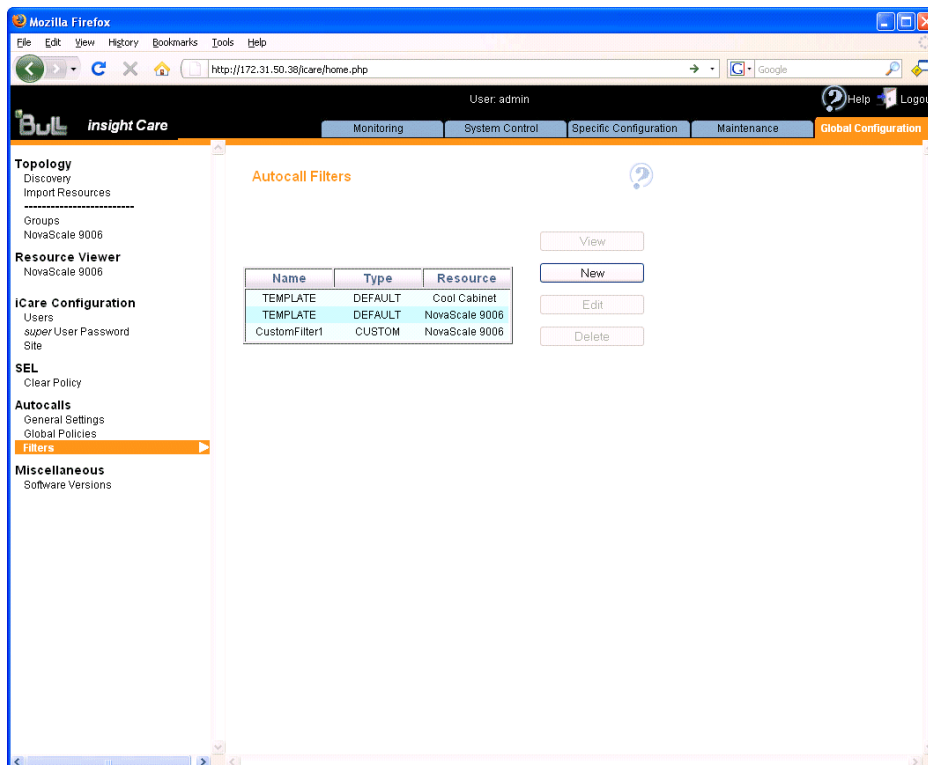
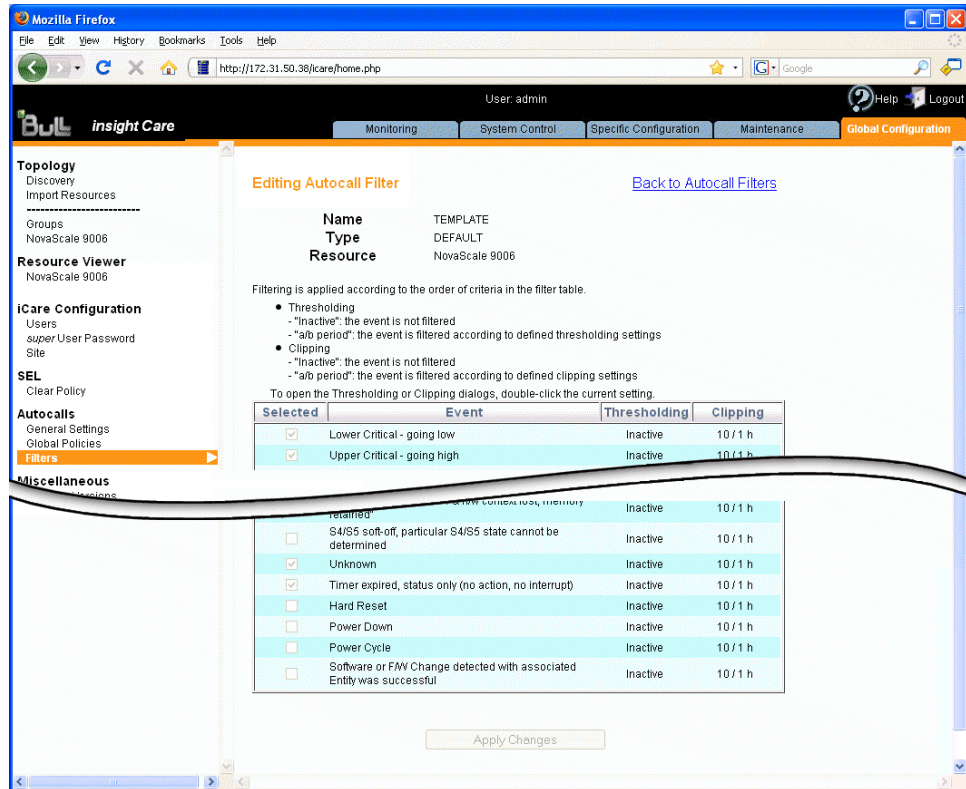


Figure 37. Autocall Filters page

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



Note This page is in read-only mode and displays the list of events selected to trigger autocal calls. For details on the Thresholding and Clipping parameters, see Editing a Custom Filter, on page 5-11.

Figure 38. Viewing Autocall Filter page

- Click Back to Autocall Filters to return to the Autocall Filters page.

Related Topics

- Creating a Custom Filter, on page 5-10
- Editing a Custom Filter, on page 5-11
- Deleting a Custom Filter, on page 5-15

5.5.2. Creating a Custom Filter

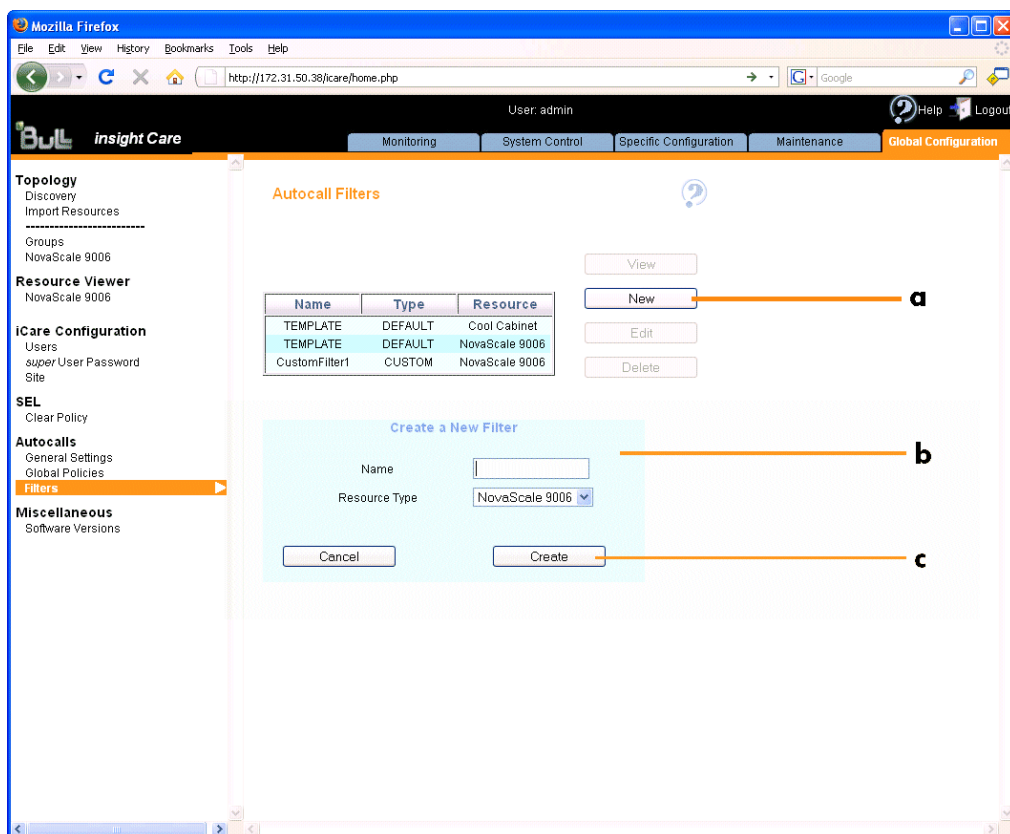
The iCare Console allows you to create your own autocall custom filter to finely tune event type filtering when the default filters supplied with the console do not cover your needs.

Prerequisites

- None.

Procedure

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



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

Figure 39. 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 5-11.

Related Topics

- Editing a Custom Filter, on page 5-11
- Deleting a Custom Filter, on page 5-15

5.5.3. 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.

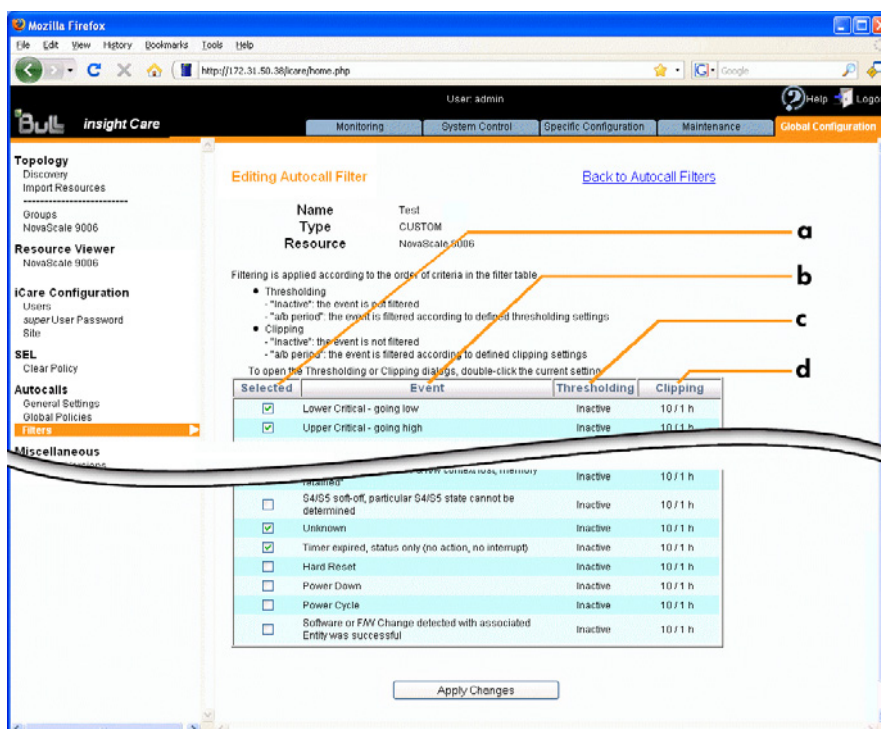
Prerequisites

- The custom filter has been created, as explained in Creating a Custom Filter, on page 5-10.

Procedure

Note Criteria differ according to hardware resource type.
This procedure is based on the NovaScale 9006 Server 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.

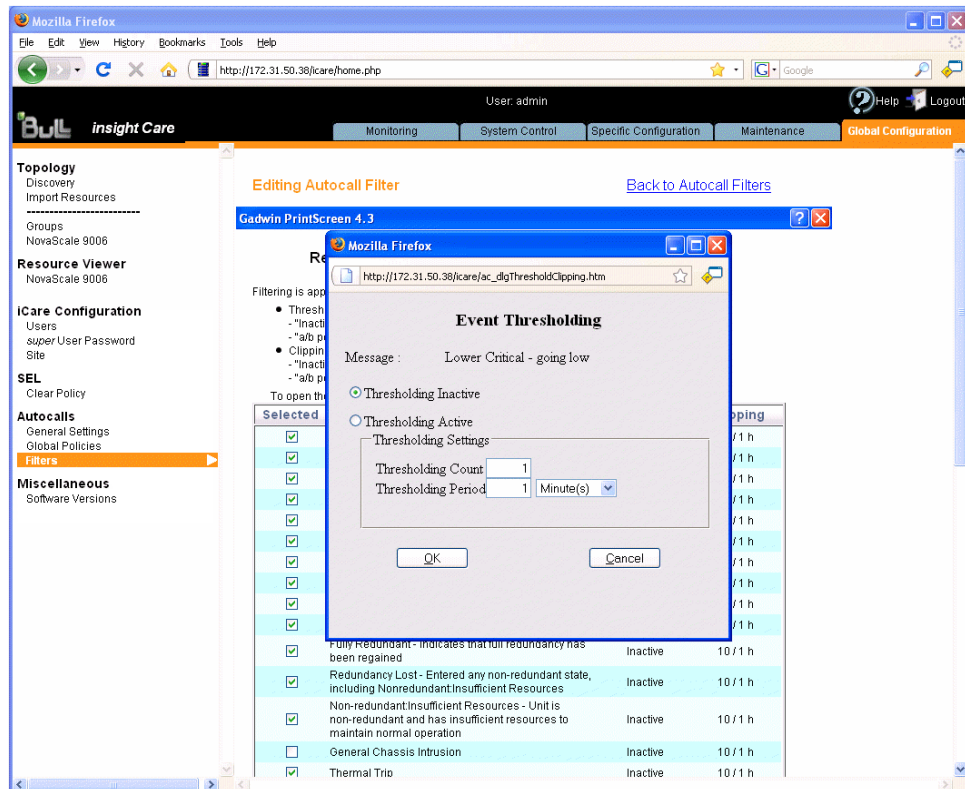


Editing Autocall Filter	
Selected column (a)	By default, the selected check boxes are the same as for the default autocall filter for the hardware resource type. When a check box is selected, the corresponding event message is included in the custom filter.
Event column (b)	Message associated with the 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 40. Editing Autocall Filter page

3. For each listed event:

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

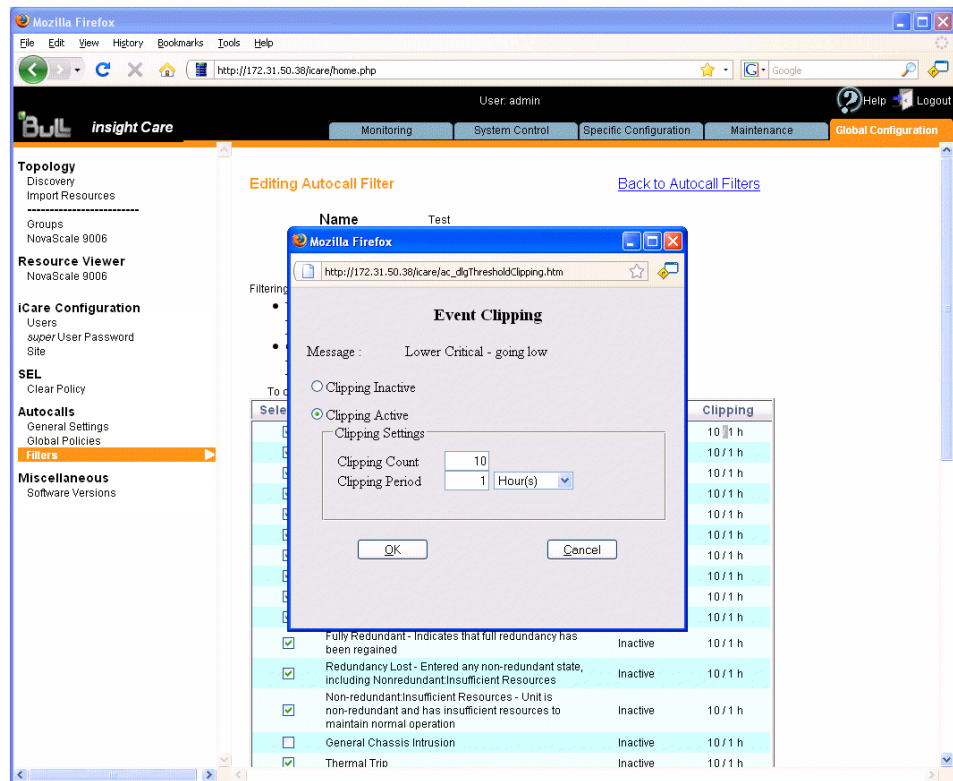


Event Thresholding Box	
Thresholding is defined on a Count / Period basis aimed at transmitting significant event messages only. Identical event messages are counted and if the number of event messages indicated in the Thresholding Count field is reached within the period of time indicated in the Thresholding Period field, this event message is selected for transmission.	
Thresholding Inactive	Deactivates thresholding: if the event is selected, all messages are transmitted as autocalls.

Event Thresholding Box (continued)	
Thresholding Active	Activates thresholding using the values displayed in the Thresholding Count and Thresholding Period fields.
Thresholding Count	Number of identical event messages to be reached.
Thresholding Period	Period of time, in seconds, minutes, hours or days.

Figure 41. Event Thresholding box description

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



Event Clipping Box	
Clipping is defined on a Count / Period basis aimed at transmitting a pre-defined number of event messages only. Identical event messages are counted and when the number of event messages indicated in the Clipping Count field is reached within the period of time indicated in the Clipping Period field, no other event messages will be selected for 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 42. Event Clipping box description

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

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

Related Topics

- [Creating a Custom Filter](#), on page 5-10
- [Deleting a Custom Filter](#), on page 5-15
- [Selecting Global Autocall Policies](#), on page 5-4
- [Selecting Specific Autocall Policies](#), on page 5-6

5.5.4. Deleting a Custom Filter

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

Note You cannot delete default autocall filters.

Prerequisites

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

Procedure

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

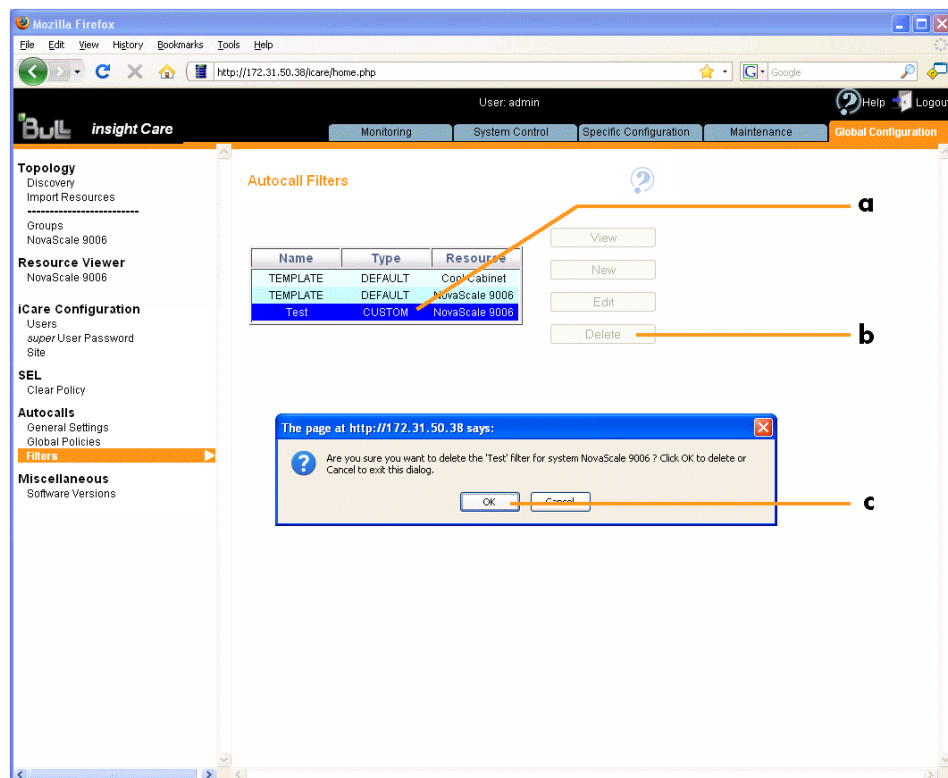


Figure 43. Autocall Filters page (Delete a filter)

Related Topics

- Creating a Custom Filter, on page 5-10
- Selecting Global Autocall Policies, on page 5-4
- Selecting Specific Autocall Policies, on page 5-6

Chapter 6. Managing Intervention Reports and Action Requests

This chapter explains how to create and manage intervention reports and action request packages in order to facilitate problem analysis as well as preventive and corrective maintenance operations. It includes the following topics:

- Creating an Intervention Report, on page 6-2
- Viewing the List of Intervention Reports, on page 6-3
- Creating an Action Request Package, on page 6-4

6.1. Creating an Intervention Report

You are advised to create an intervention report to 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 are 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).

The screenshot shows the 'Intervention Report Creation' page in the iCare Console. The page is displayed in a Mozilla Firefox browser window. The URL is <http://172.31.50.38/icare/home.php>. The user is logged in as 'admin'. The page has a navigation bar with tabs for 'Monitoring', 'System Control', 'Specific Configuration', 'Maintenance', and 'Global Configuration'. The 'Maintenance' tab is active, and the 'Intervention Report Creation' sub-tab is selected. On the left, there is a 'Groups' tree with 'DefaultGroup' expanded, showing several resources: 'Banc-de-Test', 'SRV4-SRV', 'Hydra-1', 'Inux1 29', 'SRV-LARA-231', and 'Linux_230'. The 'SRV4-SRV' resource is selected. The main area of the page is titled 'Intervention Report Creation' and shows '1 Resource(s) Selected'. Below this, there are three sections: 'Reference' with 'Operator name' and 'Order number' fields; 'Intervention Dates' with 'Start date (YYYY-MM-DD)', 'End date (YYYY-MM-DD)', and 'Total intervention time (hours)' fields; and 'Intervention Description' with a large text area. A 'Create' button is at the bottom right. Three orange arrows labeled 'a', 'b', and 'c' point to the 'DefaultGroup' tree item, the 'Refresh' button, and the 'Total intervention time (hours)' field respectively.

Figure 44. 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. You can now view the report(s) using the **Intervention Report Viewer**.

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.

Related Topics

- Viewing the List of Intervention Reports, on page 6-3
- Creating an Action Request Package, on page 6-4

6.2. Viewing the List of Intervention Reports

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

Prerequisites

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

Procedure

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

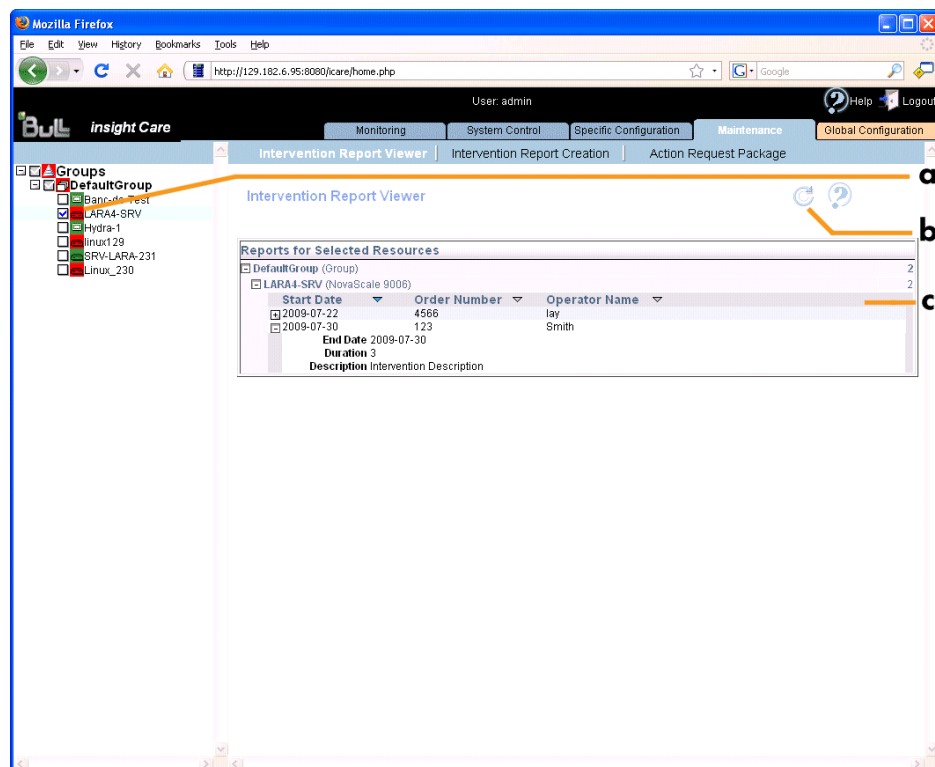


Figure 45. Intervention Report Viewer page

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

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

Related Topics

- Creating an Intervention Report, on page 6-2
- Creating an Action Request Package, on page 6-4

6.3. 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.

Prerequisites

- You have completed the Site form, as detailed in *Completing the Site Form*, on page 7-7.
- If you are using Internet Explorer, check the following security parameters :
 - In the **Tools** menu, click **Internet Options**.
 - In the displayed dialog box, select the **Security** tab and click the **Custom Level** button.
 - In the displayed window, scroll down to bottom and in the **Downloads** section, check the following parameter values:

Parameter	Value
Automatic prompting for file downloads	Enable
File download	Enable

- The hardware resources for which you want to create an action request package are in the Resource tree.
- You have the Action Request Package reference number sent by the Bull Support Center.

Procedure

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

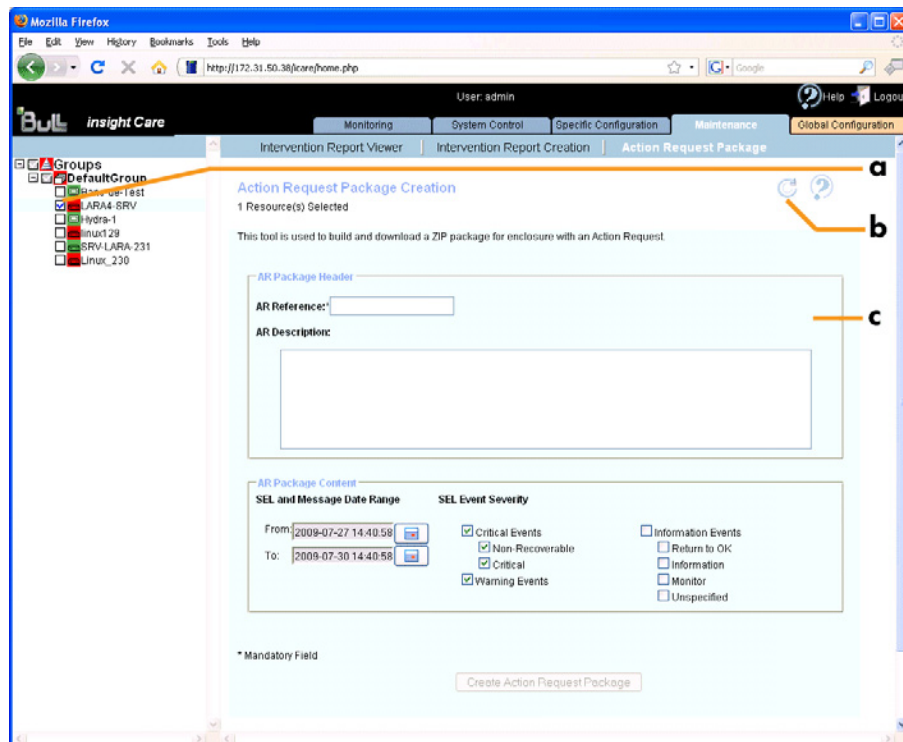


Figure 46. Action Request Package Creation page

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 three PDF files for each hardware resource: SEL Events, Message Events and Identity Card.
5. When requested, save the ZIP file and send it to the Bull Support Center for analysis.

Related Topics

- Creating an Intervention Report, on page 6-2
- Viewing the List of Intervention Reports, on page 6-3

Chapter 7. Performing Other Configuration Tasks

This chapter explains how to perform standard global configuration tasks. It completes the global configuration information given in Chapter 2. Managing the Resource Tree and Chapter 5. Configuring Autocalls. It includes the following topics:

- Managing User Accounts, on page 7-2
- Setting Up the BMC Super User Password, on page 7-5
- Completing the Site Form, on page 7-7
- Enabling/Disabling the Automatic Clear SEL Policy, on page 7-8
- Displaying iCare and Other Software Version Information, on page 7-9

7.1. Managing User Accounts

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

7.1.1. Creating a User Account

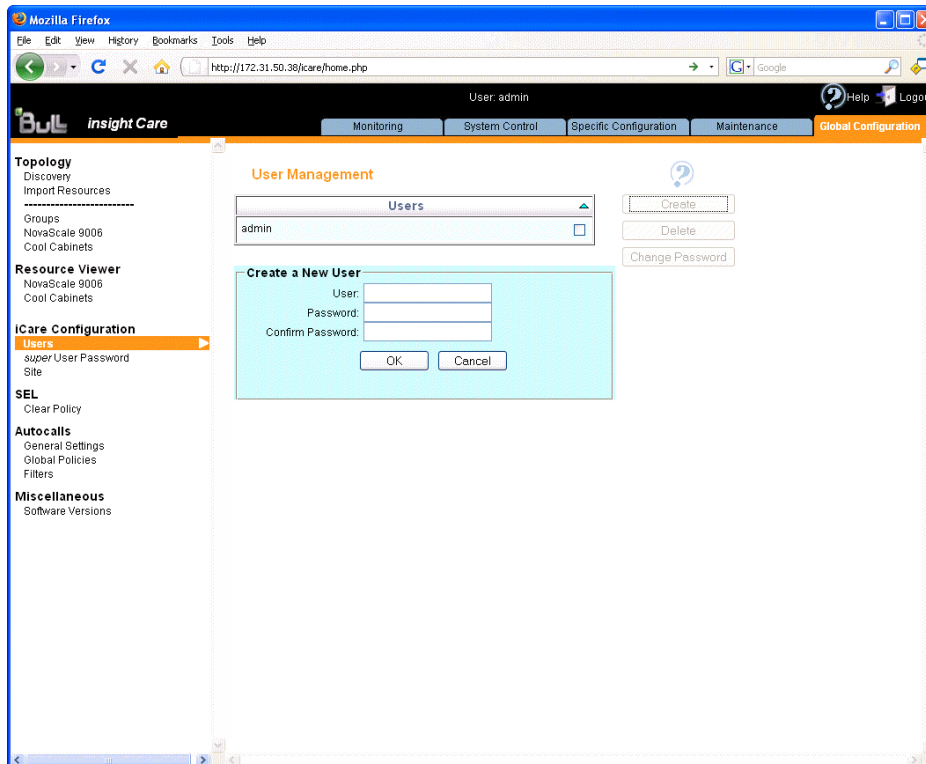
You can create a personal user account for each person that needs to log onto and use the iCare Console.

Prerequisites

- None.

Procedure

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



Create a New User	
User	Name the user will use to log on. <ul style="list-style-type: none"> • Name limited to 16 characters - CASE SENSITIVE. • The following characters are not allowed: \backslash " & ' + * % = > < : ! ? ; , ~ and space.
Password	Password the user will use to log on. <ul style="list-style-type: none"> • Maximum password length: 16 characters • No character restriction - CASE SENSITIVE.
Confirm Password	

Figure 47. User Management page (Create a New User box)

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

Related Topics

- Deleting a User Account, on page 7-3
- Changing a User Account Password, on page 7-4

7.1.2. Deleting a User Account

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

Note You cannot delete the predefined user account admin. However, the default admin user password can be changed, as detailed in Changing a User Account Password, on page 7-4.

Prerequisites

- None.

Procedure

1. From the Global Configuration tab, click iCare Configuration > Users. The User Management page appears.

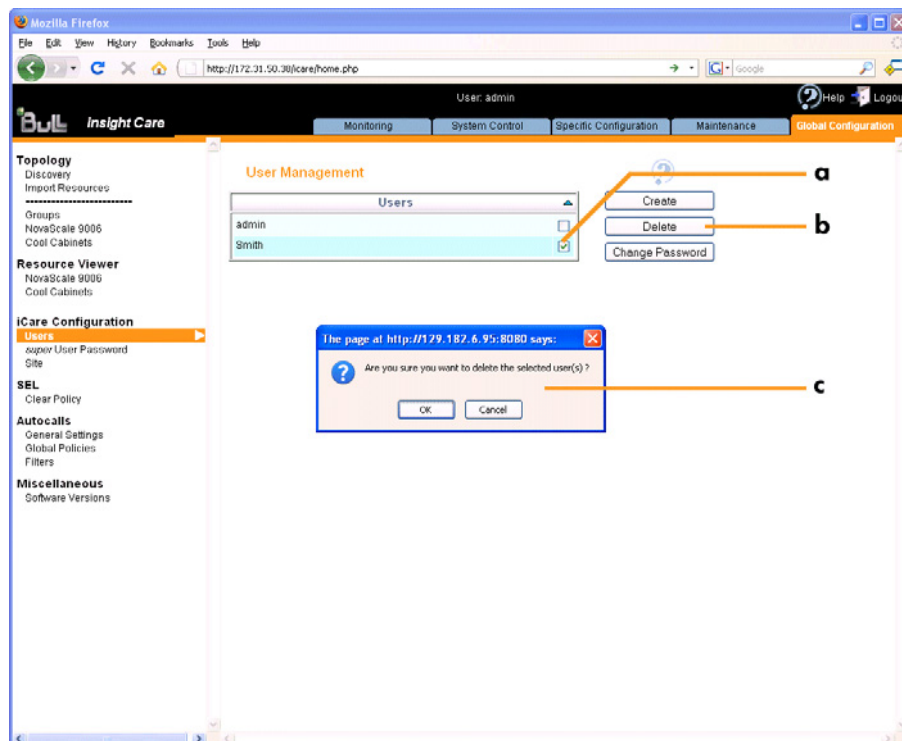


Figure 48. User Management page (Delete User Account)

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 created and disappears from the User Management page.

Related Topics

- Creating a User Account, on page 7-2
- Changing a User Account Password, on page 7-4

7.1.3. Changing a User Account Password

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

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

Prerequisites

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

Procedure

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

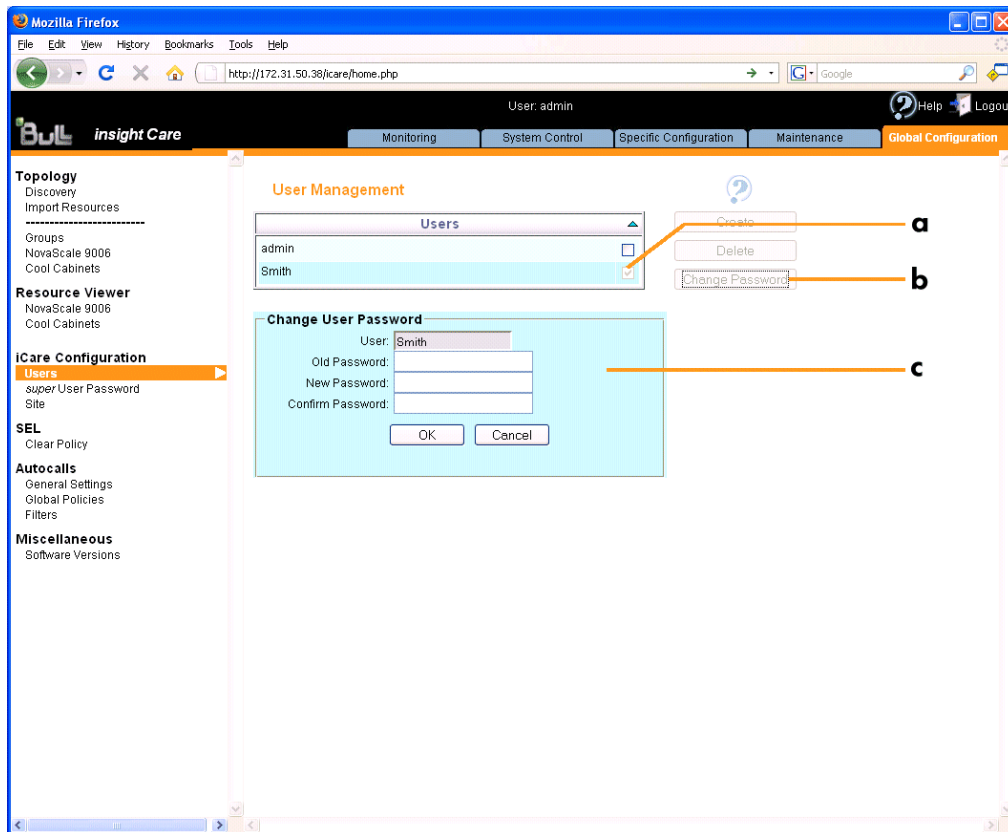


Figure 49. User Management page (Change User Password box)

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

Related Topics

- Creating a User Account, on page 7-2
- Deleting a User Account, on page 7-3

7.2. Setting Up the BMC Super User Password

The iCare Console communicates with the hardware resources it monitors via the Baseboard Management Controllers (BMC) embedded on each of these hardware resources. The iCare Console connects to the hardware resource BMCs using the super user account.

An identical **super user account** must be set up, using the resource's hardware console, for each resource monitored via the iCare Console. Once you have set up this account on all the hardware resources you want to monitor, you must then declare the same super user password in the iCare Console.

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

- login: `super`
- password: `pass`

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



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

Prerequisites

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

Procedure

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

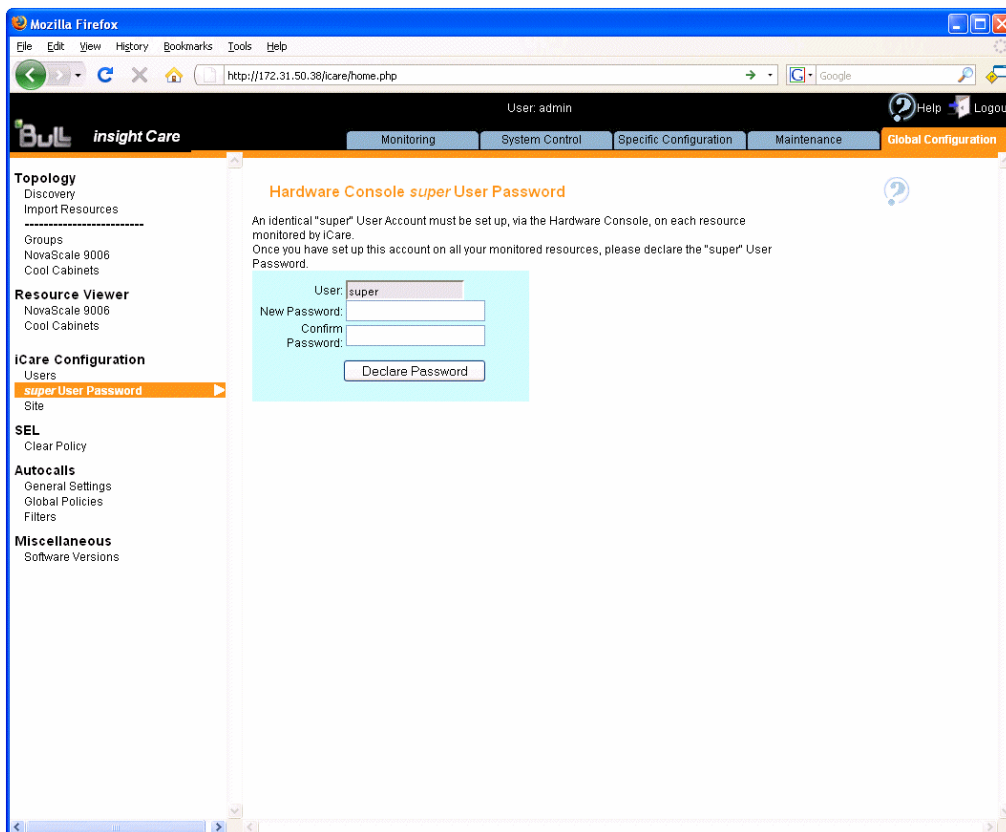


Figure 50. *super* User Password page

2. Complete the fields and click Declare Password.

Related Topics

- Connecting to a Resource Console, on page 3-1
- Manually Importing Multiple Hardware Resources, on page 2-4

7.3. Completing the Site Form

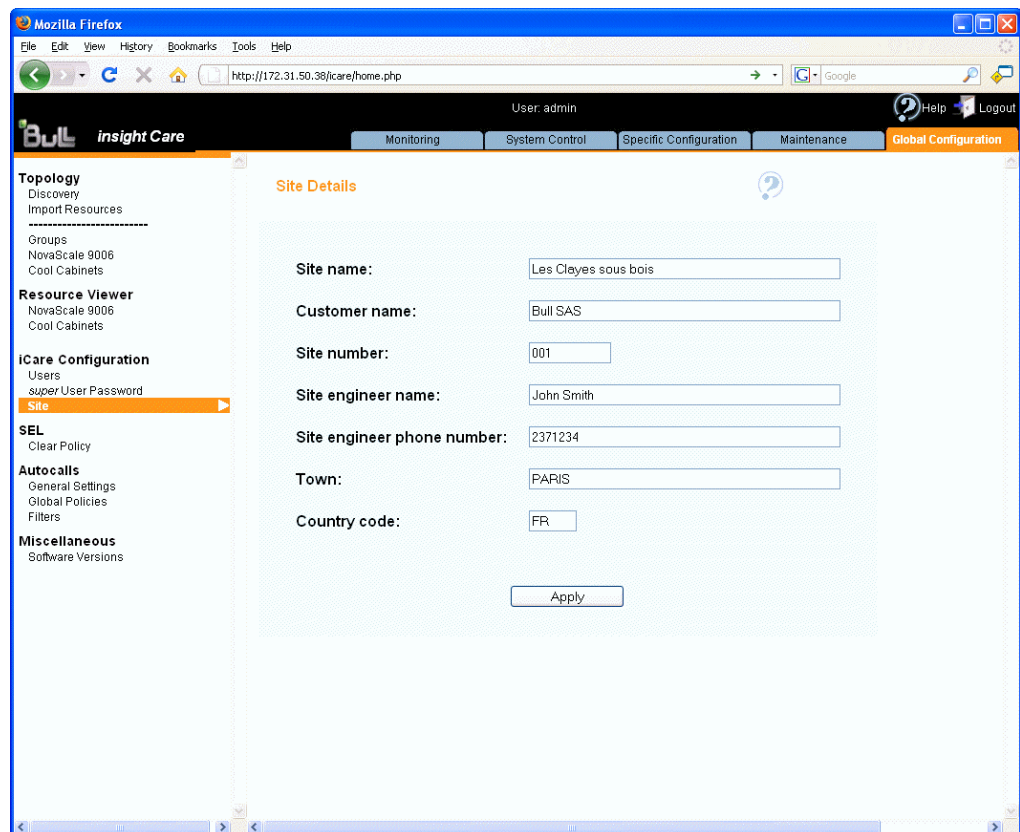
You are advised to fill in the site form, which adds site information to the autocalls and to the Action Request Packages sent to Bull Support services.

Prerequisites

- None.

Procedure

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



The screenshot shows a web browser window displaying the 'Site Parameters' page. The browser is Mozilla Firefox, and the URL is http://172.31.50.38/icare/home.php. The user is logged in as 'admin'. The interface has a navigation bar with tabs: Monitoring, System Control, Specific Configuration, Maintenance, and Global Configuration (selected). The left sidebar contains a tree view with categories: Topology (Discovery, Import Resources), Groups (NovaScale 9006, Cool Cabinets), Resource Viewer (NovaScale 9006, Cool Cabinets), iCare Configuration (Users, super User Password, Site), SEL (Clear Policy), Autocalls (General Settings, Global Policies, Filters), and Miscellaneous (Software Versions). The 'Site' option under iCare Configuration is selected. The main content area is titled 'Site Details' and contains a form with the following fields: 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), and Country code (FR). An 'Apply' button is located at the bottom of the form.

Figure 51. Site Parameters page

2. Complete the form as shown in the previous illustration and click Apply.

7.4. Enabling/Disabling the Automatic Clear SEL Policy

The System Event Log of each monitored hardware resource can only store up to 512 entries at a time. Once this limit is reached, the LOG IS NOT AUTOMATICALLY EMPTIED to allow for the arrival of new events. Beyond the 512-entry limit, NEW EVENTS ARE NOT RECORDED. Use the automatic clear SEL option to automatically empty SEL logs when the limit is reached so that the latest events can be logged.

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

Prerequisites

- The hardware resources are present and monitored in the Resource tree.
- The same **super** user password is set up on all monitored resources. For details, see Setting Up the BMC Super User Password, on page 7-5.

Procedure

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

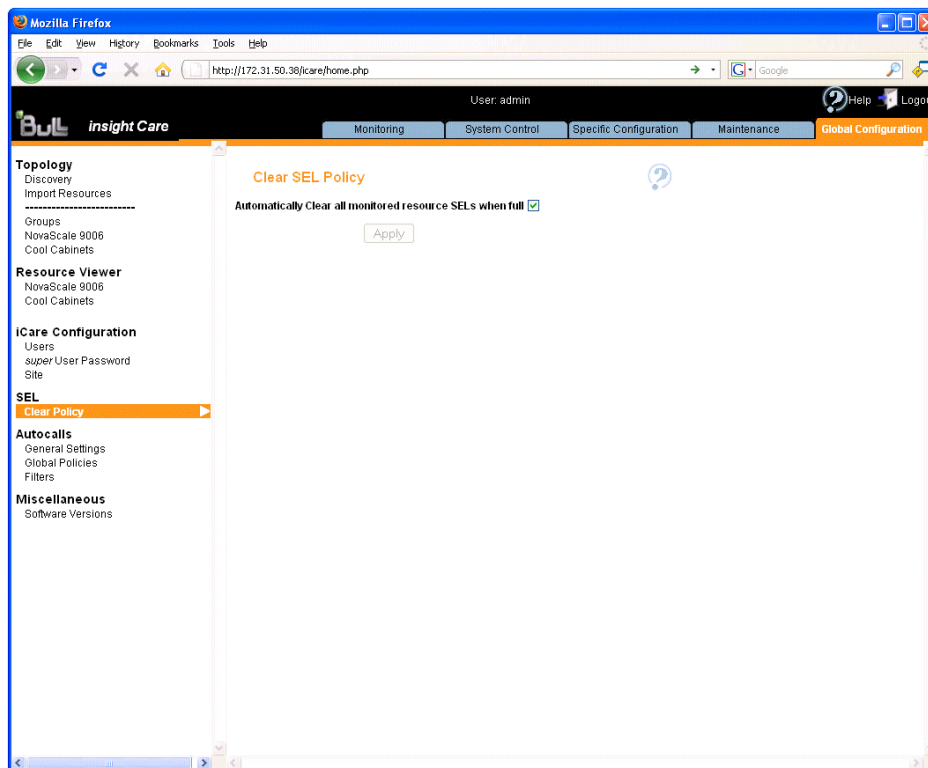


Figure 52. Clear SEL Policy page

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

Related Topics

- Manually Importing Multiple Hardware Resources, on page 2-4
- Setting Up the BMC Super User Password, on page 7-5

7.5. Displaying iCare and Other Software Version Information

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

Prerequisites

- None.

Procedure

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

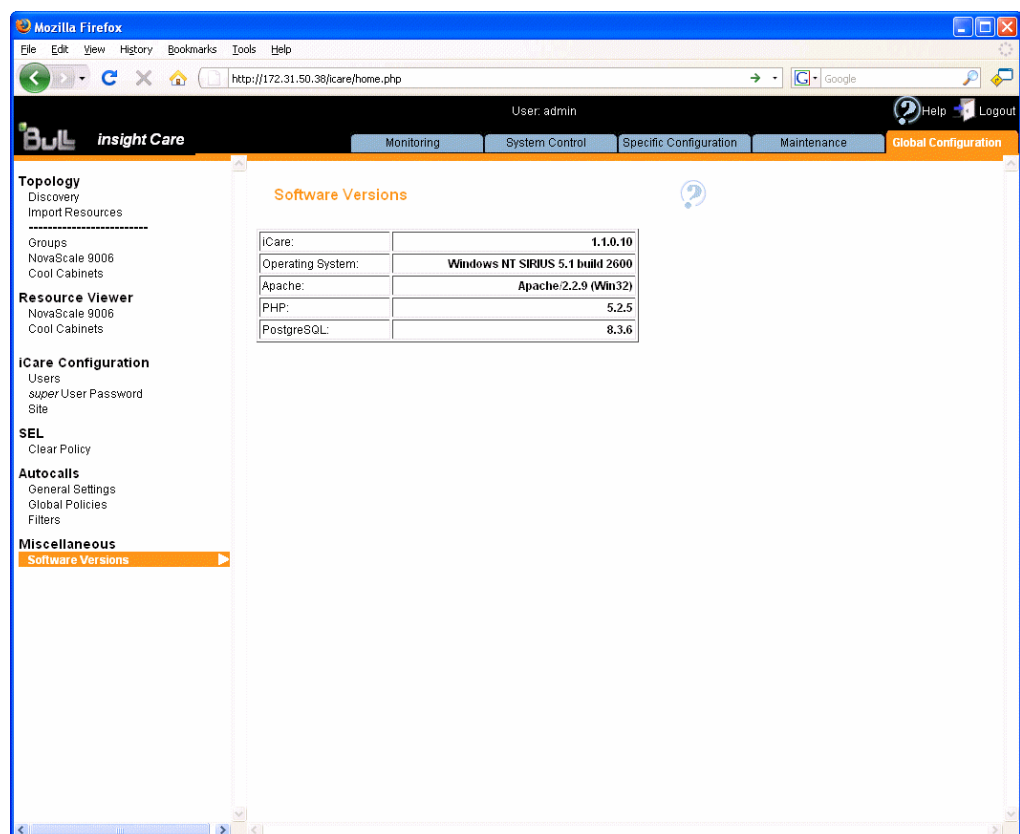


Figure 53. Software Versions page

Glossary

A

ACPI

Advanced Configuration and Power Interface.

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

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. A ARU is also known as an PMU.

B

Backup

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

Base Operating System

The Operating System that is booted at initialization.

BCS

Bull Coherent Switch. This is the Bull eXternal Node Controller. Provides SMP upgradeability up to 16 processors. The BCS ensures global memory and cache coherence, with optimized traffic and latencies, in both IPF-preferred and XPF-preferred variants.

BIOS

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

BIST

Built-In Self-Test.

See POST.

Bit

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

BMC

Baseboard Management Controller. See Embedded Management Controller.

BT

Block Transfer. One of the three standardized IPMI System interfaces used by system software for transferring IPMI messages to the BMC. A per-block handshake is used to transfer data (higher performance).

Byte

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

C

Cache Memory

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

CD-ROM

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

CIM

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

Clipping

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

CMC

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

CMCI

Corrected Memory Check Interrupt.

CMCV

Corrected Memory Check Vector.

CMOS

Complementary Metal Oxide Semiconductor.

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

Cold Reset

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

Core

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

CPLD

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

CRU

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

CSE

Customer Service Engineer.

D**Default Setting**

The factory setting your server uses unless instructed otherwise.

Device Driver

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

DIMM

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

DMA

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

DNS

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

DPS

Distributed Power Supply.

DRAM

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

DSIB

Dummy BCS Interconnect Board.

DVO

Digital Video Out.

E**EEPROM**

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

EFI

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

EFI Shell

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

EMI

Electro-Magnetic Interference.

Embedded Management Controller

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

EMM

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

EPROM

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

ERP

Error Recovery Procedure.

Error

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

Error Detection

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

ESD

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

Event

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

Exclude

See Include / Exclude.

F

Fail-Over

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

Fatal Error

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

Fault

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

Flash EPROM

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

Firewall

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

Firmware

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

FPGA

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

FRU

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

FTP

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

G

GUI

Graphical User Interface.

H

HA

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

Hard Reset

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

Hardware

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

Hardware Corrected Error

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

Hardware Partition

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

Hard Partitioning

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

Hardware Uncorrected Error

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

HPC

High Performance Computing.

Host Operating System

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

Hot-Plugging

The operation of adding a component without interrupting system activity.

Hot-Swapping

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

HT

HyperThreading. See Multi-Threading.

HTTP

HyperText Transfer Protocol.

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

I**I2C**

Intra Integrated Circuit.

The I2C (Inter-IC) bus is a bi-directional two-wire serial bus that provides a communication link between integrated circuits (ICs).

The I2C bus supports 7-bit and 10-bit address space devices and devices that operate under different voltages.

IB

InfiniBand.

IC

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

iCare

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

ICH

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

ICMB

Intelligent Chassis Management Bus.

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

ILB I/O Legacy Board.

Interface

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

Include / Exclude

A physically present ARU can be logically connected to / disconnected from the hardware partition at boot time, under control of the Platform Management software. This is a static logical operation.

An excluded ARU can be reserved as a spare, locked for future user (Pay-As-You-Grow), or marked as failed.

Initialization

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

I/O

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

IOH

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

IP

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

IPL

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

IPM

Intelligent Platform Management.

IPMB

Intelligent Platform Management Bus.

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

IPMI

Intelligent Platform Management Interface.

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

J**Jumper**

A small electrical connector used for configuration on computer hardware.

K**KCS**

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

KVM

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

L**LAN**

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

LCP

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

LDAP

Lightweight Directory Access Protocol. Application protocol for querying and modifying directory services running over TCP/IP.

LED

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

Legacy Application

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

Logical Partition

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

Logical Processor

See Thread.

LUN

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

M**MAC**

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

MC

Management Controller.

MESCA

Multiple Environments on a Scalable Csi-based Architecture.

Memory

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

Microprocessor

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

MII

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

MIMD

Multiple Instruction Multiple Data

Mirrored volumes

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

MTB

Memory and Tukwila Board.

MTBF

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

Multicore

Presence of two or more processors on a single chip.

Multimedia

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

Multi-Tasking

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

Multi-Threading

The ability of a single processor core to provide software visibility similar to that of several cores and execute several threads in apparent (to software) simultaneity while using limited additional hardware resources with respect to a core without multi-threading.

Depending on core design, the instructions issued for execution by the core at a given cycle may be either **Hyper-Threading (HT)** - from a single thread, switching to another thread upon occurrence of specific events (e.g. cache misses) or **Simultaneous Multi-Threading (SMT)** - from both threads.

N

NFS

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

NIC

Network Interface Controller.

NUMA

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

NVRAM

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

O

OF

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

Off-Lining

See On-Lining / Off-Lining.

On-Lining / Off-Lining

On-lining and off-lining are dynamic logical operations.

On-lining is the non-physical addition of an ARU to the running OS. The on-lined unit already exists in the configuration as an inactive unit (present and connected).

Off-lining is the non-physical removal of an ARU from the running OS. The off-lined unit remains in the configuration as an inactive unit, ready to be on-lined.

OOB

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

Operating System

See OS.

OPMA

Open Platform Management Architecture Board.

OS

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

P**Password**

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

PCI

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

PCIe

PCI Express. Latest standard in PCI expansion cards.

PDB

Power Distribution Board. Sub-assembly of the Power Supply Module.

PDU

Power Distribution Unit. Power bus used for the connection of peripheral system components.

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.

ping

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

PIROM

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

Plugging / Unplugging

Plugging and unplugging are static physical operations and represent the physical insertion / removal of a standard ARU.

Plugging and unplugging procedures guarantee the electrical protection of live parts.

PMU

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

PNP

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

POR

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

POST

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

Power-up Reset

See Cold Reset.

Processor

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

PROM

Programmable Read-Only Memory.

PSB

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

PSMI

Power Supply Management Interface.

PSU

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

Q**QPI**

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

R**RADIUS**

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

RAID

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

RAM

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

RAS

Reliability, Availability, Serviceability.

Real-Time Clock

The Integrated Circuit in a computer that maintains the time and date.

Reset

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

Recoverable Error

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

RFB

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

RFI

Radio Frequency Interference.

RMII

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

RJ45

8-contact regular jack.

ROM

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

RTC

Real Time Clock.

S**SAS**

Serial Attached SCSI. A data 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.

SDR

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

SDRR

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

SDRAM

Synchronous Dynamic Random Access Memory.

A type of DRAM that runs at faster clock speeds than conventional memory. See DRAM.

SEL

System Event Log. A record of system management events. The information stored includes the name of the event, the date and time the event occurred and event data. Event data may include POST error codes that reflect hardware errors or software conflicts within the system.

A non-volatile storage area into the BMC and associated interfaces for storing System platform Event information for later retrieval.

Server Hardware Console

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

Simultaneous Multi-Threading

See Multi-Threading.

SMBIOS

System Management BIOS.

SM-BUS

System Management Bus.

SMI

System Management Interrupt.

SMP

Symmetrical Multi Processor. The processing of programs by multiple processors that share a common operating system and memory.

SMT

Simultaneous Multi-Threading.

SNC

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

SNMP

Simple Network Management Protocol. The protocol governing network management and the monitoring of network devices and their functions.

SOAP

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

Socket

Central Processing Unit multicore interface.

SOL

Serial Over LAN. Mechanism that enables the input and output of the serial port of a managed system to be redirected via an IPMI session over IP.

SPD

Serial Presence Detect. DIMM PROM.

SR

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

SRAM

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

SSH

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

Surprise Reset

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

SVGA

Super Video Graphics Array.

T**TCP**

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

TCP/IP

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

T&D

Tests and Diagnostics.

Thread

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

Thresholding

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

TKW

TUKWILA Intel Itanium Processor (4 cores per die).

U**Unplugging**

See Plugging / Unplugging.

URL

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

USB

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

V**VGA**

Video Graphics Array.

VLAN

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

VMM

Virtual Machine Monitor.

W**WAN**

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

Warm Reset

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

WOL

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

X**XCSI**

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

XML

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

XNC

External Node Controller. See BCS.

Y

No entries.

Z**ZOAR**

Double port Intel GB Ethernet chips.

Index

A

- Action request package, creating, 6-4
- Adding, resources (manual import), 2-9
- Already Monitored Resources tab, 2-14
- Autocall filter
 - configuring, 5-8
 - creating, 5-10
 - deleting, 5-15
 - editing, 5-11
 - viewing, 5-8
- Autocalls
 - configuring, 5-1
 - definition, 5-2
 - disabling, 5-4
 - enabling/disabling, 5-2
 - global policy, 5-4
 - introducing, 5-2
 - selecting specific policy, 5-6
 - setting up dispatch mode, 5-2
- Automatic clear SEL policy, enabling/disabling, 7-8
- Automatic discovery, 2-2

B

- BMC super user, changing password, 7-5
- Building
 - messages query report, 4-5
 - SEL query report, 4-2

C

- Changing
 - SEL event status, 4-7
 - super user password, 7-5
 - user account password, 7-4
- Clear SEL policy, enabling/disabling, 7-8
- Completing, site form, 7-7
- Configuration, initial, 1-6
- Configuring
 - autocall filters, 5-8
 - autocalls, 5-1
- Connecting , hardware console, 3-1
- Console
 - default password, 1-2
 - default username, 1-2
 - interface areas, 1-4
 - menu bar, 1-6
 - overview, 1-3
 - resource tree, 1-5
 - starting, 1-2
 - stopping, 1-7
 - tabs, 1-4
 - tree pane, 1-4
 - version number, 7-9
 - work pane, 1-4

- Creating
 - action request package, 6-4
 - intervention report, 6-2
 - resource group, 2-22
 - resource XML file, 2-4
 - user account, 7-2
- Custom filter (autocall)
 - creating, 5-10
 - deleting, 5-15
 - editing, 5-11
 - viewing, 5-8

D

- Default filter (autocall), viewing, 5-8
- Default password, 1-2
- Default username, 1-2
- DefaultGroup (definition), 2-22
- Deleting
 - autocall filter, 5-15
 - resource, 2-19
 - resource group, 2-26
 - user account, 7-3
- Disabling
 - autocalls, 5-2, 5-4
 - clear SEL policy, 7-8
 - resource monitoring, 2-20
- Discovery results
 - Already Monitored Resources tab, 2-14
 - Error on Discovered Resources tab, 2-15
 - Newly Discovered Resources tab, 2-12
 - troubleshooting, 2-16
- Discovery Results page description, 2-12
- Dispatch mode, setting up, 5-2
- Displaying, console version, 7-9

E

- Editing
 - autocall filter, 5-11
 - resource group, 2-24
- Electrical safety, x
- Enabling
 - autocalls, 5-2
 - clear SEL policy, 7-8
 - resource monitoring, 2-20
- Error messages (resource discovery), 2-16
- Error on Discovered Resources tab, 2-15
- Events, changing status, 4-7

F

- Filter. See Autocall filter
- FTP dispatch mode (autocalls), 5-3

G

Group. See Resource group

H

Hardware resource. See Resource

I

iCare Console. See Console

Importation methods

- manual (multiple resources - overview), 2-4
- resource tree, 2-2

Importing, resource XML file, 2-7

Initial, configuration, 1-6

Interface areas, 1-4

Intervention report

- creating, 6-2
- viewing list, 6-3

L

Laser safety, xi

Local dispatch mode (autocalls), 5-3

M

Manual import, multiple resources (overview), 2-4

Menu bar, 1-6

Messages query report, building, 4-5

Monitoring, resources, 4-1

Moving, resources, 2-27

N

Network Discovery Results. See Discovery results

Newly Discovered Resources tab, 2-12

Notices

- electrical safety, x
- laser safety, xi
- safety, x

O

Overview, 1-3

Q

Query reports (messages), building, 4-5

Query reports (SEL), building, 4-2

R

Resource

- connecting to consoles, 3-1
- deleting, 2-19
- Discovery Results page, 2-12
- monitoring, 4-1
- moving, 2-27
- viewing details, 4-10

Resource group

- creating, 2-22
- deleting, 2-26
- editing, 2-24

Resource monitoring, enabling/disabling, 2-20

Resource tree, 1-5

- automatic discovery, 2-2
- creating XML file, 2-4
- importation methods, 2-2
- manual import, 2-9
- XML file import, 2-7

Resource XML file, 2-7

Running, automatic discovery, 2-2

S

Safety, notices, x

SEL query report, building, 4-2

Selecting

- autocall specific policy, 5-6
- global autocall policy, 5-4

Site form, completing, 7-7

Starting

- console, 1-2
- resource hardware console, 3-1

Stopping, console, 1-7

Super user account

- changing password, 7-5
- default values, 7-5

Supported operating systems, xii

T

Tabs, 1-4

Tree pane, 1-4

Troubleshooting errors (resource discovery), 2-16

U

User account

- changing password, 7-4
- creating, 7-2
- deleting, 7-3

V

Version number, 7-9

Viewing

- autocall filter details, 5-8
- console version, 7-9
- intervention report list, 6-3
- resource details, 4-10

W

Work pane, 1-4

X

XML file (resource tree), 2-4

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

REFERENCE
86 A1 71FA 00